

# CallManagerでのマルチSAN Tomcat証明書の再利用の実装

## 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](#)

[設定](#)

[CallManagerでのTomcat証明書の再使用](#)

[確認](#)

---

## はじめに

このドキュメントでは、CUCMのCallManagerでマルチSAN Tomcat証明書を再利用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。

- Cisco Unified Communications Manager ( CUCM )
- CUCM証明書
- ID信頼リスト(ITL)

### 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リリース15 SU1

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。

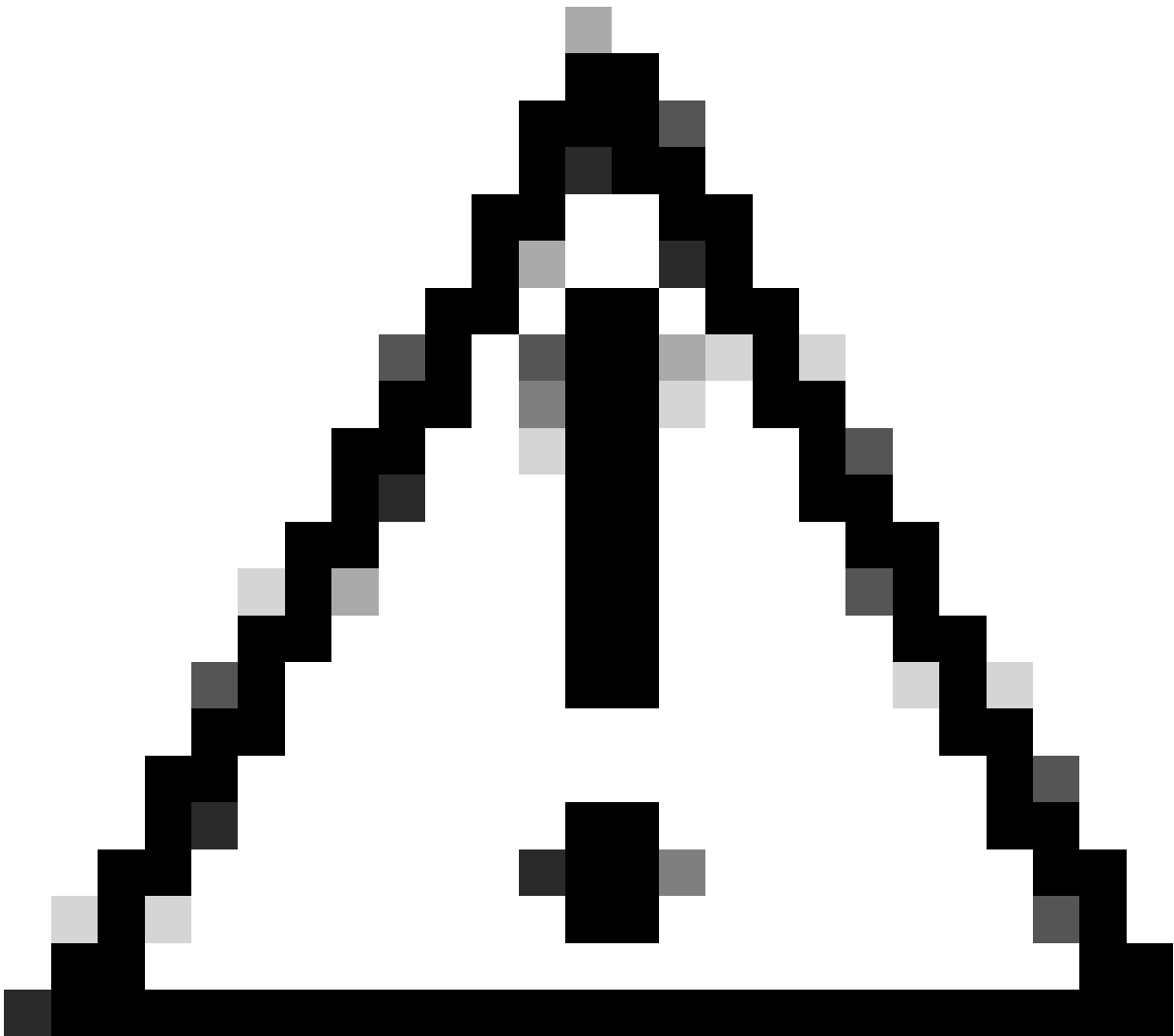
## 背景説明

CUCMの以前のバージョンでは、クラスタ全体でサービスごとに異なる証明書が使用されていた

ため、証明書が増加し、コストが増加しました。これには、それぞれのID証明書を持つ CUCMで実行されている重要なサービスであるCisco TomcatおよびCisco CallManagerが含まれません。

