

# Configurer l'ISE pour l'intégration à un serveur LDAP

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurer OpenLDAP](#)

[Intégrer OpenLDAP à l'ISE](#)

[Configurer le WLC](#)

[Configurer EAP-GTC](#)

[Vérifier](#)

[Dépannage](#)

---

## Introduction

Ce document décrit comment configurer un moteur Cisco Identity Services Engine (ISE) pour l'intégration à un serveur Cisco LDAP.

## Conditions préalables

### Exigences

Aucune exigence spécifique n'est associée à ce document.

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles et matérielles suivantes :

- Cisco ISE version 1.3 avec correctif 2
- Microsoft Windows Version 7 x64 avec OpenLDAP installé
- Contrôleur LAN sans fil Cisco (WLC) version 8.0.10.0
- Cisco AnyConnect version 3.1 pour Microsoft Windows

- Éditeur de profil Cisco Network Access Manager

---

 Remarque : ce document est valide pour les configurations qui utilisent LDAP comme source d'identité externe pour l'authentification et l'autorisation ISE.

---

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Ces méthodes d'authentification sont prises en charge avec LDAP :

- Extensible Authentication Protocol - Carte à jeton générique (EAP-GTC)
- Protocole EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
- Protocole PEAP-TLS (Protected Extensible Authentication Protocol - Transport Layer Security)

## Configurer

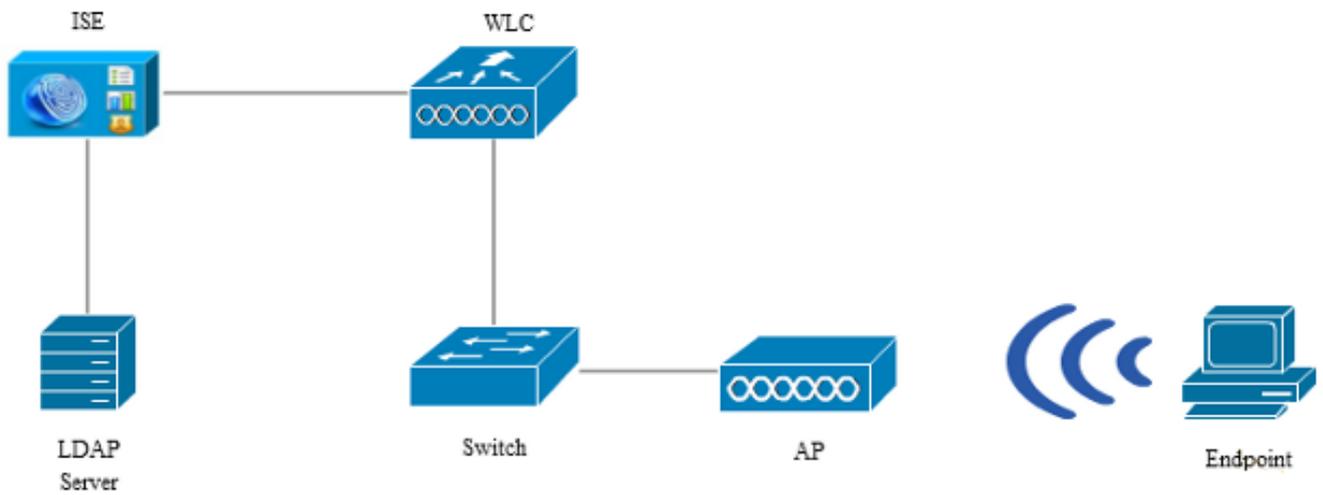
Cette section décrit comment configurer les périphériques réseau et intégrer l'ISE à un serveur LDAP.

### Diagramme du réseau

Dans cet exemple de configuration, le point d'extrémité utilise une carte sans fil afin de s'associer au réseau sans fil.

Le réseau local sans fil (WLAN) sur le WLC est configuré afin d'authentifier les utilisateurs via l'ISE. Sur ISE, LDAP est configuré en tant que magasin d'identités externe.

Cette image illustre la topologie de réseau utilisée :



## Configurer OpenLDAP

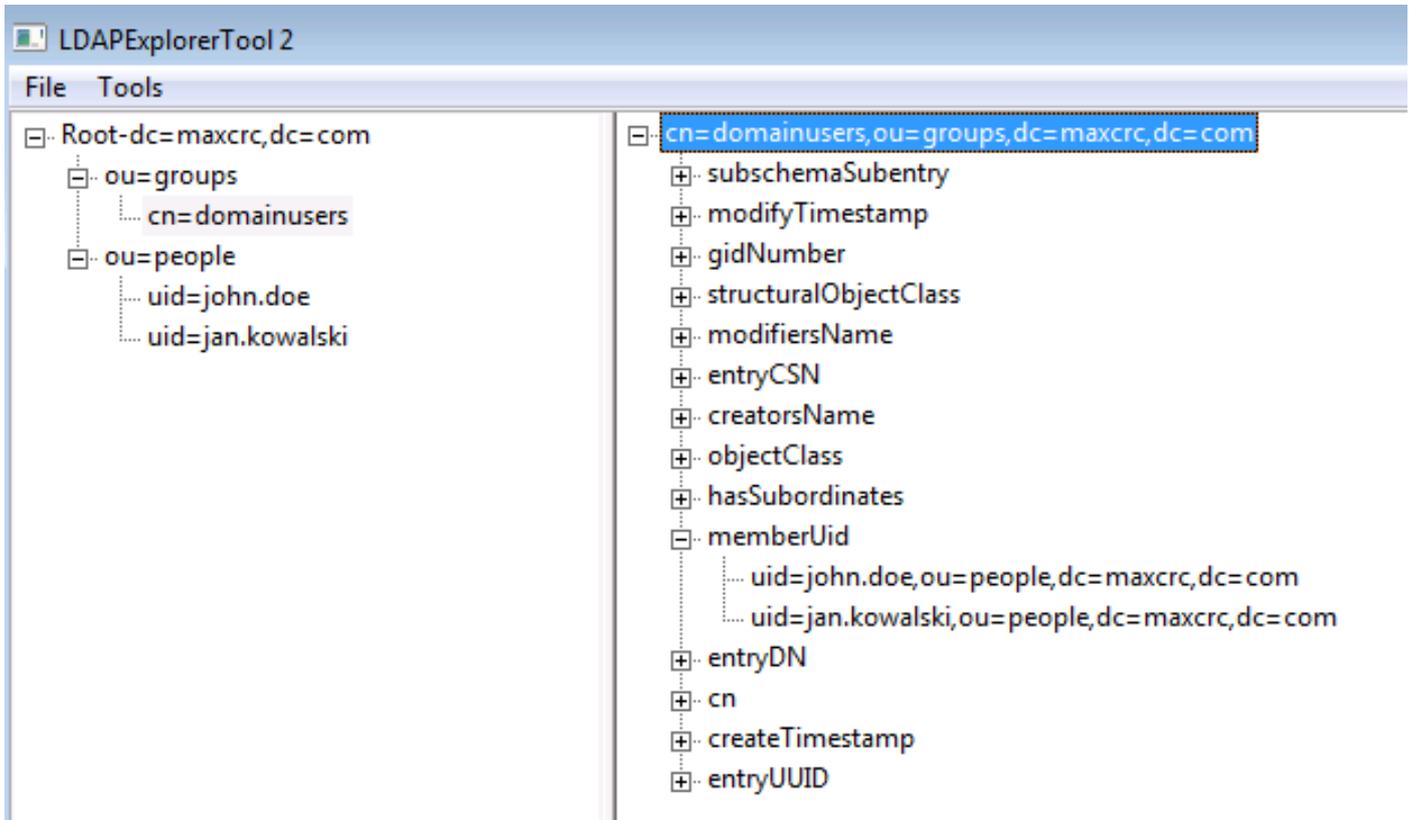
L'installation d'OpenLDAP pour Microsoft Windows est effectuée via l'interface graphique utilisateur, et c'est simple. L'emplacement par défaut est C: > OpenLDAP. Après l'installation, vous devriez voir ce répertoire :

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

Prenez note de deux répertoires en particulier :

- ClientTools - Cet annuaire inclut un ensemble de binaires qui sont utilisés afin de modifier la base de données LDAP.
- Idifdata - Il s'agit de l'emplacement dans lequel vous devez stocker les fichiers avec des objets LDAP.

Ajoutez cette structure à la base de données LDAP :



Dans le répertoire Root, vous devez configurer deux unités d'organisation (OU). L'unité d'organisation OU=groups doit avoir un groupe enfant (cn=domainusers dans cet exemple).

L'unité d'organisation OU=people définit les deux comptes d'utilisateur qui appartiennent au groupe cn=domainusers.

Pour remplir la base de données, vous devez d'abord créer le fichier ldif. La structure mentionnée précédemment a été créée à partir de ce fichier :

```
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
```

Afin d'ajouter les objets à la base de données LDAP, utilisez le binaire ldapmodify :

```
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"

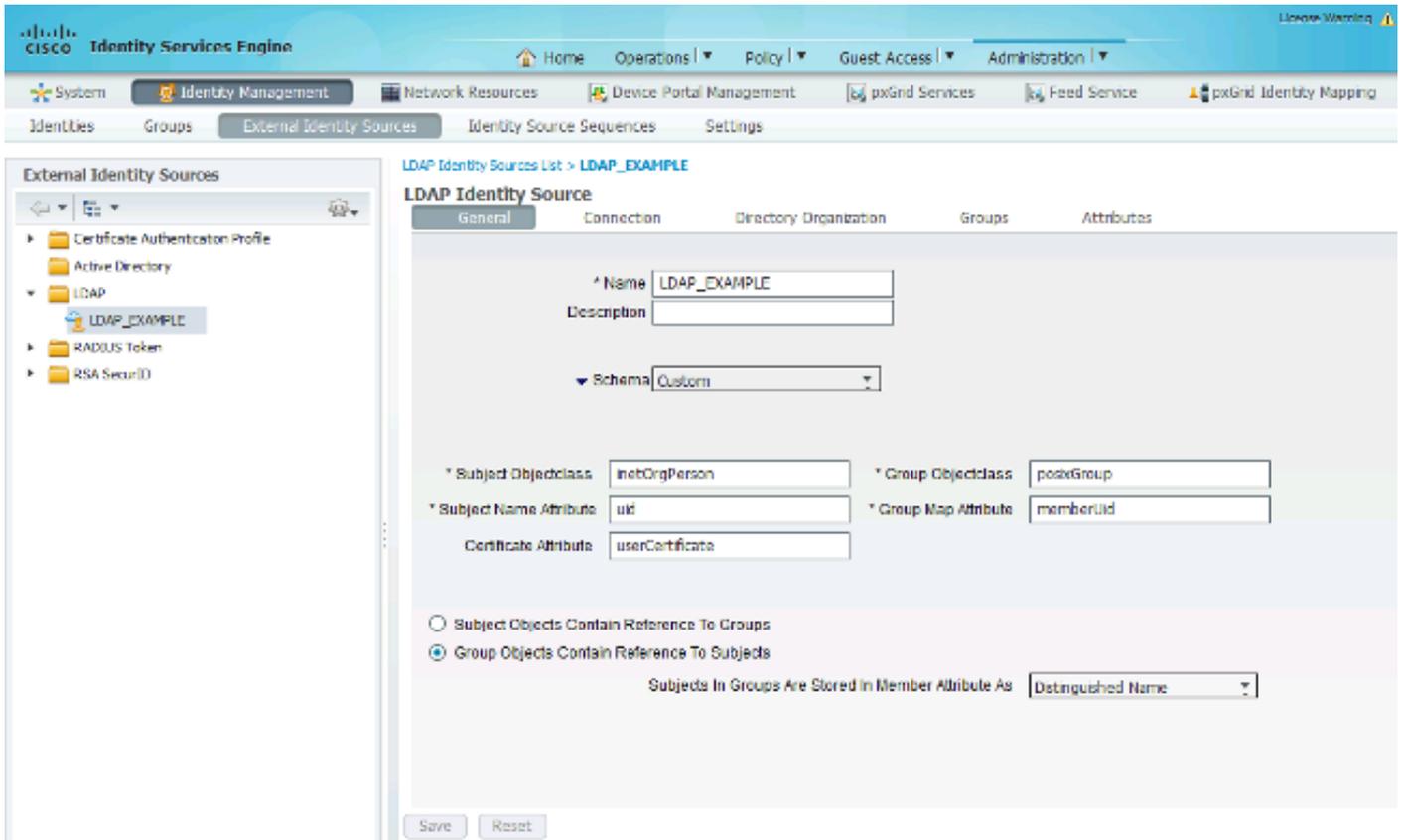
adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

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

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

## Intégrer OpenLDAP à l'ISE

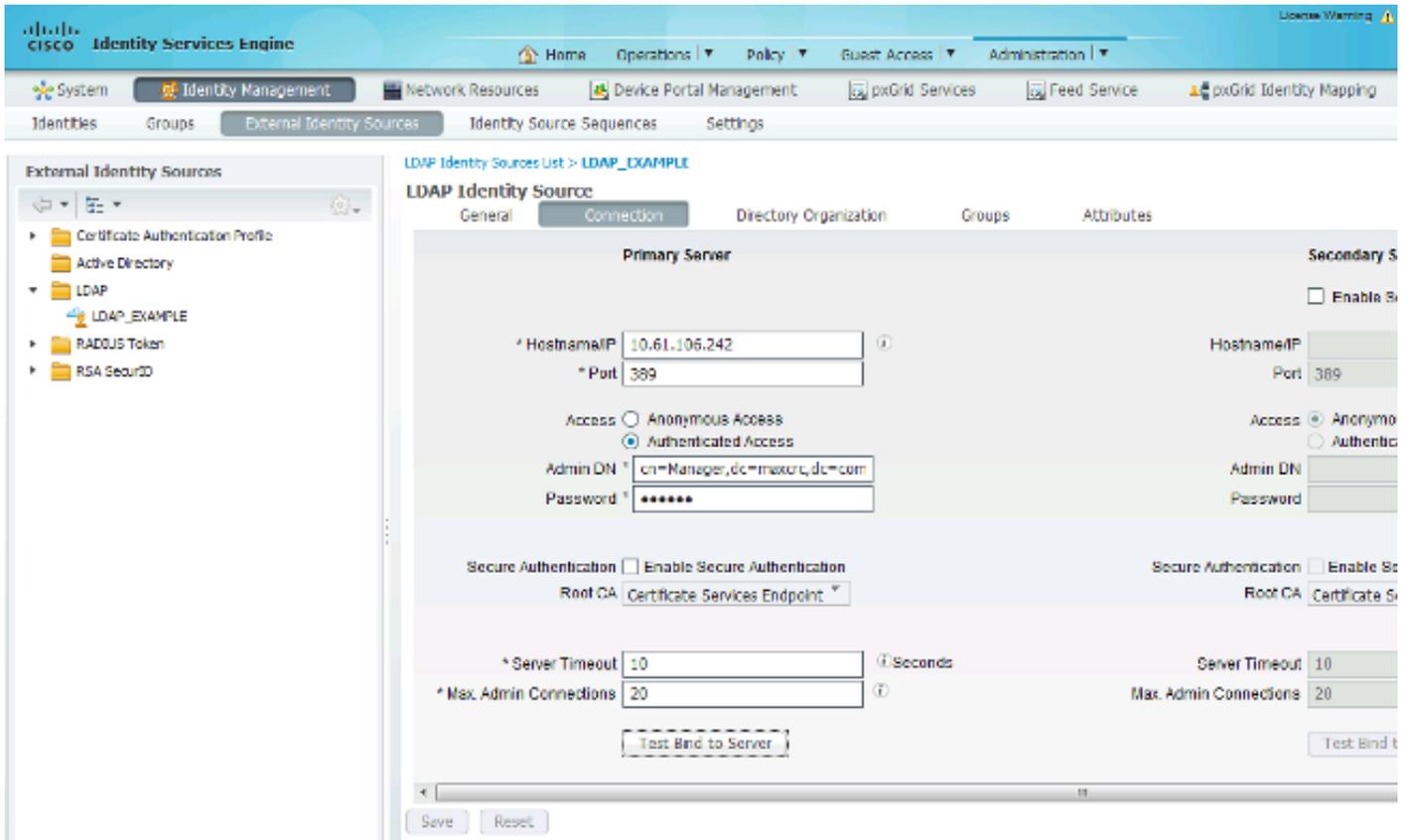
Utilisez les informations fournies dans les images tout au long de cette section afin de configurer LDAP en tant que magasin d'identités externe sur l'ISE.



Vous pouvez configurer ces attributs à partir de l'onglet Général :

- Subject Objectclass - Ce champ correspond à la classe d'objet des comptes d'utilisateurs dans le fichier ldif. Selon la configuration LDAP. Utilisez l'une des quatre classes suivantes :
  - Haut
  - Personne
  - PersonneOrganisationnelle
  - PersonnelnetOrg
- Attribut de nom de sujet - Attribut récupéré par le serveur LDAP lorsque l'ISE demande si un nom d'utilisateur spécifique est inclus dans une base de données. Dans ce scénario, vous devez utiliser john.doe ou jan.kowalski comme nom d'utilisateur sur le point d'extrémité.
- Group Objectclass - Ce champ correspond à la classe d'objet d'un groupe dans le fichier ldif. Dans ce scénario, la classe d'objet pour le groupe cn=domainusers est posixGroup.
- Attribut de mappage de groupe - Cet attribut définit la façon dont les utilisateurs sont mappés aux groupes. Sous le groupe cn=domainusers dans le fichier ldif, vous pouvez voir deux attributs memberUid qui correspondent aux utilisateurs.

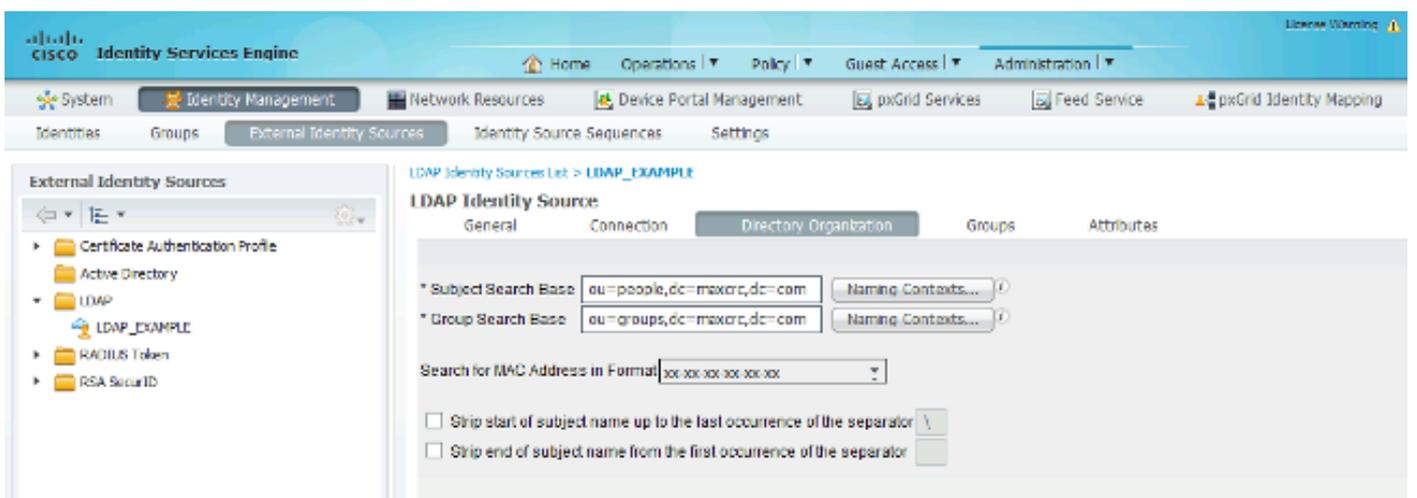
ISE propose également des schémas préconfigurés (Microsoft Active Directory, Sun, Novell) :



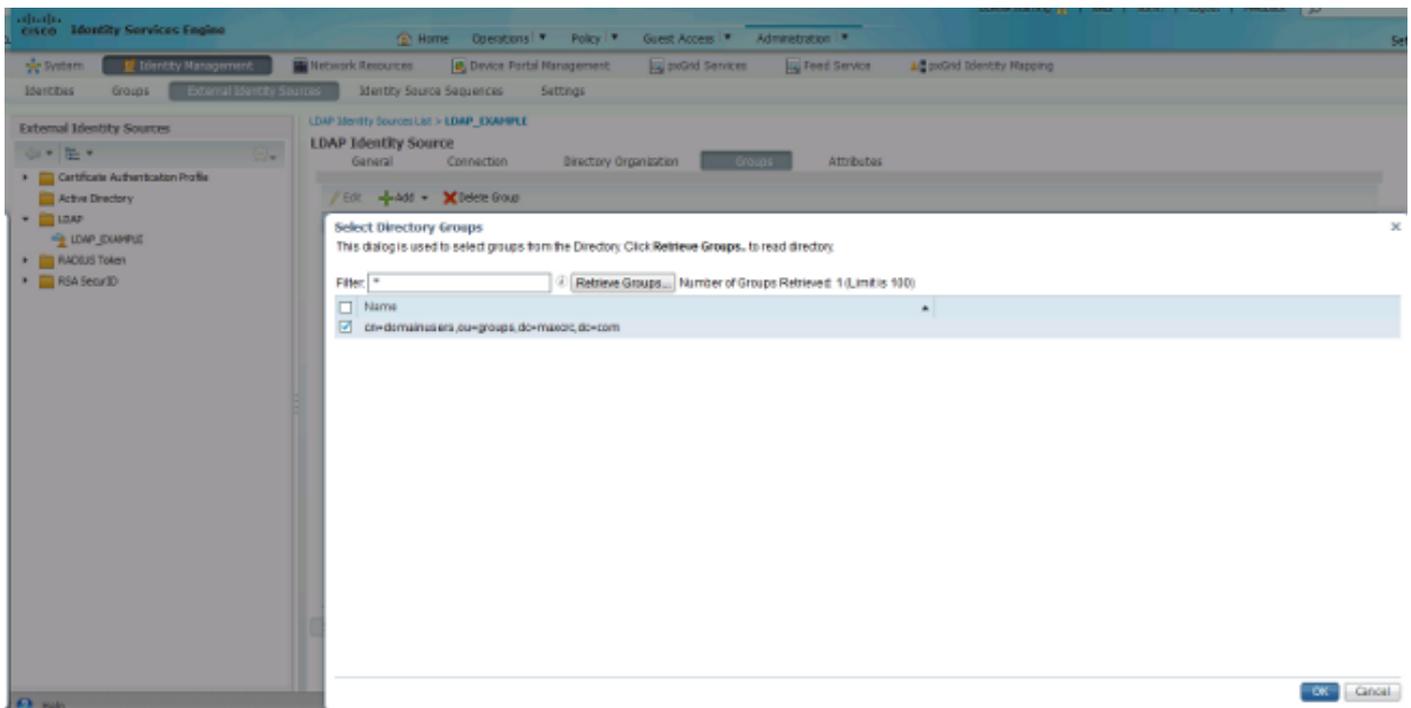
Après avoir défini l'adresse IP et le nom de domaine administratif corrects, vous pouvez tester la liaison au serveur. À ce stade, vous ne récupérez aucun objet ou groupe, car les bases de recherche ne sont pas encore configurées.

Dans l'onglet suivant, configurez la base de recherche des sujets/groupes. Il s'agit du point de jonction entre l'ISE et le LDAP. Vous ne pouvez récupérer que les sujets et les groupes qui sont des enfants de votre point de jonction.

Dans ce scénario, les sujets de l'OU=people et les groupes de l'OU=groups sont récupérés :

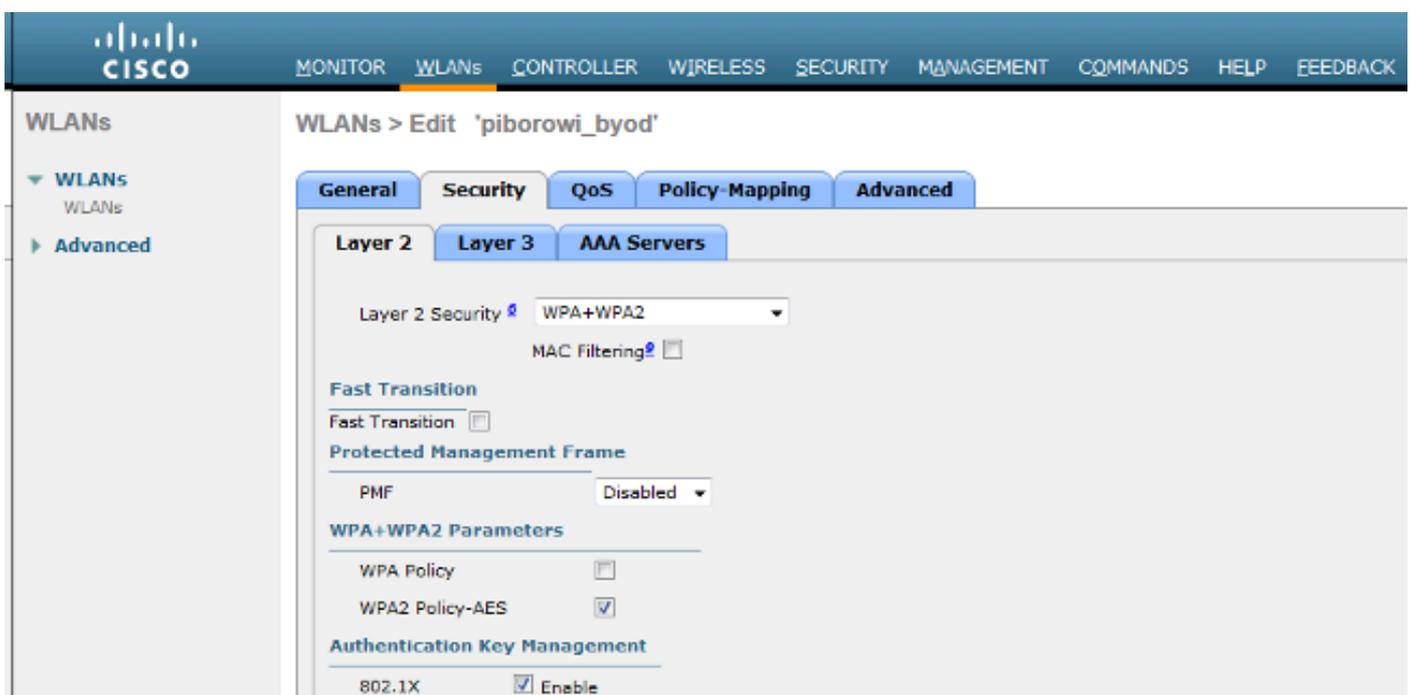


Dans l'onglet Groups, vous pouvez importer les groupes à partir du LDAP sur l'ISE :



## Configurer le WLC

Utilisez les informations fournies dans ces images afin de configurer le WLC pour l'authentification 802.1x :



The screenshot shows the Cisco AnyConnect configuration interface for the WLAN 'piborowi\_byod'. The 'Advanced' tab is selected, and the 'AAA Servers' sub-tab is active. The configuration includes:

- General:** Security, QoS, Policy-Mapping, Advanced
- Layer 2 / Layer 3 / AAA Servers:** Layer 2, Layer 3, AAA Servers
- Select AAA servers below to override use of default servers on this WLAN**
- Radius Servers:**
  - Radius Server Overwrite interface:  Enabled
- Authentication Servers:**
  - Enabled
  - Server 1: IP:10.62.145.51, Port:1812
  - Server 2: None
  - Server 3: None
  - Server 4: None
  - Server 5: None
  - Server 6: None
- Accounting Servers:**
  - Enabled
  - Server 1: IP:10.62.145.51, Port:1813
  - Server 2: None
  - Server 3: None
  - Server 4: None
  - Server 5: None
  - Server 6: None
- EAP Parameters:**
  - Enable:

This screenshot is identical to the one above, showing the configuration for the WLAN 'piborowi\_byod' with the AAA Servers section expanded.

## Configurer EAP-GTC

EAP-GTC est l'une des méthodes d'authentification prises en charge pour LDAP. Il est disponible dans Cisco AnyConnect, mais vous devez installer l'Éditeur de profil Network Access Manager pour configurer correctement le profil.

Vous devez également modifier la configuration du Gestionnaire d'accès réseau, qui (par défaut) se trouve ici :

```
C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager
> system > fichier configuration.xml
```

Utilisez les informations fournies dans ces images afin de configurer l'EAP-GTC sur le terminal :

The screenshot shows the 'AnyConnect Profile Editor - Network Access Manager' interface. The main window is titled 'Networks' and shows the configuration for a profile named 'eap\_gtc'. The profile path is '...ility Client\Network Access Manager\system\configuration.xml'. The configuration is divided into several sections:

- Name:** eap\_gtc
- Group Membership:** In all groups (Global) is selected. The 'In group' dropdown is set to 'Local networks'.
- Choose Your Network Media:** 'Wi-Fi (wireless) Network' is selected. The 'Wired (802.3) Network' option is also visible with instructions: 'Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.' The 'Wi-Fi (wireless) Network' option has instructions: 'Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.' The SSID (max 32 chars) is 'pborowi\_byod'. There are checkboxes for 'Hidden Network' and 'Corporate Network', both of which are unchecked. The Association Timeout is set to 5 seconds.
- Common Settings:** A text box for a script or application to run when connected is empty. A 'Browse Local Machine' button is next to it. The Connection Timeout is set to 40 seconds.

At the bottom of the window, there are 'Next' and 'Cancel' buttons. On the right side, there is a vertical list of tabs: 'Media Type', 'Security Level', 'Connection Type', 'User Auth', and 'Credentials'. The 'Media Type' tab is currently selected.



## 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

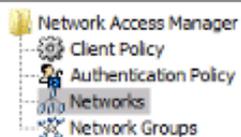
authPeriod (sec.)	<input type="text" value="30"/>	startPeriod (sec.)	<input type="text" value="30"/>
heldPeriod (sec.)	<input type="text" value="60"/>	maxStart	<input type="text" value="3"/>

### Association Mode

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

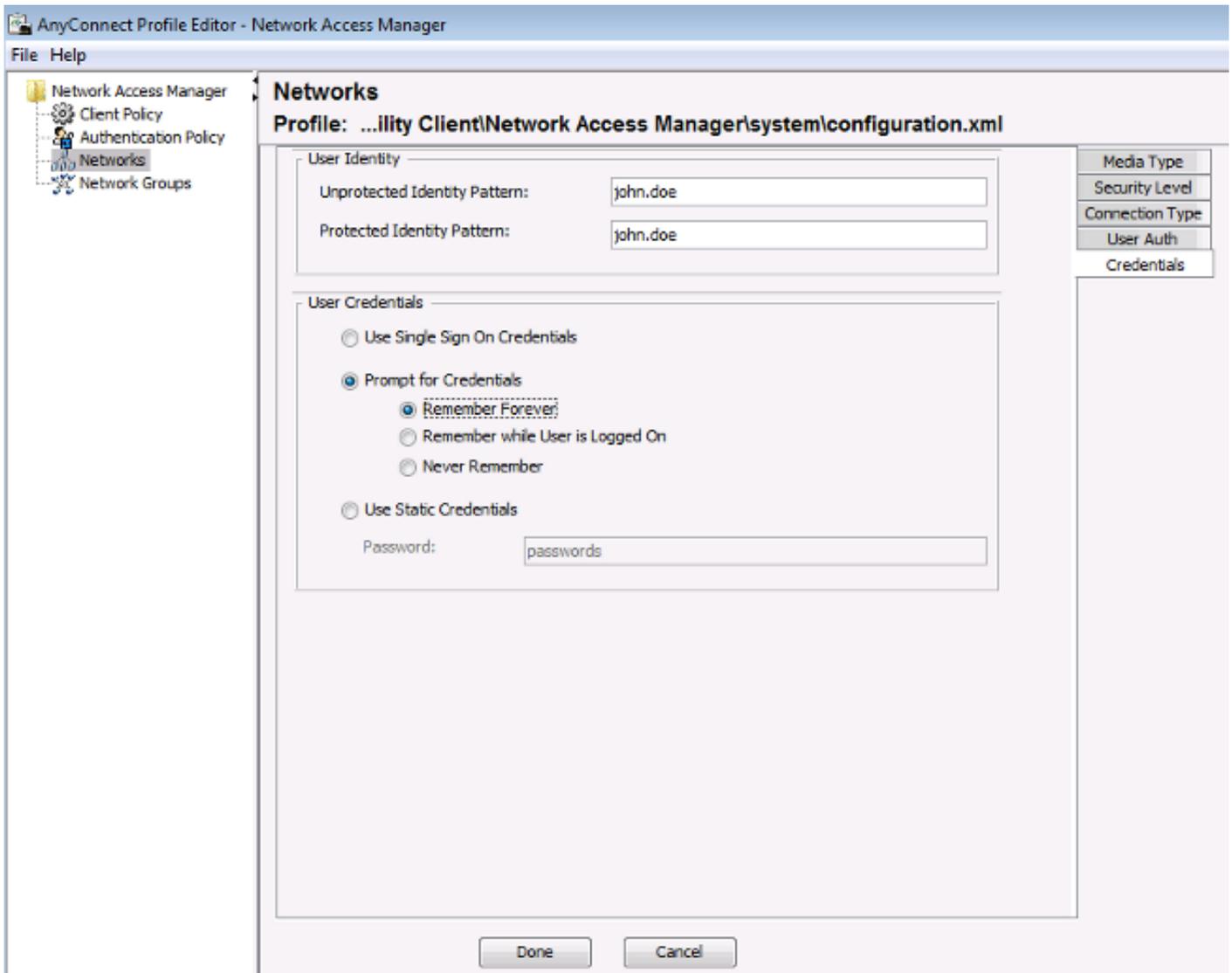
EAP-TLS, using a Certificate

Authenticate using a Token and EAP-GTC

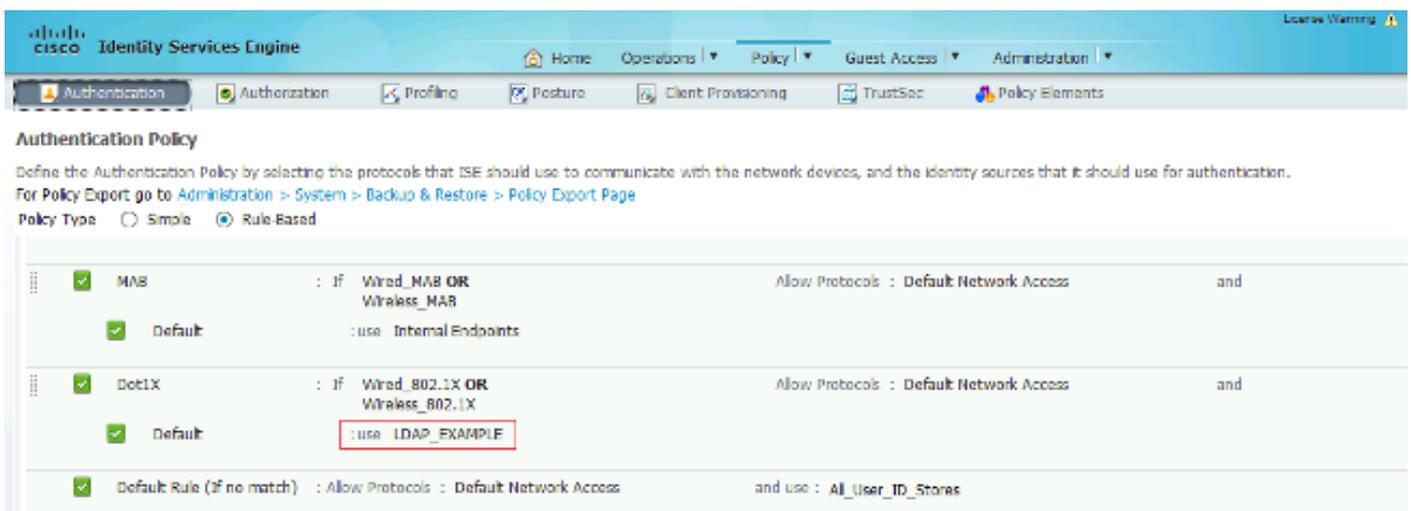
- Media Type
- Security Level
- Connection Type
- User Auth
- Credentials

Next

Cancel



Utilisez les informations fournies dans ces images afin de modifier les stratégies d'authentification et d'autorisation sur l'ISE :



**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

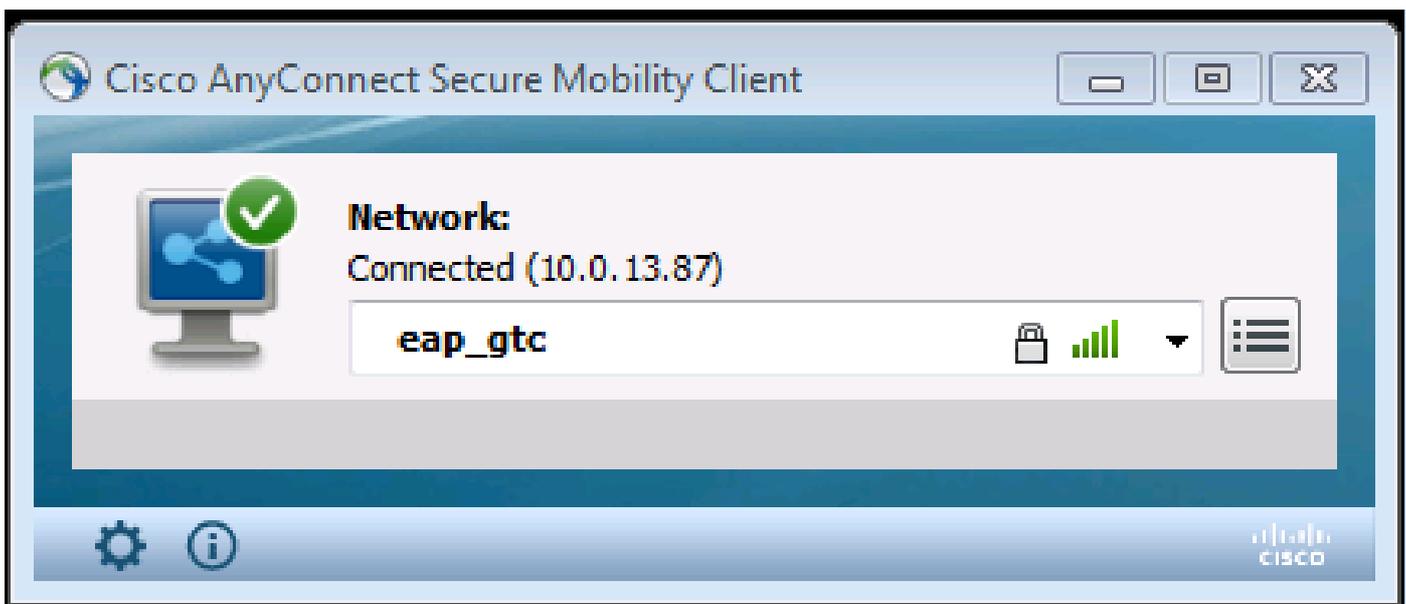
First Matched Rule Applies

Exceptions (0)

Standard

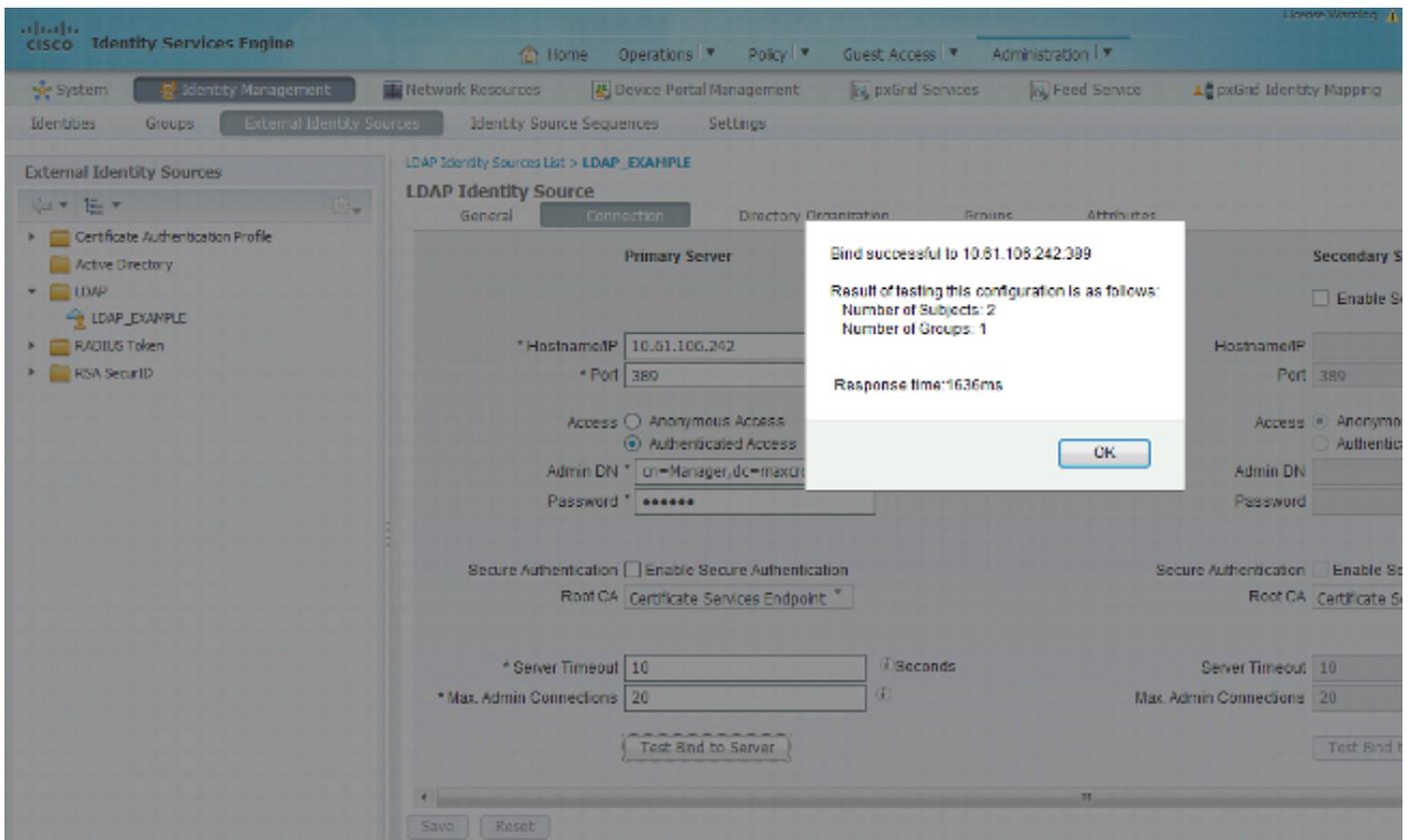
Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✔	Users in LDAP store	if (Wireless_802.1X AND LDAP_EXAMPLE:ExternalGroups EQUALS cn=domainusers,ou=groups,dc=mxcorp,dc=com )	then PermitAccess
✔	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access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

Après avoir appliqué la configuration, vous devriez pouvoir vous connecter au réseau :

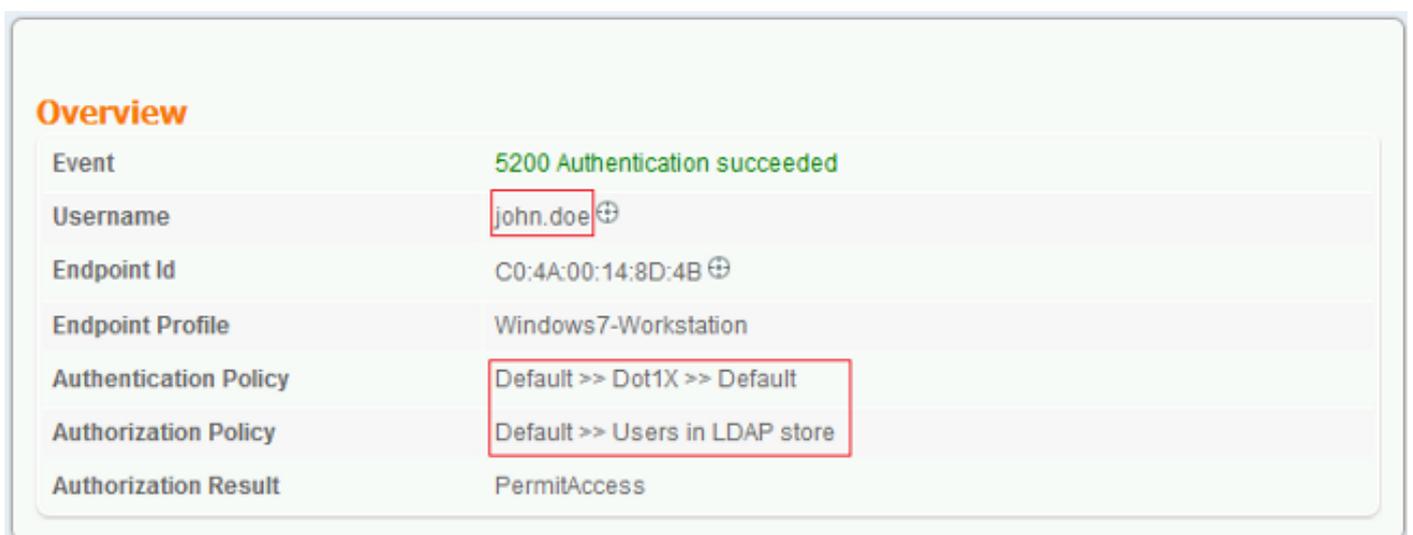
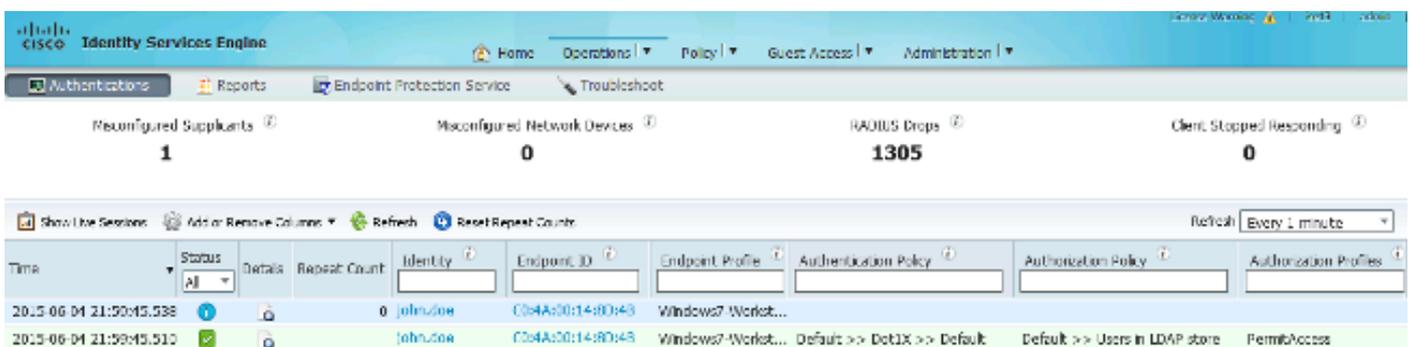


## Vérifier

Afin de vérifier les configurations LDAP et ISE, récupérez les sujets et les groupes avec une connexion test au serveur :



Ces images illustrent un exemple de rapport de l'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

## Dépannage

Cette section décrit quelques erreurs courantes rencontrées avec cette configuration et explique comment les résoudre :

- Après l'installation d'OpenLDAP, si vous rencontrez une erreur indiquant qu'un gssapi.dll est manquant, redémarrez Microsoft Windows.
- Il n'est peut-être pas possible de modifier le fichier configuration.xml pour Cisco AnyConnect directement. Enregistrez votre nouvelle configuration à un autre emplacement, puis utilisez-la pour remplacer l'ancien fichier.
- Le rapport d'authentification contient le message d'erreur suivant :

```
<#root>
```

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

Ce message d'erreur indique que la méthode sélectionnée n'est pas prise en charge par LDAP.

Assurez-vous que le protocole d'authentification dans le même rapport affiche l'une des méthodes prises en charge (EAP-GTC, EAP-TLS ou PEAP-TLS).

- Dans le rapport d'authentification, si vous remarquez que l'objet n'a pas été trouvé dans le magasin d'identités, le nom d'utilisateur du rapport ne correspond pas à l'attribut Nom de l'objet pour tout utilisateur de la base de données LDAP.

Dans ce scénario, la valeur a été définie sur uid pour cet attribut, ce qui signifie que l'ISE recherche les valeurs uid pour l'utilisateur LDAP lorsqu'il tente de trouver une correspondance.

- Si les sujets et les groupes ne sont pas récupérés correctement lors d'un test de liaison au serveur, la configuration des bases de recherche est incorrecte.

N'oubliez pas que la hiérarchie LDAP doit être spécifiée de leaf à root et dc (peut être constituée de plusieurs mots).

---

 Conseil : Afin de dépanner l'authentification EAP du côté du WLC, référez-vous au document [Exemple de configuration d'authentification EAP avec des contrôleurs WLAN \(WLC\)](#) Cisco.

---

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.