# 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.

<b>R</b>	Certificate
General De	tails Certification Path
Show: <a< td=""><td>l&gt; v</td></a<>	l> v
Field	Value ^
Issuer	testlab-DC1-CA-1, testlab, com
🔄 Valid fro	m Friday, October 11, 2019 2:03:01 AM
🔄 Valid to	Saturday, October 10, 2020 2:03:01 AM
Subject	DC1.testlab.com
Public ke	ey RSA (2048 Bits)
Certifica	DomainController
Enhance	e Client Authentication (1.3.6.1.5.5.7.3.2), Server Auth
<	III >
Other Name DS Object	e: ct Guid=04 10 a6 36 1d 3c f4 3f a8 47 83 d7 d3 d5 46 20 a3 3f
DNS Name =	DC1.testlab.com

### 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.

1	Scope Pane	¥ X	Name A	Value	Туре		
I	Softerra LDAP Browser	~	Conternet Public Servers	Not Expanded	Group		
	Internet Public Servers		estab	ldaps://dc1.testlab.com:636/DC=testlab,DC=com	Server Profile		
I	8- 🗍 testab					1	

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.

Scope Pane 👻 🗙	Name 🔺	Value	Type
Softerra LDAP Browser	CN	UserGroup	Entry
😟 📲 Internet Public Servers	CN	user2	Entry
i⊒- 🗐 testlab	CN	user1	Entry
😥 – 📴 CN=Builtin	CN	DESKTOP-19	Entry
CN=Computers	CN	ComputerGroup	Entry
OU=Domain Controllers	distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribut
CN=ForeignSecurityPrincipals	dSCorePropagationData	1/1/1601	Attribut
E- CN=Infrastructure	dSCorePropagationData	6/20/2020 2:51:11 AM	Attribut
OU=ISE Group	🗉 gPLink	[LDAP://cn={21A53B13-6971-45E8-8545-FD0C68E29790},c	Attribut
	instanceType	[Writable]	Attribut
	🗉 name	ISE OU	Attribut
CN=DESKTOP-19	objectCategory	CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=	Attribut
CN=user1	objectClass	organizationalUnit	Attribut
CN=UserCroup	objectClass	top	Attribut
	Ξou	ISE OU	Attribut
E-CN=LostAndFound	uSNChanged	607428	Attribut
H- CN=Managed Service Accounts	uSNCreated	603085	Attribut
E-CN=NTDS Quotas	whenChanged	6/21/2020 2:44:06 AM	Attribut
😟 🛅 CN=Program Data	whenCreated	6/20/2020 2:51:11 AM	Attribut
CN=System	objectGUID	{44F45D1D-17B7-48DF-ABC6-3ED27FA4F694}	Binary A

# Integration der ISE mit dem LDAPS-Server

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

•	dudu lde	entity Services	Engine	Home	Contex	t Visibility	Operations	Policy	→ Administr	ation	Work Centers			
ĺ		Identity Mar	nagement +	Networ	k Resources	Device i	Portal Manageme	ent pxGrid	Services F	ed Servi	ice + Threat Cent	ric NAC		
	Deployme	nt Licensing	- Certificates	+ Lo	ogging → M	aintenance	Upgrade +	Backup & R	estore + Admir	Access	<ul> <li>Settings</li> </ul>			
	- Certificat	e Management	0		Friendly Name DC1	9		•	Status	Truste	d For	Serial Number	Issued To	Issued B
	System (	Certificates			DC1-CA				Enabled	Infrast Cisco Endpo	ructure Services sints	18 29 1C A7 00 13	testlab-DC1-CA-1	testlab-D
L	Trusted (	renncates												

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.

dialo cisco	Identity Service	es Engine	Home	Context Visibility	<ul> <li>Operation</li> </ul>	ns + Policy	+ Administration	Work Centers		
► Sys	tem 👻 Identity N	lanagement	Network R	esources + Device	Portal Manage	ment pxGrid Ser	vices + Feed Se	rvice + Threat Centr	ic NAC	
Ider	ntities Groups	External Ider	ntity Sources	Identity Source Sequ	uences + Se	ttings				
Ex 🖑	ternal Identity S Certificate Auth Active Directory testlab LDAP testlab_Idapt ODBC RADIUS Token RSA SecurID	ources entication Profil	@ <b>.</b>	LDAP Identity So LDAP Identit General	vrces List > tes y Source Conne Name [ Description [ ↓ Schema [	ttiab_Idaps ection Dir testlab_Idaps Custom	ectory Organization	Groups	Attributes	Advanced Settings
	SAML Id Provid	iers		Subject I     Group N     Subject I     Group N     Group Group	Name Attribute lame Attribute tt Objects Conta Objects Contai	sAMAccountName dn ain Reference To Gr n Reference To Sub	oups	* Group Map Attribute Certificate Attribute	memberOf userCertificate	
				User Info	Attributes (j)	Subjects In	Groups Are Stored I	In Member Attribute As	Distinguished Name	Ť
					First Name	givenName		Department	department	
					Last Name	sn		Organizational Unit	company	
					Job Title	title		Locality	1	
					Email	mail		State or Province	st	
					Telephone	telephoneNumber	·	Country	C0	
				:	Street Address	streetAddress				
				Save Rese	:					

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 👻	K Filter Name	user 1	
Softerra LDAP Browser	Name	Value	Type
	≡ cn ≡ displayName ≡ distinguishedName	user 1 user 1 CN=user 1,OU=ISE OU,DC=testlab,DC=com	Attribute Attribute Attribute
B − CN=ForeignSecurityPrincipals CN=Infrastructure OU=ISE Group	givenName     same     sAMAccountName	user1 user1 user1	Attribute Attribute Attribute
CN=ComputerGroup	<ul> <li>userPrincipalName</li> <li>userCertificate</li> </ul>	user 1@testlab.com user 1	Attribute 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 👻	r X	Name	Value	Туре
Softerra LDAP Browser		🗉 cn	UserGroup	Attrib
🖻 🗐 testlab	_	distinguishedName	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attrib
😟 - 🛅 CN=Builtin	- 1	dSCorePropagationData	1/1/1601	Attrib
E- CN=Computers		groupType	[GlobalScope, Security]	Attrib
OU=Domain Controllers		instanceType	[ Writable ]	Attrib
CN=ForeignSecurityPrincipals		member	CN=user1,OU=ISE OU,DC=testlab,DC=com	Attrib
E CN=Infrastructure		member	CN=user2,OU=ISE OU,DC=testlab,DC=com	Attrib
OU=ISE Group		🗉 name	UserGroup	Attrib
OU=ISE OU		objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attrib
E-CN=ComputerGroup		objectClass	group	Attrib
CN=DESKTOP-19		objectClass	top	Attrib
CN=User1		sAMAccountName	UserGroup	Attrib
CN=UserGroup		sAMAccountType	< samGroupObject >	Attrib

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

ON=ComputerGroup     ObjectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
H- ON=DESKTOP-19	{39967F90-89BE-44B5-9CC5-B28C0B0EB234}	Binary Attribute
H- ObjectClass	top	Attribute
CN=user2     ObjectClass	group	Attribute
CN=LiserGroup     E objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab	,DC=com Attribute

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

Scope Pane 👻 🗙	Filter Name	UserGroup	
Softerra LDAP Browser	Name	Value 🔺	Туре
B- CN=Builtin		CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute
CN=Computers			
OU=Domain Controllers			
CN=ForeignSecurityPrincipals			
B- OU=ISE Group			
- DU=ISE OU			
CN=ComputerGroup			
CN=DESKTOP-19			
- CN=user1			

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.

L DOLL DE LOUIS DE LO			
⊟- OU=ISE OU	userPrincipalName	user1@testlab.com	Attribute
😟 – 📴 CN=ComputerGroup	userCertificate	user1	Binary Attribute
CN=DESKTOP-19 CN=user1			

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

LDAP Identity Source       General       Connection       Directory Organization       Groups       Attributes       Advanced Settings         Primary Server       Primary Server       Secondary Server       Enable Secondary Server         • Hostname/IP       dc1.testlab.com       I       Hostname/IP       389
General       Connection       Directory Organization       Groups       Attributes       Advanced Settings         Primary Server       Secondary Server <ul> <li>Enable Secondary Server</li> <li>Enable Secondary Server</li> <li>Mostname/IP</li> <li>dc1.testlab.com</li> <li>Port</li> <li>636</li> <li>Port</li> <li>389</li> </ul>
Primary Server       Secondary Server            Enable Secondary Server           Enable Secondary Server          * Hostname/IP       dc1.testlab.com       Hostname/IP         * Port       636       Port
* Hostname/IP       dc1.testlab.com       I       Hostname/IP       I       I         * Port       636       Port       389       I
*Hostname/IP dc1.testlab.com () Hostname/IP Hostname/IP () 389
* Hostname/IP     dc1.testlab.com     Hostname/IP       * Port     636     Port     389
* Port 636 Port 389
Specify server for each ISE node       Access       Anonymous Access       Access       Anonymous Access         Access       Authenticated Access       Authenticated Access       Authenticated Access         Admin DN       * CN=poongarg,CN=Users,DC=test       Admin DN       Admin DN         Password       * •••••••       Password       Password
Secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication         Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication         Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication         Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication         Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication         Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication         Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication         Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication         Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication         Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication       Image: Constraint of the secure Authentication
LDAP Server Root CA DC1-CA T I LDAP Server Root CA DST Root CA X3 Certificate A
Issuer CA of ISE Certificates DC1-CA (optional)

* Server Timeout	10	().Seconds	Server Timeout	10	@Secon
* Max. Admin Connections	20		Max. Admin Connections	20	Ð
	Force reconnect every	(1) Minutes		Force reconnect every	<li>④ Minute</li>
	Test Bind to Server			Test Bind to Server	
Failover	Always Access Primary Server I     Failback To Primary Server After	First	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.

LDAP Identity Sources Lis	t > <b>testlab_idap</b>	5			
LDAP Identity Source	ce				
General	Connection	Directory Organization	Groups	Attributes	Advanced Settin
* Subject Search Base	OU=ISE OU,D	C=testlab,DC=com Naming C	contexts i		
* Group Search Base	OU=ISE OU,D	C=testlab,DC=com Naming C	Contexts i		
	-				
Search for MAC Addres	ss in Format 🔀	-xx-xx-xx-xx *			
Strip start of su	bject name up to	the last occurrence of the separate	or \		
Strip end of sub	pject name from th	ne first occurrence of the separator	r		
	LDAP Identity Sources Lis LDAP Identity Sources General * Subject Search Base * Group Search Base Search for MAC Addres Strip start of sub Strip end of sub	LDAP Identity Sources List > testlab_Idapt         General       Connection         * Subject Search Base       OU=ISE OU,D         * Group Search Base       OU=ISE OU,D         Search for MAC Address in Format       xx         Strip start of subject name up to       Strip end of subject name from the	LDAP Identity Sources         General       Connection       Directory Organization         * Subject Search Base       OU=ISE OU,DC=testlab,DC=com       Naming O         * Group Search Base       OU=ISE OU,DC=testlab,DC=com       Naming O         Search for MAC Address in Format       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	LDAP Identity Sources List > testlab_Idaps         General       Connection       Directory Organization       Groups         * Subject Search Base       OU=ISE OU,DC=testlab,DC=com       Naming Contexts i         * Group Search Base       OU=ISE OU,DC=testlab,DC=com       Naming Contexts i         Search for MAC Address in Format       Image: Ima	LDAP Identity Sources List > testlab_Idaps         LDAP Identity Source         General       Connection       Directory Organization       Groups       Attributes         * Subject Search Base       OU=ISE OU,DC=testlab,DC=com       Naming Contexts i       i         * Group Search Base       OU=ISE OU,DC=testlab,DC=com       Naming Contexts i       i         Search for MAC Address in Format       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. 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.

LDAP Identity Source	es List > <b>testlab_ldap</b> e ource	•		
General	Connection	Directory Organization	Groups	Attributes
/ Edit 🕂 Add 🗸	🗙 Delete Group			
Name				•
CN=UserGrou	up,OU=ISE OU,DC=te	estlab,DC=com		

#### 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 xxxxx
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.

		×
Networking	Authentication Sharing	
Select t this Eth Choose Micros	his option to provide authenticated network access for emet adapter. le IEEE 802.1X authentication e a network authentication method: oft: Smart Card or other certificate sember my credentials for this connection each I'm logged on	c
Falls	eack to unauthorized network access	
Addit	ional Settings	

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.

pciPassthru0 Properties	Advanced settings	×
Networking Authentication Sha	802.1X settings	
Select this option to provide au this Ethernet adapter.	Specify authentication mode User authentication Save credentials	
Enable IEEE 802.1X auther	Delete credentials for all users	
Choose a network authenticati	Enable single sign on for this network	
Microsoft: Smart Card or other	Perform immediately before user logon	
	O Perform immediately after user logon	
Remember my credentials for time I'm logged on	Maximum delay (seconds):	
Fallback to unauthorized ne	Allow additional dialogs to be displayed during single sign on	
Additional Settings	☐ This network uses separate virtual LANs for machine and user authentication	
	OK Cance	

### 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.

cisco	Identity Servic	es Engine	Home	Context Visibility	<ul> <li>Operations</li> </ul>	+ Policy	+ Administr	ration	Work Centers
+ Sys	tem 👻 Identity M	Management	Network R	esources + Device P	Portal Management	pxGrid Ser	vices + Fe	eed Servi	ce
► Ide	ntities Groups	External Ider	ntity Sources	Identity Source Seque	nces + Settings				
Ex ¢	ternal Identity S	iources	<u>ي</u> .	Certificate Authent Certificate Aut	ication Profiles List >	LDAPS_cer file	i i		
	Active Director	y			* Name	LDAPS_0	ert		
•	LDAP ODBC				Description	EAP-TLS	certificate bas	sed authe	intication with <u>LDAPS</u>
,	RADIUS Token RSA SecuriD SAML Id Provid Social Login	ders			Identity Store	testlab_ld	aps		<b>.</b>
					Use Identity From	<ul> <li>Certific</li> </ul>	ate Attribute	Subjec	tt - Common Name 🝸 🛞
						<ul> <li>Any St</li> </ul>	ubject or Alter	mative Na	ame Attributes in the Certificate (for Active Directory Only) $\;$ (
				Match Clie Certificate	nt Certificate Agains In Identity Store ()	New	r.		
						<ul> <li>Only</li> </ul>	to resolve id	entity aml	biguity
						<ul> <li>Alway</li> </ul>	ys perform b	inary com	aparison
				Save Reset	)				

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

cisco	Identity Services E	Engine	Home	Context	Visibility	<ul> <li>Operations</li> </ul>	▶ Policy	- Administration	Work Centers
<ul> <li>Sys</li> </ul>	tem 👻 Identity Mana	agement	Network Re	esources	Device F	Portal Management	pxGrid Se	rvices + Feed Se	rvice
Ider	ntities Groups Ex	ternal Identi	ty Sources	Identity Se	ource Seque	ences + Settings			
Ident	ity Source Seque	nce							
- Id	entity Source Sequ	uence							
	* Name LDAPS								
Des	scription								
								le	
								1115	
<b>+</b> (	Certificate Based A	uthenticat	tion						
	Select Certification	te Authentic	ation Profile	LDAPS_ce	ert	ť			
-	uthentication Sea	rch List							
	A set of		recenthet will	ha accesso	d in convers	ee until first authorit	ination success	ada	
	A Set 0	ridentity sou	rces triat will	De accesse	su in sequer	ice unui irsi autreni	ication succe	1005	
4	Available				Selected				
	Internal Endpoints			>	testlab_	Idaps			
	Guest Users			<					
	All_AD_Join_Points								
	100			≫					
				«				×	
- 1	Advanced Search Li	ist Setting	s						
If a	selected identity store	cannot be ac	cessed for au	uthenticatio	n				
C	Do not access other	stores in the	sequence an	nd set the "/	Authenticatio	onStatus" attribute to	ProcessEr	ror"	
•	Treat as if the user w	as not found	and proceed	to the nex	t store in the	e sequence			
Save	Reset								

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

altalta cisco	Identity Ser	rvices Engine Home	Context Visibil	ty Operations		Administration	Work Conters
Policy	Sets Prof	filing Posture Client Provisio	ning + Policy	Elements			
Policy	y Sets →	Wired Dot1x					
	Status	Policy Set Name	Description	1	Conditio	ns	
Searc	sh						
	Ø	Wired Dot1x				Wired_802.1X	
✔ Au	uthentication	n Policy (2)					
G	Cintur	Dute Name	Candline	-			
	Status	Rule Name	Condition	15			
Sea	arch						
	0	Dot1x	₽ N	etwork Access-Network	DeviceNam	e EQUALS LAB-Switch	1
	Ø	Default					
► Auti	horization P	olicy (2)					

Results

Profiles

× PermitAccess

× DenyAccess

÷

+

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

testlab\_Idaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com

+

Search

Status Rule Name

Default

Users in LDAP Store

 $\odot$ 

 $\odot$ 

Conditions

忠

	atus	
neral		
onnection		
IPv4 Connectiv	ity:	Internet
IPv6 Connectiv	ity:	No network access
Media State:		Enabled
Duration:		00:01:21
Speed:		1.0 Gbps
ctivity ———	Sent	Received
tivity ———	Sent —	Received
:tivity Bytes:	Sent — 3,093	Received
tivity Bytes:	Sent — 3,093	Received 676 Diagnose

# Überprüfung

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

SW1#sh auth sessions in	t 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:	ØA6A26390000130798C66612
Acct Session ID:	0x00001224
Handle:	0x6800002E
Current Policy:	POLICY_Gi2/0/47
Local Policies:	
Service Templat	e: DEFAULT LINKSEC POLICY SHOULD SECURE (priority 150)
Jerree renpede	e. permoel_eximple_reace_breene (preside; xbo)
Server Policies:	
Method status list:	
Method	State
dotlx	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 > testiab_ide	sps				
LDAP Identity Source					
General Connection	Directory Organization Gro	ups Attributes Advar	ced Settings		
Access	Anonymous Accord		Access	Anonymous Access	
Admin DN	Authenticated A Ldap bind su     Number of S     Number of C	ucceeded to dc1.testlab.com:636 Subjects 3 Sroups 2	Admin DNI	Authenticated Access	
Admin UN	CN=poongarg,C Response tir	me 73ms	Admin DN		
Password		ОК	Password		
Secure Authentication	C Enable Secure Authentication		Secure Authentication	Enable Secure Authentication	
	Enable Server Identity Check			Enable Server Identity Check	
LDAP Server Root CA	DC1-CA	٤.	LDAP Server Root CA	DST Root CA X3 Certificate # *	Ð
Issuer CA of ISE Certificates	DC1-CA *	Ð	Issuer CA of ISE Certificates	Select if required (optional)	۲
* Server Timeout	10	7 Seconds	Server Timeout	10	(7 Seco
* May Admin Connections	20	] @	Max Admin Connections	20	
Max. Admin Connections		] @	wax. Admin Connections	20	w.
	Force reconnect every	(j) Minutes		Force reconnect every	(i) Minut
	Test Bind to Server			Test Bind to Server	
Failover	Always Access Primary Server	First			

### 3. Überprüfen Sie den Benutzerauthentifizierungsbericht:

2	Refresh O Reset Repeat Coun	its 💄 Expor	t To 🕶					
	Time	Status	Details	Identity	Endpoint ID	Authentication Po	Authorization Policy	Authorization Profi
×		•		Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles
	Jun 24, 2020 04:45:21.727 AM	•	0	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	2	0	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:

Event	5200 Authentication succeeded
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 10.106.38.165					
IPv4 Address						
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_Idaps
24031	Sending request to primary LDAP server - testlab_Idaps
24016	Looking up user in LDAP Server - testlab_Idaps
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_Idaps.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:

N	lo.	Time		Source	Destination	Protocol	Length	Address	64bits	Info
1	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 S
	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] Seg=0 Ack=1 Win=8192 Len=0
T	22	2828-86-24	10:40:24.206613	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 - 636 [ACK] Seg=1 Ack=1 Win=29312 Len=0 TSva
	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 duri
	25	2828-86-24	10:40:24.210508	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 - 636 [ACK] Seg=142 Ack=1971 Win=33152 Len=8
	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 Sp
J	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
t	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
1	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	2828-86-24	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 captur
	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] Seg=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	2828-86-24	10:40:24.253658	10,197,164,21	18, 197, 164, 22	TLSv1.2	295	00:50:56:a0:3e:7f.0_		Application Data
	35	2828-86-24	10:40:24,293322	18,197,164,22	10,197,164,21	TCP	66	00:0c:29:98:ca:28.0.		28057 -+ 636 [ACK] Seg=879 Ack=4221 Win=39688 Len=8
	86	2828-86-24	18:48:57.946553	18, 197, 164, 22	10.197.164.21	TI Sv1.2	151	88:8c:29:98:ca:28.8		Application Data
÷	87	2828-85-24	18:48:57.947688	10,197,164,22	18, 197, 164, 21	TCP	66	88:8c:29:98:ca:28.8	_	28857 + 636 [FIN, ACK] Sec=964 Ack=4221 Win=39688
3	Frame 2 Etherne	28: 199 bytes et II, Src: V	s on wire (1592 bi Vmware_a0:3e:7f (0	ts), 199 bytes captur 0:50:56:a0:3e:7f), Ds	ed (1592 bits) t: Vmware_98:ca:28	(00:0c:29:	98:ca:28	)		
.)	<ul> <li>Internet</li> </ul>	et Protocol V	Version 4, Src: 10	.197.164.22, Dst: 10.	197.164.21					
1	v Transmi	ission Contro	ol Protocol, Src P	ort: 28057, Dst Port:	636, Seq: 336, Ac	:k: 2078, Le	n: 133			
	Sou	rce Port: 28	857							
	Dest	tination Por	t: 636							
	[St	ream index: 2	2]							
	[TCI	P Segment Ler	n: 133]							
	Seq	uence number	: 336 (relative	sequence number)						
	[Ne:	xt sequence i	number: 469 (re	lative sequence number	er)]					
	Ack	nowledgment i	number: 2078 (r	elative ack number)						
	100	0 = Head	der Length: 32 byt	es (8)						
	▶ Flag	gs: 0x018 (P	SH, ACK)							
	Wind	dow size val	ue: 259							
	[Ca	lculated wind	dow size: 33152]							
	EWin	ndow size sca	aling factor: 128]							
	Che	cksum: 0x5e6	1 [unverified]							
	[Che	ecksum Statu:	s: Unverified)							
	Urg	ent pointer:	0							
	▶ Opt	ions: (12 by	tes), No-Operation	(NOP), No-Operation	(NOP), Timestamps					
	▶ [SEI	Q/ACK analys:	is]							
	▶ [Tip	mestamps]								
	TCP	payload (13)	3 bytes)							
4	Secure	Sockets Lave	er							
	TLS:	v1.2 Record I	Laver: Application	Data Protocol: Idao						
	100 1000	Content Type	: Application Data	(23)						
		Version: TLS	1.2 (0x0303)					Encruptor	1 Da	ta
		Length: 128						- Encrypter	Da	la
		Encrypted An	plication Data: 17	3d1b0b2f280a13cc1781	5e54447bb9ac8af8a8	81a9eb84				
ł										

## 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 Prrt-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

- <u>https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/119149-configure-ise-00.html#anc9</u>
- <u>https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214975-configure-eap-tls-authentication-with-is.html</u>

#### 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.