

Configurar e solucionar problemas do ISE com armazenamento de identidade LDAPS externo

Contents

- [Introdução](#)
- [Pré-requisitos](#)
- [Requisitos](#)
- [Componentes Utilizados](#)
- [Configurar](#)
- [Diagrama de Rede](#)
- [Configurar LDAPS no Ative Directory](#)
- [Instalar Certificado de Identidade no Controlador de Domínio](#)
- [Acessar estrutura de diretório LDAPS](#)
- [Integrar o ISE com o servidor LDAPS](#)
- [Configurar o switch](#)
- [Configurar o endpoint](#)
- [Configurar definição de política no ISE](#)
- [Verificar](#)
- [Troubleshooting](#)
- [Informações Relacionadas](#)

Introdução

Este documento descreve a integração do Cisco ISE com o servidor LDAPS seguro como uma fonte de identidade externa.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da administração do Identity Service Engine (ISE)
- Conhecimento básico do Ative Directory/Secure Lightweight Directory Access Protocol (LDAPS)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE 2.6 Patch 7
- Microsoft Windows versão 2012 R2 com Ative Directory Lightweight Directory Services instalado
- PC com sistema operacional Windows 10 com suplicante nativo e certificado do usuário instalado
- Switch Cisco C3750X com imagem 152-2.E6

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O LDAPS permite a criptografia de dados LDAP (que incluem credenciais de usuário) em trânsito quando uma ligação de diretório é estabelecida. O LDAPS usa a porta TCP 636.

Esses protocolos de autenticação são suportados com LDAPS:

- Placa de token genérica EAP (EAP-GTC)
- PAP (Password Authentication Protocol Protocolo de Autenticação de Senha)
- EAP Transport Layer Security (EAP-TLS)
- Segurança da camada de transporte EAP protegida (PEAP-TLS)

Observação: EAP-MSCHAPV2 (como um método interno de PEAP, EAP-FAST ou EAP-TTLS), LEAP, CHAP e EAP-MD5 não são suportados com a Origem de identidade externa LDAPS.

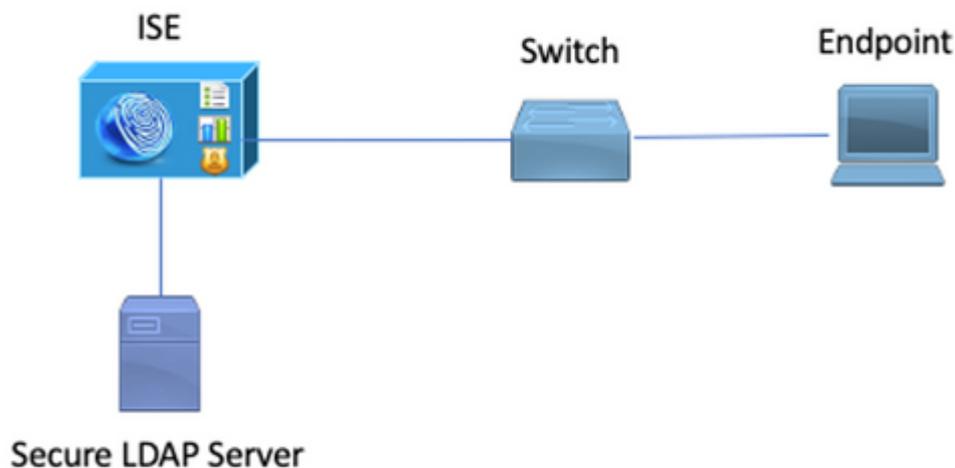
Configurar

Esta seção descreve a configuração dos dispositivos de rede e a integração do ISE com o servidor LDAP do Microsoft Active Directory (AD).

Diagrama de Rede

Neste exemplo de configuração, o endpoint usa uma conexão Ethernet com um switch para se conectar à rede local (LAN). A porta de switch conectada está configurada para autenticação 802.1x para autenticar os usuários com o ISE. No ISE, o LDAPS é configurado como um armazenamento de identidade externo.

Esta imagem ilustra a topologia de rede que é usada:

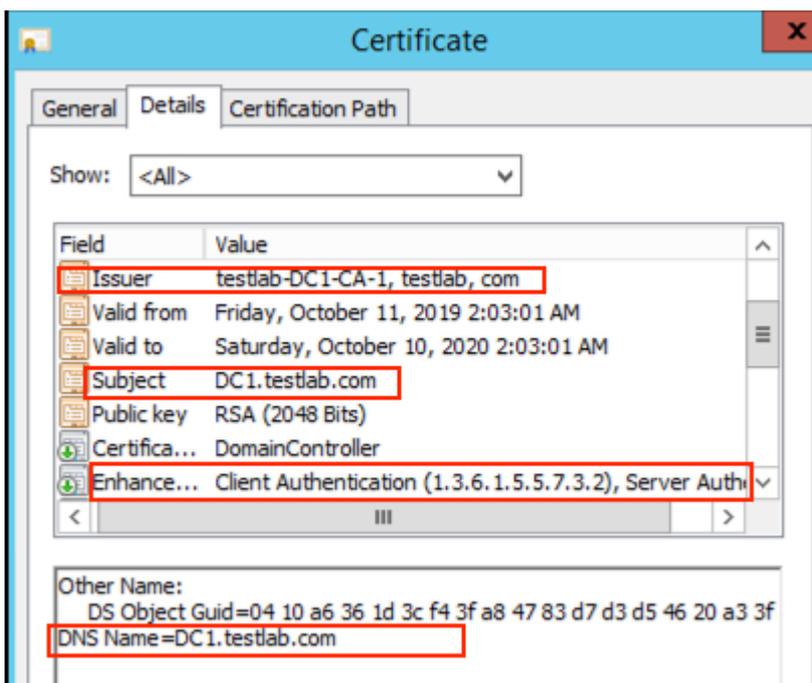


Configurar LDAPS no Active Directory

Instalar Certificado de Identidade no Controlador de Domínio

Para habilitar o LDAPS, instale um certificado no DC (Controlador de Domínio) que atenda aos seguintes requisitos:

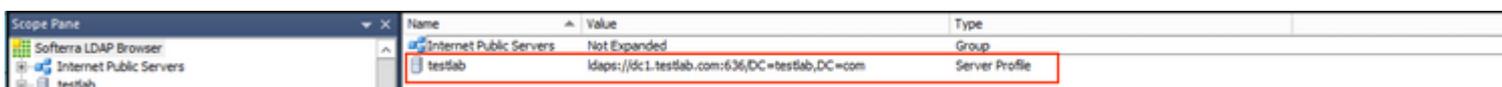
1. O certificado LDAPS está localizado no Repositório de Certificados Pessoais do Controlador de Domínio.
2. Uma chave privada que corresponde ao certificado está presente no repositório do Controlador de Domínio e corretamente associada ao certificado.
3. A extensão Enhanced Key Usage inclui o identificador de objeto (1.3.6.1.5.5.7.3.1) de Autenticação do Servidor (também conhecido como OID).
4. O Nome de Domínio Totalmente Qualificado (FQDN) do Controlador de Domínio (por exemplo, DC1.testlab.com) deve estar presente em um destes atributos: O Nome Comum (CN) no campo Assunto e a entrada DNS na Extensão de Nome Alternativo do Assunto.
5. O certificado deve ser emitido por uma CA (Autoridade de Certificação) em que o Controlador de Domínio e os clientes LDAPS confiam. Para uma comunicação segura confiável, o cliente e o servidor devem confiar na CA raiz um do outro e nos certificados de CA intermediários que emitiram certificados para eles.
6. O provedor de serviços de criptografia (CSP) Schannel deve ser usado para gerar a chave.



