CUCM の混合モード クラスタでの Cisco IP Phone の保護

Document ID: 113333

Updated: 2011 年 11 月 28 日

関連製品

- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7960G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7961G
- + 詳細情報

目次

概要

このドキュメントでは、セキュア モードの IP Phone 1 台を、IP Phone にインストールされている証明書信頼リスト（CTL）ファイルを手動操作することなく、移動元 Cisco Unified Communication Manager（CUCM）クラスタから移動先 CUCM クラスタへ移動する手順について説明します。

注: この手順は次の条件には依存しません。

1. 電話で使用されているシグナリング プロトコル。 送信元クラスタと宛先クラスタのシグナ

リング プロトコルは、特定の IP Phone については同じままであると仮定しています。
2. 電話機のモデル（ただし Cisco 7940/7960 モデルを除く。7940/7960 の電話にはビルトインの MIC がないため、認証文字列を配置するためのエンド ユーザの介入が必要なため）。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Unified Communications Manager 7.x に基づくものです。

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。 ネットワークが稼働中の場合は、コマンド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。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

証明書信頼リスト

CUCM クラスタ内のすべてのサーバは、自己署名証明書を生成します。 電話は、自身の証明書（次の 2 つのタイプのうちいずれか）を取得します。

1. 製造元でインストールされた証明書（新しい電話を購入するときにシスコから提供されます）。
2. Cisco Authority Proxy Function で処理される、ローカルで有効な証明書。

CTL は、電話が信頼できる CUCM クラスタ内のすべてのサーバからの自己署名証明書のリストです。 CTL は TFTP サーバ上に格納されており、IP Phone へ送信されます。

デバイス、ファイル、およびシグナリング認証は CTL ファイルの作成を利用しています。CTL ファイルは、USB ポートを備えている単一の Windows ワークステーションまたはサーバ上に Cisco CTL Client をインストールおよび設定するときに作成されます。

CTL ファイルには各サーバのサーバ証明書、公開鍵、シリアル番号、署名、発行者名、サブジェクト名、サーバ機能、DNS 名、および IP アドレスが含まれています。 CTL ファイルにファイアウォールを設定すると、セキュアな Cisco Unified Communications Manager システムの一部として Cisco ASA Firewall を保護することができます。 Cisco CTL Client は、ファイアウォール証明書を *CCM* 証明書として表示します。 Cisco Unified Communications Manager Administration は eToken を使用して、Cisco CTL Client と Cisco CTL Provider 間の TLS 接続を認証します。

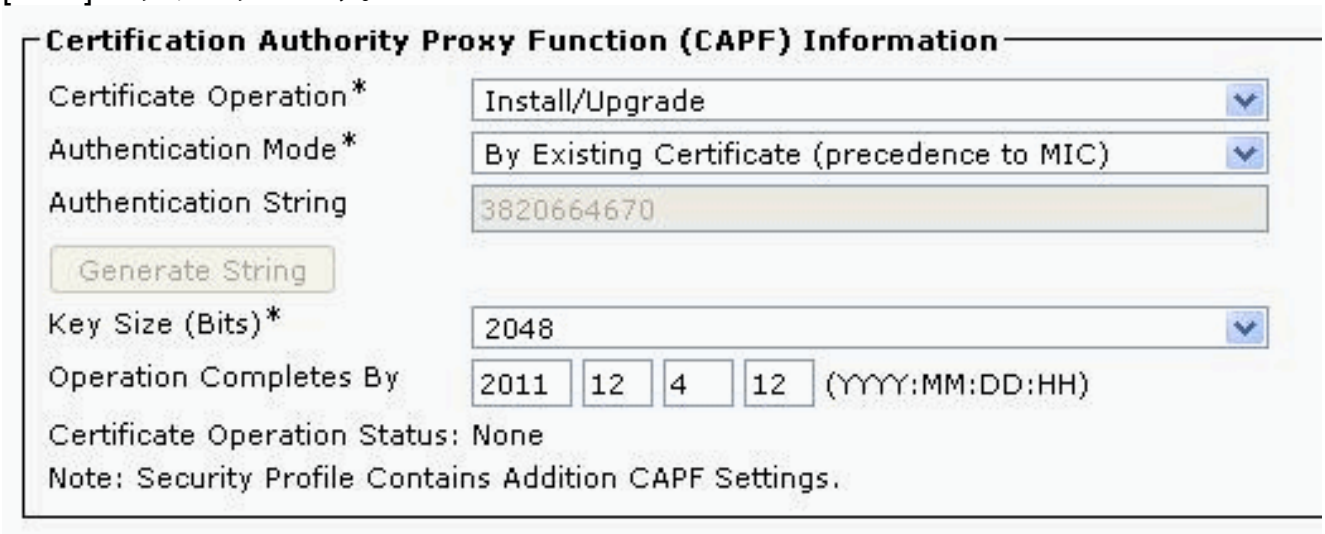
CUCM バージョン 8.X 以降では、CTL ファイルが作成されていなくても、IP Phone はデフォルトで CTL ファイルを要求します。 CTL ファイルは必須のものではなく、 CUCM 8.x に付随している新しいセキュリティ機能の一部です。 詳細については、『Cisco CTL Client の設定』を参照してください。

IP Phone を保護する方法

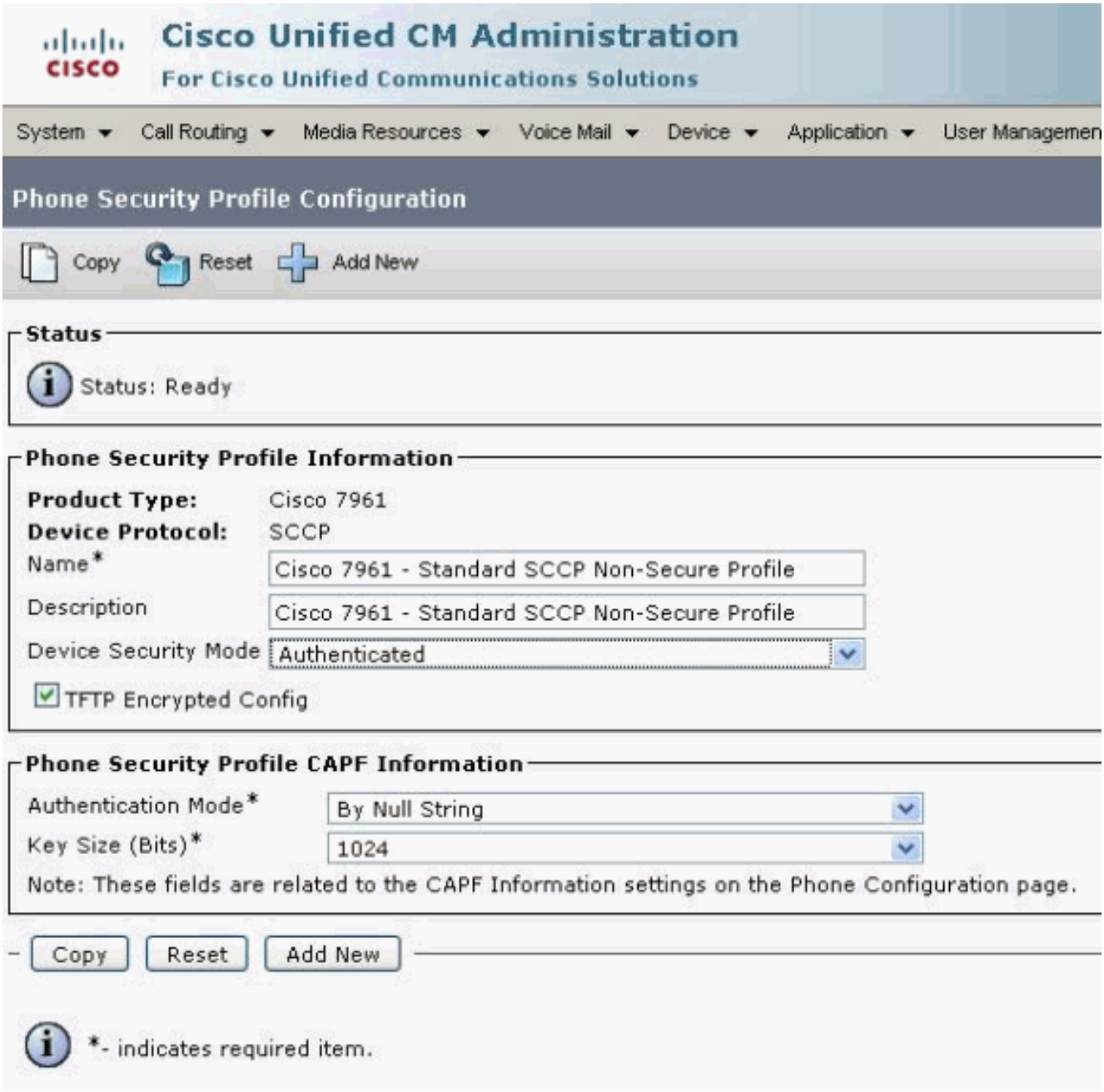
電話が、既存のものを削除せずに任意のクラスタから CTL ファイルを受け取るようにするには、各クラスタの CTL ファイルが eToken の同じ共有セットによって署名されていることが必要です。 つまり、クラスタごとに 1 つの CTL ファイルを作成し、そのすべての CTL ファイルに同じ eToken で署名する必要があります。 また、電話が集中型 TFTP サーバを信頼するためには、各 CTL ファイルに集中型 TFTP サーバを追加する必要があります。

IP Phone のセキュリティ プロパティを設定するには、次の手順を実行します。

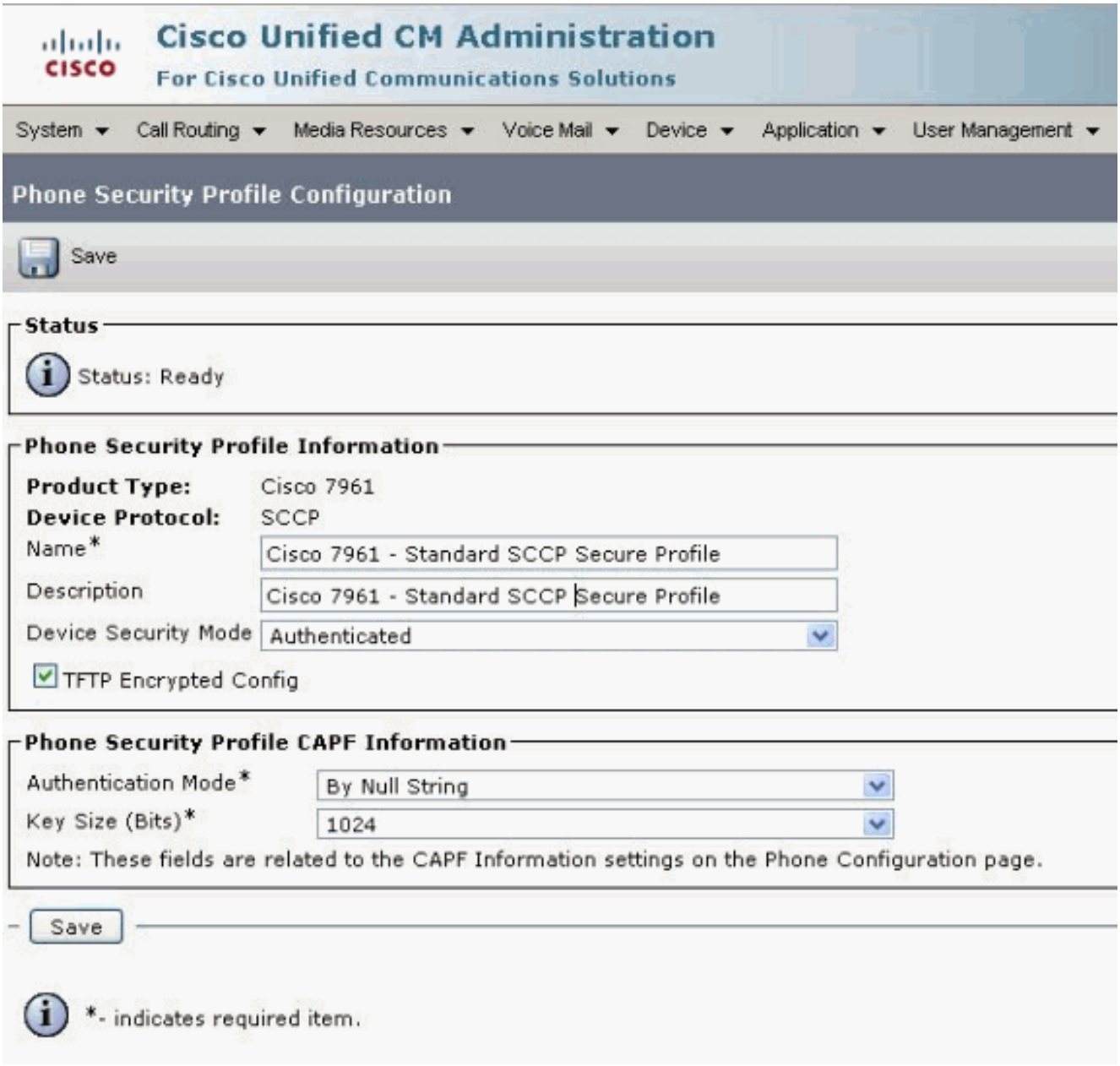
1. デバイス セキュリティ プロファイルを設定します。 IP Phone の設定ページでドロップダウン リストの中に適切なデバイス セキュリティ プロファイルがない場合は、デフォルトの [Standard Non-Secure Profile] のままにします。
2. IP Phone が、宛先 CUCM クラスタによって署名されている新しい LSC を取得するには、[Certification Authority Proxy Function (CAPF) Information] を設定します。これは CUCM の電話の設定ページで行います。 次のように、値をドロップダウン メニューから選択し、[Save] をクリックします。



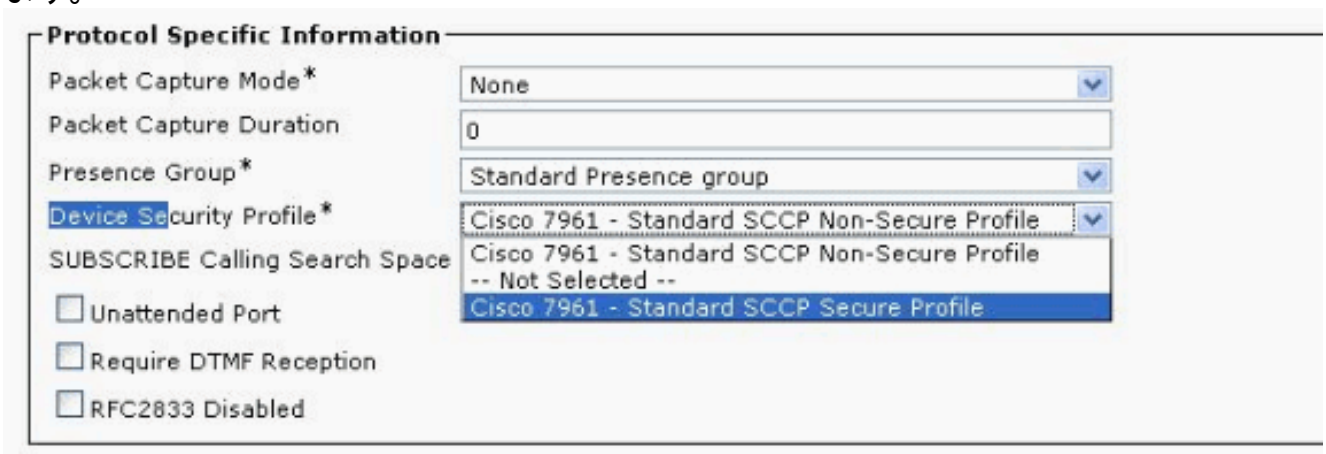
3. 新しく作成したデバイス セキュリティ プロファイルを設定します。[System] > [Security Profile] > [Phone Security Profile] を選択します。[Find] をクリックします。電話のタイプを選択し、詳細を入力します。



[Copy] をクリックします。ここで、次に示すように設定して [Save] します。



4. IP Phone の設定ページで、正しい [Device Security Mode] が設定されていることを再確認します。



5. IP Phone を再起動します。
6. 電話は宛先クラスタから新しい CTL ファイルをダウンロードし、宛先クラスタで署名された LSC を取得するはずです。
7. 電話は、デバイス セキュリティ プロファイルで設定されたセキュリティ モードで稼動します。

関連情報

- シスコ セキュリティ アドバイザリ： Cisco Unified Communications Manager CTL プロバイダー ヒープ オーバーフロー
- IP Phone のセキュリティと CTL (証明書信頼リスト)
- 音声に関する技術サポート
- 音声とユニファイド コミュニケーションに関する製品サポート
- Cisco IP Telephony のトラブルシューティング
- テクニカルサポートとドキュメント - Cisco Systems

Cisco サポート コミュニティ - 特集対話

Cisco サポート コミュニティでは、フォーラムに参加して情報交換することができます。

このドキュメントで使用されている表記法の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Updated: 2011 年 11 月 28 日
Document ID: 113333