ASA 8.X： AnyConnect SCEP 登録の設定例

目次

概要

SCEP 登録機能は、AnyConnect スタンドアロン クライアント 2.4 で導入されました。 このプロセスでは、SCEP に関連する設定を含めるように AnyConnect XML プロファイルを変更し、証明書登録用の特定のグループ ポリシーおよび接続プロファイルを作成します。 AnyConnect ユーザがこの特定のグループに接続すると、AnyConnect から CA サーバに証明登録要求が送信され、CA サーバは要求を自動的に承諾または拒否します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 8.x を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco AnyConnect VPN バージョン 2.4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく

必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

AnyConnect 用の自動 SCEP 登録の目的は、安全でスケーラブルな方法でクライアントに対して証明書を発行することです。 たとえば、ユーザは CA サーバから証明書を要求する必要はありません。 この機能は、AnyConnect クライアントに組み込まれています。 証明書は、XML プロファイル ファイルに記載されている証明書パラメータに基づいて、クライアントに対して発行されます。

必要な変更の概要

AnyConnect SCEP 登録機能では、特定の証明書パラメータが XML プロファイルで定義されていることが必要です。 証明書登録用にグループ ポリシーおよび接続プロファイルが ASA 上に作成され、XML プロファイルがそのポリシーに関連付けられます。 AnyConnect クライアントは、この特定ポリシーを使用する接続プロファイルに接続して、XML ファイルで定義されているパラメータを使用して証明書の要求を送信します。 Certificate Authority（CA; 認証局）により、要求が自動的に承諾または拒否されます。 AnyConnect クライアントは、クライアント プロファイルで <CertificateSCEP> 要素が定義されている場合、SCEP プロトコルを使用して証明書を取得します。

AnyConnect による新しい証明書の自動取得が試行される前に、クライアント証明書認証が失敗する必要があります。そのため、有効な証明書がすでにインストールされている場合は、登録は実行されません。

ユーザが特定のグループにログインすると、ユーザは自動的に登録されます。 証明書は手動で取得することもでき、この場合ユーザには [Get Certificate] ボタンが表示されます。 ただし、これはクライアントが CA サーバに直接アクセスできる（トンネルを経由しない）場合のみ機能します。

詳細は、『Cisco AnyConnect VPN Client 管理者ガイド、リリース 2.4』を参照してください。

Anyconnect SCEP 機能をイネーブルにする XML 設定

次に、AnyConnect XML ファイルで定義する必要のある重要な要素を示します。 詳細は、『Cisco AnyConnect VPN Client 管理者ガイド、リリース 2.4』を参照してください。

- <AutomaticSCEPHost>— SCEP 証明書の取得を設定する ASA ホスト名および接続プロファイル（トンネル グループ）を指定します。 この値は、ASA の完全修飾ドメイン名\接続プロファイル名、または ASA の IP アドレス\接続プロファイル名の形式にする必要があります。
- <CAURL> — SCEP CA サーバを識別します。
- <CertificateSCEP>— 証明書の内容がどのように要求されるかを定義します。
- <DisplayGetCertButton>— AnyConnect GUI に [Get Certificate] ボタンが表示されるかどうかを定義します。 このボタンを使用すると、ユーザは手動で証明書の更新またはプロビジョニングを要求できます。

次にプロファイルの例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
     ReconnectAfterResume
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
    Automatic
  </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
     http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

AnyConnect 用 SCEP プロトコルをサポートする ASA の設定

プライベート Registration Authority（RA; 登録局）へのアクセスを提供するために、ASA の管理者は、目的の RA へのプライベート サイド ネットワーク接続を制限する ACL を持つエイリアスを作成する必要があります。 証明書を自動的に取得するには、ユーザはこのエイリアスに接続して認証する必要があります。

