CUCM 証明書の再生成/更新プロセス

目次

概要
概要
使用するコンポーネント
証明書を再生成するタイミング
証明書ストアによるサービスへの影響
DRS バックアップの作成
クラスタが混合モードか確認する
クラスタが混合モードの場合
クラスタのデフォルト セキュリティを確認する
「Prepare Cluster for Rollback to pre 8.0」機能を使用する
特定の順序で証明書を再生成する
CUCM での証明書の削除と再生成
CLI での証明書の再生成
CLI での証明書の削除
Web GUI での証明書の再生成
Web GUI での証明書の削除
証明書の再生成と削除の後
電話機の LSC のインストールと更新
結論
Cisco サポート コミュニティ - 特集対話

概要

このドキュメントでは、Communications Manager（CUCM）リリース 8.x 以降でサポートされている証明書の再生成手順を、順を追って説明します。 望ましくないシステムの停止を回避するため、デフォルトのセキュリティ機能（ITL）および混合モード（CTL）についても説明します。 電話機の登録時の問題や、電話機が設定変更またはファームウェアを受け入れない問題を回避する方法などを扱います。

> **注意**： 証明書の再生成は、常にメンテナンス ウィンドウで実行することを推奨します。

概要

このドキュメントでは、次のサービス向けの証明書の再生成プロセスについて説明します。

- callmanager
- CAPF（Certificate Authority Proxy Function）
- IPSec
- Tomcat
- TVS（信頼検証サービス）

- ITLRecovery（CUCM 10.X 以降のみ）
- phone-vpn-trust
- phone-sast-trust
- phone-trust
- phone-ctl-trust

次の電話機の証明書についても説明します。

- LSC（ローカルで有効な証明書）
- MIC（製造元でインストールされた証明書）

使用するコンポーネント

このドキュメントに示される出力およびスクリーンショットは CUCM リリース 9.1(2) SU2a に基づいていますが、説明する手順は CUCM リリース8.x 以降でも使用できます。 リリース固有の違いは該当するセクションに記載されています。

このドキュメントの情報は、クリアな（デフォルト）設定で作業を開始したラボ環境にあるデバイスに基づいています。 ネットワークが稼働中の場合は、コマンドおよび操作が及ぼす潜在的な影響を十分に理解しておく必要があります。

証明書を再生成するタイミング

新規インストール後に CUCM で使用される証明書の多くは、デフォルトで 5 年間有効な自己署名証明書です。 現在、CUCM では 5 年の時間範囲をより短く変更することはできないことに注意してください。 ただし、認証局（CA）はほぼあらゆる時間範囲で証明書を発行することができます。

また、事前にロードされ、有効期間がより長い、信頼できる証明書もあります（CAPF-trust や CallManager-trust など）。 たとえば、「Cisco Manufacturing CA」証明書は、特定の機能に対して CUCM 信頼ストアで提供され、2029 年まで期限が切れません。

証明書は、満了する前に再生成する必要があります。 証明書の期限が近くなると、RTMT（Syslog Viewer）で警告が発行され、電子メールで通知が送信されます（設定している場合）。

次に、「CUCM01.der」証明書が信頼ストア「tomcat-trust」上のサーバ CUCM02 で「5 月 19 日（月）14 時 46 分」に終了することを伝える証明書の有効期限の通知例を示します。

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
SyslogSeverityMatchFound events generated:

SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent
```

```
ClusterID :

NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

サービス証明書（「-trust」とラベリングされない証明書ストア）がすでに失効している場合でも、それらを再生成することは可能です。 クラスタの設定によっては、期限切れの証明書が CUCM 機能に影響する可能性があることを考慮してください。 考慮事項については、次のセクションで説明します。

証明書ストアによるサービスへの影響

システムの良好な機能には、CUCM クラスタ全体ですべての証明書を更新しておくことが重要です。 証明書が失効または無効になると、システムの正常な機能に深刻な影響を与える可能性があります。 特定の証明書が無効または失効した場合に発生し得る潜在的な問題のリストをここに示します。 この影響は、システムの設定に応じて異なる可能性があります。

CallManager.pem

- 暗号化または認証された電話機が登録されません。
- TFTP が信頼されません（電話機は署名付きの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。
- 安全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）、Xcoders など）が登録されない、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。
- 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、CUCM の Web GUI 問題が発生します。
- エクステンション モビリティおよびクラスタ間のエクステンション モビリティの問題が発生します。

CAPF.pem

- 電話機が、電話 VPN 802.1x または電話プロキシを認証しません。
- 電話機の LSC 証明書を発行できません。
- 暗号化されたコンフィギュレーション ファイルが機能しません。

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）が正しく動作しない可能性があります。
- 他の CUCM クラスタにつながるゲートウェイ（GW）への IPSec トンネルが動作しません。

TVS（信頼検証サービス）

- 電話機が HTTPS サービスを認証できません。 電話機がコンフィギュレーション ファイルを認証できません（これは CUCM のほぼすべてに影響を与える可能性があります）。

phone-vpn-trust

- VPN の HTTPS URL を認証できないため、電話 VPN が機能しません。

  注: これが存在しなくても問題ありません。 これは、特定のコンフィギュレーションに限ります。

phone-sast-trust

- 以前の CTL/eToken が CTL を更新または変更できません。

  注: これが存在しなくても問題ありません。 これは、特定のコンフィギュレーションに限ります。

phone-trust および phone-ctl-trust

- Visual Voicemail が Unity または Unity Connection で機能しません。

  注: これが存在しなくても問題ありません。 これは、特定のコンフィギュレーションに限ります。

LSC または MIC

- 電話機が登録できず、電話機が電話 VPN、電話プロキシ、または 802.1x を認証しません。

  注: MIC はほとんどの電話機モデルにデフォルトで付属しています。 LSC は CAPF によって署名され、デフォルトで 5 年間有効です。 CIPC（Cisco IP Communicator）および Jabber などのソフトウェア クライアントは、MIC がインストールされていません。

DRS バックアップの作成

このような大きな変更を行う前に、DRS のバックアップを作成することを推奨します。 CUCM DRF バックアップは、クラスタ内のすべての証明書をバックアップします。 すべての DRS バックアップ/復元手順は、シスコの『Cisco Unified Communications Manager のためのディザスタ リカバリ システム管理ガイド』で確認できます。

> **注意**： Cisco bug ID CSCtn50405（CUCM DRF バックアップでは証明書がバックアップされない）を確認してください。

クラスタが混合モードか確認する

クラスタが CTL/Secure/混合モードのどのモードで実行されているかを調べるには、[Cisco Unified CM Administration] > [System] > [Enterprise Parameters] > [Cluster Security Mode] を選択します（0 == Non-Secure、 1 == 混合モード）。

クラスタが混合モードの場合

CUCM クラスタを混合モードで実行している場合、すべての証明書を変更した後で、CTL ファイルを更新する変更があることを意味します。 この方法の手順は、『シスコ セキュリティ ガイド』に記載しています。 ただし、混合モード機能を最初に開始したときの eToken が少なくとも 1 つあり、eToken のパスワードを把握していることを確認してください。

注: CTL の更新は、自動的に行われません（ITL ファイルの場合と同様）。 これは、CTL クライアントまたは CLI コマンドを使用して、管理者が手動で実行する必要があります。

CUCM 10.X 以降では、次の 2 つの方法でクラスタを混合モードにすることができます。

- CLI コマンド：この方法を使用すると、CTL ファイルがパブリッシャ サーバの CallManager.pem 証明書によって署名されます。 admin:**show ctl**

```
The checksum value of the CTL file:
0c05655de63fe2a042cf252d96c6d609(MD5)
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1156
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 694 E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
A5 A3 8C 9C (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

- CTL クライアント：この方法を使用すると、CTL ファイルがハードウェア eToken のいずれかによって署名されます。 admin:**show ctl**

```
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

注: 使用する方法は、CUCM 混合モードとトークンを使用しない CTL の間で切り替えできます。

クラスタのセキュリティを保護する方法に応じて、適切な CTL 更新手順を実行する必要があります。 CTL クライアントを再実行するか、または CLI から **utils ctl update CTLfile** コマンドを入力します。

クラスタのデフォルト セキュリティを確認する

ITL の問題は多くの機能に障害を発生させたり、電話機が設定変更に従うことを拒否する原因となるため、ITL の問題を回避することが重要です。 ITL の問題は、次の 2 つの方法で回避できます。

