Configurazione di ISE per l'integrazione con un server LDAP

Sommario

Introduzione

In questo documento viene descritto come configurare un Cisco Identity Services Engine (ISE) per l'integrazione con un server LDAP Cisco.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE versione 1.3 con patch 2
- Microsoft Windows versione 7 x64 con OpenLDAP installato
- Cisco Wireless LAN Controller (WLC) versione 8.0.100.0
- Cisco AnyConnect versione 3.1 per Microsoft Windows

- Editor profili di Cisco Network Access Manager

Nota: questo documento è valido per le configurazioni che usano LDAP come origine dell'identità esterna per l'autenticazione e l'autorizzazione ISE.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questi metodi di autenticazione sono supportati con LDAP:

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

Configurazione

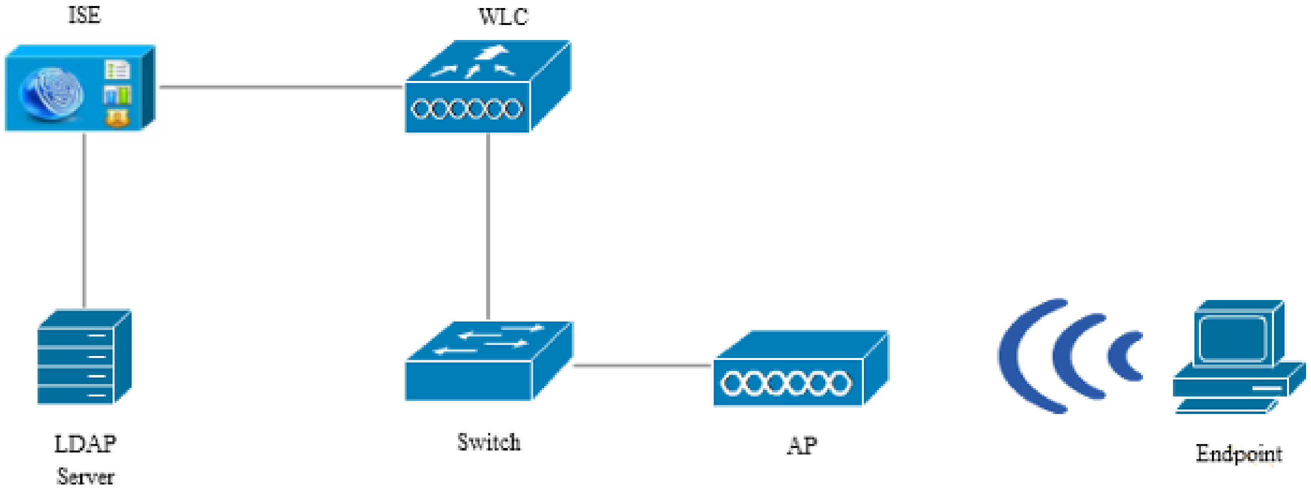
Questa sezione descrive come configurare i dispositivi di rete e integrare ISE con un server LDAP.

Esempio di rete

In questo esempio di configurazione, l'endpoint utilizza una scheda wireless per l'associazione alla rete wireless.

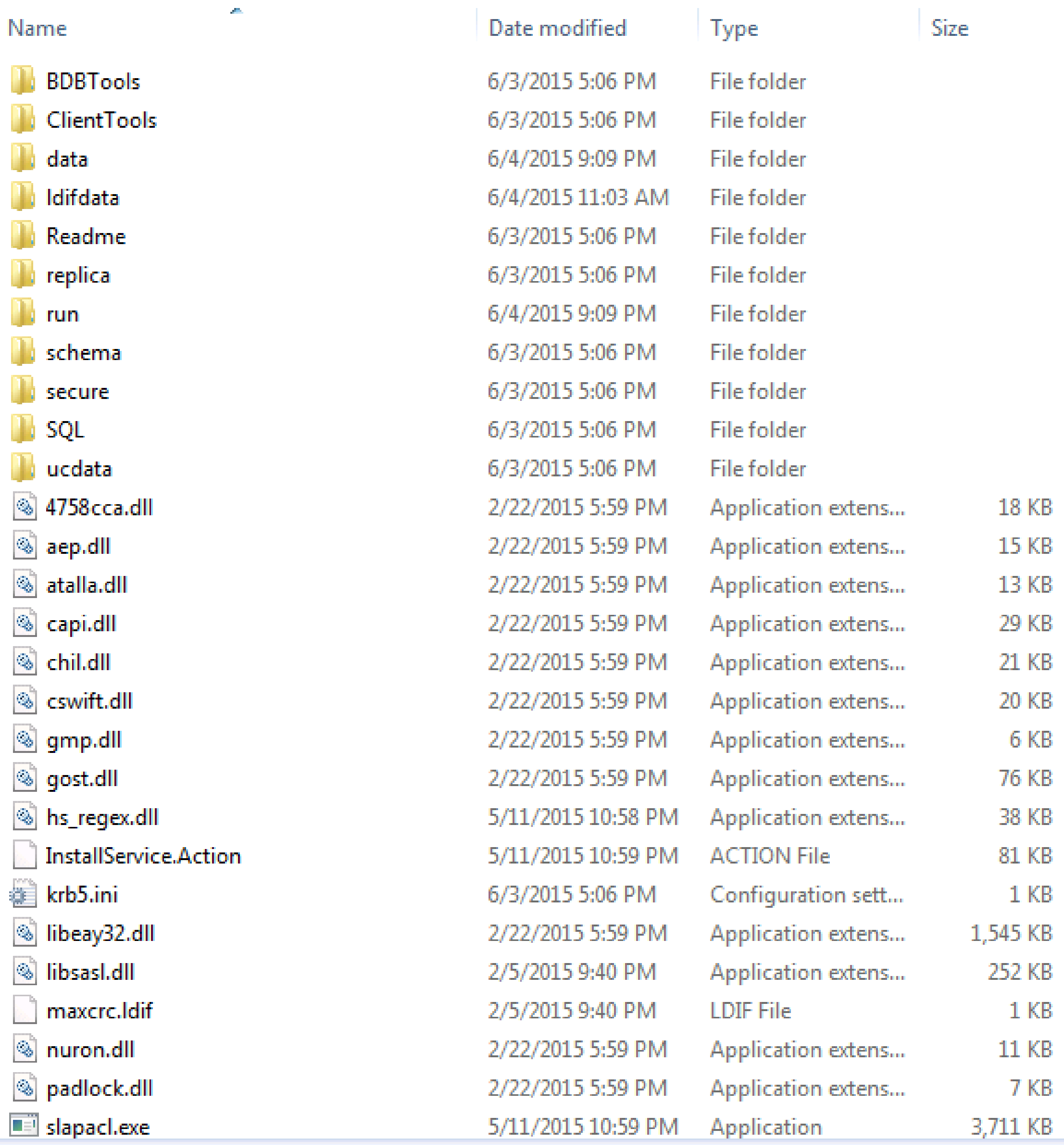
La LAN wireless (WLAN) sul WLC è configurata in modo da autenticare gli utenti tramite l'ISE. Nell'ISE, LDAP è configurato come un archivio identità esterno.

Nell'immagine è illustrata la topologia di rete utilizzata:



Configura OpenLDAP

L'installazione di OpenLDAP per Microsoft Windows viene completata tramite la GUI ed è semplice. La posizione predefinita è C: > OpenLDAP. Dopo l'installazione, dovrebbe essere visualizzata la seguente directory:



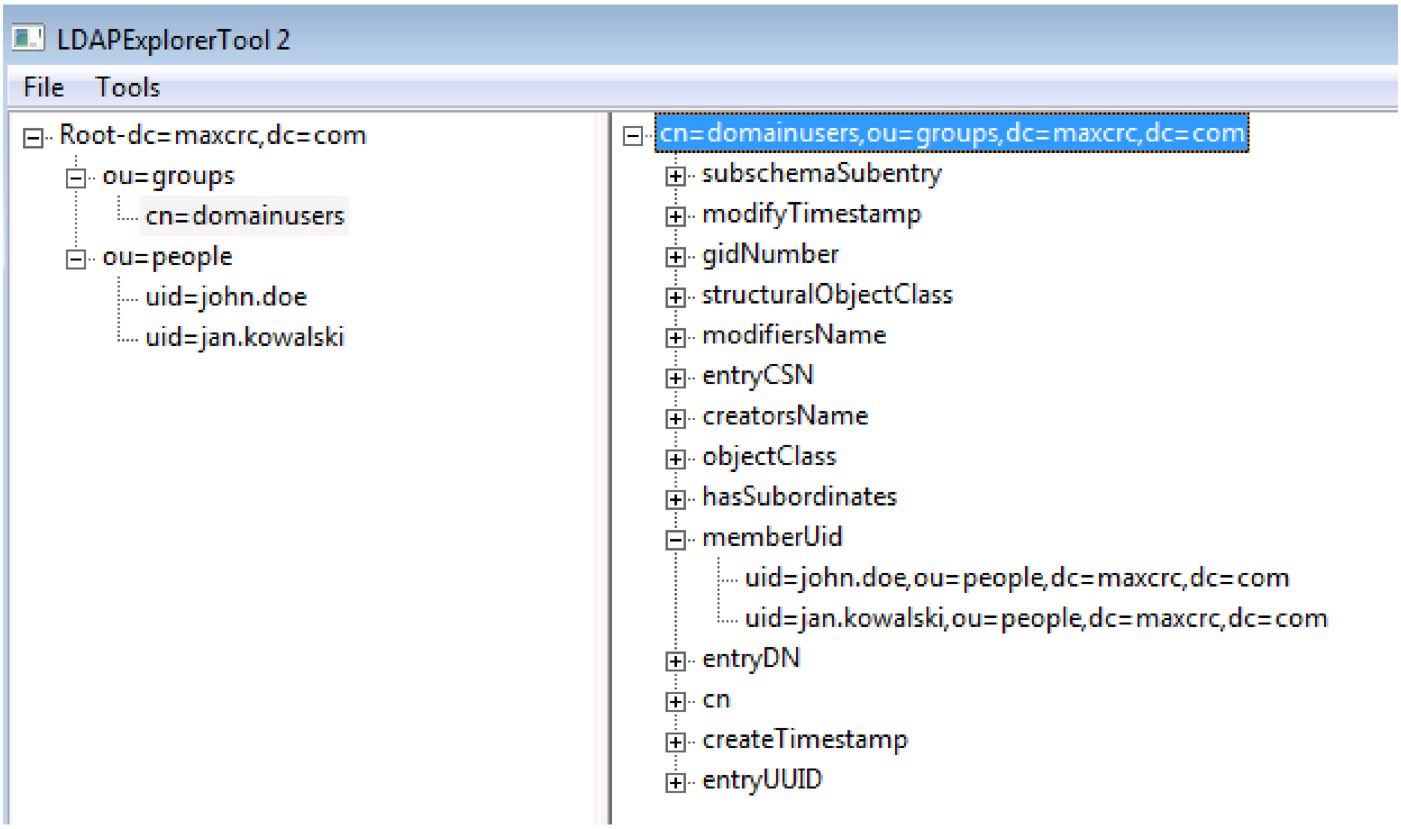
Name	Date modified	Type	Size
BDBTools	6/3/2015 5:06 PM	File folder	
ClientTools	6/3/2015 5:06 PM	File folder	
data	6/4/2015 9:09 PM	File folder	
ldifdata	6/4/2015 11:03 AM	File folder	
Readme	6/3/2015 5:06 PM	File folder	
replica	6/3/2015 5:06 PM	File folder	
run	6/4/2015 9:09 PM	File folder	
schema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

Prendere nota in particolare di due directory:

- ClientTools: questa directory include un set di file binari utilizzati per modificare il database LDAP.

- ldifdata: posizione in cui memorizzare i file con oggetti LDAP.

Aggiungere la seguente struttura al database LDAP:



```
Root-dc=maxcrc,dc=com
  ou=groups
    cn=domainusers
  ou=people
    uid=john.doe
    uid=jan.kowalski
```

```
cn=domainusers,ou=groups,dc=maxcrc,dc=com
  subschemaSubentry
  modifyTimestamp
  gidNumber
  structuralObjectClass
  modifiersName
  entryCSN
  creatorsName
  objectClass
  hasSubordinates
  memberUid
    uid=john.doe,ou=people,dc=maxcrc,dc=com
    uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
  entryDN
  cn
  createTimestamp
  entryUUID
```

Nella directory principale è necessario configurare due unità organizzative. L'unità organizzativa OU=groups deve avere un gruppo figlio (cn=domainusers in questo esempio).

L'unità organizzativa OU=people definisce i due account utente che appartengono al gruppo cn=domainusers.

Per popolare il database, è necessario prima creare il file ldif. La struttura sopra indicata è stata creata a partire da questo 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
```

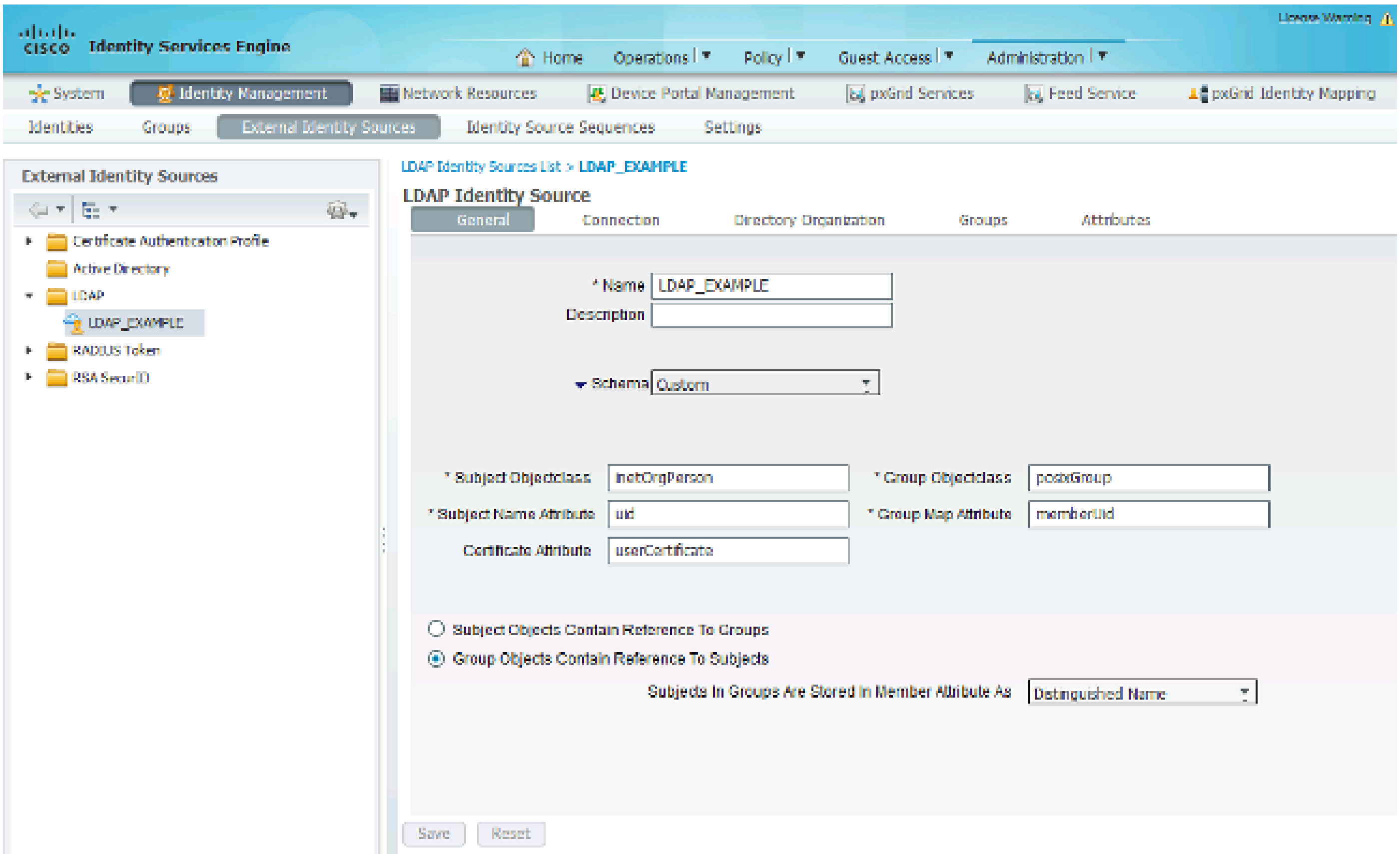
```
mail: john.doe@example.com
userPassword: password

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
```

Per aggiungere gli oggetti al database LDAP, utilizzare il binario 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"
```

Integrazione di OpenLDAP con ISE

Utilizzare le informazioni fornite nelle immagini di questa sezione per configurare LDAP come archivio identità esterno sull'ISE.



LDAP Identity Sources List > LDAP_EXAMPLE

LDAP Identity Source

General | Connection | Directory Organization | Groups | Attributes

* Name: LDAP_EXAMPLE

Description:

Schema: Custom

* Subject Objectclass: inetOrgPerson

* Group Objectclass: posixGroup

* Subject Name Attribute: uid

* Group Map Attribute: memberUid

Certificate Attribute: userCertificate

○ Subject Objects Contain Reference To Groups

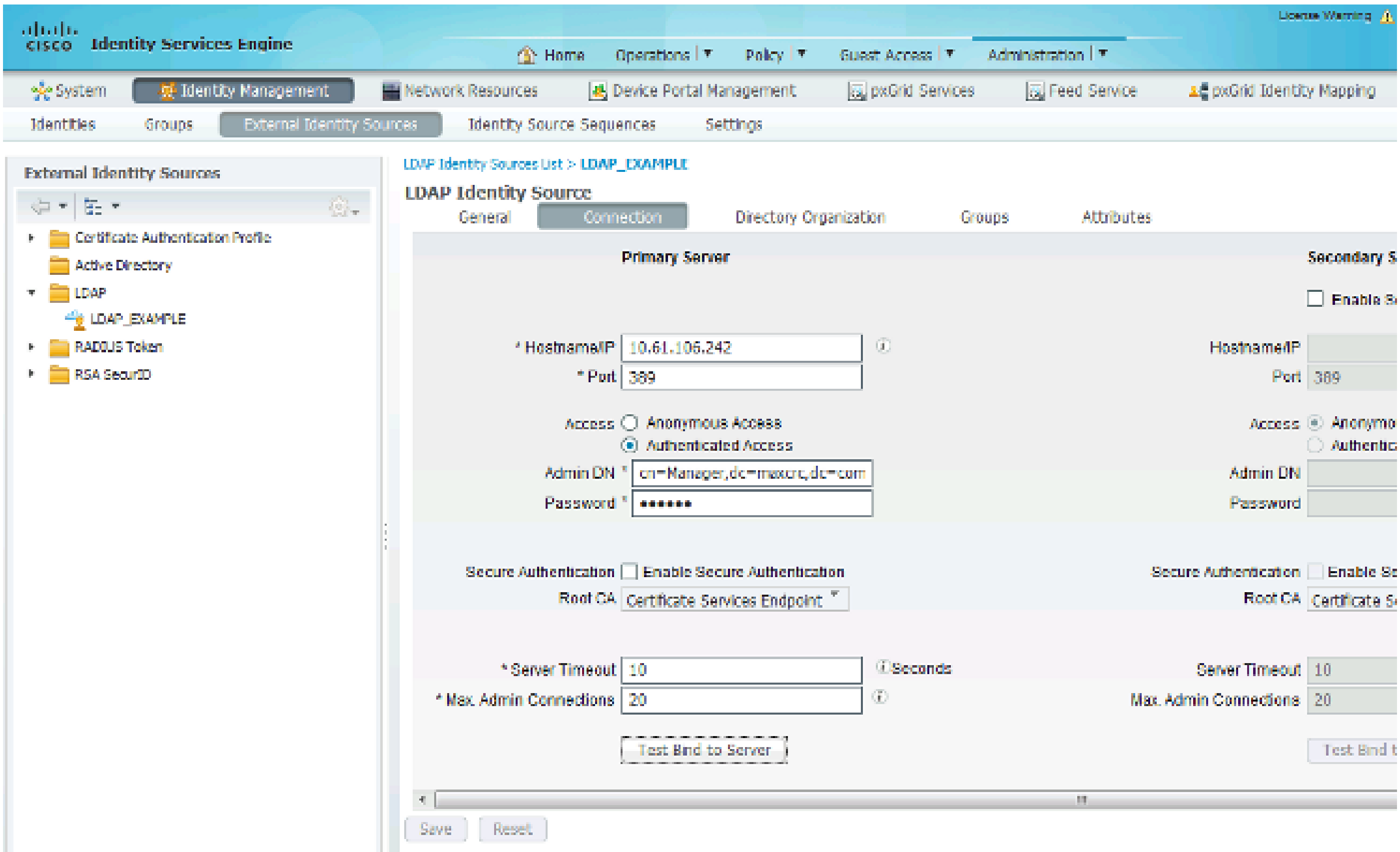
● Group Objects Contain Reference To Subjects

Subjects In Groups Are Stored In Member Attribute As: Distinguished Name

È possibile configurare questi attributi dalla scheda Generale:

- Oggetto Classe oggetto: questo campo corrisponde alla classe oggetto degli account utente nel file ldif. In base alla configurazione LDAP. utilizzare una delle seguenti quattro classi:
  - In alto
  - Persona
  - PersonaOrganizzazione
  - PersonaOrganizzazioneRete
- Attributo nome soggetto: si tratta dell'attributo recuperato da LDAP quando ISE richiede se un nome utente specifico è incluso in un database. In questo scenario è necessario utilizzare john.doe o jan.kowalski come nome utente sull'endpoint.
- Classe oggetto gruppo: questo campo corrisponde alla classe oggetto per un gruppo nel file ldif. In questo scenario, la classe oggetto per il gruppo cn=domainusers è posixGroup.
- Attributo mappa gruppo: definisce il modo in cui gli utenti vengono mappati ai gruppi. Nel gruppo cn=domainusers del file ldif vengono visualizzati due attributi memberUid che corrispondono agli utenti.