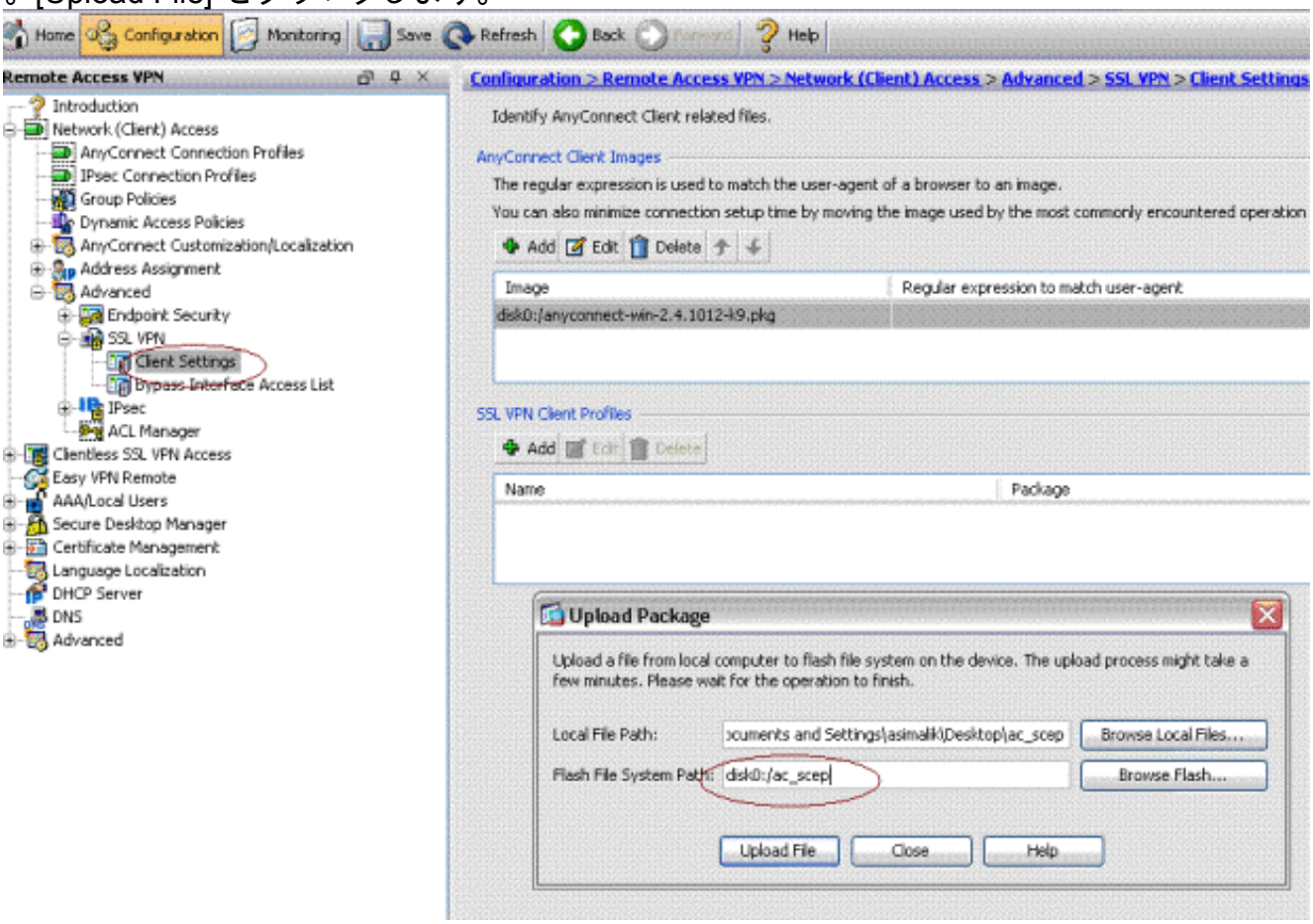
次の手順を実行します。

1. ASA にエイリアスを作成して、特定の設定済みグループをポイントします。

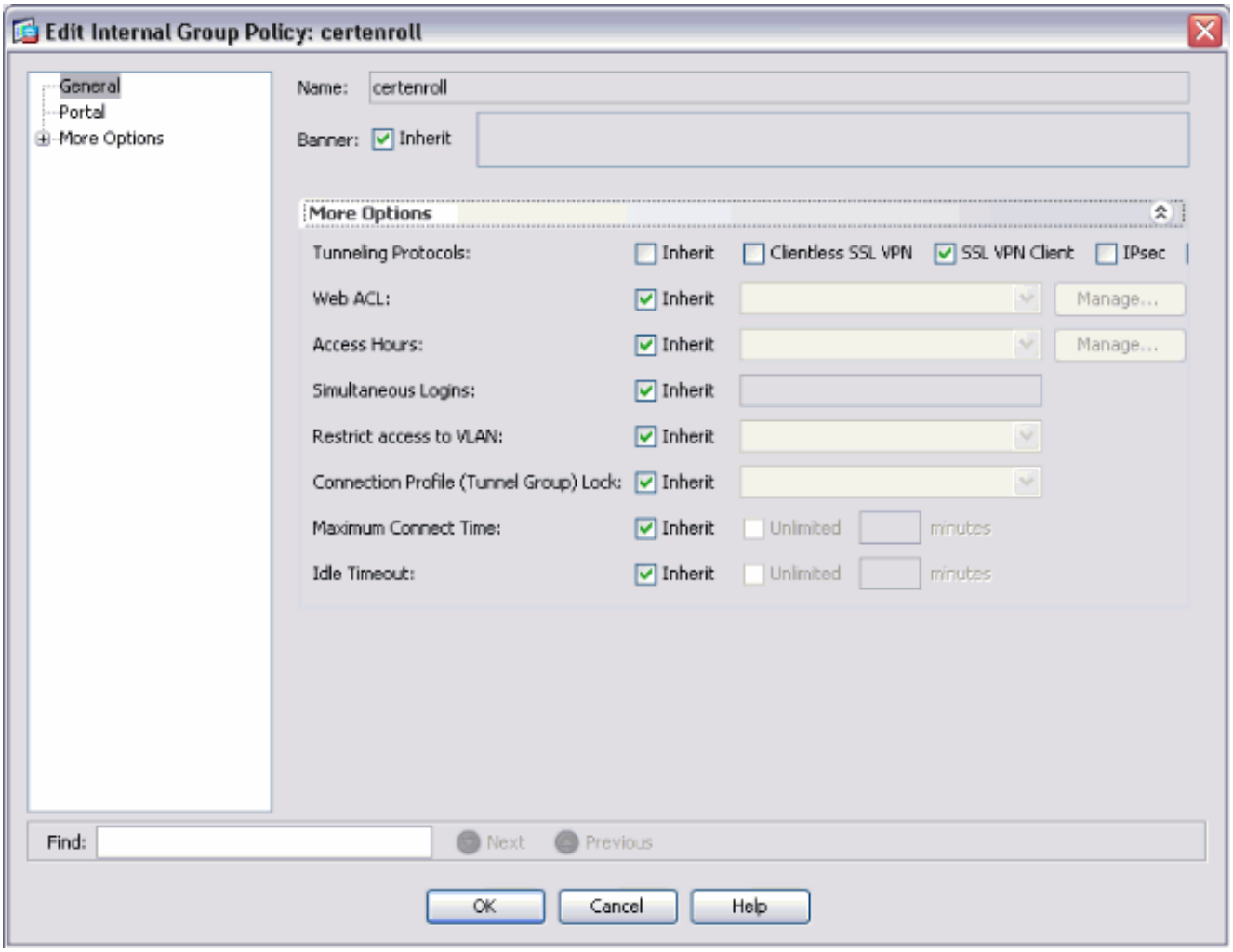
2. ユーザのクライアント プロファイルで <AutomaticSCEPHost> 要素を指定します。
3. 特定の設定済みグループに対する <CertificateEnrollment> が含まれるクライアント プロファイルを添付します。
4. 特定の設定済みグループに ACL を設定して、プライベート サイド RA へのトラフィックを制限します。

次の手順を実行します。

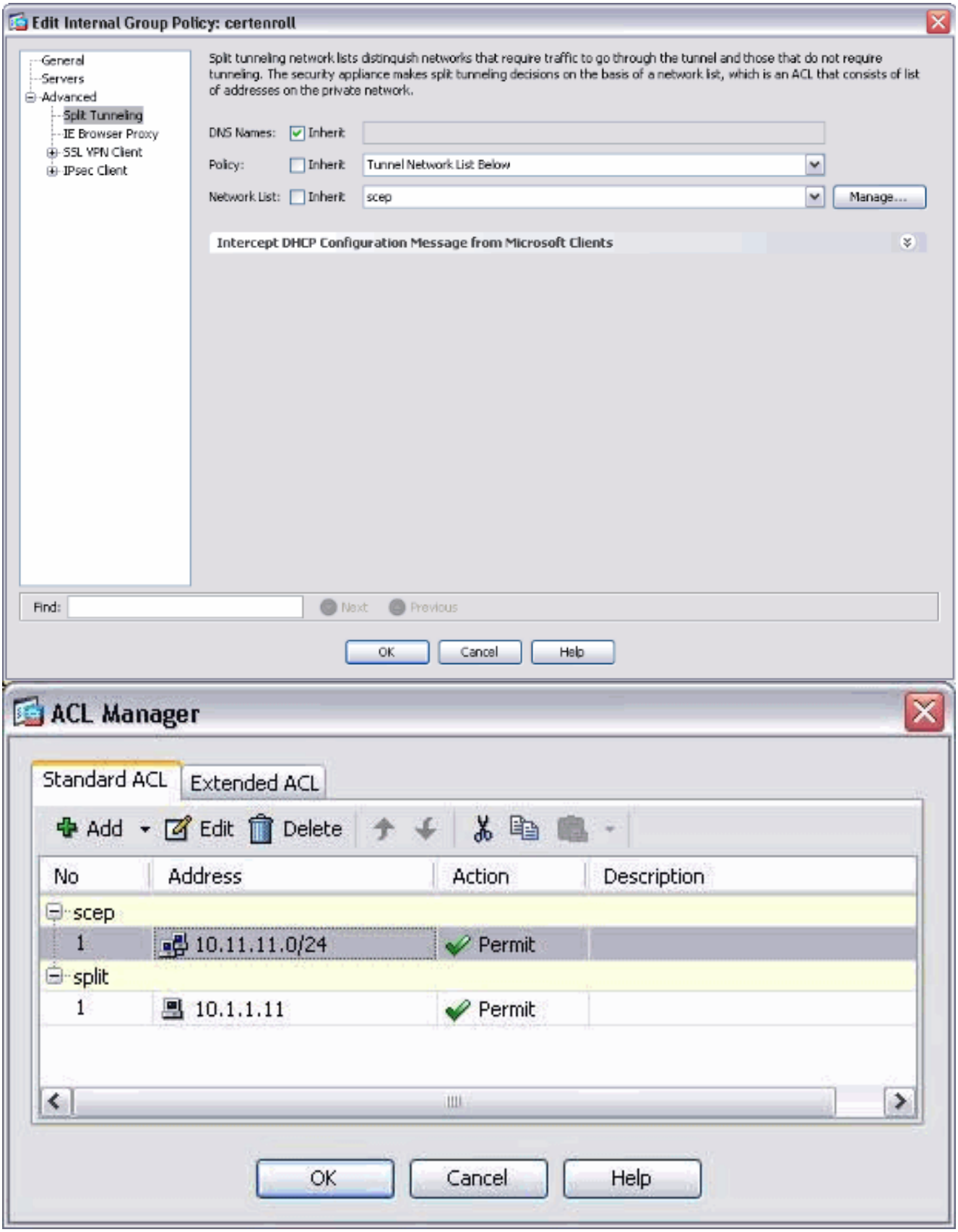
1. XML プロファイルを ASA にアップロードします。[Remote Access VPN] > [Network (client) access] > [Advanced] > [SSL VPN] > [Client settings] を選択します。[SSL VPN Client Profiles] の下で、[Add] をクリックします。[Browse Local Files] をクリックしてプロファイル ファイルを選択し、[Browse Flash] をクリックしてフラッシュ ファイル名を指定します。[Upload File] をクリックします。



