ローカル CA サーバおよび AnyConnect ヘッドエンドとしての ASA の設定

目次

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス（ASA）を認証局（CA）サーバおよび Cisco AnyConnect セキュア モビリティ クライアント用のセキュア ソケット レイヤ（SSL）ゲートウェイとしてセットアップする方法説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- ソフトウェア バージョン 9.1.x を実行する基本的な ASA 設定
- ASDM 7.3 以降

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 9.1(6) が稼働する Cisco 5500 シリーズ ASA

- AnyConnect セキュア モビリティ クライアント バージョン 4.x（Windows 用）
- 互換性チャートごとにサポートされている OS が稼働する PC。
- Cisco Adaptive Security Device Manager（ASDM）バージョン 7.3

  注: シスコの「ソフトウェア ダウンロード」ページ（登録ユーザ専用）から、AnyConnect VPN Client パッケージ（anyconnect-win*.pkg）をダウンロードします。 AnyConnect VPN Client を ASA のフラッシュ メモリにコピーします。これは、ASA との SSL VPN 接続を確立するためにリモート ユーザ コンピュータにダウンロードされます。 詳細については、ASA のコンフィギュレーション ガイドの「AnyConnect Client のインストール」セクションを参照してください。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

ASA の認証局は次の機能を提供します。

- ASA の基本的な認証局の動作を統合する。
- 証明書を導入する。
- 発行済み証明書のセキュアな失効チェックを実行する。
- ブラウザ ベース（WebVPN）とクライアント ベース（AnyConnect）の両方で SSL VPN 接続とともに、ASA 上に認証局を提供する。
- 外部の証明書認証に依存することなく、ユーザに信頼できるデジタル証明書を提供する。
- 証明書認証のためのセキュアな内部認証局を提供し、Web サイト ログインを使用した簡単なユーザ登録を実現する。

注意事項と制約事項

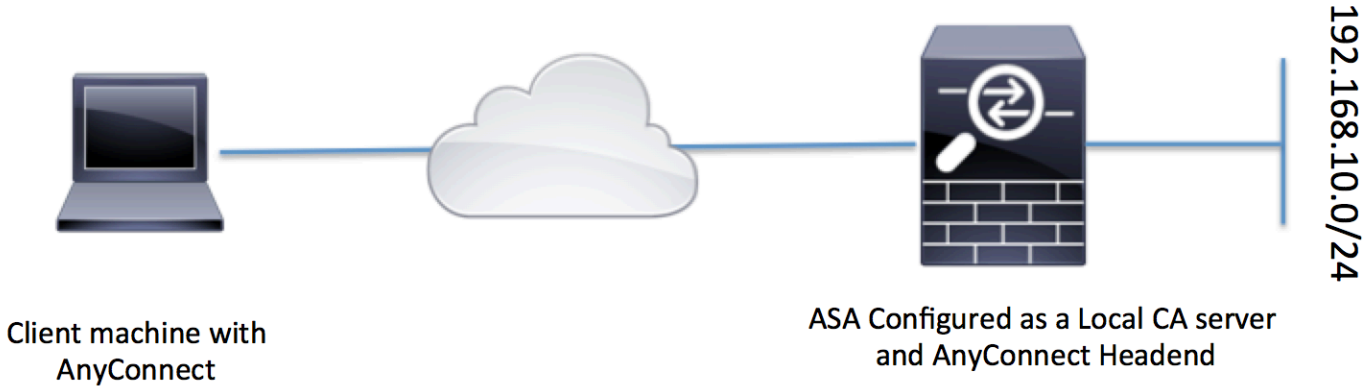
- ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。
- 一度に 1 つのローカル CA サーバのみ ASA に常駐できます。
- ローカル CA サーバ機能としての ASA は、フェールオーバー設定ではサポートされません。
- ローカル CA サーバとして機能する ASA は現在、SHA1 証明書の生成のみサポートします。
- ローカル CA サーバは、ブラウザ ベースとクライアント ベースの両方の SSL VPN 接続に使用することができます。 現在、IPSec にはサポートされていません。
- ローカル CA の VPN ロード バランシングをサポートしていません。
- ローカル CA は別の CA に従属することはできません。 ルート CA としてのみ機能できます。
- 現在、ASA はアイデンティティ証明書のローカル CA サーバに登録することはできません。
- 証明書の登録が完了すると、ASA により、ユーザのキー ペアと証明書チェーンを含む PKCS12 ファイルが保存されます。これには、登録ごとに約 2 KB のフラッシュ メモリまたはディスク領域が必要です。 実際のディスク領域の量は、設定されている RSA キー サイズと証明書フィールドによって異なります。 使用できるフラッシュ メモリの量が限られている ASA に、保留中の証明書登録を多数追加する場合には、このガイドラインに注意してください。これらの PKCS12 ファイルは、設定されている登録の取得タイムアウトの間、フラッシュ メモリに保存されます。

設定

このセクションでは、Cisco ASA をローカル CA サーバとして設定する方法について説明します。

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

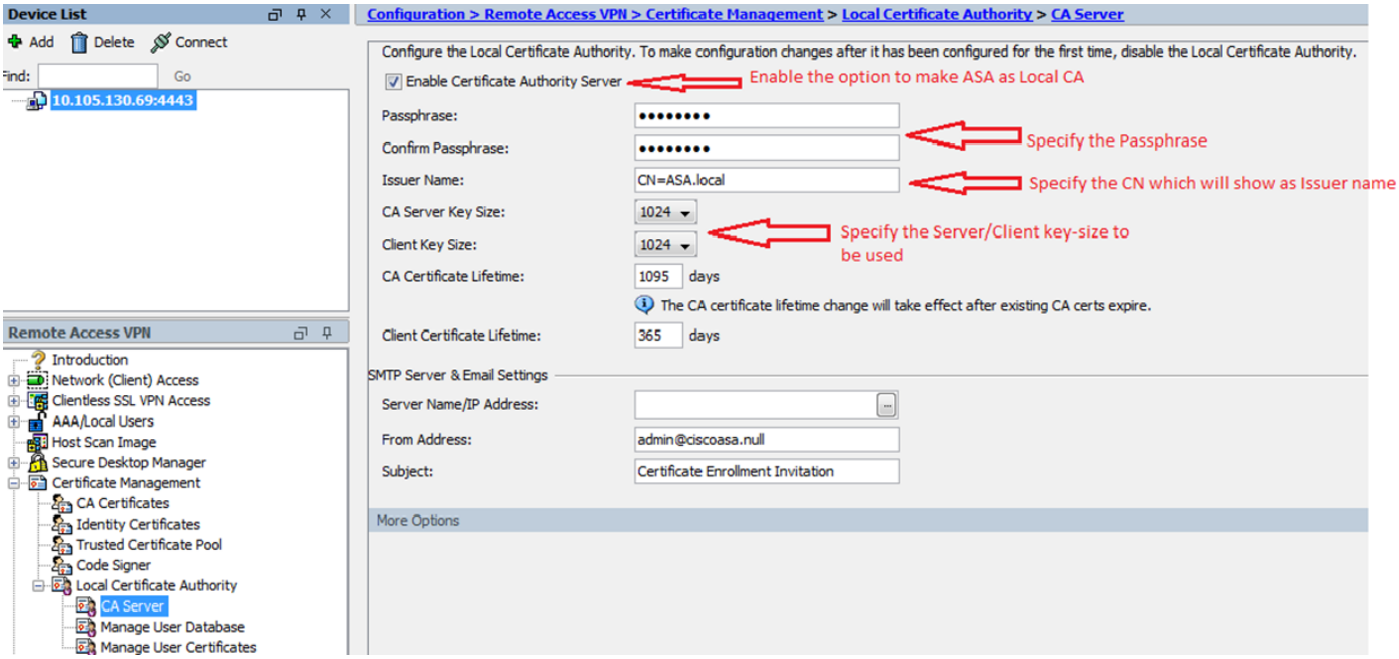


ローカル CA サーバとしての ASA

ステップ 1：ローカル CA サーバを ASA 上で設定し、有効にする

- [Configuration] > [Remote Access VPN] > [Certificate Management] > [Local Certificate Authority] > [CA Server] の順に移動します。 [Enable Certificate Authority server] オプションをチェックします。
- パスフレーズを設定します。 パスフレーズは最低 7 文字にする必要があります。これは、ローカル CA 証明書とキー ペアを含む PKCS12 ファイルのエンコードと保存のために使用されます。 CA 証明書またはキー ペアが失われた場合は、パスフレーズを使用して PKCS12 アーカイブをロック解除します。
- 発行元名を設定します。 このフィールドは、ルート証明書 CN として表示されます。 次の形式で指定できます。 CN（共通名）、OU（組織ユニット）、O（組織）、L（地名）、S（州）、C（国）
- **オプション設定：** [SMTP Server and Email Server settings] を、OTP がメールを介してエンド クライアントに受信されて登録が完了するように設定します。 ローカル Email/SMTP サーバのホスト名または IP アドレスを設定することができます。 また、クライアントが受信する電子メールの [From address] および [Subject] フィールドを設定することもできます。 デフォルトでは、[From Address] は **admin@<ASA hostname>.null** で、[Subject] は **Certificate Enrollment Invitation**.です。

- **オプション設定：** Client key size、CA server key size、Ca Certificate Lifetime、および Client certificate lifetime などのオプション パラメータを設定できます。



CLI の同等の設定：

```
ASA(config)# crypto ca server
ASA(config-ca-server)# issuer-name CN=ASA.local
ASA(config-ca-server)# subject-name-default CN=ASA.local
ASA(config-ca-server)# lifetime certificate 365
ASA(config-ca-server)# lifetime ca-certificate 1095
ASA(config-ca-server)# passphrase cisco123
ASA(config-ca-server)# no shutdown
% Some server settings cannot be changed after CA certificate generation.
Keypair generation process begin. Please wait...

Completed generation of the certificate and keypair...

Archiving certificate and keypair to storage... Complete
```

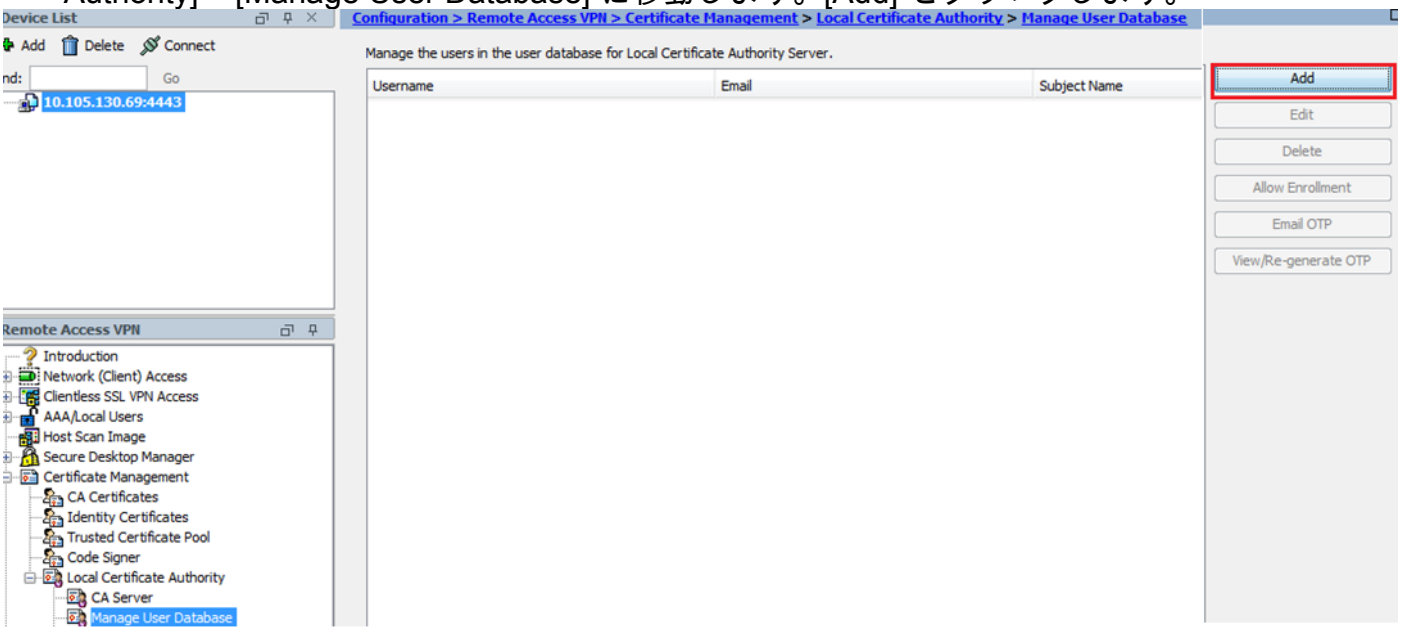
これらは、ローカル CA サーバの設定で構成できる追加のフィールドです。

CRL Distribution point URL	これは ASA での CRL の場所です。 デフォルトの場所は、http://hostname.domain/+CSCOCA+/asa_ca.crl ですが、URL は
Publish-CRL Interface and Port	特定のインターフェイスおよびポートで、CRL に HTTP ダウンロードできるようにす publish-CRL インターフェイスを選択します。 次に、1 ~ 65535 の任意のポート番号 **TCP ポート 80 です。**
CRL のライフタイム	ローカル CA は、ユーザ証明書が無効化または無効化解除されるたびに、CRL を更新 更がない場合、CRL ライフタイム 1 回ごとに、CRL が自動的に再発行されます。ライ **lifetime crl** コマンドで指定した期間です。 CRL のライフタイムを指定しない場合、デ
データベース ストレージの場所	ASA では、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装に口 **このデータベースは、デフォルトでローカル フラッシュ メモリに存在するか、**または 外部のファイル システム上に設定することもできます。
Default Subject Name	発行された証明書のユーザ名に追加されるデフォルト サブジェクト（DN 文字列）を 指定できます。 • CN（共通名）SN（姓） • O（組織名） • L(地名)

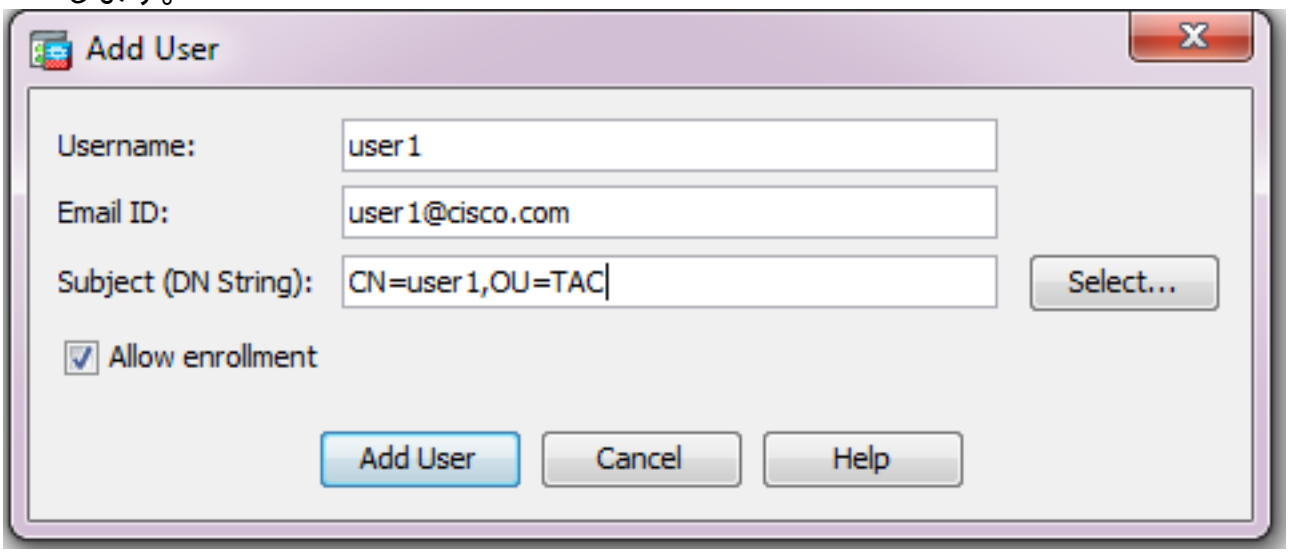
	• C(国) • OU (組織ユニット) • EA (電子メール アドレス) • ST (州/都道府県) • T(タイトル)
Enrollment Period	ユーザが ASA から PKCS12 ファイルを取得できる登録制限時間を設定します (時間 デフォルト値は 24 時間です。 : ユーザ証明書が含まれる PKCS12 ファイルを取得する前に登録の有効期間が切れた
One Time Password Expiration	OTP のユーザ登録有効期間を定義します (時間単位)。 この期間は、ユーザが登録を 値は 72 時間です。
Certificate Expiration Reminder	証明書の有効期限までの日数を指定します。この日数が経過すると、再登録に関する

手順 2 : ユーザを作成し、ASA データベースに追加する

- [Configuration] > [Remote Access VPN] > [Certificate Management] > [Local Certificate Authority] > [Manage User Database] に移動します。[Add] をクリックします。



- ユーザの詳細を指定します。次の画像に示すように、ユーザ名、電子メール ID、件名を指定します。

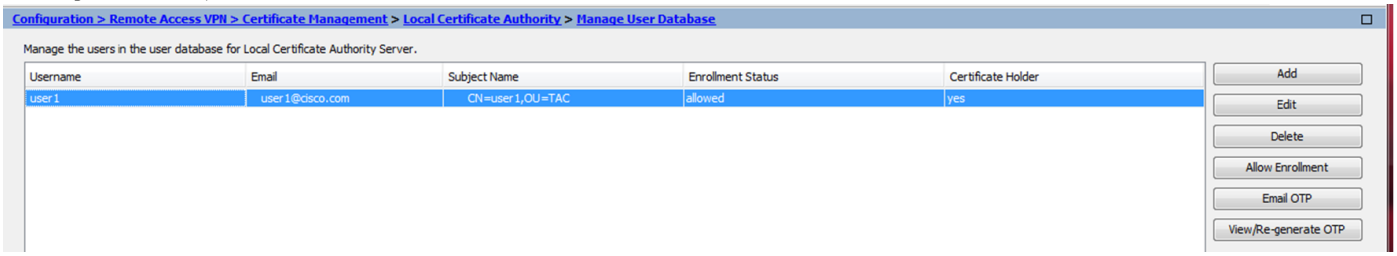


- 認証のための登録ができるように、[Allow Enrollment] がチェックされていることを確認します。
- [Add User] をクリックして、ユーザ設定を完了します。

CLI の同等の設定：

```
ASA(config)# crypto ca server user-db add user1 dn CN=user1,OU=TAC email user1@cisco.com
```

- ユーザがユーザ データベースに追加されると、登録ステータスは [Allowed to Enroll] として示されます。



ユーザのステータスを確認するための CLI：

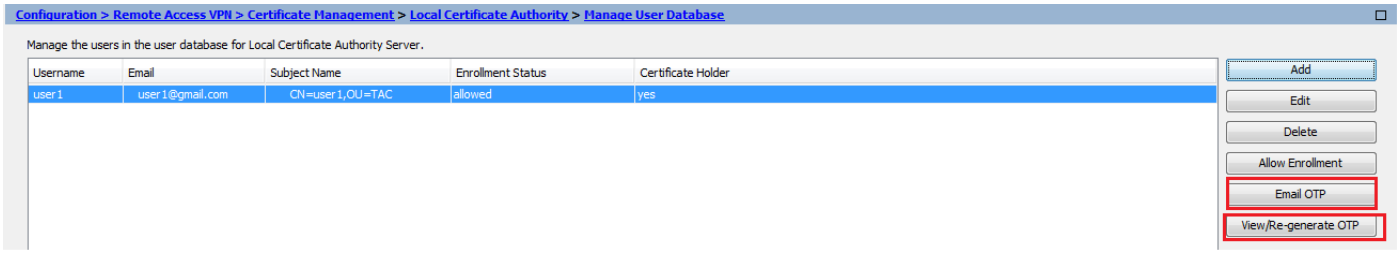
```
ASA# show crypto ca server user-db
username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

- ユーザがユーザ データベースに追加されると、ユーザが登録を完了できるように、次のいずれかの方法で One Time Password（OTP）を提供できます。

OTP に電子メールを送信する（CA サーバ設定で [SMTP server and Email Settings] が必要）。

または

OTP を直接表示し、[View/Re-generate OTP] をクリックしてユーザと共有する。 これは、OTP の再生成にも使用できます。



CLI の同等の設定：

```
ASA# show crypto ca server user-db
username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

手順 3：WAN インターフェイスで WebVPN を有効にする

- クライアントが登録を要求できるように、ASA で Web アクセスを有効にします。

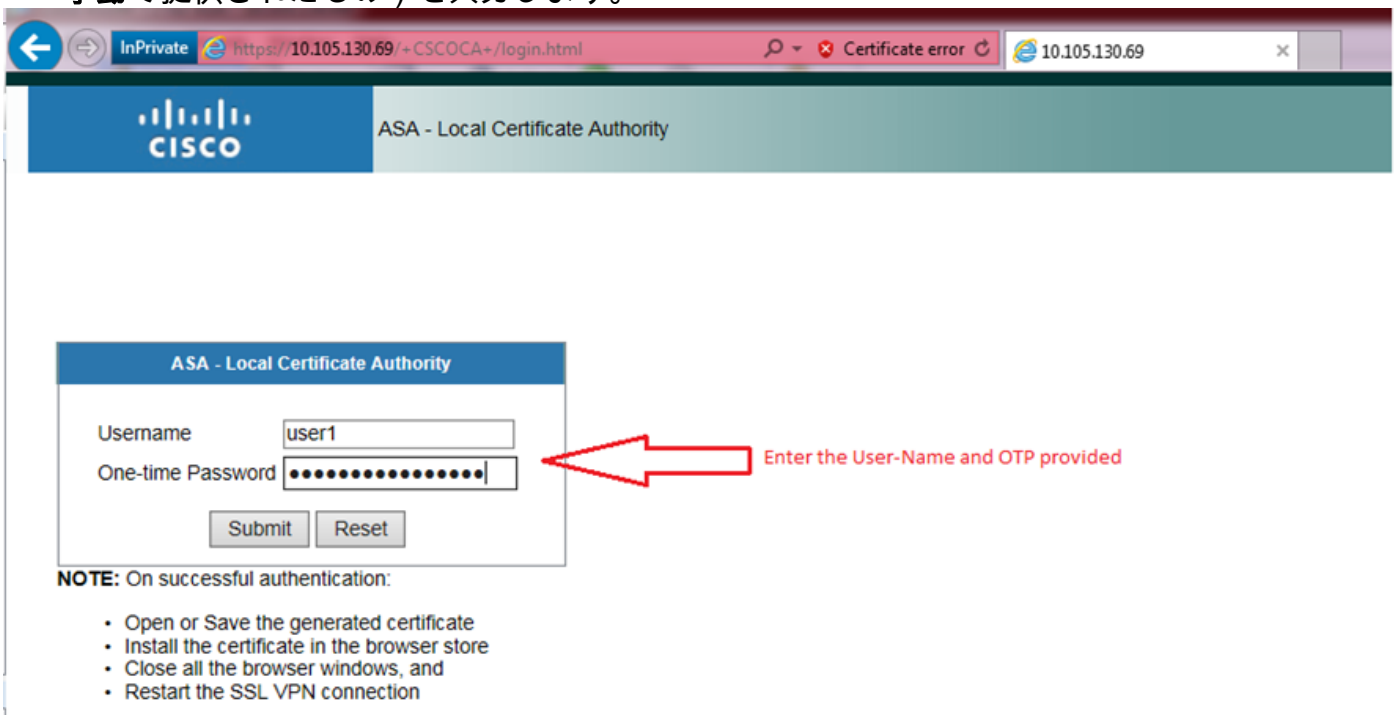
```
ASA# show crypto ca server user-db
username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

手順 4：証明書をクライアント マシンにインポートする

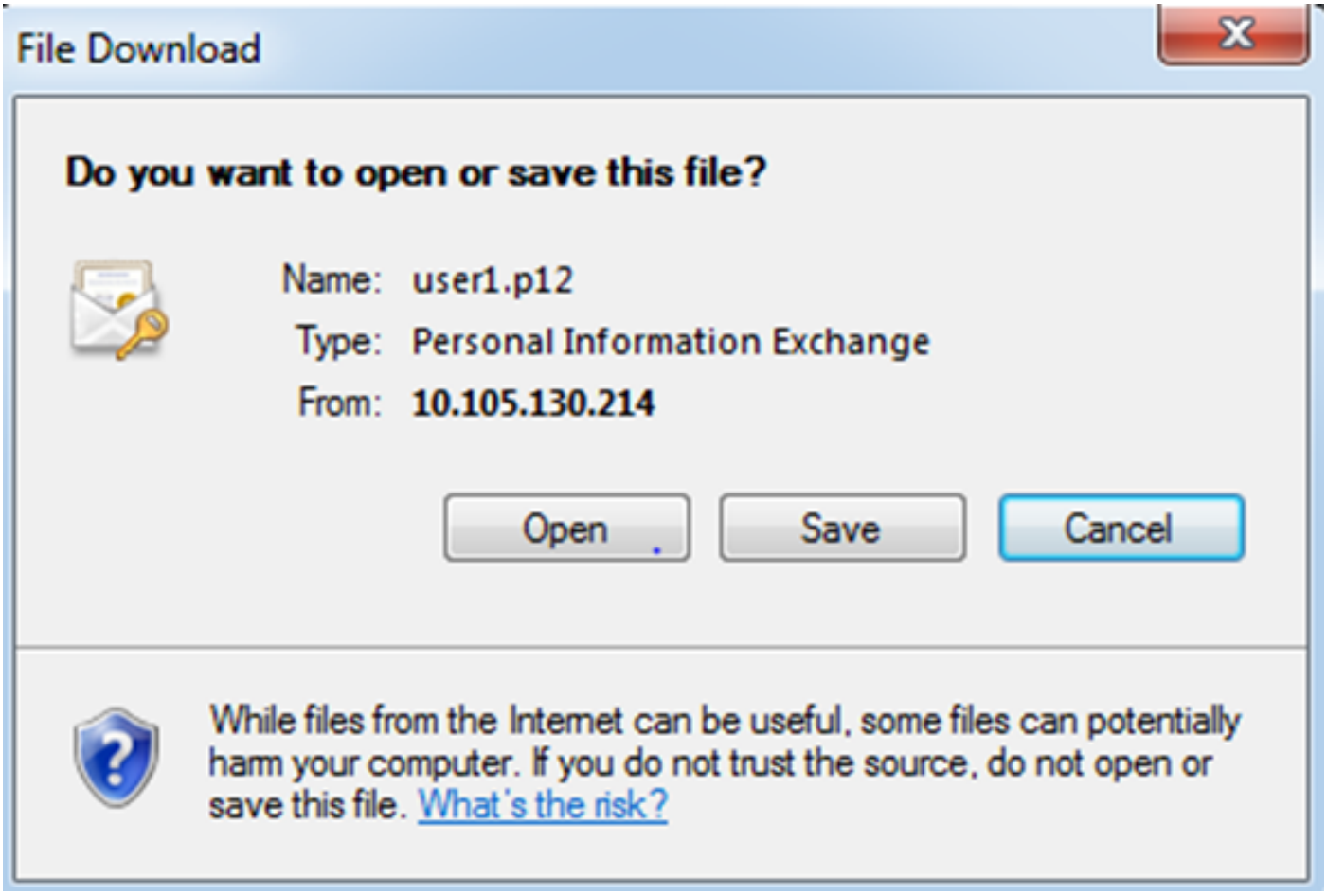
- クライアント ワークステーションでブラウザを開き、登録を完了するためにリンクに移動します。
- このリンクで使用される IP/FQDN は、前の手順で webvpn が有効にされたインターフェイス、つまり インターフェイス Internet の IP である必要があります。

https://<ASA IP/FQDN>/+CSCOCA+/enroll.html

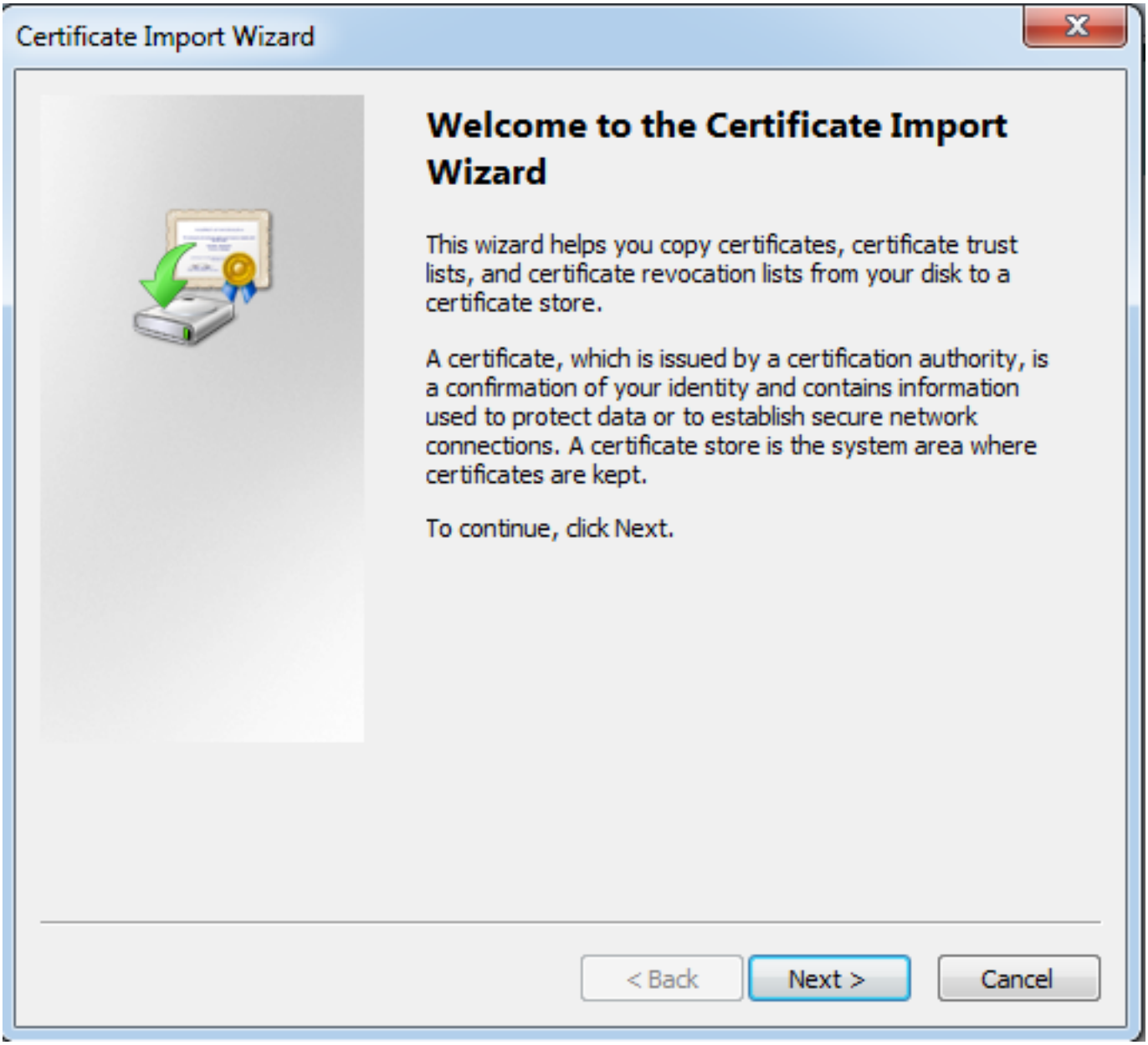
- ユーザ名（手順 2、オプション A の ASA で設定したもの）および OTP（電子メールまたは手動で提供されたもの）を入力します。



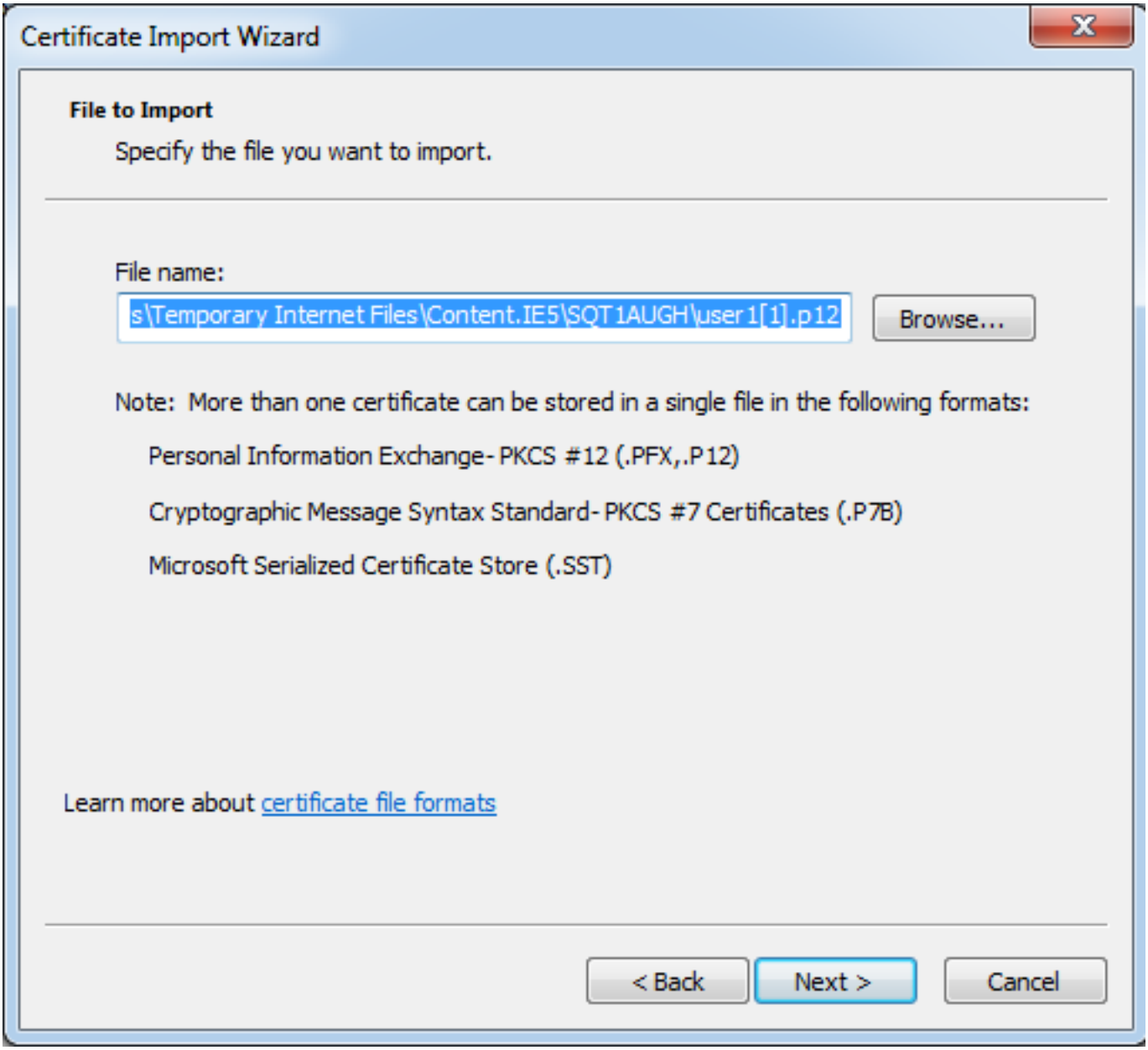
- [Open] をクリックして、ASA から受け取ったクライアント証明書を直接インストールします。
- クライアント証明書をインストールするパスフレーズは、前に受け取った OTP と同じです。



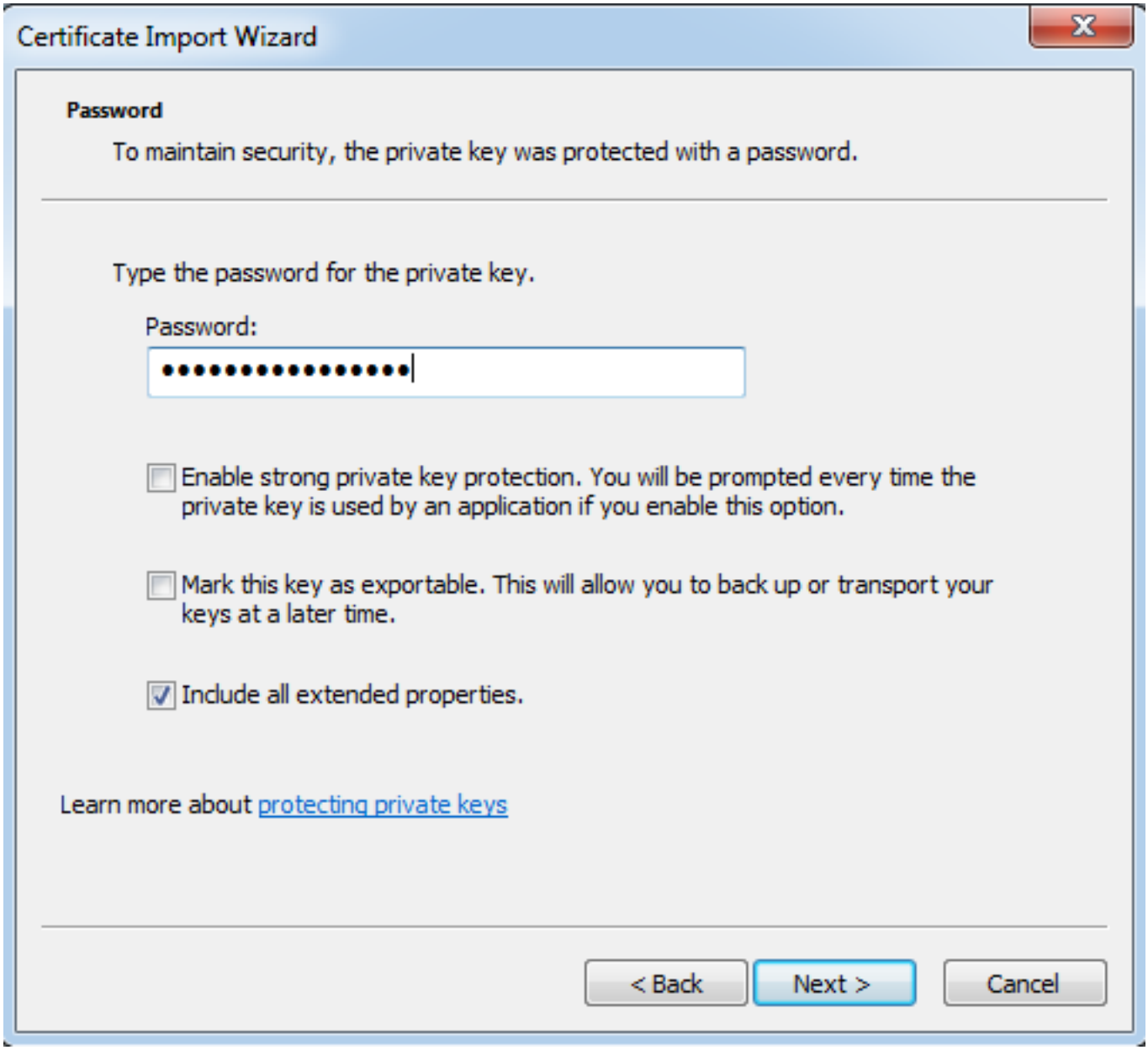
- [Next] をクリックします。



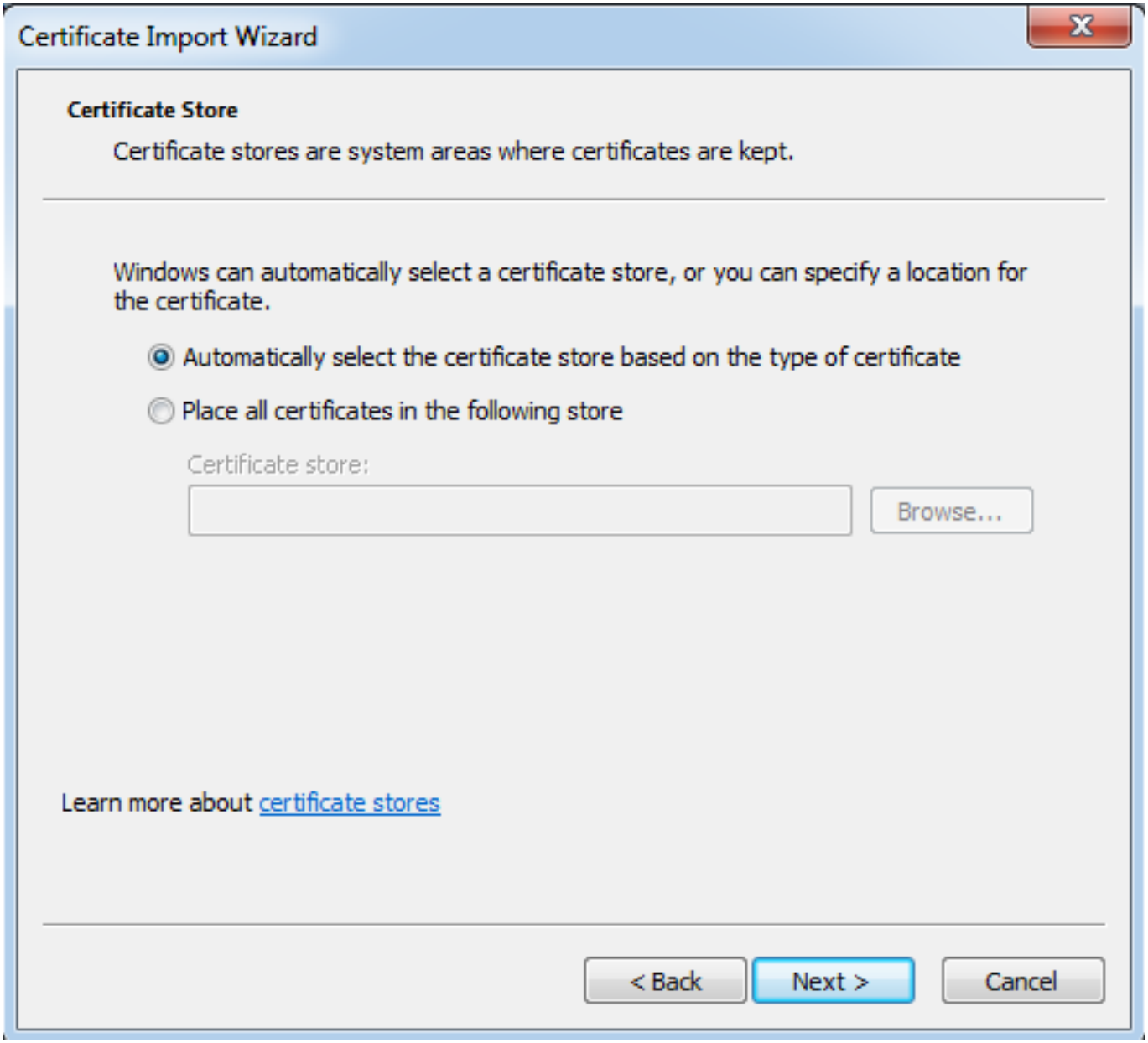
- パスはデフォルト値のままにして、[Next] をクリックします。



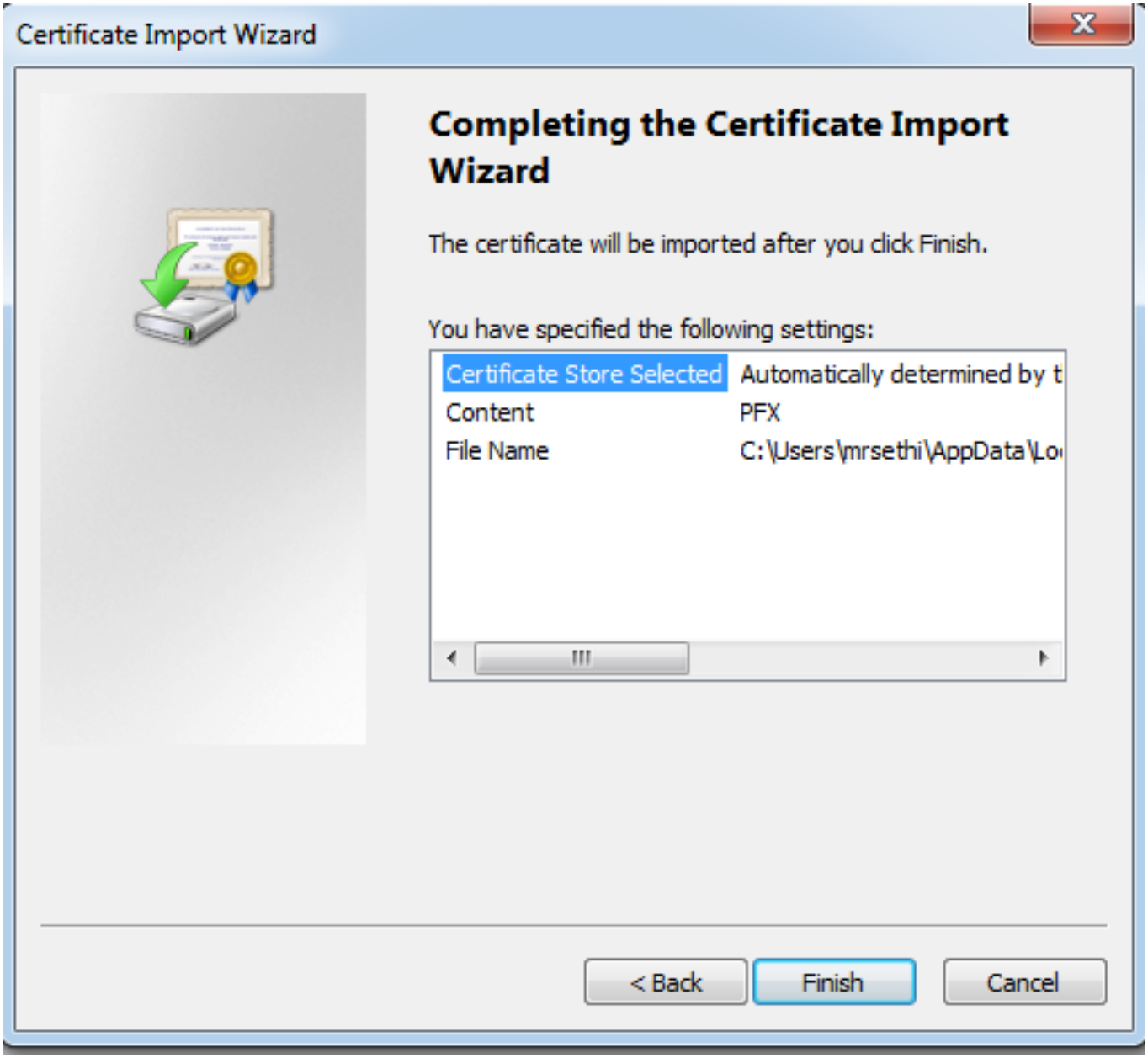
- [Password] フィールドに OTP を入力します。
- 必要に応じて、将来、キーをワークステーションからエクスポートできるようにするために、[Mark this key as exportable] オプションを選択できます。
- [Next] をクリックします。

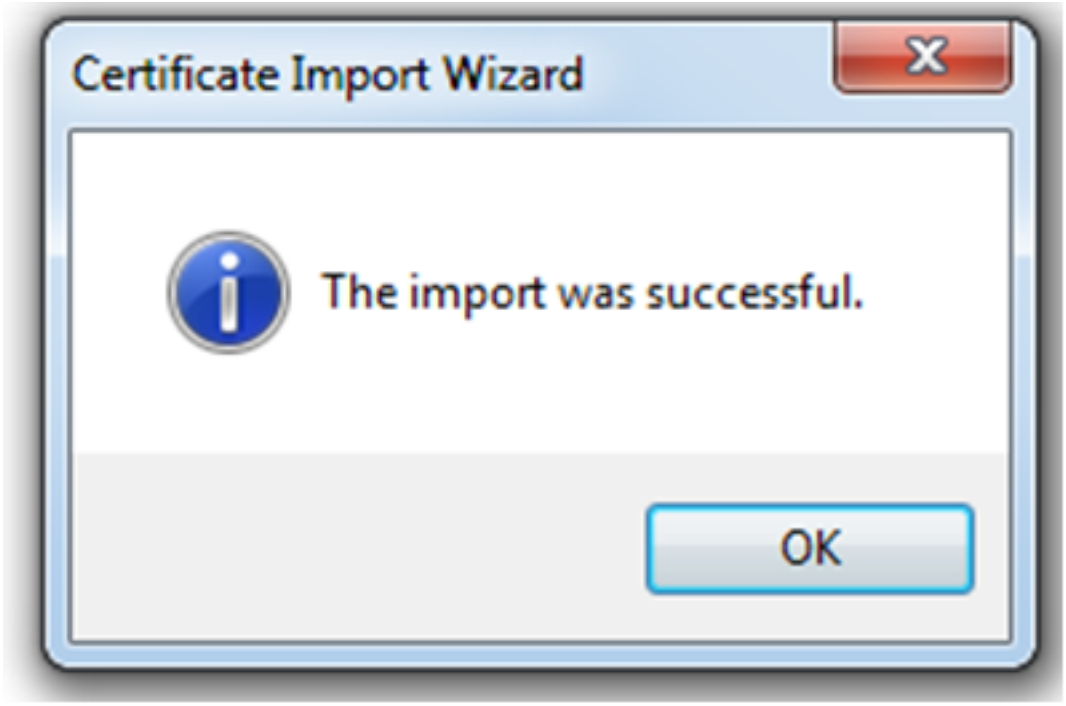


- 特定の証明書ストアに手動で認証をインストールするか、またはそのままにして自動的にストアを選択することができます。
- [Next] をクリックします。

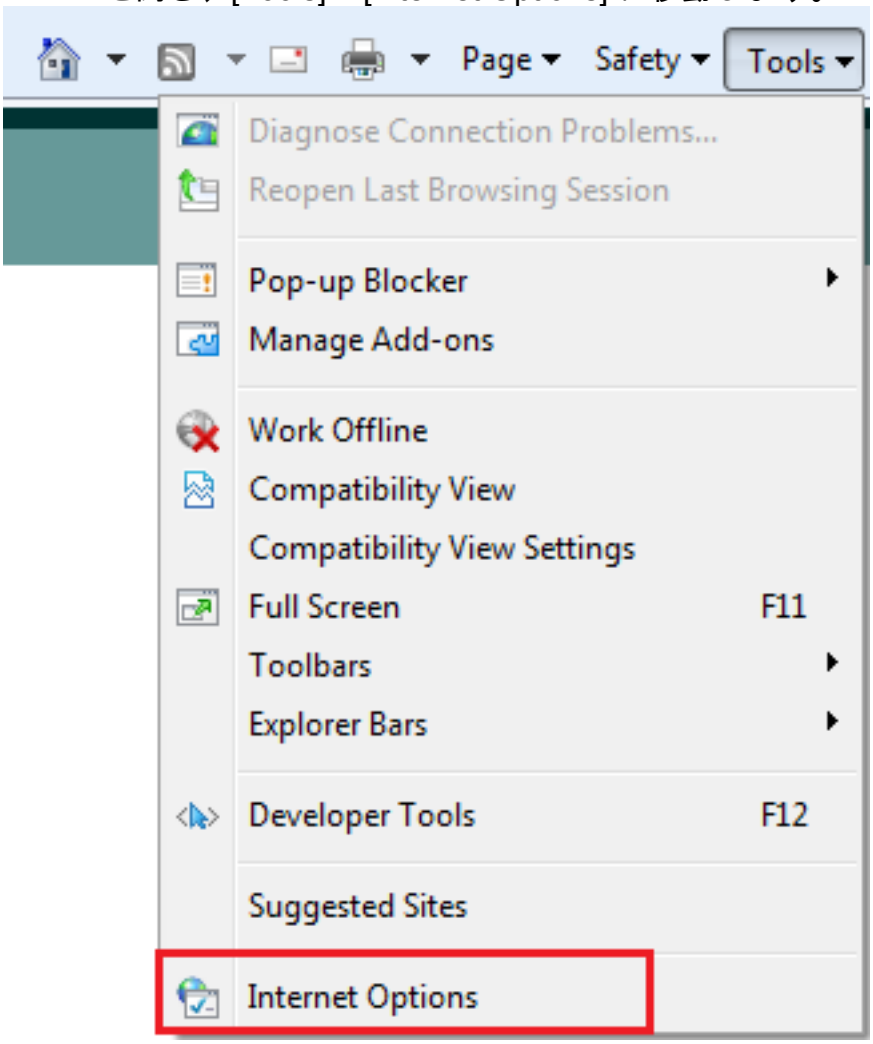


- [Finish] をクリックして、インストールを完了します。

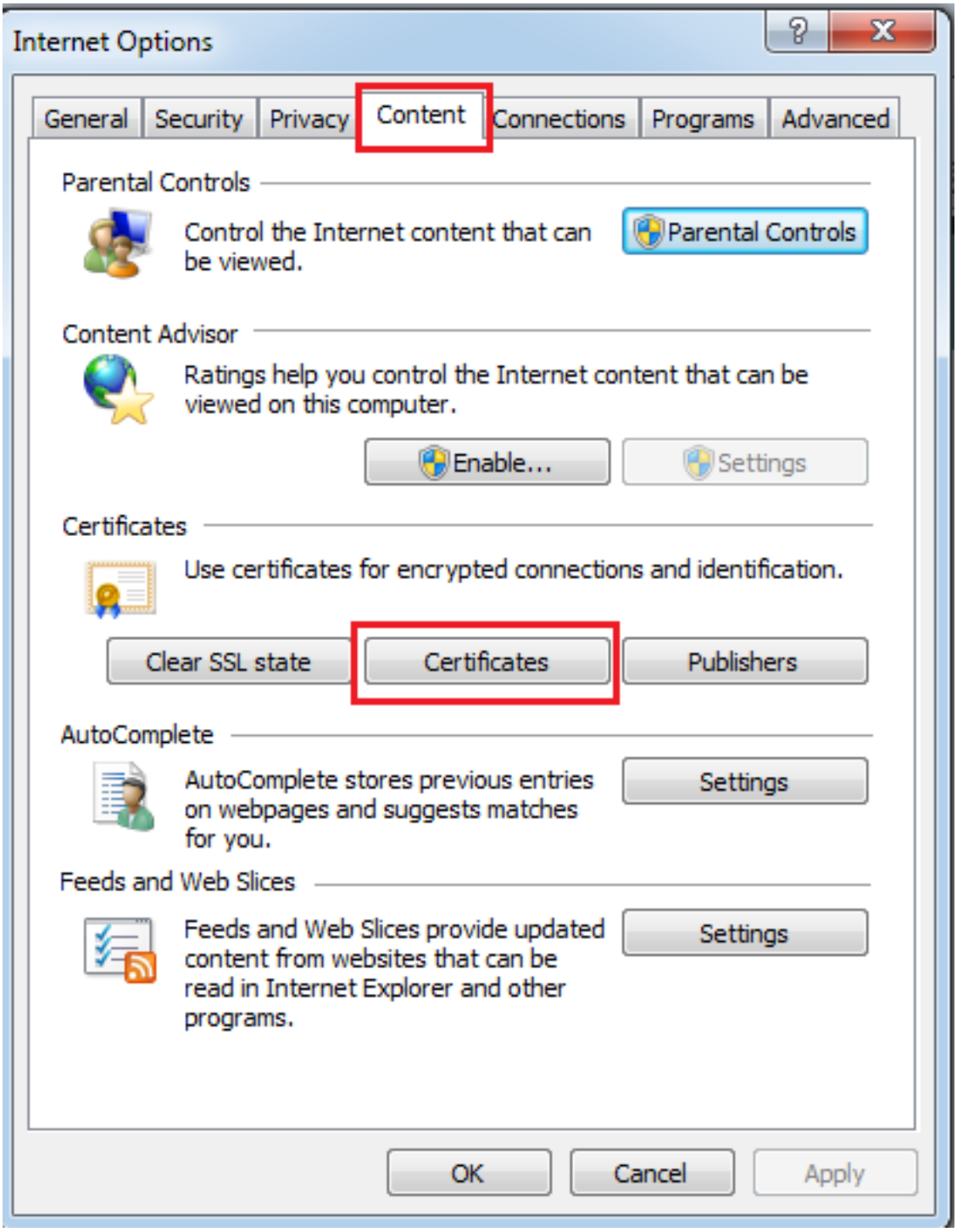

Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected
Automatically determined by t
Content
PFX
File Name
C:\Users\mrsethi\AppData\Lo
< Back
Finish
Cancel


Certificate Import Wizard
The import was successful.
OK

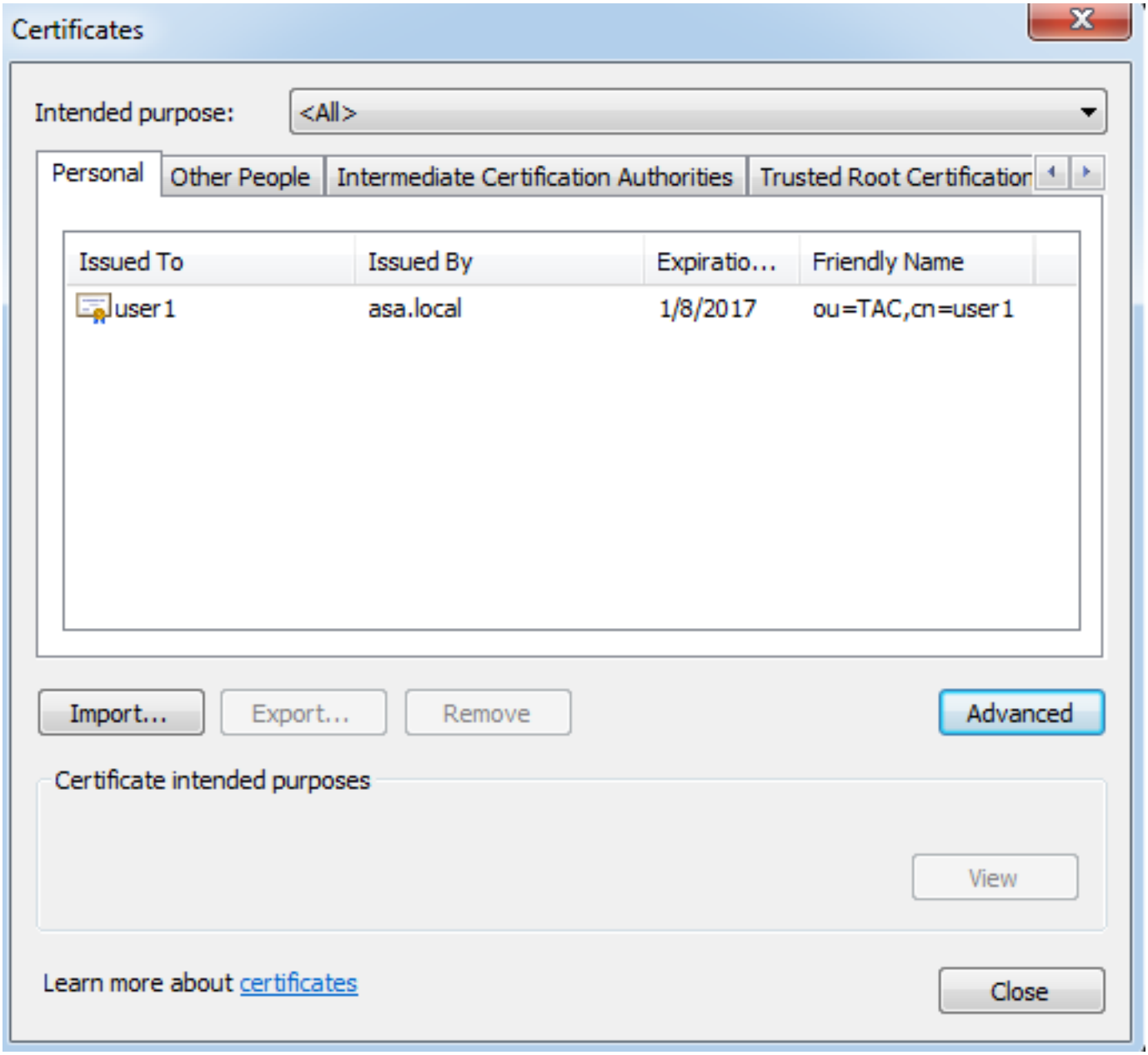
- 証明書が正常にインストールされたら、これを確認できます。
- IE を開き、[Tools] > [Internet Options] に移動します。



- 次の画像に示すように、[Content] タブに移動して、[Certificates] をクリックします。



- [Personal] ストアでは、ASA から受信した証明書を表示できます。



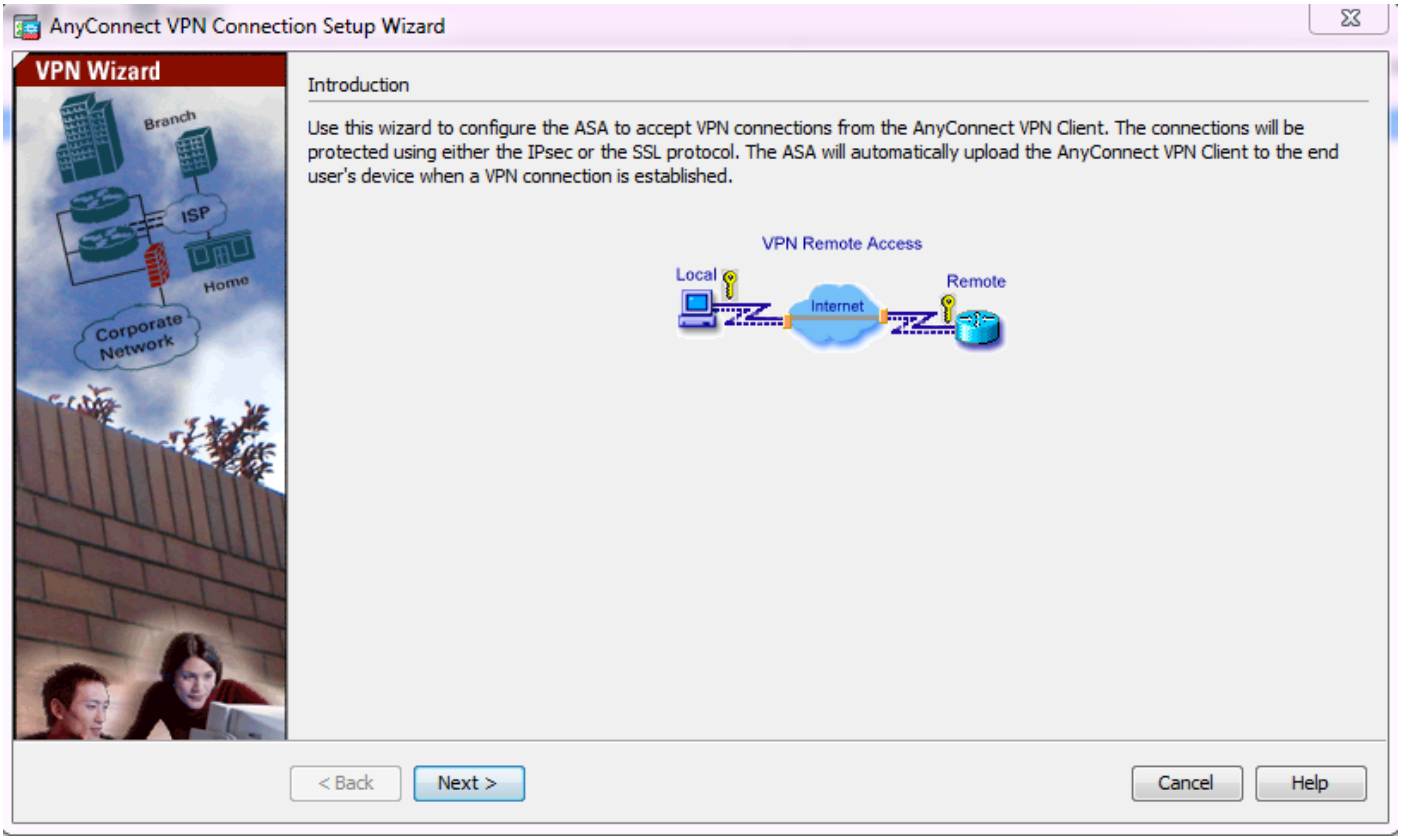
AnyConnect クライアント用の SSL ゲートウェイとしての ASA

ASDM AnyConnect 構成ウィザード

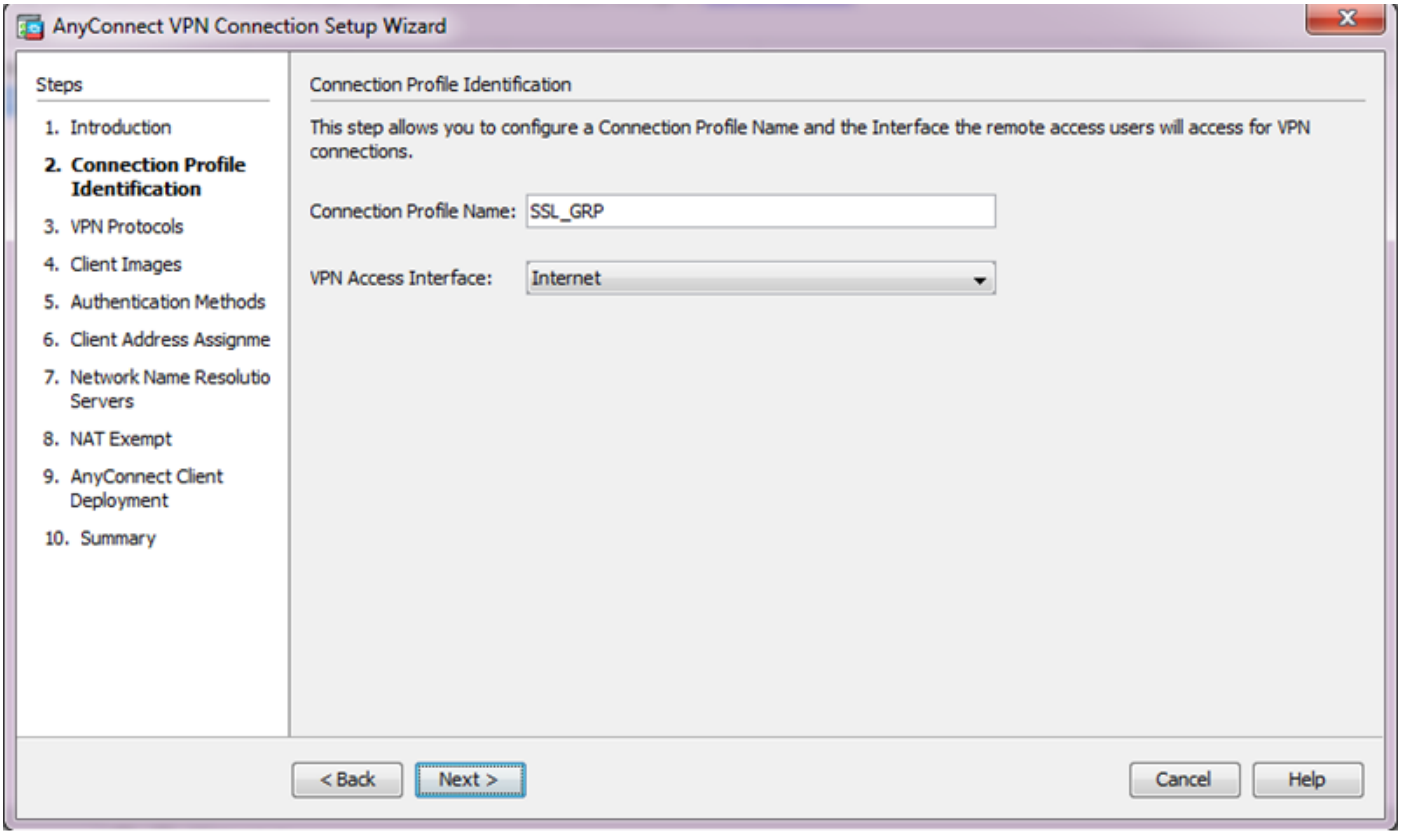
AnyConnect 構成ウィザード/CLI は、AnyConnect セキュア モビリティ クライアントを設定するために使用できます。 先に進む前に、AnyConnect クライアント パッケージが ASA ファイアウォールのフラッシュまたはディスクにアップロードされていることを確認します。

