

Configurar e solucionar problemas do ISE com o Repositório de identidade LDAPS externo

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar LDAPS no Ative Directory](#)

[Instalar certificado de identidade no controlador de domínio](#)

[Acesse a estrutura do diretório LDAPS](#)

[Integre o ISE ao servidor LDAPS](#)

[Configurar o switch](#)

[Configurar o endpoint](#)

[Configurar o conjunto de políticas no ISE](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve a integração do Cisco Identity Service Engine (ISE) com o servidor Secure Lightweight Directory Access Protocol (LDAPS) como uma fonte de identidade externa. O LDAPS permite a criptografia de dados LDAP (que inclui credenciais de usuário) em trânsito quando uma associação de diretório é estabelecida. O LDAPS usa a porta TCP 636.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da administração do ISE
- Conhecimento básico do Ative Directory/LDAP

Componentes Utilizados

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

- Patch 7 do Cisco ISE 2.6
- Microsoft Windows versão 2012 R2 com Serviços LDS do Ative Directory instalados

- Windows 10 OS PC com suplicante nativo e certificado de usuário instalado
- Switch Cisco C3750X com imagem 152-2.E6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Esses protocolos de autenticação são suportados com LDAPS:

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

Note: EAP-MSCHAPV2 (como um método interno de PEAP, EAP-FAST ou EAP-TTLS), LEAP, CHAP e EAP-MD5 não são suportados com LDAPS External Identity Source.

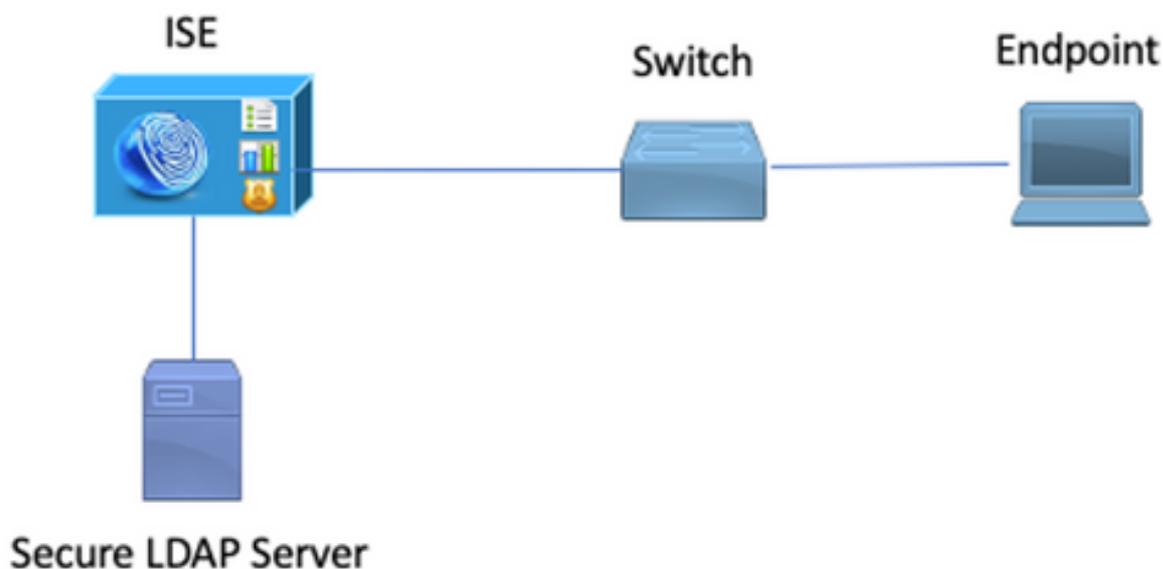
Configurar

Esta seção descreve a configuração dos dispositivos de rede e a integração do ISE com o servidor LDAPS 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 do switch conectado está configurada para autenticação 802.1x para autenticar os usuários com ISE. No ISE, o LDAPS é configurado como um repositório de identidade externo.

Esta imagem ilustra a topologia de rede usada:

