VPN クライアント

VPN クライアントの概要

Cisco Unified IP 電話 向け Cisco VPN Client により、在宅勤務の従業員のためのセキュアな VPN 接続が実現します。Cisco VPN Client の設定はすべて Cisco Unified Communications Manager Administration で設定します。社内で電話を設定したら、ユーザはその電話をブロードバンドルータにつなぐだけで瞬時に組織のネットワークに接続できます。

（注） VPN メニューとそのオプションは、米国無制限輸出対象バージョンの Unified Communications Manager では利用できません。

VPN クライアントの前提条件

電話を事前にプロビジョニングし、社内ネットワーク内で初期接続を確立し、電話の設定を取得します。設定はすでに電話に取り込まれているため、これ以降はVPNを使用して接続を確立できます。

VPN クライアント設定のタスク フロー

電話を事前にプロビジョニングし、社内ネットワーク内で初期接続を確立し、電話の設定を取得します。設定はすでに電話に取り込まれているため、これ以降はVPNを使用して接続を確立できます。

手順

	コマンドまたはアクション	目的
Step 1	Cisco IOS の前提条件の完了 （3 ページ）	Cisco IOS の前提条件を満たします。Cisco IOS VPN を設定するには、このアクションを実行します。
Step 2	IP Phone をサポートするための Cisco IOS SSL VPN の設定 （3 ページ）	IP Phone で VPN クライアントの Cisco IOS を設定します。Cisco IOS VPN を設定するには、このアクションを実行します。
Step 3	AnyConnect 用の ASA 前提条件への対応 （5 ページ）	AnyConnect 用の ASA 前提条件を満たします。ASA VPN を設定するには、このアクションを実行します。
Step 4	IP Phone での VPN クライアント用の ASA の設定 （6 ページ）	IP Phone で VPN クライアントの ASA を設定します。ASA VPN を設定するには、このアクションを実行します。
Step 5	VPN ゲートウェイごとに VPN コンセントレータを設定します。	ユーザがリモート電話のファームウェアや設定情報をアップグレードするときに遅延が長くなるのを回避するため、VPN コンセントレータはネットワーク内の TFTP サーバまたは Unified Communications Manager サーバの近くにセットアップします。これがネットワーク内で不可能な場合、代替 TFTP サーバまたはロードサーバを VPN コンセントレータの横にセットアップすることもできます。
Step 6	VPN コンセントレータの証明書のアップロード （8 ページ）	VPN コンセントレータの証明書をアップロードします。
Step 7	VPN ゲートウェイの設定 （9 ページ）	VPN ゲートウェイを設定します。
Step 8	VPN グループの設定 （10 ページ）	VPN グループを作成した後、設定した VPN ゲートウェイのいずれかをそのグループに追加できます。
Step 9	次のいずれかを実行します。 • VPN プロファイルの設定 （11 ページ） • VPN 機能のパラメータの設定 （13 ページ）	VPN プロファイルを設定する必要があるのは、複数の VPN グループを使用している場合だけです。[VPN Profle] フィールドは、[VPN Feature Configuration] フィールドよりも優先されます。
Step 10	共通の電話プロファイルへの VPN の詳細の追加 （15 ページ）	共通の電話プロファイルに VPN グループおよび VPN プロファイルを追加します。

	コマンドまたはアクション	目的
Step 11	Cisco Unified IP 電話 のファームウェアを、VPN をサポートしているバージョンにアップグレードします。	To run the Cisco VPN client, a supported Cisco Unified IP 電話 must be running firmware release 9.0（2） or higher. ファームウェアのアップグレードの詳細については、ご使用の Cisco Unified IP 電話 モデルの Unified Communications Manager に関する『*Cisco Unified IP Phone Administration Guide*』を参照してください。
Step 12	サポートされている Cisco Unified IP 電話を使用して、VPN 接続を確立します。	Cisco Unified IP 電話 を VPN に接続します。

Cisco IOS の前提条件の完了

次の手順を使用して、Cisco IOS の前提条件を完了します。

手順

Step 1 Cisco IOS ソフトウェアバージョン 15.1(2)T 以降をインストールします。

機能セット/ライセンス：Universal（Data & Security & UC）for IOS ISR-G2 および ISR-G3

機能セット/ライセンス：Advanced Security for IOS ISR

Step 2 SSL VPN ライセンスをアクティベートします。

IP Phone をサポートするための Cisco IOS SSL VPN の設定

IP 電話をサポートするための Cisco IOS SSL VPN を実行するには、次の手順を使用します。

手順

Step 1 Cisco IOS をローカルで設定します。

a) ネットワーク インターフェイスを設定します。

例：

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b) 次のコマンドを使用してスタティック ルートとデフォルト ルートを設定します。

router(config)# **ip route** <*dest_ip*> < *mask*> < *gateway_ip*>

例：

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

Step 2 CAPF 証明書を生成および登録して LSC の入った IP Phone を認証します。

Step 3 Unified Communications Manager から CAPF 証明書をインポートします。

a) [Cisco Unified OS Administration] から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

