使用外部LDAPS身份库配置并排除ISE故障

目录

简介

本文档介绍思科ISE与作为外部身份源的安全LDAPS服务器的集成。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎(ISE)管理基础知识
- Active Directory/安全轻型目录访问协议(LDAPS)基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE 2.6补丁7
- 安装了Active Directory轻型目录服务的Microsoft Windows版本2012 R2
- 安装了本地请求方和用户证书的Windows 10 OS PC
- 带152-2.E6映像的思科交换机C3750X

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

LDAPS允许在建立目录绑定时对传输中的LDAP数据（包括用户凭证）进行加密。LDAPS使用TCP端口636。

LDAPS支持以下身份验证协议：

- EAP通用令牌卡(EAP-GTC)
- 密码 认证 协议 (PAP)
- EAP传输层安全(EAP-TLS)
- 受保护的EAP传输层安全(PEAP-TLS)

注意：LDAPS外部身份源不支持EAP-MSCHAPV2（作为PEAP、EAP-FAST或EAP-TTLS的内部方法）、LEAP、CHAP和EAP-MD5。

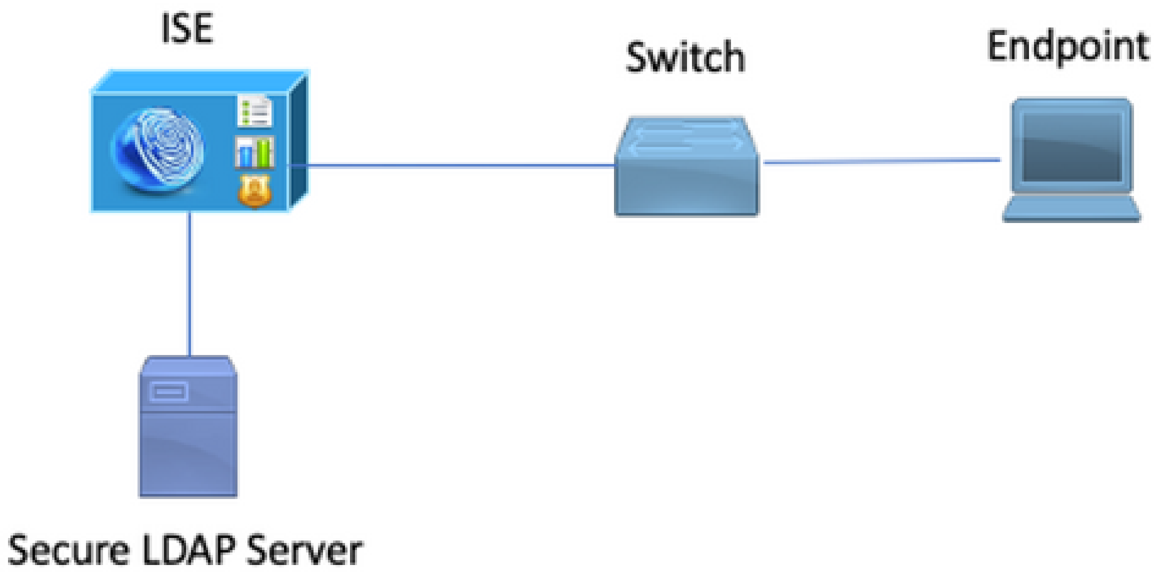
配置

本节介绍网络设备的配置以及ISE与Microsoft Active Directory(AD)LDAPS服务器的集成。

网络图

在此配置示例中，终端使用以太网连接与交换机连接以与局域网(LAN)连接。已连接的交换机端口配置为802.1x身份验证，以使用ISE对用户进行身份验证。在ISE上，LDAPS配置为外部身份库。

下图说明了使用的网络拓扑：

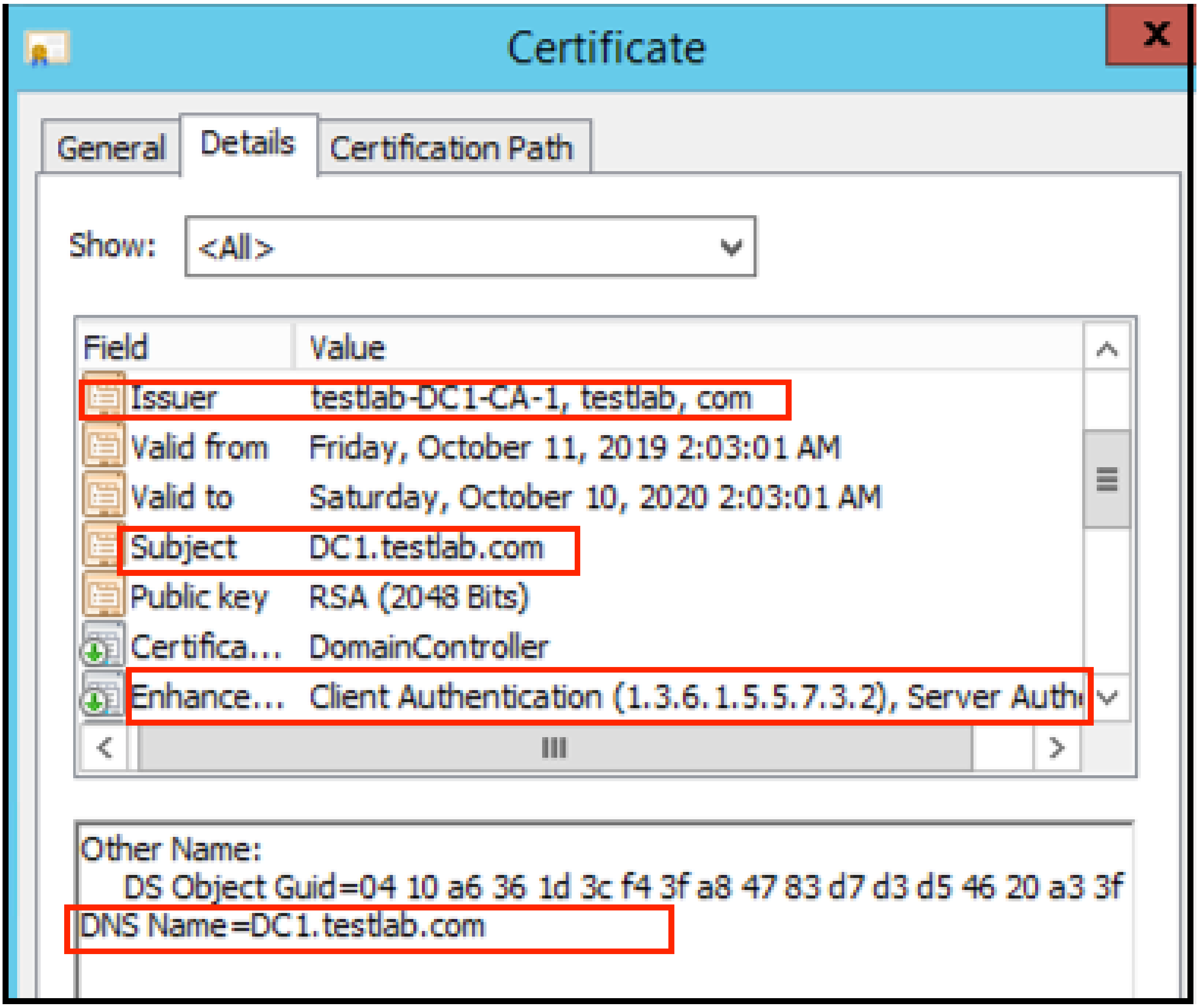


在Active Directory上配置LDAP

在域控制器上安装身份证书

要启用LDAPS，请在符合以下要求的域控制器(DC)上安装证书：

1. LDAPS证书位于域控制器的个人证书存储中。
2. 与证书匹配的私钥存在于域控制器的存储中，并且与证书正确关联。
3. 增强型密钥使用扩展包括服务器身份验证(1.3.6.1.5.5.7.3.1)对象标识符（也称为OID）。
4. 域控制器的完全限定域名(FQDN)(例如，DC1.testlab.com)必须存在于以下属性之一：Subject字段中的Common Name(CN)和Subject Alternative Name Extension中的DNS条目。
5. 证书必须由域控制器和LDAPS客户端信任的证书颁发机构(CA)颁发。对于受信任的安全通信，客户端和服务器必须信任彼此的根CA和向其颁发证书的中间CA证书。
6. 必须使用信道加密服务提供程序(CSP)生成密钥。



Certificate

Show: <All>

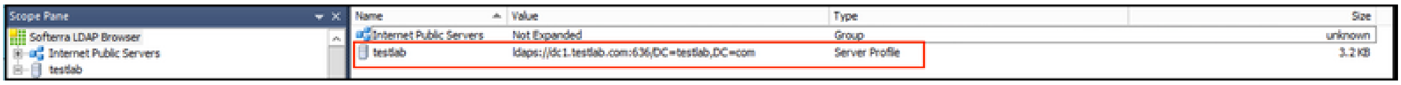
Field	Value
Issuer	testlab-DC1-CA-1, testlab, com
Valid from	Friday, October 11, 2019 2:03:01 AM
Valid to	Saturday, October 10, 2020 2:03:01 AM
Subject	DC1.testlab.com
Public key	RSA (2048 Bits)
Certifica...	DomainController
Enhance...	Client Authentication (1.3.6.1.5.5.7.3.2), Server Auth

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

访问LDAPS目录结构

要访问Active Directory服务器上的LDAPS目录，请使用任何LDAP浏览器。本实验使用Softerra LDAP Browser 4.5。

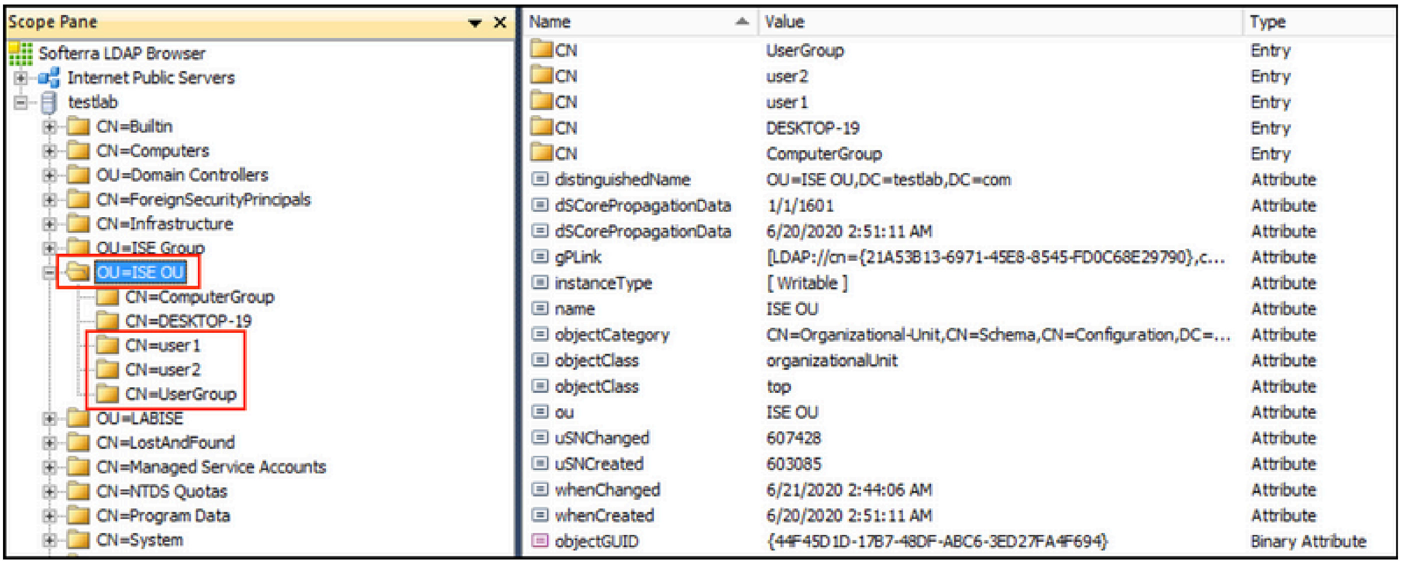
1.在TCP端口636上建立与域的连接。



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.为简单起见，在AD中创建名为ISE OU的组织单位(OU)，并且必须具有一个名为UserGroup的组。创建两个用户（user1和user2），并使其成为UserGroup组的成员。

