CHAPTER 37

ルータのプロビジョニング

ルータをプロビジョニングするときには、ルータに直接接続された USB デバイス、または Secure Device Provisioning（SDP）を使用できます。SDP を Cisco CP で使用できるようにするには、使用している Cisco IOS リリースで SDP がサポートされている必要があります。

Secure Device Provisioning

このウィンドウでは、Secure Device Provisioning（SDP）を使用して、CA サーバに対するルータの登録やルータの構成などの作業を完了できます。[SDP の起動] ボタンをクリックして SDP Web ブラウザ アプリケーションに転送し、プロセスを完了します。

証明書を取得する場合、Cisco CP では証明書ウィンドウが表示されます。このウィンドウには、CA から取得した証明書が表示されます。

SDP を使用した登録に必要な準備については、「SDP のトラブルシューティングのヒント」を参照してください。

SDP の詳細については、次のリンクをクリックしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

（注） [SDP の起動] ボタンが表示されない場合は、使用しているルータの Cisco IOS リリースで SDP がサポートされていません。[SDP の起動] ボタンが無効になっている場合は、Cisco CP にルート以外のビュー ユーザとしてログインしています。

USB からのルータのプロビジョニング

このウィンドウには、ルータに接続されている USB トークンまたは USB フラッシュ デバイスが Cisco CP によって検出されたかどうかが示されます。[ルータのプロビジョニング] ボタンをクリックすると、USB トークンまたは USB フラッシュ デバイスのコンフィギュレーション ファイルを選択できます。

ルータをこの方法でプロビジョニングすると、USB トークンまたは USB フラッシュ デバイスのコンフィギュレーション ファイルがルータの実行コンフィギュレーション ファイルとマージされて、新しい実行コンフィギュレーション ファイルが作成されます。

USB からのルータのプロビジョニング（ロード ファイル）

このウィンドウでは、ルータに接続された USB トークンまたは USB フラッシュ デバイスのコンフィギュレーション ファイルをロードできます。このファイルがルータの実行コンフィギュレーション ファイルとマージされて、新しい実行コンフィギュレーション ファイルが作成されます。

コンフィギュレーション ファイルをロードするには、次の手順に従ってください。

ステップ 1　ドロップダウン メニューから、デバイスのタイプを選択します。

ステップ 2　［ファイル名］にコンフィギュレーション ファイルの名前をフル パスを含めて入力するか、［参照］をクリックして［ファイルの選択］ウィンドウでファイルを選択します。

ステップ 3　デバイス タイプが USB トークンの場合、［トークンの PIN］にトークンにログインするためのパスワードを入力します。

ステップ 4　ファイルをプレビューする場合は、［ファイルのプレビュー］をクリックして、ファイルの内容を詳細ペインに表示します。

ステップ 5　［OK］をクリックして、選択したファイルをロードします。

SDP のトラブルシューティングのヒント

Secure Device Provisioning（SDP）を使用して登録を行う前に、このトピックの情報を参照してルータと証明書サーバの間の接続を準備してください。登録時に問題が発生した場合は、準備のために行った作業を見直すことで、問題のある場所を判断できます。

ガイドライン

- SDP が起動したら、このヘルプ トピックが表示されているブラウザ ウィンドウを最小化して、SDP の Web アプリケーションが見えるようにする。
- SDP を使用してルータを設定しようとしている場合は、WAN 接続を設定した後すぐにその設定を行う。
- SDP で設定の変更を行ったときは、Cisco CP に戻ってツールバーの［更新］をクリックし、［ルータ証明書］ウィンドウの［VPN コンポーネント］ツリーでトラストポイントのステータスを確認する。

トラブルシューティングのヒント

ここに記載されている推奨事項は、ローカル ルータと CA サーバでの準備作業を必要とします。CA サーバの管理者に必要な作業を伝える必要があります。確認が必要な事項は、次のとおりです。

- ローカル ルータと CA サーバが相互に IP 接続可能である。ローカル ルータは証明書サーバに ping を正常に実行できなければならず、証明書サーバはローカル ルータに ping を正常に実行できなければならない。
- CA サーバ管理者が JavaScript をサポートする Web ブラウザを使用している。
- CA サーバ管理者がローカル ルータに対するイネーブル特権を持っている。
- ローカル ルータ上のファイアウォールで、証明書サーバとの間で送受信されるトラフィックが許可される。
- 申請者（Petitioner）と登録者（Registrar）の一方または両方でファイアウォールが設定されている場合は、Cisco CP と SDP アプリケーションが起動された PC からの HTTP トラフィックまたは HTTPS トラフィックがそのファイアウォールで許可されていることを確認する必要がある。

SDP の詳細については、次の Web ページを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332