

De ISE voor integratie met een LDAP-server configureren

Inhoud

- [Inleiding](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Achtergrondinformatie](#)
- [Configureren](#)
- [Netwerkdigram](#)
- [OpenLDAP configureren](#)
- [OpenDAP integreren met de ISE-software](#)
- [De WLC configureren](#)
- [EAP-GTC configureren](#)
- [Verifiëren](#)
- [Problemen oplossen](#)

Inleiding

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

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversies:

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

Opmerking: dit document is geldig voor instellingen die LDAP gebruiken als externe identiteitsbron voor de ISE-verificatie en -autorisatie.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Deze verificatiemethoden worden ondersteund met LDAP:

- Uitbreidbaar verificatieprotocol - Generic Token Card (EAP-GTC)
- Uitbreidbaar verificatieprotocol - Transport Layer Security (EAP-TLS)
- Protected Extensible Verification Protocol - Transport Layer Security (PEAP-TLS)

Configureren

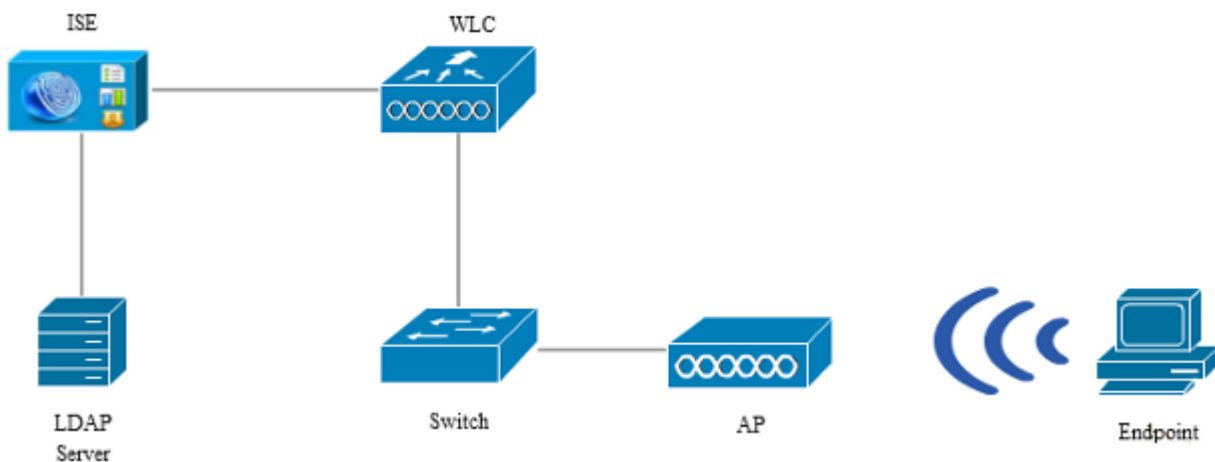
In dit deel wordt beschreven hoe u de netwerkapparaten kunt configureren en de ISE kunt integreren met een LDAP-server.

Netwerkdigram

In dit configuratievoorbeeld gebruikt het eindpunt een draadloze adapter om een koppeling te maken met het draadloze netwerk.





























Draadloze LAN (WLAN) op de WLC is geconfigureerd om de gebruikers via de ISE te verifiëren. Op de ISE is LDAP ingesteld als externe identiteitsopslag.

Dit beeld illustreert de netwerktopologie die wordt gebruikt:



OpenLDAP configureren

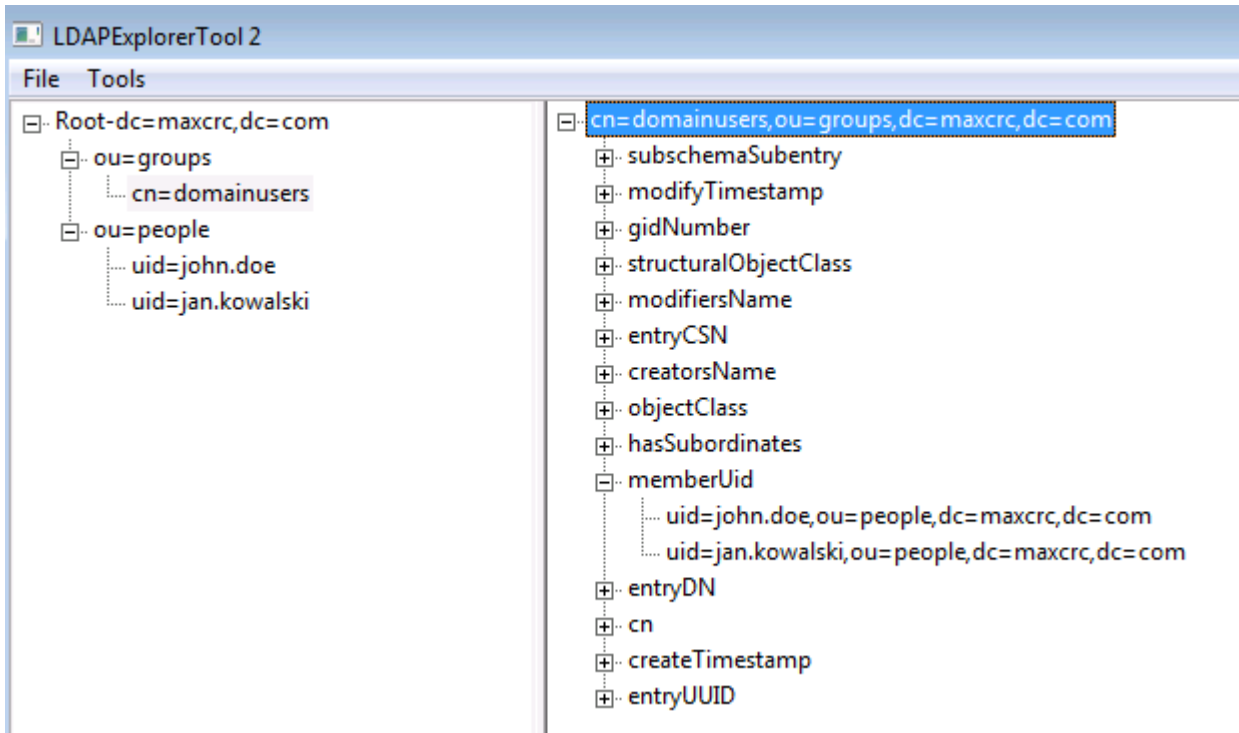
De installatie van OpenLDAP voor Microsoft Windows is voltooid via de GUI, en het is eenvoudig. De standaardlocatie is **C: > OpenLDAP**. Na installatie, zou u deze folder moeten zien:

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	
 Idifdata	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 nota van twee directory's:

- **ClientTools** - Deze map bevat een aantal binaire bestanden die worden gebruikt om de LDAP-database te bewerken.
- **Idifdata** - Dit is de locatie waar u de bestanden met LDAP-objecten moet opslaan.

Voeg deze structuur toe aan de LDAP-database:



Onder de map *Root* moet u twee Organisatorische Eenheden (OU's) configureren. OU = *groups* OU zou één kindgroep moeten hebben (**cn=domainusers** in dit voorbeeld).

De *OE=people* OE definieert de twee gebruikersaccounts die behoren tot de groep *cn=domainusers*.

U moet het *ldif*-bestand eerst maken om de database te kunnen vullen. De eerder vermelde structuur is met behulp van dit bestand gemaakt:

```
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, gebruikt u het binaire **ldapmodificatie**:

```
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"

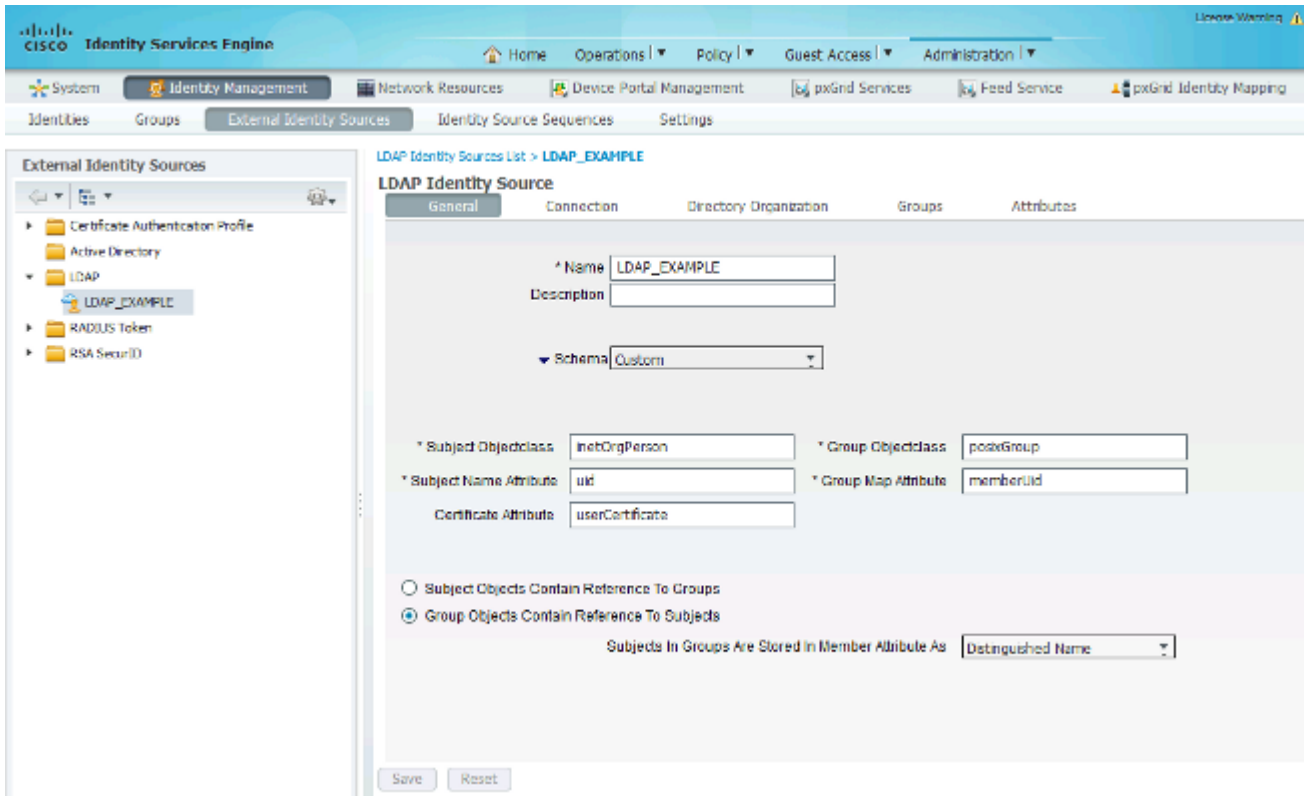
adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

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

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

OpenDAP integreren met de ISE-software

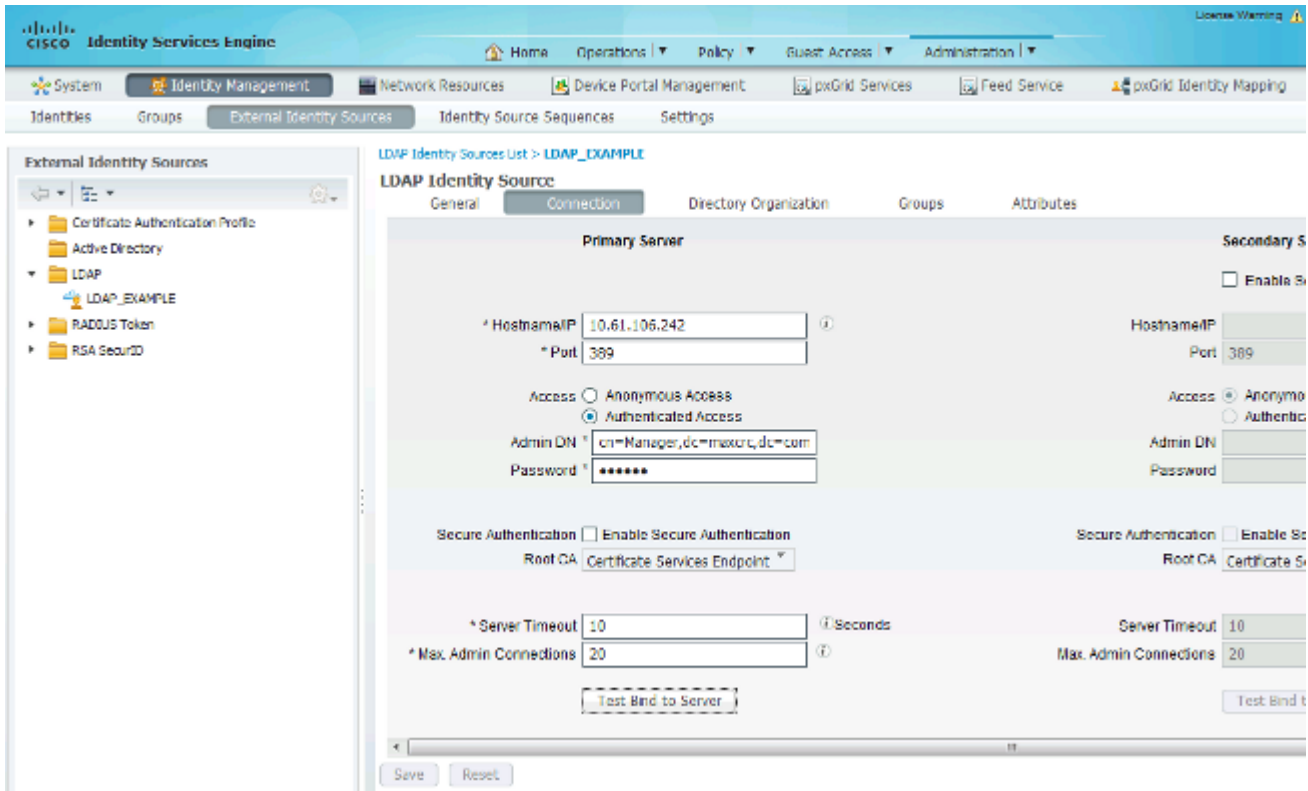
Gebruik de informatie die in de beelden door deze sectie wordt verstrekt om LDAP als externe identiteitsopslag op ISE te vormen.



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

- **Object class** - Dit veld komt overeen met de objectklasse van de gebruikersaccounts in het *ldif*-bestand. Volgens de LDAP-configuratie. Gebruik een van deze vier klassen:
 - top
 - Persoon
 - Organisator
 - InetOrgPerson
- **Attribuut onderwerpnaam** - Dit is het attribuut dat 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 Objectklasse** - Dit veld komt overeen met de objectklasse voor een groep in het *ldif*-bestand. In dit scenario is de objectklasse voor de groep *cn=domainusers* **posixGroup**.
- **Group Map Attribute** - Deze eigenschap bepaalt hoe de gebruikers aan de groepen worden toegewezen. Onder de groep *cn=domainusers* in het *ldif*-bestand kunt u twee *memberUid*-kenmerken zien die overeenkomen met de gebruikers.

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



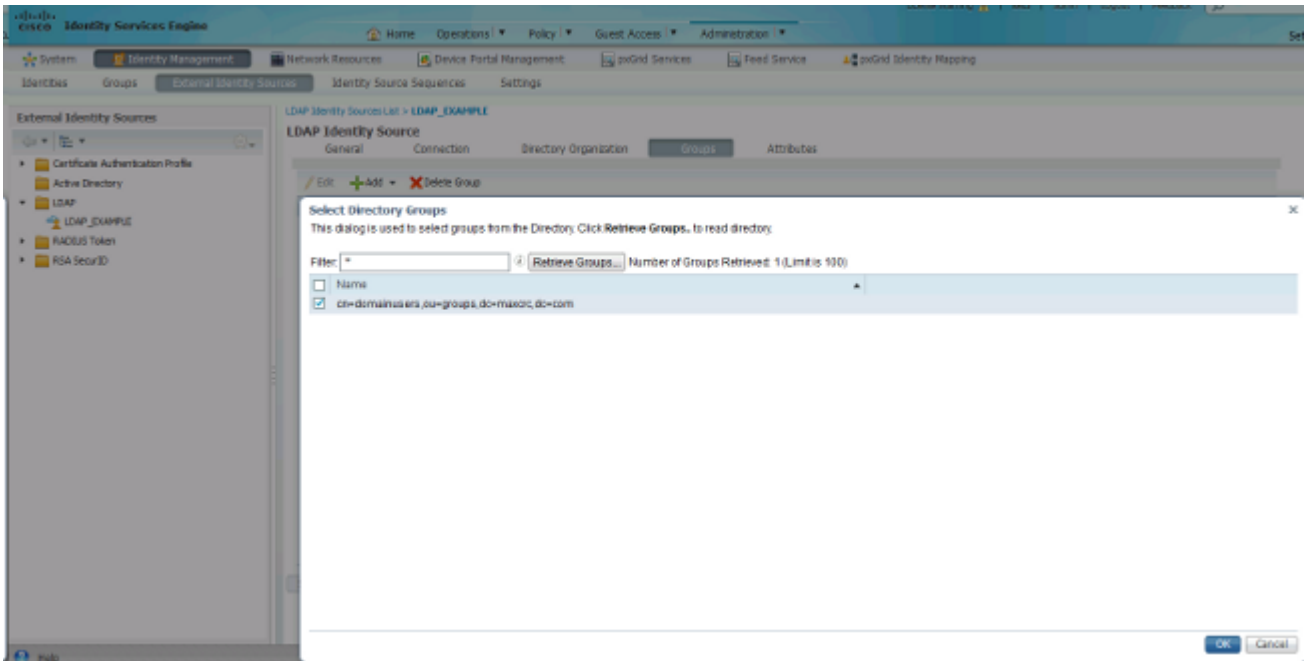
Nadat u het juiste IP-adres en de beheerdomeinnaam hebt ingesteld, kunt u *Bind testen* op de server. Op dit punt, vindt u geen onderwerpen of groepen terug omdat de zoekbases nog niet zijn geconfigureerd.

In het volgende tabblad configureert u de Onderwerp/Groep Zoekbasis. Dit is het *samenvoegpunt* voor de ISE naar de LDAP. Je kunt alleen onderwerpen en groepen ophalen die kinderen zijn van je toetredingspunt.

In dit scenario worden de onderwerpen uit *OU=people* en de groepen uit *OU=groups* opgehaald:

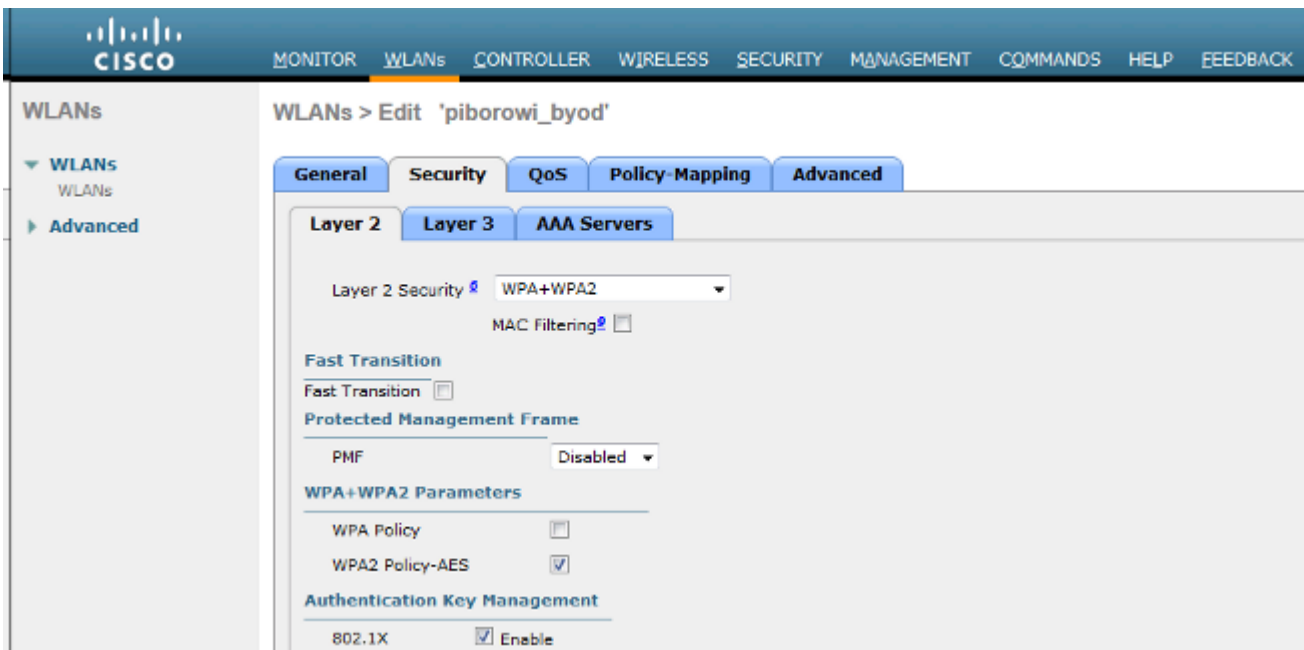


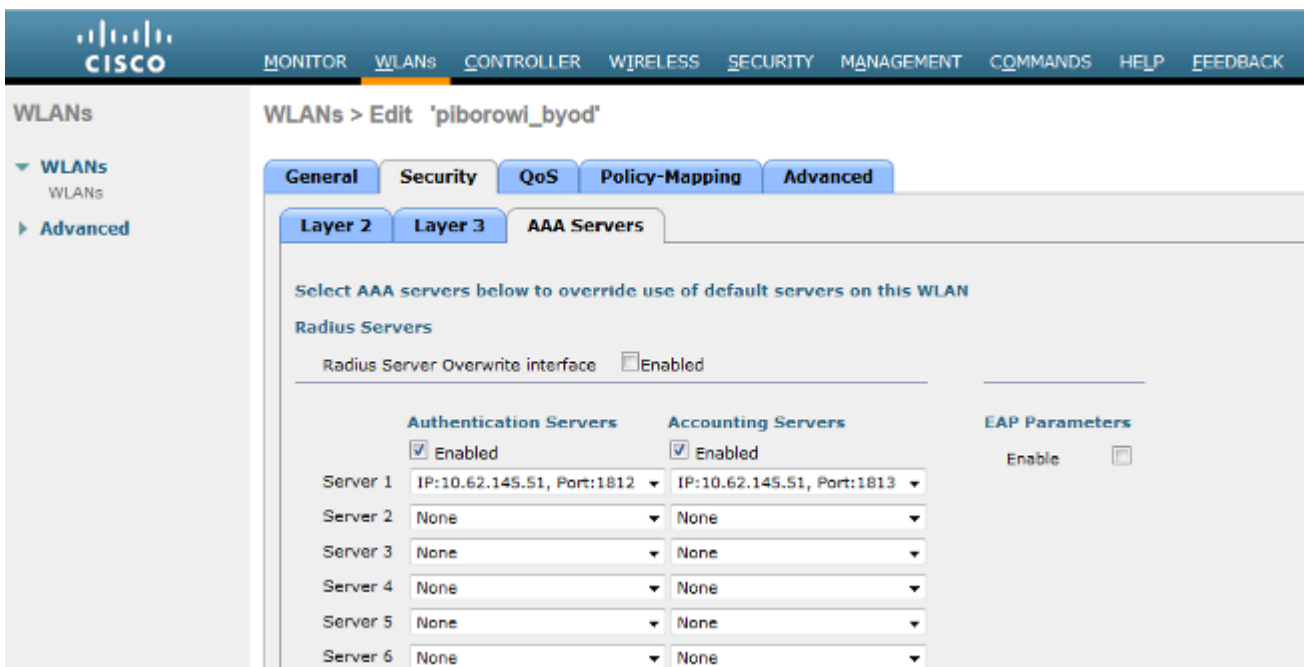
Vanuit het tabblad *Groepen* kunt u de groepen importeren vanuit de LDAP op de ISE:



De WLC configureren

Gebruik de informatie in deze afbeeldingen om de WLC voor 802.1x-verificatie te configureren:





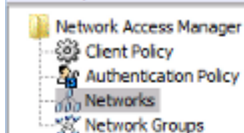
EAP-GTC configureren

Een van de ondersteunde verificatiemethoden voor LDAP is EAP-GTC. Het is beschikbaar in Cisco AnyConnect, maar u moet de Network Access Manager Profile Editor installeren om het profiel correct te kunnen configureren.

U moet ook de configuratie van Network Access Manager bewerken, die (standaard) hier te vinden is:

C: > Program Data > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > systeem > Configuration.xml-bestand

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



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Name:	<input type="text" value="eap_gtc"/>
Group Membership	
<input type="radio"/> In group:	<input type="text" value="Local networks"/>
<input checked="" type="radio"/> In all groups (Global)	
Choose Your Network Media	
<input type="radio"/> Wired (802.3) Network	
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.	
<input checked="" type="radio"/> 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):	<input type="text" value="piborowi_byod"/>
<input type="checkbox"/> Hidden Network	
<input type="checkbox"/> Corporate Network	
Association Timeout	<input type="text" value="5"/> seconds
Common Settings	
Script or application on each user's machine to run when connected.	
<input type="text"/>	<input type="button" value="Browse Local Machine"/>
Connection Timeout	<input type="text" value="40"/> seconds

Media Type
Security Level
Connection Type
User Auth
Credentials

- Network Access Manager
- Client Policy
- Authentication Policy
- Networks**
- Network Groups

Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

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.)	<input type="text" value="30"/>	startPeriod (sec.)	<input type="text" value="30"/>
heldPeriod (sec.)	<input type="text" value="60"/>	maxStart	<input type="text" value="3"/>

Association Mode

WPA2 Enterprise (AES) ▼

Media Type

Security Level

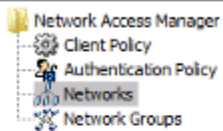
Connection Type

User Auth

Credentials

Next

Cancel



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

- 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

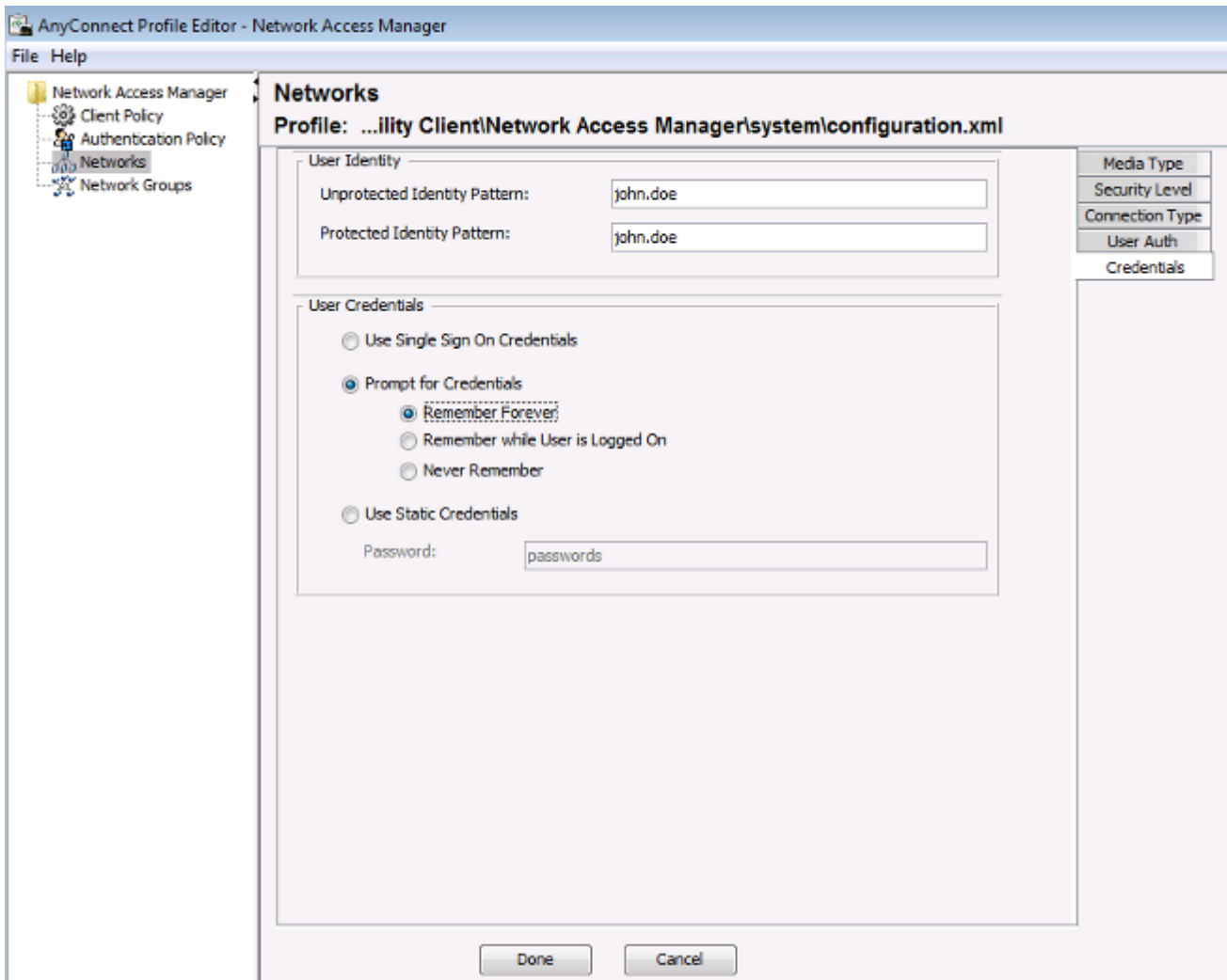
Inner Methods based on Credentials Source

- Authenticate using a Password
 - EAP-MSCHAPv2
 - EAP-GTC
- EAP-TLS, using a Certificate
- Authenticate using a Token and EAP-GTC

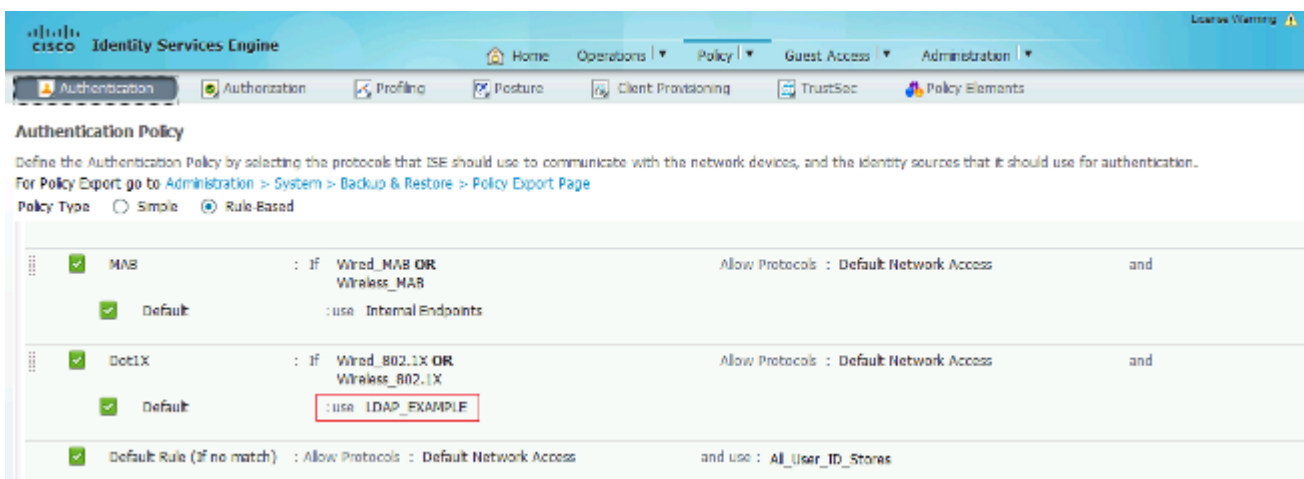
- Media Type
- Security Level
- Connection Type
- User Auth
- Credentials

Next

Cancel



Gebruik de informatie in deze afbeeldingen om het authenticatie- en autorisatiebeleid op de ISE te wijzigen:



Identity Services Engine

Home Operations Policy Guest Access Administration

Authentication Authorization Profiling Posture Client Provisioning TrustSec Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
 For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

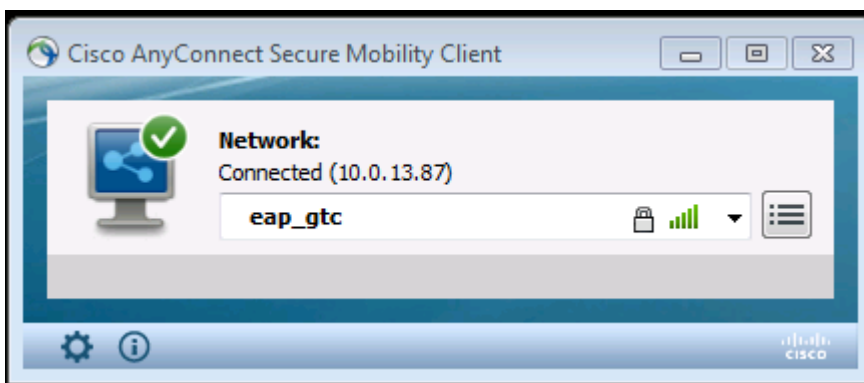
First Matched Rule Applies

Exceptions (0)

Standard

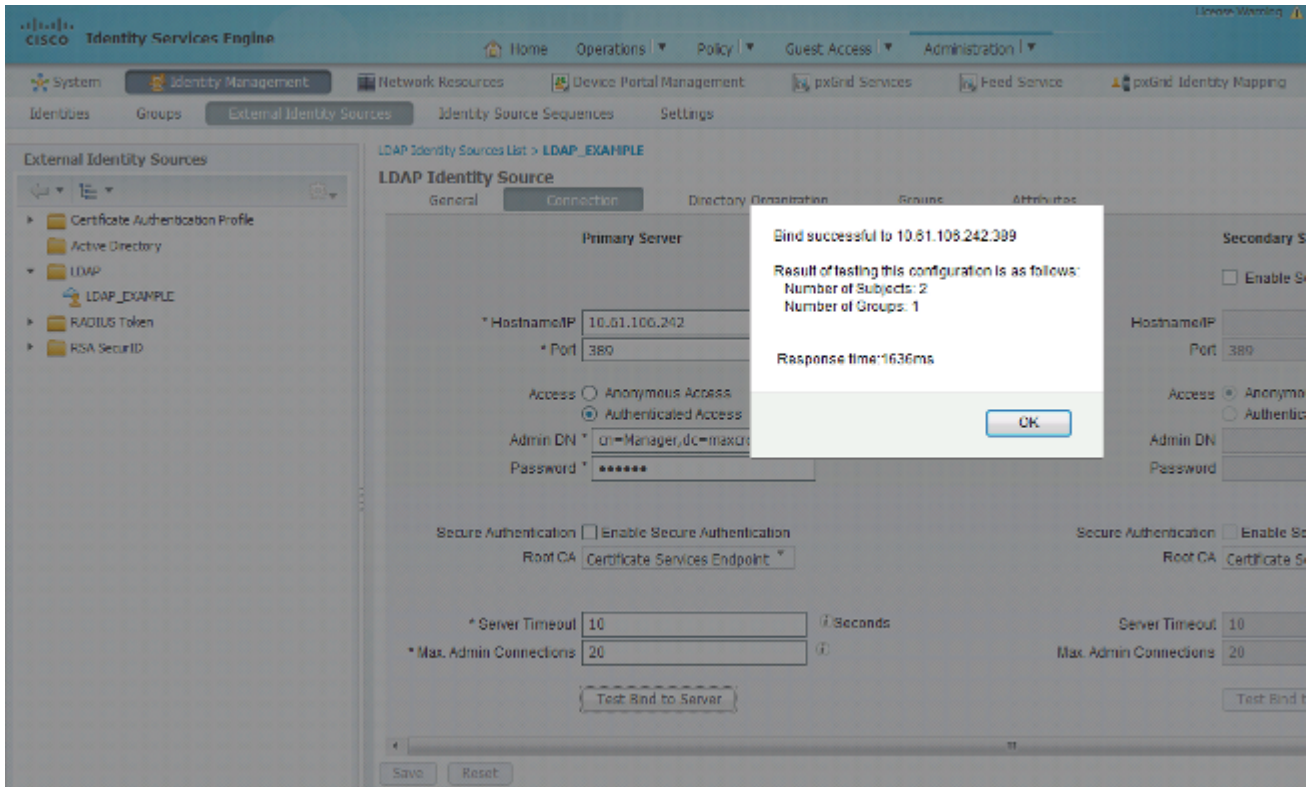
Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✓	Users in LDAP store	if (Wireless_802.1X AND LDAP_EXAMPLE:ExternalGroups EQUALS cn=domainusers,ou=groups,dc=maxxc,dc=com)	then PermitAccess
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
✓	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then PermitAccess
✓	Default	if no matches, then	DenyAccess

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

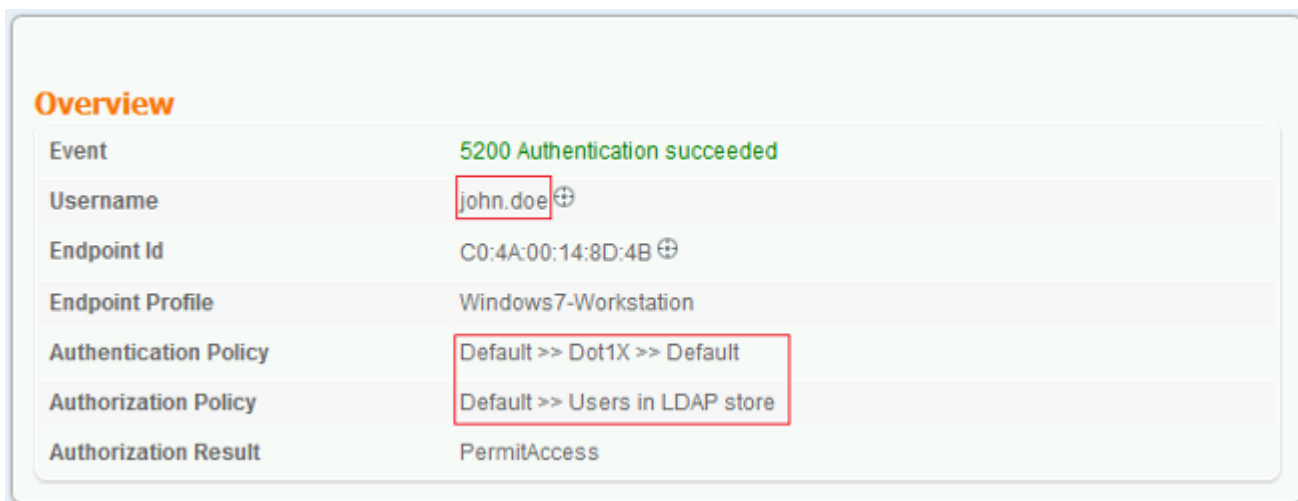
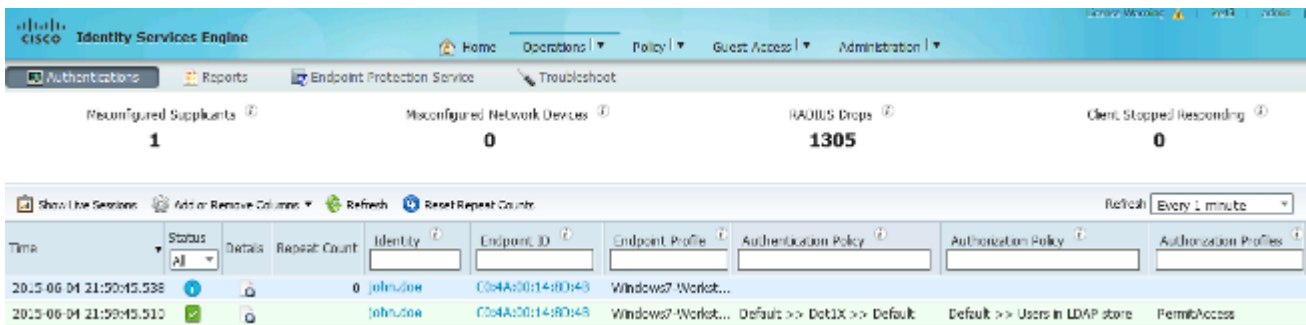


Verifiëren

Om de LDAP- en ISE-configuraties te verifiëren, haalt u de onderwerpen en groepen op 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 deze sectie worden enkele veelvoorkomende fouten beschreven die bij deze configuratie worden aangetroffen en hoe u deze kunt oplossen:

- Na installatie van de OpenLDAP, als u een fout tegenkomt om aan te geven dat een **gssapi.dll** ontbreekt, start Microsoft Windows opnieuw.
- Mogelijk is het niet mogelijk het bestand *Configuration.xml* voor Cisco AnyConnect rechtstreeks te bewerken. Sla uw nieuwe configuratie op een andere locatie op en gebruik deze om het oude bestand te vervangen.
- In het verificatierapport staat deze foutmelding:

```
<#root>
```

```
Authentication method is not supported by any applicable identity store
```

Deze foutmelding geeft aan dat de gekozen methode niet wordt ondersteund door LDAP.

Zorg ervoor dat het *verificatieprotocol* in hetzelfde rapport een van de ondersteunde methoden toont (EAP-GTC, EAP-TLS of PEAP-TLS).

- Als u in het verificatierapport opmerkt dat het onderwerp niet in het identiteitsarchief is gevonden, komt de gebruikersnaam uit het rapport niet overeen met het *kenmerk Onderwerpnaam* voor een gebruiker in de LDAP-database.

In dit scenario is de waarde ingesteld op **uid** voor deze eigenschap, wat betekent dat de ISE naar de *uid*-waarden voor de LDAP-gebruiker kijkt wanneer deze een overeenkomst probeert te vinden.

- Als de onderwerpen en groepen niet correct worden teruggehaald tijdens een *bind aan server* test, is het een onjuiste configuratie voor de zoekbases.

Vergeet niet dat de LDAP-hiërarchie van blad tot wortel en *dc* moet worden gespecificeerd (kan uit meerdere woorden bestaan).

Tip: Raadpleeg voor het oplossen van problemen met EAP-verificatie aan de WLC-zijde het [configuratievoorbeeld van EAP-verificatie met WLAN-controllers \(WLC\) voor](#) Cisco-document.

Over deze vertaling

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