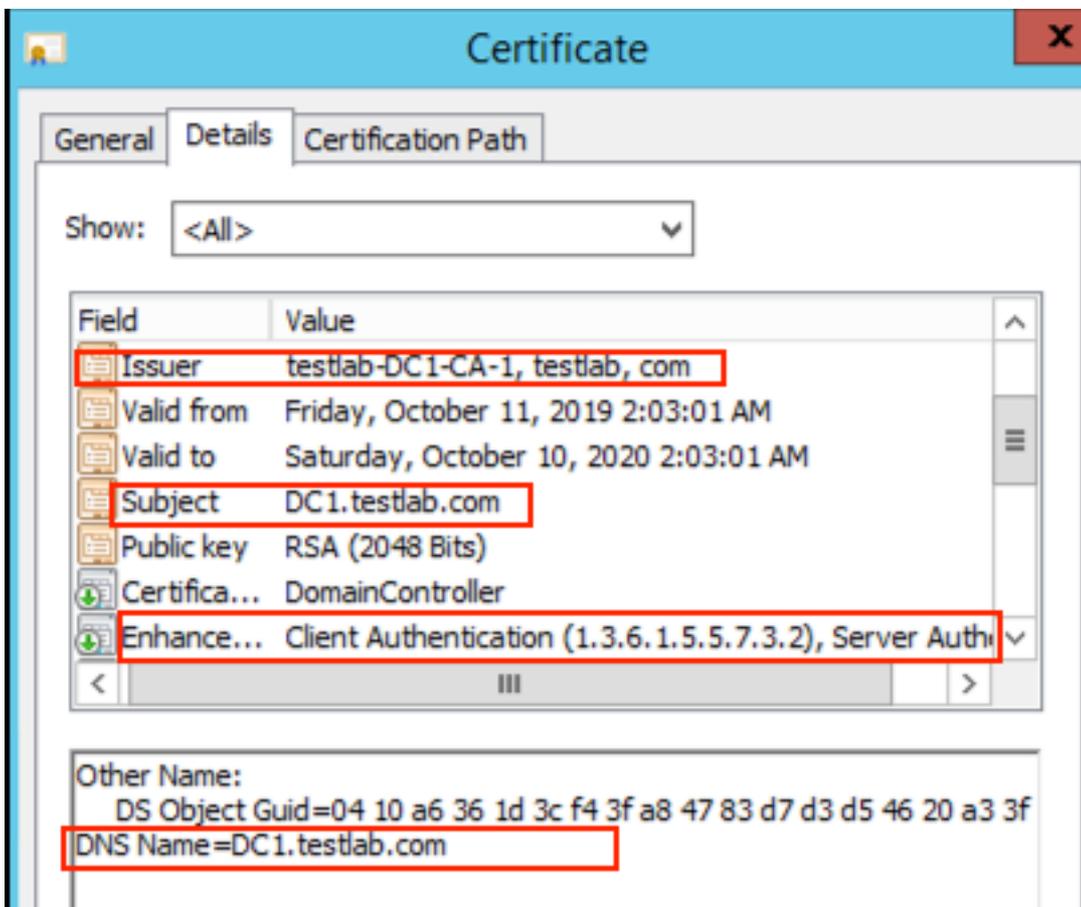


Configurar LDAPS no Ative Directory

Instalar certificado de identidade no controlador de domínio

Para habilitar o LDAPS, instale um certificado no controlador de domínio (DC) 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 armazenamento do Controlador de Domínio e está corretamente associada ao certificado.
3. A extensão Enhanced Key Usage inclui o identificador de objeto da Autenticação de servidor (1.3.6.1.5.5.7.3.1) (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 autoridade de certificação (CA) confiável pelo controlador de domínio e pelos clientes LDAPS. Para uma comunicação segura confiável, o cliente e o servidor devem confiar na AC raiz um do outro e nos certificados CA intermediários que lhes emitiram certificados.
6. O provedor de serviços de criptografia Schannel (CSP) deve ser usado para gerar a chave.



Acesse a estrutura do diretório LDAPS

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

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



2. Para simplificar, crie uma unidade organizacional (OU) chamada **ISE OU** no AD e deve ter um grupo chamado **UserGroup**. Crie dois usuários (**user1** e **user2**) e torne-os membros do grupo **UserGroup**.

Note: A origem de identidade LDAP no ISE é usada somente para autenticação de usuário.

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 Attribute

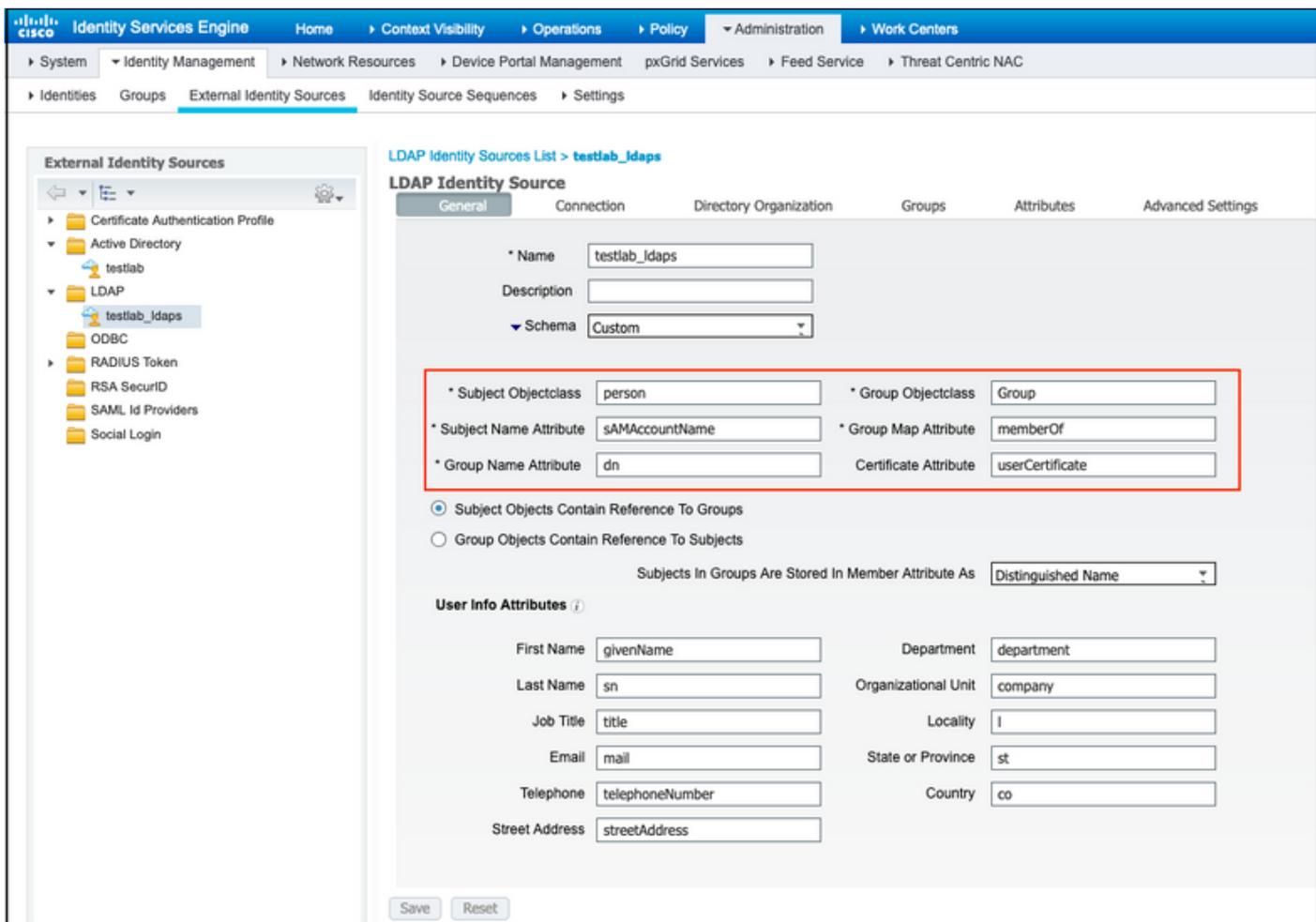
Integre o ISE ao servidor LDAPS

1. Importar o certificado CA raiz do servidor LDAP no certificado confiável.

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 o certificado de administração do ISE e assegure-se de que o certificado de emissor do certificado de administração do ISE também esteja presente no Repositório de Certificados Confiáveis.

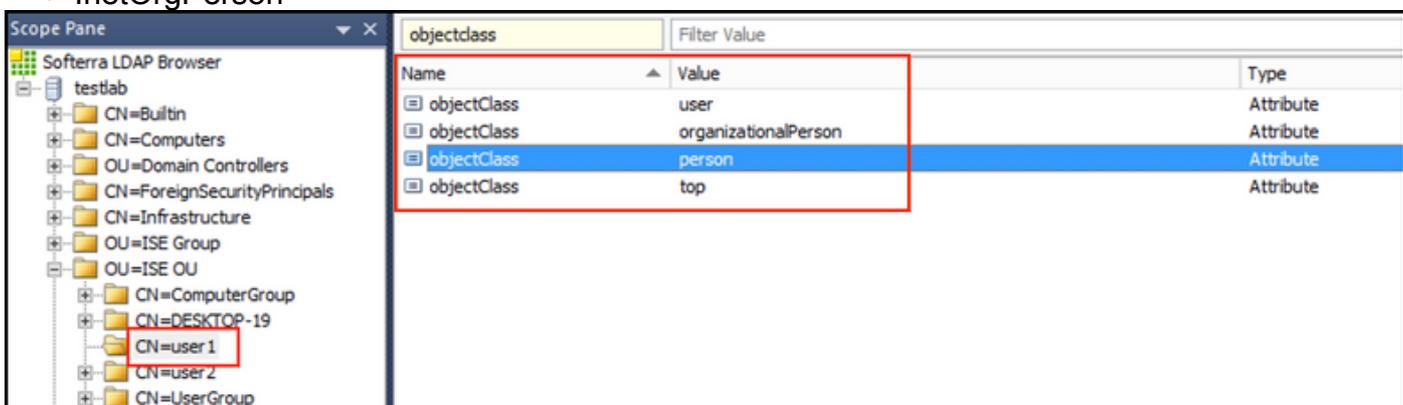
3. Para integrar o servidor LDAPS, use os diferentes atributos LDAP do diretório LDAPS. Navegue até **Administração > Gerenciamento de identidade > Fontes de identidade externas > Fontes de identidade LDAP > Adicionar**.



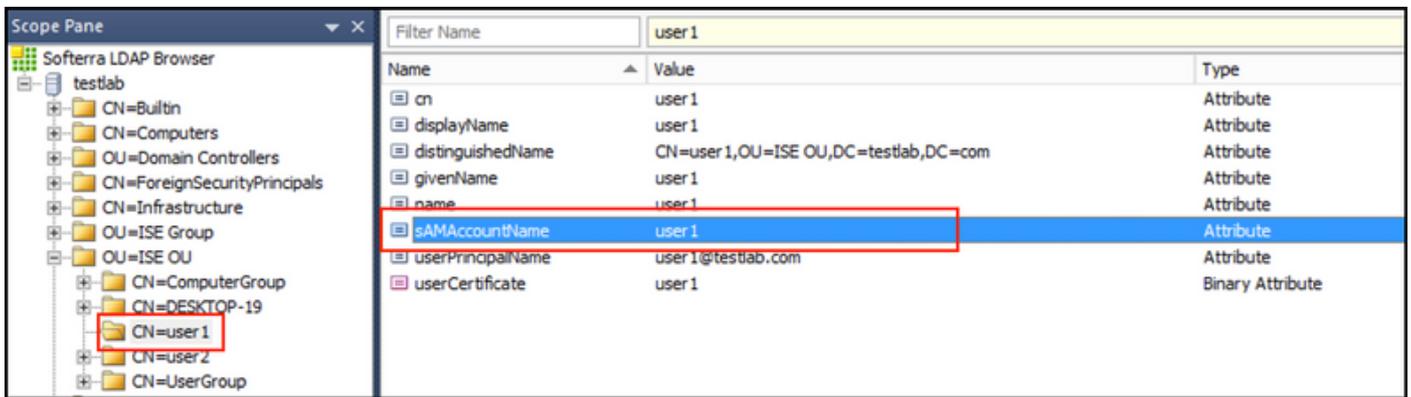
4. Configure estes atributos na **guia Geral**:

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

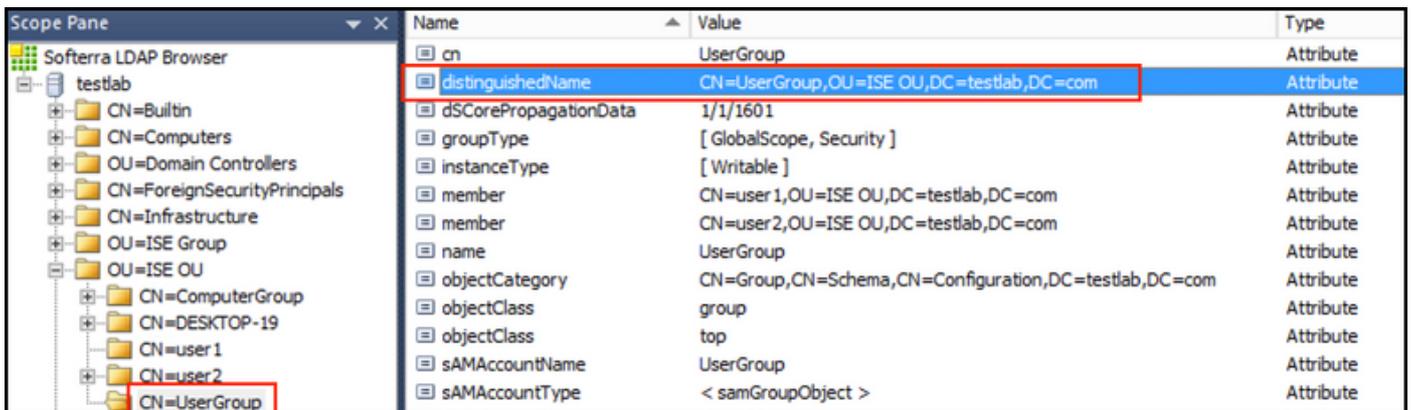
- Superior
- Pessoa
- PessoaOrganizacional
- InetOrgPerson



