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関する情報を提供します。

- Cisco CTL セットアップについて （1 ページ）
- 復旧用 CTL ファイルに 2 番目の Sast ロールを追加 （3 ページ）
- CLI による SIP Oauth の構成 （4 ページ）
- Cisco CTL Provider Service をアクティベートする （5 ページ）
- Cisco CAPF サービスのアクティベーション （6 ページ）
- セキュアポートのセットアップ （6 ページ）
- Cisco CTL クライアントのセットアップ （8 ページ）
- SASTのCTLファイルの役割 （10 ページ）
- あるクラスターから別のクラスターに電話を移行する （10 ページ）
- eToken ベースの CTL ファイルからトークンレス 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 （15 ページ）
- Smart Card サービスを開始または自動に設定する （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 セットアップについて

デバイス、ファイル、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、Cisco 証明書信頼リスト（CTL）をインストールして設定するときに作成されます。

（注）

- 混合モードを有効にする、または CTL ファイルを更新するには、Unified Communications Manager で、[輸出規制による機能限定の許可（Allow export-controlled functionality）] が有効になっているスマートアカウントまたは仮想アカウントから受け取った登録トークンを使用して、スマートライセンス登録が完了していることを確認します。 Cisco Smart Software Licensing の設定方法については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*Cisco Unified Communications Manager* システム設定ガイド』の「「スマート ソフトウェア ライセンシング」」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ときに Unified Communications Manager が輸出規制による機能限定を有効にしていない場合、*ClusterModeSecurityFailedExportControlNotAllow* という名前の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。

- システム管理者セキュリティトークン（SAST）
- 同一のサーバ上で実行されている CiscoCallManager および CiscoTFTP サービス
- 認証局プロキシ 機能（CAPF）
- TFTP サーバー
- ASA ファイアウォール
- ITL リカバリ

Call Manager 証明書が自己署名の場合、CTL ファイルには各サーバのサーバ証明書、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 アドレスが含まれます。

Multi-SAN Call Manager 証明書の場合、CTL ファイルにはパブリッシャーの Call Manager 証明書が含まれています。

次に電話が初期化されるときに、TFTP サーバから CTL ファイルが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。 TFTP サーバに証明書が含まれていない場合、電話機は署名されていないファイルを要求します。

Cisco CTL クライアントがサーバ証明書を CTL ファイルに追加したら、以下の 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 混合モード
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 ノンセキュア モード
CTL ファイルを更新し、クラスタをノンセキュア モードに設定します。

utils ctl update CTLFile
クラスターの各ノードで 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ことで、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セキュアにすることができます。 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。 Security by Default をサポートしない電話機は、電話機から CTL ファイルを手動で削除しない限り、新しい CTL ファイルを受け入れません。 電話からの CTL ファイルの削除については、お使いの電話モデルの *Cisco IP Phone* 管理ガイド を参照してください。

復旧用 CTL ファイルに 2 番目の Sast ロールを追加

Unified Communications Manager の以前のリリースでは、エンドポイントが 1 つの Cisco サイト管理者セキュリティトークン（SAST）のみを信頼するトークンレスのアプローチがありました。 この SAST（セキュリティ認証サービストークン）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）ファイルには、CTL ファイルの署名に使用される 1 つの SAST（セキュリティ認証サービストークン）レコードのみが含まれていました。 1 つの SAST（セキュリティ認証サービストークン）のみが使用されたため、SAST（セキュリティ認証サービストークン）署名者を更新すると、エンドポイントがロックアウトされました。 以下のポイントは、SAST（セキュリティ認証サービストークン）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たシナリオを示しています。

- 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。 この再生成は、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ていることを意味していました。
- 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。エンドポイントの信頼リストに更新された証明書がなかったからです。そのため、エンドポイントは CTL ファイルをダウンロードせずに拒否しました。
- エンドポイントが、Transport Layer Security (TLS) 経由で安全に ccm サービスに接続しようとしました。ccmservice は、TLS 交換の一部としてエンドポイントに更新された CallManager 証明書を提供しました。 更新された証明書がエンドポイントの信頼リストになかったため、エンドポイントが CTL ファイルをダウンロードせずに拒否しました。
- エンドポイントは ccmservice と通信せず、結果としてロックアウトされます。

