

# ASA 8.x: Configuratie AnyConnect SSL VPN CAC-SmartCards voor Windows

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Cisco ASA-configuratie](#)

[Overwegingen bij implementatie](#)

[Configuratie van verificatie, autorisatie, accounting \(AAA\)](#)

[LDAP-server configureren](#)

[Certificaten beheren](#)

[Toetsen genereren](#)

[CA-certificaten \(root\) installeren](#)

[Inschrijven ASA en identiteitscertificaat installeren](#)

[AnyConnect VPN-configuratie](#)

[Een IP-adresgroep maken](#)

[Tunnelgroep en groepsbeleid maken](#)

[Tunnelgroep-interface en afbeeldingsinstellingen](#)

[Regels voor matching van certificaten \(indien OCSP wordt gebruikt\)](#)

[OCSP configureren](#)

[OCSP-antwoordcertificaat configureren](#)

[CA configureren voor gebruik van OCSP](#)

[OCSP-regels configureren](#)

[Configuratie Cisco AnyConnect-client](#)

[Cisco AnyConnect VPN-client downloaden - Windows](#)

[Cisco AnyConnect VPN-client starten - Windows](#)

[Nieuwe verbinding](#)

[Externe toegang starten](#)

[Bijlage A - LDAP-toewijzing en DAP](#)

[Scenario 1: Active Directory-handhaving met inbellen via externe toegangsrechten - Toegang toestaan/weigeren](#)

[Active Directory instellen](#)

[ASA-configuratie](#)

[Scenario 2: Active Directory Enforcement met groepslidmaatschap om toegang toe te staan/te weigeren](#)

[Active Directory instellen](#)

[ASA-configuratie](#)

[Scenario 3: Dynamisch toegangsbeleid voor meerdere leden van Kenmerken](#)

[ASA-configuratie](#)

---

[Bijlage B - ASA CLI-configuratie](#)

[Bijlage C - Probleemoplossing](#)

[AAA en LDAP voor probleemoplossing](#)

[Voorbeeld 1: Toegestane verbinding met juiste attribuuttoewijzing](#)

[Voorbeeld 2: Toegestane verbinding met verkeerd geconfigureerde Cisco-kenmerktoewijzing](#)

[DAP voor probleemoplossing](#)

[Voorbeeld 1: Toegestane verbinding met DAP](#)

[Voorbeeld 2: Ontkende verbinding met DAP](#)

[Certificaatautoriteit voor probleemoplossing/OCSP](#)

[Bijlage D - LDAP-objecten controleren in MS](#)

[LDAP-viewer](#)

[Active Directory-interfaceeditor](#)

[Aanhangsel E](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document biedt een voorbeeldconfiguratie op Cisco adaptieve security applicatie (ASA) voor AnyConnect VPN externe toegang voor Windows met de Common Access Card (CAC) voor verificatie.

Dit document is bedoeld voor de configuratie van Cisco ASA met Adaptive Security Device Manager (ASDM), Cisco AnyConnect VPN-client en Microsoft Active Directory (AD)/Lichtgewicht Directory Access Protocol (LDAP).

De configuratie in deze handleiding maakt gebruik van Microsoft AD/LDAP-server. Dit document bevat ook geavanceerde functies zoals OCSP, LDAP-attribuutkaarten en Dynamic Access Policies (DAP).

## Voorwaarden

### Vereisten

Een basiskennis van Cisco ASA, Cisco AnyConnect Client, Microsoft AD/LDAP en Public Key Infrastructure (PKI) is nuttig voor een goed begrip van de volledige installatie. Bekendheid met AD-groepslidmaatschap, gebruikerseigenschappen en LDAP-objecten helpen bij de correlatie van het autorisatieproces tussen certificaatkenmerken en AD/LDAP-objecten.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5500 Series adaptieve security applicatie (ASA) die de softwareversie 8.0(x) en hoger uitvoert
- Cisco Adaptieve Security Device Manager (ASDM) versie 6.x voor ASA 8.x

- Cisco AnyConnect VPN-client voor Windows

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Cisco ASA-configuratie

Deze sectie behandelt de configuratie van Cisco ASA via ASDM. Het dekt de noodzakelijke stappen om een VPN externe toegangstunnel te implementeren via een SSL AnyConnect-verbinding. Het CAC-certificaat wordt gebruikt voor verificatie en het kenmerk User Principal Name (UPN) in het certificaat wordt ingevuld in de actieve directory voor autorisatie.

### Overwegingen bij implementatie

- Deze handleiding is NIET van toepassing op basisconfiguraties zoals interfaces, DNS, NTP, routing, apparaattoegang, ASDM-toegang enzovoort. Er wordt aangenomen dat de netwerkexploitant bekend is met deze configuraties.

Raadpleeg [Multifunctionele security applicaties](#) voor meer informatie.

- De secties die in rood worden gemarkeerd zijn verplichte configuraties die nodig zijn voor eenvoudige VPN-toegang. Een VPN-tunnel kan bijvoorbeeld worden geconfigureerd met de CAC-kaart zonder OCSP-controles, LDAP-toewijzingen en DAP-controles (Dynamic Access Policy) uit te voeren. DoD machtigt OCSP controleren maar de tunnel werkt zonder OCSP geconfigureerd.
- De secties die in BLAUW worden gemarkeerd, zijn geavanceerde functies die kunnen worden opgenomen om meer beveiliging aan het ontwerp toe te voegen.
- ASDM en AnyConnect/SSL VPN kunnen niet dezelfde poorten op dezelfde interface gebruiken. Het wordt aanbevolen om de poorten op de ene of de andere te wijzigen om toegang te krijgen. Gebruik bijvoorbeeld poort 445 voor ASDM en laat poort 443 voor AC/SSL VPN staan. De ASDM URL-toegang is gewijzigd in 8.x. Gebruik `https://<ip_address>:<port>/admin.html`.
- De ASA afbeelding vereist is minimaal 8.0.2.19 en ASDM 6.0.2.
- AnyConnect/CAC wordt ondersteund met Vista.
- Zie [Bijlage A](#) voor LDAP & Dynamic Access Policy mapping-voorbeelden voor extra beleidshandhaving.
- Zie [Bijlage D](#) voor hoe u LDAP-objecten in MS kunt controleren.
- Zie [Verwante informatie](#) voor een lijst met toepassingspoorten voor firewallconfiguratie.

# Configuratie van verificatie, autorisatie, accounting (AAA)

U wordt geauthentiseerd met het gebruik van het certificaat in hun Gemeenschappelijke Toegangskaat (CAC) door de server van de Autoriteit van het DISACertificaat (CA) of de server van CA van hun eigen organisatie. Het certificaat moet geldig zijn voor externe toegang tot het netwerk. Naast de verificatie moet u ook geautoriseerd zijn om een Microsoft Active Directory of Lichtgewicht Directory Access Protocol (LDAP)-object te gebruiken. Het Ministerie van Defensie (DoD) vereist het gebruik van het attribuut Gebruiker Principal Name (UPN) voor autorisatie, dat deel uitmaakt van de sectie Onderwerp Alternatieve Naam (SAN) van het certificaat. UPN of EDI/PI moet in dit formaat zijn, 1234567890@mil. Deze configuraties tonen hoe u de AAA-server in de ASA kunt configureren met een LDAP-server voor autorisatie. Zie [Bijlage A](#) voor aanvullende configuratie met LDAP-objecttoewijzing.

## LDAP-server configureren

Voer de volgende stappen uit:

1. Kies Remote Access VPN > AAA-instelling > AAA-servergroep.
2. Klik in de tabel AAA-servergroepen op Add 3.
3. Voer de naam van de servergroep in en kies LDAP in het keuzerondje Protocol. Zie figuur 1.
4. Klik in Servers in de geselecteerde groepstabel op Toevoegen. Zorg dat de server die u hebt gemaakt, in de vorige tabel is gemarkeerd.
5. Voltooi de volgende stappen in het venster AAA-server bewerken. Zie figuur 2.

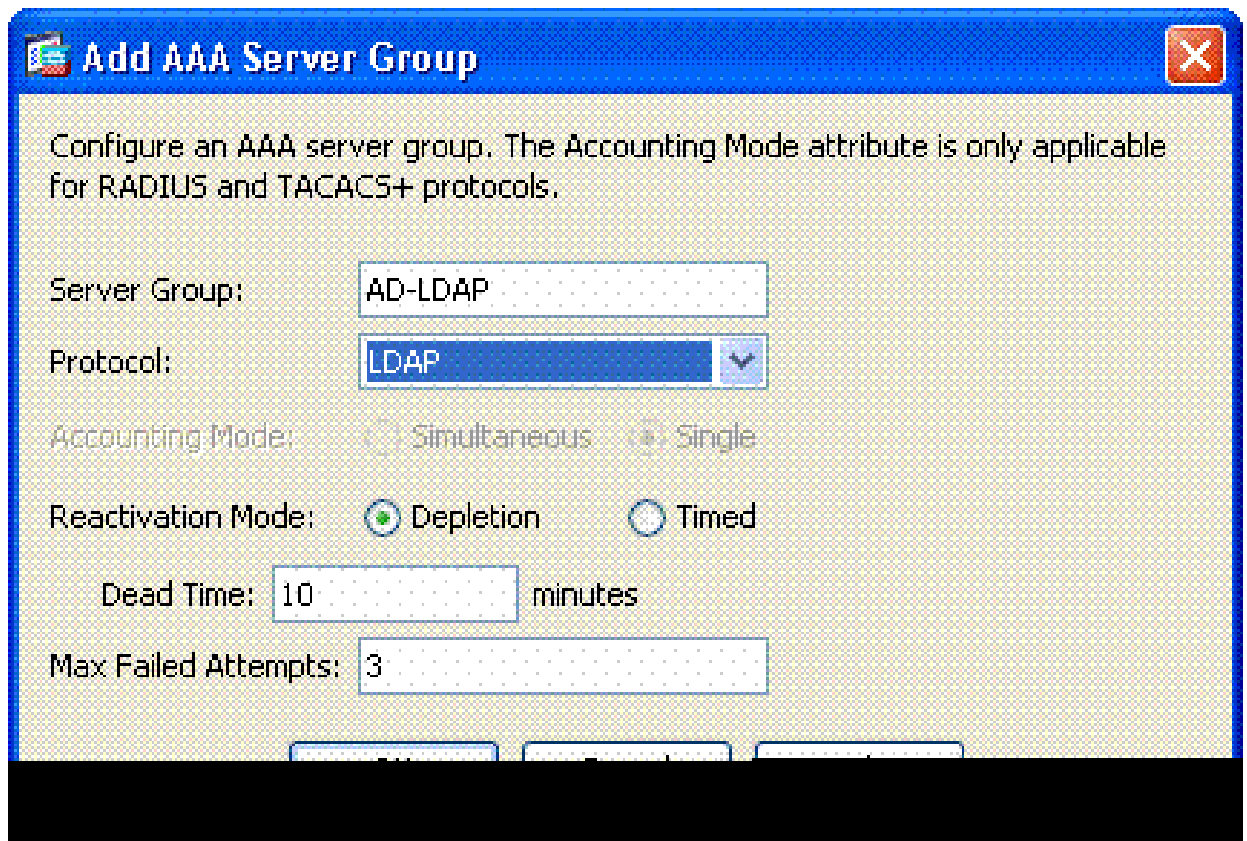
---

Opmerking: Kies de optie LDAP over SSL inschakelen als uw LDAP/AD is geconfigureerd voor dit type verbinding.

---

- a. Kies de interface waar de LDAP zich bevindt. Deze gids toont binnen de interface.
- b. Voer het IP-adres van de server in.
- c. Voer de serverpoort in. De standaard LDAP poort is 389.
- d. Kies het servertype.
- e. Voer Base-DN in. Vraag uw AD/LDAP-beheerder om deze waarden.

Afbeelding 1



- f. Kies het juiste antwoord in het kader van de toepassingsoptie. Dit is afhankelijk van de basis-DN. Vraag uw AD/LDAP-beheerder om hulp.
- g. Voer in het attribuut name userPrincipalName in. Dit is het kenmerk dat wordt gebruikt voor gebruikersautorisatie in de AD/LDAP-server.
- h. Voer in het inlogbestand DN de beheerder DN in.

---

Opmerking: u hebt beheerdersrechten of rechten om de LDAP-structuur te bekijken/doorzoeken die gebruikersobjecten en groepslidmaatschap omvat.

---

- i. Voer in het inlogwachtwoord het wachtwoord van de beheerder in.
- j. Laat de LDAP-eigenschap aan niets over.

Figuur 2

Opmerking: u gebruikt deze optie later in de configuratie om andere AD/LDAP-  
objecten toe te voegen voor autorisatie.

k. Kies OK.

6. Kies OK.

## Certificaten beheren

Er zijn twee stappen om certificaten op de ASA te installeren. Installeer eerst de CA-certificaten

(Root and Subordinate Certificate Authority) die nodig zijn. Ten tweede, schrijf ASA in bij een specifieke CA en verkrijg het identiteitscertificaat. DoD PKI maakt gebruik van deze certificaten, Root CA2, Class 3 Root, CA## Intermediate waarmee de ASA is ingeschreven, ASA ID-certificaat en OCSP-certificaat. Maar als u ervoor kiest geen OCSP te gebruiken, hoeft het OCSP-certificaat niet te worden geïnstalleerd.

---

Opmerking: Neem contact op met uw beveiligingscontactpunt om basiscertificaten te verkrijgen en instructies over hoe u zich kunt inschrijven voor een identiteitsbewijs voor een apparaat. Een SSL-certificaat moet voldoende zijn voor de ASA voor toegang op afstand. Een dubbel SAN-certificaat is niet vereist.

---

Opmerking: de lokale machine moet ook de DoD CA-keten hebben geïnstalleerd. De certificaten kunnen worden bekeken in de Microsoft Certificate Store met Internet Explorer. DoD heeft een batchbestand geproduceerd dat automatisch alle CA's aan de machine toevoegt. Vraag uw PKI POC om meer informatie.

---

Opmerking: DoD CA2 en Class 3 Root en het ASA ID en CA tussenproduct dat de ASA cert heeft afgegeven, zouden de enige CA's moeten zijn die nodig zijn voor gebruikersverificatie. Alle huidige CA-tussenproducten vallen onder de CA2- en Class 3 Root-keten en worden vertrouwd zolang de CA2- en Class 3-roots worden toegevoegd.

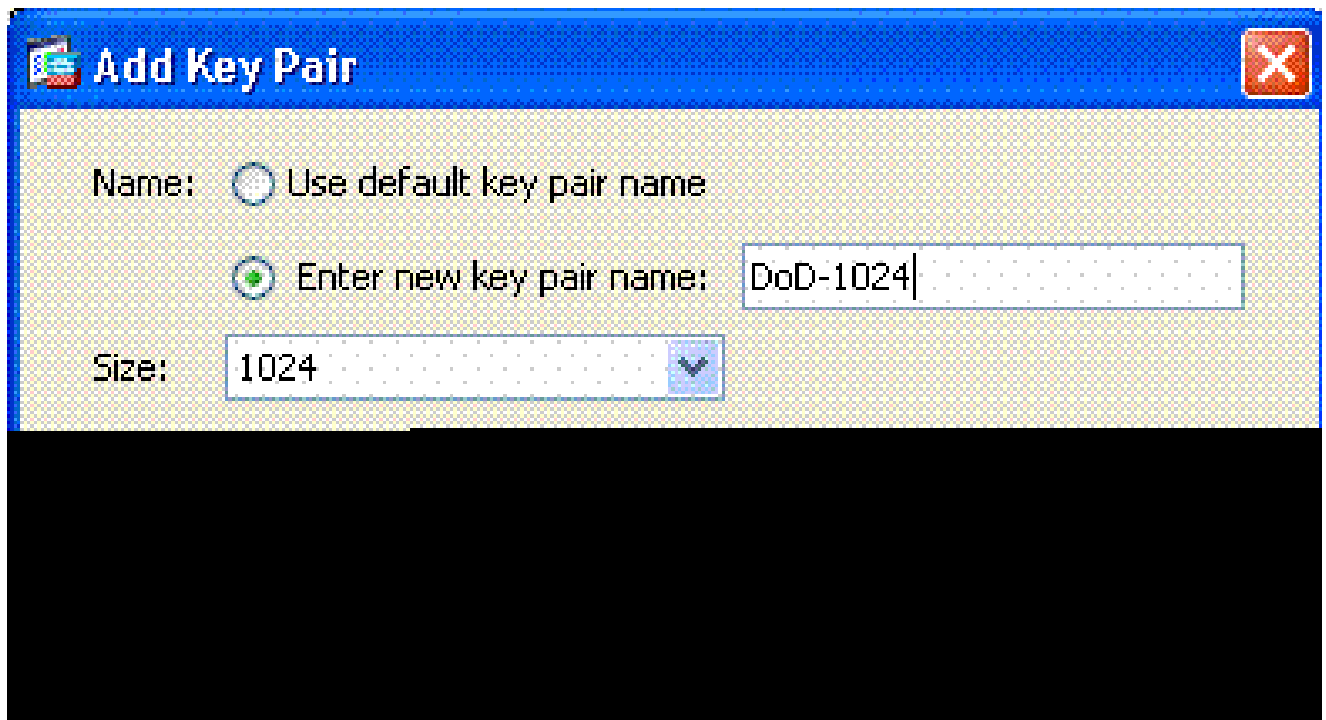
---

## Toetsen genereren

Voer de volgende stappen uit:

1. Kies Remote Access VPN > Certificaatbeheer > Identiteitscertificaat > Toevoegen.
2. Kies Een nieuw ID-certificaat toevoegen en dan Nieuw bij de sleutelpaaroptie.
3. Voer in het venster Toetsenpaar toevoegen een sleutelnaam in, DoD-1024. Klik op de radio om een nieuwe sleutel toe te voegen. Zie figuur 3.

Afbeelding 3



4. Kies de grootte van de toets.
5. Gebruik voor algemene doeleinden behouden.
6. Klik op Generate Now (Nu genereren).

---

Opmerking: DoD Root CA 2 gebruikt een 2048-bits sleutel. Er moet een tweede sleutel met een 2048-bits sleutelpaar worden gegenereerd om deze CA te kunnen gebruiken. Voltooi de voorgaande stappen om een tweede toets toe te voegen.

---

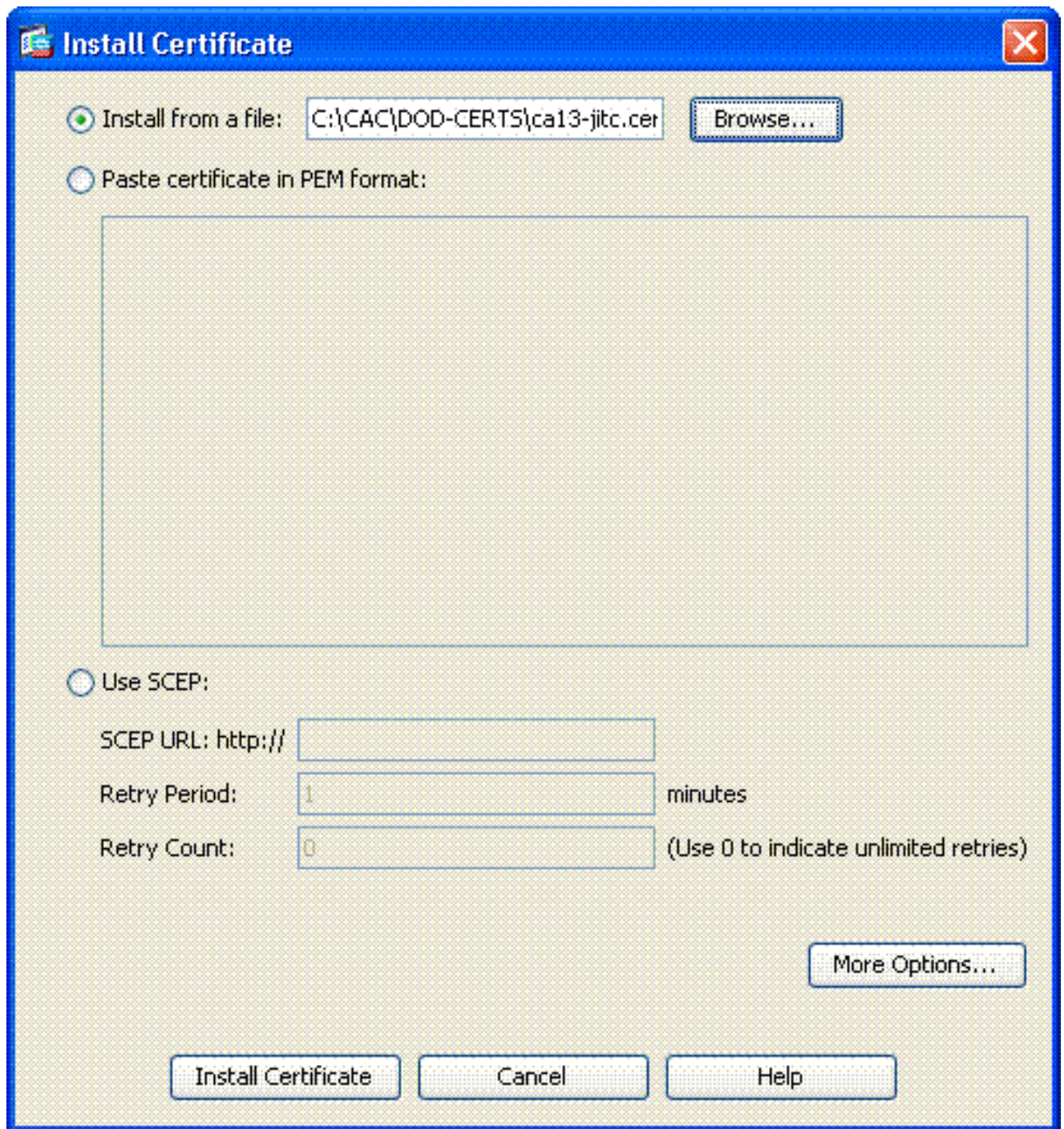
## CA-certificaten (root) installeren

Voer de volgende stappen uit:

1. Kies Remote Access VPN > Certificaatbeheer > CA-certificaat > Toevoegen.
2. Kies Installeren uit bestand en blader naar het certificaat.
3. Kies Installatiecertificaat.

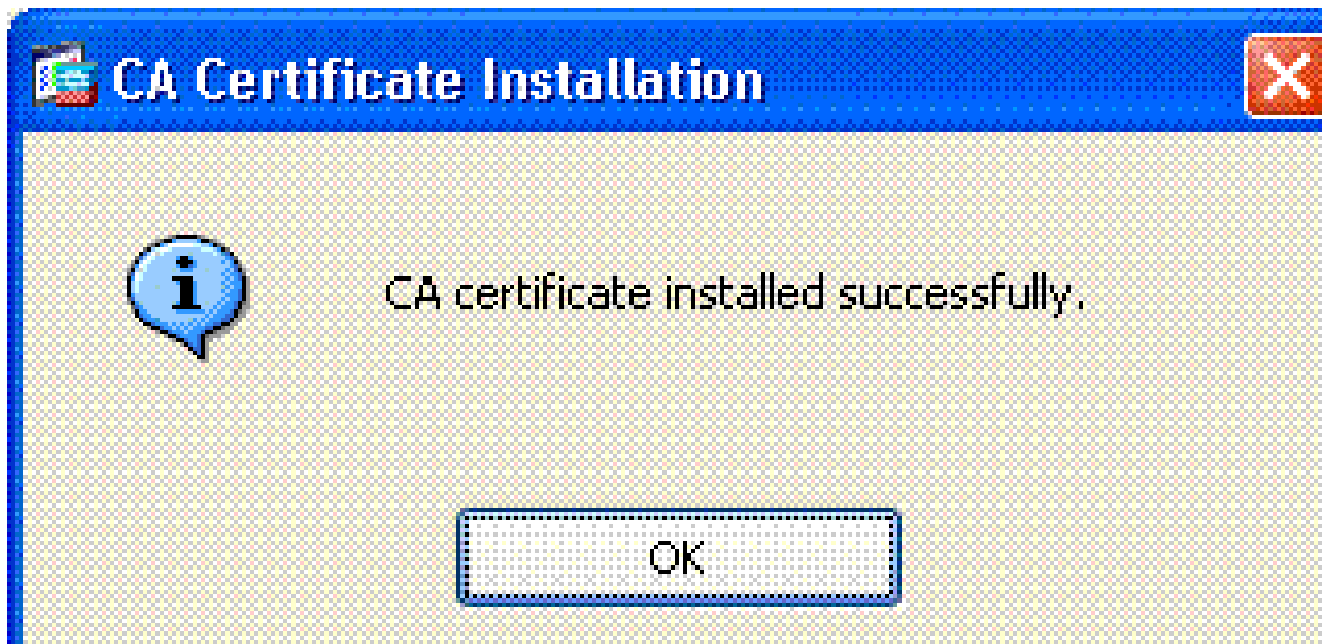
Afbeelding 4: Root-certificaat installeren





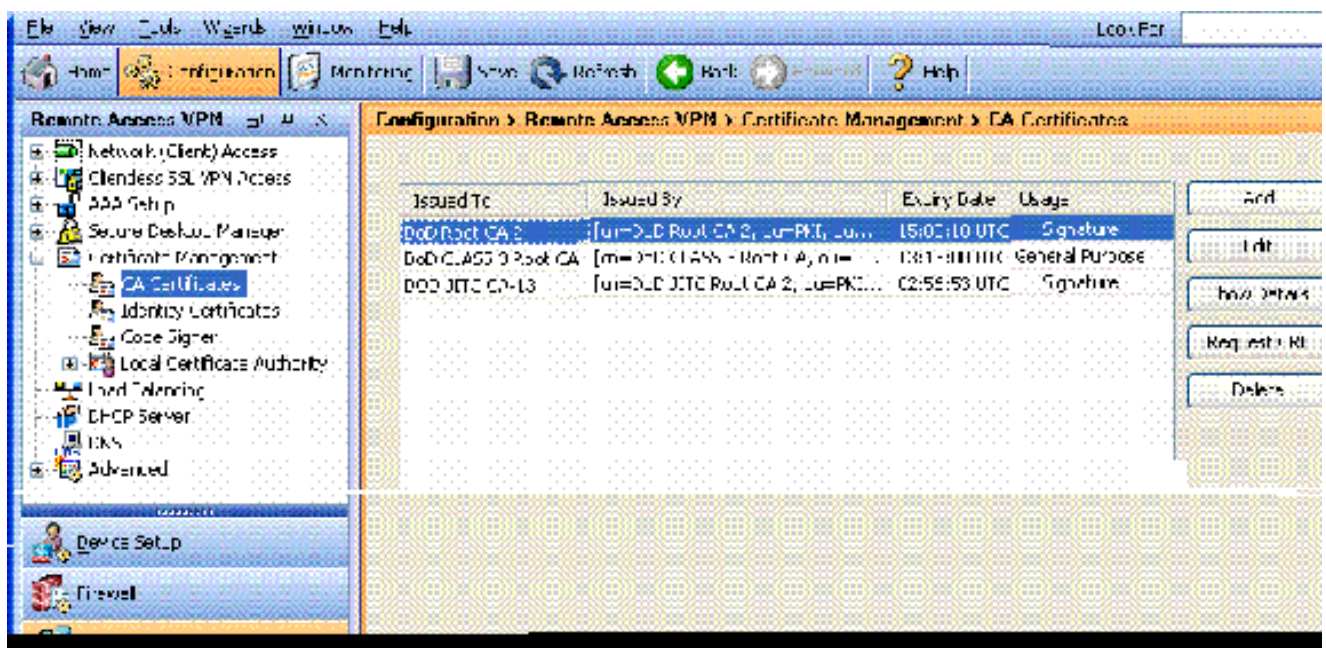
4. Dit venster moet verschijnen. Zie figuur 5.

Afbeelding 5



Opmerking: Herhaal stap 1 tot en met 3 voor elk certificaat dat u wilt installeren. DoD PKI vereist een certificaat voor elk van deze: Root CA 2, Class 3 Root, CA## Intermediate, ASA ID en OCSP Server. Het OCSP-certificaat is niet nodig als u geen OCSP gebruikt.

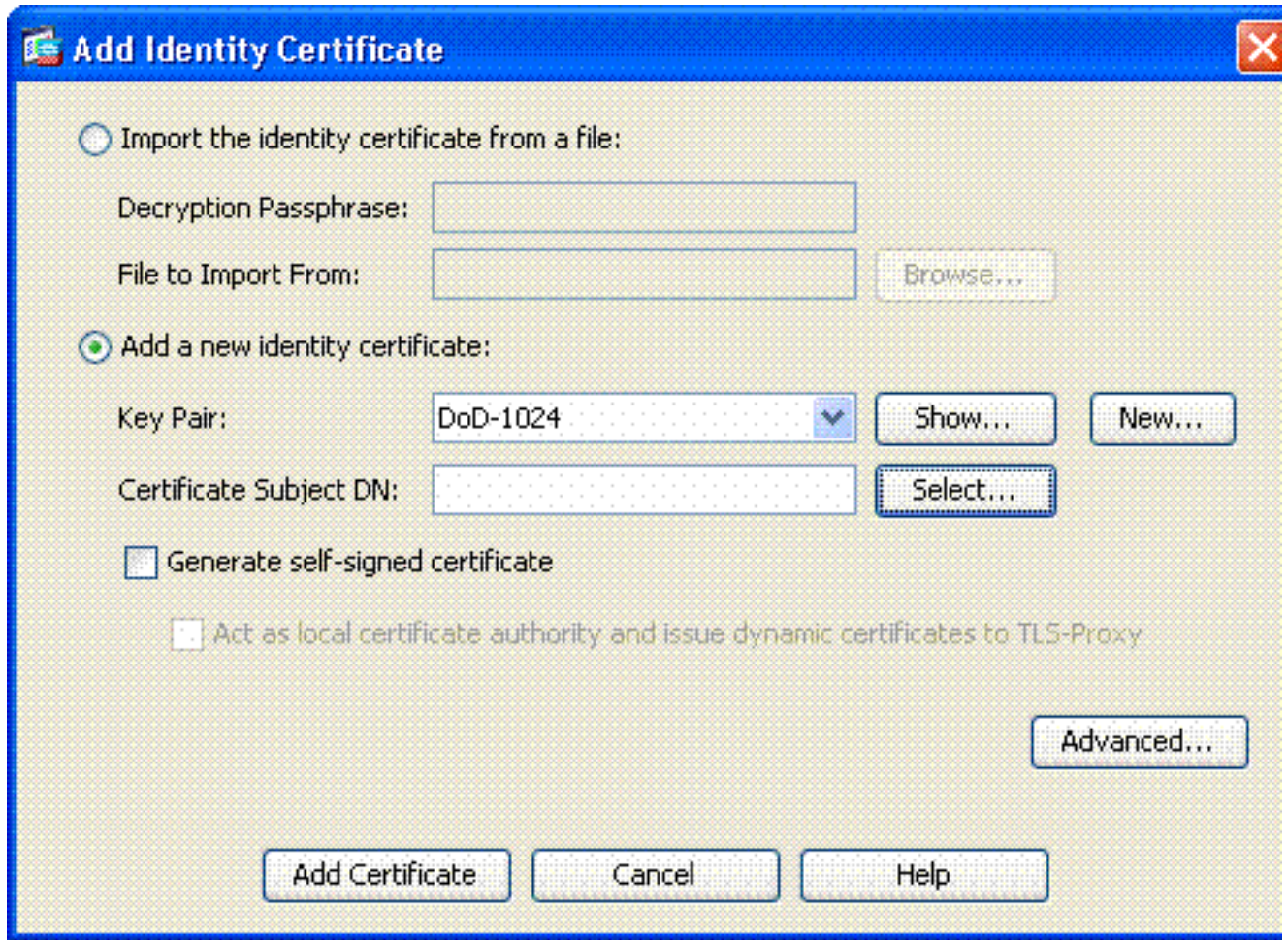
Afbeelding 6: Root-certificaat installeren



## Inschrijven ASA en identiteitscertificaat installeren

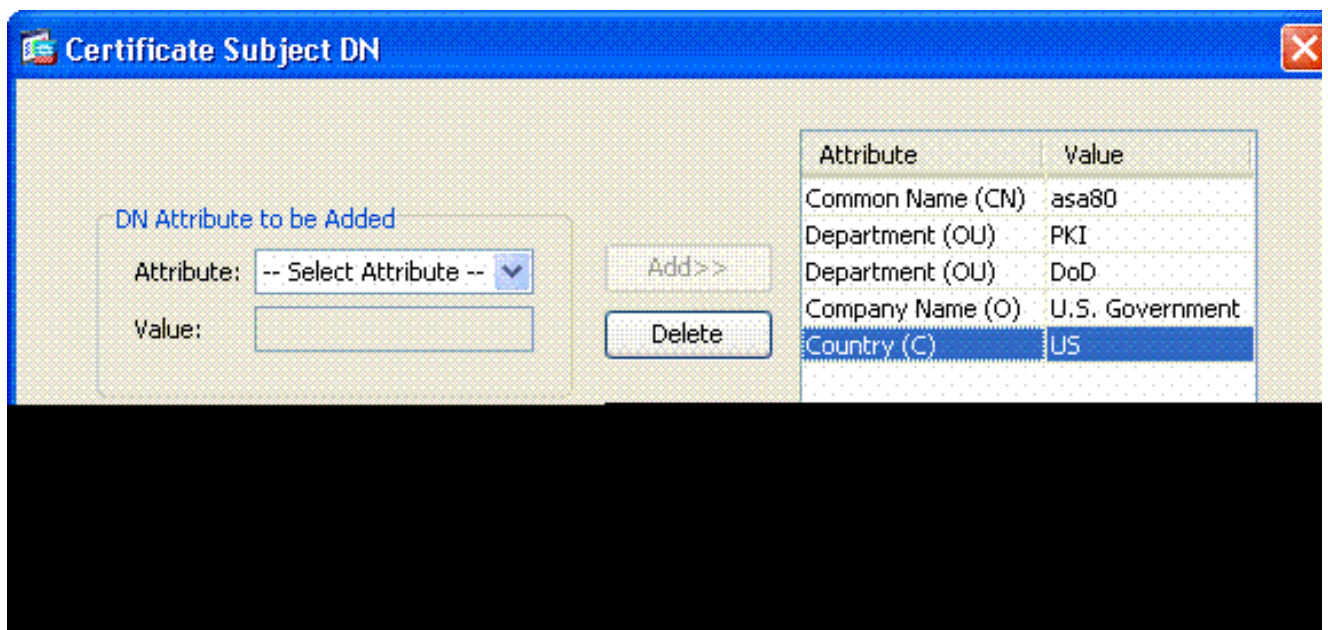
1. Kies Remote Access VPN > Certificaatbeheer > Identiteitscertificaat > Toevoegen.
2. Kies Een nieuw ID-certificaat toevoegen.
3. Kies het DoD-1024 sleutelpaar. Zie figuur 7

Afbeelding 7: Parameters voor identiteitscertificaten



4. Ga naar het veld Certificaatonderwerp DN en klik op Selecteren.
5. Voer in het venster Certificaatonderwerp DN de informatie van het apparaat in. Zie bijvoorbeeld afbeelding 8.

Afbeelding 8: ISDN bewerken



6. Kies OK.

---

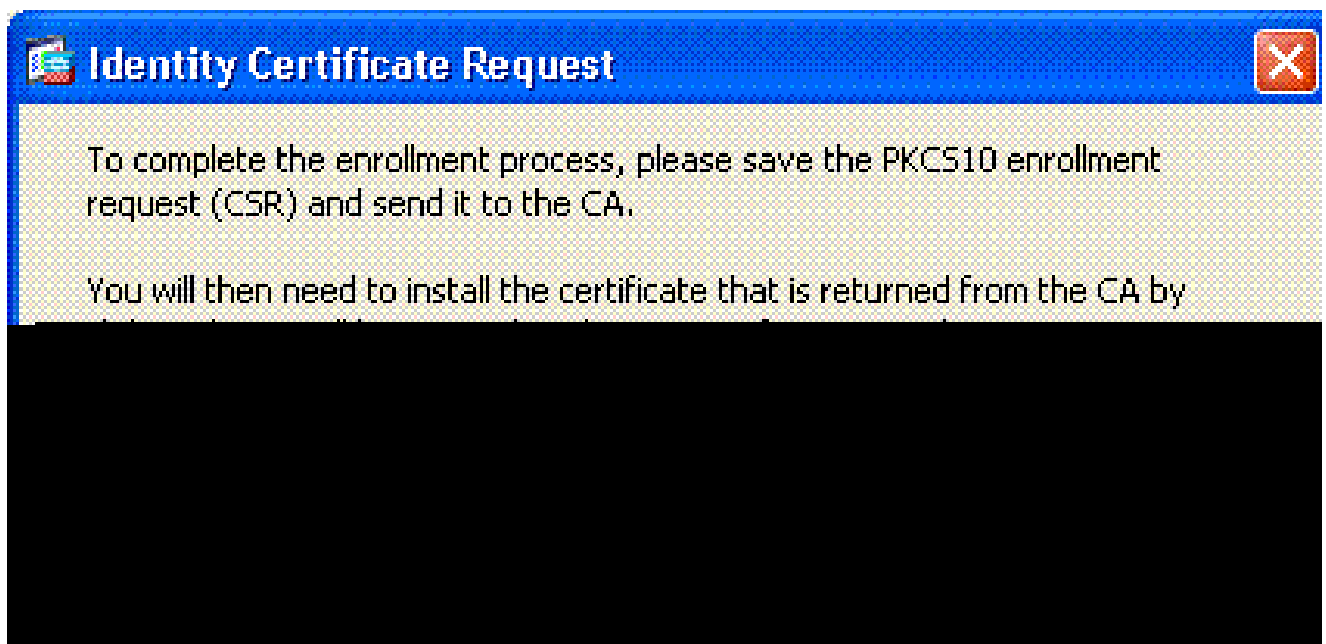
Opmerking: Zorg ervoor dat u de hostnaam gebruikt van het apparaat dat in uw systeem is geconfigureerd wanneer u de onderwerp-DN toevoegt. De PKI POC kan u vertellen welke verplichte velden er nodig zijn.

---

7. Kies Certificaat toevoegen.

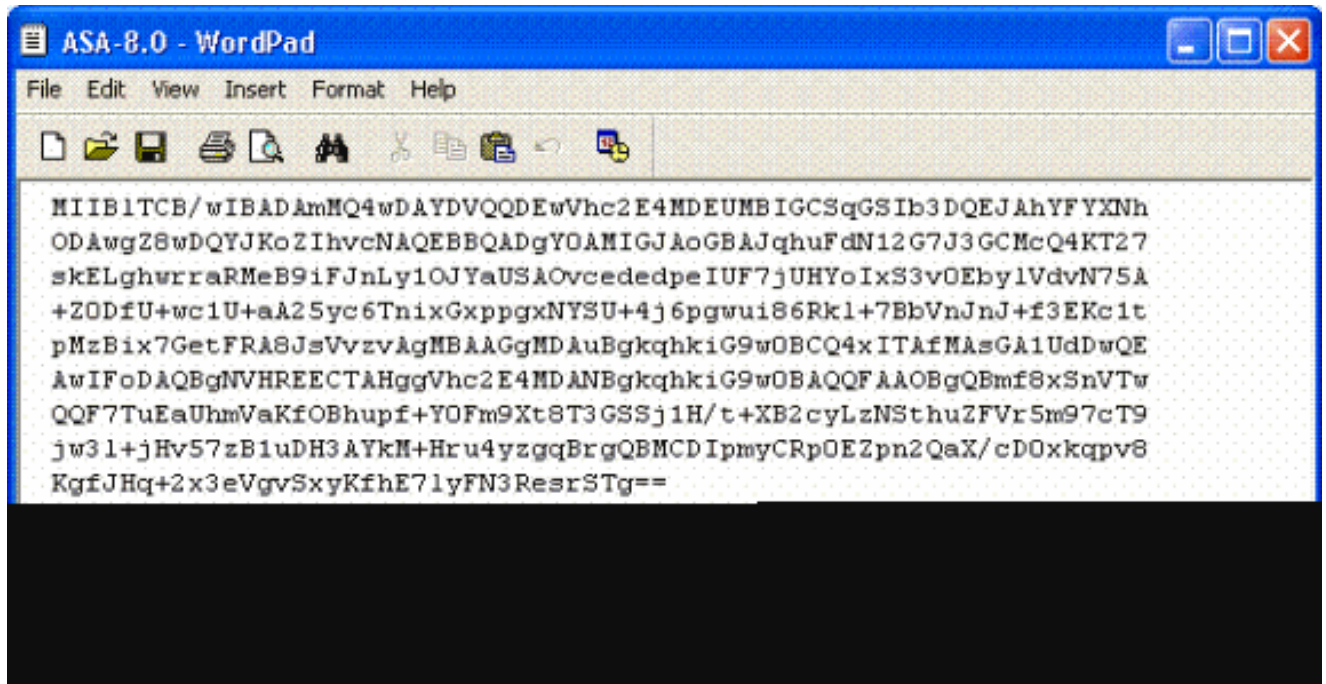
8. Klik op Bladeren om de map te selecteren waarin u de aanvraag wilt opslaan. Zie figuur 9.

Afbeelding 9: Certificaataanvraag



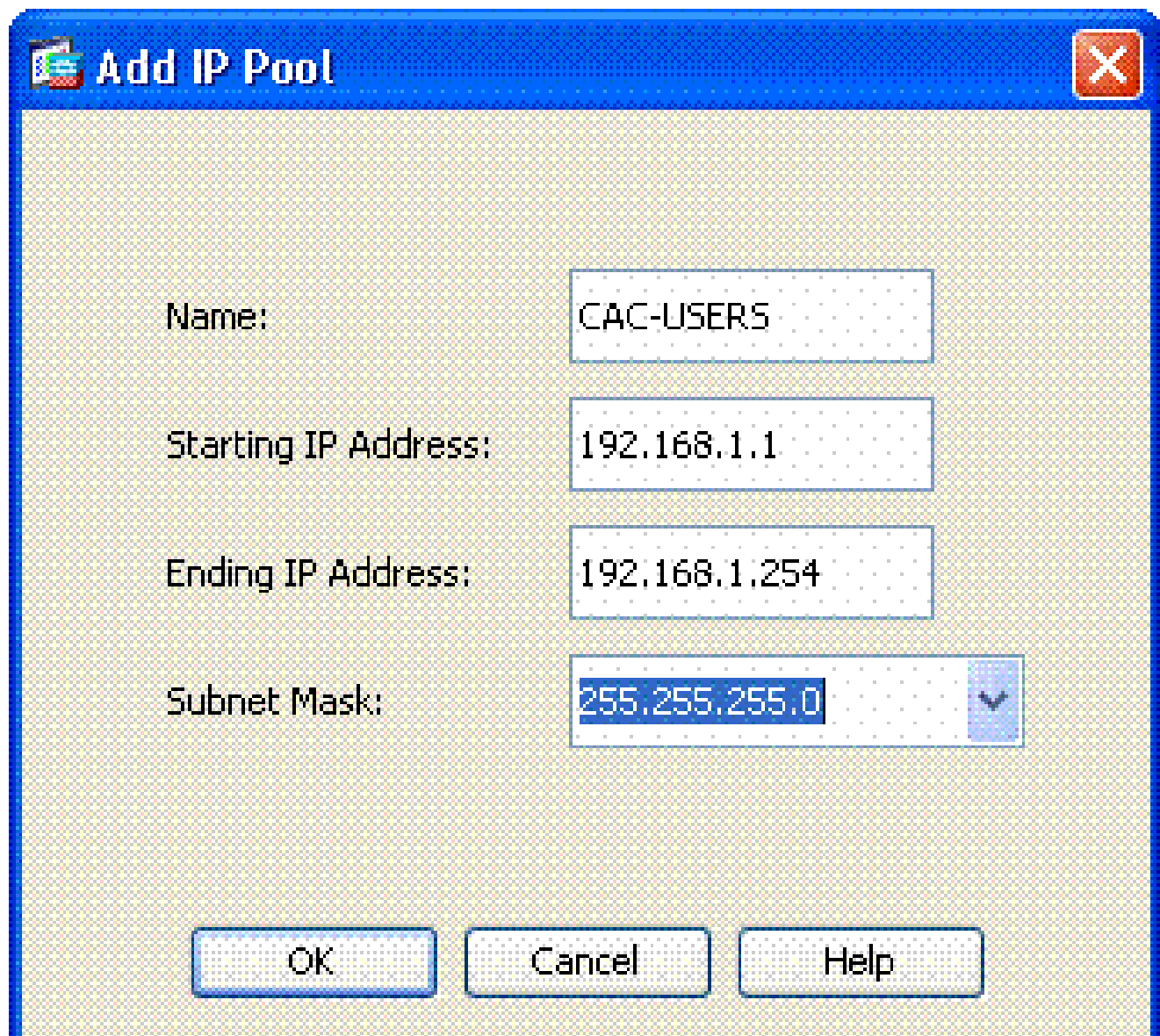
9. Open het bestand met WordPad, kopieer het verzoek naar de juiste documentatie en verstuur het naar uw PKI POC. Zie figuur 10.

Afbeelding 10: Aanvraag voor inschrijving



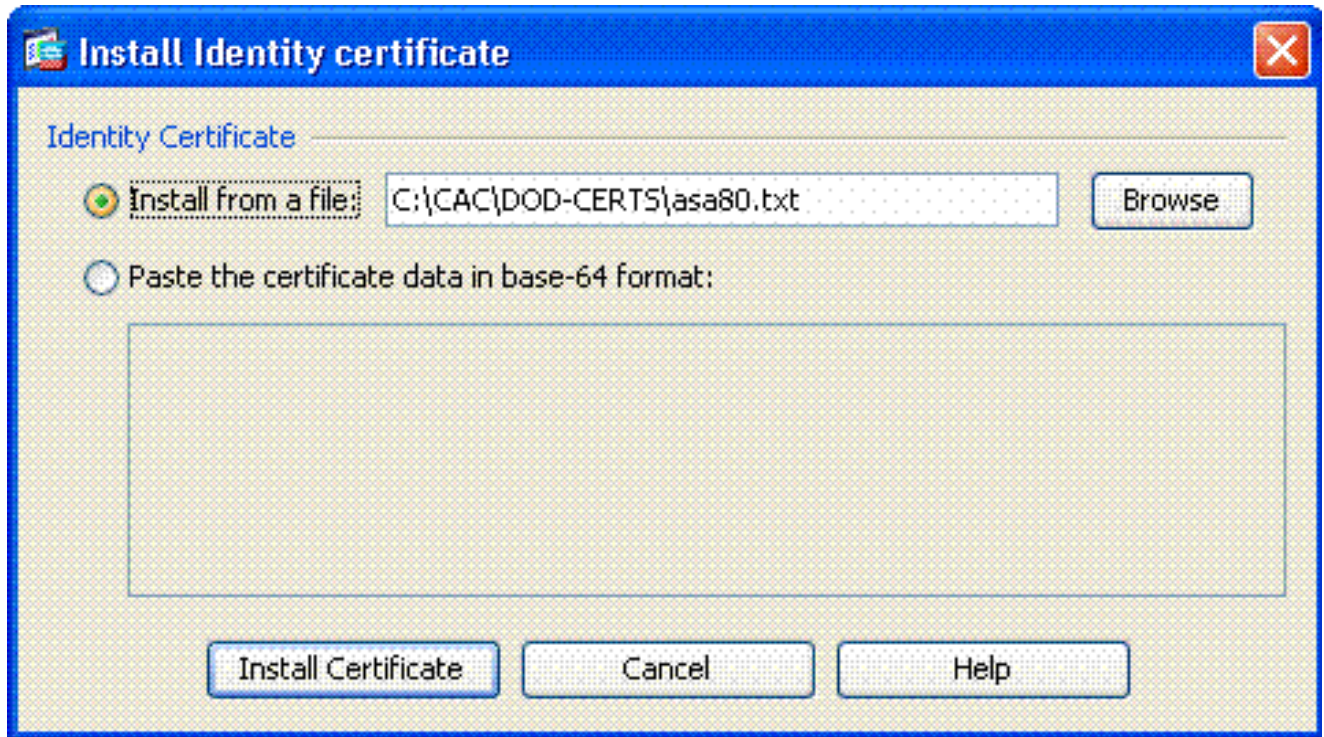
10. Zodra u het certificaat van de CA-beheerder hebt ontvangen, kiest u Remote Access VPN > Certificaatbeheer > ID-certificaat > Installeren. Zie figuur 11.

Afbeelding 11: Identificatiecertificaat invoeren



11. Blader in het venster Certificaat installeren naar het ID-cert en kies Certificaat installeren. Zie bijvoorbeeld afbeelding 12.

Afbeelding 12: Identiteitscertificaat installeren



---

Opmerking: aanbevolen wordt om het vertrouwingspunt voor het ID-certificaat uit te voeren om het afgegeven certificaat en de sleutelparen op te slaan. Hierdoor kan de ASA-beheerder het certificaat en de sleutelparen importeren in een nieuwe ASA in het geval van RMA- of hardwarestoringen. Raadpleeg [Trustpoints voor export en import](#) voor meer informatie.

---

Opmerking: klik op OPSLAAN om de configuratie op te slaan in het flitsgeheugen.

---

## AnyConnect VPN-configuratie

Er zijn twee opties om de VPN-parameters in ASDM te configureren. De eerste optie is om de SSL VPN wizard te gebruiken. Dit is een eenvoudig te gebruiken tool voor gebruikers die nieuw zijn in VPN-configuratie. De tweede optie is om het handmatig te doen en door elke optie te gaan. Deze configuratiehandleiding gebruikt de handmatige methode.

---

Opmerking: er zijn twee methoden om de AC-client naar de gebruiker te brengen:

---

1. U kunt de client downloaden van de Cisco-website en op hun computer installeren.
  2. De gebruiker kan de ASA benaderen via een webbrowsen en de client kan worden gedownload.
- 

Opmerking: <https://asa.test.com> bijvoorbeeld. Deze gids gebruikt de tweede methode. Nadat de AC-client permanent op het clientsysteem is geïnstalleerd, start u gewoon de AC-client vanuit de toepassing.

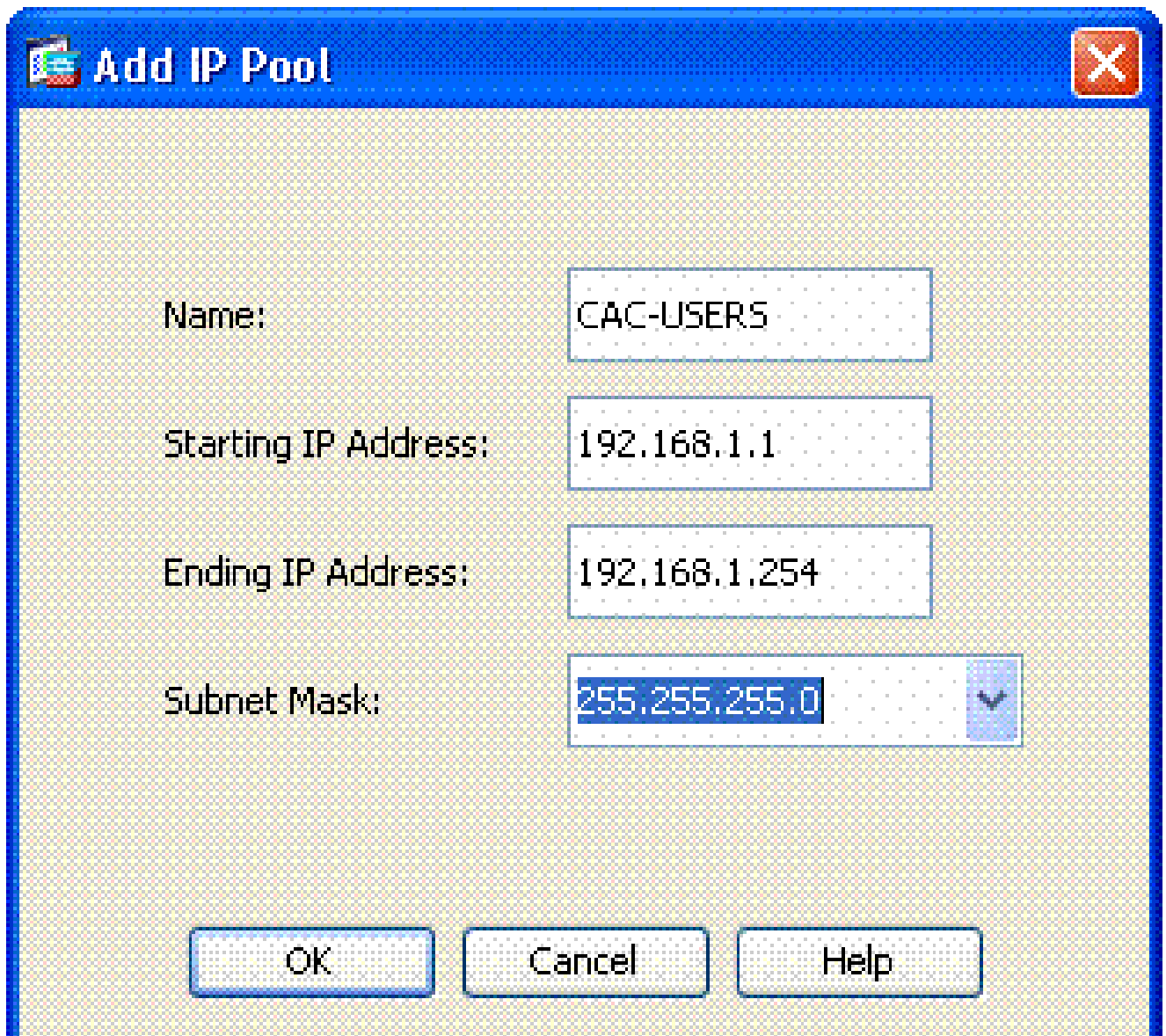
---

## Een IP-adresgroep maken

Dit is optioneel als u een andere methode zoals DHCP gebruikt.

1. Kies voor Remote Access VPN > Netwerктоegang (client) > Adrestoewijzing > Adrespools.
2. Klik op Add (Toevoegen).
3. Voer in het venster IP-pool toevoegen de naam in van de IP-pool, beginnend en eindigend IP-adres en kies een subnetmasker. Zie figuur 13.

Afbeelding 13: IP-pool toevoegen



The screenshot shows a dialog box titled "Add IP Pool". The dialog contains the following fields and values:

| Field                | Value         |
|----------------------|---------------|
| Name:                | CAC-USERS     |
| Starting IP Address: | 192.168.1.1   |
| Ending IP Address:   | 192.168.1.254 |
| Subnet Mask:         | 255.255.255.0 |

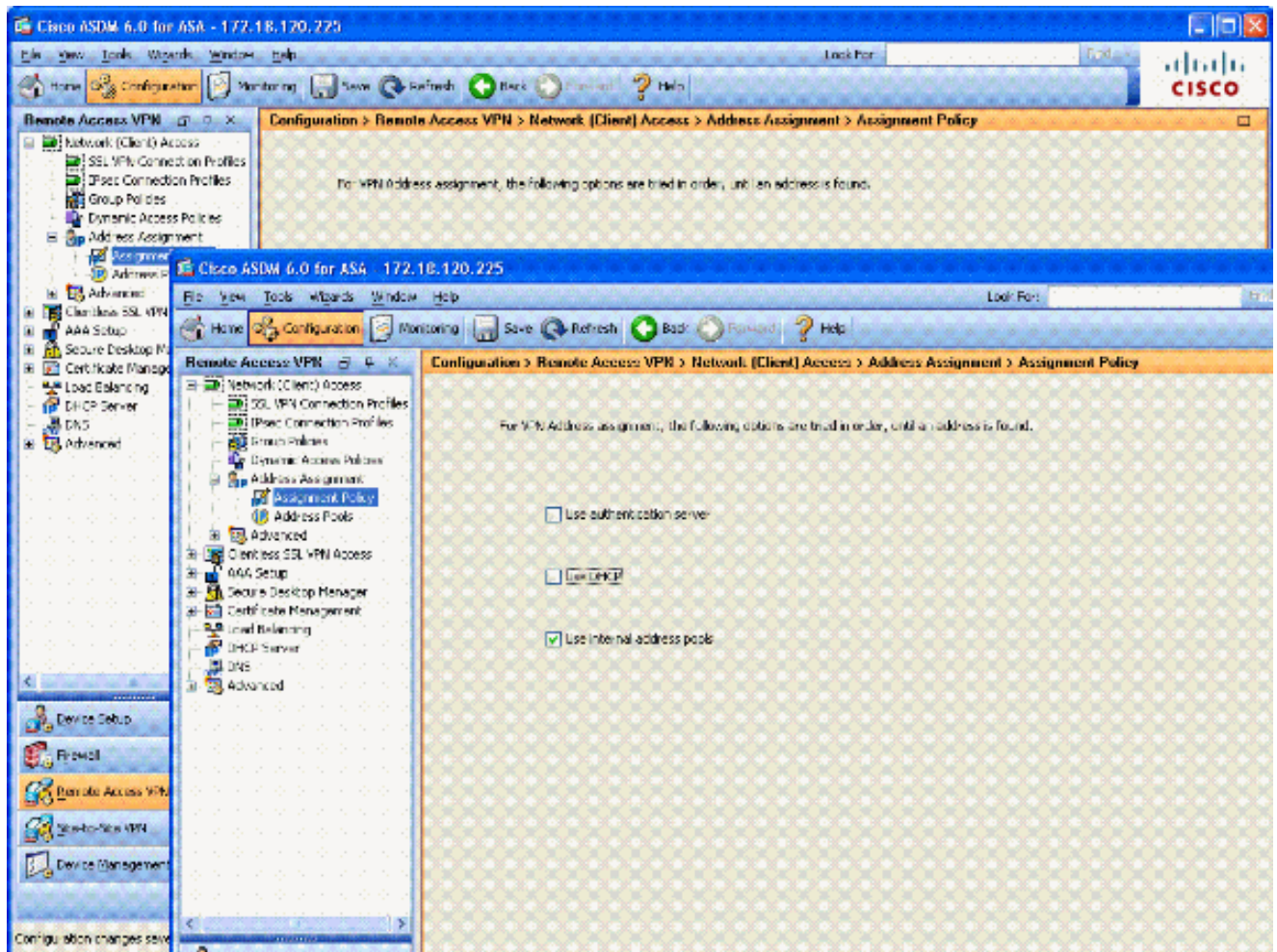
At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

4. Kies OK.
5. Kies voor Remote Access VPN > Netwerктоegang (client) > Adrestoewijzing > Toekenningbeleid.
6. Selecteer de juiste methode voor IP-adrestoewijzing. Deze gids gebruikt de interne



adrespools. Zie figuur 14.

Afbeelding 14: Methode voor de toewijzing van IP-adressen



7. Klik op Apply (Toepassen).

## Tunnelgroep en groepsbeleid maken

### Groepsbeleid

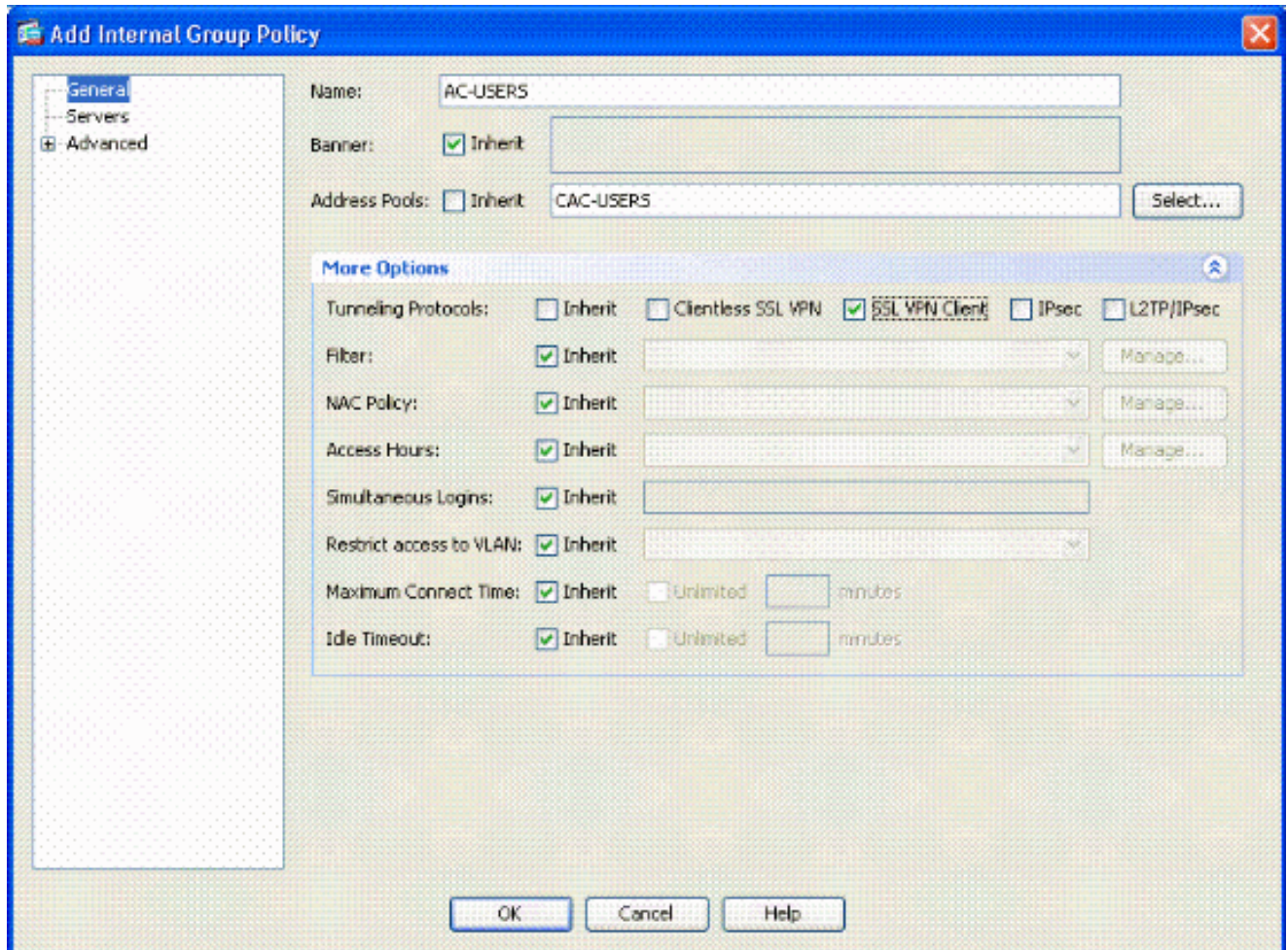
---

Opmerking: als u geen nieuw beleid wilt maken, kunt u het standaard ingebouwde groepsbeleid gebruiken.

---

1. Kies voor externe toegang via VPN -> Netwerktogang (client) -> Groepsbeleid.
2. Klik op Add en kies Internal Group Policy.
3. Voer in het venster Intern groepsbeleid toevoegen de naam voor het groepsbeleid in het tekstvak Naam in. Zie figuur 15.

Afbeelding 15: Een intern groepsbeleid toevoegen



- a. Kies op het tabblad Algemeen de SSL VPN-client in de optie Tunneling Protocollen, tenzij u andere protocollen gebruikt zoals Clientless SSL.
- b. In de sectie van Servers, uncheck het inherit controlevakje en ga het IP adres van DNS in en WINT servers in. Voer, indien van toepassing, het DHCP-bereik in.
- c. In het gedeelte Servers deselecteert u het aankruisvakje Overerven in het Standaarddomein en voert u de juiste domeinnaam in.
- d. Op het tabblad Algemeen deselecteert u het aanvinkvakje Overerven in het gedeelte Adresgroep en voegt u de adresgroep toe die met de vorige stap is gemaakt. Als u een andere methode voor IP-adrestoewijzing gebruikt, laat u dit over om te erven en de juiste wijziging aan te brengen.
- e. Alle andere configuratietabbladen blijven standaard ingesteld.

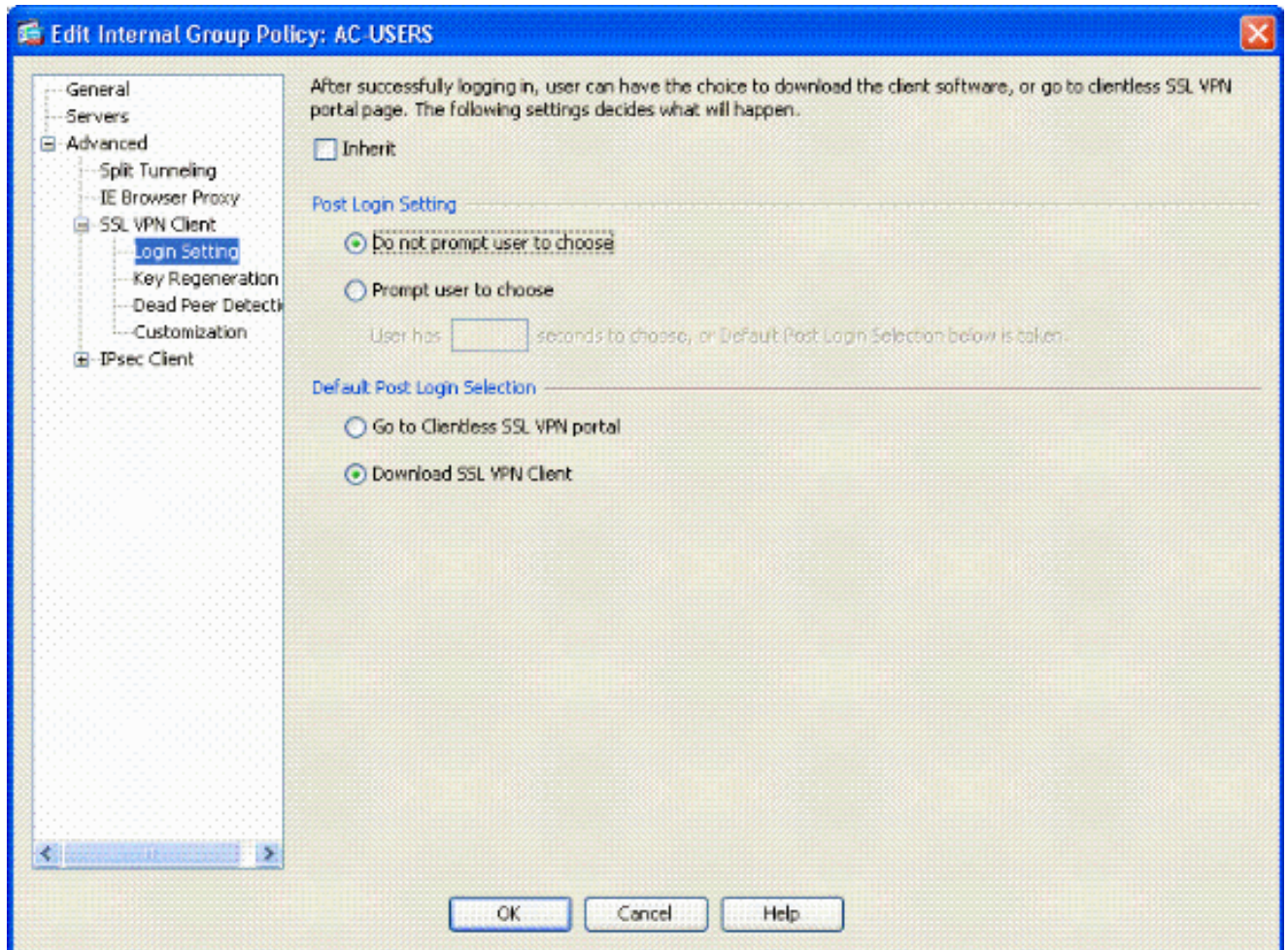
---

Opmerking: er zijn twee methoden om de AC-client naar de eindgebruikers te brengen. Eén methode is om naar Cisco.com te gaan en de AC-client te downloaden. De tweede methode is de ASA de client naar de gebruiker te laten downloaden wanneer de gebruiker probeert verbinding te maken. Dit voorbeeld laat de laatste methode zien.

---

4. Kies vervolgens Geavanceerd > SSL VPN-client > Aanmeldingsinstellingen. Zie figuur 16.

Afbeelding 16: Een intern groepsbeleid toevoegen



- Deselecteer het aanvinkvakje Inherit.
- Kies de juiste Post Login-instelling die bij uw omgeving past.
- Kies de juiste standaard post login selectie die past bij uw omgeving.
- Kies OK.

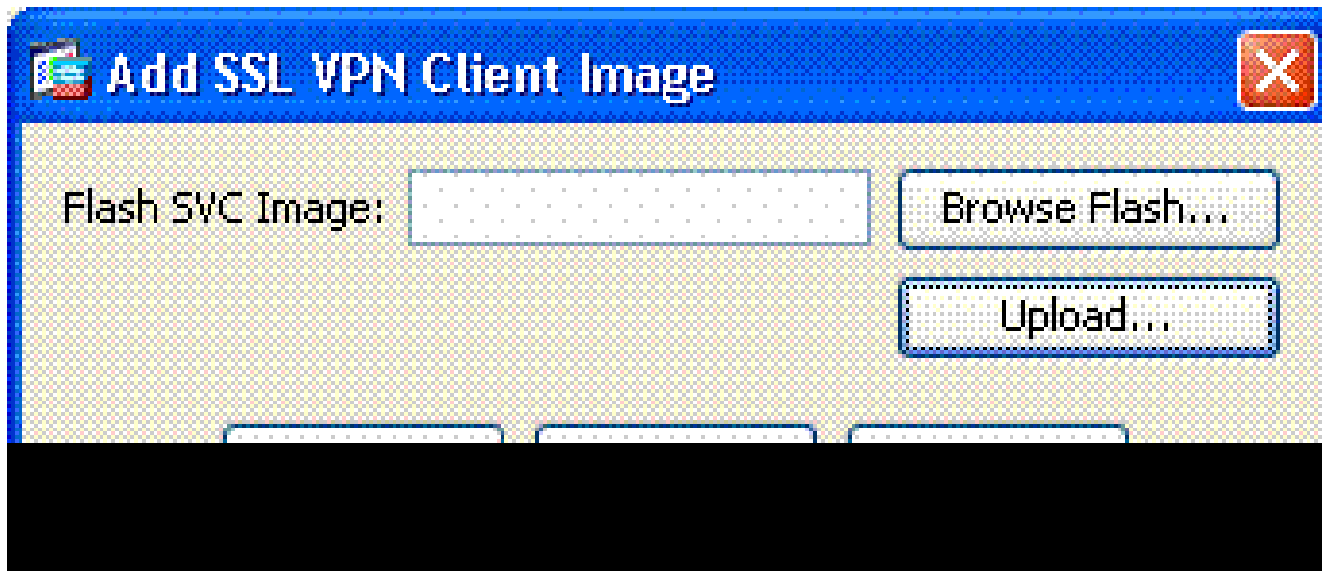
## Tunnelgroep-interface en afbeeldingsinstellingen

Opmerking: als u geen nieuwe groep wilt maken, kunt u de standaard ingebouwde groep gebruiken.

- Kies voor Remote Access VPN > Netwerктоegang (client) > SSL VPN-verbindingprofiel.
- Kies Cisco AnyConnect-client inschakelen.....
- Er verschijnt een dialoogvenster met de vraag wilt u een SVC-afbeelding toewijzen?
- Kies Ja.

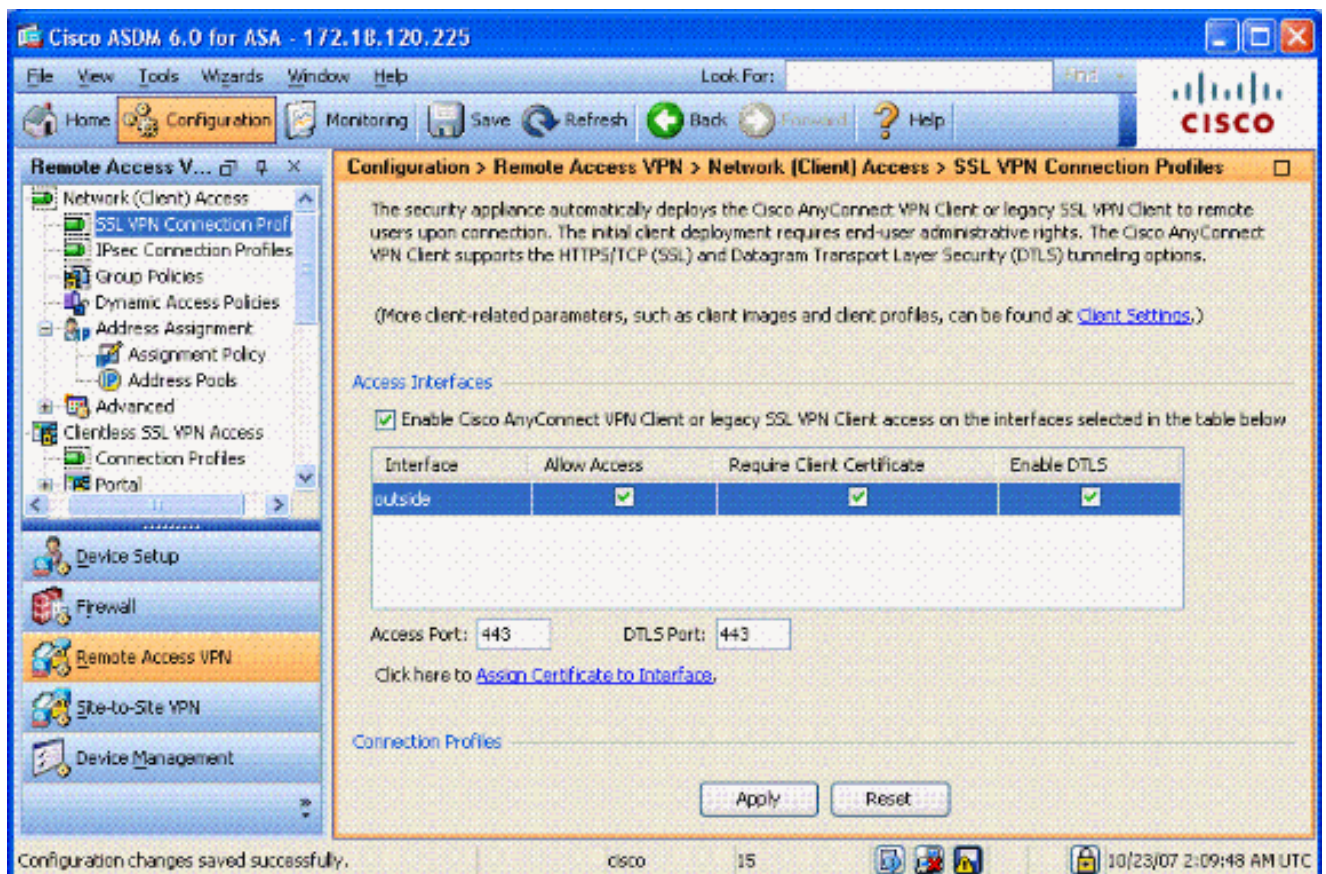
- Als er al een afbeelding is, kiest u de afbeelding die u wilt gebruiken met de functie Bladeren in Flash. Als de afbeelding niet beschikbaar is, kiest u Upload en bladert u naar het bestand op de lokale computer. Zie figuur 17. De bestanden kunnen worden gedownload van Cisco.com; er is een Windows-, MAC- en Linux-bestand.

Afbeelding 17: Voeg SSL VPN-clientafbeelding toe



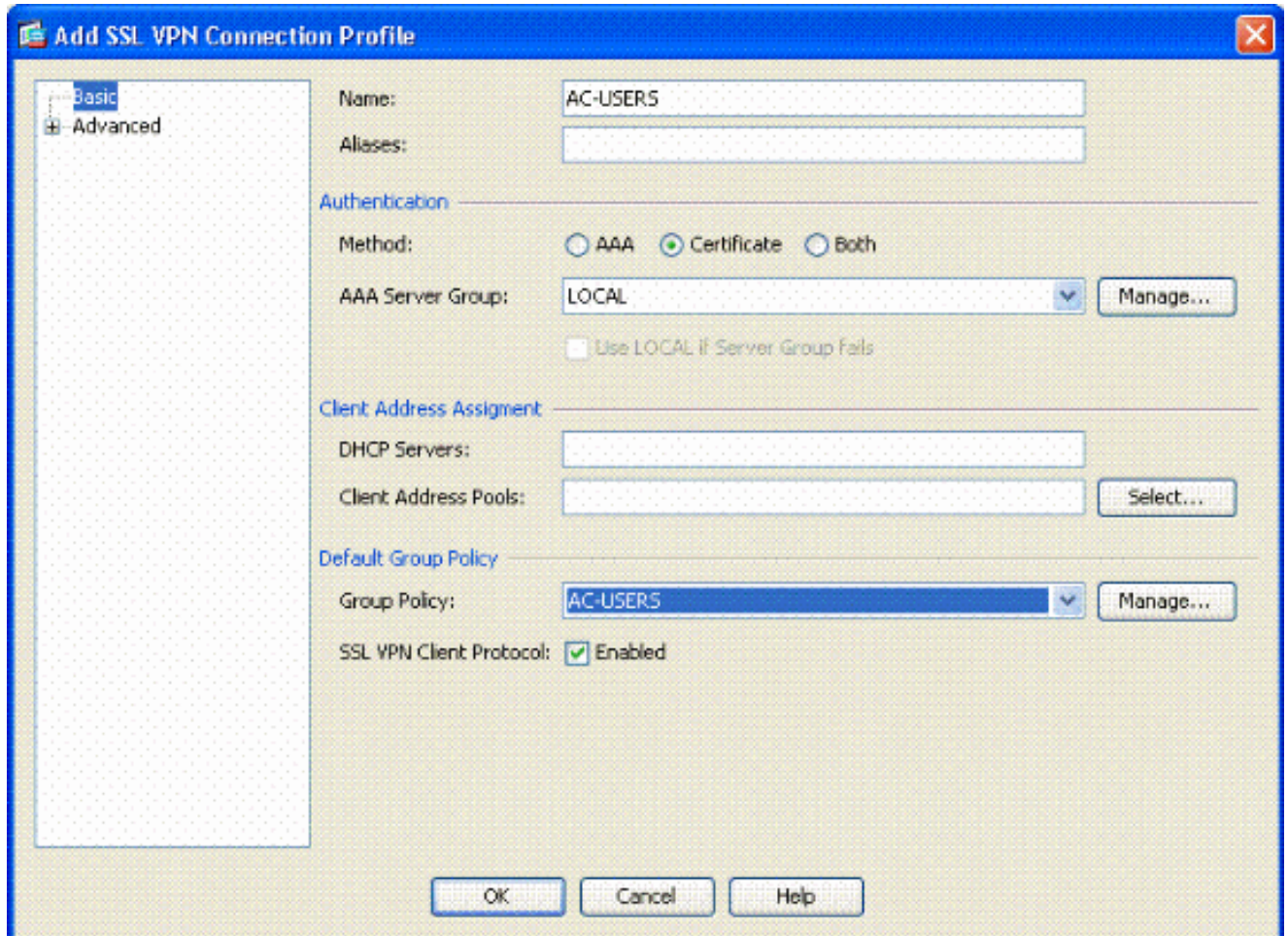
- Geef vervolgens toegang toe, vereis clientconversie en schakel optioneel DTLS in. Zie figuur 18.

Afbeelding 18: Toegang inschakelen



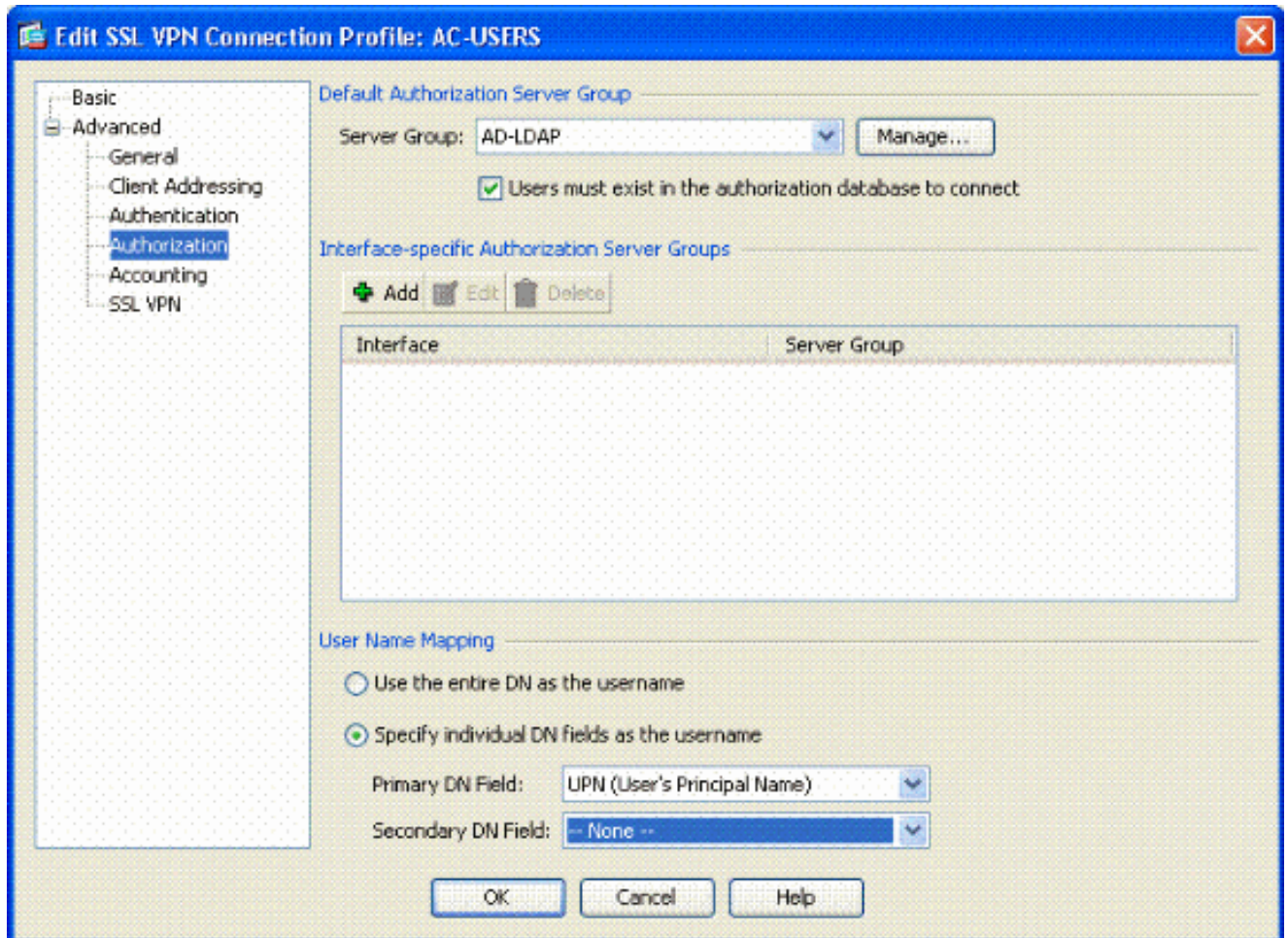
7. Klik op Apply (Toepassen).
8. Maak vervolgens een verbindingsprofiel/tunnelgroep. Kies voor Remote Access VPN > Netwerктоegang (client) > SSL VPN-verbindingsprofiel.
9. Klik in het gedeelte Verbindingsprofielen op Toevoegen.

Afbeelding 19: Verbindingsprofiel toevoegen



- a. Geef de groep een naam.
  - b. Kies Certificaat in de verificatiemethode.
  - c. Kies het groepsbeleid dat eerder is gemaakt.
  - d. Zorg ervoor dat SSL VPN Client is ingeschakeld.
  - e. Laat andere opties standaard staan.
10. Kies vervolgens Geavanceerd > Autorisatie. Zie figuur 20

Afbeelding 20: Vergunning

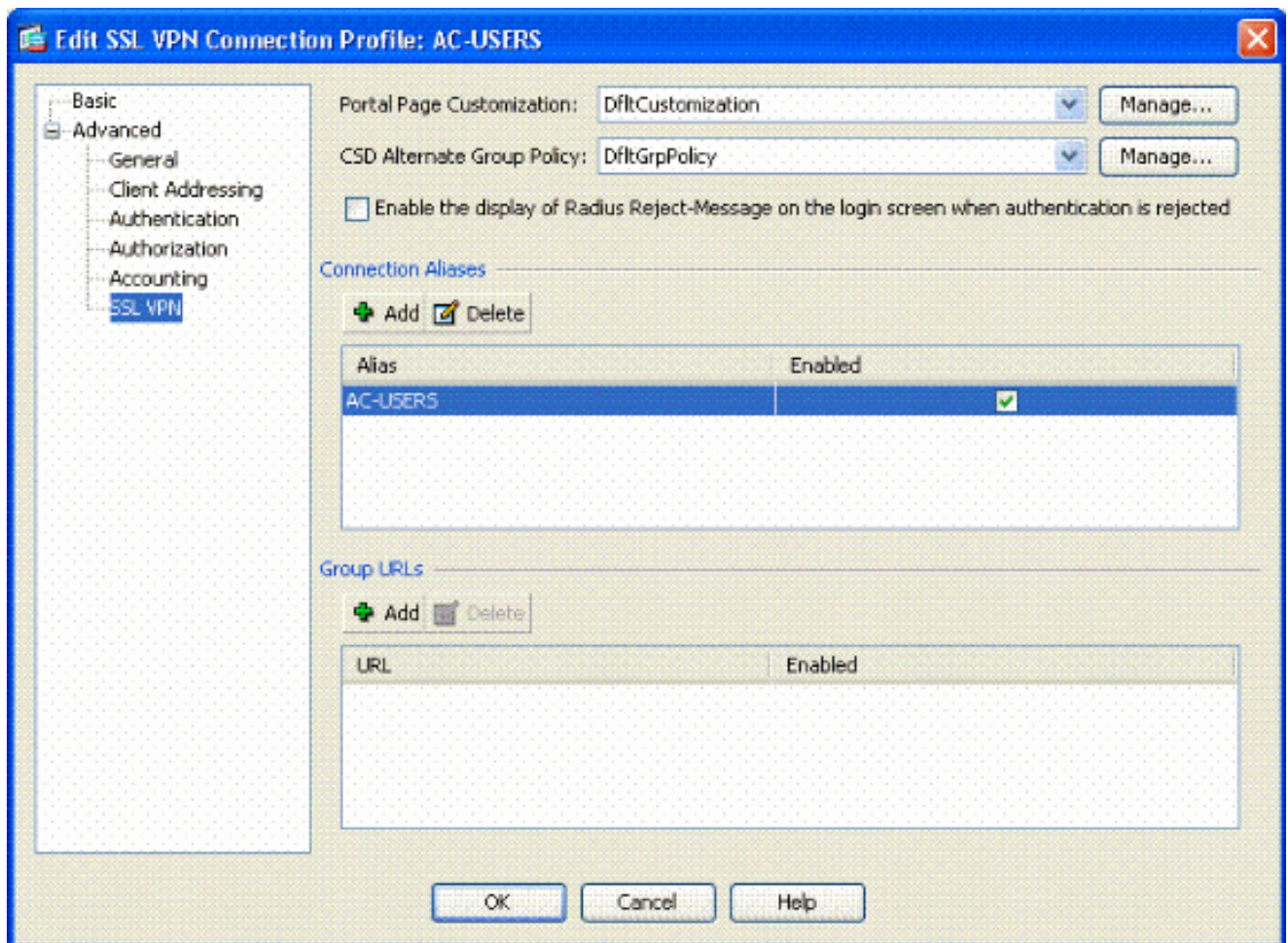


- a. Kies de AD-LDAP groep die eerder is gemaakt.
- b. Controleer of Gebruikers moeten bestaan... om verbinding te maken.
- c. Kies in de afbeeldingsvelden UPN voor de primaire en geen voor secundaire.

11. Kies de SSL VPN sectie van het menu.

12. Voltooi de volgende stappen in het gedeelte Verbindingsaliassen:

Afbeelding 21: Verbindingsaliassen



- a. Kies Toevoegen.
- b. Voer de groepsalias in die u wilt gebruiken.
- c. Zorg ervoor dat Ingeschakeld is ingeschakeld. Zie figuur 21.

13. Klik op OK.

---

Opmerking: Klik op Opslaan om de configuratie op te slaan in het flitsgeheugen.

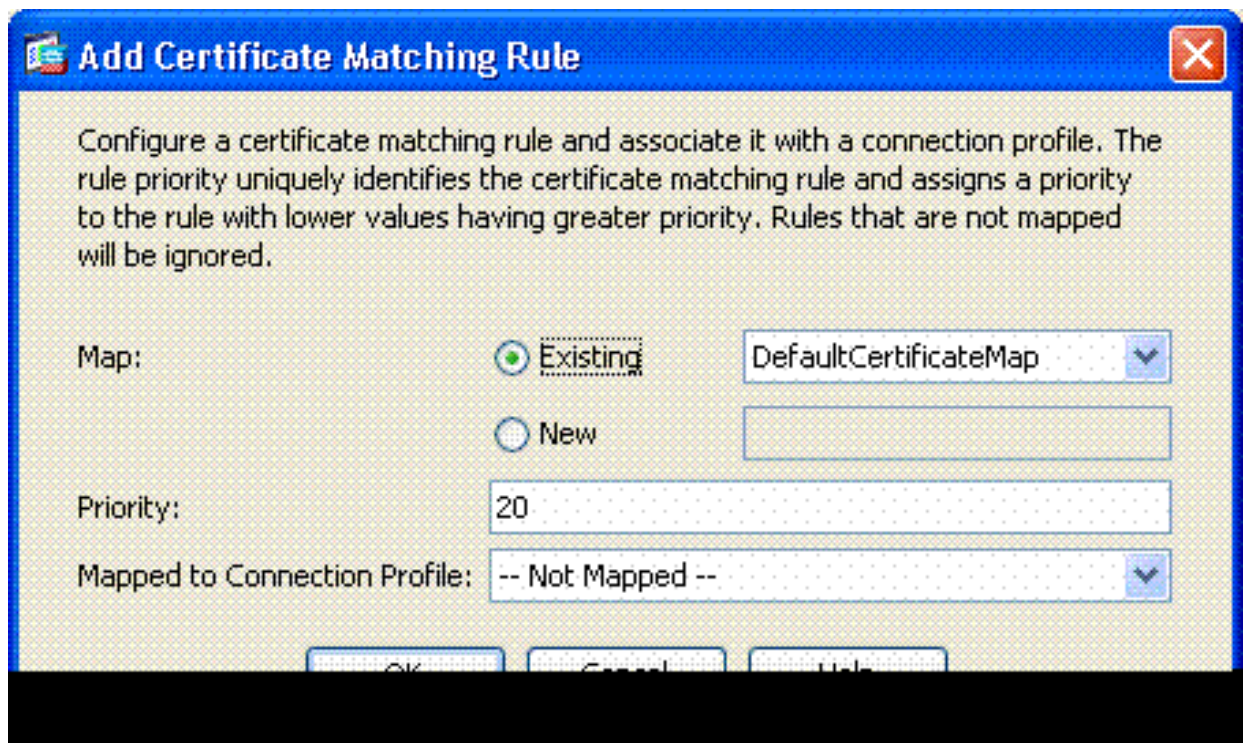
---

## Regels voor matching van certificaten (indien OCSP wordt gebruikt)

1. Kies Remote Access VPN > Geavanceerd > Certificaat aan SSL VPN-verbindingprofielkaarten. Zie figuur 22.
  - a. Kies de optie Toevoegen in het gedeelte Certificaat aan verbindingprofielkaarten.
  - b. U kunt de bestaande kaart als DefaultCertificateMap in het kaartgedeelte behouden of een nieuwe kaart maken als u al bepaalde kaarten voor IPsec gebruikt.
  - c. Houd de regelprioriteit.
  - d. Laat onder in kaart gebrachte groep staan als — Niet in kaart gebracht —. Zie figuur

22.

Afbeelding 22: Toevoeging van regel voor overeenkomende certificaten



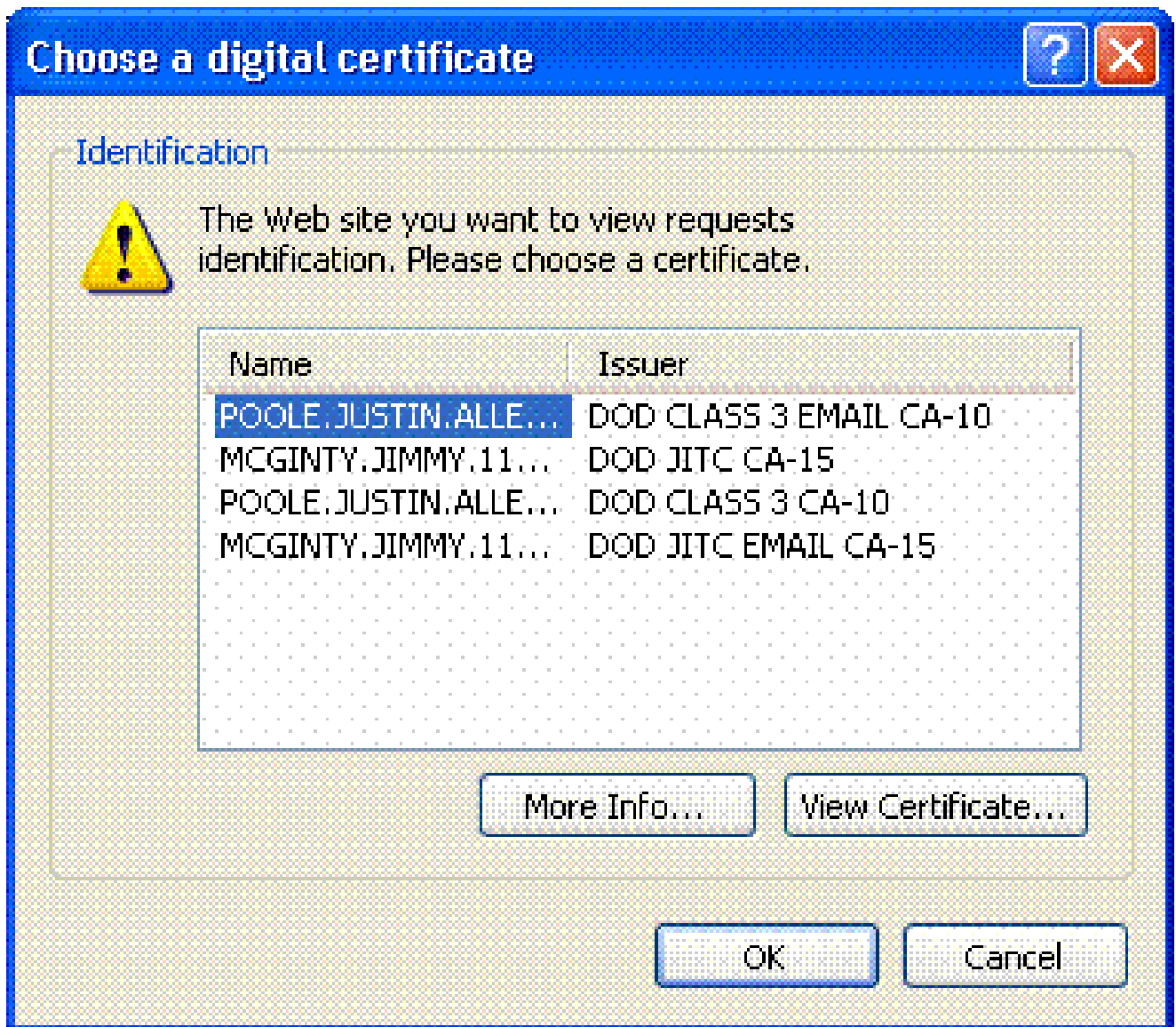
e. Klik op OK.

2. Klik op Add in de onderste tabel.

3. Voltooi de volgende stappen in het venster Criterium voor overeenkomende certificaten toevoegen:

Afbeelding 23: Criterium voor overeenstemmingsregels voor certificaten





- Houd de kolom Veld in de onderwerpregel.
- De kolom Component in het hele veld houden.
- Verander de kolom Operator in Is niet gelijk.
- Typ in de kolom Waarde twee dubbele aanhalingstekens "".
- Klik op OK en pas toe. Zie bijvoorbeeld afbeelding 23.

## OCSP configureren

De configuratie van een OCSP kan verschillen en is afhankelijk van de verkoper van de OCSP-responder. Lees de handleiding van de verkoper voor meer informatie.

### OCSP-antwoordcertificaat configureren

- Vraag een zelfgemaakt certificaat aan bij de OCSP-responder.

2. Voltooi de eerder vermelde procedures en installeer een certificaat voor de OSCP-server.

---

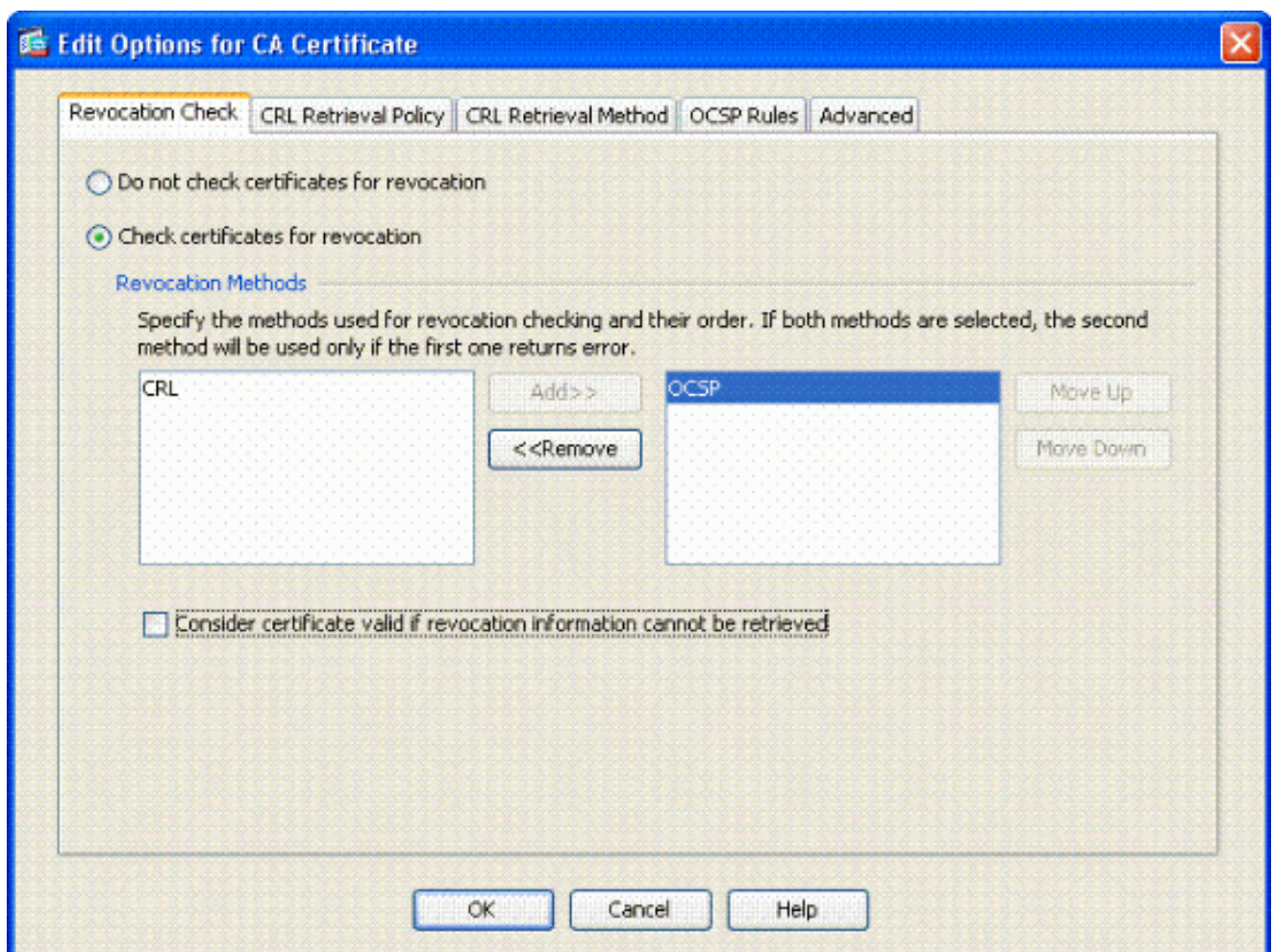
Opmerking: controleer de certificaten voor herroeping niet op het OCSP-certificaat trustpoint.

---

## CA configureren voor gebruik van OCSP

1. Kies Remote Access VPN> Certificaatbeheer > CA-certificaten.
2. Markeer een OCSP om een CA te kiezen voor configuratie voor gebruik van OCSP.
3. Klik op Edit (Bewerken).
4. Zorg ervoor dat het controlecertificaat voor herroeping is gecontroleerd.
5. Voeg OCSP toe in het gedeelte Herroepingsmethoden. Zie figuur 24.

### OCSP-herroepingscontrole



6. Zorg ervoor dat Certificaat geldig...niet kan worden opgehaald is niet aangevinkt als u strikte OCSP-controle wilt volgen.

---

Opmerking: alle CA-server die OCSP gebruikt voor herroeping configureren/bewerken.

---

## OCSP-regels configureren

---

Opmerking: controleer of er een beleid voor overeenkomende certificaatgroepen is gemaakt en of de OCSP-responder is geconfigureerd voordat u deze stappen uitvoert.

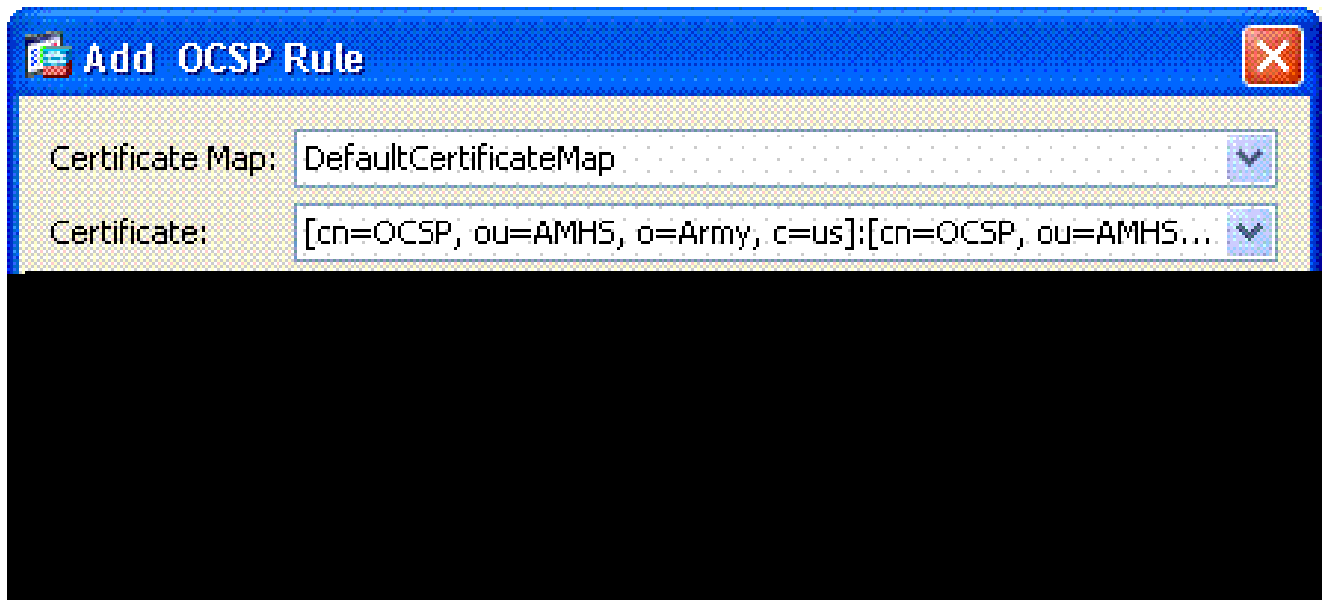
---

Opmerking: in sommige OCSP-implementaties kan voor de ASA een DNS A- en PTR-record nodig zijn. Deze controle wordt uitgevoerd om te verifiëren dat ASA van een .mil plaats is.

---

1. Kies Remote Access VPN > Certificaatbeheer > CA-certificaten 2.
2. Markeer een OCSP om een CA te kiezen voor configuratie voor gebruik van OCSP.
3. Kies Bewerken.
4. Klik op het tabblad OCSP-regel.
5. Klik op Add (Toevoegen).
6. Voltooi de volgende stappen in het venster OCSP-regel toevoegen. Zie figuur 25.

Afbeelding 25: OCSP-regels toevoegen



- a. Kies in de optie Certificaatplaattegrond DefaultCertificateMap of kies een kaart die eerder is gemaakt.
- b. Kies in de optie Certificaat de optie OCSP-responder.
- c. Typ bij de indexoptie 10.
- d. Voer in de URL-optie het IP-adres of de hostnaam van de OCSP-responder in. Als u

de hostnaam gebruikt, zorg er dan voor dat DNS-server op ASA is geconfigureerd.

e. Klik op OK.

f. Klik op Apply (Toepassen).

## Configuratie Cisco AnyConnect-client

Deze sectie behandelt de configuratie van de Cisco AnyConnect VPN-client.

Aannames - Cisco AnyConnect VPN-client en middleware-toepassing is al geïnstalleerd op de host-pc. ActivCard Gold en ActivClient zijn getest.

---

Opmerking: deze handleiding gebruikt de methode groep-url voor de eerste installatie van AC-clients. Nadat de AC-client is geïnstalleerd, start u de AC-toepassing net als de IPsec-client.

---

---

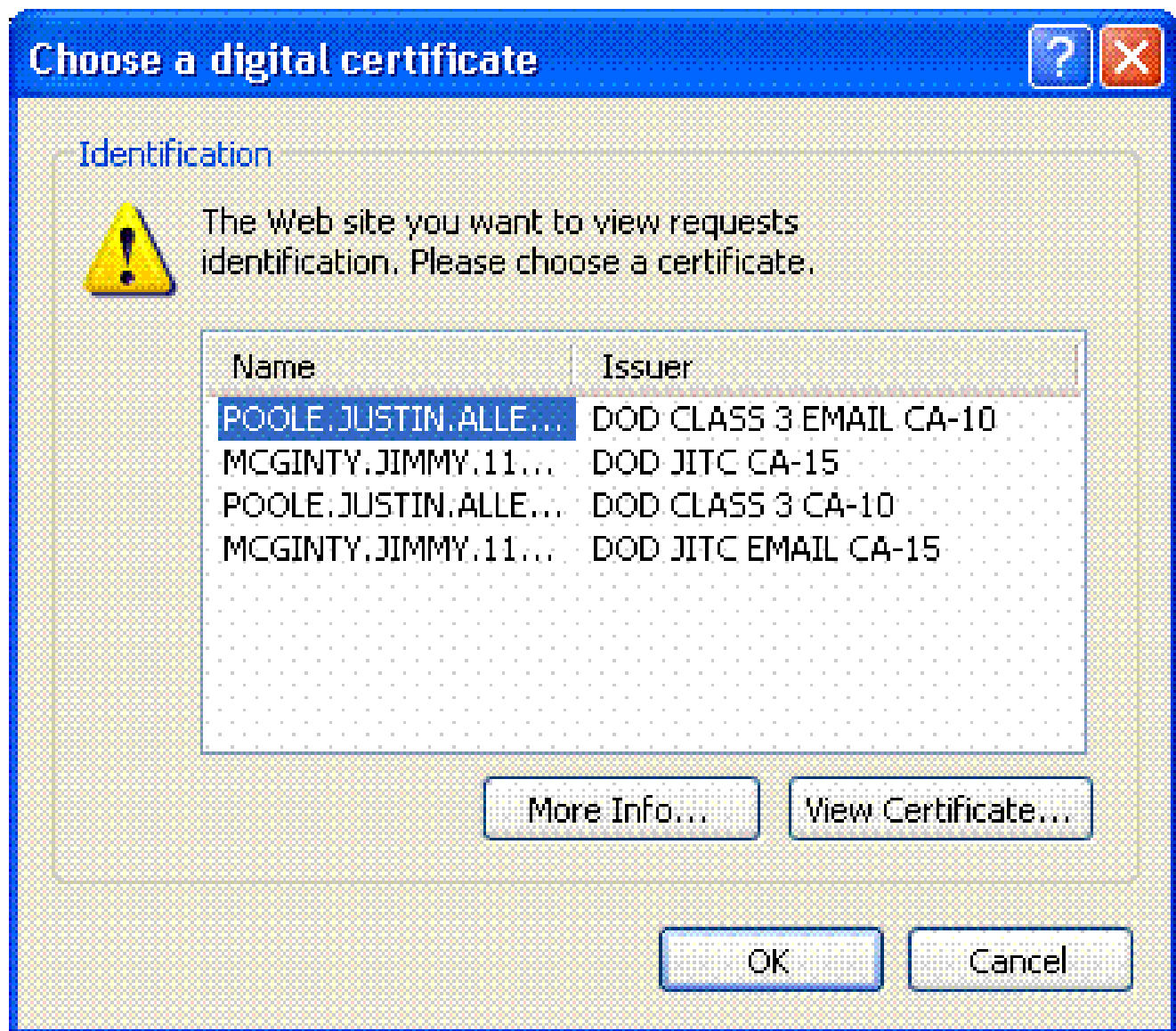
Opmerking: de DoD-certificaatketen moet op de lokale machine geïnstalleerd zijn. Controleer bij de PKI POC om de certificaten/het batchbestand te verkrijgen.

---

### Cisco AnyConnect VPN-client downloaden - Windows

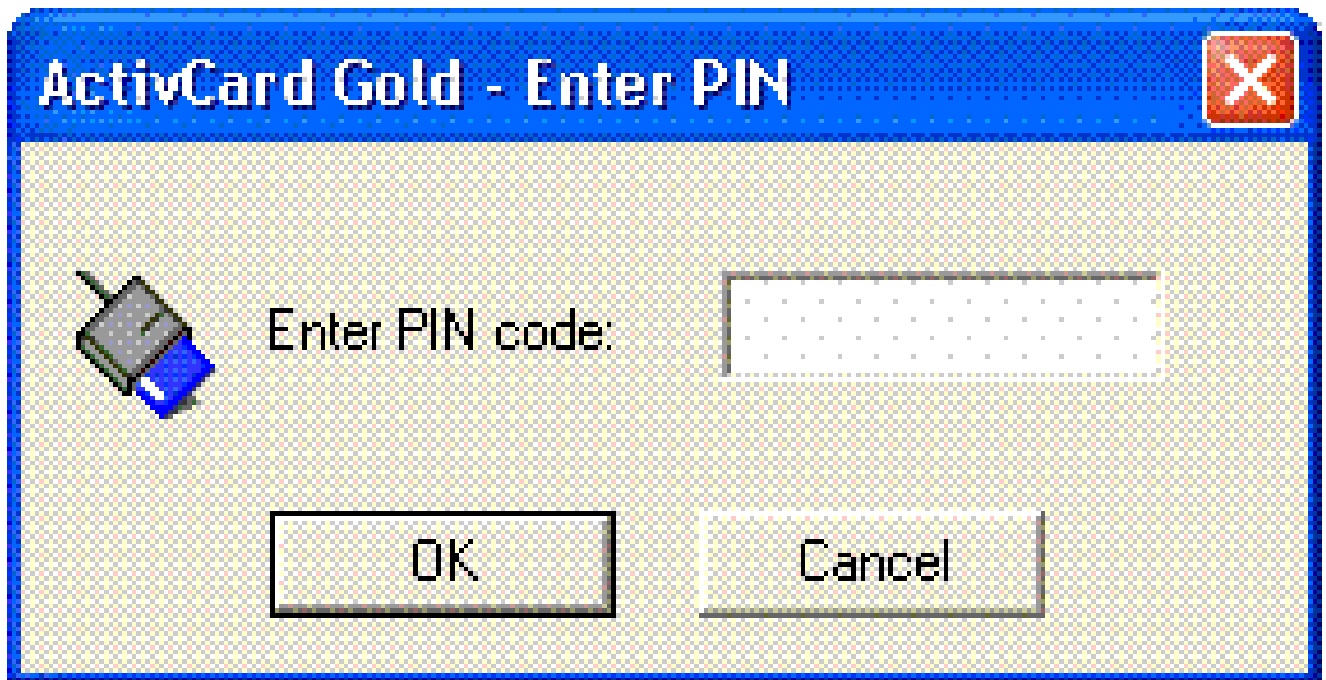
1. Start een websessie voor de ASA via Internet Explorer. Het adres moet de vorm hebben van <https://Outside-Interface>. Bijvoorbeeld <https://172.18.120.225>.
2. Kies het handtekeningcertificaat dat u wilt gebruiken voor toegang. Zie figuur 26.

Afbeelding 26: Kies het juiste certificaat



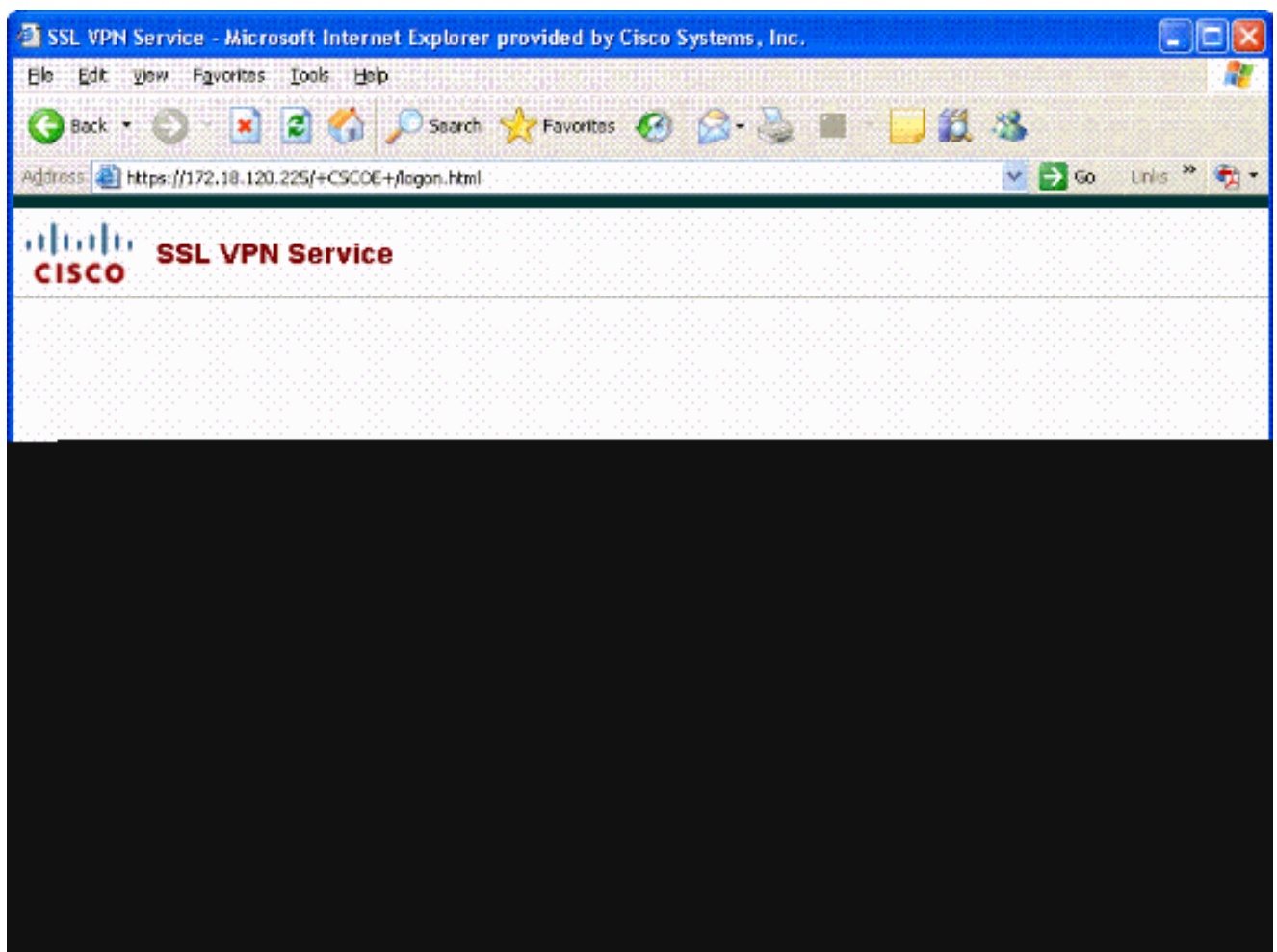
3. Voer uw pincode in als hierom wordt gevraagd.

Afbeelding 27: pincode invoeren



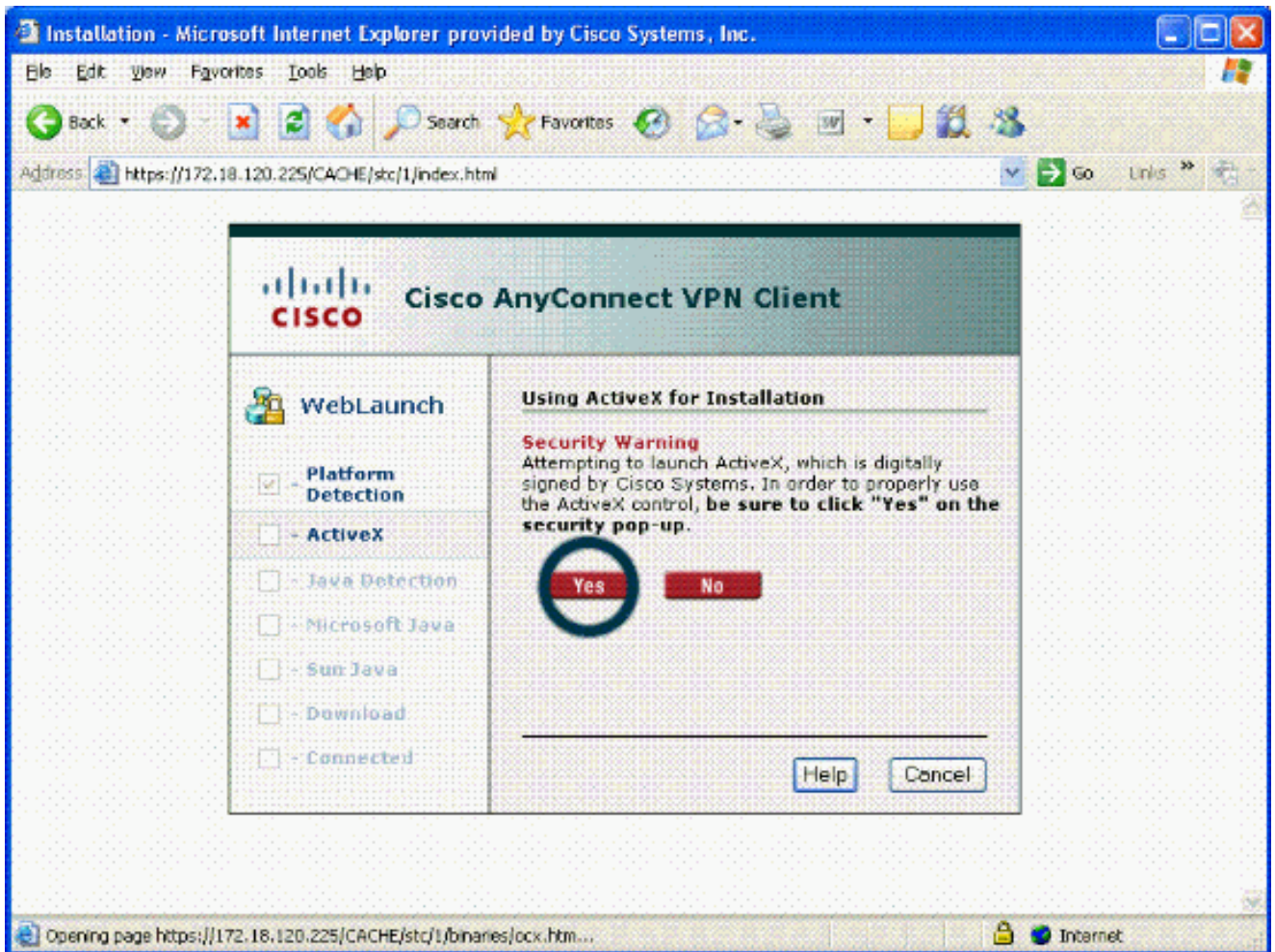
4. Klik op Ja om de veiligheidswaarschuwing te accepteren.
5. Eenmaal op de SSL Login Pagina, kies Login. Het clientcertificaat wordt gebruikt om in te loggen. Zie figuur 28.

Afbeelding 28: SSL-aanmelding



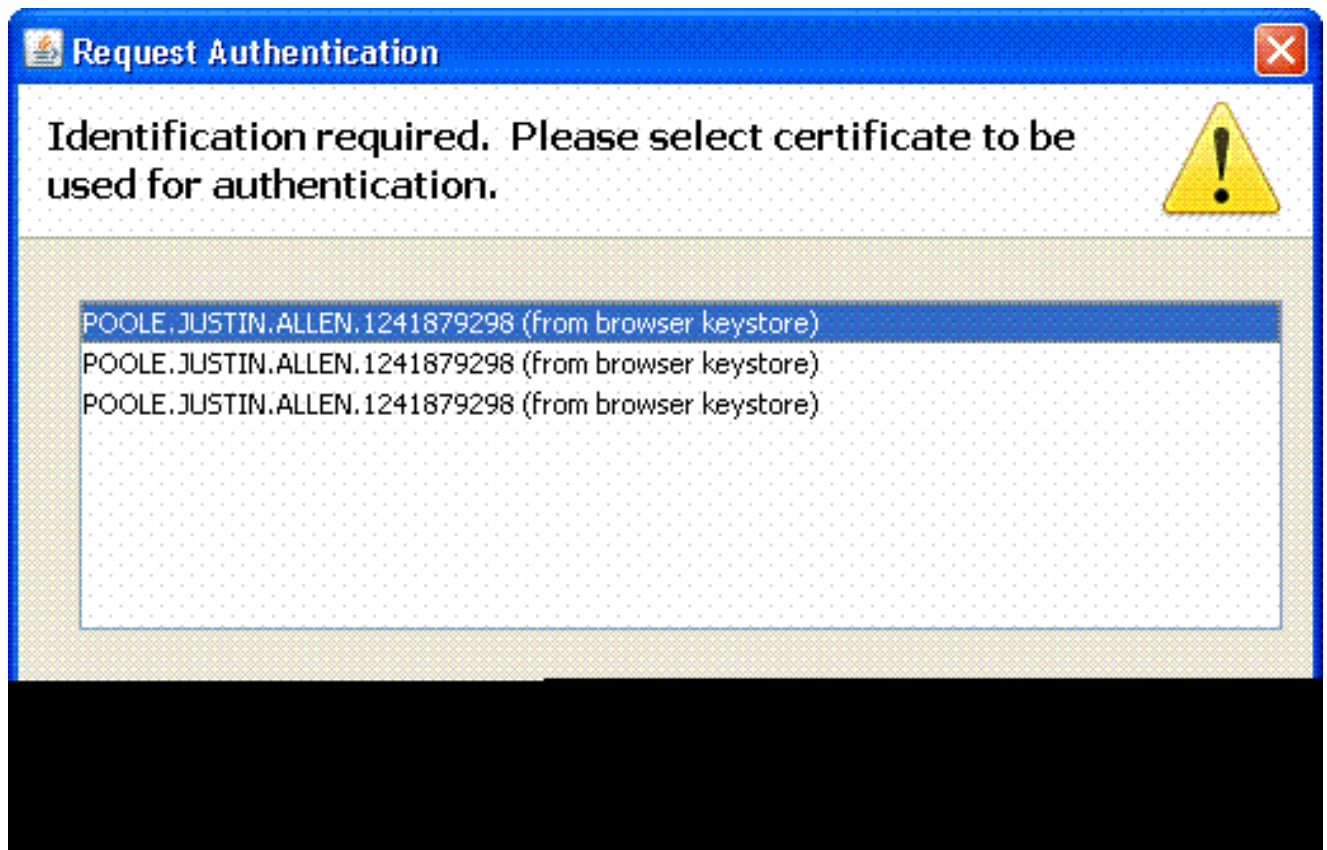
6. AnyConnect begint de client te downloaden. Zie figuur 29.

Afbeelding 29: Installatie van AnyConnect



7. Kies het juiste certificaat dat u wilt gebruiken. Zie figuur 30. AnyConnect blijft installeren. Met de ASA-beheerder kan de client permanent op elke ASA-verbinding installeren of installeren.

Afbeelding 30: Certificaat



## Cisco AnyConnect VPN-client starten - Windows

Kies Start > Alle programma's > Cisco > AnyConnect VPN-client op de host-pc.

---

Opmerking: zie Bijlage E voor de optionele configuratie van een clientprofiel voor AnyConnect.

---

## Nieuwe verbinding

1. Het venster AC verschijnt. Zie figuur 34.

Afbeelding 34: Nieuwe VPN-verbinding





2. Kies de juiste host als AC niet automatisch de verbinding probeert.
3. Voer uw pincode in als hierom wordt gevraagd. Zie figuur 35.

Afbeelding 35: PIN invoeren



## Externe toegang starten

Kies de groep en de host waarmee u verbinding wilt maken.

Aangezien er certificaten worden gebruikt, kiest u Verbinden om de VPN te openen. Zie figuur 36.

Afbeelding 36: Aansluiten



Connection



Statistics



About



Connect to:

172.18.120.225



Group:

AC-USERS



Username:

Password:

Connect

Please enter your username and password.

---

Opmerking: aangezien de verbinding certificaten gebruikt, hoeft u geen gebruikersnaam en wachtwoord in te voeren.

---

Opmerking: zie Bijlage E voor de optionele configuratie van een clientprofiel voor AnyConnect.

---

## Bijlage A - LDAP-toewijzing en DAP

In ASA/PIX release 7.1(x) en hoger werd een functie genaamd LDAP mapping geïntroduceerd. Dit is een krachtige eigenschap die een afbeelding tussen een attribuut van Cisco en voorwerpen LDAP/attribuut verstrekt, die de behoefte aan LDAP schemaverandering ontkent. Voor CAC-verificatie-implementatie kan dit extra beleidshandhaving op externe toegangsverbinding ondersteunen. Dit zijn voorbeelden van LDAP-mapping. Houd er rekening mee dat u beheerdersrechten nodig hebt om wijzigingen aan te brengen in de AD/LDAP-server. In ASA 8.x-software is de functie Dynamic Access Policy (DAP) geïntroduceerd. DAP kan in samenwerking met CAC werken om te kijken naar meerdere AD-groepen en naar beleid, ACL's, enzovoort.

### Scenario 1: Active Directory-handhaving met inbellen via externe toegangsrechten - Toegang toestaan/weigeren

In dit voorbeeld wordt het AD-kenmerk msNPALowDailin toegewezen aan het Cisco-kenmerk cVPN3000-Tunneling-Protocol.

- De waarde van het AD attribuut: TRUE = Allow; FALSE = Deny
- Cisco-kenmerkwaarde: 1 = FALSE, 4 (IPSec) of 20 (4 IPSEC + 16 WebVPN) = TRUE,

Voor TOESTAAN staat u in kaart:

- TRUE = 20

Voor de inbelvoorwaarde DENY, brengt u het volgende in kaart:

- VALS = 1

---

Opmerking: controleer of TRUE en FALSE in alle caps staan. Raadpleeg [Gebruikersautorisatie voor een externe server voor security applicatie configureren](#) voor meer informatie.

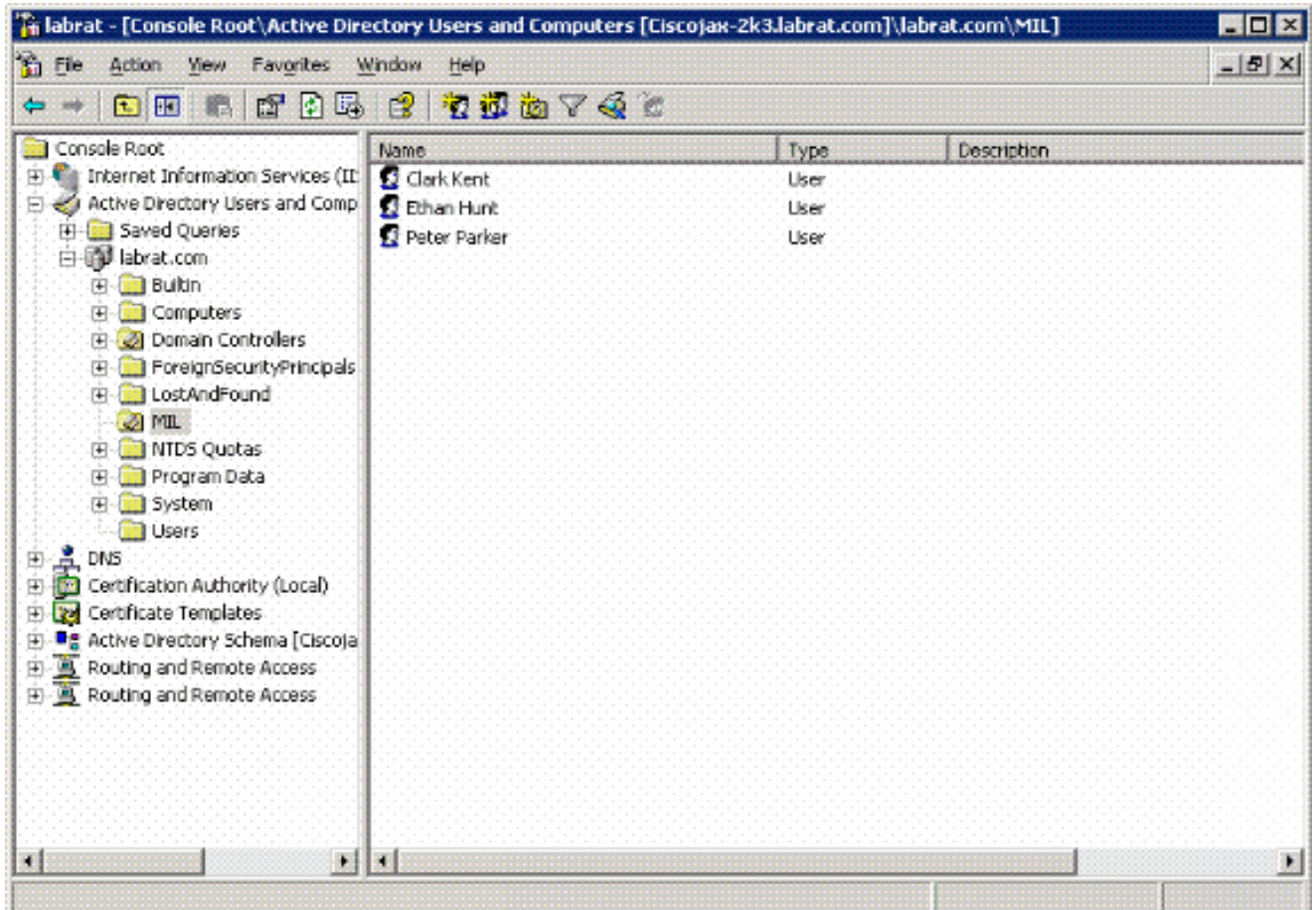
---

### Active Directory instellen

1. Klik in de Active Directory-server op Start > Uitvoeren.
2. Typ in het tekstvak Openen dsa.msc en klik vervolgens op OK. Hiermee start u de actieve directory-beheerconsole.

3. Klik in de Active Directory-beheerconsole op het plusteken om de Active Directory-gebruikers en -computers uit te breiden.
4. Klik op het plusteken om de domeinnaam uit te breiden.
5. Als u een OE hebt gemaakt voor uw gebruikers, vouw de OE uit om alle gebruikers te bekijken; als u alle gebruikers hebt toegewezen in de map Gebruikers, vouw die map uit om ze te bekijken. Zie figuur A1.

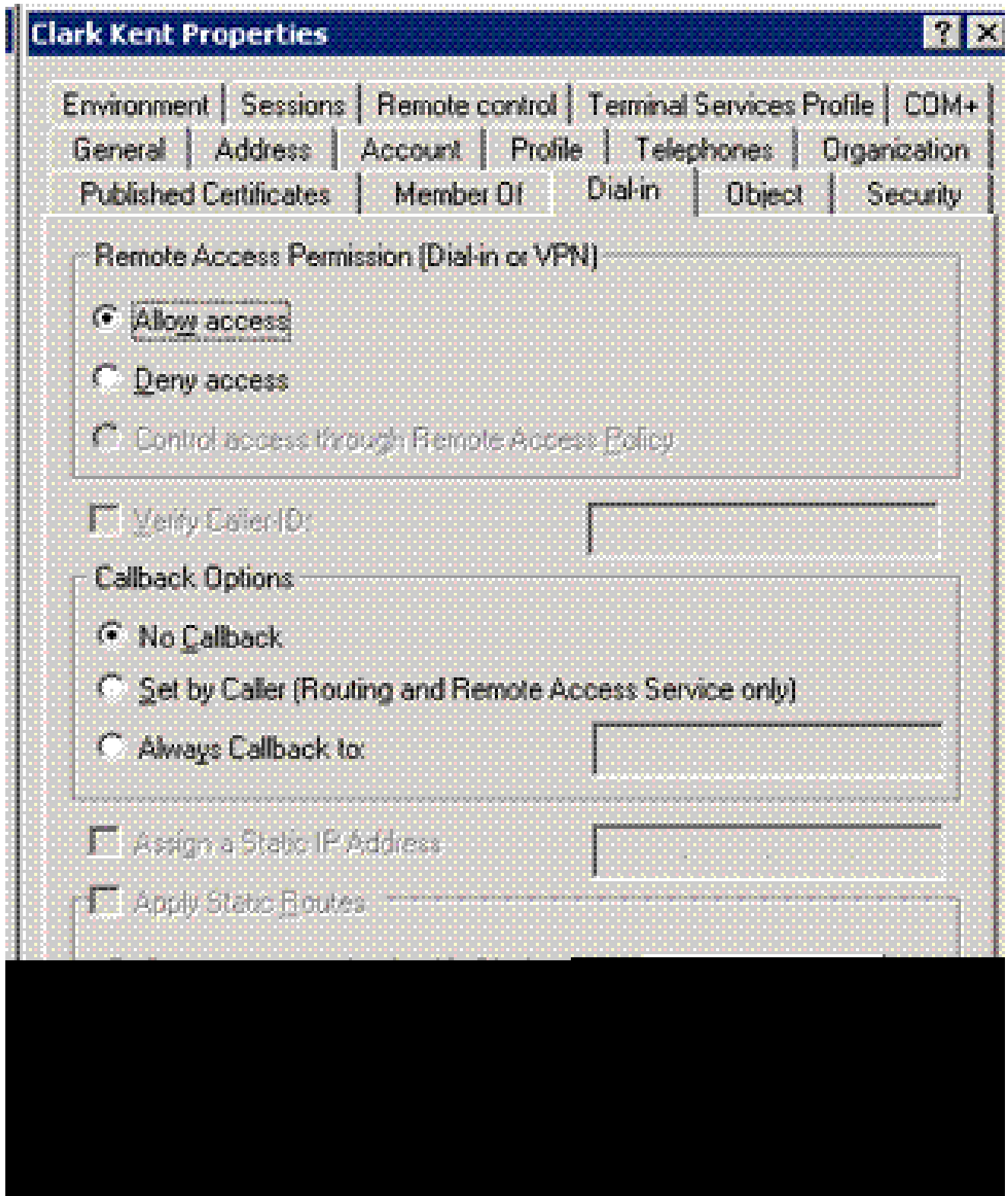
Afbeelding A1: Active Directory-beheerconsole



6. Dubbelklik op de gebruiker die u wilt bewerken.

Klik op het tabblad Inbellen op de pagina met gebruikerseigenschappen en klik op Toestaan of weigeren. Zie figuur A2.

Afbeelding A2: Gebruikerseigenschappen

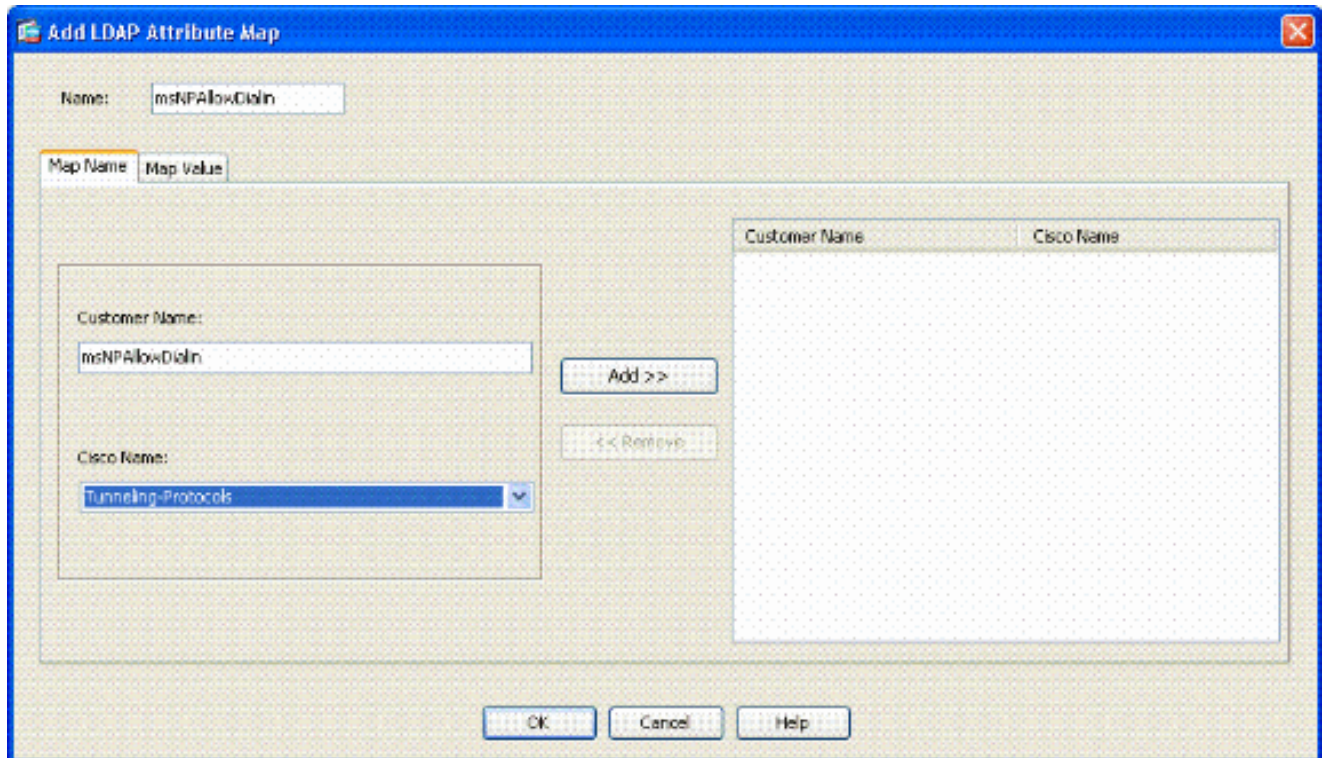


7. Klik vervolgens op OK.

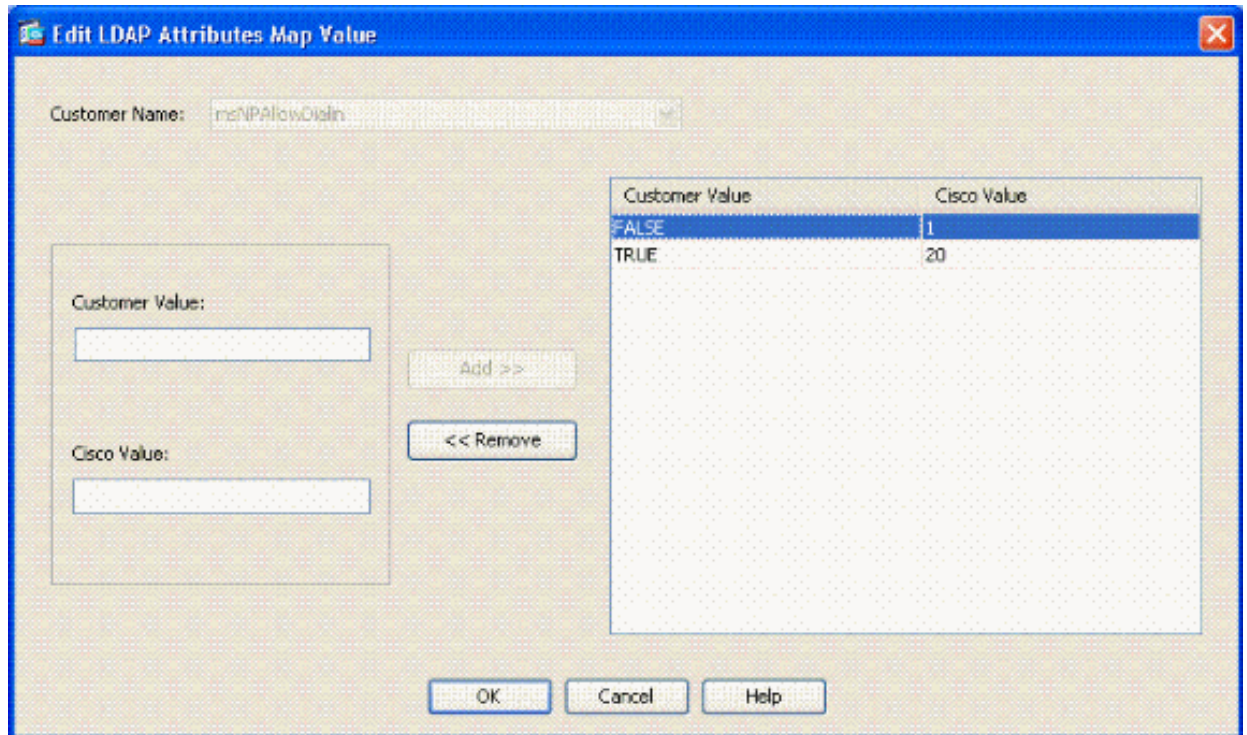
## ASA-configuratie

1. Kies in ASDM de optie Remote Access VPN> AAA Setup > LDAP Attribute Map.
2. Klik op Add (Toevoegen).
3. Voltooi de volgende stappen in het venster Add LDAP Attribute Map. Zie figuur A3.

Afbeelding A3: Toevoeging van LDAP-kenmerkkaart



- a. Voer in het tekstvak Naam een naam in.
- b. Typ in het tabblad Map Name msNPAllowDialIn in het tekstvak Customer Name.
- c. Kies in het tabblad Map naam de optie Tunneling-protocollen in de vervolgkeuzelijst in de naam van Cisco.
- d. Klik op Add (Toevoegen).
- e. Kies het tabblad Waarde kaart.
- f. Klik op Add (Toevoegen).
- g. Typ in het venster Waarde voor LDAP-kaart toevoegen TRUE in het tekstvak Naam van klant en typ 20 in het tekstvak Cisco-waarde.
- h. Klik op Add (Toevoegen).
- i. Typ FALSE in het tekstvak Naam van klant en type 1 in het tekstvak Cisco-waarde. Zie figuur A4.



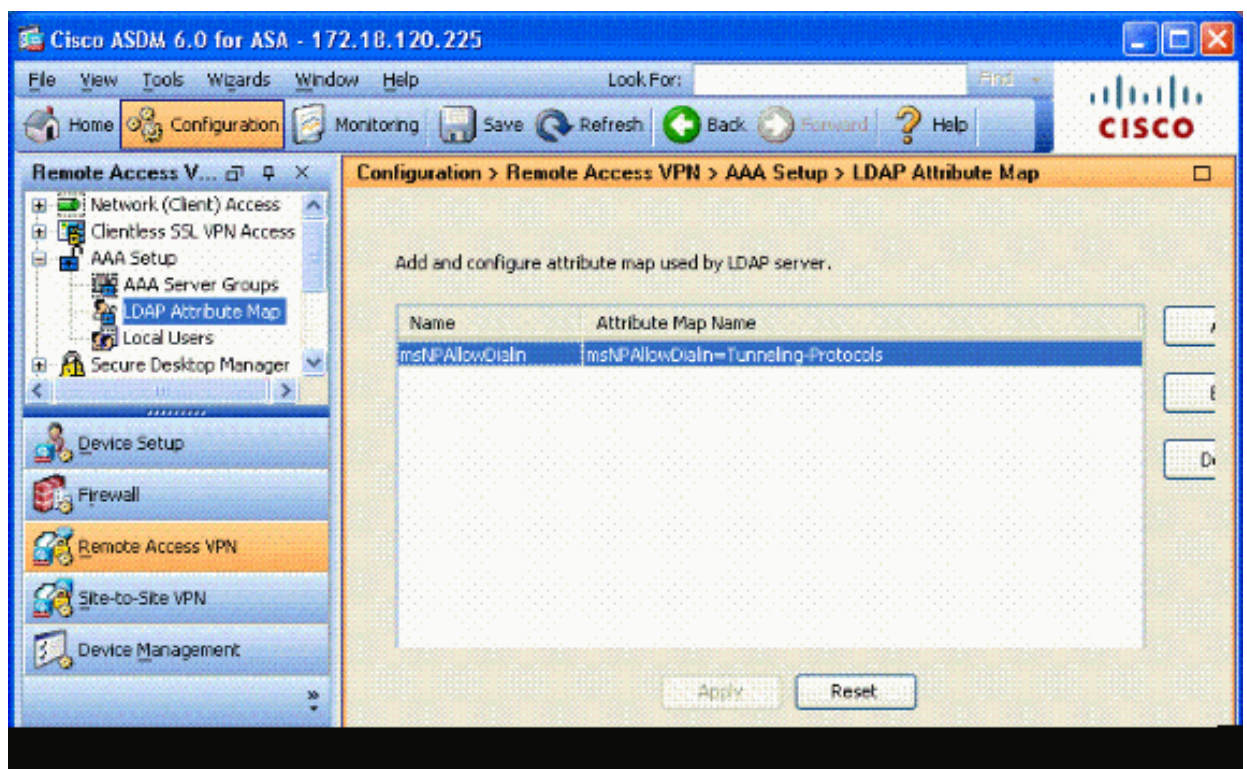
j. Klik op OK.

k. Klik op OK.

l. Klik op Apply (Toepassen).

m. De configuratie moet er uitzien als afbeelding A5.

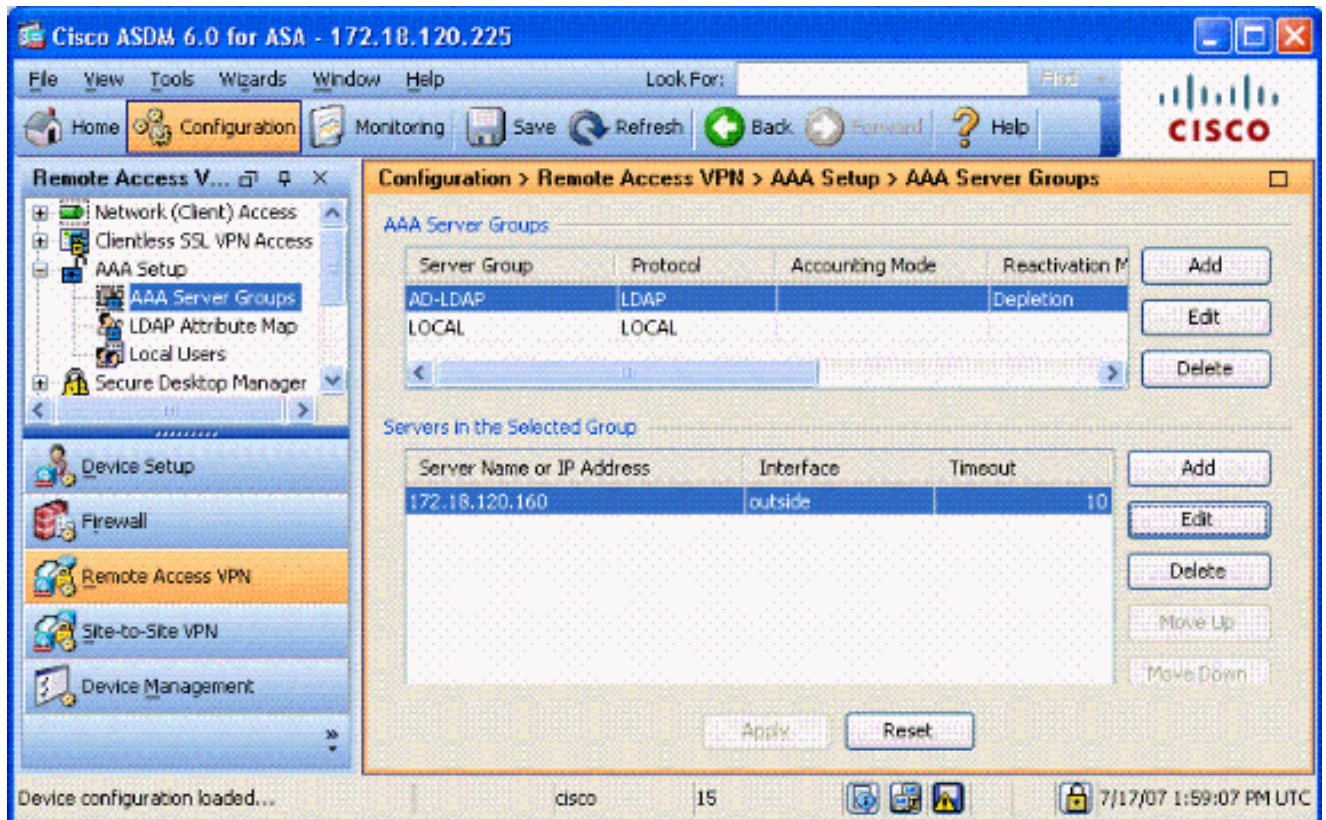
Afbeelding A5: Configuratie LDAP Attribute Map





4. Kies Remote Access VPN> AAA-instelling > AAA-servergroepen. Zie figuur A6.

Afbeelding A6: AAA-servergroepen



5. Klik op de servergroep die u wilt bewerken. Kies in het gedeelte Servers in de sectie Geselecteerde groep het IP-adres of de hostnaam van de server en klik vervolgens op Bewerken.

6. Kies in het venster AAA-server bewerken in het tekstvak LDAP Attribute Map de LDAP-kenmerkkaart die in het vervolgkeuzemenu is gemaakt. Zie figuur A7

Afbeelding A7: LDAP-kenmerkkaart toevoegen

**Edit AAA Server**

Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

**LDAP Parameters**

Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=gsgseclab,DC=org

Scope: One level beneath the Base DN

7. Klik op OK.

---

Opmerking: Zet LDAP-debugging aan terwijl u test om te controleren of LDAP-binding en attribuut mapping goed werken. Zie Bijlage C voor opdrachten voor probleemoplossing.

---

Scenario 2: Active Directory Enforcement met groepslidmaatschap om toegang toe te staan/te weigeren

Dit voorbeeld gebruikt het LDAP attribuut memberOf om aan het Tunneling Protocol attribuut in kaart te brengen om een groepslidmaatschap als voorwaarde te vestigen. Om dit beleid te laten werken, moet je aan de volgende voorwaarden voldoen:

- Gebruik een groep die al bestaat of maak een nieuwe groep voor ASA VPN-gebruikers om lid te zijn van voor ENABLE-voorwaarden.
- Gebruik een groep die al bestaat of maak een nieuwe groep voor niet ASA gebruikers om lid te zijn van voor DENY voorwaarden.
- Controleer in de LDAP viewer of u de juiste DN voor de groep hebt. Zie aanhangsel D. Als de DN niet goed werkt, werkt de mapping niet goed.

---

Opmerking: houd er rekening mee dat de ASA alleen de eerste tekenreeks van het kenmerk memberOf in deze release kan lezen. Zorg dat de nieuwe groep boven in de lijst staat. De andere optie is om een speciaal teken voor de naam te zetten, aangezien AD eerst naar speciale tekens kijkt. Om dit voorbehoud te omzeilen, gebruik DAP in 8.x software om te kijken naar meerdere groepen.

---

Opmerking: Zorg ervoor dat een gebruiker deel uitmaakt van de deny-groep of ten minste één andere groep, zodat het lidOf altijd naar de ASA wordt teruggestuurd. U hoeft niet de FALSE deny voorwaarde te specificeren, maar de beste praktijk is om dit te doen. Als de bestaande groepsnaam of de groepsnaam een spatie bevat, voert u het kenmerk als volgt in:

```
CN=Backup Operators, CN=Builtin, DC=gsgseclab, DC=org
```

---

Opmerking: met DAP kan de ASA kijken naar meerdere groepen in het kenmerk memberOf en naar de basisautorisatie van de groepen. Zie het DAP-gedeelte.

---

## TOEWIJZING

- De waarde van het AD-kenmerk:
  - memberOf CN=ASAUUsers,CN=Gebruikers,DC=gsgseclab,DC=org
  - memberOf CN=TelnetClients,CN=Gebruikers,DC=labrat,DC=com
- Cisco attribuut value: 1 = FALSE, 20 = TRUE,

Voor toestand TOESTAAN brengt u het volgende in kaart:

- memberOf CN=ASAUUsers,CN=Gebruikers,DC=gsgseclab,DC=org= 20

Voor de voorwaarde DENY, brengt u in kaart:

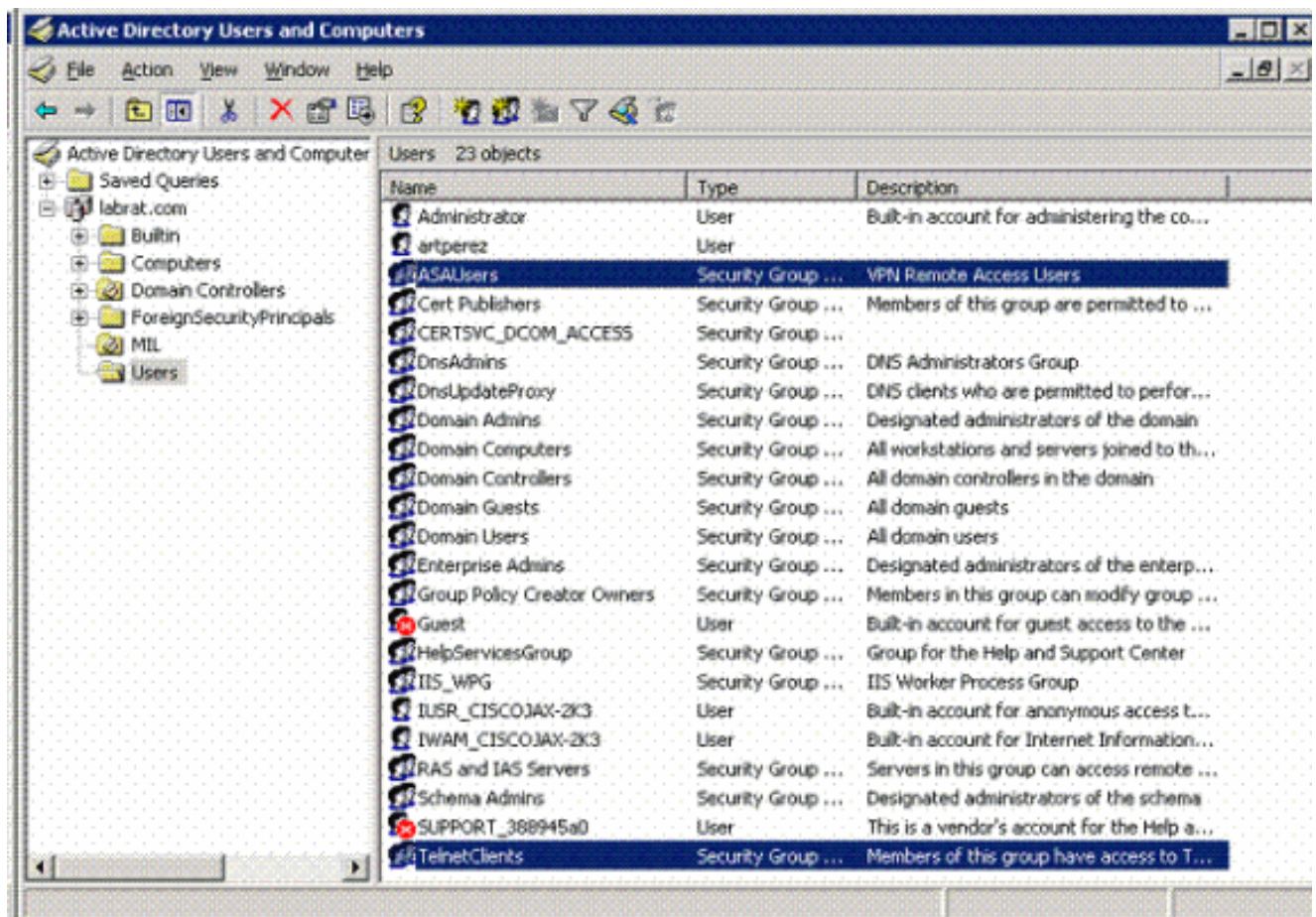
- memberOf CN=TelnetClients,CN=Gebruikers,DC=gsgseclab,DC=org = 1

Opmerking: in de toekomst release is er een Cisco-kenmerk om verbinding toe te staan en te weigeren. Raadpleeg [Gebruikersautorisatie voor een externe server voor security applicatie configureren](#) voor meer informatie over Cisco-kenmerken.

## Active Directory instellen

1. Kies Start > Uitvoeren in de Active Directory-server.
2. Typ in het tekstvak Openen dsa.msc en klik vervolgens op OK. Hiermee start u de actieve directory-beheerconsole.
3. Klik in de Active Directory-beheerconsole op het plusteken om de Active Directory-gebruikers en -computers uit te breiden. Zie figuur A8

Afbeelding A8: Active Directory-groepen



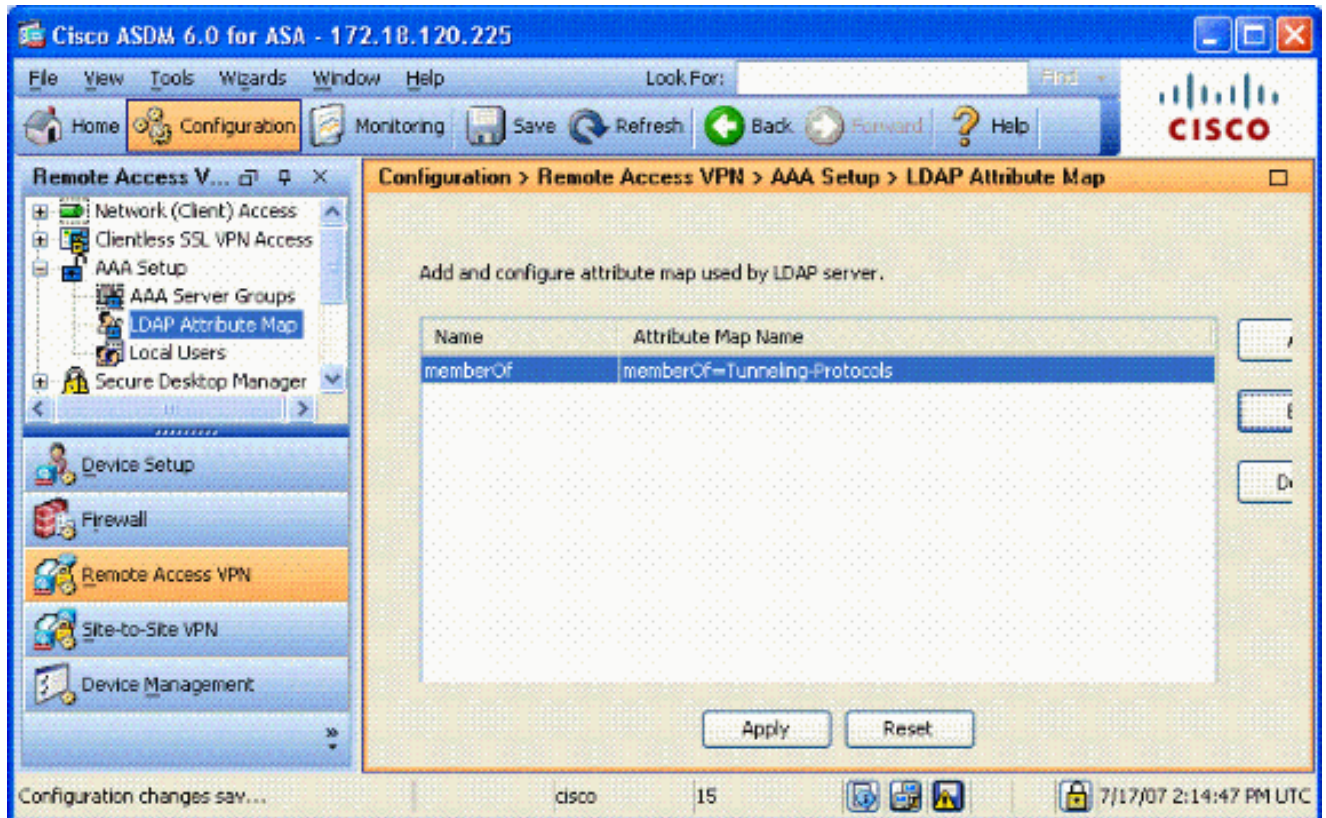
4. Klik op het plusteken om de domeinnaam uit te breiden.
5. Klik met de rechtermuisknop op de map Gebruikers en kies Nieuw > Groep.
6. Voer een groepsnaam in. Bijvoorbeeld: ASAUsers.
7. Klik op OK.
8. Klik op de map Gebruikers en dubbelklik op de groep die u zojuist hebt gemaakt.

9. Kies het tabblad Leden en klik vervolgens op Toevoegen.
10. Typ de naam van de gebruiker die u wilt toevoegen en klik vervolgens op OK.

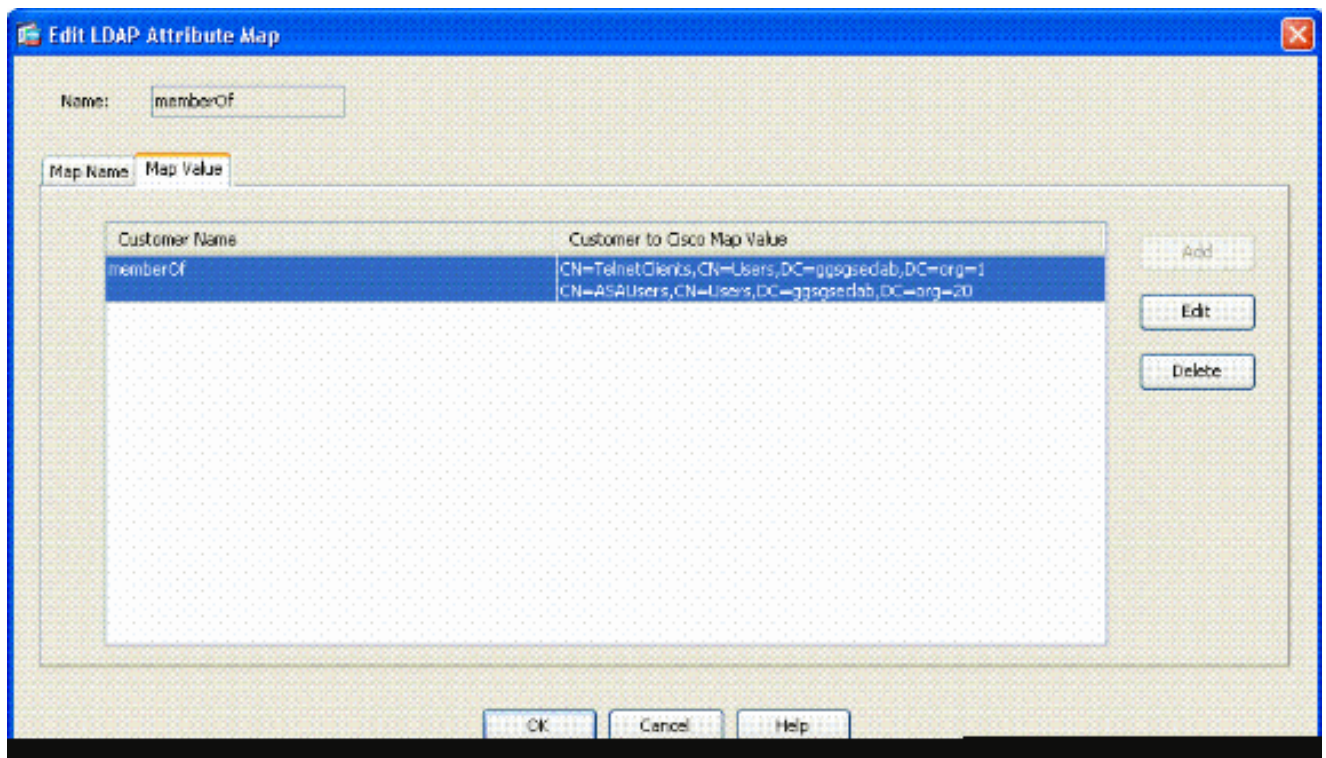
## ASA-configuratie

1. Kies in ASDM Remote Access VPN > AAA Setup > LDAP Attribute Map.
2. Klik op Add (Toevoegen).
3. Voltooi de volgende stappen in het venster Add LDAP Attribute Map. Zie figuur A3.
  - a. Voer in het tekstvak Naam een naam in.
  - b. Typ in het tabblad Map Name memberOf in het tekstvak Customer Name c.
  - c. Kies in het tabblad Map naam de optie Tunneling-protocollen in de vervolgkeuzelijst in de naam van Cisco.
  - d. Kies Toevoegen.
  - e. Klik op het tabblad Waarde kaart.
  - f. Kies Toevoegen.
  - g. In het venster LDAP-kaartwaarde van kenmerk toevoegen typt CN=ASAUsers,CN=users,DC=gsgseclab,DC=org in het tekstvak Naam van klant en typt 20 in het tekstvak Cisco-waarde.
  - h. Klik op Add (Toevoegen).
    - i. Type CN=TelnetClients, CN=Gebruikers, DC=gsgseclab, DC=org in het tekstvak Klantnaam en type 1 in het tekstvak Cisco-waarde. Zie figuur A4.
    - j. Klik op OK.
    - k. Klik op OK.
    - l. Klik op Apply (Toepassen).
  - m. De configuratie moet er uitzien als afbeelding A9.

Afbeelding A9 LDAP-kenmerkaart



4. Kies Remote Access VPN> AAA-instelling > AAA-servergroepen.
5. Klik op de servergroep die u wilt bewerken. Selecteer in het gedeelte Servers in de sectie Geselecteerde groep het IP-adres of de hostnaam van de server en klik vervolgens op Bewerken



6. Selecteer in het venster AAA-server bewerken in het tekstvak LDAP-kenmerkkaart de LDAP-kenmerkkaart die in het vervolgkeuzemenu is gemaakt.

## 7. Klik op OK.

---

Opmerking: Zet LDAP-debugging aan terwijl u test om te controleren of LDAP-binding en attribuuttoewijzingen goed werken. Zie Bijlage C voor opdrachten voor probleemoplossing.

---

### Scenario 3: Dynamisch toegangsbeleid voor meerdere leden van Kenmerken

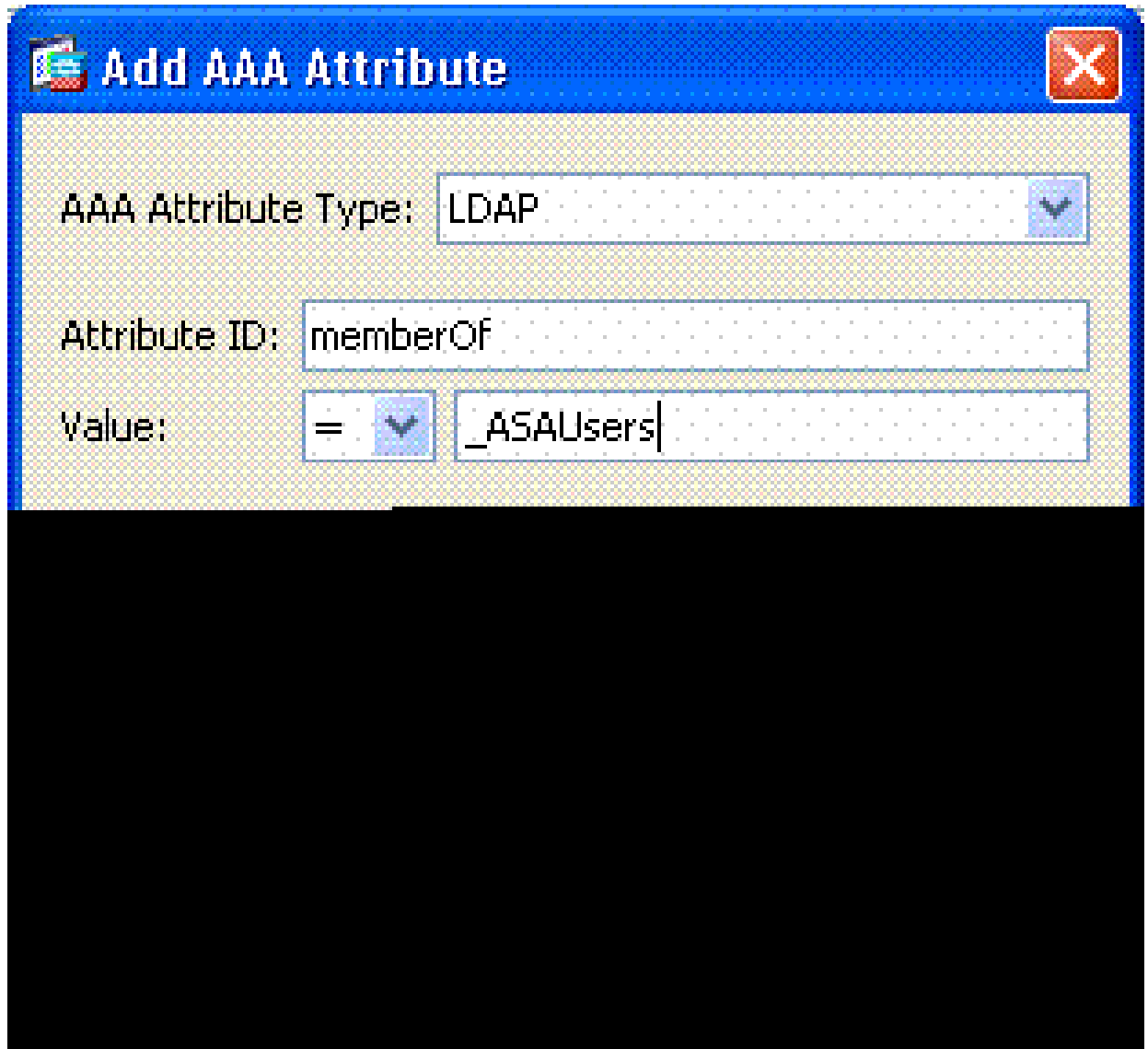
In dit voorbeeld wordt DAP gebruikt om te kijken naar meerdere memberOf-kenmerken om toegang mogelijk te maken op basis van Active Directory-groepslidmaatschap. Voorafgaand aan 8.x, leest ASA alleen het eerste memberOf attribuut. Met 8.x en hoger kan de ASA alle attributen van memberOf bekijken.

- Gebruik een groep die al bestaat of maak een nieuwe groep (of meerdere groepen) waarin ASA VPN-gebruikers lid kunnen zijn van de groep voor TOESTAAN.
- Gebruik een groep die al bestaat of maak een nieuwe groep voor niet ASA gebruikers om lid te zijn van voor DENY voorwaarden.
- Controleer in de LDAP viewer of u de juiste DN voor de groep hebt. Zie aanhangsel D. Als de DN niet goed werkt, werkt de mapping niet goed.

### ASA-configuratie

1. Kies in ASDM voor externe toegang VPN> Netwerktoegang (client) > Dynamisch toegangsbeleid.
2. Klik op Add (Toevoegen).
3. Voltooi de volgende stappen in het beleid Dynamische toegang toevoegen:
  - a. Voer in het tekstvak Naam een naam in b.
  - b. Geef in het prioriteitsgedeelte 1 of een getal groter dan 0 op.
  - c. Klik in het gedeelte Selectiecriteria op Toevoegen.
  - d. Kies LDAP in het kenmerk AAA toevoegen.
  - e. In de sectie van attributidentificatie, ga memberOf in.
  - f. In het waardegedeelte kiest u = en voert u de naam van de AD-groep in. Herhaal deze stap voor elke groep waarnaar u wilt verwijzen. Zie figuur A10.

Afbeelding A10 AAA-kenmerkkaart

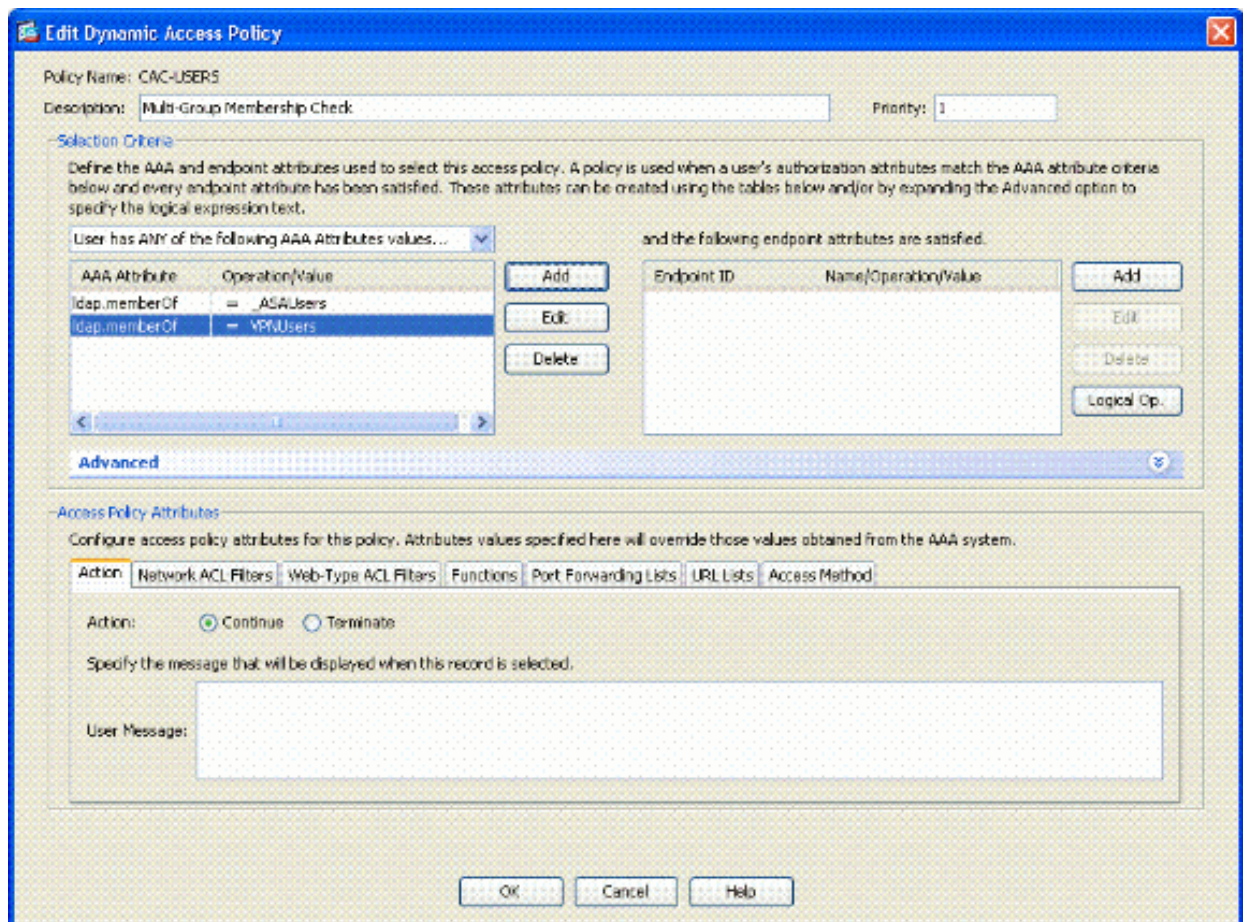


g. Klik op OK.

h. Kies Doorgaan in het gedeelte Access Policy Attributes. Zie figuur A11.

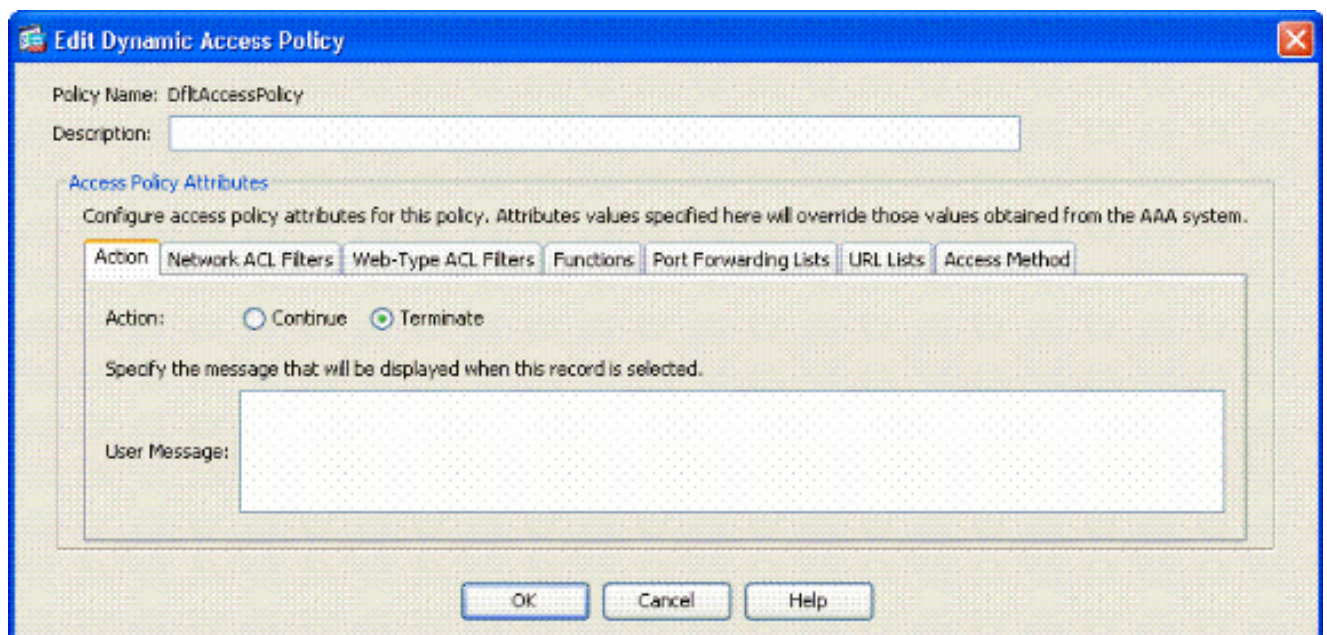
Afbeelding A11 Dynamisch beleid toevoegen





4. Kies in ASDM voor externe toegang VPN> Netwerктоegang (client) > Dynamisch toegangsbeleid.
5. Kies Standaardtoegangsbeleid en kies Bewerken.
6. De standaardactie dient op Beëindigen te worden ingesteld. Zie figuur A12.

Afbeelding A12 Dynamisch beleid bewerken



## 7. Klik op OK.

Opmerking: als Beëindigen niet is geselecteerd, mag u ook inloggen als er geen groepen zijn, omdat de standaardinstelling is om door te gaan.

## Bijlage B - ASA CLI-configuratie

### ASA 5510 router

```
<#root>
ciscoasa#
show running-config

: Saved
:
ASA Version 8.0(2)
!
hostname asa80
domain-name army.mil
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address x.x.x.x 255.255.255.128
!
interface GigabitEthernet0/1
nameif inside
security-level 100
no ip address
!
boot system disk0:/asa802-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name army.mil
!
-----ACL's-----
access-list out extended permit ip any any
-----

pager lines 24
logging console debugging
mtu outside 1500
!
-----VPN Pool-----
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0
-----

!
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
access-group out in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.120.129 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout uauth 0:05:00 absolute
!
-----LDAP Maps & DAP-----
ldap attribute-map memberOf
map-name memberOf Tunneling-Protocols
March 11, 2008 ASA - CAC Authentication for AnyConnect VPN Access
Company Confidential. A printed copy of this document is considered uncontrolled.
49
map-value memberOf CN=_ASAUsers,CN=Users,DC=gsgsec1ab,DC=org 20
ldap attribute-map msNPAAllowDialin
map-name msNPAAllowDialin Tunneling-Protocols
map-value msNPAAllowDialin FALSE 1
map-value msNPAAllowDialin TRUE 20
dynamic-access-policy-record CAC-USERS
description "Multi-Group Membership Check"
priority 1
dynamic-access-policy-record DfltAccessPolicy
action terminate
-----
!
-----LDAP Server-----
aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
ldap-base-dn CN=Users,DC=gsgsec1ab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn CN=Administrator,CN=Users,DC=gsgsec1ab,DC=org
-----
!
aaa authentication http console LOCAL
http server enable 445
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
!
-----CA Trustpoints-----
crypto ca trustpoint ASDM_TrustPoint0
revocation-check ocsp
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
cr1 configure
crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp
enrollment terminal
fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S. Government,C=US
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
cr1 configure
crypto ca trustpoint ASDM_TrustPoint2
```

```
revocation-check oosp
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override oosp trustpoint
ASDM_TrustPoint5 10 url http://oosp.disa.mil
no client-types
cr1 configure
crypto ca trustpoint ASDM_TrustPoint3
revocation-check oosp none
enrollment terminal
cr1 configure
!
```

```
-----Certificate Map-----
```

```
crypto ca certificate map DefaultCertificateMap 10
subject-name ne ""
```

```
-----CA Certificates (Partial Cert is Shown)-----
```

```
crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311b3019 06035504 03131244 6f44204a 49544320 526f6f74
```

```
crypto ca certificate chain ASDM_TrustPoint1
certificate 319e
30820411 3082037a a0030201 02020231 9e300d06 092a8648 86f70d01
01050500
305c310b 30090603 55040613 02555331 18301606 0355040a 130f552e
532e2047
6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06
0355040b
```

```
crypto ca certificate chain ASDM_TrustPoint2
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e 1be959a5
6fc20a76
```

```
crypto ca certificate chain ASDM_TrustPoint3
certificate ca 05
30820370 30820258 a0030201 02020105 300d0609 2a864886 f70d0101
05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 31163014 06035504 03130d44 6f442052 6f6f7420 43412032
301e170d
30343132 31333135 30303130 5a170d32 39313230 35313530 3031305a
305b310b
30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047
6f766572
6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b
1303504b
```

```
49311630 14060355 0403130d 446f4420 526f6f74 20434120 32308201
crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04
```

```
30820267 308201d0 a0030201 02020104 300d0609 2a864886 f70d0101
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353 20332052
6f6f7420
```

```
!
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
```

```
!
service-policy global_policy global
!
```

```
-----SSL/WEBvpn-windows-----
ssl certificate-authentication interface outside port 443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
```

```
-----VPN Group/Tunnel Policy-----
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-windows-tunnel-protocol svc
address-pools value CAC-USERS
webvpn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-windows-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
```

```
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
-----
prompt hostname context
```

## Bijlage C - Probleemoplossing

### AAA en LDAP voor probleemoplossing

- debug ldap 255—Hier wordt LDAP-uitwisseling weergegeven
- debug aaa algemene 10-displays AAA-uitwisselingen

### Voorbeeld 1: Toegestane verbinding met juiste attribuuttoewijzing

Dit voorbeeld toont de output van debug ladder en debug een gemeenschappelijk tijdens een succesvolle verbinding met scenario 2 getoond in Bijlage A.

#### Afbeelding C1: debug LDAP en debug aaa common output - correcte mapping

```
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap:// 172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160, status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=gsgsec1ab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
```

```
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
0..50...../.....60...*.H.....0@1.0.....&....,d....com1.0.....
&....,d...
[78] userCertificate: value =
0..'0...../..t.....50...*.H.....0@1.0.....&....,d....com1.0.....
&....,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value = CN=ASAUsers,CN=Users,DC=gsgsec1ab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = .....q.....mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
```

```

User: CAC-USER
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#

```

## Voorbeeld 2: Toegestane verbinding met verkeerd geconfigureerde Cisco-kenmerktoewijzing

Dit voorbeeld toont de output van debug ladder en debug een gemeenschappelijk tijdens een toegestane verbinding met scenario 2 getoond in Bijlage A.

### Afbeelding C2: debug LDAP en debug aaa common output - incorrecte mapping

```

AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction

```



```
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389, status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=gsgsec1ab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0..50...../.....60...*.H.....0@1.0.....&....,d....com1.0.....
&....,d...
[82] userCertificate: value =
0..'0...../..t.....50...*.H.....0@1.0.....&....,d....com1.0.....
&....,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value = CN=ASAUsers,CN=Users,DC=gsgsec1ab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=gsgsec1ab,DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = .....q.....mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
```

```
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "gsgsec1ab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
```

```
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

## DAP voor probleemoplossing

- debug dap fouten—Hier worden DAP fouten weergegeven
- debug dap trace—Hier wordt DAP-functiespoor weergegeven

### Voorbeeld 1: Toegestane verbinding met DAP

Dit voorbeeld toont de output van debug dap fouten en debug dap spoor tijdens een succesvolle verbinding met scenario 3 getoond in Bijlage A. Merk meerdere memberOf attributen op. U kunt tot zowel \_ASAUUsers als VPNUsers of top één van beide groepen behoren, die afhankelijk is van de ASA-configuratie.

Afbeelding C3: debug DAP

```
<#root>
#
debug dap errors
debug dap errors enabled at level 1
#
debug dap trace
debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for user:
1241879298@mil
-----
1: action = continue
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=gsgsec1ab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
```

```
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1 = VPUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2 = _ASUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
.....F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgsec1ab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
```

```

"VPNUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "CACUSERS";
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.

```

## Voorbeeld 2: Ontkende verbinding met DAP

Dit voorbeeld toont de output van debug dap fouten en debug dap spoor tijdens een onsuccesvolle verbinding met scenario 3 getoond in Bijlage A.

Afbeelding C4: debug DAP

```
<#root>
```

```
#
debug dap errors

debug dap errors enabled at level 1
#
debug dap trace

debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for user:
1241879298@mil
-----
---
1: action = terminate
DAP_TRACE: DAP_open: C91154E8
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=gsgsec1ab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf = DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
.....F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
```

```
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgsec1ab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] = "DnsAdmins";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAAllowDialin"] = "TRUE";
```

```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
```

## Certificaatautoriteit voor probleemoplossing/OCSP

- debug crypto ca 3
- In de configuratiemodus—vastlegging klasse kan console(of buffer) debuggen

Deze voorbeelden tonen een geslaagde certificaatsvalidatie met de OCSP-responder en een mislukt beleid voor overeenkomende certificaatgroepen.

Afbeelding C3 toont de debug-uitvoer met een gevalideerd certificaat en een beleid voor werkgroepmatching.

Afbeelding C4 toont de debug-uitvoer van een verkeerd geconfigureerd overeenkomend beleid voor certificaatgroepen.

Afbeelding C5 toont de debug-uitvoer van een gebruiker met een ingetrokken certificaat.

### Afbeelding C5: OCSP-debugging - succesvolle certificaatvalidatie

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint: ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert with serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
```



```

CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap, index 10 for
WebVPN group map processing. No tunnel group is configured.
CRYPTO_PKI: Peer cert could not be authorized with map:
DefaultCertificateMap.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.
CRYPTO_PKI: Ignoring match on map SSL, index 20 for WebVPN group map

```

Afbeelding C5: Uitvoer van een mislukt overeenkomend beleid voor een certificaatgroep

Figuur C5: Uitvoering van een ingetrokken certificaat

```

n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,validid cor =noct
oamuthori,zed.
map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
Tunnel Group Match on map DefaultCertificateMap sequence # 10.
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
already in the database...
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Found a suitable authenticated trustpoint trustpoint0.
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=gsgseclab,dc=org, issuer_name:
cn=gsgseclab,dc=gsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=Ethan Hunt,ou=MIL,dc=gsgseclab,dc=org, map rule: subject-name
ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is revoked, serial
number: 2FB5FC74000000000035, subject name: cn=Ethan

```

```
Hunt,ou=MIL,dc=gsgsec1ab,dc=org  
CRYPTO_PKI: Certificate not validated
```

## Bijlage D - LDAP-objecten controleren in MS

In de cd van Microsoft server 2003 zijn er extra gereedschappen die kunnen worden geïnstalleerd om de LDAP-structuur en de LDAP-objecten/kenmerken te bekijken. Als u deze tools wilt installeren, gaat u naar de directory Support op de CD en vervolgens naar Tools. Installeer SUPTOOLS.MSI.

### LDAP-viewer

1. Kies Start > Uitvoeren na de installatie.
2. Typ ldp en klik vervolgens op OK. Hiermee start de LDAP-viewer.
3. Kies Verbinding > Verbinden.
4. Voer de servernaam in en klik op OK.
5. Kies Verbinding > Bind.
6. Voer een gebruikersnaam en wachtwoord in.

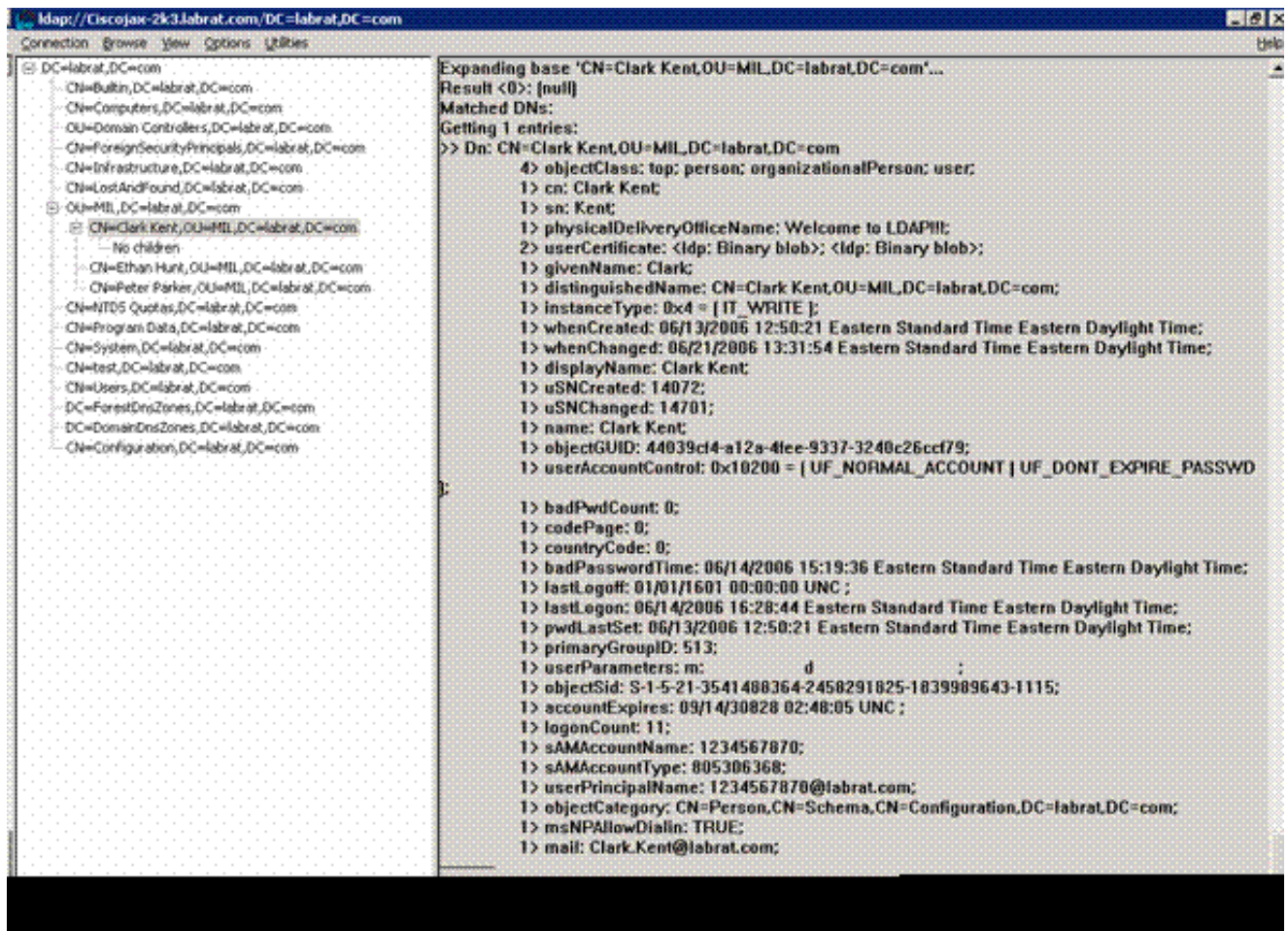
---

Opmerking: u hebt beheerdersrechten nodig.

---

7. Klik op OK.
8. LDAP-objecten bekijken. Zie figuur D1.

Afbeelding D1: LDAP Viewer

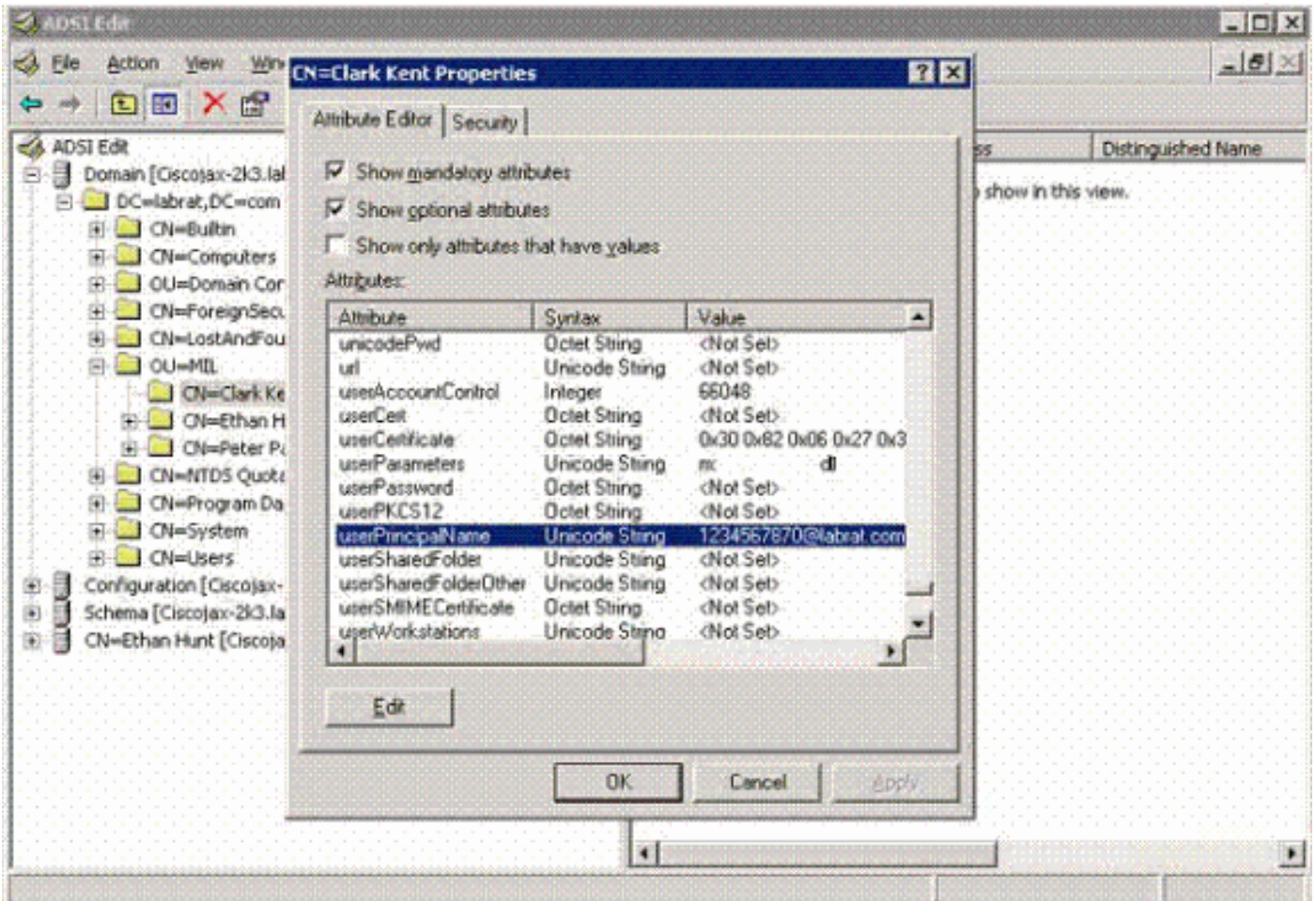


## Active Directory-interfaceditor

- Kies Start > Uitvoeren in de Active Directory-server.
- Type adsiedit.msc. Dit start de editor.
- Klik met de rechtermuisknop op een object en klik op Eigenschappen.

Dit gereedschap toont alle kenmerken voor specifieke objecten. Zie figuur D2.

Afbeelding D2: ADSI Edit



## Aanhangsel E

U kunt een AnyConnect-profiel maken en aan een werkstation toevoegen. Het profiel kan verwijzen naar verschillende waarden zoals ASA hosts of certificaat matching parameters zoals voorname naam of emittent. Het profiel wordt opgeslagen als een .xml bestand en kan worden bewerkt met Kladblok. Het bestand kan handmatig aan elke client worden toegevoegd of vanuit de ASA via een groepsbeleid worden gedrukt. Het bestand wordt opgeslagen in:

C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile

Voer de volgende stappen uit:

1. Kies AnyConnectProfile.tmpl en open het bestand met Kladblok.
2. Voer de juiste wijzigingen in het bestand uit, zoals de emittent of de host-IP. Zie bijvoorbeeld afbeelding F1.
3. Als u klaar bent, slaat u het bestand op als .xml.

Raadpleeg de documentatie van Cisco AnyConnect voor profielbeheer. Kortom:

- Een profiel moet uniek worden genoemd naar uw Bedrijf. Een voorbeeld is: CiscoProfile.xml
- De profielnaam moet hetzelfde zijn, ook al is deze verschillend voor individuele groepen binnen de onderneming.

Dit bestand is bedoeld om te worden onderhouden door een beheerder van een beveiligde gateway en vervolgens te worden gedistribueerd met de clientsoftware. Het profiel op basis van deze XML kan op elk moment worden gedistribueerd naar clients. De ondersteunde distributiemechanismen worden aangeboden als een gebundeld bestand met de softwaredistributie of als onderdeel van het automatische downloadmechanisme. Het automatische downloadmechanisme is alleen beschikbaar voor bepaalde producten van Cisco Secure Gateway.

---

Opmerking: Beheerders worden sterk aangeraden om het XML-profiel dat ze maken te valideren met een online validatietool of via de profielimportfunctionaliteit in ASDM. Validatie kan worden uitgevoerd met de AnyConnectProfile.xsd in deze map. AnyConnect Profile is het basiselement dat het AnyConnect-clientprofiel vertegenwoordigt.

---

Dit is een voorbeeld van een XML-bestand van Cisco AnyConnect VPN-clientprofiel.

```

<#root>

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">

!--- The ClientInitialization section represents global settings !--- for the client. In some cases, fo
!--
-->
-
<ClientInitialization>

!--- The Start Before Logon feature can be used to activate !--- the VPN as part of the logon sequence.
-->
<UseStartBeforeLogon UserControllable="false">>false</UseStartBeforeLogon>

!--- This control enables an administrator to have a one time !--- message displayed prior to a users
-->

<ShowPreConnectMessage>>false</ShowPreConnectMessage>

```

```

!-- This section enables the definition of various attributes !--- that can be used to refine client c
-->
-
<CertificateMatch>

!--- Certificate Distinguished Name matching allows !--- for exact match criteria in the choosing of a

- <DistinguishedName>
- <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
<Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition>
</DistinguishedName>
</CertificateMatch>
</ClientInitialization>
-
!-- This section contains the list of hosts from which !--- the user is able to select.
-
<ServerList>

!--- This is the data needed to attempt a connection to !--- a specific host.

-->
-
<HostEntry>
<HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress>
</HostEntry>
- <HostEntry>
<HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>

```

## Gerelateerde informatie

- [Certificaten en CRL's die zijn gespecificeerd door X.509 en RFC 3280](#)
- [OCSP bepaald door RFC 2560](#)
- [Public Key infrastructuur - introductie](#)
- ["Lichtgewicht OCSP" geprofileerd door conceptstandaard](#)
- [SSL/TLS opgegeven door RFC 2246](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.