

اهحال صا و هئا طخا فاشك ت ساو ISE نيوك ت ي ج راخ ل LDAP في رعت ن زخم مادخت سا ب

تا يوت حمل ا

[عمدق م ا](#)

[ةيس اس ا ل ا تا ب ل ط ت م ا](#)

[تا ب ل ط ت م ا](#)

[عمدخت س م ا تا نو ك م ا](#)

[نيوك ت ل ا](#)

[ةكب ش ل ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[ل ا ج م ل ا ب م ك ح ت ل ا ة د ح و ي ل ع ة ي و ه ل ا ة د ا ه ش ت ي ب ت](#)

[LDAP ل ي ل د ة ي ن ب ي ل ل ا ل و ص و ل ا](#)

[LDAP م داخ عم ISE ج م د](#)

[ل و ح م ل ا ن ي و ك ت](#)

[ة ي ا ه ن ل ل ا ة ط ق ن ن ي و ك ت](#)

[ISE ي ل ع ح و ن ل ل ا ة ع و م ح م ن ي و ك ت](#)

[ة ح ص ل ل ا ن م ق ق ح ت ل ا](#)

[اه حال ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا](#)

[ة ل ص ت ا ذ ت ا م و ل ع م](#)

عمدق م ا

ي ج راخ ة ي و ه ر د ص م ك ن م ا ل LDAP م داخ عم Cisco ISE ل م ا ك ت د ن ت س م ل ا ا ذ ه ف ص ي

ةيس اس ا ل ا تا ب ل ط ت م ا

تا ب ل ط ت م ا

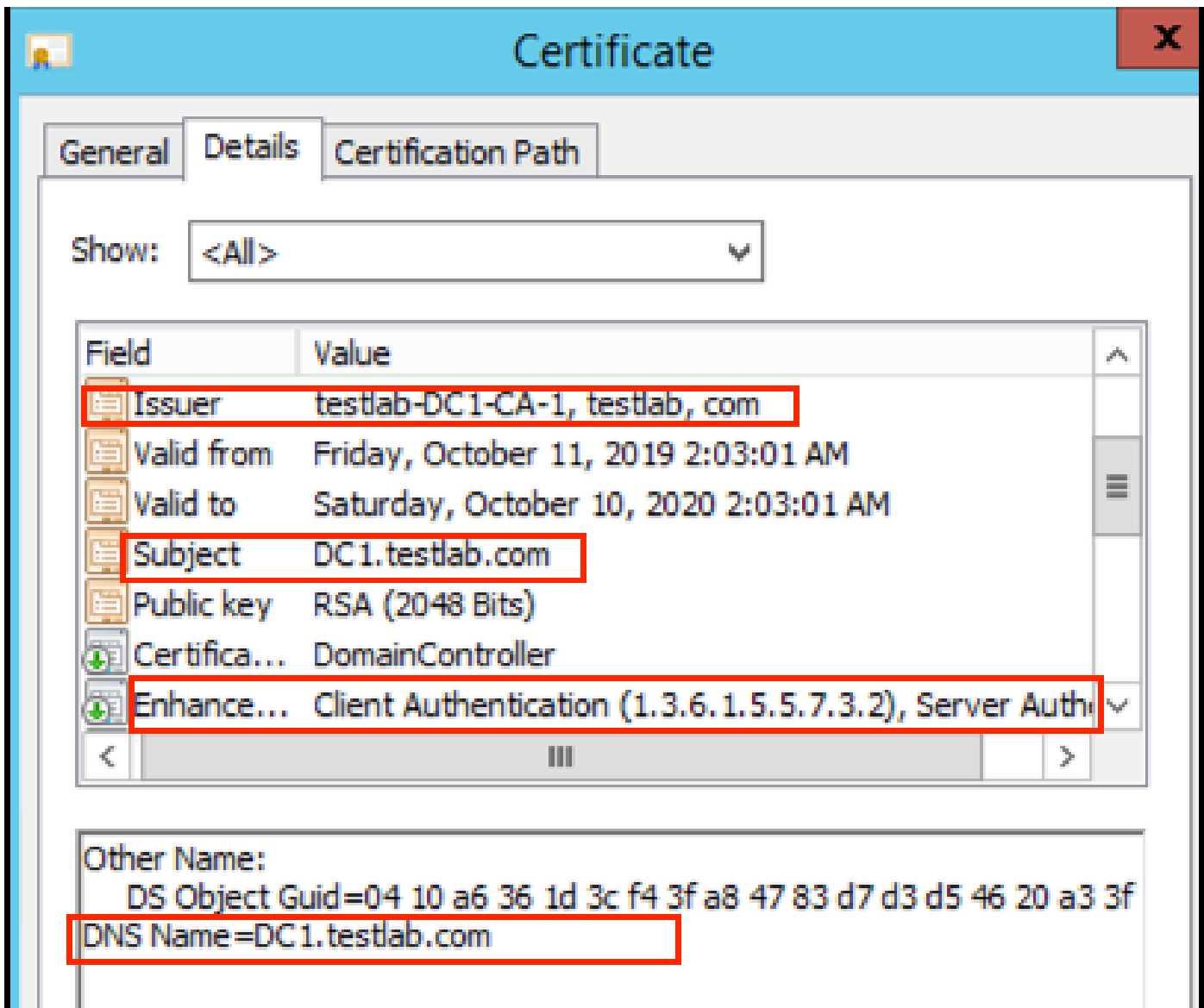
ة ي ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت:

- (ISE) ة ي و ه ل ا ة م د خ ك ر ح م ة ر ا د ا ل ة ي س ا س ا ل ا ة ف ر ع م ل ا
- Active Directory/ل ي ل د ل ا ي ل ل و ص و ل ل ف ي ف خ ل ل ن م ا ل ل و ك و ت و ر ب ل ا ب ة ي س ا س ا ل ا ة ف ر ع م (LDAPs)

عمدخت س م ل ا تا نو ك م ا

ة ي ل ا ت ل ا ة ي د ا م ل ا تا نو ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ا ي ل ل د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت

- Cisco ISE 2.6 Patch 7
- Microsoft Windows ا ل ا ر ا د ص ا ل ا 2012 R2 م داخ عم Active Directory Lightweight Directory



LDAP ليلد ةينب ىل لوصول

اذه في LDAP ضرعتسم ي مدختسأ، Active Directory م داخ ىل LDAPs ليلد ىل لوصول
 4.5 رادصإا، Softera LDAP ح فرصت م ادختسإا متي، ربتخمال

1. TCP 636 ذفنم ىل لاجملاب لاصتا عاشنإا مق.



2. نأ بچيو، نالعالا في ISE OU ىمست (OU) ةيميظنت ةدحو عاشنإا مق، ةطاسبلا لجا نم.
 (user1 و user2) ني مدختسمل نم ني نثا عاشنإا مق. UserGroup ىمست ةعومجم ىل يوتحت
 UserGroup ةعومجم في نيوضع امهل عوجو.

