配置ISE以與LDAP伺服器整合

目錄

簡介

本文檔介紹如何配置思科身份服務引擎(ISE)以便與思科LDAP伺服器整合。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下軟體和硬體版本：

- 帶補丁2的Cisco ISE版本1.3
- 安裝了OpenLDAP的Microsoft Windows版本7 x64
- Cisco無線LAN控制器(WLC)版本8.0.100.0
- 適用於Microsoft Windows的Cisco AnyConnect版本3.1
- 思科網路存取管理員設定檔編輯器

注意：對於使用LDAP作為ISE身份驗證和授權的外部身份源的設定，本文檔有效。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

LDAP支援以下身份驗證方法：

- 可擴充驗證通訊協定 — 通用權杖卡(EAP-GTC)
- 可擴展身份驗證協定 — 傳輸層安全(EAP-TLS)
- 受保護的可擴展身份驗證協定 — 傳輸層安全(PEAP-TLS)

設定

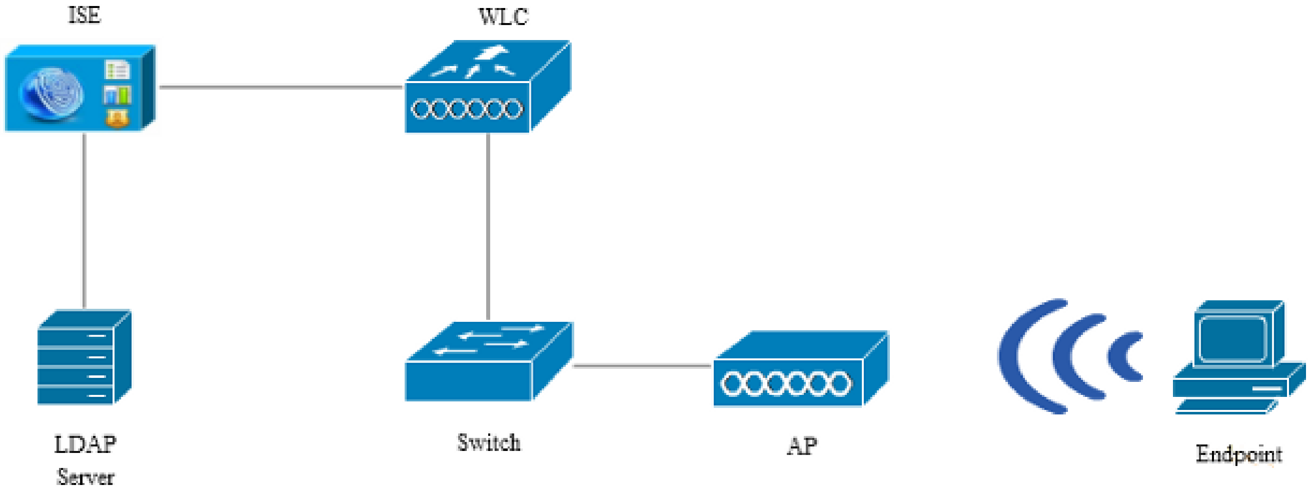
本節介紹如何配置網路裝置並將ISE與LDAP伺服器整合。

網路圖表

在此配置示例中，終端使用無線介面卡以便與無線網路關聯。

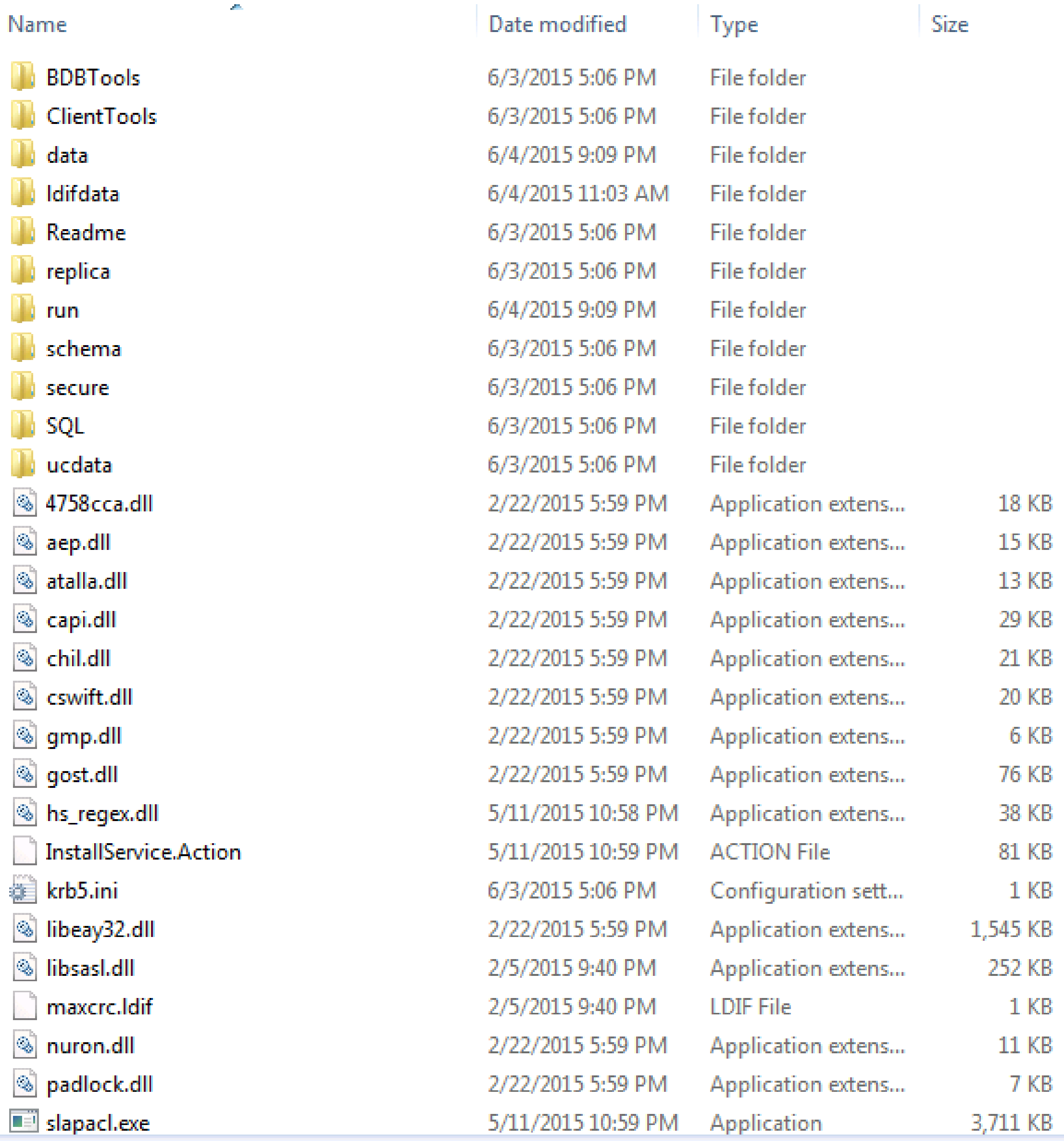
WLC上的無線LAN(WLAN)設定為透過ISE驗證使用者。在ISE上，LDAP配置為外部身份庫。

此圖說明所使用的網路拓撲：



配置OpenLDAP

Microsoft Windows的OpenLDAP安裝通過GUI完成，並且非常簡單。預設位置為C: > OpenLDAP。安裝後，您應該會看到以下目錄：

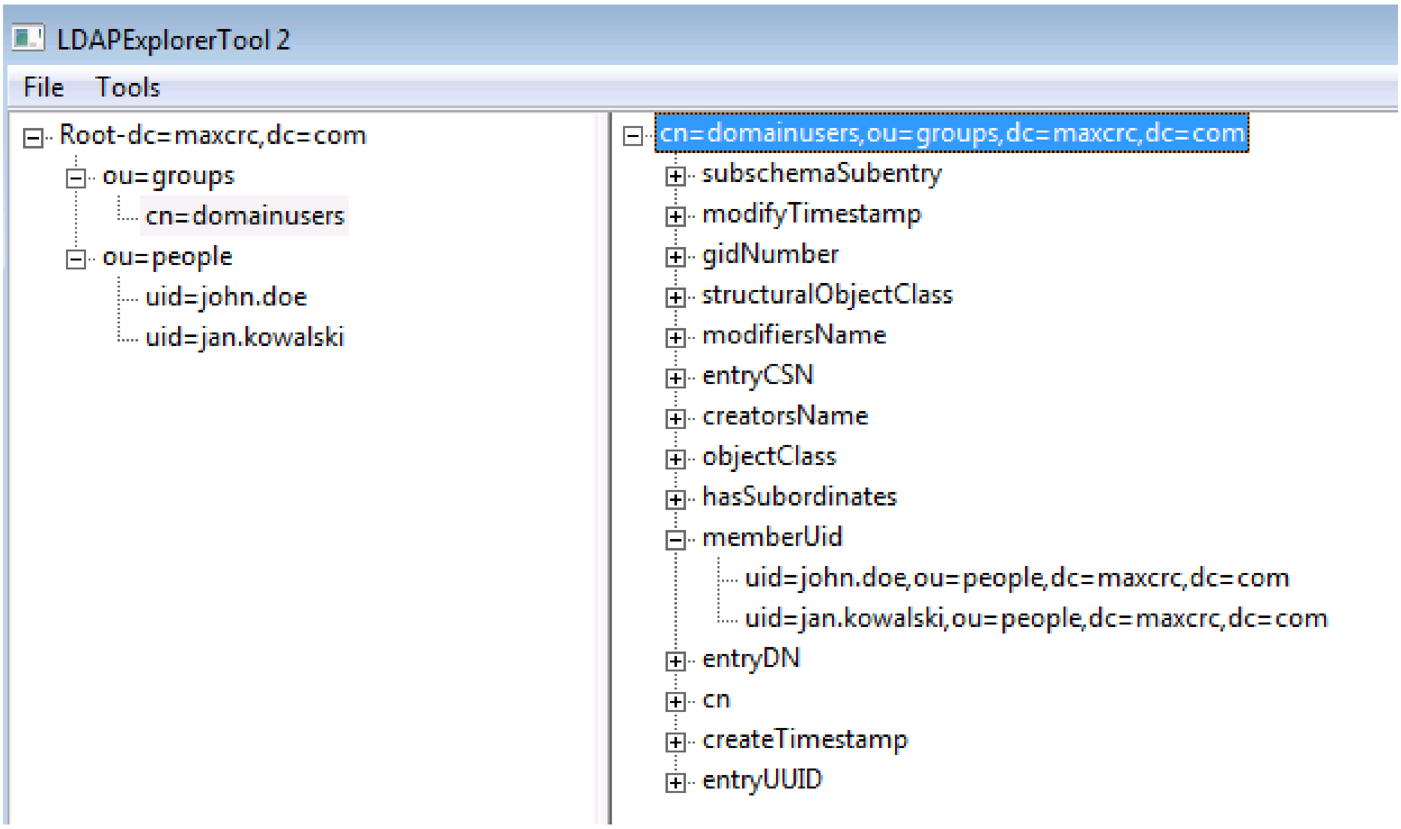


Name	Date modified	Type	Size
BDBTools	6/3/2015 5:06 PM	File folder	
ClientTools	6/3/2015 5:06 PM	File folder	
data	6/4/2015 9:09 PM	File folder	
ldifdata	6/4/2015 11:03 AM	File folder	
Readme	6/3/2015 5:06 PM	File folder	
replica	6/3/2015 5:06 PM	File folder	
run	6/4/2015 9:09 PM	File folder	
schema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