Acessar estrutura de diretório LDAPS

Para acessar o Diretório LDAP no servidor do Active Directory, use qualquer navegador LDAP. Neste LABORATÓRIO, o Softerra LDAP Browser 4.5 é usado.

1. Estabeleça uma conexão com o domínio na porta TCP 636.



2. Para simplificar, crie uma Unidade Organizacional (UO) chamada ISE OU no AD e ela deve ter um

Grupo chamado UserGroup. Crie dois usuários (user1 e user2) e torne-os membros do grupo UserGroup.

Observação: a origem de identidade LDAP no ISE é usada somente para autenticação de usuário.

The screenshot shows the Active Directory console with the 'Scope Pane' on the left and a list of objects on the right. The 'OU=ISE OU' is highlighted in the tree, and its properties are shown in the right pane. The properties include:

Name	Value	Type
cn	UserGroup	Entry
cn	user2	Entry
cn	user1	Entry
cn	DESKTOP-19	Entry
cn	ComputerGroup	Entry
distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribute
dSCorePropagationData	1/1/1601	Attribute
dSCorePropagationData	6/20/2020 2:51:11 AM	Attribute
gPLink	[LDAP://cn={21A53B13-6971-45E8-8545-FD0C68E29790},c...	Attribute
instanceType	[Writable]	Attribute
name	ISE OU	Attribute
objectCategory	CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=...	Attribute
objectClass	organizationalUnit	Attribute
objectClass	top	Attribute
ou	ISE OU	Attribute
uSNChanged	607428	Attribute
uSNCreated	603085	Attribute
whenChanged	6/21/2020 2:44:06 AM	Attribute
whenCreated	6/20/2020 2:51:11 AM	Attribute
objectGUID	{44F45D1D-17B7-48DF-ABC6-3ED27FA4F694}	Binary A

Integrar o ISE com o servidor LDAPS

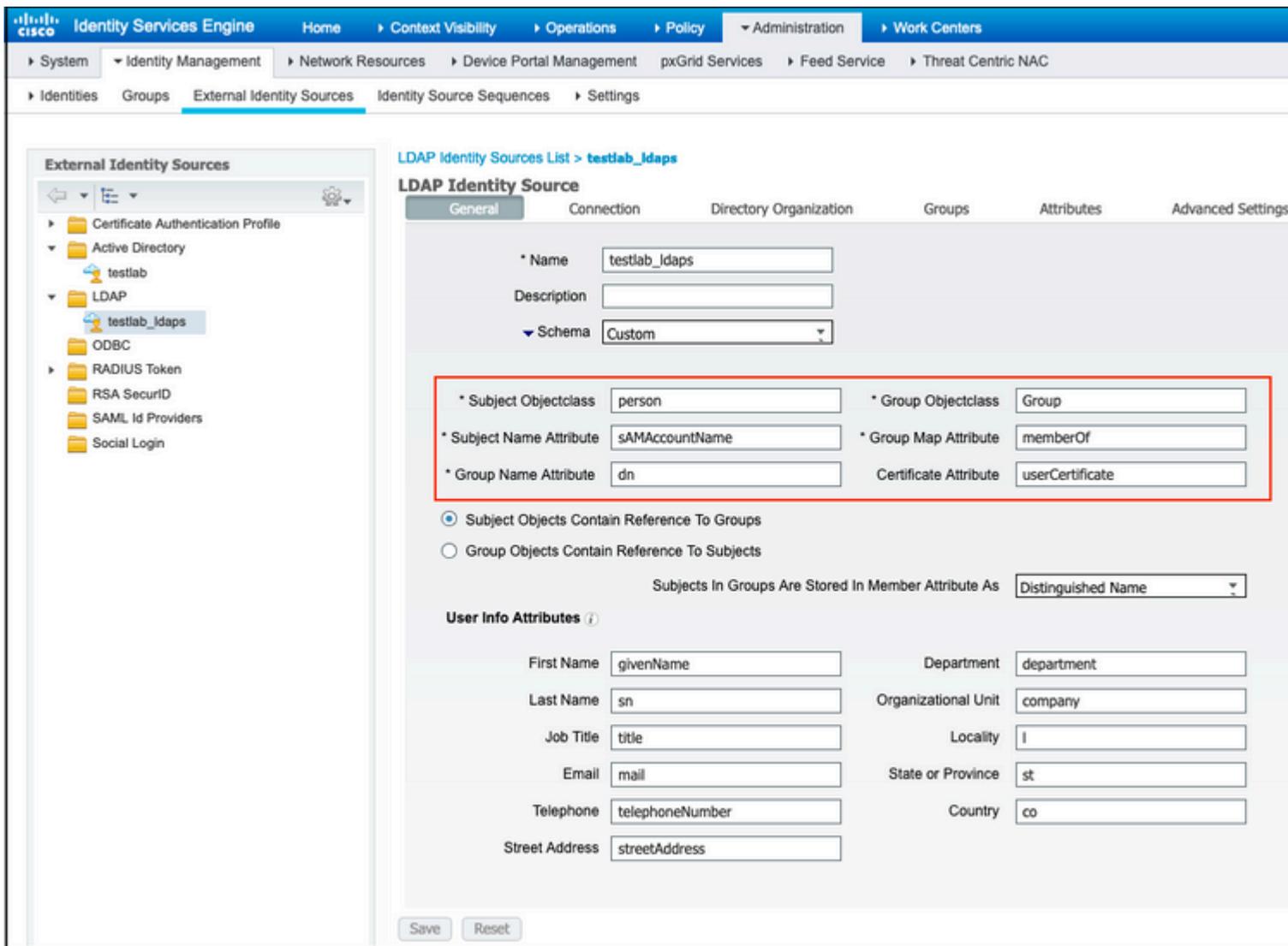
1. Importe o certificado CA raiz do servidor LDAP no Certificado Confiável.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The 'Certificate Management' section is active, displaying a table of certificates. The 'DC1-CA' certificate is highlighted with a red box. The table columns are:

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

2. Valide o certificado de administrador do ISE e verifique se o certificado do emissor do certificado de administrador do ISE também está presente no Repositório de Certificados Confiáveis.

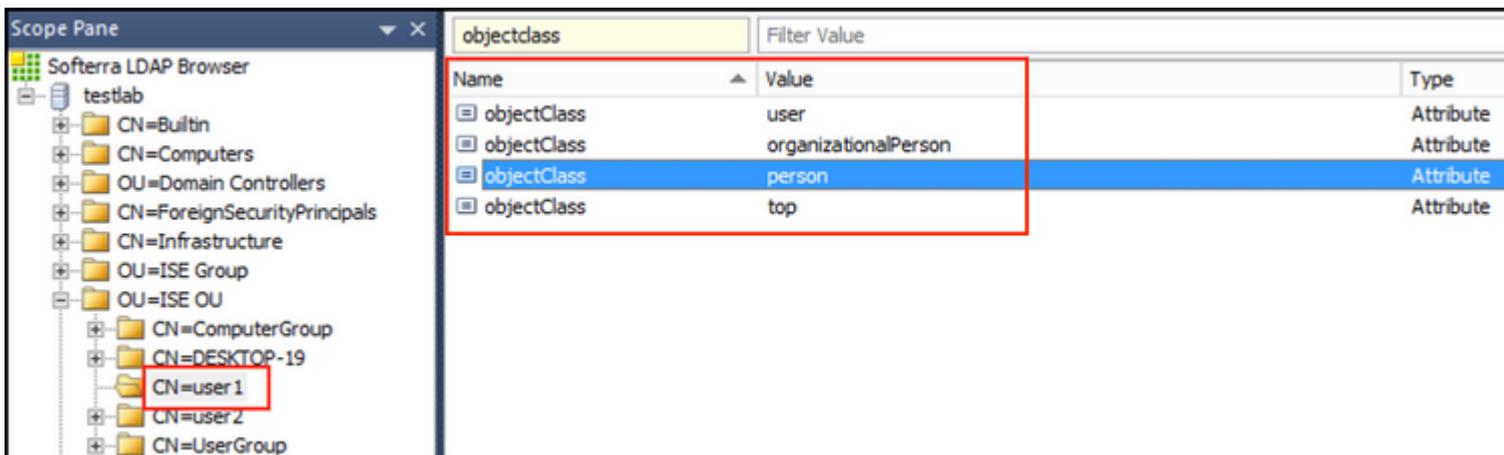
3. Para integrar o servidor LDAPS, use os diferentes atributos LDAP do diretório LDAPS. Navegue até **Administração > Gerenciamento de identidades > Origens de identidade externas > Origens de identidade LDAP > Adicionar.**



4. Configure estes atributos a partir da Guia Geral:

Classe de Objeto do Assunto: Esse campo corresponde à classe Objeto das contas de usuário. Você pode usar uma das quatro classes aqui:

- Superior
- Pessoa
- PessoaOrganizacional
- InetOrgPerson



Atributo do Nome do Assunto: Este campo é o nome do atributo que contém o nome de usuário da solicitação. Esse atributo é recuperado do LDAPS quando o ISE consulta um nome de usuário específico no banco de dados LDAP (você pode usar cn, sAMAccountName etc.). Neste cenário, o nome de usuário user1 no ponto final é usado.

Name	Value	Type
cn	user 1	Attribute
displayName	user 1	Attribute
distinguishedName	CN=user 1,OU=ISE OU,DC=testlab,DC=com	Attribute
givenName	user 1	Attribute
name	user 1	Attribute
sAMAccountName	user 1	Attribute
userPrincipalName	user1@testlab.com	Attribute
userCertificate	user 1	Binary Attribute

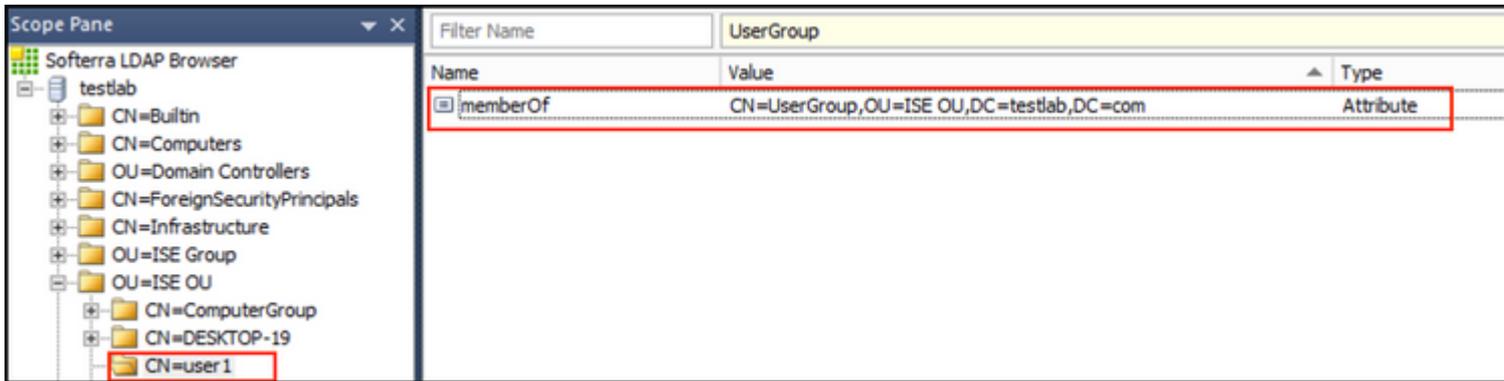
Atributo do Nome do Grupo: Este é o atributo que contém o nome de um grupo. Os valores do atributo Nome do grupo no diretório LDAP devem corresponder aos nomes do grupo LDAP na página Grupos de usuários

Name	Value	Type
cn	UserGroup	Attrib
distinguishedName	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attrib
dSCorePropagationData	1/1/1601	Attrib
groupType	[GlobalScope, Security]	Attrib
instanceType	[Writable]	Attrib
member	CN=user 1,OU=ISE OU,DC=testlab,DC=com	Attrib
member	CN=user 2,OU=ISE OU,DC=testlab,DC=com	Attrib
name	UserGroup	Attrib
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attrib
objectClass	group	Attrib
objectClass	top	Attrib
sAMAccountName	UserGroup	Attrib
sAMAccountType	< samGroupObject >	Attrib

Group Objectclass: esse valor é usado em pesquisas para especificar os objetos que são reconhecidos como grupos.

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

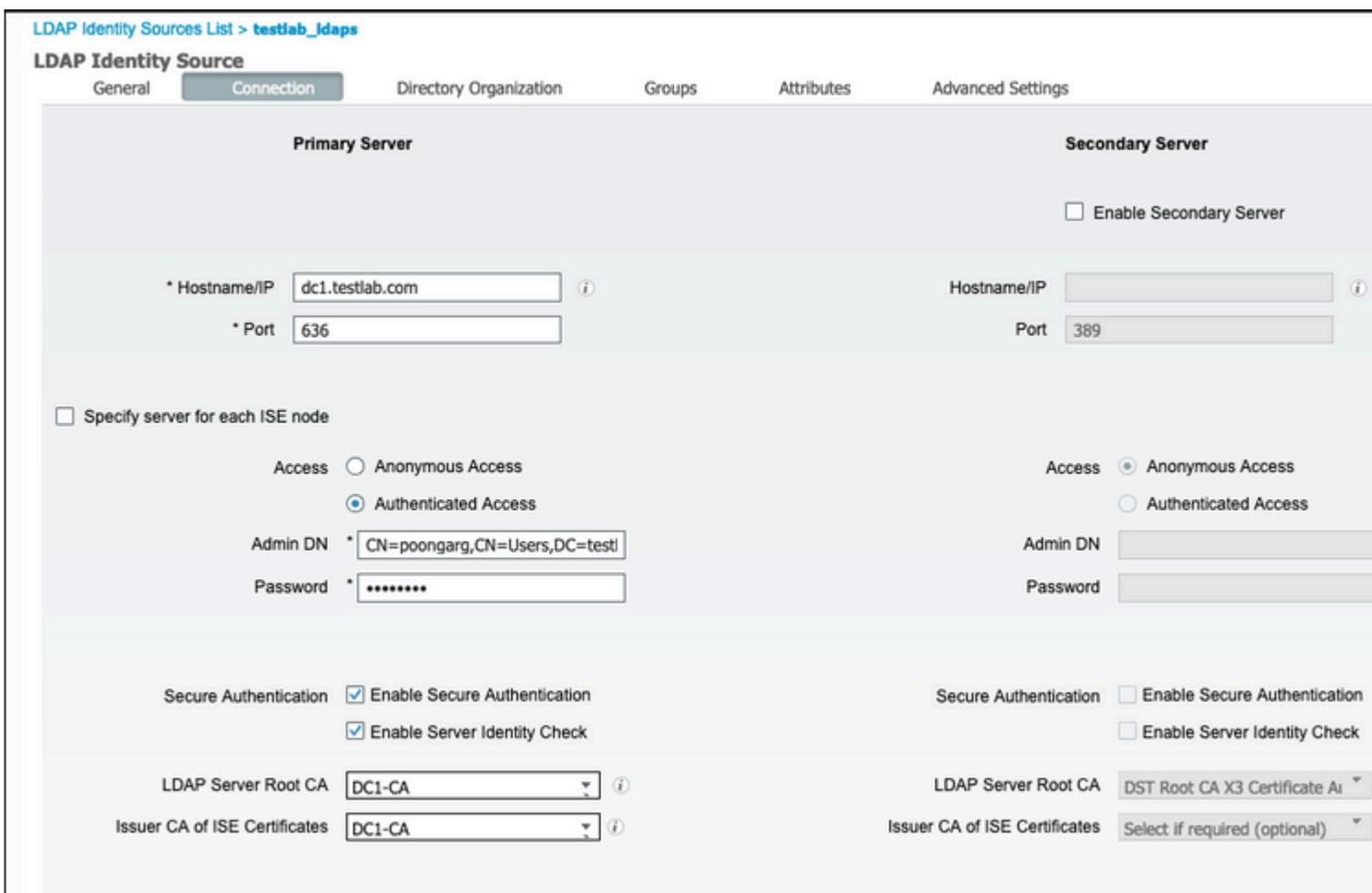
Atributo de mapa de grupo: este atributo define como os usuários são mapeados para os grupos.



Atributo do Certificado: Informe o atributo que contém as definições do certificado. Essas definições podem ser usadas opcionalmente para validar certificados apresentados por clientes quando eles são definidos como parte de um perfil de autenticação de certificado. Nesses casos, uma comparação binária é realizada entre o certificado do cliente e o certificado recuperado da origem da identidade LDAP.



5. Para configurar a conexão LDAPS, navegue até a guia **Connection**:



* Server Timeout: 10 Seconds

* Max. Admin Connections: 20

Force reconnect every: Minutes

Test Bind to Server

Failover:

- Always Access Primary Server First
- Fallback To Primary Server After 5 Minutes

6. Execute dsquery no controlador de domínio para obter o DN do nome de usuário a ser usado para estabelecer uma conexão com o servidor LDAP:

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

Etapa 1. Defina o endereço IP ou o nome de host correto do servidor LDAP, defina a porta LDAPS (TCP 636) e o DN Admin para fazer uma conexão com o LDAP sobre SSL.

Etapa 2. Opção Habilitar Autenticação Segura e Verificação de Identidade de Servidor.

Etapa 3. No menu suspenso, selecione o certificado CA raiz do servidor LDAP e o certificado administrador ISE Emissor CA (usamos autoridade de certificação, instalada no mesmo servidor LDAP para emitir o certificado admin ISE também).

Etapa 4. Selecione Testar Ligação com o servidor. Neste ponto, nenhum assunto ou grupo será recuperado porque as bases de pesquisa ainda não estão configuradas.

7. Na guia **Directory Organization**, configure a Base de Pesquisa de Assunto/Grupo. É o ponto de junção do ISE com o LDAP. Agora você pode recuperar apenas assuntos e grupos que são filhos do ponto de união. Nesse cenário, o assunto e o grupo são recuperados da OU=ISE OU

LDAP Identity Sources List > testlab_ldaps

LDAP Identity Source

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

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

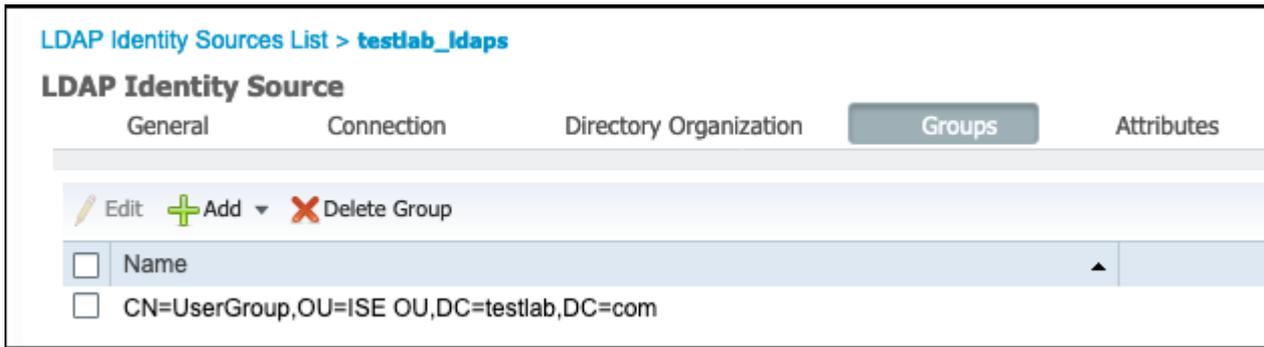
* Group Search Base: OU=ISE OU,DC=testlab,DC=com Naming Contexts...

Search for MAC Address in Format: XX-XX-XX-XX-XX-XX

Strip start of subject name up to the last occurrence of the separator \

Strip end of subject name from the first occurrence of the separator

8. Em Grupos, clique em Adicionar para importar os grupos do LDAP no ISE e recuperar os grupos, como mostrado nesta imagem.



Configurar o switch

Configure o switch para a autenticação 802.1x. O PC com Windows está conectado à porta 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
!

