

CISCO ISE Identity Services Engine User Guide

[Home](#) » [Cisco](#) » CISCO ISE Identity Services Engine User Guide 



Contents

- [1 Introduction](#)
- [2 Prerequisites](#)
- [3 Configure](#)
- [4 Configure LDAPS on Active Directory](#)
- [5 Integrate ISE with LDAPS Server](#)
- [6 Configure the Switch](#)
- [7 Verify](#)
- [8 Troubleshoot](#)
- [9 Documents / Resources](#)
 - [9.1 References](#)

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.

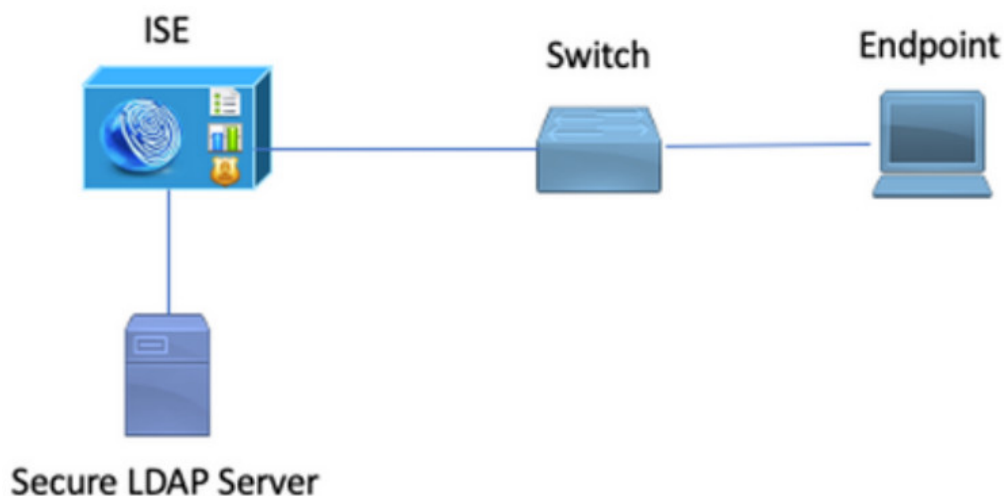
Configure

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:

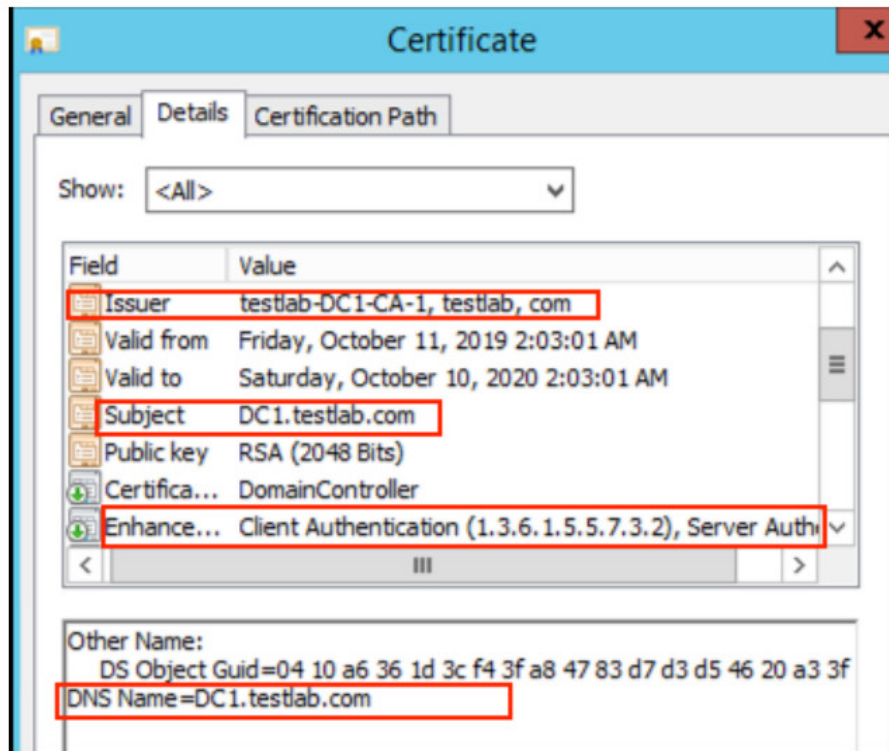


Configure LDAPS on Active Directory

Install Identity Certificate on Domain Controller

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

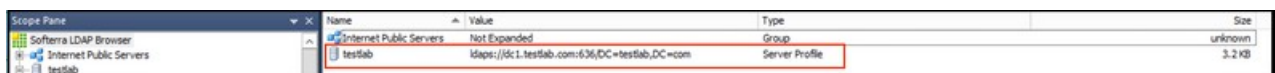
1. The LDAPS certificate is located in the Domain Controller's Personal Certificate Store.
2. A private key that matches the certificate is present in the Domain Controller's store and is correctly associated with the certificate.
3. The Enhanced Key Usage extension includes Server Authentication (1.3.6.1.5.5.7.3.1) object identifier (also known as OID).
4. The Fully Qualified Domain Name (FQDN) of the Domain Controller (for example, [DC1.testlab.com](https://www.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.



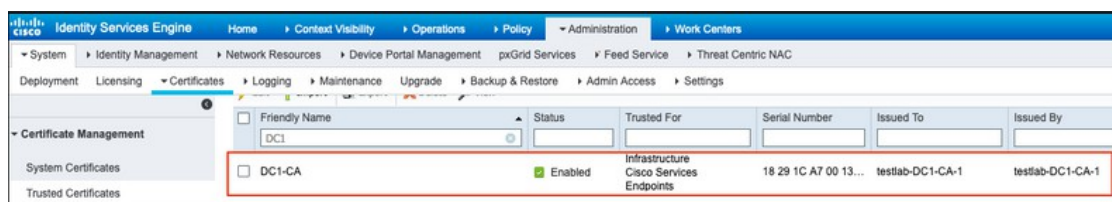
2. For simplicity, Create an Organizational Unit (OU) named ISE OU in the AD, and it must have a Group named UserGroup. Create two users (user1 and user2) and make them members of the group UserGroup.

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

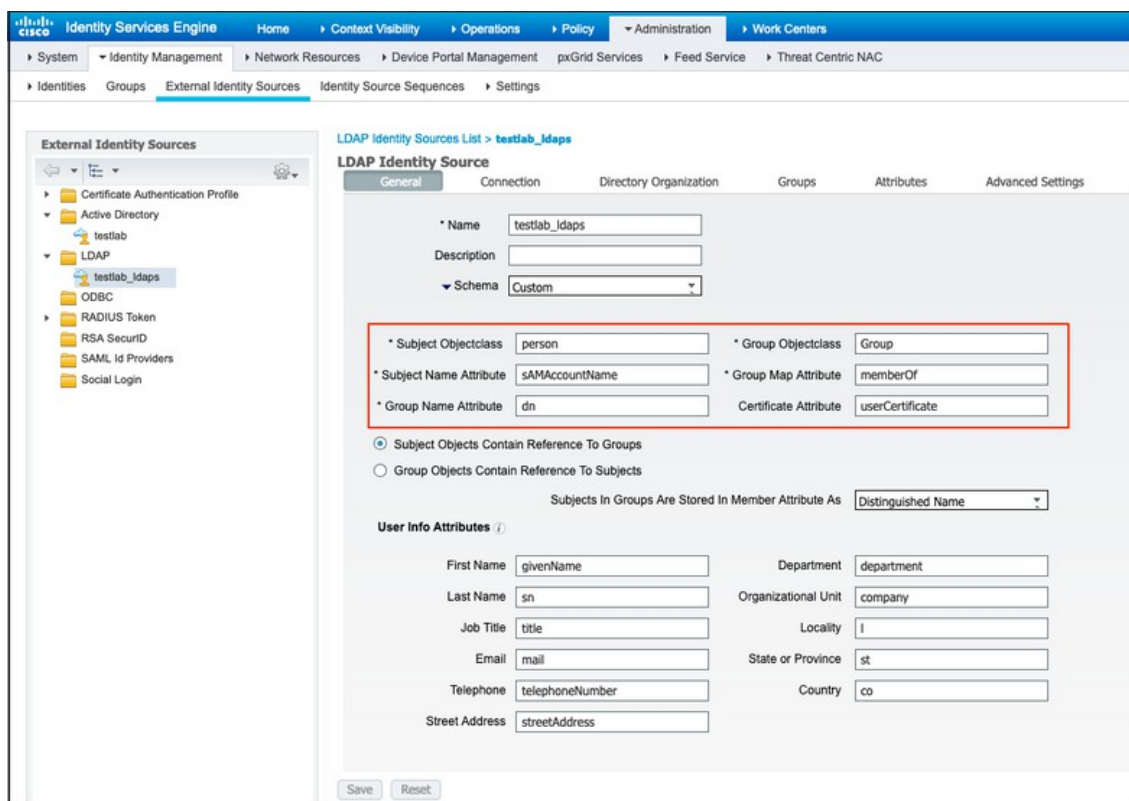
Scope Pane	Name	Value	Type
Softerra LDAP Browser	CN	UserGroup	Entry
Internet Public Servers	CN	user 2	Entry
testlab	CN	user 1	Entry
CN=Builtin	CN	DESKTOP-19	Entry
CN=Computers	CN	ComputerGroup	Entry
OU=Domain Controllers	distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribute
CN=ForeignSecurityPrincipals	dSCorePropagationData	1/1/1601	Attribute
CN=Infrastructure	dSCorePropagationData	6/20/2020 2:51:11 AM	Attribute
OU=ISE Group	gPLink	[LDAP://cn={21A53813-6971-45E8-8545-FD0C68E29790},c...	Attribute
OU=ISE OU	instanceType	[Writable]	Attribute
CN=ComputerGroup	name	ISE OU	Attribute
CN=DESKTOP-19	objectCategory	CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=...	Attribute
CN=user 1	objectClass	organizationalUnit	Attribute
CN=user 2	objectClass	top	Attribute
CN=UserGroup	ou	ISE OU	Attribute
OU=LABISE	uSNChanged	607428	Attribute
CN=LostAndFound	uSNCreated	603085	Attribute
CN=Managed Service Accounts	whenChanged	6/21/2020 2:44:06 AM	Attribute
CN=NTDS Quotas	whenCreated	6/20/2020 2:51:11 AM	Attribute
CN=Program Data	objectGUID	{4F45D1D-17B7-48DF-ABC6-3ED27FA4F694}	Binary Attribute
CN=System			

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

objectclass	Filter Value
Name	Value
objectClass	user
objectClass	organizationalPerson
objectClass	person
objectClass	top

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.

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

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

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.

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.

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

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

LDAP Identity Sources List > testlab_idaps

LDAP Identity Source

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

* Subject Search Base ⓘ

* Group Search Base ⓘ

Search for MAC Address in Format

☐ 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.

LDAP Identity Sources List > testlab_idaps

LDAP Identity Source

General Connection Directory Organization **Groups** Attributes

<input type="checkbox"/> Name
<input type="checkbox"/> 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

```

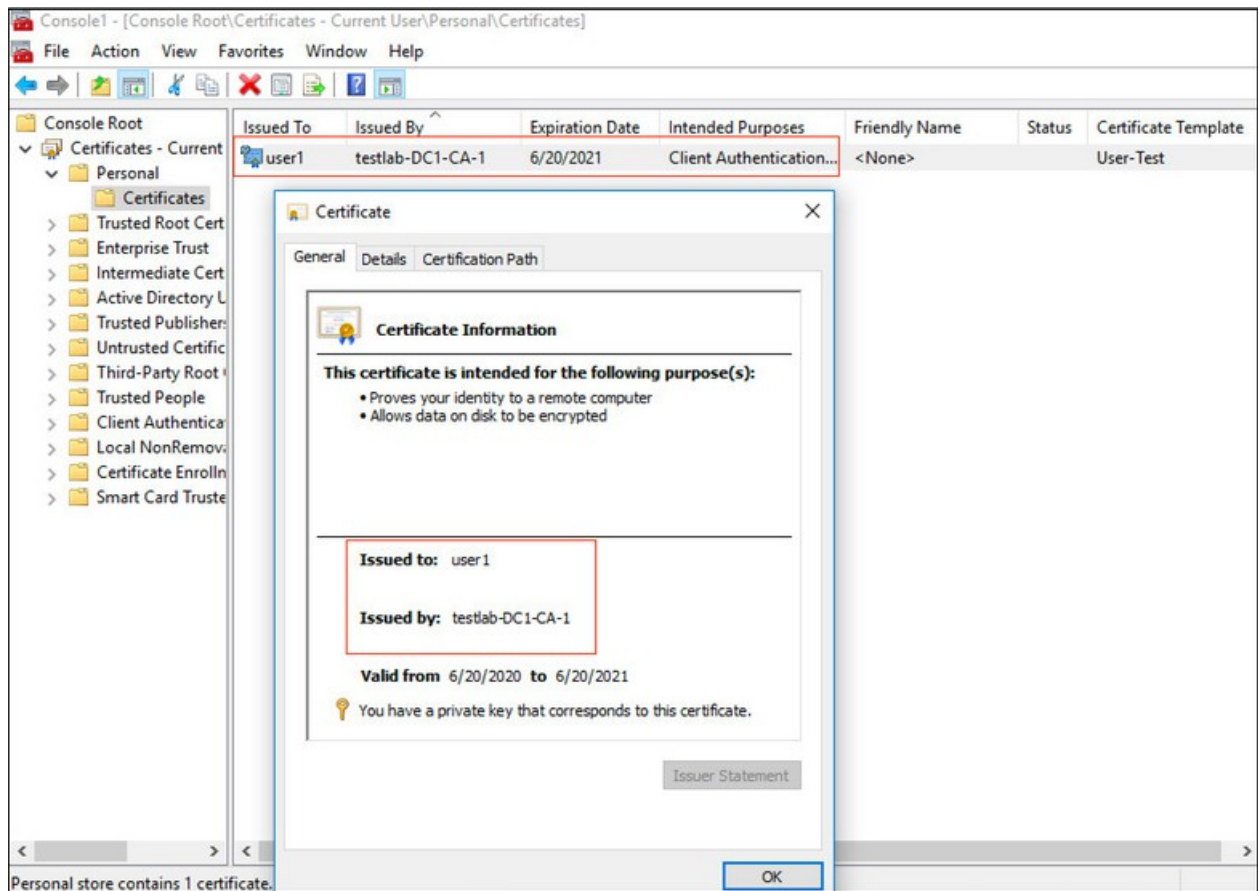
aaa new-model
radius server ISE
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key xxxxxx
aaa group server radius ISE_SERVERS
server name ISE
!
aaa server radius dynamic-author
client x.x.x.x server-key xxxxxx
!
aaa authentication dot1x default group ISE_SERVERS local
aaa authorization network default 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.

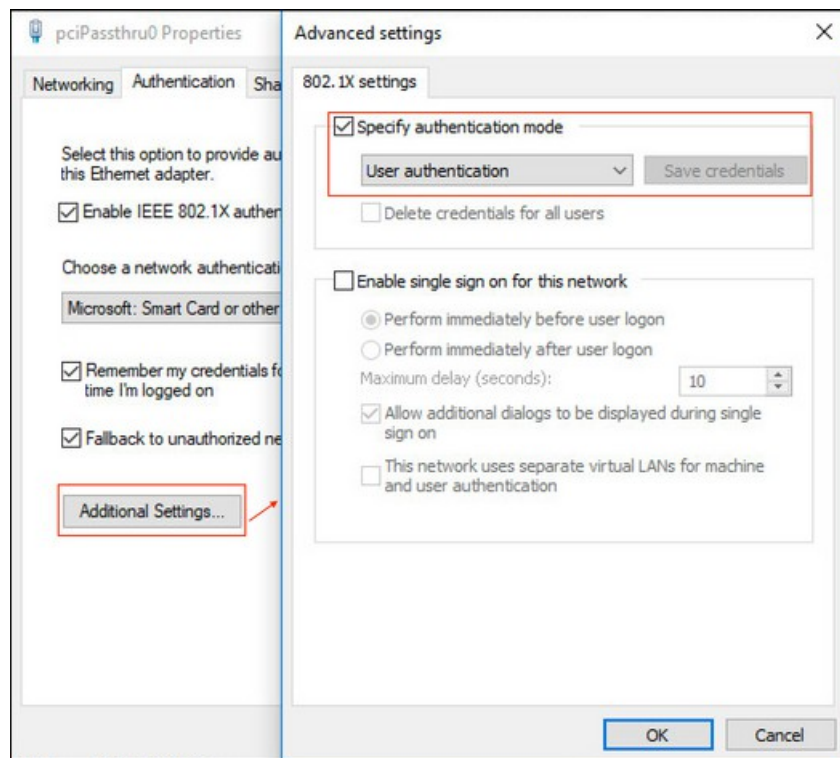
1. Ensure that PC is provisioned with user certificate (for user1) and have intended purpose as Client Authentication and in the Trusted Root Certification Authorities, the issuer certificate chain is present on the PC.



2. Enable Dot 1x authentication and Select Authentication method as Microsoft:Smart Card or other certificate for EAP-TLS authentication.

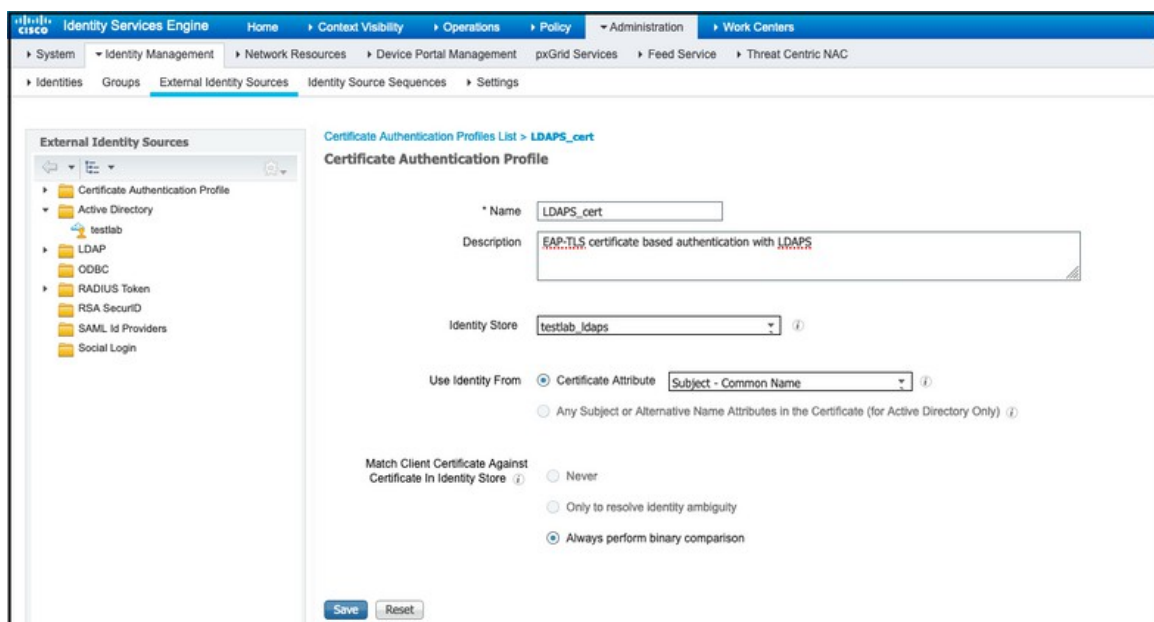


3. Click on Additional Settings, and a window opens. Check the box with specify authentication mode and choose user authentication, as shown in this image.



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:

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

Now configure policy set for Wired Dot1x authentication:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Wired Dot1x

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

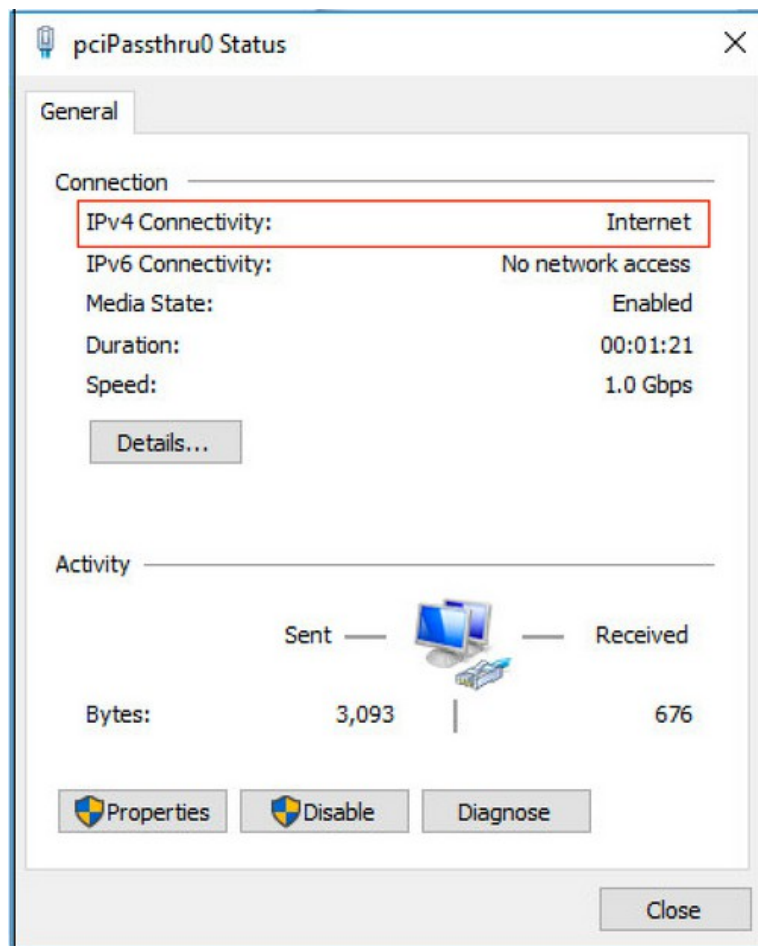
Authentication Policy (2)

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

Authorization Policy (2)

Status	Rule Name	Conditions	Results	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, 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: 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_idaps

LDAP Identity Source

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

Access ☐ Anonymous Access ☒ Authenticated Access

Admin DN * CN=poongarg.CN

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

Falover ☐ 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 / 3ms

3. Verify the user authentication report:

<div>Refresh</div> <div>Reset Repeat Counts</div> <div>Export To</div> <div>Filter</div>										
Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...	Network De...	Device Port	Authentication Pro...
x			Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port	Authentication Protocol
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 10:48:24.285431	10.197.164.22	10.197.164.21	TCP	74	00:08:c2:98:ca:28,0.	20857 → 636 [SYN]	Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=148972872 TSecr=0 WS=128
21	2020-06-24 10:48:24.286585	10.197.164.21	10.197.164.22	TCP	74	00:08:c2:98:ca:28,0.	636 → 20857 [SYN, ACK]	Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=30155962 TSecr=148972872
22	2020-06-24 10:48:24.286613	10.197.164.22	10.197.164.21	TCP	66	00:08:c2:98:ca:28,0.	20857 → 636 [ACK]	Seq=1 Ack=1 Win=29312 Len=0 TSval=148972873 TSecr=30155962
23	2020-06-24 10:48:24.286961	10.197.164.22	10.197.164.21	TLSv1.2	207	00:08:c2:98:ca:28,0.		Client Hello
24	2020-06-24 10:48:24.288413	10.197.164.21	10.197.164.22	TLSv1.2	2036	00:08:c2:98:ca:28,0.		Server Hello, Certificate[Packet size limited during capture]
25	2020-06-24 10:48:24.210588	10.197.164.22	10.197.164.21	TCP	66	00:08:c2:98:ca:28,0.		20857 → 636 [ACK] Seq=142 Ack=1971 Win=33152 Len=0 TSval=148972877 TSecr=30158962
26	2020-06-24 10:48:24.215211	10.197.164.22	10.197.164.21	TLSv1.2	268	00:08:c2:98:ca:28,0.		Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27	2020-06-24 10:48:24.218678	10.197.164.21	10.197.164.22	TLSv1.2	173	00:08:c2:98:ca:28,0.		Change Cipher Spec, Encrypted Handshake Message
28	2020-06-24 10:48:24.219113	10.197.164.22	10.197.164.21	TLSv1.2	199	00:08:c2:98:ca:28,0.		Application Data
29	2020-06-24 10:48:24.218384	10.197.164.21	10.197.164.22	TLSv1.2	167	00:08:c2:98:ca:28,0.		Application Data
30	2020-06-24 10:48:24.211712	10.197.164.22	10.197.164.21	TLSv1.2	279	00:08:c2:98:ca:28,0.		Application Data
31	2020-06-24 10:48:24.238809	10.197.164.21	10.197.164.22	TLSv1.2	1879	00:08:c2:98:ca:28,0.		Application Data[Packet size limited during capture]
32	2020-06-24 10:48:24.238958	10.197.164.22	10.197.164.21	TCP	66	00:08:c2:98:ca:28,0.		20857 → 636 [ACK] Seq=682 Ack=3992 Win=36864 Len=0 TSval=148972985 TSecr=30158965
33	2020-06-24 10:48:24.251944	10.197.164.22	10.197.164.21	TLSv1.2	263	00:08:c2:98:ca:28,0.		Application Data
34	2020-06-24 10:48:24.253658	10.197.164.21	10.197.164.22	TLSv1.2	295	00:08:c2:98:ca:28,0.		Application Data
35	2020-06-24 10:48:24.293322	10.197.164.22	10.197.164.21	TCP	66	00:08:c2:98:ca:28,0.		20857 → 636 [ACK] Seq=879 Ack=4221 Win=39680 Len=0 TSval=148972968 TSecr=30158967
86	2020-06-24 10:48:57.946553	10.197.164.22	10.197.164.21	TLSv1.2	151	00:08:c2:98:ca:28,0.		Application Data
87	2020-06-24 10:48:57.947688	10.197.164.22	10.197.164.21	TCP	66	00:08:c2:98:ca:28,0.		20857 → 636 [FIN, ACK] Seq=964 Ack=4221 Win=39680 Len=0 TSval=141886614 TSecr=30158967

```
> Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
> Ethernet II, Src: Vmware_08:00:3e:7f (00:08:00:08:00:3e: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: 20857, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133
  Source Port: 20857
  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)
  0000 .... = 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: 173b1b0b2f280a13cc17815e5447bb9ac8af8a881a9eb84...
    > Encrypted Data
```

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
= SSL alert: code=0x22A=554 ; source=local ; type=fatal ; message="Server certificate identity verification failed:
host IP didnt match SAN IP.s3_clnt.c:1290
```

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



Documents / Resources

<p>Configure and Troubleshoot ISE with External LDAP Identity Store</p> <p>Contents</p> <ul style="list-style-type: none"> Chapter 1: Introduction Chapter 2: Prerequisites Chapter 3: Configuring ISE with External LDAP Identity Store Chapter 4: Troubleshooting <p>Introduction</p> <p>This document provides information about the configuration and troubleshooting of the ISE with External LDAP Identity Store.</p> <p>Prerequisites</p> <p>Before configuring ISE with External LDAP Identity Store, ensure that the following prerequisites are met:</p> <ul style="list-style-type: none"> ISE is installed and configured correctly. LDAP server is installed and configured correctly. ISE is connected to the LDAP server. <p>Configuring ISE</p> <p>To configure ISE with External LDAP Identity Store, follow these steps:</p> <ol style="list-style-type: none"> Configure the LDAP server. Configure the ISE with External LDAP Identity Store. <p>Troubleshooting</p> <p>If you encounter any issues while configuring ISE with External LDAP Identity Store, refer to the Troubleshooting chapter for more information.</p>	<p>CISCO ISE Identity Services Engine [pdf] User Guide</p> <p>ISE Identity Services Engine, ISE, Identity Services Engine, Services Engine</p>
---	--

References

- [Configure the ISE for Integration with an LDAP Server - Cisco](#)
- [Configure EAP-TLS Authentication with ISE - Cisco](#)
- [User Manual](#)