認証局プロキシ 機能

認証局プロキシ機能（CAPF）の概要

認証局プロキシ 機能 (CAPF) は、Locally Significant Certificates (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 で実行され、以下のタスクを実行します:

- サポートされている Cisco Unified IP 電話 に LSC を発行します。
- 混合モード中に電話を認証します。
- 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 のインストール時に自動的にインストールされ、CAPF 指定のシステム証明書が生成されます。

重要 次のメモはリリース 14SU2 以降にのみ適用されます。

（注） CAPF 証明書には、次のデフォルトの X509 拡張子が含まれている必要があります。

X509v3 の基本的制約:

CA:TRUE, pathlen:0

X509v3 キーの使用法:

デジタル署名、証明書署名

これらの拡張機能が CAPF 証明書に存在しない場合、TLS 接続エラーが発生します。

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。

表 *1: CAPF* 実行モード

モード	説明
Cisco Authority Proxy 機能	デフォルトでは、CAPF サービスで Unified Communications Manager CAPF サービス署名 LSC を発行します。
オンライン CA	[オンライン CA (Online 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。証明書署名リクエスト（CSR）が手動で送信された場合、CA は署名し、CA の署名済み LSC を自動的に返します。
オフライン CA	オフライン CA: このオプションは、オフラインの外部 CA を使用して LSC for phone に署名する場合に使用します。 LSC を手動でダウンロードし、CA に提出し、準備ができたら CA 署名付き証明書をアップロードします。 （注） サードパーティの CA を使用して LSC に署名する場合は、**オフライン CA** オプションの代わりに **オンライン CA** オプションをおすすめします。 **オンライン CA** は自動化され、より迅速になり、問題が発生する可能性が低くなります。

LSC を生成する前に、以下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を含む Cisco Unified IP 電話 および Jabber。
- 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、電話を認証する方法も決めてください。

LSC を必要なトラストストアに生成する前に、CA ルートおよび HTTPS 証明書を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 connection 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 トラストで Unified Communications Manager-トラストをたどります。 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。

以下は、さまざまな証明書をアップロードするシナリオです。

表 *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。
CA ルート証明書は異なる中間 CA および 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。
CA ルートと HTTPS の証明書は異なり、同じ CA ルート証明書によって発行されます。	CA ルートおよび HTTPS 証明書をアップロードする。

（注） スケジュールされたメンテナンス期間中にCAPFを使用することを推奨します。複数の証明書を同時に生成すると、コール処理が中断される可能性があるためです。

認証局のプロキシ機能の構成タスクフロー

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。

（注） 新しい CAPF 証明書を再生成またはアップロードした後に、CAPF サービスを再起動する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 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。 それ以外の場合は、この作業をスキップできます。
ステップ 2	認証局（CA）ルート証明書のアップロード （5 ページ）	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。
ステップ 3	オンライン認証局の設定 （6 ページ）	電話機LSC証明書を生成するには、次の手順を使用します。
ステップ 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。
ステップ 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に、重要な CAPF サービスをアクティブにします。
ステップ 6	次のいずれかの手順を使用して、Unified Communications Managerの CAPF 設定を構成します。 • CAPD 設定をユニバーサルデバイステンプレートで設定します。 （8 ページ） • バルク Admin による CAPF 設定の更新 （10 ページ） • 電話機の CAPF 設定の設定 （11 ページ）	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。 • 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することができます。 • 一括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。
ステップ 7	キープアライブ タイマーの設定 （12 ページ）	ファイアウォールによってタイムアウトにならないように、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て、外部 CA を使用して LSC 証明書に署名します。

（注） サードパーティ CA を使用して LSCs に署名しない場合は、このタスクをスキップできます。

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書目的]** ドロップダウンリストで、**[CallManager 信頼]** を選択します。

ステップ 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。**

ステップ 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。

ステップ 6 [アップロード（Upload）]をクリックします。

ステップ 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

（注） 中間またはルート CA 証明書の共通名に「CAPF-」部分文字列が含まれていないことを確認してください。「CAPF-」共通名は、CAPF 証明書用に予約されています。

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 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。

ステップ 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。**

ステップ 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。

ステップ 6 [アップロード（Upload）]をクリックします。

重要 この注意事項は、リリース 14 SU2 以降に適用されます。

（注） ルート CA 証明書または中間 CA 証明書には、次のデフォルトの X509 拡張機能を含める必要があります。

X509v3 の基本的制約:

CA:TRUE, pathlen:0

X509v3 キーの使用法:

デジタル署名、証明書署名

これらの拡張機能が証明書に存在しない場合、TLS 接続エラーが発生します。

重要 この注意事項は、リリース 14 SU3 以降の IPSec 証明書にのみ適用されます。

（注） CA 署名付き IPSec 証明書の場合、次の拡張機能を含めることはできません。

X509v3 の基本的制約:

CA:TRUE

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にあるこの手順を使用します。

ステップ 1 Cisco Unified CM の管理から、**[システム（System）] > [サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 **[サーバ]** ドロップダウン リストから、[Cisco 認証局プロキシ機能（アクティブ）] サービスを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco 認証局プロキシ機能（アクティブ）（Cisco 認証局プロキシ 機能 (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。

ステップ 4 [エンドポイントへの証明書発行者（Certificate Issuer to Endpoint）] ドロップダウン リストから、[オンラインCA（Online CA）] を選択します。 CA 署名付き証明書では、オンライン CA を使用することを推奨しています。

ステップ 5 **[証明書の有効期間（日数）]** 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。

ステップ 6 [オンラインCAパラメータ（Online CA Parameters）] 画面で次のパラメータを設定し、オンライン CA セクションに対する接続を作成します。

- オンライン CA ホスト名：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。

  （注） 設定されているホスト名は、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）でホストされる HTTPS 証明書の共通名（CN）と同じです。

- オンライン CA ポート: オンライン CA のポート番号（443 など）を入力します。
- オンライン CA テンプレート：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。

  （注） このフィールドが有効になるのは、オンライン CA タイプが Microsoft CA の場合のみです。

- オンライン CA タイプ: エンドポイント証明書の自動登録には、Microsoft CA または EST でサポートされる CA を選択します。
  - Microsoft CA：CA が Microsoft CA である場合は、このオプションを使用してデジタル証明書をデバイスに割り当てます。

    （注） FIPS 対応モードは、Microsoft CA ではサポートされていません。

  - **重要** リリース 14SU2 以降でサポートされます。

EST サポート CA：CA が自動登録用の組み込み EST サーバーモードをサポートしている場合は、このオプションを使用します。

- オンライン CA ユーザ名：CA サーバのユーザ名を入力します。
- オンライン CA パスワード：CA サーバのユーザ名のパスワードを入力します。
- 証明書登録プロファイル ラベル: EST がサポートする CA のデジタル ID を有効な文字で入力します。

（注） このフィールドが有効になるのは、オンライン CA タイプが EST サポート CA の場合のみです。

ステップ 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。

ステップ 8 **[保存]** をクリックします。

ステップ 9 変更内容を有効にするには、**Cisco 認証局プロキシ機能** サービスを再起動します。 Cisco Certificate Enrollment service を自動的に再起動します。

現在のオンライン CA の制限

- CA サーバが英語以外の言語を使用している場合、オンライン CA 機能は動作しません。 CA サーバは英語でのみ応答します。
- オンライン CA 機能は、CA での mTLS 認証をサポートしていません。
- LSC 操作にオンライン CA を使用している場合、LSC 証明書に「デジタル署名」と「キー暗号化」のキー使用法が指定されていないと、デバイスのセキュア登録は失敗します。
- LSC 操作にオンライン CA を使用している場合、LSC 証明書に「デジタル署名」と「キー暗号化」が指定されていないと、デバイスのセキュア登録は失敗します。

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。

（注） 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 お使いの電話機の LSC 用に **CSR** を生成します。

ステップ 5 認証局に**CSR** を送信します。

ステップ 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 システムを設定した後に、重要な 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。

ステップ 1 Cisco Unified Serviceability から**[ツール]** > **[サービス アクティベーション]** を選択します。

ステップ 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。

ステップ 3 **[セキュリティサービス]** ペインから、次の該当す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のチェックをオンにし、そうでない場合はチェックを外したままにします。
- **Cisco Certificate Authority プロキシ機能**: このサービスをオフ (非アクティブ) にした場合は、チェックを入れます。 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。

ステップ 4 いずれかの設定を変更した場合、**[保存]** をクリックします。

ステップ 5 **Cisco 認証局プロキシ 機能** 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]**ドロップダウン リストから **[コントロールセンター-ネットワークサービス]**を選択し、**[移動]** をクリックします。

b) **[セキュリティの設定]**ペインから、**シスコ認証局プロキシ機能**サービスを確認し、**[再起動]** をクリックします。

ステップ 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) CAPD 設定をユニバーサル デバイス テンプレートで設定します。 （8 ページ）

b) バルク Admin による CAPF 設定の更新 （10 ページ）

c) 電話機の CAPF 設定の設定 （11 ページ）

CAPD 設定をユニバーサル デバイス テンプレートで設定します。

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

します。テンプレートのCAPF設定が、このテンプレートを使用する同期済みのすべてのデバイスに適用されます。

（注） Universal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 （10 ページ）を参照してください。

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（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）]** を選択します。

ステップ 2 次のいずれかを実行します。

- **[検索]** をクリックし、既存のテンプレートを**選択**します。
- [新規追加] をクリックします。

ステップ 3 **認証局プロキシ機能（CAPF）の設定**領域の拡張

ステップ 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。

ステップ 5 **[認証モード]** ドロップダウンメニューで、デバイスを認証するオプションを選択します。

ステップ 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。

（注） 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。

ステップ 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。

ステップ 8 **[保存]** をクリックします。

（注） 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法で構成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。

ステップ 9 このプロファイルを使用するデバイスにテンプレート設定を適用します。

a) ユニバーサルデバイステンプレートを Feature Group テンプレートの設定に追加します。
b) 機能グループ テンプレートを、同期されていない LDAP ディレクトリ設定に追加します。
c) 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 ディレクトリ同期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「Configure End Users」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

一括管理の**電話機の更新**クエリを使用して、多数の既存の電話機の CAPF 設定と lsc 証明書を 1 回の操作で構成します。

（注） まだ電話機をプロビジョニングしていない場合は、一括管理の**[電話機の挿入]**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認証方法と文字列と同じように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、「電話機のマニュアル」を参照してください。

ステップ 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** > **電話機** > **電話機の更新** > **クエリ**

ステップ 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]** をクリックします。

たとえば、**[電話機の検索場所]** ドロップダウンを使用して、LSC が特定の日付の前期限切れになるすべての電話機またはデバイスプール内の電話機を選択することができます。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 **ログアウト/リセット/再起動** セクションから**[設定の適用]**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。

ステップ 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。

ステップ 6 **[証明書の操作]** 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]** 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。

ステップ 7 **[認証モード]** ドロップダウンから、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。

（注） 電話機で同じ認証方法を設定します。

ステップ 8 **認証モード**として**認証文字列**で選択した場合は、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**ことを確認してください。
- 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]** テキストボックスに文字列を入力するか、**[文字列の生成]** をクリックします。

ステップ 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。

ステップ 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。

（注） スケジュールされた時刻にジョブを実行する場合は、**[後で実行する]** 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。

ステップ 11 [送信（Submit）]をクリックします。

（注） この手順で **[設定の適用]** オプションを選択しなかった場合は、更新されたすべての電話機の **[電話機の設定]** ウィンドウで設定を適用します。

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。

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

電話機は、この手順で追加する認証方法と文字列と同じように設定します。 それ以外の場合、電話機は CAPF に対して自身を認証しません。 電話機で認証を設定する方法の詳細については、「電話機のマニュアル」を参照してください。

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[デバイス]** > **[電話]**

ステップ 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。 **[電話設定]** ページが表示されます。

ステップ 3 **[認証局プロキシ機能 (CAPF) の情報]** ペインに移動します。

ステップ 4 **[証明書の操作]** 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]** 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。

ステップ 5 **[認証モード]** ドロップダウンから、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。

（注） 電話機は、同じ認証方法を使用するように設定されている必要があります。

ステップ 6 **[認証文字列]** で選択した場合は、テキスト文字列を入力するか、**[文字列の生成]** をクリックして、システムが文字列を生成するようにします。

ステップ 7 **[電話機の設定（Phone Configuration）]** ページで **[認証局プロキシ機能 (CAPF) の情報]** ペインの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。

ステップ 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。

ステップ 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。

ステップ 2 `utils capt set keep_alive` CLI コマンドを実行します。

ステップ 3 5 ~ 60 (分) の間の数値を**入力**し、確定キーをクリックします。

認証局のプロキシ機能の管理タスクフロー

CAPF が設定され LSC 証明書が発行されたら、継続的に LSC 証明書を管理します。

手順

	コマンドまたはアクション	目的
ステップ 1	CAPF 経由の LSC 生成	CAPF を設定し、設定した認証文字列を電話に追加します。 キーと証明書の交換は、電話と CAPF の間で行われます。
ステップ 2	古い LSC レポートの実行	Cisco Unified Reporting から無効な LSC レポートを実行します。 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。
ステップ 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。
ステップ 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 Unified 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。

（注） 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。

ステップ 1 Cisco Unified Reporting から **[System Reports]** をクリックします。

ステップ 2 左側のナビゲーションバーで、[**古い LSCs**] を選択します。

ステップ 3 **[新規レポートの生成]** 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 の間で行われます。次のような場合があります。

- 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。

（注） 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。

（注） キー生成の優先順位を低く設定すると、処理中に電話機を動作させることができます。 証明書生成中にも電話は正常に機能しますが、TLS トラフィックが増加することで、電話での通話の処理に最小限の中断が発生す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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 システムの相互作用

表 *3: CAPF* システム インタラクション

機能	データのやり取り
認証文字列（Authentication String）	CAPF認証方法で操作を行った後、電話に同じ認証文字列を入力しないと、操作は失敗します。 TFTP Encrypted Configuration エンタープライズ パラメータが有効で、認証文字列の入力に失敗した場合、一致する認証文字列が電話機に入力されるまで電話機に障害が発生し、回復しない可能性があります。
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ーは、CAPF がクラスタ内のすべてのサーバを認証できるように、同じ管理者のユーザ名とパスワードを使用する必要があります
セキュアな電話機の移行	セキュアな電話が別のクラスタに移動した場合、クラスタ Unified Communications Manager はその電話から送信された LSC 証明書を信頼しません。これは、その電話が別の CAPF により発行され、その証明書が CTL ファイルに含まれていないためです。 既存の CTL ファイルを削除して、セキュア電話を登録できるようにします。 その後、[インストール/アップグレード] オプションを使用して、新しい CAPF を持つ新しい LSC 証明書をインストールし、新しい CTL ファイルに対して電話をリセットします (または MIC を使用します)。 **[電話機の設定（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、電話を移動する前に既存の LSC を削除します。

機能	データのやり取り
Cisco Unified IP Phones 6900、7900、8900、および 9900 シリーズ	Cisco Unified IP 電話の 6900、7900、8900、9900 シリーズをアップグレードして、LSC を使用して Unified Communications Manager への TLS 接続し、そして、 Unified Communications Manager トラストストアから MIC ルート証明書を削除することをお勧めします。互換性の問題を避けるためです。 MIC を使って Unified Communications Manager への TLS 接続を行う電話モデルでは、登録ができない場合があります。 管理者は次の MIC ルート証明書を Unified Communications Manager 信頼ストアから削除する必要があります: • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
停電	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。 • 電話機に証明書をインストールしている間に通信障害が発生すると、電話機は証明書の取得を 30 秒間隔で 3 回試みます。 これらの値を構成することはできません。 • 電話が CAPF でセッションを試みている間に停電が発生した場合、電話はフラッシュに保存されている認証モードを使用します。 電話が TFTP サーバから新しい構成ファイルをロードできない場合、システムはフラッシュの値をクリアします。
証明書の暗号化	Unified Communications Manager リリース 11.5 (1) SU1 から始まり、CAPF サービスが発行するすべての LSC 証明書に SHA-256 アルゴリズムにより署名されます。 そのため、IP 電話 7900/8900/9900 シリーズのモデルは、SHA-256 署名済み LSC 証明書と外部 SHA2 アイデンティティ証明書 (Tomcat、 Unified Communications Manager、CAPF、TVS など) をサポートしています。 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。 （注） ソフトウェアメンテナンス終了または製品寿命終了の電話モデルについては、11.5(1) SU1 リリース Unified Communications Manager 前のリリースを使用することをおすすめします。

7942 および 7962 電話機を含む CAPF の例

CAPFがユーザーまたは Cisco Unified IP 電話 が電話をリセットしたときに、7962および7942とどのように対話するかを検討してください。 Unified Communications Manager

（注） 例では、電話にLSCが存在せず、CAPF認証モードで **既存の証明書** を選択すると、CAPF証明書の操作が失敗します。

例：非セキュア デバイス セキュリティ モード

この例では、[Device Security Mode] を **[Nonsecure]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[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。 電話にダウンロードされた LSC がインストールされたら、[デバイス セキュリティ モード] を [認証済み] または [暗号化済み] 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、**[Device Security Mode]** を **[Authenticated]** または **[Encrypted]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[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、電話に LSC がインストールされるまで、電話はプライマリ Unified Communications Manager に登録されません。 セッションが終了すると、電話が登録され、直ちに認証済みまたは暗号化済みモードで動作します。

この例では **認証文字列により** 設定することはできません。電話が CAPF サーバに自動的に接続しないためです。 電話に有効な LSC がない場合、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、またはその両方のタイプのアドレスを使用する電話に対し、証明書の発行とアップグレードを実行できます。 IPv6 アドレスを使用して SCCP を実行している電話用の証明書を発行またはアップグレードするには、 **IPv6を有効にする** サービスパラメータを **True** に設定します。 Cisco Unified Communications Manager Administration

CAPF は、 **IPv6 を有効にする** エンタープライズパラメータの構成を使用して、電話への証明書を発行またはアップグレードします。 エンタープライズパラメータが **False** の場合、CAPF は IPv6 アドレスを使用する電話からの接続を無視/拒否し、電話は証明書を受け取りません。

IPv4、IPv6、またはその両方のタイプのアドレスを使用する電話から CAPF への接続方法について、次の表で説明します。

表 *4 : IPv6* または *IPv4* 電話から *CAPF* への接続方法

電話の IP モード	電話の IP アドレス	CAPF IP アドレス	電話から CAPF への接続方法
2 スタック	IPv4 と IPv6 が利用可能	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。 電話が IPv6 アドレス経由で接続できない場合、IPv4 アドレスを使用して接続を試みます。
2 スタック	IPv4	IPv4、IPv6	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	IPv6	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。 試行に失敗すると、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	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	電話は 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	電話が CAPF に接続できません。
2 スタック	IPv6	IPv4	電話が 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。

電話の IP モード	電話の IP アドレス	CAPF IP アドレス	電話から CAPF への接続方法
IPv4 スタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4、IPv6	電話は 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	電話が 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	電話が CAPF に接続できません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。