CUCM 14でのCallManager用のTomcat証明書再利用の設定

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](#)

- [1. Tomcat証明書をマルチSANとして設定する](#)
  - [自己署名](#)
  - [CA署名付き](#)
- [2. CallManager用のTomcat証明書の再利用](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Unified Communications Manager(CUCM)サーバ上のCallManagerでマルチSAN Tomcat(MST)証明書を再利用する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
- リアルタイム監視ツール(RTMT)
- 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、CUCM 14.0.1.13900-155に基づくものです。

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2つの主なサービスは、TomcatとCallManagerです。以前のバージョンでは、クラスタ全体に対してサービスごとに異なる証明書が必要でした。CUCMバージョン14では、CallManagerサービスでもマルチSAN Tomcat証明書を再利用する新機能が追加されました。この機能を使用する利点は次のとおりです。

- CA署名付き証明書の1つのクラスタに対してパブリック認証局(CA)によって署名された2つの証明書を取得するコストを削減します。
- この機能により、ITLファイルのサイズが小さくなり、オーバーヘッドが削減されます。

Low Impact　Medium Impact.　High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat	Low	-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec	Low	-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF	Medium	CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager	Medium	CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS	Medium	ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery	High	CTL + ITL	Signer or SAST backup for ITL/CTL	All	

設定

⚠ 注意: Tomcat証明書をアップロードする前に、シングルサインオン(SSO)が無効になっていることを確認してください。SSOを有効にする場合は、Tomcat証明書の再生成プロセスが完了したら、SSOを無効にして再度有効にする必要があります。

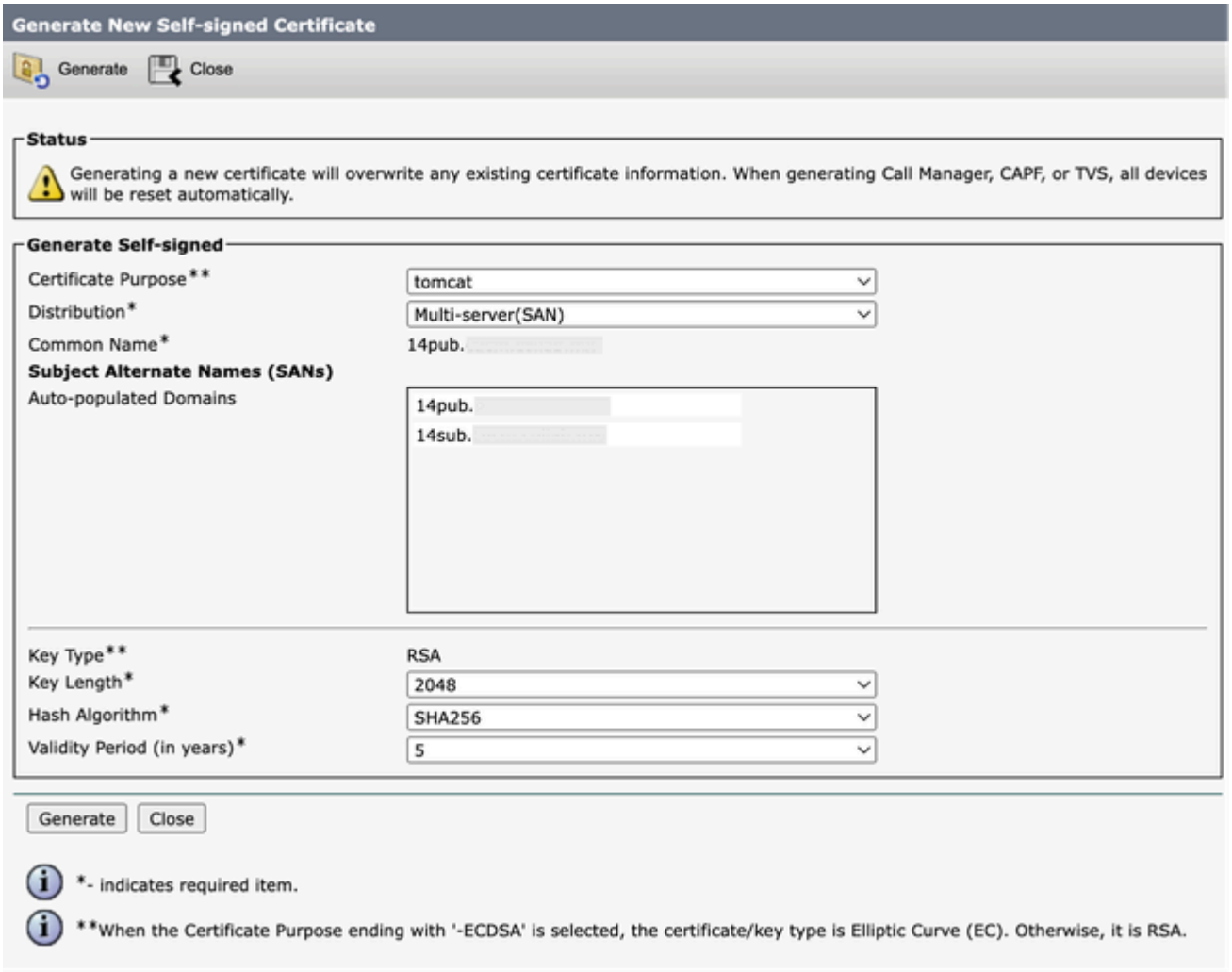
1. Tomcat証明書をマルチSANとして設定する　Low Impact

CUCM 14では、TomcatマルチSAN証明書は自己署名またはCA署名付きにすることができます。Tomcat証明書がすでにマルチSANの場合は、このセクションを省略します。

自己署名

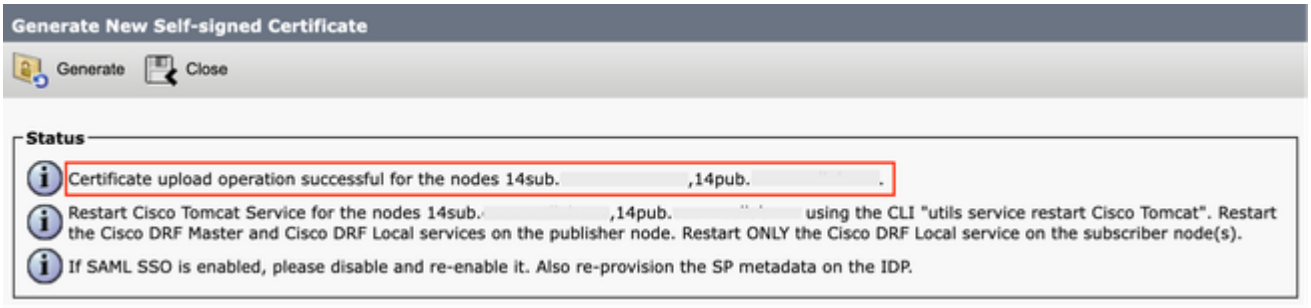
ステップ 1： Publisher > Operating System (OS) Administrationにログインし、 Security > Certificate Management > Generate Self-Signedの順に選択します。

ステップ 2：Certificate Purpose: tomcat > Distribution: Multi-Server SANの順に選択します。 SANドメインと親ドメインに自動入力される



自己署名マルチSAN Tomcat証明書の生成画面

ステップ 3：Generateをクリックして、Certificate upload operation successfulメッセージの下にすべてのノードが表示されていることを確認します。[Close] をクリックします。



自己署名マルチSAN Tomcat生成の成功メッセージ

ステップ 4：tomcatサービスを再起動し、クラスタのすべてのノードに対してCLIセッションを開き、utils service restart Cisco Tomcatコマンドを実行します。

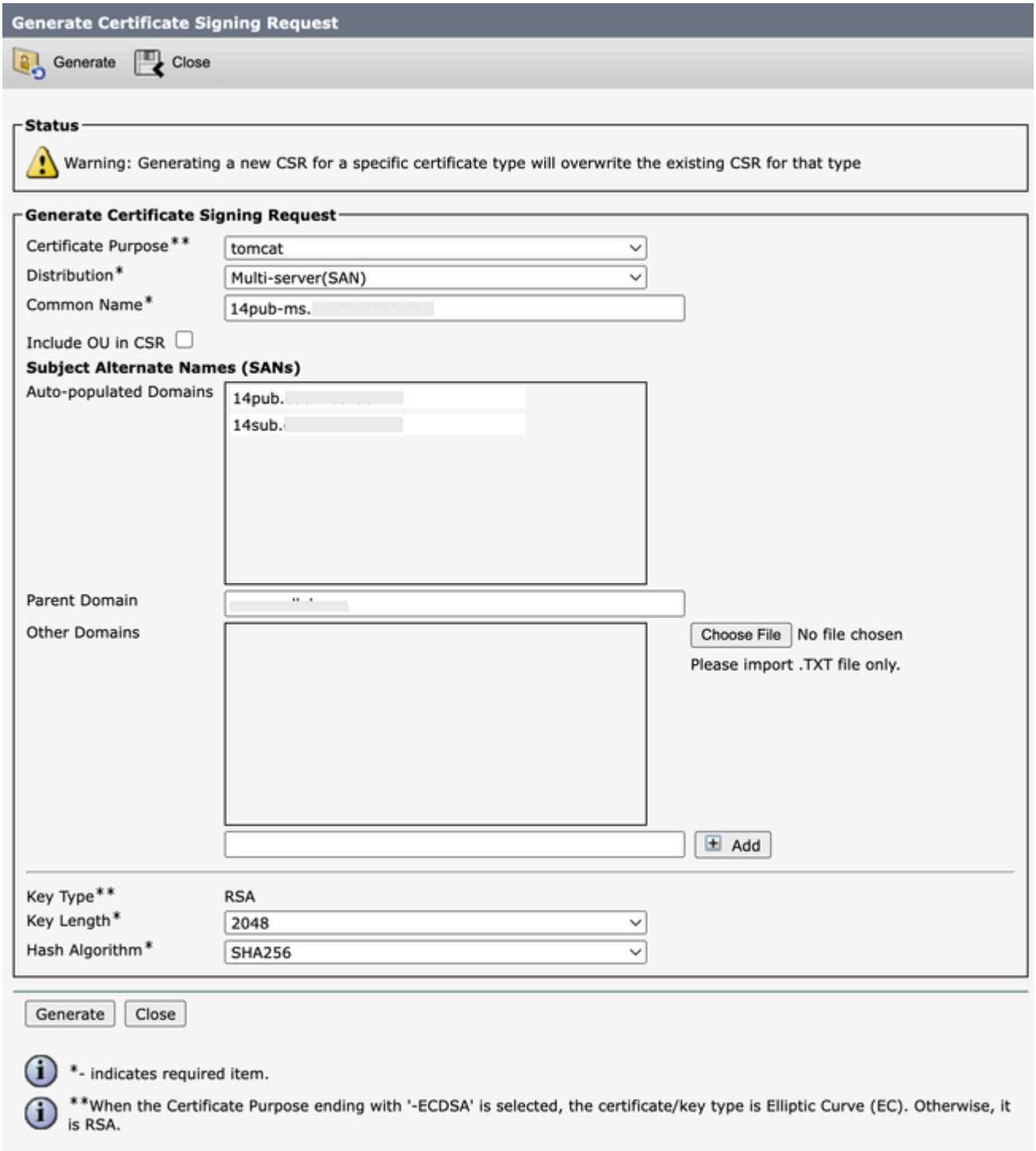
ステップ 5： Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Servicesの順に選択し、Cisco DRF Master ServiceとCisco DRF Local Serviceを再始動します。

手順 6：各Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Servicesに移動し、Cisco DRF Local Serviceを再起動します。

CA署名付き

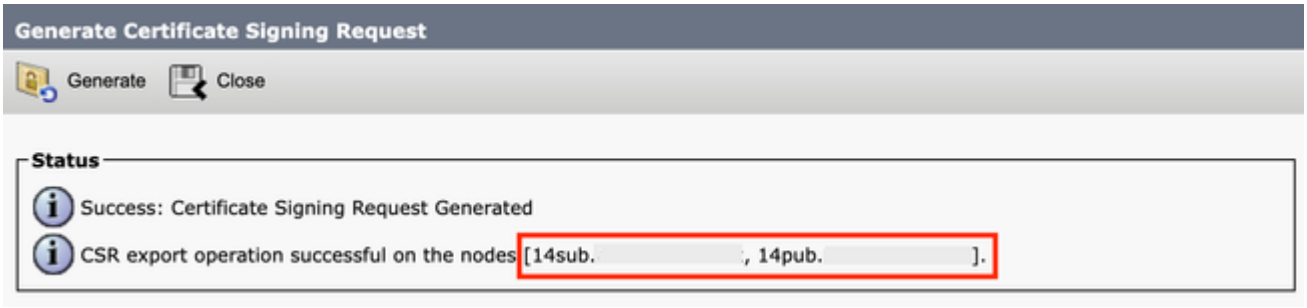
ステップ 1： Publisher > Operating System (OS) Administrationにログインし、Security > Certificate Management > Generate CSRの順に選択します。

ステップ 2：Certificate Purpose: tomcat > Distribution: Multi-Server SANの順に選択します。 SANドメインと親ドメインに自動入力される



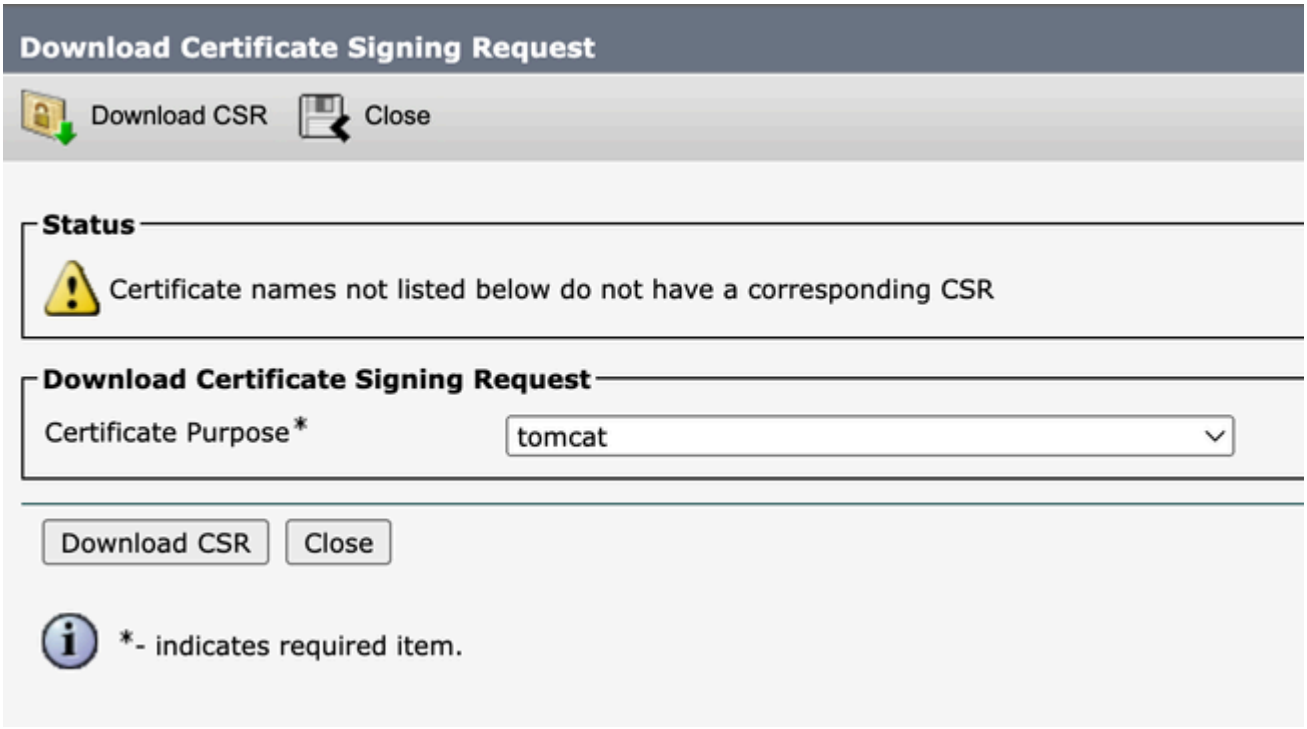
Tomcat証明書用マルチSAN CSRの生成画面

ステップ 3：Generateをクリックして、すべてのノードがCSR export operation successfulメッセージの下に表示されていることを確認します。[Close] をクリックします。



マルチSAN CSR Tomcatの生成成功メッセージ

ステップ 4：Download CSR > Certificate Purpose: tomcat > Downloadの順にクリックします。



Tomcat CSRのダウンロード画面

ステップ 5：署名のためにCSRをCAに送信します。

手順 6：CA信頼チェーンをアップロードするには、Certificate Management > Upload certificate > Certificate Purpose: tomcat-trustの順に移動します。 証明書の説明を設定し、トラストチェーンファイルを参照します。

手順 7：CA署名付き証明書をアップロードし、Certificate Management > Upload certificate > Certificate Purpose: tomcatの順に移動します。証明書の説明を設定し、CA署名付き証明書ファイルを参照します。

ステップ 8：tomcatサービスを再起動し、クラスタのすべてのノードに対してCLIセッションを開き、utils service restart Cisco Tomcatコマンドを実行します。

ステップ 9： Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Servicesの順に選択し、Cisco DRF Master ServiceとCisco DRF Local Serviceを再始動します。

ステップ 10：各Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Servicesに移動し、Cisco DRF Local Serviceを再起動します。

2. CallManager用のTomcat証明書の再利用 Medium Impact.

⚠ 注意:CUCM 14では、新しいエンタープライズパラメータPhone Interaction on Certificate Updateが導入されました。このフィールドは、TVS、CAPF、またはTFTP(CallManager/ITLRecovery)証明書のいずれかが更新されたときに、必要に応じて手動または自動で電話をリセットするために使用します。このパラメータは、デフォルトで電話機を自動的にリセットするように設定されています。証明書を再生成、削除、および更新した後、適切なサービスが再起動されていることを確認します。

