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。

暗号化された TFTP 設定ファイルの概要

この機能は、登録プロセスを実行している TFTP サーバから電話機が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、デバイス登録中にデータを保護します。この設定ファイルには、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 クレデンシャルなどの機密情報が含まれている場合があり、暗号化しない場合、このような機密情報はクリアテキストで送信されます。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。

TFTP 設定ファイルを暗号化するには、[Cisco Unified CM Administration] に移動して、[**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、[**TFTP 暗号化設定（TFTP Encrypted Config）**] チェックボックスをオンにします。

[TFTP 暗号化設定（TFTP Encrypted Config）] オプションを有効にした後、[Unified Communications Manager Administration] および電話機で必要なパラメータを設定してから [Cisco Unified Serviceability] で必要なサービスを再起動すると、TFTP サーバは次の作業を実行します。

1. ディスク上のプレーン 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、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 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、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。

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、[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。

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。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。

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 IP Phone 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 IP Phone 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 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。

暗号化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 7800 または 6921	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 ユニファイド IP Phone 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）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 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 、7961G-GE、7941G-GE Cisco 統一 IP Phone 79 31g, (sccp のみ) CISCO 統一されたワイヤレス Ip Phone 79 25g, 79 25G-EX, 79 26g Cisco Unified IP Phone 8941 および 8945 Cisco Unified IP Phone 8961、9951、および 9971 Cisco IP Phone 7811、7821、7841、7861 Cisco IP Conference Phone 7832 Cisco IP Phones 8811、8841、8845、8851、8851NR、8861、8865、および 8865NR Cisco Unified IP Conference Phone 8831 Cisco Conference Phone 8832 Cisco Wireless IP Phone 8821	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、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 TFTP 設定ファイルのヒント

電話機がダウンロードする機密データを保護するために、[TFTP 暗号化設定（TFTP Encrypted Config）] フラグを有効化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] と電話で対称キーを設定する必要があります。電話と 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 7800、7942、7962（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 暗号化設定（TFTP Encrypted Config）] のデフォルト設定は False（オフ）です。デフォルト設定である非セキュア 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 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 Unified Communications Manager が要求することはありません。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、暗号化されていない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、この方法は推奨されません。
- Cisco Unified IP Phone 7800、7942、7962（SIP のみ）の場合、[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、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 [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。

電話設定ファイルの暗号化のタスク フロー

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。

始める前に

- クラスタ セキュリティが混合モードになっていることを確認します。
- クラスタ内の電話機のうち、手動キー暗号化および公開キー暗号化をサポートしている電話機を確認します。
- SHA-1 および SHA-512 をサポートしている電話機を確認します。

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 （7 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 署名アルゴリズムの設定 （8 ページ）	（任意）。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。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。
ステップ 3	手動キー配布の設定 （9 ページ）	手動のキーを使用する電話の場合は、手動キー配布を設定する必要があります。
ステップ 4	電話の対称キーの入力 （10 ページ）	手動のキーを使用する電話では、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 （11 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 （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。
ステップ 7	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。
ステップ 8	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を完了したら、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 [**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 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。

（注） 電話設定ファイルの暗号化を無効にするには、[Unified Communications Manager Administration] で電話セキュリティ 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。

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システムをアップグレードするには、以下の任意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は、システム更新後に電話機が動作しなくなります。

始める前に

TFTP 暗号化の有効化 （7 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[システム(System)]** > **[Ent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 [**セキュリティ パラメータ（Security Parameters**）] セクションに移動します。

ステップ 3 [**TFTP ファイル署名アルゴリズム（TFTP File Signature Algorithm**）] ドロップダウンリストから、[**SHA-512**] を選択します。

ステップ 4 **[保存 (Save)]** をクリックします。

手動キー配布の設定

手動キーを使用する電話の場合は、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。
- 電話機が手動キー配布をサポートしている。

手順

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

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 [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） この設定を行った後は、キーは変更できません。

ステップ 4 **[Save]** をクリックします。

ステップ 5 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。

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 ユニファイド IPPhone s の 7942 および 7962 (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

前述の手順を使用して、Unified Communications Manager で電話機の手動キーを設定した場合は、次の手順を実行して電話機にキーを入力します。

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。

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では、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 Phone に適用されます。ご使用の電話機が 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機モデル」セクションを参照してください。

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。
- [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。

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 LSC または MIC が電話機に存在するかを Unified Communications Manager で確認するには、[電話の設定（Phone Configuration）] ウィンドウの CAPF 設定セクションにある [**トラブルシュート（Troubleshoot**）] オプションを選択します。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、電話機の [セキュリティ設定（Security Configuration）] をチェックする方法でも、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。詳細については、このバージョンの Unified Communications Manager に対応した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、認証局プロキシ機能（CAPF）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

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。

サービスの再起動

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 つのサービスを選択し、[**停止（Stop**）] をクリックします。

- Cisco CallManager
- Cisco TFTP

ステップ 3　これら2つのサービスが停止したら、両方を再度選択し、[**再起動（Restart**）] をクリックします。

電話のリセット

始める前に

暗号化された TFTP 設定ファイルの更新をすべて完了した後、必ず電話機をリセットしてください。

手順

ステップ 1 [Cisco Unified CM Administration] から、**[デバイス（Device）]** > **[電話（Phones）]** 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 [すべて選択（Select All）] をクリックします。

ステップ 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

電話設定ファイルの暗号化を無効にするには、対象の電話機に関連付けられている電話セキュリティ 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 Unified Communications Manager データベース内に残ります。

Cisco IP Phone 7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、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。

Cisco Unified IP Phone が SCCP および SIP で実行されている場合は、暗号化設定が無効に変更されたときに、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、管理者が電話の GUI から対称キーを削除する必要があります。

- SCCP で実行される Cisco Unified IP Phone 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。

- SIP で実行される Cisco Unified IP Phone は、6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G-GE、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。

ヒント Cisco Unified IP Phone 7942 および 7962（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 （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ユニファイド IP Phone s 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。