# 電話の設定



## エンタープライズモビリティ管理アプリケーションの構成

エンタープライズモビリティ管理（EMM）アプリケーションを構成してQRコードを生成し、電話機を WLAN と EMM アプリケーション に接続するようにプログラムすることをお勧めします。各電話機がEMMアプリケーションに登録されると、電話アプリ、証明書、およびCisco Unified Communications Manager に関連しないすべての機能の構成を受け取ります。

## エンタープライズ モビリティ マネージャ アプリケーションに電話機を登録する

Device Owner メソッドを介して エンタープライズモビリティ管理（EMM）アプリケーションに電話機を登録します。

詳細については、「EMM アプリケーション ドキュメント」を参照してください。

### 始める前に

バッテリが完全に充電されていることを確認してください。

次のアプリを許可していることを確認してください。

- Cisco 電話：com.cisco.phone
- システムアップデータ：com.cisco.sysupdater
- UCM クライアント：com.cisco.ucmclient
- ロギング：com.cisco.logging

- アプリケーション URL：com.cisco.appurl
- ポートマネージャ：com.cisco.portmanager

（注） EMM アプリケーションに基づき、Google キーボード（Gboard）アプリを追加する必要があります。

また、Google Play ストアにいくつかのシスコアプリがあり、これを追加できます。

**手順**

**ステップ 1** 電話機が振動して最初の画面が表示されるまで、**[電源（Power）]** ボタンを押し続けます。

**ステップ 2** 起動画面で、ディスプレイをすばやく 6 回タップします。

**ステップ 3** QR コードをスキャンします。

**関連トピック**

シスコアプリパッケージ名

# Cisco Wireless Phone 構成管理ツール

エンタープライズモビリティ管理（EMM）アプリケーション を使用して電話機を構成しない場合は、シスコ ワイヤレス電話機構成管理 ツールを使用することをお勧めします。Cisco Wireless Phone 構成管理ツール[展開構成（Deployment Configuration）] タブには、アプリと設定へのアクセスを制限できる 2 つのアプリがあります。

- **スマートランチャ**アプリ を使用すると、ホームランチャ画面で表示するアプリを指定できます。次のモードを構成できます。
  - 単一アプリモード：シスコ電話アプリなどの 1 つのアプリを指定して、スマートランチャに表示します。ユーザーは他のアプリを使用できません。
  - 複数アプリモード：スマートランチャに表示する複数のアプリを指定します。ユーザーは他のアプリを使用できません。
- **デバイス ポリシー コントローラ**アプリ を使用すると、電話機上のアプリを禁止して、ユーザーがランチャ画面にないアプリに別のアプリからアクセスできないようにすることができます。たとえば、ユーザーが Webex メッセージで受信した Web サイトへのリンクをクリックすると、Chrome アプリが許可されていないリストにない場合、リンクはブラウザで開きます。

Cisco Wireless Phone 構成管理ツール では、さまざまなシスコアプリの設定を変更またはロックダウンすることもできます。

（注） ユーティリティによって生成され、Cisco Unified Communications Manager（CUCM）にロードされる構成ファイルを使用するには、管理者は次の手順を実行する必要があります。

1. 電話機を工場出荷時の設定にリセットします。
2. 設定ツールの [初期プロビジョニング（Initial Provisioning）] タブを使用して QR コードを生成します。
3. QR コードをスキャンします。

*電話機をオンボーディングするための QR コードのスキャンに失敗すると、電話機がワイヤレスネットワークに参加して CUCM に登録されているときに、CUCM から構成ファイルをダウンロードできなくなります。

スマートランチャモードの場合、電話機には、デスクトップの明るさ、懐中電灯、音量調整、終了ランチャの 4 つのクイック設定しかありません。ただし、通知シェードには、Android 設定アプリを開くための歯車アイコンも表示されます。Cisco Wireless Phone 構成管理ツール のカスタム設定アプリで **[通知シェード設定ギアを許可する（Allow Notification Shade Settings Gear）]** を無効にすることをお勧めします。そうしないと、スマートランチャにないアプリが簡単に開いてしまいます。

