Configure and Troubleshoot ISE with External LDAPS Identity Store

Contents

Introduction

This document describes the integration of the Cisco ISE with the Secure LDAPS server as an External Identity Source.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Identity Service Engine (ISE) administration
- Basic knowledge of Active Directory/Secure Lightweight Directory Access Protocol (LDAPS)

Components Used

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

- Cisco ISE 2.6 Patch 7
- Microsoft Windows version 2012 R2 with Active Directory Lightweight Directory Services installed
- Windows 10 OS PC with native supplicant and user certificate installed
- Cisco Switch C3750X with 152-2.E6 image

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

LDAPS allows for the encryption of LDAP data (which includes user credentials) in transit when a directory bind is established. LDAPS uses TCP port 636.

These authentication protocols are supported with LDAPS:

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

✎ **Note**: EAP-MSCHAPV2 (as an inner method of PEAP, EAP-FAST or EAP-TTLS), LEAP, CHAP, and EAP-MD5 are not supported with LDAPS External Identity Source.

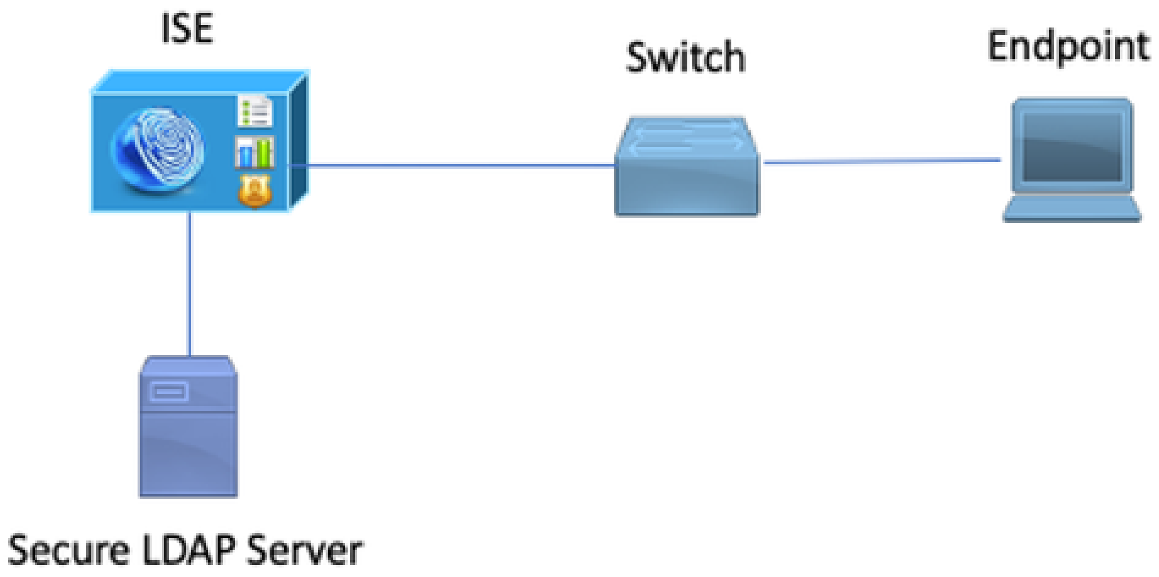
Configure

This section describes the configuration of the network devices and integration of the ISE with Microsoft Active Directory (AD) LDAPS server.

Network Diagram

In this configuration example, the endpoint uses an Ethernet connection with a switch to connect with the Local Area Network (LAN). The connected switchport is configured for 802.1x authentication to authenticate the users with ISE. On the ISE, LDAPS is configured as an external identity store.

This image illustrates the network topology that is used:



Configure LDAPS on Active Directory

Install Identity Certificate on Domain Controller

In order to enable LDAPS, Install a certificate on Domain Controller (DC) that meets these requirements:

1. The LDAPS certificate is located in the Domain Controller Personal Certificate Store.

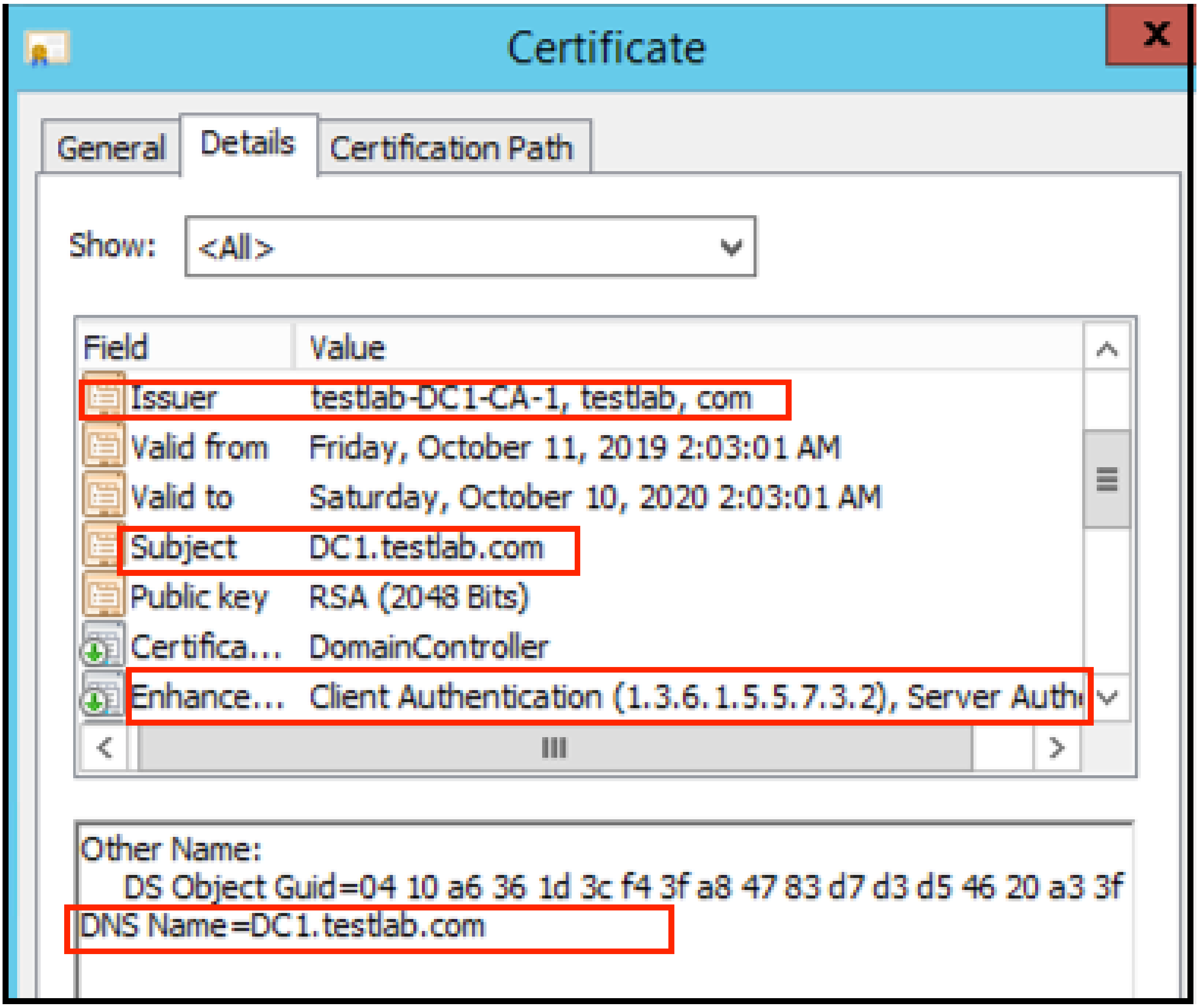
2. A private key that matches the certificate is present in the Domain Controller's store and is correctly associated with the certificate.

3. The Enhanced Key Usage extension includes Server Authentication (1.3.6.1.5.5.7.3.1) object identifier (also known as OID).

4. The Fully Qualified Domain Name (FQDN) of the Domain Controller (for example, DC1.testlab.com) must be present in one of these attributes: The Common Name (CN) in the Subject field and DNS entry in the Subject Alternative Name Extension.

5. The certificate must be issued by a Certificate Authority(CA) that the Domain Controller and the LDAPS clients trust. For a trusted secure communication, the client and the server must trust each other's root CA and the intermediate CA certificates which issued certificates to them.

6. The Schannel cryptographic service provider (CSP) must be used to generate the key.



Show: <All>

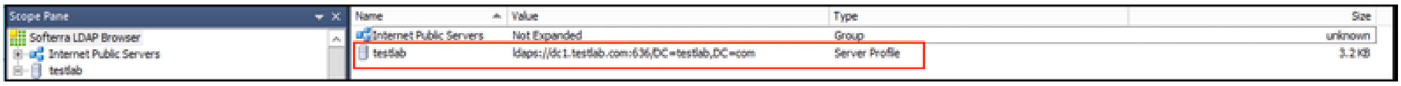
Field	Value
Issuer	testlab-DC1-CA-1, testlab, com
Valid from	Friday, October 11, 2019 2:03:01 AM
Valid to	Saturday, October 10, 2020 2:03:01 AM
Subject	DC1.testlab.com
Public key	RSA (2048 Bits)
Certifica...	DomainController
Enhance...	Client Authentication (1.3.6.1.5.5.7.3.2), Server Auth

Other Name:
DS Object Guid=04 10 a6 36 1d 3c f4 3f a8 47 83 d7 d3 d5 46 20 a3 3f
DNS Name=DC1.testlab.com

Access LDAPS Directory Structure

In order to access the LDAPS Directory on the Active Directory server, make use of any LDAP browser. In this LAB, Softerra LDAP Browser 4.5 is used.

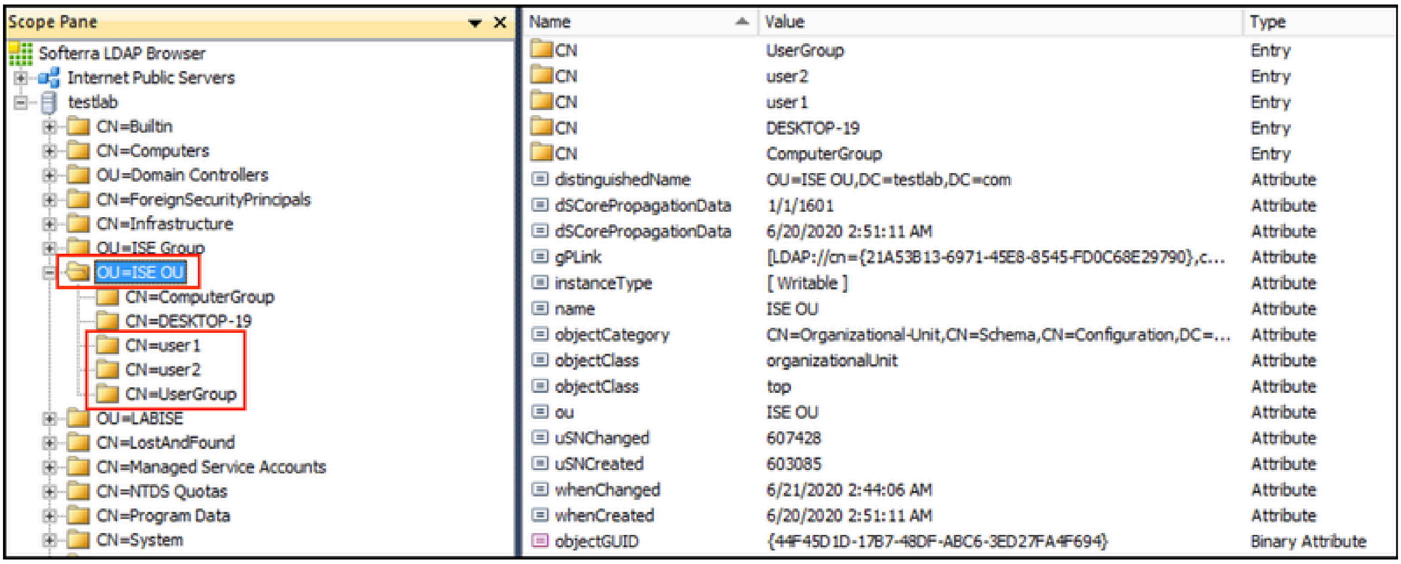
1. Establish a connection to the domain on TCP port 636.



Name	Value	Type	Size
Internet Public Servers	Not Expanded	Group	unknown
testlab	ldaps://dc1.testlab.com:636/DC=testlab,DC=com	Server Profile	3.2 KB

2. For simplicity, Create an Organizational Unit (OU) named ISE OU in the AD, and it must have a Group named UserGroup. Create two users (user1 and user2) and make them members of the group UserGroup.

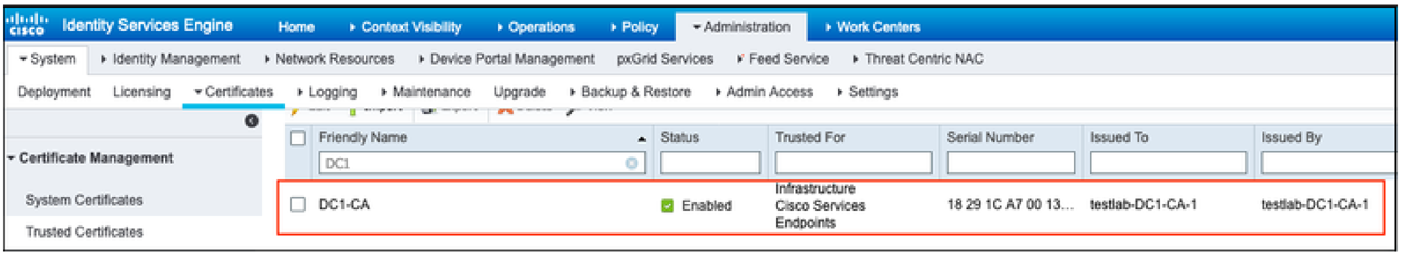
Note: LDAP Identity Source on ISE is used only for User authentication.



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

Integrate ISE with LDAPS Server

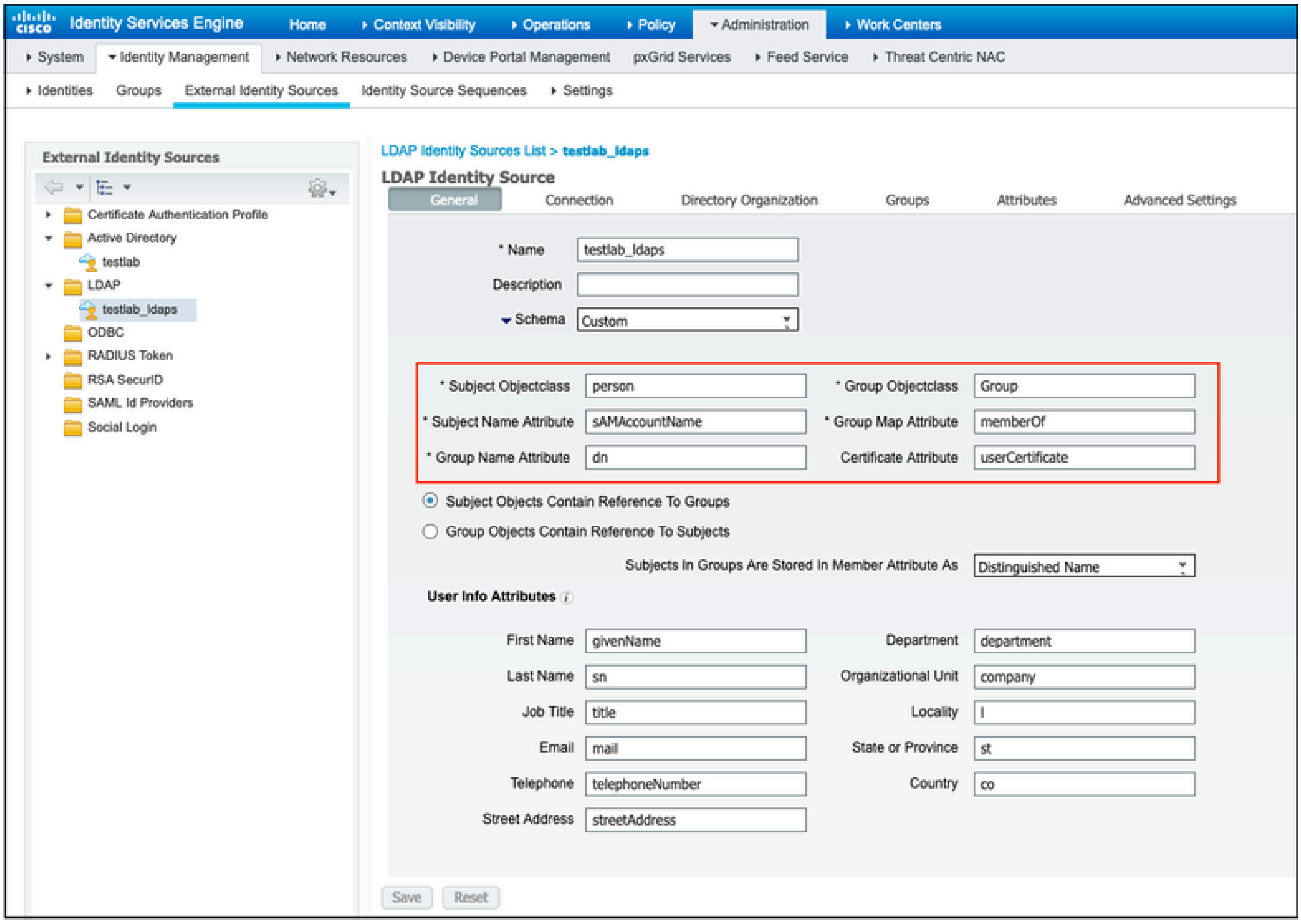
1. Import the LDAP Server Root CA certificate in the Trusted Certificate.



☐	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. Validate the ISE admin certificate and ensure that the ISE admin certificate issuer certificate is also present in the Trusted Certificate Store.

3. In order to integrate the LDAPS server, make use of the different LDAP attributes from the LDAPS directory. Navigate to **Administration > Identity Management > External Identity Sources > LDAP Identity Sources > Add**:



LDAP Identity Source

* Name	testlab_ldaps
Description	
Schema	Custom

* Subject Objectclass	person	* Group Objectclass	Group
* Subject Name Attribute	sAMAccountName	* Group Map Attribute	memberOf
* Group Name Attribute	dn	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

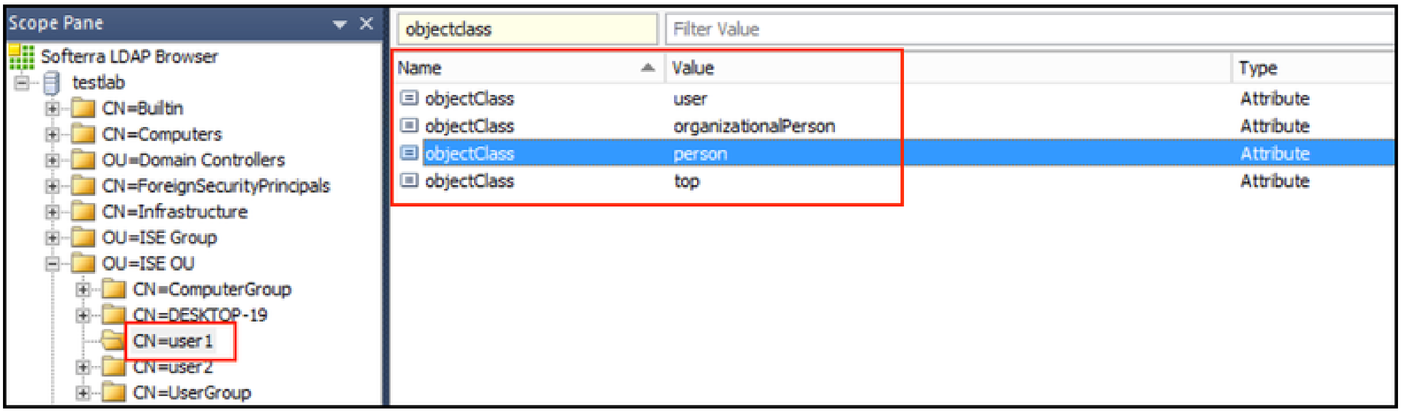
User Info Attributes

First Name	givenName	Department	department
Last Name	sn	Organizational Unit	company
Job Title	title	Locality	l
Email	mail	State or Province	st
Telephone	telephoneNumber	Country	co
Street Address	streetAddress		

4. Configure these attributes from the General Tab:

Subject Objectclass: This field corresponds to the Object class of user accounts. You can use one of the four classes here:

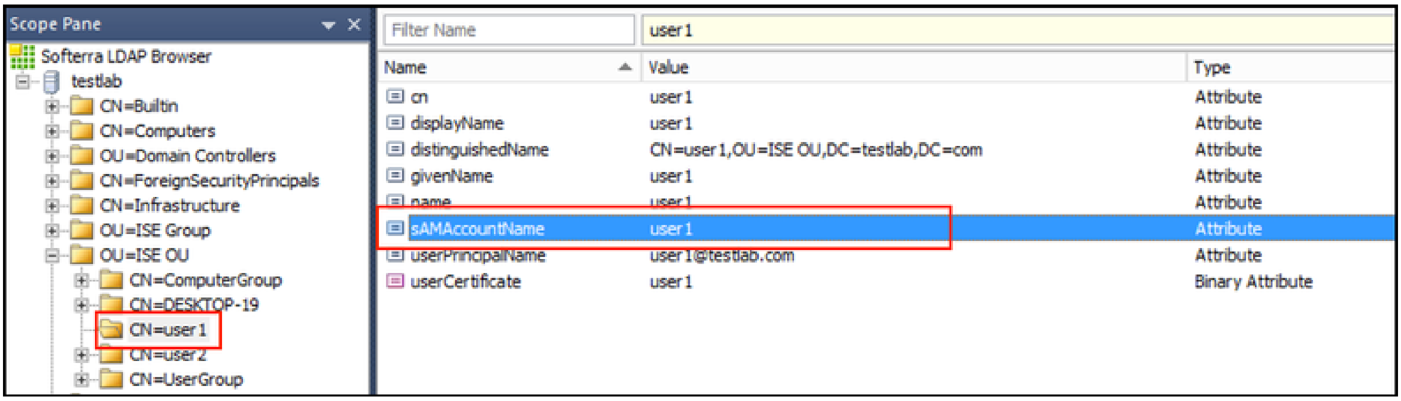
- Top
- Person
- OrganizationalPerson
- InetOrgPerson



objectclass

Name	Value	Type
objectClass	user	Attribute
objectClass	organizationalPerson	Attribute
objectClass	person	Attribute
objectClass	top	Attribute

Subject Name Attribute: This field is the name of the attribute containing the username from the request. This attribute is retrieved from the LDAPS when the ISE inquires a specific user name in the LDAP database (you can use cn, sAMAccountName, etc). In this scenario, user1 username on the endpoint is used.

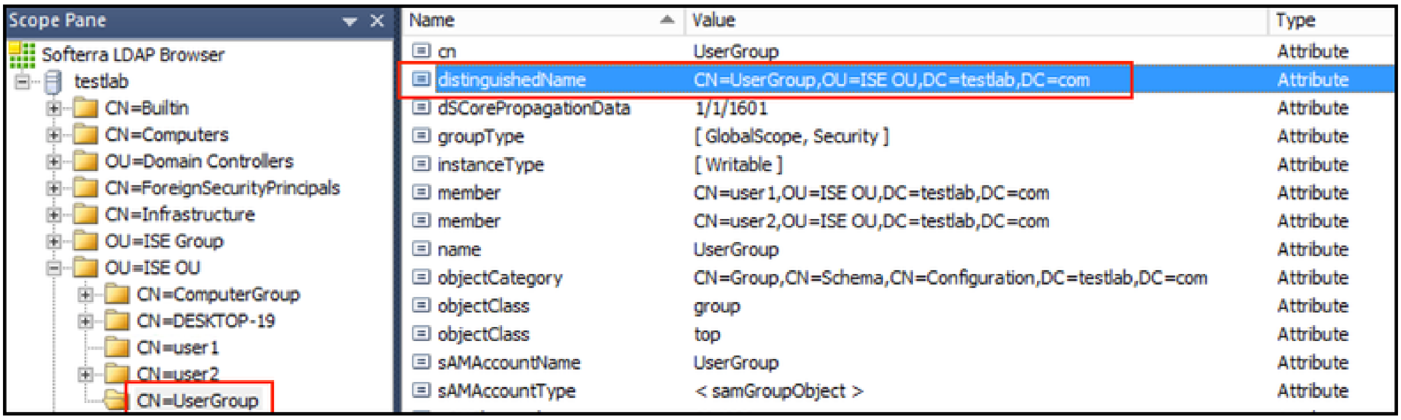


Scope Pane
Softerra LDAP Browser
testlab
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=Infrastructure
OU=ISE Group
OU=ISE OU
CN=ComputerGroup
CN=DESKTOP-19
CN=user1
CN=user2
CN=UserGroup

Filter Name: user1

Name	Value	Type
cn	user1	Attribute
displayName	user1	Attribute
distinguishedName	CN=user1,OU=ISE OU,DC=testlab,DC=com	Attribute
givenName	user1	Attribute
name	user1	Attribute
sAMAccountName	user1	Attribute
userPrincipalName	user1@testlab.com	Attribute
userCertificate	user1	Binary Attribute

