



# SSL Certificate Management

---

この章では、Admin Portal の SSL Certificate Management オプションについて説明します。

このオプションでは、自己署名 SSL 証明書の生成、その証明書の Certificate Signing Request (CSR; 証明書署名要求) の作成、および証明書のインポートとアップロードを行うことができます。

## SSL 証明書プロセスの概要

Cisco Unified Mobility Advantage Proxy Server には、Verisign が発行する署名付き SSL 証明書が必要です。

Cisco Unified Mobility Advantage Enterprise Server には、Verisign が発行する署名付き SSL 証明書を推奨しますが、必須ではありません。Enterprise Server では、署名付き SSL 証明書の代わりに自己署名証明書を使用できます。ただし、自己署名証明書を使用した場合、エンドユーザに「Certificate is Untrusted.」という警告が Cisco Unified Mobile Communicator User Portal で表示されます。

インストール時に Configuration Wizard を使用して SSL 証明書プロセスを実行することを推奨します。詳細については、『Cisco Unified Mobility Advantage Installation Guide』を参照してください。

## 新しい証明書の生成



### 注意

このプロセスを開始する前に、Node Manager Server と Managed Server をシャットダウンしてください。プロセスの完了後に、これらのサーバを再起動します。

Admin Portal を使用して新しい証明書を作成するには、次の手順を実行します。

### 手順

**ステップ 1** SSL Certificate Management > Generate New Certificate を選択します。

**ステップ 2** 表 8-1 に示す情報を入力します。

表 8-1 Generate Certificate Signing Request (CSR) 画面

フィールド	定義
Server Name	証明書を生成するサーバ (Cisco Unified Mobility Advantage Proxy Server または Cisco Unified Mobility Advantage Enterprise Server) の完全修飾ホスト名を入力します。
Department Name	Cisco Unified Mobility Advantage を使用する部署の名前を入力します (1 つの部署に限定する場合)。
Company Name	社名を入力します。
City	部署または会社の所在地の市を入力します。
State	市が位置している都道府県 (米国では州) を入力します。フルネームをスペルアウトする必要があります。例: California (CA は不可)
Country Code	会社の所在地の国を表す 2 文字のコードを入力します。例: US (USA は不可)
Password	この SSL 証明書ファイルに割り当てるパスワードを入力します。パスワードの長さは、6 文字以上にする必要があります。

**ステップ 3** Submit をクリックします。

Cisco Unified Mobility Advantage Enterprise Server は一時的なファイル名を持つ証明書ストア ファイルを作成し、Admin Portal にリンクを表示します。このリンクから証明書ストア ファイルをローカル コンピュータにダウンロードできます。

**ステップ 4** リンクをクリックし、Admin Portal からローカル コンピュータに証明書ストア ファイルをダウンロードします。

このファイルを任意の場所に保存します。証明書ストア ファイルのデフォルトのファイル名は、**orative.keystore** です。



### 注意

証明書ストア ファイルの保存場所とパスワードは、忘れないようにしてください。次の項で説明する手順で、これらの情報が必要になります。

## 証明書署名要求の取得

Retrieve CSR を使用すると、前の項 P.8-2 の「新しい証明書の生成」で生成した証明書ストア ファイルを使用して、証明書署名要求 (CSR) を取得できます。

CSR を取得するには、次の手順を実行します。

### 手順

**ステップ 1** SSL Certificate Utilities > Retrieve CSR を選択します。

**ステップ 2** 表 8-2 に示す情報を入力します。

表 8-2 Retrieve CSR

フィールド	定義
Certificate File	前の手順でダウンロードした <b>keystore</b> ファイルを見つけて表示します。
Password	ファイルの生成時に割り当てたパスワードを入力します。

**ステップ 3** **Submit** をクリックします。

証明書署名要求 (CSR) のテキストが表示されます。

**ステップ 4** ステップ 3 で生成された CSR テキストをコピーし、Verisign の Web サイト (www.verisign.com) にアクセスし、このテキストのコピーを送信して SSL 証明書を要求します。



### 注意

Verisign からの応答があるまで待機する必要があります。応答まで 1 時間から数週間かかる場合があります。

## SSL 証明書のインポート

CSR を Verisign に送信すると、Verisign から SSL 証明書が交付されます。この SSL 証明書を証明書ストア ファイルにインポートする必要があります。

Verisign から交付される証明書によっては、ルート証明書へのチェーンを完成するための中間証明書が必要になる場合があります。このような場合、中間証明書を証明書ストア ファイルにインポートしてから、最終的な SSL 証明書をインポートする必要があります。

Verisign の中間証明書は、次のサイトから入手できます。

<http://www.verisign.com/support/install/intermediate.html>

SSL 証明書をインポートするには、次の手順を実行します。

### 手順

**ステップ 1** SSL Certificate Utilities > Import SSL Certificate を選択します。



**ステップ 2** 表 8-3 に示す情報を入力します。

Proxy Server 用の署名付き証明書をインポートする場合は、Proxy Server の情報を入力します。Enterprise Server 用の署名付き証明書をインポートする場合は、Enterprise Server の情報を入力します。

表 8-3 Import SSL Certificate

フィールド	定義
Certificate File	証明書ストア ファイルの名前と保存場所を入力するか、 <b>Browse</b> をクリックしてローカル Admin コンピュータ上で証明書ストア ファイルを見つけます。
Password	ファイルの生成時に割り当てたパスワードを入力します。
Intermediate Certificate?	中間証明書ファイルがある場合は、 <b>True</b> を選択します。 最終的な証明書ファイルがある場合は、 <b>False</b> を選択します。

表 8-3 Import SSL Certificate (続き)

フィールド	定義
Certificate	<p><b>中間証明書ファイルがある場合：</b></p> <ol style="list-style-type: none"> <li>1. 中間証明書のテキストをテキスト ファイルにコピー アンド ペーストします。</li> </ol> <p> (注) ---BEGIN CERTIFICATE--- と ---END CERTIFICATE--- を必ず挿入してください。</p> <ol style="list-style-type: none"> <li>2. ステップ 1 で貼り付けた中間証明書のテキストの下に、最終的な証明書のテキストを貼り付けます。</li> </ol> <p> (注) ---BEGIN CERTIFICATE--- と ---END CERTIFICATE--- を必ず挿入してください。2つの証明書の間に、空白行を入れないようにしてください。</p> <ol style="list-style-type: none"> <li>3. このテキスト ファイルの内容を Certificate フィールドに貼り付けます。</li> </ol> <p><b>最終的な証明書ファイルがある場合：</b></p> <p>最終的な証明書を Certificate フィールドにコピー アンド ペーストします。---BEGIN CERTIFICATE--- と ---END CERTIFICATE--- を必ず挿入してください。</p>

**ステップ 3** **Submit** をクリックします。

更新された証明書ストア ファイルをダウンロードするためのリンクを受信します。

**ステップ 4** **Managed Server** を再起動します。

## SSL 証明書のアップロード

SSL 証明書ファイルをアップロードするには、次の手順を実行します。

**ステップ 1** SSL Certificate Utilities > Upload Certificate を選択します。

**ステップ 2** 表 8-4 に示す情報を入力します。

表 8-4 Upload Certificate

フィールド	定義
Certificate File	SSL 証明書ファイルの名前と保存場所を入力するか、 <b>Browse</b> をクリックしてローカル Admin コンピュータ上で SSL 証明書ファイルを見つけます。
Password	ファイルの生成時に割り当てたパスワードを入力します。

**ステップ 3** Submit をクリックします。

## Proxy Server 証明書ファイルの設定

この項では、SSL 証明書を Proxy Server にインポートして Proxy Server 設定値を設定する方法について説明します。

初めて Proxy Server をインストールするときに、Configuration Wizard が証明書ストア ファイルを要求し、証明書ストア ファイルを **\$CUMA.ROOT/conf/orative.keystore** にコピーします。Admin Portal で Proxy Server 設定の設定値を修正して、Proxy Server 証明書ストア ファイルを **\$CUMA.ROOT/conf/orative.keystore** に設定する必要があります。

新しい SSL 証明書ファイルをインストールする場合は、**\$CUMA.ROOT/conf/new.keystore** にある keystore ファイルを Proxy Server マシンにインポートします。その後、Admin Portal で Proxy Server Configuration Keystore File フィールドが次の値に設定されるように修正します。

**/opt/cisco/conf/new.keystore**

Keystore Password フィールドに適切なパスワードを設定します。

Proxy Server 設定値を設定するには、次の手順を実行します。

### 手順

**ステップ 1** 新しい Proxy 証明書ストア ファイルを **\$CUMA.ROOT/conf** にインポートします。**\$CUMA.ROOT** は、Cisco Unified Mobility Advantage Proxy Server がインストールされている場所です。

**ステップ 2** Admin Portal で、**Proxy Configuration > Listen Ports** を選択します。

**ステップ 3** 新しい keystore ファイルの保存場所およびファイル名と一致するように、Keystore File フィールドを修正します。

**ステップ 4** 新しい keystore パスワードと一致するように、Keystore Password フィールドを修正します。