



Certificate Authority Proxy Function

- [認証局プロキシ機能の概要, on page 1](#)
- [認証局プロキシ機能の設定タスクフロー, on page 3](#)
- [認証局プロキシ機能の管理タスクフロー, on page 11](#)
- [CAPF システムの連携動作と制限事項, on page 14](#)

認証局プロキシ機能の概要

認証局プロキシ機能（CAPF）は、ローカルで重要な証明書（LSC）を発行し、エンドポイントを認証します。

CAPF サービスは Unified Communications Manager 上で実行され、次のタスクを実行します。

- サポートされる Cisco Unified IP Phone に LSC を発行します。
- 混合モード中に電話機を認証します。
- 電話機用の既存の LSCs をアップグレードします。
- 表示およびトラブルシューティングを行うために電話の証明書を取得する。

CAPF サービス証明書

CAPF サービスは Unified Communications Manager のインストールで自動的にインストールされ、CAPF 固有のシステム証明書が生成されます。

次のモードで動作するように CAPF を設定することができます。

Table 1: CAPF 実行モード

モード	説明
Cisco Authority Proxy Function	デフォルトでは、Unified Communications Manager 上の CAPF サービスが、CAPF サービスで署名された LSC を発行します。

モード	説明
オンライン CA	外部オンライン CA が「電話用 LSC」として署名している場合は、このオプションを使用します。CAPF サービスは、自動的に外部 CA に接続されます。CA 署名 LSC は、証明書署名要求 (CSR) が送信されると自動的に返されます。
オフライン CA	外部オンライン CA が「電話用 LSC」として署名している場合は、このオプションを使用します。SC を手動でダウンロードして CA に提出し、CA 署名の証明書の準備ができてからそれらをアップロードします。 Note LSC の署名にサードパーティ CA を使用する場合は、[オフライン CA (Offline CA)] ではなく [オンライン CA (Online CA)] オプションをお勧めします。[オンライン CA (Online CA)] は自動化されていて、はるかに速く、問題が発生する可能性が低いです。

LSC を生成する前に、次のものを用意していることを確認してください。

- Unified Communications Manager リリース 12.5 以降。
- 証明書に CAPF を使用するエンドポイント (Cisco Unified IP Phone および Jabber を含む)。
- CA が設定された Microsoft Windows Server 2012 および 2016。
- ドメインネームサービス (DNS)

前提条件として、電話機を認証する方法も決定します。

LSC を生成する前に、CA ルート証明書と HTTPS 証明書を必要な信頼ストアにアップロードします。インターネットインフォメーションサービス (IIS) は、HTTPS 証明書をホストします。セキュア SIP 接続では、HTTPS 証明書は CAPF-トラストを通過し、CA ルート証明書は CAPF 信頼と Unified Communications Manager 信頼の両方を通過します。CA ルート証明書は、証明書署名要求 (CSRs) への署名に使用されます。

次に、さまざまな証明書をアップロードするシナリオを示します。

Table 2: 証明書のアップロードシナリオ

シナリオ	アクション
CA ルートおよび HTTPS 証明書は同じです。	CA ルート証明書をアップロードする。
CA ルート証明書と HTTPS の証明書は異なり、HTTPS 証明書は同じ CA ルート証明書によって発行されます。	CA ルート証明書をアップロードする。

シナリオ	アクション
CAルート証明書は、異なる中間 CA 証明書と HTTPS 証明書を発行します。	CA ルート証明書をアップロードする。
同じ CA ルート証明書が、異なる CA ルート証明書と HTTPS 証明書を発行します。	CA ルートおよび HTTPS 証明書をアップロードする。



Note 複数の証明書を同時に生成すると、コールプロセスが中断される可能性があるため、スケジュールされたメンテナンス期間中に CAPF を使用することをお勧めします。

認証局プロキシ機能の設定タスクフロー

次のタスクを実行して、証明機関プロキシ機能 (CAPF) サービスがエンドポイント用 LSCs を発行するように設定します。

Procedure

	Command or Action	Purpose
Step 1	サードパーティの認証局のルート証明書のアップロード	LSCにサードパーティのCA署名を適用する場合は、CA ルート証明書チェーンをCAPF 信頼ストアにアップロードします。その他の場合は、このタスクをスキップします。
Step 2	認証局 (CA) ルート証明書のアップロード, on page 5	CA ルート証明書を Unified Communications Manager 信頼ストアにアップロードします。
Step 3	オンライン認証局の設定, on page 5	電話機の LSC 証明書を生成するには、次の手順を使用します。
Step 4	オフライン認証局の設定の設定	オフライン CA を使用して電話機 LSC 証明書を生成するには、次の手順を使用します。
Step 5	CAPF サービスをアクティブ化または再起動する	CAPF システム設定を構成した後、必須の CAPF サービスをアクティブにします。

	Command or Action	Purpose
Step 6	次のいずれかの手順を使用して、Unified Communications Manager で CAPF 設定を構成します。 <ul style="list-style-type: none"> ユニバーサル デバイス テンプレートでの CAPD 設定の設定, on page 8 バルク Admin による CAPF 設定の更新, on page 9 電話機の CAPF 設定の設定, on page 10 	次のオプションのいずれかを使用して、CAPF 設定を電話機の設定に追加します。 <ul style="list-style-type: none"> まだ LDAP ディレクトリを同期していない場合、CAPF 設定をユニバーサルデバイステンプレートに追加し、初期 LDAP 同期を使用して設定を適用します。 バルク管理ツールを使用すると、1回の操作で多数の電話機に CAPF 設定を適用できます。 CAPF 設定を電話機ごとに適用することができます。
Step 7	キープアライブ タイマーの設定, on page 11	ファイアウォールがタイムアウトしないように、CAPF エンドポイント接続のキープアライブ値を設定します。デフォルト値は 15 分です。

サードパーティの認証局のルート証明書のアップロード

CA ルート証明書を CAPF 信頼ストアと Unified Communications Manager 信頼ストアにアップロードし、外部 CA を使用して LSC 証明書に署名します。



Note LSC の署名にサードパーティ CA を使用しない場合は、このタスクをスキップします。

Procedure

- Step 1** [Cisco Unified OSの管理 (Cisco Unified OS Administration)] から、以下を選択します。[セキュリティ (Security)] > [証明書の管理 (Certificate Management)]。
- Step 2** [Upload Certificate/Certificate chain] をクリックします。
- Step 3** [証明書の目的 (Certificate Purpose)] ドロップダウンリストで、[CAPF 信頼 (CAPF-trust)] を選択します。
- Step 4** 証明書の説明を [説明 (Description)] に入力します。たとえば、外部 LSC 署名 CA の証明書などです。
- Step 5** [参照 (Browse)] をクリックしてファイルに移動してから、[開く (Open)] をクリックします。
- Step 6** [アップロード (Upload)] をクリックします。

- Step 7** このタスクを繰り返して、証明書の目的で使用される発信者管理者の信頼に証明書をアップロードします。

認証局（CA）ルート証明書のアップロード

クラスタ全体の証明書をアップロードし、クラスタ内のすべてのサーバに配布します。

Procedure

- Step 1** [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。[セキュリティ（Security）]>[証明書の管理（Certificate Management）]。
- Step 2** [Upload Certificate/Certificate chain] をクリックします。
- Step 3** [証明書目的（Certificate Purpose）] ドロップダウンリストで、[CallManager 信頼（CallManager-trust）] を選択します。
- Step 4** 証明書の説明を [説明（Description）] に入力します。たとえば、外部 LSC 署名 CA の証明書などです。
- Step 5** [参照（Browse）] をクリックしてファイルに移動してから、[開く（Open）] をクリックします。
- Step 6** [アップロード（Upload）] をクリックします。

オンライン認証局の設定

オンライン CAPF を使用して電話機 LSC を生成するには、Unified Communications Manager でこの手順を使用します。



Note FIPS 対応モードは、オンライン CAPF および CAPFips3 をサポートしません。

Procedure

- Step 1** [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。[システム（System）]>[サービスパラメータ（Service Parameters）]。
- Step 2** [サーバ（Server）] ドロップダウンリストから、[Cisco Certificate Authority Proxy Function（アクティブ）（Cisco Certificate Authority Proxy Function (Active)）] サービスをアクティブにしたノードを選択します。
- Step 3** [サービス（Service）] ドロップダウンリストから、[Cisco Certificate Authority Proxy Function（アクティブ）（Cisco Certificate Authority Proxy Function (Active)）] を選択します。サービス名の横に「Active」と表示されることを確認します。

- Step 4** [**Certificate Issuer To Endpoint**] ドロップダウンリストから、[**Online CA**] を選択します。CA 署名付き証明書の場合、オンライン CA を使用することを推奨します。
- Step 5** [証明書の有効期間（日数）（**Duration Of Certificate Validity (in Days)**）] フィールドに、CAPF が発行した証明書が有効である日数を表す数値を、1 ～ 1825 の間で指定します。
- Step 6** [**Online CA Parameters**] セクションで、**Online CA** セクションへの接続を作成するために次のパラメータを設定します。
- [Online CA Hostname]: サブジェクト名または共通名 (CN) は、HTTPS 証明書の完全修飾ドメイン名 (FQDN) と同じである必要があります。
- Note** 設定されたホスト名は、Microsoft CA で実行されているインターネットインフォメーションサービス (IIS) によってホストされる HTTPs 証明書の共通名 (CN) と同じです。
- **Online CA Port**: オンライン CA のポート番号を入力します。たとえば、443。
 - **Online CA Template**: テンプレートの名前を入力します。Microsoft CA がテンプレートを作成します。
 - **Online CA Type**: デフォルトのタイプとして [Microsoft CA] を選択します。
 - **Online CA Username**: CA サーバのユーザ名を入力します。
 - **Online CA Password**: CA サーバのユーザ名のパスワードを入力します。
- Step 7** 残りの CAPF サービスパラメータを完了します。サービスパラメータのヘルプシステムを表示するには、パラメータ名をクリックします。
- Step 8** [保存 (Save)] をクリックします。
- Step 9** 変更内容を有効にするには、**Cisco Certificate Authority Proxy Function** を再起動します。Cisco Certificate Enrollment サービスが自動的に再起動します。

オフライン認証局の設定の設定

オフライン CA を使用して電話機 LSC 証明書を生成することを決定した場合は、次の高度なプロセスに従うことができます。



Note オフライン CA オプションを使用すると、オンライン CA よりも時間がかかり、手動による手順が非常に多くなります。証明書の生成および送信プロセス中に問題（たとえば、ネットワークの停止や電話機のリセットなど）が発生した場合は、プロセスを再起動する必要があります。

Procedure

- Step 1** サードパーティ認証局からルート証明書チェーンをダウンロードします。

- Step 2** ルート証明書チェーンを Unified Communications Manager 内の必要な信頼（CallManager 信頼 CAPF 信頼）にアップロードします。
- Step 3** [エンドポイントへの証明書の発行（Certificate Issue to Endpoint）] サービスパラメータを [オフライン CA（Offline CA）] に設定して、オフライン CA を使用するように Unified Communications Manager を設定します。
- Step 4** お使いの電話機の LSC 用に CSR を生成します。
- Step 5** 認証局に CSR を送信します。
- Step 6** CSR から署名付き証明書を取得します。

オフライン CA を使用して電話機 LSC を生成する方法の詳細な例については、「[CUCM サードパーティ CA 署名済み LSC の作成およびインポートの設定](#)」を参照してください。

CAPF サービスをアクティブ化または再起動する

CAPF システム設定を構成した後、必須の CAPF サービスをアクティブにします。CAPF サービスがすでにアクティブ化されている場合は、再起動します。

Procedure

- Step 1** Cisco Unified Serviceability から次を選択します。[ツール（Tools）] > [サービスアクティベーション（Service Activation）]。
- Step 2** [サーバ（Server）] ドロップダウン リストからパブリッシャ ノードを選択し、[移動（Go）] をクリックします。
- Step 3** [セキュリティサービス（Security Services）] ペインで、適用されるサービスを確認します。
- **Cisco Certificate Enrollment Service:** オンライン CA を使用している場合は、このサービスをオンにし、そうでない場合はオフのままにします。
 - **Cisco Certificate Authority Proxy Function:** オフになっている（非アクティブ）場合は、このサービスをオンにします。このサービスがすでにアクティブ化されている場合は、再起動します。
- Step 4** 設定を編集した場合は、[保存（Save）] をクリックします。
- Step 5** **Cisco Certificate Authority Proxy Function** サービスがすでにチェックされている場合は（アクティブ）、再起動します。
- a) [関連リンク（Related Links）] ドロップダウンリストから [コントロールセンター - 機能サービス（Control Center - Feature Services）] を選択し、[移動（Go）] をクリックします。
 - b) [セキュリティ設定（Security Settings）] ペインで、[Cisco Certificate Authority Proxy Function] サービスをオンにして、[再起動（Restart）] をクリックします。
- Step 6** 次の手順のいずれかを実行して、個々の電話機に対して CAPF 設定を構成します。
- a) [ユニバーサル デバイス テンプレートでの CAPD 設定の設定, on page 8](#)
 - b) [バルク Admin による CAPF 設定の更新, on page 9](#)

- c) [電話機の CAPF 設定の設定, on page 10](#)

ユニバーサル デバイス テンプレートでの CAPD 設定の設定

CAPF 設定をユニバーサルデバイステンプレートに設定するには、次の手順を実行します。テンプレートは、機能グループテンプレートの設定を使用して、LDAP ディレクトリ同期に適用することができます。テンプレートの CAPF 設定は、このテンプレートを使用する同期のすべてのデバイスに適用されます。



Note ユニバーサルデバイステンプレートは、まだ同期されていない LDAP ディレクトリにしか追加することができません。初期 LDAP 同期が発生した場合は、一括管理を使用して電話機を更新します。詳細については、[バルク Admin による CAPF 設定の更新, on page 9](#)を参照してください。

Procedure

- Step 1** [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[ユーザ管理 (User Management)] > [ユーザ/電話の追加 (User/Phone Add)] > [ユニバーサル デバイス テンプレート (Universal Device Template)]。
- Step 2** 次のいずれかを実行します。
- [検索 (Find)] をクリックして、既存のテンプレートを選択します。
 - [新規追加 (Add New)] をクリックします。
- Step 3** 認証局プロキシ機能 (CAPF) の設定領域の拡張
- Step 4** [証明書の操作 (Certificate Operation)] ドロップダウンリストで、[インストール/アップグレード (Install/Upgrade)] を選択します。
- Step 5** [認証モード (Authentication Mode)] ドロップダウンリストメニューから、デバイスを認証するためのオプションを選択します。
- Step 6** 認証文字列の使用を選択した場合は、テキストボックスに認証文字列を入力するか、[文字列の生成 ([文字列の生成])] をクリックして、システムによって文字列が生成されるようにします。
- Note** この文字列がデバイス上で設定されていない場合、認証は失敗します。
- Step 7** 残りのフィールドで、キー情報を設定します。フィールドの詳細については、オンラインヘルプを参照してください。
- Step 8** [保存 (Save)] をクリックします。
- Note** このテンプレートを使用するデバイスは、この手順で割り当てたのと同じ認証方式で設定されていることを確認してください。それ以外の場合、デバイス認証は失敗します。電話機の認証を設定する方法の詳細については、電話機のマニュアルを参照してください。

- Step 9** 次の手順に従って、このプロファイルを使用しているデバイスにテンプレートの設定を適用します。
- ユニバーサル デバイス テンプレートを [機能グループテンプレートの設定 (Feature Group Template Configuration)] に追加します。
 - 同期されていない LDAP ディレクトリ設定に機能グループテンプレートを追加します。
 - LDAP 同期を完了します。CAPF 設定は、同期されているすべてのデバイスに適用されます。

機能グループテンプレートと LDAP ディレクトリの設定の詳細については、[Cisco Unified Communications Manager システム設定ガイド](#)の「エンドユーザの設定」セクションを参照してください。

バルク Admin による CAPF 設定の更新

バルク管理の**電話機の更新**クエリを使用して、1回の操作で多くの既存の電話機に CAPF 設定と LSC 証明書を設定します。



Note まだ電話機をプロビジョニングしていない場合は、バルク管理の [電話機の挿入 (Insert phone)] メニューを使用して、CSV ファイルからの capf 設定で新しい電話機をプロビジョニングできます。CSV ファイルから電話機を挿入する方法の詳細については、[Cisco Unified Communications Manager 一括管理ガイド](#)の「電話機の挿入」セクションを参照してください。

電話機は、この手順で追加する文字列と認証方式と同じ文字列と認証方式で設定されていることを確認します。それ以外の場合、お使いの電話機は CAPF に対して認証しません。電話機で認証を設定する方法の詳細については、[電話ドキュメンテーション](#)を参照してください。

Procedure

-
- Step 1** [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[バルク管理 (Bulk Administration)] > [電話機 (Phones)] > [電話機の更新 (Update Phones)] > [クエリ (Query)]。
- Step 2** フィルタオプションを使用して、更新する電話機に検索を制限し、[検索 (Find)] をクリックします。
- たとえば、[電話機の検索場所] ドロップダウンリストを使用して、特定の日付の前に LSC の有効期限が切れる、または特定のデバイスプールにあるすべての電話機を選択します。
- Step 3** 「次へ (Next)」をクリックします。
- Step 4** [ログアウト/リセット/再開 (Logout/Reset/Restart)] セクションから、[設定の適用 (Apply Config)] ラジオボタンを選択します。ジョブを実行すると、CAPF アップデートは更新されたすべての電話に適用されます。

- Step 5** [証明機関プロキシ関数 (capf)]の情報で、[証明書の操作 (Certificate Operation)] チェックボックスをオンにします。
- Step 6** [証明書の操作 (Certificate Operation)] ドロップダウンリストから、[インストール/アップグレード (Install/Upgrade)] を選択して、新しい LSC 証明書を電話機にインストールします。
- Step 7** [認証モード (Authentication Mode)] ドロップダウンリストから、LSC インストール時に電話機を認証する方法を選択します。
- Note** 電話機で同じ認証方式を設定します。
- Step 8** [認証モード (Authentication Mode)] として [認証文字列による (By Authentication String)] を選択した場合は、次の手順のいずれかを実行します。
- 各デバイスに対して一意の認証文字列を使用する場合は、[各デバイスに対して一意の認証文字列を生成する (Generate unique authentication string for each device)] をオンにします。
 - すべてのデバイスに同じ認証文字列を使用する場合は、[認証文字列 (Authentication String)] テキストボックスに文字列を入力するか、[文字列の生成 (Generate String)] をクリックします。
- Step 9** [電話の更新 (Update Phones)] ウィンドウで [CAPF の情報 (Certification Authority Proxy Function (CAPF) Information)] セクションの残りのフィールドを入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。
- Step 10** [ジョブ情報 (Job Information)] セクションで、[今すぐ実行 (Run Immediately)] を選択します。
- Note** スケジュールされた時刻にジョブを実行する場合は、[後で実行 (Run Later)] を選択します。ジョブのスケジュール設定の詳細については、[Cisco Unified Communications Manager 一括管理ガイド](#)の「スケジュールされたジョブの管理」セクションを参照してください。
- Step 11** [送信 (Submit)] をクリックします。
- Note** この手順で [設定の適用 (Apply Config)] オプションを選択しなかった場合は、[電話機の設定 (Phones Configuration)] ウィンドウですべての更新された電話機に設定を適用します。

電話機の CAPF 設定の設定

個々の電話機の LSC 証明書の CAPF 設定を設定するには、次の手順を実行します。



Note LDAP 設定を多数の電話機に適用するには、バルク管理または CAPF ディレクトリ同期を使用します。

この手順で追加するのと同じ文字列と認証方式で電話機を設定します。それ以外の場合、電話機は CAPF に対してそれ自体を認証しません。電話機で認証を設定する方法の詳細については、電話ドキュメンテーションを参照してください。

Procedure

-
- Step 1** [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[デバイス (Device)] > [電話 (Phone)]。
- Step 2** 既存の電話機を選択するには、[検索 (Find)] をクリックします。[電話の設定 (Phone Configuration)] ページが表示されます。
- Step 3** [認証局プロキシ機能 (CAPF) 情報 (Certification Authority Proxy Function (CAPF) Information)] ペインに移動します。
- Step 4** [証明書の操作 (Certificate Operation)] ドロップダウンリストから、[インストール/アップグレード (Install/Upgrade)] を選択して、新しい LSC 証明書を電話機にインストールします。
- Step 5** [認証モード (Authentication Mode)] ドロップダウンリストから、LSC インストール時に電話機を認証する方法を選択します。
- Note** 電話機は、同じ認証方式を使用するように設定する必要があります。
- Step 6** [認証文字列による (By Authentication String)] を選択した場合は、テキスト文字列を入力するか、[文字列の生成 (Generate String)] をクリックして文字列を生成します。
- Step 7** [電話の設定 (Phone Configuration)] ページの [認証局プロキシ機能 (CAPF) 情報 (Certification Authority Proxy Function (CAPF) Information)] ペインで、残りのフィールドに詳細を入力します。フィールドとその設定の詳細については、オンラインヘルプを参照してください。
- Step 8** [保存 (Save)] をクリックします。
-

キープアライブタイマーの設定

ファイアウォールによって接続がタイムアウトしないように、次の手順を実行して、CAPF-エンドポイント接続のクラスターワイドキープアライブタイマーを設定します。デフォルト値は 15 分です。各間隔の後、CAPF サービスは電話機にキープアライブ信号を送信して、接続を開いた状態にします。

Procedure

-
- Step 1** 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。
- Step 2** `utils capt set keep_alive CLI` コマンドを実行します。
- Step 3** 5 ~ 60 (分) の間の数値を入力し、**Enter** キーを押します。
-

認証局プロキシ機能の管理タスクフロー

CAPF を設定して LSC 証明書を発行したら、LSC 証明書を継続的に管理します。

Procedure

	Command or Action	Purpose
Step 1	CAPF 経由の LSC 生成	CAPF を設定した後、設定されている認証文字列を電話機に追加します。キーと証明書の交換は、電話機と CAPF の間で行われます。
Step 2	古い LSC レポートの実行	Cisco Unified Reporting から古い LSC レポートを実行します。古い LSC は、エンドポイント CSR への応答として生成された証明書ですが、古くなった LSC がインストールされる前に新しい CSR がエンドポイントにより生成されたため、インストールされません。
Step 3	保留中の CSR リストの表示	保留中の CAPF CSR ファイルのリストを表示します。すべての CSR ファイルはタイムスタンプされます。
Step 4	古い LSC 証明書の削除	古い LSC 証明書をシステムから削除します。

古い LSC レポートの実行

次の手順を使用して、古い LSC レポートを Cisco ユニファイドレポートから実行します。古い LSCs は、エンドポイント CSR への応答として生成された証明書ですが、古くなった LSCs がインストールされる前に新しい CSR が生成されたため、インストールされませんでした。



Note また、パブリッシャーノードで `utils capf stale-lsc list` CLI コマンドを実行することによって、古い LSC 証明書のリストを取得することもできます。

Procedure

- Step 1** Cisco Unified Reporting から 「システムレポート (System Reports)」 をクリックします。
- Step 2** 左側のナビゲーションバーで、「古い LSC (Stale LSCs)」 を選択します。
- Step 3** [新規レポートの生成 (Generate a new report)] をクリックします。

CAPF 経由の LSC 生成

CAPFを設定した後、電話機に設定されている認証文字列を追加します。キーと証明書の交換は、電話機と CAPF の間で行われ、以下が発生します。

- 電話機は、設定された認証方法を使用して CAPF に対して自身を認証します。
- 電話機は公開/秘密キー ペアを生成します。
- 電話機は、署名されたメッセージの中で、公開キーを CAPF に転送します。
- 秘密キーは電話に残り、外部に公開されることはありません。
- 証明書は CAPF によって署名され、署名付きメッセージによって電話に送り返されます。



Note 電話のユーザが証明書操作の中断や、電話の動作ステータスの確認を実行できることに注意してください。



Note キーの生成を低い優先順位で設定すると、アクションの発生中に、電話機が機能します。電話機は証明書生成中に機能しますが、TLS トラフィックが追加された場合、電話機でのコールプロセスの中断が最小限に抑えられる可能性があります。たとえば、インストールの最後に証明書がフラッシュに書き込まれると、音声信号が発生することがあります。

保留中の CSR リストの表示

保留中の CAPF CSR ファイルのリストを表示するには、この手順を使用します。すべての CSR ファイルはタイムスタンプされます。

Procedure

- Step 1** 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。
- Step 2** `utils core active list CLI` コマンドを実行します。
保留中の CSR ファイルのタイムスタンプリストが表示されます。

古い LSC 証明書の削除

古い LSC 証明書をシステムから削除するには、次の手順を使用します。

Procedure

- Step 1** 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。
- Step 2** [utils capf state-lsc delete all CLI コマンド] を実行します。
古い LSC 証明書はすべてシステムから削除されます。

CAPF システムの連携動作と制限事項

Table 3: CAPF システムの連携動作と制限事項

機能	データのやり取り
認証文字	CAPF 認証方式での操作の後、電話機で同じ認証文字列を入力します。そうでない場合、操作が失敗します。[TFTP 暗号化設定 (TFTP Encrypted Config)] エンタープライズパラメータが有効な状態で認証文字列の入力に失敗した場合、電話の設定は失敗し、該当する認証文字列が電話に入力されるまで回復しません。
クラスタサーバクレデンシャル	Unified Communications Manager クラスタ内のすべてのサーバで、同じ管理者ユーザ名とパスワードを使用する必要があります。これにより、CAPF でクラスタ内のすべてのサーバを認証することができます。
セキュアな電話機の移行	<p>セキュアな電話機が別のクラスタに移動した場合、LSC 証明書が CTL ファイルにない別の CAPF により発行されているため、Unified Communications Manager は電話機が送信した LSC 証明書を信頼しません。</p> <p>セキュアな電話を登録可能にするには、既存の CTL ファイルを削除します。その後、[インストール/アップグレード (Install/Upgrade)] オプションを使用して新しい CAPF により新規 LSC 証明書をインストールし、新しい CTL ファイルのために電話をリセットします（または MIC を使用します）。電話を移動する前に、[電話の設定 (Phone Configuration)] ウィンドウの [CAPF] セクションにある [削除 (Delete)] オプションを使用して、既存の LSC を削除します。</p>

機能	データのやり取り
Cisco Unified IP 電話 6900、7900、8900、および 9900 シリーズ	<p>今後の互換性の問題を回避するために、Cisco Unified IP Phone 6900、7900、8900、および 9900 シリーズをアップグレードして、Unified Communications Manager への TLS 接続に LSC を使用し、Unified Communications Manager 信頼ストアから MIC ルート証明書を削除することをお勧めします。Unified Communications Manager への TLS 接続に MIC を使用する一部の電話機モデルでは、登録できない場合があります。</p> <p>管理者は Unified Communications Manager 信頼ストアから次の MIC ルート証明書を削除する必要があります。</p> <ul style="list-style-type: none"> • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
停電	<p>以下の情報は、通信障害や電源障害の発生時に適用されます。</p> <ul style="list-style-type: none"> • 電話機は、電話機への証明書のインストール中に通信障害が発生した場合に、30 秒の間隔で 3 回証明書の取得を試行します。これらの値をユーザが設定することはできません。 • 電話機が CAPF とのセッションを試行している間に電源が故障した場合、電話機はフラッシュに保存された認証モードを使用します。電話機が TFTP サーバから新しい設定ファイルを読み込めない場合、システムはフラッシュ値をクリアします。
証明書の暗号化	<p>Unified Communications Manager リリース 11.5(1) SU1、SHA-256 アルゴリズム署名以降、すべての LSC 証明書は CAPF サービスによって発行されます。したがって、IP 電話 7900/8900/9900 シリーズのモデルは、SHA-256 署名済み LSC 証明書および外部 SHA2 アイデンティティ証明書 (Tomcat、Unified Communications Manager、CAPF、TVS など) をサポートします。署名の検証が必要な、その他の暗号化の操作では、SHA-1 のみがサポートされます。</p> <p>Note 電話機を使用する場合は、ソフトウェア保守の最後にある電話機モデル、またはサポート終了モデルには、11.5(1) SU1 リリースより前の Unified Communications Manager を使用することをお勧めします。</p>

7942 および 7962 電話機を含む CAPF の例

ユーザまたは Unified Communications Manager が電話機をリセットする際に、CAPF が Cisco Unified IP Phone 7962 および 7942 と相互に作用する方法を検討してください。

**Note**

この例で、CAPF 証明書操作は、LSC が電話機に存在しない場合に、[CAPF 認証モード (CAPF Authentication Mode.)] に [既存の証明書 (By Existing Certificate)] を選択すると失敗します。

例: 非セキュア デバイス セキュリティ モード

この例では、[デバイスセキュリティモード (Device Security Mode)] を [非セキュア (Nonsecure)] に設定し、[CAPF 認証モード (CAPF Authentication Mode)] を [Null 文字列 (By Null String)] または [既存の証明書 (優先) (By Existing Certificate (Precedence))] に設定した後、電話がリセットされます。リセットした電話は直ちにプライマリ Unified Communications Manager に登録され、設定ファイルを受信します。その後、電話によって LSC をダウンロードするための CAPF セッションが自動的に開始されます。ダウンロードした LSC を電話にインストールした後、[デバイスセキュリティモード (Device Security Mode)] を [認証済み (Authenticated)] または [暗号化 (Encrypted)] に設定します。

例: 認証済み/暗号化済みデバイス セキュリティ モード

この例では、[デバイスセキュリティモード (Device Security Mode)] を [認証済み (Authenticated)] または [暗号化 (Encrypted)] に設定し、[CAPF 認証モード (CAPF Authentication Mode)] を [NULL 文字列 (By Null String)] または [既存の証明書 (優先) (By Existing Certificate (Precedence))] に設定した後、電話がリセットされます。CAPF セッションが終了して電話機が LSC をインストールするまで、電話機はプライマリ Unified Communications Manager に登録しません。セッションが終了すると、電話機が登録され、すぐに認証モードまたは暗号化モードで実行されます。

この例では、電話機が CAPF サーバに自動的に接続しないため、[認証文字列 (By Authentication String)] を設定することはできません。電話機に有効な LSC が存在しない場合、登録は失敗します。

IPv6 アドレッシングとの CAPF のインタラクション

CAPF は、IPv4、IPv6、または両方のタイプのアドレスを使用する電話機に証明書を発行し、アップグレードします。IPv6 アドレスを使用する SCCP が実行されている電話機に対して証明書を発行またはアップグレードするには、Cisco Unified Communications Manager Administration で [IPv6 の有効化 (Enable IPv6)] サービスパラメータを [True] に設定する必要があります。

CAPF では [Enable IPv6 (IPv6 の有効化)] エンタープライズパラメータの設定を使用して、その電話機への証明書の発行またはアップグレードを実行します。このエンタープライズパラメータが [False] に設定された場合、CAPF は IPv6 アドレスを使用する電話機からの接続を無視または拒否し、その電話機は証明書を受け取りません。

次の表では、IPv4、IPv6、または両方のタイプのアドレスを持つ電話機が CAPF に接続する方法について説明します。

Table 4: IPv6 または IPv4 電話機の CAPF への接続方法

電話機の IP モード	電話機の IP アドレス	CAPF IP アドレス	電話機から CAPF への接続方法
2 スタック	IPv4 および IPv6 が使用可能	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。電話機は、IPv6 アドレスを介して接続できない場合、IPv4 アドレスを使用して接続を試行します。
2 スタック	IPv4	IPv4、IPv6	電話機は、CAPF に接続するために IPv4 アドレスを使用します。
2 スタック	IPv6	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。試行に失敗した場合、電話機は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv6	電話機は、および IPv6 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv6	電話機は CAPF に接続できません。
2 スタック	IPv6	IPv4	電話機は CAPF に接続できません。
2 スタック	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。

電話機の IP モード	電話機の IP アドレス	CAPF IP アドレス	電話機から CAPF への接続方法
IPv4 スタック	IPv4	IPv4、IPv6	電話機は、CAPF に接続するために IPv4 アドレスを使用します。
IPv6 スタック	IPv6	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv6	電話機は CAPF に接続できません。
IPv6 スタック	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4	電話機は CAPF に接続できません。