



VPN ゲートウェイの設定

VPN ゲートウェイを設定するには、最初に、VPN コンセントレータの証明書をアップロードしてから、VPN ゲートウェイを設定する必要があります。

この章は、次の内容で構成されています。

- 「VPN コンセントレータの証明書のアップロード」(P.18-1)
- 「VPN ゲートウェイの設定」(P.18-2)

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 ASA をセットアップする場合は、ASA で証明書を生成することをお勧めします。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、この項の手順を使用して Cisco Unified Communications Manager にアップロードします。Cisco Unified Communications Manager は、証明書を電話と VPN 間の信頼リストに保存します。

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 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。

Cisco Unified IP Phone はデフォルトでその Manufacturer Installed Certificate (MIC; 製造元でインストールされる証明書) を送信します。CAPF サービスを設定している場合には、Cisco Unified IP Phone はその Locally Significant Certificate (LSC; ローカルで有効な証明書) を送信します。

デバイス レベルの証明書認証を使用する場合は、Cisco Unified IP Phone が信頼されるように、ルート MIC または CAPF 証明書を ASA にインストールする必要があります。

Cisco Unified Communications オペレーティング システムを使用して、証明書を Cisco Unified Communications Manager にアップロードします。次の手順に従って、VPN コンセントレータの証明書をアップロードします。

手順

- ステップ 1** Cisco Unified Communications オペレーティング システムの管理から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
[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 (Upload Certificate)] をクリックします。
[証明書のアップロード (Upload Certificate)] ポップアップ ウィンドウが表示されます。
- ステップ 3** [証明書の名前 (Certificate Name)] プルダウン メニューから、[電話と VPN 間の信頼性 (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 (Upload File)] をクリックします。
- ステップ 6** アップロードするファイルをさらに選択するか、または [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、『Cisco Unified Communications Operating System Administration Guide』の第 6 章「Security」を参照してください。

VPN ゲートウェイの設定

この項は、次の内容で構成されています。

- 「VPN ゲートウェイの検索」 (P.18-2)
- 「VPN ゲートウェイの設定」 (P.18-3)

VPN ゲートウェイの検索

VPN ゲートウェイを検索するには、次の手順を実行します。

手順

- ステップ 1** Cisco Unified Communications Manager の管理ページで、[拡張機能 (Advanced Features)] > [VPN] > [VPN ゲートウェイ (VPN Gateway)] の順に選択します。

[VPN ゲートウェイの検索と一覧表示 (Find and List VPN Gateways)] ウィンドウが表示されます。アクティブな（前の）クエリーのレコードもウィンドウに表示される場合があります。

- ステップ 2** データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、**ステップ 3** に進みます。

レコードをフィルタリングまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスから、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスから、検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。



(注) 検索条件を追加するには、[+] ボタンをクリックします。条件を追加すると、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

- ステップ 3** [検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4 表示されたレコードリストから、目的のレコードのリンクをクリックします。



(注) リストの見出しに上向きまたは下向きの矢印がある場合は、その矢印をクリックして、ソート順序を逆にします。

ウィンドウに選択した項目が表示されます。

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。

手順

ステップ 1 Cisco Unified Communications Manager の管理ページで、[拡張機能 (Advanced Features)] > [VPN] > [VPN ゲートウェイ (VPN Gateway)] の順に選択します。

ステップ 2 次の作業のいずれかを実行します。

- 新しいプロファイルを追加するには、検索ウィンドウの [新規追加 (Add New)] をクリックし、**ステップ 3** に進みます。
- 既存の VPN ゲートウェイをコピーするには、「VPN ゲートウェイの検索」(P.18-2) の説明に従い、適切なプロファイルを見つけて、コピーする VPN ゲートウェイの横に表示されている [コピー (Copy)] ボタンをクリックし、**ステップ 3** に進みます。
- 既存のプロファイルを更新するには、「VPN ゲートウェイの検索」(P.18-2) の説明に従い、適切な VPN ゲートウェイを見つけて、**ステップ 3** に進みます。

[新規追加 (Add New)] をクリックすると、各フィールドのデフォルト設定を示し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、設定をコピーした設定ウィンドウが表示されます。

ステップ 3 表 18-1 の説明に従って、適切な設定を入力します。

ステップ 4 [保存 (Save)] をクリックします。

表 18-1 VPN ゲートウェイの設定値

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。

表 18-1 VPN ゲートウェイの設定値 (続き)

フィールド	説明
[VPN ゲートウェイの URL (VPN Gateway URL)]	<p>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。</p> <p>(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。</p> <p>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。</p> <ul style="list-style-type: none"> 『<i>SSL VPN Client (SVC) on ASA with ASDM Configuration Example</i>』 http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008071c428.shtml
[この場所の VPN 証明書 (VPN Certificates in this Location)]	<p>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。証明書をゲートウェイに割り当てなかった場合、VPN クライアントはそのコンセントレータへの接続に失敗します。</p> <p>(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。</p>