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	

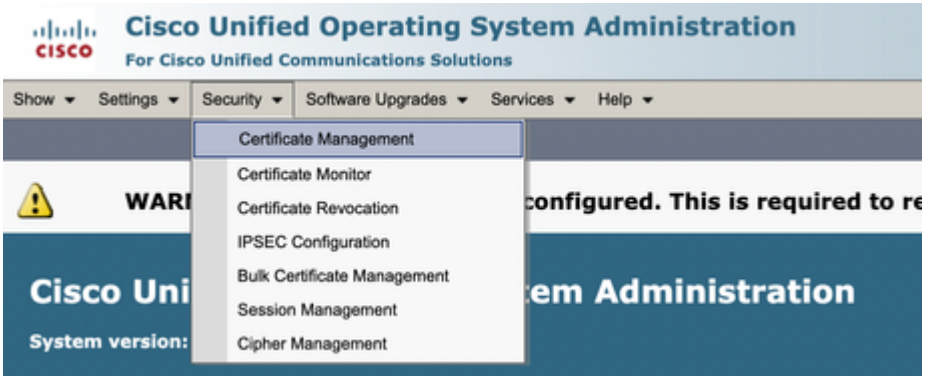
シナリオ1:Call Manager、TVS、およびITL証明書の更新後に電話機が登録されない

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。

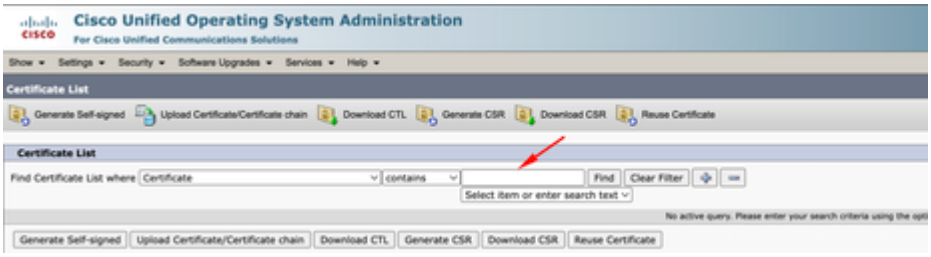
Call Manager(CM)、TVS、およびITL証明書が期限切れになり、同時に更新された場合、すべての電話が未登録状態になり、システムに大きな影響を与えます。これは、電話がCUCMで信頼されないことをトリガーする予期された動作です。

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

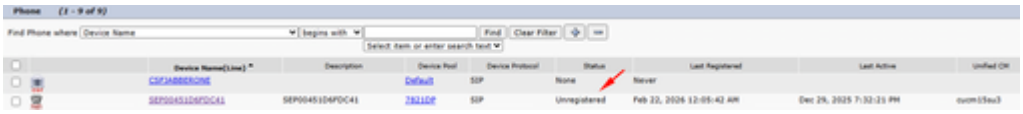


2. ページ上部のフィルタの下にあるCallmanager、TVS、またはITLで検索し、「次を含む」または「次で始まる」オプションを使用します。



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）。

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。

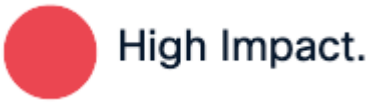


ソリューション

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. パブリッシャノードの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。



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グリーメン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.authenticatio
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。

