ASA 8.x: AnyConnect SSL VPN CAC-Smart Cards-configuratie met MAC-ondersteuning

Inhoud

Inleiding

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

Het bereik van dit document is dat het de configuratie van Cisco ASA met Adaptieve Security Devices Manager (ASDM), Cisco AnyConnect VPN-client en Microsoft Active Directory (AD)/Light Directory Access Protocol (LDAP) bestrijkt.

De configuratie in deze gids gebruikt Microsoft AD/LDAP server. Dit document heeft ook betrekking op geavanceerde functies zoals OCSP, LDAP-kaarten en Dynamisch toegangsbeleid (DAP).

Voorwaarden

Vereisten

Een basisbegrip van Cisco ASA, Cisco AnyConnect Client, Microsoft AD/LDAP en PKI (Public Key Infrastructure) is gunstig voor het begrip van de volledige installatie. Bekendheid met AD-groepslidmaatschap, gebruikerseigenschappen en LDAP-objecten helpen bij de correlatie van het vergunningsproces tussen certificaareigenschappen 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 uitvoeren
- Cisco Adaptieve Security Devices Manager (ASDM) versie 6.x voor ASA 8.x

- Cisco AnyConnect VPN-client 2.2 met MAC-ondersteuning

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.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Cisco ASA-configuratie

Deze sectie betreft de configuratie van Cisco ASA via ASDM. Het bestrijkt de benodigde stappen om een VPN-tunnel op afstand in te zetten via een SSL AnyConnect-verbinding. Het CAC-certificaat wordt gebruikt voor echtheidscontrole en de gebruikersbenaming (UPN) in het certificaat wordt in een actieve map voor autorisatie ingevuld.

Invoeringsoverwegingen

- Deze gids heeft GEEN betrekking op basisconfiguraties zoals interfaces, DNS, NTP, routing, apparaattoegang, ASDM-toegang enzovoort. Verondersteld wordt dat de netwerkexploitant bekend is met deze configuraties.Raadpleeg multifunctionele security applicaties voor meer informatie.
- De secties die in RED worden gemarkeerd zijn verplichte configuraties nodig voor basisVPN-toegang. Een VPN-tunnel kan bijvoorbeeld worden ingesteld met de CAC-kaart zonder OCSP-controles, LBP-mappingen en Dynamische Access Policy (DAP)-controles uit te voeren. DoD verplicht OCSP-controle maar de tunnelwerking werkt zonder OCSP ingesteld.
- De in BLUE gemarkeerde secties zijn geavanceerde functies die kunnen worden toegevoegd om het ontwerp meer beveiliging toe te voegen.
- ASDM en AnyConnect/SSL VPN kunnen niet dezelfde poorten op dezelfde interface gebruiken. Aanbevolen wordt om de havens aan de ene of de andere te veranderen om toegang te verkrijgen. Gebruik bijvoorbeeld poort 445 voor ASDM en verlaat 443 voor AC/SSL VPN. De ASDM URL toegang is veranderd in 8.x. Gebruik `https://<ip_adres>:<poort>/admin.html`.
- De vereiste ASA-afbeelding is ten minste 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 over de controle van LGO-objecten in MS.
- Zie Verwante informatie voor een lijst met toepassingspoorten voor firewallconfiguratie.

Configuratie van verificatie, autorisatie, accounting (AAA)

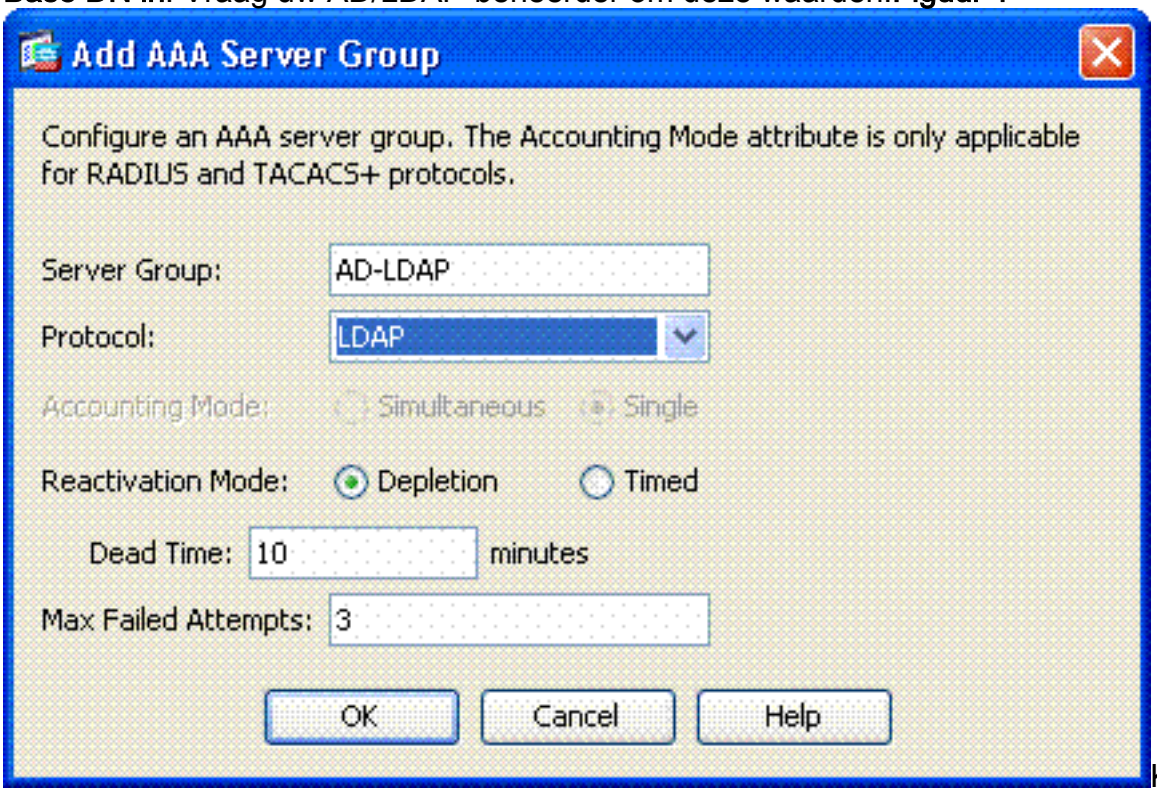
U bent geauthentiseerd met het gebruik van het certificaat in hun Gemeenschappelijke Toegangskaart (CAC) door de server van de Beslissingsinstantie (CA) of de server CA van hun eigen organisatie. Het certificaat moet geldig zijn voor toegang op afstand tot het netwerk. Naast authenticatie moet u ook geautoriseerd worden om een Microsoft Active Directory of Lichtgewicht

Directory Access Protocol (LDAP) object te gebruiken. Het Department of Defense (DoD) schrijft voor dat de gebruikersbenaming (UPN) voor de vergunning wordt gebruikt, die deel uitmaakt van het vak Onderwerp Alternative Name (SAN) van het certificaat. Het UPN of EDI/PI moeten in deze indeling zijn, 1234567890@mil. Deze configuraties tonen hoe u AAA-server in de ASA kunt configureren met een LDAP-server voor autorisatie. Zie Bijlage A voor aanvullende configuratie met LDAP-objectmapping.

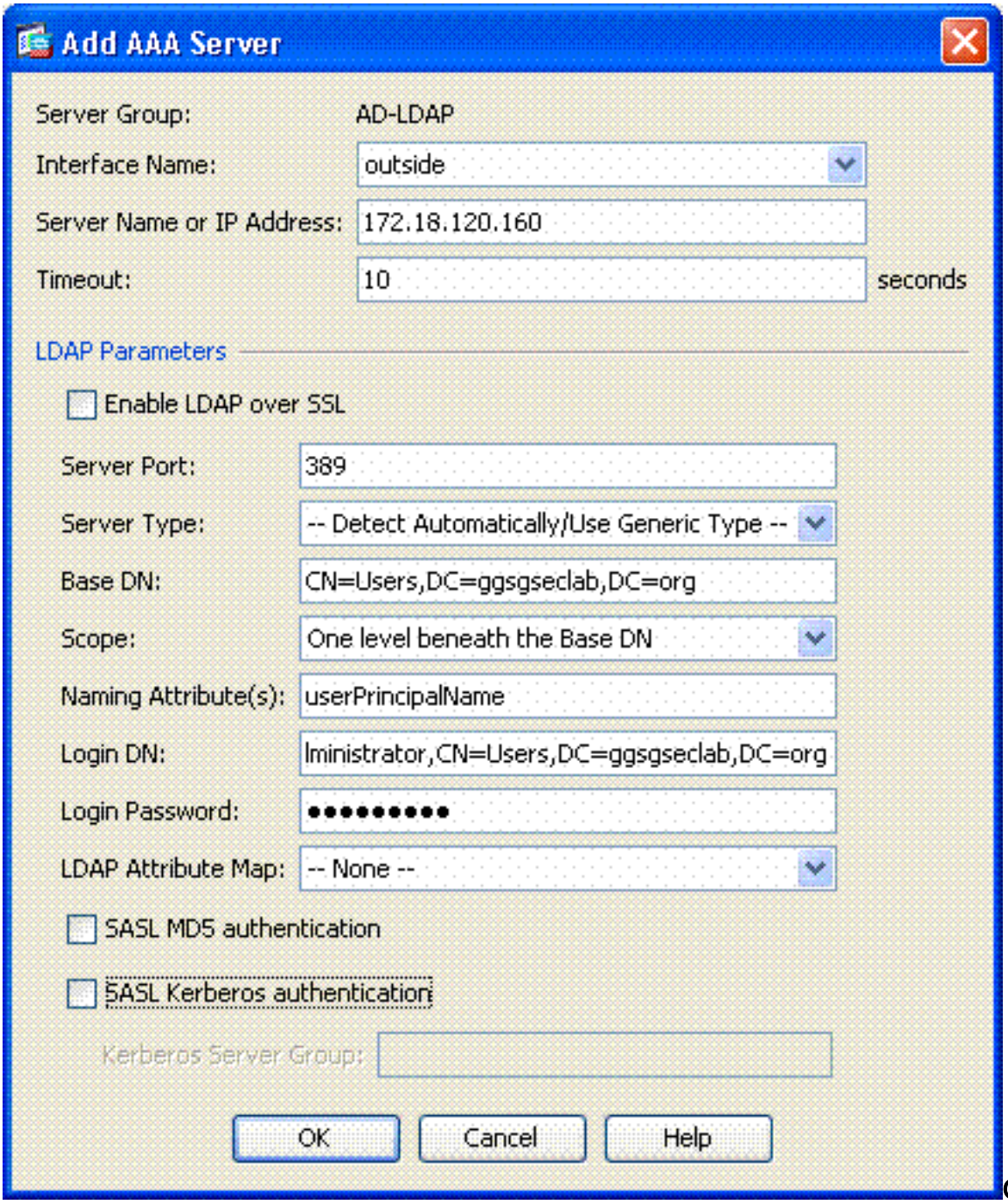
LDAP-server configureren

Voer de volgende stappen uit:

1. Kies **Remote Access VPN > AAA-instelling > AAA-servergroep.**
2. Klik in tabel met AAA-servergroepen op **Toevoegen 3**.
3. Voer de naam van de servergroep in en kies **LDAP** in de radioknop van het protocol. Zie afbeelding 1.
4. Klik in servers in de geselecteerde groepstabel op **Toevoegen**. Zorg ervoor dat de server die u maakt, wordt gemarkeerd in de vorige tabel.
5. Voltooi de volgende stappen in het venster AAA-server. Zie afbeelding 2.**Opmerking:** Kies de optie **LDAP via SSL** als uw LDAP/AD voor dit type verbinding is ingesteld.Kies de interface waar de LDAP zich bevindt. Deze gids toont binnen de interface.Voer het IP-adres van de server in.Geef de **serverpoort op**. De standaard LDAP poort is 389.Kies **servertype**.Voer **Base DN in**. Vraag uw AD/LDAP-beheerder om deze waarden.**Figuur 1**



Kies het juiste antwoord onder het toepassingsgebied. Dit is afhankelijk van de basis DNA. Vraag uw AD/LDAP-beheerder om hulp.Voer in de naamgevingseigenschap **userPrincipalName in**. Dit is de eigenschap die wordt gebruikt voor gebruikersautorisatie in de AD/LDAP server.Voer in de Meld DNA de beheerder in.**Opmerking:** U hebt administratieve rechten of rechten om de LDAP-structuur te bekijken of te doorzoeken, die gebruikersobjecten en groepslidmaatschap omvat.Typ het wachtwoord van de beheerder in het inlogwachtwoord.Laat de LDAP eigenschap aan **niemand** staan.**Figuur 2**



Opmerking: U gebruikt deze optie later in de configuratie om andere AD/LDAP-objecten voor autorisatie toe te voegen.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 Subcoördinate certificaatinstantie) die nodig zijn. Ten tweede moet de ASA bij een bepaald CA worden ingeschreven en het identiteitsbewijs worden verkregen. DoD PKI gebruikt deze certificaten, Root CA2, Class 3 Root, CA## Intermediate dat de ASA met, ASA ID certificaat en OCSP certificaat wordt ingeschreven. Maar als u ervoor kiest om OCSP niet te gebruiken, hoeft het OCSP-certificaat *niet* te worden geïnstalleerd.

Opmerking: Neem contact op met uw security POC om wortelcertificaten te verkrijgen evenals instructies hoe u zich voor een identiteitsbewijs voor een apparaat kunt aanmelden. Een SSL-certificaat moet voldoende zijn voor de ASA voor toegang op afstand. Een dubbel SAN-certificaat

is *niet* vereist.

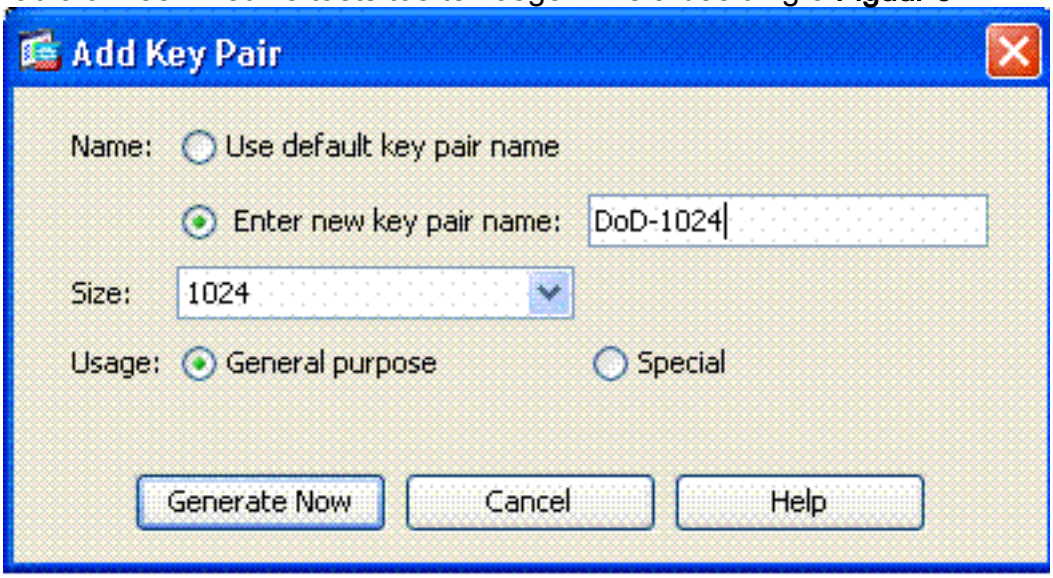
Opmerking: de lokale machine moet ook de DoD CA-keten hebben geïnstalleerd. De certificaten kunnen worden bekeken in de Microsoft certificaatwinkel met Internet Explorer. DoD heeft een batchbestand gemaakt dat automatisch alle CA's aan de machine toevoegt. Vraag uw PKI POC om meer informatie.

Opmerking: DoD CA2 en Class 3 Root evenals het ASA ID en CA tussenstation dat de ASA cert heeft afgegeven, dienen de enige CA's te zijn die nodig zijn voor gebruikersverificatie. Alle huidige CA-tussenproducten vallen onder de CA2- en Klasse 3-roetketen 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 > identiteitsbewijs > Toevoegen**.
2. Kies **een nieuw id certificaat toevoegen** en vervolgens **Nieuw** door de optie sleutelpaar.
3. Voer in het venster Toetsenpaneel toevoegen een sleutelnaam in, **DoD-1024**. Klik op de radio om een nieuwe toets toe te voegen. Zie afbeelding 3.**Figuur 3**

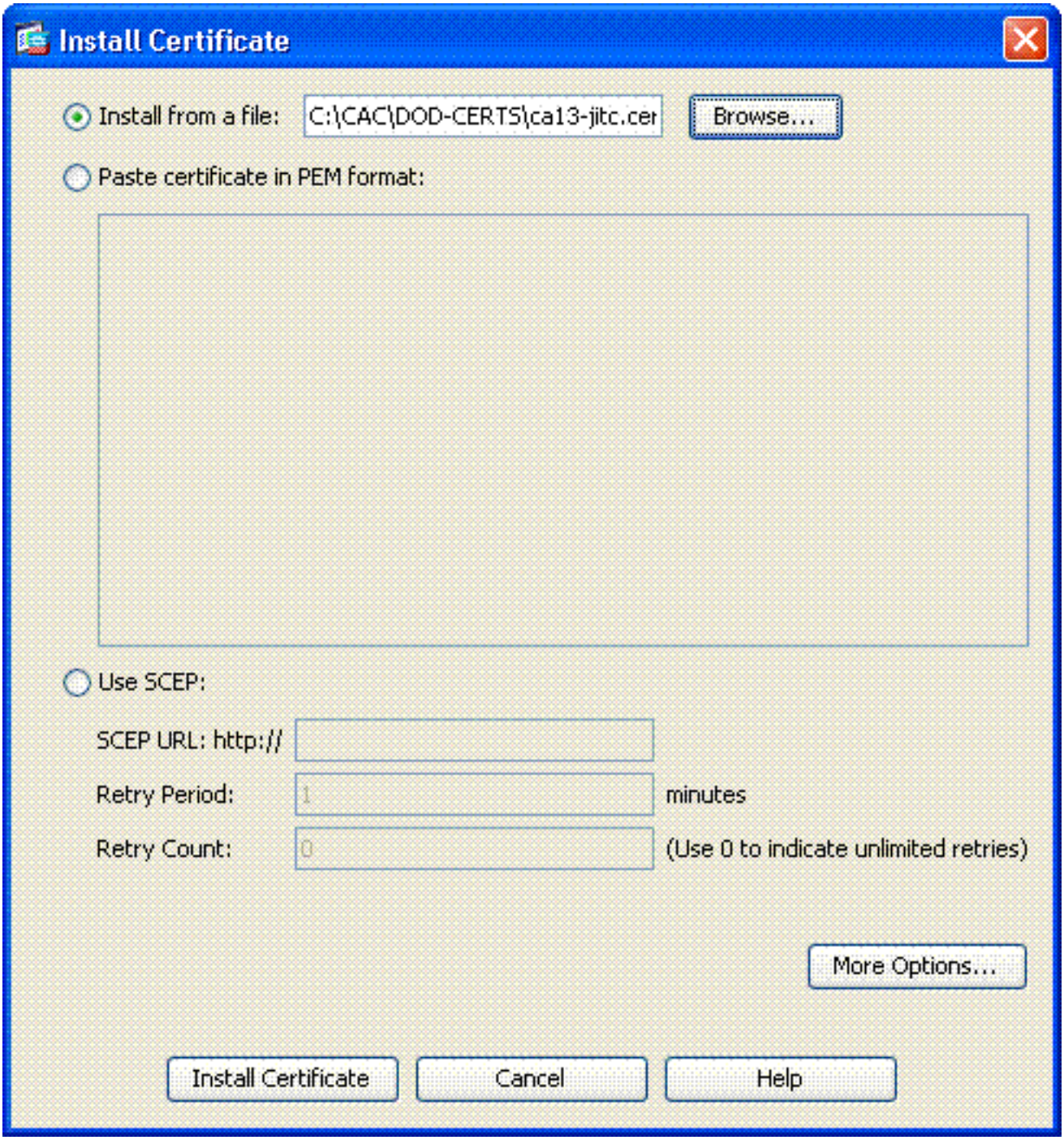


4. Kies grootte van de toets.
5. Houd gebruik voor **algemene doeleinden**.
6. Klik op **Generate Now**.**Opmerking:** DoD Root CA 2 gebruikt een 2048-bits toets. Een tweede toets die een 2048 bit key-paar gebruikt moet worden gegenereerd om deze CA te kunnen gebruiken. Voltooi de bovenstaande stappen om een tweede toets toe te voegen.

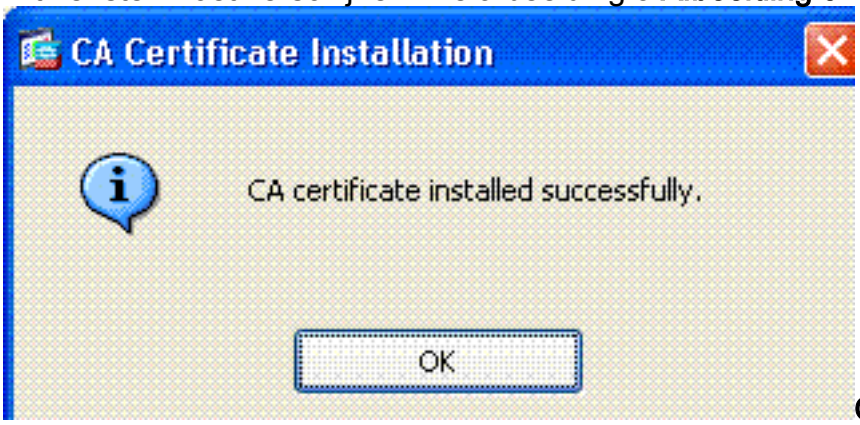
Root CA-certificaten installeren

Voer de volgende stappen uit:

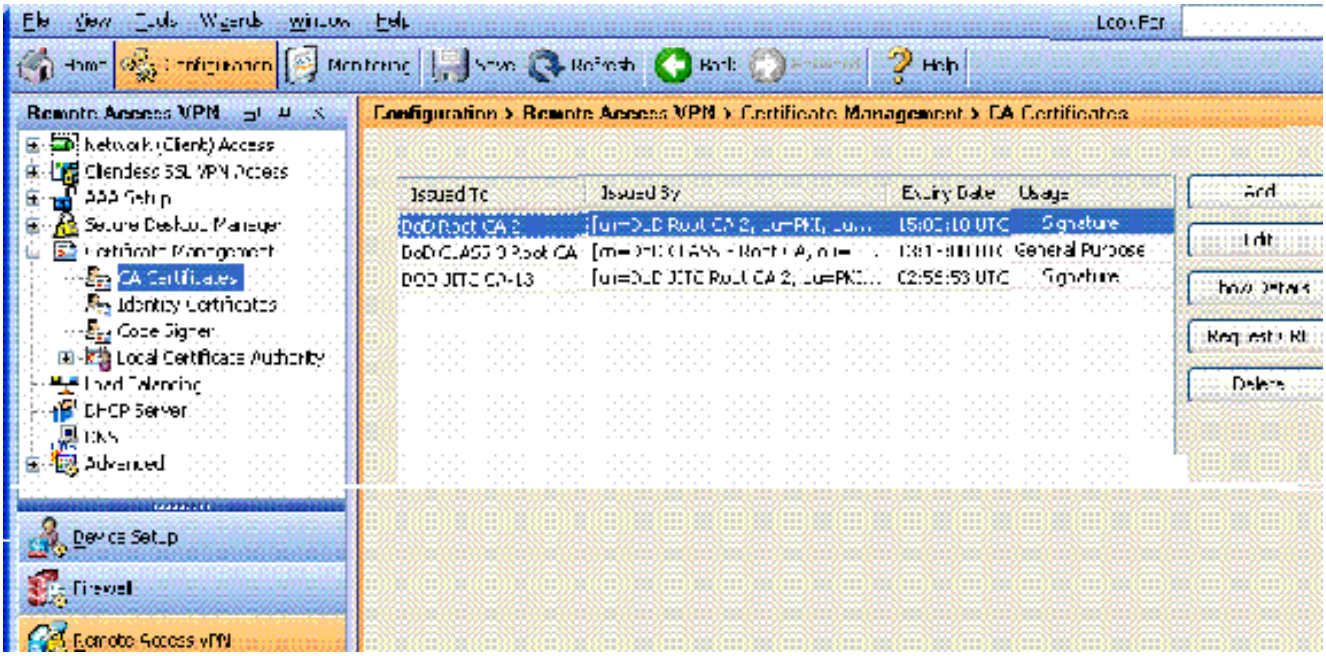
1. Kies **Remote Access VPN > certificaatbeheer > CA-certificaat > Add**.
2. Kies **Installeer uit bestand** en blader naar het certificaat.
3. Kies **installatiecertificaat**.**Afbeelding 4: Root-certificaat installeren**



4. Dit venster moet verschijnen. Zie afbeelding 5.**Afbeelding 5**

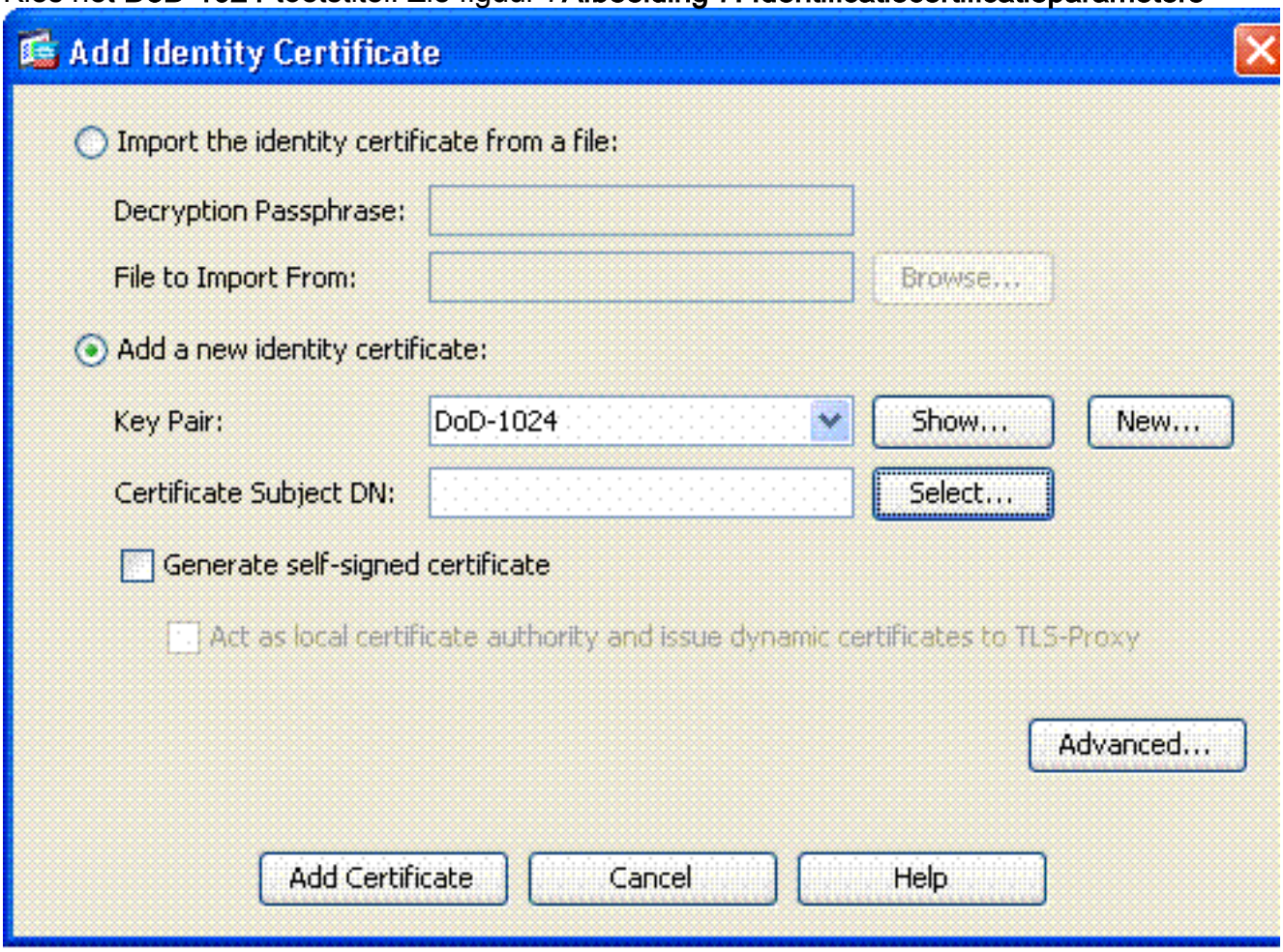


Opmerking: Herhaal stap 1 tot en met 3 voor elk certificaat dat u wilt installeren. DoD PKI vereist een certificaat voor elk van deze: Root CA 2, Class 3 Root, CA# Intermediate, ASA ID en OCSP Server. Het OCSP-certificaat is niet nodig als u OCSP niet gebruikt.**Afbeelding 6: Root-certificaat installeren**

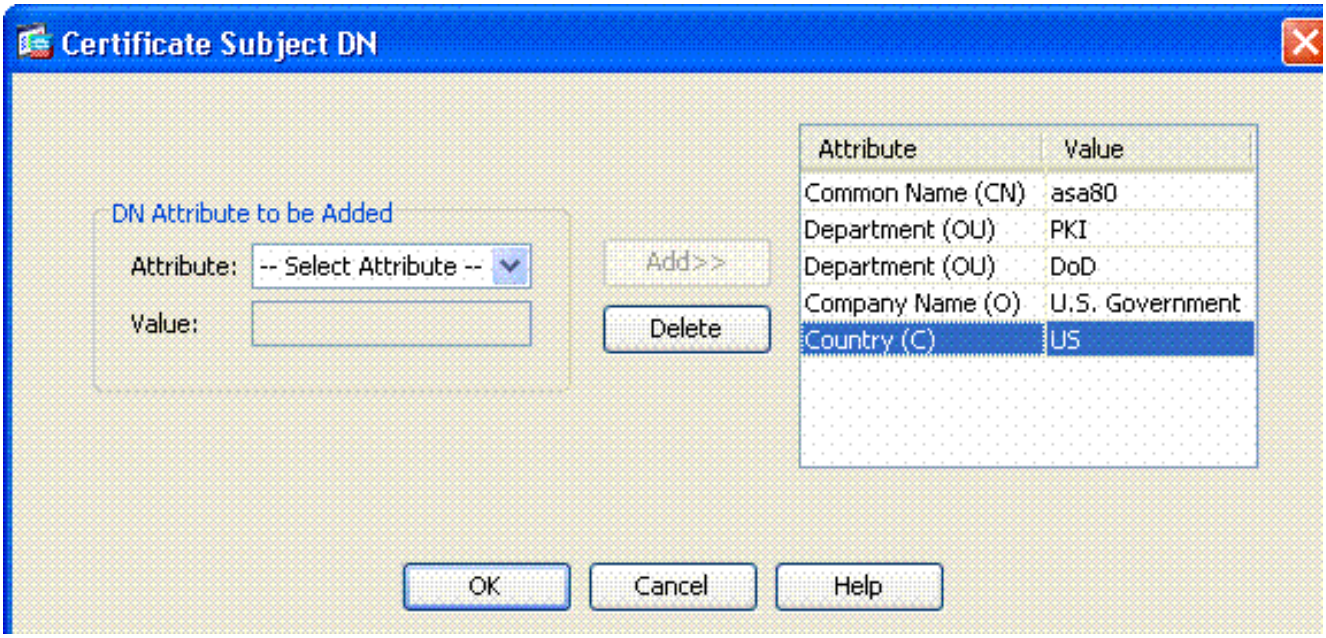


ASA invoeren en identiteitsbewijs installeren

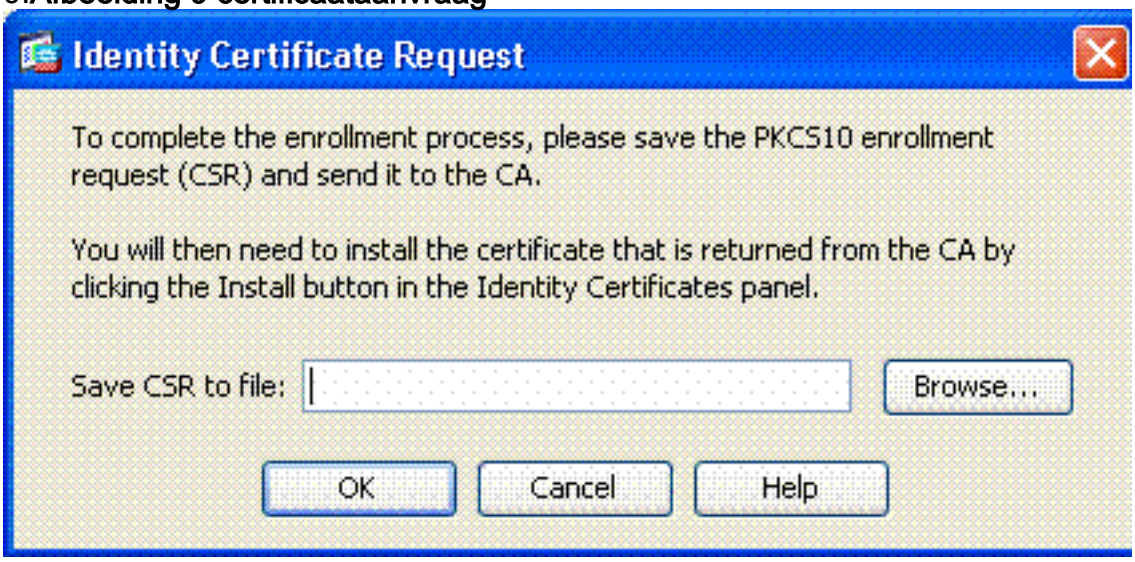
1. Kies **Remote Access VPN > certificaatbeheer > identiteitsbewijs > Toevoegen**.
2. Kies **een nieuw certificaat toevoegen**.
3. Kies het **DoD-1024-**toetstitel. Zie figuur 7**Afbeelding 7: Identificatiecertificatieparameters**



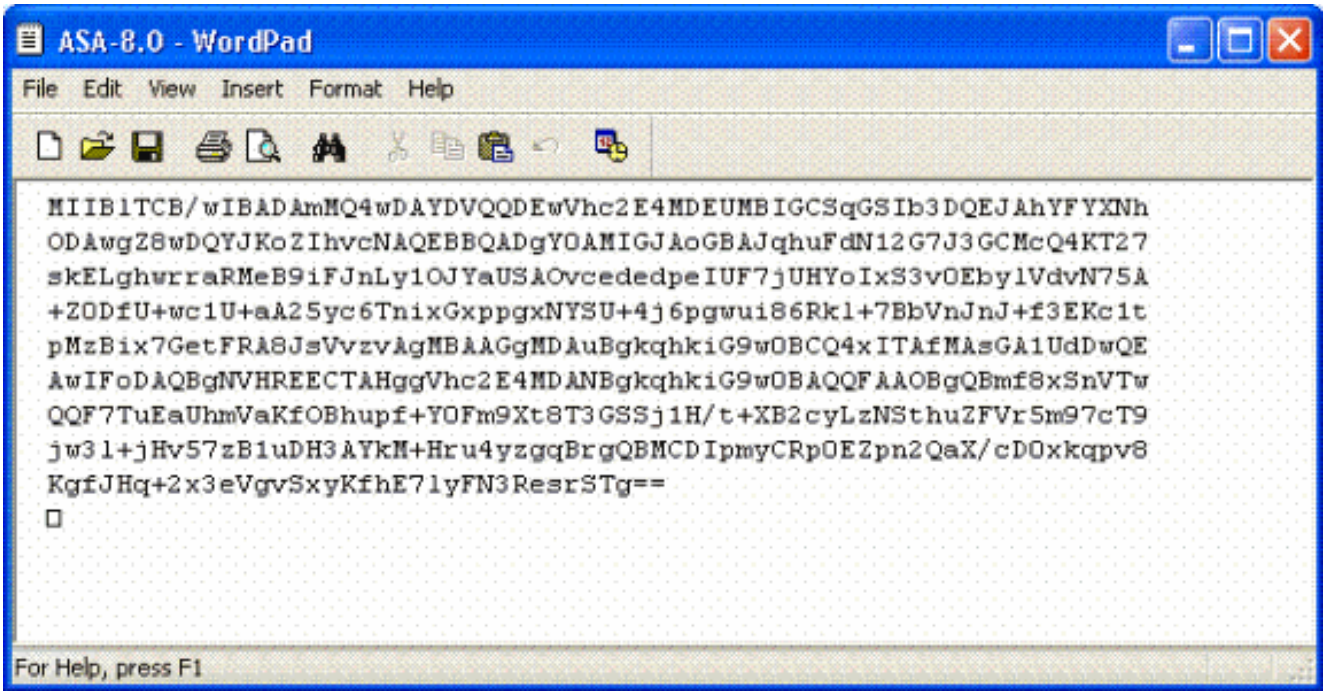
4. Ga naar het veld DN-certificaat en klik op **Selecteren**.
5. Voer in het venster Onderwerp van het certificaat de informatie van het apparaat in. Zie bijvoorbeeld afbeelding 8.**Afbeelding 8: DN bewerken**



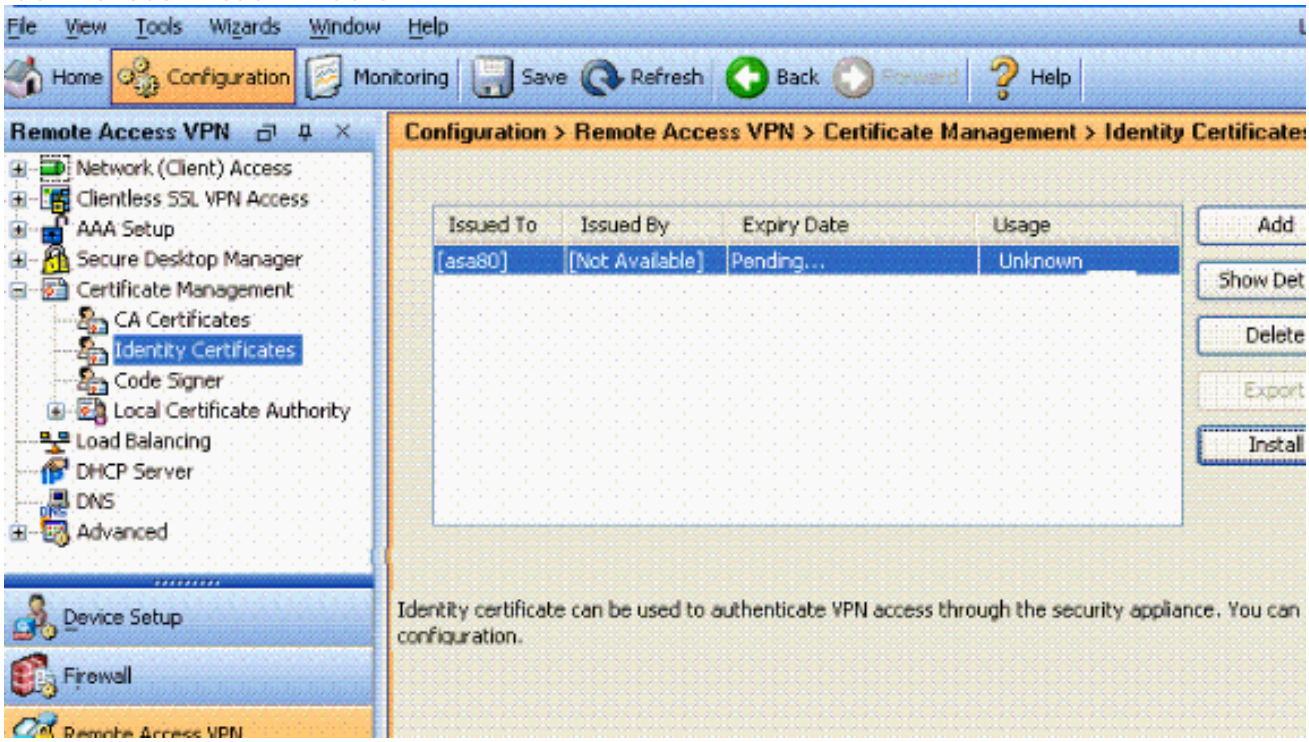
6. Kies **OK**.**Opmerking:** Zorg ervoor dat u de hostname van het apparaat gebruikt dat in uw systeem is ingesteld wanneer u de onderwerpregel DNA toevoegt. De PKI POC kan u de verplichte velden vertellen.
7. Kies **certificaat toevoegen**.
8. Klik op **Bladeren** om de map te selecteren waar u het verzoek wilt opslaan. Zie afbeelding 9.**Afbeelding 9 certificaataanvraag**



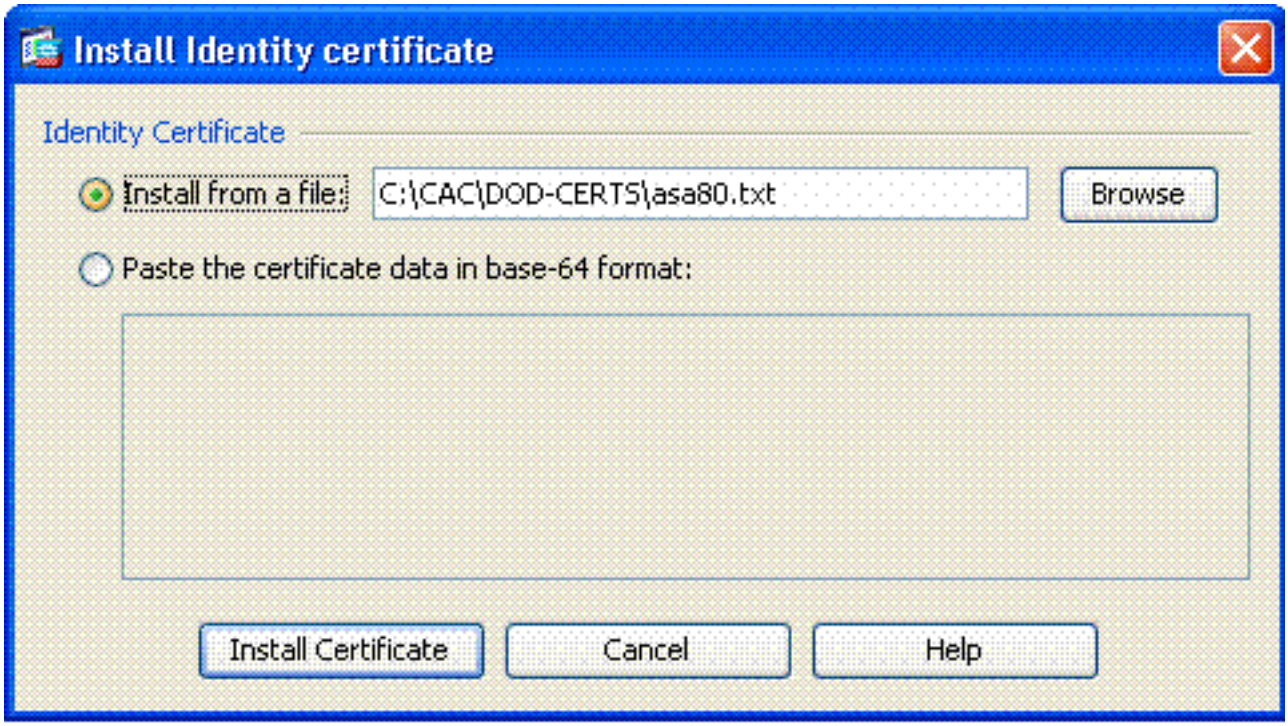
9. Open het bestand met WordPad, kopieer het verzoek naar de juiste documentatie en stuur het naar uw PKI POC. Zie afbeelding 10.**Afbeelding 10: Aanvraag tot inschrijving**



10. Nadat u het certificaat van de CA-beheerder hebt ontvangen, kiest u **Remote Access VPN > certificaatbeheer > ID-certificaat > Installatie**. Zie afbeelding 11.**Afbeelding 11: Identiteitscertificaat invoeren**



11. Blader in het venster Installeer het certificaat en **kies** de optie **Certificaat installeren**. Zie bijvoorbeeld afbeelding 12.**Afbeelding 12: Identiteitsbewijs installeren**



Opmerking: Aanbevolen wordt het vertrouwenspoint van het ID-certificaat uit te voeren om het afgegeven certificaat en de belangrijkste paar op te slaan. Hiermee kan de ASA-beheerder het certificaat en de sleutelparen naar een nieuwe ASA importeren in het geval van RMA- of hardwarestoring. Raadpleeg Trustpoints exporteren en importeren voor meer informatie.**Opmerking:** Klik op **SAVE** om de configuratie in het flitsgeheugen op te slaan.

AnyConnect VPN-configuratie

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

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

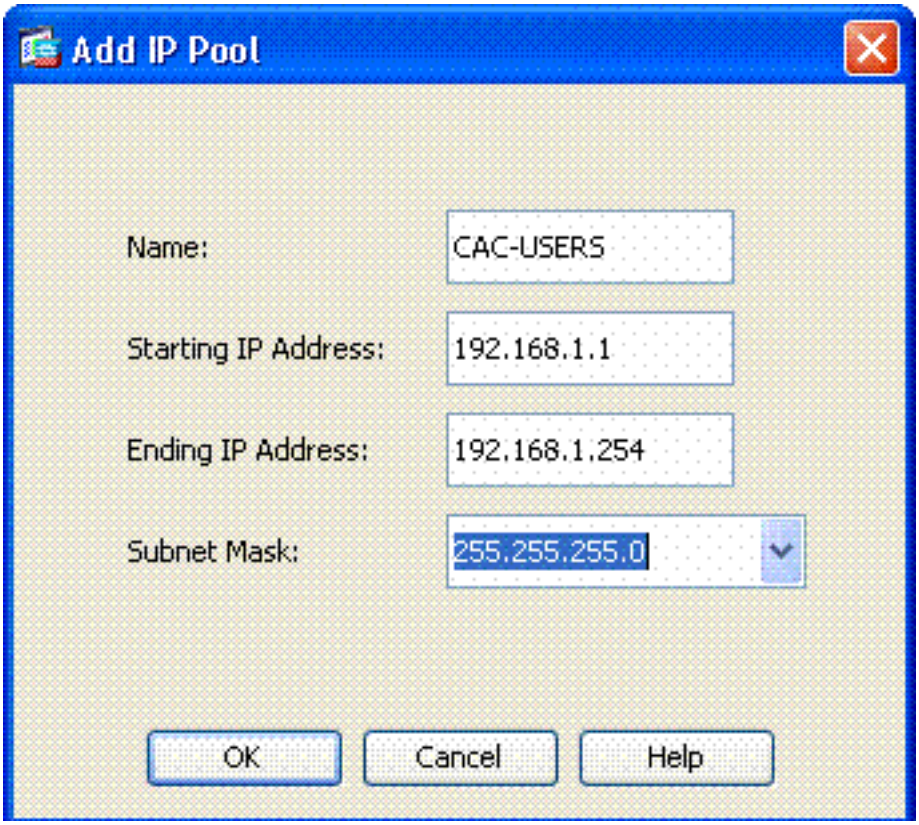
1. U kunt de client vanaf de Cisco-website downloaden en op hun computer installeren.
2. De gebruiker kan de ASA benaderen via een webbrowser en de client kan worden gedownload.

Opmerking: Bijvoorbeeld https://asa.test.com. Deze gids gebruikt de tweede methode. Nadat de AC client permanent op de client is geïnstalleerd, start u gewoon de AC client vanaf de applicatie.

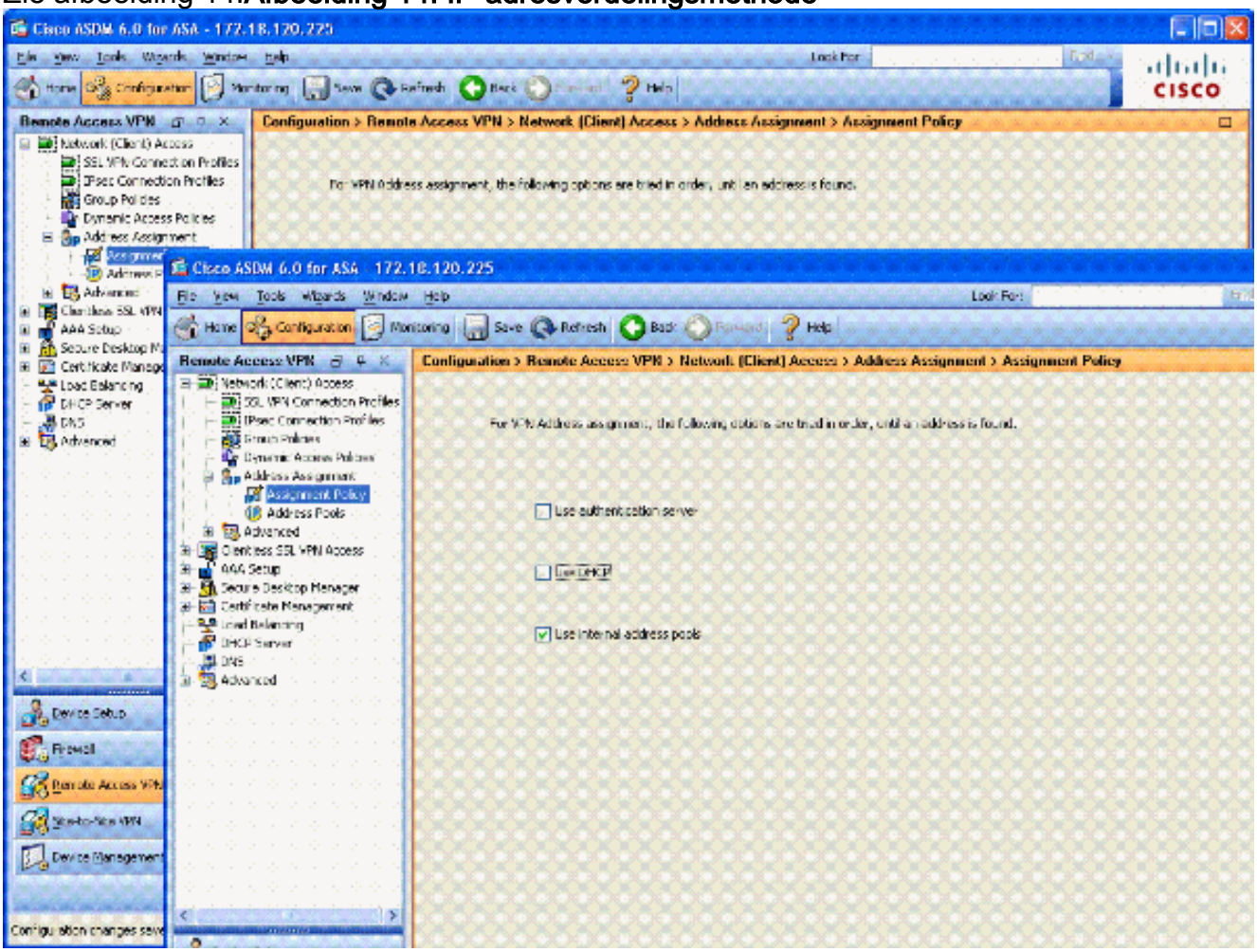
Een IP-adresgroep maken

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

1. Kies **Remote Access VPN > Network (Client) Access > Adres toewijzing > Adres Pools**.
2. Klik op **Toevoegen**.
3. In het venster Pool toevoegen voert u de naam van de IP-pool in, begint en eindigt IP-adres en kiest u een subnetmasker. Zie afbeelding 13.**Afbeelding 13: IP-pool toevoegen**



4. Kies **OK**.
5. Kies **Remote Access VPN > Network (Client) Access > adrestoewijzing > Toekenningsbeleid**.
6. Selecteer de juiste IP-adrestoewijzingsmethode. Deze gids gebruikt de interne adrespools. Zie afbeelding 14.**Afbeelding 14: IP-adresverdelingsmethode**



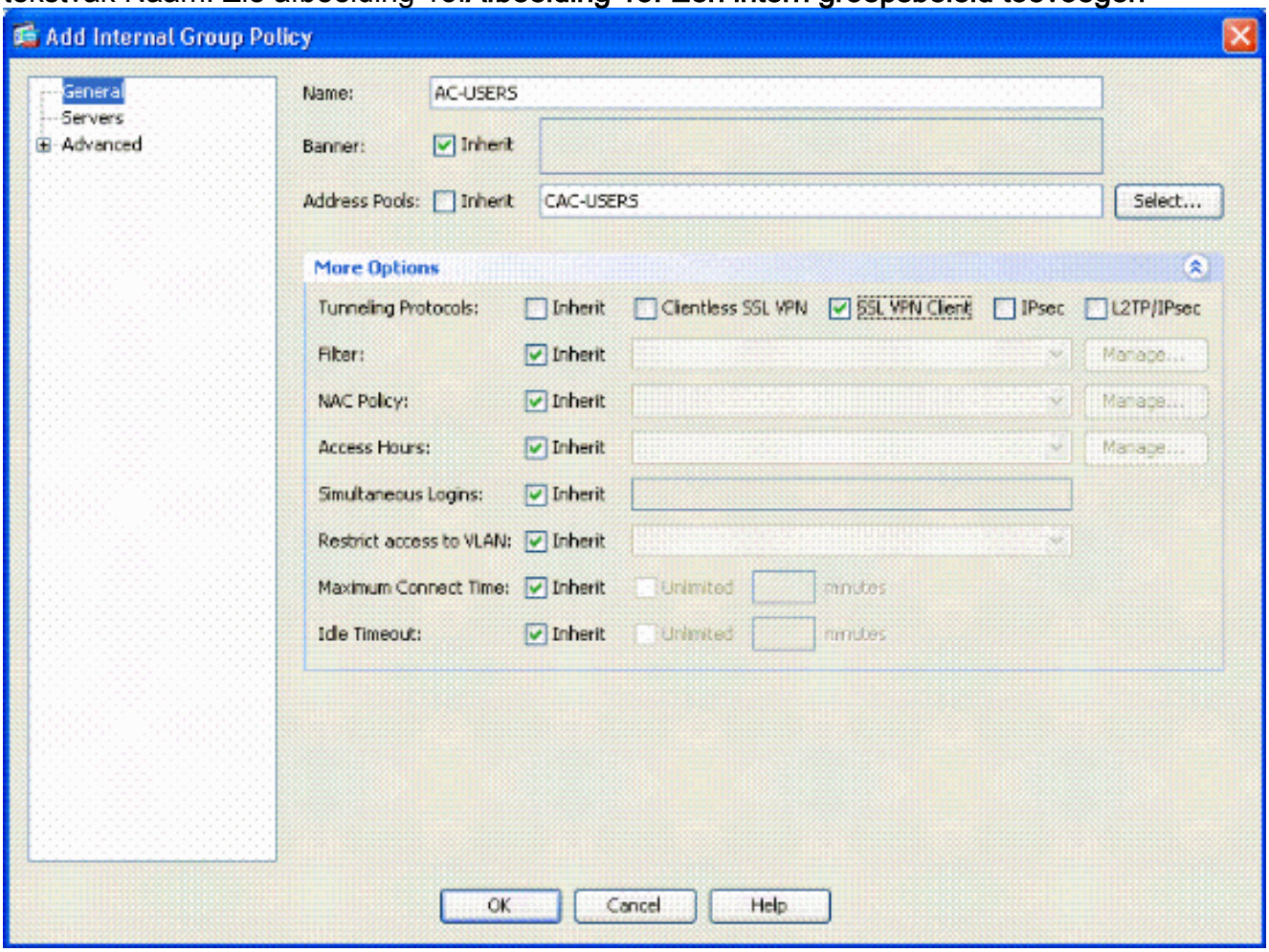
7. Klik op **Toepassen**.

Tunnelgroep en groepsbeleid maken

Groepsbeleid

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

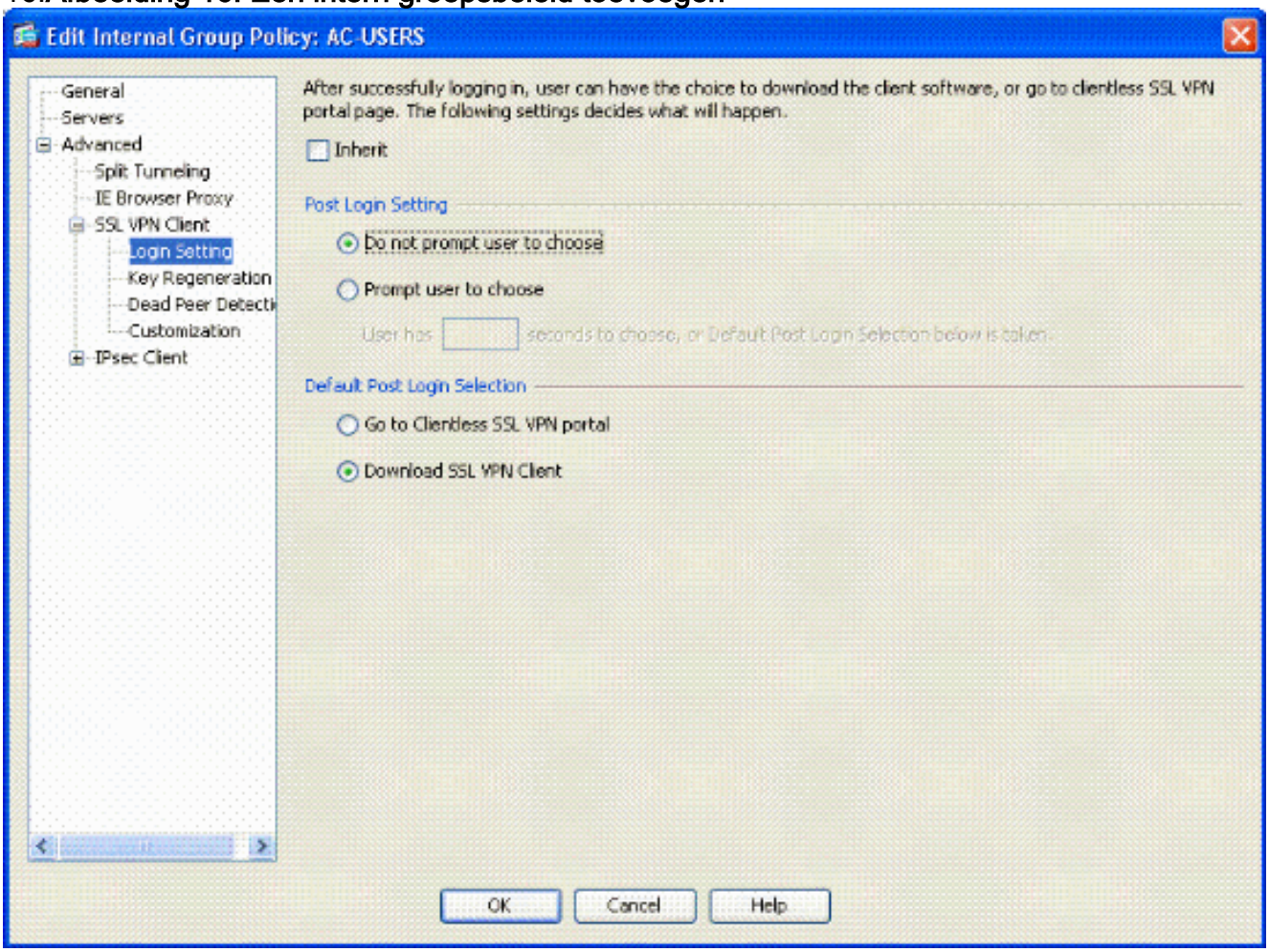
1. Kies **Remote Access VPN -> Netwerktoegang (client) -> Groepsbeleid**.
2. Klik op **Toevoegen** en kies **intern groepsbeleid**.
3. Typ in het venster Intern groepsbeleid toevoegen de naam voor het groepsbeleid in het tekstvak Naam. Zie afbeelding 15.**Afbeelding 15: Een intern groepsbeleid toevoegen**



Kies op het tabblad Algemeen de **SSL VPN-client in de** optie **Tunneling Protocols**, tenzij u andere protocollen zoals Clientless SSL gebruikt.Schakel in het gedeelte servers de optie **erven** uit en voer het IP-adres van DNS- en WINS-servers in. Voer, indien van toepassing, DHCP-bereik in.In het gedeelte servers deselecteert u het aankruisvakje voor **erven** in het standaard domein en voert u de juiste domeinnaam in.In het tabblad Algemeen deselecteert u het aankruisvakje voor **erven** in het gedeelte van de adrespool en voegt u de adrepool toe die in de vorige stap is gemaakt. Als u een andere methode van IP adrestoewijzing gebruikt, laat dit dan om te erven en de aangewezen verandering maken.Alle andere configuratietabbladen moeten standaardinstellingen blijven.**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 om de ASA client naar de gebruiker te laten downloaden wanneer de gebruiker probeert verbinding te maken. Dit voorbeeld toont de laatste methode.

4. Kies vervolgens **Advanced > SSL VPN-client > Aanmelden-instellingen**. Zie afbeelding

16.**Afbeelding 16: Een intern groepsbeleid toevoegen**

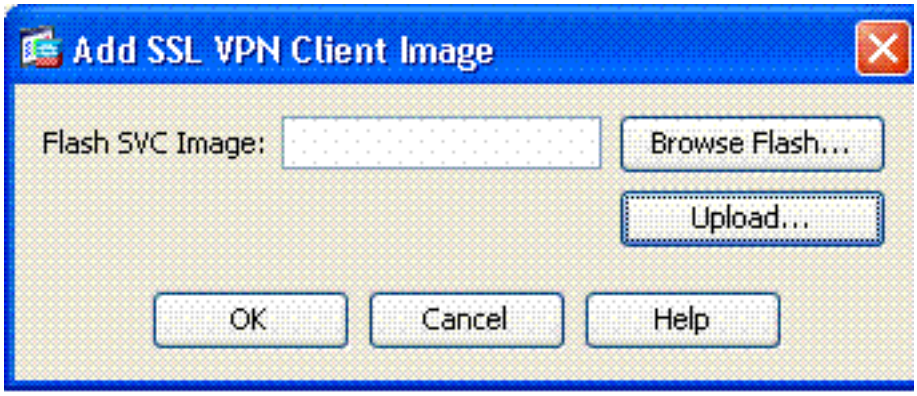


Schakel het selectieteken **Inherit uit**.Kies de juiste POPUT-instelling die bij uw omgeving past.Kies de juiste selectie voor de standaardmelding die bij de omgeving past.Kies **OK**.

Instellingen voor tunnelgroep en -afbeelding

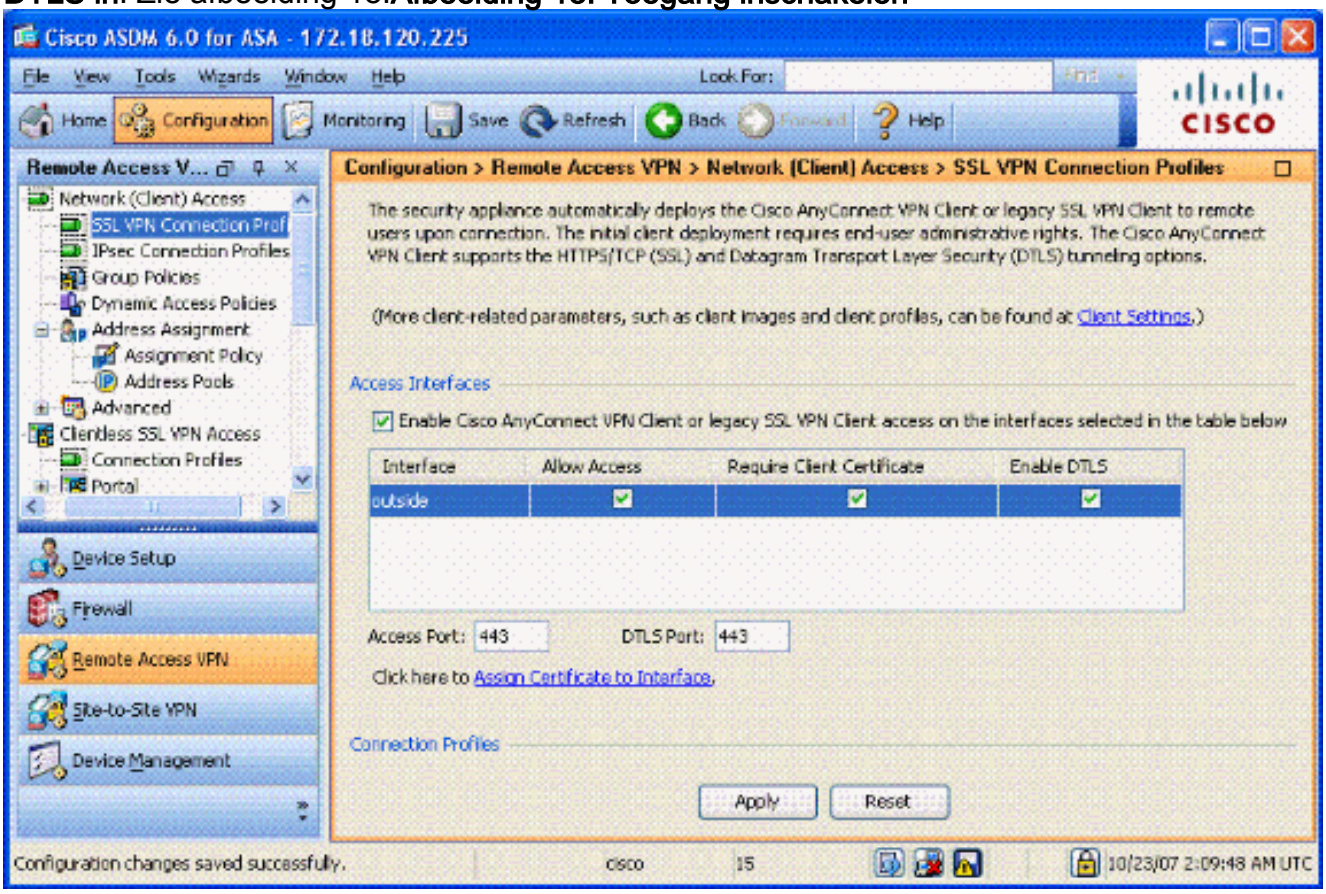
Opmerking: Als u geen nieuwe groep wilt maken, kunt u de standaard ingebouwde groep gebruiken.

1. Kies **Remote Access VPN > Network (Client) Access > SSL VPN-verbindingsprofiel**.
2. Kies **Cisco AnyConnect-client inschakelen.....**.
3. Er verschijnt een dialoogvenster met de vraag `Wilt u een SVC-afbeelding aanwijzen?`
4. Kies **ja**.
5. Als er al een afbeelding is, kies dan de afbeelding die u met Bladeren flitser wilt gebruiken. Als de afbeelding niet beschikbaar is, kiest u **Upload** en vervolgens bladert u naar het bestand op de lokale computer. Zie Afbeelding 17. De bestanden kunnen vanaf Cisco.com worden gedownload. er is een Windows-, MAC- en Linux-bestand.**Afbeelding 17: Voeg SSL**

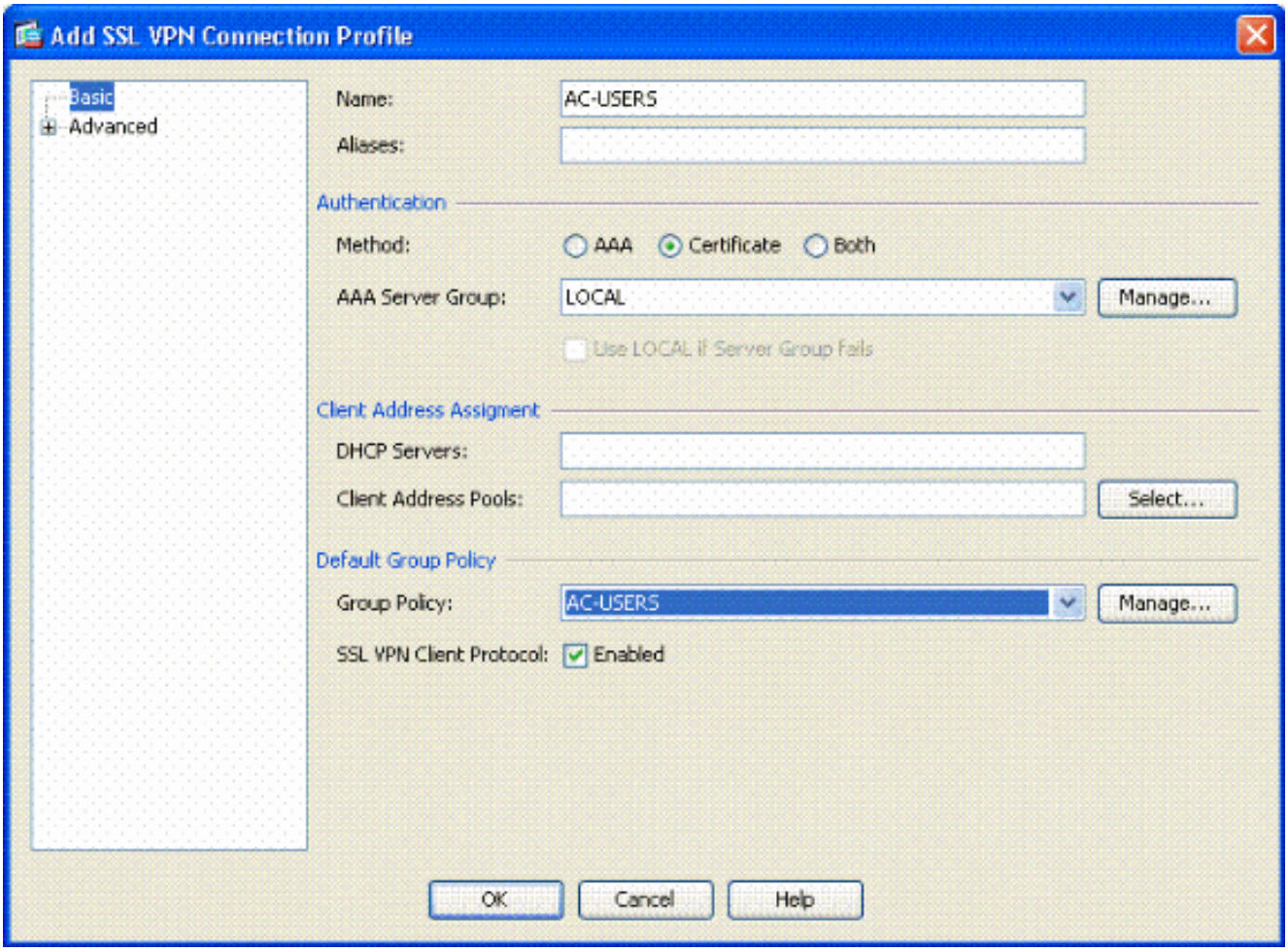


VPN-clientafbeelding toe

6. Vervolgens **toestaan** van **toegang**, **vereist u een clientwaarschuwing** en **schakelt u** optioneel **DTLS in**. Zie afbeelding 18.**Afbeelding 18: Toegang inschakelen**

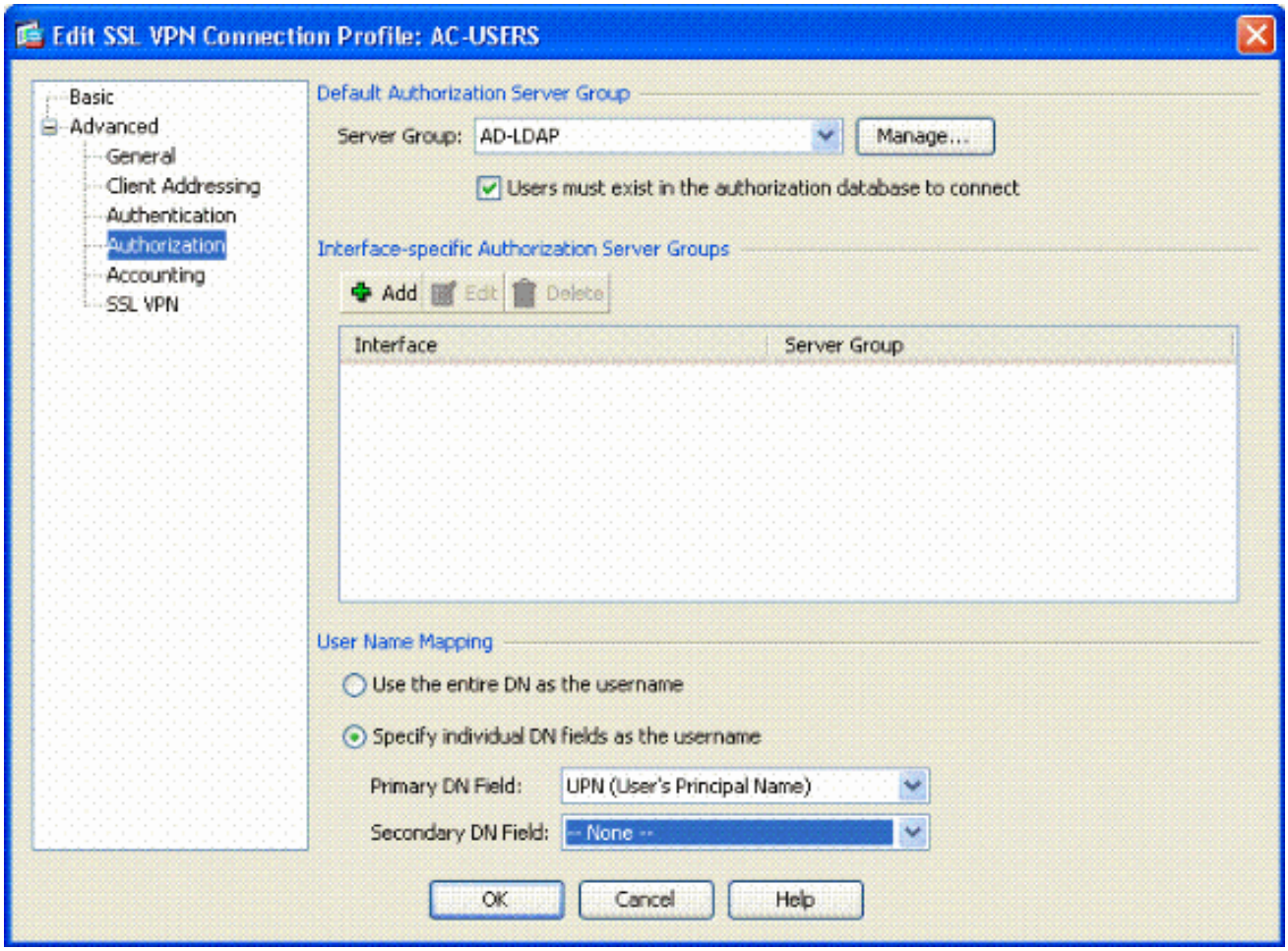


7. Klik op **Toepassen**.
8. Maak vervolgens een Connection Profile/Tunnel Group. Kies **Remote Access VPN > Network (Client) Access > SSL VPN-verbindingsprofiel**.
9. Klik in het gedeelte verbindingsprofielen op **Toevoegen**.**Afbeelding 19: verbindingsprofiel toevoegen**



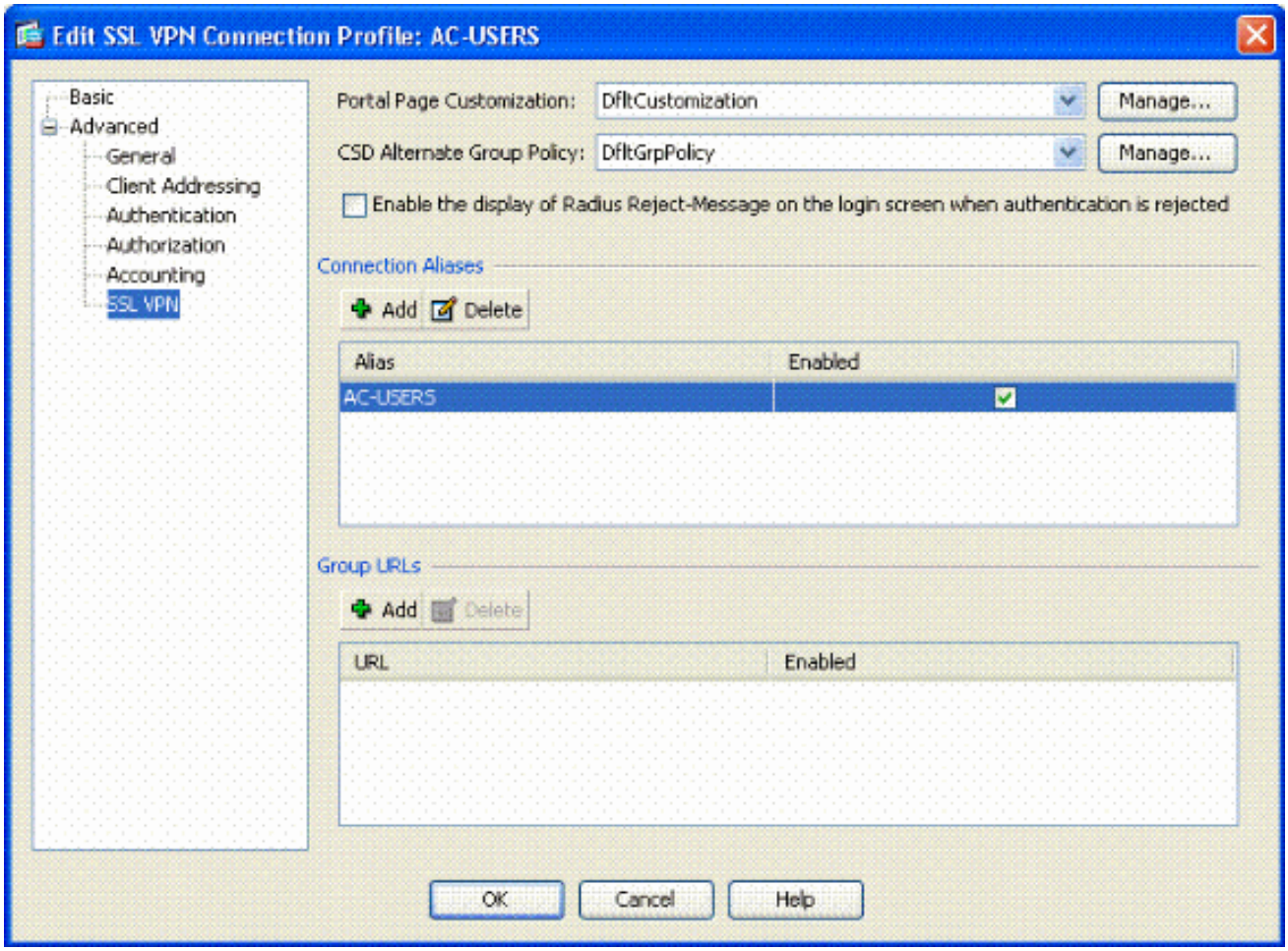
Geef de groep een naam.Kies **Certificaat** in de authenticatiemethode.Kies het groepsbeleid dat eerder is gemaakt.Zorg ervoor dat **SSL VPN-client** is ingeschakeld.Laat standaard andere opties staan.

10. **Kies** vervolgens **Advanced > Authorization**. Zie afbeelding 20**Afbeelding 20: Authorization**



Kies de AD-LDAP groep die eerder is gemaakt.Controleer of **gebruikers moeten bestaan... om verbinding te maken.**In de mapping velden kiest u **UPN** voor de primaire en **geen** voor de secundaire optie.

11. Kies het **SSL VPN-**gedeelte van het menu.
12. Voltooi de volgende stappen in het gedeelte Connection-alias:**Afbeelding 21: Connection-alias**



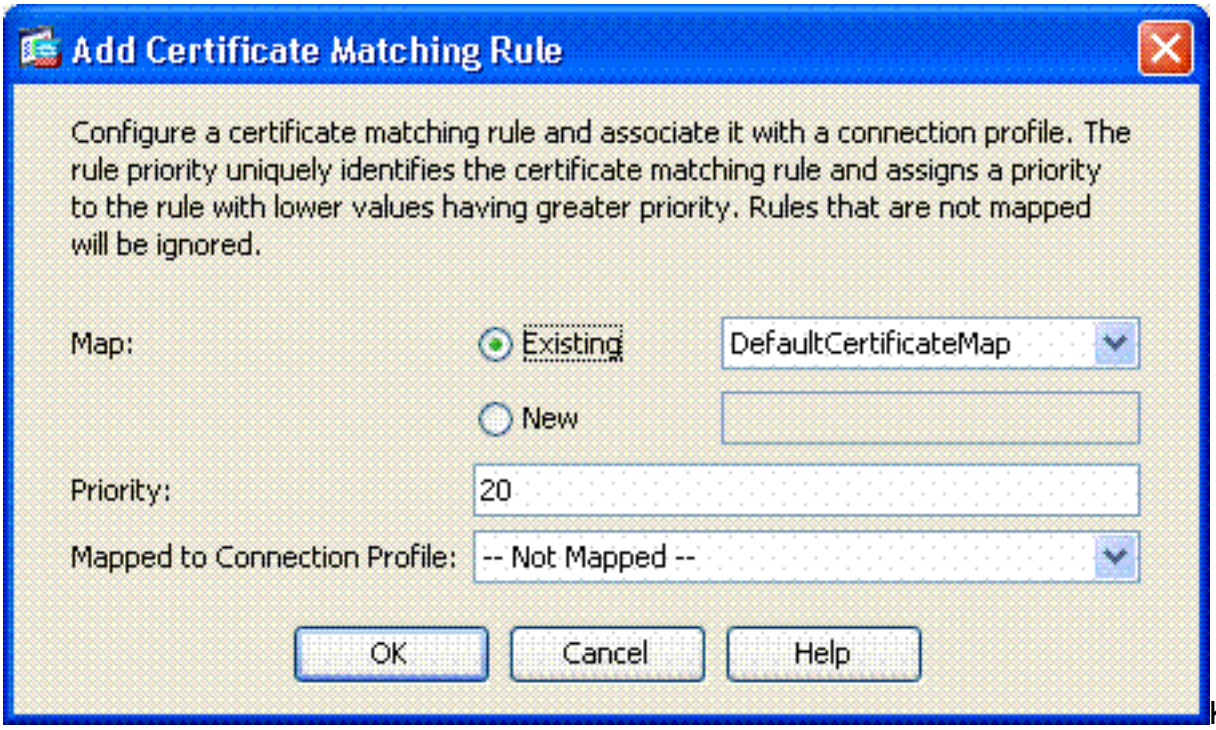
Kies **Toevoegen**.Voer de groepsalias in die u wilt gebruiken.Zorg ervoor dat **deze** ingeschakeld is. Zie afbeelding 21.

13. Klik op **OK**.

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

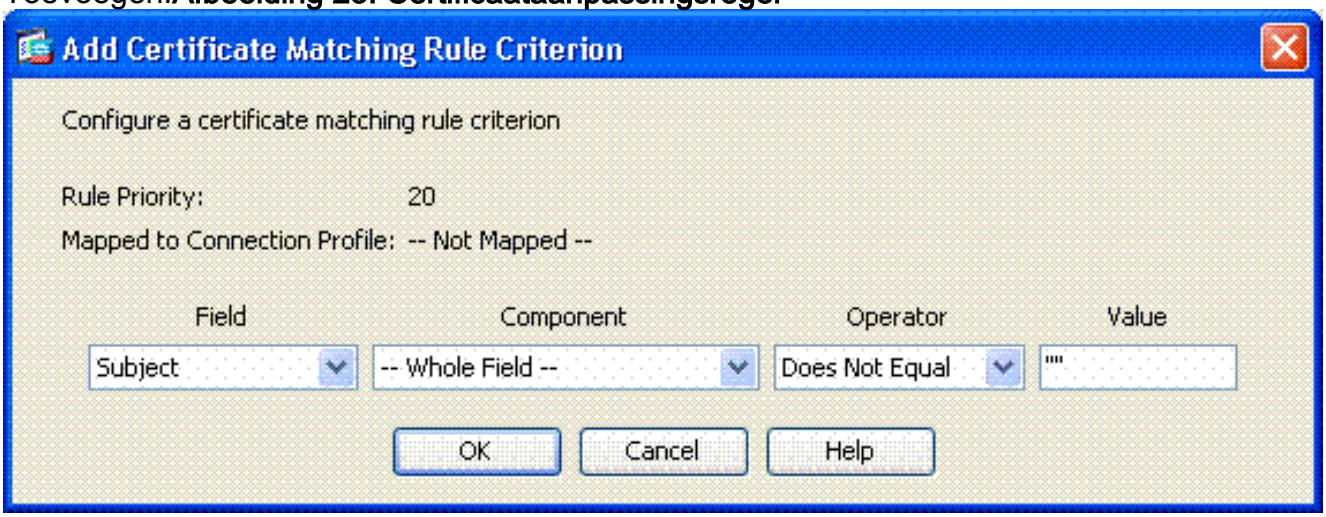
Overeenkomende regels van het certificaat (als OCSP wordt gebruikt)

1. Kies **Remote Access VPN > Geavanceerd > Document to SSL VPN Connection Profile Maps**. Zie afbeelding 22.Kies **Toevoegen** in het vak Certificaat aan verbindingsprofiel.U kunt de bestaande kaart als Defaultcertificaatkaart in het kaartgedeelte behouden of een nieuwe kaart maken als u al bepaalde kaarten voor IPsec gebruikt.Hou de regel prioriteit.Onder in kaart gebracht groep, verlaat als **— niet in kaart gebracht —**. Zie afbeelding 22.**Afbeelding 22: Aangepaste certificaatregel toevoegen**



Klik op **OK**.

2. Klik op **Toevoegen** in de onderste tabel.
3. Voltooi de volgende stappen in het venster Criterium van de aanpassingsregel Toevoegen:**Afbeelding 23: Certificaataanpassingsregel**



Bewaar de veldkolom aan **Onderwerp**.Bewaar de kolom voor de component in **het hele veld**.Verander de kolom van de operator om **niet gelijk te maken**.Voer in de kolom Waarde twee dubbele quotes in **""**.Klik op **OK** en **Toepassen**. Zie bijvoorbeeld afbeelding 23.

OCSP configureren

De configuratie van een OCSP kan variëren en is afhankelijk van de OCSP-responderverkoper. Lees de handleiding van de map voor meer informatie.

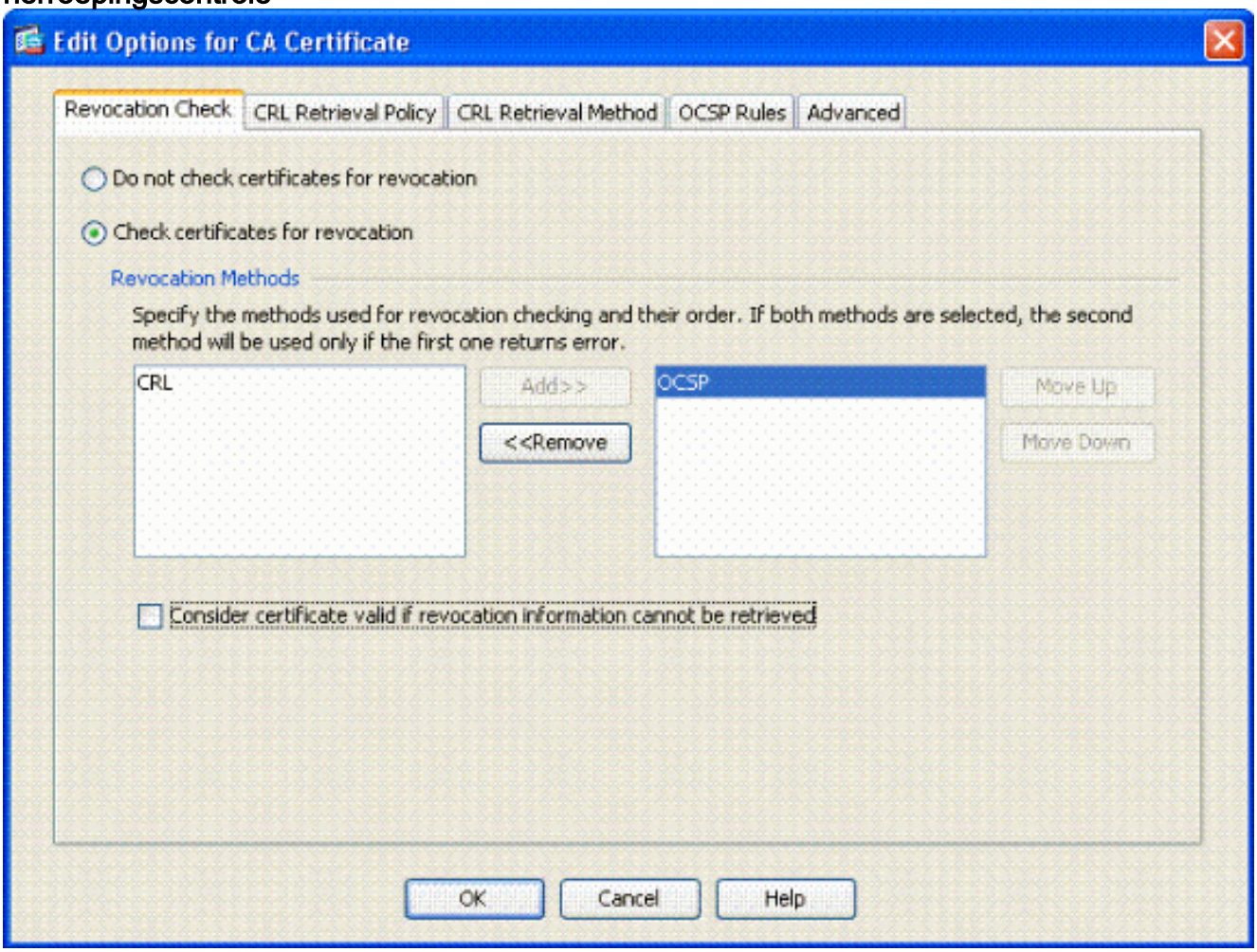
OCSP-reservecertificaat configureren

1. Verkrijg een zelf-gegenereerd certificaat van de OCSP responder.
2. Voltooi de eerder genoemde procedures en installeer een certificaat voor de OSCP server.**Opmerking:** Zorg ervoor dat **Niet-controleren of de certificaten voor herroeping** zijn

geselecteerd voor 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 om te configureren om OCSP te gebruiken.
3. Klik op **Bewerken**.
4. Controleer of **het certificaat voor herroeping** is gecontroleerd.
5. Voeg in het gedeelte Herroeping Methods **OCSP** toe. Zie afbeelding 24.**OCSP-herroepingscontrole**



6. Zorg ervoor dat **certificaat geldig is...niet kan worden opgehaald** als u strikte OCSP-controles wilt uitvoeren.

Opmerking: Configuratie/bewerking alle CA-server die OCSP voor herroeping gebruikt.

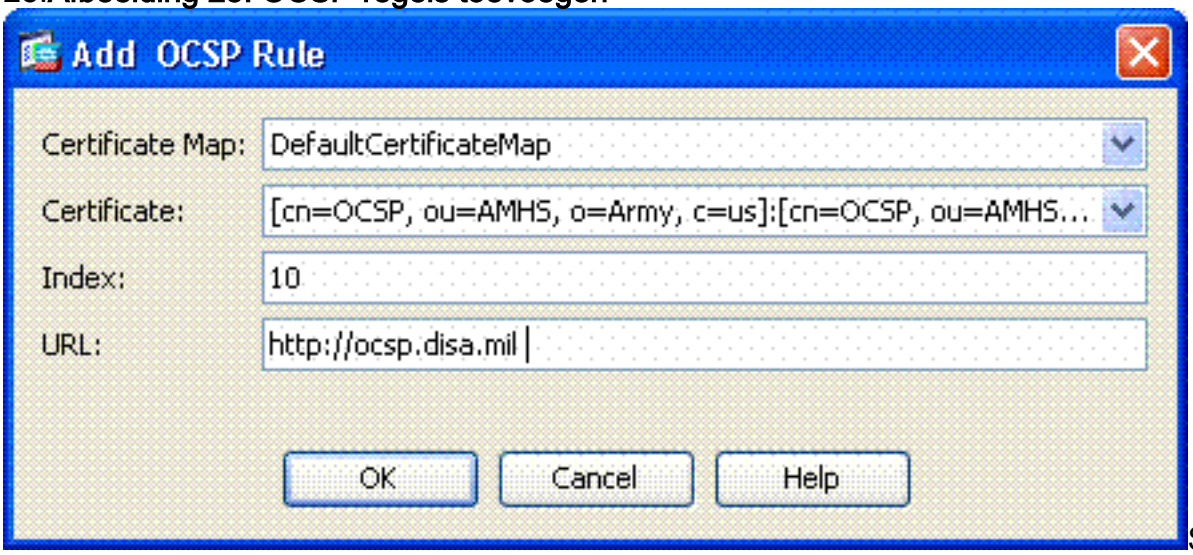
OCSP-regels configureren

Opmerking: Controleer dat er een beleid voor overeenkomende certificaten en de OCSP-responder zijn ingesteld voordat u deze stappen uitvoert.

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

1. Kies **Remote Access VPN> certificaatbeheer > CA-certificaten 2**.
2. Markeer een OCSP om een CA te kiezen om te configureren om OCSP te gebruiken.
3. Kies **Bewerken**.

4. Klik op het tabblad **OCSP Rule**.
5. Klik op **Toevoegen**.
6. Voltooi de volgende stappen in het venster OCSP-regel toevoegen. Zie afbeelding 25.**Afbeelding 25: OCSP-regels toevoegen**



Selecteer in de optie certificaatkaart de optie **Defaultcertificaatkaart** of een kaart die u eerder hebt gemaakt.Selecteer in de optie Certificaat de optie **OCSP-responder**.Voer in de indexoptie **10 in**.Voer in de URL optie het IP-adres of de hostnaam van de OCSP-responder in. Als u de hostname gebruikt, zorg er dan voor dat de DNS-server op ASA is geconfigureerd.Klik op **OK**.Klik op **Toepassen**.

Cisco AnyConnect-clientconfiguratie

Deze sectie betreft 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 werden getest.

Opmerking: deze handleiding gebruikt de groepsmodus voor alleen eerste AC-client installeren. Nadat de AC-client is geïnstalleerd, start u de AC-toepassing net als de IPsec-client.

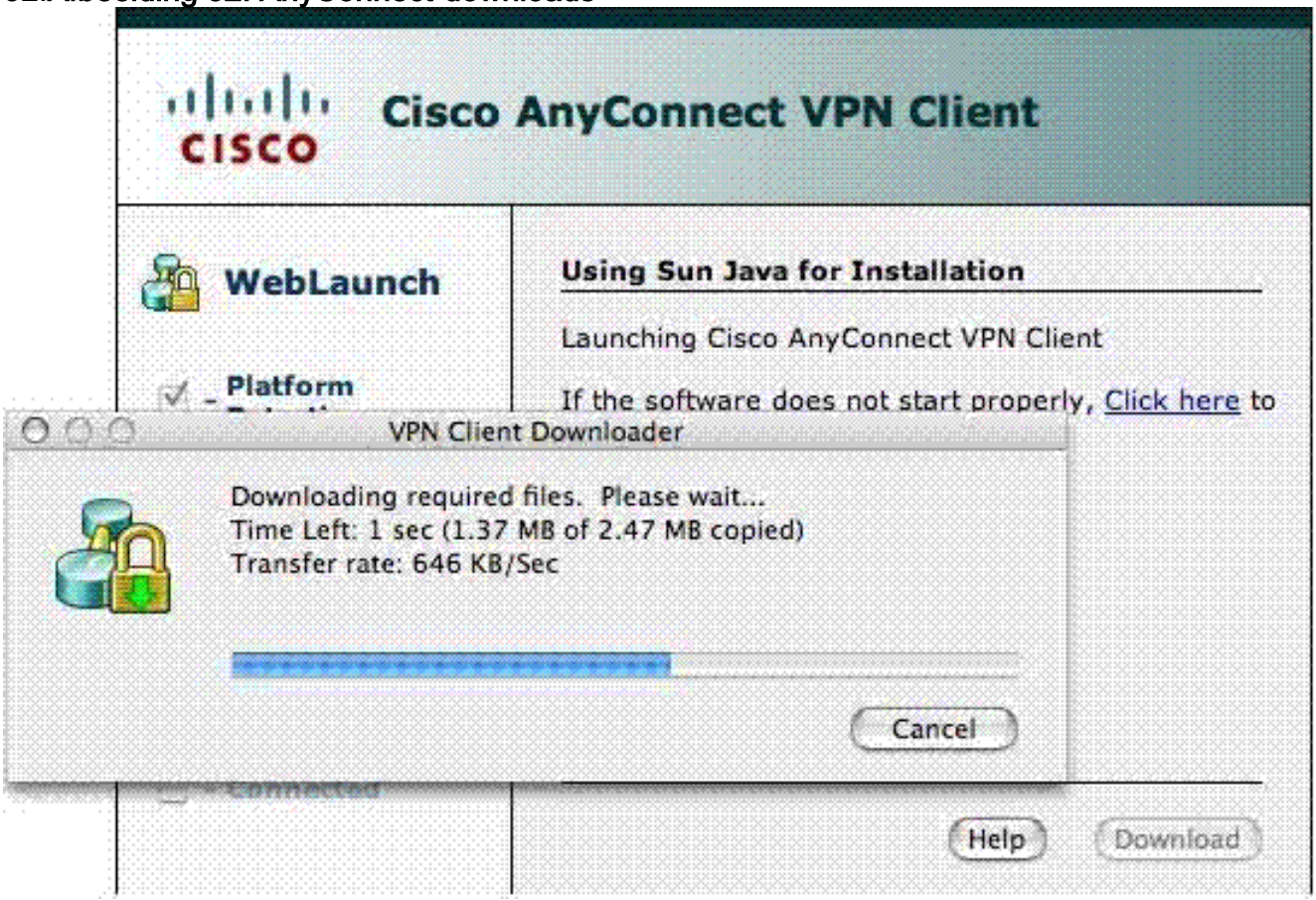
N.B.: De DOD-certificeringsketen moet op de lokale machine worden geïnstalleerd. Raadpleeg de PKI POC om de certificaten/het batchbestand te verkrijgen.

Opmerking: het kaartlezer stuurprogramma voor MAC OSX is al geïnstalleerd en compatibel met de huidige OS-versie die u gebruikt.

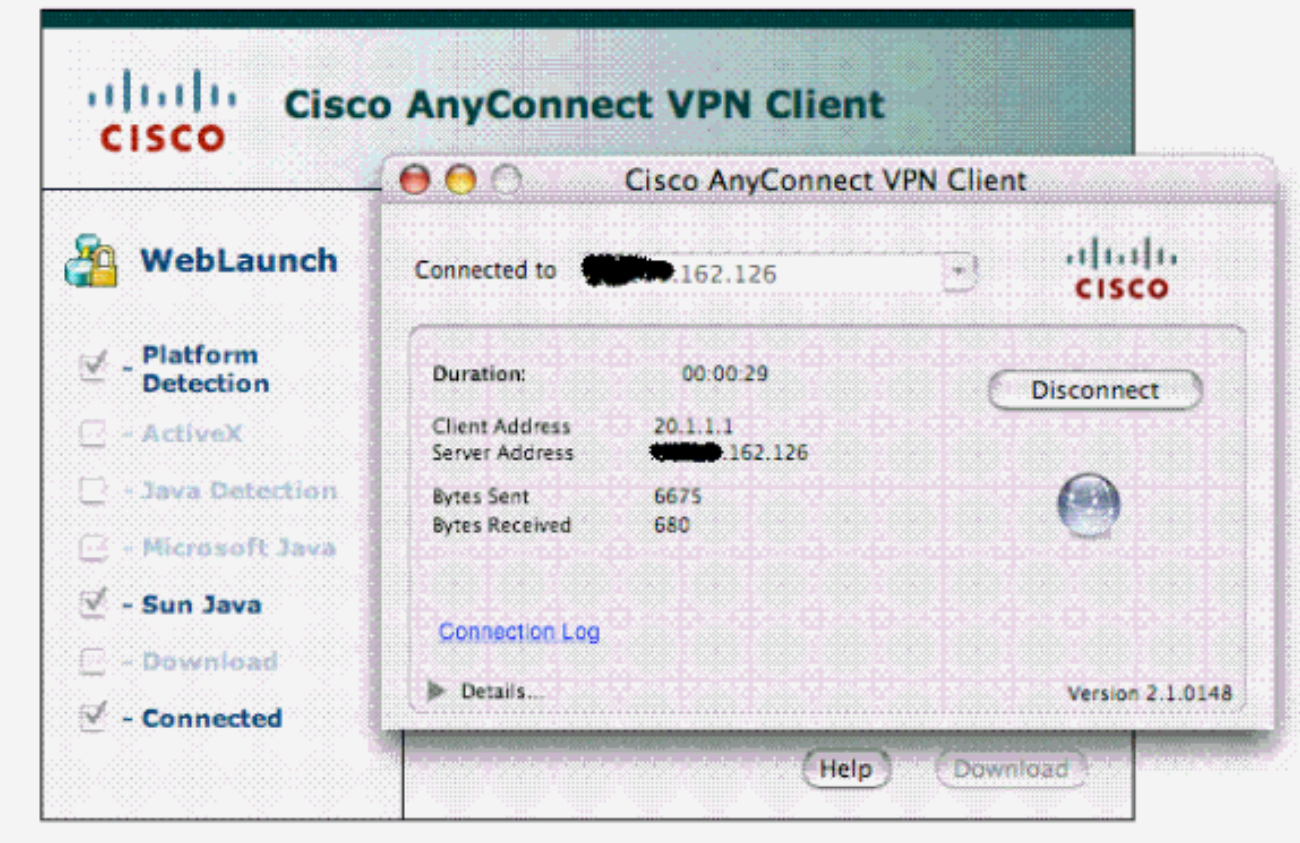
Cisco AnyConnect VPN-client - Mac OS X downloaden

1. Start een websessie naar de ASA met Safari. Het adres moet in het formaat van https://Outside-Interface liggen. Bijvoorbeeld https://172.18.120.225.
2. Een pop-upvenster vraagt om het certificaat van de ASA te controleren. Klik op **Doorgaan**.
3. Er verschijnt een ander pop-upvenster om de CAC-sleutelketen te ontgrendelen. Geef het pinnummer op. Zie afbeelding 31.**Afbeelding 31: PIN invoeren**

4. Klik nadat de SSL VPN-service webpagina verschijnt op **Doorgaan**.
5. Nadat u de sleutelketting hebt ontgrendeld, vraagt de browser u of u het certificaat van de ASA vertrouwt. Klik op **vertrouwen**.
6. Voer het basiswachtwoord in om de sleutelketting te ontgrendelen om een beveiligde verbinding op te zetten en klik vervolgens op **OK**.
7. Kies het certificaat dat u wilt gebruiken voor verificatie van de client en klik vervolgens op **OK**.
8. Vervolgens vraagt de browser om het root/user wachtwoord zodat AnyConnect-klanten kunnen worden gedownload.
9. Als echt gemaakt is, begint de AnyConnect-client te downloaden. Zie afbeelding 32.**Afbeelding 32: AnyConnect-downloads**



10. Nadat de toepassing is gedownload, vraagt de browser u om het ASA certificaat te aanvaarden. Klik op **Aanvaarden**.
11. Verbinding wordt gemaakt. Afbeelding 33.**Afbeelding 33:AnyConnect verbonden**



Start Cisco AnyConnect VPN-client - Mac OS X

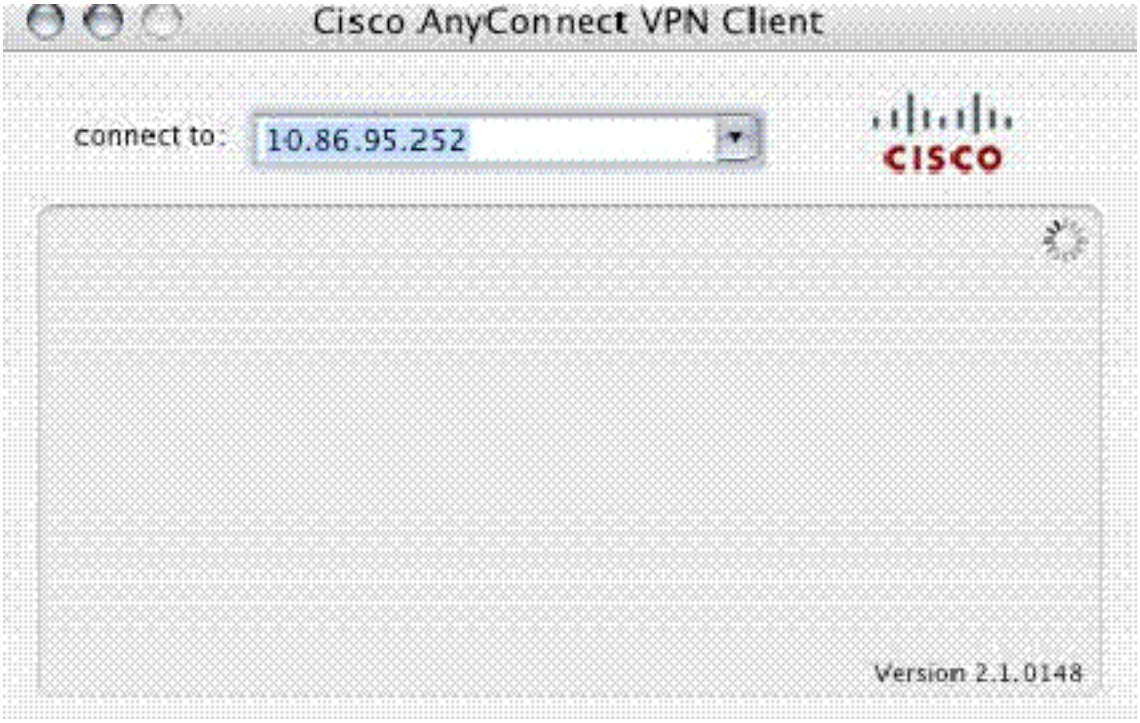
Van vinder—**toepassingen > Cisco AnyConnect VPN-client**

Opmerking: Zie Bijlage E voor de optionele AnyConnect-clientconfiguratie.

Nieuwe verbinding

Het AC-venster verschijnt. Zie afbeelding 37.

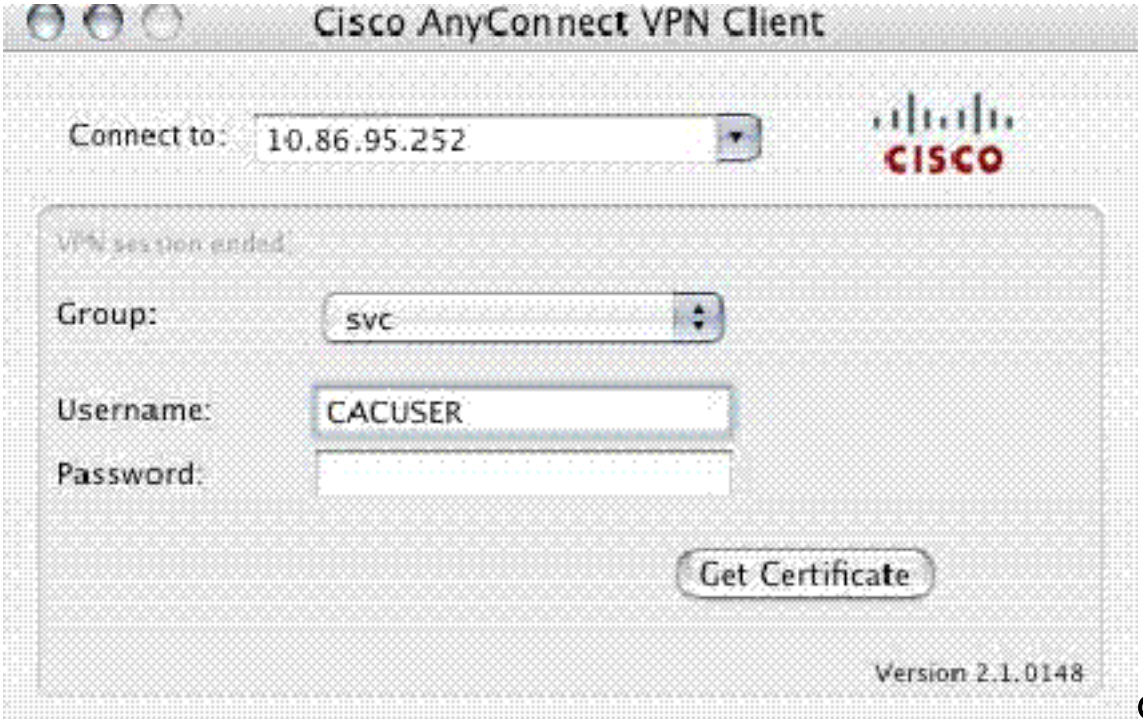
Afbeelding 37: Nieuwe VPN-verbinding



1. Kies de juiste host als AC de verbinding niet automatisch probeert.
2. Voer uw PIN in wanneer dit wordt gevraagd. Zie afbeelding 38.**Afbeelding 38: PIN invoeren**

Externe toegang starten

1. Kies de groep en de host waartoe u wilt verbinding maken.
2. Aangezien certificaten worden gebruikt, kiest u **Connect** om VPN op te zetten. Zie afbeelding 39.**Opmerking:** Aangezien de verbinding certificaten gebruikt, hoeft u geen gebruikersnaam en wachtwoord in te voeren.**Afbeelding 39: Aansluiten**



Opmerking: Zie Bijlage E voor de optionele AnyConnect-clientconfiguratie.

Bijlage A - Toewijzing en DAP van de LDAP

In ASA/PIX release 7.1(x) en later werd een functie geïntroduceerd die LDAP mapping heet. Dit is een krachtige functie die een mapping biedt tussen een Cisco-eigenschap en LDAP-objecten/eigenschappen, die de noodzaak van een wijziging van het Ldap-schema negeren. Voor de implementatie van CAC-authenticatie kan dit extra beleidshandhaving op afstandstoegangsverbinding ondersteunen. Dit zijn voorbeelden van LDAP mapping. Let erop dat u beheerderrechten nodig hebt om wijzigingen aan te brengen in de AD/LDAP server. In ASA 8.x-software werd de Dynamic Access Policy (DAP) optie geïntroduceerd. DAP kan in combinatie met CAC werken om naar meerdere AD-groepen te kijken en beleid, ACL's enzovoort te duwen.

Scenario 1: Handhaving van actieve map met behulp van inbel voor externe toegang - Toegang toestaan/weigeren

Dit voorbeeld brengt de AD-eigenschap msNPAlowDailin in kaart met Cisco's attribuut cVPN3000-Tunneling-Protocol.

- De AD-waarde: TRUE = staat toe; FALSE = Denken
- Cisco attributiewaarde: 1 = FALSE, 4 (IPSec) of 20 (4 IPSEC + 16 WebVPN) = TRUE,

Voor ALLOW conditie, kaart u in:

- TRUE = 20

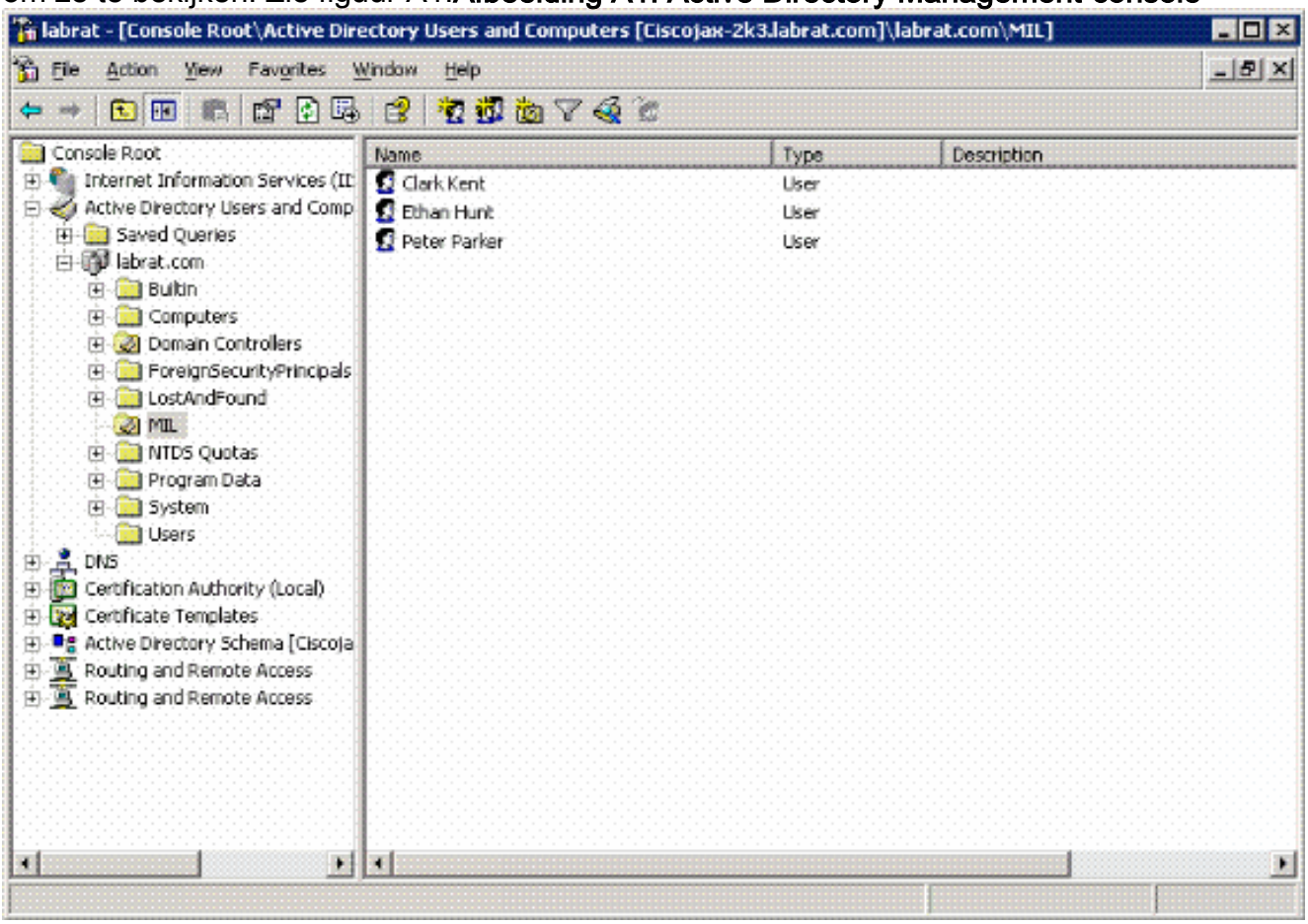
Voor de inbelmodus DENY kunt u in kaart brengen:

- FALSE = 1

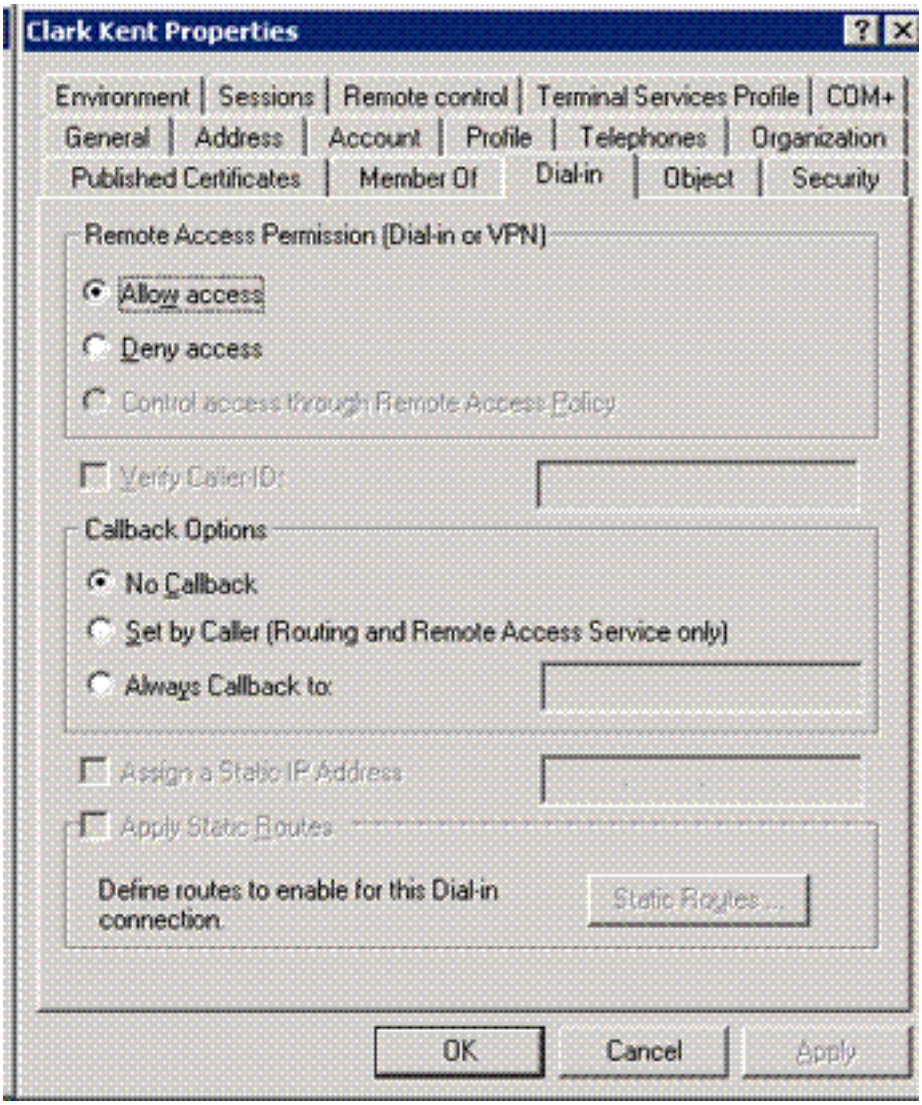
Opmerking: Zorg dat TRUE en FALSE in alle zakken staan. Zie Een externe server configureren voor security applicatie, autorisatie voor meer informatie.

Actief directory instellen

1. Klik in de Active Directory Server op **Start > Run**.
2. Typ vervolgens **in** het tekstvak Open **dsa.msc** en klik op **OK**. Dit start de actieve directory management console.
3. In de Active Directory Management console klikt u op het plusteken om de actieve gebruikers en computers uit te vouwen.
4. Klik op het plusteken om de domeinnaam uit te vouwen.
5. Als u een OU hebt die voor uw gebruikers is gemaakt, vouwt u de OU uit om alle gebruikers te bekijken. als u alle gebruikers hebt toegewezen in de gebruikersmap, vouwt u die map uit om ze te bekijken. Zie figuur A1.**Afbeelding A1: Active Directory Management-console**



6. Dubbelklik op de gebruiker die u wilt bewerken.Klik op het tabblad Inbellen in de pagina met gebruikerseigenschappen en klik op **Toestaan** of **ontkennen**. Zie figuur A2.**Afbeelding A2:**

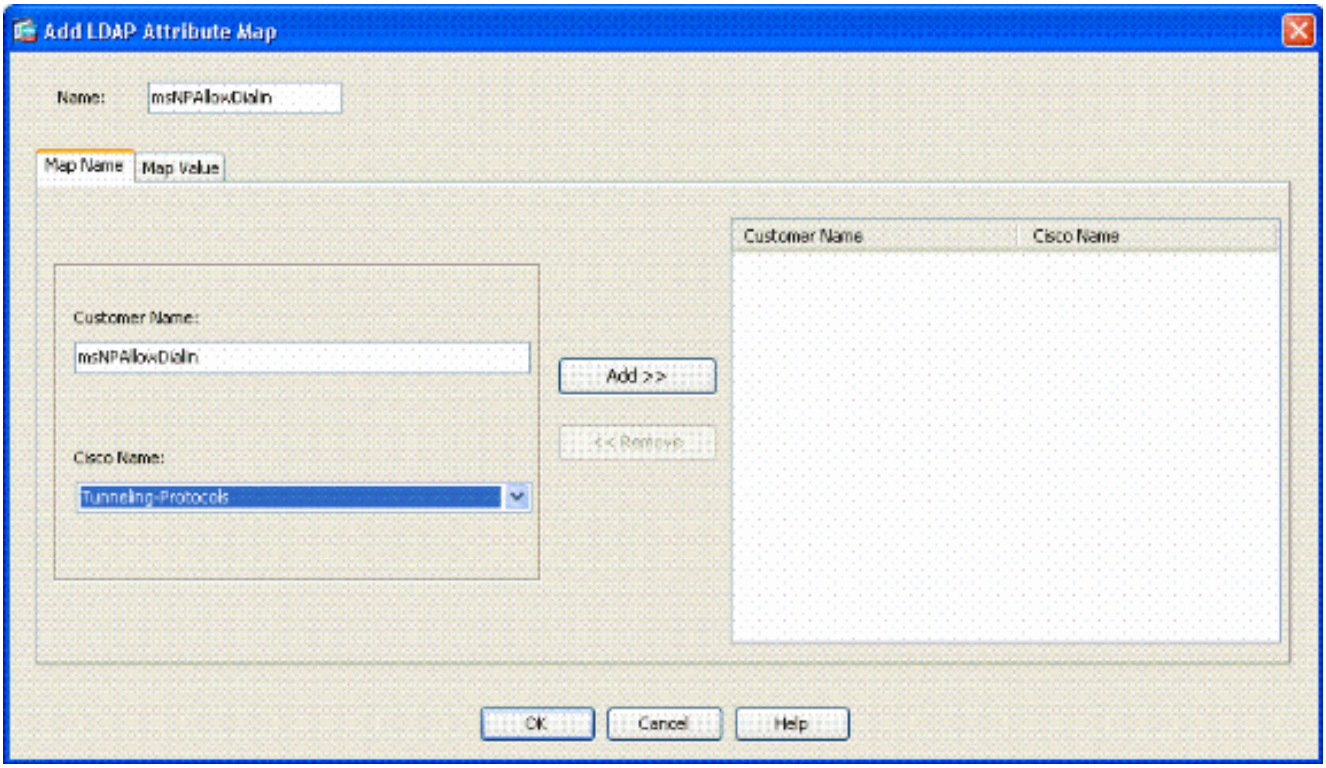


Gebruikerspatronen

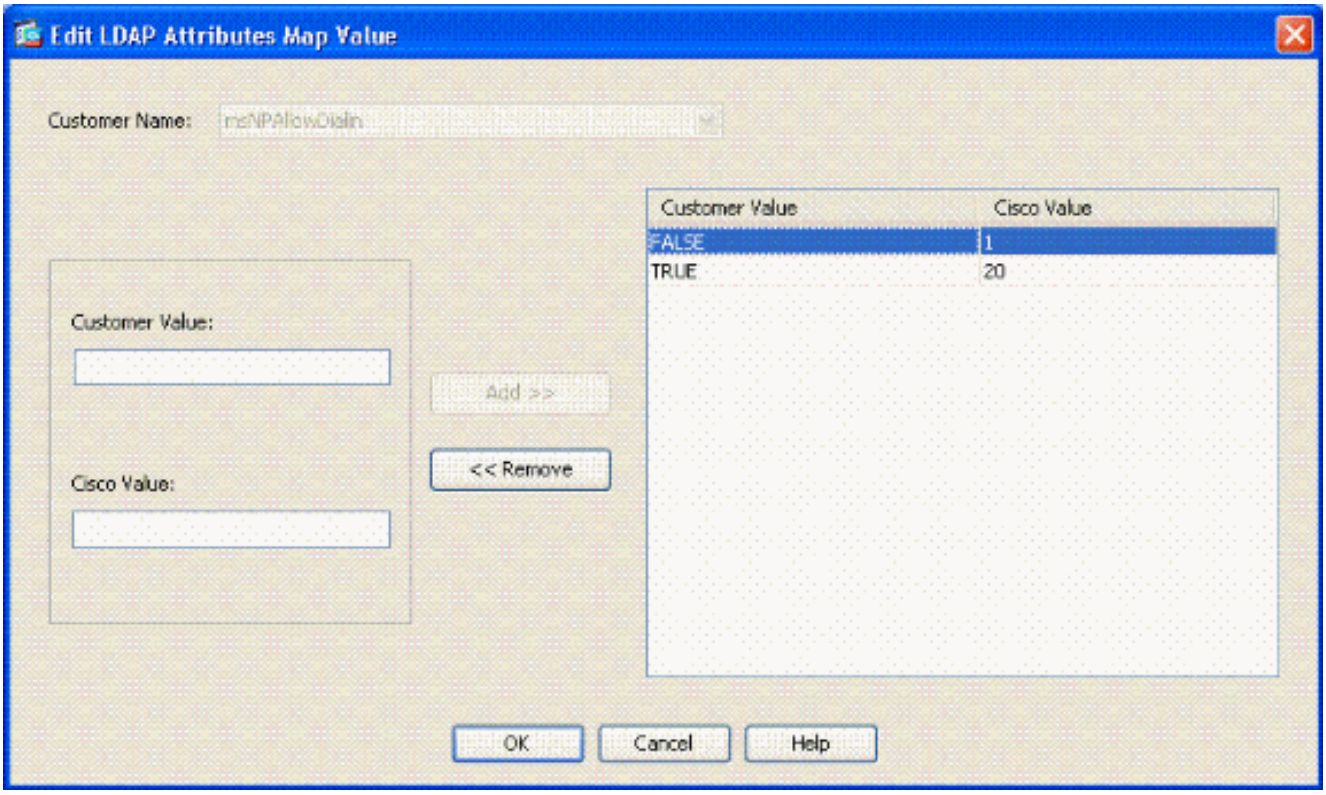
7. Klik vervolgens op **OK**.

ASA-configuratie

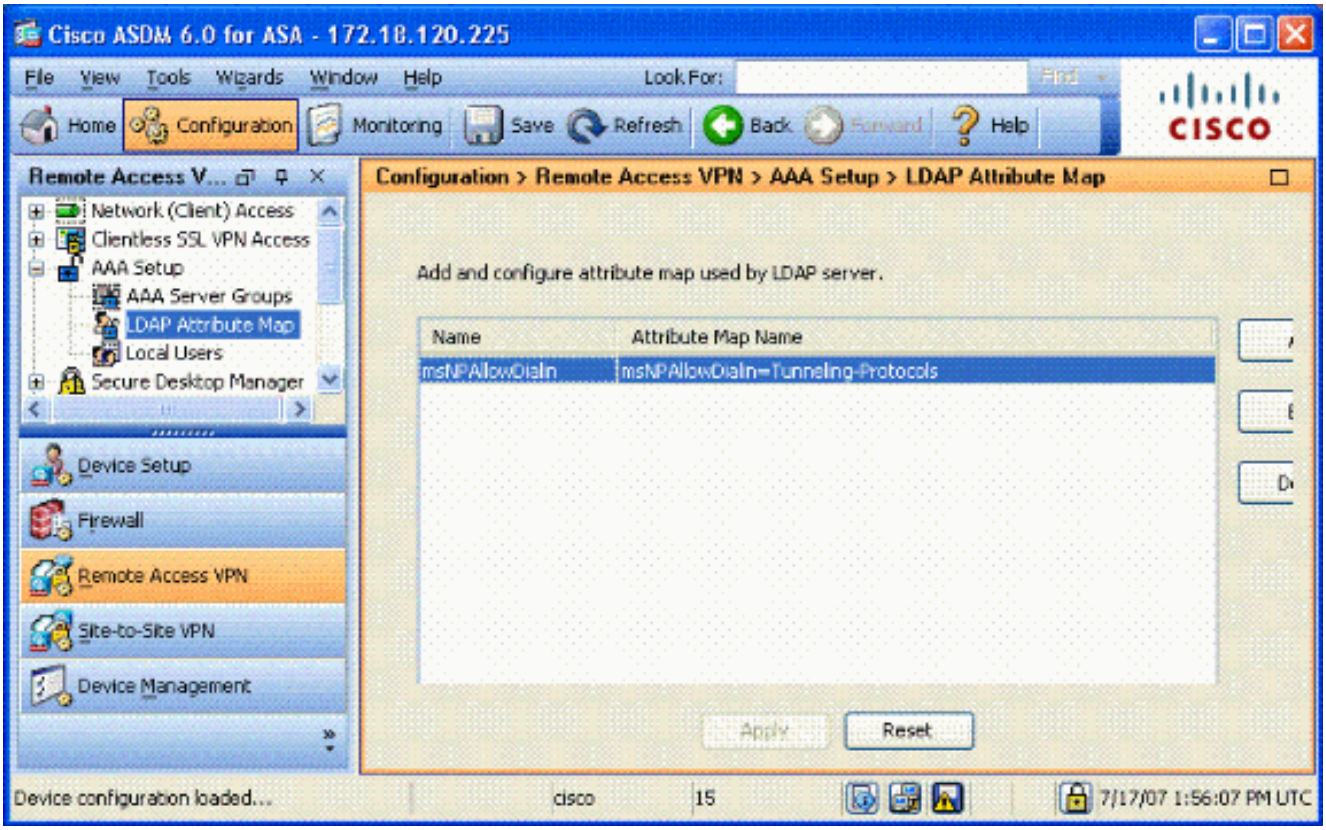
1. Kies in ASDM de optie **Remote Access VPN> AAA-instelling > Ldap-kenmerk**.
2. Klik op **Toevoegen**.
3. Voltooi de volgende stappen in het venster Tekstkenmerken toevoegen. Zie figuur A3.**Afbeelding A3: Toevoegen van LPDP-kenmerk**



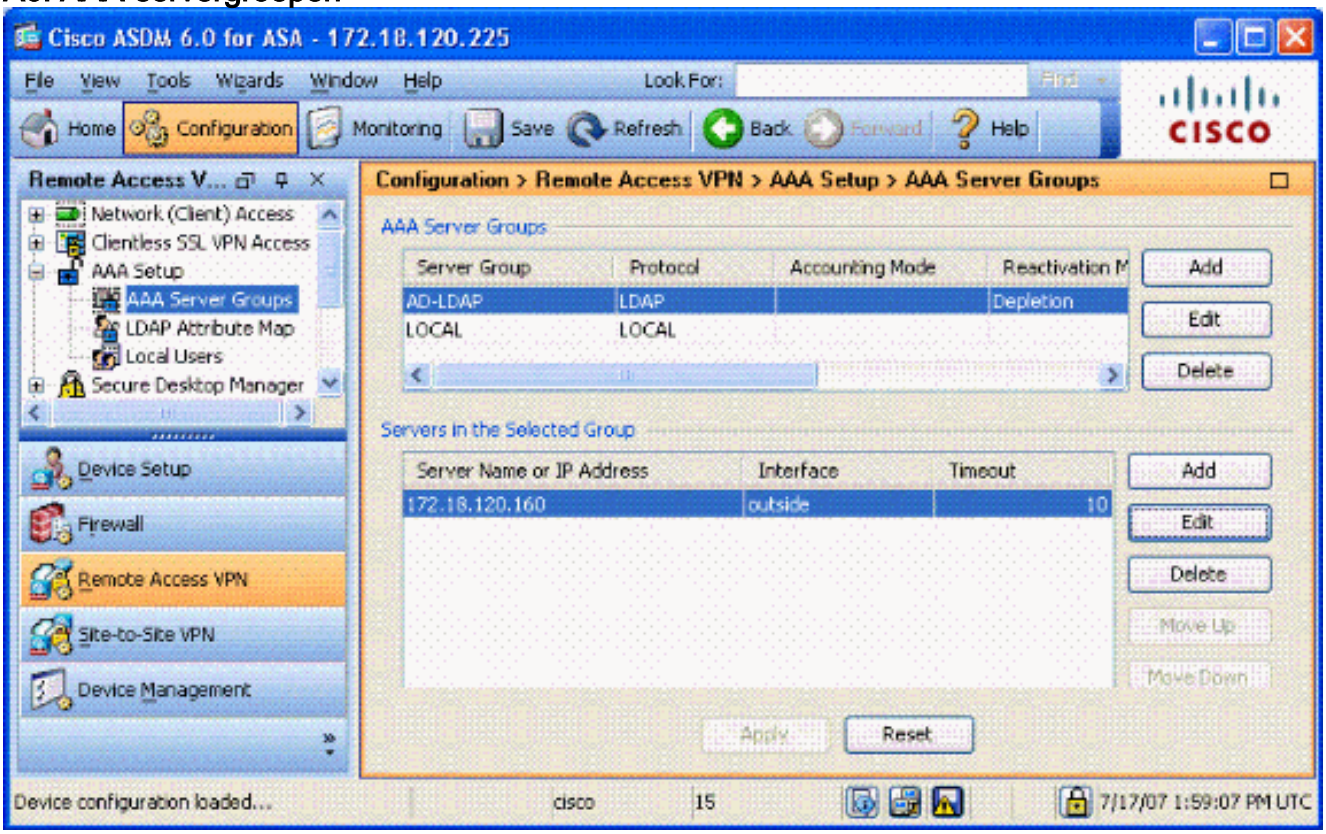
Typ een naam in het Tekstvak Naam.Typ in het tabblad Naam map **de** optie **msNPAlow** in het tekstvak Naam van de klant.Selecteer in het tabblad Map Name de optie **Tunneling-Protocols** in de vervolgkeuzelijst in de Cisco Name.Klik op **Toevoegen**.Kies het tabblad **Map Waarde**.Klik op **Toevoegen**.Typ in het venster Waarde van kenmerk LDAP de optie **TRUE** in het tekstvak Naam van de klant en type **20** in het tekstvak Cisco Value.Klik op **Toevoegen**.Typ **FALSE** in het tekstvak Naam van de klant en type **1** in het tekstvak Cisco Waarde. Zie figuur
A4.



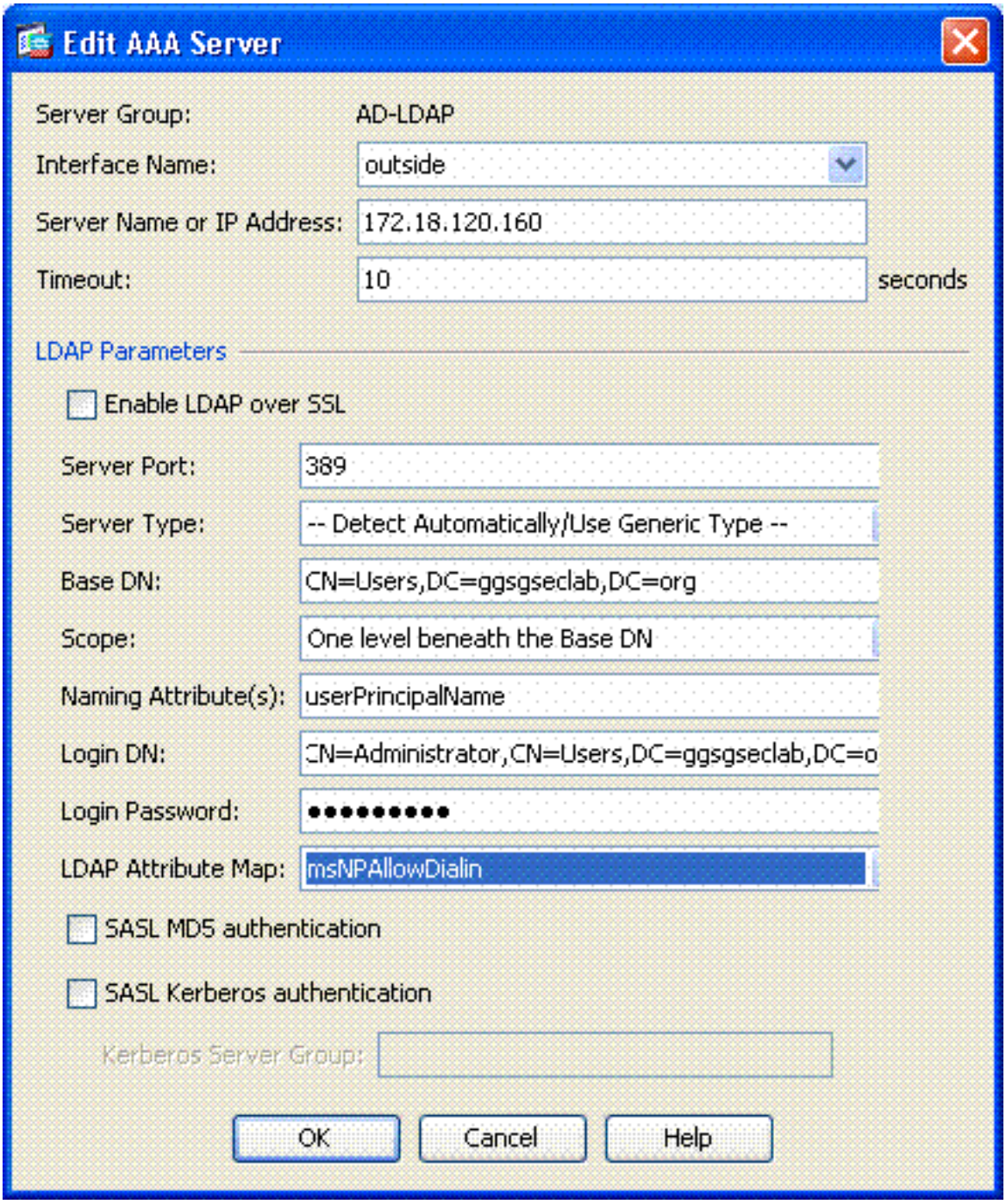
Klik op **OK**.Klik op **OK**.Klik op **Toepassen**.De configuratie dient op afbeelding A5 te lijken.**Afbeelding A5: Configuratie van LDP-kenmerken**



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 de sectie Geselecteerde groep het IP-adres van de server of de hostnaam en klik vervolgens op **Bewerken**.
6. Selecteer in het venster AAA-server bewerken in het tekstvak Map van LPDP-kenmerken de LMOP-attributenkaart die in het vervolgkeuzemenu is gemaakt. Zie figuur A7**Afbeelding A7: Toevoegen van LPDP-kenmerk**



7. Klik op **OK**.

Opmerking: Schakel de functie voor het foutoptreden van de LDAP in terwijl u test om na te gaan of de functie voor het koppelen van de LMBP goed werkt. Zie Bijlage C voor opdrachten voor het oplossen van problemen.

Scenario 2: Handhaving van actieve map met groepslidmaatschap om toegang toe te staan/te weigeren

In dit voorbeeld wordt gebruik gemaakt van de LMBP-eigenschap lidOf om in kaart te brengen aan de eigenschap Tunneling Protocol om een groepslidmaatschap als voorwaarde vast te stellen. Om dit beleid te laten werken, moet je aan de volgende voorwaarden voldoen:

- Gebruik een groep die reeds bestaat of een nieuwe groep voor ASA VPN-gebruikers maakt om lid van te zijn voor ALLOW-voorwaarden.
- Gebruik een groep die reeds bestaat of een nieuwe groep voor niet ASA gebruikers om lid

van voor de voorwaarden van DENY te zijn.
- Controleer in de LDAP-viewer of u de goede DNA voor de groep hebt. Zie appendix D. Als de DN fout is, werkt de mapping niet goed.

Opmerking: Let erop dat de ASA alleen de eerste string van het lidOf attribuut in deze release kan lezen. Zorg ervoor dat de nieuwe groep bovenaan de lijst staat. De andere optie is om een speciaal teken voor de naam te plaatsen aangezien AD speciale tekens eerst bekijkt. Om rond dit voorbehoud te werken, gebruik DAP in 8.x software om naar meerdere groepen te kijken.

Opmerking: Zorg ervoor dat een gebruiker deel uitmaakt van de ontkenningsgroep of ten minste één andere groep, zodat het lidOf altijd wordt teruggestuurd naar de ASA. U hoeft de FALSE-ontkenningsvoorwaarde niet te specificeren, maar de beste praktijk is dit te doen. Als de bestaande groepsnaam of de groepsnaam een ruimte bevat, geeft u de eigenschap dan op:

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

Opmerking: DAP biedt de ASA de mogelijkheid om meerdere groepen in het lidOf toe te wijzen en de basisautorisatie van de groepen te onderzoeken. Zie de DAP sectie.

MAPPEN

- De AD-waarde:lid van CN=ASAUsers,CN=Gebruikers,DC=ggsgseclab,DC=orglid van CN=TelnetClients,CN=Gebruikers,DC=labrat,DC=com
- Cisco attributiewaarde: 1 = FALSE, 20 = TRUE,

Voor **ALLOW**-conditie:

- lid van CN=ASAUsers,CN=Gebruikers,DC=ggsgseclab,DC=org= 20

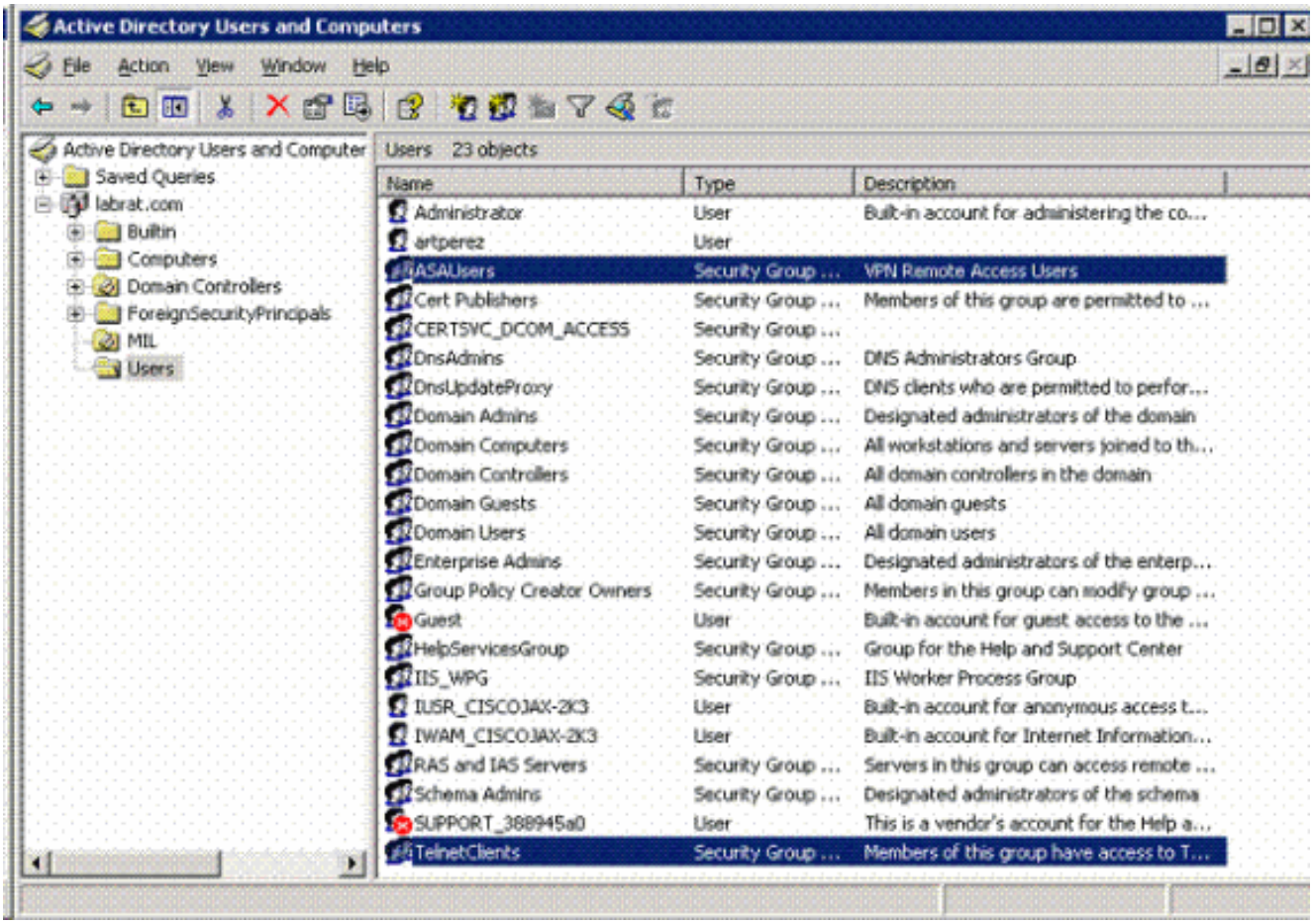
Voor de toestand van de **DICHTHEID**, kaart u:

- lid van CN=TelnetClients,CN=Gebruikers,DC=ggsgseclab,DC=org = 1

Opmerking: In future release is er een Cisco-eigenschap om verbinding toe te staan en te ontkennen. Raadpleeg Een externe server configureren voor security applicatie, gebruikersautorisatie voor meer informatie over Cisco-eigenschappen.

Actief directory instellen

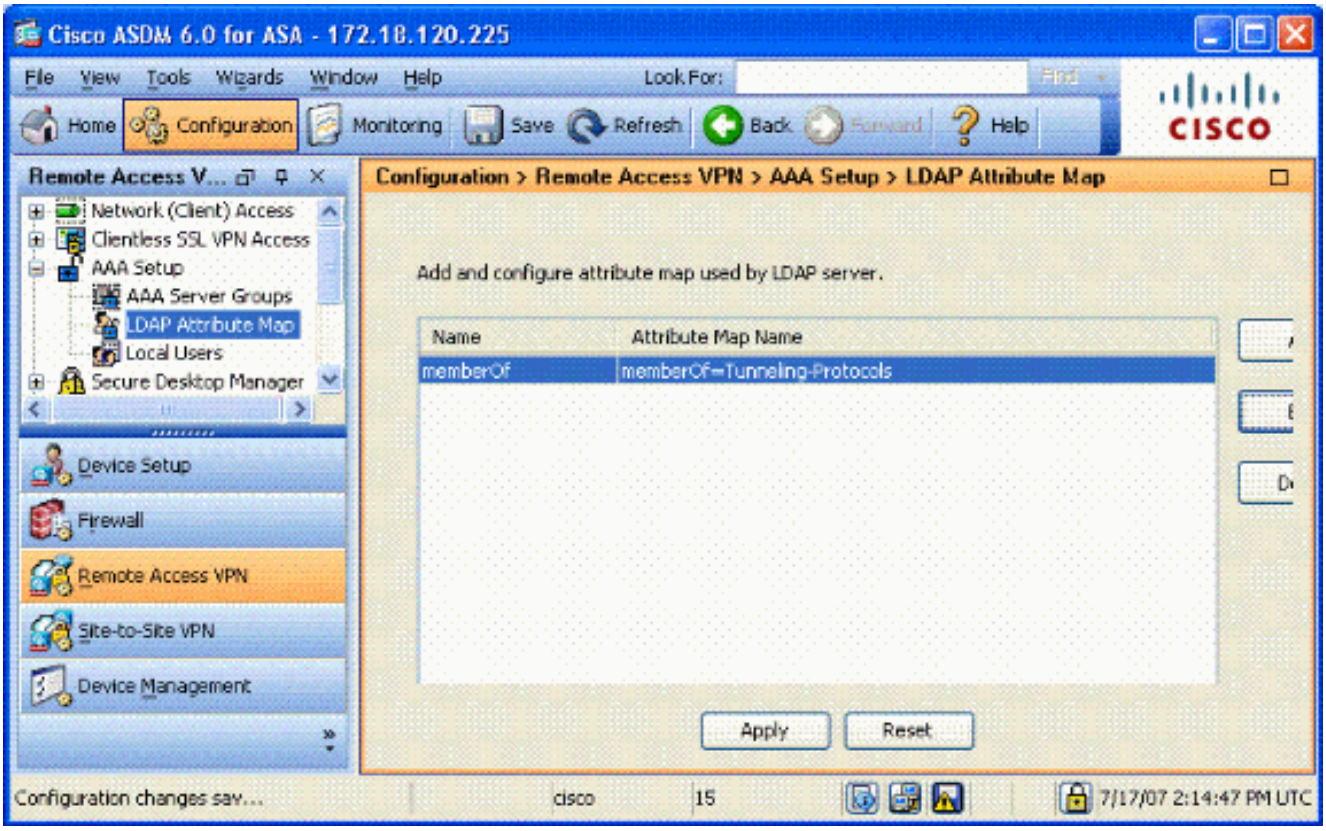
1. Kies **Start > Start** in de Active Directory Server.
2. Typ in het tekstvak Open **dsa.msc** en klik vervolgens op **OK**. Dit start de actieve directory management console.
3. In de Active Directory Management console klikt u op het plusteken om de actieve gebruikers en computers uit te vouwen. Zie figuur A8**Afbeelding A8: Actieve Map-groepen**



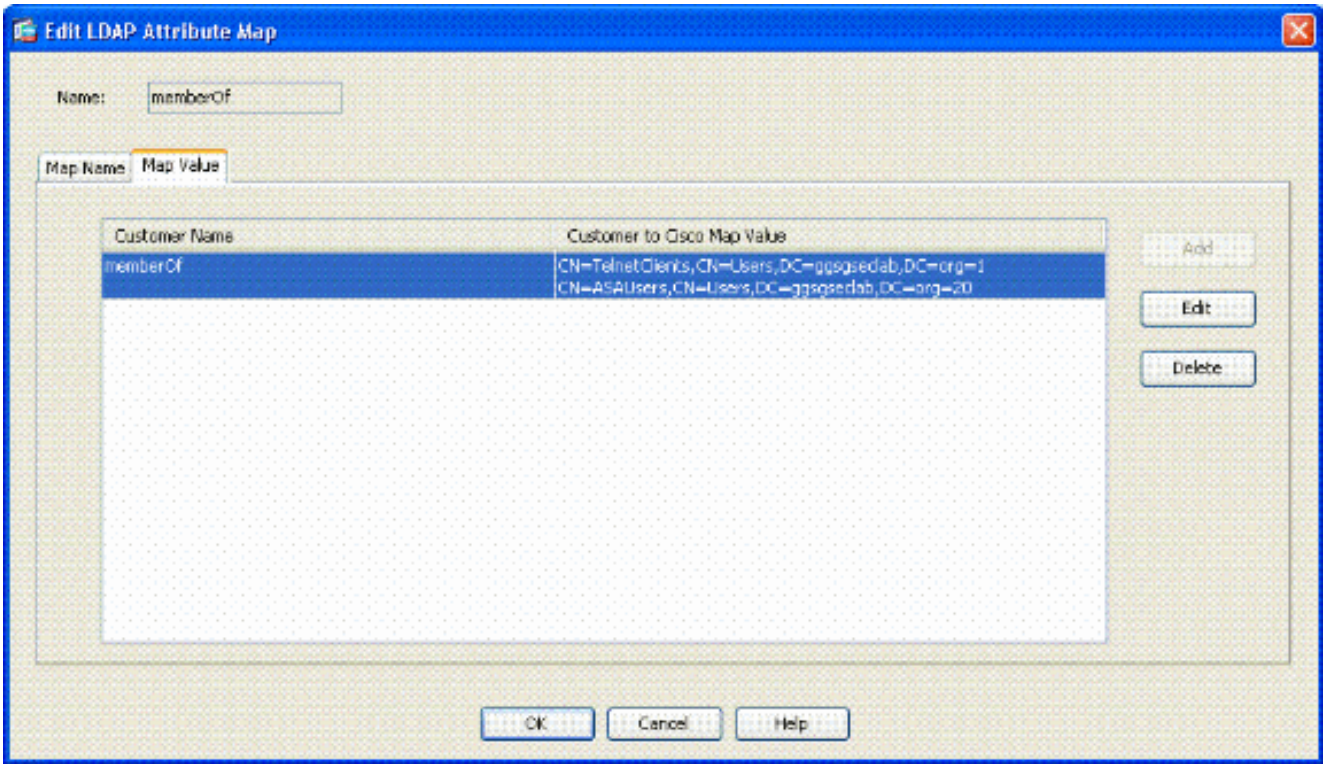
4. Klik op het plusteken om de domeinnaam uit te vouwen.
5. Klik met de rechtermuisknop op de map **Gebruikers** en kies **Nieuw > Groep**.
6. Voer een groepsnaam in. Bijvoorbeeld: ASAUsers.
7. Klik op **OK**.
8. Klik op de map **Gebruikers** en dubbelklik op in de groep die u zojuist hebt gemaakt.
9. 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 de optie **Remote Access VPN > AAA-instelling > Ldap-kenmerk**.
2. Klik op **Toevoegen**.
3. Voltooi de volgende stappen in het venster Tekstkenmerken toevoegen. Zie figuur A3.Typ een naam in het Tekstvak Naam.Typ **lid van** de **map** in het tekstvak **Naam** van de klant c. in het tabblad Map Name.Selecteer in het tabblad Map Name de optie **Tunneling-Protocols** in de vervolgkeuzelijst in de Cisco Name.Kies **Toevoegen**.Klik op het tabblad **Map Value**.Kies **Toevoegen**.In het venster Waarde van de Kaart van Toevoegingskenmerk LDAP, type **CN=ASAUsers,CN=Gebruikers, DC=ggsgseclab,DC=org** in het tekstvak Naam van de klant en type **20** in het tekstvak Cisco Value.Klik op **Toevoegen**.Type **CN=TelnetClients, CN=Gebruikers, DC=ggsgseclab,DC=org** in het tekstvak Naam van de klant en type **1** in het tekstvak Cisco Value. Zie figuur A4.Klik op **OK**.Klik op **OK**.Klik op **Toepassen**.De configuratie zou op figuur A9 moeten lijken.**Afbeelding A9 Ldap-kenmerk**



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



6. Selecteer in het Tekstvenster AAA-server bewerken in het Tekstvenster van LDAP-kenmerken de LDAP-attributenkaart die in het vervolgkeuzemenu is gemaakt.
7. Klik op **OK**.

Opmerking: Schakel de functie voor het fouilleren van LDAP in terwijl u test om de binding van LDAP te controleren en om de karakterisering goed te controleren. Zie Bijlage C voor opdrachten voor het oplossen van problemen.

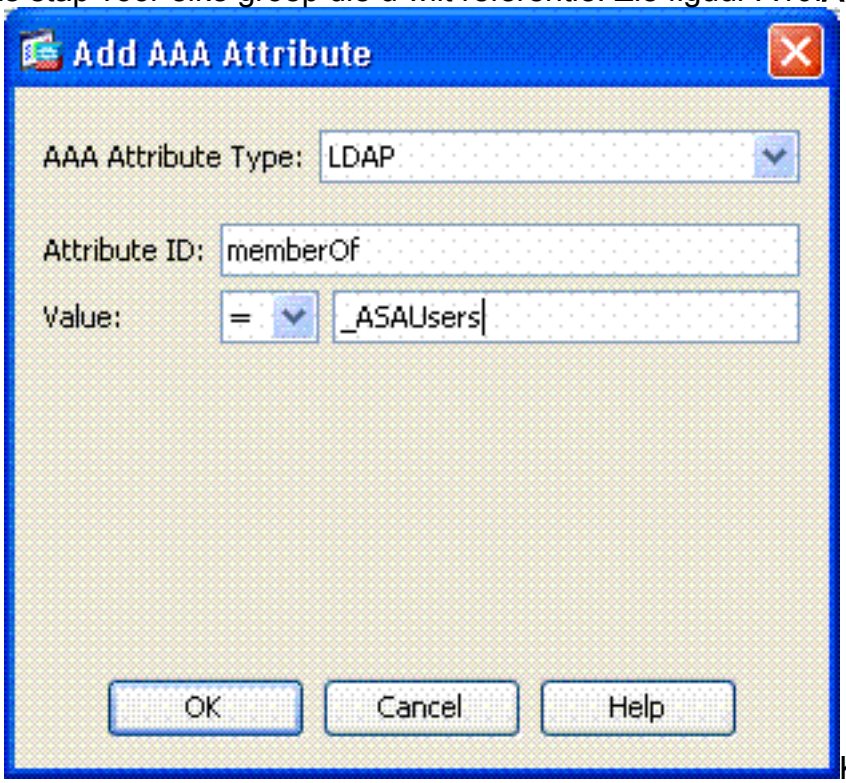
Scenario 3: Dynamisch toegangsbeleid voor meerdere leden van kenmerken

Dit voorbeeld gebruikt DAP om meerdere leden van eigenschappen te bekijken om toegang gebaseerd van Actieve groepsleden toe te staan. Vóór 8.x werd alleen het eerste lid van de eigenschap gelezen. Met 8.x en later kan de ASA alle leden van de eigenschappen bekijken.

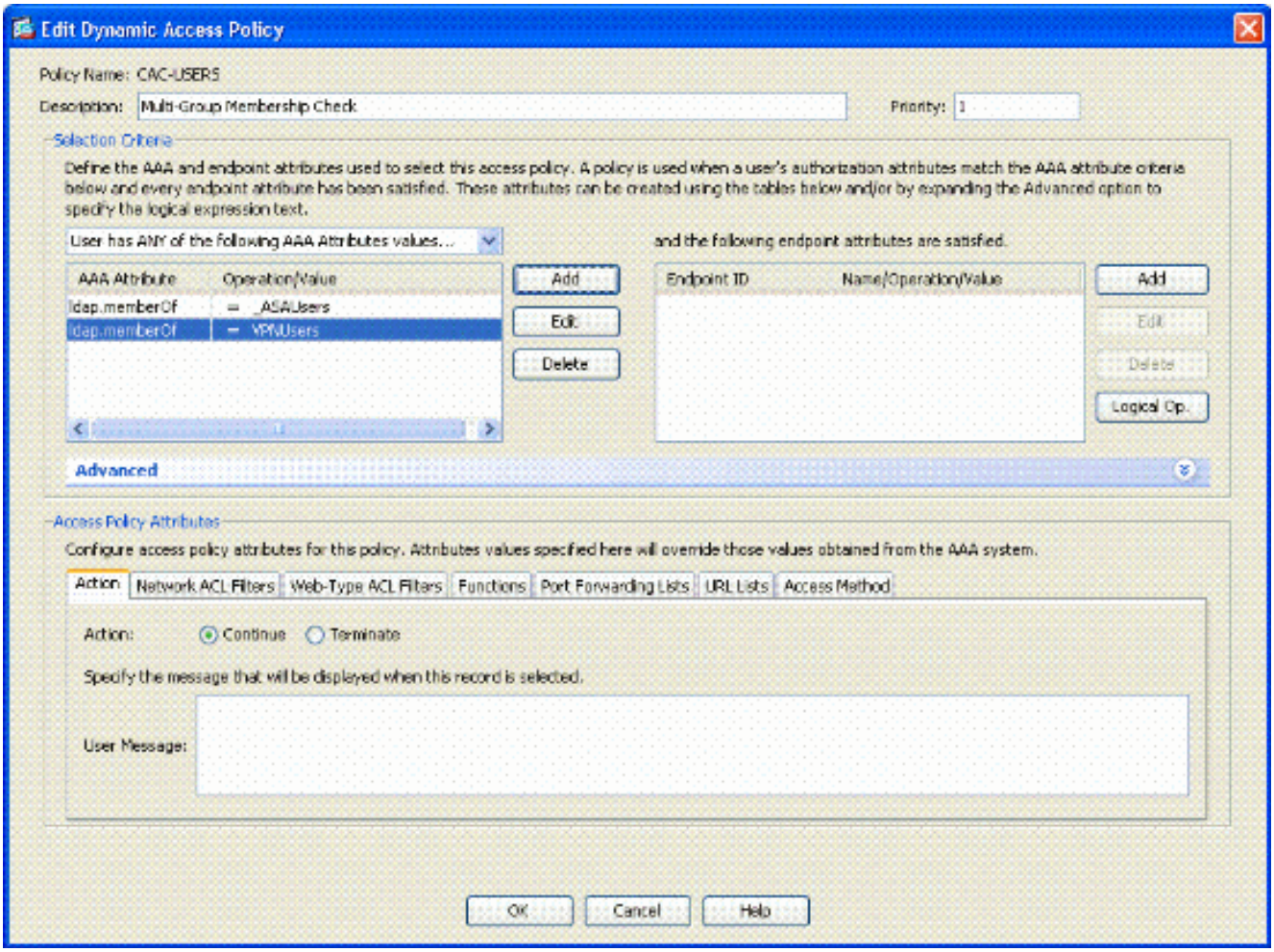
- Gebruik een groep die al bestaat of een nieuwe groep (of meerdere groepen) maakt voor ASA VPN-gebruikers om lid te zijn van een OCR-functie.
- Gebruik een groep die reeds bestaat of een nieuwe groep voor niet ASA gebruikers om lid van voor de voorwaarden van DENY te zijn.
- Controleer in de LDAP-viewer of u de goede DNA voor de groep hebt. Zie appendix D. Als de DN fout is, werkt de mapping niet goed.

ASA-configuratie

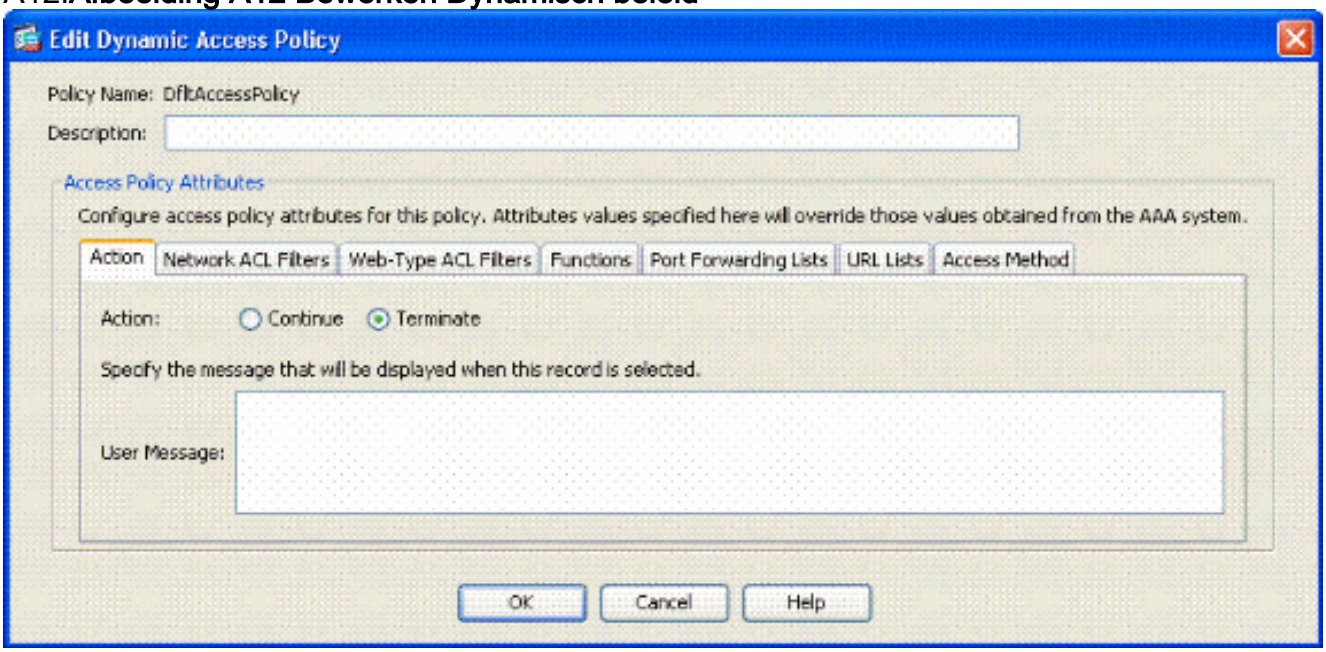
1. Kies in ASDM de optie **Remote Access VPN> Network (Client) Access > Dynamisch toegangsbeleid**.
2. Klik op **Toevoegen**.
3. Voltooi de volgende stappen in het toegangsbeleid toevoegen:Typ een naam in het Tekstvak van de naam b.Voer in het prioriteitsgedeelte **1** in, of een getal groter dan 0.Klik in de selectiecriteria op **Toevoegen**.Selecteer in het kenmerk Add AAA **en kies LDAP**.Voer in de sectie eigenschap ID in op **lid**.Kies in het waardegedeelte **=** en voer de AD groepsnaam in. Herhaal deze stap voor elke groep die u wilt referentie. Zie figuur A10.**Afbeelding A100 AAA-functiekaart**



Klik op **OK**.**Kies** in het gedeelte Access Policy Attributes **de optie** Doorgaan. Zie figuur A11.**Afbeelding 11 Voeg dynamisch beleid toe**



4. Kies in ASDM de optie **Remote Access VPN> Network (Client) Access > Dynamisch toegangsbeleid**.
5. Kies **Standaardtoegangsbeleid** en kies **Bewerken**.
6. De standaardinstelling is dat deze **functie** wordt ingesteld op **Beëindiging**. Zie figuur A12.**Afbeelding A12 Bewerken Dynamisch beleid**



7. Klik op **OK**.

N.B.: Als **Terminate** niet geselecteerd is, mag u inbellen, zelfs als dit niet in een groep gebeurt, omdat Standaard **Doorgaan** is.

Bijlage B - ASA CLI-configuratie

ASA 5510

```
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=ggsgseclab,DC=org 20
ldap attribute-map msNPAllowDialin
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin 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=ggsgseclab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn
CN=Administrator,CN=Users,DC=ggsgseclab,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
crl 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
crl configure
crypto ca trustpoint ASDM_TrustPoint2
revocation-check ocsp
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override ocsp
trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint3
revocation-check ocsp none
enrollment terminal
crl 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---------------------
---------------
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-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-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 - Problemen oplossen

AAA en LDAP probleemoplossing

- **debug ldap 255**—Hier worden LDAP-uitwisselingen weergegeven
- **debug een gebruikelijk 10**-displays AAA-uitwisselingen

Voorbeeld 1: Toegestane verbinding met juiste attributenafbeelding

Dit voorbeeld toont de output van **debug ldap** en **debug a common** tijdens een succesvolle verbinding met scenario 2 in Bijlage A.

Afbeelding C1: Debug LDAP en debug a 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=ggsgseclab,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=ggsgseclab,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 niet-geconfigureerd Cisco-attributenafbeelding

Dit voorbeeld toont de output van **debug ldap** en **debug a common** tijdens een toegestane verbinding met scenario 2 in Bijlage A.

Afbeelding C2: Debug LDAP en debug a common output - onjuiste 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=ggsgseclab,DC=org]
```

```
Filter = [userPrincipalName=12345678900@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=ggsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,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=ggsgseclab,DC=or
g
[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 "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 (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

DAP voor probleemoplossing

- **bug van scherpfouten**—Hier worden DAP-fouten weergegeven
- **debug** van **dap-overtrek**: Hier wordt de DAP-functie ook weergegeven

Voorbeeld 1: Toegelaten verbinding met DAP

Dit voorbeeld toont de output van **debug dap fouten** en **debug dap trace** tijdens een succesvolle verbinding met scenario 3 dat in Bijlage A wordt getoond. Merk op dat er meerdere ledenVan-eigenschappen zijn. U kunt behoren tot zowel _ASAUsers als VPNUsers of tp een van beide groepen, wat van de ASA configuratie afhangt.

Afbeelding C3: debug DAP

```
#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=ggsgseclab,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
= VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2
= _ASAUsers
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=ggsgseclab,DC=or
g
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"]["physicalDeliveryOfficeN
ame"] =
"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=ggsgseclab,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"] =
"_ASAUsers";
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=ggsgseclab,DC=o
rg";
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: Geëigende verbinding met DAP

Dit voorbeeld toont de uitvoer van **debug van dap fouten** en **debug dap trace** tijdens een onsuccesvolle verbinding met scenario 3 dat in Bijlage A wordt getoond.

Afbeelding C4: debug DAP

```
#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:
12418792980@mil
------------------------------------------------------
---------------
---
1: action = terminate
DAP_TRACE: DAP_open: C91154E8
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.cn =
12418792980
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.givenName
= 12418792980
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.distinguishedName =
CN=12418792980,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.instanceType = 4
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.displayName = 12418792980
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.uSNCreated
= 33691
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.memberOf =
DnsAdmins
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.uSNChanged
= 53274
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.department
= NETADMIN
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.name =
12418792980
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.objectGUID
=
....+..F.."5....
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.codePage =
0
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.countryCode = 0
DAP_TRACE: Username: 12418792980@mil,
aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 12418792980@mil, aaa.ldap.lastLogoff
= 0
DAP_TRACE: Username: 12418792980@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=ggsgseclab,DC=or
g
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"]["physicalDeliveryOfficeN
ame"] =
"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=ggsgseclab,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=ggsgseclab,DC=o
rg";
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: 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
```

certificaatinstantie voor probleemoplossing / OCSP

- **debug van crypto ' s 3**
- In de configuratie mode-**logklasse kan console(of buffer) het zuiveren**

Deze voorbeelden tonen een geslaagde certificatie met de OCSP-responder en een mislukt beleid voor het op elkaar afstemmen van certificatengroepen.

Afbeelding C3 toont de debug-uitvoer die is voorzien van een gevalideerd certificaat en een goed werkend beleid voor het koppelen van certificaten.

Afbeelding C4 toont de debug-uitvoer van een niet-ingesteld beleid voor het koppelen van certificaten.

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

Afbeelding C5: OCSP-debugging - succesvolle certificatie

```
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 beleid voor het koppelen van certificaten

Afbeelding C5: Uitvoer van een ingetrokken certificaat

```
n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled
uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,valdid 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:
```

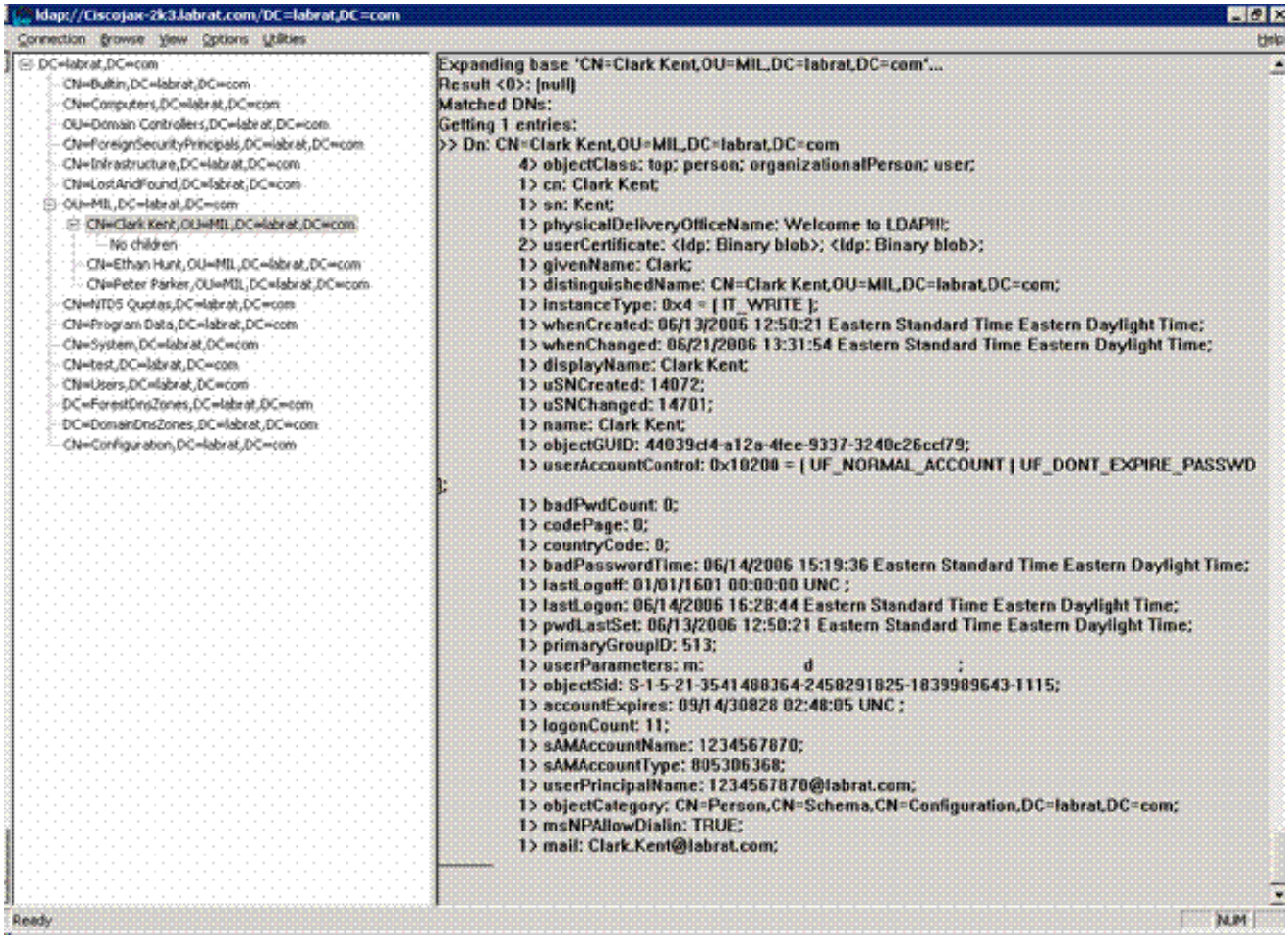
```
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org, issuer_name:
cn=ggsgseclab,dc=ggsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for
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=ggsgseclab,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=ggsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

Aanhangsel D - Verifieer LDAP-objecten in de lidstaten

Op de CD van Microsoft Server 2003 kunnen extra gereedschappen worden geïnstalleerd om zowel de LDAP-structuur als de LDAP-objecten/eigenschappen te bekijken. Om deze tools te installeren, gaat u naar de **Support** folder op de CD en vervolgens **Gereedschappen**. Installeer **SUPTOOLS.MSI**.

LDAP Viewer

- Kies na de installatie **Start > Uitvoeren**.
- Typ **ldp** en klik vervolgens op **OK**. Dit start de LDAP-viewer.
- Kies **verbinding > Connect**.
- Voer de servernaam in en klik vervolgens op **OK**.
- Kies **verbinding > Bind**.
- Voer een gebruikersnaam en wachtwoord in.**Opmerking:** u hebt beheerrechten nodig.
- Klik op **OK**.
- Bekijk LDAP objecten. Zie figuur D1.**Afbeelding D1: LDAP Viewer**

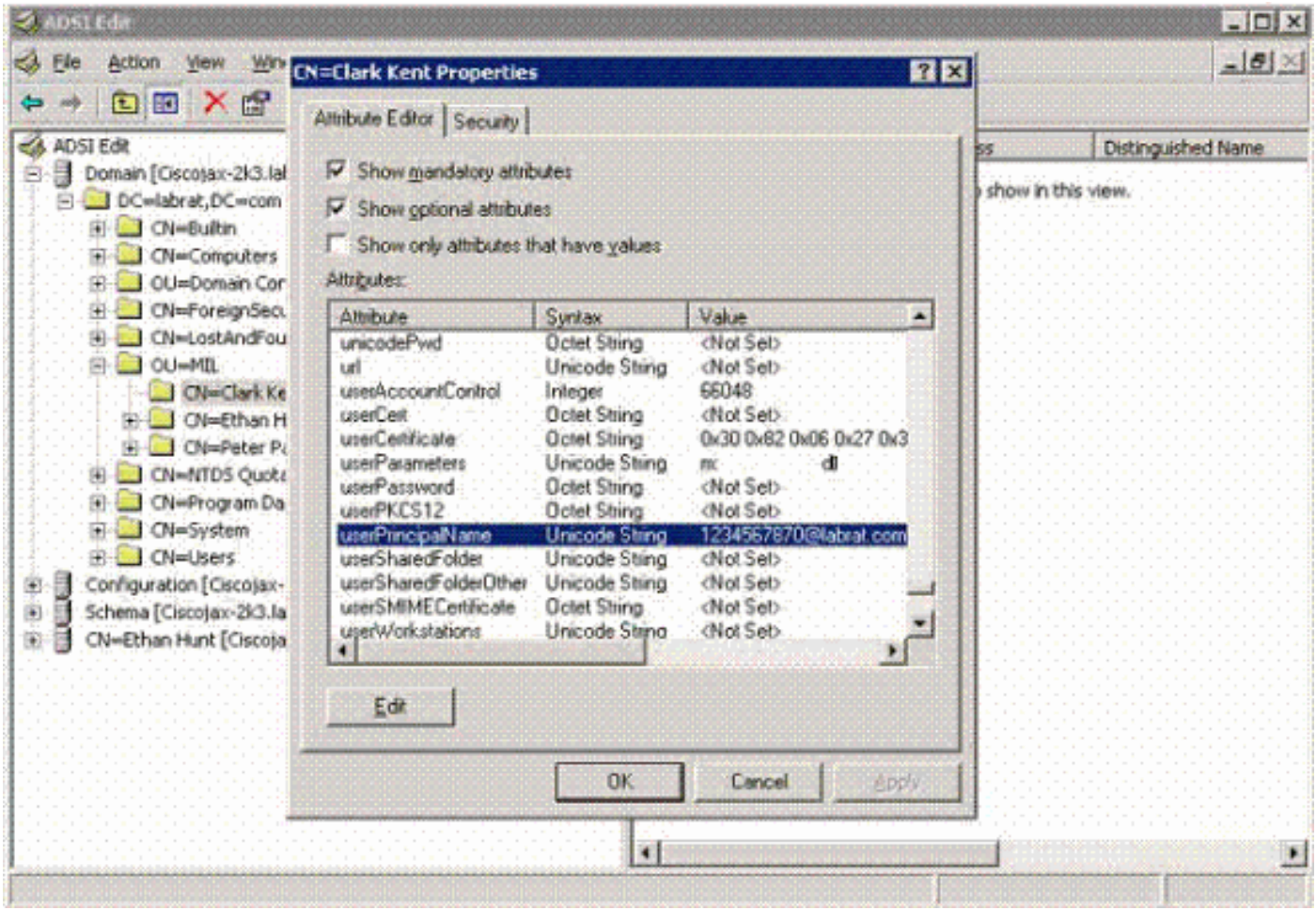


Interface-editor voor actieve mappen

- Kies **Start > Run** in de server **van** Active Directory.
- Type **adsiedit.msc**. Dit begint de redacteur.
- Klik met de rechtermuisknop op een object en klik op **Eigenschappen**.

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

Afbeelding D2: ADSI bewerken



Aanhangsel E

Een AnyConnect-profiel kan worden gemaakt en aan een werkstation worden toegevoegd. Het profiel kan verschillende waarden als ASA-hosts of overeenkomende parameters voor certificaten zoals een vooraanstaande naam of uitgevende instelling als referentie gebruiken. Het profiel wordt opgeslagen als een bestand .xml en kan met Kladblok worden bewerkt. Het bestand kan handmatig aan elke client worden toegevoegd of via een groepsbeleid uit de ASA worden geduwd. 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 de AnyConnectProfile.tmpl en open het bestand met Kladblok.
2. Breng de nodige wijzigingen aan in het bestand zoals de emittent of de host IP. Zie bijvoorbeeld afbeelding F1.
3. Als dit klaar is, slaat u het bestand op als een .xml.

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

Raadpleeg de Cisco AnyConnect-documentatie voor het profielbeheer. In het kort:

- Een profiel moet een unieke naam hebben voor uw bedrijf. Een voorbeeld is: CiscoProfile.xml
- De naam van het profiel moet gelijk zijn, ook al verschilt het voor de afzonderlijke groep binnen de onderneming.

Dit bestand moet worden onderhouden door een beveiligde gateway-beheerder en vervolgens

worden gedistribueerd met de clientsoftware. Het profiel dat op deze XML is gebaseerd kan op elk moment aan cliënten worden verspreid. De ondersteunde distributiemechanismen zijn een gebundeld bestand met de softwaredistributie of als onderdeel van het automatische downloadmechanisme. Het automatische downloadmechanisme is alleen beschikbaar voor bepaalde Cisco Secure Gateway-producten.

Opmerking: Administrateurs worden sterk aangemoedigd om het XML-profiel dat zij creëren te valideren met behulp van een online validatiemiddel of met behulp van de profielimportfunctionaliteit in ASDM. De validatie kan worden uitgevoerd met AnyConnectProfile.xsd in deze map. AnyConnectProfile is het basiselement dat het AnyConnect-clientprofiel vertegenwoordigt.

```
xml version="1.0" encoding="UTF-8"
- -




!--- The ClientInitialization section represents global
settings !--- for the client. In some cases, for
example, BackupServerList, host specific !--- overrides
are possible. !-- --> -




!--- The Start Before Logon feature can be used to
activate !--- the VPN as part of the logon sequence. !--
- UserControllable: Does the administrator of this
profile allow the user !--- to control this attribute
for their own use. Any user setting !--- associated with
this attribute is stored elsewhere. -->




!--- This control enables an administrator to have a one
time !--- message displayed prior to a users first
connection attempt. As an !--- example, the message can
be used to remind a user to insert their smart !--- card
into its reader. !--- The message to be used with this
control is localizable and can be !--- found in the
AnyConnect message catalog. !--- (default: "This is a
pre-connect reminder message.")




!-- This section enables the definition of various
attributes !--- that can be used to refine client
certificate selection. --> -
```

```
!--- Certificate Distinguished Name matching allows for
exact !--- match criteria in the choosing of acceptable
client !--- certificates. -




- !-- This section contains the list of hosts from which
!--- the user is able to select. -




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


        -
```

Gerelateerde informatie

- Certificaten en CRL's gespecificeerd door X.509 en RFC 3280
- OCSP gespecificeerd door RFC 2560
- Inleiding publieke sleutelinfrastructuur
- "Lichtgewicht OCSP" geprofileerd door conceptstandaard
- SSL / TLS gespecificeerd door RFC 2246
- Technische ondersteuning en documentatie – Cisco Systems