請特別注意以下兩種目錄：

- ClientTools — 此目錄包含一組用於編輯LDAP資料庫的二進位制檔案。
- ldifdata — 這是您應該儲存具有LDAP對象的檔案的位置。

將此結構新增到LDAP資料庫：



```
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
```

在Root目錄下，必須配置兩個組織單位(OU)。OU=groups OU應具有一個子組(在本例中為cn=domainusers)。

OU=people OU定義屬於cn=domainusers組的兩個使用者帳戶。

要填充資料庫，必須首先創建ldif檔案。前面提到的結構是根據以下檔案建立的：

```
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
```

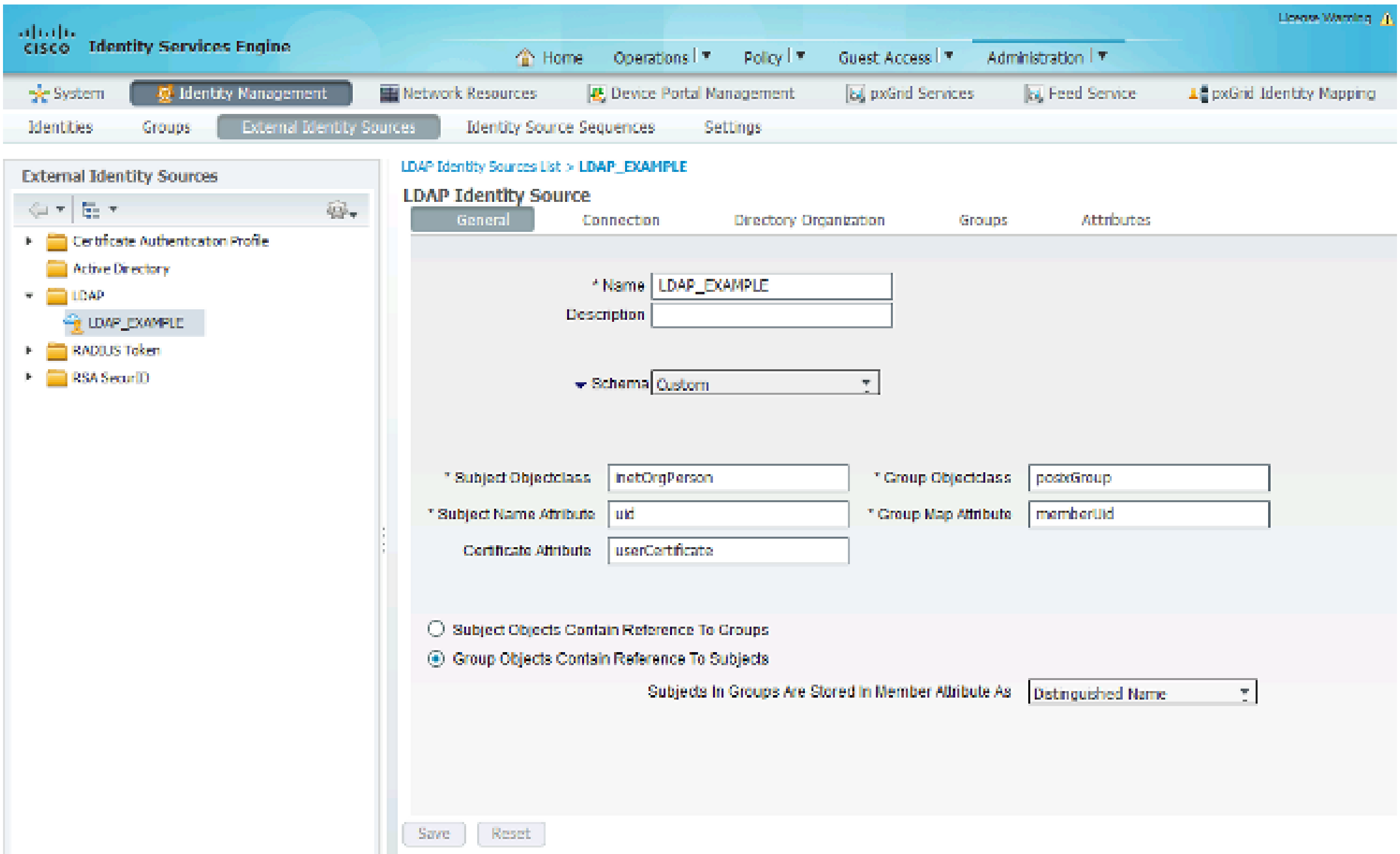
```
dn: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: jan.kowalski
givenName: Jan
sn: Kowalski
cn: Jan Kowalski
mail: jan.kowalski@example.com
userPassword: password

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
```

若要將對象新增到LDAP資料庫，請使用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"
```

將OpenLDAP與ISE整合

使用本節中影象提供的資訊，將LDAP配置為ISE上的外部身份庫。



LDAP Identity Source

* Name: LDAP_EXAMPLE

Description:

Schema: Custom

* Subject Objectclass: inetOrgPerson

* Subject Name Attribute: uid

Certificate Attribute: userCertificate

* Group Objectclass: posixGroup

* Group Map Attribute: memberUid

○ Subject Objects Contain Reference To Groups

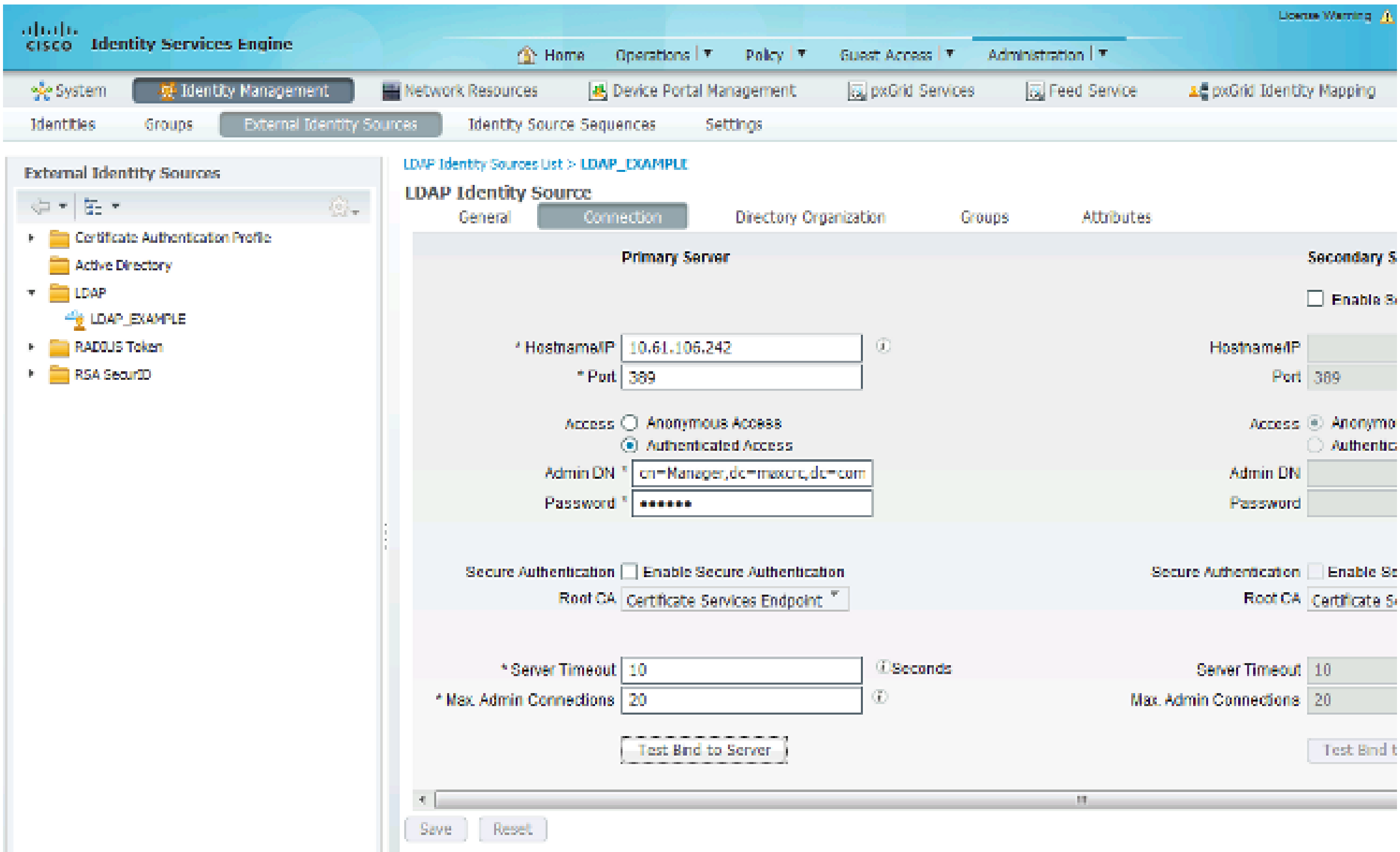
● Group Objects Contain Reference To Subjects

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

可以從General頁籤配置以下屬性：

- Subject Objectclass — 此欄位與ldif檔案中使用者帳戶的對象類對應。根據LDAP配置。請使用以下四個類之一：
  - 頂端
  - 人員
  - 組織人員
  - InetOrgPerson
- Subject Name Attribute — 這是LDAP在ISE查詢資料庫中是否包含特定使用者名稱時檢索的屬性。在此方案中，必須使用john.doe或jan.kowalski作為端點上的使用者名稱。
- Group Objectclass — 此欄位與ldif檔案中組的對象類對應。在此方案中，cn=domainusers組的object類是posixGroup。
- 組對映屬性 — 此屬性定義如何將使用者對映到組。在ldif檔案的cn=domainusers組下，可以看到兩個與使用者對應的memberUid屬性。

ISE還提供一些預配置的架構(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

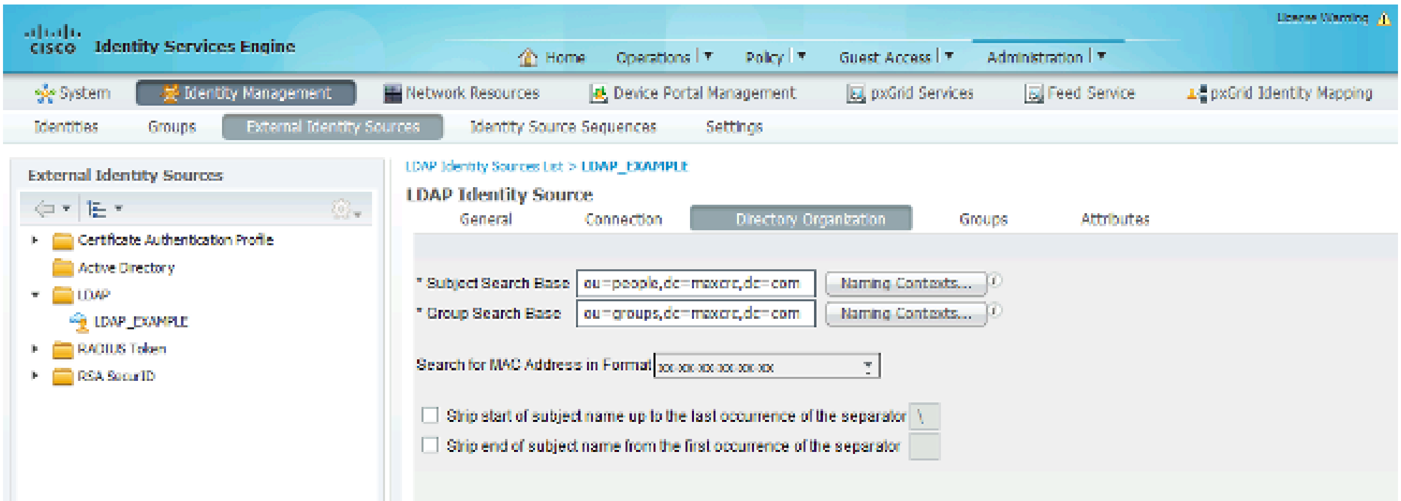
Secondary S

	□ 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

在設定正確的IP地址和管理域名後，您可以測試繫結到伺服器。此時，您不會檢索任何主題或組，因為尚未配置搜尋庫。

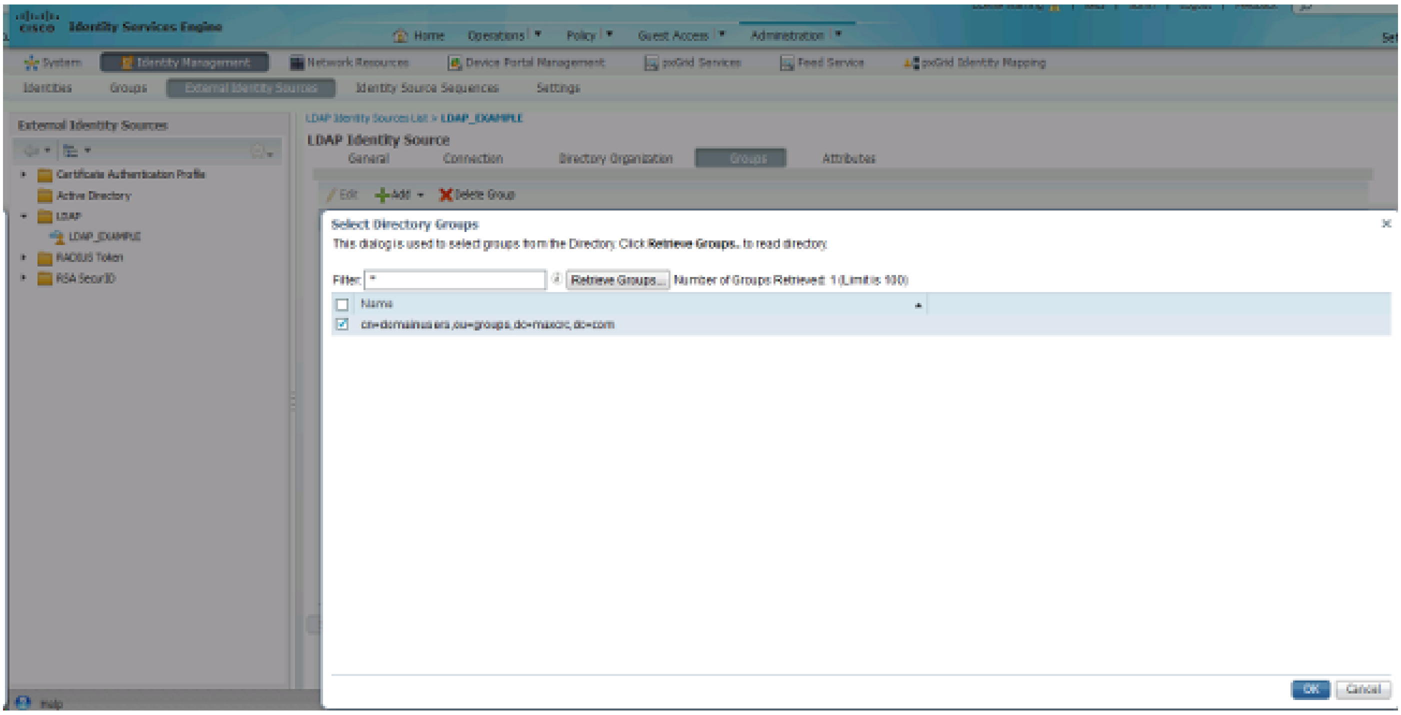
在下一個頁籤中，配置主題/組搜尋庫。這是ISE到LDAP的連線點。您只能檢索作為加入點子項的主題和組。

在此方案中，將檢索OU=people中的主題和OU=groups中的組：



* 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	

在Groups頁籤中，您可以從ISE上的LDAP匯入組：



Select Directory Groups

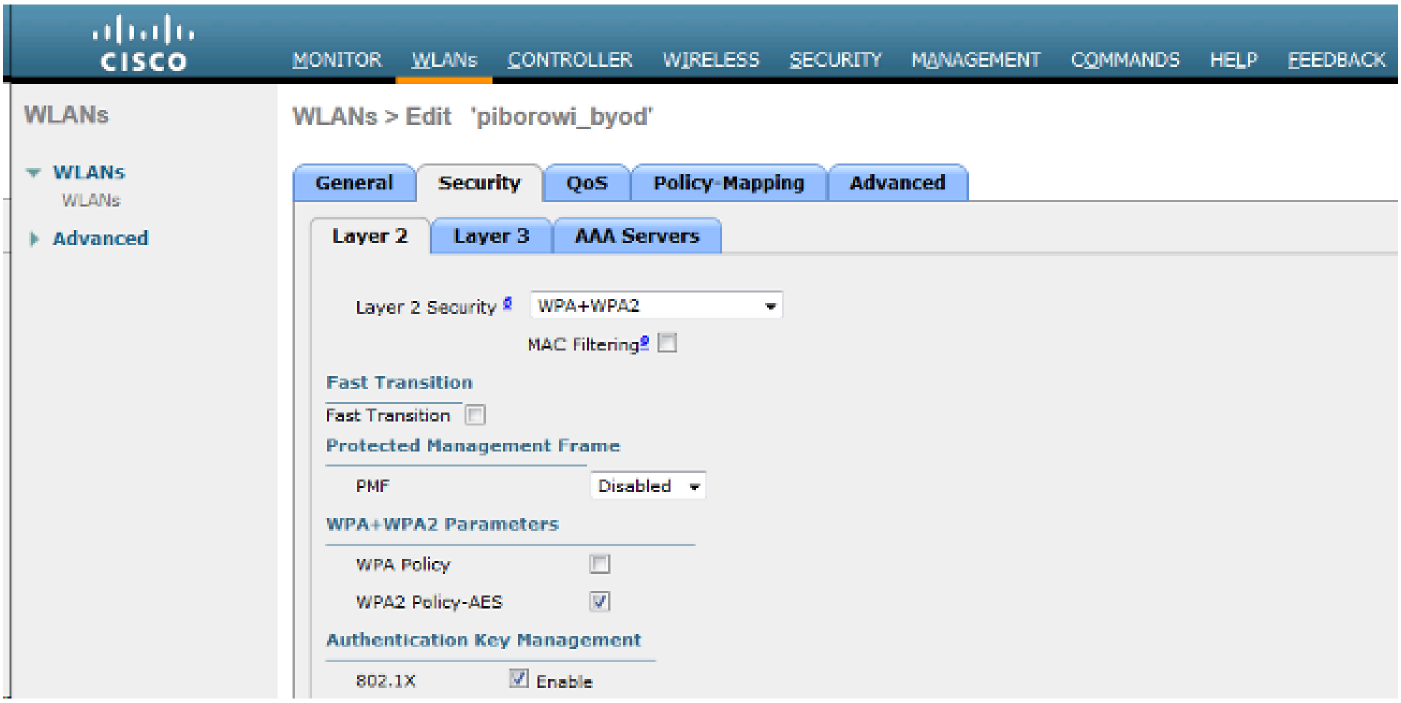
This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.

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

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

設定WLC

使用這些映像中提供的資訊來設定WLC以進行802.1x驗證：



WLANs > Edit 'piborowi_byod'

Layer 2 Security: WPA+WPA2

MAC Filtering □

Fast Transition

Fast Transition □

Protected Management Frame

PMF: Disabled

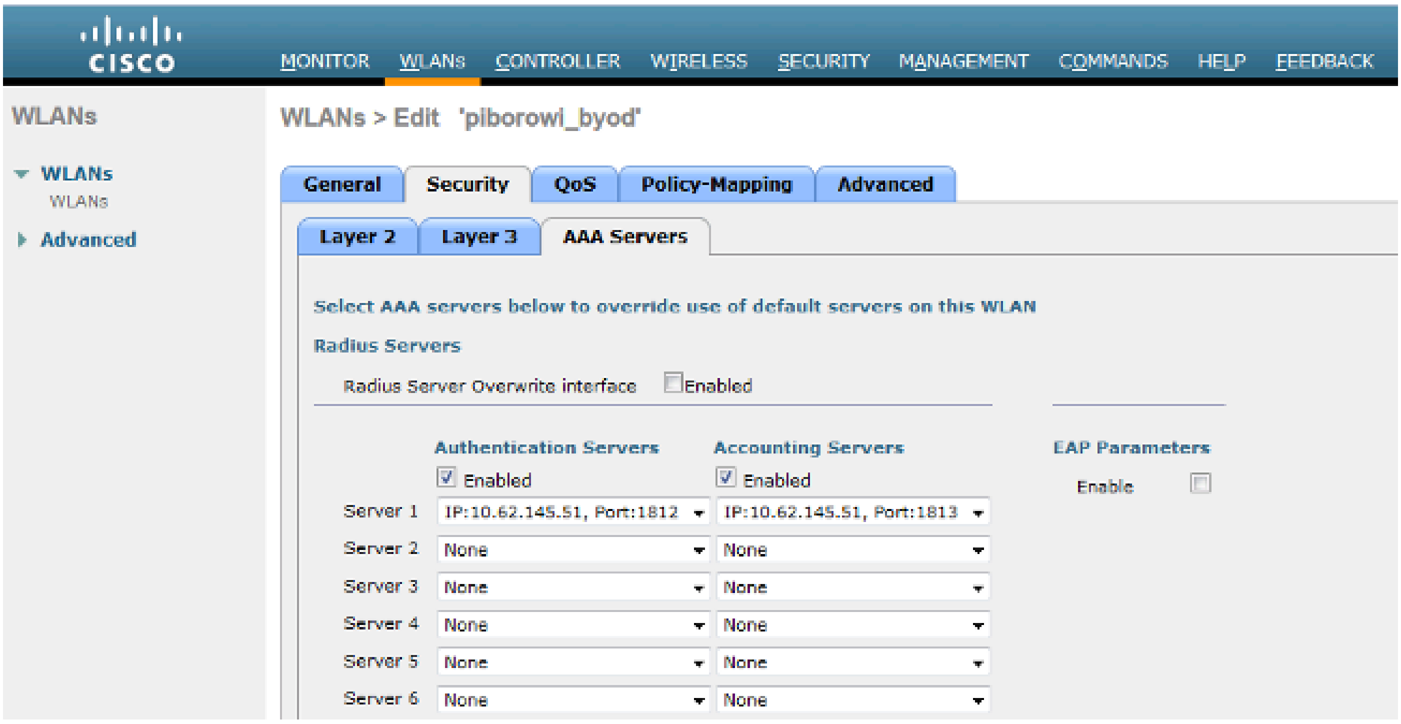
WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy-AES ☑

Authentication Key Management

802.1X ☑ Enable


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers

WLANs > Edit 'piborowi_byod'

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

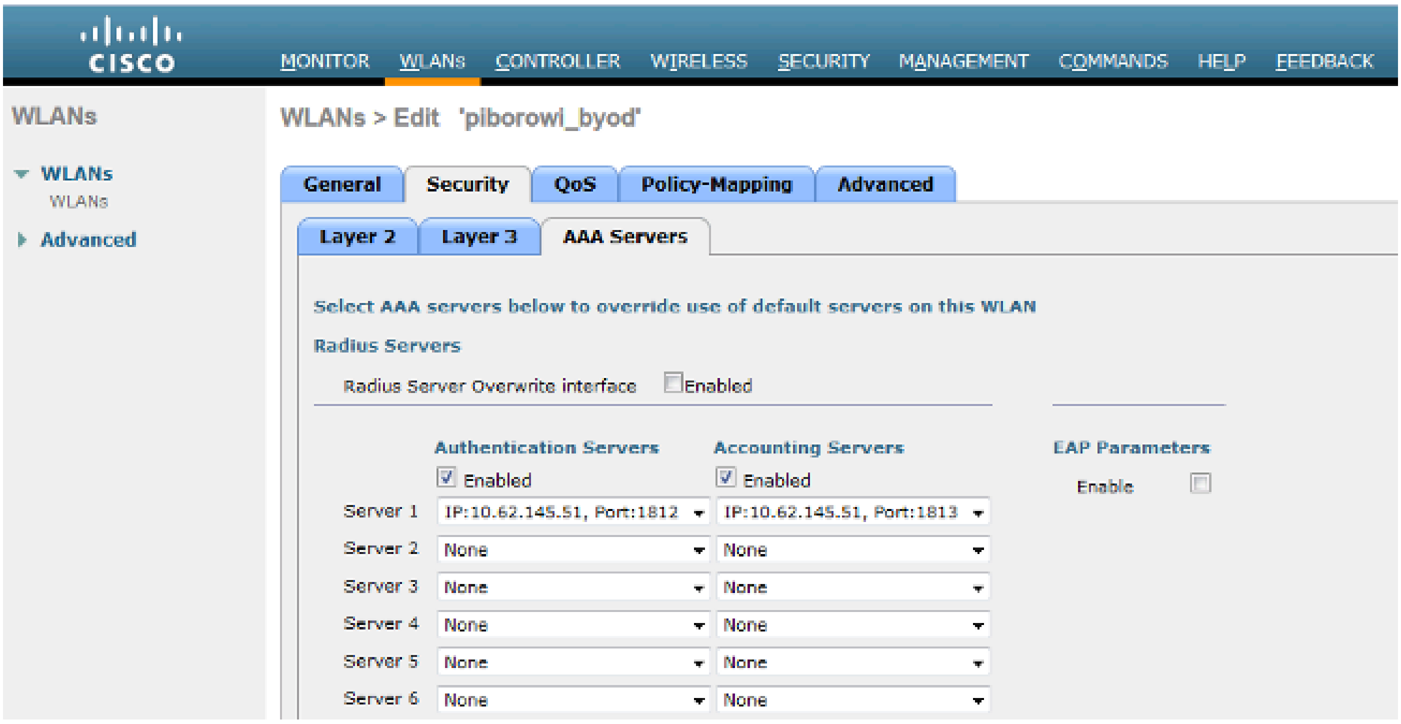
Radius Servers

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 □

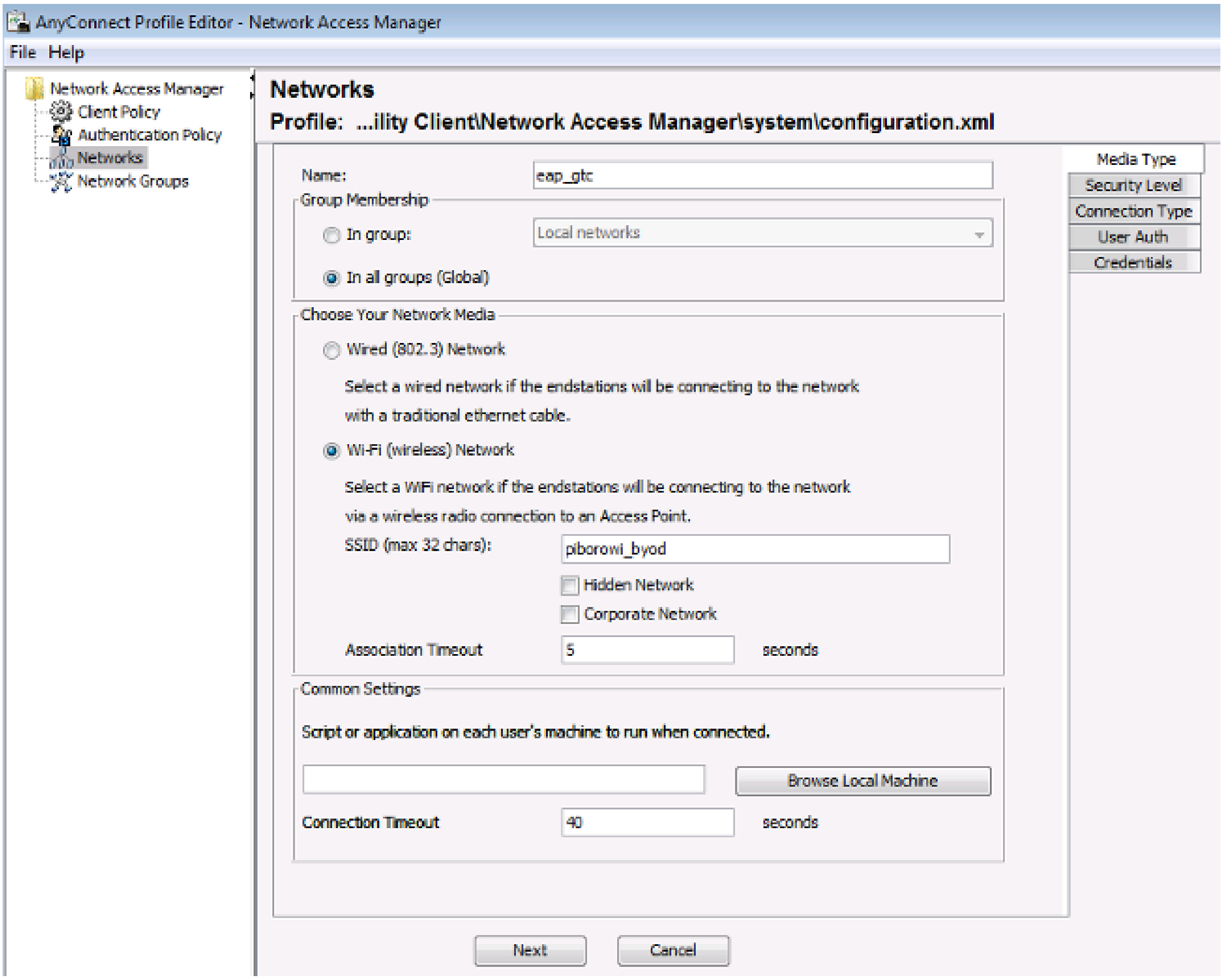
配置EAP-GTC

LDAP支援的身份驗證方法之一是EAP-GTC。它在Cisco AnyConnect中可用，但必須安裝網路訪問管理器配置檔案編輯器才能正確配置配置檔案。

您還必須編輯網路訪問管理器配置，預設情況下該配置位於以下位置：

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

使用這些映像中提供的資訊在終端上配置EAP-GTC:



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

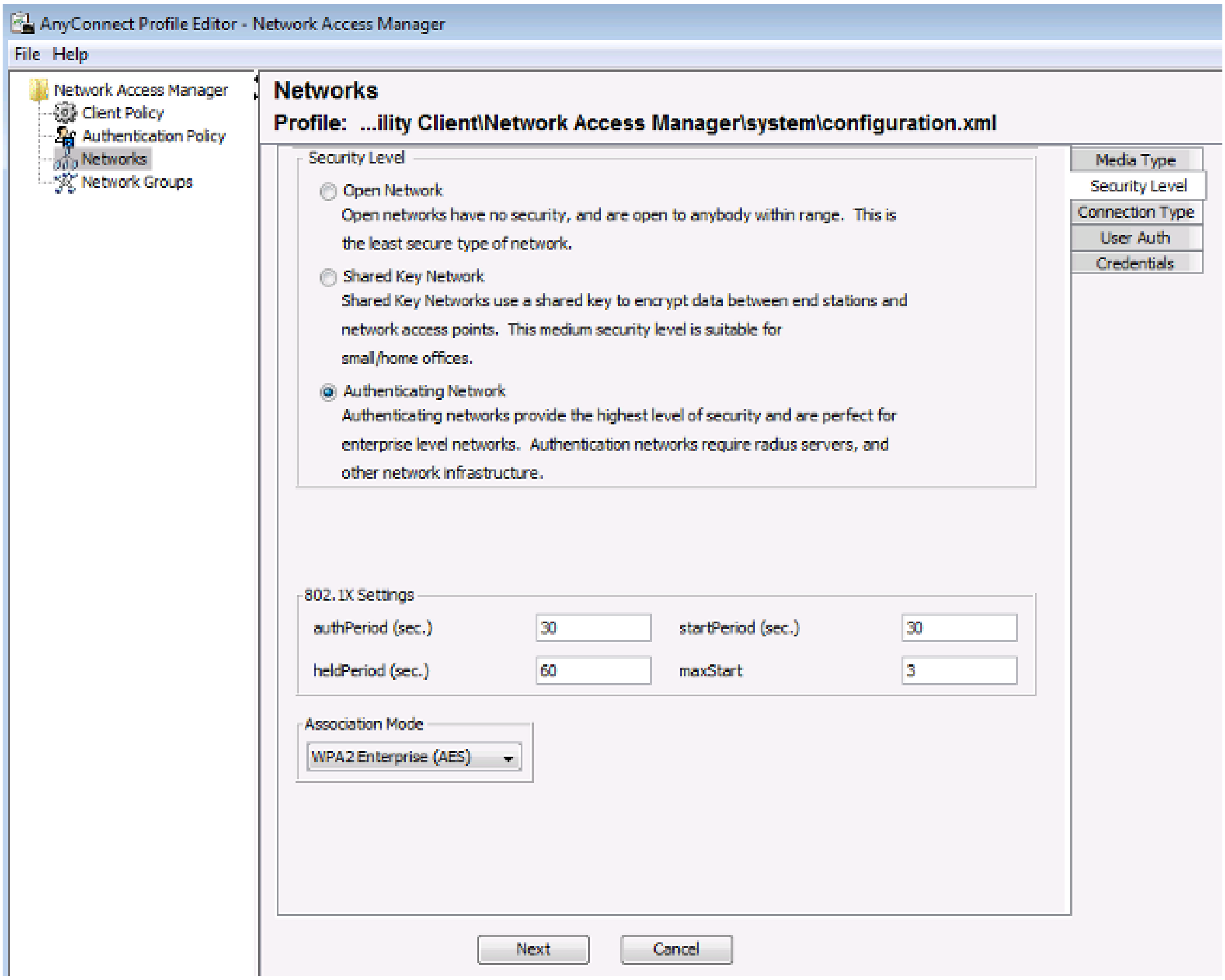
□ Corporate Network

Association Timeout 5 seconds

Common Settings

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

Connection Timeout 40 seconds



AnyConnect Profile Editor - Network Access Manager

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.

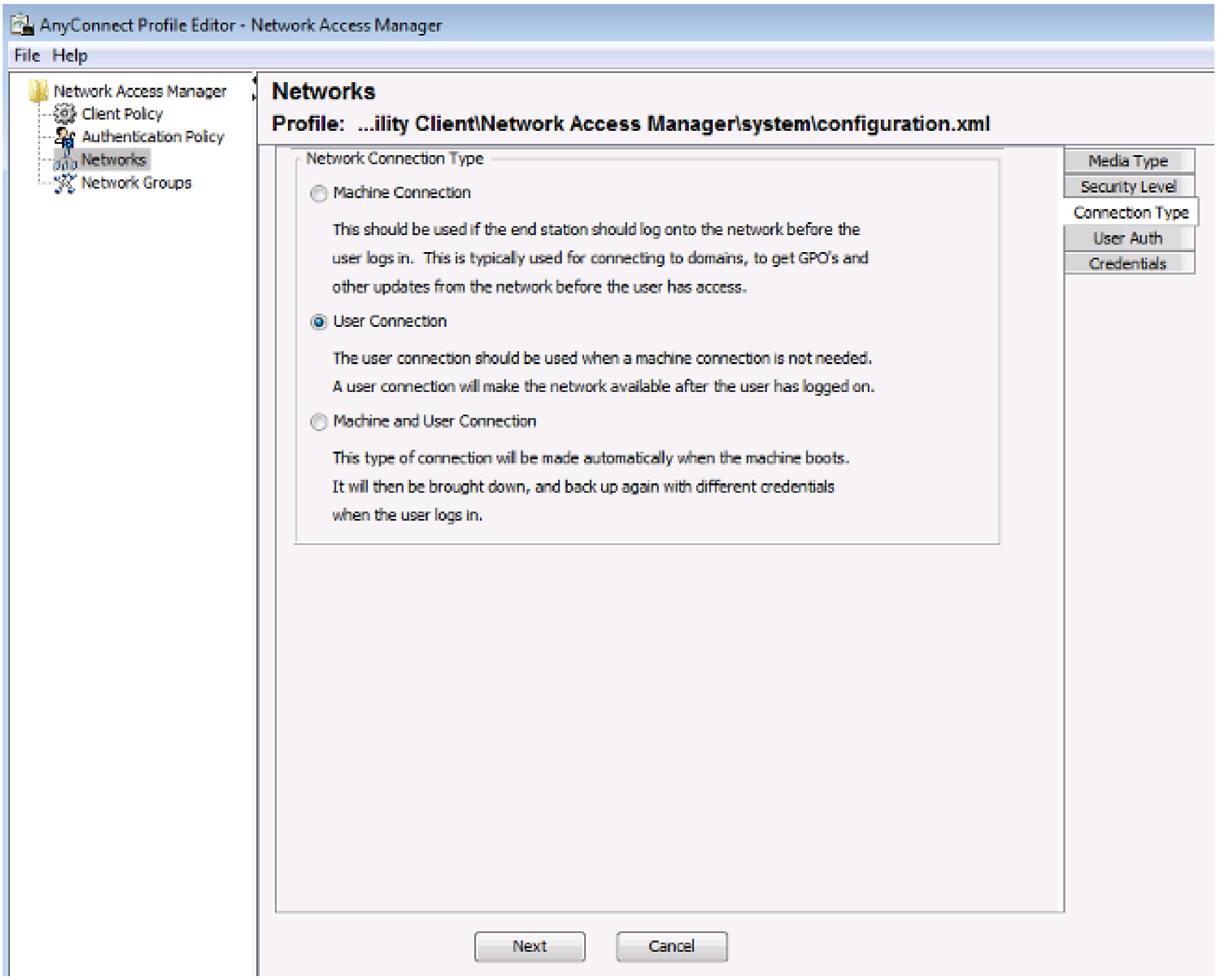
● Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

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

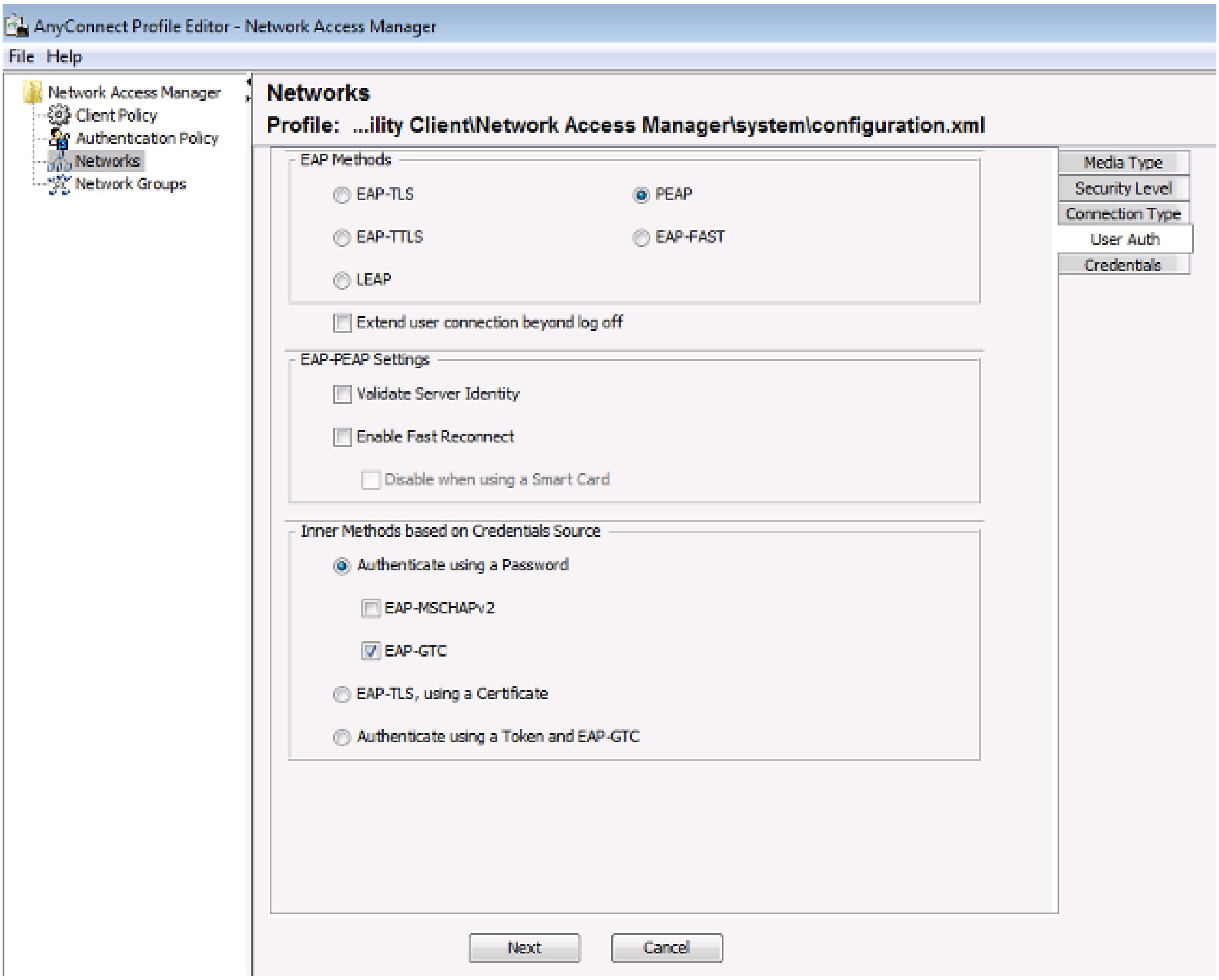
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.

● 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.



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

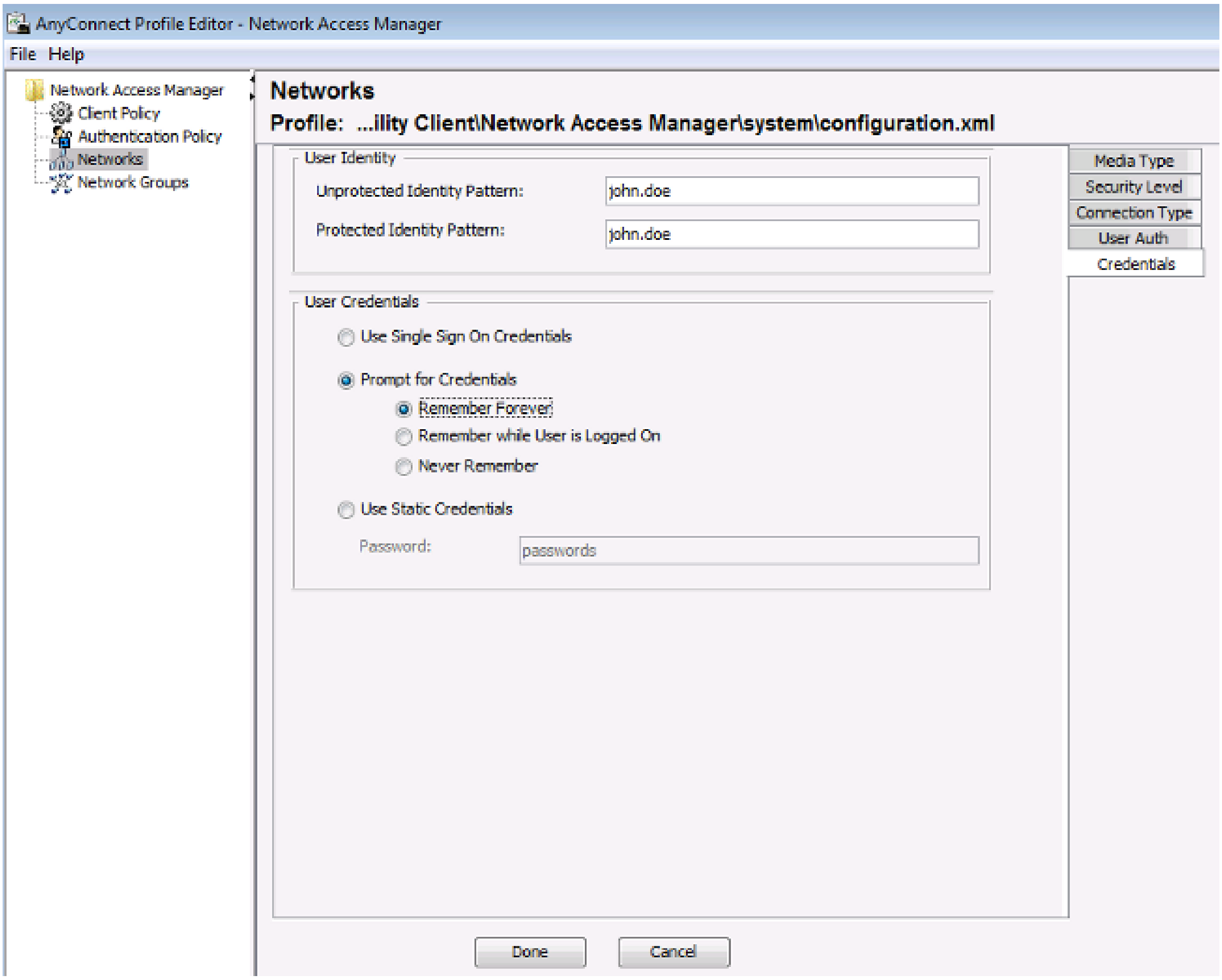
● Authenticate using a Password

□ 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

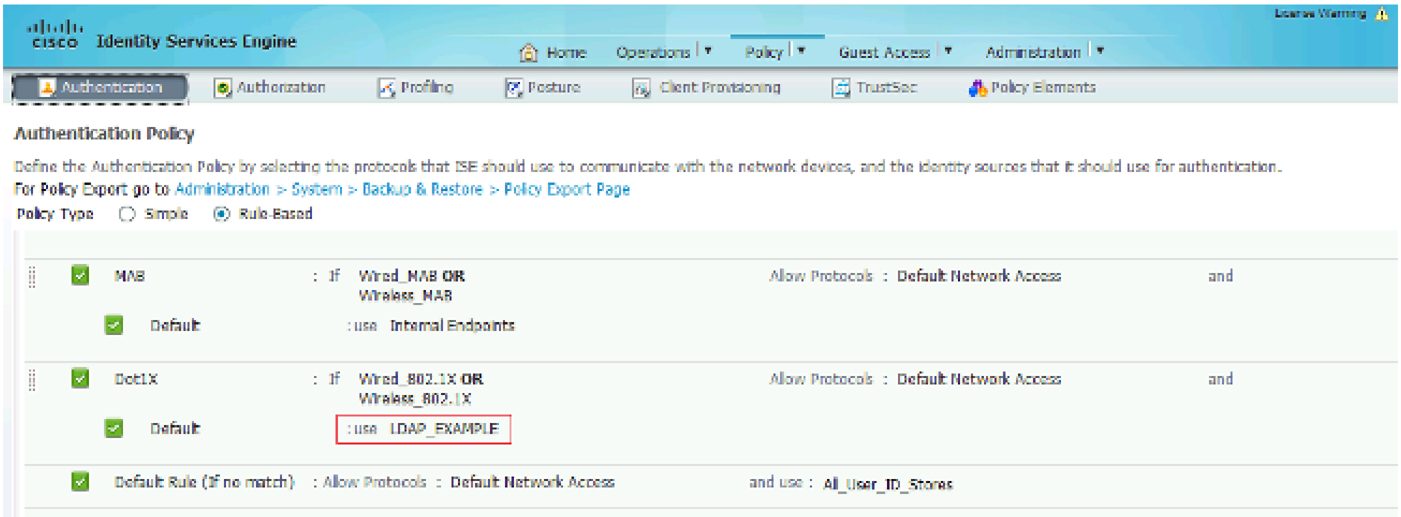
○ Remember while User is Logged On

○ Never Remember

○ Use Static Credentials

Password: passwords

使用這些映像中提供的資訊更改ISE上的身份驗證和授權策略：



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

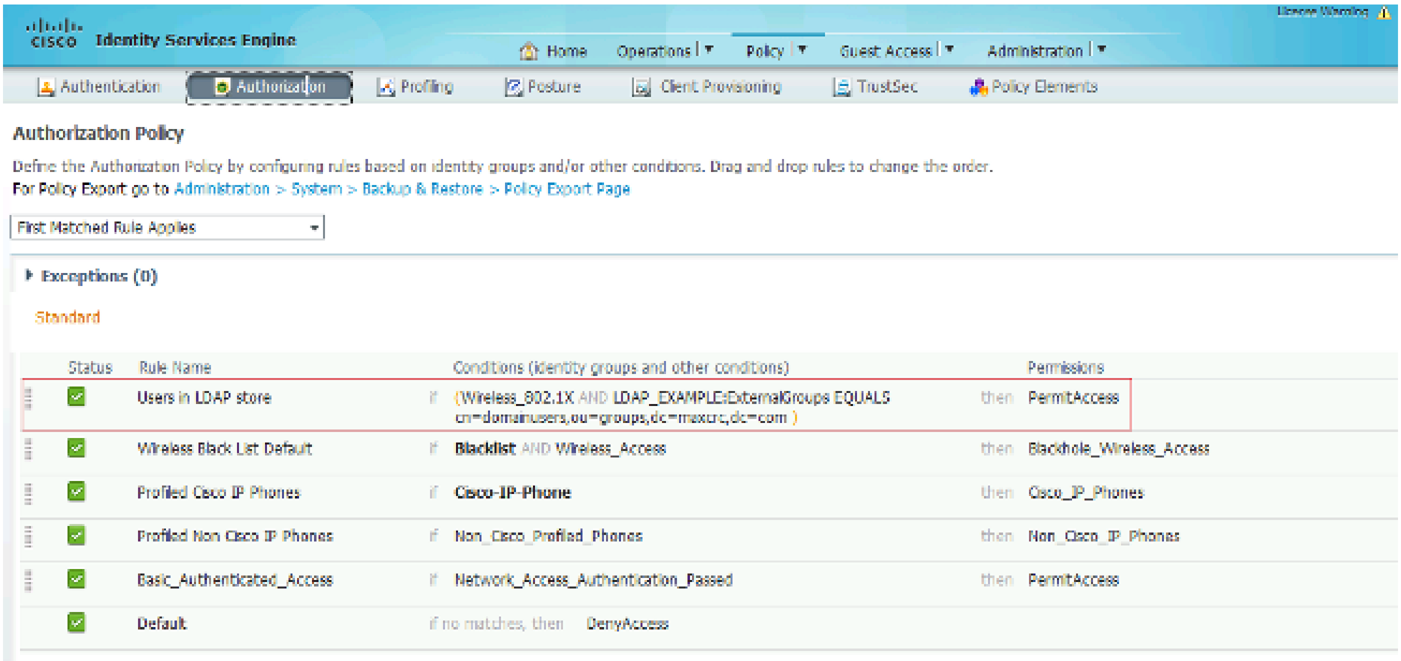
☑ MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and

☑ 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

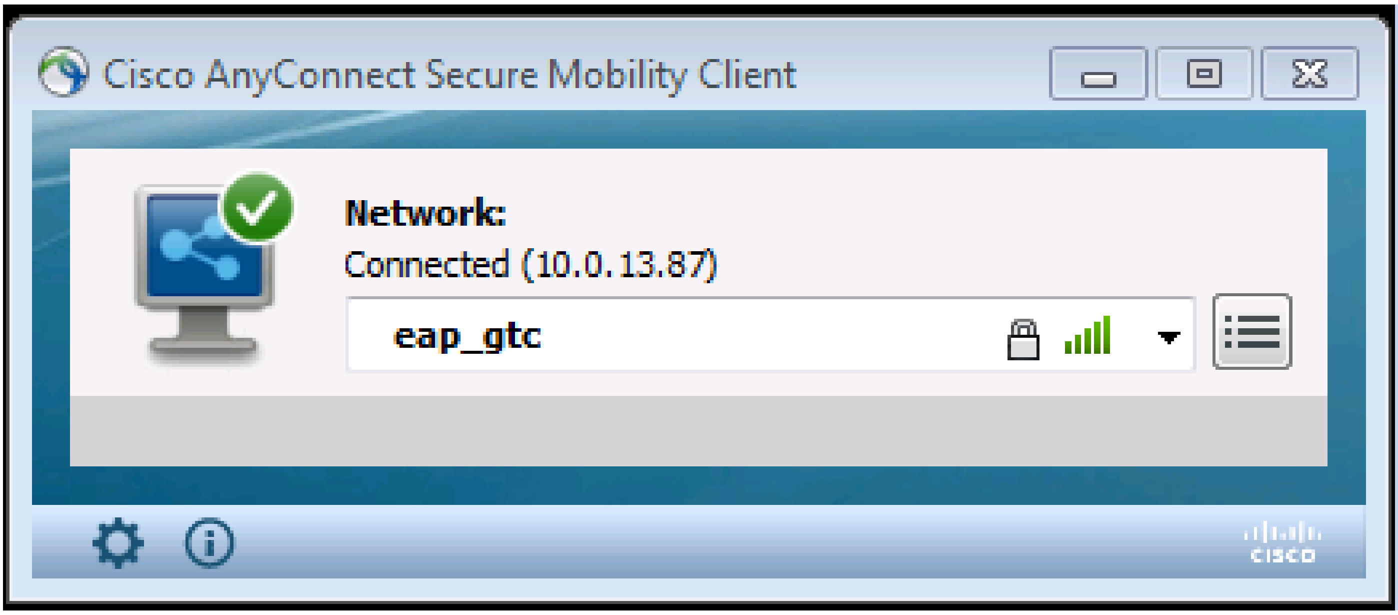
First Matched Rule Applies

Exceptions (0)

Standard

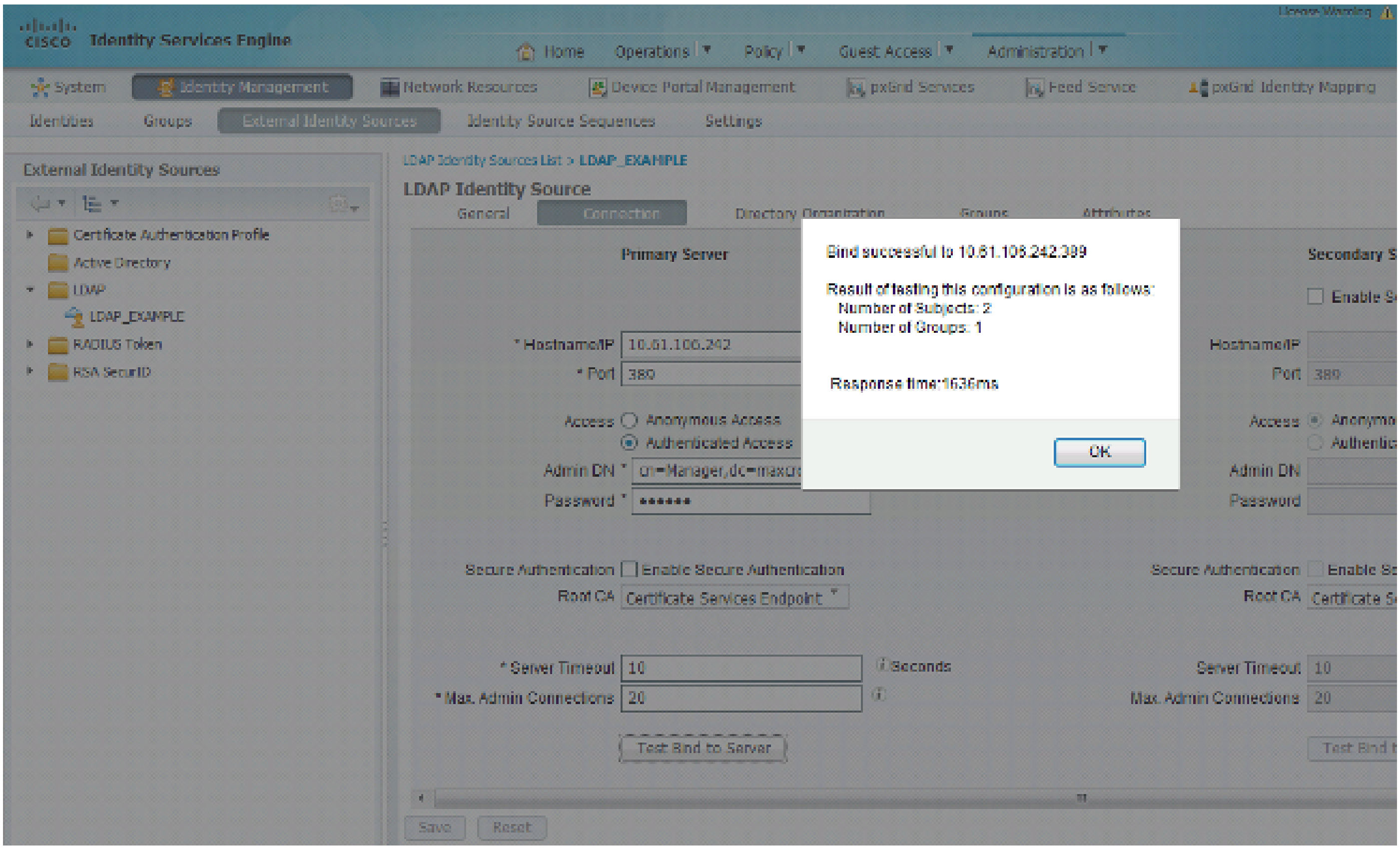
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	Users in LDAP store	if	(Wireless_802.1X AND LDAP_EXAMPLE:ExternalGroups EQUALS cn=domainusers,ou=groups,dc=maxrc,dc=com)	then	PermitAccess
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access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

套用組態後，您應該能連線到網路：



驗證

為了驗證LDAP和ISE配置，請檢索與伺服器具有測試連線的主題和組：



LDAP Identity Source

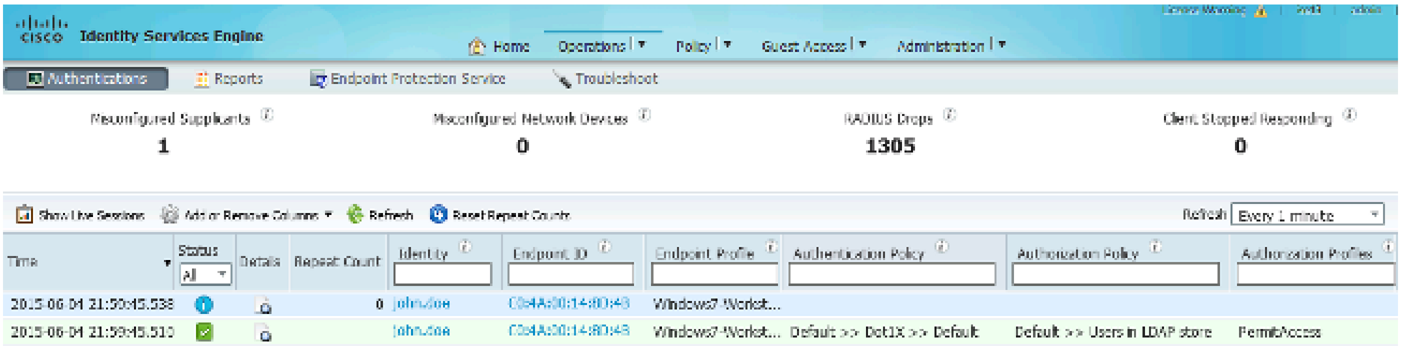
Bind successful to 10.61.106.242:389

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

Response time:1636ms

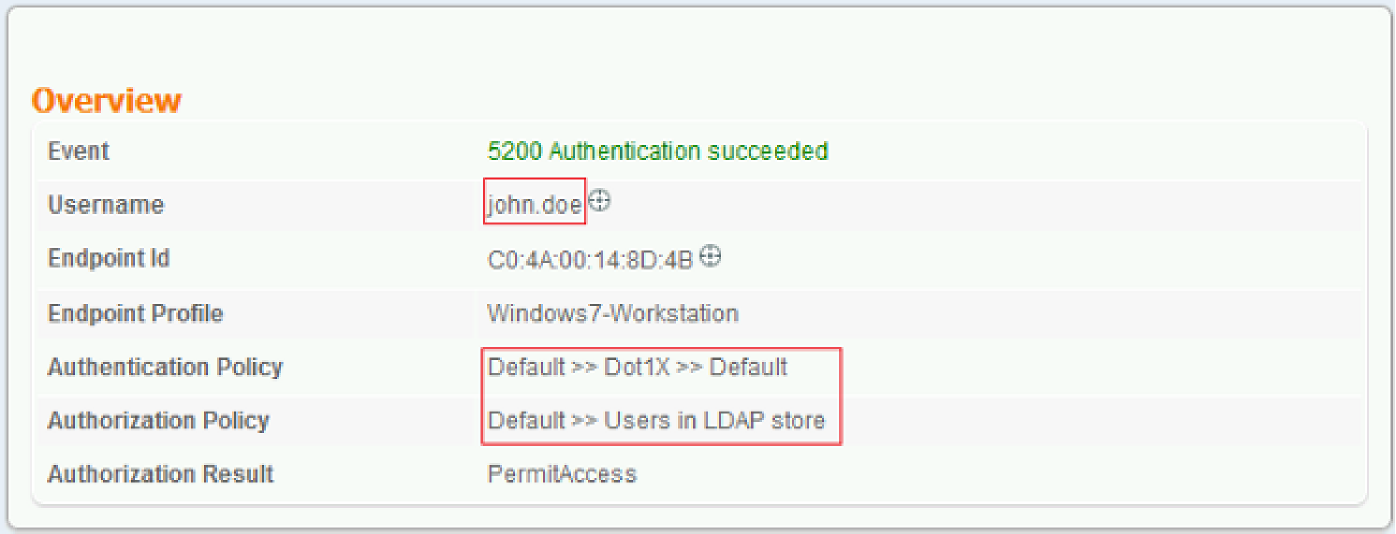
* Hostname/IP	10.61.106.242
* Port	389
Access	○ Anonymous Access ● Authenticated Access
Admin DN *	cn=Manager,dc=maxcr
Password *	●●●●●●
Secure Authentication	□ Enable Secure Authentication
Root CA	Certificate Services Endpoint
* Server Timeout	10 Seconds
* Max. Admin Connections	20

以下影象說明來自ISE的示例報告：



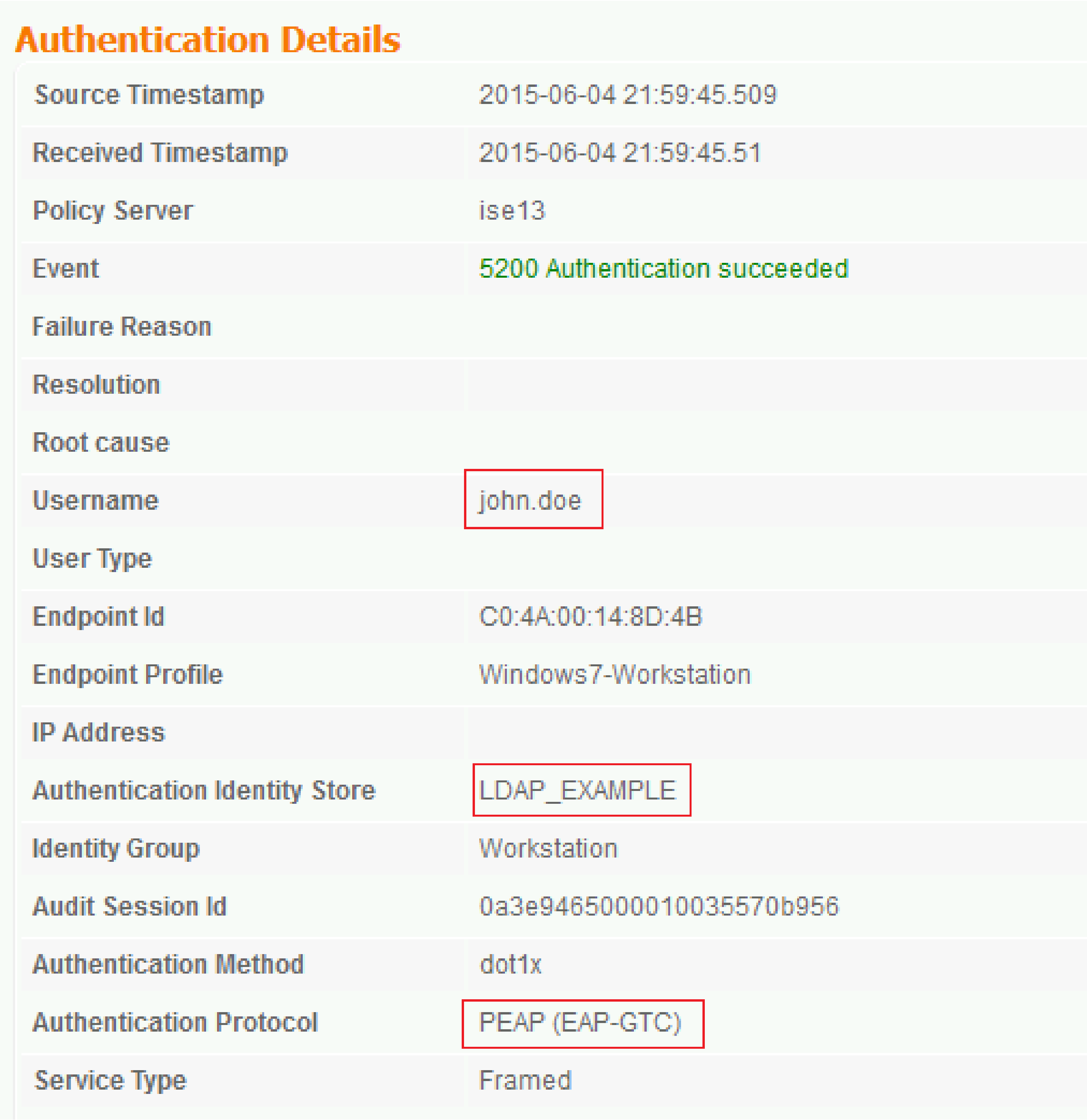
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding
1	0	1305	0

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2015-06-04 21:50:45.538	ⓘ		0	john.doe	C0:4A:00:14:8D:4B	Windows7-Workst...			
2015-06-04 21:50:45.510	✓			john.doe	C0:4A:00:14:8D:4B	Windows7-Workst...	Default >> Dot1X >> Default	Default >> Users in LDAP store	PermitAccess



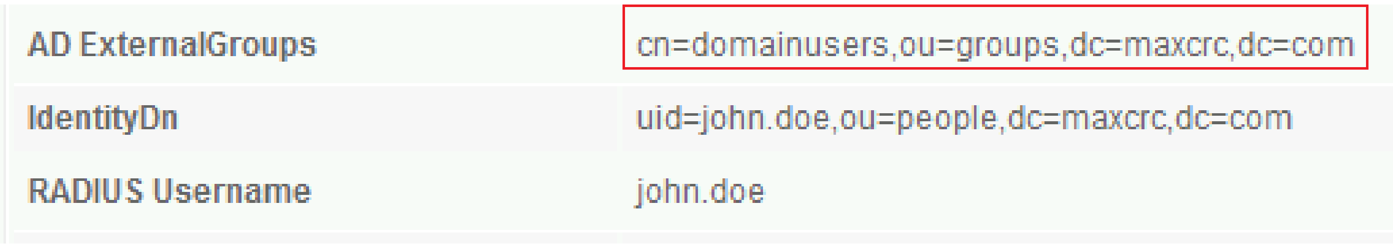
Overview

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

疑難排解

本節介紹此設定遇到的一些常見錯誤以及如何進行疑難排解：

- 安裝OpenLDAP後，如果您遇到錯誤指示gssapi.dll丟失，請重新啟動Microsoft Windows。
- 可能無法直接編輯Cisco AnyConnect的configuration.xml檔案。將新配置儲存到其他位置，然後使用它替換舊檔案。
- 在驗證報告中，出現以下錯誤消息：

  <#root>

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

  此錯誤消息表明LDAP不支援您選擇的方法。

確保同一報告中的身份驗證協定顯示其中一個受支援的方法（EAP-GTC、EAP-TLS或PEAP-TLS）。

- 在身份驗證報告中，如果您注意到在身份儲存中找不到主題，則報告中的使用者名稱與LDAP資料庫中任何使用者的主題名稱屬性不匹配。

在此方案中，此屬性值設定為uid，這意味著ISE在嘗試查詢匹配項時查詢LDAP使用者的uid值。

- 如果在繫結到伺服器測試期間未正確檢索到主題和組，則搜尋庫的配置不正確。

請記住，必須從枝葉到根和dc（可包含多個單詞）指定LDAP層次結構。

提示：若要對WLC端的EAP身份驗證進行故障排除，請參閱使用WLAN控制器(WLC)的EAP身份驗證配置示例思科文檔。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。