Autenticazione ASA 8.x Anyconnect con carta eID belga

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Premesse](#)
[Configurazione PC locale](#)
[Sistema operativo](#)
[Lettore di schede](#)
[Software runtime eID](#)
[Certificato di autenticazione](#)
[Installazione di AnyConnect](#)
[Requisiti dell'ASA](#)
[Configurazione ASA](#)
[Passaggio 1. Abilitare l'interfaccia esterna](#)
[Passaggio 2. Configurare il nome di dominio, la password e l'ora di sistema](#)
[Passaggio 3. Abilitare un server DHCP sull'interfaccia esterna.](#)
[Passaggio 4. Configurare il pool di indirizzi VPN eID](#)
[Passaggio 5. Importazione del certificato CA radice (Belgio)](#)
[Passaggio 6. Configurare Secure Sockets Layer](#)
[Passaggio 7. Definizione dei Criteri di gruppo predefiniti](#)
[Passaggio 8. Definizione del mapping dei certificati](#)
[Passaggio 9. Aggiungere un utente locale](#)
[Passaggio 10. Riavviare l'appliance ASA](#)
[Ottimizzazione](#)
[Configurazione in un minuto](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare l'autenticazione ASA 8.x Anyconnect per usare la scheda eID belga.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA 5505 con il software ASA 8.0 appropriato
- Client AnyConnect
- ASDM 6.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

L'eID è una scheda PKI (Public Key Infrastructure) rilasciata dal governo belga che gli utenti devono utilizzare per l'autenticazione su un PC Windows remoto. Il client software AnyConnect è installato sul PC locale e riceve le credenziali di autenticazione dal PC remoto. Al termine dell'autenticazione, l'utente remoto potrà accedere alle risorse centrali tramite un tunnel SSL completo. All'utente remoto viene assegnato un indirizzo IP ottenuto da un pool gestito dall'ASA.

Configurazione PC locale

Sistema operativo

Il sistema operativo (Windows, MacOS, Unix o Linux) del PC locale deve essere aggiornato e tutte le patch necessarie devono essere installate.

Lettore di schede

Per utilizzare la scheda eID è necessario che sul computer locale sia installato un lettore di schede elettroniche. Il lettore di schede elettroniche è un dispositivo hardware che stabilisce un canale di comunicazione tra i programmi sul computer e il chip sulla scheda ID.

Per un elenco dei lettori di schede approvati, fare riferimento al seguente URL: http://www.cardreaders.be/en/default.htm

Nota: per utilizzare il lettore di schede, è necessario installare i driver consigliati dal fornitore dell'hardware.

Software runtime eID

Ènecessario installare il software runtime eID fornito dal governo belga. Questo software consente all'utente remoto di leggere, convalidare e stampare il contenuto della scheda eID. Il software è disponibile in francese e olandese per Windows, MAC OS X e Linux.

Per ulteriori informazioni, fare riferimento a questo URL:

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

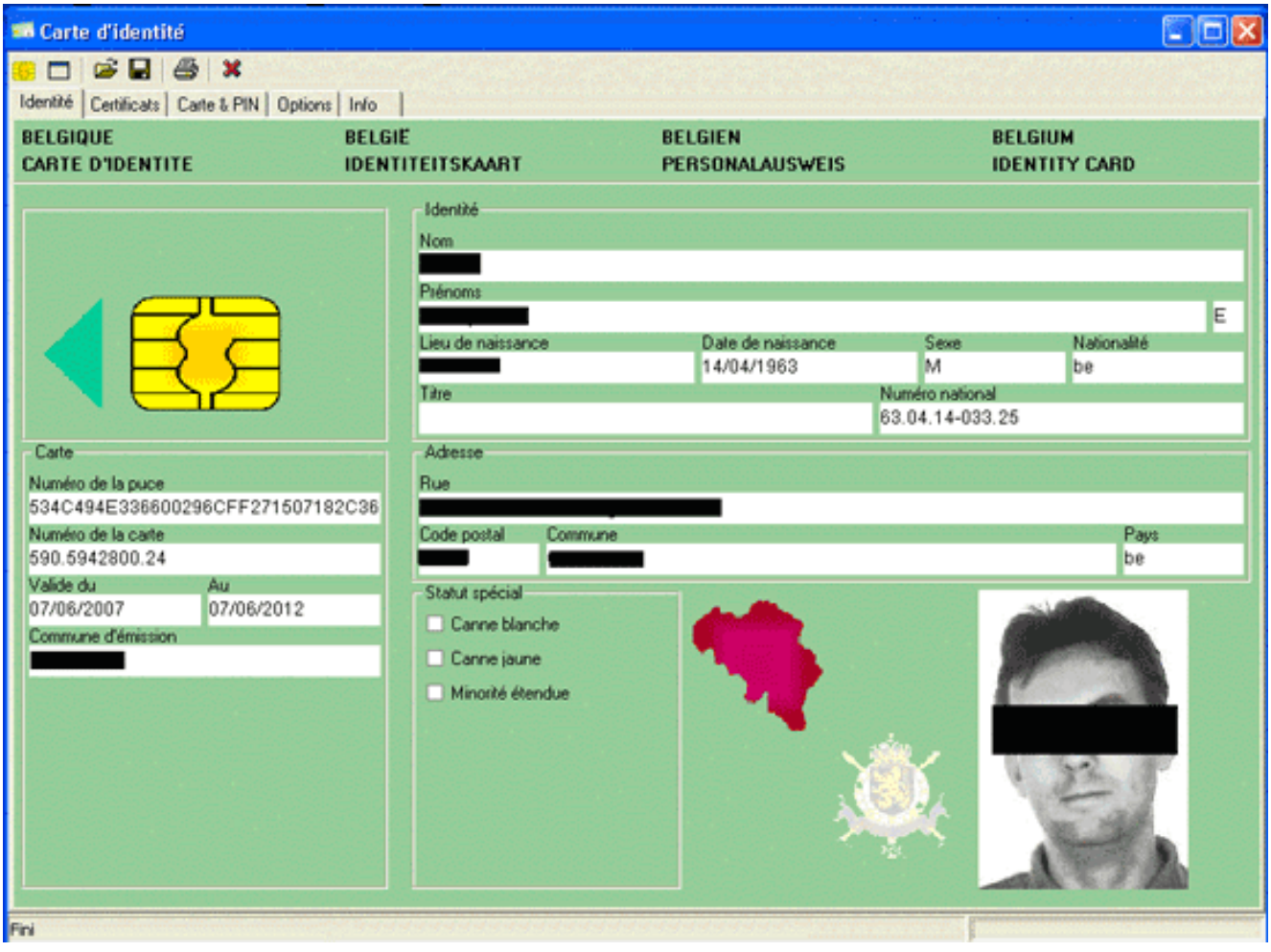
Certificato di autenticazione

Ènecessario importare il certificato di autenticazione nell'archivio di Microsoft Windows nel PC locale. Se non si importa il certificato nell'archivio, il client AnyConnect non sarà in grado di stabilire una connessione SSL all'appliance ASA.

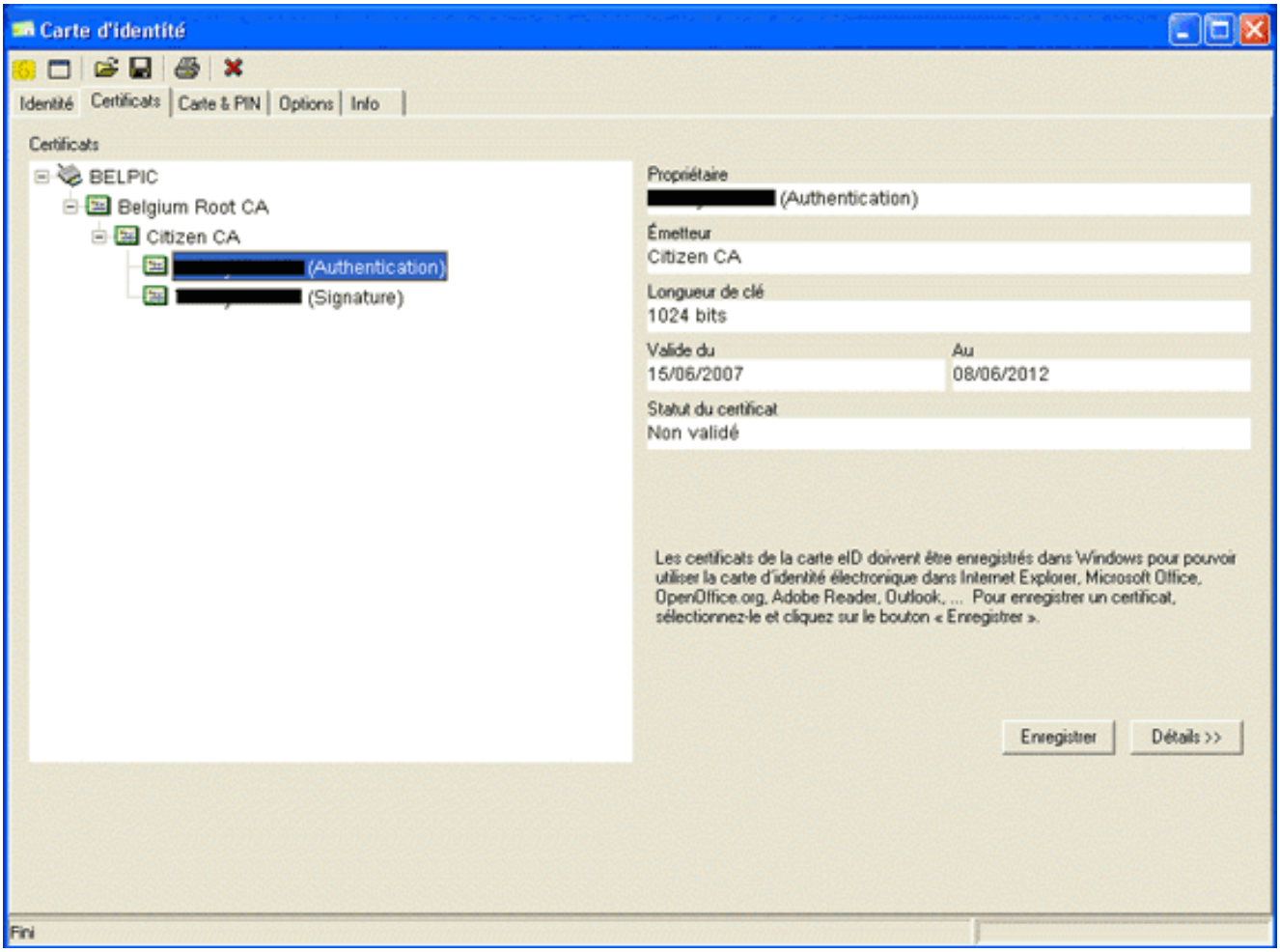
Procedura

Per importare il certificato di autenticazione nell'archivio di Windows, eseguire la procedura seguente:

1. Inserire l'eID nel lettore di schede e avviare il middleware per accedere al contenuto della scheda eID.Viene visualizzato il contenuto della scheda eID.



2. Fare clic sulla scheda **Certificati** (FR).Viene visualizzata la gerarchia dei certificati.



3. Espandere **Belgio Root CA**, quindi espandere **Citizen CA**.
4. Scegliere la versione di **autenticazione** del certificato specificato.
5. Fare clic sul pulsante **Registra** (FR).Il certificato viene copiato nell'archivio di Windows.

Nota: quando si fa clic sul pulsante **Dettagli**, viene visualizzata una finestra che mostra i dettagli relativi al certificato. Per visualizzare il campo Numero di serie della scheda Dettagli, selezionare il campo **Oggetto**. Il campo Numero di serie contiene un valore univoco utilizzato per l'autorizzazione dell'utente. Ad esempio, il numero seriale "56100307215" rappresenta un utente la cui data di nascita è il 3 ottobre 1956 con un numero progressivo di 072 e una cifra di controllo di 15. *Per memorizzare questi numeri, è necessario presentare una richiesta di approvazione da parte delle autorità federali. È responsabilità dell'utente fare le dichiarazioni ufficiali appropriate relative alla manutenzione di una banca dati dei cittadini belgi nel suo paese*.

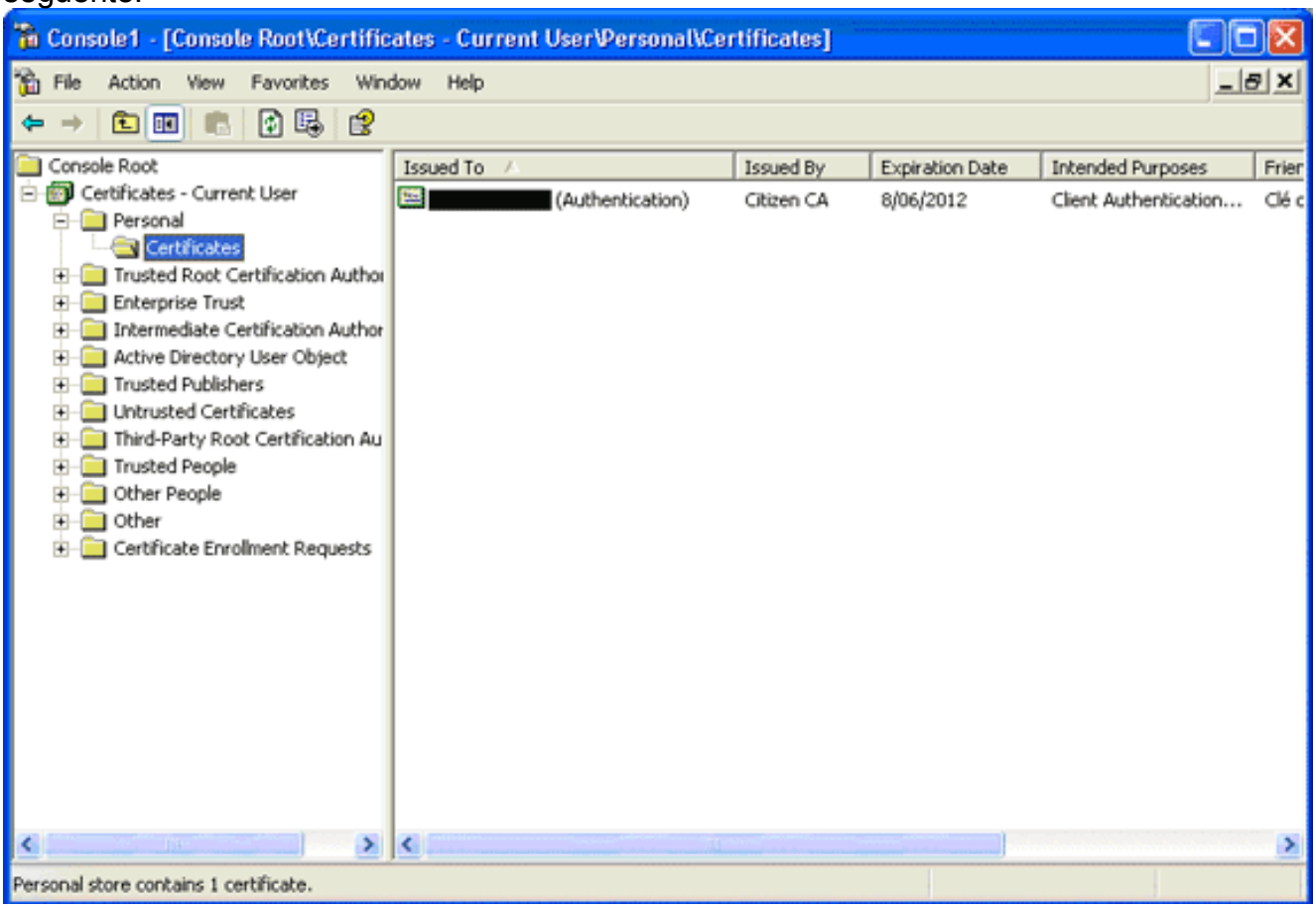
Verifica

Per verificare che il certificato sia stato importato correttamente, eseguire la procedura seguente:

1. Su un computer Windows XP, aprire una finestra DOS e digitare il comando **mmc**.Viene visualizzata l'applicazione Console.
2. Scegliete **File > Aggiungi/Rimuovi snap-in** (o premete Ctrl+M).Verrà visualizzata la finestra di dialogo Aggiungi/Rimuovi snap-in.
3. Fare clic sul pulsante **Aggiungi**.Verrà visualizzata la finestra di dialogo Aggiungi snap-in autonomo.
4. Nell'elenco Snap-in autonomi disponibili selezionare **Certificati** e quindi fare clic su **Aggiungi**.
5. Fare clic sul pulsante di opzione **Account utente** e quindi su **Fine**.Lo snap-in Certificato verrà visualizzato nella finestra di dialogo Aggiungi/Rimuovi snap-in.
6. Fare clic su **Chiudi** per chiudere la finestra di dialogo Aggiungi snap-in autonomo e quindi su

OK nella finestra di dialogo Aggiungi/Rimuovi snap-in per salvare le modifiche e tornare all'applicazione Console.

7. Nella cartella Directory principale della console espandere **Certificati - Utente corrente**.
8. Espandere **Personale**, quindi **Certificati**.Il certificato importato deve essere visualizzato nell'archivio di Windows come illustrato nell'immagine seguente:



Installazione di AnyConnect

Ènecessario installare il client AnyConnect sul PC remoto. Il software AnyConnect utilizza un file di configurazione XML che può essere modificato per preimpostare un elenco di gateway disponibili. Il file XML è archiviato nel percorso seguente nel PC remoto:

C:\Documents e impostazioni*%USERNAME%*\Application Data\Cisco\Cisco AnyConnect VPN Client

dove *%USERNAME%* è il nome dell'utente sul PC remoto.

Il nome del file XML è *preferences.xml*. Di seguito è riportato un esempio del contenuto del file:

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

dove *192.168.0.1* è l'indirizzo IP del gateway ASA.

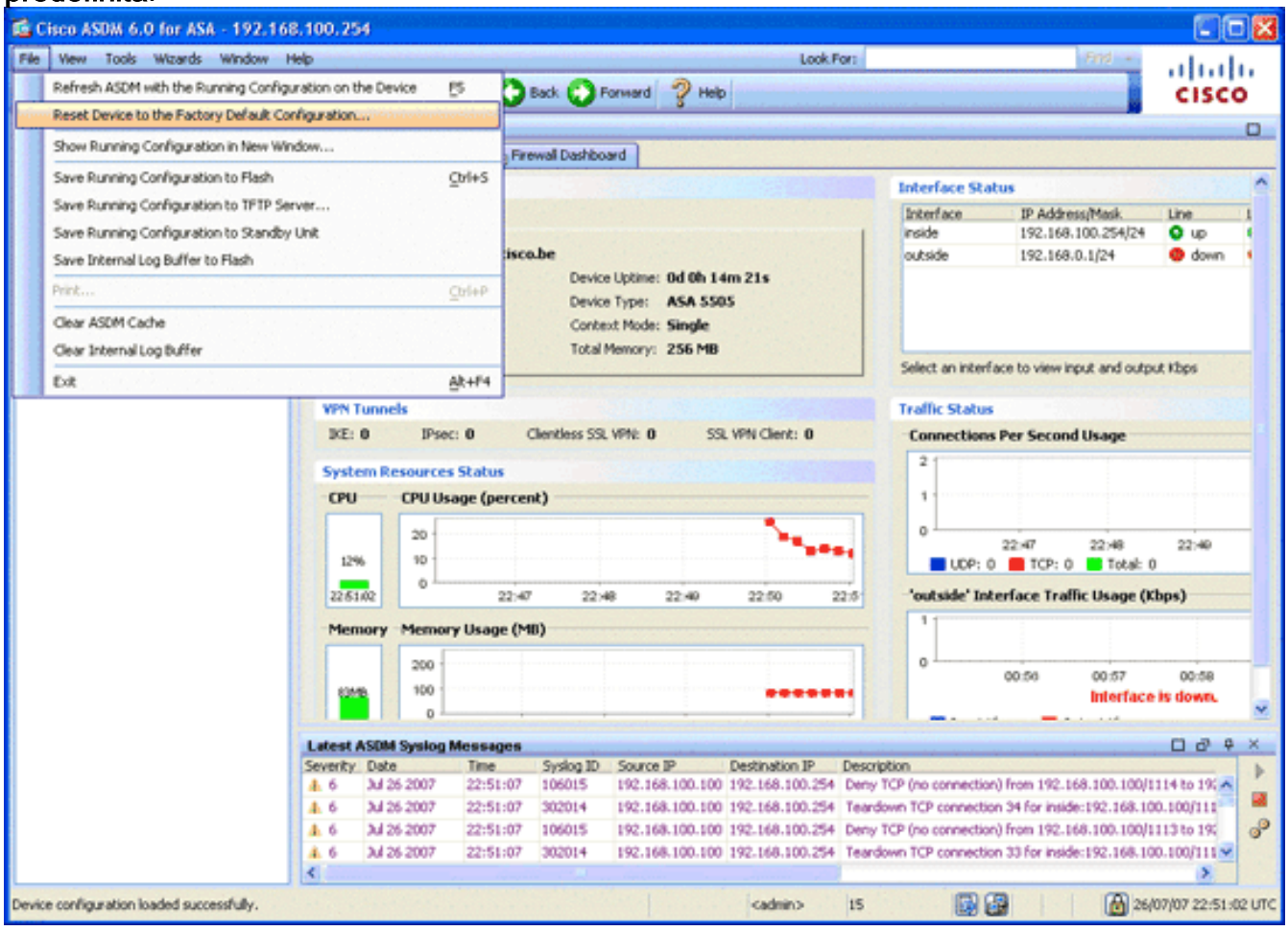
Requisiti dell'ASA

Verificare che l'ASA soddisfi i seguenti requisiti:

- AnyConnect e ASDM devono essere eseguiti nella memoria flash.Per completare le procedure descritte in questo documento, usare un'appliance ASA 5505 con il software ASA 8.0 appropriato installato. Le applicazioni AnyConnect e ASDM devono essere precaricate nella memoria flash. Usare il comando **show flash** per visualizzare il contenuto del flash:

```
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
```

- L'appliance ASA deve essere eseguita con i valori predefiniti.Se si usa un nuovo chassis ASA per completare le procedure descritte in questo documento, è possibile ignorare questo requisito. In caso contrario, completare questa procedura per ripristinare l'ASA ai valori predefiniti:Nell'applicazione ASDM, connettersi allo chassis ASA e scegliere **File > Reimposta dispositivo alla configurazione predefinita**.



Lasciare i valori predefiniti nel modello.Collegare il PC all'interfaccia Ethernet 0/1 interna e rinnovare l'indirizzo IP su cui verrà eseguito il provisioning dal server DHCP dell'appliance ASA.**Nota:** per ripristinare le impostazioni predefinite dell'ASA dalla riga di comando, usare i seguenti comandi:

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

Configurazione ASA

Dopo aver ripristinato le impostazioni predefinite dell'ASA, è possibile avviare ASDM su

192.168.0.1 per collegarsi all'ASA sull'interfaccia Ethernet 0/1 interna.

Nota: la password precedente viene mantenuta (o può essere vuota per impostazione predefinita).

Per impostazione predefinita, l'ASA accetta una sessione di gestione in entrata con un indirizzo IP di origine nella subnet 192.168.0.0/24. Il server DHCP predefinito abilitato sull'interfaccia interna dell'ASA fornisce gli indirizzi IP compresi nell'intervallo 192.168.0.2-129/24, validi per la connessione all'interfaccia interna con ASDM.

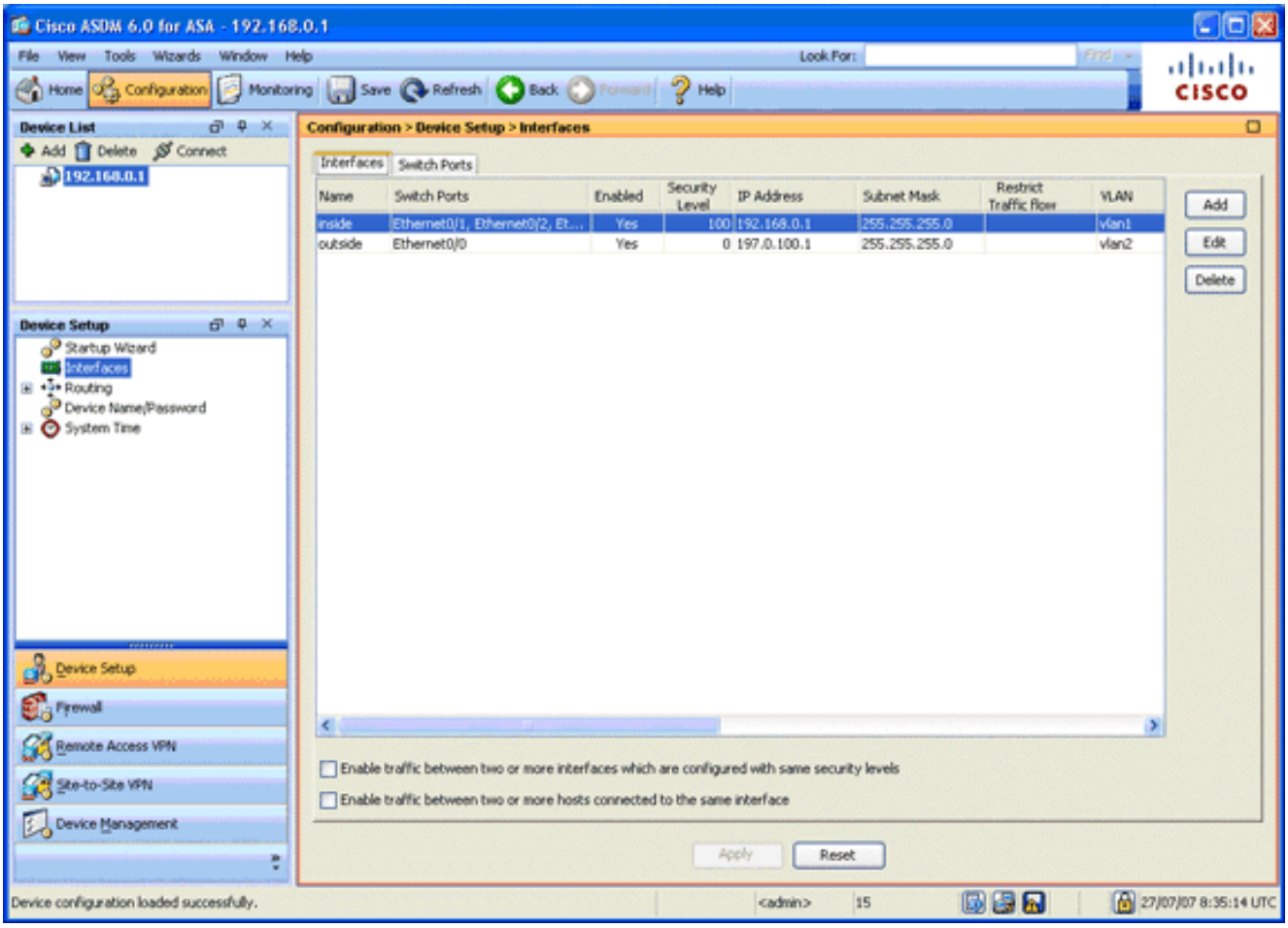
Per configurare l'ASA, effettuare i seguenti passaggi:

1. Abilita interfaccia esterna
2. Configurare il nome di dominio, la password e l'ora di sistema
3. Abilitare un server DHCP sull'interfaccia esterna
4. Configurare il pool di indirizzi VPN eID
5. Importa certificato CA radice (Belgio)
6. Configura Secure Sockets Layer
7. Definire i Criteri di gruppo predefiniti
8. Definisci mapping certificati
9. Aggiungi utente locale
10. Riavviare l'appliance ASA

Passaggio 1. Abilitare l'interfaccia esterna

In questo passaggio viene descritto come abilitare l'interfaccia esterna.

1. Nell'applicazione ASDM, fare clic su **Configuration**, quindi su **Device Setup**.
2. Nell'area Device Setup, selezionare **Interfacce**, quindi fare clic sulla scheda **Interfacce**.

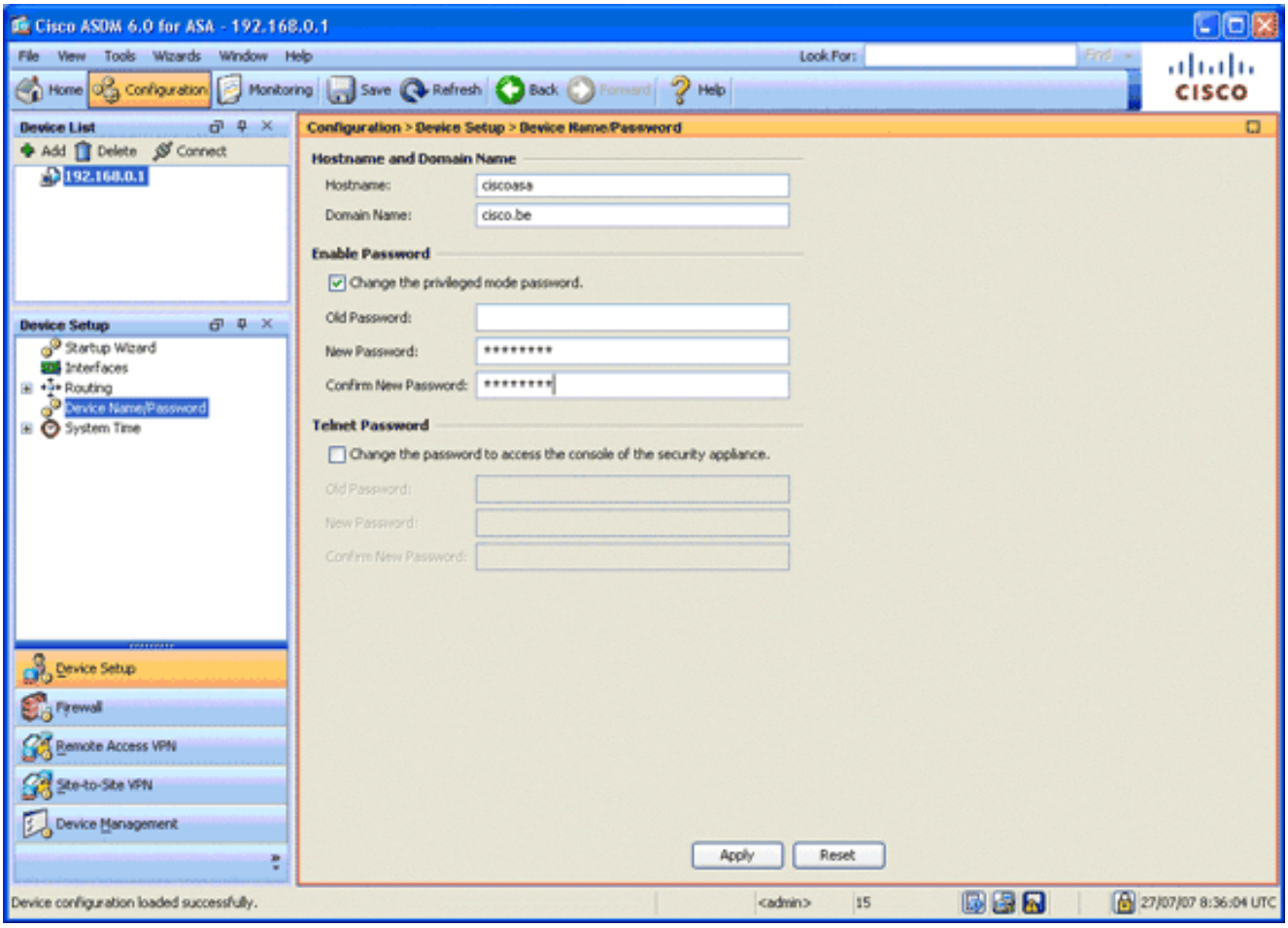


3. Selezionare l'interfaccia esterna e fare clic su **Modifica**.
4. Nella sezione Indirizzo IP della scheda Generale, scegliere l'opzione **Usa indirizzo IP statico**.
5. Immettere **197.0.100.1** per l'indirizzo IP e **255.255.255.0** per la subnet mask.
6. Fare clic su **Apply** (Applica).

Passaggio 2. Configurare il nome di dominio, la password e l'ora di sistema

In questo passaggio viene descritto come configurare il nome di dominio, la password e l'ora di sistema.

1. Nell'area Device Setup (Configurazione dispositivo), selezionare **Device Name/Password** (Nome/password
dispositivo).

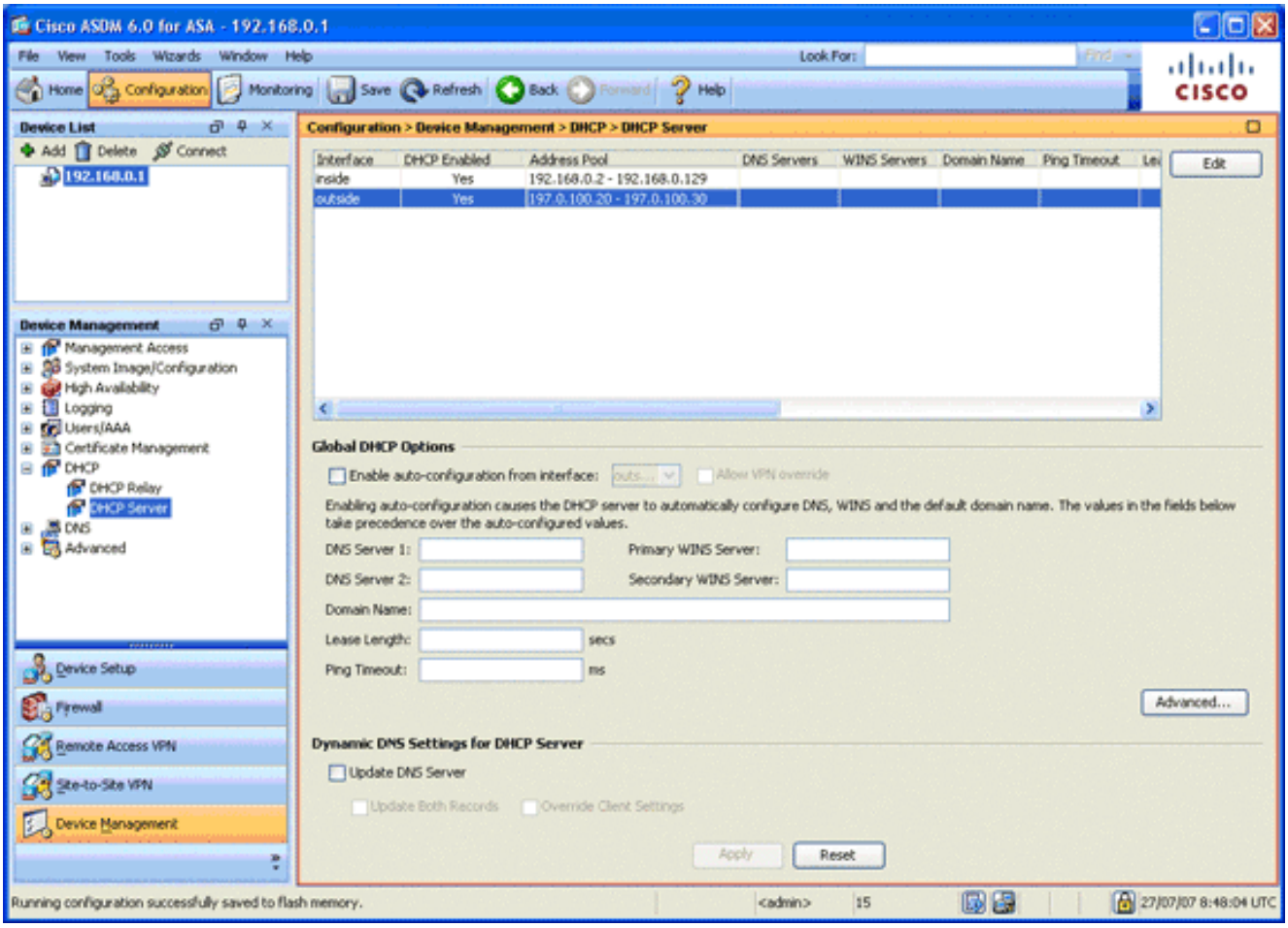


2. Immettere **cisco.be** come nome di dominio e **cisco123** come valore per Abilita password.**Nota:** per impostazione predefinita, la password è vuota.
3. Fare clic su **Apply** (Applica).
4. Nell'area Device Setup (Configurazione dispositivo), selezionare **System Time** (Ora di sistema), quindi modificare il valore dell'orologio (se necessario).
5. Fare clic su **Apply** (Applica).

Passaggio 3. Abilitare un server DHCP sull'interfaccia esterna.

In questo passaggio viene descritto come abilitare un server DHCP sull'interfaccia esterna per semplificare il test.

1. Fare clic su **Configurazione** e quindi su **Gestione dispositivi**.
2. Nell'area Device Management (Gestione dispositivi), espandere **DHCP**, quindi selezionare **DHCP**
   Server.

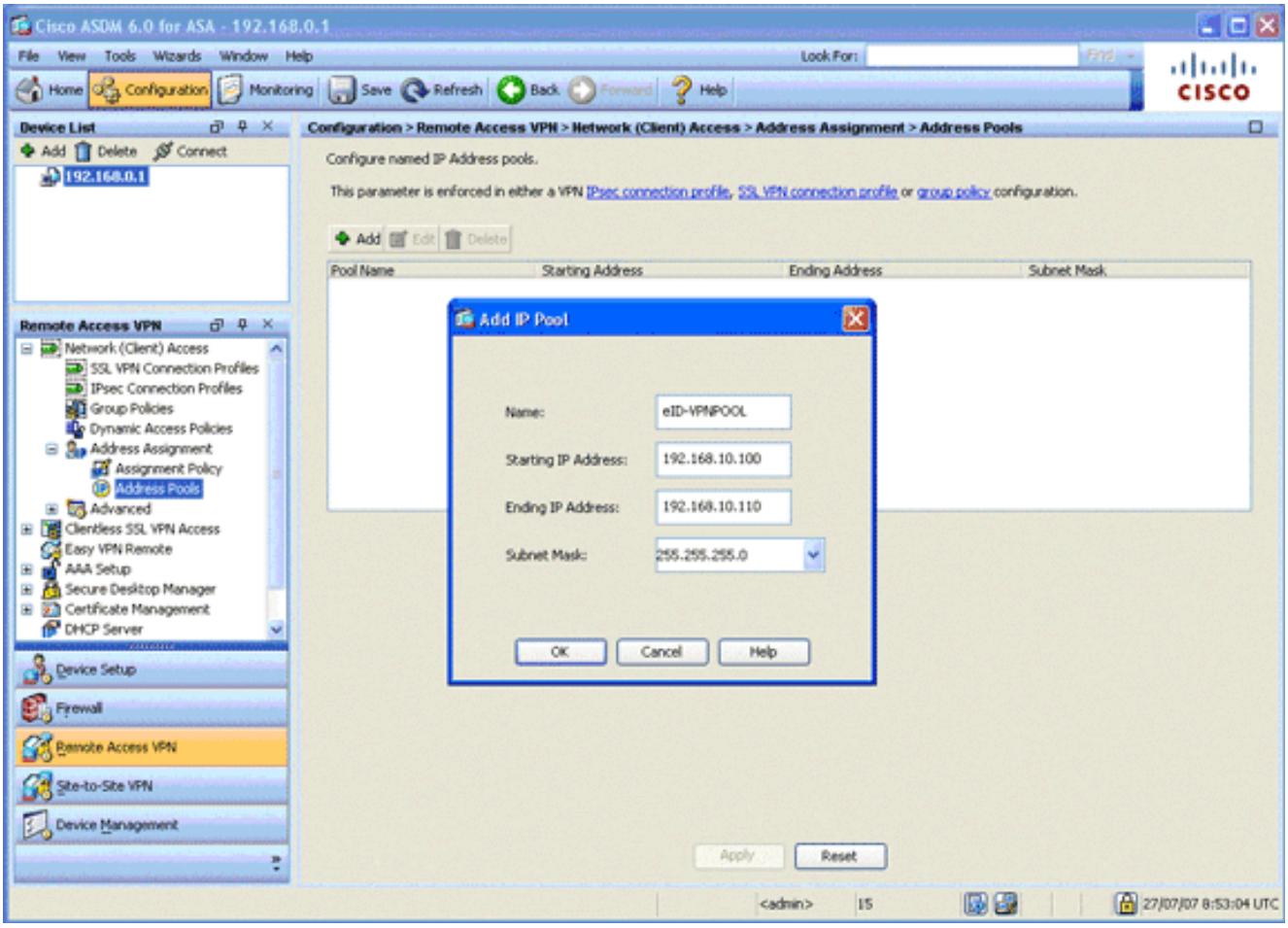


3. Selezionare l'interfaccia esterna dall'elenco Interfaccia e fare clic su **Modifica**.Verrà visualizzata la finestra di dialogo Modifica server DHCP.
4. Selezionare la casella di controllo **Abilita server DHCP**.
5. Nel pool di indirizzi DHCP, immettere un indirizzo IP compreso tra 197.0.100.20 e 197.0.100.30.
6. Nell'area Global DHCP Options (Opzioni DHCP globali), deselezionare la casella di controllo **Enable auto-configuration from interface (Abilita configurazione automatica dall'interfaccia)**.
7. Fare clic su **Apply** (Applica).

Passaggio 4. Configurare il pool di indirizzi VPN eID

In questo passaggio viene descritto come definire un pool di indirizzi IP da utilizzare per effettuare il provisioning dei client AnyConnect remoti.

1. Fare clic su **Configurazione** e quindi su **VPN ad accesso remoto**.
2. Nell'area Rimuovi VPN accesso espandere **Accesso di rete (client)**, quindi **Assegnazione indirizzo**.
3. Scegliere **Pool di indirizzi**, quindi fare clic sul pulsante **Aggiungi** nell'area Configura pool di indirizzi IP denominati.Verrà visualizzata la finestra di dialogo Aggiungi pool IP.



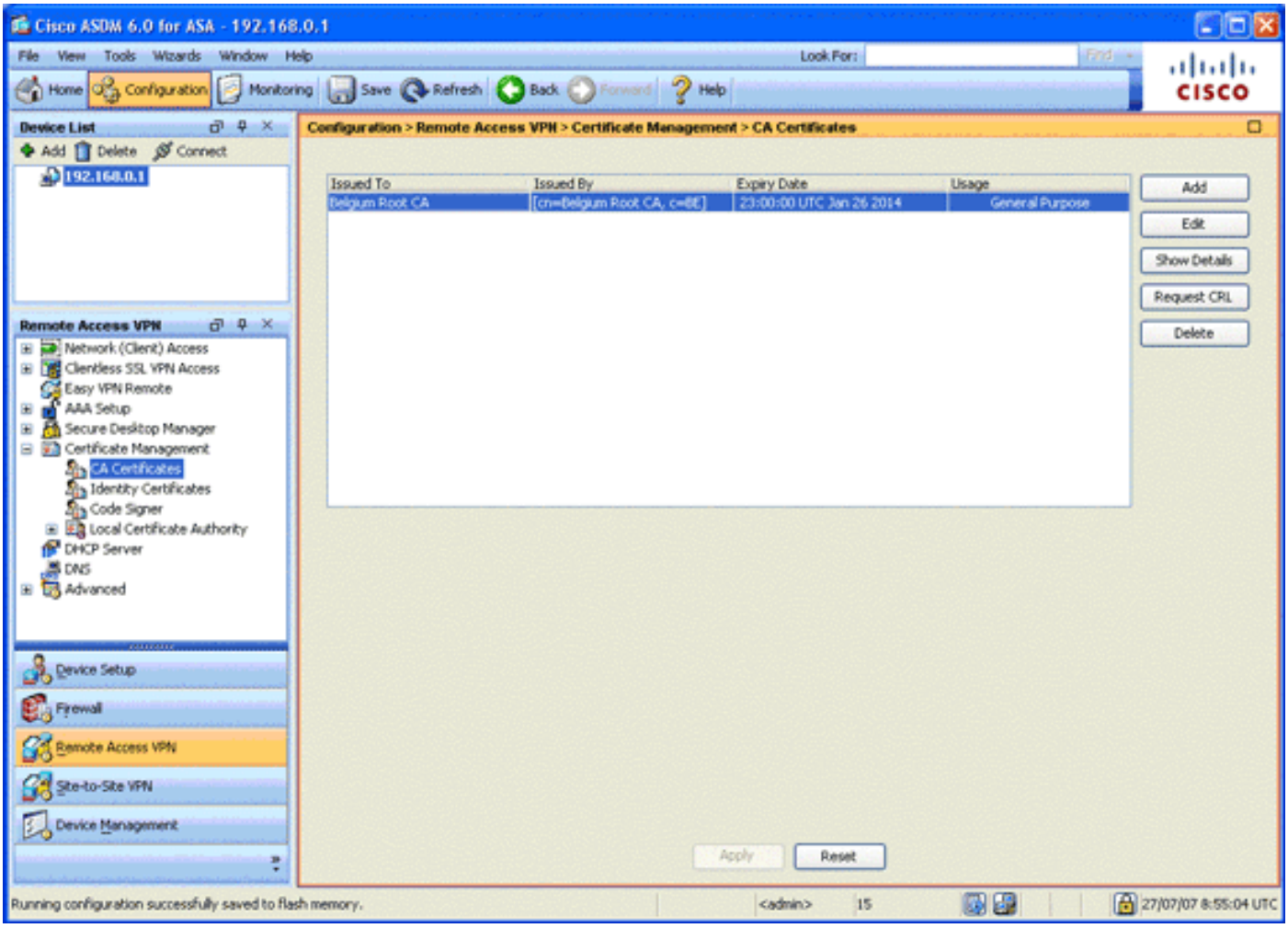
4. Nel campo Nome, immettere **eID-VPNPOOL**.
5. Nei campi Indirizzo IP iniziale e Indirizzo IP finale immettere un intervallo di indirizzi IP compreso tra 192.168.10.100 e 192.168.10.110.
6. Selezionare **255.255.255.0** dall'elenco a discesa Subnet mask, fare clic su **OK**, quindi su **Applica**.

Passaggio 5. Importazione del certificato CA radice (Belgio)

In questo passaggio viene descritto come importare nell'appliance ASA il certificato della CA radice (Belgio).

1. Scaricare e installare i certificati CA radice (belgiumrca.crt e belgiumrca2.crt) dal sito Web governativo e memorizzarli sul PC locale.Il sito web del governo belga si trova al seguente indirizzo: http://certs.eid.belgium.be/
2. Nell'area VPN ad accesso remoto espandere **Gestione certificati** e quindi **Certificati CA**.
3. Fare clic su **Add**, quindi su **Install from file**.
4. Selezionare il percorso in cui è stato salvato il file del certificato CA radice (belgiumrca.crt) e fare clic su **Installa certificato**.
5. Per salvare le modifiche, fare clic su **Apply** (Applica).

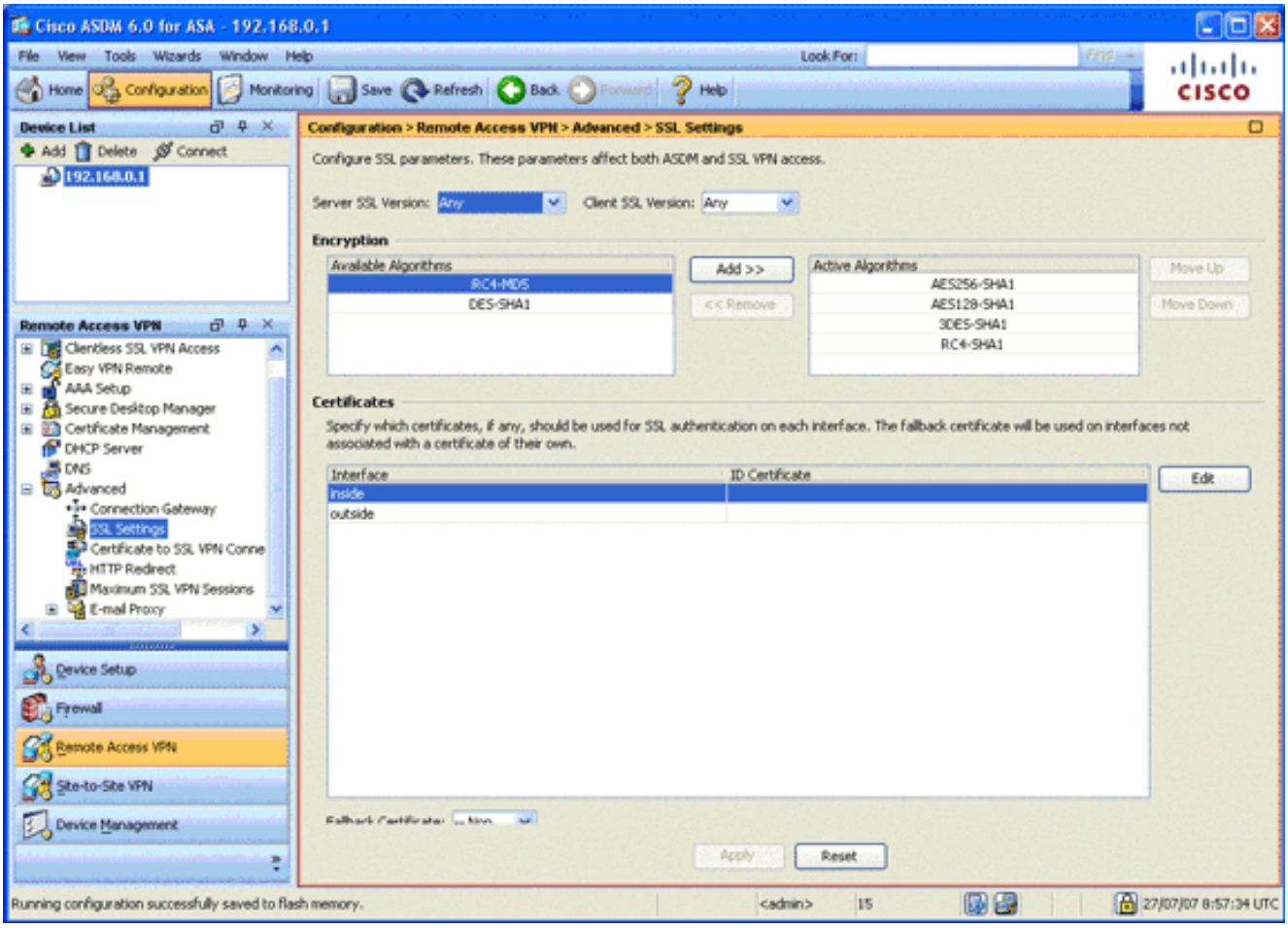
Nell'immagine viene mostrato il certificato installato sull'appliance ASA:



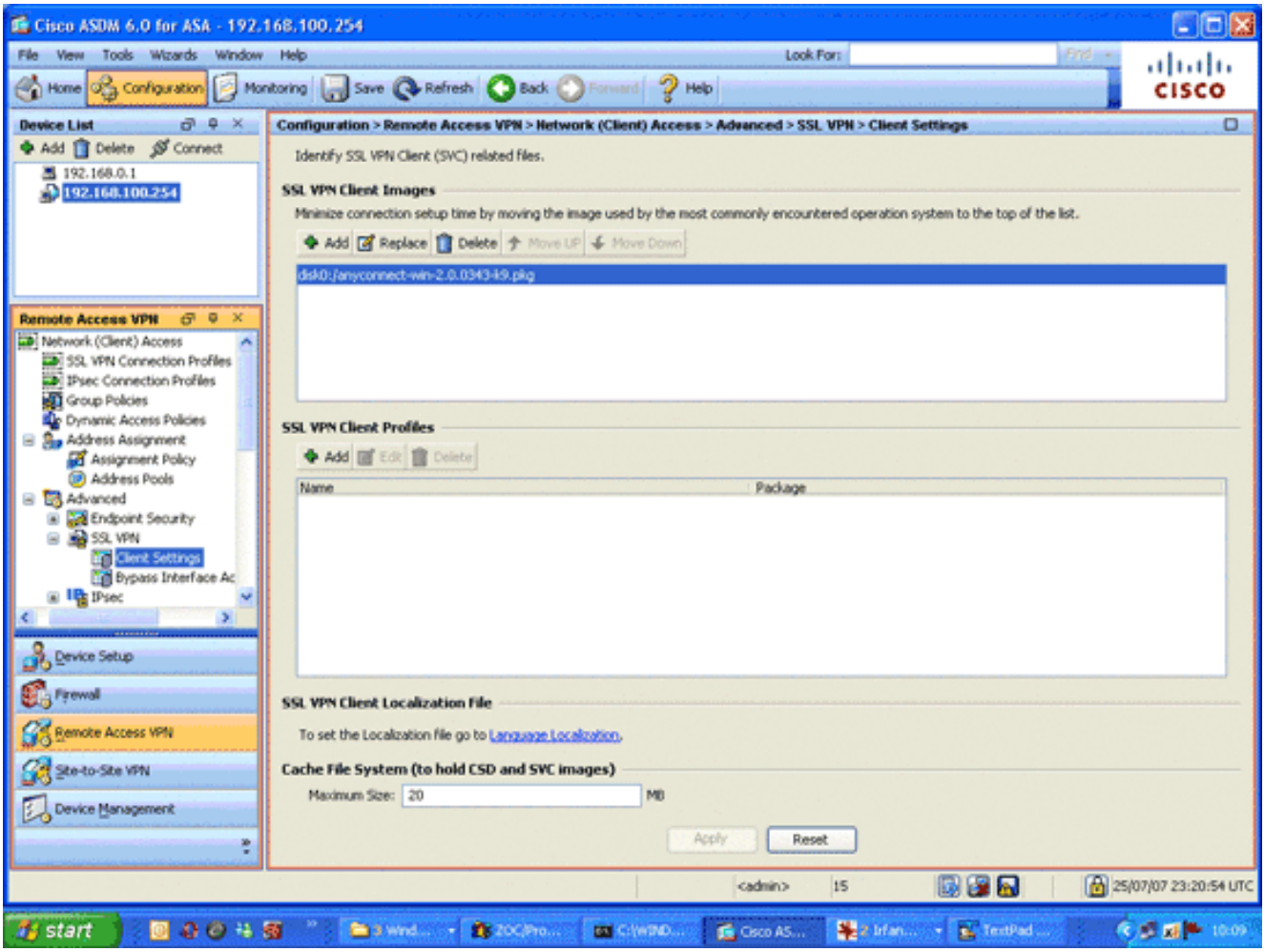
Passaggio 6. Configurare Secure Sockets Layer

In questo passaggio viene descritto come assegnare priorità alle opzioni di crittografia protetta, definire l'immagine client VPN SSL e definire il profilo di connessione.

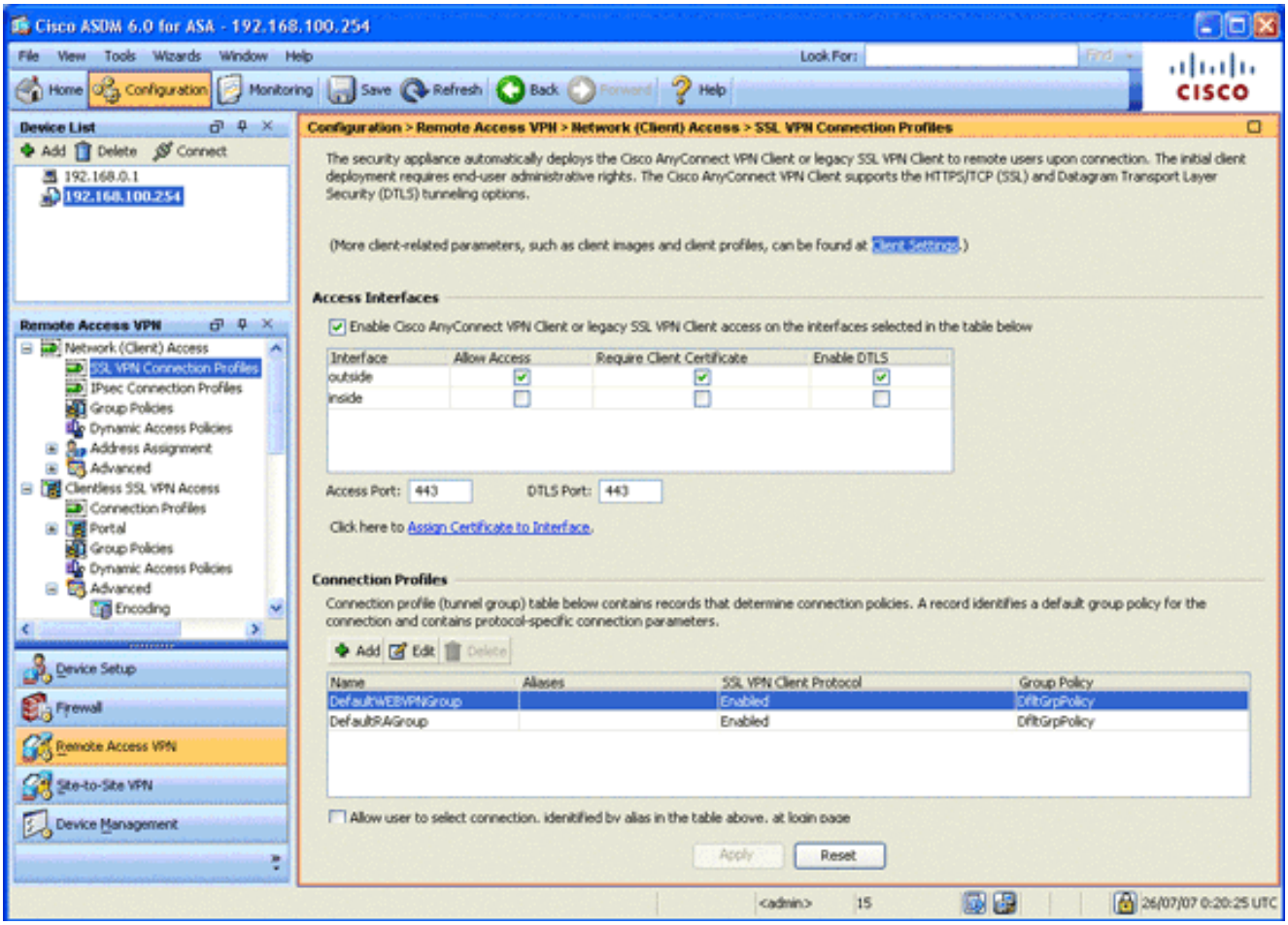
1. Assegnare priorità alle opzioni di crittografia più sicure.Nell'area VPN ad accesso remoto espandere **Avanzate** e scegliere **Impostazioni SSL**. Nella sezione Crittografia, gli algoritmi attivi sono impilati, dall'alto verso il basso, come indicato di seguito:AES256-SHA1AES128-SHA13DES-SHA1RC4-
   SHA1



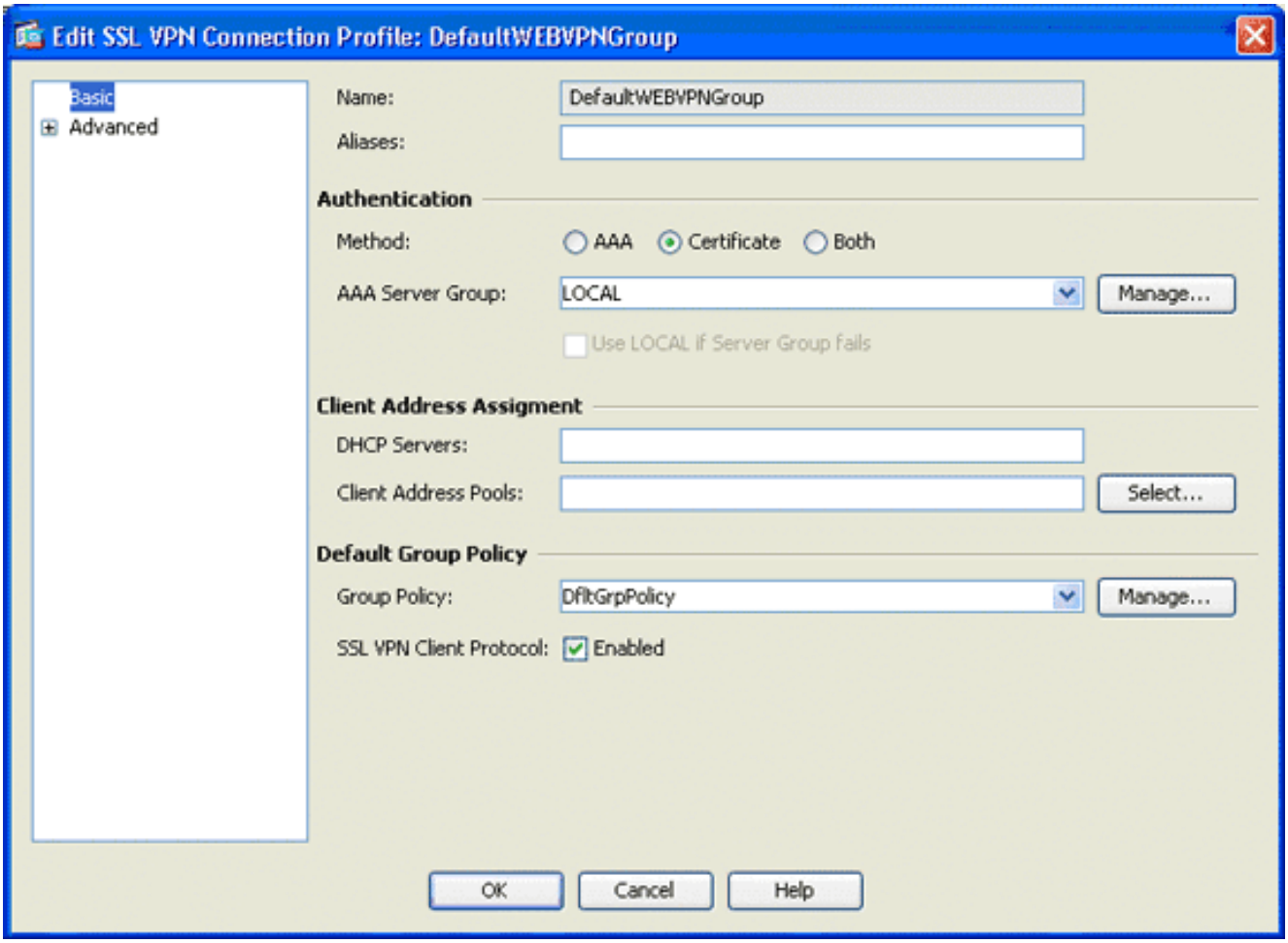
2. Definire l'immagine del client VPN SSL per il client AnyConnect.Nell'area VPN ad accesso remoto espandere **Avanzate**, **SSL VPN** e scegliere **Impostazioni client**.Nell'area Immagini client VPN SSL fare clic su **Aggiungi**.Selezionare il pacchetto AnyConnect archiviato nella memoria flash.Il pacchetto AnyConnect viene visualizzato nell'elenco delle immagini del client VPN SSL come mostrato
nell'immagine:



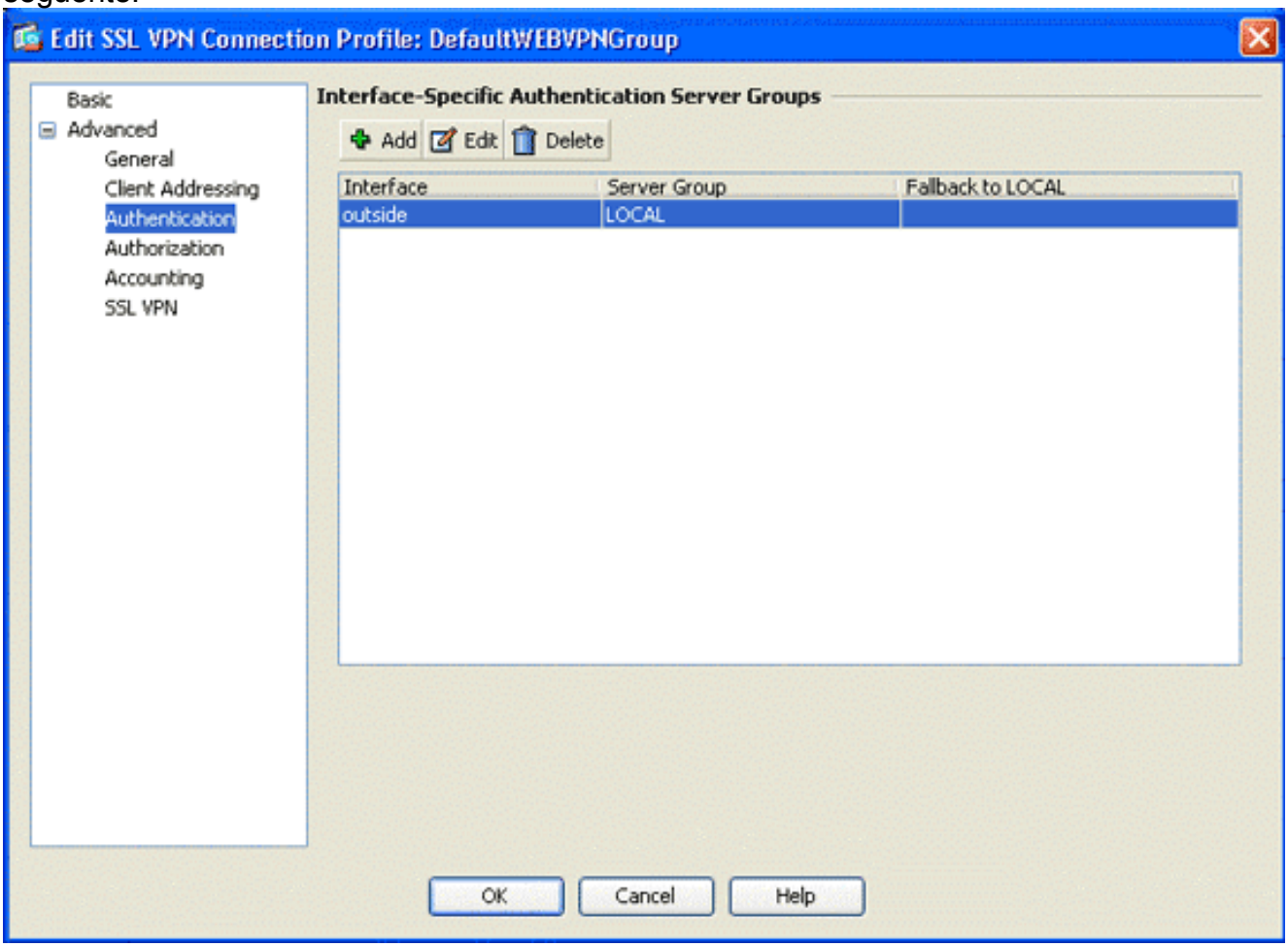
3. Definire il profilo di connessione DefaultWEBVPNGroup.Nell'area VPN ad accesso remoto espandere **Accesso di rete (client)** , quindi scegliere **Profili connessione VPN SSL**.Nell'area Interfacce di accesso, selezionare la **casella di controllo Abilita client VPN Cisco AnyConnect**.Per l'interfaccia esterna, selezionare le caselle di controllo **Consenti accesso**, **Richiedi certificato client** e **Abilita DTLS**, come mostrato nell'immagine:



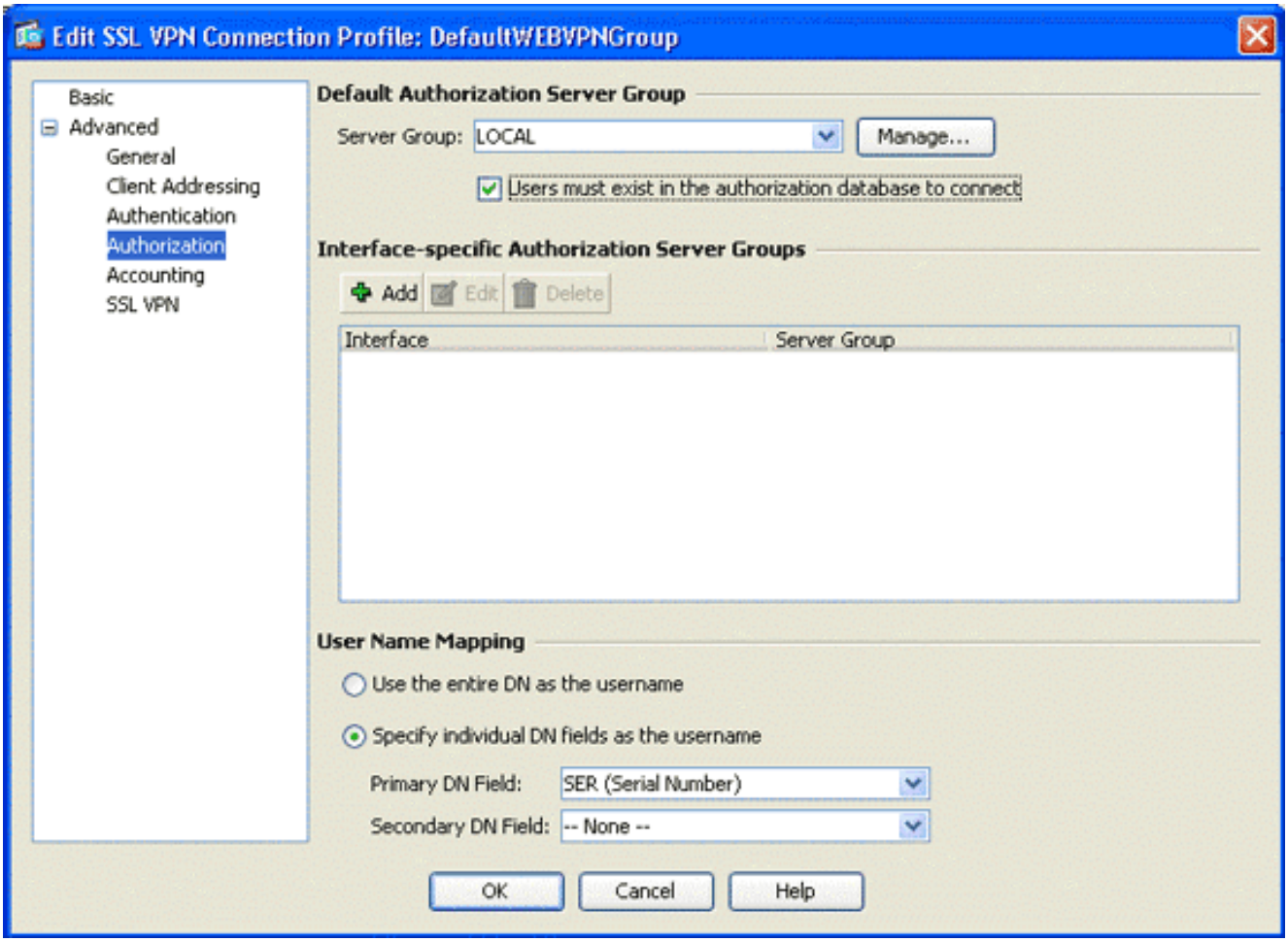
Nell'area Profili di connessione, scegliere **DefaultWEBVPNGroup**, quindi fare clic su **Modifica**.Verrà visualizzata la finestra di dialogo Modifica profilo connessione VPN SSL.



Nell'area di navigazione, scegliere **Base**.Nell'area Autenticazione fare clic sul pulsante di opzione **Certificato**.Nell'area Criteri di gruppo predefiniti selezionare la casella di controllo **SSL VPN Client Protocol**.Espandere **Avanzate** e scegliere **Autenticazione**.Fare clic su **Add** (Aggiungi), quindi aggiungere l'interfaccia esterna con un gruppo di server locale, come mostrato nell'immagine
seguente:



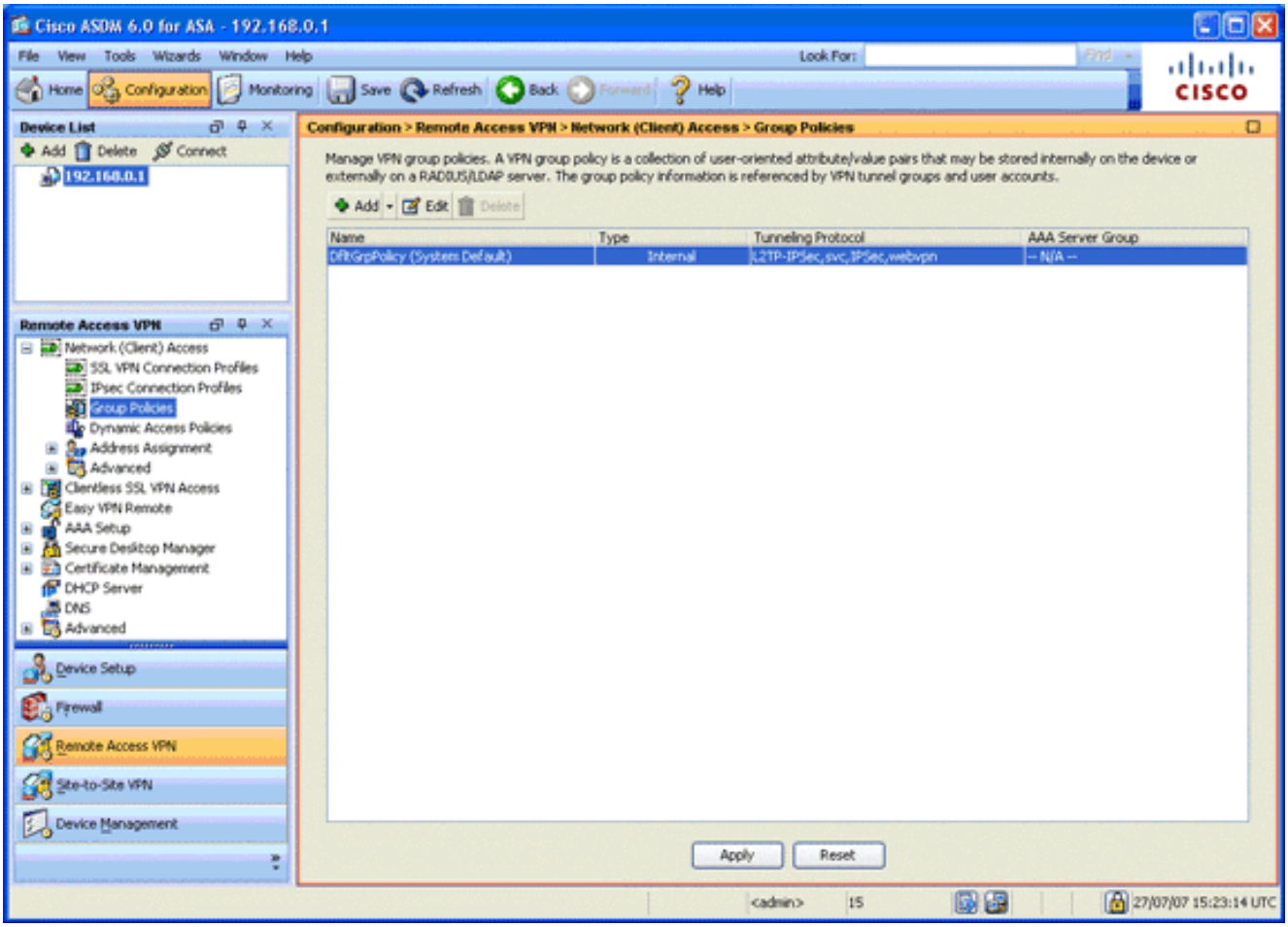
Nell'area di navigazione, scegliere **Autorizzazione**.Nell'area Gruppo di server di autorizzazione predefinito scegliere **LOCAL** dall'elenco a discesa Gruppo di server e selezionare la casella di controllo **Gli utenti devono esistere nel database di autorizzazione per la connessione**.Nell'area Mapping nomi utente scegliere **SER (Numero di serie)** dall'elenco a discesa Campo DN primario, scegliere **Nessuno** dal Campo DN secondario e fare clic su
OK.



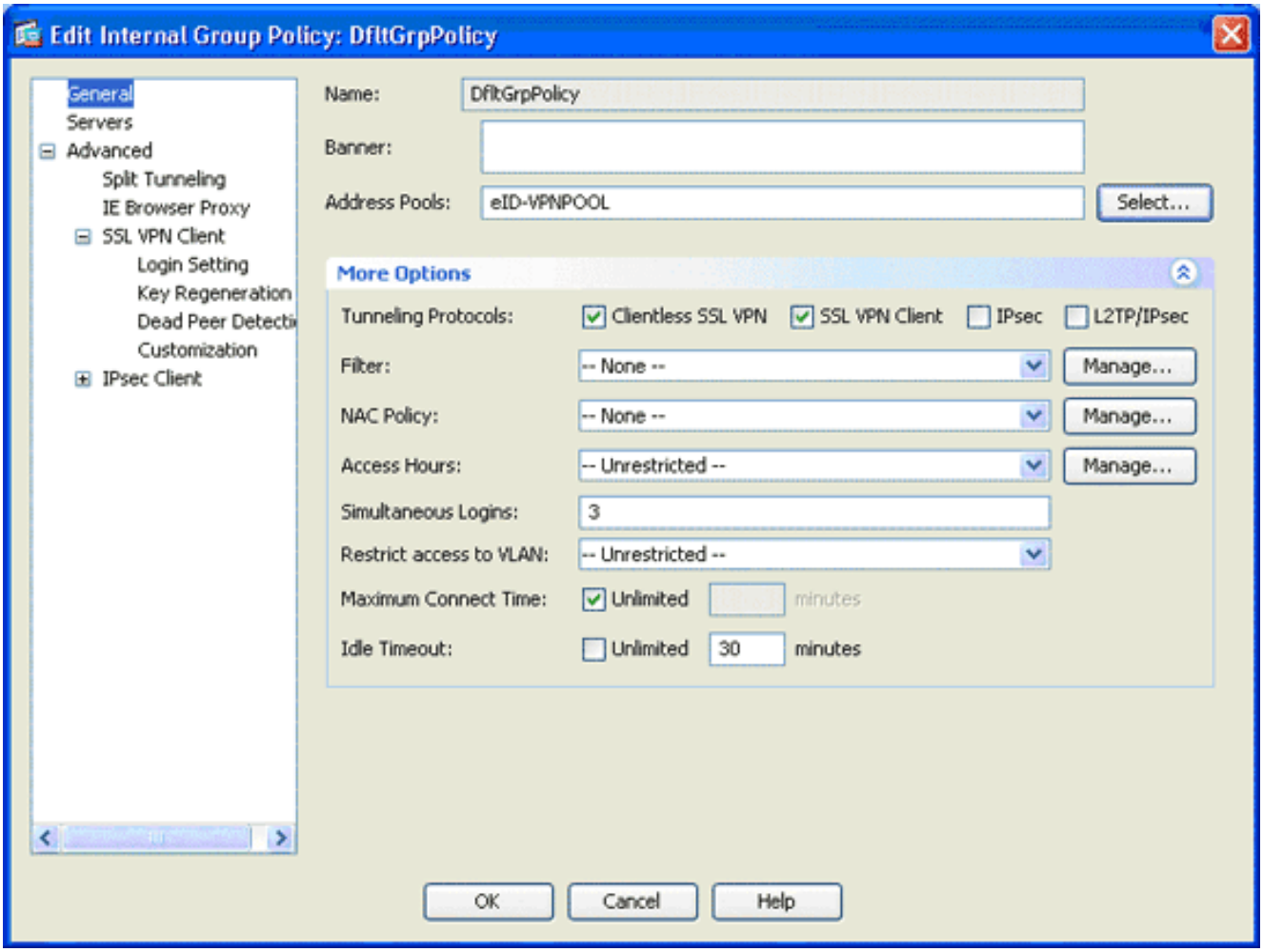
Passaggio 7. Definizione dei Criteri di gruppo predefiniti

In questo passaggio viene descritto come definire i Criteri di gruppo predefiniti.

1. Nell'area VPN ad accesso remoto espandere **Accesso di rete (client)** e scegliere **Criteri di gruppo**.



2. Scegliere **DfltGrpPolicy** dall'elenco dei criteri di gruppo e fare clic su **Modifica**.
3. Verrà visualizzata la finestra di dialogo Modifica Criteri di gruppo interni.

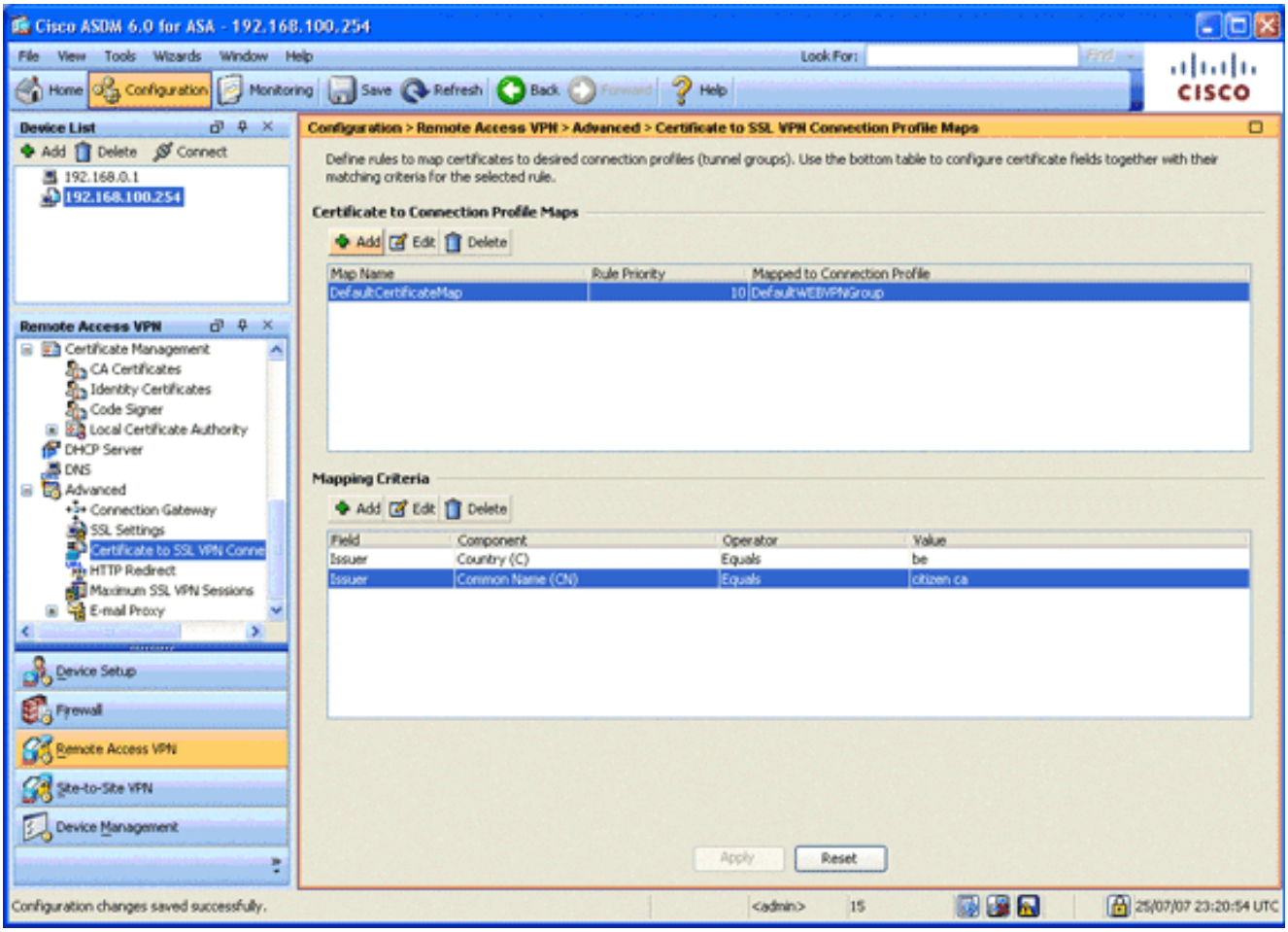


4. Nell'area di navigazione, scegliere **Generale**.
5. Per Pool di indirizzi, fare clic su **Seleziona** per scegliere un pool di indirizzi, quindi scegliere **eID-VPNPOOL**.
6. Nell'area Altre opzioni, deselezionare le caselle di controllo **IPsec** e **L2TP/IPsec**, quindi fare clic su **OK**.

Passaggio 8. Definizione del mapping dei certificati

In questo passaggio viene descritto come definire i criteri di mapping dei certificati.

1. Nell'area VPN ad accesso remoto fare clic su **Avanzate** e scegliere **Mappe profilo connessione VPN da certificato a SSL**.
2. Nell'area Mappe da certificato a profilo di connessione fare clic su **Aggiungi**, quindi scegliere **Mappa certificati predefinita** dall'elenco delle mappe.Questa mappa deve corrispondere a *DefaultWEBVPNProfile* nel campo Mappato a profilo connessione.
3. Nell'area Criteri di mapping fare clic su **Aggiungi** e aggiungere i seguenti valori:Campo: Emittente, Paese (C), Uguale a, "be"Campo: Emittente, nome comune (CN), uguale, "cittadino ca"I criteri di mappatura dovrebbero essere visualizzati come mostrato nella seguente
immagine:

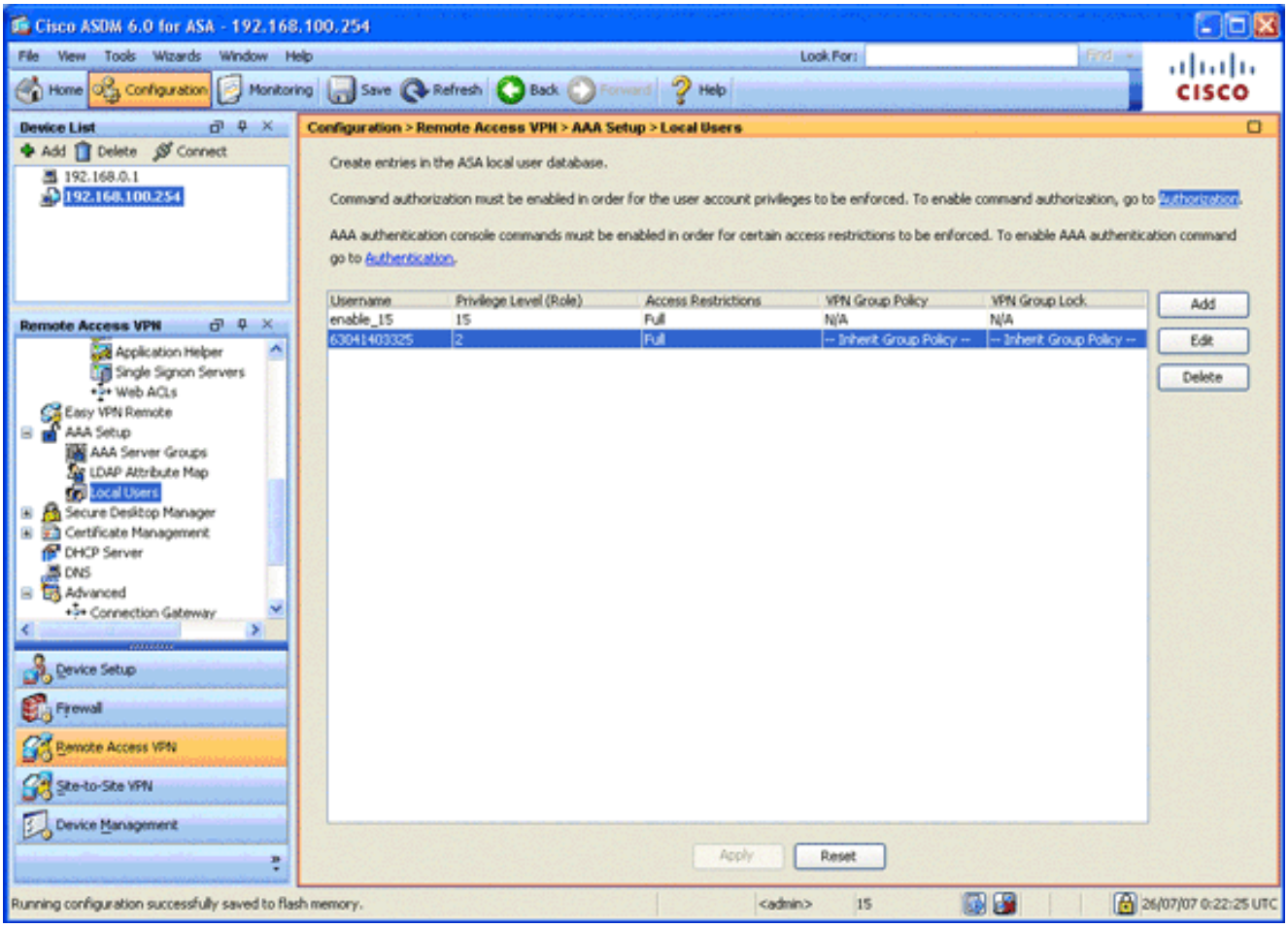


4. Fare clic su **Apply** (Applica).

Passaggio 9. Aggiungere un utente locale

In questo passaggio viene descritto come aggiungere un utente locale.

1. Nell'area VPN ad accesso remoto, espandere **AAA Setup**, quindi selezionare **Local Users** (Utenti locali).
2. Nell'area Utenti locali fare clic su **Aggiungi**.
3. Nel campo Nome utente, immettere il numero di serie del certificato utente. Ad esempio, 56100307215 (come descritto nella sezione Certificato di autenticazione di questo documento).



4. Fare clic su **Apply** (Applica).

Passaggio 10. Riavviare l'appliance ASA

Riavviare l'appliance ASA per verificare che tutte le modifiche vengano applicate ai servizi di sistema.

Ottimizzazione

Durante il test, alcuni tunnel SSL potrebbero non essere chiusi correttamente. Poiché l'ASA presume che il client AnyConnect possa disconnettersi e riconnettersi, il tunnel non viene scartato e può quindi essere riconnesso. Tuttavia, durante i test di laboratorio con una licenza di base (per impostazione predefinita, 2 tunnel SSL), è possibile che la licenza venga scaduta quando i tunnel SSL non vengono chiusi correttamente. Se si verifica questo problema, usare il comando **vpn-sessiondb logoff <*option*>**per chiudere la sessione di tutte le sessioni SSL attive.

Configurazione in un minuto

Per creare rapidamente una configurazione di lavoro, ripristinare l'ASA ai valori predefiniti e incollare la configurazione in modalità di configurazione:

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
```

Informazioni correlate

- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems