Cisco CTL クライアントの設定

この章は、次の内容で構成されています。

Cisco CTL クライアントの概要

デバイス認証、ファイル認証、およびシグナリング認証は、Certificate Trust List（CTL; 証明書信頼リスト）ファイルの作成に依存します。このファイルは、Cisco Certificate Trust List（CTL）クライアントを USB ポートのある単一の Windows 2000 ワークステーションまたはサーバ（Cisco CallManager サーバなど）にインストールおよび設定したときに作成されます。CTL ファイルには、次のサーバまたはセキュリティ トークンのためのエントリが含まれています。

- Site Administrator Security Token（SAST）
- 同一のサーバで実行される Cisco CallManager および Cisco TFTP
- Certificate Authority Proxy Function （CAPF）
- 代替の Cisco TFTP

CTL ファイルには、サーバのサーバ証明書、公開キー、シリアル番号、シグニチャ、発行者名、件名、サーバ機能、DNS 名、および IP アドレスが含まれます。CTL ファイルを作成したら、Cisco CallManager Serviceability で Cisco CallManager および Cisco TFTP サービスを、これらのサービスを実行するクラスタ内のすべてのサーバで、再起動する必要があります。次回、電話機を初期化するときには、CTL ファイルが TFTP サーバからダウンロードされます。CTL ファイルに自己署名証明書を持つ TFTP サーバ エントリが含まれている場合、電話機は .sgn 形式の署名付き設定ファイルを要求します。どの TFTP サーバにも証明書がない場合、電話機は署名なしファイルを要求します。

（注）　Cisco CallManager は .tlv 形式の CTL ファイルを TFTP File Location および TFTP Alternate File Locations で指定されたディレクトリに格納します。

Cisco CTL クライアントをインストールおよび設定し、証明書が電話機に存在することを確認して、デバイスに認証または暗号化を設定したら、電話機は TLS SCCP ポートを介して TLS 接続を確立します。このポートは、443 を加算（+）したポート番号に設定されています。デフォルトでは、電話機は TLS を使用してポート 2443 に接続します。ハンドシェイクによって証明書が認証され、保護された接続が確立されます。

関連項目

- Cisco CTL クライアントの設定用チェックリスト（P.3-4）
- 認証および整合性の概要（P.1-24）

Cisco CTL クライアントの設定用チェックリスト

表 3-1 に、初めて Cisco CTL クライアントをインストールおよび設定する場合に実行する設定作業のリストを示します。

表 3-1　Cisco CTL クライアントの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	クラスタにある各 Cisco CallManager および Cisco TFTP サーバの Cisco CallManager Serviceability で Cisco CTL Provider サービスをアクティブにします。 **ヒント**　Cisco CallManager　のアップグレード前にこのサービスをアクティブにした場合は、サービスを再度アクティブにする必要はありません。アップグレード後にサービスは自動的にアクティブになります。	Cisco CTL Provider サービスのアクティブ化（P.3-6）
ステップ 2	パブリッシャ データベース サーバの CiscoCallManager Serviceability で Cisco Certificate Authority Proxy サービスをアクティブにします。 **ワンポイントアドバイス**　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作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。	Certificate Authority Proxy Function サービスのアクティブ化（P.4-14）
ステップ 3	デフォルト設定を使用しない場合は、TLS 接続用のポートを設定します。 **ヒント**　これらの設定を Cisco CallManager のアップグレード前に設定した場合、設定は自動的に移行されます。	TLS 接続用ポートの設定（P.3-9）

表 3-1　Cisco CTL クライアントの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	Cisco CTL クライアント用に設定するサーバについて、少なくとも 2 つのセキュリティ トークンとパスワード、ホスト名または IP アドレス、およびポート番号を入手します。	Cisco CTL クライアントの設定（P.3-15）
ステップ 5	Cisco CTL クライアントをインストールします。 **ヒント**　Cisco CallManager 4.0 で使用できた Cisco CTL クライアントは使用できません。Cisco CallManager 4.1(3) にアップグレードした後で CTL ファイルを更新するには、Cisco CallManager Administration 4.1(3) で使用可能なプラグインをインストールする必要があります。	• システム要件（P.1-5） • セキュリティのインストール（P.1-13） • Cisco CTL クライアントのインストール（P.3-11）
ステップ 6	Cisco CTL クライアントを設定します。 **ヒント**　Cisco CallManager のアップグレード前に CTL ファイルを作成した場合、CTL ファイルはアップグレード時に自動的に移行されます。Cisco CallManager Release リリース 4.1(3) にアップグレードした後で CTL ファイルを更新するには、Cisco CallManager Administration 4.1(3) で使用可能な Cisco CTL クライアントをインストールおよび設定する必要があります。	Cisco CTL クライアントの設定（P.3-15）

