ASA Remote Access VPN IKE/SSL - Wachtwoord verlopen en wijzigen voor RADIUS, TACACS en LDAP-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft de wachtwoordwijziging en de eigenschappen van een VPN-tunnel op afstand die op een Cisco adaptieve security applicatie (ASA) wordt afgesloten. Het document heeft betrekking op:

- Verschillende klanten: Cisco VPN-client en Cisco AnyConnect beveiligde mobiliteit
- Verschillende protocollen: TACACS, RADIUS en lichtgewicht Directory Access Protocol (LDAP)
- Verschillende winkels in Cisco Secure Access Control System (ACS): lokale en actieve map (AD)

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van ASA-configuratie via de opdrachtregel-interface (CLI)
- Basiskennis van VPN-configuratie op een ASA
- Basiskennis van de Cisco beveiligde ACS

Gebruikte componenten

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

- Cisco adaptieve security applicatie, versie 8.4 en hoger
- Microsoft Windows Server 2003 SP1
- Cisco Secure Access Control System, versie 5.4 of hoger
- Cisco AnyConnect Secure Mobility, versie 3.1
- Cisco VPN-client, release 5

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.

Configureren

> **Opmerkingen:**
>
> Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.
>
> Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

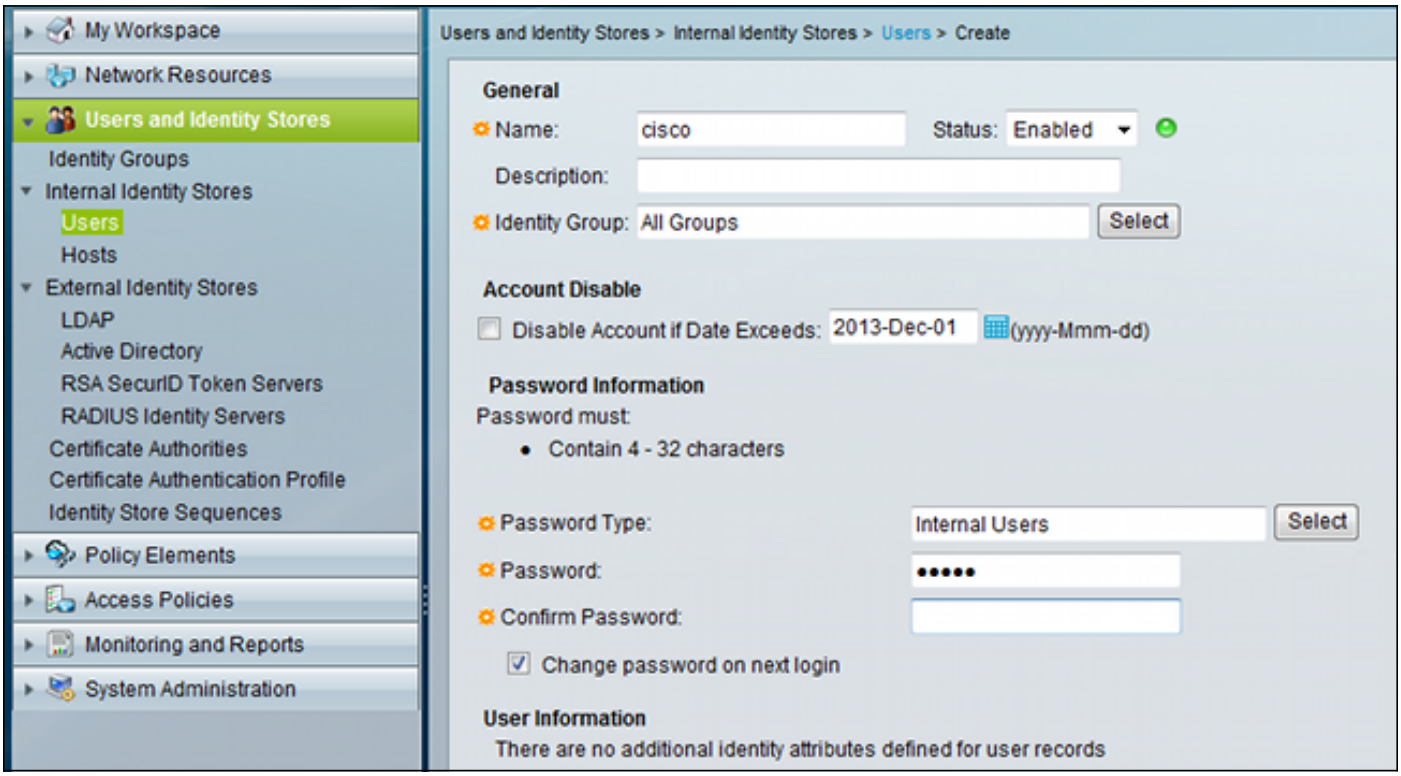
ASA met lokale verificatie

Een ASA met lokaal gedefinieerde gebruikers staat het gebruik van wachtwoordverloopfuncties of wachtwoordveranderingsfuncties niet toe. Een externe server, zoals RADIUS, TACACS, LDAP of Windows NT, is vereist.

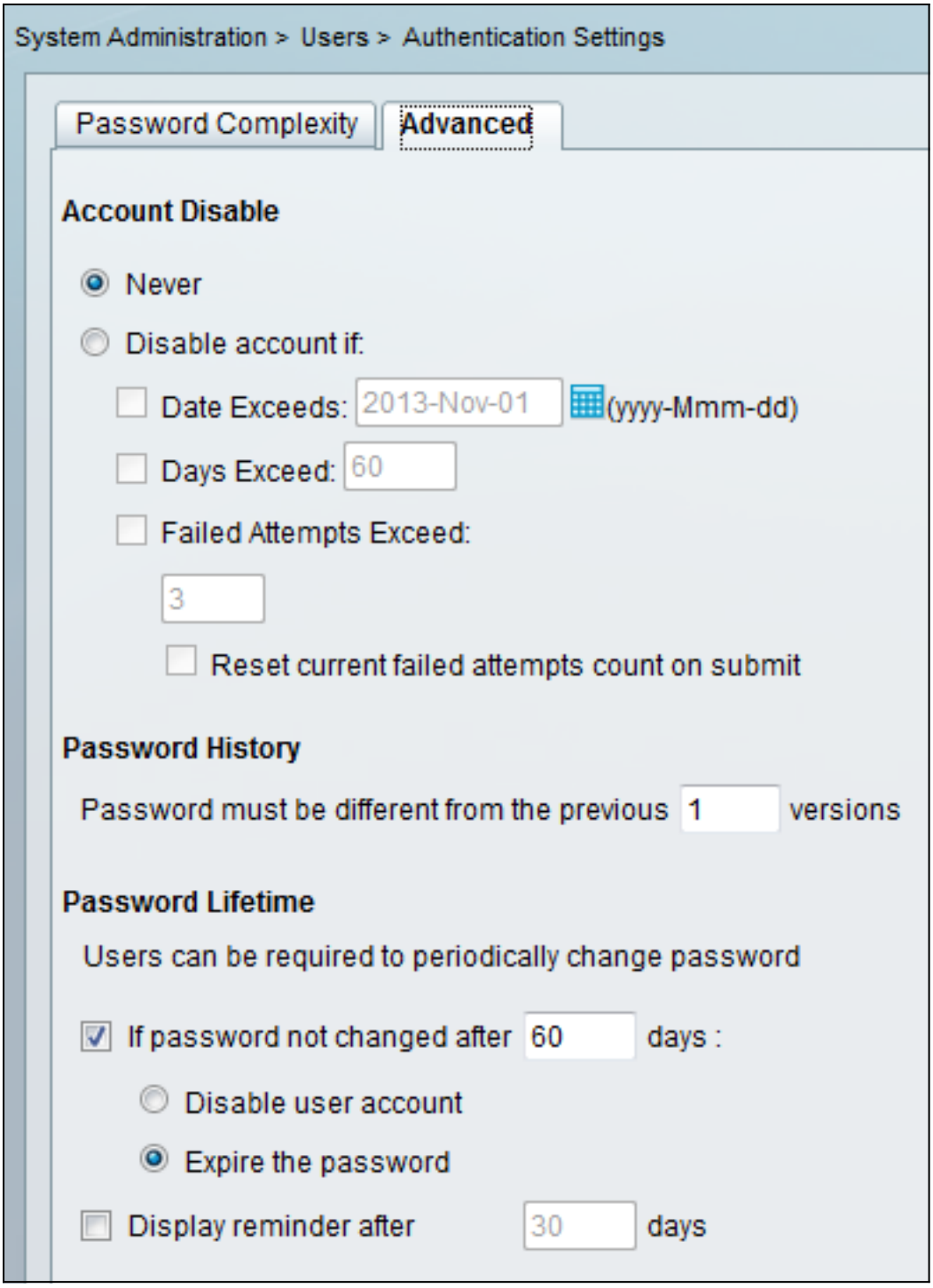
ACS- en lokale gebruikers

ACS ondersteunt zowel de wachtwoordafloop als de wachtwoordwijziging voor de lokaal gedefinieerde gebruikers. U kunt bijvoorbeeld nieuwe gebruikers dwingen om hun wachtwoord bij

hun volgende inloggen te wijzigen of u kunt een account op een bepaalde datum uitschakelen:

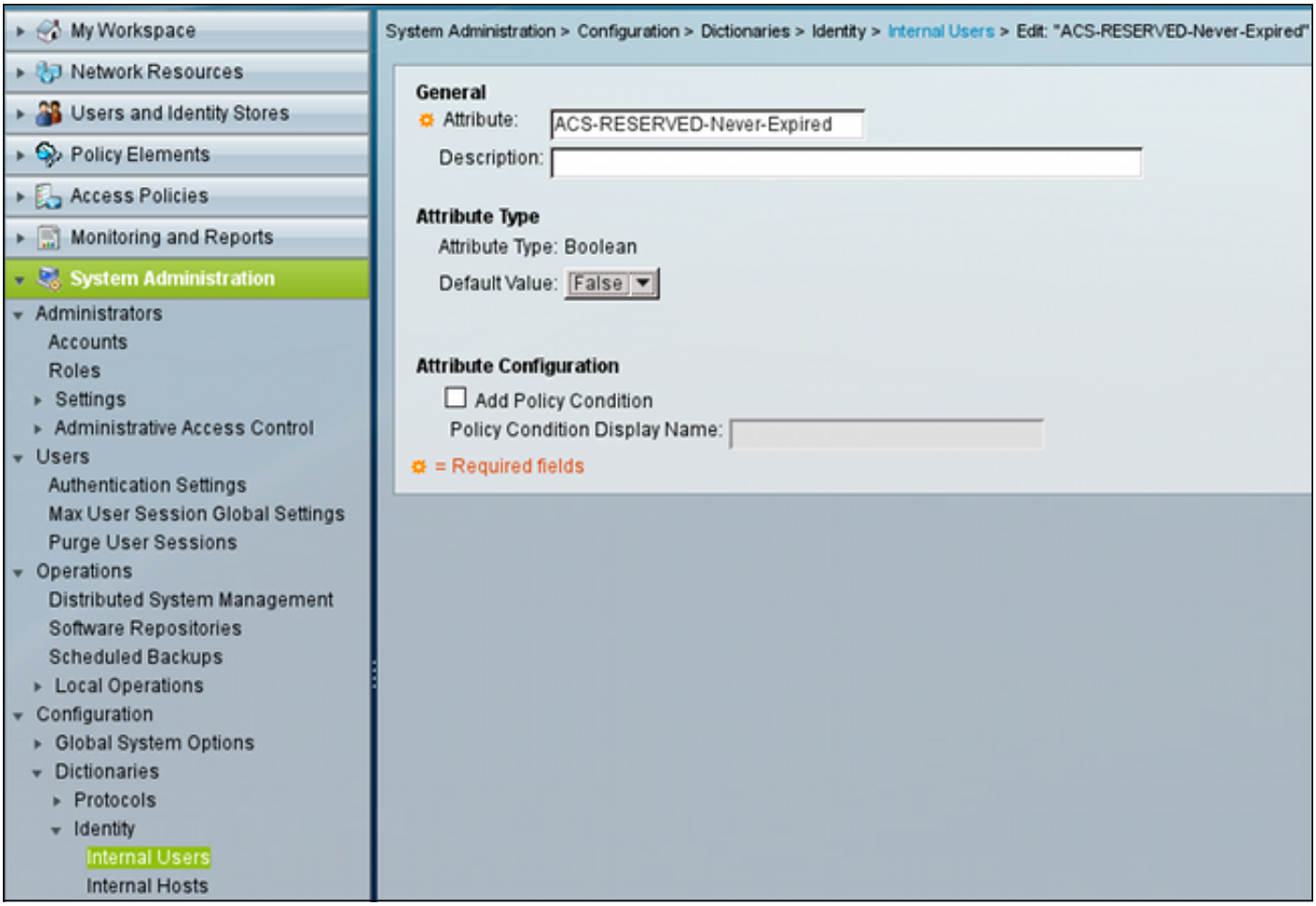


U kunt een wachtwoordbeleid voor alle gebruikers instellen. Nadat een wachtwoord is verlopen, kunt u de gebruikersaccount bijvoorbeeld uitschakelen (blokkeren zonder inlogmogelijkheid) of de optie aanbieden om het wachtwoord te wijzigen:

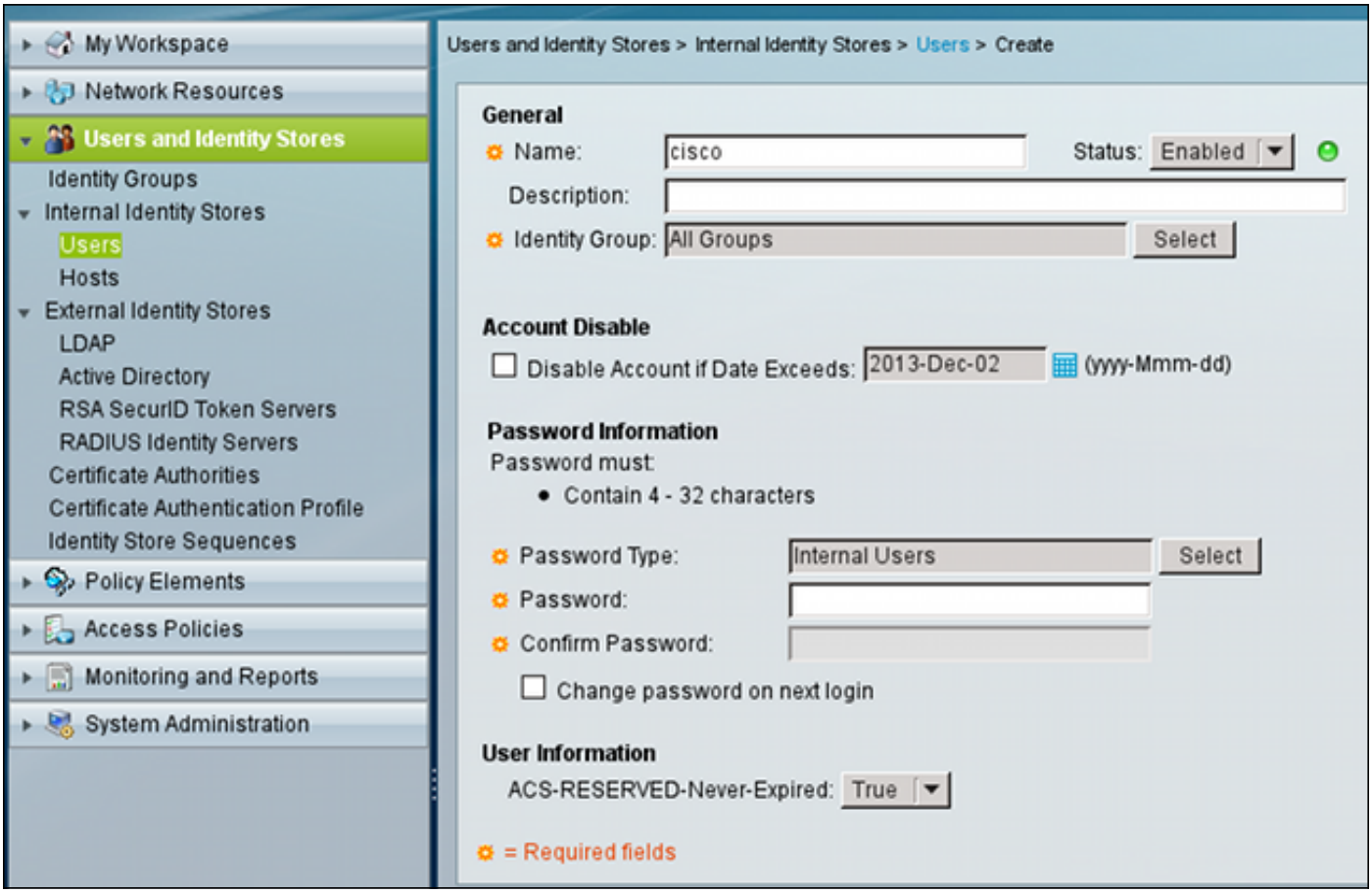


Gebruiker-specifieke instellingen hebben voorrang op mondiale instellingen.

ACS-RESERVED-Never-Expired is een interne eigenschap voor gebruikersidentiteit.



Deze eigenschap wordt ingeschakeld door gebruiker en kan worden gebruikt om de algemene instellingen voor het verlopen van account uit te schakelen. Met deze instelling wordt een account niet uitgeschakeld, zelfs niet als het algemene beleid aangeeft dat het moet zijn:

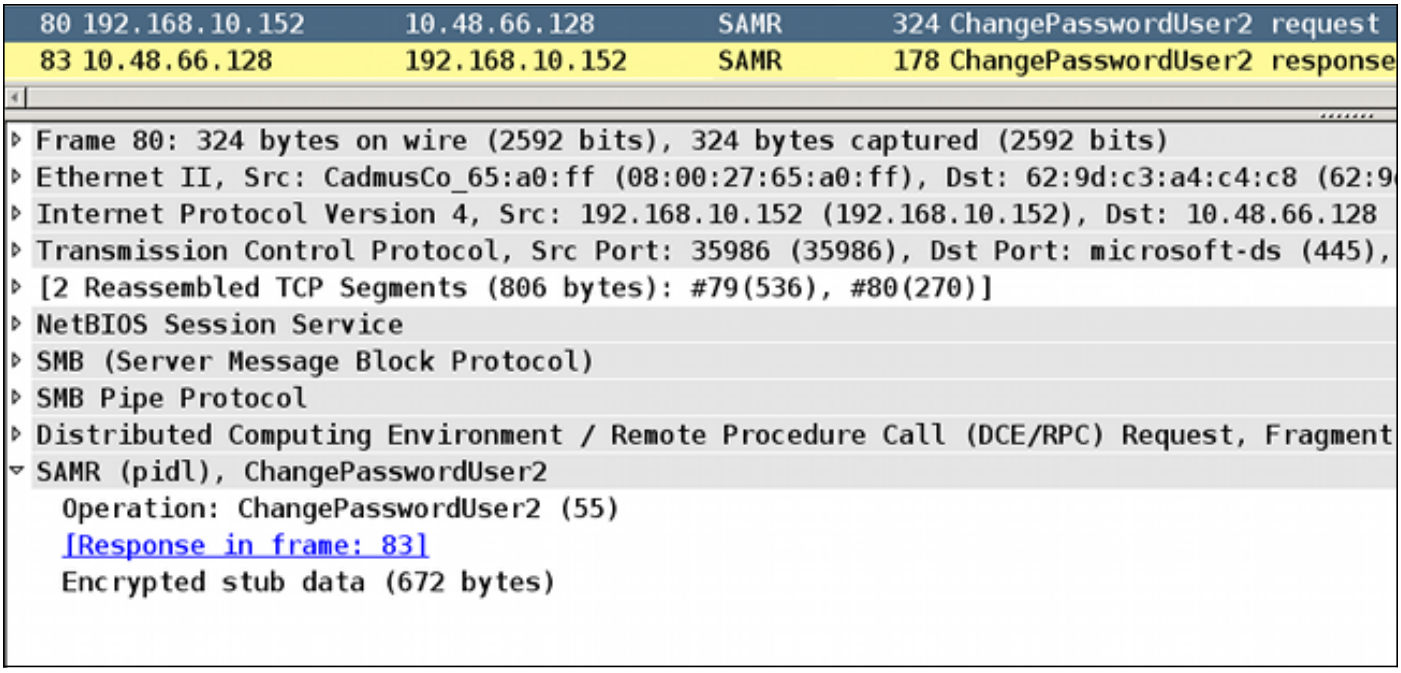


Gebruikers van ACS en actieve map

ACS kan worden ingesteld om de gebruikers in een AD-database te controleren. De wachtwoordvervaldatum en de verandering worden ondersteund wanneer Microsoft Challenge Handshake Authentication Protocol, versie 2 (MSCHAPv2) wordt gebruikt. Zie Gebruikershandleiding voor Cisco Secure Access Control System 5.4: Verificatie in ACS 5.4: Verificatieprotocol en compatibiliteit van Identity Store voor meer informatie.

Op een ASA, kunt u de wachtwoordbeheeroptie gebruiken, zoals beschreven in de volgende sectie, om de ASA te dwingen MSCHAPv2 te gebruiken.

ACS gebruikt de Common Internet File System (CIFS) Distributed Computing Environment/Remote Procedure Call (DCE/RPC) wanneer deze de Domain Controller-map (DC) contacteert om het wachtwoord te wijzigen:



ASA kan zowel de RADIUS- als de TACACS+-protocollen gebruiken om contact te hebben met de ACS voor een AD-wachtwoordwijziging.

ASA met ACS via RADIUS

Het RADIUS-protocol ondersteunt geen wachtwoordwijziging. Meestal wordt het Password Authentication Protocol (PAP) gebruikt bij RADIUS. ASA stuurt de gebruikersnaam en het wachtwoord in onbewerkte tekst en het wachtwoord wordt dan versleuteld door gebruik van het RADIUS-gedeelde geheim.

In een typisch scenario wanneer het gebruikerswachtwoord is verlopen, keert ACS een bericht van Radius-Afwijzen naar de ASA terug. ACS merkt op dat:

Authentication Summary	
Logged At:	October 2,2013 8:24:52.446 AM
RADIUS Status:	Authentication failed : 24203 User need to change password
NAS Failure:	
Username:	cisco
MAC/IP Address:	192.168.10.67
Network Device:	ASA3 : 192.168.11.250 :
Access Service:	Default Network Access
Identity Store:	Internal Users
Authorization Profiles:	
CTS Security Group:	
Authentication Method:	PAP_ASCII

Voor de ASA is het een eenvoudig bericht van de Radius-Afwijzing, en de authenticatie faalt.

Om dit probleem op te lossen, staat de ASA gebruik van de **wachtwoord-beheer** opdracht toe onder de tunnel-groepsconfiguratie:

```
tunnel-group RA general-attributes
 authentication-server-group ACS
 password-management
```

De opdracht **wachtwoordbeheer** verandert het gedrag zodat de ASA in het Radius-request-moest MSCHAPv2 in plaats van PAP gebruiken.

Het MSCHAPv2 protocol ondersteunt wachtwoordwijziging. Dus als een VPN-gebruiker in die specifieke tunnelgroep is geland tijdens de Xauth-fase, omvat het Radius-verzoek van ASA nu een MS-CHAP-Challenge:

```
▼ Attribute Value Pairs
  ▷ AVP: l=7  t=User-Name(1): cisco
  ▷ AVP: l=6  t=NAS-Port(5): 3979366400
  ▷ AVP: l=6  t=Service-Type(6): Framed(2)
  ▷ AVP: l=6  t=Framed-Protocol(7): PPP(1)
  ▷ AVP: l=15  t=Called-Station-Id(30): 192.168.1.250
  ▷ AVP: l=15  t=Calling-Station-Id(31): 192.168.10.67
  ▷ AVP: l=6  t=NAS-Port-Type(61): Virtual(5)
  ▷ AVP: l=15  t=Tunnel-Client-Endpoint(66): 192.168.10.67
  ▼ AVP: l=24  t=Vendor-Specific(26) v=Microsoft(311)
    ▷ VSA: l=18 t=MS-CHAP-Challenge(11): 205d20e2349fe2bb15e3ed5c570d354c
  ▼ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
    ▷ VSA: l=52 t=MS-CHAP2-Response(25): 0000fb52f2f8dcc50b0fe2aa79b2cdd428
  ▷ AVP: l=6  t=NAS-IP-Address(4): 192.168.11.250
  ▷ AVP: l=34  t=Vendor-Specific(26) v=Cisco(9)
```

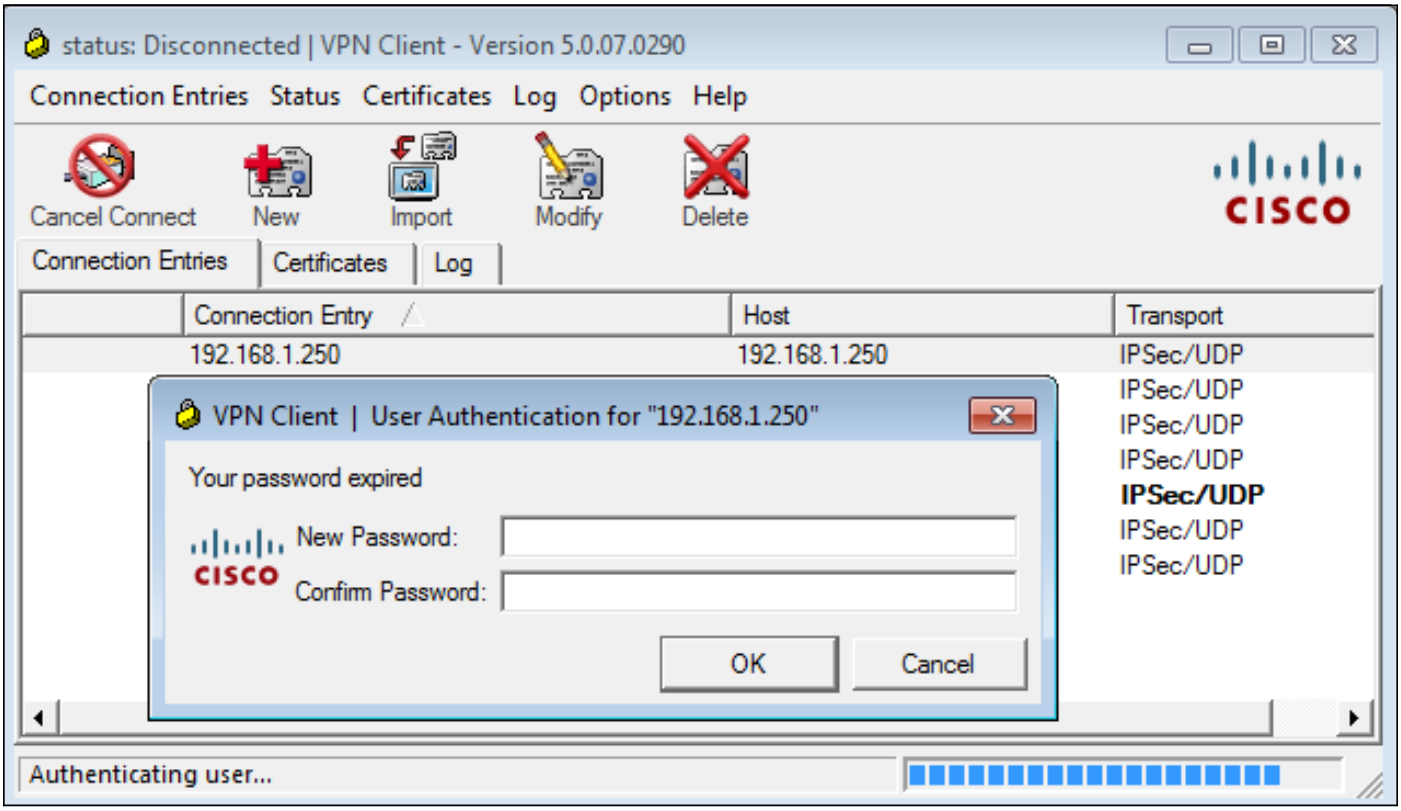
Als ACS opmerkt dat de gebruiker het wachtwoord moet wijzigen, geeft het een Radius-Afwijzen bericht met MSCHAPv2 fout 648 terug.

```
▽ Attribute Value Pairs
  ▽ AVP: l=57  t=Vendor-Specific(26) v=Microsoft(311)
    ▷ VSA: l=51 t=MS-CHAP-Error(2): \000E=648 R=0 C=205
```

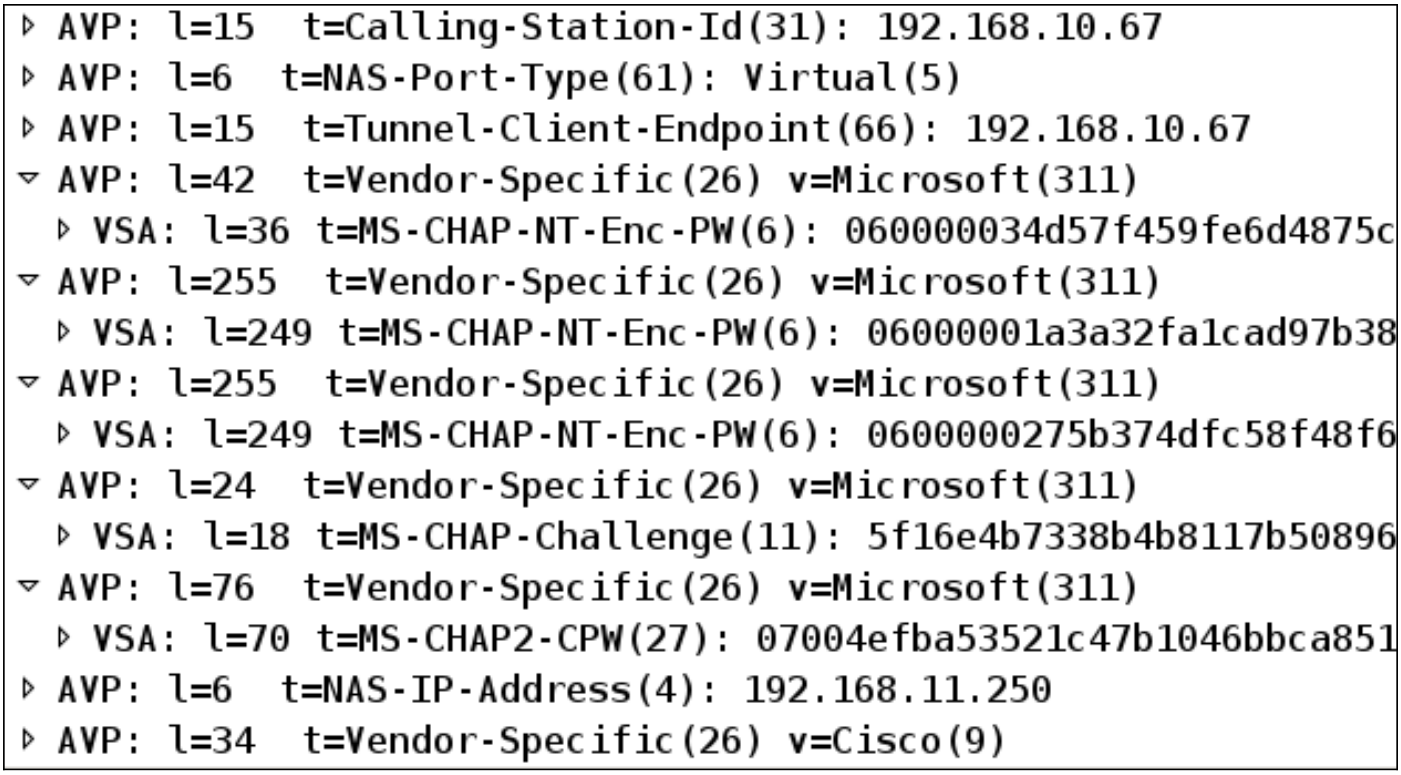
ASA begrijpt dat bericht en gebruikt MODE_CFG om het nieuwe wachtwoord te vragen bij de Cisco VPN-client:

```
Oct 02 06:22:26 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received Password Expiration from Auth server!
```

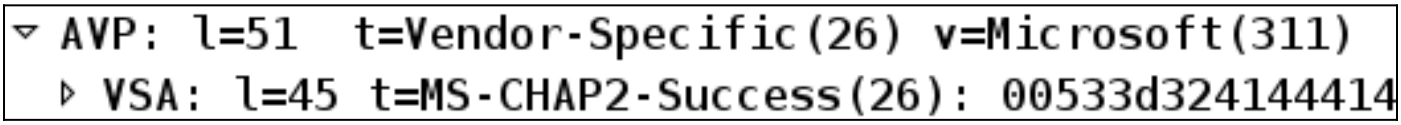
De client van Cisco VPN toont een dialoogvenster dat om een nieuw wachtwoord vraagt:



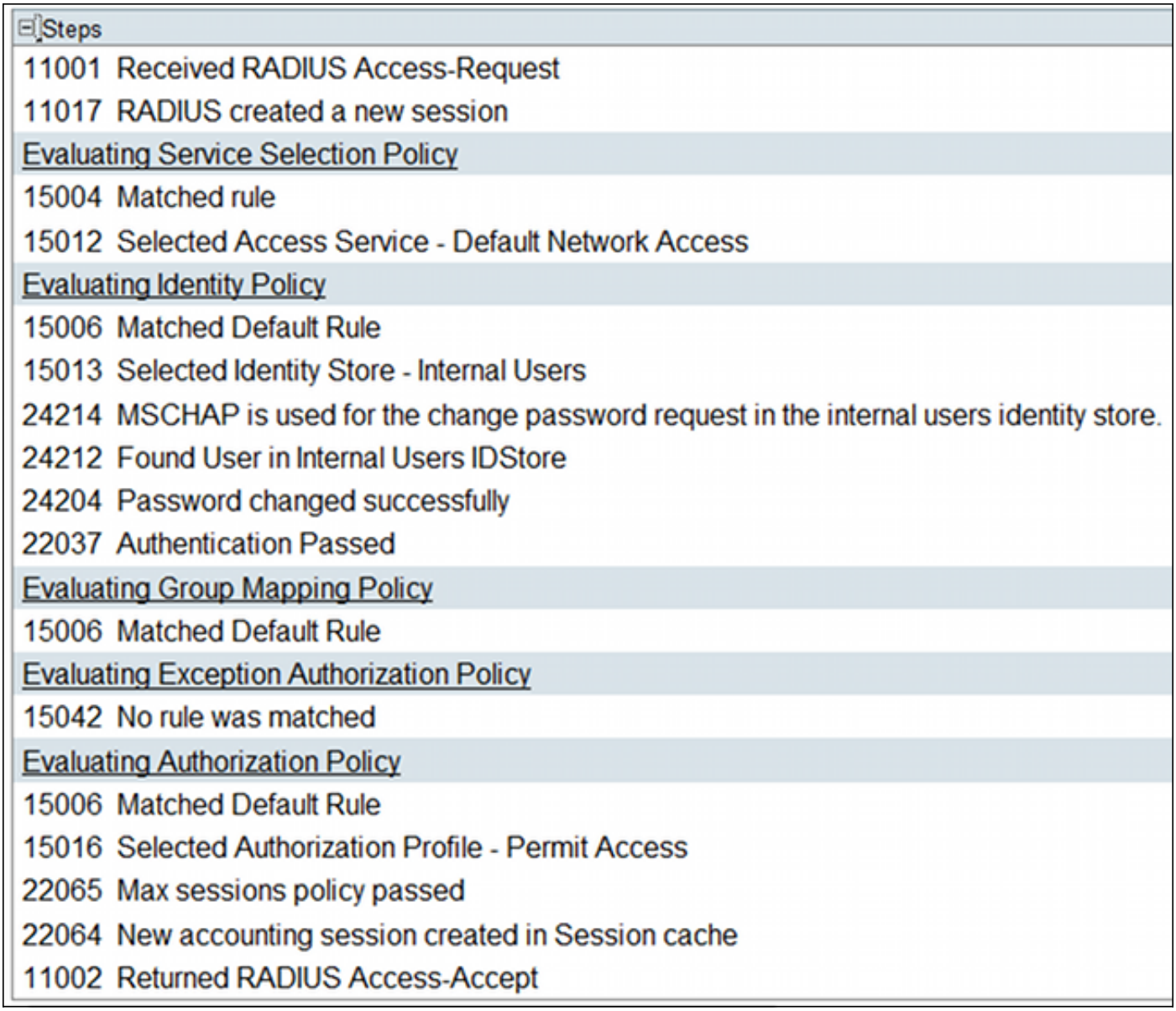
ASA stuurt een ander Radius-verzoek met een MS-CHAP-CPW en MS-CHAP-NT-NT-Enc-PW lading (het nieuwe wachtwoord):



ACS bevestigt het verzoek en keert een Radius-Accept met MS-CHAP2-Success terug:



Dit kan worden geverifieerd op ACS, dat meldt dat een '24204 Wachtwoord met succes is gewijzigd':



ASA rapporteert dan succesvolle verificatie en gaat verder met het QM-proces (Quick Mode):

```
Oct 02 06:22:28 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

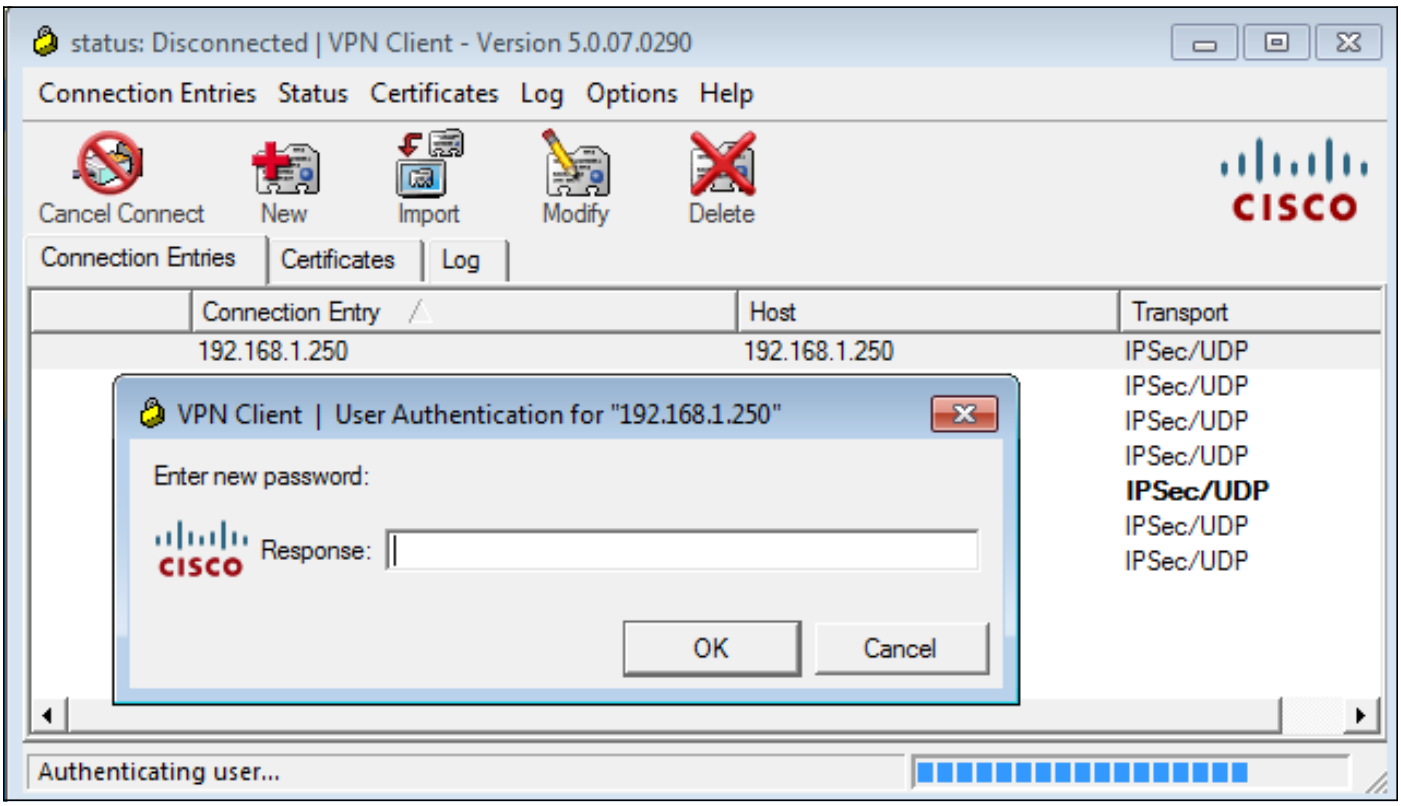
ASA met ACS via TACACS+

Op dezelfde manier kan TACACS+ worden gebruikt voor het verlopen van het wachtwoord en voor het wijzigen van het wachtwoord. De wachtwoordbeheerfunctie is niet nodig, omdat de ASA TACACS+ nog steeds gebruikt met een verificatietype van ASCII in plaats van MSCHAPv2.

Er worden meerdere pakketten uitgewisseld en ACS vraagt om een nieuw wachtwoord:

```
Decrypted Reply
    Status: 0x3 (Send Data)
    Flags: 0x01 (NoEcho)
    Server message length: 20
    Server message: Enter new password:
    Data length: 0
```

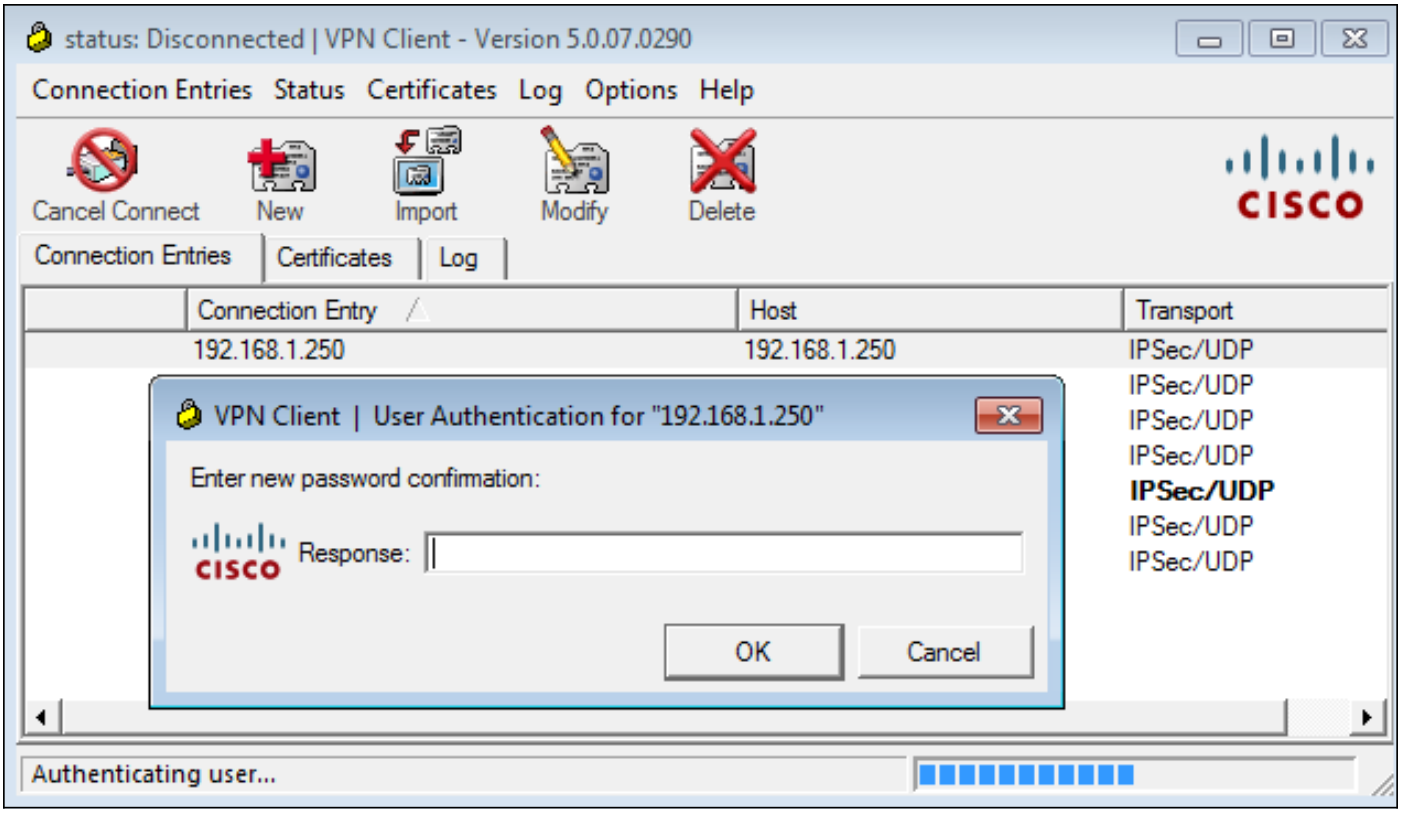
De client van Cisco VPN biedt een dialoogvenster (dat verschilt van het dialoogvenster dat met RADIUS wordt gebruikt) dat om een nieuw wachtwoord vraagt:



ACS vraagt om bevestiging van het nieuwe wachtwoord:

```
Decrypted Reply
    Status: 0x3 (Send Data)
    Flags: 0x01 (NoEcho)
    Server message length: 33
    Server message: Enter new password confirmation:
    Data length: 0
```

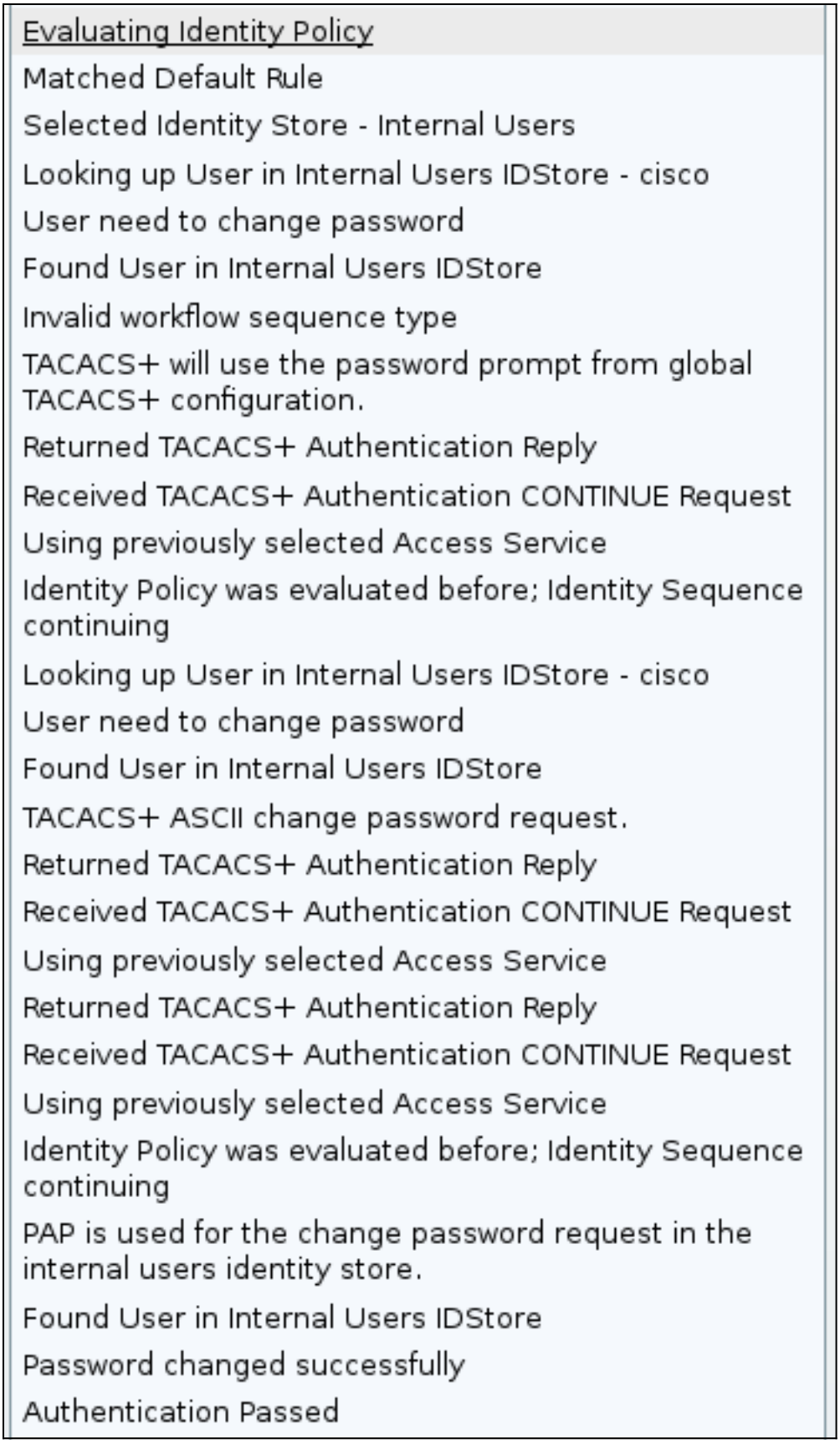
De Cisco VPN-client biedt een bevestigingsvenster:



Indien de bevestiging juist is, rapporteert ACS een succesvolle echtheidscontrole:

```
Decrypted Reply
    Status: 0x1 (Authentication Passed)
    Flags: 0x00
    Server message length: 0
    Data length: 0
```

ACS logt dan een gebeurtenis in dat het wachtwoord met succes is gewijzigd:



De ASA-debugs tonen het gehele proces van uitwisseling en succesvolle authenticatie:

```
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
```

```
Processing MODE_CFG Reply attributes
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
   Received challenge status!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
process_attr(): Enter!
Oct 02 07:44:40 [IKEv1 DEBUG]Group = RA, Username = cisco, IP = 192.168.10.67,
Processing MODE_CFG Reply attributes.
Oct 02 07:44:41 [IKEv1]Group = RA, Username = cisco, IP = 192.168.10.67,
User (cisco) authenticated.
```

Die wachtwoordverandering is volledig transparant voor ASA. Het is slechts een beetje langer de TACACS+ sessie met meer verzoek en antwoordpakketten, die door de VPN-client worden geparseerd en aan de gebruiker worden aangeboden die het wachtwoord wijzigt.

ASA met LDAP

De het verstrijken en de verandering van het wachtwoord worden volledig ondersteund door het Microsoft AD en het SON LDAP serverschema.

Voor een verandering van wachtwoord geven de servers 'bindresponse = ongeldigeCredentials' terug met 'error = 773'. Deze fout geeft aan dat de gebruiker het wachtwoord moet resetten. De meeste foutcodes zijn:

Foutcode	Fout
525	Gebruiker niet gevonden
52 sexies	Ongeldige referenties
530	Kan op dit moment niet worden aangemeld
531	Niet toegestaan om zich bij dit werkstation aan te melden
532	Wachtwoord verlopen
533	Account uitgeschakeld
701	Account verlopen
773	Gebruiker moet wachtwoord opnieuw instellen
775	Gebruiker Account geblokkeerd

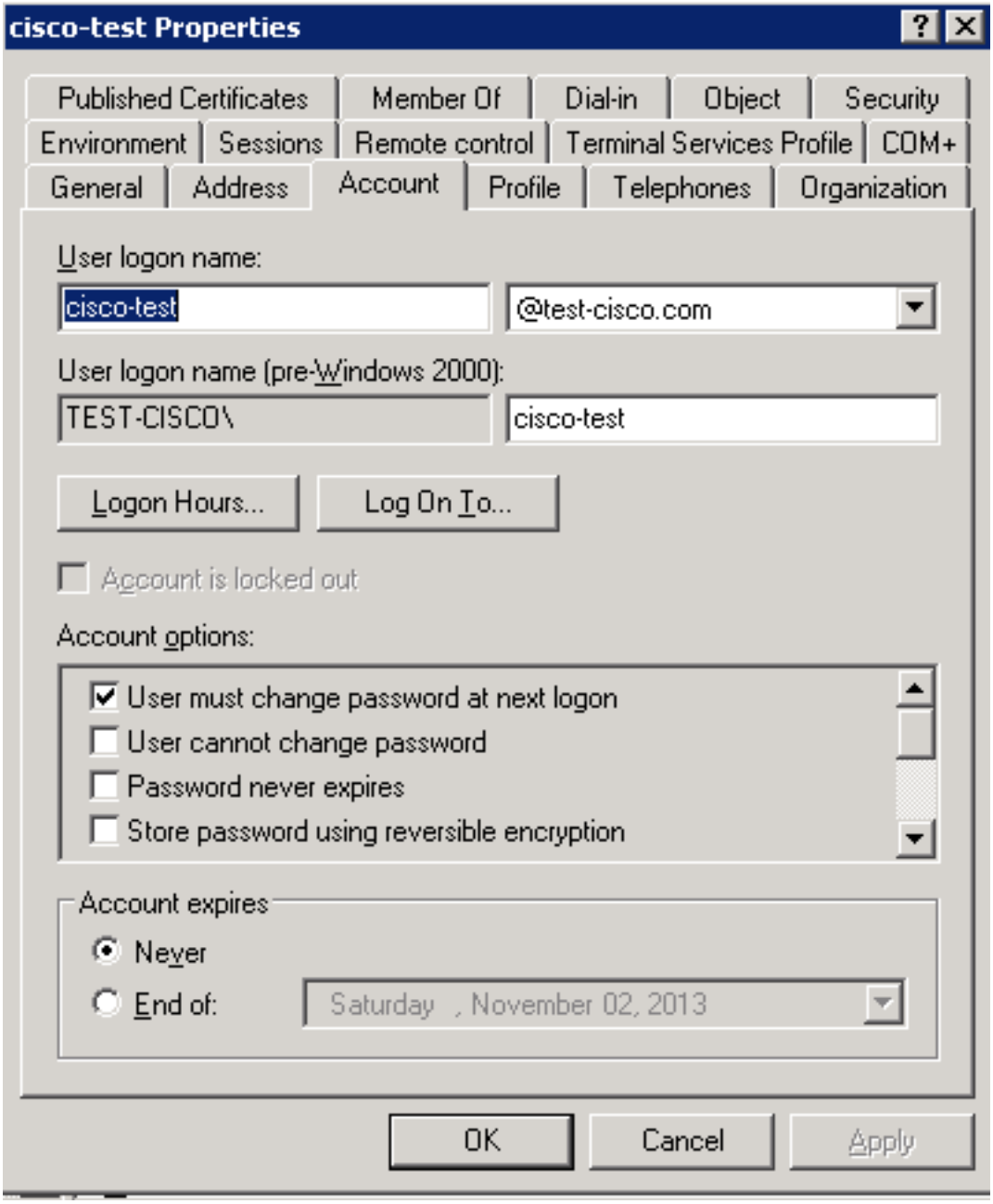
Configuratie van de LDAP server:

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host 10.48.66.128
 ldap-base-dn CN=USers,DC=test-cisco,DC=com
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn CN=Administrator,CN=users,DC=test-cisco,DC=com
 server-type microsoft
```

Gebruik die configuratie voor de tunnelgroep en de wachtwoordbeheerfunctie:

```
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group LDAP
 default-group-policy MY
 password-management
```

Configureer de AD-gebruiker zodat er een wachtwoord moet worden gewijzigd:



Wanneer de gebruiker probeert de Cisco VPN-client te gebruiken, meldt de ASA een ongeldig wachtwoord:

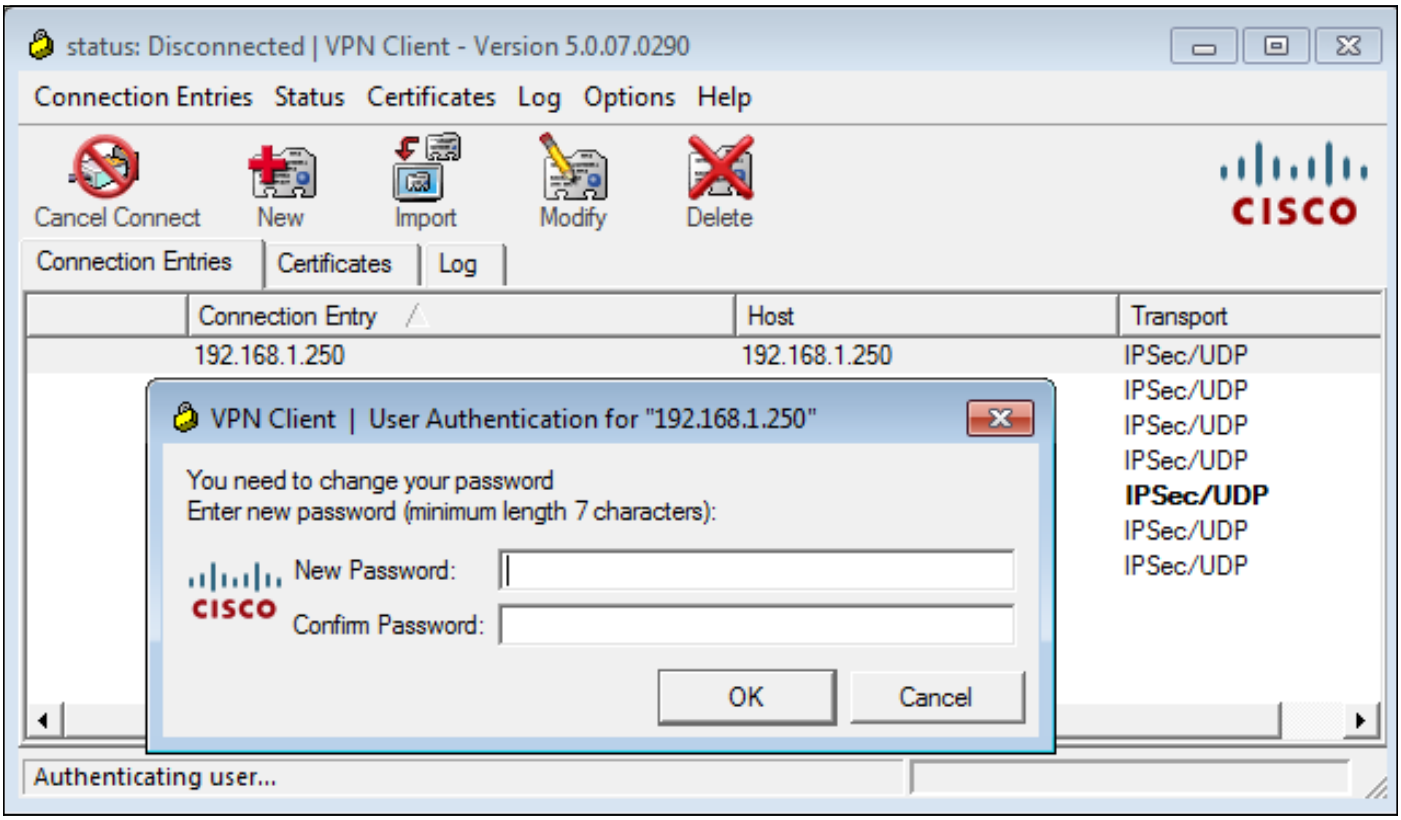
```
ASA(config-tunnel-general)# debug ldap 255
<some output ommited for clarity>

[111] Session Start
[111] New request Session, context 0xbd835c10, reqType = Authentication
[111] Fiber started
[111] Creating LDAP context with uri=ldap://10.48.66.128:389
[111] Connect to LDAP server: ldap://10.48.66.128:389, status = Successful
[111] supportedLDAPVersion: value = 3
[111] supportedLDAPVersion: value = 2
[111] Binding as Administrator
[111] Performing Simple authentication for Administrator to 10.48.66.128
[111] LDAP Search:
       Base DN = [CN=USers,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=cisco-test]
       Scope   = [SUBTREE]
[111] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
```

```
[111] Talking to Active Directory server 10.48.66.128
[111] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
DC=test-cisco,DC=com
[111] Read bad password count 2
[111] Binding as cisco-test
[111] Performing Simple authentication for cisco-test to 10.48.66.128
[111] Simple authentication for cisco-test returned code (49) Invalid
credentials
[111] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 773, vece
[111] Invalid password for cisco-test
```

Als de aanmeldingsgegevens ongeldig zijn, wordt de fout van 52e weergegeven:

```
[110] Message (cisco-test): 80090308: LdapErr: DSID-0C090334, comment:
AcceptSecurityContext error, data 52e, vece
```

De Cisco VPN-client vraagt vervolgens om een wachtwoordwijziging:



Dit dialoogvenster verschilt van het dialoogvenster dat door TACACS of RADIUS wordt gebruikt, omdat het beleid wordt weergegeven. In dit voorbeeld is het beleid een minimum wachtwoordlengte van zeven tekens.

Zodra de gebruiker het wachtwoord wijzigt, kan de ASA dit mislukkingsbericht krijgen van de LDAP server:

```
[113] Modify Password for cisco-test successfully converted password to unicode
[113] modify failed, no SSL enabled on connection
```

Het beleid van Microsoft vereist gebruik van de Secure Socket Layer (SSL) voor wachtwoordwijziging. Verandert de configuratie:

```
aaa-server LDAP (outside) host 10.48.66.128
 ldap-over-ssl enable
```

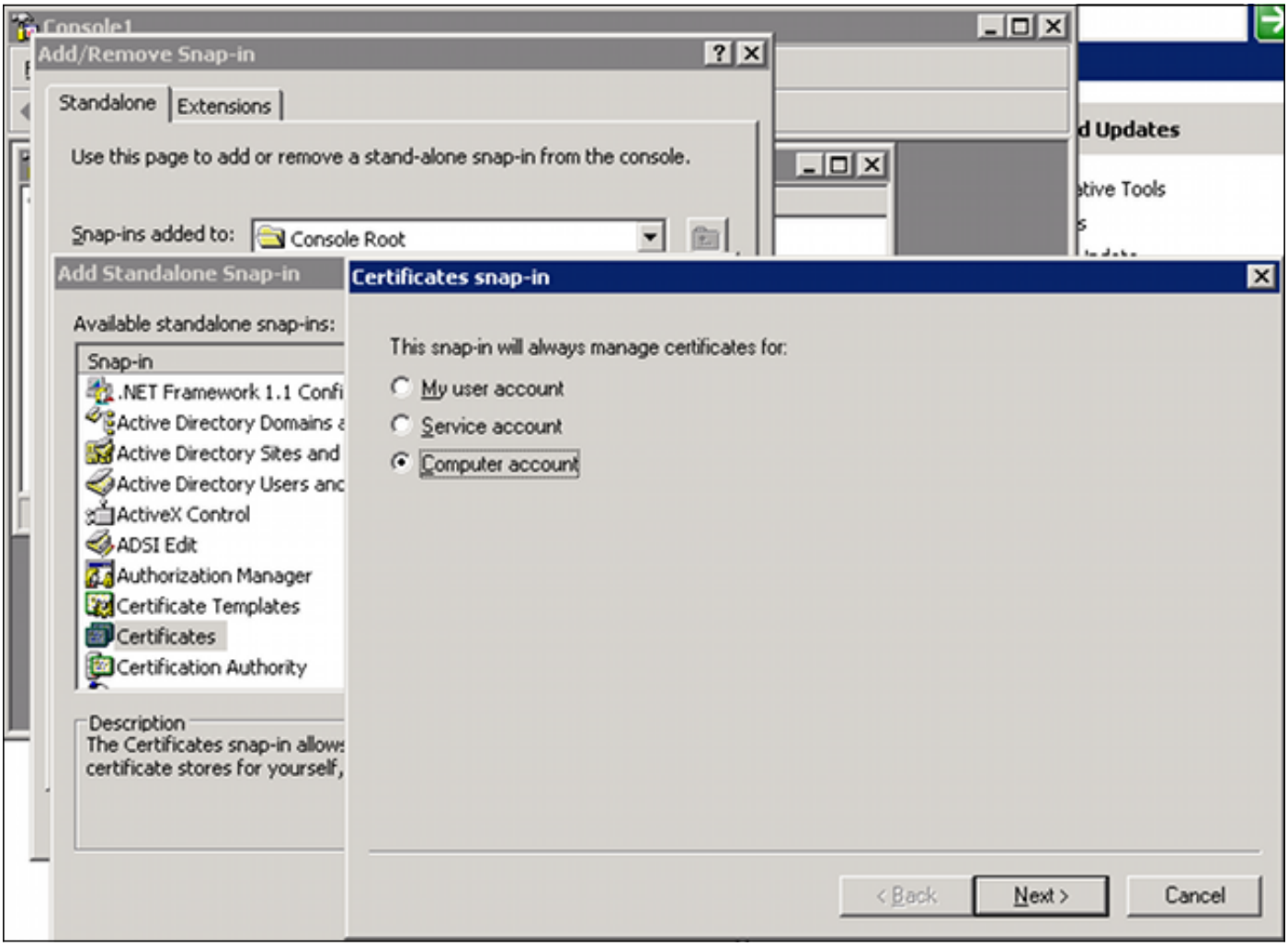
Microsoft LDAP voor SSL

Standaard werkt Microsoft LDAP via SSL niet. Om deze functie in te schakelen, moet u het certificaat voor de computeraccount installeren met de juiste bestandsextensie. Zie Hoe LDAP via SSL met een certificeringsinstantie van derden voor meer informatie mogelijk te maken.

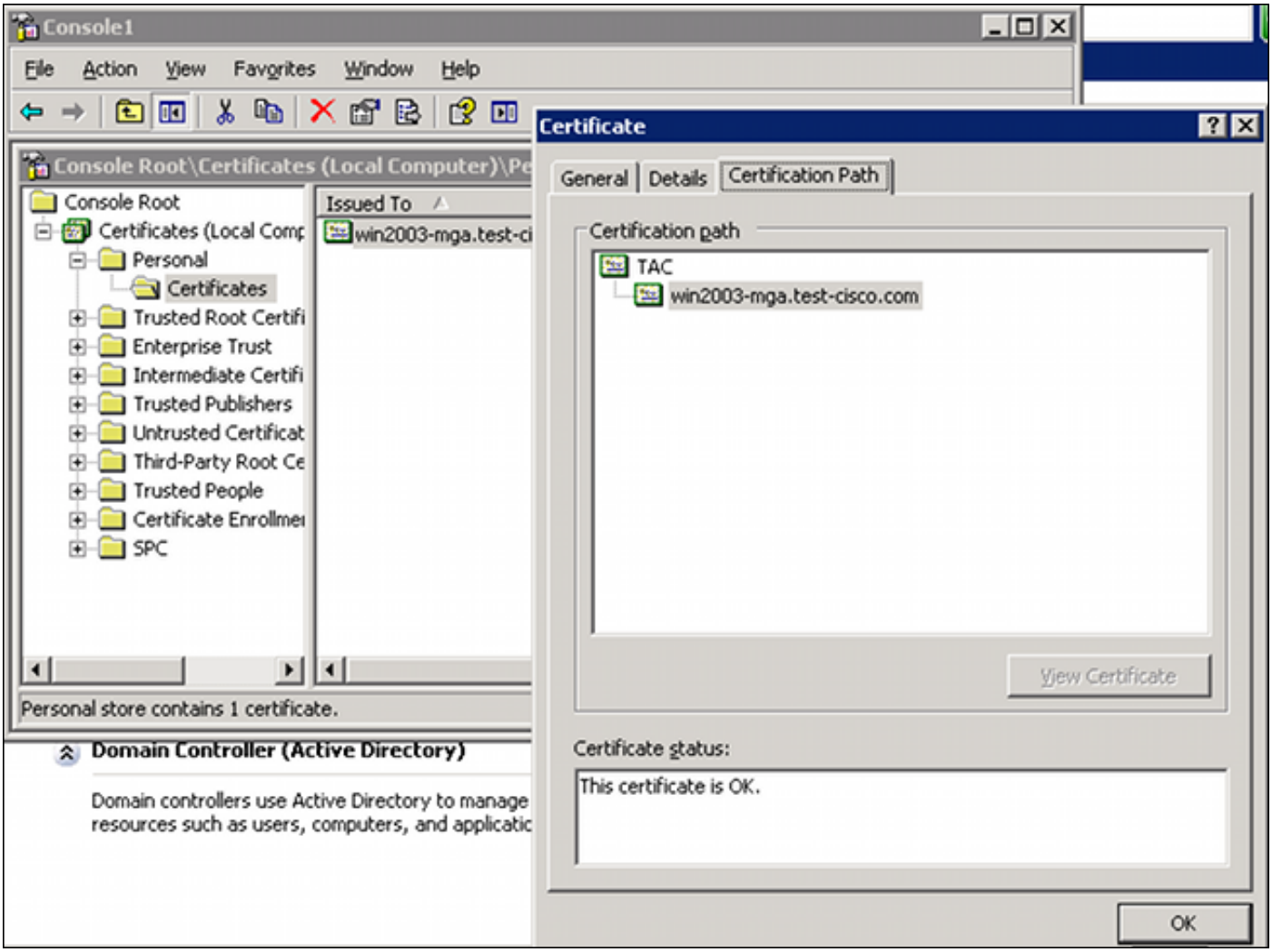
Het certificaat kan zelfs een zichzelf ondertekend certificaat zijn, omdat de ASA het LDAP-certificaat niet verifieert. Zie Cisco Bug ID CSCui40212, "Sta ASA toe om certificaat vanaf LDAPS server te valideren" voor een gerelateerde verbeteringsaanvraag.

> **Opmerking:** ACS verifieert het LDAP-certificaat in versie 5.5 en later.

Als u het certificaat wilt installeren, opent u de mmc-console, selecteert u **Magnetisch** toevoegen**/verwijderen**, voegt u het certificaat toe en kiest u **Computer-account**:



Selecteer **Plaatselijke computer**, voer het certificaat naar de persoonlijke winkel en verplaats het bijbehorende certificaat van de certificaatinstantie (CA) naar de vertrouwde winkel. Controleer of het certificaat is vertrouwd:



Er is een bug in ASA versie 8.4.2, waar deze fout kan worden teruggegeven wanneer u LDAP via SSL probeert te gebruiken:

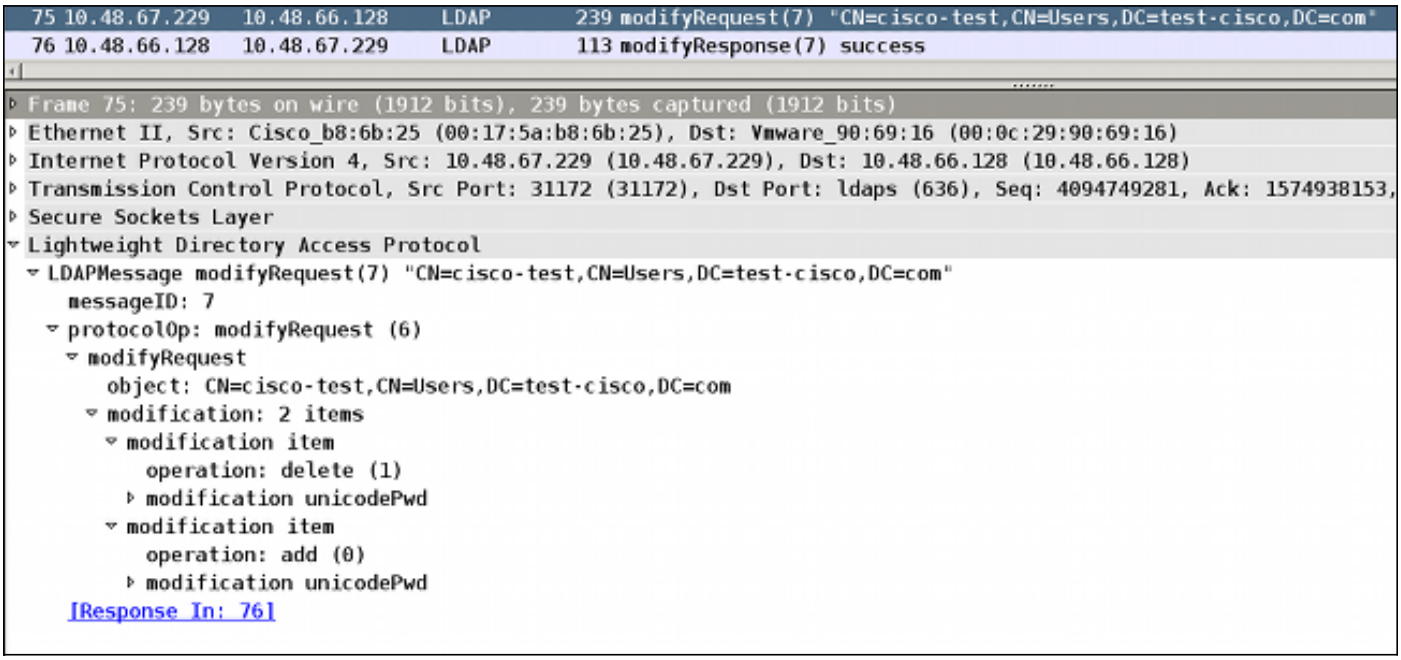
```
ASA(config)# debug ldap 255

[142] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[142] supportedLDAPVersion: value = 3
[142] supportedLDAPVersion: value = 2
[142] Binding as Administrator
[142] Performing Simple authentication for Administrator to 10.48.66.128
[142] LDAP Search:
       Base DN = [CN=Users,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=Administrator]
       Scope   = [SUBTREE]
[142] Request for Administrator returned code (-1) Can't contact LDAP server
```

ASA versie 9.1.3 werkt correct met dezelfde configuratie. Er zijn twee LDAP sessies. De eerste sessie geeft een fout terug met code 773 (het wachtwoord is verlopen), terwijl de tweede sessie wordt gebruikt voor de wachtwoordwijziging:

```
[53] Session Start
[53] New request Session, context 0xadebe3d4, reqType = Modify Password
[53] Fiber started
[53] Creating LDAP context with uri=ldaps://10.48.66.128:636
[53] Connect to LDAP server: ldaps://10.48.66.128:636, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
```

```
[53] Binding as Administrator
[53] Performing Simple authentication for Administrator to 10.48.66.128
[53] LDAP Search:
       Base DN = [CN=Users,DC=test-cisco,DC=com]
       Filter  = [sAMAccountName=cisco-test]
       Scope   = [SUBTREE]
[53] User DN = [CN=cisco-test,CN=Users,DC=test-cisco,DC=com]
[53] Talking to Active Directory server 10.48.66.128
[53] Reading password policy for cisco-test, dn:CN=cisco-test,CN=Users,
DC=test-cisco,DC=com
[53] Read bad password count 0
[53] Change Password for cisco-test successfully converted old password to
unicode
[53] Change Password for cisco-test successfully converted new password to
unicode
[53] Password for cisco-test successfully changed
[53] Retrieved User Attributes:

<....most attributes details ommitted for clarity>
accountExpires: value = 130256568000000000 <----- 100ns intervals since
January 1, 601 (UTC)
```

Kijk op de pakketten om de wachtwoordwijziging te controleren. De privésleutel van de LDAP server kan door Wireshark worden gebruikt om SSL-verkeer te decrypteren:



Internet Key Exchange (IKE)/Authentication, Authorization en Accounting (AAA)-debugs in de ASA zijn zeer vergelijkbaar met die welke in het RADIUS-verificatiescenario worden gepresenteerd.

LDAP en waarschuwing voor afloop

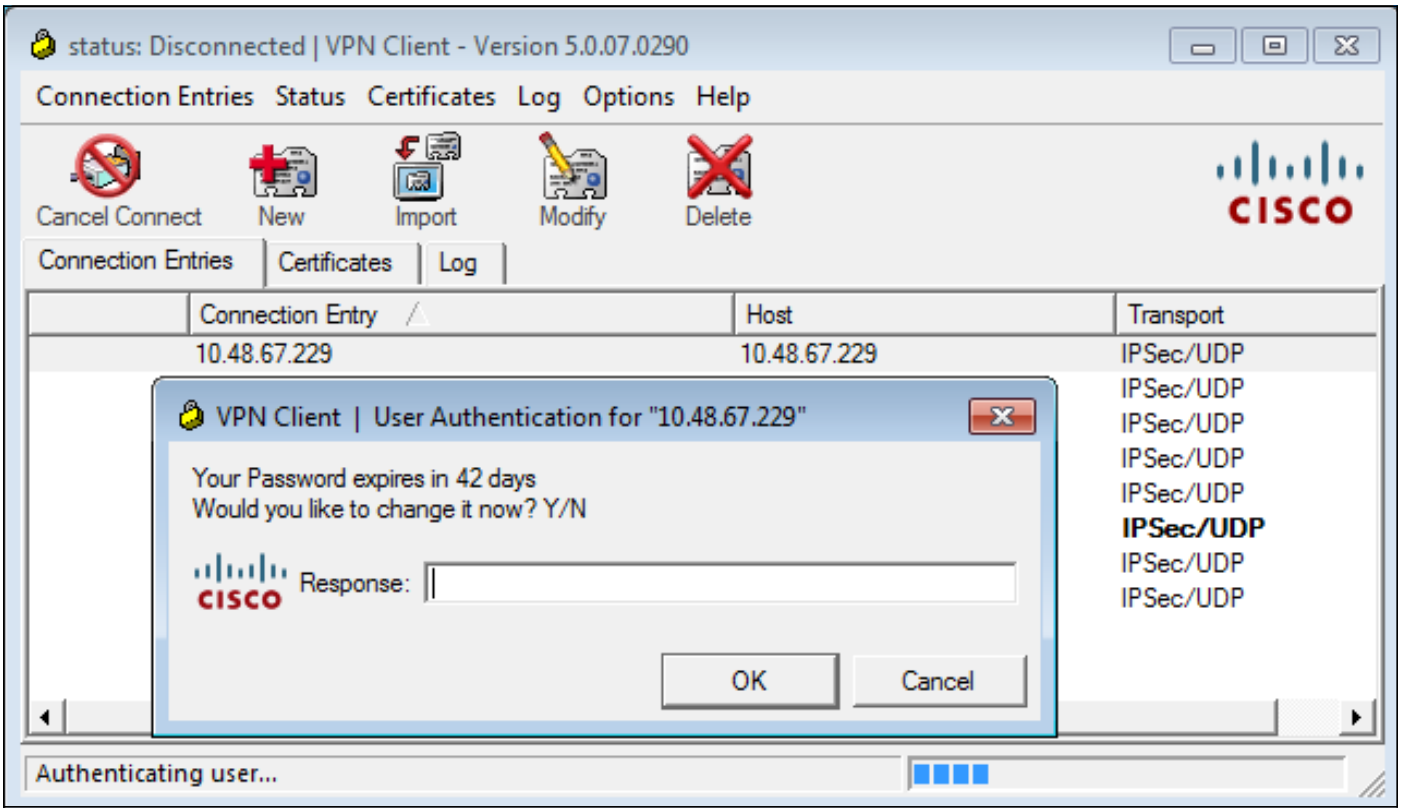
Voor LDAP kunt u een functie gebruiken die een waarschuwing verstuurt voordat het wachtwoord vervalt. ASA waarschuwt de gebruiker 90 dagen voor het verstrijken van het wachtwoord met deze instelling:

```
tunnel-group RA general-attributes
 password-management password-expire-in-days 90
```

Hier verloopt het wachtwoord binnen 42 dagen en de gebruiker probeert in te loggen:

```
ASA# debug ldap 255
<some outputs removed for clarity>

[84] Binding as test-cisco
[84] Performing Simple authentication for test-cisco to 10.48.66.128
[84] Processing LDAP response for user test-cisco
[84] Message (test-cisco):
[84] Checking password policy
[84] Authentication successful for test-cisco to 10.48.66.128
[84] now: Fri, 04 Oct 2013 09:41:55 GMT, lastset: Fri, 04 Oct 2013 09:07:23
GMT, delta=2072, maxage=1244139139 secs
[84] expire in: 3708780 secs, 42 days
[84] Password expires Sat, 16 Nov 2013 07:54:55 GMT
[84] Password expiring in 42 day(s),threshold 90 days
```

ASA stuurt een waarschuwing en biedt de optie voor een wachtwoordwijziging:



Als de gebruiker ervoor kiest het wachtwoord te wijzigen, wordt er een nieuw wachtwoord gevraagd en wordt de normale wachtwoordveranderingsprocedure gestart.

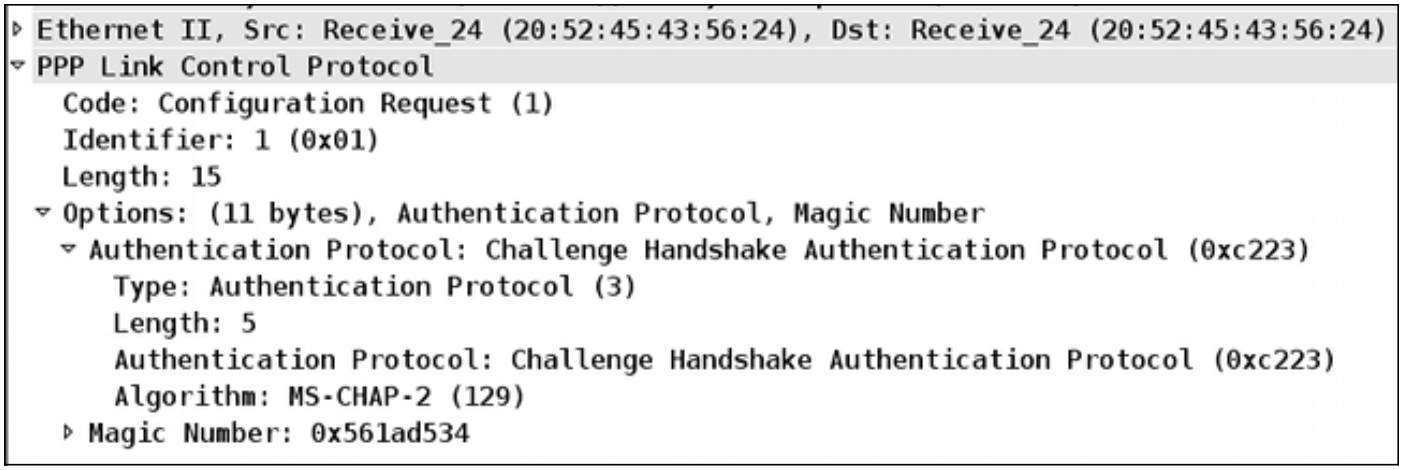
ASA en L2TP

De vorige voorbeelden presenteerden IKE, versie 1 (IKEv1) en een IPSec VPN.

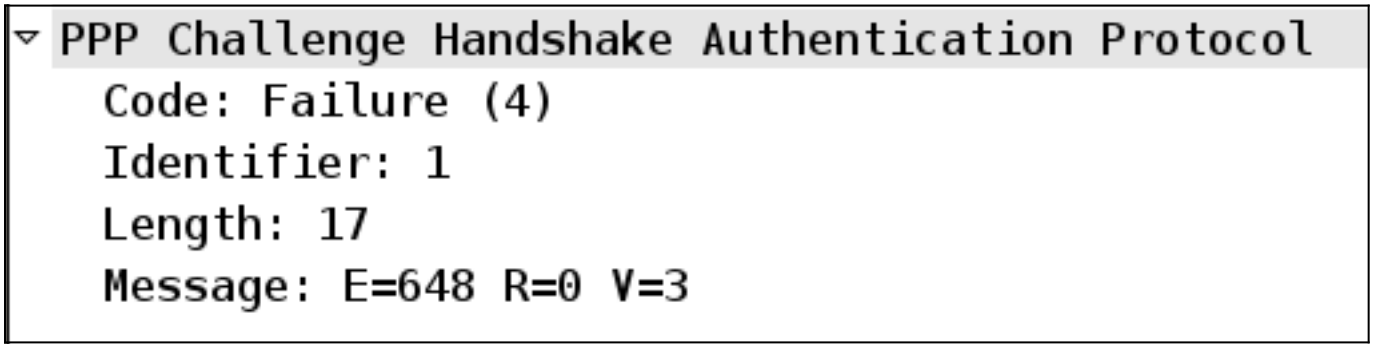
Voor Layer 2 Tunneling Protocol (L2TP) en IPSec wordt PPP gebruikt als transport voor authenticatie. MSCHAPv2 is vereist in plaats van PAP voor een wachtwoordverandering om te werken:

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)# authentication ms-chap-v2
```

Voor uitgebreide verificatie in L2TP binnen de PPP-sessie wordt MSCHAPv2 onderhandeld:



Wanneer het gebruikerswachtwoord is verlopen, wordt een storing met code 648 teruggegeven:



U moet dan een wachtwoord wijzigen. De rest van het proces lijkt sterk op het scenario voor RADIUS met MSCHAPv2.

Zie L2TP over IPsec tussen Windows 2000/XP PC en PIX/ASA 7.2 Gebruik van Pre-Shared Key Configuration Voorbeeld voor extra informatie over de manier waarop u L2TP moet configureren.

ASA SSL VPN-client

De vorige voorbeelden verwezen naar IKEv1 en de Cisco VPN-client, die end-of-life (EOL) is.

De aanbevolen oplossing voor een VPN-toegang op afstand is Cisco AnyConnect Secure Mobility, die de IKE versie 2 (IKEv2) en SSL-protocollen gebruikt. De functies voor het wijzigen van het wachtwoord en het verlopen van het wachtwoord werken precies het zelfde voor Cisco AnyConnect als zij voor de Cisco VPN-client deden.

Voor IKEv1 werden de wachtwoordverandering en de vervalgegevens uitgewisseld tussen de ASA en de VPN-client in fase 1.5 (Xauth/mode configuratie).

voor IKEv2 is het vergelijkbaar; de configuratiemodus gebruikt CFG_REQUEST/CFG_REPLY-pakketten.

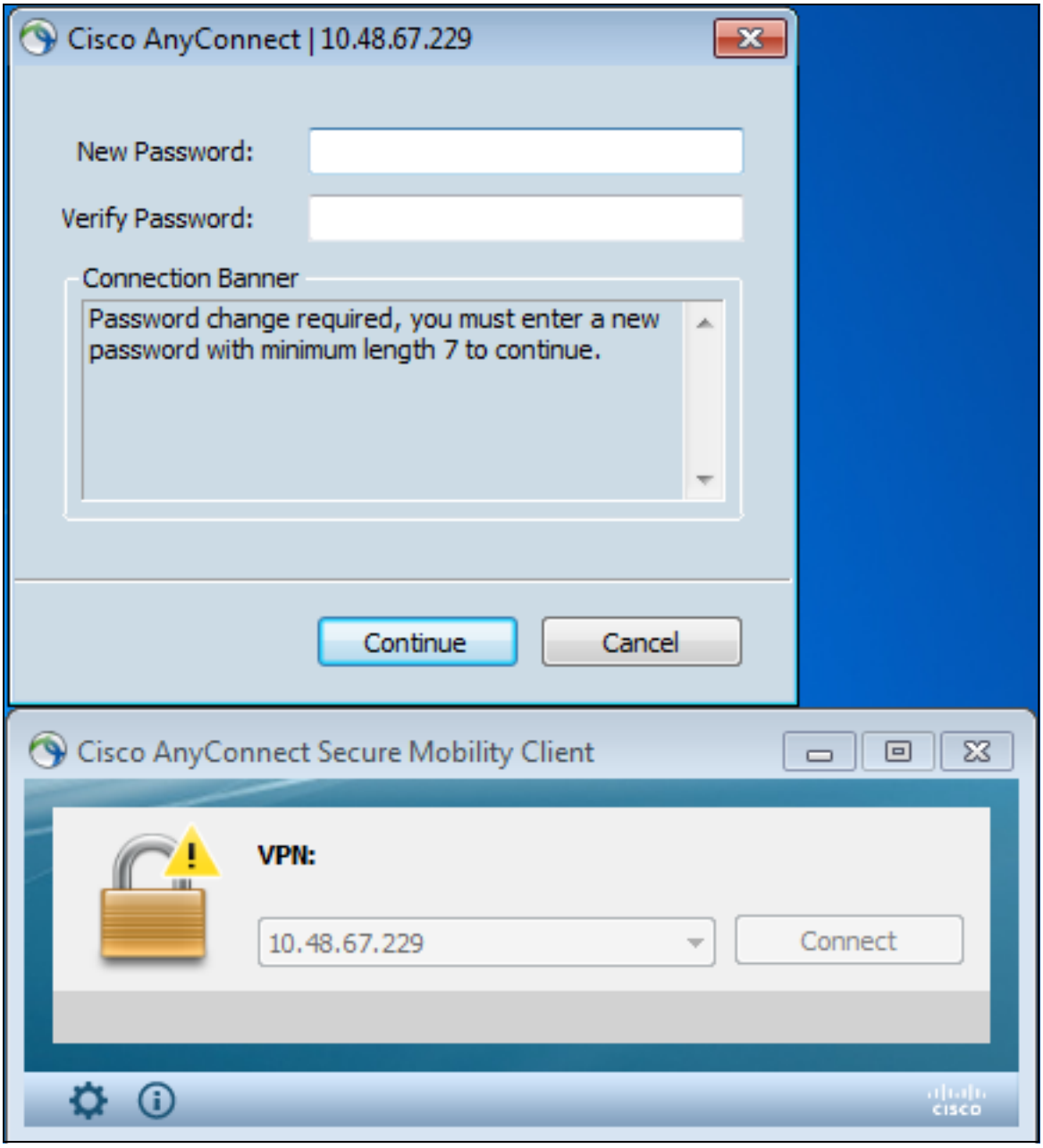
Voor SSL zijn de gegevens in de controle Datagram Transport Layer Security (DTLS) sessie.

De configuratie is hetzelfde voor de ASA.

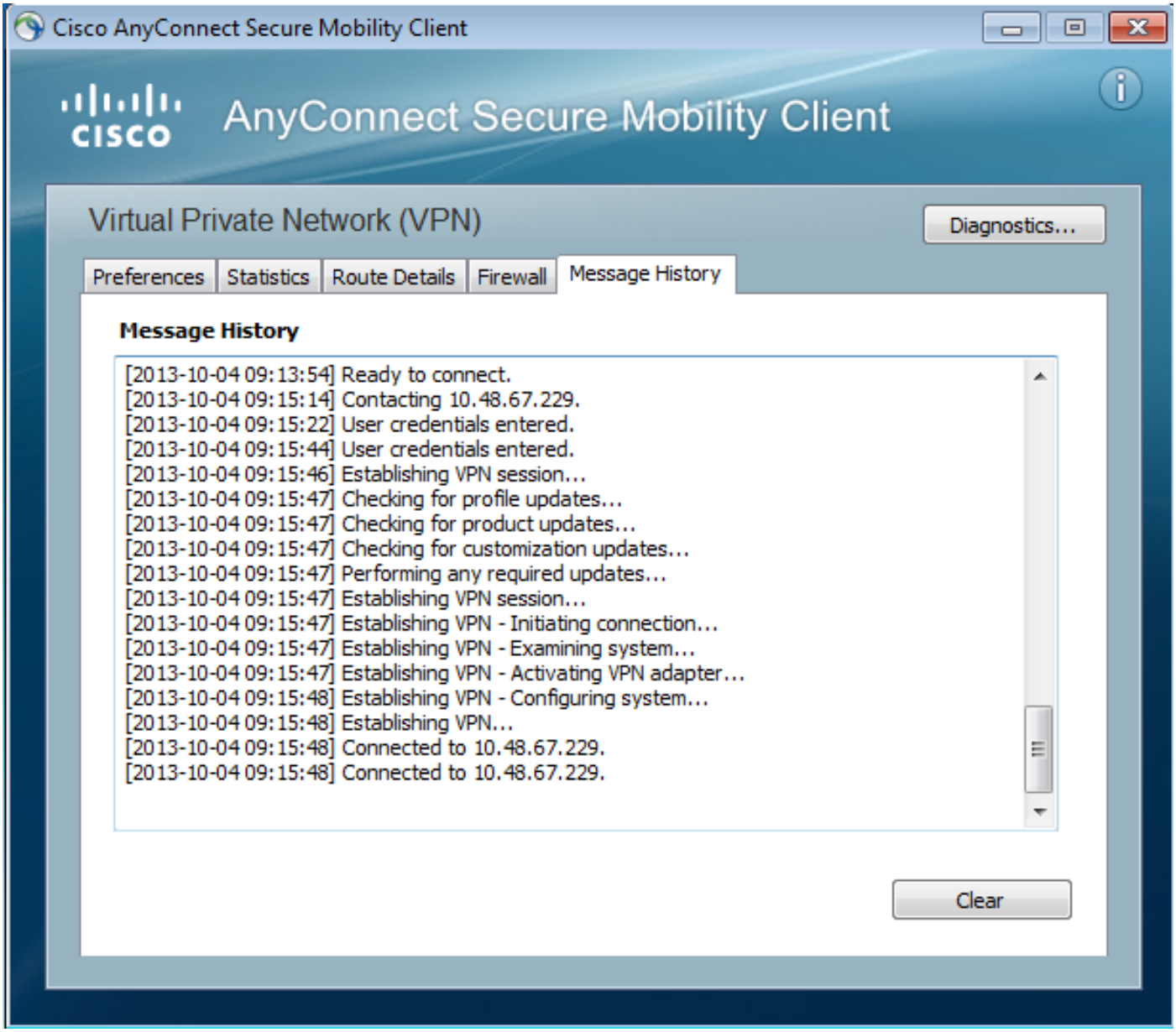
Dit is een voorbeeldconfiguratie met Cisco AnyConnect en het SSL-protocol met een LDAP-server via SSL:

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host win2003-mga.test-cisco.com
 ldap-base-dn CN=Users,DC=test-cisco,DC=com
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn CN=Administrator,CN=users,DC=test-cisco,DC=com
 ldap-over-ssl enable
 server-type microsoft

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy MY internal
group-policy MY attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group LDAP
 default-group-policy MY
 password-management
tunnel-group RA webvpn-attributes
 group-alias RA enable
 without-csd

ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0
```

Zodra het juiste wachtwoord (dat is verlopen) is voorzien, probeert Cisco AnyConnect een nieuw wachtwoord te verbinden en vraagt u om een nieuw wachtwoord:



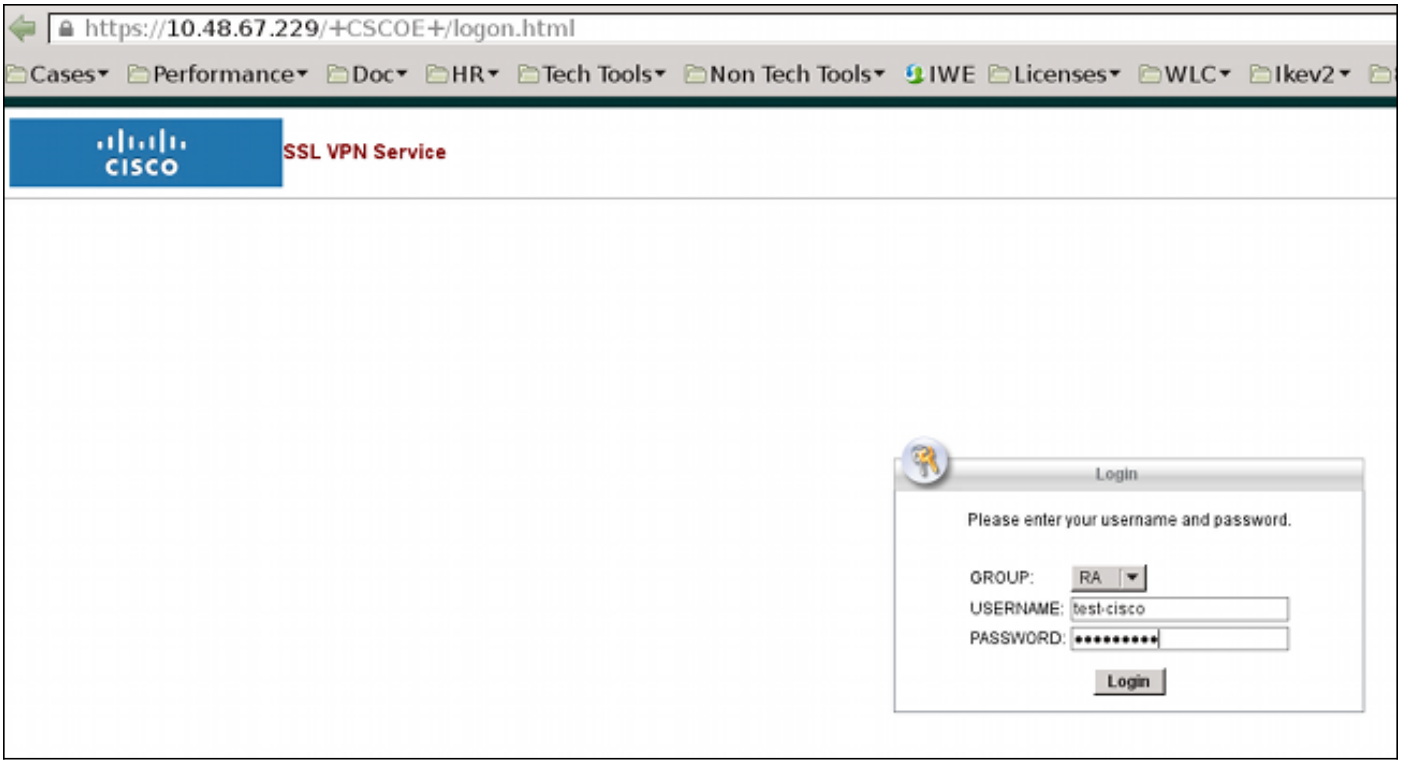
In de logbestanden wordt aangegeven dat de gebruikersreferenties twee keer zijn ingevoerd:



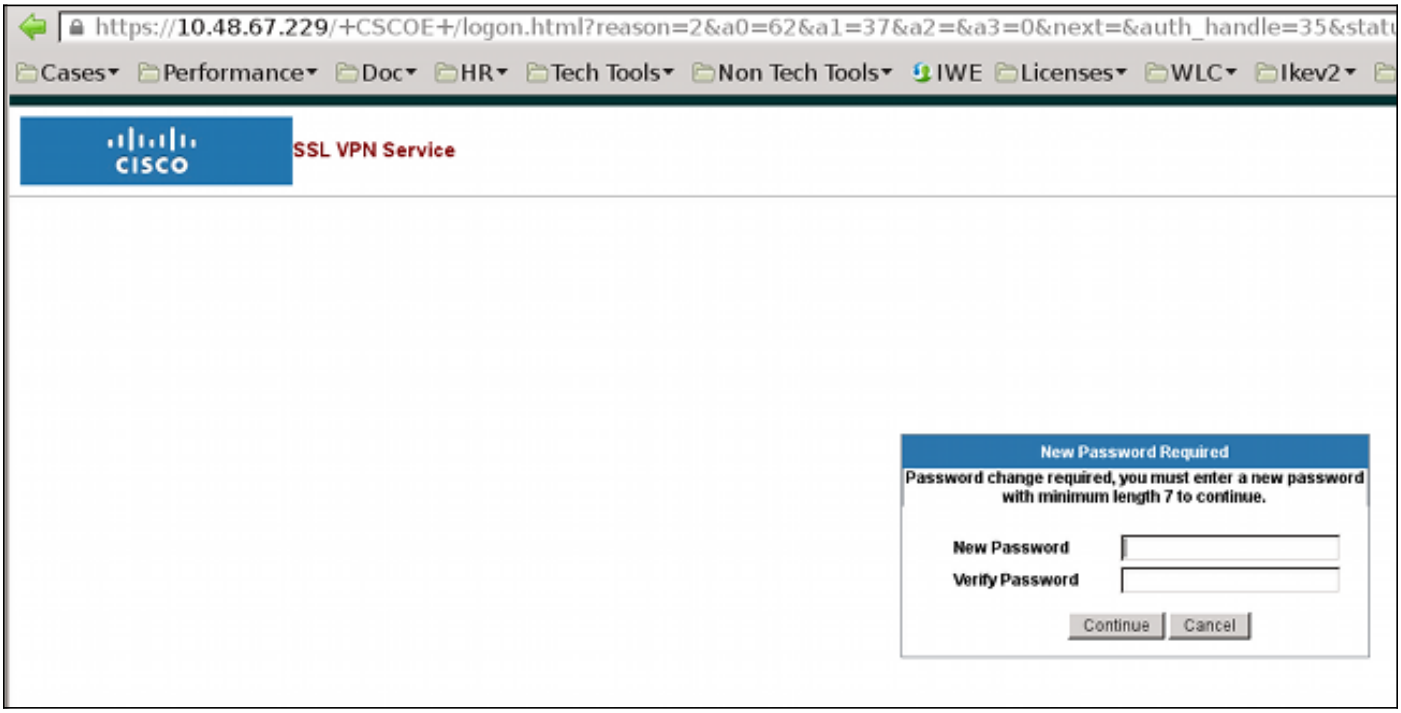
Er zijn gedetailleerdere logbestanden beschikbaar in het Diagnostic AnyConnect Reporting Tool (DART).

ASA SSL-webportal

Dezelfde inlogprocedure vindt plaats op de webportal:



Er is hetzelfde wachtwoord voor het verlopen en het wijzigen van het proces:



ACS-gebruikerswijzigingswachtwoord

Als het niet mogelijk is om het wachtwoord via VPN te wijzigen, kunt u de ACS User Change Password (UCP) speciale webservice gebruiken. Zie Software Development's Guide for Cisco Secure Access Control System 5.4: De UCP Web Services gebruiken.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco ASA 5500 Series configuratiegids met behulp van de CLI, 8.4 en 8.6: Een externe server configureren voor security applicatie, gebruikersautorisatie
- Technische ondersteuning en documentatie – Cisco Systems