使用比利時eID卡的ASA 8.x Anyconnect身份驗證

目錄

簡介

本文檔介紹如何設定ASA 8.x Anyconnect身份驗證以使用比利時的eID卡。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA 5505及相應的ASA 8.0軟體
- AnyConnect客戶端
- ASDM 6.0

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。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

eID是比利時政府頒發的PKI（公開金鑰基礎架構）卡，使用者必須使用該卡才能在遠端Windows PC上進行驗證。AnyConnect軟體客戶端安裝在本地PC上，並從遠端PC獲取身份驗證憑證。完成身份驗證後，遠端使用者將通過完整的SSL隧道訪問中央資源。遠端使用者使用從ASA管理的池獲取的IP地址進行調配。

本地PC設定

作業系統

本地PC上的作業系統（Windows、MacOS、Unix或Linux）必須最新並安裝了所有必需的修補程式。

讀卡器

您的本地電腦上必須安裝電子讀卡器才能使用eID卡。電子讀卡器是建立電腦程式與身份證晶片之間通訊通道的硬體裝置。

有關批准的讀卡器清單，請參閱以下URL:http://www.cardreaders.be/en/default.htm

註：要使用讀卡器，必須安裝硬體供應商推薦的驅動程式。

eID運行時軟體

您必須安裝比利時政府提供的eID運行時軟體。此軟體允許遠端使用者讀取、驗證和列印eID卡的內容。該軟體提供法語和荷蘭語版本，適用於Windows、MAC OS X和Linux。

如需詳細資訊，請參閱以下URL:

- http://www.belgium.be/zip/eid_datacapture_nl.html

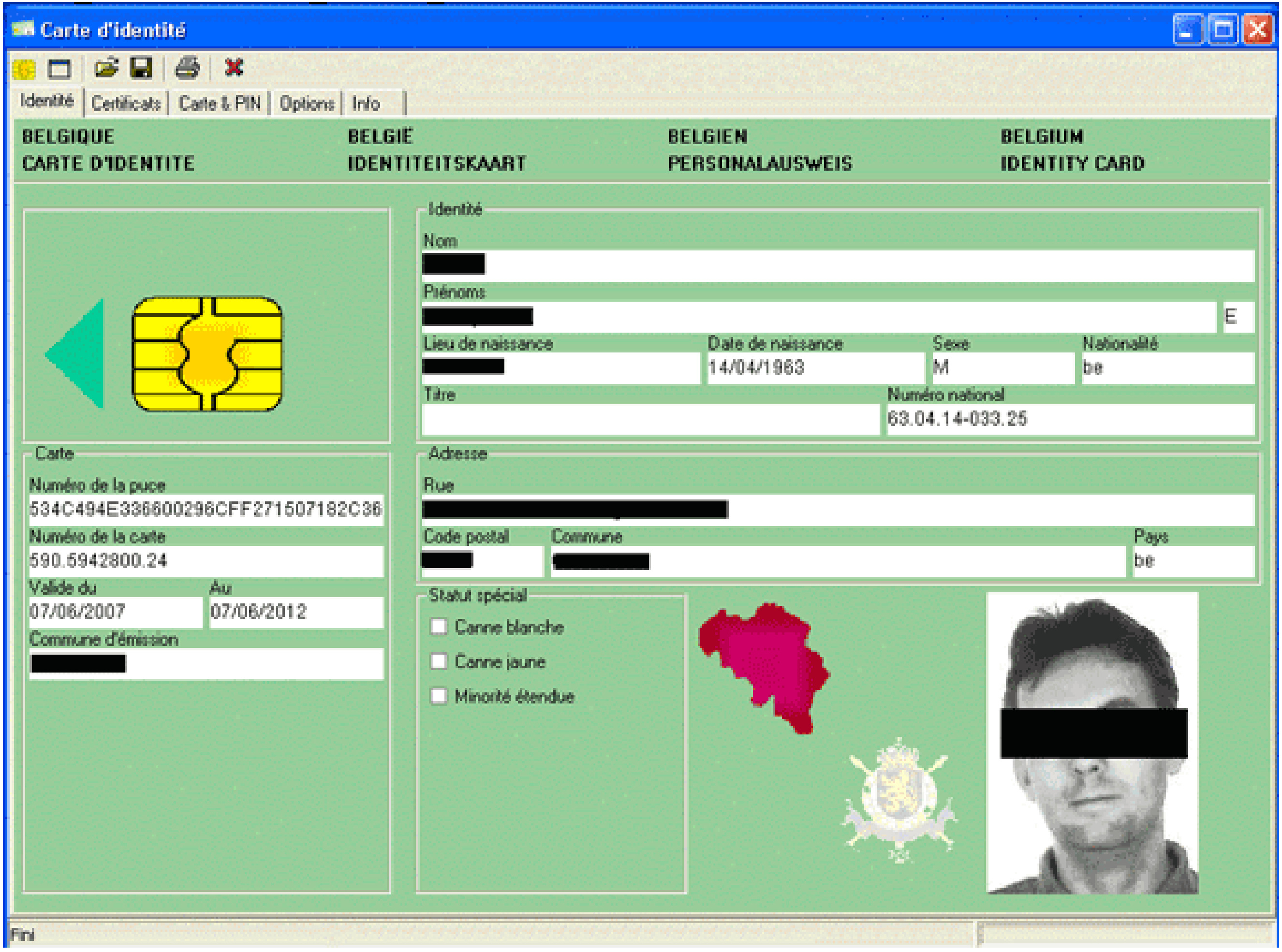
驗證憑證

必須將身份驗證證書匯入本地PC上的Microsoft Windows應用商店。如果無法將證書匯入到儲存區，AnyConnect客戶端將無法建立到ASA的SSL連線。

程式

若要將驗證憑證匯入Windows儲存區，請完成以下步驟：

1. 將eID插入讀卡器，然後啟動中介軟體以訪問eID卡的內容。此時將顯示eID卡的內容。



Carte d'identité

BELGIQUE
CARTE D'IDENTITE

BELGIË
IDENTITEITSKAART

BELGIEN
PERSONALAUSWEIS

BELGIUM
IDENTITY CARD

Identité

Nom: [redacted]

Prénoms: [redacted] E

Lieu de naissance: [redacted]

Date de naissance: 14/04/1963

Sexe: M

Nationalité: be

Titre:

Numéro national: 63.04.14-033.25

Carte

Numéro de la puce: 534C494E336600296CFF271507182C36

Numéro de la carte: 590.5942800.24

Valide du: 07/06/2007

Au: 07/06/2012

Commune d'émission: [redacted]

Adresse

Rue: [redacted]

Code postal: [redacted]

Commune: [redacted]

Pays: be

Statut spécial

☐ Canne blanche

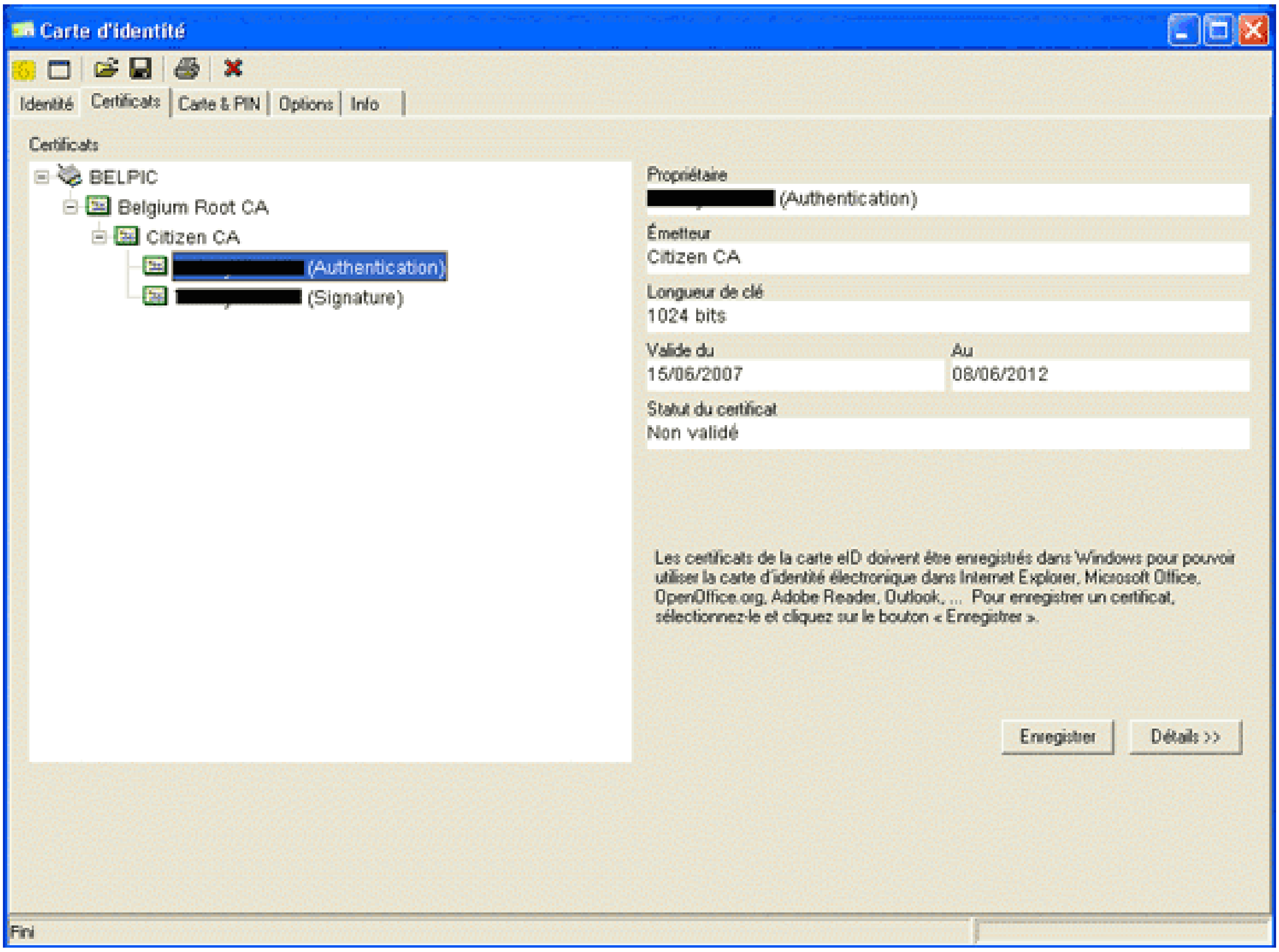
☐ Canne jaune

☐ Minorité étendue

[redacted]

Fini

2. 按一下**Certificates**(FR)頁籤。將顯示證書層次結構。



Certificats

- BELPIC
  - Belgium Root CA
    - Citizen CA
      - [redacted] (Authentication)
      - [redacted] (Signature)

Propriétaire
[redacted] (Authentication)

Émetteur
Citizen CA

Longueur de clé
1024 bits

Valide du
15/06/2007

Au
08/06/2012

Statut du certificat
Non validé

Les certificats de la carte eID doivent être enregistrés dans Windows pour pouvoir utiliser la carte d'identité électronique dans Internet Explorer, Microsoft Office, OpenOffice.org, Adobe Reader, Outlook, ... Pour enregistrer un certificat, sélectionnez-le et cliquez sur le bouton « Enregistrer ».

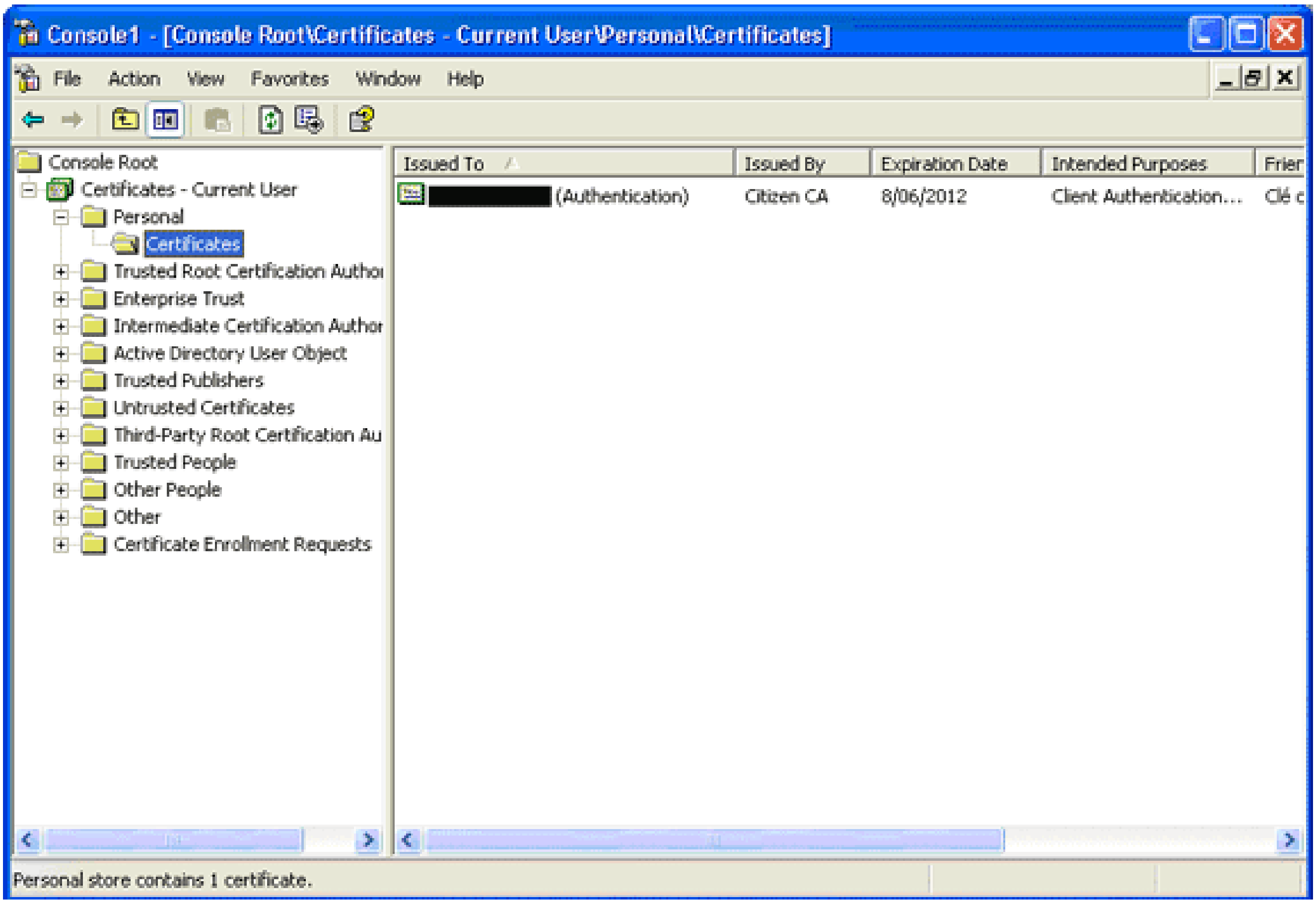
3. 展開**Belgium Root CA**，然後展開**Citizen CA**。
4. 選擇**Authentication**版本的指定證書。
5. 按一下**Enregistrer**(FR)按鈕。證書將複製到Windows應用商店。

註：單擊Details按鈕時**出現**一個視窗，顯示有關證書的詳細資訊。在詳細資訊頁籤中，選擇**Subject**欄位以檢視Serial Number欄位。Serial Number欄位包含一個用於使用者授權的唯一值。例*如，序列號"56100307215"表示其出生日期為1956年10月3日的用戶，其序號為072，校驗位為15。您必須提交聯邦當局的批准請求才能儲存這些號碼。您有責任就維護貴國比利時公民資料庫作出適當的官方宣告。*

驗證

若要確認憑證是否成功匯入，請完成以下步驟：

1. 在Windows XP電腦上，開啟DOS視窗，然後鍵入**mmc**命令。系統將顯示Console應用程式。
2. 選擇**File > Add/Remove Snap-in**（或按Ctrl+M）。將出現「新增/刪除管理單元」對話方塊。
3. 按一下**Add**按鈕。將出現「新增獨立管理單元」對話方塊。
4. 在可用獨立管理單元清單中，選擇**證書**，然後按一下**新增**。
5. 按一下**My user account**單選按鈕，然後按一下**Finish**。「證書」管理單元出現在「新增/刪除管理單元」對話方塊中。
6. 按一下**關閉**以關閉「新增獨立管理單元」對話方塊，然後在「新增/刪除管理單元」對話方塊中按一下**確定**，以儲存更改並返回到Console應用程式。
7. 在Console Root資料夾下，展開**Certificates - Current User**。
8. 展開**Personal**，然後展開**Certificates**。匯入的證書必須出現在Windows應用商店中，如下圖所示
   ：


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Author
Enterprise Trust
Intermediate Certification Author
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Other People
Other
Certificate Enrollment Requests

Issued To	Issued By	Expiration Date	Intended Purposes	Frier
[redacted] (Authentication)	Citizen CA	8/06/2012	Client Authentication...	Clé c

Personal store contains 1 certificate.

AnyConnect安裝

必須在遠端PC上安裝AnyConnect客戶端。AnyConnect軟體使用可編輯的XML配置檔案，以預置可用網關的清單。XML檔案儲存在遠端PC上的以下路徑中：

C:\Documents和設定\*%USERNAME%*\Application Data\Cisco\Cisco AnyConnect VPN客戶端

其中*%USERNAME%*是遠端PC上使用者的名稱。

XML檔案的名稱為*preferences.xml*。以下是檔案內容的範例：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectPreferences>
<DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences>
```

其中*192.168.0.1*是ASA網關的IP地址。

ASA要求

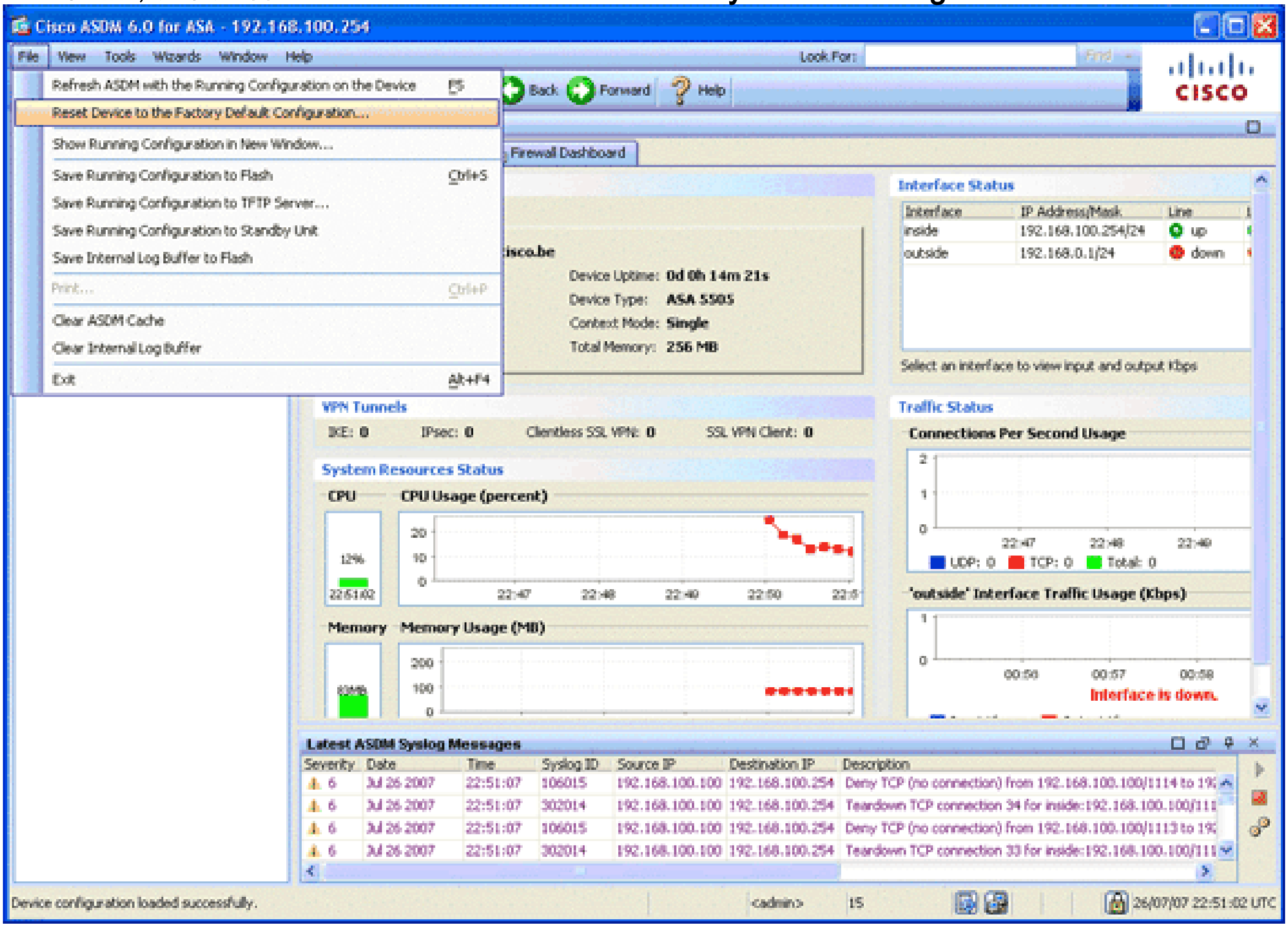
確保ASA滿足以下要求：

- AnyConnect和ASDM必須在快閃記憶體中運行。要完成本文檔中的步驟，請使用安裝了適當ASA 8.0軟體的ASA 5505。必須在快閃記憶體中預載入AnyConnect和ASDM應用程式。使用**show flash**命令以檢視flash：的內容

  ```
  ciscoasa#show flash:
  --#--  --length--  -----date/time------  path
     66  14524416    Jun 26 2007 10:24:02  asa802-k8.bin
  ```

```
    67   6889764      Jun 26 2007 10:25:28  asdm-602.bin
    68   2635734      Jul 09 2007 07:37:06  anyconnect-win-2.0.0343-k9.pkg
```

- ASA必須使用出廠預設設定運行。如果您使用新的ASA機箱來完成本文檔中的步驟，則可以跳過此要求。否則，請完成以下步驟，將ASA重置為出廠預設值：在ASDM應用中，連線到ASA機箱，然後選擇**File > Reset Device to the Factory Default Configuration**。

  
  Cisco ASDM 6.0 for ASA - 192.168.100.254
File
View
Tools
Wizards
Window
Help
Look For:
Find
Refresh ASDM with the Running Configuration on the Device F5
Reset Device to the Factory Default Configuration...
Show Running Configuration in New Window...
Save Running Configuration to Flash Ctrl+S
Save Running Configuration to TFTP Server...
Save Running Configuration to Standby Unit
Save Internal Log Buffer to Flash
Print... Ctrl+P
Clear ASDM Cache
Clear Internal Log Buffer
Exit Alt+F4
Back
Forward
Help
CISCO
Firewall Dashboard
Interface Status
VPN Tunnels
Traffic Status
System Resources Status
CPU
CPU Usage (percent)
Memory
Memory Usage (MB)
Connections Per Second Usage
'outside' Interface Traffic Usage (Kbps)
Latest ASDM Syslog Messages

  isco.be
  Device Uptime: 0d 0h 14m 21s
  Device Type: ASA 5505
  Context Mode: Single
  Total Memory: 256 MB

Interface	IP Address/Mask	Line
inside	192.168.100.254/24	up
outside	192.168.0.1/24	down

  Select an interface to view input and output Kbps

  IKE: 0 IPsec: 0 Clientless SSL VPN: 0 SSL VPN Client: 0

  UDP: 0 TCP: 0 Total: 0

  Interface is down.

Severity	Date	Time	Syslog ID	Source IP	Destination IP	Description
6	Jul 26 2007	22:51:07	106015	192.168.100.100	192.168.100.254	Deny TCP (no connection) from 192.168.100.100/1114 to 19
6	Jul 26 2007	22:51:07	302014	192.168.100.100	192.168.100.254	Teardown TCP connection 34 for inside:192.168.100.100/111
6	Jul 26 2007	22:51:07	106015	192.168.100.100	192.168.100.254	Deny TCP (no connection) from 192.168.100.100/1113 to 19
6	Jul 26 2007	22:51:07	302014	192.168.100.100	192.168.100.254	Teardown TCP connection 33 for inside:192.168.100.100/111

  Device configuration loaded successfully. <admin> 15 26/07/07 22:51:02 UTC

  在模板中保留預設值。將您的PC連線到Ethernet 0/1內部介面，並續訂由ASA的DHCP伺服器調配的IP地址。**注意：**要從命令列將ASA重置為出廠預設值，請使用以下命令：

  ```
  ciscoasa#conf t
  ciscoasa#config factory-default 192.168.0.1 255.255.255.0
  ```

ASA配置

重置ASA出廠預設設定後，可以將ASDM啟動到192.168.0.1，以便連線到Ethernet 0/1內部介面上的ASA。

注意：您以前的密碼將被保留（或者預設情況下可以為空）。

預設情況下，ASA接受源IP地址在子網192.168.0.0/24中的傳入管理會話。在ASA內部介面上啟用的預設DHCP伺服器提供192.168.0.2-129/24範圍內的IP地址，這些地址對於通過ASDM連線到內部介面有效。

完成以下步驟以配置ASA:

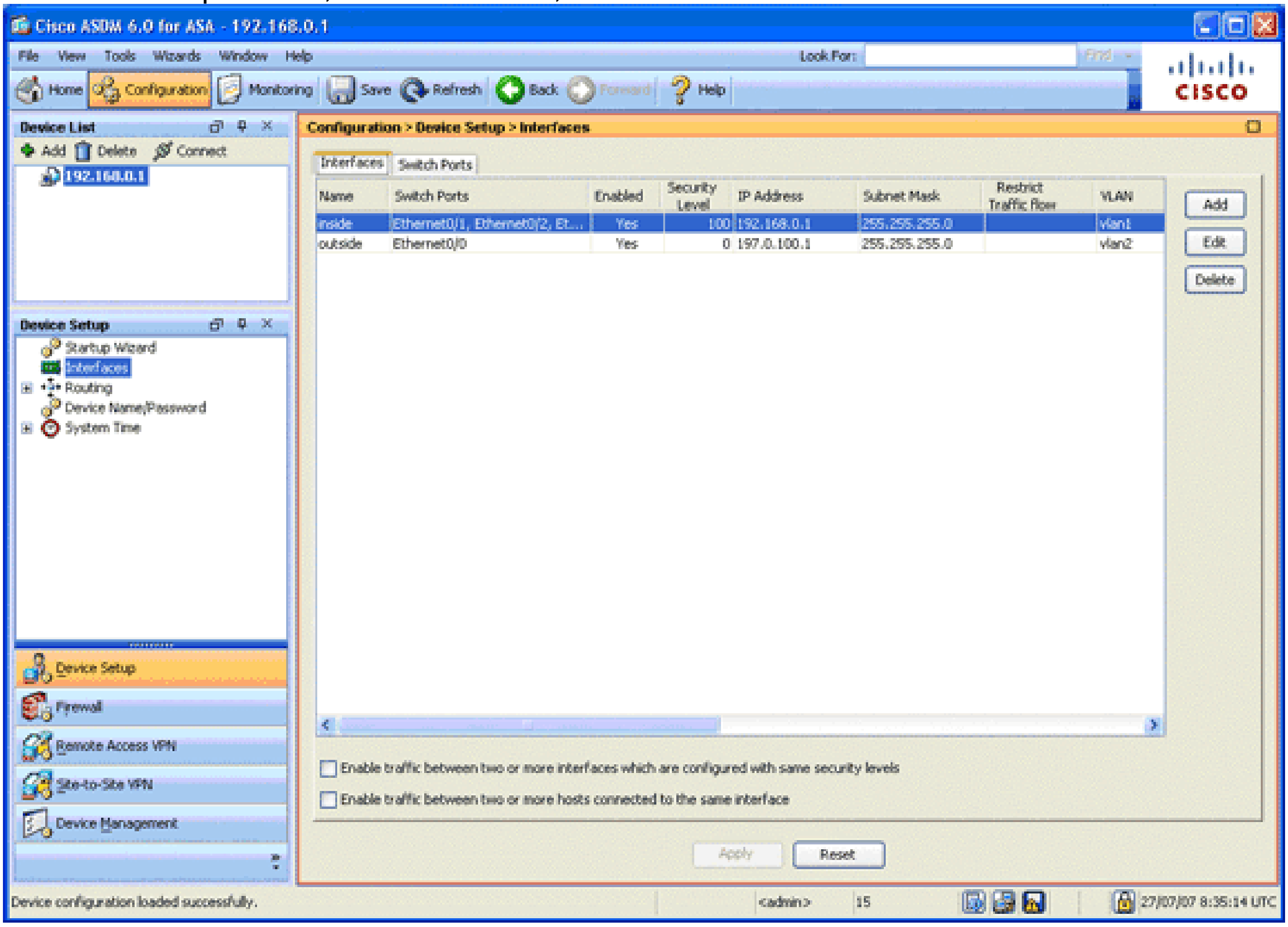
1. 啟用外部介面
2. 配置域名、密碼和系統時間
3. 在外部介面上啟用DHCP伺服器
4. 配置eID VPN地址池

5. 匯入比利時根CA證書
6. 配置安全套接字層
7. 定義預設組策略
8. 定義證書對映
9. 新增本地使用者
10. 重新啟動ASA

步驟1.啟用外部介面

此步驟說明如何啟用外部介面。

1. 在ASDM應用程式中，按一下**Configuration**，然後按一下**Device Setup**。
2. 在Device Setup區域中，選擇**Interfaces**，然後按一下**Interfaces**頁籤。



Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask	Restrict Traffic Flow	VLAN
inside	Ethernet0/1, Ethernet0/2, Et...	Yes	100	192.168.0.1	255.255.255.0		vlan1
outside	Ethernet0/0	Yes	0	197.0.100.1	255.255.255.0		vlan2

☐ Enable traffic between two or more interfaces which are configured with same security levels

☐ Enable traffic between two or more hosts connected to the same interface

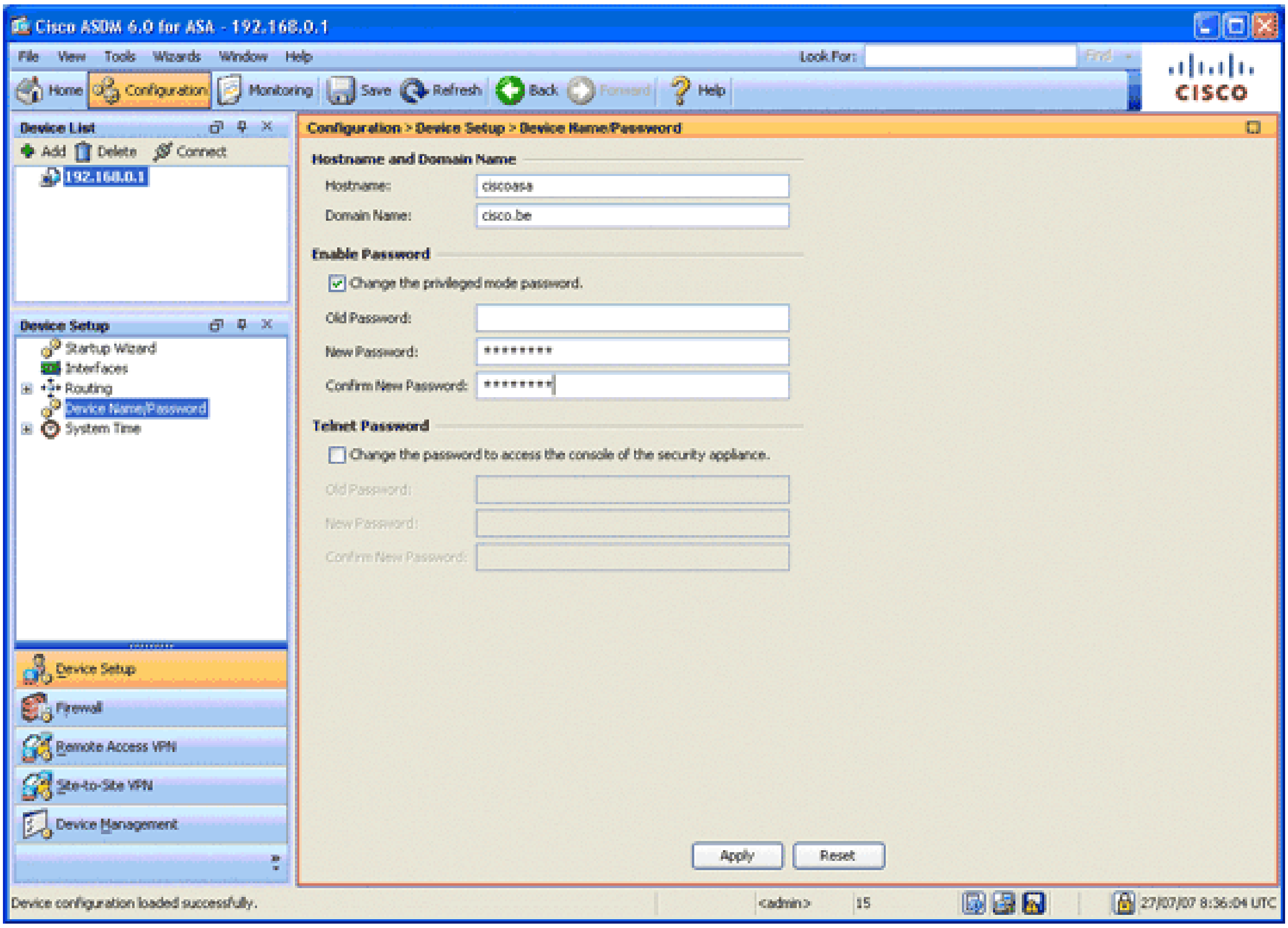
Device configuration loaded successfully. <admin> 15 27/07/07 8:35:14 UTC

3. 選擇外部介面，然後按一下**Edit**。
4. 在General頁籤的IP address部分，選擇**Use Static IP**選項。
5. 輸入**197.0.100.1**作為IP地址，**255.255.255.0**作為子網掩碼。
6. 按一下「**Apply**」。

步驟2.配置域名、密碼和系統時間

此步驟說明如何配置域名、密碼和系統時間。

1. 在Device Setup區域中，選擇**Device Name/Password**。



Configuration > Device Setup > Device Name/Password

Hostname and Domain Name

Hostname: ciscoasa

Domain Name: cisco.be

Enable Password

☑ Change the privileged mode password.

Old Password:

New Password: ********

Confirm New Password: ********

Telnet Password

☐ Change the password to access the console of the security appliance.

Old Password:

New Password:

Confirm New Password:

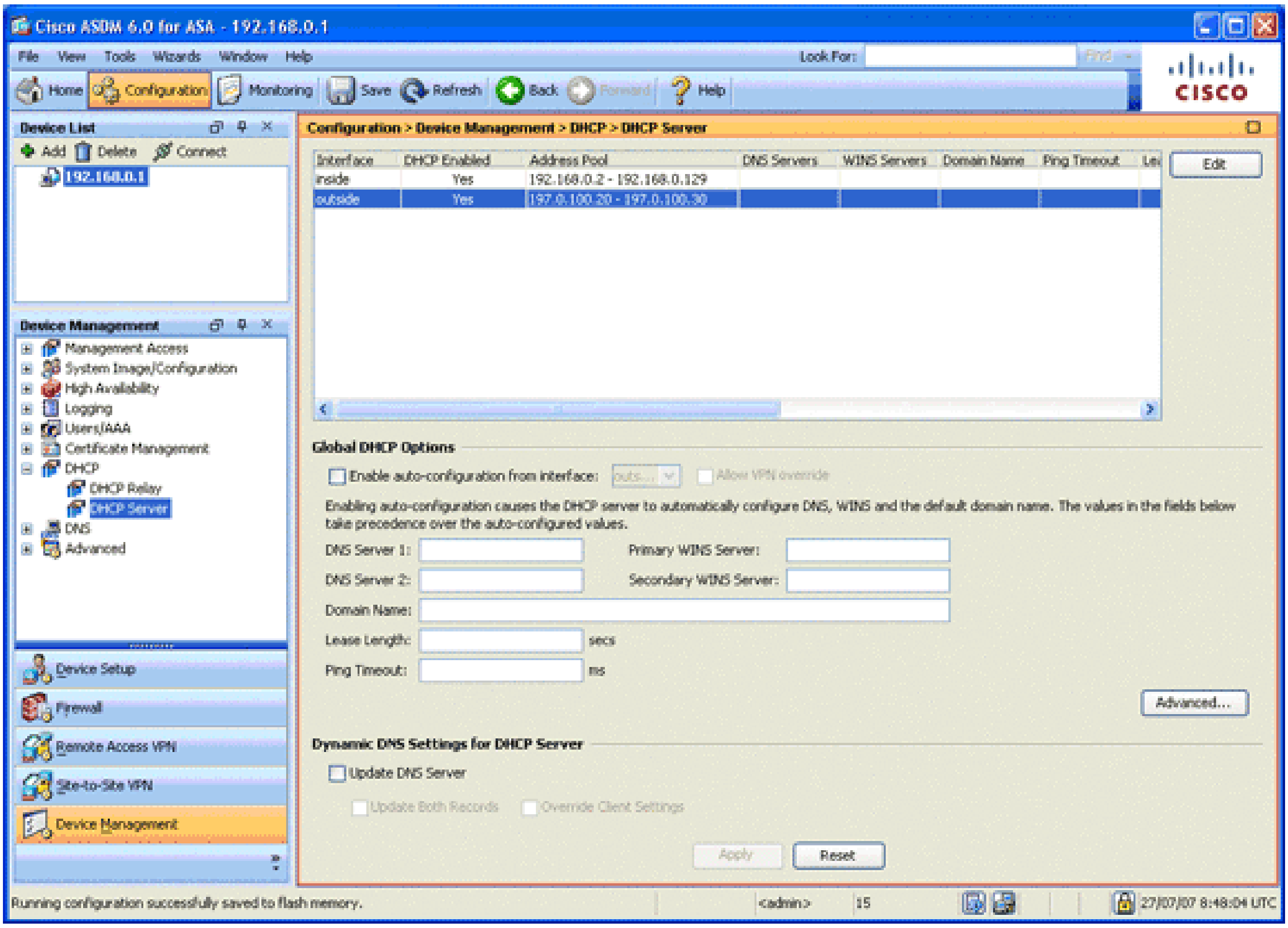
Device configuration loaded successfully. <admin> 15 27/07/07 8:36:04 UTC

2. 輸入**cisco.be**作為域名，輸入**cisco123**作為啟用密碼值。**注意：**預設情況下，密碼為空。
3. 按一下「**Apply**」。
4. 在Device Setup區域中，選擇**System Time**，然後更改時鐘值（如有必要）。
5. 按一下「**Apply**」。

步驟3.在外部介面上啟用DHCP伺服器。

此步驟描述如何在外部介面上啟用DHCP伺服器以便進行測試。

1. 按一下**Configuration**，然後按一下**Device Management**。
2. 在Device Management區域中，展開**DHCP**，然後選擇**DHCP Server**。



Interface	DHCP Enabled	Address Pool	DNS Servers	WINS Servers	Domain Name	Ping Timeout	Le
inside	Yes	192.168.0.2 - 192.168.0.129					
outside	Yes	197.0.100.20 - 197.0.100.30					

Global DHCP Options

☐ Enable auto-configuration from interface: outs... ☐ Allow VPN override

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

DNS Server 1:　　Primary WINS Server:

DNS Server 2:　　Secondary WINS Server:

Domain Name:

Lease Length: secs

Ping Timeout: ms

Dynamic DNS Settings for DHCP Server

☐ Update DNS Server

☐ Update Both Records ☐ Override Client Settings

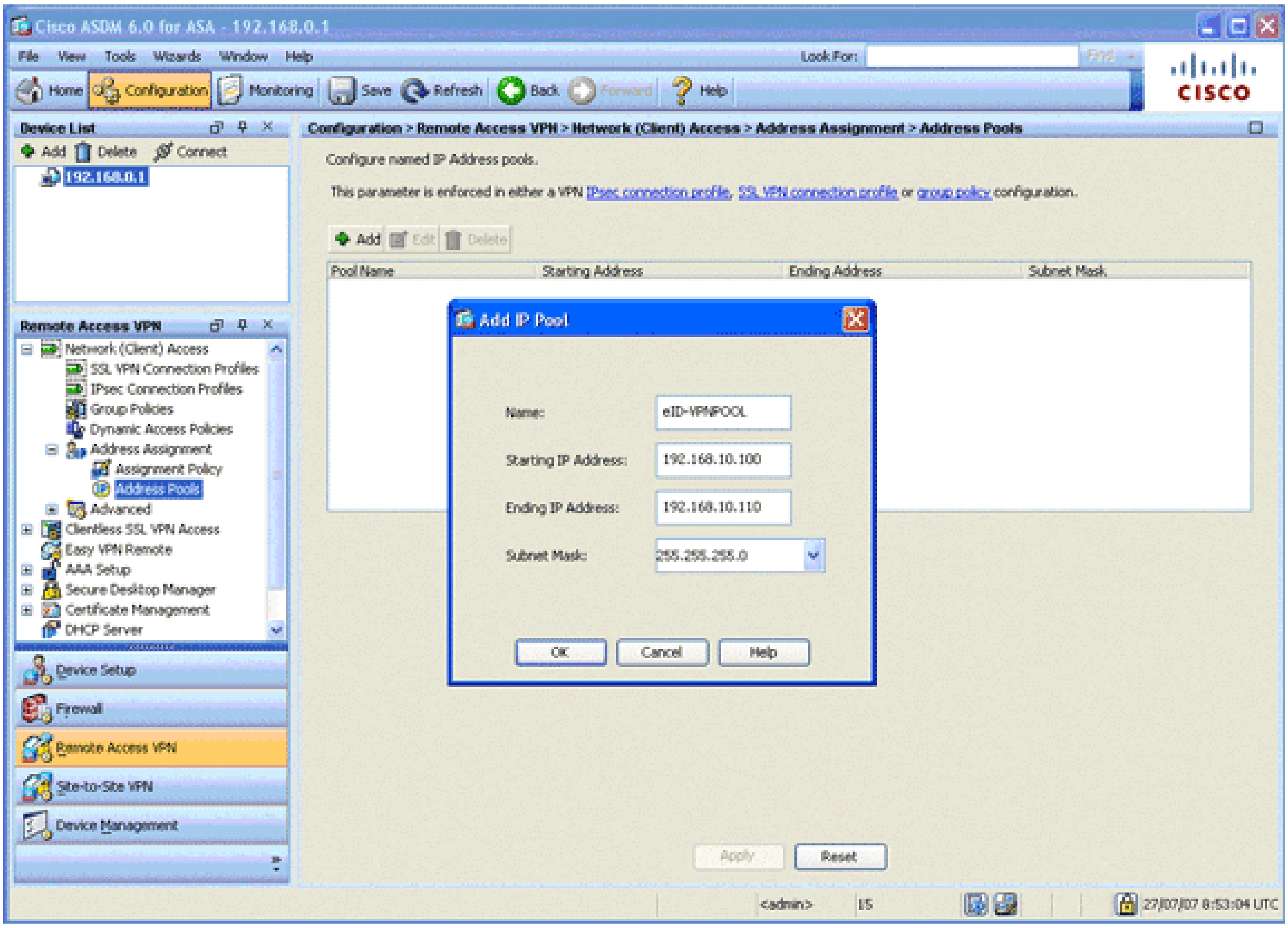