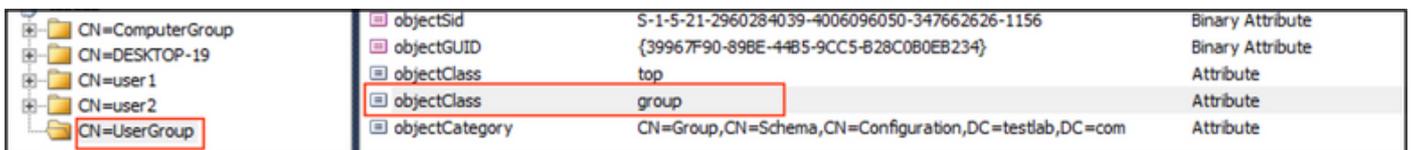
Atributo do nome do assunto: este campo é o nome do atributo que contém o nome de usuário da solicitação. Este atributo é recuperado do LDAPS quando o ISE pergunta um nome de usuário específico no banco de dados LDAP (você pode usar cn, sAMAccountName etc.). Nesse cenário, é usado o nome de usuário user1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



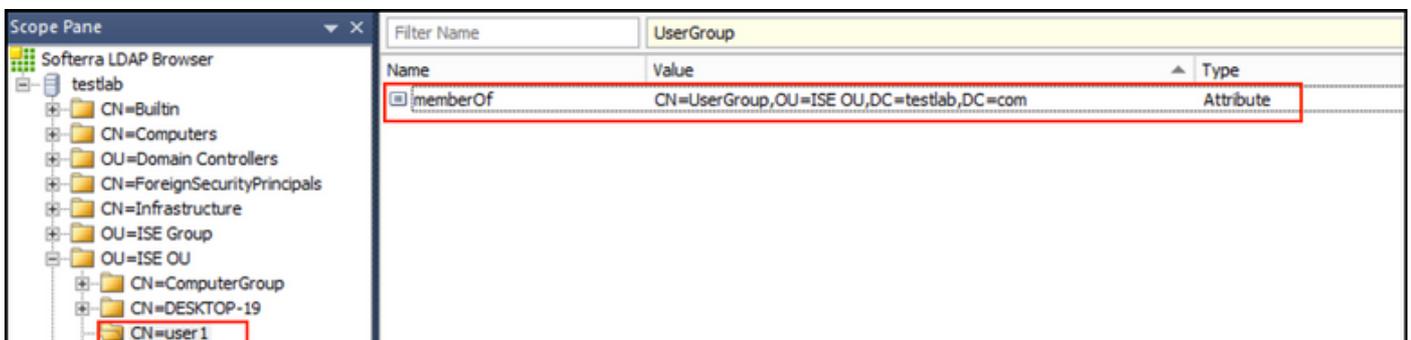
Atributo do nome do grupo: Este é o atributo que contém o nome de um grupo. Os valores dos **atributos do nome do grupo** no diretório LDAP devem corresponder aos nomes dos grupos LDAP na página **Grupos de usuários**



Classe de objeto do grupo: esse valor é usado em pesquisas para especificar os objetos reconhecidos como grupos.



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



Atributo do certificado: Insira o atributo que contém as definições do certificado. Opcionalmente, essas definições podem ser usadas 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 executada entre o certificado do cliente e o certificado recuperado da origem da identidade LDAP.



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

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

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,DC=com	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. Execute **dsquery** no controlador de domínio para obter o nome de usuário DN a ser usado para fazer uma conexão com o servidor LDAP:

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

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

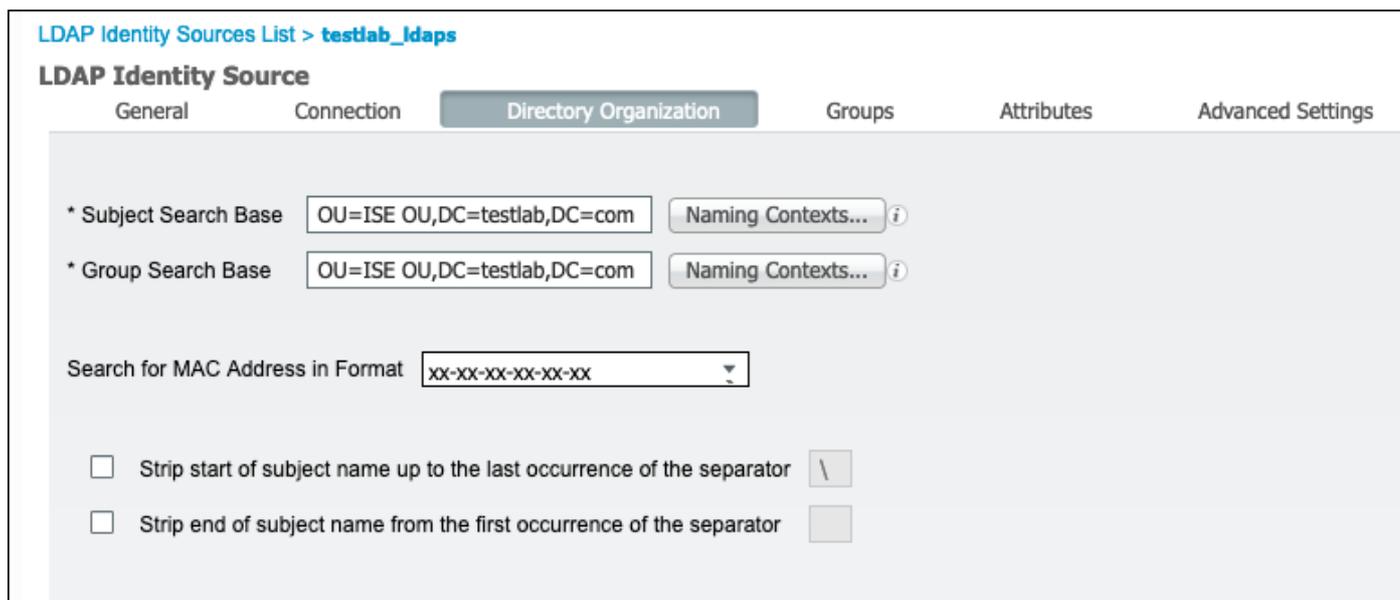
Etapa 2. Ativar a opção Autenticação segura e Verificação de identidade do servidor.