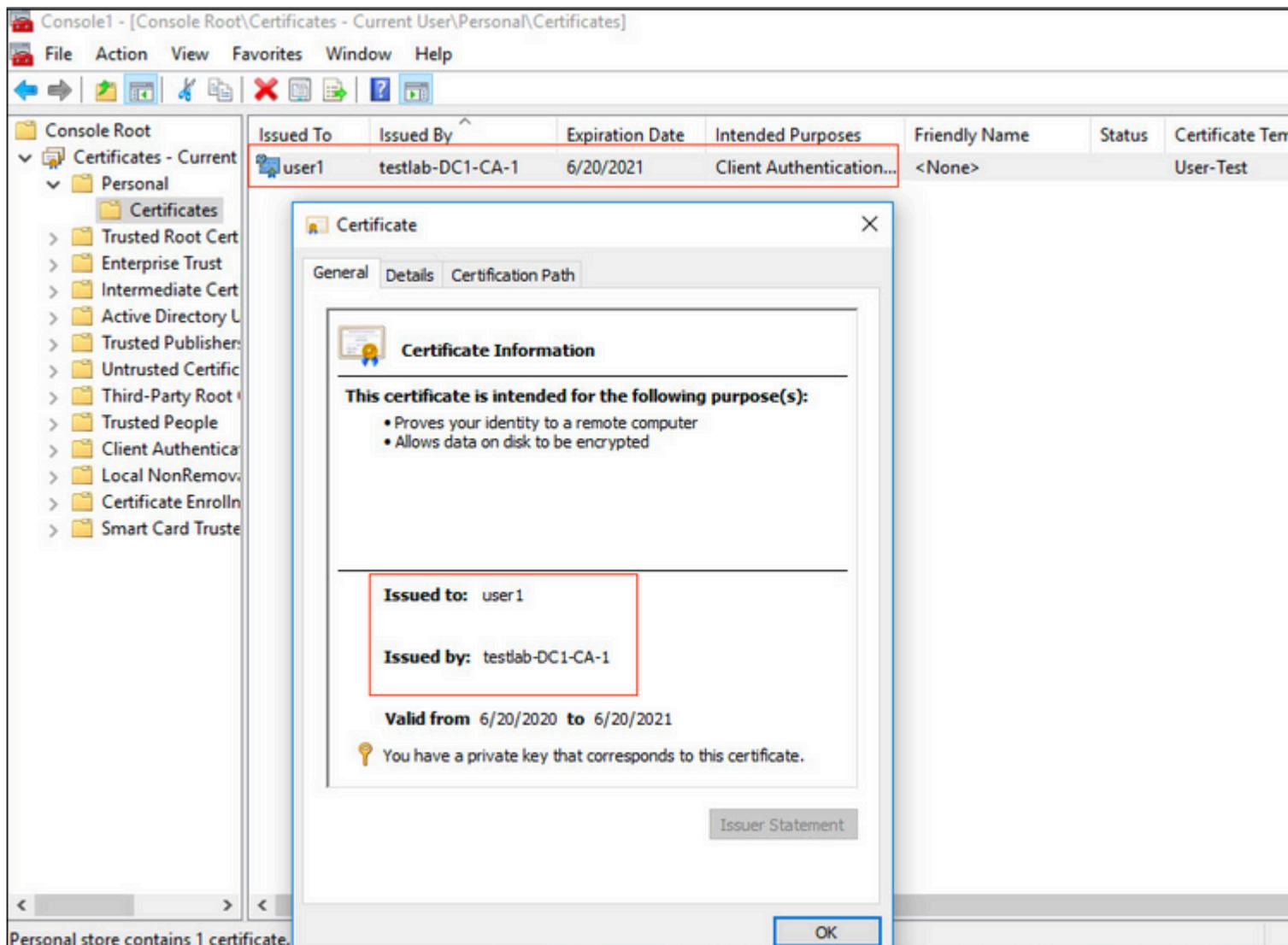
!

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

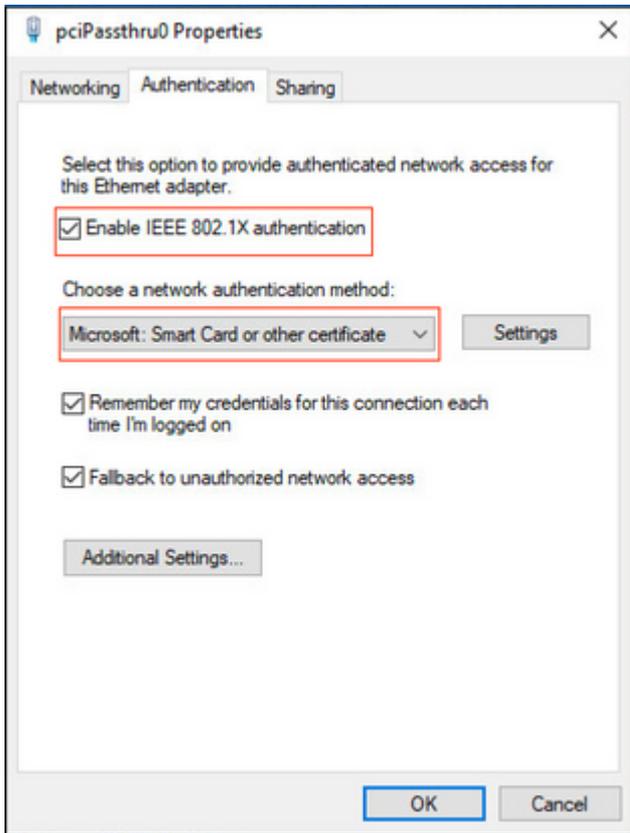
Configurar o endpoint

O Windows Native Sspplicant é usado e um dos protocolos EAP suportados pelo LDAP é utilizado, EAP-TLS para autenticação e autorização do usuário.

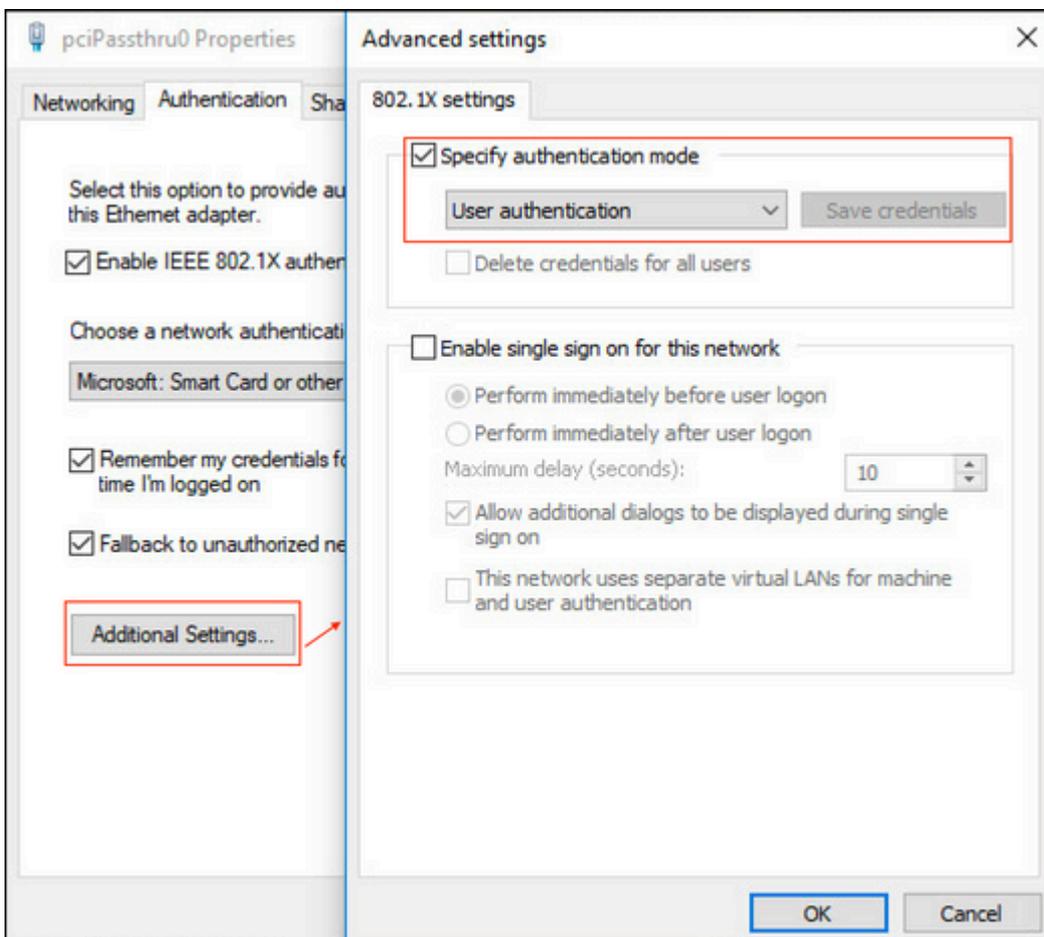
1. Verifique se o PC foi provisionado com o certificado do usuário (para o usuário1) e se a finalidade pretendida é a Autenticação do Cliente e, nas Autoridades de Certificação Raiz Confiáveis, se a cadeia de certificados do emissor está presente no PC.



