

ASA 8.x: Konfigurationsbeispiel für die AnyConnect SCEP-Registrierung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Übersicht der erforderlichen Änderungen](#)

[XML-Einstellungen zum Aktivieren der AnyConnect SCEP-Funktion](#)

[Konfigurieren der ASA zur Unterstützung des SCEP-Protokolls für AnyConnect](#)

[AnyConnect SCEP testen](#)

[Zertifikatsspeicherung in Microsoft Windows nach SCEP-Anforderung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

Die SCEP-Anmeldungsfunktion wird in AnyConnect Standalone Client 2.4 eingeführt. Bei diesem Prozess ändern Sie das AnyConnect XML-Profil, um eine SCEP-bezogene Konfiguration einzuschließen, und erstellen eine bestimmte Gruppenrichtlinie und ein bestimmtes Verbindungsprofil für die Zertifikatregistrierung. Wenn ein AnyConnect-Benutzer eine Verbindung zu dieser bestimmten Gruppe herstellt, sendet AnyConnect eine Zertifikatsanmeldungsanfrage an den CA-Server, und der CA-Server akzeptiert oder verweigert die Anforderung automatisch.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliances der Serie ASA 5500 mit Softwareversion 8.x
- Cisco AnyConnect VPN Version 2.4

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Ziel der automatischen SCEP-Registrierung für AnyConnect ist die sichere und skalierbare Ausstellung eines Zertifikats für den Client. Beispielsweise müssen Benutzer kein Zertifikat von einem CA-Server anfordern. Diese Funktion ist im AnyConnect-Client integriert. Die Zertifikate werden den Clients basierend auf den in der XML-Profildatei erwähnten Zertifikatsparametern ausgestellt.

Übersicht der erforderlichen Änderungen

Für die SCEP-Registrierung bei AnyConnect müssen bestimmte Zertifikatsparameter im XML-Profil definiert werden. Auf der ASA wird eine Gruppenrichtlinie und ein Verbindungsprofil für die Zertifikatsregistrierung erstellt, und das XML-Profil ist dieser Richtlinie zugeordnet. Der AnyConnect-Client stellt eine Verbindung zum Verbindungsprofil her, das diese spezifische Richtlinie verwendet, und sendet eine Anforderung für ein Zertifikat mit den Parametern, die in der XML-Datei definiert sind. Die Zertifizierungsstelle (Certificate Authority, CA) akzeptiert oder verweigert die Anfrage automatisch. Der AnyConnect-Client ruft Zertifikate mit dem SCEP-Protokoll ab, wenn das <CertificateSCEP>-Element in einem Clientprofil definiert ist.

Die Client-Zertifikatsauthentifizierung muss fehlgeschlagen sein, bevor AnyConnect versucht, die neuen Zertifikate automatisch abzurufen. Wenn Sie also bereits ein gültiges Zertifikat installiert haben, erfolgt die Registrierung nicht.

Wenn sich Benutzer bei der bestimmten Gruppe anmelden, werden sie automatisch registriert. Es gibt auch eine manuelle Methode zum Abrufen von Zertifikaten, bei der Benutzern eine Schaltfläche **Zertifikat abrufen** angezeigt wird. Dies funktioniert nur, wenn der Client direkten Zugriff auf den CA-Server hat, nicht über den Tunnel.

Weitere Informationen finden Sie im [Administratorhandbuch für den Cisco AnyConnect VPN-Client, Version 2.4](#).

XML-Einstellungen zum Aktivieren der AnyConnect SCEP-Funktion

Dies sind die wichtigen Elemente, die in der XML-Datei von AnyConnect definiert werden müssen. Weitere Informationen finden Sie im [Administratorhandbuch für den Cisco AnyConnect VPN-Client, Version 2.4](#).

- <AutomaticSCEPHost> - Gibt den ASA-Hostnamen und das Verbindungsprofil (Tunnelgruppe) an, für die der SCEP-Zertifikatsabruf konfiguriert ist. Der Wert muss im

Format des vollqualifizierten Domännennamens des ASA\Connection-Profilnamens oder der IP-Adresse des ASA\Connection-Profilnamens sein.

- <CAURL> - Identifiziert den SCEP CA-Server.
- <CertificateSCEP>: Definiert, wie der Inhalt des Zertifikats angefordert wird.
- <DisplayGetCertButton>: Bestimmt, ob die AnyConnect-GUI die Schaltfläche Zertifikat abrufen anzeigt. Benutzer können die Verlängerung oder Bereitstellung des Zertifikats manuell beantragen.

Hier ein Beispielprofil:

```
<?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>
<PPPEExclusion UserControllable="false">Automatic
<PPPEExclusionServerIP UserControllable="false"></PPPEExclusionServerIP>
</PPPEExclusion>
<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>
```

[Konfigurieren der ASA zur Unterstützung des SCEP-Protokolls](#)

für AnyConnect

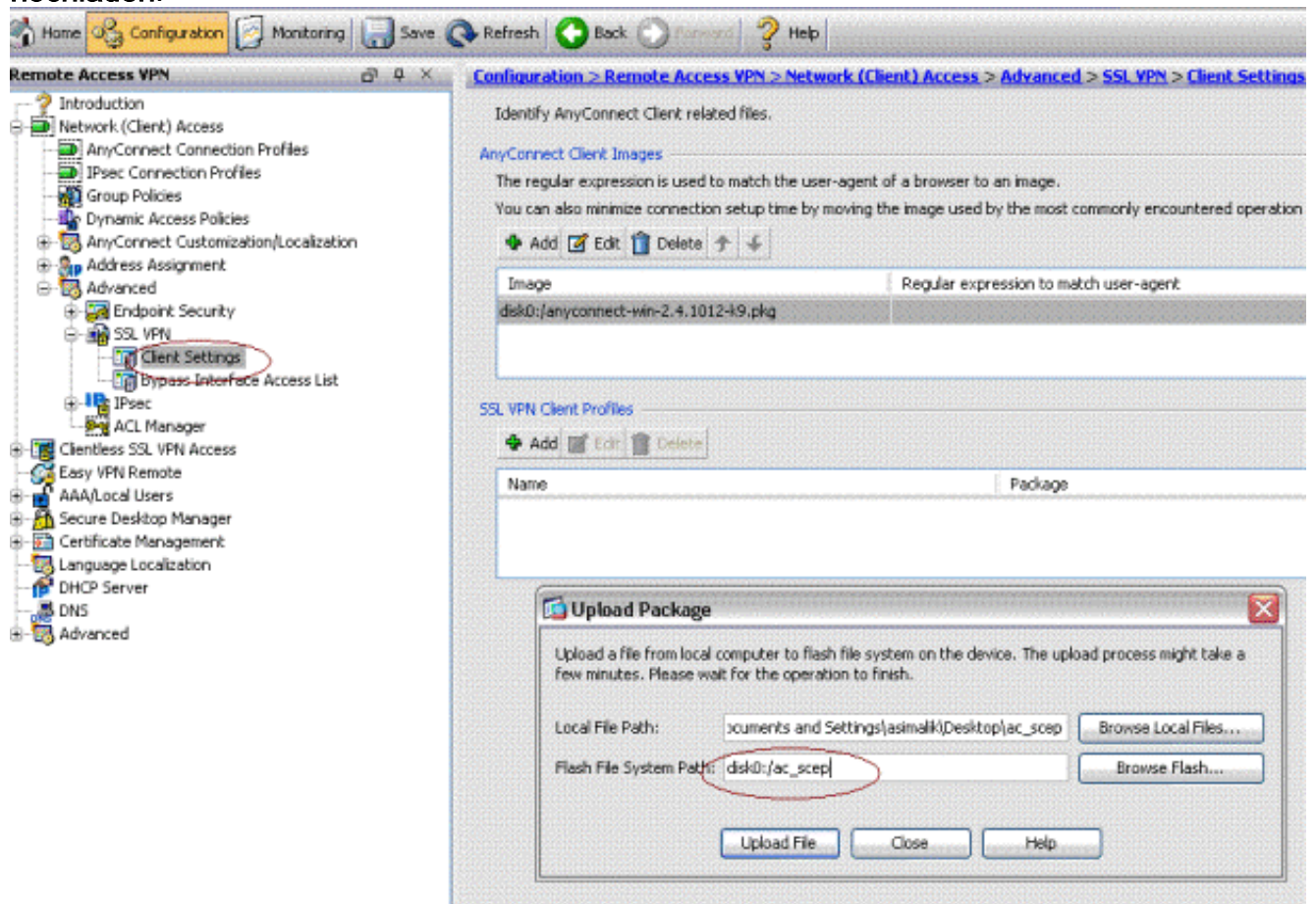
Um den Zugriff auf eine private Registrierungs-Authority (RA) zu ermöglichen, muss der ASA-Administrator einen Alias erstellen, der über eine ACL verfügt, die die private Netzwerkverbindung auf das gewünschte RA beschränkt. Um ein Zertifikat automatisch abzurufen, verbinden sich Benutzer und authentifizieren sich bei diesem Alias.

Gehen Sie wie folgt vor:

1. Erstellen Sie einen Alias auf der ASA, um auf die spezifische konfigurierte Gruppe zu zeigen.
2. Geben Sie den Alias im <AutomaticSCEPHost>-Element im Clientprofil des Benutzers an.
3. Hängen Sie das Clientprofil, das den <CertificateEnrollment>-Abschnitt enthält, an die spezifische konfigurierte Gruppe an.
4. Legen Sie eine ACL für die spezifische konfigurierte Gruppe fest, um den Datenverkehr auf die private RA zu beschränken.

Gehen Sie wie folgt vor:

1. Laden Sie das XML-Profil auf ASA hoch. Wählen Sie **Remote Access VPN > Network (Client) access > Advanced > SSL VPN > Client settings** aus. Klicken Sie unter SSL VPN-Clientprofile auf **Hinzufügen**. Klicken Sie auf **Lokale Dateien durchsuchen**, um die Profildatei auszuwählen, und klicken Sie auf **Flash durchsuchen**, um den Namen der Flash-Datei anzugeben. Klicken Sie auf **Datei hochladen**.



2. Richten Sie eine **certenroll**-Gruppenrichtlinie für die Zertifikatsregistrierung ein. Wählen Sie **Remote Access VPN > Network Client Access > Group Policy (Remote-Zugriffs-VPN > Netzwerk-Client-Zugriff > Gruppenrichtlinie)** aus, und klicken Sie auf **Add**

(Hinzufügen).

General
Portal
+ More Options

Name: certenroll

Banner: Inherit

More Options

Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec

Web ACL: Inherit Manage...

Access Hours: Inherit Manage...

Simultaneous Logins: Inherit

Restrict access to VLAN: Inherit

Connection Profile (Tunnel Group) Lock: Inherit

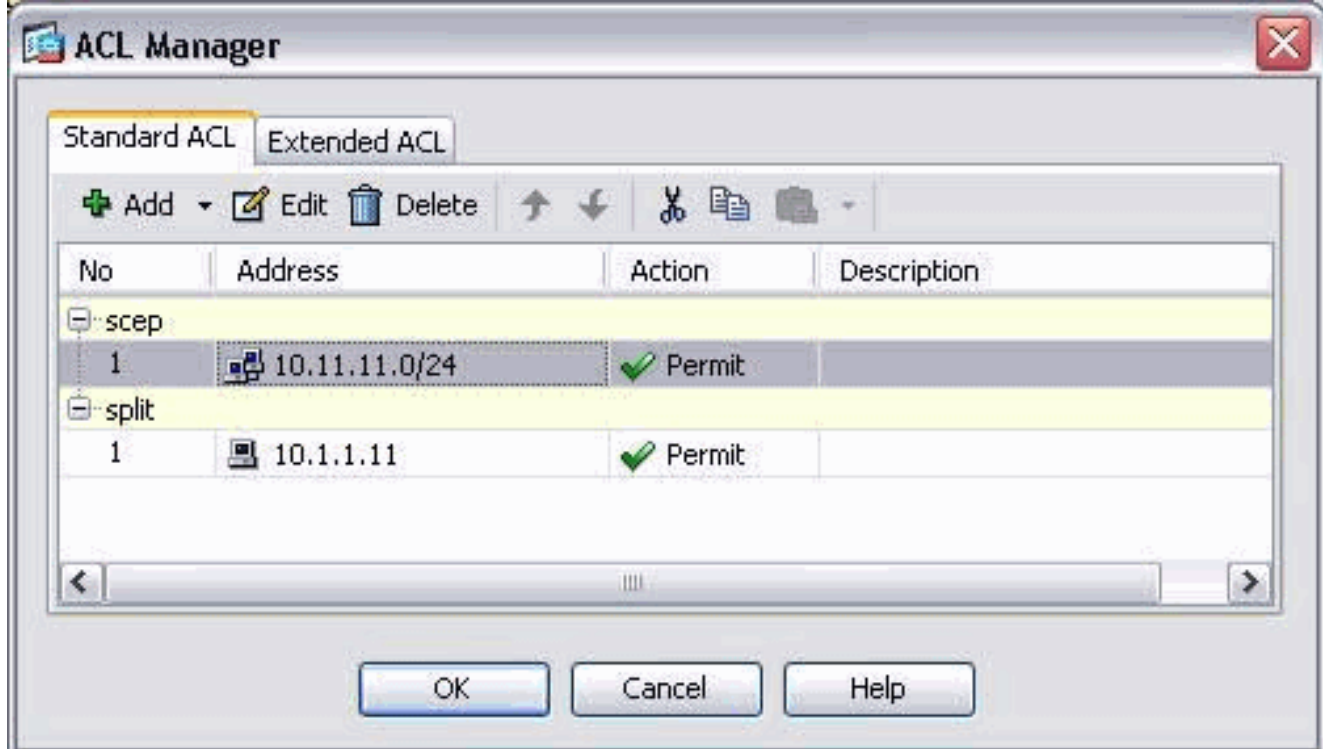
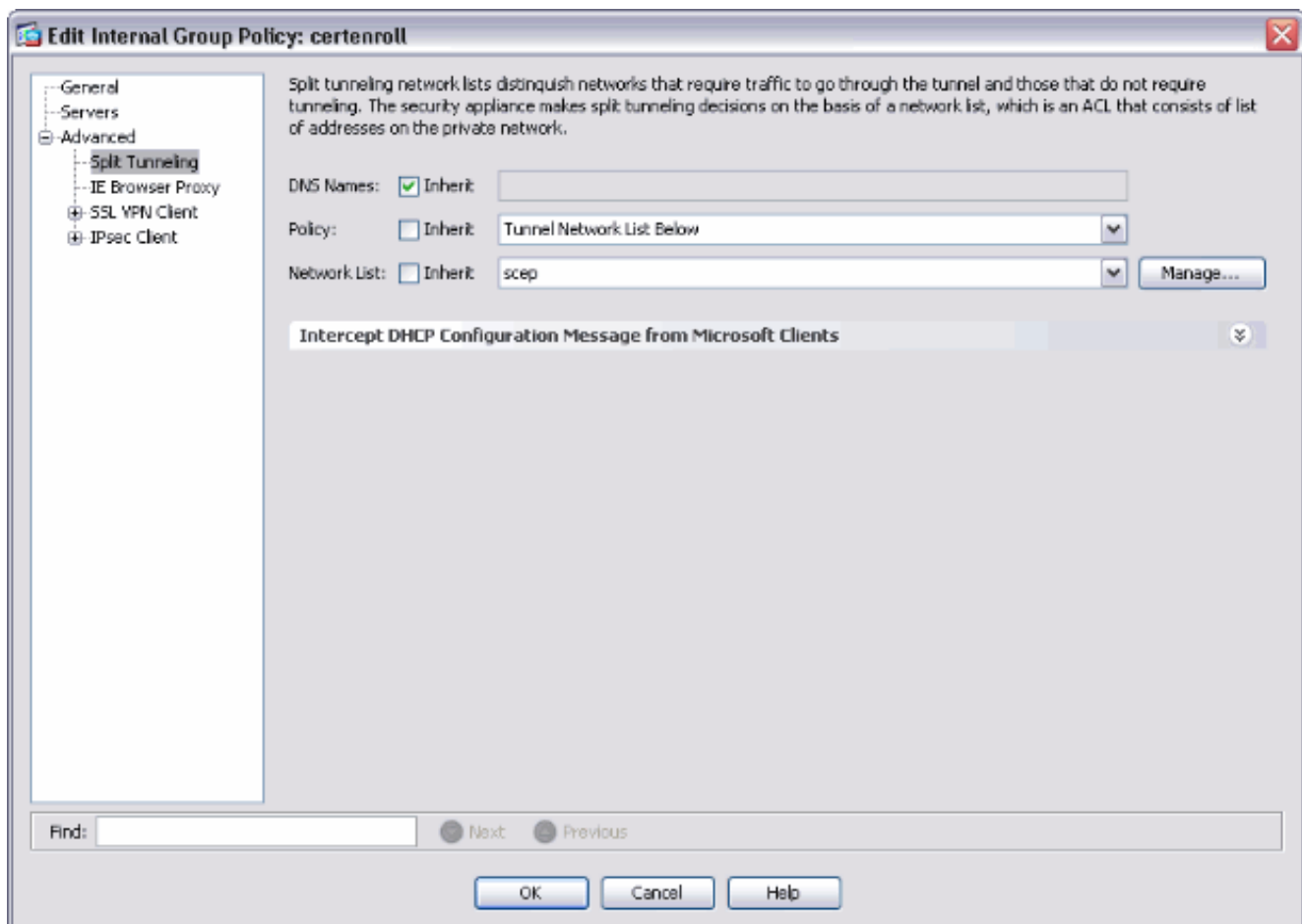
Maximum Connect Time: Inherit Unlimited [] minutes

Idle Timeout: Inherit Unlimited [] minutes

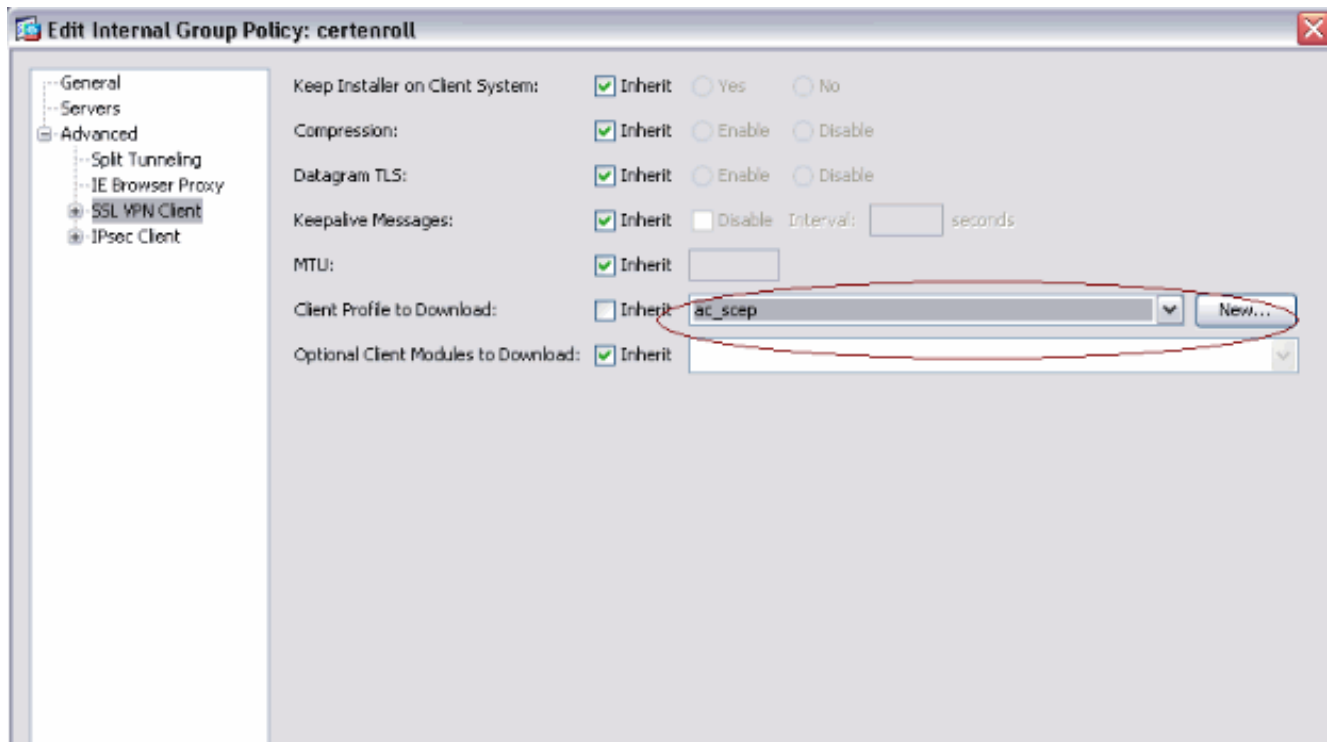
Find: [] Next Previous

OK Cancel Help

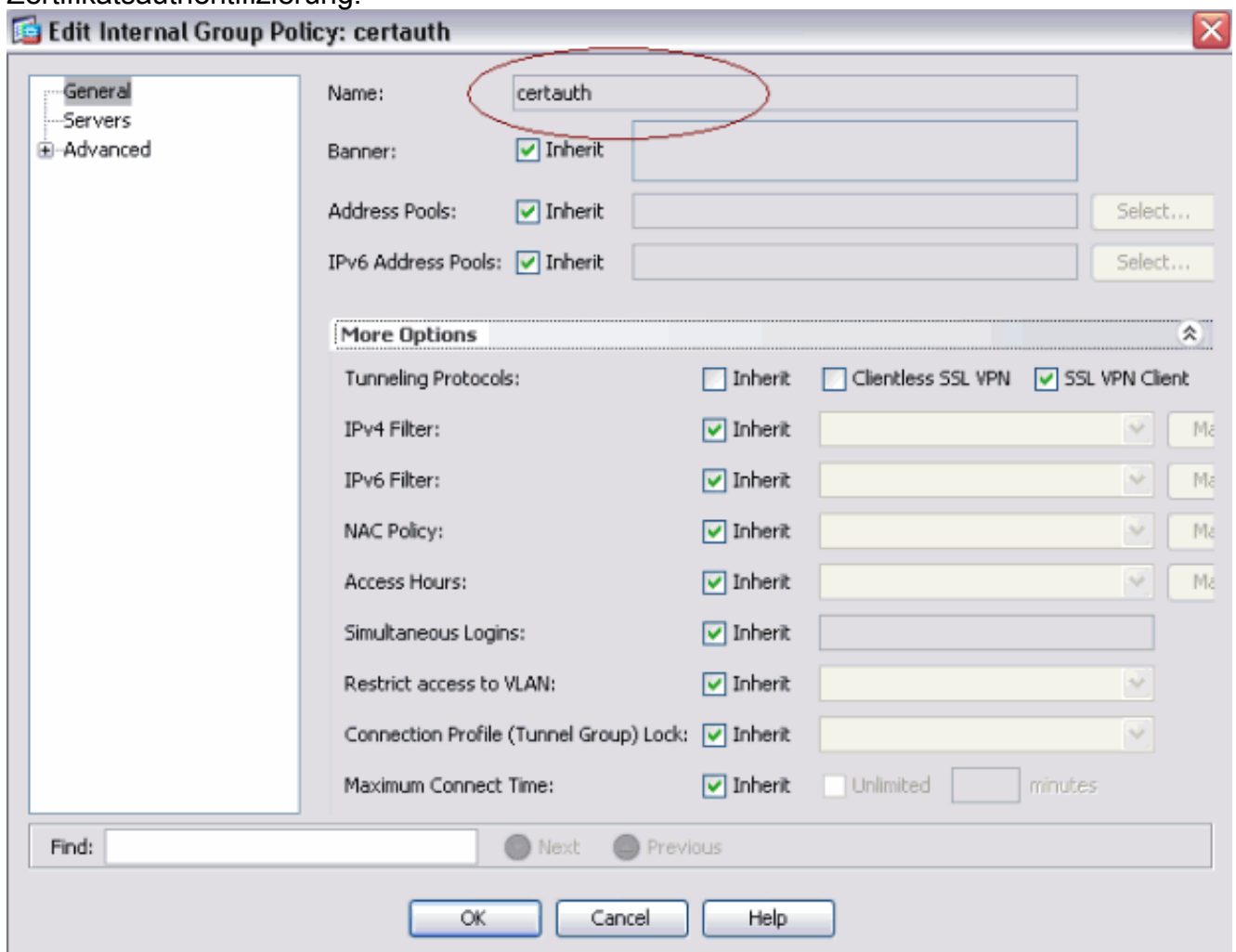
Fügen Sie einen Split-Tunnel für CA-Server hinzu. Erweitern Sie **Erweitert**, und wählen Sie dann **Getrenntes Tunneling aus**. Wählen Sie **unten** im Menü Richtlinien die Option Tunnel Network List (Tunnel-Netzwerkliste) aus, und klicken Sie auf **Manage (Verwalten)**, um die Zugriffskontrollliste hinzuzufügen.



Wählen Sie **SSL VPN Client** aus, und wählen Sie das Profil für die Registrierung im Menü **Client Profile to Download (Client-Profil zu Download)** aus.

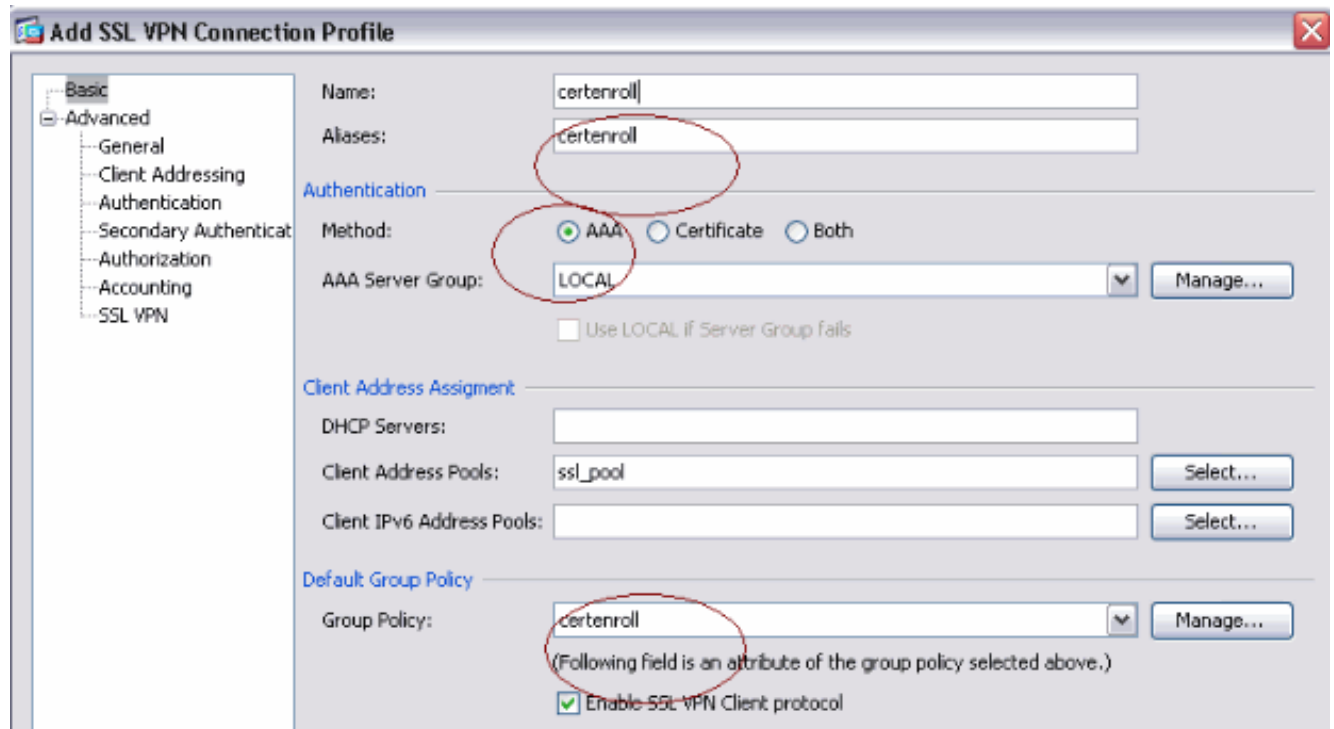


- Erstellen Sie eine weitere Gruppe mit dem Namen **certauth** für die Zertifikatsauthentifizierung.

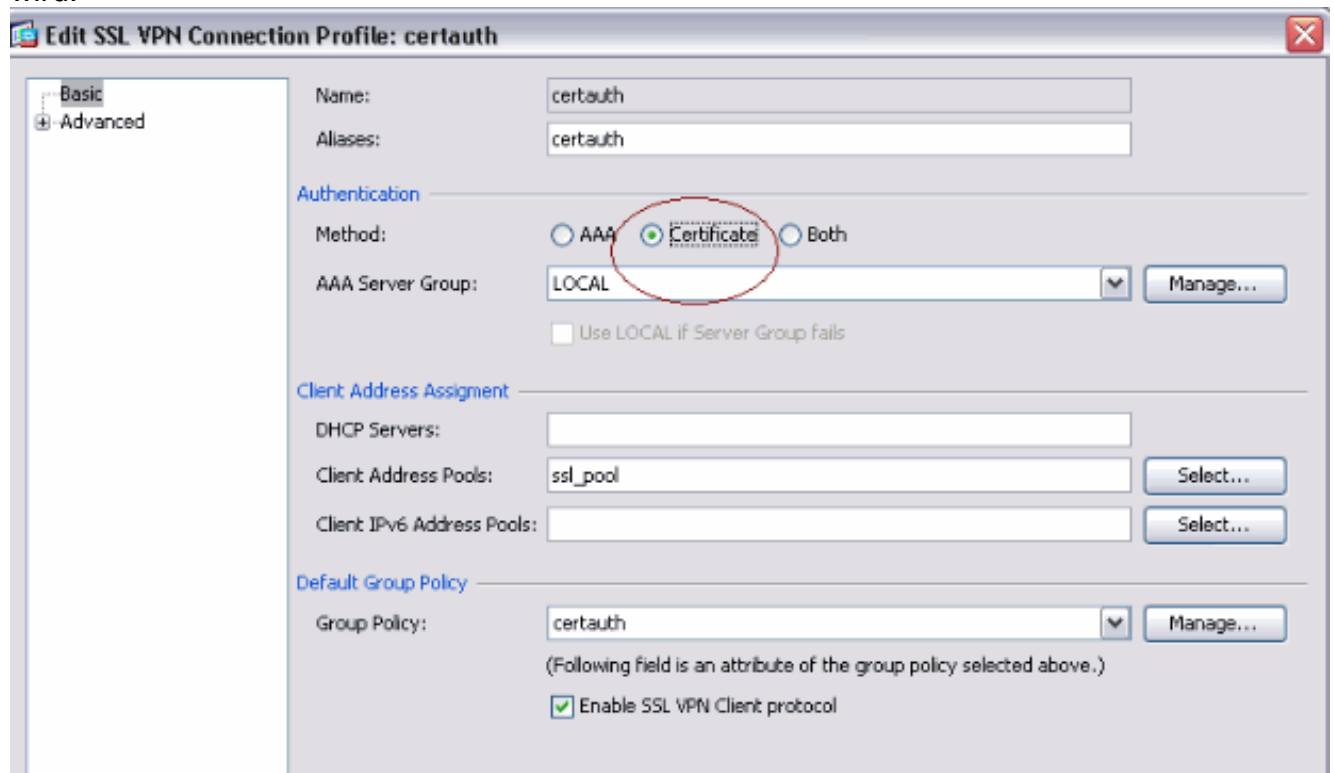


- Erstellen Sie ein certenroll-Verbindungsprofil. Wählen Sie **Remote Access VPN > Network Client Access > AnyConnect connection connection profiles (Remotezugriffs-VPN > Netzwerkclientzugriff > AnyConnect-Verbindungsprofile)** aus, und klicken Sie auf **Hinzufügen**. Geben Sie im Feld Aliase die Gruppe **certenroll** ein. **Hinweis:** Der Aliasname

muss mit dem im AnyConnect-Profil unter AutomaticSCEPHost verwendeten Wert übereinstimmen.



- Erstellen Sie ein anderes Verbindungsprofil mit dem Namen **certauth** mit Zertifikatauthentifizierung. Dies ist das tatsächliche Verbindungsprofil, das nach der Registrierung verwendet wird.



- Um sicherzustellen, dass die Verwendung von Alias aktiviert ist, aktivieren Sie **auf der Anmeldeseite** das Kontrollkästchen Verbindungsprofil, das durch seinen Alias identifiziert wird, zulassen. Andernfalls ist DefaultWebVPNGroup das Verbindungsprofil.

The screenshot shows the Cisco AnyConnect Configuration interface. The left sidebar contains a navigation tree with categories like Introduction, Network (Client) Access, IPsec Connection Profiles, Group Policies, Dynamic Access Policies, AnyConnect Customization/Localization, Address Assignment, Advanced, Endpoint Security, SSL VPN, Client Settings, Bypass Interface Access List, IPsec, ACL Manager, Clientless SSL VPN Access, Easy VPN Remote, AAA/Local Users, Secure Desktop Manager, Certificate Management, Language Localization, DHCP Server, DNS, and Advanced.

The main content area is titled "Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles". It contains the following sections:

- Access Interfaces:** A checkbox "Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below" is checked. Below it is a table:

Interface	Allow Access	Enable DTLS
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

 Below the table are input fields for "Access Port: 443" and "DTLS Port: 443", and a link "Click here to Assign Certificate to Interface."
- Login Page Setting:** A checkbox "Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile." is checked. This section is circled in red in the original image.
- Connection Profiles:** A description "Connection profile (tunnel group) specifies how user is authenticated and other parameters." is followed by "Add", "Edit", and "Delete" buttons. Below is a table:

Name	Enabled	Aliases	Authentication Method
certenroll	<input checked="" type="checkbox"/>	certenroll	AAA(LOCAL)
Sales	<input checked="" type="checkbox"/>	Sales	AAA(LOCAL)
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)
certauth	<input checked="" type="checkbox"/>	certauth	Certificate
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	default	AAA(LOCAL)

[AnyConnect SCEP testen](#)


In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Starten Sie den AnyConnect-Client, und stellen Sie eine Verbindung zum certenroll-Profil



her. AnyConnect leitet die Registrierungsanfrage über SCEP an den CA-Server

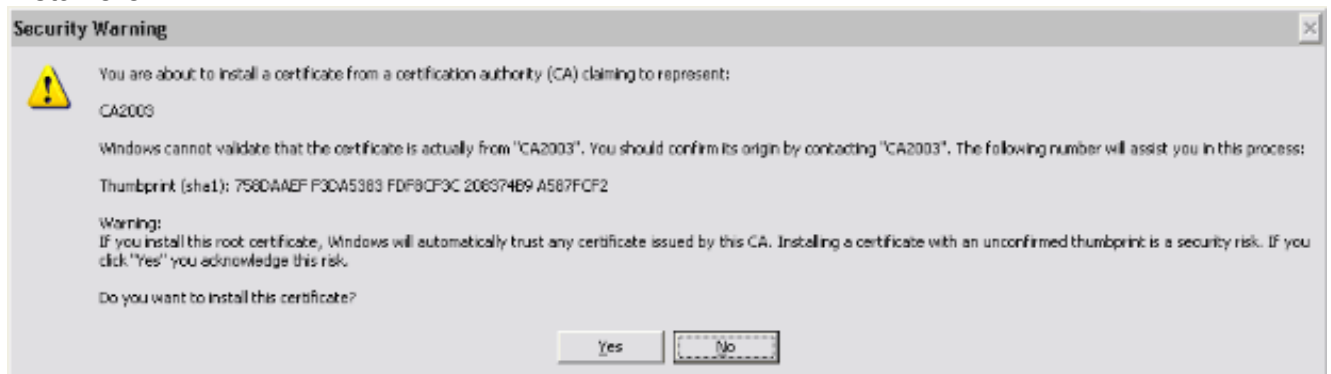


weiter.  AnyConnect durchläuft die Registrierungsanfrage direkt und nicht über den Tunnel, wenn die Schaltfläche **Zertifikat**



abrufen verwendet wird.

2. Diese Warnung wird angezeigt. Klicken Sie auf **Ja**, um den Benutzer und das Stammzertifikat zu installieren.

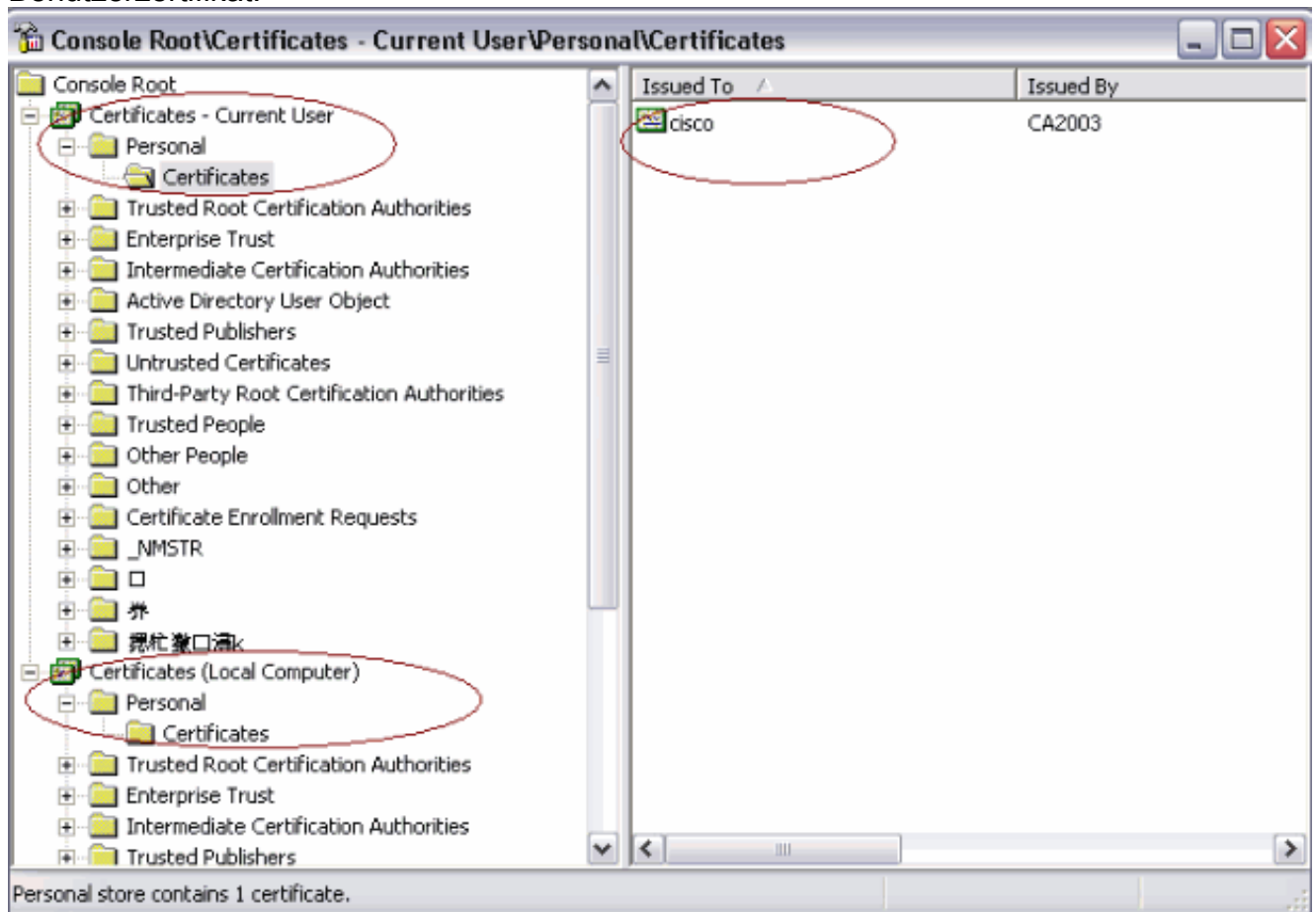


3. Wenn das Zertifikat registriert ist, stellen Sie eine Verbindung zum **sicheren** Profil her.

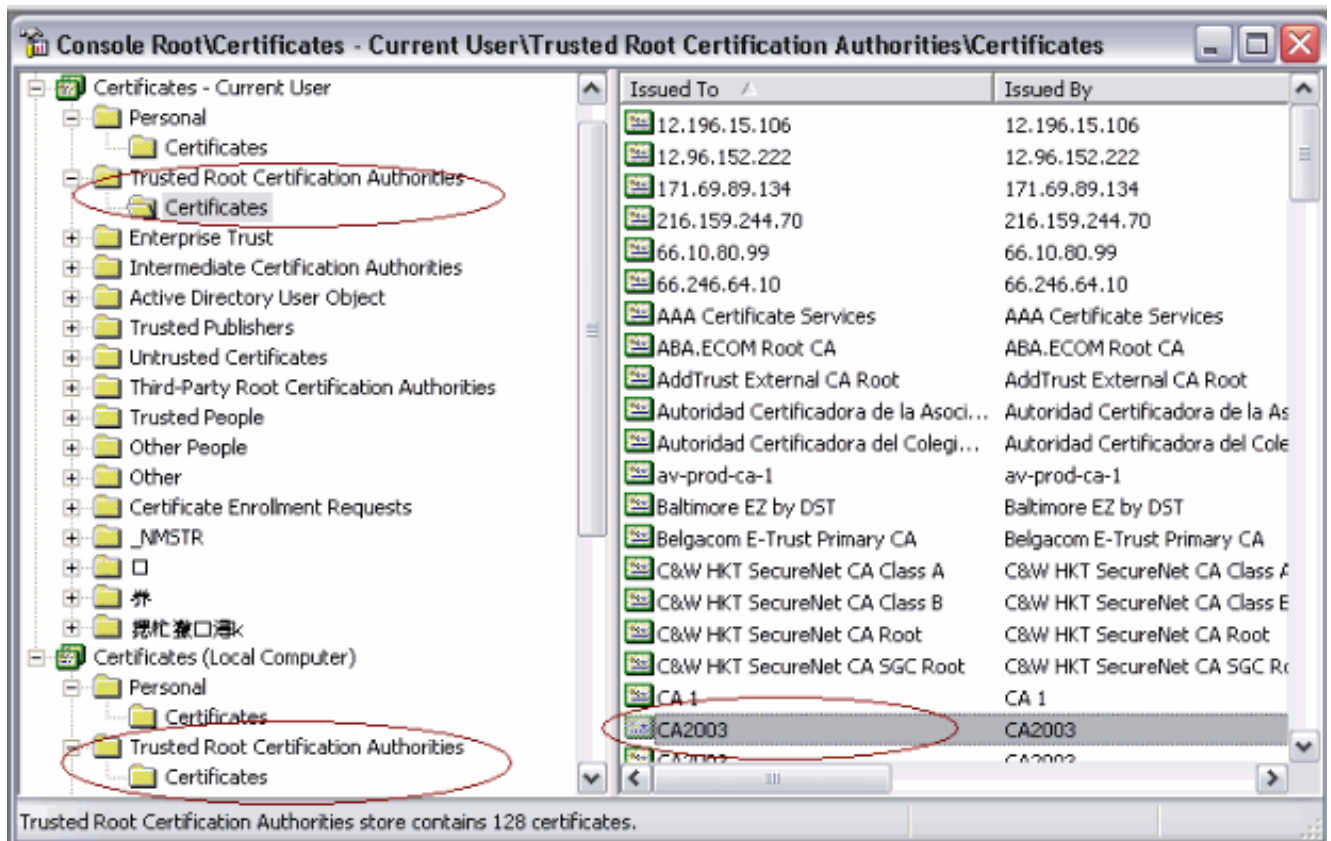
[Zertifikatsspeicherung in Microsoft Windows nach SCEP-Anforderung](#)

Gehen Sie wie folgt vor:

1. Klicken Sie auf **Start > Ausführen > MMC**.
2. Klicken Sie auf **Snap-In hinzufügen/entfernen**.
3. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zertifikate** aus.
4. Fügen Sie die Zertifikate **Mein Benutzerkonto** und **Computerkonto hinzu**. Dieses Bild zeigt das im Windows-Zertifikatsspeicher installierte Benutzerzertifikat:



Dieses Bild zeigt das im Windows-Zertifikatsspeicher installierte CA-Zertifikat:



Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Die SCEP-Registrierung für AnyConnect funktioniert nur, wenn die Zertifikatsauthentifizierung fehlschlägt. Wenn sie sich nicht anmeldet, überprüfen Sie den Zertifikatsspeicher. Wenn Zertifikate bereits installiert sind, löschen Sie sie und testen Sie sie erneut.
- Die SCEP-Registrierung funktioniert nur, wenn der Befehl **SSL Certificate-Authentication Interface außerhalb des Ports 443** verwendet wird. Weitere Informationen finden Sie unter den folgenden Cisco Bug-IDs: Cisco Bug-ID [CSCtf06778](#) (nur [registrierte](#) Kunden) - Die Anmeldung für AnyConnect SCEP funktioniert nicht mit Auth 2 des Zertifikats pro Gruppe. Cisco Bug-ID [CSCtf06844](#) (nur [registrierte](#) Kunden) - AnyConnect SCEP-Registrierung funktioniert nicht mit ASA Pro-Group-Zertifizierung
- Wenn sich der CA-Server außerhalb von ASA befindet, stellen Sie sicher, dass das Hairpinning mit dem Befehl für den **Datenverkehr mit derselben Sicherheit (permit intra-interface)** zugelassen wird. Fügen Sie außerdem die Befehle `nat outside` und `access list` hinzu, wie in diesem Beispiel gezeigt:

```
nat (outside) 1
access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87
```

Dabei steht 172.16.1.0 für den AnyConnect-Pool und 171.69.89.87 für die IP-Adresse des CA-Servers.

- Wenn sich der CA-Server im Inneren befindet, stellen Sie sicher, dass dieser in die Split-Tunnel-Zugriffsliste für die **certenroll**-Gruppenrichtlinie aufgenommen wird. In diesem Dokument wird davon ausgegangen, dass sich der CA-Server im Inneren befindet.

```
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
```

Zugehörige Informationen

- [Administratorhandbuch für den Cisco AnyConnect VPN-Client, Version 2.4](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)