（注） この場所は Unified Communications Manager のバージョンに基づきます。

b) Cisco_Manufacturing_CA および CAPF 証明書を見つけます。.pem ファイルをダウンロードし、.txt ファイルとして保存します。

c) Cisco IOS ソフトウェアでトラストポイントを作成します。

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

Base 64 で暗号化された CA 証明書を求められた場合は、ダウンロードした .pem ファイルのテキストを BEGIN 行および END 行とともにコピーし、貼り付けます。この手順を他の証明書にも繰り返します。

d) 次の Cisco IOS 自己署名証明書を生成して Unified Communications Manager に登録するか、または CA からインポートした証明書で置き換えます。

- 自己署名証明書を生成します。

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 2048 2048
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Unified Communications Manager の VPN プロファイルでホスト ID チェックを有効にして、自己署名証明書を生成します。

例：

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain
name>Router(config-ca-trustpoint)# subject-name CN=<full domain
name>, CN=<IP>Router(ca-trustpoint)#authorization username
subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- 生成された証明書を Unified Communications Manager に登録します。

  例：

  ```
  Router(config)# crypto pki export <name> pem terminal
  ```

  端末からテキストをコピーして、.pem ファイルとして保存し、これを Cisco Unified OS の管理を使用して、Unified Communications Manager にアップロードします。

Step 4 AnyConnect を Cisco IOS にインストールします。

AnyConnect パッケージを cisco.com からダウンロードし、フラッシュにインストールします。

例：

```
router(config)#webvpn install svc
flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

Step 5 VPN 機能を設定します。

（注） 電話で証明書とパスワード認証の両方を使用する場合は、電話の MAC アドレスを使用してユーザを作成します。ユーザ名の照合では、大文字と小文字が区別されます。次に例を示します。

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

AnyConnect 用の ASA 前提条件への対応

AnyConnect の前提条件を完了するには、次の手順を使用します。

手順

Step 1 ASA ソフトウェア（バージョン 8.0.4 以降）および互換性のある ASDM をインストールします。

Step 2 互換性のある AnyConnect パッケージをインストールします。

Step 3 ライセンスをアクティベートします。

a) 次のコマンドを実行して、現在のライセンスの機能を確認してください。

show activation-key detail

b) 必要な場合は、追加の SSL VPN セッションで新しいライセンスを取得し、Linksys 電話を有効にします。

Step 4 デフォルト以外の URL を持つトンネル グループが設定されていることを確認します。

```
tunnel-group phonevpn type remote-access
tunnel-group phonevpn general-attribute
  address-pool vpnpool
tunnel-group phonevpn webvpn-attributes
  group-url https://172.18.254.172/phonevpn enable
```

デフォルト以外の URL を設定するときは、次のことを考慮してください。

- ASA の IP アドレスにパブリック DNS エントリが含まれている場合、これを完全修飾ドメイン名（FQDN）に置き換えることができます。
- You can only use a single URL （FQDN or IP address） on the VPN gateway in Unified Communications Manager.
- 証明書 CN またはサブジェクト代行名が必要な場合は、グループ URL の FQDN または IP アドレスを一致させます。
- ASA 証明書の CN や SAN が FQDN や IP アドレスと一致しない場合は、Unified Communications Manager のホスト ID チェックボックスをオフにします。

IP Phone での VPN クライアント用の ASA の設定

VPN クライアント用の ASA を IP 電話で設定するには、次の手順を使用します。

（注） ASA 証明書を置き換えると、Unified Communications Manager は使用できなくなります。

手順

Step 1 ローカル設定

a) ネットワーク インターフェイスを設定します。

例：

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) スタティック ルートとデフォルト ルートを設定します。

ciscoasa(config)# **route** <interface_name> <ip_address> <netmask> <gateway_ip>

例：

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) DNS を設定します。

例：

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

Step 2 Unified Communications Manager と ASA に必要な証明書を生成して登録します。

から次の証明書をUnified Communications Managerインポートします。

- CallManager：TLS ハンドシェイク時の Cisco UCM の認証（混合モードのクラスタでのみ必要）。
- Cisco_Manufacturing_CA：製造元でインストールされる証明書（MIC）を使用した IP Phone の認証。
- CAPF：LSC を使用した IP Phone の認証。

これら Unified Communications Manager 証明書をインストールするには、次の手順を実行します。

a) [Cisco Unified OS Administration] から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

b) 証明書 Cisco_Manufacturing_CA と CAPF を見つけます。.pem ファイルをダウンロードし、.txt ファイルとして保存します。

c) ASA でトラストポイントを作成します。

例：

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

Base 64 でエンコードされた CA 証明書を求められた場合は、ダウンロードした .pem ファイル内のテキストを BEGIN 行および END 行とともにコピーして、貼り付けます。この手順を他の証明書にも繰り返します。

d) 次の ASA 自己署名証明書を生成して Unified Communications Manager に登録するか、または CA からインポートした証明書で置き換えます。

- 自己署名証明書を生成します。

  例：

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# keypair <name>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Unified Communications Manager の VPN プロファイルでホスト ID チェックを有効にして、自己署名証明書を生成します。

  例：

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
```

```
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- 生成された証明書を Unified Communications Manager に登録します。

  例：

  ```
  ciscoasa(config)# crypto ca export <name> identity-certificate
  ```

  端末からテキストをコピーして、.pem ファイルとして保存し、Unified Communications Manager にアップロードします。

Step 3 VPN 機能を設定します。以下に示すサンプル ASA 設定の概要を、設定のガイドとして利用できます。

（注） 電話で証明書とパスワード認証の両方を使用する場合は、電話の MAC アドレスを使用してユーザを作成します。ユーザ名の照合では、大文字と小文字が区別されます。次に例を示します。

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9
encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

ASA 証明書の設定

ASA 証明書の設定に関する詳細は、「ASA 上の証明書認証を使用した AnyConnect VPN 電話の設定」を参照してください。

VPN コンセントレータの証明書のアップロード

VPN 機能をサポートするようにセットアップする際に、ASA で証明書を生成します。生成された証明書を PC またはワークステーションにダウンロードしてから、この項で説明されている手順に従って、Unified Communications Manager にアップロードします。Unified Communications Manager は証明書を Phone-VPN-trust リストに保存します。

ASA は SSL ハンドシェイク時にこの証明書を送信し、Cisco Unified IP 電話 は、この証明書を電話と VPN 間の信頼リストに格納されている値と比較します。

ローカルで重要な証明書 (LSC) が Cisco Unified IP 電話 にインストールされている場合、デフォルトではその LSC が送信されます。

デバイス レベルの証明書認証を使用するには、ASA にルート MIC または CAPF 証明書をインストールして、Cisco Unified IP 電話 が信頼されるようにします。

Unified Communications Manager に証明書をアップロードするには、Cisco Unified OS Administration を使用します。

手順

Step 1 [Cisco Unified OS 管理（Cisco Unified OS Administration）] から、以下を選択します。 **[セキュリティ] > [証明書の管理]**

Step 2 [証明書のアップロード] をクリックします。

Step 3 [証明書の目的（Certificate Purpose）] ドロップダウンリストで、[Phone-VPN-trust] を選択します。

Step 4 [ブラウズ（Browse）] をクリックして、アップロードするファイルを選択します。

Step 5 **[ファイルのアップロード（Upload File）]** をクリックします。

Step 6 アップロードする別のファイルを選択するか、[閉じる（Close）] をクリックします。

詳細については、「証明書の管理」の 章を参照 してください。

VPN ゲートウェイの設定

VPN ゲートウェイごとに VPN コンセントレータが設定されていることを確認します。VPN コンセントレータの設定後、VPN コンセントレータの証明書をアップロードします。詳細については、VPN コンセントレータの証明書のアップロード（8 ページ）を参照してください。

VPN ゲートウェイを設定するには、この手順を使用します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[拡張機能（Advanced Features）] > [VPN] > [VPN ゲートウェイ（VPN Gateway）]** を選択します。

Step 2 次のいずれかの操作を実行します。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。

b) コピーする VPN ゲートウェイの横にある **[コピー（Copy）]**をクリックします。

c) 適切な VPN ゲートウェイを見つけて、設定を変更し、既存のプロファイルを更新します。

Step 3 [VPN Gateway Configuration] ウィンドウでフィールドを設定します。詳細については、VPN クライアントの VPN ゲートウェイ フィールド（9 ページ）を参照してください。

Step 4 **[保存]** をクリックします。

VPN クライアントの VPN ゲートウェイ フィールド

VPN クライアントの VPN ゲートウェイフィールドについての説明をします。

表 *1 : VPN* クライアントの *VPN* ゲートウェイ フィールド

フィールド	説明
[VPNゲートウェイ名(VPN Gateway Name)]	VPN ゲートウェイの名前を入力します。
[VPNゲートウェイの説明(VPN Gateway Description)]	VPN ゲートウェイの説明を入力します。
[VPNゲートウェイのURL(VPN Gateway URL)]	ゲートウェイ内の主要な VPN コンセントレータの URL を入力します。 （注） VPN コンセントレータに 1 つのグループ URL を設定し、この URL をゲートウェイ URL として使用する必要があります。 設定情報については、次のような VPN コンセントレータのマニュアルを参照してください。 • 『*SSL VPN Client (SVC) on ASA with ASDM Configuration Example*』
[この場所のVPN証明書(VPN Certificates in this Location)]	上矢印キーおよび下矢印キーを使用して、証明書をゲートウェイに割り当てます。ゲートウェイに証明書を割り当てないと、VPN クライアントはこのコンセントレータへの接続に失敗します。 （注） 最大 10 の証明書を 1 つの VPN ゲートウェイに割り当てることができます。また、各ゲートウェイに少なくとも 1 つの証明書を割り当てる必要があります。電話と VPN 間の信頼性権限に関係付けられた証明書だけが、使用可能な VPN 証明書のリストに表示されます。

VPN グループの設定

VPN グループを設定するには、この手順を使用します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[拡張機能（Advanced Features）] > [VPN] > [VPN グループ（VPN Group）]** を選択します。

Step 2 次のいずれかの操作を実行します。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。
b) 既存の VPN グループをコピーする VPN グループの横にある **[コピー（copy）]** をクリックします。
c) 適切な VPN ゲートウェイを見つけて、設定を変更し、既存のプロファイルを更新します。

Step 3 [VPN Group Configuration] ウィンドウ内の各フィールドを設定します。詳細については、フィールド説明の詳細について、VPN クライアントの VPN ゲートウェイ フィールド（9 ページ） を参照してください。

Step 4 **[保存]** をクリックします。

VPN クライアントの VPN グループ フィールド

この表では、VPN クライアントの VPN グループフィールドについて説明しています。

表 *2: VPN* クライアントの *VPN* グループ フィールド

フィールド	定義
[VPNグループ名(VPN Group Name)]	VPN グループの名前を入力します。
[VPNグループの説明(VPN Group Description)]	VPN グループの説明を入力します。
[使用可能なすべてのVPNゲートウェイ(All Available VPN Gateways)]	スクロールして、使用可能なすべての VPN ゲートウェイを表示します。
[このVPNグループ内で選択されたゲートウェイ(Selected VPN Gateways in this VPN Group)]	上矢印ボタンと下矢印ボタンを使用して、使用可能な VPN ゲートウェイをこの VPN グループに入れたりグループから外したりします。 VPN クライアントで重要なエラーが発生し、特定の VPN ゲートウェイに接続できない場合は、リストの次の VPN ゲートウェイへの移動を試みます。 （注） 1 つの VPN グループに最大 3 つの VPN ゲートウェイを追加できます。また、VPN グループ内の証明書数は、合計で 10 までです。

VPN プロファイルの設定

VPN プロファイルを設定するには、この手順を使用します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[拡張機能（Advanced Features）] > [VPN] > [VPN プロファイル（VPN Profile）]** を選択します。

Step 2 次のいずれかの操作を実行します。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。

b) 既存のプロファイルをコピーする VPN プロファイルの横にある **[コピー（copy）]** をクリックします。

c) 既存のプロファイルを更新するには、該当するフィルタを [Find VPN Profile Where] で指定し、[検索（Find）] をクリックして設定を変更します。

Step 3 [VPN Profile Configuration] ウィンドウで各フィールドを設定します。詳細については、フィールド説明の詳細について、VPN クライアントの VPN プロファイル フィールド（12 ページ） を参照してください。

Step 4 **[保存]** をクリックします。

VPN クライアントの VPN プロファイル フィールド

この表では、VPN プロファイルフィールドの詳細について説明します。

表 3 : VPN プロファイル フィールドの詳細

フィールド	定義
名前	VPN プロファイルの名前を入力します。
説明	VPN プロファイルの説明を入力します。
[自動ネットワーク検出を有効化(Enable Auto Network Detect)]	このチェックボックスをオンにすると、VPN クライアントは、社内ネットワーク外にあることが検出された場合に限り実行できます。 デフォルト：[無効(Disabled)]
最大伝送ユニット（MTU）	最大伝送ユニット（MTU）のサイズをバイト数で入力します。 デフォルト：1290 バイト
[接続の失敗(Fail to Connect)]	VPN トンネルの作成中に、ログインまたは接続操作が完了するまで待機する時間を指定します。 デフォルト：30 秒