ISE offre anche alcuni schemi preconfigurati (Microsoft Active Directory, Sun, Novell):



Primary Server

* Hostname/IP 10.61.106.242

* Port 389

Access ○ Anonymous Access

● Authenticated Access

Admin DN * cn=Manager,dc=maxcrc,dc=com

Password * ••••••

Secure Authentication □ Enable Secure Authentication

Root CA Certificate Services Endpoint

* Server Timeout 10 Seconds

* Max. Admin Connections 20

Secondary S

□ Enable S

Hostname/IP

Port 389

Access ● Anonymo

○ Authentic

Admin DN

Password

Secure Authentication □ Enable Se

Root CA Certificate S

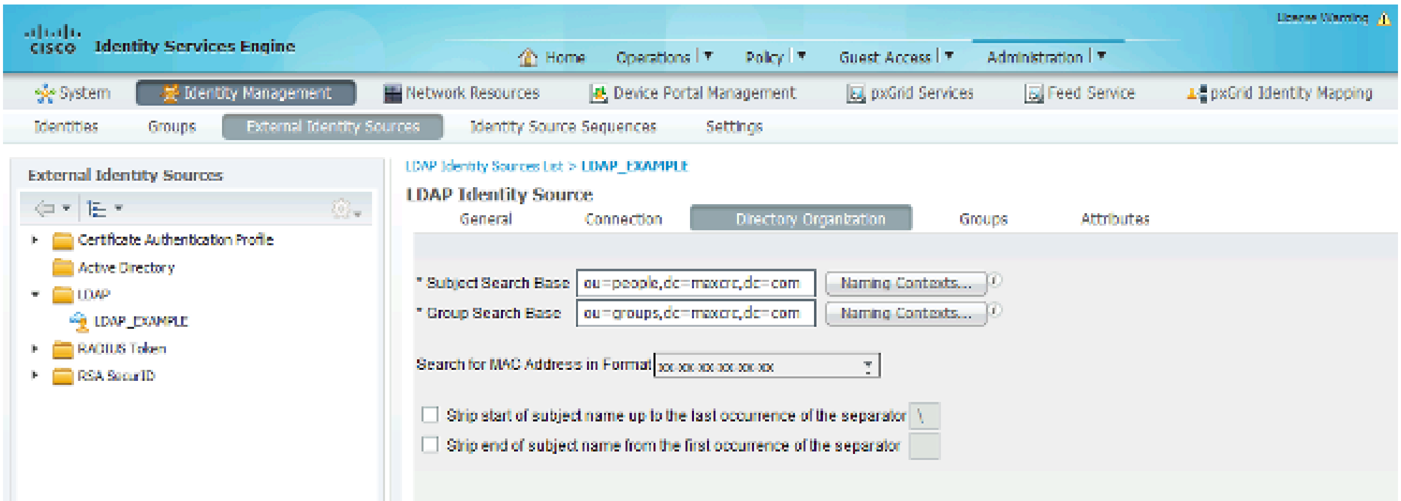
Server Timeout 10

Max. Admin Connections 20

Dopo aver impostato l'indirizzo IP e il nome di dominio amministrativo corretti, è possibile eseguire il test del binding al server. A questo punto, non è possibile recuperare alcun oggetto o gruppo poiché le basi di ricerca non sono ancora configurate.

Nella scheda successiva, configurare la base di ricerca Oggetto/Gruppo. Questo è il punto di join dell'ISE al LDAP. È possibile recuperare solo gli oggetti e i gruppi figli del punto di unione.

In questo scenario vengono recuperati gli oggetti da OU=people e i gruppi da OU=groups:



* Subject Search Base ou=people,dc=maxcrc,dc=com

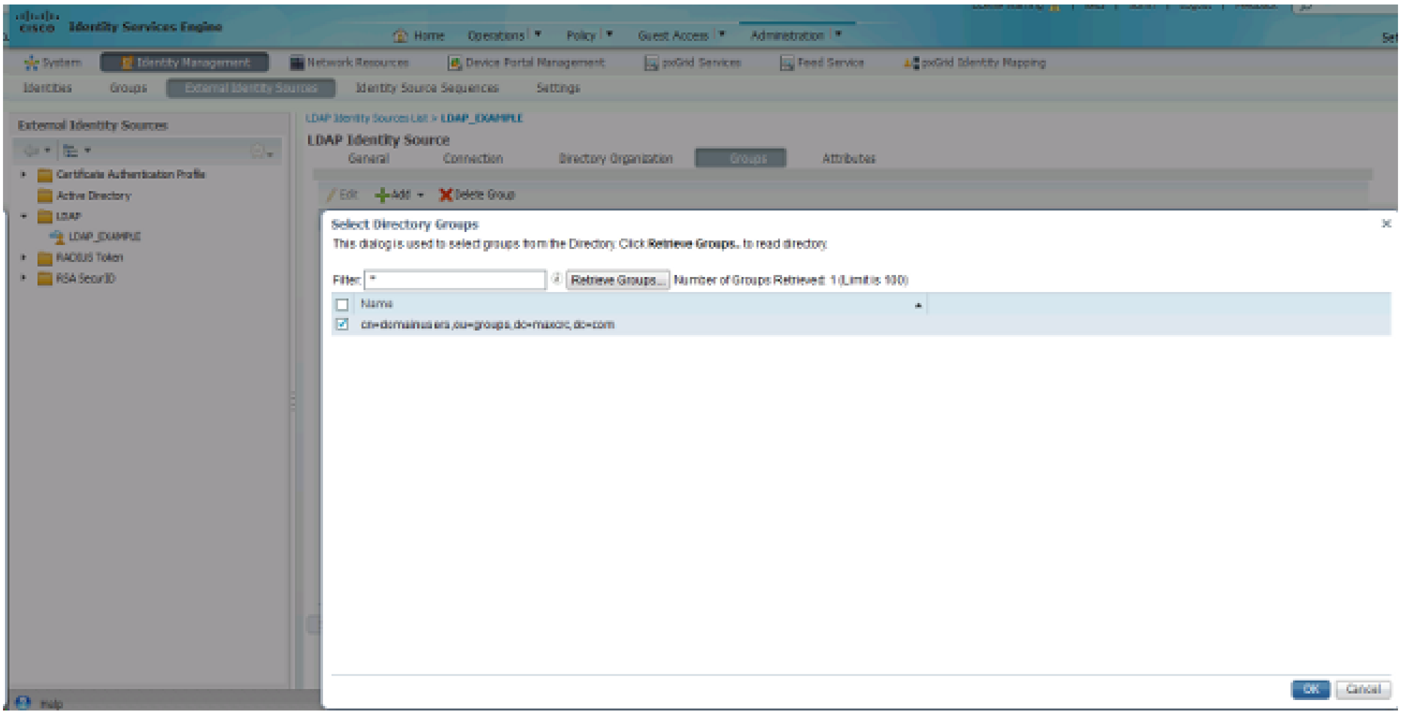
* Group Search Base ou=groups,dc=maxcrc,dc=com

Search for MAC Address in Format xx xx xx xx xx xx

□ Strip start of subject name up to the last occurrence of the separator \

□ Strip end of subject name from the first occurrence of the separator

Dalla scheda Gruppi, è possibile importare i gruppi dal server LDAP sull'ISE:



LDAP Identity Sources List > LDAP_EXAMPLE

LDAP Identity Source

Select Directory Groups

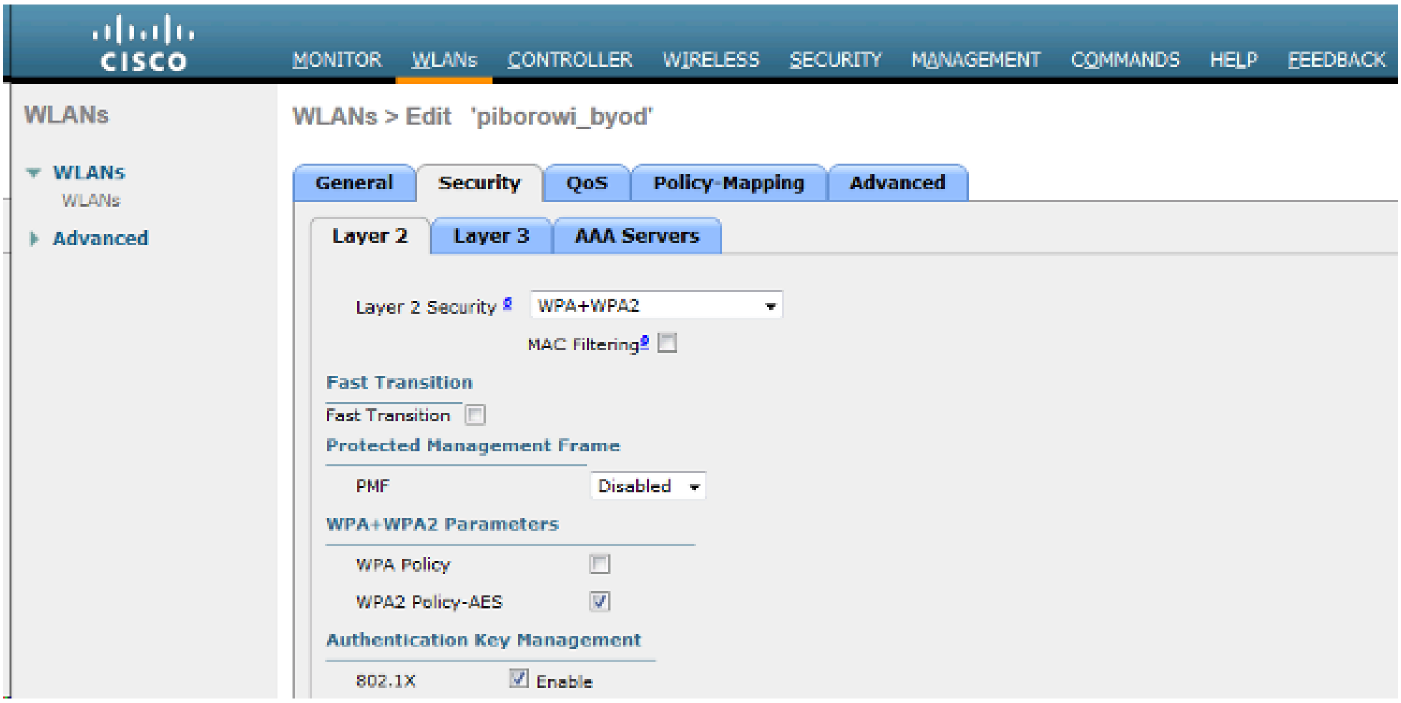
This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.

Filter: * Number of Groups Retrieved: 1 (Limit is 100)

☑ cn=domainusers,ou=groups,dc=maxcrc,dc=com

Configurare il WLC

Usare le informazioni fornite in queste immagini per configurare il WLC per l'autenticazione 802.1x:



WLANs > Edit 'piborowi_byod'

Layer 2 Security: WPA+WPA2

MAC Filtering □

Fast Transition

Fast Transition □

Protected Management Frame

PMF: Disabled

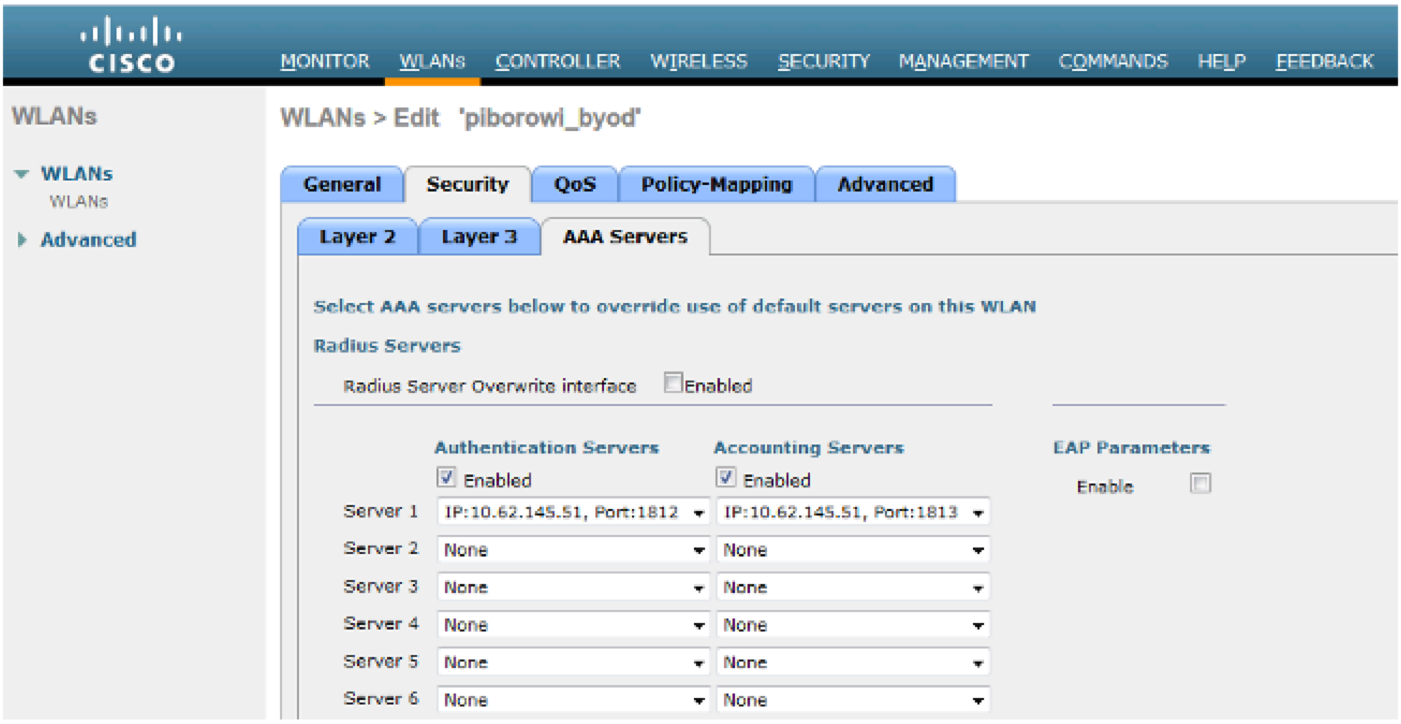
WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy-AES ☑

Authentication Key Management

802.1X ☑ Enable



WLANs > Edit 'piborowi_byod'

Select AAA servers below to override use of default servers on this WLAN

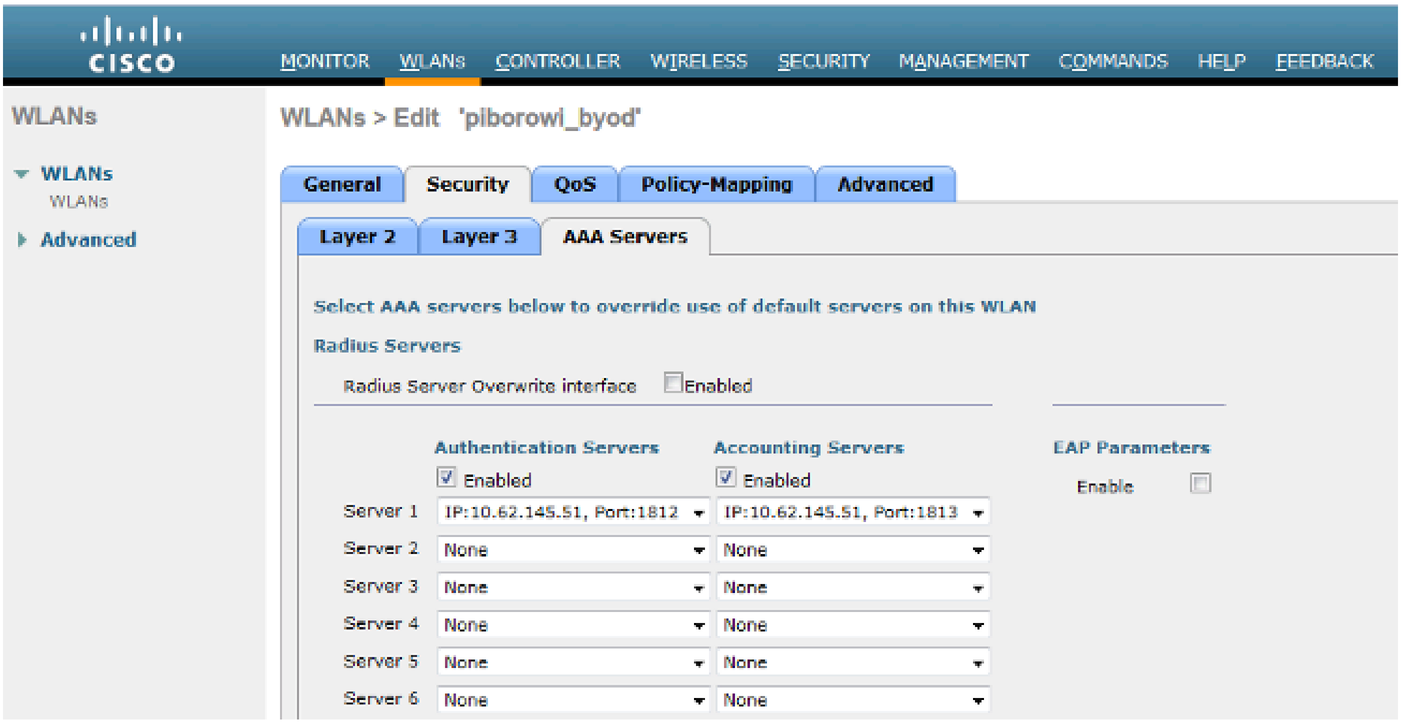
Radius Servers

Radius Server Overwrite interface □Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.62.145.51, Port:1812	IP:10.62.145.51, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

EAP Parameters

Enable □


WLANs > Edit 'piborowi_byod'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface □Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.62.145.51, Port:1812	IP:10.62.145.51, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