2. Ative a autenticação Dot1x e selecione o método de autenticação como Microsoft:Smart Card ou outro certificado para a autenticação EAP-TLS.

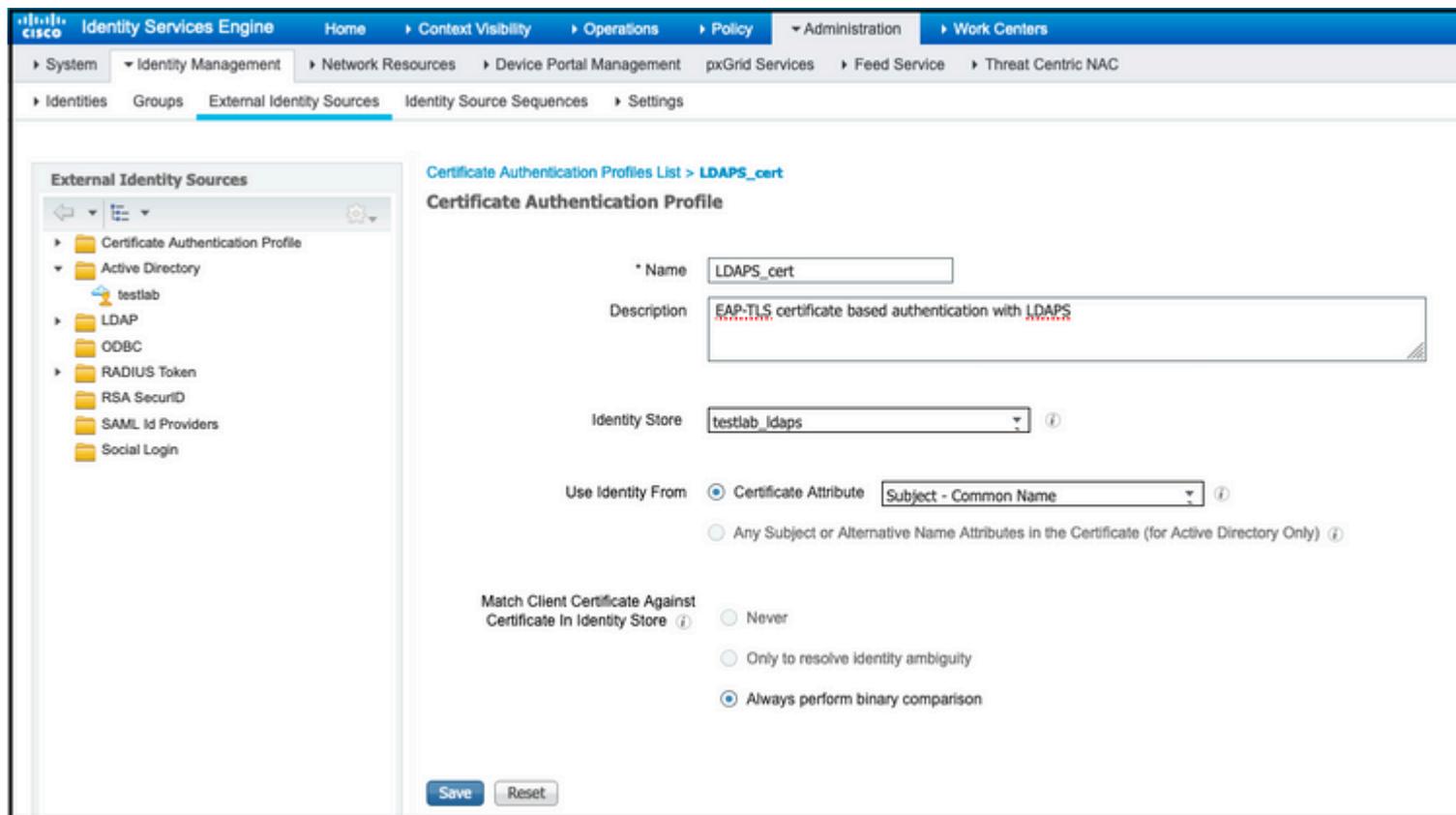


3. Clique em Configurações Adicionais e uma janela será aberta. Marque a caixa com especificar o modo de autenticação e escolha a autenticação do usuário, conforme mostrado nesta imagem.



Configurar definição de política no ISE

Como o protocolo EAP-TLS é usado, antes de o conjunto de políticas ser configurado, o perfil de autenticação de certificado precisa ser configurado e a sequência de origem de identidade é usada mais tarde na política de autenticação.



The screenshot displays the Cisco Identity Services Engine (ISE) configuration page for a Certificate Authentication Profile. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > External Identity Sources > Identity Source Sequences > Settings. The left sidebar shows a tree view of External Identity Sources, including Certificate Authentication Profile, Active Directory, testlab, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The main content area is titled "Certificate Authentication Profile" and shows the configuration for a profile named "LDAPS_cert". The description is "EAP-TLS certificate based authentication with LDAPS". The Identity Store is set to "testlab_ldaps". The "Use Identity From" section has "Certificate Attribute" selected, with "Subject - Common Name" chosen from the dropdown. The "Match Client Certificate Against Certificate In Identity Store" section has "Always perform binary comparison" selected. The "Save" and "Reset" buttons are at the bottom.

