將ASA配置為本地CA伺服器和AnyConnect頭端

目錄

簡介

必要條件

需求

採用元件

背景資訊

設定

網路圖表

ASA作為本地CA伺服器

步驟 1.在ASA上配置並啟用本地CA伺服器

步驟 2.建立使用者並將其增加到ASA資料庫

步驟 3.在WAN介面上啟用webvpn

步驟 4.在客戶端電腦上導入證書

ASA作為AnyConnect客戶端的SSL網關

ASDM AnyConnect配置嚮導

配置AnyConnect的CLI

驗證

疑難排解

相關資訊

簡介

本文檔介紹如何將思科自適應安全裝置(ASA)設定為證書頒發機構(CA)伺服器以及作為Cisco AnyConnect安全移動客戶端的安全套接字層(SSL)網關。

必要條件

需求

思科建議您瞭解以下主題：

- 運行軟體版本9.1.x的基本ASA配置
- ASDM 7.3或更高版本

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本9.1(6)的Cisco 5500系列ASA
- 適用於Windows的AnyConnect安全行動化使用者端4.x版

- 根據相容性圖表運行受支援的作業系統的PC。
- 思科調適型安全裝置管理員(ASDM)版本7.3

註：從Cisco軟體下載下載AnyConnect VPN客戶端軟體套件(anyconnect-win*.pkg)(僅限註冊客戶)。將AnyConnect VPN客戶端複製到ASA的快閃記憶體，快閃記憶體將下載到遠端使用者電腦，以便與ASA建立SSL VPN連線。有關詳細資訊，請參閱ASA配置指南的安裝AnyConnect客戶端部分。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

ASA上的證書頒發機構提供以下功能：

- 在ASA上整合基本證書授權操作。
- 部署證書。
- 提供對已頒發證書的安全吊銷檢查。
- 提供ASA上的證書頒發機構，用於基於瀏覽器(WebVPN)和基於客戶端(AnyConnect)的SSL VPN連線。
- 向使用者提供受信任的數位證書，無需依賴外部證書授權。
- 提供安全的內部證書身份驗證授權，並透過網站登入提供直接的使用者註冊。

準則和限制

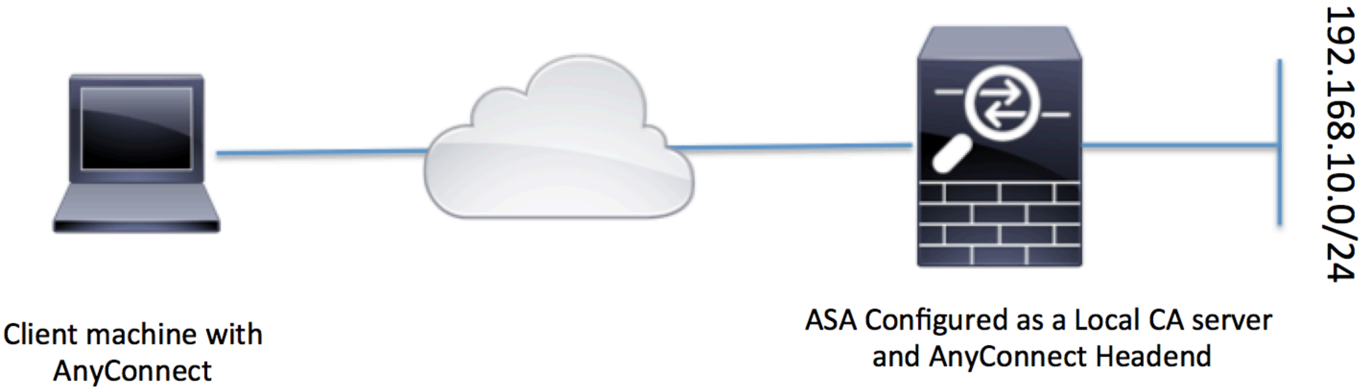
- 在路由和透明防火牆模式下受支援。
- 一次只能有一個本地CA伺服器駐留在ASA上。
- 故障切換設定中不支援ASA作為本地CA伺服器功能。
- 目前，ASA作為本地CA伺服器僅支援生成SHA1證書。
- 本地CA伺服器可用於基於瀏覽器和基於客戶端的SSL VPN連線。目前不支援IPSec。
- 不支援本地CA的VPN負載均衡。
- 本地CA不能是另一個CA的下屬。它只能作為根CA。
- 當前，ASA無法註冊到本地CA伺服器以獲取身份證書。
- 完成證書註冊後，ASA會儲存包含使用者金鑰對和證書鏈的PKCS12檔案，每個註冊需要約2 KB的快閃記憶體或磁碟空間。實際磁碟空間量取決於配置的RSA金鑰大小和證書欄位。在可用快閃記憶體數量有限的ASA上增加大量待處理的證書註冊時，請記住此指南，因為這些PKCS12檔案在配置的註冊檢索超時期間儲存在快閃記憶體中。

設定

本節介紹如何將Cisco ASA配置為本地CA伺服器。

注意：使用命令查詢工具(僅供註冊客戶使用)可獲取有關此部分中所用命令的更多資訊。

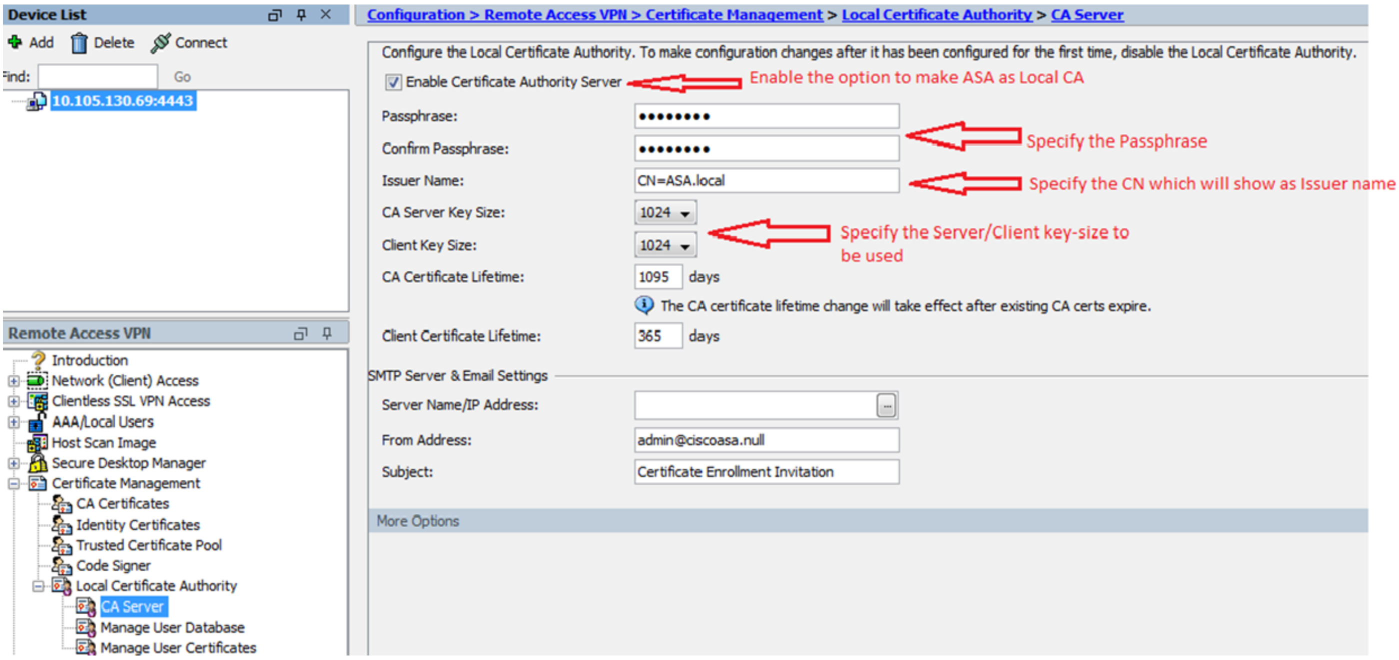
網路圖表


Client machine with AnyConnect
ASA Configured as a Local CA server and AnyConnect Headend
192.168.10.0/24

ASA作為本地CA伺服器

步驟 1.在ASA上配置並啟用本地CA伺服器

- 導航到Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server。選中Enable Certificate Authority server 選項。
- 配置密碼。密碼短語應最少為7個字元，用於編碼和儲存包含本地CA證書和金鑰對的PKCS12檔案。如果CA證書或金鑰對丟失，密碼短語會解鎖PKCS12存檔。
- 配置頒發者名稱。此欄位將顯示為根證書CN。這可以用下列格式指定：CN（一般名稱）、OU（組織單位）、(O)組織、L（地點）、S（州）和C（國家）。
- 可選配置：配置SMTP伺服器和電子郵件伺服器設定，以確保終端客戶端可以透過郵件接收OTP以完成註冊。您可以配置本地電子郵件/SMTP伺服器的主機名或IP地址。還可以配置客戶端將收到的電子郵件的發件人地址和主題欄位。預設情況下，發件人地址是admin@<ASA主機名>.null ，主題是證書註冊邀請。
- 可選配置：還可以配置可選引數，如客戶端金鑰大小、CA伺服器金鑰大小、Ca證書有效期和客戶端證書有效期。



Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server

Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority.

☑ Enable Certificate Authority Server — Enable the option to make ASA as Local CA

Passphrase: ••••••••

Confirm Passphrase: •••••••• — Specify the Passphrase

Issuer Name: CN=ASA.local — Specify the CN which will show as Issuer name

CA Server Key Size: 1024

Client Key Size: 1024 — Specify the Server/Client key-size to be used

CA Certificate Lifetime: 1095 days

The CA certificate lifetime change will take effect after existing CA certs expire.

Client Certificate Lifetime: 365 days

SMTP Server & Email Settings

Server Name/IP Address:

From Address: admin@ciscoasa.null

Subject: Certificate Enrollment Invitation

等效的CLI命令：

```
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
```

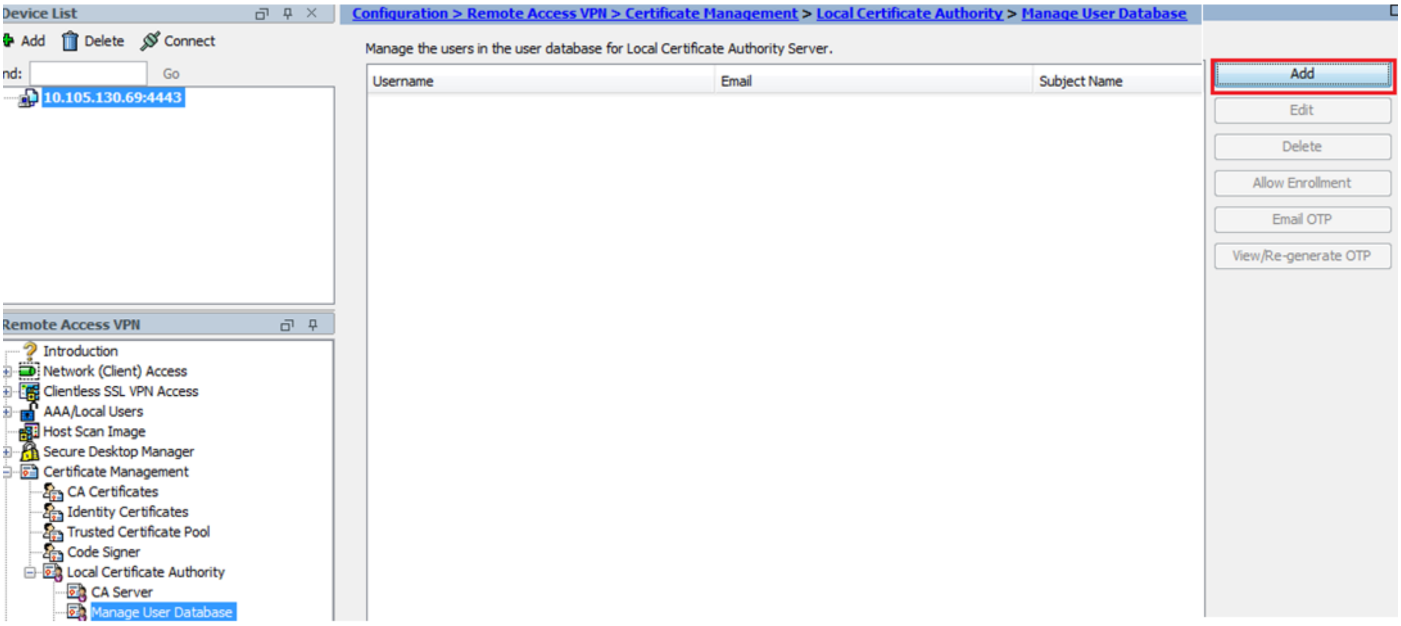
以下是可以在本地CA伺服器配置下配置的其他欄位。

CRL分發點URL	這是ASA上的CRL位置。 預設位置是http://hostname.domain/+CSCOCA+/asa_ca.crl，但可以修改url。
Publish-CRL介面和埠	要使CRL可用於在給定介面和埠上進行HTTP下載，請從下拉選單中選擇一個publish-CRL介面。然後輸入埠號，可以是從1到65535的任何埠號。預設埠號為TCP埠80。
CRL存留期	每次撤銷或取消撤銷使用者證書時，本地CA都會更新並重新頒發CRL，但是如果沒有撤銷更改，則每隔CRL生存期(您在本地CA配置期間使用lifetime crlcommand指定的時間段)一次，CRL將自動重新頒發。如果不指定CRL生存期，則預設時間段為六小時。

資料庫儲存位置	ASA使用本地CA資料庫訪問和實施使用者資訊、頒發的證書和撤銷清單。預設情況下，此資料庫駐留在本地快閃記憶體中，或者可以配置為駐留在已裝載並可由ASA訪問的外部檔案系統上。
預設主體名稱	輸入預設主體（DN字串）以附加到已簽發憑證上的使用者名稱。以下清單提供允許的DN屬性： ·CN （一般名稱）SN （姓氏） ·O （組織名稱） ·L（地區） ·C（國家/地區） ·OU （組織單位） ·EA （電子郵件地址） ·ST（州/省） ·T（標題）
註冊期間	設定使用者從ASA檢索PKCS12檔案的註冊時間限制（小時）。 預設值為24小時。 注意：如果註冊期間在使用者檢索包括使用者證書的PKCS12檔案之前到期，則不允許註冊。
一次性密碼過期	定義OTP對使用者註冊有效的時間量（小時）。此時間段從允許使用者註冊時開始。預設值為72小時。
憑證到期提醒	指定證書到期之前向證書所有者傳送重新註冊的初始提醒的天數。

步驟 2.建立使用者並將其增加到ASA資料庫

- 導航到Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database。按一下Add。

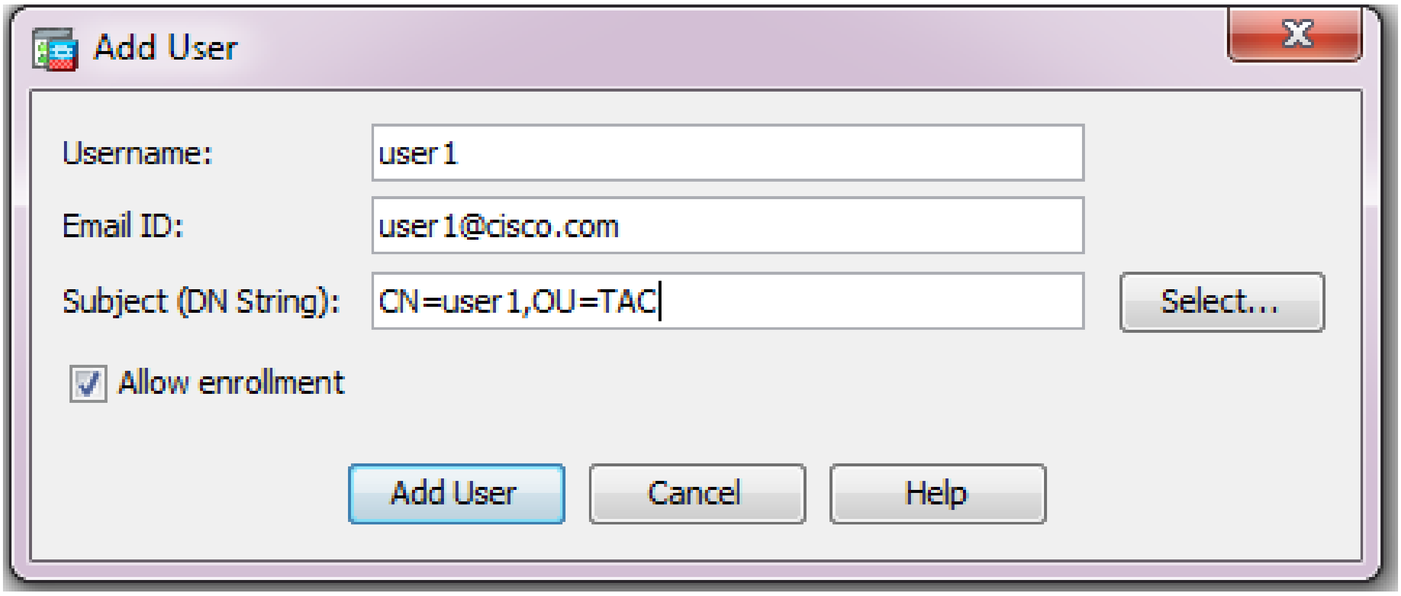


Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

Manage the users in the user database for Local Certificate Authority Server.

