署名付きCA証明書からの新しい証明書の作成

内容
<u>はじめに</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
事前チェック情報
<u>証明書の設定と再生成</u>
Tomcat証明書
<u>CallManager証明書</u>
<u>IPSec証明書</u>
<u>CAPF証明書</u>
<u>TVS証明書</u>
<u>アップロードされる証明書の一般的なエラーメッセージのトラブルシューティング</u>
<u>CA証明書が信頼ストアで使用できない</u>
<u>ファイル/usr/local/platform/.security/tomcat/keys/tomcat.csrが存在しません</u>
<u>CSR公開キーと証明書の公開キーが一致しない</u>
<u>CSRサブジェクトの別名(SAN)と証明書SANが一致しない</u>
<u>同じCNの信頼証明書は置き換えられません</u>

はじめに

このドキュメントでは、Cisco Unified Communications Manager(CUCM)で認証局(CA)によって署 名された証明書を再生成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。

- ・ リアルタイム監視ツール(RTMT)
- CUCM証明書

使用するコンポーネント

• CUCMリリース10.x、11.x、および12.x。

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

事前チェック情報

◇ 注:自己署名証明書の再生成については、『<u>証明書の再生成ガイド</u>』を参照してください。 CA署名付きマルチSAN証明書の再生成については、『<u>マルチSAN証明書の再生成ガイド</u>』 を参照してください。

各証明書とその再生成の影響を理解するには、『<u>自己署名再生成ガイド</u>』を参照してください。

証明書署名要求(CSR)タイプごとにキー使用法が異なり、署名付き証明書に必要なキー使用法も 異なります。『<u>セキュリティガイド</u>』には、証明書のタイプごとに必要なキーの使用法が記載さ れたテーブルがあります。

サブジェクトの設定(地域、州、組織単位など)を変更するには、次のコマンドを実行します。

• set web-security orgunit orgname locality state [country] [alternatehostname]

set web-securityコマンドを実行すると、Tomcat証明書が自動的に再生成されます。Tomcatサービスが 再起動されるまで、新しい自己署名証明書は適用されません。このコマンドの詳細については、 次のガイドを参照してください。

- <u>コマンドラインリファレンスガイド</u>
- シスココミュニティの手順へのリンク
- ・ <u>ビデオ</u>

証明書の設定と再生成

CAによって署名されたCUCMクラスタでシングルノード証明書を再生成する手順は、証明書のタ イプごとに示されています。クラスタ内のすべての証明書の有効期限が切れていない場合は、証 明書を再生成する必要はありません。

Tomcat証明書

▲ 注意:クラスタでSSOが無効になっていることを確認します(CM Administration > System > SAML Single Sign-On)。SSOを有効にする場合は、SSOを無効にして、Tomcat証明書の再生成プロセ スが完了したら有効にする必要があります。

クラスタのすべてのノード(CallManagerおよびIM&P)で、次の操作を行います。

ステップ1:「Cisco Unified OS Administration > Security > Certificate Management > Find」に移動し、Tomcat証明書の有効期限を確認します。

ステップ2:をクリックします。Generate CSR > Certificate Purpose: tomcat証明書に必要な設定を選択し、 Generateをクリックします。成功のメッセージが表示されるまで待ち、Closeをクリックします。

Generate Certificate Signing	Request	
💽 Generate 📑 Close		
Status	Request Generated	
Generate Certificate Signing	Request	
Certificate Purpose**	tomcat	v
Distribution *	115pub	v
Common Name*	115pub	
Subject Alternate Names (SA Parent Domain	Ns)	
Key Type**	RSA	
Key Length*	2048	v
Hash Algorithm*	SHA256	~
Generate Close i *- indicates required item. i **When the Certificate Put	rpose ending with '-ECDSA' is :	elected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

ステップ3: CSRをダウンロードします。Download CSRをクリックし、を選択して Certificate Purpose: tomcat,、をクリックしDownloadます。

Download Certificate Signing Request	
Download CSR Close	
Status	
Certificate names not listed below do not have a	a corresponding CSR
Download Certificate Signing Request	
Certificate Purpose	tomcat v
Download CSR Close	
 indicates required item. 	

ステップ4:認証局にCSRを送信します。

ステップ 5:認証局は、署名付き証明書チェーン用に2つ以上のファイルを返します。証明書を次の順序でアップロードします。

- tomcat-trustとしてのルートCA証明書。[証明書の説明を設Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. 定]に移動し、ルート証明書ファイルを参照します。
- tomcat-trustとしての中間証明書(オプション)。Certificate Management > Upload certificate > Certificate

Purpose: tomcat-trustに移動します。証明書の説明を設定し、中間証明書ファイルを参照します。

- ✤ 注:一部のCAは中間証明書を提供しません。ルート証明書だけを指定した場合は、この手順を省略できます。
 - tomcatとしてのCA署名付き証明書Certificate Management > Upload certificate > Certificate Purpose: tomcatに移動 します。 証明書の説明を設定し、現在のCUCMノードのCA署名付き証明書ファイルを参照 します。
- ◆ 注:この時点で、CUCMはCSRとアップロードされたCA署名付き証明書を比較します。情報が一致すると、CSRが消去され、新しいCA署名付き証明書がアップロードされます。証明書のアップロード後にエラーメッセージが表示された場合は Upload Certificate Common Error Messages、の項を参照してください。

手順 6:新しい証明書をサーバに適用するには、CLIを使用してCisco Tomcatサービスを再起動す る必要があります(パブリッシャで開始し、サブスクライバを1つずつ再開する)。次のコマンド を使用します utils service restart Cisco Tomcat.

Tomcat証明書がCUCMで使用されていることを確認するには、ノードのWebページに移動し、ブ ラウザで Site Information (ロックアイコン)を選択します。オプションをクリックし certificateて、新 しい証明書の日付を確認します。

# Cisco Unified	I CM Console × +	
$\ \ \leftarrow \ \ \rightarrow \ \ G$	115pub //ccmadmin/showHome.	do
cisco For	X Connection is secure Your information (for example, passwords or credit	
Cisco U	card numbers) is private when it is sent to this site. Learn more	
	Certificate (Valid)	
	Cookies (1 in use)	
Copyright © 1999	Site settings	

 and the second	100 C 100 C 100 C	

19	Certificat	e Information	
Thes.	Ensures the	a intended for the follow a identity of a remote com	ving purpose(s): cuter
_			
	Issued to:	115put	
	Termed her		
	199060 04:		
ſ	Valid from	9/16/2020 to 9/16/2022	2
			Issuer Statement

CallManager証明書



×

⚠️ ス全体を終了し、電話機が再登録されたら、TVSのプロセスを開始します。

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

クラスタのすべてのCallManagerノードに対して、次の手順を実行します。

ステップ1:に移動 Cisco Unified OS Administration > Security > Certificate Management > Find し、CallManager証明書 の有効期限を確認します。

ステップ2:をクリックします。Generate CSR > Certificate Purpose: CallManager証明書に必要な設定を選択し 、Generateをクリックします。成功のメッセージが表示されるまで待ち、Closeをクリックします。

ステップ3: CSRをダウンロードします。をクリックします。Download CSR. Select Certificate Purpose: CallManager and click Download

ステップ4: CSRをCertificate Authorityに送信します。

ステップ5:認証局は、署名付き証明書チェーン用に2つ以上のファイルを返します。証明書を次 の順序でアップロードします。

- CallManager-trustとしてのルートCA証明書。Certificate Management > Upload certificate > Certificate Purpose: CallManager-trustに移動します。証明書の説明を設定し、ルート証明書ファイルを参 照します。
- CallManager-trustとしての中間証明書(オプション)。Certificate Management > Upload certificate > Certificate Purpose: CallManager-trustに移動します。証明書の説明を設定し、中間証明書ファイ ルを参照します。

💊 注:一部のCAは中間証明書を提供しません。ルート証明書だけを指定した場合は、この手 順を省略できます。

・ CallManagerとしてのCA署名付き証明書Certificate Management > Upload certificate > Certificate Purpose: CallManagerに移動します。証明書の説明を設定し、現在のCUCMノードのCA署名付き証明書 ファイルを参照します。

💊 注:この時点で、CUCMはCSRとアップロードされたCA署名付き証明書を比較します。情 報が一致すると、CSRが消去され、新しいCA署名付き証明書がアップロードされます。証 明書のアップロード後にエラーメッセージを受信する場合は、「証明書のアップロードの一 般的なエラーメッセージ」セクションを参照してください。

手順6:クラスタが混合モードの場合、サービスを再起動する前にCTLを更新します(トークンま たはトークンレス)。クラスタが非セキュアモードの場合は、この手順を省略してサービスの再起 動に進みます。

手順7:新しい証明書をサーバーに適用するには、必要なサービスを再起動する必要があります

(サービスが実行され、アクティブな場合のみ)。次のとおりに移動します。

- Cisco Unified Serviceability > Tools > Control Center Network Services > Cisco Trust Verification Service
- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco CTIManager

ステップ8:すべての電話機をリセットします。

 Cisco Unified CM Administration > System > Enterprise Parameters > Resetに移動します。ポップアッ プウィンドウに、「You are about to reset all devices in the system」というステ ートメントが表示されます。この操作は元に戻せません。続行しますか?[OK]を選択し、[Reset]をクリックします。

✤ 注:RTMTを使用してデバイス登録をモニタします。すべての電話機を登録し直したら、次の 証明書タイプに進むことができます。

IPSec証明書

⚠ 注意: IPSec証明書が再生成される際は、バックアップタスクまたは復元タスクをアクティ ブにしないでください。

クラスタのすべてのノード(CallManagerおよびIM&P)について、次の手順を実行します。

ステップ1: Cisco Unified OS Administration > Security > Certificate Management > Findに移動し、ipsec証明書の有効 期限を確認します。

ステップ 2: Generate CSR > Certificate Purpose: ipsecの順にクリックします。証明書に必要な 設定を選択し、Generateをクリックします。成功のメッセージが表示されるまで待ってから、 Closeをクリックします。

ステップ 3: CSRをダウンロードします。[Download CSR] をクリックします。Certificate Purpose ipsecを選択して、Downloadをクリックします。

ステップ4:認証局にCSRを送信します。

ステップ 5:認証局は、署名付き証明書チェーン用に2つ以上のファイルを返します。証明書を次の順序でアップロードします。

- ipsec-trustとしてのルートCA証明書。Certificate Management > Upload certificate > Certificate Purpose: ipsec-trustの順に移動します。証明書の説明を設定し、ルート証明書フ アイルを参照します。
- ipsec-trustとしての中間証明書(オプション)。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、中間証明書 ファイルを参照します。

✤ 注:一部のCAは中間証明書を提供しません。ルート証明書だけを指定した場合は、この手順を省略できます。

- ipsecとしてのCA署名付き証明書。Certificate Management > Upload certificate > Certificate Purpose: ipsecの順に移動します。証明書の説明を設定し、現在のCUCMノ ードのCA署名付き証明書ファイルを参照します。
- ◇ 注:この時点で、CUCMはCSRとアップロードされたCA署名付き証明書を比較します。情報が一致すると、CSRが消去され、新しいCA署名付き証明書がアップロードされます。証明書のアップロード後にエラーメッセージを受信する場合は、「証明書のアップロードの一般的なエラーメッセージ

手順 6:新しい証明書をサーバーに適用するには、必要なサービスを再起動する必要があります (サービスが実行され、アクティブな場合のみ)。次のとおりに移動します。

- Cisco Unified Serviceability > Tools > Control Center Network Services > Cisco DRF Master (パブリッシャ)
- Cisco Unified Serviceability > Tools > Control Center Network Services > Cisco DRF Local (パブリッシャおよびサブスクライバ)

CAPF証明書

- № 注:クラスタが混合モードであるかどうかを確認するには、Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode(0 == Non-Secure; 1 == Mixed Mode)に移動します。
- 注:CAPFサービスはパブリッシャでのみ実行され、これが使用される唯一の証明書です。サ ブスクライバノードは使用されないため、CAによって署名されたサブスクライバノードを 取得する必要はありません。サブスクライバで証明書が期限切れになり、期限切れの証明書 のアラートを回避したい場合は、サブスクライバCAPF証明書を自己署名として再生成でき ます。詳細については、「自己署名としてのCAPF証明書」を参照してください。

パブリッシャ :

ステップ1: Cisco Unified OS Administration > Security > Certificate Management > Findに移動 し、CAPF証明書の有効期限を確認します。

ステップ 2: Generate CSR > Certificate Purpose: CAPFの順にクリックします。証明書に必要な 設定を選択し、Generateをクリックします。成功のメッセージが表示されるまで待ってから、 Closeをクリックします。

ステップ 3:CSRをダウンロードします。[Download CSR] をクリックします。Certificate Purpose CAPFを選択して、Downloadをクリックします。 ステップ4:認証局にCSRを送信します。

ステップ5:認証局は、署名付き証明書チェーン用に2つ以上のファイルを返します。証明書を 次の順序でアップロードします。

- CAPF-trustとしてのルートCA証明書。Certificate Management > Upload certificate > Certificate Purpose: CAPF-trustの順に移動します。証明書の説明を設定し、ルート証明書ファイルを参照します。
- CAPF-trustとしての中間証明書(オプション)。Certificate Management > Upload certificate > Certificate Purpose: CAPF-trustの順に移動します。証明書の説明を設定し 、中間証明書ファイルを参照します。
- ✤ 注:一部のCAは中間証明書を提供しません。ルート証明書だけを指定した場合は、この手順を省略できます。
 - CAPFとしてのCA署名付き証明書。Certificate Management > Upload certificate > Certificate Purpose: CAPFの順に移動します。証明書の説明を設定し、現在のCUCMノードのCA署名付き証明書ファイルを参照します。

◆ 注:この時点で、CUCMはCSRとアップロードされたCA署名付き証明書を比較します。情報が一致すると、CSRが消去され、新しいCA署名付き証明書がアップロードされます。証明書のアップロード後にエラーメッセージを受信する場合は、「証明書のアップロードの一般的なエラーメッセージ」セクションを参照してください。

手順6:クラスタが混合モードの場合、サービスを再起動する前にCTLを更新します(<u>トークン</u>ま たは<u>トークンレス</u>)。クラスタが非セキュアモードの場合は、この手順を省略してサービスの再起 動に進みます。

手順 7:新しい証明書をサーバーに適用するには、必要なサービスを再起動する必要があります (サービスが実行され、アクティブな場合のみ)。次のとおりに移動します。

- Cisco Unified Serviceability > Tools > Control Center Network Services > Cisco Trust Verification Service (サービスが稼働するすべてのノード)
- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco TFTP(サ ービスが稼働するすべてのノード)
- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco Certificate Authority Proxy Function (パブリッシャ)

ステップ8: すべての電話機をリセットします。

 Cisco Unified CM Administration > System > Enterprise Parameters > Resetの順に移動しま す。ポップアップウィンドウに、「You are about to reset all devices in the system」という ステートメントが表示されます。この操作は元に戻せません。続行しますか?OKを選択し 、Resetをクリックします。 ✤ 注:RTMTを使用してデバイス登録をモニタします。すべての電話機を登録し直したら、次の 証明書タイプに進むことができます。

TVS証明書

// 注意:CallManager証明書とTVS証明書を同時に再生成しないでください。これにより、エンドポイントにインストールされているITLと回復不能なミスマッチが引き起こされ、クラスタ内のすべてのエンドポイントからITLを削除する必要があります。CallManagerのプロセス全体を終了し、電話機が再登録されたら、TVSのプロセスを開始します。

クラスタのすべてのTVSノードに対して、次の手順を実行します。

ステップ1: Cisco Unified OS Administration > Security > Certificate Management > Findに移動 し、TVS証明書の有効期限を確認します。

ステップ 2: Generate CSR > Certificate Purpose: TVSの順にクリックします。証明書に必要な設 定を選択し、Generateをクリックします。成功のメッセージが表示されるまで待ってから、 Closeをクリックします。

ステップ 3:CSRをダウンロードします。[Download CSR] をクリックします。Certificate Purpose TVSを選択し、Downloadをクリックします。

ステップ4:認証局にCSRを送信します。

ステップ 5:認証局は、署名付き証明書チェーン用に2つ以上のファイルを返します。証明書を次の順序でアップロードします。

- TVS-trustとしてのルートCA証明書。Certificate Management > Upload certificate > Certificate Purpose: TVS-trustの順に移動します。証明書の説明を設定し、ルート証明書フ ァイルを参照します。
- TVS-trustとしての中間証明書(オプション)。Certificate Management > Upload certificate
 > Certificate Purpose: TVS-trustの順に移動します。証明書の説明を設定し、中間証明書フ アイルを参照します。
- № 注:一部のCAは中間証明書を提供しません。ルート証明書だけを指定した場合は、この手順を省略できます。
 - TVSとしてのCA署名付き証明書Certificate Management > Upload certificate > Certificate
 Purpose: TVSの順に移動します。証明書の説明を設定し、現在のCUCMノードのCA署名付
 き証明書ファイルを参照します。
- ◇ 注:この時点で、CUCMはCSRとアップロードされたCA署名付き証明書を比較します。情報が一致すると、CSRが消去され、新しいCA署名付き証明書がアップロードされます。証明書のアップロード後にエラーメッセージを受信する場合は、「証明書のアップロードの一般的なエラーメッセージ」セクションを参照してください。

手順 6:新しい証明書をサーバーに適用するには、必要なサービスを再起動する必要があります (サービスが実行され、アクティブな場合のみ)。次のとおりに移動します。

- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco TFTP(サ ービスが稼働するすべてのノード)
- Cisco Unified Serviceability > Tools > Control Center Network Services > Cisco Trust Verification Service (サービスが稼働するすべてのノード)

手順7:すべての電話機をリセットします。

- Cisco Unified CM Administration > System > Enterprise Parameters > Resetの順に移動しま す。ポップアップウィンドウに、「You are about to reset all devices in the system」という ステートメントが表示されます。この操作は元に戻せません。続行しますか?OKを選択し 、Resetをクリックします。
- ◆ 注:RTMTを使用してデバイス登録をモニタします。すべての電話機を登録し直したら、次の 証明書タイプに進むことができます。

アップロードされる証明書の一般的なエラーメッセージのトラブ ルシューティング

このセクションでは、CA署名付き証明書がアップロードされる際の最も一般的なエラーメッセージの一部を示します。

CA証明書が信頼ストアで使用できない

このエラーは、ルート証明書または中間証明書がCUCMにアップロードされなかったことを意味 します。サービス証明書をアップロードする前に、これら2つの証明書が信頼ストアとしてアップ ロードされていることを確認します。

ファイル/usr/local/platform/.security/tomcat/keys/tomcat.csrが存在しません

このエラーは、証明書(tomcat、callmanager、ipsec、capf、tvs)のCSRが存在しない場合に表示 されます。CSRが以前に作成され、証明書がそのCSRに基づいて作成されたことを確認します。 留意すべき重要なポイント:

- サーバおよび証明書タイプごとに1つのCSRのみ存在できます。つまり、新しいCSRを作成 すると、古いCSRが置き換えられます。
- ワイルドカード証明書はCUCMではサポートされていません。
- 新しいCSRがないと、現在有効なサービス証明書を置き換えることはできません。
- 同じ問題に関する別のエラーとして、「The file /usr/local/platform/upload/certs//tomcat.der could not be uploaded」が考えられます。これは、CUCMのバージョンによって異なりま す。

