概要

システム要件

Unified Communications Manager を認証または暗号化するためのシステム要件を次に示します。

- Unified Communications Manager パブリッシャの Cisco Unified Communications Manager Administration CLI にログインし、**util ctl** コマンドを実行してクラスタを混合モード（セキュアモード）に設定します。
- Unified Communications Manager で TLS 接続を認証するために、すべての電話機にローカルで有効な証明書（LSC）が存在します。

（注） LSC が存在しない場合は、一部のエンドポイントでも MIC が使用されますが、LSC を使用することを常に推奨します。

ベストプラクティス

シスコでは、次のベスト プラクティスを強く推奨します。

- 大規模なネットワークに導入する前に、安全なラボ環境でインストールと設定のタスクを常に実行してください。
- リモートロケーションにあるゲートウェイおよびその他のアプリケーションサーバに IPSec を使用します。

警告 これらのインスタンスで IPSec を使用しないと、セッション暗号キーが暗号化されずに転送されます。

- 電話料金の詐欺行為の防止するため、『Cisco Unified Communications Manager システム設定ガイド』で説明されている電話会議の機能拡張を設定します。同様に、コールの外部転送を制限する設定作業を実行することもできます。この作業の実行方法については、『Cisco Unified Communications Manager 機能設定ガイド』を参照してください。

デバイスのリセット、サーバとクラスタのリブート、およびサービスの再起動

次の表に、リセット、再起動、およびリブートの詳細を含むセキュリティアクションを示します。

表 *1:* リセット、再起動、およびリブートを含むセキュリティアクションの詳細：

シリアル番号	操作	リセット（あり/なし）	再起動（あり/なし）
1	セキュリティプロファイルの適用	○	いいえ
2	電話機のセキュリティ強化の適用	—	—
3	セキュリティモードの変更	ありすべてのデバイス	ありCallManager サービスを再起動します。
4	CTL ファイルの更新	—	はい。すべての暗号化および認証された電話機は、更新されたCTL ファイルを取得するためにリセットする必要があります。
5	TLS 接続のポートの更新	—	ありCTL プロバイダーサービスを再起動します。
6	CAPF サービスパラメータの更新/設定	—	ありシスコ認証局プロキシ機能サービスの再起動

シリアル番号	操作	リセット（あり/なし）	再起動（あり/なし）
7	CTL プロバイダーサービスの開始または停止	—	ありすべての Cisco CallManager サービスおよび Cisco TFTP サービスを再起動します。
7	セキュアな SRST リファレンスの設定	あり従属デバイスのリセット	—
8	スマートカードサービスを開始および自動に変更	—	はい
9	アプリケーションユーザの CAPF プロファイルに関連付けられているセキュリティ関連サービスパラメータを設定します。	—	ありその後、Cisco IP Manager Assistant サービス、Cisco Web Dialer Web サービス、および Cisco Extended Functions サービスを再起動します。

Unified Communications Manager サービスを再起動するには、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

電話の設定を更新した後に単一のデバイスをリセットするには、電話セキュリティプロファイルの適用に関連するトピックを参照してください。

デバイス、サーバ、クラスタ、およびサービスのリセット

このセクションでは、Cisco Unified Serviceability で、デバイス、サーバ、クラスタ、およびサービスをリセットするシナリオについて説明します。

クラスタ内のすべてのデバイスをリセットするには、次の手順を実行します。

ステップ 1 Unified Communications Managerから、**[システム（System）] > [CiscoUnifiedCM]** を選択します。

ステップ 2 [検索（Find）] をクリックします。

設定されている Unified Communications Manager サーバの リストが表示されます。

ステップ 3 デバイスをリセットする Unified Communications Manager を選択します。

ステップ 4 [リセット（Reset）] をクリックします。

ステップ 5 クラスタ内のサーバごとにステップ 2 とステップ 4 を実行します。

割り込みセットアップによるメディア暗号化

暗号化用に Cisco Unified IP Phone 7962 および 7942 の割り込みを設定し、 Cisco Unified Communications Manager Administration で次のタスクを実行します。

- CLI コマンド（utils ctl set cluster mixed-mode）を使用してクラスターセキュリティモードを更新します。
- **[サービスパラメータ（Service Parameter）]** ウィンドウで、[有効な組み込みブリッジ（Builtin Bridge Enable）] パラメータを更新します。

タスクが完了すると、次のメッセージが表示されます。

注目 Cisco Unified IP Phone モデル 7962 および 7942 の暗号化を設定する場合、暗号化されたデバイスは、暗号化されたコールに参加しているときに割り込みリクエストを受け入れることができません。コールが暗号化されていると、割り込みの試行は失敗します。

Cisco Unified IP Phone7962 および 7942 （暗号化されたセキュリティプロファイルで設定済み）では、[電話の設定（Phone Configuration）] ウィンドウにメッセージが表示 されません。[組み込みブリッジ（Built In Bridge）] 設定に **[デフォルト（Default）]** を選択するか、または [Default] と同等のデフォルト設定を選択します。いずれの選択にも同じ制限が適用されます。

ヒント 変更を有効にするには、依存する Cisco IP デバイスをリセットする必要があります。

一般的なアイコン

Unified Communications Manager は、コールに参加するサーバおよびデバイスのセキュリティレベルに応じてコールのセキュリティステータスを提供します。

セキュリティアイコンをサポートするすべての電話機に、コールのセキュリティレベルが表示されます。

- シグナリングセキュリティレベルが認証済みのコールに対して、保護アイコンが表示されます。シールドは、Cisco IP デバイス間のセキュリティで保護された接続を識別します。つまり、デバイスは認証済みで、暗号化済みのシグナリングを使用していることを意味します。
- 暗号化されたメディアを使用するコールにはロックアイコンが表示されます。これは、デバイスが暗号化されたシグナリングと暗号化メディアを使用していることを意味します。

（注） 一部の電話機モデルでは、ロックアイコンのみが表示されます。

コールのセキュリティステータスは、ポイントツーポイント、クラスタ間、クラスタ間、およびマルチホップコールで変更できます。SCCP回線、SIP回線、およびh.323シグナリングは、参加しているエンドポイントに対するコールセキュリティステータスの変更に関する通知をサポートします。

音声コールとビデオコールは、コールセキュリティステータスのベースとなります。音声とビデオの両方がセキュアである場合に限り、安全とみなされます。

（注） 「Override BFCP Application Encryption Status When Designating Call Security Status」サービスパラメータは、パラメータ値が [True] で音声がセキュアであると、ロックアイコンを表示します。この状態は、他のすべてのメディアチャネルのセキュリティステータスを無視します。デフォルト パラメータ値は [False] です。

会議および割り込みコールの場合、[セキュリティ(security)]アイコンに会議のセキュリティステータスが表示されます。

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。