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

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）
- 同じサーバで実行されている CiscoCallManager および CiscoTFTP 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。

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。
- ITLRecovery 証明書を再生成すると、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。

リカバリのための CTL ファイルへの2番目の SAST ロールの追加

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 ファイルに署名するために使用された1つの SAST レコードだけが含まれていました。1つの SAST のみが使用されているため、SAST 署名者の更新によってエンドポイントのロックアウトが発生しました。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。

- エンドポイントは、登録時に CallManager 証明書を使用して署名された CTL ファイルを受け入れました。
- 管理者が CallManager 証明書を再生成し、CTL ファイルを更新しました。これは、更新された CTL ファイルが既存の CallManager 証明書ではなく、更新された CallManager 証明書によって署名されたことを暗示しています。
- 更新された証明書がエンドポイントの信頼リストで使用できなかったため、エンドポイントは更新された CallManager 証明書を信頼しませんでした。そのため、エンドポイントは、CTL ファイルをダウンロードする代わりに拒否しました。
- エンドポイントは、Transport Layer Security (TLS) を介して ccm サービスに安全に接続しようとしました。 ccmservice は更新された CallManager 証明書を TLS 交換の一部としてエンドポイントに提供しました。更新された証明書は、エンドポイントの信頼リストでは使用できなかったため、エンドポイントはその 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2つの SAST トークン (CallManager レコードと ITLRecovery レコード) が含まれています。

ITLRecovery 証明書は、次の理由により他の証明書よりも選択されます。

- ホスト名の変更などの二次的な理由によって変更されることはありません。
- すでに ITL ファイルで使用されています。

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 *14*』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 Unified Communications Manager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 コマンドを実行すします。

Cisco CTL Provider サービスの有効化

Cisco CTL クライアントを設定すると、Cisco CTL Provider サービスによってセキュリティモードが非セキュアモードから混合モードに変更され、サーバ証明書が CTL ファイルに転送されます。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 CiscoCTL 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

Step 1　Cisco Unified Serviceability で、**[Tools]** > **[Service Activation]** を選択します。

Step 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。

Step 3　**CiscoCTL Provider** サービスのオプションボタンをクリックします。

Step 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）　CiscoCTL Provider サービスをアクティブにする前に、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場合は、TLS 接続用のポートの設定に関連するトピックを参照してください。

Step 5　サービスがサーバ上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。

関連トピック

セキュア ポートの設定, on page 6
CTL クライアントの設定に関する詳細情報の入手先

Cisco CAPF サービスのアクティベーション

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 サービスをアクティブにすると、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 サービスの有効化

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。

- TLS 接続の Cisco CTL プロバイダーのデフォルトポートは2444に相当します。Cisco CTL プロバイダーポートは、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、Cisco CTL クライアント要求を処理します。

（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は、SCCP を実行している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を介して接続します。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。このポートを変更する場合は、 Cisco Unified Serviceability の CiscoCallManager サービスを再起動し、SIP を実行している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 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 クライアントが実行されているデータ VLAN に対して CTL ポートを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

Step 1　変更するポートに応じて、次のタスクを実行します。

a) Cisco CTL Provider サービスのポート番号パラメータを変更するには、Step 2 （7 ページ） ~ Step 6 （7 ページ）を実行します。

b) イーサネット電話ポートまたは SIP 電話のセキュアポートの設定をStep 7 （7 ページ）変更 Step 11 （7 ページ）するには、~ を実行します。

Step 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。

Step 3　[サーバ（Server）] ドロップダウンリストで、CiscoCTL Provider サービスが実行されているサーバを選択します。

Step 4　[サービス (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。

Step 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。

（注）　12.X 以降では、[パラメータ値（Parameter Value）] フィールドの [ポート番号（Port Number）] パラメータの値を変更できません。

Step 6　**[保存（Save）]** をクリックします。

Step 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、[Unified Communications Manager Administration] で **[システム（System）] > [CiscoUnifiedCM]** を選択します。

Step 8　『*Administration Guide for Cisco Unified Communications Manager*』の説明に従い、CiscoCallManager 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。

Step 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。

Step 10　電話機をリセットし、Cisco Unified Serviceability の CiscoCallManager サービスを再起動します。

Step 11　[保存（Save）] をクリックします。

関連トピック

CTL クライアントの設定に関する詳細情報の入手先

Cisco CTL クライアントのセットアップ

重要 < x xid = "i 7000.1.1" id = "x253"/> **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） また、Cisco CTL クライアントは、最大16の呼処理サーバ、1台のパブリッシャ、2つの TFTP サーバ、最大9個のメディアリソースサーバをサポートします。

  ヒント TFTP サービスを再起動し、クラスタ内でこれらの
  いるすべてのサーバで CallManager する必要がある
  されたメンテナンス期間中に CTL ファイルを更新

  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。
  - 設定されているすべての TFTP サーバにファイルを書き込みます。
  - 設定されているすべての ASA ファイアウォールにファイルを書き込みます。
  - Ctl ファイルを作成したときに、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。

関連トピック

Cisco CTL ファイルの詳細, on page 14
デバイス、サーバ、クラスタ、およびサービスのリセット
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
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	ITLRecovery（署名者） CallManager
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

Step 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。

Step 2 [検索（Find）] をクリックします。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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。

Step 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**ユーティリティ ctl**を使用してクラスタセキュリティを管理する場合、この手順は必要ありません。

次のシナリオが発生した場合は、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
- 設定されている任意の TFTP サーバの IP アドレスまたはホスト名を変更する場合
- 設定されている 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場合
- シスコユニファイドサービスで Cisco Certificate Authority Function サービスを有効にした場合
- 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場合
- TFTP サーバを追加または削除する必要がある場合
- 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
- 10.5 より前のユニファイドコミュニケーションマネージャバージョンからバージョン10.5 以降に更新する場合は、「ハードウェア eTokens からトークンレスソリューションへの移行」の項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 シスコでは、最小限のコール処理の中断が発生した場合に、ファイルを更新することを強く推奨しています。

注意 ユニファイドコミュニケーションマネージャが、セキュアな SIP または SCCP を使用して Unity Connection 10.5 以降と統合されている場合、セキュアコールは Unity Connection での動作を停止する可能性があります。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 インターフェイスを使用してポートグループをリセットするには、[Telephony] [**統合** > **ポートグループ**] に移動し、リセットするポートグループを選択して、[**ポートグループの基本**] ページで [**リセット**] 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
Cisco CTL クライアントの設定, on page 1
詳細情報の入手先

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

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

Step 1 CLI コマンドの`monitorctl set クラスタ混合モード`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。

Step 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。

関連トピック

CTL ファイルの更新, on page 12

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。混合モードのみが、認証、暗号化されたシグナリング、および暗号化されたメディアをサポートしています。

（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* の構成時の設定

設定	説明
Unified Communications Managerサーバ	
セキュリティ モード（**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 電話 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	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。 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。 **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。
CTL エントリ	
置換可能なトークン	サーバまたはワークステーションに最初に挿入したトークンを削除していない場合は、削除します。アプリケーションからプロンプトが表示されたら、次のトークンを挿入し、[**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、これらのタスクを繰り返します。
[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、代替 TFTP サーバのタブ設定を表示した後に [**ヘルプ (Help)**] ボタンをクリックしてください。設定を入力したら、[**次へ (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。

関連トピック

Cisco CTL クライアントの設定のヒント
詳細情報の入手先

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

Step 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。

Step 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。この値は、Cisco CTL クライアントを設定した後に表示されます。

関連トピック

CTL クライアントの設定に関する詳細情報の入手先

開始または自動のスマートカードサービスのセットアップ

Cisco CTL クライアントのインストールでスマートカードサービスが無効になっていることが検出された場合は、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スマートカードサービスを自動に設定し、起動する必要があります。

ヒント　サービスが [開始 (on)] および [自動 (automatic)] に設定されていない場合、CTL ファイルにセキュリティトークンを追加することはできません。

ヒント　オペレーティングシステムをアップグレードし、サービスリリースを適用し、 Cisco Unified Communications Managerをアップグレードした後、スマートカードサービスが開始され、自動であることを確認します。

サービスを開始および自動に設定するには、次の手順を実行します。

手順

Step 1　Cisco CTL クライアントをインストールしたサーバまたはワークステーションで、[スタート] [プログラム] [＞ ＞ **管理ツール** ＞] [サービス]、または [**スタート** ＞ **] [コントロールパネル]** ＞ **[管理ツール]** ＞ **[サービス]** を選択します。

Step 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。

Step 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。

Step 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。

Step 5　**[適用（Apply）]** をクリックします。

Step 6　[Service Status] エリアで [Start] をクリックします。

Step 7　[OK] をクリックします。

Step 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

CTL クライアントの設定に関する詳細情報の入手先

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 ファイルは削除されません。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。これを選択した場合は、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

Step 1 **[Start]** > **[Control Panel]** > **[Add or Remove Programs]** の順に選択します。

Step 2 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、 **CISCO CTL クライアント**を見つけます。

Step 3 クライアントをアンインストールするには、[**Remove**] をクリックします。

関連トピック

CTL クライアントの設定に関する詳細情報の入手先