[ホストIDチェックを有効化(Enable Host ID Check)]	このチェックボックスがオンの場合、ゲートウェイ証明書の subjectAltName または CN が、VPN クライアントの接続先の URL と一致している必要があります。 デフォルト：[有効(Enabled)]

フィールド	定義
[クライアント認証方式(Client Authentication Method)]	ドロップダウン リストから、クライアント認証方式を選択します。 • [ユーザおよびパスワード(User and password)] • [パスワードのみ(Password only)] • [証明書(Certificate)]（LSC または MIC）
[永続的パスワードを有効化(Enable Password Persistence)]	このチェックボックスをオンにすると、ログインの失敗、ユーザによる手動のパスワードのクリア、電話のリセット、または電源が切れるまで、ユーザのパスワードは電話に保存されます。

VPN 機能のパラメータの設定

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[拡張機能（Advanced Features）] > [VPN] > [VPN 機能設定（VPN Feature Configuration）]**。

Step 2 [VPN Feature Configuration] ウィンドウのフィールドを設定します。詳細については、VPN 機能のパラメータ （13 ページ）を参照してください。

Step 3 **[保存] をクリックします。**

次の作業を行います。

- Cisco Unified IP Phone のファームウェアを、VPN をサポートしているバージョンにアップグレードします。ファームウェアのアップグレード方法の詳細については、ご使用の Cisco Unified IP 電話 モデルの『*Cisco Unified IP Phone Administration Guide*』を参照してください。
- サポートされている Cisco Unified IP 電話 を使用して、VPN 接続を確立します。

VPN 機能のパラメータ

VPN 機能パラメータの説明を表に示します。

表 *4: VPN* 機能のパラメータ

フィールド	デフォルト
[自動ネットワーク検出を有効化(Enable Auto Network Detect)]	[True] の場合、VPN クライアントは、社内ネットワーク外にあることが検出された場合に限り実行できます。 デフォルト：False

フィールド	デフォルト
最大伝送ユニット（MTU）	最大伝送単位を指定します。 デフォルト：1290 バイト 最小値：256 バイト 最大値：1406 バイト
[Keep Alive]	キープ アライブ メッセージを送信する間隔を指定します。 （注） この値がゼロ以外であり、かつ Unified Communications Manager で指定された値よりも小さい場合、VPN コンセントレータのキープ アライブ設定によってこの設定が上書きされます。 デフォルト：60 秒 最小値：0 秒 最大値：120 秒
[接続の失敗(Fail to Connect)]	VPN トンネルの作成中に、ログインまたは接続操作が完了するまで待機する時間を指定します。 デフォルト：30 秒 最小値：0 秒 最大値：600 秒
[クライアント認証方式(Client Authentication Method)]	ドロップダウン リストから、クライアント認証方式を選択します。 • [ユーザおよびパスワード(User and password)] • [パスワードのみ(Password only)] • [証明書(Certificate)]（LSC または MIC） デフォルト：[ユーザおよびパスワード(User and password)]
[永続的パスワードを有効化(Enable Password Persistence)]	Trueの場合、リセットにResetボタンまたは「**#**」が使用されていると、ユーザーのパスワードが電話機に保存されます。電話機の電源が切れた場合、または工場出荷時の設定にリセットされた場合、パスワードは保存されず、電話機は認証情報の入力を求めるプロンプトを表示します。 デフォルト：False
[ホストIDチェックを有効化(Enable Host ID Check)]	[True] の場合、ゲートウェイ証明書の subjectAltName または CN が、VPN クライアントの接続先の URL と一致している必要があります。 デフォルト：[True]

共通の電話プロファイルへの VPN の詳細の追加

一般的な電話プロファイルに VPN の詳細を追加するには、次の手順を使用します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[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）]**。

Step 2 [検索（**Find**）] をクリックして、VPN の詳細を追加する共通電話プロファイルを選択します。

Step 3 [VPN情報（VPN Information）] セクションで、適切な [VPNグループ（VPN Group）] および [VPNプロファイル（VPN Profile）] を選択します。

Step 4 [保存（**Save**）] と [設定の適用（**Apply Config**）] をクリックします。

Step 5 設定の適用ウィンドウで [**OK**] をクリックします。