

# Konfiguration und Fehlerbehebung bei ISE mit externem LDAPS Identity Store

## Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Konfigurieren](#)
- [Netzwerkdiagramm](#)
- [Konfigurieren von LDAPS in Active Directory](#)
- [Installieren des Identitätszertifikats auf dem Domänencontroller](#)
- [Zugriff auf die LDAP-Verzeichnisstruktur](#)
- [Integration der ISE mit dem LDAPS-Server](#)
- [Konfigurieren des Switches](#)
- [Konfigurieren des Endpunkts](#)
- [Konfigurieren des Richtliniensatzes auf der ISE](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)
- [Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird die Integration der Cisco ISE mit dem Secure LDAPS-Server als externe Identitätsquelle beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Identity Service Engine (ISE)-Administration
- Grundkenntnisse von Active Directory/Secure Lightweight Directory Access Protocol (LDAPS)

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE 2.6 Patch 7
- Microsoft Windows 2012 R2 mit installierten Active Directory Lightweight Directory Services
- Windows 10-Betriebssystem-PC mit nativem Supplicant und installiertem Benutzerzertifikat
- Cisco Switch C3750X mit 152-2.E6-Image

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

LDAPS ermöglicht die Verschlüsselung von LDAP-Daten (einschließlich Benutzeranmeldeinformationen) bei der Übertragung, wenn eine Verzeichnisbindung eingerichtet wird. LDAPS verwendet TCP-Port 636.

Diese Authentifizierungsprotokolle werden von LDAPS unterstützt:

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

---

**Hinweis:** EAP-MSCHAPV2 (als innere Methode von PEAP, EAP-FAST oder EAP-TTLS), LEAP, CHAP und EAP-MD5 werden von der externen LDAPS-Identitätsquelle nicht unterstützt.

---

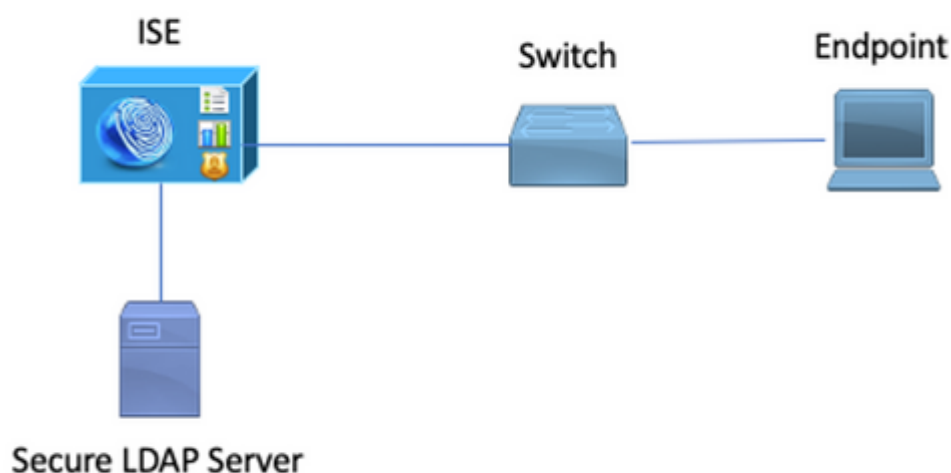
## Konfigurieren

In diesem Abschnitt werden die Konfiguration der Netzwerkgeräte und die Integration der ISE in den LDAPS-Server von Microsoft Active Directory (AD) beschrieben.

### Netzwerkdiagramm

In diesem Konfigurationsbeispiel verwendet der Endpunkt eine Ethernet-Verbindung mit einem Switch für die Verbindung mit dem LAN. Der verbundene Switch-Port ist für die 802.1x-Authentifizierung konfiguriert, um die Benutzer mithilfe der ISE zu authentifizieren. Auf der ISE wird LDAPS als externer Identitätsspeicher konfiguriert.

Dieses Bild zeigt die Netzwerktopologie, die verwendet wird:

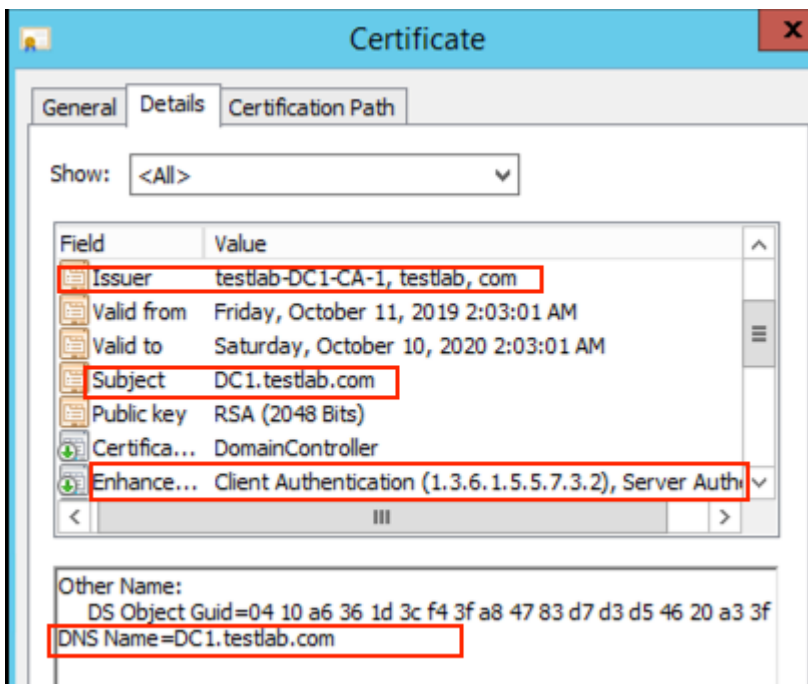


## Konfigurieren von LDAPS in Active Directory

## Installieren des Identitätszertifikats auf dem Domänencontroller

Um LDAPS zu aktivieren, installieren Sie ein Zertifikat auf dem Domänencontroller (DC), das folgende Anforderungen erfüllt:

1. Das LDAPS-Zertifikat befindet sich im persönlichen Zertifikatspeicher des Domänencontrollers.
2. Ein privater Schlüssel, der mit dem Zertifikat übereinstimmt, ist im Speicher des Domänencontrollers vorhanden und dem Zertifikat richtig zugeordnet.
3. Die Erweiterung "Erweiterte Schlüsselverwendung" enthält die Objektkennung für die Serverauthentifizierung (1.3.6.1.5.5.7.3.1) (auch als OID bezeichnet).
4. Der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) des Domänencontrollers (z. B. DC1.testlab.com) muss in einem der folgenden Attribute vorhanden sein: dem Common Name (CN) im Feld "Subject" (Betreff) und dem DNS-Eintrag in der Subject Alternative Name Extension (Erweiterung des alternativen Betreffs).
5. Das Zertifikat muss von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestellt werden, der der Domänencontroller und die LDAP-Clients vertrauen. Für eine vertrauenswürdige sichere Kommunikation müssen der Client und der Server der Stammzertifizierungsstelle und den zwischengeschalteten Zertifizierungsstellenzertifikaten der jeweils anderen Seite vertrauen, die Zertifikate für diese ausgestellt haben.
6. Zur Generierung des Schlüssels muss der Channel Cryptographic Service Provider (CSP) verwendet werden.



## Zugriff auf die LDAP-Verzeichnisstruktur

Um auf das LDAPS-Verzeichnis auf dem Active Directory-Server zuzugreifen, verwenden Sie einen beliebigen LDAP-Browser. In dieser Übung wird der Softerra LDAP-Browser 4.5 verwendet.

1. Stellen Sie eine Verbindung zur Domäne auf dem TCP-Port 636 her.

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

2. Erstellen Sie der Einfachheit halber eine Organisationseinheit (OU) mit dem Namen ISE OU im AD, und diese muss über eine Gruppe mit dem Namen UserGroup verfügen. Erstellen Sie zwei Benutzer (user1 und user2), und machen Sie sie zu Mitgliedern der Benutzergruppe.

**Hinweis:** Die LDAP-Identitätsquelle auf der ISE wird nur für die Benutzerauthentifizierung verwendet.

Name	Value	Type
OU=ISE OU		Organizational Unit
OU=ISE Group		Organizational Unit
CN=UserGroup		Group
CN=user2		User
CN=user1		User
CN=DESKTOP-19		Computer
CN=ComputerGroup		Group
distinguishedName	OU=ISE OU,DC=testlab,DC=com	String
dSCorePropagationData	1/1/1601	String
dSCorePropagationData	6/20/2020 2:51:11 AM	String
gPLink	[LDAP://cn={21A53B13-6971-45E8-8545-FD0C68E29790},c...	String
instanceType	[ Writable ]	String
name	ISE OU	String
objectCategory	CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=...	String
objectClass	organizationalUnit	String
objectClass	top	String
ou	ISE OU	String
uSNChanged	607428	String
uSNCreated	603085	String
whenChanged	6/21/2020 2:44:06 AM	String
whenCreated	6/20/2020 2:51:11 AM	String
objectGUID	{44F45D1D-17B7-480F-ABC6-3ED27FA4F694}	Binary

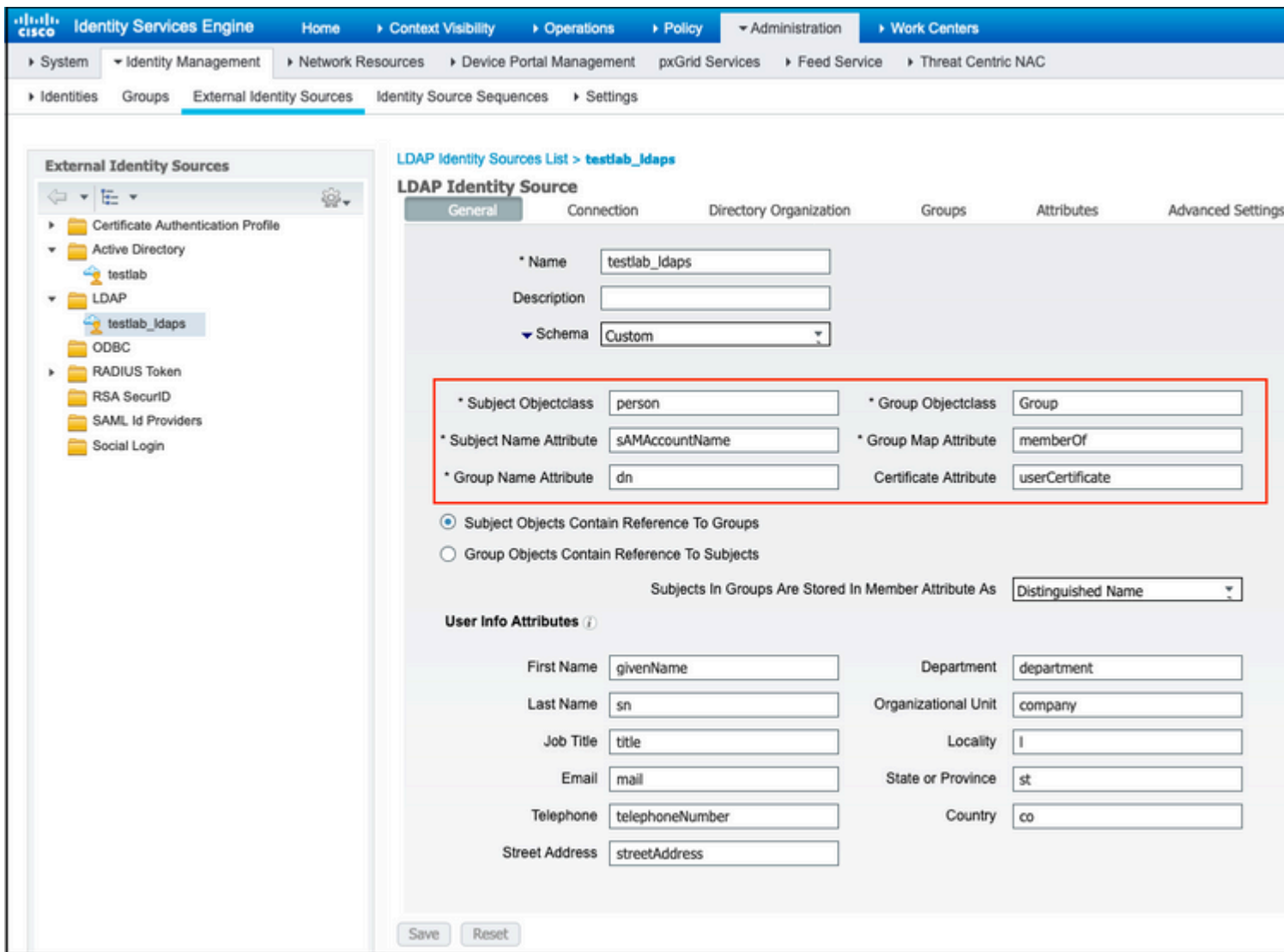
## Integration der ISE mit dem LDAPS-Server

1. Importieren Sie das Zertifikat der LDAP-Server-Stammzertifizierungsstelle in das vertrauenswürdige Zertifikat.

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

2. Validieren Sie das ISE-Admin-Zertifikat, und stellen Sie sicher, dass das ISE-Admin-Zertifikat auch im vertrauenswürdigen Zertifikatspeicher vorhanden ist.

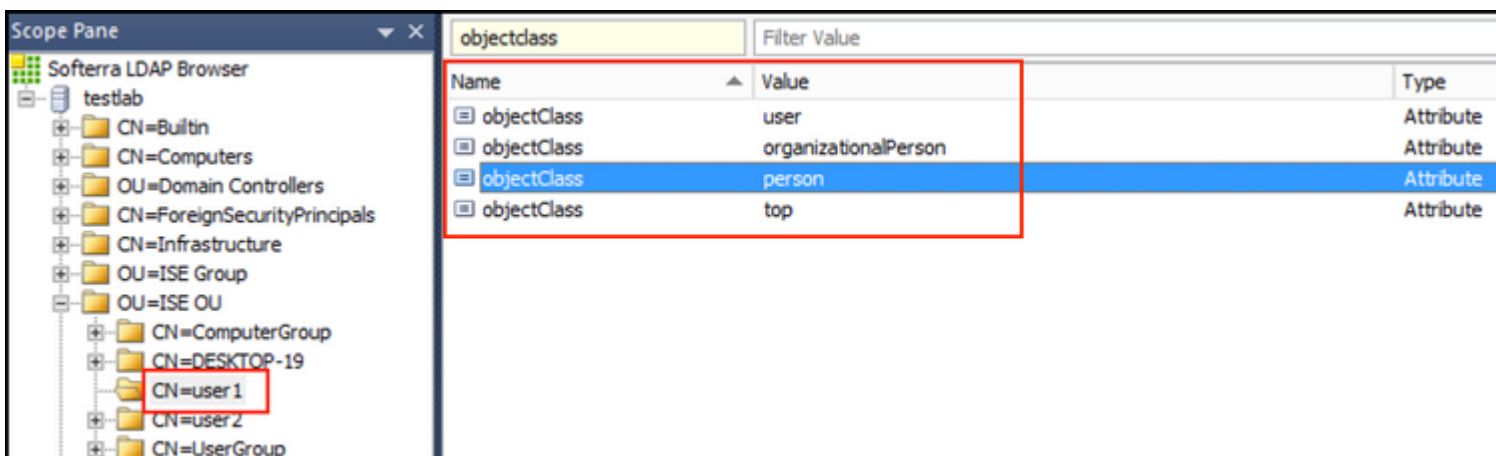
3. Um den LDAPS-Server zu integrieren, nutzen Sie die verschiedenen LDAP-Attribute aus dem LDAPS-Verzeichnis. Navigieren Sie zu **Administration > Identity Management > External Identity Sources > LDAP Identity Sources > Add**.



4. Konfigurieren Sie diese Attribute über die Registerkarte Allgemein:

Subject Object class: Dieses Feld entspricht der Object-Klasse von Benutzerkonten. Hier können Sie eine der vier Klassen verwenden:

- Oben
- Person
- Organisatorische Person
- InetOrgPerson



Subject Name Attribute (Attribut für den Antragstellernamen): Dieses Feld ist der Name des Attributs, das den Benutzernamen aus der Anforderung enthält. Dieses Attribut wird vom LDAPS abgerufen, wenn die ISE einen bestimmten Benutzernamen in der LDAP-Datenbank anfordert (Sie können cn, sAMAccountName usw. verwenden). In diesem Szenario wird der Benutzername user1 auf dem Endpunkt verwendet.

Scope Pane

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
<b>sAMAccountName</b>	<b>user1</b>	<b>Attribute</b>
userPrincipalName	user1@testlab.com	Attribute
userCertificate	user1	Binary Attribute

Gruppennamen-Attribut: Dies ist das Attribut, das den Namen einer Gruppe enthält. Die Attributwerte des Gruppennamen in Ihrem LDAP-Verzeichnis müssen mit den LDAP-Gruppennamen auf der Seite Benutzergruppen übereinstimmen.

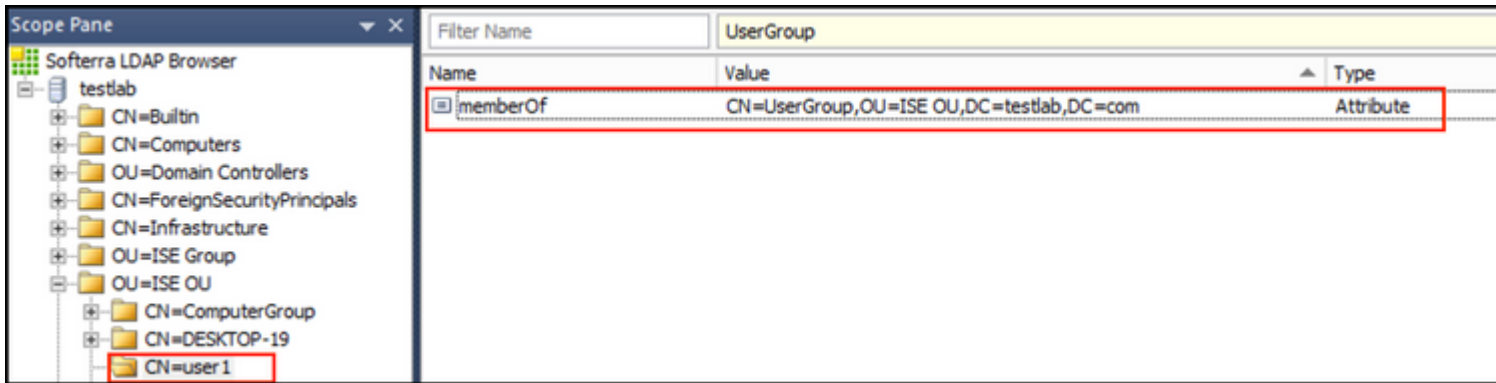
Scope Pane

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

Group ObjectClass (Gruppenobjektklasse): Dieser Wert wird bei Suchvorgängen verwendet, um die als Gruppen erkannten Objekte anzugeben.

objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
objectGUID	{39967F90-898E-44B5-9CC5-B28C0B0EB234}	Binary Attribute
objectClass	top	Attribute
<b>objectClass</b>	<b>group</b>	<b>Attribute</b>
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute

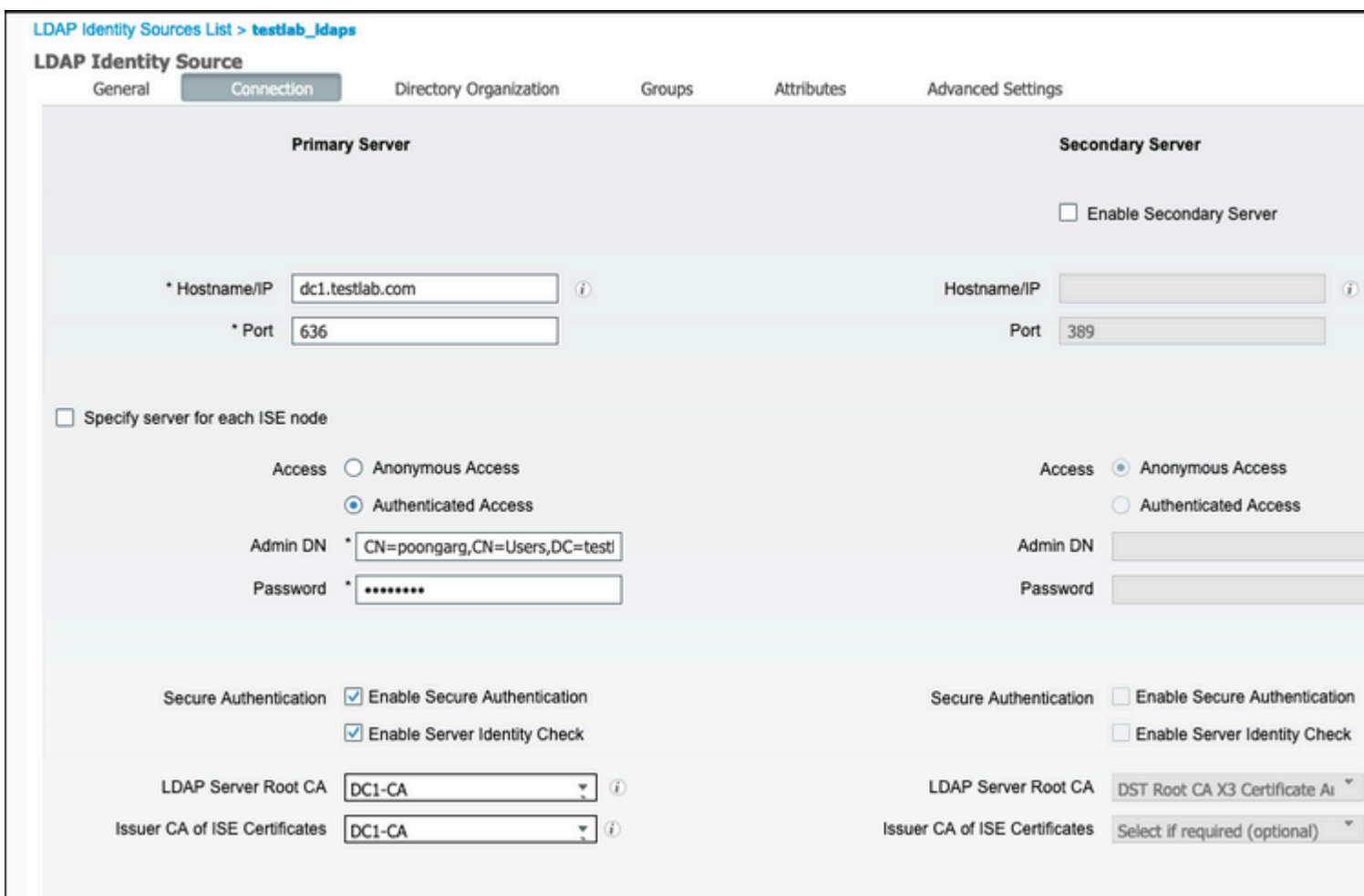
Gruppenzuordnungsattribut: Dieses Attribut definiert, wie die Benutzer den Gruppen zugeordnet werden.

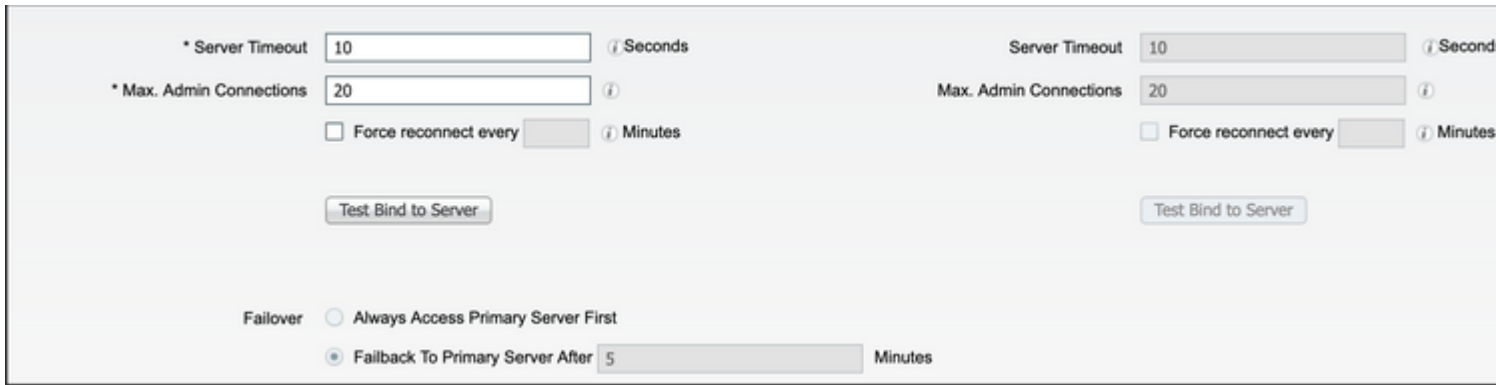


Zertifikatattribut: Geben Sie das Attribut ein, das die Zertifikatdefinitionen enthält. Diese Definitionen können optional verwendet werden, um Zertifikate zu validieren, die von Clients vorgelegt werden, wenn sie als Teil eines Zertifikatauthentifizierungsprofils definiert werden. In diesem Fall wird ein Binärvergleich zwischen dem Clientzertifikat und dem aus der LDAP-Identitätsquelle abgerufenen Zertifikat durchgeführt.



5. Um die LDAPS-Verbindung zu konfigurieren, navigieren Sie zur Registerkarte **Verbindung**:





\* Server Timeout  (i) Seconds

\* Max. Admin Connections  (i)

Force reconnect every  (i) Minutes

Failover  Always Access Primary Server First

Failback To Primary Server After  Minutes

6. Führen Sie dsquery auf dem Domänencontroller aus, um den Benutzernamen-DN abzurufen, mit dem eine Verbindung zum LDAP-Server hergestellt werden soll:

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

Schritt 1: SLegen Sie die richtige IP-Adresse oder den richtigen Hostnamen des LDAP-Servers fest, legen Sie den LDAPS-Port (TCP 636) fest, und richten Sie eine Admin-DN ein, um eine Verbindung mit dem LDAP über SSL herzustellen.

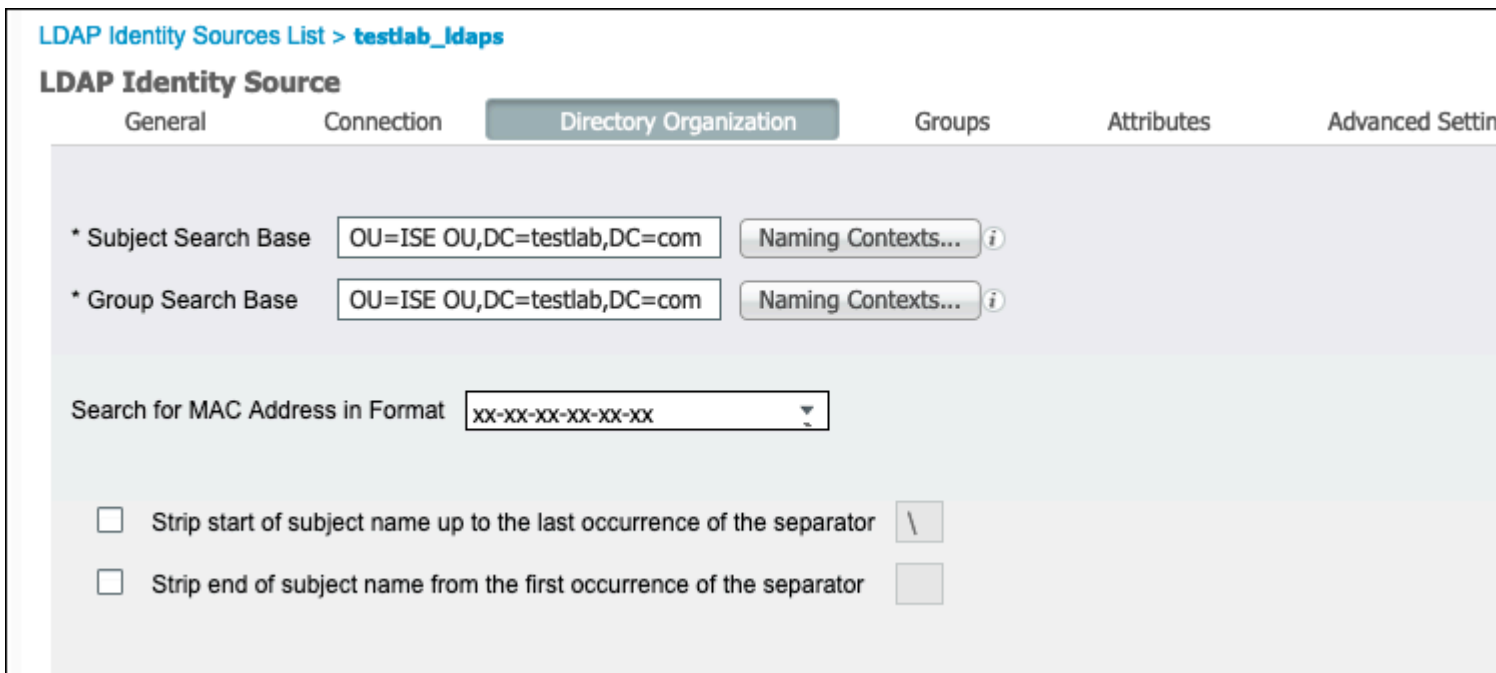
Schritt 2: Aktivieren Sie die Option Sichere Authentifizierung und Serveridentitätsprüfung.

Schritt 3: Wählen Sie aus dem Dropdown-Menü das Zertifikat der LDAP-Server-Stammzertifizierungsstelle und das ISE-Admin-Zertifikat des Isser-Zertifizierungsstellenzertifikats aus (Wir haben die Zertifizierungsstelle verwendet, die auf demselben LDAP-Server installiert ist, um auch das ISE-Admin-Zertifikat auszustellen).

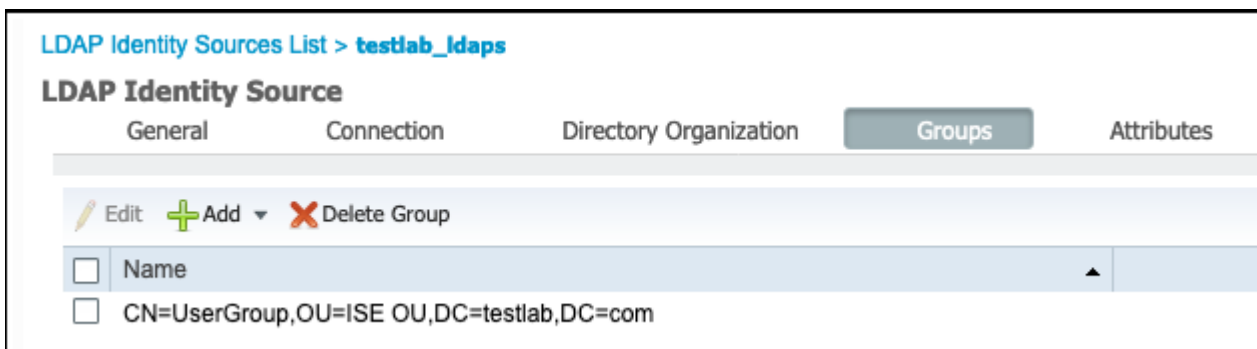
Schritt 4: Wählen Sie die Testbindung an den Server aus. An dieser Stelle werden keine Themen oder Gruppen abgerufen, da die Suchbasis noch nicht konfiguriert ist.

7. Konfigurieren Sie auf der Registerkarte **Verzeichnisorganisation** die Suchbasis für Betreff/Gruppe. Dies ist der Verknüpfungspunkt zwischen der ISE und dem LDAP. Jetzt können Sie nur Themen und Gruppen abrufen, die Kinder des Verbindungspunkts sind. In diesem Szenario werden der Betreff und die Gruppe aus der OU=ISE-OU abgerufen.





8. Klicken Sie unter Gruppen auf Hinzufügen, um die Gruppen aus dem LDAP auf der ISE zu importieren und die Gruppen abzurufen, wie in diesem Bild dargestellt.



## Konfigurieren des Switches

Konfigurieren Sie den Switch für die 802.1x-Authentifizierung. Windows PC ist mit Switch-Port Gig2/0/47 verbunden

```
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
```

!

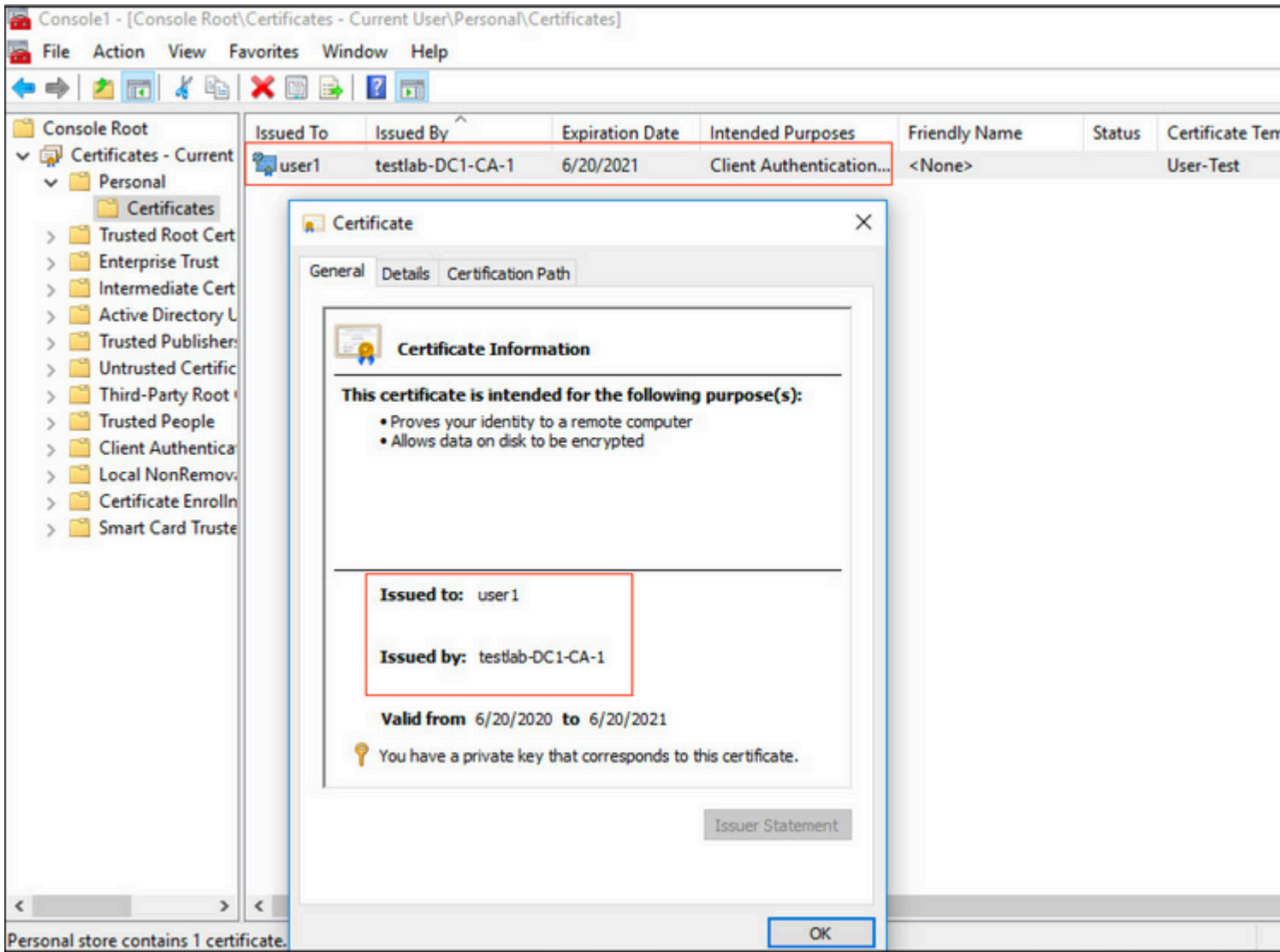
```
aaa authentication dot1x default group ISE_SERVERS local
aaa authorization network default group ISE_SERVERS
```

```
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
```

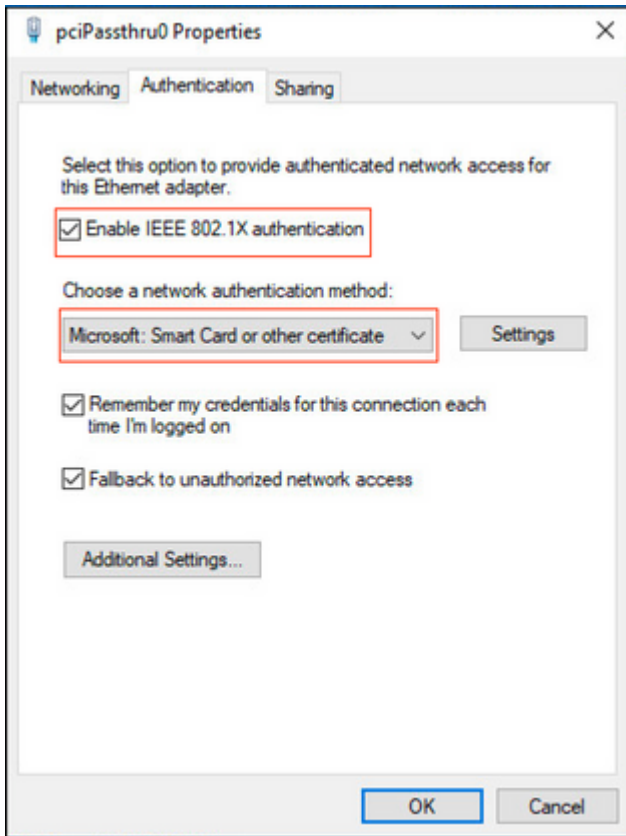
## **Konfigurieren des Endpunkts**

Windows Native Supplicant wird verwendet, und eines der LDAP-unterstützten EAP-Protokolle wird verwendet, EAP-TLS für die Benutzerauthentifizierung und -autorisierung.

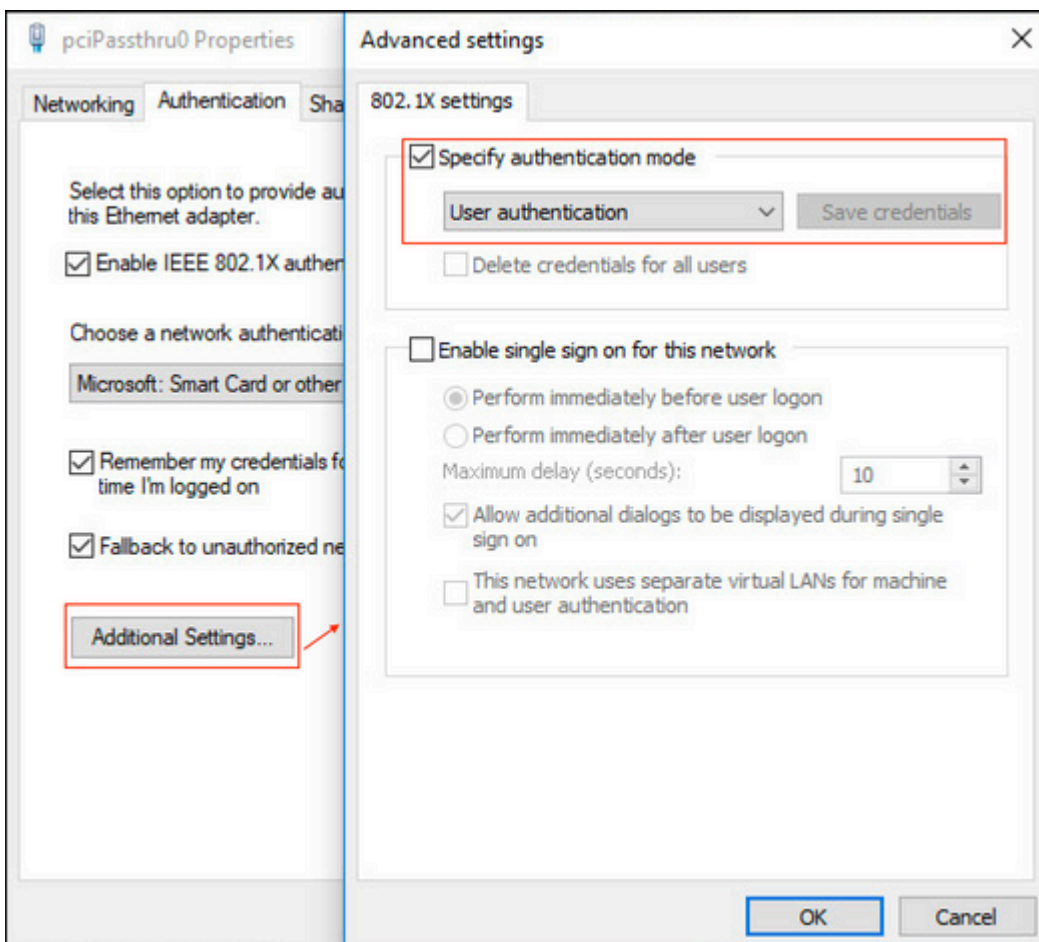
1. Stellen Sie sicher, dass der PC mit dem Benutzerzertifikat (für Benutzer1) ausgestattet ist und für die Clientauthentifizierung und in den vertrauenswürdigen Stammzertifizierungsstellen vorgesehen ist, dass die Zertifikatskette des Ausstellers auf dem PC vorhanden ist.



2. Aktivieren Sie die Dot1x-Authentifizierung und die Select-Authentifizierungsmethode als Microsoft:Smart Card- oder anderes Zertifikat für die EAP-TLS-Authentifizierung.



3. Klicken Sie auf Zusätzliche Einstellungen, und ein Fenster wird geöffnet. Aktivieren Sie das Kontrollkästchen mit dem Angeben des Authentifizierungsmodus, und wählen Sie die Benutzerauthentifizierung aus, wie in diesem Bild gezeigt.



## Konfigurieren des Richtliniensatzes auf der ISE

Da das EAP-TLS-Protokoll verwendet wird, muss vor der Konfiguration des Richtliniensatzes das Zertifikatauthentifizierungsprofil konfiguriert werden, und die Identitätsquellensequenz wird später in der Authentifizierungsrichtlinie verwendet.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > External Identity Sources > Identity Source Sequences > Settings. The left sidebar shows a tree view of External Identity Sources, with 'Certificate Authentication Profile' selected. The main content area is titled 'Certificate Authentication Profile List > LDAPS\_cert' and 'Certificate Authentication Profile'. The configuration fields are as follows:

- Name: LDAPS\_cert
- Description: EAP-TLS certificate based authentication with LDAPS
- Identity Store: testlab\_idaps
- 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:  Always perform binary comparison

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

Verwenden Sie das Zertifikatauthentifizierungsprofil in der Identitätsquellensequenz, und definieren Sie die externe LDAPS-Identitätsquelle in der Authentifizierungssuchliste:

**Identity Services Engine** Home > Context Visibility > Operations > Policy > Administration > Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

### Identity Source Sequence

**Identity Source Sequence**

\* Name

Description

**Certificate Based Authentication**

Select Certificate Authentication Profile

**Authentication Search List**

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

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

**Advanced Search List Settings**

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Save Reset

Konfigurieren Sie jetzt den Richtlinienatz für die kabelgebundene Dot1x-Authentifizierung:

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
	Wired Dot1x		Wired_802.1X

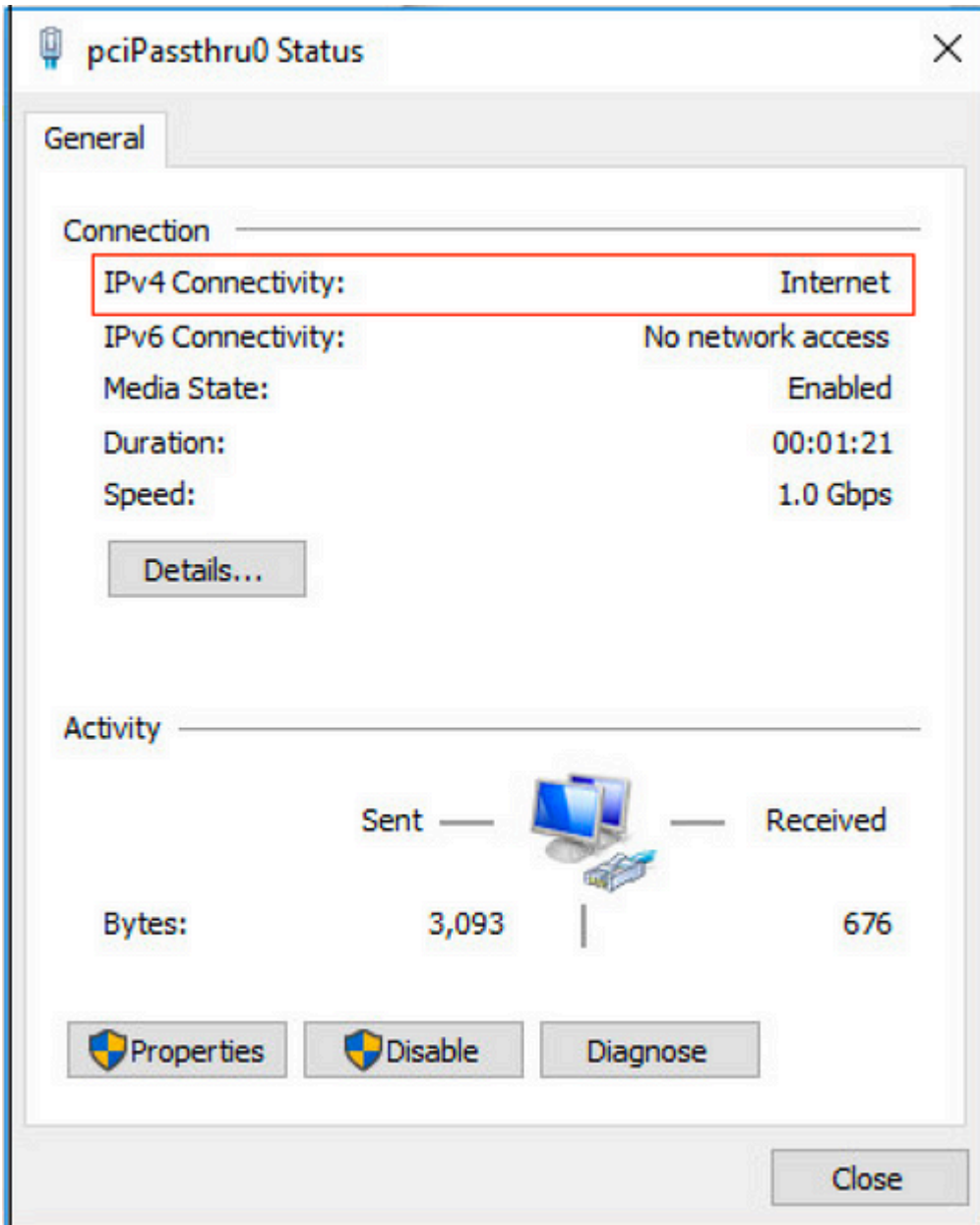
Authentication Policy (2)

+ Status	Rule Name	Conditions
	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch
	Default	

Authorization Policy (2)

+ Status	Rule Name	Conditions	Results	Profiles
	Users in LDAP Store	testlab_ldaps-ExternalGroups EQUALS CN=UserGroup,OU=iSE OU,DC=testlab,DC=com	PermiAccess	
	Default		DenyAccess	

Nach dieser Konfiguration können wir den Endpunkt mithilfe des EAP-TLS-Protokolls anhand der LDAPS-Identitätsquelle authentifizieren.



## Überprüfung

1. Überprüfen Sie die Authentifizierungssitzung am mit dem PC verbundenen Switch-Port:



```
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. Um die LDAPS- und ISE-Konfigurationen zu verifizieren, können Sie die Subjekte und Gruppen mit einer Testverbindung zum Server abrufen:

LDAP Identity Sources List > testlab\_ldaps

### LDAP Identity Source

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

Access  Anonymous Access  Authenticated Access

Admin DN \* CN=poongarg,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

Fallover  Always Access Primary Server First

Save Reset

Ldap bind succeeded to dc1.testlab.com:636

Number of Subjects 3

Number of Groups 2

Response time 73ms

OK

3. Überprüfen Sie den Benutzerauthentifizierungsbericht:

Refresh Reset Repeat Counts Export To

Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...
Jun 24, 2020 04:45:21.727 AM	<span style="color: blue;">i</span>		user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess
Jun 24, 2020 04:45:20.671 AM	<span style="color: green;">✓</span>		user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess

4. Überprüfen Sie den detaillierten Authentifizierungsbericht für den Endpunkt:

## Overview

Event 5200 Authentication succeeded

Username user1

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

Endpoint Profile Unknown

Authentication Policy Wired Dot1x >> Dot1x

Authorization Policy Wired Dot1x >> Users in LDAP Store

Authorization Result PermitAccess

## Authentication Details

Source Timestamp 2020-06-24 04:40:52.124

Received Timestamp 2020-06-24 04:40:52.124

Policy Server ISE26-1

Event 5200 Authentication succeeded

Username user1

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

Calling Station Id B4-96-91-26-DE-C0

Endpoint Profile Unknown

IPv4 Address 10.106.38.165

Authentication Identity Store testlab\_idaps

Identity Group Unknown

Audit Session Id 0A6A26390000130C98CE6088

Authentication Method dot1x

Authentication Protocol EAP-TLS

Service Type Framed

Network Device LAB-Switch

15041 Evaluating Identity Policy  
15048 Queried PIP - Network Access.NetworkDeviceName  
22072 Selected identity source sequence - LDAPS  
22070 Identity name is taken from certificate attribute  
15013 Selected Identity Source - testlab\_ldaps  
24031 Sending request to primary LDAP server - testlab\_ldaps  
24016 Looking up user in LDAP Server - testlab\_ldaps  
24023 User's groups are retrieved - testlab\_ldaps  
24004 User search finished successfully - testlab\_ldaps  
22054 Binary comparison of certificates succeeded  
22037 Authentication Passed  
12506 EAP-TLS authentication succeeded

15036 Evaluating Authorization Policy  
24209 Looking up Endpoint in Internal Endpoints IDStore - user1  
24211 Found Endpoint in Internal Endpoints IDStore  
15048 Queried PIP - testlab\_ldaps.ExternalGroups  
15016 Selected Authorization Profile - PermitAccess  
22081 Max sessions policy passed  
22080 New accounting session created in Session cache  
11503 Prepared EAP-Success  
11002 Returned RADIUS Access-Accept

5. Überprüfen Sie, ob die Daten zwischen dem ISE- und dem LDAPS-Server verschlüsselt sind, indem Sie die Paketerfassung auf der ISE zum LDAPS-Server durchführen:

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 SA...
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 M...
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...
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 durin...
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
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 Spe...
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
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
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 L...

```

▶ 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

## Fehlerbehebung

In diesem Abschnitt werden einige häufige Fehler beschrieben, die bei dieser Konfiguration aufgetreten sind, und es wird beschrieben, wie diese Fehler behoben werden.

- Im Authentifizierungsbericht wird folgende Fehlermeldung angezeigt:

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

Diese Fehlermeldung zeigt an, dass die ausgewählte Methode nicht von LDAP unterstützt wird. Stellen Sie sicher, dass im Authentifizierungsprotokoll desselben Berichts eine der unterstützten Methoden (EAP-GTC, EAP-TLS oder PEAP-TLS) angezeigt wird.

- Die Testbindung an den Server wurde mit einem Fehler beendet.

In der Regel ist dies auf den Fehler bei der Validierung des LDAPS-Serverzertifikats zurückzuführen. Um solche Probleme zu beheben, sollten Sie eine Paketerfassung auf der ISE durchführen und alle drei Komponenten der Laufzeit und des Prt-jni auf Debugebene aktivieren, das Problem neu erstellen und die Datei prrt-server.log überprüfen.

Bei der Paketerfassung wird ein ungültiges Zertifikat gemeldet, und der Port-Server zeigt Folgendes an:

**Hinweis:** Der Hostname auf der LDAP-Seite muss mit dem Antragstellernamen des Zertifikats (oder einem anderen Antragstellernamen) konfiguriert werden. Wenn Sie diese also nicht im Betreff oder SAN haben, funktioniert sie nicht. Das Zertifikat mit der IP-Adresse in der SAN-Liste wird benötigt.

---

3. Im Authentifizierungsbericht konnten Sie feststellen, dass der Betreff nicht im Identitätsspeicher gefunden wurde. Das bedeutet, dass der Benutzername aus dem Bericht nicht mit dem Subject Name Attribute (Betreffattribut) für einen Benutzer in der LDAP-Datenbank übereinstimmt. In diesem Szenario wurde der Wert für dieses Attribut auf sAMAccountName festgelegt, d. h., die ISE sucht beim Versuch, eine Übereinstimmung zu finden, nach den sAMAccountName-Werten für den LDAP-Benutzer.

4. Die Subjekte und Gruppen konnten während einer Bindung an den Servertest nicht korrekt abgerufen werden. Die wahrscheinlichste Ursache für dieses Problem ist eine falsche Konfiguration für die Suchbasis. Denken Sie daran, dass die LDAP-Hierarchie von Leaf-to-Root und DC angegeben werden muss (kann aus mehreren Wörtern bestehen).

## Zugehörige Informationen

- <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>

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.