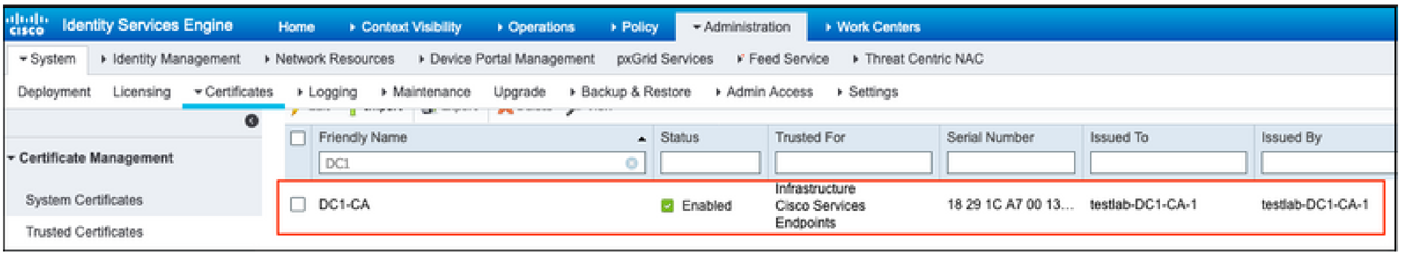
注意:ISE上的LDAP身份源仅用于用户身份验证。



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

将ISE与LDAPS服务器集成

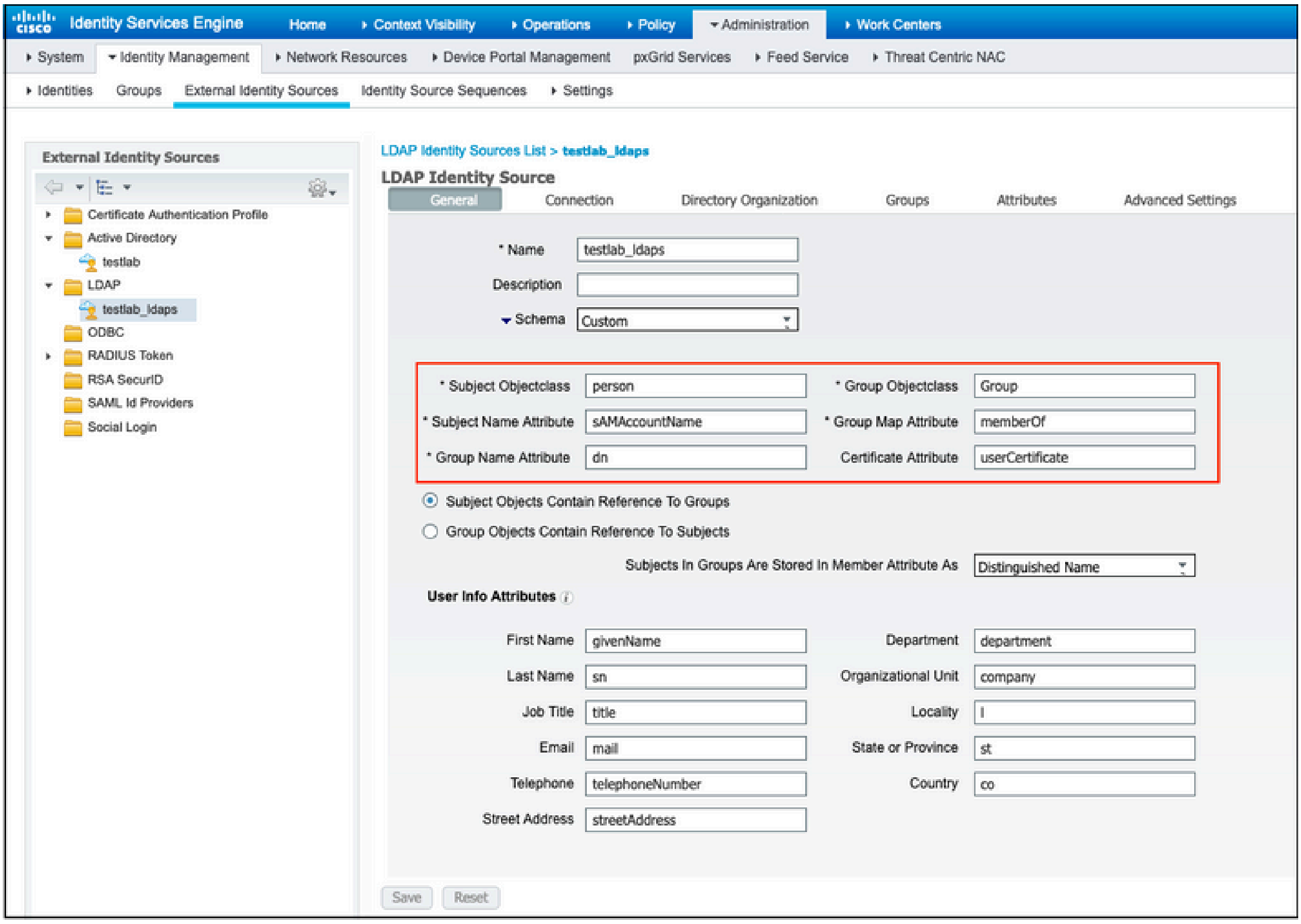
1.导入受信任证书中的LDAP服务器根CA证书。



☐	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.验证ISE管理员证书并确保ISE管理员证书颁发者证书也存在于受信任证书库中。

3.为了集成LDAPS服务器，请使用LDAPS目录中的不同LDAP属性。导航到管理>身份管理>外部身份源> LDAP身份源>添加。



* Name: testlab_ldaps

Description:

Schema: Custom

* Subject Objectclass: person

* Subject Name Attribute: sAMAccountName

* Group Name Attribute: dn

* Group Objectclass: Group

* Group Map Attribute: memberOf

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

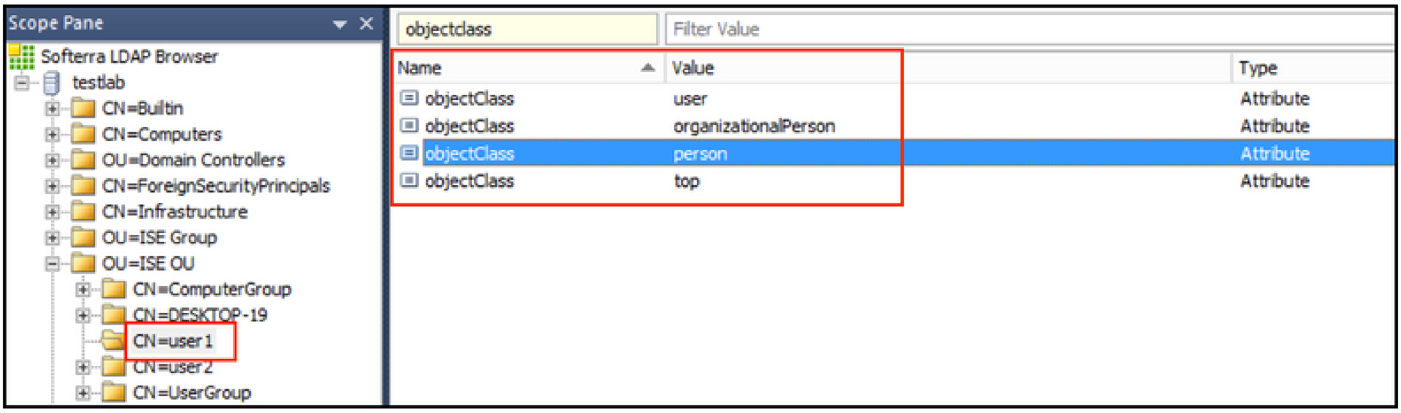
User Info Attributes

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.从“常规”选项卡配置以下属性：

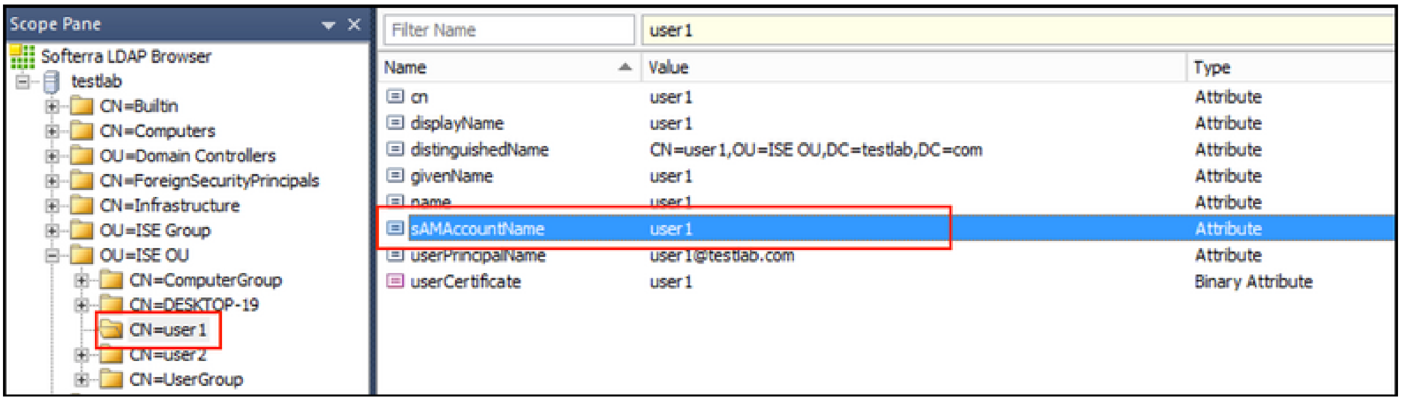
Subject Objectclass：此字段对应于用户帐户的对象类。您可以在此处使用四个类之一：

- 顶部
- 人员
- 组织人员
- InetOrgPerson



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

Subject Name Attribute：此字段是包含请求的用户名的属性的名称。当ISE在LDAP数据库中查询特定用户名时，会从LDAPS中检索此属性（您可以使用cn、sAMAccountName等）。在此方案中，使用终端上的user1用户名。

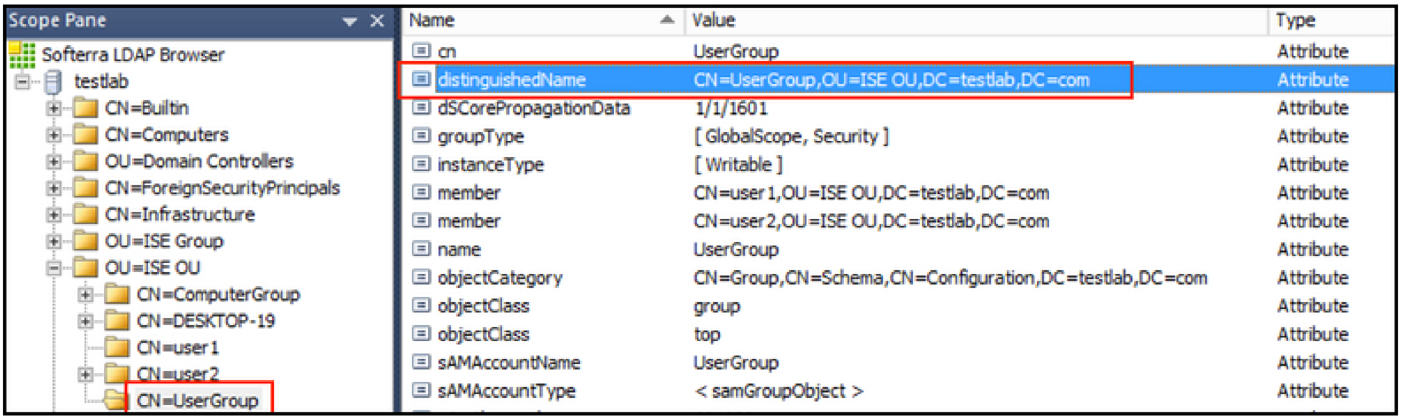


Scope Pane
Softerra LDAP Browser
testlab
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=Infrastructure
OU=ISE Group
OU=ISE OU
CN=ComputerGroup
CN=DESKTOP-19
CN=user1
CN=user2
CN=UserGroup