مدختسمل ةقداصل مل طقف ISE ىل LDAP ةيوه رصم مدختسي: ةظالم

Name	Value	Type
CN	UserGroup	Entry
CN	user2	Entry
CN	user1	Entry
CN	DESKTOP-19	Entry
CN	ComputerGroup	Entry
distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribute
dSCorePropagationData	1/1/1601	Attribute
dSCorePropagationData	6/20/2020 2:51:11 AM	Attribute
gPLink	[LDAP://cn={21A53B13-6971-45E8-8545-FD0C68E29790},c...	Attribute
instanceType	[Writable]	Attribute
name	ISE OU	Attribute
objectCategory	CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=...	Attribute
objectClass	organizationalUnit	Attribute
objectClass	top	Attribute
ou	ISE OU	Attribute
uSNChanged	607428	Attribute
uSNCreated	603085	Attribute
whenChanged	6/21/2020 2:44:06 AM	Attribute
whenCreated	6/20/2020 2:51:11 AM	Attribute
objectGUID	{44F45D1D-17B7-48DF-ABC6-3ED27FA4F694}	Binary Attribute

LDAP مداخل عم ISE جم

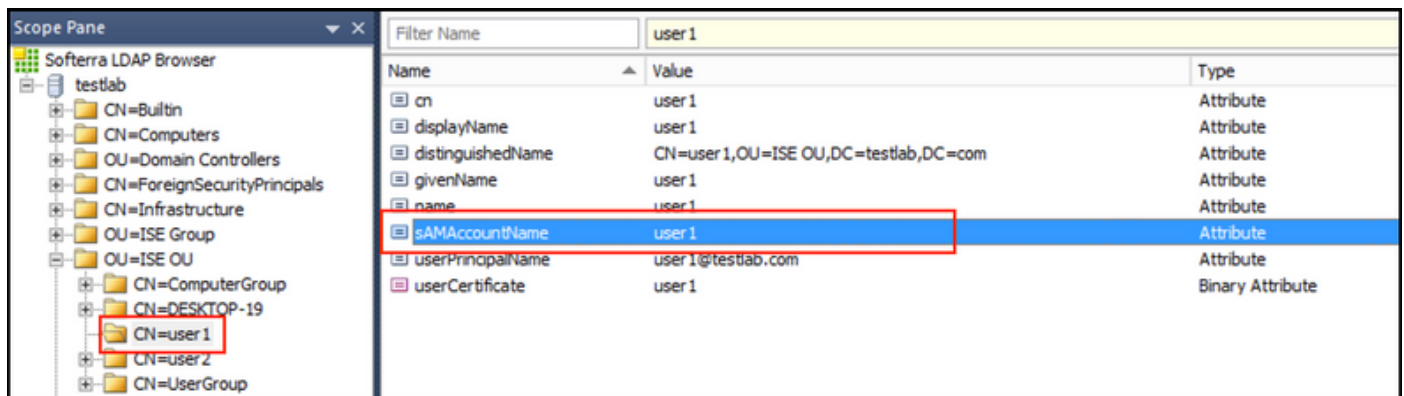
1. اہب قوتومال عداہشلل یف LDAP مداخل رذلجلا قدصملا عجرملا عداہش داریتسلا.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
DC1					
DC1-CA	Enabled	Infrastructure Cisco Services Endpoints	18 29 1C A7 00 13...	testlab-DC1-CA-1	testlab-DC1-CA-1

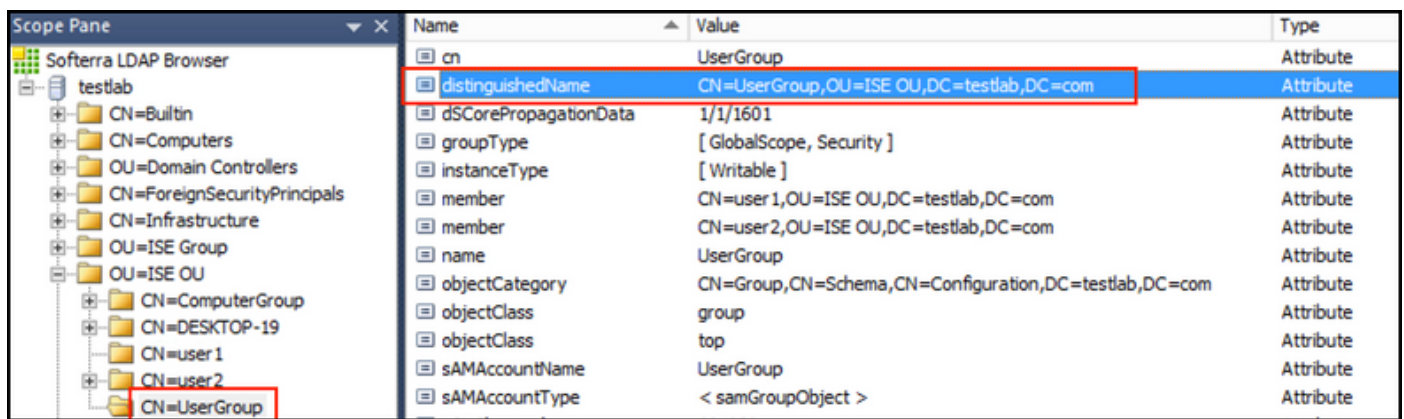
2. یف اضیأ ةدوجوم ISE لوؤسم عداہش ردصم عداہش نأ نم دکأتو ISE لوؤسم عداہش نم ققحت .
ہب قوتوملا تاداہشلل نزم.

3. ةرادإ یلل لقتنا LDAPs لیلد نم ةفلتخملا LDAP تامس مدختسأ، LDAP مداخل لملکت لچأ نم .
ةفاضلا > LDAP ةیوه رداصم > ةیجرالخلا ةیوهلا رداصم > ةیوهلا ةرادا >

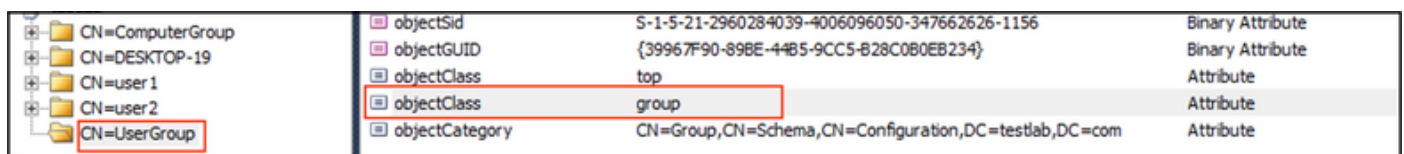
مٲي ،ويرانيسلا اذه في .(كلذى لى امو ، sAMAccountName، cn مادختسا كنكمي) LDAP تانايب ةياهنلا ةطقن لىل مٲمادختسا مٲسا مٲمادختسا



