Configure the ISE for Integration with an LDAP Server

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Network Diagram
- Configure OpenLDAP
- Integrate OpenLDAP with the ISE
- Configure the WLC
- Configure EAP-GTC

Verify

Troubleshoot

Introduction

This document describes how to configure a Cisco Identity Services Engine (ISE) for integration with a Cisco LDAP server.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information this document is based on these software and hardware versions:

- Cisco ISE Version 1.3 with patch 2
- Microsoft Windows Version 7 x64 with OpenLDAP installed
- Cisco Wireless LAN Controller (WLC) Version 8.0.100.0
- Cisco AnyConnect Version 3.1 for Microsoft Windows
- Cisco Network Access Manager Profile Editor

Note: This document is valid for setups that use LDAP as the external identity source for the ISE

authentication and authorization.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

These authentication methods are supported with LDAP:

- 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)

Configure

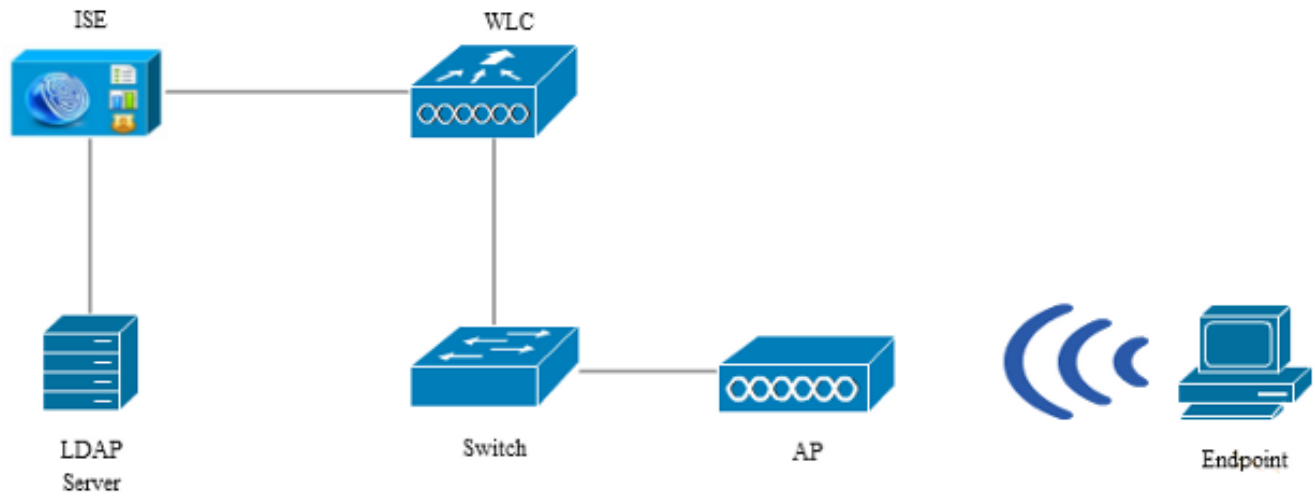
This section describes how to configure the network devices and integrate the ISE with an LDAP server.

Network Diagram

In this configuration example, the endpoint uses a wireless adapter in order to associate with the wireless network.

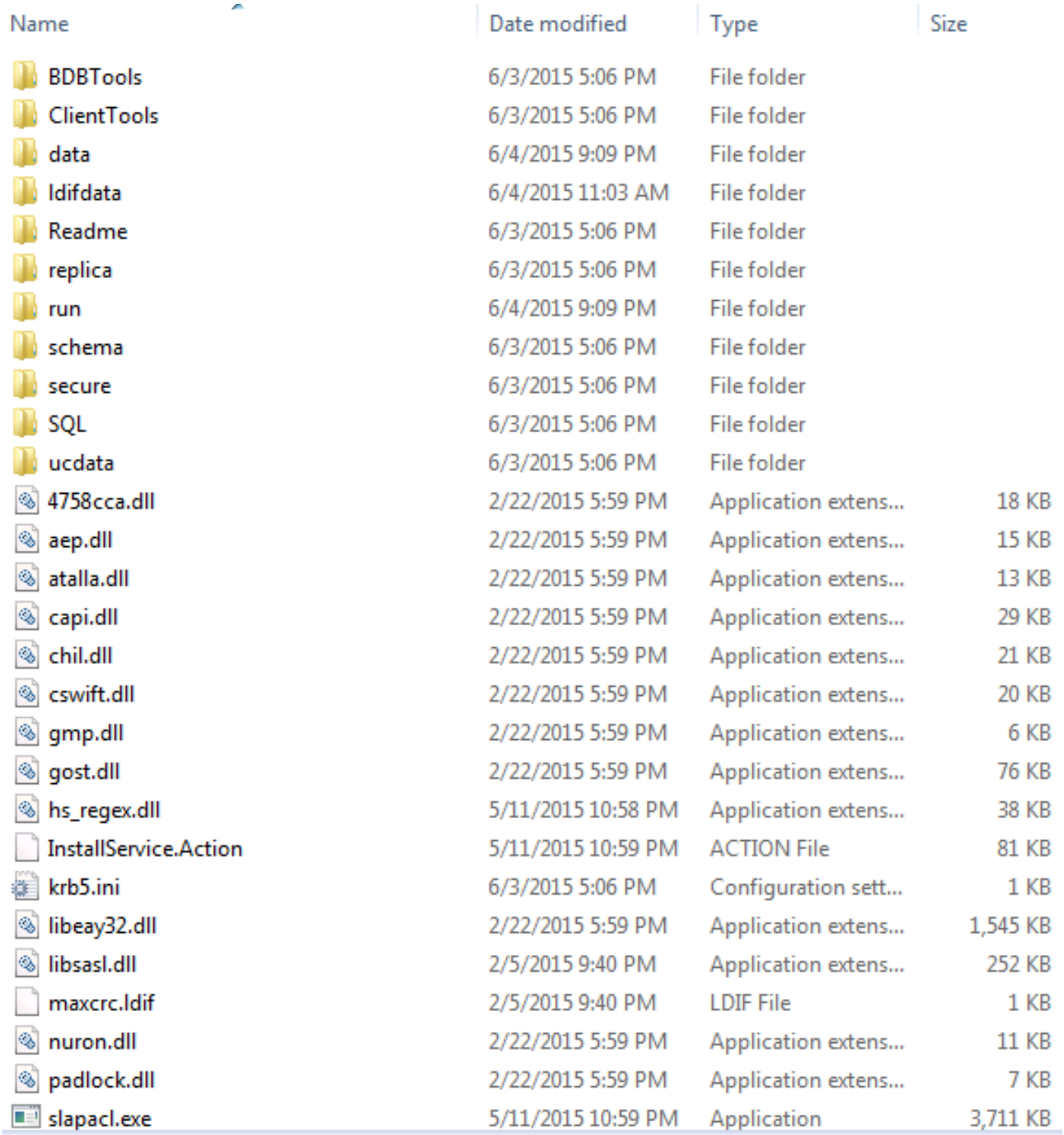
The Wireless LAN (WLAN) on the WLC is configured in order to authenticate the users via the ISE. On the ISE, LDAP is configured as an external identity store.

This image illustrates the network topology that is used:



Configure OpenLDAP

Installation of the OpenLDAP for Microsoft Windows is completed via the GUI, and it is straightforward. The default location is **C: > OpenLDAP**. After installation, you then see this directory:

