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： 生成するおよびダウンロード証明書署名要求（CSR）](#)
[ステップ 2： 認証局からのルート、中間物（該当する場合）およびアプリケーション 認証を得て下さい](#)
[ステップ 3： サーバへのアップロード認証](#)
[技巧サーバ:](#)
[CUIC サーバ:](#)
a) [技巧プライマリ サーバのアップロード CUIC サーバ原証明](#)
b) [CUIC プライマリ サーバのアップロード技巧ルート\中間認証](#)
[Cisco サポート コミュニティ - 特集対話](#)

概要

HTTPS を技巧および Cisco Unified Intelligence Center（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 認証 セットアップは必要です。 デフォルトでこれらのサーバは使用するまたは顧客は認証局（CA）認証を手に入れ、インストールできます自己署名 certifcates 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 internaly 生成 することができます。

この資料は技巧および 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）認証を得、インストールするために手順を詳しく説明することを向けます。

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。

- Cisco パッケージ コンタクトセンター 企業（PCCE）
- Cisco Unified Intelligence Center（CUIC）
- Cisco Finesse
- CA証明

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。

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、クリアな（デフォルト）設定で作業を開始しています。 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

設定して技巧および Cisco Unified Intelligence Center （CUIC）サーバ

- 生成するおよびダウンロード証明書署名要求（CSR）。
- CSR を使用して認証局からのルート、中間物（該当する場合）およびアプリケーション 認証を得て下さい。
- サーバに認証をアップロードして下さい。

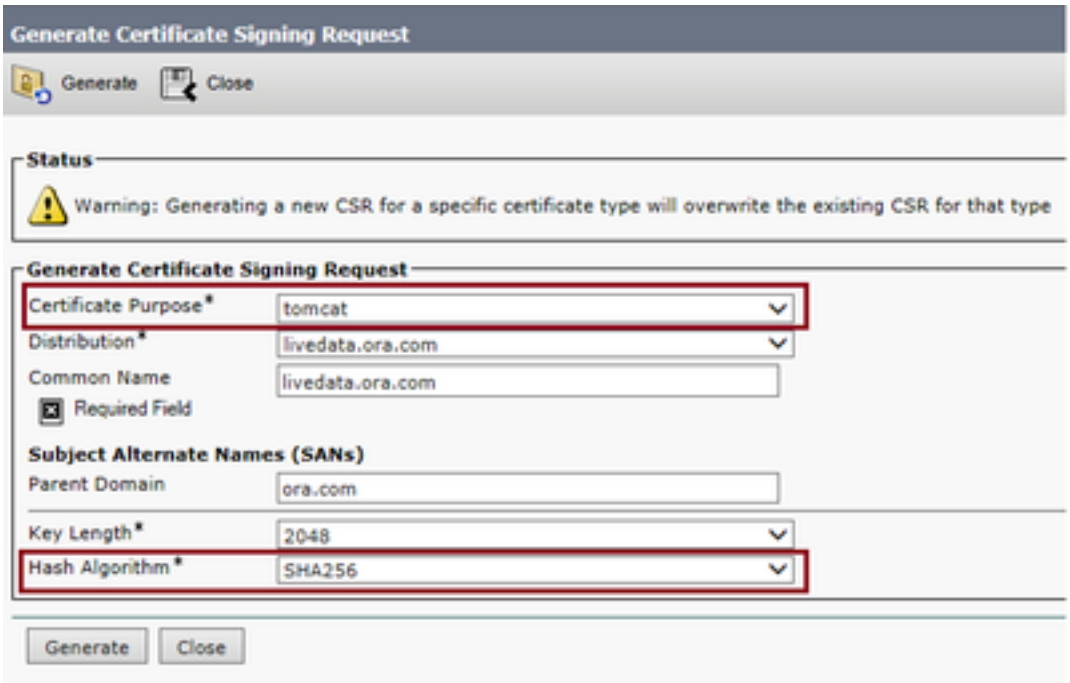
ステップ 1： 生成するおよびダウンロード証明書署名要求（CSR）

---

1. CSR を生成し、ダウンロードするために下記のステップは技巧および CUIC サーバのため同じです。

2. Cisco Unified Communications オペレーティング システム管理 ページを下記の示された URL を使用して開き、インストールプロセスの間に作成される 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/cmplatform の https://hostname

3. 生成する 証明書署名要求（CSR）

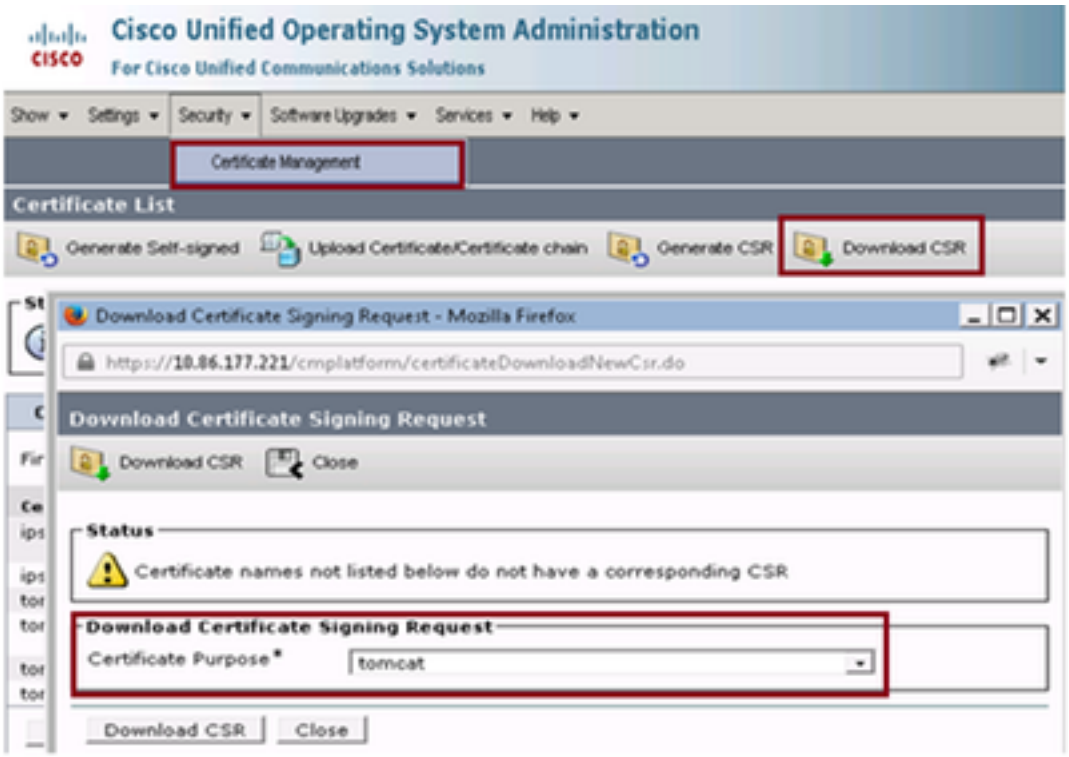


a) > Certificate Management > 生成する CSR を『Security』 を選択 して下さい。

b) 認証目的名前ドロップダウン 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) CSR を『Generate』 をクリック して下さい。

4. 証明書署名要求（CSR）のダウンロード



a) > Certificate Management > ダウンロード CSR を『Security』 を選択 して下さい。
b) 証明書名ドロップダウン リストから、Tomcat を選択して下さい。
c) [Download CSR] をクリックします。

注：

認証局のための CSR を得るために secondory サーバ/cmplatform の URL 「https://hostname」を使用して secondory サーバの前述のステップを実行して下さい。

ステップ 2： 認証局からのルート、中間物（該当する場合）およびアプリケーション 認証を得て下さい

---

1. VeriSign、Thawte、GeoTrust 先祖などのようなサード パーティ Certifcate 機関（CA）にプライマリおよび secondory サーバ証明書署名要求（CSR）情報を提供します

2. Certifcate 機関（CA）から 1 つはプライマリおよび secondory サーバのための次の証明書 チェーンを受け取る必要があります。

- **技巧サーバ:** ルート、中間物およびアプリケーション 認証
- **CUIC サーバ:** ルートおよびアプリケーション 認証

ステップ 3： サーバへのアップロード認証

このセクションは方法で技巧および Cisco Unified Intelligence Center （CUIC）サーバ

技巧サーバ:

==========

1. **アップロード プライマリ技巧サーバルート 認証**

a) 選り抜きプライマリ サーバ Cisco Unified Communications オペレーティング システム管理 ページ

セキュリティ > Certificate Management > アップロード認証。

b) 証明書名ドロップダウン 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、原証明 ファイルに『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. **プライマリ技巧サーバ中間物認証をアップロードして下さい。**

a) 証明書名ドロップダウン リストから、Tomcat 信頼を選択して下さい。
b) ファイルされる原証明では前の手順でアップロードした原証明の名前を入力して下さい。

ルート/公共認証がインストールされたときに生成されるこれは .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 > ClickFind にナビゲート して下さい。 認証リスト .pem ファイル名で Tomcat 信頼に対してリストされていて下さい。
c) アップ ロード File フィールドで、中間証明書ファイルに『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技巧サーバルートをアップロードするためにプライマリおよび secondory サーバの間で複製されると同時に必要ではないですまたはセカンダリへの中間物認証はサーバをうまく解決します。

3.アップロード プライマリ技巧サーバアプリケーション 認証。

a) 証明書名ドロップダウン リストから、Tomcat を選択して下さい。

b) 原証明 フィールドでは、前のステップでアップ ロードした中間認証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 証明書ファイルに『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. **secondory 技巧サーバルートおよび中間物認証をアップロードして下さい。**

a) 認証のための secondory サーバで (1) および (2) の同じステップに前述のように従って下さい

注：
Tomcat 信頼ストアが' secondory 技巧サーバルートをアップロードするためにプライマリおよび secondory サーバの間で複製されると同時に必要ではないですまたはプライマリへの中間物認証はサーバをうまく解決します。

5.アップロード secondory 技巧サーバアプリケーション 認証。

a)

6. **サーバを再起動して下さい**

プライマリおよび secondory 技巧サーバの 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」を入力して下さい。

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) 認証**

a) 選り抜きプライマリ サーバ Cisco Unified Communications オペレーティング システム管理 ページ

セキュリティ > Certificate Management > アップロード認証。

b) 証明書名ドロップダウン 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、原証明 ファイルに『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 信頼ストアがセカンダリ CUIC サーバにプライマリ CUIC サーバルート 認証をアップロードするためにプライマリおよび secondory サーバの間で複製されると同時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) 認証**
a) 証明書名ドロップダウン リストから、Tomcat を選択して下さい。
b) 原証明 フィールドでは、前のステップでアップ ロードした原証明の名前を入力して下さい。

ルート/公共認証がインストールされたときに生成されるこれは .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 > ClickFind にナビゲート して下さい。 認証リスト .pem ファイル名で Tomcat 信頼に対してリストされていて下さい。

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) 証明書ファイルに『Browse』 をクリック し、参照して下さい。
d) ファイルを『Upload』 をクリック して下さい

3. **cuic secondory サーバルート (パブリック) 認証をアップロードして下さい**

a) secondory cuic サーバで原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 CUIC サーバに secondory CUIc サーバルート 認証をアップロードするためにプライマリおよび secondory サーバの間で複製されると同時に必要ではないです。

4.Upload cuic secondory サーバアプリケーション (プライマリ) 認証。
a) 自身の認証のための secondory 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。

6. **サーバを再起動して下さい**

プライマリおよび secondory 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」を入力して下さい。

