暗号化された電話設定ファイルの設定

この章では、暗号化された電話機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を行った後、電話機の設定ファイルには、ダイジェストパスワードや電話管理者パスワードなどの機密情報が含まれています。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。

暗号化された TFTP 設定ファイルの概要

TFTP 設定は、電話機が登録プロセスを実行する際に TFTP サーバからダウンロードする設定ファイルを暗号化することによって、デバイスの登録プロセス中にデータを保護します。このファイルには、ユーザ名、パスワード、IP アドレス、ポートの詳細、電話機の SSH ログイン情報などの機密情報が含まれます。この機能が設定されていない場合、設定ファイルはクリアテキストで送信されます。この機能を導入すると、登録プロセス中に攻撃者がこの情報を傍受できなくなります。この情報は暗号化解除され、クリアテキストで送信されます。したがって、データを保護するために、TFTP 設定ファイルを暗号化することを推奨します。

警告 SIP 電話でダイジェスト認証オプションを有効にし、TFTP で暗号化設定オプションを無効にした場合は、ダイジェストログイン情報がクリアテキストで送信されます。

TFTP の設定後、TFTP サーバは次の手順を実行します。

- 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
- 暗号化されたバージョンのコンフィギュレーションファイルを生成します。

電話機が暗号化された電話設定ファイルをサポートし、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、電話機は設定ファイルの暗号化バージョンを要求します。

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ません。電話機のモデルとプロトコルによって、コンフィギュレーションファイルを暗号化するためにシステムが使用する方法が決定されます。サポートされる方式は、Unified Communications Manager の機能と、暗号化された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暗号化されていない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。

暗号化キーの配布

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を推奨します。

Unified Communications Manager は、次の方式をサポートします。

- 手動キー配布
- 電話の公開キーによる対称キーの暗号化

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、[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, on page 2
電話機の公開キーによる対称キーの暗号化, on page 3
電話機モデルのサポート
暗号化された TFTP 設定ファイルの無効化, on page 13

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、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、Unified Communications Manager に **[Phone Configuration]** ウィンドウで生成させることもできます。キーがデータベースに存在する場合、管理者またはユーザは電話機のユーザインターフェイスにアクセスして、電話にキーを入力する必要があります。[**承認 (Accept)**] ソフトキーを押すとすぐに、電話機はフラッシュにキーを保存します。キーを入力すると、電話機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。必要なタスクが発生すると、対称キーは RC4 または AES 128 暗号化アルゴリズムを使用してコンフィギュレーションファイルを暗号化します。どの電話機が RC4 または AES 128 暗号化アルゴリズムを使用するかを確認するには、「暗号化をサポートする電話機モデル（4 ページ）」を参照してください。

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。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。

電話機は、フラッシュに保存されている対称キーを使用して、ファイルの内容を復号化します。復号化に失敗した場合、設定ファイルは電話機に適用されません。

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) が含まれている場合、電話機にはPKI暗号化に使用される公開キーと秘密キーのペアが含まれています。

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。電話機が問題を特定しない場合、電話機がリセットされた後、電話機は 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 IP 電話 を 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、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存在し、電話機がリセットされると、データベースが TFTP に電話機の公開キーが存在することを通知した後に、対称キー暗号化プロセスが開始されます。TFTP サーバは、Advanced Encryption Standard (AES) 128 暗号化アルゴリズムを使用してコンフィギュレーションファイルを暗号化する 128 ビットの対称キーを生成します。次に、電話の公開キーによって対称キーが暗号化されます。このキーには、コンフィギュレーションファイルの署名付きエンベロープヘッダーが含まれています。電話機はファイルの署名を検証し、署名が有効であれば、電話機は 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します。対称キーは、ファイルの内容を復号化します。

コンフィギュレーションファイルを更新するたびに、TFTPサーバは自動的に新しいキーを生成してファイルを暗号化します。

ヒント この暗号化方式をサポートする電話の場合、電話機はコンフィギュレーションファイルの暗号化設定フラグを使用して、暗号化または暗号化されていないファイルを要求するかどうかを決定します。[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 IP 電話が暗号化ファイル（.enc.sgn ファイル）を要求すると、Unified Communications Manager は [file not found error] 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されたファイル (...) を要求します。

TFTP 暗号化設定が有効になっていても、電話機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した場合、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 Unified Communications Manager データベースを同期できます。エラー状態が解決された場合、電話機は、次回のリセット時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

暗号化をサポートする電話機モデル

次のCisco Unified IP 電話 の電話機設定ファイルを暗号化できます。

電話機のモデルとプロトコル	[暗号化方式（Encryption Method）]
Cisco Unified IP 電話 7800 または 6921	手動キー配布: 暗号化アルゴリズム: RC4Key サイズ: 256 ビット ファイル署名のサポート: いいえ
Cisco Unified IP 電話 7942 または 7962 (SIP のみ)	手動キー配布：暗号化アルゴリズム：Advanced Encryption Standard (AES) 128Key サイズ：128 ビット ファイル署名のサポート: SIP を実行している電話機は、署名された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。

電話機のモデルとプロトコル	[暗号化方式（Encryption Method）]
Cisco Unified IP 電話 6901、6911、6921、6941、6945 および 6961 Cisco Unified IP 電話 79 g、Cisco Unified IP 電話 7961g、7961G、または 7965G;Cisco Unified IP 電話 79 41G、79 42g、または 7945G;Cisco Unified IP 電話 7911G;Cisco Unified IP 電話 の 79 06g Cisco Unified IP 電話 、7961G-GE、7941G-GE Cisco Unified IP 電話 7931G, (SCCP のみ) Cisco Unified ワイヤレス IP 電話 7925G, 7925G-EX, 7926G Cisco Unified IP 電話 8941 および 8945 Cisco Unified IP 電話 8961、9951、および 9971 Cisco IP 電話 7811、7821、7841、7861 Cisco IP 会議用電話 7832 Cisco IP 電話s 8811、8841、8845、8851、8851NR、8861、8865、および 8865NR Cisco Unified IP 会議用電話 8831 Cisco 会議用電話 8832 Cisco ワイヤレス IP 電話 8821	電話機の公開キーによる対称キーの暗号化：暗号化アルゴリズム：AES128Key サイズ：128 ビット ファイル署名のサポート: はい （注） Cisco Unified IP 電話 6901 および6911 は、デフォルトでは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 電話 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、Unified Communications Manager クラスタは、Cisco Unified IP 電話（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 TFTP 設定ファイルのヒント

電話機のダウンロードで機密データを保護するには、TFTP暗号化設定ファイルを有効にすることをお勧めします。電話に PKI 機能がない場合、[Unified Communications Manager Administration] と電話で対称キーも設定する必要があります。対称キーが電話機または Unified Communications Managerのいずれかに存在しない場合、またはTFTP暗号化設定ファイルの設定時に不一致が発生した場合、電話機は登録できません。

Unified Communications Manager で暗号化された設定ファイルを設定する場合は、次の点を考慮してください。

- 暗号化された設定ファイルをサポートしている電話機にのみ、[電話機のセキュリティプロファイルの設定（Phone Security Profile Configuration）] ページ)に [TFTP 暗号化設定（TFTP Encrypted Config）] チェックボックスが表示されます。暗号化された設定ファイルを Cisco Unified IP 電話 の 7800、7942、および 7962（SCCP のみ）に設定することはできません。これらの電話機は設定ファイルのダウンロードで機密データを受信しないからです。

