

配置ISE以与LDAP服务器集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置OpenLDAP](#)

[将OpenLDAP与ISE集成](#)

[配置 WLC](#)

[配置EAP-GTC](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何配置思科身份服务引擎(ISE)，以便与思科LDAP服务器集成。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带补丁2的思科ISE版本1.3
- 安装了OpenLDAP的Microsoft Windows版本7 x64
- 思科无线局域网控制器(WLC)版本8.0.100.0
- 适用于Microsoft Windows的Cisco AnyConnect版本3.1
- 思科网络访问管理器配置文件编辑器



注：本文档对使用LDAP作为ISE身份验证和授权的外部身份源的设置有效。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

LDAP支持以下身份验证方法：

- 可扩展身份验证协议 — 通用令牌卡(EAP-GTC)
- 可扩展身份验证协议 — 传输层安全(EAP-TLS)
- 受保护的可扩展身份验证协议 — 传输层安全(PEAP-TLS)

配置

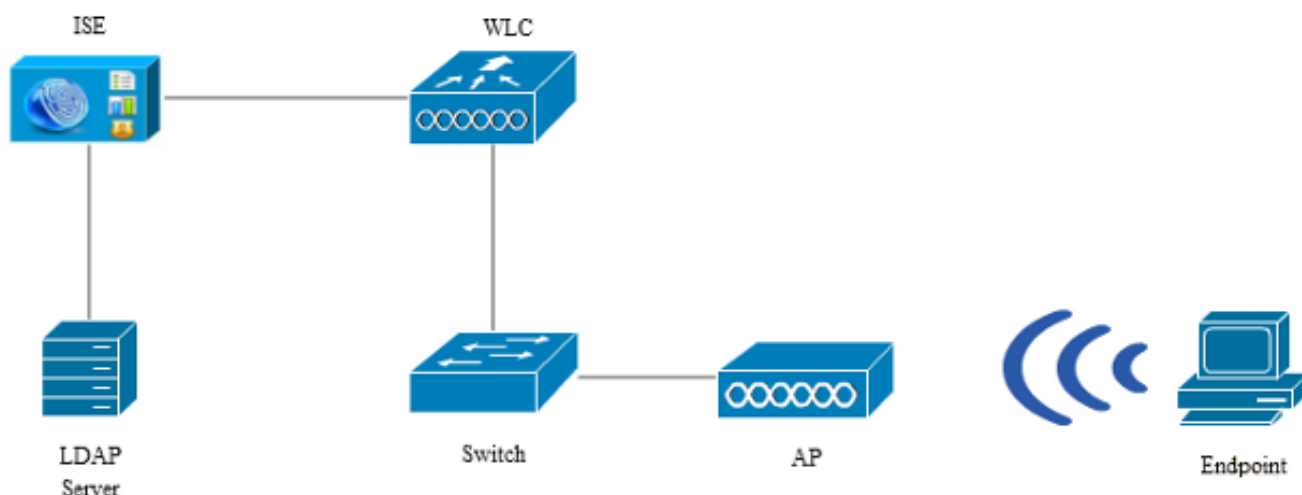
本节介绍如何配置网络设备并将ISE与LDAP服务器集成。

网络图

在此配置示例中，终端使用无线适配器以便与无线网络关联。





























WLC上的无线LAN(WLAN)配置为通过ISE对用户进行身份验证。在ISE上，LDAP配置为外部身份库。

下图说明了使用的网络拓扑：



配置OpenLDAP

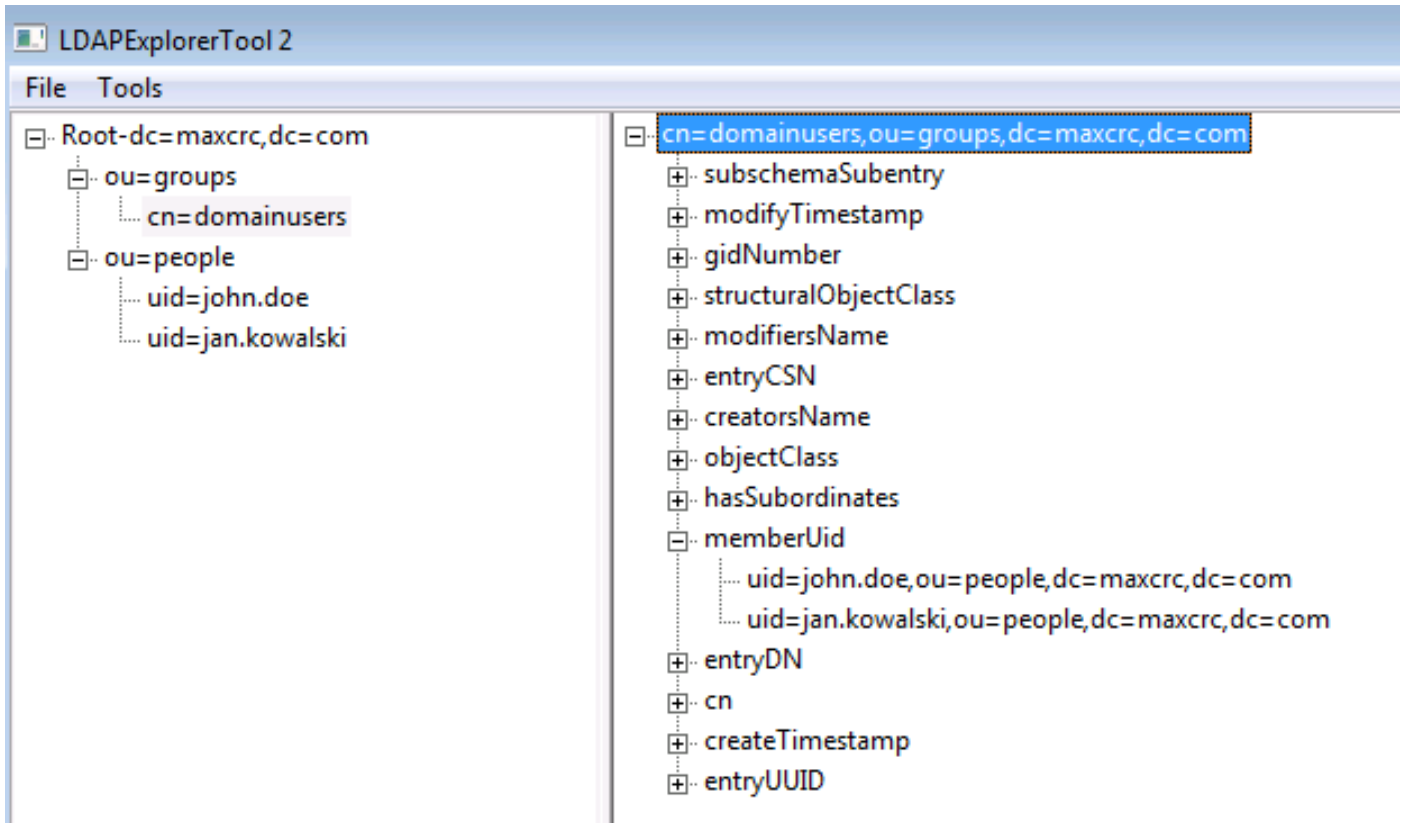
OpenLDAP for Microsoft Windows的安装通过GUI完成，并且非常简单。默认位置为C: > OpenLDAP。安装后，您应该看到以下目录：

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

请特别注意以下两个目录：

- ClientTools — 此目录包含一组用于编辑LDAP数据库的二进制文件。
- Idifdata — 这是应存储具有LDAP对象的文件的位置。

将此结构添加到LDAP数据库：



在Root目录下，必须配置两个组织单位(OU)。OU=groups OU应有一个子组(在本例中为cn=domainusers)。

OU=people OU定义属于cn=domainusers组的两个用户帐户。

要填充数据库，必须先创建ldif文件。前面提到的结构是从以下文件创建的：

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

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

```
dn: uid=john.doe,ou=people,dc=maxcsrc,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
```

要将对象添加到LDAP数据库，请使用ldapmodify二进制：

```
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"

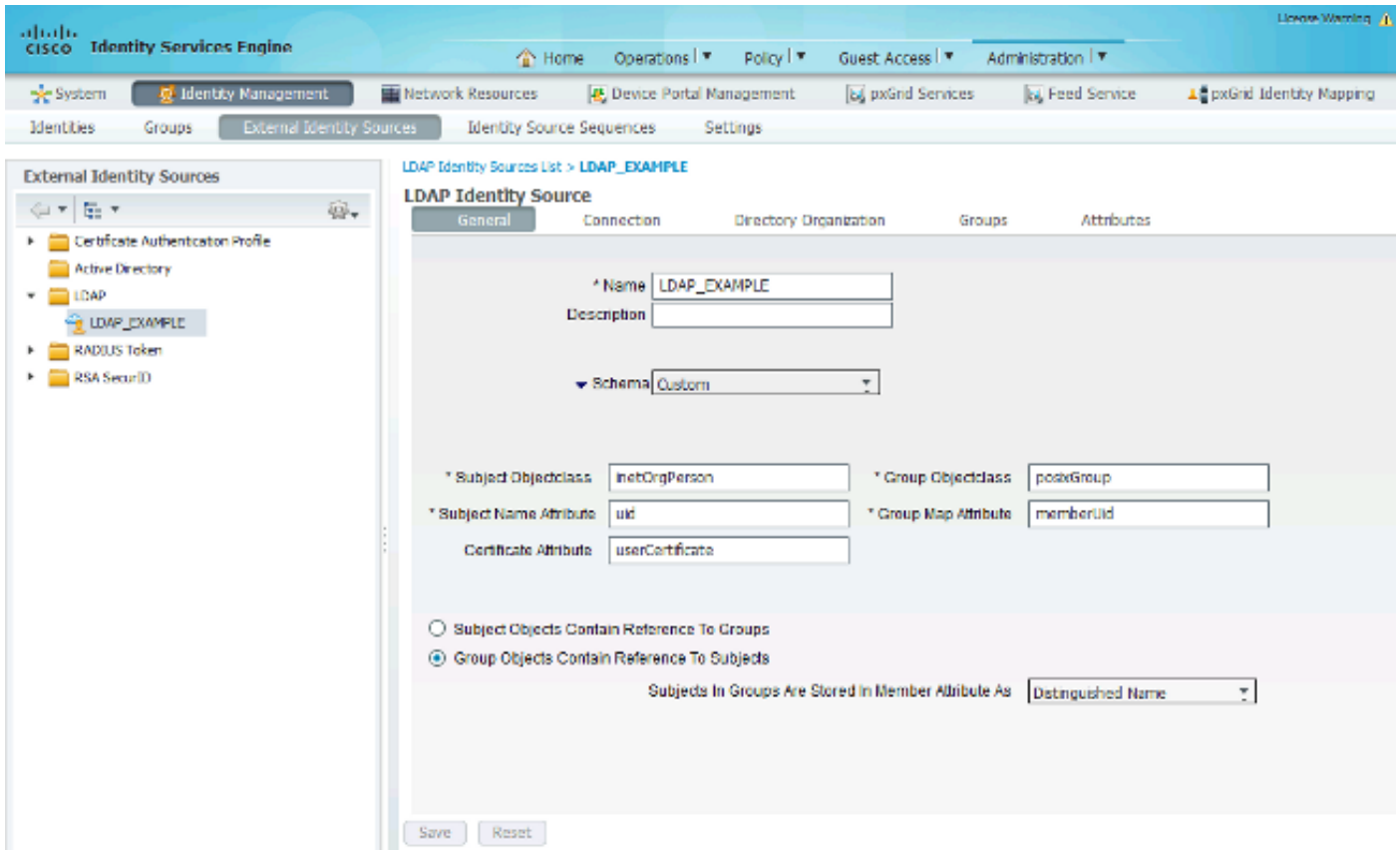
adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

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

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

将OpenLDAP与ISE集成

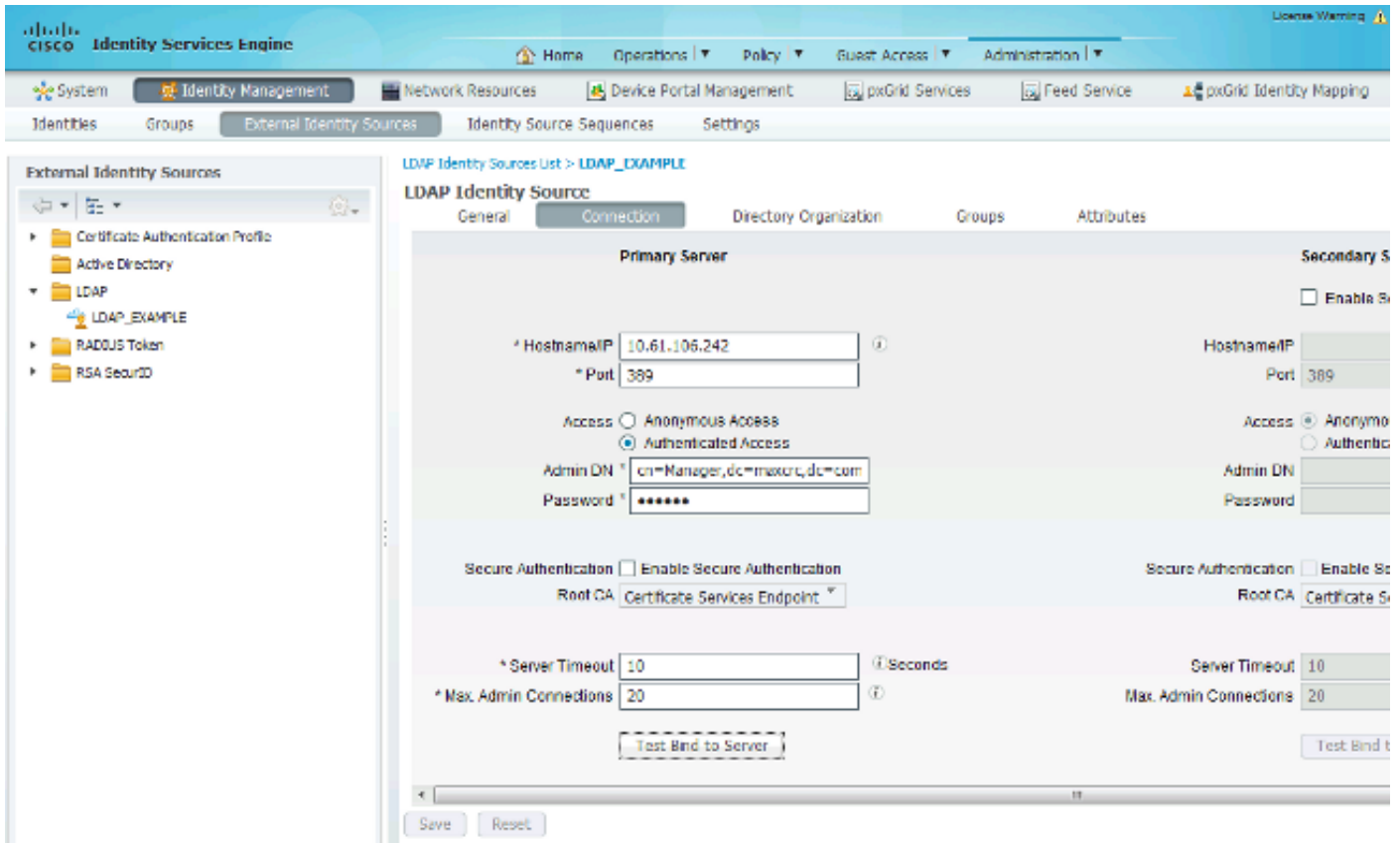
使用本部分中的映像中提供的信息，以便将LDAP配置为ISE上的外部身份库。



可以从General选项卡配置以下属性：

- Subject Objectclass — 此字段对应于Idif文件中用户帐户的对象类。根据LDAP配置，请使用以下四个类之一：
 - 顶部
 - 人员
 - 组织人员
 - InetOrgPerson
- Subject Name Attribute — 这是当ISE查询数据库中是否包含特定用户名时由LDAP检索的属性。在这种情况下，您必须使用john.doe或jan.kowalski作为终端上的用户名。
- Group Objectclass — 此字段与Idif文件中组的对象类对应。在此方案中，cn=domainusers组的对象类是posixGroup。
- 组映射属性 — 此属性定义如何将用户映射到组。在Idif文件中的cn=domainusers组下，可以看到与用户对应的两个memberUid属性。

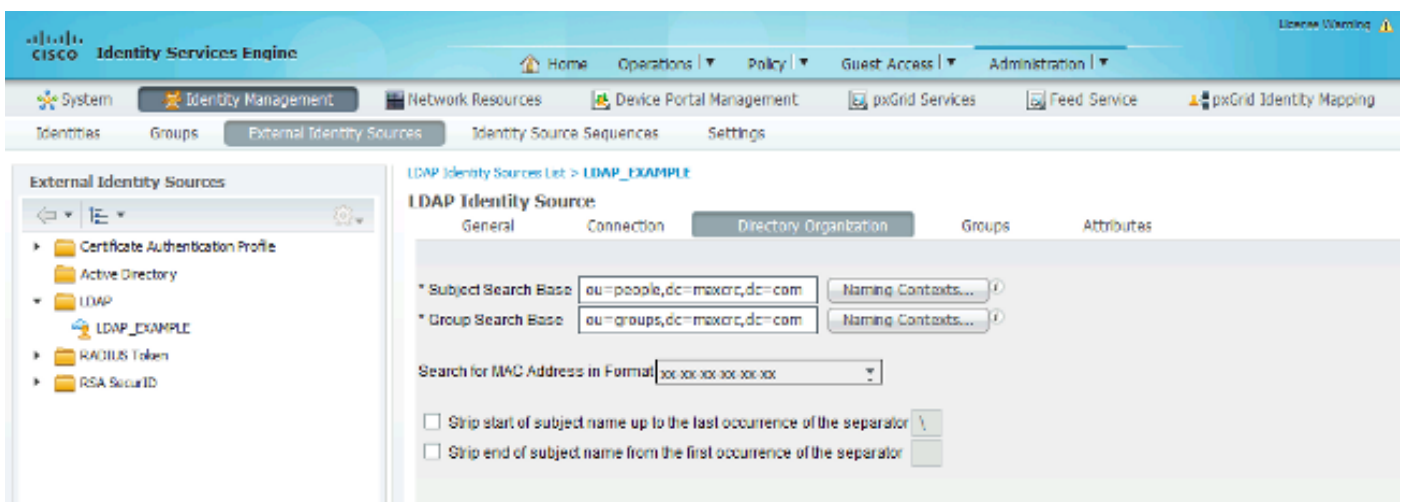
ISE还提供一些预配置的方案(Microsoft Active Directory、Sun、Novell):



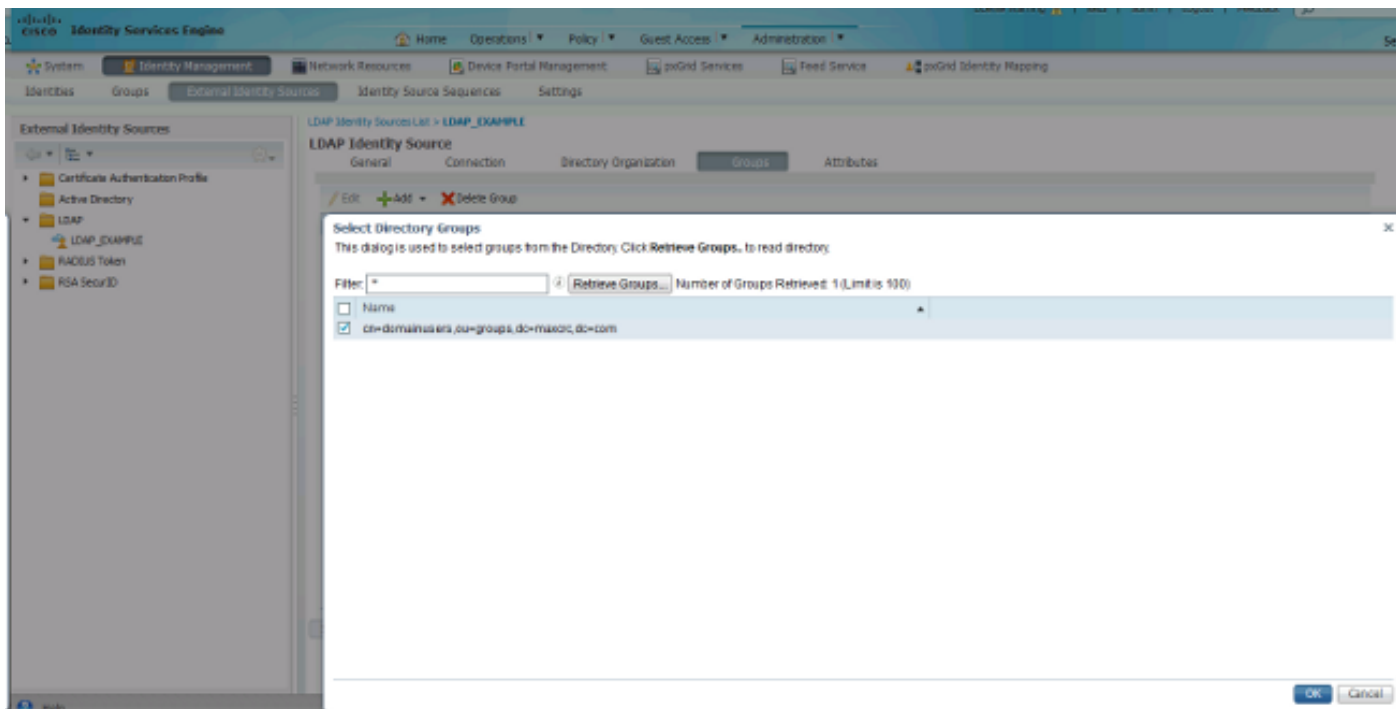
在设置正确的IP地址和管理域名后，您可以Test Bind到服务器。此时，由于尚未配置搜索库，您不会检索任何主题或组。

在下一个选项卡中，配置主题/组搜索库。这是ISE到LDAP的加入点。您只能检索作为加入点子项的主题和组。

在此场景中，检索OU=people中的主题和OU=groups中的组：

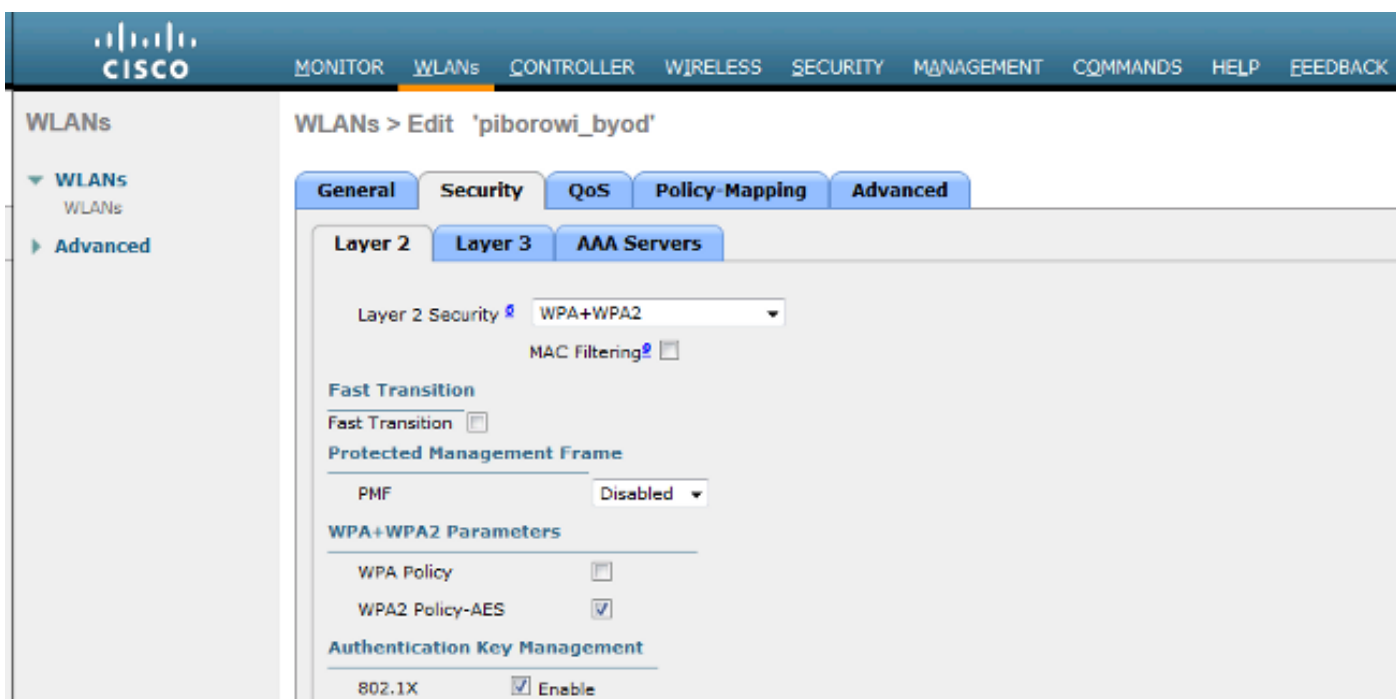


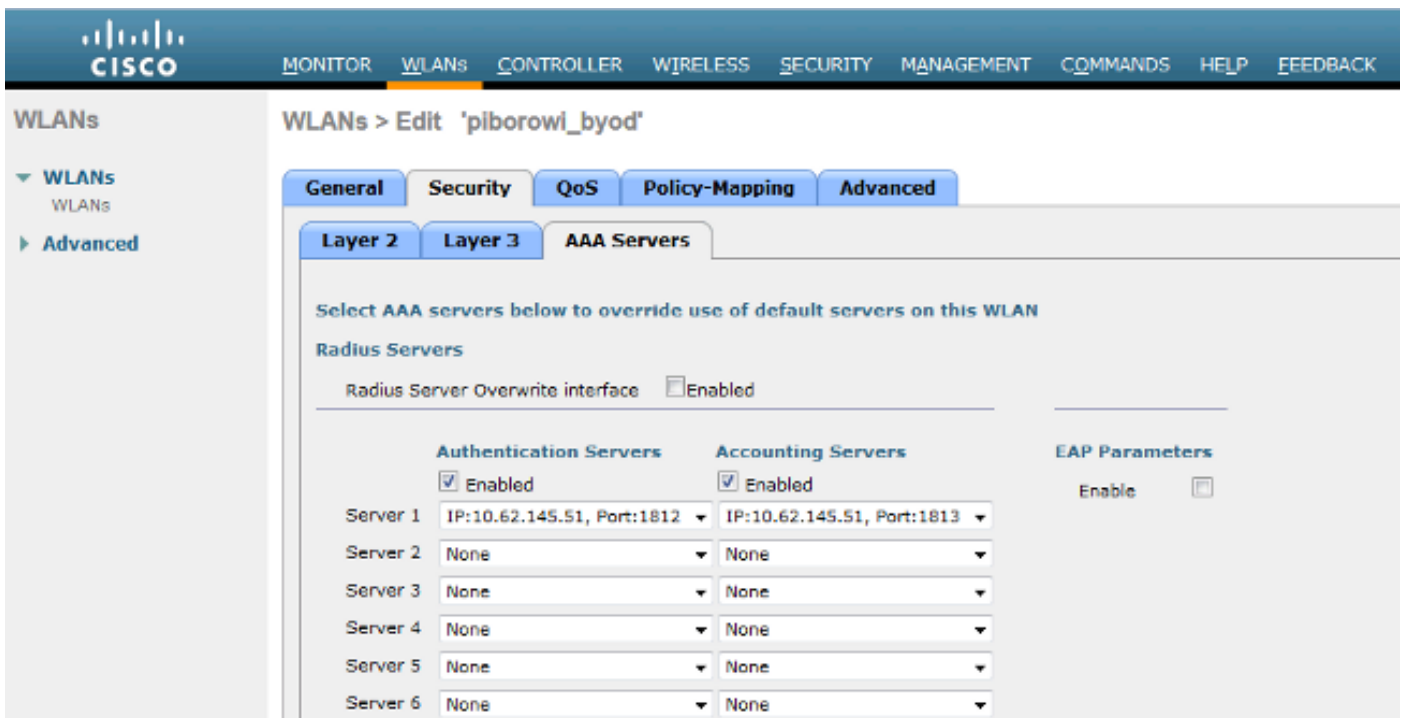
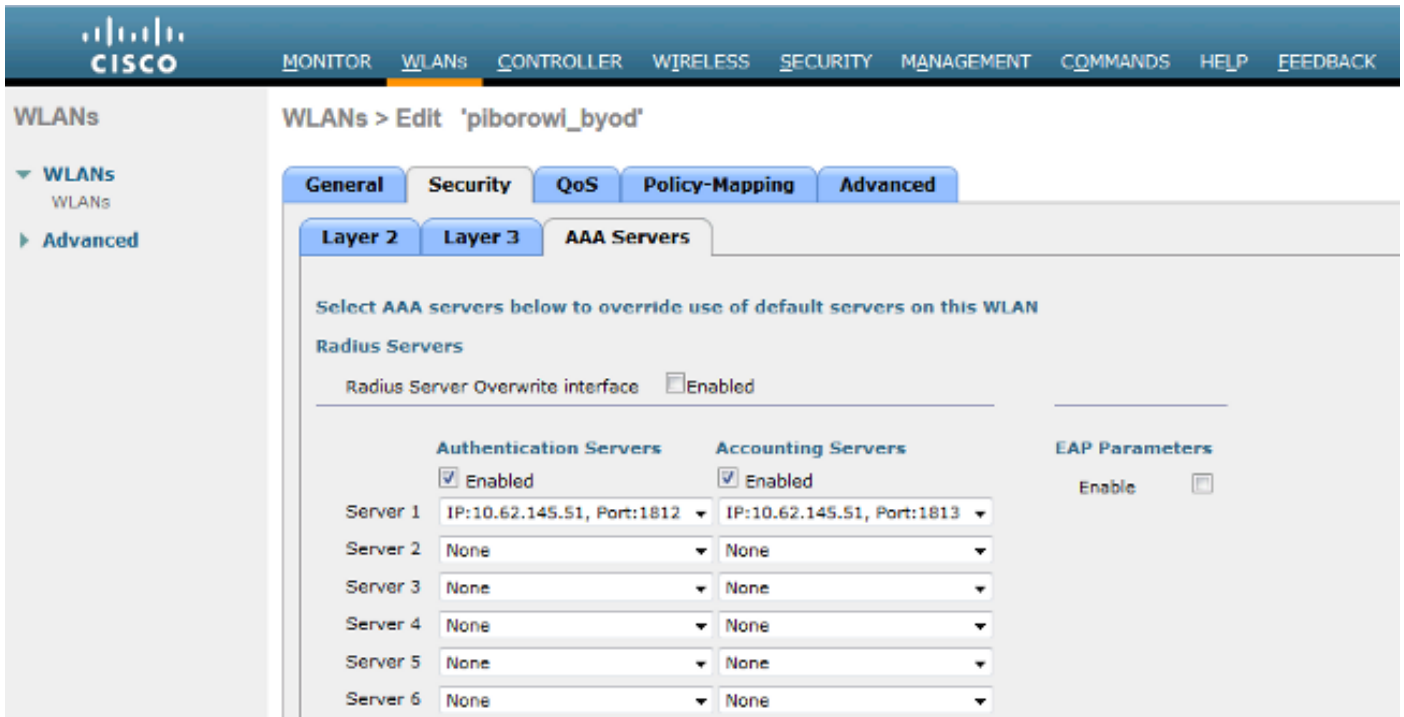
在Groups选项卡中，您可以从ISE上的LDAP导入组：



配置 WLC

使用这些映像中提供的信息配置WLC进行802.1x身份验证：





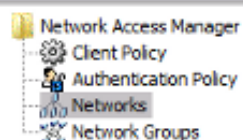
配置EAP-GTC

LDAP支持的身份验证方法之一是EAP-GTC。它在Cisco AnyConnect中可用，但必须安装网络访问管理器配置文件编辑器才能正确配置配置文件。

您还必须编辑网络访问管理器配置，默认情况下，该配置位于以下位置：

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

使用这些映像中提供的信息在终端上配置EAP-GTC:



Networks

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

Name:

Group Membership

In group:

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):

Hidden Network

Corporate Network

Association Timeout: seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout: 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

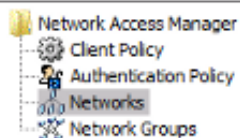
authPeriod (sec.)	<input type="text" value="30"/>	startPeriod (sec.)	<input type="text" value="30"/>
heldPeriod (sec.)	<input type="text" value="60"/>	maxStart	<input type="text" value="3"/>

Association Mode

- 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

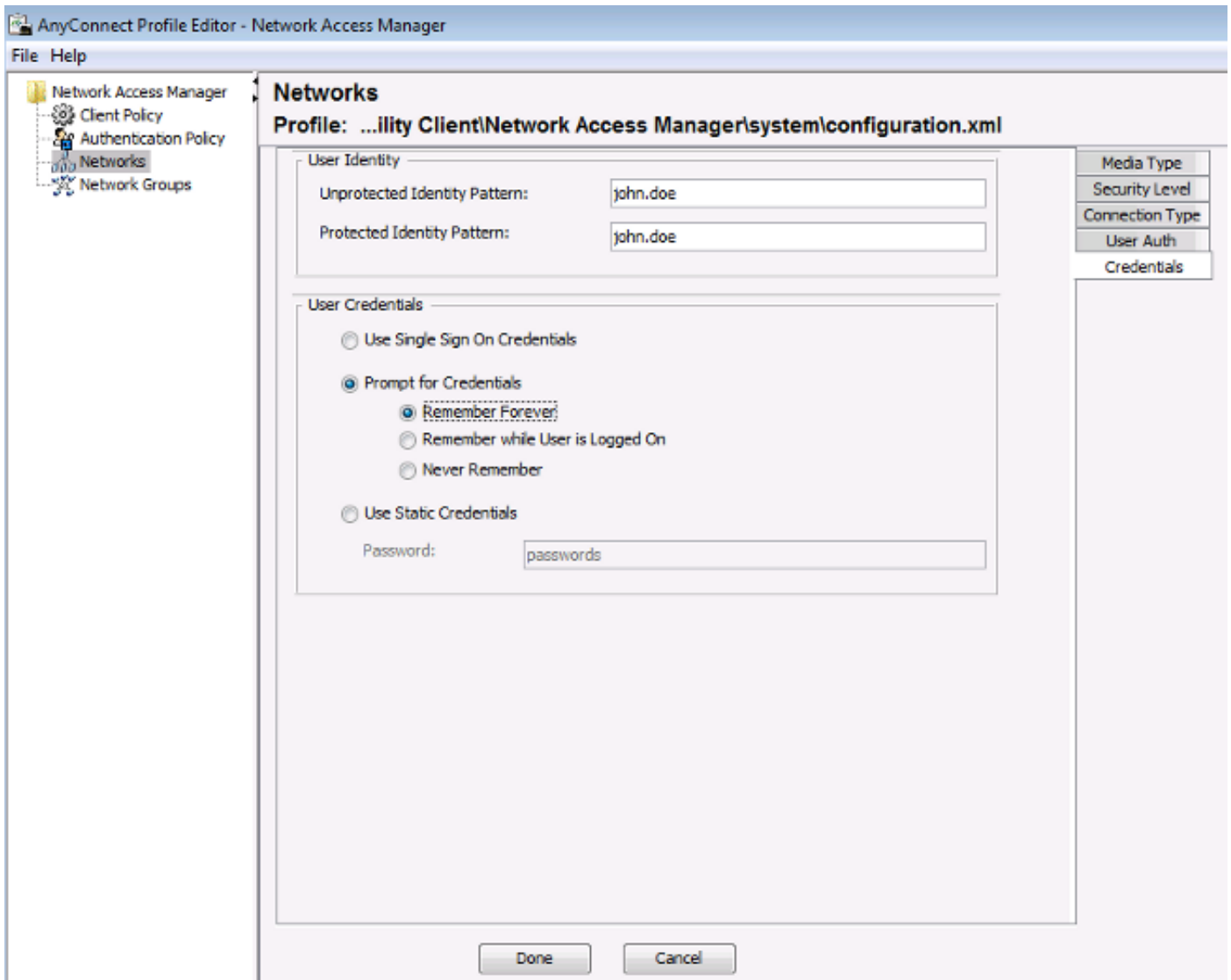
EAP-TLS, using a Certificate

Authenticate using a Token and EAP-GTC

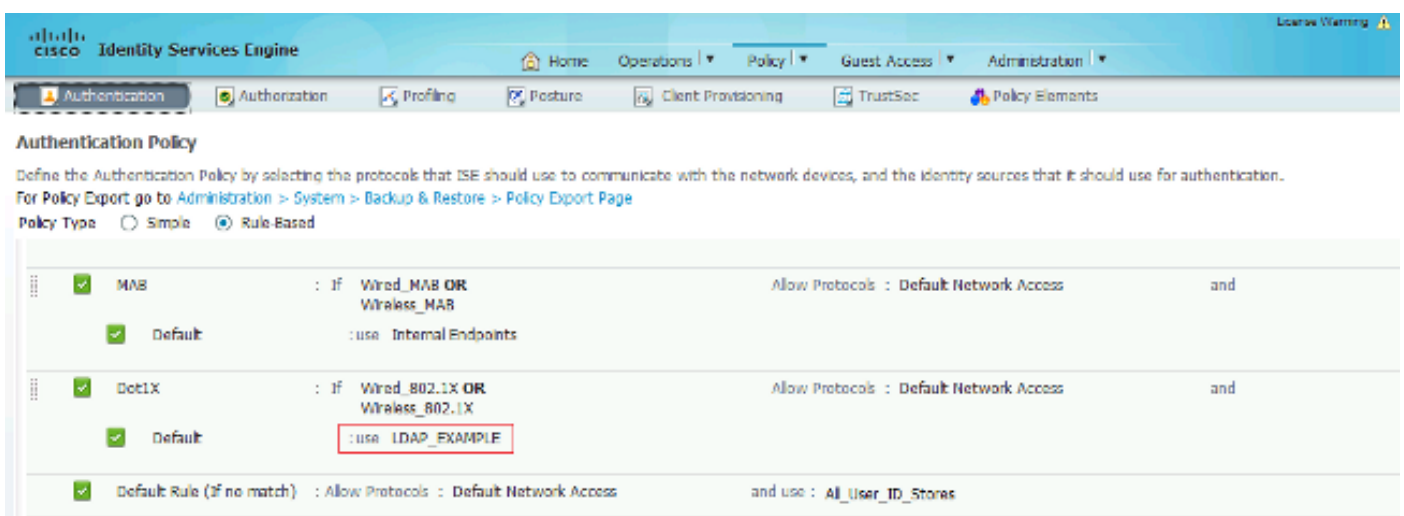
- Media Type
- Security Level
- Connection Type
- User Auth
- Credentials

Next

Cancel



使用这些映像中提供的信息更改ISE上的身份验证和授权策略：



CISCO Identity Services Engine License Warning

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

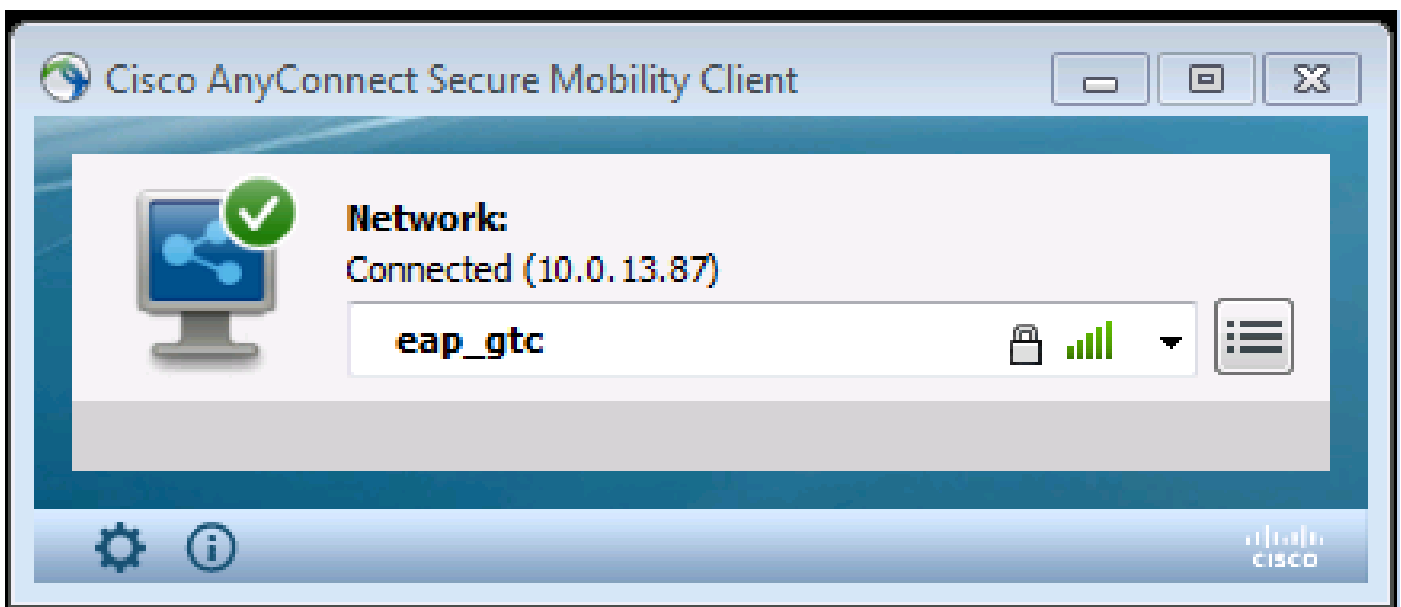
First Matched Rule Applies

Exceptions (0)

Standard

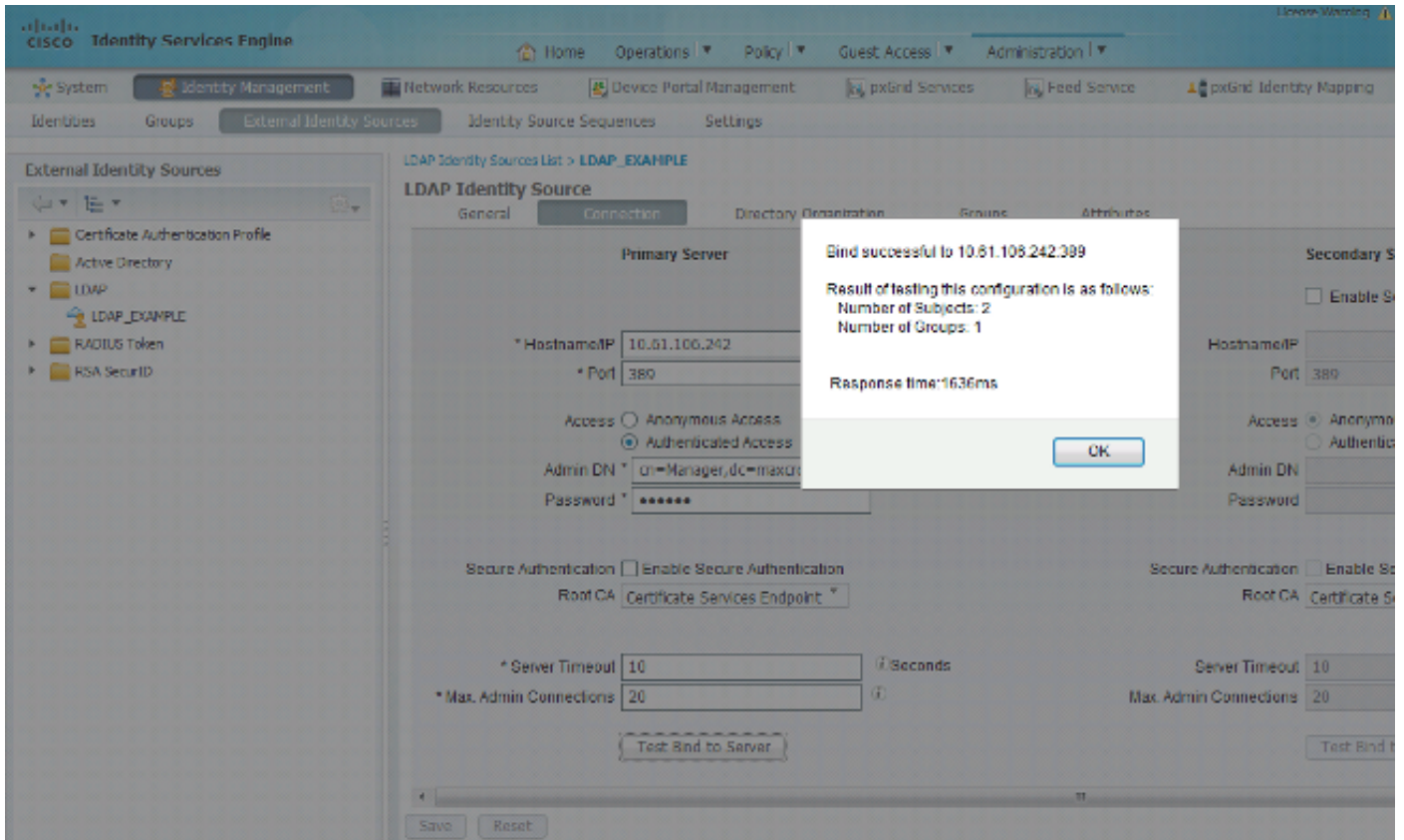
Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✔	Users in LDAP store	if (Wireless_802.1X AND LDAP_EXAMPLE:ExternalGroups EQUALS cn=domainusers,ou=groups,dc=mxarc,dc=com)	then PermitAccess
✔	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access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

应用配置后，您应该能够连接到网络：

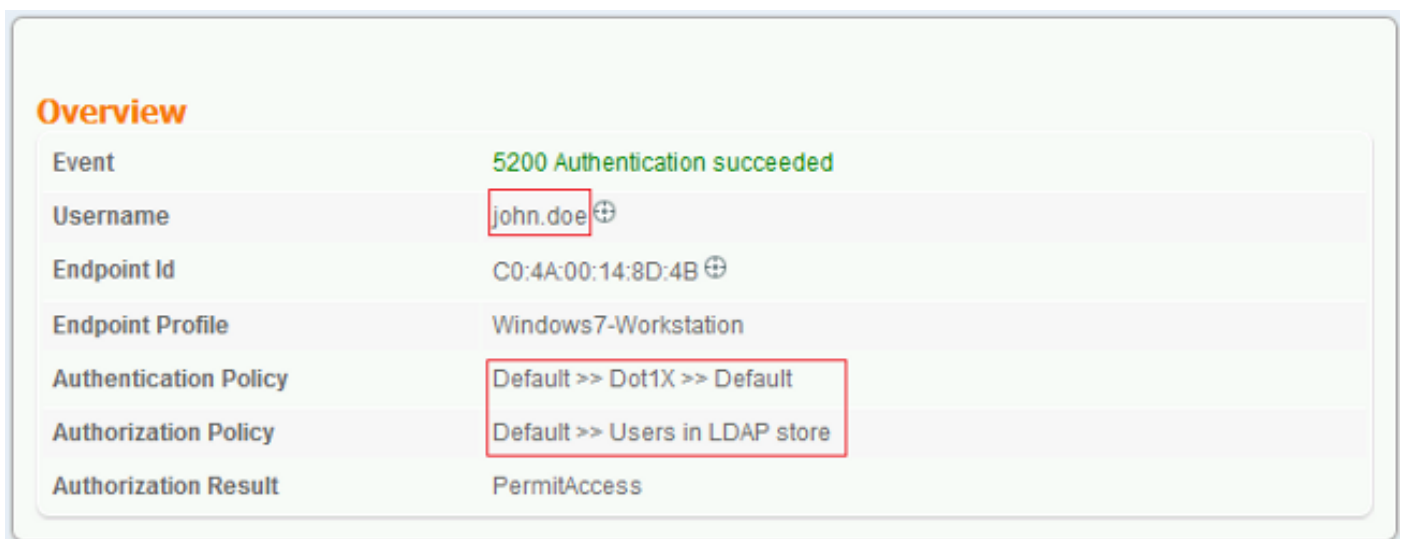
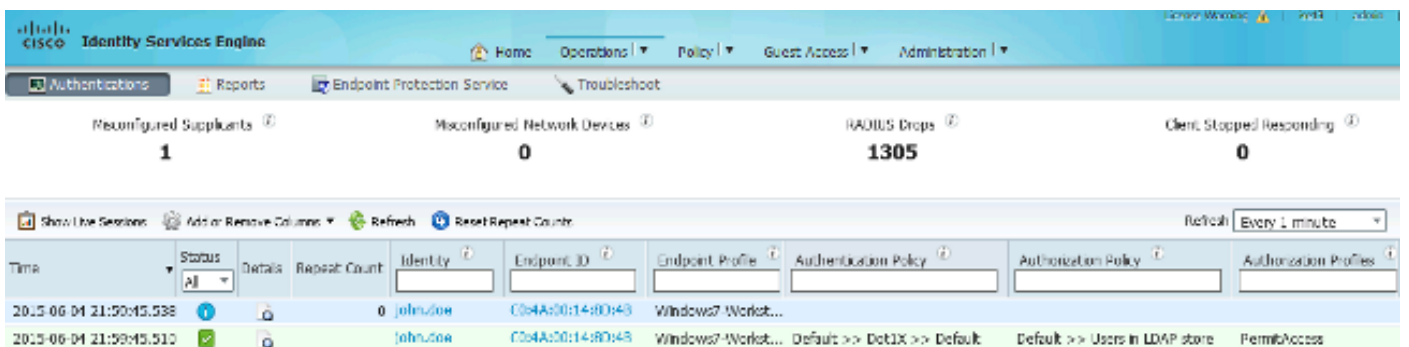


验证

要验证LDAP和ISE配置，请检索与服务器的测试连接的主题和组：



以下图像说明来自ISE的示例报告：



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

故障排除

本节介绍此配置遇到的一些常见错误以及如何排除这些错误：

- 安装OpenLDAP后，如果您遇到错误以指示gssapi.dll丢失，请重新启动Microsoft Windows。
- 可能无法直接编辑Cisco AnyConnect的configuration.xml文件。将新配置保存到其他位置，然后使用它替换旧文件。
- 在身份验证报告中，出现以下错误消息：

```
<#root>
```

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

此错误消息表明LDAP不支持您选择的方法。


确保同一报告中的身份验证协议显示其中一个受支持的方法（EAP-GTC、EAP-TLS或PEAP-TLS）。

- 在身份验证报告中，如果您注意到在身份存储中找不到主题，则报告中的用户名与LDAP数据库中任何用户的Subject Name Attribute不匹配。

在此方案中，此属性值设置为uid，这意味着ISE在尝试查找匹配项时查找LDAP用户的uid值。

- 如果在绑定到服务器测试期间未正确检索主题和组，则搜索库的配置不正确。

请记住，必须从枝叶到根和dc（可包含多个单词）指定LDAP层次结构。

 提示：要对WLC端的EAP身份验证进行故障排除，请参阅[使用WLAN控制器的EAP身份验证\(WLC\)配置示例](#)思科文档。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。