プロビジョニングメソッド

- BroadSoft サーバを使用した電話機のプロビジョニング （1 ページ）
- プロビジョニング例の概要 （2 ページ）
- 基本の再同期 （2 ページ）
- TFTP 再同期 （3 ページ）
- 固有のプロファイル、マクロ展開、および HTTP （7 ページ）
- デバイスの自動再同期 （10 ページ）
- アクティベーションコードのオンボーディング用に電話を設定する （20 ページ）
- お使いの電話機を企業の電話機に直接移行 （22 ページ）
- 承認失敗の再試行タイマーを設定する （23 ページ）
- セキュア HTTPS 再同期 （24 ページ）
- プロファイル管理 （32 ページ）
- 電話機のプライバシー ヘッダーの設定 （35 ページ）
- MIC 証明書の更新 （36 ページ）

BroadSoft サーバを使用した電話機のプロビジョニング

BroadSoft サーバユーザのみ。

Cisco IP マルチプラットフォームフォンを BroadWorks プラットフォームに登録することができます。

手順

ステップ 1 BroadSoft Xchange から、 CPEキットをダウンロードします。 最新の送付状キットを入手するには、 https://xchange.broadsoft.comに移動します。

ステップ 2 最新の DTAF ファイルを BroadWorks (システムレベル) サーバにアップロードします。

詳細については、(https://xchange.broadsoft.com/node/1031047)にアクセスします。 *BroadSoft* パートナー 設定ガイドにアクセスし、[*BroadWorks* デバイスプロファイルタイプの設定」セクションを参照してください。

ステップ 3 Broadworks デバイスプロファイルタイプを設定します。

デバイスプロファイルタイプを設定する方法の詳細については、次の URL を参照してください。

https://xchange.broadsoft.com/node/1031047. *BroadSoft* パートナー 設定ガイドにアクセスし、[*BroadWorks* デバイスプロファイルタイプの設定」セクションを参照してください。

プロビジョニング例の概要

この章では、電話機とプロビジョニング サーバの間で設定プロファイルを転送するための手順の例を示します。

設定プロファイルの作成については、プロビジョニング形式を参照してください。

基本の再同期

このセクションでは、電話機の基本の再同期機能をデモンストレーションします。

syslog を使用したメッセージの記録

情報を取得するには、電話機のウェブインターフェイスにアクセスして、**情報** > **デバッグ情報** > **制御ログ** を選択し、**メッセージ**をクリックします。

始める前に

手順

ステップ 1 syslog サーバをローカル PC にインストールし、有効化します。

ステップ 2 [システム（System）]タブをクリックし、ローカルの syslog サーバの値を Syslog_Server パラメータに入力します。

ステップ 3 TFTP 再同期 （3 ページ）の説明に従って再同期操作を繰り返します。

デバイスは、再同期中に 2 つの syslog メッセージを生成します。 最初のメッセージは、要求が進行中であることを示します。 2 番目のメッセージは、再同期の成功または失敗を示します。

ステップ 4 syslog サーバが次のようなメッセージを受信したことを確認します。

これらのメッセージの内容は、次のパラメータを使用して設定できます。

これらのパラメータのいずれかを無効にすると、対応する syslog メッセージは生成されません。

TFTP 再同期

電話機は、設定プロファイルを取得するための複数のネットワーク プロトコルをサポートします。 最も基本的なプロファイル転送プロトコルは、TFTP（RFC1350）です。 TFTP は、プライベート LAN ネットワーク内のネットワーク デバイスのプロビジョニングに広く使用されています。 TFTP は、インターネット経由のリモート エンドポイントの導入には推奨されませんが、小規模な組織内での導入、社内での事前プロビジョニング、および開発とテストで使用するには便利です。 社内での事前プロビジョニングの詳細については、社内デバイスの事前プロビジョニングを参照してください。 次の手順では、TFTP サーバからファイルをダウンロードした後、プロファイルを変更します。

手順

ステップ 1 LAN 環境内で、PC と電話機をハブ、スイッチ、または小型ルータに接続します。

ステップ 2 PC に、TFTP サーバをインストールしてアクティブにします。

ステップ 3 例に示すように、テキスト エディタを使用して、GPP_A の値を 12345678 に設定する設定プロファイルを作成します。

```
<flat-profile>
  <GPP_A> 12345678
  </GPP_A>
</flat-profile>
```

ステップ 4 プロファイルを `basic.txt` の名前で TFTP サーバのルート ディレクトリに保存します。

TFTP サーバが正しく設定されていることを確認できます。電話機以外の TFTP クライアントを使用して `basic.txt` ファイルを要求します。 プロビジョニング サーバとは異なるホストで実行されている TFTP クライアントを使用することをお勧めします。

ステップ 5 **[音声（Voice）] > [プロビジョニング（Provisioning）]**タブを選択し、汎用パラメータ GPP_A ～ GPP_P の値を確認します。 これらは空でなければなりません。

ステップ 6 Web ブラウザ ウィンドウで resync URL を開いて、テスト電話機を `basic.txt` 設定プロファイルと再同期します。

TFTP サーバの IP アドレスが 192.168.1.200 の場合、コマンドは次の例のようになります。

```
http://192.168.1.100/admin/resync?tftp://192.168.1.200/basic.txt
```

電話機がこのコマンドを受け取ると、アドレス 192.168.1.100 のデバイスは、IP アドレス 192.168.1.200 にある TFTP サーバに `basic.txt` ファイルを要求します。 次に、電話機はダウンロードしたファイルを解析して、GPP_A パラメータを値 12345678 で更新します。

ステップ 7 パラメータが正しく更新されたことを確認します。PC の Web ブラウザの設定ページを更新し、**[音声（Voice）]** > **[プロビジョニング（Provisioning）]** タブを選択します。

これで、GPP_A パラメータに値 12345678 が含まれます。

Syslog サーバへのログ メッセージ

パラメータを使用してsyslogサーバを電話機に設定している場合、再同期およびアップグレード操作のメッセージが syslog サーバに送信されます。 メッセージはリモート ファイル リクエストの開始時（設定プロファイルまたはファームウェアのロード）、および操作の完了時（成功または失敗を示す）に生成できます。

XML（cfg.xml）コードを使用して電話機構成ファイルのパラメータを設定することもできます。 各パラメータを設定するには、システム ログ パラメータ （5 ページ）の文字列のシンタックスを参照してください。

始める前に

- syslogサーバーがインストールおよび設定されます。
- 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

手順

ステップ 1 **[音声（Voice）]** > **[システム（System）]**をクリックします。

ステップ 2 **オプションのネットワーク設定**セクションで、**syslogサーバ**にサーバ IP を入力し、必要に応じて、システム ログ パラメータ （5 ページ）で定義したとおりに **syslog 識別子**を指定します。

ステップ 3 必要に応じて、システム ログ パラメータ （5 ページ）で定義されている **ログリクエスト Msg** 、**ログ成功Msg** 、および**ログ失敗 Msg** を使用して、syslogメッセージの内容を定義します。

Syslog メッセージの内容を定義するフィールドは、**[音声（Voice）]** > **[プロビジョン（Provisioning）]** タブの **[設定プロファイル（Configuration Profile）]** セクションにあります。 メッセージの内容を指定しない場合は、フィールドのデフォルトの設定が使用されます。 これらのパラメータのいずれかを無効にすると、対応する Syslog メッセージは生成されません。

ステップ 4 **すべての変更を送信** をクリックして変更を適用します。

ステップ 5 設定が有効であることを確認します。

a) TFTP 再同期を実行します。 TFTP 再同期 （3 ページ）を参照してください。

デバイスは、再同期中に 2 つの syslog メッセージを生成します。 最初のメッセージは、要求が進行中であることを示します。 2 番目のメッセージは、再同期の成功または失敗を示します。

b) syslog サーバが次のようなメッセージを受信したことを確認します。

```
CP-78xx-3PCC 00:0e:08:ab:cd:ef -- Requesting resync tftp://192.168.1.200/basic.txt

CP-88xx-3PCC 00:0e:08:ab:cd:ef -- Successful resync tftp://192.168.1.200/basic.txt
```

システム ログ パラメータ

次の表で、電話機のウェブページの **[音声（Voice）]** > **[システム（System）]** タブの下にある **[オプションネットワーク設定（Optional Network Configuration）]** セクションにおける、syslog パラメータの機能と使用方法を定義します。 また、パラメータを設定するために、XML コードを含む電話設定ファイルに追加される文字列のシンタックスも定義します。

表 1 : syslog パラメータ

パラメータ名	説明とデフォルト値
syslog サーバ	Phone システム情報や重大なイベントを記録するサーバを指定します。 デバッグ サーバと Syslog サーバの両方が指定されている場合、Syslog メッセージもデバッグ サーバに記録されます。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Syslog_Server ua="na">10.74.30.84</Syslog_Server>` • **電話機のウェブページ**で、Syslog サーバを指定します。

パラメータ名	説明とデフォルト値
Syslog 識別子	syslog サーバにアップロードされる syslog メッセージに含めるデバイス識別子を選択します。デバイス識別子は、各メッセージのタイムスタンプの後に表示されます。 識別子のオプションは次のとおりです。 • 無し：デバイス ID がありません。 • $MA：電話の MAC アドレス。連続した小文字と数字で表されます。例：`c4b9cd811e29` • $MAU：電話の MAC アドレス。連続した大文字と数字で表されます。例：`C4B9CD811E29` • $MAC：コロンで区切られた標準形式の電話機の MAC アドレス。 例：`c4:b9:cd:81:1e:29` • $SN：電話の製品シリアル番号。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Syslog_Identifier ua="na">$MAC</Syslog_Identifier>` • **電話機のウェブページ**で、リストから識別子を選択します。 デフォルト：なし
[ログ要求メッセージ（Log Request Msg）]	再同期の試行開始時に syslog サーバに送信されるメッセージ。 値が指定されていない場合、syslog メッセージは生成されません。 デフォルト値は、 `$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH`です • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Log_Request_Msg ua="na">$PN $MAC -- Requesting resync $SCHEME://$SERVIP:$PORT$PATH</Log_Request_Msg>`
[ログ成功メッセージ（Log Success Msg）]	再同期の試行が正常に完了した時点で発行される syslog メッセージ。 値が指定されていない場合、syslog メッセージは生成されません。 **XML（cfg.xml）を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。`<Log_Success_Msg ua="na">$PN $MAC -- Successful resync $SCHEME://$SERVIP:$PORT$PATH</Log_Success_Msg>`

パラメータ名	説明とデフォルト値
[ログ失敗メッセージ（Log Failure Msg）]	再同期の試行が失敗した後に発行される syslog メッセージ。 値が指定されていない場合、syslog メッセージは生成されません。 デフォルト値は `$PN $MAC -- Resync failed: $ERR` です。 **XML（cfg.xml）を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。`<Log_Failure_Msg ua="na">$PN $MAC -- Resync failed: $ERR</Log_Failure_Msg>`

固有のプロファイル、マクロ展開、および HTTP

各電話機の User_ID や Display_Name などのパラメータに個別の値を指定する必要がある導入では、サービスプロバイダーが、導入されるデバイスごとに固有のプロファイルを作成し、プロビジョニング サーバでそれらのプロファイルをホストできます。 事前に決定されたプロファイルの命名規則に従って、各電話が次々に独自のプロファイルと再同期されるよう設定する必要があります。

組み込み変数のマクロ展開を使用して、プロファイルの URL シンタックスに、MAC アドレスやシリアル番号など、各電話機に固有の識別情報を含めることができます。 マクロ展開によって、各プロファイル内の複数の場所でこれらの値を指定する必要がなくなります。

電話機にルールが適用される前に、プロファイル ルールでマクロ展開が実行されます。 マクロ展開は、次のように値の数を制御します。

- $MA は、ユニットの 12 桁の MAC アドレス（小文字の 16 進を使用して）に展開されます。 たとえば、000e08abcdef となります。
- $SN はユニットのシリアル番号に展開されます。 たとえば、88012BA01234 となります。

すべての汎用パラメータ（GPP_A ～ GPP_P）を含む他の値はこの方法でマクロ展開されます。このプロセスの例については、TFTP 再同期 （3 ページ）を参照してください。 マクロ展開は URL ファイル名に限定されず、プロファイル ルール パラメータの任意の部分にも適用できます。 これらのパラメータは、$A ～ $P として参照されます。 マクロ展開で使用可能な変数の一覧については、マクロ展開変数を参照してください。

この演習では、電話機に固有のプロファイルが TFTP サーバ上でプロビジョニングされます。

TFTP サーバ上の特定のIPフォン プロファイルのプロビジョニング

手順

ステップ 1 製品ラベルから電話機の MAC アドレスを取得します（MAC アドレスは、000e08aabbcc など、数字と小文字の 16 進数を使用する数値です）。

ステップ 2 TFTP サーバの仮想ルート ディレクトリに新しいファイルを移動します。

ステップ 3 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

ステップ 4 **[音声（Voice）] > [プロビジョニング（Provisioning）]** を選択します。

ステップ 5 [すべての変更の送信（Submit All Changes）]をクリックします。 これにより、リブートと再同期がすぐに行われます。

次に再同期が実行されると、電話機は $MA マクロ式をその MAC アドレスに展開して新しいファイルを取得します。

HTTP GET 再同期

HTTP は TCP 接続を確立し、TFTP は信頼性の低い UDP を使用しているため、HTTP は TFTP よりも信頼性の高い非同期メカニズムを提供します。 また、HTTP サーバは、TFTP サーバに比べてフィルタリングとロギングの機能が改善されています。

クライアント側では、HTTP を使用して再同期するためにサーバに特別な設定は不要です。 GET メソッドで HTTP を使用するための Profile_Rule パラメータ シンタックスは、TFTP に使用するシンタックスに似ています。 標準規格の Web ブラウザが HTTP サーバからプロファイルを取得できる場合、電話機も同じ動作を実行できる必要があります。

HTTP GET を使用した再同期

手順

ステップ 1 ローカル PC または他のアクセス可能なホストに HTTP サーバをインストールします。

オープン ソースの Apache サーバをインターネットからダウンロードできます。

ステップ 2 `basic.txt` 設定プロファイル（TFTP 再同期 （3 ページ）を参照）をインストールしたサーバの仮想ルート ディレクトリにコピーします。

ステップ 3 適切なサーバのインストールと `basic.txt` へのファイル アクセスを確認するには、Web ブラウザを使用してプロファイルにアクセスします。

ステップ 4 プロファイルが定期的にダウンロードできるようにするために、テスト用電話機の Profile_Rule を変更して TFTP サーバの代わりに、HTTP サーバを指すようにします。

たとえば、HTTP サーバが 192.168.1.300 とした場合、次の値を入力します。

```
<Profile_Rule>
http://192.168.1.200/basic.txt
</Profile_Rule>
```

ステップ 5 [すべての変更の送信（Submit All Changes）]をクリックします。 これにより、リブートと再同期がすぐに行われます。

ステップ 6 電話機から送信する syslog メッセージを確認します。 定期的な再同期で、HTTP サーバからプロファイルが取得されるようになります。

ステップ 7 HTTP サーバのログで、テスト用電話機を識別する情報がユーザエージェントのログにどのように表示されるのか確認します。

この情報には、製造者、製品名、現在のファームウェアバージョン、およびシリアル番号を含める必要があります。

Cisco XML を介したプロビジョニング

電話機ごとに（ここでは xxxx と表される）、Cisco XML の機能を介してプロビジョニングされます。

XML オブジェクトを SIP Notify パケットにより電話機に送信するか、HTTP Post を使用して電話機の CGI インターフェイス `http://IPAddressPhone/CGI/Execute` に送信できます。

CP-xxxx-3PCC では、Cisco XML 機能が拡張され、XML オブジェクトを介したプロビジョニングがサポートされます。

```
<CP-xxxx-3PCCExecute>
        <ExecuteItem URL=Resync:[profile-rule]/>
</CP-xxxx-3PCCExecute>
```

電話機は XML オブジェクトを受け取ると、プロビジョニング ファイルを [profile-rule] からダウンロードします。 このルールでは、マクロを使用して XML サービス アプリケーションの開発を容易にできます。

マクロ展開を使用した URL 解決

複数のプロファイルがあるサーバ上のサブディレクトリは、導入された多数のデバイスを管理するのに便利です。 プロファイルの URL には、次を含めることができます。

- プロビジョニング サーバ名または明示的な IP アドレス。 プロファイルで、プロビジョニング サーバが名前で識別される場合、電話機は DNS ルックアップを使用して名前を解決します。
- サーバ名の後に標準シンタックス `:port` を使用して、URL で指定される非標準サーバ ポート。
- 標準 URL 表記を使用して指定され、マクロ展開で管理される、プロファイルが保存されているサーバ仮想ルート ディレクトリのサブディレクトリ。

たとえば、次の Profile_Rule は、ポート 6900 の接続をリスニングしているホスト prov.telco.com で実行中の TFTP サーバに対し、サーバ サブディレクトリ `/cisco/config` 内のプロファイル ファイル（$PN.cfg）を要求します。

```
<Profile_Rule>
tftp://prov.telco.com:6900/cisco/config/$PN.cfg
```

```
</Profile_Rule>
```

