Configurar LSC no telefone IP com CUCM

Contents

Introduction

Este documento descreve como instalar um Locally Significant Certificate (LSC) em um Cisco Internet Protocol Phone (Cisco IP Phone).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Opções do modo de segurança de cluster do Cisco Unified Communications Manager (CUCM)
- Certificados X.509
- Certificados de instalação na fábrica (MICs)
- LSCs
- Operações de certificado CAPF (Certificate Authority Proxy Function)
- Segurança por padrão (SBD)
- Arquivos da Lista de Confiabilidade Inicial (ITL)

Componentes Utilizados

As informações neste documento são baseadas nas versões do CUCM que suportam SBD, ou seja, CUCM 8.0(1) e superior.

> **Observação**: ela se refere apenas a telefones que suportam Segurança por padrão (SBD). Por exemplo, os telefones 7940 e 7960 não suportam SBD, nem os telefones de conferência 7935, 7936 e 7937. Para obter uma lista de dispositivos que suportam SBD em sua versão do CUCM, navegue para **Cisco Unified Reporting > System Reports > Unified CM Phone Feature List** e execute um relatório em Feature: Security By Default.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

MICs versus LSCs

Se você usar a autenticação baseada em certificado para 802.1X ou Anyconnect Phone VPN, é importante entender a diferença entre MICs e LSCs.

Todos os telefones da Cisco vêm com um MIC pré-instalado na fábrica. Este certificado é assinado por um dos certificados de CA de fabricação da Cisco, pelo certificado de CA de fabricação da Cisco, CA de fabricação da Cisco SHA2, CAP-RTP-001 ou CAP-RTP-002. Quando o telefone apresenta esse certificado, ele prova que é um telefone Cisco válido, mas isso não valida se o telefone pertence a um cliente específico ou cluster CUCM. Pode ser um telefone invasor comprado no mercado aberto ou trazido de um site diferente.

Os LSCs, por outro lado, são instalados intencionalmente em telefones por um administrador e assinados pelo certificado CAPF do Editor do CUCM. Você configuraria o 802.1X ou o Anyconnect VPN para confiar apenas nos LSCs emitidos por autoridades de certificação CAPF conhecidas. Basear a autenticação de certificado em LSCs em vez de MICs fornece um controle muito mais granular sobre quais dispositivos de telefone são confiáveis.

