

# LDAP مداخل عم لمكتل ل ISE نيوكت

## تايوت حمل

---

[عمدق مل](#)

[ةيساس أال تابل طتم مل](#)

[تابل طتم مل](#)

[عمدختس مل تانوك مل](#)

[ةيساس أ تامول عم](#)

[نيوكت مل](#)

[ةكبش ل ل يطيطخت مل مسر مل](#)

[OpenLDAP نيوكت](#)

[ISE عم OpenLDAP حم](#)

[\(WLC\) ةكل لس ال ةل حمل ةكبش ل ل ف مكحت مل رصنع نيوكت](#)

[EAP-GTC نيوكت](#)

[ةحص مل نم ققحت مل](#)

[اهل صاوا عا طخ أال فاشك تس](#)

---

## عمدق مل

مداخ عم لمكتل ل Cisco نم (ISE) ةيوه ل تامدخ كرحم نيوكت ةيفي ك دن تس مل اذه فصي Cisco LDAP.

## ةيساس أال تابل طتم مل

### تابل طتم مل

دنتس مل اذهل ةصاخ تابل طتم دجوت ال

### عمدختس مل تانوك مل

ةيلال ةيدام ل تانوك مل او حم اربل تارادص ل دن تس مل اذه ف ةدراول تامول عم مل دن تس:

- Cisco ISE رادص ل 1.3 عم 2 حي حصت عم
- Microsoft Windows OpenLDAP تي بثت عم 7 x64 رادص ل
- Cisco 8.0.100.0 رادص ل، Cisco نم (WLC) ةكل لس ال LAN ةكبش ل ف مكحت ل ةدحو
- Cisco AnyConnect، Microsoft Windows ل 3.1 رادص ل
- Cisco نم ةكبش ل ل ل لوصول ريدم في رعت فلم ررحم

✎ **تجربا لآ ؤي وهال رءصمك LDAP مءءءسء ءءللا ءاوءالل ءلاص ءنءسمل اءه: ؤءءالم اءب صاءل لضءفءللا ؤ ؤءصم ل**

ءصا ؤءلم عم ؤئب ءف ؤءوءومل ؤزهال نم ءنءسمل اءه ءف ؤءراولل ءامل عملل ءاشنل مء ءنلك اءل. (ءضارءفا) ءوسمم نءوكءب ءنءسمل اءه ءف ؤمءءسمل ؤزهال ءءمء ءءب رمل ءل لمءءم لل رءءال لل كمهف نم ءكأءف، لءفءشءل ءءق كءكءبش

## ءءسسا ءامل عمل

LDAP عم ؤمءءم هءه ؤءصم لءبءل ساء:

- (EAP-GTC) ماعل ؤءممل ؤمزل ؤءاطب - عسوءم ل ؤءصم ل لوكوءورب
- (EAP-TLS) لقلل ؤءبء نامأ - عسوءم ل ؤءصم ل لوكوءورب
- (PEAP-TLS) لقلل ؤءبء نامأ - ءمءم ل عسوءم ل ؤءصم ل لوكوءورب

## نءوكءل

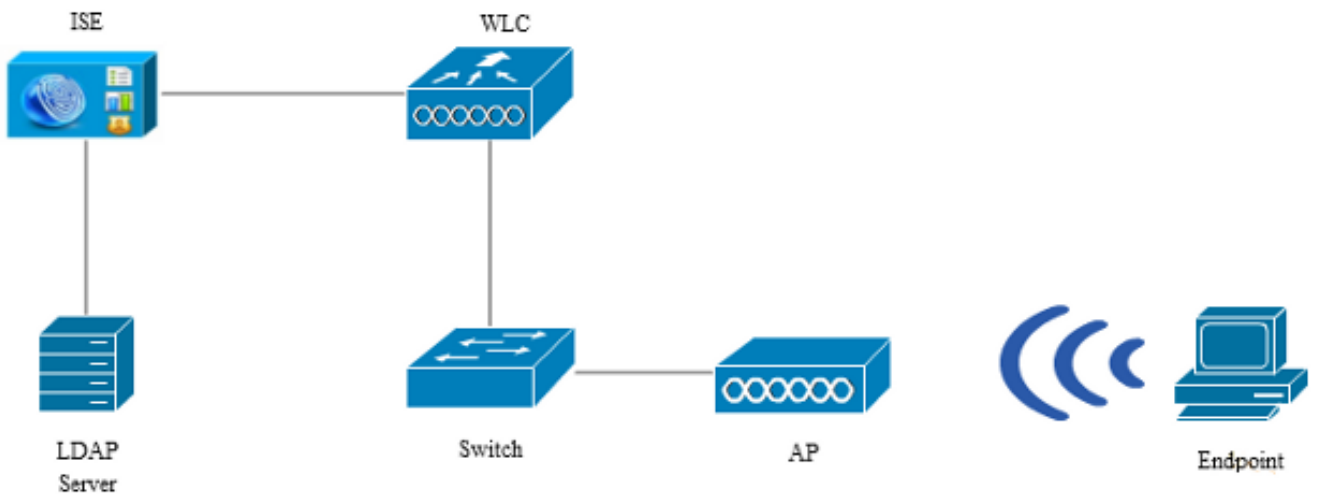
LDAP مءاء عم ISE ءمءوء ؤءبش ل ؤزهال نءوكء ؤءفءك مسقلل اءه فصء

## ءءبش ل لءطءءل مسرل

ءءبش ل لء نارئال ل ؤل سالل لوءم ؤءاه نل ؤءقن مءءءسء، اءه نءوكءل لاءم ءف ؤءل سالل.

ISE ل ؤءرء نع لمءءسمل ءقءاص ءل WLC ل ؤل ؤل (WLAN) ؤل سالل LAN ل ءل ؤل ءف ءءرا ؤءه نءءمك LDAP نءوكء مء، ISE ءف

هءاءءس ل مءء ءل ؤل ؤءبش ل لءطءم ؤرءص ل اءه ءضوء



## OpenLDAP نءوكء

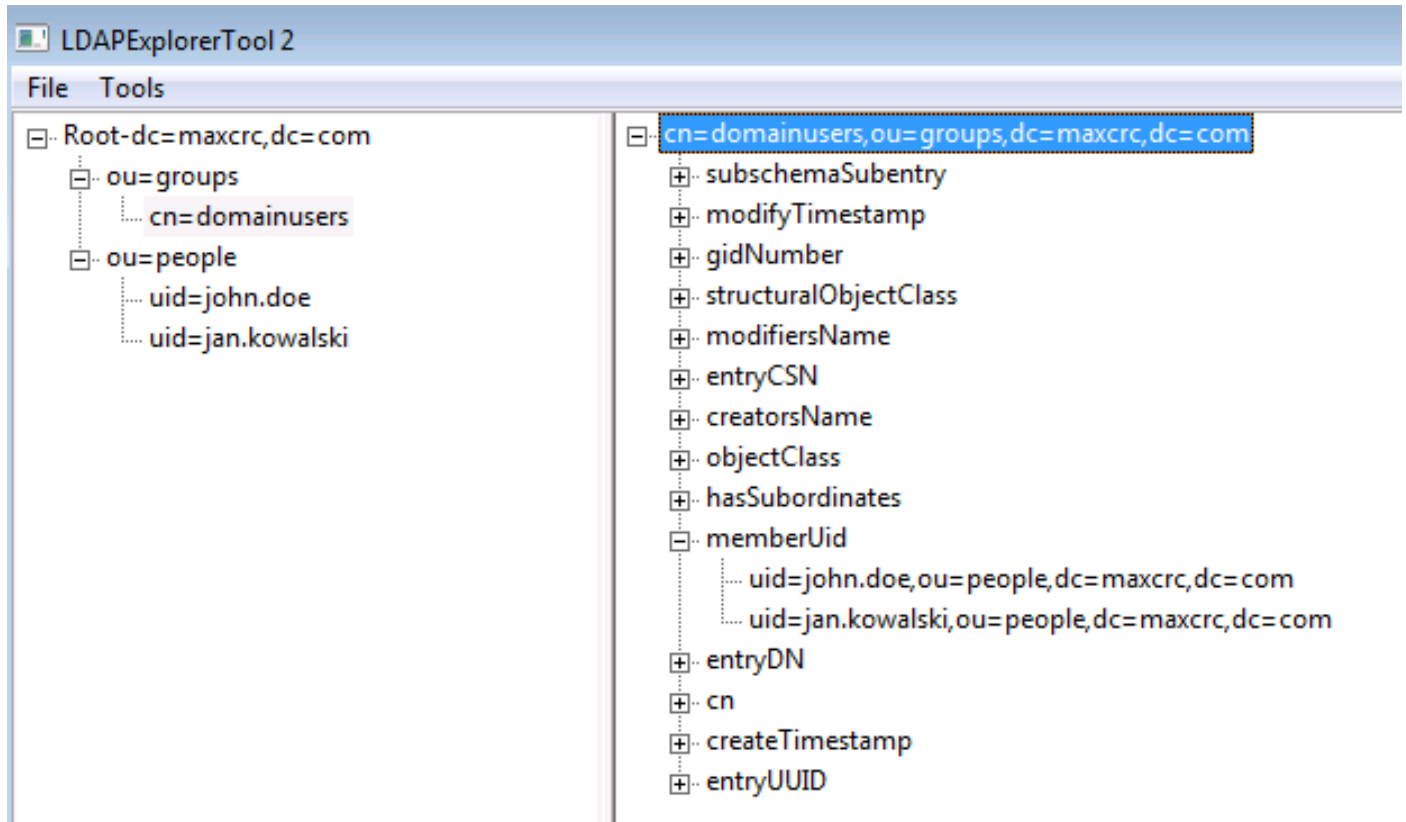
(GUI)، مدموسرلا مدختسمل اةءاو لالء نم Microsoft Windows ل OpenLDAP تيبثت لم تءك اءه ىرت نأ بءي، تيبثتل اءءب C: > OpenLDAP. وه ىضارتفال اءءومل. ءرشابم وءءضاو ىه و لىلءل:

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
slapd.exe	5/11/2015 10:59 PM	Application	3,711 KB

صوصءلل هءو ىلء نىلءلءب املء ءءالء:

- ClientTools - نمضتى اءه نمضتى - ClientTools
- ldifdata - اءه - ldifdata

LDAP: تانايب ةدعاق ىل لكةهل اذه ةفاضل



تحت OU=groups OU يوتحت نأ بجي (OUs) ني تي سسؤم ني تدحو ني وك ت بجي ، رذجل ليل دلل تحت (لثمل اذه ف cn=domainUsers ةدحاو ةي عرف ةومجم ىل

cn=domainUsers. ةومجم ىل ناي متني ني ذلل مدختسمل يباسح OU=people فرعت

نم اقباس ةروكذمل ةينبل ءاشنإ م. ال أو ldif فلم ءاشنإ كيلي بجي ، تانايب ال ةدعاق علم فللم اذه

```
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
```

LDAP، تانايي بةدعاق ىلإ تانئالكلا ةفاضلإ  
ldapmodify binary رمألإ مدختسأ

```
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"

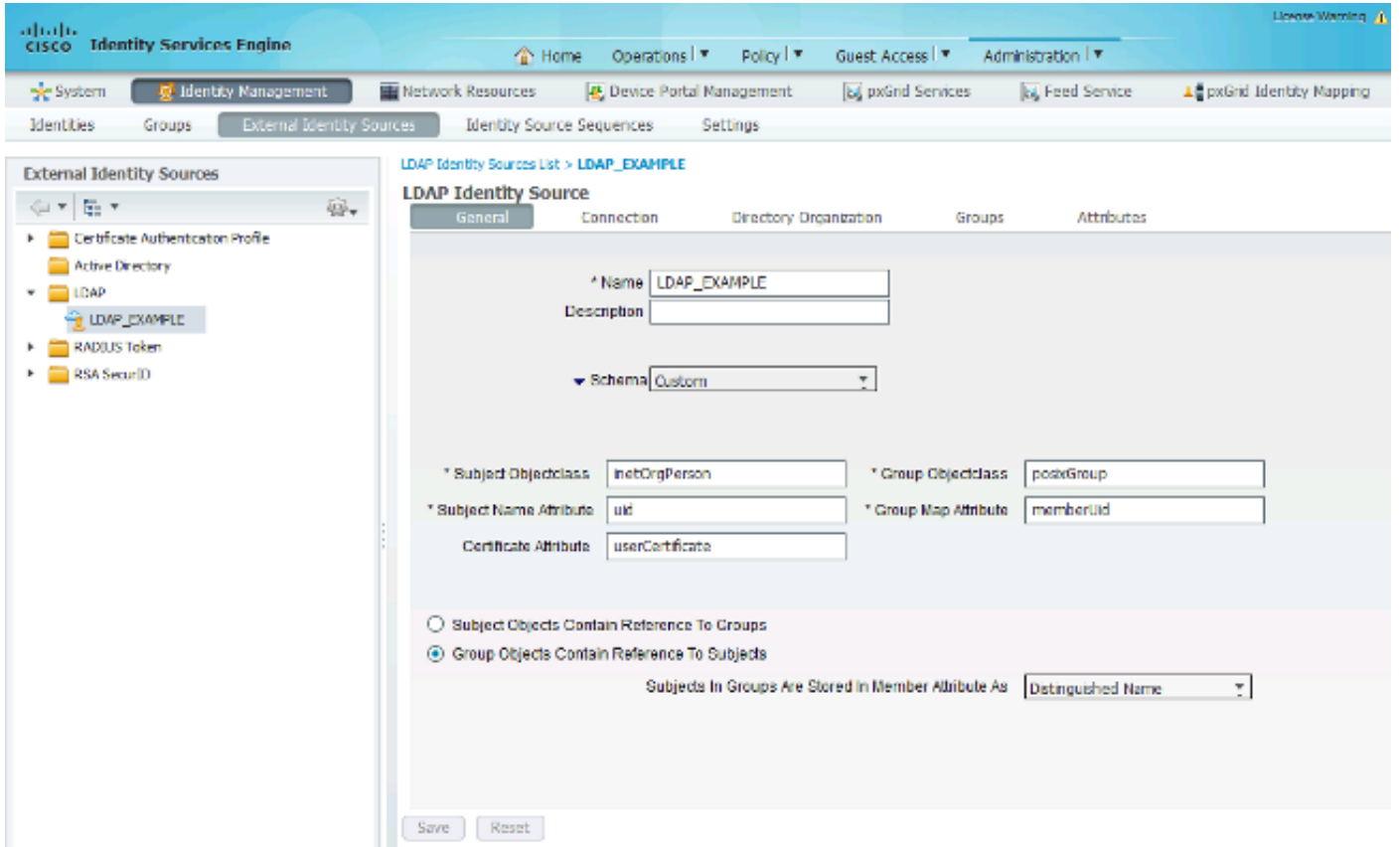
adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

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

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

## ISE م OpenLDAP جمرد

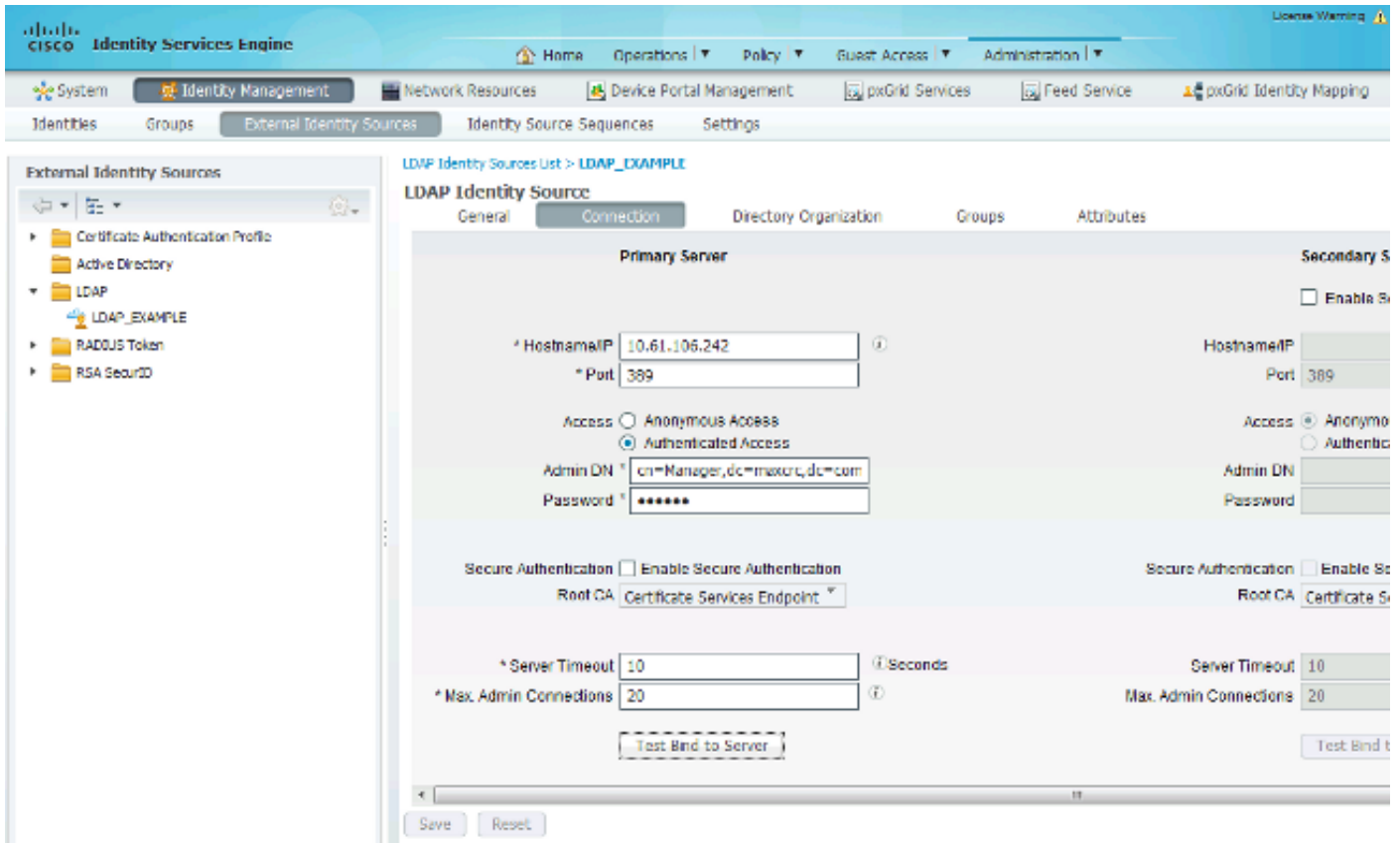
LDAP تلكش in order to مسق اذه لالخ نم روصلال ي ف تدوز نوكي نأ ةمولعملال تلمعتسا  
ISE. لال ىلع نزم ةيوهك



مراجع بيوتال الة ماع نم تامس ال هذه نيوكت كنكمي

- لقبط Idif فلم يف مدختسم ال تاباسحل نئالك الة ئف لقحل ال اذه لثاميف - SubjectClass  
عبرال تائف ال هذه نم دحاو مدختسأ LDAP نيوكتل
  - لىل
  - صخش
  - يمظنت فظوم
  - InetOrgPerson
- ام دنع LDAP ةطساوب اهدادرتسإ متي يتل الة مسل ال هه - عوضوم ال مس الة مس  
ف. ال ما تانايب ةدعاق يف نمضم ددحم مدختسم مس اكانه ناك اذا امع ISE رسفتسي  
ةطقن لىل مدختسم مس اك jan.kowalski و John.doe مادختسإ بجي، ويرانيس ال اذه  