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- testlab
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Certificate Authentication Profiles List > LDAPS_cert

Certificate Authentication Profile

Name: LDAPS_cert

Description: EAP-TLS certificate based authentication with LDAPS

Identity Store: testlab_ldaps

Use Identity From: Certificate Attribute: Subject - Common Name

Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store: Never, Only to resolve identity ambiguity, Always perform binary comparison

Save Reset

Consulte o Perfil de autenticação de certificado na Sequência de origem da identidade e defina a origem de identidade externa LDAPS na lista de pesquisa de autenticação:

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

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

Authentication Search List

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

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

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

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

Save Reset

Agora configure o conjunto de políticas para autenticação 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

Status	Policy Set Name	Description	Conditions
	Wired Dot1x		Wired_802.1X

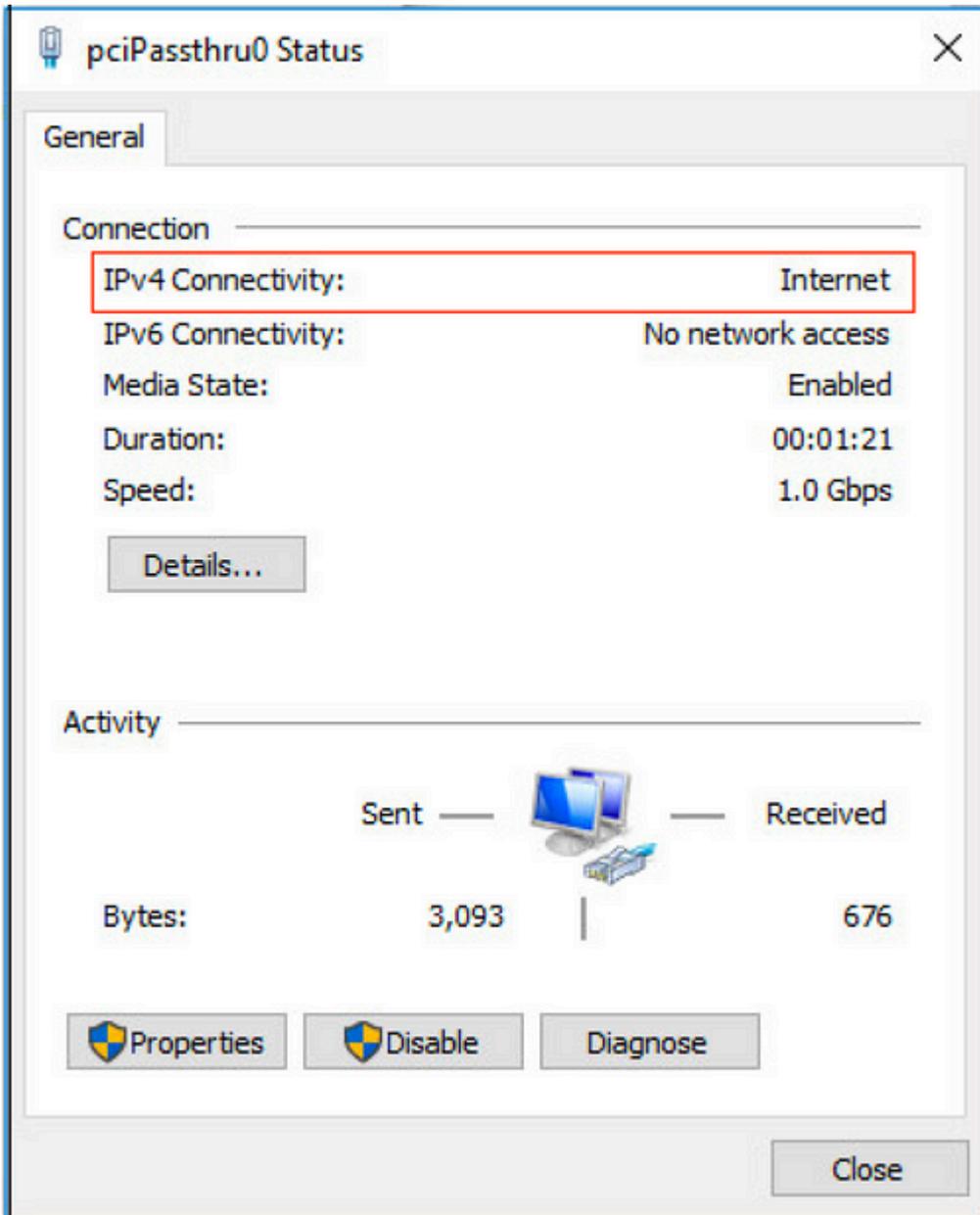
Authentication Policy (2)

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

Authorization Policy (2)

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

Após essa configuração, podemos autenticar o endpoint usando o protocolo EAP-TLS na fonte de identidade LDAPS.



Verificar

1. Verifique a sessão de autenticação na porta do switch conectada ao PC:

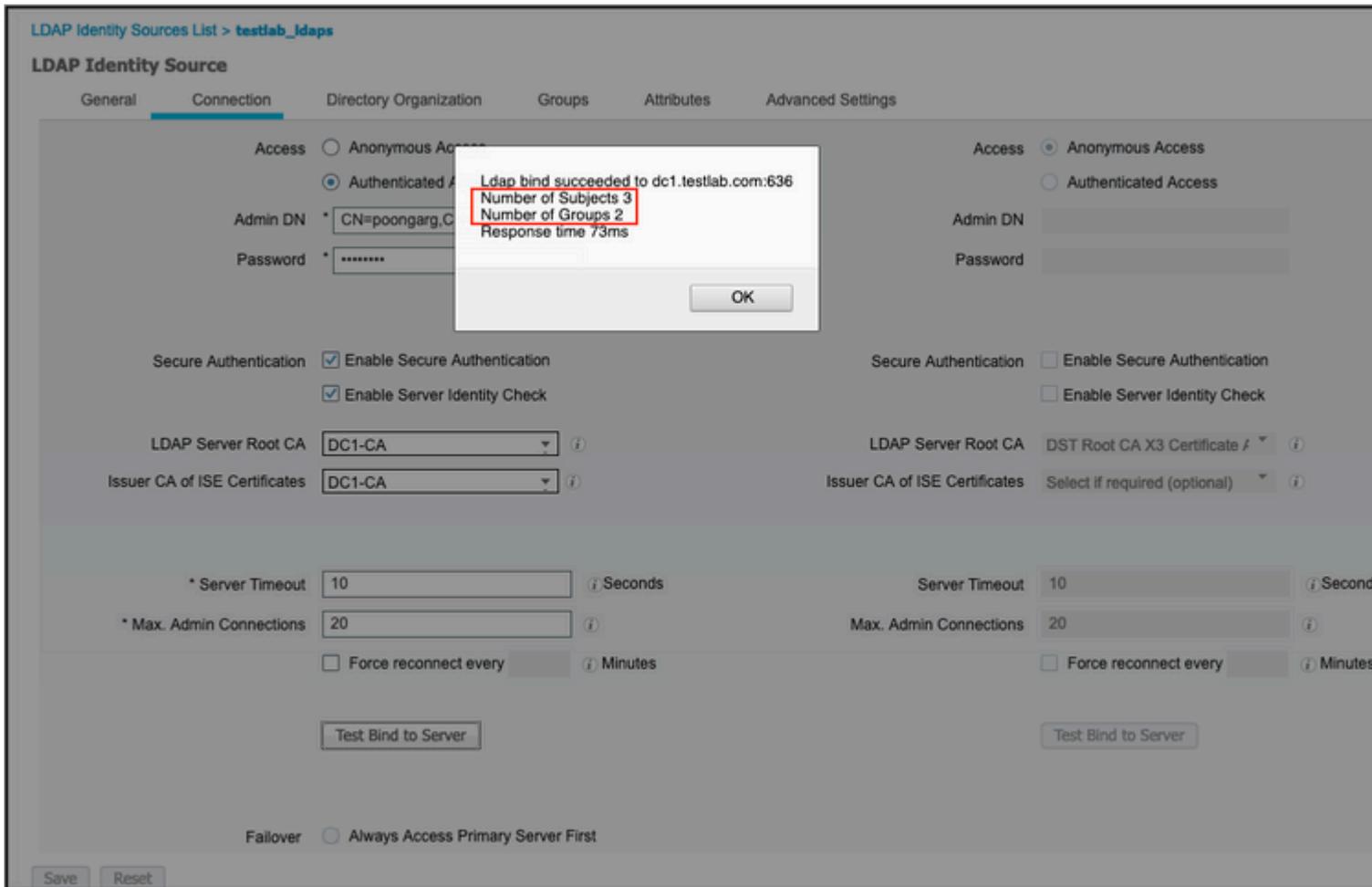
```
SW1#sh auth sessions int g2/0/47 de
  Interface: GigabitEthernet2/0/47
  MAC Address: b496.9126.dec0
  IPv6 Address: Unknown
  IPv4 Address: 10.106.38.165
  User-Name: user1
  Status: Authorized
  Domain: DATA
  Oper host mode: single-host
  Oper control dir: both
  Session timeout: N/A
  Restart 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 as configurações de LDAPS e ISE, você pode recuperar os assuntos e grupos com uma conexão de teste com o servidor:



3. Verifique o relatório de autenticação do usuário:

Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...
Jun 24, 2020 04:45:21.727 AM	i		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	✓		user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess

4. Verifique o relatório de autenticação detalhado do ponto final:

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 se os dados estão criptografados entre o ISE e o servidor LDAPS, fazendo a captura de pacotes no ISE para o 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 SA...
21	2020-06-24 10:40:24.206505	10.197.164.21	10.197.164.22	TCP	74	00:50:56:a0:3e:7f,0...		636 → 28057 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 M...
22	2020-06-24 10:40:24.206613	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval...
23	2020-06-24 10:40:24.206961	10.197.164.22	10.197.164.21	TLSv1.2	207	00:0c:29:98:ca:28,0...		Client Hello
24	2020-06-24 10:40:24.210413	10.197.164.21	10.197.164.22	TLSv1.2	2036	00:50:56:a0:3e:7f,0...		Server Hello, Certificate[Packet size limited durin...
25	2020-06-24 10:40:24.210508	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=142 Ack=1971 Win=33152 Len=0
26	2020-06-24 10:40:24.215211	10.197.164.22	10.197.164.21	TLSv1.2	260	00:0c:29:98:ca:28,0...		Certificate, Client Key Exchange, Change Cipher Spe...
27	2020-06-24 10:40:24.218678	10.197.164.21	10.197.164.22	TLSv1.2	173	00:50:56:a0:3e:7f,0...		Change Cipher Spec, Encrypted Handshake Message
28	2020-06-24 10:40:24.219113	10.197.164.22	10.197.164.21	TLSv1.2	199	00:0c:29:98:ca:28,0...		Application Data
29	2020-06-24 10:40:24.230384	10.197.164.21	10.197.164.22	TLSv1.2	167	00:50:56:a0:3e:7f,0...		Application Data
30	2020-06-24 10:40:24.231712	10.197.164.22	10.197.164.21	TLSv1.2	279	00:0c:29:98:ca:28,0...		Application Data
31	2020-06-24 10:40:24.238889	10.197.164.21	10.197.164.22	TLSv1.2	1879	00:50:56:a0:3e:7f,0...		Application Data[Packet size limited during capture...
32	2020-06-24 10:40:24.238958	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=682 Ack=3992 Win=36864 Len=0
33	2020-06-24 10:40:24.251944	10.197.164.22	10.197.164.21	TLSv1.2	263	00:0c:29:98:ca:28,0...		Application Data
34	2020-06-24 10:40:24.253658	10.197.164.21	10.197.164.22	TLSv1.2	295	00:50:56:a0:3e:7f,0...		Application Data
35	2020-06-24 10:40:24.293322	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=879 Ack=4221 Win=39680 Len=0
86	2020-06-24 10:40:57.946553	10.197.164.22	10.197.164.21	TLSv1.2	151	00:0c:29:98:ca:28,0...		Application Data
87	2020-06-24 10:40:57.947680	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [FIN, ACK] Seq=964 Ack=4221 Win=39680 L...

```

▶ Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
▶ Ethernet II, Src: Vmware_a0:3e:7f (00:50:56:a0:3e:7f), Dst: Vmware_98:ca:28 (00:0c:29:98:ca:28)
▶ Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21
▼ Transmission Control Protocol, Src Port: 28057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133
  Source Port: 28057
  Destination Port: 636
  [Stream index: 2]
  [TCP Segment Len: 133]
  Sequence number: 336 (relative sequence number)
  [Next sequence number: 469 (relative sequence number)]
  Acknowledgment number: 2078 (relative ack number)
  1000 ... = Header Length: 32 bytes (8)
  ▶ Flags: 0x018 (PSH, ACK)
  Window size value: 259
  [Calculated window size: 33152]
  [Window size scaling factor: 128]
  Checksum: 0x5e61 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
  ▶ [Timestamps]
  TCP payload (133 bytes)
  Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Application Data Protocol: ldap
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 128
    Encrypted Application Data: 173d1b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84...

```

Encrypted Data

Troubleshooting

Esta seção descreve alguns erros comuns encontrados com essa configuração e como solucioná-los.

- No relatório de autenticação, você pode ver esta mensagem de erro:

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

Esta mensagem de erro indica que o método selecionado não é suportado pelo LDAP. Verifique se o protocolo de autenticação no mesmo relatório mostra um dos métodos suportados (EAP-GTC, EAP-TLS ou PEAP-TLS).

- O teste de ligação ao servidor terminou com um erro.

Geralmente, isso se deve a uma falha na verificação de validação de certificado do servidor LDAPS. Para solucionar esses tipos de problemas, capture um pacote no ISE e ative todos os três componentes de tempo de execução e prt-jni no nível de depuração, recrie o problema e verifique o arquivo prrt-server.log.

A captura de pacotes reclama de um certificado incorreto e o servidor de porta mostra:

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

Observação: o nome do host na página LDAP deve ser configurado com o nome do assunto do certificado (ou qualquer um dos Nomes Alternativos do Assunto). Portanto, a menos que isso esteja no assunto ou na SAN, isso não funcionará, o certificado com o endereço IP na lista de SANs será necessário.

3. No relatório de autenticação, você pode observar que o assunto não foi encontrado no armazenamento de identidade. Isso significa que o nome de usuário do relatório não corresponde ao atributo de nome do assunto de nenhum usuário no banco de dados LDAP. Nesse cenário, o valor foi definido como sAMAccountName para esse atributo, o que significa que o ISE procura os valores de sAMAccountName para o usuário LDAP quando ele tenta encontrar uma correspondência.

4. Não foi possível recuperar corretamente os assuntos e grupos durante um teste de ligação com o servidor. A causa mais provável desse problema é uma configuração incorreta das bases de pesquisa. Lembre-se de que a hierarquia LDAP deve ser especificada de folha para raiz e dc (pode consistir em várias palavras).

Informações Relacionadas

- <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>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.