暗号化された電話設定ファイルの設定

この章では、暗号化された電話設定ファイルの設定について説明します。セキュリティ関連の設定後、電話設定ファイルにはダイジェスト パスワードや電話管理者のパスワードなどの機密情報が含まれるようになります。設定ファイルのプライバシーを確保するには、設定ファイルに暗号化を設定する必要があります。

電話設定ファイルの暗号化について

Cisco Unified Communications Manager からのダウンロードで、ダイジェスト クレデンシャルとパスワードが確実に暗号化されて送受信されるよう、[Phone Security Profile Configuration] ウィンドウで [TFTP Encrypted Config] オプションを有効にし、[Cisco Unified Communications Manager Administration] でいくつかのタスクを実行する必要があります。

[TFTP Encrypted Config] オプションを有効にした後、[Cisco Unified Communications Manager Administration] と電話で必要なパラメータを設定し、Cisco Unified Serviceability の必要なサービスを再起動すると、TFTP サーバにより次の操作が実行されます。

1. ディスク上のクリア テキストの設定ファイルをすべて削除
2. 設定ファイルの暗号化バージョンの生成

電話が暗号化された電話設定ファイルをサポートしており、電話設定ファイルの暗号化に必要なタスクを行った場合は、電話は暗号化バージョンの設定ファイルを要求します。

警告 TFTP 暗号化設定が False であるが、SIP を実行している電話でダイジェスト認証が True に設定されている場合、ダイジェスト クレデンシャルがクリア テキストで送信される可能性があります。

一部の電話は、暗号化された電話設定ファイルをサポートしていません。電話のモデルとプロトコルによって、設定ファイルの暗号化方法が決定します。サポートされる方式は、Cisco Unified Communications Manager の機能と暗号化設定ファイルをサポートするファームウェア ロードに依存します。電話のファームウェア ロードを、暗号化に対応していないバージョンにまでダウングレードすると、TFTP サーバは最低限の設定を行う平文の設定ファイルを送ります。この場合、電話が期待された機能を発揮できないことがあります。

キー情報のプライバシーを確実に維持できるように、暗号化された電話機設定ファイルに関連するタスクをセキュアな環境で実行することが強く推奨されます。

Cisco Unified Communications Manager は次の方式をサポートしています。

- 手動キー配布
- 電話の公開キーによる対称キー暗号化

手動キー配布と電話の公開キーによる対称キー暗号化のための設定情報は、混合モードが設定済みで、[Cisco Unified Communications Manager Administration] の [TFTP Encrypted Config] パラメータが有効になっていることを前提としています。

関連トピック

手動キー配布, （2 ページ）
電話の公開キーによる対称キーの暗号化, （3 ページ）
電話モデルのサポート
電話の設定ファイルの暗号化の無効化, （16 ページ）

手動キー配布

手動キー配布を使用すると、電話リセット後に、Cisco Unified Communications Manager データベースに保存された 128 ビットまたは 256 ビットの対称キーを使用して電話設定ファイルが暗号化されます。電話モデルのキー サイズを判別する。

設定ファイルを暗号化するために、管理者はキーを手動で入力することも、Cisco Unified Communications Manager に [Phone Configuration] ウィンドウで生成させることもできます。データベースにキーが存在するようになった後、管理者またはユーザは電話のユーザ インターフェイスにアクセスしてキーを電話に入力する必要があります。[Accept] ソフトキーを押すと、電話はすぐにキーをフラッシュに保存します。キーの入力以降、電話はリセット後に暗号化された設定ファイルを要求します。必要なタスクが実行された後、RC4 または AES 128 暗号化アルゴリズムを使

用して、対称キーにより設定ファイルが暗号化されます。どの電話が RC4 と AES 128 暗号化アルゴリズムを使用するかを判別する。

電話に対称キーが含まれる場合、その電話は暗号化された設定ファイルを常に要求します。Cisco Unified Communications Manager によって、TFTP サーバによって署名された暗号化設定ファイルが電話にダウンロードされます。すべての電話タイプで設定ファイルの署名者が検証されるわけではありません。

電話はフラッシュに保存された対称キーを使用して、ファイルの内容を復号します。復号に失敗すると、設定ファイルが電話に適用されません。

ヒント [TFTP Encrypted Config] の設定が無効にされた場合、管理者は電話の GUI で対称キーを削除する必要があります。これにより、次回リセットされたときに電話が暗号化されていない設定ファイルを要求します。

関連トピック

電話モデルのサポート

電話の公開キーによる対称キーの暗号化

製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話に含まれている場合、電話には公開キーと秘密キーのペアが含まれ、これらのキーは PKI 暗号化に使用されます。

この方法を初めて使用する場合、電話は設定ファイルにある電話の証明書の MD5 ハッシュと LSC または MIC の MD5 ハッシュとを比較します。電話で問題が特定されない場合、電話はリセット後に暗号化された設定ファイルを TFTP サーバに要求します。電話が問題を特定した場合、たとえばハッシュが一致しない、電話に証明書がない、MD5 値がブランクであるなどの場合、電話は CAPF 認証モードが [By Authentication String] に設定されていない限り、CAPF とのセッションを開始しようとします（[By Authentication String] に設定されている場合は文字列の手動入力が必要です）。Certificate Authority Proxy Function（CAPF）は Cisco Unified IP Phone を Cisco Unified Communications Manager に対して認証し、電話の証明書（LSC）を発行します。CAPF は、LSC または MIC から電話の公開キーを抽出し、MD5 ハッシュを生成し、Cisco Unified Communications Manager データベースに公開キーの値および証明書ハッシュを保存します。公開キーがデータベースに格納された後、電話はリセットされ、新しい設定ファイルが要求されます。

公開キーがデータベースに保存され電話がリセットされた後、データベースが TFTP に電話の公開キーが存在することを通知すると、対称キー暗号化プロセスが開始されます。TFTP サーバは 128 ビット対称キーを生成します。これにより、Advanced Encryption Standard（AES）128 暗号化アルゴリズムで設定ファイルが暗号化されます。次に、電話の公開キーで対称キーが暗号化され、設定ファイルの署名付きエンベロープ ヘッダーに含まれます。電話はファイルの署名を確認し、署名が有効であれば、電話は LSC または MIC の秘密キーを使用して暗号化された対称キーを復号化します。次に、対称キーによってファイルの内容が復号化されます。

設定ファイルを更新するたびに、TFTP サーバは自動的にファイルを暗号化するための新しいキーを生成します。

ヒント　この暗号化方式をサポートする電話では、設定ファイルの暗号化設定フラグを使用して、暗号化ファイルを要求するかまたは非暗号化ファイルを要求するかを判断します。[TFTP Encrypted Config] 設定が無効な場合に、この暗号化方式をサポートする Cisco Unified IP Phone が暗号化ファイル（.enc.sgn file）を要求すると、Cisco Unified Communications Manager は [file not found error] エラーを電話に送信します。次に、電話は暗号化されていない署名付きファイル（.sgn ファイル）を要求します。

[TFTP Encrypted Config] 設定が有効な場合に、電話が何らかの理由で暗号化されていない設定ファイルを要求すると、TFTP サーバは最小限の設定を含む暗号化されていないファイルを提供します。電話は最小限の設定を受信した後、キーの不一致などのエラー状態を検出でき、CAPF でセッションを開始して電話の公開キーと Cisco Unified Communications Manager データベースを同期できます。エラー条件が解決されると、電話は次回リセットされるときに暗号化された設定ファイルを要求します。

関連トピック

Certificate Authority Proxy Function について
電話モデルのサポート

AES 256 Encryption Support for TLS and SIP SRTP

Cisco Collaboration ソリューションは、Transport Layer Security（TLS）および Secure Real-time Transport Protocol（SRTP）を使用し、シグナリングとメディア暗号化を行います。現在、暗号化アルゴリズムとして、128 ビットの暗号キーを使用した Advanced Encryption Standard（AES）が使用されています。AES では、認証方式として Hash-based Message Authentication Code Secure Hash Algorithm-1（HMAC-SHA-1）も使用されます。これらのアルゴリズムは、変化していく不可欠なセキュリティとパフォーマンスのニーズを満たすために有効に拡張できません。セキュリティとパフォーマンスの要件の増大に対応するため、Next-Generation Encryption（NGE）での、暗号化、認証、デジタル署名、およびキー交換用のアルゴリズムとプロトコルが開発されています。また、AES 128 の代わりに、AES 256 暗号化のサポートが、NGE をサポートする TLS and Session Initiation Protocol（SIP）SRTP に提供されています。