Username	Email	Subject Name

- 指定使用者詳細資訊，例如使用者名稱、電子郵件ID和主體名稱，如下圖所示。



Add User

Username: user1

Email ID: user1@cisco.com

Subject (DN String): CN=user1,OU=TAC

☑ Allow enrollment

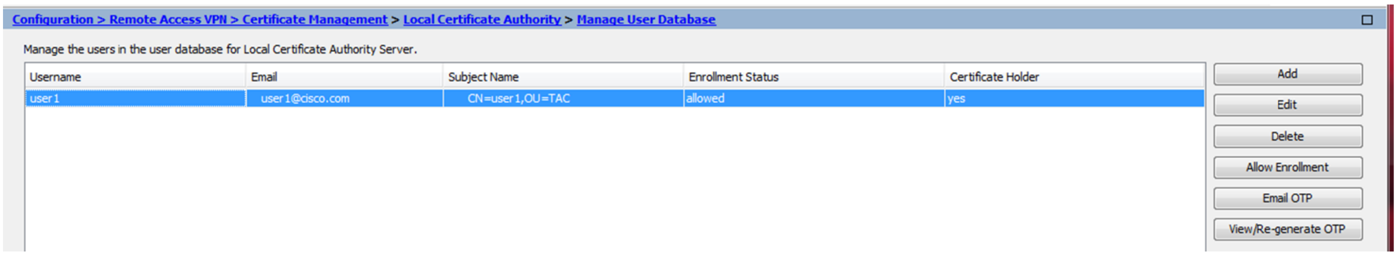
- 確保選中Allow Enrollment，以便您可以註冊證書。
- 按一下Add User以完成使用者配置。

等效的CLI命令：

<#root>

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

- 將使用者增加到使用者資料庫後，註冊狀態顯示為Allowed to Enroll。


Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

Manage the users in the user database for Local Certificate Authority Server.

Username	Email	Subject Name	Enrollment Status	Certificate Holder
user1	user1@cisco.com	CN=user1,OU=TAC	allowed	yes

CLI驗證使用者狀態：

<#root>

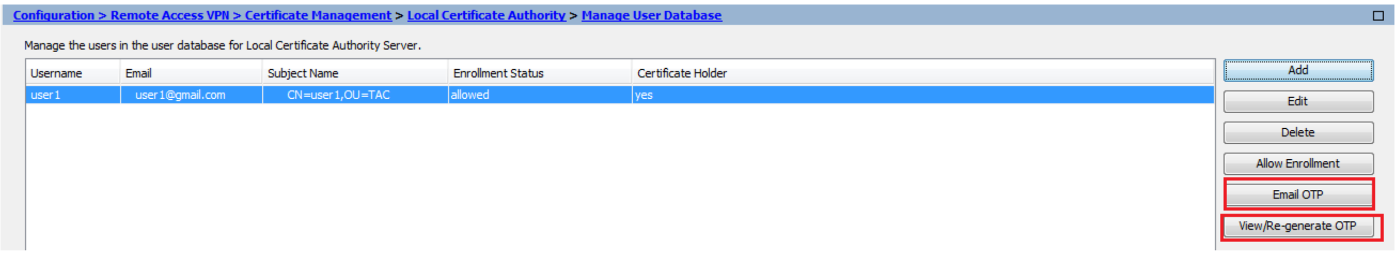
```
ASA# show crypto ca server user-db

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
```

- 將使用者新增至使用者資料庫後，可以使用下列其中一種方式來提供使用者完成註冊的一次性密碼(OTP)：

向OTP傳送電子郵件（需要在CA伺服器配置下配置SMTP伺服器和電子郵件設定）。

或

直接檢視OTP，然後按一下檢視/重新產生OTP，與使用者共用。這也可以用來重新產生OTP。


Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

Manage the users in the user database for Local Certificate Authority Server.

Username	Email	Subject Name	Enrollment Status	Certificate Holder
user1	user1@gmail.com	CN=user1,OU=TAC	allowed	yes

等效的CLI命令：

```
!! Email the OTP to the user
ASA# crypto ca server user-db allow user1 email-otp

!! Display the OTP on terminal
ASA# crypto ca server user-db allow user1 display-otp
Username: user1
OTP: 18D14F39C8F3DD84
Enrollment Allowed Until: 14:18:34 UTC Tue Jan 12 2016
```

步驟 3.在WAN介面上啟用webvpn

- 在ASA上啟用Web訪問，使客戶端能夠請求註冊。

```
!! Enable web-access on the "Internet" interface of the ASA
ASA(config)# webvpn
ASA(config-webvpn)#enable Internet
```

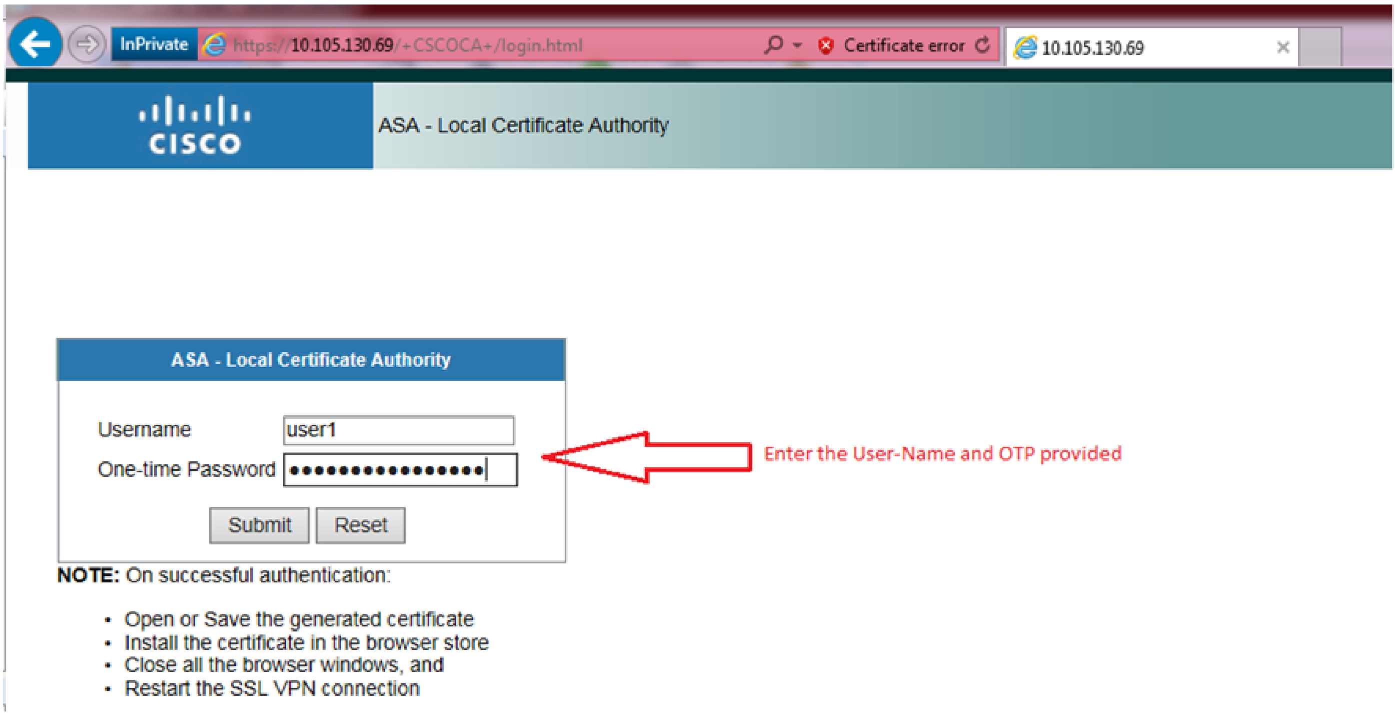
步驟 4.在客戶端電腦上導入證書

- 在客戶端工作站上，打開瀏覽器並導航到連結以完成註冊。
- 此鏈路中使用的IP/FQDN應該是該步驟中已啟用webvpn的介面的IP，即介面Internet。

<#root>

```
https://

         <>

          IP/FQDN>/+CSCOCA+/enroll.html

         <>
```

- 輸入使用者名稱(在ASA上的第2步（選項A）下配置)和OTP(透過郵件或手動提供)。



InPrivate
https://10.105.130.69/+CSCOCA+/login.html
Certificate error
10.105.130.69
cisco

ASA - Local Certificate Authority

ASA - Local Certificate Authority

Username: user1

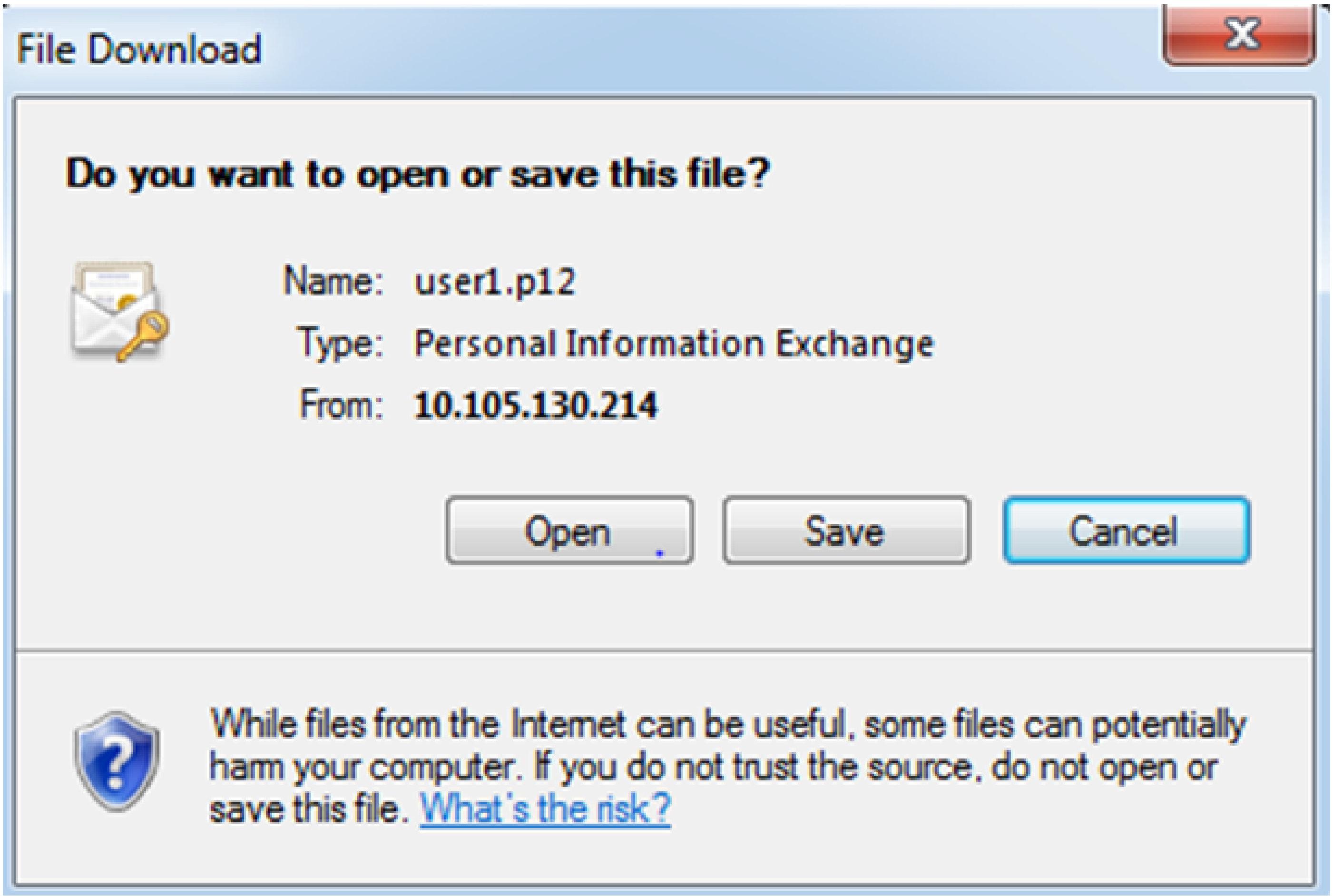
One-time Password: ●●●●●●●●●●●●●●●●

Submit
Reset
Enter the User-Name and OTP provided

NOTE: On successful authentication:

- Open or Save the generated certificate
- Install the certificate in the browser store
- Close all the browser windows, and
- Restart the SSL VPN connection

- 按一下Open以直接安裝從ASA接收的客戶端證書。
- 安裝使用者端憑證的密碼與之前收到的OTP相同。



File Download

Do you want to open or save this file?

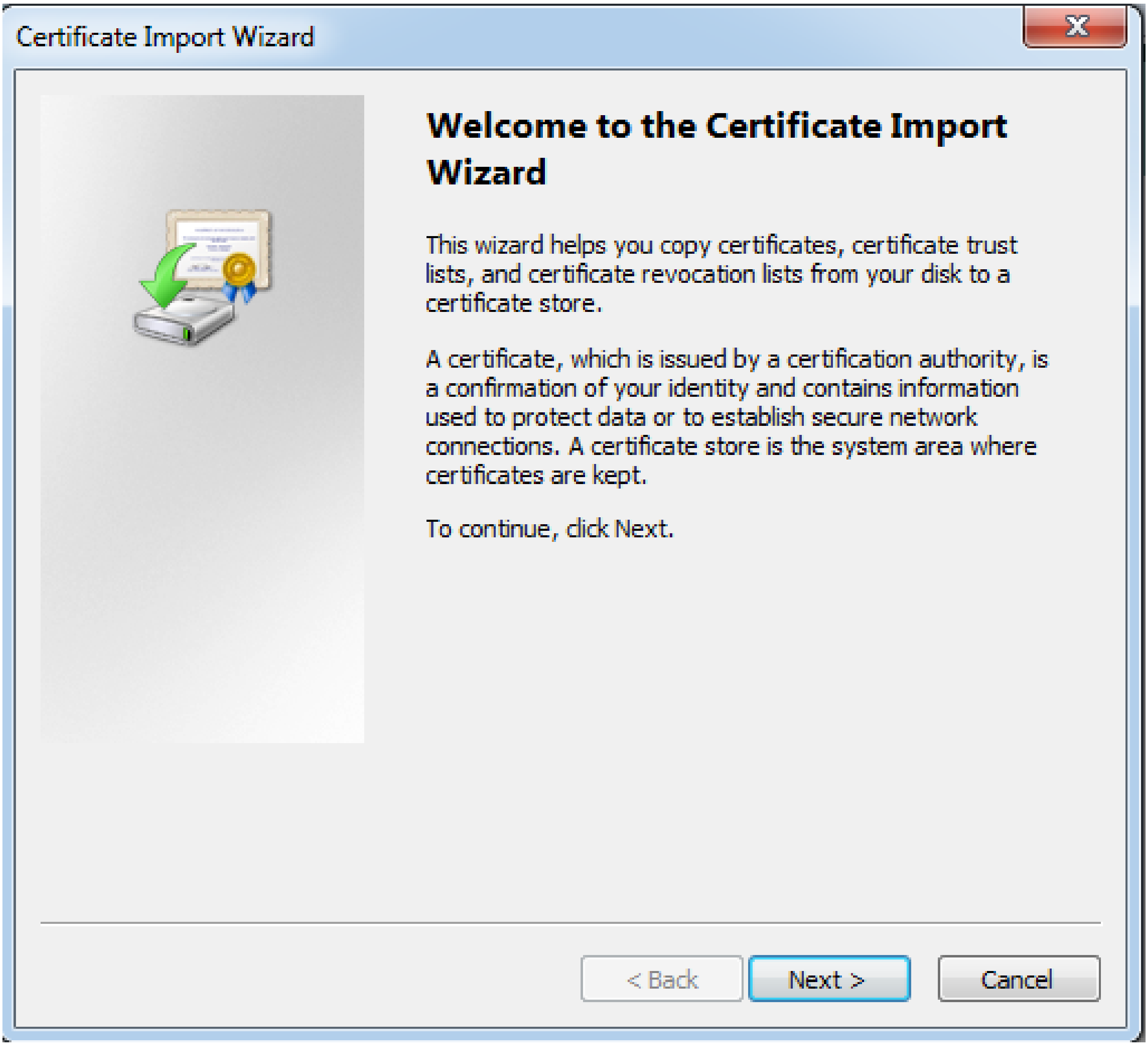
Name: user1.p12

Type: Personal Information Exchange

From: 10.105.130.214

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

- 按「Next」（下一步）。



Certificate Import Wizard

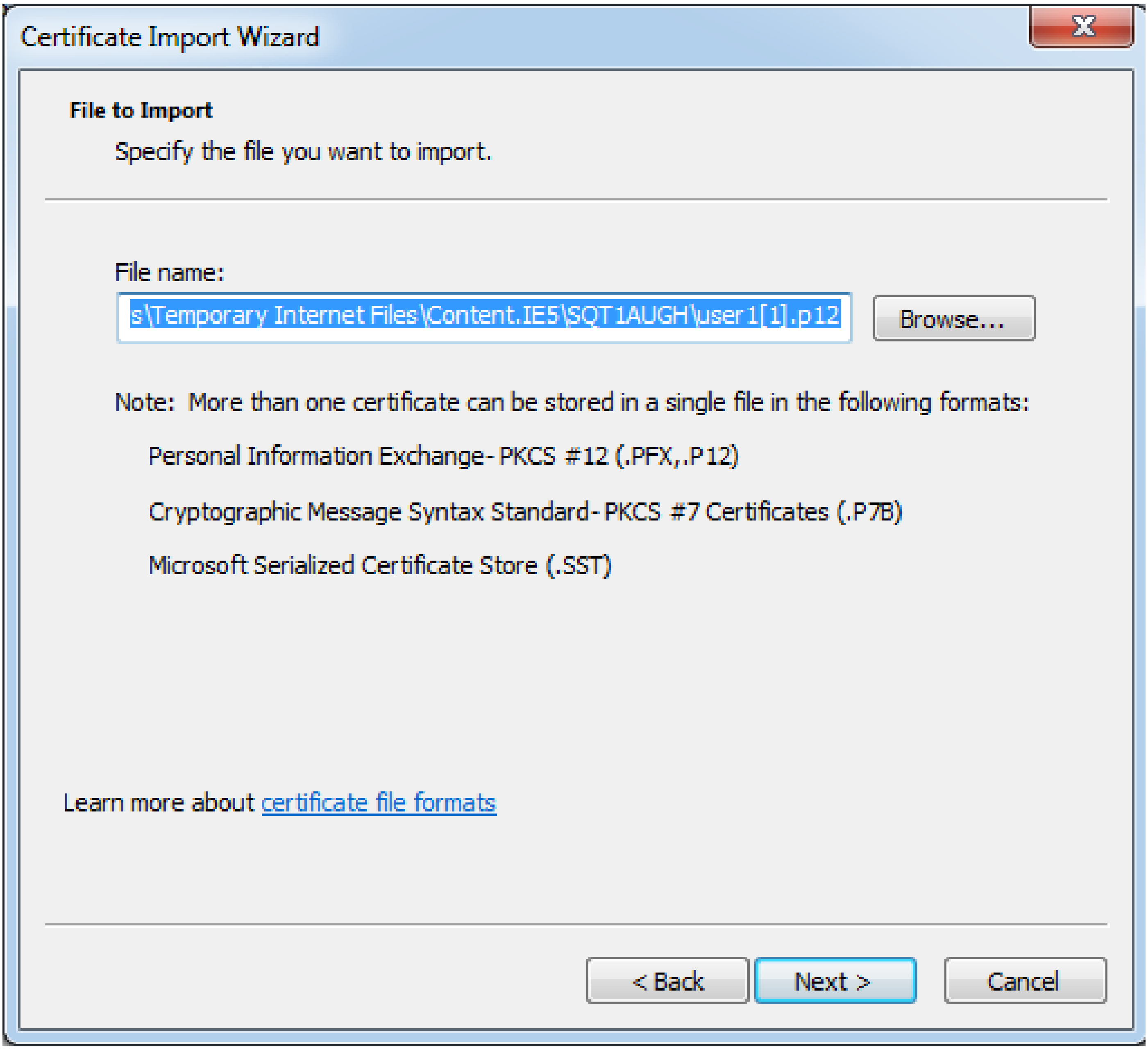
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

- 保留預設路徑並按一下Next。



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

s\Temporary Internet Files\Content.IE5\SQT1AUGH\user1[1].p12

Note: More than one certificate can be stored in a single file in the following formats:

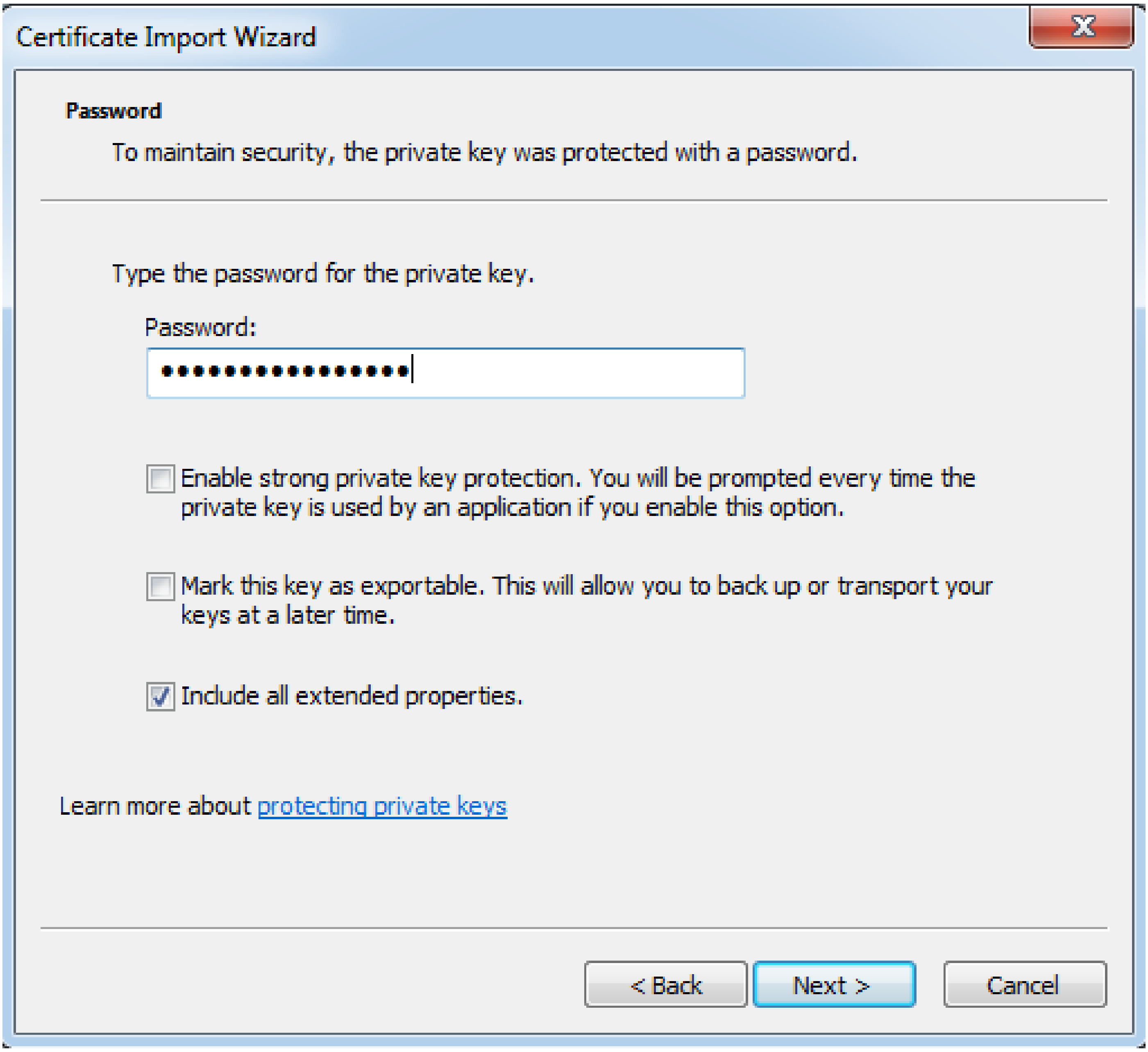
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

- 在「密碼」欄位中輸入OTP。
- 您可以選擇Mark this key as exportable選項，以便將來需要時可從工作站中導出金鑰。
- 按一下下一步



Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

●●●●●●●●●●●●●●●●

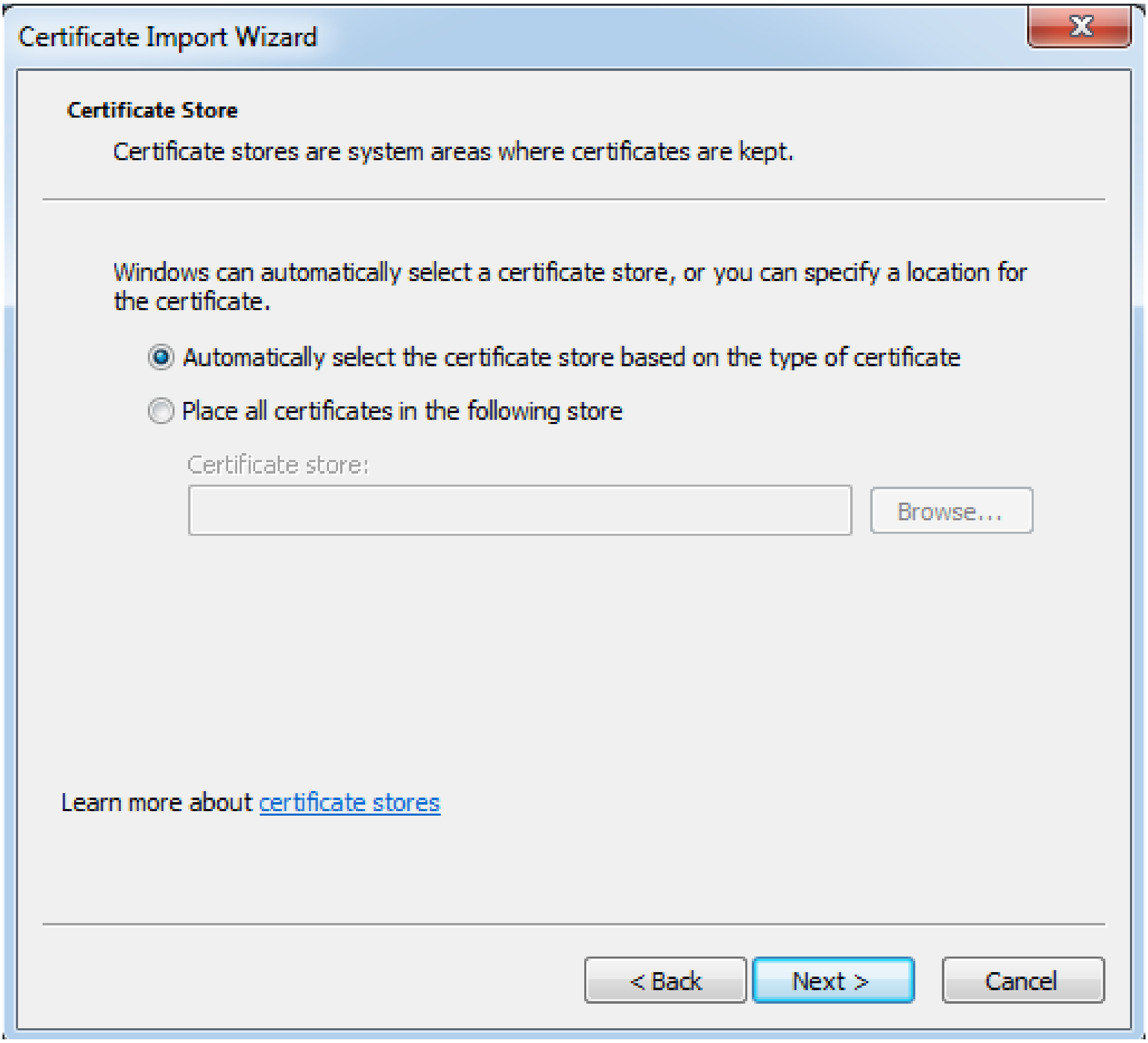
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

- 您可以手動將憑證安裝在特定憑證存放區，或讓其自動選擇存放區。
- 按「Next」（下一步）。



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

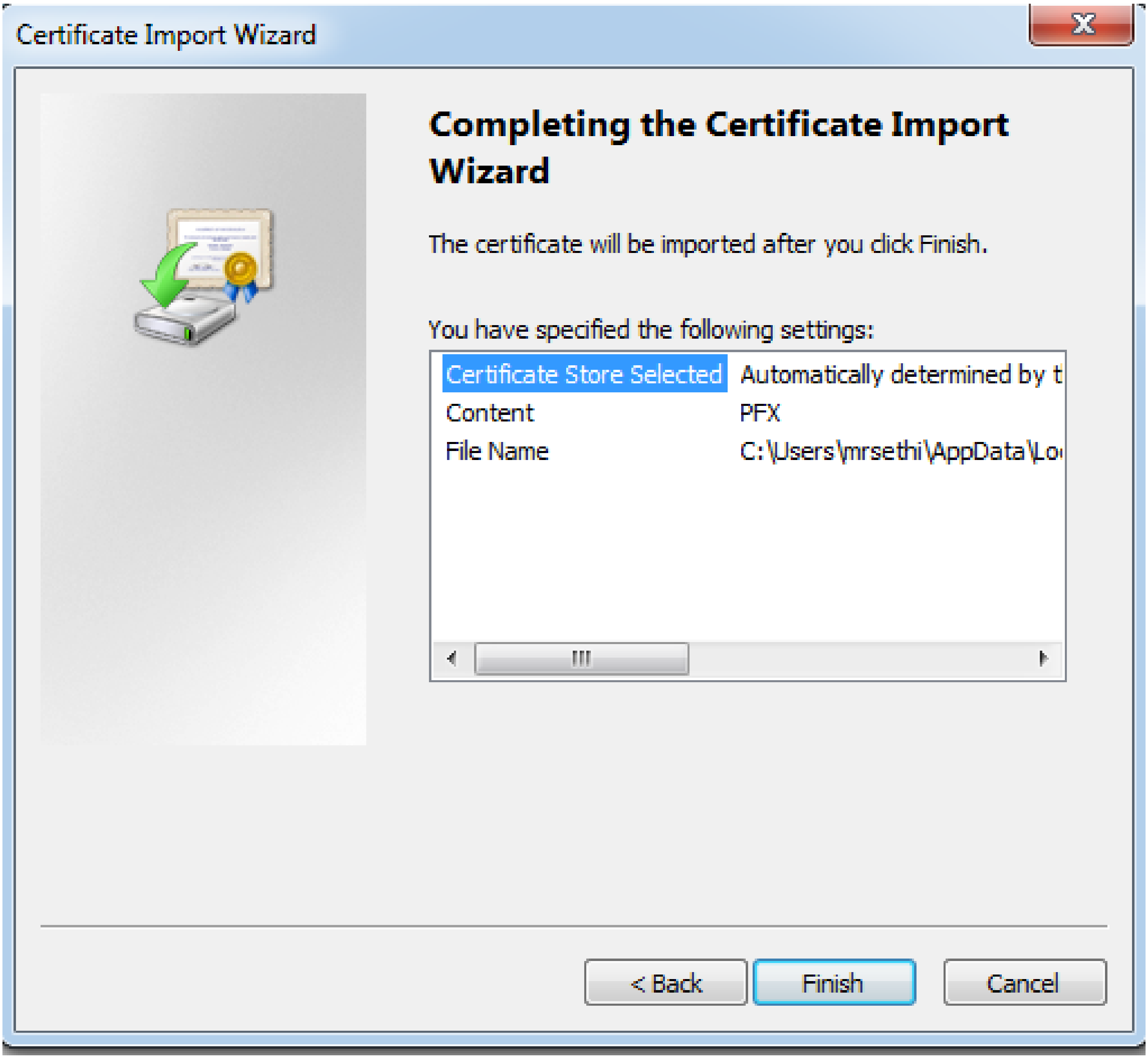
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Learn more about certificate stores

- 按一下完成以完成安裝。

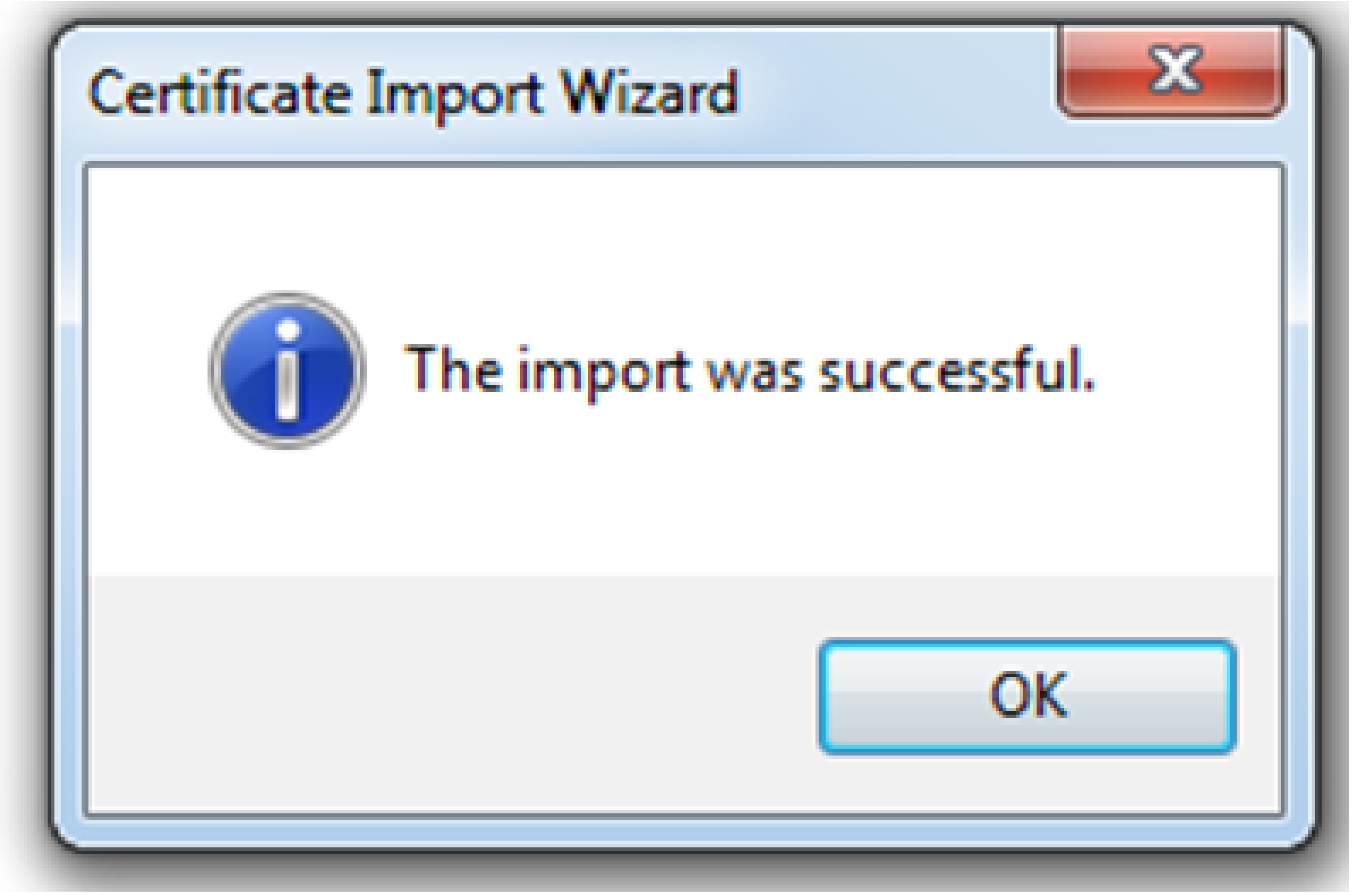


Completing the Certificate Import Wizard

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

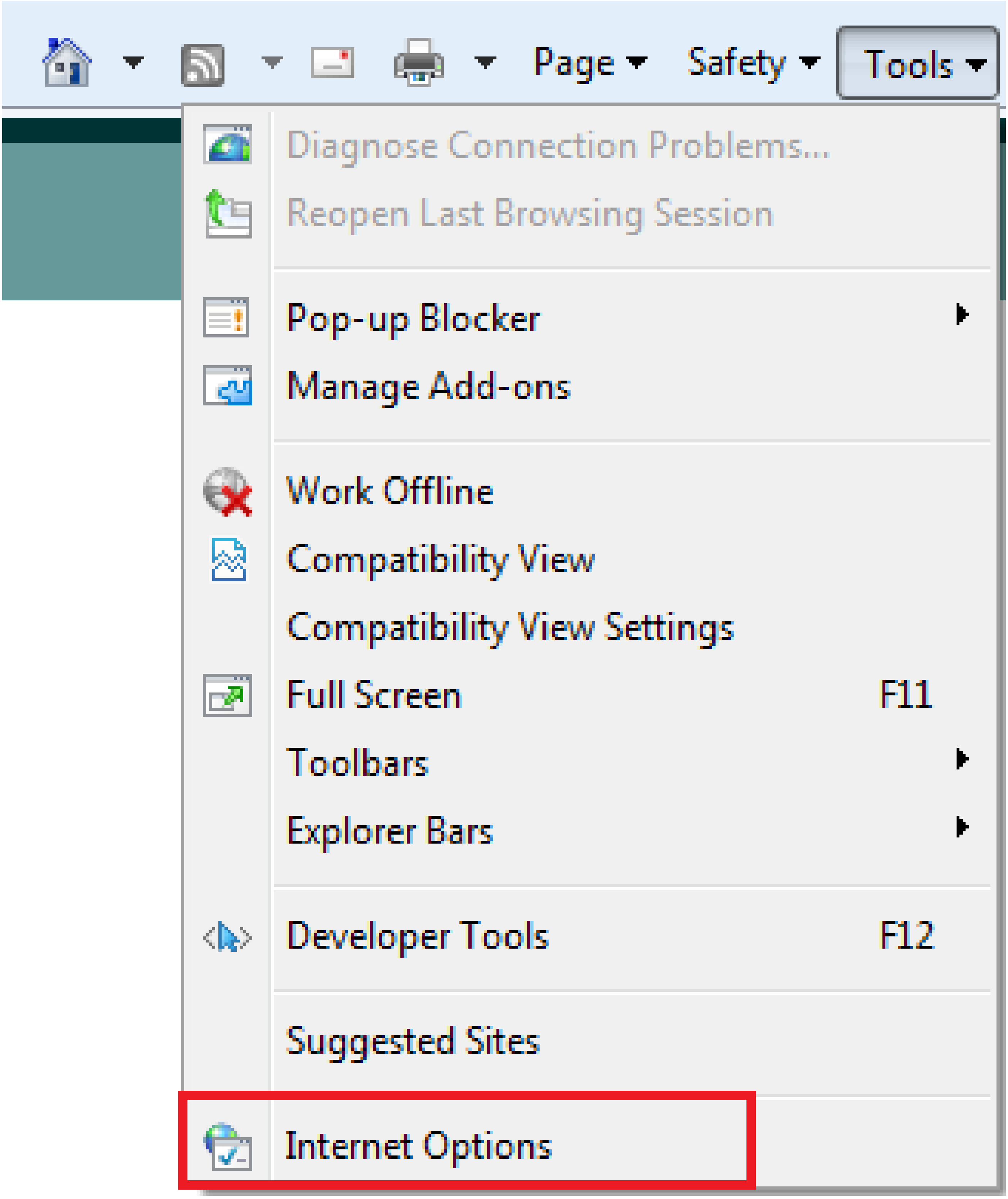


Certificate Import Wizard

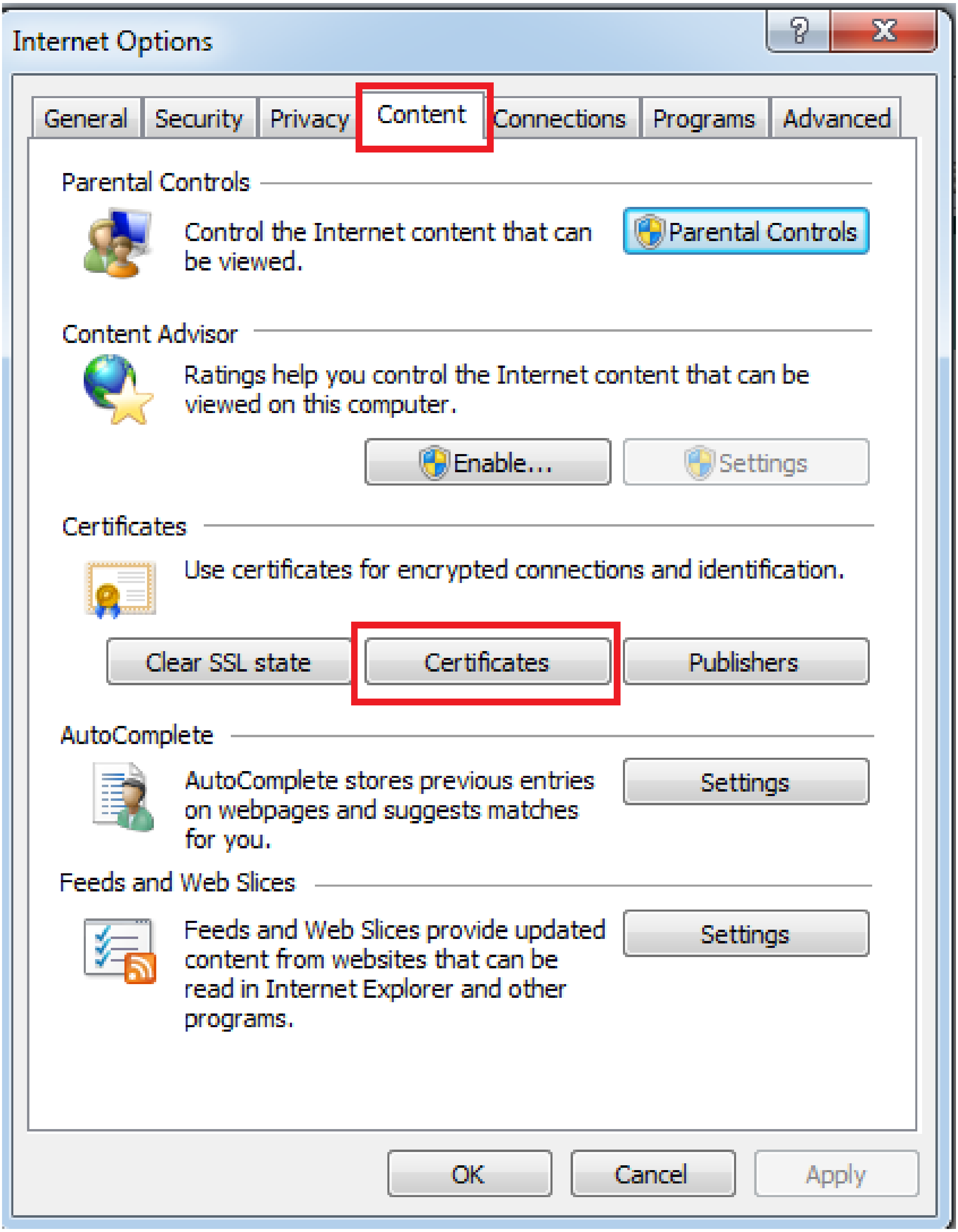
The import was successful.

- 成功安裝憑證後，您就可以進行驗證。
- 打開IE並導航到工具> Internet選項。

- 導覽至內容索引標籤，然後按一下Certificates，如下圖所示。

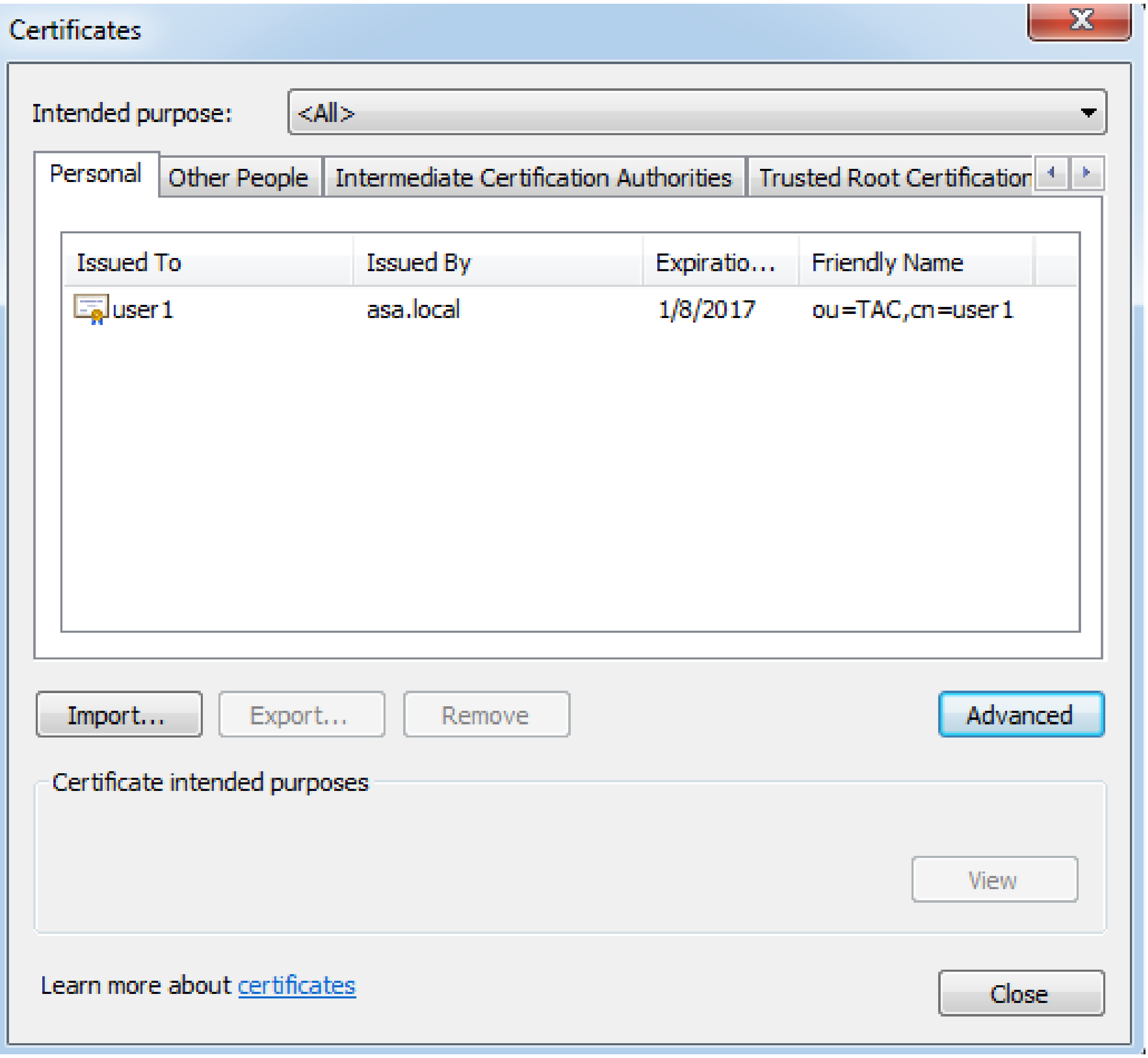


- 導覽至內容索引標籤，然後按一下Certificates，如下圖所示。



Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Parental Controls
Control the Internet content that can be viewed.
Parental Controls
Content Advisor
Ratings help you control the Internet content that can be viewed on this computer.
Enable...
Settings
Certificates
Use certificates for encrypted connections and identification.
Clear SSL state
Certificates
Publishers
AutoComplete
AutoComplete stores previous entries on webpages and suggests matches for you.
Settings
Feeds and Web Slices
Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.
Settings
OK
Cancel
Apply

- 在個人儲存下，您可以看到從ASA收到的證書。


Certificates
Intended purpose: <All>
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Learn more about certificates
Close

Issued To	Issued By	Expiratio...	Friendly Name
user1	asa.local	1/8/2017	ou=TAC,cn=user1

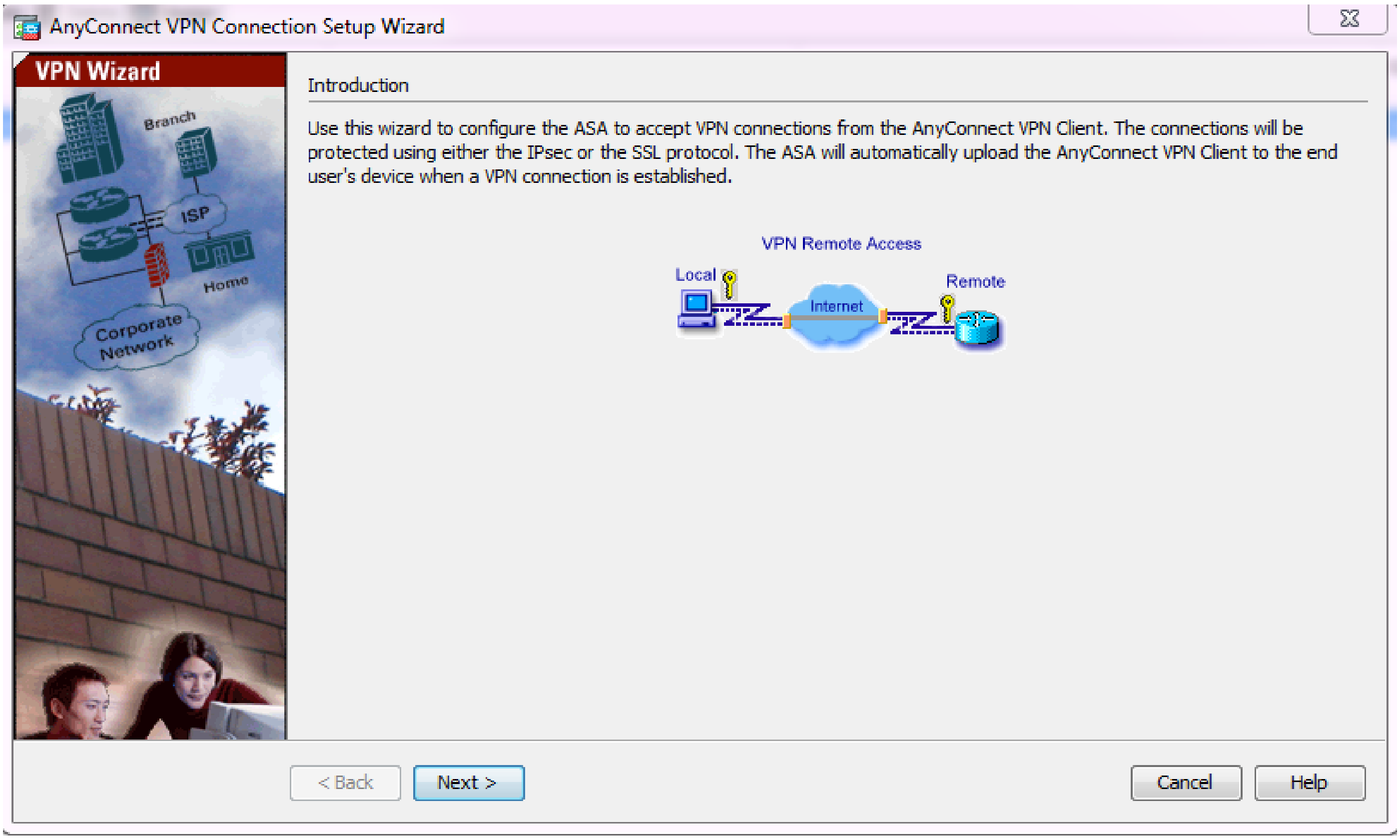
ASA作為AnyConnect客戶端的SSL網關

ASDM AnyConnect配置嚮導

AnyConnect配置嚮導/CLI可用於配置AnyConnect安全移動客戶端。在繼續操作之前，請確保已將AnyConnect客戶端軟體套件上傳到ASA防火牆的快閃記憶體/磁碟。

要透過配置嚮導配置AnyConnect安全移動客戶端，請完成以下步驟：

1. 登入ASDM並導航到嚮導> VPN嚮導> AnyConnect VPN嚮導啟動配置嚮導，然後按一下下一步。



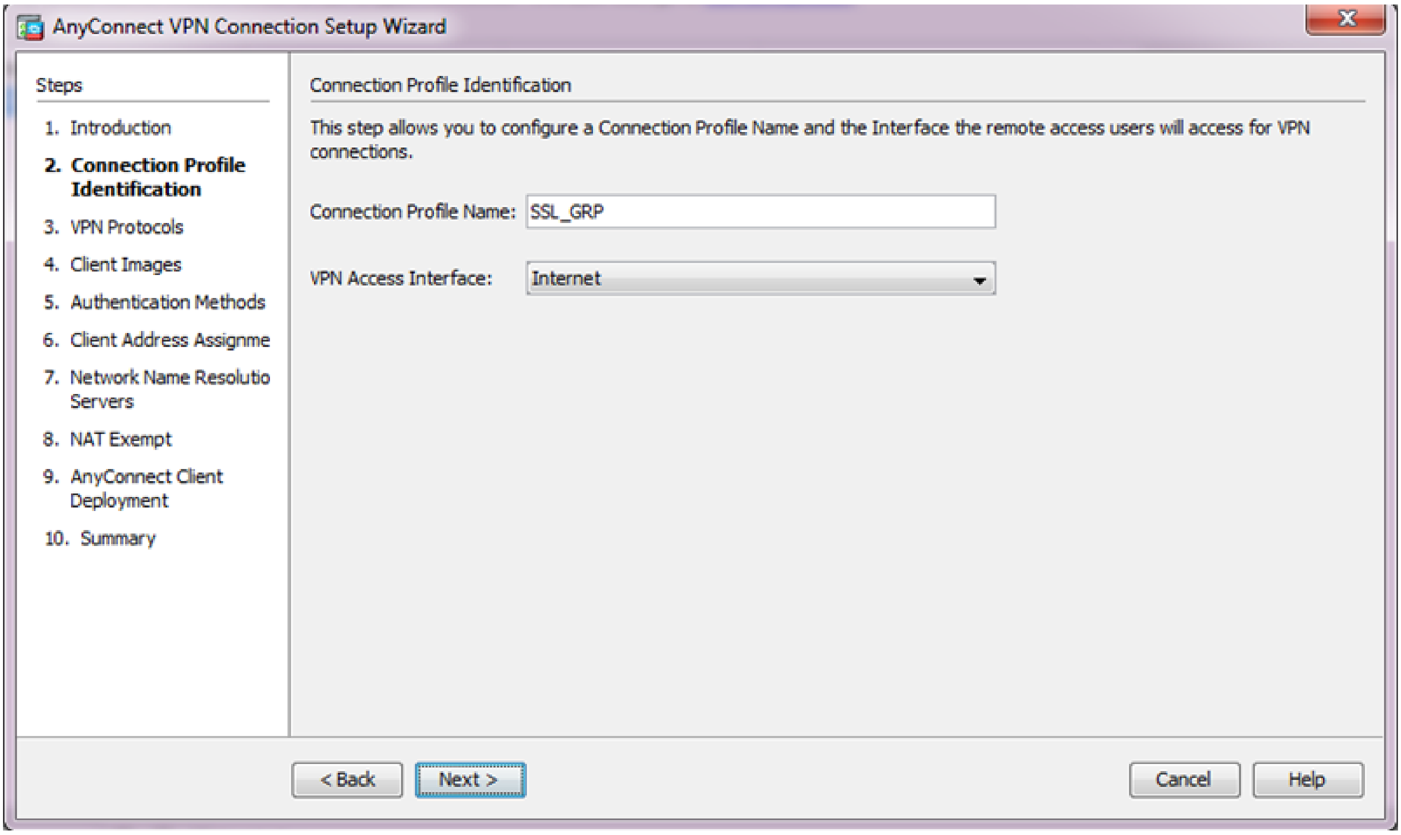
AnyConnect VPN Connection Setup Wizard

VPN Wizard

Introduction

Use this wizard to configure the ASA to accept VPN connections from the AnyConnect VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the AnyConnect VPN Client to the end user's device when a VPN connection is established.

2. 輸入連線配置檔名稱，從VPN Access Interface下拉選單中選擇要終止VPN的介面，然後按一下Next。



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. **Connection Profile Identification**
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Connection Profile Identification

This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.

Connection Profile Name: SSL_GRP

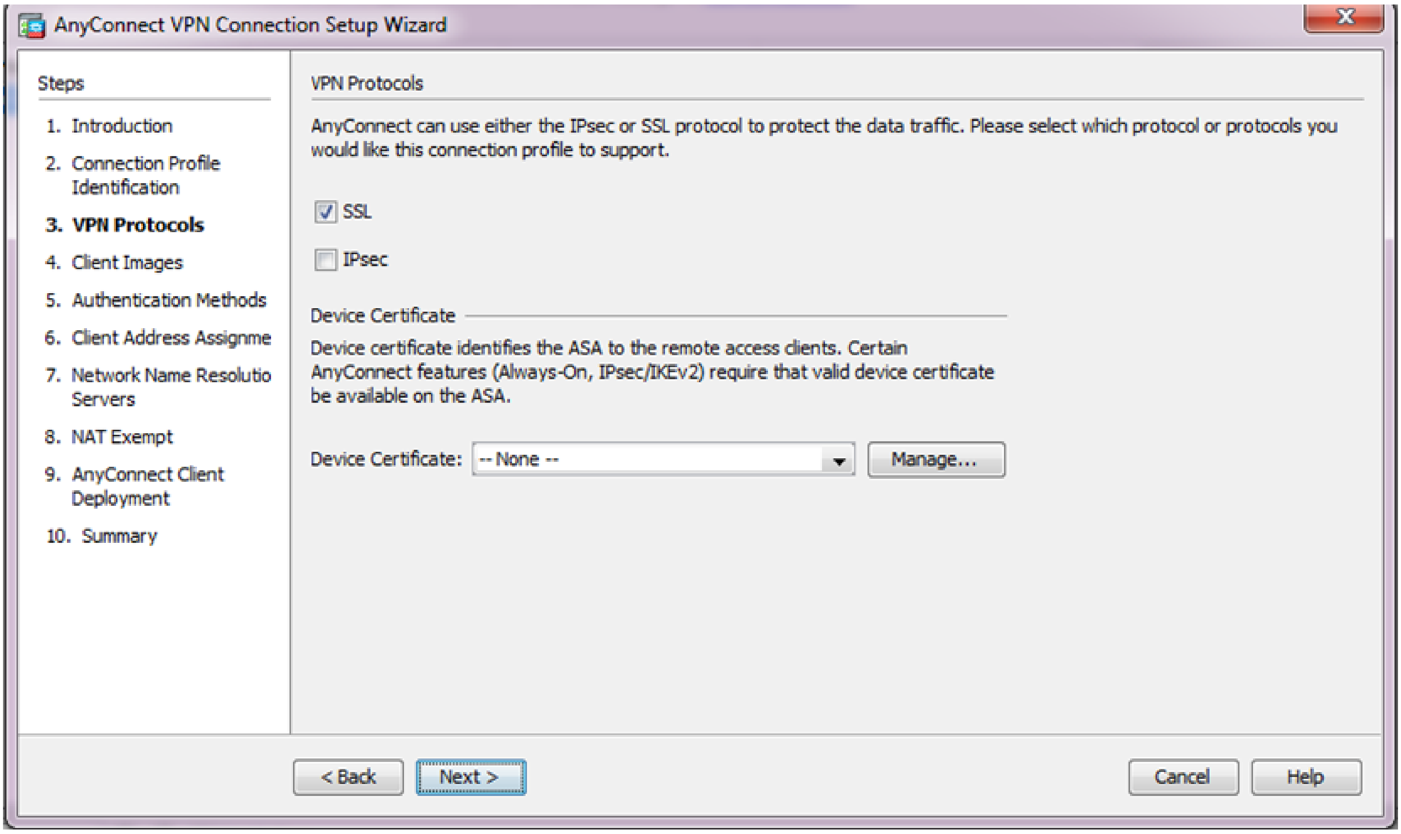
VPN Access Interface: Internet

3. 選中SSL覈取方塊以啟用Secure Sockets Layer (SSL)。裝置證書可以是受信任的第三方證書頒發機構(CA)頒發的證書（例如Verisign或Entrust），也可以是自簽名證書。如果證書已安裝在ASA上，則可透過下拉選單選擇證書。

1. 注意：此證書是ASA向SSL客戶端提供的伺服器端證書。如果ASA上當前未安裝任何必須生成自簽名證書的伺服器證書，請按一下Manage。

要安裝第三方證書，請完成ASA 8.x手動安裝第三方供應商證書以用於WebVPN配置示例思科文檔中所述的步驟。

- 啟用VPN協定和裝置證書。
- 按「Next」（下一步）。


AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. **VPN Protocols**
4. Client Images
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

VPN Protocols

AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.

☑ SSL

□ IPsec

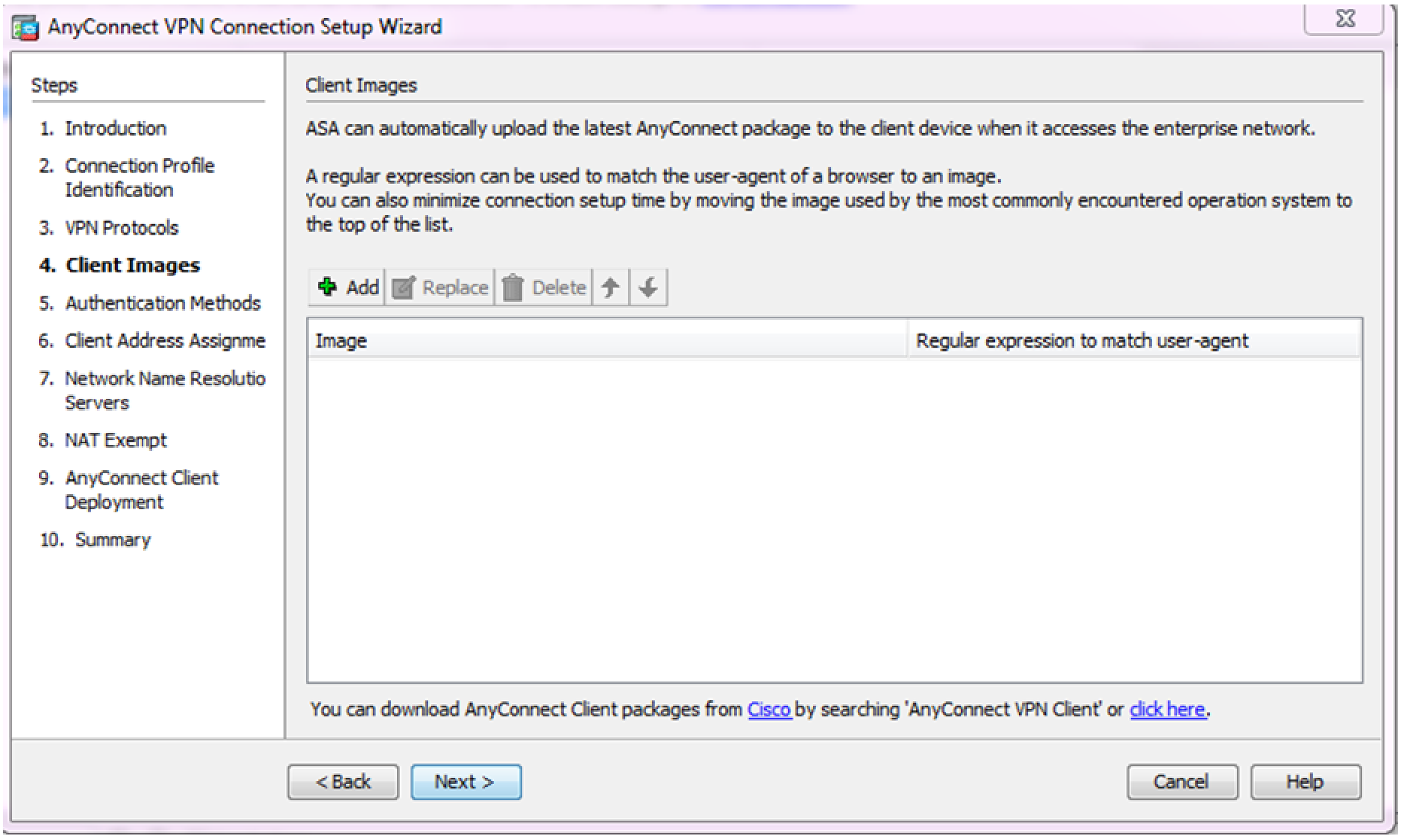
Device Certificate

Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

Device Certificate: -- None --

4. 按一下Add以便從本地驅動器或ASA快閃記憶體/磁碟中增加AnyConnect客戶端軟體套件（.pkg檔案）。

按一下Browse Flash以從快閃記憶體驅動器增加映像，或按一下Upload以從主機的本地驅動器增加映像。



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. **Client Images**
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Client Images

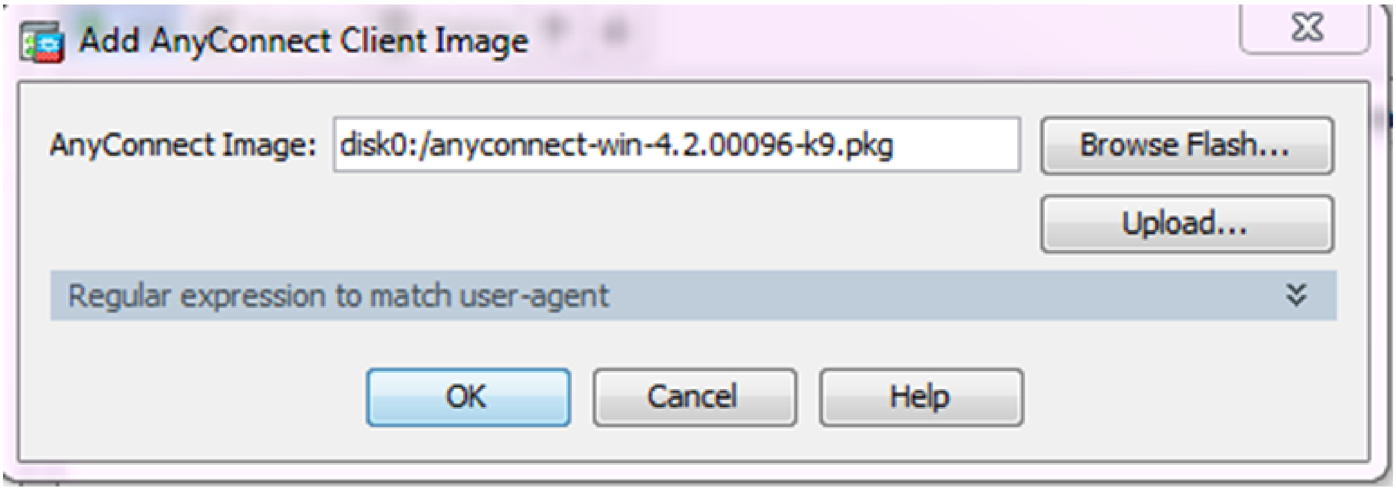
ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.

A regular expression can be used to match the user-agent of a browser to an image.
You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent

You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or click here.

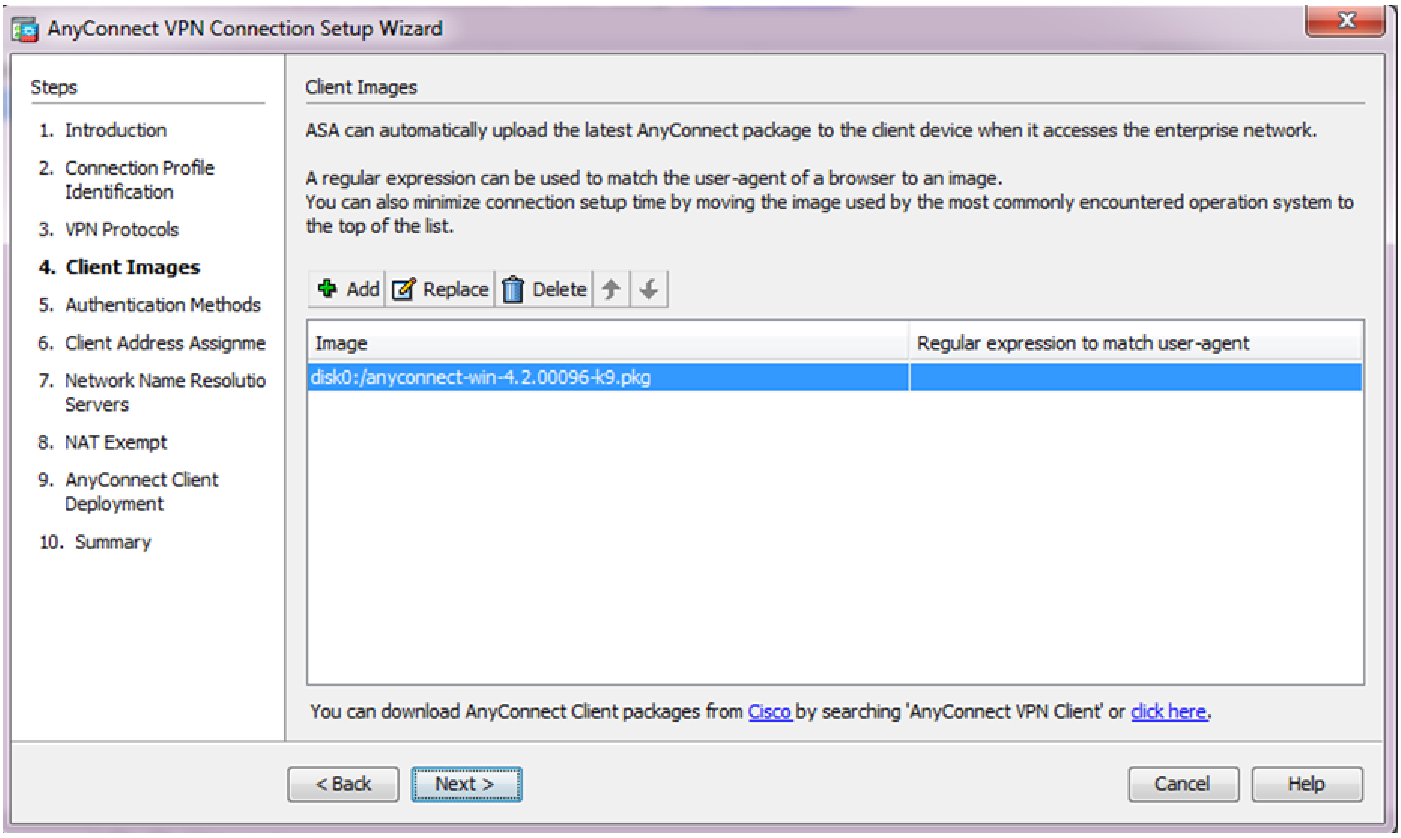
- 您可以從ASA快閃記憶體/磁碟（如果軟體套件已存在）或從本地驅動器上傳AnyConnect.pkg檔案。
- 瀏覽快閃記憶體-從ASA快閃記憶體/磁碟中選擇AnyConnect軟體套件。
- 上傳-從主機的本地驅動器中選擇AnyConnect軟體套件。
- 按一下「OK」（確定）。



Add AnyConnect Client Image

AnyConnect Image: disk0:/anyconnect-win-4.2.00096-k9.pkg

- 按「Next」（下一步）。



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. **Client Images**
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Client Images

ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.

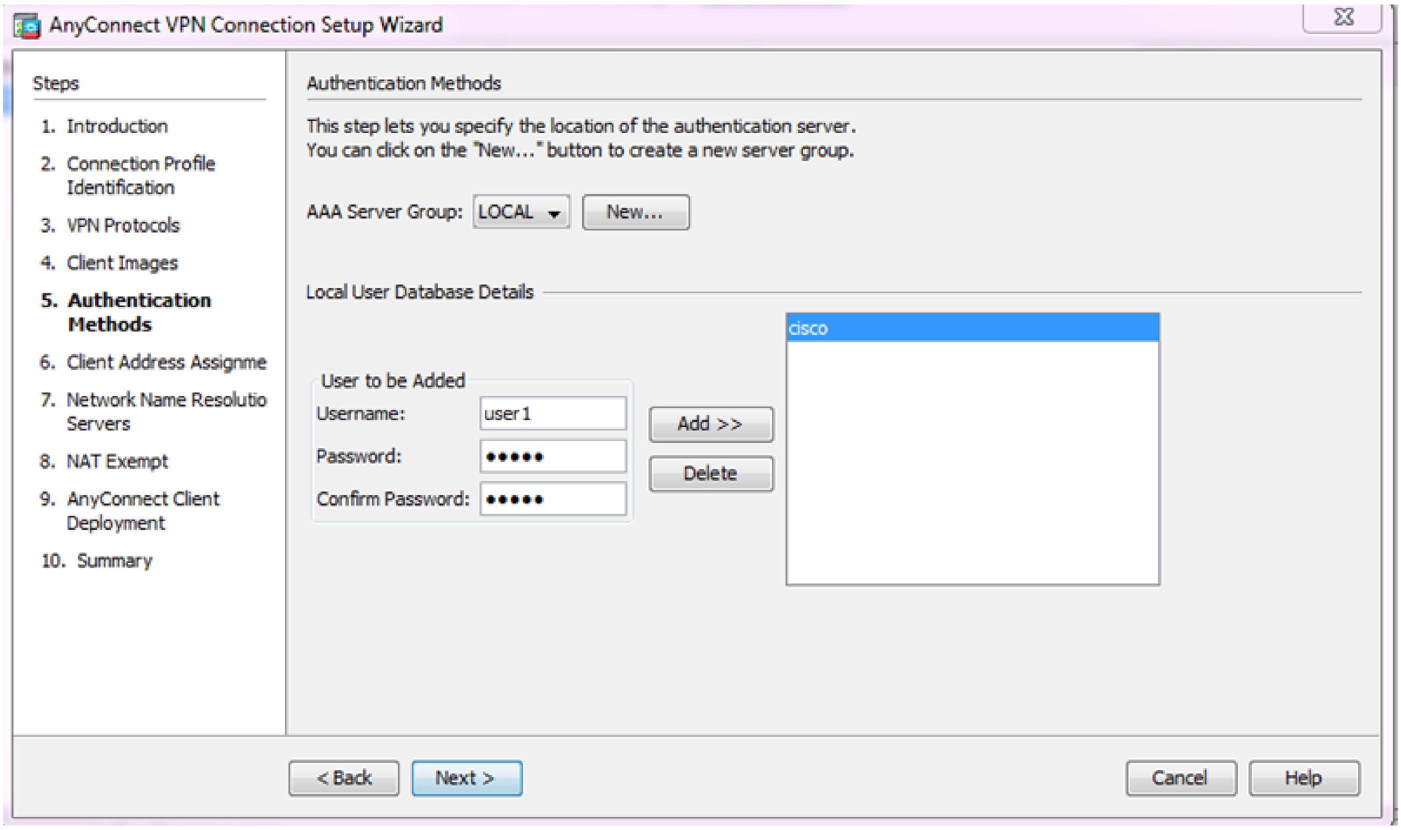
A regular expression can be used to match the user-agent of a browser to an image.
You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent
disk0:/anyconnect-win-4.2.00096-k9.pkg	

You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or click here.

5.　使用者身份驗證可以透過「身份驗證」、「授權」和「記帳」(AAA)伺服器組完成。如果已配置使用者，請選擇LOCAL，然後按一下Next。否則，請將使用者增加到本地使用者資料庫，然後按一下Next。

注意：在本示例中，配置了LOCAL身份驗證，這意味著將使用ASA上的本地使用者資料庫進行身份驗證。



AnyConnect VPN Connection Setup Wizard

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. **Authentication Methods**
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Authentication Methods

This step lets you specify the location of the authentication server.
You can click on the "New..." button to create a new server group.

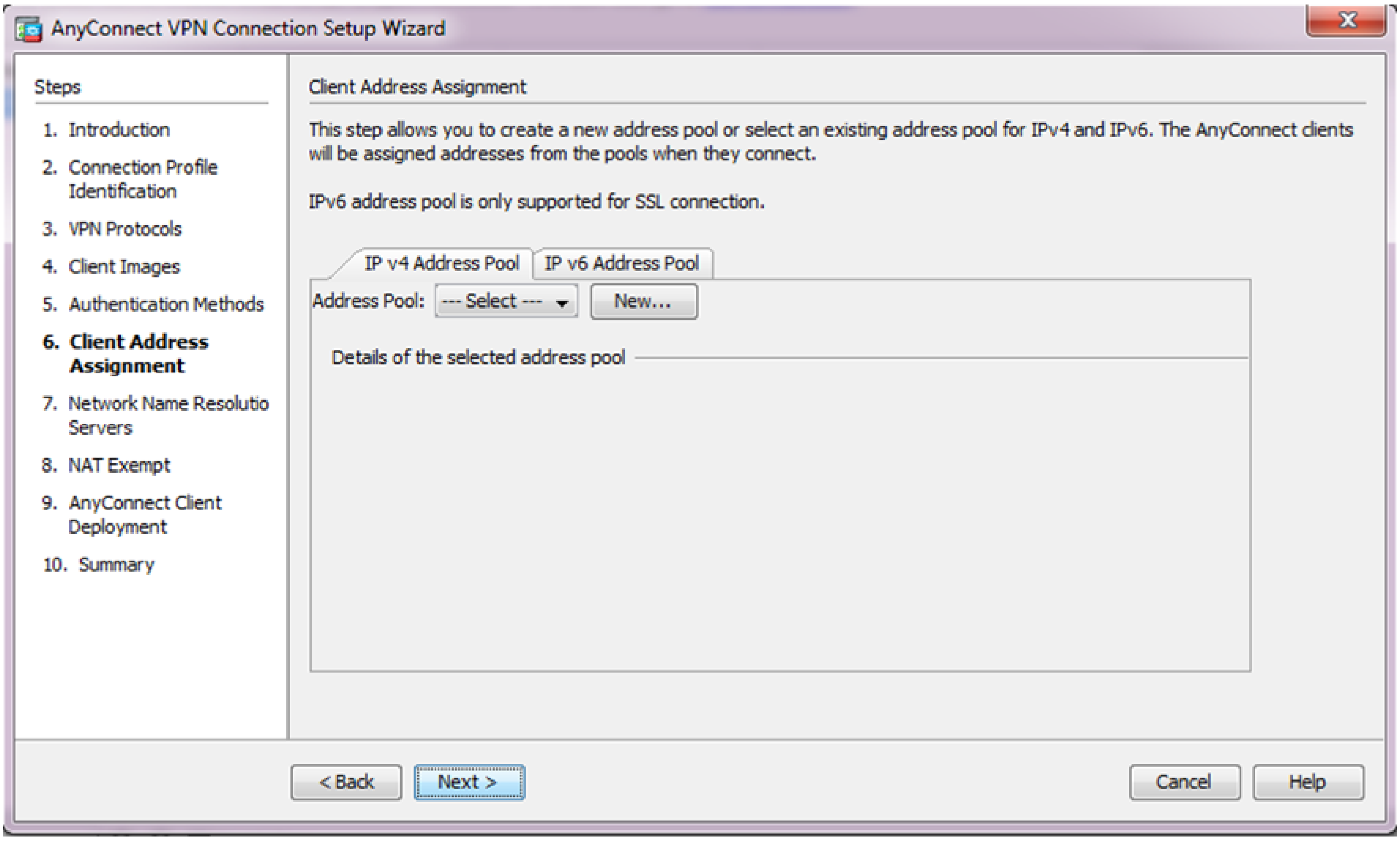
AAA Server Group: LOCAL

Local User Database Details

User to be Added
Username: user1
Password: •••••
Confirm Password: •••••

cisco

6. 確保已配置VPN客戶端的地址池。如果已經配置了ip池，請從下拉選單中選擇該池。否則，請按一下新建以進行配置。完成後，按一下Next。



AnyConnect VPN Connection Setup Wizard

Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. **Client Address Assignment**
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

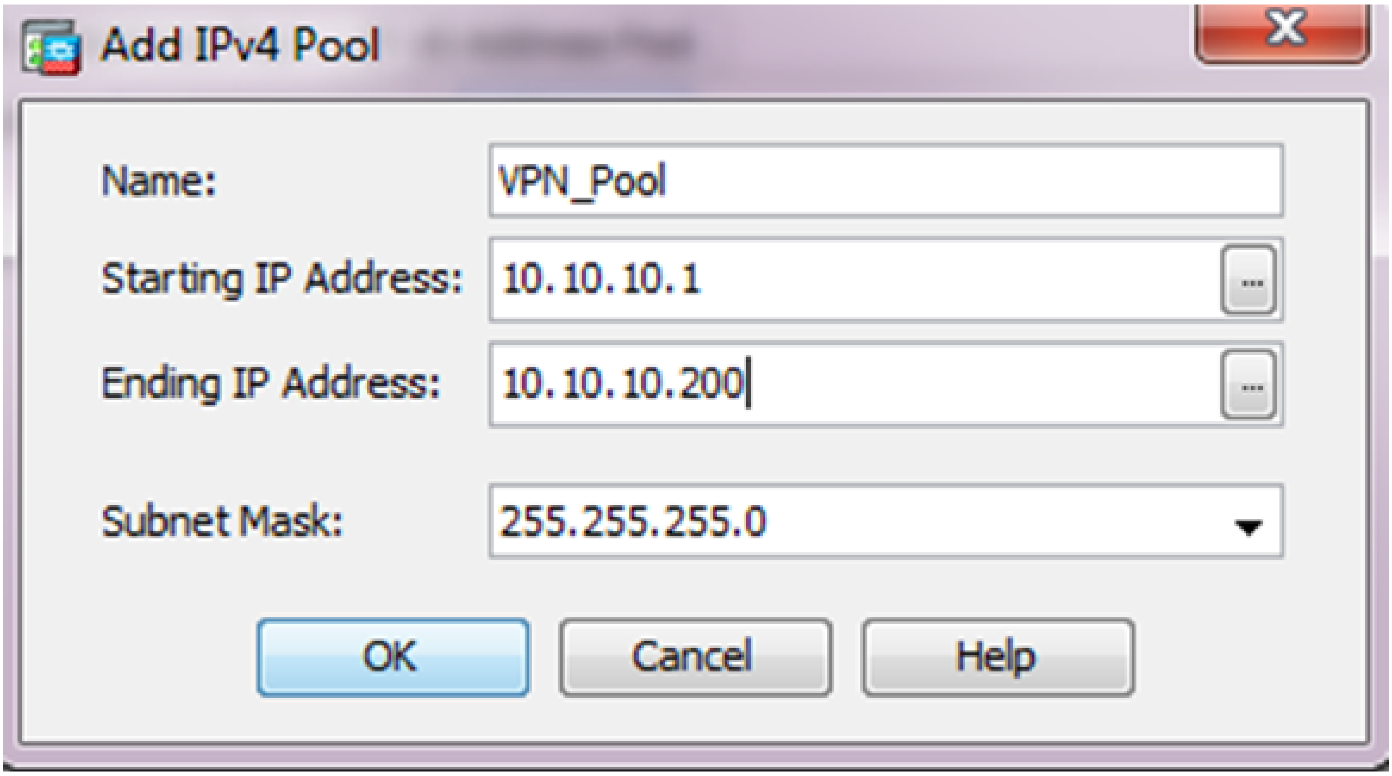
Client Address Assignment

This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

Address Pool: --- Select ---

Details of the selected address pool


Add IPv4 Pool

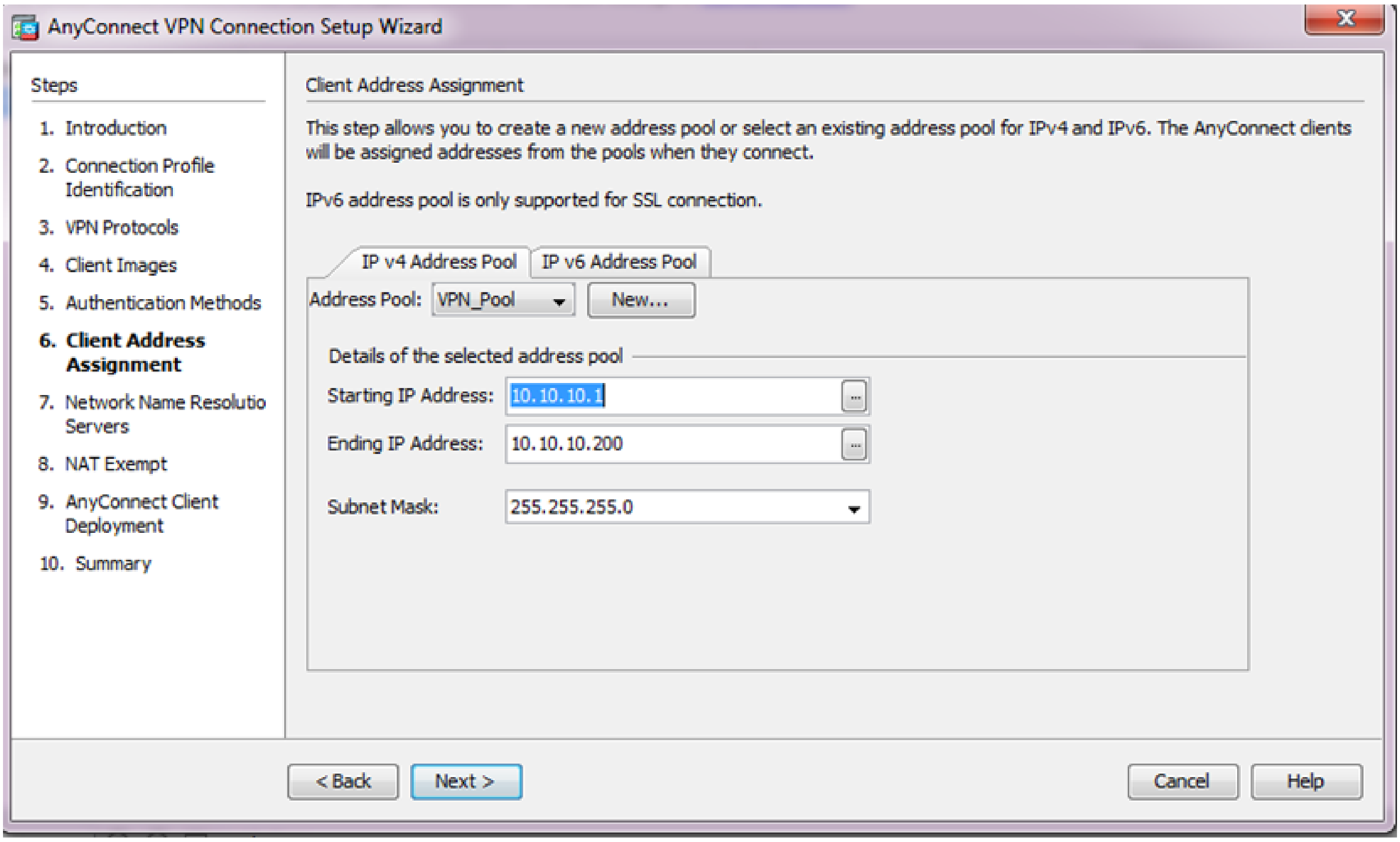
Name: VPN_Pool

Starting IP Address: 10.10.10.1

Ending IP Address: 10.10.10.200

Subnet Mask: 255.255.255.0

- 按「Next」（下一步）。


AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. **Client Address Assignment**
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Client Address Assignment

This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

IP v4 Address Pool | IP v6 Address Pool

Address Pool: VPN_Pool

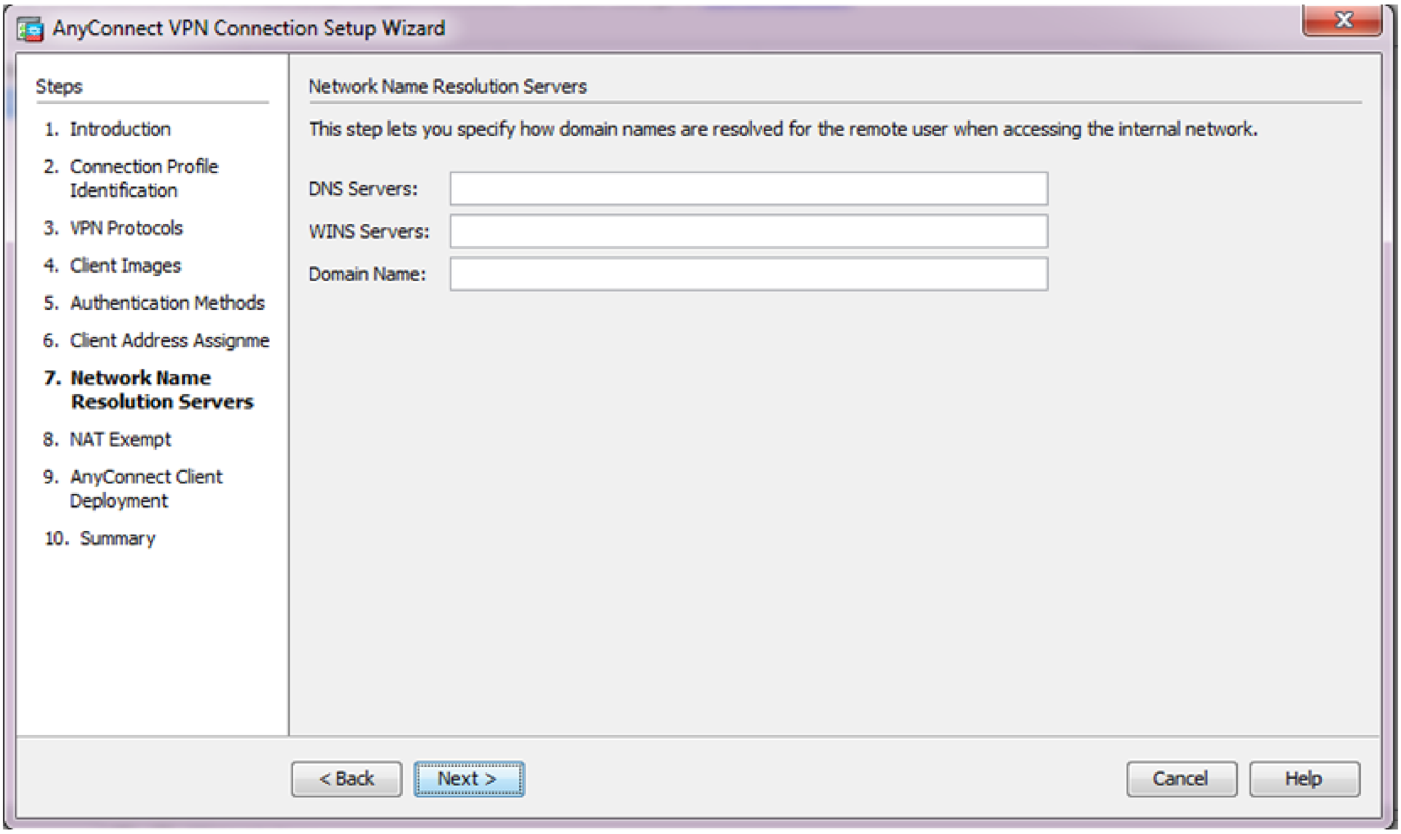
Details of the selected address pool

Starting IP Address: 10.10.10.1

Ending IP Address: 10.10.10.200

Subnet Mask: 255.255.255.0

7. 選擇性地在DNS和「域名」欄位中配置域名系統(DNS)伺服器和DN，然後按一下下一步。


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolution Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

Network Name Resolution Servers

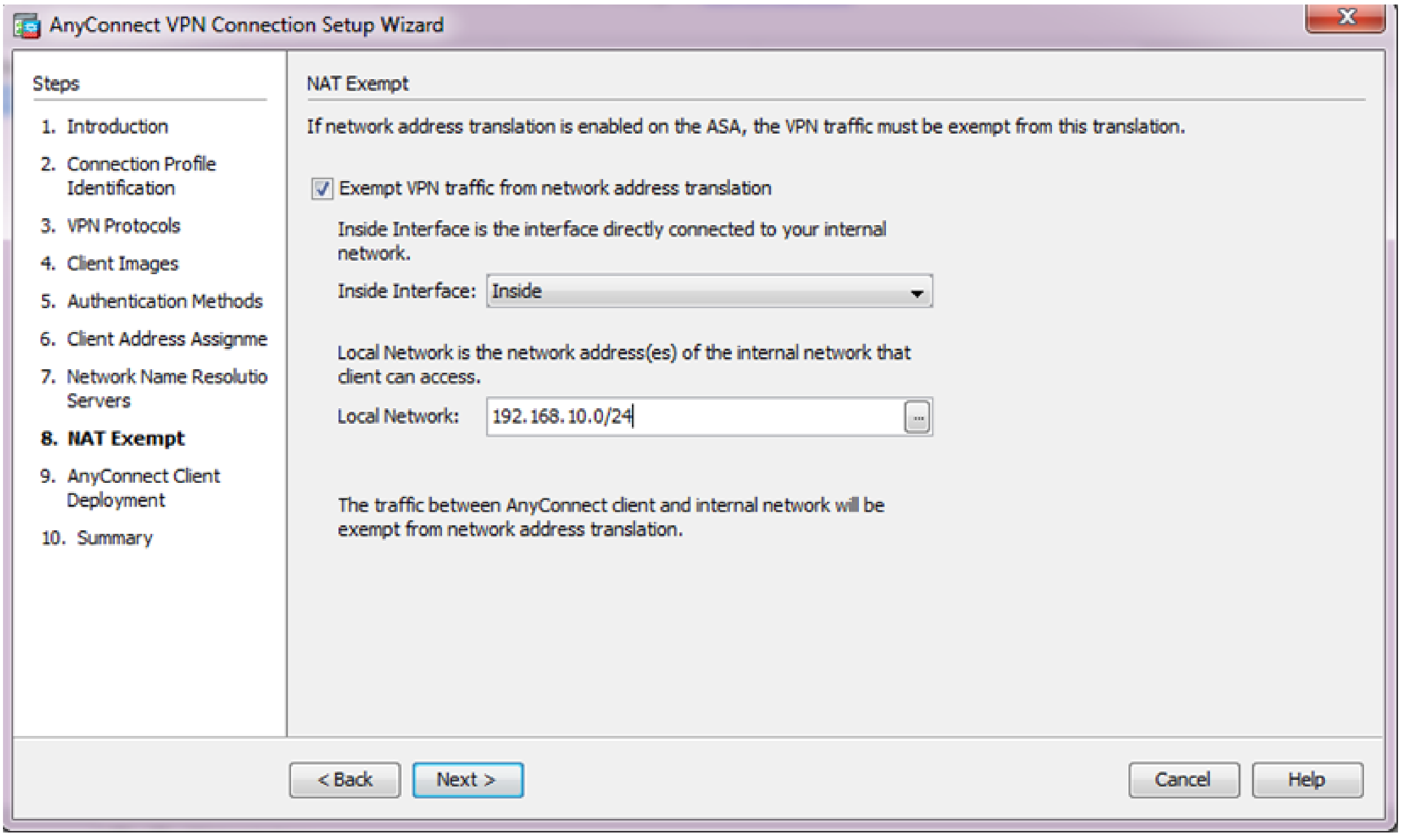
This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers:

WINS Servers:

Domain Name:

8.　確保客戶端和內部子網之間的流量必須免除任何動態網路地址轉換(NAT)。啟用Exempt　VPN traffic from network address translation覈取方塊並配置用於免除的LAN介面。此外，請指定必須免除的本地網路，然後按一下下一步。


AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

NAT Exempt

If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

☑ Exempt VPN traffic from network address translation

Inside Interface is the interface directly connected to your internal network.

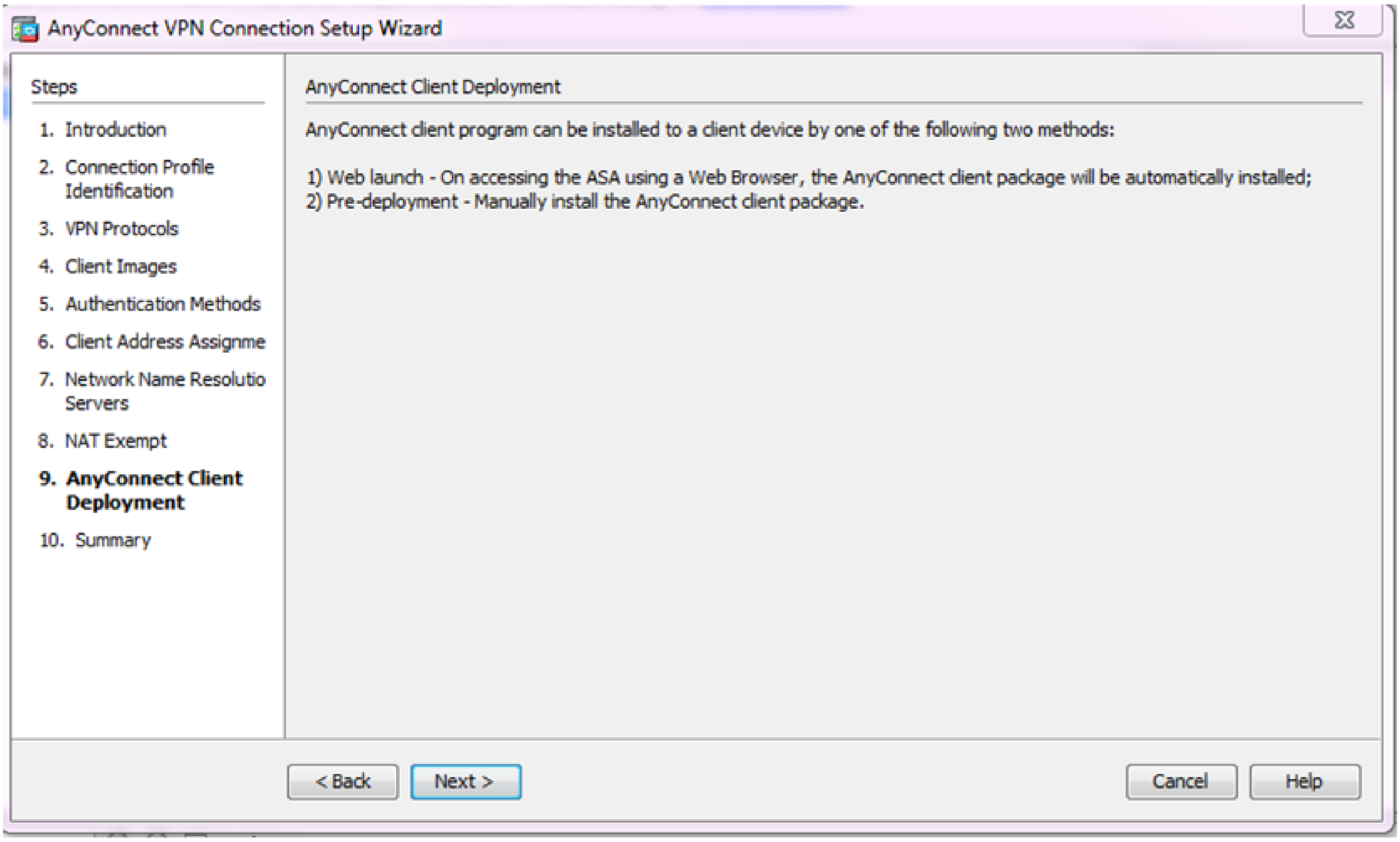
Inside Interface: Inside

Local Network is the network address(es) of the internal network that client can access.

Local Network: 192.168.10.0/24

The traffic between AnyConnect client and internal network will be exempt from network address translation.

9. 按一下下一步。



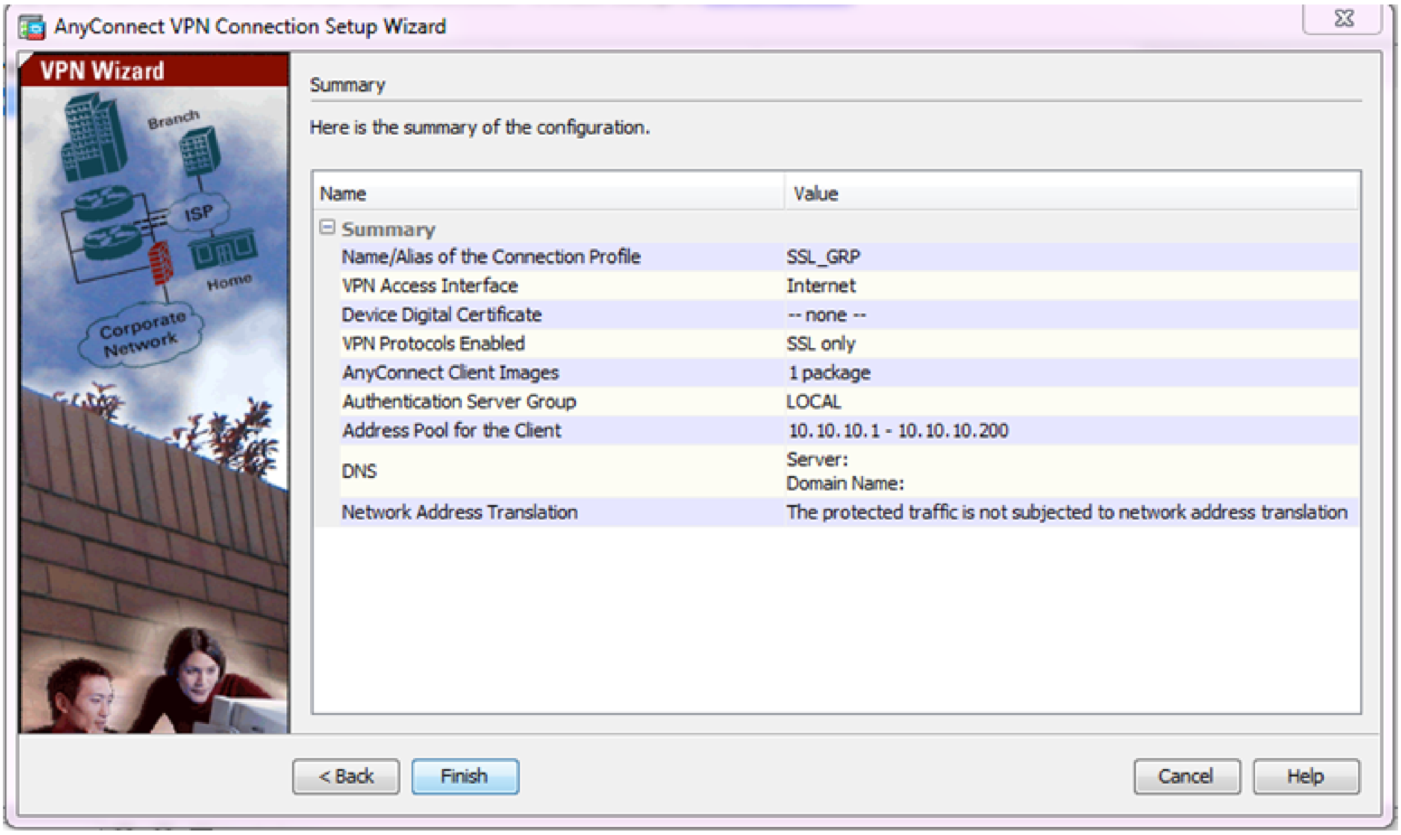
AnyConnect VPN Connection Setup Wizard
Steps
1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary
< Back
Next >
Cancel
Help

AnyConnect Client Deployment

AnyConnect client program can be installed to a client device by one of the following two methods:

1) Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed;
2) Pre-deployment - Manually install the AnyConnect client package.

10. 最後一個步驟顯示彙總，按一下完成完成設定。



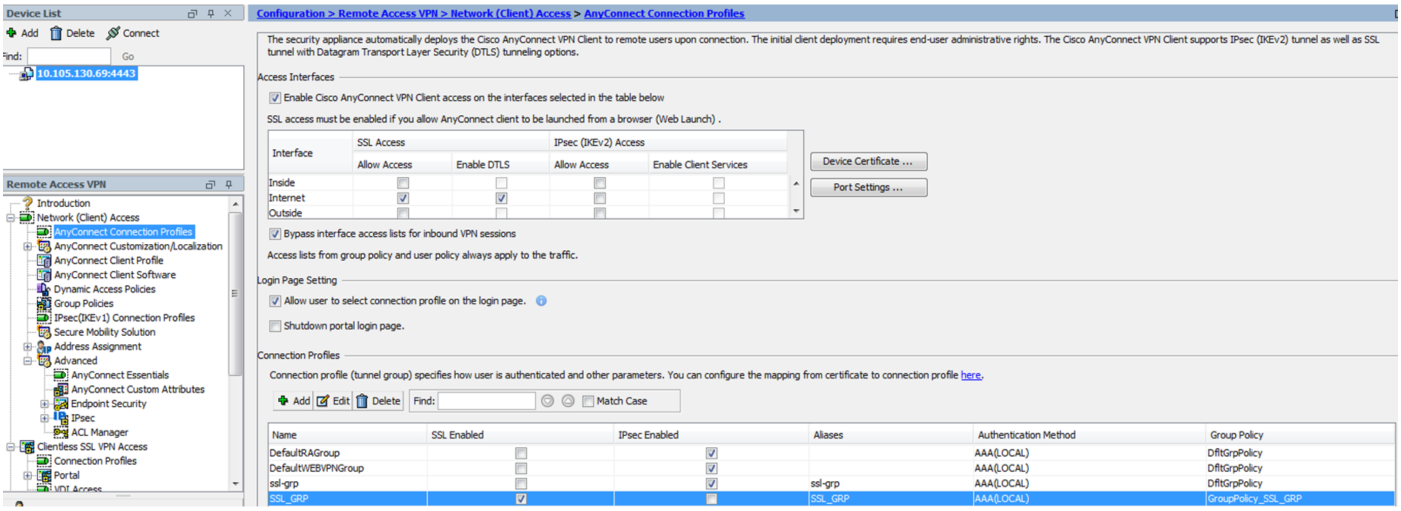
Summary

Here is the summary of the configuration.

Name	Value
⊟ Summary	
Name/Alias of the Connection Profile	SSL_GRP
VPN Access Interface	Internet
Device Digital Certificate	-- none --
VPN Protocols Enabled	SSL only
AnyConnect Client Images	1 package
Authentication Server Group	LOCAL
Address Pool for the Client	10.10.10.1 - 10.10.10.200
DNS	Server: Domain Name:
Network Address Translation	The protected traffic is not subjected to network address translation

AnyConnect客戶端配置現已完成。但是，當您透過配置嚮導配置AnyConnect時，預設情況下它會將身份驗證方法配置為AAA。要透過證書和使用者名稱/密碼對客戶端進行身份驗證，必須將隧道組（連線配置檔案）配置為使用證書和AAA作為身份驗證方法。

- 導航到配置>遠端接入VPN >網路（客戶端）接入> AnyConnect連線配置檔案。
- 您應該會看到新的增加連線配置檔案SSL_GRP已列出。



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
Inside	□	□	□	□
Internet	☑	☑	□	□
Outside	□	□	□	□

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☑ Allow user to select connection profile on the login page.

□ Shutdown portal login page.

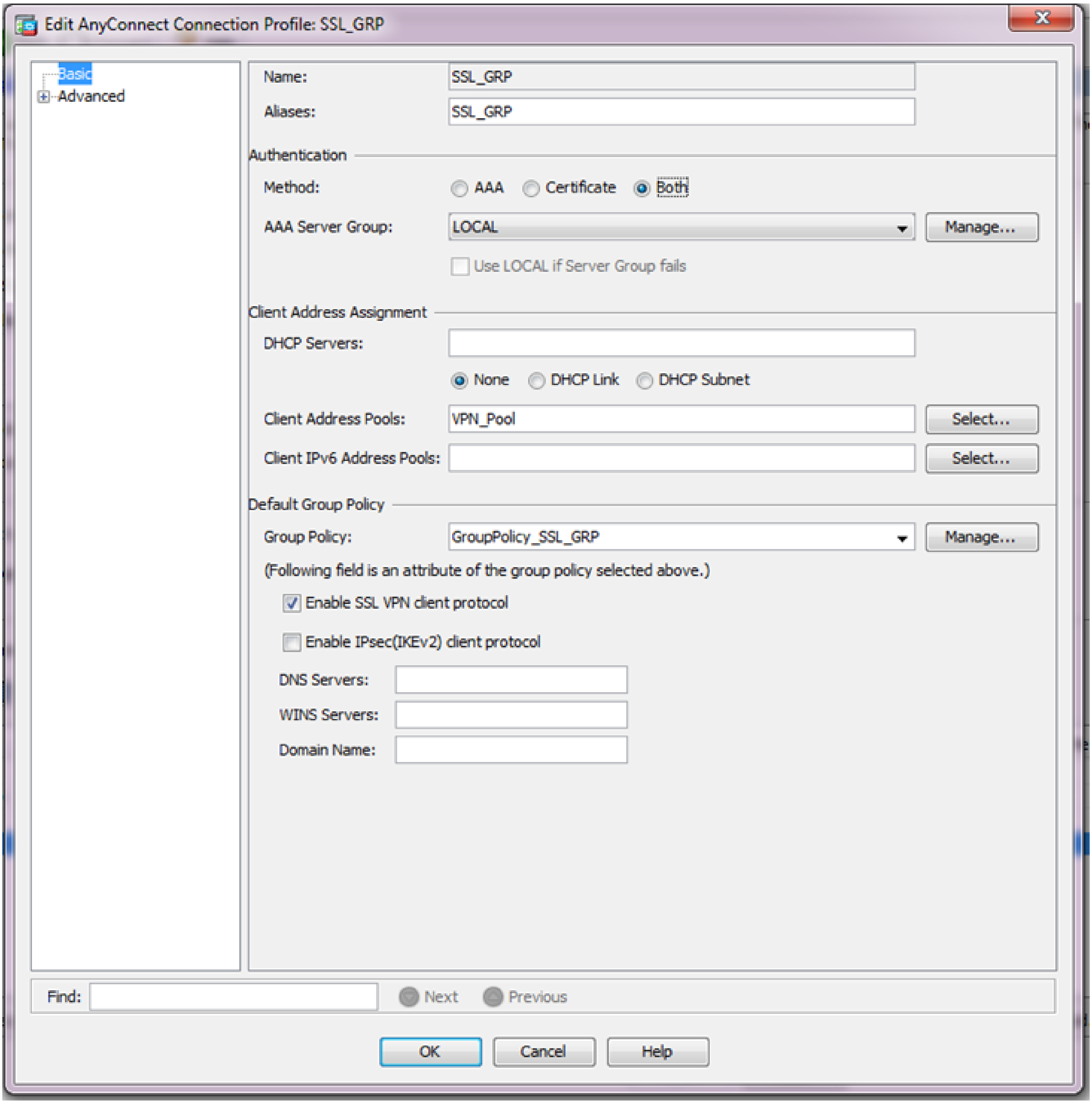
Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

□ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	□	☑		AAA(LOCAL)	DfltGrpPolicy
ssl-grp	□	☑	ssl-grp	AAA(LOCAL)	DfltGrpPolicy
SSL_GRP	☑	□	SSL_GRP	AAA(LOCAL)	GroupPolicy_SSL_GRP

- 要配置AAA和Certificate Authentication，請選擇連線配置檔案SSL_GRP，然後按一下Edit。
- 在身份驗證方法下，選擇Both。



Edit AnyConnect Connection Profile: SSL_GRP

Name: SSL_GRP

Aliases: SSL_GRP

Authentication

Method: ○ AAA ○ Certificate ● Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: VPN_Pool

Client IPv6 Address Pools:

Default Group Policy

Group Policy: GroupPolicy_SSL_GRP

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

□ Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

Domain Name:

配置AnyConnect的CLI

<#root>

```
!! *****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 destinati
```

驗證

使用本節內容，確認您的組態是否正常運作。

附註： Output Interpreter工具(僅限註冊客戶)支援某些show指令。使用命令輸出解釋程式工具檢視show命令輸出的分析。

確保已啟用CA伺服器。

show crypto ca server

<#root>

```
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!!
```

確保增加以下內容後允許該使用者註冊：

<#root>

```
*****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
```

您可以透過CLI或ASDM檢查anyconnect連線的詳細資訊。

透過CLI

show vpn-sessiondb detail anyconnect

<#root>

```
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 :
```

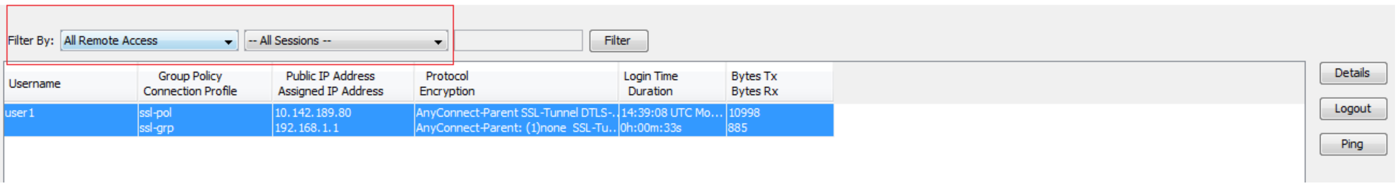
透過ASDM

- 導航至監控> VPN > VPN統計資訊>會話。
- 選擇Filter By作為All Remote Access。
- 您可以對選定的AnyConnect客戶端執行任一操作。

詳細資訊-提供有關會話的詳細資訊

註銷-從頭端手動註銷使用者

Ping -從頭端ping AnyConnect客戶端



Filter By: All Remote Access | -- All Sessions --

Username	Group Policy Connection Profile	Public IP Address Assigned IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
user1	ssl-pol ssl-grp	10.142.189.80 192.168.1.1	AnyConnect-Parent SSL-Tunnel DTLS-.. AnyConnect-Parent: (1)none SSL-Tu..	14:39:08 UTC Mo... 0h:00m:33s	10998 885

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

> 附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

> 注意：在ASA上，您可以設定各種調試級別；預設情況下，使用級別1。如果更改調試級別，調試的冗長可能會增加。請謹慎執行此操作，尤其是在生產環境中。

- debug crypto ca
- debug crypto ca server
- debug crypto ca message
- debug crypto ca transactions
- debug webvpn anyconnect

使用no shut命令啟用CA伺服器時，此調試輸出會顯示。

<#root>

```
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!
```

此調試輸出顯示客戶端的註冊

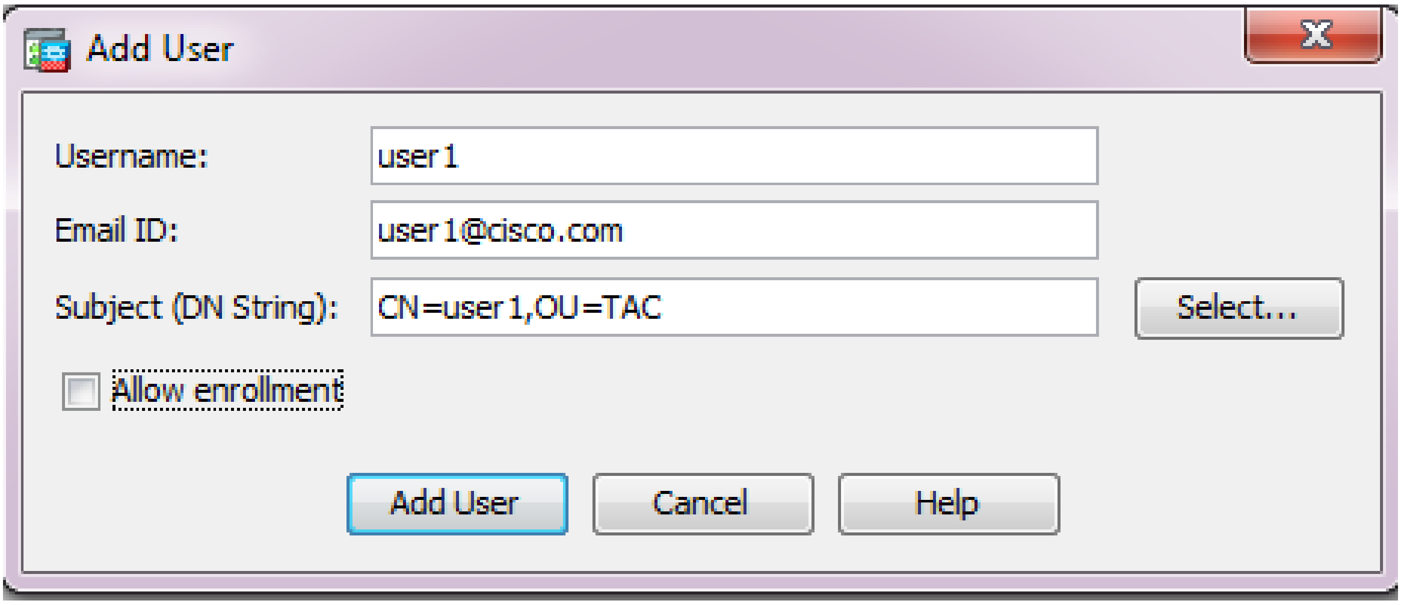
<#root>

```
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
```

在下列情況下，使用者端註冊可能會失敗：

案例 1.

- 使用者在CA伺服器資料庫中建立，沒有註冊許可權。


Add User

Username: user1

Email ID: user1@cisco.com

Subject (DN String): CN=user1,OU=TAC

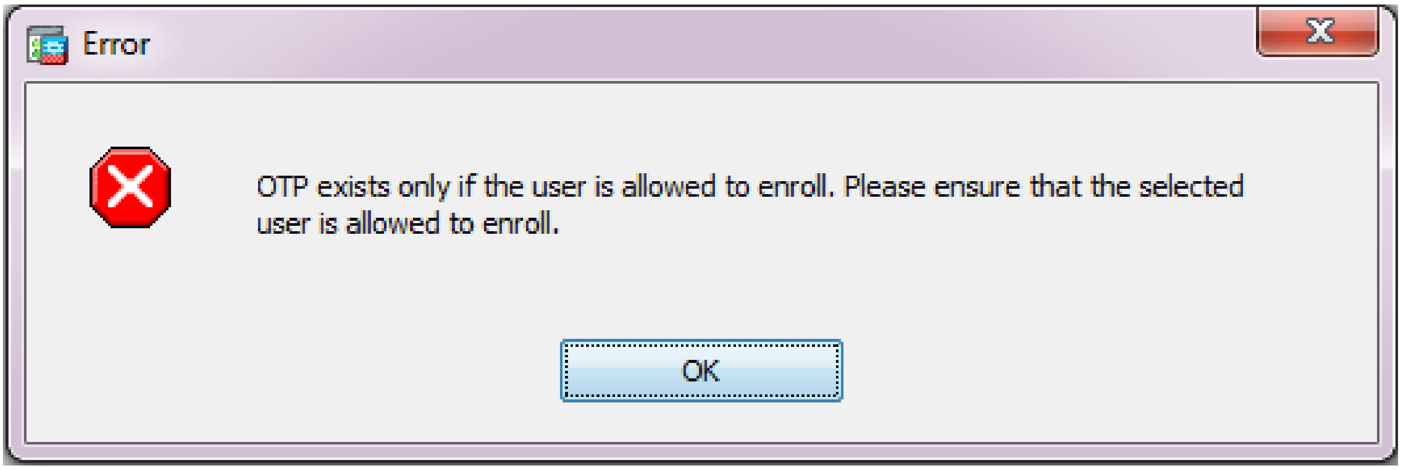
□ Allow enrollment

等效的CLI命令：

<#root>

```
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
```

- 如果不允許使用者註冊，則嘗試產生/以電子郵件寄送使用者的OTP會產生此錯誤訊息。



OTP exists only if the user is allowed to enroll. Please ensure that the selected user is allowed to enroll.

案例 2.

- 使用show run webvpn 命令驗證註冊門戶所在的埠和介面。預設埠為443，但可以修改。
- 確保客戶端能夠與在用於成功訪問註冊門戶的埠上啟用webvpn的介面IP地址網路連通。

在下列情況下，客戶端可能無法訪問ASA的註冊門戶：

1. 如果任何中間裝置在指定埠上阻止從客戶端到ASA的webvpn IP的傳入連線，請執行以下操作：
2. 啟用了webvpn的介面狀態為down。

- 此輸出顯示註冊門戶在自定義埠4433上位於網際網路介面的IP地址。

<#root>

```
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
```

案例 3.

- CA伺服器資料庫儲存的預設位置是ASA的快閃記憶體。
- 確保快閃記憶體具有在註冊過程中為使用者生成和儲存pkcs12檔案的可用空間。
- 如果快閃記憶體沒有足夠的可用空間，ASA將無法完成客戶端的註冊過程並生成以下調試日誌：

<#root>

```
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
```

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- AnyConnect VPN客戶端故障排除指南-常見問題
- AnyConnect會話的管理、監控和故障排除
- 技術支援與文件 - Cisco Systems

關於此翻譯