VPN クライアント

VPN クライアントの概要

Cisco Unified IP Phone 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 CM の管理（Cisco Unified CM 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 Cisco 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て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 クライアントの設定タスク フロー

はじめる前に

- VPN クライアントの前提条件，（1 ページ）を確認してください。

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 フォン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。
ステップ 3	AnyConnect 用の ASA 前提条件の充足, （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際は、長い遅延を回避するため、ネットワーク内で TFTP サーバまたは Cisco 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, （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。
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。
ステップ 9	次のいずれかを実行します。 • VPN プロファイルの設定, （13 ページ） • VPN 機能のパラメータの設定, （15 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 Profile] 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, （17 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
ステップ 11	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。	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 Phone 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については、使用している Cisco Unified IP Phone モデルの『*Cisco Unified IP Phone* Administration Guide for Cisco Unified Communications Manager』を参照してください。
ステップ 12	VPN をサポートしている Cisco Unified IP Phone を使用し、VPN 接続を確立します。	Cisco Unified IP Phone を VPN に接続します。

Cisco IOS の前提条件の完了

IP 電話で VPN クライアントの Cisco IOS 設定を作成する前に、次の手順を実行してください。

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：IOS ISR-G2 用 Universal (Data & Security & UC)

機能セット/ライセンス：IOS ISR 用の高度なセキュリティ

ステップ 2 SSL VPN ライセンスをアクティベートします。

次の作業

IP フォンをサポートするための Cisco IOS SSL VPN の設定, （3 ページ）

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

はじめる前に

Cisco IOS の前提条件の完了, （3 ページ）

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 フォンを認証します。

ステップ 3 Cisco 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 のバージョンによって変わる可能性があります。

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 Cisco 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> 1024 1024
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Cisco 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 Cisco 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 の管理を使って Cisco 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） 電話機で証明書とパスワード認証の両方を使用する場合は、電話機の MAC アドレスを持つ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
```

次の作業

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。

AnyConnect 用の ASA 前提条件の充足

IP 電話で VPN クライアントの ASA 設定を作成する前に、次の手順を実行してください。

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 をもったトンネル 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 アドレスがパブリック DNS にエントリしている場合、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。
- Cisco Unified Communications Manager の VPN ゲートウェイでは、単一 URL（FQDN または IP アドレス）のみ使用できます。
- 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、Cisco Unified Communications Manager のホスト ID チェックを無効にします。

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、Cisco Unified Communications Manager は使用できなくなります。

IP Phone で VPN クライアント用に ASA を設定するには、次の手順を実行します。

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 Cisco Unified Communications Manager および ASA に必要な証明書を生成して登録します。
Cisco 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：Manufacturer Installed Certificate（MIC; 製造元でインストールされた証明書）を使用した IP Phone の認証。
- CAPF：LSC を使用した IP Phone の認証。

Cisco Unified Communications Manager のこれらの証明書をインポートするには、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。他の証明書について、この手順を繰り返します。

d) 次の ASA 自己署名証明書を生成して Cisco 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
```

- Cisco 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 Cisco 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、Cisco 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。次の項に示したサンプルの ASA 設定の概要を設定のガイドとして利用できます。

（注） 電話機で証明書とパスワード認証の両方を使用する場合は、電話機の MAC アドレスを持つ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 証明書の設定の詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a0080bef910.shtml 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ためにセットアップする際に、ASAで証明書を作成します。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、このセクションで説明されている手順で Cisco Unified Communications Manager にアップロードします。Cisco Unified Communications Manager は、電話と VPN 間の信頼リストの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 Phone が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。

Cisco Unified IP Phone は、製造元でインストールされる証明書（MIC）をデフォルトで送信します。認証局プロキシ機能（CAPF）サービスを設定すると、Cisco Unified IP Phone はローカルで有効な証明書（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 または認証局プロキシ機能（CAPF）をインストールして、Cisco Unified IP Phone が信頼されるようにします。

Cisco 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

ステップ 1 [Cisco Unified OS の管理（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。
[証明書の一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 [証明書のアップロード] 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 [証明書目的（Certificate Purpose）] ドロップダウンリストで、[電話と VPN 間の信頼（Phone-VPN-trust）] を選択します。

ステップ 4 [参照（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] 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。
証明書の管理の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.htmlの『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

次の作業

VPN ゲートウェイの設定, （9 ページ）

VPN ゲートウェイの設定

VPN ゲートウェイを追加、更新またはコピーするには、次の手順を実行します。

はじめる前に

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, （8 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] で、[詳細機能（Advanced Features）] > [VPN] > [VPN ゲートウェイ（VPN Gateway）] を選択します。

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追加するには、[新規追加（Add New）] をクリックします。

b) 既存の VPN ゲートウェイをコピーするには、適切なプロファイルを見つけ、コピーする VPN ゲートウェイの横にある [コピー（Copy）] ボタンをクリックします。

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。

[新規追加（Add New）] をクリックすると、各フィールドがデフォルト設定になっている設定ウィンドウが表示されます。[コピー（Copy）] をクリックすると、設定ウィンドウにコピーされた設定が表示されます。

ステップ 3 [VPN ゲートウェイ設定（VPN Gateway Configuration）] ウィンドウでフィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクション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。

次の作業

VPN グループの設定, （11 ページ）

関連トピック

VPN クライアントの VPN ゲートウェイ フィールド, （10 ページ）

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。

フィールド	説明
[VPN ゲートウェイの URL（VPN Gateway URL）]	ゲートウェイのメインの 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テーションを参照してください。 • 『*SSL VPN Client (SVC) on ASA with ASDM Configuration Example*』
[このゲートウェイの VPN 証明書（VPN Certificates in this Gateway）]	↑キーと↓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

VPN グループを追加、更新、またはコピーするには、次の手順を実行します。

はじめる前に

VPN ゲートウェイの設定, （9 ページ）

手順

ステップ 1 [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] で、[拡張機能（Advanced Features）] > [VPN] > [VPN グループ（VPN Group）] を選択します。

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追加するには、[新規追加（Add New）] をクリックします。

b) 既存の VPN グループをコピーするには、適切なプロファイルを見つけて、コピーする VPN グループの横にある [コピー（Copy）] ボタンをクリックします。
c) 既存のプロファイルを更新するには、適切な VPN グループを見つけて、その設定を変更します。
[新規追加（Add New）] をクリックすると、各フィールドにデフォルト設定が含まれた設定ウィンドウが表示されます。[コピー（Copy）] をクリックすると、コピーした設定が含まれた設定ウィンドウが表示されます。

ステップ 3 [VPN グループの設定（VPN Group Configuration）] ウィンドウ内の各フィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクション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。

次の作業

次のいずれかの作業を実行します。

- VPN プロファイルの設定, （13 ページ）
- VPN 機能のパラメータの設定, （15 ページ）

関連トピック

VPN クライアントの VPN グループ フィールド, （12 ページ）
VPN クライアントの VPN グループ フィールド, （12 ページ）

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、すべての使用可能な VPN ゲートウェイを確認できます。

フィールド	定義
[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）]	↑キーと↓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

VPN プロファイルの追加、更新、またはコピーを行うには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] で、[拡張機能（Advanced Features）] > [VPN] > [VPN プロファイル（VPN Profile）] を選択します。

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追加するには、[新規追加（Add New）] をクリックします。

b) 既存のプロファイルをコピーするには、適切なプロファイルを検索し、VPN プロファイルの横にある[コピー（Copy）] ボタンをクリックします。

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 [VPN プロファイルの検索（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。
[新規追加（Add New）] をクリックすると、各フィールドにデフォルト設定が入力された設定ウィンドウが表示されます。[コピー（Copy）]をクリックすると、コピーした設定が入力された設定ウィンドウが表示されます。

ステップ 3 [VPN プロファイル設定（VPN Profile Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクション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。

関連トピック

VPN クライアントの VPN プロファイル フィールド, （14 ページ）

VPN クライアントの VPN プロファイル フィールド

フィールド	定義
[名前（Name）]	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：無効
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
[接続の失敗（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を待つ、またはオペレーションに接続して完了するまでの時間を指定します。 デフォルトは 30 秒です。
[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をオンにすると、ゲートウェイの証明書の subjectAltName または CN は、VPN クライアントが接続されている相手の URL と一致する必要があります。 デフォルト：有効
[クライアント認証方法（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。 • ユーザおよびパスワード • パスワードのみ • 証明書（LSC または MIC）
[イネーブル パスワード永続化（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

ステップ 1 [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] で、[詳細機能（Advanced Features）] > [VPN] > [VPN 機能設定（VPN Feature Configuration）] を選択します。

ステップ 2 [VPN 機能設定（VPN Feature Configuration）] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、関連項目のセクション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。

次の作業

次の作業を実行します。

- 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 Phone のモデルの『 *Cisco Unified IP Phone Administration Guide* 』を参照してください。
- VPN をサポートしている Cisco Unified IP Phone を使用し、VPN 接続を確立します。

関連トピック

VPN 機能のパラメータ, （15 ページ）

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：[いいえ（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。 最小値は 256 バイトです。 最大値は 1406 バイトです。

フィールド	デフォルト
[キープアライブ（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） これがゼロ以外で、 Cisco Unified Communications Manager で指定された値より少ない場合、VPN コンセントレータのキープアライブ設定はこの設定を上書きします。 デフォルトは 60 秒です。 最小値：0 最大値：120 秒
[接続の失敗（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を待つ、またはオペレーションに接続して完了するまでの時間を指定します。 デフォルトは 30 秒です。 最小値：0 最大値：600 秒
[クライアント認証方法（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。 • ユーザおよびパスワード • パスワードのみ • 証明書（LSC または MIC） デフォルト：ユーザおよびパスワード
イネーブルパスワード永続化（Enable Password Persistence）	True の場合、リセット 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機内に保存されます。電話機の電源が切断されたり、工場出荷時の状態にリセットすると、パスワードは保存されず電話にクレデンシャルの入力が求められます。 デフォルト：[いいえ（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：[はい（True）]

共通の電話プロファイルへの VPN の詳細の追加

はじめる前に

VPN プロファイルの設定, （13 ページ）

手順

ステップ 1 [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）] の順に選択します。
[共通の電話プロファイルの検索と一覧表示（Find and List Common Phone Profiles）] ウィンドウが開きます。

ステップ 2 使用する検索条件を選択します。

ステップ 3 **[検索（Find）]** をクリックします。
検索条件に一致する共通の電話プロファイルの一覧がウィンドウに表示されます。

ステップ 4 VPN の詳細を追加する共通の電話プロファイルをクリックします。
[共通の電話プロファイルの設定（Find and List Common Phone Profiles）] ウィンドウが開きます。

ステップ 5 [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 6 [保存（Save）] をクリックします。

ステップ 7 [設定の適用（Apply Config）] をクリックします。
[設定を適用（Apply Configuration）] ウィンドウが表示されます。

ステップ 8 [OK] をクリックします。

次の作業

次の作業を実行します。

- 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 Phone のモデルの『 *Cisco Unified IP Phone Administration Guide* 』を参照してください。
- VPN をサポートしている Cisco Unified IP Phone を使用し、VPN 接続を確立します。