構成ウィザードを使用して AnyConnect セキュア モビリティ クライアントを設定するために、次の手順を実行します。

1. ASDM にログインし、[Wizards] > [VPN Wizards] > [AnyConnect VPN Wizard] に移動して設定ウィザードを起動し、[Next] をクリックします。

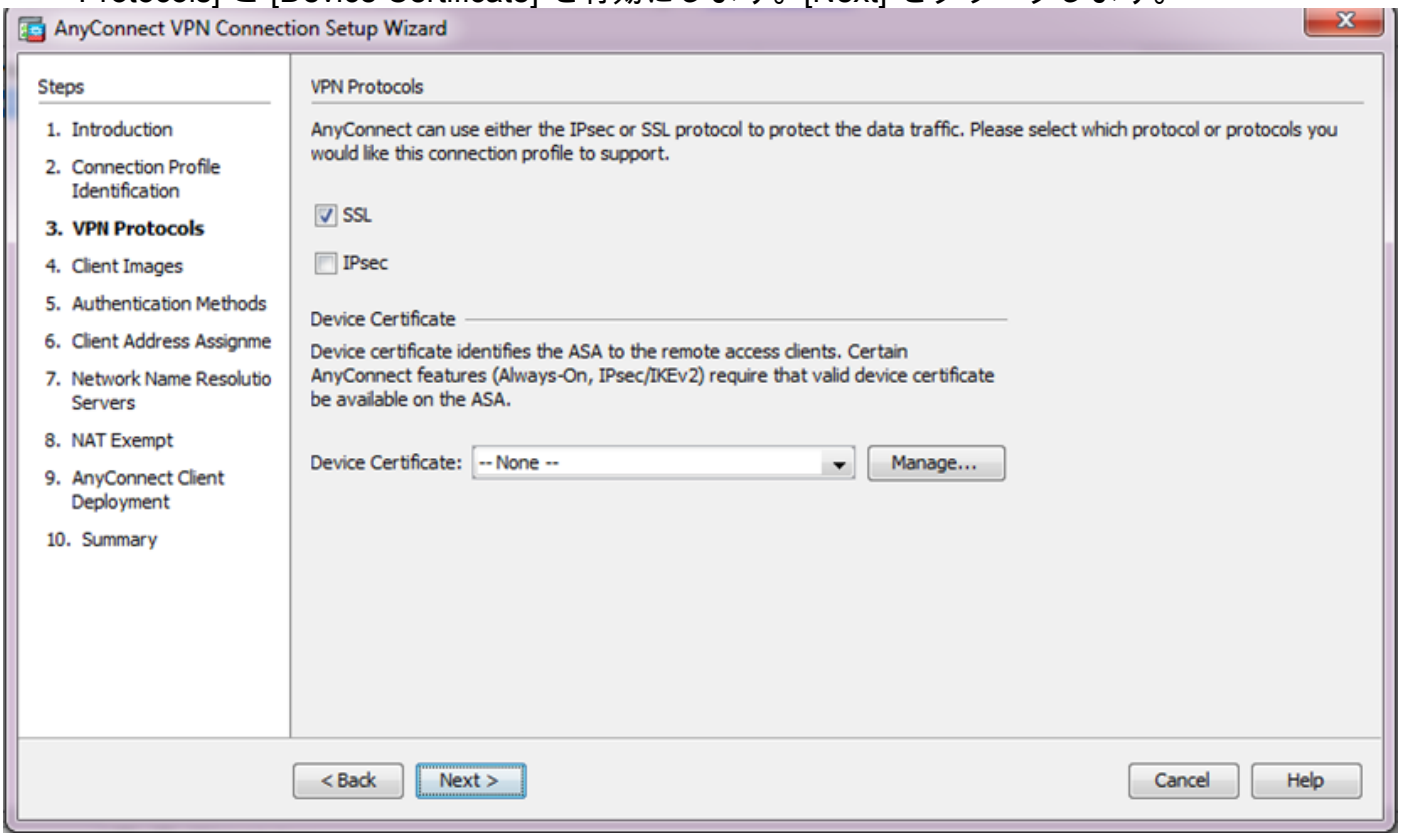


2. [Connection Profile Name] を入力し、VPN から終端されるインターフェイスを [VPN Access Interface] ドロップダウン メニューから選択して、[Next] をクリックします。



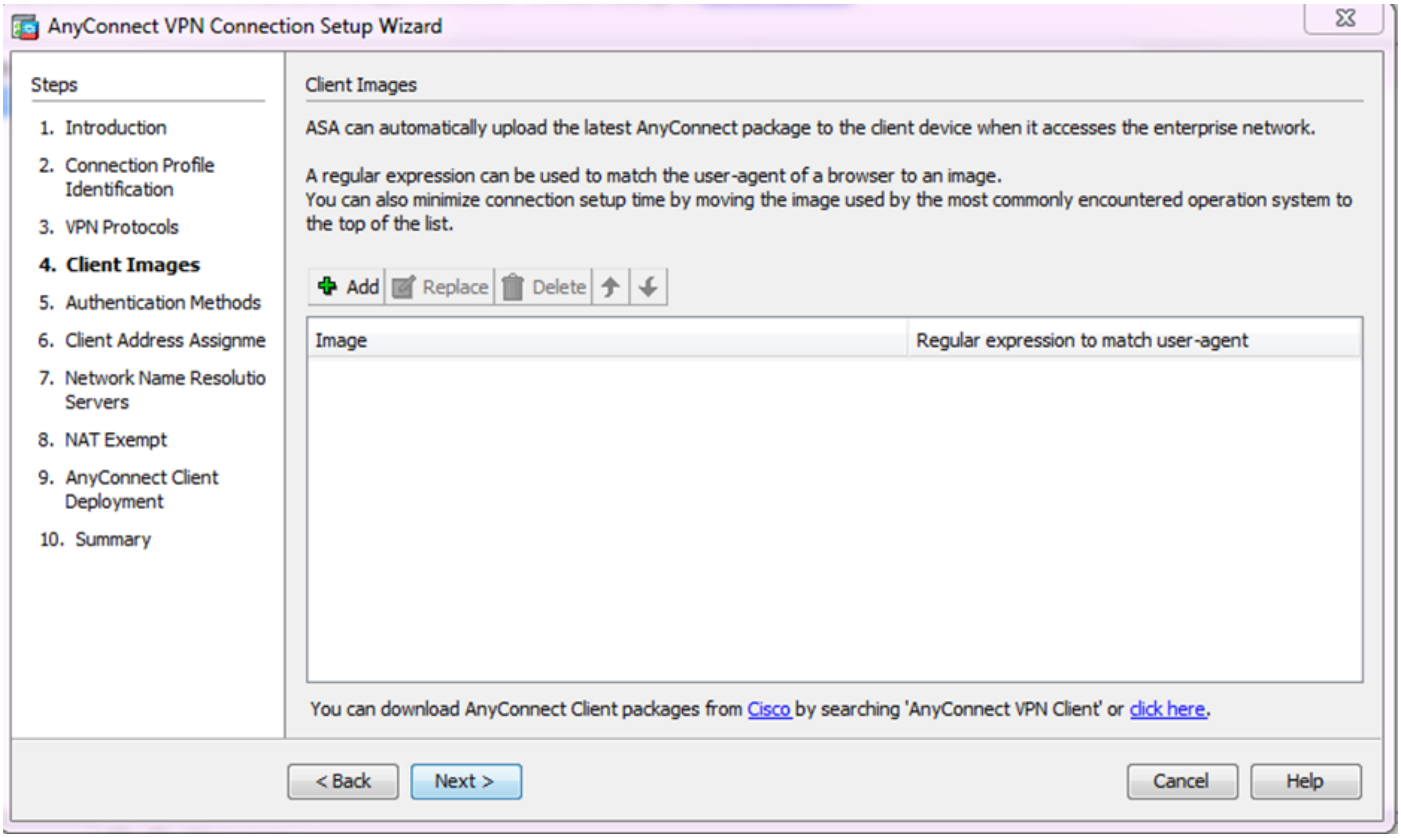
3. セキュア ソケット レイヤ（SSL）を有効にするために、[SSL] チェックボックスにチェックを入れます。 デバイス証明書は、信頼できるサードパーティの認証局（CA）によって発行された証明書（Verisign、Entrust など）や自己署名証明書にすることができます。 証明書がすでに ASA にインストールされている場合、ドロップダウン メニューから選択できます。

1. **注:** この証明書は ASA によって SSL クライアントに提示されるサーバ側の証明書です。ASA に現在インストールされているサーバ証明書がない場合、自己署名証明書を生成する必要があります。その後、[Manage] をクリックします。サードパーティの証明書をインストールするために、シスコの ASA 8.x WebVPN で使用するサードパーティ ベンダーの証明書を手動でインストールする設定例の資料で説明されている手順を実行します。[VPN Protocols] と [Device Certificate] を有効にします。[Next] をクリックします。

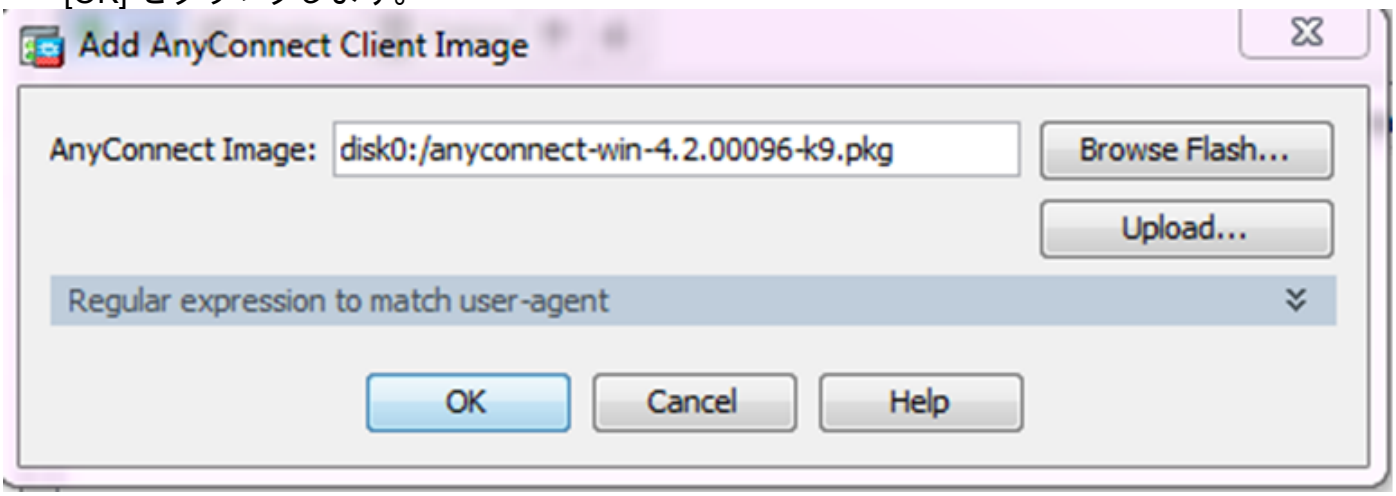


4. ローカル ドライブまたは ASA のフラッシュ/ディスクから AnyConnect クライアント パッケージ（.pkg ファイル）を追加するために、[Add] をクリックします。

