Certificate Authority Proxy Function

この章では、Certificate Authority Proxy Function について説明します。

Certificate Authority Proxy Function について

Certificate Authority Proxy Function（CAPF）は、Cisco Unified Communications Manager とともに自動的にインストールされ、設定に応じて次のタスクを実行します。

- 既存の製造元でインストールされた証明書（MIC）、ローカルで有効な証明書（LSC）、ランダムに生成された認証文字列、または安全性の低いオプションの「「null」」認証によって認証する。
- サポートされる Cisco IP Phone に対してローカルで有効な証明書を発行する。
- 電話にある既存のローカルで有効な証明書をアップグレードする。
- 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。

インストール時に、CAPF に固有の証明書が生成されます。Cisco CTL クライアントによってクラスタ内のすべての Cisco Unified Communications Manager サーバにコピーされるこの CAPF 証明書では、拡張子 .0 を使用します。

Cisco IP Phone と CAPF のインタラクション

電話とCAPFとのインタラクションが発生すると、電話は認証文字列、既存のMICまたはLSC証明書、または「「null」」を使用して自身を CAPF に認証し、公開キーと秘密キーのペアを生成し、署名付きメッセージによって公開キーをCAPFサーバに転送します。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。

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、Cisco IP 電話 6900、7800、7900、8800、8900、および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） 11.5 (1) SU1 リリースを使用する前に、Cisco ユニファイドコミュニケーションマネージャーを使用することを推奨します。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モデル、または寿命が終了しているモデルを使用します。

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。

- 電話での証明書インストールの実行中に通信障害が発生した場合、電話は証明書の取得を 30 秒間隔でさらに 3 回試行します。これらの値は設定できません。
- 電話によるCAPFとのセッション試行中に電源障害が発生した場合、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。つまり、電話の再起動後に TFTP サーバから新しい設定ファイルをロードできなかった場合です。証明書操作が完了すると、システムはフラッシュの値をクリアします。

ヒント 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。

ヒント　キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。キーの生成が完了するまでに、30 分以上かかることがあります。

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へ書き込まれるとき、オーディオにノイズが発生する場合があります。

ユーザまたはCisco 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 Phone 7960G および 7940G 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）　次の例では、LSC が電話に存在せず、CAPF 認証モードとして既存の証明書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 Cisco 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。電話でLSCをインストールした後、[Device Security Mode] を [Authenticated] または [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 Cisco 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、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。

証明書取得のために電話が CAPF に接続されると、CAPF では [Enable IPv6] エンタープライズ パラメータの設定を使用して、その電話の証明書の発行またはアップグレードを実行するかど

うかが決定されます。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からの接続を無視または拒否し、その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 *1 : 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
デュアルスタック	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。IPv6 アドレスでは接続できない場合、電話は IPv4 アドレスを使用して接続を試みます。
デュアルスタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
デュアルスタック	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。
デュアルスタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
デュアルスタック	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。
デュアルスタック	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。
デュアルスタック	IPv4	IPv6	電話は CAPF に接続できません。
デュアルスタック	IPv6	IPv4	電話は CAPF に接続できません。

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
デュアルスタック	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv4	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv6	IPv6	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv4	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv4	IPv4	IPv6	電話は CAPF に接続できません。
IPv6	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv6	IPv6	IPv4	電話は CAPF に接続できません。

表 *2 : 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。IPv6 アドレスでは接続できない場合、電話は 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	電話は IPv4 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
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	電話は CAPF に接続できません。
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。
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	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	電話は CAPF に接続できません。

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
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。

CAPF システム インタラクションと要件

CAPF には次の要件が存在します。

- CAPF を使用する前に、Cisco CTL クライアントのインストールと設定に必要なすべてのタスクを実行したことを確認します。CAPF を使用するには、最初のノードで Cisco Certificate Authority Proxy Function サービスをアクティブにする必要があります。
- 証明書のアップグレードまたはインストール中に、電話の CAPF 認証方式が [By Authentication String] である場合は、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。
- 多く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。
- 証明書操作の全期間を通じて、最初のノードが正常に実行されていることを確認します。
- 証明書操作の全期間を通じて、電話が正常に機能していることを確認します。
- セキュアな電話が別のクラスタに移動されると、Cisco 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、[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）。[Phone Configuration] ウィンドウの [CAPF] セクションにある [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。

ヒント Cisco IP Telephony の Backup And Restore System（BARS）によって CAPF のデータがバックアップされ、レポートされます。これは、情報が Cisco Unified Communications Manager によって Cisco Unified Communications Manager データベースに保存されるためです。

Cisco Unified Serviceability での CAPF の設定

Cisco Unified Serviceability で次の作業を行います。

- Cisco Certificate Authority Proxy Function サービスを有効にします。
- CAPF のトレースを設定します。

詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

CAPF のセットアップ

ローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングするには、次の作業を実行します。

手順

ステップ 1 ローカルで有効な証明書が電話に存在するかどうかを確認します。

CAPF データを Unified Communications Manager パブリッシャ データベース サーバにコピーする必要があるかどうかを確認します。音声品質メトリックへのアクセス方法の詳細については、電話機モデルの『*Cisco Unified IP Phone* アドミニストレーション ガイド』を参照してください。

。

ヒント Unified Communications Manager 4.0 で CAPF ユーティリティを使用していて、CAPF データが Unified Communications Manager データベースに存在することを確認した場合は、Unified Communications Manager 4.0 で使用していた CAPF ユーティリティを削除できます。

ステップ 2 Cisco Certificate Authority Proxy Function サービスが実行されていることを確認します。

ヒント このサービスは、すべての CAPF 操作時に実行されている必要があります。また、このサービスは CTL ファイルに CAPF 証明書を組み込むために、Cisco CTL クライアントでも実行されている必要があります。

ステップ 3 Cisco CTL クライアントのインストールおよび設定に必要なすべての作業を実行したことを確認します。CAPF 証明書が Cisco CTL ファイル内に存在することを確認します。

ステップ 4 必要に応じて、CAPF サービス パラメータを更新します。

ステップ 5 電話でローカルで有効な証明書をインストール、アップグレード、またはトラブルシューティングするには、[Unified Communications Manager Administration] を使用します。

ステップ 6 証明書の操作に認証文字列が必要な場合は、それを電話に入力します。

Certificate Authority Proxy Function サービスの有効化

Cisco Unified Communications Manager は Cisco Unified Serviceability の Certificate Authority Proxy Function サービスを自動でアクティブにしません。

Cisco CTL クライアントをインストールして設定する前に、このサービスをアクティブにしなかった場合、CTL ファイルを更新する必要があります。このサービスは、最初のノードだけで有効化してください。

このサービスを有効化するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Serviceability で、**[Tools]** > **[Service Activation]** を選択します。

ステップ 2 [Server] ドロップダウン リスト ボックスから、Certificate Authority Proxy Function サービスを有効にするサーバを選択します。

ステップ 3 [Enable Certificate Authority Proxy Function] チェックボックスをオンにします。

ステップ 4 **[保存 (Save)]** をクリックします。

CAPF サービス パラメータの更新

[CAPF Service Parameter] ウィンドウには、証明書の有効年数、システムによるキー生成の最大再試行回数などの情報が表示されます。

CAPF サービス パラメータのステータスが [Cisco Unified Communications Manager Administration] でアクティブとして表示されるようにするには、Certificate Authority Proxy Function サービスをアクティブにする必要があります。

CAPF サービス パラメータを更新するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communications Manager Administration] で、**[System]** > **[Service Parameters]** を選択します。

ステップ 2 [Server] ドロップダウン リスト ボックスからサーバを選択します。

ヒント クラスタ内の最初のノードを選択する必要があります。

ステップ 3 [Service] ドロップダウン リスト ボックスで、[Cisco Certificate Authority Proxy Function] サービスを選択します。

ステップ 4 パラメータごとに表示されるヘルプの説明に従い、CAPF サービス パラメータを更新します。

（注） CAPF サービス パラメータのヘルプを表示するには、疑問符またはパラメータ名リンクをクリックします。

ステップ 5 変更内容を有効にするには、Cisco Certificate Authority Proxy Function サービスを再起動します。

サードパーティ CA 署名付き LSC の生成とインポート

CAPF LSC はローカルで署名されています。しかし、電話がサードパーティ CA 署名付き LSC を使用しなければいけないようにすることもできます。

（注） ステップ 1 と 2 を一度実行し、電話での必要な LSC 操作をすべて設定するまで残りの手順を繰り返します。

手順

ステップ 1 Unified Communications Manager の信頼ストアにサードパーティ CA 証明書をインポートします。

ステップ 2 サービス パラメータ Certificate Issuer to Endpoint を設定するには、次の手順に従います。

a) Cisco Unified CM Administration で、**[System]** > **[Service Parameters]** を選択します。
b) ドロップダウン リスト ボックスから Unified Communications Manager サーバを選択します。
c) [Service] ドロップダウン リスト ボックスで、[Cisco Certificate Authority Proxy Function] を選択します。
d) サービス パラメータ Certificate Issuer to Endpoint で、[Offline CA] を選択します。

ステップ 3 CSR 生成の進捗状況を調べます。電話の再登録後、CLI コマンド **utils capf csr count** を使用して、CSR が生成されているかどうかを調べます。

ステップ 4 CLI コマンド **utils capf csr dump** を使用して、CSR を任意の場所（FTP や TFTP を介してローカル ディレクトリまたはリモート ディレクトリ）にダンプします。
アップロードする前に CLI tar 処理で CSR を圧縮して 1 つのファイル（`.tgz`）にまとめます。

ステップ 5 すべての署名付き証明書が CA によって提供されたら、Linux コマンド **`tar cvzf <filename.tgz> *.der`** を使用して、すべての証明書を 1 つのファイルに圧縮します。

ステップ 6 証明書を Unified Communications Manager にインポートするには、CLI コマンド **utils capf cert import** を使用します。

（注） インポートされた証明書は DER 形式である必要があり、フラット ファイル構造で tar 処理する必要があります。

CLI コマンド untar がファイルを元に戻して、各証明書を解析し確認します。証明書が有効であれば、証明書が電話に送信され、対応する CSR が削除されます。

次のタスク

以前に作成してインポートした CSR と証明書をすべて削除するには、コマンド **utils capf csr delete** を使用できます。

CAPFを使用した電話での証明書のインストール、アップグレード、トラブルシューティング、または削除

Certificate Authority Proxy Function を使用するには、次の手順を実行します。

手順

ステップ 1 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、電話を検索します。

ステップ 2 検索結果が表示されたら、証明書をインストール、アップグレード、削除、トラブルシューティングする電話を探し、その電話の [Device Name (Line)] リンクをクリックします。

ステップ 3 表 3 : CAPF の設定 （12 ページ）の説明に従って設定値を入力します。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 [リセット（Reset）] をクリックします。

CAPF の設定

[Cisco Unified Communications Manager Administration] の [Phone Configuration] ウィンドウの CAPF 設定について、次の表で説明します。

表 *3 : CAPF* の設定

設定	説明
[Certificate Operation]	ドロップダウンリストボックスから、次のいずれかのオプションを選択します。 • [No Pending Operation]：証明書の操作が行われない場合に表示されます。（デフォルト設定） • [Install/Upgrade]：電話に新しい証明書をインストールするか、既存のローカルで有効な証明書をアップグレードします。 • [Delete]：電話に存在するローカルで有効な証明書を削除します。 • [Troubleshoot]：ローカルで有効な証明書（LSC）または製造元でインストールされる証明書（MIC）を取得し、CAPF トレース ファイルで証明書クレデンシャルを表示できます。電話に両方の証明書タイプが存在する場合、Cisco Unified Communications Manager は、証明書のタイプごとに 1 つずつ、2 つのトレース ファイルを作成します。 **ヒント** [Troubleshoot] オプションを選択して、電話に LSC または MIC が存在することを確認できます。証明書が電話に存在しない場合は、[Delete] と [Troubleshoot] オプションは表示されません。
[Authentication String]	[By Authentication String] オプションを選択した場合、このフィールドが適用されます。手動で文字列を入力するか、[Generate String] ボタンをクリックして、文字列を生成します。文字列が 4 ～ 10 桁であることを確認します。 ローカルで有効な証明書のインストール、アップグレード、トラブルシューティングを行うには、電話のユーザまたは管理者が電話に認証文字列を入力する必要があります。

設定	説明
[Generate String]	CAPF が自動的に認証文字列を生成するよう設定するには、このボタンをクリックします。4 ～ 10 桁の認証文字列が [Authentication String] フィールドに表示されます。
[Key Order]	このフィールドは、CAPF のキーの並び方を指定します。ドロップダウン リストから、次のいずれかの値を選択します。 • **[RSA Only]** • **[EC Only]** • **[EC Preferred, RSA Backup]** （注） [Key Order]、[RSA Key Size]、および [EC Key Size] フィールドの値に基づいて電話を追加すると、デバイスセキュリティプロファイルがその電話に関連付けられます。値 [EC Only] を選択し、[EC Key Size] の値を [256] ビットにすると、デバイスセキュリティ プロファイルには値 **EC-256** が付加されます。
[RSA Key Size (Bits)]	ドロップダウン リスト ボックスから、[512]、[1024]、または [2048] のいずれかの値を選択します。
[EC Key Size (Bits)]	ドロップダウン リスト ボックスから、[256]、[384]、または [521] のいずれかの値を選択します。
[Operation Completes by]	このフィールドは操作を完了する必要がある期限の日時を指定します。このフィールドはすべての証明書操作オプションに対応しています。 表示される値は、最初のノードに適用されます。

設定	説明
[Operation Status]	このフィールドには、証明書操作の進行状況が表示されます。たとえば、[<operation type> pending]、[<operation type> failed]、または [<operation type> successful] が表示されます。この operation type は [Install/Upgrade]、[Delete]、または [Troubleshoot] 証明書操作オプションです。このフィールドに表示される情報は変更できません。

LSC ステータスまたは認証文字列による電話の検索

証明書の操作ステータスまたは認証文字列に基づいて電話を検索するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] で、**[デバイス（Device）] > [電話（Phone）]** を選択します。

[Find and List] ウィンドウが表示されます。このウィンドウには、アクティブな（以前の）照会のレコードも表示されることがあります。

ステップ 2 最初のドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。

a) [LSC Status]：このオプションを選択すると、ローカルで有効な証明書のインストール、アップグレード、削除、またはトラブルシューティングに CAPF を使用する電話のリストを返します。

b) [Authentication String]：このオプションを選択すると、[Authentication String] フィールドで指定された認証文字列を持つ電話のリストを返します。

ステップ 3 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。

ステップ 4 必要に応じて、適切な検索テキストを指定します。

（注） 検索条件をさらに追加するには、[+] ボタンをクリックします。 条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[Clear Filter] ボタンをクリックします。

ステップ 5 [検索（Find）] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

ステップ 6 表示されるレコードのリストから、表示するレコードへのリンクをクリックします。

（注） ソート順を逆にするには、リストのヘッダーにある上向き矢印または下向き矢印をクリックします。

ウィンドウに選択した項目が表示されます。

CAPF レポートの生成

必要に応じて、証明書の操作ステータス、認証文字列、セキュリティプロファイル、認証モードなどを表示するCAPF レポートを生成できます。このレポートには、デバイス名、デバイスの説明、セキュリティ プロファイル、認証文字列、認証モード、LSC ステータスなどの情報が含まれます。

CAPF レポートを生成するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communications Manager Administration] で、**[Device]** > **[Phone]** を選択します。

[Find/List] ウィンドウが表示されます。このウィンドウには、アクティブな（以前の）照会のレコードも表示されることがあります。

ステップ 2 データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 （15 ページ） に進みます。

レコードをフィルタまたは検索するには、次の手順を実行します。

a) 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
b) 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

（注） 検索条件をさらに追加するには、[+] ボタンをクリックします。 条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[Clear Filter] ボタンをクリックします。

ステップ 3 [検索（Find）] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

ステップ 4 [Related Links] ドロップダウン リスト ボックスで、[CAPF Report in File] を選択し、[Go] をクリックします。

ステップ 5 ファイルを覚えやすい場所に保存します。

ステップ 6 .csv ファイルを開くには、Microsoft Excel を使用します。

電話の認証文字列の入力

[By Authentication String] モードを選択し、認証文字列を生成した場合に、ローカルで有効な証明書をインストールするには、電話で認証文字列を入力する必要があります。

ヒント 認証文字列は 1 回だけ使用できます。[Phone Configuration] ウィンドウまたは CAPF レポートに表示される認証文字列を確認します。

始める前に

電話で認証文字列を入力する前に、次の条件が満たされていることを確認してください。

- CTL ファイルに CAPF 証明書が存在すること。
- Cisco Certificate Authority Proxy Function サービスがアクティブになっていること。
- 最初のノードが機能しており、実行されていること。証明書のインストールごとにサーバが稼働していることを確認します。
- デバイスが登録されていること。
- 電話に署名付きイメージが存在すること。ご使用の電話モデルに対応する Cisco IP Phone の管理マニュアルを参照してください。

手順

ステップ 1 電話機の **[アプリケーション (Applications)]** ボタンを押します。

ステップ 2 設定がロックされている場合は、[**#]（アスタリスク、アスタリスク、ポンド記号）を押してロック解除します。

ステップ 3 [Settings] メニューを下にスクロールします。「[Security Configuration]」 を強調表示して、**[Select]** ソフトキーを押します。

ステップ 4 [Security Configuration] メニューを下にスクロールします。「[LSC]」 を強調表示して、**[Update]** ソフトキーを押します。

ステップ 5 認証文字列の入力を求められたら、システムが提供する文字列を入力して、[Submit] ソフトキーを押します。

現在の CAPF 設定に応じて、電話は証明書をインストール、更新、削除、またはフェッチします。

電話に表示されるメッセージを確認して、証明書動作の進捗をモニタできます。**[Submit]** を押すと、「「Pending」」というメッセージが LSC オプションの下に表示されます。電話によって公開キーと秘密キーのペアが生成され、電話に情報が表示されます。電話でプロセスが正常に完了すると、電話に正常完了のメッセージが表示されます。電話に失敗のメッセージが表示

された場合は、入力した認証文字列が誤っていたか、または電話をアップグレードできるように設定されていません。

[Stop] オプションを選択すると、プロセスをいつでも停止できます。

電話の認証文字列の確認

[**アプリケーション (Applications)**] ボタンを押し、[**モデル情報 (Information)**] メニューを選択することで、証明書が電話機にインストールされていることを確認できます。