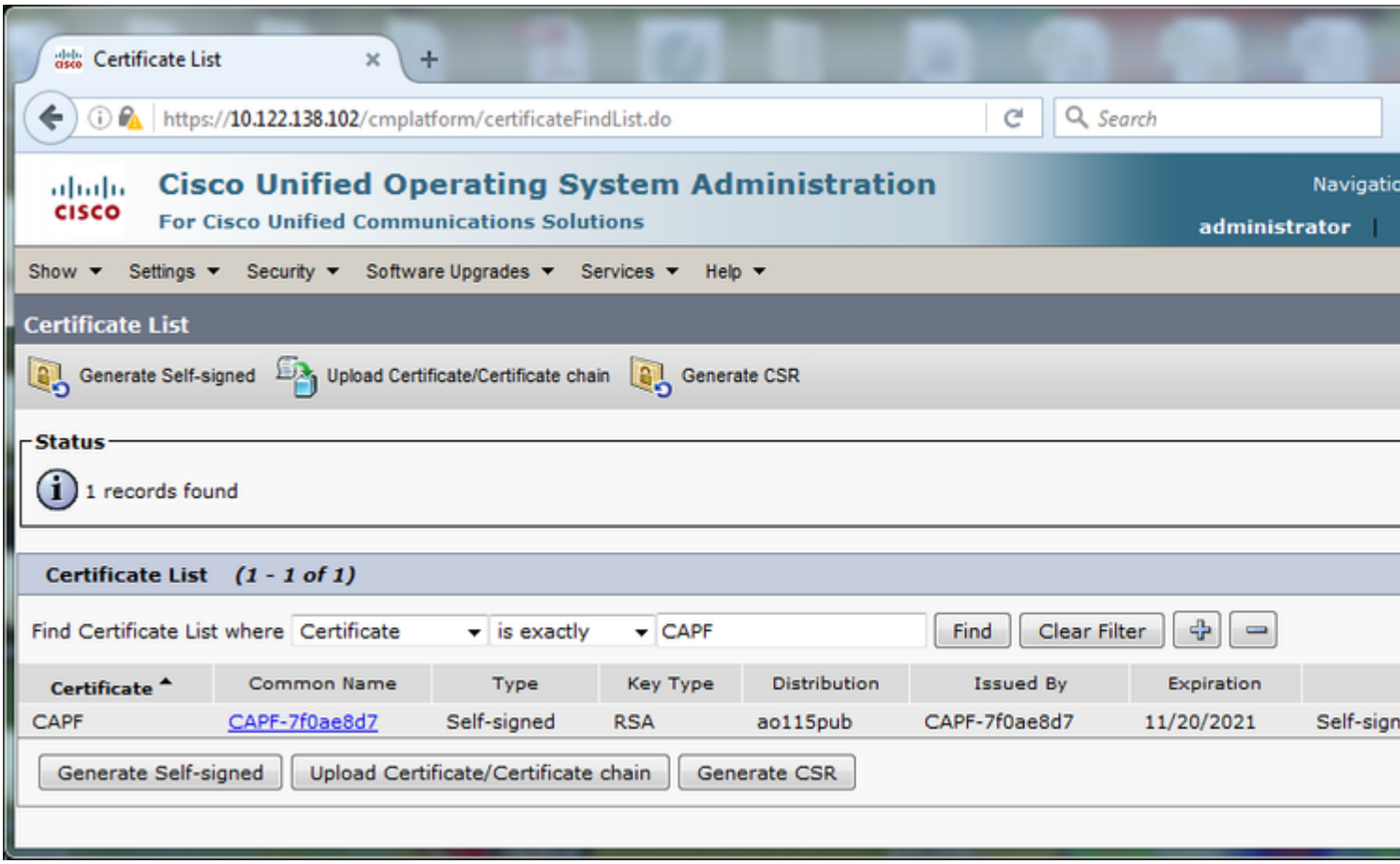
Configurar

Topologia de rede

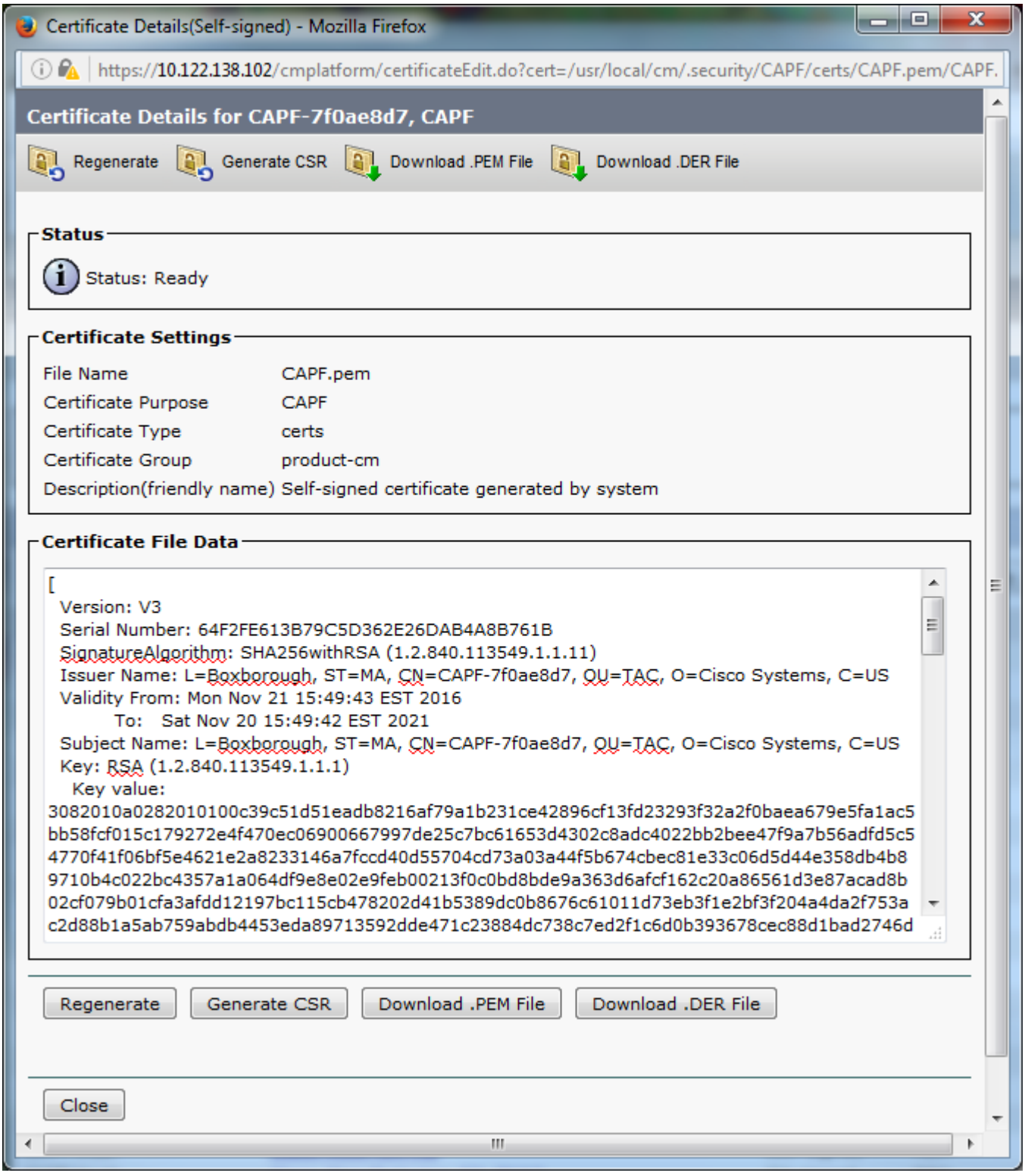
Estes servidores do laboratório CUCM foram usados para este documento:

- ao115pub - 10.122.138.102 - Publicador CUCM e servidor TFTP
- ao115sub - 10.122.138.103 - Assinante CUCM e servidor TFTP

Verifique se o certificado CAPF não expirou, nem está prestes a expirar em um futuro próximo. Navegue para **Cisco Unified OS Administration > Security > Certificate Management** e, em seguida, **Find Certificate List onde Certificate é exatamente CAPF**, como mostrado na imagem.



Clique em **Nome Comum** para abrir a página Detalhes do Certificado. Inspecione as datas Validade De: e Até: no painel **Dados do arquivo de certificado** para determinar quando o certificado expira, como mostrado na imagem.



Se o certificado CAPF tiver expirado, ou estiver prestes a expirar, recrie esse certificado. Não avance com o processo de instalação do LSC com um certificado CAPF expirado ou prestes a expirar. Isso evita a necessidade de reemitir LSCs em um futuro próximo devido à expiração do certificado CAPF. Para obter informações sobre como gerar novamente o certificado CAPF, consulte o artigo Processo de regeneração/renovação do certificado CUCM.

Da mesma forma, se você precisar que o seu certificado CAPF seja assinado por uma autoridade de certificação de terceiros, você terá a opção de fazer isso neste estágio. Conclua a geração do arquivo CSR (Certificate Signing Request) e a importação do certificado CAPF assinado agora ou continue a configuração com um LSC autoassinado para um teste preliminar. Se você precisar de um certificado CAPF assinado por terceiros, geralmente é sensato configurar esse recurso primeiro com um certificado CAPF

autoassinado, testar e verificar e depois reimplantar os LSCs assinados por um certificado CAPF assinado por terceiros. Isso simplificará a solução de problemas posteriores, se os testes com o certificado CAPF assinado por terceiros falharem.

Aviso: se você regenerar o certificado CAPF ou importar um certificado CAPF assinado por terceiros enquanto o serviço CAPF estiver ativado e iniciado, os telefones serão redefinidos automaticamente pelo CUCM. Conclua estes procedimentos em uma janela de manutenção quando for aceitável que os telefones sejam reinicializados. Para referência, consulte o bug da Cisco ID CSCue55353 - Adicionar aviso ao regenerar o certificado TVS/CCM/CAPF que os telefones reinicializam

---

Observação: se sua versão do CUCM suporta SBD, este procedimento de instalação do LSC se aplica independentemente se o cluster do CUCM está definido para modo misto ou não. O SBD faz parte do CUCM versão 8.0(1) e posterior. Nessas versões do CUCM, os arquivos ITL contêm o certificado para o serviço CAPF no Editor do CUCM. Isso permite que os telefones se conectem ao serviço CAPF para oferecer suporte a operações certificadas, como Instalação/Atualização e Solução de problemas.

Nas versões anteriores do CUCM, era necessário configurar o cluster para o modo misto para oferecer suporte a operações de certificado. Como isso não é mais necessário, isso reduz as barreiras para o uso de LSCs como certificados de identidade de telefone para autenticação 802.1X ou para autenticação de cliente AnyConnect VPN.

Execute o comando **show itl** em todos os servidores TFTP no cluster CUCM. Observe que o arquivo ITL contém um certificado CAPF.

Por exemplo, aqui está um trecho da saída do comando **show itl** do laboratório CUCM Subscriber ao115sub.

Observação: há uma entrada de Registro ITL neste arquivo com uma FUNÇÃO CAPF.