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は、リカバリ用の CTL ファイルに 2 番目の Sast を追加することで強化され

ています。この機能では、トークンレスCTLファイルには、CallManagerレコードとITLRecoveryレコードの 2 つの Sast トークンが含まれます。

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

- ホスト名の変更など、二次的な理由により変更されません。
- ITL ファイルですでに使用されています。

CLI による SIP Oauth の構成

CLI を通じて、クラスター SIP Oauth モードを設定できます。

（注） Cisco Unified Communications Manager で SIP OAuth モードを設定する方法の詳細は、『*Cisco Unified Communications Manager* 機能設定ガイド、リリース *12.5(1)*』を参照してください。

以下の点を考慮してください。

- クラスターSIP OAuthモードが有効な場合、Cisco Unified Communications Managerはセキュアなデバイスからの OAuth トークンによる SIP 登録を受け付けます。

  有効にすると、次の TLS ポートが開きます。これらはCisco Unified Communications Managerユーザインターフェイスから設定できます。

  - **SIP Oauth ポート**
  - **SIP Oauth MRA ポート**

  Cisco Unified CM Administration でポートを設定できます。**[システム（System）]** > **[Cisco Unified CM]** > **[CallManager]** ページを選択します。

- パラメータの変更を有効にするために、すべてのノードでCisco CallManagerサービスを再起動します。

暗号化オプションは以下の CLI コマンドで構成されています。

admin:utils sipOAuth-mode
クラスターの SIP OAuth モードの状況を確認します。
utils sipOAuth-mode enable
クラスターで SIP Oauth モードを有効にします。
utils sipOAuth-mode disable
クラスターで 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 Service をアクティベートする

Cisco CTL クライアントを設定すると、Cisco CTL プロバイダサービスによりセキュリティモードがノンセキュアから混合モードに変更され、サーバー証明書が CTL ファイルに転送されます。 その後、サービスは CTL ファイルをすべての Unified Communications Manager および CiscoTFTP サーバーに転送します。

このサービスを有効にしてから 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有効化します。

ヒント クラスタ内のすべてのサーバーで CiscoCTL プロバイダサービスを有効にする必要があります。

サービスを有効にするには、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）] > [サービスのアクティブ化（Service Activation）]** の順に選択します。

ステップ 2 [サーバ] ドロップダウン リスト ボックスで、Cisco CallManager または Cisco TFTP サービスを有効にしたサーバを選択します。

ステップ 3 [**CiscoCTL プロバイダ**] サービスのラジオ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）
CiscoCTL Provider サービスを有効にする前に、CTL ポートを入力することができます。 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するトピックを参照してください。

ステップ 5 サーバー上でサービスが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。

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 認証局プロキシ機能サービスをアクティブ化することで、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。

セキュアポートのセットアップ

デフォルトのポートが現在使用されている場合、またはファイアウォールを使用しており、ファイアウォール内のポートを使用できない場合は、別の TLS ポート番号を設定する必要があります。

- TLS 接続のための Cisco CTL プロバイダのデフォルトポートは 2444 です。Cisco CTL Provider ポートは Cisco CTL クライアントからのリクエストを監視します。 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は、SCCP を実行している電話からの登録要求を監視します。 非セキュアモードでは、電話はポート 2000 を通して接続します。混合モードでは、TLS 接続用の Unified Communications Manager ポートは、Unified Communications Manager ポート番号に443を加えた値となります。このため、Unified Communications Manager のデフォルトの TLS 接続は 2443 となります。ポート番号が使用中であるか、ファイアウォールを使用していてその中でポートを使用できない場合にのみ、この設定を更新します。
- SIP セキュアポートにより、 Unified Communications Manager は、SIP を実行している電話からの SIP メッセージをリッスンすることができます。 デフォルト値は 5061 です。このポートを変更する場合、Cisco Unified Serviceability で Cisco CallManager 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 ポートを更新したら、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、以下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、以下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、ステップ 2 （7 ページ） から ステップ 6 （7 ページ） までの手順を実行します。

b) イーサネット電話ポートまたは SIP 電話セキュアポート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 プロバイダポートを変更するには、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] ドロップダウンリストで、CiscoCTL プロバイダー サービスが実行されるサーバを選択します。

