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] メニューおよびこのメニューのオプションは、Unified Communications Manager の U.S. 輸出制限バージョンでは使用できません。

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

始める前に

手順

	コマンドまたはアクション	目的
ステップ 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。
ステップ 2	IP Phone をサポートするための Cisco IOS SSL VPN の設定 （4 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。
ステップ 3	AnyConnect 用の ASA 前提条件への対応 （5 ページ）	AnyConnect 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。
ステップ 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。
ステップ 5	VPN ゲートウェイごとに VPN コンセントレータを設定	リモート電話のファームウェアや設定情報をユーザがアップグレードする際の長い遅延を回避するには、ネットワーク内で TFTP サーバまたは Unified Communications Manager サーバの近くで VPN コンセントレータを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。
ステップ 6	VPN コンセントレータの証明書のアップロード （9 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。
ステップ 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。
ステップ 8	VPN グループの設定 （11 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。

	コマンドまたはアクション	目的
ステップ 9	次のいずれかの操作を行います。 • VPN プロファイルの設定 （12 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。
ステップ 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。
ステップ 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。	Cisco VPN クライアントを実行するには、サポートされている Cisco Unified IP 電話 でファームウェア リリース 9.0(2) 以降が稼動している必要があります。ファームウェアのアップグレード方法の詳細は、ご使用の Cisco Unified IP 電話 のモデルの Unified Communications Manager 向け『*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。
ステップ 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

手順

ステップ 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

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

ステップ 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

手順

ステップ 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
```

ステップ 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。

ステップ 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 ソフトウェア上に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。他の証明書について、この手順を繰り返します。

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 からインポートする証明書と置き換えます。

- 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> 1024 1024
```

```
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
```

- 生成した証明書を 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 Administration] を使って Unified Communications Manager にアップロードします。

ステップ 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
```

ステップ 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

手順

ステップ 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。

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

ステップ 3 ライセンスをアクティベートします。

a) 次のコマンドを使用して、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) 必要に応じて、追加の SSL VPN セッションと LINKSYS 電話が有効になっている新しいライセンスを取得します。

ステップ 4 デフォルト以外の URL を使用してトンネル グループが設定されていることを次のように確認してください。

```
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。
- Unified Communications Manager では VPN ゲートウェイに対して単一 URL（FQDN または IP アドレス）のみを使用できます。
- 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（Host 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

（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

ステップ 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
```

ステップ 2 Unified Communications Manager と ASA に必要な証明書を生成および登録します。

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

- 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ついて繰り返します。

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 からインポートする証明書と置き換えます。

- 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
```

- 生成した証明書を 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。

ステップ 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 での証明書認証済みの 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を使用して Unified Communications Manager にアップロードします。Unified Communications Manager は、電話と VPN 間の信頼リストに証明書を保存します。

ASA は SSL ハンドシェイク中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 間の信頼リストに保存されている値と比較します。

Cisco Unified IP 電話 は、[製造元でインストールされる証明書（MIC）（Manufacturer Installed Certificate (MIC)）]をデフォルトで送信します。CAPF サービスを設定すると、Cisco Unified IP 電話 は [ローカルで有効な証明書（LSC）（Locally Significant Certificate (LSC)）]を送信します。

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 の管理を使用します。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[証明書のアップロード（Upload Certificate）]** をクリックします。

[証明書のアップロード（Upload Certificate）] ダイアログボックスが表示されます。

ステップ 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。

ステップ 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。

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

ステップ 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。

証明書管理の詳細については、『Administration Guide for Cisco Unified Communications Manager』を参照してください。

VPN ゲートウェイの設定

始める前に

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 （9 ページ）を参照してください。

手順

ステップ 1 [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）]**。

ステップ 2 次のいずれかの作業を実行します。

a) 新しいプロファイルを設定するには、**[新規追加（Add New）]** をクリックします。
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) 既存のプロファイルを更新するには、適切な VPN ゲートウェイを見つけて、設定を変更します。

ステップ 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 （10 ページ）を参照してください。

ステップ 4 **[保存 (Save)]** 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

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 Gateway Name]	VPN ゲートウェイの名前を入力します。
[VPN Gateway Description]	VPN ゲートウェイの説明を入力します。
[VPN Gateway URL]	ゲートウェイのメイン 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。 設定についての情報は、以下のような VPN コンセントレータのドキュメントを参照してください。 • 『*SSL VPN Client (SVC) on ASA with ASDM Configuration Example*』
[VPN Certificates in this Gateway]	上矢印キーと下矢印キーを使用して、ゲートウェイに証明書を割り当てます。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） VPN ゲートウェイには最大 10 の証明書を割り当てることができます。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。Phone-VPN-trust 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

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[高度な機能（Advanced Features）]** > **[VPN]** > **[VPN グループ（VPN Group）]**。

ステップ 2 次のいずれかの作業を実行します。

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

b) 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、既存の VPN グループをコピーします。

c) 既存のプロファイルを更新するには、適切な VPN グループを見つけて、その設定を変更します。

ステップ 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、「VPN クライアントの VPN ゲートウェイ フィールド （10 ページ）」のフィールド説明詳細を参照してください。

ステップ 4 **[保存 (Save)]** 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

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 Group Name]	VPN グループの名前を入力します。
[VPN Group Description]	VPN グループの説明を入力します。
[All Available VPN Gateways]	スクロールして、すべての使用可能な VPN ゲートウェイを確認できます。
[Selected VPN Gateways in this VPN Group]	上矢印キーと下矢印キーを使用して、使用可能な VPN ゲートウェイをこの VPN グループの内外に移動します。 VPN クライアントで重大なエラーが発生し、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の合計数は 10 以下にする必要があります。

VPN プロファイルの設定

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[高度な機能（Advanced Features）]** > **[VPN]** > **[VPN プロファイル（VPN Profile）]**。

ステップ 2 次のいずれかの作業を実行します。

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

b) 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、既存の VPN プロファイルをコピーします。

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。

ステップ 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、「VPN クライアントの VPN プロファイル フィールド （12 ページ）」のフィールド説明詳細を参照してください。

ステップ 4 **[保存 (Save)]** 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

表 *3: VPN* プロファイル フィールドの詳細

フィールド	定義
[Name]	VPN プロファイルの名前を入力します。
[Description]	VPN プロファイルの説明を入力します。
[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、社内ネットワークの外にいることを検出した場合に限り動作します。 デフォルトで、ディセーブルになっています。
[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。 デフォルト値：1290 バイト
[Fail to Connect]	このフィールドは、システムが VPN トンネルの作成中にログイン操作または接続操作が完了するまで待つ時間を指定します。 デフォルト：30 秒

フィールド	定義
[Enable Host ID Check]	このチェックボックスをオンにした場合は、ゲートウェイの証明書の 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
[Client Authentication Method]	ドロップダウンリストからクライアント認証方法を選択します。 • [User and Password] • [Password only] • [Certificate (LSC or MIC)]
[Enable Password Persistence]	このチェックボックスをオンにすると、ログイン試行の失敗、ユーザによるパスワードの手動でのクリア、または電話機のリセットや電源切断が発生するまで、ユーザ パスワードが電話機に保存されます。

VPN 機能のパラメータの設定

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[高度な機能（Advanced Features）]** > **[VPN]** > **[VPN 機能設定（EMCC Feature Configuration）]**。

ステップ 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 （14 ページ）を参照してください。

ステップ 3 **[保存（Save）]** をクリックします。

次のタスク

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は、ご使用の Cisco Unified IP 電話 のモデルの『*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。
- 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

表 *4 : VPN* 機能のパラメータ

フィールド	デフォルト
[Enable Auto Network Detect]	True の場合、VPN クライアントは、社内ネットワークの外にいることを検出した場合に限り動作します。 デフォルト：False
[MTU]	このフィールドは最大伝送ユニットを指定します。 デフォルト値は 1290 バイトです。 最小値：256 バイト 最大値：1406 バイト
[Keep Alive]	このフィールドは、システムがキープアライブ メッセージを送信するレートを指定します。 （注） Unified Communications Manager で指定した値よりも小さい値（ゼロ以外）を指定した場合、この値は VPN コンセントレータのキープアライブ設定によって上書きされます。 デフォルト：60 秒 最小値：0 最大値：120 秒
[Fail to Connect]	このフィールドは、システムが VPN トンネルの作成中にログイン操作または接続操作が完了するまで待つ時間を指定します。 デフォルト：30 秒 最小値：0 最大値：600 秒
[Client Authentication Method]	ドロップダウンリストからクライアント認証方法を選択します。 • [User and Password] • [Password only] • [Certificate (LSC or MIC)] デフォルト：User And Password

フィールド	デフォルト
[Enable Password Persistence]	[True] の場合、[Reset] ボタンまたは「**#**」 がリセットに使用されると、ユーザ パスワードは電話に保存されます。電話の電源が切断されたり、工場出荷時の状態にリセットされたりすると、パスワードは保存されず電話からクレデンシャルの入力が求められます。 デフォルト：False
[Enable Host ID Check]	[True] の場合、ゲートウェイの証明書の subjectAltName または CN が、VPN クライアントが接続する URL に一致する必要があります。 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

手順

ステップ 1 [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）]**。

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

ステップ 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。

ステップ 4 **[保存（Save）]**、**[設定の適用（Apply Config）]** の順にクリックします。

ステップ 5 [設定を適用（Apply Configuration）] ウィンドウで、**[OK]** をクリックします。