デフォルトのセキュリティ設定

このセクションでは、デフォルトのセキュリティ設定について説明します。

デフォルトのセキュリティ機能

デフォルトのセキュリティとして、Cisco Unified IP Phone には次の自動化されたセキュリティ機能が用意されています。

- 電話設定ファイルの署名
- 電話設定ファイル暗号化のサポート
- Tomcat および他の Web サービスでの https の利用（MIDlet）

Unified Communications Manager リリース 8.0 以降では、CTL クライアントが実行されているかどうかにかかわらず、これらのセキュリティ機能がデフォルトで提供されています。

信頼検証サービス

信頼検証サービス（TVS）はSBDの主要コンポーネントです。TVSを使用するとCisco Unified IP PhoneはHTTPS確立時にEMサービス、ディレクトリ、MIDletなどのアプリケーションサーバを認証できます。

TVS には次の機能があります。

- 拡張性：Cisco IP Phone リソースは信頼する証明書の数の影響を受けません。
- 柔軟性：信頼証明書の追加や削除はシステムに自動的に反映されます。
- デフォルトのセキュリティ：非メディアおよびシグナリングセキュリティ機能はデフォルトのインストールに含まれており、ユーザの介入は必要ではありません。

（注） セキュアなシグナリングおよびメディアを有効にする場合は、CTL ファイルを作成し、クラスタを混合モードに設定する必要があります。**utils ctl set-cluster mixed-mode** CLI コマンドを使用して、CTL ファイルの作成とセキュリティ モードの変更を一度に行うことができます。

TVS の説明

次の基本概念は信頼検証サービスを説明します。

- TVS は Unified Communications Manager サーバ上で動作し、Cisco IP Phone の代わりに証明書を認証します。
- 信頼できる証明書をすべてダウンロードするのではなく、Cisco IP Phone では TVS を信頼するだけで済みます。
- TVS 証明書およびいくつかのキー証明書が、初期信頼リスト ファイル（ITL）と呼ばれる新しいファイルにまとめられます。
- ITL ファイルはユーザの介入なしで自動的に生成されます。
- ITL ファイルは Cisco IP Phone によってダウンロードされ、そこから信頼情報がフローします。

初期信頼リスト

次の操作を実行するには、Cisco IP Phone に初期信頼リスト（ITL）が必要です。

- 設定ファイルの署名を認証する。

- CAPF とセキュアに通信する。設定ファイル暗号化をサポートするための前提条件です。
- TVS を使用する EM サービス、ディレクトリ、MIDlet などのアプリケーション サーバを認証します。

Cisco IP Phone に CTL ファイルがまだ存在していない場合、最初の ITL ファイルが自動的に信頼されます。テレビは、署名者に対応する証明書を返すことができる必要があります。

Cisco IP Phone に既存の CTL ファイルがある場合、ITL ファイルの署名の認証にその CTL ファイルが使用されます。

SHA-1 または MD5 アルゴリズム値は、初期信頼リスト (ITL) ファイルの値に変更があった場合にのみ変更されます。ITL ファイルのチェックサム値を使用すると、Cisco IP Phone と Unified Communications Manager クラスタの間にある ITL ファイルの差異を特定できます。ITL ファイルのチェックサム値は、ITL ファイルを変更した場合にのみ変更されます。

ITL ファイル

最初の信頼リスト (ITL) ファイルは、CTL ファイルと同じ形式になっています。ただし CTL ファイルよりも小さく、スリム化されたバージョンです。ITL ファイルには次の属性が適用されます。

- クラスタをインストールすると、システムが自動的にITLファイルをビルドします。内容が変更された場合、ITL ファイルは自動的に更新されます。
- ITL ファイルは eToken を必要としません。このファイルはソフト eToken（TFTP サーバの CallManager 証明書に関連付けられている秘密キー）を使用します。
- Cisco IP Phone は、起動時間中、リセット中、または CTL ファイルのダウンロード後に ITL ファイルをダウンロードします。

ITL ファイルの内容

ITL ファイルには次の証明書が含まれています。

- TFTP サーバの CallManager 証明書。この証明書によって、ITL ファイルの署名および電話設定ファイルの署名を認証できます。
- クラスタ内で、すべての TVS 証明書が利用可能です。これらの証明書によって、電話が TVS とセキュアに通信し、証明書の認証を要求することができます。
- CAPF 証明書：これらの証明書は、設定ファイルの暗号化をサポートしています。CAPF 証明書は必ずしも ITL ファイル内に存在する必要はありません（TVS で認証可能）が、CAPF 証明書によって CAPF への接続が簡易化されます。

ITL ファイルには証明書ごとに 1 つのレコードが含まれます。各レコードの内容は次のとおりです。

- 証明書

- Cisco IP Phone による検索を容易にするための、事前に抽出された証明書フィールド。
- 証明書の権限（TFTP、CUCM、TFTP+CCM、CAPF、TV、SAST）

TFTP サーバの CallManager 証明書は、2 つの異なる権限を持つ次の 2 つの ITL レコード内に存在します。

- TFTP 権限 または TFTP および CCM 権限：設定ファイルの署名を認証する。
- SAST 権限：ITL ファイルの署名を認証する。

ITL ファイルと CTL ファイルのインタラクション

Cisco IP Phone は、クラスタ セキュリティ モード（非セキュアまたは混合モード）を確認する際に CTL ファイルを使用します。CTL ファイルは、Unified Communications Manager レコードに Unified Communications Manager 証明書を含めることで、クラスタ セキュリティ モードを追跡します。

ITL ファイルにも、クラスタ セキュリティ モードを示す情報が含まれます。

ITLRecovery 証明書の証明書管理の変更

- ITLRecovery の有効期間が 5 年間から 20 年間に延長され、より長い期間にわたって同じ ITLRecovery 証明書が使用されるようになりました。

（注） Unified Communications Manager をアップグレードした場合、ITLRecovery 証明書の有効期間は引き続き 5 年のままです。Unified Communications Manager をアップグレードすると、新しいリリースに証明書がコピーされます。ただし、ITLRecovery 証明書を再生成するか、Unified Communications Manager の新規インストールを実行すると、ITLRecovery の有効期間が 20 年に延長されます。

- ITLRecovery 証明書を再生成する前に、警告メッセージが CLI と GUI の両方で表示されます。この警告メッセージでは、トークンレス CTL を使用している場合、および CallManager 証明書を再生成している場合には、CTL ファイルに更新された CallManager 証明書があり、その証明書がエンドポイントに対して更新されていることを確認することが指示されます。

連携動作と制限事項

Unified Communications Manager クラスタに 39 を超える証明書がある場合、Cisco IP Phone 上の ITL ファイル サイズが 64 キロバイトを超えます。ITL ファイル サイズが増加すると、電話での ITL の正常なロードに影響し、Unified Communications Manager での電話登録が失敗することになります。

Cisco Unified IP Phone の ITL ファイルの更新

電話機にインストールされている ITL ファイルで [デフォルトのセキュリティ（Security By Default）] を使用する Cisco Unified CM の集中型 TFTP では、TFTP 設定ファイルを検証しません。

（注） リモートクラスタから電話機を集中型TFTP構成に追加する前に、次の手順を実行してください。

手順

ステップ 1 中央 TFTP サーバで、**Prepare Cluster for Rollback to pre-8.0** エンタープライズ パラメータを有効にします。

ステップ 2 TVS および TFTP を再起動します。

ステップ 3 すべての電話をリセットし、ITL 署名検証を無効にする新しい ITL ファイルがダウンロードされることを確認します。

ステップ 4 [Secure https URLs] エンタープライズ パラメータで、HTTPS ではなく HTTP を使用するように設定します。

（注） Unified Communications Manager のリリース 10.5 以降では、[**クラスタの 8.0 以前へのロールバック準備（Prepare Cluster for Rollback to pre-8.0）**] エンタープライズ パラメータを有効にした後、電話が自動的にリセットされます。中央TFTPサーバのUnified Communications Managerバージョンについて、またこのパラメータを有効にする方法については、『*Cisco Unified Communications Manager* セキュリティ ガイド』の「8.0 より前のリリースにクラスタをロールバックする」のセクションを参照してください。

自動登録

自動登録は、混合モードと非セキュアモードの両方でサポートされます。また、デフォルトの設定ファイルに対する署名も行われます。「デフォルトのセキュリティ」がサポートされていない Cisco IP Phone には、署名されていないデフォルトの設定ファイルが提供されます。

Cisco Unified IP Phone サポート リストの取得

手順

ステップ 1 Cisco Unified Reporting のメイン ウィンドウで、[System Reports] をクリックします。
ステップ 2 [System Reports] リストで、[Unified CM Phone Feature List] をクリックします。
ステップ 3 [**機能（Feature）**] ドロップダウンリストから該当の機能を選択します。
ステップ 4 [Submit] をクリックします。

認定されたソリューション向けコモン クライテリアの ECDSA サポート

Unified Communications Manager は、楕円曲線デジタル署名アルゴリズム（ECDSA）証明書をサポートします。これらの証明書は、RSA ベースの証明書よりも堅牢であり、コモン クライテリア（CC）認定のある製品に必要となります。米国政府の Commercial Solutions for Classified Systems（CSfC）プログラムは、CC 認定が必要なので、Unified Communications Manager にはこれが含まれています。

ECDSA 証明書は、証明書マネージャ、SIP、Certificate Authority Proxy Function（CAPF）、Transport Layer Security（TLS）、トレース、エントロピー、HTTP、CTI Manager で既存の RSA 証明書とともに使用できます。

（注） ECDSA は、Unified Communications Manager と Tomcat についてのみサポートされています。

証明書マネージャでの ECDSA サポート

Unified Communications Manager リリース 11.0 の証明書マネージャでは、自己署名 ECDSA 証明書と ECDSA 証明書署名要求（CSR）の両方の生成がサポートされています。これより前の Unified Communications Manager では、**RSA** 証明書のみがサポートされていました。しかし、Unified Communications Manager リリース 11.0 以降では、既存の **RSA** 証明書に加えて **CallManager-ECDSA** 証明書がサポートされます。

CallManager 証明書と **CallManager-ECDSA** 証明書の両方が、共通の信頼ストアである CallManager-Trust を共有します。Unified Communications Manager によって、これらの証明書がこの信頼ストアにアップロードされます。

証明書マネージャでは、キー長の値が異なる ECDSA 証明書の生成がサポートされています。

Unified Communications Managerをインストールすると、自己署名証明書が生成されます。Unified Communications Manager リリース 11.0 には常時 ECDSA 証明書が存在し、この証明書が SIP インターフェイスで使用されます。セキュアなコンピュータ テレフォニー インテグレーション（CTI）マネージャ インターフェイスでも、ECDSA 証明書がサポートされます。CTI Managerと SIP サーバの両方で同じサーバ証明書が使用されるため、両方のインターフェイスが同期して動作します。

SIP での ECDSA サポート

Unified Communications Manager リリース 11.0 には SIP 回線と SIP トランク インターフェイス向けの ECDSA サポートが含まれています。Unified Communications Manager とエンドポイント電話またはビデオ デバイスとの間の接続は SIP 回線接続であるのに対し、2 つの Unified Communications Manager 間の接続は SIP トランク接続です。すべての SIP 接続では ECDSA 暗号方式がサポートされ、ECDSA 証明書が使用されます。

以下は、SIP が TLS（Transport Layer Security）接続を設定するシナリオです。

- SIP が TLS サーバとして機能する場合：Unified Communications Manager が着信するセキュア SIP 接続の TLS サーバとして機能する場合、SIP トランク インターフェイスは CallManager-ECDSA の証明書がディスクにあるかどうかを判断します。証明書がディスクにあり、選択された暗号スイートが **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** または **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** である場合、SIP トランクインターフェイスはCallManager-ECDSAを使用します。SIPトランク インターフェイスは ECDSA 暗号化スイートをサポートしないクライアントからの接続では RSA TLS 暗号スイートを引き続きサポートします。**[TLS Ciphers]** ドロップダウンリストには、Unified Communications Manager が TLS サーバとして機能するときにサポートされている暗号スイートの設定を許可するオプションがあります。
- SIP が TLS クライアントとして機能する場合：SIP トランク インターフェイスが TLS クライアントとして機能する場合、SIP トランク インターフェイスは Cisco Unified Communications Manager の [Enterprise Parameters] ウィンドウにある [TLS Ciphers] フィールド（[ECDSA ciphers] オプションも含む）に基づいて、要求された暗号化スイートのリストをサーバに送信します。[TLS Ciphers]。この設定は優先順位の高い順に TLS クライアント暗号化スイートのリストと、サポートされている暗号スイートを決定します。

（注） ECDSA クライアント証明書をサポートしていない以前のリリースの Unified Communications Manager と TLS 接続を確立する場合、この接続ではRSA暗号スイートが使用されます。TLS接続で送信されるクライアント証明書は、選択したTLS暗号に関連付けられている必要はありません。以前のリリースのUnified Communications Manager でも、TLS サーバが ECDSA クライアント証明書を受信して処理することがサポートされています。

Unified Communications Manager への接続に ECDSA 暗号を使用するデバイスでは、アイデンティティ信頼リスト（ITL ファイル）に CallManager-ECDSA 証明書が必要です。次に、デバイスは CallManager-ECDSA 証明書をローカル証明書ストアに組み込み、CallManager-ECDSA 証明書でセキュリティ保護された接続を信頼する必要があります。

CAPF での ECDSA サポート

Certificate Authority Proxy Function（CAPF）は、シスコのエンドポイントと Unified Communications Manager との間で証明書を交換する、シスコ独自のメソッドです。CAPF を使用するのはシスコのエンドポイントだけです。コモン クライテリア要件を達成するため、CAPF は CAPF バージョン 3 に更新され、クライアントに ECDSA ローカルで有効な証明書（LSC）を提供できるようになりました。顧客は LSC をローカルに作成します。LSC はメーカーが作成する製造者インストール証明書（MIC）の代替です。

CAPF バージョン 3 を使うことで、Unified Communications Manager サーバから電話、CTI アプリケーション、Jabber クライアントに対し、LSC で使用される EC キーの生成を指示できます。EC キーが生成されると、Unified Communications Manager は ECDSA LSC を生成して Cisco エンドポイントに送信するか、または ECDSA CSR を生成します。

エンドポイントで CAPF バージョン 3 がサポートされていない場合、[Cisco Unified CM Administration] からバックアップとして、必要な EC キー サイズと RSA キー サイズを設定して、[Phone Configuration] ウィンドウにある [EC Preferred, RSA Backup] オプションを選択できます。CAPF サーバが EC キー ペアに要求の送信を試行し、電話が EC キーをサポートしていないサーバと通信する場合、このバックアップ オプションが役立ちます。サーバは EC キー ペアの代わりに RSA キー ペアを生成するよう要求を送信します。

（注） Cisco エンドポイントが CAPF バージョン 3 をサポートしている場合、**Endpoint Advanced Encryption アルゴリズムのサポート**のパラメータを有効にした状態で [**電話の設定**（**Phone Configuration**）] で [**EC 優先、RSA バックアップ**（**EC Preferred, RSA Backup**）] オプションを選択しても、ECDSA ベースまたは RSA ベースの LSC は発行されません。Cisco エンドポイントが CAPF バージョン 3 をサポートしていない場合、**Endpoint Advanced Encryption アルゴリズムのサポート**のパラメータを有効または無効にすると、RSA ベースの LSC が発行されます。

（注） Endpoint **Advanced Encryption アルゴリズムのサポート**パラメータは、電話機が高度な TLS 暗号を使用して TFTP 設定ファイルをダウンロードすることを示します。デフォルトでは、EC の暗号が最も優先順位が高く設定されています。このソリューションは、MRA を使用しないオンプレミスの展開でのみサポートされています。

エントロピー

強力な暗号化には、エントロピーの堅牢なソースが必要です。エントロピーはデータのランダム性の指標であり、コモンクライテリア要件の最小しきい値の決定に役立ちます。暗号化などのデータ変換方式の効率もエントロピーの優れたソースの有無に依存します。ECDSA のような強力な暗号化アルゴリズムであっても、エントロピーの弱いソースを使用すれば、暗号化が容易に破られてしまいます。

Unified Communications Manager リリース 11.0 では、Unified Communications Manager のエントロピー ソースが向上しました。エントロピー モニタリング デーモンは設定が不要な組み込み機能です。ただし、Unified Communications Manager CLI によってオフにすることができます。

エントロピー モニタリング デーモン サービスの制御には、次の CLI コマンドを使用します。

CLI コマンド	説明
utils service start Entropy Monitoring Daemon	エントロピー モニタリング デーモン サービスを開始します。
utils service stop Entropy Monitoring Daemon	エントロピー モニタリング デーモン サービスを停止します。
utils service active Entropy Monitoring Daemon	エントロピー モニタリング デーモン サービスをアクティブにします。さらにカーネル モジュールがロードされます。
utils service deactive Entropy Monitoring Daemon	エントロピー モニタリング デーモン サービスを非アクティブ化します。さらにカーネル モジュールがアンロードされます。

コンフィギュレーション ダウンロードの HTTPS サポート

セキュアなコンフィギュレーション ダウンロードのため Unified Communications Manager リリース 11.0 では、以前のリリースでの HTTP および TFTP インターフェイスに加えて、HTTPS をサポートするように機能強化されました。必要な場合には、クライアントとサーバの両方が相互認証を使用します。ECDSA LSC および暗号化された TFTP コンフィギュレーションを使用して登録されたクライアントは、LSC を提示する必要があります。

HTTPS インターフェイスでは、サーバ証明書として CallManager と CallManager-ECDSA 証明書の両方が使用されます。

（注） CallManager、CallManager ECDSA、Tomcat 証明書を更新する場合、TFTP サービスを無効化してから再び有効化する必要があります。CallManager 証明書と CallManager-ECDSA 証明書の認証にはポート 6971 が使用され、Tomcat 証明書の認証にはポート 6972 が使用されます。

CTI Manager のサポート

コンピュータ テレフォニー インテグレーション（CTI）インターフェイスが、4 つの新しい暗号方式をサポートするよう強化されました。暗号スイートは **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**、**TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**、**TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**、および **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** です。これらの暗号スイートのサポートによって、CTI Manager インターフェイスでは、Unified Communications Manager 内に存在する場合に、**CallManager-ECDSA** 証明書の保有が必要となりました。SIP インターフェイスと同様、CTI Manager セキュア インターフェイスでサポートされる TLS 暗号方式の設定には、Unified Communications Manager 内のエンタープライズ パラメータ [TLS Ciphers] オプションが使用されます。

証明書の再生成

Unified Communications Manager 証明書の 1 つを再生成した場合、この項で説明する手順を実行する必要があります。

注意 証明書を再生成すると、システムの動作に影響する場合があります。証明書を再生成すると、サードパーティの署名付き証明書（アップロードされている場合）を含む既存の証明書が上書きされます。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

CAPF 証明書の再生成

CAPF 証明書を再生成するには、次の手順を実行します。

（注） CAPF 証明書がパブリッシャにある場合は、電話が各自の ITL ファイルを更新するために自動的に再起動することがあります。

手順

ステップ 1 CAPF 証明書を再生成します。

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

ステップ 2 CTL ファイルがある場合は、CTL クライアントを再実行する必要があります。

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

ステップ 3 CAPF サービスを再起動します。

詳細については、『*Cisco Unified Communications Manager Security Guide*』の「「Activating the Certificate Authority Proxy Function Service」」の項を参照してください。