Cisco CTL Provider サービスのアクティブ化

Cisco CTL クライアントの設定後、このサービスによってクラスタのセキュリティ モードがノンセキュア モードから混合モード、およびその逆に変更され、サーバ証明書が CTL ファイルに転送されます。その後、このサービスによって CTL ファイルがすべての Cisco CallManager および Cisco TFTP サーバに転送されます。

サービスをアクティブにしてから Cisco CallManager をアップグレードした場合、Cisco CallManager によってサービスはアップグレード後に自動的に再度アクティブになります。

ヒント　クラスタ内のすべてのサーバで Cisco CTL Provider サービスをアクティブにする必要があります。

ローカルの Administrator パスワードまたは Power Users アカウントのユーザ名とパスワードが、すべての Cisco CallManager および Cisco TFTP サーバ上で同期されていることを確認します。

サービスをアクティブにするには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Serviceability で **Tools > Service Activation** の順に選択します。

ステップ 2　ウィンドウの左側のペインで、Cisco CallManager または Cisco TFTP サービスをアクティブにしたサーバを選択します。

ステップ 3　**CTL Provider** サービス チェックボックスをオンにします。

ステップ 4　**Update** をクリックします。

ステップ 5　クラスタ内のすべてのサーバで、この手順を実行します。

（注）　サービスをアクティブにすると、Cisco CTL Provider サービスはデフォルトの CTL ポート（2444）に復元されます。このポートを変更する場合は、P.3-9 の「TLS 接続用ポートの設定」を参照してください。

ステップ 6　サービスがクラスタ内のすべてのサーバで実行されていることを確認します。サービスの状態を確認するには、Cisco CallManager Serviceability で **Tools > Control Center** の順に選択します。

関連項目

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability システム ガイド*
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Cisco CTL クライアントのインストール（P.3-11）

Cisco CAPF サービスのアクティブ化

このサービスのアクティブ化については、P.4-14 の「Certificate Authority Proxy Function サービスのアクティブ化」を参照してください。

ワンポイント・アドバイス　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作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。

関連項目

- Cisco CTL クライアントの設定用チェックリスト（P.3-4）
- CAPF の設定用チェックリスト（P.4-10）
- Certificate Authority Proxy Function サービスのアクティブ化（P.4-14）
- 設定用チェックリストの概要（P.1-30）

TLS 接続用ポートの設定

ポートが現在使用中の場合や、ファイアウォールを使用していてファイアウォール内のポートを使用できない場合には、異なるポート番号の設定が必要になることもあります。

Cisco CTL Provider の TLS 接続用デフォルト ポートは 2444 です。Cisco CTL Provider ポートでは Cisco CTL クライアントからの要求を監視します。このポートでは、CTL ファイルの取得、クラスタ全体のセキュリティ モード設定、CTL ファイルの TFTP サーバへの保存、クラスタ内の Cisco CallManager および TFTP サーバ リストの取得などの、Cisco CTL クライアントの要求を処理します。

Cisco CallManager ポートでは、電話機からの登録要求を監視します。ノンセキュア モードの場合、電話機はポート 2000 を介して接続されます。混合モードの場合、Cisco CallManager の TLS 接続用ポートは Cisco CallManager のポート番号に 443 を加算（+）した番号になるため、Cisco CallManager のデフォルトの TLS 接続は 2443 になります。

ヒント　ポートを更新した後は、Cisco CallManager Administration で Cisco Provider サービスを再起動する必要があります。

デフォルト設定を変更するには、次の手順を実行します。

手順

ステップ 1　変更するポートに応じて、次の作業を実行します。

- Cisco CTL Provider ポートを変更するには、ステップ 2 ～ステップ 6 を実行します。
- Cisco CallManager ポートを変更するには、ステップ 7 ～ステップ 10 を実行します。

ステップ 2　Cisco CTL Provider ポートを変更するには、Cisco CallManager Administration で **Service > Service Parameters** の順に選択します。

ステップ 3　Cisco CTL Provider サービスが実行されているサーバを選択します。

ステップ 4　**Cisco CTL Provider** サービスを選択します。

ヒント　ウィンドウの右上隅にある i ボタンをクリックすると、サービス パラメータに関する情報を確認できます。

ステップ 5　Cisco CTL Provider ポートを変更するには、Port Number フィールドに新しいポート番号を入力します。

ステップ 6　**Update** をクリックします。

ステップ 7　Cisco CallManager ポートを変更するには、Cisco CallManager Administration で **System > Cisco CallManager** の順に選択します。

ステップ 8　Cisco CallManager サービスが実行されているサーバを選択します。

ステップ 9　Ethernet Phone Port フィールドに新しいポート番号を入力します。

ステップ 10　**Update** をクリックします。

関連項目

- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Cisco CTL クライアントのインストール（P.3-11）
- Cisco CTL クライアントの設定（P.3-15）
- Cisco CTL クライアント設定（P.3-25）
- トラブルシューティング（P.9-1）

Cisco CTL クライアントのインストール

Cisco CTL クライアントは、USB ポートのある単一の Windows 2000 ワークステーションまたはサーバにインストールします。サーバまたはワークステーションはリモート サイトに置くことができます。Cisco CallManager がインストールされているサーバに USB ポートさえあれば、このサーバにクライアントをインストールすることもできます。

次のイベントが発生するときには、クライアントを使用して CTL ファイルを更新する必要があります。

- Cisco CallManager のインストール後
- Cisco CallManager サーバまたは Cisco CallManager データの復元後
- Cisco CallManager サーバの IP アドレスまたはホスト名の変更後
- セキュリティ トークン、TFTP サーバ、または Cisco CallManager サーバの追加後または削除後
- TFTP または Cisco CallManager サーバの置換後

注意　Terminal Services は、クライアントのインストールに使用しないでください。シスコは、CiscoTechnical Assistance Center （TAC）がリモートでトラブルシューティングおよび設定作業を行えるように Terminal Services をインストールしています。

プラグインを実行する前に、Cisco Security Agent （CSA）、またはシスコが認定したその他の侵入検知あるいはアンチウィルス アプリケーションを無効にしておく必要があります。アプリケーションを無効にしないと、インストールすることができずに、回復不可能なエラーが発生する場合があります。

ヒント　クライアントをインストールしようとしているサーバまたはワークステーションで、Smart Card サービスが started および automatic に設定されていない場合、インストールは失敗します。この作業を実行する方法については、P.9-1 の「トラブルシューティング」を参照してください。

プラグインのインストール中に表示される可能性があるメッセージのリストを確認するには、P.9-1 の「トラブルシューティング」を参照してください。

Cisco CTL クライアントをインストールするには、次の手順を実行します。

手順

ステップ 1　Smart Card サービスが started および automatic に設定されていることを確認します。詳細については、P.9-12 の「Smart Card サービスの Started および Automatic への設定」を参照してください。

ステップ 2　USB ポートのある Windows 2000 ワークステーションまたはサーバから Cisco CallManager Administration を参照します。この場所は、クライアントをインストールしようとしている場所です。

ステップ 3　Cisco CallManager Administration で、**Application > Install Plugins** の順に選択します。

ステップ 4　ファイルをダウンロードするには、**Cisco CTL Client** をクリックします。

ステップ 5　ファイルを任意の場所にダウンロードします。

ステップ 6　インストールを開始するには、**Cisco CTL Client**（ファイルを保存した場所によってアイコンまたは実行ファイルになります）をダブルクリックします。

ステップ 7　Cisco CTL クライアントのバージョンが表示されるので、**Continue** をクリックします。

ステップ 8　インストール ウィザードが表示されます。**Next** をクリックします。

ステップ 9　使用許諾契約に同意して **Next** をクリックします。

ステップ 10　クライアントが存在するフォルダを選択します。必要な場合は、Browse をクリックしてデフォルトの場所を変更することができます。場所を選択したら、**Next** をクリックします。

ステップ 11　インストールを開始するには、**Next** をクリックします。

ステップ 12　インストールが完了したら、**Finish** をクリックして終了します。

ヒント　クライアントがインストールされたことを確認するには、P.9-1 の「トラブルシューティング」を参照してください。

関連項目

- システム要件（P.1-5）
- 対話および制限（P.1-6）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Smart Card サービスの Started および Automatic への設定（P.9-12）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Cisco CTL クライアントの設定（P.3-15）
- CTL ファイルの更新（P.3-21）
- CTL ファイル エントリの削除（P.3-29）
- デバイス セキュリティ モードの設定（P.5-7）
- トラブルシューティング（P.9-1）

Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行

Cisco CallManager 4.1(3) にアップグレードした後で CTL ファイルを変更するには、Cisco CallManager Administration 4.1(3) で使用可能な Cisco CTL クライアントをインストールおよび設定する必要があります。

Cisco CallManager をアップグレードする前にサーバの削除や追加を実行しなかった場合は、アップグレード後に Cisco CTL クライアントを再設定する必要はありません。Cisco CallManager のアップグレードにより、CTL ファイル内のデータは自動的に移行されます。

関連項目

- Cisco CTL クライアントの設定用チェックリスト（P.3-4）
- Cisco CTL クライアントのインストール（P.3-11）
- Cisco CTL クライアントの設定（P.3-15）
- トラブルシューティング（P.9-1）

Cisco CTL クライアントの設定

ヒント　Cisco CTL クライアントは、スケジューリングされたメンテナンス画面で設定します。これは、Cisco CallManager および Cisco TFTP サービスを実行するクラスタにあるすべてのサーバの Cisco CallManager Serviceability で、これらのサービスを再起動する必要があるためです。

Cisco CTL クライアントは、次のタスクを実行します。

- Cisco CallManager クラスタのセキュリティ モードを設定する。

ヒント　Cisco CallManager Administration の Enterprise Parameters ウィンドウで、Cisco CallManager クラスタ全体に混合モードを設定することはできません。クラスタ全体のモードを設定するには、CTL クライアントを設定する必要があります。詳細については、P.3-25 の「Cisco CTL クライアント設定」を参照してください。

- Certificate Trust List（CTL; 証明書信頼リスト）を作成する。これは、セキュリティ トークン、Cisco CallManager、代替 TFTP、および CAPF サーバ用の証明書エントリが含まれたファイルです。

  CTL ファイルによって、電話接続用の TLS をサポートするサーバが示されます。クライアントは自動的に Cisco CallManager、Cisco TFTP サーバ、および Cisco CAPF サーバを検出して、これらのサーバの証明書エントリを追加します。

  代替 TFTP サーバおよび Site Administrator Security Token （SAST）は手動で CTL ファイルに追加する必要があります。

  設定時に挿入したセキュリティ トークンによって CTL ファイルが署名されます。

ヒント　代替 TFTP サーバは、異なるクラスタにある場合でも設定することができます。手動で設定することにより、代替 TFTP サーバからの証明書が CTL ファイルに追加されます。これは、TFTP サービス パラメータで指定された FileLocation パスに書き込まれます。マルチクラスタ構成では、代替 TFTP サーバ上のドライブをマッピングし、FileLocation パラメータをマッピングされたドライブに設定する必要があります。たとえば、代替 TFTP サーバとして TFTP1 を使用し、ドライブ L: を TFTP1 上のパスにマッピングした場合、FileLocation は L:\TFTPPath となります。TFTP サーバを追加する必要があります。たとえば、TFTP1 の場合、TFTP1 の有効な管理者ユーザ名とパスワードを指定して追加します。Cisco CTL クライアントによって、CTL ファイルが L:\TFTPPath に書き込まれます。

この TFTP 設定を実装する前に、マルチクラスタ環境にあるすべてのサーバで、同じバージョンの Cisco CallManager が実行され、同じクラスタ全体のセキュリティ モードが設定されている必要があります。マルチクラスタ環境にあるすべてのサーバで、Cisco CTL Provider サービスを実行する必要があることに注意してください。

始める前に

Cisco CTL クライアントを設定する前に、Cisco CTL Provider サービスおよび Cisco Certificate Authority Proxy Function サービスを Cisco CallManager Serviceability でアクティブにしたことを確認します。少なくとも 2 つのセキュリティ トークンを入手します。これらのセキュリティ トークンは、Cisco certificate authority が発行します。トークンを一度に 1 つずつサーバまたはワークステーションの USB ポートに挿入します。サーバに USB ポートがない場合、USB PCI カードを使用することができます。

次のパスワード、ホスト名または IP アドレス、ポート番号を取得します。

- Cisco CallManager 用のローカル管理者パスワード、ホスト名または IP アドレス、CTL Provider サービス用のポート番号
- 代替 TFTP 用のローカル管理者パスワードと、ホスト名または IP アドレス
- セキュリティ トークンの管理者パスワード

これらの説明については、表 3-2 を参照してください。

ヒント Cisco CTL クライアントをインストールする前に、クラスタ内の各サーバに対してネットワーク接続があることを確認してください。同様に、サーバが DNS を使用していること、および各サーバが実行中であることを確認してください。クラスタ内のすべてのサーバに対してネットワーク接続があることを確認するには、各サーバに ping コマンドを発行します。**Start > Run** の順に選択してから、**cmd** と入力し、**OK** をクリックします。コマンド プロンプトで **ping <server>** と入力します。ここで server には Cisco CallManager Administration の Server Configuration ウィンドウに表示されるサーバの名前を指定します。クラスタ内のサーバごとに、ping コマンドを繰り返します。

複数の Cisco CTL クライアントをインストールした場合、Cisco CallManager では一度に 1 台のクライアントの CTL 設定情報しか受け入れません。ただし、設定作業は同時に 5 台までの Cisco CTL クライアントで実行できます。あるクライアントで設定作業を実行している間、その他のクライアントで入力した情報は Cisco CallManager によって自動的に保存されます。

Cisco CTL クライアントの設定完了後に

Cisco CTL クライアントの設定が完了すると、CTL クライアントは次のタスクを実行します。

- CTL ファイルをクラスタ内のすべての Cisco CallManager サーバに書き込む。
- CTL ファイルを設定された代替 TFTP サーバに書き込む。
- CAPF capf.cer をクラスタ内のすべての Cisco CallManager サブスクライバに書き込む。
- PEM 形式の CAPF 証明書ファイルをクラスタ内のすべての Cisco CallManager サブスクライバに書き込む。

クライアントを設定するには、次の手順を実行します。

手順

ステップ 1　購入したセキュリティ トークンを少なくとも 2 つ入手します。

ステップ 2　次の作業のどちらかを実行します。

- インストールしたワークステーションまたはサーバのデスクトップにある **Cisco CTL Client** アイコンをダブルクリックします。
- **Start > Programs > Cisco CTL Client** の順に選択します。

ステップ 3　表 3-2 の説明に従って、Cisco CallManager サーバの設定内容を入力し、**Next** をクリックします。

ステップ 4　表 3-2 の説明にあるように、**Set CallManager Cluster to Mixed Mode** をクリックし、**Next** をクリックします。

ステップ 5　設定する内容に応じて、次の作業を実行します。

- セキュリティ トークンを追加するには、ステップ 6 ～ステップ 12 を参照します。
- 代替 TFTP サーバを追加するには、ステップ 13 ～ ステップ 15 を参照します。
- Cisco CTL クライアント設定を完了するには、ステップ 17 ～ステップ 21 を参照します。

注意　クライアントを初めて設定する場合、少なくとも 2 つのセキュリティ トークンが必要です。アプリケーションが要求しない限り、トークンを挿入しないでください。ワークステーションまたはサーバに USB ポートが 2 つある場合は、2 つのセキュリティ トークンを同時に挿入しないでください。

ステップ 6　アプリケーションが要求したら、現在 Cisco CTL クライアントを設定しているワークステーションまたはサーバで使用可能な USB ポートにセキュリティ トークンを 1 つ挿入して、**OK** をクリックします。

ステップ 7　挿入したセキュリティ トークンについての情報が表示されます。**Add** をクリックします。

ステップ 8　検出された証明書エントリがペインに表示されます。

ステップ 9　他のセキュリティ トークン（複数も可能）を証明書信頼リストに追加するには、**Add Tokens** をクリックします。

ステップ 10　サーバまたはワークステーションに挿入したトークンを取り外していない場合は、取り外します。アプリケーションが要求したら、次のトークンを挿入して **OK** をクリックします。

ステップ 11　2 番目のセキュリティ トークンについての情報が表示されます。**Add** をクリックします。

ステップ 12　すべてのセキュリティ トークンについて、ステップ 9 ～ ステップ 11 を繰り返します。

ステップ 13　証明書エントリがペインに表示されます。代替 TFTP サーバを追加する必要がある場合は、**Add TFTP Server** をクリックします。

ステップ 14　表 3-2 の説明に従って、設定内容を入力します。

ステップ 15　**Next** をクリックします。

ステップ 16　表 3-2 の説明に従って設定内容を入力し、**Next** をクリックします。

ステップ 17　すべてのセキュリティ トークンおよびサーバを追加したら、**Finish** をクリックします。

ステップ 18　表 3-2 の説明に従ってセキュリティ トークンのユーザ パスワードを入力し、**OK** をクリックします。

ステップ 19　クライアントによって CTL ファイルが作成されると、各サーバのウィンドウに、サーバ、ファイル ロケーション、および CTL ファイルのステータスが表示されます。**Finish** をクリックします。

ステップ 20　クラスタ内のすべてのデバイスをリセットします。詳細については、P.1-11 の「デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート」を参照してください。

ステップ 21　Cisco CallManager Serviceability で、クラスタ内の各サーバで実行されている Cisco CallManager および Cisco TFTP サービスを再起動します。

ステップ 22　CTL ファイルを作成したら、USB ポートからセキュリティ トークンを取り外します。すべてのセキュリティ トークンを安全な任意の場所に格納します。

ヒント　Cisco CallManager クラスタが混合モードに設定されたことを確認するには、P.9-1 の「トラブルシューティング」を参照してください。

セキュリティ トークンのパスワード変更を求めるプロンプトが表示される場合は、P.9-1 の「トラブルシューティング」を参照してください。

関連項目

- Cisco CTL クライアント設定（P.3-25）
- システム要件（P.1-5）
- 対話および制限（P.1-6）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Smart Card サービスの Started および Automatic への設定（P.9-12）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Cisco CTL クライアント設定（P.3-25）
- Cisco CTL クライアントの設定（P.3-15）
- CTL ファイルの更新（P.3-21）
- デバイス セキュリティ モードの設定（P.5-7）
- トラブルシューティング（P.9-1）

CTL ファイルの更新

次のシナリオが発生した後に CTL ファイルを更新する必要があります。

- 新しい Cisco CallManager サーバをクラスタに追加した場合
- クラスタ内の Cisco CallManager サーバの名前または IP アドレスを変更した場合
- Cisco CallManager Serviceability で Cisco Certificate Authority Function サービスを有効にした場合
- 新たなセキュリティ トークンを追加または削除した場合
- 代替 TFTP サーバを追加または削除した場合
- Cisco CallManager サーバまたは Cisco CallManager データを復元した場合

変更内容を有効にするには、Cisco CallManager および Cisco TFTP サービスを実行するすべてのサーバの Cisco CallManager Serviceability で、これらのサービスを再起動する必要があります。また、サービスの再起動後にクラスタ内のすべてのデバイスをリセットする必要もあります。この作業を実行する方法の詳細については、P.1-11 の「デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート」を参照してください。

ヒント　ファイルの更新は、コール処理がほとんど中断されないときに実行することを強く推奨します。

CTL ファイルにある情報を更新するには、次の手順を実行します。

手順

ステップ 1　最新の CTL ファイルを設定するために挿入したセキュリティ トークンを 1 つ入手します。

ステップ 2　インストールしたワークステーションまたはサーバのデスクトップにある **Cisco CTL Client** アイコンをダブルクリックします。

ステップ 3　表 3-2 の説明に従って、Cisco CallManager サーバの設定内容を入力し、**Next** をクリックします。

ヒント　このウィンドウでは、Cisco CallManager サーバについて更新します。

ステップ 4　CTL ファイルを更新するには、表 3-2 の説明にあるように **Update CTL File** をクリックし、**Next** をクリックします。

注意　すべての CTL ファイルを更新するには、すでに CTL ファイルに存在するセキュリティ トークン（1 つ）USB ポートに挿入する必要があります。クライアントでは、このトークンを使用して CTL ファイルのシグニチャを検証します。CTL クライアントによってシグニチャが検証されるまで、新しいトークンは追加できません。ワークステーションまたはサーバに USB ポートが 2 つある場合は、両方のセキュリティ トークンを同時に挿入しないでください。

ステップ 5　現在 CTL ファイルを更新しているワークステーションまたはサーバで使用可能な USB ポートにまだセキュリティ トークンを挿入していない場合は、いずれかのセキュリティ トークンを挿入してから **OK** をクリックします。

ステップ 6　挿入したセキュリティ トークンについての情報が表示されます。**Next** をクリックします。

検出された証明書エントリがペインに表示されます。

ヒント　このペインでは、Cisco CallManager および Cisco TFTP エントリを更新できません。Cisco CallManager エントリを更新するには **Cancel** をクリックし、ステップ 2 ～ ステップ 6 をもう一度実行します。

ステップ 7　既存の Cisco CTL エントリを更新するか、あるいはセキュリティ トークンを追加または削除する際は、次の点を考慮してください。

- 代替 TFTP エントリを更新するには、P.3-29 の「CTL ファイル エントリの削除」の説明に従ってエントリを削除してから、P.3-15 の「Cisco CTL クライアントの設定」の説明に従ってエントリを追加する。
- 新しいセキュリティ トークンを追加するには、P.3-15 の「Cisco CTL クライアントの設定」を参照する。
- セキュリティ トークンを削除するには、P.3-29 の「CTL ファイル エントリの削除」を参照する。

ヒント　セキュリティ トークンのパスワード変更を求めるプロンプトが表示される場合は、P.9-1 の「トラブルシューティング」を参照してください。

関連項目

- Cisco CTL クライアント設定（P.3-25）
- システム要件（P.1-5）
- 対話および制限（P.1-6）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Smart Card サービスの Started および Automatic への設定（P.9-12）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Cisco CTL クライアントの設定（P.3-15）
- CTL ファイルの更新（P.3-21）
- デバイス セキュリティ モードの設定（P.5-7）
- トラブルシューティング（P.9-1）

クラスタ全体のセキュリティ モードの更新

クラスタ全体のセキュリティ モードを設定するには、Cisco CTL クライアントを使用する必要があります。クラスタ全体のセキュリティ モードは、Cisco CallManager Administration の Enterprise Parameters ウィンドウで変更することはできません。

Cisco CTL クライアントの初期設定後にクラスタ全体のセキュリティ モードを変更するには、P.3-21 の「CTL ファイルの更新」および表 3-2 の説明に従ってCTL ファイルを更新する必要があります。クラスタ全体のセキュリティ モードを混合モードからノンセキュア モードに変更した場合、CTL ファイルはクラスタ内のサーバに存在したままですが、CTL ファイルに証明書は含まれません。CTL ファイルに証明書が存在しないため、電話機は署名なし設定ファイルを要求し、ノンセキュアとして Cisco CallManager に登録されます。

関連項目

- CTL ファイルの更新（P.3-21）
- Cisco CTL クライアント設定（P.3-25）
- トラブルシューティング（P.9-1）

Cisco CTL クライアント設定

クラスタは、表 3-2 の説明にあるように 2 つのモードのどちらかに設定できます。混合モードだけが認証をサポートしています。Cisco CTL クライアントに暗号化を設定する場合は、Set CallManager Cluster to Mixed Mode を選択する必要があります。

表 3-2 を使用して、初めての Cisco CTL クライアント設定、CTL ファイルの更新、または混合モードからノンセキュア モードへの変更を行うことができます。

表 3-2　CTL クライアントの設定

設定	説明
CallManager サーバ	
Hostname or IP Address	Cisco CallManager または Cisco TFTP サービスを実行しているクラスタ内のサーバについて、ホスト名または IP アドレスを入力します。
Port	ポート番号を入力します。これは、指定した Cisco CallManager サーバで実行されている Cisco CTL Provider サービスの CTL ポートです。デフォルトのポート番号は 2444 です。
Username and Password	Cisco CallManager サーバで管理者特権を持つユーザ名およびパスワードを入力します。 **ヒント**　Cisco CallManager の Administrator または Power User アカウントのユーザ名とパスワードを入力したことを確認します。クラスタ内のすべてのサーバで、同一のユーザ名とパスワードが必要です。

表 3-2　CTL クライアントの設定（続き）

設定	説明
オプション ボタン	
Set CallManager Cluster to Mixed Mode	混合モードでは、認証済みまたは暗号化済みの Cisco IP Phone と、認証されていない Cisco IP Phone を Cisco CallManager に登録することができます。このモードでは、認証済みまたは暗号化済みのデバイスでセキュアな SCCP ポートが使用されることを Cisco CallManager が保証します。 **（注）** クラスタを混合モードに設定すると、Cisco CallManager によって自動登録は無効になります。
Set CallManager Cluster to Non-Secure Mode	すべてのデバイスが非認証として Cisco CallManager に登録されます。Cisco CallManager ではイメージ認証だけをサポートします。 このモードを選択すると、CTL クライアントは CTL ファイルにあるすべてのエントリの証明書を削除しますが、CTL ファイルは引き続き指定したディレクトリに存在します。電話機は署名なし設定ファイルを要求し、ノンセキュアとして CiscoCallManager に登録されます。 **ヒント** 電話機をデフォルトのノンセキュア　モードに戻すには、電話機およびすべての Cisco CallManager サーバから CTL ファイルを削除する必要があります。電話機および Cisco CallManager サーバからの CTL ファイル削除については、P.9-1 の「トラブルシューティング」を参照してください。 **ヒント** このモードでは自動登録を使用できます。
Update CTL File	CTL ファイルの作成後にこのファイルを変更するには、このオプションを選択する必要があります。このオプションを選択すると、クラスタのセキュリティ モードは変更されません。

表 3-2　CTL クライアントの設定（続き）

設定	説明
代替 TFTP サーバ	
Hostname or IP Address	**（注）** 代替 TFTP サーバでは、別のクラスタにある Cisco TFTP サーバを指定します。代替 TFTP サーバ設定で 2 つの異なるクラスタを使用する場合は、両方のクラスタで同じクラスタ全体のセキュリティ モードを使用する必要があります。つまり、両方のクラスタに Cisco CTL クライアントをインストールして設定する必要があります。同様に、どちらのクラスタでも同じバージョンの Cisco CallManager を実行する必要があります。 **注意** TFTP サービス パラメータ FileLocation 内のパスが、クラスタ内のすべてのサーバで同一であることを確認してください。 TFTP サーバのホスト名または IP アドレスを入力します。
Port	ポート番号を入力します。これは、指定した TFTP サーバで実行されている Cisco CTL Provider サービスの CTL ポートです。デフォルトのポート番号は 2444 です。
Username and Password	サーバでローカルの管理者特権を持つユーザ名およびパスワードを入力します。
セキュリティ トークン	
User Password	Cisco CTL クライアントを初めて設定するときは、デフォルト パスワードの **Cisco123** を大文字と小文字を区別して入力し、証明書の秘密キーを取得して CTL ファイルが署名済みであることを確認します。 **ヒント** このパスワードを変更するには、P.9-10 の「セキュリティ トークン パスワード（Etoken）の変更」を参照してください。

関連項目

- システム要件（P.1-5）
- 対話および制限（P.1-6）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Cisco CTL クライアントのインストール（P.3-11）
- Cisco CTL クライアントの設定（P.3-15）
- CTL ファイルの更新（P.3-21）
- デバイス セキュリティ モードの設定（P.5-7）
- トラブルシューティング（P.9-1）

CTL ファイル エントリの削除

Cisco CTL クライアントの CTL Entries ウィンドウに表示される一部の CTL エントリは、いつでも削除することができます。クライアントを開いて、CTL Entries ウィンドウを表示するプロンプトに従い、**Delete Selected** をクリックしてエントリを削除します。

Cisco CallManager、Cisco TFTP、または Cisco CAPF を実行するサーバは、CTL ファイルから削除することができません。CTL ファイルに手動で追加した代替 TFTP サーバおよびセキュリティ トークンは削除できますが、クライアントによって自動検出された TFTP サーバは削除できません。

CTL ファイルには常に 2 つのセキュリティ トークン エントリが存在している必要があります。ファイルからセキュリティ トークンをすべて削除することはできません。

ヒント　Cisco CTL クライアントのアンインストール、電話機からの CTL ファイル削除、またはサーバからの CTL ファイル削除については、P.9-10 の「Cisco CTL クライアントのトラブルシューティング」を参照してください。

関連項目

- システム要件（P.1-5）
- 対話および制限（P.1-6）
- Cisco CTL Provider サービスのアクティブ化（P.3-6）
- Cisco CTL クライアントのインストール（P.3-11）
- Cisco CTL クライアントの設定（P.3-15）
- CTL ファイルの更新（P.3-21）
- デバイス セキュリティ モードの設定（P.5-7）
- トラブルシューティング（P.9-1）