- デフォルトでは、[TFTP 暗号化設定（TFTP Encrypted Config）] チェックボックスはオフになっています。このデフォルト設定、非セキュアプロファイルを電話機に適用した場合、ダイジェストログイン情報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 電話 の場合、Unified Communications Manager では [デバイスセキュリティモード（Device Security Mod）] を [認証済み (Authenticated)] または [暗号化(Encrypted)] に設定して暗号化された設定ファイルを有効にする必要はありません。Unified Communications Manager は、登録中の公開鍵をダウンロードするために CAPF プロセスを使用します。
- 環境が安全である場合や、PKI が有効になっていない電話機に対称キーを手動で設定しないようにする場合は、暗号化されていない設定ファイルを電話機にダウンロードできます。ただし、この方法を使用することはお勧めしません。
- Cisco Unified IP 電話 の 7800、7942、および 7962（SIP のみ）では、Unified Communications Manager は暗号化された設定ファイルを使用するよりも簡単で、安全性が低いダイジェストログイン情報を電話機に送信する方法を提供します。[ダイジェストログイン設定ファイルを除外（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、ダイジェストログイン情報の初期化に役立ちます。この方法では、暗号化されていないコンフィギュレーションファイルで、電話機にダイジェストクレデンシャルを送信します。ログイン情報が電話機に入力された後は、[TFTP 暗号化設定（TFTP Encrypted Config）] オプションを無効にしてから、[電話機のセキュリティ プロファイルの設定（Phone Security Profile Configuration）] ページの [設定ファイルのダイジェストクレデンシャルを除外する（Exclude Digest Credential in Configuration File）] を有効にすることをお勧 めします。これにより、今後のダウンロードからダイジェストログイン情報が除外されます。
- ダイジェストログイン情報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ログイン情報が含まれないようになると、既存のログイン情報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、電話機が工場出荷時の状態にリセットされるか、または新しいクレデンシャル (空白を含む) を受信するまで、そのまま残ります。電話機またはエンドユーザのダイジェストログイン情報を変更する場合は、対応する [電話機のセキュリティプロファイル情報（Phone Security Profile Information）] ページの [設定ファイルでのダイジェストログイン情報の除外（Exclude Digest Credential in Configuration File）] を一時的に無効にして、新しいダイジェストログイン情報を電話機にダウンロードします。

電話機の設定ファイルの暗号化のタスクフロー

TFTP 設定ファイルの暗号化を設定するには、クラスタのセキュリティが混合モードで設定されていることを確認し、手動キー暗号化と公開キー暗号化をサポートするクラスタ内の電話機を確認し、SHA-1 と SHA-512 をサポートする電話機を確認し、以下のタスクを完了します。

（注） SHA-512 クラスタ全体を有効にし、電話機がサポートしていない場合、これらの電話機は機能しません。

手順

	コマンドまたはアクション	目的
Step 1	TFTP 暗号化の有効化 （7 ページ）	電話機の [TFTP 設定ファイル (TFTP Configuration File)] オプションを有効にします。電話セキュリティプロファイルでこのオプションを有効にすることができます。
Step 2	SHA-512 署名アルゴリズムの設定 （8 ページ）	TFTP ファイル暗号化を有効化すると、デフォルトの署名アルゴリズムとしてSHA-1が設定されます。より強力な SHA-512 アルゴリズムを使用するようにシステムを更新するには、次の手順を使用します。
Step 3	LSC または MIC 証明書のインストールの確認 （11 ページ）	公開キーを使用する電話機の場合は、証明書のインストールを確認します。
Step 4	CTL ファイルの更新 （12 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。
Step 5	サービスの再起動 （12 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。
Step 6	電話のリセット （13 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、電話機をリセットします。

TFTP 暗号化の有効化

この TFTP 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。TFTP サーバからダウンロードするファイルのTFTP暗号化を有効にするには、次の手順を実行します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[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）]**

Step 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。

Step 3 **[TFTP Encrypted Config]** チェックボックスをオンにします。

Step 4 [保存（Save）] をクリックします。

Step 5 クラスタで使用されている他のすべての電話セキュリティプロファイルに対して、これらの手順を繰り返します。

（注） 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の電話セキュリティプロファイルで **[TFTP 暗号化設定（TFTP Encrypted Config）]** チェックボックスをオフにして、変更内容を保存する必要があります。

SHA-512 署名アルゴリズムの設定

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。次のオプションの手順を使用して、デジタル署名などの TFTP 設定ファイルにより強力な SHA-512 アルゴリズムを使用するようにシステムをアップグレードできます。

（注） ご使用の電話機が SHA-512 をサポートしていることを確認してください。対応していない場合は、システム更新後に電話機が動作しなくなります。

手順

Step 1 [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 2 [セキュリティパラメータ（Security Parameters）] ペインに移動します。

Step 3 [**TFTP File Signature Algorithm**] ドロップダウンリストから、[**SHA-512**] を選択します。

Step 4 [保存（Save）] をクリックします。

この手順を完了するには、ポップアップウィンドウに一覧表示されている影響を受けるサービスを再起動します。

手動キー配布の設定

手動キーを使用する電話機の場合は、手動キー配布を設定する必要があります。

始める前に

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 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。

- [Unified Communications Manager Administration] で、[TFTP 暗号化設定（TFTP Encrypted Config）] パラメータが有効に設定されている。
- お使いの電話機は、手動キー配布をサポートしています。

手順

Step 1 [Cisco Unified CM Administration] から、[**デバイス**（**Device**）] > [**電話機**（**Phone**）] の順に選択します。

Step 2 [検索（Find）] をクリックします。

Step 3 [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。

（注） 設定を行った後は、キーを変更しないようにしてください。

Step 4 [保存（Save）] をクリックします。

Step 5 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。

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:* 手動キー配布の構成時の設定

設定	説明
[対称キー（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 電話 7905G および 7912G（SIP のみ）：256 ビット • Cisco ユニファイド IPPhone s の 7942 および 7962 (SIP のみ): 128 ビット キーが設定された後は、変更しないようにしてください。
[文字列を生成（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。
[データベース値を復元（Revert to Database Value）]	データベース内の値を復元する場合は、このボタンをクリックします。

電話の対称キーの入力

前の手順を使用して、ユニファイドコミュニケーションマネージャで電話機の手動キーを設定した場合は、次の手順を使用して電話機にキーを入力します。

手順

Step 1 電話の [Setting] ボタンを押します。

Step 2 設定がロックされている場合は、[**設定 (Settings)**] メニューを下にスクロールして、[**電話のロック解除 (Unlock Phone)**] を強調表示し、 **[選択**電話機のパスワードを入力し、[**承認 (Accept)**] ソフトキーを押します。

電話機はパスワードを受け入れます。

Step 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。

Step 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。

Step 5 暗号キーの入力を求められたら、キー (16 進数) を入力します。キーをクリアする必要がある場合は、32のゼロの数字を入力します。

Step 6 キーの入力が完了したら、[**承認 (Accept)**] ソフトキーを押します。

電話機は暗号キーを受け入れます。

Step 7 電話機をリセットします。

電話機がリセットされると、電話機は暗号化された設定ファイルを要求します。

LSC または MIC 証明書のインストールの確認

公開キーを使用する電話機の場合は、証明書のインストールを確認します。

（注） この手順は、PKI 暗号化を使用するCisco Unified IP 電話に適用されます。電話機が PKI 暗号化をサポートしているかどうかを確認するには、「暗号化された設定ファイルをサポートする電話モデル」の項を参照して

次の手順は、電話機が Unified Communications Manager データベースに存在し、Unified Communications Manager で [TFTP 暗号化設定（TFTP Encrypted Config）] パラメータを有効にしていることを前提としています。

手順

Step 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。

Step 2 [Cisco Unified CM Administration] から、**[デバイス（Device）] > [電話機（Phone）]** の順に選択します。
電話機のリストが表示されます。

Step 3 [デバイス名（Device Name）] をクリックします。
[電話の設定（Phone Configuration）] ページが表示されます。

ヒント **[電話の設定（Phone Configuration）]** ページの [CAPF 設定（CAPF settings）] セクションで **[トラブルシュート（Troubleshoot）]** オプションを選択して、Unified Communications Managerの電話機に LSC または MIC が存在するかどうかを確認します。証明書が電話機に存在しない場合、[削除（Delete）] および [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　電話機のセキュリティ設定を確認することによって、電話機に LSC または MIC が存在することを確認することもできます。詳細については、 Unified Communications Manager のこのバージョンをサポートするCisco Unified IP 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。

Step 4　証明書が存在しない場合、[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 に関連するトピックを参照してください。

Step 5　CAPF を設定したら、[保存（Save）] をクリックします。

Step 6　[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。

CTL ファイルの更新

Unified Communications Manager の変更を行った後、CTL ファイルを更新します。TFTP ファイル暗号化を有効にしているので、CTL ファイルを再生成する必要があります。

手順

Step 1　コマンドライン インターフェイスにログインします。

Step 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。

サービスの再起動

暗号化された TFTP 設定ファイルの更新を完了したら、Cisco TFTP サービスと Cisco CallManager サービスを再起動して変更を有効にしてください。

手順

Step 1　[Cisco Unified Serviceability] から選択します。**[ツール（Tools）] > [コントロールセンター - 機能サービス（Control Center - Feature Services）]**

Step 2　次の 2 つのサービスを選択します。

- Cisco CallManager
- Cisco TFTP

Step 3　[再起動（Restart）] をクリックします。ただし、CallManager 証明書を再生成または更新した後は、TFTP サービスを手動で再起動する必要はありません。

電話のリセット

すべての暗号化されたTFTP設定ファイルの更新が完了したら、電話機をリセットしてください。

手順

Step 1 [Cisco Unified CM Administration] から、**[デバイス（Device）]** > **[電話（Phones）]** を選択します。

Step 2 [検索（Find）] をクリックします。

Step 3 [すべて選択（Select All）] をクリックします。

Step 4 [選択をリセットする（Reset selected）] をクリックします。

暗号化された TFTP 設定ファイルの無効化

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、ダイジェストログイン情報がクリアテキストで送信される可能性があります。

設定を更新した後、電話機の暗号キーは Unified Communications Manager データベースに残ります。

Cisco Unified IP 電話7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、 7962G、7965G、 および 7975G は暗号化ファイル（.enc、.sgn ファイル）を要求します。暗号化設定が **False** に更新された場合は、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。

Cisco Unified IP 電話 は、SCCP および SIP 上で実行されている場合に、暗号化設定が **False**に更新されると、暗号化されたファイルを要求します。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するように設定するには、電話の GUI から対称キーを削除します。

- Cisco Unified IP 電話SCCP で実行される Cisco Unified IP 電話 は、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 です。
- Cisco Unified IP 電話SIP で実行される Cisco Unified IP 電話 は、6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G、7962G、7965G、、7975G、8941、8945、8961、9971、7811、78321、7841、7861、7832、8811、8841、8845、8851、8851NR、8861、8865、8865NE、8821、8831、8832、8832NR です。

手順

	コマンドまたはアクション	目的
Step 1	電話機設定ファイルの暗号化を無効にするには、電話機に関連付けられている電話機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ます。	
Step 2	Cisco Unified IP 電話 7942 および 7962（SIP のみ）の場合は、電話画面で対称キーのキー値として「32-byte 0」を入力して暗号化を無効にします。	
Step 3	Cisco Unified IP 電話（SIP のみ）の場合は、電話画面で対称キーを削除して暗号化を無効にします。	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

初期設定後に電話機に送信される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、電話機に適用され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ユニファイド IP 電話 の 7800、7942、および 7962 (SIP のみ) でのみサポートされます。

ダイジェストクレデンシャルの変更のコンフィギュレーションファイルを更新するには、このチェックボックスをオフにする必要があります。

関連トピック

暗号化された TFTP 設定ファイルのヒント, on page 5
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