# CTI、JTAPI、および TAPI の認証および暗号化の設定

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の概要を説明します。また、CTI、TAPI、およびJTAPI アプリケーションの認証と暗号化の設定のため、[Unified Communications Manager Administration] で実行する必要がある作業についても説明します。

このドキュメントでは、[Unified Communications Manager Administration] で使用可能な Cisco JTAPI や TSP プラグインのインストール方法は説明しません。また、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も説明しません。同様に、CTI で制御するデバイスまたは回線に制限を設定する方法も、このドキュメントでは説明しません。

# CTI、JTAPI、および TAPI アプリケーションの認証

Unified Communications Manager を使用すれば、CTIManager と CTI/JTAPI/TAPI の各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。

（注） 次の情報は、Cisco JTAPI/TSP プラグインのインストール時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、または CLI コマンド セットの **utils ctl** 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も前提としています。この章で説明する作業を実行する際に、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 ポートのポート 2748 で接続されます。

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

CTIManager では、アプリケーションとの認証を行うために、Unified Communications Manager の証明書（インストール時に 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したサードパーティの CA 署名付き証明書のいずれか）を使用します。

CLI コマンド セットの **utils ctl** または Cisco CTL クライアントによって 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。アプリケーションでは、CTL ファイルを TFTP サーバからダウンロードした後で、CTIManager への接続を試みます。

JTAPI/TSP クライアントでは、初めて CTL ファイルを TFTP サーバからダウンロードする際に CTL ファイルを信頼します。JTAPI/TSP クライアントでは CTL ファイルを検証しないため、この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。JTAPI/TSP クライアントでは、後続の CTL ファイルのダウンロードを検証します。たとえば、CTL ファイルを更新すると、JTAPI/TSP クライアントでは、CTL ファイル内のセキュリティ 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の真正性を認証（確認）します。このファイルの内容には、Unified Communications Manager の証明書と CAPF サーバの証明書が含まれます。

JTAPI/TSP クライアントでは、CTL ファイルが改ざんされていると判断した場合、ダウンロードした CTL ファイルを取り替えません。つまり、クライアントでは、エラーをログに記録し、既存の CTL ファイル内の古い証明書を使用して TLS 接続の確立を試みます。CTL ファイルが変更または改ざんされている場合、正常に接続できないことがあります。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、このファイルをダウンロードするために別の TFTP サーバを設定できます。JTAPI/TAPI クライアントでは、次の場合、どのポートにも接続しません。

- 何らかの理由（CTL ファイルが存在しないなど）によって、クライアントで CTL ファイルをダウンロードできない場合。

- クライアントに既存の CTL ファイルがない場合。
- 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場合。

アプリケーションでは、CTIManager との認証を行うために、Certificate Authority Proxy Function（CAPF）で発行する証明書を使用します。アプリケーションと CTIManager との間のすべての接続で TLS を使用するには、アプリケーションの PC で実行されてい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 サービスが実行され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 1 : アプリケーション ユーザおよびエンド ユーザの CAPF プロファイルの設定 （13 ページ）の説明に従って、[Unified Communications Manager Administration] で、それぞれの [Application User CAPF Profile Configuration] または [End User CAPF Profile Configuration] 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 のインスタンスごとに新しい証明書をインストールする必要があります。

アプリケーションで TLS を有効にするには、[Unified Communications Manager Administration] 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もあります。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、アプリケーションではユーザが TLS ポートを介して接続するようになります。

# CTI、JTAPI、および TAPI アプリケーションの暗号化

ヒント　認証は暗号化の最小要件となります。つまり、認証が設定されなければ、暗号化を使用できません。

Unified Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer 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 クライアントでは、クライアントが音声パケットを送信する場合、暗号化がサポートされることがあります。

アプリケーションと CTIManager との間のメディア ストリームをセキュアにするため、Unified Communications Manager Administration の [標準 CTI に SRTP キー情報の受け入れを許可（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。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、およびクラスタ セキュリティ モードが混合モードである場合、CTIManager はアプリケーションとの TLS 接続を確立し、メディア イベントでキー情報をアプリケーションに提供します。

