



Cisco CTL クライアントの設定

この章では、Cisco CTL クライアントの設定について説明します。

- [Cisco CTL の設定について \(1 ページ\)](#)
- [リカバリのために CTL ファイル内に 2 番目の SAST 権限を追加する \(3 ページ\)](#)
- [CLI を使用した SIP OAuth 設定 \(4 ページ\)](#)
- [Cisco CTL Provider サービスの有効化 \(5 ページ\)](#)
- [CAPF サービス有効化 \(6 ページ\)](#)
- [セキュア ポートの設定 \(6 ページ\)](#)
- [Cisco CTL クライアントの設定 \(8 ページ\)](#)
- [CTL ファイルの SAST 役割 \(10 ページ\)](#)
- [クラスター間での電話の移行 \(10 ページ\)](#)
- [eToken ベースの CTL ファイルから Tokenless CTL ファイルへの移行 \(12 ページ\)](#)
- [CTL ファイルの更新 \(12 ページ\)](#)
- [Cisco Unified Communications Manager セキュリティ モードの更新 \(13 ページ\)](#)
- [Cisco CTL ファイルの詳細 \(14 ページ\)](#)
- [Cisco Unified Communications Manager セキュリティ モードの確認 \(16 ページ\)](#)
- [\[automatic\] または \[started\] への Smart Card サービスの設定 \(16 ページ\)](#)
- [Cisco CTL クライアントの確認またはアンインストール \(17 ページ\)](#)

Cisco CTL 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、シスコの証明書信頼リスト(CTL)をインストールして設定すると作成されます。



- (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、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、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> にある『System Configuration Guide for Cisco Unified Communications Manager』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、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
- ITLRecovery

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 Serviceability] でこれらのサービスを再起動する必要があります。電話が次回初期化されたときに、その電話ではこの 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 クライアントが CTL ファイルにサーバ証明書を追加した後、次の CLI コマンドを実行して CTL ファイルを更新できます。

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。

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 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。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。



- (注)
- パブリッシャ ノードで CLI コマンドを実行する必要があります。
 - CallManager 証明書を再生成すると、ファイルの署名者に変更されることに注意してください。デフォルトのセキュリティをサポートしていない電話は、電話から 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。電話機の CTL ファイルの削除の詳細については、お使いの電話機モデルの『Cisco IP 電話 Administration Guide』を参照してください。

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

以前のリリースの 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 の署名者になんらかの更新が行われると、エンドポイントがロックアウトされました。SAST の署名者の更新が原因でエンドポイントまたはデバイスが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、エンドポイントではその更新した CallManager 証明書が信頼されなかった場合。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ため、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、エンドポイントのトークンレスアプローチが拡張され、リカバリのために CTL ファイル内に 2 番目の SAST が追加されました。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 を使用した SIP OAuth 設定

CLI を使用して、クラスタ SIP OAuth モードを設定することができます。



- (注) Cisco Unified Communications Manager での SIP OAuth モードの設定方法の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*、リリース 12.5(1)』を参照してください。

次の点を考慮してください。

- クラスタ SIP OAuth モードが有効になっている場合、Cisco ユニファイドコミュニケーションマネージャーは、セキュアデバイスから OAuth トークンを受信した SIP 登録を受け入れることができます。

有効にすると、Cisco ユニファイドコミュニケーションマネージャーのユーザインターフェイスを使用して設定可能な次の TLS ポートが開かれます。

- SIP OAuth ポート
- SIP OAuth MRA ポート

[Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[システム (System)] > [Cisco Unified CM] > Call Manager ページを選択します。

- パラメータ変更を反映するには、すべてのノードで Cisco CallManager サービスを再起動してください。

この暗号化方法では次の CLI コマンドを使用します。

管理者: ユーティリティ sipOAuth モード

クラスタ内の SIP OAuth モードのステータスを確認します。

ユーティリティ sipOAuth モードの有効化

クラスタ内の SIP OAuth モードを有効にします。

ユーティリティ sipOAuth モードの無効化

クラスタ内の SIP OAuth モードを無効にします。



(注) パブリッシャ ノードでのみ CLI コマンドを実行します。

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 Provider 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。このサービスは、CTL ファイルをすべての 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、Unified Communications Manager をアップグレードすると、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 Provider 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、**[Tools] > [Service Activation]** を選択します。
- ステップ 2 **[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 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 **[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 Provider 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接続のため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、**[Tools] > [Control Center - Feature Services]** を選択し、サービスの状態を確認します。

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。

セキュア 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 Unified Communications Manager ポートは、Unified Communications Manager のポート番号に 443 を加算 (+) した番号になるため、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、Unified Communications Manager で、SIP を実行中の電話からの 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 Serviceability] で Cisco CallManager サービスを再起動して、SIP を実行中の電話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 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 \(7 ページ\)](#) から [ステップ 6 \(7 ページ\)](#) を実行します。
 - b) [Ethernet Phone Port] または [SIP Phone Secure Port] の設定を変更するには、[ステップ 7 \(7 ページ\)](#) から [ステップ 11 \(7 ページ\)](#) を実行します。
- ステップ 2** Cisco CTL Provider ポートを変更するには、[Unified Communications Manager Administration] で、**[System] > [Service Parameters]** を選択します。
- ステップ 3** [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** [Service] ドロップダウン リスト ボックスで、[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、[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** [Save] をクリックします。
- ステップ 7** [Ethernet Phone Port] または [SIP Phone Secure Port] の設定を変更するには、[Unified Communications Manager Administration] で **[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 [Name] リンクをクリックします。
- ステップ 9** Unified Communications Manager の [Configuration] ウィンドウが表示されたら、[Ethernet Phone Port] フィールドまたは [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** 電話をリセットし、[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。

Cisco CTL クライアントの設定



重要 **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ができます。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、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、およびスマートアカウントまたはバーチャル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の許可が有効になっており、そのトークンがこのクラスタに登録され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 CTLFile を更新するには、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、およびスマートアカウントまたはバーチャル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の許可が有効になっており、そのトークンがこのクラスタに登録され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 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. UCM クラスタを登録するときに、スマート/仮想アカウントから受信した製品トークンで[エクスポート制御機能を許可する]チェックボックスがオンになっていることを確認してください。

Cisco CTL CLI 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 Unified Communications Manager セキュリティモードを設定します。



- (注) Unified Communications Manager Administration の [Enterprise Parameters Configuration] ウィンドウで、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、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 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。



(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 CTL ファイルの更新は予定されたメン
ができます。これは、クラスタ内で T
CallManager を実行するすべてのサーバ
動する必要があるためです。

Cisco CTL の設定が完了すると、CTL は次のタスクを実行します。

- CTL ファイルを 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 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 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。

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 ユニファイド コミュニケーション マネージャ 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。

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 ファイルに含まれるようになります。
 - 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、ユニファイド コミュニケーション マネージャ リリース 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。

次の状況が発生したら CTL ファイルを更新する必要があります。

- 新しい 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 Unified Communications Manager*』を参照してください。

- 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
- 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

- Unified Communications Manager サーバまたは Unified Communications Manager データを復元する
- CTL ファイルを含む Cisco ユニファイドコミュニケーションマネージャークラスタのすべてのノード上で、CallManager、CAPF、またはITL回復証明書を手動で再生成した場合は、[CTL] ウィザードを再実行する必要があります。この手順は、他の証明書の生成には必要ありません。
- Unified Communications Manaver を 7.1.5 以前のバージョンから 7.1.5 以降のバージョンに更新する
- バージョン 10.5 より前の Unified Communications Manager を 10.5 以降のバージョンに更新する場合は、移行に関する「ハードウェア eToken からトークンレスの解決策へ」のセクションを参照してください。
- 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 Unified Communications Manager クラスタでドメイン名が追加または変更された場合、その電話設定ファイルを有効にするには CTL ファイルを更新する必要があります。



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。



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 でセキュアなコール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、**[Telephony Integrations] > [Port Group]** に移動し、リセットするポート グループを選択して、**[Port Group Basics]** ページで **[Reset]** をクリックします。

Cisco Unified Communications Manager 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を使用する必要があります。Unified Communications Manager のセキュリティモードは、[Unified Communications Manager Administration] の [Enterprise Parameters Configuration] 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。

手順

ステップ 1 `utils ctl set-cluster mixed-mode` CLI コマンドを実行して、クラスタ セキュリティ モードをセキュアに変更します。

ステップ 2 `utils ctl set-cluster non-secure-mode` CLI コマンドを実行して、クラスタ セキュリティ モードを非セキュアに変更します。

Cisco CTL ファイルの詳細



(注) 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の設定を行います。

表 2: CTL の設定

| 設定 | 説明 |
|--|----|
| Unified Communications Managerサーバ | |
| Security Mode | |

| 設定 | 説明 |
|--|---|
| Unified Communications Manager クラスタの混合モードへの設定 | 混合モードでは、認証済み、暗号化済み、および非セキュアな Cisco IP Phone を Unified Communications Manager に登録できます。このモードでは、認証済みまたは暗号化済みのデバイスについて、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。 |
| Unified Communications Manager クラスタの非セキュアモードへの設定 | <p>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、Unified Communications Manager によってイメージ認証のみがサポートされます。</p> <p>このモードを選択すると、CTL ファイル内にリストされているすべてのエントリの証明書が Cisco CTL クライアントによって削除されますが、CTL ファイルそのものは指定のディレクトリに引き続き存在します。未署名の設定ファイルが電話によって要求され、Unified Communications Manager に非セキュアとして登録されます。</p> <p>ヒント デフォルトの非セキュアモードに電話を戻すには、電話およびすべての 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。</p> |
| [CTL Entries] | |
| トークン | サーバまたはワークステーションに当初挿入したトークンをまだ削除していない場合は削除します。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情報が表示されたら、[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、これらの操作を繰り返します。 |
| [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。設定の詳細については、[Alternate TFTP Server] タブの設定が表示された後に [Help] ボタンをクリックします。設定を入力したら、[Next] をクリックします。 |

| 設定 | 説明 |
|----------------|--|
| [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、[Firewall] タブの設定が表示された後に [Help] ボタンをクリックします。設定を入力したら、[Next] をクリックします。 |

Cisco Unified Communications Manager 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** 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** [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 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 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。

[automatic] または [started] への Smart Card サービスの設定

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 [automatic] と [started] に設定する必要があります。



ヒント サービスが [started] および [automatic] 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 [started] および [automatic] 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、[Start] > [Programs] > [Administrative Tools] > [Services] または [Start] > [Control Panel] > [Administrative Tools] > [Services] を選択します。
- ステップ 2** [Services] ウィンドウで、[Smart Card] サービスを右クリックして、[Properties] を選択します。
- ステップ 3** [Properties] ウィンドウで [General] タブが表示されることを確認します。
- ステップ 4** [Startup Type] ドロップダウン リスト ボックスから [Automatic] を選択します。
- ステップ 5** [Apply] をクリックします。
- ステップ 6** [Service Status] エリアで [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。

Cisco CTL クライアントの確認またはアンインストール

Cisco CTL クライアントをアンインストールしても、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。アンインストールする場合は、CLI オプションを使用して Cisco CTL をアンインストールすることができます。

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には、次の手順を実行します。

手順

- ステップ 1** [Start] > [Control Panel] > [Add or Remove Programs] の順に選択します。
- ステップ 2** [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 [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。
