CHAPTER 21

CTI、JTAPI、および TAPI の認証と暗号化の設定

この章では、CTI、JTAPI、および TAPI アプリケーションを保護する方法について簡単に説明します。また、CTI、TAPI、および JTAPI アプリケーションの認証と暗号化を設定するために、Cisco Unified Communications Manager の管理で実行する必要がある作業についても説明します。

このマニュアルでは、Cisco Unified Communications Manager の管理で使用できる Cisco JTAPI または TSP プラグインのインストール方法や、インストール中にセキュリティ パラメータを設定する方法については説明していません。同じく、このマニュアルでは、CTI 制御デバイスまたは回線に制限を設定する方法も説明しません。

この章は、次の内容で構成されています。

CTI、JTAPI、および TAPI アプリケーションの認証について

Cisco Unified Communications Manager を使用して、CTIManager と CTI/JTAPI/TAPI アプリケーションとの間のシグナリング接続およびメディア ストリームを保護できます。

ヒント　次の情報では、Cisco JTAPI/TSP プラグインのインストール中にセキュリティ設定を定義したことを前提としています。また、Cisco CTL クライアントでクラスタ セキュリティ モードが混合モードに設定されていることを前提としています。この章で説明する作業を実行するときに、これらの設定が定義されていない場合、CTIManager とアプリケーションは、非セキュア ポートであるポート 2748 で接続されます。

CTIManager およびアプリケーションは、相互に認証された TLS ハンドシェイク（証明書交換）によって他方の ID を確認します。TLS 接続が確立されると、CTIManager およびアプリケーションは、TLS ポート、ポート 2749 を介して QBE メッセージを交換します。

アプリケーションとの認証を行うために、CTIManager は、Cisco Unified Communications Manager 証明書（インストール時に Cisco Unified Communications Manager サーバに自動的にインストールされる自己署名証明書、またはプラットフォームにアップロードされたサードパーティの CA 署名付き証明書）を使用します。Cisco CTL クライアントをインストールして CTL ファイルを生成した後、この証明書は CTL ファイルに自動的に追加されます。アプリケーションは、CTIManager への接続を試行する前に、TFTP サーバから CTL ファイルをダウンロードします。

JTAPI/TSP クライアントは、初めて CTL ファイルを TFTP サーバからダウンロードするときに CTL ファイルを信頼します。JTAPI/TSP クライアントは CTL ファイルを検証しないため、ダウンロードはセキュアな環境で実行することを強く推奨します。後続の CTL ファイルのダウンロードは、JTAPI/TSP クライアントで確認されます。たとえば、CTL ファイルの更新後、JTAPI/TSP クライアントは、CTL ファイルのセキュリティ トークンを使用して、ダウンロードした新しい CTL ファイルのデジタル署名を認証します。ファイルの内容には、Cisco Unified Communications Manager 証明書と CAPF サーバ証明書が含まれます。

CTL ファイルが侵害されていると判断された場合、JTAPI/TSP クライアントはダウンロードした CTL ファイルを置き換えません。クライアントはエラーをログに記録し、既存の CTL ファイルにある古い証明書を使用して、TLS 接続の確立を試行します。CTL ファイルが変更または侵害されている場合、正常に接続できない可能性があります。CTL ファイルのダウンロードに失敗し、複数の TFTP サーバが存在する場合、「Cisco CTL クライアントの設定」（P.4-1）で説明するように、別の TFTP サーバでファイルをダウンロードするように設定できます。JTAPI/TAPI クライアントは、次の条件下では、どのポートにも接続しません。

- 何らかの理由でクライアントが CTL ファイルをダウンロードできない（CTL ファイルが存在しないなど）。
- クライアントに既存の CTL ファイルがない。
- アプリケーション ユーザをセキュア CTI ユーザとして設定した。

CTIManager との認証を行うために、アプリケーションは、Certificate Authority Proxy Function（CAPF）が発行する証明書を使用します。アプリケーションと CTIManager とのすべての接続で TLS を使用するには、アプリケーション PC で実行されるインスタンスごとに一意の証明書が必要です。1 つの証明書ですべてのインスタンスがカバーされるわけではありません。Cisco IP Manager Assistant サービスを実行しているノードに証明書がインストールされるようにするには、表 21-2 の説明に従い、Cisco Unified Communications Manager の管理でそれぞれのアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルに一意のインスタンス ID を設定します。

