

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		-	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	

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。



Low Impact

1. Tomcat証明書をマルチSANとして設定する

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

Generate New Self-signed Certificate

Generate Close

Status

Generating a new certificate will overwrite any existing certificate information. When generating Call Manager, CAPF, or TVS, all devices will be reset automatically.

Generate Self-signed

Certificate Purpose** tomcat

Distribution* Multi-server(SAN)

Common Name* 14pub.

Subject Alternate Names (SANs)

Auto-populated Domains 14pub.
14sub.

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Validity Period (in years)* 5

Generate Close

(i) *- indicates required item.

(i) **When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

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。

Generate New Self-signed Certificate

Generate Close

Status

(i) Certificate upload operation successful for the nodes 14sub., 14pub.

(i) Restart Cisco Tomcat Service for the nodes 14sub., 14pub. using the CLI "utils service restart Cisco Tomcat". Restart the Cisco DRF Master and Cisco DRF Local services on the publisher node. Restart ONLY the Cisco DRF Local service on the subscriber node(s).

(i) If SAML SSO is enabled, please disable and re-enable it. Also re-provision the SP metadata on the IDP.

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

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose**

Distribution*

Common Name*

Include OU in CSR

Subject Alternate Names (SANs)

Auto-populated Domains

Parent Domain

Other Domains
Please import .TXT file only.

Key Type** RSA
Key Length* 2048
Hash Algorithm* SHA256

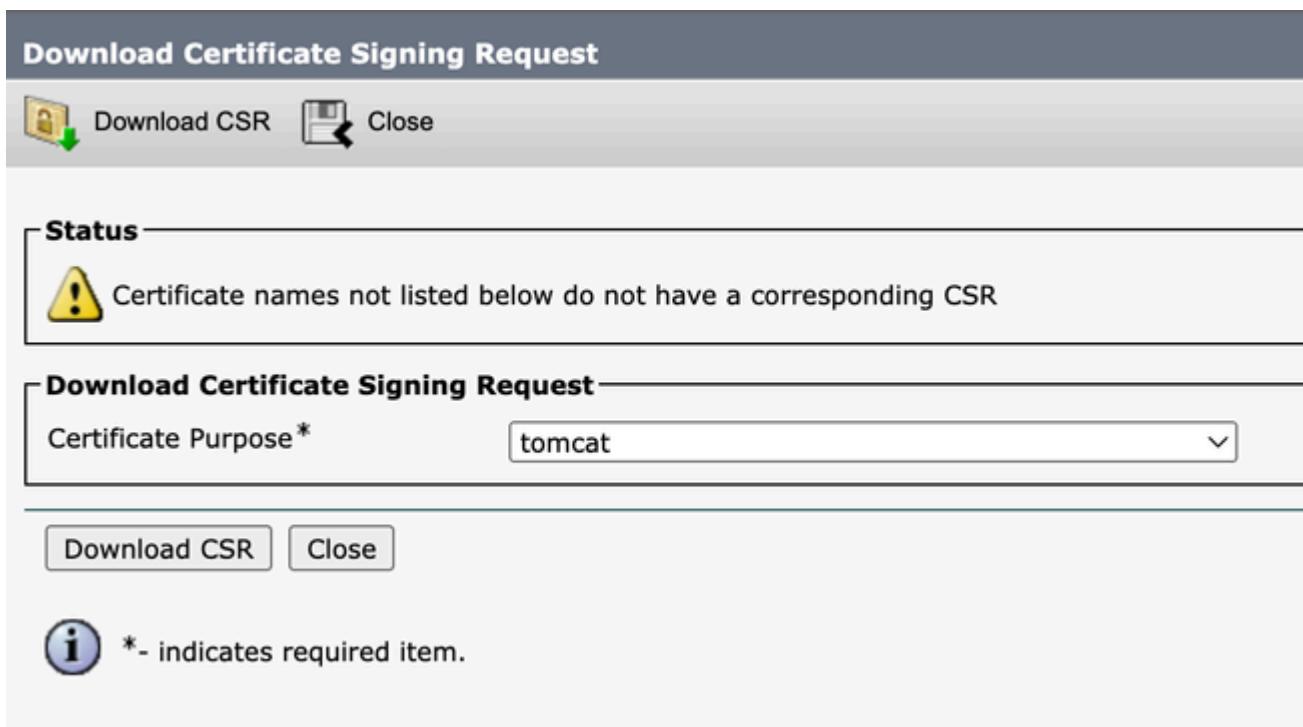
*- indicates required item.
 **When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

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。

Medium Impact.

2. CallManager用のTomcat証明書の再利用



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。

Use Tomcat Certificate For Other Services

Finish Close

Status

! Tomcat-ECDsa Certificate is Not Multi-Server Certificate
i Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type* tomcat

Replace Certificate for the following purpose

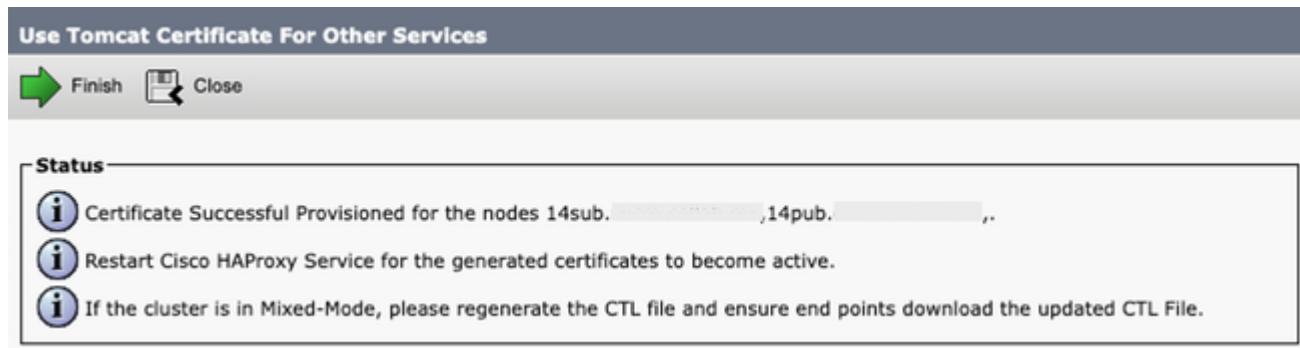
CallManager
 CallManager-ECDsa

Finish Close



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。

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR Reuse Certificate

Status

(i) 8 records found

Certificate List (1 - 8 of 8)									Rows per Page	50 ▾
Find Certificate List where Usage begins with		identity	Find	Clear Filter	▼	Select item or enter search text	▼			
Certificate ^	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description		
CallManager	14pub...45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Reusing tomcat certificate for CallManager		
CallManager-ECDSA	14pub-EC...56a32bfe30d2996d5c5851a8b7e5731f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system		
CAPF	CAPF-02a10666	Identity	Self-signed	RSA	14pub.cucm.collab.mx	CAPF-02a10666	12/20/2027	Self-signed certificate generated by system		
ipsec	14pub...6f44af5c5cd753d5fff1538c3879b44	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system		
ITLRecovery	ITLRECOVERY_14pub...727029eeaa3d929d999ca9bee38720c89e	Identity	Self-signed	RSA	ITLRECOVERY_14pub.cucm.collab.mx	ITLRECOVERY_14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system		
tomcat	14pub...45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Multi-server self-signed certificate for tomcat		
tomcat-ECDSA	14pub-EC...6ea1f2fedf8f6183cd6f2994a00447f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system		
TVS	14pub...768022f6eb2885c34068b7cb4126046	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system		

Generate Self-signed Upload Certificate/Certificate chain Generate CSR Reuse Certificate

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。