

Solucionar problemas comuns com renovação de certificado no CUCM

Introdução

Este documento descreve problemas comuns após a regeneração de certificados no Cisco Unified Communications Manager (CUCM) e como resolvê-los.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Processo de renovação de certificado do CUCM
- Interface GUI do CUCM
- Servidores Expressway
- Registro de dispositivo com processo CUCM
- Função de proxy da autoridade de certificação
- Guia de segurança do Cisco Unified Communications Manager

Componentes Utilizados

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







- CUCM versão 15

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Impacto comercial

Esta tabela exibe o impacto comercial de cada renovação de certificado em sua operação. Revise as informações cuidadosamente. Renove os certificados necessários após horas ou em períodos de silêncio, com base no nível de risco de cada certificado.

 Low Impact
  Medium Impact.
  High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat		-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec		-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF		CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager		CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS		ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery		CTL + ITL	Signer or SAST backup for ITL/CTL	All	

Cenário 1: Telefones não registrados após o Call Manager, TVS e renovação de certificado ITL



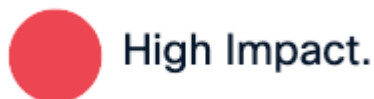
Note: Este cenário se aplica a implantações sob o CUCM de modo misto e clusters não seguros, além disso, aplica-se aos certificados autoassinados e certificados CA.

Quando os certificados Call Manager, TVS e ITL expiraram e foram renovados ao mesmo tempo, isso faz com que todos os nossos telefones fiquem em um estado não registrado que causa um grande impacto no sistema, esse é um comportamento esperado quando acionamos os telefones para não confiar no CUCM.

Verificação

1. Verifique se os certificados já expiraram em Cisco Unified OS Administration >Security > Certificate Management

Esta etapa afeta todos os telefones, inclusive telefones registrados. Certifique-se de executar isso após o horário comercial.



Cenário 2: o logon único não funciona após a renovação do certificado Tomcat



Note: Este cenário pode ser aplicado a implantações que usam acordo por nó ou em todo o cluster para a configuração de logon único

Login no CUCM com Single Sign-on (SSO), ele exibe uma mensagem de erro "Erro ao processar a resposta saml" ou "Erro ao processar a resposta saml Falha ao descriptografar a chave secreta"

Verificação

1. Certifique-se de que todos os nós contenham um certificado tomcat válido se autoassinado ou contiver o novo certificado tomcat multi-san associado.
2. Use `set samltrace level debug` em todos os nós do CUCM via CLI para ativar logs SSO no nível de depuração
3. Recrie o problema fazendo login novamente no CUCM e use o método SSO.
4. Colete logs de SSO do Tomcat após o incidente e verifique se você recebeu esta mensagem:

- ```
2026-01-10 06:06:31,274 ERROR [http-nio-81-exec-157] cpi.sso.saml.sp.security.authentication
com.sun.identity.saml2.common.SAML2Exception: Failed to decrypt the secret key.
 at com.sun.identity.saml2.xmlenc.FMEncProvider.getEncryptionKey(FMEncProvider.
 at com.sun.identity.saml2.xmlenc.FMEncProvider.decrypt(FMEncProvider.java:607)
 at com.sun.identity.saml2.assertion.impl.EncryptedAssertionImpl.decrypt(Encryp
...

```

### Solução

Exporte os metadados do CUCM após a renovação do certificado do Tomcat e importe-os para o servidor do provedor de identidade para garantir que eles tenham o novo certificado tomcat para essa comunicação.

Procedimento para renovar o tomcat com implantação de SSO habilitada:



Caution: O Centro de assistência técnica (TAC) recomenda as próximas etapas para evitar qualquer problema após a renovação do certificado do Tomcat, recomendar a execução desse procedimento após o horário comercial.