Observação: se o arquivo ITL não tiver uma entrada CAPF, faça login no editor do CUCM e confirme se o serviço CAPF está ativado. Para confirmar isso, navegue para **Cisco Unified Serviceability > Tools > Service Ativation > CUCM Publisher > Security** e ative o **Cisco Certificate Authority Proxy Function Service**. Se o serviço foi desativado e você acabou de ativá-lo, navegue para **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Server > CM Services** e reinicie o serviço Cisco TFTP em todos os servidores TFTP no cluster CUCM para gerar novamente o arquivo ITL. Além disso, certifique-se de não pressionar o bug da Cisco ID CSCuj78330.

Observação: depois de concluir, execute o comando **show itl** em todos os servidores TFTP no cluster CUCM para verificar se o certificado CAPF atual do editor do CUCM agora está incluído no arquivo.

<#root>

```
ITL Record #:1


----
```

BYTEPOS TAG LENGTH VALUE

------- --- ------ -----

1 RECORDLENGTH 2 727

2 DNSNAME 2

3 SUBJECTNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US

4 FUNCTION 2 CAPF

5 ISSUERNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US

6 SERIALNUMBER 16 64:F2:FE:61:3B:79:C5:D3:62:E2:6D:AB:4A:8B:76:1B

7 PUBLICKEY 270

8 SIGNATURE 256

11 CERTHASH 20 C3 E6 97 D0 8A E1 0B F2 31 EC ED 20 EC C5 BC 0F 83 BC BC 5E

12 HASH ALGORITHM 1 null

ITL Record #:2

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 6B:99:31:15:D1:55:5E:75:9C:42:8A:CE:F2:7E:EA:E8
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 05 9A DE 20 14 55 23 2D 08 20 31 4E B5 9C E9 FE BD 2D 55 87
12 HASH ALGORITHM 1 null

ITL Record #:3

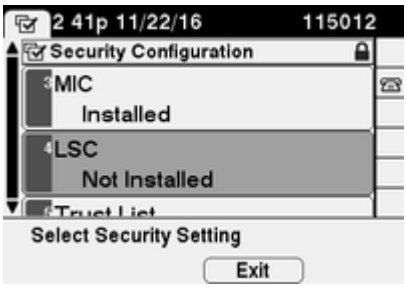
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1680

```
2 DNSNAME 2
3 SUBJECTNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 51:BB:2F:1C:EE:80:02:16:62:69:51:9A:14:F6:03:7E
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 963 DF 98 C1 DB E0 61 02 1C 10 18 D8 BA F7 1B 2C AB 4C F8 C9 D5 (SHA1 Hash HEX)
This etoken was not used to sign the ITL file.

 ITL Record #:4
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 65:E5:10:72:E7:F8:77:DA:F1:34:D5:E3:5A:E0:17:41
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 00 44 54 42 B4 8B 26 24 F3 64 3E 57 8D 0E 5F B0 8B 79 3B BF
12 HASH ALGORITHM 1 null

 ITL Record #:5
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)
This etoken was used to sign the ITL file.

 ITL Record #:6
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)

 ITL Record #:7
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1031
2 DNSNAME 9 ao115sub
3 SUBJECTNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
```

```
5 ISSUERNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 53:CC:1D:87:BA:6A:28:BD:DA:22:B2:49:56:8B:51:6C
7 PUBLICKEY 97
8 SIGNATURE 103
9 CERTIFICATE 651 E0 CF 8A B3 4F 79 CE 93 03 72 C3 7A 3F CF AE C3 3E DE 64 C5 (SHA1 Hash HEX)

The ITL file was verified successfully.
```

Com a entrada CAPF confirmada como uma entrada no ITL, você pode concluir uma operação de certificado em um telefone. Neste exemplo, um certificado RSA de 2048 bits é instalado pelo uso da autenticação de sequência nula.

