署名付きCA証明書からの新しい証明書の作成

内容

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

ください。

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、『証明書の再生成ガイド』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、『マルチSAN証明書の再生成ガイド』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、『自己署名再生成ガイド』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。『セキュリティガイド』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。

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

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。

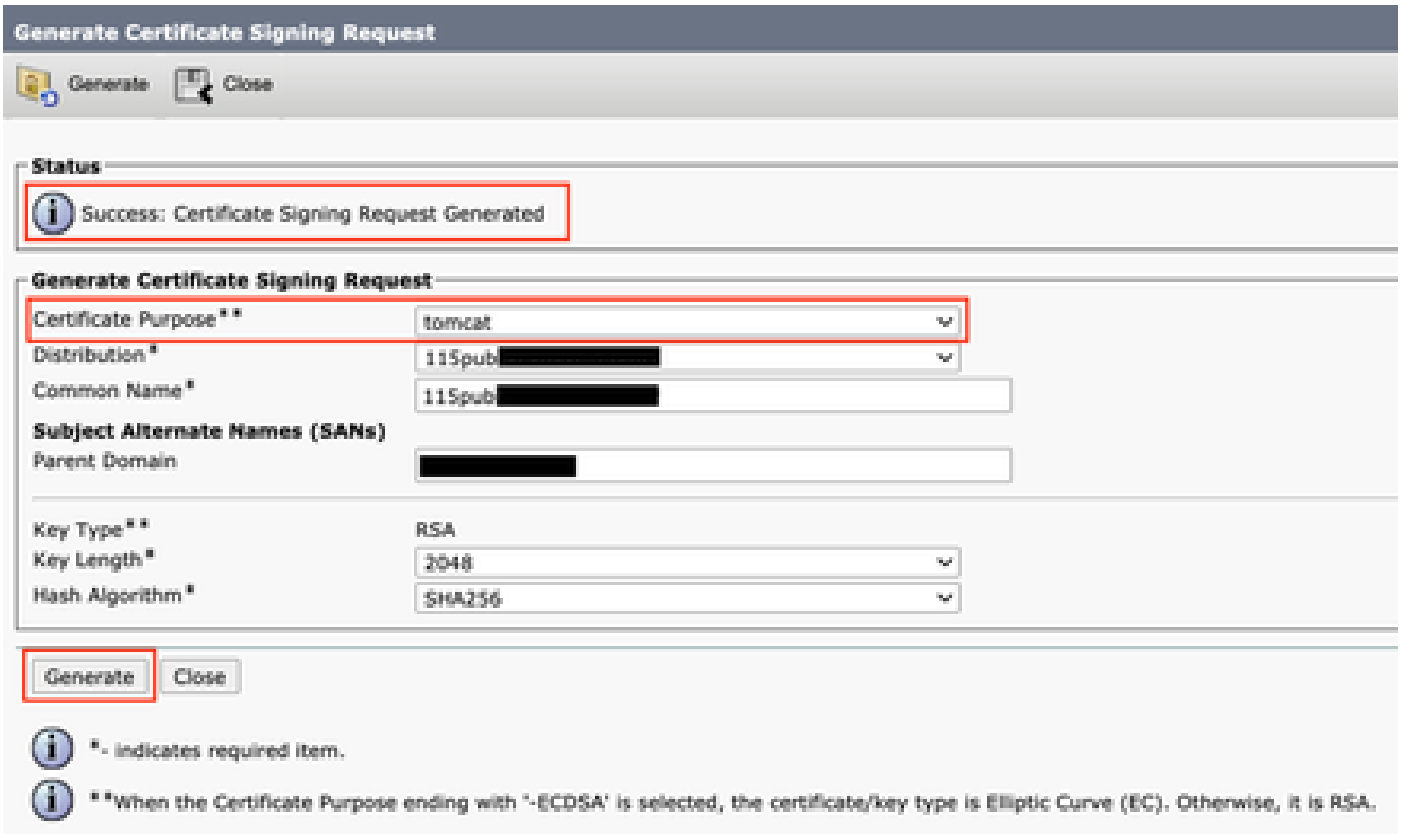
Tomcat証明書

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。

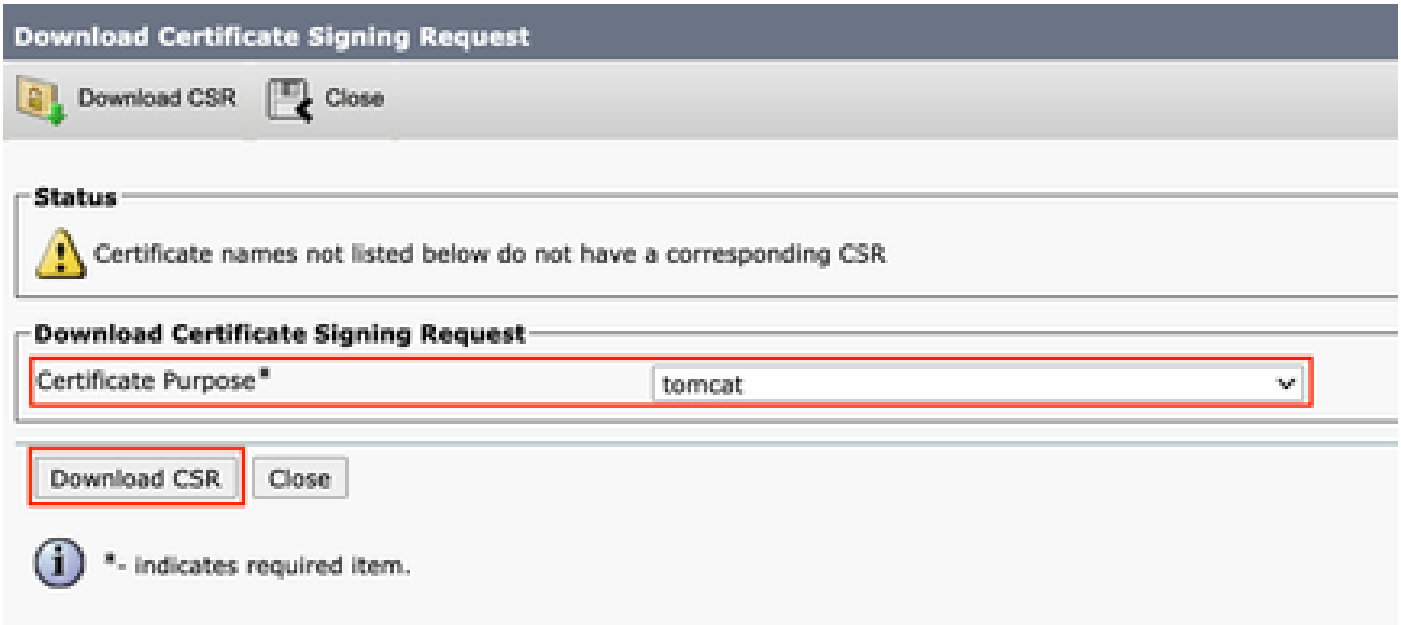
クラスタのすべてのノード（CallManagerおよびIM&P）で、次の操作を行います。

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。



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。



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。

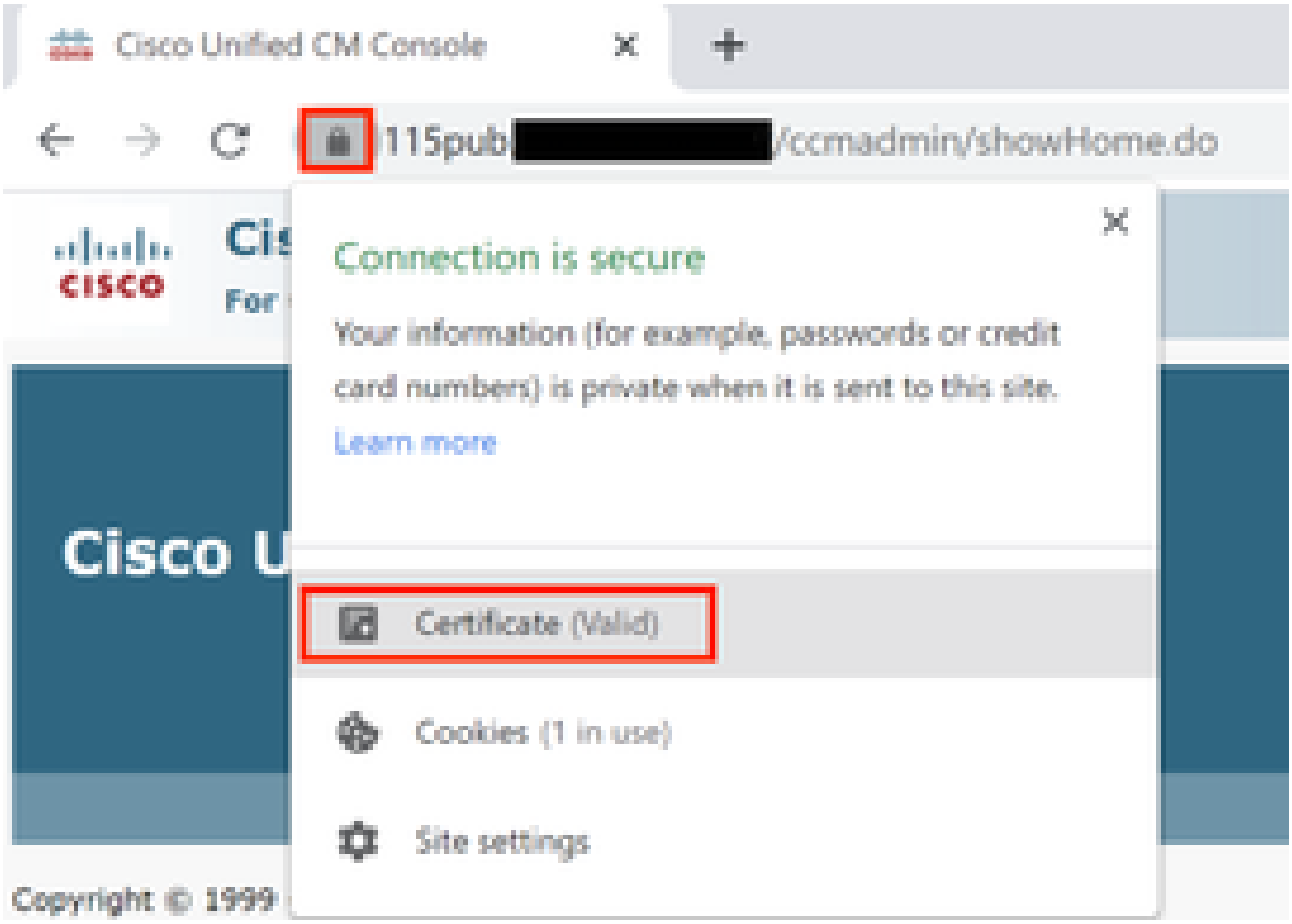
注：一部のCAは中間証明書を提供しません。ルート証明書だけを指定した場合は、この手順を省略できます。

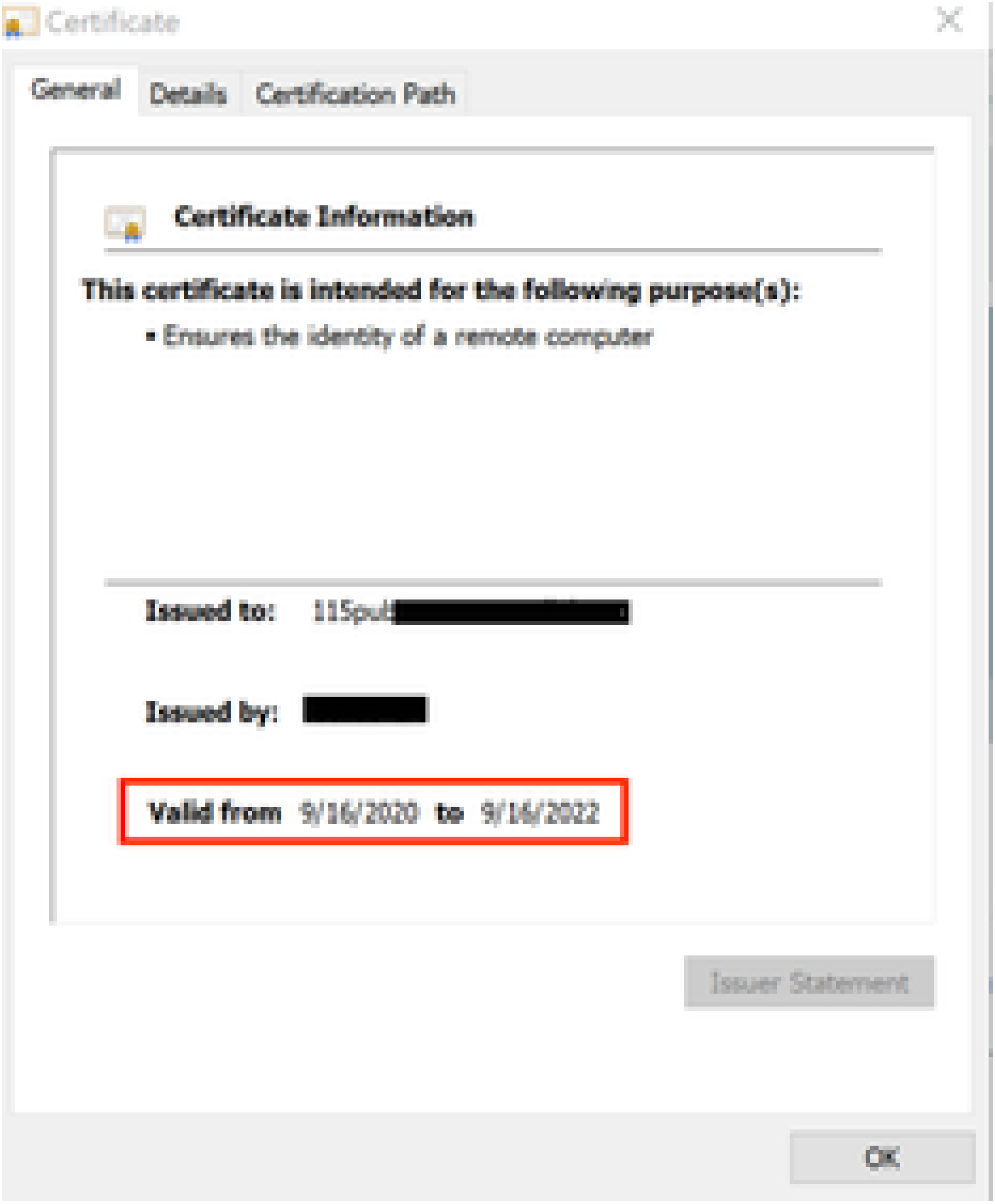
- tomcatとしてのCA署名付き証明書Certificate Management > Upload certificate > Certificate Purpose: tomcatに移動します。 証明書の説明を設定し、現在のCUCMノードのCA署名付き証明書ファイルを参照します。

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。





CallManager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。

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 CallManager
- 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、ルート証明書ファイルを参照します。
- 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< /strong>」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 - 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(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（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。

- 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：

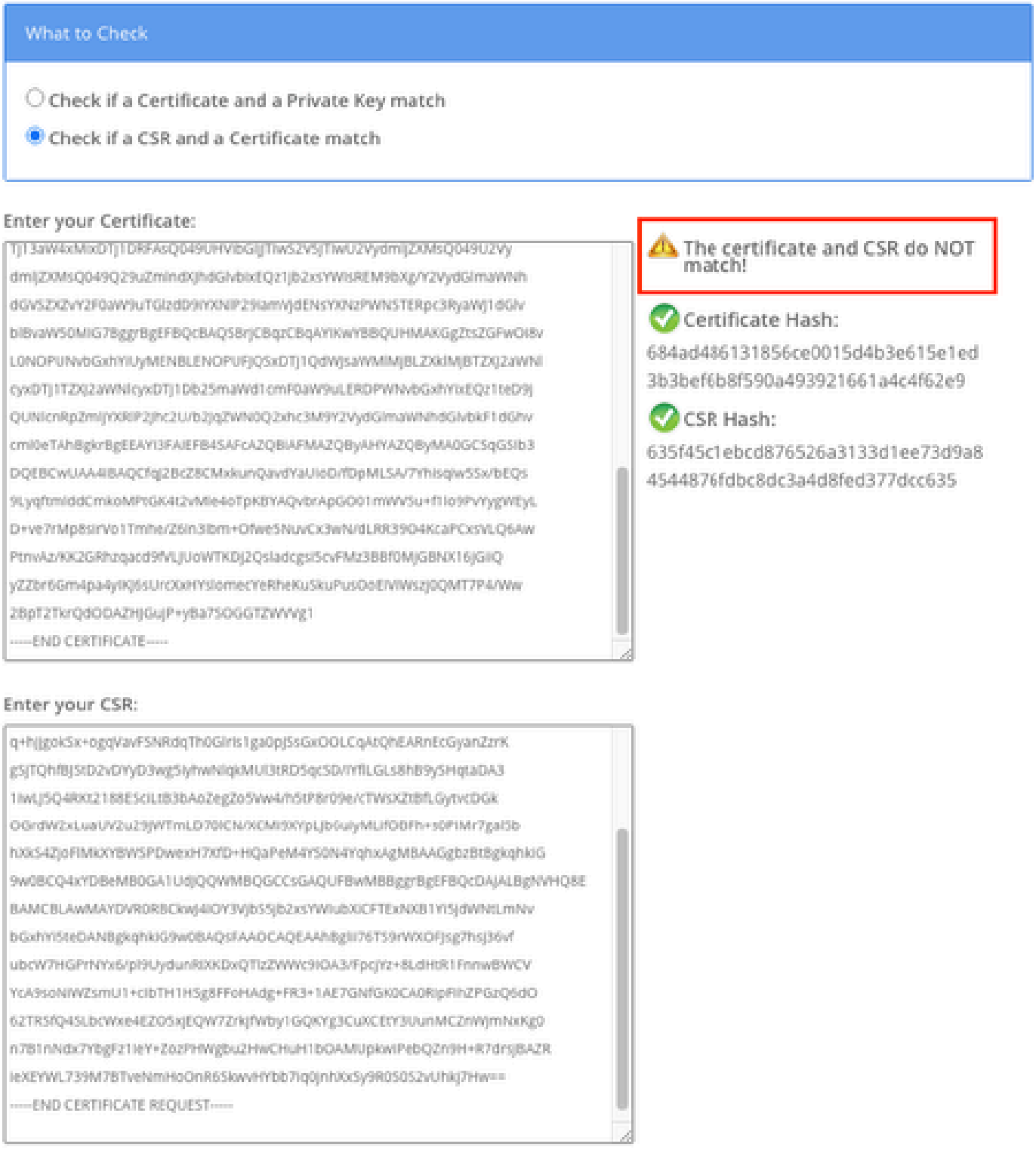
- サーバおよび証明書タイプごとに1つのCSRのみ存在できます。つまり、新しいCSRを作成すると、古いCSRが置き換えられます。
- ワイルドカード証明書はCUCMではサポートされていません。
- 新しいCSRがないと、現在有効なサービス証明書を置き換えることはできません。
- 同じ問題に関する別のエラーとして、「The file /usr/local/platform/upload/certs//tomcat.der could not be uploaded」が考えられます。 これは、CUCMのバージョンによって異なります。

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、SSLなどの複数のツールをオンラインで使用します。



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。

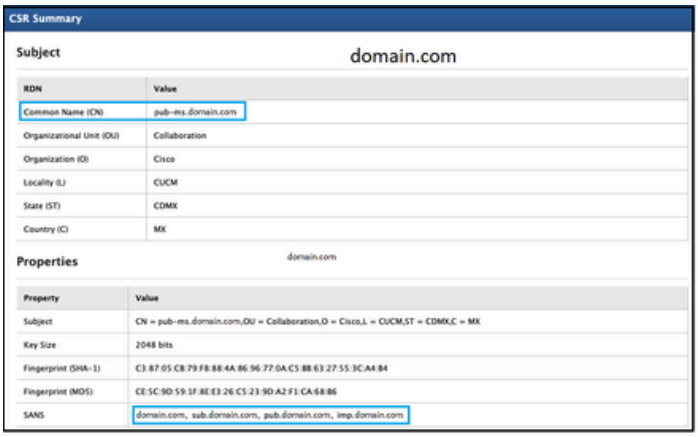
CSRサブジェクトの別名(SAN)と証明書SANが一致しない

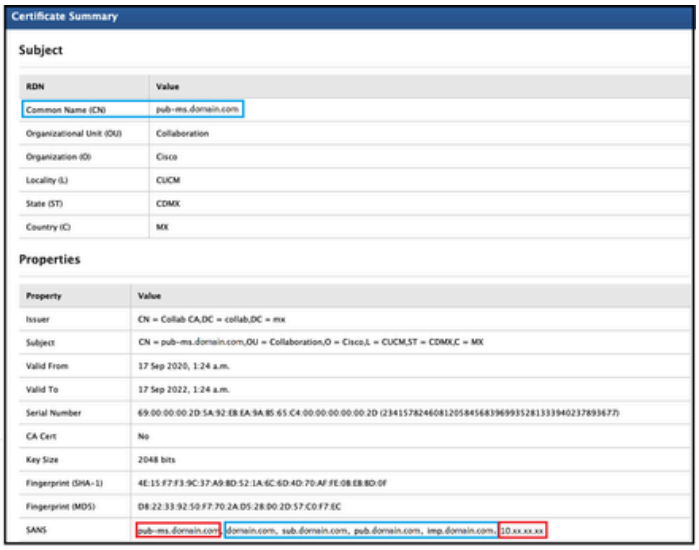
CSRと証明書の間のSANは同じである必要があります。これにより、許可されていないドメインの認証が防止されます。SANの不一致を確認するには、次の手順を実行します。

1. CSRと証明書を復号化します（ベース64）。デコーダなど、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。



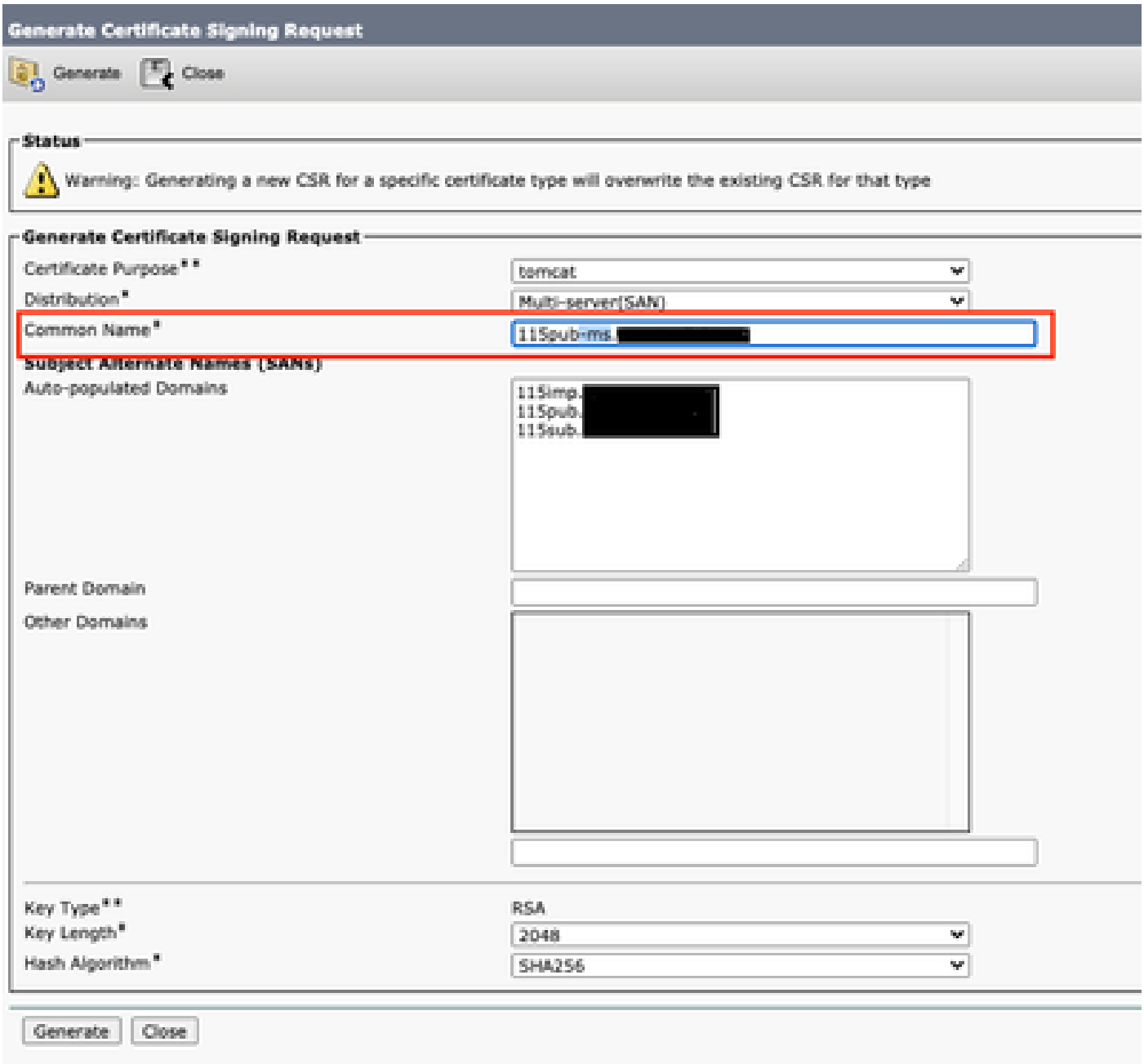


3. SANが一致しないことを確認したら、次の2つの方法で修正します。

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。

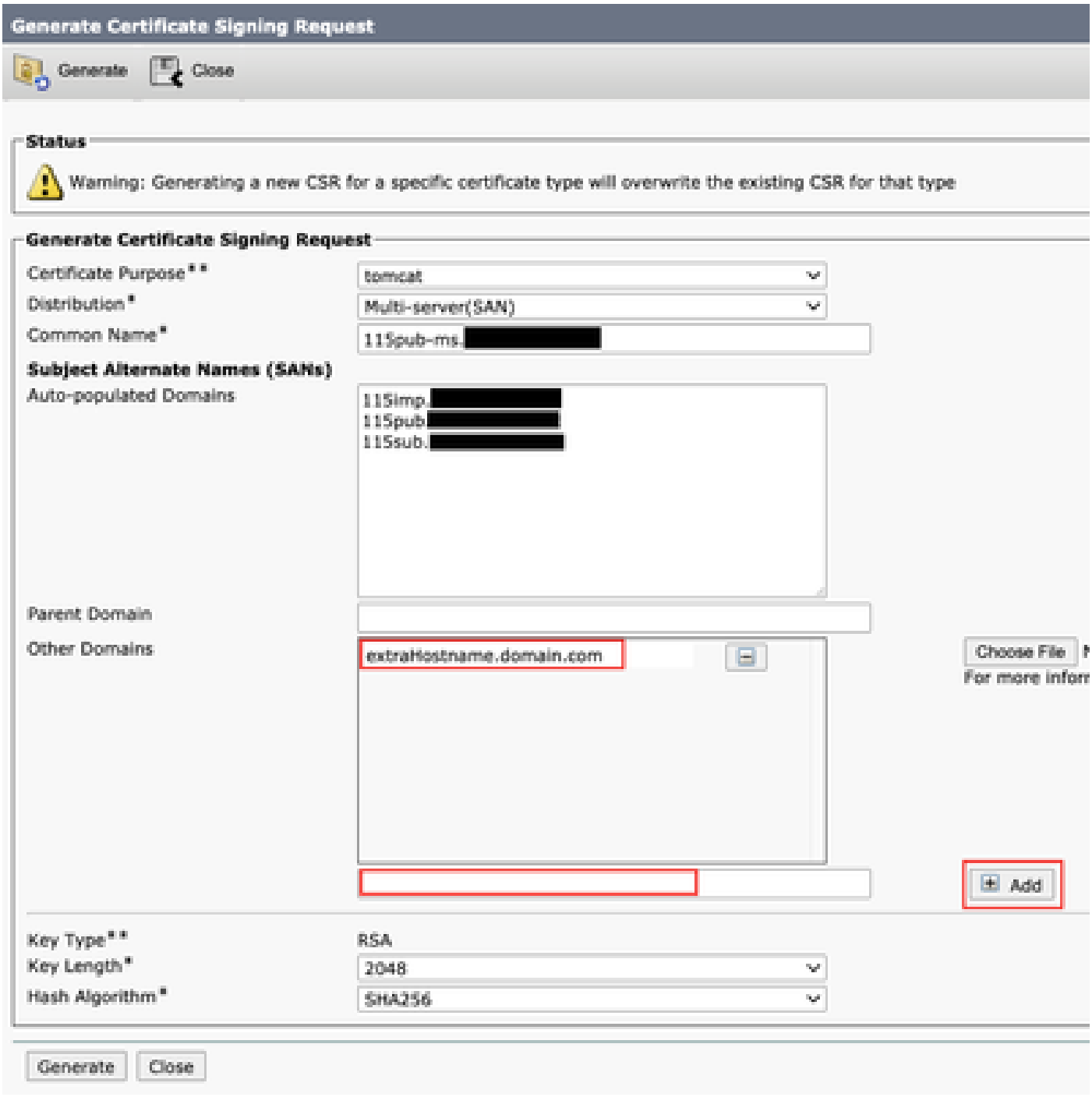
CUCMによって作成されたCSRを変更するには、次の手順を実行します。

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. マルチSAN証明書が作成された場合、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。



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）。



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）。

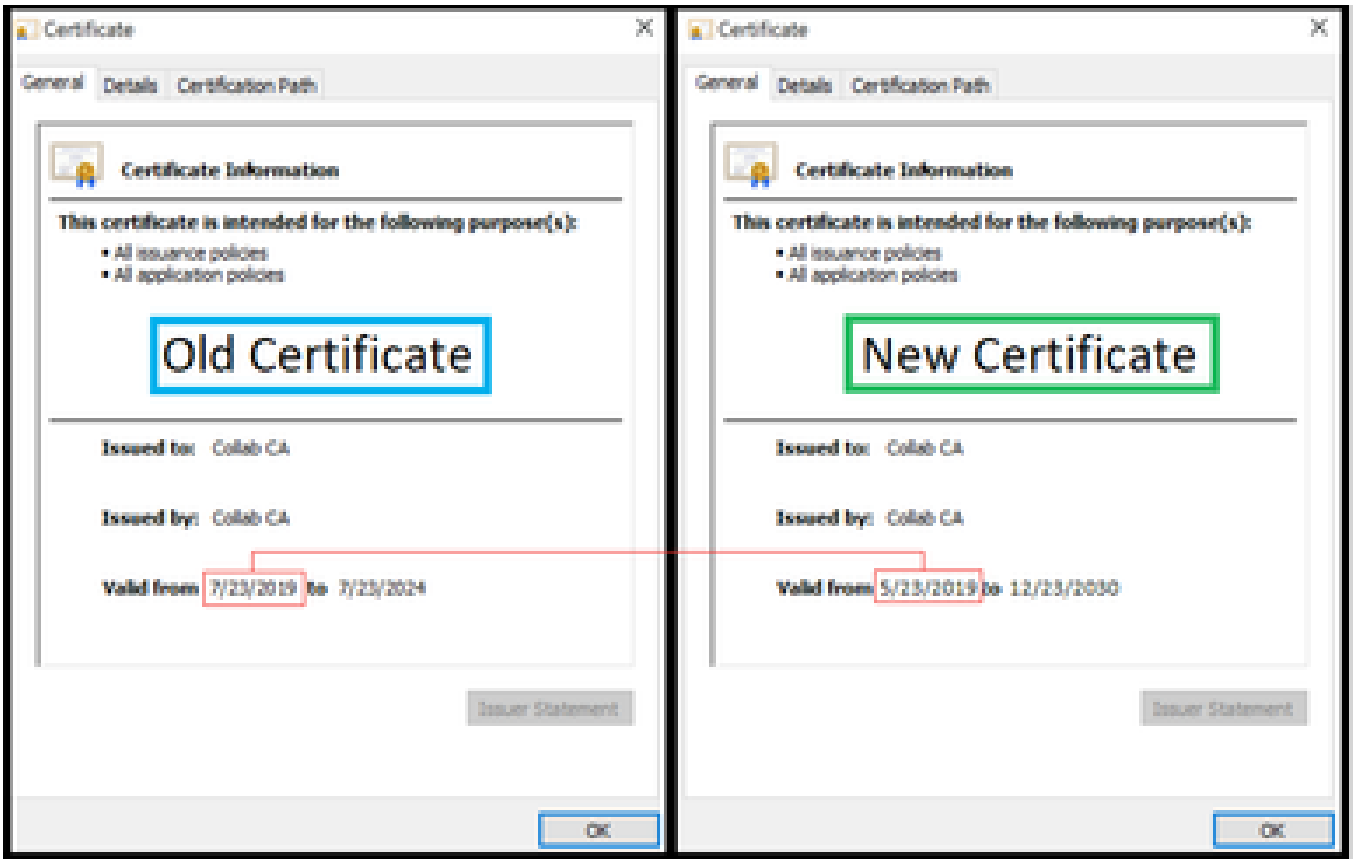
詳細については、『コマンドラインリファレンスガイド』を参照してください。

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。



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。