Running configuration successfully saved to flash memory. <admin> 15 27/07/07 8:48:04 UTC

3. 從Interface清單中選擇外部介面，然後按一下**Edit**。系統將顯示Edit DHCP Server對話方塊。
4. 選中**Enable DHCP Server**覈取方塊。
5. 在DHCP地址池中，輸入從197.0.100.20到197.0.100.30的IP地址。
6. 在Global DHCP Options區域中，取消選中**Enable auto-configuration from interface**覈取方塊。
7. 按一下「**Apply**」。

步驟4.配置eID VPN地址池

此步驟描述如何定義用於調配遠端AnyConnect客戶端的IP地址池。

1. 按一下**Configuration**，然後按一下**Remote Access VPN**。
2. 在Remove Access VPN區域中，展開**Network(Client)Access**，然後展開**Address Assignment**。
3. 選擇**Address Pools**，然後按一下Configure named IP Address pools區域中的**Add**按鈕。系統將顯示Add IP Pool對話方塊。



Cisco ASDM 6.0 for ASA - 192.168.0.1

Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools

Configure named IP Address pools.

This parameter is enforced in either a VPN IPsec connection profile, SSL VPN connection profile or group policy configuration.

Add IP Pool

Name: eID-VPNPOOL

Starting IP Address: 192.168.10.100

Ending IP Address: 192.168.10.110

Subnet Mask: 255.255.255.0

<admin> 15 27/07/07 8:53:04 UTC

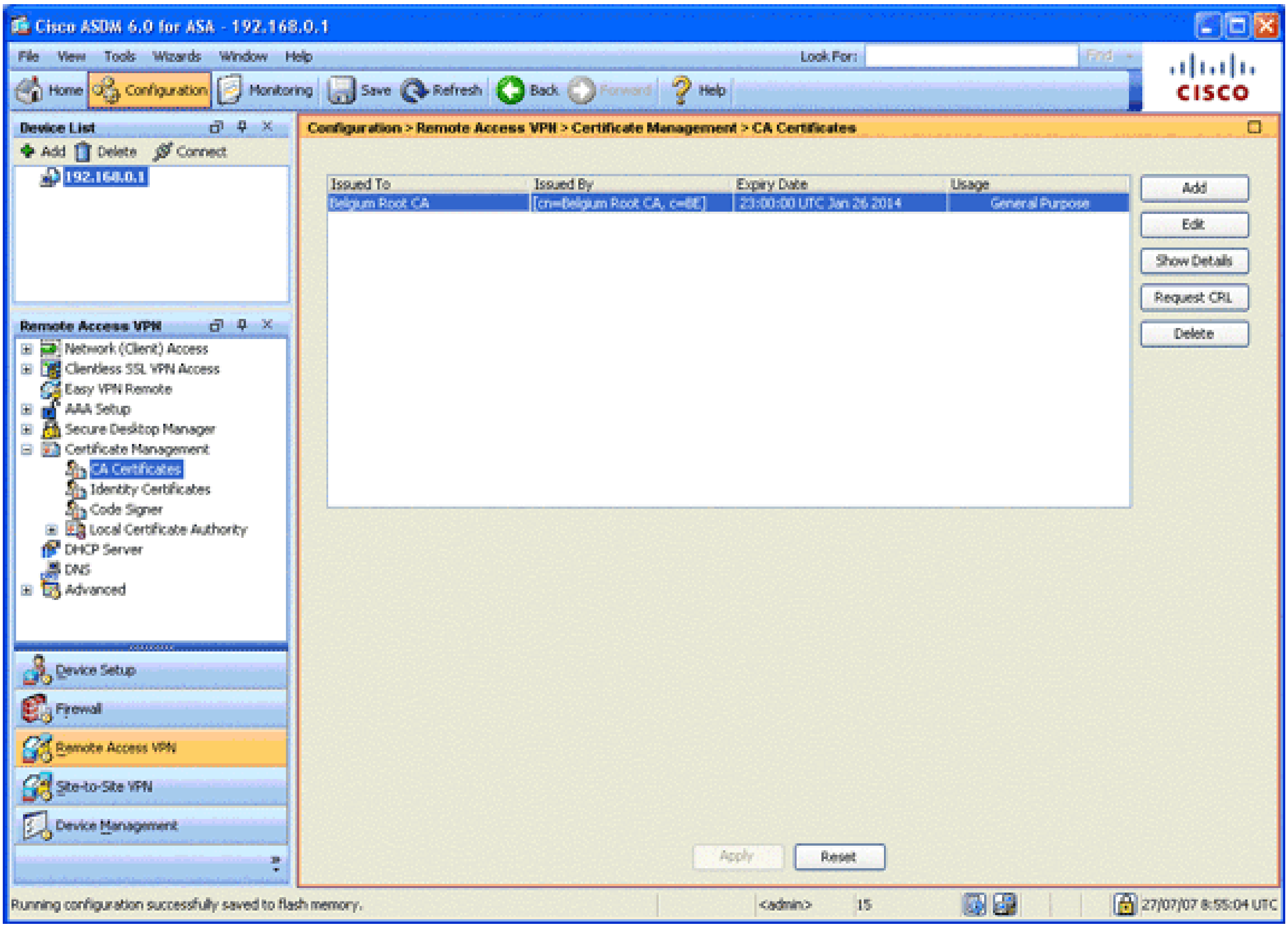
4. 在「名稱」欄位中，輸入**eID-VPNPOOL**。
5. 在Starting IP Address（起始IP地址）和Ending IP Address（結束IP地址）欄位中，輸入從192.168.10.100到192.168.10.110的IP地址範圍。
6. 從Subnet Mask下拉選單中選擇**255.255.255.0**，按一下**OK**，然後按一下**Apply**。

步驟5.匯入比利時根CA證書

此步驟說明如何將比利時根CA證書匯入ASA。

1. 從政府網站下載並安裝比利時根CA證書（belgiumrca.crt和belgiumrca2.crt），並將其儲存在本地PC上。比利時政府網站位於以下網址：http://certs.eid.belgium.be/
2. 在Remote Access VPN區域中，展開**Certificate Management**，然後選擇**CA Certificates**。
3. 按一下**Add**，然後按一下**Install from file**。
4. 瀏覽到儲存比利時根CA證書(belgiumrca.crt)檔案的位置，然後按一下**Install Certificate**。
5. 按一下「**Apply**」以儲存變更內容。

此圖顯示ASA上安裝的證書：



Configuration > Remote Access VPN > Certificate Management > CA Certificates

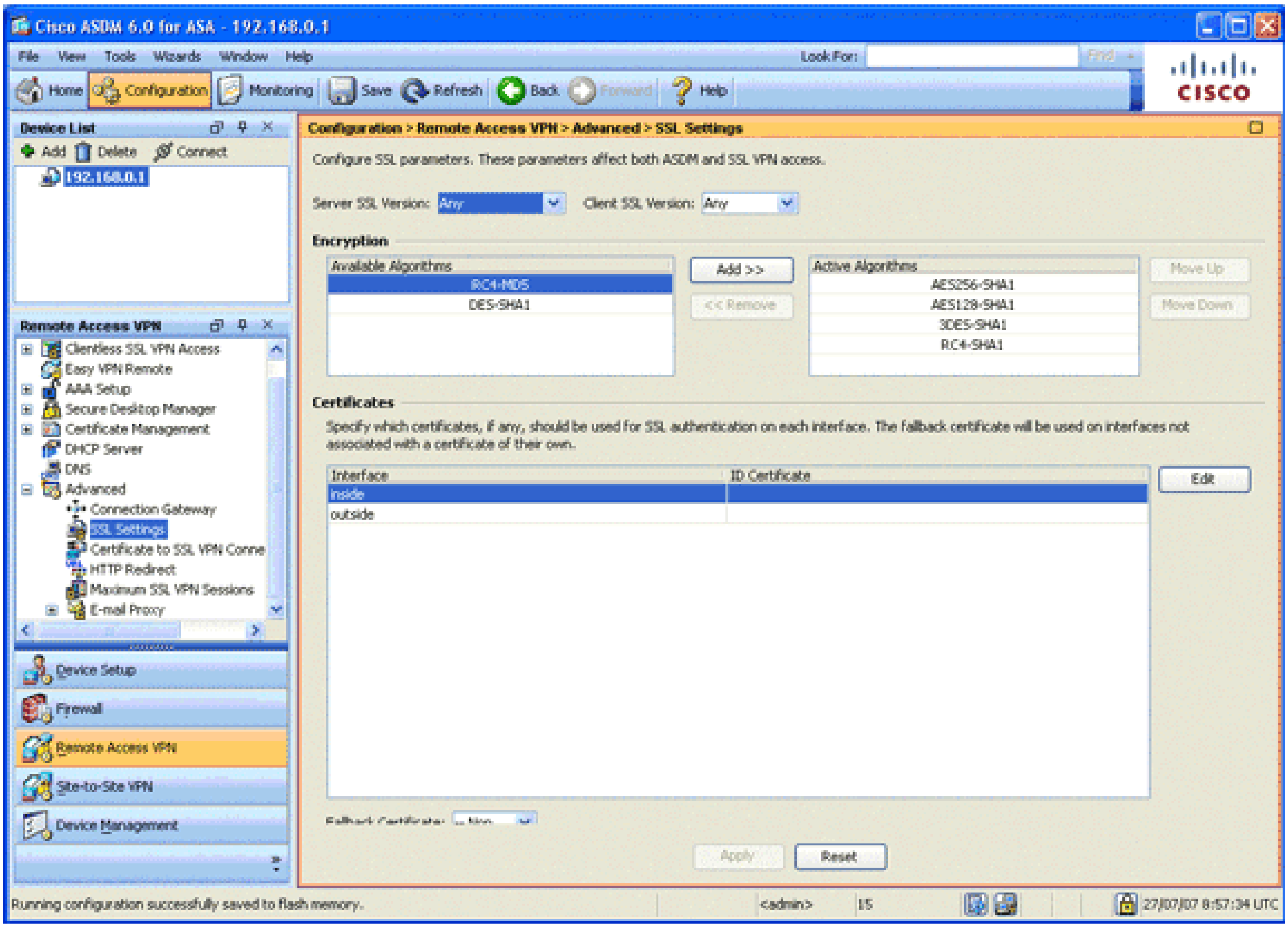
Issued To	Issued By	Expiry Date	Usage
Belgium Root CA	[cn=Belgium Root CA, c=BE]	23:00:00 UTC Jan 26 2014	General Purpose

Running configuration successfully saved to flash memory.

步驟6.配置安全套接字層

此步驟描述如何區分安全加密選項的優先順序、定義SSL VPN客戶端映像和定義連線配置檔案。

1. 優先使用最安全的加密選項。在Remote Access VPN區域中，展開**Advanced**，然後選擇**SSL Settings**。在Encryption部分中，按如下方式自上而下堆疊活動演算法：AES256-
SHA1AES128-SHA13DES-SHA1RC4-
SHA1



Configuration > Remote Access VPN > Advanced > SSL Settings

Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

Server SSL Version: Any   Client SSL Version: Any

Encryption

Available Algorithms
RC4-MD5
DES-SHA1

Active Algorithms
AES256-SHA1
AES128-SHA1
3DES-SHA1
RC4-SHA1

Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

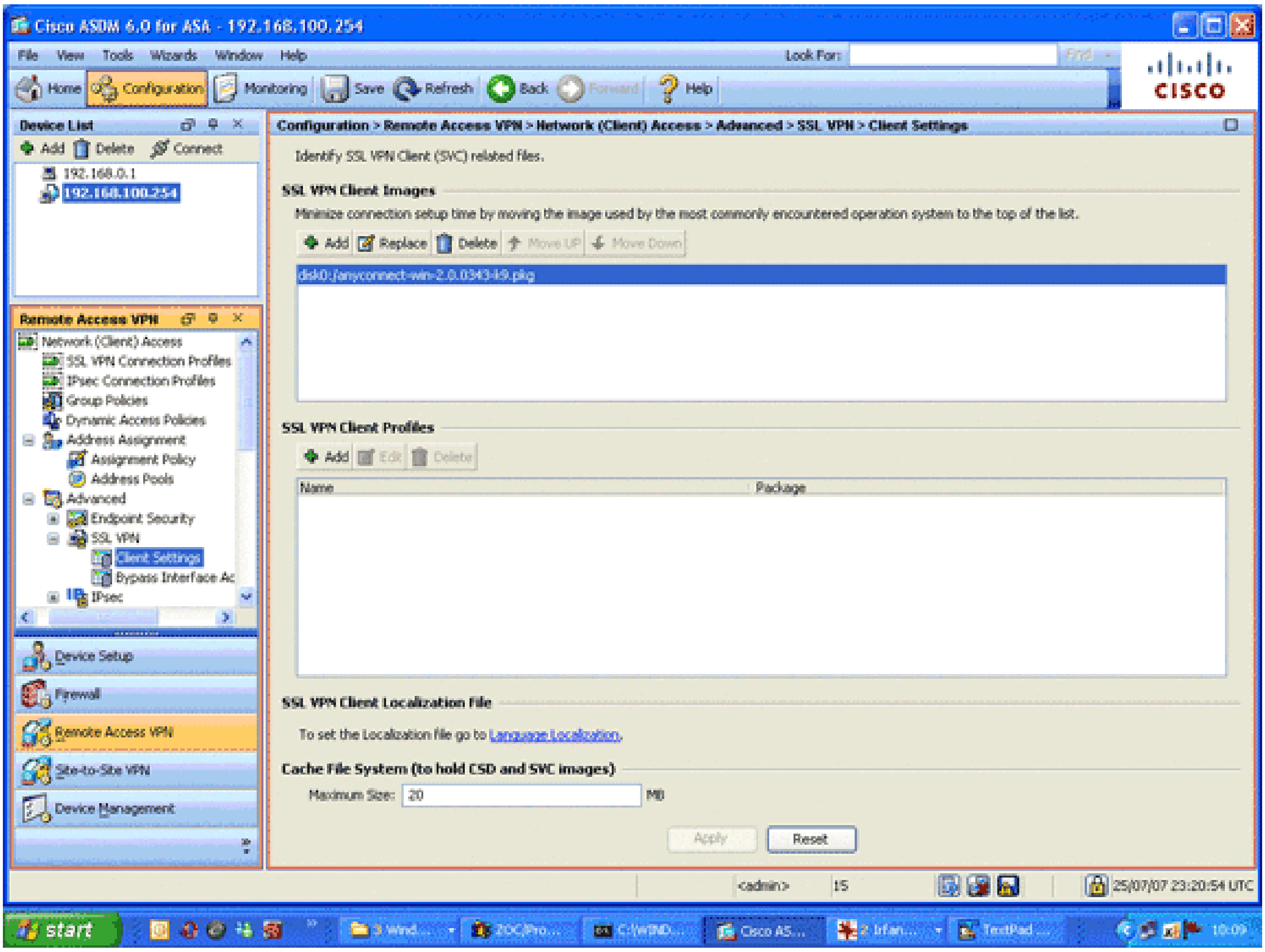
Interface	ID Certificate
inside	
outside	

Fallback Certificate: -- None --

Running configuration successfully saved to flash memory.   <admin>   15   27/07/07 8:57:34 UTC

2. 為AnyConnect客戶端定義SSL VPN客戶端映像。在Remote Access VPN區域中，展開**Advanced**，展開**SSL VPN**，然後選擇**Client Settings**。在SSL VPN Client Images區域中，按一下**Add**。選擇儲存在快閃記憶體中的AnyConnect軟體包。AnyConnect軟體包出現在SSL VPN客戶端映像清單中，如下圖所示

：



Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings

Identify SSL VPN Client (SVC) related files.

SSL VPN Client Images

Minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

disk0:/anyconnect-win-2.0.0343-k9.pkg

SSL VPN Client Profiles

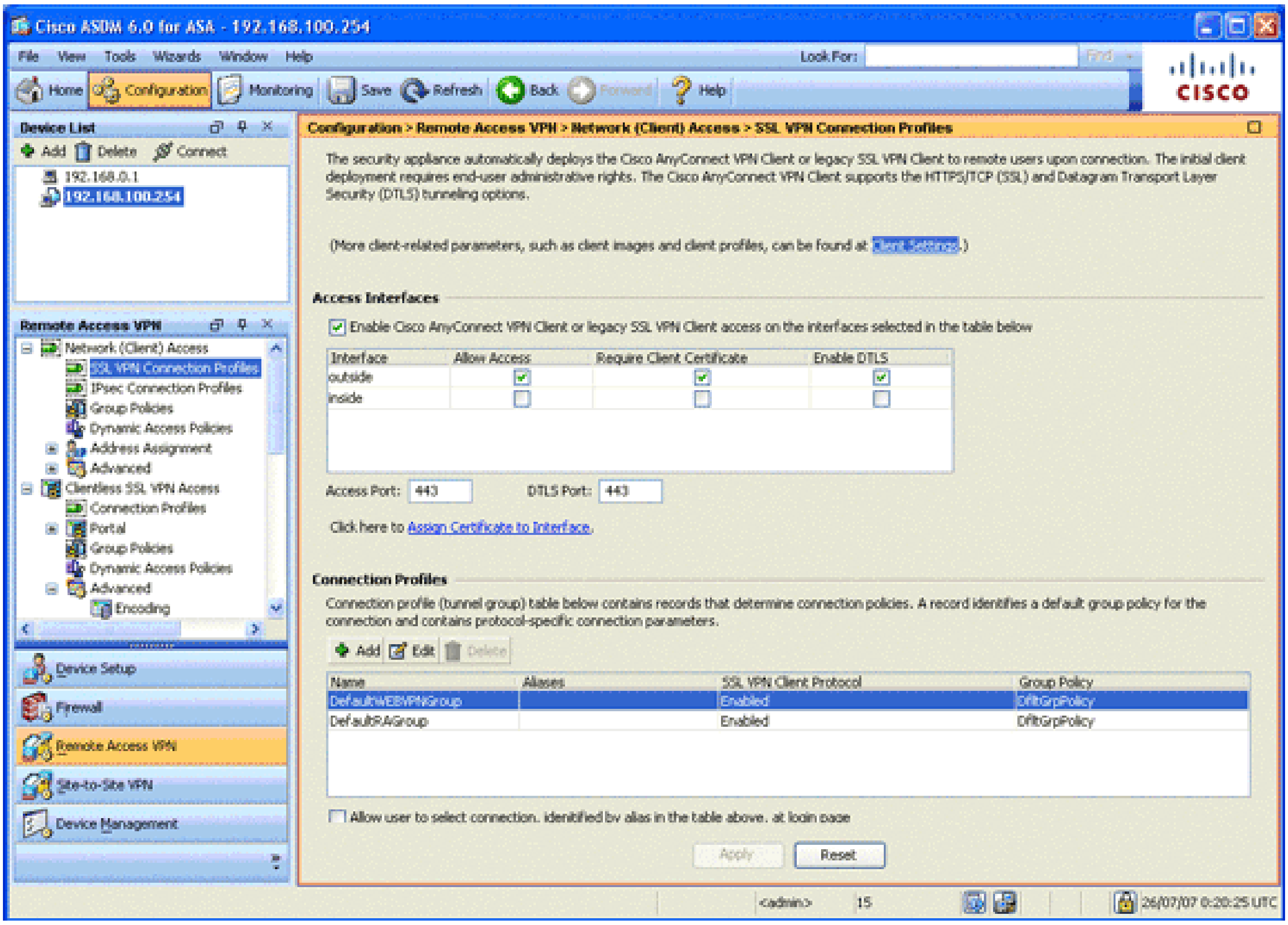
SSL VPN Client Localization File

To set the Localization file go to Language Localization.

Cache File System (to hold CSD and SVC images)

Maximum Size: 20 MB

3. 定義DefaultWEBVPNGroup連線配置檔案。在Remote Access VPN區域中，展開**Network(Client)Access**，然後選擇**SSL VPN Connection Profiles**。在Access Interfaces區域中，選中**Enable Cisco AnyConnect VPN Client**覈取方塊。對於外部介面，請選中**Allow Access**、**Require Client Certificate**和**Enable DTLS**覈取方塊，如下圖所示：



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

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at Client Settings.)

Access Interfaces

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

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	☑	☑	☑
inside	□	□	□

Access Port: 443 DTLS Port: 443

Click here to Assign Certificate to Interface.

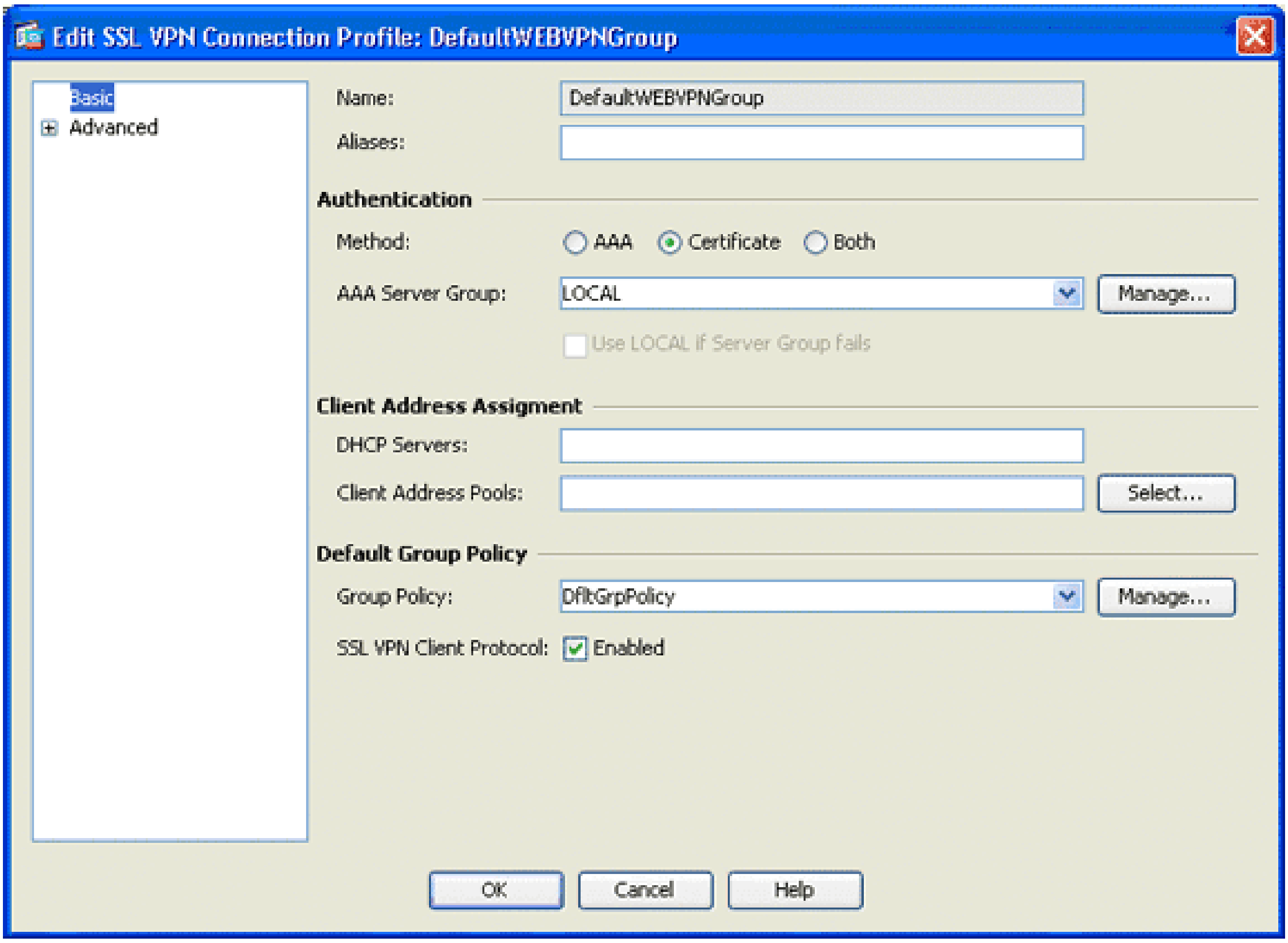
Connection Profiles

Connection profile (tunnel group) table below contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters.

Name	Aliases	SSL VPN Client Protocol	Group Policy
DefaultWEBVPNGroup		Enabled	DfltGrpPolicy
DefaultRAGroup		Enabled	DfltGrpPolicy

□ Allow user to select connection, identified by alias in the table above, at login page

在「連線配置檔案」區域中，選擇**DefaultWEBVPNGroup**，然後按一下**Edit**。系統將顯示Edit SSL VPN Connection Profile對話方塊。



Name: DefaultWEBVPNGroup

Aliases:

Authentication

Method: ○ AAA ● Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools:

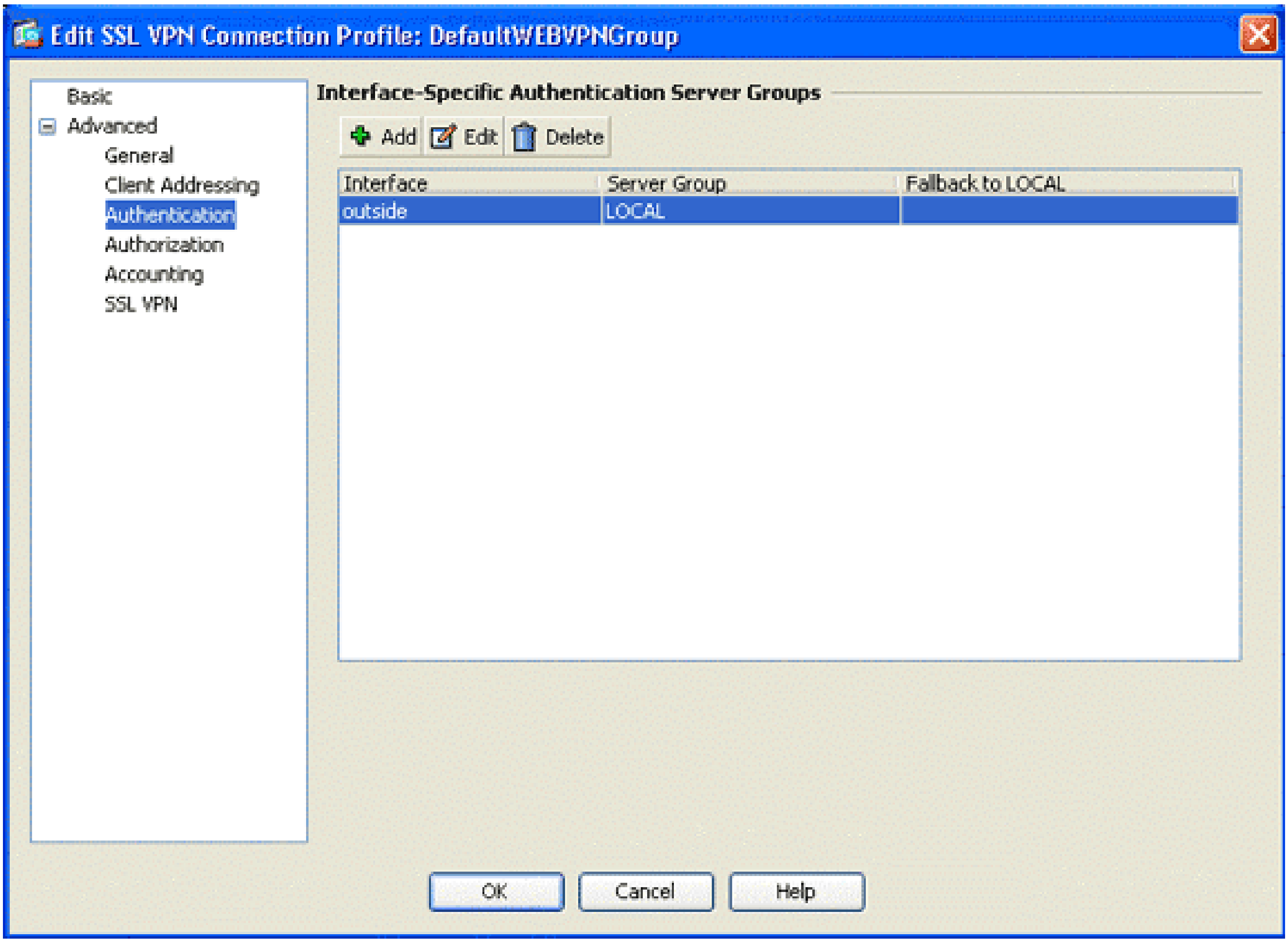
Default Group Policy

Group Policy: DfltGrpPolicy

SSL VPN Client Protocol: ☑ Enabled

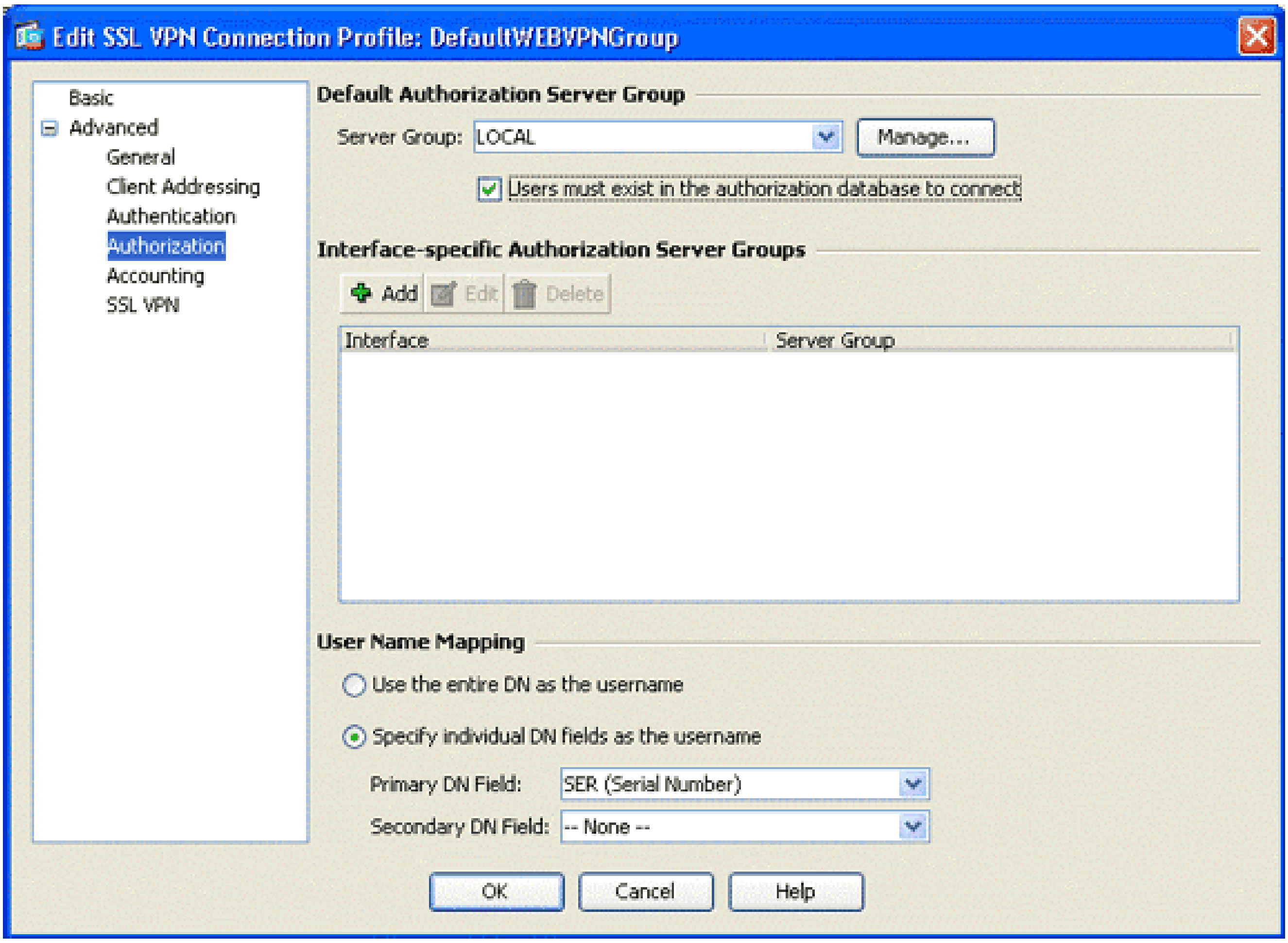
在導航區域中，選擇**Basic**。在Authentication區域中，按一下**Certificate**單選按鈕。在Default

Group Policy區域中，選中**SSL VPN Client Protocol**複選框。展開**Advanced**，然後選擇**Authentication**。按一下**Add**，然後使用本機伺服器群組新增外部介面，如下圖所示：



Interface	Server Group	Fallback to LOCAL
outside	LOCAL	

在導航區域中，選擇**Authorization**。在Default Authorization Server Group區域中，從Server Group下拉選單中選擇**LOCAL**，並選中**Users must exist in the authorization database to connect**複選框。在User Name Mapping區域中，從Primary DN Field下拉選單中選擇**SER(Serial Number)**，從Secondary DN Field中選擇**None**，然後按一下**OK**。



Edit SSL VPN Connection Profile: DefaultWEBVPNGroup

Default Authorization Server Group

Server Group: LOCAL

☑ Users must exist in the authorization database to connect

Interface-specific Authorization Server Groups

Interface	Server Group

User Name Mapping

○ Use the entire DN as the username

● Specify individual DN fields as the username

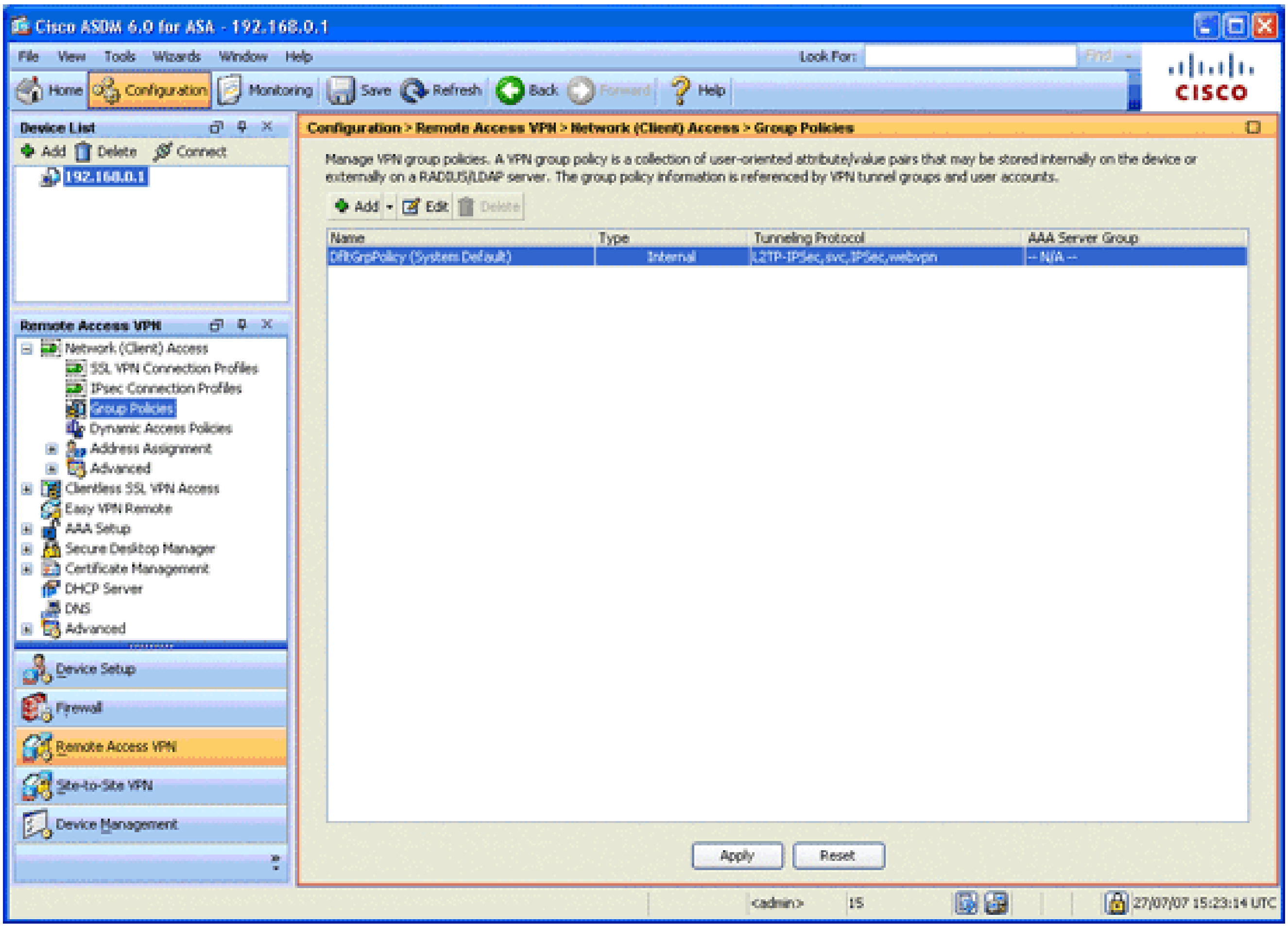
Primary DN Field: SER (Serial Number)

Secondary DN Field: -- None --

步驟7.定義預設組策略

此步驟說明如何定義預設組策略。

1. 在Remote Access VPN區域中，展開**Network(Client)Access**，然後選擇**Group Policies**。

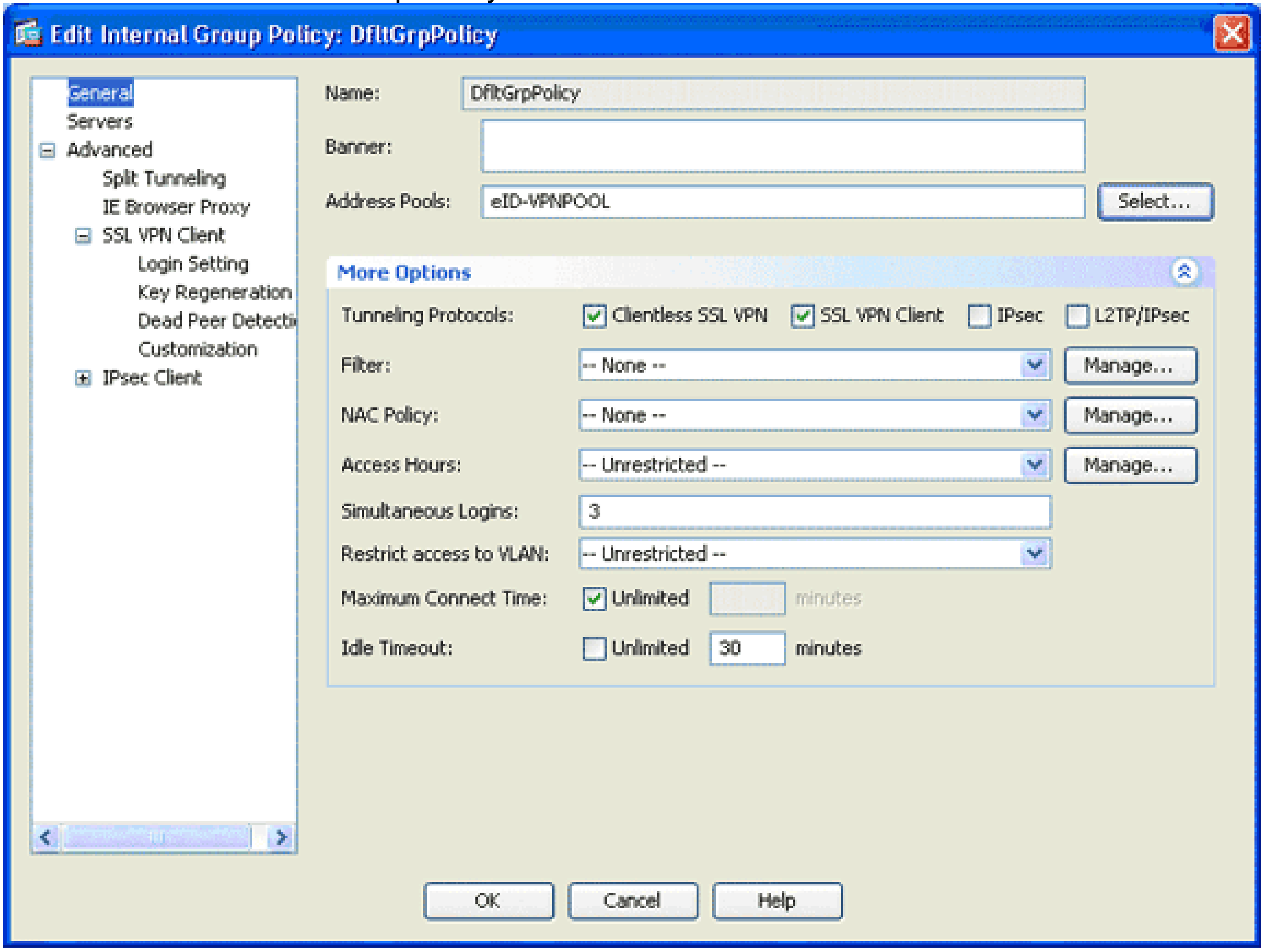


Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	AAA Server Group
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec,svc,IPSec,webvpn	-- N/A --

2. 從組策略清單中選擇**DfltGrpPolicy**，然後按一下**Edit**。
3. 系統將顯示Edit Internal Group Policy對話方塊。



Name: DfltGrpPolicy

Banner:

Address Pools: eID-VPNPOOL

Tunneling Protocols: ☑ Clientless SSL VPN ☑ SSL VPN Client □ IPsec □ L2TP/IPsec

Filter: -- None --

NAC Policy: -- None --

Access Hours: -- Unrestricted --

Simultaneous Logins: 3

Restrict access to VLAN: -- Unrestricted --

Maximum Connect Time: ☑ Unlimited minutes

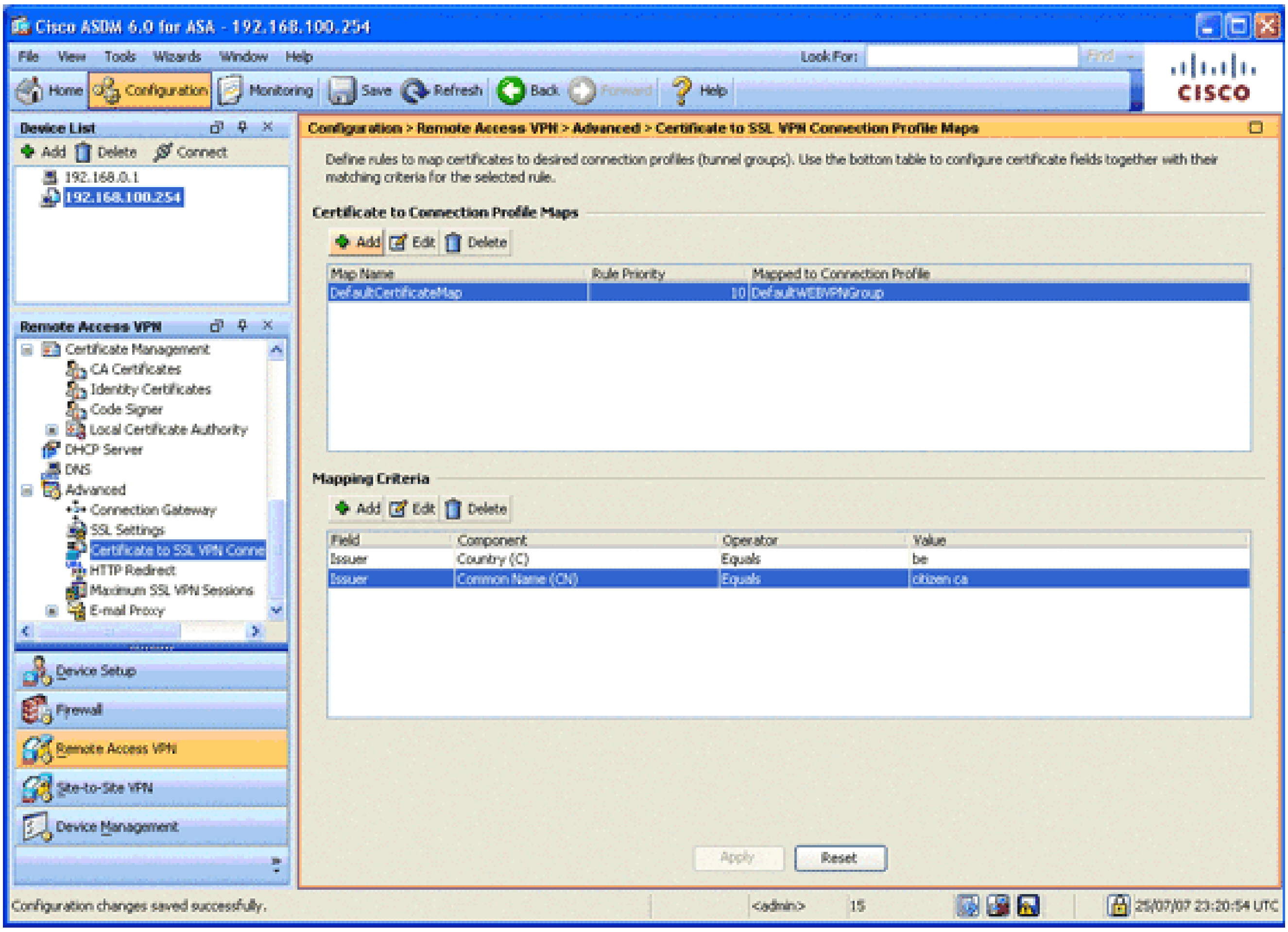
Idle Timeout: □ Unlimited 30 minutes

4. 在導航區中選擇**General**。
5. 對於地址池，按一下**Select**以選擇地址池，然後選擇**eID-VPNPOOL**。
6. 在「更多選項」區域中，取消選中**IPsec**和**L2TP/IPsec**覈取方塊，然後按一下**OK**。

步驟8.定義憑證對應

此步驟描述如何定義證書對映條件。

1. 在Remote Access VPN區域中，按一下**Advanced**，然後選擇**Certificate to SSL VPN Connection Profile Maps**。
2. 在Certificate to Connection Profile Maps區域中，按一下**Add**，然後從對映清單中選擇**DefaultCertificateMap**。此對映必須與Mapped to Connection Profile欄位中的*DefaultWEBVPNProfile*匹配。
3. 在「對映條件」區域中，按一下**新增**，然後新增以下值：欄位:簽發人，國家（地區），等於，「be」欄位:頒發者，公用名(CN)，等於，「公民ca」對映條件應如下圖所示：



Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps

Define rules to map certificates to desired connection profiles (tunnel groups). Use the bottom table to configure certificate fields together with their matching criteria for the selected rule.

Certificate to Connection Profile Maps

Map Name	Rule Priority	Mapped to Connection Profile
DefaultCertificateMap	10	DefaultWEBVPNGroup

Mapping Criteria

Field	Component	Operator	Value
Issuer	Country (C)	Equals	be
Issuer	Common Name (CN)	Equals	citizen ca

Configuration changes saved successfully.

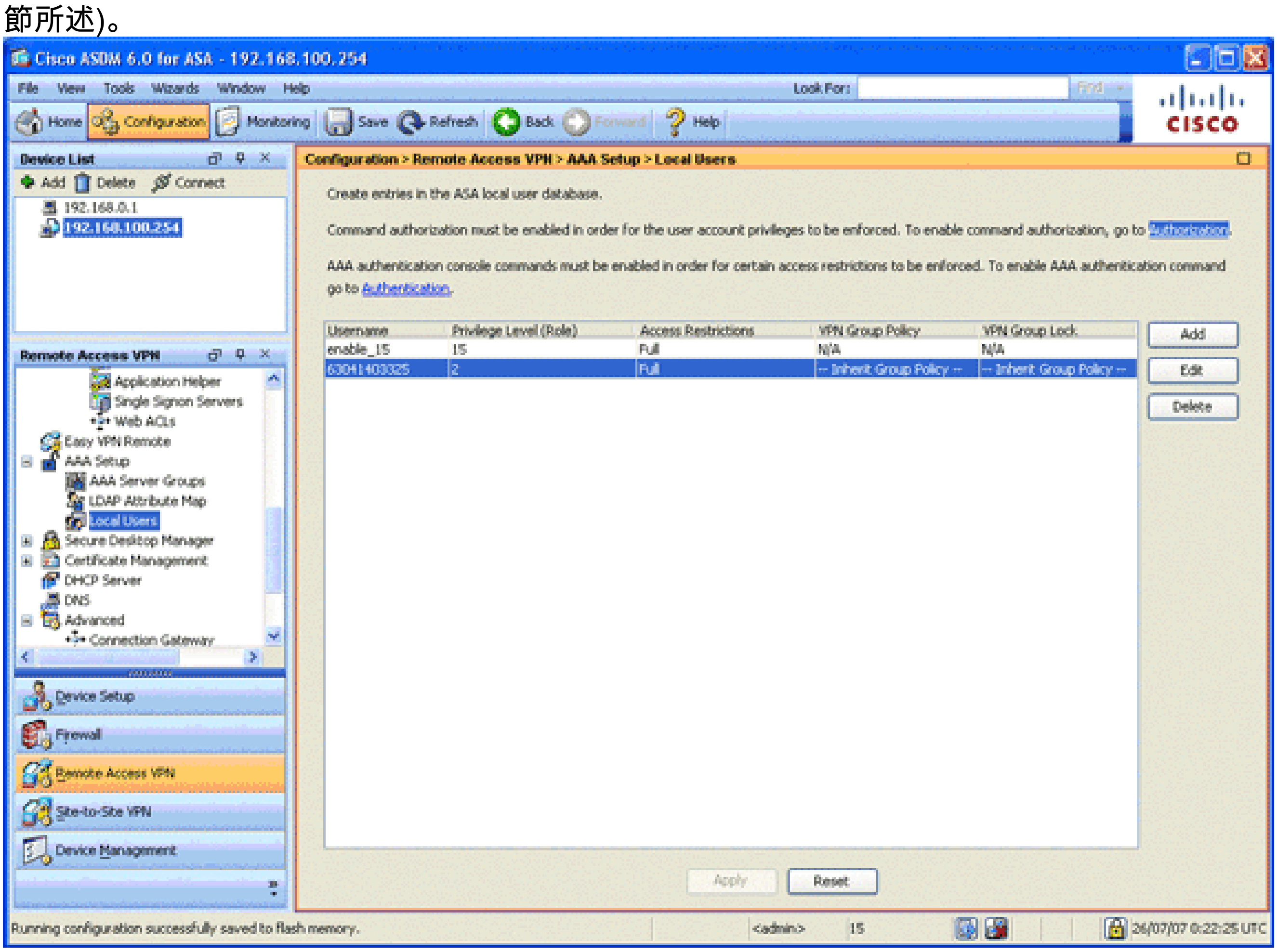
4. 按一下「**Apply**」。

步驟9.新增本地使用者

此步驟說明如何新增本地使用者。

1. 在Remote Access VPN區域中，展開**AAA Setup**，然後選擇**Local Users**。
2. 在「本地使用者」區域中，按一下**新增**。
3. 在Username欄位中，輸入使用者證書的序列號。例如，56100307215(如本檔案的驗證憑證一

節所述)。



Configuration > Remote Access VPN > AAA Setup > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization.

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
enable_15	15	Full	N/A	N/A
63041403325	2	Full	-- Inherit Group Policy --	-- Inherit Group Policy --

Running configuration successfully saved to flash memory.

4. 按一下「Apply」。

步驟10.重新啟動ASA

重新啟動ASA以確保所有更改都應用到系統服務。

微調

測試時，某些SSL隧道可能無法正確關閉。由於ASA假定AnyConnect客戶端可能會斷開連線並重新連線，因此不會丟棄隧道，從而有機會返回。但是，在使用基本許可證（預設情況下為2個SSL隧道）進行實驗室測試期間，如果未正確關閉SSL隧道，則可能會用完您的許可證。如果發生此問題，請使用**vpn-sessiondb logoff <*option*>**命令註銷所有活動的SSL會話。

一分鐘配置

為了快速建立工作配置，請將ASA重置為出廠預設設定，然後在配置模式下貼上此配置：

ciscoasa

```
ciscoasa#conf t
ciscoasa#clear configure all
ciscoasa#domain-name cisco.be
ciscoasa#enable password 9jNfZuG3TC5tCVH0 encrypted
!
interface Vlan1
```

```
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 197.0.100.1 255.255.255.0
interface Ethernet0/0
 switchport access vlan 2
 no shutdown
interface Ethernet0/1
 no shutdown
!
passwd 2KFQnbNIdI.2KYOU encrypted
dns server-group DefaultDNS
 domain-name cisco.be
ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110
mask 255.255.255.0
asdm image disk0:/asdm-602.bin
no asdm history enable
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.255.0 inside
crypto ca trustpoint ASDM_TrustPoint0
 enrollment terminal
 crl configure
crypto ca certificate map DefaultCertificateMap 10
 issuer-name attr c eq be
 issuer-name attr cn eq citizen ca
crypto ca certificate chain ASDM_TrustPoint0
 certificate ca 580b056c5324dbb25057185ff9e5a650
    30820394 3082027c a0030201 02021058 0b056c53
24dbb250 57185ff9 e5a65030
    0d06092a 864886f7 0d010105 05003027 310b3009
06035504 06130242 45311830
    16060355 0403130f 42656c67 69756d20 526f6f74
20434130 1e170d30 33303132
    36323330 3030305a 170d3134 30313236 32333030
30305a30 27310b30 09060355
    04061302 42453118 30160603 55040313 0f42656c
6769756d 20526f6f 74204341
    30820122 300d0609 2a864886 f70d0101 01050003
82010f00 3082010a 02820101
    00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d
c720eb30 915a75f5 e2d2cfc8
    4c149842 58adc711 c540406a 5af97412 2787e99c
e5714e22 2cd11218 aa305ea2
    21b9d9bb fff674eb 3101e73b 7e580f91 164d7689
a8014fad 226670fa 4b1d95c1
    3058eabc d965d89a b488eb49 4652dfd2 531576cb
145d1949 b16f6ad3 d3fdbcc2
    2dec453f 093f58be fcd4ef00 8c813572 bff718ea
96627d2b 287f156c 63d2caca
    7d05acc8 6d076d32 be68b805 40ae5498 563e66f1
30e8efc4 ab935e07 de328f12
    74aa5b34 2354c0ea 6ccefe36 92a80917 eaa12dcf
6ce3841d de872e33 0b3c74e2
    21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b
a7210687 1d27d3c4 a1c94cb0
    6f020301 0001a381 bb3081b8 300e0603 551d0f01
01ff0404 03020106 300f0603
    551d1301 01ff0405 30030101 ff304206 03551d20
```

```
043b3039 30370605 60380101
    01302e30 2c06082b 06010505 07020116 20687474
703a2f2f 7265706f 7369746f
    72792e65 69642e62 656c6769 756d2e62 65301d06
03551d0e 04160414 10f00c56
    9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609
60864801 86f84201 01040403
    02000730 1f060355 1d230418 30168014 10f00c56
9b61ea57 3ab63597 6d9fddb9
    148edbe6 300d0609 2a864886 f70d0101 05050003
82010100 c86d2251 8a61f80f
    966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59
48a74c49 37d773a1 6a01655e
    32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9
5d0f37ba 76d240bd cc2d3fd3
    4441499c fd5b29f4 0223225b 711bbf58 d9284e2d
45f4dae7 b5634544 110d2a7f
    337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1
60f2d787 f6572e7a 7e6a1380
    1ddce3d0 631e3d71 31b160d4 9e08caab f094c748
755481f3 1bad779c e8b28fdb
    83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636
ba218c97 1a21d4ea 2d3bacba
    eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297
fff26e87 7d46c974 d6efeb3d
    7de6596e 069404e4 a2558738 286a225e e2be7412
b004432a
  quit
no crypto isakmp nat-traversal
!
dhcpd address 192.168.0.2-192.168.0.129 inside
dhcpd enable inside
dhcpd address 197.0.100.20-197.0.100.30 outside
dhcpd enable outside
!
service-policy global_policy global
ssl encryption aes256-sha1 aes128-sha1 3des-sha1 rc4-
sha1
ssl certificate-authentication interface outside port
443
webvpn
 enable outside
 svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
 svc enable
certificate-group-map DefaultCertificateMap 10
DefaultWEBVPNGroup
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol svc webvpn
 address-pools value eID-VPNPOOL
username 63041403325 nopassword
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group (outside) LOCAL
 authorization-server-group LOCAL
 authorization-required
 authorization-dn-attributes SER
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
exit
copy run start
```

相關資訊

- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems