パッケージ CCE ソリューション: サード パーティ CA 証明書を入手してアップロードするプロシージャ

目次

概要

この資料は Finesse および Cisco Unified Intelligence Center （CUIC）サーバ間の HTTPS 接続を確立するために生成されるサードパーティベンダーから Certification Authority （CA） 証明書を得、インストールするために必要となるステップを記述したものです。

HTTPS を Finesse と CUIC サーバ間のセキュアコミュニケーションのために使用するために、セキュリティ 証明書設定は必要です。 デフォルトで、これらのサーバは使用するまたは顧客は CA 証明書を手に入れ、インストールできます自己署名証明書を提供します。 これらの CA 証明書は VeriSign のようなサードパーティベンダーから GeoTrust、Thawte 得る、ことができましたりまたは内部で 生成 することができます。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco パッケージ コンタクトセンター エンタープライズ（PCCE）
- CUIC
- Cisco Finesse
- CA 証明書

使用するコンポーネント

資料で使用される情報は PCCE ソリューション 11.0 （1）バージョンに基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 ネットワークがライブである場合、あらゆるステップの潜在的影響を理解することを確かめて下さい。

手順

Finesse および CUIC サーバの HTTPS コミュニケーションのための証明書を設定するために、次の手順に従って下さい:

- 生成し、ダウンロードして下さい証明書署名要求（CSR）を
- CSR の使用の CA からのルート、中間物（適当であれば）およびアプリケーション 証明書を得て下さい
- サーバに証明書をアップ ロードして下さい

CSR を生成し、ダウンロードして下さい

1. ここに記述されているステップは CSR を生成し、ダウンロードするためです。 これらのステップは Finesse および CUIC サーバのため同じです。

2. URL の **Cisco Unified Communications オペレーティング システム管理 ページを**開き、インストール プロセスの時に作成される Operating System （OS） 管理者アカウントと署名して下さい。 **プライマリ サーバー/cmplatform の https://hostname**

