

Configurazione e risoluzione dei problemi di ISE con l'archivio identità LDAPS esterno

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configura LDAPS in Active Directory](#)

[Installa certificato di identità nel controller di dominio](#)

[Struttura della directory di Access LDAPS](#)

[Integrazione di ISE con LDAPS Server](#)

[Configurazione dello switch](#)

[Configurazione dell'endpoint](#)

[Configura Policy Set su ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive l'integrazione di Cisco Identity Service Engine (ISE) con il server Secure Lightweight Directory Access Protocol (LDAPS) come origine identità esterna. LDAPS consente la crittografia dei dati LDAP (incluse le credenziali utente) in transito quando viene stabilita un'associazione alla directory. LDAPS utilizza la porta TCP 636.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dell'amministrazione ISE
- Conoscenze base di Active Directory/LDAP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE 2.6 Patch 7

- Microsoft Windows versione 2012 R2 con Active Directory Lightweight Directory Services installato
- PC con sistema operativo Windows 10 con supplicant nativo e certificato utente installato
- Cisco Switch C3750X con immagine 152-2.E6

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Con LDAPS sono supportati i seguenti protocolli di autenticazione:

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

Nota: EAP-MSCHAPV2 (come metodo interno di PEAP, EAP-FAST o EAP-TTLS), LEAP, CHAP e EAP-MD5 non sono supportati con l'origine identità esterna LDAPS.

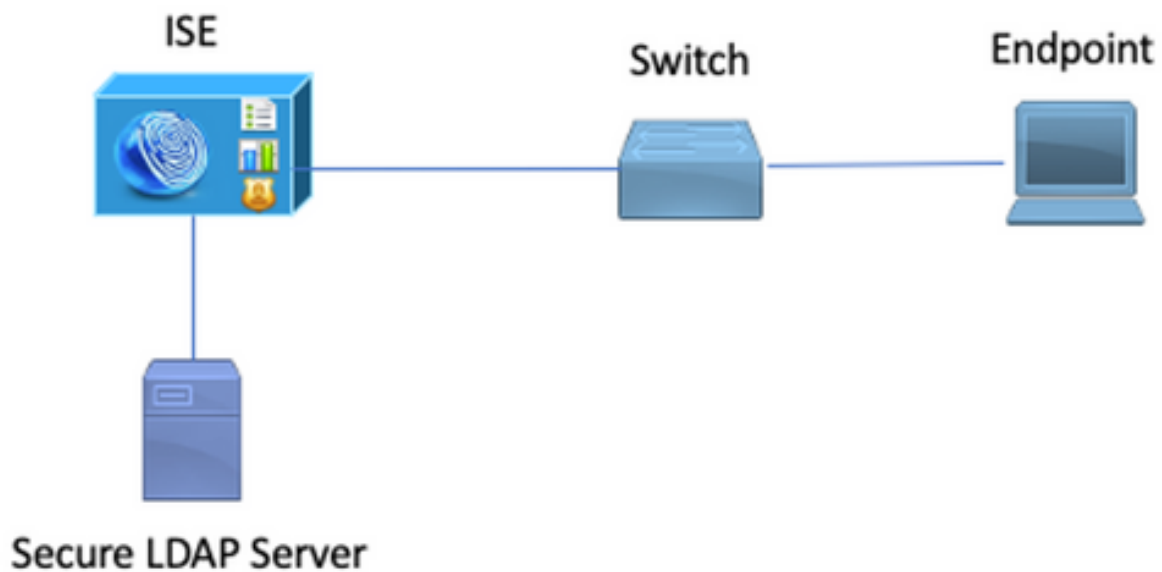
Configurazione

In questa sezione viene descritta la configurazione dei dispositivi di rete e l'integrazione dell'ISE con il server LDAPS Microsoft Active Directory (AD).

Esempio di rete

In questo esempio di configurazione, l'endpoint utilizza una connessione Ethernet con uno switch per connettersi alla LAN (Local Area Network). La porta dello switch connessa è configurata per l'autenticazione 802.1x al fine di autenticare gli utenti con ISE. Ad ISE, LDAPS è configurato come un negozio di identità esterno.

Nell'immagine è illustrata la topologia di rete utilizzata:

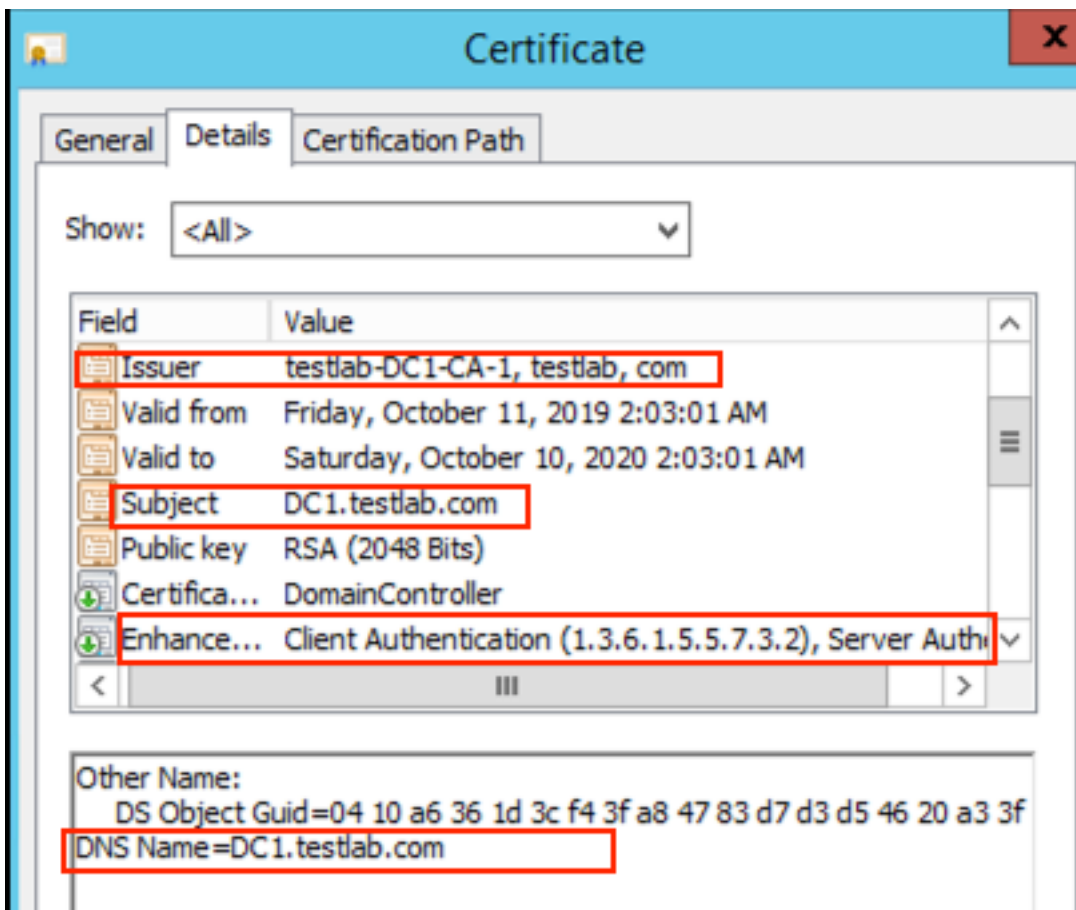


Configura LDAPS in Active Directory

Installa certificato di identità nel controller di dominio

Per abilitare LDAPS, installare un certificato nel controller di dominio che soddisfi i seguenti requisiti:

1. Il certificato LDAPS si trova nell'archivio dei certificati personali del controller di dominio.
2. Una chiave privata corrispondente al certificato è presente nell'archivio del controller di dominio ed è associata correttamente al certificato.
3. L'estensione Utilizzo chiavi avanzato include l'identificatore di oggetto Autenticazione server (1.3.6.1.5.5.7.3.1) (noto anche come OID).
4. Il nome di dominio completo (FQDN) del controller di dominio (ad esempio, DC1.testlab.com) deve essere presente in uno dei seguenti attributi: Il **nome comune (CN)** nel campo Oggetto e la voce DNS nell'estensione del **nome alternativo soggetto**.
5. Il certificato deve essere rilasciato da un'Autorità di certificazione (CA) considerata attendibile dal controller di dominio e dai client LDAPS. Per una comunicazione protetta attendibile, il client e il server devono considerare attendibili la CA radice e i certificati della CA intermedia che hanno rilasciato i certificati.
6. Per generare la chiave è necessario utilizzare il provider del servizio di crittografia (CSP) Schannel.



Struttura della directory di Access LDAPS

Per accedere alla directory LDAPS sul server Active Directory, utilizzare un browser LDAP. In questo laboratorio viene utilizzato Softerra LDAP Browser 4.5.

1. Stabilire una connessione al dominio sulla porta TCP 636.



2. Per semplicità, creare un'unità organizzativa (OU) denominata **ISE OU** in Active Directory e dovrebbe avere un gruppo denominato **UserGroup**. Creare due utenti (**user1** e **user2**) e renderli membri del gruppo **UserGroup**.

Nota: LDAP Identity Source su ISE è utilizzato solo per l'autenticazione dell'utente.

Scope Pane	Name	Value	Type
Softerra LDAP Browser	OU=ISE OU		
Internet Public Servers	OU=ISE Group		
testlab	CN=ComputerGroup		
	CN=DESKTOP-19		
	CN=user1		
	CN=user2		
	CN=UserGroup		
	OU=LABISE		
	CN=LostAndFound		
	CN=Managed Service Accounts		
	CN=NTDS Quotas		
	CN=Program Data		
	CN=System		
	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

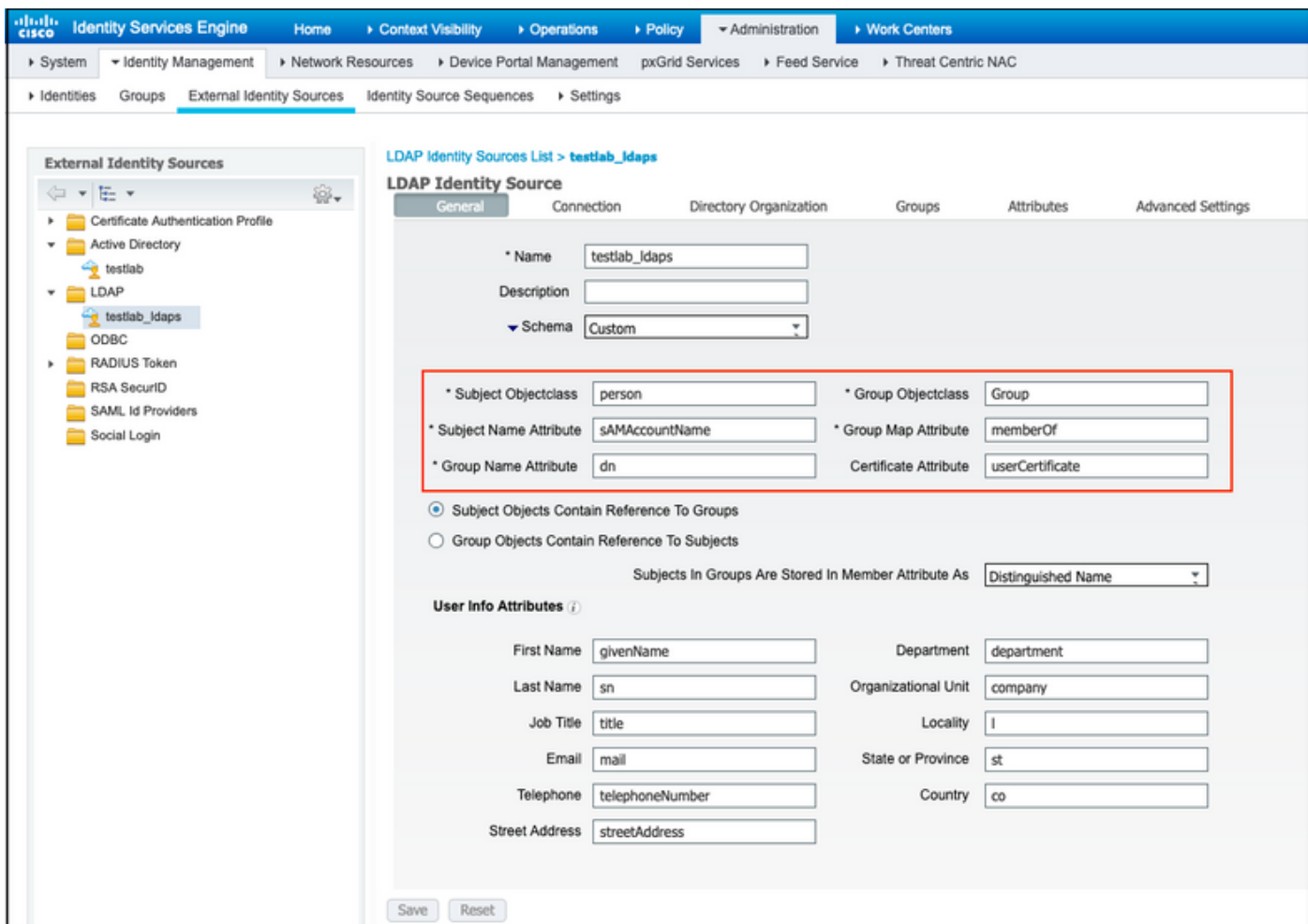
Integrazione di ISE con LDAPS Server

1. Importare il certificato CA radice del server LDAP nel certificato protetto.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
DC1					
<input type="checkbox"/> DC1-CA	<input checked="" type="checkbox"/> Enabled	Infrastructure Cisco Services Endpoints	18 29 1C A7 00 13...	testlab-DC1-CA-1	testlab-DC1-CA-1

2. Convalidare il certificato di amministrazione ISE e verificare che il certificato dell'autorità emittente del certificato di amministrazione ISE sia presente anche nell'archivio certificati attendibile.

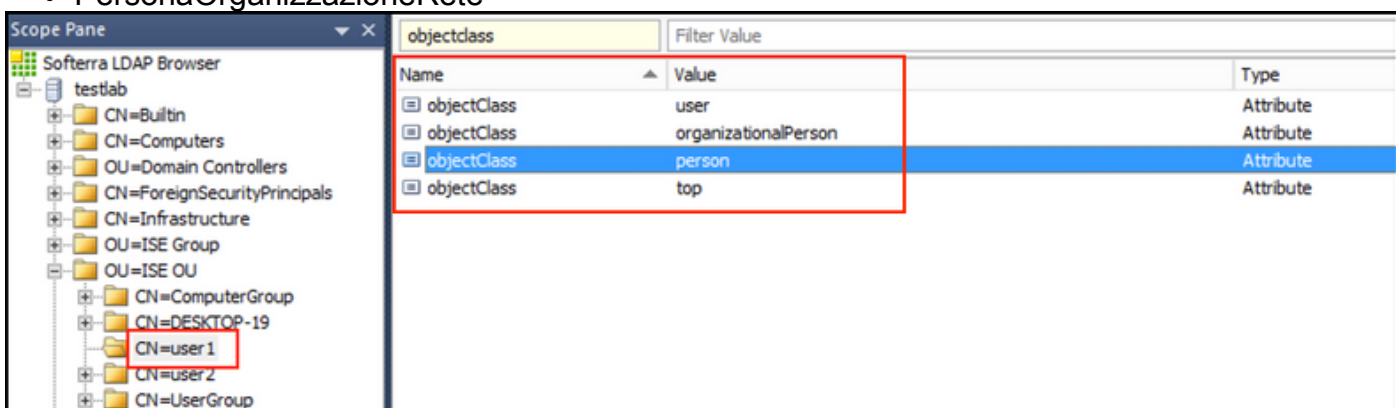
3. Per integrare il server LDAPS, utilizzare i diversi attributi LDAP della directory LDAPS. Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Origini identità LDAP > Aggiungi**.



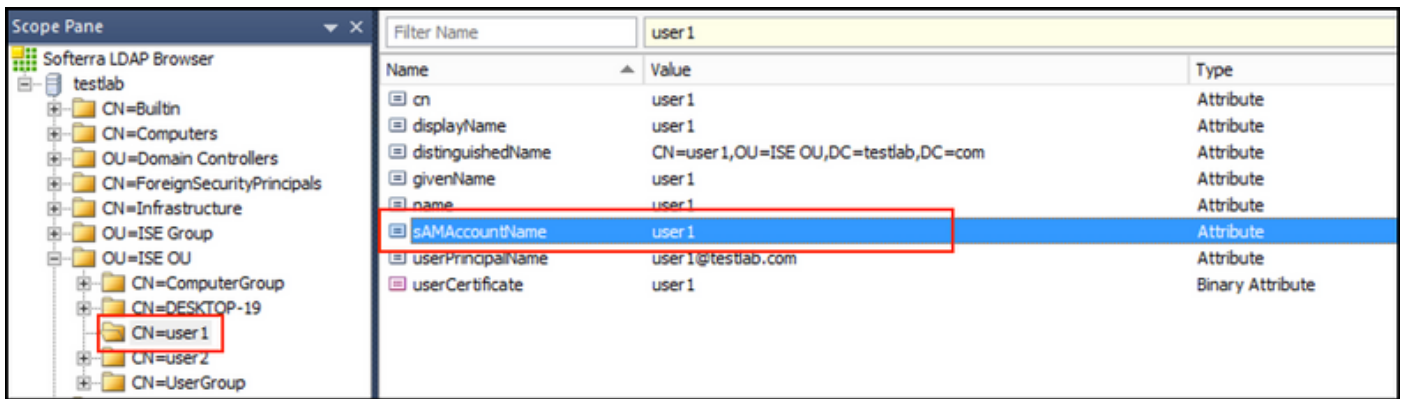
4. Configurare questi attributi dalla scheda Generale:

Oggetto Objectclass: Questo campo corrisponde alla classe Object degli account utente. È possibile utilizzare una delle quattro classi seguenti:

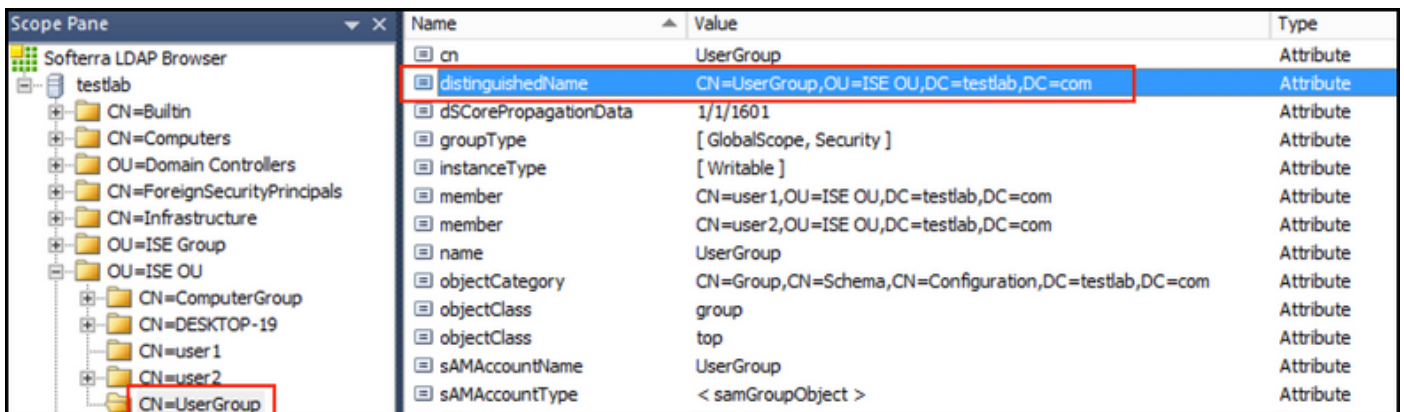
- In alto
- Persona
- PersonaOrganizzazione
- PersonaOrganizzazioneRete



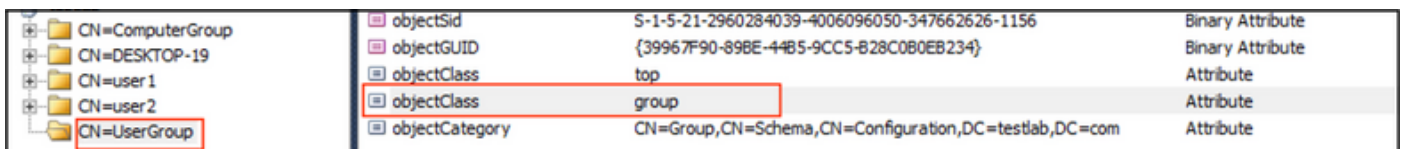
Attributo nome soggetto: questo campo è il nome dell'attributo contenente il nome utente della richiesta. Questo attributo viene recuperato da LDAPS quando ISE richiede un nome utente specifico nel database LDAP (è possibile utilizzare cn, sAMAccountName, ecc.). In questo scenario viene utilizzato il nome utente user1 sull'endpoint.



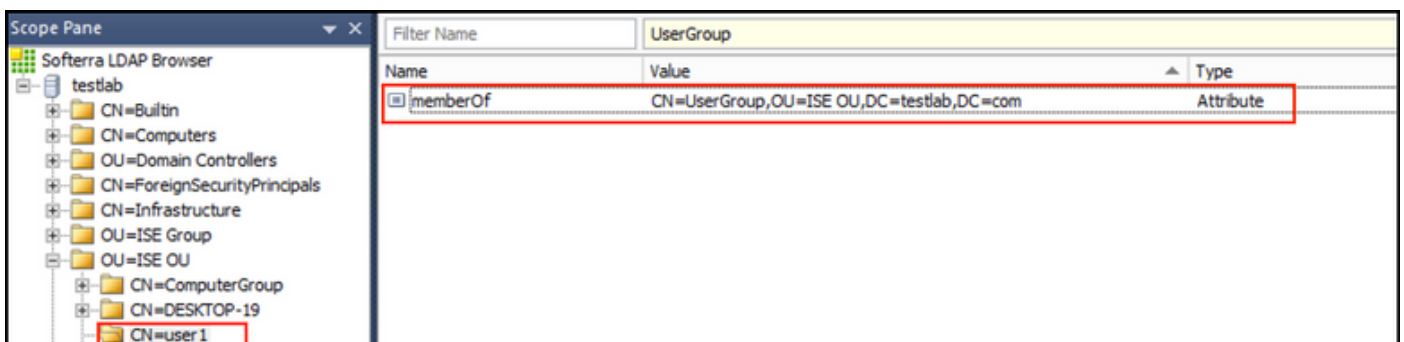
Attributo nome gruppo: Attributo che contiene il nome di un gruppo. I valori dell'**attributo Nome gruppo** nella directory LDAP devono corrispondere ai nomi dei gruppi LDAP nella pagina **Gruppi utenti**



Group Objectclass: questo valore viene utilizzato nelle ricerche per specificare gli oggetti riconosciuti come gruppi.



Attributo mappa gruppo: Questo attributo definisce la modalità di mapping degli utenti ai gruppi.



Attributo certificato: Immettere l'attributo che contiene le definizioni del certificato. Queste definizioni possono essere utilizzate facoltativamente per convalidare i certificati presentati dai client quando sono definiti come parte di un profilo di autenticazione dei certificati. In questi casi, viene eseguito un confronto binario tra il certificato client e il certificato recuperato dall'origine dell'identità LDAP.



OU=ISE OU	userPrincipalName	user1@testlab.com	Attribute
CN=ComputerGroup	userCertificate	user 1	Binary Attribute
CN=DESKTOP-19			
CN=user1			

5. Per configurare la connessione LDAPS, passare alla scheda **Connessione**:

LDAP Identity Sources List > testlab_ldaps

LDAP Identity Source

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

Primary Server	Secondary Server
<input type="checkbox"/> Enable Secondary Server	
* Hostname/IP: dc1.testlab.com	Hostname/IP:
* Port: 636	Port: 389
<input type="checkbox"/> Specify server for each ISE node	
Access: <input type="radio"/> Anonymous Access <input checked="" type="radio"/> Authenticated Access	Access: <input checked="" type="radio"/> Anonymous Access <input type="radio"/> Authenticated Access
Admin DN: CN=poongarg,CN=Users,DC=testlab	Admin DN:
Password: *****	Password:
Secure Authentication: <input checked="" type="checkbox"/> Enable Secure Authentication <input checked="" type="checkbox"/> Enable Server Identity Check	Secure Authentication: <input type="checkbox"/> Enable Secure Authentication <input type="checkbox"/> Enable Server Identity Check
LDAP Server Root CA: DC1-CA	LDAP Server Root CA: DST Root CA X3 Certificate Authority
Issuer CA of ISE Certificates: DC1-CA	Issuer CA of ISE Certificates: Select if required (optional)

* Server Timeout: 10 Seconds	Server Timeout: 10 Seconds
* Max. Admin Connections: 20	Max. Admin Connections: 20
<input type="checkbox"/> Force reconnect every: Minutes	<input type="checkbox"/> Force reconnect every: Minutes
<input type="button" value="Test Bind to Server"/>	<input type="button" value="Test Bind to Server"/>
Failover: <input type="radio"/> Always Access Primary Server First <input checked="" type="radio"/> Failback To Primary Server After: 5 Minutes	

6. Eseguire **dsquery** sul controller di dominio per ottenere il DN del nome utente da utilizzare per effettuare una connessione al server LDAP:

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

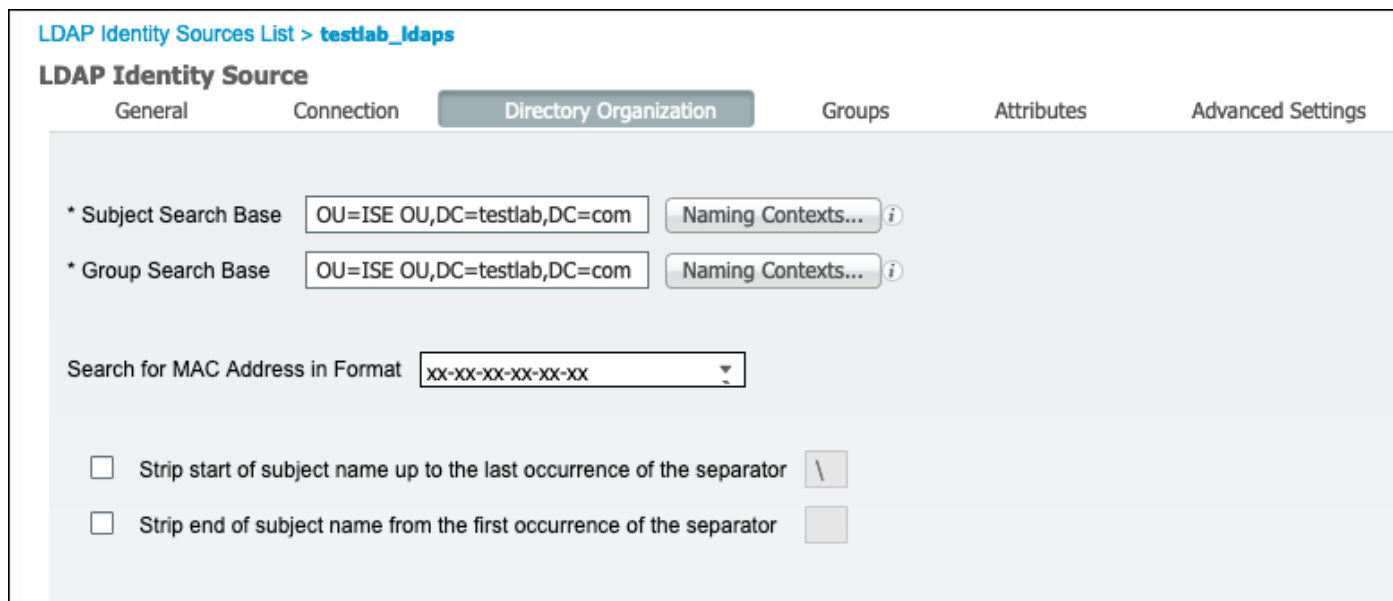
Passaggio 1. Impostare l'indirizzo IP o il nome host corretto del server LDAP, definire la porta LDAPS (TCP 636) e il DN di amministrazione per stabilire una connessione con il server LDAP tramite SSL.

Passaggio 2. Abilitare l'opzione Autenticazione sicura e Controllo identità server.

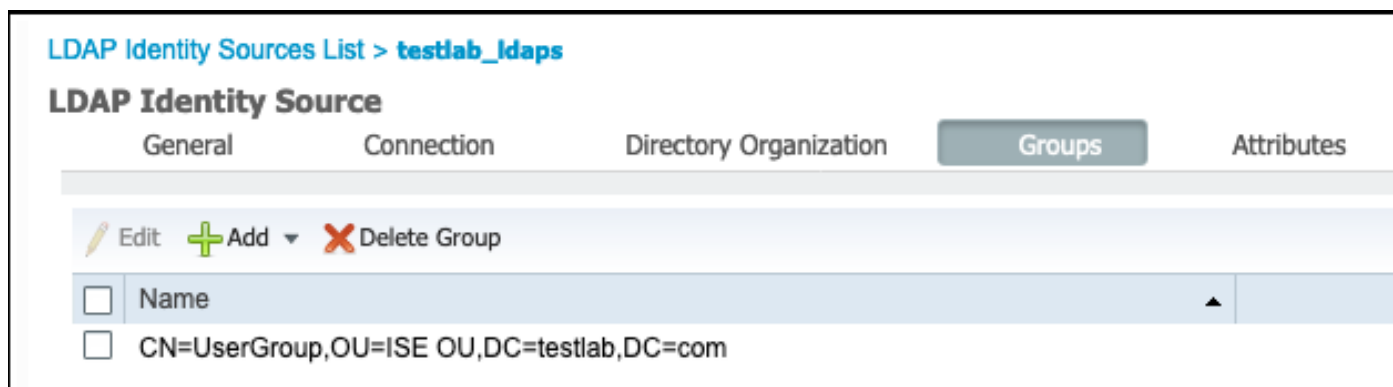
Passaggio 3. Dal menu a discesa, selezionare il certificato **CA radice del server LDAP** e il certificato **ISE admin CA emittente** (abbiamo utilizzato l'autorità di certificazione, installata sullo stesso server LDAP anche per rilasciare il certificato ISE admin),

Passaggio 4. Selezionare il **test di associazione al server**. A questo punto, gli argomenti o i gruppi non vengono recuperati perché le basi di ricerca non sono ancora configurate.

7. In **Organizzazione directory** scheda, configurare la Base di ricerca soggetto/gruppo. È il **punto di join** per ISE al LDAP. Ora è possibile recuperare solo gli oggetti e i gruppi figli del punto di giunzione. In questo scenario, l'oggetto e il gruppo vengono recuperati dall'**unità organizzativa OU=ISE**



8. In **Gruppi**, fare clic su **Aggiungi** per importare i gruppi dal server LDAP sull'ISE e recuperare i gruppi, come mostrato in questa immagine.



Configurazione dello switch

Configurare lo switch per l'autenticazione 802.1x. Il PC Windows è collegato a switchport Gig2/0/47

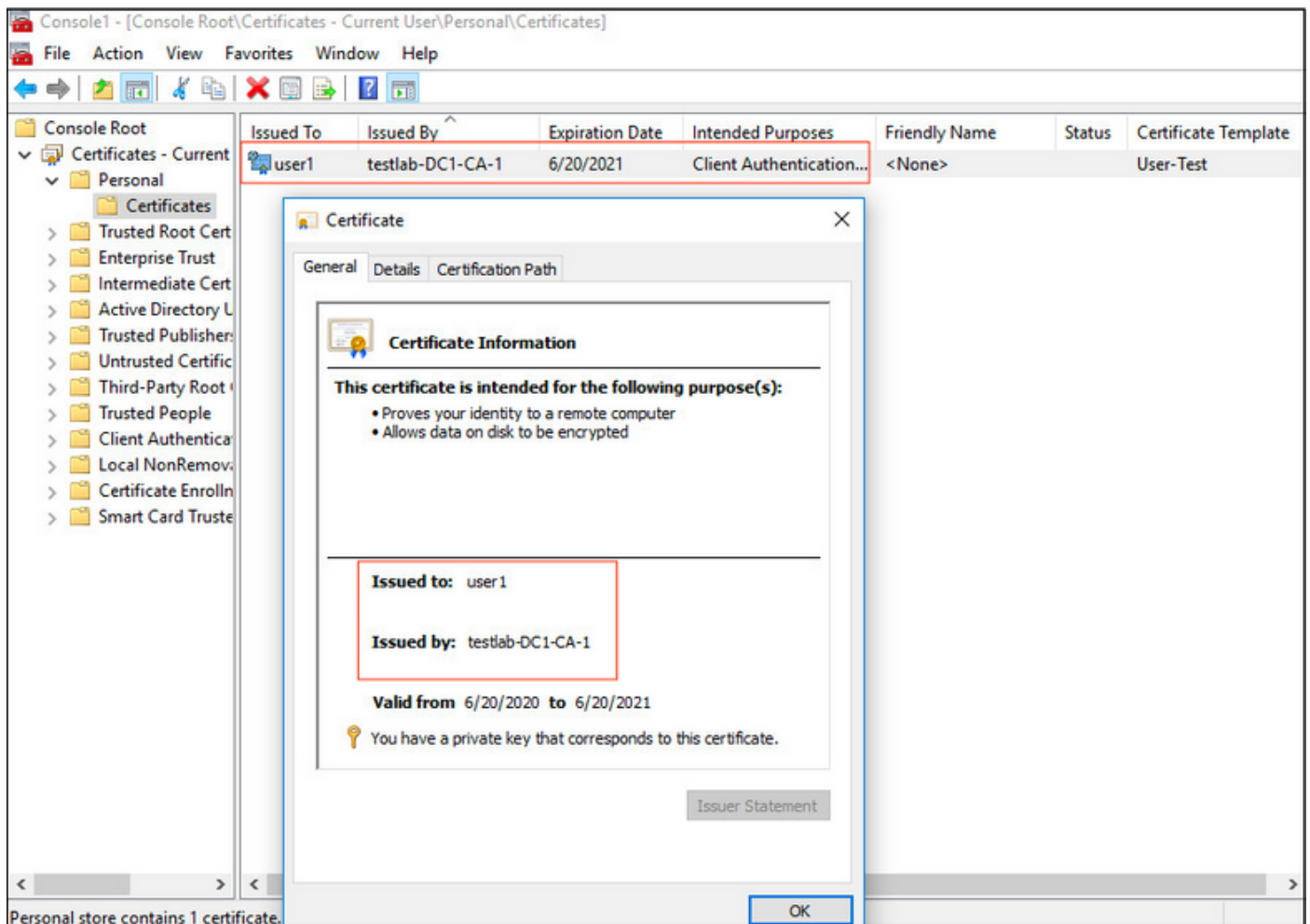
```
aaa new-model radius server ISE address ipv4 x.x.x.x auth-port 1812 acct-port 1813 key xxxxxx
aaa group server radius ISE_SERVERS server name ISE ! aaa server radius dynamic-author client
x.x.x.x server-key xxxxxx ! aaa authentication dot1x default group ISE_SERVERS local aaa
authorization network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

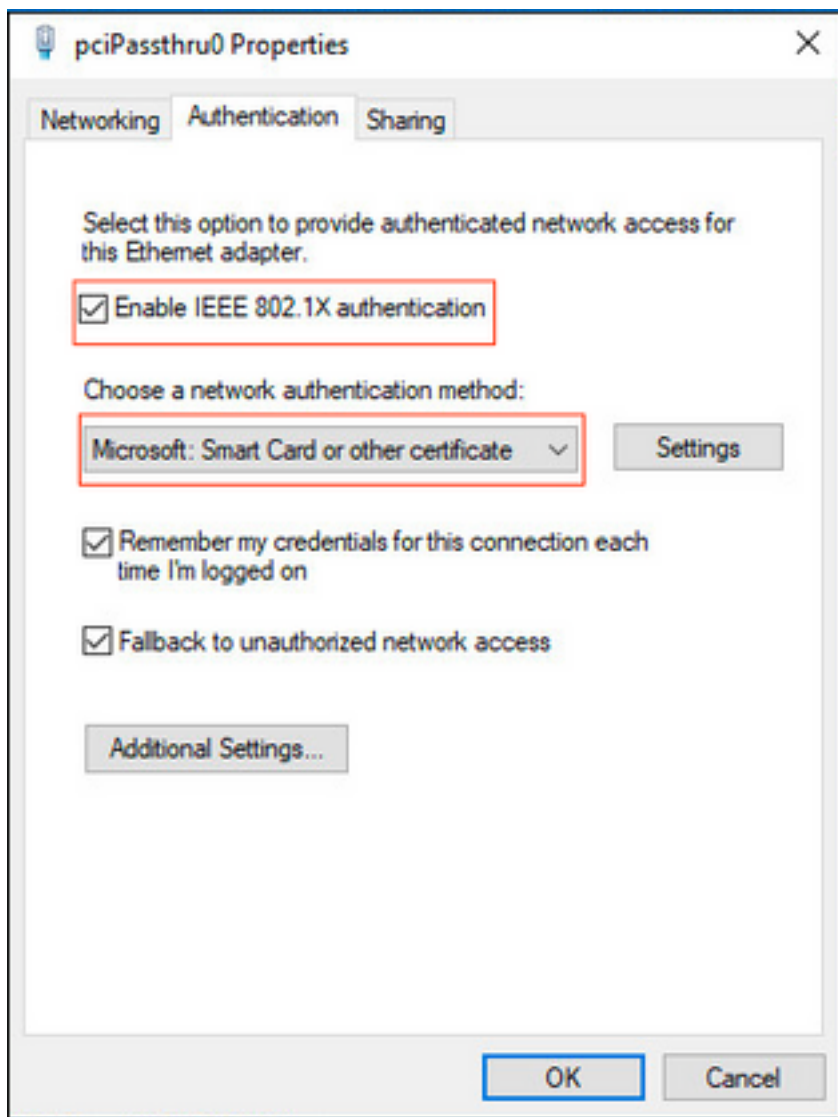
Configurazione dell'endpoint

Viene utilizzato Windows Native Supplicant e viene utilizzato uno dei protocolli EAP supportati da LDAP, EAP-TLS per l'autenticazione e l'autorizzazione degli utenti.

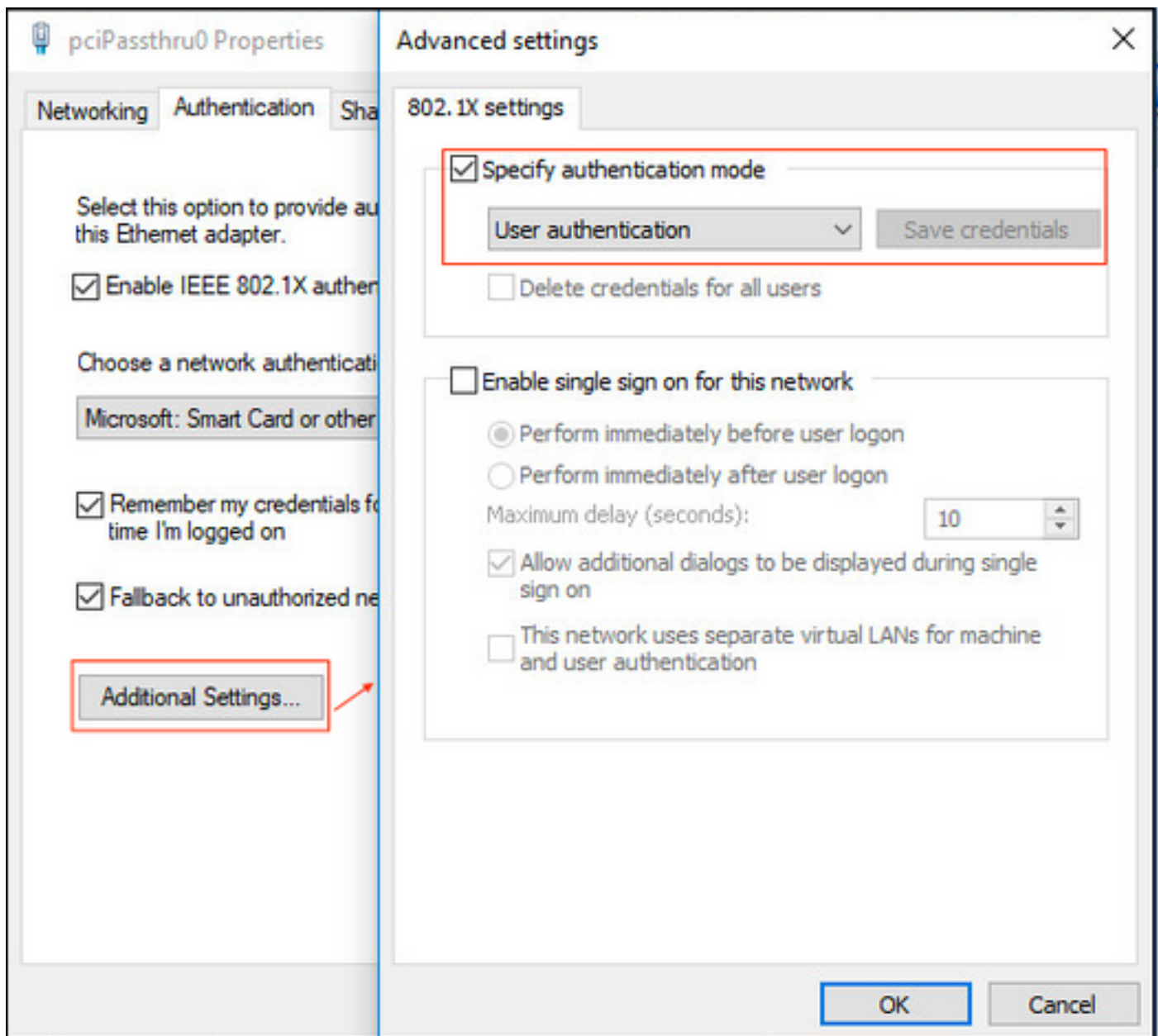
1. Verificare che il PC disponga del certificato utente (per l'utente 1) e abbia lo scopo designato come Autenticazione client e che la catena di certificati dell'autorità di certificazione principale attendibile sia presente nel PC.



2. Abilitare l'autenticazione Dot1x e selezionare il metodo di autenticazione come **Microsoft:Smart Card o altro certificato** per l'autenticazione EAP-TLS.



3. Fare clic su **Impostazioni aggiuntive**, si apre una finestra, selezionare la casella con **specificata modalità di autenticazione** e scegliere **Autenticazione utente**, come mostrato in questa immagine.



Configura Policy Set su ISE

Poiché viene utilizzato il protocollo EAP-TLS, prima della configurazione di Policy Set è necessario configurare [Certificate Authentication Profile](#) e utilizzare Identity Source Sequence nel criterio di autenticazione in un secondo momento.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows a tree view of 'External Identity Sources' with categories like Certificate Authentication Profile, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The main content area is titled 'Certificate Authentication Profiles 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_ldaps
- Use Identity From:** Certificate Attribute (Selected), Subject - Common Name
- Match Client Certificate Against Certificate in Identity Store:** Always perform binary comparison (Selected)

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

Fare riferimento al profilo di autenticazione del certificato nella sequenza Origine identità e definire l'origine identità esterna LDAPS nell'elenco di ricerca autenticazione:

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

Configurare ora il criterio impostato per l'autenticazione Dot1x per reti cablate:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Wired Dot1x Reset Policyset Hitcounts Reset Save

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

Authentication Policy (2)

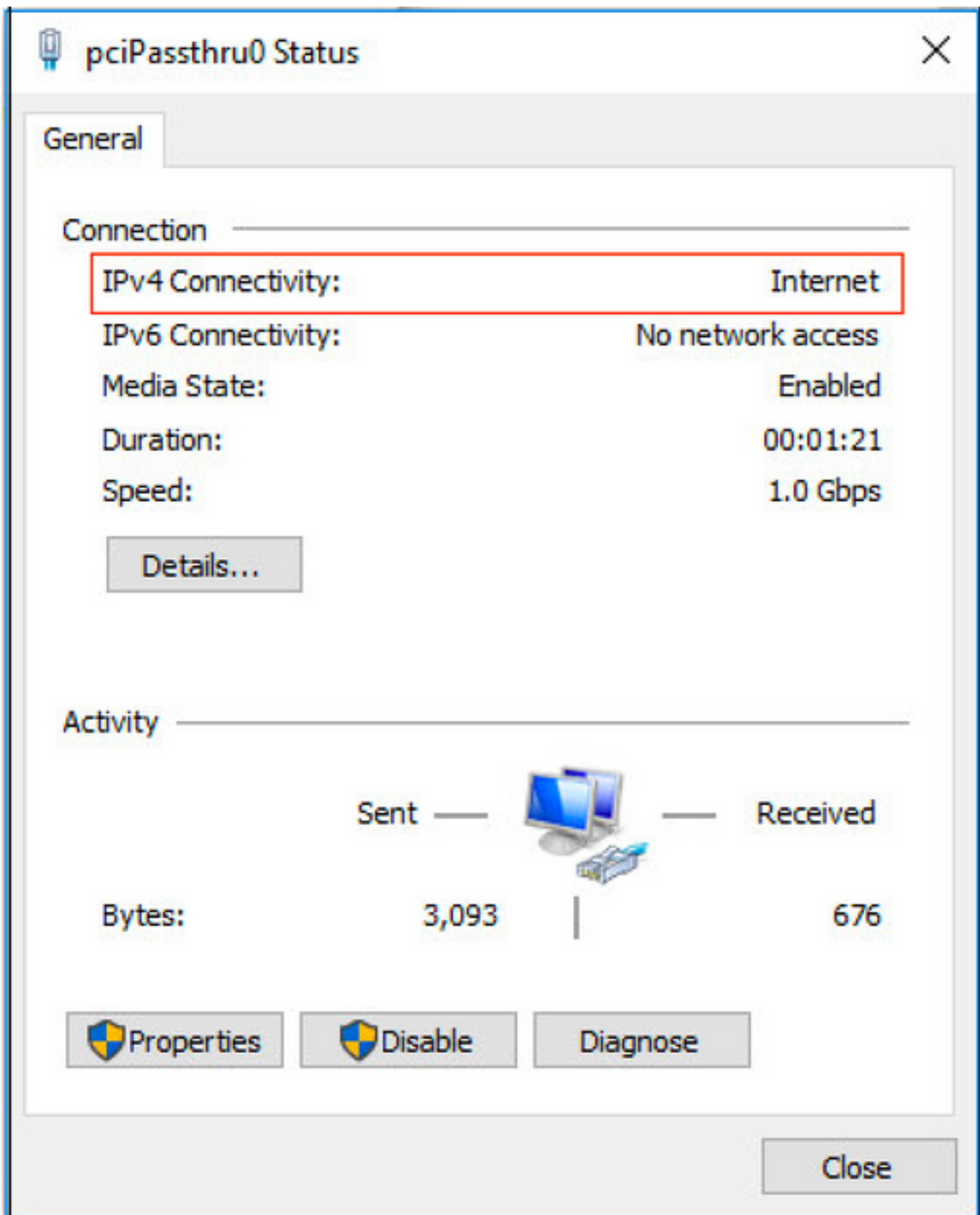
Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch	LDAPS x	223	⚙
✔	Default		LDAPS x	0	⏏ ⚙

Authorization Policy (2)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
Search							
+	✔	Users in LDAP Store	testlab_idaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	× PermitAccess +	Select from list +	207	⚙
+	✔	Default		× DenyAccess +	Select from list +	11	⚙

Reset Save

Dopo questa configurazione, l'endpoint deve essere autenticato tramite il protocollo EAP-TLS sull'origine dell'identità LDAPS.



Verifica

1. Controllare la sessione di autenticazione sulla porta dello switch collegata al PC:


```
SW1#sh auth sessions int g2/0/47 de
      Interface: GigabitEthernet2/0/47
      MAC Address: b496.9126.dec0
      IPv6 Address: Unknown
      IPv4 Address: 10.106.38.165
      User-Name: user1
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      Session timeout: N/A
      Restart timeout: N/A
      Periodic Acct timeout: N/A
      Session Uptime: 43s
      Common Session ID: 0A6A26390000130798C66612
      Acct Session ID: 0x00001224
      Handle: 0x6800002E
      Current Policy: POLICY_Gi2/0/47

Local Policies:
      Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list:
      Method          State
      dot1x           Authc Success
```

2. Per verificare le configurazioni LDAPS e ISE, è possibile recuperare gli oggetti e i gruppi con una connessione di prova al server:

LDAP Identity Sources List > testlab_idaps

LDAP Identity Source

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

Access Anonymous Access Authenticated Access

Admin DN * CN=poongarg,CN=...

Password *

Secure Authentication Enable Secure Authentication Enable Server Identity Check

LDAP Server Root CA DC1-CA

Issuer CA of ISE Certificates DC1-CA

* Server Timeout 10 Seconds

* Max. Admin Connections 20

Force reconnect every Minutes

Test Bind to Server

Failover 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. Verificare il report di autenticazione utente:

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. Verificare il report di autenticazione dettagliato per l'endpoint:

Overview

Event 5200 Authentication succeeded

Username user1

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

Endpoint Profile Unknown

Authentication Policy Wired Dot1x >> Dot1x

Authorization Policy Wired Dot1x >> Users in LDAP Store

Authorization Result PermitAccess

Authentication Details

Source Timestamp	2020-06-24 04:40:52.124
Received Timestamp	2020-06-24 04:40:52.124
Policy Server	ISE26-1
Event	5200 Authentication succeeded
Username	user1
Endpoint Id	B4:96:91:26:DE:C0
Calling Station Id	B4-96-91-26-DE-C0
Endpoint Profile	Unknown
IPv4 Address	10.106.38.165
Authentication Identity Store	testlab_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_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_idaps
24004 User search finished successfully - testlab_idaps
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. Verificare che i dati siano crittografati tra il server ISE e il server LDAPS effettuando l'acquisizione dei pacchetti sull'ISE verso il server LDAPS:

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...		28857 → 636 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=140972872 TSecr=0 WS=128
21	2020-06-24 10:40:24.206595	10.197.164.21	10.197.164.22	TCP	74	00:50:56:a0:3e:7f,0...		636 → 28857 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 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...		28857 → 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=140972873 TSecr=30158962
23	2020-06-24 10:40:24.206661	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...		28857 → 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 10:40:24.230324	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...		28857 → 636 [ACK] Seq=682 Ack=3992 Win=36864 Len=0 TSval=140972905 TSecr=30158965
33	2020-06-24 10:40:24.251944	10.197.164.21	10.197.164.22	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...		28857 → 636 [ACK] Seq=879 Ack=4221 Win=39680 Len=0 TSval=140972960 TSecr=30158967
86	2020-06-24 10:40:57.946553	10.197.164.21	10.197.164.22	TLSv1.2	151	00:0c:29:98:ca:28,0...		Application Data
87	2020-06-24 10:40:57.947608	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28857 → 636 [FIN, ACK] Seq=964 Ack=4221 Win=39680 Len=0 TSval=141086614 TSecr=30158967

```

▶ Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
▶ Ethernet II, Src: Vmware_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: 28857, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133
Source Port: 28857
OSI Model Layer: 6:36
[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)
1800 ... = 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 pointers: 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: 173d1b002f280a13cc17815e54447bb9ac8af8a881a9eb84...
  
```

Risoluzione dei problemi

In questa sezione vengono descritti alcuni errori comuni che si sono verificati con questa configurazione e viene spiegato come risolverli:

- Nel report di autenticazione potrebbe essere visualizzato il seguente messaggio di errore:

Authentication method is not supported by any applicable identity store

Questo messaggio di errore indica che il metodo selezionato non è supportato da LDAP.

Verificare che il **protocollo di autenticazione** nello stesso report mostri uno dei metodi supportati (EAP-GTC, EAP-TLS o PEAP-TLS).

- Test del binding al server terminato con un errore.

Nella maggior parte dei casi ciò è dovuto a un errore di controllo della convalida del certificato del server LDAPS. Per risolvere questi tipi di problemi, acquisire un pacchetto su ISE e abilitare tutti e tre i componenti runtime e port-jni a livello di debug, ricreare il problema e controllare il file **port-server.log**.

L'acquisizione pacchetti è in conflitto con un certificato non valido e il server di porta mostra:

```

04:10:20,197,ERROR,0x7f9c5b6f1700,LdapSslConnectionContext::checkCryptoResult(id = 1289): error message = SSL alert: code=0x22A=554 ; source=local ; type=fatal ; message="Server certificate identity verification failed: host IP didnt match SAN IP.s3_cInt.c:1290
  
```

Nota: Il nome host nella pagina LDAP deve essere configurato con il nome soggetto del certificato (o uno qualsiasi dei nomi soggetto alternativi). Pertanto, a meno che non sia presente nel soggetto o nella SAN, il certificato con l'indirizzo IP nell'elenco SAN non funziona.

3. Nel report di autenticazione è possibile notare che il soggetto non è stato trovato nell'archivio identità. Ciò significa che il nome utente del report non corrisponde all'**Attributo nome soggetto** per alcun utente nel database LDAP. In questo scenario, il valore è stato impostato su

sAMAccountName per questo attributo, il che significa che ISE cerca i valori sAMAccountName per l'utente LDAP quando tenta di trovare una corrispondenza.

4. I soggetti e i gruppi potrebbero non essere recuperati correttamente durante un test di **binding al server**. La causa più probabile è una configurazione errata delle basi di ricerca. Tenere presente che la gerarchia LDAP deve essere specificata dalla foglia alla radice e da dc (può essere costituita da più parole).

Informazioni correlate

- <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>