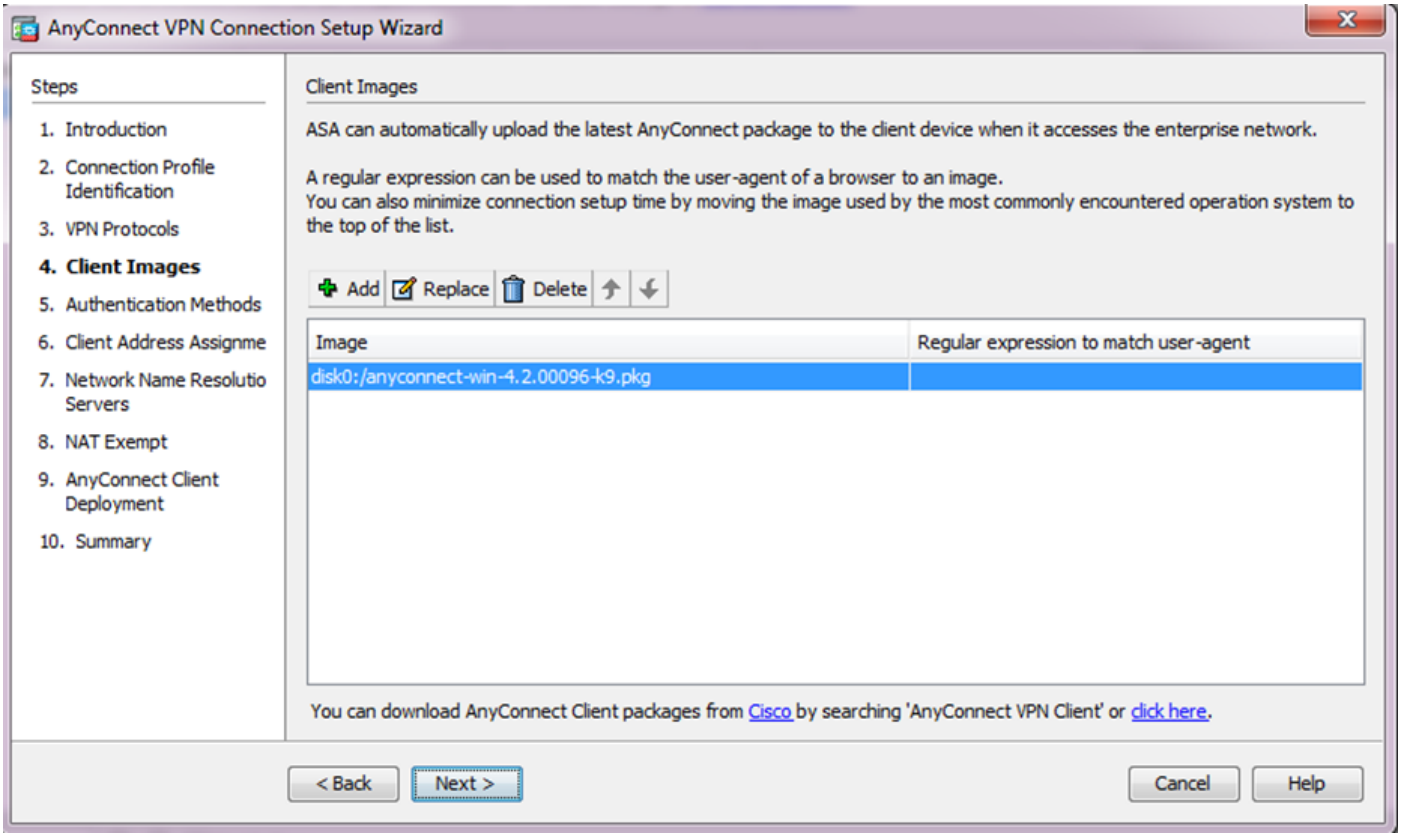
フラッシュ ドライブから画像を追加するには、[Browse Flash] をクリックし、ホスト マシンのローカル ドライブから画像を追加するには、[Upload] をクリックします。



- AnyConnect.pkg ファイルは、ASA フラッシュ/ディスク（パッケージがすでに存在する場合）またはローカル ドライブのいずれかからアップロードできます。
- Browse flash：AnyConnect パッケージを ASA フラッシュ/ディスクから選択します。
- Upload：AnyConnect パッケージをホスト マシンのローカル ドライブから選択します。
- [OK] をクリックします。

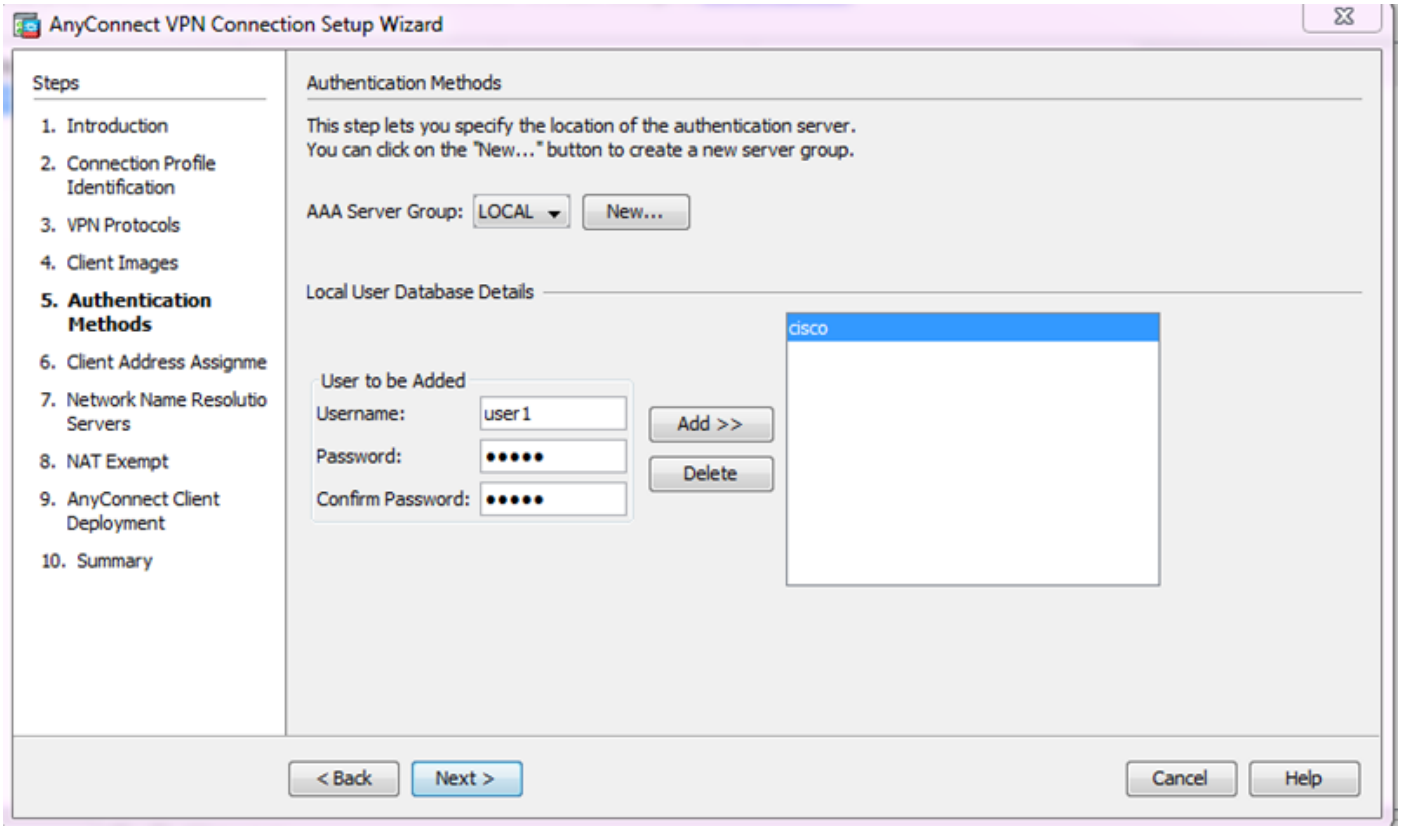


- [Next] をクリックします。

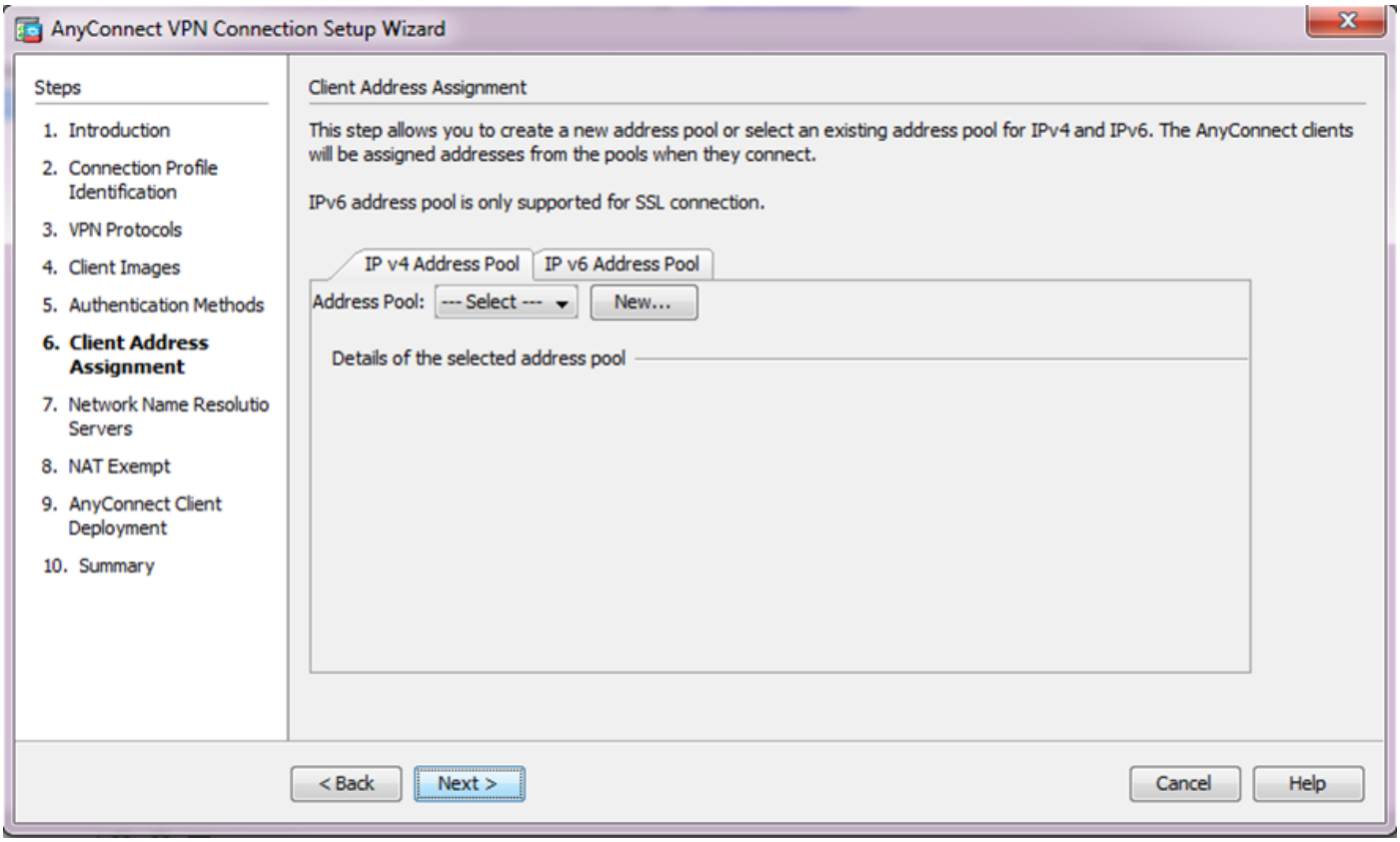


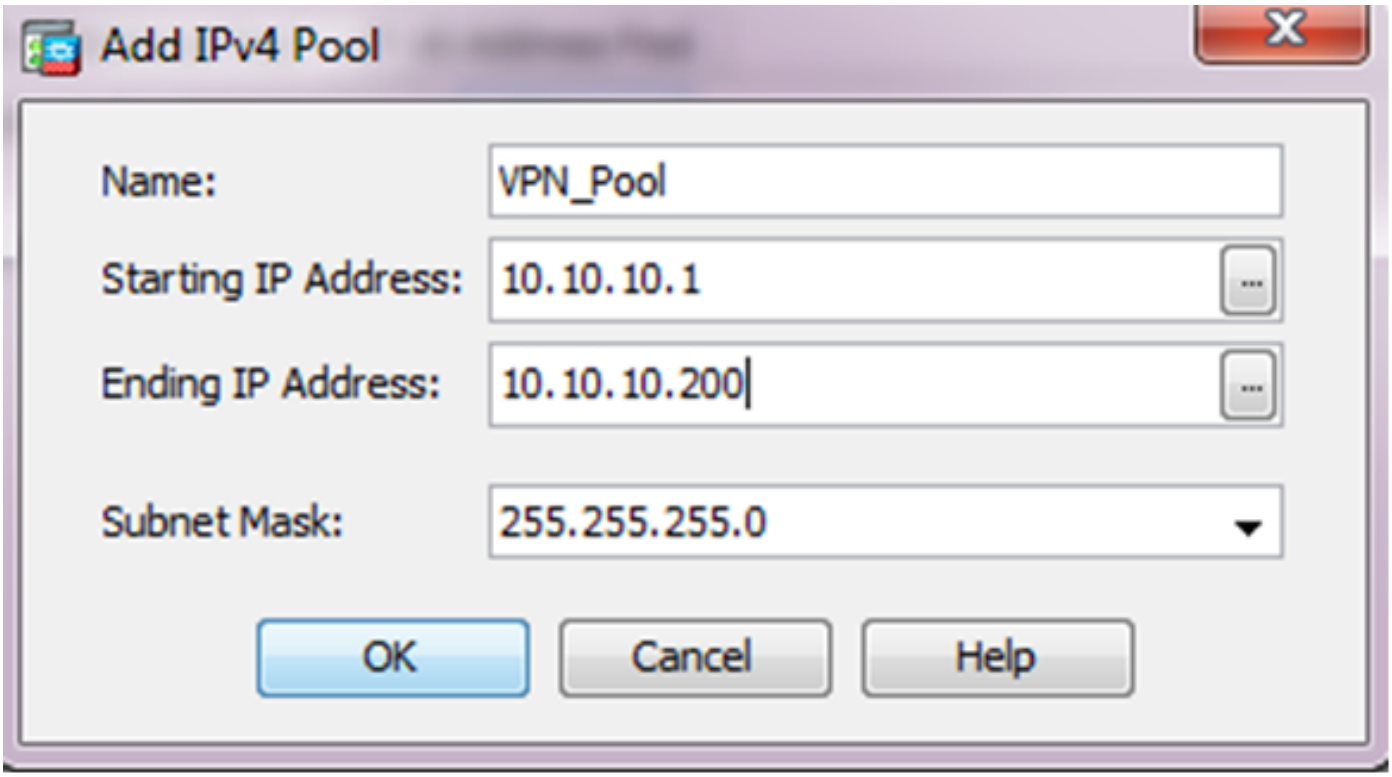
5. ユーザ認証は認証、許可、およびアカウンティング（AAA）サーバ グループを介して実行できます。 ユーザがすでに設定されている場合、[LOCAL] を選択して、[Next] をクリックします。 その他に、ユーザをローカル ユーザ データベースに追加して、[Next] をクリックします。

注: この例では、**ローカル認証**が設定されています。これは、ASA のローカル ユーザ データベースが認証に使用されることを示します。

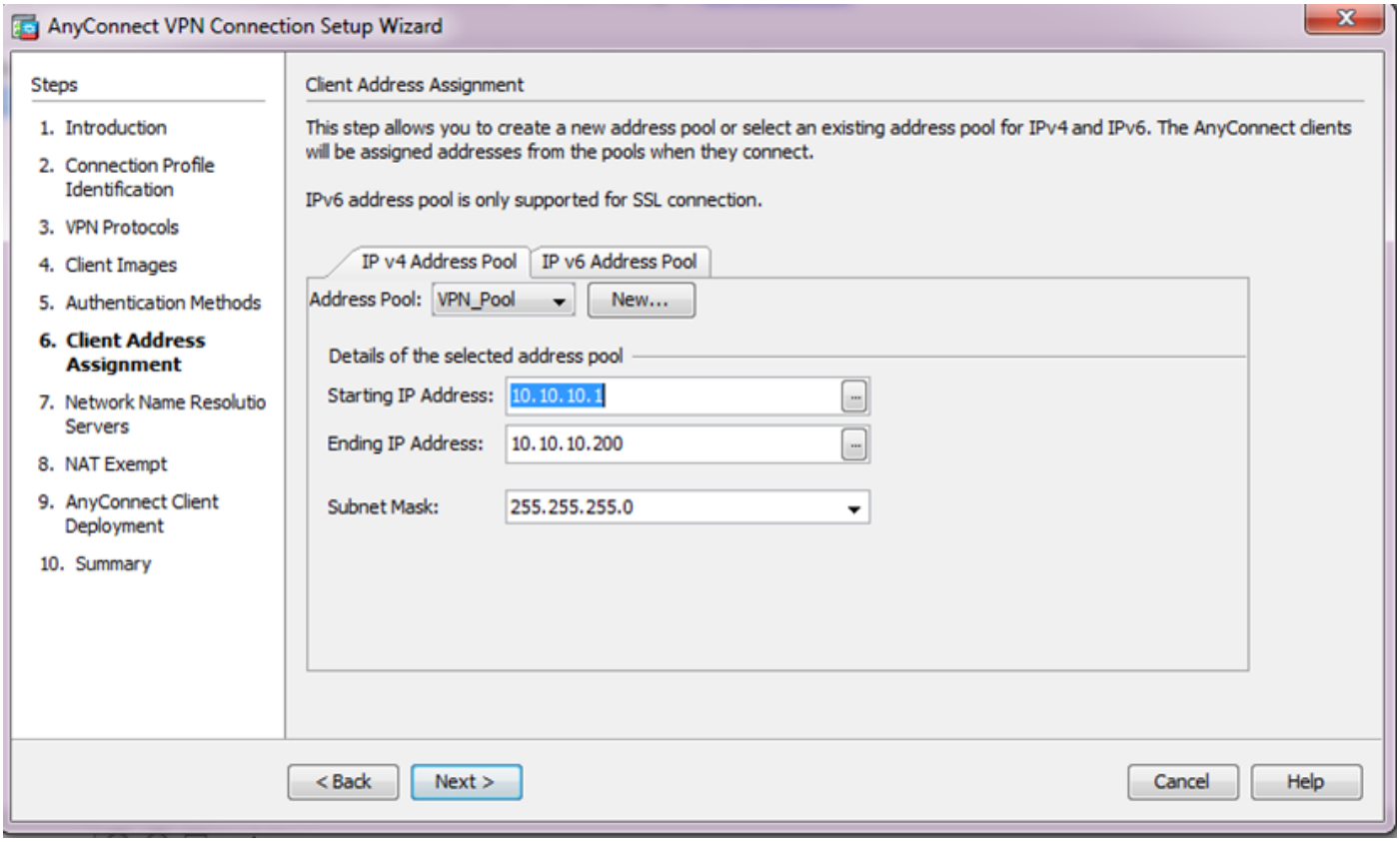


6. VPN クライアントのアドレス プールが設定されていることを確認します。 ip プールがすでに設定されている場合、ドロップダウン メニューから選択します。 設定されていない場合、[New] をクリックして設定します。 完了したら [next] をクリックします。

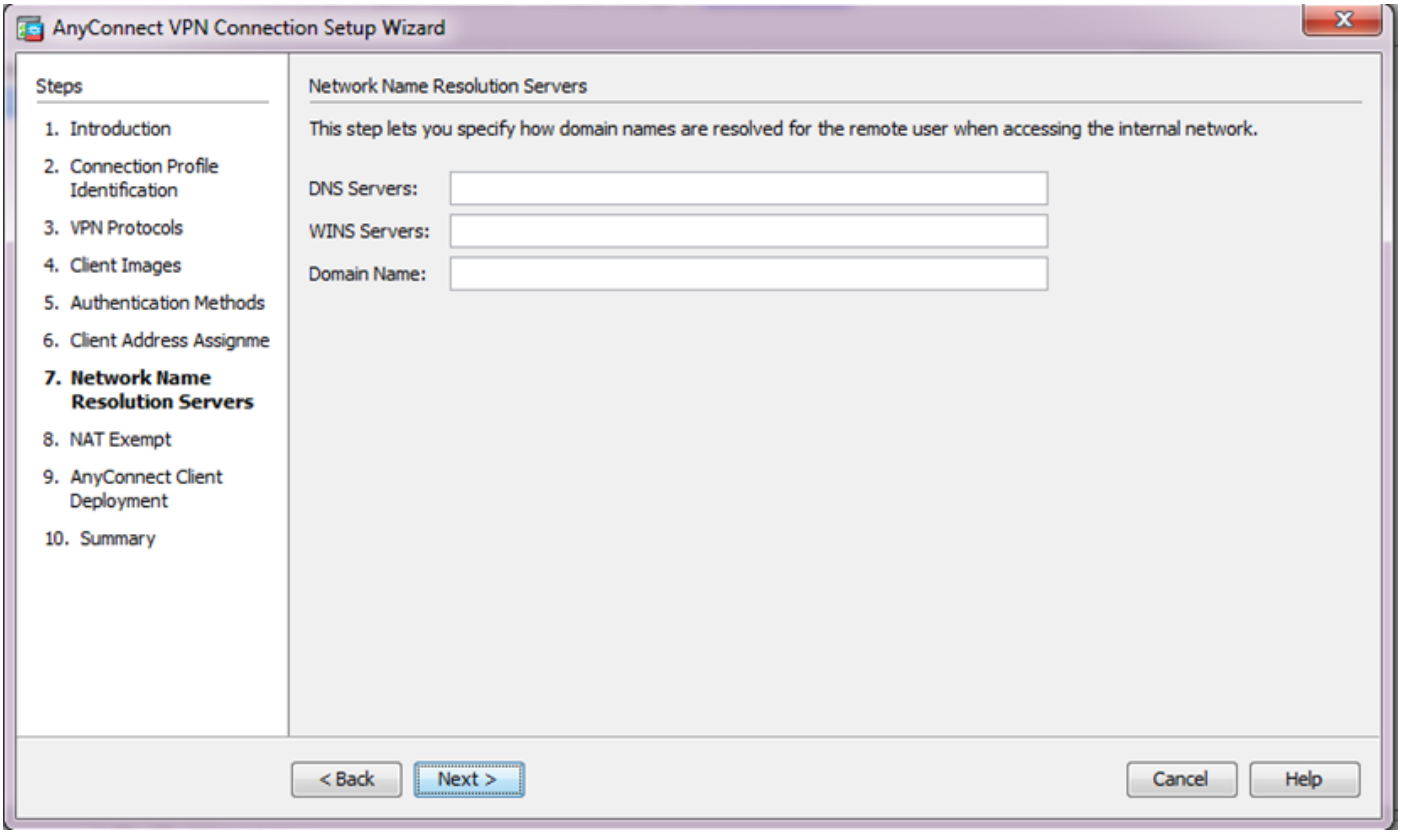




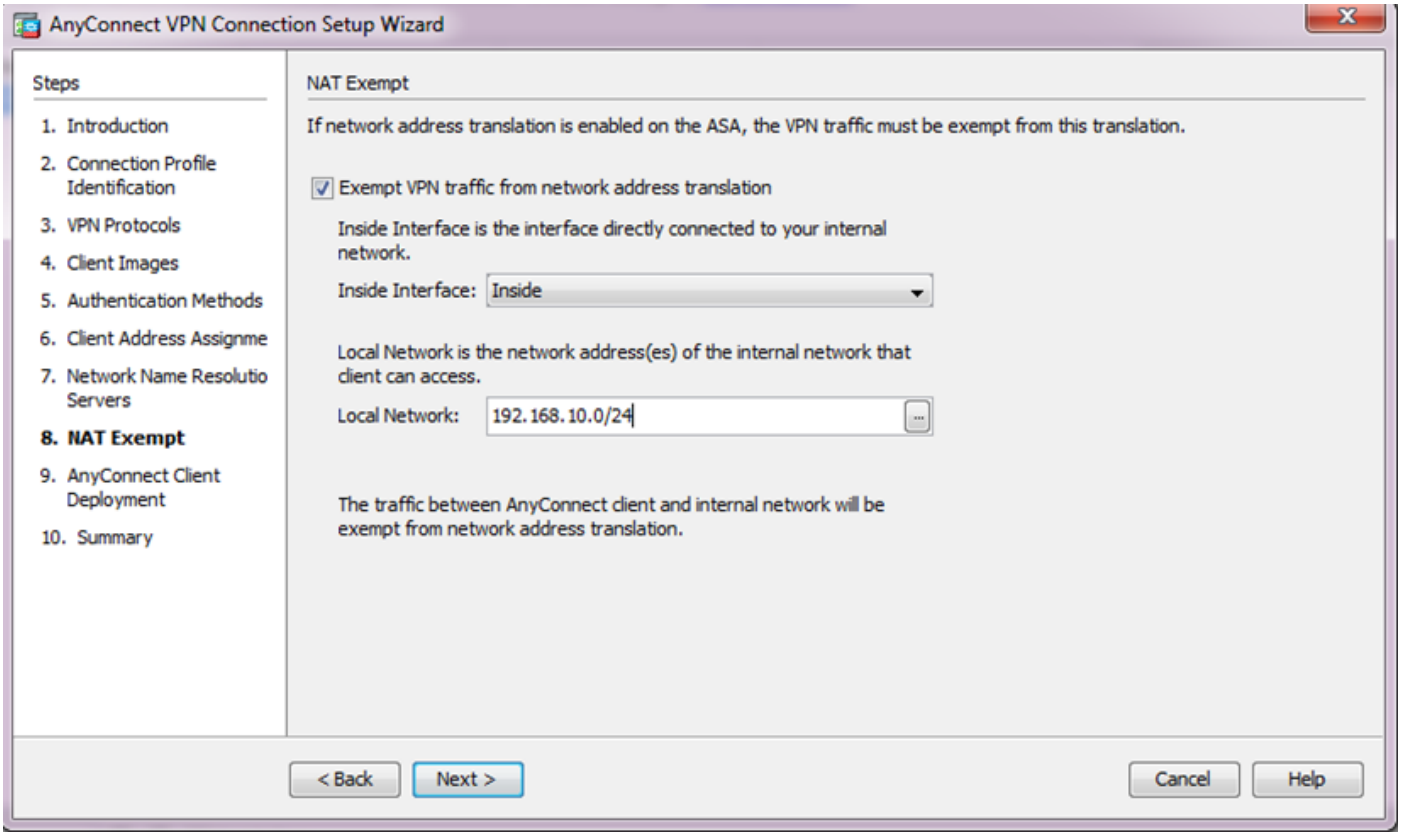