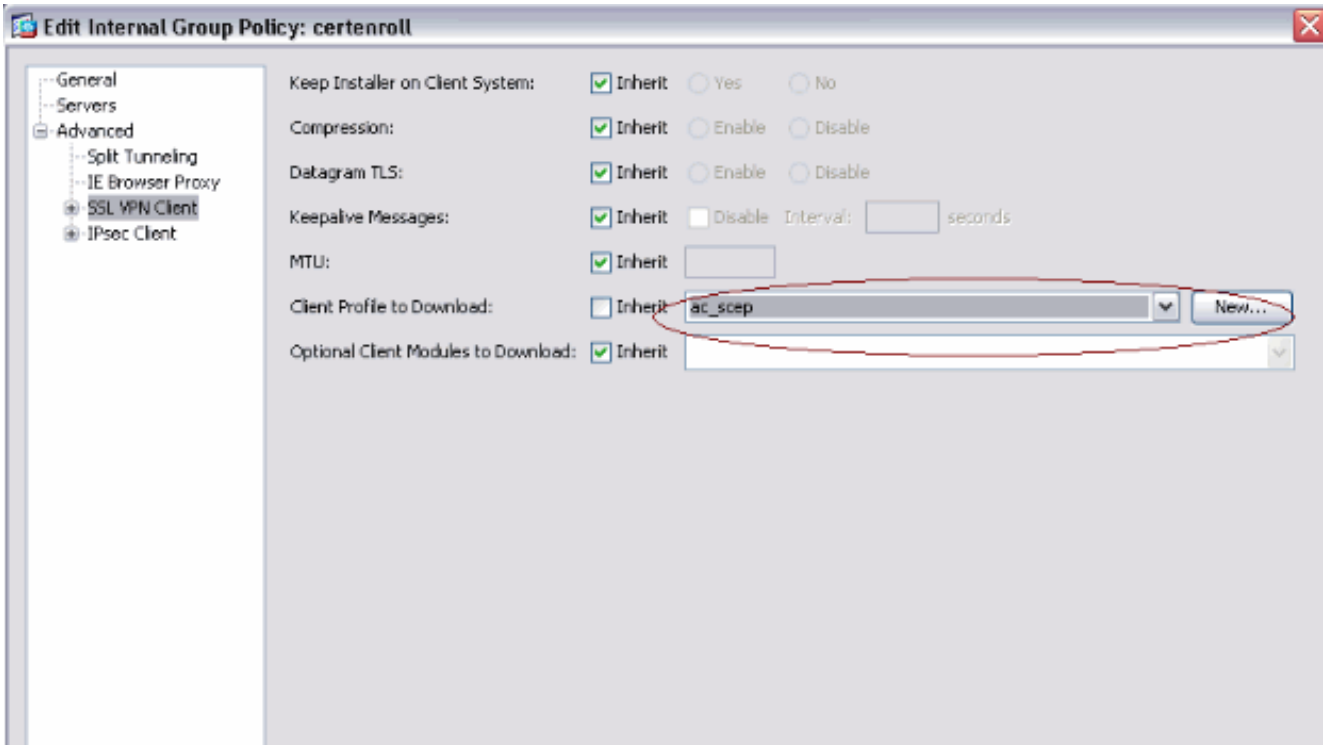
2. 証明書登録用の **certenroll** グループ ポリシーをセットアップします。[Remote access VPN] > [Network client access] > [Group Policy] を選択して、[Add] をクリックします。



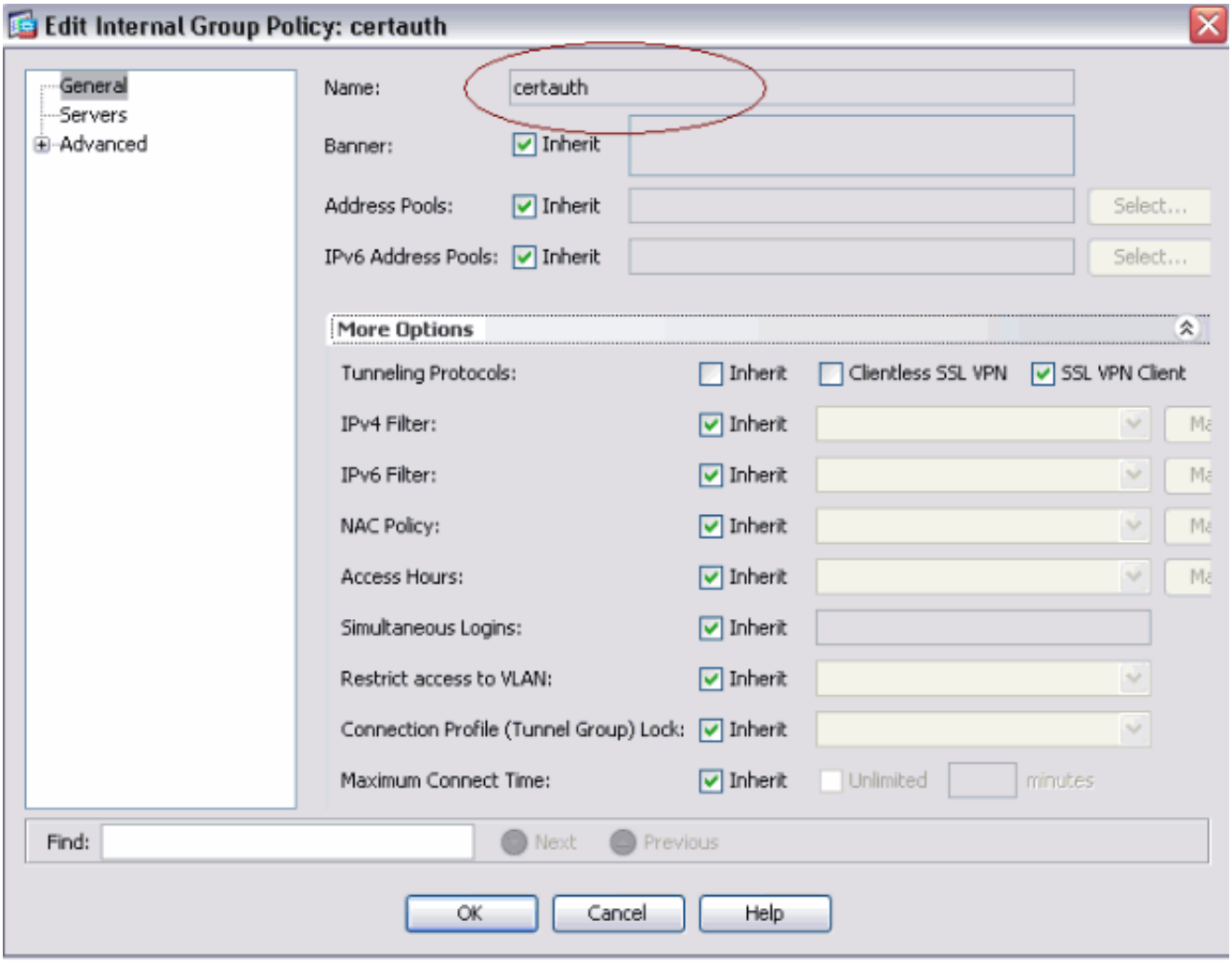
CA サーバ用のスプリット トンネルを追加します。[Advanced] を展開して、[Split Tunneling] を選択します。ポリシー メニューから [Tunnel Network List Below] を選択し、[Manage] をクリックしてアクセス コントロール リストを追加します。



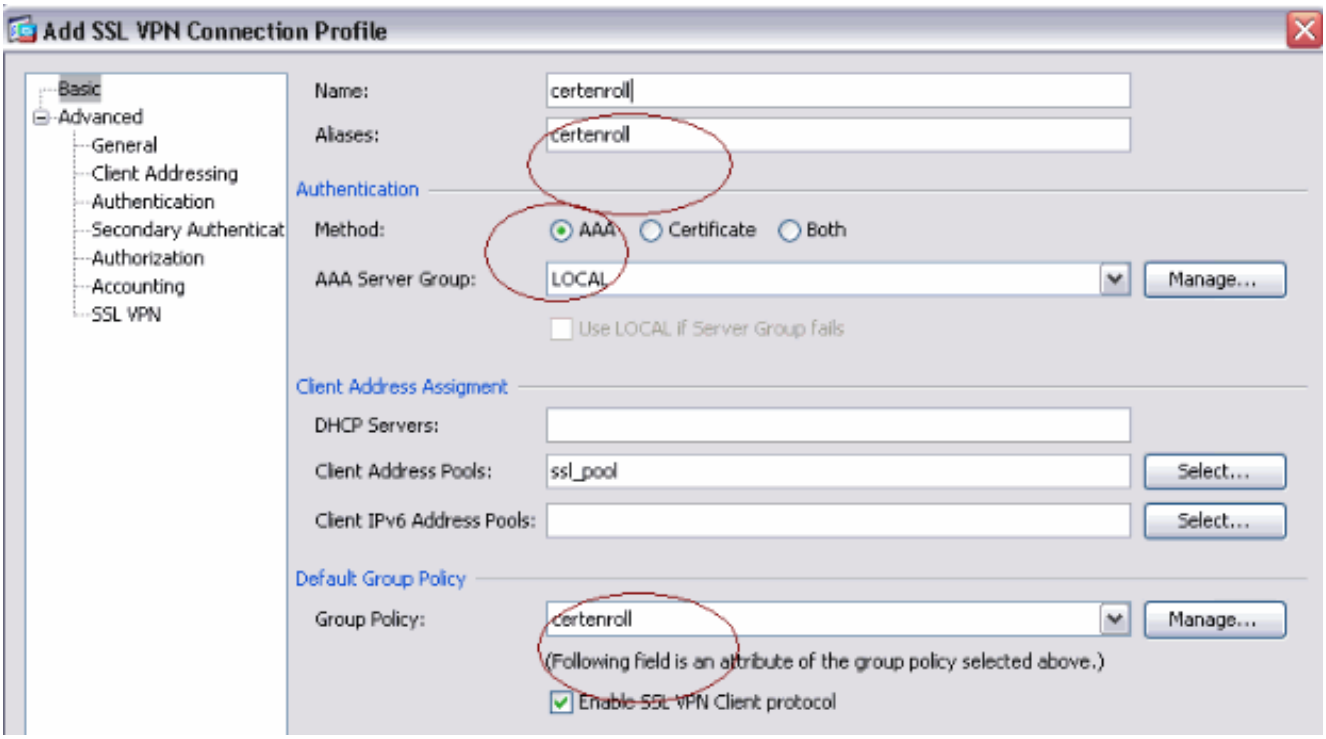
[SSL VPN Client] を選択し、[Client Profile to Download] メニューから certenroll のプロファイルを選択します。



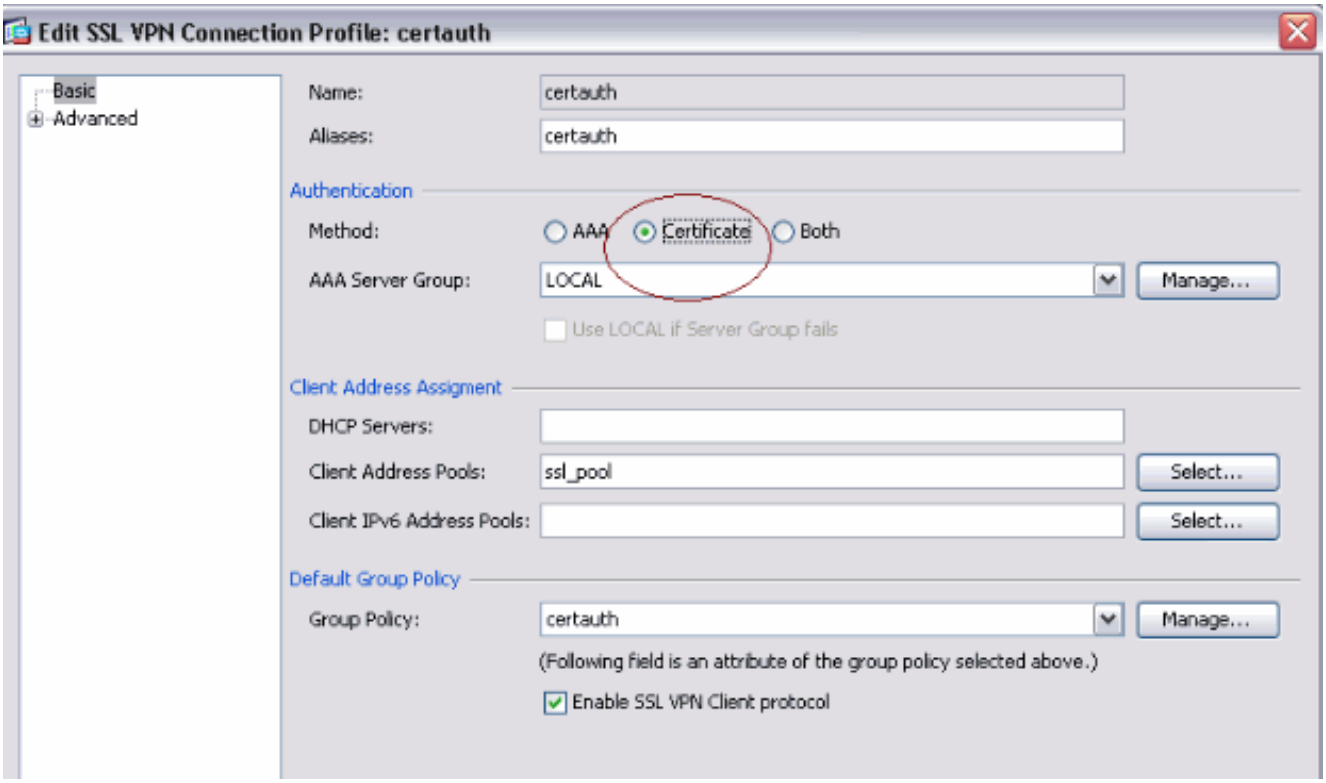
3. 証明書認証用に、**certauth** という別のグループを作成します。



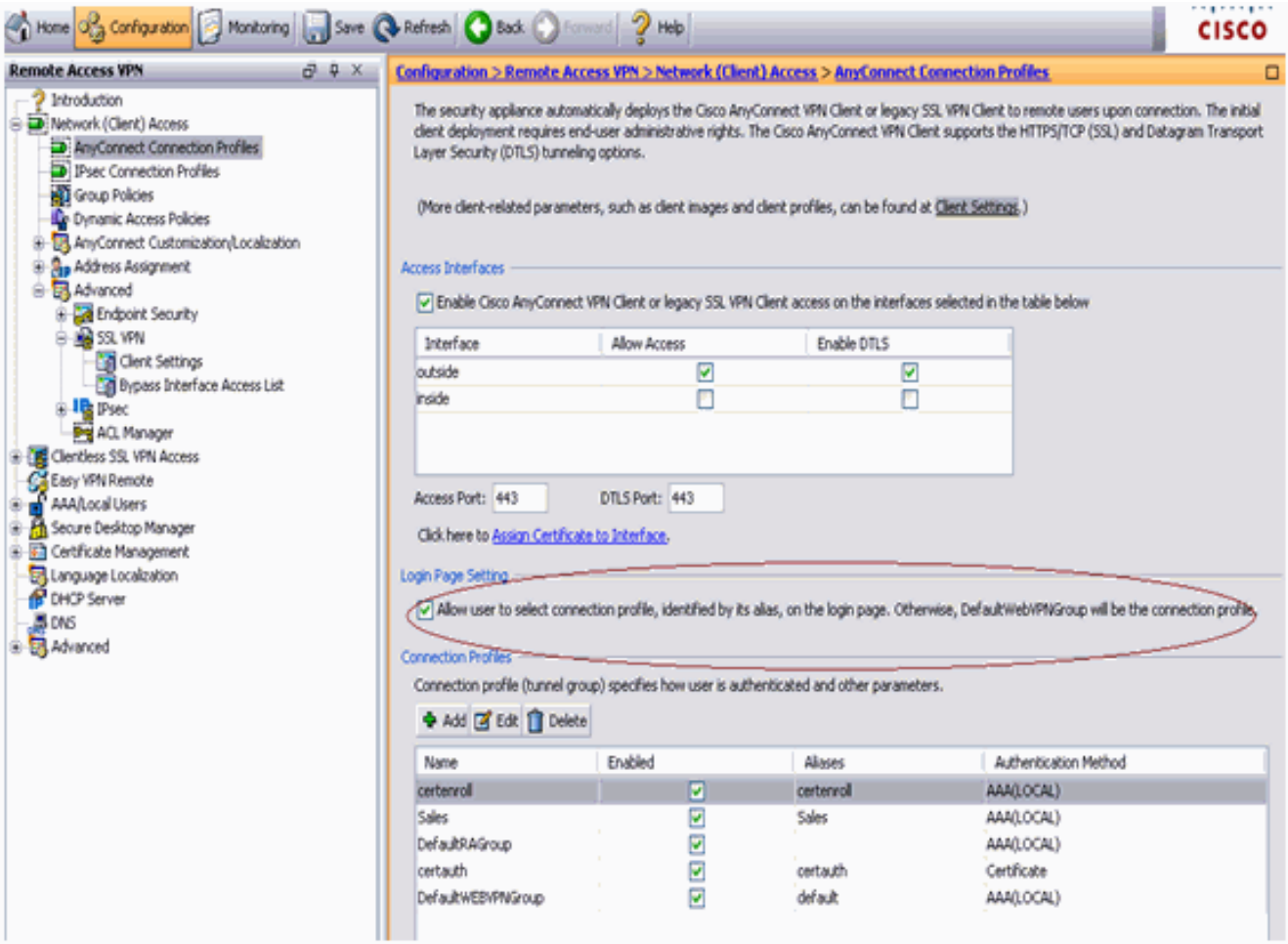
4. certenroll の接続プロファイルを作成します。[Remote access VPN] > [Network client access] > [AnyConnect connection profiles] を選択して、[Add] をクリックします。[Aliases] フィールドに **certenroll** グループを入力します。**注:** エイリアス名は、AutomaticSCEPHost の下の AnyConnect プロファイルで使用されている値と一致する必要があります。



5. 証明書認証を持つ **certauth** という名前の別の接続プロファイルを作成します。 これが、登録後に使用される実際の接続プロファイルになります。



6. エイリアスの使用がイネーブルになっていることを確認するために、[Allow user to select connection profile, identified by its alias, on the login page. **Otherwise, DefaultWebVPNGroup is the connection profile] にチェックマークを付けます。**



AnyConnect SCEP のテスト

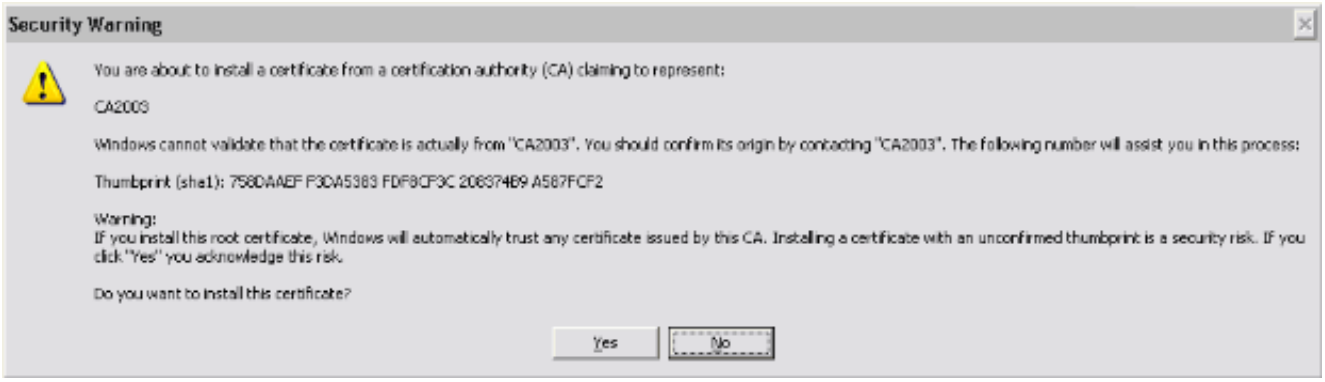
このセクションでは、設定が正常に機能していることを確認します。

1. AnyConnect クライアントを起動して、certenroll プロファイルにアクセスします。

AnyConnect は、CA サーバに対し SCEP 経由で登録要求を渡します。

[Get Certificate] ボタンが使用された場合は、AnyConnect はトンネルを経由するのではなく、登録要求を直接渡します。

2. 次の警告が表示されます。 [Yes] をクリックして、ユーザおよびルート証明書をインストールします。



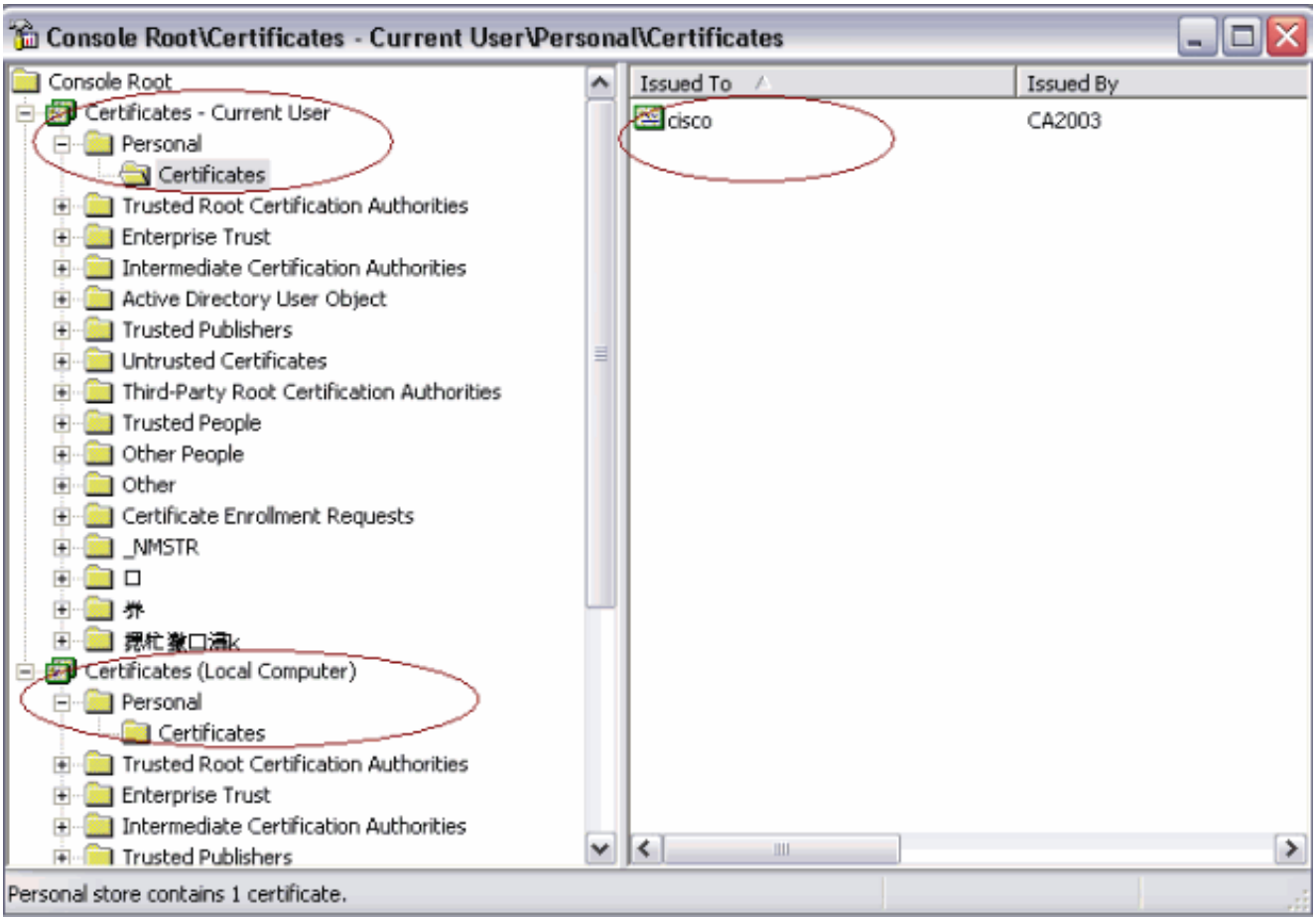
3. 証明書が登録されたら、**certauth** プロファイルに接続します。