TVS 証明書の再生成

TVS 証明書の再生成では手作業は必要はありません。

（注） TVS および TFTP 両方の証明書を再生成する場合は、TVS 証明書を再生成し、電話が再起動する場合は再起動が完了するまで待ってから、TFTP 証明書を再生成します。

TFTP 証明書の再生成

TFTP 証明書を再生成するには、次の手順を実行します。

（注） 複数の証明書を再生成する場合は、TFTP 証明書の再生成を最後に行う必要があります。電話が再起動する場合は再起動が完了するまで待ってから、TFTP 証明書を再生成します。この手順に従わないと、すべての Cisco IP Phone から ITL ファイルを手動で削除する必要が生じることがあります。

手順

ステップ 1 TFTP 証明書を再生成します。

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

ステップ 2 TFTP サービスをアクティブにしたら、すべての電話が自動的に再起動するまで待ちます。

ステップ 3 クラスタが混合モードである場合は、CTL クライアントを実行します。

第 4 章「「CTL クライアントの設定」」を参照してください。

ステップ 4 クラスタが EMCC 導入に含まれる場合、証明書の一括プロビジョニングの手順を繰り返します。

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

ITLRecovery 証明書の再生成

警告 ITLRecovery 証明書は電話機での有効期限が長く、CallManager 証明書も含まれているため、頻繁に再生成しないでください。

非セキュア クラスタの ITLRecovery 証明書の再生成

1. ITL ファイルが有効であることと、クラスタ内のすべての電話機が現在の ITL ファイルを信頼していることを確認します。
2. ITLRecovery 証明書を再生成します。

   各クラスタ内のパブリッシャに移動して ITLRecovery 証明書を再生成します。

   1. [Unified OS の管理（Unified OS Administration）] から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
   2. [検索（Find）] をクリックします。

      [証明書の一覧（Certificate List）] ウィンドウが表示されます。
   3. 表示された証明書の一覧から、[ITLRecovery.pem Certificate] リンクをクリックします。
   4. [**再生成（Regenerate**）] をクリックして ITLRecovery 証明書を再生成します。
   5. ポップアップ表示された確認メッセージで、[**OK**] をクリックします。
3. [証明書の管理（Certificate Management）] で `utils itl reset localkey` を使用して ITL ファイルに署名し、新しい ITL ファイルを受け入れます。
4. クラスタ内のすべての電話機を一括でリセットします。

（注） クラスタ内のすべての電話機が登録済みであることを確認してください。

5. 新しい ITLRecovery 証明書によって ITL ファイルが再署名されるように、TFTP サービスを再起動します。

   新しい ITLRecovery 証明書は、リセット中に電話機にアップロードされます。
6. 新しい ITL ファイルを取得するために、クラスタ内のすべての電話機に対して 2 回目の一括リセットを行います。
7. リセット後、新しい ITLRecovery 証明書が電話機にアップロードされます。

セキュア クラスタの ITLRecovery 証明書の再生成

トークンベースの ITL ファイルからトークンレスの ITL ファイルに移行する場合は、セキュリティ ガイドの「移行」の項を参照してください。

1. ITL ファイルが有効であることと、クラスタ内のすべての電話機が現在の ITL ファイルを信頼していることを確認します。
2. `show ctl` コマンドを使用して CTL ファイルを確認します。
3. ITLRecovery 証明書を再生成します。

   各クラスタ内のパブリッシャに移動して ITLRecovery 証明書を再生成します。

   1. [Unified OS の管理（Unified OS Administration）] から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [検索（Find）]** を選択します。
   2. [**検索（Find**）] をクリックして、証明書の一覧を表示します。

      [証明書の一覧（Certificate List）] ウィンドウが表示されます。
   3. 表示された証明書の一覧から、[ITLRecovery.pem Certificate] リンクをクリックします。
   4. [**再生成（Regenerate**）] をクリックして ITLRecovery 証明書を再生成します。
   5. ポップアップ表示された確認メッセージで、[**OK**] をクリックします。
4. [証明書の管理（Certificate Management）] で `utils ctl reset localkey` を使用して CTLFile に署名します。またこの操作により、新しい ITLRecovery 証明書で CTLFile が更新されます。
5. 新しい ITLRecovery 証明書に更新された新しい CTLFile を取得するために、クラスタ内のすべての電話機を一括でリセットします。

（注） クラスタ内のすべての電話機が登録済みであることを確認してください。

6. 新しい ITLRecovery 証明書によって CTLFile に再署名するため、`utils ctl update CTLFile` を使用して CTLFile を更新します。
7. 新しい ITLRecovery 証明書によって署名された新しい CTLFile を取得するために、クラスタ内のすべての電話機に対して 2 回目の一括リセットを行います。
8. リセット後、新しい ITLRecovery 証明書が電話機にアップロードされます。

Tomcat 証明書の再生成

CAPF 証明書を再生成するには、次の手順を実行します。

手順

ステップ 1 Tomcat 証明書を再生成します。

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

ステップ 2 Tomcat および TFTP サービスを再起動します。

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

ステップ 3 クラスタが EMCC 導入に含まれる場合、証明書の一括プロビジョニングの手順を繰り返します。

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

TFTP 証明書の再生成後のシステム バックアップ手順

ITL ファイルのトラスト アンカーはソフトウェア エンティティ、つまり TFTP 秘密キーです。サーバがクラッシュすると、キーは失われ、電話は新しいITLファイルを検証できなくなります。

Unified Communications Manager リリース 10.0 では、TFTP 証明書と秘密キーの両方がディザスタ リカバリ システムによってバックアップされます。システムはバックアップ パッケージを暗号化して秘密キーを保護します。サーバがクラッシュすると、以前の証明書およびキーが復元されます。

TFTP 証明書が再生成されるたびに、新しいシステムのバックアップを作成する必要があります。バックアップ手順については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unified Communications Manager リリース 7.x からリリース 8.6 以降への更新アップグレード

クラスタをリリース7.xから8.6以降にアップグレードするには、この手順に従ってください。

手順

ステップ 1 クラスタをアップグレードするための通常の手順に従ってください。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ヒント クラスタのすべてのノードを Unified Communications Manager リリース 8.6 以降にアップグレードした後、さらにこの手順に従ってご使用の Cisco Unified IP Phone をシステムに登録する必要があります。

ステップ 2 次のリリースのいずれかを混合モードで実行している場合、CTL クライアントの実行が必要です。

- Unified Communications Manager リリース 7.1(2)
  - 7.1(2) のすべての正規リリース
  - 007.001(002.32016.001) よりも前の 712 のすべての ES リリース
- Unified Communications Manager リリース 7.1(3)
  - 007.001(003.21900.003) = 7.1(3a)su1a よりも前の 713 のすべての正規リリース
  - 007.001(003.21005.001) よりも前の 713 のすべての ES リリース

（注） CTL クライアントの実行の詳細については、第 4 章「「CTL クライアントの設定」」を参照してください。

ステップ 3 Cisco IP Phone が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

注意 クラスタを復元できるようにするため、ディザスタ リカバリ システム（DRS）を使用してクラスタのバックアップを作成する必要があります。

ステップ 4 ご使用のクラスタをバックアップします。

DRS を使用してクラスタをバックアップするには、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

次のタスク

アップグレード後にパブリッシャが起動したら、CAR の移行が完了するまで再起動しないでください。このフェーズでは、古いバージョンに切り替えたり、DRS バックアップを実行することは許可されません。**[Cisco Unified Serviceability]** > **[Tools]** > **[CDR Analysis and Reporting]** を開いて CAR 移行の状態をモニタできます。

リリース 8.0 以前のクラスタへのロールバック

クラスタを Unified Communications Manager の旧リリース（リリース 8.0 よりも前）にロールバックする場合は、その前に [Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを使用したロールバックの準備が必要です。

クラスタをロールバックするための準備を行うには、クラスタの各サーバで次の手順に従います。

手順

ステップ 1 [Unified Communications Manager Administration]で 、**[System]** > **[Enterprise Parameters Configuration]** を選択します。

[Enterprise Parameters Configuration] ウィンドウが表示されます。

[Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを [True] に設定します。

（注） クラスタを Unified Communications Manager のバージョン 8.0 以前へロールバックする準備を行う場合のみ、このパラメータを有効にします。このパラメータが有効になっている間、HTTPS を使う電話サービス（たとえば、エクステンション モビリティなど）は機能しません。ただし、このパラメータが有効になっていても、基本的な電話の発信および受信は引き続き可能です。

ステップ 2 Cisco IP Phone が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

ステップ 3 クラスタの各サーバを以前のリリースに戻します。

クラスタを以前のバージョンに戻す方法の詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 4 クラスタが以前のバージョンに切り替わるまで待ちます。

ステップ 5 次のリリースのいずれかを混合モードで実行している場合、CTL クライアントの実行が必要です。

- Unified Communications Manager リリース 7.1(2)
  - 7.1(2) のすべての正規リリース
  - 007.001(002.32016.001) よりも前の 712 のすべての ES リリース
- Unified Communications Manager リリース 7.1(3)
  - 007.001(003.21900.003) = 7.1(3a)su1a よりも前の 713 のすべての正規リリース
  - 007.001(003.21005.001) よりも前の 713 のすべての ES リリース

（注） CTL クライアントの実行方法の詳細については、「「CTL クライアントの設定」」の章を参照してください。

ステップ 6 「[Prepare Cluster for Rollback to pre-8.0]」 エンタープライズ パラメータが [True] に設定されている場合、社内ディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Corporate Directory] で、サービス URL を「Application:Cisco/CorporateDirectory」から「http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp」へと変更します。

ステップ 7 「[Prepare Cluster for Rollback to pre-8.0]」 エンタープライズ パラメータが [True] に設定されている場合、パーソナル ディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Personal Directory] で、サービス URL を「Application:Cisco/PersonalDirectory」から「http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=undefined」へと変更します。

戻した後のリリース 8.6 以降への再切り替え

クラスタをリリース 7.x に戻した後でリリース 8.6 以降のパーティションに再度切り替える場合は、次の手順を実行します。

手順

ステップ 1 クラスタを非アクティブのパーティションに再度切り替えるための手順に従います。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 2 次のいずれかのリリースを混合モードで使用していた場合は、CTL クライアントを実行する必要があります。

Unified Communications Manager リリース 7.1(2)

- 7.1(2) のすべての正規リリース
- 007.001(002.32016.001) よりも前の 712 のすべての ES リリース
- Unified Communications Manager リリース 7.1(3)
  - 007.001(003.21900.003) = 7.1(3a)su1a よりも前の 713 のすべての正規リリース
  - 007.001(003.21005.001) よりも前の 713 のすべての ES リリース

（注） CTL クライアントの実行方法の詳細については、「「CTL クライアントの設定」」の章を参照してください。

ステップ 3 [Unified Communications Manager Administration]で 、**[System]** > **[Enterprise Parameters Configuration]** を選択します。

[Enterprise Parameters Configuration] ウィンドウが表示されます。

[Prepare Cluster for Rollback to pre-8.6] エンタープライズ パラメータを [False] に設定します。

ステップ 4 Cisco Unified IP Phone が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

Cisco Unified Communications Manager および ITL ファイルによるクラスタ間での IP Phone の移行

Unified Communications Manager 8.0(1) 以降では、新しいデフォルトのセキュリティ機能と初期信頼リスト（ITL）ファイルが導入されました。この新機能により、異なる Unified CM クラスタ間の電話の移行では、必ず正しい手順で移行できるよう注意します。

⚠

注意 正しい手順に従わないと、数千台の電話の ITL ファイルを手動で削除しなければならない状況が発生する可能性があります。

新しい ITL ファイルをサポートする Cisco IP Phone では、Unified CM TFTP サーバからこの特別なファイルをダウンロードする必要があります。ITL ファイルが電話にインストールされると、設定ファイルおよび ITL ファイルの以降の更新では、以下のいずれかによる署名が必要となります。

- 電話に現在インストールされている TFTP サーバ証明書。
- TFTP の証明書。たとえば、いずれかのクラスタの検証済み TVS サービスなど。TVS サービスの証明書は ITL ファイルに示されているクラスタの中にあります。

この新しいセキュリティ機能により、電話を別のクラスタに移動する場合に、次の 3 つの問題が発生する可能性があります。

1. 新しいクラスタの ITL ファイルが現在の ITL ファイルの署名者によって署名されていないため、電話が新しい ITL ファイルや設定ファイルを受け入れることができない問題。
2. 電話の既存の ITL にリストされている TVS サーバは、電話が新しいクラスタに移動すると接続できなくなる可能性があるという問題。
3. TVS サーバが証明書の検証のためにアクセス可能でも、古いクラスタ サーバには新しいサーバ証明書がない可能性があるという問題。

この 3 つの問題のうち 1 つ以上が発生した場合、考えられる解決策の 1 つは、クラスタ間を移動中のすべての電話から ITL ファイルを手作業で削除することです。ただし、この解決方法は電話の数が増えるにつれて大変な労力を必要とするため、望ましい解決策ではありません。

