Cisco CTL クライアントのセットアップ

この章では、Cisco CTL クライアントのセットアップについて説明します。

Cisco CTL クライアントの設定について

デバイス認証、ファイル認証、およびシグナリング認証は、証明書信頼リスト（CTL）ファイルの作成に依存します。このファイルは、USB ポートが搭載されている Windows の単一のワークステーションまたはサーバに、シスコの CTL クライアントをインストールして設定すると作成されます。

（注） Cisco CTL クライアント用にサポートされる Windows のバージョンには、Windows Vista、Windows 7、Windows 8.1、および Windows 10 があります。Cisco CTL クライアントをインストールするために、ターミナル サービスを使用しないでください。Cisco Technical Assistance Center（TAC）がリモートからトラブルシューティングと設定作業を行えるように、シスコの方でターミナル サービスをインストールします。

（注）

- 混合モードを有効にするかまたは CTL ファイルを更新するには、エクスポート制御機能を許可するオプションを有効にする、Smart アカウントまたは仮想アカウントから受信した登録トークンを使用することにより、Cisco Unified Communications Manager で Smart ライセンス登録が完了していることを確認します。シスコ スマート ソフトウェア ライセンシングの設定方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）の「Smart Software Licensing」の章を参照してください。
- CTL クライアントを実行しているものの、Cisco Unified Communications Manager がエクスポート制御機能に対応していない場合、*ClusterModeSecurityFailedExportControlNotAllow* というアラームが送信されます。

CTL ファイルには、次のサーバまたはセキュリティ トークンのエントリが含まれています。

- System Administrator Security Token（SAST）
- 同じサーバ上で実行されている Cisco CallManager サービスと Cisco TFTP サービス
- Certificate Authority Proxy Function（CAPF）

- TFTP サーバ（複数の場合あり）
- ASA ファイアウォール

CTL ファイルには、サーバごとのサーバ証明書、公開キー、シリアル番号、署名、発行者名、サブジェクト名、サーバ機能、DNS 名、および IP アドレスが含まれています。

CTL ファイルを作成したら、Cisco CallManager サービスと Cisco TFTP サービスが実行されているすべてのノード上の [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] でこれらのサービスを再起動する必要があります。電話機が次回初期化されたときに、その電話機ではこの CTL ファイルを TFTP サーバからダウンロードします。CTL ファイルに自己署名証明書が含まれた TFTP サーバのエントリがある場合、電話機では .sgn 形式の署名付き設定ファイルを要求します。TFTP サーバに証明書が含まれていない場合、電話機では署名なしのファイルを要求します。

Cisco CTL クライアントで CTL ファイルにサーバ証明書が追加されると、CTL クライアントの GUI でその証明書を表示できます。

CTL ファイルにファイアウォールを設定すると、セキュアな Cisco Unified Communications Manager システムの一部として Cisco ASA ファイアウォールを保護できます。Cisco CTL クライアントでは、ファイアウォール証明書が「CCM」証明書として表示されます。

[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] では、etoken を使用して Cisco CTL クライアントと Cisco CTL Provider との間の TLS 接続を認証します。

リカバリのために CTL ファイル内に 2 番目の SAST ロールを追加する

以前のリリースの Cisco Unified Communications Manager では、トークンレス（トークンなし）アプローチが使用されていました。このアプローチでは、エンドポイントで 1 つの Cisco Site Administrator Security Token（SAST）だけを信頼します。この SAST は CallManager 証明書です。このアプローチでは、証明書信頼リスト（CTL）ファイルに、CTL ファイルへの署名に使用された 1 つの SAST レコードだけが含まれていました。1 つの SAST だけが使用されていたため、SAST の署名者のなんらかの更新が原因で、エンドポイントがロックアウトされて（締め出されて）いました。エンドポイントが SAST の署名者の更新が原因でロックアウトされるシナリオを次に示します。

- エンドポイントで、登録時に CallManager 証明書の使用によって署名された CTL ファイルを受け入れた場合。
- 管理者が CallManager 証明書を再度生成して、CTL ファイルを更新した場合。この再生成は、更新した CTL ファイルが既存の CallManager 証明書ではなく、更新した CallManager 証明書によって署名されたことを意味しています。
- 更新した証明書がエンドポイントの信頼リストで取得できなかったため、その更新した CallManager 証明書をエンドポイントで信頼しなかった場合。このため、そのエンドポイントでは、その CTL ファイルをダウンロードするのではなく拒否しました。

- エンドポイントで、Transport Layer Security（TLS）を使用して ccm サービスと安全に接続しようとし、ccmservice がその更新した CallManager 証明書をエンドポイントに TLS 交換の一部として提供した場合。その更新した証明書がエンドポイントの信頼リストで取得できなかったので、エンドポイントではその CTL ファイルをダウンロードするのではなく拒否しました。
- 電話機が ccmservice と通信しなくなり、その結果ロックアウトされた場合。

エンドポイントのロックアウトからのリカバリを容易にするために、エンドポイント用のトークンレス アプローチが、リカバリのために CTL ファイル内に 2 番目の SAST を追加することによって拡張されました。この機能では、トークンレス CTL ファイルに CallManager レコードと ITLRecovery レコードという 2 つの SAST トークンが含まれています。

ITLRecovery 証明書が、次の理由から他の証明書よりも優先して選択されます。

- ホスト名の変更など、二次的な理由で変化しないため。
- ITL ファイル内ですでに使用されているため。

CLI によるクラスタ暗号化設定

CLI を使用して、Cisco CTL クライアントを使用せずにクラスタ セキュリティ モードを管理できます。

次の点を考慮してください。

- この方法では、CTL ファイルは Cisco CTL クライアントを介する代わりに CLI を使用して生成されます。
- ハードウェア トークンが不要です。
- CTL ファイルは CallManager 証明書秘密キーによって署名されます。

この暗号化オプションは次の CLI コマンドから構成されます。

utils ctl set-cluster mixed-mode

CTL ファイルを更新し、クラスタを混合モードに設定します。

utils ctl set-cluster non-secure-mode

CTL ファイルを更新し、クラスタを非セキュア モードに設定します。

utils ctl update CTLFile

クラスタ内の各ノードの CTL ファイルを更新します。

（注）
- パブリッシャ ノードの CLI コマンドを実行する必要があります。
- CallManager 証明書を再作成すると、ファイルの署名者が変更されることに注意してください。デフォルトでセキュリティをサポートしていない電話機は、電話機から CTL ファイルが手動で削除されない限り、新しい CTL ファイルを受け入れません。

関連トピック

Cisco Unified IP Phone サポート リストの取得

クラスタ暗号化のための CTL クライアントへの回帰

CLI コマンドセットの **utils ctl** を使用してクラスタを暗号化した場合は、Cisco CTL クライアントのオプションに戻ることができます。

Cisco CTL クライアントによるオプションに戻るか、クラスタを非セキュア モードに戻すには、この手順に従います。

手順

ステップ 1 CLI コマンド **utils ctl set-cluster non-secure-mode** を使用して、クラスタを非セキュア モードに設定できます。