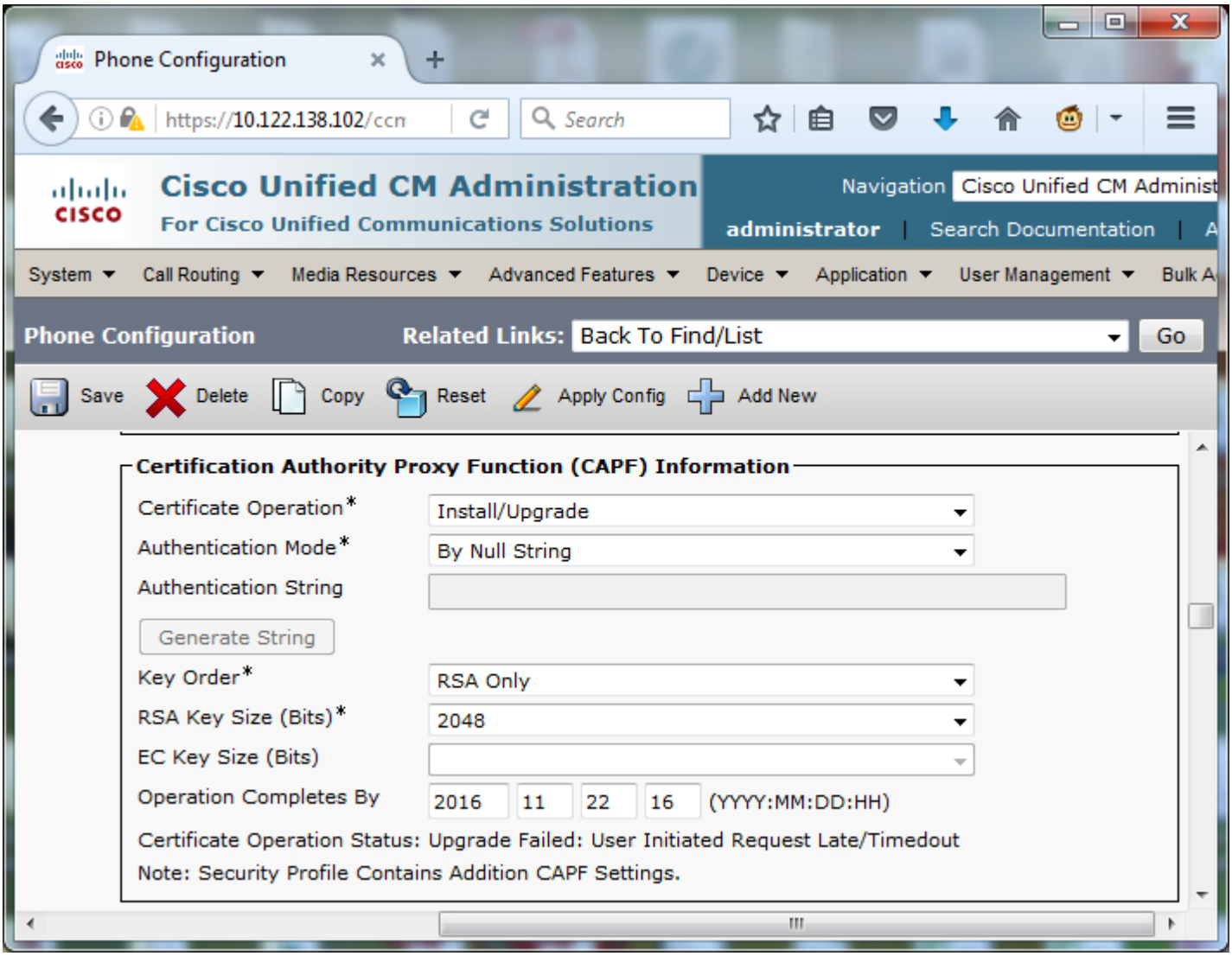
No telefone, verifique se um LSC ainda não está instalado, conforme mostrado na imagem. Por exemplo, em um telefone da série 79XX, navegue para **Settings > 4 - Security Configuration > 4 - LSC**.



Abra a página de configuração do telefone para o seu telefone. Navegue até **Cisco Unified CM Administration > Device > Phone**.

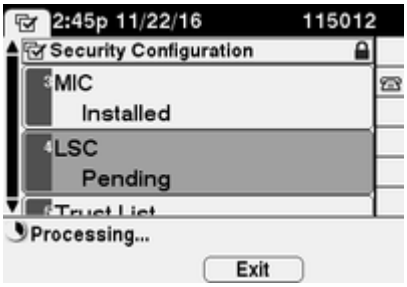
Insira estes detalhes na seção Informações de CAPF da configuração do telefone, conforme mostrado na imagem:

- Para Operação de Certificado, escolha **Instalar/Atualizar**
- Para o modo de autenticação, escolha **Por sequência de caracteres nula**
- Para este exemplo, deixe a Ordem de chaves, Tamanho da chave RSA (Bits) e Tamanho da chave EC (Bits) definidos para os padrões do sistema.
- Em Operação Concluída em, informe uma data e hora que seja pelo menos uma hora no futuro.

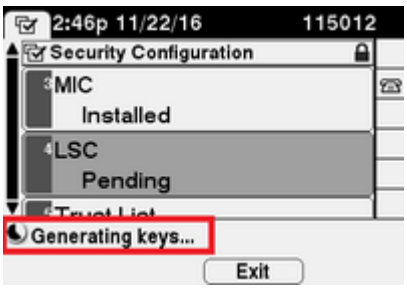


Salve suas alterações de configuração e **Aplique a configuração**.

O status LSC no telefone muda para Pendente, como mostrado na imagem.



O telefone gera teclas conforme mostrado na imagem.



O telefone é redefinido e, quando a redefinição é concluída, o status LSC do telefone muda para Instalado, como mostrado na imagem.

Isso também é visível em Mensagens de status no telefone, conforme mostrado na imagem.

Verificar

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

Para verificar a instalação do certificado LSC em vários telefones, consulte a seção Gerar Relatório CAPF do Guia de Segurança do Cisco Unified Communications Manager, Versão 11.0(1). Como alternativa, você pode exibir os mesmos dados na interface da Web de administração do CUCM usando o procedimento Find Phones by LSC Status ou Authentication String.

Para obter cópias dos certificados LSC instalados nos telefones, consulte o artigo Como recuperar certificados dos telefones IP da Cisco.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Nenhum servidor CAPF válido

Falha na instalação do LSC. As mensagens de status do telefone mostram **No valid CAPF server**. Isso indica que não há entrada CAPF no arquivo ITL. Verifique se o serviço CAPF foi ativado e reinicie o serviço TFTP. Verifique se o arquivo ITL contém um certificado CAPF após a reinicialização, redefina o telefone para capturar o arquivo ITL mais recente e repita a operação do certificado. Se a entrada do servidor CAPF no menu de configurações de segurança do telefone for exibida como nome de host ou nome de domínio totalmente qualificado, confirme se o telefone é capaz de resolver a entrada para um endereço IP.

LSC: Falha na Conexão

Falha na instalação do LSC. As mensagens de status do telefone mostram **LSC: Connection Failed**. Isso pode indicar uma destas condições:

- Incompatibilidade entre o certificado CAPF no arquivo ITL e o certificado atual; o serviço CAPF está em uso.
- O serviço CAPF foi interrompido ou desativado.
- O telefone não pode acessar o serviço CAPF pela rede.

Verifique se o serviço CAPF está ativado, reinicie o serviço CAPF, reinicie os serviços TFTP em todo o cluster, reinicie o telefone para obter o arquivo ITL mais recente e repita a operação do certificado. Se o problema persistir, capture um pacote do telefone e do Editor do CUCM e analise para ver se há comunicação bidirecional na porta 3804, a porta de serviço CAPF padrão. Caso contrário, pode haver um problema de rede.

LSC: Falha

Falha na instalação do LSC. As mensagens de status do telefone mostram **LSC: Failed**. A página da Web Configuração do telefone mostra **Status da operação de certificado: Falha na atualização: Solicitação iniciada pelo usuário atrasada/tempo limite**. Isso indica que a Operação é Concluída por hora e data expirou ou está no passado. Insira uma data e uma hora para o futuro e repita a operação do certificado.

LSC: Operação Pendente

Falha na instalação do LSC. As mensagens de status do telefone mostram **LSC: Connection Failed**. A página de configuração do telefone mostra **Status da operação de certificado: Operação pendente. Há diferentes motivos pelos quais é possível ver o status Status da operação de certificado: Operação pendente**. Alguns deles podem incluir:

- O ITL no telefone é diferente do usado atualmente nos servidores TFTP configurados.
- Problemas com ITL corrompidos. Quando isso acontece, os dispositivos perdem seu status confiável e o comando **utils itl reset localkey** precisa ser executado a partir do Editor CUCM para forçar os telefones a usar agora o certificado ITLRecovery. Se o cluster estiver em modo misto, você precisará usar o comando **utils ctl reset localkey.** Em seguida, você vê um exemplo do que pode ver quando tenta visualizar um ITL corrompido na CLI do CUCM. Se houver um erro quando você tentar visualizar o ITL e tentar executar o comando **utils itl reset localkey**, mas você vir o segundo erro, este pode ser um defeito Cisco bug ID CSCus33755. Confirme se a versão do CUCM é afetada.

```
admin:show itl
Length of ITL file: 0
ITL File not found. To generate an ITL file, activate or restart the Cisco TFTP service as thi
servers.
Error parsing the ITL File.


admin:utils itl reset localkey
Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Unable to determine the active and running  TFTP nodes in the cluster
Ensure that the DB replication is working on all nodes and the correct Password has been en
Then retry the command

Executed command unsuccessfully
chmod: changing permissions of `/var/log/active/cm/trace/dbl/sdi/replication_scripts_output
```

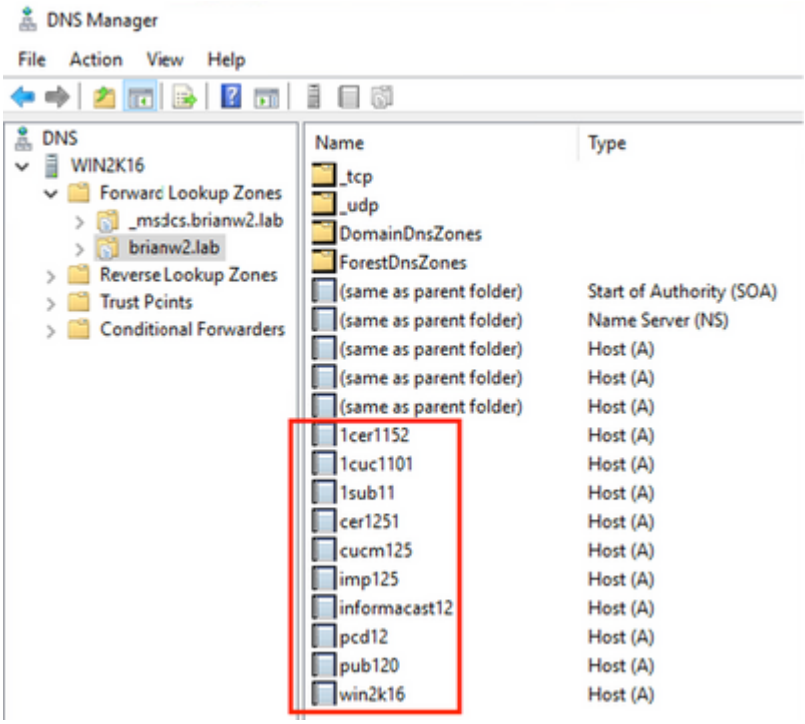
- Os telefones não autenticam o novo LSC devido a uma falha de TVS.
- O telefone usa o certificado MIC, mas a seção Informações da função de proxy da autoridade de

certificação (CAPF) na página de configuração dos telefones tem o Modo de autenticação definido como por Certificado existente (Precedência para LSC).
- O telefone não consegue resolver o FQDN do CUCM.

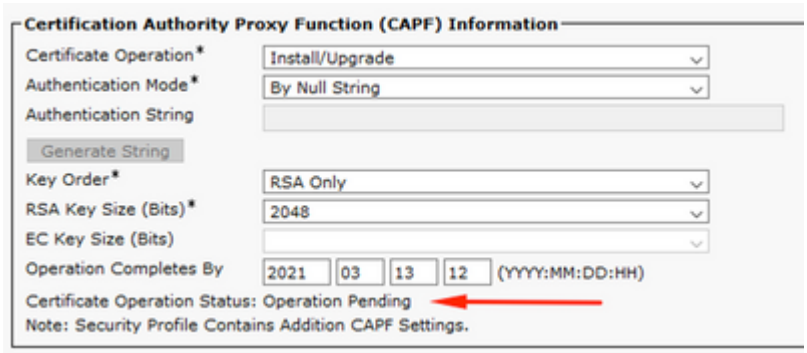
Para o último cenário, um ambiente de laboratório é configurado para simular o que você veria nos registros se um telefone não fosse capaz de resolver o FQDN do CUCM. Atualmente, o laboratório está configurado com estes servidores:

- Editor e assinante do CUCM executando a versão 11.5.1.15038-2
- Configuração do Windows 2016 Server como meu servidor DNS

Para o teste, não há uma entrada DNS para o servidor CUCM PUB11 configurado.



Tentativa de envio de um LSC para um dos telefones (8845) no laboratório. Veja se ele ainda mostra o Status de operação de certificado: Operação pendente.

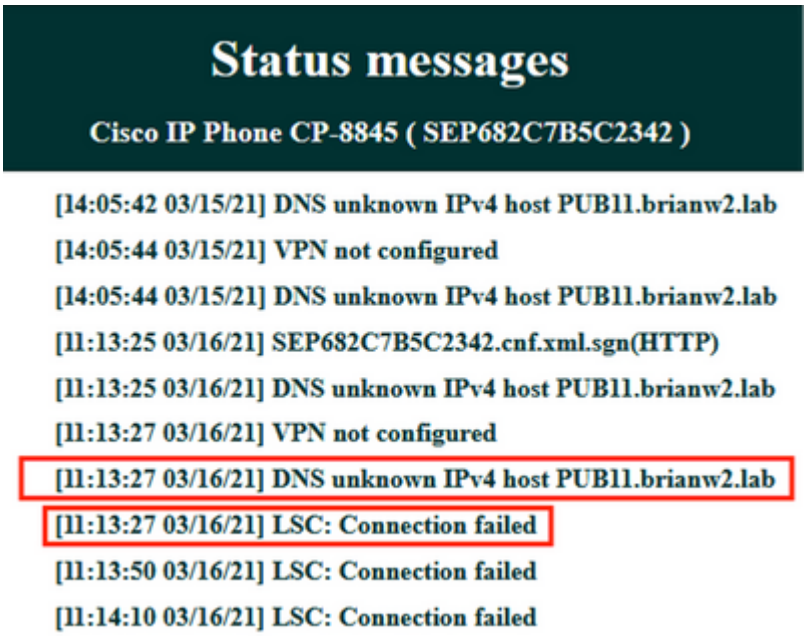


Nos registros do console do telefone, consulte o telefone tenta consultar seu cache local (127.0.0.1), antes de encaminhar a consulta para o endereço do servidor DNS configurado.

```
0475 INF Mar 12 15:07:53.686410 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0476 INF Mar 12 15:07:53.686450 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
0477 INF Mar 12 15:07:53.694909 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
```

```
0478 INF Mar 12 15:07:53.695263 dnsmasq[12864]: reply PUB11.brianw2.lab is NXDOMAIN-IPv4
0479 INF Mar 12 15:07:53.695833 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0480 INF Mar 12 15:07:53.695865 dnsmasq[12864]: cached PUB11.brianw2.lab is NXDOMAIN-IPv4
0481 WRN Mar 12 15:07:53.697091 (12905:13036) JAVA-configmgr MQThread|NetUtil.traceIPv4DNSErrors:? - DNS

++ However, we see that the phone is not able to resolve the FQDN of the CUCM Publisher. This is because

0482 ERR Mar 12 15:07:53.697267 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Failed to

++ Afterwards, we see the CAPF operation fail. This is expected because we do not have a DNS mapping for

0632 NOT Mar 12 15:07:55.760715 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty:? - Ce
0633 NOT Mar 12 15:07:55.761649 (322:17812) SECUREAPP-RCAPF_START_MODE: Start CAPF - mode:[1]([NULL_STR]
0634 NOT Mar 12 15:07:55.761749 (322:17812) SECUREAPP-CAPF_CLNT_INIT:CAPF clnt initialized
0635 NOT Mar 12 15:07:55.761808 (322:17812) SECUREAPP-CAPFClnt: SetDelayTimer - set with value <0>
0636 ERR Mar 12 15:07:55.761903 (322:17812) SECUREAPP-Sec create BIO - invalid parameter.
0637 ERR Mar 12 15:07:55.761984 (322:17812) SECUREAPP-SEC_CAPF_BIO_F: CAPF create bio failed
0638 ERR Mar 12 15:07:55.762040 (322:17812) SECUREAPP-SEC_CAPF_OP_F: CAPF operation failed, ret -7
0639 CRT Mar 12 15:07:55.863826 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty$1:? -

++ What we would expect to see is something similar to the following where DNS replies with the IP addre

4288 INF Mar 12 16:34:06.162666 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
4289 INF Mar 12 16:34:06.162826 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
4290 INF Mar 12 16:34:06.164908 dnsmasq[12864]: reply PUB11.brianw2.lab is X.X.X.X
4291 NOT Mar 12 16:34:06.165024 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Resolve Tv
```

Consulte nas mensagens de status do telefone abaixo que o telefone não é capaz de resolver PUB11.brianw2.lab. Depois, veja a mensagem **LSC: Connection failed**.



Defeitos a considerar:

ID de bug da Cisco CSCub62243 - a instalação do LSC falha intermitentemente e, posteriormente, congela o servidor CAPF

Defeito de aprimoramento a ser considerado:

ID de bug da Cisco CSCuz18034 - É necessário gerar relatórios para os endpoints instalados do LSC junto com o status de expiração

Informações Relacionadas

Esses documentos fornecem mais informações sobre o uso de LSCs no contexto da autenticação do AnyConnect VPN Client e da autenticação 802.1X.

- Telefone VPN AnyConnect - Solução de problemas de telefones IP, ASA e CUCM
- Serviços de rede baseados em identidade: Guia de implantação e configuração de telefonia IP em redes habilitadas para IEEE 802.1X

Há também um tipo avançado de configuração LSC, em que os certificados LSC são assinados diretamente por uma autoridade de certificação de terceiros, não o certificado CAPF.

Para obter detalhes, consulte: Exemplo de configuração de geração e importação de LSCs assinados por CA de terceiros do CUCM

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.