---

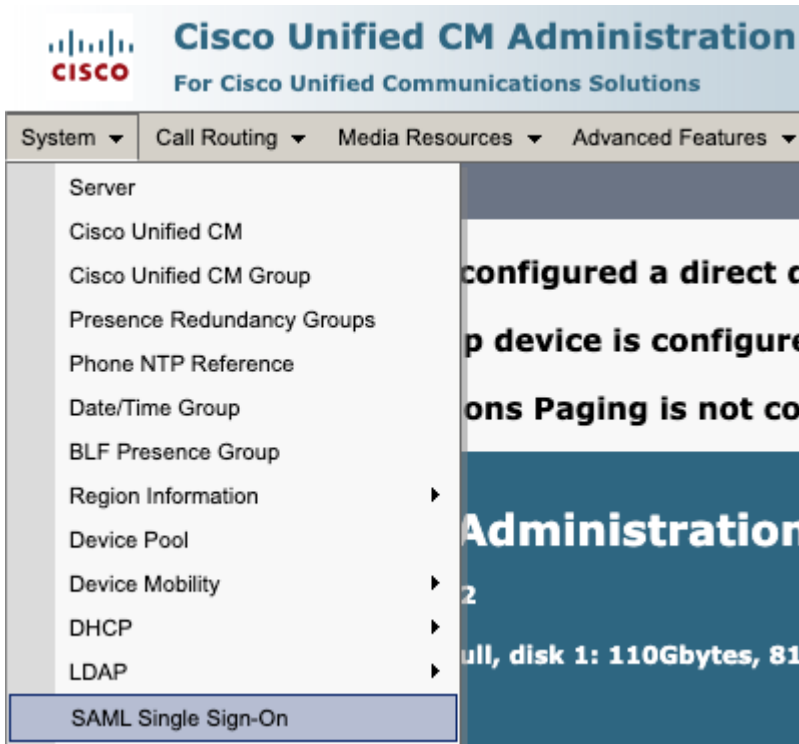


Low Impact

1. Desative o SSO em todos os nós do CUCM



- Acesso à administração do CM > Sistema > Logon Único SAML



- Selecione Disable SAML SSO



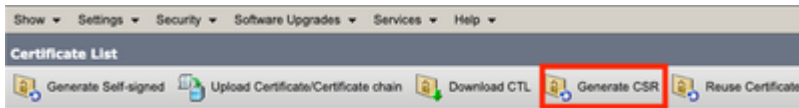
- Esse processo precisa ser executado em todos os outros nós por meio da GUI se o acordo por nó for usado.

## 2. Remova o certificado Tomcat no cluster CUCM



Procedimento geral para renovar o certificado multi-san Tomcat no cluster CUCM:

- Navegue até Administração do SO > Segurança > Gerenciamento de certificado.
- Selecione Gerar CSR



- Selecione Tomcat em Certificate Propuse.
- Selecione Multi-SAN em Distribuição.
- Verifique se todos os nós no cluster estão listados em Domínios preenchidos automaticamente.

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose\*\* tomcat

Distribution\* Multi-server(SAN)

Common Name\* cm15-pub-...cisco.com

Include OU in CSR

Subject Alternate Names (SANs)

Auto-populated Domains

|                       |
|-----------------------|
| cm15-pub-...cisco.com |
| cm15-sub-...cisco.com |

Parent Domain ...cisco.com

Other Domains

Selecionar archivo Sin archivos seleccionados  
Please import .TXT file only.

Add

Key Type\*\* RSA

Key Length\* 2048

Hash Algorithm\* SHA256

Generate Close

- Selecione Gerar. Verifique se o CSR foi criado em todos os nós no cluster.
- Baixe o CSR gerado do editor do CUCM e assine-o com um servidor de autoridade de certificação (CA).
- Vá para Administração de SO > Segurança > Gerenciamento de certificado. Selecione Carregar certificado/Cadeia de certificados.
- Carregue certificados CA como Tomcat-trust.
- Repita a etapa 6 e agora carregue o certificado assinado do Tomcat como Tomcat.
- Uma vez concluído e verificado que todos os nós têm o novo certificado tomcat aplicado, reinicie o serviço Tomcat por meio da CLI em todos os nós no cluster com este comando `utils service restart Cisco Tomcat`.

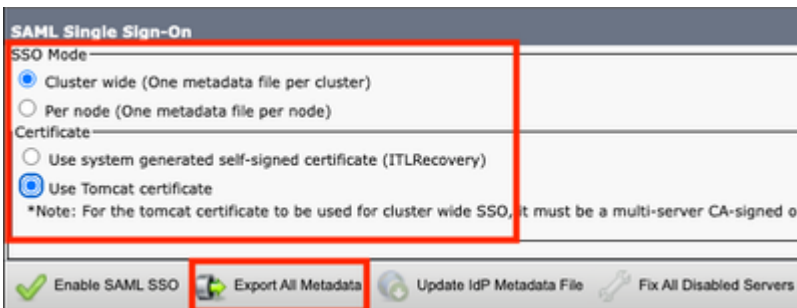
Para obter mais informações, consulte esta documentação:

- [Regenerar certificado autoassinado do Tomcat](#)
- [Regenerar o certificado assinado pela CA do Tomcat.](#)

### 3. Exportar metadados do provedor de serviços (SP)



- Vá para administração CM > Sistema > Logon único
- Configure as opções de SSO (neste caso, cluster wide no modo SSO e Use tomcat certificate no certificado está configurado como exemplo) e selecione export all metadata

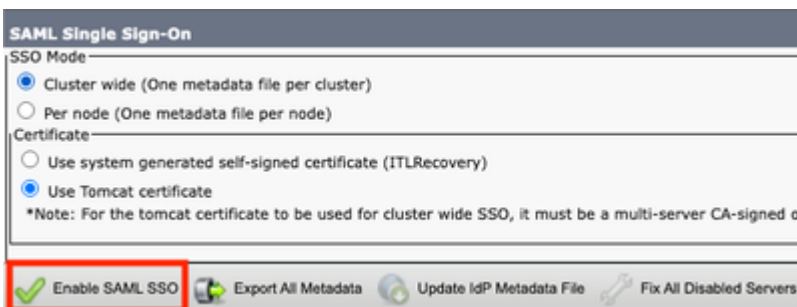



- Importe metadados da controladora de armazenamento para o servidor IdP (Identity Provider, Provedor de identidade). Para obter mais informações, consulte [Configurar SAML SSO no Provedor de Identidade](#)

### 4. Habilitar SSO no cluster CUCM




- Vá para administração CM > Sistema > Logon único
- Com as mesmas opções de SSO selecionadas durante a exportação de metadados do CUCM, selecione Enable SAML SSO e selecione continue.



 Web server connections will be restarted


Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

 Click "Export All Metadata" button


If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.  
If IDP is provisioned with cluster-wide SP metadata, you need to enable cluster-wide SAML SSO. If IDP is provisioned with per-node SP metadata, you need to enable per-node SAML SSO.

- Se estiver em todo o cluster, esta etapa estará disponível para verificar o certificado multi-san em todos os nós, selecione Test for multi-server tomcat certificate. depois de concluído, selecione Avançar.

**SAML Single Sign-On Configuration**

 Next

**Status**

 Status: Ready

**Test for Multi-Server tomcat certificate**

The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate CSR
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Download the CSR and get it signed from the CA of your choice
- 7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
- 8) Restart Tomcat service on all the nodes in the cluster
- 9) Restart TFTP service on all the TFTP nodes in the cluster

For self-signed Multi-server tomcat certificate:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate self signed Multi-server tomcat certificate
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Restart Tomcat service on all the nodes in the cluster
- 7) Restart TFTP service on all the TFTP nodes in the cluster

If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage

- Carregue os metadados de IdP, selecione Import IdP Metadata e, depois de concluir, selecione Next

**SAML Single Sign-On Configuration**

Next

**Status**

Status: Ready

Import succeeded for all servers

**Import the IdP Metadata Trust File**

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1) Select the IdP Metadata Trust File

Choose File No file chosen

2) Import this file to the Collaboration servers

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

Import IdP Metadata

Import succeeded for all servers

Next Cancel

- Em Test SSO Setup, selecione um usuário com o grupo Standard CCM Super Users atribuído e selecione Run SSO Test até obter êxito.

**SAML Single Sign-On Configuration**

Back

**Status**

The server metadata file must be installed on the IdP before this test is run.

**Test SSO Setup**

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any

1) Pick a valid username to use for this test

You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.

Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

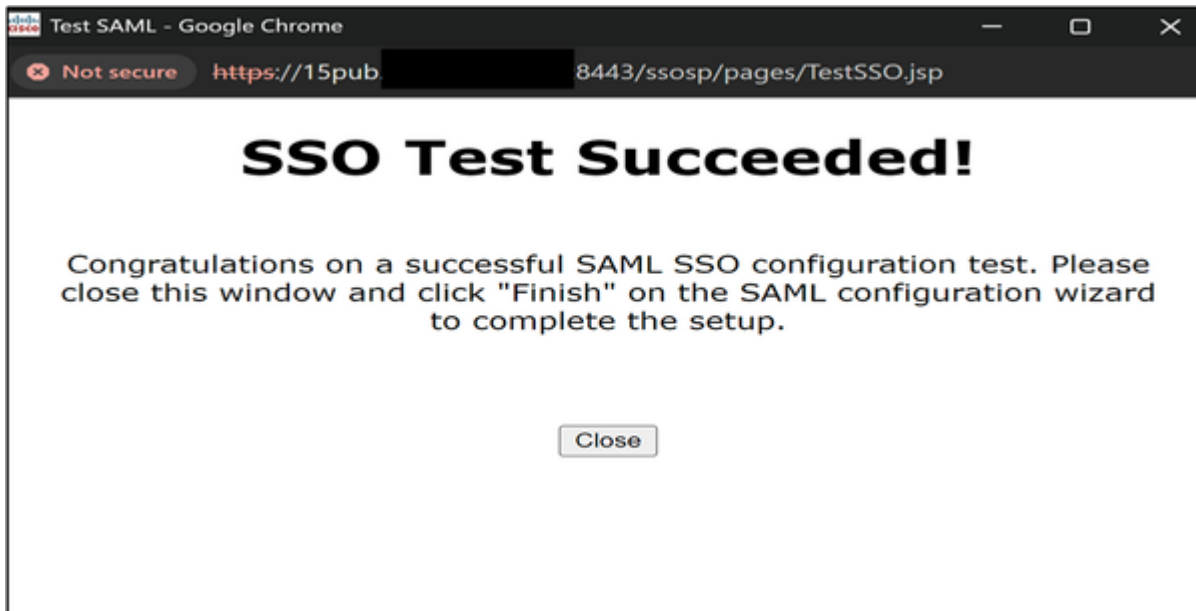
Valid administrator Usernames

admin@

2) Launch SSO test page

Run SSO Test...

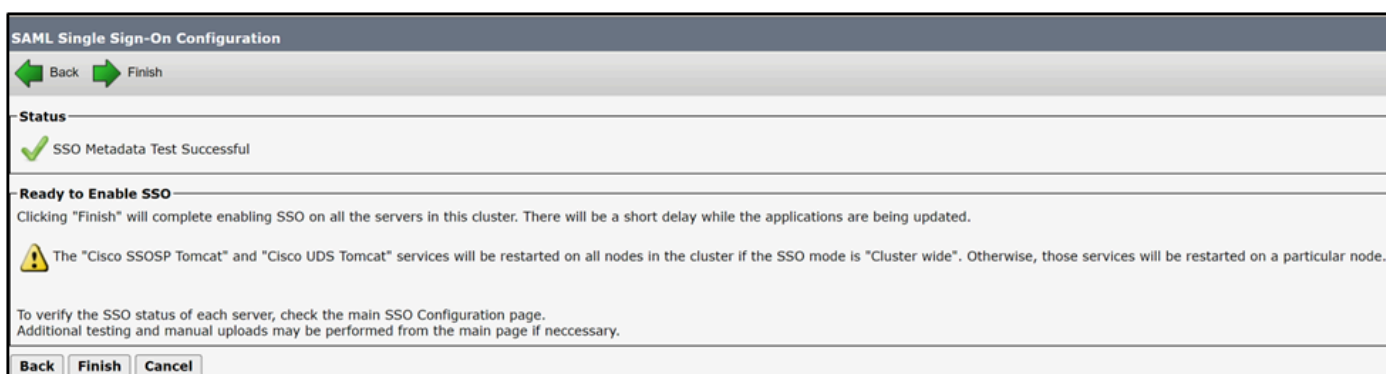
Back Cancel



4. Reinicie os serviços necessários após a habilitação do SSO.



- A habilitação de SSO reinicia o serviço tomcat.



No entanto, o TAC recomenda reiniciar o serviço Tomcat (`utils service restart Cisco Tomcat`) e UDS Tomcat (`utils service restart CiscoUDSTomcat`) manualmente em todos os nós após o processo de habilitação de SSO.

---

### Cenário 3: Problemas de registro de mobilidade e acesso remoto após a renovação do certificado

O aplicativo Webex não pode se registrar no CUCM via Mobility and Remote Access (MRA) após a renovação do gerenciador de chamadas, dos certificados Tomcat e Expressway C em implantações de modo misto.

## Verificação

1. O gerenciador de chamadas do CUCM e o certificado Tomcat são certificados assinados pela CA.
2. A implantação do CUCM e Expressway é executada em modo misto (TLS).
3. inspect Expressway-C logs mostra "SSL routines:ssl3\_read\_bytes:tlsv1 alert unknown ca" (rotinas SSL:ssl3\_read\_bytes:alerta tlsv1 desconhecido ca).

<#root>

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]: UTCTime="2026-01-29 19:01:16,974" Module HTTPMSG:
```

```
|GET /CSFmarcoalh.cnf.xml HTTP/1.1
```

```
Host: expc.cisco.com:6972
```

```
Accept: */*
```

```
Cookie:<CONCEALED>
```

```
User-Agent: WebEx/0.0.0.0
```

```
TrackingID: fxxxxxxxx-86f6-4030-8259-0b768c07723e
```

```
Client-ip: xxx.xxx.xxx.xxx
```

```
X-Forwarded-For: xxx.xxx.xxx.xxx, 127.0.0.1
```

```
Via: https/1.1 vcs[0fxxxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxxx-7feb-4xxx-9
```

|

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]:[ET_NET 1]ERROR:SSL connection failed for
```

```
SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca
```

## Solução

Exportar e importar certificados entre o CUCM e o Expressway-C para garantir a relação de confiança.