（注） 単一アプリモードの通知シェード、または複数アプリモードの **[オーバーフロー（Overflow）]** メニューからクイック設定にアクセスします。

# Cisco Wireless Phone 構成管理ツール ワークフロー

Cisco Wireless Phone 構成管理ツール を使用して次を実行します。

- 電話機を呼制御システムに登録する QR コードを生成します。
- 暗号化された構成ファイルを作成して、電話機で特定のアプリと設定を許可および制限します。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | 電話機セキュリティプロファイルで TFTP 暗号化を有効にして、TFTP を介して電話機に送信される構成データがクリアテキスト形式にならないようにします。 | 新しい電話機セキュリティプロファイルを作成するを参照してください。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | ユーザーがスマートランチャを終了して他の設定やアプリにアクセスできないように、デフォルトの**ローカル電話ロック解除パスワード** **# を更新します。 | **[デバイス（Device）]** > **[デバイス設定（Device Settings）]** > **[共通デバイスプロファイル（Common Device Profile）]** の順に選択し、シスコ Unified CM 管理 Web ページにアクセスして、パスワードを変更します。 |
| ステップ 3 | 電話機に 1.5 ソフトウェアをインストールします。 | COP ファイルを Cisco Unified Communications Manager にロードするを参照してください。 |
| ステップ 4 | 電話機を出荷時設定にリセットします。 | 電話機の設定を工場出荷時のデフォルトにリセットを参照してください。 |
| ステップ 5 | Cisco Wireless Phone 構成管理ツールの **[展開構成（Deployment Configuration）]** タブで、暗号化された電話機構成ファイルを生成します。 | 暗号化された電話機構成ファイルを作成 （6 ページ）を参照してください。 |
| ステップ 6 | 電話機構成ファイルを Cisco Unified Communications Manager にアップロードします。 | 電話機構成ファイルを Cisco Unified Communications Manager にアップロードする （10 ページ）を参照してください。 |
| ステップ 7 | Cisco Wireless Phone 構成管理ツールの **[初期プロビジョニング（Initial Provisioning）]** タブで、QR コードを生成します。 | 電話を初期化する QR コードを生成する （4 ページ）を参照してください。 |
| ステップ 8 | QR コードを使用して電話機を登録します。 | Cisco Wireless Phone 構成管理ツールQR コードで電話機を登録する （5 ページ）を参照してください。 |
| ステップ 9 | ユーザーに提供する前に、電話機を再起動してください。 | |
| ステップ 10 | （任意） zip ファイルを Cisco Wireless Phone 構成管理ツール にインポートすることにより、既存の電話機構成ファイルを更新できます。 | 既存の構成ファイルを更新する （11 ページ）を参照してください。 |

# 電話を初期化する QR コードを生成する

Cisco Wireless Phone 構成管理ツール を使用して WLAN と Cisco Unified Communications Manager に電話機を接続する Quick Response（QR）コードを生成します。

組織に必要な数の異なる QR コードを生成して保存できます。

（注） QR コードを生成したら、再利用できるように、それを PDF またはその他のスキャン可能なソースとして保存することをお勧めします。

### 始める前に

該当する場合は、Wi-Fi ログイン情報を取得します。

### 手順

**ステップ 1** ブラウザから Cisco Wireless Phone 構成管理ツール を開きます。

**ステップ 2** **[初期プロビジョニング（Initial Provisioning）]** タブをクリックします。

**ステップ 3** **[セキュリティ（Security）]** オプションのいずれかを選択します。

- なし
- **WPA-Personal**
- **WPA-Enterprise**

**ステップ 4** **SSID** を入力し、必要に応じて**パスワード**を入力します。

**ステップ 5** [生成（Generate）] をクリックします。

**ステップ 6** QR コードを開いたままにするか、保存して、電話機の登録に使用できるようにします。

# Cisco Wireless Phone 構成管理ツールQR コードで電話機を登録する

Cisco Wireless Phone 構成管理ツール QR コードで電話機を登録するには、電話機が Wi-Fi ネットワークの範囲内にある必要があります。

### 始める前に

- 電話機のソフトウェアをリリース 1.5(0) に更新してから、電話機を工場出荷時の状態にリセットします。
- Cisco Wireless Phone 構成管理ツールQR コードを生成します。

### 手順

**ステップ 1** **[Hi there]** 起動画面で、ディスプレイをすばやく 6 回タップします。

カメラが開きます。

**ステップ 2** QR コードをカメラのディスプレイの中央に配置します。

**ステップ 3** [Android セットアップ（Android setup）] 画面をタップして同意します。

電話機は Cisco Unified Communications Manager に登録され、使用可能な場合は、DHCP が Cisco Unified Communications Manager を指している場合は JSON 構成ファイルをダウンロードします。

**関連トピック**

電話機の設定を工場出荷時のデフォルトにリセット
電話を初期化する QR コードを生成する （4 ページ）
暗号化された電話機構成ファイルを作成 （6 ページ）

# 暗号化された電話機構成ファイルを作成

Cisco Wireless Phone 構成管理ツール を使用すると、組織内のさまざまなグループに必要なさまざまな構成ファイルを生成して保存できます。

すべてのアプリのデフォルト設定を使用することも、アプリの設定を変更することもできます。各設定には青い情報アイコン があり、カーソルを合わせると詳細を表示できます。設定を変更すると、設定の青い情報アイコンの左側に青い点 が表示されます。

**始める前に**

- 組織のニーズに基づいて、電話機で許可または禁止するアプリと設定を決定します。
- スマートランチャに追加するアプリがすでに電話機にインストールされていることを確認してください。

**手順**

**ステップ 1** 任意のブラウザから、Cisco Wireless Phone 構成管理ツール を開き **[展開構成（Deployment Configuration）]** タブを開きます。

**ステップ 2** [アプリケーションの選択（Choose Application）] から **[スマートランチャ（Smart Launcher）]** を選択し、これらのパラメータを設定します。

- **アプリケーションの許可リストを設定**：スマートランチャに表示するアプリを含めます。アプリパッケージ名のコンマ区切りリストをスペースなしで使用します。

  （注） デフォルトで、Cisco Wireless Phone 構成管理ツールでは、次のアプリが許可されるように設定されています。**com.cisco.phone**、**com.cisco.ptt**、**com.cisco.emergency**、**com.cisco.webapi**、**com.cisco.wx2.android**。

- **ランチャアプリケーションのタイトルを設定**：複数のアプリがあるスマートランチャに表示するタイトルを追加します。スマートランチャにアプリが 1 つだけある場合、タイトルは表示されません。タイトルに使用できる文字数は、25 文字までです。タイトルのデフォルト名は、スマートランチャです。たとえば、会社名や部署を追加します。

**ステップ 3** [アプリケーションの選択（Choose Application）] から **[デバイス ポリシー コントローラ（Device Policy Controller）]** を選択し、パラメータを設定します。

- **これらのアプリを許可しない**：電話機でアクセスしたくないアプリを含めます。アプリパッケージ名のコンマ区切りリストをスペースなしで使用します。

  **注意** このリストにシスコ電話アプリを含めないでください。

  **スマートランチャ**の許可リストにあるアプリケーションがこの禁止リストに含まれていないことを確認してください。許可されていないアプリケーションはスマートランチャのホーム画面に表示されません。

  （注） デフォルトでは、Cisco Wireless Phone 構成管理ツールには、次のアプリは許可されていません： **com.google.android.youtube、com.google.android.googlequicksearchbox、com.android.soundrecorder、com.google.android.apps.wellbeing,com.google. android.apps.maps、com.google.android.videos、com.google.android.apps.photos、com.android.vending、com.android.chrome**。

- **Wi-Fi プロファイル**：5 つの Wi-Fi プロファイルを追加：以下のいずれかの EAP メソッドがある WPA2-Personal または WPA2-Enterprise：
  - MSCHAPv2 または GTC を使用した PEAP
  - GTC、PAP、MSCHAP、または MSCHAPv2 を使用した TTLS

  （注） Cisco Wireless Phone 構成管理ツール は、PEM 証明書をサポートしています。コピーして貼り付けるときは、証明書のヘッダー、フッター、空白、または新しい行 を含めないでください。

**ステップ 4** [アプリケーションの選択（Choose Application）] から、組織の必要に応じて、次のシスコアプリをそれぞれ選択して設定します。

（注） すべてのデフォルトのアプリ設定を受け入れる場合は、変更を加える必要はありません。これらのシスコアプリ設定の詳細については、「シスコアプリ構成」を参照してください。

- **バーコード**
- **バッテリ寿命**
- **ボタン**
- **カスタム設定**
- **PTT**
- **緊急**

- 通話品質設定
- **Web API**

**ステップ 5** **[エクスポート（Export）]** をクリックします。

**ステップ 6** **[暗号化構成（Encrypt Configuration）]** チェックボックスをオンにします。

（注） 本番サーバーで暗号化されていないファイルを使用しないでください。

**ステップ 7** **[エクスポート（Export）]** をクリックします。

Cisco Wireless Phone 構成管理ツール エクスポートにより、3 つのファイルを含む zip ファイルが作成されます。

**ステップ 8** 必要に応じて構成ファイルを再利用または更新できるように、zip ファイルのコピーを保存します。

**注意** 必要に応じて、zip ファイルの名前を変更できます。ただし、後で構成ファイルを更新する予定がある場合は、内部ファイルの名前を変更せずに、そのままの zip ファイルのコピーを保持してください。

**関連トピック**

シスコアプリパッケージ名
プリインストール Android アプリ （8 ページ）
既存の構成ファイルを更新する （11 ページ）
製品固有構成レイアウトフィールド
シスコアプリ構成用 Cisco Wireless Phone 構成管理ツール

# プリインストール Android アプリ

Cisco Wireless Phone 構成管理ツール **スマートランチャ** および **デバイス ポリシー コントローラ** アプリを介してプリインストール Android アプリを電話機で許可または禁止するように設定できます。

次の表は、**デバイス ポリシー コントローラ** で、デフォルトで禁止されているプリインストール Android アプリを一覧しています。

**表 *1*: デバイス ポリシー コントローラ でデフォルトで禁止されているプリインストール *Android* アプリ**

| デフォルトで禁止されている Android アプリ | アプリパッケージ名 |
|---|---|
| Chrome | com.android.chrome |
| デジタルウェルビーイング | com.google.android.apps.wellbeing |
| Google | com.google.android.googlequicksearchbox |

| デフォルトで禁止されている Android アプリ | アプリパッケージ名 |
|---|---|
| Google TV | com.google.android.videos |
| マップ | com.google.android.apps.maps |
| Photos | com.google.android.apps.photos |
| Play ストア | com.android.vending |
| サウンドレコーダー | com.android.soundrecorder |
| YouTube | com.google.android.youtube |

これらの一般的なプリインストール Android アプリを許可または禁止リストに設定することもできます。

**表 *2:* その他のプリインストールアプリ**

| プリインストールアプリ | アプリパッケージ名 |
|---|---|
| カリキュレータ | com.google.android.calculator |
| カレンダー | ccom.google.android.calendar |
| カメラ | com.google.android.GoogleCamera |
| 時計 | com.google.android.deskclock |
| 連絡先 | com.google.android.contacts |
| 推進 | com.google.android.apps.docs |
| Duo | com.google.android.apps.tachyon |
| ファイル | com.marc.files |
| Gmail | com.google.android.gm |
| Keep Notes | com.google.android.keep |
| Webex | com.cisco.wx2.android |
| YT Music | com.google.android.apps.youtube.music |

必要に応じて、他の Android アプリを電話機にインストールすることもできます。

# 電話機構成ファイルを Cisco Unified Communications Manager にアップロードする

### 始める前に

Cisco Wireless Phone 構成管理ツール で暗号化された電話機構成 zip ファイルを作成します。

### 手順

**ステップ 1** 暗号化された電話機構成 zip ファイルの内容を抽出します。zip ファイルには、次の 3 つのファイルが含まれています。

- **config.json.enc** — Cisco Unified Communications Manager にインポートされた電話機構成が含まれます。
- **key.txt** — **config.json.enc** ファイルを復号する暗号化キーが含まれます。
- **config.json.react.enc** — Cisco Wireless Phone 構成管理ツール 用の構成フォーマットが含まれます。これは、ファイルをインポートする際に使用します。

（注） zip ファイルを抽出したら、Cisco Unified Communications Manager にアップロードする前に `config.json.enc` の名前を変更できます。さまざまなデバイスに対して複数の構成を計画している場合は、名前の変更を行うことをお勧めします。

**ステップ 2** Cisco Unified Communications Manager Administration にサインインします。

**ステップ 3** `config.json.enc` ファイルの名前を [製品固有構成レイアウト（Product Specific Configuration Layout）] ペインの **[エンタープライズモビリティ管理（EMM）代替構成（Enterprise Mobility Management (EMM) Alternative Configuration）]** フィールドに追加します。

（注） `config.json.enc` ファイルの名前を変更する場合は、新しい名前を使用してください。

**ステップ 4** `key.txt` ファイルのキーを [製品固有構成レイアウト（Product Specific Configuration Layout）] ペインの **[エンタープライズモビリティ管理（EMM）代替構成（Enterprise Mobility Management (EMM) Alternative Configuration）]** フィールドに追加します。

（注） 一括管理を使用して、デバイスタイプ全体でキーを設定することもできます。

**ステップ 5** TFTP サービスを実行しているすべての TFTP ノードに `config.json.enc` ファイルを追加し、TFTP サービスを再起動します。

### 関連トピック

製品固有構成レイアウトフィールド

# 既存の構成ファイルを更新する

既存の構成ファイルを更新する場合は、既存の構成 zip ファイルを Cisco Wireless Phone 構成管理ツール にインポートし、変更を加えて、新しい構成 zip ファイルをエクスポートします。

### 始める前に

元の構成ファイルのコピーを保持する場合は、そのままの zip ファイルをコピーして名前を変更します。

**注意** zip 内のファイルを抽出して名前を変更してから、ファイルを再圧縮しないでください。

### 手順

**ステップ 1** シスコ ワイヤレス構成展開ツールを開きます。
**ステップ 2** [展開構成（Deployment Configuration）] タブで、**[インポート（Import）]** をクリックします。
**ステップ 3** 既存の構成 zip ファイルを追加し、**[インポート（Import）]** をクリックします。
**ステップ 4** アプリと設定を更新します。
**ステップ 5** **[エクスポート（Export）]** をクリックして、新しい構成 zip ファイルを作成します。
**ステップ 6** 手順に従って、新しい暗号化された電話機構成ファイルを Cisco Unified Communications Manager にアップロードします。

### 関連トピック

暗号化された電話機構成ファイルを作成 （6 ページ）
電話機構成ファイルを Cisco Unified Communications Manager にアップロードする （10 ページ）

# 電話機の手動構成

エンタープライズモビリティ管理（EMM）アプリケーション と QR コード、または Cisco Wireless Phone 構成管理ツール からの JSON 構成ファイルと QR コードを使用しない場合は、電話機を手動で構成できます。

## Wi-Fi プロファイル構成

初期状態の電話機または工場出荷時の状態にリセットされた電話機の場合は、スタートアップ ウィザードを使用して Wi-Fi ネットワークを構成するか、**[オフラインでセットアップ（Set up offline）]** を選択します。電話機をオフラインで構成する方法は、Wi-Fi ネットワークが次のいずれかであるかどうかによって異なります。

- ブロードキャストされている
- 非ブロードキャストまたは非公開

# ブロードキャスト Wi-Fi ネットワークに電話機を追加する

電話機をブロードキャスト Wi-Fi ネットワークに追加するには、スタートアップウィザードを使用するか、オフラインで**設定**アプリ を使用します。

### 始める前に

管理者から Wi-Fi ネットワークに関する次の情報を入手します。

- ネットワーク名またはサービスセット識別子（SSID）
- ネットワーク セキュリティ モード：
  - なし
  - 事前共有キー（PSK）
  - Protected Extensible Authentication Protocol（PEAP）
  - Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル） Transport Layer Security（EAP-TLS）
  - EAP Tunneled Transport Layer Security（EAP-TTLS）
- セキュリティモードの個人識別番号またはパスキー（使用する場合）

管理者に証明書が必要かどうかを確認し、電話機に証明書をインストールするように手配してください。

### 手順

**ステップ 1** 電話機のディスプレイを下から上にスワイプして、インストールされているアプリケーションを表示します。

**ステップ 2** **設定**アプリ をタップします。

**ステップ 3** **[ネットワークとインターネット（Network & internet）]** > **[Wi-Fi]**の順に選択します。

**ステップ 4** 目的の Wi-Fi ネットワーク名をタップします。

ネットワークにセキュリティモードがない場合、電話機は自動的に Wi-Fi ネットワークに接続します。

ネットワーク セキュリティモードが PSK の場合は、8 ～ 63 の ASCII または 64 Hex Passphrase を入力します。

**ステップ 5** PEAP、EAP-TLS、またはEAP-TTLSセキュリティモードのネットワークの場合、PEAP、TLS、またはTTLSの **EAP 方式** を選択します。

**ステップ 6** EAP-TLSセキュリティモードのネットワークの場合、目的の**CA証明書**と**ユーザー証明書**を選択します。

**ステップ 7** EAP-TTLSまたはPEAPセキュリティモードのネットワークの場合、使用する**フェーズ 2 認証**方式と **CA 証明書**オプションを選択し、**ID** と**パスワード**を入力します。

**ステップ 8** **[接続（Connect）]** をタップします。

# 非ブロードキャスト Wi-Fi ネットワークに電話機を追加する

以下の手順に従って、非表示またはブロードキャストされていないWi-Fiネットワークに電話機を追加します。

### 始める前に

管理者からWi-Fiネットワークに関する次の情報を入手します。

- ネットワーク名またはサービスセット識別子（SSID）
- ネットワーク セキュリティモード：
  - なし
  - Wi-Fi Protected Access II (WPA2)-Personal：事前共有キー（PSK）
  - EAP 方式の WPA2-Enterprise
    - Protected Extensible Authentication Protocol（PEAP）
    - Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル） Transport Layer Security（EAP-TLS）
    - EAP Tunneled Transport Layer Security（EAP-TTLS）
- セキュリティモードの個人識別番号またはパスキー（使用する場合）

管理者に証明書が必要かどうかを確認し、電話機に証明書をインストールするように手配してください。

### 手順

**ステップ 1** 電話機のディスプレイを下から上にスワイプして、インストールされているアプリケーションを表示します。

**ステップ 2** **設定**アプリ をタップします。

**ステップ 3** **[ネットワークとインターネット（Network & internet）]** > **[Wi-Fi]**の順に選択します。

**ステップ 4** **[ネットワークを追加（Add Network）]** をタップします。

**ステップ 5** 希望の Wi-Fi **ネットワーク名**を入力します。

**ステップ 6** 希望の**セキュリティ**を選択します。

- オープンネットワークの場合は、**[なし（None）]** を選択します。
- PSK 対応 Wi-Fi ネットワークの場合は、**[WPA2- Personal]** を選択し、8-63 ASCII または 64 HEX の**パスワード** を入力します。
- EAP 対応の Wi-Fi ネットワークの場合は、**[WPA2-Enterprise]** を選択します。

**ステップ 7** WPA2-Enterprise ネットワークの場合は、**EAP 方式**（PEAP、TLS、または TTLS）を選択します。

**ステップ 8** EAP-TLSセキュリティモードのネットワークの場合、目的の**CA証明書**と**ユーザー証明書**を選択します。

**ステップ 9** EAP-TTLS または PEAP セキュリティモードのネットワークの場合、使用する**フェーズ 2 認証**方式と **CA 証明書**オプションを選択し、**ID** と**パスワード**を入力します。

**ステップ 10** **[詳細オプション（Advanced options）]**で、**[非表示のネットワーク（Hidden network）]** を **[はい（Yes）]** に設定します。

必要に応じて、**プロキシ**および **IP 設定**を設定することもできます。

**ステップ 11** **[保存（Save）]** をタップします。

# TFTP サーバーの構成

ネットワークが 登録先の Cisco Unified Communications Manager の DHCP オプション 150 または 66 を提供していない場合は、TFTP サーバーを構成する必要があります。

（注） 自動構成方式を使用する場合は、オプション 150 または 66 を使用して DHCP プールを構成します。

### 始める前に

次の情報が必要です。

- デフォルトのパスワードが更新された場合の**ローカル電話機ロック解除パスワード**
- TFTP サーバーの IP アドレス

### 手順

**ステップ 1** **シスコ電話**アプリ にアクセスします。

**ステップ 2** 電話機のソフトウェアバージョンに基づいて、次のいずれかを選択します。

- リリース 1.2(0) の場合は、**[オーバーフロー（Overflow）]** メニュー ⋮ をタップします。
- リリース 1.3(0) 以降の場合は、**[ドロワー（Drawer）]** メニュー ☰ をタップします。

**ステップ 3** 電話機のソフトウェアバージョンに基づいて、次のいずれかを選択します。

- リリース 1.2(0) の場合は、**[設定（Settings）]** > **[電話機の情報（Phone information）]** > **[セキュリティ（Security）]** の順に選択します。
- リリース 1.3(0) の場合は、**[ユーザー設定（User Settings）]** > **[電話機の情報（Phone information）]** > **[セキュリティ（Security）]** の順に選択します。

**ステップ 4** **ローカル電話機ロック解除パスワード**を入力します。

デフォルトのパスワードは、****#** です。

**ステップ 5** 代替 TFTP サーバーを有効にするには、**[代替 TFTP（Alternate TFTP）]** スライダを右 にスワイプします。

**ステップ 6** TFTP サーバーアドレスを入力し、**[OK]** をタップします。

**ステップ 7** 左上隅の戻る矢印を 2 回タップして変更を保存し、メニューを終了します。

# コールサーバーモードを設定する

Cisco Wireless Phone 840 および 860 は、UCM モードまたは WxC モードのいずれかで動作します。電話機は、自動と手動の両方で設定できます。コールサーバーモードで**UCM** または**WxC** を手動で選択し、自動設定の場合は **[自動検出（ Auto detect）]** を選択します。

通常、コール サーバー モードで **[自動検出（ Auto detect ）]** を選択すると、電話機は既存の動作を使用して UCM への接続を試みます。電話機が UCM から設定を取得すると、電話機は UCM モードで動作し、WxC モードは無効になります。電話機が UCM から設定を取得できない場合、電話機はWxC設定を取得しようとします。WxC設定を受信すると、UCMモードが無効になります。電話機が CUCM または WxC の設定を取得できない場合、電話機は事前設定されたバックオフ スケジュールで自動検出プロセスを再試行します。

### 始める前に

次の情報が必要です。

- デフォルトのパスワードが更新された場合の**ローカル電話機ロック解除パスワード**

### 手順

**ステップ 1** **シスコ電話**アプリ  にアクセスします。

**ステップ 2** リリース 1.6(0) 以降の場合は、**[ドロワー（Drawer）]** ☰ メニューをタップします。

**ステップ 3** **[ユーザー設定（User Settings）]** > **[電話機の情報（Phone information）]** > **[セキュリティ（Security）]** の順に選択します。

**ステップ 4** **ローカル電話機ロック解除パスワード**を入力します。

デフォルトのパスワードは、****#** です。

**ステップ 5** コールサーバーモードの次のいずれかのオプションを選択します。

- **自動検出**
- **UCM**
- **WxC**

**ステップ 6** 左上隅の戻る矢印を 2 回タップして変更を保存し、メニューを終了します。

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。