ASA 8.X: Esempio di configurazione della registrazione di AnyConnect SCEP

Sommario

Introduzione

La funzionalità di registrazione di SCEP è stata introdotta nel client standalone AnyConnect 2.4. In questo processo, è possibile modificare il profilo XML di AnyConnect in modo da includere una configurazione relativa a SCEP e creare un criterio di gruppo e un profilo di connessione specifici per la registrazione dei certificati. Quando un utente AnyConnect si connette a questo gruppo specifico, AnyConnect invia una richiesta di registrazione del certificato al server CA, che a sua volta accetta o rifiuta automaticamente la richiesta.

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:

- Cisco ASA serie 5500 Adaptive Security Appliance con software versione 8.x
- Cisco AnyConnect VPN versione 2.4

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

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

L'obiettivo della registrazione SCEP automatica per AnyConnect è quello di rilasciare un certificato al client in modo sicuro e scalabile. Ad esempio, gli utenti non devono richiedere un certificato a un server CA. Questa funzionalità è integrata nel client AnyConnect. I certificati vengono rilasciati ai client in base ai parametri di certificato indicati nel file di profilo XML.

Panoramica delle modifiche richieste

La funzionalità di registrazione di AnyConnect SCEP richiede la definizione di alcuni parametri di certificato nel profilo XML. Sull'appliance ASA per la registrazione dei certificati viene creato un profilo di connessione e un criterio di gruppo e il profilo XML viene associato a tale criterio. Il client AnyConnect si connette al profilo di connessione che utilizza questo criterio specifico e invia una richiesta di certificato con i parametri definiti nel file XML. L'Autorità di certificazione (CA) accetta o nega automaticamente la richiesta. Il client AnyConnect recupera i certificati con il protocollo SCEP se l'elemento <CertificateSCEP> è definito in un profilo client.

L'autenticazione del certificato client non può essere eseguita prima che AnyConnect tenti di recuperare automaticamente i nuovi certificati, quindi se è già installato un certificato valido, la registrazione non viene eseguita.

Quando gli utenti accedono al gruppo specifico, vengono registrati automaticamente. È inoltre disponibile un metodo manuale per il recupero dei certificati in cui agli utenti viene visualizzato il pulsante **Ottieni certificato**. Questa procedura funziona solo quando il client ha accesso diretto al server CA, non attraverso il tunnel.

Per ulteriori informazioni, consultare la guida all'amministrazione dei client VPN di Cisco AnyConnect, versione 2.4.

Impostazioni XML per abilitare la funzione Anyconnect SCEP

Questi sono gli elementi importanti che devono essere definiti nel file XML di AnyConnect. Per ulteriori informazioni, consultare la guida all'amministrazione dei client VPN di Cisco AnyConnect, versione 2.4.

- <AutomaticSCEPost>: specifica il nome host ASA e il profilo di connessione (gruppo di tunnel) per cui è configurato il recupero del certificato SCEP. Il valore deve essere nel formato del nome di dominio completo dell'ASA\nome del profilo di connessione o dell'indirizzo IP dell'ASA\nome del profilo di connessione.
- <CAURL>: identifica il server CA SCEP.

- <CertificateSCEP> - Definisce la modalità di richiesta del contenuto del certificato.
- <DisplayGetCertButton>: determina se nell'interfaccia utente di AnyConnect viene visualizzato il pulsante Ottieni certificato. Consente agli utenti di richiedere manualmente il rinnovo o il provisioning del certificato.

Di seguito è riportato un esempio di profilo:

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

Configurazione dell'ASA per il supporto del protocollo SCEP per AnyConnect

Per consentire l'accesso a un'Autorità di registrazione privata (RA), l'amministratore ASA deve

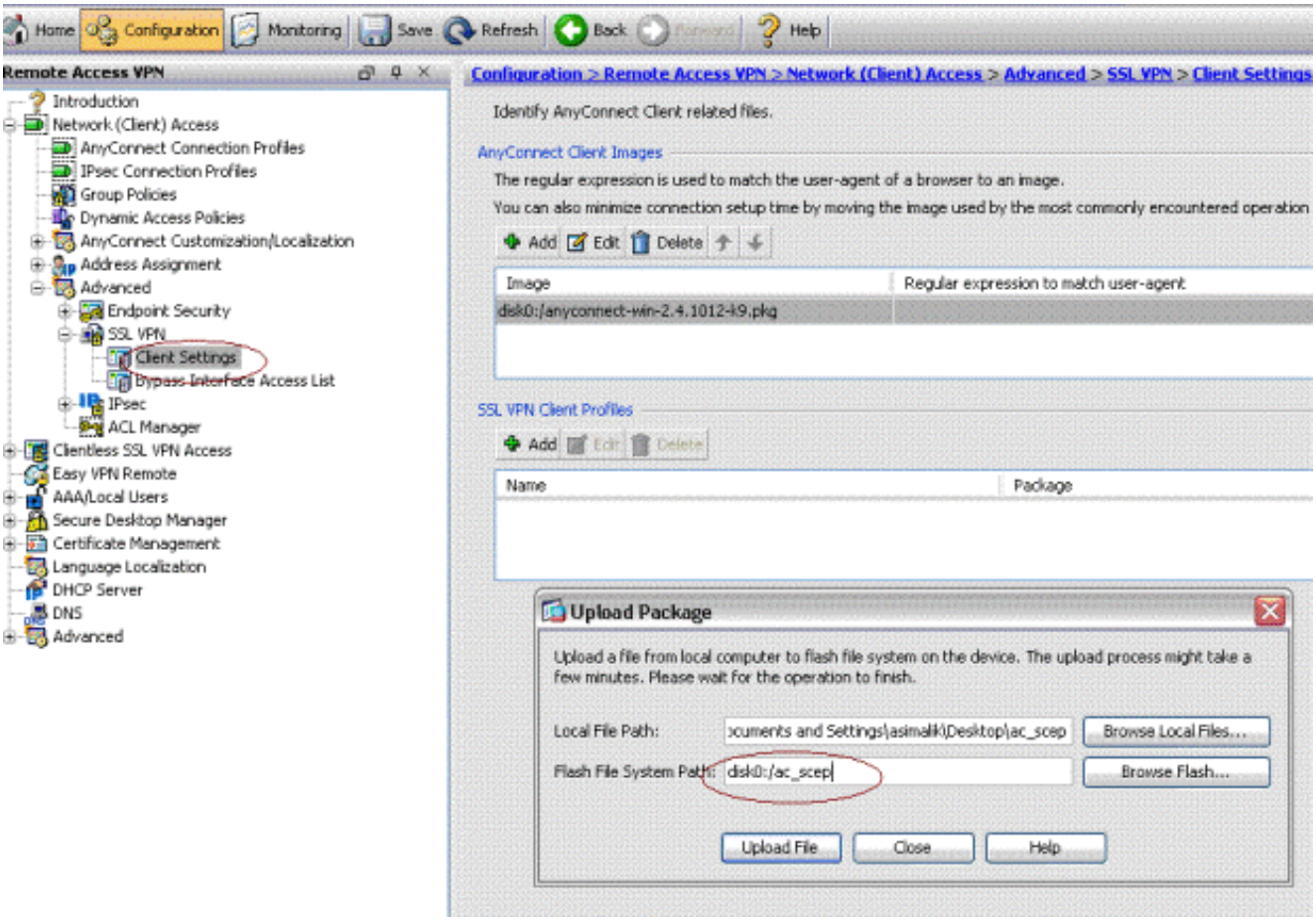
creare un alias con un ACL che limiti la connettività della rete lato privato all'RA desiderata. Per recuperare automaticamente un certificato, gli utenti si connettono e eseguono l'autenticazione a questo alias.

Attenersi alla seguente procedura:

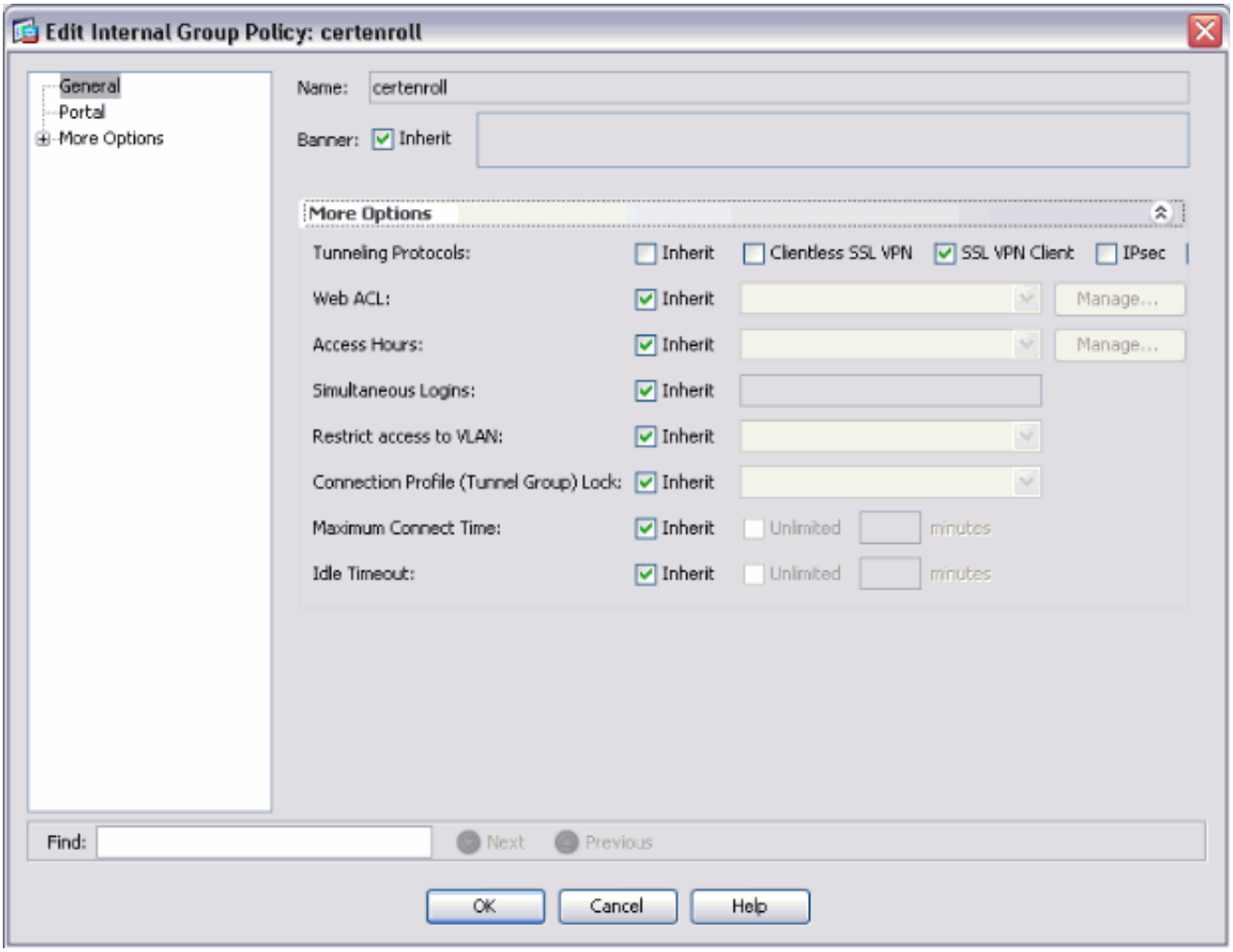
1. Creare un alias sull'appliance ASA che punti al gruppo configurato specifico.
2. Specificare l'alias nell'elemento <AutomaticSCEPHost> nel profilo client dell'utente.
3. Allegare il profilo client contenente la sezione <CertificateEnrollment> al gruppo configurato specifico.
4. Impostare un ACL per il gruppo configurato specifico per limitare il traffico all'Autorità registrazione integrità del lato privato.

Attenersi alla seguente procedura:

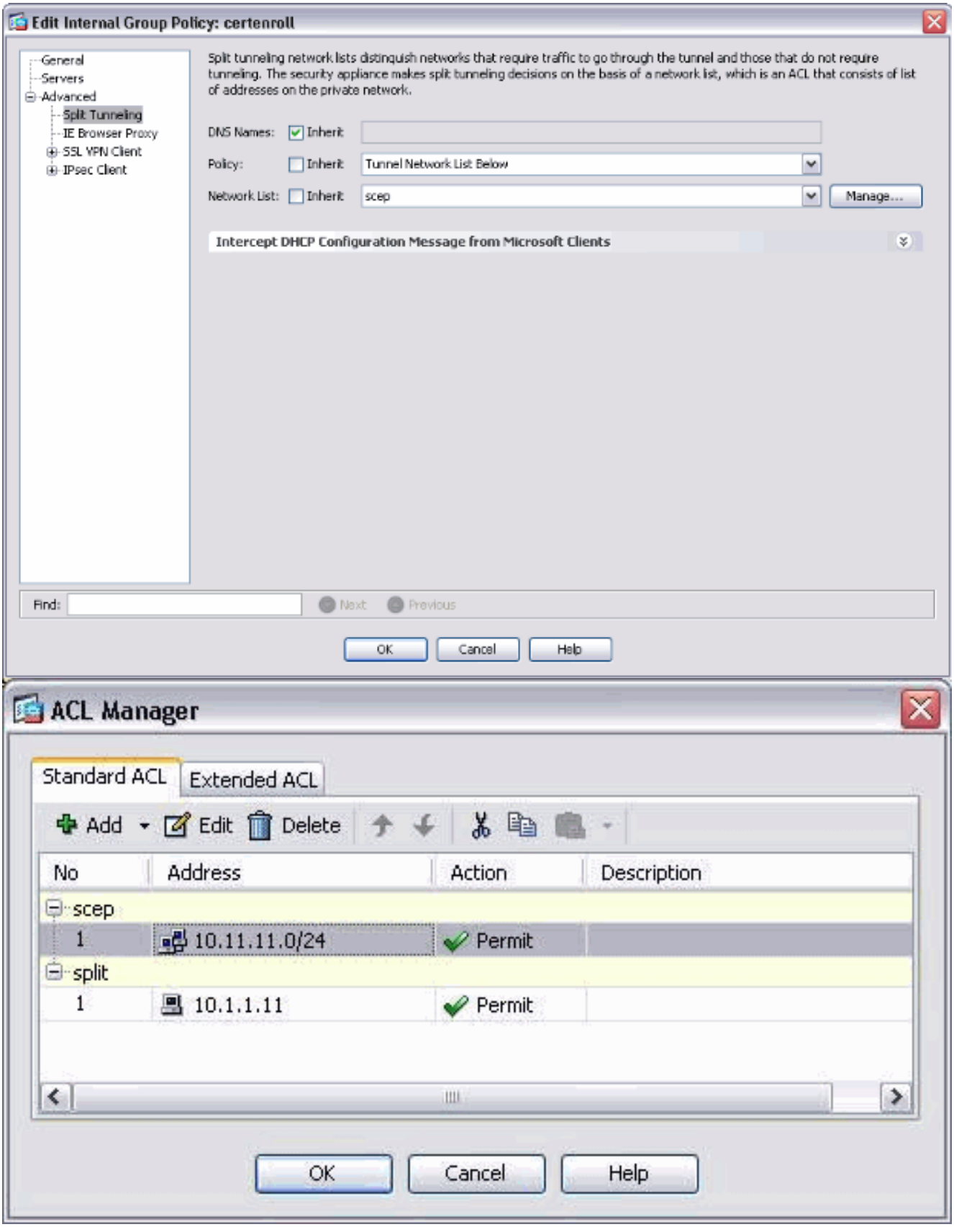
1. Caricare il profilo XML sull'appliance ASA.Scegliere **VPN ad accesso remoto > Accesso di rete (client) > Avanzate > VPN SSL > Impostazioni client**.In Profili client VPN SSL fare clic su **Aggiungi**.Fare clic su **Sfoglia file locali** per selezionare il file del profilo, quindi fare clic su **Sfoglia Flash** per specificare il nome del file flash.Fare clic su **Upload File**.



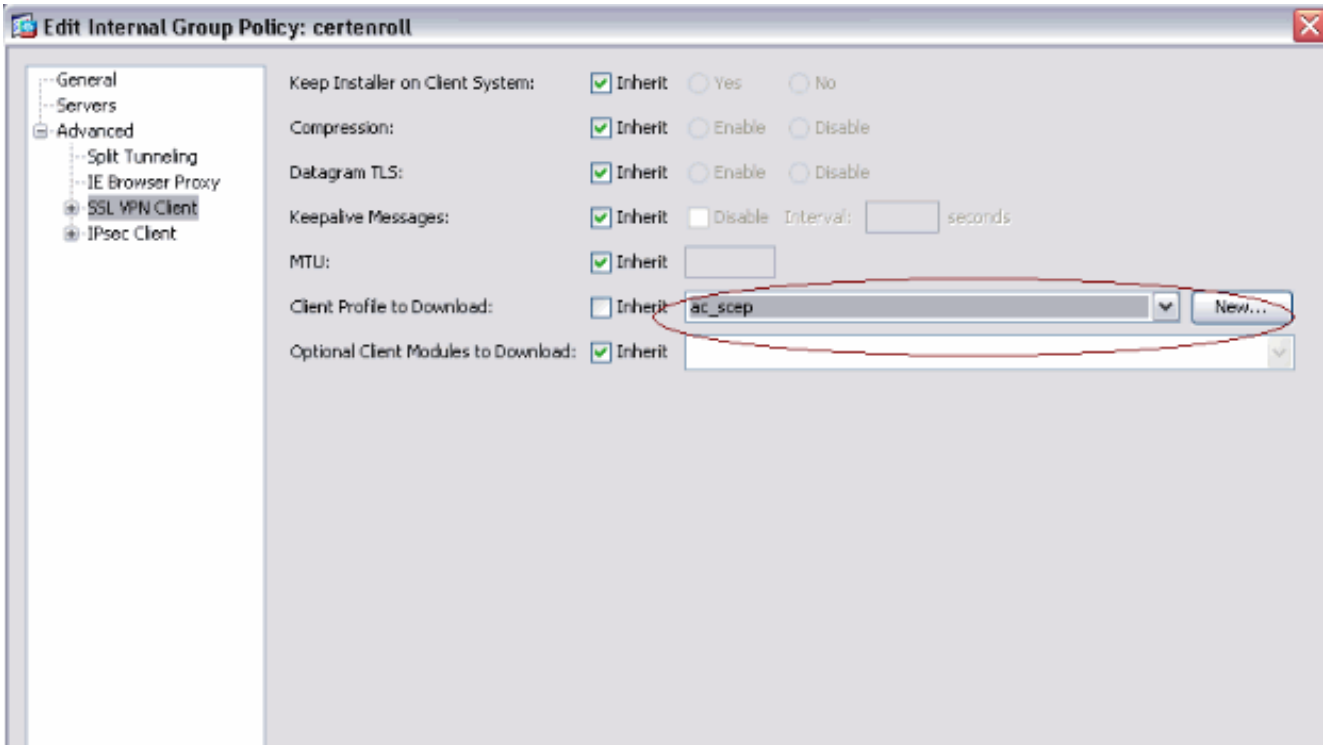
2. Impostare un criterio di gruppo di **registrazione certificati** per la registrazione dei certificati.Scegliere **VPN ad accesso remoto > Accesso client di rete > Criteri di gruppo**, quindi fare clic su **Aggiungi**.



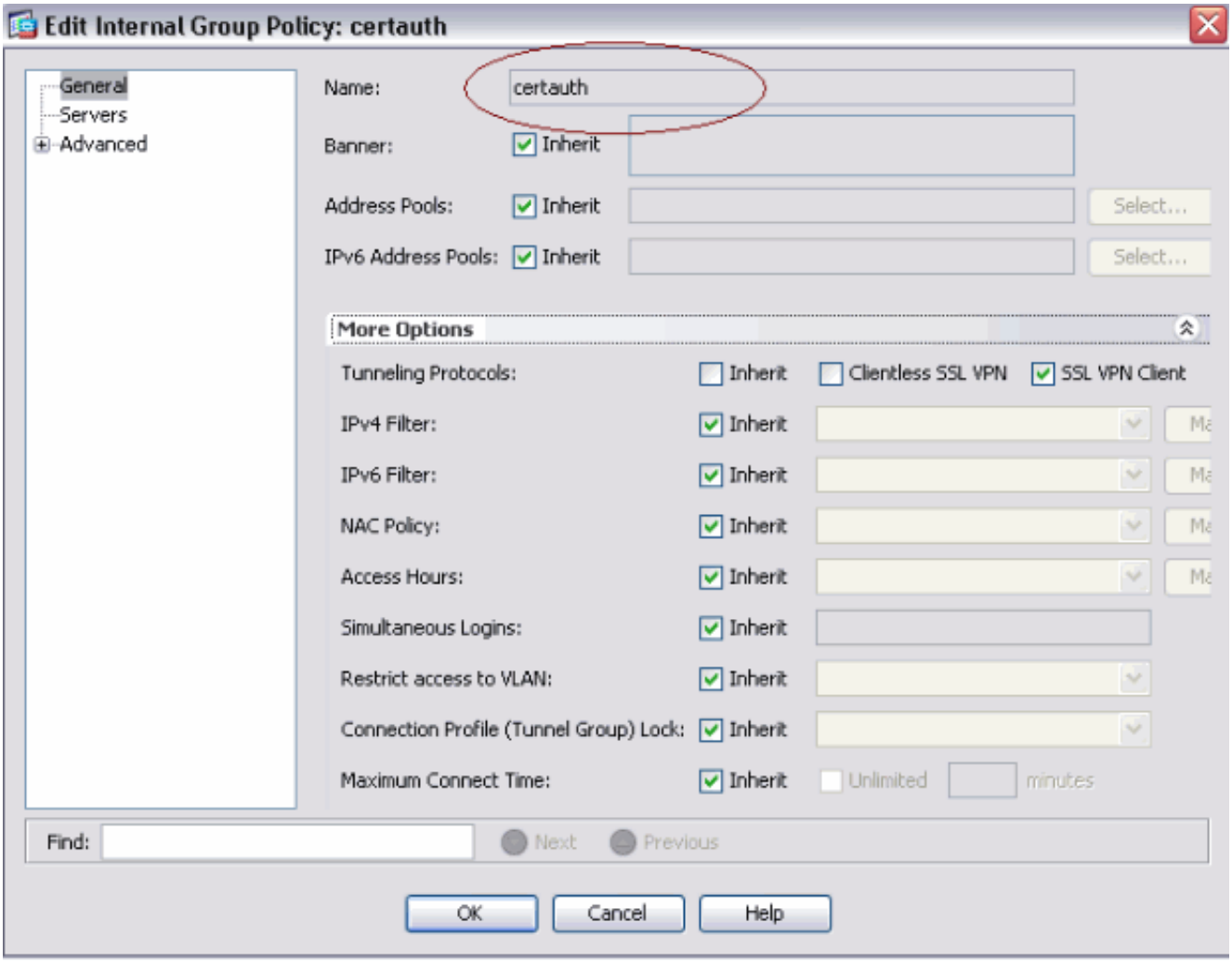
Aggiungere un tunnel suddiviso per il server CA.Espandere **Advanced** (Avanzate), quindi selezionare **Split Tunneling**.Scegliere **Elenco reti tunnel** dal menu Criteri e fare clic su **Gestisci** per aggiungere l'elenco di controllo di accesso.



Selezionare **SSL VPN Client**, quindi scegliere il profilo per il ciclo di certificazione dal menu **Profilo client da scaricare**.

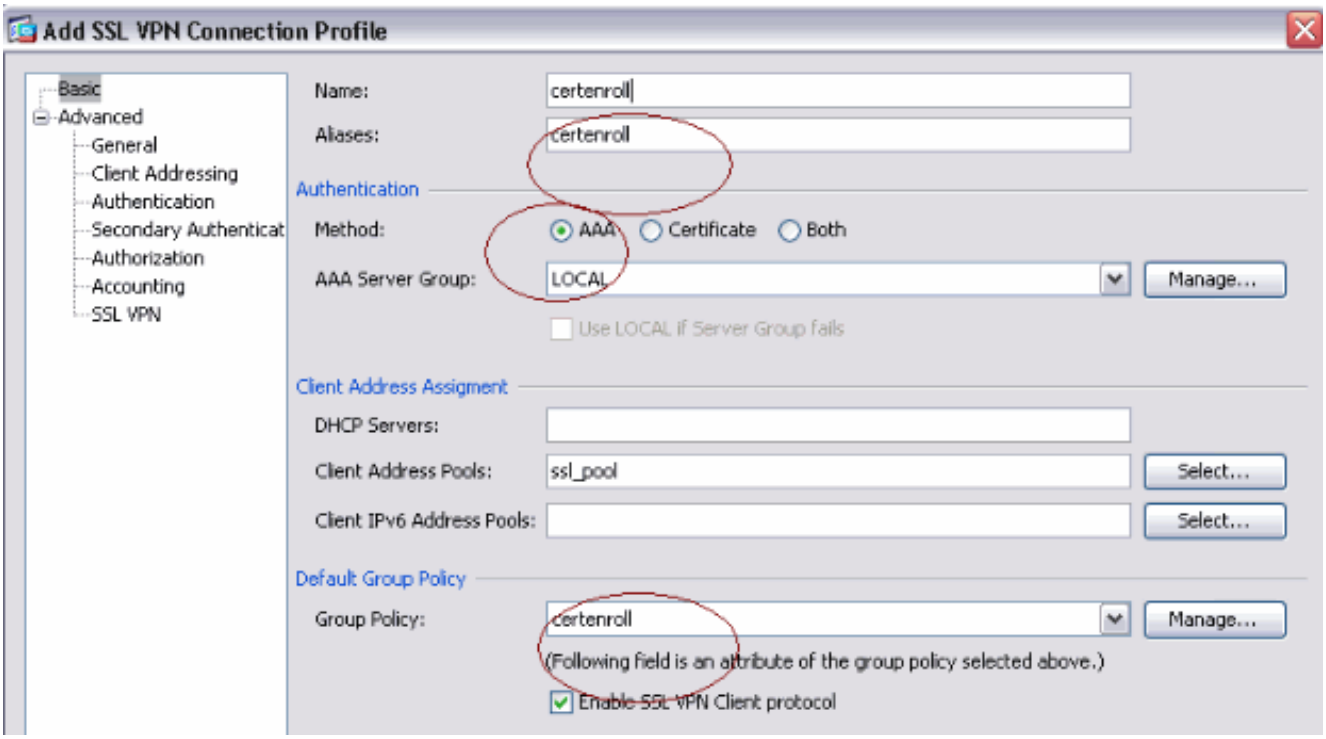


3. Creare un altro gruppo denominato **certauth** per l'autenticazione dei certificati.

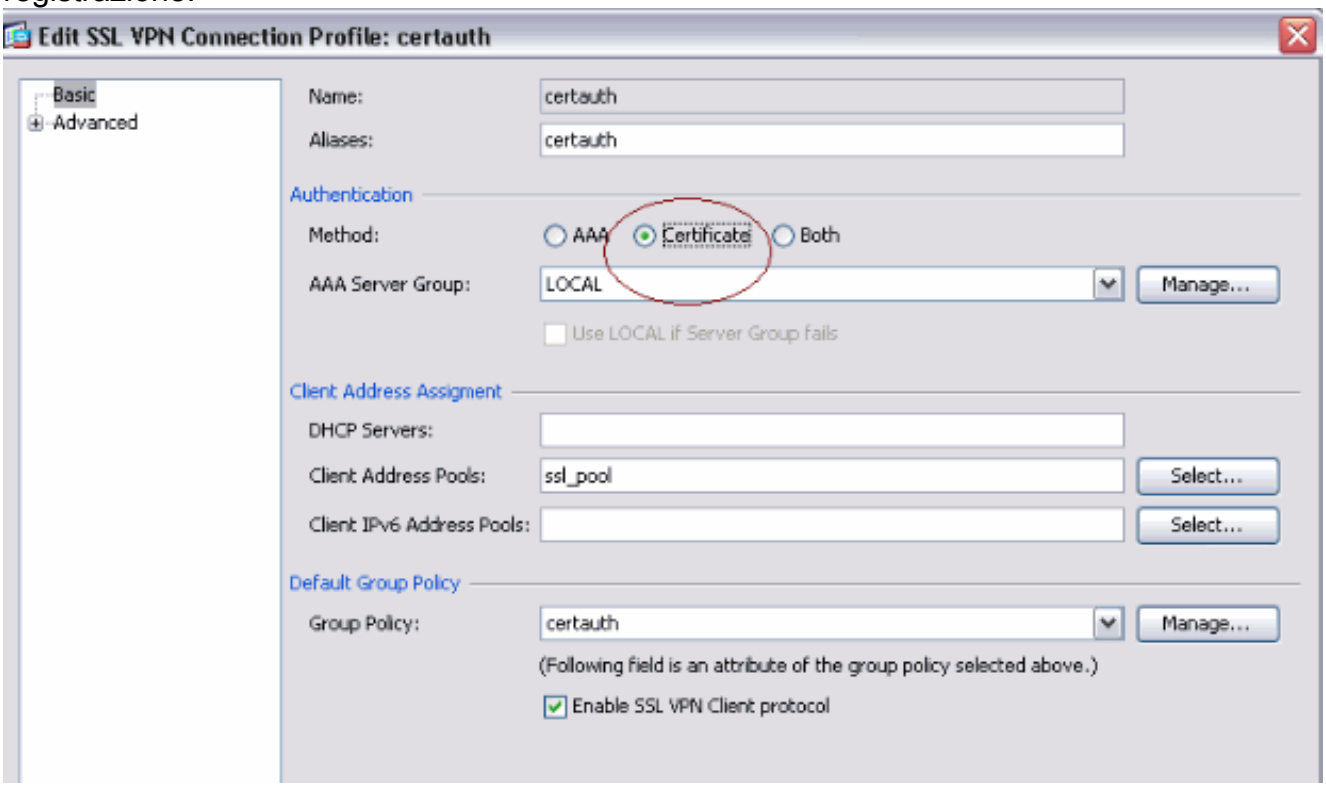


4. Creare un profilo di connessione Certenroll.Scegliere **VPN ad accesso remoto > Accesso client di rete > Profili di connessione AnyConnect**, quindi fare clic su **Aggiungi**.Immettere il gruppo **Certenroll** nel campo Alias.**Nota:** il nome alias deve corrispondere al valore utilizzato nel profilo AnyConnect in

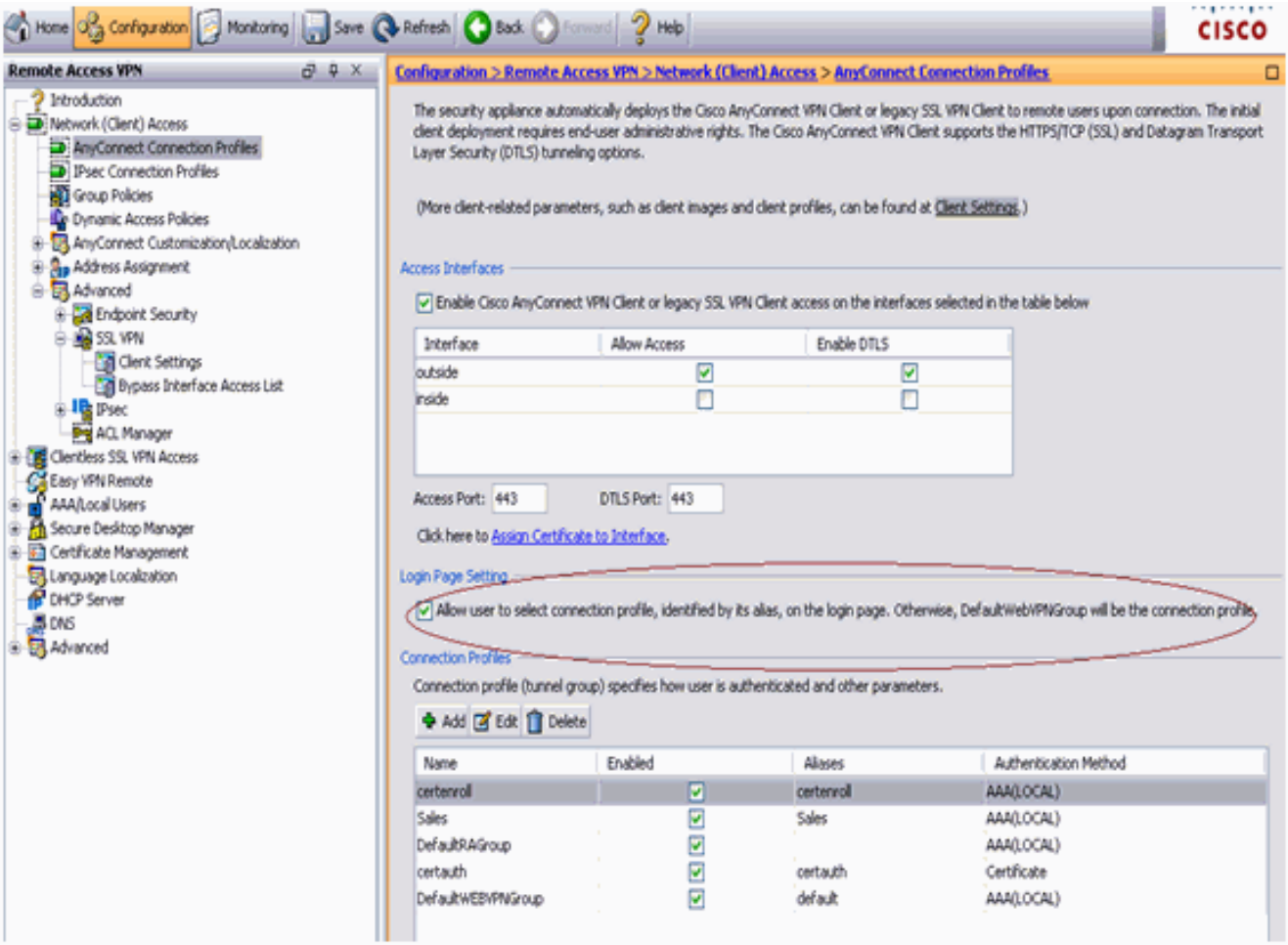
AutomaticSCEPHost.



5. Creare un altro profilo di connessione denominato **certauth** con autenticazione del certificato. Profilo di connessione effettivo utilizzato dopo la registrazione.



6. Per assicurarsi che l'uso dell'alias sia abilitato, selezionare **Consenti all'utente di selezionare il profilo di connessione, identificato dall'alias, nella pagina di accesso. In caso contrario, DefaultWebVPNGroup è il profilo di connessione.**



Test AnyConnect SCEP

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

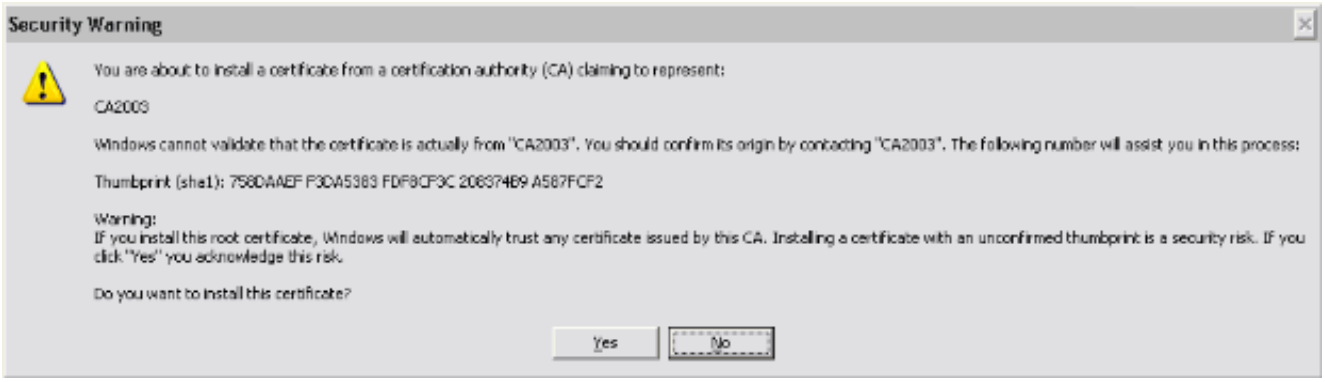
1. Avviare il client AnyConnect e connettersi al profilo del rotolo del

cert.AnyConnect passa la richiesta di registrazione al server CA tramite

SCEP. AnyConnect passa direttamente la richiesta di registrazione e non attraversa il tunnel, se viene utilizzato il pulsante **Get Certificate** (Ottieni

certificato).

2. Viene visualizzato questo avviso. Fare clic su **Sì** per installare il certificato utente e radice

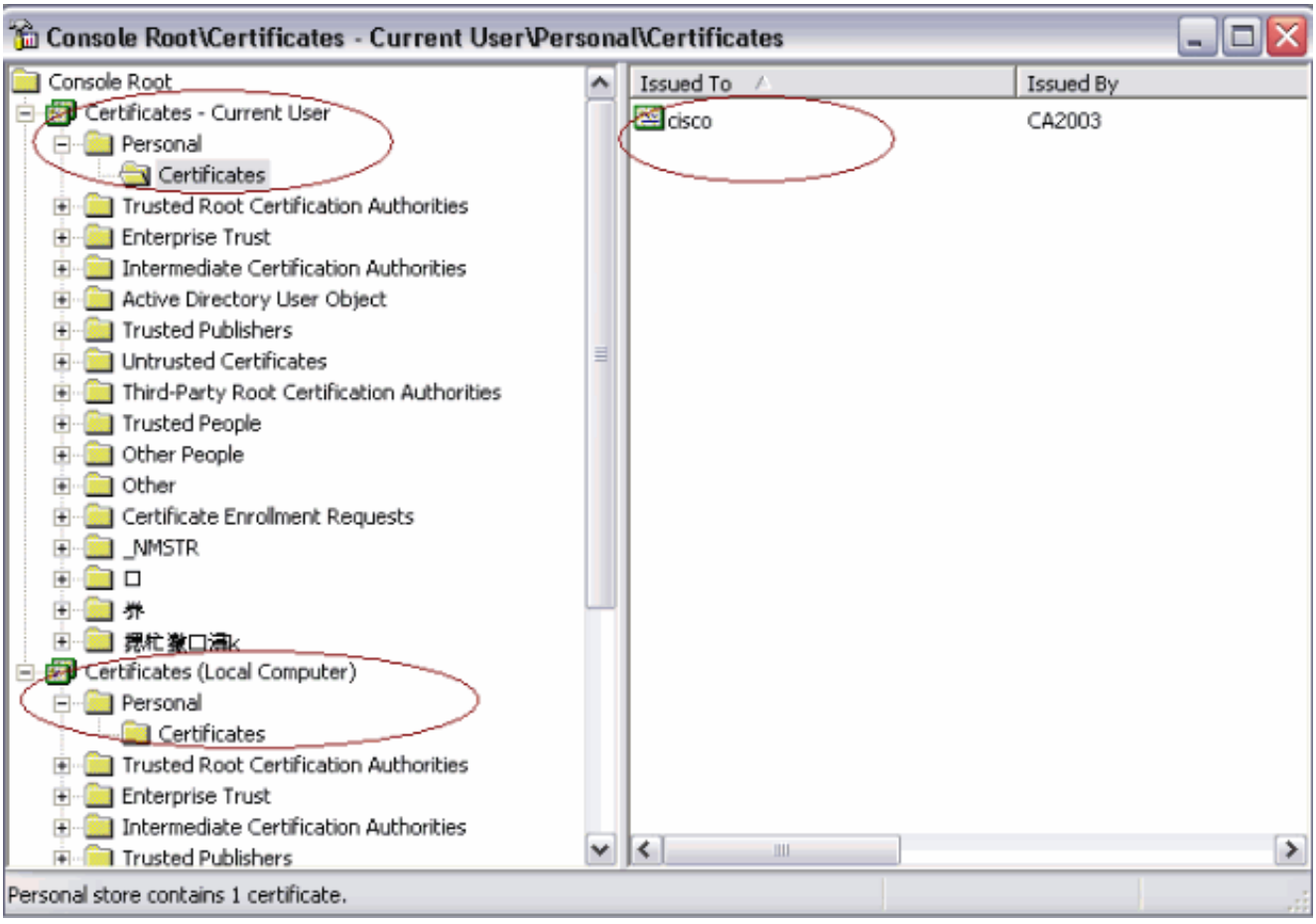


3. Una volta registrato il certificato, connettersi al profilo **di certificazione**.

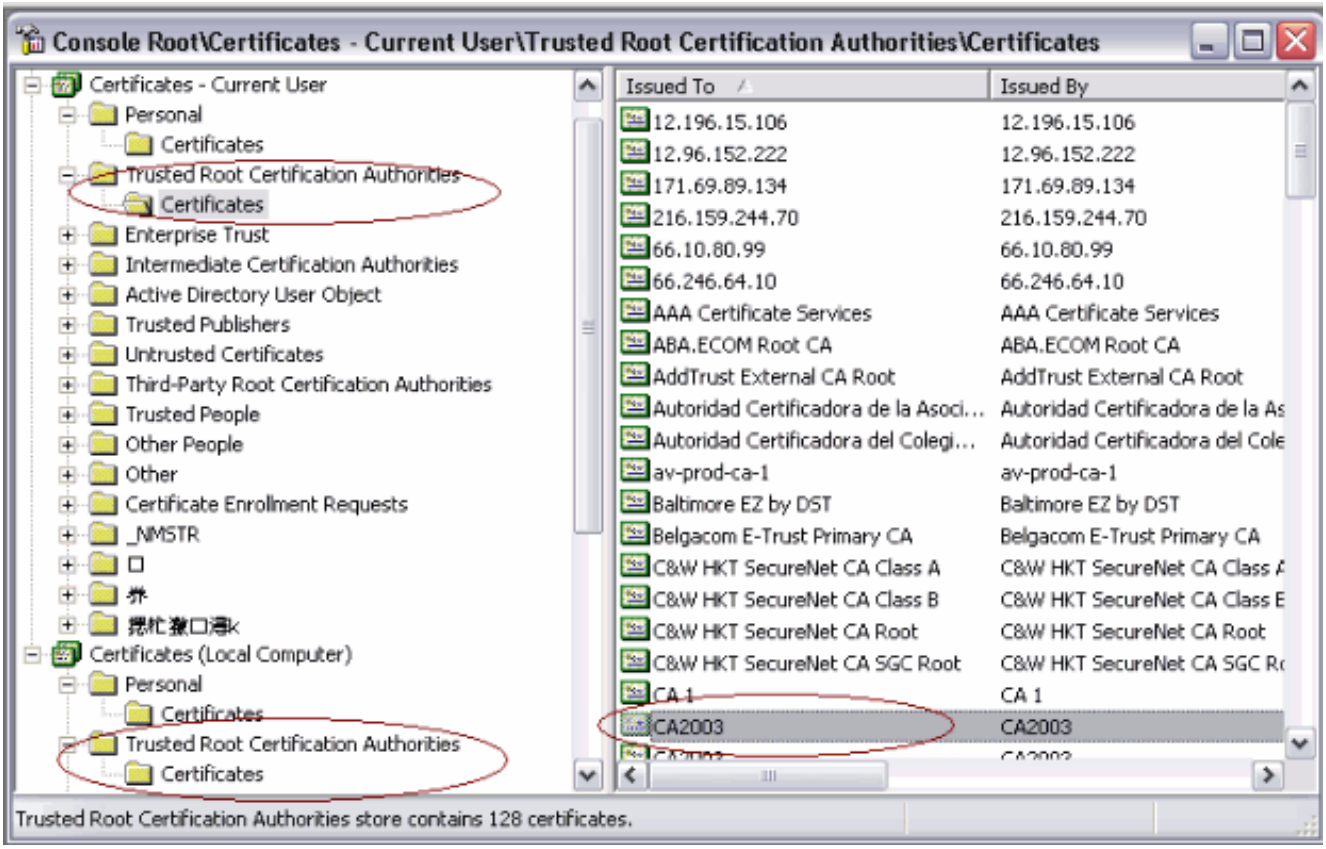
Archiviazione certificati in Microsoft Windows dopo la richiesta SCEP

Attenersi alla seguente procedura:

1. Fare clic su **Start > Esegui > mmc**.
2. Fare clic su **Aggiungi/rimuovi snap-in**.
3. Fare clic su **Aggiungi** e scegliere **certificati**.
4. Aggiungere i certificati **Account utente** e **Account computer**.Nell'immagine è illustrato il certificato utente installato nell'archivio certificati di Windows:



Nell'immagine è illustrato il certificato CA installato nell'archivio certificati di Windows:



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- La registrazione SCEP di AnyConnect funziona solo quando l'autenticazione dei certificati non riesce. In caso contrario, controllare l'archivio certificati. Se i certificati sono già installati, eliminarli e provare di nuovo.
- La registrazione SCEP non funziona a meno che non si utilizzi il comando **ssl certificate-authentication interface outside port 443**.Per ulteriori informazioni, fare riferimento agli ID dei bug Cisco seguenti:Cisco Bug ID CSCtf06778 (solo utenti registrati) —La registrazione AnyConnect SCEP non funziona con il certificato per gruppo Auth 2Cisco Bug ID CSCtf06844 (solo utenti registrati) —Iscrizione AnyConnect SCEP non funzionante con ASA Per Group Cert Auth
- Se il server CA è all'esterno dell'appliance ASA, accertarsi di usare il comando **intra-interface** per bloccare il traffico di **sicurezza**. Aggiungere anche i comandi nat outside e access-list, come mostrato nell'esempio:
```
nat (outside) 1
access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87
```
Dove 172.16.1.0 è il pool AnyConnect e 171.69.89.87 è l'indirizzo IP del server CA.
- Se il server CA si trova all'interno, assicurarsi di includerlo nell'elenco degli accessi al tunnel suddiviso per **certenroll** Criteri di gruppo. In questo documento si presume che il server CA si trovi all'interno.
```
group-policy certenroll attributes
split-tunnel-policy tunnelspecified
 split-tunnel-network-list value scep

access-list scep standard permit 171.69.89.0 255.255.255.0
```

Informazioni correlate

- Guida all'amministrazione dei client VPN di Cisco AnyConnect, versione 2.4
- Documentazione e supporto tecnico – Cisco Systems