Configureer de ISE voor integratie met een LDAP-server

Inhoud

Inleiding

Dit document beschrijft hoe u een Cisco Identity Services Engine (ISE) kunt configureren voor integratie met een Cisco Light Directory Access Protocol (LDAP) server.

> **Opmerking:** Dit document is geldig voor instellingen die LDAP als externe identiteitsbron voor de ISE-verificatie en -vergunning gebruiken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie die dit document bevat, is gebaseerd op deze software- en hardwareversies:

- Cisco ISE versie 1.3 met patch 2
- Microsoft Windows versie 7 x64 met OpenLDAP geïnstalleerd
- Cisco draadloze LAN-controller (WLC) versie 8.0.10.0
- Cisco AnyConnect versie 3.1 voor Microsoft Windows
- Cisco Network Access Manager-profiel

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.

Achtergrondinformatie

Deze authenticatiemethoden worden ondersteund met LDAP:

- Extenteerbaar verificatieprotocol, --generieke Token-kaart (EAP-GTC)
- Extensible Authentication Protocol, - Transport Layer Security (EAP-TLS)
- Beschermd Extensible Authentication Protocol, - Transport Layer Security (PEAP-TLS)

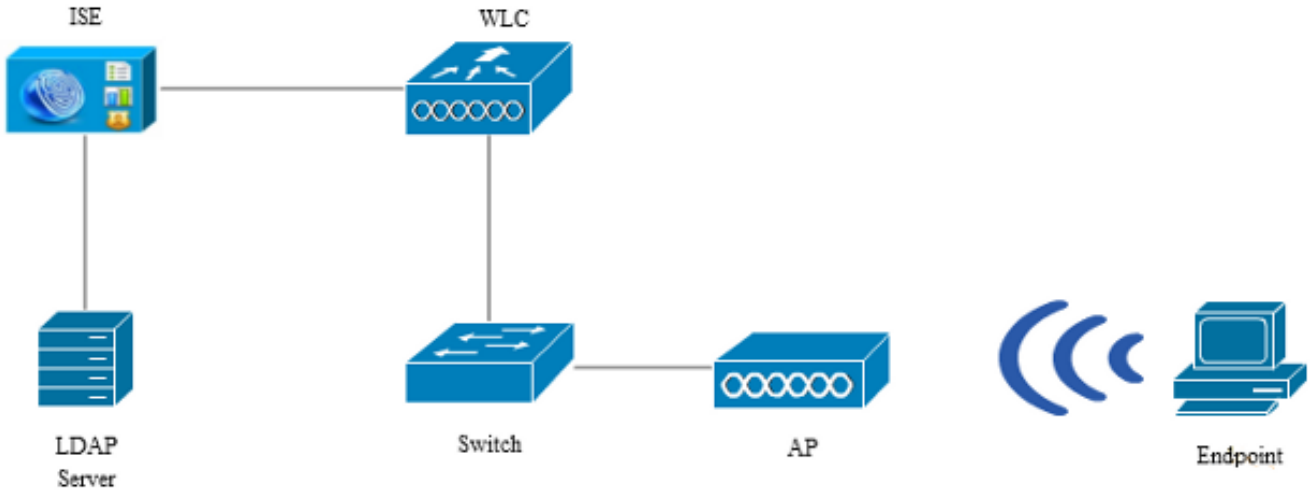
Configureren

In dit deel wordt beschreven hoe u de netwerkapparaten kunt configureren en de ISE met een LDAP-server kunt integreren.

Netwerkdiagram

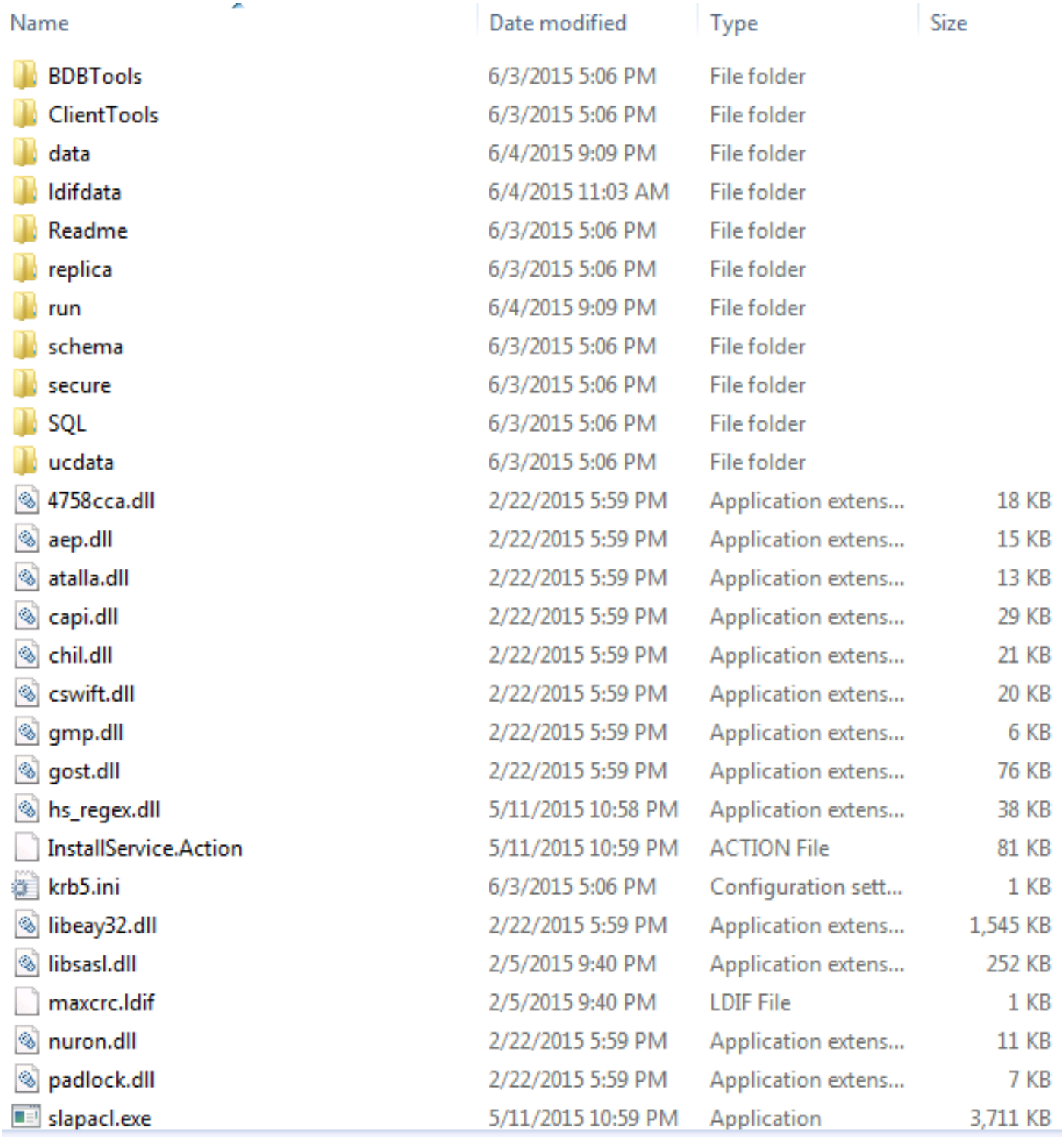
In dit configuratievoorbeeld gebruikt het eindpunt een draadloze adapter om aan het draadloze netwerk te associëren. Het draadloze LAN (WLAN) op de WLC wordt geconfigureerd om de gebruikers via de ISE te authentiseren. Op ISE wordt LDAP ingesteld als een extern identiteitsarchief.

Dit beeld illustreert de netwerktopologie die wordt gebruikt:



OpenLDAP configureren

De installatie van OpenLDAP voor Microsoft Windows is voltooid via de GUI, en is eenvoudig. De standaardlocatie is **C: > OpenLDAP**. Na installatie dient u deze map te bekijken:



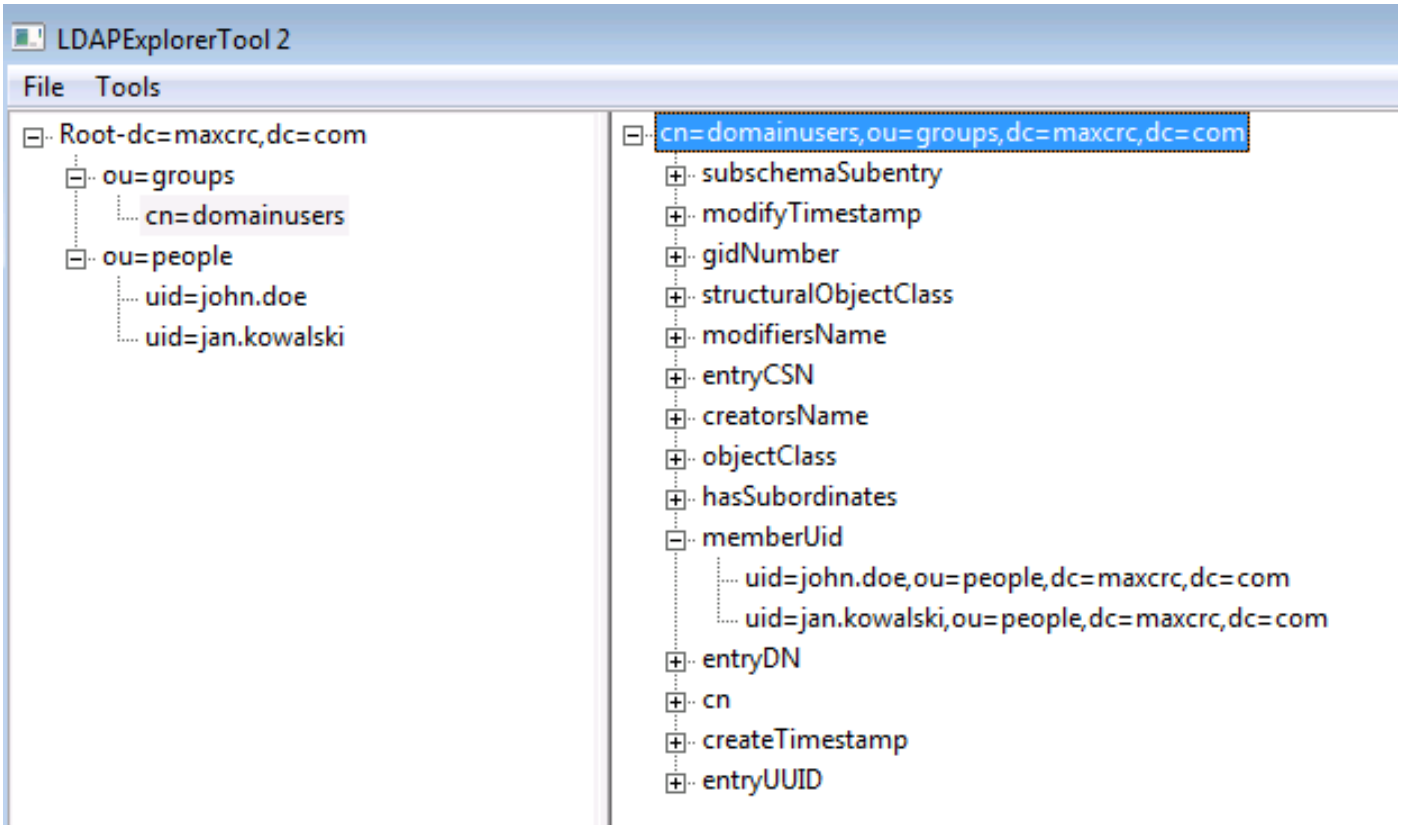
Name	Date modified	Type	Size
BDBTools	6/3/2015 5:06 PM	File folder	
ClientTools	6/3/2015 5:06 PM	File folder	
data	6/4/2015 9:09 PM	File folder	
ldifdata	6/4/2015 11:03 AM	File folder	
Readme	6/3/2015 5:06 PM	File folder	
replica	6/3/2015 5:06 PM	File folder	
run	6/4/2015 9:09 PM	File folder	
schema	6/3/2015 5:06 PM	File folder	
secure	6/3/2015 5:06 PM	File folder	
SQL	6/3/2015 5:06 PM	File folder	
ucdata	6/3/2015 5:06 PM	File folder	
4758cca.dll	2/22/2015 5:59 PM	Application extens...	18 KB
aep.dll	2/22/2015 5:59 PM	Application extens...	15 KB
atalla.dll	2/22/2015 5:59 PM	Application extens...	13 KB
capi.dll	2/22/2015 5:59 PM	Application extens...	29 KB
chil.dll	2/22/2015 5:59 PM	Application extens...	21 KB
cswift.dll	2/22/2015 5:59 PM	Application extens...	20 KB
gmp.dll	2/22/2015 5:59 PM	Application extens...	6 KB
gost.dll	2/22/2015 5:59 PM	Application extens...	76 KB
hs_regex.dll	5/11/2015 10:58 PM	Application extens...	38 KB
InstallService.Action	5/11/2015 10:59 PM	ACTION File	81 KB
krb5.ini	6/3/2015 5:06 PM	Configuration sett...	1 KB
libeay32.dll	2/22/2015 5:59 PM	Application extens...	1,545 KB
libsasl.dll	2/5/2015 9:40 PM	Application extens...	252 KB
maxcrc.ldif	2/5/2015 9:40 PM	LDIF File	1 KB
nuron.dll	2/22/2015 5:59 PM	Application extens...	11 KB
padlock.dll	2/22/2015 5:59 PM	Application extens...	7 KB
slapacl.exe	5/11/2015 10:59 PM	Application	3,711 KB

Neem met name nota van twee gidsen:

- **Clienttools** ß-Hiermee deze folder een reeks binaire gegevens bevat die worden gebruikt om de LDAP-database te bewerken.

- **ldifdata** ß$ Dit is de locatie waar je de bestanden moet opslaan met LDAP objecten.

Voeg deze structuur toe aan de LDAP-database:



Onder de folder van de *Root*, moet u twee Organisatorische Eenheden (OUs) configureren. De *OU=groepen* OU dient één kindergroep te hebben (**cn=dominee gebruikers** in dit voorbeeld). De *OU=people* OU definieert de twee gebruikersaccounts die behoren tot de groep *cn=dominee*.

U moet eerst het *ldif*-bestand maken om de database te vullen. De hierboven genoemde structuur is gemaakt uit dit bestand:

```
dn: ou=groups,dc=maxcrc,dc=com
changetype: add
ou: groups
description: All groups in organisation
objectclass: organizationalunit

dn: ou=people,dc=maxcrc,dc=com
changetype: add
ou: people
description: All people in organisation
objectclass: organizationalunit

dn: uid=john.doe,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: john.doe
givenName: John
sn: Doe
cn: John Doe
mail: john.doe@example.com
userPassword: password

dn: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
changetype: add
```

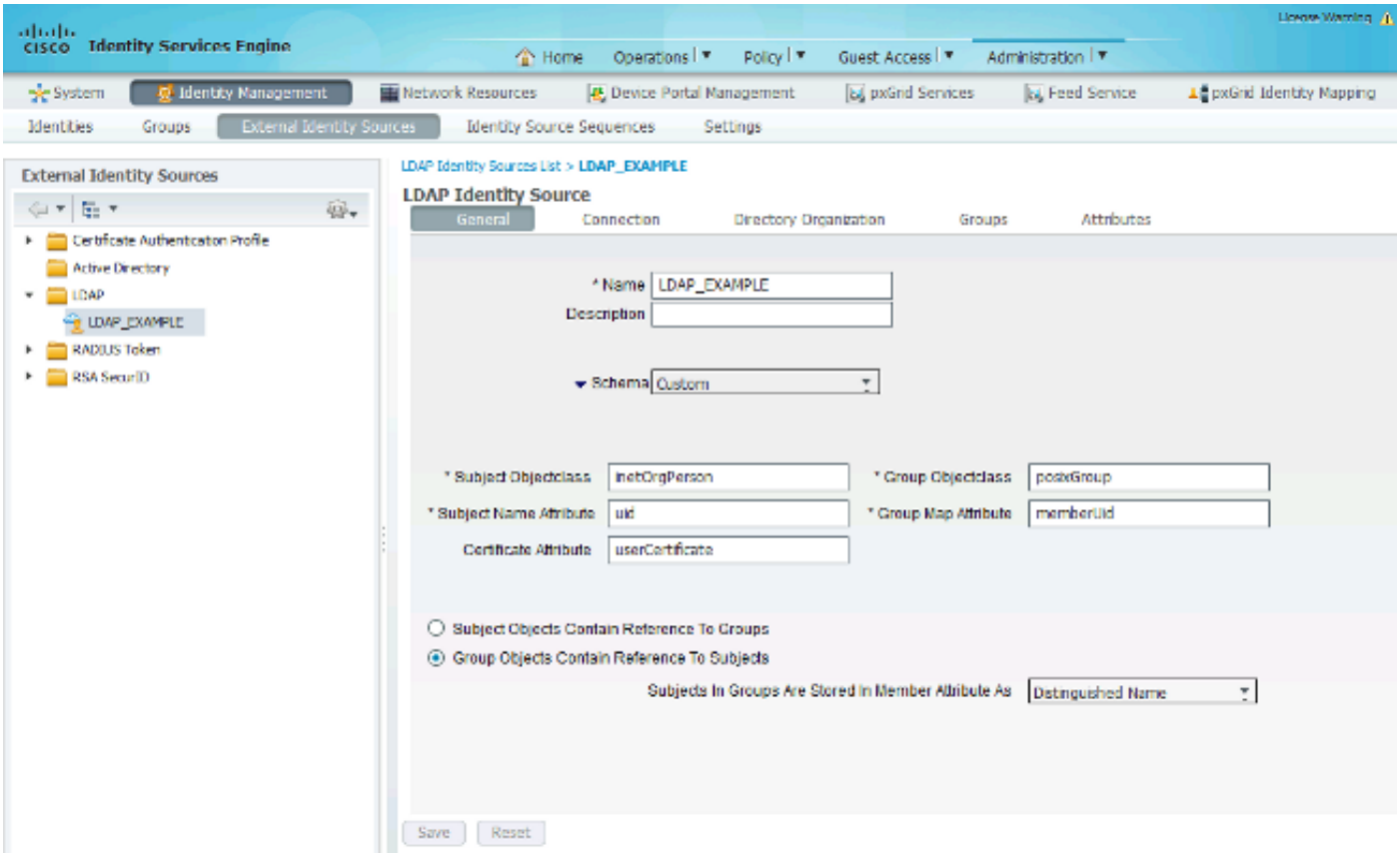
```
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: jan.kowalski
givenName: Jan
sn: Kowalski
cn: Jan Kowalski
mail: jan.kowalski@example.com
userPassword: password

dn: cn=domainusers,ou=groups,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: posixGroup
gidNumber: 678
memberUid: uid=john.doe,ou=people,dc=maxcrc,dc=com
memberUid: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
```

Om de objecten aan de LDAP database toe te voegen, kunt u het **ldapchange** binaire bestand gebruiken:

```
C:\OpenLDAP\ClientTools>ldapmodify.exe -a -x -h localhost -p 389 -D "cn=Manager,
dc=maxcrc,dc=com" -w secret -f C:\OpenLDAP\ldifdata\test.ldif
ldap_connect_to_host: TCP localhost:389
ldap_new_socket: 496
ldap_prepare_socket: 496
ldap_connect_to_host: Trying ::1 389
ldap_pvt_connect: fd: 496 tm: -1 async: 0
attempting to connect:
connect success
adding new entry "ou=groups,dc=maxcrc,dc=com"

adding new entry "ou=people,dc=maxcrc,dc=com"

adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"

adding new entry "cn=domainusers,ou=groups,dc=maxcrc,dc=com"
```

OpenLDAP met ISE integreren

Gebruik de informatie in de beelden door deze sectie om LDAP te configureren als een extern identiteitsbestand op ISE.



U kunt deze eigenschappen configureren vanuit het tabblad *Algemeen*:

- **Onderwerp Objectklasse** ßHiermee komt het veld overeen met de doelklasse van de gebruikersrekeningen in het *ldif*-bestand. Zoals in de LDAP configuratie, kunt u hier een van vier klassen gebruiken:

  Boven

  persoon

  Organisator

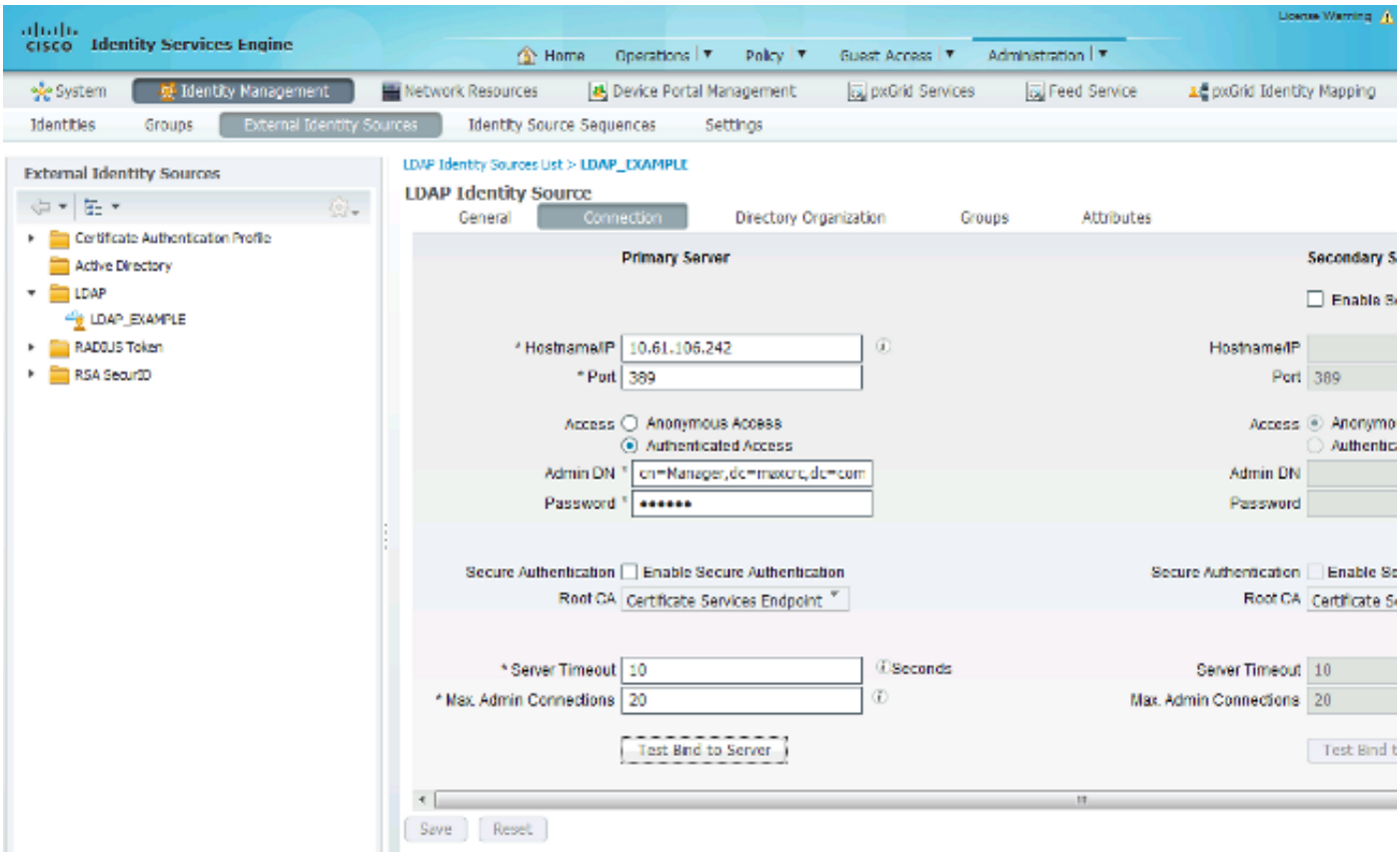
  InetOrgPerson

- **Onderwerp Naam kenmerk** ß-Hiermee wordt de eigenschap gegeven die door de LDAP wordt opgehaald wanneer de ISE vraagt of een specifieke gebruikersnaam in een database is opgenomen. In dit scenario moet u **john.doe** of **jan.kowalski** gebruiken als de gebruikersnaam op het eindpunt.

- **Groep Objectclass** ß XIV Dit veld komt overeen met de objectklasse voor een groep in het *ldif*-bestand. In dit scenario is de objectklasse voor de *cn=dominee* groep **posixGroup**.

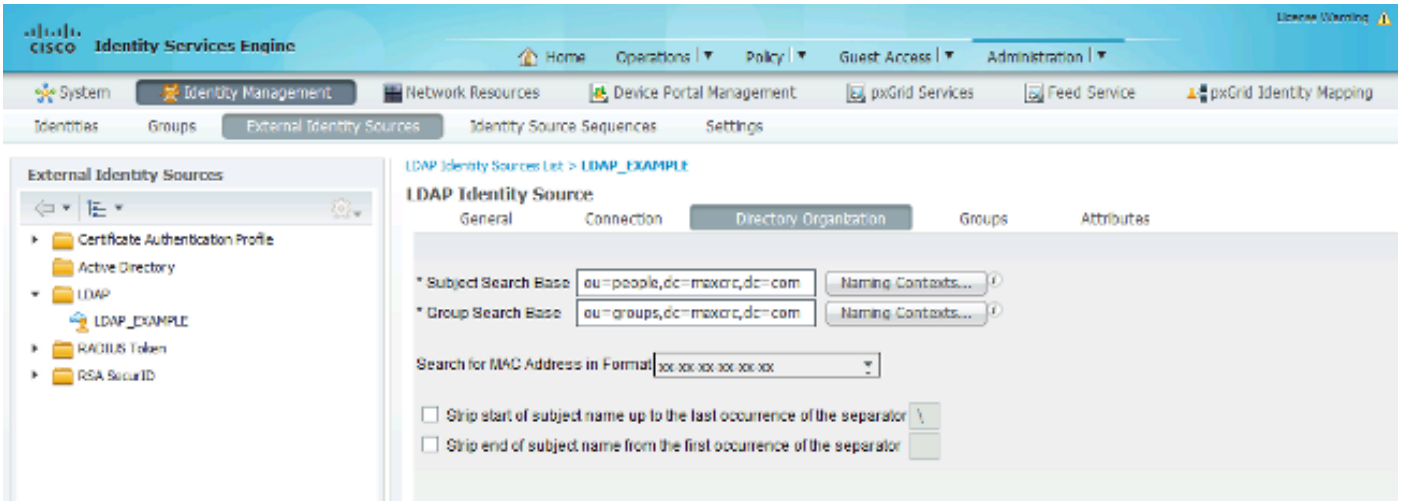
- **Groepskaartenkenmerk** ßDeze eigenschap definieert hoe de gebruikers in kaart worden gebracht aan de groepen. Onder de groep *cn=dominee* in het *ldif*-bestand kunt u twee *ledenUid* eigenschappen zien die overeenkomen met de gebruikers.

ISE biedt ook een aantal vooraf ingestelde schema's (Microsoft Active Directory, Sun, Novell):

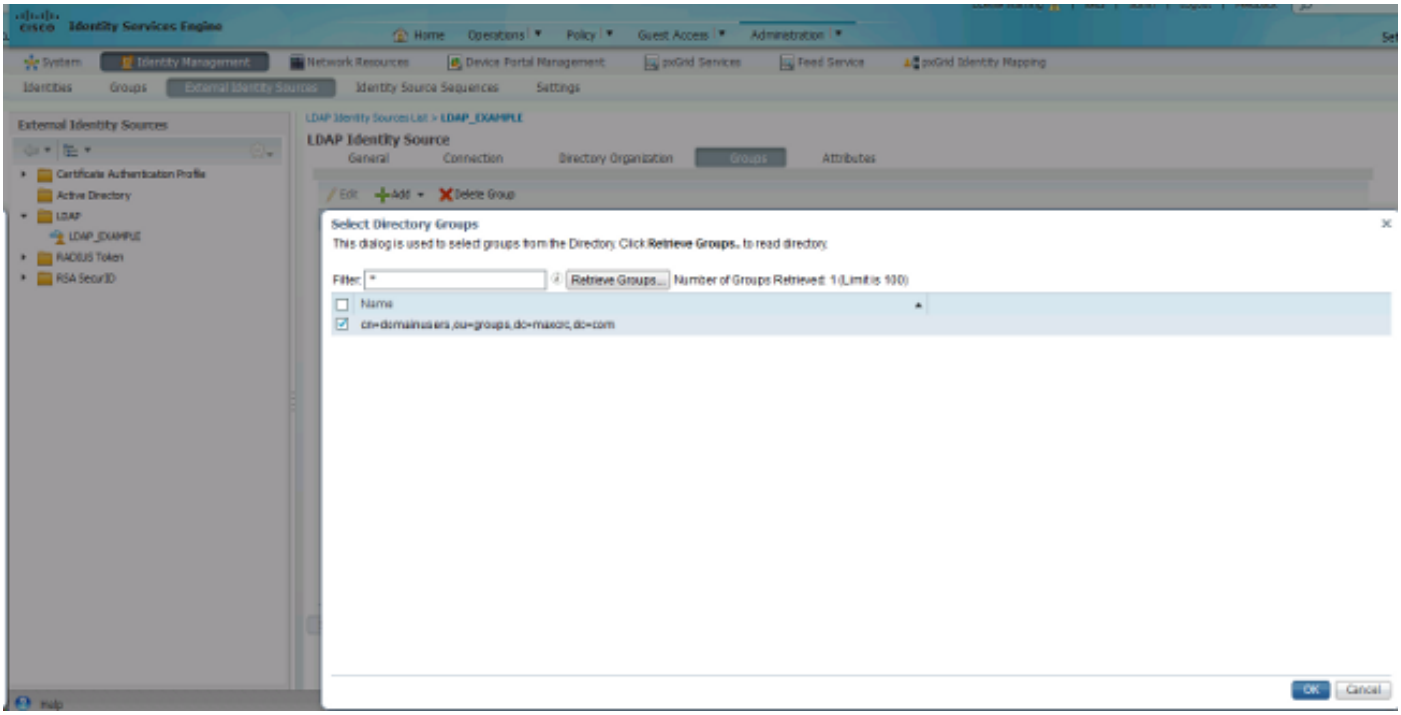


Nadat u het juiste IP-adres en de juiste beheernaam hebt ingesteld, kunt u Bind *testen* op de server. Op dit punt moet u geen proefpersonen of groepen ophalen omdat de zoekbases nog niet zijn geconfigureerd.

In het volgende tabblad kunt u de zoekbasis Onderwerp/groep configureren. Dit is het *aansluitende* punt voor de ISE aan de LDAP. Je kunt alleen maar onderwerpen en groepen terugkrijgen die kinderen zijn van je gemeenschappelijk punt. In dit scenario worden de onderwerpen van de *OU=people* en de groepen van de *OU=group* opgehaald:

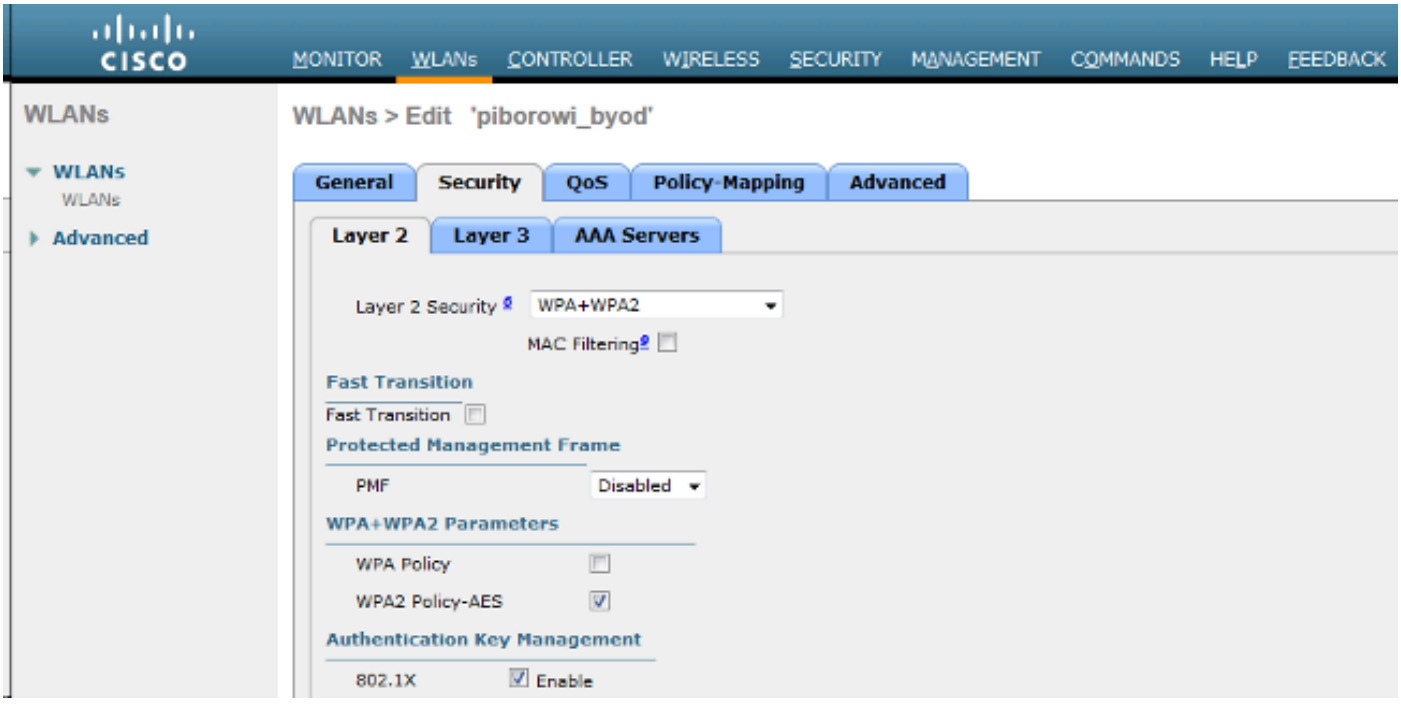


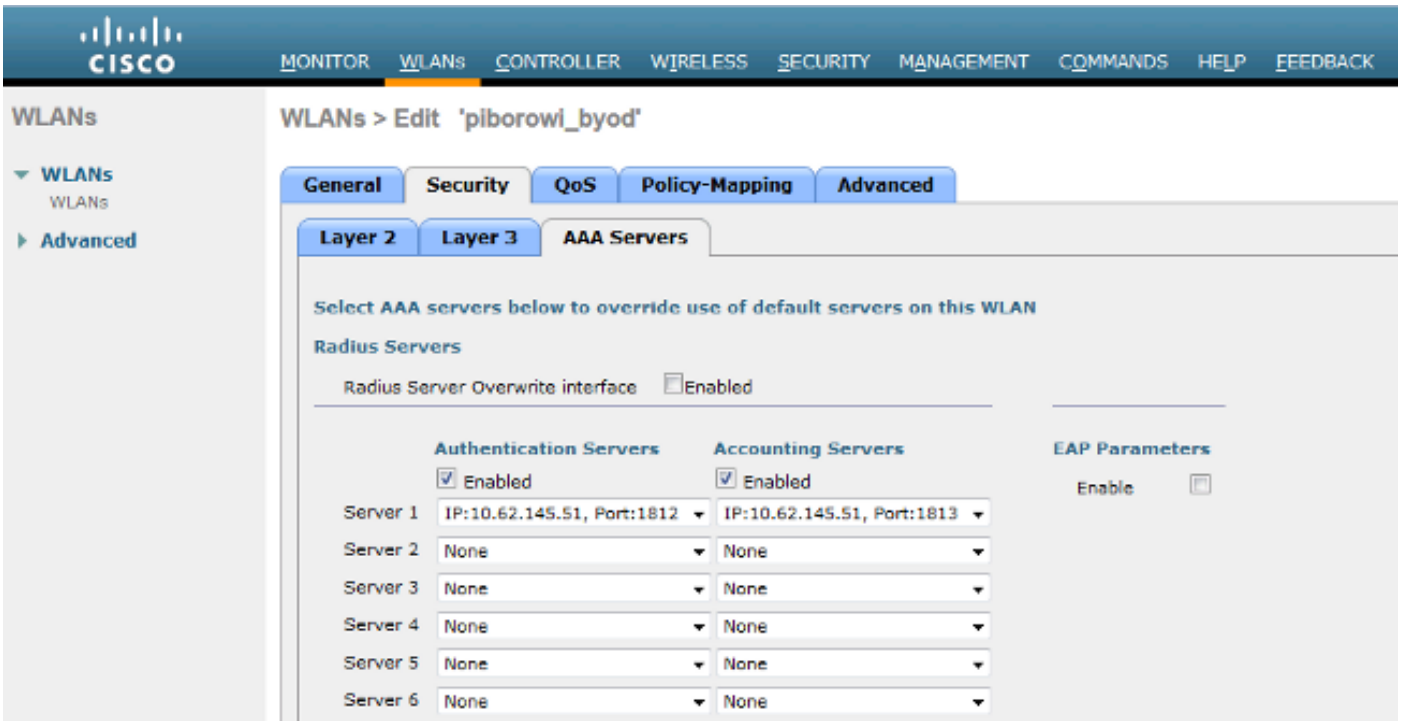
In het tabblad *Groepen* kunt u de groepen importeren uit de LDAP-indeling in de ISE:



De WLC configureren

Gebruik de informatie die in deze beelden wordt verstrekt om de WLC voor 802.1x authenticatie te configureren:



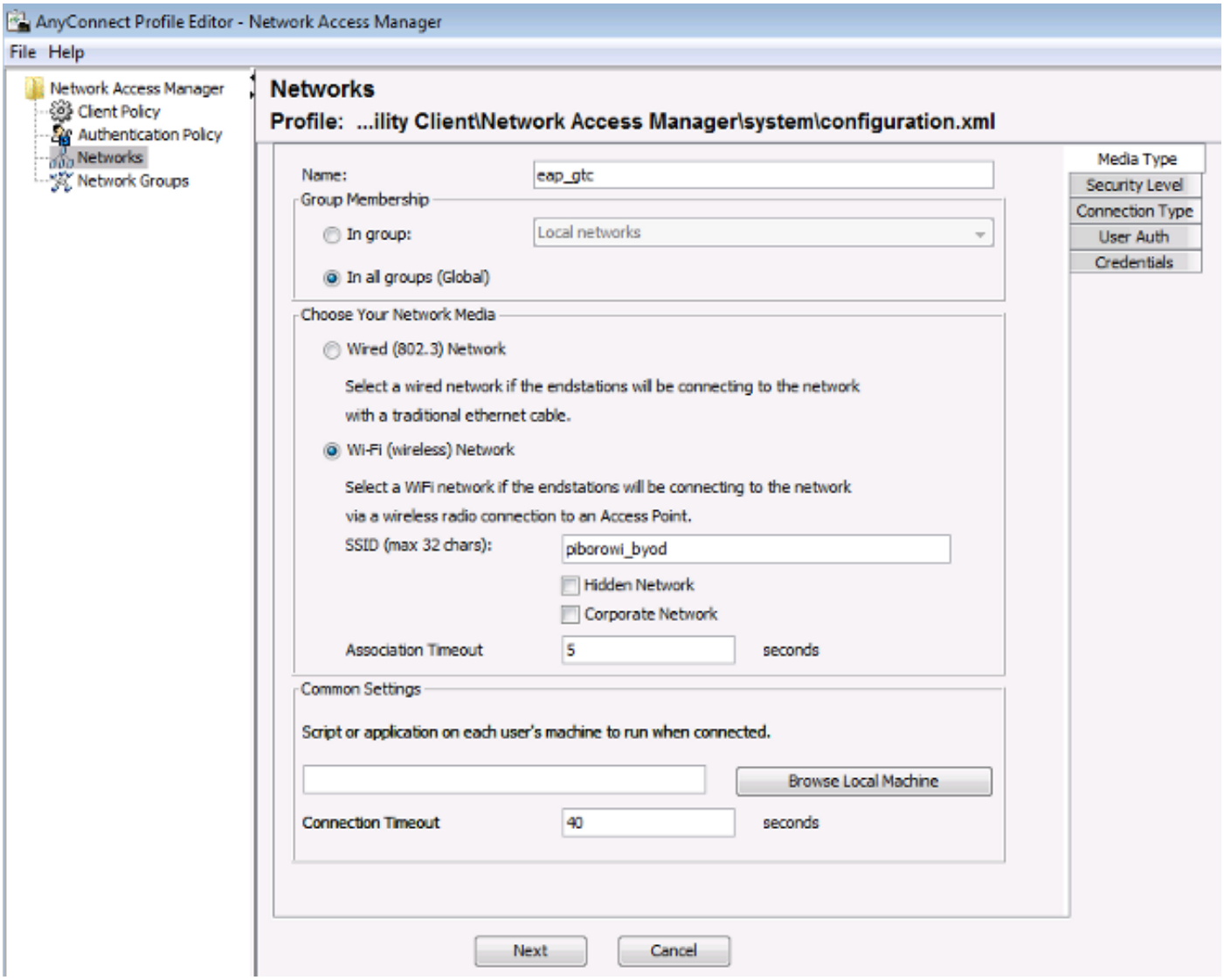


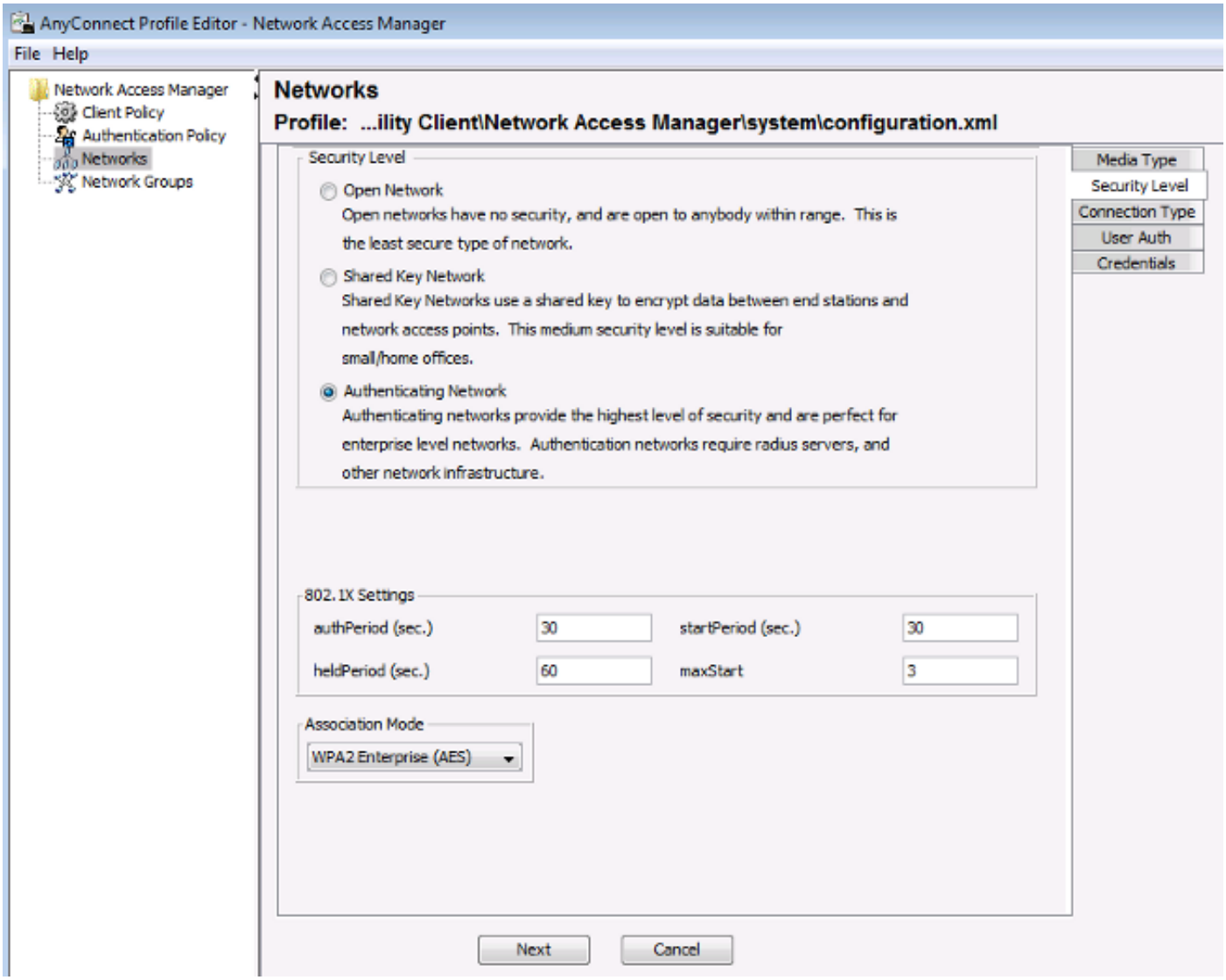
EAP-GTC configureren

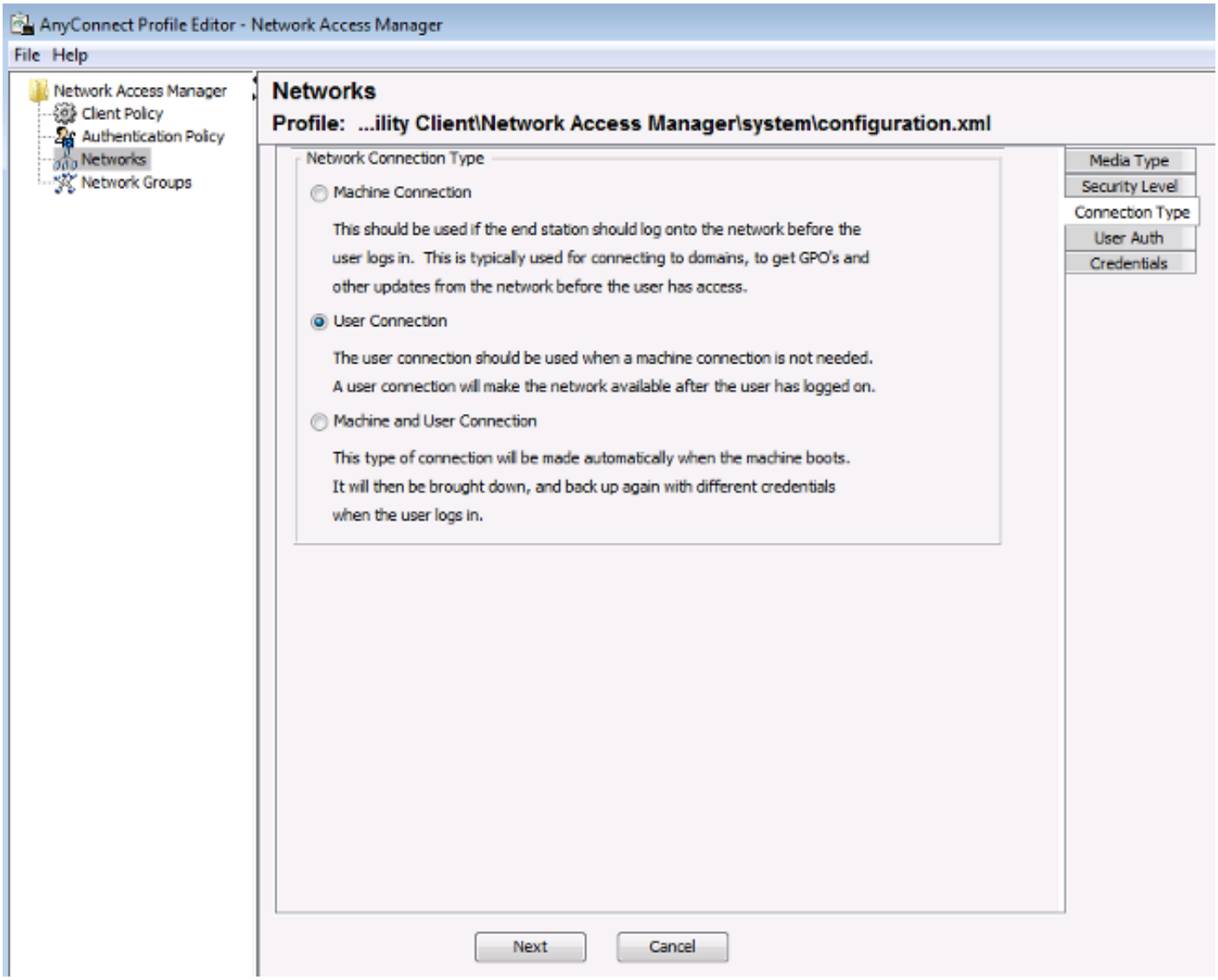
Een van de ondersteunde authenticatiemethoden voor LDAP is EAP-GTC. Het is beschikbaar in Cisco AnyConnect, maar u moet de Profieleditor van Network Access Manager installeren om het profiel correct te configureren. U moet ook de configuratie van Network Access Manager bewerken, die standaard hier is opgeslagen:

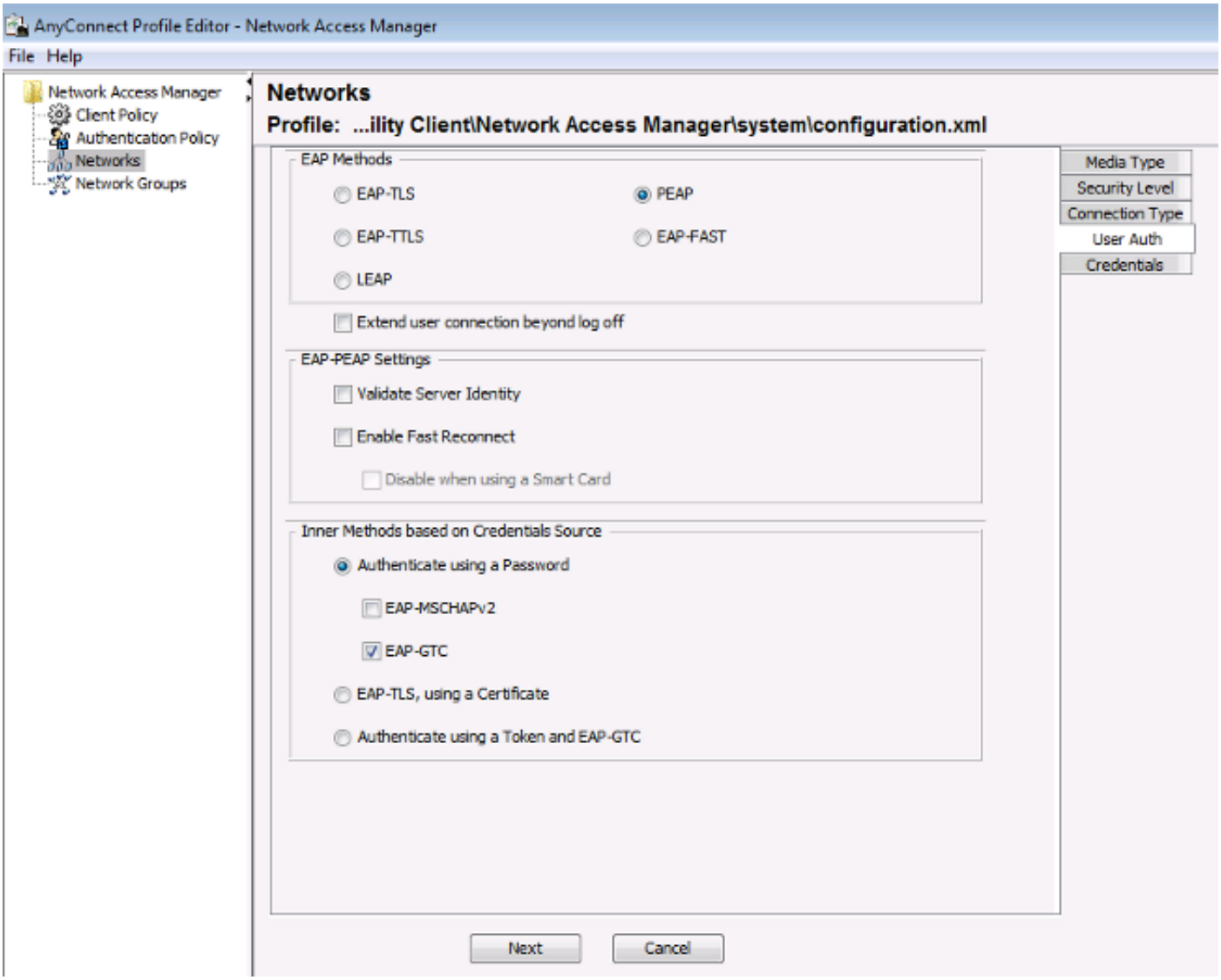
C: > Programma's > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > systeem > configuratie.xml-bestand

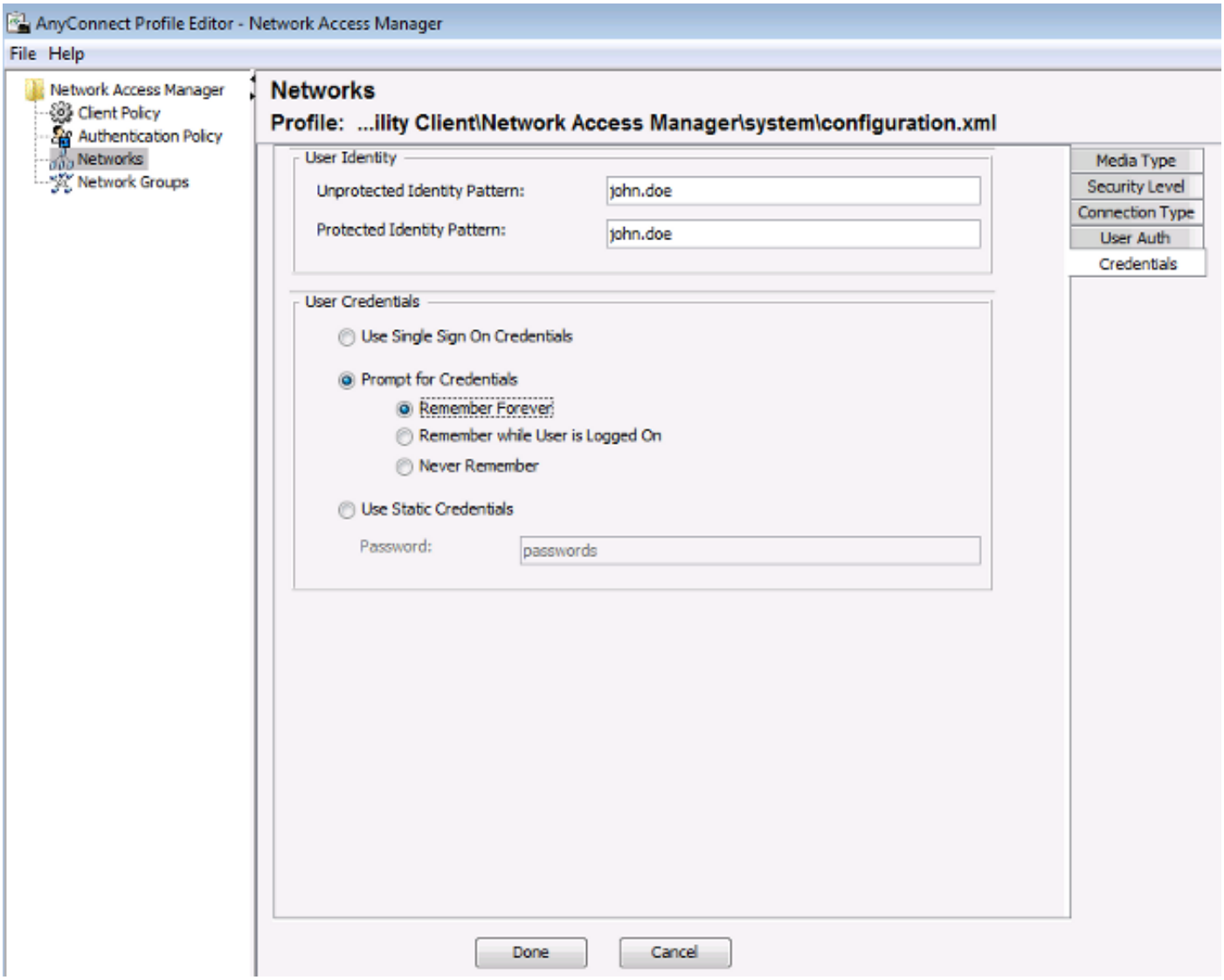
Gebruik de informatie die in deze afbeeldingen wordt verstrekt om de EAP-GTC op het eindpunt te configureren:


AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Media Type
Security Level
Connection Type
User Auth
Credentials
Name:
eap_gtc
Group Membership
In group:
Local networks
In all groups (Global)
Choose Your Network Media
Wired (802.3) Network
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.
Wi-Fi (wireless) Network
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.
SSID (max 32 chars):
piborowi_byod
Hidden Network
Corporate Network
Association Timeout
5
seconds
Common Settings
Script or application on each user's machine to run when connected.
Browse Local Machine
Connection Timeout
40
seconds
Next
Cancel

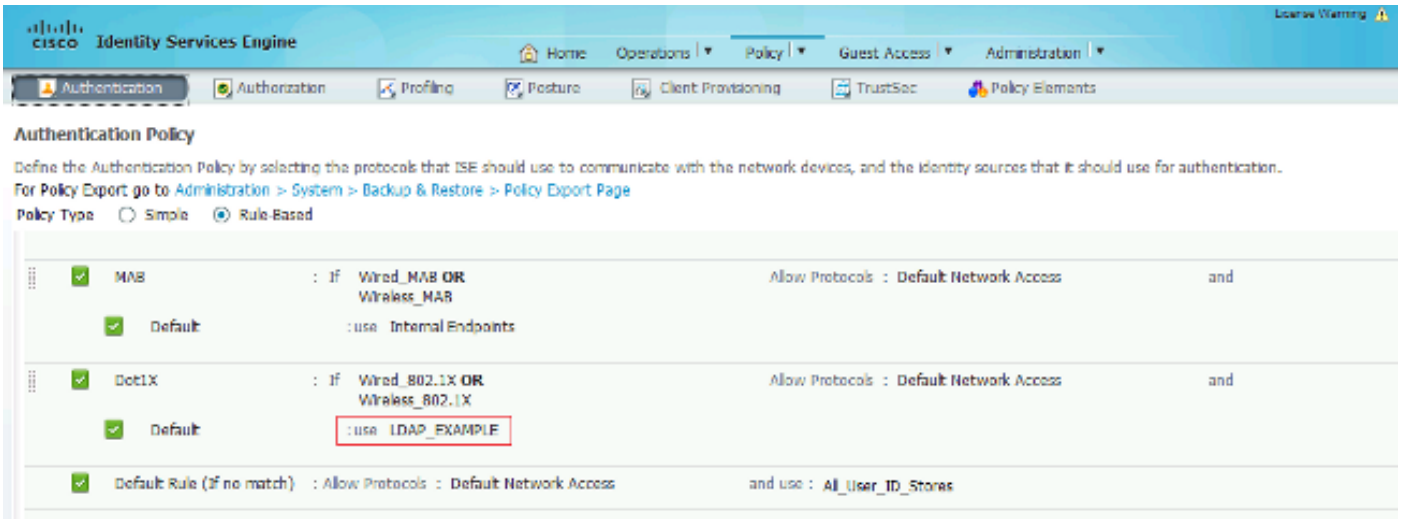

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Media Type
Security Level
Connection Type
User Auth
Credentials
Security Level
Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.
Shared Key Network
Shared Key Networks use a shared key to encrypt data between end stations and network access points. This medium security level is suitable for small/home offices.
Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.
802.1X Settings
authPeriod (sec.)
30
startPeriod (sec.)
30
heldPeriod (sec.)
60
maxStart
3
Association Mode
WPA2 Enterprise (AES)
Next
Cancel


AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Network Connection Type
Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.
User Connection
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.
Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.
Media Type
Security Level
Connection Type
User Auth
Credentials
Next
Cancel


AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
EAP Methods
EAP-TLS
PEAP
EAP-TTLS
EAP-FAST
LEAP
Extend user connection beyond log off
EAP-PEAP Settings
Validate Server Identity
Enable Fast Reconnect
Disable when using a Smart Card
Inner Methods based on Credentials Source
Authenticate using a Password
EAP-MSCHAPv2
EAP-GTC
EAP-TLS, using a Certificate
Authenticate using a Token and EAP-GTC
Media Type
Security Level
Connection Type
User Auth
Credentials
Next
Cancel



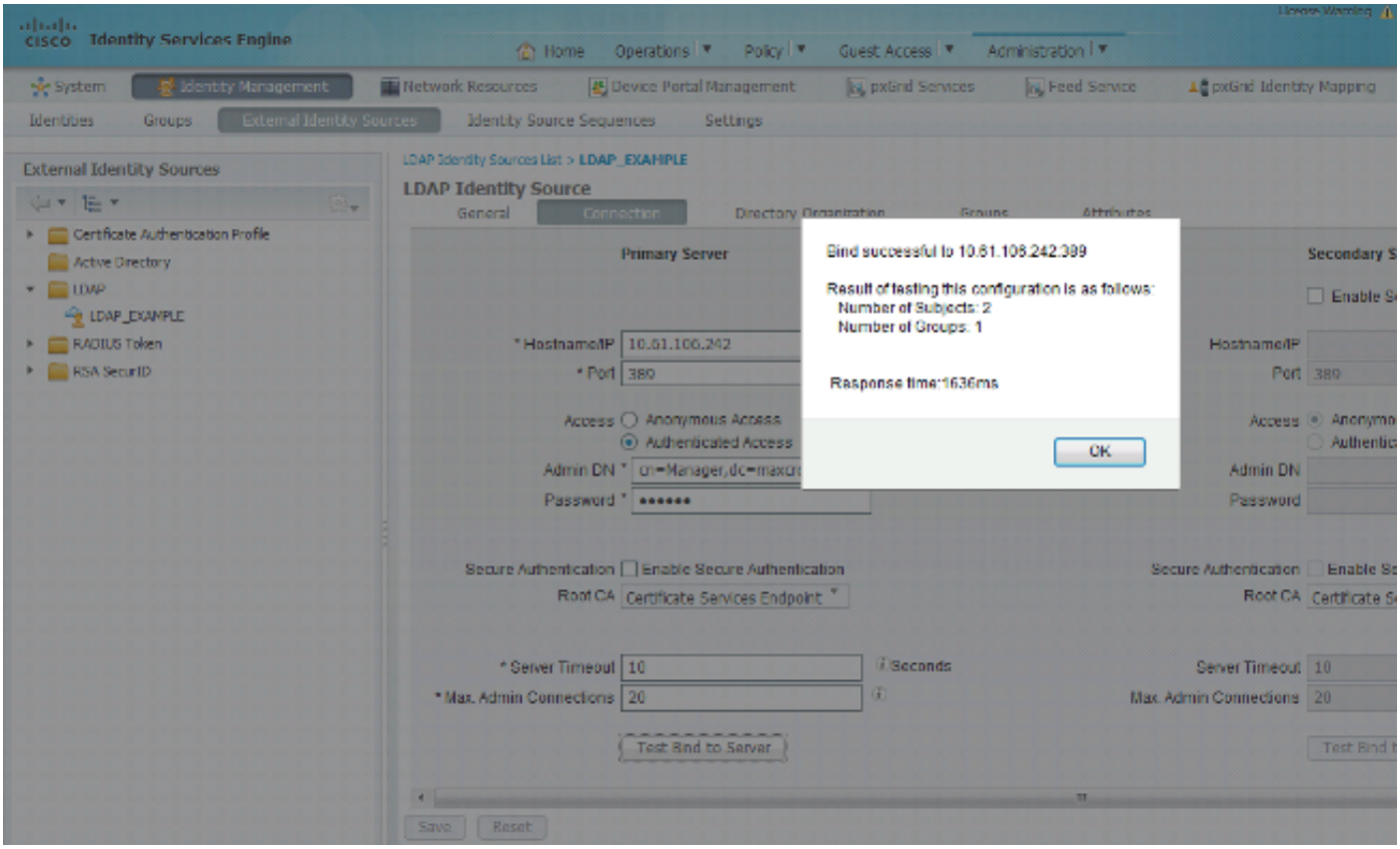
Gebruik de informatie die in deze afbeeldingen wordt verstrekt om het echtheids- en autorisatiebeleid ten aanzien van de ISE te wijzigen:



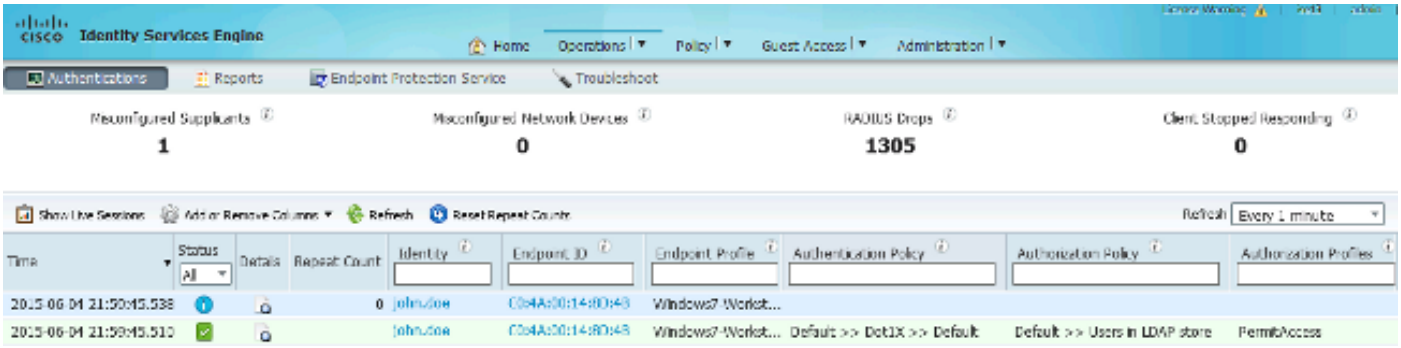
Nadat u de configuratie hebt toegepast, dient u verbinding te kunnen maken met het netwerk:

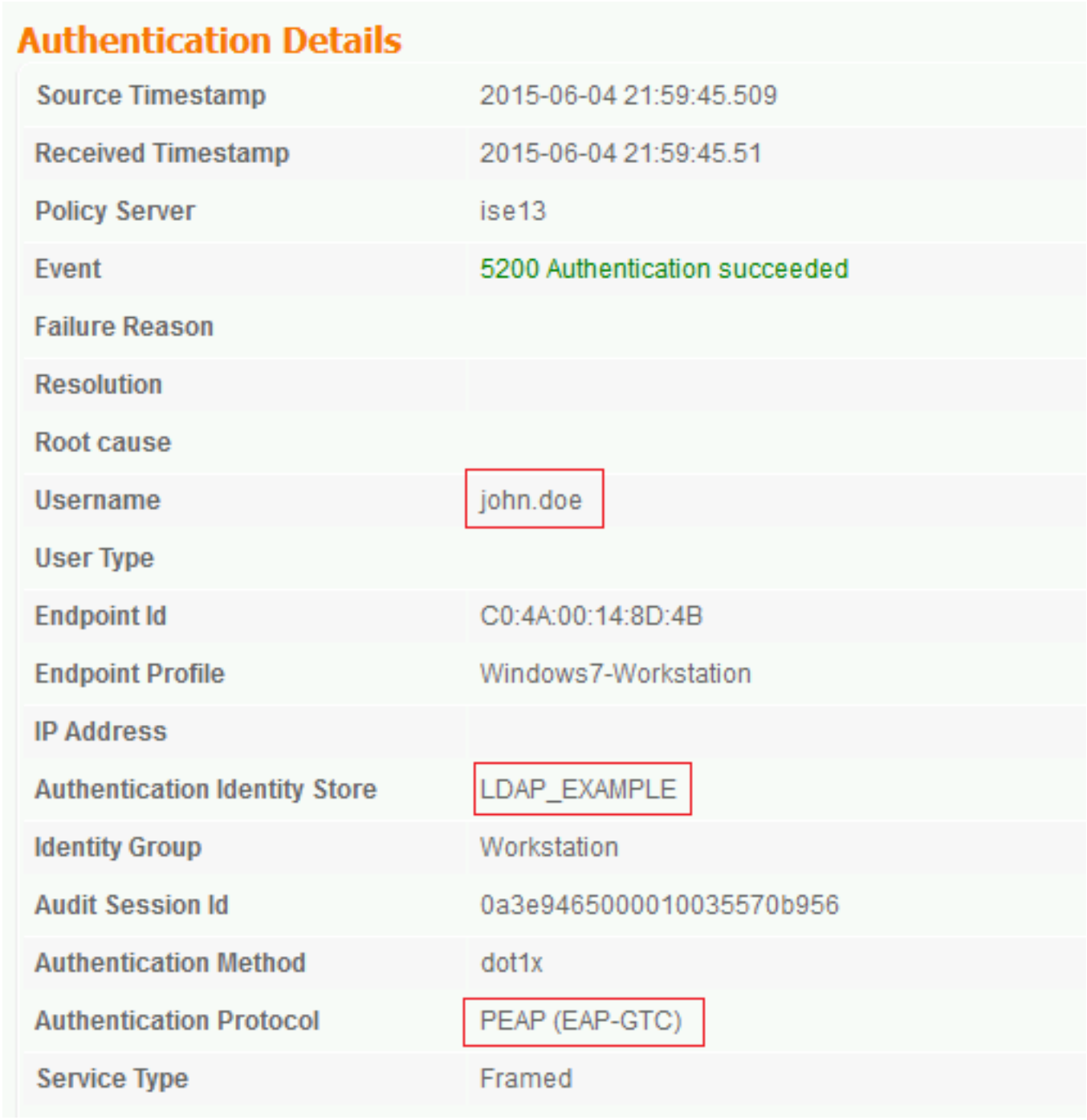
Verifiëren

Om de LDAP- en ISE-configuraties te controleren, dient u de proefpersonen en groepen te kunnen ophalen met een testverbinding naar de server:



Deze beelden illustreren een voorbeeldrapport van de ISE:





Authentication Details

Source Timestamp	2015-06-04 21:59:45.509
Received Timestamp	2015-06-04 21:59:45.51
Policy Server	ise13
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	john.doe
User Type	
Endpoint Id	C0:4A:00:14:8D:4B
Endpoint Profile	Windows7-Workstation
IP Address	
Authentication Identity Store	LDAP_EXAMPLE
Identity Group	Workstation
Audit Session Id	0a3e9465000010035570b956
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-GTC)
Service Type	Framed

AD ExternalGroups	cn=domainusers,ou=groups,dc=maxcrc,dc=com
IdentityDn	uid=john.doe,ou=people,dc=maxcrc,dc=com
RADIUS Username	john.doe

Problemen oplossen

In dit gedeelte worden enkele gebruikelijke fouten beschreven die bij deze configuratie worden aangetroffen en hoe u deze problemen kunt oplossen:

- Na installatie van de OpenLDAP kan er een fout optreden om aan te geven dat er een **gssapi.dll** ontbreekt. U moet Microsoft Windows herstarten om de fout te voorkomen.

- Het is mogelijk om het bestand *Configuration.xml* rechtstreeks voor Cisco AnyConnect te bewerken. Bewaar uw nieuwe configuratie op een andere locatie en gebruik deze om het oude bestand te vervangen.

- In het authenticatierapport ziet u deze foutmelding:

  `Authentication method is not supported by any applicable identity store`
  Deze foutmelding geeft aan dat de door u gekozen methode niet wordt ondersteund door LDAP. Zorg ervoor dat het *verificatieprotocol* in hetzelfde rapport een van de ondersteunde methoden (EAP-GTC, EAP-TLS of PEAP-TLS) toont.

- In het authenticatierapport, zou je kunnen merken dat het onderwerp niet in de identiteitswinkel gevonden werd. Dit betekent dat de naam van de gebruiker uit het rapport niet overeenkomt met de *eigenschap van de doelnaam* voor een gebruiker in de LDAP-database. In dit scenario werd de waarde ingesteld op **uid** voor deze eigenschap, wat betekent dat de ISE de *uid*-waarden voor de gebruikers van de LDAP bekijkt wanneer zij probeert een match te vinden.

- De onderwerpen en groepen zouden niet correct terug kunnen vinden tijdens *binden aan server* test. De meest waarschijnlijke oorzaak van deze kwestie is een onjuiste configuratie voor de zoekbases. Onthoud dat de LDAP-hiërarchie moet worden gespecificeerd vanaf de linker- tot *wortel*- en *dc* (dit kan uit meerdere woorden bestaan).

  Tip: Raadpleeg voor problemen oplossen bij EAP-verificatie aan WLC-zijde het MAP-verificatievoorbeeld met WLAN-controllers (WLC) Cisco-document.