

# CUCMでの証明書更新に関する一般的な問題の トラブルシューティング

## はじめに

このドキュメントでは、Cisco Unified Communications Manager(CUCM)で証明書を再生成した後  
の一般的な問題とその解決方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- CUCM証明書更新プロセス
- CUCM GUIインターフェイス
- Expresswayサーバ
- CUCMプロセスによるデバイス登録
- 認証局プロキシ機能
- Cisco Unified Communications Managerセキュリティガイド

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM バージョン 15

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

### ビジネスへの影響

この表は、操作における各証明書更新のビジネスへの影響を示しています。情報を注意深く確認します。各証明書のリスクレベルに基づいて、必要な証明書を数時間後または待機期間中に更新します。

● 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	

## シナリオ1:Call Manager、TVS、およびITL証明書の更新後に電話機が登録されない



注：このシナリオは、CUCM混合モードおよび非セキュアクラスタの下での導入に適用され、さらに、自己署名証明書およびCA証明書にも適用されます。

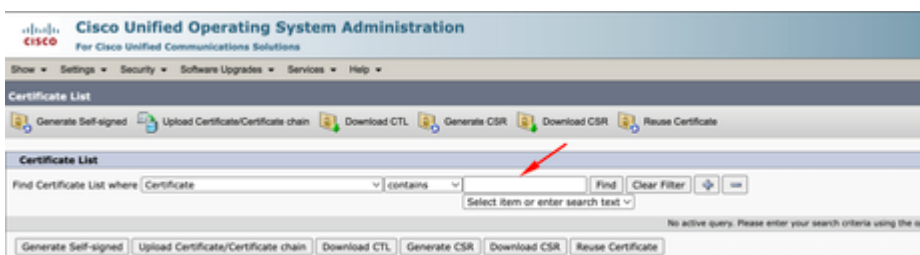
Call Manager(CM)、TVS、およびITL証明書が期限切れになり、同時に更新された場合、すべての電話が未登録状態になり、システムに大きな影響を与えます。これは、電話がCUCMで信頼されないことをトリガーする予期された動作です。

### 検証

1. Cisco Unified OS Administration > Security > Certificate Managementで、証明書がすでに期限切れであることを確認します



2. ページ上部のフィルタの下にあるCallmanager、TVS、またはITLで検索し、「次を含む」または「次で始まる」オプションを使用します。



3. 証明書の「有効期限」列に最新の状態が表示されていること（TVS証明書とITL証明書の場合も同じ）。

Certificate	Common Name/Common Name, SerialNumber	Usage	Type	Key Size	Distribution	Issued By	Expiration	Description
CallManager	888.8888.com	Identity	CSR Only	RSA	self team-cum	--	--	--
CallManager	888.8888.com_48858554h322395c33a171262888	Identity	Self-signed	RSA	self team-cum	self team-cum	888/0/0/0	Self signed certificate generated by system.

4. 証明書の更新後に問題がないことを確認できたら、電話機は未登録状態として表示されます。

Phone	Device Name(s)	Description	Device Pool	Device Protocol	State	Status	Last Registered	Last Active	Unified CM
<input type="checkbox"/>	CP7688888888		Default	SIP	None	Never			
<input type="checkbox"/>	SEP045104FDC41	SEP045104FDC41	281102	SIP	Unregistered		Feb 22, 2024 12:05:42 AM	Dec 29, 2023 7:32:23 PM	custom5ta3

## ソリューション

この問題を解決するには、次の2つの方法があります。

1. 電話機を工場出荷時の状態にリセットし、電話機で現在のセキュリティ設定を消去して、新しい証明書を取得できるようにします
2. パブリッシュャードのCLIからITLおよびCTL証明書を更新し、次のコマンドを使用します  
utils itl reset localkeyを使用します。  
この手順は、登録されている電話機を含むすべての電話機に適用されます。この手順は営業

時間外に実行してください。



High Impact.

## シナリオ2:Tomcat証明書の更新後にシングルサインオンが機能しない



注：このシナリオは、シングルサインオン設定にクラスタ全体またはノード単位のアップデートを使用する導入に適用できます

シングルサインオン(SSO)でCUCM内にログインすると、エラーメッセージ“saml応答の処理中にエラー”または“saml応答の処理中にエラーが表示されます。秘密鍵を復号化できませんでした”

### 検証

1. 自己署名されている場合は、すべてのノードに有効なtomcat証明書が含まれていることを確認し、新しいマルチsan tomcat証明書が関連付けられていることを確認します。
2. デバッグレベルでSSOログをアクティブ化するには、CLI経由ですべてのCUCMノードでset samltrace level debugを使用します
3. CUCMに再度ログインし、SSO方式を使用して問題を再現します。
4. インシデント後にTomcat SSOログを収集し、次のメッセージが表示されることを確認します。

```
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  
...
```

### ソリューション

Tomcat証明書の更新後にCUCMメタデータをエクスポートし、Identity Provider Serverにインポ

ートして、この通信に使用する新しいtomcat証明書があることを確認します。

SSO導入を有効にしてtomcatを更新する手順：



注意:Tomcat証明書の更新後の問題を防ぐために、Technical Assistance Center(TAC)では次の手順を推奨します。この手順は営業時間外に実行することをお勧めします。

---

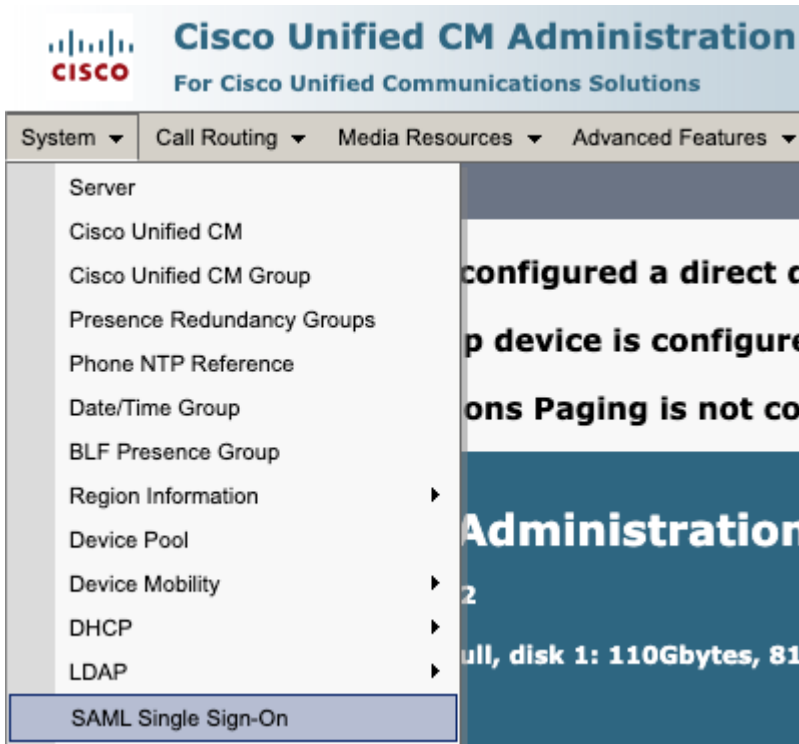


Low Impact

#### 1. すべてのCUCMノードでSSOを無効にする



- CM administration > System > SAML シングルサインオンへのアクセス



- Disable SAML SSOを選択します



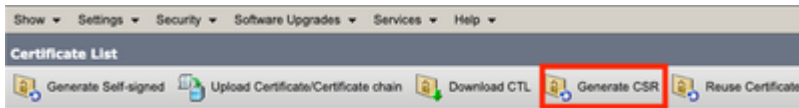
- ノード単位のアグリーメントを使用する場合、このプロセスはGUI経由で残りすべてのノードで実行する必要があります。

## 2. CUCMクラスタ内のTomcat証明書の更新

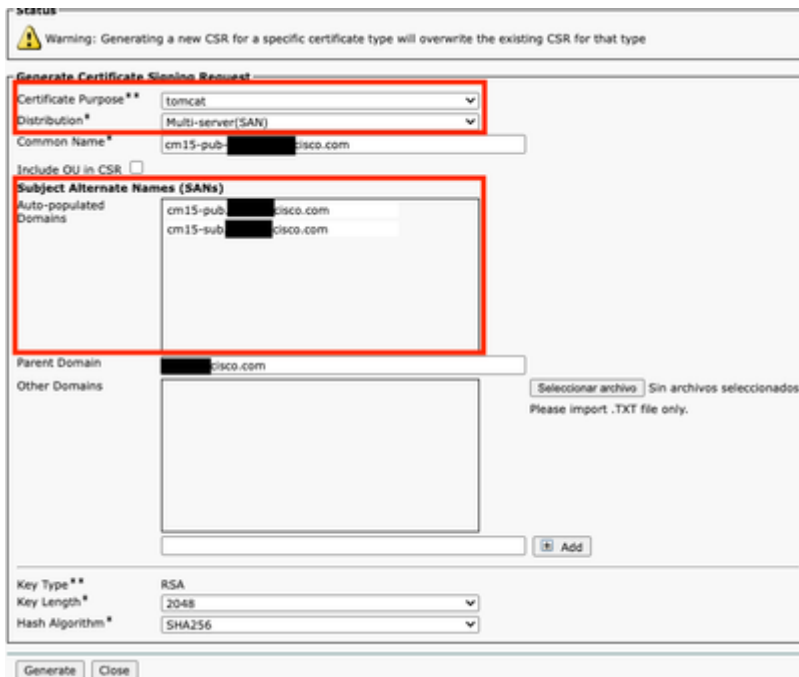


CUCMクラスタでTomcatマルチSAN証明書を更新する全体的な手順は次のとおりです。

- OS administration > Security > Certificate managementの順に移動します。
- [CSR の作成 ( Generate CSR ) ] を選択します。



- Certificate ProxyでTomcatを選択します。
- Multi-SAN in Distributionを選択します。
- クラスタ内のすべてのノードが自動入力ドメインの下にリストされていることを確認します
- 



- Generateを選択します。クラスタ内のすべてのノードでCSRが作成されていることを確認します。
- CUCMパブリッシャから生成されたCSRをダウンロードし、認証局(CA)サーバで署名します。
- OS administration > Security > Certificate managementの順に選択します。Upload certificate/Certificate chainを選択します。
- CA証明書をTomcat-trustとしてアップロードします。
- ステップ6を繰り返し、Tomcat署名付き証明書をTomcatとしてアップロードします。
- 完了してすべてのノードで新しいtomcat証明書が適用されていることを確認したら、次のコマンドを使用して、クラスタ内のすべてのノードでCLIを通じてTomcatサービスを再起動します。utils service restart Cisco Tomcat

詳細については、次のドキュメントを参照してください。

- [Tomcat自己署名証明書の再生成](#)
- [TomcatのCA署名付き証明書を再生成します。](#)

### 3. サービスプロバイダー(SP)メタデータのエクスポート



- CM administration > System > Single Sign-Onの順に選択します。
- SSOオプションを設定し(この例では、SSOモードではクラスタ全体で、証明書ではtomcat証明書を使用)、すべてのメタデータのエクスポートを選択します

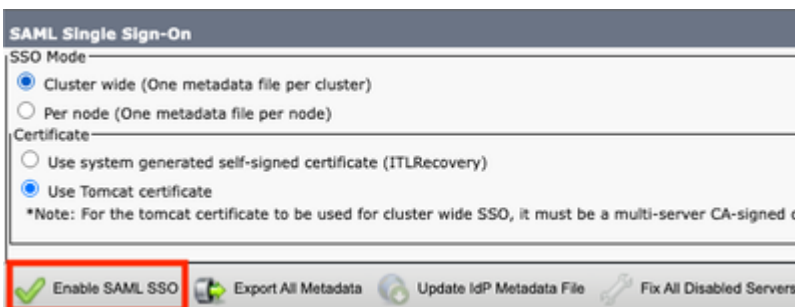



- SPメタデータをアイデンティティプロバイダー(IdP)サーバにインポートします。詳細については、「[アイデンティティプロバイダーでのSAML SSOの設定](#)」を参照してください。

### 4. CUCMクラスタでのSSOの有効化




- CM administration > System > Single Sign-Onの順に選択します。
- CUCMメタデータのエクスポート時に同じSSOオプションを選択して、Enable SAML SSOを選択し、continueを選択します。



 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.


- クラスタ全体でこの手順を使用してすべてのノードのマルチSAN証明書を確認できる場合は、Test for multi-server tomcat certificateを選択します。完了したら、Nextを選択します。

**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

- IdPメタデータをアップロードし、Import IdP Metadataを選択します。完了したら、Nextを選択します。

**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

- Test SSO Setupで、Standard CCM Super Usersグループが割り当てられているユーザを選択し、成功するまでRun SSO Testを選択します。

**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.

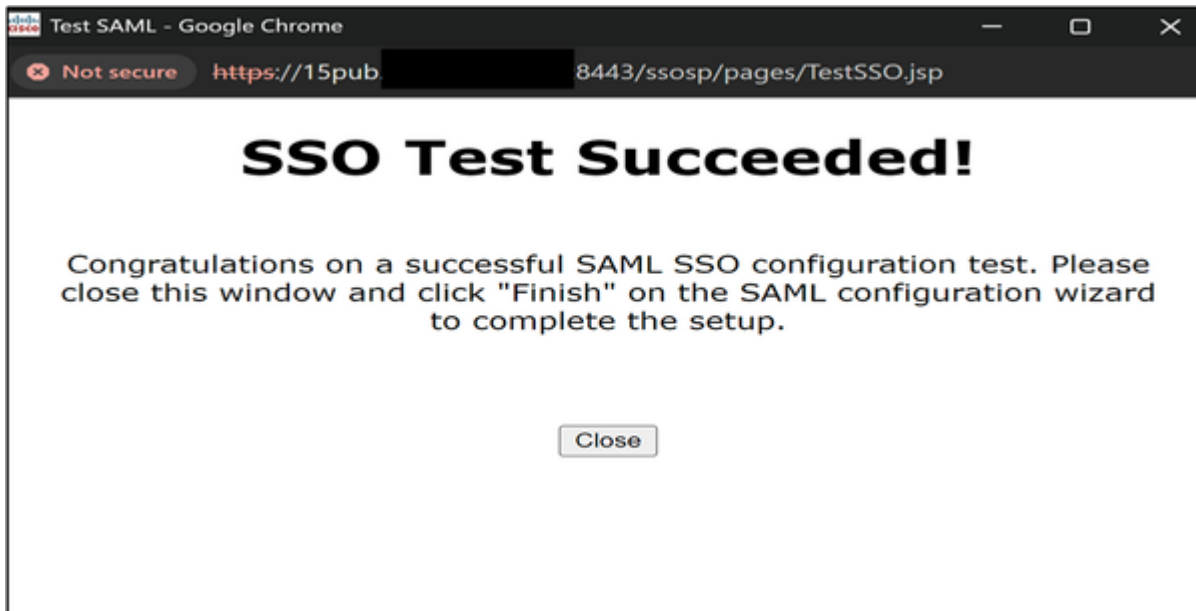
Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

Valid administrator Usernames  
admin@

2) Launch SSO test page

Run SSO Test...

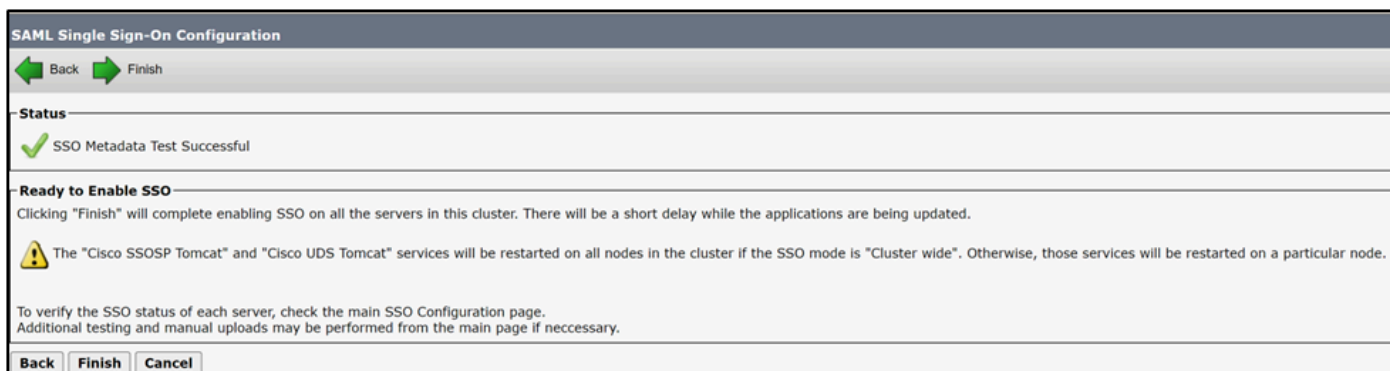
Back Cancel



4. SSOを有効にした後、必要なサービスを再起動します。



- SSOを有効にすると、tomcatサービスが再起動します。



ただし、TACでは、SSO有効化プロセスの後で、すべてのノードでTomcat(utils service restart Cisco Tomcat)およびUDS Tomcat(utils service restart CiscoUDSTomcat)サービスを手動で再起動することを推奨しています。

---

## シナリオ3：証明書の更新後のモビリティおよびリモートアクセス登録の問題

Call Manager、Tomcat、およびExpressway C証明書が混合モード導入環境で更新された後、Webexアプリがモバイルおよびリモートアクセス(MRA)経由でCUCMに登録できない。

## 検証

1. CUCM Call ManagerおよびTomcat証明書はCA署名付き証明書です。
2. CUCMとExpresswayの導入は、混合モード(TLS)で実行されます。
3. inspect Expressway-Cログに「SSL routines:ssl3\_read\_bytes:tlsv1 alert unknown ca」と表示される

```
<#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: fxxxxxxx-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[0fxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxx-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
```

## ソリューション

CUCMとExpressway-Cの間で証明書のエクスポートとインポートを行い、信頼関係を確立します。



注意：この手順ではサービスの再起動が必要になるため、TACでは営業時間外にこの手順を実行することをお勧めします。ビジネスインパクト



Medium Impact.

1. CA署名付き証明書を使用してCUCMとExpressway間の信頼関係を構築する手順



OS administration > Security > Certificate managementの順に移動し、ルートCA証明書、および Call ManagerとTomcat証明書に署名する中間証明書（存在する場合）をダウンロードします。

**Certificate List**

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR Download CSR Reuse Certificate

Status  
18 records found

**Certificate List (1 - 18 of 18)** Rows per Page

Find Certificate List where Certificate begins with callmanager Find Clear Filter

Certificate	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By
CallManager	cucm15sub- 2766.local.60000000c374e76d635a3840d0000000000c	Identity	CA- signed	RSA	Multi-server(SAN)	2766-ca-1
CallManager- ECDSA						
CallManager- trust	2766-ca- 1_642238c85deb1c8b48ad6e46d0ab241c	Trust	Self- signed	RSA	2766-ca-1	2766-ca-1

次に、Expressway-C > Maintenance > Security > Trusted CA certificateの順に移動し、Call ManagerとTomcatのCA証明書をアップロードします。

**Maintenance**

- Upgrade
- Logging
- Smart licensing
- Email Notifications
- Tools >
- Security**
- Backup and restore
- Diagnostics >
- Maintenance mode
- Language
- Restart options

Choose File No file chosen

- Trusted CA certificate**
- Server certificate
- CRL management
- Client certificate testing
- Certificate-based authentication configuration
- Secure traversal test
- Ciphers
- SSH configuration

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](#)



注：Call ManagerとTomcat証明書が自己署名のシナリオでは、実際のCall ManagerとTomcat証明書をダウンロードしてExpresswayにアップロードします。



Expressway-C > Maintenance > Security > Trusted CA certificate > Show all (PEM file)の順に移動します。

Trusted CA certificate

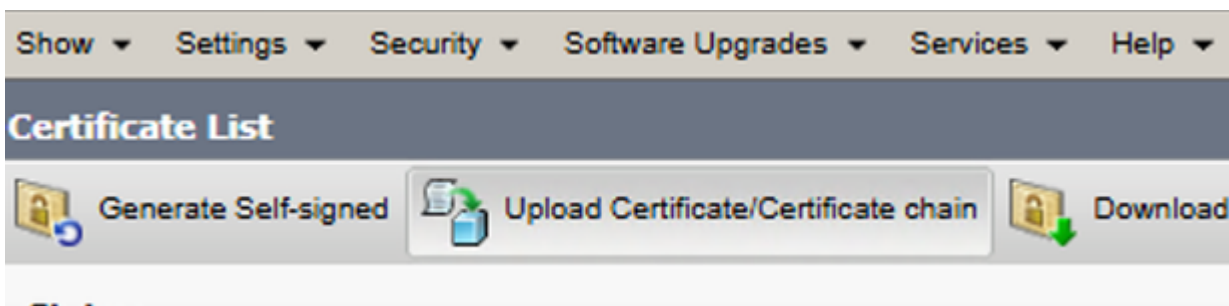
Type	Issuer
<input type="checkbox"/> Certificate	[REDACTED] ADSERVER-CA
<input type="checkbox"/> Certificate	[REDACTED]:2766-ca-1

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

Expressway-Cに署名するCA証明書のPEM値をコピーし、txtファイルに保存します。

```
expcert.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIQFBGTWjxDrp1B5NgcCLc0FTANBgkqhkiG9w0BAQsFADBO
MRUwEwYKCZImiZPyLGOBGRYFbG9jYWwxZmFzAVBgoJkiaJk/IsZAEZFgdicm9qZWRh
jsFtVBS1D0ReW61KU5gbIHS19QwbCxZHxd4a
-----END CERTIFICATE-----
```

OS administration > Security > Certificate managementの順に移動し、Upload Certificate/Certificate Chainを選択して、Expressway-C CA証明書をTomcat-trustおよびCall Manager-trustとしてアップロードします



**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\*

Description(friendly name)

Upload File  expcert.pem

---



CUCMクラスタで必要なサービスを再起動します。

- Cisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に選択し、実行しているすべてのノードでCisco CallManagerサービスを再起動します。
- Cisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に選択し、実行しているすべてのノードでCisco TFTPサービスを再起動します。
- CLIでコマンドutils service restart Cisco Tomcatを使用して、クラスタ内のすべてのノードのTomcatサービスを再起動します。
- utils service restart Cisco HAProxyコマンドを使用し、CLI経由でクラスタ内のすべてのノードのCisco HAProxyサービスを再起動します。

## シナリオ4：認証局プロキシ機能(CAPF)証明書の更新が原因

### シナリオ4.1:802.1x認証の失敗

CUCMパブリッシャでCertificate Authority Proxy Function(CAPF)証明書を再生成した後、電話機がASAで認証されません。



シナリオ4.2:TLSモードでセキュリティブロファイルを使用する電話機がCUCMに登録されない。

CUCMパブリッシャでCAPF証明書を再生成すると、電話機に「電話機が登録されています (Phone is registering)」と表示されます。

## 検証

1. 影響を受ける電話機には、TLSモードが有効なセキュリティブロファイルが含まれています。

**Phone Security Profile Information**

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

Name\*   
Description   
Nonce Validity Time\*   
Device Security Mode   
Transport Type\*  (highlighted with a red circle)

Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

2. 該当する電話機には、LSC認定がインストールされています。
3. CAPF証明書が最新であることを確認します。

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- .cisco.com	CAPF-0bc17206	10/01/2028

4. CUCMパブリッシャにログインし、古いCAPF証明書シリアル番号を表示するコマンドshow ctlを使用します。
5. 次に、電話機のセキュリティブロファイルを非セキュアに変更します。

## ソリューション

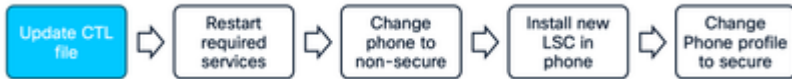
CUCMでCTLファイルを再生成し、電話機がCAPFファイルを含む新しいCTLファイルを取得するように、必要なサービスを再起動します。



注意：この手順ではサービスの再起動が必要になるため、TACでは営業時間外にこの手順を実行することをお勧めします。ビジネスインパクト

## Medium Impact.

CAPFを正常に更新するための手順。



```
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.
```

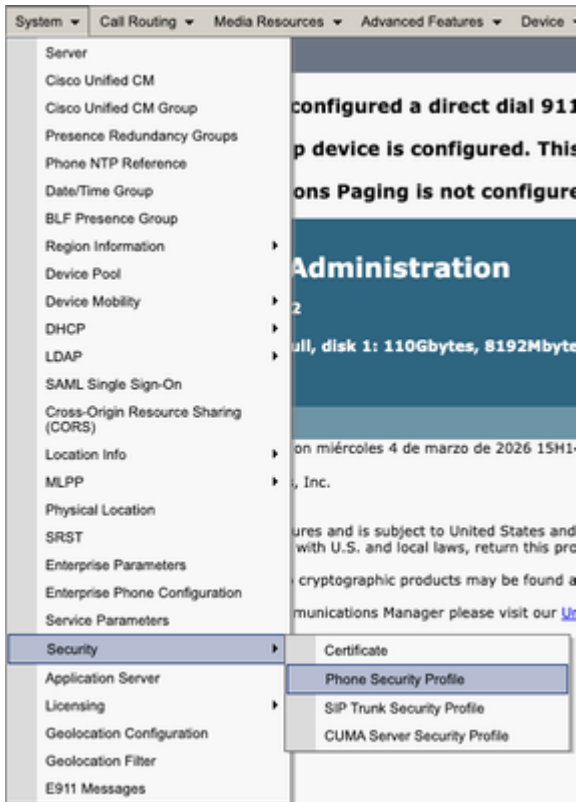
CAPF再生成後にCTLファイルを更新します。パブリッシャのCLIにログインし、コマンドutils ctl update CTLFileを入力します。



1. CUCMパブリッシャでCisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に移動し、CAPFサービスを再起動します。
2. Cisco Unified Serviceability > Tools > Control Center - Network Servicesの順に選択し、実行しているすべてのノードでCisco Trust Verification Serviceを再起動します。
3. Cisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に選択し、実行しているすべてのノードでCisco TFTP Serviceを再起動します



- CM administration > System > Security > Phone Security Profileの順に選択します。



- 必要な電話機に割り当てられている現在の電話セキュリティプロファイルをコピーします。



- 名前とデバイスセキュリティモードをNon Secureに変更し、Save and Apply Configを選択して、この変更を必要なすべての電話に適用します。

**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

- 作成したデバイスセキュリティプロファイルを必要な電話機の設定に適用します。次に、Save and Apply Configを選択します。

**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



該当する電話機のデバイス設定のCAPF情報セクションを使用して、必要な電話機にLSC証明書をインストールします。

- CAPF情報では、Certificate OperationでInstall/Upgradeを選択します。

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

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	<input type="text"/>
<input type="button" value="Generate String"/>	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	
Operation Completes By	2026 03 14 12 (YYYY:MM:DD:HH)
Certificate Operation Status:	None
Note: Security Profile Contains Additional CAPF Settings.	

- Save and Apply Configを選択します。
- Certificate Operation StatusにOperation completedと表示されるまで待ちます。



Phone ConfigurationのProtocol Specific Informationセクションで、作成したTLSを有効にしたセキュリティプロファイルを選択します。

**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 - Secure profile
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile <a href="#">View Details</a>
Digest User	< None >

**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\*   
Description   
Nonce Validity Time\*   
Device Security Mode   
Transport Type\*

Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

## 関連情報

- <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)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。