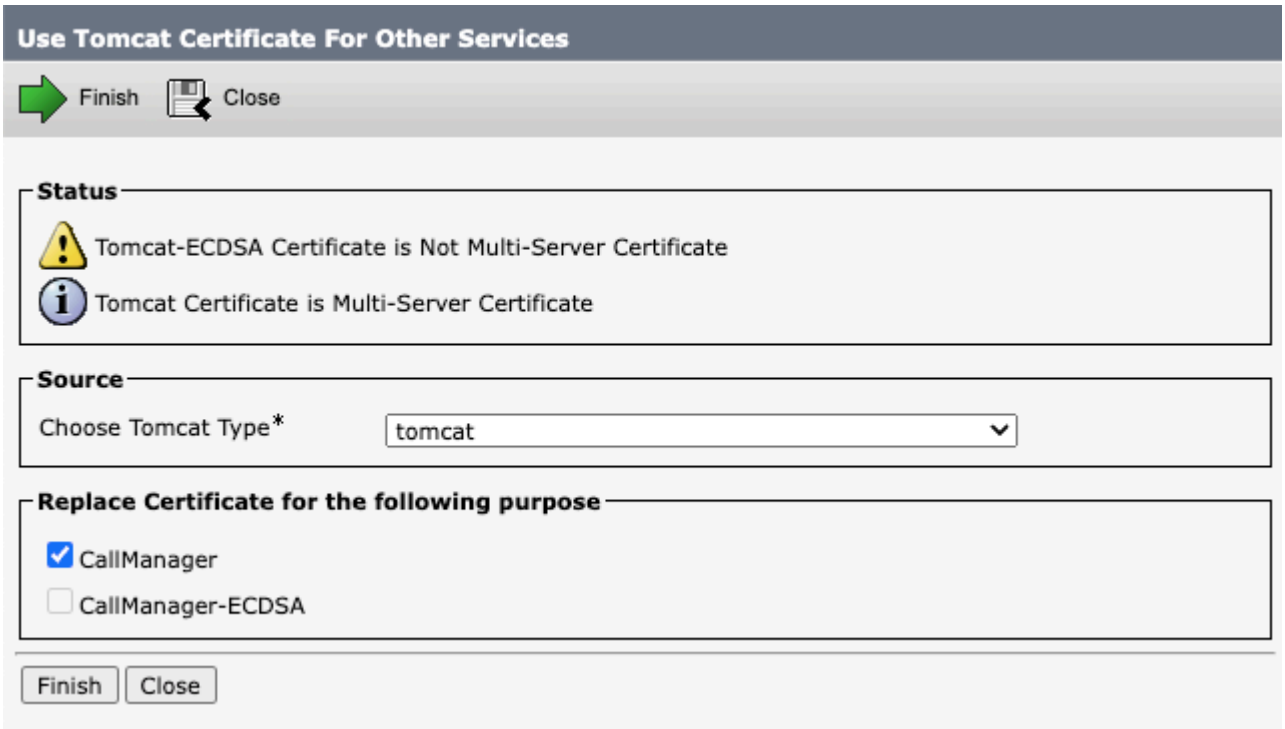
通常のCallManager証明書の再生成のためにサービスを再起動する必要があります。Regenerate Certificates In Unified Communications Managerチェックボックスをオンにします。

ステップ 1：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 2：Reuse Certificateをクリックします。

ステップ 3：**choose Tomcat type**ドロップダウンリストから、tomcatを選択します。

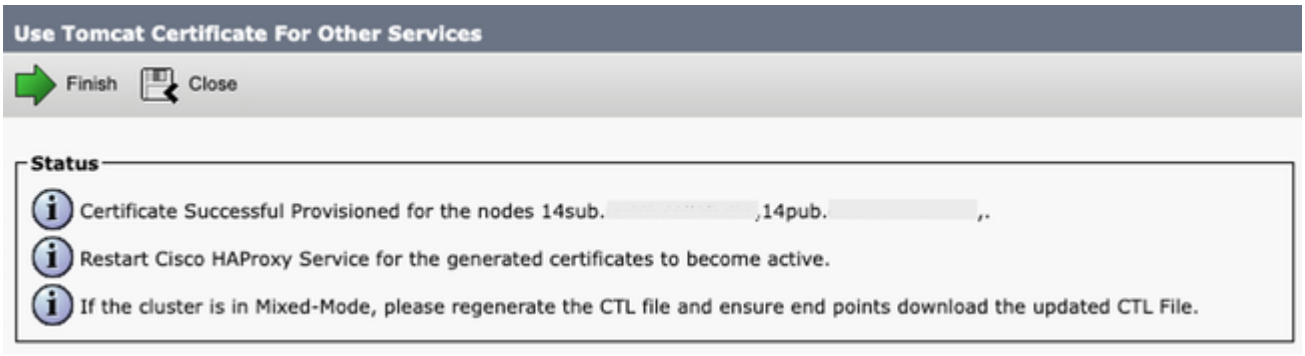
ステップ 4：Replace Certificate for the following purposeペインで、CallManagerチェックボックスにチェックマークを付けます。



