デフォルトのセキュリティ

デフォルトのセキュリティの概要

デフォルトのセキュリティ機能は、追加の設定要件なしでサポートされる Cisco Unified IP Phone の基本的なレベルのセキュリティを提供します。

この機能は、サポートされる IP 電話機に対して次のデフォルトのセキュリティを提供します。

- TFTP のデフォルト認証
- オプションの暗号化
- 証明書の検証

デフォルトのセキュリティは、次のコンポーネントを使用して非セキュアな環境で基本的なセキュリティを提供します。

- アイデンティティ信頼リスト（ITL）：このファイルは、クラスタのインストール時に TFTP サービスがアクティブ化された後、信頼の確立のために Cisco Unified IP Phone により使用されます。
- 信頼検証サービス：このサービスは、すべての Unified Communications Manager ノードで実行され、Cisco Unified IP Phone の証明書を認証します。TVS 証明書と他のいくつかのキー証明書が ITL ファイルにバンドルされます。

初期信頼リスト

初期信頼リスト（ITL）ファイルは、エンドポイントが Unified Communications Manager を信頼できるよう、最初のセキュリティに使用されます。ITL は明示的に有効にするセキュリティ機能を必要としません。ITL ファイルは、TFTP サービスがアクティブになり、クラスタがインストールされると自動的に作成されます。Unified Communications Manager の TFTP サーバの秘密キーは、ITL ファイルの署名に使用されます。

Unified Communications Manager クラスタまたはサーバが非セキュアモードの場合、ITL ファイルはサポートされている Cisco Unified IP Phone ごとにダウンロードされます。CLI コマンド **admin:show itl** を使用して、ITL ファイルの内容を表示できます。

Cisco Unified IP Phone は、次のタスクを実行するために ITL ファイルが必要です。

- 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。
- 設定ファイルの署名を認証する。
- 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。

Note 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。

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、これはより小さく、スリムのバージョンです。

ITL ファイルには次の属性が適用されます。

- TFTP サービスがアクティブ化され、クラスタをインストールすると、システムによって ITL ファイルが自動的に作成されます。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。
- リセット中、再起動中、または CTL ファイルのダウンロード後に、Cisco Unified IP Phone は ITL ファイルをダウンロードします。

ITL ファイルには次の証明書が含まれています。

- ITLRecovery 証明書：この証明書は ITL ファイルに署名します。
- TFTP サーバの CallManager 証明書：この証明書を使用すると、ITL ファイル署名と電話機設定ファイル署名を認証できます。
- クラスタ上で使用可能なすべての TVS 証明書：これらの証明書を使用すると、電話機は TVS と安全に通信し、証明書認証を要求できます。

- CAPF 証明書: これらの証明書は、コンフィギュレーションファイルの暗号化をサポートします。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 によるルックアップ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。

信頼検証サービス

ネットワーク内に多数の電話機があり、Cisco Unified IP Phone のメモリも限られています。したがって、Unified Communications Manager は TVS を介してリモート信頼ストアとして動作するため、各電話機に証明書信頼ストアを配置する必要はありません。Cisco Unified IP Phone は CTL ファイルまたは ITL ファイルを使用して署名または証明書を検証できないため、検証のために TVS サーバに問い合わせることもできます。したがって、中央信頼ストアを持つことは、信頼ストアをすべての Cisco Unified IP Phone に持つよりも管理が簡単です。

TVS を使用すると、HTTPS を確立しているときに、Cisco Unified IP Phone で EM サービス、ディレクトリ、および MIDlet などのアプリケーションサーバを認証できます。

TV には、次の機能があります。

- 拡張性：Cisco Unified IP Phone のリソースは、信頼する証明書の数に影響されません。
- 柔軟性: 信頼証明書の追加または削除は、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。

Note 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 ファイルを作成してから、クラスタを混合モードに設定する必要があります。CTL ファイルを作成し、クラスタを混合モードに設定するには、CLI コマンド **utils ctl set-cluster mixed-mode** を使用します。

TVS を説明する基本的な概念を次に示します。

- TVS は、Unified Communications Manager サーバ 上で実行され、Cisco IP 電話に代わって証明書を認証します。
- Cisco Unified IP Phone は、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、TVS を信頼する必要があるだけです。
- 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 Unified IP Phone によりダウンロードされ、信頼はそこからフローします。

デフォルトのセキュリティ管理タスク

デフォルトのセキュリティ管理タスクを以下に示します。

Procedure

	Command or Action	Purpose
Step 1	デフォルトでのセキュリティのエンドポイントサポートの取得	Cisco Unified Reporting ページを使用して Cisco Unified IP Phone のサポートリストを取得します。
Step 2	ITL ファイルの一括リセットの実行	ITL ファイルの一括リセットの実行
Step 3	ITLRecovery 証明書の有効期間の表示	ITLRecovery 証明書の有効期間を表示します。
Step 4	ITLRecovery 証明書の有効期間の表示	CLI コマンドを使用して ITL ファイルを表示します。

Cisco ユニファイド 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を使用している Unified Communication Manager との集中型 TFTP では、TFTP 設定ファイルは検証されません。

リモートクラスタからの電話機が集中型 TFTP 展開に追加される前に、次の手順を実行します。

Procedure

Step 1 中央 TFTP サーバで、Enterprise パラメータ**Prepare cluster for PRE CM-8.0 rollback**を有効にします。

Step 2 TVS および TFTP を再起動します。

Step 3 すべての電話機をリセットして、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ていることを確認します。

Step 4 HTTPS ではなく HTTP を使用するように、エンタープライズパラメータセキュア https Url を設定します。

Note Unified Communications Manager のリリース 10.5 以降では、Prepare Cluster for Rollback to pre-8.0 エンタープライ 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 バージョンと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 より前のリリースへのクラスタのロールバック」セクションを参照してください。

デフォルトでのセキュリティのエンドポイントサポートの取得

Cisco Unified Reporting ツールを使用して、デフォルトでセキュリティをサポートするシスコエンドポイントのリストを生成します。

Procedure

Step 1 [Cisco Unified Reporting] から [システムレポート（System Reports）] をクリックします。

Step 2 [システムレポート（System Reports）] リストで、[Unified CM 電話機能一覧（Unified CM Phone Feature List）] をクリックします。

Step 3 **[製品（Product）]** ドロップダウンリストから、**[デフォルトのセキュリティ（Security By Default）]** を選択します。

Step 4 [送信（Submit）] をクリックします。
特定の電話でサポートされている機能のリストを含むレポートが生成されます。

自動登録

システムは混合モードと非セキュアモードの両方で自動登録をサポートします。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。

8.0 より前のリリースへのクラスタのロールバック

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。

Procedure

Step 1 Unified Communications Manager Administration から、次を選択します。 **[システム（System）]** > **[エンタープライズ パラメータの設定（Enterprise Parameters Configuration）]**.

[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。

Note クラスタを Unified Communications Manager の 8.0 リリース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。

Step 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。

Step 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。

Step 4 クラスタが以前のバージョンへの切り替えを完了するまで待ちます。

Step 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) のすべての通常リリース
  - 007.001 (002.32016.001) より前の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) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の713のすべての ES リリース

Note 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。

Step 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。

通常の **[デバイス（Device）] > [デバイス設定（Device Settings）] > [電話サービス（Phone Services）] > [社内ディレクトリ（Corporate Directory）]** サービス URL を「Application:Cisco/CorporateDirectory」から「http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp」に変更します

Step 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。

通常の **[デバイス（Device）] > [デバイス設定（Device Settings）] > [電話サービス（Phone Services）] > [パーソナル ディレクトリ（Personal Directory）]** サービス URL を

「Application:Cisco/PersonalDirectory」から
「http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=undefined」に変更する必要があります。

復帰後のリリース8.6 以降へのスイッチバック

クラスタをリリース7.x に戻した後にリリース8.6 またはそれ以降のパーティションに切り替える場合は、次の手順に従います。

Procedure

Step 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。

Step 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) のすべての通常リリース
- 007.001 (002.32016.001) より前の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) より前の713のすべての通常リリース = 7.1 (3a) su1a
  - 007.001 (003.21005.001) より前の713のすべての ES リリース

Note 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。

Step 3 Unified Communications Manager Administration から、次を選択します。**[システム（System）]>[エンタープライズ パラメータの設定（Enterprise Parameters Configuration）]**.

[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。

Step 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。

ITL ファイルの一括リセットの実行

この手順を実行できるのは、Unified Communications Manager パブリッシャのみからであることを確認してください。

電話機が ITL ファイル 署名者を信頼できなくなり、かつ TFTP サービスによってローカルに提供された ITL ファイルを認証できないか、TVS を使用して認証できない場合は、ITL ファイルの一括リセットが実行されます。

一括リセットを実行するには、CLI コマンド **utils itl reset** を使用します。このコマンドは新しい ITL リカバリファイルを生成し、電話機と CUCM の TFTP サービス間の信頼を再確立します。

Tip Unified Communications Manager をインストールする場合は、CLI コマンド **file get tftp** *ITLRecovery.p12* を使用して ITL リカバリペアをエクスポートしてから、DR を介してバックアップを実行します。（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も表示されます。

Procedure

Step 1 次のいずれかの手順を実行します。

- **utils itl reset localkey** を実行します。
- **utils itl reset remotekey** を実行します。

Note **utils itl reset localkey** の場合、ローカルキーはパブリッシャにあります。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。

Step 2 **show itl** を実行してリセットが正常に行われたことを確認します。

Step 3 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]**。

Step 4 [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。

Step 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。

Note 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 キーで署名された 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。

CTL ローカルキーのリセット

Unified Communications Manager クラスタ上のデバイスがロックされ、信頼されたステータスが失われる場合は、CLI コマンド **ctl reset localkey** を使用して Cisco Trust List（CTL）ファイルのリセットを実行します。このコマンドにより、新しい CTL ファイルが生成されます。

Procedure

Step 1 **utils ctl reset localkey** の実行

Note **utils ctl 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すると、CTL ファイルは ITLRecovery キーによって一時的に署名されます。

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

Step 3 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]**。
[エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ページが表示されます。

Step 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 CTL 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。

Step 5 **utils ctl update CTLFile** を実行して、ステップ 1 の変更をロールバックする必要なサービスを再起動します。

デバイスが再起動されます。これで、ITLRecovery キーで署名された CTL 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。

デバイスは、必要なキーを使用して署名された CTL ファイルをダウンロードし、Unified Communications Manager に再度正しく登録します。

ITLRecovery 証明書の有効期間の表示

ITLRecovery 証明書は電話機での有効期間が長いです。[証明書ファイルデータ（Certificate File Data）] ペインに移動し、有効期間または他の ITLRecovery 証明書の詳細を表示できます。

Procedure

Step 1 [Cisco Unified OSの管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**。

Step 2 証明書を検索し、設定の詳細を表示するには、必要な検索パラメータを入力します。
条件に一致する証明書のリストが [証明書リスト（Certificate List）] ページに表示されます。

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

ITLRecovery 証明書の詳細が [証明書ファイルデータ（Certificate File Data）] ペインに表示 されます。

有効期間は現在の年から 20 年です。