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について説明します。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 CiscoJTAPI 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、このドキュメントでは、CTI 制御デバイスまたは回線の制限を設定する方法については説明しません。

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。

（注） 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構成したとします。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。

Cisco の CTL クライアントは、リリース 14 からサポートされなくなりました。Cisco CTL プラグインではなく、CLI コマンドを使用して、Unified Communications Manager サーバーを混合モードに切り替えることをお勧めします。

CTIManager と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) によって他方の当事者の 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。

アプリケーションとの認証を行うために、CTIManager は、Unified Communications Manager 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。

CLI コマンドセットの**monitorctl**または Cisco ctl クライアントを使用して 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 クライアントが最初に TFTP サーバから CTL ファイルをダウンロードするときに、JTAPI/TSP クライアントは 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推奨します。JTAPI/TSP クライアントは、その後の CTL ファイルのダウンロードを確認します。たとえば、CTL ファイルを更新した後、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、ダウンロードする新しい 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、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 ファイル内の古い証明書を使用して TLS 接続を確立しようとします。CTL ファイルが変更されたか、または侵害された場合、接続は失敗する可能性があります。CTL ファイルのダウンロードが失敗し、複数の TFTP サーバが存在する場合は、ファイルをダウンロードするように別の TFTP サーバを設定できます。JTAPI/TAPI クライアントは、次の状況ではどのポートにも接続しません。

- クライアントは何らかの理由で CTL ファイルをダウンロードできません。たとえば、CTL ファイルは存在しません。
- クライアントには、既存の CTL ファイルがありません。
- アプリケーションユーザをセキュアな CTI ユーザとして設定しました。

アプリケーションは、CTIManager を使用して認証するために、認証局プロキシ機能（CAPF）によって発行され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つの証明書がすべてのインスタンスをカバーしていません。Cisco Unified Communications 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、「CAPF の設定項目」の説明に従って、 Cisco Unified Communications Manager Administration で、それぞれの [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）] または [エンドユーザ CAPF プロファイルの設定（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。

また、アプリケーションの TLS を有効にするには、Unified Communications Manager 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。このグループにユーザを追加して証明書をインストールすると、アプリケーションによって、ユーザが TLS ポート経由で接続することが保証されます。

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して機能します。つまり、認証を設定していない場合、暗号化を使用することはできません。

Unified Communications Manager、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしません。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 間のメディアストリームを保護するには、Unified Communications Manager でアプリケーション ユーザまたはエンドユーザを [標準 CTI SRTP キー情報の受信許可（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し、クラスタセキュリティモードが混合モードになっている場合、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アプリケーションに主要な資料を提供します。

（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能力を設定します。

アプリケーションは SRTP キー資料を記録したり保存したりしませんが、アプリケーションはキーマテリアルを使用して RTP ストリームを暗号化し、CTIManager から SRTP ストリームを復号化します。

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。制限を設定したために CTI/JTAPI/TAPI がデバイスまたは電話番号をモニタまたは制御できない場合、CTIManager はキー情報を送信しません。

ヒント　アプリケーションが SRTP セッションキーを受信するには、アプリケーションまたはエンドユーザが、Standard CTI Enabled、Standard CTI Secure Connection、および Standard CTI で SRTP キー情報の受信を許可する3つのグループに存在している必要があります。

Unified Communications Managerは、CTIports 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、セキュアコールをサポートするようにアプリケーションを設定する必要があります。

CTIports/ルートポイントは、ダイナミックまたはスタティック登録によって登録します。ポート/ルートポイントがダイナミック登録を使用している場合、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。CTIports/ルートポイントが TLS 接続を介して CTIManager に登録されると、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し、他方がセキュアである場合は、SRTP を介してメディアが暗号化されます。

CTI アプリケーションがすでに確立されているコールのモニタリングを開始すると、アプリケーションは RTP イベントを受信しません。確立されたコールの場合、CTI アプリケーションは DeviceSnapshot イベントを提供します。これは、コールのメディアがセキュアか非セキュアかを定義します。このイベントは、キー素材を提供しません。

CTI ポートの強力な暗号スイート

CTI ポートが TLS 接続を介して CTI Manager に登録されると、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し、他方がセキュアである場合は、Secure Real-Time Transport Protocol（SRTP）を介してメディアが暗号化されます。

Unified Communications Manager は、CTI ポートの Skinny Client Control Protocol（SCCP）インターフェイスに強力な暗号スイートを提供し、発信側と着信側の間のセキュアなメディア通知を可能にします。CTI ポートで SRTP を有効にするために、CTI アプリケーションは、暗号強度のサポートされているアルゴリズム ID を提供することによって登録します。

Unified Communications Manager は、CTI ポートを含むセキュアコールで次の追加アルゴリズムのネゴシエーションを許可するように拡張されています。

- CCM_AES_CM_128_HMAC_SHA1_32 (CiscoMediaEncryptionAlgorithmType.AES_128_COUNTER)
- CCM_AES_CM_128_HMAC_SHA1_80 (CiscoMediaEncryptionAlgorithmType.AES_128_COUNTER)
- CCM_AEAD_AES_128_GCM (CiscoMediaEncryptionAlgorithmType.AEAD_128_COUNTER)
- CCM_AEAD_AES_256_GCM (CiscoMediaEncryptionAlgorithmType.AEAD_256_COUNTER)

コールを受信すると、Unified Communications Manager は、CTI アプリケーションで指定されたメディアおよび暗号化機能をネゴシエートし、着信側の電話機の CTI ポートを登録します。一致するアルゴリズムがある場合、Unified CM は両側にキー情報を送信してパケットを復号化し、メディアをモニタまたは記録します。

制限

Unified Communications Manager は、CCM_F8_128_HMAC_SHA1_32 および CCM_F8_128_HMAC_SHA1_80 アルゴリズムをサポートしません。CTI アプリケーションがこれらのサポートされていないアルゴリズムを使用して CTI ポート終端メディアを登録しようとすると、Unified CM はそれを無視し、使用可能な残りのアルゴリズムのうち最適なものを選択します。システムがこれら 2 つ以外のアルゴリズムで構成されていない場合、Unified CM はデフォルトで既存の動作に切り替え、CCM_AES_CM_128_HMAC_SHA1_32 を選択します。

CTI、JTAPI、および TAPI アプリケーションの CAPF の機能

認証局プロキシ機能（CAPF）は 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。

- 認証文字列を使用して JTAPI/TSP クライアントに対して認証を行う。
- 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またはエンドユーザに証明書を発行するには、[Application User CAPF Profile Configuration] ウィンドウまたは [End User CAPF Profile Configuration] ウィンドウでそれぞれ設定を行います。次に、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、複数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 キーストア形式で 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、暗号化された形式で LSC を保存します。

次の情報は、通信または電源障害が発生した場合に適用されます。

- 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、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 クライアントでは、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、割り当てられた時間に証明書を取得しようとする回数を指定して、これらの値を設定します。両方の値について、デフォルトは0です。1(1回の再試行)、2、または3を指定することで、最大3回の再試行を設定できます。再試行ごとに30秒以内に設定できます。

- 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回復した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 システムインタラクションと要件

CAPF には次の要件があります。

- アプリケーションユーザとエンドユーザの CAPF プロファイルを設定する前に、[エンタープライズパラメータ設定（Enterprise Parameters Configuration）] ウィンドウの [クラスタセキュリティモード（Cluster Security Mode）] を 1（混合モード）に設定します。
- CAPF を使用するには、パブリッシャノードで Cisco 認証局プロキシ機能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プロセス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 を使用することを推奨します。
- 証明書操作の全期間を通じて、パブリッシャノードが正常に実行されていることを確認します。
- 証明書の操作全体で CTI/JTAPI/TAPI アプリケーションが機能していることを確認します。

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

Unified Communications Managerは、Cisco Unified Serviceability で認証局プロキシ機能サービスを自動的にはアクティブ化しません。

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。

Unified Communications Manager を混合モードに移行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。CAPF 証明書は、CAPF 証明書が存在することを検証として、Cisco Unified Communications オペレーティングシステムの GUI に表示されます。

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 アプリケーション用の重要な証明書をローカルでインストール/アップグレード/トラブルシューティングする場合は、「CAPF の設定項目」を参考にしてください。

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てからエンドユーザ CAPF プロファイルを設定することを推奨します。

手順

Step 1　Cisco Unified Communications Manager Administration で、次のいずれかのオプションを選択します。

a) **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アプリケーションユーザ CAPF プロファイル（Application User CAPF Profile）]**

b) **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [エンドユーザ CAPF プロファイル（End User CAPF Profile）]**

Step 2　次のいずれかの操作を行います。

a) 既存のプロファイルを編集するには、[検索（Find）]をクリックし、既存のプロファイルを編集します。

b) 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。

c) 既存のプロファイルから新しいプロファイルに設定をコピーするには、**[検索（Find）]** をクリックし、目的の設定がある既存のプロファイルを選択します。[コピー（Copy）]をクリックして、それらの設定を含む新しいプロファイルに名前を付けます。必要に応じて新しいプロファイルを編集します。

Step 3　「CAPF の設定項目」の説明に従って、適切な設定を入力します。

Step 4　[保存（Save）] をクリックします。

Step 5 この手順を繰り返して、さらに CAPF プロファイルを作成します。ユーザに必要な数のプロファイルを作成します。
[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 の設定項目

次の表で、**[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）]** および **[エンド ユーザ CAPF プロファイルの設定（End User CAPF Profile Configuration）]** ウィンドウの CAPF の設定項目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項目

設定	説明
[アプリケーションユーザー（Application User）]	ドロップダウンリストから、**CAPF 操作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。 この設定は、[エンドユーザ CAPF プロファイル（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から、**CAPF 操作のエンドユーザ**を選択します。この設定は設定済みのエンドユーザを示します。 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 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、証明書を操作するユーザを識別します。 アプリケーションの複数の接続先（インスタンス）を設定できます。アプリケーションと CTIManager 間の接続を保護するには、アプリケーション PC（エンドユーザ用）またはサーバ（アプリケーション ユーザ用）上で実行される各インスタンスが固有の証明書を持っていることを確認します。 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
[証明書の操作（Certificate Operation）]	ドロップダウンリストから、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場合に表示されます。（デフォルト設定） • [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。
[認証モード（Authentication Mode）]	証明書の操作が [インストール/アップグレード（Install/Upgrade）] の場合、認証モードとして [認証文字列（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 設定（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ティングが CAPF によって実行されます。
[認証文字列（Authentication String）]	手動で一意の文字列を入力するか、[文字列の生成（Generate String）] ボタンをクリックして文字列を生成します。 4 桁から 10 桁の文字列が含まれてい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（JTAPI/TSP preferences）]** 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 回の使用のみをサポートしており、文字列をインスタンスで使用した後は、再び使用できません。
[文字列の生成（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、[文字列の生成（Generate String）] ボタンをクリックします。[認証文字列（Authentication String）] フィールドに 4 桁から 10 桁の認証文字列が表示されます。
[キーの順序（Key Order）]	このフィールドは、CAPF のキーの順序を指定します。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 のみ（RSA Only）]** • **[ECのみ（EC Only）]** • **[EC 優先、RSA バックアップ（EC Preferred, RSA Backup）]** （注） [キーの順序（Key Order）]、[RSAキーサイズ（RSA Key Size）]、および [ECキーサイズ（EC Key Size）] の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はその電話に関連付けられます。値 [ECのみ（EC Only）] と [ECキーサイズ（EC Key Size）] で 256 ビットの値を選択した場合、デバイス セキュリティ プロファイルには [EC-256] の値が追加されます。

設定	説明
[RSAキーサイズ（ビット）（RSA Key Size (Bits)）]	ドロップダウンリストから、**512**、**1024**、**2048**、**3072**、または**4096**のいずれかの値を選択します。
[ECキーサイズ（ビット）（EC Key Size (Bits)）]	ドロップダウンリストから、**256**、**384**、または**521**のいずれかの値を選択します。
[操作完了期限（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。 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 操作有効期間（日数）（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アップデートできます。
[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。 このフィールドに表示される情報は変更できません。

CAPF サービス パラメータの更新

[サービスパラメータ（Service Parameter）] ウィンドウには、Cisco Certificate Authority Proxy Function のオプション設定があります。CAPF証明書の証明書発行者、オンラインCA接続設定、証明書の有効期間、キーサイズなどの設定を構成できます。

Cisco Unified Communications Manager Administration 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 Serviceability で[認証局プロキシ機能（Certificate Authority Proxy Function）] サービスを有効にします。

ヒント　電話機に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、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

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

Step 2　**[サーバ（Server）]** ドロップダウン リストからサーバを選択します。

ヒント　クラスタ内のパブリッシャノードを選択する必要があります。

Step 3　**[サービス（Service）]** ドロップダウンリストで、**[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。

Step 4　オンライン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。

Step 5　変更内容を有効にするには、Cisco Unified Serviceability で、**Cisco Certificate Authority Proxy Function** サービスを再起動します。

（注）　認証局プロキシ機能の設定方法の詳細については、「**認証局プロキシ機能**」の章を参照してください。

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

Cisco 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、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。プロファイルを使用しているデバイスを確認するには、[セキュリティ プロファイルの設定（Security Profile Configuration）] ウィンドウの [関連リンク（Related Links）] ドロップダウンリストで [依存関係レコード（Dependency Records）] を選択し、[移動（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については、Cisco Unified Communications Manager システム設定ガイドを参照してください。

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 Unified Communications Manager データベースから削除する方法を説明します。

手順

Step 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 プロファイルを検索します。

Step 2　次のいずれかの操作を行います。

a) 複数のプロファイルを削除するには、[**Find And List**] ウィンドウの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ます。次に、[**Delete Selected**] をクリックします。この選択で設定可能なすべてのレコードを削除するには、[すべて選択（Select All）] をクリックして、[選択項目の削除（Delete Selected）] をクリックします。

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ます。次に、[**Delete Selected**] をクリックします。

Step 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。

CTI、JTAPI、および TAPI の保護

次の手順では、CTI/JTAPI/TAPI アプリケーションを保護するために実行するタスクについて説明します。

手順

Step 1 CTI アプリケーションと JTAPI/TSP プラグインがインストールされ、実行されてい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。

- *Unified Communications Manager*の*Cisco JTAPI* インストールガイド
- *Unified Communications Manager*の*Cisco TAPI* インストールガイド

Step 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）。

- utlis ctl コマンドセットを実行して、Unified Communications Manager が混合モードになっているかどうかを確認します。
- CAPF サービスがインストールされ、サービスがアクティブ化されてい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 証明書を含めるために、**utils ctl** CLI コマンドに対して実行する必要があります。電話機に 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、パラメータを再度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。

Step 3 エンドユーザとアプリケーションユーザを、必要な権限を含むアクセス制御グループに割り当てます。ユーザを次のすべてのグループに割り当てます。これにより、ユーザは CTI 接続で **TLS** および **SRTP** を使用できます。

- 標準 CTI 対応

- 標準 CTI セキュア接続
- 標準 CTI SRTP 重要素材の受信許可

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のいずれか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。

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。アプリケーションまたはエンドユーザは、これら3つのグループに存在しない場合、SRTPセッションキーを受信できません。詳細については、ユーザアクセス制御グループの設定に関連するトピックを参照してください。

（注）　Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしません。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。

Step 4　エンドユーザとアプリケーションユーザの CAPF プロファイルを設定します。詳細については、「**認証局プロキシ機能**」の章を参照 してください。

Step 5　CTI/JTAPI/TAPI アプリケーションで、対応するセキュリティ関連のパラメータを有効にします。

セキュリティ関連のアクセス制御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 Unified Communications Manager 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のいずれか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。

アプリケーションとエンドユーザが SRTP を使用できるようになるには、そのユーザは、TLS のベースライン設定として機能する 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。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は、標準 CTI にユーザを追加して、SRTP キーマテリアルユーザグループの受信を許可することができます。アプリケーションが SRTP セッションキーを受信するには、アプリケーションまたはエンドユーザが、**Standard CTI Enabled**、**Standard CTI Secure Connection**、および **Standard CTI で SRTP キー情報の受信を許可する**3つのグループに存在している必要があります。

Cisco Unified Communications Manager Assistant、CiscoQRT、および Cisco Web Dialer が暗号化をサポートしていないため、アプリケーションユーザ（CCMQRTSecureSysUser、IPMASecureSysUser、および WDSecureSysUser）を標準 CTI SRTP 重要素材の受信許可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。**[ロールの設定（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

Step 1　Cisco Unified Communications Manager Administrationから、**[ユーザ管理（User Management）] > [ユーザグループ（User Group）]** を選択します。

Step 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。

Step 3　実行する内容に応じて、次のいずれかの作業を行います。

a) アプリケーション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、[標準 CTI セキュア接続（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、[標準CTI SRTP重要素材の受信許可（Standard CTI Allow Reception of SRTP Key Material）] リンクをクリックします。

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

Step 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）] をクリックします。

Step 6　アプリケーションユーザを検索するには、検索条件を指定します。次に、**[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

Step 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。

ユーザが [ユーザグループ（User Group）] ウィンドウに表示されます。

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

Step 9　[グループにユーザを追加（Add Users to Group）] をクリックします。

Step 10　エンドユーザを検索するには、検索条件を指定します。次に、**[検索 (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。

Step 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。

ユーザが [ユーザグループ（User Group）] ウィンドウに表示されます。

JTAPI/TAPI セキュリティ関連のサービスパラメータのセットアップ

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

Step 1 Cisco Unified Communications Manager Administrationから、**[System（システム）]** > **[Service Parameters（サービスパラメータ）]** 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 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。

Step 3 **[サービス（Service）]** ドロップダウン リストから、**[Cisco IP Manager Assistant]** サービスを選択します。

Step 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。

Step 5 疑問符またはパラメータ名のリンクをクリックしたときに表示されるヘルプの説明に従って、パラメータを更新します。

Step 6 [保存（Save）] をクリックします。

Step 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。

アプリケーションまたはエンドユーザの証明書の操作ステータスの表示

特定の [アプリケーションユーザ CAPF プロファイル設定（Application User CAPF Profile configuration）] または [エンドユーザ CAPF プロファイル設定（End User CAPF Profile configuration）] ウィンドウで、または（[検索/一覧表示（Find/List）] ウィンドウではなく） [JTAPI/TSP 設定（JTAPI/TSP Preferences）] GUI ウィンドウで、証明書操作ステータスを確認できます。

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。