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.

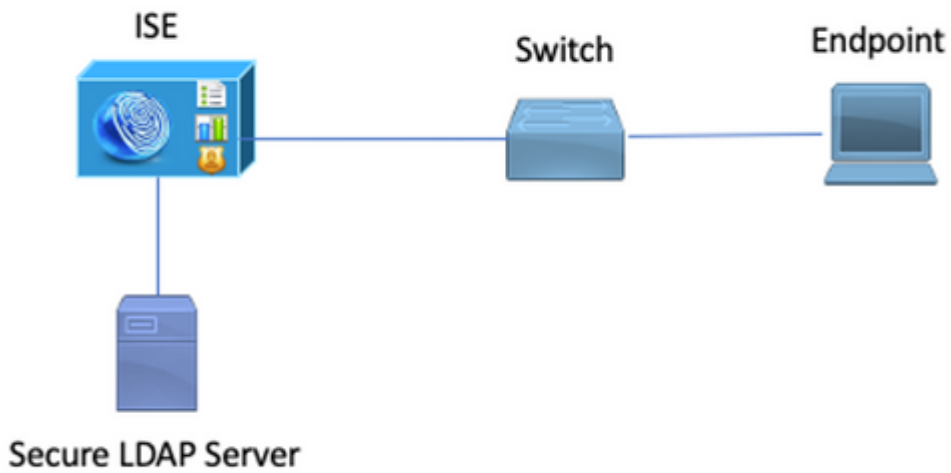
Configure

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's Personal Certificate Store.

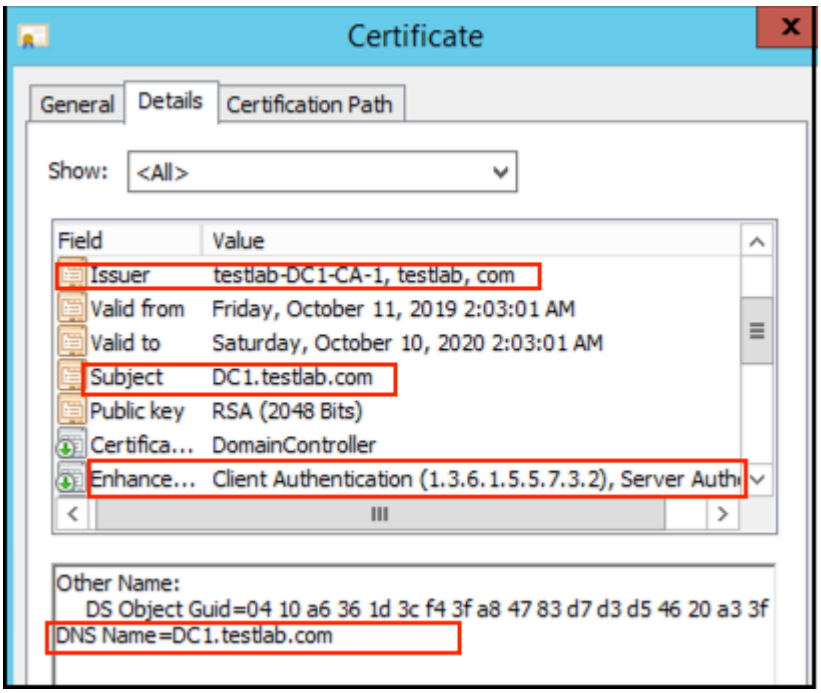
2. A private key that matches the certificate is present in the Domain Controller's store and is correctly associated with the certificate.

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.



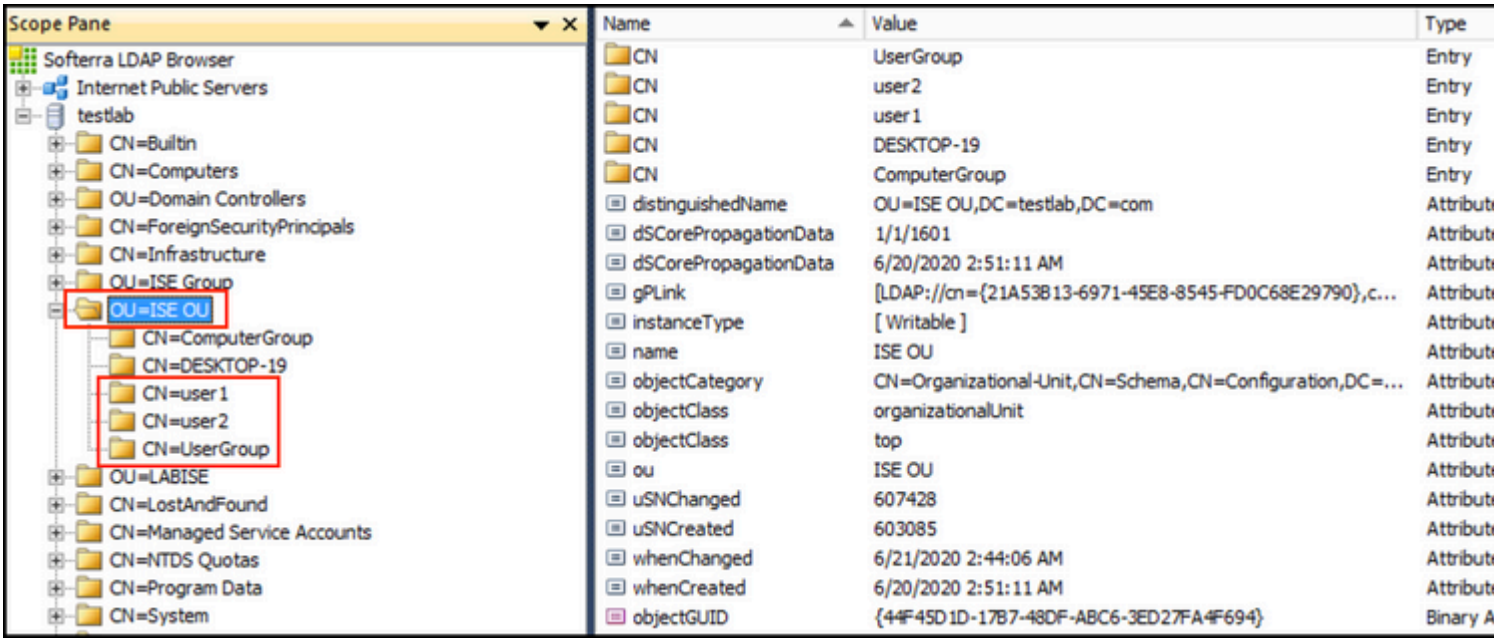
Access LDAPS Directory Structure

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.

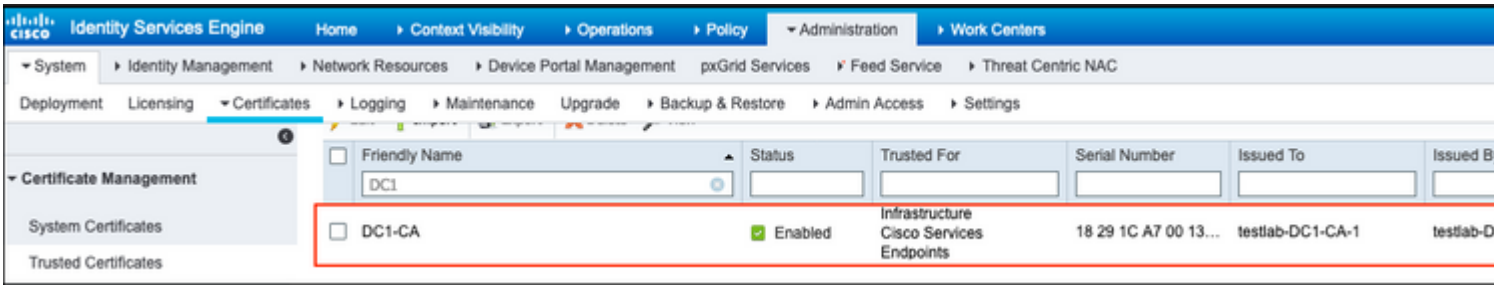
2. For simplicity, Create an Organizational Unit (OU) named ISE OU in the AD, and it must have a Group named UserGroup. Create two users (user1 and user2) and make them members of the group UserGroup.

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



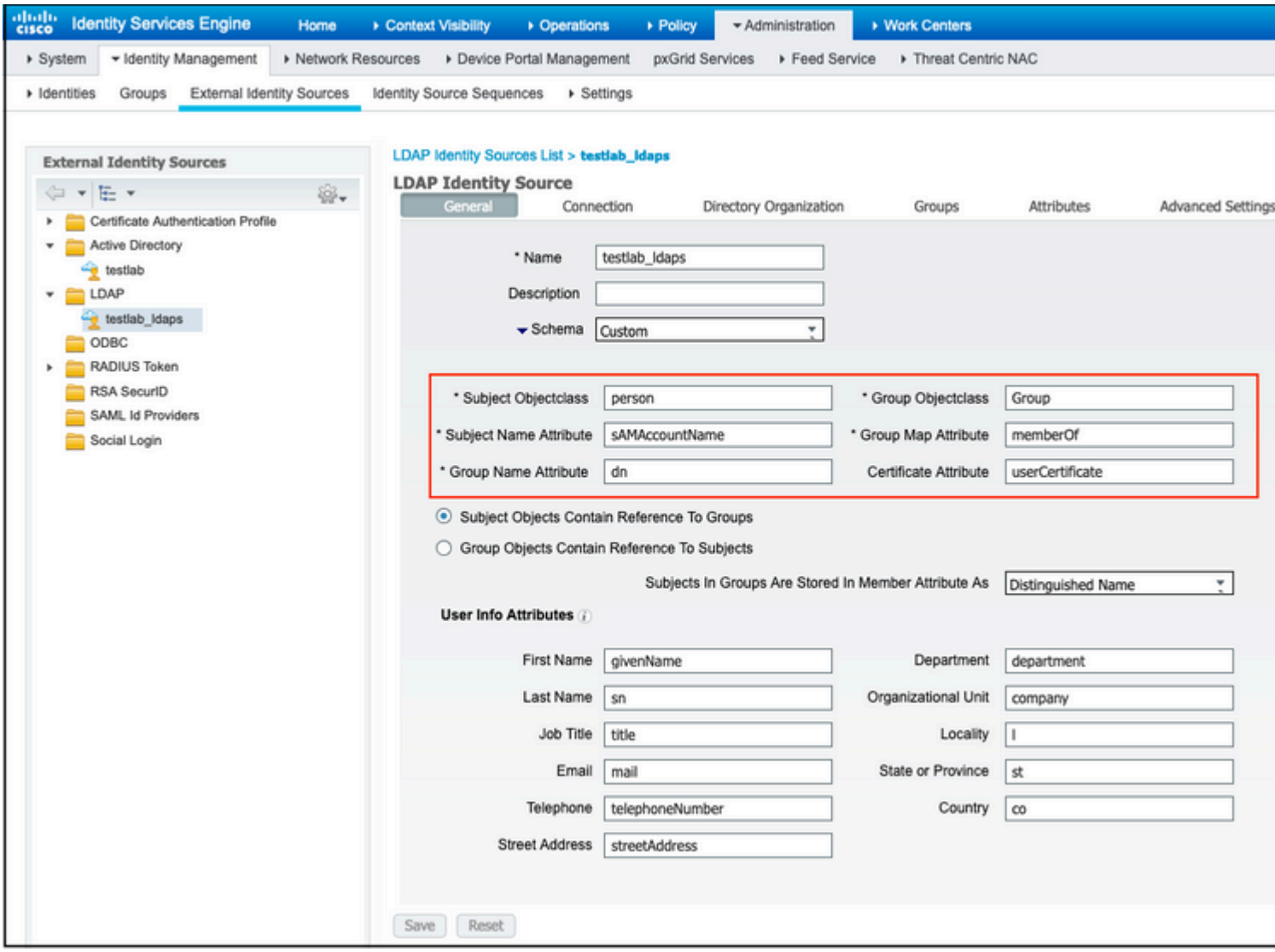
Integrate ISE with LDAPS Server

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



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

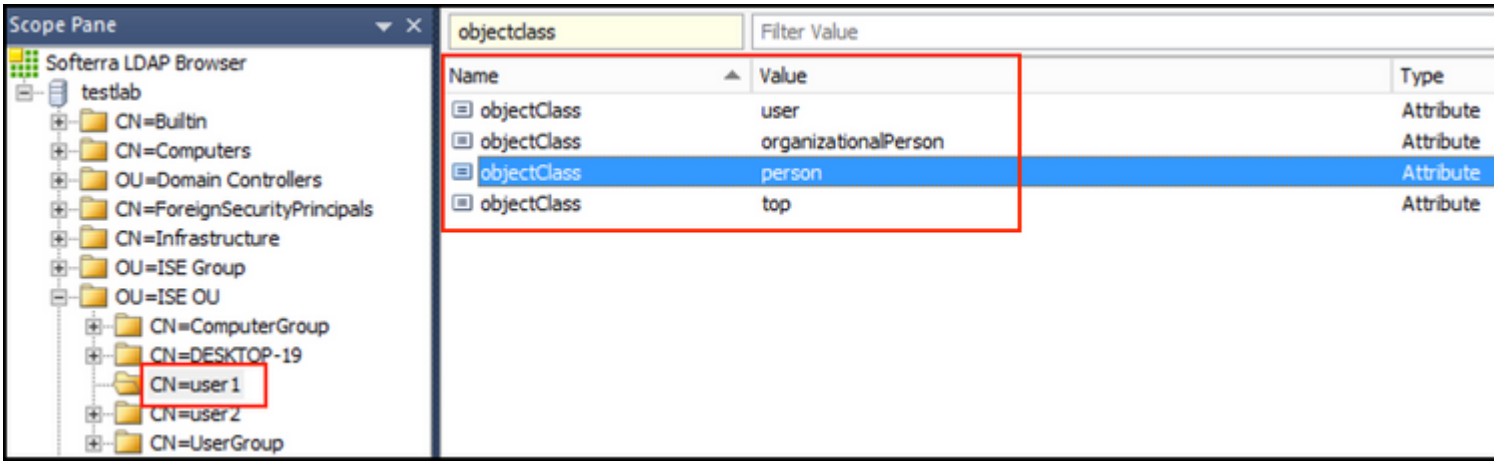
3. In order to integrate the LDAPS server, make use of the different LDAP attributes from the LDAPS directory. Navigate to **Administration > Identity Management > External Identity Sources > LDAP Identity Sources > Add**.



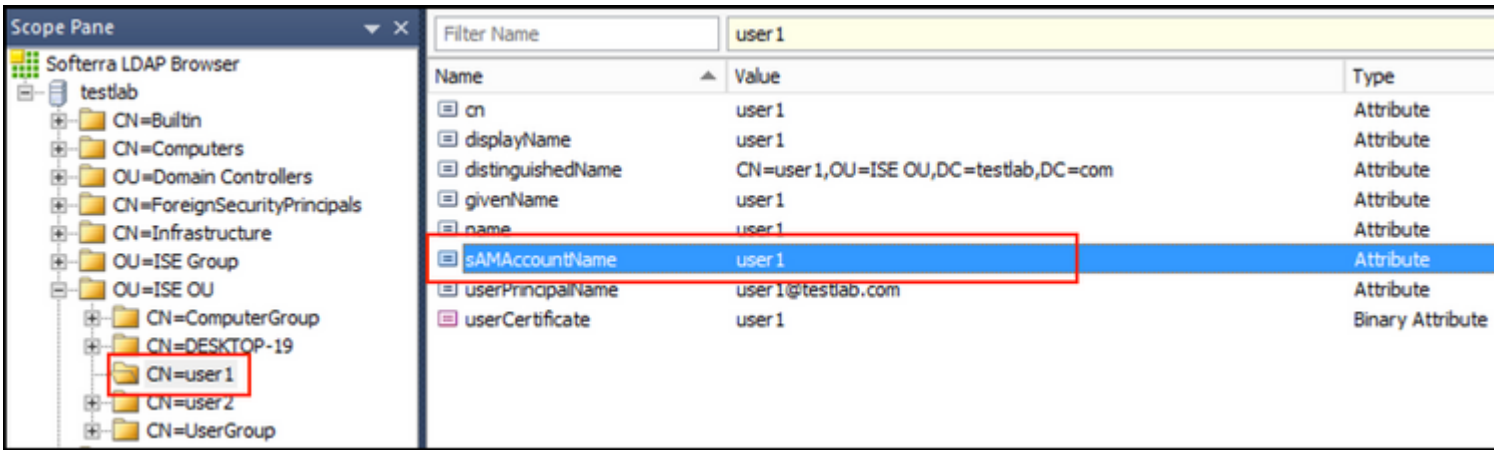
4. Configure these attributes from the General Tab:

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

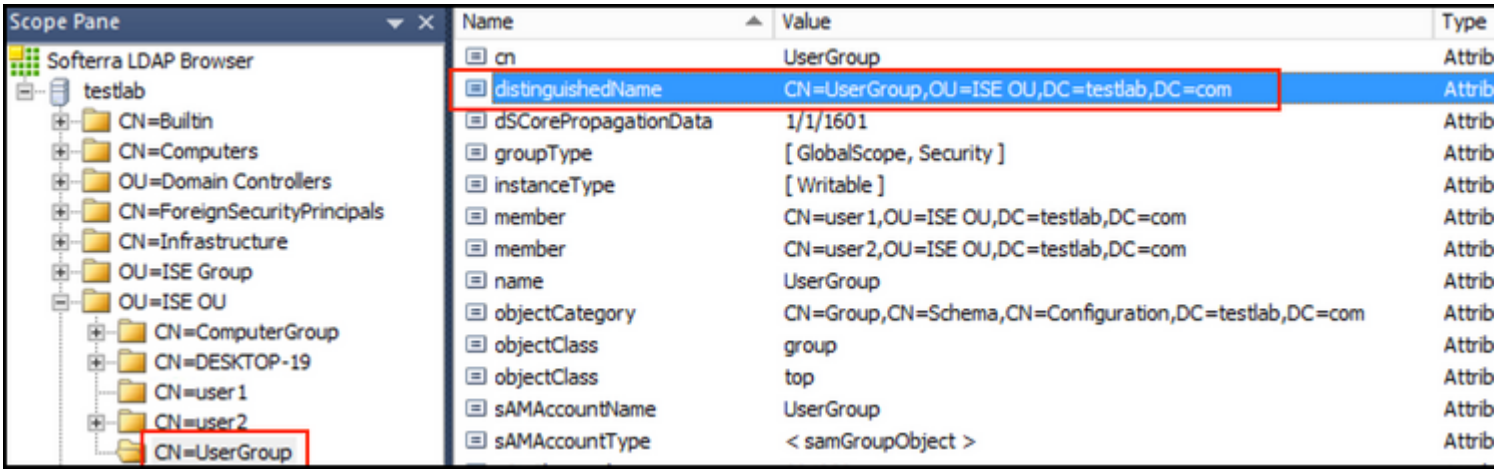
- Top
- Person
- OrganizationalPerson
- InetOrgPerson



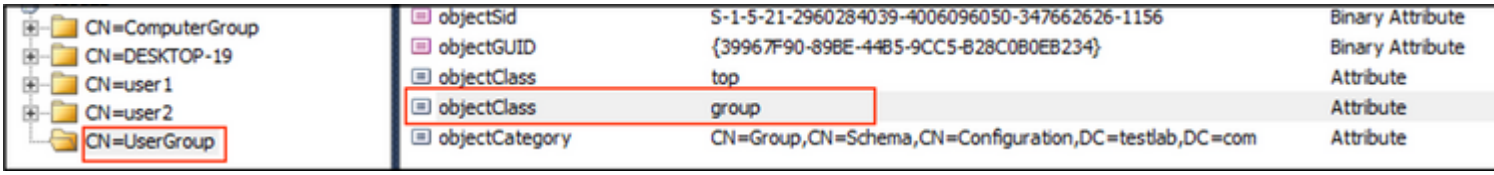
Subject Name Attribute: This field is the name of the attribute containing the username from the request. This attribute is retrieved from the LDAPS when the ISE inquires a specific user name in the LDAP database (you can use cn, sAMAccountName, etc). In this scenario, user1 username on the endpoint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



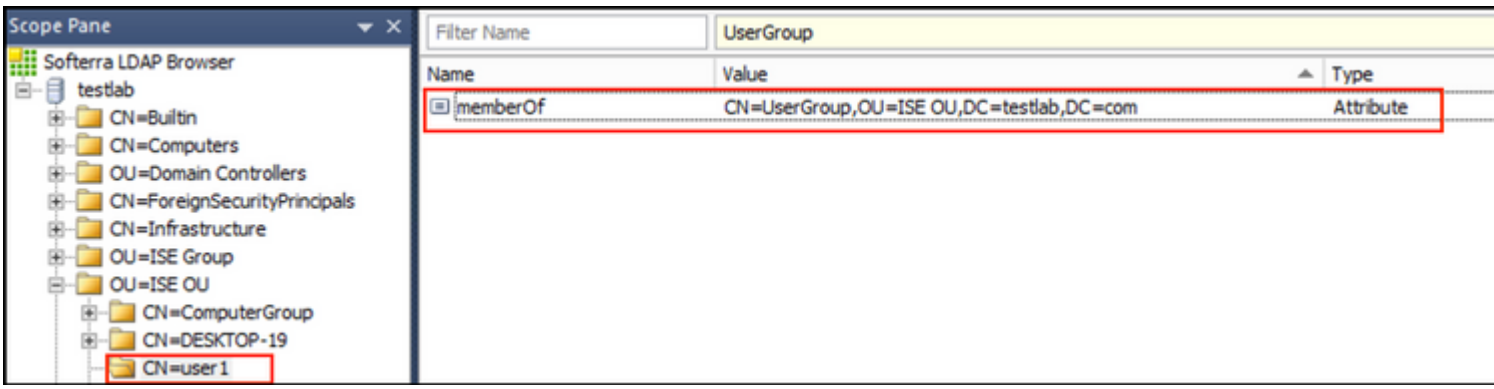
Group Name Attribute: This is the attribute holding the name of a group. The Group name attribute values in your LDAP directory must match LDAP group names on the User groups page



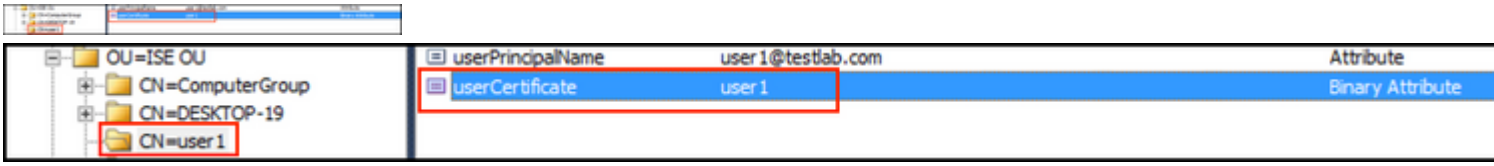
Group Objectclass: This value is used in searches to specify the objects that are recognized as groups.



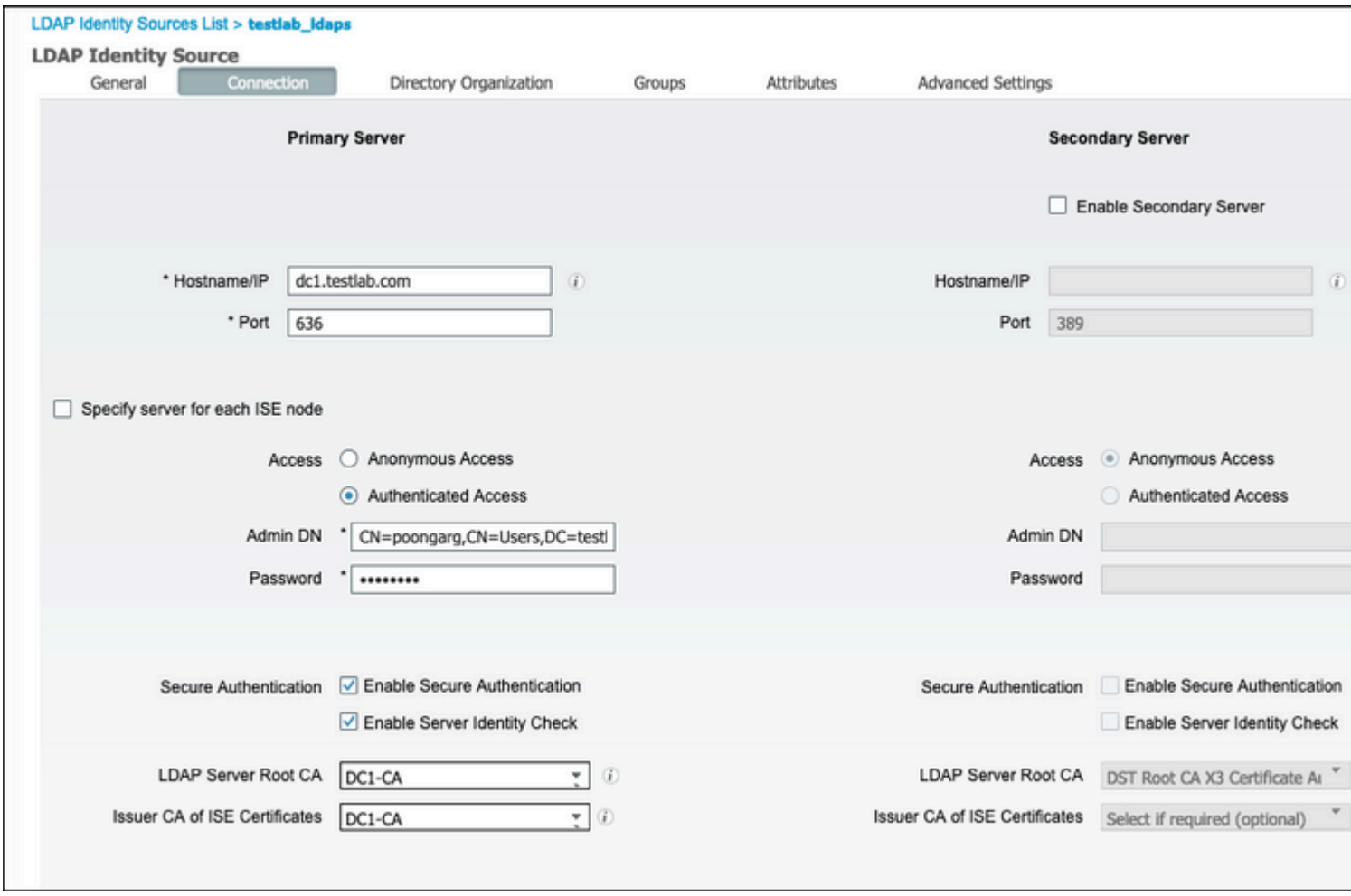
Group Map Attribute: This attribute defines how the users are mapped to the groups.

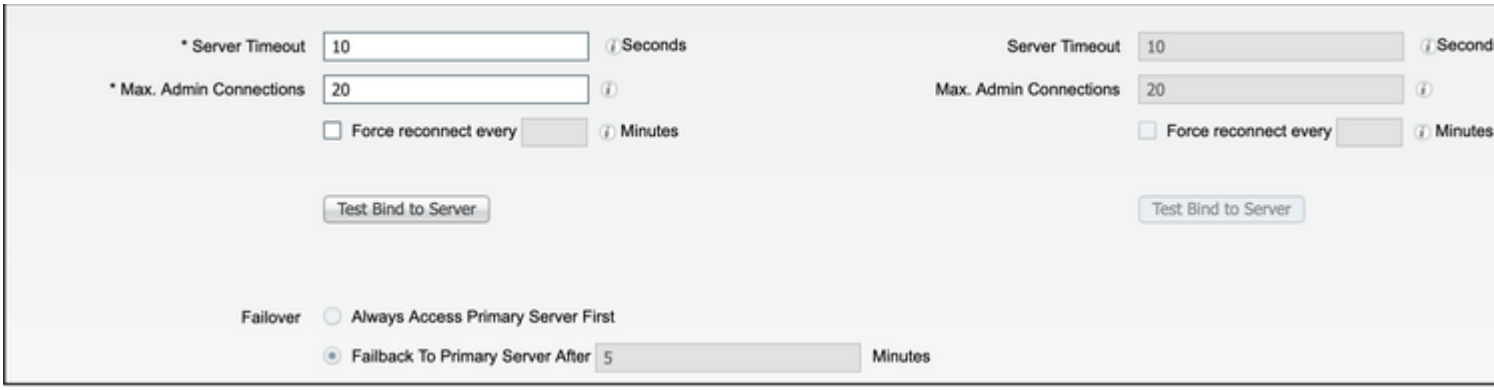


Certificate Attribute: Enter the attribute that contains the certificate definitions. These definitions can optionally be used to validate certificates that are presented by clients when they are defined as part of a certificate authentication profile. In such cases, a binary comparison is performed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





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"

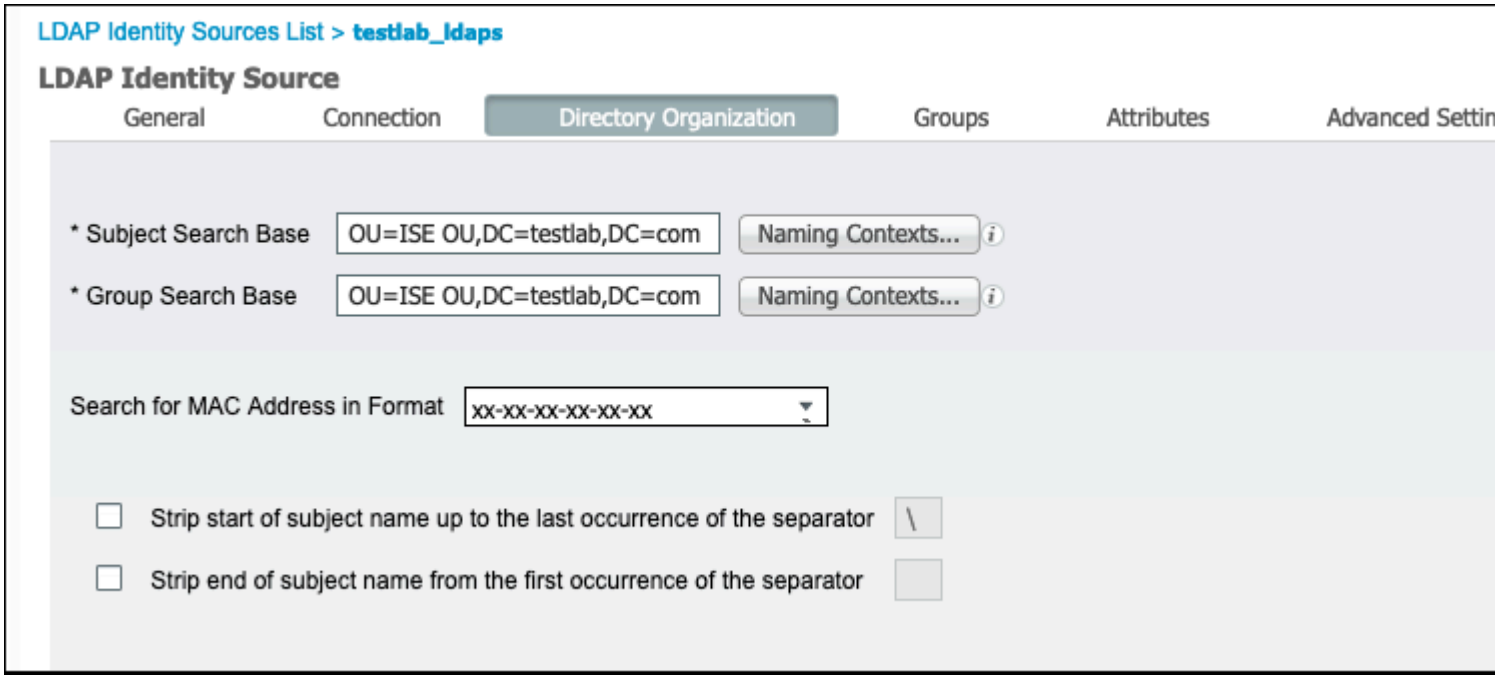
Step 1. Set the correct IP address or Hostname of the LDAP server, define the LDAPS port (TCP 636), and Admin DN to make a connection with the LDAP over SSL.

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

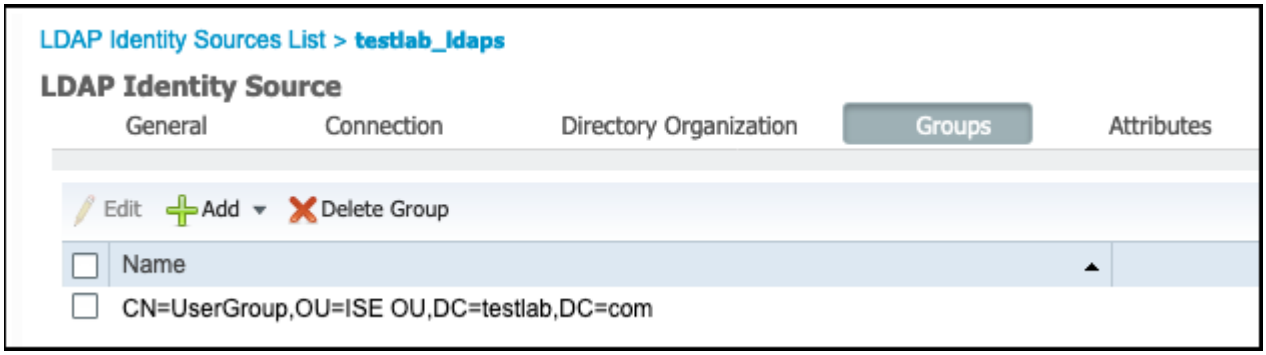
Step 3. From the drop-down menu, select the LDAP Server Root CA certificate and ISE admin certificate Isser CA certificate (We have used certificate authority, installed on the same LDAP server to issue the ISE admin certificate as well).

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



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



Configure the Switch

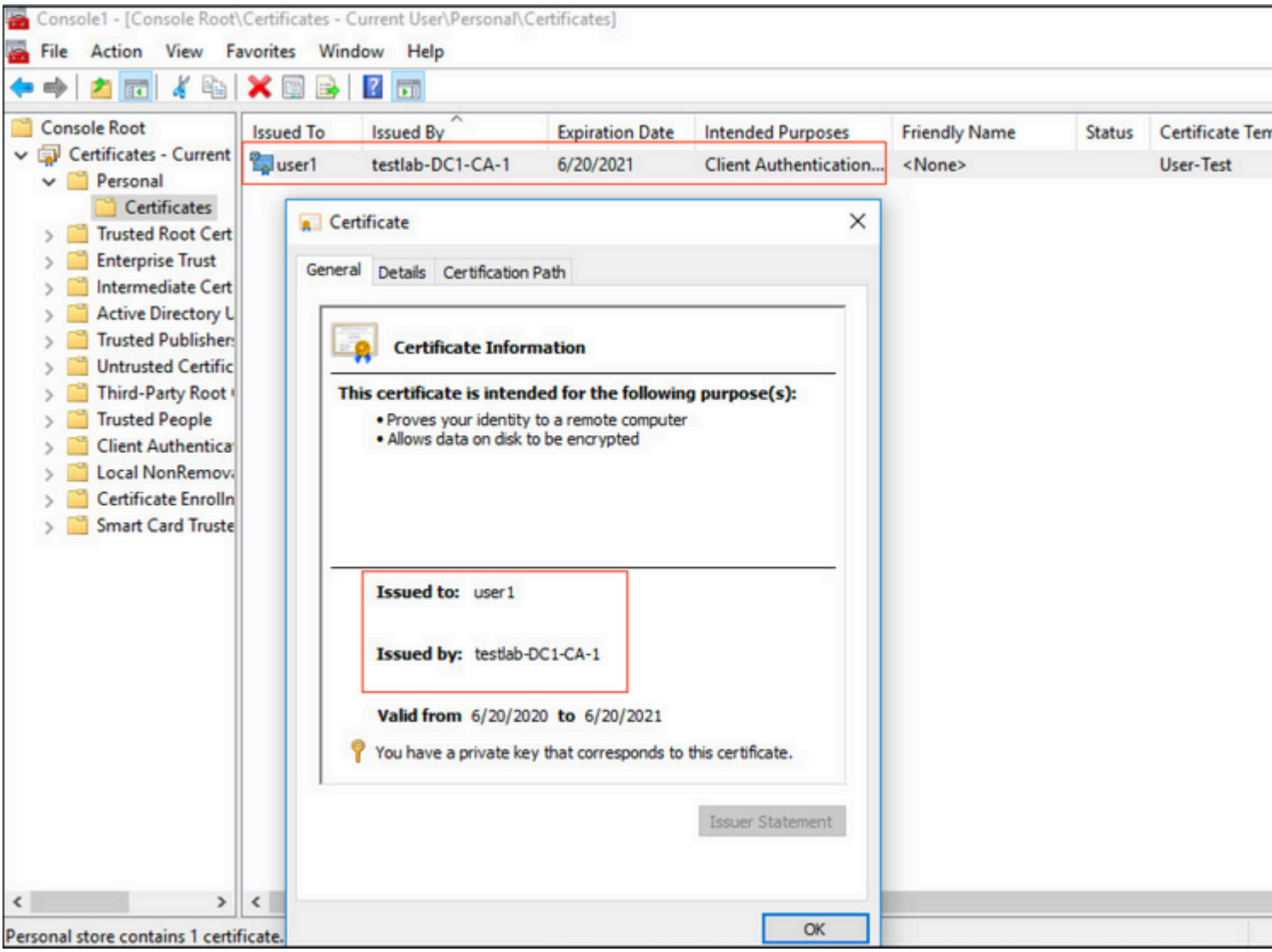
Configure the switch for 802.1x authentication. Windows PC is connected to switchport Gig2/0/47

```
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
```

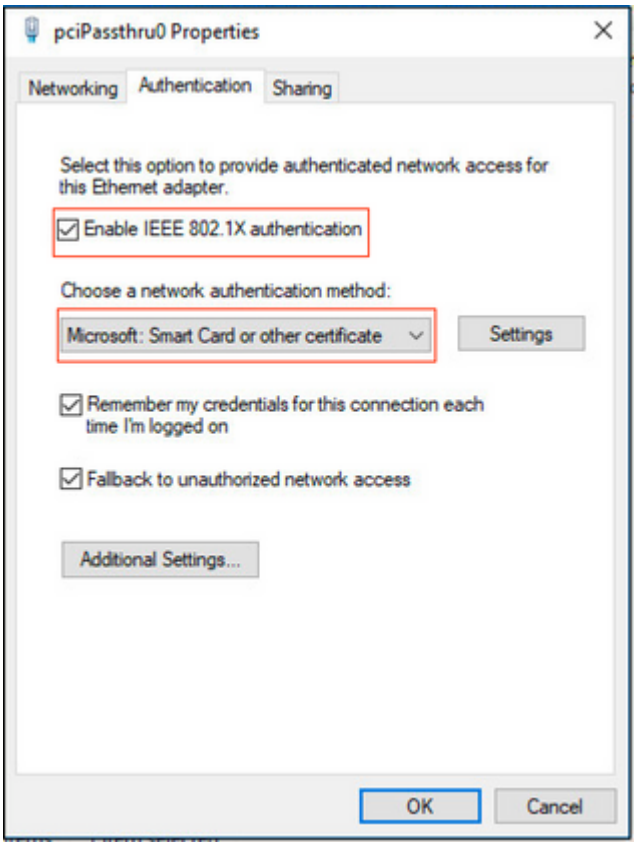
Configure the Endpoint

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

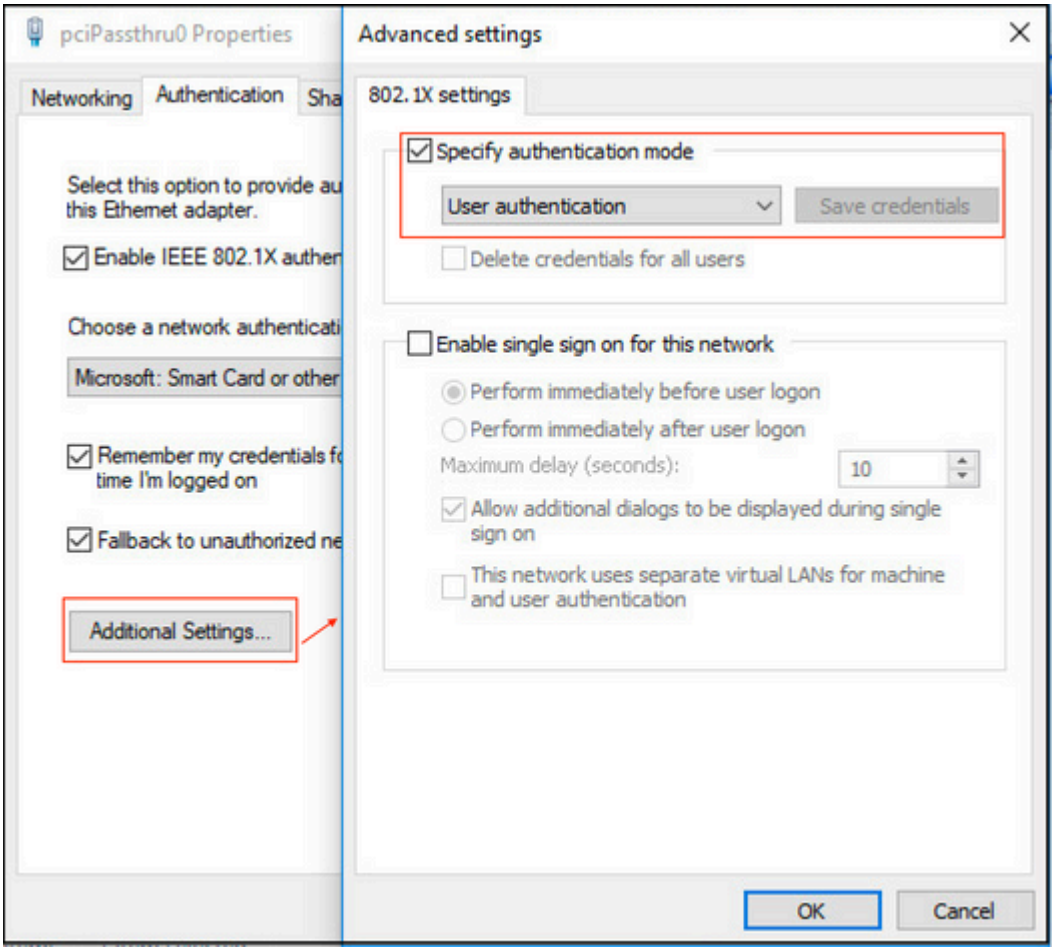
1. Ensure that PC is provisioned with user certificate (for user1) and have intended purpose as Client Authentication and in the Trusted Root Certification Authorities, the issuer certificate chain is present on the PC.



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

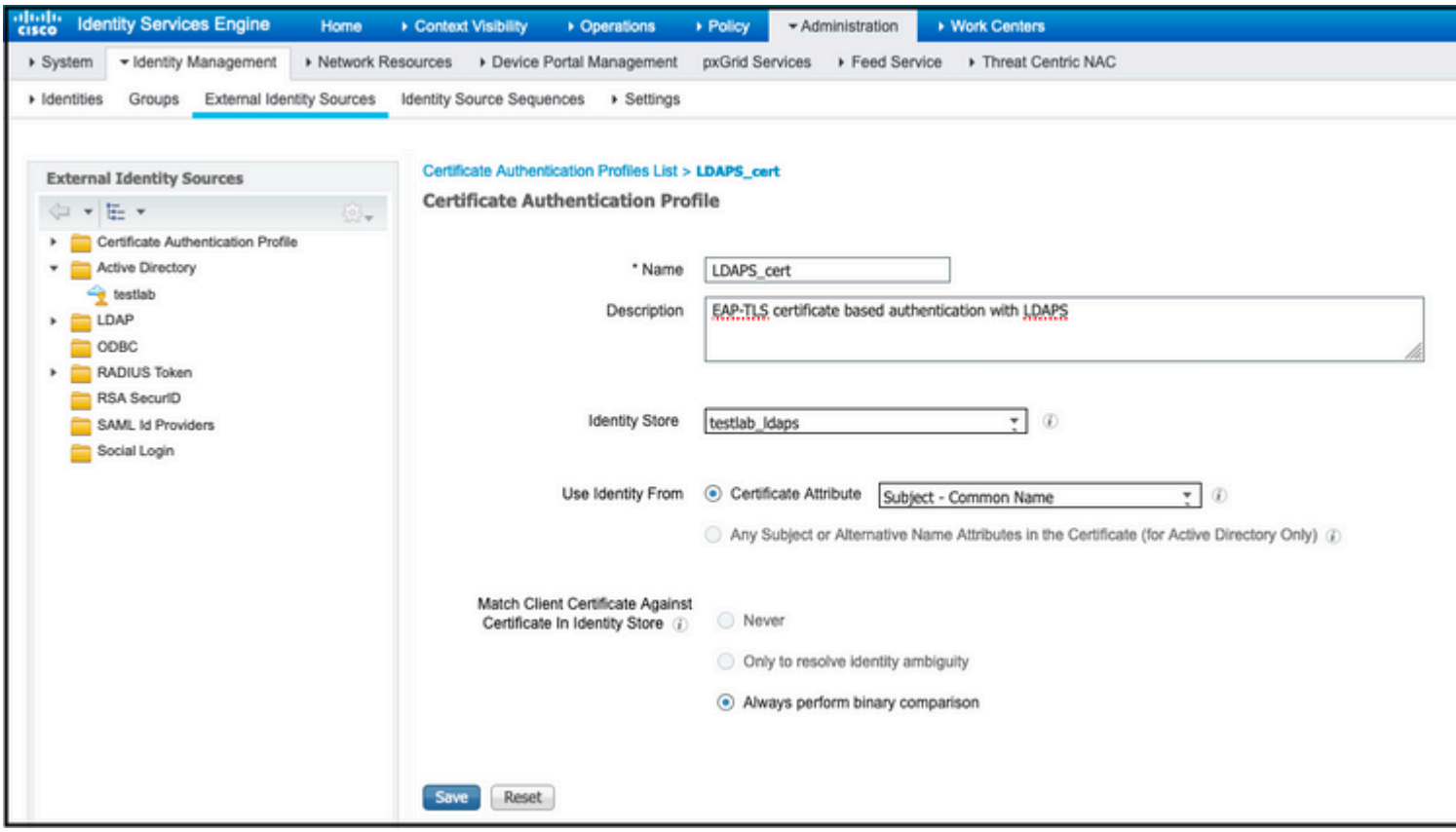


3. Click on Additional Settings, and a window opens. Check the box with specify authentication mode and choose user authentication, as shown in this image.

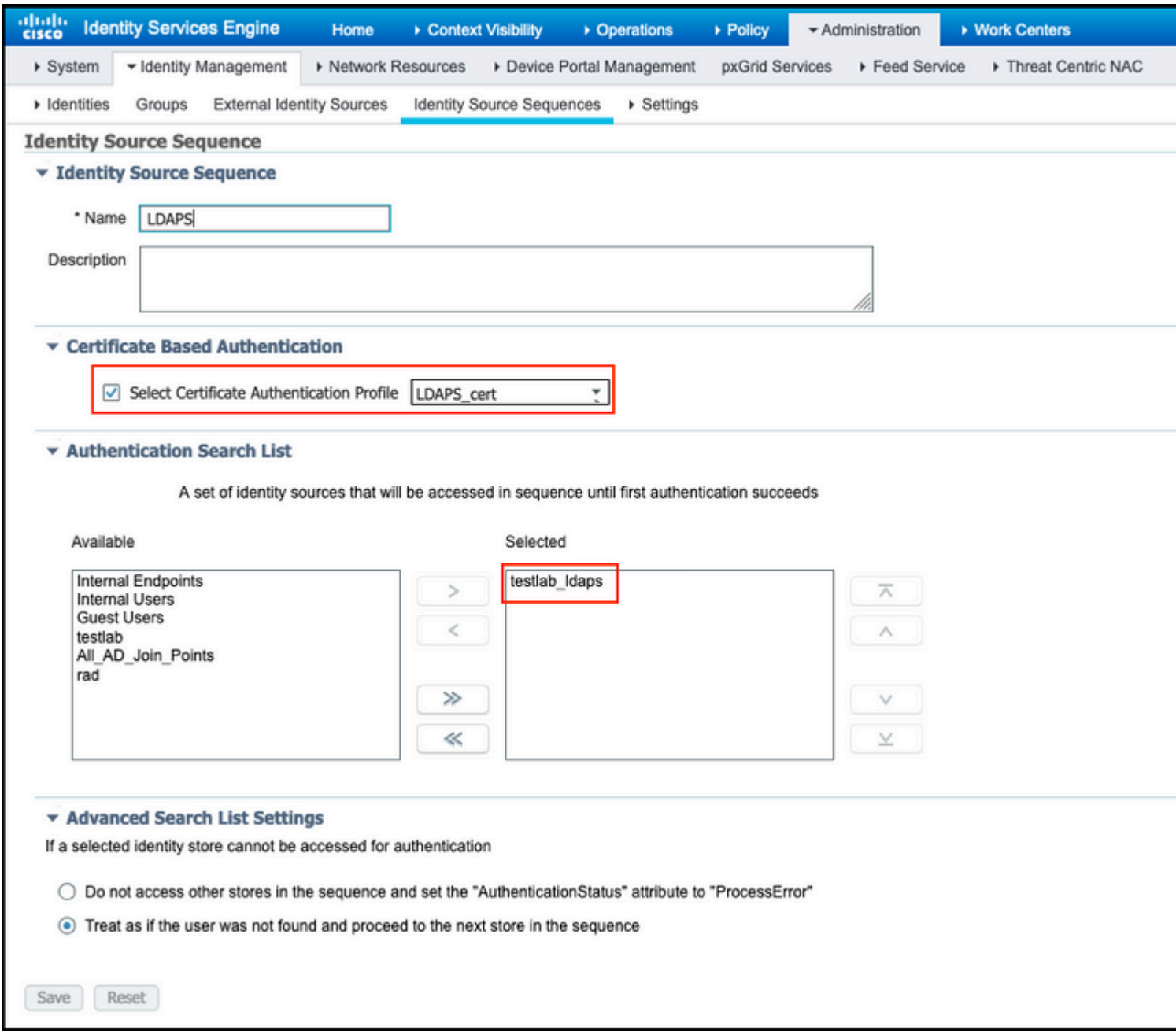


Configure Policy Set on ISE

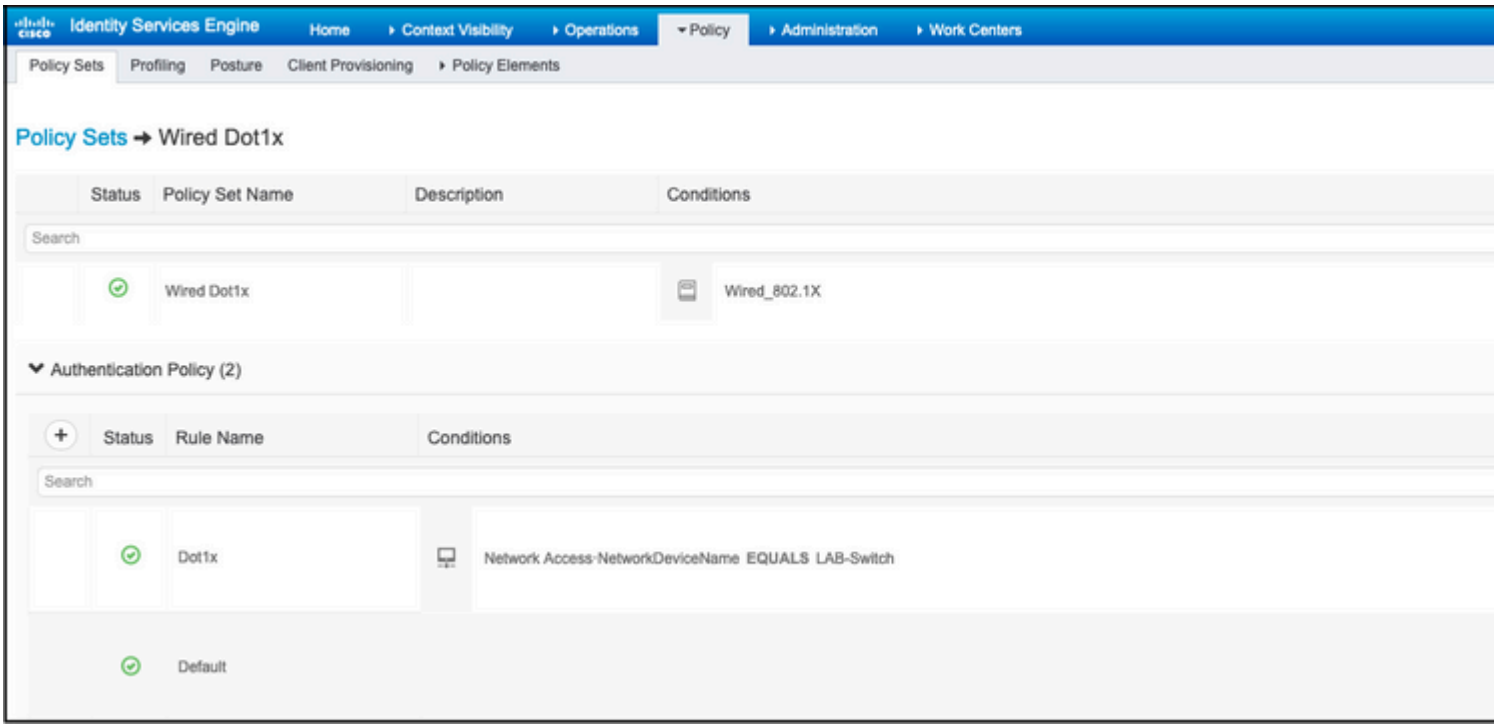
Since EAP-TLS protocol is used, before Policy Set is configured, Certificate Authentication Profile needs to be configured and the Identity Source Sequence is used in the Authentication policy later.



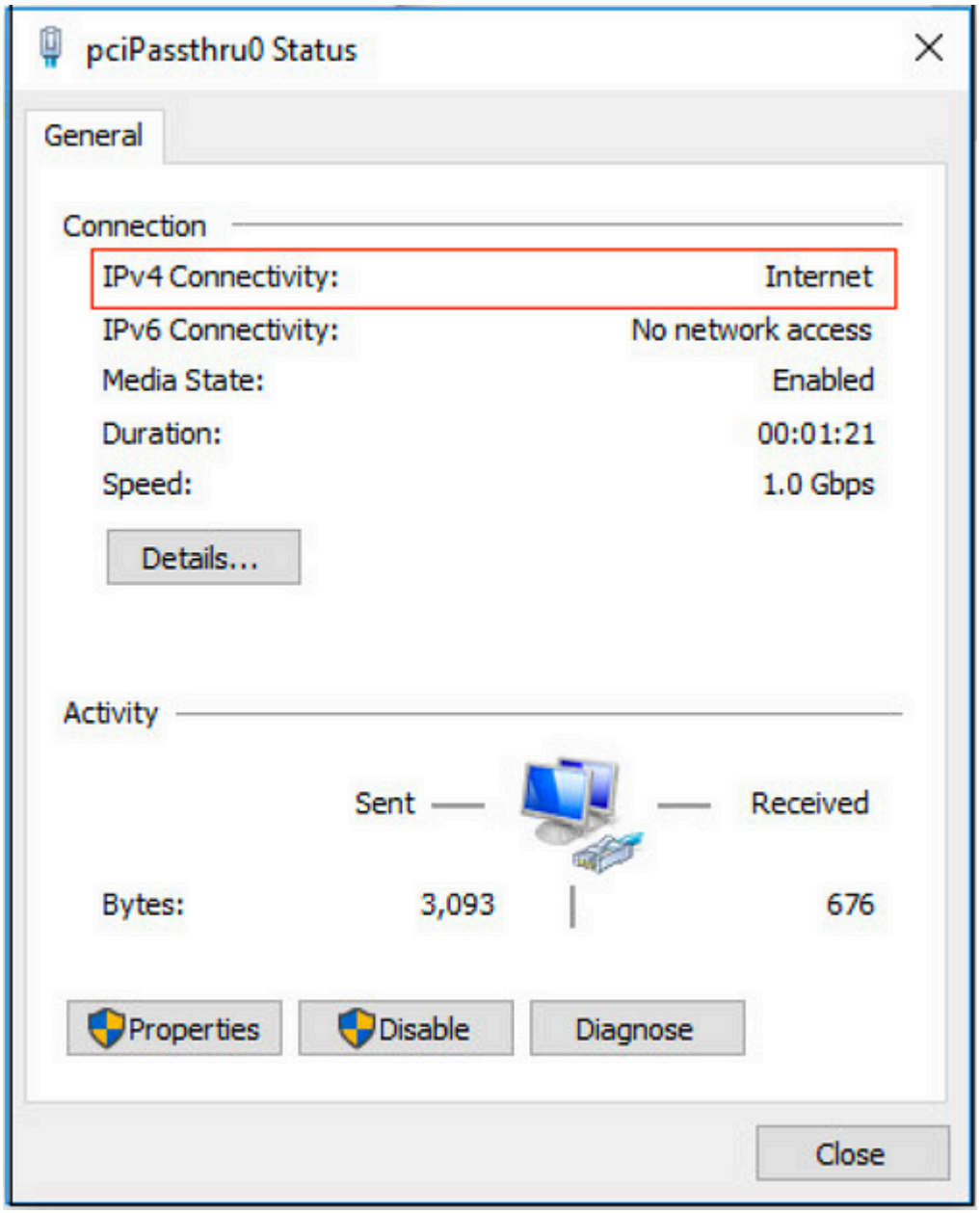
Refer to the Certificate Authentication Profile in the Identity Source Sequence and define the LDAPS external identity source in the Authentication Search list:



Now configure policy set for Wired Dot1x authentication:



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

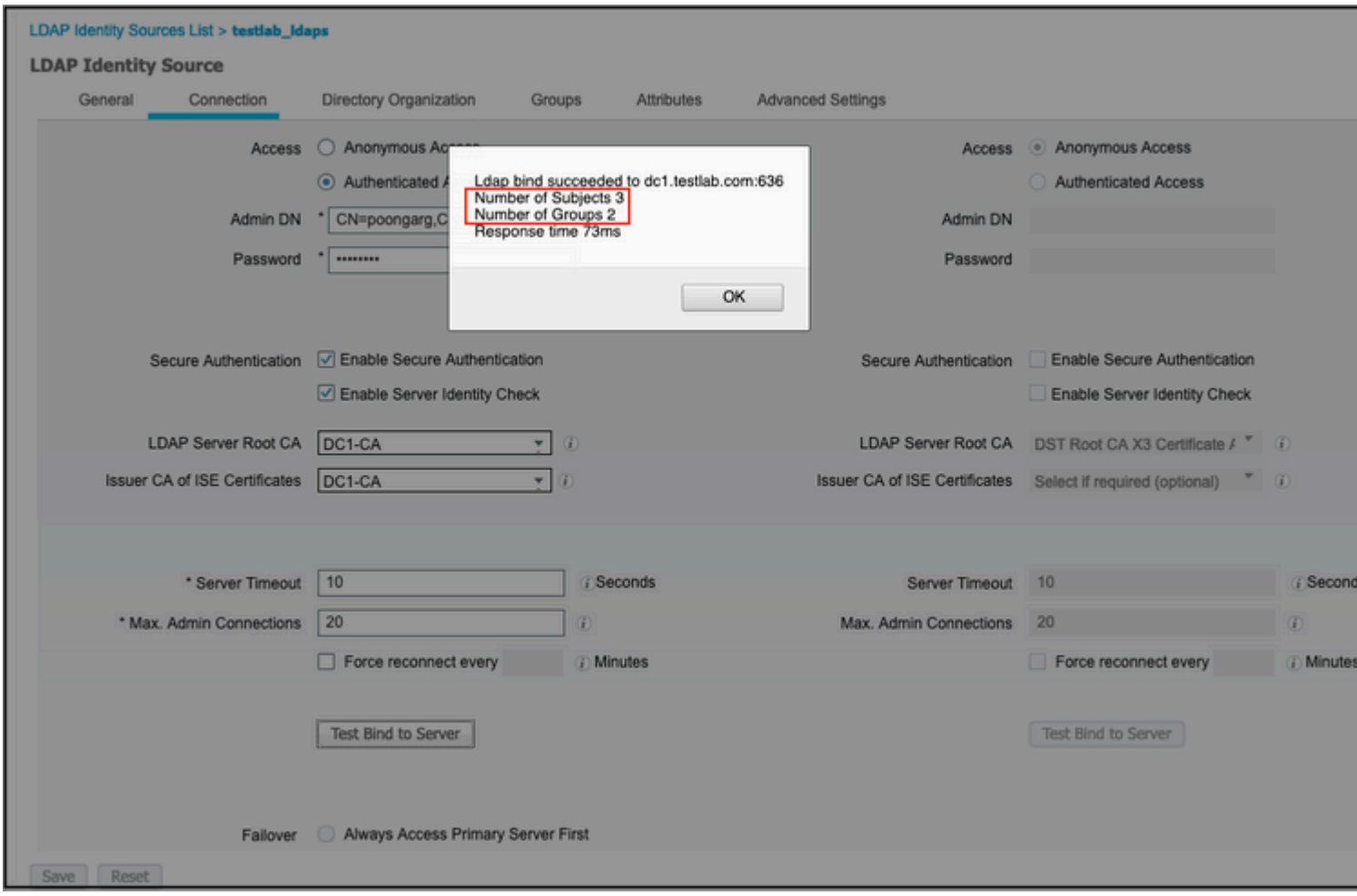


Verify

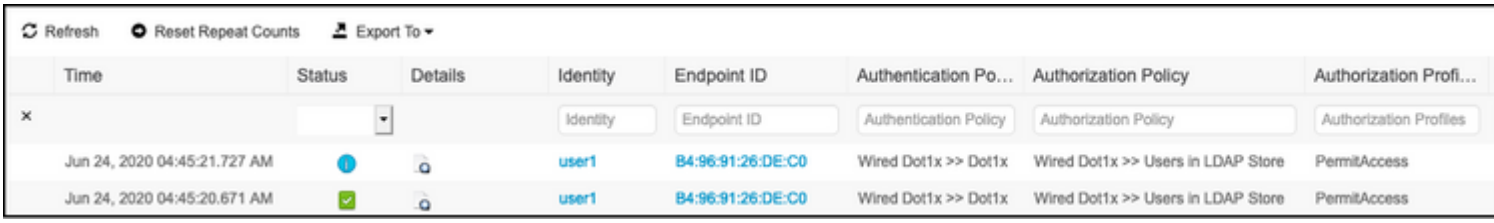
1. Check the authentication session on the switchport connected to PC:

```
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:  0A6A263900000130798C66612
     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:



3. Verify the user authentication report:



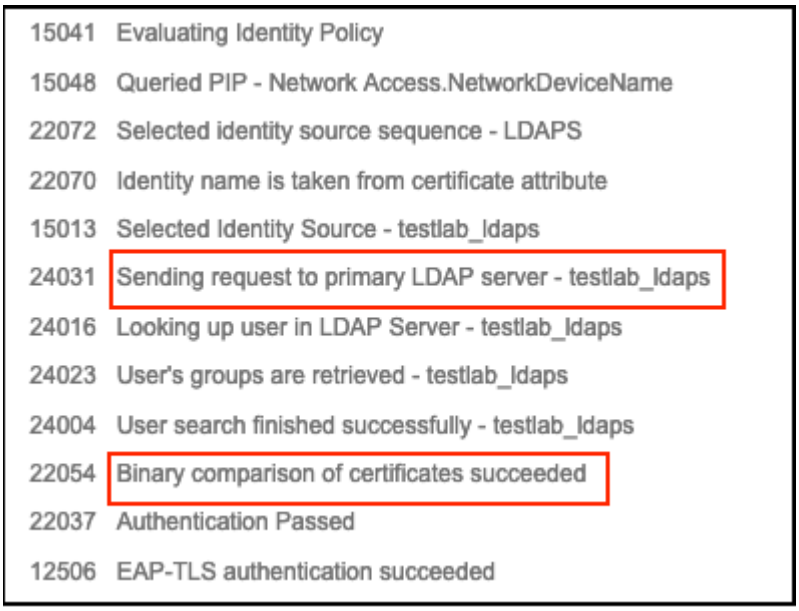
4. Check the detailed authentication report for the endpoint:

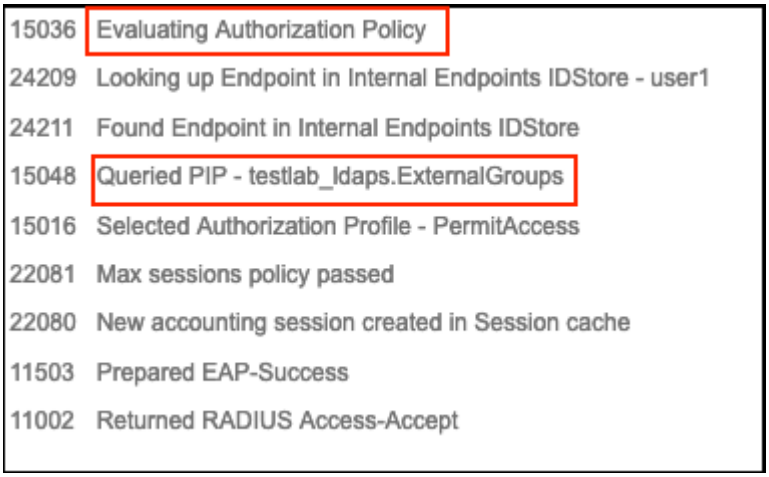
Overview

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

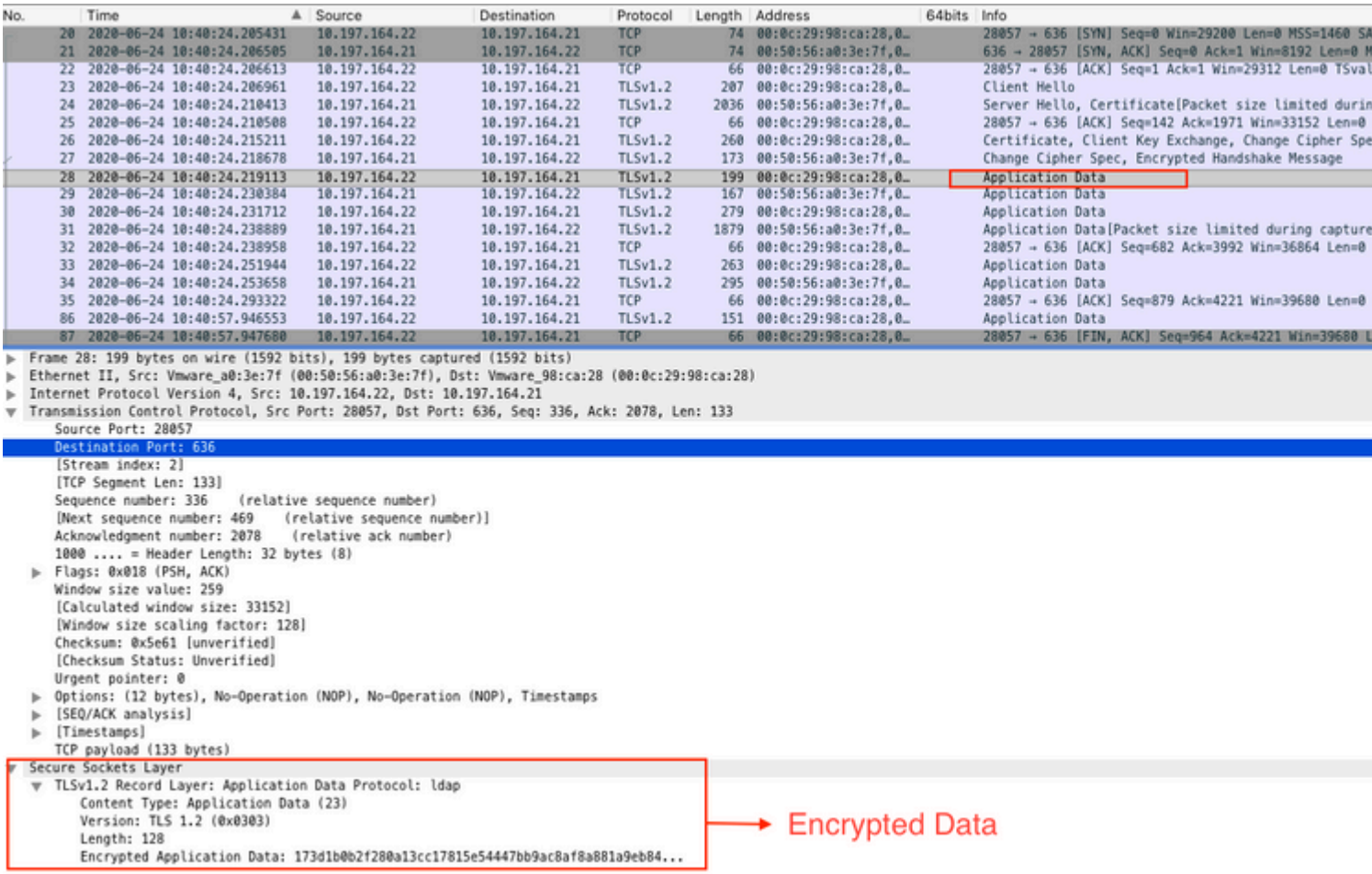
Authentication Details

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





5. Validate the data is encrypted between the ISE and LDAPS server by taking packet capture on the ISE towards the LDAPS server:



Troubleshoot

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

- 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).

- 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**