CSR公開キーと証明書の公開キーが一致しない

このエラーは、CAによって提供された証明書に、CSRファイルで送信されたものとは異なる公開 キーが含まれている場合に表示されます。考えられる理由は次のとおりです。

- 誤った証明書(別のノードからの証明書など)がアップロードされている。
- CA証明書が異なるCSRで生成されました。
- CSRが再生成され、署名付き証明書の取得に使用された古いCSRが置き換えられました。

CSRと証明書の公開キーの一致を確認するには、<u>SSL</u>などの複数のツールをオンラインで使用します。

What to Check

- O Check if a Certificate and a Private Key match
- Check if a CSR and a Certificate match

Enter your Certificate:

TJ13aW4xMxDTJ1DRFAsQG49UHVIbGIJTWS2V5JTWU2VydmIJZXMsQ049U2Vy dmIJZXMsQ049Q29uZmindXjhdGivbixEQ21jb2xsYWIsREM9bXg/Y2VydGimaWNh dGV5ZX2VY2F0aW9uTGl2dD9YXNIP29iamVjdENsYXA2PWNSTERpc3RyaWj1dGiv bIBvaW50MIG78ggrBgEFBQcBAQ58rjCBqzCBqAY1KwY8BQUHMAXGgZxsZGFwOi8v L0NOPUNvbGxhYIUyMENBLENOPUFJQ5xDTJ1QdWjsaWMIMJBLZXkIMJBTZXj2WNI cyxDTJ1TZXj2aWNIcyxDTJ1Db25maWd1cmF0aW9uLERDPWNvbGxhYrxEQ21teD9j QUNIcrRpZmIjYXRIP2jhc2U/b2jqZWN0Q2xhc3M9Y2VydGimaWNhdGivbkF1dGhv cmI0eTAhBgkrBgEEAY13FAIEFB4SAFcA2QBIAFMA2QByAHYAZQByMA0GC5qG5lb3 DQEBCwUAA4IBAQCfqj2Bc2BcMxkurQavdYaUioDrfDpML5A/7rhisqW55x/bEQs 9UyqftmiddCmkoMPtGK4t2vMie4oTpKBYAQvbrApG001mWV5u+f1io9PvTygWEyL D+ve7rMp8sirVo1Tmhe/Z6in3lbm+Ofwe5NuvCx3wN/dLRR39O4KcaPCx5VLQ6Aw PtmvAz/KK2GRhzqacd9fVLJUoWTKDJ2Qsladcgsi5cvFMz3B8f0MJGBNX16JGiQ yZ2br6Gm4pa4yIRQfsUrcX0HYslomecYeRheKuSkuPusOoENWiszJ0QMT7P4/Ww 28pT2TkrQdODAZHJGuJP+yBa750GGT2WVVg1END CERTIFICATE-....

Enter your CSR:

q+hjgokSx+ogqVavFSNRdqTh0Girls1ga0pjSsGxOOLCqAbQhEARnEcGyanZzrK gSjTQhf8jStD2vDYyD3wg5lyhwNiqkMUI3tRD5qcSD/IYfILGLs8hB9ySHqtaDA3 11wLjSQ4RXt2188ESciLt83bAoZegZo5Vw4/h5tP8r09e/cTWsX2t8fLGytvcDGk OGrdW2xLuaUV2u23JWTmLD70tCN/XCMI9XYpLjb6ulyMUI00Fh+s0P1Mr7gaf5b hxkS42joFIMkXY8WSPDwexH7XtD+HQaPeM4rS0N4TrqhxAgM8AAGgbz8t8gkqhkiG 9w08CQ4xYD8eM80GA1UdjQQWM8QGCCsGAQUF8wM88ggr8gEF8QcDAJALBgNVHQ8E BAMCBLAwMAYDVR0R8Ckwj4iOY3Vjb5Sjb2xsYWiubXtCFTExNX81YtSjdWNtLmNv bGxhr15teDAN8gkqhkiG9w08AQsFAAOCAQEAAh8glii76T59rWXOFJsg7hsJ36vf ubcW7HGPtNYx5/p19UydunRtXKDxQT1z2WWc9IOA3/Fpcfr2+8LdHtR1Fnrw8WCV YcA9soNiW2smU1+clbTH1HSg8FFoHAdg+FR3+1AE7GNfGKQCA0RipFlhZPGzQ6dO 62TRsfQ4SLbcWxe4EZOSxjEQW7ZrkjfWby1GQKYg3CuXCEtY3UunMCZrWjmNxKg0 n781nNdx7rbgFz1ieY+202PHWgbu2HwCHuH1bOAMUpkwiPebQ2n9H+R7drsjBA2R ieXEYWL739M78TveNmHoOR85kwvHYbb7iq0jnhXxSy9R0S0S2s2vUhkj7Hw== ----END CERTIFICATE REQUEST----- The certificate and CSR do NOT match!

🕜 Certificate Hash:

684ad486131856ce0015d4b3e615e1ed 3b3bef6b8f590a493921661a4c4f62e9

🕜 CSR Hash:

635f45c1ebcd876526a3133d1ee73d9a8 4544876fdbc8dc3a4d8fed377dcc635 同じ問題に関する別のエラーとして、「The file /usr/local/platform/upload/certs//tomcat.der could not be uploaded」が考えられます。 これは、CUCMのバージョンによって異なります。

CSRサブジェクトの別名(SAN)と証明書SANが一致しない

CSRと証明書の間のSANは同じである必要があります。これにより、許可されていないドメインの認証が防止されます。SANの不一致を確認するには、次の手順を実行します。

1. CSRと証明書を復号化します(ベース64)。<u>デコーダ</u>など、さまざまなデコーダをオンライン で使用できます。

2. SANエントリーを比較し、すべてのエントリーが一致していることを確認します。順序は重要 ではありませんが、CSRのすべてのエントリが証明書と同じである必要があります。

たとえば、CA署名付き証明書には、証明書の共通名と追加のIPアドレスの2つの追加SANエント リがあります。

CSR Summary		Certif	ficate Summary	
Subject	domain.com	Sub	oject	
RDN	Value	RD	N	Value
Common Name (CN)	gub-ms.domain.com	Con	mmon Name (CN)	pub-ms.domain.com
Organizational Unit (OU)	Collaboration	Org	panizational Unit (OU)	Collaboration
Organization (0)	Cisco	Org	panization (0)	Cisco
Locality (L)	CUCM	Loci	cality (L)	CUCM
State (ST)	CDMX	Stat	te (ST)	CDMX
Country (C)	MX	Cou	untry (C)	MX
Properties	domain.com	Prop	perties	
Property	Value	Pro	operty V	Value
Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX	Issu	uer C	CN = Collab CA,DC = collab,DC = mx
Key Size	2048 bits	Sub	bject C	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMRCC = MX
Fingerprint (SHA-1)	C3 87 05 C8 79 F8 88 4A 86 96 77 0A C5 88 63 27 55 3C A4 84	Vali	lid From 1	17 Sep 2020, 1:24 a.m.
Fingerprint (MD5)	CE:5C:90:59:1F-8E:81:26:C5:21:90:A2:F1:CA:68:86	Vali	lid To 1	17 Sep 2022, 1:24 a.m.
SANS	domain.com, sub.domain.com, pub.domain.com, imp.domain.com	Seri	ial Number 6	69.00.00.00.2D 5A.92.ER EA 9A.85.65.C4.00.00.00.00.00.2D (2341578246081205845683969935281333940237893677)
		CA	Cert N	No
		Key	y Size 2	2048 bits
		Fing	gerprint (SHA-1) 4	4E15 #7 #3 9C37 A9 8D 52:1A 6C 6D 4D 70 AF FE08 £8 8D 0F
		Fing	gerprint (MDS) E	08/22/33/92/50/F7/70/2A 05/28/00/2D/57/C0/F7/8C
		SAN	NS E	pub-ms.domain.com, domain.com, sub.domain.com, pub.domain.com, imp.domain.com, 10.xx.xx.xx