- [Next] をクリックします。



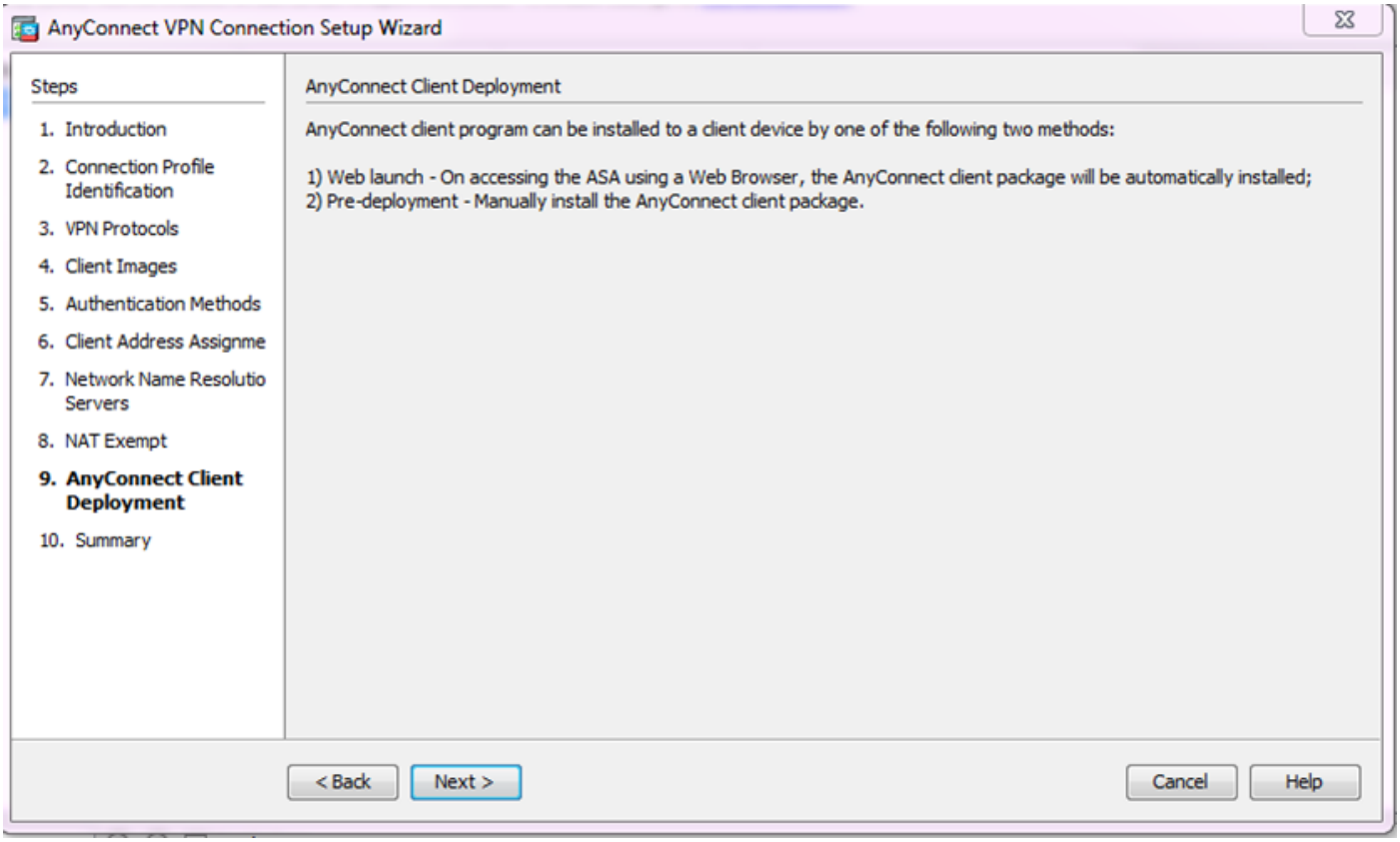
7. 必要に応じて、ドメイン ネーム システム（DNS）サーバと DN を [DNS Servers] および [Domain Name] フィールドに設定し、[Next] をクリックします。



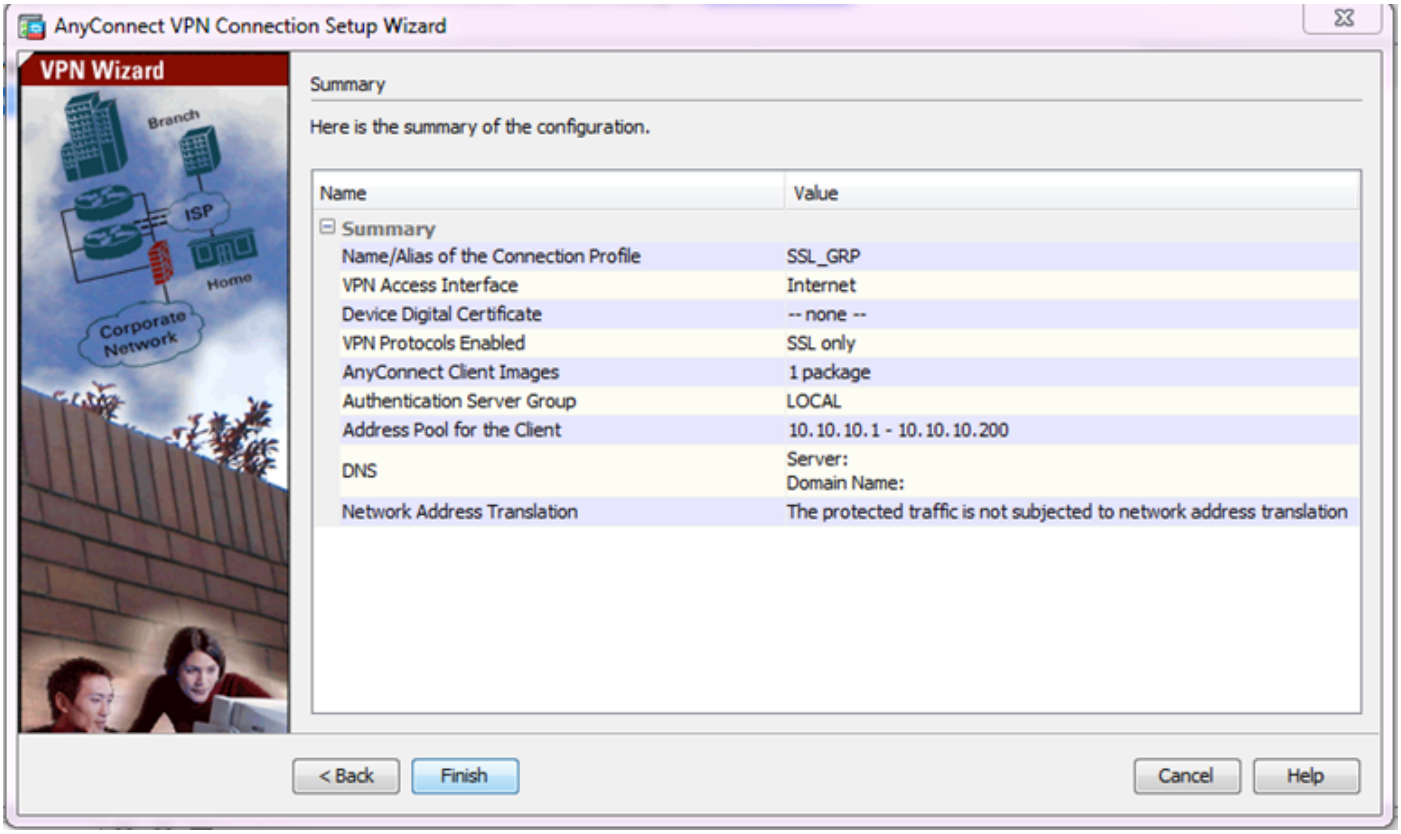
8. クライアントと内部のサブネット間のトラフィックは動的ネットワーク アドレス変換（NAT）の適用が除外される必要があります。 [Exempt VPN traffic from network address translation] チェック ボックスを有効にし、適用の除外に使用される LAN インターフェイスを設定します。 また、適用が除外されるローカル ネットワークを指定して、[Next] をクリックします。



9. [Next] をクリックします。

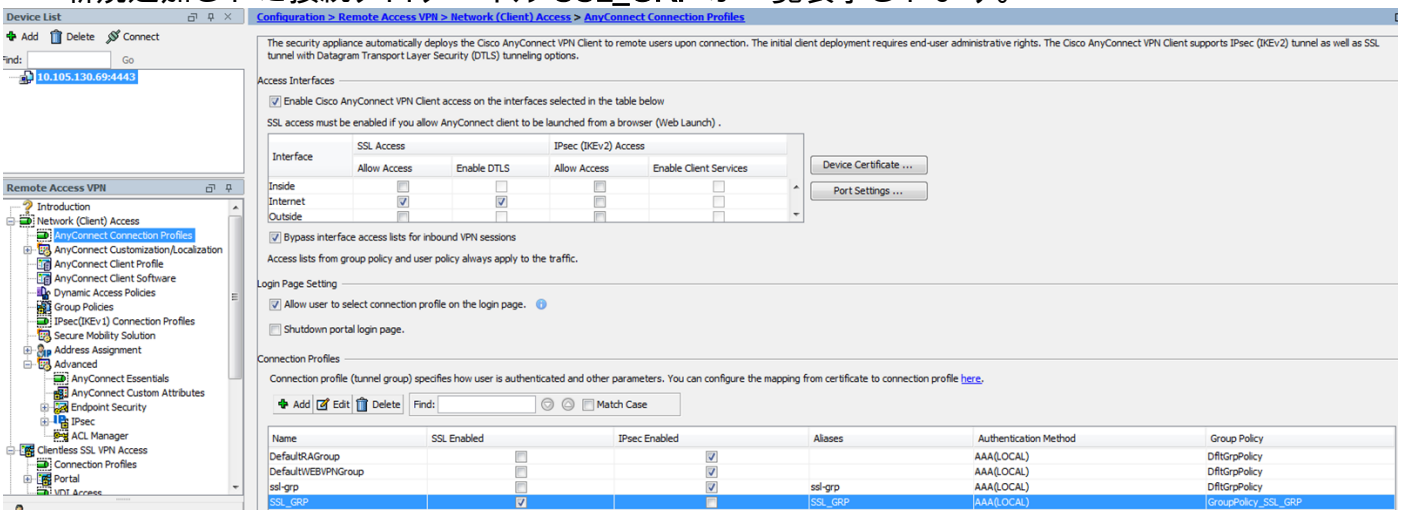


10. 最後の手順は要約を示します。設定を完了するには、[Finish] をクリックします。

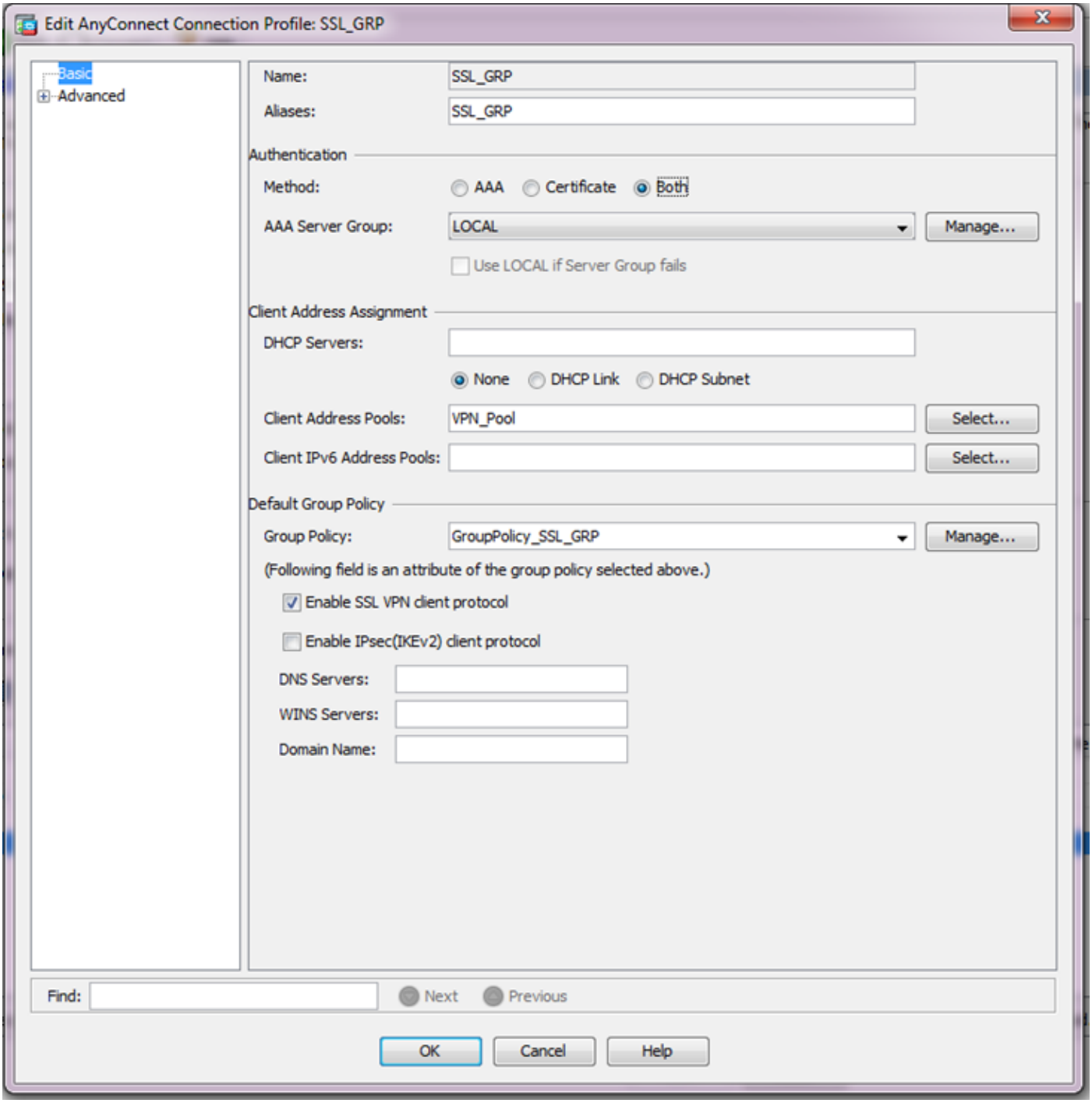


これで、AnyConnect クライアントの設定が完了しました。 ただし、構成ウィザードで AnyConnect を設定すると、**認証方式が AAA** にデフォルトで設定されます。 証明書およびユーザ名とパスワードでクライアントを認証するには、認証方式として証明書と AAA を使用するようにトンネル グループ（接続プロファイル）を設定する必要があります。

- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択します。
- 新規追加された接続プロファイル **SSL_GRP** が一覧表示されます。



- **AAA と証明書認証**を設定するために、接続プロファイルに [SSL_GRP] を選択して、[Edit] をクリックします。
- [Authentication Method] で、[Both] を選択します。



AnyConnect 用の CLI の設定

```
!! *****Configure the VPN Pool*****

ip local pool VPN_Pool 10.10.10.1-10.10.10.200 mask 255.255.255.0

!! *****Configure Address Objects for VPN Pool and Local Network*****

object network NETWORK_OBJ_10.10.10.0_24
 subnet 10.10.10.0 255.255.255.0
object network NETWORK_OBJ_192.168.10.0_24 subnet 192.168.10.0 255.255.255.0 exit !!
*****Configure WebVPN*****

webvpn enable Internet anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1 anyconnect
enable tunnel-group-list enable exit !! *****Configure User*****
```

```
username user1 password mbO2jYs13AXlIAGa encrypted privilege 2

!! *****Configure Group-Policy*****

group-policy GroupPolicy_SSL_GRP internal group-policy GroupPolicy_SSL_GRP attributes vpn-
tunnel-protocol ssl-client dns-server none wins-server none default-domain none exit !!
*****Configure Tunnel-Group*****

tunnel-group SSL_GRP type remote-access
tunnel-group SSL_GRP general-attributes
 authentication-server-group LOCAL
 default-group-policy GroupPolicy_SSL_GRP
 address-pool  VPN_Pool
tunnel-group SSL_GRP webvpn-attributes
 authentication aaa certificate
 group-alias SSL_GRP enable
 exit

!! *****Configure NAT-Exempt Policy*****

nat (Inside,Internet) 1 source static NETWORK_OBJ_192.168.10.0_24 NETWORK_OBJ_192.168.10.0_24
destination static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24 no-proxy-arp route-lookup
```

確認

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。

> **注:** 特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

CA サーバが有効であることを確認します。

show crypto ca server

```
ASA(config)# show crypto ca server
Certificate Server LOCAL-CA-SERVER:
    Status: enabled
   State: enabled
   Server's configuration is locked  (enter "shutdown" to unlock it)
   Issuer name: CN=ASA.local
   CA certificate fingerprint/thumbprint: (MD5)
       32e868b9 351a1b07 4b59cce5 704d6615
   CA certificate fingerprint/thumbprint: (SHA1)
       6136511b 14aa1bbe 334c2659 ae7015a9 170a7c4d
   Last certificate issued serial number: 0x1
   CA certificate expiration timer: 19:25:42 UTC Jan 8 2019
   CRL NextUpdate timer: 01:25:42 UTC Jan 10 2016
   Current primary storage dir: flash:/LOCAL-CA-SERVER/

   Auto-Rollover configured, overlap period 30 days
   Autorollover timer: 19:25:42 UTC Dec 9 2018

   WARNING: Configuration has been modified and needs to be saved!!
```

追加後に、ユーザが登録を許可されていることを確認します。

```
*****Before Enrollment*****

ASA# show crypto ca server user-db
username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll  >>> Shows the status "Allowed to Enroll"

*****After Enrollment*****

username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:05:14 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Enrolled, Certificate valid until 19:18:30 UTC Tue Jan 10 2017,
Renewal: Allowed
```

CLI または ASDM のいずれかを介して AnyConnect 接続の詳細を確認できます。

CLI の場合

show vpn-sessiondb detail anyconnect

```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : user1                  Index        : 1
Assigned IP  : 10.10.10.1             Public IP    : 10.142.189.181
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 13822                  Bytes Rx     : 13299
Pkts Tx      : 10                     Pkts Rx      : 137
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSL_GRP    Tunnel Group : SSL_GRP
Login Time   : 19:19:10 UTC Mon Jan 11 2016
Duration     : 0h:00m:47s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 1.1
  Public IP    : 10.142.189.181
  Encryption   : none                   Hashing      : none
  TCP Src Port : 52442                  TCP Dst Port : 443
  Auth Mode    : Certificate and userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Windows
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.2.00096
  Bytes Tx     : 6911                   Bytes Rx     : 768
```

```
  Pkts Tx       : 5                     Pkts Rx       : 1
  Pkts Tx Drop  : 0                     Pkts Rx Drop  : 0

SSL-Tunnel:
  Tunnel ID     : 1.2
  Assigned IP   : 10.10.10.1            Public IP     : 10.142.189.181
  Encryption    : RC4                   Hashing       : SHA1
  Encapsulation: TLSv1.0                TCP Src Port  : 52443
  TCP Dst Port  : 443                   Auth Mode     : Certificate and userPassword
  Idle Time Out: 30 Minutes             Idle TO Left  : 29 Minutes
  Client OS     : Windows
  Client Type   : SSL VPN Client
  Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.2.00096
  Bytes Tx      : 6911                  Bytes Rx      : 152
  Pkts Tx       : 5                     Pkts Rx       : 2
  Pkts Tx Drop  : 0                     Pkts Rx Drop  : 0

DTLS-Tunnel:
  Tunnel ID     : 1.3
  Assigned IP   : 10.10.10.1            Public IP     : 10.142.189.181
  Encryption    : AES128                Hashing       : SHA1
  Encapsulation: DTLSv1.0               UDP Src Port  : 59167
  UDP Dst Port  : 443                   Auth Mode     : Certificate and userPassword
  Idle Time Out: 30 Minutes             Idle TO Left  : 30 Minutes
  Client OS     : Windows
  Client Type   : DTLS VPN Client
  Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.2.00096
  Bytes Tx      : 0                     Bytes Rx      : 12907
  Pkts Tx       : 0                     Pkts Rx       : 142
  Pkts Tx Drop  : 0                     Pkts Rx Drop  : 0

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 51 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

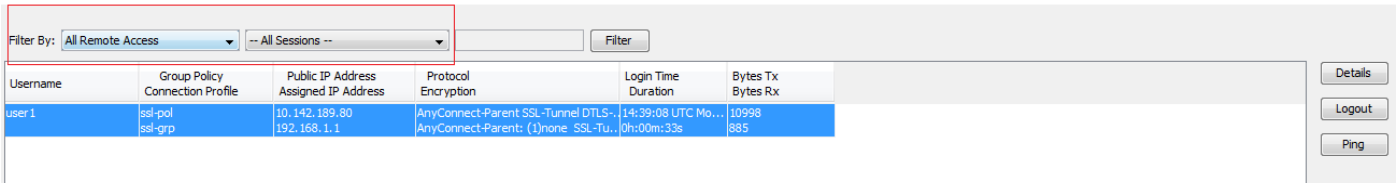
ASDM の場合

- [モニタリング（Monitoring）] > [VPN] > [VPN 統計情報（VPN Statistics）] > [セッション（Sessions）] の順に移動します。
- [Filter By] に [All Remote Access].を選択します。
- 選択した AnyConnect クライアントについていずれかの操作を実行できます。

Details：セッションに関する詳細情報が表示されます。

Logout：ヘッドエンドからユーザを手動でログアウトします。

Ping：ヘッドエンドから AnyConnect クライアントを ping します。



トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

> **注:** debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

> **注意**： ASA では、さまざまなデバッグ レベルを設定できます。 デフォルトでは、レベル 1 が使用されます。 デバッグ レベルを変更すると、デバッグの冗長性が高くなる場合があります。 特に実稼働環境では、注意して実行してください。

- **debug crypto ca**
- **debug crypto ca server**
- **debug crypto ca messages**
- **debug crypto ca transactions**
- **debug webvpn anyconnect**

次のデバッグ出力は、CA サーバが **no shut コマンド**を使用して有効にされている場合に示されます。

```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255

CRYPTO_CS: input signal enqueued: no shut   >>>>> Command issued to Enable the CA server
Crypto CS thread wakes up!

CRYPTO_CS: enter FSM: input state disabled, input signal no shut
CRYPTO_CS: starting enabling checks
CRYPTO_CS: found existing serial file.
CRYPTO_CS: started CA cert timer, expiration time is 17:53:33 UTC Jan 13 2019
CRYPTO_CS: Using existing trustpoint 'LOCAL-CA-SERVER' and CA certificate
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: DB version 1
CRYPTO_CS: last issued serial number is 0x4
CRYPTO_CS: closed ser file
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl
CRYPTO_CS: CRL file LOCAL-CA-SERVER.crl exists.
CRYPTO_CS: Read 220 bytes from crl file.
CRYPTO_CS: closed crl file
CRYPTO_PKI: Storage context locked by thread Crypto CA Server

CRYPTO_PKI: inserting CRL
CRYPTO_PKI: set CRL update timer with delay: 20250
CRYPTO_PKI: the current device time: 18:05:17 UTC Jan 16 2016

CRYPTO_PKI: the last CRL update time: 17:42:47 UTC Jan 16 2016
CRYPTO_PKI: the next CRL update time: 23:42:47 UTC Jan 16 2016
CRYPTO_PKI: CRL cache delay being set to: 20250000
CRYPTO_PKI: Storage context released by thread Crypto CA Server

CRYPTO_CS: Inserted Local CA CRL into cache!

CRYPTO_CS: shadow not configured; look for shadow cert
CRYPTO_CS: failed to find shadow cert in the db
CRYPTO_CS: set shadow generation timer
CRYPTO_CS: shadow generation timer has been set
CRYPTO_CS: Enabled CS.
```

```
CRYPTO_CS: exit FSM: new state enabled
CRYPTO_CS: cs config has been locked.

Crypto CS thread sleeps!
```

次のデバッグ出力はクライアントの登録を示します。

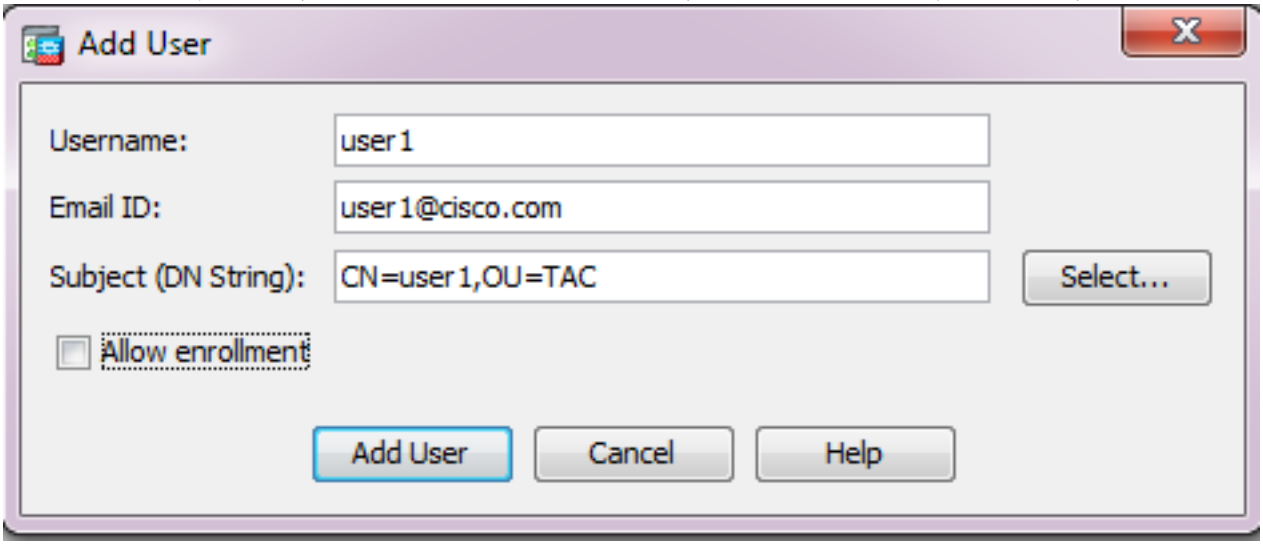
```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255

CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12
```

次の条件が発生している場合、クライアントの登録が失敗する場合があります。

シナリオ 1.

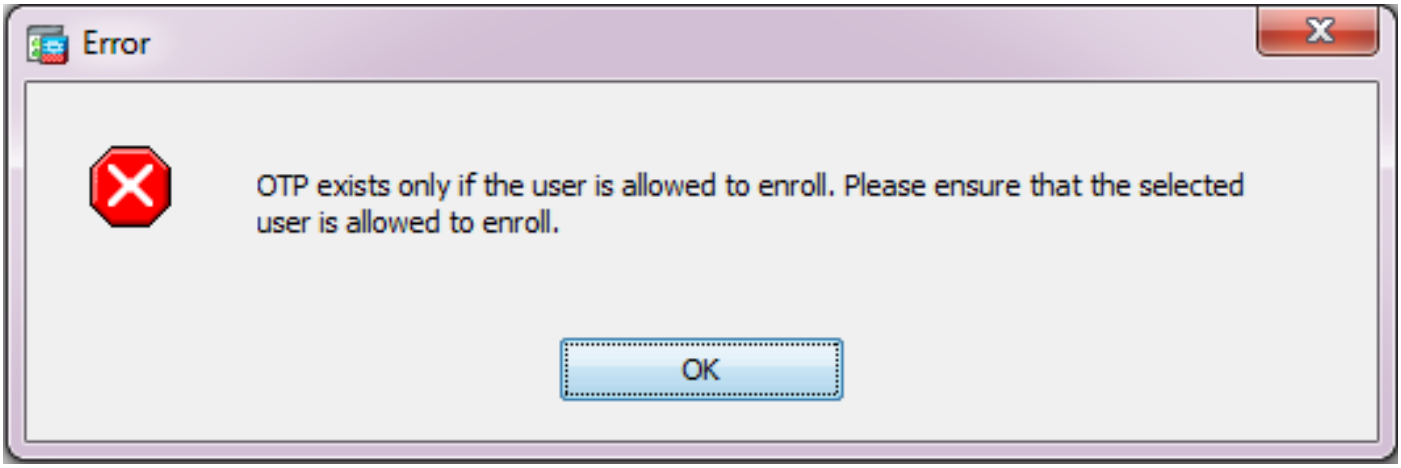
- ユーザは、登録する許可なしで CA サーバ データベースに作成されます。



CLI の同等の設定：

```
ASA(config)# show crypto ca server user-db
username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  <not allowed>
notified: 0 times
enrollment status: Not Allowed to Enroll
```

- ユーザが登録を許可されていない場合、ユーザの OTP を生成するかまたは電子メールで送信しようとすると、このエラー メッセージが出されます。



シナリオ 2.

- **show run webvpn** コマンドを使用して、登録ポータルが使用可能になっているポートおよびインターフェイスを確認します。 **デフォルト ポートは 443 です**が、変更可能です。
- クライアントが、登録ポータルへのアクセスを成功させるために使用されるポートで、**webvpn** が有効になっている**インターフェイスの IP アドレス**へのネットワーク到達可能性があることを確認します。

次のような場合、クライアントは ASA の登録ポータルにアクセスできないことがあります。

1. 中間デバイスが、クライアントから指定されたポート上の ASA の **webvpn** IP への着信接続をブロックする場合。
2. **webvpn** が有効になっているインターフェイスの状態がダウンしている場合。

- この出力は、登録ポータルをカスタム ポート **4433** の**インターフェイス Internet の IP アドレス**で使用できることを示しています。

```
ASA(config)# show run webvpn
webvpn
 port 4433
 enable Internet
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

シナリオ 3.

- CA サーバ データベース ストレージのデフォルトの場所は、ASA のフラッシュ メモリです。
- 登録時にユーザの **pkcs12** ファイルを生成して保存する空き領域がフラッシュ メモリにあることを確認します。
- フラッシュ メモリに十分な空き領域がない場合、ASA はクライアントの登録プロセスの完了に失敗し、次のデバッグ ログが生成されます。

```
ASA(config)# debug crypto ca 255
ASA(config)# debug crypto ca server 255
ASA(config)# debug crypto ca message 255
ASA(config)# debug crypto ca transaction 255
ASA(config)# debug crypto ca trustpool 255
```

```
CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12

CRYPTO_CS: Failed to write to opened PKCS12 file for user user1, fd: 0, status: -1.

CRYPTO_CS: Failed to generate pkcs12 file for user user1 status: -1.

CRYPTO_CS: Failed to process enrollment in-line for user user1. status: -1
```

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- AnyConnect VPN クライアントのトラブルシューティング ガイド - 一般的な問題
- AnyConnect セッションの管理、モニタリング、およびトラブルシューティング
- テクニカル サポートとドキュメント – Cisco Systems