暗号化された電話機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構成した後、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管理者パスワードなど、機密性が高い情報が含まれます。 設定ファイルの機密性を守るために、設定ファイルを暗号化するように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

電話機が Cisco Unified Communications Manager からダウンロードする設定ファイル内のダイジェスト信用証明書およびセキュア パスワードを保護するには、[電話セキュリティプロファイルの設定(Phone Security Profile Configuration)] ウィンドウで [TFTP暗号化設定(TFTP Encrypted Config)] オ

プションを有効にして、Cisco Unified Communications Manager の管理ページで追加作業を実行する必要があります。

[TFTP暗号化(TFTP Encrypted Config)] オプションを有効にして Cisco Unified Communications Manager の管理ページおよび電話機で、必要なパラメータを設定し、Cisco Unified サービスアビリティ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 ディスク上のクリア テキストの設定ファイルをすべて削除します。

2 暗号化されたバージョンの設定ファイルを生成します。

電話機が暗号化された電話機設定ファイルをサポートしている場合に、電話機設定ファイルの暗号化に必要な作業を実行すると、電話機は設定ファイルの暗号化されたバージョンを要求します。

警告 SIP を実行する電話機のダイジェスト認証が有効になっていて、TFTP 暗号化設定が無効になっている場合、ダイジェスト信用証明書は暗号化されずに送信されます。

一部の電話機は、暗号化された電話機設定ファイルをサポートしません。 電話機モデルとプロトコルによって、設定ファイルの暗号化に使用される方式が決まります。 サポートされる方式は、Cisco 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。 暗号化された設定ファイルをサポートしないバージョンに電話機ファームウェアをダウングレードした場合、TFTP サーバは、最小限の設定項目を含む暗号化されていない設定ファイルを提供します。その結果、電話機が期待されるとおりに動作しない可能性があります。

キー情報の機密性を維持するために、暗号化された電話機設定ファイルに関する作業は、セキュアな環境で実行することを強く推奨します。

Cisco Unified Communications Manager は次の方法をサポートします。

- キーの手動配布
- 電話機の公開キーによる対称キーの暗号化

キーの手動配布および電話機の公開キーによる対称キーの暗号化で指定する設定情報では、Cisco Unified Communications Manager の管理ページで混合モードが設定され、TFTP 暗号化設定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

キーの手動配布, （3 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
電話機設定ファイルの暗号化の無効化, （11 ページ）

キーの手動配布

キーの手動配布では、電話機がリセットされた後、Cisco Unified Communications Manager データベースに格納されている 128 ビットまたは 256 ビットの対称キーによって、電話機設定ファイルが暗号化されます。 使用中の電話機モデルのキー サイズを確認するには。

設定ファイルを暗号化するには、[電話の設定(Phone Configuration)] ウィンドウで、管理者が手動でキーを入力するか、Cisco Unified Communications Manager がキーを生成するように要求できます。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、電話機のユーザインターフェイスにアクセスして、電話機にキーを入力する必要があります。[承諾] ソフトキーを押すとすぐに、キーは電話機のフラッシュに格納されます。 キーを入力した後、電話機をリセットすると、電話機は暗号化された設定ファイルを要求します。 必要な作業を実行した後、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、設定ファイルを暗号化します。 電話機が RC4 と AES 128 のどちらの暗号化アルゴリズムを使用するかを確認するには。

電話機に対称キーが含まれている場合、電話機は必ず暗号化された設定ファイルを要求します。Cisco Unified Communications Manager は、TFTP サーバが署名した暗号化された設定ファイルを電話機にダウンロードします。 すべての電話機タイプが設定ファイルの署名者を検証するわけではありません。

電話機は、フラッシュに格納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暗号化設定(TFTP Encrypted Config)] の設定を無効にした場合、管理者は、次にリセットしたときに暗号化されていない設定ファイルを電話機が要求するように、電話機 GUI から対称キーを削除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）が含まれている場合、電話機には、PKI 暗号化で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。

この方式を初めて使うとき、設定ファイルの電話機証明書の MD5 ハッシュと、LSC または MIC の MD5 ハッシュが比較されます。 電話機で問題が検出されない場合、電話機は、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。 電話機で問題が検出された場合（ハッシュが一致しない、電話機に証明書が含まれていない、MD5 値がブランクであるなど）、CAPF 認証モードが [認証ストリング(By Authentication String)] でなければ、電話機は CAPF とのセッションを開始しようとします（[認証ストリング(By Authentication String)] の場合は、文字列を手動で入力する必要があります）。 Certificate Authority Proxy Function（CAPF）は、Cisco Unified Communications Manager に対して Cisco Unified IP Phone を認証し、電話機の証明書（LSC）を発行

します。 CAPF は、電話機の公開キーを LSC または MIC から抽出し、MD5 ハッシュを生成し、公開キーおよび証明書ハッシュの値を Cisco Unified Communications Manager データベースに格納します。 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存在するようになり、電話機がリセットされた後、電話機用の公開キーがあることをデータベースが TFTP に通知すると、対称キー暗号化処理が開始されます。 TFTP サーバは128ビット対称キーを生成します。これによって、設定ファイルは高度暗号化規格（AES）128暗号化アルゴリズムで暗号化されます。 次に、電話キー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。 電話機は、ファイルの署名を検証し、署名が有効である場合は、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、ファイルを暗号化する新しいキーを自動的に生成します。

ヒント この暗号化方式をサポートする電話機は、設定ファイルの暗号化設定フラグを使用して、暗号化されたファイルと暗号化されていないファイルのどちらを要求するかを決定します。[TFTP暗号化設定(TFTP Encrypted Config)] の設定が無効の場合、この暗号化方式をサポートする Cisco Unified IP Phone が暗号化されたファイル（.enc.sgn ファイル）を要求すると、Cisco Unified Communications Manager は「ファイルが見つかりません」エラーを電話機に送信します。 その後電話機は、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暗号化設定(TFTP Encrypted Config)] の設定が有効でも、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すると、TFTP サーバは最小限の設定項目を含む暗号化されていないファイルを提供します。 電話機は、最小限の設定を受信した後、エラー状態（キーの不一致など）を検出でき、CAPF とのセッションを開始して電話機の公開キーを Cisco Unified Communications Manager データベースと同期させることができます。 エラー状態が解消された場合、電話機は次回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

暗号化された設定ファイルをサポートする電話機モデル

次の Cisco Unified IP Phone で、電話機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
Cisco Unified IP Phone 7905G または 7912G（SIP のみ）	キーの手動配布：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：なし

電話機モデルとプロトコル	暗号化方式
Cisco Unified IP Phone 7940G または 7960G（SIP のみ）	キーの手動配布：暗号化アルゴリズム：高度暗号化規格（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機は、署名付きで暗号化された設定ファイルを受信するが、署名情報を無視
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	電話機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：あり

暗号化された設定ファイルの設定のヒント

[TFTP暗号化設定(TFTP Encrypted Config)] フラグを有効にして、電話機がダウンロードする設定ファイル内の機密データを保護することをお勧めします。 電話機に PKI 機能が備わっていない場合は、Cisco Unified Communications Managerの管理および電話機で対称キーを設定する必要もあります。 [TFTP暗号化設定(TFTP Encrypted Config)] フラグが設定されている場合、電話機または Cisco Unified Communications Manager で対称キーが欠落していたり、不一致が発生したりすると、電話機は登録できません。

Cisco Unified Communications Manager の管理ページ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する電話機のセキュリティ プロファイルだけに [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、および 7960G（SCCP のみ）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ため、これらの電話機に暗号化された設定ファイルを設定することはできません。

- [TFTP暗号化設定(TFTP Encrypted Config)] のデフォルト設定は、無効（オフ）です。 デフォルトの非セキュア プロファイルを電話機に適用すると、ダイジェスト信用証明書およびセキュア パスワードは暗号化されない状態で送信されます。
- 公開キー暗号化を使用する Cisco Unified IP Phone の場合、Cisco Unified Communications Manager で、暗号化された設定ファイルを有効にするために、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設定する必要はありません。 Cisco Unified Communications Manager は、登録中の公開キーをダウンロードするために CAPF プロセスを使用します。
- ご使用の環境がセキュアであることがわかっている場合、または PKI が有効でない電話機に対称キーを手動で設定することを避ける場合は、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することもできます。ただし、この方法はお勧めできません。
- Cisco Unified IP Phone 7905G、7912G、7940G、および 7960G（SIP のみ）の場合、Cisco Unified Communications Manager の管理に、ダイジェスト信用証明書を電話機に送信する方式として、暗号化された設定ファイルを使用するよりも簡単であるが安全性の低い方式が用意されています。 この方式は、[設定ファイル内のダイジェスト信用証明書を除外(Exclude Digest Credential in Configuration File)] 設定を使用します。これは、まず対称キーを設定して電話機に入力するという作業が不要であるため、ダイジェスト信用証明書の初期化に便利です。

この方式では、暗号化されていない設定ファイルで電話機にダイジェスト信用証明書を送信します。 電話機で信用証明書が受信された後、対応するセキュリティ プロファイル ウィンドウで TFTP ファイルの暗号化設定を無効のままにして、[設定ファイル内のダイジェスト信用証明書を除外(Exclude Digest Credential in Configuration File)] フラグを有効にすることをお勧めします。これによって、次回以降のダウンロードでダイジェスト信用証明書が除外されます。

これらの電話機にすでにダイジェスト信用証明書が存在しており、着信ファイルにダイジェスト信用証明書が含まれていない場合、既存の信用証明書が所定の場所に残ります。 ダイジェスト信用証明書は、電話機が工場出荷時の設定にリセットされるか、新しい信用証明書（ブランクを含む）を受信するまで、元の状態のまま残ります。

電話機ユーザまたはエンドユーザのダイジェスト信用証明書を変更した場合は、対応するセキュリティプロファイル ウィンドウでダイジェスト信用証明書を除外するフラグを一時的に無効にして、新しいダイジェスト信用証明書を電話機にダウンロードします。

暗号化設定ファイルの設定

次に、暗号化された設定ファイルを Cisco Unified Communications Manager の管理ページで設定する手順を示します。

手順

ステップ 1 クラスタ セキュリティ モードが混合モードに設定されていることを確認します。

（注） クラスタ セキュリティ モードは、クラスタまたはスタンドアロン サーバのセキュリティ機能を設定します。

ステップ 2 [電話セキュリティプロファイル(Phone Security Profile)] で [TFTP暗号化(TFTP Encrypted Config)] チェックボックスをオンにします。 必ず、このプロファイルを電話機に適用します。

ステップ 3 キーの手動配布をサポートする電話機、および電話機の公開キーによる対称キーの暗号化（PKI 暗号化）をサポートする電話機を確認します。

ステップ 4 使用中の電話機がキーの手動配布をサポートする場合は、キーの手動配布の作業を実行します。

ステップ 5 使用中の電話機がキーの手動配布をサポートする場合は、電話機に対称キーを入力し、電話機をリセットします。

ステップ 6 使用中の電話機が、電話機の公開キーによる対称キーの暗号化（PKI 暗号化）をサポートしている場合、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。

関連トピック

電話セキュリティ プロファイルの適用
電話機設定ファイルの暗号化の有効化, （7 ページ）
暗号化された設定ファイルの設定のヒント, （5 ページ）
電話機の対称キーの入力, （9 ページ）
キーの手動配布, （3 ページ）
電話機モデルのサポート
キーの手動配布の設定, （8 ページ）
LSC または MIC 証明書のインストールの確認, （10 ページ）

電話機設定ファイルの暗号化の有効化

TFTP サーバは、設定ファイルを構築するときに、データベースに問い合わせます。 電話機に適用されている電話セキュリティ プロファイルで TFTP 暗号化設定フラグが設定されている場合、TFTP サーバは暗号化された設定ファイルを構築します。

手順

ステップ 1 TFTP 暗号化設定フラグにアクセスするには、電話機の適切なデバイス セキュリティ プロファイルを検索します。

ステップ 2 設定ファイルの暗号化を有効にするには、[TFTP暗号化設定(TFTP Encrypted Config)] チェックボックスをオンにします。

関連トピック

電話セキュリティ プロファイルの検索
暗号化された電話機ファイルの設定の参考情報, （13 ページ）

キーの手動配布の設定

次に述べる手順では、以下の点を前提としています。

- 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 暗号化設定が有効にされている。

はじめる前に

使用中の電話機がキーの手動配布をサポートしているかどうかを確認します。

手順

ステップ 1 『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の説明に従って、電話機を検索します。

ステップ 2 [電話の設定(Phone Configuration)] ウィンドウが表示されたら、キーの手動配布の設定を行います。フィールドの説明については、キーの手動配布, （3 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。

関連トピック

暗号化された電話機ファイルの設定の参考情報, （13 ページ）

キーの手動配布の設定

次の表に、[電話の設定(Phone Configuration)] ウィンドウでの手動配布の設定項目を示します。

表 *1*：キーの手動配布の設定

設定項目	説明
[対称キー(Symmetric Key)]	対称キーに使用する 16 進文字の文字列を入力します。 数字の 0～9 と、大文字または小文字の英字（A～F または a～f）を使用できます。 キー サイズに対応した正しいビットを入力してください。そうでない場合、Cisco Unified Communications Manager は入力された値を拒否します。 Cisco Unified Communications Manager は次のキー サイズをサポートします。 • 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 キーを設定した後は、変更できません。
[文字列を生成(Generate String)]	Cisco Unified Communications Manager の管理ページで 16 進文字列を生成させる場合は、[文字列を生成(Generate String)] ボタンをクリックします。 キーを設定した後は、変更できません。
[データベース値を復元(Revert to Database Value)]	データベースに存在する値を復元する場合は、このボタンをクリックします。

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，（5 ページ）
詳細情報

電話機の対称キーの入力

Cisco Unified Communications Manager の管理ページでキーの手動配布を設定した後、電話機に対称キーを入力するには、次の手順を実行します。

手順

ステップ 1 電話機の [設定] 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、[設定] メニューを下方にスクロールし、電話のロック解除を強調表示して [選択] ソフトキーを押します。 電話機のパスワードをキー入力し、[承諾] 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。

ステップ 3 [設定] メニューを下方にスクロールし、[セキュリティ設定] を強調表示し、[選択] ソフトキーを押します。

ステップ 4 [セキュリティ設定] メニューで、[暗号キー設定項目] オプションを強調表示し、[選択] 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（16 進）を入力します。 キーをクリアする必要がある場合、ゼロを 32 回入力します。

ステップ 6 キーの入力が終了したら、[承諾] 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。

ステップ 7 電話機をリセットします。
電話機のリセット後、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

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。 使用中の電話機が、電話機の公開キーによる対称キーの暗号化（PKI 暗号化）方式をサポートす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, （4 ページ）を参照してください。

次の手順では、Cisco Unified Communications Manager データベースに電話機が存在し、Cisco Unified Communications Manager の管理ページで [TFTP暗号化設定(TFTP Encrypted Config)] パラメータを有効にした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)] ウィンドウの CAPF セクションで [トラブルシューティング(Troubleshoot)] オプションを選択することにより、LSC または MIC が電話機に存在することを Cisco Unified Communications Manager の管理ページで確認できます。 電話機に証明書が存在しない場合、[削除(Delete)] オプションと [トラブルシューティング(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調べる方法でも、電話機に LSC または MIC が存在するかどうか確認できます。 このバージョンの Cisco Unified Communications Manager をサポートする Cisco Unified IP Phone の詳細については、Cisco Unified IP Phone の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は、[電話の設定(Phone Configuration)] ウィンドウの 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 に関連したトピックを参照してください。

ステップ 3 CAPF 設定を定義した後、[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、暗号化された設定ファイルを TFTP サーバに要求します。

関連トピック

電話機モデルのサポート
暗号化された電話機ファイルの設定の参考情報, （13 ページ）

電話機設定ファイルの暗号化の確認

電話機設定ファイルを暗号化するときは、次の形式が使用されます。

- Cisco Unified IP Phone 7905G および 7912G（SIP のみ）：LD <MAC>.x
- Cisco Unified IP Phone 7940G および 7960G（SIP のみ）：SIP<MAC>.cnf.enc.sgn
- 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、および 8945。 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、7970G、7971G、7971G-GE、7975G、8941、8945、8961、9971、および 9971：SEP<MAC>.cnf.xml.enc.sgn。

電話機で設定ファイルにアクセスする方法の詳細については、暗号化とこのリリースの Cisco Unified Communications Manager をサポートする Cisco Unified IP Phone 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。

電話機設定ファイルの暗号化の無効化

電話機設定ファイルの暗号化を無効にするには、Cisco Unified Communications Manager の管理ページ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。

警告 SIP を実行する電話機のダイジェスト認証が有効になっていて、TFTP暗号化設定が無効になっている場合、ダイジェスト信用証明書は暗号化されずに送信されます。

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

Cisco Unified IP Phone 7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、および 7975G が暗号化されたファイル（.enc.sgn ファイル）を要求している場合、暗号化設定を更新して無効にすると、電話機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。

暗号化設定項目が [いいえ(False)] に更新されるときに 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-GE,7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945、8961、9971、および 9971 が暗号化されたファイルを要求した場合、電話機が次回リセットされたときに暗号化されていない設定ファイルを要求するように、管理者は電話機 GUI から対称キーを削除する必要があります。

ヒント Cisco Unified IP Phone 7940G および 7960G（SIP のみ）では、電話機 GUI で対称キーとして 32 バイトの 0 を入力して、暗号化を無効にします。 Cisco Unified IP Phone 7905G および 7912G（SIP のみ）では、電話機 GUI 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。

電話機設定ファイルのダウンロードからのダイジェスト信用証明書の除外

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信用証明書を除外するには、電話機に適用されるセキュリティ プロファイルの [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)] チェックボックスをオンにします。 Cisco Unified IP Phone 7905G、7912G、7940G、および 7960G（SIP のみ）だけが、このオプションをサポートしています。

ダイジェスト信用証明書を変更した場合は、このチェックボックスをオフにして、設定ファイルを更新する必要があります。

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，（5 ページ）
暗号化された電話機ファイルの設定の参考情報，（13 ページ）

暗号化された電話機ファイルの設定の参考情報

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, （4 ページ）
暗号化された設定ファイルの設定のヒント, （5 ページ）
暗号化設定ファイルの設定, （6 ページ）
キーの手動配布の設定, （8 ページ）
電話機の対称キーの入力, （9 ページ）
電話機設定ファイルの暗号化の確認, （11 ページ）
電話機設定ファイルの暗号化の無効化, （11 ページ）
電話セキュリティ プロファイルの設定のヒント