Certificate Authority Proxy Function

認証局プロキシ機能（CAPF）の概要

Cisco 認証局プロキシ機能（CAPF）は、ローカルで有効な証明書（LSC）を発行し、Cisco エンドポイントを認証する Cisco 専有サービスです。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 電話 に対して LSC を発行する。
- 混合モードが有効になっている場合に電話機を認証する。
- 電話機用の既存の LSC をアップグレードする。
- 表示とトラブルシューティングのために電話機証明書を取得する。

CAPF の実行モード

CAPF は、次のモードで動作するように設定することができます。

- Cisco Authority プロキシ機能：Unified Communications Manager の CAPF サービスが、CAPF サービス自体によって署名された LSC を発行します。これがデフォルトのモードです。
- オンライン CA：外部オンライン CA によって電話機用の LSC に署名する場合は、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 に接続します。CSR が送信されると CA が署名し、CA で署名された LSC が自動的に返されます。
- オフライン CA：オフラインの外部 CA によって電話機用の LSC に署名する場合は、このオプションを使用します。このオプションでは、LSC を手動でダウンロードし、CA に提出して、CA で署名された証明書の準備ができたら、それらをアップロードする必要があります。

（注） サードパーティ CA を使用して LSC に署名する必要がある場合、シスコでは、オフライン CA ではなくオンライン CA のオプションを使用することを推奨します。オンライン CA ではプロセスが自動化されるため、はるかに高速で、問題が発生する可能性も低くなります。

CAPF サービス証明書

統合コミュニケーションマネージャがインストールされている場合、CAPF サービスが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。セキュリティが適用されると、Cisco CTL クライアントは、すべてのクラスタノードに証明書をコピーします。

電話機の証明書タイプ

シスコは次の X.509v3 証明書タイプを電話で使用します。

- ローカルで有効な証明書（LSC）：このタイプの証明書は Cisco Certificate Authority Proxy Function（CAPF）に関連する必要な作業の実行後に、電話にインストールされます。デバイス セキュリティ モードを認証または暗号化に設定した後で、LSC は Unified Communications Manager と電話の間の接続を保護します。

  （注） オンライン CA の場合、LSC の有効性は CA に基づいています。また、CA が許可している限り使用できます。

- 製造元でインストールされる証明書（MIC）：Cisco Manufacturing は MIC をサポートされている電話モデルに自動的にインストールします。製造元でインストールされる証明書は LSC インストールの Cisco Certificate Authority Proxy Function（CAPF）を認証します。製造元でインストールされる証明書を上書きしたり、削除することはできません。

（注） 製造元でインストールされる証明書（MIC）を LSC のインストールでのみ使用することが推奨されます。シスコでは Unified Communications Manager との TLS 接続の認証のために LSC をサポートしています。MIC ルート証明書は侵害される可能性があるため、TLS 認証またはその他の目的に MIC を使用するように電話を設定するお客様は、ご自身の責任で行ってください。MIC が侵害された場合シスコはその責任を負いません。

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。

（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。

CAPF 前提条件

LSC 生成用の認証局のプロキシ機能を設定する前に、次の手順を実行します。

- サードパーティ CA を使用して LSCs に署名したい場合は、CA を外部に設定します。
- 電話機を認証する方法を計画します。
- LSC を生成する前に、次の条件を満た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 IP 電話 および Jabber を含む）
  - Microsoft Windows Server 2012 および 2016
  - ドメインネームサービス（DNS）が構成されている
- LSC を生成する前に、CA ルート証明書と HTTPS 証明書をアップロードする必要があります。セキュア SIP 接続では、HTTPS 証明書は CAPF 信頼を通過し、CA ルート証明書は CAPF 信頼と CallManager 信頼を通過します。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。CA ルート証明書は、証明書署名要求 (CSR) への署名に使用されます。

  証明書をアップロードする必要がある場合のシナリオを次に示します。

表 *1:* 証明書のアップロードシナリオ

シナリオ	結果
CA ルート証明書と HTTPS 証明書が同じ。	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 証明書が異なり、HTTPS 証明書は同じ CA ルート証明書によって発行される。	CA ルート証明書をアップロードする。
中間 CA 証明書と HTTPS 証明書が異なり、CA ルート証明書によって発行される。	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 証明書が異なり、同じ CA ルート証明書によって発行される。	CA ルート証明書と HTTPS 証明書をアップロードする。

（注） 複数の証明書を同時に生成するとコール処理中断の原因となるため、スケジュールされたメンテナンスの時間帯に CAPF を使用することを強く推奨します。

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。

手順

	コマンドまたはアクション	目的
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 （6 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。
Step 3	オンライン認証局の設定 （6 ページ）	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。

	コマンドまたはアクション	目的
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 サービスのアクティブ化または再起動	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。
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。 • ユニバーサル デバイス テンプレートでの CAPD 設定の構成 （9 ページ） • 一括管理による CAPF 設定の更新（11 ページ） • 電話機の CAPF 設定の構成 （12 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します。 • 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。
Step 7	キープアライブ タイマーの設定 （13 ページ）	（オプション）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。

（注） 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。

手順

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

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**のように指定します。

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、[証明書の用途（Certificate Purpose）] を [CallManager 信頼（callmanager-trust）] として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。

手順

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

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**のように指定します。

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。

（注） 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。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

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 [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 [オンラインCAパラメータ（Online CA Parameters）] セクションで、次のパラメータを設定して、オンライン CA セクションへの接続を作成します。

- [オンラインCAホスト名（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。

  （注） 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。

- [オンラインCAポート（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 のように指定します。
- [オンラインCAテンプレート（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。
- [オンラインCAタイプ（0Online CA Type）]：デフォルトのタイプである Microsoft CA を選択します。
- [オンラインCAユーザ名（Online CA Username）]：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（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。

現在のオンライン CA の制限

- オンライン CA 操作の場合、EST サーバは CUCM から TVS 証明書を使用します。TVS 証明書が CA で署名されている場合、オンライン CA は動作しません。
- 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。

手順

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 サービスのアクティブ化または再起動

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。

手順

Step 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスアクティベーション（Service Activation）]** を選択します。

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 設定の構成 （9 ページ）

b) 一括管理による CAPF 設定の更新 （11 ページ）

c) 電話機の CAPF 設定の構成 （12 ページ）

ユニバーサル デバイス テンプレートでの CAPD 設定の構成

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。

（注） 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、「一括管理による CAPF 設定の更新（11 ページ）」を参照してください。

手順

Step 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。

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（Certificate Authority Proxy Function (CAPF) Settings）] 領域を展開します。

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、[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、または [文字列を生成（Generate String）] 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。

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。

（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。

a) 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。
b) 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。
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」の項を参照してください。

一括管理による CAPF 設定の更新

Bulk Administrationの**電話機の更新**クエリを使用して、1 回の操作で多数の既存の電話機に CAPF 設定と LSC 証明書を設定します。

（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（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。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[一括管理（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（Find phones where）] 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電話機や、特定のデバイスプールにある電話機をすべて選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [ログアウト/リセット/リスタート（Logout/Reset/Restart）] セクションで、[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 [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] 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 の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）] ウィンドウの [認証局プロキシ機能（CAPF）情報（Certification Authority Proxy Function (CAPF) Information）] セクションで、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。

（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（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。

（注） 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 設定の構成

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） LDAP 設定を多数の電話機に適用するには、一括管理または 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。

手順

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 の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。

手順

Step 1 コマンド ライン インターフェイスを使用して、パブリッシャノードにログインします。

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。

CAPF の管理タスク

CAPF を設定し、LSC 証明書を発行した後、次のタスクを使用して LSC 証明書を継続的に管理します。

証明書ステータスのモニタリング

証明書のステータスを自動的に監視するようにシステムを設定することができます。証明書が期限切れに近づいたときにシステムから電子メールが送信され、期限切れ後に証明書が失効します。

証明書の監視の確認の設定方法の詳細については、「証明書の管理」の章の「証明書の監視と失効のタスクフロー」を参照してください。

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 LSC とは、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、その LSC がインストールされる前にエンドポイントによって新しい CSR が生成されたため、インストールされなかったものです。

（注） パブリッシャーノードで `utils capf stale-lsc list` CLI コマンドを実行して、古い LSC 証明書のリストを取得することもできます。

手順

Step 1 Cisco Unified Reporting から、[システムレポート（System Reports）] を選択します。

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 [新規レポートの作成（Generate a new Report）] をクリックします。

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。

手順

Step 1 コマンド ライン インターフェイスを使用して、パブリッシャノードにログインします。

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。

手順

Step 1 コマンド ライン インターフェイスを使用して、パブリッシャノードにログインします。

Step 2 `utils capf stale-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

機能	連携動作
認証文字列	電話の CAPF 認証方式については、アップグレードまたはインストールの後に同じ認証文字列を電話に入力する必要があります。入力されなかった場合、操作が失敗します。[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	CAPF が Unified Communications Manager クラスタのすべてのサーバを認証できるよう、クラスタ内のすべてのサーバで管理者のユーザ名とパスワードを同じものに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されると、Unified Communications Manager はその電話が送信する LSC 証明書を信頼しなくなります。これは、その LSC 証明書が、CTL ファイル内に証明書が存在しない別の CAPF によって発行されたものであるためです。 セキュアな電話機を登録できるようにするには、既存の CTL ファイルを削除します。その後、[Install/Upgrade] オプションを使用して新しい CAPF を使用して新しい LSC 証明書をインストールし、電話機を新しい CTL ファイルにリセット (または MIC を使用) することができます。電話機を移動する前に既存の LSC を削除するには、[電話の設定 (Phone Configuration)] ウィンドウの [CAPF] セクションの [削除 (Delete)] オプションを使用します。

機能	連携動作
Cisco Unified IP 電話 6900 シリーズ、7900 シリーズ、および 8900 シリーズ、および 9900	将来的な互換性の問題を回避するため、Unified Communications Manager との TLS 接続に LSC を使用するために Cisco Unified IP 電話 6900 シリーズ、7900 シリーズ、8900 シリーズ、9900 シリーズをアップグレードし、MIC ルート証明書を CallManager 信頼ストアから削除することが推奨されます。Cisco Unified Communications Manager との TLS 接続に MIC を使用する一部の電話モデルは登録できない場合があることに注意してください。 管理者は、CallManager 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。 • 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。 • 電話機で証明書のインストールが行われている間に通信障害が発生した場合、電話機は30秒間隔で証明書の取得を3回試行します。これらの値は設定できません。 • 電話機が CAPF とのセッションを試行している間に電源障害が発生した場合、電話機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。つまり、電話機の再起動後に、電話機が TFTP サーバから新しい設定ファイルをロードできない場合です。証明書の操作が完了すると、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	Cisco Unified Communications Manager リリース 11.5(1)SU1 以降、CAPF サービスによって発行されるすべての LSC 証明書は、SHA-256 アルゴリズムで署名されています。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、CallManager、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。 （注） ソフトウェア メンテナンスが終了またはサポートが終了した電話モデルを使用する場合は、Unified Communications Manager の 11.5(1)SU1 より前のリリースの使用を強くお勧めします。

7942 および 7962 電話機での CAPF の例

ユーザまたはUnified Communications Managerによって電話がリセットされたときのCAPFとCisco Unified IP 電話 7962 および 7942 とのインタラクションについては、以下の情報を考慮してください。

（注） 以下の例では、電話機に LSC が存在せず、CAPF 認証モードとして [既存の証明書（By Existing Certificate）] が選択されている場合、CAPF 証明書操作が失敗します。

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、電話機は CAPF とのセッションを自動的に開始して LSC をダウンロードします。電話機が LSC をインストールした後、デバイスセキュリティモードを [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、**[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 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、電話が自動的にCAPFサーバに接続されないため、**[By Authentication String]** を設定できません。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、アップグレードすることができます。IPv6 アドレスを使用する SCCP を実行する電話の証明書の発行またはアップグレードを実行するには、[Unified Communications Manager Administration] で [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。

電話機が CAPF に接続して証明書を取得すると、CAPF は [IPv6 を有効にする (Enable IPv6)] エンタープライズパラメータの設定を使用して、電話機に証明書を発行するか、またはアップグレードするかを決定します。エンタープライズパラメータが**False**に設定されている場合、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、電話機は証明書を受信しません。

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。

表 *2 : 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つのスタック	IPv4 と IPv6 が利用可能	IPv4、IPv6	電話機は、IPv6 アドレスを使用して CAPF に接続します。電話機が IPv6 アドレスを介して接続できない場合は、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つのスタック	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	電話機が CAPF に接続できない。
2 スタック	IPv6	IPv4	電話は 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	電話機が CAPF に接続できない。
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	電話は CAPF に接続できません。