ヒント　アプリケーションをある PC からアンインストールして別の PC にインストールする場合、新しい PC の各インスタンスに対して新しい証明書をインストールする必要があります。

また、アプリケーションの TLS を有効にするには、Cisco Unified Communications Manager の管理でアプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加する必要があります。ユーザをこのグループに追加し、証明書をインストールすると、アプリケーションはユーザを TLS ポート経由で接続させます。

CTI、JTAPI、および TAPI アプリケーションの暗号化について

ヒント　認証は、暗号化の最小要件です。つまり、認証を設定していない場合、暗号化は使用できません。

Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco WebDialer は暗号化をサポートしていません。CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポートすることがあります。

アプリケーションと CTIManager の間のメディア ストリームを安全にするには、Cisco Unified Communications Manager の管理でアプリケーション ユーザまたはエンド ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加します。これらのユーザが Standard CTI Secure Connection ユーザ グループにも存在する場合や、クラスタ セキュリティ モードが混合モードと等しい場合、CTIManager はアプリケーションとの TLS 接続を確立し、メディア イベント内でアプリケーションに鍵関連情報を提供します。

（注）　クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

アプリケーションは SRTP 鍵関連情報を記録または格納しませんが、鍵関連情報を使用して RTP ストリームを暗号化し、CTIManager からの SRTP ストリームを復号化します。

何らかの理由でアプリケーションが非セキュア ポートであるポート 2748 に接続した場合、CTIManager は鍵関連情報を送信しません。制限を設定しなかったために CTI/JTAPI/TAPI がデバイスまたはディレクトリ メンバーを監視または制御できない場合、CTIManager は鍵関連情報を送信しません。

ヒント　アプリケーションで SRTP セッション鍵を受信するには、アプリケーション ユーザまたはエンド ユーザが Standard CTI Enabled、Standard CTI Secure Connection、および Standard CTI Allow Reception of SRTP Key Material の 3 つのグループに存在する必要があります。

Cisco Unified Communications Manager は、CTI ポートおよびルート ポイントで送受信されるセキュア コールを円滑にしますが、アプリケーションがメディア パラメータを処理するため、アプリケーションがセキュア コールをサポートするように設定する必要があります。

CTI ポートやルート ポイントは、ダイナミック登録またはスタティック登録で登録されます。ポートやルート ポイントがダイナミック登録を使用する場合、メディア パラメータはコールごとに指定されます。スタティック登録の場合、メディア パラメータは登録時に指定され、コールごとに変更することはできません。CTI ポートやルート ポイントが TLS 接続を介して CTIManager に登録される場合、デバイスは安全に登録されます。このとき、アプリケーションが有効な暗号化アルゴリズムを使用し、相手がセキュアであれば、メディアは SRTP で暗号化されます。

CTI アプリケーションが、すでに確立されているコールの監視を開始するとき、アプリケーションは RTP イベントを受信しません。確立されたコールに対して、CTI アプリケーションは、コールのメディアがセキュアか非セキュアかを定義する DeviceSnapshot イベントを提供します。このイベントには、鍵関連情報は含まれません。

CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要

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 CTI/TAPI/TAPI アプリケーション用のタスクを実行します。

- 認証文字列によって JTAPI/TSP クライアントを認証する。
- CTI/JTAPI/TAPI アプリケーション ユーザまたはエンド ユーザに、ローカルで有効な証明書（LSC）を発行する。
- 既存のローカルで有効な証明書をアップグレードする。
- 証明書を表示およびトラブルシューティングするために取得する。

JTAPI/TSP クライアントが CAPF と相互に作用するとき、クライアントは認証文字列を使用して CAPF を認証します。次に、クライアントは公開鍵と秘密鍵のペアを生成し、署名付きメッセージで公開鍵を CAPF サーバに転送します。秘密鍵はそのままクライアントに残り、外部に公開されることはありません。CAPF は、証明書に署名し、その証明書を署名付きメッセージでクライアントに返送します。