「Prepare Cluster for Rollback to pre 8.0」機能を使用する

この機能はすべてのサーバの ITL を「無力化」するため、電話機は任意の TFTP サーバを信頼します。 このパラメータを True に設定すると、電話サービス（エクステンション モビリティなど）は機能しません。 ただし、基本的な電話の発信や受信は引き続き実行できます。

注: このパラメータを変更すると、すべての電話機がリセットします。

この機能を設定したら、プロビジョニングするすべての TFTP サーバの再起動（新しい ITL を提供するため）と、すべての電話機のリセット（これらに新しい「ブランク」ITL を要求させるため）が必要です。 証明書の変更が完了し、すべての必要なサービスを再起動したら、この機能の設定を「False」に戻し、TFTP サービスを再起動し、電話機をリセット（電話機が有効な ITL ファイルを入手できるように）することができます。 すると、すべての機能が以前と同様に機能し続けるようになります。

特定の順序で証明書を再生成する

この手順は、使用可能な信頼できる TFTP サーバから得た有効な/更新された ITL ファイルを、TFTP サーバに提供します。

1. プライマリ TFTP サーバの TFTP サービスを停止します。
2. プライマリ TFTP サーバの証明書を変更します（必要に応じて）。
3. 電話機をリセットします（新しい ITL ファイルをセカンダリ TFTP サーバから取得するため）。再生成した証明書に応じて、この手順は自動的に行われます。
4. 電話機が復帰したら、プライマリ TFTP サーバの TFTP サービスを開始します。
5. セカンダリ TFTP サーバの証明書を変更します。
6. 電話機をリセットします（新しい ITL ファイルをプライマリ TFTP サーバから取得するため）。

注意： 両方の TFTP サーバの証明書を同時に編集しないでください。 これを行うと、電話機で信頼できる TFTP サーバがなくなり、ローカル管理者は手動ですべての電話機から ITL を削除する必要があります。

CUCM での証明書の削除と再生成

サービス証明書（「-trust」とラベリングされない証明書ストア）のみを再生成できます。 信頼ストア（「-trust」とラベリングされる証明書ストア）の証明書は再生成できないため、削除する必要があります。

> **注意**： Cisco Bug ID CSCut58407（CAPF/CallManager/TVS-trust を削除した場合、デバイスが再起動してはならない）を確認してください。

すべての証明書を変更したら、変更を反映するため、それぞれのサービスを再起動する必要があります。 これについては「証明書の再生成と削除の後」セクションで説明します。

> **注意**： Cisco Bug ID CSCto86463（削除した証明書が再び表示され、CUCM から証明書を削除できない）を確認してください。 これは、削除された証明書が削除後も引き続き表示され続けるという問題です。 問題の回避策を実行します。

CLI での証明書の再生成

> **注意**： 証明書が再生成されると、クラスタ内の ITL ファイルの自動更新が発生します。これがさらに、電話機がローカル ITL の更新を引き起こすことができるように、クラスタ全体のソフト フォン リセットを引き起こします。 これは CAPF 証明書および CallManager 証明書の再生成に集中しますが、Tomcat などの CUCM 内の他の証明書ストアでも発生する可能性があります。

CAPF の再生成

CAPF 証明書が再生成されると、自動的に CAPF-trust と CallManager-trust にアップロードされます。 また、CAPF には常に固有のサブジェクト名ヘッダーがありますので、以前に使用した CAPF 証明書がそのまま認証に使用されます。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
```

