



暗号化された電話機設定ファイルのセットアップ

この章では、暗号化された電話機設定ファイルのセットアップについて説明します。セキュリティ関連の設定後、電話機設定ファイルにはダイジェストパスワードや電話機の管理者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。

- [電話機の設定ファイルの暗号化について, 1 ページ](#)
- [AES 256 Encryption Support for TLS and SIP SRTP, 4 ページ](#)
- [暗号化された設定ファイルをサポートする電話機モデル, 7 ページ](#)
- [暗号化された設定ファイルのセットアップのヒント, 8 ページ](#)
- [TFTP 暗号化の設定, 9 ページ](#)
- [電話機の設定ファイルの暗号化の無効化, 16 ページ](#)
- [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, 17 ページ](#)
- [暗号化された電話機ファイルのセットアップに関する詳細情報の入手先, 18 ページ](#)

電話機の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、[電話セキュリティプロファイル設定 (Phone Security Profile Configuration)] ウィンドウで TFTP 暗号化設定オプションを有効にし、[Cisco Unified Communications Manager の管理 (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 暗号化設定オプションを有効にした後、[Cisco Unified Communications Manager の管理 (Cisco Unified Communications Manager Administration)] と電話に必要なパラメータを設定し、Cisco Unified Serviceability の必要なサービスと TFTP サーバを再起動します

- 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します
- 2 設定ファイルの暗号化バージョンを生成します

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、暗号化バージョンの設定ファイルが必須です。



警告

TFTP 暗号化設定が False なのに 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を決定します。サポートされる方式は Cisco Unified Communications Manager の機能と搭載されている暗号化設定ファイルをサポートするファームウェアに依存します。ファームウェア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、電話に期待された機能が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、シスコは、暗号化された電話機設定ファイルに関するタスクを関連付けられているタスクをセキュアな環境で実行することを強くお勧めします。

Cisco Unified Communications Manager は次の機能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暗号化

手動キー配布と電話の公開キーによる対称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 の管理 (Cisco Unified Communications Manager Administration)] の [TFTP 暗号化設定 (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, \(2 ページ\)](#)
- [電話機の公開キーによる対称キーの暗号化, \(3 ページ\)](#)
- [電話機モデルのサポート](#)
- [電話機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、Cisco Unified Communications Manager データベースに保存された 128 ビットまたは 256 ビットの対称キーによって、電話リセット後に電話コンフィギュレーションファイルが暗号化されます。電話モデルのキー サイズを判定する。

コンフィギュレーション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 [電話の設定 (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[承認 (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コンフィギュレーション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、対称キーによりコンフィギュレーション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判定する。

電話に対称キーが含まれる場合、その電話は常時暗号化されたコンフィギュレーションファイルを要求します。Cisco Unified Communications Manager によって、TFTP サーバによって署名された、暗号化コンフィギュレーション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コンフィギュレーション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、コンフィギュレーションファイルが電話機に適用されません。



ヒント

[TFTP 暗号化設定 (TFTP Encrypted Config)] の設定が無効にされた場合、管理者は電話の GUI で対称キーを削除して、次回リセットされたときに電話が暗号化されていないコンフィギュレーションファイルを要求するようにする必要があります。

関連トピック

[電話機モデルのサポート](#)

電話機の公開キーによる対称キーの暗号化

電話機に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) がある場合は、電話機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、電話機は設定ファイルにある電話機の証明書の MD5 ハッシュと LSC または MIC の MD5 ハッシュとを比較します。電話が問題を認識しない場合、電話機はリセット後 TFTP サーバから暗号化された設定ファイルを要求します。電話機が問題を認識する場合、たとえばハッシュが一致しない、電話機に証明書がない、MD5 値が空欄になっているなどの場合、電話機は CAPF 認証モードが [認証文字列による (By Authentication String)] (この場合は文字列の手動入力が必要) に設定されていない限り、電話は CAPF でセッションを開始しようとします。認証局プロキシ機能 (CAPF) は Cisco Unified IP Phone を Cisco Unified Communications Manager に認証し電話証明書 (LSC) を発行します。CAPF は、LSC または MIC から電話機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、電話機はリセットされ、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機がリセットされた後、データベースが TFTP に公開キーは電話機内にあると通知した後で、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、設定ファイルを Advanced Encryption Standard (AES) 128 暗号化アルゴリズムで暗号化します。次に、電話機は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

る対称キーを公開キーで暗号化します。電話機は署名されているファイルを確認し、署名が有効であれば、電話は LSC または MIC から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、対称キーがファイルの内容を復号化します。

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機では、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 暗号化構成設定が無効で、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) を要求する場合、Cisco Unified Communications Manager は [ファイルが見つかりません (file not found error)] のエラーを電話に送信します。次に、電話機は暗号化されていない署名済ファイル (.sgn ファイル) を要求します。

TFTP 暗号化構成設定が有効で、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場合、TFTP サーバは最小設定を含む暗号化されていないファイルを提供します。電話機が最小構成を受信した後、電話機はキーのミスマッチなどのエラー状態を検出し、CAPF でセッションを開始して電話機の公開キーと Cisco Unified Communications Manager データベースを同期します。エラー条件が解決されると、電話機は次に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](#)

[電話機モデルのサポート](#)

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増加する要件を満たすために、NGE (Next-Generation Encryption; 次世代暗号化) 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 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 Secure Sockets Layer (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 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。

引数の説明

- 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 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 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 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では、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 Standards（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 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 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 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 接続が作成されると場合に、
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
暗号と TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 暗号を使用して 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
暗号と AEAD_AES_128_GCM 暗号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 から SIP への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機モデル

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

電話機モデルとプロトコル	暗号化方式（Encryption Method）
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

電話機モデルとプロトコル	暗号化方式 (Encryption Method)
Cisco Unified IP Phone 7940G または 7960G (SIP のみ)	<p>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</p> <p>ファイル署名のサポート：SIP を実行するこれらの電話機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。</p>
<p>Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961</p> <p>Cisco Unified IP Phone 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</p> <p>Cisco Unified IP Phone、7961G-GE、7941G-GE</p> <p>Cisco Unified IP Phone 7931G、7925G、7926G (SCCP のみ)</p> <p>Cisco Unified IP Phone 8941 および 8945</p> <p>Cisco Unified IP Phone 8961、9951、および 9971</p>	<p>電話機の公開キーの暗号化 (PKI) による対称キーの暗号化：暗号化アルゴリズム：AES 128 キーサイズ：128 ビット</p> <p>ファイル署名のサポート：はい</p> <p>(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 Cisco Unified Communications Manager クラスタは Cisco Unified IP Phone (6901 と 6911) では保護 (混合) モードに設定され Cisco Certificate Authority Proxy Function (CAPF) の詳細を含む Cisco CTL ファイルを取得し、暗号化された設定ファイルが Cisco IP Phone (6901 および 6911) で動作するように設定する必要があります。</p>

暗号化された設定ファイルのセットアップのヒント

シスコでは、[TFTP 暗号化設定 (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を推奨します。電話に PKI 機能がない場合、Unified Communications Manager Administration 内と電話内とに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 暗号化設定 (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 で暗号化されたコンフィギュレーション 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。

- 暗号化されたコンフィギュレーション ファイルをサポートする電話にのみ、セキュリティ プロファイルに [TFTP 暗号化設定 (TFTP Encrypted Config)] フラグが表示されます。Cisco Unified IP Phone 7905G、7912G、7940G、7960G (SCCP のみ) には暗号化されたコンフィギュ

レーションファイルを設定できません。これらの電話はコンフィギュレーションファイルのダウンロード時にクレデンシャルデータを受信しないためです。

- [TFTP 暗号化設定 (TFTP Encrypted Config)] のデフォルト設定は False です (マークが付いていない)。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、暗号化されたコンフィギュレーション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のを 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に、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、非暗号化コンフィギュレーション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、シスコではこのメソッド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 には、暗号化されたコンフィギュレーション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る、電話へのダイジェストクレデンシャルの送信メソッドが用意されています。[設定ファイル内のダイジェスト信用証明書を除外 (Exclude Digest Credentials in Configuration File)] 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コンフィギュレーションファイル内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 [設定ファイル内のダイジェスト信用証明書を除外 (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 [ダイジェスト信用証明書を除外 (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

暗号化を TFTP 設定ファイルに設定するには、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、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 暗号化を有効にする、(11 ページ)	使用する電話の該当する TFTP 設定ファイル 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)	これはオプションです。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に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	手動キー配布のセットアップ、(12 ページ)	手動のキーによる電話を使用する場合は、手動キー配布をセットアップします。
ステップ 4	電話機の対称キーの入力、(13 ページ)	手動のキーによる電話では、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 暗号化を有効にする

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、所定のモデルの電話の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 Communications Manager の管理 (Cisco Unified Communications Manager Administration)] で、[システム (System)]>[セキュリティ (Security)]>[電話セキュリティプロファイル (Phone Security Profile)] の順に選択します。
 - ステップ 2 [検索 (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 暗号化設定 (TFTP Encrypted Config)] チェック ボックスをオンにします。
 - ステップ 4 [保存 (Save)] をクリックします。
 - ステップ 5 クラスターで使用されている他の電話の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

これはオプションです。 [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 暗号化を有効にする, \(11 ページ\)](#)

手順

-
- ステップ 1** Cisco Unified Communications Manager の管理で、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。
- ステップ 2** [TFTP ファイル署名アルゴリズム (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** [保存 (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機用：[手動キー配布のセットアップ](#)、(12 ページ)。

公開キーを使用する電話機用：[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)

手動キー配布のセットアップ

次に述べる手順では、以下の点を前提としています。

- その電話機は Cisco Unified Communications Manager データベースに存在する。
- 互換性のあるファームウェア ロードが TFTP サーバに存在する。
- Cisco Unified Communications Manager の管理ページで、TFTP 暗号化設定パラメータが有効にされている。

はじめる前に

使用中の電話機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** [電話の設定 (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** [保存 (Save)] をクリックします。
- ステップ 4** 電話機に対称キーを入力し、電話機をリセットします。
これらの作業の実行方法については、使用中の電話機モデルをサポートする電話機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

[電話機の対称キーの入力](#), (13 ページ)

手動キー配布の設定

次の表に、[電話の設定 (Phone Configuration)] ウィンドウにある手動配布の構成時の設定について説明します。

表 1: 手動キー配布の構成時の設定

設定	説明
対称キー (Symmetric Key)	<p>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。</p> <p>キー サイズと正確にあった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:</p> <ul style="list-style-type: none"> • 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 <p>キー設定後は、変更しないでください。</p>
文字列の生成 (Generate String)	<p>Cisco Unified Communications Manager Administration に 16 進数文字列を生成させる場合、[文字列の生成 (Generate String)] ボタンをクリックします。</p> <p>キー設定後は、変更しないでください。</p>
データベース値を復元 (Revert to Database Value)	<p>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。</p>

電話機の対称キーの入力

Cisco Unified Communications Manager の管理 (Cisco Unified Communications Manager Administration) で手動のキー配布を設定したあと、対称キーを電話に入力するには、するには、次の手順に従います。

手順

-
- ステップ 1 電話の [設定 (Setting)] ボタンを押します。
 - ステップ 2 設定がロックされていれば、[設定 (Setting)] メニューをスクロールし、[電話のロックを解除 (Unlock Phone)] を強調表示して、[選択 (Select)] ソフトキーを押します。電話のパスワードを入力して [承認 (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 [設定 (Setting)] メニューをスクロールし、[セキュリティ設定 (Security Configuration)] を強調表示して、[選択 (Select)] ソフトキーを押します。
 - ステップ 4 [セキュリティ設定 (Security Configuration)] メニューで、[暗号キーの設定 (Set Cfg Encrypt Key)] オプションを強調表示し、[選択 (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 桁ゼロを入力します。
 - ステップ 6 キーの入力が終了したら、[承認 (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 電話機をリセットします。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。お使いの電話機が、電話機の公開キーを使用する対称キーの暗号化方式 (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機モデル, \(7 ページ\)](#) を参照してください。

次の手順は、電話機が Cisco Unified Communications Manager データベース内に存在し、TFTP 暗号化設定パラメータを Cisco Unified Communications Manager Administration で有効化したと仮定しています。

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) が電話機に存在することを確認します。

- ヒント [電話の設定 (Phone Configuration)] ウィンドウで認証局プロキシ機能 (CAPF) 設定セクションの [トラブルシュート (Troubleshoot)] オプションを選択すると、LSC または MIC が電話機の Cisco Unified Communications Manager Administration に存在するかを確認することができます。証明書が電話機に存在しない場合は、[削除 (Delete)] と [トラブルシュート (Troubleshoot)] オプションは表示されません。
- ヒント また、電話機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 が電話機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 をサポートする Cisco Unified IP Phone 用の 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、[電話の設定 (Phone Configuration)] ウィンドウで認証局プロキシ機能 (CAPF) 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 (CAPF) に関するトピックを参照してください。
- ステップ 3 認証局プロキシ機能 (CAPF) を設定したら、[保存 (Save)] をクリックします。
- ステップ 4 [電話の設定 (Phone Configuration)] ウィンドウで [リセット (Reset)] をクリックします。電話機はリセット後、TFTP サーバから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 [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、[停止 (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、[開始 (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 の管理 (Cisco Unified Communications Manager Administration)] から、[デバイス (Device)] > [電話 (Phone)] 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** [すべてを選択 (Select All)] をクリックします。
- ステップ 4** [選択したアイテムのリセット (Reset Selected)] をクリックします。
-

電話機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 の管理 (Cisco Unified Communications Manager Administration)] のセキュリティ プロファイルの [TFTP 暗号化設定 (TFTP Encrypted Config)] チェック ボックスをオフにし、変更を保存します。



警告

TFTP 暗号化設定が False なのに 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、および 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、7925G、7925G-EX、7926G、7931G、7940G、7941G、7941G-GE、7942G、7945G、7960G、7961G、7961G-GE、7962G、7965G、7970G、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-GE、7962G、7965G、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 で対称キーのキーの値として 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、使用中の電話機モデルをサポートする電話機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 [設定ファイル (Configuration File)] チェックボックスの [ダイジェストクレデンシャルを除外 (Exclude Digest Credential)] をオンにします。Cisco Unified IP Phone 7905G、7912G、7940G、7960G (SIP のみ) のみがこのオプションをサポートしています。

ダイジェストクレデンシャルの変更時に設定ファイルを更新するためには、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セットアップのヒント、\(8 ページ\)](#)

[暗号化された電話機ファイルのセットアップに関する詳細情報の入手先、\(18 ページ\)](#)

暗号化された電話機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

[電話機の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機モデル](#), (7 ページ)

[暗号化された設定ファイルのセットアップのヒント](#), (8 ページ)

[電話機の設定ファイルの暗号化の無効化](#), (16 ページ)

[電話機のセキュリティ プロファイルの設定のヒント](#)