[アプリケーションユーザ CAPF プロファイルの設定 (Application User CAPF Profile Configuration)] ウィンドウまたは [エンドユーザ CAPF プロファイルの設定 (End User CAPF Profile Configuration)] ウィンドウで設定内容を設定し、それぞれ、アプリケーション ユーザまたはエンド ユーザに証明書を発行します。次に、Cisco Unified Communications Manager がサポートする CAPF プロファイルの違いについて説明します。

- アプリケーション ユーザ CAPF プロファイル : このプロファイルを使用すると、ローカルで有効な証明書を発行して、アプリケーション ユーザの安全を確保することができます。これによって、CTIManager サービスとアプリケーションの間で TLS 接続が開かれます。

  1 つのアプリケーション ユーザ CAPF プロファイルが、サーバのサービスまたはアプリケーションの 1 つのインスタンスに対応します。同じサーバで複数の Web サービスまたはアプリケーションをアクティブにする場合は、サーバのサービスごとに 1 つずつ、合計 2 つのアプリケーション ユーザ CAPF プロファイルを設定する必要があります。

  クラスタ内の 2 つのサーバでサービスまたはアプリケーションをアクティブにする場合は、サーバごとに 1 つずつ、合計 2 つのアプリケーション ユーザ CAPF プロファイルを設定する必要があります。

- エンド ユーザ CAPF プロファイル : このプロファイルを使用すると、CTI クライアントにローカルで有効な証明書を発行することができます。これによって、CTI クライアントが TLS 接続を介して CTIManager サービスと通信できるようになります。

ヒント　JTAPI クライアントは LSC を Java Key Store 形式で、JTAPI の初期設定ウィンドウで設定したパスに格納します。TSP クライアントは LSC を暗号化形式で、デフォルト ディレクトリまたは設定したパスに格納します。

次の情報は、通信または電源の障害が発生した場合に適用されます。

- 証明書をインストールしているときに通信障害が発生すると、JTAPI クライアントは 30 秒間隔であと 3 回、証明書を取得しようとします。この値は設定することができません。

  TSP クライアントの場合は、再試行回数と再試行タイマーを設定できます。これらの値は、TSP クライアントが一定の時間内に証明書の取得を試行する回数を指定することで設定します。どちらの値も、デフォルトは 0 です。最大 3 回の再試行回数を設定でき、1（1 回だけ再試行）、2、または 3 を指定します。それぞれについて、再試行の時間を 30 秒以下で設定できます。

- JTAPI/TSP クライアントが 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、クライアントは電源が復帰した後で、証明書のダウンロードを試行します。

CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの相互作用および要件

CAPF には、次の要件があります。

- アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルを設定する前に、Cisco CTL クライアントをインストールして設定するために必要なすべての作業を実行したことを確認します。[エンタープライズパラメータ設定(Enterprise Parameters Configuration)] ウィンドウの Cluster Security Mode が 1（混合モード）であることを確認してください。
- 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。
- 同時に多数の証明書が生成されると、コール処理が中断される場合があるため、スケジューリングされたメンテナンス画面で CAPF を使用することを強く推奨します。
- 証明書操作の間、最初のノードが実行中で正しく機能していることを確認します。
- 証明書操作の間、CTI/JTAPI/TAPI アプリケーションが正しく機能していることを確認します。

CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト

表 21-1 に、CTI/JTAPI/TAPI アプリケーションを保護するために実行する作業のリストを示します。

表 21-1　CTI/JTAPI/TAPI のセキュリティ設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	CTI アプリケーションおよびすべての JTAPI/TSP プラグインがインストールされ、実行中であることを確認します。 **ヒント** アプリケーション ユーザは Standard CTI Enabled グループに割り当てます。	• 『*Cisco Unified Communications Manager システム ガイド*』の「コンピュータ テレフォニー統合」 • 『*Cisco JTAPI Installation Guide for Cisco Unified Communications Manager*』 • 『*Cisco TAPI Installation Guide for Cisco Unified Communications Manager*』 • 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』

表 21-1　CTI/JTAPI/TAPI のセキュリティ設定用チェックリスト （続き）

設定手順		関連手順および関連項目
ステップ 2	次の Cisco Unified Communications Manager セキュリティ機能がインストールされていることを確認します（インストールされていない場合は、これらの機能をインストールして設定します）。 • CTL ファイルが作成されるように、CTL クライアントがインストールされ、CTL ファイルが実行されていることを確認します。 • CTL プロバイダー サービスがインストールされ、サービスがアクティブであることを確認します。 • CAPF サービスがインストールされ、サービスがアクティブであることを確認します。必要に応じて、CAPF サービス パラメータを更新します。 **ヒント** CAPF 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 クライアントで実行されている必要があります。電話機で CAPF を使用したときにこれらのパラメータを更新した場合は、ここでパラメータを更新する必要はありません。 • クラスタ セキュリティ モードが混合モードに設定されていることを確認します （クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します）。 **ヒント** クラスタ セキュリティ モードが混合モードでない場合、CTI/JTAPI/TAPI アプリケーションは CTL ファイルにアクセスできません。	• 「Cisco CTL クライアントの設定」（P.4-1） • 「CAPF サービス パラメータの更新」（P.21-9） • 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』
ステップ 3	CTIManager およびアプリケーションで TLS 接続を使用する場合は、アプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加します。 **ヒント** CTI アプリケーションは、アプリケーション ユーザまたはエンド ユーザに割り当てることができますが、両方に割り当てることはできません。	「セキュリティ関連ユーザ グループへのアプリケーション ユーザとエンド ユーザの追加」（P.21-7）
ステップ 4	SRTP を使用する場合は、Standard CTI Allow Reception of SRTP Key Material ユーザ グループにアプリケーション ユーザまたはエンド ユーザを追加します。 ユーザはすでに Standard CTI Enabled および Standard CTI Secure Connection ユーザ グループに存在している必要があります。これらの 3 つのグループに存在しないアプリケーション ユーザまたはエンド ユーザは、SRTP セッション鍵を受信できません。 Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco WebDialer は暗号化をサポートしていません。CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポートすることがあります。	「セキュリティ関連ユーザ グループへのアプリケーション ユーザとエンド ユーザの追加」（P.21-7） 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「権限の設定」

表 21-1　CTI/JTAPI/TAPI のセキュリティ設定用チェックリスト （続き）

設定手順		関連手順および関連項目
ステップ 5	Cisco Unified Communications Manager の管理でアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを設定します。	• 「CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要」（P.21-4） • 「アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの設定」（P.21-11） • 「アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの CAPF 設定ウィンドウ」（P.21-12）
ステップ 6	CTI/JTAPI/TAPI アプリケーションの対応するセキュリティ関連パラメータを有効にします。	「JTAPI/TAPI セキュリティ関連サービス パラメータ」（P.21-14）

セキュリティ関連ユーザ グループへのアプリケーション ユーザとエンド ユーザの追加

Standard CTI Secure Connection ユーザ グループおよび Standard CTI Allow Reception of SRTP Key Material ユーザ グループは、デフォルトで Cisco Unified Communications Manager の管理に表示されます。これらのグループは削除できません。

CTIManager へのユーザ接続の安全を確保にするには、アプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加する必要があります。CTI アプリケーションは、アプリケーション ユーザまたはエンド ユーザに割り当てることができますが、両方に割り当てることはできません。

アプリケーションおよび CTIManager でメディア ストリームを保護するには、アプリケーション ユーザまたはエンド ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加する必要があります。

アプリケーション ユーザおよびエンド ユーザが SRTP を使用する前に、そのユーザが Standard CTI Enabled ユーザ グループおよび Standard CTI Secure Connection ユーザ グループに存在している必要があります。これが、TLS の基本設定になります。SRTP 接続には TLS が必要です。ユーザがこれらのグループに存在する場合、ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加できます。アプリケーションで SRTP セッション鍵を受信するには、アプリケーション ユーザまたはエンド ユーザが Standard CTI Enabled、Standard CTI Secure Connection、および Standard CTI Allow Reception of SRTP Key Material の 3 つのグループに存在する必要があります。

Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco WebDialer は暗号化をサポートしないため、アプリケーション ユーザである CCMQRTSecureSysUser、IPMASecureSysUser、および WDSecureSysUser を Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加する必要はありません。

ヒント　ユーザ グループからのアプリケーション ユーザまたはエンド ユーザの削除については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。[権限の設定 (Role Configuration)] ウィンドウでのセキュリティ関連の設定については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[ユーザ管理(User Management)] > [ユーザグループ(User Groups)] の順に選択します。

ステップ 2　すべてのユーザ グループを表示するには、[検索(Find)] をクリックします。

ステップ 3　目的に応じて、次のいずれかを実行します。

- アプリケーション ユーザまたはエンド ユーザが Standard CTI Enabled グループに存在することを確認する。
- [Standard CTI Secure Connection] リンクをクリックして、アプリケーション ユーザまたはエンド ユーザを Standard CTI Secure Connection ユーザ グループに追加する。
- [Standard CTI Allow Reception of SRTP Key Material] リンクをクリックして、アプリケーション ユーザまたはエンド ユーザを Standard CTI Allow Reception of SRTP Key Material ユーザ グループに追加する。

ステップ 4　アプリケーション ユーザをグループに追加するには、ステップ 5 ～ステップ 7 を実行します。

ステップ 5　[グループにアプリケーションユーザを追加(Add Application Users to Group)] ボタンをクリックします。

ステップ 6　アプリケーション ユーザを検索するには、検索条件を指定し、[検索(Find)] をクリックします。

検索条件を指定せずに [検索(Find)] をクリックすると、使用可能なすべてのオプションが表示されます。

ステップ 7　グループに追加するアプリケーション ユーザのチェックボックスをオンにして、[選択項目の追加(Add Selected)] をクリックします。

[ユーザグループの設定 (User Group Configuration)] ウィンドウにユーザが表示されます。

ステップ 8　エンド ユーザをグループに追加するには、ステップ 9 ～ステップ 11 を実行します。

ステップ 9　[グループにエンドユーザを追加(Add End Users to Group)] ボタンをクリックします。

ステップ 10　エンド ユーザを検索するには、検索条件を指定し、[検索(Find)] をクリックします。

検索条件を指定せずに [検索(Find)] をクリックすると、使用可能なすべてのオプションが表示されます。

ステップ 11　グループに追加するエンド ユーザのチェックボックスをオンにして、[選択項目の追加(Add Selected)] をクリックします。

[ユーザグループの設定 (User Group Configuration)] ウィンドウにユーザが表示されます。

追加情報

「関連項目」（P.21-15）を参照してください。

Certificate Authority Proxy Function サービスのアクティブ化

Cisco Unified Communications Manager は、Cisco Unified サービスアビリティで Certificate Authority Proxy Function サービスを自動的にはアクティブ化しません。Certificate Authority Proxy Function サービスのアクティブ化については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

CAPF 機能を使用するには、最初のノードでこのサービスをアクティブにする必要があります。

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は、「CTL ファイルの更新」（P.4-13）の説明に従って CTL ファイルを更新する必要があります。

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF に固有の鍵ペアおよび証明書が CAPF によって自動生成されます。CAPF 証明書は Cisco CTL クライアントによってスタンドアロン サーバまたはクラスタ内のすべてのサーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、Cisco Unified Communications オペレーティング システムの GUI で、CAPF 証明書を表示します。

CAPF サービス パラメータの更新

CAPF サービスのパラメータを設定するウィンドウには、証明書の有効年数、システムによる鍵生成の最大再試行回数、鍵のサイズなどの情報が表示されます。

Cisco Unified Communications Manager の管理で CAPF サービス パラメータをアクティブとして表示するには、Cisco Unified サービスアビリティで Certificate Authority Proxy Function サービスをアクティブ化する必要があります。

ヒント　電話機で CAPF を使用したときに CAPF サービス パラメータを更新した場合は、ここでサービス パラメータを更新する必要はありません。

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 の管理ページで、[システム (System)] > [サービスパラメータ (Service Parameters)] 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 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　[サービス (Service)] ドロップダウン リスト ボックスから、Cisco Certificate Authority Proxy Function サービスを選択します。サービス名の横に「Active」と表示されていることを確認します。

ステップ 4　ヘルプの説明に従って、CAPF サービス パラメータを更新します。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 Unified サービスアビリティで Cisco Certificate Authority Proxy Function サービスを再起動する必要があります。

追加情報

「関連項目」（P.21-15）を参照してください。

アプリケーション ユーザまたはエンドユーザの CAPF プロファイルの検索

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルを検索するには、次の手順に従います。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、アクセスするプロファイルに応じて、次のオプションのいずれかを選択します。

- [ユーザ管理 (User Management)] > [アプリケーションユーザ CAPF プロファイル (Application User CAPF Profile)]
- [ユーザ管理 (User Management)] > [エンドユーザ CAPF プロファイル (End User CAPF Profile)]

検索と一覧表示ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

ステップ 2　データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 3 に進みます。

レコードをフィルタリングまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスから、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスから検索パターンを選択します。
- 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、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[–] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 3　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4　レコードのリストで、表示するレコードのリンクをクリックします。

（注）　リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

追加情報

「関連項目」（P.21-15）を参照してください。

アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの設定

JTAPI/TAPI/CTI アプリケーションの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場合は、表 21-2 を参照してください。

ヒント　エンド ユーザ CAPF プロファイルを設定する前に、アプリケーション ユーザ CAPF プロファイルを設定することをお勧めします。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで次のいずれかのオプションを選択します。

- [ユーザ管理 (User Management)] > [アプリケーションユーザ CAPF プロファイル (Application User CAPF Profile)]
- [ユーザ管理 (User Management)] > [エンドユーザ CAPF プロファイル (End User CAPF Profile)]

検索と一覧表示ウィンドウが表示されます。

ステップ 2　次のいずれかを実行します。

- 新しい CAPF プロファイルを追加するには、検索ウィンドウで [新規追加 (Add New)] をクリックします （プロファイルを表示してから、[新規追加 (Add New)] をクリックすることもできます）。設定ウィンドウが表示され、各フィールドのデフォルト設定が示されます。
- 既存のプロファイルをコピーするには、「アプリケーション ユーザまたはエンドユーザの CAPF プロファイルの検索」（P.21-10）の説明に従って適切なプロファイルを見つけ、[コピー (Copy)] 列内にあるそのレコード用の [コピー(Copy)] ボタンをクリックします（プロファイルを表示してから、[コピー (Copy)] をクリックすることもできます）。設定ウィンドウが表示され、表示されたプロファイルからの設定が示されます。
- 既存のエントリを更新するには、「アプリケーション ユーザまたはエンドユーザの CAPF プロファイルの検索」（P.21-10）の説明に従い、適切なプロファイルを見つけて表示します。設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3　表 21-2 の説明に従って、適切な設定を入力します。

ステップ 4　[保存 (Save)] をクリックします。

ステップ 5　セキュリティを使用するアプリケーション ユーザおよびエンド ユーザごとに、この手順を繰り返します。

次の作業

[アプリケーションユーザ CAPF プロファイルの設定 (Application User CAPF Profile Configuration)] ウィンドウで CCMQRTSecureSysUser、IPMASecureSysUser、または WDSecureSysUser を設定する場合は、「JTAPI/TAPI セキュリティ関連サービス パラメータ」（P.21-14）の説明に従って、サービス パラメータを設定する必要があります。

追加情報

「関連項目」（P.21-15）を参照してください。

アプリケーションユーザCAPFプロファイルおよびエンドユーザCAPFプロファイルのCAPF設定ウィンドウ

表 21-2 に、[アプリケーションユーザCAPFプロファイルの設定(Application User CAPF Profile Configuration)] ウィンドウおよび [エンドユーザCAPFプロファイルの設定(End User CAPF Profile Configuration)] ウィンドウでの CAPF 設定を示します。

- 設定のヒントについては、「CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの相互作用および要件」（P.21-5）を参照してください。
- 関連する情報および手順については、「関連項目」（P.21-15）を参照してください。