Reuse Tomcat Certificate for Other Services画面

注：証明書タイプとしてTomcatを選択した場合は、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。

ステップ 5：CallManager証明書をTomcatマルチSAN証明書で置き換えるには、Finishをクリックします。



Tomcat証明書の再使用成功メッセージ

手順 6： Cisco HAProxyサービスを再起動し、クラスタのすべてのノードへのCLIセッションを開き、utils service restart Cisco HAProxyコマンドを実行します。

注：クラスタが混合モードであるかどうかを判断するには、Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode(0 == Non-Secure; 1 == Mixed Mode)に移動します。

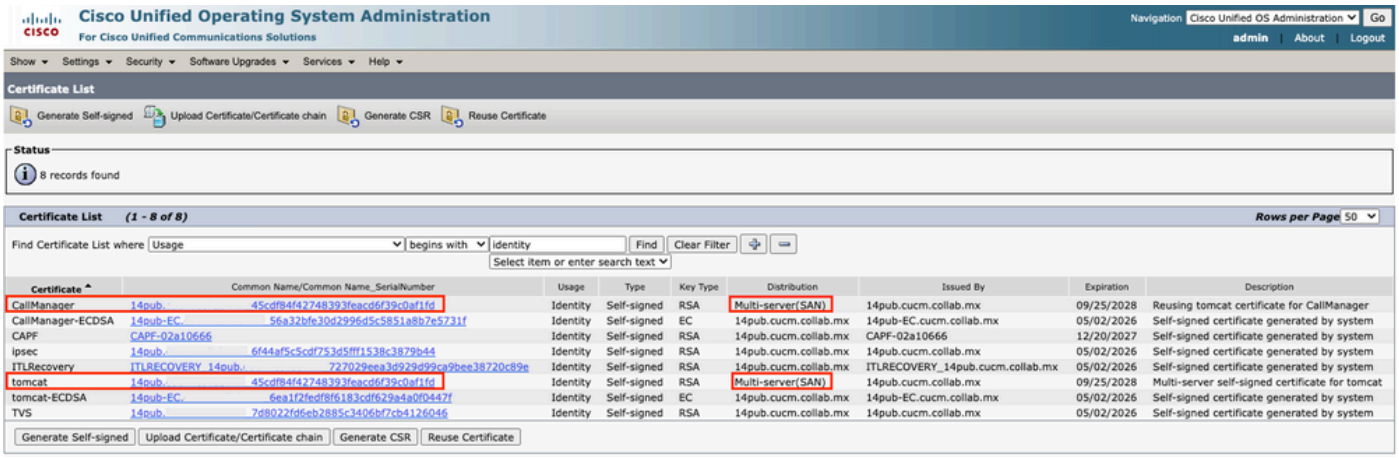
手順 7：クラスタが混合モードの場合、パブリッシャノードへのCLIセッションを開き、**utils ctl update CTLFile**コマンドを実行して、クラスタのすべての電話機をリセットし、CTLファイルの更新を有効にします。

確認

ステップ 1：CUCMパブリッシャに移動してから、Cisco Unified OS Administration > Security > Certificate Managementに移動します。

ステップ 2：Find Certificate List where: Usage > begins with: identityでフィルタリングし、Findをクリックします。

ステップ 3：CallManager証明書とTomcat証明書は同じCommon Name_Serial Number値で終わる必要があります。



CallManagerでのTomcat証明書の再利用の確認

注:SU4以降では、証明書の再利用が有効になっている場合、Call Manager証明書はGUIに表示されませんが、両方の証明書はSU2とSU3で表示されます。

関連情報

- Cisco Unified Communications Managerセキュリティガイド14
- シスコのテクニカルサポートとダウンロード

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。