最も推奨されるオプションは、Cisco Unified CM エンタープライズ パラメータ [Prepare Cluster for Rollback to pre-8.0] を使用することです。このパラメータを [True] に設定すると、電話は空の TVS および TFTP 証明書セクションを含む特殊な ITL ファイルをダウンロードします。

電話に空の ITL ファイルがあると、（8.x 以前の Unified CM クラスタへの移行の場合）電話は署名のない設定ファイルをすべて受け入れます。また、（異なる Unified CM 8.x クラスタへの移行の場合）新しい ITL ファイルをすべて受け入れます。

空の ITL ファイルは、電話の **[Settings]** > **[Security]** > **[Trust List]** > **[ITL]** をチェックすることで確認できます。古い TVS や TFTP サーバが指定されていた場所には、空のエントリが表示されます。

新しい空の ITL ファイルをダウンロードできるまで、電話には古い Unified CM サーバにアクセスできる必要があります。

古いクラスタをオンラインにしておく場合は、デフォルトのセキュリティを復元するため、[Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを無効にします。

証明書の一括エクスポート

新旧のクラスタが同時にオンラインになっている場合には証明書の一括移行による方法を使用できます。

Cisco Unified IP Phone は、ダウンロードしたすべてのファイルを、ITL ファイルまたは ITL ファイルに指定されている TVS サーバと照合することに注意してください。電話を新しいクラスタに移動する必要がある場合、新しいクラスタが提示する ITL ファイルは、古いクラスタの TVS 証明書ストアの信頼を得る必要があります。

（注） 証明書の一括エクスポートは、電話の移行中、両方のクラスタがネットワークに接続され、オンラインである場合のみ機能します。

（注） 証明書一括インポート中、Cisco Extension Mobility Cross Cluster（EMCC）が動作を継続するには、訪問クラスタとホーム クラスタの両方において付加的な ITLRecovery 証明書をインポートすることが必要です。[証明書の一括管理（Bulk Certificate Management）] の [証明書タイプ（Certificate Type）] ドロップダウン リストに、ITL_Recovery 証明書をインポートするための新しいオプションが追加されています。

証明書の一括エクスポートを使用するには、以下の手順を実行します。

手順

ステップ 1 [Cisco Unified Operating System Administration] から、**[Security]** > **[Bulk Certificate Management]** を選択します。

ステップ 2 新しい宛先クラスタ（TFTP のみ）から中央の SFTP サーバに証明書をエクスポートします。

ステップ 3 証明書の一括インターフェイスを使用して、SFTP サーバの証明書（TFTP のみ）を統合します。

ステップ 4 元のクラスタで証明書の一括機能を使用し、中央 SFTP サーバから TFTP 証明書をインポートします。

ステップ 5 DHCP オプション 150 またはその他の方式を使用して、電話を新しい宛先クラスタにポイントします。

電話は新しい宛先クラスタの ITL ファイルをダウンロードし、既存の ITL ファイルと照合することを試みます。証明書は既存の ITL ファイル内に存在しないため、電話は古い TVS サーバに新しい ITL ファイルの署名の確認を要求します。この要求を行うため、電話は古い元のクラスタの TCP ポート 2445 に TVS クエリを送信します。

証明書のエクスポート、統合、インポートが正常に行われると、TVS は成功を返し、電話のメモリにある ITL ファイルは新しくダウンロードされた ITL ファイルに置き換わります。

これで、電話は新しいクラスタから署名付き設定ファイルをダウンロードおよび認証できるようになりました。

自己署名証明書の生成

手順

ステップ 1 [Cisco Unified OS Administration] から **[Security]** > **[Certificate Management]** を選択します。[証明書リスト（Certificate List）] ウィンドウが表示されます。

ステップ 2 検索パラメータを入力して、証明書を検索して設定の詳細を表示します。
すべての条件に一致したレコードが [Certificate List] ウィンドウに表示されます。

ステップ 3 新しい自己署名証明書を生成するには、[Generate Self-Signed Certificate] をクリックします。[Generate New Self-Signed Certificate] ウィンドウが表示されます。

ステップ 4 [Certificate Purpose] ドロップダウン ボックスから、[CallManager-ECDSA] などのシステム セキュリティ証明書を選択します。

ステップ 5 [Generate New Self-Signed Certificate] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

ステップ 6 [Generate] をクリックします。

関連トピック

自己署名証明書のフィールド （21 ページ）

自己署名証明書のフィールド

表 *1:* 自己署名証明書のフィールド

フィールド	説明
[Certificate Purpose]	ドロップダウンリストから必要なオプションを選択します。 次のいずれかのオプションを選択すると、[**キー タイプ（Key Type）**] フィールドが自動的に **RSA** に設定されます。 • tomcat • ipsec • ITLRecovery • CallManager • CAPF • TVS 次のいずれかのオプションを選択すると、[**キー タイプ（Key Type）**] フィールドが **EC**（楕円曲線）に自動的に設定されます。 • tomcat-ECDSA • CallManager-ECDSA
[Distribution]	ドロップダウンリストから Unified Communications Manager サーバを選択します。
[Common Name]	[**Distribution**] ドロップダウンリストで選択した Unified Communications Manager サーバの名前が表示されます。

フィールド	説明
[Auto-populated Domains]	[**Certificate Purpose**] ドロップダウンリストから次のオプションのいずれかを選択した場合にのみ表示されます。 • tomcat • tomcat-ECDSA • CallManager • CallManager-ECDSA • TVS このフィールドには、1 つの証明書によって保護されるホストの名前がリスト表示されます。証明書の共通名はホスト名と同じです。**CallManager-ECDSA** 証明書と **tomcat-ECDSA** 証明書の両方には、ホスト名と異なる共通名があります。 このフィールドには、**CallManager-ECDSA** 証明書用の完全修飾ドメイン名が表示されます。
Key Type	このフィールドは秘密/公開キーのペアの暗号化と復号化に使用されるキー タイプを示します。 Unified Communications Manager は **EC** および **RSA** キー タイプをサポートしています。