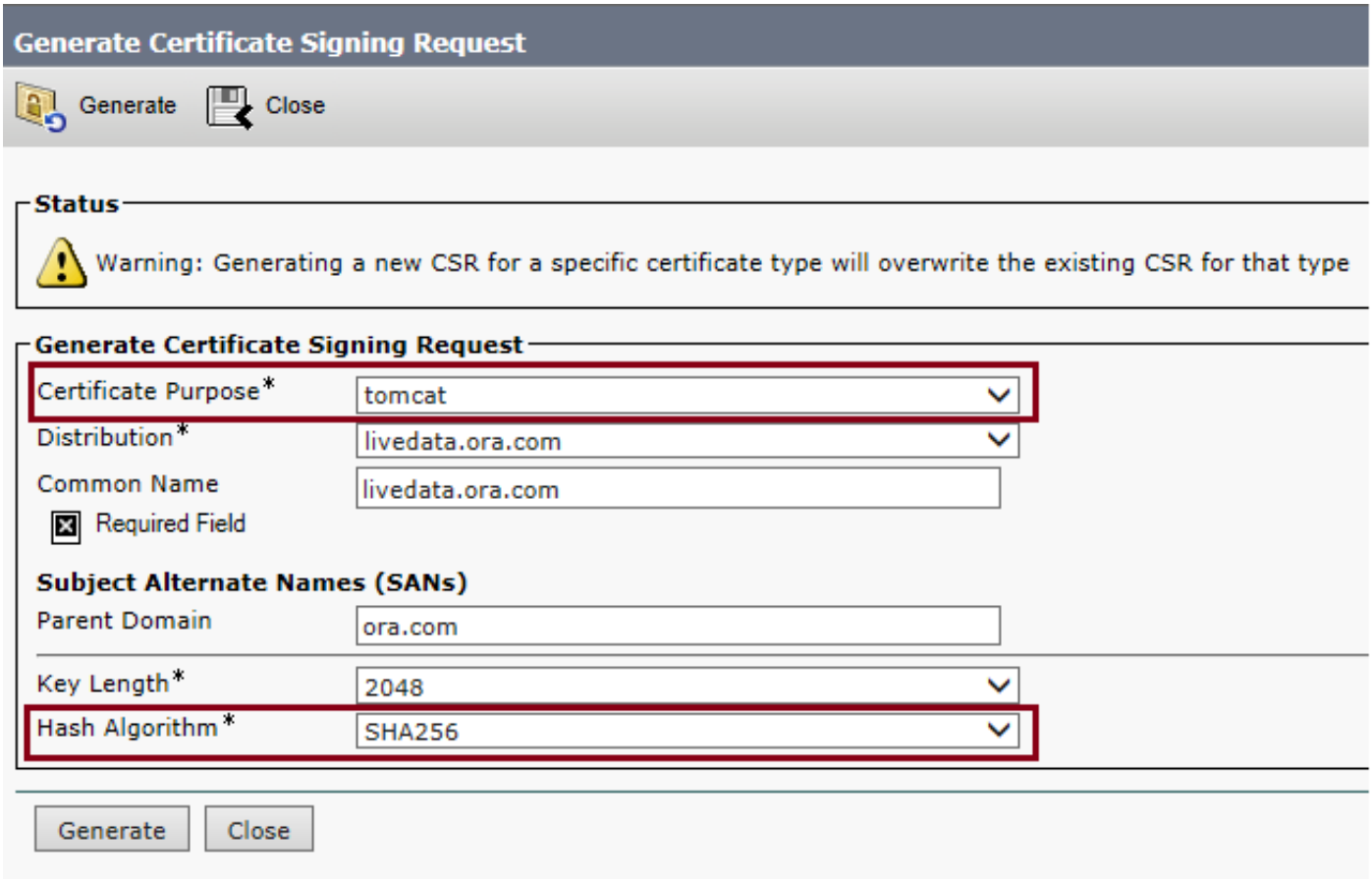
3. 生成する 証明書署名要求。

a. **セキュリティ > Certificate Management > 生成する CSR** にナビゲートして下さい。

b. 証明書 Purpose* ドロップダウン リストから、**Tomcat を**選択して下さい。

c. **SHA256** としてハッシュ アルゴリズムを選択して下さい。

d. イメージに示すように『Generate』 をクリック して下さい。

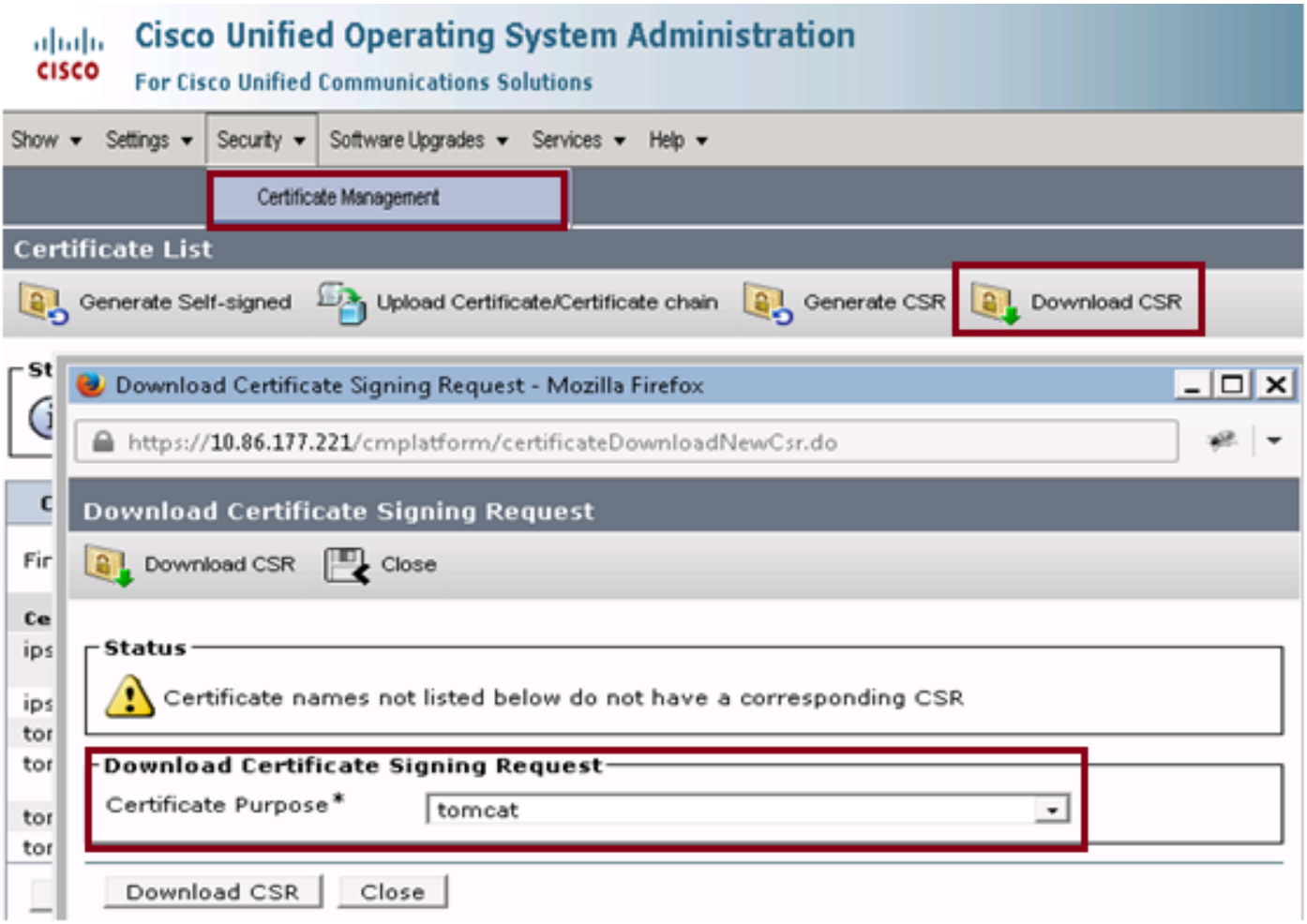


4. CSR をダウンロードして下さい。

a. **セキュリティ > Certificate Management > ダウンロード CSR** にナビゲートして下さい。

b. 証明書 Purpose* ドロップダウン リストから、**Tomcat を**選択して下さい。

c. イメージに示すように **CSR を**『Download』 をクリック して下さい。



注: CA のための CSR を得るために**セカンダリサーバ/cmplatform の** URL **https://hostname** とセカンダリサーバのこれらのステップを実行して下さい。

CA からのルート、中間物（適当であれば）およびアプリケーション 証明書を得て下さい

1. VeriSign、Thawte、GeoTrust 先祖などのようなサード パーティ CA にプライマリおよびセカンダリサーバの CSR 情報を提供します

2. CA から、これらのプライマリおよびセカンダリサーバのための証明書 チェーンを受け取って下さい:

- Finesse サーバ: ルート、中間物およびアプリケーション 証明書
- CUIC サーバ: ルートおよびアプリケーション 証明書

サーバへのアップ ロード証明書

このセクションは方法で Finesse および CUIC サーバで証明書 チェーンを正しくアップ ロードする記述します。

Finesse サーバ

1. アップ ロード プライマリ Finesse サーバルート 証明書:

a. プライマリ サーバの **Cisco Unified Communications オペレーティング システム管理 ページ**で、**セキュリティ > Certificate Management > アップ ロード証明書**にナビゲートして下さい。

b. 証明書目的ドロップダウン リストから、Tomcat **信頼を**選択して下さい。

c. アップ ロード File フィールドで、**ルート証明ファイルを**『Browse』 をクリック し、参照して下さい。

d. [Upload File] をクリックします。

2. プライマリ Finesse サーバ中間証明書をアップ ロードして下さい:

a. 証明書目的ドロップダウン リストから、Tomcat **信頼を**選択して下さい。

b. ファイルされるルート証明では前のステップでアップ ロードされるルート証明の名前を入力して下さい。 これはルート/公共証明書がインストールされたときに生成される **.pem** ファイルです。

このファイルを表示するために、**証明書管理 > 検索**にナビゲートします。 証明書リストでは、**.pem** ファイル名は Tomcat 信頼に対してリストされています。

c. アップ ロード File フィールドで、**中間証明書ファイルを**『Browse』 をクリック し、参照して下さい。

d. [Upload File] をクリックします。

> **注:** Tomcat 信頼ストアがプライマリとセカンダリサーバの間で複製されると同時にセカンダリ Finesse サーバにプライマリ Finesse サーバルートか中間物証明書をアップ ロードするために、必要ではないです。

3. アップ ロード プライマリ Finesse サーバアプリケーション 証明書:

a. 証明書目的ドロップダウン リストから、**Tomcat を**選択して下さい。

b. ルート証明 フィールドでは、前のステップでアップ ロードされる中間証明書の名前を入力して下さい。 **.pem** 拡張を含んで下さい（ たとえば、テスト SSLCA.pem ）。

c. アップ ロード File フィールドで、**アプリケーション 証明書ファイルを**『Browse』 をクリックし、参照して下さい。

d. [Upload File] をクリックします。

4. セカンダリ Finesse サーバルートおよび中間物証明書をアップ ロードして下さい:

a. 証明書のためのセカンダリサーバのステップ 1 および 2 に言及されているように同じステップに従って下さい。

> **注:** Tomcat 信頼ストアがプライマリとセカンダリサーバの間で複製されると同時にプライマリ Finesse サーバにセカンダリ Finesse サーバルートか中間物証明書をアップ ロードするために、必要ではないです。

5. アップ ロード セカンダリ Finesse サーバアプリケーション 証明書:

a. 自身の証明書のためのセカンダリサーバのステップ 3.に言及されているように同じステップに従って下さい。

6. 再始動サーバ:

a. プライマリおよびセカンダリ Finesse サーバの CLI にアクセスし、サーバを再起動するためにコマンド **utils システム 再始動を**実行して下さい。

CUIC サーバ

1. アップ ロード CUIC プライマリ サーバルート (パブリック) 証明書:

a. プライマリ サーバの **Cisco Unified Communications オペレーティング システム管理 ページ**で、**セキュリティ > Certificate Management > アップ ロード証明書**にナビゲートして下さい。

b. 証明書目的ドロップダウン リストから、Tomcat **信頼を**選択して下さい。

c. アップ ロード File フィールドで、**ルート証明ファイルを**『Browse』 をクリック し、参照して下さい。

d. [Upload File] をクリックします。

> **注:** Tomcat 信頼ストアがプライマリとセカンダリサーバの間で複製されると同時にセカンダリ CUIC サーバにプライマリ CUIC サーバルート 証明書をアップ ロードするために、必要ではないです。

2. アップ ロード CUIC プライマリ サーバアプリケーション (プライマリ) 証明書:

a. 証明書目的ドロップダウン リストから、**Tomcat を**選択して下さい。

b. ルート証明 フィールドでは、前のステップでアップ ロードされるルート証明の名前を入力して下さい。

これはルート/公共証明書がインストールされたときに生成される **.pem** ファイルです。 このファイルを表示するために、**証明書管理 > 検索**にナビゲートします。

証明書リスト **.pem** でファイル名は Tomcat 信頼に対してリストされています。 その .pem 拡張を含んで下さい (たとえば、テスト SSLCA.pem) 。

c. アップ ロード File フィールドで、**アプリケーション (プライマリ) 証明書ファイルを**『Browse』 をクリック し、参照して下さい。

d. [Upload File] をクリックします。

3. CUIC セカンダリサーバ ルート (パブリック) 証明書をアップ ロードして下さい:

a. セカンダリ CUIC サーバで、ルート証明のためのステップ 1.に言及されているように同じステップに従って下さい。

注: Tomcat 信頼ストアがプライマリとセカンダリサーバの間で複製されると同時にプライマリ CUIC サーバにセカンダリ CUIC サーバルート 証明書をアップ ロードするために、必要ではないです。

4. アップ ロード CUIC セカンダリサーバ アプリケーション（プライマリ）証明書:

a. 自身の証明書のためのセカンダリサーバのステップ 2.で既述のとおりに同じプロセスに従って下さい。

5. 再始動サーバ:

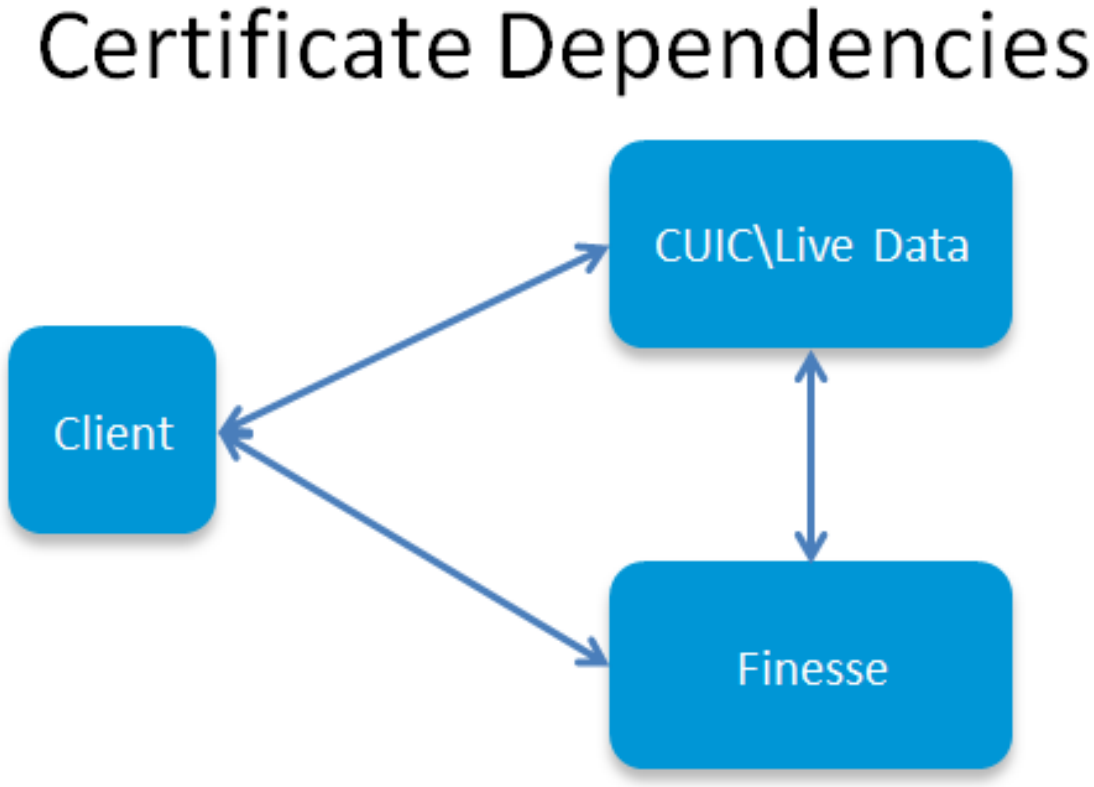
a. プライマリおよびセカンダリ CUIC サーバの CLI にアクセスし、サーバを再起動するためにコマンド **utils システム 再始動を**実行して下さい。

注: 警告する証明書 例外を避けるために完全修飾ドメイン名 （FQDN）の使用のサーバにアクセスして下さい。

証明書 依存関係

Finesse エージェントおよびスーパバイザが CUIC 小道具を報告目的のために利用するので、これらのサーバ間の HTTPS コミュニケーションのための証明書 依存関係を維持するためにここに述べられる順序でおよびイメージに示すようにルート証明をこれらのサーバのまたアップ ロードしなければなりません。

- Finesse プライマリ サーバの CUIC サーバ ルート証明をアップ ロードして下さい
- CUIC プライマリ サーバの Finesse ルート\中間証明書をアップ ロードして下さい



Finesse プライマリ サーバの CUIC サーバ ルート証明をアップ ロードして下さい

1. プライマリ Finesse サーバで、URL の開いた **Cisco Unified Communications オペレーティング システム管理 ページは**インストール プロセスの時に作成される OS 管理者アカウントと署名し、:

プライマリ Finesse サーバ/cmplatform の https://hostname

2. アップ ロード プライマリ CUIC ルート証明。

a. **セキュリティ > Certificate Management > アップ ロード証明書**にナビゲートして下さい。

b. 証明書目的ドロップダウン リストから、Tomcat **信頼を**選択して下さい。

c. アップ ロード File フィールドで、**ルート証明ファイルを**『Browse』 をクリック し、参照して下さい。

d. [Upload File] をクリックします。

3. セカンダリ CUIC ルート証明をアップ ロードして下さい。

a. **セキュリティ > Certificate Management > アップ ロード証明書**にナビゲートして下さい。

b. 証明書目的ドロップダウン リストから、Tomcat **信頼を**選択して下さい。

c. アップ ロード File フィールドで、**ルート証明ファイルを**『Browse』 をクリック し、参照して下さい。

d. [Upload File] をクリックします。

> **注:** Tomcat 信頼ストアがプライマリとセカンダリサーバの間で複製されると同時にセカンダリ Finesse サーバに CUIC ルート証明をアップ ロードするために、必要ではないです。

4. プライマリおよびセカンダリ Finesse サーバの CLI にアクセスし、サーバを再起動するためにコマンド **utils システム 再始動を**実行して下さい。

CUIC プライマリ サーバの Finesse ルート/中間証明書をアップ ロードして下さい

1. プライマリ CUIC サーバで、URL の開いた **Cisco Unified Communications オペレーティング システム管理 ページは**インストール プロセスの時に作成される OS 管理者アカウントと署名し、:

プライマリ CUIC サーバ/cmplatform の https://hostname

2. アップ ロード プライマリ Finesse ルート証明:

a. **セキュリティ > Certificate Management > アップ ロード証明書**にナビゲートして下さい。

b. 証明書目的ドロップダウン リストから、Tomcat **信頼を**選択して下さい。

c. アップ ロード File フィールドで、**ルート証明ファイルを**『Browse』 をクリック し、参照して下さい。

d. [Upload File] をクリックします。

3.Upload プライマリ Finesse 中間証明書:

a. 証明書目的ドロップダウン リストから、Tomcat **信頼を**選択して下さい。

b. ファイルされるルート証明では前のステップでアップ ロードされるルート証明の名前を入力して下さい。

c. アップ ロード File フィールドで、**中間証明書ファイルを**『Browse』 をクリック し、参照して下さい。

d. [Upload File] をクリックします。

4. 同じステップ 2 およびプライマリ ライブ データ サーバのセカンダリ Finesse ルート\中間証明書のためのステップ 3.を実行して下さい。

> **注:** Tomcat 信頼ストアがプライマリとセカンダリサーバの間で複製されると同時にセカンダリ CUIC サーバに Finesse ルート /Intermediate 証明書をアップ ロードするために、必要ではないです。

5. プライマリおよびセカンダリ CUIC サーバの CLI にアクセスし、サーバを再起動するためにコマンド **utils システム 再始動を**実行して下さい。