



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および暗号化を設定するために、Cisco CallManager Administration で実行する必要がある作業についても説明します。

このマニュアルでは、Cisco CallManager Administration 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は説明しません。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 \(P.11-2\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの暗号化について \(P.11-4\)](#)
- [CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 \(P.11-5\)](#)
- [CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの対話および要件 \(P.11-6\)](#)
- [CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト \(P.11-7\)](#)
- [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 ユーザおよびエンド ユーザの追加 \(P.11-9\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.11-10\)](#)
- [CAPF サービス パラメータの更新 \(P.11-11\)](#)
- [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 \(P.11-12\)](#)
- [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 \(P.11-13\)](#)
- [Application User CAPF Profile ウィンドウおよび End User CAPF Profile ウィンドウの CAPF 設定 \(P.11-14\)](#)
- [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 \(P.11-16\)](#)
- [JTAPI/TAPI セキュリティ関連サービス パラメータ \(P.11-17\)](#)
- [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 \(P.11-17\)](#)
- [その他の情報 \(P.11-18\)](#)

CTI、JTAPI、および TAPI アプリケーションの認証について

Cisco CallManager 5.0 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 Cluster Security Mode が Secure Mode 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、ノンセキュア ポートであるポート 2748 で接続されます。

CTIManager とアプリケーションは、相互認証 TLS ハンドシェイク（証明書交換）で相手の ID を確認します。TLS 接続が発生すると、CTIManager とアプリケーションは、TLS ポート（ポート 2749）で 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 CallManager 5.0 のインストール時に Cisco CallManager サーバに自動的にインストールされる Cisco CallManager 自己署名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、CTL ファイルを生成した後、この証明書が自動的に CTL ファイルに追加されます。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 ファイルを更新し、JTAPI/TSP クライアントがこのファイルを TFTP サーバからダウンロードした後、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、新しい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 CallManager 自己署名証明書と 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、P.3-1 の「Cisco CTL クライアントの設定」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、Cisco CallManager の 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。たとえば、Cisco IPMA が、クラスタ内の 2 つの異なるノードで 2 つのサービス インスタンスを実行している場合、各インスタンスに独自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。IPMA 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 11-2 の説明に従い、Cisco CallManager 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。



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。

アプリケーションに対して TLS を有効にするには、前述の作業に加えて、Cisco CallManager 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 IPMA、Cisco QRT、および Cisco WebDialer 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、暗号化をサポートしないことがあります。

アプリケーションと CTIManager の間のメディア ストリームを保護するには、Cisco CallManager 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 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。クラスタ セキュリティ モードが Secure Mode の場合、アプリケーション ユーザおよびエンド ユーザをこのグループと Standard CTI Secure Connection ユーザ グループに追加すると、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鍵関連情報を提供します。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。アプリケーションが SRTP 鍵関連情報を記録または格納しないことに注意してください。

何らかの理由でアプリケーションがノンセキュア 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 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 グループに存在することを確認します。これが、TLS の基本設定になります。TLS は、SRTP 接続に必要です。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 CallManager 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ノン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 CallManager と共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 と対話するとき、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。

Application User CAPF Profile Configuration ウィンドウまたは 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 CallManager 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、セキュア アプリケーション ユーザにローカルで有効な証明書を発行できます。証明書を発行し、その他のセキュリティ関連作業を実行すると、CTIManager サービスとアプリケーションの間で、TLS 接続が開始されます。

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。たとえば、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。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、たとえば、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できます。証明書を発行し、その他のセキュリティ関連作業を実行すると、CTI クライアントは TLS 接続で CTIManager サービスと通信します。



ヒント

JTAPI クライアントは LSC を Java Key Store 形式で、JTAPI Preferences 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 システムの対話および要件

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。Cisco CTL クライアントで Cluster Security Mode が Secure Mode に設定されていることを確認します。
- 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。
- 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 11-1 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 11-1 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
<p>ステップ 1</p>	<p>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。</p> <p> 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られている必要があります。</p>	<ul style="list-style-type: none"> 『Cisco CallManager システム ガイド Release 5.0』の「コンピュータ テレフォニー統合」 Cisco JTAPI インストールガイド for Cisco CallManager 5.0 Cisco TAPI インストールガイド for Cisco CallManager 5.0 Cisco CallManager アドミニストレーションガイド Release 5.0
<p>ステップ 2</p>	<p>次の CallManager 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)。</p> <ul style="list-style-type: none"> CTL ファイルが作成されるように、5.0 用の 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 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。必要に応じて、CAPF サービス パラメータを更新します。 <p> 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。</p> <ul style="list-style-type: none"> クラスタ セキュリティ モードが Secure Mode に設定されていることを確認します。 <p> ヒント クラスタ セキュリティ モードが Secure Mode 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。</p>	<ul style="list-style-type: none"> Cisco CTL クライアントの設定 (P.3-1) CAPF サービス パラメータの更新 (P.11-11) Cisco CallManager アドミニストレーションガイド
<p>ステップ 3</p>	<p>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。</p> <p> 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せんが、両方に割り当てることはできません。</p>	<p>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およびエンドユーザの追加 (P.11-9)</p>

表 11-1 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 4	<p>SRTP を使用して CTIManager とアプリケーションの間のメディア 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 グループに追加します。</p> <p>アプリケーション ユーザまたはエンドユーザが 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 グループに存在することを確認します。これが、TLS および SRTP 接続の基本設定になります。これらのグループにユーザを追加した後、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。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。</p> <p>Cisco IPMA、Cisco QRT、および Cisco WebDialer 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、暗号化をサポートしないことがあります。</p>	<p>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 ユーザおよびエンドユーザの追加 (P.11-9)</p> <p>『Cisco CallManager アドミニストレーションガイド』の「ロールの設定」</p>
ステップ 5	<p>Cisco CallManager 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 プロファイルを設定します。</p>	<ul style="list-style-type: none"> • CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 (P.11-5) • 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.11-13) • Application User CAPF Profile ウィンドウおよび End User CAPF Profile ウィンドウの CAPF 設定 (P.11-14)
ステップ 6	<p>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。</p>	<p>JTAPI/TAPI セキュリティ関連サービス パラメータ (P.11-17)</p>

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 ユーザおよびエンド 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 CallManager Administration に表示されます。これらのグループは削除できません。

アプリケーション ユーザまたはエンド ユーザが CTIManager と通信するときに TLS 接続を使用するには、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ができません。

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。TLS は、SRTP 接続に必要です。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 IPMA、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

アプリケーション ユーザまたはエンド ユーザをユーザ グループから削除する方法については、『Cisco CallManager アドミニストレーションガイド』を参照してください。Role Configuration ウィンドウのセキュリティ関連設定の詳細については、『Cisco CallManager 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 CallManager Administration で **User Management > 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、**Find** をクリックします。

ステップ 3 目的に応じて、次の作業のいずれか 1 つを実行します。

- 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 **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、検索基準を指定し、**Find** をクリックします。

検索基準を指定せずに **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、**Add Selected** をクリックします。

User Group 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 **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、検索基準を指定し、**Find** をクリックします。

検索基準を指定せずに **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、**Add Selected** をクリックします。

User Group ウィンドウにユーザが表示されます。

追加情報

詳細については、[P.11-18](#) の「[関連項目](#)」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 CallManager 5.0(1) では、Cisco CallManager Serviceability で Certificate Authority Proxy Function サービスが自動的にアクティブになりません。Certificate Authority Proxy Function サービスのアクティブ化の詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』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、[P.3-12](#) の「[CTL ファイルの更新](#)」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 に固有な鍵の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 IPT Platform 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。



ヒント

このリリースの Cisco CallManager は、SCEP または Microsoft CA や Keon CA などサードパーティの CA 署名付き LSC 証明書をサポートしません。サードパーティ証明書のサポートは、将来のリリースで予定されています。現在、サードパーティ CA を使用している場合は、5.0 に移行する前に、有効期間が長い（6 か月以上の）証明書を再発行し、サードパーティ証明書がサポートされる前に失効しないようにしてください。

CAPF サービス パラメータが、Cisco CallManager Administration で Active として表示されるようにするには、Cisco CallManager Serviceability で、Certificate Authority Proxy Function サービスをアクティブに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 CallManager Administration で、**System > Service Parameters** の順に選択します。
- ステップ 2** Server ドロップダウン リスト ボックスから、最初のノードを選択します。
- ステップ 3** Service ドロップダウン リスト ボックスから、Cisco 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 CallManager Serviceability 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

詳細については、[P.11-18](#) の「[関連項目](#)」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 アクセスするプロファイルに応じて、Cisco CallManager Administration で次のオプションのどちらかを選択します。

- **User Management > Application User CAPF Profile**
- **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 ドロップダウン リスト ボックスから、表示するプロファイルの検索基準を選択し、**Find** をクリックします。



(注) データベースに登録されているすべて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 プロファイルを検索するには、検索基準を指定せずに、**Find** をクリックします。

ウィンドウが更新され、検索基準と一致するプロファイルが表示されます。

ステップ 3 表示するプロファイルの **Instance ID** リンク、**Application User** リンク (アプリケーション ユーザ CAPF プロファイルのみ)、または **End User ID** リンク (エンド ユーザ CAPF プロファイルのみ) をクリックします。



ヒント 検索結果の中で Instance ID、Application User (アプリケーション ユーザ CAPF プロファイルのみ)、または End User ID (エンド ユーザ CAPF プロファイルのみ) を検索するには、**Search Within Results** チェックボックスをオンにし、この手順の説明に従って検索基準を入力し、**Find** をクリックします。

追加情報

詳細については、[P.11-18](#) の「[関連項目](#)」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 11-2](#) を参照してください。



ヒント

次の手順は、アプリケーション ユーザ CAPF プロファイルとエンド ユーザ CAPF プロファイルの両方をサポートしますが、両方を同時に設定することはできません。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が推奨されます。

手順

- ステップ 1** Cisco CallManager Administration で、次のオプションのどちらかを選択します。
 - **User Management > Application User CAPF Profile**
 - **User Management > End User CAPF Profile**
- ステップ 2** Find/List Application User CAPF Profile Configuration ウィンドウまたは Find/List End User CAPF Profile Configuration ウィンドウが表示されたら、次の作業のどちらかを実行します。
 - 既存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 プロファイルを検索するには、検索基準を指定し、**Find** をクリックします。
検索基準を指定せずに Find をクリックすると、システムにあるすべて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 プロファイルが表示されます。
 - 新し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 プロファイルを追加するには、**Add New** をクリックします。
- ステップ 3** CAPF Profile プロファイル設定ウィンドウが表示されたら、[表 11-2](#) の説明に従って、設定内容を入力します。
- ステップ 4** **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。

追加の手順

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、[P.11-17](#) の「JTAPI/TAPI セキュリティ関連サービス パラメータ」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

詳細については、[P.11-18](#) の「[関連項目](#)」を参照してください。

Application User CAPF Profile ウィンドウおよび End User CAPF Profile ウィンドウの CAPF 設定

表 11-2 で、Cisco CallManager Administration の Application User CAPF Profile ウィンドウおよび End User CAPF Profile ウィンドウの CAPF 設定について説明します。関連する手順については、P.11-18 の「関連項目」を参照してください。

表 11-2 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
Application User	<p>この設定には、Application User ウィンドウに存在するユーザが表示されません。ドロップダウン リスト ボックスから、CAPF 操作を実行する対象のアプリケーション ユーザを選択します。</p> <p>この設定は、End User CAPF Profile ウィンドウには表示されません。</p>
End User	<p>この設定には、End User ウィンドウに存在するユーザが表示されます。ドロップダウン リスト ボックスから、CAPF 操作を実行する対象のエンド ユーザを選択します。</p> <p>この設定は、Application User CAPF Profile ウィンドウには表示されません。</p>
Instance ID	<p>クラスタでは、アプリケーションの複数の接続 (インスタンス) を実行できます。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 (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必要です。たとえば、クラスタの 2 つのサーバでサービスまたはアプリケーションのインスタンスが 2 つ実行されている場合、各インスタンスに独自の証明書が必要です。</p> <p>CAPF は、Application User または End User と Instance ID の設定を使用して、証明書操作を実行する場所を判別します。設定しているアプリケーション ユーザまたはエンド ユーザに対して、a ~ z、A ~ Z、ダッシュ (-)、アンダースコア (_)、またはピリオド (.) を使用して、一意の文字列を入力します。</p> <p>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、P.11-17 の「JTAPI/TAPI セキュリティ関連サービス パラメータ」を参照してください。</p>
Certificate Operation	<p>ドロップダウン ボックスから、次のオプションのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> • 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)。 • 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 11-2 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 (続き)

設定	説明
Authentication Mode	認証モードは、指定された証明書操作のときに、アプリケーションが CAPF で認証する方法として機能します。デフォルトでは、Cisco CallManager Administration は By Authentication String を表示して、ユーザまたは管理者が JTAPI/TSP Preferences 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します。
Authentication String	一意の文字列を手動で入力するか、あるいは 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 Preferences GUI 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。
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 Authentication String フィールドに表示されます。
Key Size (bits)	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 秒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 CallManager 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。
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 パラメータと組み合わせて使用します。このパラメータは、必要に応じて更新できます。
Operation Status	このフィールドは証明書操作の進行状況を表示します。たとえば、<operation type> pending、failed、successful など、operating type には、指定した Certificate Operation 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。

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 CallManager 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 CallManager Administration 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前に、別のプロファイルをデバイスに適用するか、当該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。当該プロファイルを使用しているデバイスを検索するには、Security Profile Configuration ウィンドウの Related Links ドロップダウン リスト ボックスから **Dependency Records** を選択して、**Go** をクリックします。

システムで Dependency Records 機能が有効になっていない場合は、レコードの依存性の概要ウィンドウに、Dependency Records 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、Dependency Records 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せん。Dependency Records の詳細については、『Cisco CallManager システム ガイド』を参照してください。

手順

-
- ステップ 1** P.11-12 の「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」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** 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、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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。
- ステップ 3** 単一のプロファイルを削除するには、次の作業のどちらかを実行します。
- Find and List 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、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。
 - Find and List ウィンドウで、プロファイルの Name リンクをクリックします。指定した Application User CAPF Profile Configuration ウィンドウまたは End User CAPF Profile Configuration ウィンドウが表示されたら、**Delete Selected** アイコンまたは **Delete Selected** ボタンをクリックします。
- ステップ 4** 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、**Cancel** をクリックして削除操作を取り消します。
-

追加情報

詳細については、P.11-18 の「関連項目」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、Web サービスまたはアプリケーションに対して、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 CallManager Administration で、**System > Service Parameters** の順に選択します。
 - ステップ 2** Server ドロップダウン リスト ボックスから、Web サービスまたはアプリケーション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、Web サービスまたはアプリケーションを選択します。
 - 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** **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 (Find/List ウィンドウではありません)、または JTAPI/TSP Preferences GUI ウィンドウで、証明書操作のステータスを表示できます。

その他の情報

関連項目

- [Cisco CTL クライアントの設定 \(P.3-1\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの認証について \(P.11-2\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの暗号化について \(P.11-4\)](#)
- [CTI、JTAPI、および TAPI アプリケーションに対する CAPF の概要 \(P.11-5\)](#)
- [CTI、JTAPI、および TAPI アプリケーションに対する CAPF システムの対話および要件 \(P.11-6\)](#)
- [CTI、JTAPI、および TAPI のセキュリティ設定用チェックリスト \(P.11-7\)](#)
- [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 ユーザおよびエンド ユーザの追加 \(P.11-9\)](#)
- [Certificate Authority Proxy Function サービスのアクティブ化 \(P.11-10\)](#)
- [CAPF サービス パラメータの更新 \(P.11-11\)](#)
- [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 \(P.11-12\)](#)
- [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 \(P.11-13\)](#)
- [Application User CAPF Profile ウィンドウおよび End User CAPF Profile ウィンドウの CAPF 設定 \(P.11-14\)](#)
- [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 \(P.11-16\)](#)
- [JTAPI/TAPI セキュリティ関連サービス パラメータ \(P.11-17\)](#)
- [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 \(P.11-17\)](#)

シスコの関連マニュアル

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