

Ative o recurso de configuração criptografada no CUCM

Contents

[Introduction](#)

[Informações de Apoio](#)

[Visão geral do recurso de configuração criptografada](#)

[Ativar recurso de configuração criptografada](#)

[Troubleshoot](#)

Introduction

Este documento descreve o uso de arquivos de configuração criptografados do telefone no Cisco Unified Communications Manager (CUCM).

Informações de Apoio

O uso de arquivos de configuração criptografados para telefones é um recurso de segurança opcional que está disponível no CUCM.

Não é necessário executar o cluster CUCM no modo Misto para que este recurso funcione corretamente, pois as informações do certificado da Função de Proxy da Autoridade de Certificação (CAPF) estão contidas no arquivo da Lista de Confiança de Identidades (ITL).

Note: Esse é o local padrão para todas as versões 8.X e posteriores do CUCM. Para versões do CUCM anteriores à versão 8.X, você deve garantir que o cluster seja executado no modo Misto se desejar usar esse recurso.

Visão geral do recurso de configuração criptografada

Esta seção descreve o processo que ocorre quando os arquivos de configuração criptografada do telefone são usados no CUCM.

Quando você habilita esse recurso, redefine o telefone e faz o download do arquivo de configuração, você recebe uma solicitação para o arquivo com uma extensão `.cnf.xml.sgn`:

```
73.824626 10.147.94.55 10.48.46.4 HTTP GET /ITLSEPA45630BBFA40.tlv HTTP/1.1
74.110351 10.147.94.55 10.48.46.4 HTTP GET /SEPA45630BBFA40.cnf.xml.sgn HTTP/1.1
```



No entanto, depois que o recurso de configuração criptografada é ativado no CUCM, o serviço

TFTP não gera mais um arquivo de configuração completo com a extensão **.cnf.xml.sgn**. Em vez disso, ele gera o arquivo de configuração parcial, como mostrado no próximo exemplo.

Note: Quando você usa esse método pela primeira vez, o telefone compara o hash MD5 do certificado do telefone no arquivo de configuração com o hash MD5 do LSC (Locally Significant Certificate) ou do MIC (Manufacturing Installed Certificate).

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
```

```
</device>
```

Se o telefone identificar um problema, ele tentará iniciar uma sessão com o CAPF, a menos que o modo de autenticação CAPF corresponda a *Por sequências de caracteres de autenticação*, caso em que você deve inserir manualmente a string. Aqui estão alguns problemas que o telefone pode identificar:

- O hash não corresponde.
- O telefone não contém um certificado.
- O valor MD5 está em branco (como no exemplo anterior).



Note: O telefone inicia uma sessão TLS (Transport Layer Security) para o serviço CAPF na porta 3804 por padrão.

O certificado CAPF deve ser conhecido para o telefone, portanto ele deve ser incluído no arquivo ITL ou no arquivo CTL (Certificate Trust List, Lista de confiança de certificado) (se o cluster for executado no modo Misto).

76.804108	10.147.94.55	10.48.46.4	TCP	51292 > cisco-con-capf [ACK] seq=1 ack=1 win=5840 Len=0 Tsv=159397051 Tser=162819875
76.805662	10.147.94.55	10.48.46.4	TLSv1	Client Hello
76.805690	10.48.46.4	10.147.94.55	TCP	cisco-con-capf > 51292 [ACK] seq=1 ack=55 win=5792 Len=0 Tsv=162819927 Tser=159397051
76.805866	10.48.46.4	10.147.94.55	TLSv1	server Hello, certificate, server Hello done
76.855825	10.147.94.55	10.48.46.4	TCP	51292 > cisco-con-capf [ACK] seq=55 ack=720 win=7280 Len=0 Tsv=159397056 Tser=162819927
76.864678	10.147.94.55	10.48.46.4	TLSv1	Client Key Exchange, change cipher spec, Encrypted Handshake Message
76.870861	10.48.46.4	10.147.94.55	TLSv1	change cipher spec, Encrypted Handshake Message
76.871012	10.48.46.4	10.147.94.55	TLSv1	Application data, Application data

Depois que a comunicação CAPF é estabelecida, o telefone envia informações ao CAPF sobre o LSC ou o MIC que é usado. Em seguida, o CAPF extrai a chave pública do telefone do LSC ou do MIC, gera um hash MD5 e armazena os valores para a chave pública e o hash de certificado no banco de dados do CUCM.

```
admin:run sql select md5hash,name from device where name='SEPA45630BBFA40'
```

```
md5hash name
```

```
=====
6e566143c1c14566c9da943d949a79c8 SEPA45630BBFA40
```

Depois que a chave pública é armazenada no banco de dados, o telefone é redefinido e solicita um novo arquivo de configuração. O telefone tenta baixar o arquivo de configuração com a extensão **cnf.xml.sgn** novamente.



```
128.078706 10.147.94.55 10.48.46.4 HTTP GET /SEPA45630BBFA40.cnf.xml.sgn HTTP/1.1
```

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
```

```
</device>
```

O telefone compara o **cerHash** novamente e, se não detectar o problema, ele faz o download do arquivo de configuração criptografado com a extensão **.cnf.xml.enc.sgn**.



```
130.708816 10.147.94.55 10.48.46.4 HTTP GET /SEPA45630BBFA40.cnf.xml.enc.sgn HTTP/1.1
```

```
.....c..)CN=cucm85;OU=It;O=Cisco;L=KRK;ST=PL;C=PL....Z.....)CN=cucm85;
OU=It;O=Cisco;L=KRK;ST=PL;C=PL.....
.....C.<...Y6.Lh.|(..w+...0.a.&
O.....V...T...Z..R^..f...|.=.e.@...5.....G...[.....n.....=
.A..H.(...Z...{.!%[... SEPA45630BBFA40.cnf.xml.enc.sgn...R.DD..M.....
Uu.C..@.....
.....m.b.....6y ..x.^b..-8.^'..^'.4.<Wb.n.....5...we.0@..g..
V7.,..r.9
Qs>..).w....pt/...}A.']
.r.t%G..d_./u.rEI.pr.F
....M..r...o.N
.=..g.^P....Pz....J..E.S...d|Z).....J..&..I....7.r..g8.{f..o.....:~...U...5G+V.
[...]
```

Ativar recurso de configuração criptografada


Para ativar os arquivos de configuração criptografados do telefone, você deve criar um novo (ou editar um atual) Perfil de segurança do telefone e atribuí-lo ao telefone. Conclua estes passos para habilitar o recurso de configuração criptografada no CUCM:

1. Faça login na página de administração do CUCM e navegue até **System > Security > Phone Security Profile**:


Security	Certificate
Application Server	Phone Security Profile
Licensing	SIP Trunk Security Profile
Geolocation Configuration	CUMA Server Security Profile

2. Copie um perfil de segurança de telefone atual ou crie um novo e marque a caixa de seleção **TFTP Encrypted Config**:

Phone Security Profile Configuration

 Save

Status

 Status: Ready

Phone Security Profile Information

Product Type: Cisco 7942
Device Protocol: SCCP
Name*
Description
Device Security Mode ▼
 TFTP Encrypted Config

Phone Security Profile CAPF Information

Authentication Mode* ▼
Key Size (Bits)* ▼
 Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

3. Atribua o perfil ao telefone:

Protocol Specific Information

Packet Capture Mode* ▼
Packet Capture Duration
BLF Presence Group* ▼
Device Security Profile* ▼
SUBSCRIBE Calling Search Space ▼
 Unattended Port
 Require DTMF Reception
 RFC2833 Disabled

Device Security Profile* dropdown menu items:
 -- Not Selected --
 Cisco 7942 - Standard SCCP Encrypted Config
 Cisco 7942 - Standard SCCP Non-Secure Profile
 Universal Device Template - Model-independent Security Profile

Troubleshoot

Conclua estes passos para solucionar problemas do sistema em relação ao recurso de configuração criptografada:

1. Certifique-se de que o serviço CAPF está ativo e é executado corretamente no nó Publisher no cluster CUCM.
2. Baixe o arquivo de configuração parcial e verifique se a porta e o endereço IP do serviço CAPF estão acessíveis pelo telefone.

3. Verifique a comunicação TCP na porta 3804 para o nó do Publisher.
4. Execute o comando SQL (Structured Query Language) mencionado anteriormente para verificar se o serviço CAPF tem informações sobre o LSC ou o MIC usado pelo telefone.
5. Se o problema persistir, talvez seja necessário coletar informações adicionais do sistema. Reinicie o telefone e reúna estas informações:

Registros do console do telefone
Logs do Cisco TFTP
Logs do Cisco CAPF
Capturas de pacotes do CUCM e do telefone

Consulte estes recursos para obter informações adicionais sobre como executar capturas de pacotes do CUCM e do telefone:

- [Coleta de rastreamentos do CUCM 8.6.2 para um TAC SR](#)
- [Captura de pacote no modelo do dispositivo Unified Communications Manager](#)
- [Coletando uma captura de pacote de um telefone IP da Cisco](#)

Nos registros e capturas de pacotes, você deve garantir que o processo descrito nas seções anteriores funcione corretamente. Especificamente, verifique se:

- O telefone baixa o arquivo de configuração parcial com as informações de CAPF corretas.
- O telefone se conecta via TLS ao serviço CAPF e as informações sobre o LSC ou o MIC são atualizadas no banco de dados.
- O telefone baixa o arquivo de configuração criptografado completo.