ステップ 4　[サービス] ドロップダウンリストボックスから、 Cisco CTL Provider サービスを選択します。

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　ポート番号パラメータの値を変更するには、[パラメータ値]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、[パラメータ値] フィールドで [ポート番号] パラメータの値を変更することはできません。

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または SIP 電話セキュアポート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。

ステップ 8　『 *Cisco Unified Communications Manager* 管理ガイド』の説明に従って、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、サーバの **名前** リンクをクリックします。

ステップ 9　Unified Communications Manager 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] または [SIP 電話セキュアポート] 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 CiscoCallManager 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 クライアントのセットアップ

重要 **utils ctl** CLI コマンドセットを使用して、暗号化をセットアップできます。 CLI の使用の詳細については、『*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、クラスタを混合モードに設定します。 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 [輸出規制による機能限定の許可（Allow export-controlled functionality）] 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、CTLFile を更新します。 CTLFIle を混合モードで更新するには、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 [輸出規制による機能限定の許可（Allow export-controlled functionality）] 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。
- Unified Communications Manager が、[輸出規制による機能限定の許可（Allow export-controlled functionality）] が有効になっている登録トークンで登録されておらず、さらに **utils ctl set-cluster mixed-mode** および **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。

  `Unified Communications Manager クラスタが ［輸出規制による機能限定の許可（Allow export-controlled functionality）］ でスマート/仮想アカウントに登録されていないため、コマンドを実行できません。 UCM クラスターの登録時に、スマート/仮想アカウントから受け取った製品トークンで ［輸出規制による機能限定の許可（Allow export-controlled functionality）］ にチェックが入っていることを確認します。`

Cisco CTL CLI は以下のタスクを実行します。

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

Cisco CTL クライアントのセットアップ

（注） Unified Communications Manager クラスタ セキュリティ パラメータを、Unified Communications Manager Administration の [エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ウィンドウから混合モードに設定することはできません。 クラスタセキュリティモードは、Cisco CTL クライアントまたは CLI コマンド set **utils ctl** で設定できます。

- 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、CAPF サーバーの証明書エントリを含むファイルです。

  CTL ファイルは、電話接続の TLS をサポートするサーバを示します。 クライアントは、Unified Communications Manager、Cisco CAPF、および ASA ファイアウォールを自動的に検出し、これらのサーバー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：最大 16 台のコール処理サーバー、1 台のパブリッシャ、2 台の TFTP サーバー、そして最大 9 台のメディアリソースサーバーをサポートします。

ヒント TFTP サービスを再起動してから、クラスタ内でこれらのサービスを実行するすべてのサーバー上で CallManager を再起動する必要があるため、スケジュールされたメンテナンス期間中に CTL ファイルを更新できます。

Cisco CTL の設定が完了した後、CTL は以下のタスクを実行します。

- CTL ファイルを Unified Communications Manager サーバー（複数可）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(最初のノードではない)に書き込みます。
- クラスタ内のすべての Unified Communications Manager の後続ノード (最初のノードではない) に PEM 形式の CAPF 証明書ファイルを書き込みます。
- すべての設定済み TFTP サーバにファイルを書き込みます。
- 設定済みのすべての ASA ファイアウォールにファイルを書き込みます。
- CTL ファイルの作成時に USB ポート内に存在していたセキュリティトークンの秘密鍵を使って、CTL ファイルに署名します。

SASTのCTLファイルの役割

（注） *次の表に記載されている署名者は、CTL ファイルへの署名に使用されます。

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

Cisco Unified Communications Manager のバージョン	トークンベースのCTLファイルのシステム管理者セキュリティトークン（SAST）の役割	トークンレスのCTLファイルのシステム管理者セキュリティトークン（SAST）の役割
12.0(1)	トークン 1 (署名者*) トークン 2 ITL リカバリ CallManager	ITLRecovery (署名者) CallManager
11.5(x)	トークン 1 (署名者) トークン 2 ITL リカバリ CallManager	CallManager (署名者) ITL リカバリ
10.5(2)	トークン 1 (署名者) トークン 2	CallManager (署名者) ITL リカバリ
10.5(1) (サポートされていません)	トークン 1 (署名者) トークン 2	CallManager (署名者)
10.0(1) (サポートされていません)	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	なし

あるクラスターから別のクラスターに電話を移行する

次の手順を使用して、電話を1つのクラスタから別のクラスタに移行します。たとえば、クラスター 1 からクラスター 2 に。

手順

ステップ 1 Cisco Unified OS Administration のクラスタ 2 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 証明書のリストから、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して、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 証明書のリストから、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して、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 Cisco Unified OS Administration のクラスタ 1 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**をクリックして、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、[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）]** フィールドについて、**[ファイルを選択（Choose File）]** をクリックし、ステップ 3 でダウンロードした ITLRecovery ファイルを参照し、**[ファイルをアップロード（Upload File）]** をクリックします。
アップロードされた ITLRecovery ファイルは、クラスタ 1 の **[証明書一覧（Certificate List）]** ウィンドウに **Phone-SAST-Trust** 証明書として表示されます。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 1 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 証明書はクラスタ 2 の CAPF 信頼ストアにアップロードされる必要があります。

ステップ 10 （任意） この手順は、クラスターが混合モードの場合にのみ適用できます。 CLI で **utils ctl update CTLFile** コマンドを実行し、クラスター 1 で CTL ファイルを再生成します。

（注）
- `show ctl` CLI コマンドを実行して、クラスタ 2 の ITLRecovery 証明書と CallManager 証明書が、SASTの役割を持つ CTL ファイルに含まれていることを確認します。
- 電話が新しい CTL および ITL ファイルを受信したことを確認します。 更新された CTL ファイルには、クラスター 2 の ITLRecovery 証明書があります。

クラスタ 1 からクラスタ 2 に移行する電話は、クラスタ 2 の ITLRecovery 証明書を受け入れるようになります。

ステップ 11　1 つのクラスタから別のクラスタに電話を移行します。

eToken ベースの CTL ファイルからトークンレス CTL ファイルへの移行

トークンレス CTL ファイルの場合、管理者は、Unified Communications Manager リリース 12.0(1) 以降で、USB トークンを使用して生成され、アップロードされた CTL ファイルをエンドポイントがダウンロードするようにする必要があります。 ダウンロード後、トークンレス CTL ファイルに切り替えることができます。 その後、 `util ctl update` CLI コマンドを実行できます。

CTL ファイルの更新

（注）　CLI コマンドの set **utils ctl でクラスターの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、CTL ファイルを更新する必要があります。 以下を行った場合：

- 新しい Unified Communications Manager サーバーをクラスタに追加した場合

（注）　セキュアなクラスタにノードを追加するには、「*Unified Communications Manager* をインストールする」を参照してください。新しいノードの追加方法と新しいノードのセキュリティ設定方法について説明しています。

- Unified Communications Manager サーバーの名前または IP アドレスを変更した場合
- 設定済みの TFTP サーバーの IP アドレスまたはホスト名を変更した場合
- 設定済みの 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した場合
- Cisco 認証局機能サービスを Cisco Unified Serviceability で有効にした場合
- セキュリティトークンを追加または削除した場合
- TFTP サーバーを追加または削除した場合
- Unified Communications Manager サーバーを追加または削除した場合
- ASA ファイアウォールを追加または削除した場合

- CTL ファイルを含む Cisco Unified Communications Manager クラスタ上の任意のノードで、CallManager、CAPF、または ITL 回復証明書を手動で再生成する場合は、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。
- 7.1.5 以前の Unified Communications Manager バージョンを 7.1.5 またはそれ以降のバージョンに更新した場合。
- 10.5 より前の Unified Communications Manager バージョンを 10.5 以降に更新した場合は、「ハードウェア eToken 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場合。