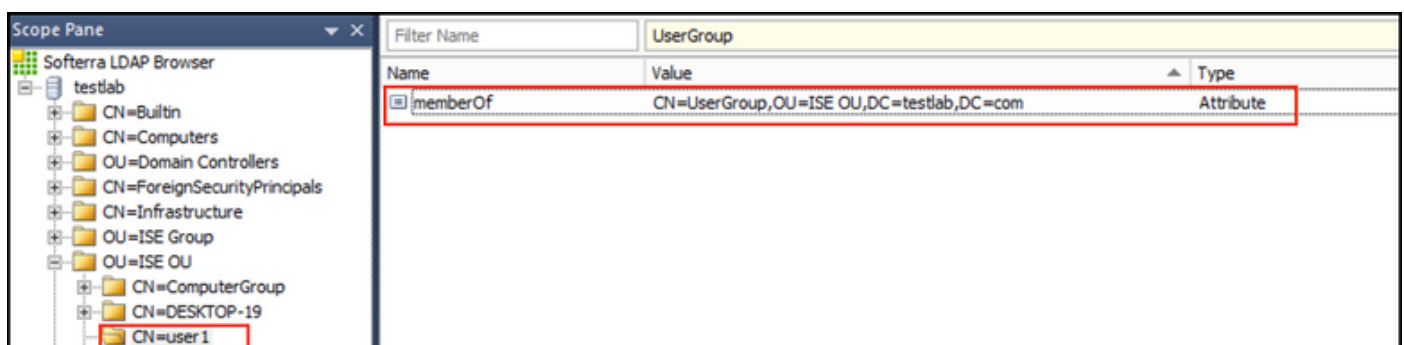
مٲسا ةمس مٲيق قباطت نا بجي .ةومجم مٲسا لمحت يتلا ةمسلا يه هذه :ةومجم مٲسا ةمس تاعومجم ةحفص في ةدوجومال LDAP ةومجم ءامسا عم LDAP لىلد في ةدوجومال ةومجم مٲسا مٲمادختسا



تاناكلا دىدحتل شحبال تايلمع في ةمٲقلا هذه مادختسا مٲي :ةومجم لىل ObjectClass تاعومجم كهيلع فرعت مٲسا



تاعومجم لىل مٲمادختسا مٲسا نييعت ةي في ةمسلا هذه ددحت :ةومجم مٲسا طخم ةمس

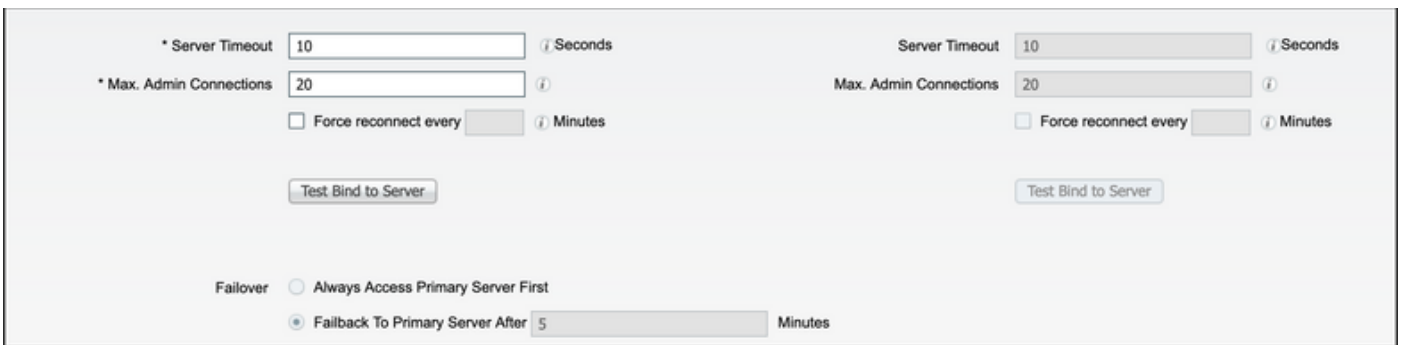
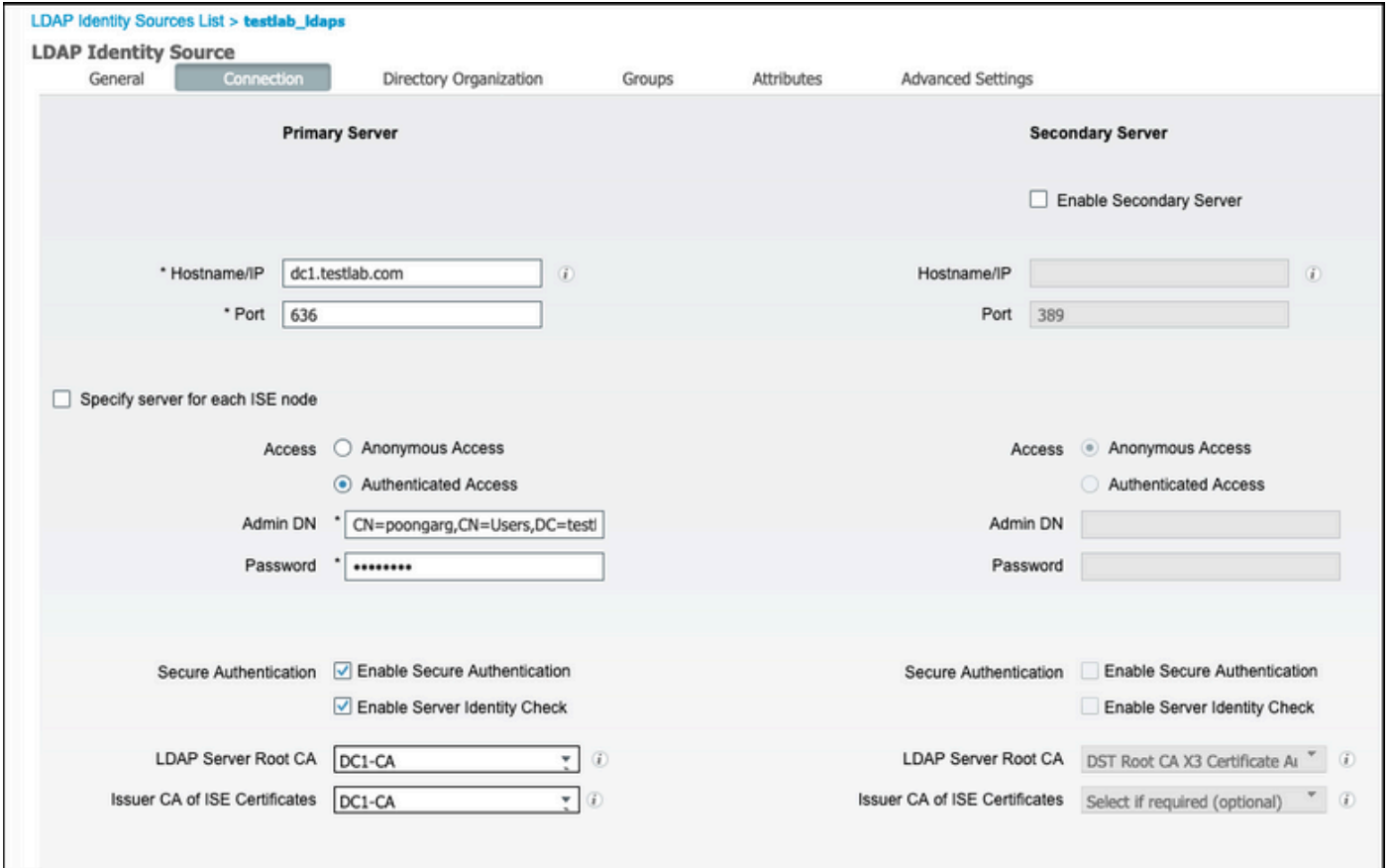