الاهنل.
- اذه يف Idif فلم يف ةومجمل نئالك الة ئف لقحل ال اذه لثاميف - ObjectClass ةومجمل  
ال هه posixGroup يف ةومجمل نئالك الة ئف نوكت، ويرانيس ال
- اةومجمل ال لىل ني مدختسم ال ني عت ةيفيكة مسل ال هذه دحت - ةومجمل ال ططخم ةمس  
memberUid نانثا تي ارعي طتسي تنأ، دربم ال Idif ال يف ةومجمل cn=domainUsers ال تحت  
لمعتسم ال فداري نأ ةمس.

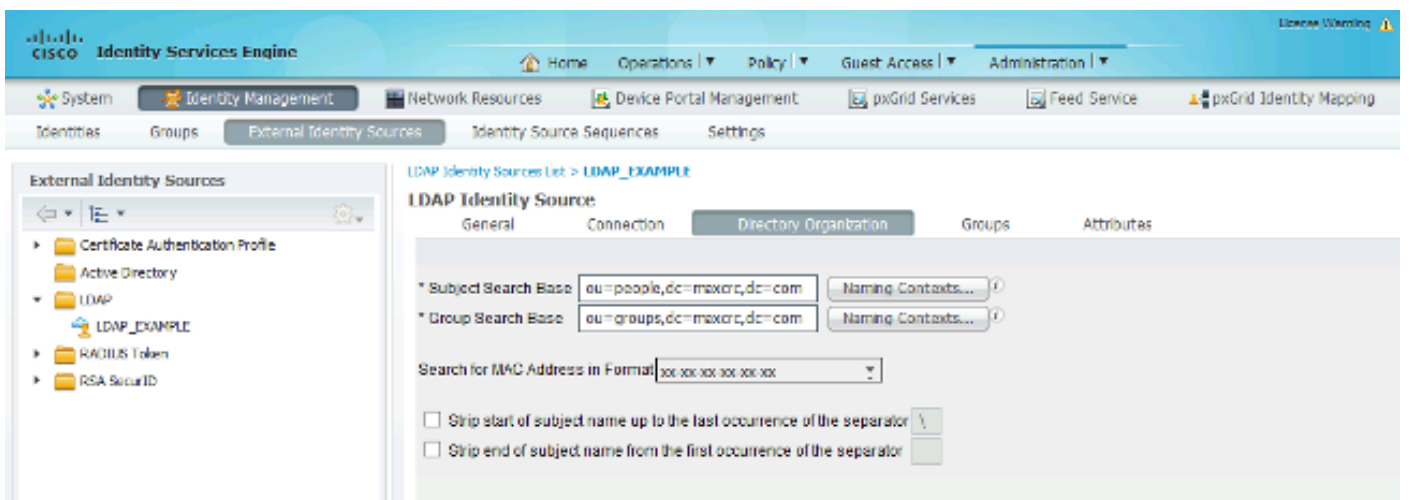
ال: (Microsoft Active Directory و Sun و Novell) لقبسم ةأيهم ال اةططخم ال ضعب ISE مدقي امك



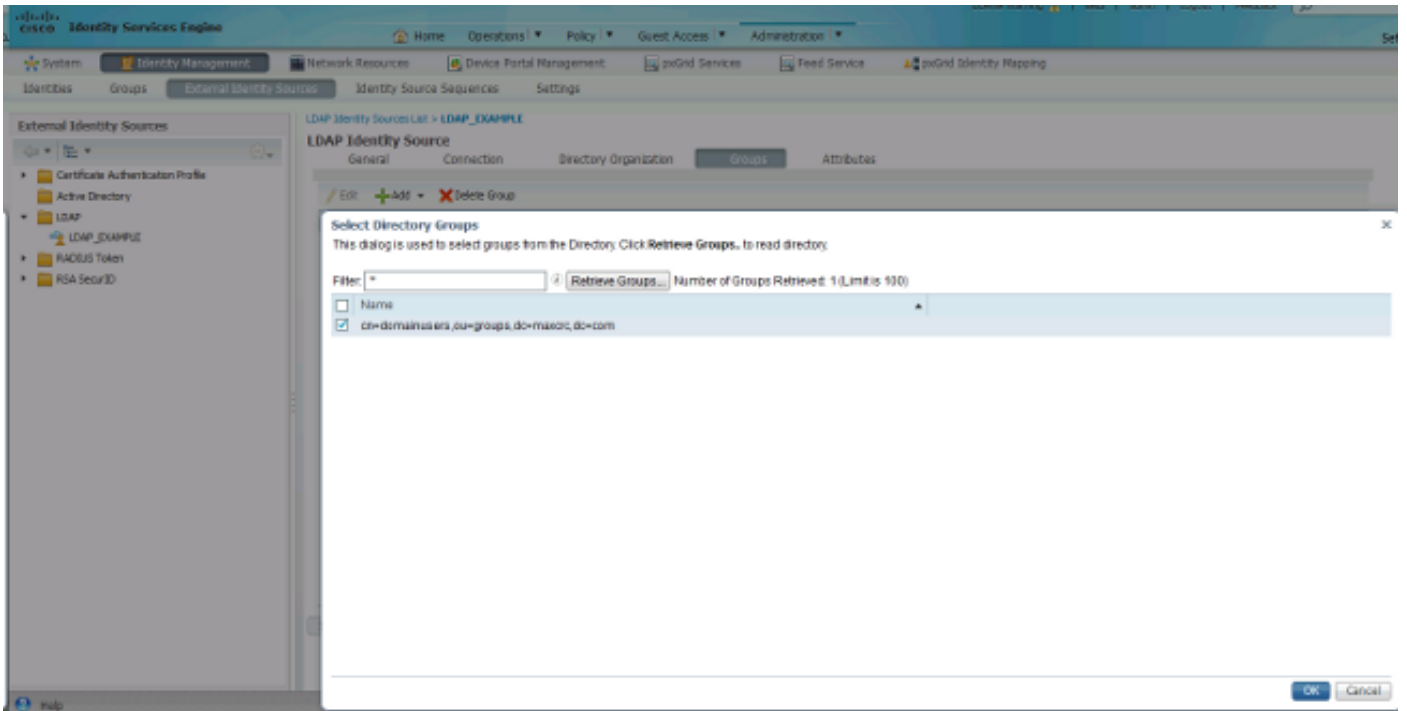
مداخل الـ LDAP إلى طبقات الخوادم، يراد إلّا لاجمالمس او حوصال الـ IP اونوع طبضب موقت نأ دع  
هناويوكت متي مل شحب الـ دعاوق نال تاوعومجم واعيضاوم يا دادرستس كنكمي ال، ةطقنل هذه دع  
دع.

ةطقنل هه. ةوعومجمال/عوضومل شحب ةدعاوق نيويوكتب مق، ةيلال الـ بيوبتال ةمالع يف  
ةطقنل الـ افطأ دع يال تاوعومجمال او تاوعوضومل دادرستس كنكمي الـ ISE لـ طببرال  
طقف كمامضنا.

تاوعومجم نم تاوعومجمال او OU=People نم تاوعوضومل دادرستس متي، ويرانيسل اذه يف  
OU=Groups:

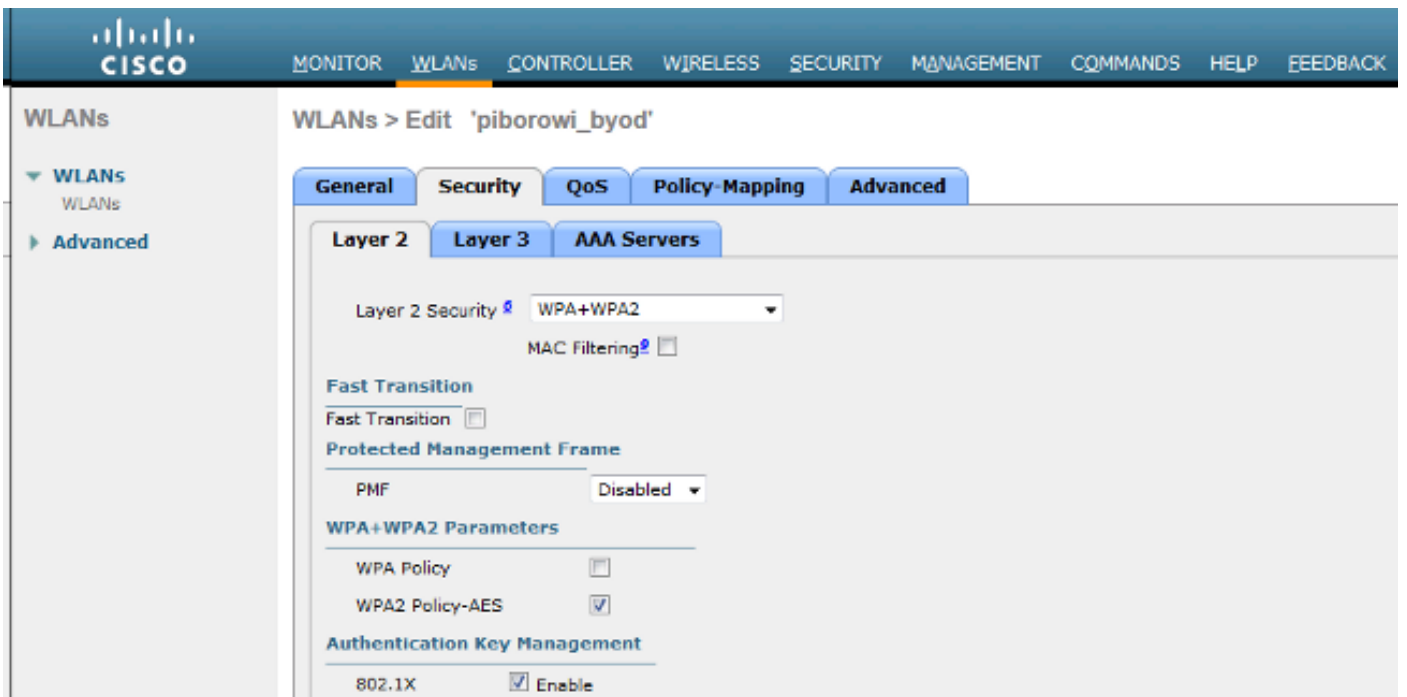


ISE الـ LDAP نم تاوعومجمال دادرستس كنكمي، تاوعومجم بيوبتال ةمالع نم



WLC) ةيكل سلال ةيكل حمل ةكبش لاي ف مكحت لارصنع نيوكت

ةيكل حمل ةكبش لاي ف مكحت لارصنع نيوكت لاروصل هذه يف ةمدقم لارمول عمل مدختسأ  
ةيكل سلال (WLC) ةقداصل 802.1x:







ةياهنلا ةطقن ىلع EAP-GTC نيوكتل روصلا هذه في ةمدقملا تامولعمل مدختسأ

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

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

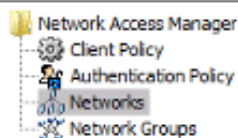
Association Timeout:  seconds

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



## 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

- 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

- 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

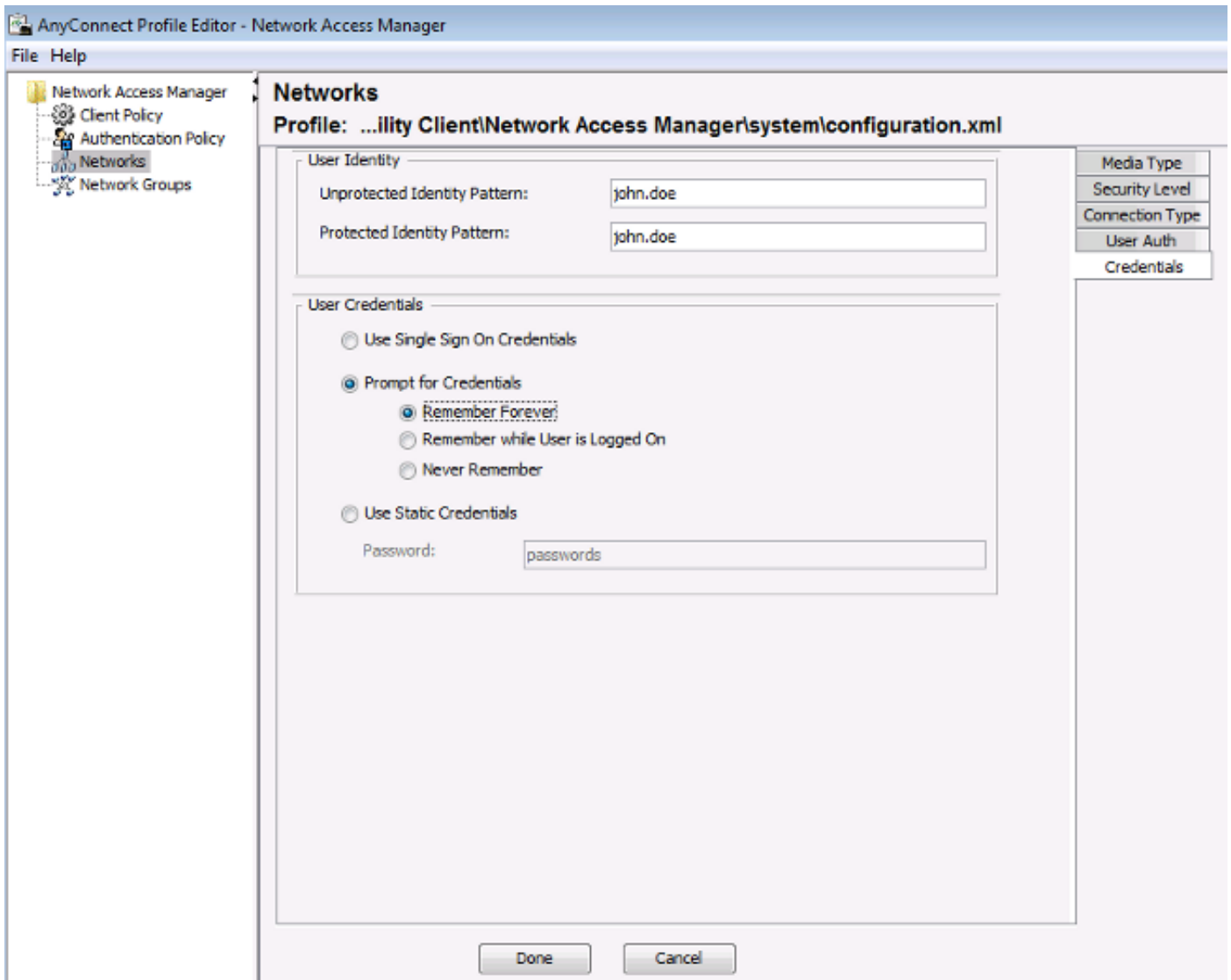
EAP-TLS, using a Certificate

Authenticate using a Token and EAP-GTC

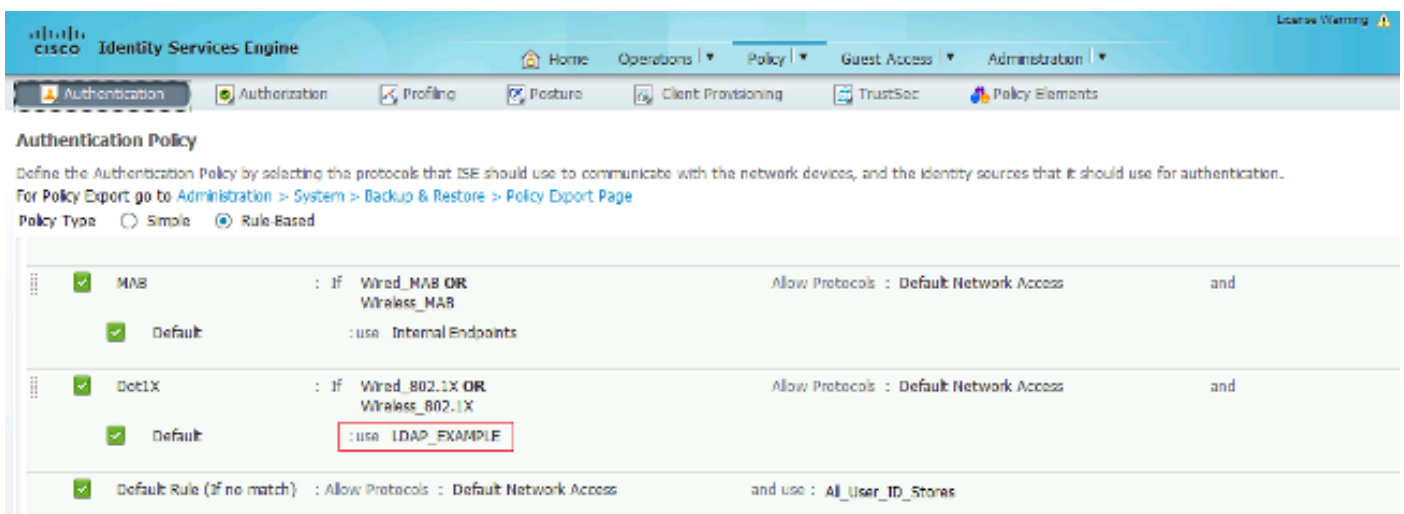
- Media Type
- Security Level
- Connection Type
- User Auth
- Credentials

Next

Cancel



لدى ضيوفت لاوة قداصلما تاسايس ريغتل روصلا هذه يف ةمدقملا تامولعمل مدختسا  
ISE:



**CISCO 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

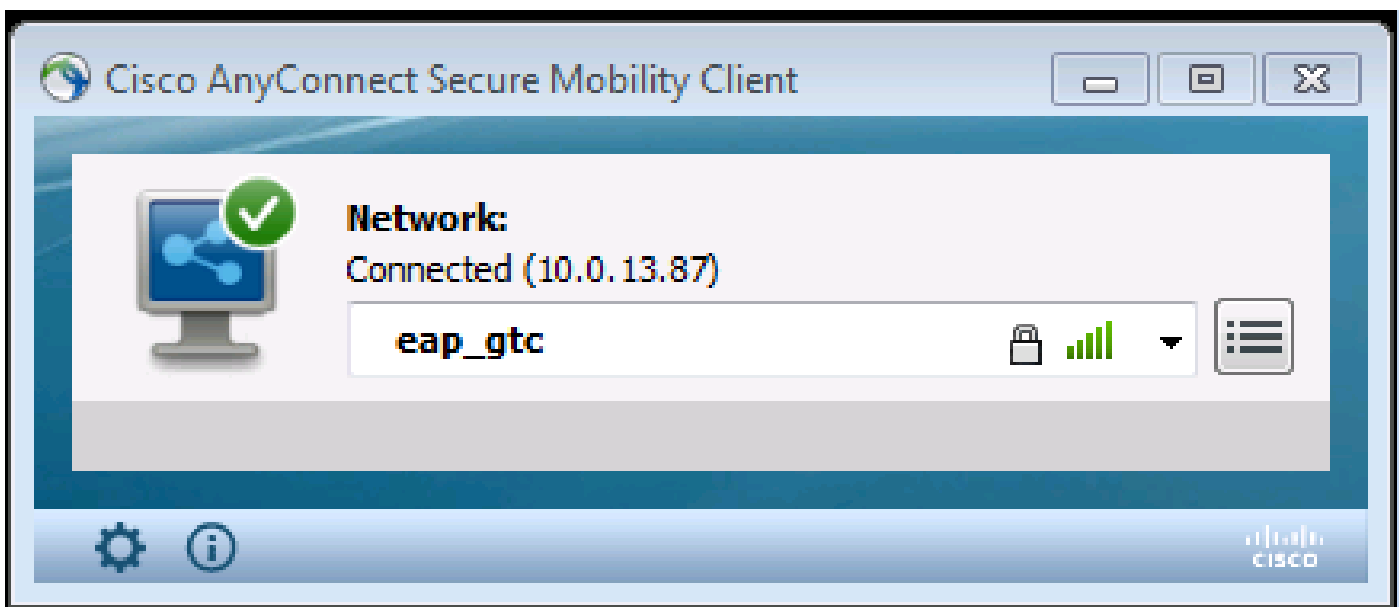
First Matched Rule Applies

Exceptions (0)

Standard

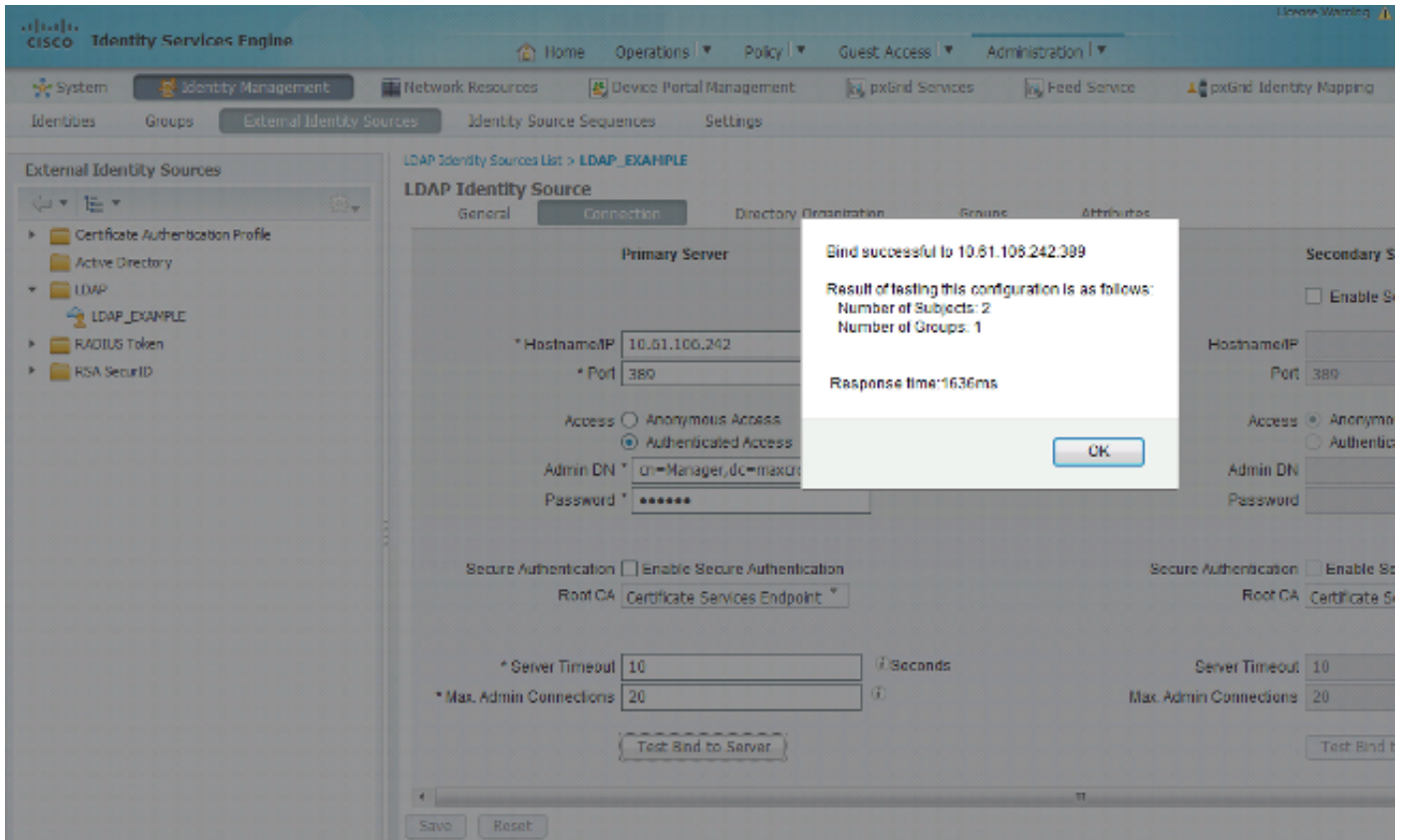
Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✓	Users in LDAP store	if (Wireless_802.1X AND LDAP_EXAMPLE:ExternalGroups EQUALS cn=domainusers,ou=groups,dc=mxcorp,dc=com )	then PermitAccess
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access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

ةكبشلاب لاصتالا ىلع ارداق نوكت نأ بجي ،نيوكتلا قيبطت دع

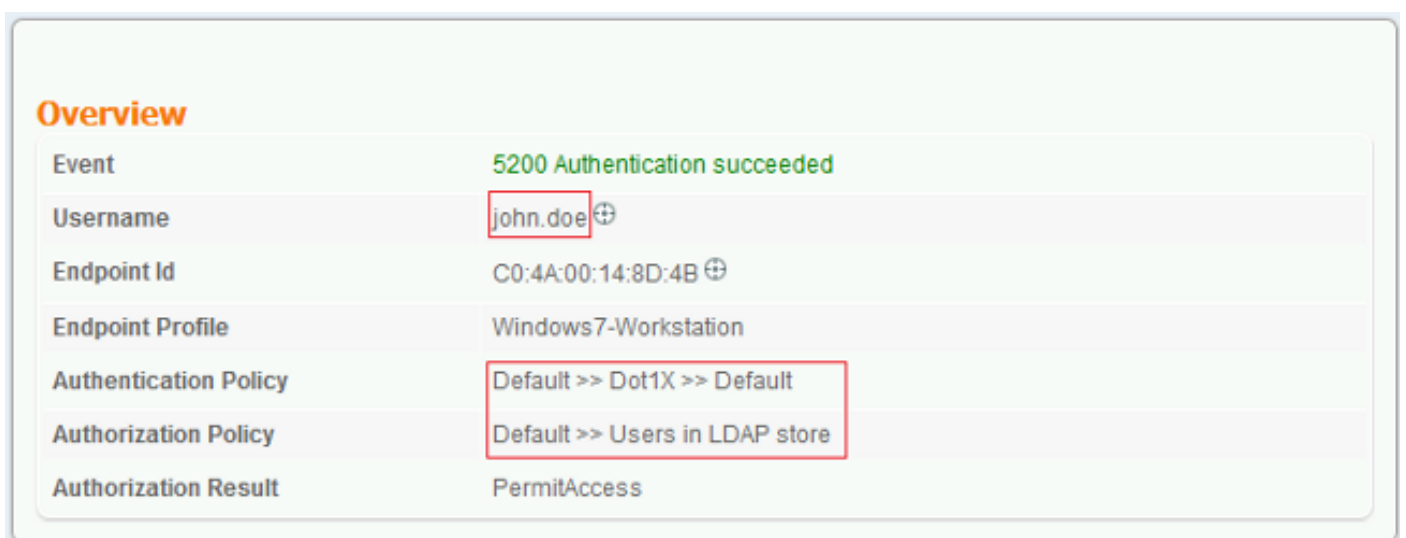
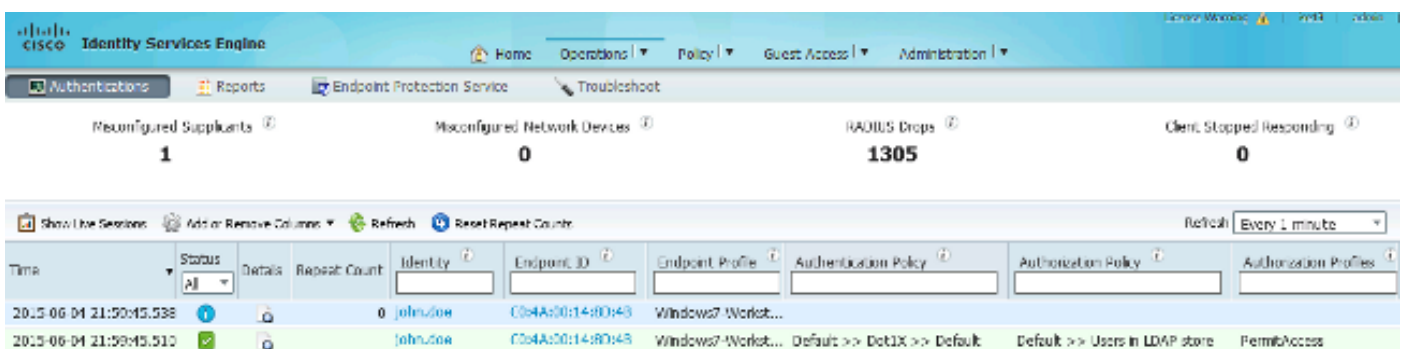


## ةحصللا نم ققحتلا

لاصتا مادختساب تاعومجمل او تاعوضوملا دادرثساب مق ،ISE و LDAP تانويكت نم ققحتلل  
مداخلاب رابتخا:



ISE ل نام ایچ ڈوم ن اری رقت روص ل هذ حضوت:





## 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

## هه حالص او عا طخال فاشك ت سا

ة فيكي و ني وكتل اذه عم اهت فداصم مت يتل اة عئاشل ا عا طخال ضعب مسقلا اذه فص ي  
اه حالص او عا طخال فاشك ت سا:

- ليغشت ةداعإب مق gssapi.dll نادقف لىل ةراشإلل أطخ تهجاو اذا، OpenLDAP تيبتت دعب Microsoft Windows.
- ظفحا .ةرشابم Cisco AnyConnect ل configuration.xml فلم ريرحت انكمم نوكي ال دق .ميدقلا فلملا لادبتسال هم دختسا م ث رخأ عقوم يف ديدجلا نيوكتللا
- هذه أطخللا ةلاسر دجوت ،ةقداصملا ريرقت يف :

<#root>

Authentication method is not supported by any applicable identity store

LDAP ةطساوب دمتعم ريغ هترتخا يذلا بولسألا نأ لىل هذه أطخللا ةلاسر ريرشت


ةم ودملا قرطالا يدحإ حضوي ريرقتلا سفن يف ةقداصملا لوكوتورب نأ نم دكأت (EAP-GTC) ةم ودملا قرطالا يدحإ حضوي ريرقتلا سفن يف ةقداصملا لوكوتورب نأ نم دكأت (EAP-TLS أو PEAP-TLS).

- ال ،تاىوهلا نزخم يف عوضوملا لىل ع روثلعلا مدع تظحال اذا ،ةقداصملا ريرقت يف ةدعاق يف مدختسم يأل عوضوملا مساةم سم عم ريرقتلا نم مدختسملا مساقباطي LDAP تانايب

رظني ISE نأ ينعى امم ،ةمسلا هذهل ديرف فرعم لىل ةميقلا نييعت مت ،ويرانيسلا اذه يف قباطت لىل ع روثلعلا لواحي امدنع LDAP مدختسمب ةصاخلا مدختسملا فرعم ميق لىل

- ،مداخلاب طبر رابتخا ءانثأ حىحص لكشب تاعومجملاو تاعوضوملا دادرستسا متي مل اذا ،ثحبلا دعاوقل حىحص ريغ نيوكت اذهف

نأ نكمي) dc و رذجال لىل ةيفرطالا ةدحو لا نم LDAP ل يمرهلا جردتلا ديدحت بجي هنأ ركذت (ةددعتم تاملك نم نوكتي

 [ةقداصم](#) لىل عجرا ،WLC بناج لىل ع احوال صإو EAP ةقداصم ءاطخأ فاشكتسال :حيملت دنتسم (WLC) [ةيكلساللا ةيلجمللا ةكبشلا مكحت تادحو نيوكت لاثم مادختساب EAP](#) Cisco.

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد ىوتحم مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتحم مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءاد ءوچرلاب ةصوءو تامچرتل هذه ةقء نء اهءل ءوئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءنل دن تسمل