Caution: O TAC recomenda executar isso após o horário comercial, pois esse procedimento requer a reinicialização dos serviços. O impacto comercial é



Medium Impact.

1. Procedimento para concluir a relação de confiança entre o CUCM e o Expressway com

## certificados assinados CA



Navegue até OS administration > Security > Certificate management e baixe o certificado raiz CA e o intermediário (se houver) que assina o Call Manager e o certificado Tomcat.

| Certificate       | Common Name/Common Name_SerialNumber                                        | Usage    | Type        | Key Type | Distribution      | Issued By |
|-------------------|-----------------------------------------------------------------------------|----------|-------------|----------|-------------------|-----------|
| CallManager       | <a href="#">cucm15sub-2766.local:6f0000000c374e76d635a3840d00000000000c</a> | Identity | CA-signed   | RSA      | Multi-server(SAN) | 2766-ca-1 |
| CallManager-ECDSA |                                                                             |          |             |          |                   |           |
| CallManager-trust | <a href="#">2766-ca-1_647238c85deb1c8b48ad6e45d0ab241c</a>                  | Trust    | Self-signed | RSA      | 2766-ca-1         | 2766-ca-1 |

Em seguida, navegue até Expressway-C > Manutenção > Segurança > Certificado de CA confiável e carregue o certificado de CA do Call Manager e do certificado Tomcat.

- Maintenance
  - Upgrade
  - Logging
  - Smart licensing
  - Email Notifications
  - Tools >
  - Security**
    - Trusted CA certificate**
    - Server certificate
    - CRL management
    - Client certificate testing
    - Certificate-based authentication configuration
    - Secure traversal test
    - Ciphers
    - SSH configuration
  - Backup and restore
  - Diagnostics >
  - Maintenance mode
  - Language
  - Restart options

Choose File No file chosen

Upload

Select the file containing trusted CA certificates Choose File No file chosen

Trusted CA certificate You are here: Maintenance

File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.

| Type                                 | Issuer               | Subject        | Expiration date | Validity | View                           |
|--------------------------------------|----------------------|----------------|-----------------|----------|--------------------------------|
| <input type="checkbox"/> Certificate | [REDACTED]           | Matches Issuer | Mar 29 2025     | Valid    | <a href="#">View (decoded)</a> |
| <input type="checkbox"/> Certificate | [REDACTED]:2766-ca-1 | Matches Issuer | Feb 09 2025     | Valid    | <a href="#">View (decoded)</a> |

[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Unselect all](#)



Note: Em cenários com o Call Manager e o certificado Tomcat como autoassinados, baixe o Call Manager e o certificado Tomcat reais e carregue-os no Expressway.



Navegue até Expressway-C > Manutenção > Segurança > Certificado CA confiável > Mostrar tudo (arquivo PEM)

Trusted CA certificate

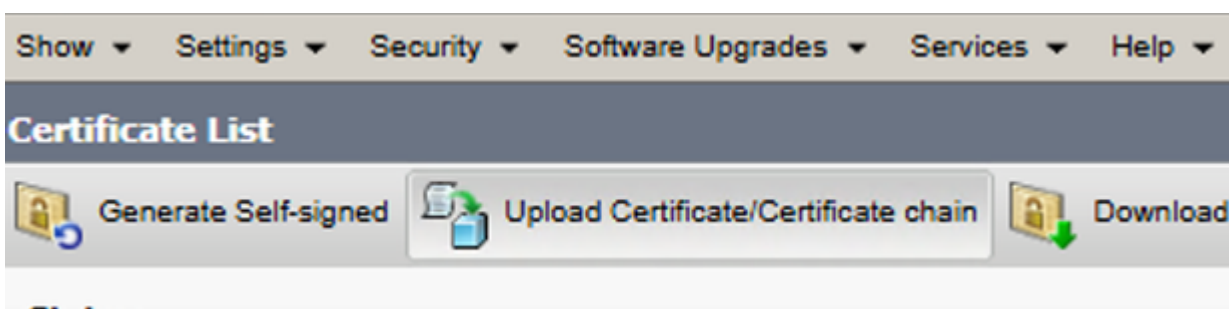
| Type                                 | Issuer                 |
|--------------------------------------|------------------------|
| <input type="checkbox"/> Certificate | [REDACTED] ADSERVER-CA |
| <input type="checkbox"/> Certificate | [REDACTED]:2766-ca-1   |

[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Unselect all](#)

Copie o valor PEM do certificado CA que assina o Expressway-C e salve-o em um arquivo txt.

```
expcert.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIQFBGTWjxDrp1B5NgcCLc0fTANBgkqhkiG9w0BAQsFADBO
MRUwEwYKCZImiZPyLGBGRYFbG9jYWwxZmFzAVBgoJkiaJk/IsZAEZFgdicm9qZWRh
jsFtVBS1D0ReW61KU5gbIHS19QwbCxZHxd4a
-----END CERTIFICATE-----
```

Navegue até OS administration > Security > Certificate management e selecione Upload Certificate/Certificate Chain e carregue o certificado da CA expressway-C como Tomcat-trust e Call Manager-trust



**Upload Certificate/Certificate chain**

Upload Close

**Status**

**i** Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager-trust

Description(friendly name)

Upload File Choose File expcert.pem

Upload Close



Reinicie os serviços necessários no cluster do CUCM:

- Navegue para Cisco Unified Serviceability > Tools > Control Center - Feature Services e reinicie o serviço Cisco CallManager em todos os nós que o executam.
- Navegue para Cisco Unified Serviceability > Tools > Control Center - Feature Services e reinicie o serviço Cisco TFTP em todos os nós que o executam.
- Reinicie o serviço Tomcat em todos os nós no cluster via CLI com o comando `utils service restart Cisco Tomcat`.
- Reinicie o serviço Cisco HAproxy em todos os nós no cluster via CLI com o comando `utils service restart Cisco HAProxy`.

## Cenário 4 : Renovação da causa do certificado da Função de Proxy de Autoridade de Certificação

### Cenário 4.1 : Falha na autenticação 802.1x

O telefone não autentica com o ASA após gerar novamente o certificado da função de proxy de autoridade de certificação (CAPF) no editor do CUCM.

## Verificação

1. As mensagens de status do telefone mostram "Autenticação 802.1x: Falhou"

**12:12:36p 802.1X Authentication: Failed**

**12:12:57p 802.1X Authentication: Failed**

**12:13:33p 802.1X Authentication: Failed**

**12:14:11p 802.1X Authentication: Failed**

**12:14:48p 802.1X Authentication: Failed**

**12:15:32 802.1X Authentication: Failed**

**12:16:08 802.1X Authentication: Failed**

2. Inspeção os registros do telefone do servidor afetado e localize "SSL\_ERROR\_WANT\_READ"

```
4592 NOT Feb 17 11:01:25.041733 (349-349) PAE: -Secure Connection Handshake in progress - status SSL_ER
4593 NOT Feb 17 11:01:25.041826 (349-349) PAE: -EV_REQUEST_REC, ST_AUTHENTICATING->ST_AUTHENTICATING
++ EAP-Failure
4594 NOT Feb 17 11:01:25.041898 (349-349) PAE: -send EAP-Resp/TLS - id 9
4595 NOT Feb 17 11:01:25.042032 (349-349) PAE: -authWhile timer set: 30 sec
4596 NOT Feb 17 11:01:27.061822 (349-349) PAE: -[0001-0] 08-cc-a7-1c-bb-ae vid=0xffff=4095 static=0 pri=0
4597 NOT Feb 17 11:01:27.061950 (349-349) PAE: -port=0
4598 NOT Feb 17 11:01:27.062009 (349-349) PAE: -cprCdpGetPort address: 8:CC:A7:1C:BB:AE Phyport=0 app
4599 NOT Feb 17 11:01:27.062068 (349-349) PAE: - >>>>>>>>>> port obtained = 0 for mac macAddress 08:0
4600 NOT Feb 17 11:01:27.062134 (349-349) PAE: -rcvd EAP-Failure
4601 NOT Feb 17 11:01:27.062189 (349-349) PAE: -EV_FAILURE, ST_AUTHENTICATING->ST_HELD
4602 WRN Feb 17 11:01:27.062462 (349-349) PAE: -802.1X auth FAILED
4603 NOT Feb 17 11:01:27.062550 (349-349) PAE: -paeInfoToInetd: PAE info sent to NETSD
4604 NOT Feb 17 11:01:27.062717 (1786-1880) JAVA-Calling handleNetSDEvent
4605 WRN Feb 17 11:01:27.062953 (1786-1880) JAVA-Thread-11|cip.sec.Security:? - Security: Received a pro
4606 DEB Feb 17 11:01:27.063039 (1786-1880) JAVA-openQue(): que->/tmp/pae_msg_que, key->0x101019ab
4607 DEB Feb 17 11:01:27.063069 (1786-1880) JAVA-openQue(): que->/tmp/pae_rsp_que, key->0x10101c4c
4608 DEB Feb 17 11:01:27.063091 (1786-1880) JAVA-getpaeinfo: send pae info message paeCmd.mtype=1880, pa
4609 DEB Feb 17 11:01:27.063121 (1786-1880) JAVA-getpaeinfo: rcv pae info resp ret=-1, errno=No message
4610 NOT Feb 17 11:01:27.063306 (349-349) PAE: -paeInfoToInetd: Netsd event NETSD_EV_PAE sent to NETSD
4611 NOT Feb 17 11:01:27.063370 (349-349) PAE: - PAE RE-AUTH, not sending SEC_DOWN Netsd event for CDP
4612 NOT Feb 17 11:01:27.063423 (349-349) PAE: -paeSetLastSupStatus: LastSupStatus 0
4613 NOT Feb 17 11:01:27.063475 (349-349) PAE: -heldWhile timer set: 60 sec
4614 NOT Feb 17 11:01:27.064074 (349-349) PAE: -paeNetsdRcvMsg(349): PAE event: status: FAIL : Resource
```

## Solução

Baixe o certificado CAPF do editor do CUCM e carregue-o no servidor de autenticação, ignore o 802.1x para permitir o registro e instale o certificado LSC nos telefones afetados.

Cenário 4.2 : Os telefones não são registrados com o CUCM que usa o perfil de segurança no modo TLS.

Os telefones mostram "O telefone está registrando" após gerar novamente o certificado CAPF no editor do CUCM.

## Verificação

1. Telefones afetados contém perfil de segurança com modo TLS ativado.

**Phone Security Profile Information**

**Product Type:** Cisco 8845  
**Device Protocol:** SIP

**Name\***   
**Description**   
**Nonce Validity Time\***   
**Device Security Mode**   
**Transport Type\***  (circled in red)  
 Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

2. Os telefones afetados têm o certificado LSC instalado.
3. Verifique se o certificado CAPF está atualizado.

**Certificate List (1 - 15 of 15)**

Find Certificate List where  begins with

Select item or enter search text

| Certificate * | Common Name/Common Name_SerialNumber | Usage    | Type        | Key Type | Distribution        | Issued By     | Expiration |
|---------------|--------------------------------------|----------|-------------|----------|---------------------|---------------|------------|
| CAPF          | <a href="#">CAPF-0bc17206</a>        | Identity | Self-signed | RSA      | cm15-<br>.cisco.com | CAPF-0bc17206 | 10/01/2028 |

4. Faça login no editor do CUCM e use o comando `show ctl` que mostra o número de série do certificado CAPF antigo.
5. Em seguida, altere o perfil de segurança do telefone para não seguro.

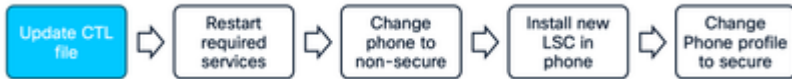
## Solução

Gere novamente o arquivo CTL no CUCM e reinicie os serviços necessários para garantir que os telefones obtenham o novo arquivo CTL com o arquivo CAPF.



Caution: O TAC recomenda executar isso após o horário comercial, pois esse procedimento requer a reinicialização dos serviços. O impacto comercial é

Procedimento para garantir a renovação da CAPF com êxito.



```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n): y

Updating CTL file
CTL file Updated
Please reset all Encrypted and Authenticated phones for the CTL file updates to take effect.
```

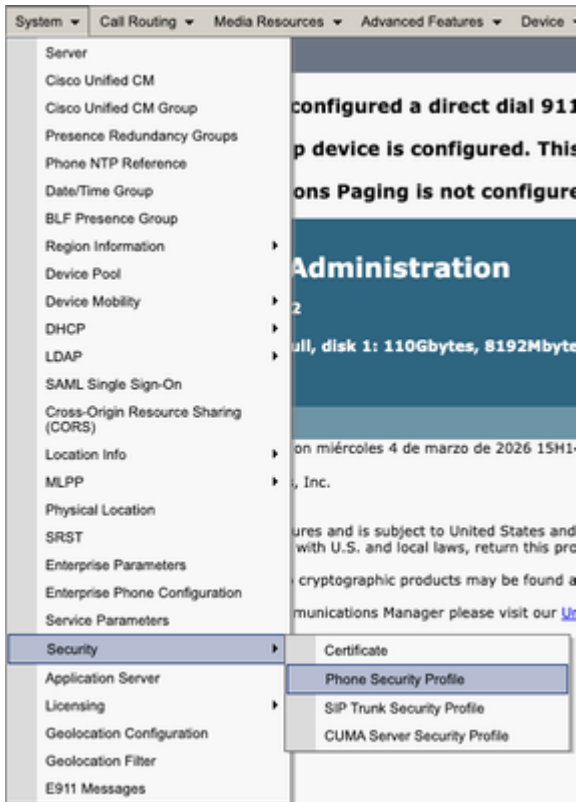
Atualize o arquivo CTL após a regeneração de CAPF. Efetue login na CLI do Publicador e insira o comando `utils ctl update CTLFile`.



1. Navegue para Cisco Unified Serviceability > Tools > Control Center - Feature Services no editor do CUCM e reinicie o serviço CAPF.
2. Navegue para Cisco Unified Serviceability > Tools > Control Center - Network Services e reinicie o Cisco Trust Verification Service em todos os nós que o executam.
3. Navegue para Cisco Unified Serviceability > Tools > Control Center - Feature Services e reinicie o Cisco TFTP Service em todos os nós que o executam



- Navegue até Administração CM > Sistema > Segurança > Perfil de segurança do telefone.



- Copie o perfil de segurança do telefone atual atribuído aos telefones necessários.



- Altere o modo de segurança do nome e do dispositivo para Não seguro e selecione Salvar e aplicar configuração para aplicar essa alteração a todos os telefones necessários.

**Phone Security Profile Configuration**

Save Delete Copy Reset Apply Config Add New

**Status**  
Update successful

**Phone Security Profile Information**

Product Type: Cisco 8845

**Device Protocol:** SIP

Name\*: Cisco 8845 - non Secure profile

Description: Cisco 8845 - Secure profile

Nonce Validity Time\*: 600

Device Security Mode: Non Secure

Transport Type\*: TCP

Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

**Phone Security Profile CAPF Information**

Authentication Mode\*: By Null String

Key Order\*: RSA Only

RSA Key Size (Bits)\*: 2048

EC Key Size (Bits): < None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**Parameters used in Phone**

SIP Phone Port\*: 5060

Save Delete Copy Reset Apply Config Add New

- Aplique o Perfil de segurança do dispositivo criado à configuração de telefones necessária, selecione Salvar e aplicar configuração.

**Protocol Specific Information**

Packet Capture Mode\*: None

Packet Capture Duration: 0

BLF Presence Group\*: Standard Presence group

SIP Dial Rules: < None >

MTP Preferred Originating Codec\*: 711ulaw

Device Security Profile\*: Cisco 8845 - non Secure profile

Rerouting Calling Search Space: < None >

SUBSCRIBE Calling Search Space: < None >

SIP Profile\*: Standard SIP Profile [View Details](#)

Digest User: < None >

Media Termination Point Required  
 Unattended Port  
 Require DTMF Reception



Use a seção de informações CAPF na configuração do dispositivo dos telefones afetados para instalar o certificado LSC nos telefones necessários.

- Nas informações de CAPF, selecione Instalar/Atualizar em Operação de Certificado.

**Certification Authority Proxy Function (CAPF) Information**

Certificate Operation\*

Authentication Mode\*

Authentication String

Key Order\*

RSA Key Size (Bits)\*

EC Key Size (Bits)

Operation Completes By     (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Additional CAPF Settings.

- Selecione Save and Apply Config.
- Aguarde até que o Status da operação de certificado mostre Operação concluída.



Na seção Protocol Specific Information em Phone Configuration, selecione o perfil de segurança com TLS ativado que foi criado.

**Protocol Specific Information**

Packet Capture Mode\*

Packet Capture Duration

BLF Presence Group\*

SIP Dial Rules

MTP Preferred Originating Codec\*

Device Security Profile\*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile\*  [View Details](#)

Digest User

**Phone Security Profile Configuration**

Save Delete Copy Reset Apply Config Add New

**Status**

Status: Ready

**Phone Security Profile Information**

**Product Type:** Cisco 8845  
**Device Protocol:** SIP

Name\* Cisco 8845 - Secure profile  
Description Cisco 8845 - Secure profile  
Nonce Validity Time\* 600  
Device Security Mode Encrypted  
Transport Type\* TLS

Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

## Informações Relacionadas

- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/214231-certificate-regeneration-process-for-cis.html>
- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/217138-regeneration-of-cucm-ca-signed-certifica.html>
- <https://www.cisco.com/c/en/us/support/docs/content-networking/certificates/213295-how-to-install-an-lsc-on-a-cisco-ip-phon.html>
- [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X15-2/mra/exwy\\_b\\_mra-deployment-guide-x152.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-2/mra/exwy_b_mra-deployment-guide-x152.html)

## 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.