



## Cisco Unified IP Phone の設定値の設定

Cisco Unified IP Phone には、設定可能な数多くのネットワーク設定値が用意されています。電話機をユーザが使用できる状態にするには、これらの設定値の修正が必要になる場合もあります。電話機のメニューを使用して、これらの設定値にアクセスし、その一部を変更することができます。電話機で表示専用になっている設定値は、Cisco Unified Communications Manager の管理ページで設定できます。

この章は、次の項で構成されています。

- 「Cisco Unified IP Phone の設定メニュー」 (P.4-1)
- 「[ネットワークのセットアップ (Network Setup) ]メニュー」 (P.4-4)
- 「[IPv4 のセットアップ (IPv4 Setup) ]メニューのオプション」 (P.4-7)
- 「[セキュリティ設定 (Security Configuration) ]メニュー」 (P.4-9)

## Cisco Unified IP Phone の設定メニュー

Cisco Unified IP Phone には、次の設定メニューが用意されています。

- [ネットワークのセットアップ (Network Setup) ]: さまざまなネットワーク設定値を表示および設定するためのオプションを提供します。詳細については、「[ネットワークのセットアップ (Network Setup) ]メニュー」 (P.4-4) を参照してください。
- [IPv4 設定 (IPv4 Configuration) ]: [ネットワークのセットアップ (Network Setup) ]メニューのサブメニューです。IPv4 のメニュー項目を使用して、追加のネットワーク オプションを表示、設定できます。詳細については、「[IPv4 のセットアップ (IPv4 Setup) ]メニューのオプション」 (P.4-7) を参照してください。

[ネットワークのセットアップ (Network Setup) ]メニューにあるオプション設定値を変更するには、オプションのロックを編集のために解除しておく必要があります。手順は、「オプションのロック解除とロック」 (P.4-3) を参照してください。

オプション設定値の編集や変更に使用できるキーについては、「設定値の編集」 (P.4-3) を参照してください。

Cisco Unified Communications Manager の管理ページの [電話の設定 (Phone Configuration) ]ウィンドウにある設定アクセス フィールドを使用すると、電話機のユーザが電話機の設定にアクセスできるかどうかを制御できます。

### 関連項目

- 「設定メニューの表示」 (P.4-2)
- 「オプションのロック解除とロック」 (P.4-3)
- 「設定値の編集」 (P.4-3)

- 「[ネットワークのセットアップ (Network Setup) ]メニュー」 (P.4-4)
- 「[IPv4 のセットアップ (IPv4 Setup) ]メニューのオプション」 (P.4-7)

## 設定メニューの表示

設定メニューを表示するには、次の手順を実行します。



(注)

Cisco Unified Communications Manager の管理ページの [電話の設定 (Phone Configuration) ] ウィンドウにある設定アクセス フィールドを使用すると、[設定 (Settings) ]メニューや、このメニューのオプションに電話機でアクセスできるかどうかを制御できます。設定アクセス フィールドでは、次の値を設定できます。

- [有効 (Enabled) ]: [設定 (Settings) ]メニューへのアクセスを許可します。
- [無効 (Disabled) ]: [設定 (Settings) ]メニューへのアクセスを禁止します。
- [非許可 (Restricted) ]: [ユーザ設定 (User Preferences) ]メニューへのアクセスを許可し、音量の変更を保存することを許可します。[設定 (Settings) ]メニューの他のオプションへのアクセスは禁止します。

[管理者設定 (Administrator Settings) ]メニューのオプションにアクセスできない場合は、設定アクセス フィールドを確認してください。

### 手順

- ステップ 1** アプリケーション ボタンを押します。
- ステップ 2** [管理者設定 (Admin Settings) ]を選択します。



(注) [ステータス (Status) ]メニューの詳細については、第 7 章「Cisco Unified IP Phone のモデル情報、ステータス、および統計の表示」を参照してください。[設定のリセット (Reset Settings) ]メニューの詳細については、第 9 章「トラブルシューティングおよびメンテナンス」を参照してください。

- ステップ 3** パスワードを入力し、選択ボタンを押します。管理者設定パスワードは、Cisco Unified Communications Manager の管理ページにある [共通の電話プロファイルの設定 (Common Phone Profile Configuration) ]の [電話ロック解除パスワード (Local Phone Unlock Password) ]パラメータで設定します。



(注) [電話ロック解除パスワード (Local Phone Unlock Password) ]パラメータが設定されていない場合、ユーザは、パスワードを入力せずに、[管理者設定 (Admin Settings) ]にアクセスできます。

- ステップ 4** 次のいずれかの操作を実行して、目的のメニューを表示します。
- ナビゲーション バーを使用して目的のメニューを選択し、選択ボタンを押します。
  - 電話機のキーパッドを使用して、メニューに対応する番号を入力します。
- ステップ 5** サブメニューを表示するには、ステップ 4 を繰り返します。

**ステップ 6** メニューを終了するには、[ 終了 (Exit) ] ソフトキーを押します。

#### 関連項目

- 「オプションのロック解除とロック」 (P.4-3)
- 「設定値の編集」 (P.4-3)
- 「[ ネットワークのセットアップ (Network Setup) ] メニュー」 (P.4-4)
- 「[ IPv4 のセットアップ (IPv4 Setup) ] メニューのオプション」 (P.4-7)

## オプションのロック解除とロック

電話機にパスワードを設定すると、電話機画面の [ 管理者設定 (Admin Settings) ] でパスワードを入力しない限り、管理者オプションを変更できなくなります。


電話機にパスワードを適用するには、Cisco Unified Communications Manager の管理ページで、[ 共通の電話プロファイルの設定 (Common Phone Profile Configuration) ] ウィンドウを表示します ([ デバイス (Device) ] > [ デバイスの設定 (Device Settings) ] > [ 共通の電話プロファイル (Common Phone Profile) ])。[ 電話ロック解除パスワード (Local Phone Unlock Password) ] オプションで、パスワードを入力します。電話機が使用する共通の電話プロファイルに、パスワードを適用します。

#### 関連項目

- 「設定メニューの表示」 (P.4-2)
- 「設定値の編集」 (P.4-3)
- 「[ ネットワークのセットアップ (Network Setup) ] メニュー」 (P.4-4)
- 「[ IPv4 のセットアップ (IPv4 Setup) ] メニューのオプション」 (P.4-7)

## 設定値の編集

オプション設定値を編集するときは、次のガイドラインに従ってください。

- 数値と文字を入力するには、キーパッド上のキーを使用します。
- キーパッドを使用して文字を入力するには、対応する数値キーを使用します。キーを 1 回または何回か押して、個々の文字を表示します。たとえば、2 キーを 1 回押すと「a」、すばやく 2 回押すと「b」、すばやく 3 回押すと「c」です。しばらく待機すると、カーソルが自動的に進んで、次の文字を入力できるようになります。
- (IP アドレスなどに含まれる) ペリオドを入力するには、キーパッドの \* を押します。
- カーソルを左端の文字に移動するには、ナビゲーションバーの上向き矢印を押します。右端の文字に移動するには、ナビゲーションバーの下向き矢印を押します。
- 押し間違えた場合は  を押します。このソフトキーを押すと、カーソルの左側にある文字が削除されます。
- 行った変更をすべて破棄するには、[ 保存 (Save) ] ソフトキーを押す前に [ キャンセル (Cancel) ] ソフトキーを押します。



(注) Cisco Unified IP Phone では、必要に応じて、いくつかの方法でオプション設定値をリセットまたは復元することができます。詳細については、「Cisco Unified IP Phone のリセットまたは復元」(P.9-12)を参照してください。

#### 関連項目

- 「設定メニューの表示」(P.4-2)
- 「オプションのロック解除とロック」(P.4-3)
- 「[ネットワークのセットアップ (Network Setup) ]メニュー」(P.4-4)

## [ネットワークのセットアップ (Network Setup) ]メニュー

[ネットワークのセットアップ (Network Setup) ]メニューは、さまざまなネットワーク設定値を表示および設定するためのオプションを提供します。表 4-1 では、これらのオプションと、変更可能な場合は、変更方法について説明します。

[ネットワークのセットアップ (Network Setup) ]メニューにアクセスする方法については、「設定メニューの表示」(P.4-2)を参照してください。

オプションの編集に使用できるキーについては、「設定値の編集」(P.4-3)を参照してください。

表 4-1 [ネットワークのセットアップ (Network Setup) ]メニューのオプション

オプション	説明	変更の手順
IPv4 のセットアップ (IPv4 Setup)	<p>[IPv4 のセットアップ (IPv4 Setup) ]サブメニューでは、次の作業を実行できます。</p> <ul style="list-style-type: none"> <li>• DHCP サーバによって割り当てられた IP アドレスの、電話機による使用のオン/オフ。</li> <li>• IP アドレス、サブネット マスク、デフォルト ルータ、DNS サーバ、および代替 TFTP サーバの手動設定。</li> </ul> <p>IPv4 のアドレス フィールドの詳細については、表 4-2 を参照してください。</p>	[IPv4 のセットアップ (IPv4 Setup) ]までスクロールし、[選択 (Select) ]を押します。
ホスト名 (Host Name)	DHCP サーバが電話機に割り当てた、一意のホスト名。	表示のみ (変更不可)。
ドメイン名 (Domain Name)	電話機が常駐している Domain Name System (DNS; ドメイン ネーム システム) ドメインの名前。	<ol style="list-style-type: none"> <li>1. [DHCP を使う (DHCP Enabled) ]オプションを [No] に設定します。</li> <li>2. [ドメイン名 (Domain Name) ]オプションまでスクロールし、[編集 (Edit) ]ソフトキーを押して、新しいドメイン名を入力します。</li> <li>3. [適用 (Apply) ]ソフトキーを押し、[保存 (Save) ]を押します。</li> </ol>

表 4-1 【ネットワークのセットアップ (Network Setup)】メニューのオプション (続き)

オプション	説明	変更の手順
オペレーショナル VLAN ID (Operational VLAN ID)	電話機が所属する、Cisco Catalyst スイッチに設定された補助 Virtual Local Area Network (VLAN; 仮想 LAN)。 電話機が補助 VLAN をまだ受信していない場合、このオプションは管理 VLAN を示しています。 補助 VLAN と管理 VLAN のどちらも設定されていない場合、このオプションは 4095 というデフォルトの VLAN ID に設定されます。	表示のみ (変更不可)。 電話機は、電話機が接続されているスイッチから、シスコ検出プロトコル (CDP) を通じてオペレーショナル VLAN ID を取得します。VLAN ID を手動で割り当てるには、[管理 VLAN ID (Admin VLAN ID)] オプションを使用します。
管理 VLAN ID (Admin VLAN ID)	電話機がメンバーになっている補助 VLAN。 電話機がスイッチから補助 VLAN を受信していない場合のみ使用され、その他の場合は無視されます。	<ol style="list-style-type: none"> <li>[管理 VLAN ID (Admin VLAN ID)] オプションまでスクロールし、[編集 (Edit)] ソフトキーを押して、新しい管理 VLAN 設定値を入力します。</li> <li>[適用 (Apply)] ソフトキーを押し、[保存 (Save)] を押します。</li> </ol>
PC VLAN	ボイス VLAN をサポートしないサードパーティ スイッチと電話機が連携できるようにします。このオプションを変更する前に、[管理 VLAN ID (Admin VLAN ID)] オプションを設定する必要があります。	<ol style="list-style-type: none"> <li>[管理 VLAN ID (Admin VLAN ID)] オプションが設定されていることを確認してください。</li> <li>[PC VLAN] オプションまでスクロールし、[編集 (Edit)] ソフトキーを押して、新しい PC VLAN 設定値を入力します。</li> <li>[適用 (Apply)] ソフトキーを押し、[保存 (Save)] を押します。</li> </ol>
SW ポート設定 (SW Port Configuration)	ネットワーク ポートの速度と二重化モード。有効な値は、次のとおりです。 <ul style="list-style-type: none"> <li>自動ネゴシエーション</li> <li>100 ハーフ : 100-BaseT/半二重</li> <li>100 フル : 100-BaseT/全二重</li> <li>10 ハーフ : 10-BaseT/半二重</li> <li>10 フル : 10-BaseT/全二重</li> </ul> 電話機がスイッチに接続されている場合は、スイッチ上のポートを電話機と同じ速度および二重化方式に設定するか、両方を自動ネゴシエーションに設定します。 このオプションの設定値を変更する場合は、[PC ポート設定 (PC Port Configuration)] オプションを同じ設定値に変更する必要があります。	<ol style="list-style-type: none"> <li>ネットワークのセットアップのオプションのロックを解除します。</li> <li>[SW ポート設定 (SW Port Configuration)] オプションまでスクロールし、[編集 (Edit)] ソフトキーを押します。</li> <li>目的の設定値までスクロールし、選択ボタンを押します。</li> </ol>

表 4-1 [ネットワークのセットアップ (Network Setup) ] メニューのオプション (続き)

オプション	説明	変更の手順
PC ポート設定 (PC Port Configuration)	<p>アクセス ポートの速度と二重化モード。有効な値は、次のとおりです。</p> <ul style="list-style-type: none"> <li>自動ネゴシエーション</li> <li>100 ハーフ : 100-BaseT/半二重</li> <li>100 フル : 100-BaseT/全二重</li> <li>10 ハーフ : 10-BaseT/半二重</li> <li>10 フル : 10-BaseT/全二重</li> </ul> <p>電話機がスイッチに接続されている場合は、スイッチ上のポートを電話機と同じ速度および二重化方式に設定するか、両方を自動ネゴシエーションに設定します。</p> <p>このオプションの設定値を変更する場合は、[SW ポート設定 (SW Port Configuration) ] オプションを同じ設定値に変更する必要があります。</p>	<ol style="list-style-type: none"> <li>ネットワークのセットアップのオプションのロックを解除します。</li> <li>[PC ポート設定 (PC Port Configuration) ] オプションまでスクロールし、[編集 (Edit) ] ソフトキーを押します。</li> <li>目的の設定値までスクロールし、選択ボタンを押します。</li> </ol>
LLDP-MED : スイッチポート (LLDP-MED: Switch Port)	<p>スイッチ ポートの Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) を有効化および無効化します。電話機で特定の検出プロトコルが使用されるようにするには、この設定を使用します。このプロトコルは、スイッチでサポートされるプロトコルと一致している必要があります。次の設定があります。</p> <ul style="list-style-type: none"> <li>[有効 (Enabled) ] : デフォルト</li> <li>[無効 (Disabled) ]</li> </ul>	<p>Cisco Unified Communications Manager の管理ページで、[デバイス (Device) ] &gt; [電話 (Phone) ] &gt; [電話の設定 (Phone Configuration) ] を選択します。</p>

## [IPv4 のセットアップ (IPv4 Setup) ]メニューのオプション

[IPv4 のセットアップ (IPv4 Setup) ]メニューは、[ネットワークの設定 (Network Setup) ]メニューのサブメニューです。[IPv4 のセットアップ (IPv4 Setup) ]メニューにアクセスするには、[ネットワークの設定 (Network Setup) ]メニューで [IPv4] オプションを選択します。

表 4-2 に、[IPv4 の設定 (IPv4 Setup) ]メニューのオプションの説明を示します。

オプションの編集に使用できるキーについては、「設定値の編集」(P.4-3) を参照してください。

表 4-2 [IPv4 のセットアップ (IPv4 Setup) ]メニューのオプション

オプション	説明	変更の手順
DHCP	電話機の DHCP が有効か無効かを示します。 DHCP が有効な場合、DHCP サーバによって電話に IP アドレスが割り当てられます。DHCP が無効な場合、管理者が、電話機に手動で IP アドレスを割り当てる必要があります。	[DHCP] オプションまでスクロールし、[編集 (Edit) ] ソフトキーを押した後、[No] ソフトキーを押して DHCP を無効にするか、[Yes] ソフトキーを押して DHCP を有効にします。
IP アドレス (IP Address)	電話機の Internet Protocol (IP; インターネット プロトコル) アドレス。 IP アドレスをこのオプションで割り当てる場合は、サブネット マスクとデフォルト ルータも割り当てる必要があります。この表の [サブネット マスク (Subnet Mask) ] オプションと [デフォルト ルータ (Default Router) ] オプションを参照してください。	<ol style="list-style-type: none"> <li>[DHCP] オプションを [No] に設定します。</li> <li>[IP アドレス (IP Address) ] オプションまでスクロールし、[編集 (Edit) ] ソフトキーを押して、新しい IP アドレスを入力します。</li> <li>[適用 (Apply) ] ソフトキーを押し、[保存 (Save) ] を押します。</li> </ol>
サブネット マスク (Subnet Mask)	電話機で使用されるサブネット マスク。	<ol style="list-style-type: none"> <li>[DHCP を使う (DHCP Enabled) ] オプションを [No] に設定します。</li> <li>[サブネット マスク (Subnet Mask) ] オプションまでスクロールし、[編集 (Edit) ] ソフトキーを押して、新しいサブネット マスクを入力します。</li> <li>[適用 (Apply) ] ソフトキーを押し、[保存 (Save) ] を押します。</li> </ol>
デフォルト ルータ 1 (Default Router 1)	電話機で使用されるデフォルト ルータ ([デフォルト ルータ 1 (Default Router 1) ] )。	<ol style="list-style-type: none"> <li>[DHCP を使う (DHCP Enabled) ] オプションを [No] に設定します。</li> <li>目的の [デフォルト ルータ (Default Router) ] オプションまでスクロールし、[編集 (Edit) ] ソフトキーを押して、新しいルータの IP アドレスを入力します。</li> <li>[適用 (Apply) ] ソフトキーを押し、[保存 (Save) ] を押します。</li> </ol>

## ■ [IPv4 のセットアップ (IPv4 Setup) ] メニューのオプション

表 4-2 [IPv4 のセットアップ (IPv4 Setup) ] メニューのオプション (続き)

オプション	説明	変更の手順
DNS サーバ 1 (DNS Server 1)	電話機で使用されるプライマリ DNS サーバ ([DNS サーバ 1 (DNS Server 1) ]) およびオプションのバックアップ DNS サーバ ([DNS サーバ 2 (DNS Server 2) ] ~ [DNS サーバ 5 (DNS Server 5) ])。	<ol style="list-style-type: none"> <li>1. [DHCP を使う (DHCP Enabled) ] オプションを [No] に設定します。</li> <li>2. 目的の [DNS サーバ (DNS Server) ] オプションまでスクロールし、[編集 (Edit) ] ソフトキーを押して、新しい DNS サーバの IP アドレスを入力します。</li> <li>3. [適用 (Apply) ] ソフトキーを押し、[保存 (Save) ] を押します。</li> </ol>
代替 TFTP (Alternate TFTP)	電話機が代替 TFTP サーバを使用しているかどうかを示します。	電話機で代替 TFTP サーバを使用する場合は、[代替 TFTP (Alternate TFTP) ] オプションまでスクロールし、[Yes] ソフトキーを押します。使用しない場合は、[No] ソフトキーを押します。
TFTP サーバ 1 (TFTP Server 1)	電話機で使用される、プライマリの Trivial File Transfer Protocol (TFTP) サーバ。ネットワークで DHCP を使用していない場合、このサーバを変更するには [TFTP サーバ 1 (TFTP Server 1) ] オプションを使用する必要があります。  [代替 TFTP (Alternate TFTP) ] オプションを [Yes] に設定した場合は、[TFTP サーバ 1 (TFTP Server 1) ] オプションに 0 以外の値を入力する必要があります。	<ol style="list-style-type: none"> <li>1. DHCP を有効にしている場合は、[代替 TFTP (Alternate TFTP) ] オプションを [Yes] に設定します。</li> <li>2. [TFTP サーバ 1 (TFTP Server 1) ] オプションまでスクロールし、[編集 (Edit) ] ソフトキーを押して、新しい TFTP サーバの IP アドレスを入力します。</li> <li>3. [適用 (Apply) ] ソフトキーを押し、[保存 (Save) ] を押します。</li> </ol>
TFTP サーバ 2 (TFTP Server 2)	プライマリの TFTP サーバが使用不能の場合に、電話機で使用されるオプションのバックアップ TFTP サーバ。	<ol style="list-style-type: none"> <li>1. [TFTP サーバ 1 (TFTP Server 1) ] オプションに IP アドレスを入力します。</li> <li>2. [TFTP サーバ 2 (TFTP Server 2) ] オプションまでスクロールし、[編集 (Edit) ] ソフトキーを押して、新しいバックアップ TFTP サーバの IP アドレスを入力します。</li> <li>3. [適用 (Apply) ] ソフトキーを押し、[保存 (Save) ] を押します。</li> </ol>
DHCP アドレス解放 (DHCP Address Released)	DHCP で割り当てられた IP アドレスを解放します。	[DHCP アドレス解放 (DHCP Address Released) ] オプションまでスクロールし、[編集 (Edit) ] ソフトキーを押した後、[Yes] ソフトキーを押して DHCP アドレスを解放します。

## 関連項目

- 「設定メニューの表示」 (P.4-2)
- 「オプションのロック解除とロック」 (P.4-3)
- 「設定値の編集」 (P.4-3)



## [セキュリティ設定 (Security Configuration) ]メニュー

[セキュリティ設定 (Security Configuration) ]メニューには、さまざまなセキュリティ設定に関する情報が表示されます。このメニューから、信頼リストファイルの画面と 802.1X 認証にアクセスできます。

表 4-3 にこのメニューのオプションを示します。

表 4-3 セキュリティメニュー設定

オプション	説明	変更の手順
セキュリティモード (Security Mode)	電話機に設定されているセキュリティモードを表示します。	Cisco Unified Communications Manager の管理ページで、[デバイス (Device) ]>[電話 (Phone) ]>[電話の設定 (Phone Configuration) ]を選択します。
LSC	ローカルで有効な証明書 (セキュリティ機能に使用) が電話機にインストールされている ([インストール済み (Installed) ]) か、インストールされていない ([未インストール (Not Installed) ]) かを示します。	電話機の LSC を管理する方法については、『Cisco Unified Communications Manager Security Guide』の「Using the Certificate Authority Proxy Function」の章を参照してください。
CTL	CTL がインストールされているかどうかを示します。	表示のみ (変更不可)。
信頼リスト (Trust List)	[信頼リスト (Trust List) ]には、信頼できるサーバ、CAPF サーバ、Call Manager/TFTP サーバのリストのサブメニューが表示されます。	詳細については、「[信頼リスト (Trust List) ]メニュー」(P.4-9) を参照してください。
802.1X 認証 (802.1X Authentication)	デバイス認証、EAP/MD5、トランザクションステータスを表示します。	「[802.1X 認証 (802.1X Authentication) ]および [802.1X 認証ステータス (802.1X Authentication Status) ]」(P.4-10) を参照してください。

## [信頼リスト (Trust List) ]メニュー

[信頼リスト (Trust List) ]メニューには、電話機が信頼しているすべてのサーバに関する情報が表示されます。表 4-4 に示すオプションが含まれます。

[信頼リスト (Trust List) ]メニューを終了するには、[戻る (Back) ]ソフトキーを押します。

表 4-4 [信頼リスト (Trust List) ]メニューの設定


オプション	説明	変更の手順
CTL 署名 (CTL Signature)	CTL ファイルの MD5 ハッシュを表示します。	このファイルの詳細については、『Cisco Unified Communications Manager Security Guide』の「Configuring the Cisco CTL Client」の章を参照してください。
CAPF サーバ (CAPF Server)	電話機で使用される CAPF サーバの (Cisco Unified Communications Manager 証明書に含まれる) 共通名。サーバが認証サーバの場合、認証済みのアイコン  が表示されます。	このファイルの詳細については、『Cisco Unified Communications Manager Security Guide』の「Configuring the Cisco CTL Client」の章を参照してください。

表 4-4 [信頼リスト (Trust List) ] メニューの設定 (続き)

オプション	説明	変更の手順
Unified CM/TFTP サーバ (Unified CM/TFTP Server)	電話機で使用される Cisco Unified Communications Manager および TFTP サーバの (Cisco Unified Communications Manager 証明書に含まれる) 共通名。サーバが認証サーバの場合、認証済みのアイコン  が表示されます。	このファイルの詳細については、『Cisco Unified Communications Manager Security Guide』の「 <a href="#">Configuring the Cisco CTL Client</a> 」の章を参照してください。
SRST ルータ (SRST Router)	電話機で使用可能な信頼できる SRST ルータが Cisco Unified Communications Manager の管理ページで設定されている場合、そのルータの (Cisco Unified Communications Manager 証明書に含まれる) 共通名。サーバが認証サーバの場合、認証済みのアイコン  が表示されます。	このファイルの詳細については、『Cisco Unified Communications Manager Security Guide』の「 <a href="#">Configuring the Cisco CTL Client</a> 」の章を参照してください。

## [802.1X 認証 (802.1X Authentication) ] および [802.1X 認証ステータス (802.1X Authentication Status) ]

[802.1X Authentication (802.1X 認証) ] および [802.1X 認証ステータス (802.1X Authentication Status) ] メニューでは、802.1X 認証を有効にし、トランザクション ステータスを表示できます。  
表 4-5 にこれらのオプションを示します。

これらのメニューを終了するには、[終了 (Exit) ] ソフトキーを押します。

表 4-5 802.1X 認証の設定

オプション	説明	変更の手順
デバイス認証 (Device Authentication)	<p>802.1X 認証が有効かどうかを示します。</p> <ul style="list-style-type: none"> <li>[有効 (Enabled) ]: 電話機は 802.1X 認証を使用してネットワーク アクセスを要求します。</li> <li>[無効 (Disabled) ]: デフォルト設定。電話機は CDP を使用して VLAN およびネットワークにアクセスします。</li> </ul>	<ol style="list-style-type: none"> <li>[アプリケーション (Applications) ] &gt; [管理者設定 (Admin Settings) ] &gt; [セキュリティ設定 (Security Config) ] &gt; [802.1X 認証 (802.1X Authentication) ] &gt; [デバイス認証 (Device Authentication) ] を選択します。</li> <li>[編集 (Edit) ] ソフトキーを押します。</li> <li>[デバイス認証 (Device Authentication) ] オプションを [有効 (Enabled) ] または [無効 (Disabled) ] に設定します。</li> <li>[保存 (Save) ] ソフトキーを押します。</li> </ol>
EAP-MD5	<p>[デバイス ID (Device ID) ]: 電話機のモデル番号と一意の MAC アドレスから生成され、CP-&lt;model&gt;-SEP-&lt;MAC&gt; の形式で表示されます。</p> <p>[共有シークレット (Shared Secret) ]: 電話機および認証サーバで使用するパスワードを選択します。パスワードには 6 ~ 32 文字の数字と文字を組み合わす。</p> <p>(注) 802.1X 認証を無効にするか、工場出荷時の状態にリセットすると、共有シークレットは削除されます。</p> <p>[レルム (Realm) ]: ユーザ ネットワーク ドメインを示します。常に [ネットワーク (Network) ] に設定されます。</p>	<ol style="list-style-type: none"> <li>[アプリケーション (Applications) ] &gt; [管理者設定 (Admin Settings) ] &gt; [セキュリティ設定 (Security Config) ] &gt; [802.1X 認証 (802.1X Authentication) ] &gt; [EAP/MD5] &gt; [デバイス ID (Device ID) ] を選択します。</li> <li>[編集 (Edit) ] ソフトキーを押します。</li> <li>デバイス ID を設定します。</li> <li>[保存 (Save) ] ソフトキーを押します。</li> </ol> <p>削除された共有シークレットを元に戻す方法については、「Cisco Unified IP Phone セキュリティのトラブルシューティング」(P.9-8) を参照してください。</p> <ol style="list-style-type: none"> <li>[アプリケーション (Applications) ] &gt; [管理者設定 (Admin Settings) ] &gt; [セキュリティ設定 (Security Config) ] &gt; [802.1X 認証 (802.1X Authentication) ] &gt; [EAP/MD5] &gt; [共有シークレット (Shared Secret) ] を選択します。</li> <li>[編集 (Edit) ] ソフトキーを押します。</li> <li>共有シークレットを入力します。</li> <li>[保存 (Save) ] ソフトキーを押します。</li> </ol>
トランザクション ステータス (Transaction Status)	802.1X 認証のトランザクション ステータスを表示します。	<ol style="list-style-type: none"> <li>[アプリケーション (Applications) ] &gt; [管理者設定 (Admin Settings) ] &gt; [セキュリティ設定 (Security Configuration) ] &gt; [802.1X 認証 (802.1X Authentication Status) ] を選択します。</li> </ol>