EAP Parameters

Enable □

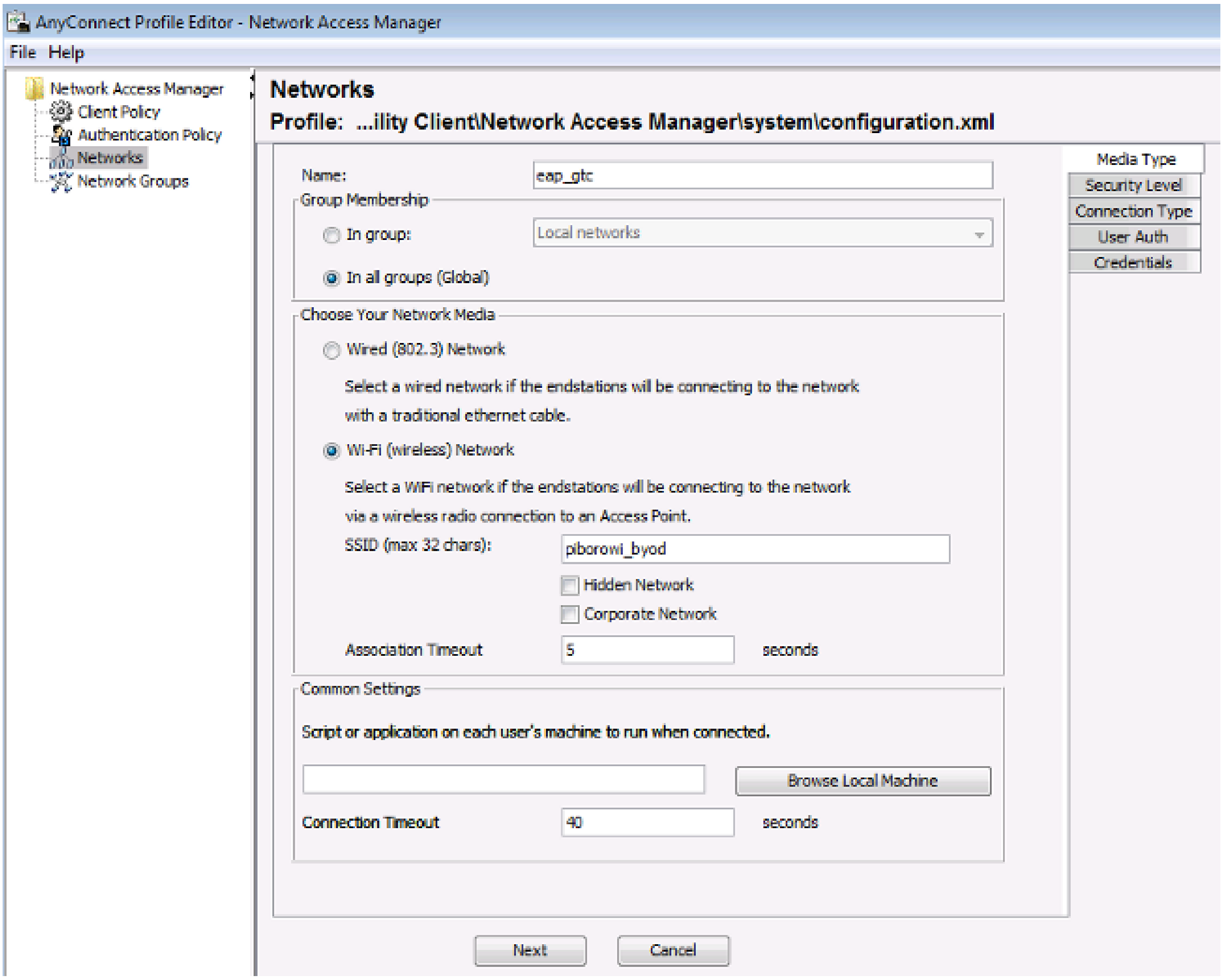
Configurazione di EAP-GTC

Uno dei metodi di autenticazione supportati per LDAP è EAP-GTC. È disponibile in Cisco AnyConnect, ma per configurare correttamente il profilo è necessario installare l'Editor profili di Network Access Manager.

È inoltre necessario modificare la configurazione di Network Access Manager, che per impostazione predefinita si trova qui:

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

Utilizzare le informazioni fornite in queste immagini per configurare il protocollo EAP-GTC sull'endpoint:



Networks

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

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

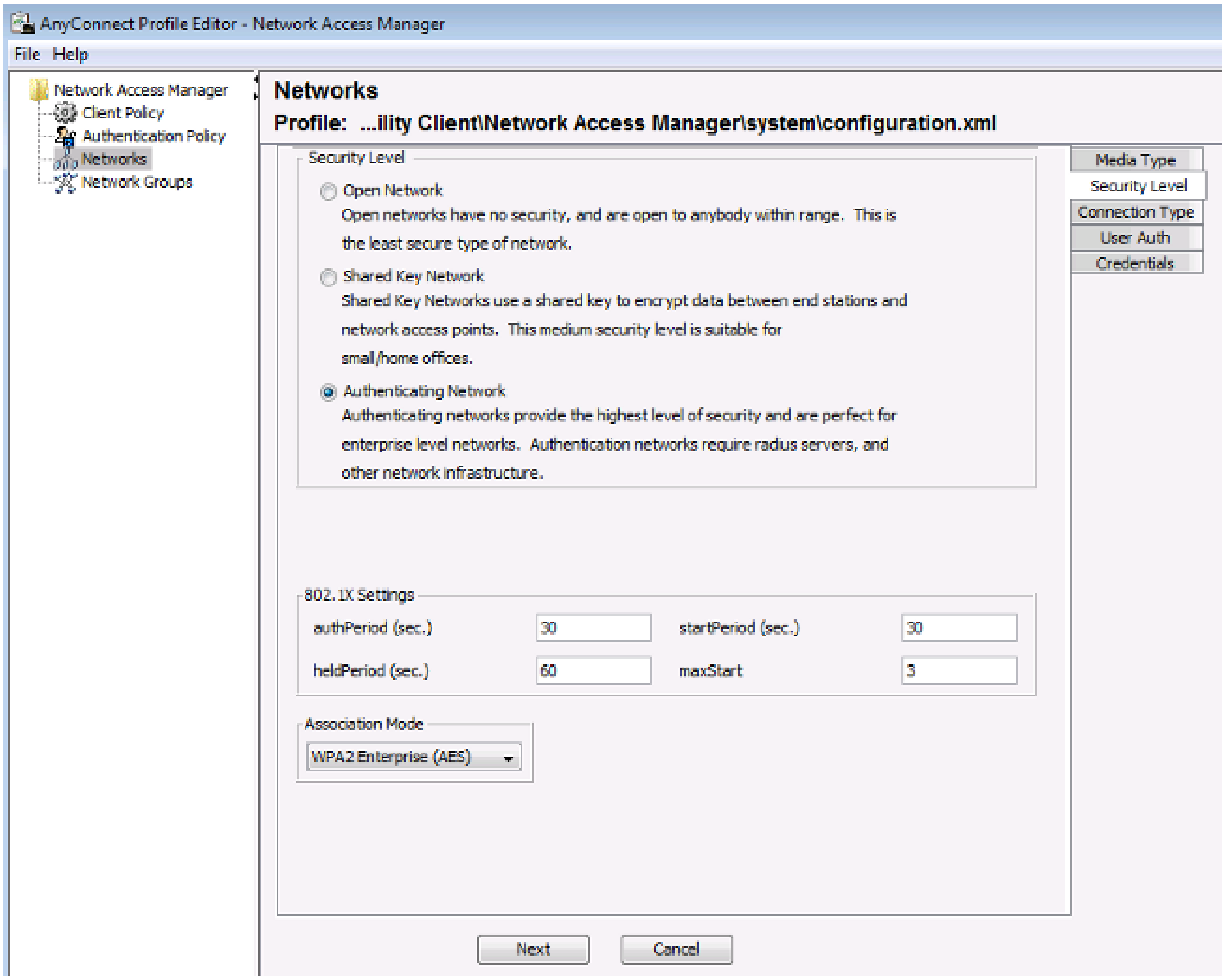
□ Corporate Network

Association Timeout 5 seconds

Common Settings

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

Connection Timeout 40 seconds



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.

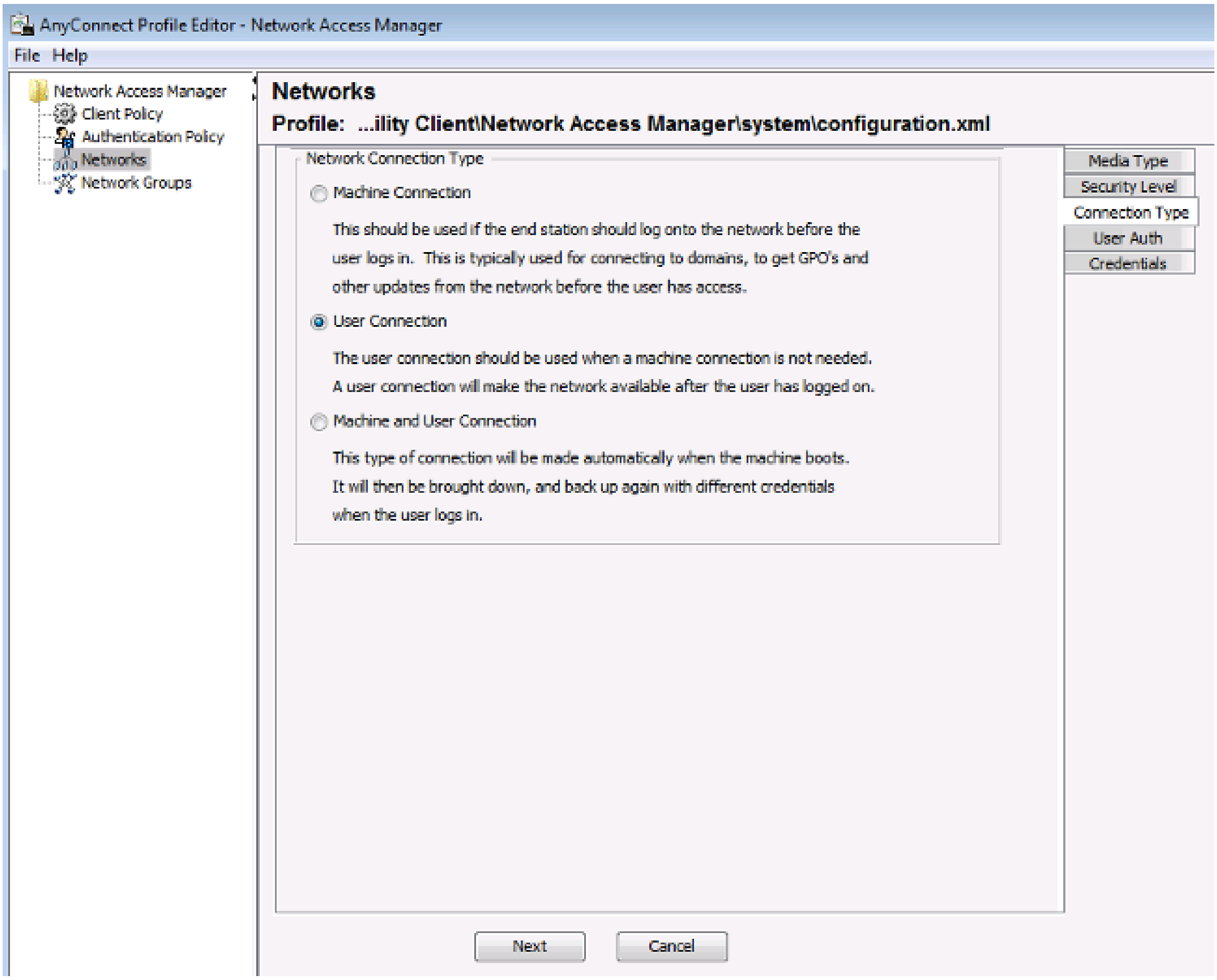
○ Shared Key Network
Shared Key Networks use a shared key to encrypt data between end stations and network access points. This medium security level is suitable for small/home offices.

● 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.)	30	startPeriod (sec.)	30
heldPeriod (sec.)	60	maxStart	3

Association Mode: WPA2 Enterprise (AES)



Networks

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

Network Connection Type

○ Machine Connection

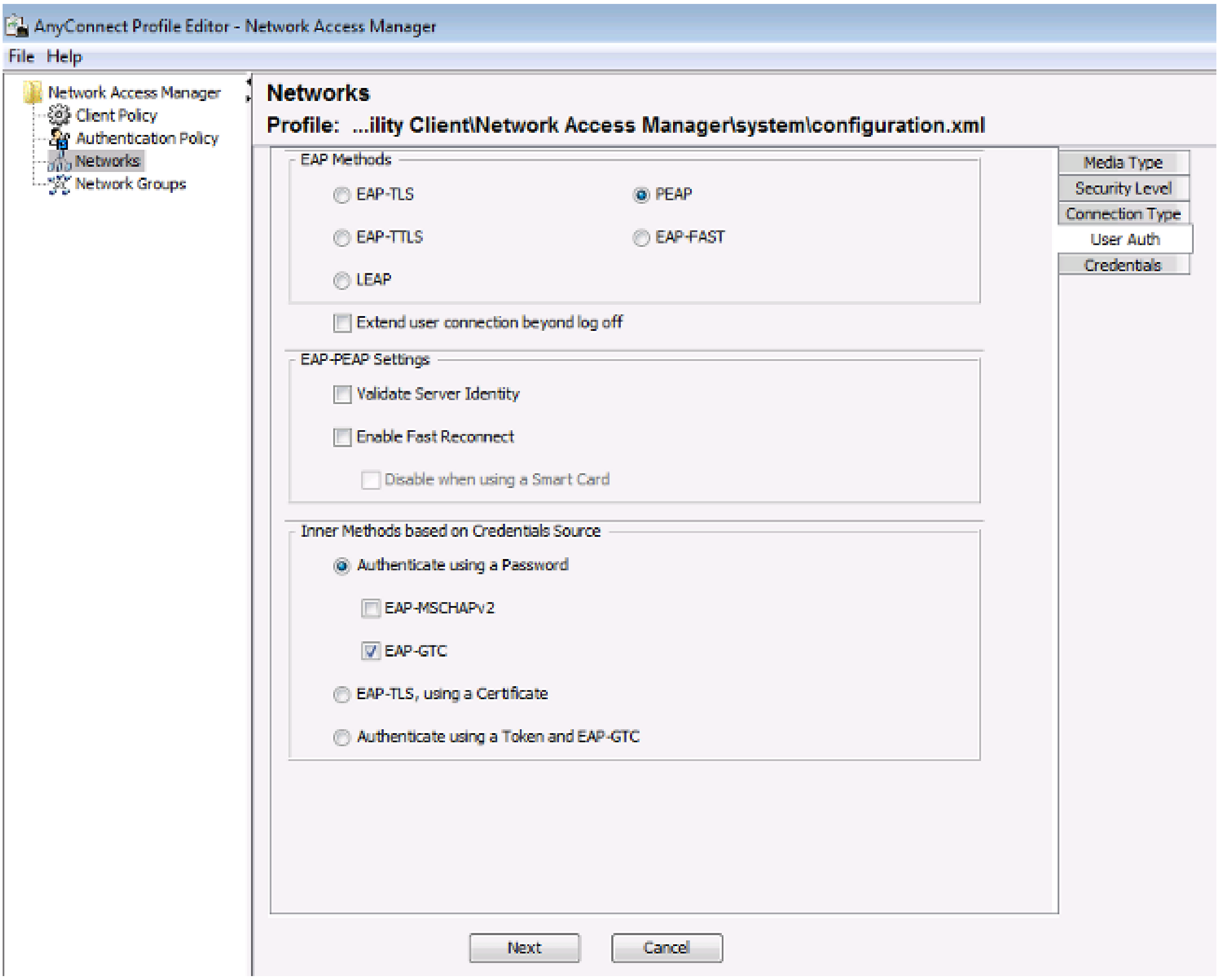
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

● 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.



AnyConnect Profile Editor - Network Access Manager

File Help

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

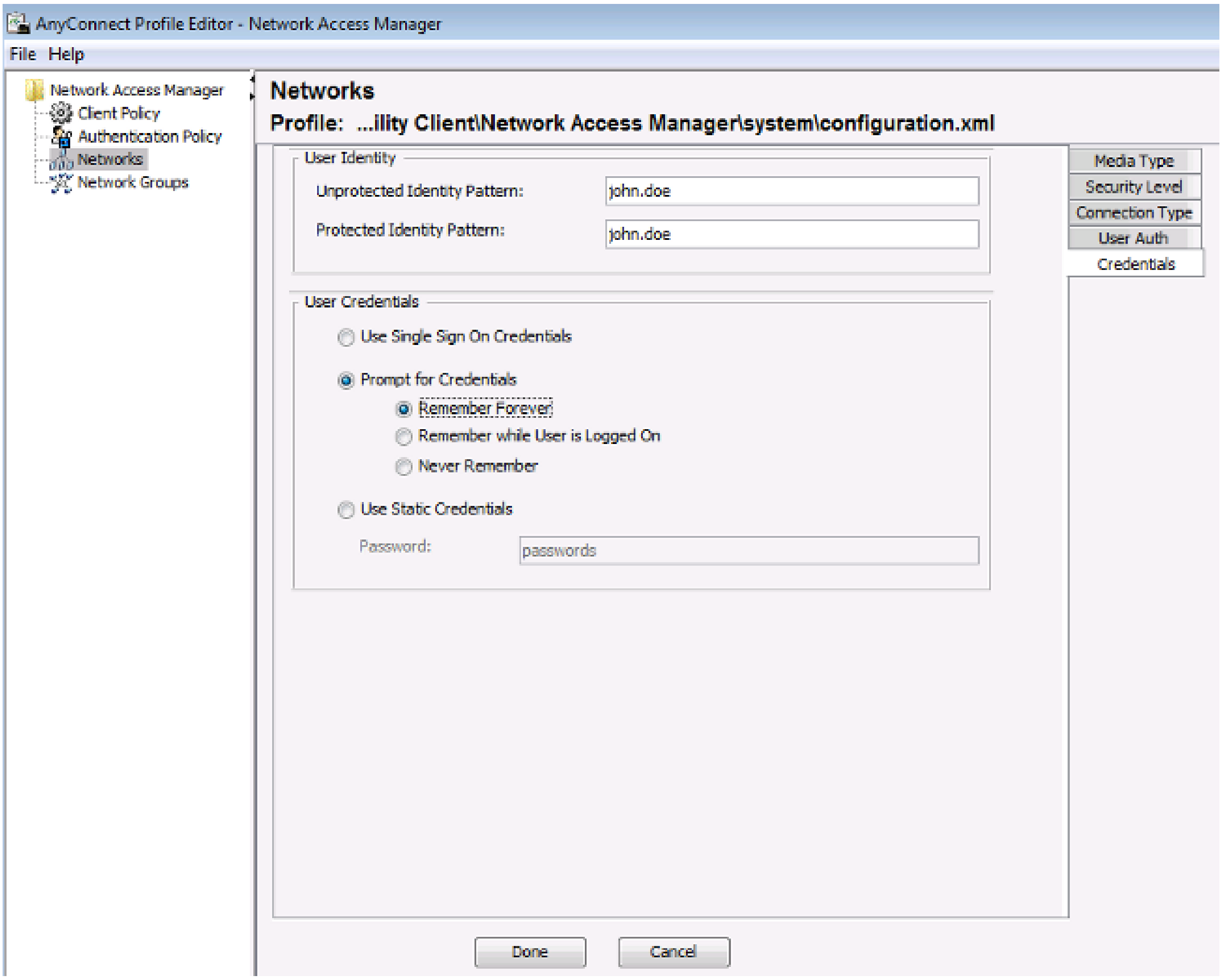
● Authenticate using a Password

□ EAP-MSCHAPv2

☑ EAP-GTC

○ EAP-TLS, using a Certificate

○ Authenticate using a Token and EAP-GTC



Networks

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

User Identity

Unprotected Identity Pattern: john.doe

Protected Identity Pattern: john.doe

User Credentials

○ Use Single Sign On Credentials

● Prompt for Credentials

● Remember Forever

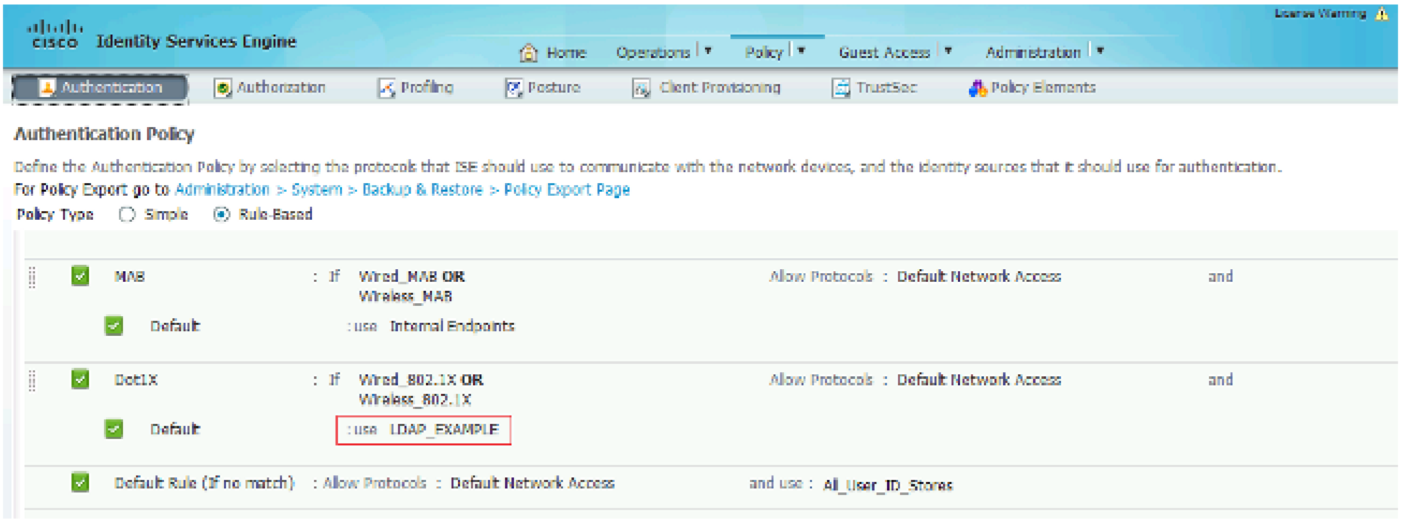
○ Remember while User is Logged On

○ Never Remember

○ Use Static Credentials

Password: passwords

Utilizzare le informazioni fornite in queste immagini per modificare i criteri di autenticazione e autorizzazione sull'ISE:



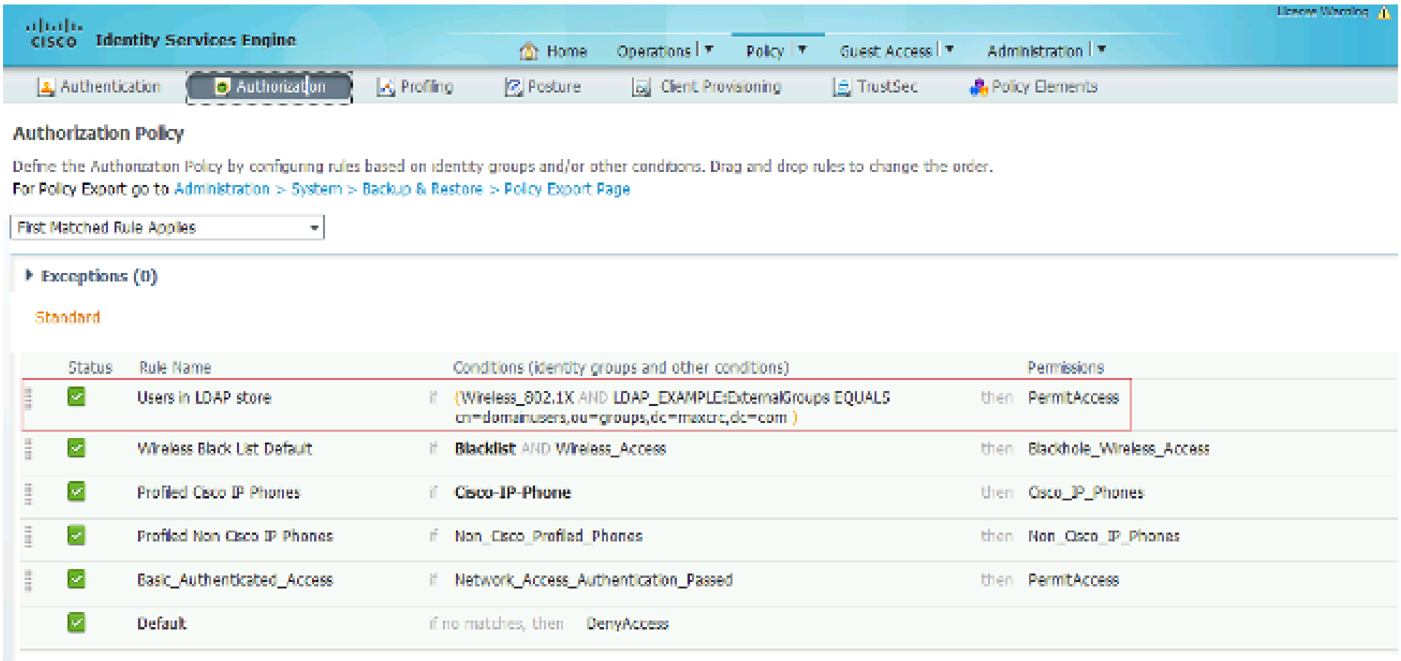
Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type ○ Simple ● Rule-Based

☑ MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access	and
☑ Default	: use Internal Endpoints		
☑ Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access	and
☑ Default	: use LDAP_EXAMPLE		
☑ Default Rule (If no match)	: Allow Protocols : Default Network Access	and use : All_User_ID_Stores	



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

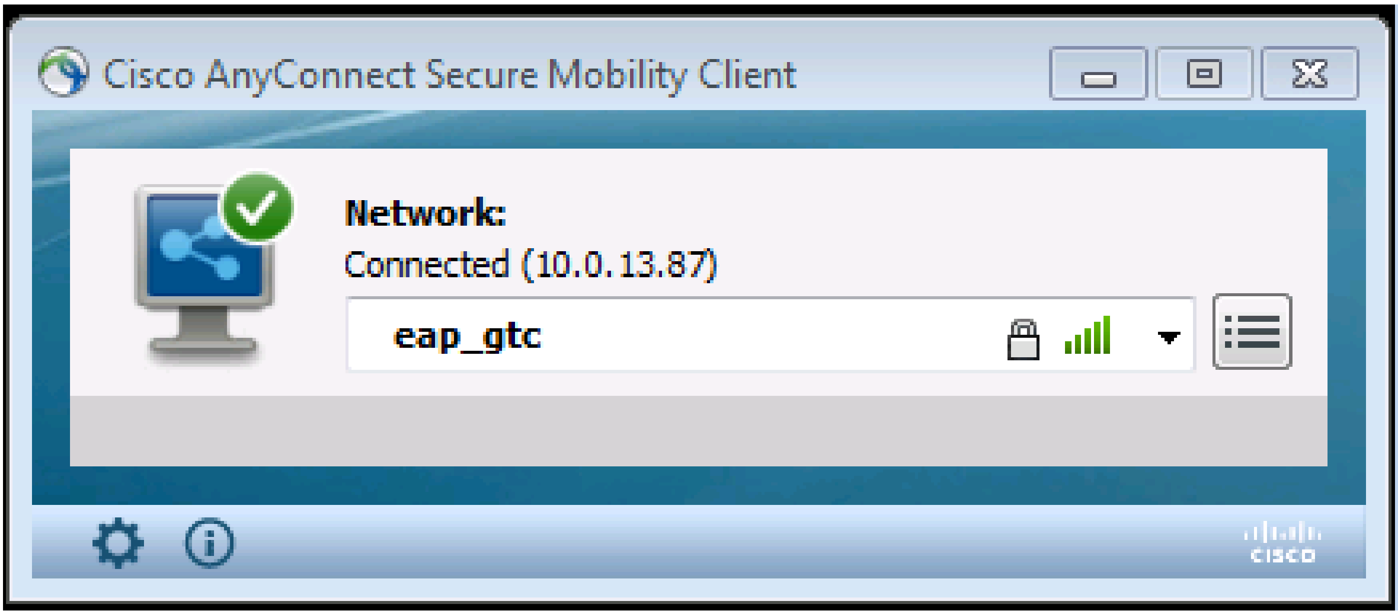
First Matched Rule Applies

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=maxcrc,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		

Dopo aver applicato la configurazione, dovrebbe essere possibile connettersi alla rete:

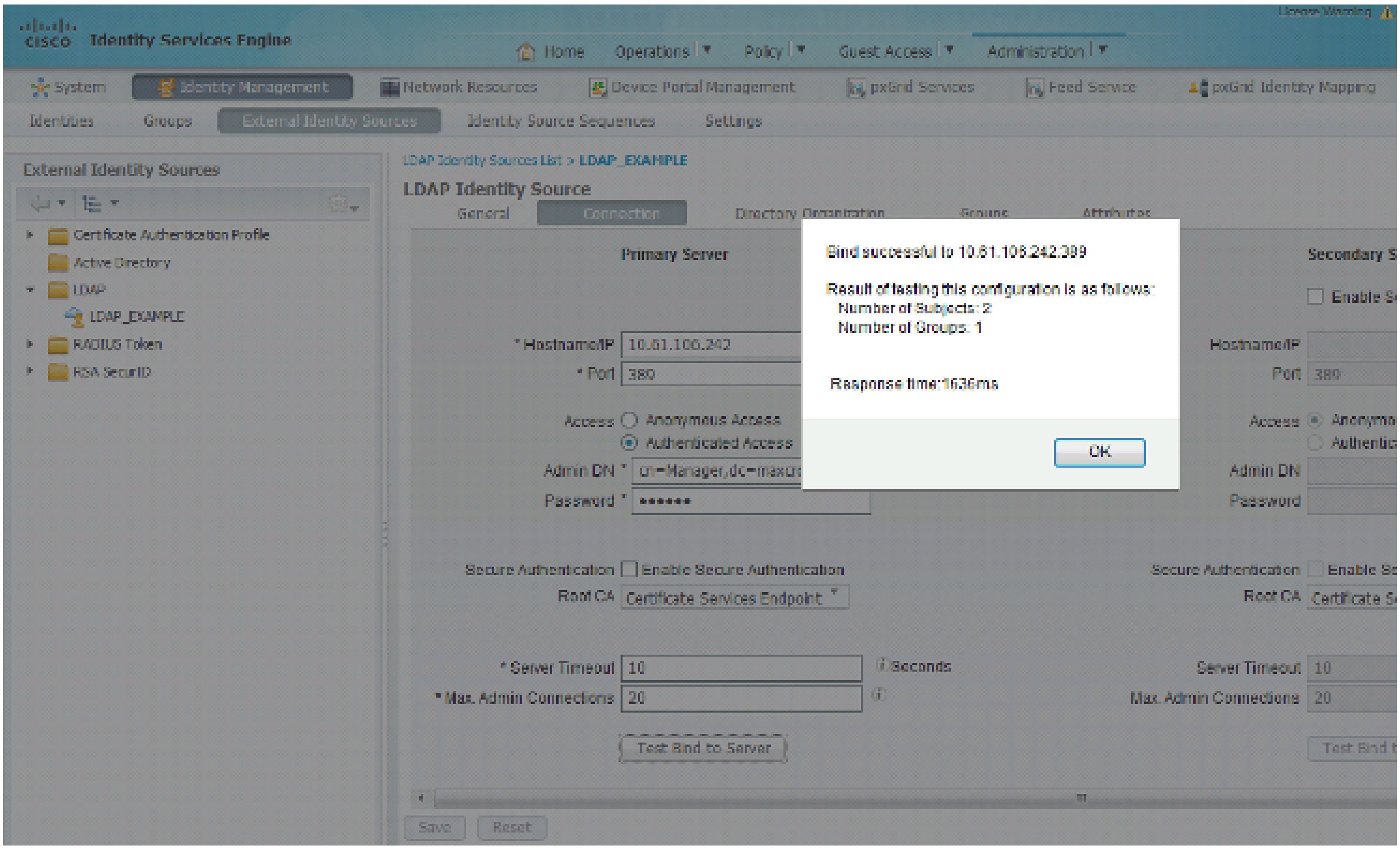


Network:
Connected (10.0.13.87)

eap_gtc

Verifica

Per verificare le configurazioni LDAP e ISE, recuperare gli oggetti e i gruppi con una connessione di prova al server:



LDAP Identity Source

Primary Server

* Hostname/IP 10.61.106.242

* Port 389

Access ○ Anonymous Access ● Authenticated Access

Admin DN * cn=Manager,dc=maxcr

Password * ••••••

Secure Authentication □ Enable Secure Authentication

Root CA Certificate Services Endpoint

* Server Timeout 10 Seconds

* Max. Admin Connections 20

Secondary Server

□ Enable S

Hostname/IP

Port 389

Access ● Anonymo ○ Authentic

Admin DN

Password

Secure Authentication □ Enable Se

Root CA Certificate S

Server Timeout 10

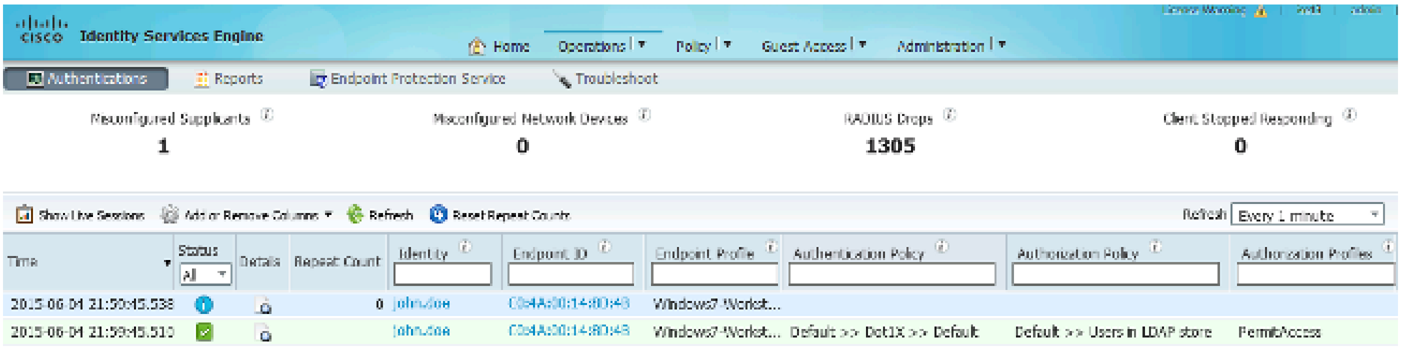
Max. Admin Connections 20

Bind successful to 10.61.106.242:389

Result of testing this configuration is as follows:
Number of Subjects: 2
Number of Groups: 1

Response time:1636ms

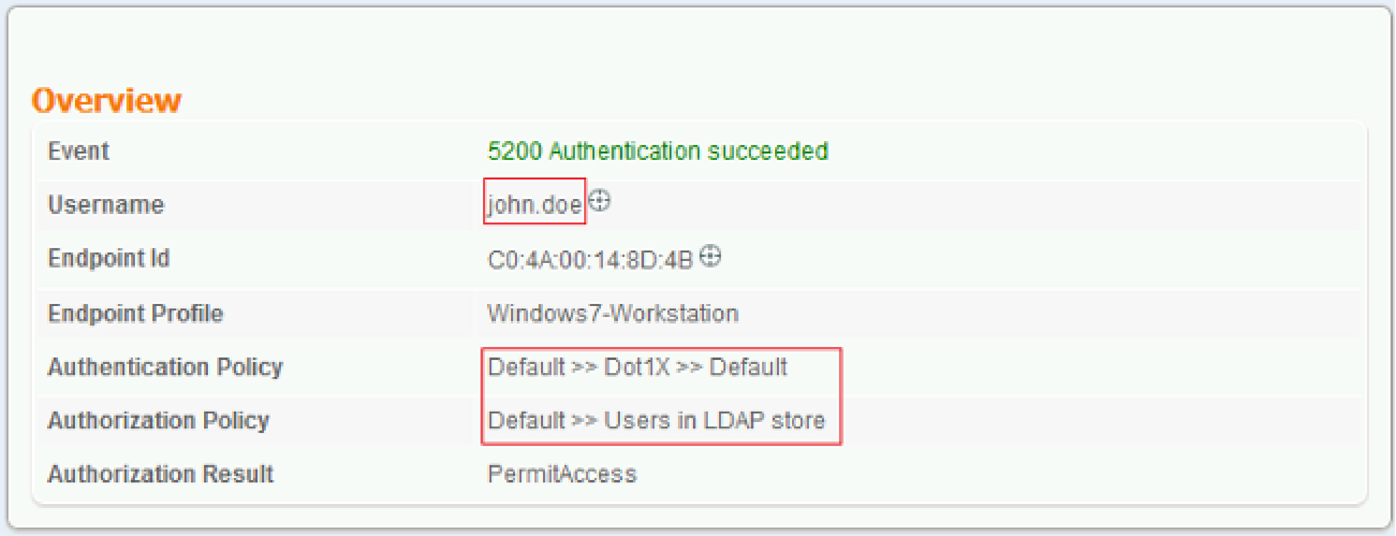
Di seguito viene riportato un esempio di report generato dall'ISE:



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding
1	0	1305	0

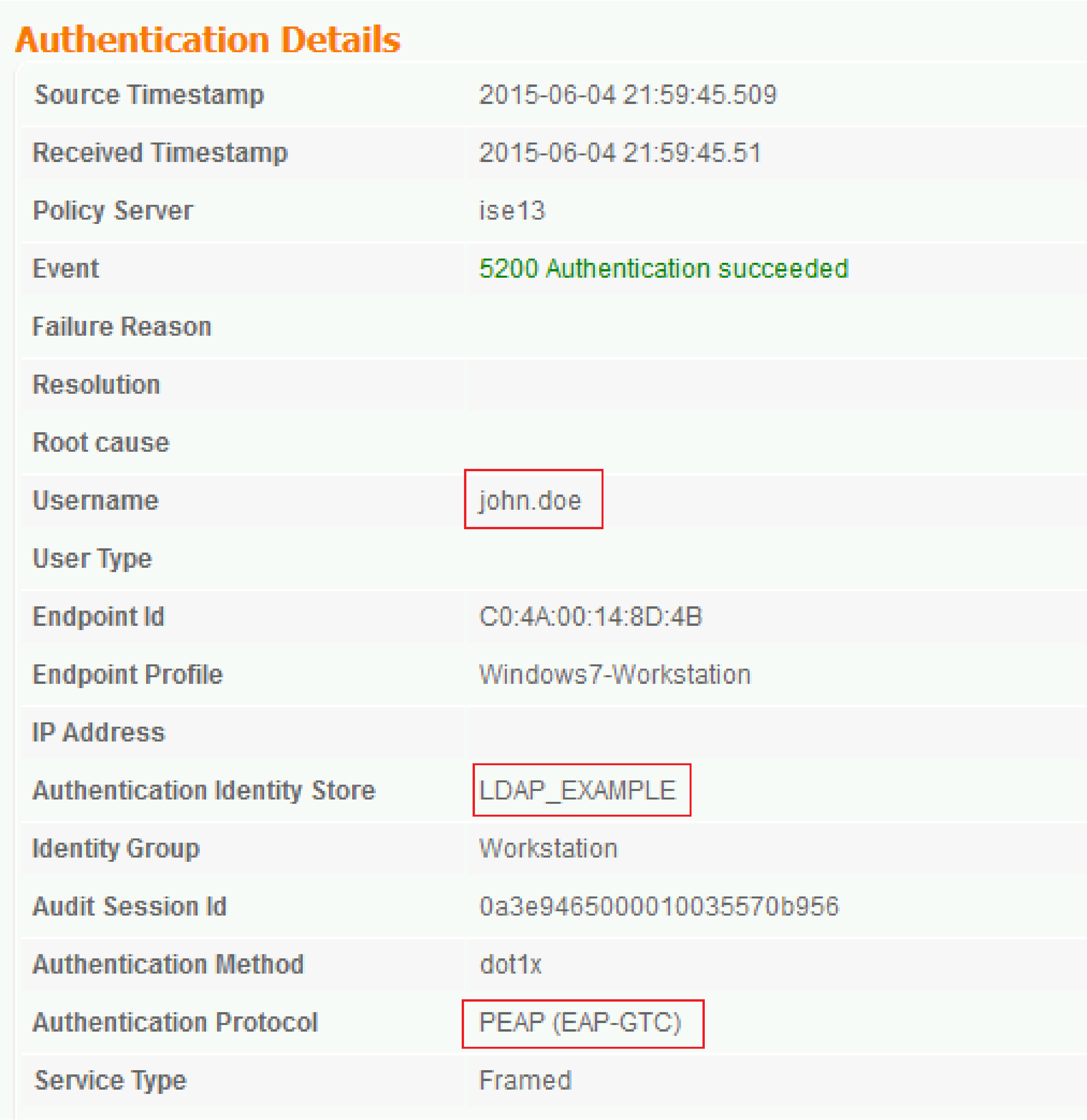
Refresh Every 1 minute

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
	All								
2015-06-04 21:59:45.538	●		0	john.doe	C0:4A:00:14:8D:4B	Windows7-Workst...			
2015-06-04 21:59:45.510	✓			john.doe	C0:4A:00:14:8D:4B	Windows7-Workst...	Default >> Dot1X >> Default	Default >> Users in LDAP store	PermitAccess



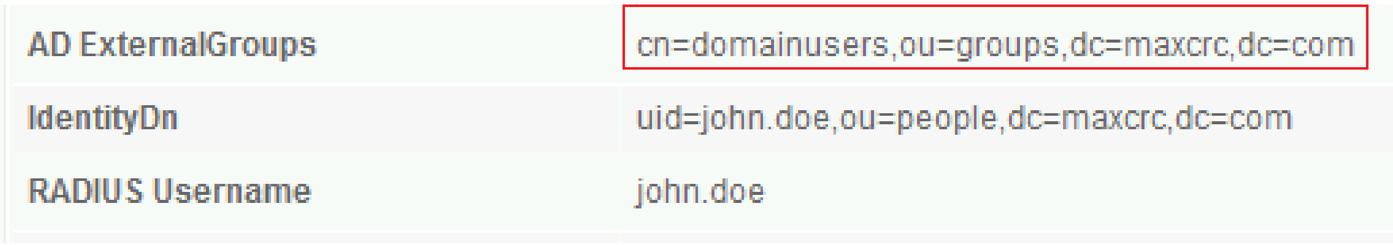
Overview

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

Risoluzione dei problemi

In questa sezione vengono descritti alcuni errori comuni che si sono verificati con questa configurazione e viene spiegato come risolverli:

- Dopo l'installazione di OpenLDAP, se si verifica un errore che indica la mancanza del file gssapi.dll, riavviare Microsoft Windows.
- Potrebbe non essere possibile modificare direttamente il file configuration.xml di Cisco AnyConnect. Salvare la nuova configurazione in un'altra posizione e quindi utilizzarla per sostituire il file precedente.
- Nel report di autenticazione viene visualizzato il seguente messaggio di errore:

  <#root>

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

  Questo messaggio di errore indica che il metodo selezionato non è supportato da LDAP.

Verificare che il protocollo di autenticazione nello stesso report mostri uno dei metodi supportati (EAP-GTC, EAP-TLS o PEAP-TLS).

- Nel report di autenticazione, se si nota che il soggetto non è stato trovato nell'archivio delle identità, il nome utente del report non corrisponde all'Attributo nome soggetto per alcun utente nel database LDAP.

In questo scenario, il valore è stato impostato su uid per questo attributo, il che significa che ISE cerca i valori uid per l'utente LDAP quando cerca di trovare una corrispondenza.

- Se i soggetti e i gruppi non vengono recuperati correttamente durante un test di binding al server, si tratta di una configurazione errata per le basi di ricerca.

Tenere presente che la gerarchia LDAP deve essere specificata dall'elemento foglia alla radice e da dc (può essere costituita da più parole).

Suggerimento: per risolvere i problemi di autenticazione EAP sul lato WLC, fare riferimento al documento di esempio dell'autenticazione EAP con i controller WLAN (WLC).