フィールド	説明
[Key Length]	ドロップダウンリストから、次の値のいずれかを選択します。 • 1024 • 2048 • 3072 • 4096 キー長に応じて、自己署名証明書の要求によりハッシュアルゴリズムの選択肢が限定されます。ハッシュアルゴリズムの選択が限定されることで、キー長の強度以上のハッシュ アルゴリズム強度が確保されます。 • キー長の値が256の場合、サポートされるハッシュアルゴリズムは、SHA256、SHA384、またはSHA512です。 • キー長の値が384の場合、サポートされるハッシュアルゴリズムは、SHA384またはSHA512です。 （注） **キー長**の値が3072または4096の証明書を選択するのは、RSA 証明書の場合のみです。これらのオプションは、ECDSA 証明書については使用できません。 （注） CallManagerの **[Certificate Purpose]** で選択されたRSA **キー長**の値が2048を超えると、電話機のモデルによっては登録に失敗する場合があります。 詳細については、Cisco Unified Reporting Tool（CURT）の [**Unified CM Phone Feature List Report**] で、**3072/4096 RSA キー サイズ サポート**に対応した電話機モデルの一覧を確認できます。
Hash Algorithm	ドロップダウンリストからキー長以上の値を選択します。 （注） • [**Key Length**] フィールドで選択した値に基づいて、[**ハッシュ アルゴリズム（Hash Algorithm**）] ドロップダウンリストの値が変更されます。 • システムがFIPSモードで実行されている場合は、必ずハッシュ アルゴリズムとしてSHA256を選択する必要があります。

証明書署名要求の生成

特定の証明書タイプに対する新しい証明書署名要求を生成すると、アプリケーションはその証明書タイプの既存の証明書署名要求を上書きします。

Cisco Unified オペレーティング システムの管理から CSR を生成し、CA に示すことで、CA 署名の証明書をアップロードすることができます。CSR を生成するたびに、CSR と一緒に新しい秘密キーが生成されます。

秘密キーは、CSR を生成するときに選択した、サーバとサービスに一意なファイルです。セキュリティ コンプライアンスのため、この秘密キーは誰とも共有しないでください。秘密キーを誰かに渡すと、証明書のセキュリティが損なわれます。また、古い CSR を使用して証明書を作成する場合は、同じサービス用の新しい CSR を再生成しないでください。Unified Communications Manager は古い CSR と秘密キーを削除し、それらの両方を新しいものに置き換えて、古い CSR を使用不能にします。

（注） Unified Communications Manager リリース 11.0 以降では、TFTP またはすべての一括操作ユニットを選択した場合は、ECDSA 証明書は RSA 証明書に含まれるようになります。

手順

ステップ 1 [Cisco Unified OS Administration] から **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
[証明書リスト（Certificate List）] ウィンドウが表示されます。

ステップ 2 [Generate CSR] をクリックします。
[Generate Certificate Signing Request] ウィンドウが表示されます。

ステップ 3 検索パラメータを入力して、証明書を検索して設定の詳細を表示します。
すべての条件に一致したレコードが [Certificate List] ウィンドウに表示されます。

ステップ 4 [Certificate Purpose] ドロップダウン ボックスから、[CallManager-ECDSA] などのシステム セキュリティ証明書を選択します。

ステップ 5 [Generate Certificate Signing Request] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

ステップ 6 [Generate] をクリックします。

関連トピック

証明書署名要求のフィールド （25 ページ）

証明書署名要求のフィールド

表 *2:* 証明書署名要求のフィールド

フィールド	説明
[Certificate Purpose]	ドロップダウン ボックスから値を選択します。 • **CallManager** • **CallManager-ECDSA**

[Distribution]	Unified Communications Manager サーバを選択します。
	ECDSA の MultiServer にこのフィールドを選択すると、構文は次のとおりです。
	`Callmanager-ecdsa common name: <host-name>-EC-ms.<domain>`
	RSA の MultiServer にこのフィールドを選択すると、構文は次のとおりです。
	`Callmanager common name: <host-name>-ms.<domain>`

Common Name	デフォルトでは、**[Distribution]** フィールドで選択した Unified Communications Manager アプリケーションの名前が表示されます。
[Auto-populated Domains]	このフィールドは [Subject Alternate Names（SANs）] セクションに表示されます。1 つの証明書によって保護されるホストの名前をリストします。
[Parent Domain]	このフィールドは [Subject Alternate Names（SANs）] セクションに表示されます。デフォルトドメイン名を表示します。必要に応じてドメイン名を変更できます。
[Key Type]	このフィールドは秘密/公開キーのペアの暗号化と復号化に使用されるキー タイプを示します。 Unified Communications Manager は **EC** および **RSA** キー タイプをサポートしています。

フィールド	説明
[Key Length]	[Key Length] ドロップダウン ボックスから、値を 1 つ選択します。 キーの長さに応じて、CSR 要求によりハッシュ アルゴリズムの選択肢が限定されます。ハッシュ アルゴリズムの選択に制限が加わることで、キー長の強度以上のハッシュ アルゴリズム強度が確保されます。たとえばキー長が 256 の場合、サポートされるハッシュ アルゴリズムは、SHA256、SHA384、SHA512 です。同様にキー長が 384 の場合、サポートされるハッシュ アルゴリズムは SHA384 または SHA512 です。 （注） RSA 証明書については、[Key Length] の値が 3072 または 4096 の証明書のみを選択できます。これらのオプションは、ECDSA 証明書については使用できません。 （注） CallManager が [Certificate Purpose] で選択した RSA の [key length] が 2048 より大きいと、一部の電話モデルが登録に失敗する場合があります。Cisco Unified Reporting Tool（CURT）の [Unified CM Phone Feature List Report] で、3072/4096 RSA キー サイズ サポート機能をサポートする電話モデルの一覧を確認できます。
[Hash Algorithm]	楕円曲線のキー長と同じ強さのハッシュ アルゴリズムになるように、値を [Hash Algorithm] ドロップダウン ボックスから選択します。[Hash Algorithm] ドロップダウン ボックスから、値を 1 つ選択します。 （注） • [Key Length] フィールドで選択した値に基づいて [Hash Algorithm] フィールドの値は変化します。 • システムが FIPS モードで実行されている場合は、必ずハッシュアルゴリズムとして SHA256 を選択する必要があります。

連携動作と制限事項

- **TLS_ECDHE_ECDSA_WITH_AES256_SHA384**および TLS_ECDHE_ECDSA_WITH_AES128_SHA256 をサポートしない SIP デバイスは、引き続き TLS_ECDHE_RSA_WITH_AES_256_SHA384 、**TLS_ECDHE_RSA_WITH_AES_128_SHA256**、または **AES128_SHA** に接続できます。これらのオプションは、選択した TLS 暗号オプションによって異なります。[ECDSA only]

オプションを選択すると、ECDSA 暗号化をサポートしないデバイスは SIP インターフェイスへの TLS 接続を確立できません。[ECDSA only] オプションを選択すると、このパラメータの値は **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** および **TLS_ECDHE_ECDSA_WITH_AES256_SHA384** になります。