هذه مادختسا كنكمي .ةداهشلا تافيرعت لىل ويوتحت يتلا ةمسلا لخدأ :ةداهشلا ةمس

امدنع ءالمعلا ةطساوب اهميدقت متي يتلا تاداهشلا ةحص نم ققحتلل ايراي تخا تافيرتلا ءارجا متي ،تالاحل هذه لثم فيو .ءداهشلا ةقداصم فيرعت فلم نم عزك اهفيرت متي LDAP ةيوه ردصم نم اءادرتسا مت يتلا ةداهشلاو ليمعلا ةداهش ني ةيئانث ةنراقم



5. ليصوت بيوبتلا ةمالع ىلإ لقتنا ،LDAPs لاصتا نيوكتل :



6. DN مدختسملا مسا ىلع لوصحلل لاجملا ب مكحتلا ةدحو ىلع تانايبلا ليغشتب مق . LDAP مداخب لاصتا ءارجا في هءادختسال

PS C:\Users\Administrator> مدختسم مدختسم -name poongarg
"CN=poongarg,CN=Users,DC=testlab,DC=com"

ذفنم فيرعتب مقو ،LDAP مداخل حيحصلا فيضملا مسا وأ حيحصلا IP ناوع ددح . 1 ةوطخل

LDAPs (TCP 636)، و SSL مع LDAP عم لاصتا ءارجال Admin DN و.

مدخال ءي وه نم ققحتل رايخو ءنم آلا ءقداصلم لني كمتب مق 2. ءوطلال

لوؤسم ءداهش و LDAP مدخال رذجل قداصلم لءجرم لءداهش دح، ءلدسنم لءمئاق ل نم 3. ءوطلال LDAP مدخال سفن لءع تبثم لءداهش لءجرم انمدختس لءق ل) قداصلم لءجرم لءداهش ISE (اضئ أ ISE لوؤسم ءداهش رادصل ل).

ءاعومجم و أ صاخشأ ئ أ دادرءس ل مءئ ال، ءطقن لءه دنع .مدخال ل طبرل رابءل دح 4. ءوطلال دعب ءحبل دءاق نئوكء مءئ مل هنأل

هنأ .ءومجم لءعوضوم ل ءحب ءءاق نئوكءب مق، لءلدل ءسسؤم بئوبءل ءمالع ءءء 7. ئه ئءل ءاعومجم لءعوضوم لءطق ءءرءس لءنكم ئ نأل . LDAP عم ISE ل طبرل ءطقن نم ءومجم لءعوضوم ل نم لك دادرءس ل مءئ، وئرانئس لءه ئ ف . طبرل ءطقن لءفءأ OU=ISE OU

The screenshot shows the 'LDAP Identity Sources List > testlab_idaps' page. The 'LDAP Identity Source' section is active, with the 'Directory Organization' tab selected. The 'Subject Search Base' and 'Group Search Base' are both set to 'OU=ISE OU,DC=testlab,DC=com'. There are 'Naming Contexts...' buttons next to each. Below, there is a 'Search for MAC Address in Format' dropdown set to 'xx-xx-xx-xx-xx-xx'. At the bottom, there are two checkboxes: 'Strip start of subject name up to the last occurrence of the separator' (unchecked) and 'Strip end of subject name from the first occurrence of the separator' (unchecked).

ءادرءس او ISE لءع LDAP نم ءاعومجم لءدارئس لء ءفاضل قوف رقنا، ءاعومجم لءءءء 8. ءروصل ءه ئ فءءوم وه امك، ءاعومجم لء

The screenshot shows the 'LDAP Identity Sources List > testlab_idaps' page. The 'LDAP Identity Source' section is active, with the 'Groups' tab selected. At the top, there are 'Edit', 'Add', and 'Delete Group' buttons. Below, there is a table with two rows: 'Name' and 'CN=UserGroup,OU=ISE OU,DC=testlab,DC=com'. The 'Name' row has a dropdown arrow on the right.

لوحم ل نيوكت

switchport gig2/0/47 ب ل ص ت م Windows رت و ي ب م ك ز ا ه ج . 802.1x ة ق د ا ص م ل ل و ح م ل ن ي و ك ت ب م ق

```
aaa new-model

radius server ISE
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key xxxxxx
aaa group server radius ISE_SERVERS
server name ISE

!

aaa server radius dynamic-author
client x.x.x.x server-key xxxxxx

!

aaa authentication dot1x default group ISE_SERVERS local
aaa authorization network default group ISE_SERVERS
aaa accounting dot1x default start-stop group ISE_SERVERS
!
dot1x system-auth-control

ip device tracking
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
!

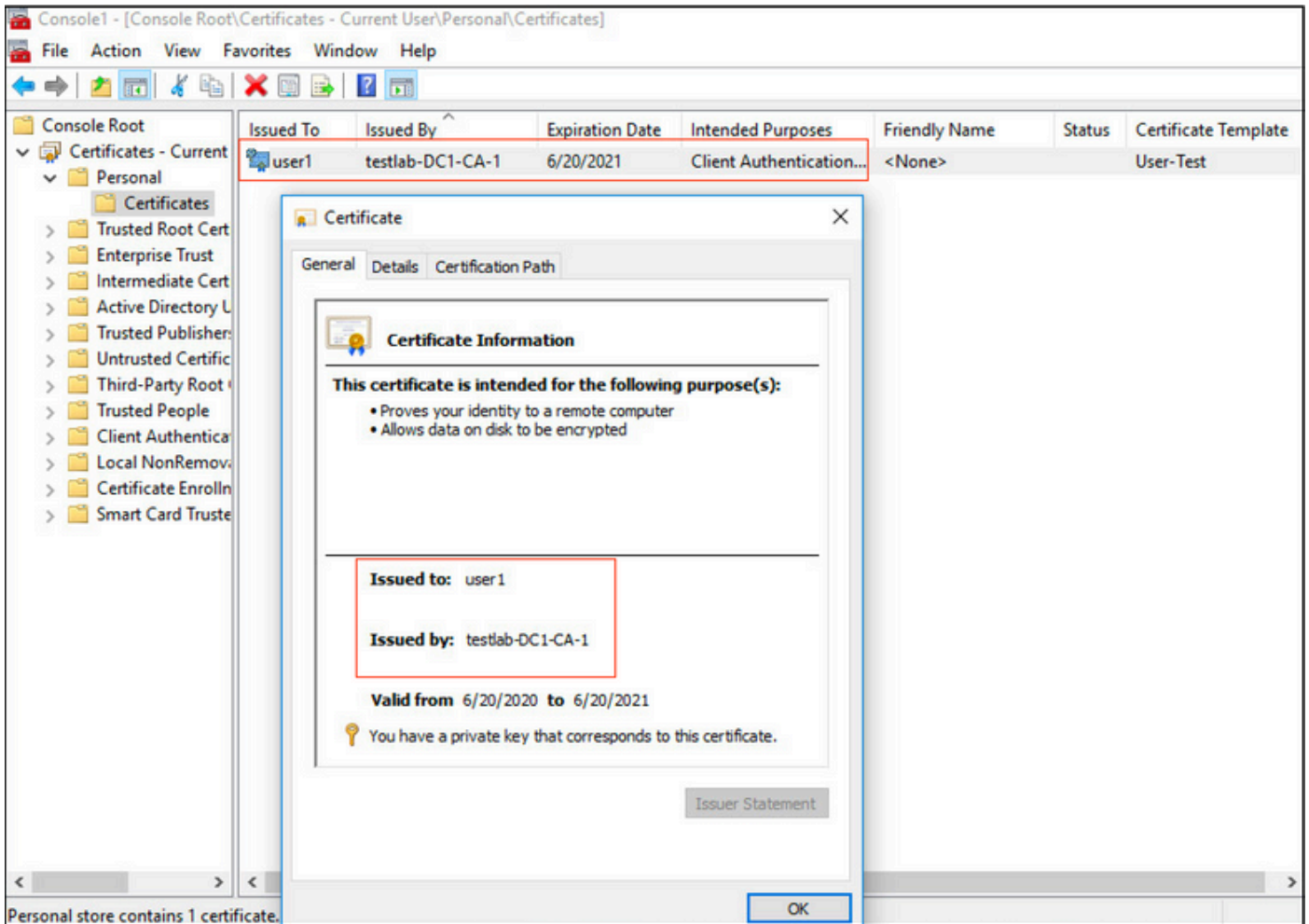
!

interface GigabitEthernet2/0/47
switchport access vlan xx
switchport mode access
authentication port-control auto
dot1x pae authenticator
```

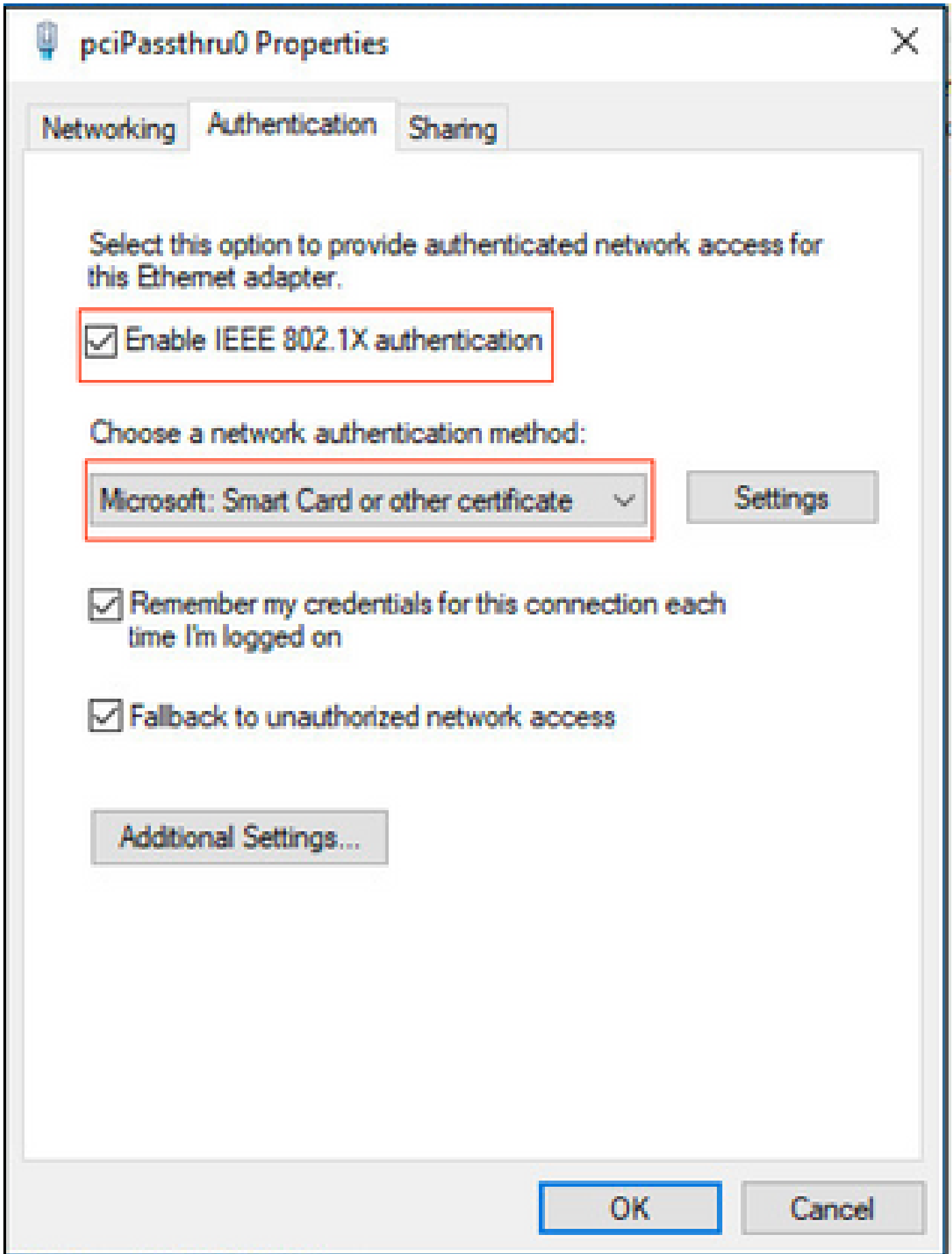
ة ي ا ه ن ل ل ة ط ق ن ن ي و ك ت

LDAP، EAP-TLS ة م و ع د م ل ل EAP ت ا ل و ك و ت و ر ب د ح ا م د خ ت س ي و Windows Native Plus م د خ ت س ي
ض ي و ف ت ل ل ا و م د خ ت س م ل ل ة ق د ا ص م ل

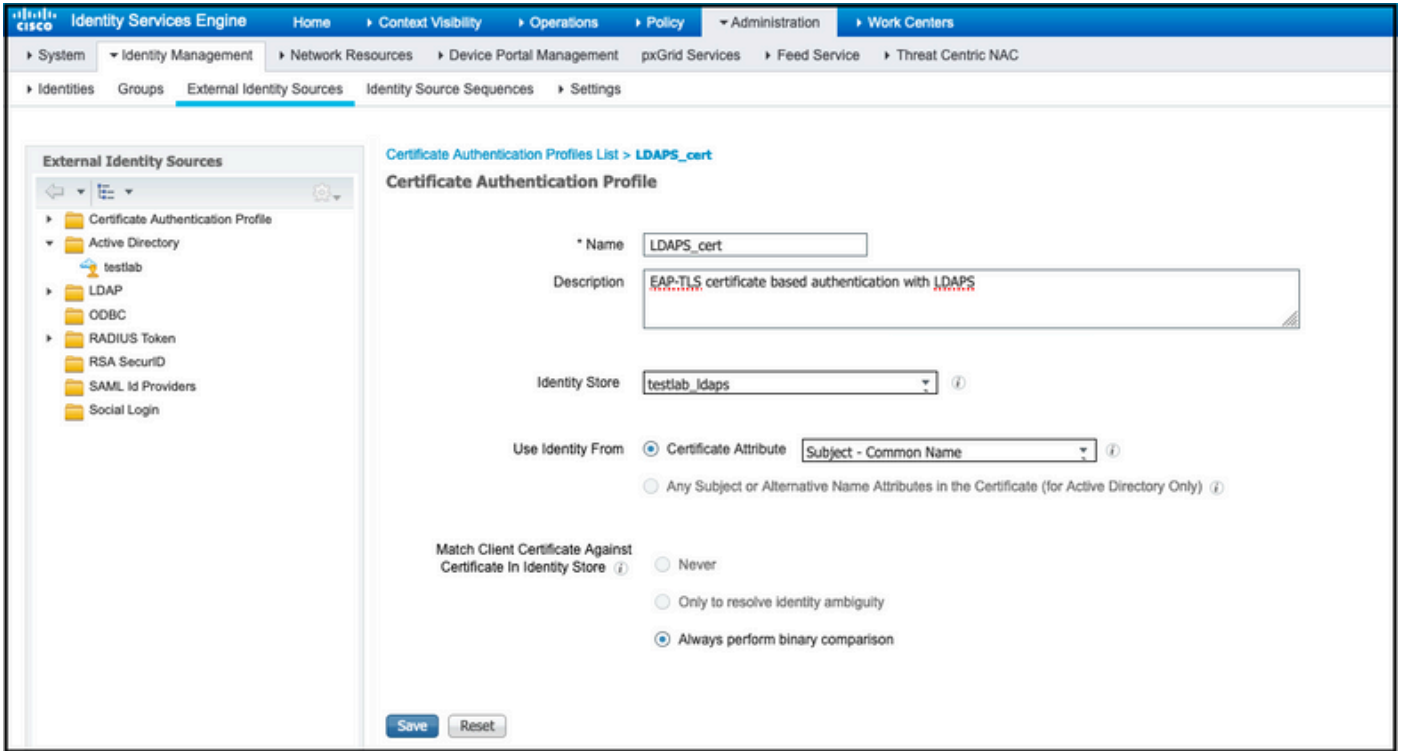
د و ص ق م ل ل ض ر غ ل ل د و ج و ن م و (1 م د خ ت س م ل ل) م د خ ت س م ل ل ة د ا ه ش ب ر ت و ي ب م ك ل ل د ي و ز ت ن م د ك ا ت .
ت ا د ا ه ش ة ل س ل س ن ا و ، " ا ه ب ق و ث و م ل ل ر ذ ج ل ل ق ي د ص ت ل ل ت ا ئ ي ه " ي ف و ل ي م ع ل ل ة ق د ا ص م ك ه ن م
ي ص خ ش ل ل ر ت و ي ب م ك ل ل ل ع ة د و ج و م ر د ص م ل ل



2. ىرخأ ةداهش وأ Microsoft:Smart ةقاطبك ةقداصل ل بولسأ ديدحت و dot1x ةقداصل نيكم ت. EAP-TLS ةقداصل ل.



رتخاو ةقداصملا عضو ديدحت عم عبرملا دح .راطا حتفيو ،"ةيفاضا تاداعا" قوف رقنا 3. ةروصلا هذه يف حضوم وه امك ،مدختسملا ةقداصم



يُجرى إدخال هوية العميل ودخول هوية الخادم لإجراء مصادقة هوية العميل مع الخادم باستخدام بروتوكول EAP-TLS مع مصادقة هوية العميل باستخدام بروتوكول LDAPS:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected	
Internal Endpoints	>	testlab_ldaps	⌵
Internal Users	<		⬆
Guest Users	>>		⬇
testlab	<<		⬇
All_AD_Join_Points			⬇
rad			⬇

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

Save Reset

Wired Dot1x: ةقداصل نآلا جهنلا ةومجم نيوكت

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Wired Dot1x Reset Policyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wired Dot1x		Wired_802.1X	Default Network Access	453

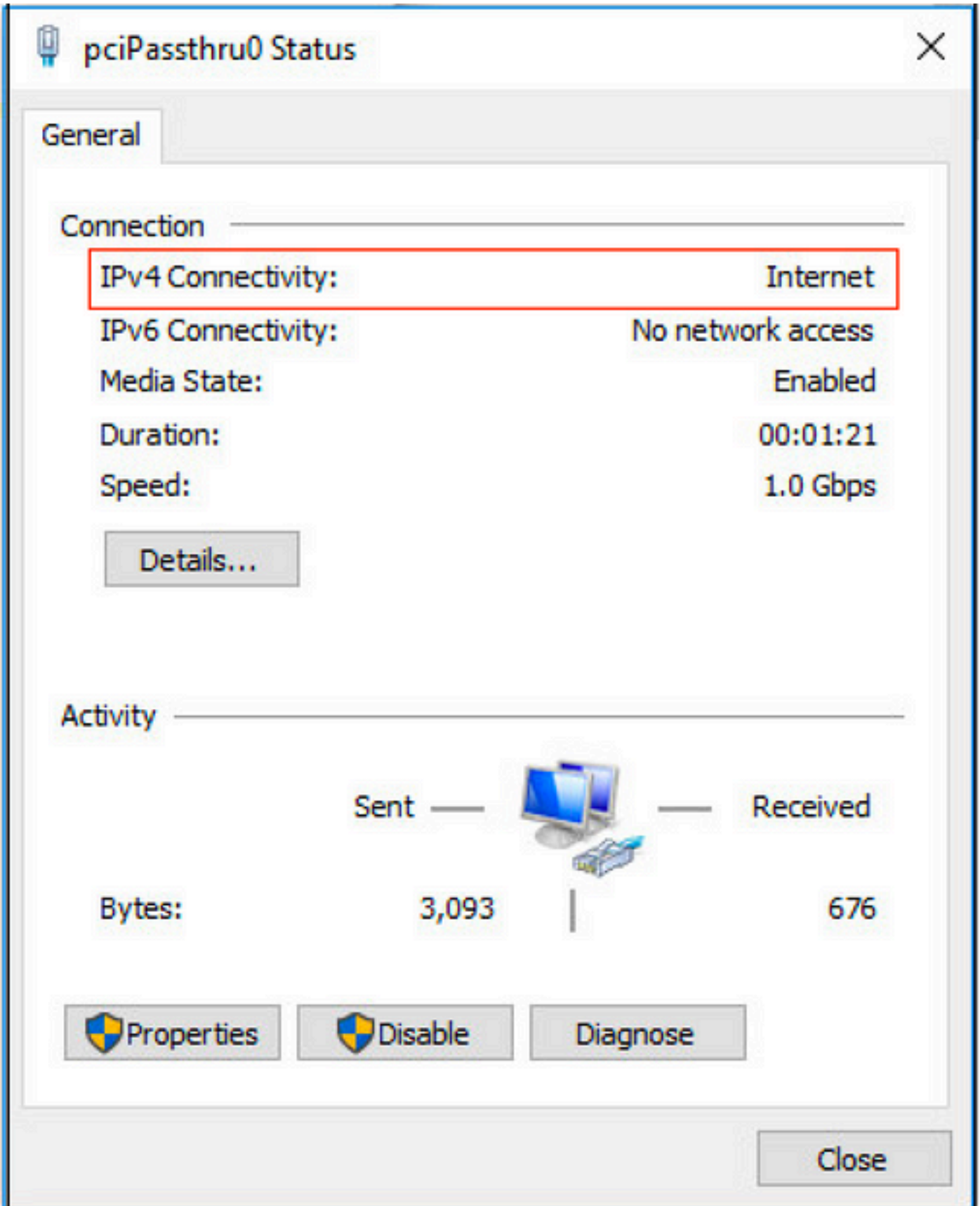
Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch	LDAPS	223	Options
✔	Default		LDAPS	0	Options

Authorization Policy (2)							
+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
Search							
<input checked="" type="checkbox"/>	Users in LDAP Store		testlab_idaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	PermitAccess	Select from list	207	
<input checked="" type="checkbox"/>	Default			DenyAccess	Select from list	11	

Reset Save

لإتمام EAP-TLS لوكوت ورب مادت ساب ةياهن لة طقن ةقداصم اننكم ي، نيوكت لة اذة دعب LDAP. ةيوة ردصم



ةحصلا نم ققحتلا

ي:صخشلا رتوي بمكللاب لصتملا Switchport لىل ةقداصملا ةسلج نم ققحت 1.

```
SW1#sh auth sessions int g2/0/47 de
      Interface: GigabitEthernet2/0/47
      MAC Address: b496.9126.dec0
      IPv6 Address: Unknown
      IPv4 Address: 10.106.38.165
      User-Name: user1
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      Session timeout: N/A
      Restart timeout: N/A
      Periodic Acct timeout: N/A
      Session Uptime: 43s
      Common Session ID: 0A6A26390000130798C66612
      Acct Session ID: 0x00001224
      Handle: 0x6800002E
      Current Policy: POLICY_Gi2/0/47

Local Policies:
      Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list:
      Method          State
      dot1x           Authc Success
```

مادختساب تاعومجملاو تاعوضوملا دادرئسإ كنكمي، ISE و LDAP تانيوكت نم ققحتلل 2. مداخلاب رابتخإ لاصتا

LDAP Identity Sources List > testlab_ldaps

LDAP Identity Source

General **Connection** Directory Organization Groups Attributes Advanced Settings

Access Anonymous Access Authenticated Access

Admin DN * CN=poongarg,C... Password *

Secure Authentication Enable Secure Authentication Enable Server Identity Check

LDAP Server Root CA DC1-CA Issuer CA of ISE Certificates DC1-CA

* Server Timeout 10 Seconds * Max. Admin Connections 20

Force reconnect every Minutes

Test Bind to Server

Failover Always Access Primary Server First

Save Reset

Ldap bind succeeded to dc1.testlab.com:636
 Number of Subjects 3
 Number of Groups 2
 Response time 73ms

OK

3. مداخلت سمالا قداصم ريرقت نم ققحت ال:

Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...	Network De...	Device Port	Authentication Pro...
Jun 24, 2020 04:45:21.727 AM	●		user1	B4-96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess	GigabitEthernet2/0/47	EAP-TLS	
Jun 24, 2020 04:45:20.671 AM	●		user1	B4-96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess	LAB-Switch	GigabitEthernet2/0/47	EAP-TLS

4. ةيانهنلا ةطقنل يليصفتلا قداصم ال ريرقت نم ققحت:

Overview

Event 5200 Authentication succeeded

Username user1

Endpoint Id B4:96:91:26:DE:C0

Endpoint Profile Unknown

Authentication Policy Wired Dot1x >> Dot1x

Authorization Policy Wired Dot1x >> Users in LDAP Store

Authorization Result PermitAccess

Authentication Details

Source Timestamp	2020-06-24 04:40:52.124
Received Timestamp	2020-06-24 04:40:52.124
Policy Server	ISE26-1
Event	5200 Authentication succeeded
Username	user1
Endpoint Id	B4:96:91:26:DE:C0
Calling Station Id	B4-96-91-26-DE-C0
Endpoint Profile	Unknown
IPv4 Address	10.106.38.165
Authentication Identity Store	testlab_idaps
Identity Group	Unknown
Audit Session Id	0A6A26390000130C98CE6088
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	LAB-Switch

15041 Evaluating Identity Policy

15048 Queried PIP - Network Access.NetworkDeviceName

22072 Selected identity source sequence - LDAPS

22070 Identity name is taken from certificate attribute

15013 Selected Identity Source - testlab_ldaps

24031 Sending request to primary LDAP server - testlab_ldaps

24016 Looking up user in LDAP Server - testlab_ldaps

24023 User's groups are retrieved - testlab_ldaps

24004 User search finished successfully - testlab_ldaps

22054 Binary comparison of certificates succeeded

22037 Authentication Passed

12506 EAP-TLS authentication succeeded

15036 Evaluating Authorization Policy

24209 Looking up Endpoint in Internal Endpoints IDStore - user1

24211 Found Endpoint in Internal Endpoints IDStore

15048 Queried PIP - testlab_ldaps.ExternalGroups

15016 Selected Authorization Profile - PermitAccess

22081 Max sessions policy passed

22080 New accounting session created in Session cache

11503 Prepared EAP-Success

11002 Returned RADIUS Access-Accept

5. حاجة ISE لى ع مزحل طاق التال لالخ نم LDAP مداخ و ISE ني ب تاناي بل ريفشت نم ققحت مداخ LDAPs:

No.	Time	Source	Destination	Protocol	Length	Address	64bits	Info
20	2020-06-24 10:40:24.205431	10.197.164.22	10.197.164.21	TCP	74	00:0c:29:98:ca:28,0...	28057	→ 636 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=140972072 TSecr=0 WS=128
21	2020-06-24 10:40:24.206505	10.197.164.21	10.197.164.22	TCP	74	00:50:56:a0:3e:7f,0...	636	→ 28057 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 MS=256 SACK_PERM=1 TSval=30158962 TSecr=140972872
22	2020-06-24 10:40:24.206613	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...	28057	→ 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=140972873 TSecr=30158962
23	2020-06-24 10:40:24.206961	10.197.164.22	10.197.164.21	TLSv1.2	207	00:0c:29:98:ca:28,0...		Client Hello
24	2020-06-24 10:40:24.210413	10.197.164.21	10.197.164.22	TLSv1.2	2036	00:50:56:a0:3e:7f,0...		Server Hello, Certificate [Packet size limited during capture]
25	2020-06-24 10:40:24.210508	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...	28057	→ 636 [ACK] Seq=142 Ack=1971 Win=33152 Len=0 TSval=140972877 TSecr=30158962
26	2020-06-24 10:40:24.215211	10.197.164.22	10.197.164.21	TLSv1.2	260	00:0c:29:98:ca:28,0...		Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27	2020-06-24 10:40:24.218678	10.197.164.21	10.197.164.22	TLSv1.2	173	00:50:56:a0:3e:7f,0...		Change Cipher Spec, Encrypted Handshake Message
28	2020-06-24 10:40:24.219113	10.197.164.22	10.197.164.21	TLSv1.2	199	00:0c:29:98:ca:28,0...		Application Data
29	2020-06-24 10:40:24.230384	10.197.164.21	10.197.164.22	TLSv1.2	167	00:50:56:a0:3e:7f,0...		Application Data
30	2020-06-24 10:40:24.231712	10.197.164.22	10.197.164.21	TLSv1.2	279	00:0c:29:98:ca:28,0...		Application Data
31	2020-06-24 10:40:24.238809	10.197.164.21	10.197.164.22	TLSv1.2	1079	00:50:56:a0:3e:7f,0...		Application Data [Packet size limited during capture]
32	2020-06-24 10:40:24.238958	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...	28057	→ 636 [ACK] Seq=602 Ack=3992 Win=36864 Len=0 TSval=140972905 TSecr=30158965
33	2020-06-24 10:40:24.251944	10.197.164.22	10.197.164.21	TLSv1.2	263	00:0c:29:98:ca:28,0...		Application Data
34	2020-06-24 10:40:24.253658	10.197.164.21	10.197.164.22	TLSv1.2	295	00:50:56:a0:3e:7f,0...		Application Data
35	2020-06-24 10:40:24.293322	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...	28057	→ 636 [ACK] Seq=879 Ack=4221 Win=39680 Len=0 TSval=140972960 TSecr=30158967
86	2020-06-24 10:40:57.946553	10.197.164.22	10.197.164.21	TLSv1.2	151	00:0c:29:98:ca:28,0...		Application Data
87	2020-06-24 10:40:57.947600	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...	28057	→ 636 [FIN, ACK] Seq=964 Ack=4221 Win=39680 Len=0 TSval=141006614 TSecr=30158967

```

> Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
> Ethernet II, Src: Vmware_00:3e:7f (00:50:56:a0:3e:7f), Dst: Vmware_98:ca:28 (00:0c:29:98:ca:28)
> Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21
> Transmission Control Protocol, Src Port: 28057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133
  Source Port: 28057
  Destination Port: 636
  [Stream index: 2]
  [TCP Segment Len: 133]
  Sequence number: 336 (relative sequence number)
  [Next sequence number: 469 (relative sequence number)]
  Acknowledgment number: 2078 (relative ack number)
  1000 ... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
  Window size value: 259
  [Calculated window size: 33152]
  [Window size scaling factor: 128]
  Checksum: 0x5e61 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [SEQ/ACK analysis]
  > [Timestamps]
  > TCP payload (133 bytes)
  Secure Sockets Layer
  > TLSv1.2 Record Layer: Application Data Protocol: ldap
  Content Type: Application Data (23)
  Version: TLS 1.2 (0x0303)
  Length: 128
  Encrypted Application Data: 17301b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84...
  
```

→ Encrypted Data

اهال صا و اطاخال فاشك سا

ةي فيكو ني وك تال اذه عم اهت فداصم مت يت لة عئاش ل اطاخال ضعب مس قلا اذه فصي اهال صا و اطاخال فاشك سا.

- هذه اطاخال ةلاسر ةي ةر كنكمي، ةقداصم لارقت يف

Authentication method is not supported by any applicable identity store

نأ نم دكأت LDAP. ةطساوب دم تعم ريغ هترتخا يذلا بولسأل نا لى اذه اطاخال ةلاسر ريرشت (EAP-TLS أو EAP-GTC) ةم و عدم ل قرطال اذح ارضوي ريرقت ل س فن يف ةقداصم ل لوك و تورب (PEAP-TLS أو).

- اطاخ شود عم مدخال اب طبر ل رابتخا هت نا.

LDAPs. in order to ليغشت تقو ةثالث all the تنكمو ISE لى ع طاق تال طبر تذخا، رادصا عون اذه تيرتخا prrt-server.log ل تصحفو، رادصا ل تشعنأ، اطاخال احيصت يوتسم لى ع prrt-jni تانوكمو درم.

ذف نم ل مداخ ضرعو ةئيس ةداهش لوح ةمزحل طاق تال وكشي

04:10:20,197,ERROR,0x7f9c5b6f1700,LdapSslConnectionContext::checkCryptoResult(id = 1289): error message

✎ مسا يا وأ) ةداهشلا عوضوم مسا اب LDAP ةحفص ي ف فيضمال مسا نيوكت بجي :ةظحالمة كبش وأ عوضوملا ي ف اذه لثم كيدل نكي مل ام كلذل .(عوضوملل ليدبال مسا الام ةكبش ةمئاق ي ف IP ناوعب صيخرت كمزلي ف ،لمعي الف ،(SAN) نيختلا ةقطنم (SAN) نيختلا ةقطنم

3. اذه .ةيوهلا نزخم ي ف عوضوملا يلع روثعال مدع ةظحالمة كنكمي ،ةقداصمال ريرقت ي ف .ةدعاق ي ف مدختسم ي ف عوضوملا مسا ةمسق قباطي ال ريرقتلا نم مدختسملا مسا نا ينع ي ف ،ةمسلا هذهل SAMAccountName لى ةميقلا نييعت مت ،ويرانيسلا اذه ي ف .LDAP تانايب يلع روثعال لواحي ام دنع LDAP مدختسم ل SAMAccountName ميقي لى رظني ISE نا ينع ي ف قباطت

4. ببسلا .مداخالاب طبر رابتخا ءانثأ حيحص لكشب تاعومجملاو عيضاوملا دادرتسا رذعت .ديدحت بجي هنا ركذت .ثحبلا دعاوقل حيحص ريغ نيوكت وه ةلكشملا هذهل الامتحا رثكألا تاملك نم نوكتي نا نكمي) dc و رذجال لى ةيفرطلا ةدحوللا نم LDAP ل يلكيهال لسلسلا (ةددعتم

ةلص تاذا تاملعم

- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/119149-configure-ise-00.html#anc9>
- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214975-configure-eap-tls-authentication-with-is.html>

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل