パッケージ CCE ソリューション： サードパーティ CA 証明書を取得してアップロードする手順

目次

概要
前提条件
要件
使用するコンポーネント
手順
ステップ 1： 証明書署名要求（CSR）の生成とダウンロード
ステップ 2： 認証局からのルート、中間（該当する場合）、およびアプリケーション証明書の取得
ステップ 3： サーバへの証明書のアップロード
Finesse サーバ：
CUIC サーバ：
a) CUIC サーバのルート証明書を Finesse プライマリ サーバにアップロードする
b) Finesse のルート\中間証明書を CUIC プライマリ サーバにアップロードする
Cisco サポート コミュニティ - 特集対話

概要

Finesse サーバと Cisco Unified Intelligence Center（CUIC）サーバの間で HTTPS を使用したセキュア通信を保護するために、セキュリティ証明書の設定が必要です。 デフォルトでは、これらのサーバは使用される自己署名証明書を提供し、顧客が認証局（CA）証明書を取得し、インストールすることもできます。 これらの CA 証明書は、VeriSign、Thawte、GeoTrust などのサードパーティ ベンダーから取得するか、または内部で調達できます。

このドキュメントでは、サードパーティ ベンダーから生成された認証局（CA）証明書を取得およびインストールし、Finesse サーバと Cisco Unified Intelligence Center（CUIC）サーバとの間で HTTPS 接続を確立するための手順を詳しく説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Package Contact Center Enterprise（PCCE）
- Cisco Unified Intelligence Center（CUIC）
- Cisco Finesse
- CA 証明書

使用するコンポーネント

このドキュメント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。 ネットワークが稼働中の場合は、各手順が及ぼす潜在的な影響を十分に理解しておく必要があります。

手順

Finesse サーバと Cisco Unified Intelligence Center（CUIC）サーバの HTTPS 通信を実現するための証明書の設定では次の手順が必要です。

- 証明書署名要求（CSR）の生成とダウンロード。
- CSR を使用して、認証局からのルート、中間（該当する場合）、およびアプリケーション証明書を取得します。
- サーバへの証明書のアップロード。

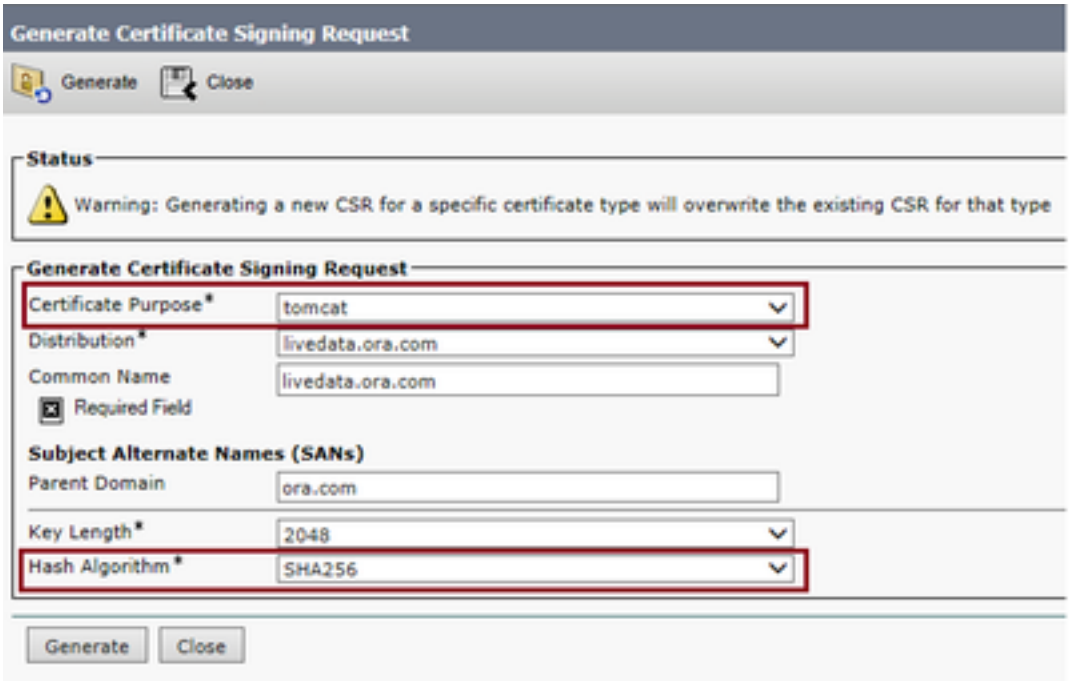
ステップ 1： 証明書署名要求（CSR）の生成とダウンロード

---

1. CSRを生成してダウンロードするには、次の手順では、FinesseおよびCUICサーバで同じです。

2. 下で指定された URL を使用して [Cisco Unified Communications Operating System Administration] ページを開き、インストール プロセスで作成された OS 管理者アカウントでサインインします
https://hostname of primary server/cmplatform

3. 証明書署名要求（CSR）の生成

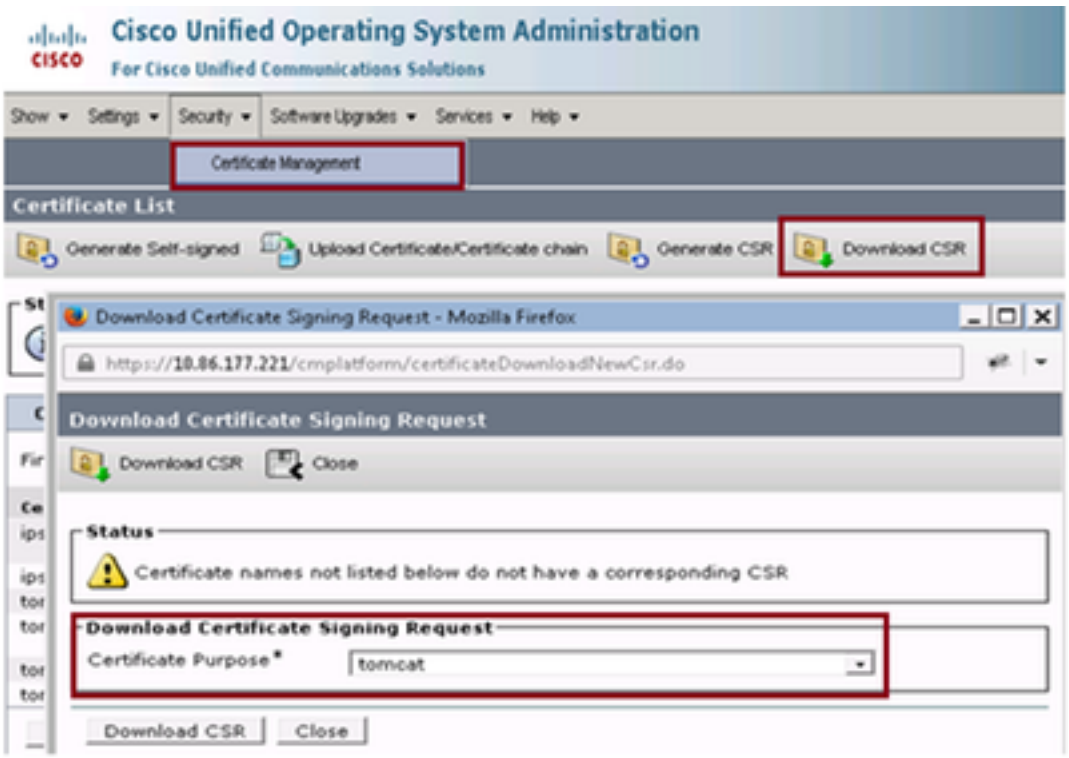


a) [Security] > [Certificate Management] > [Generate CSR] を選択します。

b) [Certificate Purpose Name] ドロップダウン リストから、[tomcat] を選択します。

c) [Hash Algorithm] として [SHA256] を選択します。
d) [Generate CSR] をクリックします。

4. 証明書署名要求（CSR）のダウンロード



a) [Security] > [Certificate Management] > [Download CSR] を選択します。
b) [Certificate Name] ドロップダウン リストから、[tomcat] を選択します。
c) [Download CSR] をクリックします。

注：

URL「https://hostname of secondory server/cmplatform」を使用し、セカンダリ サーバで上記の手順を実行して、認証局の CSR を取得します。

ステップ 2： 認証局からのルート、中間（該当する場合）、およびアプリケーション証明書の取得

---

1. プライマリおよびセカンダリ サーバの証明書署名要求（CSR）情報を VeriSign、Thawte、GeoTrust などのサードパーティ認証局（CA）に提供します。

2. 認証局（CA ）から、プライマリおよびセカンダリ サーバに関する次の証明書チェーンを受信する必要があります。

- **Finesse サーバ： ルート、中間、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**

ステップ 3： サーバへの証明書のアップロード

このセクションでは、Finesse および Cisco Unified Intelligence Center（CUIC）サーバに証明書チェーンを正しくアップロードする方法について説明します。