- CTI Manager のセキュア クライアントは、**TLS_ECDHE_RSA_WITH_AES_128_SHA256**、**TLS_ECDHE_RSA_WITH_AES_256_SHA384**、**TLS_ECDHE_ECDSA_WITH_AES_128_SHA256**、および **TLS_ECDHE_ECDSA_WITH_AES_256_SHA384** をサポートしていません。ただし、**AES128_SHA** を使用して接続できます。

ITL ファイルの一括リセットの実行

Unified Communications Manager クラスタのデバイスがロックされて、信頼のステータスを失った場合は、CLI コマンド **utils itl reset** を使用してアイデンティティ信頼リスト（ITL）ファイルの一括リセットを行います。このコマンドにより、新しい ITL リカバリ ファイルが生成されます。

ヒント Unified Communications Manager の新規インストールを実行した場合は、できるだけ早く ITL キーをエクスポートし、ディザスタ リカバリ システムによるバックアップを行います。

ITL リカバリ ペアをエクスポートする CLI コマンドは次のとおりです。

file get tftp *ITLRecovery.p12*

（キーのエクスポート先となる）SFTP サーバとパスワードの入力を求めるプロンプトが表示されます。

始める前に

この手順は必ず Unified Communications Manager パブリッシャで実行してください。必要に応じて、パブリッシャからキーをエクスポートします。

手順

ステップ 1 次のいずれかの手順を実行します。

- **utils itl reset localkey**の実行
- **utils itl reset remotekey**の実行

（注） **utils itl reset localkey**では、ローカルキーはパブリッシャ側にあります。このコマンドを発行しているとき、ITL回復キーをリセットしている間、ITLファイルはCallManagerキーによって一時的に署名されます。

ステップ 2 リセットが正常に行われたことを確認するには **show itl** を実行します。

ステップ 3 [Unified Communications Manager Administration] で、**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

ステップ 4 [リセット（Reset）] をクリックします。

デバイスが再起動されます。これで、CallManager キーで署名された ITL ファイルをダウンロードし、設定ファイルを受け入れる準備が整いました。

ステップ 5 TFTP サービスを再起動し、すべてのデバイスを再起動します。

（注） TFTP サービスを再起動すると、ITL ファイルが ITLRecovery キーによって署名され、ステップ 1 の変更がロールバックされます。

デバイスは ITLRecovery キーで署名されている ITL ファイルをダウンロードし、Unified Communications Manager に正しく再登録します。

ITLRecovery 証明書の有効期間の表示

手順

ステップ 1 [Cisco Unified OS Administration] から、**[Security] > [Certificate Management]** を選択します。[Certificate List] ウィンドウが表示されます。

ステップ 2 検索パラメータを入力して、証明書を検索して設定の詳細を表示します。
すべての条件に一致したレコードが [Certificate List] ウィンドウに表示されます。

ステップ 3 [ITLRecovery] リンクをクリックして、有効期間を確認します。

ステップ 4 [OK] をクリックします。

連絡先検索の認証設定タスク フロー

Unified Communications Manager で連絡先検索の認証をセットアップするには、次のタスクを実行します。この機能が設定されている場合、ユーザはディレクトリで他のユーザを検索する前にユーザ自身を認証する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	連絡先検索の認証の電話サポートの確認（29 ページ）	電話でこの機能がサポートされていることを確認します。Cisco Unified Reporting

	コマンドまたはアクション	目的
		で [Unified CM Phone Feature List] レポートを実行し、この機能をサポートしている電話モデルのリストを確認します。
ステップ 2	連絡先検索の認証の有効化 （29 ページ）	Unified Communications Manager で連絡先検索の認証を設定します。
ステップ 3	連絡先検索用のセキュアなディレクトリサーバの設定 （30 ページ）	電話のユーザがディレクトリで他のユーザを検索したときに示される URL を Unified Communications Manager で設定するには、次の手順を実行します。

連絡先検索の認証の電話サポートの確認

導入環境内の電話が連絡先検索の認証をサポートしていることを確認します。[Phone Feature List] レポートを実行して、この機能をサポートしているすべての電話モデルのリストを取得します。

手順

ステップ 1 Cisco Unified Reporting から [システム レポート(System Reports)] をクリックします。
ステップ 2 [ユニファイド CM 電話機能 (Unified CM Phone Feature)] を選択します。
ステップ 3 [ユニファイド CM 電話機能 (Unified CM Phone Feature)] レポートをクリックします。
ステップ 4 [製品 (Product)] フィールドはデフォルト値のままにします。
ステップ 5 [機能 (Feature)] ドロップダウンから [Authenticated Contact Search] を選択します。
ステップ 6 [Submit] をクリックします。`

次のタスク

連絡先検索の認証の有効化 （29 ページ）

連絡先検索の認証の有効化

電話ユーザの連絡先検索の認証を設定するには、Unified Communications Manager でこの手順に従います。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils contactsearchauthentication status** コマンドを実行し、このノードの連絡先検索の認証の設定を確認します。

ステップ 3 連絡先検索の認証の設定が必要な場合、

- 認証を有効にするには、**utils contactsearchauthentication enable** コマンドを実行します。
- 認証を無効にするには、**utils contactsearchauthentication disable** コマンドを実行します。

ステップ 4 すべての Unified Communications Manager クラスタ ノードでこの手順を繰り返します。

（注） 変更を有効にするには、電話をリセットする必要があります。

次のタスク

連絡先検索用のセキュアなディレクトリ サーバの設定 （30 ページ）

連絡先検索用のセキュアなディレクトリ サーバの設定

UDS がユーザ検索リクエストを送信するディレクトリ サーバ URL を Unified Communications Manager に設定するには、次の手順を使用します。デフォルトの値は `https://<cucm-fqdn-or-ip>:port/cucm-uds/users` です。

（注） デフォルトの UDS ポートは 8443 です。連絡先検索の認証が有効になると、デフォルトの UDS ポートは 9443 に切り替わります。その後、連絡先検索の認証を無効にした場合は、UDS ポートを手動で 8443 に戻す必要があります。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム(System)]** > **[Enterprise Parameters]** の順に選択します。

ステップ 2 [Secure Contact Search URL] テキスト ボックスに、セキュアな UDS ディレクトリ要求の URL を入力します。

（注） URL には、Cisco TFTP サービスを実行していないノードを選択することを推奨します。Cisco TFTP と UDS サービスのいずれかのサービスが再起動すると、互いに悪影響が及ぶ可能性があります。

ステップ 3 **[保存 (Save)]** をクリックします。