

# Konfigurieren der ISE für die Integration mit einem LDAP-Server

## Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [Konfigurieren](#)
- [Netzwerkdiagramm](#)
- [OpenLDAP konfigurieren](#)
- [Integration von OpenLDAP in die ISE](#)
- [Konfigurieren des WLC](#)
- [Konfigurieren von EAP-GTC](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie eine Cisco Identity Services Engine (ISE) für die Integration mit einem Cisco LDAP-Server konfigurieren.

## Voraussetzungen

### Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

Die in diesem Dokument enthaltenen Informationen basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ISE Version 1.3 mit Patch 2
- Microsoft Windows Version 7 x64 mit installiertem OpenLDAP
- Cisco Wireless LAN Controller (WLC) Version 8.0.100.0
- Cisco AnyConnect Version 3.1 für Microsoft Windows
- Profileditor für Cisco Network Access Manager

---

**Hinweis:** Dieses Dokument gilt für Einrichtungen, die LDAP als externe Identitätsquelle für die ISE-Authentifizierung und -Autorisierung verwenden.

---

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Diese Authentifizierungsmethoden werden von LDAP unterstützt:

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

## Konfigurieren

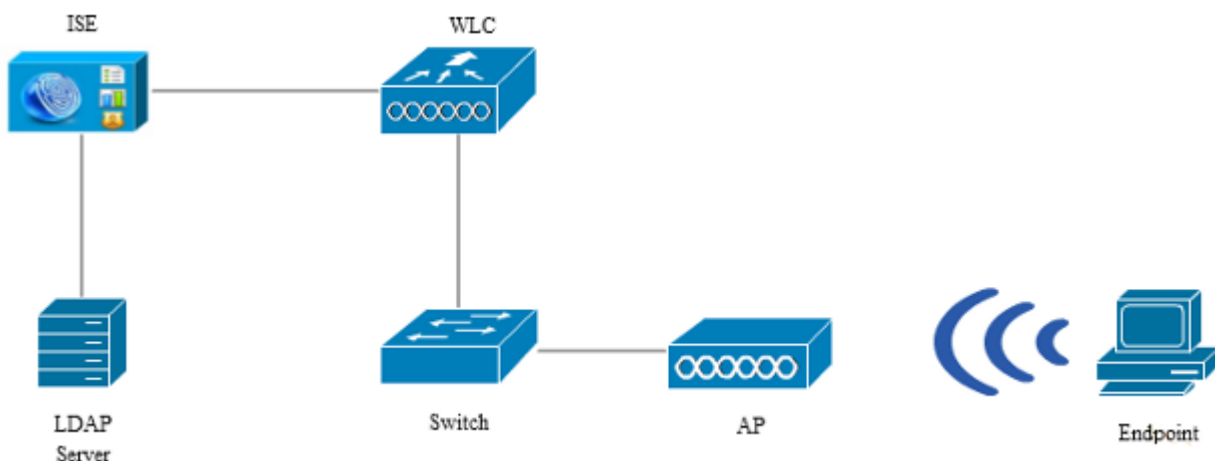
In diesem Abschnitt wird beschrieben, wie Sie die Netzwerkgeräte konfigurieren und die ISE in einen LDAP-Server integrieren.

## Netzwerkdiagramm

In diesem Konfigurationsbeispiel verwendet der Endpunkt einen Wireless-Adapter, um eine Verbindung mit dem Wireless-Netzwerk herzustellen.





























Das Wireless LAN (WLAN) auf dem WLC wird so konfiguriert, dass die Benutzer über die ISE authentifiziert werden. Auf der ISE wird LDAP als externer Identitätsspeicher konfiguriert.

Dieses Bild zeigt die Netzwerktopologie, die verwendet wird:



## OpenLDAP konfigurieren

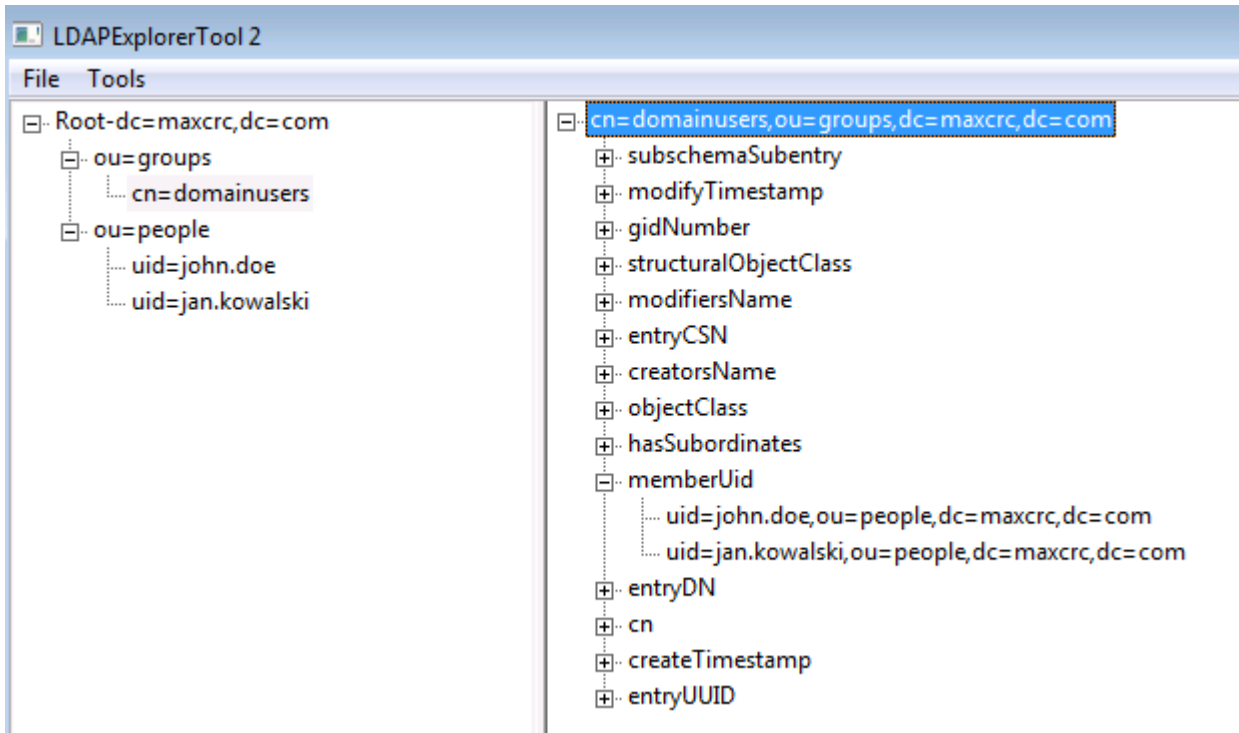
Die Installation von OpenLDAP für Microsoft Windows erfolgt über die GUI und ist einfach. Der Standardspeicherort ist **C: > OpenLDAP**. Nach der Installation sollte das folgende Verzeichnis angezeigt werden:

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

Beachten Sie insbesondere zwei Verzeichnisse:

- **ClientTools** - Dieses Verzeichnis enthält eine Reihe von Binärdateien, die zum Bearbeiten der LDAP-Datenbank verwendet werden.
- **Idifdata** - Dies ist der Speicherort, an dem Sie die Dateien mit LDAP-Objekten speichern sollten.

Fügen Sie diese Struktur der LDAP-Datenbank hinzu:



Unter dem *Stammverzeichnis* müssen Sie zwei Organisationseinheiten (OUs) konfigurieren. Die *OU=groups*-OU sollte eine untergeordnete Gruppe aufweisen (in diesem Beispiel **cn=domainusers**).

Die *OU=people* OU definiert die beiden Benutzerkonten, die zur Gruppe *cn=domainusers* gehören.

Um die Datenbank zu füllen, müssen Sie zuerst die *ldif*-Datei erstellen. Die zuvor erwähnte Struktur wurde aus dieser Datei erstellt:

```
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
```

Um die Objekte zur LDAP-Datenbank hinzuzufügen, verwenden Sie die Binärdatei **ldapchange**:

```
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"

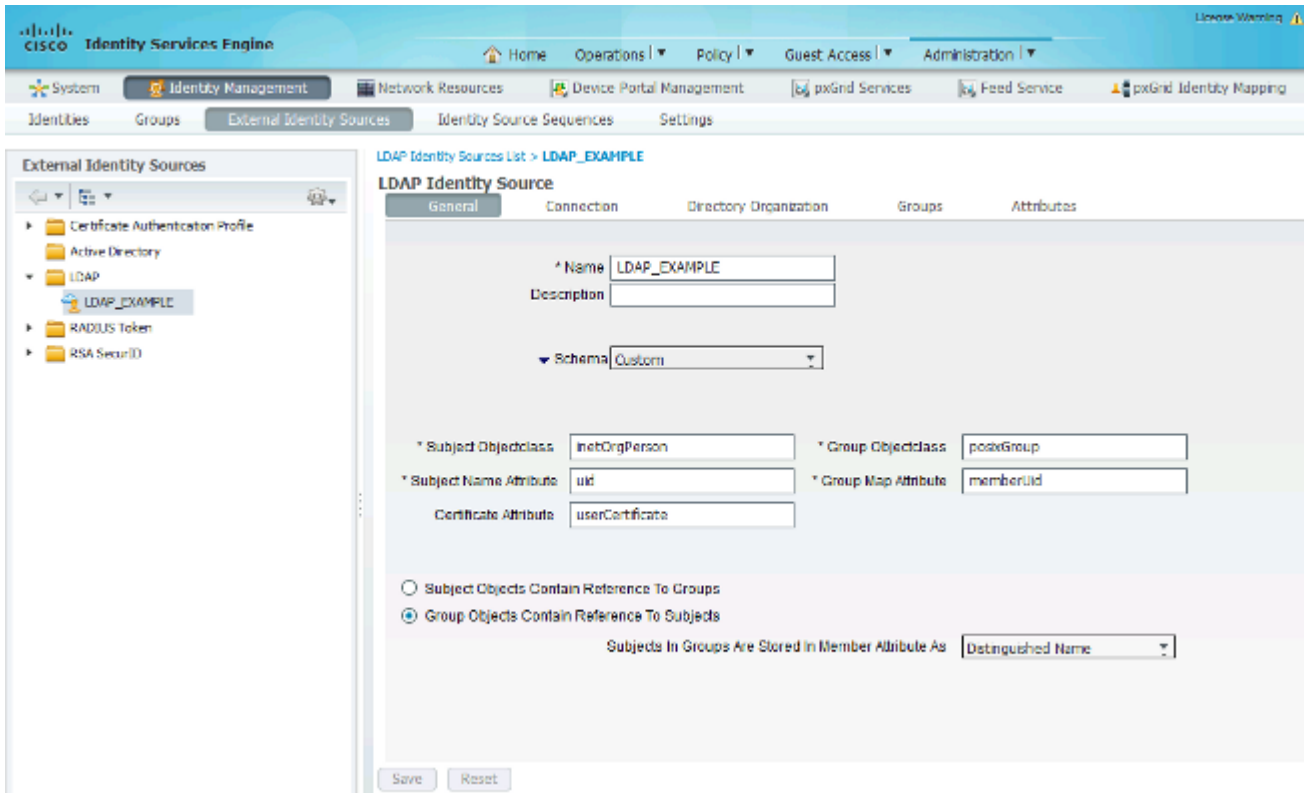
adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

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

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

## **Integration von OpenLDAP in die ISE**

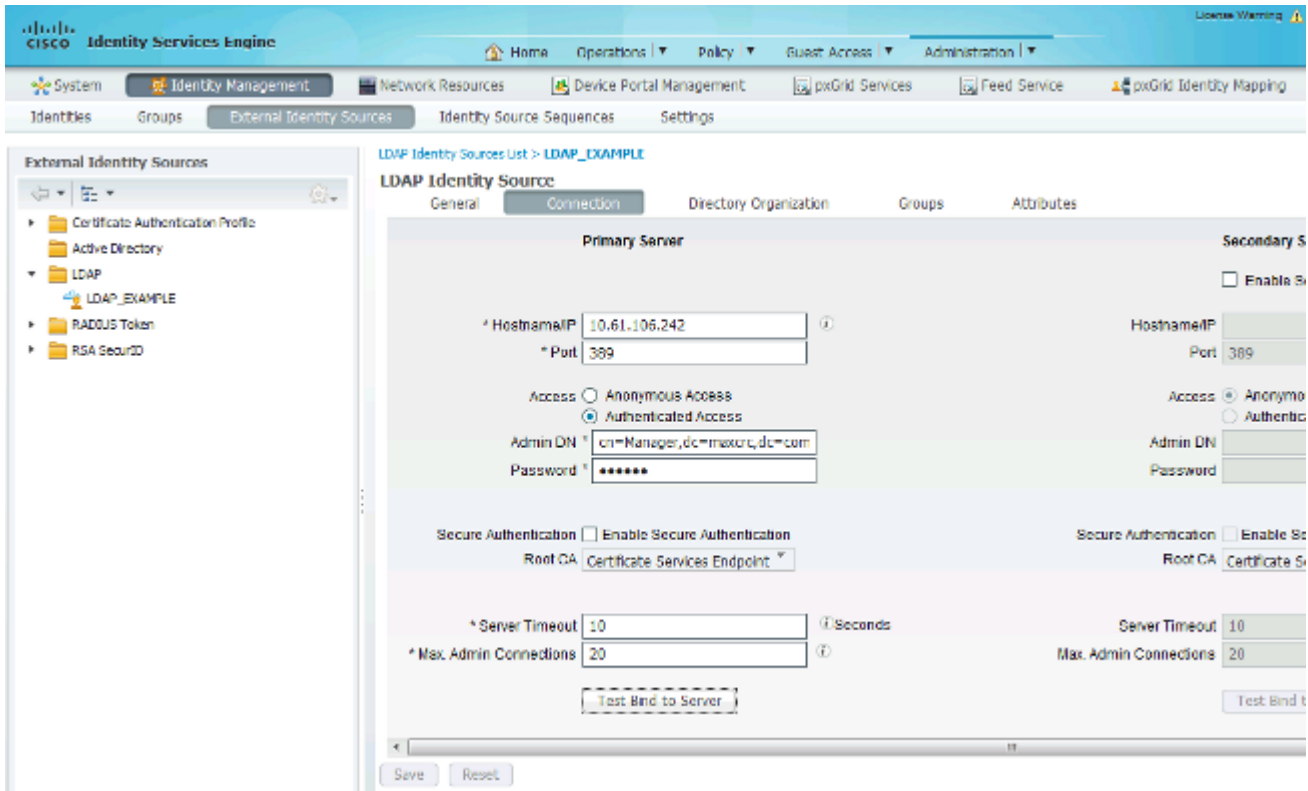
Verwenden Sie die Informationen, die in den Abbildern in diesem Abschnitt bereitgestellt werden, um LDAP als externen Identitätsspeicher auf der ISE zu konfigurieren.



Sie können diese Attribute auf der Registerkarte *Allgemein* konfigurieren:

- **Subject ObjectClass** (Betreff-Objektklasse): Dieses Feld entspricht der Objektklasse der Benutzerkonten in der *ldif*-Datei. Verwenden Sie gemäß der LDAP-Konfiguration eine dieser vier Klassen:
  - Oben
  - Person
  - Organisatorische Person
  - InetOrgPerson
- **Betreffnamenattribut** - Dies ist das Attribut, das vom LDAP abgerufen wird, wenn die ISE abfragt, ob ein bestimmter Benutzername in einer Datenbank enthalten ist. In diesem Szenario müssen Sie **john.doe** oder **jan.kowalski** als Benutzernamen auf dem Endpunkt verwenden.
- **Group ObjectClass** (Gruppenobjektklasse) - Dieses Feld entspricht der Objektklasse für eine Gruppe in der *ldif*-Datei. In diesem Szenario ist die Objektklasse für die Gruppe *cn=domainusers* **posixGroup**.
- **Gruppenzuordnungsattribut** - Dieses Attribut definiert, wie die Benutzer den Gruppen zugeordnet werden. Unter der Gruppe *cn=domainusers* in der Datei *ldif* sehen Sie zwei *memberUid*-Attribute, die den Benutzern entsprechen.

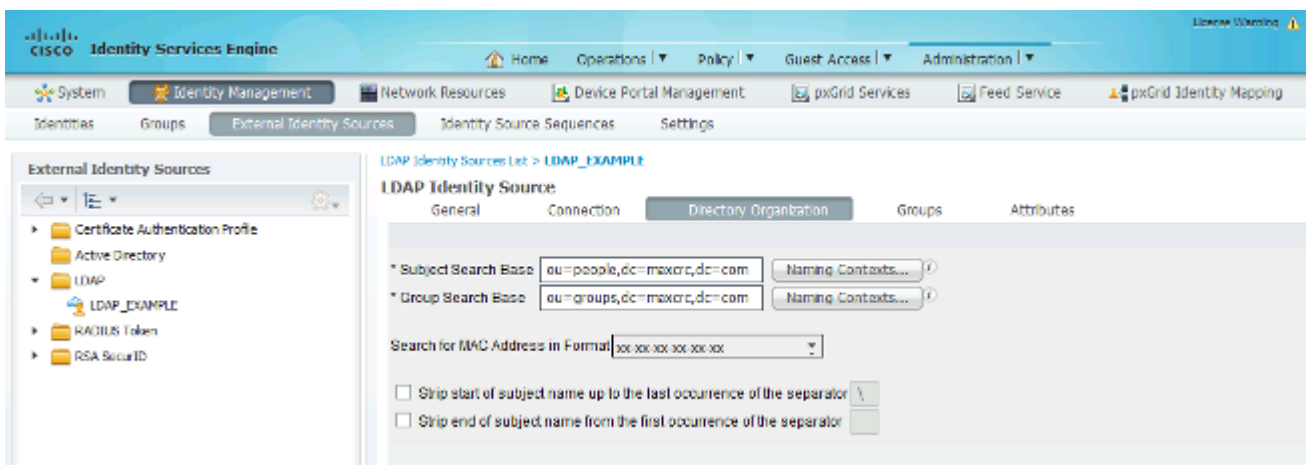
Die ISE bietet auch einige vorkonfigurierte Schemas (Microsoft Active Directory, Sun, Novell):



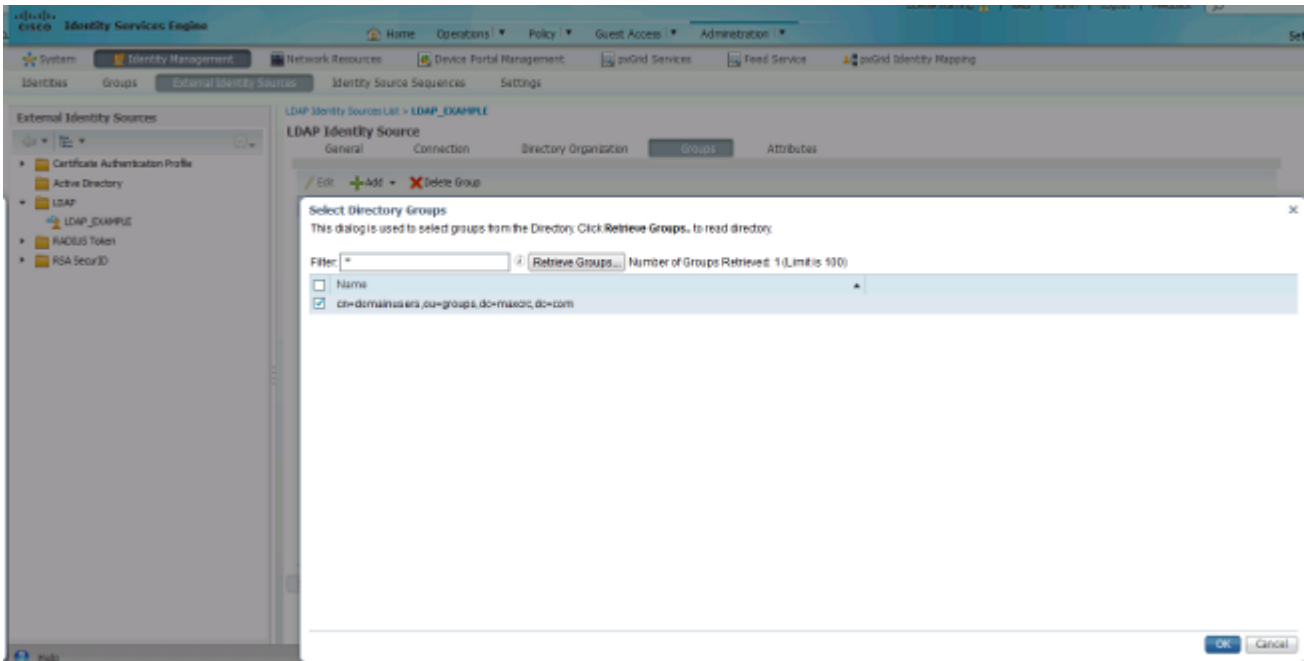
Nachdem Sie die richtige IP-Adresse und den richtigen Domännennamen festgelegt haben, können Sie die *Testbindung* an den Server durchführen. An dieser Stelle rufen Sie keine Themen oder Gruppen ab, da die Suchbasis noch nicht konfiguriert ist.

Konfigurieren Sie auf der nächsten Registerkarte die Suchbasis für Betreff/Gruppe. Dies ist der *Verknüpfungspunkt* für die ISE mit dem LDAP. Sie können nur Themen und Gruppen abrufen, die untergeordnete Elemente Ihres Verbindungspunkts sind.

In diesem Szenario werden die Subjekte aus der *OU=people* und die Gruppen aus der *OU=groups* abgerufen:

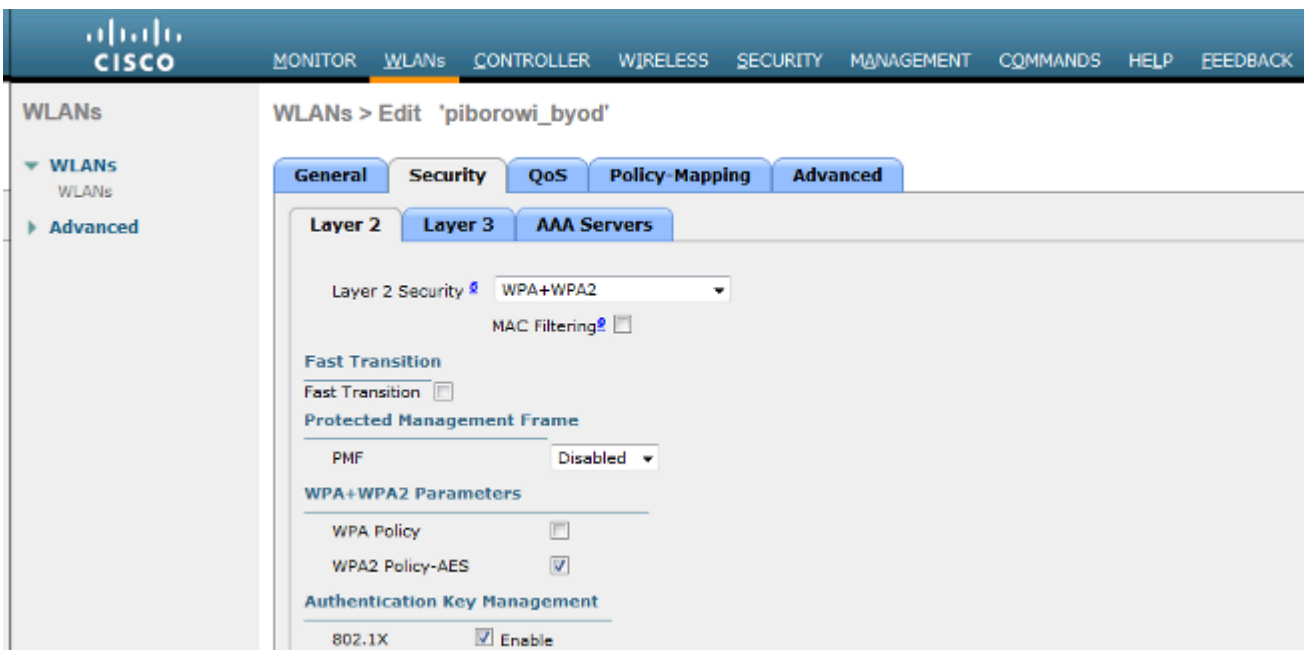


Auf der Registerkarte *Gruppen* können Sie die Gruppen aus dem LDAP auf der ISE importieren:

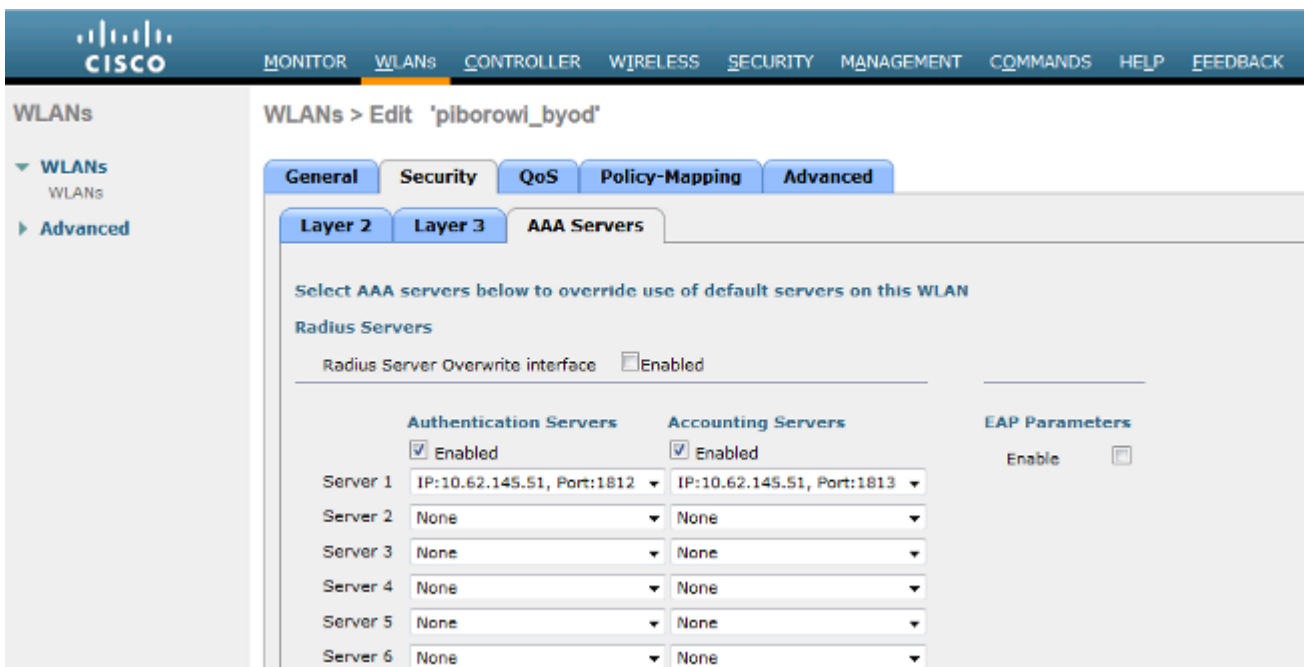


## Konfigurieren des WLC

Verwenden Sie die Informationen in diesen Images, um den WLC für die 802.1x-Authentifizierung zu konfigurieren:







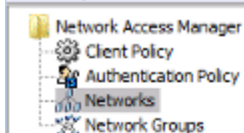
## Konfigurieren von EAP-GTC

Eine der unterstützten Authentifizierungsmethoden für LDAP ist EAP-GTC. Die Funktion ist in Cisco AnyConnect verfügbar, Sie müssen jedoch den Network Access Manager Profile Editor installieren, um das Profil richtig zu konfigurieren.

Sie müssen auch die Konfiguration des Network Access Manager bearbeiten, die sich (standardmäßig) hier befindet:

**C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > System > configuration.xml-Datei**

Verwenden Sie die Informationen in diesen Images, um EAP-GTC auf dem Endpunkt zu konfigurieren:

**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

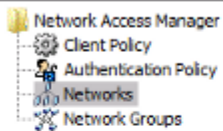
Connection Type

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
- EAP-TTLS
- LEAP
- PEAP
- EAP-FAST

Extend user connection beyond log off

### EAP-PEAP Settings

- Validate Server Identity
- Enable Fast Reconnect
- Disable when using a Smart Card

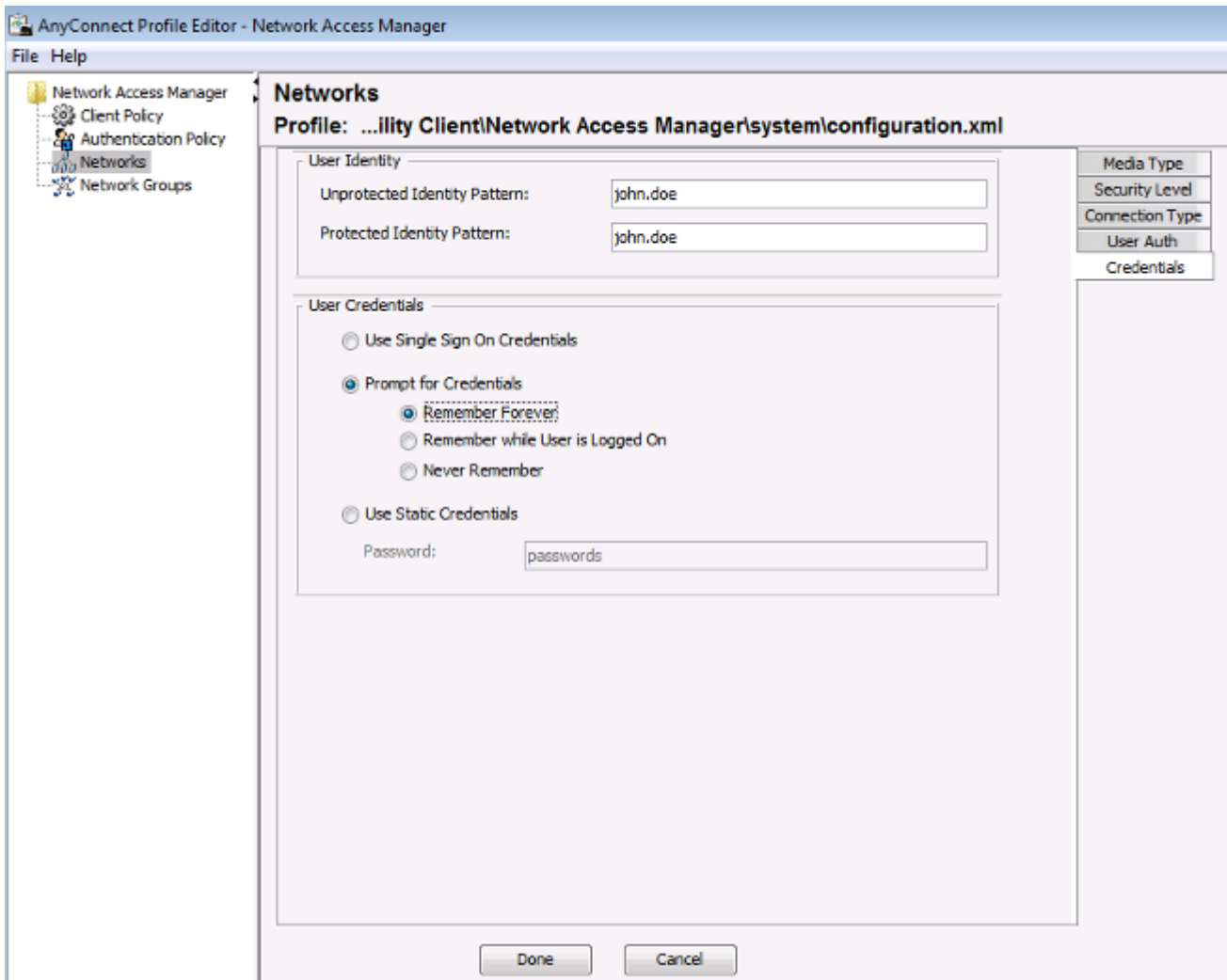
### Inner Methods based on Credentials Source

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

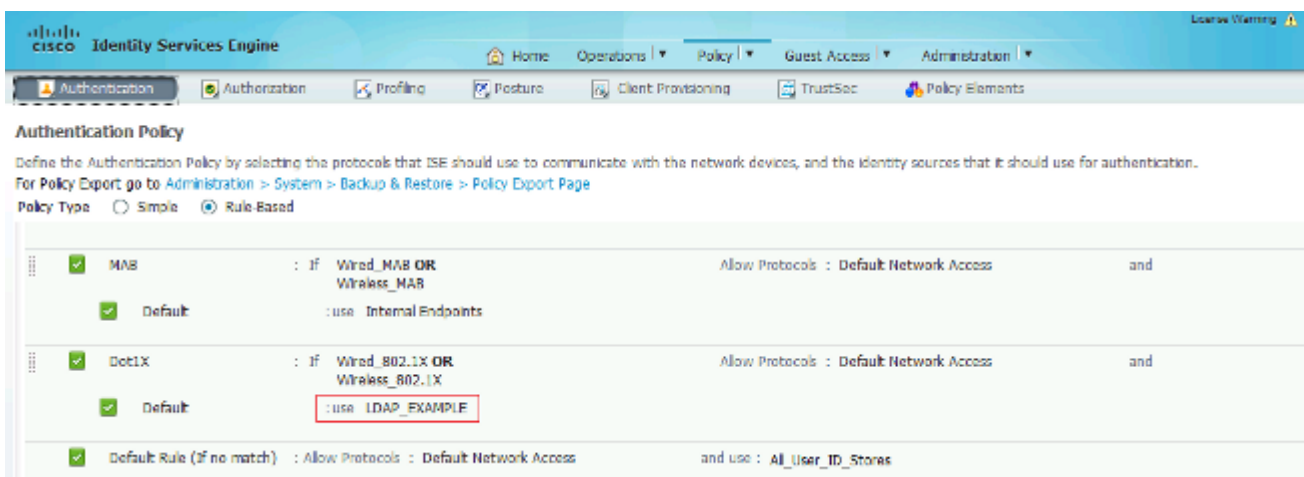
- Media Type
- Security Level
- Connection Type
- User Auth
- Credentials

Next

Cancel



Verwenden Sie die Informationen in diesen Images, um die Authentifizierungs- und Autorisierungsrichtlinien auf der ISE zu ändern:



**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

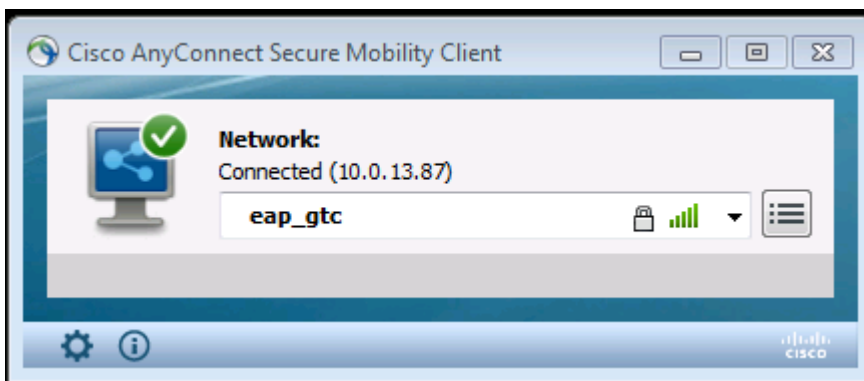
First Matched Rule Applies

Exceptions (0)

Standard

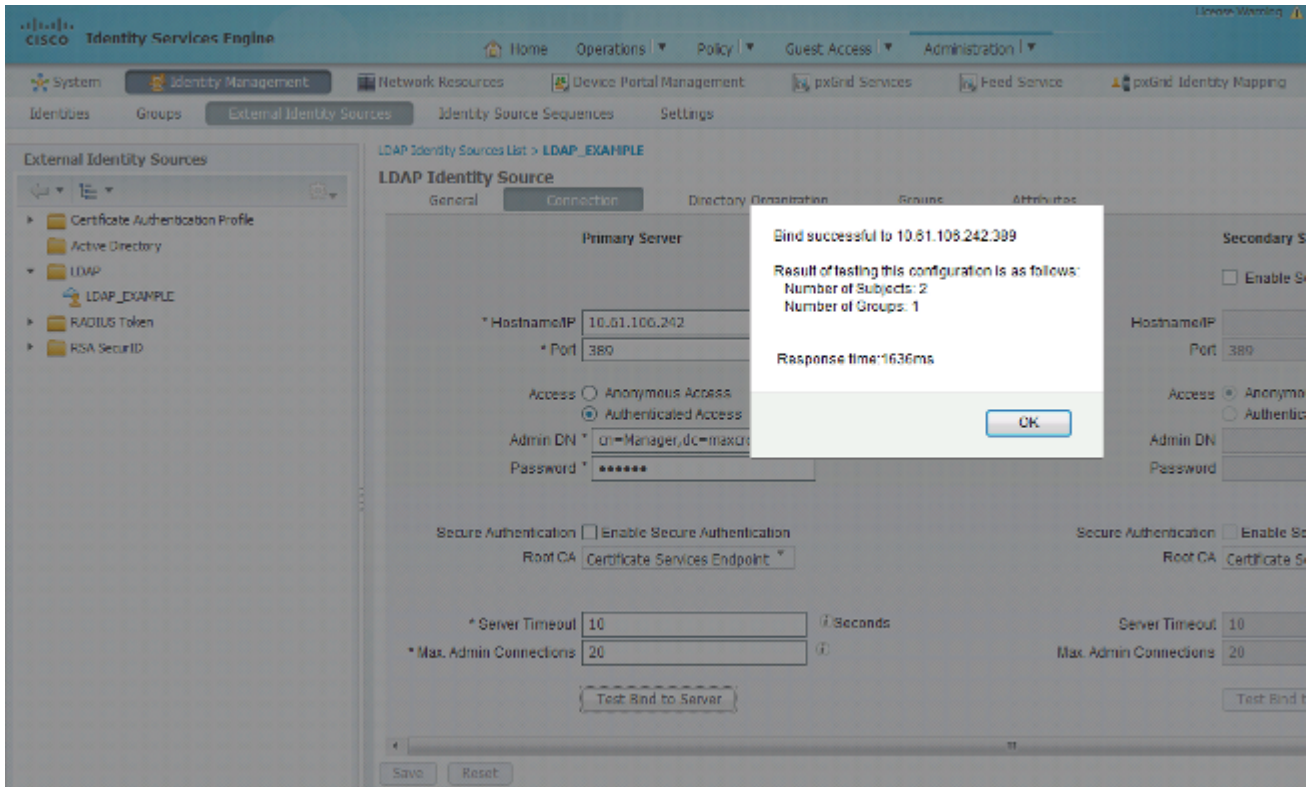
Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✓	Users in LDAP store	if (Wireless_802.1X AND LDAP_EXAMPLE:ExternalGroups EQUALS cn=domainusers,ou=groups,dc=maxxc,dc=com )	then PermitAccess
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	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

Nachdem Sie die Konfiguration angewendet haben, sollten Sie in der Lage sein, eine Verbindung zum Netzwerk herzustellen:



## Überprüfung

Um die LDAP- und ISE-Konfigurationen zu überprüfen, rufen Sie die Themen und Gruppen mit einer Testverbindung zum Server ab:



Die folgenden Bilder illustrieren einen Beispielbericht der ISE:

The dashboard shows the following summary statistics:

- Reconfigured Suppliants: 1
- Misconfigured Network Devices: 0
- RADIUS Drops: 1305
- Client Stopped Responding: 0

Below the statistics is a table of sessions with the following columns: Time, Status, Details, Repeat Count, Identity, Endpoint ID, Endpoint Profile, Authentication Policy, Authorization Policy, and Authorization Profiles.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2013-06-04 21:50:45.538	ⓘ		0	john.doe	C0:4A:00:14:8D:4B	Windows7-Workst...			
2013-06-04 21:59:45.510	✔			john.doe	C0:4A:00:14:8D:4B	Windows7-Workst...	Default >> Dot1X >> Default	Default >> Users in LDAP store	PermitAccess

The 'Overview' section of the report displays the following details for the event:

- Event:** 5200 Authentication succeeded
- Username:** john.doe
- Endpoint Id:** C0:4A:00:14:8D:4B
- Endpoint Profile:** Windows7-Workstation
- Authentication Policy:** Default >> Dot1X >> Default
- Authorization Policy:** Default >> Users in LDAP store
- Authorization Result:** PermitAccess



## 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

## Fehlerbehebung

In diesem Abschnitt werden einige häufige Fehler beschrieben, die bei dieser Konfiguration aufgetreten sind, und es wird beschrieben, wie diese Fehler behoben werden:

- Wenn nach der Installation von OpenLDAP ein Fehler auftritt, der anzeigt, dass eine **gssapi.dll** fehlt, starten Sie Microsoft Windows neu.
- Möglicherweise ist es nicht möglich, die Datei *configuration.xml* für Cisco AnyConnect direkt zu bearbeiten. Speichern Sie die neue Konfiguration an einem anderen Speicherort, und ersetzen Sie dann die alte Datei.
- Im Authentifizierungsbericht wird die folgende Fehlermeldung angezeigt:

```
<#root>
```

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

Diese Fehlermeldung zeigt an, dass die ausgewählte Methode nicht von LDAP unterstützt wird.

Stellen Sie sicher, dass das *Authentifizierungsprotokoll* im gleichen Bericht eine der unterstützten Methoden anzeigt (EAP-GTC, EAP-TLS oder PEAP-TLS).

- Wenn Sie im Authentifizierungsbericht feststellen, dass der Betreff nicht im Identitätsspeicher gefunden wurde, stimmt der Benutzername aus dem Bericht nicht mit dem *Betreffnamenattribut* für einen Benutzer in der LDAP-Datenbank überein.

In diesem Szenario wurde der Wert für dieses Attribut auf **uid** gesetzt, was bedeutet, dass die ISE die *uid*-Werte für den LDAP-Benutzer überprüft, wenn sie versucht, eine Übereinstimmung zu finden.

- Wenn die Themen und Gruppen während eines *Binding an Server*-Tests nicht korrekt abgerufen werden, ist dies eine falsche Konfiguration für die Suchbasen.

Denken Sie daran, dass die LDAP-Hierarchie von Leaf-to-Root und *DC* angegeben werden muss (kann aus mehreren Wörtern bestehen).

---

**Tipp:** Informationen zur Fehlerbehebung der EAP-Authentifizierung auf WLC-Seite finden Sie im Dokument [EAP Authentication with WLAN Controllers \(WLC\) Configuration Example](#) Cisco.

---

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.