ステップ 2 CLI コマンド **file delete tftp** *CTLFile.tlv* を使用してパブリッシャ ノードの `CTLFile.tlv` を削除します。

ステップ 3 Windows のマシンでは、Safenet 8.2 ユーティリティを開き、次の手順を実行します。

a) [詳細ビュー（Advanced View）] > [Safenet 認証クライアントツール（Safenet Authentication Client Tools）] > [トークン（Token）] に移動します。
b) 最初の USB トークンを挿入し、証明書を右クリックします。
c) PC 上の任意の場所にエクスポートします。
d) 2 つめの USB トークンについて同じ手順を実行します。

ステップ 4 Cisco Unified OS の管理 GUI で [セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [証明書のアップロード（Upload Certificate）] に移動し、次のステップを実行します。

a) [証明書のアップロード（Upload Certificate）] から、証明書の名前「Phone-SAST-Trust」を選択します。
b) 手順 3 で USB トークンからエクスポートされた証明書の中で、インポートする最初の証明書を選択します。
c) 上記の手順により、残りの USB トークンの証明書をインポートします。

信頼フォルダに 2 つの証明書をインポートした後、Cisco CTL クライアントを実行し、クラスタをセキュア モードに移行できます。

eToken Run Time Environment 3.00 for CTL Client 5.0 プラグインの削除

CTL クライアント プラグイン 5.0 または 5.2 にアップグレードする場合は、次の手順を実行して、最初に eToken Run Time Environment 3.00 を削除する必要があります。

手順

ステップ 1 次の URL で Windows Installer Cleanup ユーティリティをダウンロードします。
http://support.microsoft.com/kb/290301

ステップ 2 ユーティリティを PC にインストールします。

ステップ 3 ユーティリティを実行します。

ステップ 4 プログラムの一覧で eToken rte3.0 を見つけて、削除します。

ステップ 5 CTL クライアントのインストールに進みます。

Cisco CTL クライアントの設定のヒント

Cisco Unified Communications Manager で Cisco CTL クライアントを設定する場合、以下の情報を検討してください。

- 電話では大きなサイズの CTL ファイルを受け付けられないため、Cisco CTL クライアントでは CTL ファイルのサイズが 64 キロバイトに制限されています。CTL ファイルのサイズには、以下の要素が影響します。
  - クラスタ内のノード数

    ノードが増えると、CTL ファイル内の証明書も増やす必要があります。
  - TLS プロキシに使用されているファイアウォールの数

    TLS プロキシ機能を備えたファイアウォールは、ノードと同様であるため、CTL ファイルに組み込まれます。
  - 外部認証局（CA）が CAPF 証明書と CallManager 証明書に署名するかどうか

    外部 CA によって署名された証明書（CAPF/CallManager）は、デフォルトの自己署名証明書に比べて大幅に大きなものになるため、CTL ファイルに入る証明書の最大数が制限される場合があります。

    これらの要素が 64 キロバイトの CTL ファイルに入れられる証明書の最大数に影響し、セキュアな Cisco Unified Communications Manager デプロイに含めることのできるノードとファイアウォールの数が決まります。

- Cisco CTL クライアントのインストールされたリモート PC で Cisco Unified Communications Manager ノードのホスト名を解決できることを確認します。解決できない場合、Cisco CTL クライアントは正常に機能しません。
- Cisco CTL Provider サービスをアクティブにする必要があります。クラスタ環境が存在する場合、クラスタ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。
- CTL ファイルの作成または更新の後には、Cisco CallManager サービスと Cisco TFTP サービスが実行されている Cisco Unified Communications Manager すべてとクラスタ内のすべての TFTP サーバで、Cisco Unified Serviceability にあるこれらのサービスを再起動する必要があります。
- Cisco CTL クライアントに、代替または集中型 TFTP サーバなどのオフクラスタ サーバ エントリが含まれる場合、これらのサーバでも Cisco CTL Provider サービスを実行する必要があります。
- Cisco CTL クライアント GUI の 代替 TFTP サーバセクションは、別のクラスタに存在する Cisco TFTP サーバを指定します。[代替 TFTP サーバ（Alternate TFTP Server）] タブの設定を使用して、Cisco CTL クライアントの代替および集中型 TFTP サーバを設定します。

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

- 集中型 TFTP 構成の場合、混合モードで稼働しているクラスタ外の TFTP サーバすべては、マスター TFTP サーバまたはマスター TFTP サーバ IP アドレスをクラスタ外 CTL ファイルに追加する必要があります。マスター TFTP サーバは、マスター TFTP サーバに設定された代替ファイル リスト内のすべての代替 TFTP サーバの設定ファイルを処理します。集中型 TFTP 構成内のクラスタでは、同じセキュリティ モードを使用する必要がありません。各クラスタにそれぞれのモードを選択できます。

Cisco CTL クライアントの設定

CTL クライアント オプションを使用している場合は、次の手順を実行します。

（注） この手順では、Cisco CTL クライアント用に設定する複数のサーバについて、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することが必要です。

次の表に、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。Cisco Unified Communications Manager をアップグレードする場合の CTL ファイルの設定に関する詳細については、Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行に関連したトピックを参照してください。

手順

ステップ 1 Cisco CTL クライアント用に設定する複数のサーバについて、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。

ステップ 2 クラスタ内のすべてのサーバがオンラインになっており、CTL クライアントを実行予定の PC から到達可能であることを確認します。サーバがホスト名を使用して設定されている場合、そのホスト名を ping して到達可能であることを確認します。

ステップ 3 クラスタ サーバのすべてのホスト名が、パブリッシャ サーバに設定されている DNS サーバで定義されていることを確認します。

ステップ 4 [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] で Cisco CTL Provider サービスをアクティブにします。
クラスタ内の各 Cisco Unified Communications Manager サーバで Cisco CTL Provider サービスをアクティブにします。

ヒント Cisco Unified Communications Manager のアップグレードの前に、このサービスをアクティブにしていた場合、このサービスを再度アクティブにする必要はありません。このサービスは、アップグレード後に自動的にアクティブになります。

ステップ 5 [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] で Cisco Certificate Authority Proxy サービスをアクティブにします。

ヒント クラスタ内の最初のノードでのみ 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。

ステップ 6 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 Cisco Unified Communications Manager のアップグレードの前に、これらの設定項目を設定していた場合は、設定項目は自動的に移行されます。

ステップ 7 Cisco CTL クライアントをインストールします。

ステップ 8 Cisco CTL クライアントを設定します。

関連トピック

Certificate Authority Proxy Function（CAPF）サービスの有効化
Cisco CTL Provider サービスの有効化, （9 ページ）
Cisco CTL クライアントのインストール, （12 ページ）
CTL クライアント、SSL、認証局プロキシ機能（CAPF）、およびセキュリティ トークンのインストール
TLS 接続のポートの設定, （10 ページ）
システム要件
Cisco CTL クライアントのアップグレードと Cisco CTL ファイルの移行, （14 ページ）