Etapa 3. No menu suspenso, selecione o certificado LDAP Server Root CA e certificado de

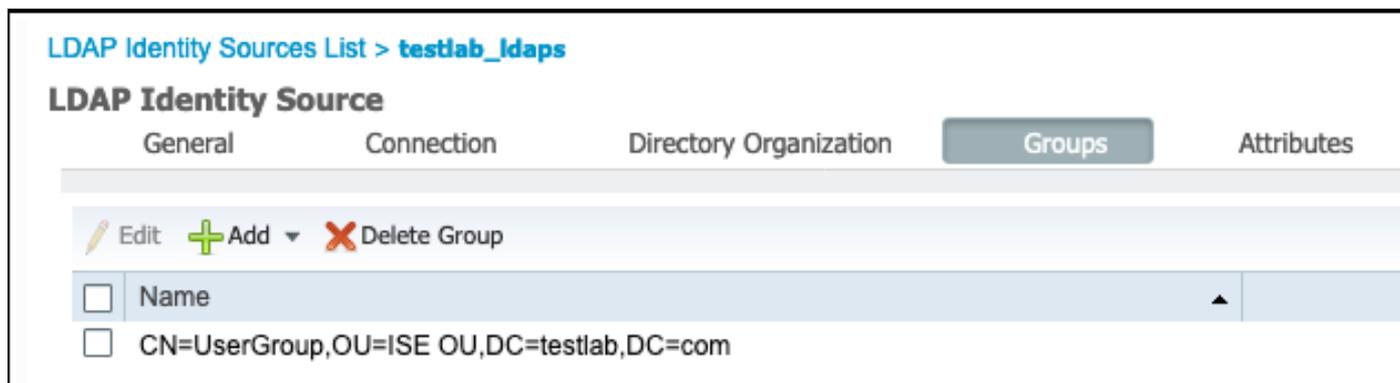
administrador ISE Isser CA certificado (também usamos autoridade de certificado, instalada no mesmo servidor LDAP para emitir o certificado de administrador ISE),

Etapa 4. Selecione o **Test Bind to server**. Nesse 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 Assunto/Grupo. É o **ponto de junção** do ISE para o LDAP. Agora, você pode recuperar apenas os assuntos e grupos que são filhos do ponto de união. Neste cenário, o assunto e o grupo são recuperados da **OU=ISE OU**



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 autenticação 802.1x. O PC Windows está conectado à porta do switch Gig2/0/47

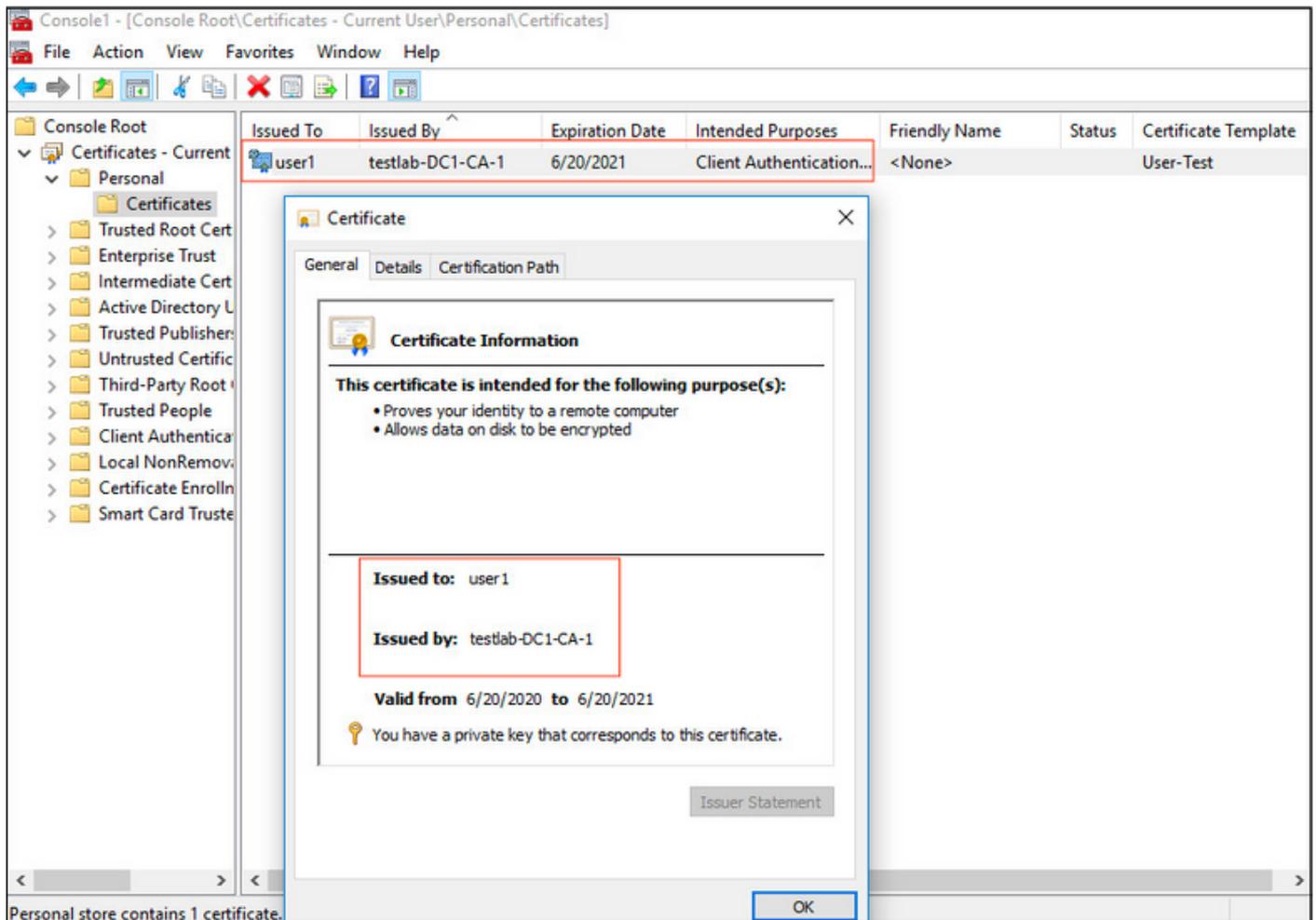
```
aaa new-model
radius server ISE address ipv4 x.x.x.x auth-port 1812 acct-port 1813 key xxxxxx
aaa group server radius ISE_SERVERS server name ISE !
aaa server radius dynamic-author client x.x.x.x server-key xxxxxx !
aaa authentication dot1x default group ISE_SERVERS local aaa
authorization network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

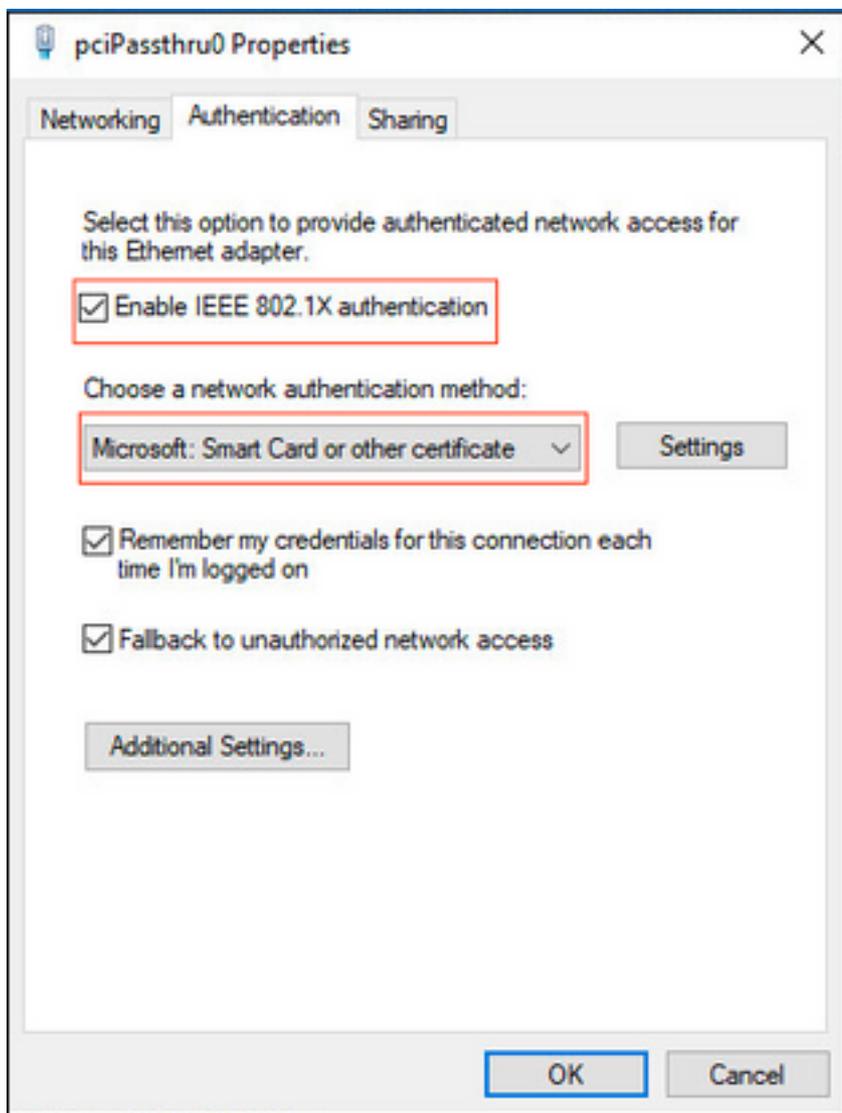
Configurar o endpoint

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

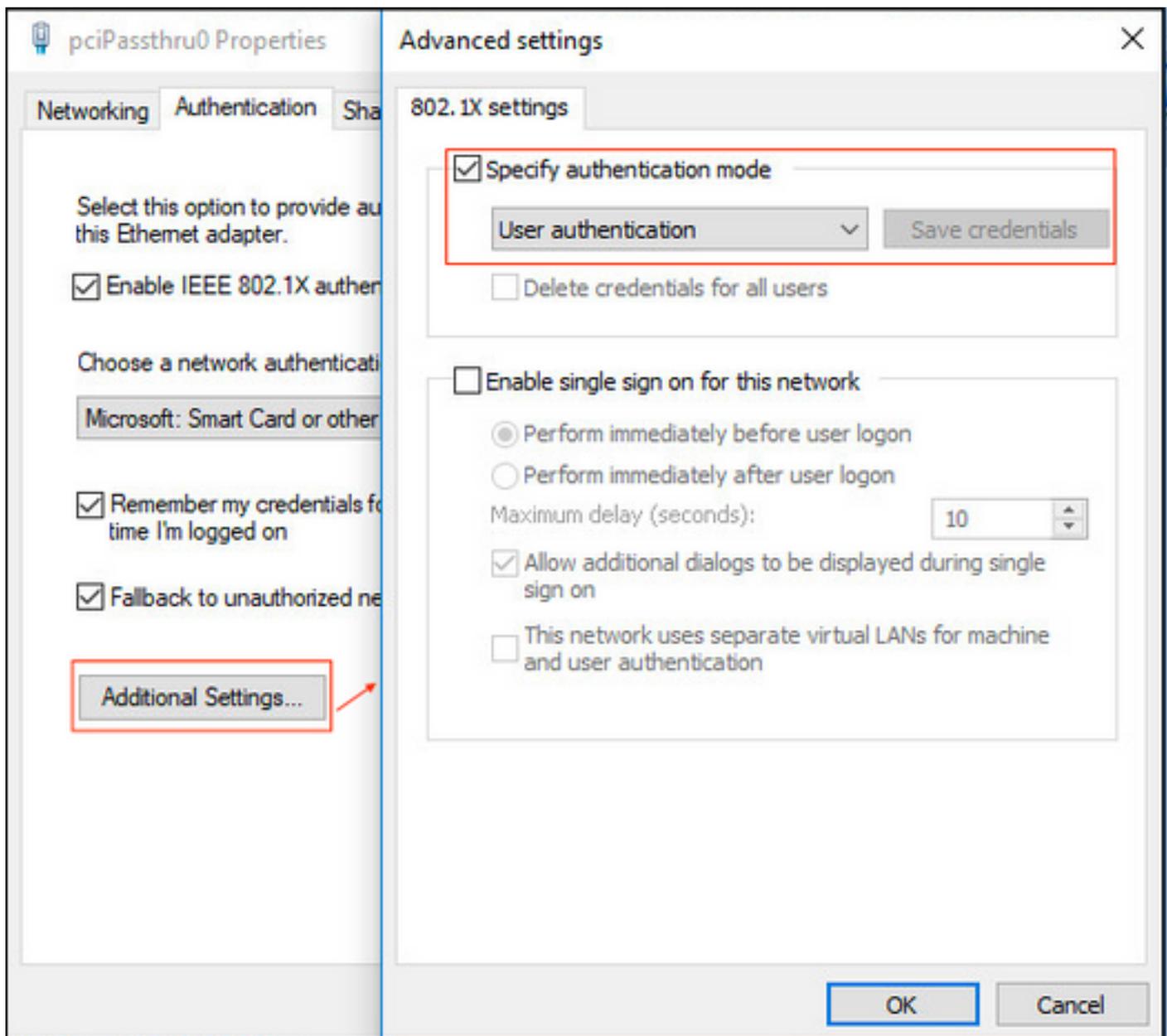
1. Certifique-se de que o PC esteja equipado com certificado de usuário (para usuário1) e tenha uma finalidade específica como Autenticação de cliente e, nas Autoridades de Certificação de Raiz Confiável, a cadeia de certificados do emissor está presente no PC.



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 **Additional Settings (Configurações adicionais)**, uma janela será aberta, marque a caixa com **especificar modo de autenticação** e escolha **User authentication**, como mostrado nesta imagem.



Configurar o conjunto de políticas no ISE

Como o protocolo EAP-TLS é usado, antes que o Conjunto de políticas seja configurado, o [Perfil de autenticação do certificado](#) precisa ser configurado e a sequência de origem da identidade será usada posteriormente na política de autenticação.

The screenshot displays the Cisco Identity Services Engine (ISE) administration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The breadcrumb trail shows 'System' > 'Identity Management' > 'Network Resources' > 'Device Portal Management' > 'pxGrid Services' > 'Feed Service' > 'Threat Centric NAC'. The main menu includes 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The left sidebar, titled 'External Identity Sources', shows a tree view 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' is 'LDAPS_cert'; 'Description' is 'EAP-TLS certificate based authentication with LDAPS'; 'Identity Store' is 'testlab_ldaps'; 'Use Identity From' is set to 'Certificate Attribute' with a dropdown menu showing 'Subject - Common Name'; 'Match Client Certificate Against Certificate in Identity Store' is set to 'Always perform binary comparison'. 'Save' and 'Reset' buttons are at the bottom.

Consulte o Perfil de Autenticação de Certificado na Sequência de Origem da Identidade e defina a origem de identidade externa LDAPS na lista 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

Agora configure a política definida para a autenticação Wired Dot1x:

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)

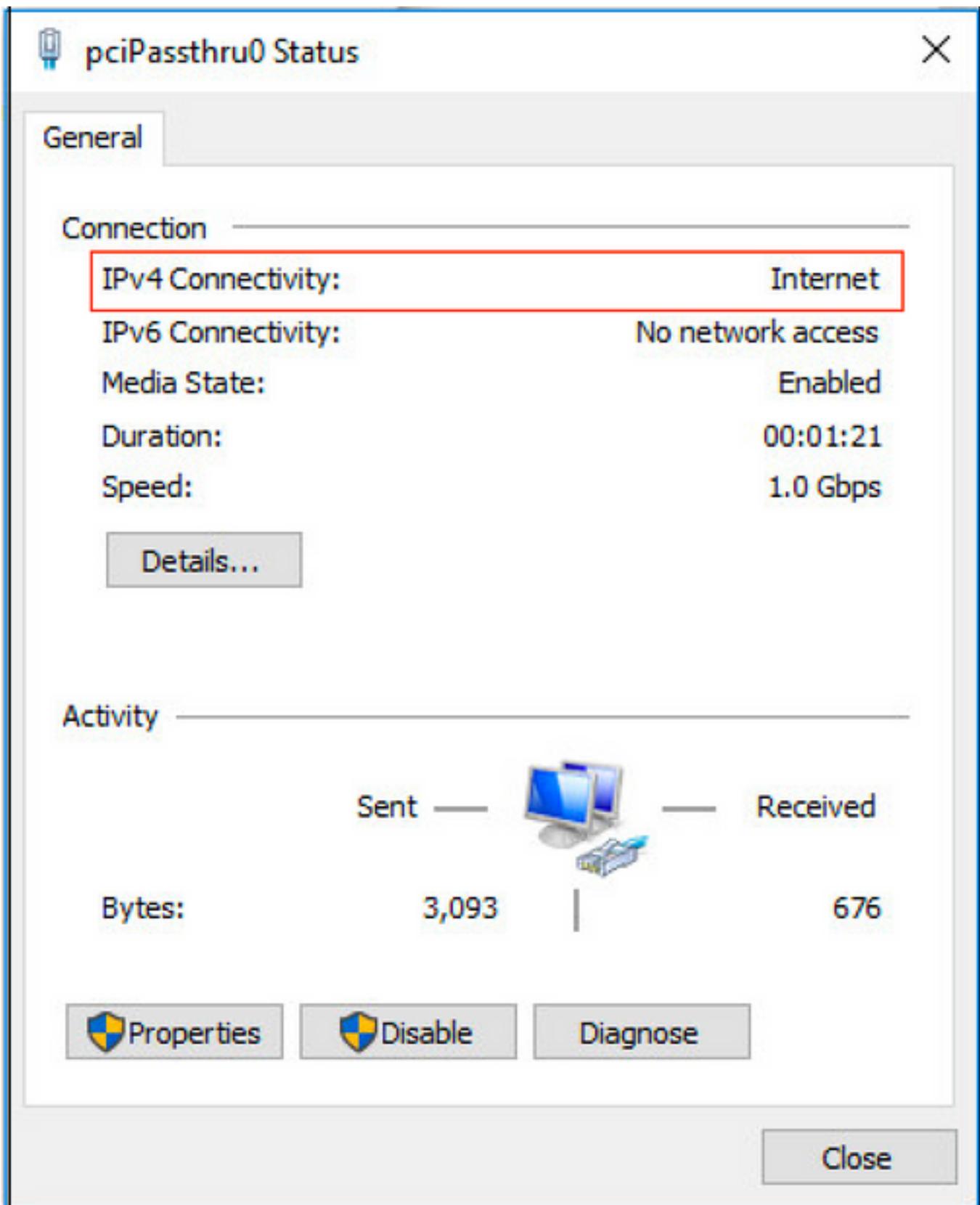
Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch	LDAPS x	223	Options
✔	Default		LDAPS x	0	Options

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

Depois dessa configuração, devemos ser capazes de autenticar o endpoint usando o protocolo EAP-TLS contra a origem da identidade LDAPS.



Verificar

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

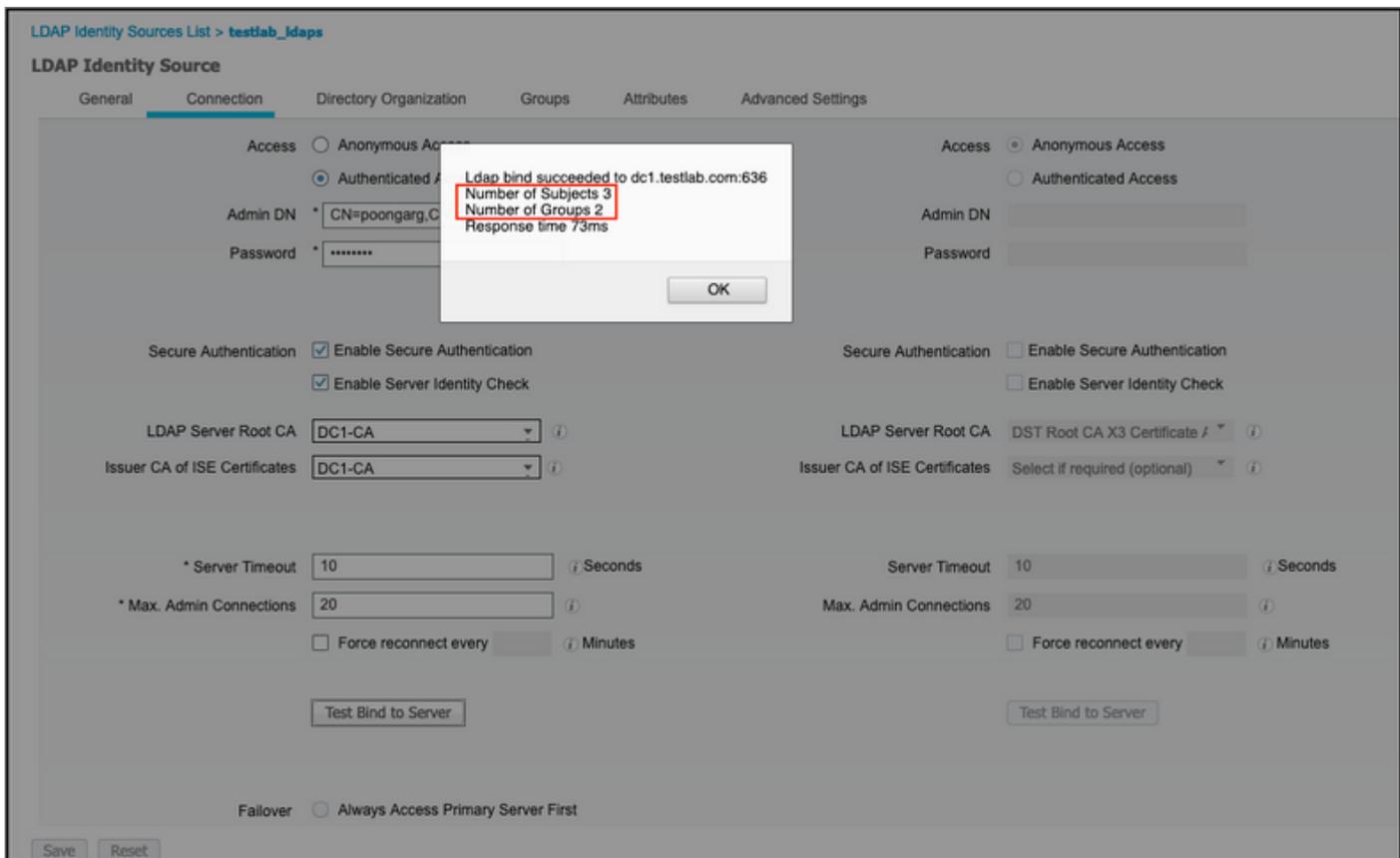
```
SW1#sh auth sessions int g2/0/47 de
      Interface: GigabitEthernet2/0/47
      MAC Address: b496.9126.dec0
      IPv6 Address: Unknown
      IPv4 Address: 10.106.38.165
      User-Name: user1
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      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 participantes e os 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...	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. Verifique o relatório de autenticação detalhado para o 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. Valide se os dados estão criptografados entre o servidor ISE e LDAPS levando 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.		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 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.		28857 - 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=140972873 TSecr=30158962
23	2020-06-24 10:40:24.206613	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	10.197.164.21	10.197.164.22	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 10:40:24.238084	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	10.197.164.22	10.197.164.21	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	10.197.164.22	10.197.164.21	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_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: 28857, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133
 Source Port: 28857

Stream 0: 2020-06-24 10:40:24.219113
 [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 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: 173d1b002f280a13cc17815e5447bb9ac8af8a881a9eb84...

→ Encrypted Data

Troubleshoot

Esta seção descreve alguns erros comuns encontrados com esta 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

Essa mensagem de erro indica que o método selecionado não é suportado pelo LDAP. Certifique-se de que o **Protocolo de Autenticação** no mesmo relatório mostra um dos métodos suportados (EAP-GTC, EAP-TLS ou PEAP-TLS).

- A associação de teste ao servidor terminou com um erro.

Mais comumente isso é devido à falha na verificação de validação do certificado do servidor LDAPS. Para solucionar esses tipos de problemas, faça uma captura de pacote no ISE e habilite todos os três componentes de tempo de execução e prrt-jni no nível de depuração, recree o problema e verifique o arquivo **prrt-server.log**.

A captura de pacote reclama sobre certificado defeituoso e o servidor de 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
```

Note: 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 você tenha esse tipo no assunto ou na SAN, ele não funciona, o certificado com o endereço IP na lista da SAN é necessário.

3. No relatório de autenticação, você pode observar que o assunto não foi encontrado no repositório de identidade. Isso significa que o nome de usuário do relatório não corresponde ao **Atributo do nome do assunto** para qualquer usuário no banco de dados LDAP. Neste cenário, o

valor foi definido como **sAMAccountName** para este atributo, o que significa que o ISE procura os valores sAMAccountName para o utilizador LDAP quando tenta encontrar uma correspondência.

4. Os participantes e grupos podem não ser recuperados corretamente durante um teste **de ligação ao servidor**. A causa mais provável desse problema é uma configuração incorreta para as bases de pesquisa. Lembre-se de que a hierarquia LDAP deve ser especificada de leaf-to-root 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>