（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、電話構成ファイルを有効にするために CTL ファイルを更新する必要があります。

ヒント 最小限のコール処理の中断が発生するときにファイルを更新することを強くお勧めします。

注意 Unified Communications Manager が安全な 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、セキュアコールが Unity Connection で機能しなくなる場合があります。 この問題を解決するには、Unity Connection の対応するポート グループをリセットする必要があります。

Unity Connection Administration インターフェイスからポートグループをリセットするには、リセットするポートグループを選択し、**[ポートグループの基本（Port Group Basics）]** ページで **[リセット（Reset）]** をクリックした後、**[テレフォニー統合（Telephony Integrations）]** > **[ポートグループ（Port Group）]** に移動します。

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 Administration の [エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ウィンドウから Unified Communications Manager セキュリティモードを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 CLI コマンド `utils ctl set-cluster mixed-mode` 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 CLI コマンド `utils ctl set-cluster non-secure-mode` 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） **utils ctl** CLI コマンドセットを使用して暗号化をセットアップできます。これにはセキュリティトークンは必要ありません。 CLI の使用の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

クラスタ セキュリティ モードは、次の表に示すように、非セキュア モードまたは混合モードに設定できます。 混在モードのみが、認証、暗号化シグナリング、暗号化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。

表 *2: CTL* の設定項目

設定	説明
Unified Communications Manager サーバ	
Security Mode	
Unified Communications Manager クラスタを混合モードに設定する	混合モードでは、認証済み、暗号化済み、ノンセキュア Cisc 録が許可されます。 このモードでは、 Unified Communication セキュアなポートを使用することを保証します。

設定	説明
Unified Communications Manager クラスタを非セキュアモードに設定する	非セキュアモードに設定すると、すべてのデバイスが未認は画像認証のみに対応します。 このモードを選択すると、Cisco CTL クライアントは、CT証明書を削除しますが、CTLファイルは指定したディレク定ファイルをリクエストし、Unified Communications Mana ヒント 電話をデフォルトのノンセキュアモードに戻すには、電話から CTL ファイルを削除する必要があります。
CTL エントリ	
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ケーションから次のトークンを挿入するように指示されます。 追加トークンのセキュリティトークン情報が表示されリティ トークンについて、これらのタスクを繰り返しま
TFTP サーバの追加	証明書信頼リストに代替 TFTP サーバを追加するには、こは、[代替 TFTP サーバー（Alternate TFTP Server）] タブのクリックします。 設定を入力したら、[**次へ**] をクリック
ファイアウォールの追加	このボタンをクリックして、証明書信頼リストに ASA フは、[ファイアウォール（Firewall）] タブの設定が表示されさい。 設定を入力したら、[**次へ**] 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、以下の手順を実行します。

（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。

手順

ステップ 1 Unified Communications Manager の管理で、 **[システム]** > **[エンタープライズパラメータの設定]** を選択します。

ステップ 2 **クラスターセキュリティモード** フィールドを見つけます。 フィールドの値が **1** と表示される場合、 Unified Communications Manager が混在モードで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詳細が表示されます。)

ヒント
この値は Unified Communications Manager Administration では設定できません。 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。

Smart Card サービスを開始または自動に設定する

Cisco CTL クライアントのインストールにより、Smart Card サービスが無効になっていることが検出された場合、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ーまたはワークステーションで、Smart Card サービスを自動および開始に設定する必要があります。

ヒント サービスが開始済みおよび自動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処理を行った後は、Smart Card サービスが自動的に開始され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、以下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たサーバー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）]** を選択します。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] ウィンドウから [**Smart Card**] サービスを右クリックし、[プロパティ] を選択します。

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

ステップ 4 [スタートアップの種類（Startup type）] ドロップダウンリストから、**[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 [サービス状況（Service Status）] エリアで、**[開始（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再起動し、サービスが実行中であ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。 そうしたい場合は、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、以下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 Remove Programs）]** を選択します。

ステップ 2 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、 **Cisco CTL Client** を探します。

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。