各電話機のプロファイルは汎用パラメータで識別できます。その値は、マクロ展開を使用して共通のプロファイル ルール内で参照されます。

たとえば、GPP_B が `Dj6Lmp23Q` として定義されているとします。

Profile_Rule は次の値になります。

```
tftp://prov.telco.com/cisco/$B/$MA.cfg
```

デバイスが再同期されて、マクロが展開されると、000e08012345 の MAC アドレスを持つ電話機は、次の URL にデバイスの MAC アドレスを含む名前を持つプロファイルを要求します。

```
tftp://prov.telco.com/cisco/Dj6Lmp23Q/000e08012345.cfg
```

デバイスの自動再同期

デバイスは、（エンドポイントに明示的な再同期要求を送信するのではなく）定期的にプロビジョニング サーバと再同期することで、サーバ上で行われたすべてのプロファイル変更をエンドポイント デバイスに確実に伝達できます。

電話機をサーバと定期的に再同期させるためには、設定プロファイルの URL を Profile_Rule パラメータを使用して定義し、再同期期間を Resync_Periodic パラメータを使用して定義します。

始める前に

電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

手順

ステップ 1 **[音声（Voice）] > [プロビジョニング（Provisioning）]** を選択します。

ステップ 2 Profile_Rule パラメータを定義します。 この例では、TFTP サーバの IP アドレスを 192.168.1.200 とします。

ステップ 3 [定期再同期（Resync Periodic）]フィールドに、**30** 秒など、テスト用の小さい値を入力します。

ステップ 4 [すべての変更の送信（Submit All Changes）]をクリックします。

新しいパラメータ設定で、電話機は URL で指定された設定ファイルに対して 1 分間に 2 回再同期を行います。

ステップ 5 syslog トレースで結果のメッセージを確認します（syslog を使用したメッセージの記録 （2 ページ）セクションを参照）。

ステップ 6 [リセット時の再同期（Resync On Reset）]フィールドが [はい（Yes）]に設定されます。

```
<Resync_On_Reset>Yes</Resync_On_Reset>
```

ステップ 7 電源を再投入して、電話機をプロビジョニング サーバと強制的に再同期させます。

サーバが応答していないなど、何らかの理由で再同期操作が失敗する場合、ユニットは（[再同期エラー再試行遅延（Resync Error Retry Delay）]で設定された秒数）待機した後、再同期を再試行します。 [再同期エラー再試行遅延（Resync Error Retry Delay）]が 0 の場合、電話機は再同期が失敗した後に再同期を試行しません。

ステップ 8 （オプション）[再同期エラー再試行遅延（Resync Error Retry Delay）]フィールドの値を **30** などの小さい数に設定します。

```
<Resync_Error_Retry_Delay>30</Resync_Error_Retry_Delay>
```

ステップ 9 TFTP サーバを無効にして、syslog 出力で結果を確認します。

プロファイルの再同期パラメータ

次の表で、電話ウェブページの **[音声（Voice）]** > **[プロビジョニング（Provisioning）]** タブの下にある **[設定プロファイル（Configuration Profile）]** セクションにおける、プロファイル再同期パラメータの機能と使用方法を定義します。 また、パラメータを設定するために、XML コードを含む電話設定ファイルに追加される文字列のシンタックスも定義します。

パラメータ	説明
[プロビジョン有効（Provision Enable）]	再同期操作設定を許可または拒否します。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Provision_Enable ua="na">可</Provision_Enable>` • **電話機のウェブページ**で、再同期操作を許可する場合は**[はい（Yes）]**を、ブロックする場合は **[いいえ（Yes）]** を設定します。 デフォルト：はい（Yes）

パラメータ	説明
[リセット時の再同期（Resync On Reset）]	電源を入れた後やアップグレードを試行した後に、電話機がプロビジョニングサーバで設定を再同期するかどうかを指定します。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Resync_On_Reset ua="na">可</Resync_On_Reset>` • **電話機のウェブページ**で、このフィールドを **[はい（Yes）]** に設定すると、起動時またはリセット時に再同期が可能になり、また、**[いいえ（No）]** を設定すると、それを拒否します。 デフォルト：はい（Yes）
[再同期ランダム遅延（Resync Random Delay）]	多数のデバイスの電源が同時に投入され、初期設定が試行された場合のプロビジョニング サーバの過負荷状態を回避します。 この遅延は、デバイスの電源投入時またはリセット後の最初の設定試行時にのみ有効になります。 このパラメータは、プロビジョニングサーバに接続する前にデバイスが待機する最大時間間隔です。 実際の遅延は、0 ~ この値の範囲の擬似乱数です。 このパラメータの単位は 20 秒です。 有効値は 0 から 65535 の範囲です。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Resync_Random_Delay ua="na">2</Resync_Random_Delay>` • **電話機のウェブページ**で、電話機が起動またはリセット後の再同期を遅延させるために、0 ~ 65535 の秒単位のユニット数（20 秒）を指定します。 デフォルト値は 2 (40 秒) です。

パラメータ	説明
[再同期時刻（HHmm）（Resync At (HHmm)）]	電話機をプロビジョニング サーバと再同期する時間（HHmm）。 このフィールドの値は、HHmm 形式で時刻を示すために 0000 から 2400 までの範囲の 4 桁の数字でなければなりません。 たとえば、0959 は 09:59 を示します。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Resync_At__HHmm_ ua="na">0959</Resync_At__HHmm_>` • **電話機のウェブページ**で、電話機の再同期を開始する時間を HHMM 形式で指定します。 デフォルト値は空です。 値が無効な場合、パラメータは無視されます。このパラメータに有効な値が設定される場合、**定期再同期（Resync Periodic**）パラメータが無視されます。
[再同期時刻ランダム遅延（Resync At Random Delay）]	多数のデバイスの電源が同時に起動するときの、プロビジョニング サーバの過負荷状態を回避できます。 複数の電話機からサーバへの再同期要求のフラッディングを回避するために、電話機は、時間と分の範囲と、時間と分およびランダム遅延（hhmm、hhmm+random_delay）を再同期します。 たとえば、ランダム遅延 =（ランダム遅延での再同期 + 30）/60 分である場合、秒単位の入力値が分に変換され、次の分に切り上げられて、最終的な random_delay 間隔が計算されます。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Resync_At_Random_Delay ua="na">600</Resync_At_Random_Delay>` • **電話機のウェブページ**で、期間を秒単位で指定します。 有効値は 600 から 65535 の範囲です。 値が 600 未満の場合、ランダム遅延内部は 0 ~ 600 です。 デフォルト値は 600 秒（10 分）です。

パラメータ	説明
[定期再同期（Resync Periodic）]	プロビジョニング サーバでの定期的な再同期の時間間隔。 サーバで同期が最初に成功した後にのみ関連付けられている再同期タイマーがアクティブになります。 有効なフォーマットは以下のとおりです。 • 整数 例：の入力 **3000** 次の再同期が 3000 秒以内に行われることを示します。 • 複数の整数 例：入力値 **600、1200、300** は、最初の再同期が 600 秒後に行われ、2 番目の再同期は最初の再同期から 1200 秒後に行われ、3 番目の再同期は 2 番目の再同期から 300 秒後に行われることを示します。 • 時間範囲 例、入力値 **2400 + 30** は、再同期が成功した後、2400 秒から 2430 秒後に次の再同期が行われることを示します。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Resync_Periodic ua="na">3600</Resync_Periodic>` • **電話機のウェブページ**で、期間を秒単位で指定します。 定期再同期を無効にするには、このパラメータを 0 に設定します。 デフォルト値は 3600 秒です。

パラメータ	説明
[再同期エラー再試行遅延（Resync Error Retry Delay）]	電話機がサーバからプロファイルを取得できなかった、ダウンロードしたファイルが破損している、あるいは内部エラーが発生しているために再同期操作が失敗した場合、電話機はここで指定した時間（秒単位）が経過した後に再同期を再試行します。 有効なフォーマットは以下のとおりです。 • 整数 例: **300**の入力は、次の再試行が 300 秒で発生することを示しています。 • 複数の整数 例：入力値 **600、1200、300** は、最初の再試行が失敗から 600 秒後に行われ、2回目の再試行が最初の再試行の失敗から1200秒後に行われ、3 回目の再試行が 2 回目の再試行の失敗から 300 秒後に行われることを意味します。 • 時間範囲 たとえば、入力値**2400 + 30** は、再同期の失敗後、2400 秒から 2430 秒後に次の再試行が行われることを示します。 遅延が 0 に設定されている場合、デバイスは再同期が失敗しても、再同期を再試行しません。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Resync_Error_Retry_Delay ua="na">60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400</Resync_Error_Retry_Delay>` • **電話機のウェブページ**で、期間を秒単位で指定します。 デフォルト:60,120,240,480,960,1920,3840,7680,15360,30720,61440,86400

パラメータ	説明
[強制再同期遅延（Forced Resync Delay）]	電話機が再同期を実行するまでの待機時間の最大遅延（秒単位）。 電話回線のいずれかがアクティブな間、デバイスは再同期しません。再同期には数秒かかるため、デバイスが長時間アイドルになるまで待機してから再同期することをお勧めします。これにより、ユーザは中断することなく通話できます。 デバイスには、すべての回線がアイドル状態になったときにカウントダウンを開始するタイマーがあります。このパラメータは、カウンタの初期値です。再同期イベントは、このカウンタが 0 になるまで遅延します。 有効値は 0 から 65535 の範囲です。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Forced_Resync_Delay ua="na">14400</Forced_Resync_Delay>` • **電話機のウェブページ**で、期間を秒単位で指定します。 デフォルト値は 14,400 秒です。
[SIPからの再同期（Resync From SIP）]	サービス プロバイダーのプロキシ サーバから電話機に送信される SIP NOTIFY イベント経由の再同期操作に対するリクエストを制御します。有効にされた場合は、プロキシが Event: resync ヘッダーを含む SIP NOTIFY メッセージをデバイスに送信することによって、再同期を要求できます。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Resync_From_SIP ua="na">可</Resync_From_SIP>` • **電話機のウェブページで、[はい（Yes）]** を選択してこの機能を有効にし、**[いいえ（No）]** を選択して無効にします。 デフォルト：はい（Yes）
[アップグレード試行後の再同期（Resync After Upgrade Attempt）]	アップグレードの実行後の再同期操作を有効または無効にします。**[はい（Yes）]** を選択すると、ファームウェアアップグレード後に同期がトリガーされます。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Resync_After_Upgrade_Attempt ua="na">可 </Resync_After_Upgrade_Attempt>` • **電話機のウェブページ**で、ファームウェアアップグレード後に再同期をトリガーする場合は**[はい（Yes）]** を、再同期しない場合は**[いいえ（no）]** を選択します。 デフォルト：はい（Yes）

パラメータ	説明

[再起動トリガー1（Resync Trigger 1）]
[再起動トリガー2（Resync Trigger 2）]
	これらのパラメータの論理式が FALSE と評価した場合、**[リセット時の再同期（Resync On Reset）]** が **TRUE** に設定されていても再同期はトリガーされません。 直接アクション URL と SIP 通知による再同期のみが、これらの再同期トリガーを無視します。
	このパラメータは、マクロ展開を行う条件式でプログラムできます。 有効なマクロ展開については、マクロ展開変数を参照してください。
	• **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。
	`<Resync_Trigger_1 ua="na">$UPGTMR gt 300 および $PRVTMR ge 600</Resync_Trigger_1>`
	`<Resync_Trigger_2 ua="na"/>`
	• **電話機のウェブページ**で、トリガーを指定します。
	デフォルト：空白

[ユーザ設定可能再同期（User Configurable Resync）]	ユーザが電話画面メニューから電話機を再同期できるようにします。 **[はい（Yes）]**に設定すると、ユーザは電話機からプロファイルルールを入力して電話機の設定を再同期できます。 [いいえ（No）] に設定した場合、**プロファイルルール**パラメータは、電話機画面メニューに表示されません。 **プロファイルルール**パラメータは、**アプリケーション** > **デバイスの管理下**では機能しません。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<User_Configurable_Resync ua="na">可</User_Configurable_Resync>` • **電話機のウェブページ**で、**[はい（Yes）]**を選択して電話メニューに**プロファイルルール**パラメーターを表示し、**[いいえ（No）]**を選択してこのパラメーターを非表示にします。 デフォルト：はい（Yes）

パラメータ	説明
[FNF時の再同期失敗（Resync Fails On FNF）]	通常、再同期は、要求されたプロファイルがサーバから受信されなかった場合に失敗と見なされます。このパラメーターは、この動作をオーバーライドします。**[いいえ（No）]**に設定すると、デバイスはサーバからのファイルが見つかりません（file-not-found）応答を正常な再同期として受け入れます。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Resync_Fails_On_FNF ua="na">可</Resync_Fails_On_FNF>` • **電話機のウェブページ**で、ファイルが見つかりません（file-not-found）という応答を失敗した再同期として受け取るには **[はい（Yes）]** を選択し、成功した再同期として受け取るには **[いいえ（No）]** を選択します。 デフォルト：はい（Yes）

パラメータ	説明
[プロファイル認証タイプ（Profile Authentication Type）]	プロファイル アカウントの認証に使用する認証情報を指定します。 次のオプションを使用できます。 • **[無効化（Disabled）]**：プロファイルアカウント機能を無効にします。この機能を無効にすると、**[プロファイル アカウントのセットアップ（Profile account setup）]** メニューは電話機の画面に表示されません。 • **[基本的な HTTP 認証（Basic HTTP Authentication）]**：HTTP ログイン資格情報は、プロファイル アカウントの認証に使用されます。 • **[XSI 認証（XSI Authentication）]**：XSI ログイン認証情報または XSI SIP認証情報は、プロファイルアカウントの認証に使用されます。 認証の資格情報は、電話機の **[XSI 認証タイプ（XSI Authentication Type）]**によって異なります。 • 電話機の **[XSI 認証タイプ（XSI Authentication Type）]** が**[ログイン認証情報（Login Credentials）]** に設定されている場合、XSI ログイン資格情報が使用されます。 • 電話機の **[XSI 認証タイプ（XSI Authentication Type）]** が **[SIP クレデンシャル（SIP Credentials）]**に設定されている場合、SIP 資格情報が使用されます。 • **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。 `<Profile_Authentication_Type ua="na">基本 Http 認証 </Profile_Authentication_Type>` • **電話機のウェブページ**で、電話機のプロファイルの再同期を認証するためのリストからオプションを選択します。 デフォルト：基本的な HTTP 認証

パラメータ	説明

[プロファイルルール（Profile Rule）]
[プロファイルルールB（Profile Rule B）]
[プロファイルルールC（Profile Rule C）]
[プロファイルルールD（Profile Rule D）]
	各プロファイルルールは、プロファイル（設定ファイル）を取得するソースを電話機に通知します。すべての再同期操作の間、電話機はすべてのプロファイルを順番に適用します。
	構成ファイルに AES-256-CBC 暗号化を適用する場合は、次のように **–キー**キーワード付きの暗号キーを指定します。
	[--key <encryption key>]
	オプションで暗号キーを二重引用符（"）で囲むことができます。
	• **XML (cfg.xml)を使用した電話機の設定ファイルでは**、次の形式で文字列を入力します。
	`<Profile_Rule ua="na">/$PSN.xml</Profile_Rule>`
	`<Profile_Rule_B ua="na"/>`
	`<Profile_Rule_C ua="na"/>`
	`<Profile_Rule_D ua="na"/>`
	• **電話機のウェブページ**で、プロファイルルールを指定します。
	デフォルト：**/$PSN.xml**

[使用するDHCPオプション（DHCP Option To Use）]	ファームウェアおよびプロファイルを取得するために使用される、コンマで区切られた DHCP オプション。 デフォルト：66,160,159,150,60,43,125
[使用するDHCPv6オプション（DHCPv6 Option To Use）]	ファームウェアおよびプロファイルを取得するために使用される、コンマで区切られた DHCP オプション。 デフォルト：17,160,159

アクティベーションコードのオンボーディング用に電話を設定する

ネットワークがアクティベーションコードオンボードを使用するように設定されている場合、新しい電話機を安全な方法で自動的に登録するように設定することができます。 一意の 16 桁のアクティベーションコードを生成し、各ユーザに提供します。ユーザがアクティベーションコードを入力すると、電話機が自動的に登録されます。 この機能は、ユーザが有効なアクティベーションコードを入力するまで電話機を登録できないため、ネットワークを安全に維持します。

アクティベーションコードは 1 回だけ使用でき、有効期限があります。 ユーザが期限切れのコードを入力すると、電話機は無効なアクティベーションコードと画面上に表示します。 この問題が発生した場合は、ユーザに新しいコードを提供します。

この機能は, ファームウェアリリース 11-2-3MSR1、BroadWorks アプリケーション サーバ リリース 22.0 (パッチ AP.as 22.0.1123。ap368163 およびその依存) で利用できます。 ただし、この機能を使用するために、旧バージョンのファームウェアで電話機を変更することができます。 これを行うには、次の手順を使用します。

始める前に

アクティベーションコード経由でオンボードをサポートできるようにactivation.webex.com サービスがファイアウォールを通過できることを確認します。

オンボード用のプロキシサーバーをセットアップする場合は、プロキシサーバーが正しく設定されていることを確認します。 プロキシサーバーをセットアップするを参照してください。

