

Configuración y solución de problemas de ISE con almacenamiento de identidad LDAPS externo

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de LDAPS en Active Directory](#)

[Instalar certificado de identidad en controlador de dominio](#)

[Acceso a la estructura del directorio LDAPS](#)

[Integración de ISE con el servidor LDAP](#)

[Configuración del switch](#)

[Configuración del terminal](#)

[Configurar conjunto de políticas en ISE](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe la integración de Cisco ISE con el servidor Secure LDAP como fuente de identidad externa.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos sobre la administración de Identity Service Engine (ISE)
- Conocimientos básicos de Active Directory/protocolo ligero de acceso a directorios seguro (LDAPS)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Parche 7 de Cisco ISE 2.6
- Microsoft Windows versión 2012 R2 con Active Directory Lightweight Directory Services instalado
- PC con sistema operativo Windows 10 con suplicante nativo y certificado de usuario instalado
- Switch Cisco C3750X con imagen 152-2.E6


La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

LDAPS permite el cifrado de datos LDAP (que incluye credenciales de usuario) en tránsito cuando se establece un enlace de directorio. LDAPS utiliza el puerto TCP 636.

Estos protocolos de autenticación son compatibles con LDAPS:

- EAP-tarjeta de testigo genérica (EAP-GTC)
- Protocolo de autenticación de contraseña (PAP)
- EAP-seguridad de la capa de transporte (EAP-TLS)
- EAP protegido con seguridad de la capa de transporte (PEAP-TLS)

 Nota: EAP-MSCHAPV2 (como método interno de PEAP, EAP-FAST o EAP-TTLS), LEAP, CHAP y EAP-MD5 no son compatibles con la fuente de identidad externa LDAPS.

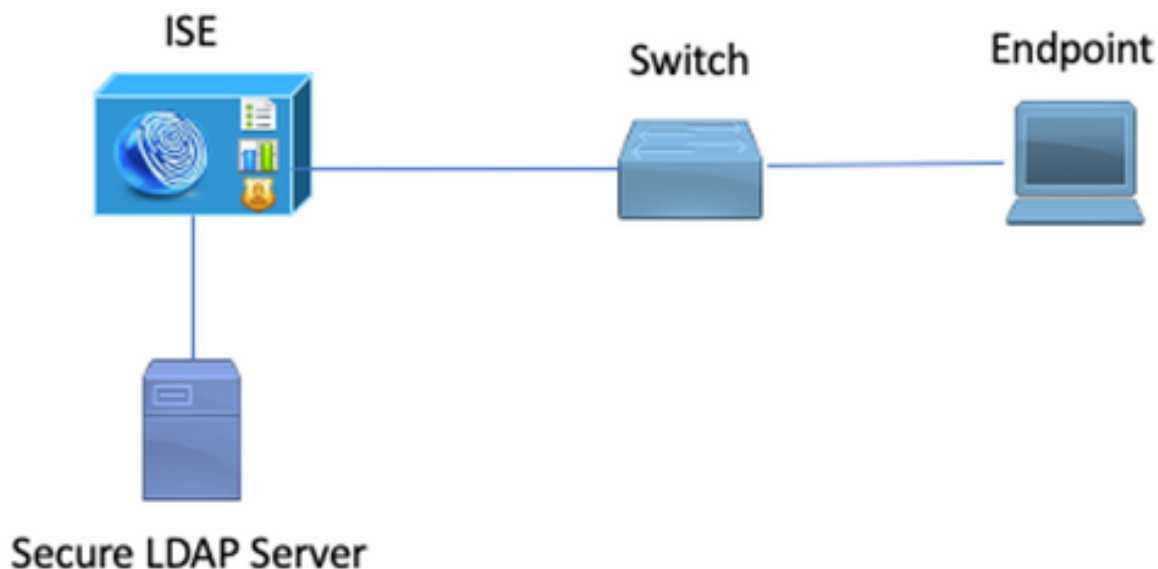
Configurar

Esta sección describe la configuración de los dispositivos de red y la integración de ISE con el servidor LDAP de Microsoft Active Directory (AD).

Diagrama de la red

En este ejemplo de configuración, el terminal utiliza una conexión Ethernet con un switch para conectarse con la red de área local (LAN). El puerto de switch conectado está configurado para la autenticación 802.1x con el fin de autenticar a los usuarios con ISE. En ISE, los LDAPS se configuran como un almacén de identidades externo.

Esta imagen ilustra la topología de red que se utiliza:



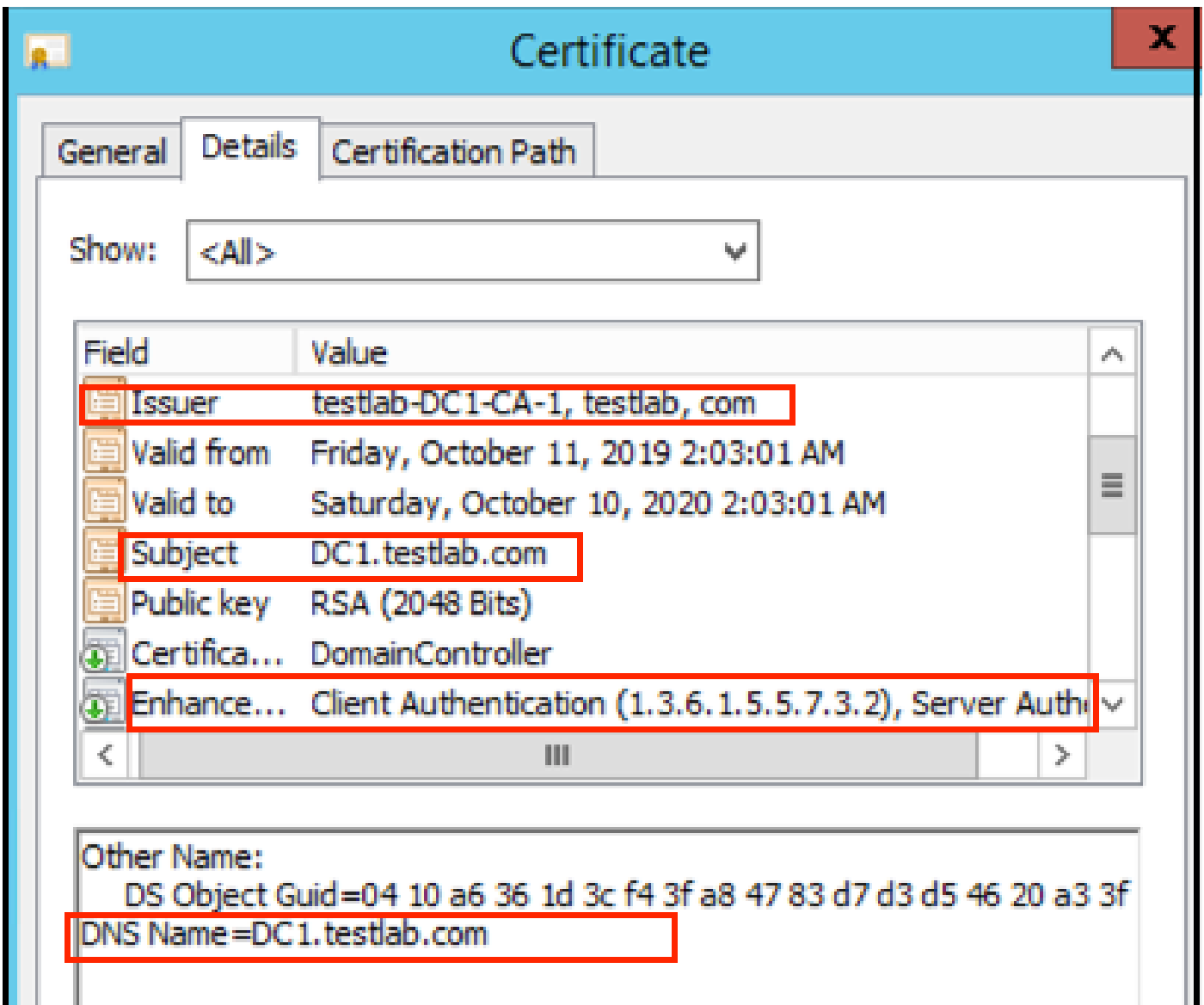
Configuración de LDAPS en Active Directory

Instalar certificado de identidad en controlador de dominio

Para habilitar LDAPS, instale un certificado en el controlador de dominio (DC) que cumpla estos requisitos:

1. El certificado LDAPS se encuentra en el almacén de certificados personales del controlador de dominio.
2. Hay una clave privada que coincide con el certificado en el almacén del controlador de dominio y está asociada correctamente al certificado.
3. La extensión Enhanced Key Usage (Uso mejorado de claves) incluye el identificador de objeto de autenticación de servidor (1.3.6.1.5.5.7.3.1) (también conocido como OID).
4. El nombre de dominio completo (FQDN) del controlador de dominio (por ejemplo, DC1.testlab.com) debe estar presente en uno de estos atributos: El nombre común (CN) en el campo Asunto e entrada DNS en la extensión de nombre alternativo del sujeto.
5. El certificado debe ser emitido por una autoridad certificadora (CA) en la que confíen el controlador de dominio y los clientes LDAPS. Para una comunicación segura de confianza, el cliente y el servidor deben confiar en la CA raíz de la otra entidad y en los certificados de CA intermedia que les han emitido certificados.

6. Se debe utilizar el proveedor de servicios criptográficos (CSP) de Schannel para generar la clave.



Acceso a la estructura del directorio LDAPS

Para acceder al directorio LDAP en el servidor de Active Directory, utilice cualquier explorador LDAP. En este LABORATORIO, se utiliza el Explorador LDAP 4.5 de Softerra.

1. Establezca una conexión con el dominio en el puerto TCP 636.



2. Para simplificar, cree una unidad organizativa (OU) denominada OU de ISE en AD y debe tener un grupo denominado UserGroup. Cree dos usuarios (user1 y user2) y conviértalos en miembros del grupo UserGroup.

 Nota: El origen de identidad LDAP en ISE solo se utiliza para la autenticación de usuarios.

Name	Value	Type
OU=ISE OU		Entry
OU=LABISE		Entry
CN=ComputerGroup		Entry
CN=DESKTOP-19		Entry
CN=user1		Entry
CN=user2		Entry
CN=UserGroup		Entry
CN=LABISE		Entry
CN=LostAndFound		Entry
CN=Managed Service Accounts		Entry
CN=NTDS Quotas		Entry
CN=Program Data		Entry
CN=System		Entry
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

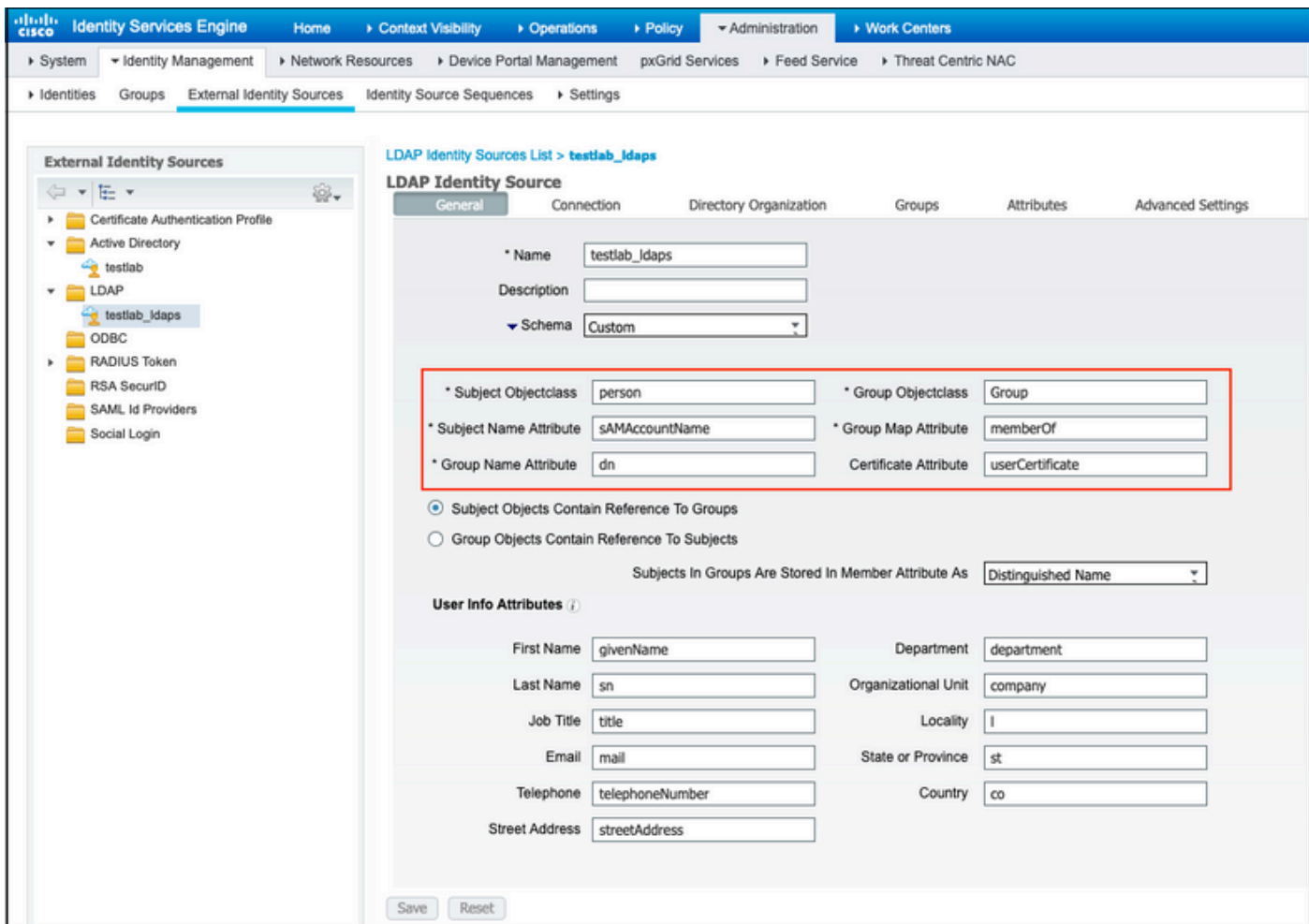
Integración de ISE con el servidor LDAP

1. Importe el certificado de CA raíz del servidor LDAP en el certificado de confianza.

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

2. Valide el certificado de administrador de ISE y asegúrese de que el certificado de emisor del certificado de administrador de ISE también esté presente en el almacén de certificados de confianza.

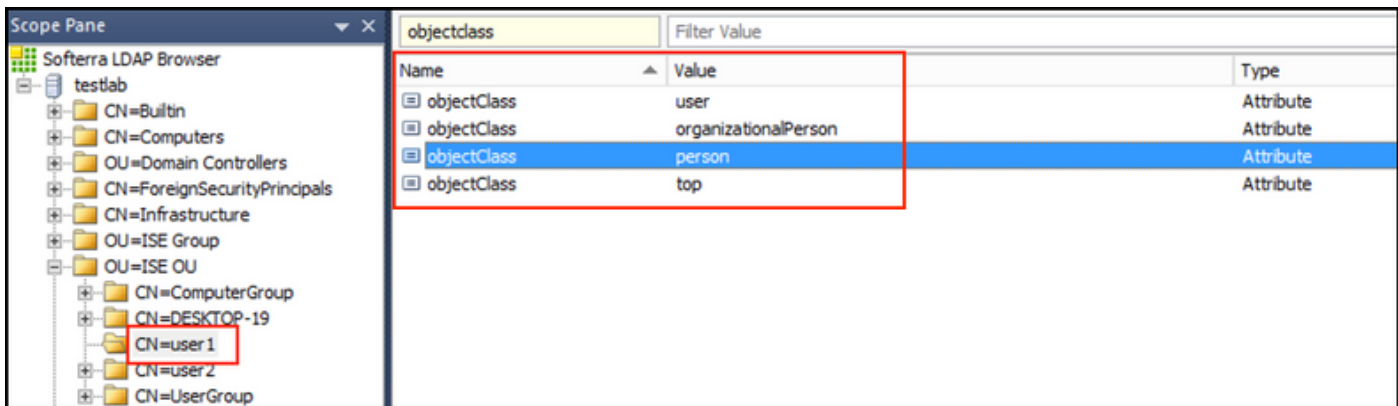
3. Para integrar el servidor LDAP, utilice los diferentes atributos LDAP del directorio LDAP. Vaya a Administration > Identity Management > External Identity Sources > LDAP Identity Sources > Add.



4. Configurar estos atributos desde la pestaña General:

Subject Objectclass: este campo corresponde a la clase Object de las cuentas de usuario. Puede utilizar una de las cuatro clases aquí:

- Arriba
- Persona
- PersonaOrganizativa
- InetOrgPerson



Atributo de nombre de asunto: este campo es el nombre del atributo que contiene el nombre de usuario de la solicitud. Este atributo se recupera de LDAPS cuando ISE consulta un nombre de

usuario específico en la base de datos LDAP (puede utilizar cn, sAMAccountName, etc). En esta situación, se utiliza el nombre de usuario user1 en el terminal.

Scope Pane: Softerra LDAP Browser, testlab

Filter Name: user1

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

Atributo de nombre de grupo: atributo que contiene el nombre de un grupo. Los valores de atributo de nombre de grupo del directorio LDAP deben coincidir con los nombres de grupo LDAP de la página Grupos de usuarios

Scope Pane: Softerra LDAP Browser, testlab

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

Clase de objeto de grupo: este valor se utiliza en búsquedas para especificar los objetos que se reconocen como grupos.

Scope Pane: Softerra LDAP Browser, testlab

objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
objectGUID	{39967F90-89BE-44B5-9CC5-B28C080EB234}	Binary Attribute
objectClass	top	Attribute
objectClass	group	Attribute
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute

Atributo de asignación de grupo: este atributo define cómo se asignan los usuarios a los grupos.

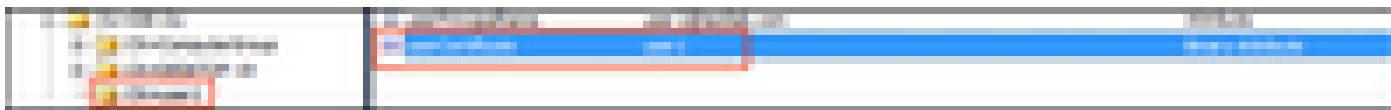
Scope Pane: Softerra LDAP Browser, testlab

Filter Name: UserGroup

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

Atributo de certificado: introduzca el atributo que contiene las definiciones de certificado. Estas

definiciones se pueden utilizar opcionalmente para validar los certificados que presentan los clientes cuando se definen como parte de un perfil de autenticación de certificados. En estos casos, se realiza una comparación binaria entre el certificado de cliente y el certificado recuperado del origen de identidad LDAP.



5. Para configurar la conexión LDAPS, navegue hasta la pestaña Connection :

LDAP Identity Sources List > testlab_idaps

LDAP Identity Source

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

Primary Server

Secondary Server

Enable Secondary Server

* Hostname/IP ⓘ

* Port

Specify server for each ISE node

Access Anonymous Access Authenticated Access

Admin DN *

Password *

Secure Authentication Enable Secure Authentication Enable Server Identity Check

LDAP Server Root CA ⓘ

Issuer CA of ISE Certificates ⓘ

Hostname/IP ⓘ

Port

Access Anonymous Access Authenticated Access

Admin DN

Password

Secure Authentication Enable Secure Authentication Enable Server Identity Check

LDAP Server Root CA ⓘ

Issuer CA of ISE Certificates ⓘ

* Server Timeout ⓘ Seconds

* Max. Admin Connections ⓘ

Force reconnect every ⓘ Minutes

Failover Always Access Primary Server First Fallback To Primary Server After Minutes

Server Timeout ⓘ Seconds

Max. Admin Connections ⓘ

Force reconnect every ⓘ Minutes

6. Ejecute dsquery en el controlador de dominio para obtener el DN de nombre de usuario que se utilizará para establecer una conexión con el servidor LDAP:

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

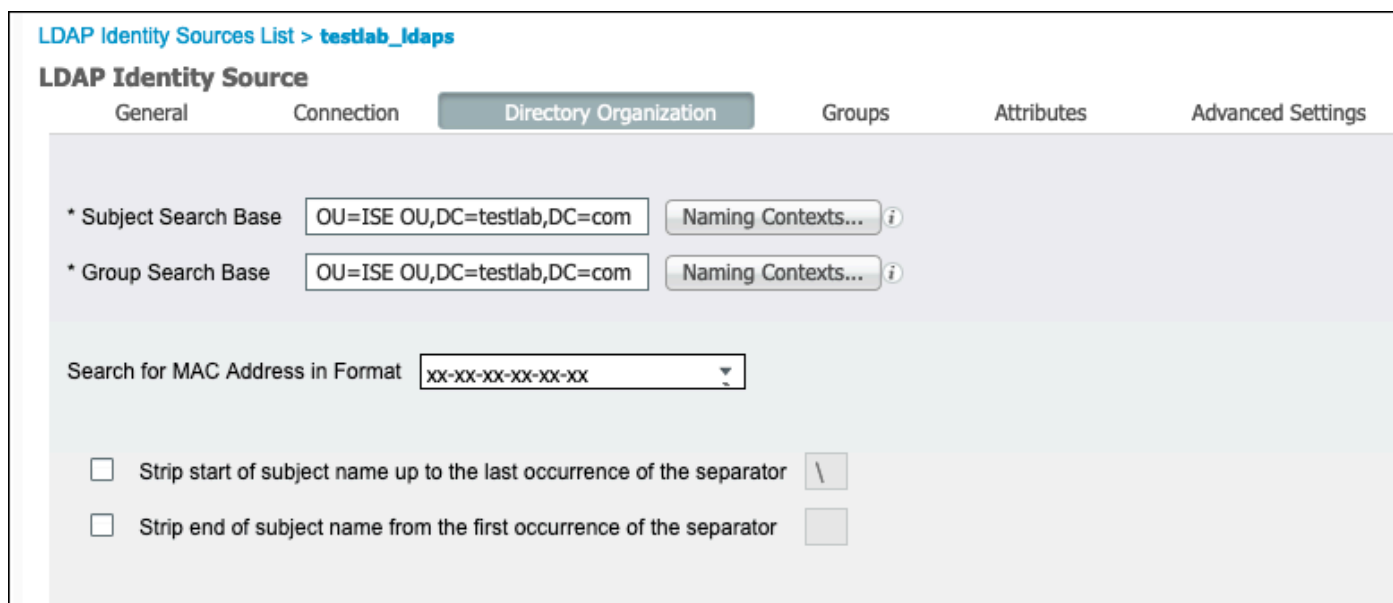

Paso 1. Establezca la dirección IP o el nombre de host correcto del servidor LDAP, defina el puerto LDAP (TCP 636) y el DN de administrador para establecer una conexión con LDAP sobre SSL.

Paso 2. Habilitar autenticación segura y la opción de comprobación de identidad del servidor.

Paso 3. En el menú desplegable, seleccione el certificado de CA raíz del servidor LDAP y el certificado de administrador de ISE Certificado de CA del emisor (hemos utilizado la autoridad de certificación instalada en el mismo servidor LDAP para emitir también el certificado de administrador de ISE).

Paso 4. Seleccione el enlace de prueba al servidor. En este momento, no se recuperan los temas o grupos porque las bases de búsqueda aún no están configuradas.

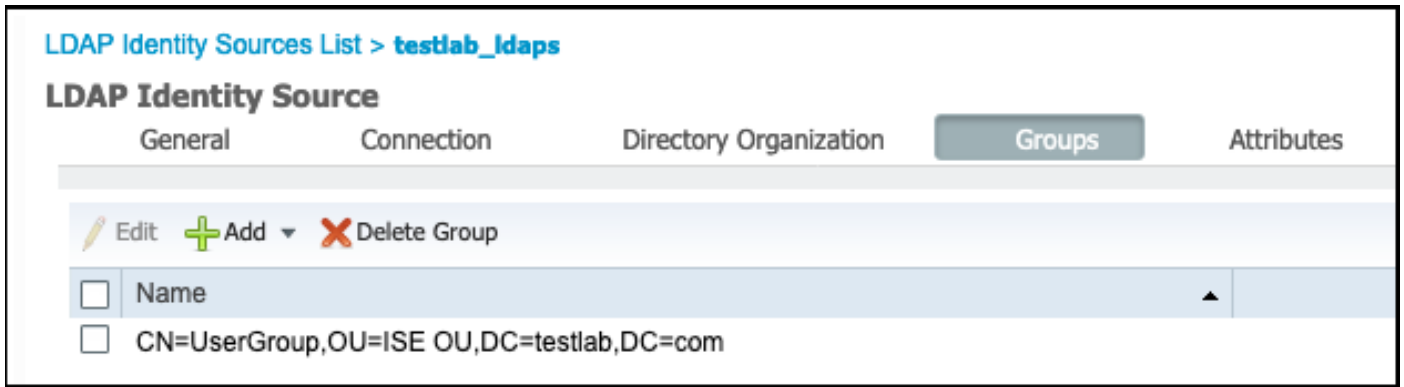
7. En la pestaña Organización de Directorios, configure la base de búsqueda de sujetos/grupos. Es el punto de unión de ISE con LDAP. Ahora sólo puede recuperar sujetos y grupos que sean hijos del punto de unión. En esta situación, tanto el sujeto como el grupo se recuperan de la unidad organizativa OU=ISE



The screenshot shows the 'LDAP Identity Sources List > testlab_ldaps' page. The 'LDAP Identity Source' section is active, with the 'Directory Organization' tab selected. The configuration includes:

- Subject Search Base:** OU=ISE OU,DC=testlab,DC=com
- Group Search Base:** OU=ISE OU,DC=testlab,DC=com
- Search for MAC Address in Format:** xx-xx-xx-xx-xx-xx
- Strip start of subject name up to the last occurrence of the separator:** \
- Strip end of subject name from the first occurrence of the separator:**

8. En Grupos, haga clic en Agregar para importar los grupos desde LDAP en ISE y recuperar los grupos, como se muestra en esta imagen.



Configuración del switch

Configure el switch para la autenticación 802.1x. PC con Windows conectado al puerto de switch 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
!

!

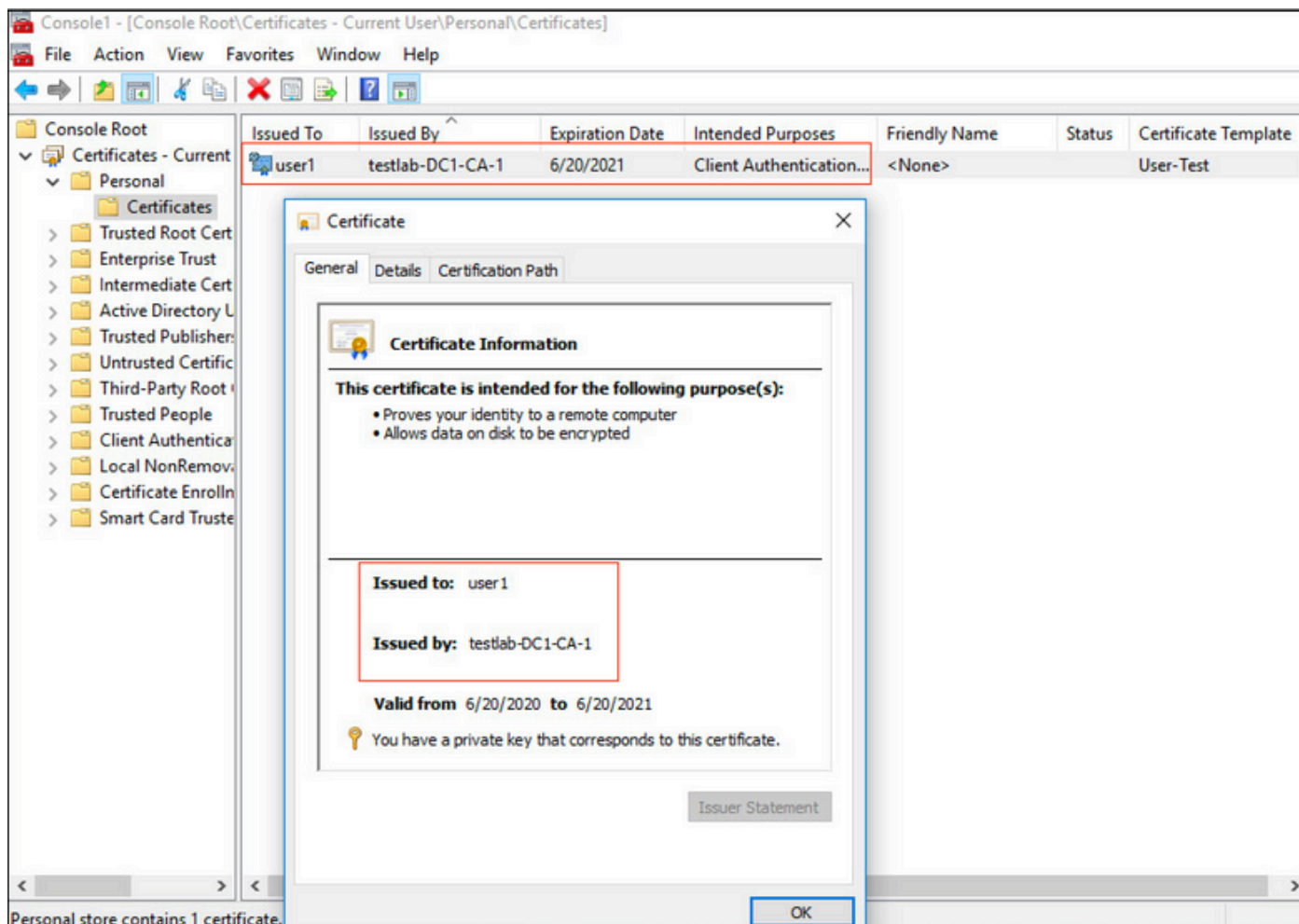
interface GigabitEthernet2/0/47
switchport access vlan xx
switchport mode access
authentication port-control auto
dot1x pae authenticator

```

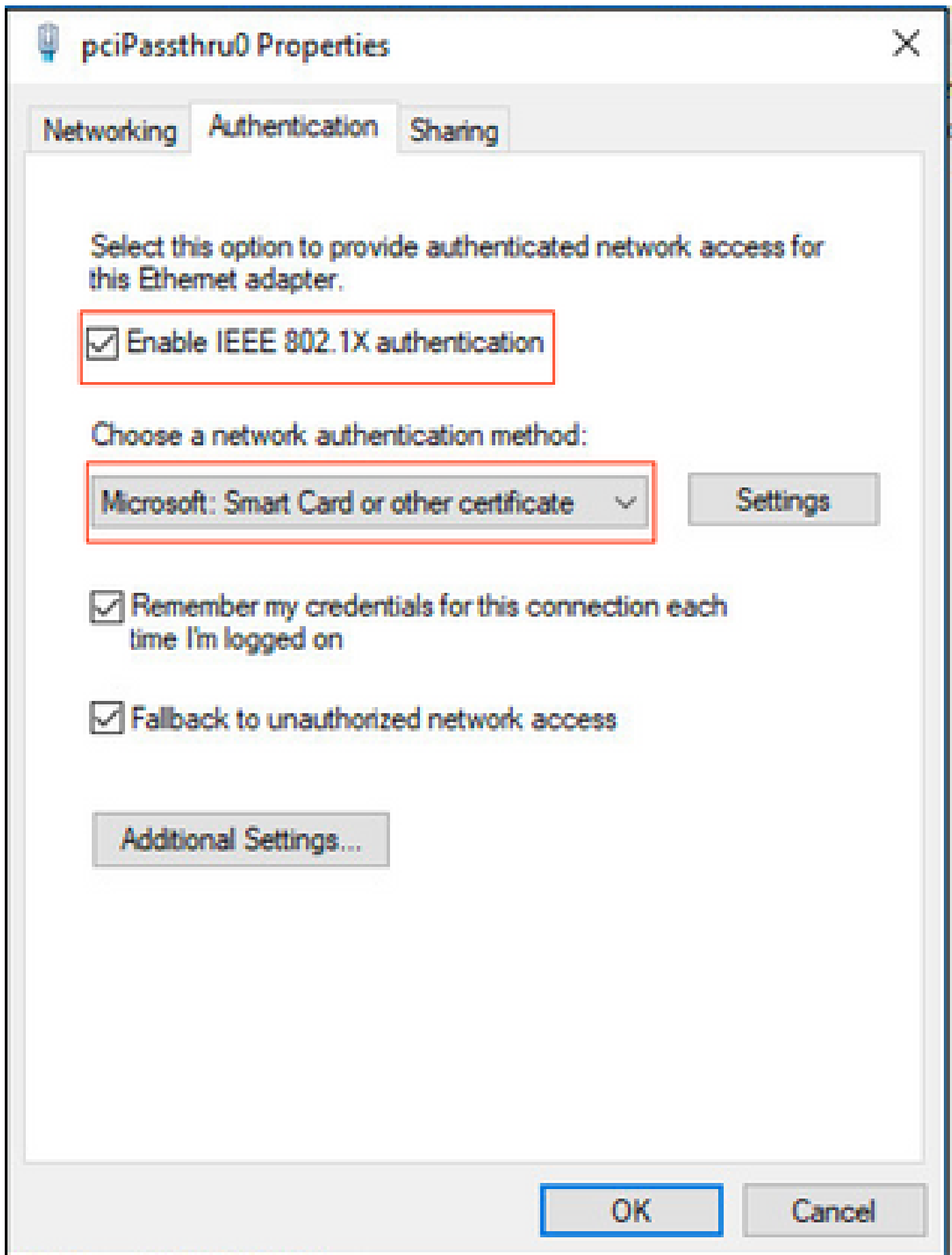
Configuración del terminal

Se utiliza el suplicante nativo de Windows y se utiliza uno de los protocolos EAP compatibles con LDAP, EAP-TLS, para la autenticación y autorización de usuarios.

1. Asegúrese de que el equipo esté aprovisionado con un certificado de usuario (para el usuario 1) y tenga el propósito previsto como Autenticación de cliente y en las Entidades de certificación raíz de confianza, la cadena de certificados del emisor esté presente en el equipo.

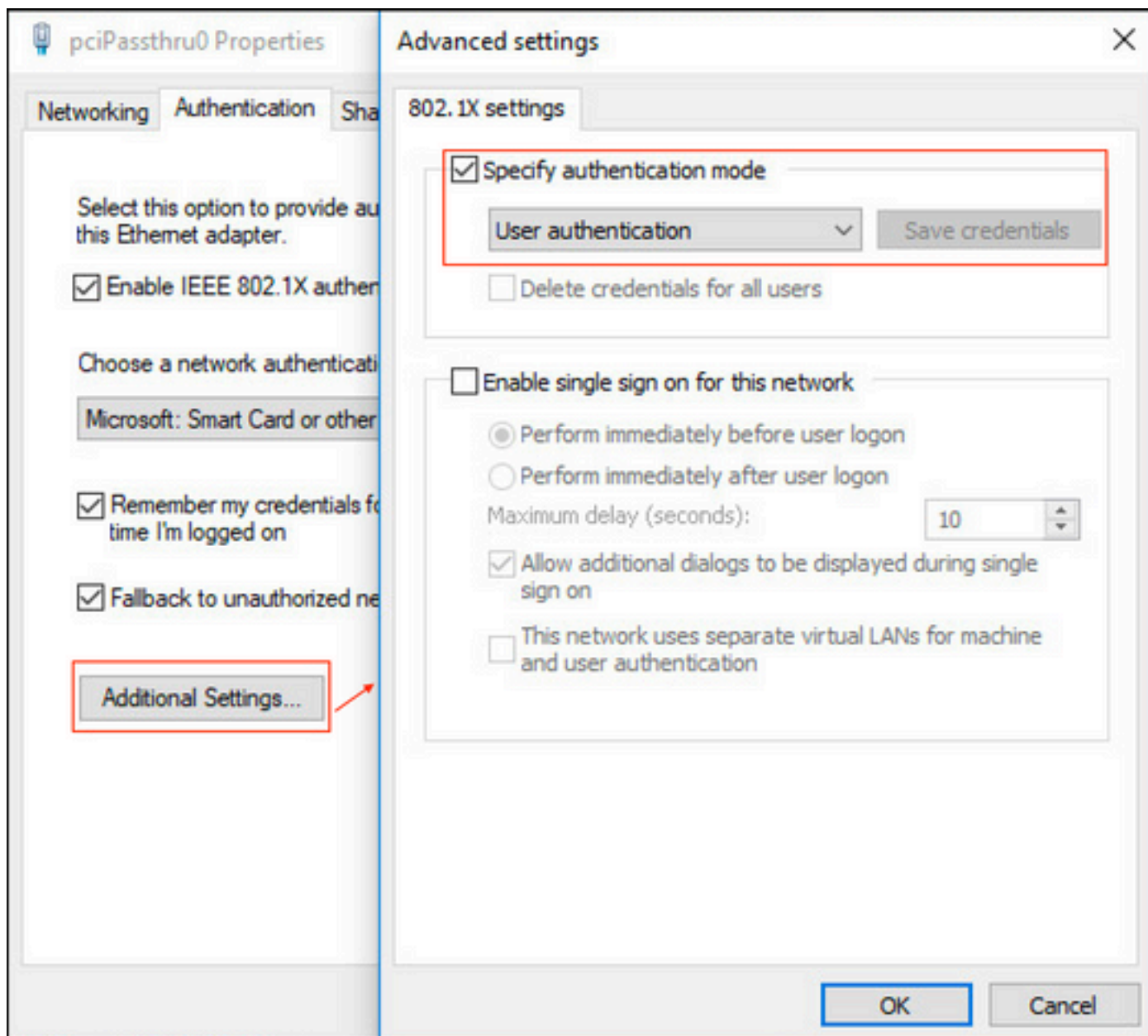


2. Habilite la autenticación Dot1x y el método Select Authentication como Microsoft:Tarjeta inteligente u otro certificado para la autenticación EAP-TLS.



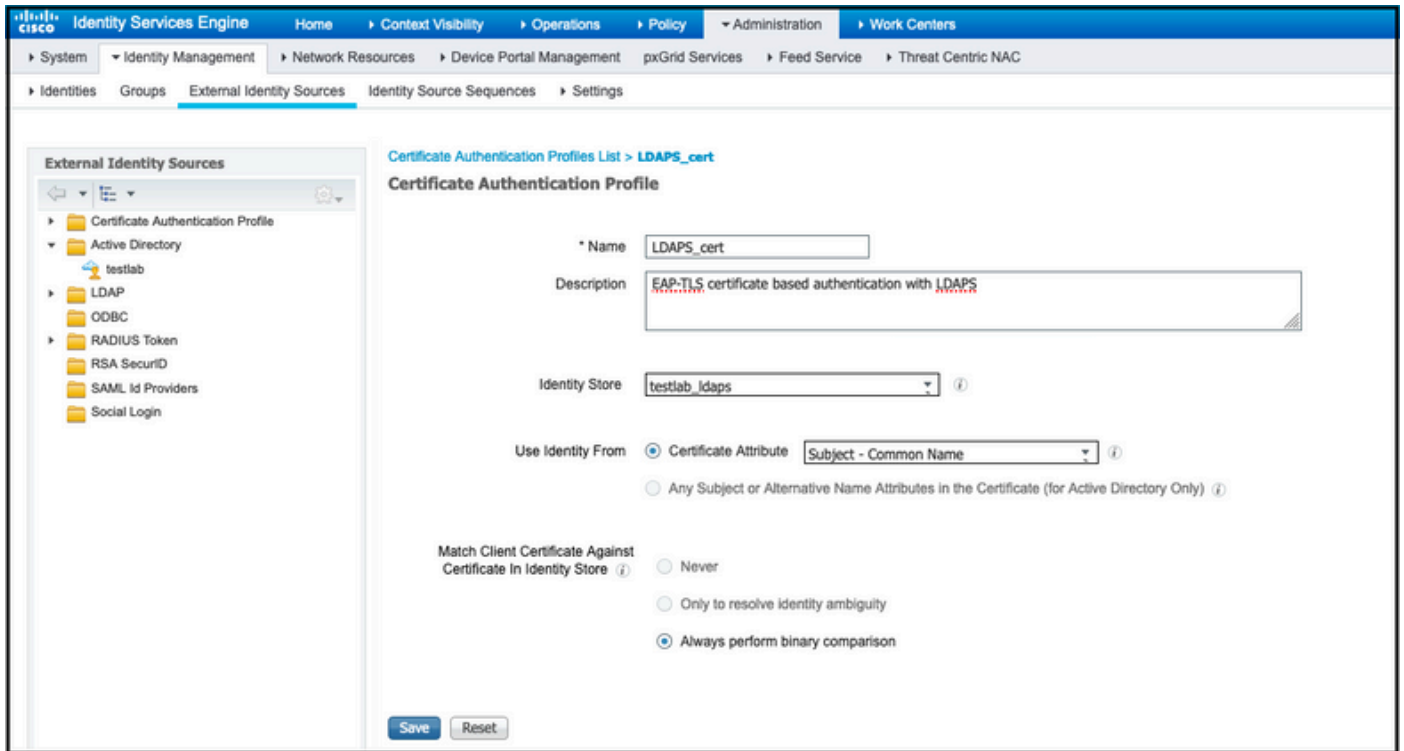
3. Haga clic en Additional Settings (Parámetros adicionales) y se abrirá una ventana. Marque la casilla con especificar el modo de autenticación y elija la autenticación de usuario, como se

muestra en esta imagen.



Configurar conjunto de políticas en ISE

Dado que se utiliza el protocolo EAP-TLS, antes de configurar el conjunto de políticas, es necesario configurar el perfil de autenticación de certificado y utilizar la secuencia de origen de identidad en la política de autenticación más adelante.



Consulte Perfil de Autenticación de Certificado en la Secuencia de Origen de Identidad y defina el origen de identidad externo LDAPS en la lista Búsqueda de Autenticación:

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

Ahora configure el conjunto de políticas para la autenticación Wired Dot1x:

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

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	453

Authentication Policy (2)

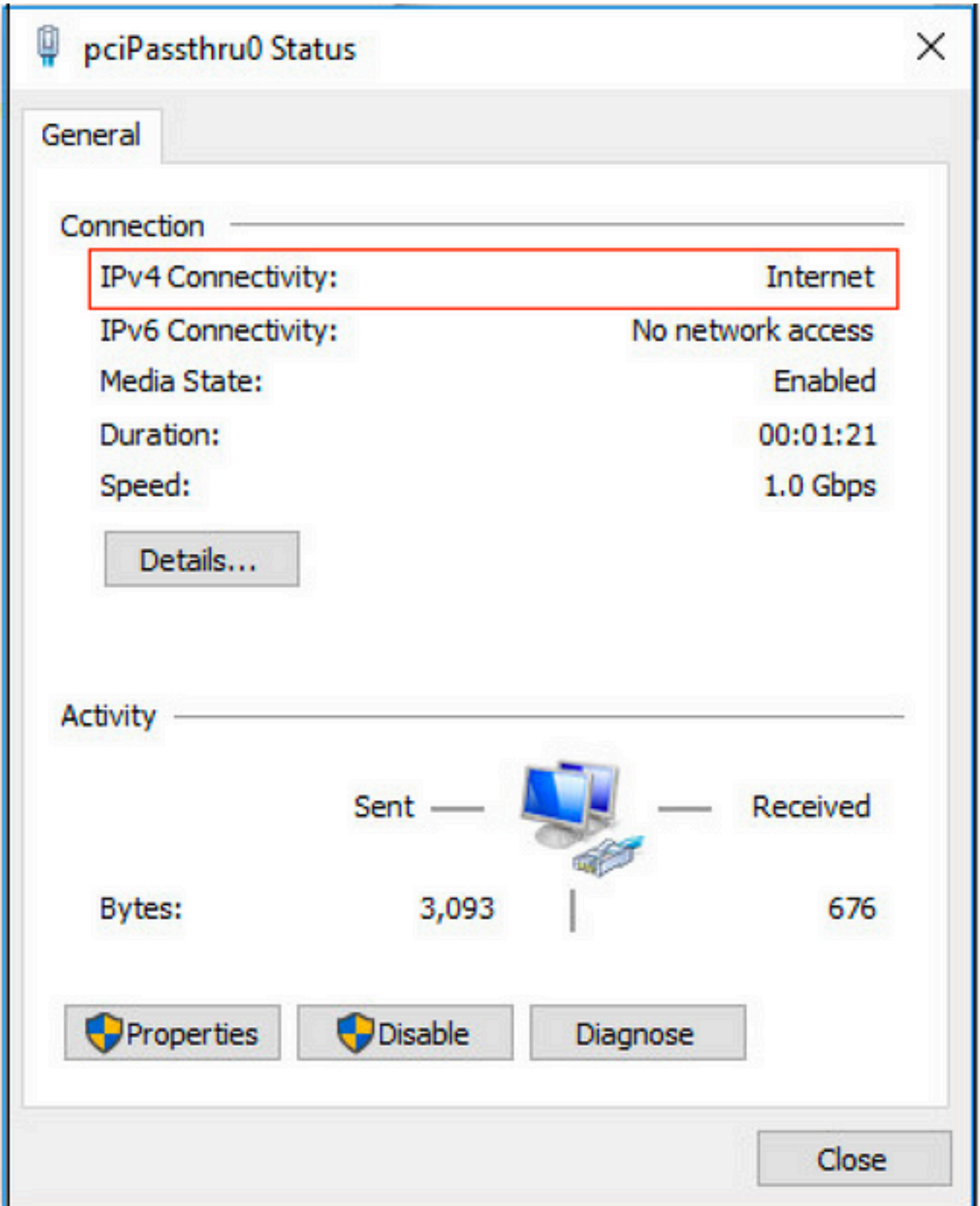
Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch	LDAPS	223	Options
✔	Default		LDAPS	0	Options

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

Después de esta configuración, podemos autenticar el punto final usando el protocolo EAP-TLS contra el origen de identidad LDAP.



Verificación

1. Verifique la sesión de autenticación en el puerto de switch conectado al PC:

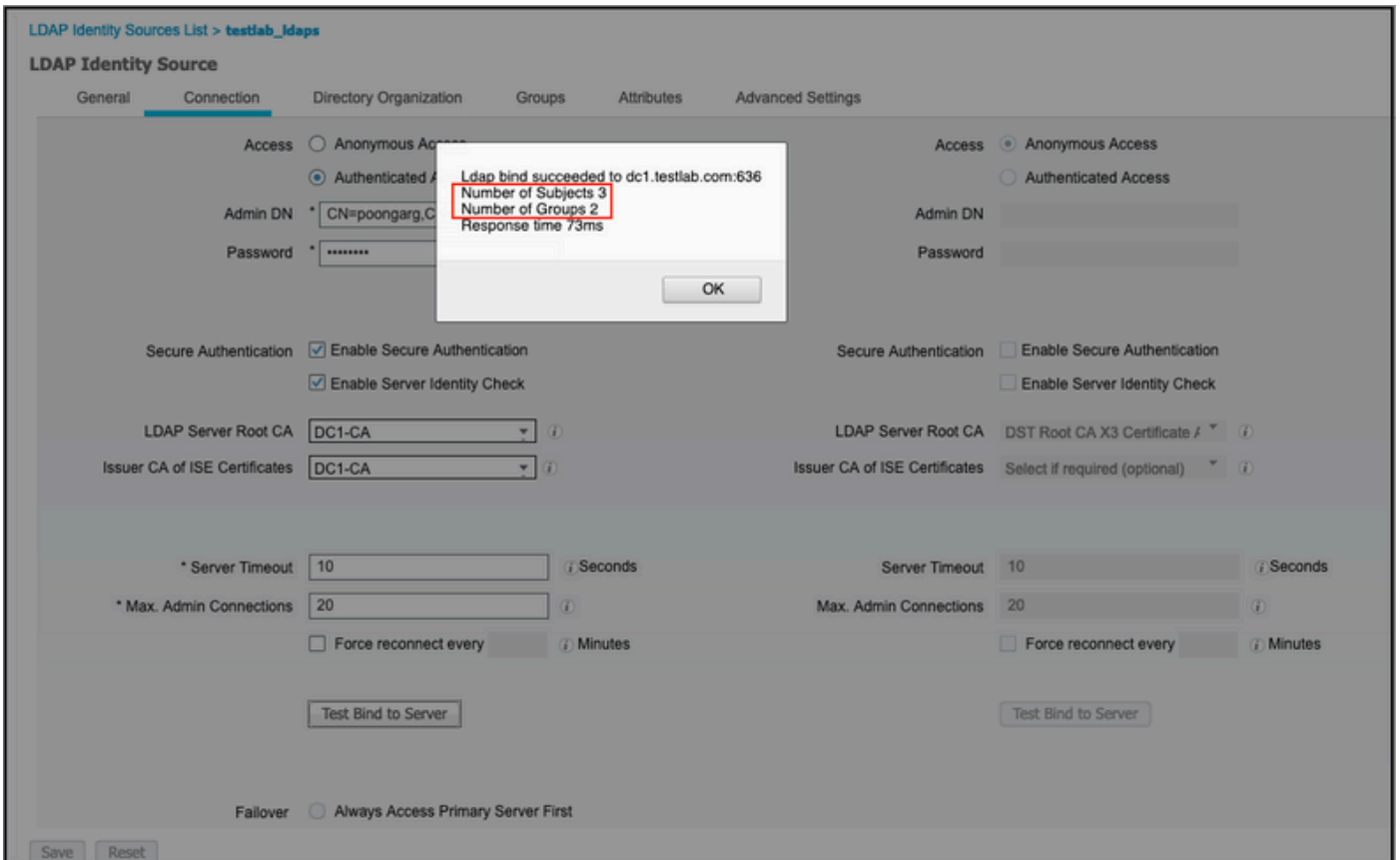
```
SW1#sh auth sessions int g2/0/47 de
      Interface: GigabitEthernet2/0/47
      MAC Address: b496.9126.dec0
      IPv6 Address: Unknown
      IPv4 Address: 10.106.38.165
      User-Name: user1
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      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. Para verificar las configuraciones LDAPS e ISE, puede recuperar los sujetos y grupos con una conexión de prueba al servidor:



3. Verifique el informe de autenticación de usuario:

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. Compruebe el informe de autenticación detallado para el terminal:

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. Valide que los datos se cifran entre el servidor ISE y el servidor LDAPS tomando la captura de paquetes en el ISE hacia el servidor 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...		28057 → 636 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=140972072 TSecr=0 WS=128
21	2020-06-24 10:40:24.206505	10.197.164.21	10.197.164.22	TCP	74	00:50:56:a0:3e:7f,0...		636 → 28057 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=30158962 TSecr=140972872
22	2020-06-24 10:40:24.206613	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=140972873 TSecr=30158962
23	2020-06-24 10:40:24.206961	10.197.164.22	10.197.164.21	TLSv1.2	207	00:0c:29:98:ca:28,0...		Client Hello
24	2020-06-24 10:40:24.210413	10.197.164.21	10.197.164.22	TLSv1.2	2036	00:50:56:a0:3e:7f,0...		Server Hello, Certificate [Packet size limited during capture]
25	2020-06-24 10:40:24.210508	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=142 Ack=1971 Win=33152 Len=0 TSval=140972877 TSecr=30158962
26	2020-06-24 10:40:24.215211	10.197.164.22	10.197.164.21	TLSv1.2	260	00:0c:29:98:ca:28,0...		Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27	2020-06-24 10:40:24.218678	10.197.164.21	10.197.164.22	TLSv1.2	173	00:50:56:a0:3e:7f,0...		Change Cipher Spec, Encrypted Handshake Message
28	2020-06-24 10:40:24.219113	10.197.164.22	10.197.164.21	TLSv1.2	199	00:0c:29:98:ca:28,0...		Application Data
29	2020-06-24 10:40:24.230304	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 10:40:24.238809	10.197.164.21	10.197.164.22	TLSv1.2	1079	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=602 Ack=3992 Win=36864 Len=0 TSval=140972905 TSecr=30158965
33	2020-06-24 10:40:24.251944	10.197.164.22	10.197.164.21	TLSv1.2	263	00:0c:29:98:ca:28,0...		Application Data
34	2020-06-24 10:40:24.253658	10.197.164.21	10.197.164.22	TLSv1.2	295	00:50:56:a0:3e:7f,0...		Application Data
35	2020-06-24 10:40:24.293322	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=879 Ack=4221 Win=39680 Len=0 TSval=140972960 TSecr=30158967
86	2020-06-24 10:40:57.946553	10.197.164.22	10.197.164.21	TLSv1.2	151	00:0c:29:98:ca:28,0...		Application Data
87	2020-06-24 10:40:57.947600	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [FIN, ACK] Seq=964 Ack=4221 Win=39680 Len=0 TSval=141006614 TSecr=30158967


```

Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
Ethernet II, Src: Vmware_00:3e: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: 17301b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84...
    
```

→ Encrypted Data

Troubleshoot

Esta sección describe algunos errores comunes que se encuentran con esta configuración y cómo solucionarlos.

- En el informe de autenticación, puede ver este mensaje de error:

Authentication method is not supported by any applicable identity store


Este mensaje de error indica que el método seleccionado no es soportado por LDAP. Asegúrese de que el protocolo de autenticación del mismo informe muestre uno de los métodos compatibles (EAP-GTC, EAP-TLS o PEAP-TLS).

- El enlace de prueba al servidor finalizó con un error.

Normalmente, esto se debe a un error en la comprobación de validación del certificado del servidor LDAP. Para resolver este tipo de problemas, tome una captura de paquetes en ISE y habilite los tres componentes en tiempo de ejecución y port-jni en el nivel de depuración, vuelva a crear el problema y verifique el archivo prt-server.log.

La captura de paquetes se queja de un certificado incorrecto y el servidor de puertos muestra:

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

 Nota: El nombre de host en la página LDAP debe configurarse con el nombre de sujeto del certificado (o cualquiera de los nombres alternativos de sujeto). Por lo tanto, a menos que tenga estos datos en el asunto o en la SAN, no funcionan, se necesita el certificado con la dirección IP en la lista de SAN.

3. En el informe de autenticación, puede observar que el sujeto no se encontró en el almacén de identidades. Esto significa que el nombre de usuario del informe no coincide con el atributo de nombre de sujeto para ningún usuario de la base de datos LDAP. En este escenario, el valor se estableció en sAMAccountName para este atributo, lo que significa que ISE busca los valores de sAMAccountName para el usuario LDAP cuando intenta encontrar una coincidencia.

4. Los sujetos y grupos no se pudieron recuperar correctamente durante una prueba de enlace al servidor. La causa más probable de este problema es una configuración incorrecta de las bases de búsqueda. Recuerde que la jerarquía de LDAP debe especificarse desde la hoja hasta la raíz y desde el dc (puede constar de varias palabras).

Información Relacionada

- <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>

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).