- 3. SANが一致しないことを確認したら、次の2つの方法で修正します。
 - 1. CSRで送信されるのとまったく同じSANエントリを持つ証明書を発行するようにCA管理者 に依頼します。
 - 2. CAの要件を満たすCSRをCUCMで作成します。

CUCMによって作成されたCSRを変更するには、次の手順を実行します。

- 1. CAがドメインを削除すると、ドメインなしでCUCM内にCSRを作成できます。CSRの作成 中に、デフォルトで設定されているドメインを削除します。
- 2. <u>マルチSAN証明書</u>が作成された場合、共通名の msを受け入れないCAがあります。-msは 、CSRの作成時にCSRから削除できます。

Generate Certificate Signing Request	
💽 Generate 🌁 Close	
C Status	
Warning: Generating a new CSR for a specific ce	rtificate type will overwrite the existing CSR for that type
Generate Certificate Signing Request	
Certificate Purpose**	tomcat
Distribution*	Multi-server(SAN)
Common Name*	11Spub-ms.
Subject Alternate Names (SANS)	
Auto-populated Domains	115pub. 115pub.
Other Domains	
Key Type** Key Length*	RSA V
Hash Algorithm*	SHA256 ¥
Generate Close	

3. CUCMによって自動補完された名前以外の代替名を追加するには、次の手順を実行します。

1. マルチSAN証明書を使用する場合は、追加のFQDNを使用できます。(IPアドレスは受け付けられません)。

Generate 🖳 Close			
Status Warning: Generating a new	CSR for a specific certificate type will overwrit	e the existing CSR for that type	
Generate Certificate Signing I	Request		
Certificate Purpose**	tomcat	~	
Distribution*	Multi-server(SAN)	~	
Common Name*	11Spub-ms		
Subject Alternate Names (SA	Ns)		
Auto-populated Domains	11Simp. 11Spub 11Ssub		
Parent Domain			
Other Domains	extraHostname.domain.com	E Cheo For m	se File ore info
]	udd
Key Type**	RSA		
Key Length*	2048	~	
Hash Algorithm*	SHA256	~	

b.証明書がシングルノードの場合は、set web-securityコマンドを使用します。このコマンドは、マル チSAN証明書にも適用されます。(任意の種類のドメインを追加できます。また、IPアドレスも 許可されます)。

詳細については、『<u>コマンドラインリファレンスガイド』</u>を参照してください<u>。</u>

同じCNの信頼証明書は置き換えられません

CUCMは、同じ共通名(CN)と同じ証明書タイプを持つ証明書を1つだけ保存するように設計され ています。つまり、tomcat-trustの証明書がデータベースにすでに存在し、同じCNの最新の証明 書に置き換える必要がある場合、CUCMは古い証明書を削除して、新しい証明書に置き換えます 。 CUCMが古い証明書を置き換えない場合があります。

- 1. アップロードされた証明書の有効期限が切れています。CUCMでは、有効期限が切れた証明 書をアップロードすることはできません。
- 2. 古い証明書の方が、新しい証明書よりも新しい日付のFROMを持っています。CUCMは最新 の証明書を保持し、古い開始日は古い日付としてカタログ化されます。このシナリオでは、 不要な証明書を削除してから、新しい証明書をアップロードする必要があります。

Certificate	х	Certificate	×
General Details Certification Path		General Details Certification Path	
Certificate Information		Certificate Information	
This certificate is intended for the following purpose(s): • Al issuance policies • Al application policies		This certificate is intended for the following purpose(s): • Al issuance policies • Al application policies	
Old Certificate		New Certificate	
Issued to: Colab CA		Issued to: Colab CA	
Issued by: Colab CA		Issued by: Colab CA	
Valid from 7/23/2019 to 7/23/2024		Valid from 5/23/2019 to 12/23/2030	
Issuer Statement	Í	Issuer Statement	
OK		ox	

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。