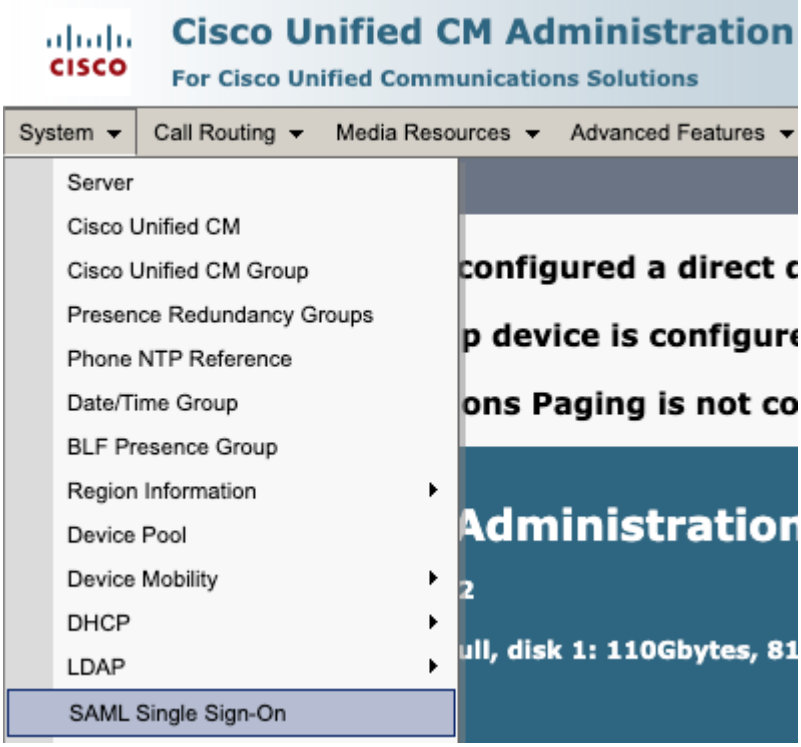
SSO導入を有効にしてtomcatを更新する手順：

⚠ 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。

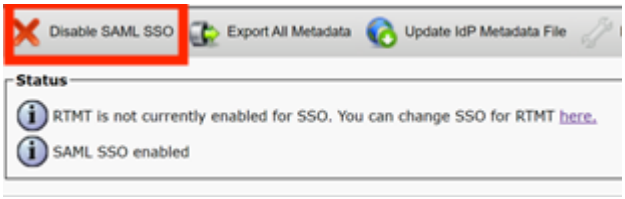
Low Impact

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

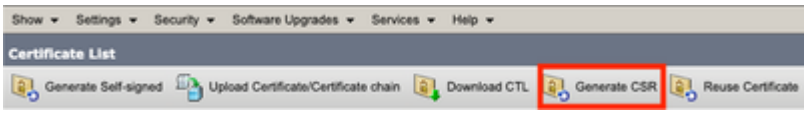


- ノード単位のアグリーメントを使用する場合、このプロセスはGUI経由で残りすべてのノードで実行する必要があります。

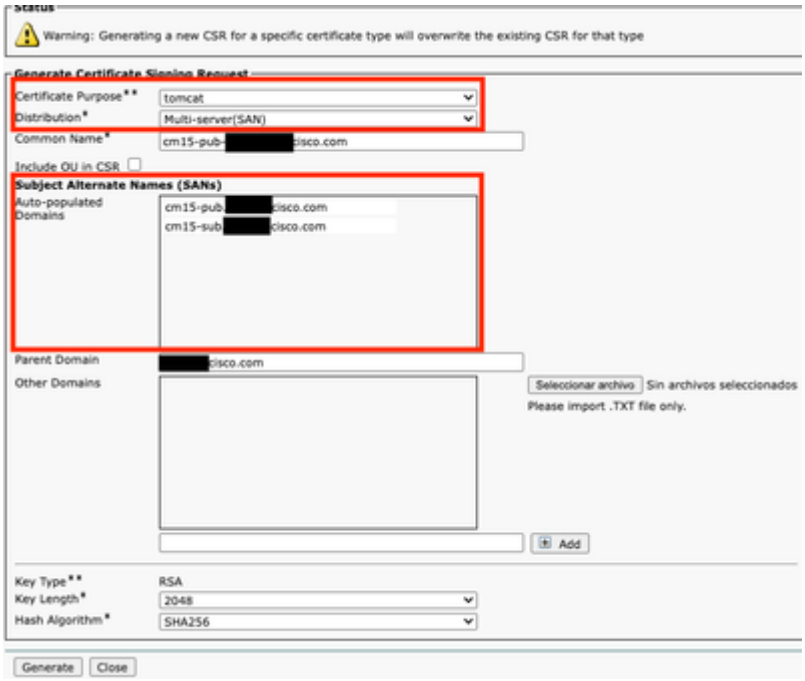
2. CUCMクラスタ内のTomcat証明書の更新

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。

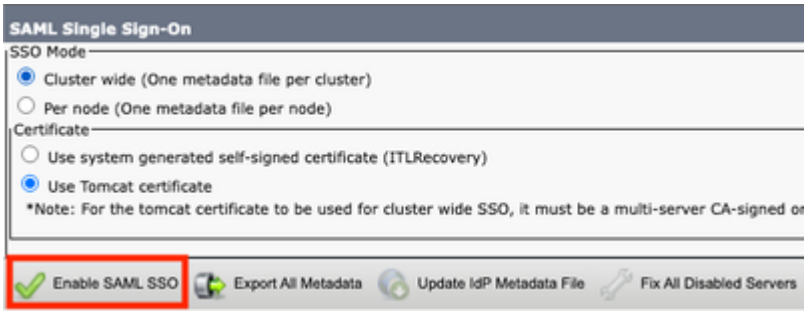
3. サービスプロバイダー(SP)メタデータのエクスポート

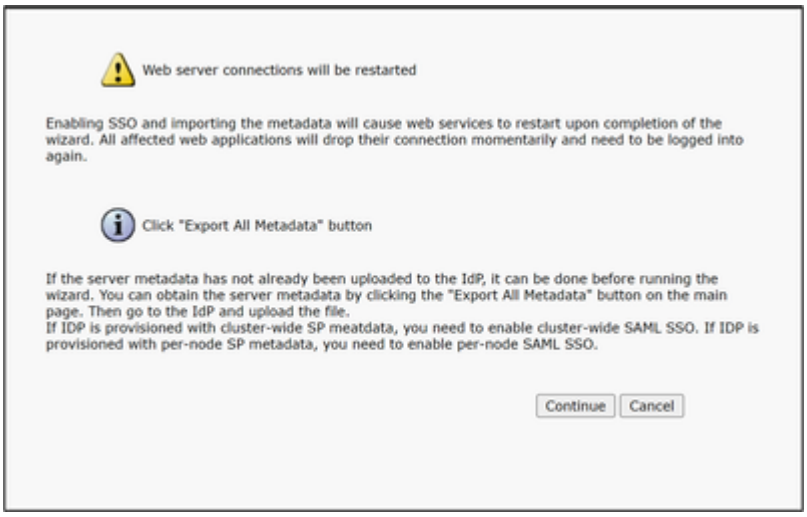
- CM administration > System > Single Sign-Onの順に選択します。
- SSOオプションを設定し(この例では、SSOモードではクラスタ全体で、証明書ではtomcat証明書を使用)、すべてのメタデータのエクスポートを選択します

- 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。

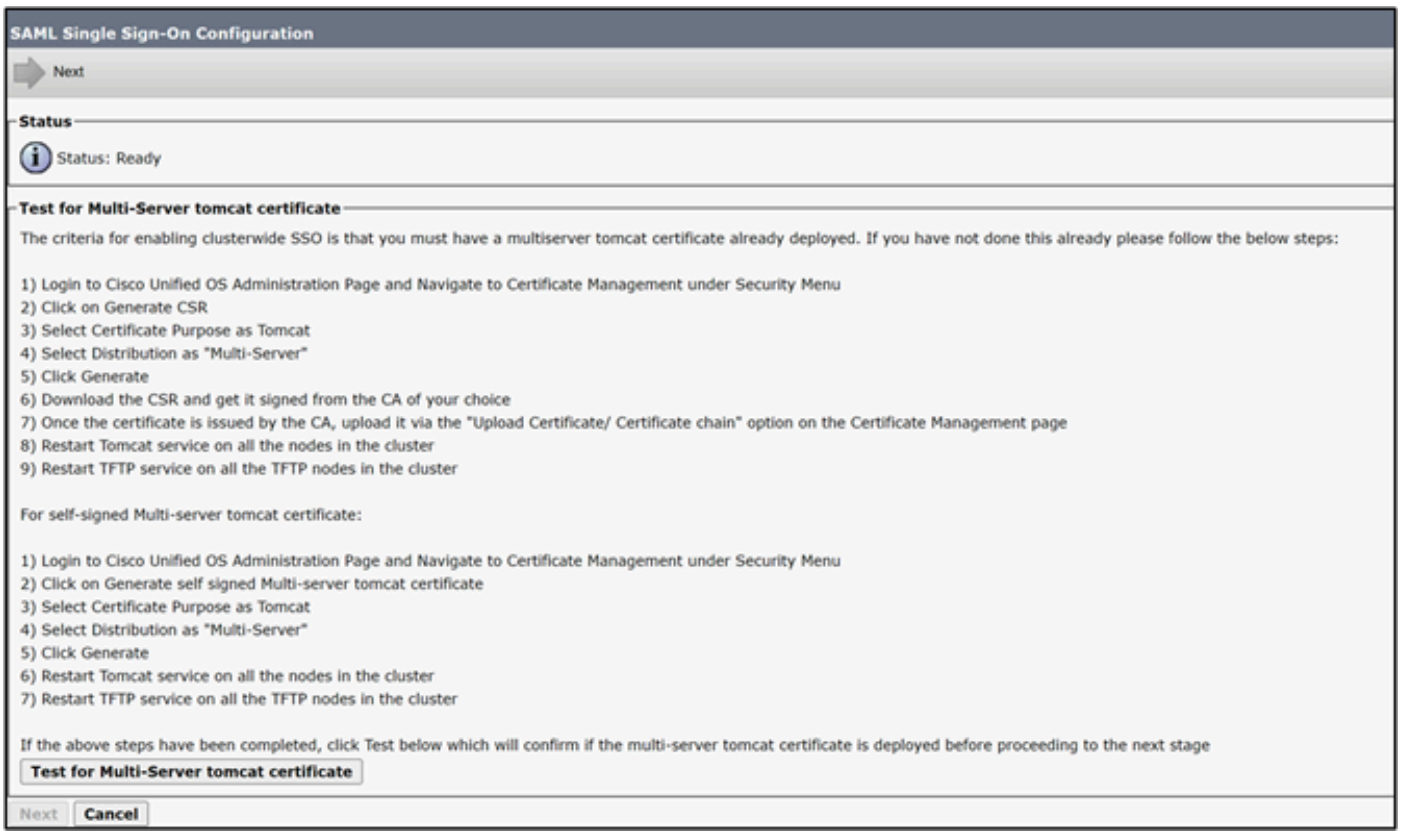
4. CUCMクラスタでのSSOの有効化

- 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。

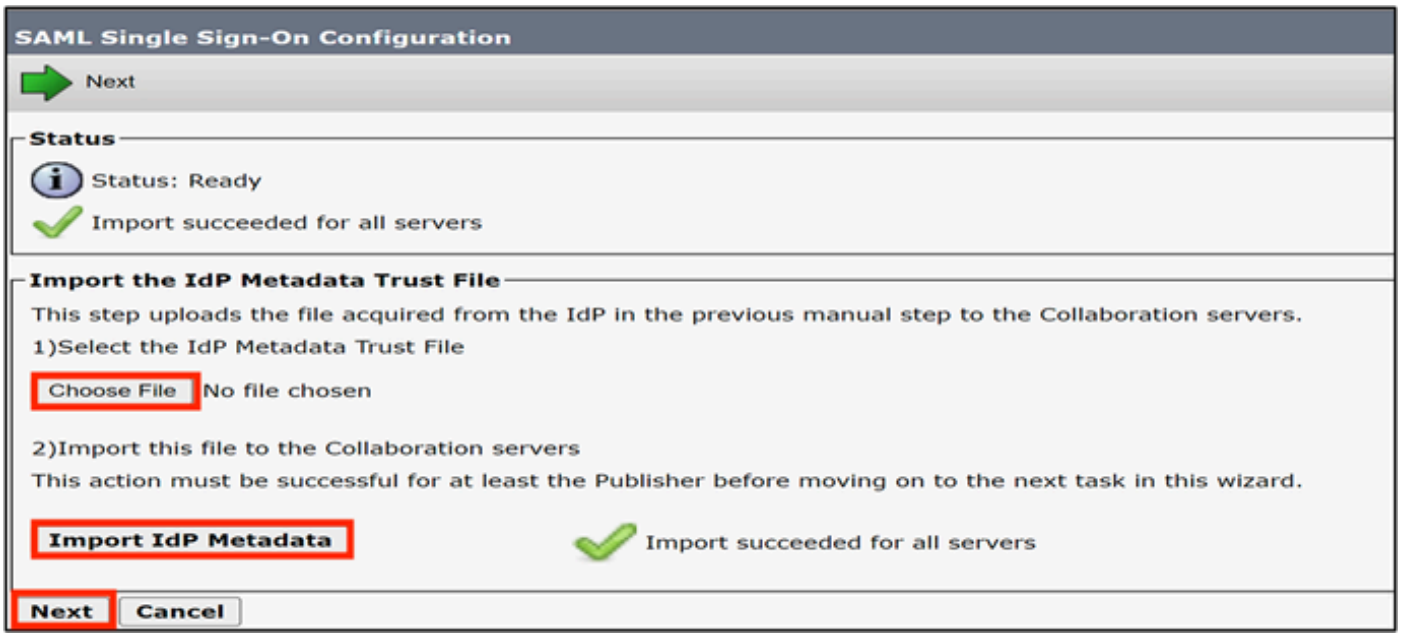




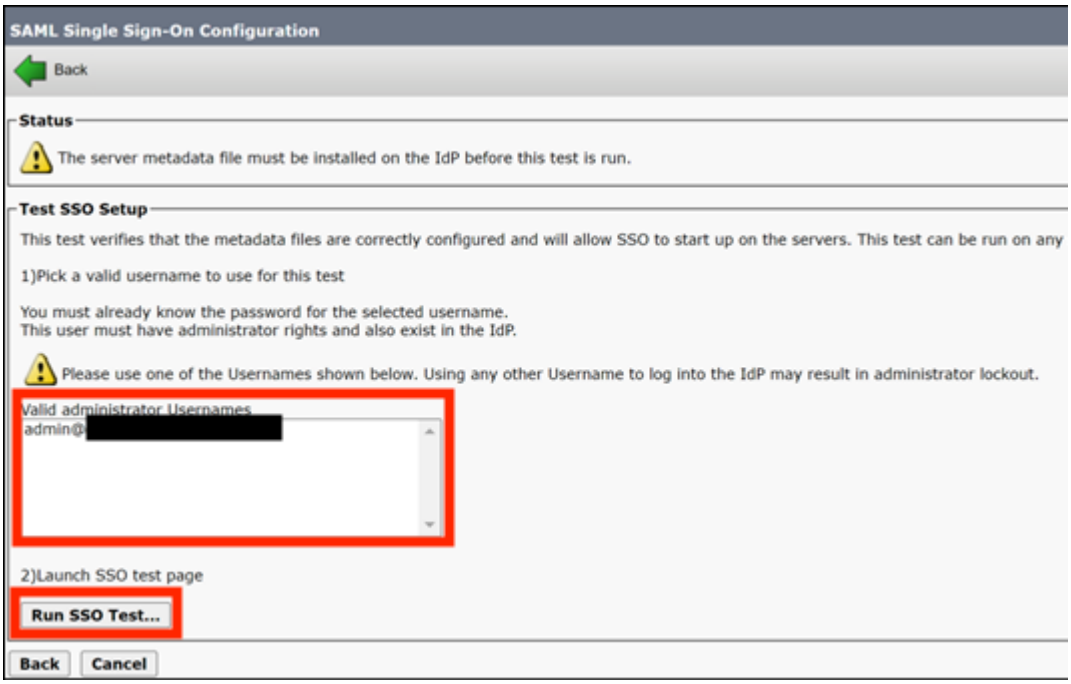
- クラスタ全体でこの手順を使用してすべてのノードのマルチSAN証明書を確認できる場合は、Test for multi-server tomcat certificateを選択します。完了したら、Nextを選択します。

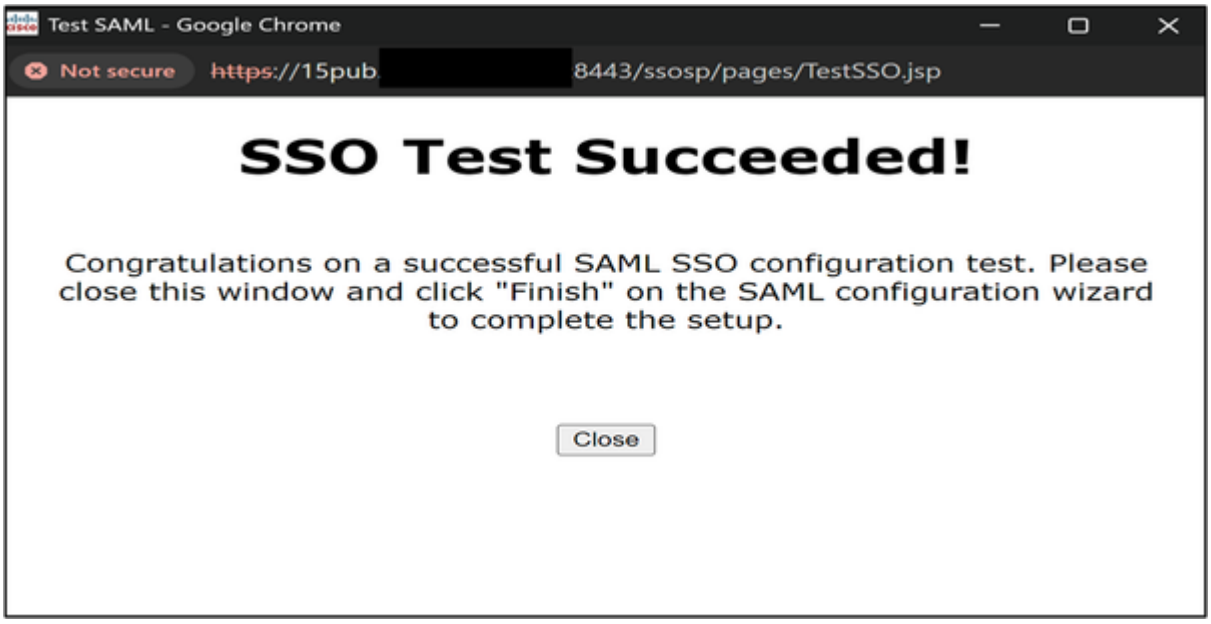


- IdPメタデータをアップロードし、Import IdP Metadataを選択します。完了したら、Nextを選択します。



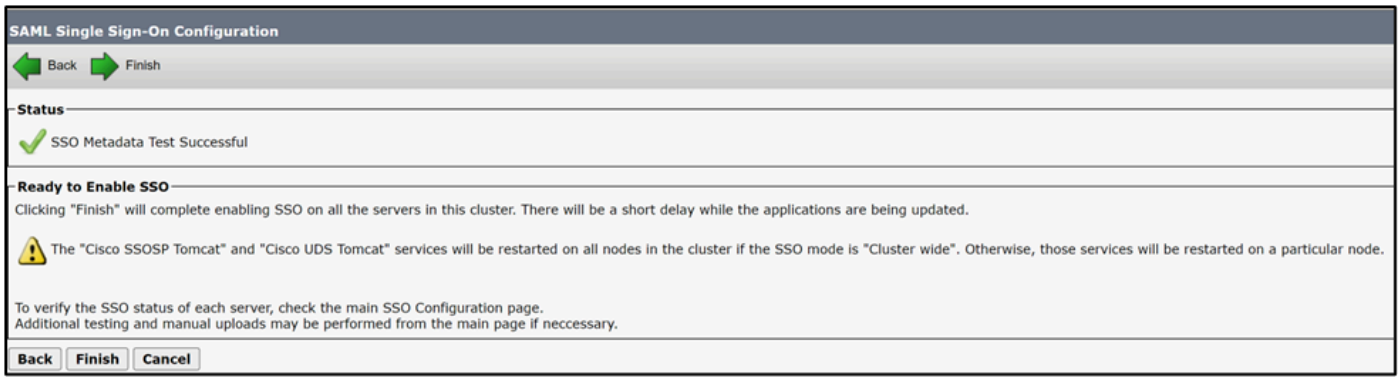
- Test SSO Setupで、Standard CCM Super Usersグループが割り当てられているユーザを選択し、成功するまでRun SSO Testを選択します。





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アプリがモビリティ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

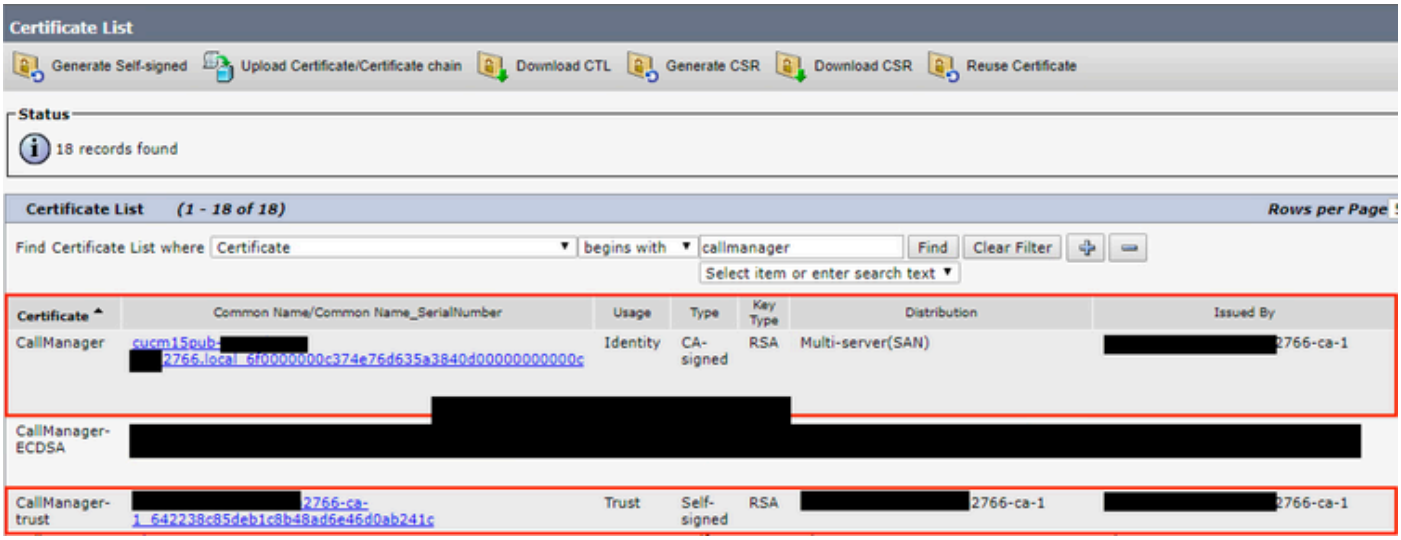
CUCMとExpressway-Cの間で証明書のエクスポートとインポートを行い、信頼関係を確立します。

⚠ 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

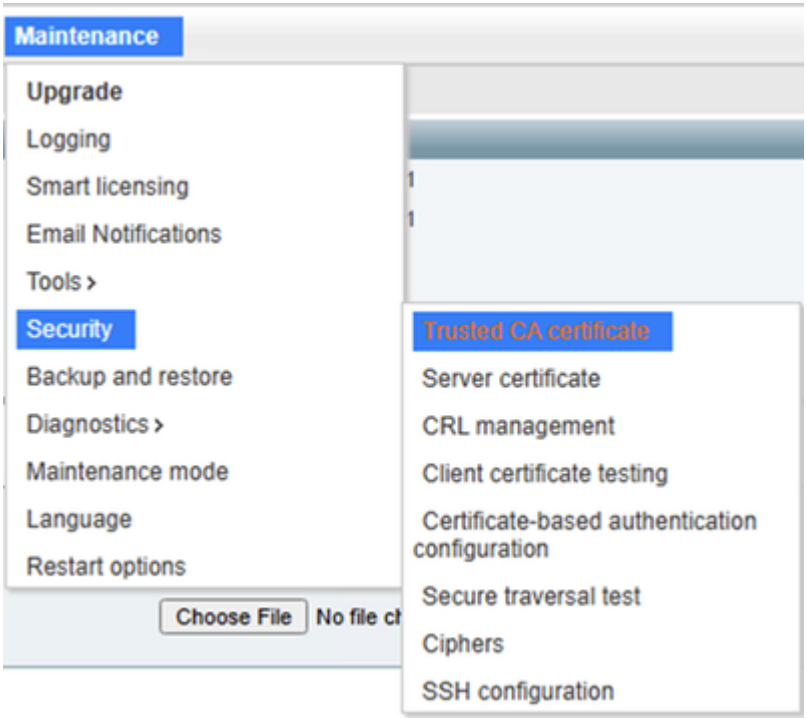
Medium Impact.

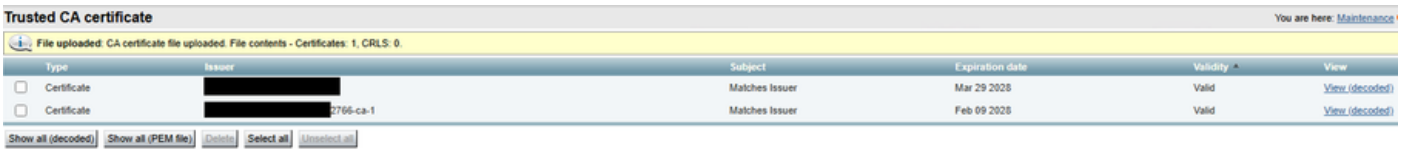
1. CA署名付き証明書を使用してCUCMとExpressway間の信頼関係を構築する手順

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。



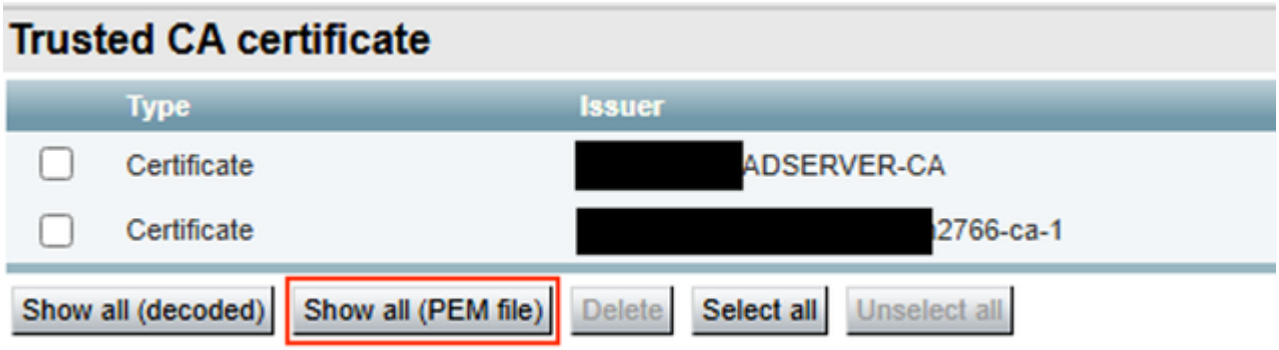
次に、Expressway-C > Maintenance > Security > Trusted CA certificateの順に移動し、Call ManagerとTomcatのCA証明書をアップロードします。



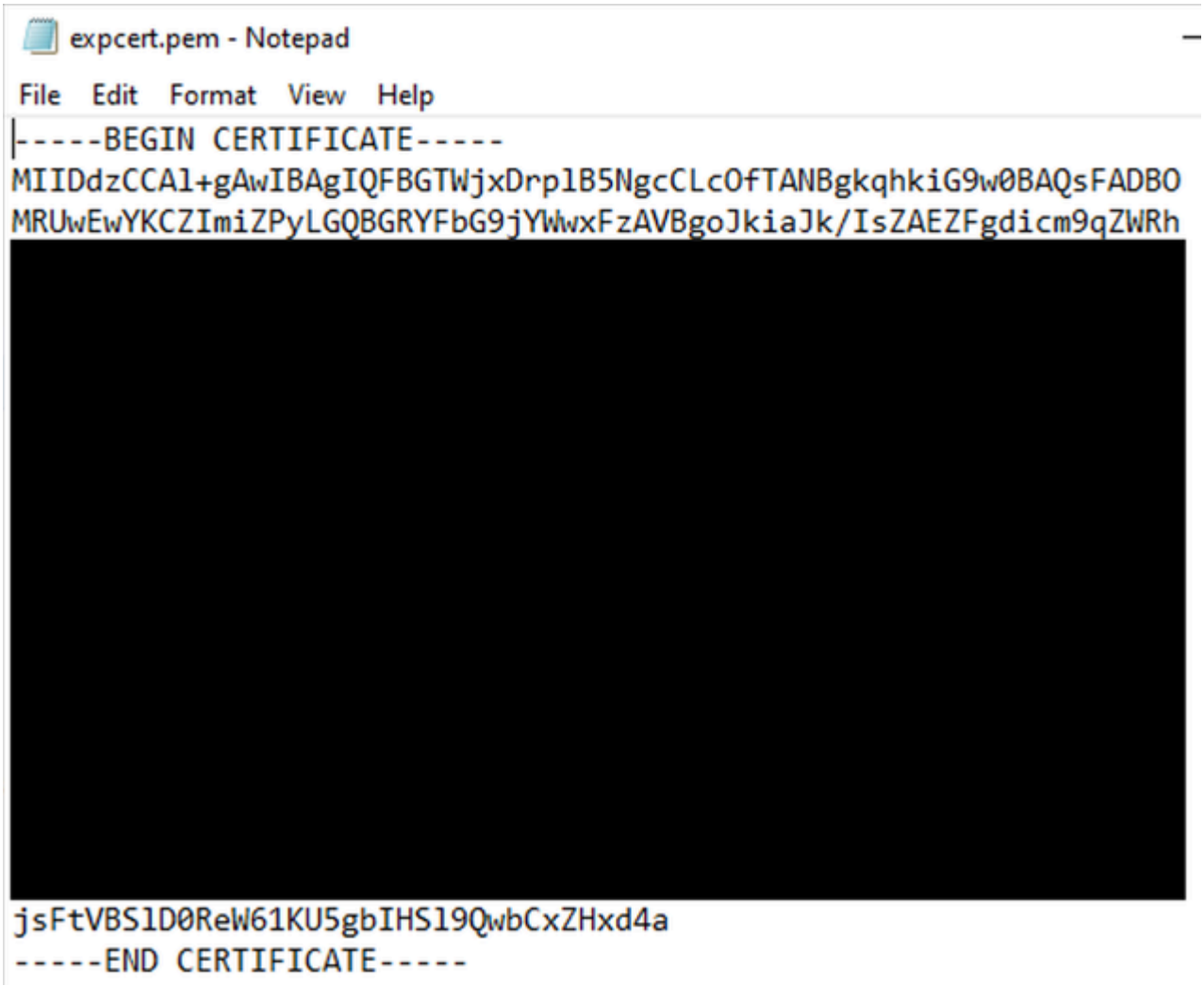


注：Call ManagerとTomcat証明書が自己署名のシナリオでは、実際のCall ManagerとTomcat証明書をダウンロードしてExpresswayにアップロードします。

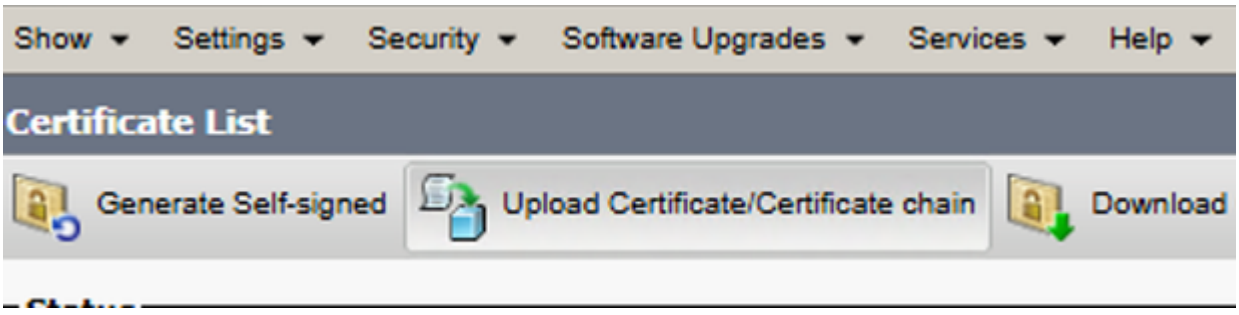
Expressway-C > Maintenance > Security > Trusted CA certificate > Show all (PEM file)の順に移動します。

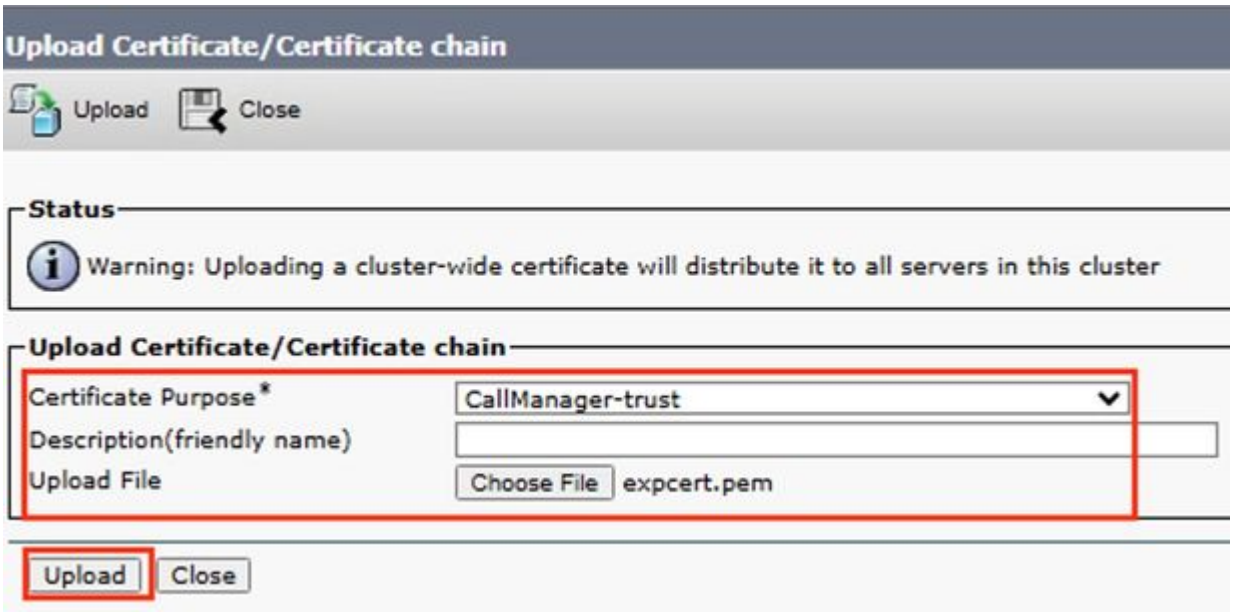


Expressway-Cに署名するCA証明書のPEM値をコピーし、txtファイルに保存します。



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





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。

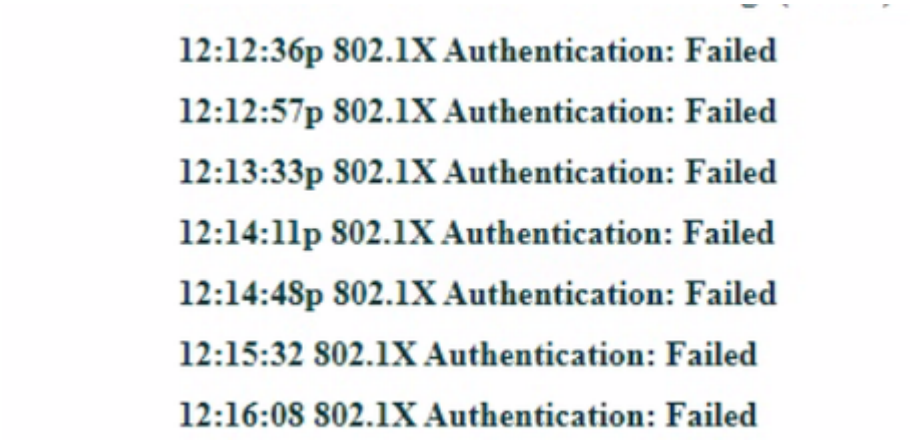
シナリオ4：認証局プロキシ機能(CAPF)証明書の更新が原因

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。

検証

1. 電話ステータスメッセージに「802.1x Authentication: Failed」と表示される



2. 影響を受けるサーバの電話ログを調べ、「SSL_ERROR_WANT_READ」を見つけます。

```
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=0xfff=4095 static=0 pri=
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:
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 pr
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, p
4609 DEB Feb 17 11:01:27.063121 (1786-1880) JAVA-getpaeinfo: recv pae info resp ret=-1, errno=No messag
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
```

ソリューション

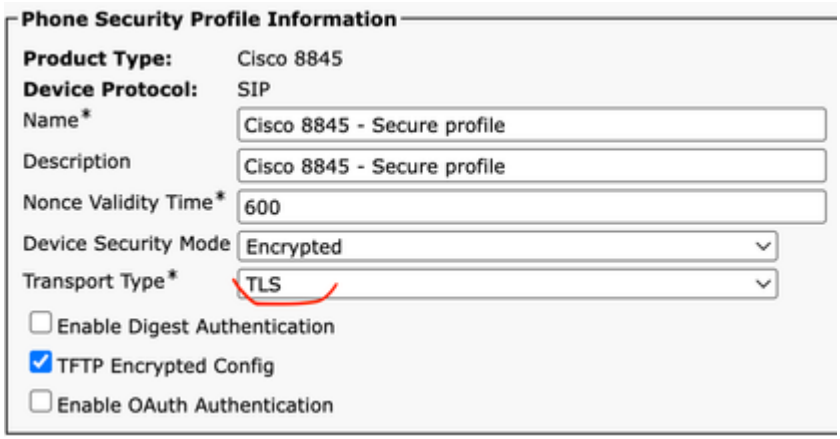
CUCMパブリッシャからCAPF証明書をダウンロードし、認証サーバにアップロードします。
802.1xをバイパスし、登録を許可して、該当する電話機にLSC証明書をインストールします。

シナリオ4.2:TLSモードでセキュリティプ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プロファイルが含まれています。



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。

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プ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.
```

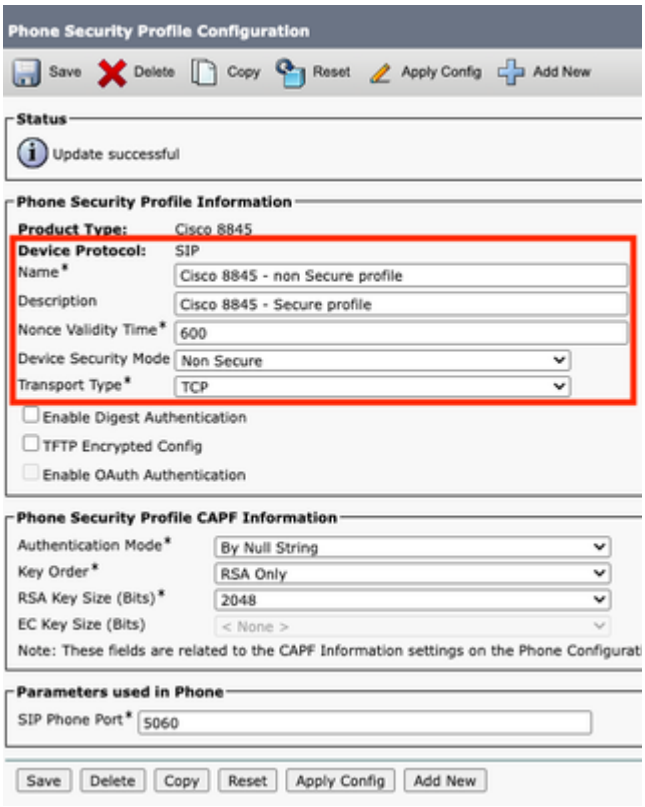
CAPF再生成後にCTLファイルを更新します。 パブリッシャのCLIにログインし、コマンドutils ctl update CTLFileを入力します。

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

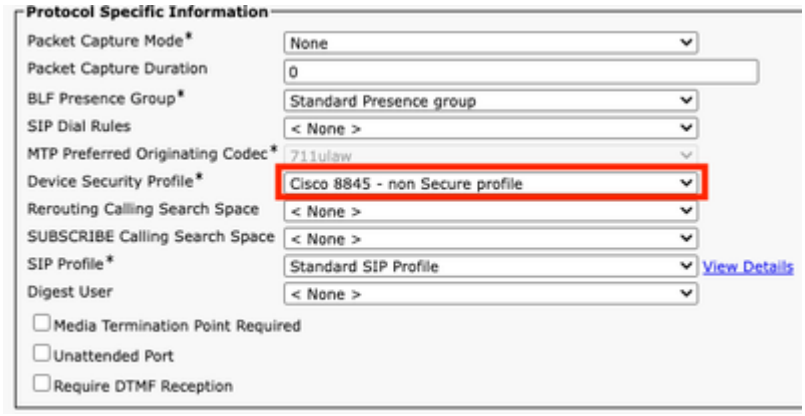
- CM administration > System > Security > Phone Security Profileの順に選択します。

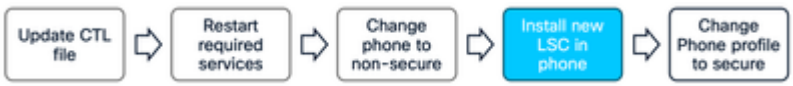
- 必要な電話機に割り当てられている現在の電話セキュリティプロファイルをコピーします。

- 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。



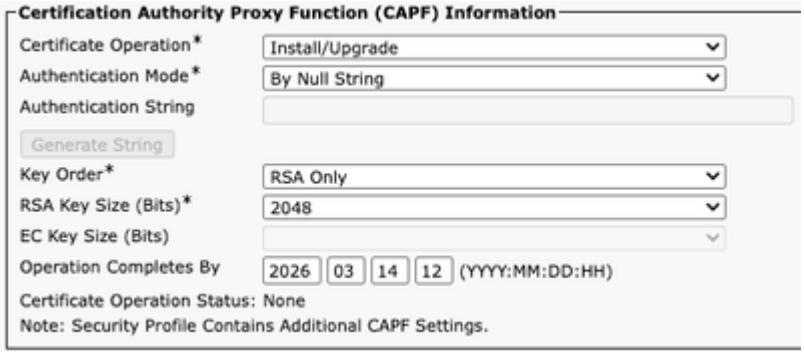
- 作成したデバイスセキュリティプロファイルを必要な電話機の設定に適用します。次に、Save and Apply Configを選択します。





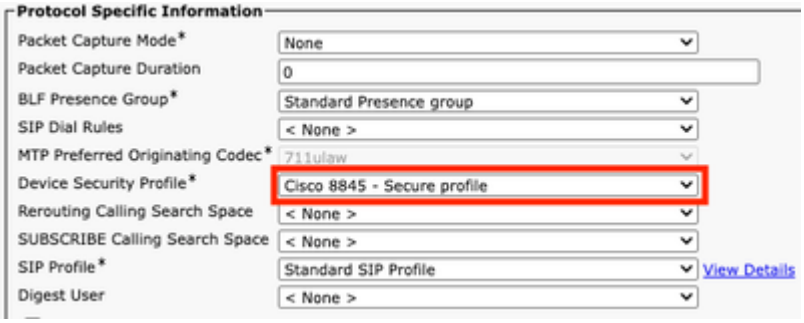
該当する電話機のデバイス設定のCAPF情報セクションを使用して、必要な電話機にLSC証明書をインストールします。

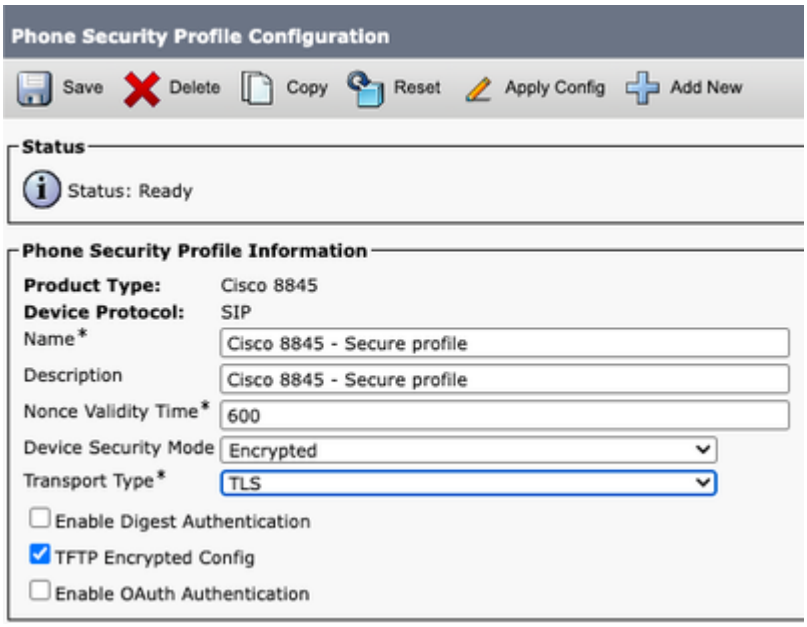
- CAPF情報では、Certificate OperationでInstall/Upgradeを選択します。



- 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。





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

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。