```
This etoken was used to sign the CTL file.
```

注: CAPF 証明書が期限切れとなると、CUCM はその証明書を拒否するため、LSC を使用する電話機は CUCM に登録できなくなります。 ただし、新しい CAPF 証明書のある電話機に新しい LSC を生成することはできます。 電話機を再起動すると、電話機は設定をダウンロードし、LSC を更新するため CAPF に接続します。 LSC が更新されると、電話機は登録されます。 これは、新しい CAPF 証明書が ITL ファイルにあり、電話機が自分の署名した証明書（callmanager.pem）をダウンロードして信頼している場合に限り、機能します。

CallManager の再生成

CallManager が再生成されると、自動的に CallManager-trust にアップロードされます。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

IPsec の再生成

IPsec 証明書が再生成されると、自動的に ipsec-trust にアップロードされます。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
```

```
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Tomcat の再生成

Tomcat 証明書が再生成されると、自動的に tomcat-trust にアップロードされます。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

TVS の再生成

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

この処理による影響

CLI で証明書を再生成すると、この変更の確認が求められます。 [Yes] と入力し、Enter キーを押します。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

CLI での証明書の削除

CAPF-trust 証明書の削除

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

CallManager-trust 証明書の削除

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
```

```
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

ipsec-trust 証明書の削除

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Tomcat-trust 証明書の削除

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
```

```
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

TVS-trust 証明書の削除

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Web GUI での証明書の再生成

CAPF の再生成

CAPF 証明書が再生成されると、自動的に CAPF-trust と CallManager-trust にアップロードされます。 また、CAPF 証明書には常に固有のサブジェクト名ヘッダーがありますので、以前に使用した CAPF 証明書がそのまま認証に使用されます。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
```

```
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

CallManager の再生成

CAPF 証明書が再生成されると、自動的に CallManager-trust にアップロードされます。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

IPsec の再生成

IPsec 証明書が再生成されると、自動的に ipsec-trust にアップロードされます。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
```

```
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Tomcat の再生成

Tomcat 証明書が再生成されると、自動的に tomcat-trust にアップロードされます。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

TVS の再生成

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Web GUI での証明書の削除

```
admin:show ctl
The checksum value of the CTL file:
```

```
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

証明書の再生成と削除の後

証明書ストアから証明書を削除または再生成したら、変更を反映するため、それぞれのサービスを再起動する必要があります。

ストア	サービスの再起動	方法（C == CLI、 W == Web GUI）
Tomcat	Tomcat	C： utils service restart Cisco Tomcat G： [Cisco Unified Serviceability] > [Tools] > [Control Ce - [Feature Services] >（サーバを選択） > [Cisco CallManager] を選択 > 再起動
callmanager	CallManager; TFTP	および G： [Cisco Unified Serviceability] > [Tools] > [Control Ce - [Feature Services] >（サーバを選択） > [Cisco Tftp] を > 再起動
CAPF	CAPF（パブリッシャでのみ）	G： [Cisco Unified Serviceability] > [Tools] > [Control Ce - [Feature Services] >（サーバを選択） > [Cisco Certific Authority Proxy Function] を選択 > 再起動
TVS	信頼検証サービス（各サーバで）	G： [Cisco Unified Serviceability] > [Tools] > [Control Cer [Network Services] >（サーバを選択） > [Cisco Trust Verification Service] を選択 > 再起動
IPSec	Cisco DRF Local（すべてのノードで）、 Cisco DRF Master（パブリッシャで）	C： utils service restart Cisco DRF Local および C： utils service restart Cisco DRF Master

電話機の LSC のインストールと更新

CAPF 証明書が再生成されたら、クラスタ内のすべての電話機の LSC 証明書を、新しい CAPF 証明書によって署名された LSC で更新する必要があります。

1. [CUCM Serviceability] > [Service Activation] を選択します。 パブリッシャ サーバで Cisco CTL Provider および Cisco Certificate Authority Proxy Function をアクティブにします。
2. CUCM CCMAdmin から、[Device] > [Phone] を選択します。 LSC をプロビジョニングする

IP Phone を選択します。
3. [Certificate Operation] の [Device configuration] ページで、[Install / Upgrade] > [By Null String] を選択します。
4. CCMAdmin の電話機設定を保存し、[Apply Config] を選択します。

LSC のインストールに問題がある場合、電話機で次の操作を実行してください。

電話機がリセットしたら、実際の電話機で [Settings] > (6) [Security Configuration] > (4) [LSC] > **# (この操作により GUIのロックが解除され、次のステップに進むことができます) > [Update] (前の手順を実行するまで更新は非表示です) > [Submit] を選択します。

無線電話 (7921/25) でない限り、電話機に証明書を割り当てないでください。 無線電話は自身を認証するためにサード パーティ認証局 (CA) を使用します。

結論

この手順で問題が発生したか、またはサポートが必要な場合、Cisco Technical Assistance Center (TAC) にお問い合わせください。 この場合、DRF バックアップを準備しておいてください。TAC が他の方法でサービスを復元できない場合、サービスを復元するための最後の手段として使用します。