Cisco Unified Communications Manager リリース 10.5(2) では、AES 256 Encryption Support for TLS and SIP SRTP が、シグナリング暗号化とメディア暗号化での AES 256 暗号化のサポートに重点を置くために拡張されています。この機能は、Cisco Unified Communications Manager 上で実行されているアプリケーションが、SHA-2（Secure Hash Algorithm）標準規格および Federal Information Processing Standards（FIPS）に準拠する、AES-256 ベースの暗号を使用して TLS 1.2 接続を開始してサポートするために役立ちます。

この機能には、次の要件があります。

- SIP トランクおよび SIP 回線が開始する接続であること。
- Cisco Unified Communications Manager が SIP 回線と SIP トランクを通じた SRTP コール用にサポートする暗号化であること。

TLS での AES 256 および SHA-2 のサポート

Transport Layer Security（TLS）プロトコルでは、2つのアプリケーション間の通信の認証、データの整合性、および機密性が提供されます。TLS 1.2 はセキュア ソケット レイヤ（SSL）プロトコル バージョン 3.0 をベースにしていますが、これら 2 つのプロトコルに相互の互換性はありません。TLS はクライアント/サーバ モードで動作し、一方がサーバとして機能し、もう一方がクライアントとして機能します。SSL は Transmission Control Protocol（TCP）層とアプリケーション間のプロトコル層として位置付けられ、各クライアントとサーバ間にセキュアな接続を形成して、それらがネットワークを通じて安全に通信できるようにします。TLS が動作するためには、信頼性の高いトランスポート層プロトコルとして TCP が必要です。

Cisco Unified Communications Manager リリース 10.5(2) における、TLS 1.2 での AES 256 および SHA-2（Secure Hash Algorithm-2）のサポートは、SIP トランクおよび SIP 回線によって開始される接続を処理するための機能強化です。AES 256 および SHA-2 に準拠する、サポートされる暗号方式は次のとおりです。

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256：暗号ストリングは ECDH-RSA-AES128-GCM-SHA256 です。
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384：暗号ストリングは ECDH-RSA-AES256-GCM-SHA384 です。

値は次のとおりです。

- TLS は、Transport Layer Security です
- ECDH は、アルゴリズムの楕円曲線 Diffie-Hellman です
- RSA は、アルゴリズムの Rivest Shamir Adleman です
- AES は、Advanced Encryption Standards です
- GCM は、Galois/Counter Mode です

新しくサポートされた暗号方式に加えて、Cisco Unified Communications Manager リリース 10.5(2) では、TLS_RSA_WITH_AES_128_CBC_SHA が引き続きサポートされています。この暗号方式の暗号ストリングは AES128-SHA です。

（注）
- Cisco Unified Communications Manager の証明書は、RSA に基づいています。
- Cisco Unified Communications Manager 10.5(2) では、シスコの各エンドポイント（各電話）で、上記の TLS 1.2 用の新しい暗号方式はサポートされません。
- Cisco Unified Communications Manager 10.5(2) において TLS 1.2 での AES 256 および SHA-2（Secure Hash Algorithm-2）のサポート機能強化を使用すると、Certificate Authority Proxy Function（CAPF）のデフォルトのキー サイズが 2048 ビットに増えます。

SRTP SIP コール シグナリングでの AES 256 のサポート

Secure Real-Time Transport Protocol（SRTP）では、Real-time Transport Protocol（RTP）の音声メディアとビデオ メディアの両方と、それらに付随する Real-time Transport Control Protocol（RTCP）ストリームに対して機密性およびデータの整合性を提供する方法を定義します。SRTP では、暗号化とメッセージ認証ヘッダーを使用して、この方法を実装します。SRTP では、暗号化は RTP パケットのペイロードだけに適用され、RTP のヘッダーには適用されません。ただし、メッセージ認証は RTP のヘッダーと RTP のペイロードの両方に適用されます。また、メッセージ認証がヘッダー内の RTP のシーケンス番号に適用されるため、SRTP ではリプレイ アタックに対する保護も間接的に提供されます。SRTP は、暗号化方法として 128 ビットの暗号キーによる Advanced Encryption Standard（AES）を使用します。また、認証方式として、Hash-based Message Authentication Code Secure Hash Algorithm-1（HMAC-SHA-1）も使用します。

Cisco Unified Communications Manager 10.5(2) では、SIP 回線と SIP トランクを通じた SRTP コール用の暗号方式がサポートされます。これらの暗号方式は、AEAD_AES_256_GCM と AEAD_AES_128_GCM で、AEAD は Authenticated-Encryption with Associated-Data、GCM は Galois/Counter Mode です。これらの暗号方式は GCM に基づいています。これらの暗号方式が Session Description Protocol（SDP）内に存在する場合、AES 128 ベースの暗号方式および SHA-1 ベースの暗号方式に比べてより高い優先順位で処理されます。シスコの各エンドポイント（電話）では、Cisco Unified Communications Manager 10.5(2) に SRTP のために追加した、これらの新しい暗号方式はサポートされません。

新たにサポートされる暗号方式に加えて、Cisco Unified Communications Manager 10.5(2) では次の暗号方式が引き続きサポートされます。

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 暗号化は、次のコールでサポートされます。

- SIP 回線から SIP 回線へのコール シグナリング
- SIP 回線から SIP トランクへのシグナリング
- SIP トランクから SIP トランクへのシグナリング

Cisco Unified Communications Manager の要件

- SIP トランクと SIP 回線接続について TLS バージョン 1.2 がサポートされました。
- 暗号のサポート：TLS 1.2 接続時に、TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（暗号ストリング ECDHE-RSA-AES256-GCM-SHA384）および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（暗号ストリング ECDHE-RSA-AES128-GCM-SHA256）が利用可能です。これらの暗号方式は GCM に基づいており、SHA-2 カテゴリに準拠しています。

- Cisco Unified Communications Manager は TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 暗号方式と TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 暗号方式を使用して TLS 1.2 を開始します。ピアが TLS 1.2 をサポートしていない場合、Cisco Unified Communications Manager は既存の AES128-SHA 暗号方式を使用した TLS 1.0 にフォールバックします。
- SIP 回線と SIP トランクを介した SRTP コールでは、GCM ベースの AEAD_AES_256_GCM 暗号方式と AEAD_AES_128_GCM 暗号方式がサポートされます。

連携動作と制限事項

- Cisco Unified Communications Manager の要件は、SIP 回線と SIP トランク、および基本的な SIP 間コールのみに適用されます。
- 非 SIP プロトコルに基づくデバイス タイプでは、これまでのサポートされていた暗号による TLS バージョン使用時の動作が引き続きサポートされます。Skinny Call Control Protocol（SCCP）では、これまでにサポートされていた暗号による TLS 1.2 もサポートされています。
- SIP から非 SIP へのコールでは、引き続き AES 128 および SHA-1 ベースの暗号が使用されます。

暗号化された設定ファイルをサポートする電話モデル

以下の Cisco Unified IP Phone では電話の設定ファイルを暗号化できます。

電話モデルとプロトコル	暗号化方式
Cisco Unified IP Phone 7905G または 7912G（SIP のみ）	手動キー配布：暗号化アルゴリズム：RC4 キーサイズ：256 ビット ファイル署名のサポート：いいえ
Cisco Unified IP Phone 7940G または 7960G（SIP のみ）	手動キー配布：暗号化アルゴリズム：Advanced Encryption Standard（AES）128 キーサイズ：128 ビット ファイル署名のサポート：SIP を実行するこれらの電話は、署名付きで暗号化された設定ファイルを受信しますが、署名情報を無視します。

電話モデルとプロトコル	暗号化方式
Cisco Unified IP Phone 6901、6911、6921、6941、6945、および 6961 Cisco Unified IP Phone 7970G、7971G、または 7975G。 Cisco Unified IP Phone 7961G、7962G、または 7965G。Cisco Unified IP Phone 7941G、7942G、または 7945G。Cisco Unified IP Phone 7911G。 Cisco Unified IP Phone 7906G Cisco Unified IP Phone 7971G-GE、7961G-GE、7941G-GE Cisco Unified IP Phone 7931G、7921G、7925G、7926G（SCCP のみ） Cisco Unified IP Phone 8941 および 8945 Cisco Unified IP Phone 8961、9951、および 9971	電話の公開キーによる対称キーの暗号化（PKI 暗号化）：暗号化アルゴリズム：AES 128 キーサイズ：128 ビット ファイル署名のサポート：はい （注） Cisco Unified IP Phone 6901 および 6911 はデフォルトでセキュリティをサポートしていないため、ITL ファイルを要求しません。したがって、暗号化された設定ファイルが Cisco IP Phone（6901 および 6911）で動作するための Cisco Certificate Authority Proxy Function（CAPF）の詳細を含む Cisco CTL ファイルを取得するため、Cisco Unified Communications Manager クラスタは、Cisco Unified IP Phone（6901 と 6911）ではセキュア（混合）モードに設定する必要があります。

暗号化された設定ファイルの設定のヒント

[TFTP Encrypted Config] フラグを有効化して電話ダウンロードの機密データを保護できるようにすることが推奨されます。電話に PKI 機能がない場合、[Cisco Unified Communications Manager Administration] と電話で対称キーを設定する必要があります。電話と Cisco Unified Communications Manager のいずれかに対称キーが存在しない場合、または [TFTP Encrypted Config] フラグが設定されている場合に不一致が発生した場合、その電話は登録できません。

[Cisco Unified Communications Manager Administration] で暗号化された設定ファイルを設定する場合、以下の情報を検討してください。

- 暗号化された設定ファイルをサポートする電話でのみ、セキュリティ プロファイルに [TFTP Encrypted Config] フラグが表示されます。Cisco Unified IP Phone 7905G、7912G、7940G、7960G（SCCP のみ）には暗号化された設定ファイルを設定できません。これらの電話は設定ファイルのダウンロード時に機密データを受信しないためです。
- [TFTP Encrypted Config] のデフォルト設定は False です（オフ）。デフォルトの非セキュア プロファイルを電話に適用する場合、ダイジェスト クレデンシャルとセキュア パスワードはクリア テキストで送信されます。
- 公開キー暗号化を使用する Cisco Unified IP Phone の場合、暗号化された設定ファイルを有効化するためにデバイス セキュリティ モードを認証済みまたは暗号化済みにすることを Cisco Unified Communications Manager が要求することはありません。Cisco Unified Communications Manager では、登録の間の公開キーのダウンロードに CAPF プロセスが使用されます。

- 環境がセキュアであるとわかっている場合、またはPKIが有効でない電話への対称キーの手動設定を避けるために、非暗号化設定ファイルを電話にダウンロードすることを選択することも可能です。ただし、シスコではこの方法を推奨していません。
- Cisco Unified IP Phone 7905G、7912G、7940G、7960G（SIP のみ）の場合、[Cisco Unified Communications Manager Administration] では電話へのダイジェスト クレデンシャルを送信することができますが、この方法では暗号化された設定ファイルの使用に比べて使いやすいものの安全性は低くなります。[Exclude Digest Credentials in Configuration File] 設定を使用するこの方法は、最初に対称キーを設定して電話に入力する必要がないため、ダイジェストクレデンシャルの初期化に役立ちます。

この方法の場合、ダイジェスト クレデンシャルは暗号化されていない設定ファイルで電話に送られます。電話にクレデンシャルが存在するようになった後には、TFTPファイル暗号化設定を無効のままにし、対応するセキュリティ プロファイル ウィンドウの [Exclude Digest Credentials in Configuration File] フラグを有効化することで、その後のダウンロードからダイジェスト クレデンシャルを除外することを推奨します。

ダイジェストクレデンシャルが電話に存在するようになり、着信ファイルにダイジェストクレデンシャルが含まれないようになると、既存のクレデンシャルがそのまま使用されます。ダイジェスト クレデンシャルは、出荷時の状態へのリセットや新規クレデンシャル（空白を含む）の受信まで、電話にそのまま残ります。

電話またはエンドユーザのダイジェスト クレデンシャルを変更する場合、対応するセキュリティ プロファイル ウィンドウの [Exclude Digest Credentials] フラグを一時的に無効化し、新しいダイジェスト クレデンシャルを電話にダウンロードします。

TFTP 暗号化の設定

TFTP 設定ファイルに暗号化を設定するには、次のタスクを実行します。

はじめる前に

- クラスタ セキュリティが混合モードである必要があります。
- クラスタの電話のうち、手動キー暗号化をサポートするものと公開キー暗号化をサポートするものを区別して確認します。
- SHA-1とSHA-512をサポートしている電話を区別して確認します。クラスタ全体でSHA-512を有効にすると、この暗号をサポートしていない電話は機能しません。

手順

	コマンドまたはアクション	目的
ステップ 1	TFTP 暗号化の有効化, （10 ページ）	使用する電話の [TFTP Configuration File] オプションを有効にします。このオプションは電話セキュリティ プロファイルで有効にできます。
ステップ 2	SHA-512 暗号化の設定, （11 ページ）	オプション。TFTP ファイル暗号化が有効になると、デフォルトの暗号化アルゴリズムとしてSHA-1が設定されます。強力な SHA-512 アルゴリズムを使用できるようシステムを更新するには、次の手順を実行します。SHA-1 を使用するには、このステップは省略できます。 （注） ご使用の電話が SHA-512 に対応していることを確認します。対応していない場合は電話が機能しません。
ステップ 3	手動キー配布の設定, （12 ページ）	手動キーを使用する電話では、手動キー配布をセットアップします。
ステップ 4	電話の対称キーの入力, （13 ページ）	手動キーを使用する電話では、Cisco Unified Communications Manager にキーを入力します。
ステップ 5	LSC または MIC 証明書のインストールの確認, （14 ページ）	公開キーを使用する電話では、証明書のインストールを確認します。
ステップ 6	CTL ファイルの更新, （15 ページ）	TFTP設定ファイルの更新が完了したら、CTL ファイルを再生成します。
ステップ 7	サービスの再起動, （15 ページ）	Cisco CallManager サービスおよび Cisco TFTP サービスを再起動します。
ステップ 8	電話のリセット, （16 ページ）	暗号化された TFTP設定ファイルの更新が完了したら、電話をリセットします。

TFTP 暗号化の有効化

TFTPサーバからダウンロードするファイルの暗号化を有効にするには、次の手順を使用します。このオプションは、特定のモデルの電話の電話セキュリティ プロファイル内で有効にできます。

手順

ステップ 1 [Cisco Unified CM Administration] で、[System] > [Security] > [Phone Security Profile] の順に選択します。

ステップ 2 [Find] をクリックし、電話セキュリティ プロファイルを選択します。

ステップ 3 [TFTP Encrypted Config] チェック ボックスをオンにします。

ステップ 4 [Save] をクリックします。

ステップ 5 クラスタで使用されている他の電話セキュリティ プロファイルについて、ここまでの手順を繰り返します。

次の作業

オプション。 SHA-512 暗号化の設定, （11 ページ）

SHA-512 暗号化の設定

SHA-1 は TFTP ファイル暗号化のデフォルトのアルゴリズムです。デジタル署名など、TFTP 設定ファイルに対してより堅牢な SHA-512 アルゴリズムを使用できるようにシステムをアップグレードするには、この手順（オプション）を使用します。

（注） ご使用の電話が SHA-512 に対応していることを確認します。対応していない場合、電話のシステムを更新すると、電話が機能しなくなります。

はじめる前に

TFTP 暗号化の有効化, （10 ページ）

手順

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

ステップ 2 [TFTP File Signature Algorithm] エンタープライズ パラメータを [SHA-512] に設定します。

ステップ 3 [Save] をクリックします。

次の作業

手動のキーを使用する電話の場合：手動キー配布の設定, （12 ページ）。

公開キーを使用する電話の場合：LSC または MIC 証明書のインストールの確認, （14 ページ）。

すでにキーを設定して確認済みの場合、 CTL ファイルの更新, （15 ページ）

手動キー配布の設定

次に述べる手順では、以下の点を前提としています。

- 電話が Cisco Unified Communications Manager データベースに存在している。
- 互換性のあるファームウェア ロードが TFTP サーバに存在している。
- [Cisco Unified Communications Manager Administration] で、[TFTP Encrypted Config] パラメータが有効にされている。

はじめる前に

使用中の電話が手動キー配布をサポートしているかの確認

手順

ステップ 1 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、電話を検索します。

ステップ 2 [Phone Configuration] ウィンドウが表示されたら、手動キー配布の設定を行います。
フィールドの説明については、手動キー配布, （2 ページ）を参照してください。

（注） この設定を行った後は、キーは変更できません。

ステップ 3 [Save] をクリックします。

ステップ 4 電話に対称キーを入力し、電話をリセットします。
これらの作業の実行方法については、使用している電話のモデルに対応する電話のアドミニストレーション ガイドを参照してください。

次の作業

電話の対称キーの入力, （13 ページ）

手動キー配布の設定

次の表に、[Phone Configuration] ウィンドウでの手動配布の設定について説明します。

表 *1*：手動キー配布の設定

設定	説明
[Symmetric Key]	対称キーに使用する16進数の文字列を入力します。有効な文字は、数字の 0～9、大文字（小文字）の A～F（または a～f）です。 キー サイズに対応した正確なビット数を入力するようにしてください。不正確な値は Cisco Unified Communications Manager に拒否されます。Cisco Unified Communications Manager では次のキー サイズがサポートされています: • Cisco Unified IP Phone 7905G および 7912G（SIP のみ）：256 ビット • Cisco Unified IP Phone 7940G および 7960G（SIP のみ）：128 ビット キー設定後は、キーを変更しないでください。
[Generate String]	[Cisco Unified Communications Manager Administration] で 16 進数文字列を生成させる場合、[Generate String] ボタンをクリックします。 キー設定後は、キーを変更しないでください。
[Revert to Database Value]	データベースに存在する値を復元するには、このボタンをクリックします。

電話の対称キーの入力

[Cisco Unified Communications Manager Administration] で手動のキー配布を設定した後で対称キーを電話に入力するには、次の手順に従います。

手順

ステップ 1 電話の [Setting] ボタンを押します。

ステップ 2 設定がロックされている場合は、[Setting] メニューをスクロールし、[Unlock Phone] を強調表示して、[Select] ソフトキーを押します。電話のパスワードを入力して [Accept] ソフトキーを押します。
電話がパスワードを受け入れます。

ステップ 3 [Setting] メニューをスクロールし、[Security Configuration] を強調表示して、[Select] ソフトキーを押します。

ステップ 4 [Security Configuration] メニューで [Set Cfg Encrypt Key] オプションを強調表示し、[Select] ソフトキーを押します。

ステップ 5 暗号キーの入力を要求されたら、キーを入力します（16 進数）。キーをクリアする必要がある場合は 32 桁のゼロを入力します。

ステップ 6 キーの入力が終了したら、[Accept] ソフトキーを押します。
電話が暗号キーを受け入れます。

ステップ 7 電話をリセットします。
電話のリセット後、電話は暗号化された設定ファイルを要求します。

次の作業

CTL ファイルの更新, （15 ページ）

LSC または MIC 証明書のインストールの確認

この手順は、PKI 暗号化を使用する Cisco Unified IP Phone に適用されます。お使いの電話が、電話の公開キーを使用する対称キー暗号化方式（PKI 暗号化）をサポートするかを確認するには、暗号化された設定ファイルをサポートする電話モデル, （7 ページ）を参照してください。

次の手順は、電話が Cisco Unified Communications Manager データベース内に存在し、[TFTP Encrypted Config] パラメータを [Cisco Unified Communications Manager Administration] で有効化していることを前提としています。

手順

ステップ 1 製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話に存在することを確認します。

ヒント [Phone Configuration] ウィンドウの CAPF 設定セクションで [Troubleshoot] オプションを選択すると、[Cisco Unified Communications Manager Administration] で LSC または MIC が電話に存在しているかどうかを確認できます。証明書が電話に存在しない場合は、[Delete] と [Troubleshoot] オプションは表示されません。

ヒント また、電話のセキュリティ設定をチェックすることでも、LSC または MIC が電話に存在するかを確認することができます。詳細は、Cisco Unified Communications Manager に対応する Cisco Unified IP Phone 向けの Cisco Unified IP Phone アドミニストレーション ガイドを参照してください。

ステップ 2 証明書がない場合、[Phone Configuration] ウィンドウで CAPF 機能を使用して、LSC をインストールします。LSC のインストール方法については、Certificate Authority Proxy Function に関するトピックを参照してください。

ステップ 3 CAPF を設定したら、[Save] をクリックします。

ステップ 4 [Phone Configuration] ウィンドウで [Reset] をクリックします。電話はリセット後、TFTP サーバの暗号化された設定ファイルを要求します。

次の作業

CTL ファイルの更新, （15 ページ）

CTL ファイルの更新

TFTP ファイル暗号化を有効にした後、CTL ファイルを再生成します。

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 パブリッシャ ノードで **utils ctl update CTLfile** コマンドを実行します。

次の作業

サービスの再起動, （15 ページ）

サービスの再起動

CTL ファイルを再生成した後、サービスを再起動します。

手順

ステップ 1 Cisco Unified Serviceability で [Tools] > [Control Center - Feature Services] を選択します。

ステップ 2 以下の 2 つのサービスをそれぞれ選択し、[Stop] をクリックします。

- Cisco CallManager
- Cisco TFTP

ステップ 3 両方のサービスが停止したら、両方を再度選択し、[Start] をクリックします。

次の作業

電話のリセット，（16 ページ）

電話のリセット

暗号化された TFTP 設定ファイルの更新をすべて完了したら、電話をリセットします。

手順

ステップ 1 [Cisco Unified CM Administration] から、[Device] > [Phones] を選択します。
ステップ 2 [Find] をクリックします。
ステップ 3 [Select All] をクリックします。
ステップ 4 [Reset Selected] をクリックします。

電話の設定ファイルの暗号化の無効化

電話設定ファイルの暗号化を無効にするには、[Cisco Unified Communications Manager Administration] で電話セキュリティプロファイルの [TFTP Encrypted Config] チェック ボックスをオフにし、変更を保存する必要があります。

警告 TFTP 暗号化設定が False であるが、SIP を実行している電話でダイジェスト認証が True に設定されている場合、ダイジェスト クレデンシャルがクリア テキストで送信される可能性があります。

設定の更新後、電話の暗号キーは Cisco Unified Communications Manager データベース内に残ります。

Cisco Unified IP Phone 7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、7975G は暗号化ファイル（.enc、.sgn ファイル）を必要とします。暗号化設定が false に変更された場合は、電話は暗号化されていない、署名されたファイル（.sgn ファイル）を要求します。

SCCP を実行している Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961、7906G、7911G、7921G、7925G、7925G-EX、7926G、7931G、7940G、7941G、7941G-GE、7942G、7945G、7960G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945 と、SIP を実行している Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G-GE7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945、8961、および 9971 が、暗号化設定が False に変更されたときに暗号化されたファイルを要求する場合、管理者は電話の GUI で対称キーを削除する必要があります。これにより、電話が次回リセットされるときに、暗号化されていない設定ファイルが要求されます。

ヒント　Cisco Unified IP Phone 7940G および 7960G（SIP のみ）では、暗号化を無効にするために電話の GUI で対称キーのキー値として 32 バイトの 0 を入力します。Cisco Unified IP Phone 7905G および 7912G（SIP のみ）では、暗号化を無効にするために電話の GUI で対称キーを削除します。これらの作業の実行方法については、使用している電話のモデルに対応する電話のアドミニストレーション ガイドを参照してください。

電話設定ファイルダウンロードからのダイジェストクレデンシャルの除外

初期設定後、電話に送信された設定ファイルからダイジェスト クレデンシャルを除外するには、電話に適用されているセキュリティ プロファイルの [Exclude Digest Credentials in Configuration File] チェック ボックスをオンにします。このオプションは、Cisco Unified IP Phone 7905G、7912G、7940G、7960G（SIP のみ）でのみサポートされています。

ダイジェスト クレデンシャルを変更するために設定ファイルを更新する場合には、このチェック ボックスをオフにすることが必要となることがあります。

関連トピック

暗号化された設定ファイルの設定のヒント，（8 ページ）
暗号化された電話ファイルのセットアップに関する詳細情報の入手先，（17 ページ）

暗号化された電話ファイルのセットアップに関する詳細情報の入手先

関連トピック

電話設定ファイルの暗号化について，（1 ページ）
暗号化された設定ファイルをサポートする電話モデル，（7 ページ）
暗号化された設定ファイルの設定のヒント，（8 ページ）
電話の設定ファイルの暗号化の無効化，（16 ページ）
電話セキュリティ プロファイルの設定のヒント