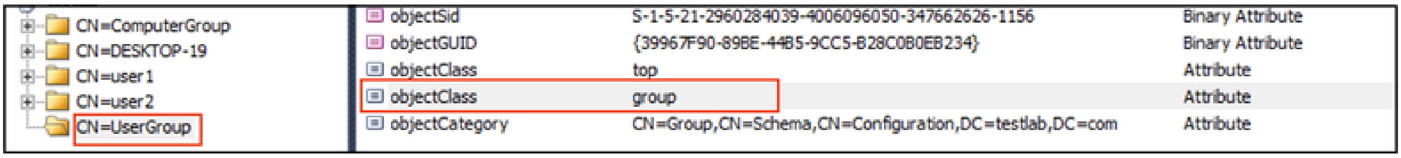
Group Name Attribute: This is the attribute holding the name of a group. The Group name attribute values in your LDAP directory must match LDAP group names on the User groups page



Scope Pane
Softerra LDAP Browser
testlab
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=Infrastructure
OU=ISE Group
OU=ISE OU
CN=ComputerGroup
CN=DESKTOP-19
CN=user1
CN=user2
CN=UserGroup

Name	Value	Type
cn	UserGroup	Attribute
distinguishedName	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute
dSCorePropagationData	1/1/1601	Attribute
groupType	[GlobalScope, Security]	Attribute
instanceType	[Writable]	Attribute
member	CN=user1,OU=ISE OU,DC=testlab,DC=com	Attribute
member	CN=user2,OU=ISE OU,DC=testlab,DC=com	Attribute
name	UserGroup	Attribute
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute
objectClass	group	Attribute
objectClass	top	Attribute
sAMAccountName	UserGroup	Attribute
sAMAccountType	< samGroupObject >	Attribute

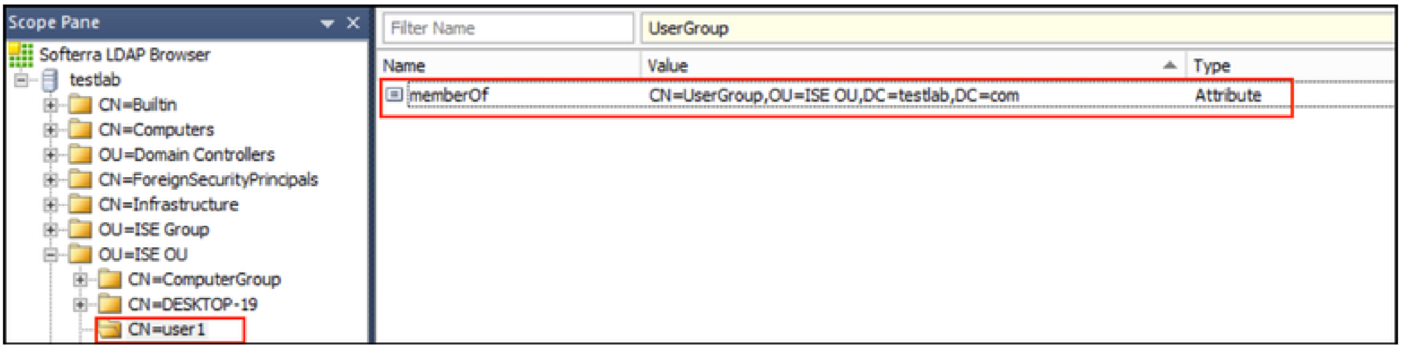
Group Objectclass: This value is used in searches to specify the objects that are recognized as groups.



CN=ComputerGroup
CN=DESKTOP-19
CN=user1
CN=user2
CN=UserGroup

objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
objectGUID	{39967F90-89BE-44B5-9CC5-B28C0B0EB234}	Binary Attribute
objectClass	top	Attribute
objectClass	group	Attribute
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute

Group Map Attribute: This attribute defines how the users are mapped to the groups.

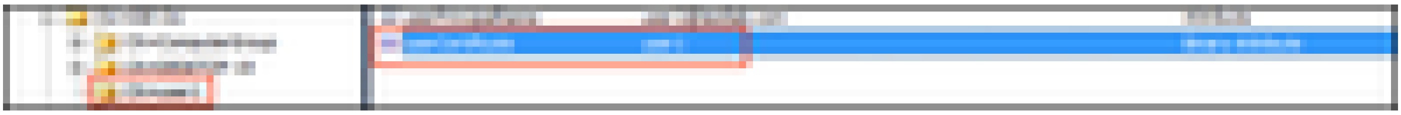


Scope Pane
Softerra LDAP Browser
testlab
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=Infrastructure
OU=ISE Group
OU=ISE OU
CN=ComputerGroup
CN=DESKTOP-19
CN=user1

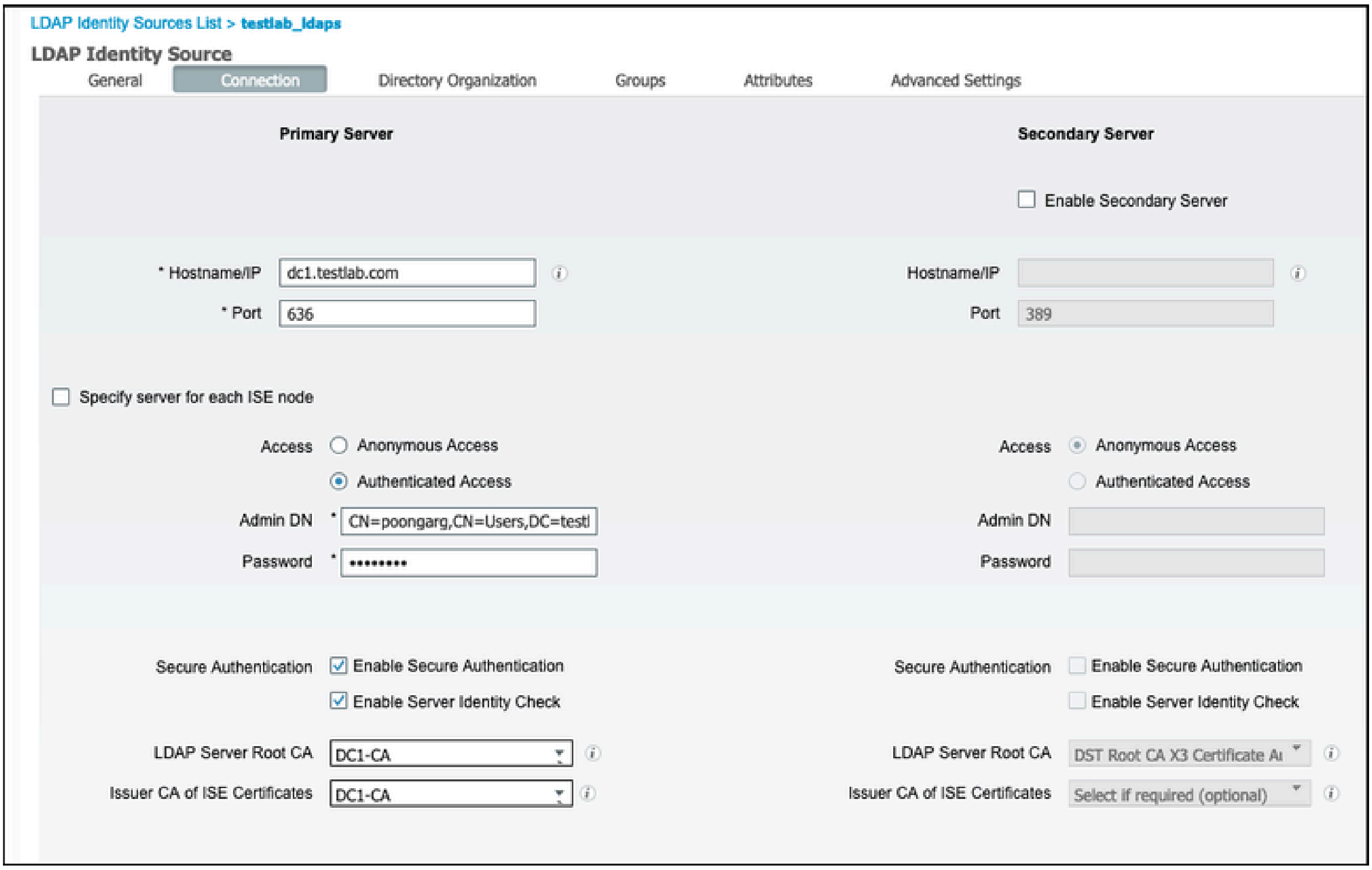
Filter Name: UserGroup

Name	Value	Type
memberOf	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute

Certificate Attribute: Enter the attribute that contains the certificate definitions. These definitions can optionally be used to validate certificates that are presented by clients when they are defined as part of a certificate authentication profile. In such cases, a binary comparison is performed between the client certificate and the certificate retrieved from the LDAP identity source.



5. In order to configure the LDAPS connection, navigate to the **Connection** tab:



LDAP Identity Sources List > testlab_ldaps

LDAP Identity Source

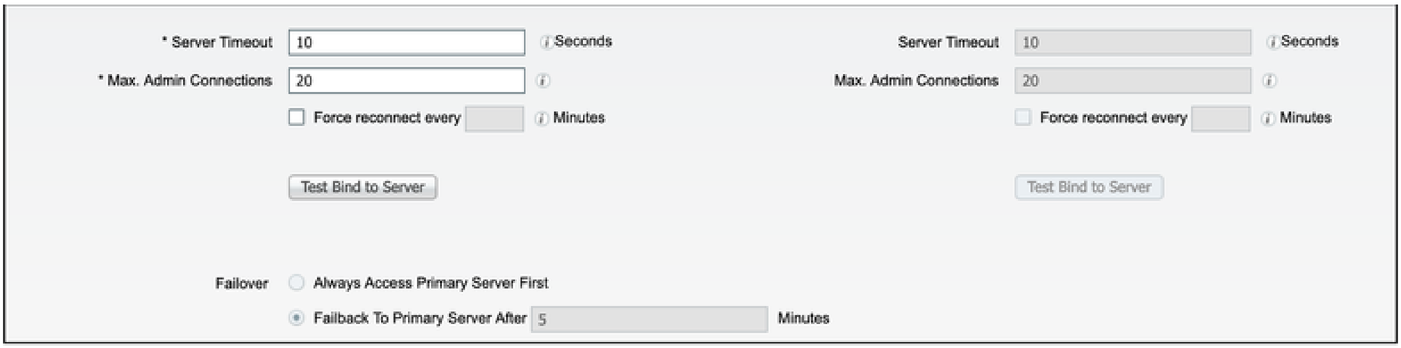
General | Connection | Directory Organization | Groups | Attributes | Advanced Settings

Primary Server

- * Hostname/IP: dc1.testlab.com
- * Port: 636
- ☐ Specify server for each ISE node
- Access: ○ Anonymous Access ● Authenticated Access
- Admin DN *: CN=poongarg,CN=Users,DC=testl
- Password *: ••••••••
- Secure Authentication: ☑ Enable Secure Authentication ☑ Enable Server Identity Check
- LDAP Server Root CA: DC1-CA
- Issuer CA of ISE Certificates: DC1-CA

Secondary Server

- ☐ Enable Secondary Server
- Hostname/IP:
- Port: 389
- Access: ● Anonymous Access ○ Authenticated Access
- Admin DN:
- Password:
- Secure Authentication: ☐ Enable Secure Authentication ☐ Enable Server Identity Check
- LDAP Server Root CA: DST Root CA X3 Certificate Au
- Issuer CA of ISE Certificates: Select if required (optional)



Primary Server

- * Server Timeout: 10 Seconds
- * Max. Admin Connections: 20
- ☐ Force reconnect every Minutes
- Test Bind to Server

Secondary Server

- Server Timeout: 10 Seconds
- Max. Admin Connections: 20
- ☐ Force reconnect every Minutes
- Test Bind to Server

Failover: ○ Always Access Primary Server First ● Failback To Primary Server After 5 Minutes

6. Run **dsquery** on Domain controller to get the username DN to be used to make a connection to LDAP server:

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

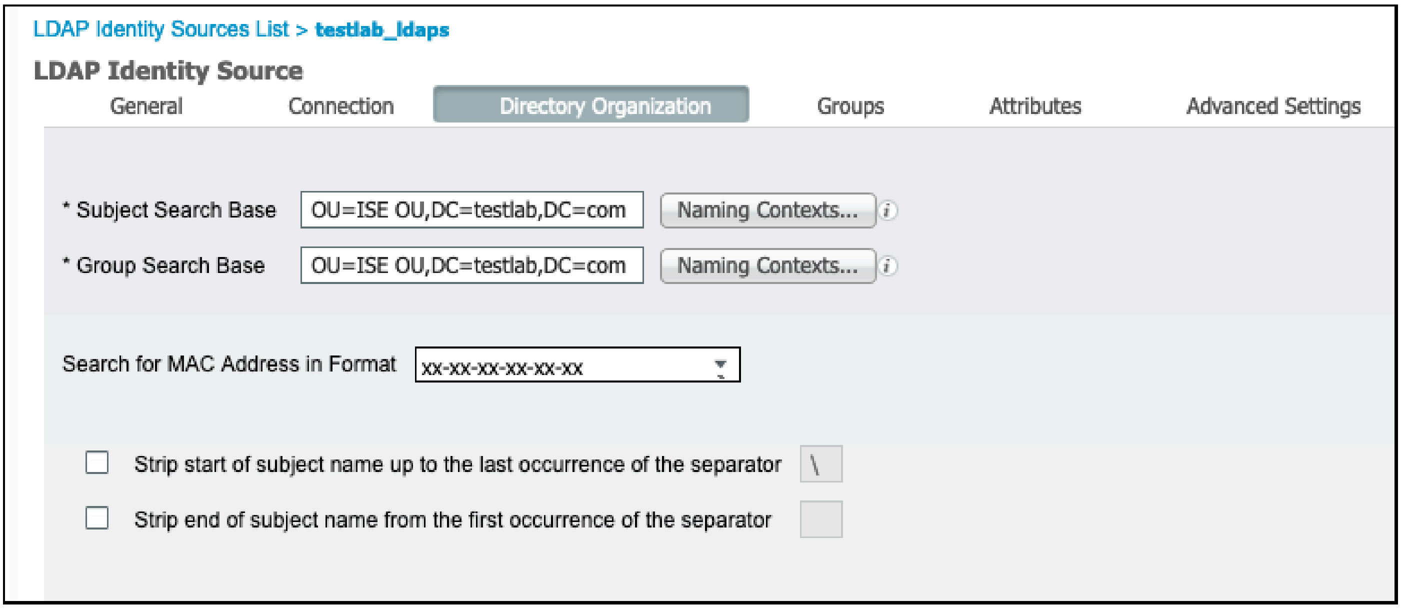
Step 1. Set the correct IP address or Hostname of the LDAP server, define the LDAPS port (TCP 636), and Admin DN to make a connection with the LDAP over SSL.

Step 2. Enable Secure Authentication and Server Identity Check option.

Step 3. From the drop-down menu, select the LDAP Server Root CA certificate and ISE admin certificate Issuer CA certificate (We have used certificate authority, installed on the same LDAP server to issue the ISE admin certificate as well).

Step 4. Select the Test Bind to server. At this point, any subjects or groups are not retrieved because the search bases are not yet configured.

7. Under **Directory Organization** tab, configure the Subject/Group Search Base. It is the join point for the ISE to the LDAP. Now you are able to retrieve only subjects and groups that are children of the joining point. In this scenario, both the subject and group are retrieved from the OU=ISE OU:



* Subject Search Base: OU=ISE OU,DC=testlab,DC=com

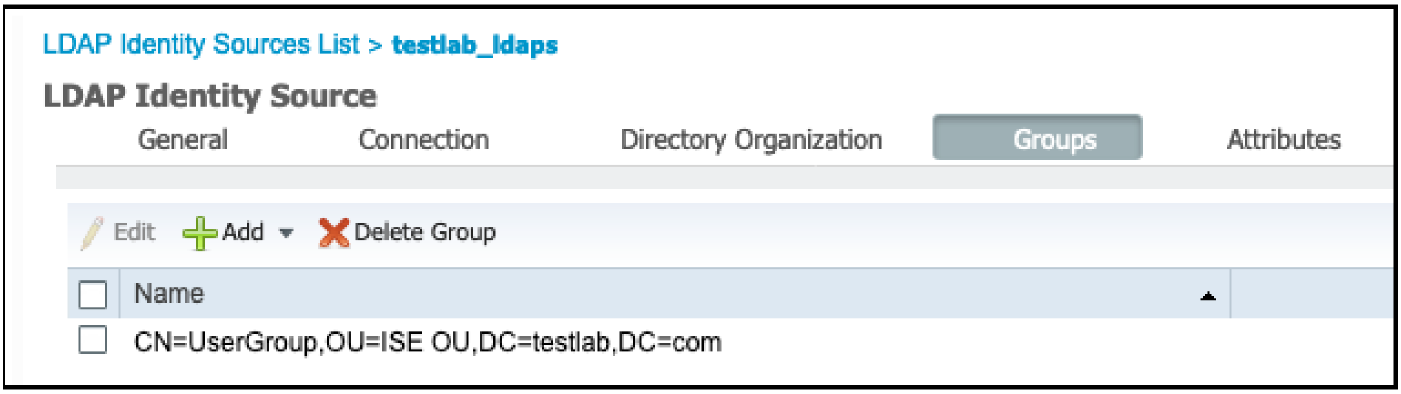
* Group Search Base: OU=ISE OU,DC=testlab,DC=com

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

8. Under Groups, click Add to import the groups from the LDAP on the ISE and retrieve the groups, as shown in this image:



□	Name
□	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com

Configure the Switch

Configure the switch for 802.1x authentication. Windows PC is connected to switchport Gig2/0/47

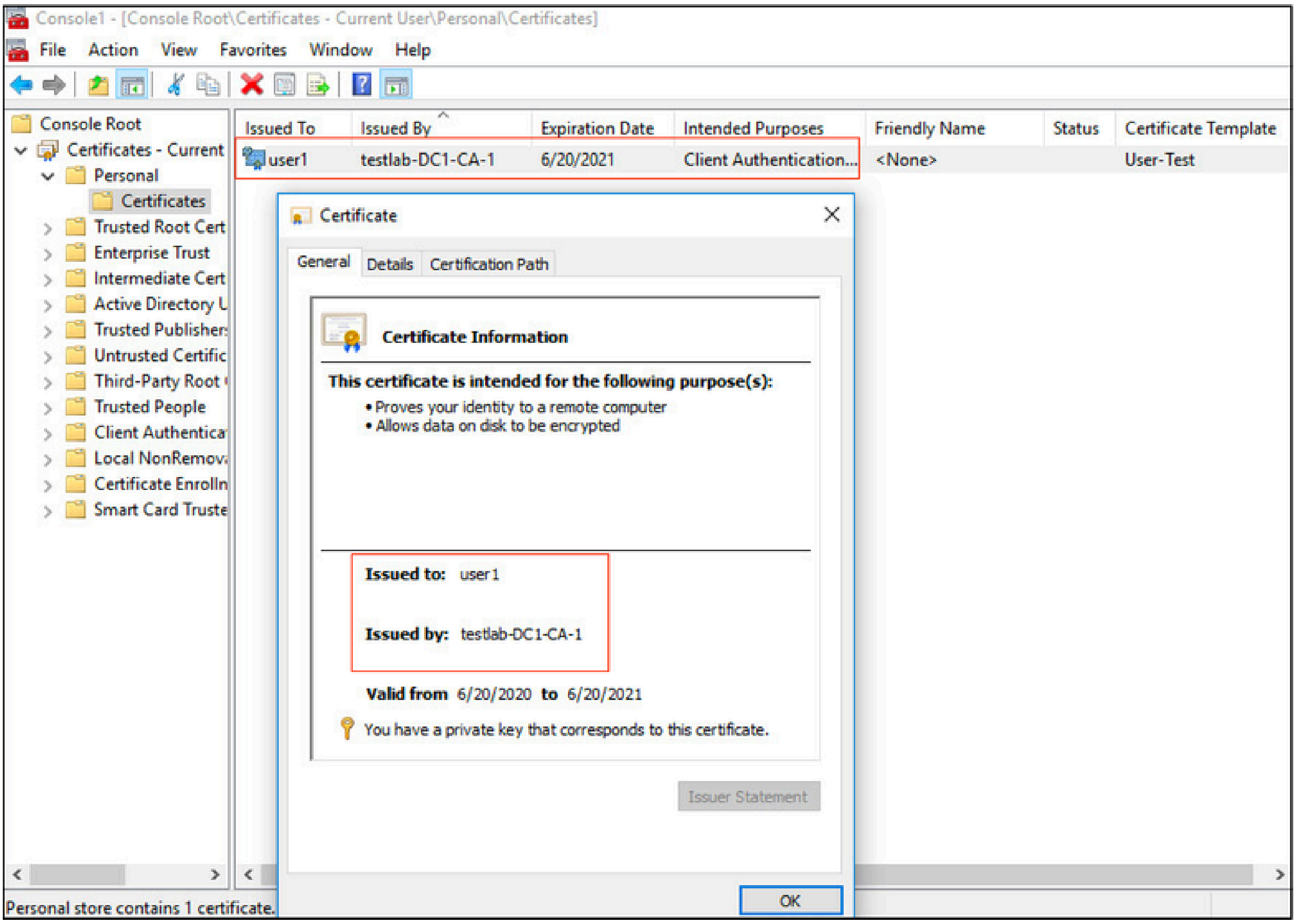
```
aaa new-model

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
```

Configure the Endpoint

Windows Native Supplicant is used and one of the LDAP supported EAP protocol is utilized, EAP-TLS for user authentication and authorization.

1. Ensure that PC is provisioned with user certificate (for user1) and have intended purpose as Client Authentication and in the Trusted Root Certification Authorities, the issuer certificate chain is present on the PC:



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
user1	testlab-DC1-CA-1	6/20/2021	Client Authentication...	<None>		User-Test

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Allows data on disk to be encrypted

Issued to: user1

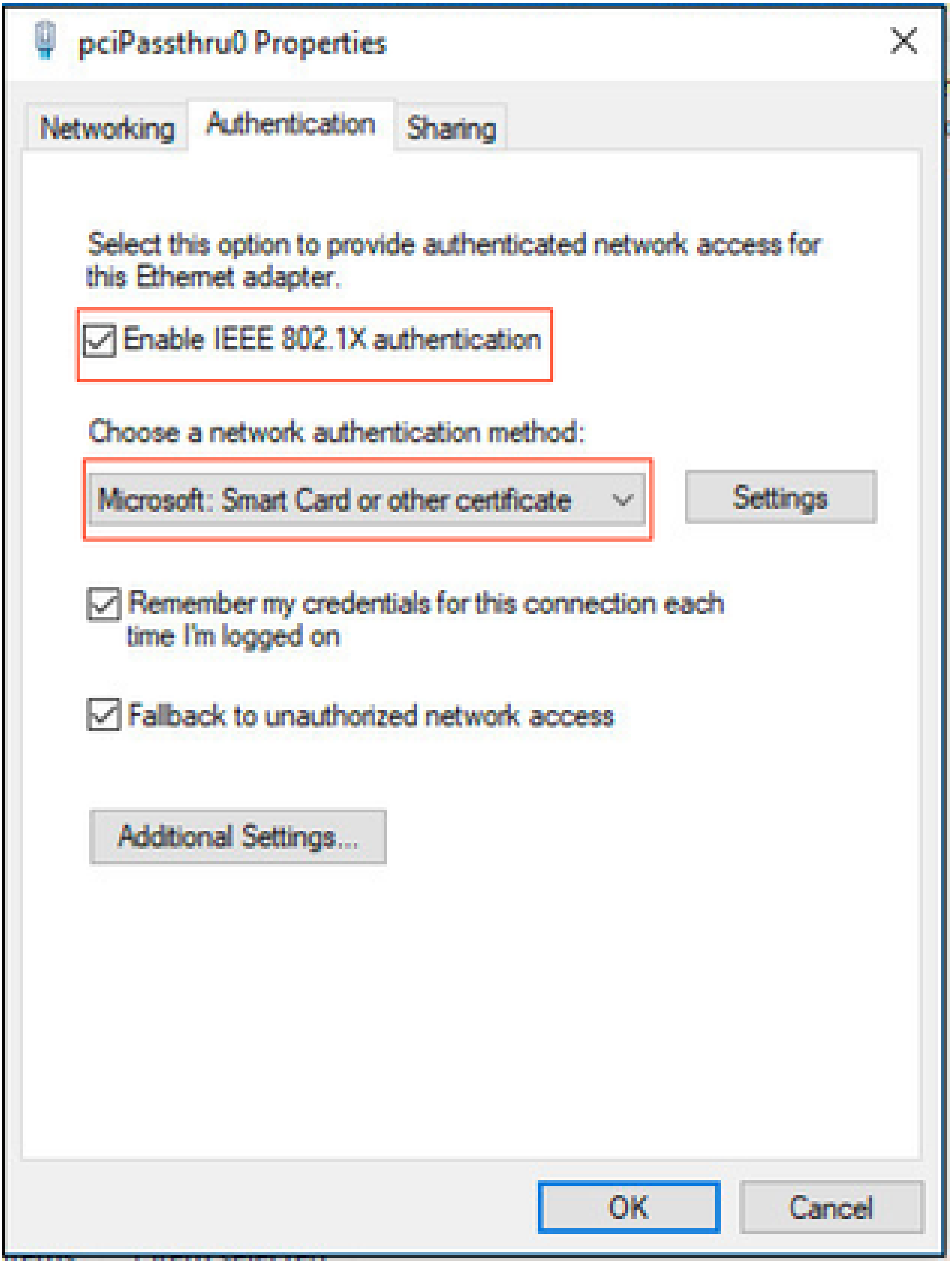
Issued by: testlab-DC1-CA-1

Valid from 6/20/2020 **to** 6/20/2021

You have a private key that corresponds to this certificate.

Personal store contains 1 certificate.

2. Enable Dot1x authentication and Select Authentication method as Microsoft:Smart Card or other certificate for EAP-TLS authentication:



pciPassthru0 Properties

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

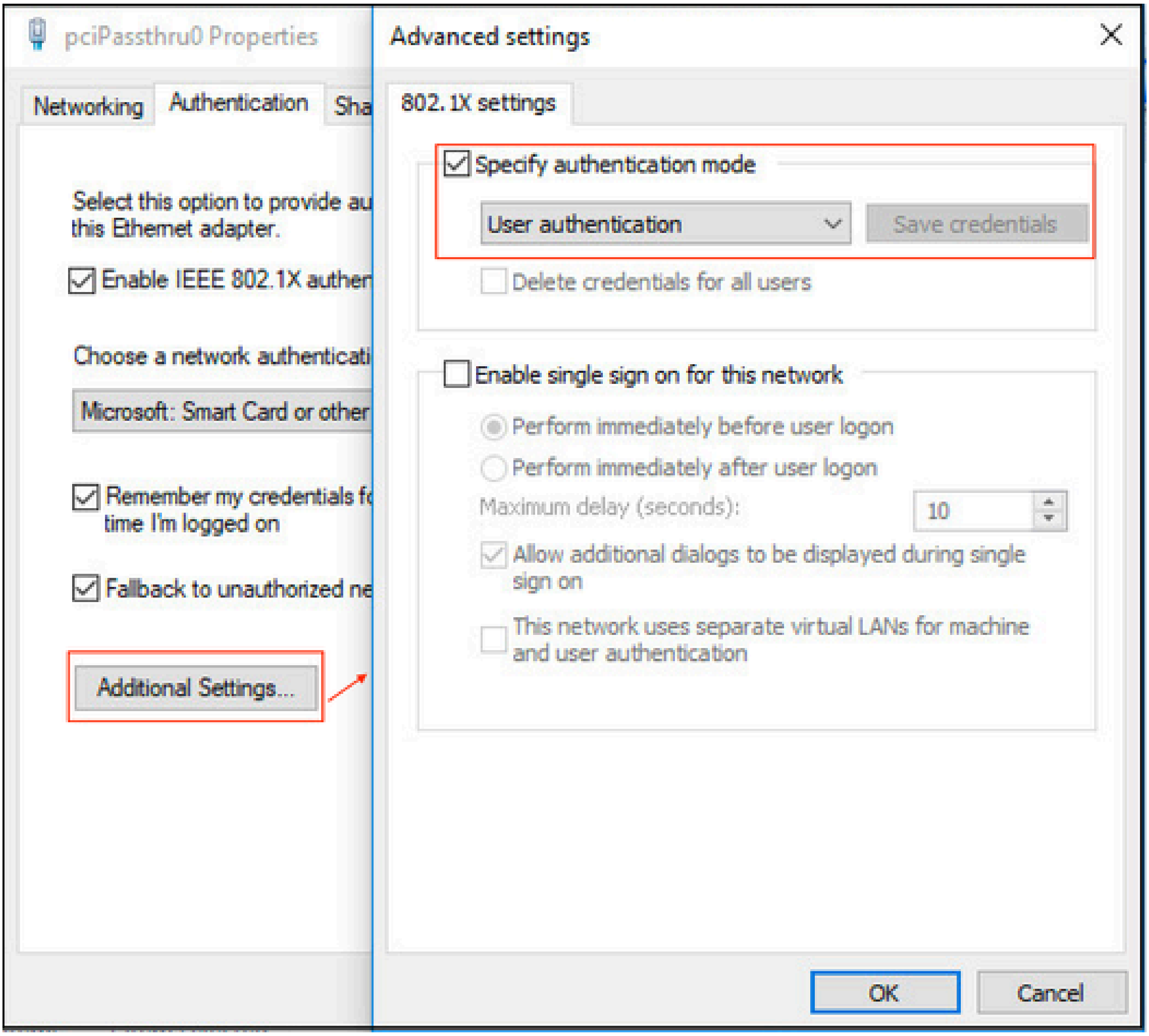
Choose a network authentication method:

Microsoft: Smart Card or other certificate

☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

3. Click on **Additional Settings**, and a window opens. Check the box with specify authentication mode and choose user authentication, as shown in this image:



pciPassthru0 Properties

Networking | Authentication | Sha

Select this option to provide au
this Ethernet adapter.

☑ Enable IEEE 802.1X authen

Choose a network authenticati

Microsoft: Smart Card or other

☑ Remember my credentials fo
time I'm logged on

☑ Fallback to unauthorized ne

Additional Settings...

Advanced settings

802.1X settings

☑ Specify authentication mode

User authentication | Save credentials

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

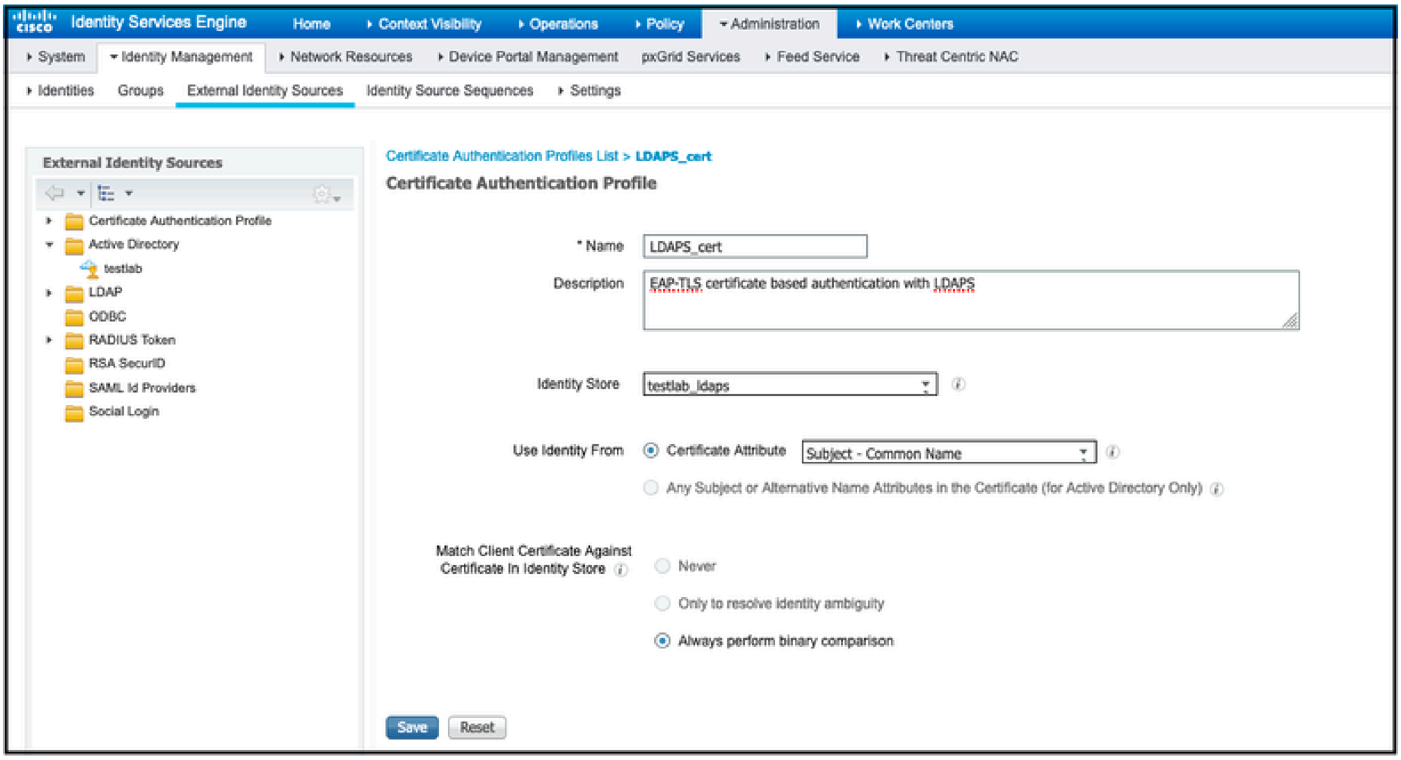
☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

OK | Cancel

Configure Policy Set on ISE

Since EAP-TLS protocol is used, before Policy Set is configured, Certificate Authentication Profile needs to be configured and the Identity Source Sequence is used in the Authentication policy later.



Certificate Authentication Profiles List > LDAPS_cert

Certificate Authentication Profile

* Name: LDAPS_cert

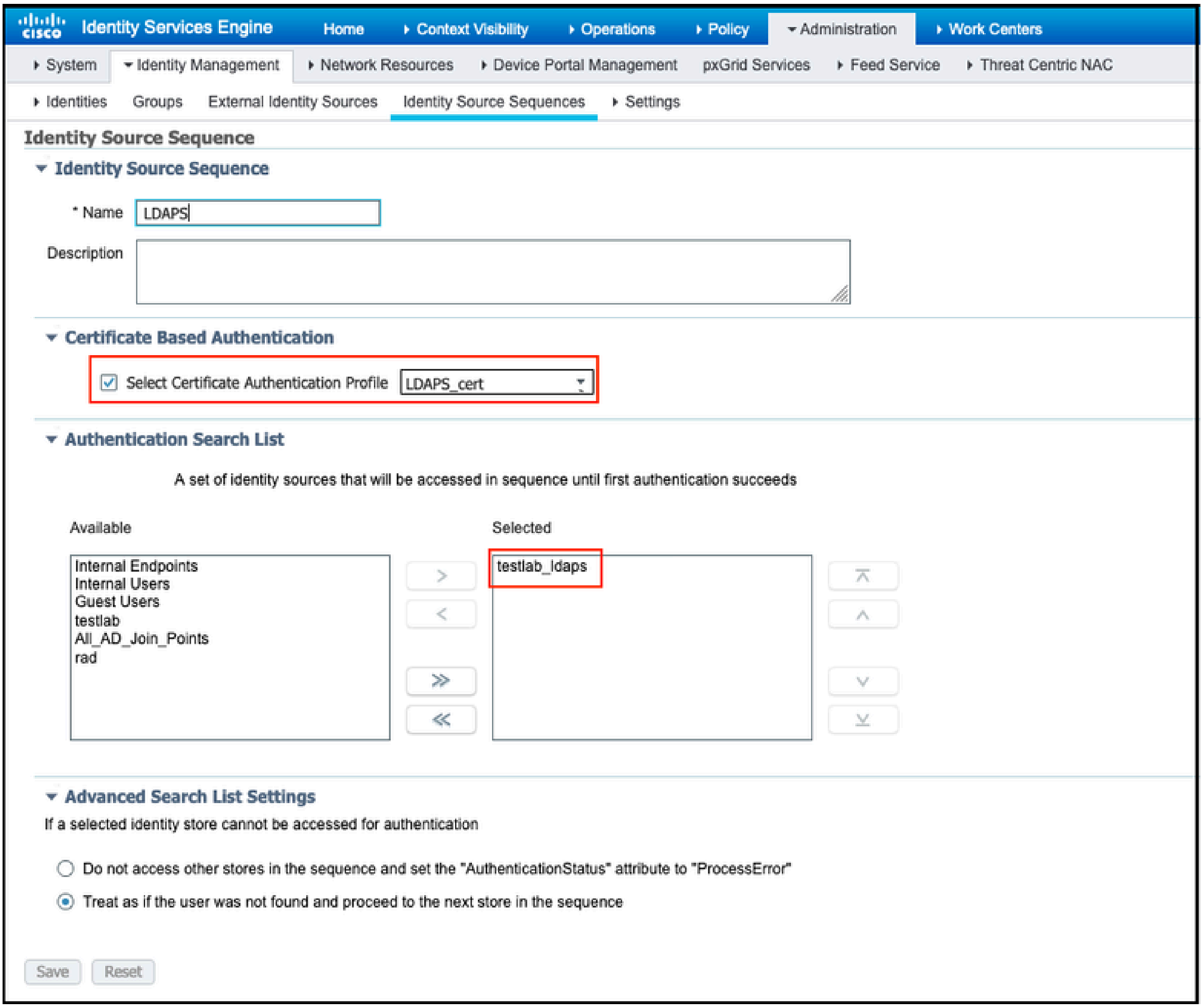
Description: EAP-TLS certificate based authentication with LDAPS

Identity Store: testlab_ldaps

Use Identity From:
● Certificate Attribute: Subject - Common Name
○ Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store:
○ Never
○ Only to resolve identity ambiguity
● Always perform binary comparison

Refer to the Certificate Authentication Profile in the Identity Source Sequence and define the LDAPS external identity source in the Authentication Search list:



Identity Source Sequence

▾ Identity Source Sequence

* Name: LDAPS

Description:

▾ Certificate Based Authentication

☑ Select Certificate Authentication Profile: LDAPS_cert

▾ Authentication Search List

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

Available:
Internal Endpoints
Internal Users
Guest Users
testlab
All_AD_Join_Points
rad

Selected:
testlab_ldaps

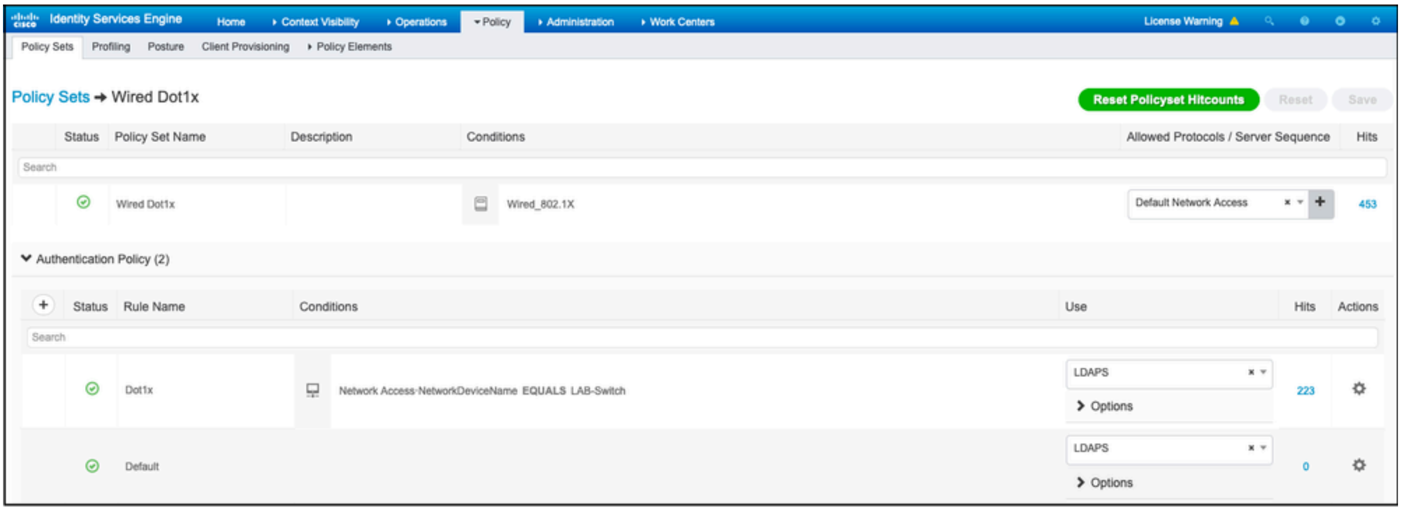
▾ Advanced Search List Settings

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

Now configure policy set for Wired Dot1x authentication:

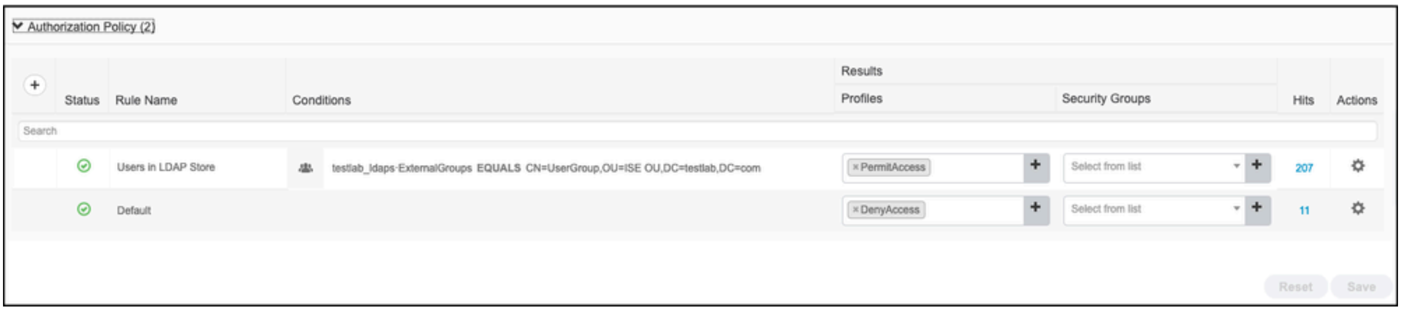


Policy Sets → Wired Dot1x

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

▾ Authentication Policy (2)

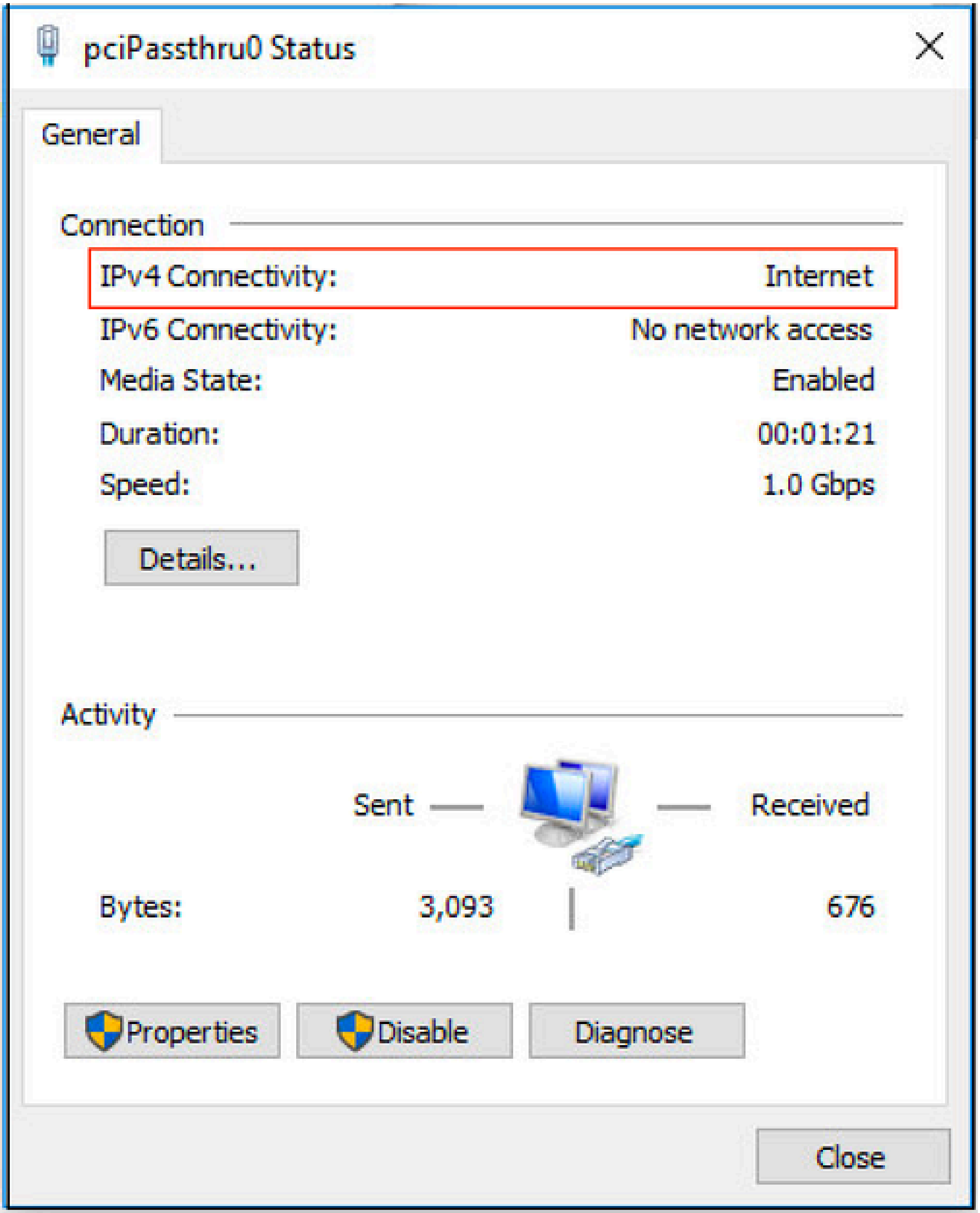
Status	Rule Name	Conditions	Use	Hits	Actions
✓	Dot1x	Network Access·NetworkDeviceName EQUALS LAB-Switch	LDAPS › Options	223	⚙
✓	Default		LDAPS › Options	0	⚙



Authorization Policy (2)

Status	Rule Name	Conditions	Results Profiles	 Security Groups	Hits	Actions
✓	Users in LDAP Store	testlab_ldaps·ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	×PermitAccess	Select from list	207	⚙
✓	Default		×DenyAccess	Select from list	11	⚙

After this configuration, authenticate the Endpoint using EAP-TLS protocol against the LDAPS Identity source.



pciPassthru0 Status

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 00:01:21

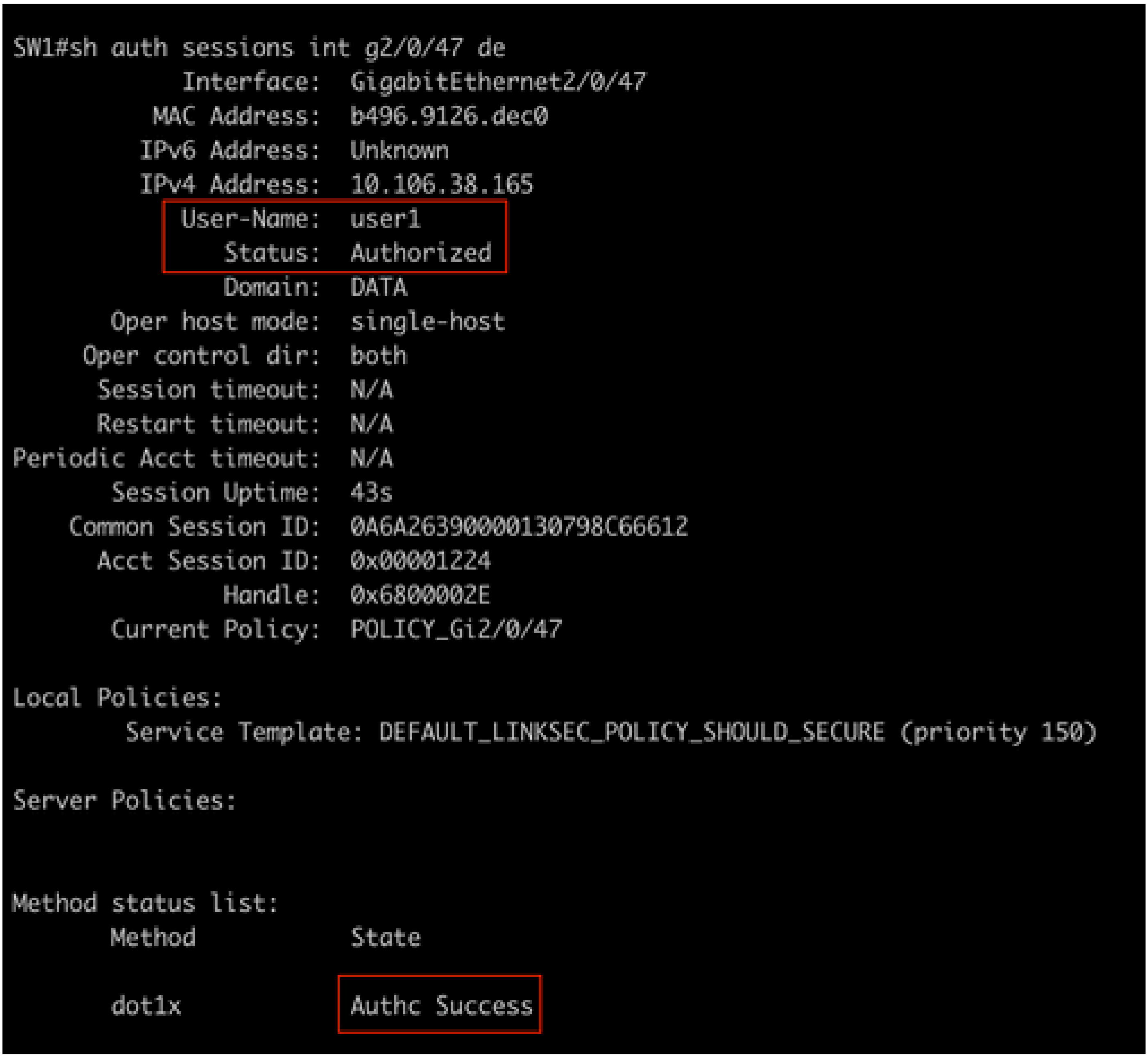
Speed: 1.0 Gbps

Activity

Bytes: Sent 3,093 Received 676

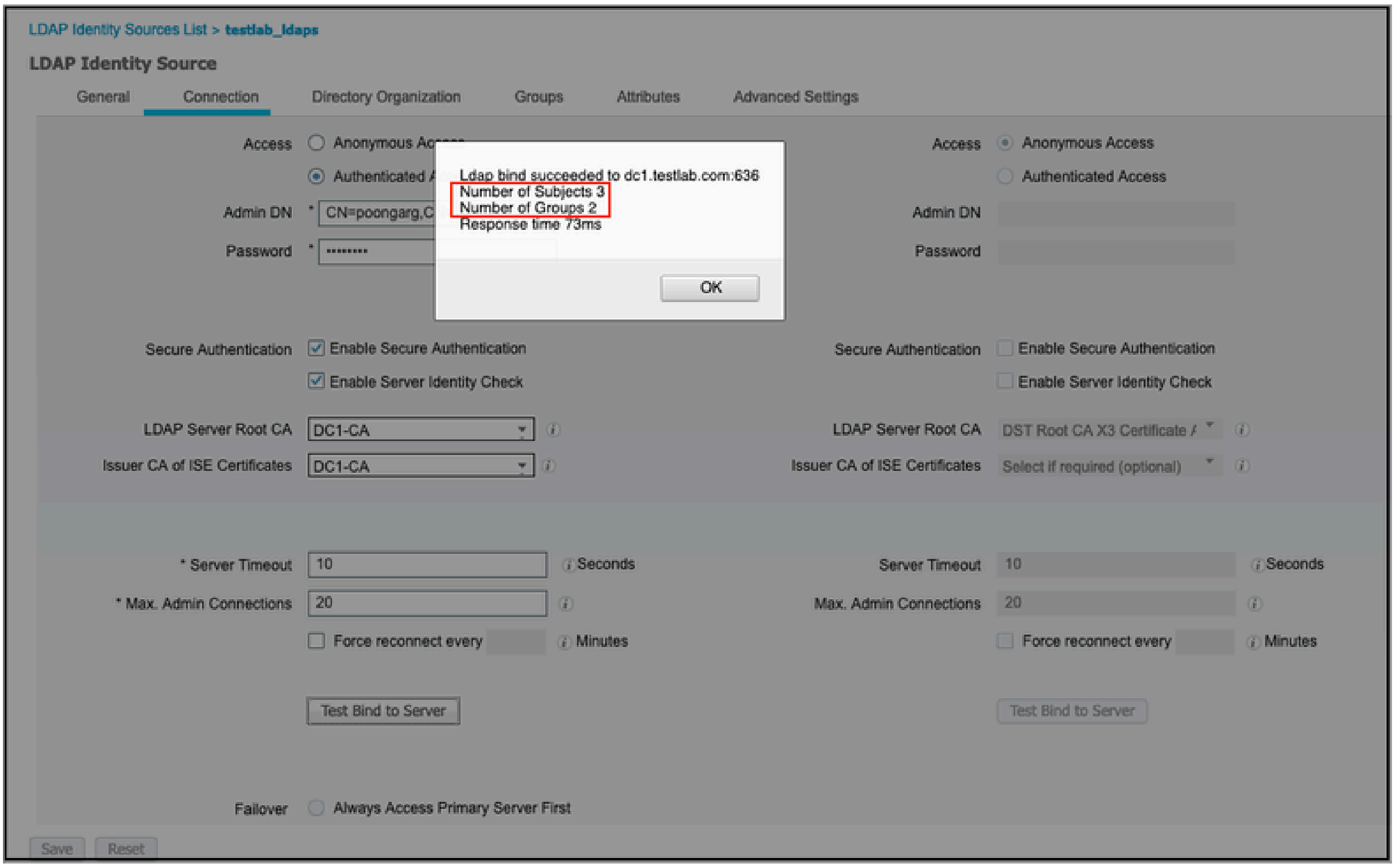
Verify

1. Check the authentication session on the switchport connected to PC:



```
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
```

2. In order to verify the LDAPS and ISE configurations, you are able to retrieve the subjects and groups with a test connection to the server:



LDAP Identity Sources List > testlab_ldaps

LDAP Identity Source

Access ○ Anonymous Access ● Authenticated Access

Admin DN * CN=poongarg,C

Password * ••••••••

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

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

Access ● Anonymous Access ○ Authenticated Access

Admin DN

Password

Secure Authentication □ Enable Secure Authentication

□ Enable Server Identity Check

LDAP Server Root CA DST Root CA X3 Certificate /

Issuer CA of ISE Certificates Select if required (optional)

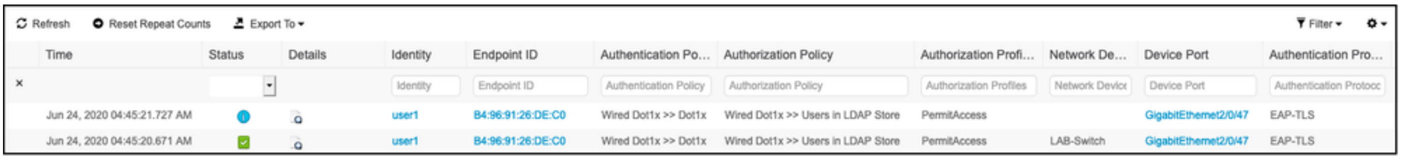
Server Timeout 10 Seconds

Max. Admin Connections 20

□ Force reconnect every Minutes

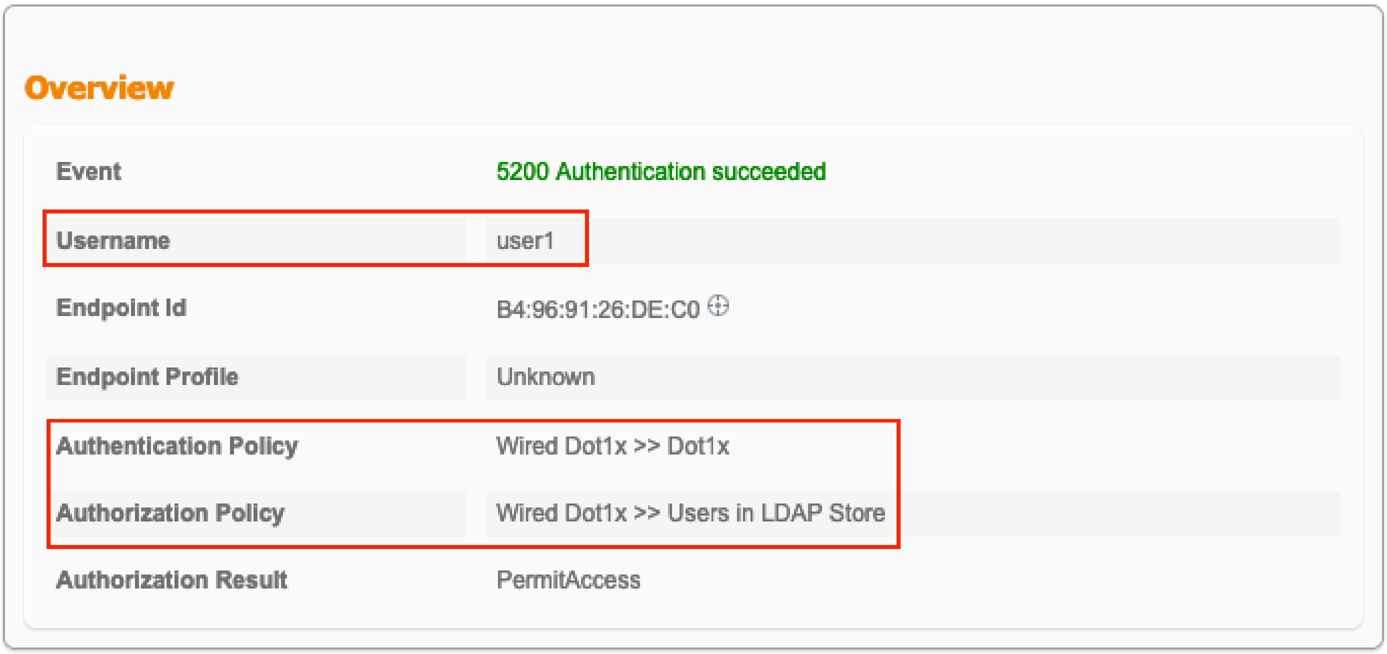
Failover ○ Always Access Primary Server First

3. Verify the user authentication report:



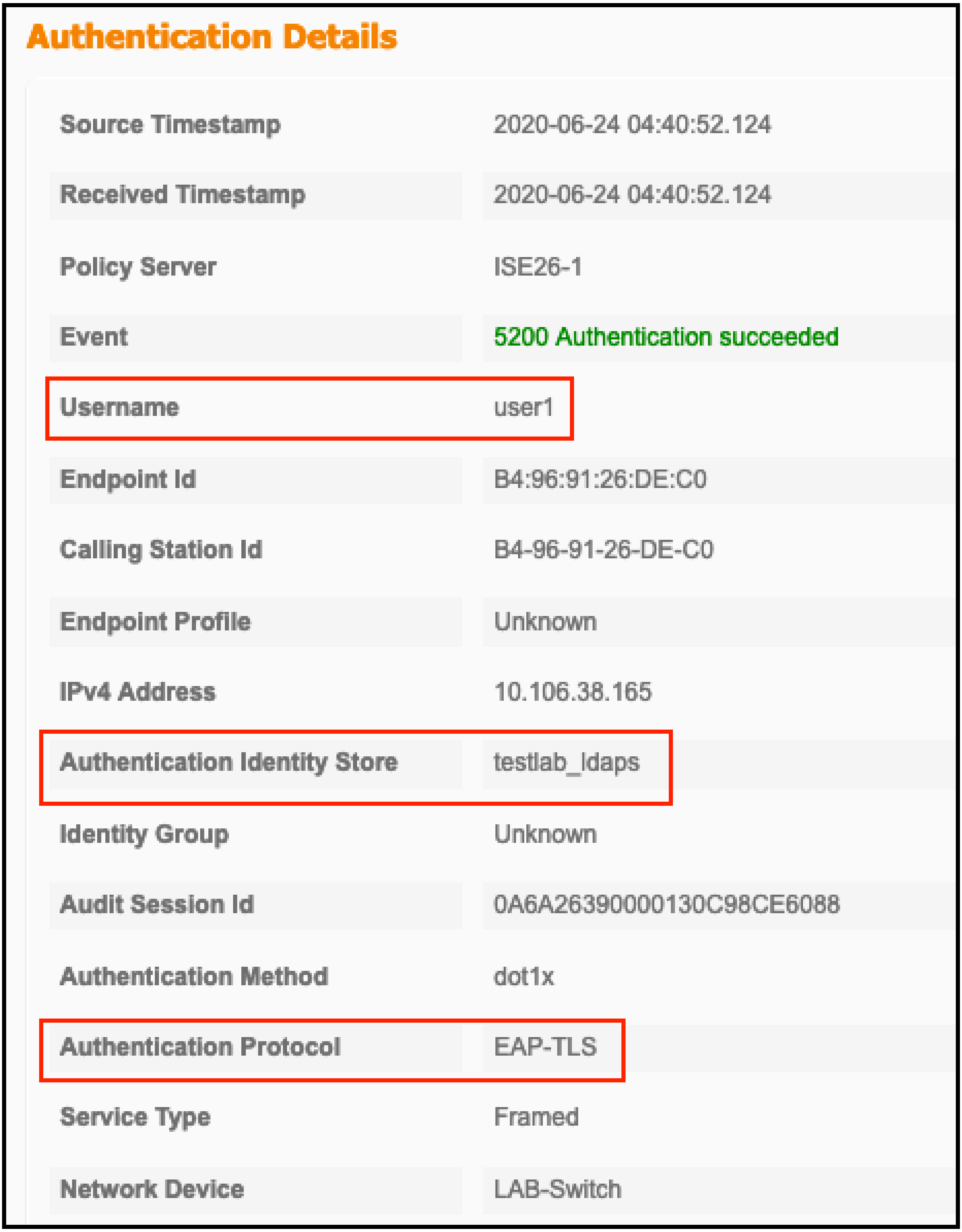
Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...	Network De...	Device Port	Authentication Pro...
Jun 24, 2020 04:45:21.727 AM	●		user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess		GigabitEthernet2/0/47	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. Check the detailed authentication report for the endpoint:



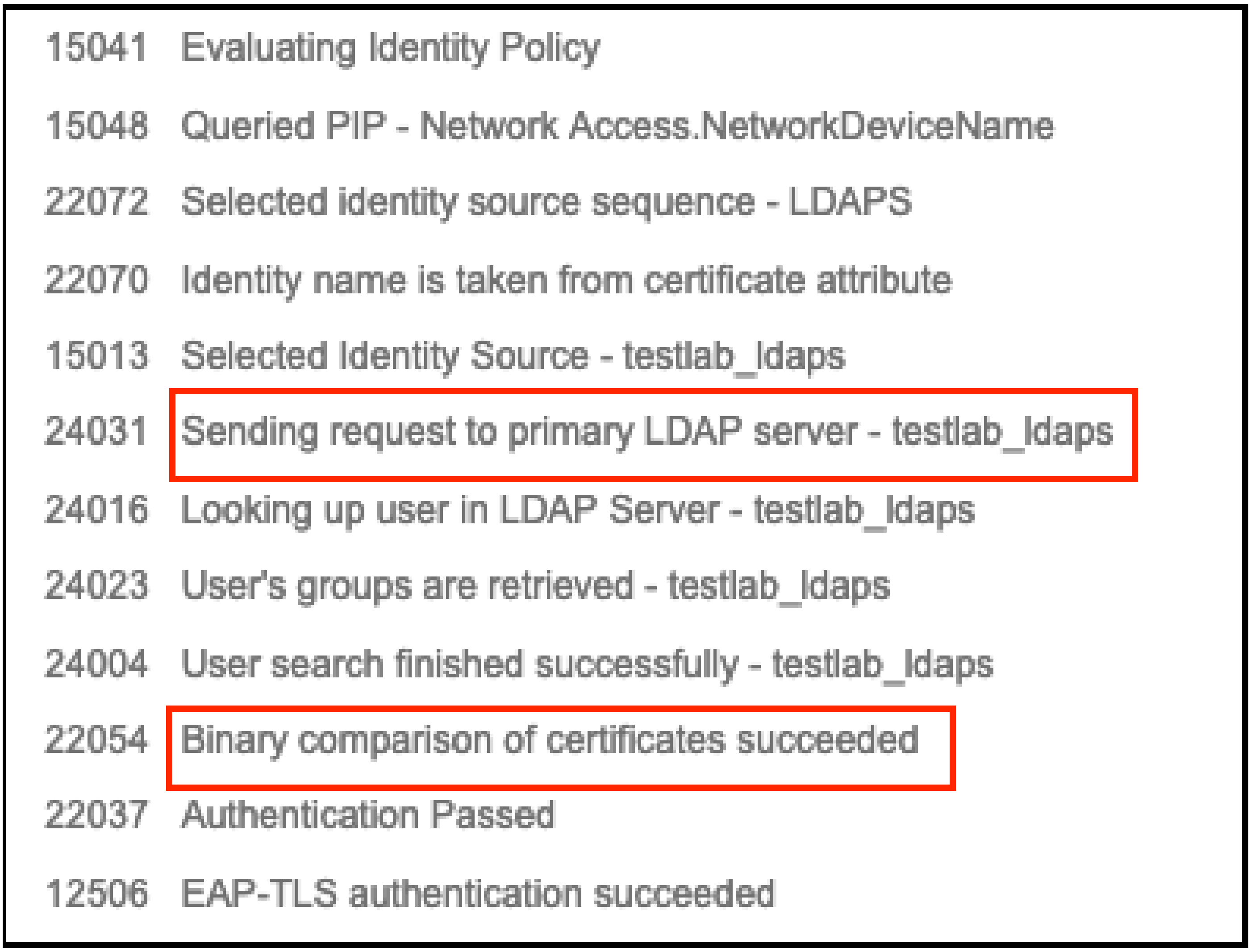
Overview

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

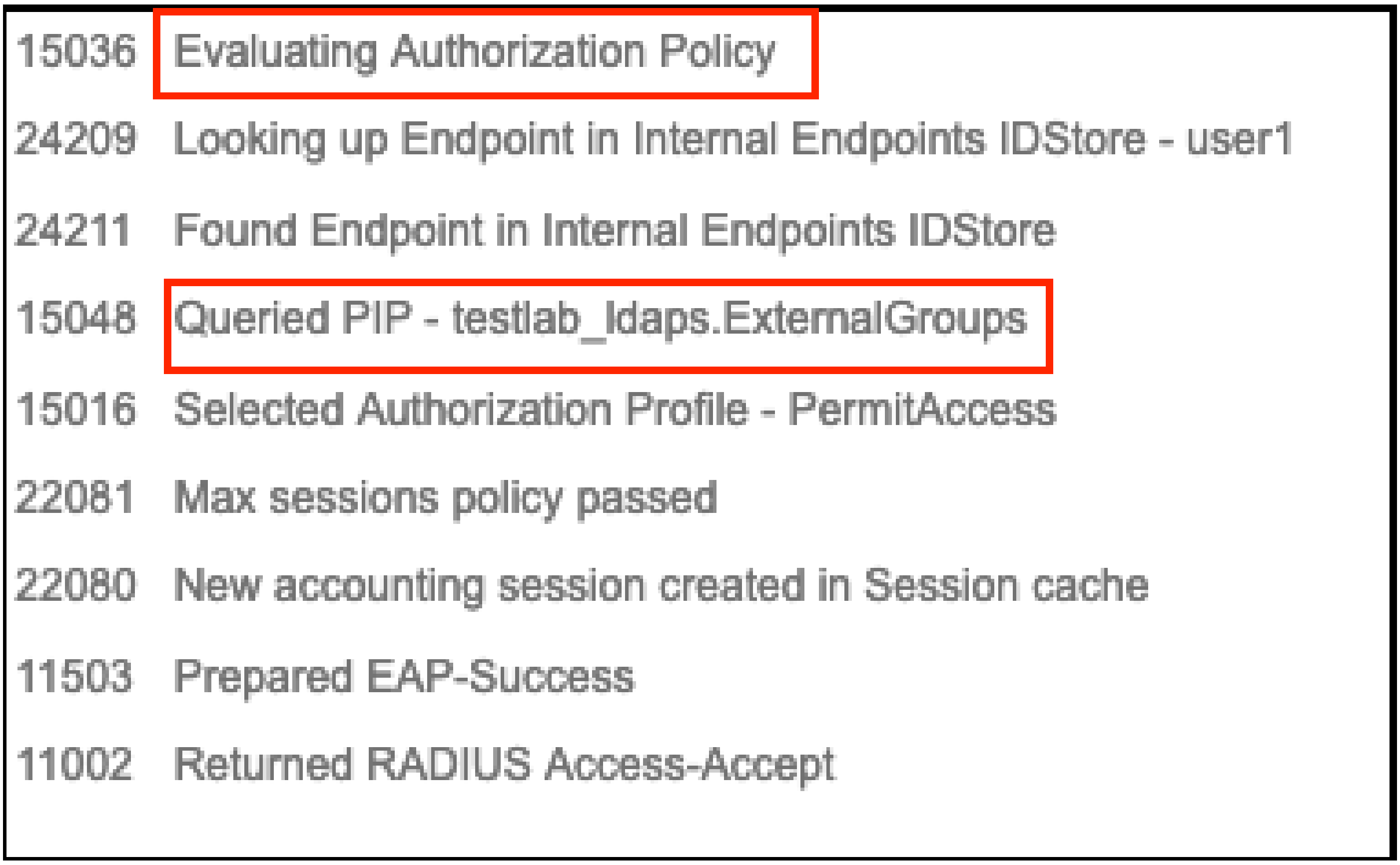


Authentication Details

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_ldaps
Identity Group	Unknown
Audit Session Id	0A6A26390000130C98CE6088
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	LAB-Switch

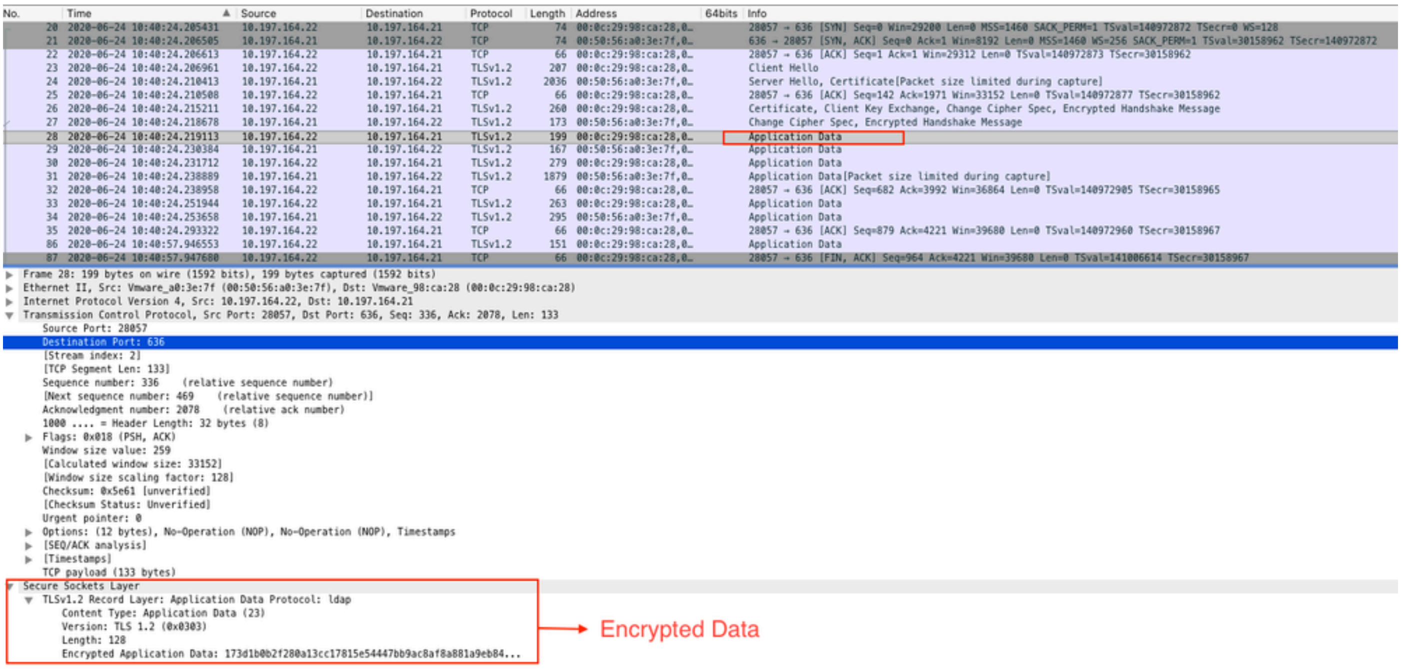


```
15041   Evaluating Identity Policy
15048   Queried PIP - Network Access.NetworkDeviceName
22072   Selected identity source sequence - LDAPS
22070   Identity name is taken from certificate attribute
15013   Selected Identity Source - testlab_ldaps
24031   Sending request to primary LDAP server - testlab_ldaps
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. Validate the data is encrypted between the ISE and LDAPS server by taking packet capture on the ISE towards the LDAPS server:



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=140972872 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 WS=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 10:40:24.238889	10.197.164.21	10.197.164.22	TLSv1.2	1879	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=682 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 10:40:57.947680	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_a0:3e: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: 173d1b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84...
```

Encrypted Data

Troubleshoot

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

1. In the authentication report, you could see this error message:

```
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).

2. Test bind to server ended with an error.

Most commonly this is due to the LDAPS server certificate validation check failure. In order to troubleshoot such types of issues, take a packet capture on ISE and enable all the three runtime and prrt-jni components at debug level, recreate the issue, and check the prrt-server.log file.

Packet capture complains about a bad certificate and prrt-server shows:

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

Note: The hostname in the LDAP page must be configured with the subject name of the certificate (or any of the Subject Alternate Name). So unless you have such in the subject or SAN, it does not work,

✎ the certificate with the IP address in the SAN list is needed.

3. In the authentication report, you could notice that the subject was not found in the identity store. This means that 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 sAMAccountName for this attribute, which means that the ISE looks to the sAMAccountName values for the LDAP user when it attempts to find a match.

4. The subjects and groups could not be retrieved correctly during a bind to server test. The most probable cause of this issue 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).

Related Information

- **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**