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

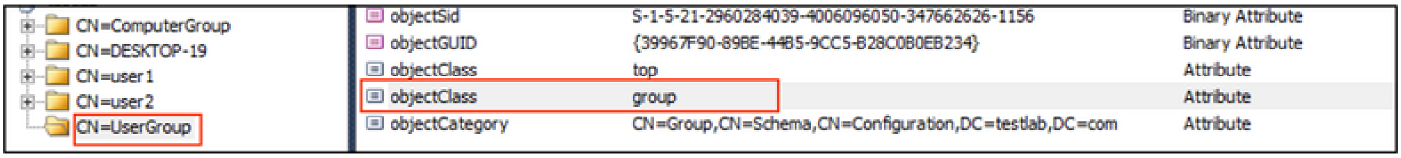
组名称属性：这是保存组名称的属性。LDAP目录中的组名称属性值必须与“用户组”页面上的LDAP组名称匹配



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

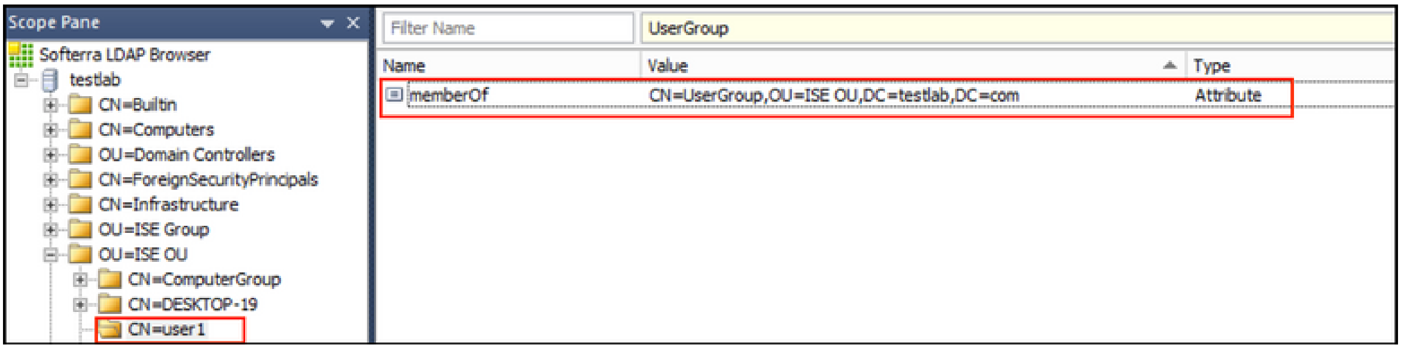
Group Objectclass:该值用于搜索以指定识别为组的对象。



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

组映射属性：此属性定义如何将用户映射到组。

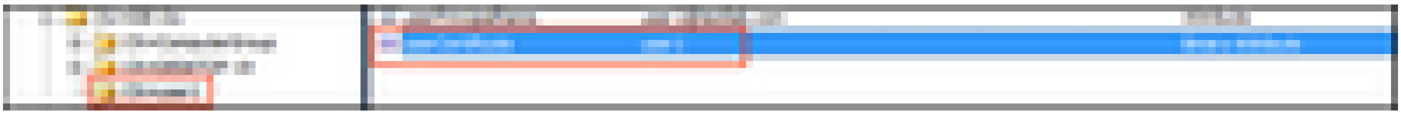


Scope Pane
Softerra LDAP Browser
testlab
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=Infrastructure
OU=ISE Group
OU=ISE OU
CN=ComputerGroup
CN=DESKTOP-19
CN=user1

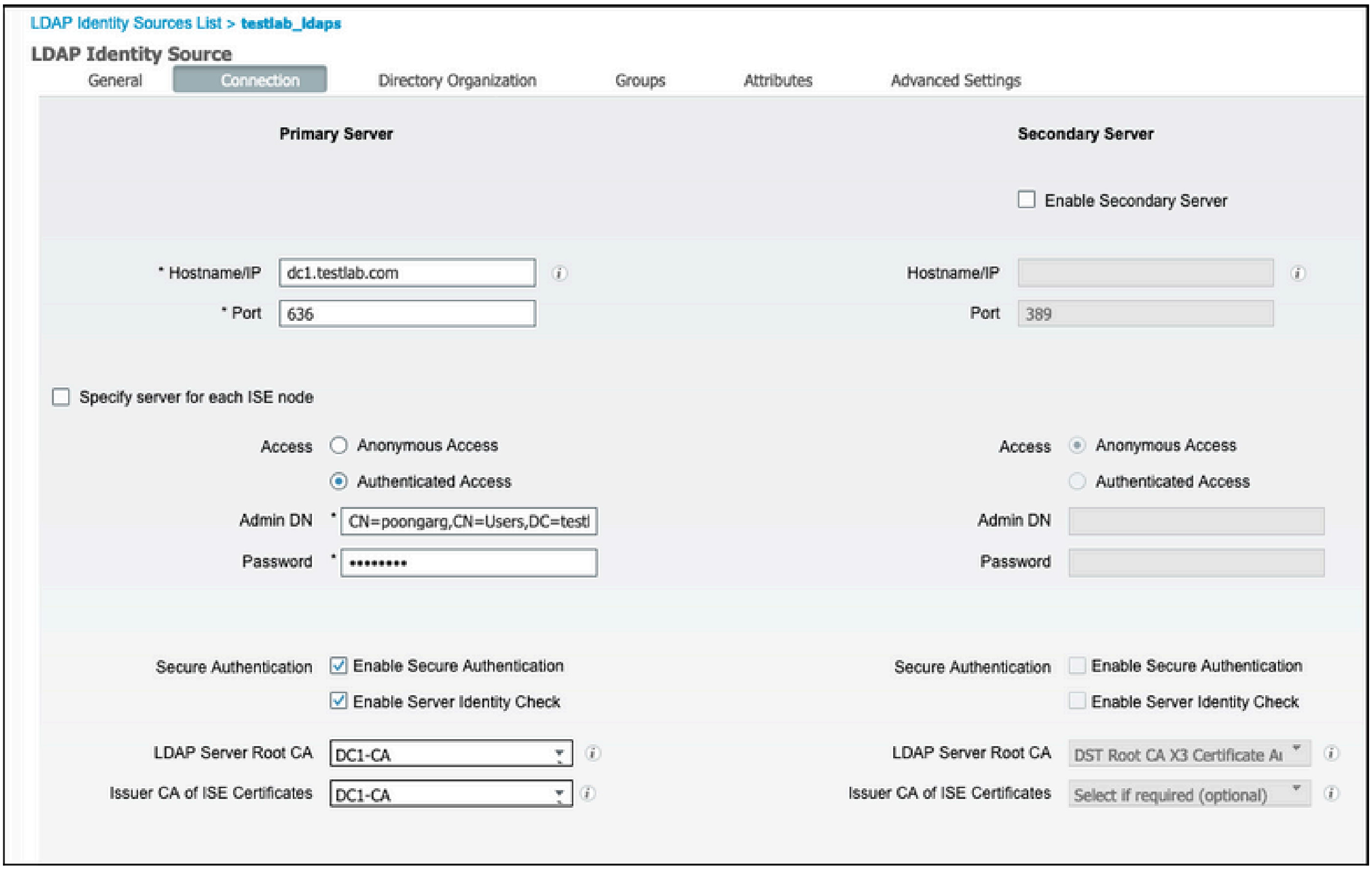
Filter Name | UserGroup

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

Certificate Attribute：输入包含证书定义的属性。这些定义可选用于在客户端被定义为证书身份验证配置文件的一部分时验证客户端提供的证书。在这种情况下，会在客户端证书和从LDAP身份源检索的证书之间执行二进制比较。



5.要配置LDAPS连接，请导航到连接选项卡：



LDAP Identity Sources List > testlab_ldaps

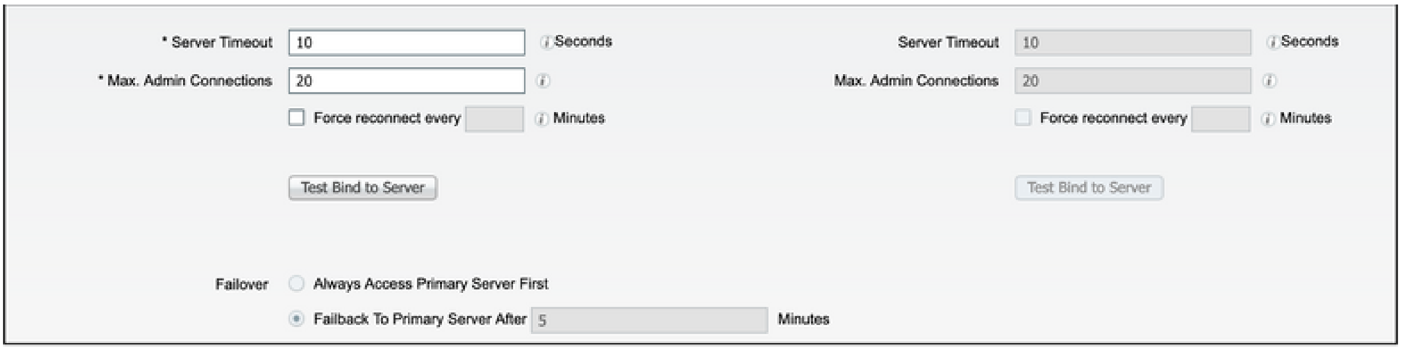
LDAP Identity Source

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 Timeout: 10 Seconds
- * Max. Admin Connections: 20
- □ Force reconnect every Minutes

Secondary:

- Server Timeout: 10 Seconds
- Max. Admin Connections: 20
- □ Force reconnect every Minutes

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

6.在域控制器上运行dsquery以获取用于连接到LDAP服务器的用户名DN:

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

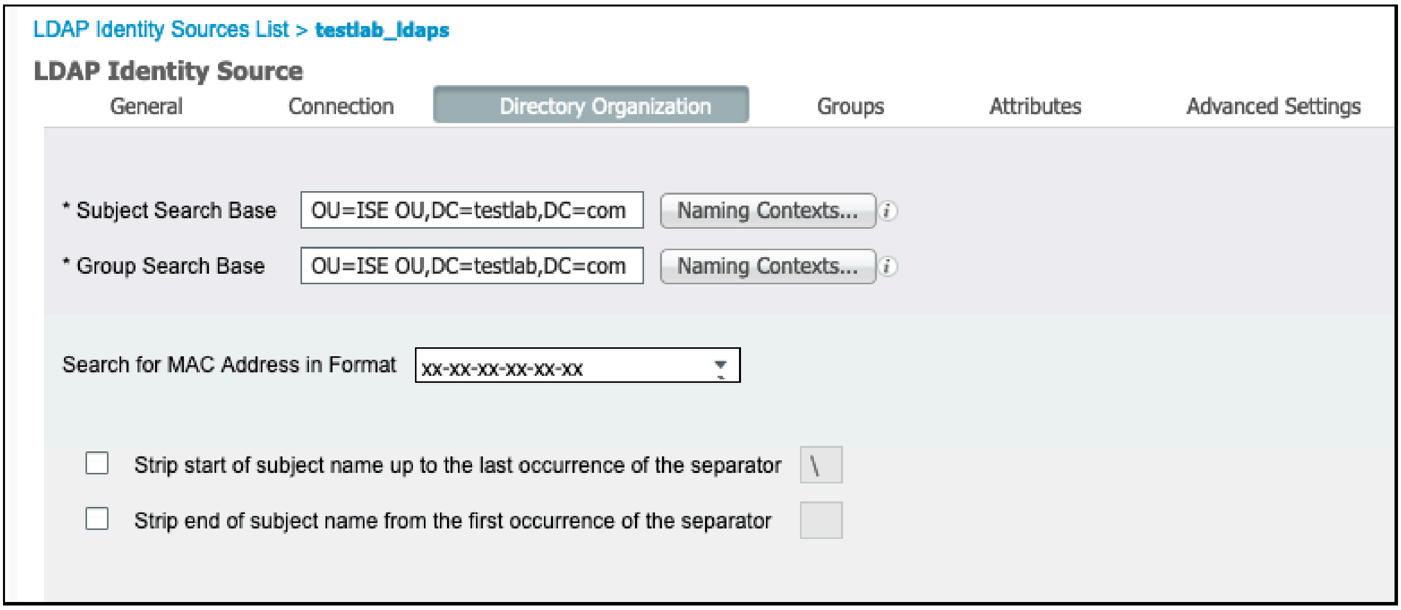
步骤1:S设置LDAP服务器的正确IP地址或主机名，定义LDAPS端口(TCP 636)和管理DN，以通过SSL与LDAP建立连接。

第二步：启用安全身份验证和服务器身份检查选项。

第三步：从下拉菜单中，选择LDAP服务器根CA证书和ISE管理员证书Isser CA证书（我们使用证书颁发机构，安装在同一LDAP服务器上以颁发ISE管理员证书）。

第四步：选择Test Bind to server。此时，由于尚未配置搜索库，因此不会检索任何主题或组。

7.在Directory Organization选项卡下，配置主题/组搜索库。它是ISE到LDAP的加入点。现在您只能检索作为加入点子级的主体和组。在此方案中，主题和组都从OU=ISE OU检索



LDAP Identity Sources List > **testlab_ldaps**

LDAP Identity Source

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

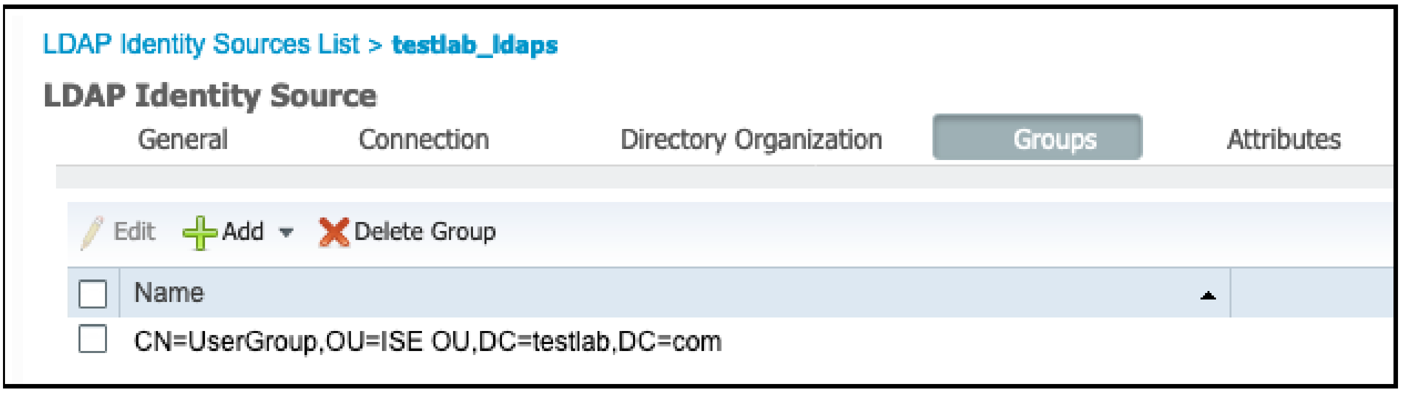
* Group Search Base: OU=ISE OU,DC=testlab,DC=com Naming Contexts...

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.在Groups下，点击Add从ISE上的LDAP导入组并检索组，如下图所示。



LDAP Identity Sources List > **testlab_ldaps**

LDAP Identity Source

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

配置交换机

配置交换机以进行802.1x身份验证。Windows PC连接到switchport Gig2/0/47

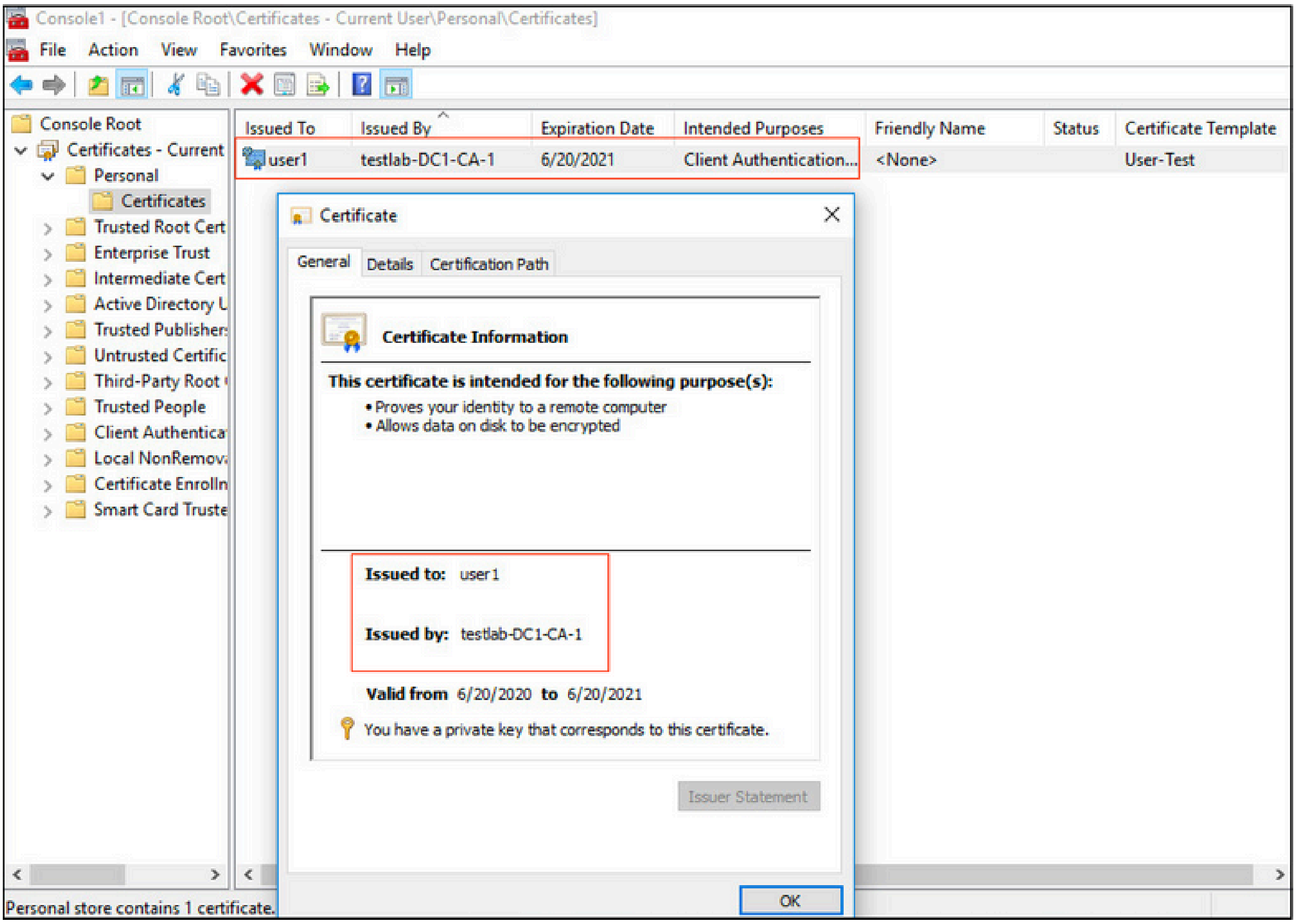
```
aaa new-model

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
```

配置终端

使用Windows Native Supplicant客户端，并且使用LDAP支持的EAP协议之一，EAP-TLS用于用户身份验证和授权。

1.确保PC已配置用户证书（用于user1），并且其目标用途为客户端身份验证，在受信任的根证书颁发机构中，PC上存在颁发者证书链。



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

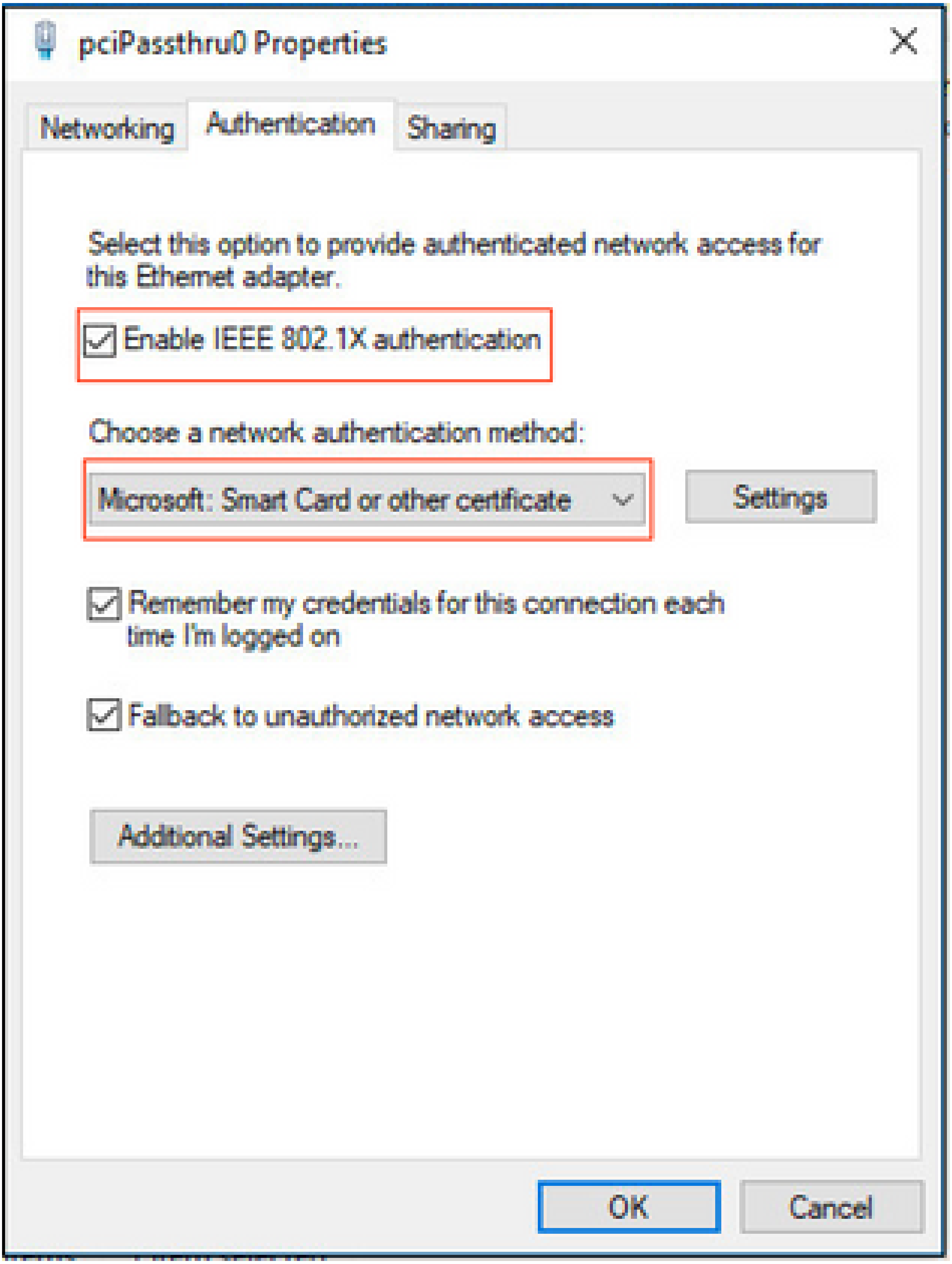
Issued by: testlab-DC1-CA-1

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.启用Dot1x身份验证并将身份验证方法选择为Microsoft：智能卡或其他证书进行EAP-TLS身份验证。



pciPassthru0 Properties

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

☑ Enable IEEE 802.1X authentication

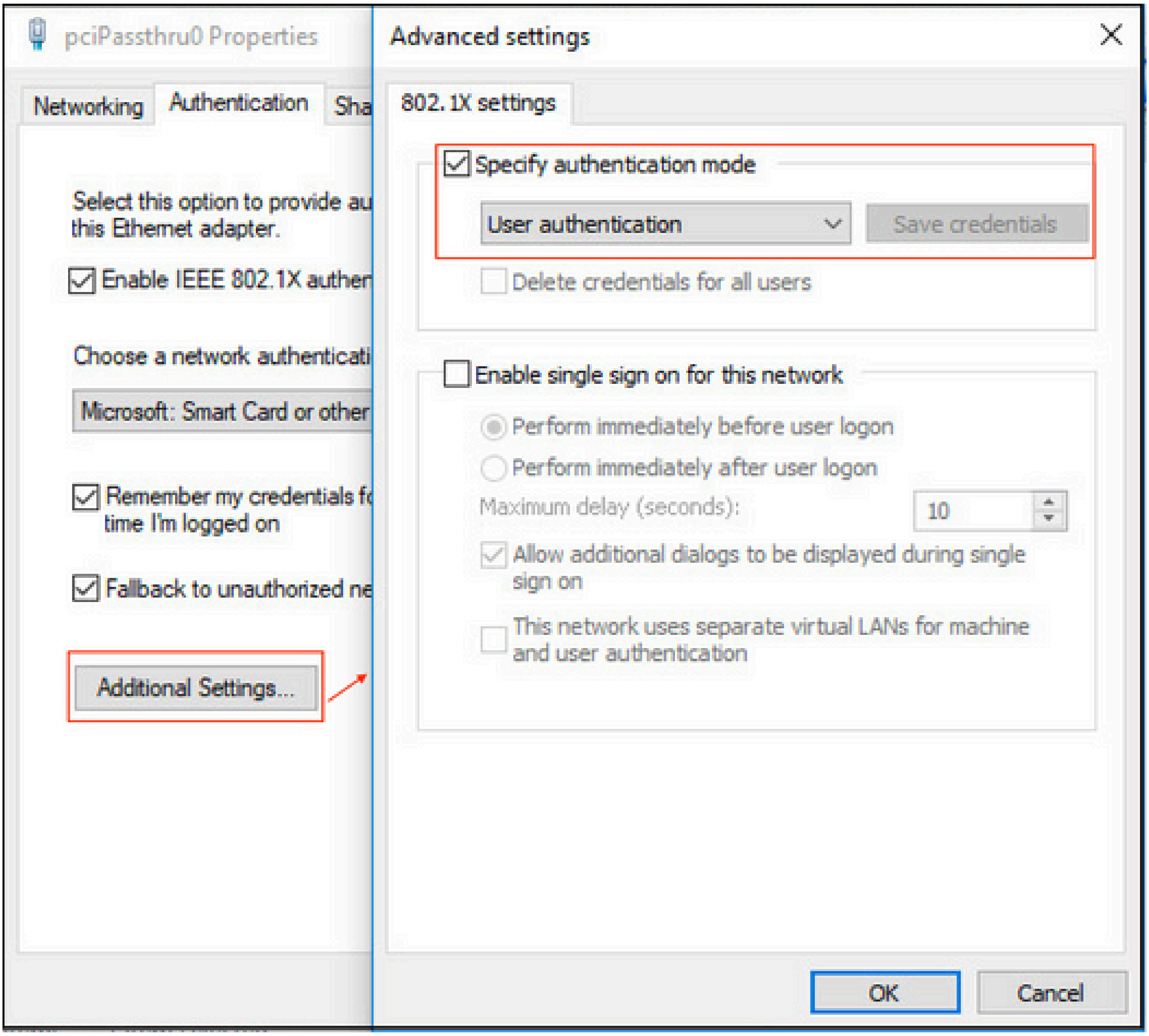
Choose a network authentication method:

Microsoft: Smart Card or other certificate

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

☑ Fallback to unauthorized network access

3.单击“其它设置”，此时将打开一个窗口。选中specify authentication mode复选框，然后选择user authentication，如下图所示。



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

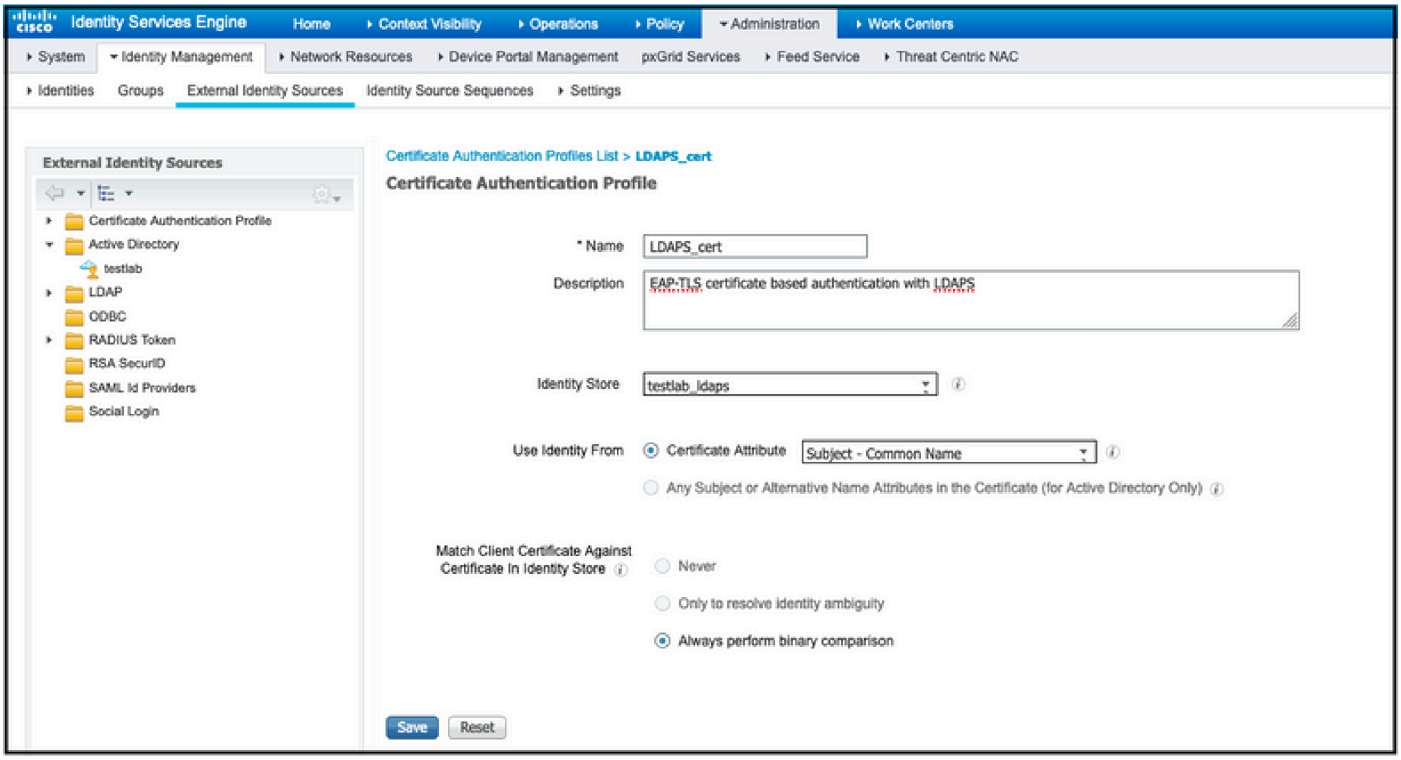
☑ Allow additional dialogs to be displayed during single sign on

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

OK | Cancel

在ISE上配置策略集

由于使用EAP-TLS协议，因此在配置策略集之前，需要配置证书身份验证配置文件，并在稍后在身份验证策略中使用身份源序列。



Certificate Authentication Profiles List > LDAPS_cert

Certificate Authentication Profile

* Name: LDAPS_cert

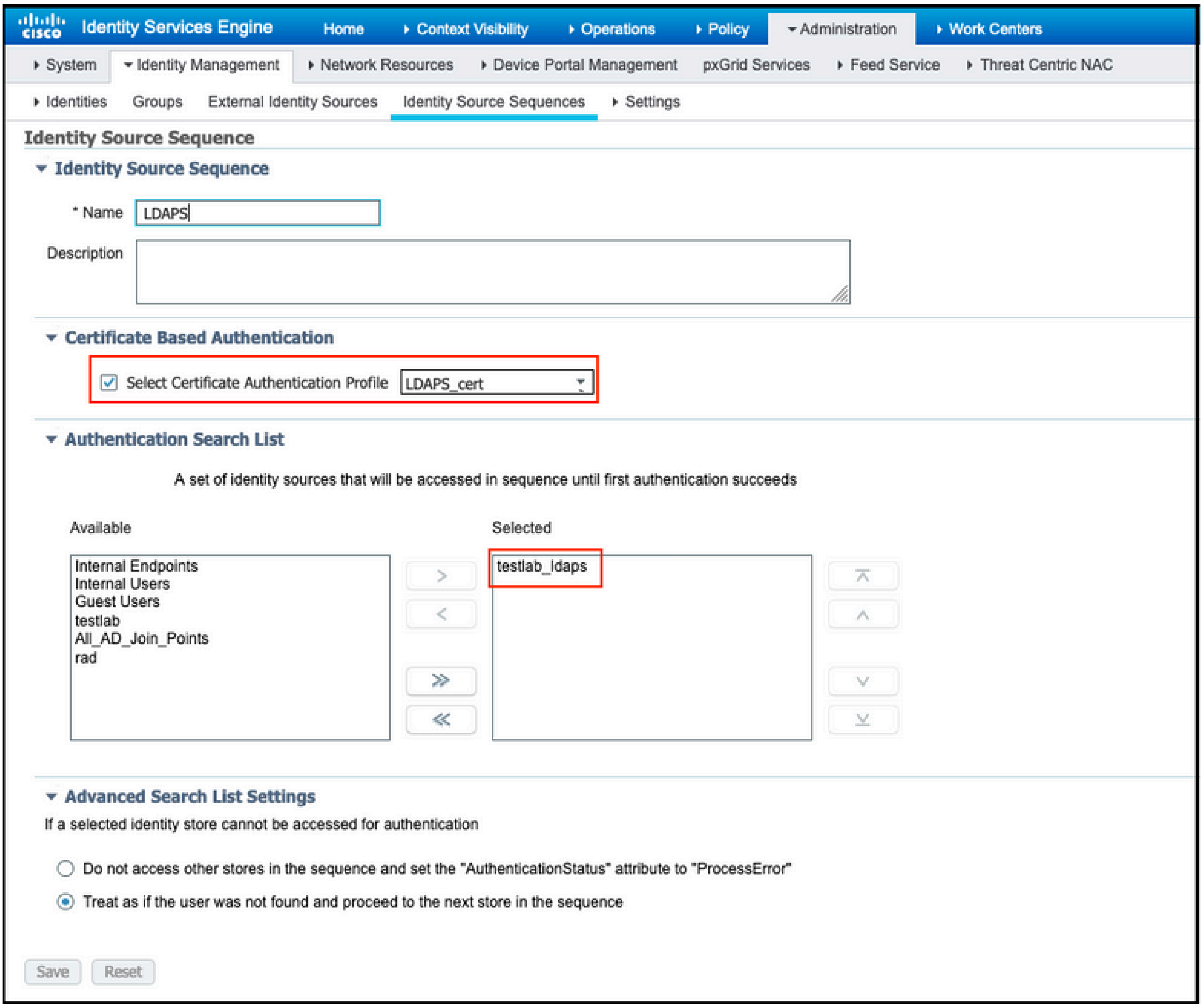
Description: EAP-TLS certificate based authentication with LDAPS

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

请参阅Identity Source Sequence中的Certificate Authentication Profile，并在Authentication Search列表中定义LDAPS外部身份源：



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	Selected
Internal Endpoints Internal Users Guest Users testlab All_AD_Join_Points rad	testlab_ldaps

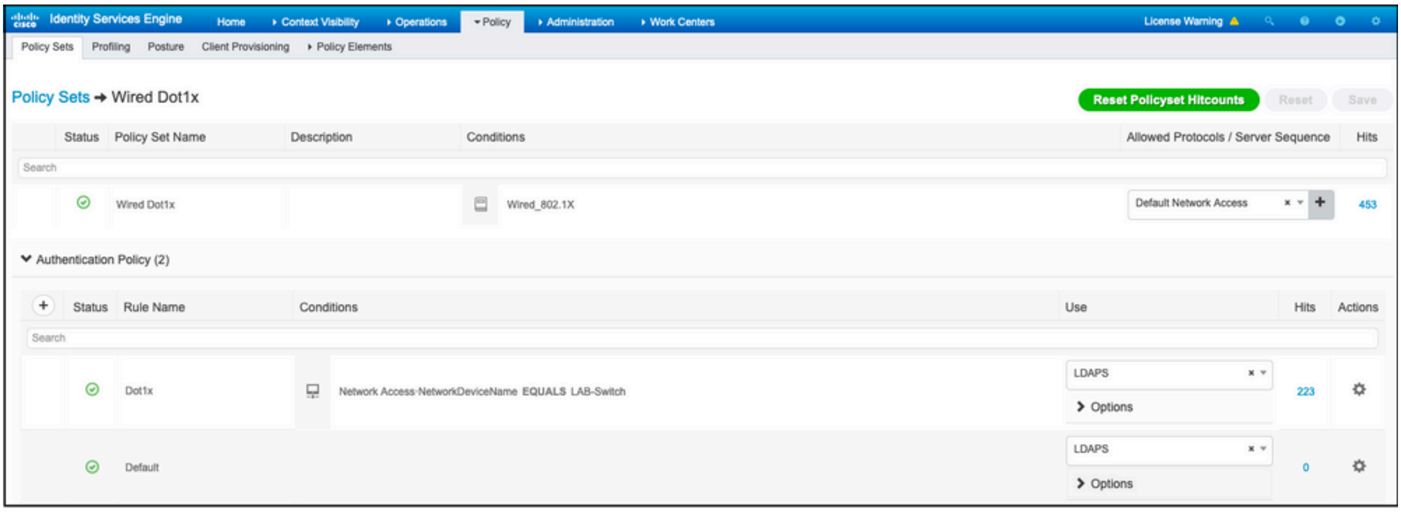
Advanced Search List Settings

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

现在配置有线Dot1x身份验证的策略集：

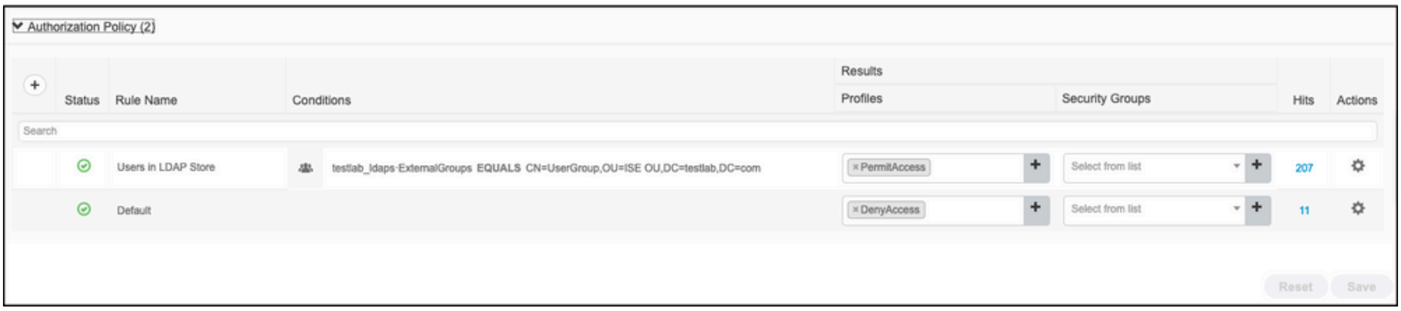


Policy Sets → Wired Dot1x

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

Authentication Policy (2)

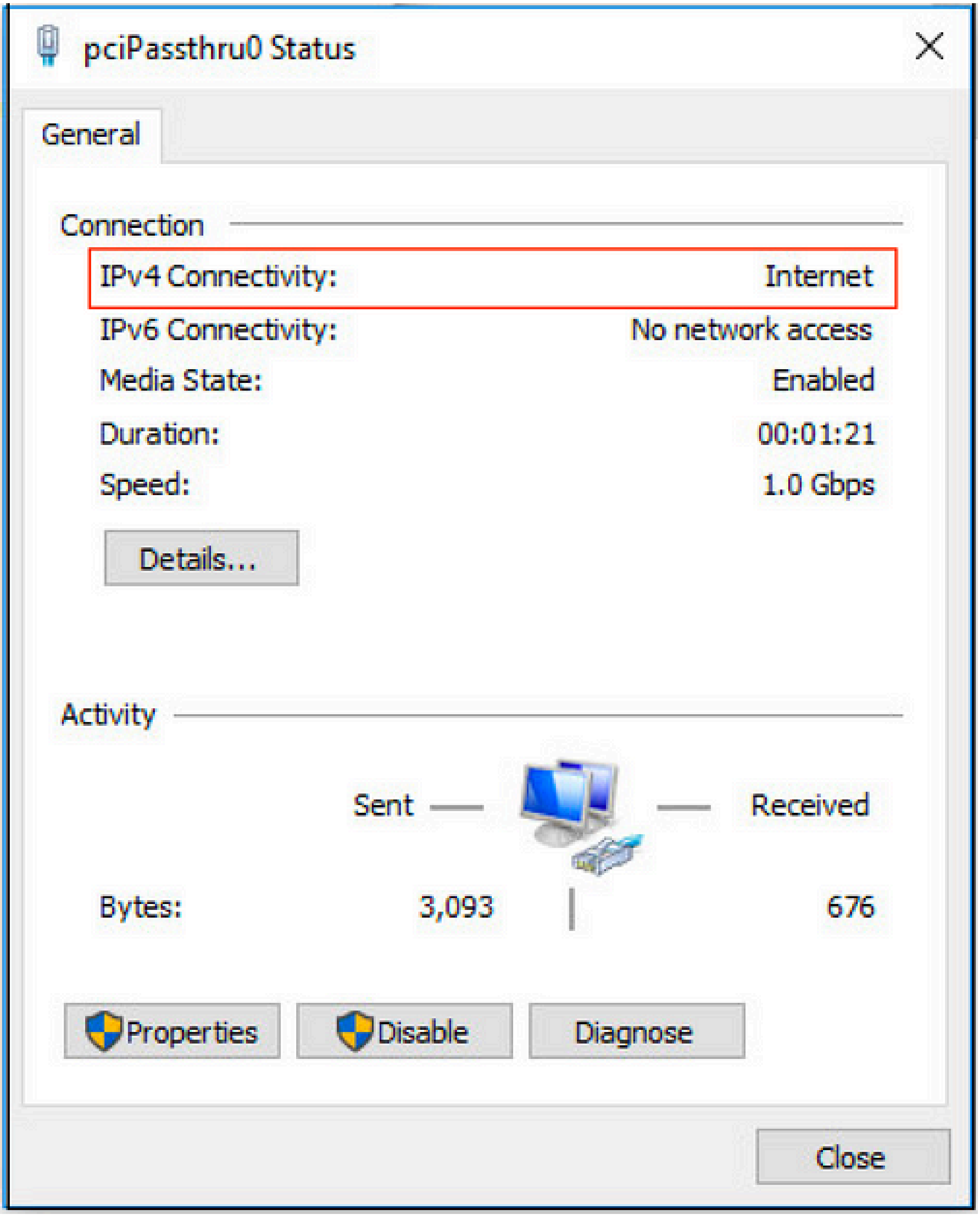
Status	Rule Name	Conditions	Use	Hits	Actions
✓	Dot1x	Network Access·NetworkDeviceName EQUALS LAB-Switch	LDAPS Options	223	
✓	Default		LDAPS Options	0	



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	⚙

完成此配置后，我们可以根据LDAPS身份源使用EAP-TLS协议对终端进行身份验证。



pciPassthru0 Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

Duration: 00:01:21

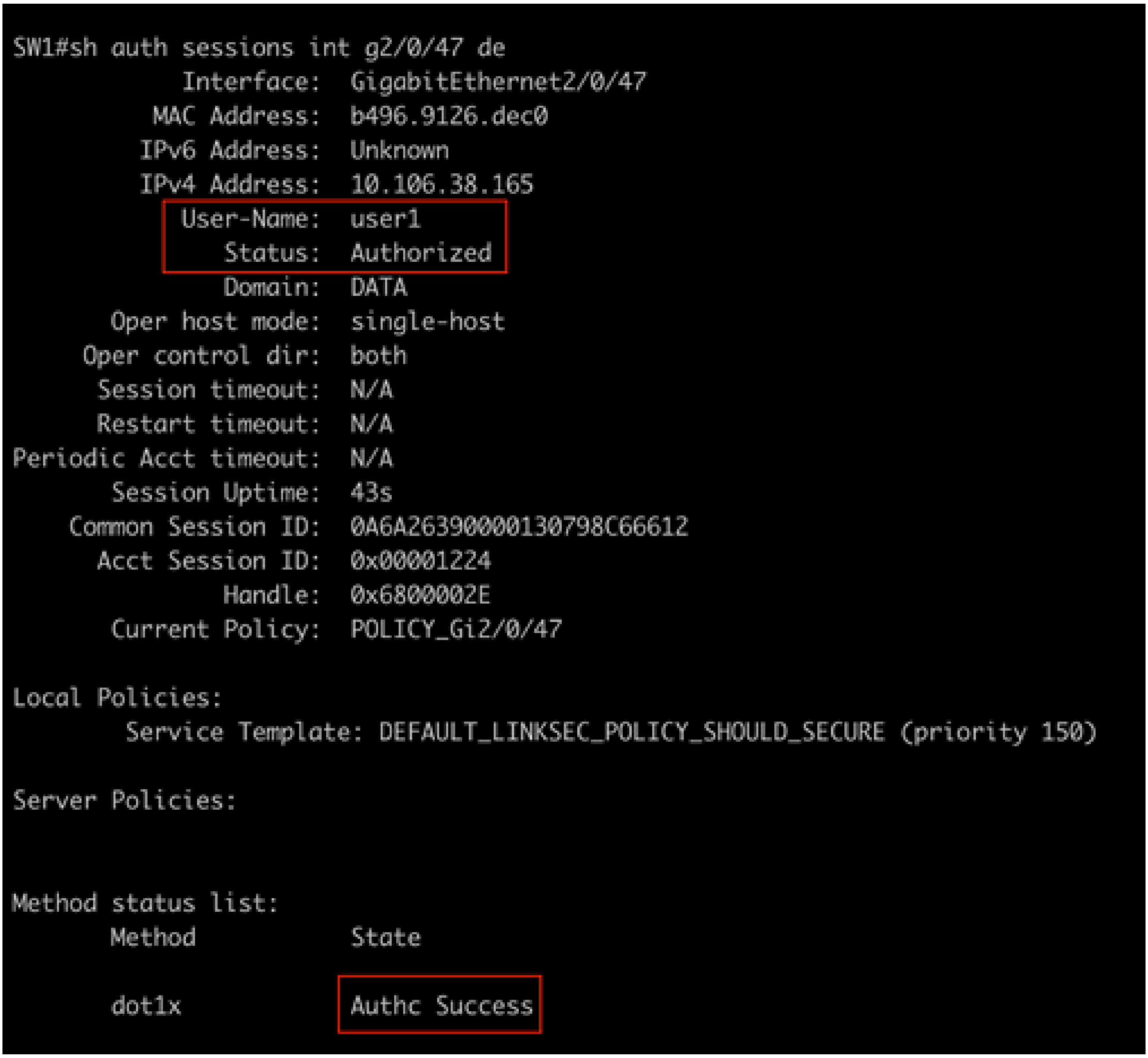
Speed: 1.0 Gbps

Activity

Bytes: 3,093 676

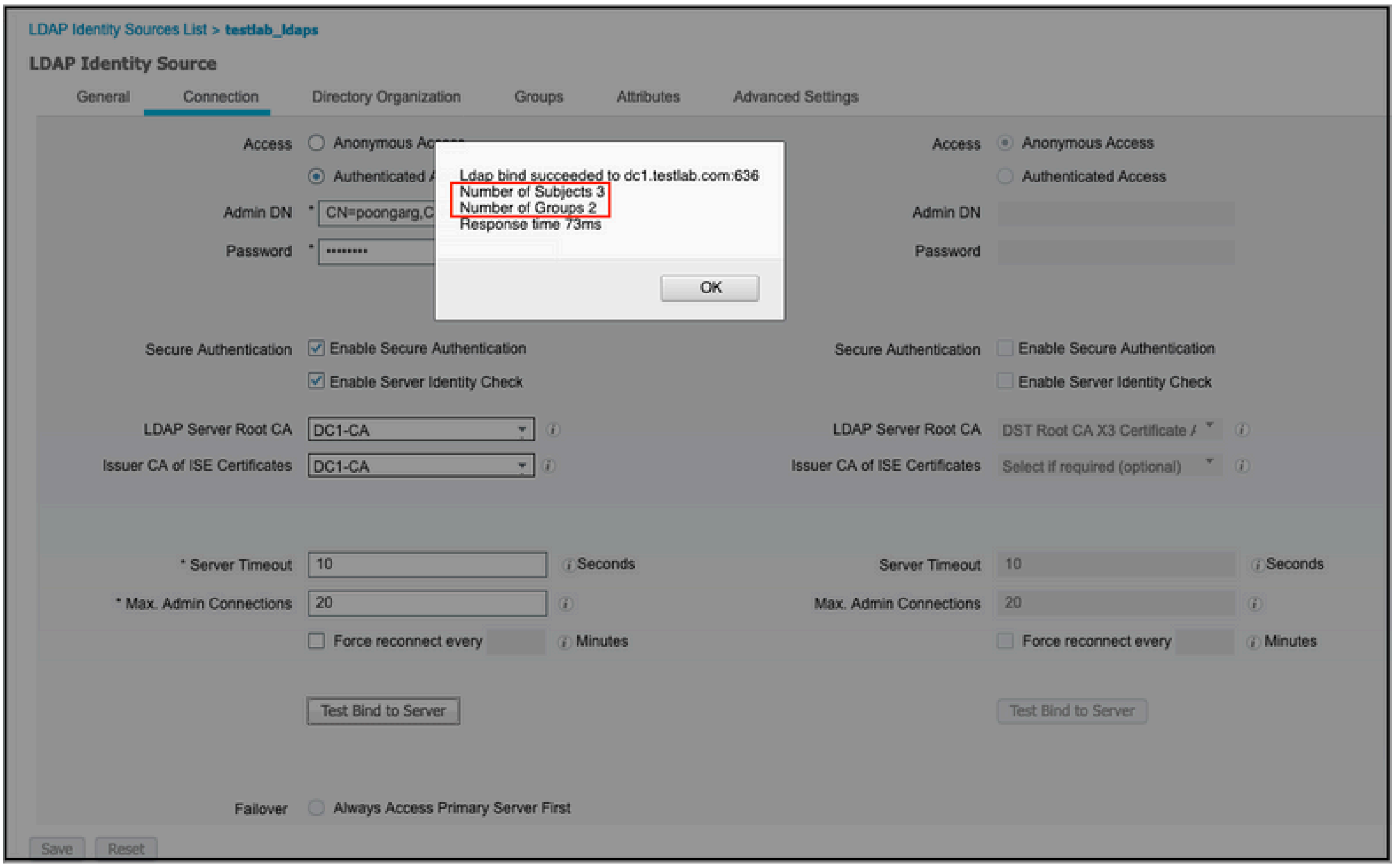
验证

1.检查连接到PC的交换机端口上的身份验证会话：



```
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.为了验证LDAPS和ISE配置，您可以通过测试服务器连接来检索主题和组：



LDAP Identity Sources List > testlab_ldaps

LDAP Identity Source

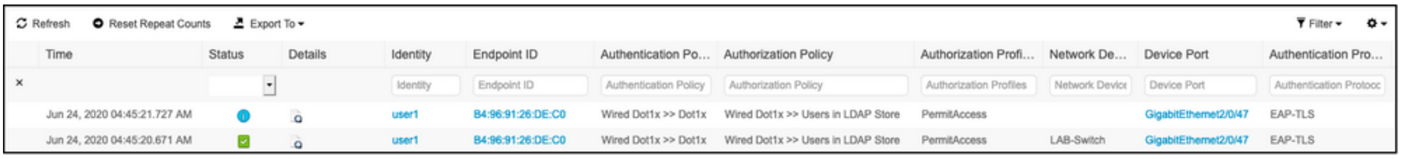
Ldap bind succeeded to dc1.testlab.com:636
Number of Subjects 3
Number of Groups 2
Response time 73ms

OK

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

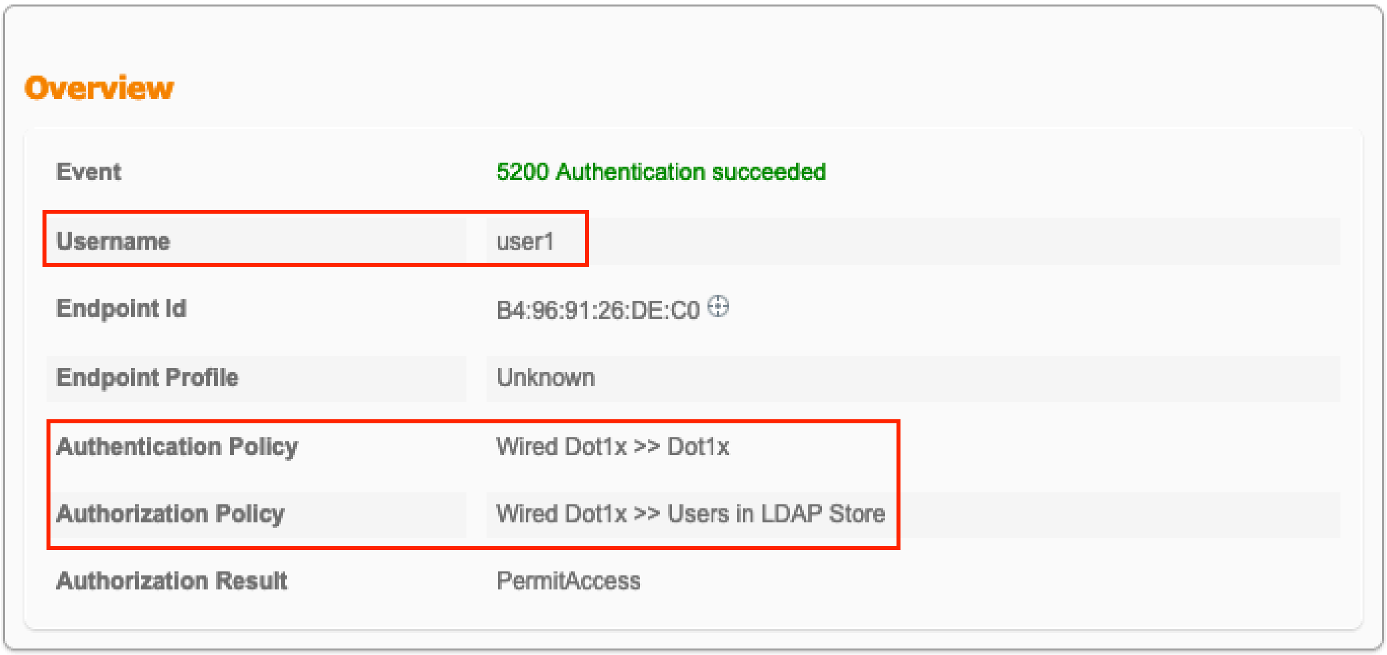
Access	● Anonymous Access ○ Authenticated Access
Admin DN	
Password	
Secure Authentication	□ Enable Secure Authentication □ Enable Server Identity Check
LDAP Server Root CA	DST Root CA X3 Certificate /
Issuer CA of ISE Certificates	Select if required (optional)
Server Timeout	10 Seconds
Max. Admin Connections	20
	□ Force reconnect every Minutes
	Test Bind to Server

3.验证用户身份验证报告：



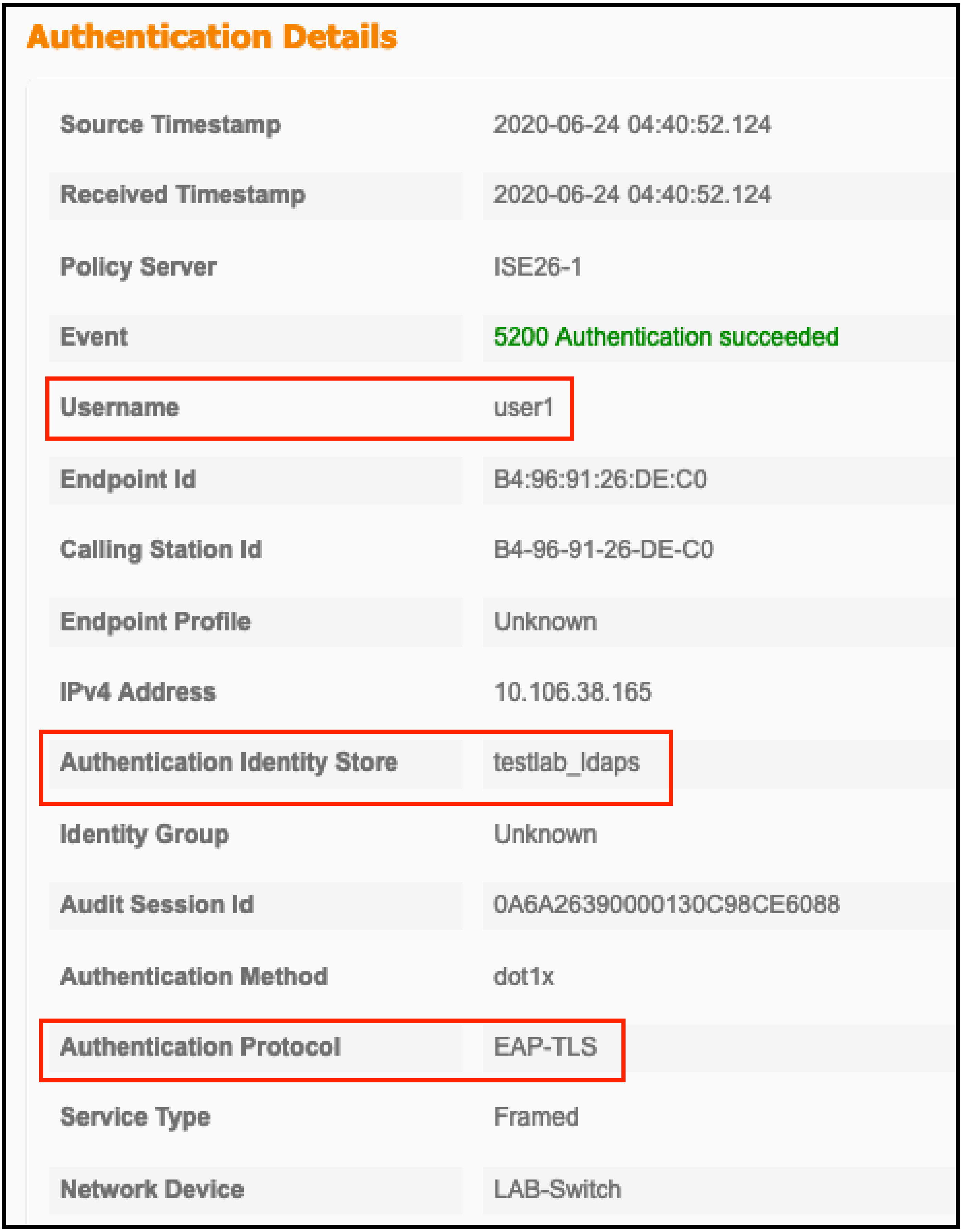
Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...	Network De...	Device Port	Authentication Pro...
Jun 24, 2020 04:45:21.727 AM	●		user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess		GigabitEthernet2/0/47	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.检查终端的详细身份验证报告：



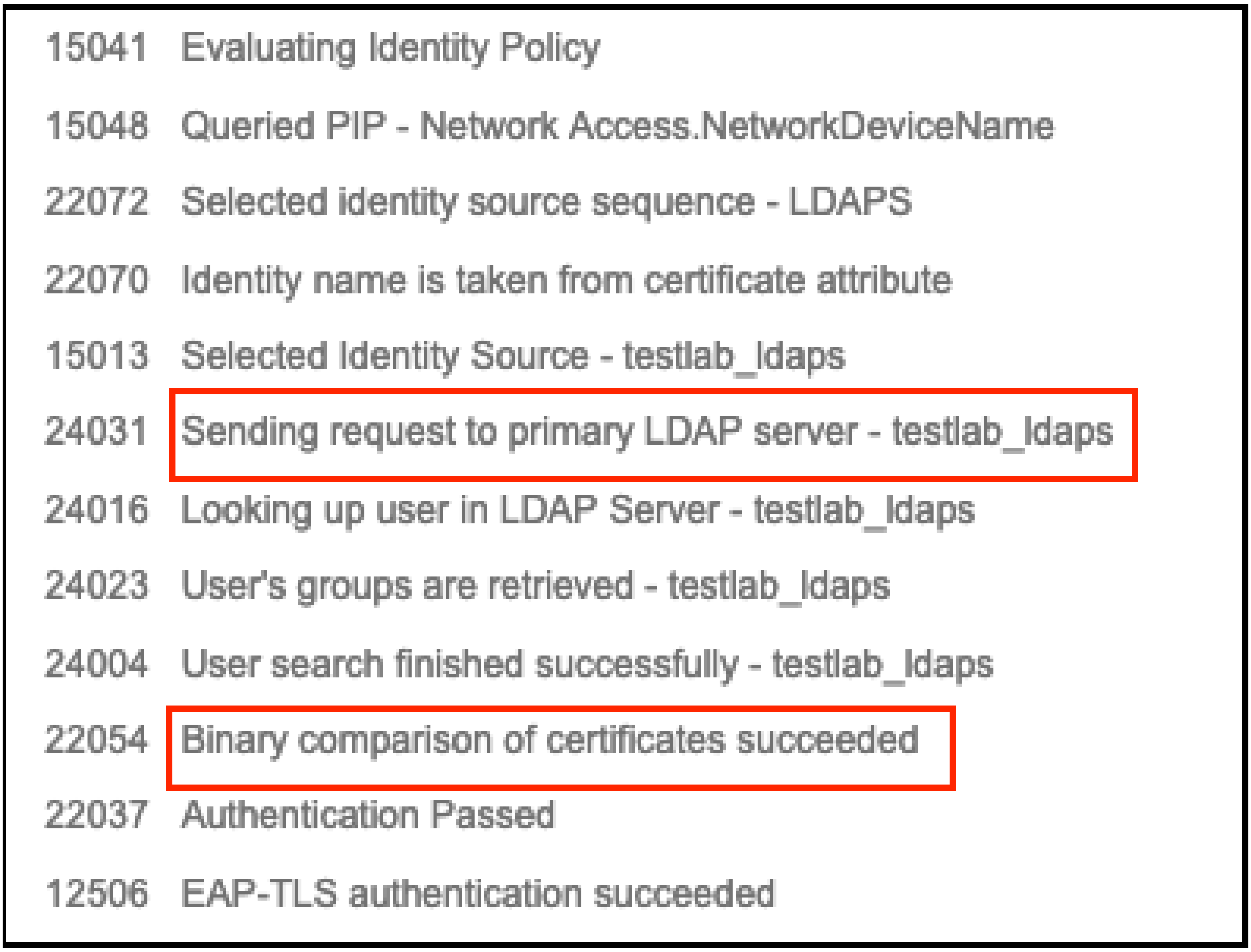
Overview

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

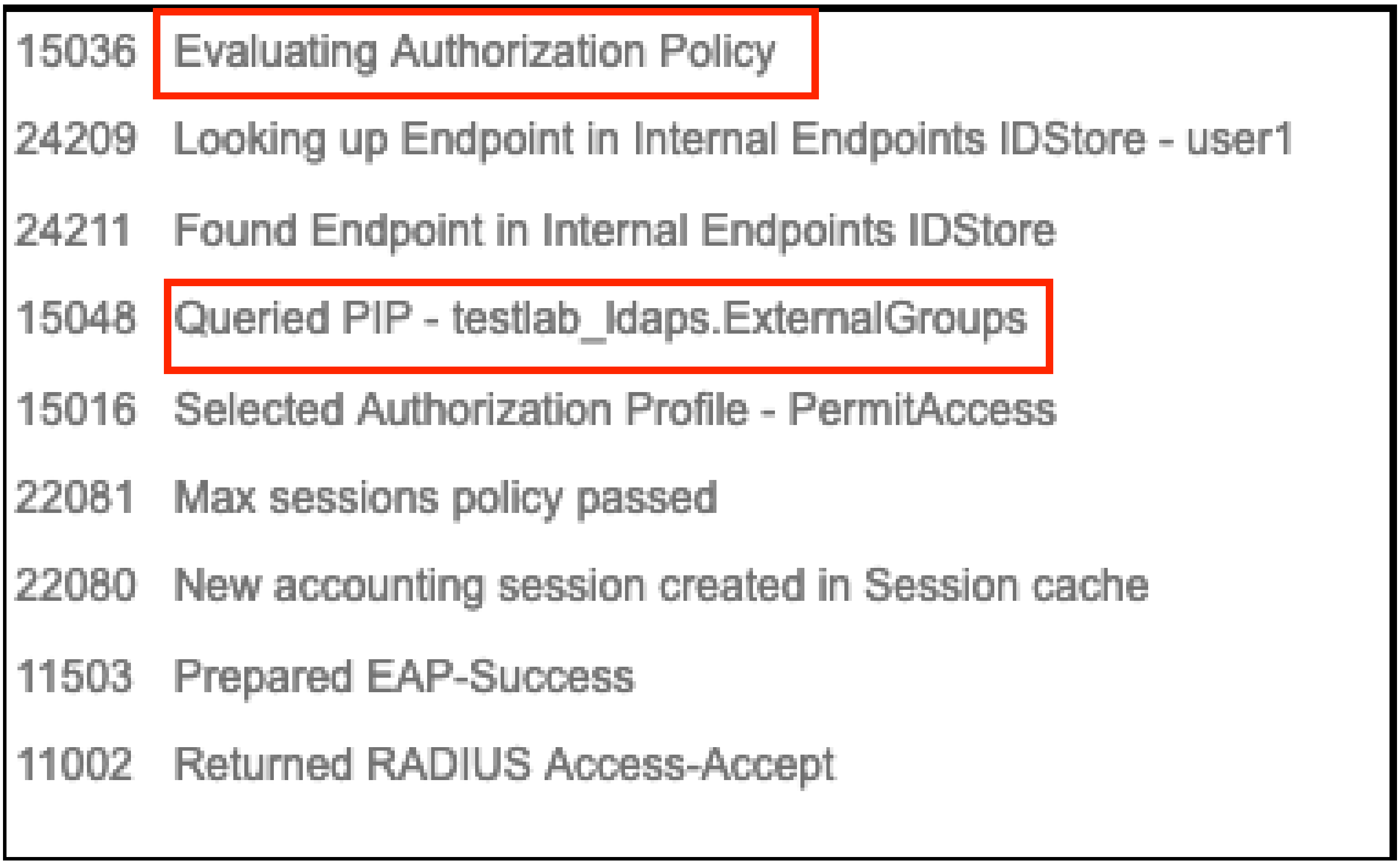


Authentication Details

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

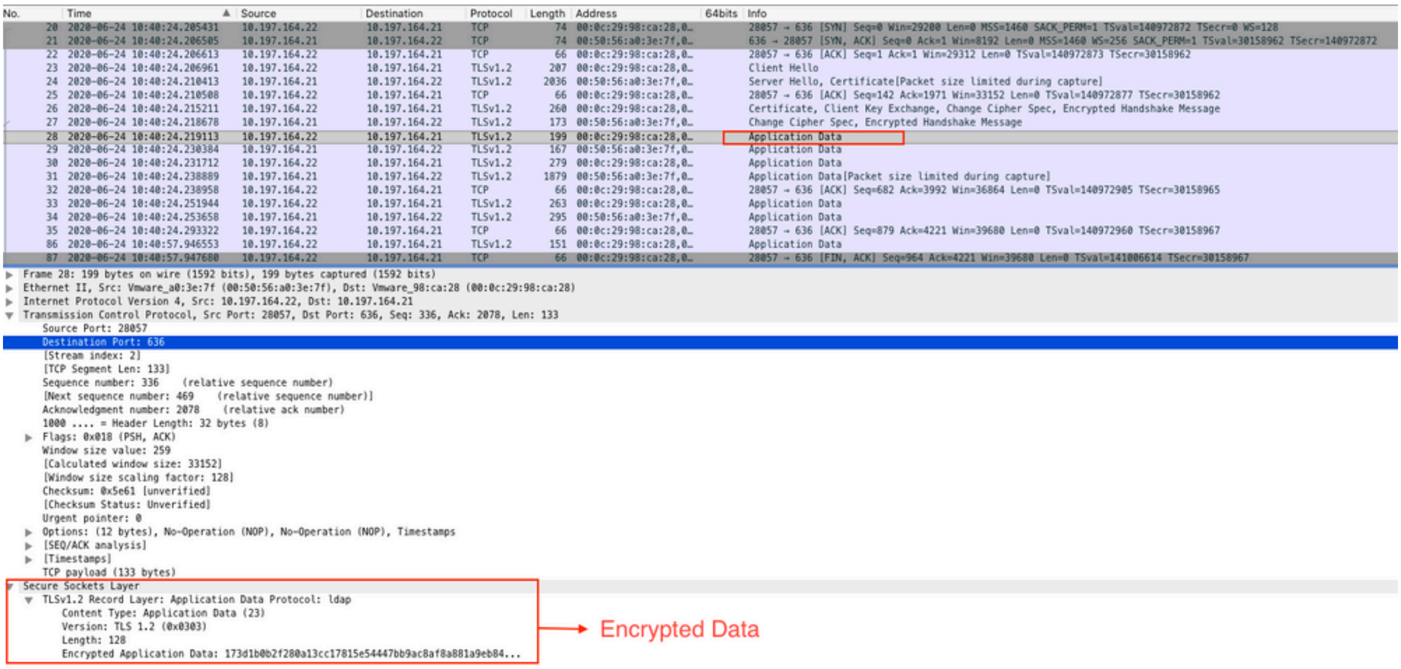


```
15041   Evaluating Identity Policy
15048   Queried PIP - Network Access.NetworkDeviceName
22072   Selected identity source sequence - LDAPS
22070   Identity name is taken from certificate attribute
15013   Selected Identity Source - testlab_ldaps
24031   Sending request to primary LDAP server - testlab_ldaps
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.通过在ISE上捕获指向LDAPS服务器的数据包，验证ISE和LDAPS服务器之间的数据已加密：



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

故障排除

本节介绍此配置遇到的一些常见错误以及如何进行故障排除。

- 在身份验证报告中，您可能会看到以下错误消息：

```
Authentication method is not supported by any applicable identity store
```

此错误消息表明LDAP不支持您选择的方法。确保同一报告中的身份验证协议显示其中一个受支持的方法（EAP-GTC、EAP-TLS或PEAP-TLS）。

- 到服务器的测试绑定已结束，但出现错误。

这通常是由于LDAPS服务器证书验证检查失败。为了排除此类故障，请在ISE上捕获数据包，并在调试级别启用所有三个运行时和prrt-jni组件，重新创建问题，然后检查prrt-server.log文件。

数据包捕获投诉错误的证书，并且prrt-server显示：

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

注意：LDAP页面中的主机名必须使用证书的使用者名称（或任何使用者替代名称）进行配置。因此，除非主题或SAN中有此类证书，否则它不起作用，因此需要使用SAN列表中具有IP地址的证书。

3.在身份验证报告中，您可能会注意到未在身份库中找到主题。这意味着报告的用户名与LDAP数据库中任何用户的主题名称属性都不匹配。在此方案中，此属性值设置为sAMAccountName，这意味着ISE在尝试查找匹配项时查找LDAP用户的sAMAccountName值。

4.在绑定到服务器测试期间无法正确检索主题和组。导致此问题的最可能原因是搜索库配置不正确。请记住，必须从枝叶到根和dc（可包含多个单词）指定LDAP层次结构。

相关信息

- 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