

# Unified Communications Managerでの証明書の再生成

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

#### [Real Time Monitoring Tool\(RTMT\)のインストール](#)

#### [RTMTによるエンドポイントのモニタ](#)

#### [クラスタセキュリティモードの識別](#)

#### [ITLおよびCTL](#)

#### [証明書ストアによる影響](#)

#### [CallManager.pem](#)

#### [Tomcat.pem](#)

#### [CAPF.pem](#)

#### [IPSec.pem](#)

#### [信頼検証サービス\(TVS\)](#)

### [証明書の再生成プロセス](#)

#### [Tomcat証明書](#)

#### [IPSEC証明書](#)

#### [CAPF証明書](#)

#### [CallManager証明書](#)

#### [TVS証明書](#)

#### [ITLRecovery証明書](#)

### [期限切れの信頼証明書の削除](#)

### [検証](#)

### [トラブルシュート](#)

---

## はじめに

このドキュメントでは、Unified Communications Managerで証明書を再生成する手順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。

- リアルタイム監視ツール(RTMT)
- Cisco Unified Communications Managerセキュリティガイド
- CUCM証明書
- 認証局プロキシ機能

## 使用するコンポーネント

次のツールをインストールしておくことを推奨します。

- リアルタイム監視ツール(RTMT)
- Cisco Unified Communications Manager(CUCM)リリース10.5、12.0、14.0、15.0に基づく情報

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ました。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。

## 背景説明

このドキュメントでは、Cisco Unified Communications Manager(CUCM)リリース8.X以降で証明書を再生成する手順について説明します。ご使用のリリースの『セキュリティガイド』を参照してください。

Communications Manager(CUCM)リリース8.X ~ 11.5.X:ITLはCall Manager証明書によって署名されます。

Communications Manager(CUCM)リリース12.0以降では、ITLはITLRecovery証明書によって署名されています。

### ITLファイルとCTLファイルのインタラクション

Cisco IP Phoneは、CTLファイルを使用してクラスタセキュリティモード(非セキュアモードまたは混合モード)を認識します。CTLファイルは、Unified Communications Manager証明書をUnified Communications Managerレコードに含めることによって、クラスタセキュリティモードを追跡します。ITLファイルには、クラスタセキュリティモードの表示も含まれています。

ITL signed by CUCM server (8.x-11.5)				ITL Signed by ITLRecovery certificate (12.0+)			
BYTEPOS	TAG	LENGTH	VALUE	BYTEPOS	TAG	LENGTH	VALUE
1	RECORDLENGTH	2	1662	1	RECORDLENGTH	2	1696
2	DNSNAME	2		2	DNSNAME	2	
3	SUBJECTNAME	64	CN=CM105PUB.my-lab-domain.local;	3	SUBJECTNAME	75	CN=ITLRECOVERY_1251SU6.my-lab-domain.local;
4	FUNCTION	2	System Administrator Security To	4	FUNCTION	2	System Administrator Security Token
5	ISSUENAME	64	CN=CM105PUB.my-lab-domain.local;	5	ISSUENAME	75	CN=ITLRECOVERY_1251SU6.my-lab-domain.local;
6	SERIALNUMBER	16	47:B2:57:50:62:DC:29:0E:AE:69:A4	6	SERIALNUMBER	16	64:79:5C:33:D9:0F:CB:05:4B:5C:E2:F5:76:4D:7
7	PUBLICKEY	270		7	PUBLICKEY	270	
8	SIGNATURE	256		8	SIGNATURE	256	
9	CERTIFICATE	959	DD 76 73 F9 4D 20 1A C1 1D 97 0A	9	CERTIFICATE	971	7A A9 21 CE D9 79 D0 5B 24 46 3D 1D 2E 3F C

This etoken was used to sign the ITL file.

ITL署名者の比較


## Real Time Monitoring Tool(RTMT)のインストール

- Call ManagerからRTMTツールをダウンロードしてインストールします。
  - Call Manager (CM) Administration: Application > Plugins > Find > Cisco Unified Real-Time Monitoring Tool - Windows > Downloadの順に選択します。インストールして起動します。


## RTMTによるエンドポイントのモニタ

- RTMTを起動し、IPアドレスまたは完全修飾ドメイン名(FQDN)を入力してから、ユーザ名とパスワードを入力してツールにアクセスします。
  - Voice/Videoタブを選択します。
  - Device Summaryを選択します。
    - このセクションでは、登録されたエンドポイントの総数と、各ノードへの数を示します。
    - エンドポイントのリセット中に監視し、次の証明書の再生成前に登録を確認します。

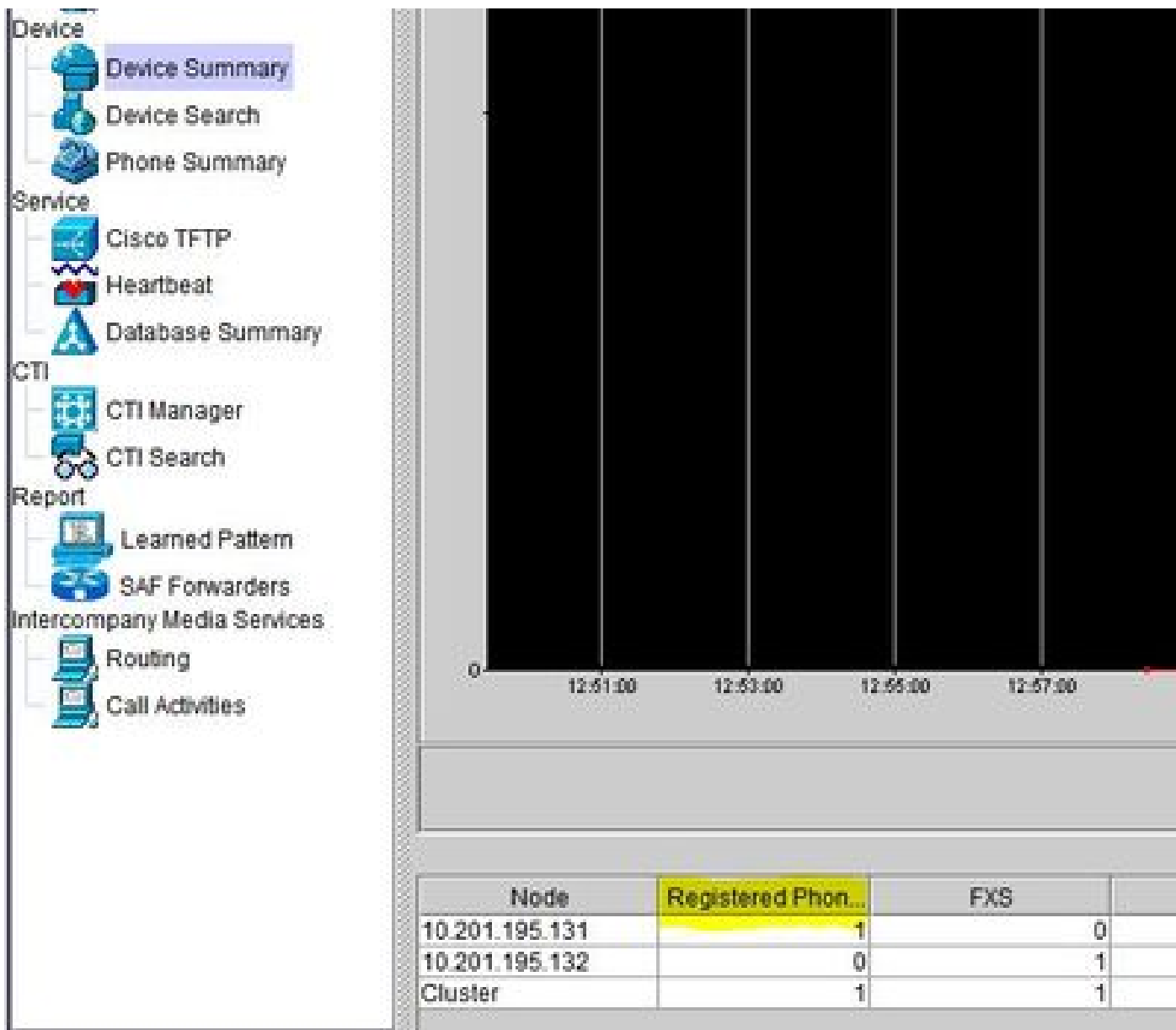
---

 ヒント：一部の証明書の再生成プロセスは、エンドポイントに影響を与える可能性があります。サービスの再起動と電話機の再起動が必要なため、通常の営業時間後にアクションプランを検討してください。プロセスの実行前、実行中、実行後に、RTMTを使用して電話機の登録を確認することを強く推奨します。サービスがサーバ上で実行されている場合にのみ、サービスを再起動する必要があります。

---

 警告：現在ITLの不一致(Bad ITL)があるエンドポイントでは、このプロセスの後に登録の問題が発生する可能性があります。不正なITLがあるデバイスでは、エンドポイントでのITLの削除は、再生成プロセスが完了し、他のすべての電話機が登録された後の一般的なベストプラクティスソリューションです。ITL/CTL (セキュリティ) 証明書を削除する方法については、特定の電話機モデルを確認してください。

---



## クラスタセキュリティモードの識別

- CM Administration: System > Enterprise Parameters > Security Parameters > Cluster Security Modeの順に移動します。

Security Parameters	
Cluster Security Mode *	0 <- Nonsecure Cluster
LBM Security Mode *	Insecure
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
Enable Caching *	True
TLS Ciphers *	All supported AES-256, AES-128 ciphers
SRTP Ciphers *	All supported AES-256, AES-128 ciphers

Security Parameters	
<b>Cluster Security Mode *</b>	<b>1 &lt;- Mixed Mode Cluster</b>
CEM Security Mode	Insecure
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
Enable Caching *	True
TLS Ciphers *	All supported AES-256, AES-128 ciphers
SRTP Ciphers *	All supported AES-256, AES-128 ciphers

## ITLおよびCTL

- Initial Trust List(ITL)には、Call Manager TFTP、ITLRecovery、およびクラスタ内のすべてのTVS証明書の証明書ロールが含まれています。また、サービスが実行されている場合は、Certificate Authority Proxy Function(CAPF)も含まれています。バージョン12.0以降では、ITLはITLRecovery証明書によって署名されています。これは、CLIにログインし、コマンド show itlを入力して確認できます。12.0より前のバージョンでは、ITLはCall Manager証明書によって署名されていました。
- CTLには、同じサーバ上で実行されるSystem Administrator Security Token(SAST)、Cisco CallManagerおよびCisco TFTPサービス、CAPF、ITLRecovery、TFTPサーバ、および適応型セキュリティアプライアンス(ASA)ファイアウォールのエントリが含まれています。TVSはCTLでは参照されません。CTLは、サービス(Cisco CTL Provider)が実行されている場合にエンドポイントに提供されます。
- CUCM 14SU(3)の時点で、Cisco CTL ProviderサービスはCTLトークンをサポートしなくなり、トークンレスがデフォルトでサポートされる方式になっています。

## 証明書ストアによる影響

システムが正常に機能するためには、CUCMクラスタ全体ですべての証明書を更新することが重要です。証明書の有効期限が切れているか無効な場合、システムの通常の機能に大きな影響を与える可能性があります。影響は、システムの設定によって異なる場合があります。無効または期限切れの特定の証明書に対するサービスのリストを次に示します。

### CallManager.pem

- 暗号化または認証された電話機が登録されません。
- Trivial File Transfer Protocol(TFTP ; トリビアルファイル転送プロトコル)が信頼されていない ( 電話機は署名付きコンフィギュレーションファイルやITLファイルを受け付けません )。
- 電話サービスが影響を受ける可能性があります。
- セキュアなセッション開始プロトコル(SIP)トランクまたはメディアリソース(会議ブリッジ、メディアターミネーションポイント(MTP)、Xcoderなど)が登録または機能しません。
- AXL 要求が失敗します。

### Tomcat.pem

- 電話機が社内ディレクトリなどの CUCM ノードでホストされる HTTPS サービスにアクセスできません。
- CUCMには、クラスタ内の他のノードからサービスページにアクセスできないなど、さまざま

まなWebの問題があります。

- エクステンションモビリティ(EM)またはクラスタ間のエクステンションモビリティの問題
- シングルサインオン(SSO)
- Expresswayトラバーサルゾーンがダウンしている ( TLS Verifyが有効 )。
- Unified Contact Center Express(UCCX)が統合されている場合、CCX 12.5からのセキュリティ変更のために、CUCM Tomcat証明書 ( 自己署名 ) またはTomcatルートおよび中間証明書 ( CA署名付き ) をUCCX tomcat-trustストアにアップロードしておく必要があります。これは、Finesseデスクトップログインに影響を与えるためです。

#### CAPF.pem

- この証明書は、エンドポイント ( オンラインおよびオフラインCAPFモードを除く )、電話VPN、802.1x、および電話プロキシにLSCを発行するために使用されます。
- Unified Communications Managerリリース11.5(1) SU1以降では、CAPFサービスによって発行されたすべてのLSC証明書はSHA-256アルゴリズムで署名されます。
- CTI、JTAPI、およびTAPIの認証と暗号化の設定。

#### IPSec.pem

- ディザスタリカバリシステム(DRS)/ディザスタリカバリフレームワーク(DRF)が正常に機能しません。
- ゲートウェイ(GW)または他のCUCMクラスタへのIPsecトンネルが機能しません。

#### 信頼検証サービス(TVS)

信頼検証サービス(TVS)は、デフォルトではセキュリティの主要なコンポーネントです。TVSを使用すると、HTTPSの確立時にCisco Unified IP PhoneでEMサービス、ディレクトリ、MIDletなどのアプリケーションサーバを認証できます。

TVSには次の機能があります。

- 拡張性 : Cisco Unified IP Phoneのリソースは、信頼する証明書の数の影響を受けません。
- 柔軟性 : 信頼証明書の追加または削除は、システムに自動的に反映されます。
- デフォルトのセキュリティ : メディアおよび信号セキュリティ以外の機能はデフォルトのインストールに含まれており、ユーザの介入は必要ありません。

#### ITLRecovery ( 信頼検証サービス )

- 8.X - 11.5 ITLの不一致がある電話機のリカバリ、電話機の移行、およびEMCCからCUCM 12.0+への移行。
- 12.0+ ITL/CTLのSSO、EMCCおよびプライマリ署名者で使用されます。
- 12.5+ ITLリカバリは、パブリッシャによってのみ生成されます。


#### Certificate Manager ECDSAのサポート

Unified Communications Managerリリース11.0では、証明書マネージャは自己署名ECDSA証明書の生成とECDSA証明書署名要求(CSR)の両方をサポートします。 Unified Communications Managerの以前のリリースでは、RSA証明書だけがサポートされていました。ただし、Unified

Communications Managerリリース11.0以降では、CallManager-ECDSA証明書が既存のRSA証明書とともに追加されています。


CallManagerとCallManager-ECDSAの両方の証明書が、共通の証明書信頼ストアであるCallManager-Trustを共有します。Unified Communications Managerは、これらの証明書をこの信頼ストアにアップロードします。

## サードパーティCA署名付きID証明書

 注：サードパーティとは、内部の認証局(CA)、またはGo-Daddy、Verisignなどの外部ソースを意味します。ID証明書は、特定のロール ( Tomcat、Call Managerなど ) のサーバ証明書です。

1. クラスタ内の各サーバに移動します ( マルチSAN CSRを作成している場合を除き、Webブラウザの個別のタブで )。パブリッシャから開始し、各サブスクリバが成功します。  
Cisco Unified OS Administration > Security > Certificate Managementの順に移動します。
2. [CSR の作成 ( Generate CSR ) ] を選択します。
3. Certificate Purposeドロップダウンを選択し、証明書を選択します。
4. Distributionタイプを選択します。シングルサーバまたはマルチサーバ(SAN)。
  - マルチサーバ(SAN)には、SANセクションのすべてのCUCMおよびCUPノードが含まれます。
5. Generateを選択します。
6. CSRをダウンロードし、認証局に提供します。
7. 署名付き証明書を受信したら、チェーン順に証明書をアップロードします。
  - ルートを信頼証明書としてアップロードします。
  - 中間証明書を信頼証明書としてアップロードします。
  - 証明書タイプとして署名付き証明書をアップロードします。
  - ポップアップで特定された適切なサービスを再起動します。

## 証明書の再生成プロセス

 注：証明書を再生成する前に、すべてのエンドポイントの電源をオンにして登録する必要があります。それ以外の場合は、接続されていない電話機でITLを削除する必要があります。

### Tomcat証明書

TomcatおよびTomcat-ECDSAの再生成プロセスは、サービスの再起動を含めて同じです。

サードパーティの証明書が使用されているかどうかを確認します。

1. Webブラウザの個別のタブで、クラスタ内の各サーバに移動します。パブリッシャから始まり、サブスクリバごとに続きます。 Cisco Unified OS Administration > Security > Certificate Management > Findの順に移動します。
  - 「Description」列で、「Tomcat」が「Self-signed certificate generated by system」と表示されるかどうかを確認します。Tomcatがサードパーティによって署名されている

場合は、提供されているリンクを使用して、Tomcatの再生成後に次の手順を実行します。

- サードパーティの署名付き証明書については、『[CCMAdmin Web GUI証明書のCUCMへのアップロード](#)』を参照してください。
2. Findを選択してすべての証明書を表示します。
    - 「Find Tomcat Pem」を選択します。
    - 開いたら、Regenerateを選択し、Successポップアップが表示されるまで待ってからポップアップを閉じるか、戻ってFind/Listを選択します。
  3. 後続の各サブスクリバで手順2と同じ手順を実行し、クラスタ内のすべてのサブスクリバで完了します。
  4. すべてのノードでTomcat証明書を再生成した後、すべてのノードでtomcatサービスを再起動します。パブリッシャから開始し、サブスクリバから続行します。
    - tomcatを再起動するには、各ノードのCLIセッションを開き、コマンドutils service restart Cisco Tomcatを実行する必要があります。

```
admin:
admin:utils service restart Cisco Tomcat
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```


5. 次の手順は、CCX環境から使用されます (該当する場合)。


- 自己署名証明書を使用する場合は、CUCMクラスタのすべてのノードからUnified CCX Tomcat信頼ストアにTomcat証明書をアップロードします。
- CA署名付き証明書またはプライベートCA署名付き証明書を使用する場合、CUCMのルートCA証明書をUnified CCX Tomcat信頼ストアにアップロードします。
- CCXの証明書の再生成に関するドキュメントの説明に従って、サーバを再起動します。


その他の参考資料:

- [UCCXソリューション証明書管理ガイド](#)
- [Unified CCXヘルスチェックユーティリティ](#)

## IPSEC証明書

 注：バージョン10.Xより前のCUCM/Instant Messaging and Presence(IM&P)では、DRF<sub>Master</sub> AgentはCUCMパブリッシャとIM&Pパブリッシャの両方で動作します。DRFローカルサービスは、加入者でそれぞれ実行されます。バージョン10.X以降では、DRF<sub>Master</sub> AgentはCUCMパブリッシャだけで動作し、DRF LocalサービスはCUCMサブスクリバ、IM&Pパブリッシャ、およびサブスクリバで動作します。


 注：デザスタリカバリシステムは、CUCMクラスタノード間のデータの認証と暗号化に、Masterエージェントとローカルエージェント間のSecure Socket Layer(SSL)ベースの通信を使用します。DRSは、公開/秘密キーの暗号化にIPSec証明書を使用します。Certificate


 ManagementページからIPSECトラストストア(hostname.pem)ファイルを削除すると、DRSが期待どおりに動作しなくなることに注意してください。IPSEC-trustファイルを手動で削除する場合は、必ずIPSEC証明書をIPSEC信頼ストアにアップロードしてください。詳細については、『Cisco Unified Communications Managerセキュリティガイド』の証明書管理のヘルプページを参照してください。

1. クラスタ内の各サーバに移動し ( Webブラウザの個別のタブで )、パブリッシャから開始し、各サブスクリバが成功します。Cisco Unified OS Administration > Security > Certificate Management > Findの順に移動します。
  - 証明書を選択します。IPSEC PEM
  - 開いたら、Regenerateを選択し、Successポップアップが表示されるまで待つてからポップアップを閉じるか、前に戻ってFind/Listを選択します。
2. 後続のサブスクリバで続行します。ステップ1と同じ手順を実行し、クラスタ内のすべてのサブスクリバで完了します。
3. すべてのノードがIPSEC証明書を再生成した後、サービスを再起動します。
  - パブリッシャのCisco Unified Serviceabilityに移動します。
    1. Cisco Unified Serviceability > Tools > Control Center - Network Services
    2. Restart on Cisco DRF Master Serviceを選択します。
    3. サービスの再起動が完了したら、パブリッシャのCisco DRF Local ServiceでRestartを選択し、サブスクリバで続行してCisco DRF LocalでRestartを選択します。

パブリッシャのIPSEC.pem証明書が有効であり、すべてのサブスクリバにIPSECトラストストアとして存在する必要があります。サブスクリバのIPSEC.pem証明書が、標準の展開でIPSEC-trustとしてパブリッシャに存在しない。有効性を確認するために、パブリッシャからのIPSEC.pem証明書のシリアル番号とSUBのIPSEC-trustを比較します。これらは一致する必要があります。

## CAPF証明書

 注:CUCM 14以降、CAPF証明書はパブリッシャ上でのみ見つかります。

 **警告**：続行する前に、クラスタが混合モードであるかどうかを確認してください。「クラスタセキュリティモードの特定」のセクションを参照してください。

1. Cisco Unified CM Administration > System > Enterprise Parametersの順に移動します。
  - セクション「セキュリティパラメータ」を確認し、クラスタセキュリティモードが0または1に設定されていることを確認します。値が0の場合、クラスタは非セキュアモードです。1の場合、クラスタは混合モードであり、サービスを再起動する前にCTLファイルを更新する必要があります。トークンおよびトークンレスリンクを参照してください。
2. クラスタ内の各サーバに移動します ( Webブラウザの個別のタブで )。最初にパブリッシャを指定し、次に各サブスクリバを指定します。Cisco Unified OS Administration > Security > Certificate Management > Findの順に移動します。
  - 証明書を選択します。CAPF PEM


- 開いたら、Regenerateを選択し、Successポップアップが表示されるまで待ってからポップアップを閉じるか、戻ってFind/Listを選択します。
3. 後続のサブスクリイバで続行します。ステップ2と同じ手順を実行し、クラスタ内のすべてのサブスクリイバで完了します。
    - クラスタが混合モードであるか、またはCTLが802.1Xに使用されている場合、先に進む前にCTLを更新する必要があります。
      - 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
      - 
      - CTLファイルの更新を有効にするために、暗号化および認証済みのすべての電話機をリセットします。
  4. すべてのノードがCAPF証明書を再生成した後、サービスを再起動します。
    - パブリッシャのCisco Unified Serviceabilityに移動します。
      1. Cisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に選択します。
      2. パブリッシャを選択し、Cisco Certificate Authority Proxy Function ServiceでRestartを選択します (アクティブな場合のみ)。
  5. Cisco Unified Serviceability > Tools > Control Center - Network Servicesの順に移動します。
    - パブリッシャから開始し、サブスクリイバを使用して続行し、Restart on Cisco Trust Verification Serviceを選択します。
    - Cisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に移動します。
    - パブリッシャから開始し、サブスクリイバを使用して続行し、ステータスがStartedのCisco TFTP Serviceを再起動します。
  6. すべての電話機をリポートします。
    - オプション 1
    - Cisco Unified CM Administration > System > Enterprise Parameters
    - Resetを選択すると、「You are about reset all devices in the system.この操作は元に戻せません。Continue?」と表示されたら、OKを選択し、次にResetを選択します。
      - このメソッドは、Call Managerのすべてのコンポーネントをリセットします。
    - オプション 2
    - Cisco Unified CM Administration > Bulk Administration > 電話>電話の更新>クエリ
      - デバイス名は、SEP > Next > Reset Phones > Run Immediatelyで始まる名前で検索します。

これで電話機がリセットされます。RTMTツールを使用して各自のアクションをモニタし、リセットが成功してデバイスがCUCMに再登録されたことを確認します。電話機の登録が完了してから、次の証明書に進みます。電話機の登録プロセスには、時間がかかる場合があります。再生成プロセスの前に不良ITLがあったデバイスは、削除されるまでクラスタに登録されません。


## CallManager証明書

CallManagerとCallManager-ECDSAの再生成プロセスは、サービスの再起動を含めて同じです。

---

 **警告**：続行する前に、クラスタが混合モードであるかどうかを確認してください。「クラスタセキュリティモードの特定」のセクションを参照してください。

---

 **警告**：バージョン8.x ~ 11.5ではCallManager.PEM証明書とTVS.PEM証明書を同時に再生成しないでください。また、ITLがCall Manager証明書によって署名されている場合は再生成しないでください。これにより、クラスタ内のすべてのエンドポイントからITLを削除するか、DRSから復元して証明書の更新を再度開始する必要があるエンドポイントにインストールされたITLとの間に、回復不能な不一致が発生します。

1. Cisco Unified CM Administration > System > Enterprise Parametersの順に移動します。
  - セクション「セキュリティパラメータ」を確認し、クラスタセキュリティモードが0または1に設定されていることを確認します。値が0の場合、クラスタは非セキュアモードです。1の場合、クラスタは混合モードであり、サービスを再起動する前にCTLファイルを更新する必要があります。トークンおよびトークンレスリンクを参照してください。
2. クラスタ内の各サーバに移動します ( Webブラウザの個別のタブで )。最初にパブリッシャを指定し、次に各サブスクリバを指定します。Cisco Unified OS Administration > Security > Certificate Management > Findの順に移動します。
  - CallManager pem Certificateを選択します。
  - 開いたら、Regenerateを選択し、Successポップアップが表示されるまで待つてからポップアップを閉じるか、戻ってFind/Listを選択します。
3. 後続のサブスクリバで続行します。ステップ2と同じ手順を実行し、クラスタ内のすべてのサブスクリバで完了します。
  - クラスタが混合モードの場合、またはCTLが802.1Xで使用されている場合は、先に進む前にCTLを更新する必要があります。
    - 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。
    - CTLファイルの更新を有効にするために、暗号化および認証済みのすべての電話機をリセットします。
4. パブリッシャのCisco Unifiedサービスアビリティにログインします。
  - Cisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に移動します。
  - パブリッシャから開始して、サブスクリバを使用し続けます。ステータスがStartedのCisco CallManager Serviceだけを再起動します。
5. Cisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に移動します。
  - パブリッシャから開始して、サブスクリバを使用し続け、ステータスがStartedのCisco CTIManager Serviceを再起動します。
6. Cisco Unified Serviceability > Tools > Control Center - Network Serviceの順に移動します。
  - パブリッシャから開始し、サブスクリバで続行して、Cisco Trust Verification Serviceを再起動します。
7. Cisco Unified Serviceability > Tools > Control Center - Feature Servicesの順に移動します。
  - パブリッシャから開始して、サブスクリバを使用し続け、ステータスがStartedのCisco TFTP Serviceを再起動します。
8. すべての電話機をリポートします。
  - オプション 1
  - Cisco Unified CM Administration > System > Enterprise Parameters
    - Resetを選択すると、「You are about reset all devices in the system.この操作は元に戻せません。Continue?」と表示されたら、OKを選択し、次にResetを選択


します。

- このメソッドは、Call Managerのすべてのコンポーネントをリセットします。
- オプション 2
- Cisco Unified CM Administration > Bulk Administration > 電話>電話の更新>クエリ
  - デバイス名はSEP > Next > Reset Phones > Run Immediatelyで始まる検索


これで電話機がリセットされます。RTMTツールを使用して各自のアクションをモニタし、リセットが成功してデバイスがCUCMに再登録されたことを確認します。電話機の登録が完了してから、次の証明書に進みます。電話機の登録プロセスには、時間がかかる場合があります。再生成プロセスの前に不良ITLがあったデバイスは、ITLが削除されるまでクラスタに登録されません。

## TVS証明書

---

 **警告**：バージョン8.x ~ 11.5ではCallManager.PEM証明書とTVS.PEM証明書を同時に再生成しないでください。また、ITLがCall Manager証明書によって署名されている場合は再生成しないでください。これにより、クラスタ内のすべてのエンドポイントからITLを削除するか、DRSから復元して証明書の更新を再度開始する必要があるエンドポイントにインストールされたITLとの間に、回復不能な不一致が発生します。

---

 **注**:TVSは、Call Managerに代わって証明書を認証します。この証明書を最後に再生成します。

---

クラスタ内の各サーバに移動します ( Webブラウザの個別のタブで )。最初にパブリッシャを指定し、次に各サブスクリバを指定します。 Cisco Unified OS Administration > Security > Certificate Management > Findの順に移動します。


- TVS pem証明書を選択します。
  - 開いたら、Regenerateを選択し、成功のポップアップが表示されるまで待ってからポップアップを閉じるか、戻ってFind/Listを選択します。
1. 後続のサブスクリバで続行します。ステップ1と同じ手順を実行し、クラスタ内のすべてのサブスクリバで完了します。
    - すべてのノードがTVS証明書を再生成した後、サービスを再起動します。
      - パブリッシャのCisco Unified Serviceabilityにログインします。
        - Cisco Unified Serviceability > Tools > Control Center - Network Servicesの順に移動します。
        - パブリッシャで、Restart on Cisco Trust Verification Serviceを選択します
        - 
        - サービスの再起動が完了したら、サブスクリバで続行し、Cisco Trust Verification Serviceを再起動します。
  2. パブリッシャから開始し、サブスクリバを使用して続行し、ステータスがStartedになっているCisco TFTP Serviceを再起動します。
  3. すべての電話機をリブートします。
    - オプション 1
    - Cisco Unified CM Administration > System > Enterprise Parameters
      - Resetを選択すると、「You are about reset all devices in the system.この操作は

元に戻せません。Continue?」と表示されたら、OKを選択し、次にResetを選択します。

- このメソッドは、Call Managerのすべてのコンポーネントをリセットします。
- オプション 2
- Cisco Unified CM Administration > Bulk Administration > 電話>電話の更新>クエリ
  - デバイス名は、SEP > Next > Reset Phones > Run Immediatelyで始まる名前で検索します。

これで電話機がリセットされます。RTMTツールを使用して各自のアクションをモニタし、リセットが成功してデバイスがCUCMに再登録されたことを確認します。電話機の登録が完了してから、次の証明書に進みます。電話機の登録プロセスには、時間がかかる場合があります。再生成プロセスの前に不良ITLがあったデバイスは、ITLが削除されるまでクラスタに登録されません。

## ITLRecovery証明書

 注:ITLRecovery証明書は、デバイスが信頼できるステータスを失ったときに使用されます。証明書はITLとCTLの両方に表示されます(CTLプロバイダーがアクティブの場合、Cisco bug [IDCSCwf85275](https://tools.cisco.com/bugtools/bugsearch/show/IDCSCwf85275))。

12.5+以降では、ITLRecoveryはパブリッシャによって生成され、サブスクリバに配布される単一の証明書です。

デバイスの信頼ステータスが失われた場合は、非セキュアクラスタにはutils itl reset localkeyコマンドを、ミックスマードクラスタにはutils ctl reset localkeyコマンドを使用できます。ITLRecovery証明書の使用方法および信頼できるステータスを回復するために必要なプロセスについて理解するには、使用しているCall Managerバージョンのセキュリティガイドをお読みください。


クラスタが2048のキー長をサポートするバージョンにアップグレードされ、クラスタサーバ証明書が2048に再生成された場合、ITLRecoveryが再生成されておらず、現在のキー長が1024である場合、ITL回復コマンドは失敗し、ITLRecoveryメソッドは使用されません。

1. クラスタ内の各サーバに移動します ( Webブラウザの個別のタブで )。最初にパブリッシャを指定し、次に各サブスクリバを指定します。 Cisco Unified OS Administration > Security > Certificate Management > Findの順に移動します。
  - ITLRecovery pem証明書を選択します。
  - 開いたら、Regenerateを選択し、成功のポップアップが表示されるまで待つからポップアップを閉じるか、戻ってFind/Listを選択します。
2. ITLRecovery証明書が再生成された後、サービスを再起動する必要があります。
  - クラスタが混合モードであるか、CTLが802.1Xに使用されている場合は、先に進む前にCTLを更新する必要があります。
    - 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。
    - CTLファイルの更新を有効にするために、暗号化および認証済みのすべての電話機をリセットします。
  - パブリッシャにログイン Cisco Unified Serviceability.
    - Cisco Unified Serviceability > Tools > Control Center - Network Servicesの順に移動します。
    - パブリッシャで、Restart on Cisco Trust Verification Serviceを選択します。


- サービスの再起動が完了したら、サブスクライバで続行し、Cisco Trust Verification Serviceを再起動します。
- 3. パブリッシャから開始して、サブスクライバを使用し続け、ステータスがStartedになっているCisco TFTP Serviceを再起動します。
- 4. すべての電話機をリポートします。
  - オプション 1
  - Cisco Unified CM Administration > System > Enterprise Parameters
    - Resetを選択すると、「You are about reset all devices in the system.この操作は元に戻せません。Continue?」と表示されたら、OKを選択し、次にResetを選択します。
    - このメソッドは、Call Managerのすべてのコンポーネントをリセットします。
  - オプション 2
  - Cisco Unified CM Administration > Bulk Administration > 電話>電話の更新>クエリ
    - デバイス名は、SEP > Next > Reset Phones > Run Immediatelyで始まる名前で検索します。

## 期限切れの信頼証明書の削除

---

 **警告：** 証明書を削除すると、システムの動作に影響を与える可能性があります。証明書が既存のチェーンの一部である場合は、証明書チェーンを解除することもできます。Certificate Listウィンドウの関連する証明書のユーザ名とサブジェクト名で、この関係を確認します。

---

 **注:** 削除できる証明書の種類は、信頼できる証明書のみです。システムによって生成された自己署名証明書は削除できません。 削除する必要がある、不要になった、または有効期限が切れた信頼証明書を特定します。CallManager.pem、tomcat.pem、ipsec.pem、CAPF.pem、およびTVS.pemを含む5つの基本証明書は削除しないでください。信頼証明書は、必要に応じて削除できます。次に再起動するサービスは、それらのサービス内のレガシー証明書の情報をクリアするように設計されています。

---

1. Cisco Unified Serviceability > Tools > Control Center - Network Servicesの順に移動します。
  - ドロップダウンから、CUCMパブリッシャを選択します。
    - CUCM 11.5以下の場合、
    - Stop Certificate Change Notificationを選択します。この要件は、CUCMバージョン12.0以降では不要です。
    - クラスタ内のすべてのCall Managerノードに対して、この手順を繰り返します。
  - IMPサーバがある場合：
    - ドロップダウンメニューからIMPサーバを1つずつ選択し、Stop Platform Administration Web Services and Cisco Intercluster Sync Agentを選択します。この要件は、IMPバージョン12.0以降では不要です。
2. Cisco Unified OS Administration > Security > Certificate Management > Findの順に移動します。
  - 期限切れの信頼証明書を検索します。(バージョン10.X以降では、有効期限でフィルタリングできます。10.0より前のバージョンの場合は、証明書を手動で識別するか、受信した場合はRTMTアラートを使用します)。

- 同じ信頼証明書を複数のノードに表示できます。各ノードから個別に削除する必要があります。
  - 削除する信頼証明書を選択します (バージョンによって、ポップアップが表示されるか、同じページで証明書に移動します)。
    - Deleteを選択します。(「you are about to permanently delete this certificate」で始まるポップアップが表示されます。)
    - OKを選択します。
3. 削除するすべての信頼証明書について、この手順を繰り返します。
  4. 完了時に、削除された証明書に直接関連するサービスを再起動する必要があります。このセクションでは、電話機をリブートする必要はありません。 Call ManagerとCAPFはエンドポイントに影響を与えます。
    - Tomcat-trust : コマンドラインからTomcatサービスを再起動します (「Tomcat」の項を参照)。
    - CAPF-trust: Cisco Certificate Authority Proxy Functionを再起動します (「CAPF」の項を参照)。 エンドポイントをリブートしないでください。
    - CallManager-trust: CallManagerサービス/CTIManager (「CallManagerのセクション」を参照)。 エンドポイントをリブートしないでください。
      - エンドポイントに影響を与え、再起動を引き起こします。
    - IPSEC-trust: DRF Master/DRF Local (「IPSEC」の項を参照)。
    - TVS (自己署名) には信頼証明書がありません。
  5. ステップ1で停止したサービスを再起動します。

## 検証

この設定では、確認手順は使用できません。

## トラブルシューティング

この設定では、トラブルシューティング手順は使用できません。

## 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。