表 21-2　アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの設定内容

設定	説明
[アプリケーションユーザ(Application User)]	ドロップダウン リスト ボックスから、CAPF オペレーション用のアプリケーション ユーザを選択します。これによって、設定されたアプリケーション ユーザが表示されます。 この設定は、[エンドユーザCAPFプロファイルの設定(End User CAPF Profile Configuration)] ウィンドウには表示されません。
[エンドユーザID (End User Id)]	ドロップダウン リスト ボックスから、CAPF オペレーション用のエンド ユーザを選択します。これによって、設定されたエンド ユーザが表示されます。 この設定は、[アプリケーションユーザ CAPF プロファイルの設定(Application User CAPF Profile Configuration)] ウィンドウには表示されません。
[インスタンスID(Instance Id)]	1 ～ 128 字の英数字（a ～z、A ～ Z、0 ～ 9）を入力します。インスタンス ID は、証明書操作のためユーザを識別します。 1 つのアプリケーションに対して複数の接続（インスタンス）を設定できます。アプリケーションと CTIManager との接続の安全を確保するには、アプリケーション PC（エンド ユーザの場合）またはサーバ（アプリケーション ユーザの場合）で実行されるインスタンスごとに一意の証明書があることを確認します。 このフィールドは、Web サービスおよびアプリケーションをサポートする CAPF Profile Instance ID for Secure Connection to CTIManager サービス パラメータに関係があります。このパラメータにアクセスする方法については、「JTAPI/TAPI セキュリティ関連サービス パラメータ」（P.21-14）を参照してください。
[証明書の操作(Certificate Operation)]	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。 • [保留中の操作なし(No Pending Operation)] : 証明書の操作が発生しないときに表示されます （デフォルトの設定）。 • [インストール / アップグレード(Install/Upgrade)] : アプリケーションのローカルで有効な証明書を新しくインストールするか、あるいは既存の証明書をアップグレードします。

表 21-2　アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの設定内容

設定	説明
[認証モード (Authentication Mode)]	証明書のインストールまたはアップグレード操作の認証モードは [認証ストリング (By Authentication String)] です。これは、ユーザまたは管理者が JTAPI/TSP の初期設定ウィンドウで CAPF 認証文字列を入力したときにだけ、ローカルで有効な証明書がインストール、アップグレード、またはトラブルシューティングされることを意味します。
[認証文字列 (Authentication String)]	一意の文字列を手動で入力するか、あるいは [文字列を生成 (Generate String)] ボタンをクリックして文字列を生成します。 文字列は 4 ～ 10 桁にしてください。 ローカルで有効な証明書をインストールまたはアップグレードするには、アプリケーション PC の JTAPI/TSP の初期設定ウィンドウで、管理者が認証文字列を入力する必要があります。この文字列は、1 回だけ使用できます。あるインスタンスに文字列を使用した場合、その文字列をもう一度使用することはできません。
[文字列を生成 (Generate String)]	CAPF で自動的に認証文字列を生成する場合は、このボタンをクリックします。4 ～ 10 桁の認証文字列が [認証文字列 (Authentication String)] フィールドに表示されます。
[キーサイズ (Key Size、ビット)]	ドロップダウン リスト ボックスから、証明書の鍵のサイズを選択します。デフォルト設定値は 1024 です。これ以外のオプションには、512 と 2048 があります。 鍵生成を低いプライオリティで設定すると、アクションの実行中もアプリケーションの機能を利用できます。鍵生成が完了するまで、30 分以上の時間がかかることがあります。 証明書に 2048 ビットの鍵を選択した場合、アプリケーションと Cisco Unified Communications Manager の間で接続を確立するために、60 秒以上の時間がかかることがあります。最高のセキュリティ レベルを使用する場合を除き、2048 ビットの鍵は設定しないでください。
[操作の完了 (Operation Completes By)]	このフィールドは、すべての証明書操作をサポートし、操作を完了する必要がある期限の日付と時刻を指定します。 表示される値は、最初のノードに適用されます。 この設定は、証明書操作を完了する必要があるデフォルトの日数を指定する CAPF Operation Expires in (days) エンタープライズ パラメータとともに使用します。このパラメータはいつでも更新できます。
[証明書の操作ステータス (Certificate Operation Status)]	このフィールドは、pending、failed、successful など、証明書操作の進行状況を表示します。 このフィールドに表示される情報は変更できません。

アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルの削除

ここでは、アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを Cisco Unified Communications Manager データベースから削除する方法を説明します。

始める前に

Cisco Unified Communications Manager の管理でアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを削除する前に、別のプロファイルをデバイスに適用するか、該当プロファイルを使用するすべてのデバイスを削除してください。該当プロファイルを使用しているデバイスを検索するには、セキュリティプロファイルの設定ウィンドウの [関連リンク (Related Links)] ドロップダウン リスト ボックスから [依存関係レコード (Dependency Records)] を選択して、[移動 (Go)] をクリックします。