SCEP 要求後の Microsoft Windows への証明書の保存

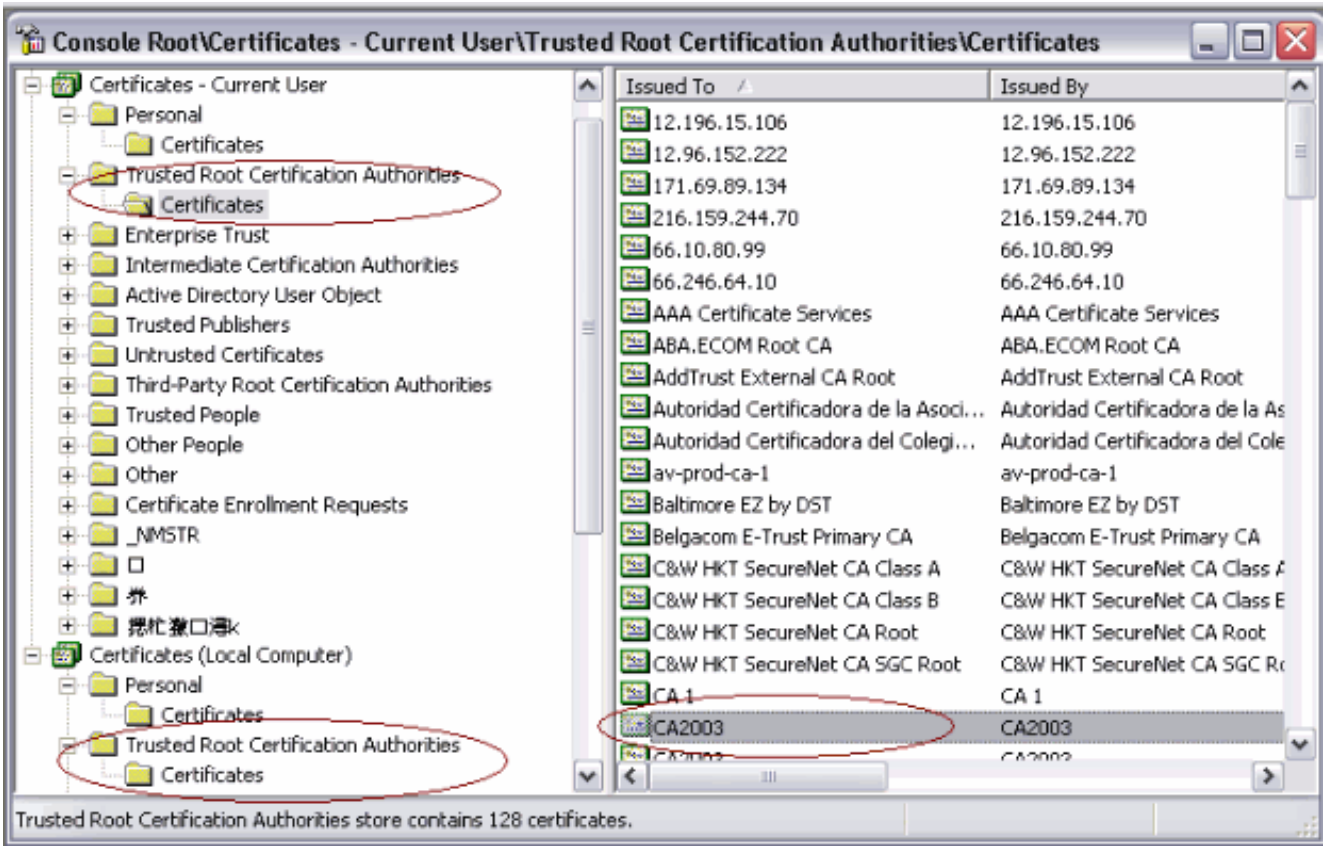
次の手順を実行します。

1. [Start] > [run] > [mmc] をクリックします。
2. [Add/remove snap in] をクリックします。

3. [Add] をクリックして、[certificates] を選択します。
4. **My user account** および **computer account** 証明書を追加します。このイメージは Windows ce rtificate ストアにインストールされるユーザ許可証を示します
:



このイメージは Windows ce rtificate ストアにインストールされる CA 認証を示します
:



トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

- AnyConnect SCEP 登録は、証明書認証が失敗した場合のみ、機能します。 登録が実行されない場合は、証明書ストアを確認してください。 証明書がすでにインストールされている場合は、証明書を削除し、再度テストしてください。
- SCEP 登録は、**ssl certificate-authentication interface outside port 443** コマンドを使用しない限り、機能しません。詳細については、次の Cisco Bug ID を参照してください。Cisco Bug ID CSCtf06778（登録ユーザ専用）：AnyConnect SCEP 登録が Per Group Cert Auth 2 で機能しないCisco Bug ID CSCtf06844（登録ユーザ専用）：AnyConnect SCEP 登録が ASA Per Group Cert Auth で機能しない
- CA サーバが ASA の外部にある場合は、**same-security-traffic permit intra-interface** コマンドによるヘアピニングが許可されていることを確認してください。 また、次の例のように nat outside および access-list コマンドを追加してください。`nat (outside) 1 access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87`ここで、172.16.1.0 は AnyConnect プール、171.69.89.87 は CA サーバの IP アドレスです。
- CA サーバが内部にある場合は、**certenroll** グループ ポリシーのスプリット トンネル アクセス リストに含まれていることを確認してください。 このドキュメントでは、CA サーバが内部にあることを前提としています。

```
group-policy certenroll attributes
split-tunnel-policy tunnelspecified
 split-tunnel-network-list value scep

access-list scep standard permit 171.69.89.0 255.255.255.0
```

関連情報

- Cisco AnyConnect VPN Client 管理者ガイド、リリース 2.4
- テクニカルサポートとドキュメント - Cisco Systems