CUCMバージョン14以降では、CallManagerサービスでマルチSAN Tomcat証明書を再利用するための新機能が追加されました。

この機能を使用する利点は、CAから1つの証明書を取得し、それを複数のアプリケーションで使用できることです。これにより、コストの最適化と管理の削減が実現し、ITLファイルのサイズが小さくなるため、オーバーヘッドが削減されます。



注意：再使用の設定に進む前に、Tomcat証明書がマルチサーバSAN証明書であることを確認してください。TomcatマルチSAN証明書は、自己署名またはCA署名にすることができます。



警告：続行する前に、クラスタが混合モードか非セキュアモードかを特定してください。

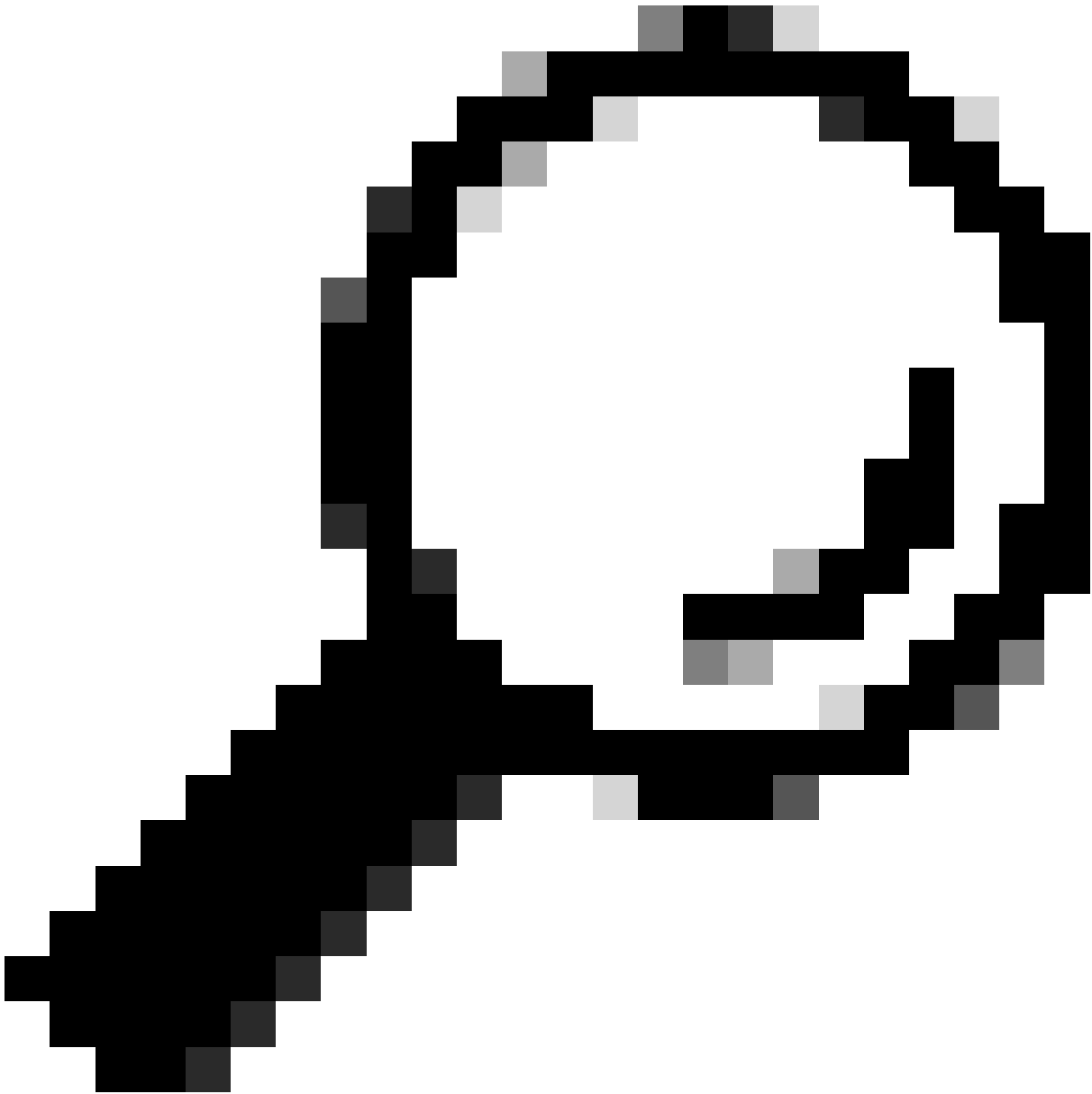
---

ステップ 1：Cisco Unified CM Administration > System > Enterprise Parametersの順に移動します。

セクションSecurity Parametersを確認し、Cluster Security Modeが0または1に設定されているかどうかを確認します。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。

ステップ 2：CUCMパブリッシャに移動し、Cisco Unified OS Administration > Security > Certificate Managementに移動します。

ステップ 3：Multi-SAN Tomcat CA証明書チェーンをCallManager信頼ストアにアップロードします。



ヒント: Tomcat用の自己署名マルチサーバSAN証明書を使用する場合は、このステップを省略できます。

---

証明書を再使用する前に、( tomcat ID証明書に署名した ) CA証明書チェーンをCallManager信頼ストアに手動でアップロードしたことを確認します。

CallManager信頼にtomcat証明書チェーンをアップロードするときに、これらのサービスを再起動します。

- CallManager: Cisco HAProxyサービス
- CallManager-ECDSA: Cisco CallManagerサービスおよびCisco HAProxyサービス

ステップ 4 : Reuse Certificateをクリックします。「Use Tomcat Certificates For Other Services」ページが表示されます。

## Use Tomcat Certificate For Other Services



Finish



Close

### Status



Tomcat-ECDSA Certificate is Not Multi-Server Certificate



Tomcat Certificate is Multi-Server Certificate

### Source

Choose Tomcat Type\*

tomcat



### Replace Certificate for the following purpose



CallManager



CallManager-ECDSA

Finish

Close

ステップ 5 : Tomcat type ドロップダウンリストから、Tomcat または Tomcat-ECDSA を選択します。

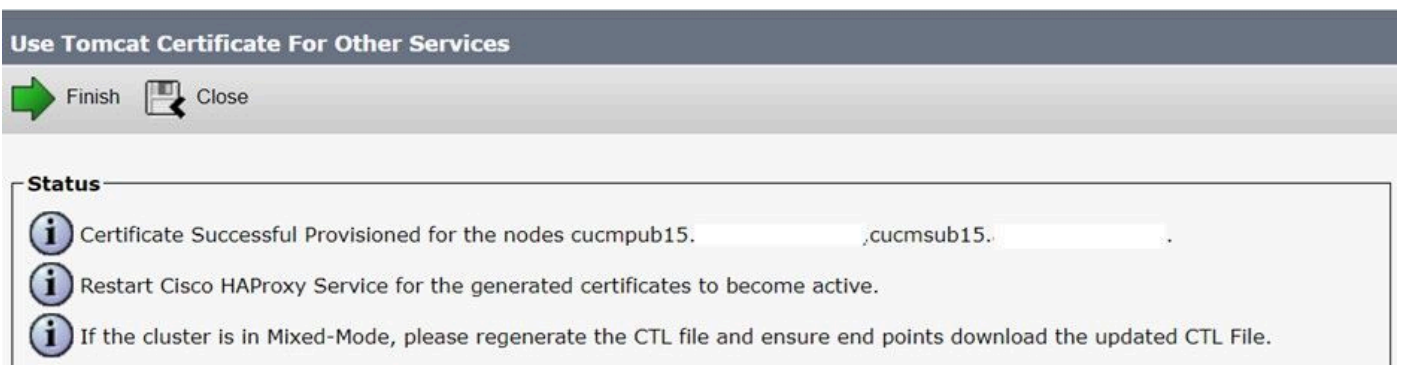
手順 6 : Replace Certificate for the following purpose ペインで、前のステップで選択した証明書に基づいて CallManager または CallManager-ECDSA チェックボックスのいずれかにチェックマークを付けます。

---

注：証明書タイプとしてTomcatを選択した場合、CallManagerが置き換え用に有効になります。証明書タイプとしてtomcat-ECDSAを選択した場合、CallManager-ECDSAが置き換え用として有効になります。

---

手順 7 : Finishをクリックして、CallManager証明書をtomcatマルチサーバSAN証明書で置き換えます。



**Use Tomcat Certificate For Other Services**

Finish Close

**Status**

- Information Certificate Successful Provisioned for the nodes cucmpub15. .cucmsub15.
- Information Restart Cisco HAProxy Service for the generated certificates to become active.
- Information If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

ステップ 8 : CLIでutils service restart Cisco HAProxyコマンドを実行して、クラスタのすべてのノードでCisco HAProxyサービスを再起動します。

```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin: █
```

ステップ 9 : クラスタが混合モードの場合、CUCMパブリッシャのCLIからutils ctl update CTLFileコマンドを実行してCTLファイルを更新し、電話機のリセットに進んで新しいCTLファイルを取得します。

**確認**

---

注：証明書を再利用する場合、CallManager証明書はGUIに表示されません。

---

CLIからコマンドを実行して、CallManagerがTomcat証明書を再利用することを確認できます。

- show cert list own ( オプション )

```
admin:show cert list own
tomcat/tomcat.pem: Certificate Signed by AKASH-WINSERVLAB-CA
tomcat-ECDSA/tomcat-ECDSA.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system
ITLRecovery/ITLRecovery.pem:
CallManager-ECDSA/CallManager-ECDSA.pem: Self-signed certificate generated by system
CallManager/CallManager.pem: Reusing tomcat certificate for CallManager
TVS/TVS.pem: Self-signed certificate generated by system

admin:█
```



## 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。