Finesse サーバ：

==========

1. **プライマリ Finesse サーバ ルート証明書のアップロード**

a) プライマリ サーバの [Cisco Unified Communications Operating System Administration] ページで、

[Security] > [Certificate Management] > [Upload Certificate] を選択します。

b) [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
c) [Upload File] フィールドで、[browse] をクリックし、ルート証明書ファイルを参照します。
d) [Upload File] をクリックします。

2. **プライマリ Finesse サーバ中間証明書のアップロード**

a) [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
b) [ルート証明書（Root Certificate）] フィールドに、前の手順でアップロードしたルート証明書の名前を入力します。

これは、ルート/パブリック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には、[certificate management] に移動して、[Find] をクリックします。 証明書リストでは、.pem ファイル名は tomcast-trust の横にリストされます。
c) [Upload File] フィールドで [Browse] をクリックし、中間証明書ファイルを参照します。
d) [Upload File] をクリックします。

注：
tomcat-trust ストアはプライマリおよびセカンダリ サーバ間で複製されるので、プライマリ Finesse サーバのルートまたは中間証明書をセカンダリ Finesse サーバにアップロードする必要はありません。

３．プライマリ Finesse サーバのアプリケーション証明書をアップロードします。

a) [Certificate Name] ドロップダウン リストから、[tomcat] を選択します。

b）[Root Certificate] フィールドに、前の手順でアップロードした中間証明書の名前を入力します。 .pem の拡張子を記入してください（例：TEST-SSL-CA.pem）。

c）[Upload File] フィールドで [Browse] をクリックし、アプリケーション証明書ファイルを参照します。
d) [Upload File] をクリックします。

4. **セカンダリ Finesse サーバのルートおよび中間証明書をアップロードします。**

a) セカンダリ サーバの証明書について、上記（１）および（２）と同じ手順に従います。

注：
tomcat-trust ストアはプライマリおよびセカンダリ サーバ間で複製されるので、セカンダリ Finesse サーバのルートまたは中間証明書をプライマリ Finesse サーバにアップロードする必要はありません。

5. アップロードのsecondory Finesseアプリケーション サーバの証明書。

a) セカンダリ サーバ独自の証明書について、上記 (3) と同じ手順に従います。

6. **サーバの再起動**

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、コマンド「utils system restart」を入力してサーバを再起動します。

CUIC サーバ :

==========

1. **CUIC プライマリ サーバのルート (パブリック) 証明書のアップロード**

a) プライマリ サーバの [Cisco Unified Communications Operating System Administration] ページで、

[Security] > [Certificate Management] > [Upload Certificate] を選択します。

b) [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
c) [Upload File] フィールドで、[browse] をクリックし、ルート証明書ファイルを参照します。
d) [Upload File] をクリックします。

注：
tomcat-trust ストアはプライマリおよびセカンダリ サーバ間で複製されるので、プライマリ CUIC サーバのルート証明書をセカンダリ CUIC サーバにアップロードする必要はありません。

2. **CUIC プライマリ サーバのアプリケーション (プライマリ) 証明書のアップロード**
a) [Certificate Name] ドロップダウン リストから、[tomcat] を選択します。
b) [Root Certificate] フィールドに、前の手順でアップロードしたルート証明書の名前を入力します。

これは、ルート/パブリック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には、[certificate management] に移動して、[Find] をクリックします。 証明書リストでは、.pem ファイル名は tomcast-trust の横にリストされます。.pem の拡張子を記入してください (例：TEST-SSL-CA.pem) 。

c) [Upload File] フィールドで [Browse] をクリックし、アプリケーション (プライマリ) 証明書ファイルを参照します。
d) [ファイルのアップロード (Upload File)] をクリックします。

3. **CUIC セカンダリ サーバのルート (パブリック) 証明書のアップロード**

a) セカンダリ CUIC サーバのルート証明書について、上記ステップ (1) と同じ手順に従います。

注：

tomcat-trust ストアはプライマリおよびセカンダリ サーバ間で複製されるので、セカンダリ CUIC サーバのルート証明書をプライマリ CUIC サーバにアップロードする必要はありません。

4. CUIC セカンダリ サーバのアプリケーション (プライマリ) 証明書のアップロード
a) セカンダリ サーバ独自の証明書について、上記ステップ (2) と同じ手順に従います。

6. **サーバの再起動**

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、コマンド「utils system restart」を入力してサーバを再起動します。

注 :