注：

警告する認証 例外を避けることは完全修飾ドメイン名（FQDN）名前を使用してサーバにアクセスする必要があります。

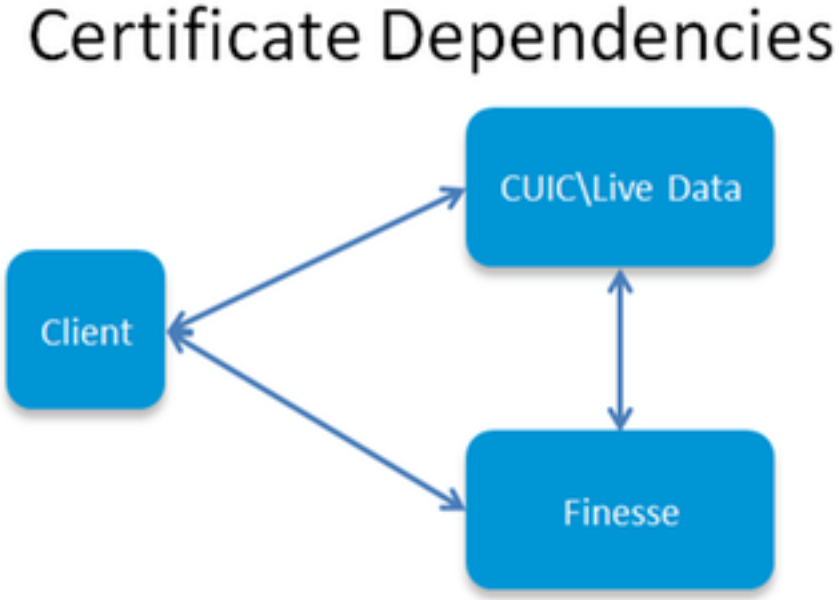
認証 依存関係

==========

ように

技巧エージェントおよびスーパバイザは CUIC 小道具報告目的のために 1 をこれらのサーバ間の HTTPS 通信のための認証 依存関係を維持する以下の順のこれらのサーバの原証明を同様にアップロードしなければなりません

- 技巧プライマリ サーブの CUIC サーバ原証明をアップロードして下さい
- CUIC プライマリ サーバの技巧ルート\中間認証をアップロードして下さい



a) 技巧プライマリ サーバの CUIC サーバ原証明をアップロードして下さい

1.On 下記の示された URL を使用して 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 provcess の間に作成される OS 管理者アカウントと署名し、

プライマリ技巧サーバ/cmplatform の https://hostname

2.Upload プライマリ CUIC 原証明。

a) > Certificate Management > アップロード認証を『Security』 を選択 して下さい。
b) 証明書名ドロップダウン 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、原証明 ファイルに『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 Secondory CUIC 原証明。

a) > Certificate Management > アップロード認証を『Security』 を選択 して下さい。
b) 証明書名ドロップダウン 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、原証明 ファイルに『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 信頼ストアがセカンダリに CUIC 原証明をアップロードするためにプライマリおよび secondory サーバの間で複製されると同時に必要うまく解決しますサーバをではないです。

4.プライマリおよび secondory 技巧サーバの 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」を入力して下さい。

b) CUIC プライマリ サーバの技巧ルート\中間認証をアップロードして下さい

1.On 下記の示された URL を使用してプライマリ CUIC サーバ開いた 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 provcess の間に作成される 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.Upload プライマリ技巧原証明。
a) > Certificate Management > アップロード認証を『Security』 を選択 して下さい。
b) 証明書名ドロップダウン 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、原証明 ファイルに『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.プライマリ技巧中間物認証をアップロードして下さい

i)
ii) ファイルされる原証明では前の手順でアップロードした原証明の名前を入力して下さい。
iii) アップ ロード File フィールドで、中間証明書ファイルに『Browse』 をクリック し、参照して下さい。
iv) ファイルを『Upload』 をクリック して下さい。

4. 同じステップを実行して下さい (プライマリ ライブ データ サーバの secondory 技巧ルート\中間認証のための 2 及び 3) 。

注：

Tomcat 信頼ストアがセカンダリ CUIC サーバに技巧ルート /intermediate 認証をアップロードするためにプライマリおよび secondory サーバの間で複製されると同時に必要ではないです。

5. プライマリおよび secondory 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」を入力して下さい。