電話機のウェブページにアクセス 電話機 ウェブインターフェイスへのアクセス

手順

ステップ 1 電話機を工場出荷時の設定にリセットします。

ステップ 2 **音声** > **プロビジョニング** > **設定プロファイル**を選択します。

ステップ 3 表のアクティベーションコードのプロビジョニングパラメータ （21 ページ）説明に従って **プロファイルルール** フィールドにプロファイルルールを入力します。

ステップ 4 （任意） **ファームウェアアップグレード** セクションで、アクティベーションコードのプロビジョニングパラメータ （21 ページ）表の説明に従って **アップグレードルール**フィールドにアップグレードルールを入力します。

ステップ 5 すべての変更を送信します。

アクティベーションコードのプロビジョニングパラメータ

次の表で、電話ウェブページの **[音声（Voice）]** > **[プロビジョニング（Provisioning）]** タブの下にある **[設定プロファイル（Configuration Profile）]** セクションのアクティベーションコードパラメータの機能と使用方法を定義します。 また、パラメータを設定するために、XML コードを含む電話設定ファイルに追加される文字列のシンタックスも定義します。

パラメータ	説明

[プロファイルルール（Profile Rule）]
[プロファイルルールB（Profile Rule B）]
[プロファイルルールC（Profile Rule C）]
[プロファイルルールD（Profile Rule D）]
	順番に評価されるリモート設定プロファイル。各再同期操作で、別のサーバによって管理される可能性のある複数のファイルを取得できます。
	次のいずれかを実行します。
	• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。
	`<Profile_Rule ua="na">gds://</Profile_Rule>`
	• 電話機のウェブインターフェイスにおいて、次の形式で文字列を入力します。
	`gds://`
	デフォルト：/$PSN.xml

アップグレードルール	アップグレード条件と関連するファームウェアURLを定義するファームウェアアップグレードスクリプトを指定します。プロファイル ルールと同じシンタックスが使用されます。
	次のいずれかを実行します。
	• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。
	`<Upgrade_Rule ua="na">http://<server ip address>/ sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>`
	• 電話機のウェブインターフェイスで、アップグレードルールを次のように入力します。
	`protocol://server[:port]/profile_pathname`
	次に例を示します。
	`tftp://192.168.1.5/image/sip88xx.11-2-3MSR1-1.loads`
	プロトコルが指定されない場合、TFTP が選択されます。サーバー名を指定しない場合、URL をリクエストするホストがサーバー名として使用されます。ポートが指定されていない場合、デフォルトポートが使用されます（TFTP の場合は 69、HTTP の場合は 80、HTTPS の場合は 443）。
	デフォルト：空白

お使いの電話機を企業の電話機に直接移行

移行ファームウェアロードを使用せずに、1 つの手順で電話機を企業の電話機に簡単に移行することができます。

始める前に

電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

手順

ステップ 1 **[音声（Voice）]** > **[プロビジョニング（Provisioning）]** を選択します。

ステップ 2 **[アップグレードルール]** フィールドに、ファームウェアアップグレードスクリプトを入力して [アップグレードルール] パラメータを設定します。 構文の詳細については、「アップグレード条件と関連するファームウェア URL を定義する」を参照してください。 プロファイル ルールと同じシンタックスが使用されます。 スクリプトを入力し、次の形式を使用してアップグレードルールを入力します。

```
<tftp|http|https>://<ipaddress>/image/<load name>
```

次に例を示します。

```
tftp://192.168.1.5/image/sip78xx.14-1-1MN-366.loads
```

ステップ 3 サーバからライセンスを取得して承認する値を入力して、**移行承認ルール**パラメータを設定します。

次の形式で文字列を入力することによって、設定ファイル (cfg .xml) でこのパラメータを設定することもできます。

```
<Trans_Auth_Rule ua="na">http://10.74.51.81/prov/migration/E2312.lic</Trans_Auth_Rule>
```

ステップ 4 **[移行承認タイプ]** パラメータで、ライセンスタイプを **[従来の設定]** に設定します。

次の形式で文字列を入力することによって、設定ファイル (cfg .xml) でこのパラメータを設定することもできます。

```
<Trans_Auth_Type ua="na">Classic</Trans_Auth_Type>
```

ステップ 5 [すべての変更の送信（Submit All Changes）]をクリックします。

承認失敗の再試行タイマーを設定する

電話がライセンスアップグレードの承認に失敗した場合に、電話が認証を再試行するまでの時間間隔を設定できます。

始める前に

- 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。
- **[移行承認タイプ（Transition Authorization Type）]** が **[クラシック（Classic）]** に設定されていること。

手順

ステップ 1 **[音声（Voice）]** > **[プロビジョニング（Provisioning）]** を選択します。

ステップ 2 時間間隔を設定するには、**[移行承認エラー再試行遅延（Transition Authorization Error Retry Delay）]** フィールドに値（秒数）を追加します。

次の形式で文字列を入力することによって、設定ファイル (cfg .xml) でこのパラメータを設定することもできます。

<Transition_Authorization_Error_Retry_Delay>1800</Transition_Authorization_Error_Retry_Delay>

デフォルト：1800

ステップ 3 [すべての変更の送信（Submit All Changes）]をクリックします。

セキュア HTTPS 再同期

安全な通信プロセスを使用して再同期するために、電話機で以下の方法を使用できます。

- 基本の HTTPS 再同期
- クライアント証明書認証を使用した HTTPS
- HTTPS クライアントのフィルタリングとダイナミック コンテンツ

基本の HTTPS 再同期

HTTPS では、リモート プロビジョニングの HTTP に SSLが追加され、以下が可能になります。

- 電話機はプロビジョニング サーバを認証できます。
- プロビジョニング サーバは電話機を認証できます。
- 電話機とプロビジョニング サーバ間で交換される情報の機密性が確保されます。

SSL は、電話機とプロビジョニング サーバに事前にインストールされた公開キーと秘密キーのペアを使用して、各接続に対する秘密（対称）キーを生成し、電話機とプロビジョニング サーバ間で交換します。

クライアント側では、HTTPS を使用して再同期を可能にするためにサーバで特別な設定を行う必要はありません。 GET メソッドで HTTPS を使用するための Profile_Rule パラメータ シンタックスは、HTTP または TFTP に使用するシンタックスに似ています。 標準規格の Web ブラウザが HTTPS サーバからプロファイルを取得できる場合、電話機も同じ動作を実行できる必要があります。

HTTPS サーバのインストールに加えて、シスコが署名する SSL サーバ証明書は、プロビジョニング サーバにインストールする必要があります。 デバイスは、サーバがシスコが署名した

サーバ証明書を提供していない限り、HTTPS を使用しているサーバに再同期できません。 音声製品用の署名付き SSL 証明書を作成する手順は、https://supportforums.cisco.com/docs/DOC-9852 を参照してください。

基本の HTTPS 再同期による認証

手順

ステップ 1 通常のホスト名変換を使って、ネットワーク DNS サーバで IP アドレスが認識されているホストに HTTPS サーバをインストールします。

オープン ソースの Apache サーバは、オープン ソースの mod_ssl パッケージとともにインストールされる際、HTTPS サーバとして動作するように設定できます。

ステップ 2 サーバ用のサーバ証明書署名要求を生成します。 この手順では、オープン ソース OpenSSL パッケージまたは同等なソフトウェアのインストールが必要になる場合があります。 OpenSSL を使用している場合、基本の CSR ファイルを生成するコマンドは次のとおりです。

```
openssl req -new -out provserver.csr
```

このコマンドは公開キーと秘密キーのペアを生成します。それらのキーは`privkey.pem`ファイルに保存されます。

ステップ 3 CSR ファイル（provserver.csr）を署名のためにシスコに提出します。

署名されたサーバ証明書は、Sipura CA クライアント ルート証明書 spacroot.cert とともに返送（provserver.cert）されます。

詳細については、https://supportforums.cisco.com/docs/DOC-9852を参照してください。

ステップ 4 署名されたサーバ証明書、秘密キーのペア ファイル、およびクライアント ルート証明書をサーバの該当の場所に格納します。

Linux に Apache をインストールする場合、通常これらの場所は次のようになります。

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.cert
# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/pivkey.pem
# Certificate Authority:
SSLCACertificateFile /etc/httpd/conf/spacroot.cert
```

ステップ 5 サーバを再起動します。

ステップ 6 `basic.txt` 設定ファイル（TFTP 再同期 （3 ページ）を参照）を HTTPS サーバの仮想ルート ディレクトリにコピーします。

ステップ 7 ローカル PC から標準のブラウザを使用して HTTPS サーバから `basic.txt` をダウンロードし、サーバの適切な動作を確認します。

ステップ 8 サーバが提供するサーバ証明書を確認します。

ブラウザがシスコをルート CA として受け入れるように事前に設定されていない限り、ブラウザはおそらく証明書を認識しません。しかしながら、電話機では証明書がこの方法で署名されるものと想定されます。

HTTPS サーバへの参照を含むようにテストデバイスの Profile_Rule を次の例のように変更します。

```
<Profile_Rule>
https://my.server.com/basic.txt
</Profile_Rule>
```

この例では、HTTPS サーバの名前を **my.server.com** とします。

ステップ 9 [すべての変更の送信（Submit All Changes）]をクリックします。

ステップ 10 電話機から送信する syslog トレースを確認します。

syslog メッセージには、再同期で HTTPS サーバからプロファイルが取得されることが示される必要があります。

ステップ 11 （任意） 電話機のサブネットでイーサネット プロトコル アナライザを使用して、パケットが暗号化されていることを確認します。

この演習では、クライアント証明書の検証は有効化されていません。電話機とサーバ間の接続は暗号化されます。ただし、ファイル名とディレクトリの場所を知っている場合、どのクライアントでもサーバに接続してファイルを要求できるため、転送は安全ではありません。安全な再同期を行うため、クライアント証明書認証を使用した HTTPS （26 ページ）で説明されている演習に示すように、サーバはクライアントを認証する必要もあります。

クライアント証明書認証を使用した HTTPS

工場出荷時のデフォルト設定では、サーバはクライアントに SSL クライアント証明書を要求しません。 どのクライアントでもサーバに接続してプロファイルを要求できるため、プロファイルの転送は安全ではありません。 設定を編集してクライアント認証を有効にすることができます。サーバは接続要求を受け入れる前に電話機を認証するために、クライアント証明書が必要です。

この要件があるため、適切なクレデンシャルがないブラウザを使って再同期操作を個別にテストすることはできません。 テスト用電話機とサーバ間での HTTPS 接続内での SSL キー交換は ssldump ユーティリティで確認できます。 ユーティリティのトレースには、クライアントとサーバ間の相互通信が示されます。

クライアント証明書認証を使用したHTTPSを認証する

手順

ステップ1 HTTPS サーバでクライアント証明書認証を有効にします。

ステップ2 Apache（v.2）では、サーバ設定ファイルに次を設定します。

```
SSLVerifyClient  require
```

また、基本の HTTPS 再同期 （24 ページ）の演習で示されているように、spacroot.cert が格納されていることを確認します。

ステップ3 HTTPS サーバを再起動し、電話機の syslog トレースを確認します。

サーバと再同期するたびに対称認証が実行されるため、サーバ証明書とクライアント証明書の両方が検証されてから、プロファイルが転送されます。

ステップ4 ssldump を使用して、電話機と HTTPS サーバ間の再同期接続をキャプチャします。

クライアント証明書の検証がサーバで正しく有効化されている場合、ssldump トレースには、プロファイルを含む暗号化されたパケットの前に証明書が相互に交換されていることが示されます（最初にサーバからクライアントへ、次にクライアントからサーバへ）。

クライアント認証が有効な場合、有効なクライアント証明書と一致する MAC アドレスを持つ電話機のみが、プロビジョニング サーバにプロファイルを要求できます。 サーバは、通常のブラウザまたはその他の不正なデバイスからの要求を拒否します。

クライアントフィルタリングと動的コンテンツ用にHTTPSサーバーを設定する

HTTPS サーバがクライアント証明書を要求するよう設定されている場合、証明書の情報によって再同期している電話機を識別し、それに適切な設定情報を提供します。

HTTPS サーバは、証明書情報を、再同期要求の一部として呼び出される CGI スクリプト（またはコンパイルされた CGI プログラム）で利用可能にします。 例を示す目的で、この演習ではオープン ソースの Perl スクリプト言語を使用し、Apache（v.2）が HTTPS サーバとして使用されているものとします。

手順

ステップ1 HTTPS サーバを実行しているホストに Perl をインストールします。

ステップ2 次の Perl リフレクタ スクリプトを生成します。

```
#!/usr/bin/perl -wT
use strict;
print "Content-Type: text/plain\n\n";
print "<flat-profile><GPP_D>";

print "OU=$ENV{'SSL_CLIENT_I_DN_OU'},\n";
print "L=$ENV{'SSL_CLIENT_I_DN_L'},\n";
print "S=$ENV{'SSL_CLIENT_I_DN_S'}\n";
print "</GPP_D></flat-profile>";
```

ステップ 3 このファイルを `reflect.pl` のファイル名で HTTPS サーバの CGI スクリプトのディレクトリに、実行権限（Linux では chmod 755）で保存します。

ステップ 4 サーバ上の CGI スクリプトのアクセシビリティ（`/cgi-bin/...`）を確認します。

ステップ 5 次の例のように、テストデバイスで Profile_Rule を変更し、リフレクタ スクリプトと再同期させます。

```
https://prov.server.com/cgi-bin/reflect.pl?
```

ステップ 6 [すべての変更の送信（Submit All Changes）]をクリックします。

ステップ 7 syslog トレースで、再同期が成功していることを確認します。

ステップ 8 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

ステップ 9 **[音声（Voice）] > [プロビジョニング（Provisioning）]** を選択します。

ステップ 10 GPP_D パラメータに、スクリプトでキャプチャされた情報が含まれているか確認します。

テスト デバイスが製造者からの一意の証明書を保持する場合、この情報には製品名、MAC アドレス、およびシリアル番号が含まれます。ユニットがファームウェア リリース 2.0 より前に製造された場合、この情報には汎用文字列が含まれます。

同様のスクリプトによって、再同期しているデバイスに関する情報を判断してから、適切な設定パラメータ値を持つデバイスを提供できます。

HTTPS 証明書

電話機は、デバイスからプロビジョニング サーバへの HTTPS リクエストに基づく信頼性の高い安全なプロビジョニング戦略を提供します。 サーバ証明書とクライアント証明書の両方が、電話機からサーバ、およびサーバから電話機の認証に使用されます。

Cisco が発行した証明に加えて、電話機は、頻繁に使用される SSL 証明書プロバイダーからもサーバ証明書を受け入れます。

電話機で HTTPS を使用するには、証明書署名要求（CSR）を生成して、シスコに提出する必要があります。 電話機は、プロビジョニング サーバへのインストール用の証明書を生成します。 電話機は、プロビジョニング サーバとの HTTPS 接続を確立しようとするときに、この証明書を受け入れます。

HTTPS 方式

HTTPSは、クライアントとサーバ間の通信を暗号化して、他のネットワークデバイスからメッセージの内容を保護します。クライアントとサーバ間の通信本文の暗号化方式は、対称キー暗号化に基づいています。対称キー暗号化では、クライアントとサーバが、公開キーまたは秘密キーの暗号化によって保護される安全なチャネルで単一の秘密キーを共有します。

秘密キーで暗号化されたメッセージは、同じキーを使用しないと復号化できません。 HTTPSは、幅広い対称暗号化アルゴリズムをサポートしています。 電話機には、128 ビットの RC4に加えて、米国暗号化標準（AES）を使用した最大 256 ビットの対称暗号化が実装されています。

HTTPS では、安全なトランザクションで実行されるサーバとクライアントの認証も提供しています。 この機能により、プロビジョニング サーバと各クライアントは、ネットワーク上の他のデバイスによりスプーフィングされることはありません。 この機能は、リモート エンドポイントのプロビジョニングでは必須です。

サーバとクライアントの認証は、公開キーを含む証明書を使って、公開キーまたは秘密キーの暗号化により実行されます。公開キーで暗号化されたテキストは、対応する秘密キーでなければ復号化できません（その逆も同じです）。 電話機は、公開キーと秘密キーの暗号化でRivest-Shamir-Adleman（RSA）アルゴリズムをサポートします。

SSL サーバ証明書

安全な各プロビジョニング サーバには、シスコが直接署名したセキュア ソケット レイヤ（SSL）サーバ証明書が発行されます。 電話機で実行されるファームウェアは、シスコの証明書のみ有効な証明書として認識します。 クライアントは HTTPS を使用してサーバに接続すると、シスコで署名されていないサーバ証明書を拒否します。

この方法により、電話機への不正アクセスや、プロビジョニング サーバをスプーフィングする試みからサービス プロバイダーを保護します。 このような保護を行わないと、攻撃者は電話機を再プロビジョニングして構成情報を取得したり、別の VoIP サービスを使用する可能性があります。 有効なサーバ証明書に対応する秘密キーがない場合、攻撃者は電話機との通信を確立できません。

サーバ証明書の取得

手順

ステップ 1 シスコ サポートの証明書プロセス担当者にお問い合わせください。 特定のサポート担当者がいない場合は、要求を ciscosb-certadmin@cisco.com 宛てに送信してください。

ステップ 2 CSR（証明書署名要求）で使用される秘密キーを生成します。 このキーは秘密キーであるため、シスコ サポートに提供する必要はありません。 オープン ソース「openssl」を使用して、キーを生成します。 次に例を示します。

```
openssl genrsa -out <file.key> 1024
```

ステップ 3 組織と場所を識別するフィールドが含まれている CSR を生成します。 次に例を示します。

```
openssl req -new -key <file.key> -out <file.csr>
```

次の情報が必要です。

- 件名フィールド：共通名（CN）を入力します。FQDN（完全修飾ドメイン名）シンタックスにする必要があります。 電話機は、SSL 認証ハンドシェイク中に、受信した証明書がそれを提出したマシンからのものであるか確認します。
- サーバのホスト名：provserv.domain.com など。
- 電子メールアドレス：必要な場合にカスタマーサポートがユーザに連絡を取れる電子メール アドレスを入力します。 この電子メール アドレスは、CSR に表示されます。

ステップ 4 CSR（zip ファイル形式）をシスコのサポート担当者または ciscosb-certadmin@cisco.com 宛てに送信してください。 証明書はシスコによって署名されます。 シスコは、システムにインストールする証明書を送信します。

クライアント証明書

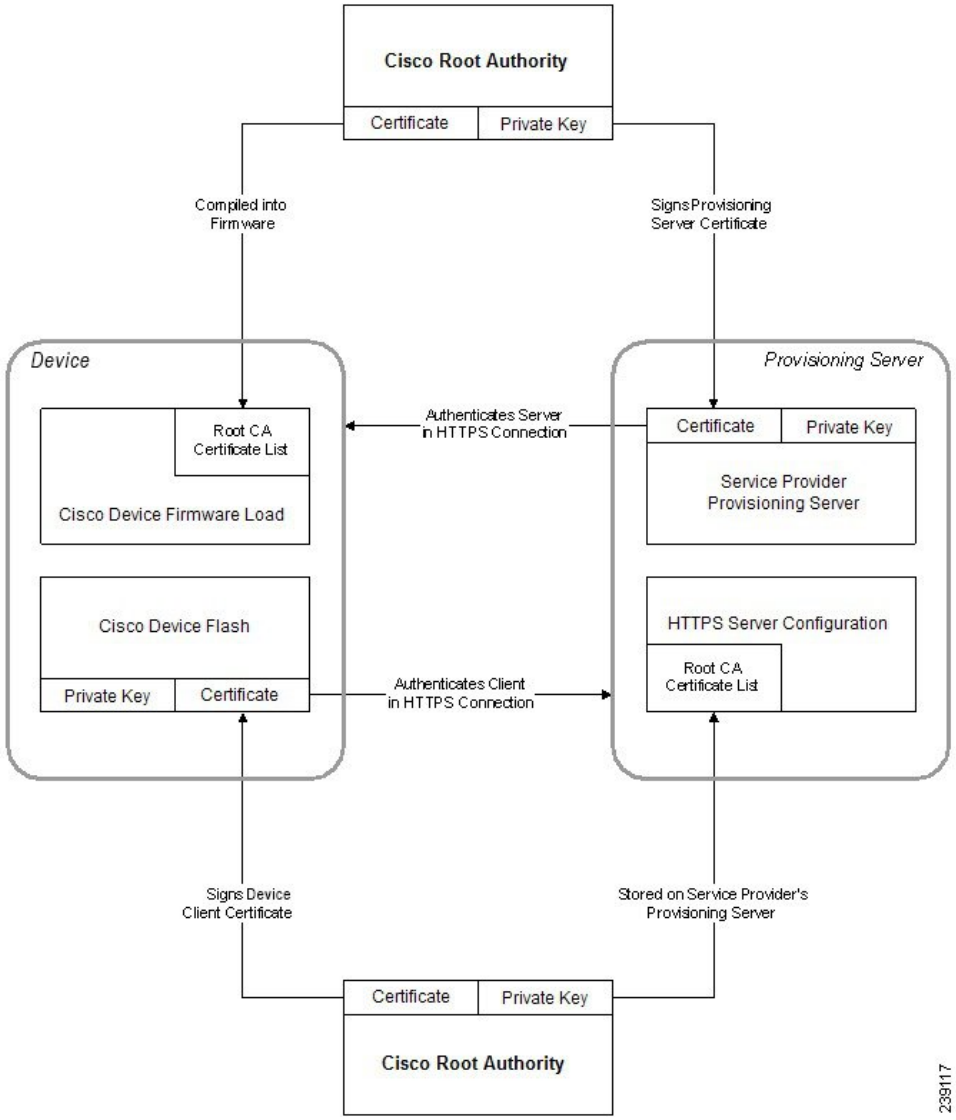
電話機に対する直接攻撃に加え、攻撃者は標準規格の Web ブラウザまたは別の HTTPS クライアントからプロビジョニング サーバにアクセスを試み、プロビジョニング サーバから設定プロファイルを取得する場合があります。 この種の攻撃を防ぐためには、各個々のエンドポイントに関する識別情報を含む、シスコが署名した一意のクライアント証明書を電話機でも伝送します。 デバイスのクライアント証明書を認証できる認証局ルート証明書は、各サービス プロバイダに与えられます。 この認証パスにより、プロビジョニング サーバは設定プロファイルの不正要求を拒否できます。

証明書の構造

サーバ証明書とクライアント証明書を組み合わせると、リモートの電話機とそのプロビジョニング サーバ間のセキュア通信が確保されます。 次の図は、シスコ クライアント、プロビジョニング サーバ、認証局における、証明書、公開キーと秘密キーのペア、および署名ルート認証局の関係と配置を示しています。

図の上半分は、個々のプロビジョニング サーバ証明書の署名に使用されるプロビジョニング サーバ ルート認証局を示しています。 該当するルート証明書はファームウェアにコンパイルされ、電話機は承認されたプロビジョニング サーバを認証できます。

図 *1* : 認証局のフロー



カスタム認証局の設定

デジタル証明書は、ネットワーク上のネットワークデバイスとユーザを認証するために使用できます。また、ネットワーク ノード間のIPSecセッションのネゴシエートにも使用できます。

サードパーティは認証局の証明書を使用して、通信しようとしている2つ以上のノードを検証して認証します。 各ノードが公開鍵と秘密鍵を保持します。 公開キーでデータを暗号化します。 秘密キーでデータを復号します。 これらのノードは同じ発行元から証明書を取得しているため、互いの身元を確認できます。

デバイスは、サード パーティ認証局（CA）によって提供されるデジタル証明書を使用してIPSec 接続を認証できます。

電話機は、ファームウェアに組み込まれて事前にロードされる、次の一連のルート認証局をサポートしています。

- Cisco Small Business CA 証明書
- CyberTrust CA 証明書
- Verisign CA 証明書
- Sipura ルート CA 証明書
- Linksys ルート CA 証明書

始める前に

電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセスを参照してください。

手順

ステップ 1 **[情報（Info）]** > **[ステータス（Status）]** を選択します。

ステップ 2 [カスタムCA情報（Custom CA Info）]までスクロールし、次のフィールドを参照します。

- [カスタムCAプロビジョニングステータス（Custom CA Provisioning Status）]：プロビジョニングのステータスを示します。
  - 最後のプロビジョニングが mm/dd/yyyy HH:MM:SS に成功した
  - 最後のプロビジョニングが mm/dd/yyyy HH:MM:SS に失敗した
- [カスタムCA情報（Custom CA Info）]：カスタム CA に関する情報を示します。
  - [インストール済み（Installed）]：「CN 値」が表示されます。ここで、「CN 値」は最初の証明書の件名フィールドの CN パラメータの値です。
  - [未インストール（Not Installed）]：カスタムの CA 証明書がインストールされていない場合に表示されます。

プロファイル管理

このセクションでは、ダウンロードの準備として設定プロファイルの構成について説明します。 機能を説明するために、ローカル PC からの TFTP を再同期方法として使用しますが、HTTP または HTTPS も使用できます。

gzip によるオープン プロファイルの圧縮

プロファイルですべてのパラメータが個別に指定されている場合、XML 形式の設定プロファイルが非常に大きくなる場合があります。 プロビジョニング サーバの負荷を減らすために、電話機は、gzip ユーティリティ（RFC 1951）がサポートするデフレート圧縮形式を使用して XML ファイルの圧縮をサポートします。

（注） 圧縮および暗号化された XML プロファイルを電話機で認識できるように、暗号化の前に圧縮を実行する必要があります。

カスタマイズされたバックエンドプロビジョニング サーバ ソリューションに統合するために、オープン ソース zlib 圧縮ライブラリをスタンドアロン gzip ユーティリティの代わりに使用して、プロファイルの圧縮を実行できます。 ただし、電話機には有効な gzip ヘッダーを含むファイルが必要です。

手順

ステップ 1 ローカル PC に gzip をインストールします。

ステップ 2 コマンド ラインから gzip を呼び出して、`basic.txt` 設定プロファイル（TFTP 再同期 （3 ページ）を参照）を圧縮します。

```
gzip basic.txt
```

これにより、デフレートされたファイル `basic.txt.gz` が生成されます。

ステップ 3 TFTP サーバの仮想ルート ディレクトリに `basic.txt.gz` ファイルを保存します。

ステップ 4 次の例に示すように、テスト デバイスで Profile_Rule を変更して、元の XML ファイルの代わりにデフレートされたファイルと再同期します。

```
tftp://192.168.1.200/basic.txt.gz
```

ステップ 5 **Submit All Changes** をクリックします。

ステップ 6 電話機から syslog トレースを確認します。

再同期するときに、電話機は新しいファイルをダウンロードしてパラメータの更新に使用します。

OpenSSL によるプロファイルの暗号化

圧縮または圧縮解除されたプロファイルを暗号化することができます（ただし、ファイルは暗号化する前に圧縮する必要があります）。 暗号化は、電話機とプロビジョニング サーバ間の

通信に TFTP または HTTP を使用する場合など、プロファイル情報の機密性が特に重要な場合に役に立ちます。

電話機は、256 ビットの AES アルゴリズムを使用して対称キーの暗号化をサポートします。この暗号化は、オープン ソースの OpenSSL パッケージを使用して実行できます。

手順

ステップ 1 ローカル PC に OpenSSL をインストールします。 ここで、AES を有効にするために OpenSSL アプリケーションの再コンパイルが必要な場合があります。

ステップ 2 `basic.txt` 設定ファイル（TFTP 再同期 （3 ページ）を参照）を使用して、暗号化されたファイルを次のコマンドで生成します。

```
>openssl enc -aes-256-cbc -k MyOwnSecret -in basic.txt -out basic.cfg
```

XML プロファイルは圧縮と暗号化の両方が可能なため、gzip によるオープン プロファイルの圧縮 （33 ページ）で作成した圧縮済み `basic.txt.gz` ファイルも使用できます。

ステップ 3 暗号化された `basic.cfg` ファイルを TFTP サーバの仮想ルート ディレクトリに保存します。

ステップ 4 テスト デバイスで Profile_Rule を変更して、元の XML ファイルの代わりに暗号化されたファイルと再同期します。 暗号キーは、次の URL オプションで電話機に認識されます。

```
[--key MyOwnSecret ] tftp://192.168.1.200/basic.cfg
```

ステップ 5 [すべての変更の送信（Submit All Changes）]をクリックします。

ステップ 6 電話機から syslog トレースを確認します。

再同期するときに、電話機は新しいファイルをダウンロードしてパラメータの更新に使用します。

パーティション化されたプロファイルの作成

電話機では、再同期ごとに複数の個別のプロファイルがダウンロードされます。 この方法により、個別サーバに関するさまざまな種類のプロファイル情報を管理し、アカウント固有の値とは異なる共通の設定パラメータ値をメンテナンスできます。

手順

ステップ 1 以前の演習とは異なる値をパラメータに指定する新しいXMLプロファイル`basic2.txt`を作成します。 たとえば、`basic.txt` プロファイルに次を追加します。

```
<GPP_B>ABCD</GPP_B>
```

ステップ 2 TFTP サーバの仮想ルート ディレクトリに basic2.txt プロファイルを保存します。

ステップ 3 以前の演習で使用した最初のプロファイル ルールはフォルダに残しますが、新しいファイルを指す 2 番目のプロファイル ルール（Profile_Rule_B）を設定します。

```
<Profile_Rule_B>tftp://192.168.1.200/basic2.txt
</Profile_Rule_B>
```

ステップ 4 [すべての変更の送信（Submit All Changes）]をクリックします。

電話は、再同期操作の時間になるたびに、1 番目と 2 番目のプロファイルの両方に、その順序で再同期します。

ステップ 5 syslog トレースを確認して、予想される動作を確認します。

電話機のプライバシー ヘッダーの設定

SIP メッセージのユーザ プライバシー ヘッダーにより、信頼されたネットワークからのユーザ プライバシーのニーズが設定されます。

ユーザ プライバシー ヘッダーの値は、config.xml ファイルで XML タグを使用して、回線の内線番号ごとに設定できます。

プライバシー ヘッダーのオプションを次に示します。

- [無効(Disabled)]（デフォルト）
- none：ユーザは、プライバシー サービスがこの SIP メッセージにプライバシー機能を適用しないように要求します。
- header：ユーザは識別情報を削除できないヘッダーを隠すためにプライバシー サービスを必要とします。
- session：ユーザは、プライバシー サービスがこのセッションに匿名性を提供するように要求します。
- user：ユーザは、仲介者によってのみプライバシー レベルを要求します。
- id：ユーザは IP アドレスまたはホスト名を明らかにしない ID を代わりに使用するようにシステムに要求します。

手順

ステップ 1 テキスト エディタまたは XML エディタで電話機の config.xml ファイルを編集します。

ステップ 2 **<Privacy_Header_N_ ua="na">*Value*</Privacy_Header_N_>** タグを挿入します。ここで、N は回線の内線番号（1 ～ 10）で、次のいずれかの値を使用します。

- デフォルト値：**Disabled**
- **なし**
- **ヘッダー**
- **セッション**
- **ユーザ**
- **id**

ステップ 3 （任意）同じタグを使用する追加の内線を、必要な内線番号を使用してプロビジョニングします。

ステップ 4 変更内容を `config.xml` ファイルに保存します。

MIC 証明書の更新

指定されたまたはデフォルトの Secure Unique Device Identifier (SUDI) サービスによって、Manufacture Installed Certificate (MIC) を更新できます。 MIC 証明書の期限が切れると、SSL/TLS を使用する機能は動作しません。

始める前に

- ファイアウォールから `sudirenewal.cisco.com` サービス（ポート 80）が MIC 証明書の更新をサポート許可します。
- 電話管理の Web ページにアクセスします。 電話機 ウェブインターフェイスへのアクセス を参照してください。

手順

ステップ 1 **[音声（Voice）]** > **[プロビジョニング（Provisioning）]** を選択します。

ステップ 2 **[MIC 証明書の設定]** セクションで、SUDI サービスによる MIC 証明書更新のパラメータ （37 ページ）で定義されているようにパラメータを設定します。

ステップ 3 [すべての変更の送信（Submit All Changes）]をクリックします。
証明書の更新が正常に完了すると、電話機が再起動します。

ステップ 4 （任意） **[情報（Info）]** > **[ダウンロードステータス（Download Status）]** の **[MIC 証明書の更新ステータス（MIC Cert Refresh Status）]** セクションで、MIC 証明書の更新の最新のステータスを確認します。

（注） 電話機を工場出荷時の設定に復元した場合でも、電話機は更新された証明書を使用します。

SUDI サービスによる MIC 証明書更新のパラメータ

次の表で、**[音声（Voice）]** > **[プロビジョニング（Provisioning）]** タブの **[MIC 証明書設定（MIC Cert Settings）]** セクションの各パラメータの機能と使用方法を定義します。

表 *2 : SUDI* サービスによる *MIC* 証明書更新のパラメータ

パラメータ名	説明とデフォルト値
MIC 証明書更新有効	デフォルトまたは指定されたセキュア一意デバイス識別子（SUDI）サービスによって、Manufacture Installed Certificate (MIC) の更新を有効にするかどうかを制御します。 次のいずれかを実行します。 • XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。 `<MIC_Cert_Refresh_Enable ua="na">Yes</MIC_Cert_Refresh_Enable>` • 電話機の Web インターフェイスで、**[はい]** または **[いいえ]** を選択して MIC 証明書の更新を有効または無効にします。 有効値: はい と いいえ デフォルト : [いいえ（No）]

パラメータ名	説明とデフォルト値

MIC 証明書更新ルール	更新された MIC 証明書を提供する SUDI サービスの HTTP URL を入力します。例：
	`http://sudirenewal.cisco.com/`
	（注） URL を変更する必要があります。 MIC 証明書の更新では、デフォルトの URL のみサポートされます。
	次のいずれかを実行します。
	• XML (cfg.xml)を使用した電話機の設定ファイルでは、次の形式で文字列を入力します。
	`<MIC_Cert_Refresh_Rule ua="na">http://sudirenewal.cisco.com/</MIC_Cert_Refresh_Rule>`
	• 電話機のウェブインターフェイスで、使用する HTTP URL を入力します。
	有効値: 1024 文字を超えない有効な URL
	デフォルト：`http://sudirenewal.cisco.com/`

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。