証明書の例外の警告が発生しないようにするには、完全修飾ドメイン名 (FQDN) を使用し、サーバにアクセスする必要があります。

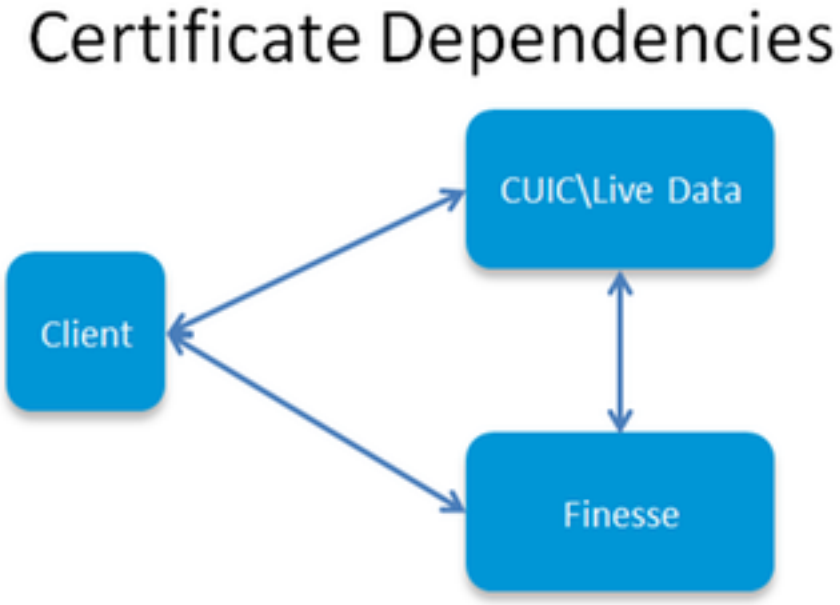
証明書の依存関係 :

==========

As

Finesse エージェントとスーパーバイザは CUIC ガジェットをレポート目的で利用します。これらのサーバ間の HTTPS 通信の証明書依存関係を維持するために、これらのサーバのルート証明を次の順序でアップロードする必要もあります。

- CUIC サーバのルート証明書を Finesse プライマリ サーバにアップロードする
- Finesse のルート\中間証明書を CUIC プライマリ サーバにアップロードする



a) CUIC サーバのルート証明書を Finesse プライマリ サーバにアップロードする

----

1. プライマリ Finesse サーバで、下で指定された URL を使用して [Cisco Unified Communications Operating System Administration] ページを開き、インストール プロセスで作成

された OS 管理者アカウントでサインインします

https://hostname of primary Finesse server/cmplatform

2. プライマリ CUIC ルート証明書をアップロードします。
a) [Security] > [Certificate Management] > [Upload Certificate] を選択します。
b) [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
c) [Upload File] フィールドで、[Browse] をクリックし、ルート証明書ファイルを参照します。
d) [Upload File] をクリックします。

3. セカンダリ CUIC ルート証明書をアップロードします。

a) [Security] > [Certificate Management] > [Upload Certificate] を選択します。
b) [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
c) [Upload File] フィールドで、[Browse] をクリックし、ルート証明書ファイルを参照します。
d) [Upload File] をクリックします。

注：
tomcat-trust ストアはプライマリおよびセカンダリ サーバ間で複製されるので、CUIC ルート証明書をセカンダリ Finesse サーバにアップロードする必要はありません。

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、コマンド「utils system restart」を入力してサーバを再起動します。

b) Finesse のルート\中間証明書を CUIC プライマリ サーバにアップロードする

---

1. プライマリ CUIC サーバで、下で指定された URL を使用して [Cisco Unified Communications Operating System Administration] ページを開き、インストール プロセスで作成された OS 管理者アカウントでサインインします
https://hostname of primary CUIC server/cmplatform

2. プライマリ Finesse ルート証明書をアップロードします。
a) [Security] > [Certificate Management] > [Upload Certificate] を選択します。
b) [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
c) [Upload File] フィールドで、[Browse] をクリックし、ルート証明書ファイルを参照します。
d) [Upload File] をクリックします。

３．プライマリ Finesse 中間証明書のアップロード

i) [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
ii) [Root Certificate] フィールドに、前の手順でアップロードしたルート証明書の名前を入力します。
iii) [Upload File] フィールドで [Browse] をクリックし、中間証明書ファイルを参照します。
iv) [Upload File] をクリックします。

4. プライマリの稼働中データ サーバで、セカンダリ Finesse ルート\中間証明書について、同じステップ (2 および 3) を実行します。

注：

tomcat-trust ストアはプライマリおよびセカンダリ サーバ間で複製されるので、Finesse ルート /中間証明書をセカンダリ CUIC サーバにアップロードする必要はありません。

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、コマンド「utils system restart」を入力してサーバを再起動します。