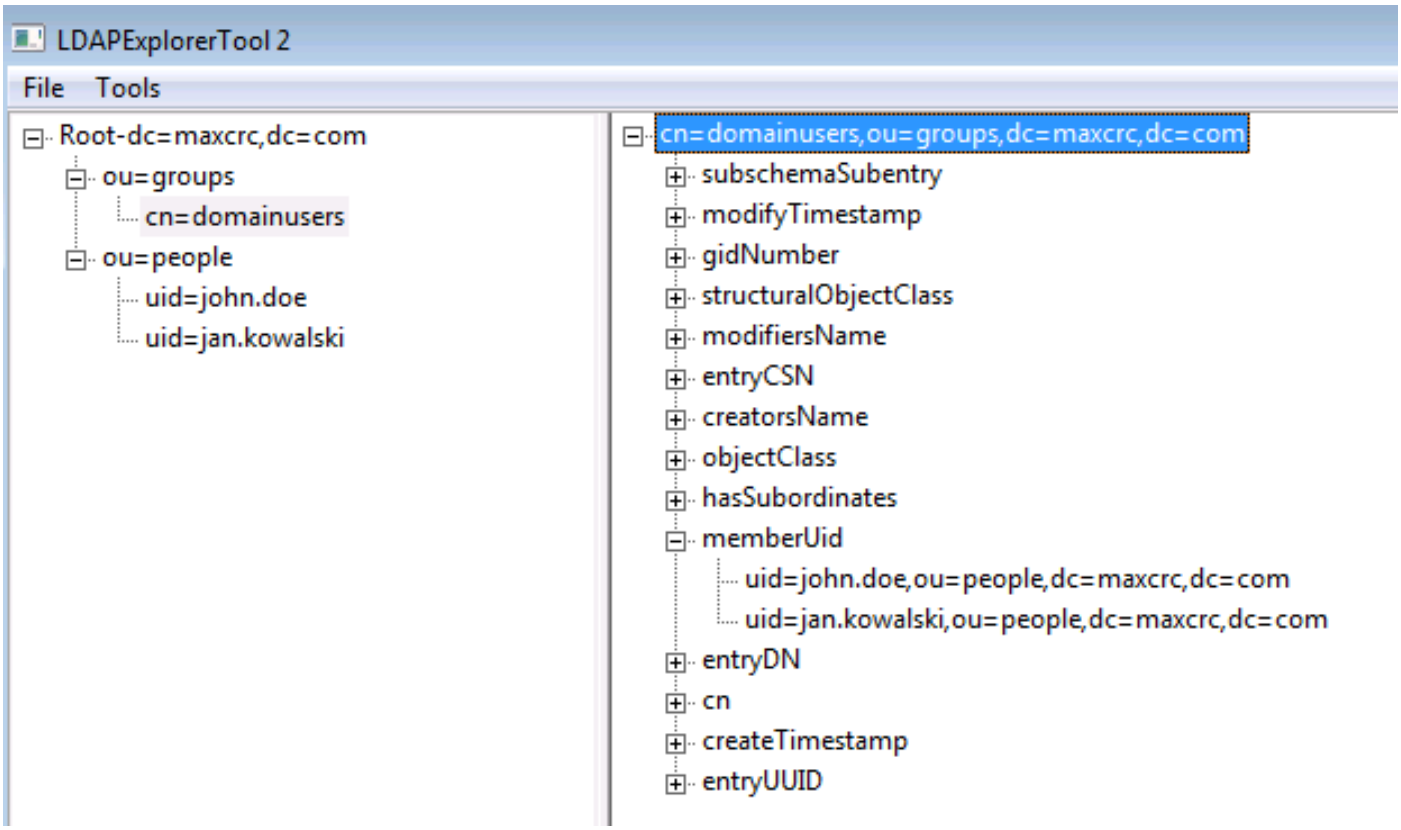


Name	Date modified	Type	Size
BDBTools	6/3/2015 5:06 PM	File folder	
ClientTools	6/3/2015 5:06 PM	File folder	
data	6/4/2015 9:09 PM	File folder	
ldifdata	6/4/2015 11:03 AM	File folder	
Readme	6/3/2015 5:06 PM	File folder	
replica	6/3/2015 5:06 PM	File folder	
run	6/4/2015 9:09 PM	File folder	
schema	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

Take note of two directories in particular:

- **ClientTools** – This directory includes a set of binaries that are used in order to edit the LDAP database.
- **ldifdata** – This is the location in which you must store the files with LDAP objects.

Add this structure to the LDAP database:



Under the *Root* directory, you must configure two Organizational Units (OUs). The *OU=groups* OU must have one child group (**cn=domainusers** in this example).

The *OU=people* OU defines the two user accounts that belong to the *cn=domainusers* group.

In order to populate the database, you must create the *ldif* file first. The previously mentioned structure was created from this file:

```
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
```

In order to add the objects to the LDAP database, use the **ldapmodify** binary:

```
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"

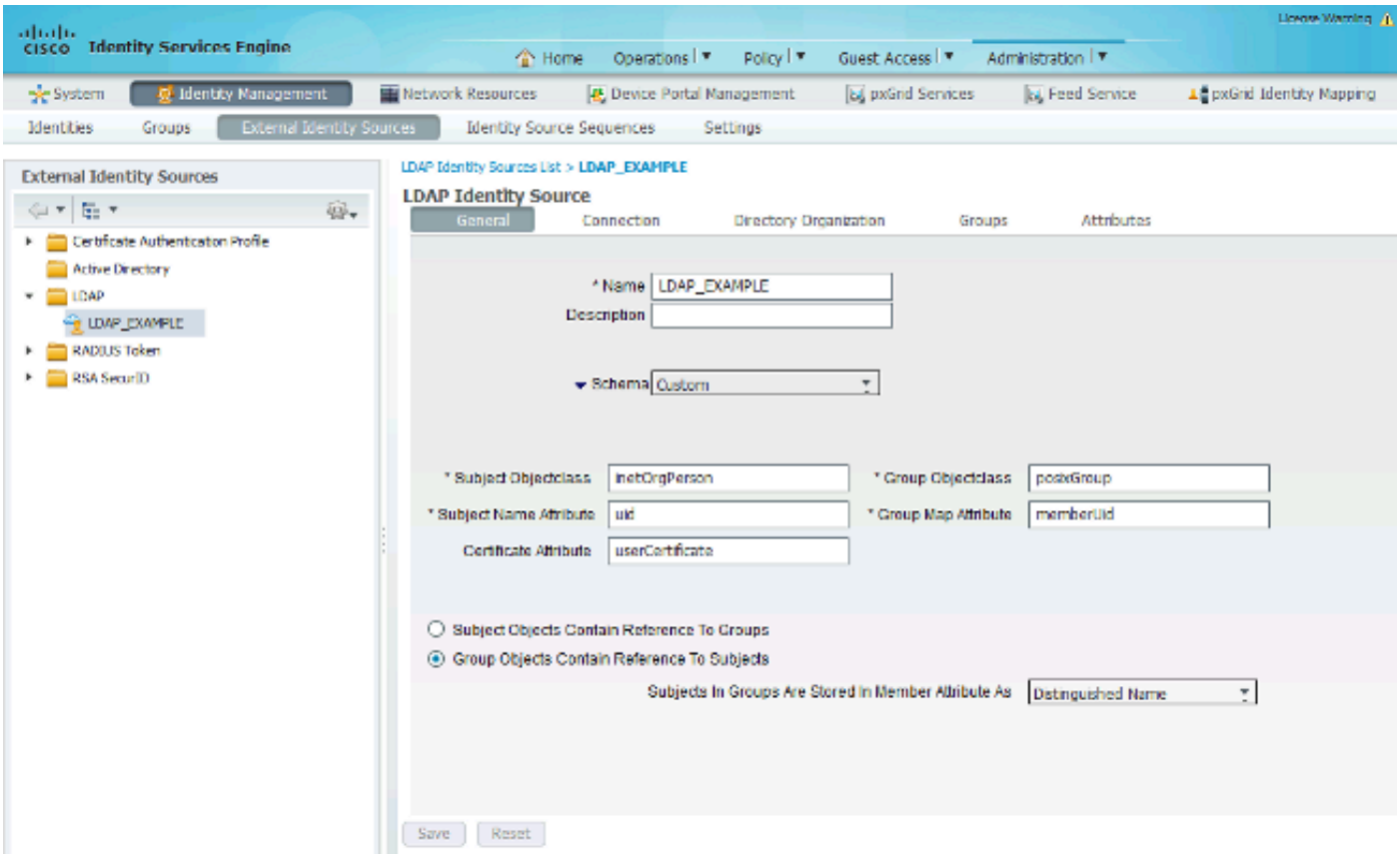
adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

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

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

Integrate OpenLDAP with the ISE

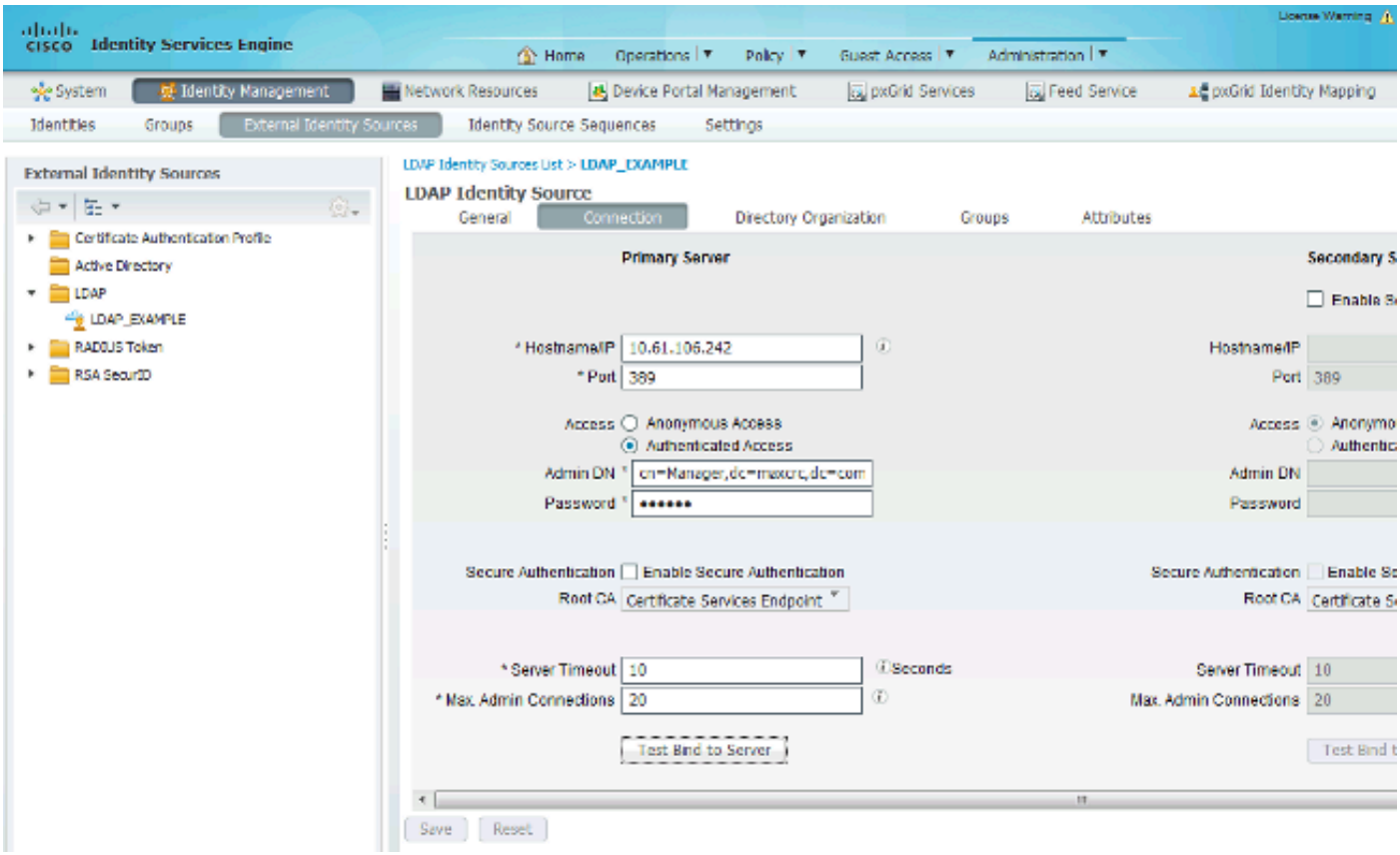
Use the information that is provided in the images throughout this section in order to configure LDAP as an external identity store on the ISE.



You can configure these attributes from the *General* tab:

- **Subject Objectclass** – This field corresponds to the object class of the user accounts in the *ldif* file. As per the LDAP configuration. use one of these four classes:
    - Top
    - Person
    - OrganizationalPerson
    - InetOrgPerson
- **Subject Name Attribute** – This is the attribute that is retrieved by the LDAP when the ISE inquires whether a specific user name is included in a database. In this scenario, you must use **john.doe** or **jan.kowalski** as the user name on the endpoint.
- **Group Objectclass** – This field corresponds to the object class for a group in the *ldif* file. In this scenario, the object class for the *cn=domainusers* group is **posixGroup**.
- **Group Map Attribute** – This attribute defines how the users are mapped to the groups. Under the *cn=domainusers* group in the *ldif* file, you can see two *memberUid* attributes that correspond to the users.

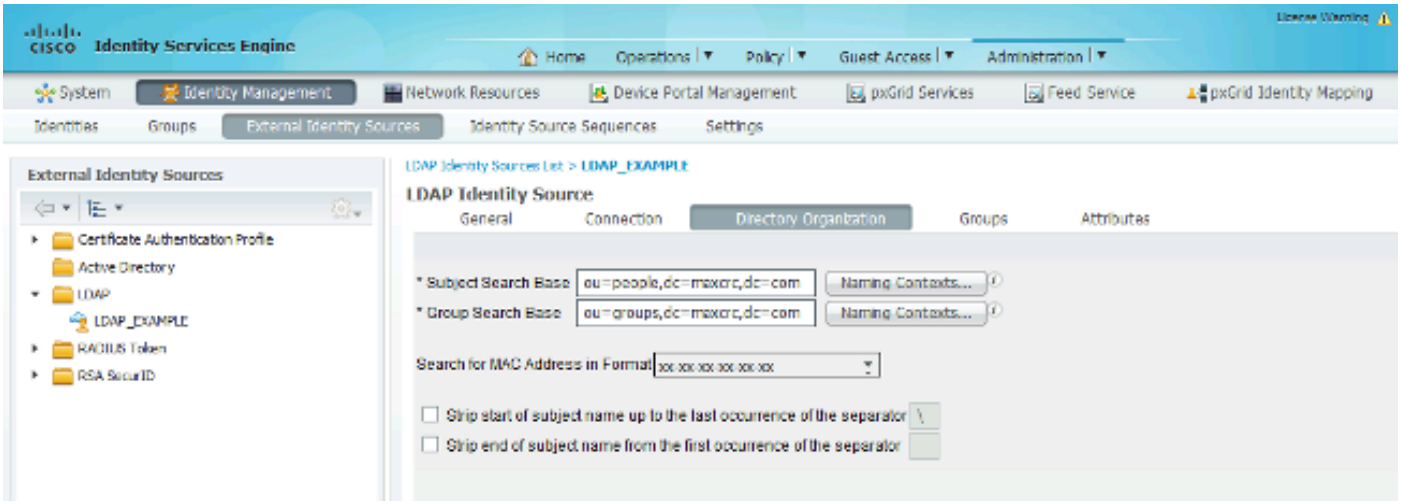
The ISE also offers some pre-configured schemas (Microsoft Active Directory, Sun, Novell):



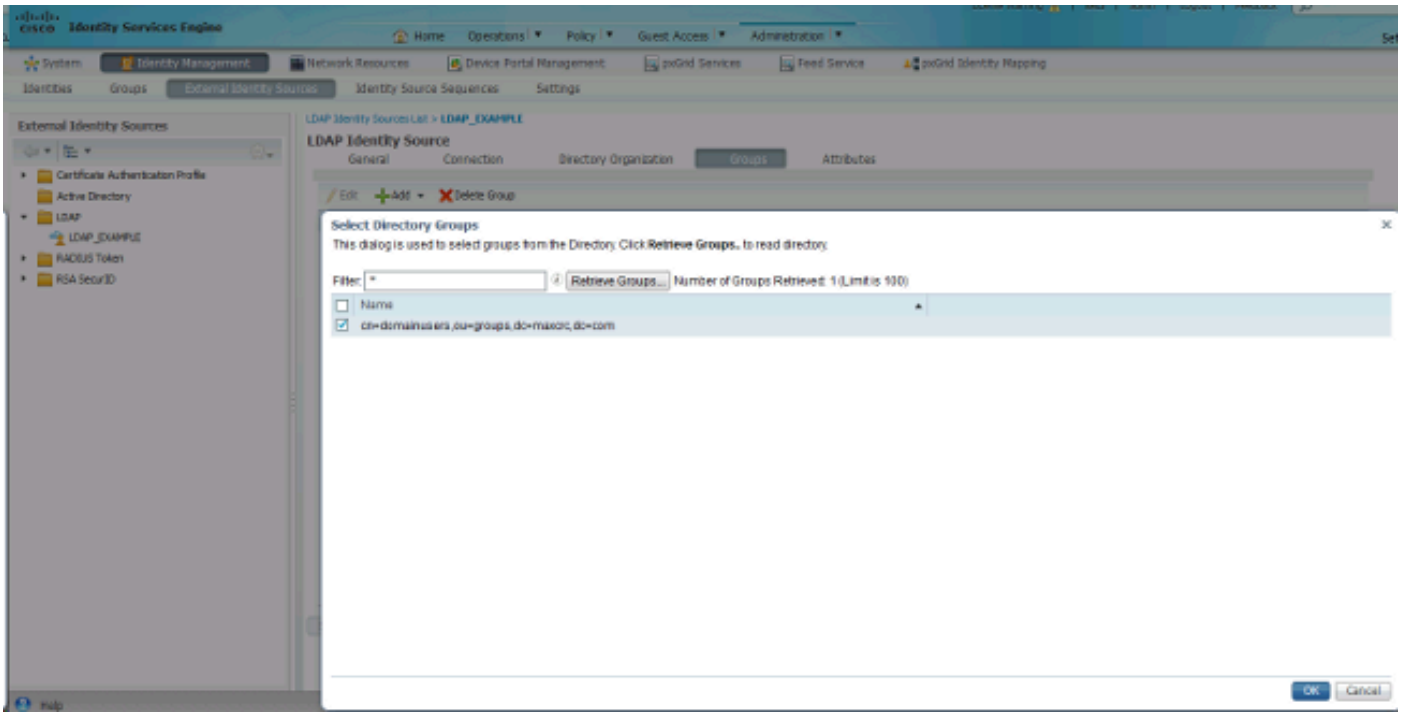
After you set the correct IP address and administrative domain name, you can *Test Bind* to the server. At this point, you do not retrieve any subjects or groups because the search bases are not yet configured.

In the next tab, configure the Subject/Group Search Base. This is the *join* point for the ISE to the LDAP. You are able to retrieve only subjects and groups that are children of your joining point.

In this scenario, the subjects from the *OU=people* and the groups from the *OU=groups* are retrieved:

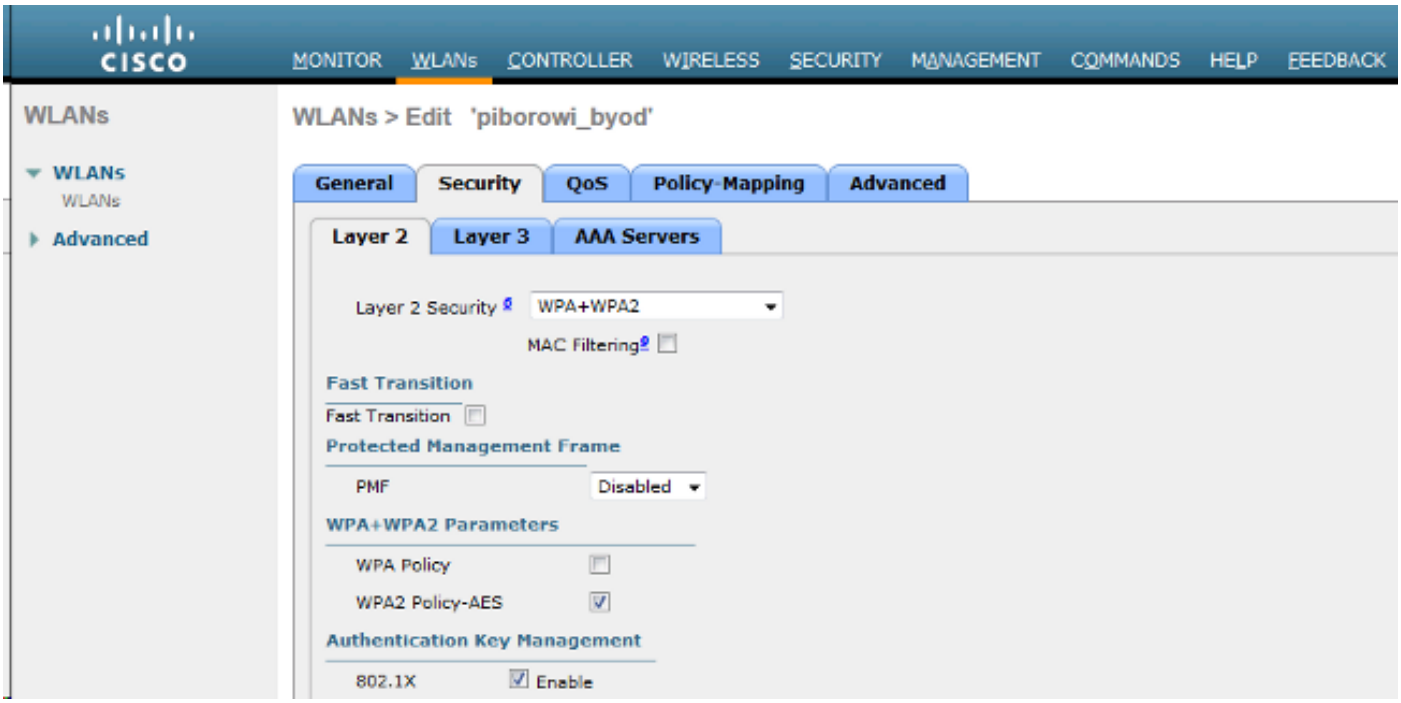


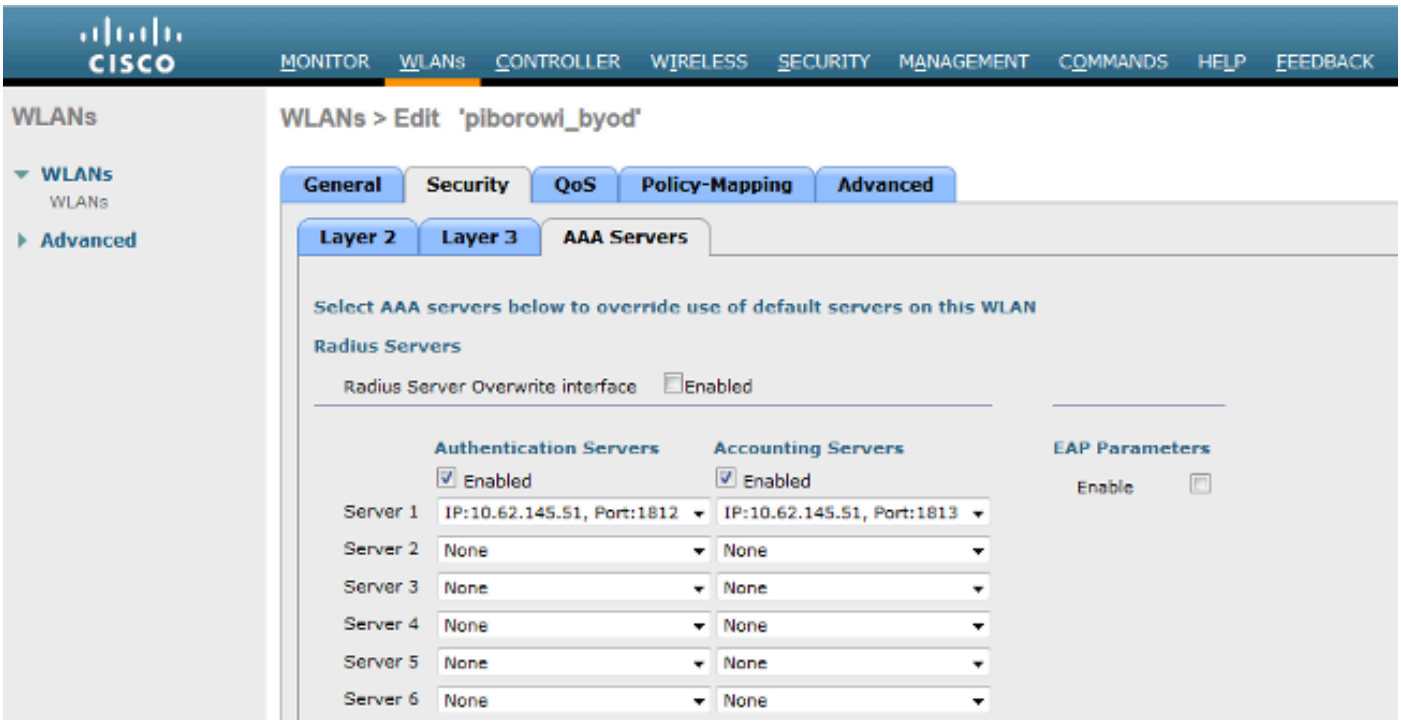
From the *Groups* tab, you can import the groups from the LDAP on the ISE:

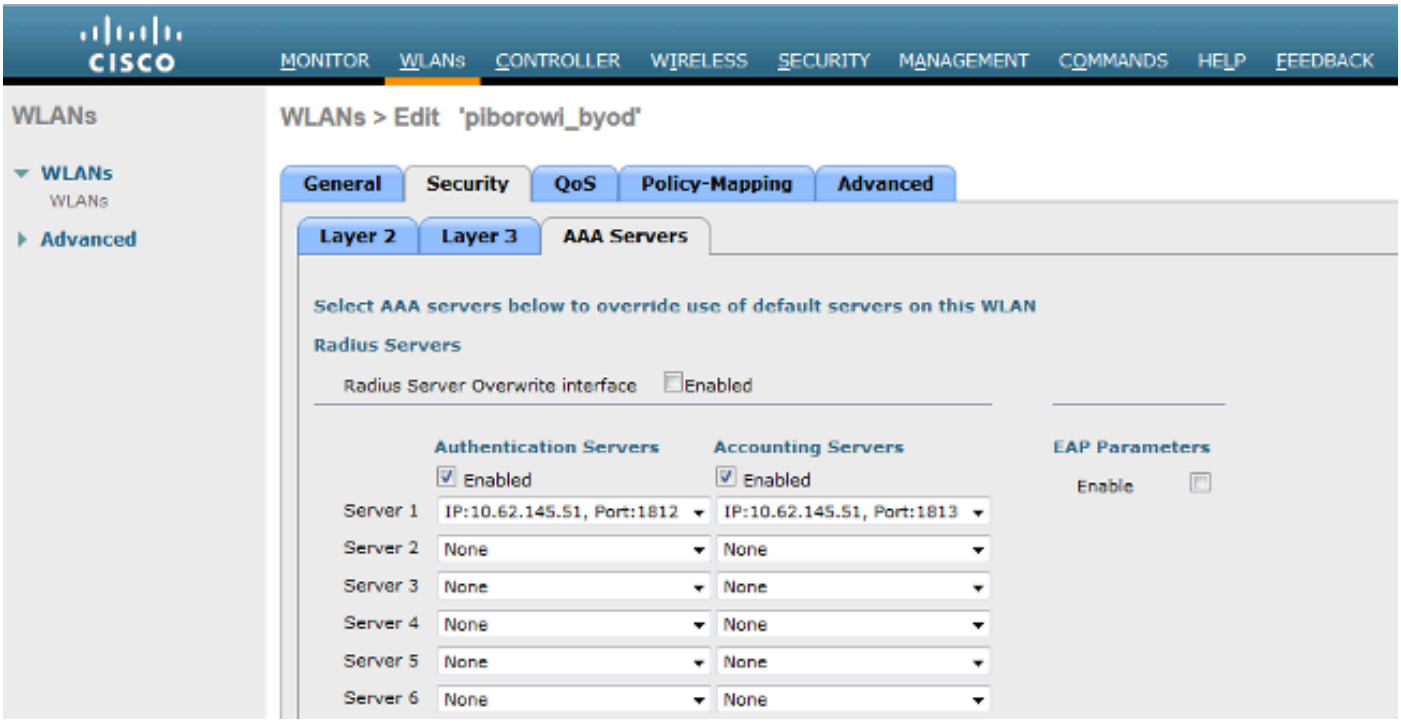


Configure the WLC

Use the information that is provided in these images in order to configure the WLC for 802.1x authentication:







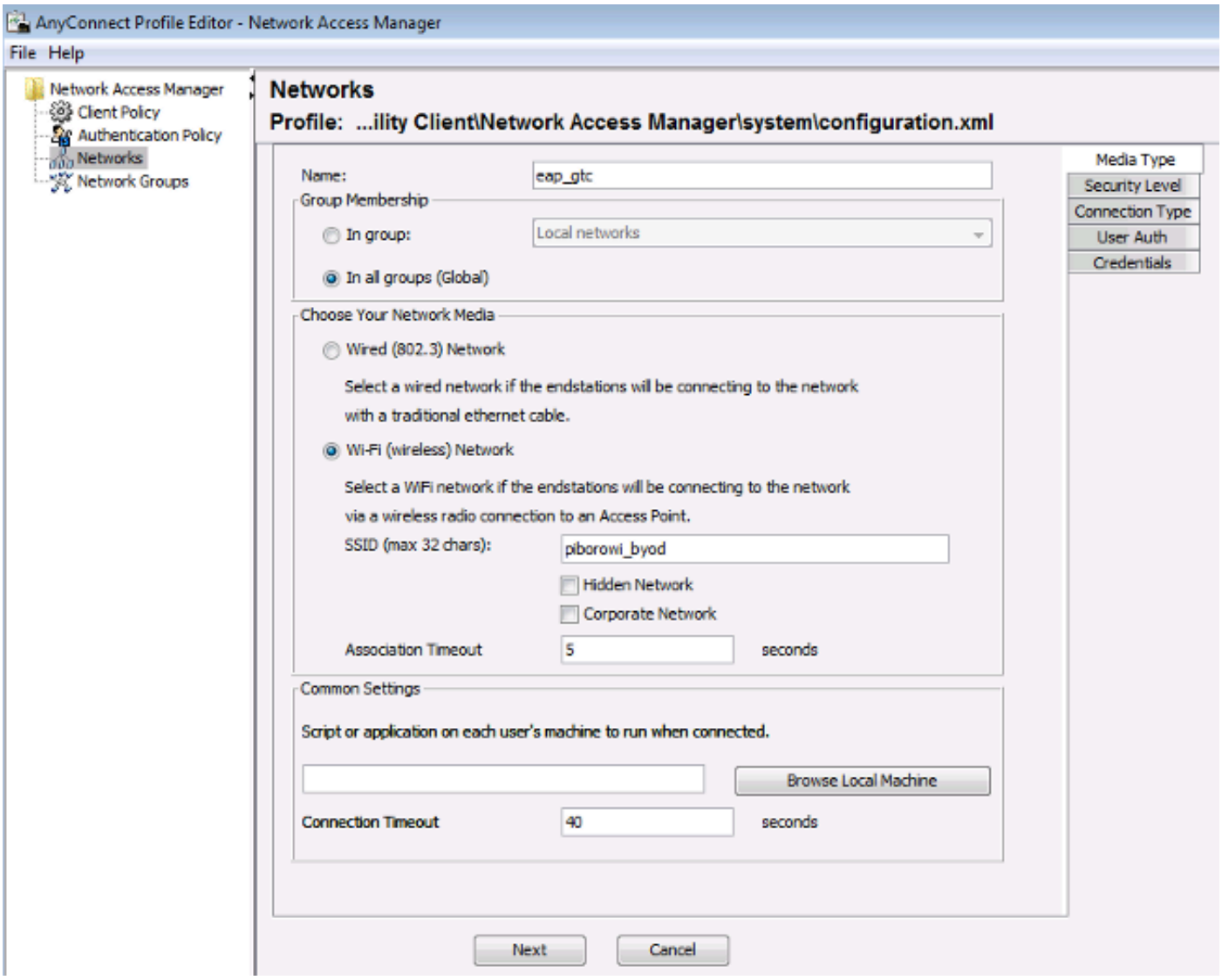
Configure EAP-GTC

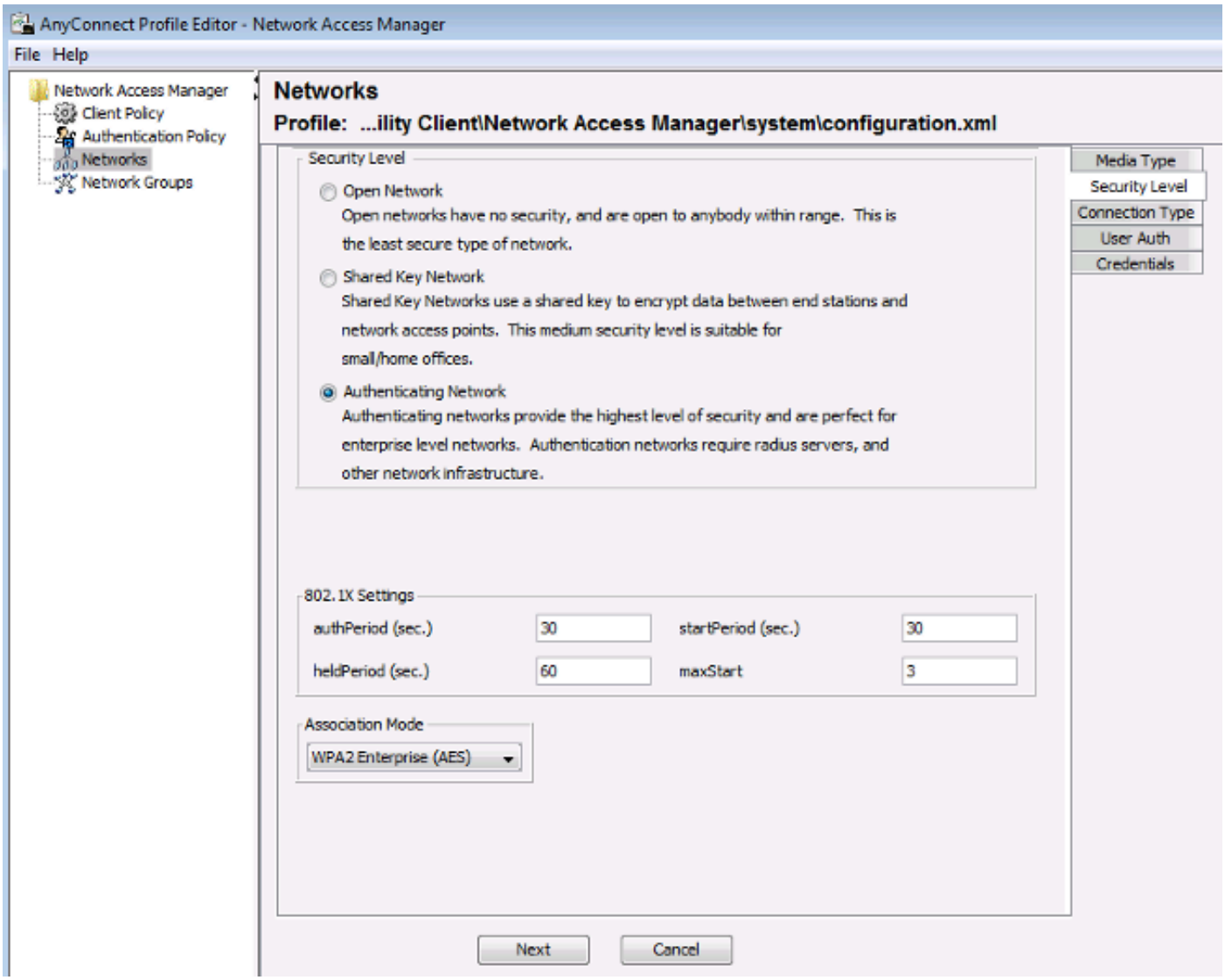
One of the supported authentication methods for LDAP is EAP-GTC. It is available in Cisco AnyConnect, but you must install the Network Access Manager Profile Editor in order to configure the profile correctly.

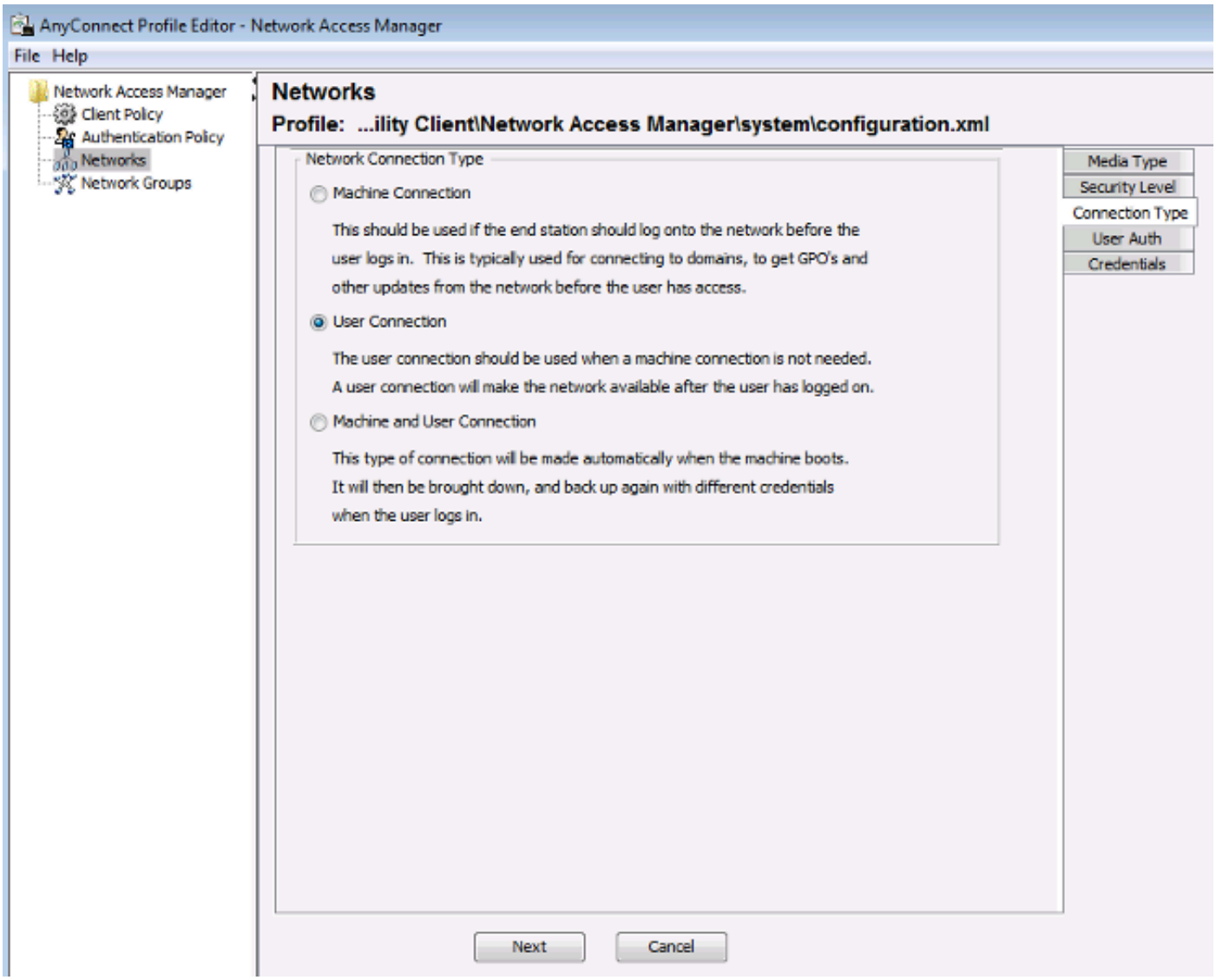
You must also edit the Network Access Manager configuration, which (by default) is located here:

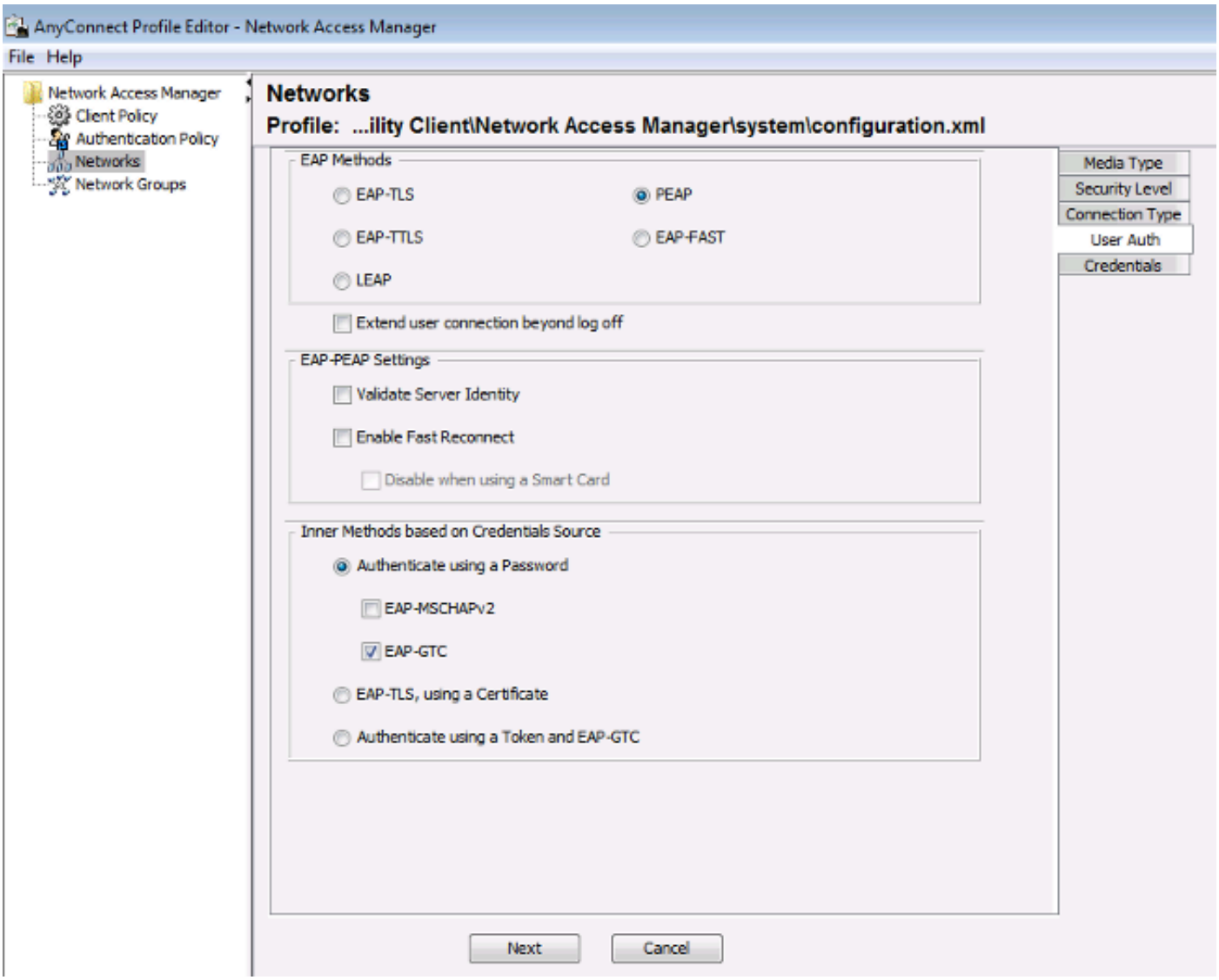
C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > system > configuration.xml file

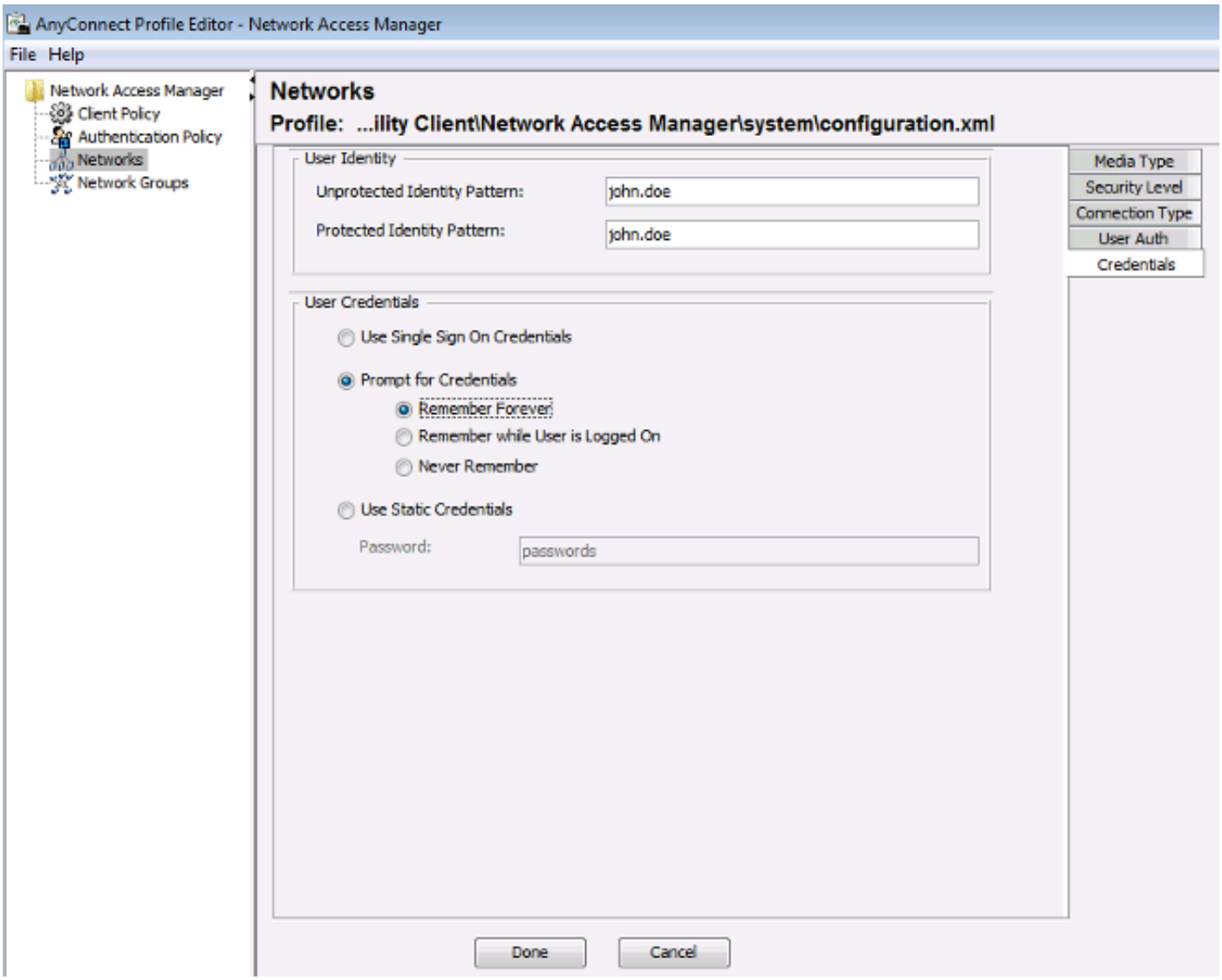
Use the information that is provided in these images in order to configure the EAP-GTC on the endpoint:


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

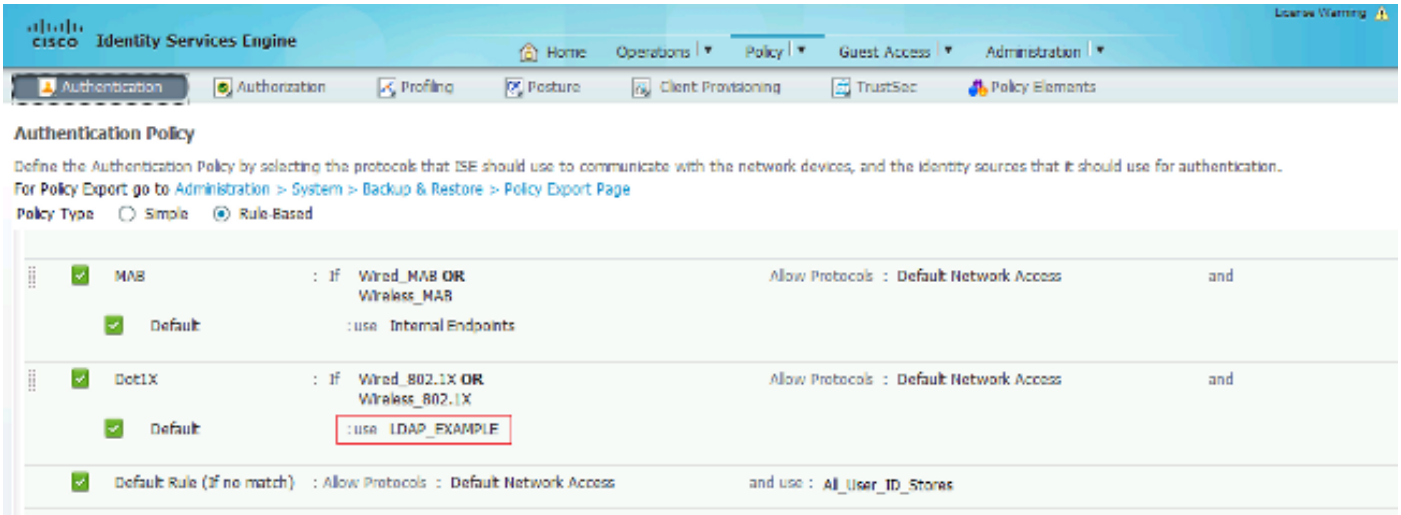

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Security Level
Open Network
Open networks have no security, and are open to 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.
Media Type
Security Level
Connection Type
User Auth
Credentials
802.1X Settings
authPeriod (sec.)
30
startPeriod (sec.)
30
heldPeriod (sec.)
60
maxStart
3
Association Mode
WPA2 Enterprise (AES)
Next
Cancel

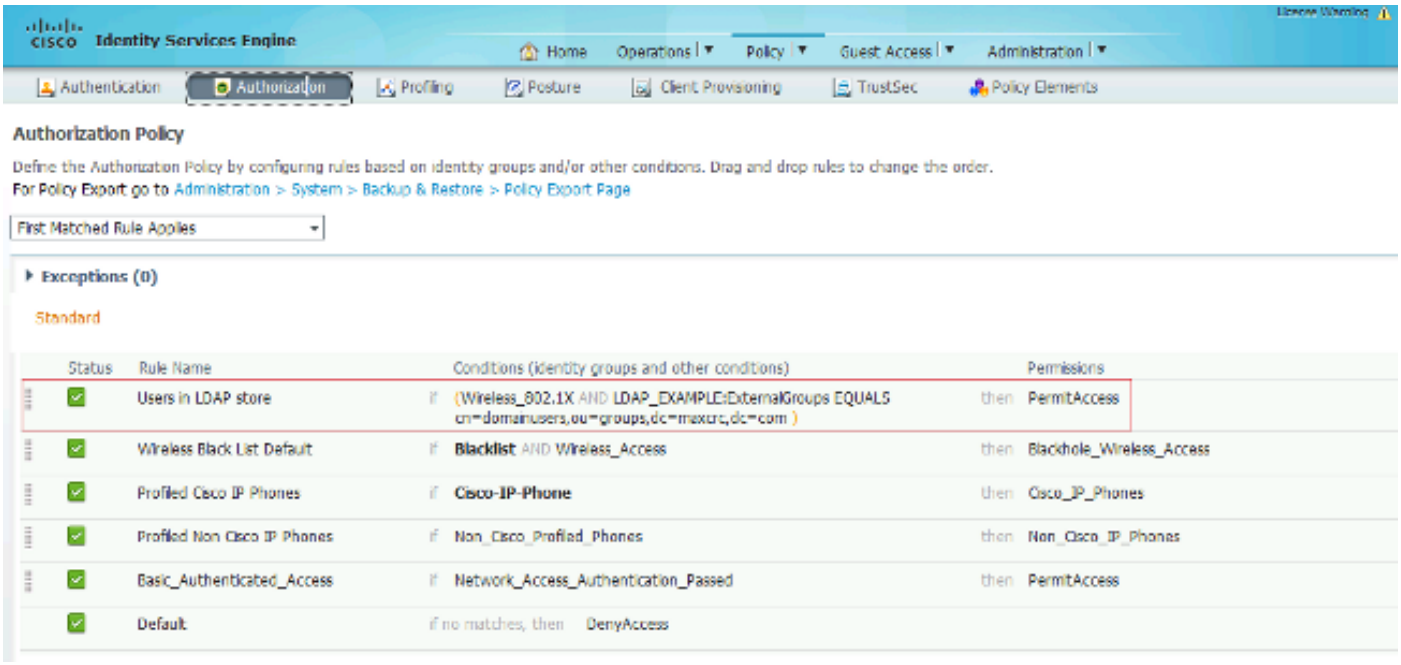

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Network Connection Type
Machine Connection
This should be used if the end station 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

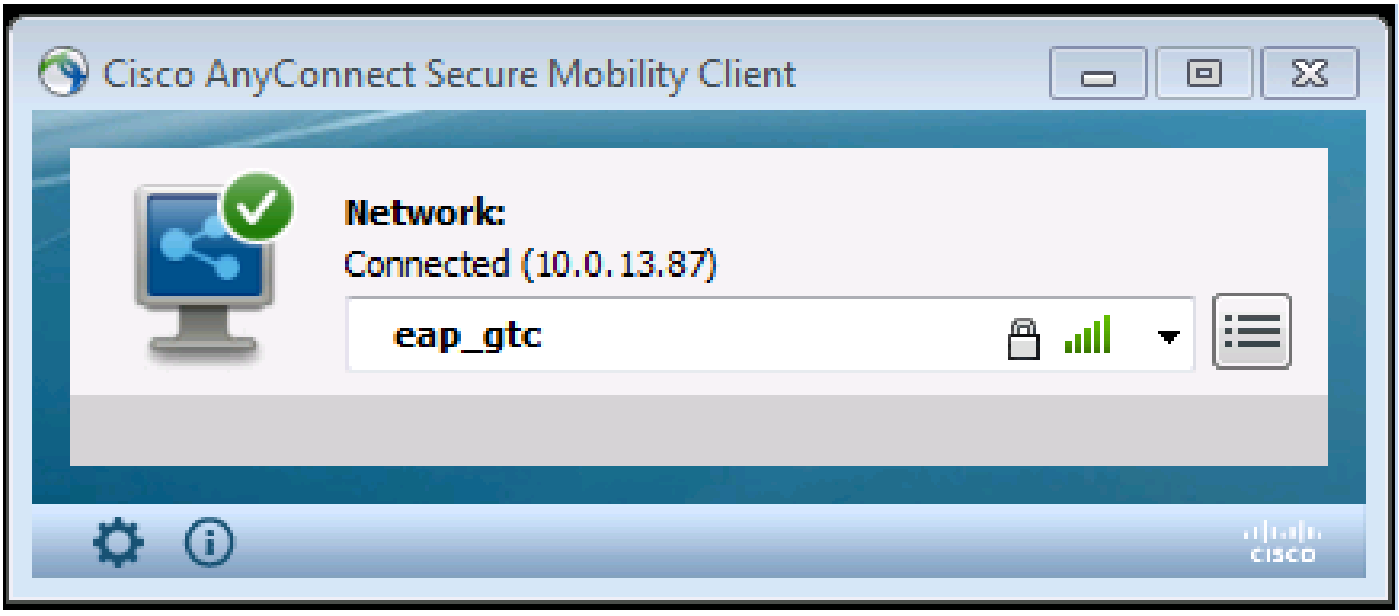


Use the information that is provided in these images in order to change the authentication and authorization policies on the ISE:



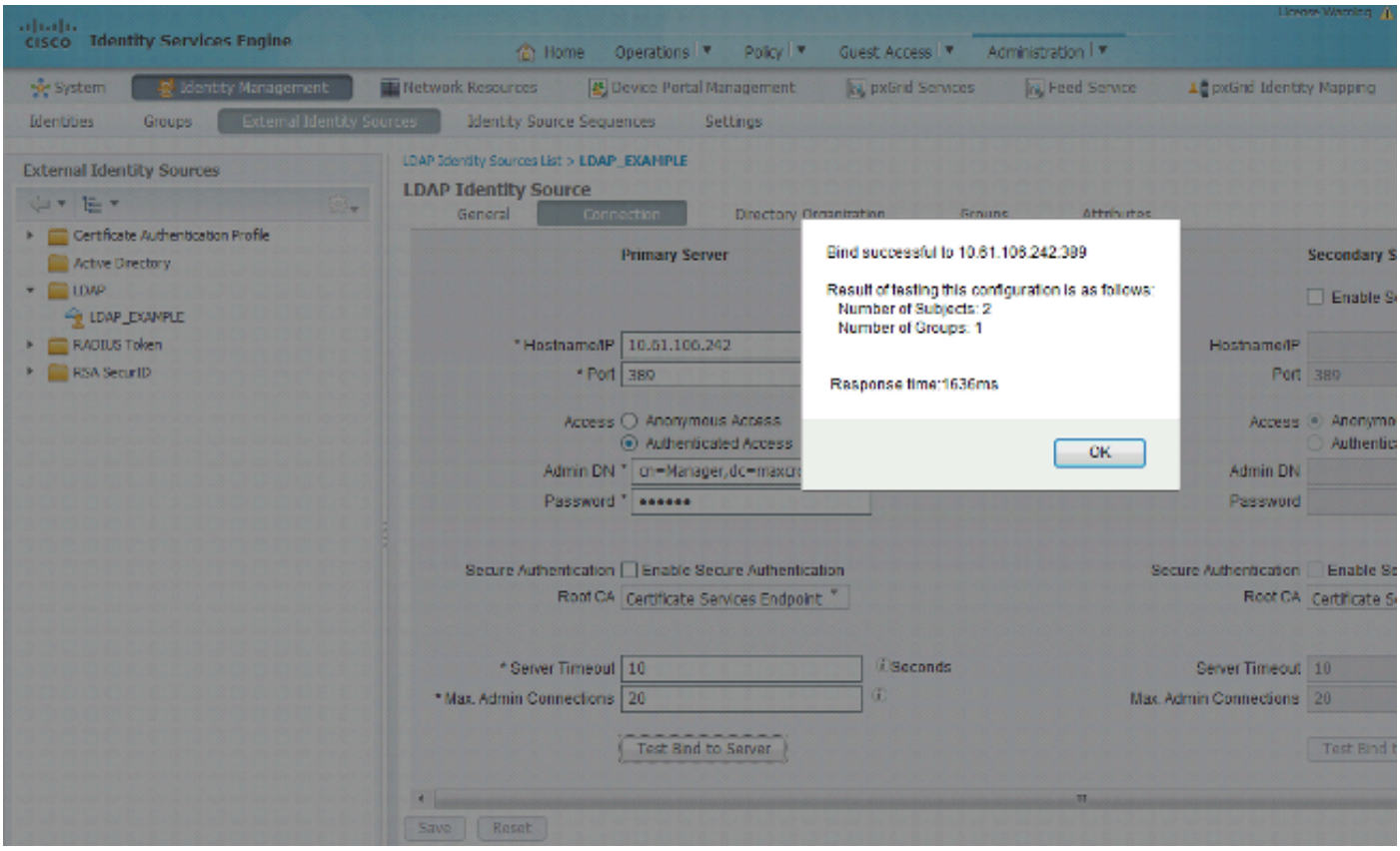


After you apply the configuration, you are able to connect to the network:

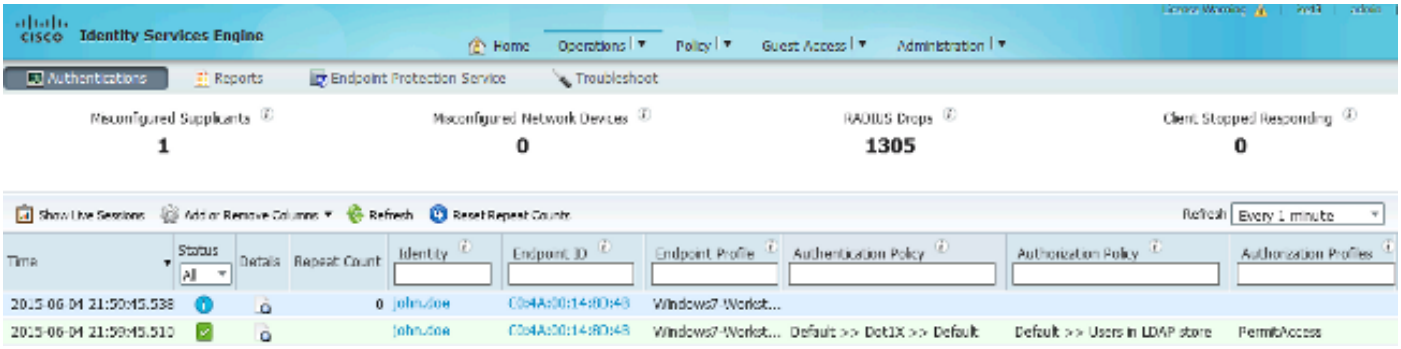


Verify

In order to verify the LDAP and ISE configurations, retrieve the subjects and groups with a test connection to the server:



These images illustrate a sample report from the 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

Troubleshoot

This section describes some common errors that are encountered with this configuration and how to troubleshoot them:

- After installation of the OpenLDAP, if you encounter an error to indicate that a **gssapi.dll** is missing, restart Microsoft Windows.
- It might not be possible to edit the *configuration.xml* file for Cisco AnyConnect directly. Save your new configuration in another location and then use it to replace the old file.
- In the authentication report, there is this error message:

  <#root>

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

  This error message indicates that the method you picked is not supported by LDAP.

Ensure that the *Authentication Protocol* in the same report shows one of the supported methods (EAP-GTC, EAP-TLS, or PEAP-TLS).

- In the authentication report, if you notice that the subject was not found in the identity store, the user name from the report does not match the *Subject Name Attribute* for any user in the LDAP database.

In this scenario, the value was set to **uid** for this attribute, which means that the ISE looks to the *uid* values for the LDAP user when it attempts to find a match.

- If the subjects and groups are not retrieved correctly during a *bind to server* test, it is an incorrect configuration for the search bases.

Remember that the LDAP hierarchy must be specified from the leaf-to-root and *dc* (can consist of multiple words).

Tip: In order to troubleshoot EAP authentication on the WLC side, refer to the EAP Authentication with WLAN Controllers (WLC) Configuration Example Cisco document.