システムで依存関係レコード機能が有効になっていない場合は、レコードの [依存関係レコード要約 (Dependency Records Summary)] ウィンドウに、依存関係レコードを有効にすると実行できるアクションを示すメッセージが表示されます。また、依存関係レコード機能を使用すると、CPU 使用率が高くなるという情報も表示されます。依存関係レコードの詳細については、『*Cisco Unified Communications Manager システム ガイド*』を参照してください。

手順

ステップ 1　「アプリケーション ユーザまたはエンドユーザの CAPF プロファイルの検索」（P.21-10）の説明に従い、アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを検索します。

ステップ 2　次の作業のいずれかを実行します。

- 複数のプロファイルを削除するには、検索と一覧表示ウィンドウで、適切なチェックボックスの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。この選択に対するすべての設定可能なレコードを削除するには、[すべてを選択 (Select All)] をクリックしてから [選択項目の削除 (Delete Selected)] をクリックします。
- 単一のプロファイルを削除するには、検索と一覧表示ウィンドウで、適切なプロファイルの横に表示されているチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックします。

ステップ 3　削除操作の確認を要求するプロンプトが表示されたら、[OK] をクリックして削除するか、[キャンセル (Cancel)] をクリックして削除操作を取り消します。

追加情報

「関連項目」（P.21-15）を参照してください。

JTAPI/TAPI セキュリティ関連サービス パラメータ

アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを設定した後、Cisco IP Manager Assistant サービスに対して、次のサービス パラメータを設定する必要があります。

- CTIManager Connection Security Flag
- CAPF Profile Instance ID for Secure Connection to CTIManager

サービス パラメータにアクセスするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、[システム (System)] > [サービスパラメータ (Service Parameters)] 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 ボックスから、Cisco IP Manager Assistant サービスがアクティブになっているサーバを選択します。

ステップ 3　[サービス (Service)] ドロップダウン リスト ボックスから、**Cisco IP Manager Assistant** サービスを選択します。

ステップ 4　パラメータが表示されたら、CTIManager Connection Security Flag パラメータおよび CAPF Profile Instance ID for Secure Connection to CTIManager パラメータを見つけます。

ステップ 5　疑問符またはパラメータ名リンクをクリックすると表示されるヘルプの説明に従い、パラメータを更新します。

ステップ 6　[保存 (Save)] をクリックします。

ステップ 7　サービスがアクティブになっているサーバごとに、この手順を繰り返します。

アプリケーション ユーザまたはエンド ユーザに対する証明書操作のステータスの表示

特定のアプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルの設定ウィンドウ（検索と一覧表示ウィンドウではありません）、または JTAPI/TSP の初期設定ウィンドウで、証明書操作のステータスを表示できます。

参考情報

関連項目

- 「Cisco CTL クライアントの設定」（P.4-1）
- 「CTI、JTAPI、および TAPI アプリケーションの認証について」（P.21-2）
- 「CTI、JTAPI、および TAPI アプリケーションの暗号化について」（P.21-3）
- 「CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要」（P.21-4）
- 「CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの相互作用および要件」（P.21-5）
- 「CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト」（P.21-5）
- 「セキュリティ関連ユーザ グループへのアプリケーション ユーザとエンド ユーザの追加」（P.21-7）
- 「Certificate Authority Proxy Function サービスのアクティブ化」（P.21-8）
- 「CAPF サービス パラメータの更新」（P.21-9）
- 「アプリケーション ユーザまたはエンドユーザの CAPF プロファイルの検索」（P.21-10）
- 「アプリケーション ユーザまたはエンド ユーザの CAPF プロファイルの設定」（P.21-11）
- 「アプリケーション ユーザ CAPF プロファイルおよびエンド ユーザ CAPF プロファイルの CAPF 設定ウィンドウ」（P.21-12）

- 「アプリケーション ユーザ CAPF プロファイルまたはエンド ユーザ CAPF プロファイルの削除」（P.21-14）
- 「JTAPI/TAPI セキュリティ関連サービス パラメータ」（P.21-14）
- 「アプリケーション ユーザまたはエンド ユーザに対する証明書操作のステータスの表示」（P.21-15）

シスコの関連マニュアル

- 『*Cisco JTAPI Installation Guide for Cisco Unified Communications Manager*』
- 『*Cisco TAPI Installation Guide for Cisco Unified Communications Manager*』
- 『*Cisco Unified Communications Manager システム ガイド*』の「コンピュータ テレフォニー統合」
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』