

パッケージ CCE ソリューション: サードパーティ CA 証明書入手してアップロードするプロセス

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[手順](#)

[生成するおよびダウンロード CSR](#)

[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 証明書を取得下さい](#)

[サーバに証明書をアップロードして下さい](#)

[サーバをうまく解決して下さい](#)

[CUIC サーバ](#)

[証明書 依存関係](#)

[Finesse プライマリ サーバのアップロード CUIC サーバルート証明](#)

[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](#)

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、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お勧めします。

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、次の手順に従ってください:

- 生成し、ダウンロードしてくだ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
得てください
- サーバに証明書をアップロードしてください

CSR を生成し、ダウンロードしてください

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ください。**プライマリ サーバ/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** にナビゲートしてください。
 - b. 証明書 Purpose* ドロップダウン リストから、**Tomcat** を選択してください。
 - c. **SHA256** としてハッシュ アルゴリズムを選択してください。
 - d. イメージに示すように 『Generate』 をクリックしてください。

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*	tomcat
Distribution*	livedata.ora.com
Common Name	livedata.ora.com
<input checked="" type="checkbox"/> Required Field	
Subject Alternate Names (SANs)	
Parent Domain	ora.com
Key Length*	2048
Hash Algorithm*	SHA256

Generate

Close

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。



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

Certificate Management

Certificate List



Generate Self-signed



Upload Certificate/Certificate chain



Generate CSR



Download CSR



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 **信頼**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. 証明書目的のドロップダウン 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、必要ではありません。

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. 証明書目的のドロップダウン 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、必要ではありません。

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.で既述のとおりと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。

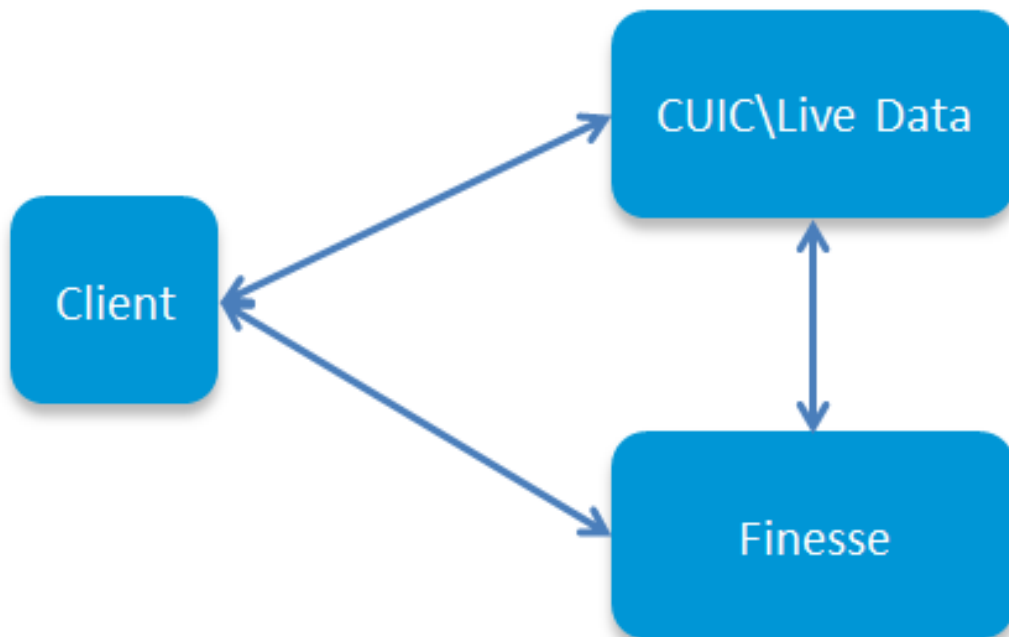
注: 警告する証明書 例外を避けるために完全修飾ドメイン名 (FQDN) の使用のサーバにアクセスして下さい。

証明書 依存関係

Finesse エージェントおよびスーパーバイザが 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

Certificate Dependencies



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. 証明書目的のドロップダウン 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. 証明書目的のドロップダウン 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. 証明書目的のドロップダウン 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、必要ではありません。

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。