（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能力を設定します。

アプリケーションでは SRTP キー情報の記録や保存は行われませんが、アプリケーションはキー情報を使用して RTP ストリームを暗号化し、CTIManager からの SRTP ストリームを復号します。

アプリケーションが非セキュア ポートであるポート 2748 に何らかの理由で接続されると、CTIManager はキー情報を送信しません。制限が設定されているために CTI/JTAPI/TAPI からデバイスまたは電話番号のモニタリングや制御が行えない場合、CTIManager はキー情報を送信しません。

ヒント SRTP セッション キーを受け取るアプリケーションの場合、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、Standard CTI Allow Reception of SRTP Key Material の 3 グループに存在している必要があります。

Unified Communications Manager では CTI ポートおよびルート ポイントとのセキュア コールを使用できますが、メディア パラメータはアプリケーションによって扱われるため、セキュア コールをサポートするようアプリケーションを設定する必要があります。

CTI ポートおよびルート ポイントは、ダイナミック登録またはスタティック登録によって登録されます。ポート/ルート ポイントによってダイナミック登録が使用されると、各コールに対してメディア パラメータが指定されます。スタティック登録が使用されると、メディア パラメータは登録時に指定され、コールごとに変更できません。CTI ポート/ルート ポイントが TLS 接続を介して CTIManager に登録するとき、デバイスはセキュアに登録され、アプリケーションがデバイス登録要求で有効な暗号化アルゴリズムを使用する場合、および他の参加者がセキュアである場合、メディアは SRTP を介して暗号化されます。

CTI アプリケーションは、すでに確立されているコールのモニタリングを開始するときには 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判断する DeviceSnapshot イベントを提供します。このイベントではキー情報が提供されません。

# CTI、JTAPI、および TAPI アプリケーションの CAPF の機能

Unified Communications Manager と同時に自動的にインストールされる認証局プロキシ機能（CAPF）は、設定に応じて、CTI/TAPI/TAPI アプリケーションについて次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。
- 表示やトラブルシューティングのために証明書を取得する。

JTAPI/TSP クライアントが CAPF と対話するとき、クライアントは認証文字列を使用して CAPF に認証されます。その後、クライアントが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。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クライアントに送り返されます。

アプリケーション ユーザとエンド ユーザには、それぞれ [Application User CAPF Profile Configuration] ウィンドウと [End User CAPF Profile Configuration] ウィンドウでの設定によって証明書を発行できます。Unified Communications Manager でサポートされる CAPF プロファイル間の相違点について、以下に説明します。

- アプリケーション ユーザ CAPF プロファイル：このプロファイルでは、CTIManager サービスとアプリケーションの間で TLS 接続をオープンできるようにするため、セキュアなアプリケーション ユーザに対してローカルで有効な証明書を発行できます。

  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 サービスや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 台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、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：このプロファイルでは、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、CTI クライアントに対してローカルで有効な証明書を発行できます。

**ヒント** JTAPI クライアントは、[JTAPI Preferences] ウィンドウで設定したパスに、Java Key Store 形式で LSC を保存します。TSP クライアントは、デフォルト ディレクトリまたは設定したパスに、暗号化形式で LSC を保存します。

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。

- 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、JTAPI クライアントは証明書の取得を 30 秒間隔でさらに 3 回試行します。この値は設定できません。

  TSP クライアントの場合、再試行回数と再試行タイマーを設定できます。TSP クライアントが一定時間内に証明書の取得を試行する回数を指定するには、次の値を設定します。どちらの値も、デフォルトは 0 です。最大 3 回までの再試行回数を、1（再試行 1 回）、2、3 で指定します。再試行間隔は 30 秒以内で設定できます。

- JTAPI/TSP クライアントと CAPF とのセッション試行中に電源障害が発生した場合、クライアントは電源復旧後に証明書のダウンロードを試行します。

# CTI、JTAPI、および TAPI アプリケーションの CAPF システムのインタラクションおよび要件

CAPF には次の要件が存在します。

- アプリケーションユーザとエンドユーザの CAPF プロファイルを設定する前に、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作業を実行したことを確認します。[Enterprise Parameters Configuration] ウィンドウの [Cluster Security Mode] を 1 に設定します（混合モード）。
- 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。
- 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、CTI/JTAPI/TAPI アプリケーションが正常に機能していることを確認します。

# CTI、JTAPI、および TAPI の保護

次の手順は、CTI、JTAPI および TAPI アプリケーションを保護するために実行する作業を示します。

**手順**

**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 ユーザを Standard CTI Enabled グループに割り当てます。

詳細については、次の資料を参照してください。

- 『*Computer Telephony Integration, System Configuration Guide for Cisco Unified Communications Manager*』
- 『*Cisco JTAPI Installation Guide for Cisco Unified Communications Manager*』
- 『*Cisco TAPI Installation Guide for Cisco Unified Communications Manager*』
- 『*Administration Guide for Cisco Unified Communications Manager*』

**ステップ 2** 次の 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 クライアントがインストールされ、CTL ファイルが実行済みであり、CTL ファイルが作成されていることを確認します。

- CTL Provider 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　CTL ファイルに CAPF 証明書を組み込むために、CAPF サービスを Cisco CTL クライアント用に実行する必要があります。電話で CAPF を使用したときにこれらのパラメータを更新済みの場合は、ここで再度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。

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

**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。

**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 キーを受信できません。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』の権限設定に関連する項目を参照してください。

（注）　Unified Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer 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 クライアントでは、クライアントが音声パケットを送信する場合、暗号化がサポートされることがあります。

**ステップ 5**　Unified Communications Manager の管理でアプリケーション ユーザまたはエンド ユーザの CAPF プロファイルを設定します。

**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。

# 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とエンド ユーザの追加

Standard CTI Secure Connection ユーザ グループと Standard CTI Allow Reception of SRTP Key Material ユーザ グループはデフォルトで [Unified Communications Manager Administration] に表示されます。これらのグループは削除できません。

CTIManager へのユーザ接続を保護するには、Standard CTI Secure Connection 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。

アプリケーションと CTIManager でメディア ストリームを保護する場合は、アプリケーション ユーザまたはエンド ユーザを Standard CTI 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 ユーザとエンド ユーザが SRTP を使用するには、TLS のベースラインの構成として機能する Standard CTI Enabled ユーザ グループと Standard CTI Secure Connection ユーザ グループに、これらのユーザが存在している必要があります。SRTP 接続には TLS が必要です。これらのグループにユーザを確保できたら、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。SRTP セッション キーを受け取るアプリケーションの場合、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、Standard CTI Allow Reception of SRTP Key Material の 3 グループに存在している必要があります。

Unified Communications Manager Assistant、Cisco QRT、Cisco Web Dialer は暗号化をサポートしていないため、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、CCMQRTSecureSysUser、IPMASecureSysUser、WDSecureSysUser を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、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。[Role Configuration] ウィンドウのセキュリティに関する設定については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

## 手順

**ステップ 1** [Unified Communications Manager Administration] で、**[User Management]** > **[User Groups]** を選択します。

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

**ステップ 3** 目的に応じて、次のいずれかの作業を実行します。

a) Standard CTI Enabled グループにアプリケーション ユーザまたはエンド ユーザが存在することを確認します。
b) Standard CTI Secure Connection 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 ユーザを追加するには、[Standard CTI Secure Connection] リンクをクリックします。
c) 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するには、[Standard CTI Allow Reception of SRTP Key Material] リンクをクリックします。

**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 （9 ページ）～ステップ 7 （9 ページ）を実行します。

**ステップ 5** [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、[Find] をクリックします。

検索条件を指定せずに [Find] をクリックすると、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（複数可）をオンにし、[Add Selected] をクリックします。

[User Groups] ウィンドウにユーザが表示されます。

**ステップ 8** グループにエンド ユーザを追加するには、ステップ 9 （9 ページ）～ステップ 11 （9 ページ）を実行します。

**ステップ 9** [Add 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、[Find] をクリックします。

検索条件を指定せずに [Find] をクリックすると、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（複数可）をオンにし、[Add Selected] をクリックします。

[User Groups] ウィンドウにユーザが表示されます。

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

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。

CAPF 機能を使用するには、このサービスを最初のノード上で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、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 固有のキー ペアおよび証明書が CAPF によって自動的に生成されます。Cisco CTL クライアントでスタンドアロン サーバまたはクラスタ内のすべてのサーバにコピーする CAPF 証明書の拡張子は .0 です。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 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。

Unified Communications Manager Administration で認証局プロキシ機能（CAPF）サービス パラメータがアクティブとして表示されるためには、Cisco Unified Serviceability で Certificate Authority Proxy Function サービスを有効化する必要があります。

ヒント　CAPF を電話に使用する際に CAPF サービス パラメータを更新する場合は、サービス パラメータを再度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 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。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**　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。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**　変更を有効にするには、[Cisco Unified Serviceability] で Cisco Certificate Authority Proxy Function サービスを再起動します。

# 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、次の手順を実行します。

**手順**

**ステップ 1** [Unified Communications Manager Administration] で、アクセスするプロファイルに応じて次のいずれかのウィンドウを選択します。

a) **[ユーザ管理]** > **[Application User CAPF Profile]**。
b) **[ユーザ管理]** > **[End User CAPF Profile]**。

[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** 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 （11 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。

- 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。

a) 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。
b) 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** 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。

# 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 の各アプリケーション用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 1 : アプリケーション ユーザおよびエンド ユーザの CAPF プロファイルの設定 （13 ページ）を参照してください。

ヒント　アプリケーション ユーザ CAPF プロファイルを設定した後で、エンド ユーザ CAPF プロファイルを設定することを推奨します。

## 手順

**ステップ 1**　[Unified Communications Manager Administration] で、次のいずれかのオプションを選択します。

a) **[User Management]** > **[Application User CAPF Profile]**。

b) **[User Management]** > **[End User CAPF Profile]**。

[Find and List] ウィンドウが表示されます。

**ステップ 2**　次のいずれかの作業を実行します。

a) 新しい CAPF プロファイルを追加するには、[Find] ウィンドウで [Add New] をクリックします（プロファイルを表示してから、[Add New] をクリックすることもできます）。各フィールドにデフォルト設定が取り込まれた設定ウィンドウが表示されます。

b) 既存のプロファイルをコピーするには、適切なプロファイルを見つけ、[Copy] 列内にあるそのレコード用の [Copy] アイコンをクリックします（プロファイルを表示してから、[Copy] をクリックすることもできます）。表示されたプロファイルからの設定が取り込まれた設定ウィンドウが表示されます。

c) 既存のエントリを更新するには、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 1 : アプリケーション ユーザおよびエンド ユーザの CAPF プロファイルの設定 （13 ページ）に示すように、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。

### 次のタスク

[Application User CAPF Profile Configuration] ウィンドウで CCMQRTSecureSysUser、IPMASecureSysUser、または WDSecureSysUser を設定した場合は、サービス パラメータを設定する必要があります。

# CAPF の設定

次の表で、[Application User CAPF Profile Configuration] および [End User CAPF Profile Configuration] ウィンドウの CAPF 設定について説明します。

**表 *1:* アプリケーション ユーザおよびエンド ユーザの *CAPF* プロファイルの設定**

| 設定 | 説明 |
|---|---|
| Application User | ドロップダウンリスト ボックスから、CAPF 操作用のアプリケーション ユーザを選択します。この設定には、設定されたアプリケーション ユーザが表示されます。<br>この設定は、[End User CAPF Profile Configuration] ウィンドウには表示されません。 |
| [End User ID] | ドロップダウンリスト ボックスから、CAPF 操作用のエンド ユーザを選択します。この設定には、設定されたエンド ユーザが表示されます。<br>この設定は、[Application User CAPF Profile Configuration] ウィンドウには表示されません。 |
| [Instance ID] | 1 ～ 128 文字の英数字（a ～ z、A ～ Z、0 ～ 9）を入力します。インスタンス ID は、証明書操作のユーザを指定します。<br>1 つのアプリケーションに複数の接続（インスタンス）を設定できます。アプリケーションと CTIManager との接続を保護するため、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）で実行されるそれぞれのインスタンスに固有の証明書があることを確認します。<br>このフィールドは、Web サービスと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 パラメータに関連します。 |

| 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。<br>• [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）<br>• [Install/Upgrade]：アプリケーション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。 |
| [Authentication Mode] | 証明書の操作が [Install/Upgrade] の場合、認証モードとして [By Authentication String] が指定されます。つまり、ユーザ/管理者によって [JTAPI/TSP Preferences] ウィンドウに CAPF 認証文字列が入力された場合にのみ、ローカルで有効な証明書のインストール/アップグレードまたはトラブルシュートが CAPF によって実行されます。 |
| [Authentication String] | 手動で一意の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。<br>文字列が 4 ～ 10 桁であることを確認します。<br>ローカルで有効な証明書のインストールまたはアップグレードを実行する場合、アプリケーション PC の JTAPI/TSP 設定 GUI に管理者が認証文字列を入力することが必要です。この文字列は 1 回だけ使用できます。このインスタンスで使用した文字列を再び使用することはできません。 |
| [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。 |

| 設定 | 説明 |
| --- | --- |
| [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。<br>• **[RSA Only]**<br>• **[EC Only]**<br>• **[EC Preferred, RSA Backup]**<br>（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]、[2048,]、[3072]、または [4096] 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に対応しています。<br>表示される値は、最初のノードに適用されます。<br>この設定は、証明書の操作を完了する必要がある期間の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 パラメータと併用します。このパラメータはいつでも更新できます。 |
| [Certificate Operation Status] | このフィールドには、保留中、失敗、成功といった証明書の操作の進行状況が表示されます。<br>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

この項では、Unified Communications Manager データベースからアプリケーション 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方法について説明します。

### 始める前に

[Unified Communications Manager Administration] 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、デバイスに別のプロファイルを適用するか、そのプロファイルを使用するすべてのデバイスを削除する必要があります。プロファイルを使用しているデバイスを確認するには、[Security Profile Configuration] ウィンドウの [Related Links] ドロップダウン リスト ボックスで [Dependency Records] を選択し、[Go] をクリックします。

依存関係レコード機能がシステムで有効でない場合は、依存関係レコード概要ウィンドウに、依存関係レコードを有効にするために実行できる操作が表示されます。また、依存関係レコード機能に関連して CPU 負荷が高くなることについての情報も表示されます。依存関係レコードの詳細は、『*System Configuration Guide for Cisco Unified Communications Manager*』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 CAPF プロファイルまたはエンド ユーザ CAPF プロファイルを探します。

**ステップ 2** 次のいずれかの作業を実行します。

a) 複数のプロファイルを削除するには、[Find and List] ウィンドウで該当するチェック ボックスの横にあるチェック ボックスをオンにし、[Delete Selected] をクリックします。[Select All] をクリックし、次に [Delete Selected] をクリックすると、設定可能なすべてのレコードが削除されます。

b) 1 つのプロファイルを削除するには、[Find and List] ウィンドウで該当するプロファイルの横にあるチェック ボックスをオンにし、[Delete Selected] をクリックします。

**ステップ 3** 削除操作を確認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、[Cancel] をクリックして削除の操作をキャンセルします。

# JTAPI/TAPI セキュリティ関連のサービス パラメータの設定

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** [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、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** [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の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** **[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の証明書操作ステータスの表示

[JTAPI/TSP Preferences] GUI ウィンドウまたは（[Find/List] ウィンドウではなく）特定の [Application User CAPF Profile configuration] または [End User CAPF Profile configuration] ウィンドウで、証明書操作のステータスを確認できます。