Cisco CTL Provider サービスの有効化

Cisco CTL クライアントの設定後、Cisco CTL プロバイダー サービスのセキュリティ モードは非セキュアから混合モードに変わり、サーバの証明書を CTL ファイルに伝送します。サービスは、CTL ファイルをすべての Cisco Unified Communications Manager および Cisco TFTP サーバに伝送します。

このサービスを有効にし、Cisco Unified Communications Manager をアップグレードすると、Cisco Unified Communications Manager は、アップグレード後に自動的にサービスを再起動します。

ヒント クラスタ内のすべてのサーバで Cisco CTL プロバイダー サービスを有効化する必要があります。

このサービスを有効化するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Serviceability で、[ツール（Tools）] > [サービスの有効化（Service Activation）] を選択します。

ステップ 2 [サーバ（Servers）] ドロップダウン リスト ボックスで、Cisco CallManager または Cisco TFTP サービスが有効になっているサーバを選択します。

ステップ 3 [Cisco CTL プロバイダー（Cisco CTL Provider）] サービスのオプション ボタンをクリックします。

ステップ 4 [保存（Save）] をクリックします。

ヒント 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） Cisco CTL プロバイダー サービスを有効にする前に、CTL ポートを入力できます。デフォルトのポート番号を変更するには、TLS 接続へのポートの設定に関するトピックを参照してください。

ステップ 5 サービスがサーバで実行されていることを確認します。Cisco Unified Serviceability で、[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）] を選択し、サービスの状態を確認します。

関連トピック

TLS 接続のポートの設定, （10 ページ）

シスコ認証局プロキシ機能（CAPF）サービス有効化

警告 Cisco CTL クライアントをインストールして設定する前に、Cisco Certificate Authority Proxy Function（CAOF）サービスを有効化すると、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。

関連トピック

Certificate Authority Proxy Function（CAPF）サービスの有効化

TLS 接続のポートの設定

デフォルト ポートが現在使用中の場合、または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、異なる TLS ポート番号の設定が必要になることがあります。

- Cisco CTL Provider の TLS 接続用のデフォルト 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モニタします。このポートでは、CTL ファイルの取得、クラスタ セキュリティ モードの設定、TFTP サーバへの CTL ファイルの保存などの、Cisco CTL クライアントの要求を処理します。

（注） クラスタ セキュリティ モードでは、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。

- イーサネット電話ポートでは、SCCP を実行中の電話機からの登録要求をモニタします。非セキュア モードでは、電話機はポート 2000 を介して接続されます。混合モードでは、TLS 接続用の Cisco Unified Communications Manager ポートは、Cisco Unified Communications Manager のポート番号に 443 を加算（+）した番号になるため、Cisco Unified Communications Manager のデフォルトの TLS 接続ポートは 2443 になります。この設定は、ポート番号が使用中の場合、または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のみ更新します。
- SIP セキュア ポートを使用すると、Cisco Unified Communications Manager で、SIP を実行中の電話機からの SIP メッセージをリッスンできます。デフォルト値は 5061 です。このポートを変更した場合は、[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] で Cisco CallManager サービスを再起動して、SIP を実行中の電話機をリセットする必要があります。

ヒント　ポートを更新した後、[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] で Cisco CTL Provider サービスを再起動する必要があります。

ヒント　CTL ポートは、CTL クライアントが実行されている場所からデータ VLAN に対して開く必要があります。

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。

a) Cisco CTL Provider サービスの Port Number パラメータを変更するには、ステップ 2, （11 ページ）からステップ 6, （12 ページ）を実行します。

b) [イーサネット電話ポート（Ethernet Phone Port）] または [SIP 電話セキュア ポート（SIP Phone Secure Port）] の設定を変更するには、ステップ 7, （12 ページ）からステップ 11, （12 ページ）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 Unified CM の管理（Cisco Unified Communications Manager Administration）] 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 3　[サーバ（Server）] ドロップダウン リストで、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　[サービス（Service）] ドロップダウン リスト ボックスで、[Cisco CTL Provider サービス（Cisco CTL Provider service）] を選択します。

ヒント　サービス パラメータの詳細については、疑問符またはリンク名をクリックしてください。

ステップ 5 Port Number パラメータの値を変更するには、[パラメータ値（Parameter Value）] 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 [保存（Save）] をクリックします。

ステップ 7 [イーサネット電話ポート（Ethernet Phone Port）] または [SIP 電話セキュア ポート（SIP Phone Secure Port）] の設定を変更するには、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で [システム（System）] > [Cisco Unified CM] を選択します。

ステップ 8 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従い、Cisco CallManager サービスが実行されているサーバを検索します。結果が表示されたら、そのサーバの[名前（Name）] リンクをクリックします。

ステップ 9 Cisco Unified Communications Manager の [設定] ウィンドウが表示されたら、[イーサネット電話ポート（Ethernet Phone Port）] フィールドまたは [SIP 電話セキュア ポート（SIP Phone Secure 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 電話機をリセットし、[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] で Cisco CallManager サービスを再起動します。

ステップ 11 [保存（Save）] をクリックします。

関連トピック

Cisco CTL クライアントのインストール

（注） CLI を使ってクラスタ セキュリティを管理する場合は、この手順は必要ありません。

次のイベントの発生時には、クライアントを使用して CTL ファイルを更新してください。

- クラスタ セキュリティ モードをはじめて設定するとき
- CTL ファイルをはじめて作成するとき
- Cisco Unified Communications Manager をインストールした後
- Cisco Unified Communications Manager サーバまたは Cisco Unified Communications Manager データを復元した後
- Cisco Unified Communications Manager サーバの IP アドレスやホスト名を変更した後
- Cisco CTL クライアントを使用したセキュリティ トークンの追加後または削除後
- ASA ファイアウォールの追加後または削除後
- TFTP サーバの追加後または削除後
- Cisco Unified Communications Manager サーバの追加後または削除後
- サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後

ヒント　クライアントをインストールする予定のサーバまたはワークステーションでSmart Cardサービスが起動しており、自動で起動するように設定されていないと、インストールは失敗します。

Windows 用の Cisco CTL クライアントのインストール

Windows Vista、Windows 7、Windows 8.1、Windows 10 へ 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　クライアントをインストールするWindowsワークステーションまたはサーバから、『*Administration Guide for Cisco Unified Communications Manager*』の説明に沿って Cisco Unified Communications Manager Administration を参照します。

ステップ 2　[Cisco Unified Communications Managerの管理（Cisco Unified Communications Manager Administration）] で、[アプリケーション（Application）] > [プラグイン（Plugin）] を選択します。
[プラグインの検索/一覧表示（Find and List Plugins）] ウィンドウが表示されます。

ステップ 3　[プラグイン タイプ（Plugin Type equals）] ドロップダウン リスト ボックスから、[インストール（Installation）] を選択し、[検索（Find）] をクリックします。

ステップ 4　Cisco CTL クライアントを探します。

ステップ 5　ファイルをダウンロードするには、ウィンドウ左側にある Cisco CTL クライアント プラグイン名の反対にある [ダウンロード（Download）] をクリックします。

ステップ 6　[保存（Save）] をクリックして、ファイルを適切な場所に保存します。ファイルの場所を控えておいてください。

ステップ 7　インストールを開始するには、[Cisco CTL クライアント（Cisco CTL Client）]（ファイルの保存場所によりアイコンまたは実行ファイル）をダブルクリックします。
（注）　または、[ダウンロードの完了（Download Complete）] ボックスで [開く（Open）] をクリックします。

ステップ 8　Cisco CTL クライアントのバージョンが表示されますので、[次へ（Next）] をクリックします。

ステップ 9　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 10　使用許諾契約に同意して、[次へ（Next）] をクリックします。

ステップ 11　クライアントをインストールするフォルダを選択します。必要に応じて、[参照（Browse）] をクリックし、場所を選択して [次へ（Next）] をクリックすることでデフォルトの場所を変更できます。

ステップ 12　インストールを開始するには、[次へ（Next）] をクリックします。

ステップ 13　インストールが完了したら、[終了（Finish）] をクリックします。

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

Cisco Unified Communications Manager リリース 5.x から 6.x へのアップグレード後に CTL ファイルを変更する場合は、アップグレード前にインストールした Cisco CTL クライアントをアンインストールし、最新の Cisco CTL クライアントをインストールして CTL ファイルを再生成する必要があります。アップグレード前にサーバを削除または追加しなかった場合は、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 Unified Communications Manager のアップグレードで、データが CTL ファイルに自動的に移行されます。

Cisco Unified Communications Manager リリース 4.x からリリース 6.x にアップグレードして、セキュリティがクラスタで有効な場合は、アップグレード前にインストールした Cisco CTL クライアントをアンインストールし、最新の Cisco CTL クライアントをインストールして CTL ファイルを再生成する必要があります。アップグレードされたクラスタのセキュリティを有効にするには、次の手順に従います。

手順

ステップ 1 既存の Cisco CTL クライアントをアンインストールします。

ステップ 2 新しい Cisco CTL クライアントをインストールします。

ステップ 3 以前に使用していた USB キーの少なくとも 1 つを使用して、Cisco CTL クライアントを実行します。

ステップ 4 クラスタ内の Cisco CallManager と Cisco TFTP サービスを実行するすべての Cisco Unified Communications Manager サーバとすべての TFTP サーバの Cisco Unified Serviceability でCisco CallManager と Cisco TFTP サービスを再起動します。

関連トピック

Cisco CTL クライアントのインストール, （12 ページ）
詳細情報の入手先

Cisco CTL クライアントの設定

重要 この情報は CTL クライアント暗号化オプションに適用されます。また、**utils ctl** CLI コマンドセットを使用して暗号化を設定することもできます。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

（注）

- CLI コマンド **utils ctl set-cluster mixed-mode** は、混合モードでクラスタを設定します。混合モードを有効にするには、Cisco Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されていること、また、このクラスタへの登録中に、Smart アカウントまたは仮想アカウントから受信した登録トークンで、エクスポート制御機能を許可するオプションが有効になっていることを確認します。
- CLI コマンド **utils ctl update CTLFile** は、CTL ファイルを更新します。混合モードで CTL ファイルを更新にするには、Cisco Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されていること、また、このクラスタへの登録中に、Smart アカウントまたは仮想アカウントから受信した登録トークンで、エクスポート制御機能を許可するオプションが有効になっていることを確認します。
- エクスポート制御機能を許可するオプションが有効になっている登録トークンに Cisco Unified Communications Manager が登録されていない場合、**utils ctl set-cluster mixed-mode** コマンドまたは **utils ctl update CTLFile** コマンドを実行すると、次のエラー メッセージが表示されます。

  ```
  Command cannot be executed because the Unified Communications Manager
  cluster is not registered to a Smart/Virtual Account with Allow
  export-controlled functionality.Please ensure Product Token received
  from the Smart/Virtual Account has Allow export-controlled
  functionality checked when registering the UCM Cluster.
  ```

Cisco CTL クライアントでは、次のタスクが実行されます。

- クラスタまたはスタンドアロン サーバ用の Cisco Unified Communications Manager セキュリティモードを設定します。

（注） Cisco Unified Communications Manager Administration のエンタープライズ パラメータ設定ウィンドウで、Cisco Unified Communications Manager のクラスタ セキュリティパラメータを混合モードに設定することはできません。Cisco CTL クライアントまたは CLI コマンドセット **utils ctl** からクラスタ セキュリティモードを設定できます。

- 証明書信頼リスト（CTL）を作成します。これは、セキュリティ トークン、Cisco Unified Communications Manager、ASA ファイアウォール、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 Unified Communications Manager、Cisco CAPF、および ASA ファイアウォールを検出し、これらのサーバの証明書エントリを追加します。

  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。

（注） Cisco CTL クライアントは、スーパークラスタ サポートも提供します。スーパークラスタには、最大 16 のコールを処理するサーバ、1 つのパブリッシャ、2 つの TFTP サーバ、および最大 9 つのメディア リソース サーバが含まれます。

ヒント Cisco CTL クライアントの設定は予定されたメンテナンス期間中に行います。これは、クラスタ内で Cisco CallManager サービスおよび Cisco TFTP サービスを実行するすべてのサーバ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 Cisco Unified Communications Manager サーバに書き込みます。
- CAPF capf.cer をクラスタ内のすべての Cisco Unified Communications Manager 後続ノード（最初のノード以外）に書き込みます。
- PEM 形式の CAPF 証明書ファイルをクラスタ内のすべての Cisco Unified Communications Manager 後続ノード（最初のノード以外）に書き込みます。
- すべての設定済み TFTP サーバにこのファイルを書き込みます。
- すべての設定済み ASA ファイアウォールにこのファイルを書き込みます。
- CTL ファイルを作成した時点で USB ポートに存在するセキュリティ トークンの秘密キーを使用して、CTL ファイルに署名します。

クライアントを設定するには、次の手順を実行します。

（注） CLI コマンド セット **utils ctl** でクラスタ セキュリティを管理する場合は、この手順は必要ありません。

はじめる前に

ヒント Cisco Unified Communications Manager をアップグレードする場合の CTL ファイルの設定に関するより詳細な情報については、Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行に関連したトピックを参照してください。

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 Unified 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、シスコの認証局が発行します。シスコから取得したセキュリティ トークンを使用する必要があります。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 ポートがない場合は、USB PCI カードを使用できます。

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 Unified Communications Manager の管理ユーザ名とパスワード

ヒント　管理ユーザ名は、エンドユーザではなく、アプリケーションユーザである必要があり、また、スーパーユーザ権限を持つスーパー ユーザ グループのメンバーでなければなりません。

- セキュリティ トークンの管理者パスワード
- ASA ファイアウォールの管理ユーザ名とパスワード

これらの情報の説明については、表 2：CTL クライアント構成時の設定, （26 ページ） 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、サーバへのネットワーク接続を確認します。ネットワーク接続が確立されていることを確認するには、『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って ping コマンドを実行します。 クラスタの設定で、クラスタ内のすべてのサーバにネットワーク接続できることを確認してください。

複数の Cisco CTL クライアントをインストールした場合、Cisco Unified Communications Manager 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 Unified Communications Manager 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 Cisco Unified Communications Manager サーバに書き込みます。
- CAPF capf.cer をクラスタ内のすべての Cisco Unified Communications Manager 後続ノード（最初のノード以外）に書き込みます。
- PEM 形式の CAPF 証明書ファイルをクラスタ内のすべての Cisco Unified Communications Manager 後続ノード（最初のノード以外）に書き込みます。
- すべての設定済み TFTP サーバにこのファイルを書き込みます。
- すべての設定済み ASA ファイアウォールにこのファイルを書き込みます。
- CTL ファイルを作成した時点で USB ポートに存在するセキュリティ トークンの秘密キーを使用して、CTL ファイルに署名します。

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　次のいずれかの作業を実行します。

a) Cisco CTL クライアントを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 クライアント] アイコンをダブルクリックします。
b) [スタート（Start）]>[プログラム（Programs）]>[Cisco CTL クライアント（Cisco CTL Client）] の順に選択します。

ステップ 3 表 2：CTL クライアント構成時の設定, （26 ページ） の説明に従って、Cisco Unified Communications Manager サーバの設定項目を入力して、[次へ（Next）] をクリックします。

ステップ 4 [Cisco Unified Communications Manager クラスタを混合モードに設定する（Set Cisco Unified Communications Manager Cluster to Mixed Mode）] をクリックして、[次へ（Next）] をクリックします。
フィールドの説明については、表 2：CTL クライアント構成時の設定, （26 ページ）を参照してください。

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。

a) セキュリティ トークンを追加するには、Cisco CTL クライアントのセットアップ, （1 ページ）～Cisco CTL クライアントのセットアップ, （1 ページ）を参照します。
b) Cisco CTL クライアントの設定を完了するには、Cisco CTL クライアントのセットアップ, （1 ページ）～Cisco CTL クライアントのセットアップ, （1 ページ）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。[追加（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、[トークンの追加（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次のトークンを要求したら、そ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 番めのセキュリティ トークンについての情報が表示されます。[追加（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、Cisco CTL クライアントのセットアップ, （1 ページ）～ Cisco CTL クライアントのセットアップ, （1 ページ）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。

ステップ 14 設定項目を入力します。
フィールドの説明については、表 2：CTL クライアント構成時の設定, （26 ページ）を参照してください。

ステップ 15 [Next] をクリックします。

ステップ 16 設定項目を入力して、[次へ（Next）] をクリックします。
フィールドの説明については、表 2：CTL クライアント構成時の設定, （26 ページ）を参照してください。

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、[終了（Finish）] をクリックします。

ステップ 18 セキュリティ トークンのユーザ名とパスワードを入力し、[OK] をクリックします。
フィールドの説明については、表 2：CTL クライアント構成時の設定, （26 ページ）を参照してください。

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、ファイルの場所、および CTL ファイルのステータスが表示されます。[終了（Finish）] をクリックします。

ステップ 20 スタンドアロン サーバまたはクラスタのすべてのデバイスをリセットします。

ステップ 21 Cisco Unified Serviceability で、Cisco CallManager サービスと Cisco TFTP サービスを再起動します。
ヒント これらのサービスを実行するすべての Cisco Unified Communications Manager サーバとクラスタ内のすべての TFTP サーバで、これらのサービスを再起動します。

ステップ 22 CTL クライアントを通じて CTL ファイルを作成したら、USB ポートからセキュリティ トークンを取り外すことができます。すべてのセキュリティ トークンを覚えやすい安全な場所に格納します。

関連トピック

Cisco CTL クライアントの設定, （25 ページ）
デバイスのリセット、サーバとクラスタのリブート、サービスの再起動
Cisco CTL クライアントのアップグレードと Cisco CTL ファイルの移行, （14 ページ）
詳細情報の入手先

CTL ファイルの SAST 役割

（注） CTL ファイルに署名するには、次の表に記載されている*署名者が使用されます。

表 *1* : *CTL* ファイルのシステム管理者セキュリティ トークン（*SAST*）役割

Cisco Unified Communications Manager のバージョン	トークンベースの CTL ファイルでの SAST 役割	Tokenless CTL ファイルでの SAST 役割
12.0(1)	トークン 1（署名者*） トークン 2 ITLRecovery CallManager	CallManager（署名者） ITLRecovery
11.5(x)	トークン 1（署名者） トークン 2 ITLRecovery CallManager	CallManager（署名者） ITLRecovery
10.5(2)	トークン 1（署名者） トークン 2	CallManager（署名者） ITLRecovery
10.5(1) （サポート外）	トークン 1（署名者） トークン 2	CallManager（署名者）
10.0(1) （サポート外）	トークン 1（署名者） トークン 2	CallManager（署名者）
9.1(2)	トークン 1（署名者） トークン 2	N/A

クラスタ間での電話の移行

クラスタ間で電話を移動するには、次の手順に従ってください。たとえば、クラスタ 1 からクラスタ 2 に移動するとします。

（注） トークン ベースの CTL クライアント アプローチなら、移行はシームレスです。電話移行の場合は、両方のクラスタで CTL ファイル生成のために使用される etoken が同じであることを管理者が確認する必要があります。

手順

ステップ 1 クラスタ 2 で、Cisco Unified OS の管理から、[セキュリティ（Security）]>[証明書の管理（Certificate Management）] を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 証明書の一覧で、ITLRecovery 証明書をクリックし、[.PEM ファイルのダウンロード（Download .PEM File）] または [.DER ファイルのダウンロード（Download .DER File）] のいずれかをクリックすることにより、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 4 証明書の一覧で、CallManager 証明書をクリックし、[.PEM ファイルのダウンロード（Download .PEM File）] または [.DER ファイルのダウンロード（Download .DER File）] のいずれかをクリックすることにより、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 5 クラスタ 1 で、Cisco Unified OS の管理から、[セキュリティ（Security）]>[証明書の管理（Certificate Management）] を選択します。
[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 6 [証明書チェーンのアップロード（Upload Certificate Chain）] をクリックすることにより、ダウンロードした証明書をアップロードします。

ステップ 7 [証明書の目的（Certificate Purpose）] ドロップダウン リストで、[電話と SAST 間の信頼（Phone-SAST-trust）] を選択します。

ステップ 8 [ファイルのアップロード（Upload File）] フィールドで、[ファイルの選択（Choose File）] をクリックし、手順 3 でダウンロードした ITLRecovery ファイルを参照し、[ファイルのアップロード（Upload File）] をクリックします。

アップロードされた ITLRecovery ファイルが、クラスタ 1 の [証明書リスト（Certificate List）] ウィンドウで [電話と SAST 間の信頼（Phone-SAST-Trust）] 証明書に対して表示されます。新しい ITL ファイルにクラスタ 2 の ITLRecovery 証明書がある場合は、コマンド `show itl` を実行します。

ステップ 9 クラスターの電話にローカルで有効な証明書（LSC）がある場合、クラスタ 1 からの CAPF 証明書をクラスタ 2 の CAPF 信頼ストアにアップロードしなければなりません。

ステップ 10 （任意） この手順は、クラスタが混合モードの場合にのみ適用可能です。CLI で **utils ctl update CTLFile** コマンドを実行することにより、CTL ファイルをクラスタ 1 で再生成します。

（注）
- `show ctl` CLI コマンドを実行することにより、クラスタ 2 の ITLRecovery 証明書と CallManager 証明書が、SAST としての役割で CTL ファイルに含められるようにします。
- 電話が新しい CTL ファイルおよび ITL ファイルを受け取っていることを確認します。更新された CTL ファイルには、クラスタ 2 の ITLRecovery 証明書が含まれています。

クラスタ 1 からクラスタ 2 に移行する電話が、クラスタ 2 の ITLRecovery 証明書を受け付けるようになります。

ステップ 11 クラスタ間で電話を移行します。

eToken ベースの CTL ファイルから Tokenless CTL ファイルへの移行

Tokenless CTL ファイルについては、Cisco Unified Communications Manager Release 12.0(1) で USB トークンを使用して生成されたアップロード済み CTL ファイルのダウンロードをエンドポイントで実行するよう、管理者が確認する必要があります。ダウンロード後、管理者は Tokenless CTL ファイルに切り替えることができます。次に、`utils ctl upgrade` CLI コマンドを実行することができます。

CTL ファイルの更新

（注） CLI コマンド セット **utils ctl** でクラスタ セキュリティを管理する場合は、この手順は必要ありません。

次のシナリオが発生したら CTL ファイルを更新する必要があります。

- 新しい Cisco Unified Communications Manager サーバをクラスタに追加する

  （注） ノードをセキュア クラスタに追加するには、ノードの追加方法および新しいノード用のセキュリティの設定方法を説明している『*Installing Cisco Unified Communications Manager*』を参照してください。

- Cisco Unified Communications Manager サーバの名前または IP アドレスを変更する
- 設定されたすべての TFTP サーバの IP アドレスまたはホスト名を変更する
- 設定されたすべての ASA ファイアウォールの IP アドレスまたはホスト名を変更する
- Cisco Unified Serviceability で Cisco Certificate Authority Function サービスを有効にする
- セキュリティ トークンを追加または削除する必要がある
- TFTP サーバを追加または削除する必要がある
- Cisco Unified Communications Manager サーバを追加または削除する必要がある
- ASA ファイアウォールを追加または削除する必要がある
- Cisco Unified Communications Manager サーバまたは Cisco Unified Communications Manager データを復元する
- CTL ファイルを含むCisco Unified Communications Manager クラスタで、手動で証明書を再作成する

- CUCM バージョンの 7.1.5 以前から 7.1.5 以降に更新する
- サードパーティの CA 署名付き証明書をプラットフォームにアップロードした後

（注） 混合モードの Cisco Unified Communications Manager クラスタでドメイン名が追加または変更されると、CTL クライアントを再実行する必要があります。これが行われない場合、電話機の設定ファイルへの変更が適用されません。

ヒント ファイルの更新は、呼処理中断がもっとも少ない時期に行うことが推奨されます。

手順

ステップ 1 最新の CTL ファイルを設定するの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 Cisco CTL クライアントを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 クライアント] アイコンをダブルクリックします。

ステップ 3 Cisco Unified Communications Manager サーバの構成設定を入力し、[次へ（Next）] をクリックします。
フィールドの説明については、表 2：CTL クライアント構成時の設定, （26 ページ）を参照してください。

ヒント Cisco Unified Communications Manager サーバの更新はこのウィンドウで行います。

ステップ 4 CTL ファイルを更新するには、[CTLファイルを更新（Update CTL File）] をクリックして、[次へ（Next）] をクリックします。
フィールドの説明については、表 2：CTL クライアント構成時の設定, （26 ページ）を参照してください。

注意 CTL クライアント オプションを使用してすべての CTL ファイルを更新するには、CTL ファイルにすでに存在するセキュリティ トークン 1 つを USB ポートに挿入する必要があります。クライアントは、このトークンを使用して CTL ファイルの署名を検証します。Cisco CTL クライアントによって署名が検証されるまで、新しいトークンを追加できません。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の利用可能な USB ポートにまだセキュリティ トークン 1 つを挿入していない場合、セキュリティ トークンを挿入して [OK] をクリックします。

ステップ 6 挿入したセキュリティ トークンの情報が表示されるので、[次へ（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 このペインから Cisco Unified Communications Manager、Cisco TFTP、ASA ファイアウォールを更新することはできません。Cisco Unified Communications Manager エントリを更新するには、[キャンセル（Cancel）] をクリックして、ステップ 2, （23 ページ）からステップ 6, （23 ページ）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、セキュリティ トークンを追加または削除します。

ステップ 8 CTL ファイルの更新が終了したら、Cisco Unified Serviceability で Cisco CallManager と TFTP サービスを再起動します。

ヒント これらのサービスを実行しているクラスタのすべてのノードで TFTP と Cisco CallManager サービスを再起動します。

注意 セキュアな SIP または SCCP を使用して Unified Communications Manager が Unity Connection 10.5 以降と統合されている場合は、Unity Connection でセキュアな通話が停止することがあります。この問題を解決するには、Unity Connection で対応するポート グループをリセットする必要があります。

Unity Connection Administration インターフェイスでポート グループをリセットするには、[テレフォニー インテグレーション（Telephony Integrations）] > [ポート グループ（Port Group）] からリセットするポート グループを選択して、**ポート グループ ベーシック** ページで [リセット（Reset）] をクリックします。

関連トピック

CTL ファイル エントリの削除, （24 ページ）
詳細情報の入手先

CTL ファイル エントリの削除

Cisco CTL クライアントの [CTL エントリ（CTL Entries）] ウィンドウに表示される CTL エントリはいつでも削除できます。

Cisco Unified Communications Manager、Cisco TFTP、ASA ファイアウォールまたは Cisco CAPF を実行するサーバは CTL ファイルから削除できません。

CTL ファイルには、常に 2 つのセキュリティ トークン エントリが存在する必要があります。ファイルからすべてのセキュリティ トークンは削除できません。または、CLI コマンドの **utils ctl update CTLFile** を使用して CTL ファイルを更新できます。

手順

クライアントを開いて、プロンプトに従い [CTL エントリ（CTL Entries）] ウィンドウを表示したら、削除する項目を強調表示し、[選択項目の削除（Delete Selected）] をクリックしてエントリを削除します。

関連トピック

Cisco Unified Communications Manager のセキュリティ モードの更新

クラスタ 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。Cisco Unified Communications Manager のセキュリティ モードは、Cisco Unified Communications Manager Administration のエンタープライズ パラメータ設定ウィンドウから変更することはできません。

（注） クラスタ セキュリティ モードでは、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の設定を行います。

Cisco CTL クライアントの初期設定後にクラスタ セキュリティ モードを変更するには、CTL ファイルを更新する必要があります。

混合モードから非セキュア モードにクラスタ セキュリティ モードを変更すると、CTL ファイルはサーバに存在するものの、この CTL ファイルには証明書が含まれていません。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、Cisco Unified Communications Manager に非セキュアとして登録します。

手順

クラスタ セキュリティ モード ウィンドウに移動して、モードの設定を変更し、[次へ（Next）]、そして [終了（Finish）]をクリックします。
詳細については、表 2：CTL クライアント構成時の設定, （26 ページ）を参照してください。

関連トピック

CTL ファイルの更新, （22 ページ）

Cisco CTL クライアントの設定

重要 この情報は CTL クライアント暗号化オプションに適用されます。セキュリティ トークンが不要な **utils ctl**CLI コマンド セットを使用して暗号化を設定することもできます。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

次の表に示すように、クラスタ セキュリティ モードを非セキュア モードまたは混合モードに設定できます。認証、シグナリング暗号化、およびメディア暗号化は混合モードでのみサポートされます。

（注） クラスタ セキュリティ モードでは、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。

Cisco CTL クライアントの初回設定、CTLファイルの更新、または混合モードから非セキュア モードへの変更を行うには、次の表を使用して設定します。

表 *2*：*CTL* クライアント構成時の設定

設定	説明
Cisco Unified Communications Manager サーバ	
[ホスト名（Hostname）] または [IP アドレス（IP Address）]	最初のノードのホスト名または IP アドレスを入力します。
[ポート（Port）]	この Cisco Unified Communications Manager サーバで実行されている Cisco CTL Provider サービスの CTL ポート番号を入力します。デフォルトのポート番号は 2444 です。
ユーザ名とパスワード	最初のノードのスーパーユーザ管理者権限を持つのと同じアプリケーション ユーザ名とパスワードを入力します。
セキュリティ モード（Security Mode）	
Cisco Unified Communications Manager クラスタの混合モードへの設定	混合モードでは、承認済み、暗号化済み、および非セキュアの Cisco Unified IP Phone を Cisco Unified Communications Manager に登録できます。このモードでは、承認済みまたは暗号化済みのデバイスについて、Cisco Unified Communications Manager によってセキュアなポートの使用が確保されます。

設定	説明
Cisco Unified Communications Manager クラスタの非セキュア モードへの設定	非セキュア モードに設定すると、すべてのデバイスが非認証として登録され、Cisco Unified Communications Manager によってイメージ認証のみがサポートされます。 このモードを選択すると、Cisco CTL クライアントによって CTL ファイル内の一覧にあるすべてのエントリの証明書が削除されますが、CTL ファイルそのものは指定のディレクトに引き続き存在します。未署名のコンフィギュレーション ファイルが電話によってリクエストされ、Cisco Unified Communications Manager に非セキュアとして登録されます。 **ヒント** デフォルトの非セキュアモードに電話機を戻すには、電話およびすべての Cisco Unified Communications Manager サーバから CTL ファイルを削除する必要があります。
CTL ファイルの更新	CTL ファイルの作成後に CTL 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、Cisco Unified Communications Manager のセキュリティ モードが変更されなくなります。
CTL エントリ	
[トークンの追加（Add Tokens）]	証明書信頼リストにセキュリティ トークンを追加するには、このボタンをクリックします。 まだ削除されていない場合、サーバまたはワークステーションに当初挿入されたトークンを削除します。アプリケーションが次のトークンを要求したら、そのトークンを挿入して [OK] をクリックします。追加したセキュリティ トークンについての追加情報が表示されたら、[追加（Add）]をクリックします。すべてのセキュリティ トークンについて、これらのタスクを繰り返します。
[TFTP サーバの追加（Add TFTP Server）]	証明書信頼リストに代替 TFTP サーバを追加するには、このボタンをクリックします。設定については、[代替 TFTP サーバ（Alternate TFTP Server）] タブ設定が表示された後に [ヘルプ（Help）] ボタンをクリックします。設定を入力したら、[次へ（Next）] をクリックします。
[ファイアウォールの追加（Add Firewall）]	証明書信頼リストに ASA ファイアウォールを追加するには、このボタンをクリックします。設定の詳細については、[ファイアウォール（Firewall）] タブの設定画面の後に [ヘルプ（Help）] ボタンをクリックします。設定を入力したら、[次へ（Next）] をクリックします。
代替 TFTP サーバ	

設定	説明
[ホスト名（Hostname）]または [IP アドレス（IP Address）]	TFTP サーバのホスト名または IP アドレスを入力します。 代替 TFTP サーバは、別のクラスタに存在する Cisco TFTP サーバを指定します。代替 TFTP サーバの設定に 2 つのクラスタを使用する場合、両方のクラスタが同じクラスタ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、両方のクラスタで同じバージョンの Cisco Unified Communications Manager が実行されている必要があります。 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じであることを確認します。
[ポート（Port）]	このリリースの Cisco Unified Communications Manager では不要です。
ユーザ名とパスワード	このリリースの Cisco Unified Communications Manager では不要です。
ファイアウォール	
[ホスト名（Hostname）]または [IP アドレス（IP Address）]	ファイアウォールのホスト名または IP アドレスを入力します。
[ポート（Port）]	設定不可システムは Cisco Unified Communications Manager のポートを使用します。デフォルトのポート番号は 2444 です。
ユーザ名とパスワード	設定不可システムは Cisco Unified Communications Manager のインストール時に設定された管理者名とパスワードを使用します。
セキュリティ トークン	
[ユーザ パスワード（User password）]	Cisco CTL クライアントの初回設定時に Cisco123 と入力し（大文字と小文字が区別されるデフォルト パスワード）、証明書のプライベート キーを取得して CTL ファイルが署名されることを確認します。

関連トピック

Cisco CTL クライアントの設定のヒント, （6 ページ）
詳細情報の入手先

Cisco Unified Communications Manager のセキュリティ モードの確認

クラスタ セキュリティ モードを確認するには、次の手順を実行します。

（注） クラスタ セキュリティ モードでは、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の設定を行います。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、[システム（System）] > [エンタープライズ パラメータの設定（Enterprise Phone Configuration）] を選択します。

ステップ 2 [クラスタ セキュリティ モード（Cluster Security Mode）] フィールドを見つけます。フィールドの値が **1** と表示されている場合、混合モード用に Cisco Unified Communications Manager が正しく設定されています。（フィールド名をクリックすると追加情報を参照できます。）

ヒント Cisco Unified Communications Manager Administration でこの値を設定することはできません。Cisco CTL クライアントの設定後、この値が表示されます。

関連トピック

[自動（automatic）] または [実行中（started）] への Smart Card サービスの起動設定

インストールされている Cisco CTL クライアントが Smart Card サービスの無効を検出した場合、Cisco CTL クライアント プラグインをインストールするサーバまたはワークステーションで SmartCard サービスを [自動（automatic）] と [実行中（started）] に設定する必要があります。

ヒント サービスが実行中および自動に設定されていない限り、CTL ファイルにセキュリティ トークンを追加できません。

ヒント オペレーティング システムのアップグレード、サービス リリースの適用、Cisco Unified Communications Manager のアップグレードなどの後には、Smart Card サービスが実行中で自動になっていることを確認します。

サービスを実行中および自動に設定するには、次の手順を実行します。

手順

ステップ 1 Cisco CTL クライアントをインストールしてあるサーバまたはワークステーションで、[スタート（Start）]>[プログラム（Programs）]>[管理ツール（Administrative Tools）]>[サービス（Services）] または [スタート（Start）]>[コントロールパネル（Control Panel）]>[管理ツール（Administrative Tools）]>[サービス（Services）] を選択します。

ステップ 2 [サービス（Services）] ウィンドウで、[Smart Card] サービスを右クリックして、[プロパティ（Properties）] を選択します。

ステップ 3 [プロパティ（Properties）] ウィンドウで [一般（General）] タブが表示されることを確認します。

ステップ 4 [起動タイプ（Startup Type）] ドロップダウン リスト ボックスから [自動（Automatic）] を選択します。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 [サービスのステータス（Service Status）] エリアで [スタート（Start）] をクリックします。

ステップ 7 [OK] をクリックします。

ステップ 8 サーバまたはワークステーションをリブートし、サービスが実行されていることを確認します。

関連トピック

セキュリティ トークン パスワード（eToken）の変更

（注） CLI コマンド セット **utils ctl** でクラスタ セキュリティを管理する場合は、この手順は必要ありません。

この管理者パスワードは証明書の秘密キーを取得し、CTL ファイルが署名されたことを確認します。各セキュリティ トークンにはデフォルトのパスワードが設定されています。セキュリティ トークン パスワードはいつでも変更できます。Cisco CTL クライアントによりパスワードの変更を求めるプロンプトが表示されたら、設定を続行する前にパスワードを変更します。

パスワード設定の関連情報を確認するには、[ヒントを表示（Show Tips）] ボタンをクリックします。 何らかの理由でパスワードを設定できない場合は、表示されるヒントを確認してください。

Windows での eToken パスワード変更

重要 この情報は CTL クライアント暗号化オプションに適用されます。セキュリティ トークンが不要な **utils ctl**CLI コマンド セットを使用して暗号化を設定することもできます。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

Windows Vista、Windows 7、Windows 8.1、Windows 10 のサーバまたはワークステーションでセキュリティ トークンのパスワードを変更するには、次の手順を実行します。

手順

ステップ 1 Windows サーバまたはワークステーションに Cisco CTL クライアントがインストールされていることを確認します。

ステップ 2 インストールされていない場合は、Cisco CTL クライアントをインストールしてある別の Windows サーバまたはワークステーションの USB ポートにセキュリティ トークンを挿入します。

ステップ 3 インストールされていない場合は、Cisco CTL クライアントをインストールしてある別の Windows サーバまたはワークステーションの USB ポートにセキュリティ トークンを挿入します。

ステップ 4 [スタート（Start）] > [プログラム（Programs）] > [etoken] > [eTokenのプロパティ（Etoken Properties）] を選択し、[etoken] を右クリックして [eToken のパスワード変更（Change etoken password）] を選択します。

ステップ 5 [現在のパスワード（Current Password）] フィールドに、このトークン用に最初に作成したパスワードを入力します。

ステップ 6 新しいパスワードを入力します。

ステップ 7 確認のためもう一度新しいパスワードを入力します。

ステップ 8 [OK] をクリックします。

Cisco Unified IP Phone での CTL ファイルの削除

注意 Cisco Unified Communications Manager サーバから CTL ファイルを削除する計画がない場合は特に、このタスクをセキュアなラボ環境で実行することを推奨します。

次のケースで、Cisco Unified IP Phone の CTL ファイルを削除します。

- CTL ファイルに署名したセキュリティ トークンがすべて失われた。
- CTL ファイルに署名したセキュリティ トークンが漏洩したと見られる。

- セキュア環境から、ストレージ エリアなどに電話を移動する。
- 非セキュア クラスタまたはドメインの異なる別のセキュア クラスタに電話機を移動する。
- 未知のセキュリティ ポリシーを持つエリアから、セキュアな Cisco Unified Communications Manager に電話を移動する。
- 代替 TFTP サーバ アドレスを CTL ファイル内に存在しないサーバに変更する。

Cisco Unified IP Phone で CTL ファイルを削除するには、次のテーブル内のタスクを実行します。

表 *3* : *Cisco Unified IP Phone* での *CTL* ファイルの削除

Cisco Unified IP Phone モデル	タスク
Cisco Unified IP Phone 7960G および 7940G	電話の [セキュリティ設定（Security Configuration）] メニューで [CTL ファイル（CTL file）]、[ロック解除（unlock）]、または [**#]、さらに [削除（erase）] を押下します。
	次のいずれかのメソッドを実行します。 • 『*Administration Guide for Cisco Unified Communications Manager*』に説明されているように、[セキュリティ設定（Security Configuration）] メニューのロックを解除します。[CTL] オプションで、[削除（Erase）] ソフトキーを押下します。 • [設定（Settings）] メニューで、[削除（Erase）] ソフトキーを押下します。 （注） [設定（Settings）] メニューの [削除（Erase）] キーを押すと、CTL ファイル以外の他の情報も削除されます。詳細については、『*Administration Guide for Cisco Unified Communications Manager*.』を参照してください。

関連トピック

Cisco CTL クライアントのバージョンの確認

ご使用の Cisco CTL クライアントのバージョンを確認するには、次の手順を実行します。

手順

ステップ 1 次のいずれかの作業を実行します。

a) デスクトップの [Cisco CTL クライアント（Cisco CTL Client）] アイコンをダブルクリックします。

b) [スタート（Start）]>[プログラム（Programs）]>[Cisco CTL クライアント（Cisco CTL Client）] を選択します。

ステップ 2 [Cisco CTL クライアント（Cisco CTL Client）] ウィンドウの左上の隅にあるアイコンをクリックします。

ステップ 3 [Cisco CTL クライアントについて（About Cisco CTL Client）] を選択します。クライアントのバージョンが表示されます。

関連トピック

Cisco CTL クライアントの確認またはアンインストール

Cisco CTL クライアントのアンインストールでは、CTL ファイルが削除されません。同様に、クライアントをアンインストールしても、クラスタ セキュリティ モードと CTL ファイルは変更されません。必要に応じて、Cisco CTL クライアントをアンインストールし、クライアントを異なる Windows ワークステーションまたはサーバにインストールし、引き続き同じ CTL ファイルを使用できます。

Cisco CTL クライアントがインストールされていることを確認するは、次の手順を実行します。

手順

ステップ 1 [スタート（Start）]>[コントロール パネル（Control Panel）]>[プログラムの追加と削除（Add or Remove Programs）] の順に選択します。

ステップ 2 [Cisco CTL クライアント（Cisco CTL Client）] を見つけて、クライアントがインストールされていることを確認します。

ステップ 3 [削除（Remove）] をクリックして、クライアントをアンインストールします。

関連トピック