802.1x EAP-TLS met een binaire certificaatvergelijking van AD- en NAM-profielen

Inhoud

Inleiding

Dit document beschrijft de configuratie 802.1x met Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) en Access Control System (ACS), aangezien zij een binaire certificaatvergelijking uitvoeren tussen een client-certificaat dat door de aanvrager is geleverd en hetzelfde certificaat dat in Microsoft Active Directory (AD) wordt bewaard. Het AnyConnect Network Access Manager (NAM) profiel wordt gebruikt voor aanpassing. De configuratie voor alle onderdelen wordt in dit document weergegeven, samen met de scenario's voor het oplossen van problemen in de configuratie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

Configureren

Topologie

- 802.1x applicatie - Windows 7 met Cisco AnyConnect Secure Mobility Client release 3.1.010/65 (NAM-module)
- 802.1x authenticator - 2960 switch
- 802.1x verificatieserver - ACS release 5.4
- ACS geïntegreerd met Microsoft AD - Domain Controller - Windows 2008-server

Details topologie

- ACS - 192.168.10.152
- 2960 - 192.168.10.10 (e0/0 - aangesloten op smeekbede)
- DC - 19.2.168.10.101
- Windows 7 - DHCP

Flow

Op het Windows 7-station is AnyConnect NAM geïnstalleerd, dat als zodanig wordt gebruikt om met de EAP-TLS-methode op de ACS-server te bevestigen. De switch met 802.1x treedt in als authentiek. Het gebruikerscertificaat wordt door het ACS gecontroleerd en de beleidsvergunning past een beleid toe dat gebaseerd is op de gemeenschappelijke naam (GN) van het certificaat. Bovendien halen de ACS het gebruikerscertificaat van AD en voeren zij een binaire vergelijking uit met het door de aanvrager verstrekte certificaat.

Switch-configuratie

De switch heeft een basisconfiguratie. Standaard is de poort in quarantaine VLAN 666. Dat VLAN

heeft een beperkte toegang. Nadat de gebruiker is geautoriseerd, wordt de poort-VLAN opnieuw geconfigureerd.

```
aaa authentication login default group radius local
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control

interface Ethernet0/0
switchport access vlan 666
switchport mode access
ip device tracking maximum 10
duplex auto
authentication event fail action next-method
authentication order dot1x mab
authentication port-control auto
dot1x pae authenticator
end

radius-server host 192.168.10.152 auth-port 1645 acct-port 1646 key cisco
```

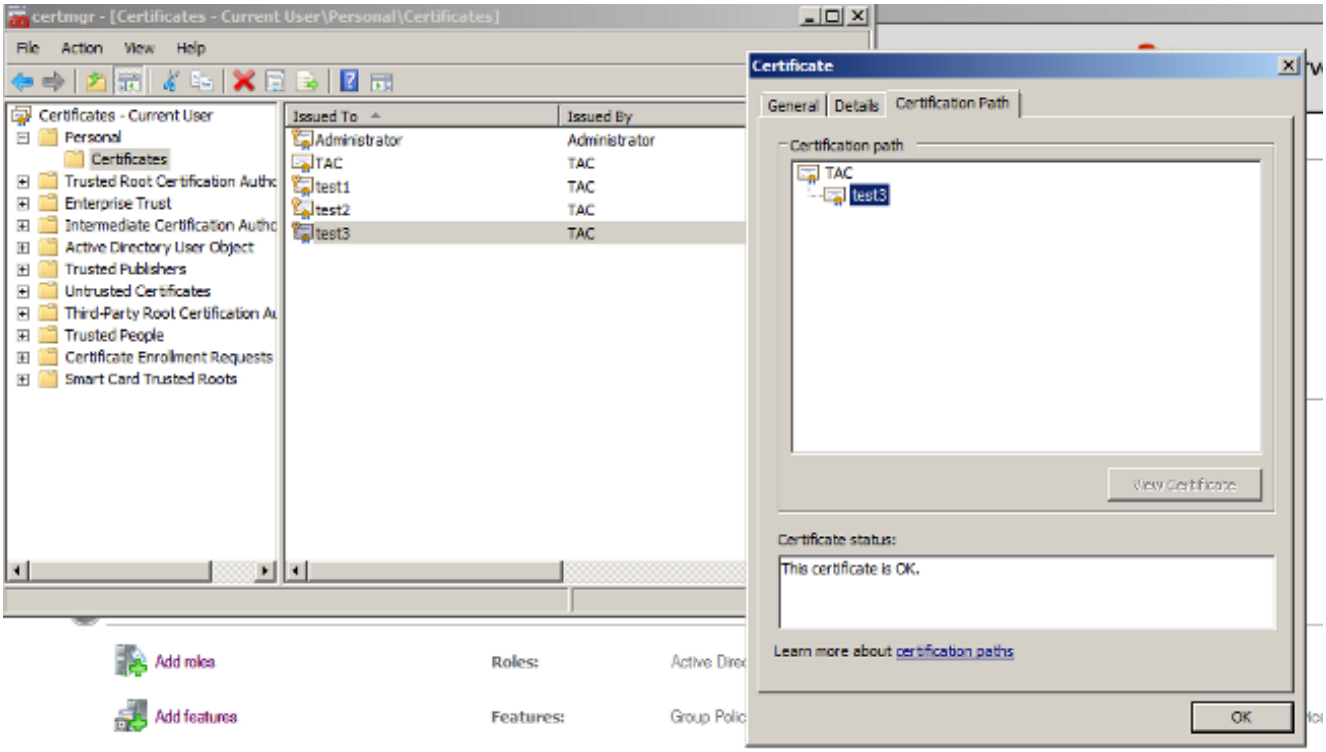
Voorbereiding van het certificaat

Voor EAP-TLS is een certificaat vereist voor zowel de aanvrager als de authenticatieserver. Dit voorbeeld is gebaseerd op OpenSSL gegenereerde certificaten. Microsoft certificaatinstantie (CA) kan worden gebruikt om de implementatie in ondernemingsnetwerken te vereenvoudigen.

1. U kunt de CA als volgt genereren:
   ```
   openssl genrsa -des3 -out ca.key 1024
   openssl req -new -key ca.key -out ca.csr
   cp ca.key ca.key.org
   openssl rsa -in ca.key.org -out ca.key
   openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
   ```
   Het CA-certificaat wordt bewaard in het ca.crt-bestand en de privétoets (en onbeschermd) in het bestand ca.key.
2. Drie gebruikerscertificaten en een certificaat voor ACS genereren, allemaal ondertekend door die CA: CN=test1CN=test2CN=test3GN=acs54Het script dat gebruikt wordt om één certificaat te genereren dat ondertekend is door Cisco's CA is:
   ```
   openssl genrsa -des3 -out server.key 1024
   openssl req -new -key server.key -out server.csr

   cp server.key server.key.org
   openssl rsa -in server.key.org -out server.key

   openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial
   -out server.crt -days 365
   openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
   -certfile ca.crt
   ```
   De privé sleutel is in het server.key bestand en het certificaat is in het server.crt bestand. De PC12 versie is in het server.pfx bestand.
3. Dubbelklik op elk certificaat (.pfx-bestand) om het in de Domain Controller te importeren. In de Domain Controller zouden alle drie de certificaten moeten worden vertrouwd.

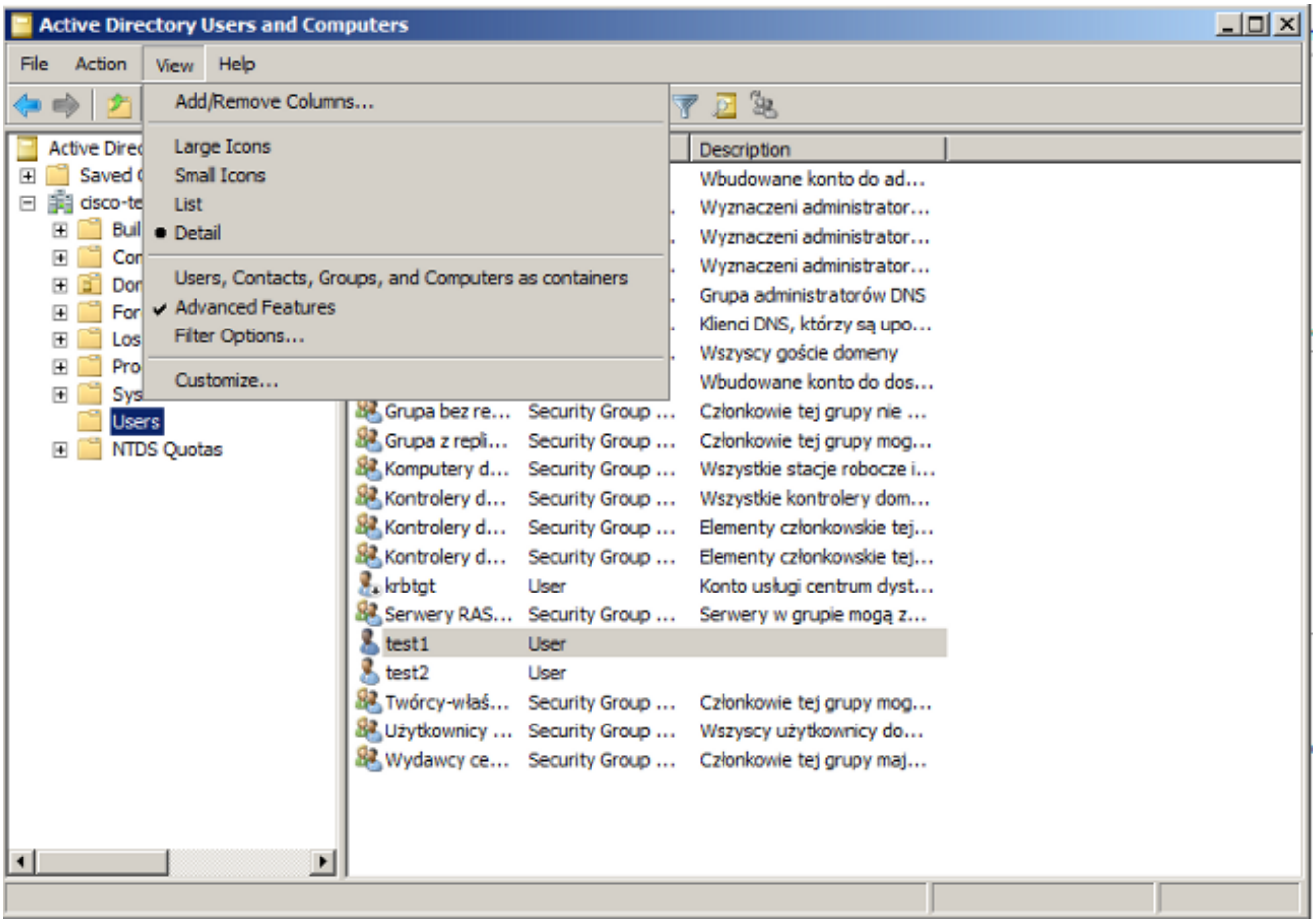


Hetzelfde proces kan in Windows 7 (smeekbede) worden gevolgd of actieve map worden gebruikt om de gebruikerscertificaten aan te drukken.

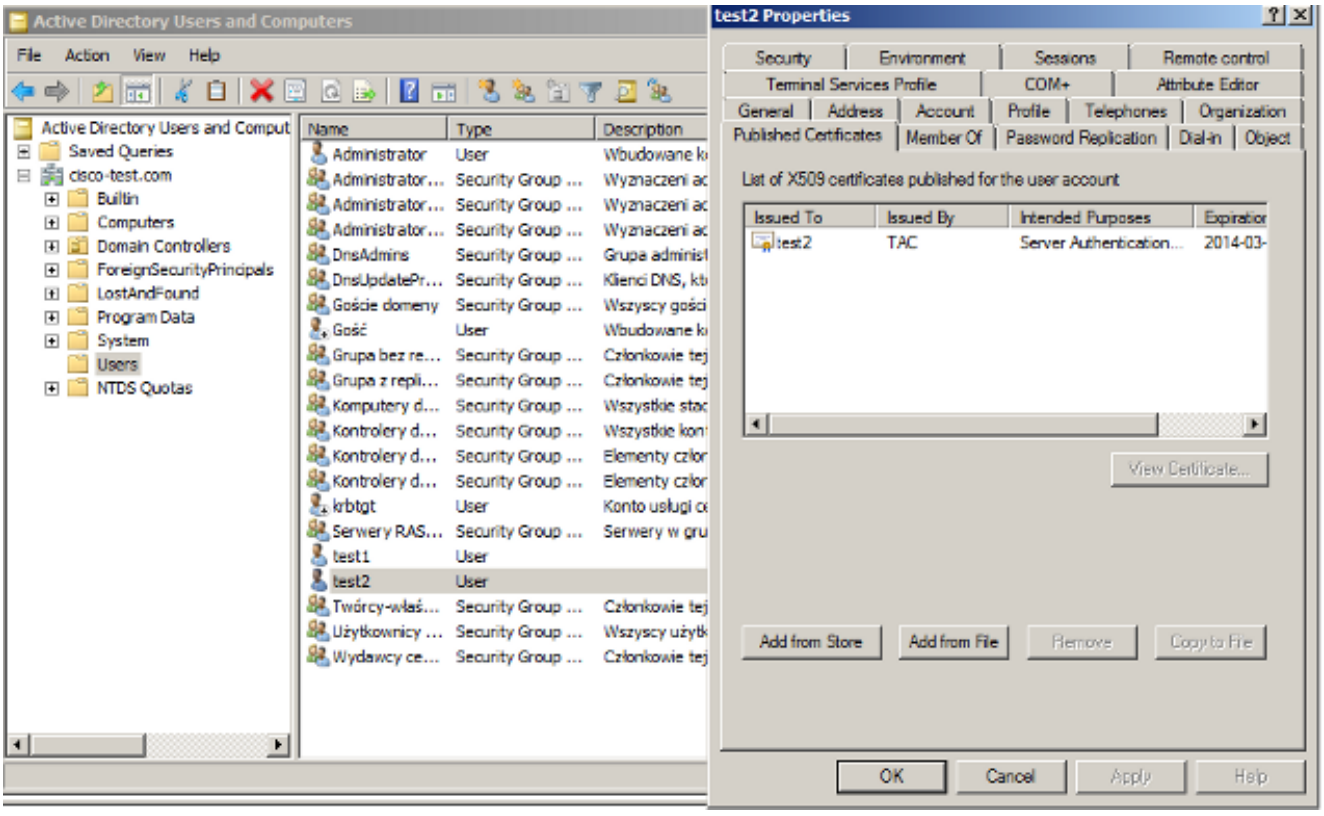
Configuratie van controller

Het specifieke certificaat moet in kaart worden gebracht aan de specifieke gebruiker in AD.

1. Vanuit Active Directory-gebruikers en -computers navigeer naar de **gebruikersmap**.
2. Kies in het menu Beeld de optie **Geavanceerde functies**.



3. Voeg deze gebruikers toe: test1test2test3**Opmerking:** Het wachtwoord is niet belangrijk.
4. Kies in het venster Eigenschappen het tabblad **Gepubliceerde certificaten**. Kies het specifieke certificaat voor de test. Bijvoorbeeld, voor test1 is de gebruiker CN test1.**Opmerking:** Gebruik geen Name mapping (klik met de rechtermuisknop op de gebruikersnaam). Het wordt gebruikt voor verschillende diensten.



In dit stadium is het certificaat gebonden aan een specifieke gebruiker in AD. Dit kan worden

geverifieerd met behulp van ldapsearch:

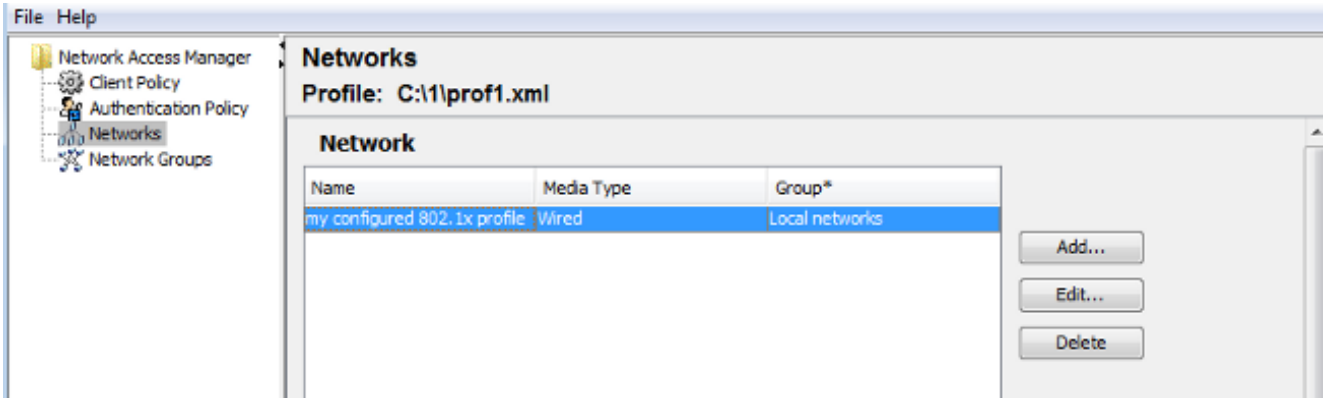
```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
Adminpass -b "DC=cisco-test,DC=com"
```

De resultaten van test2 zijn als volgt:

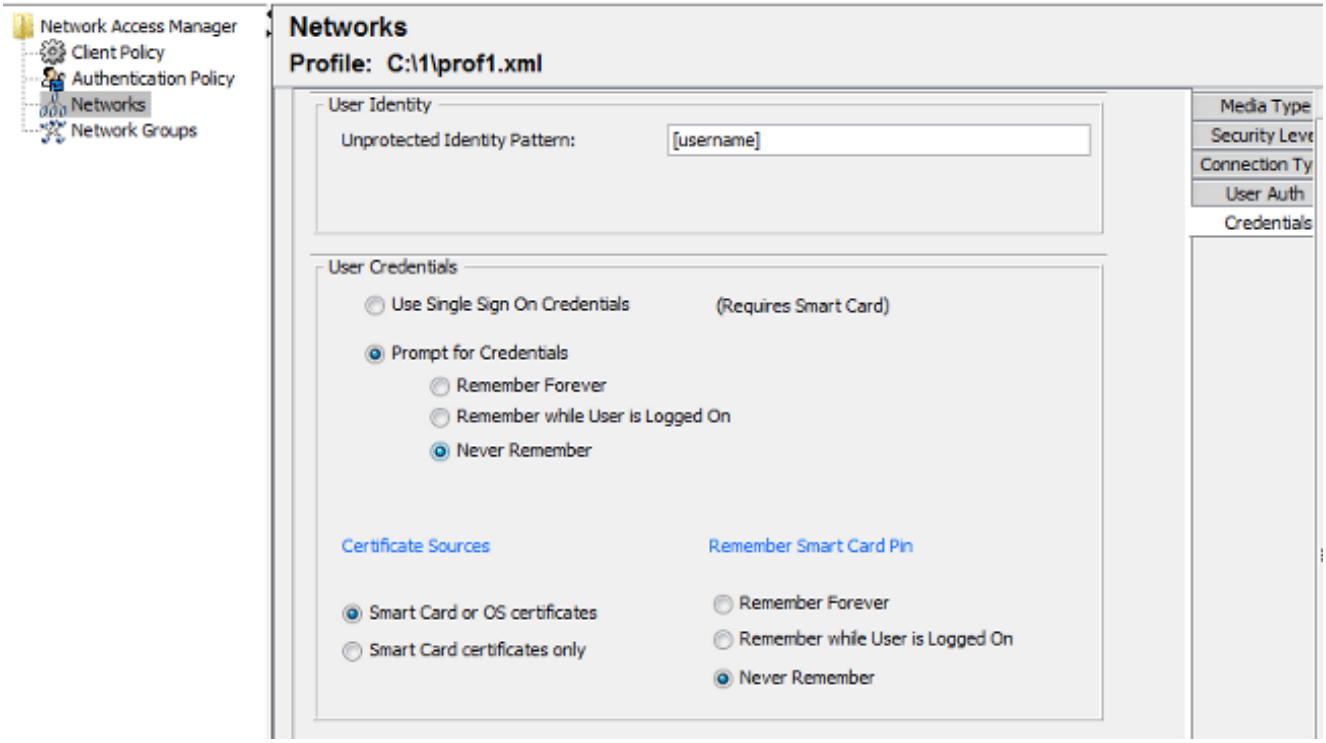
```
# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
.................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF
oxCzAJBgNVBAYTAlBMMQswCQYDVQQIDAJQTDEPMA0GA1UEBwwGS3Jha293MQ4wDAYDVQQKDAVDaXN
jbzENMAsGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs8qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav8HYD
aRznaK1LURt1PeGtHlcTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR
iZpXC444eKOh6wO/+yWb4bAgMBAAGjgYkwgYYwCwYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU
FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC
FQYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJKwYBBAGCNxUGBggrBgEFBQcDAjANBgkqhkiG9w0BA
QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmCtH7Pn+VILagf9o
tiFl5ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCeZRoxfAO94n
PulwF4nkcnu1xO/B7x+LpcjxjhQ==
```

Configuratie van leveranciers

1. Installeer deze profieleditor, anyconnect-profileeditor-win-3.1.00495-k9.exe.
2. Open de editor van het netwerktoegangsprofiel en bevestig het specifieke profiel.
3. Maak een specifiek bekabeld netwerk.



In dit stadium is het van groot belang de gebruiker de keuze te geven het certificaat bij elke echtheidscontrole te gebruiken. Stel die keuze niet in. Gebruik ook de "gebruikersnaam" als de onbeschermde identificatie. Het is belangrijk eraan te herinneren dat het niet dezelfde identificatie is die door ACS wordt gebruikt om AD voor het certificaat te vragen. Die hulp zal in ACS worden
ingesteld.

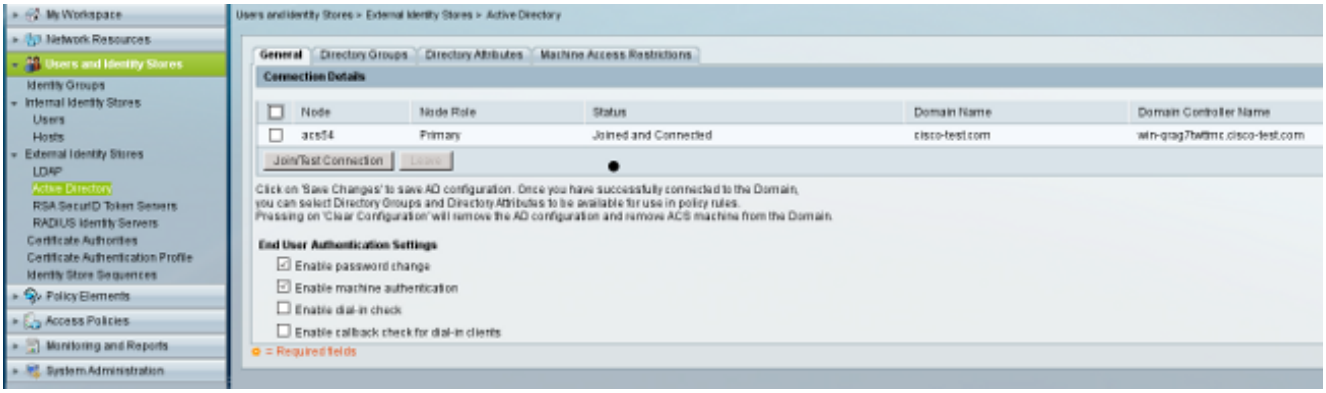


4. Het bestand .xml opslaan als c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
5. Start de Cisco AnyConnect NAM-service opnieuw.

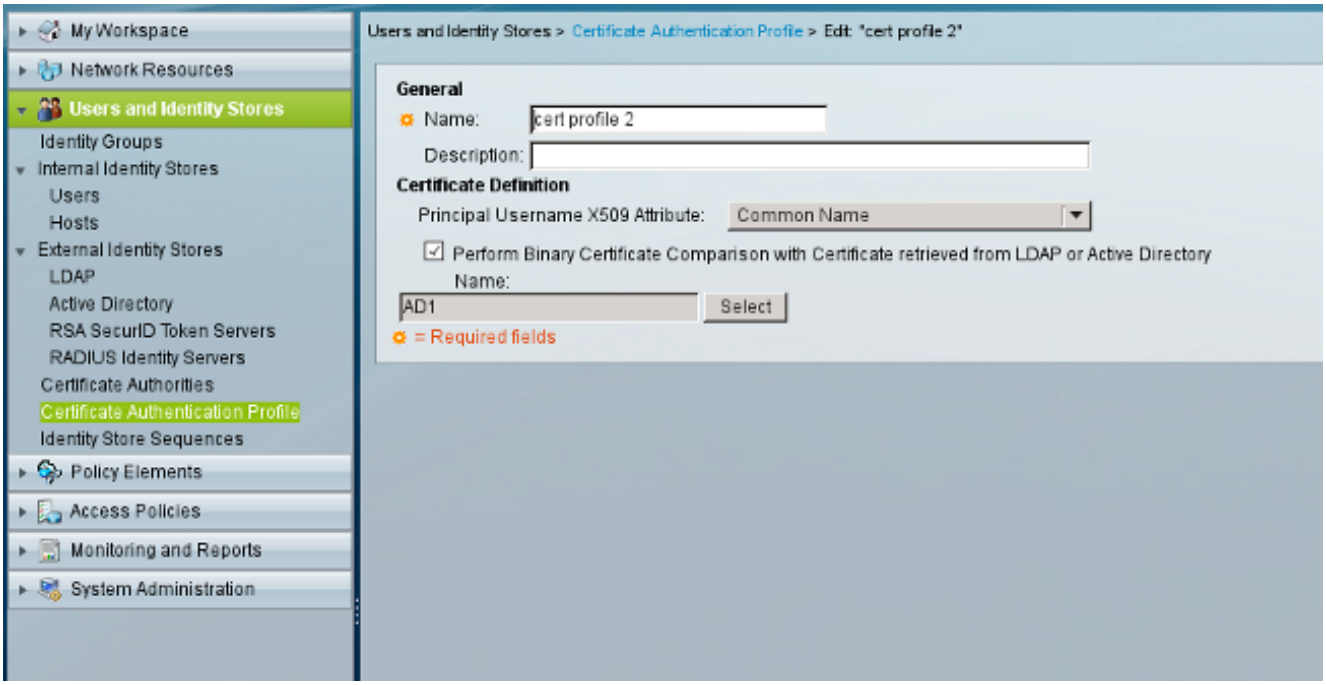
Dit voorbeeld toonde een handmatige profielplaatsing. AD zou kunnen worden gebruikt om dat bestand voor alle gebruikers in te voeren. ASA zou ook kunnen worden gebruikt om het profiel te voorzien bij integratie met VPN's.

ACS-configuratie

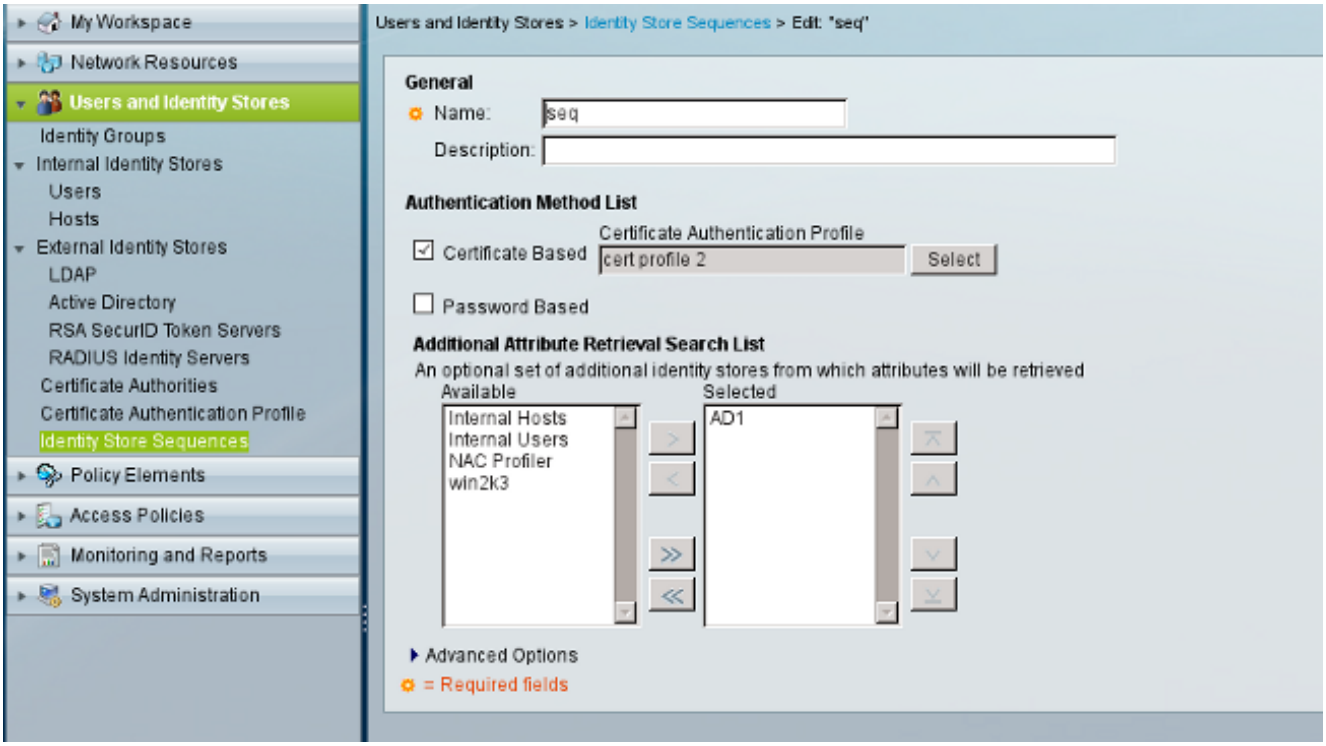
1. Doe mee met het AD-domein.



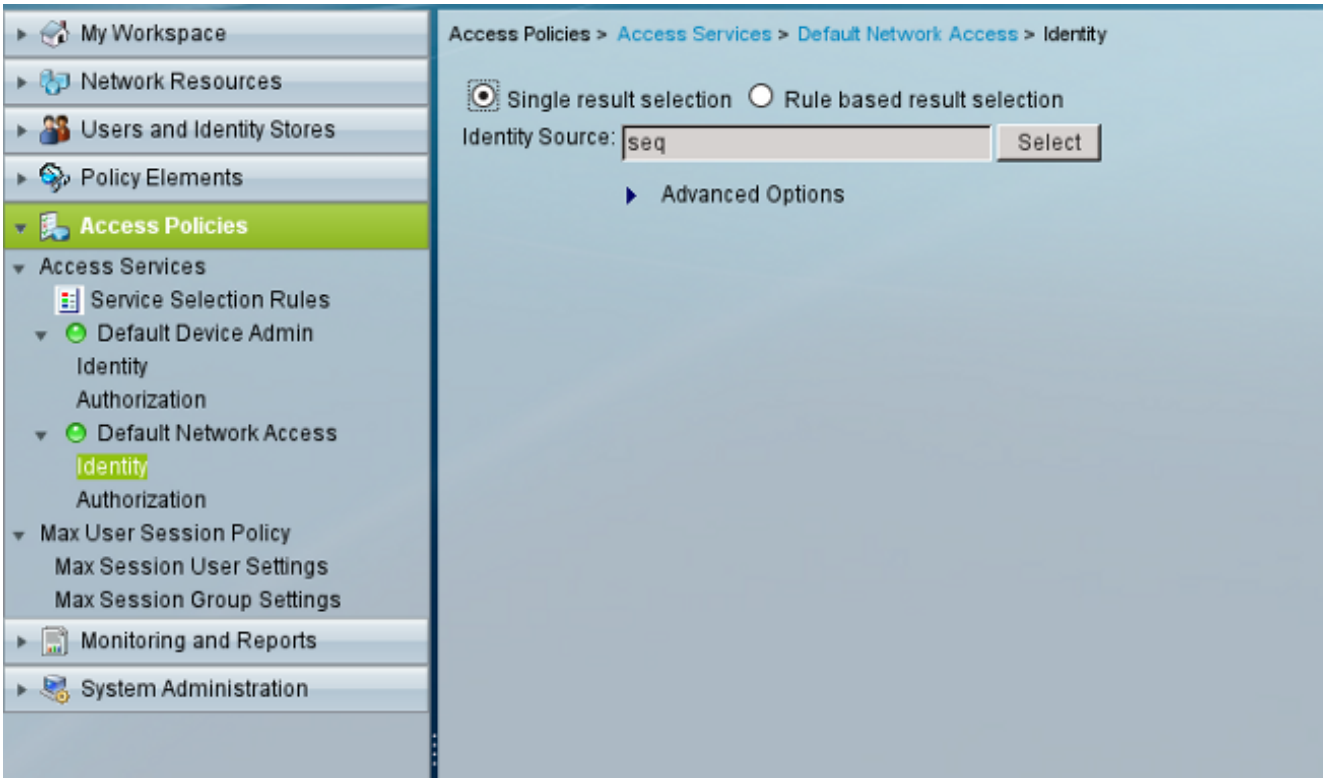
ACS komt overeen met AD-gebruikersnamen met gebruikmaking van het GN-veld van het certificaat dat van de aanvrager is ontvangen (in dit geval is het test1, test2 of test3). Binaire vergelijking wordt ook ingeschakeld. Dit dwingt ACS om het gebruikerscertificaat van AD te verkrijgen en vergelijkt het met het zelfde certificaat dat door de aanvrager wordt ontvangen. Als deze niet overeenkomt, faalt de authenticatie.



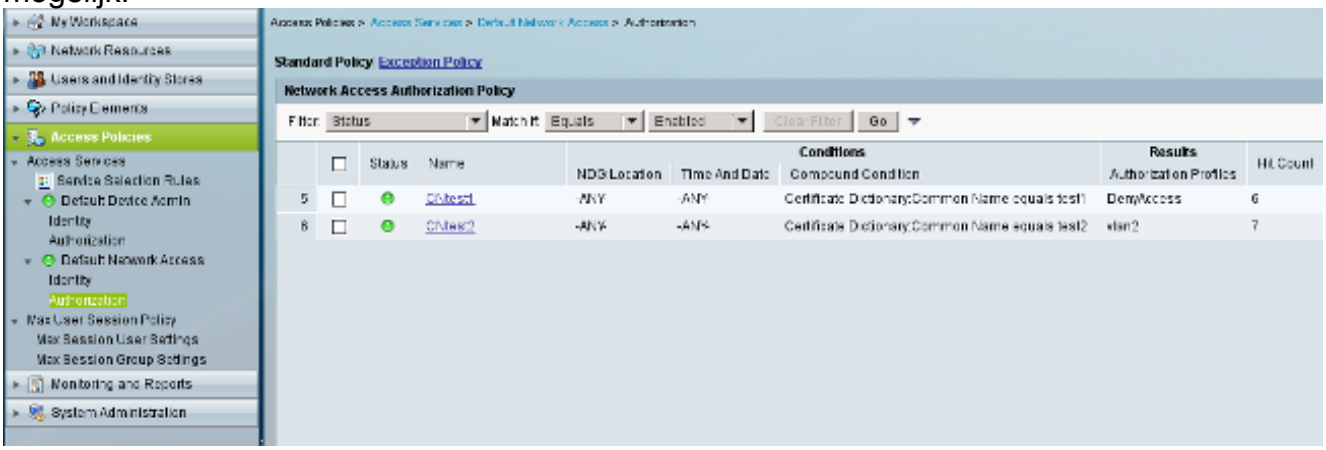
2. Configureer de sequenties van de Identity Store. Deze zijn gebaseerd op AD voor certificatie op basis van certificaten en hebben tevens betrekking op het certificeringsprofiel.



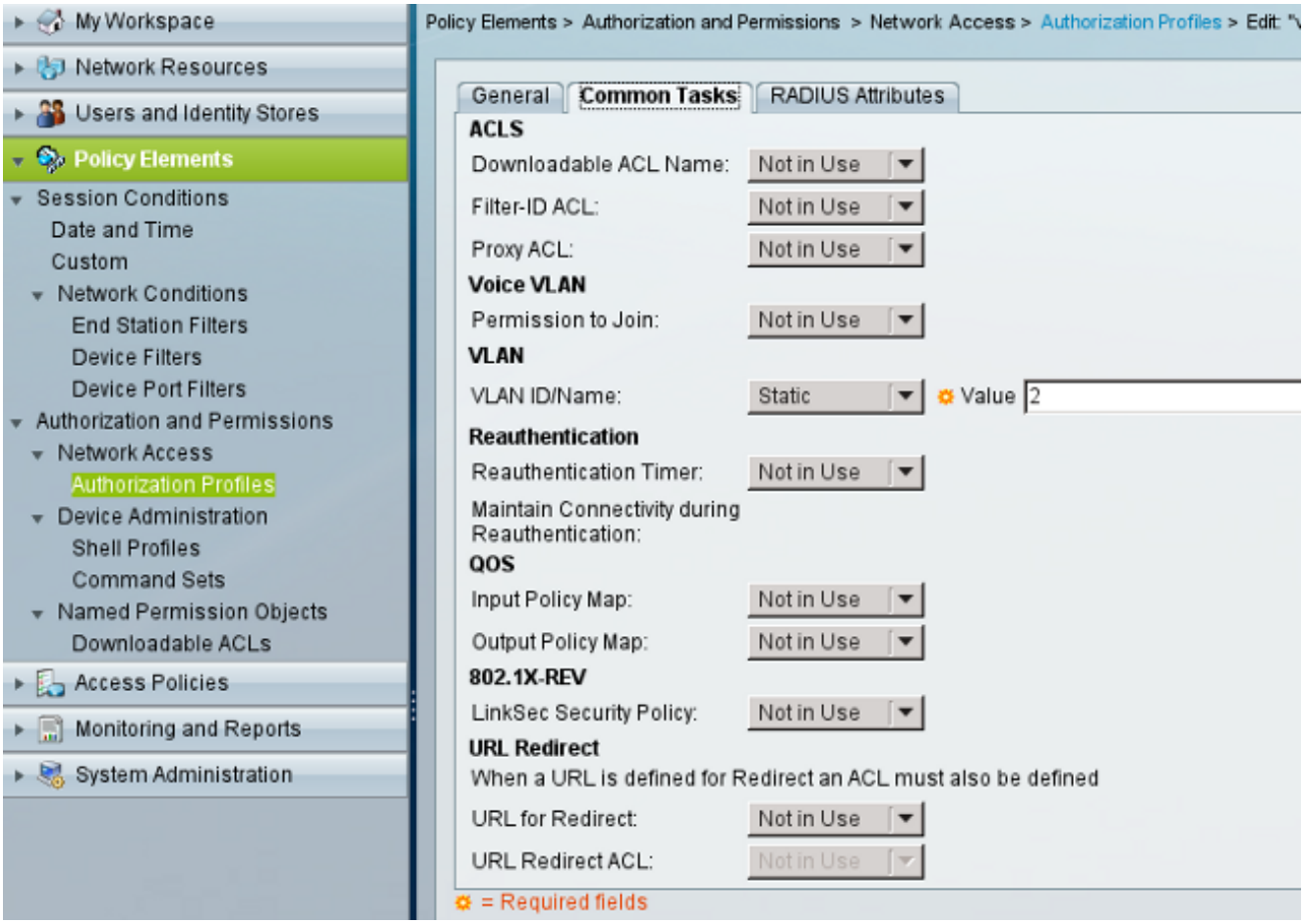
Dit wordt gebruikt als de Bron van de Identiteit in het beleid van de Identiteit van de RADIUS.



3. Configureer twee autorisatiebeleid. Het eerste beleid wordt gebruikt voor test1 en ontkent toegang tot die gebruiker. Het tweede beleid wordt gebruikt voor test 2 en het maakt toegang met het VLAN2 profiel
mogelijk.

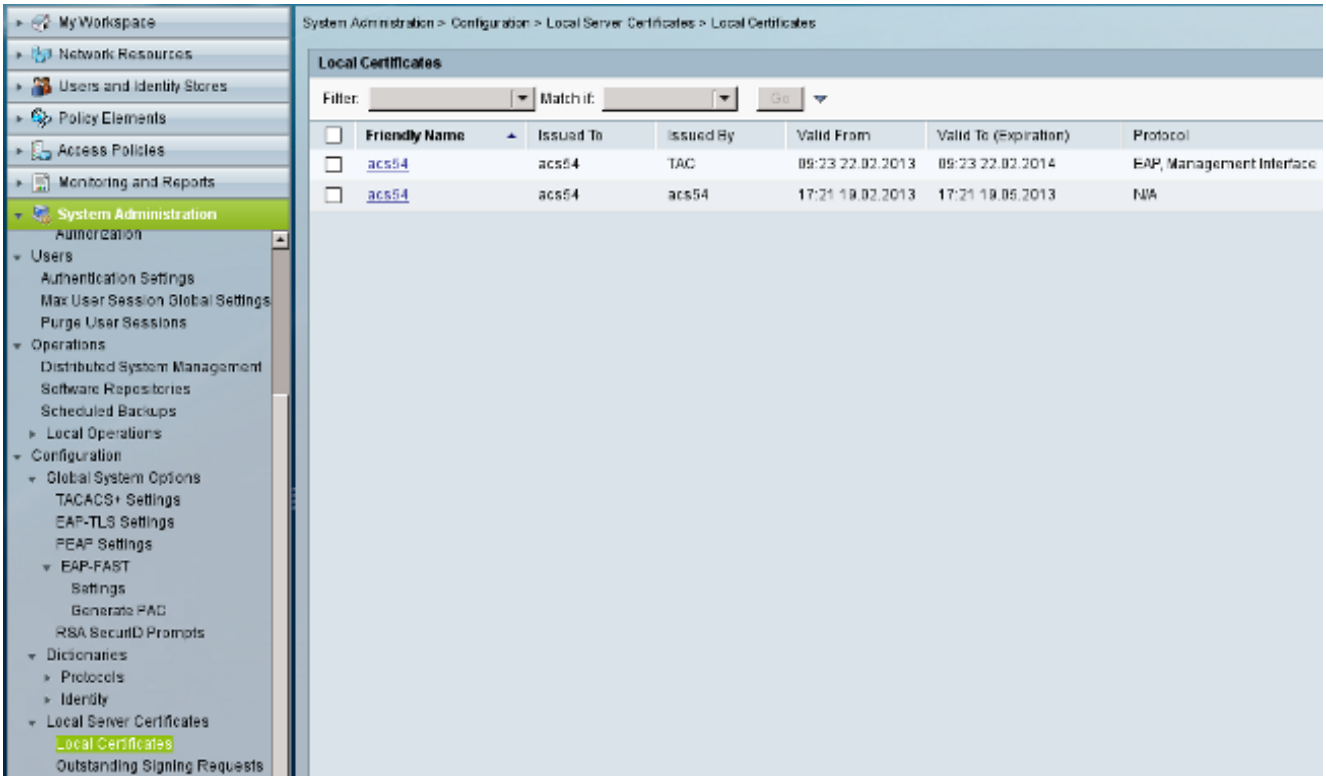


VLAN2 is het autorisatieprofiel dat de eigenschappen van de RADIUS teruggeeft die de gebruiker aan VLAN2 op de switch
binden.



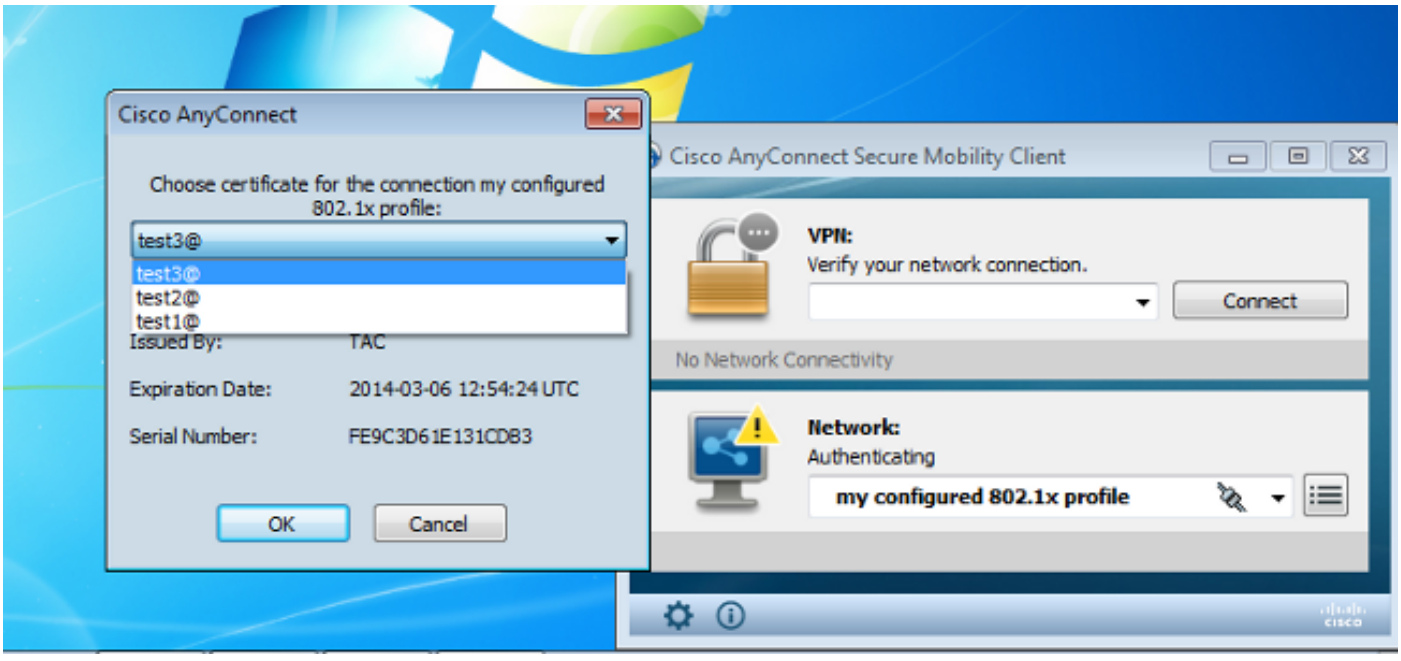
4. Installeer het CA-certificaat op ACS.

5. Generate en installeer het certificaat (voor Verlenbaar Verificatieprotocol) dat door Cisco's CA voor ACS wordt ondertekend.



Verifiëren

Het is een goede praktijk om native 802.1x-service op de Windows 7-applicatie uit te schakelen omdat AnyConnect NAM wordt gebruikt. Bij het ingestelde profiel mag de client een specifiek certificaat selecteren.



Wanneer het test2 certificaat wordt gebruikt, ontvangt de switch een succesrespons samen met de RADIUS-kenmerken.

```
00:02:51: %DOT1X-5-SUCCESS: Authentication successful for client
(0800.277f.5f64) on Interface Et0/0
00:02:51: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x'
for client (0800.277f.5f64) on Interface Et0/0
```

```
switch#
00:02:51: %EPM-6-POLICY_REQ: IP=0.0.0.0| MAC=0800.277f.5f64|
       AUDITSESID=C0A80A0A00000001000215F0| AUTHTYPE=DOT1X|
       EVENT=APPLY

switch#show authentication sessions interface e0/0
           Interface:  Ethernet0/0
          MAC Address:  0800.277f.5f64
           IP Address:  Unknown
           User-Name:  test2
           Status:  Authz Success
           Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  2
      Session timeout:  N/A
         Idle timeout:  N/A
   Common Session ID:  C0A80A0A00000001000215F0
      Acct Session ID:  0x00000005
           Handle:  0xE8000002

Runnable methods list:
      Method   State
      dot1x    Authc Succes
```

Merk op dat VLAN 2 is toegewezen. Het is mogelijk andere RADIUS-kenmerken aan dat autorisatieprofiel toe te voegen op ACS (zoals geavanceerde toegangscontrolelijst of hermachtigingstermijnen).

De logbestanden op ACS zijn als volgt:

12813 Extracted TLS CertificateVerify message.
12804 Extracted TLS Finished message.
12801 Prepared TLS ChangeCipherSpec message.
12802 Prepared TLS Finished message.
12816 TLS handshake succeeded.
12509 EAP-TLS full handshake finished successfully
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006 Matched Default Rule
24432 Looking up user in Active Directory - test2
24416 User's Groups retrieval from Active Directory succeeded
24469 The user certificate was retrieved from Active Directory successfully.
22054 Binary comparison of certificates succeeded.
22037 Authentication Passed
22023 Proceed to attribute retrieval
22038 Skipping the next IDStore for attribute retrieval because it is the one we authenticated against
22016 Identity sequence completed iterating the IDStores
Evaluating Group Mapping Policy
12506 EAP-TLS authentication succeeded
11503 Prepared EAP-Success
Evaluating Exception Authorization Policy
15042 No rule was matched
Evaluating Authorization Policy
15004 Matched rule
15016 Selected Authorization Profile - vlan2
22065 Max sessions policy passed
22064 New accounting session created in Session cache
11002 Returned RADIUS Access-Accept

Problemen oplossen

Ongeldige tijdinstellingen voor ACS

Mogelijke fout - interne fout in ACS actieve map

12504 Extracted EAP-Response containing EAP-TLS challenge-response
12571 ACS will continue to CRL verification if it is configured for specific CA
12571 ACS will continue to CRL verification if it is configured for specific CA
12811 Extracted TLS Certificate message containing client certificate.
12812 Extracted TLS ClientKeyExchange message.
12813 Extracted TLS CertificateVerify message.
12804 Extracted TLS Finished message.
12801 Prepared TLS ChangeCipherSpec message.
12802 Prepared TLS Finished message.
12816 TLS handshake succeeded.
12509 EAP-TLS full handshake finished successfully
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006 Matched Default Rule
24432 Looking up user in Active Directory - test1
24416 User's Groups retrieval from Active Directory succeeded
24463 Internal error in the ACS Active Directory
22059 The advanced option that is configured for process failure is used.
22062 The 'Drop' advanced option is configured in case of a failed authentication request.

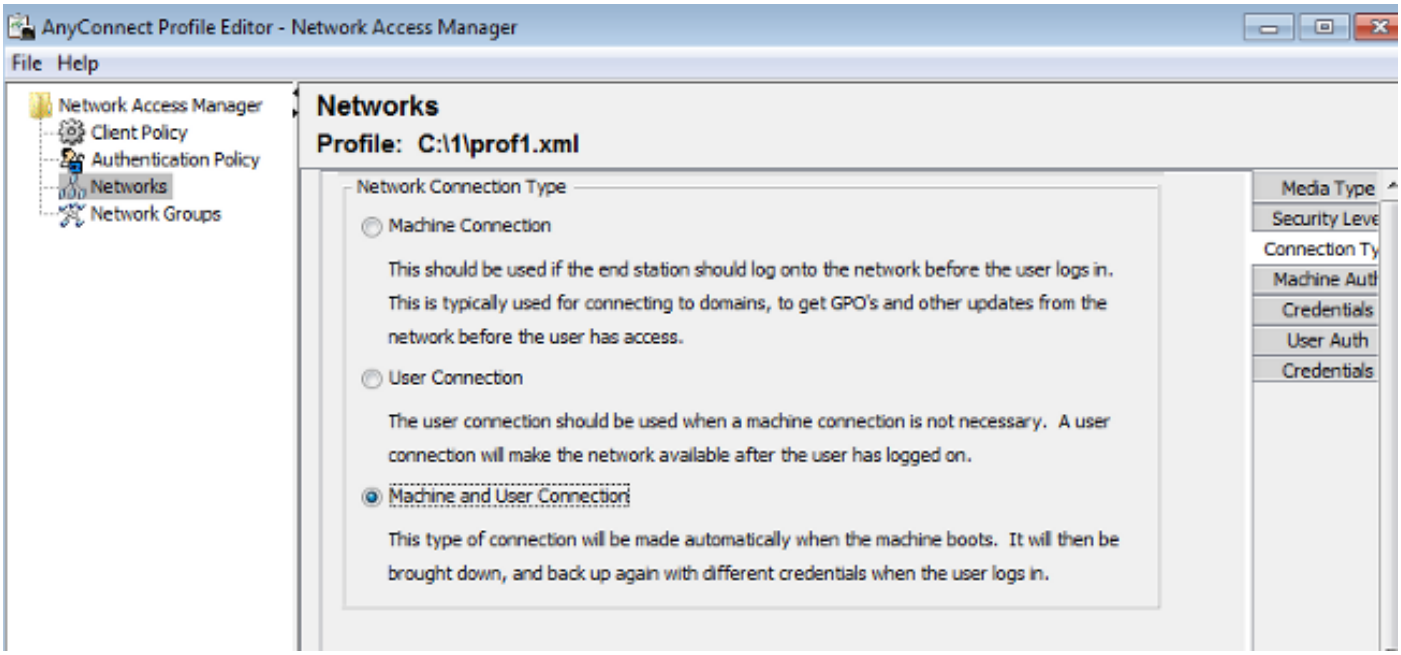
Geen certificaat ingesteld en gebonden op AD DC

Mogelijke fout - heeft het gebruikerscertificaat niet uit actieve map opgehaald

12571 ACS will continue to CRL verification if it is configured for specific CA
12811 Extracted TLS Certificate message containing client certificate.
12812 Extracted TLS ClientKeyExchange message.
12813 Extracted TLS CertificateVerify message.
12804 Extracted TLS Finished message.
12801 Prepared TLS ChangeCipherSpec message.
12802 Prepared TLS Finished message.
12816 TLS handshake succeeded.
12509 EAP-TLS full handshake finished successfully
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006 Matched Default Rule
24432 Looking up user in Active Directory - test2
24416 User's Groups retrieval from Active Directory succeeded
24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.
24468 Failed to retrieve the user certificate from Active Directory.
22049 Binary comparison of certificates failed
22057 The advanced option that is configured for a failed authentication request is used.
22061 The 'Reject' advanced option is configured in case of a failed authentication request.
12507 EAP-TLS authentication failed
11504 Prepared EAP-Failure
11003 Returned RADIUS Access-Reject

Aanpassing van NAM-profiel

In Enterprise-netwerken is het raadzaam zowel de machine- als de gebruikerscertificaten te authentiseren. In dat geval is het raadzaam de modus open 802.1x op de switch met beperkt VLAN te gebruiken. Na het opnieuw opstarten van de machine voor 802.1x, wordt de eerste authenticatiesessie gestart en gewaarmerkt met het gebruik van het AD machine certificaat. Daarna, nadat de gebruiker geloofsbrieven en loggen op het domein verstrekt, wordt de tweede authentificatiesessie begonnen met het gebruikerscertificaat. De gebruiker wordt in het juiste (vertrouwde) VLAN gezet met volledige netwerktoegang. Het is volledig geïntegreerd in Identity Services Engine (ISE).



Vervolgens kan u afzonderlijke authenticaties configureren naast de tabbladen Machine en Gebruikersverificatie.

Als de modus 802.1x open niet acceptabel is op de switch, kan de 802.1x-modus worden gebruikt voordat de inlogfunctie is ingesteld in het clientbeleid.

Gerelateerde informatie

- Gebruikershandleiding voor Cisco Secure Access Control System 5.3
- Cisco AnyConnect Secure Mobility Client-beheerdershandleiding, release 3.0
- AnyConnect Secure Mobility Client 3.0: Network Access Manager en Profile Editor voor Windows
- Technische ondersteuning en documentatie – Cisco Systems