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

Contents

Introduction

Este documento descreve a integração do Cisco Identity Service Engine (ISE) com o servidor Secure Lightweight Diretory 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 Diretory/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 Diretory 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.

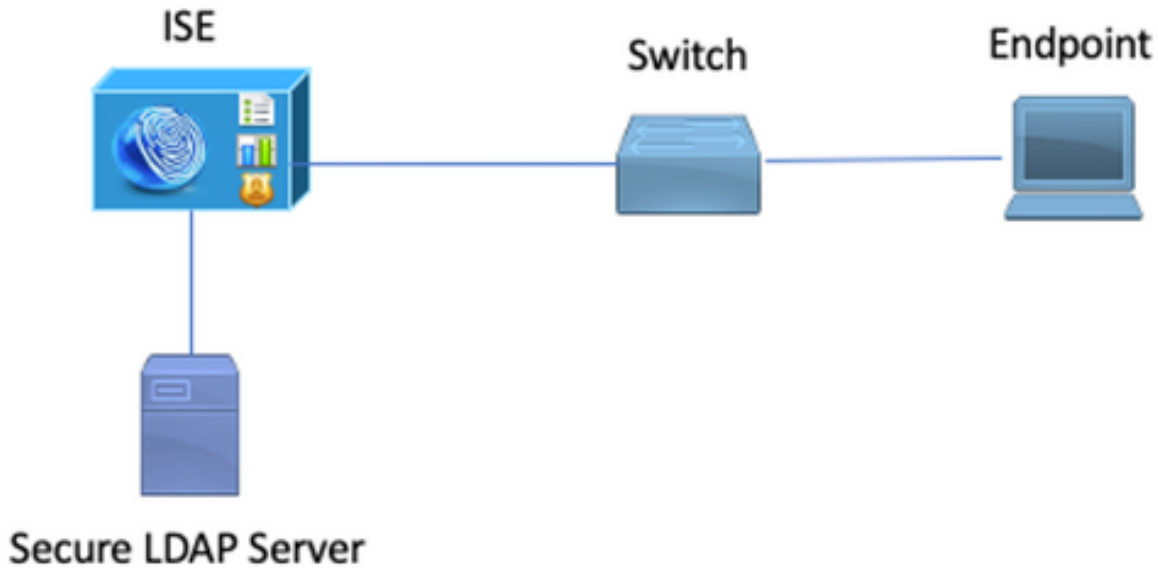
Configurar

Esta seção descreve a configuração dos dispositivos de rede e a integração do ISE com o servidor LDAPS do Microsoft Ative Diretory (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 Diretory

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.

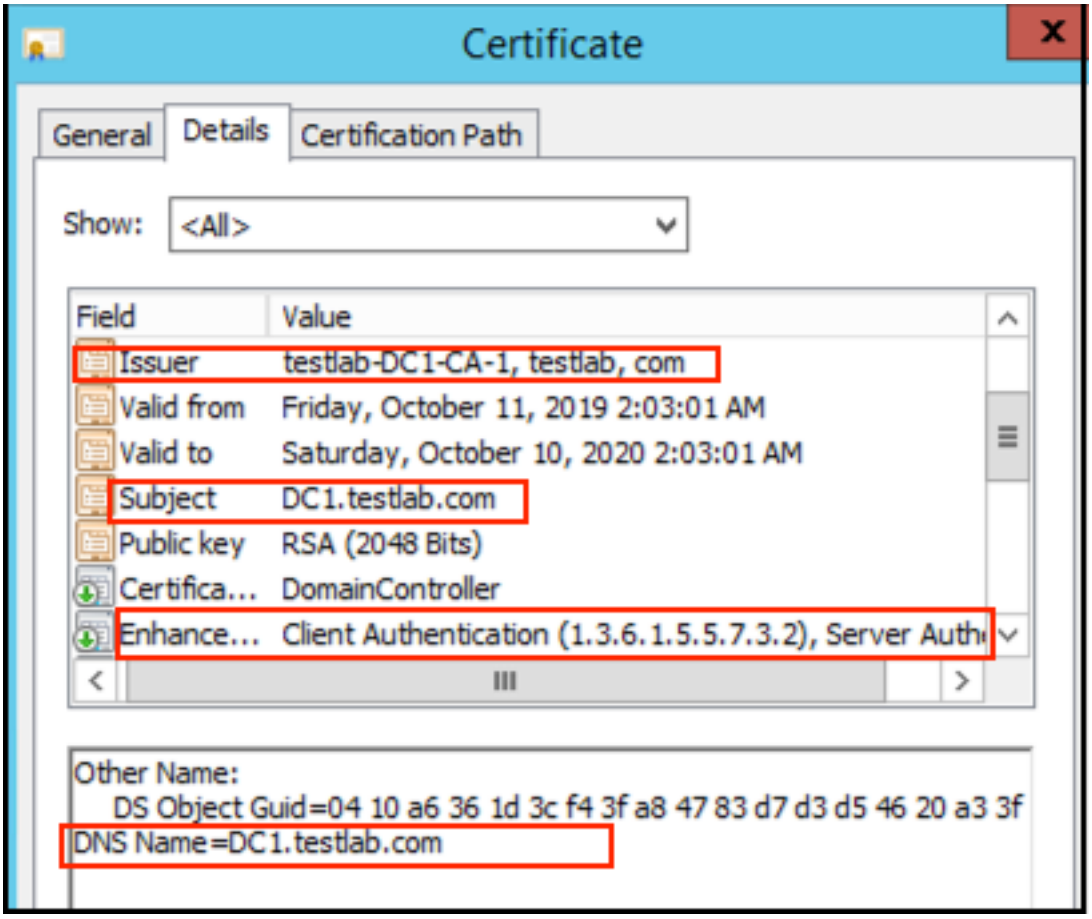
2. Uma chave privada que corresponde ao certificado está presente no armazenamento do Controlador de Domínio e está corretamente associada ao certificado.

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.



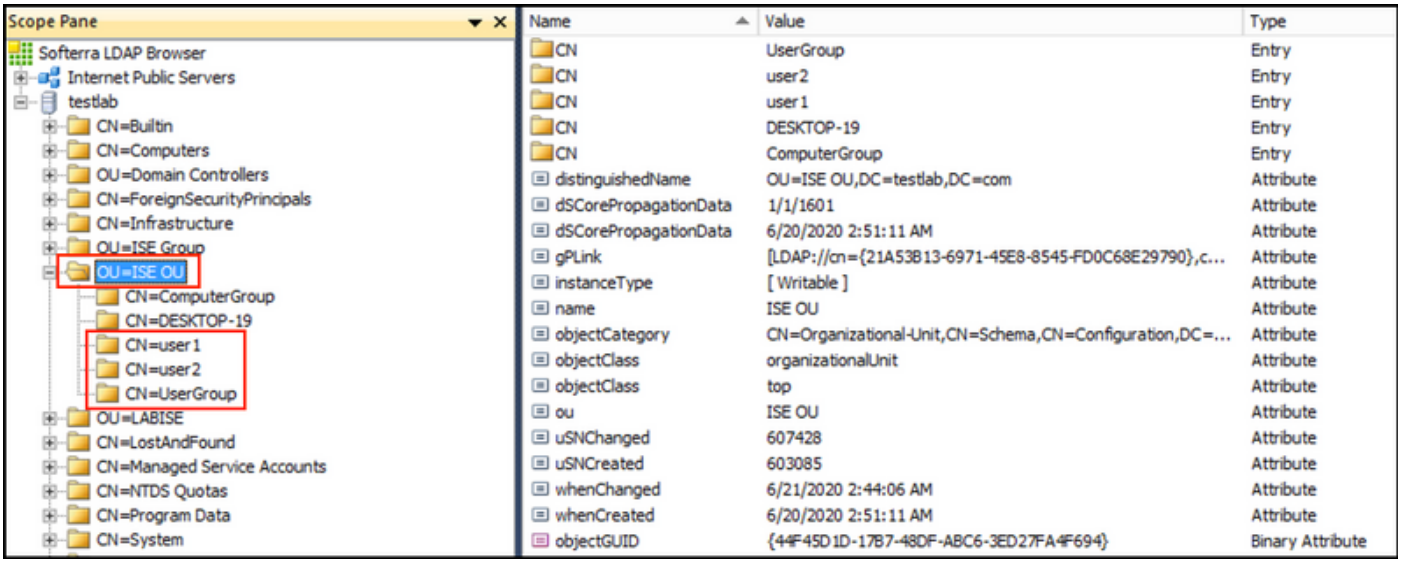
Acesse a estrutura do diretório LDAPS

Para acessar o diretório LDAPS no servidor do Ative Diretory, 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.

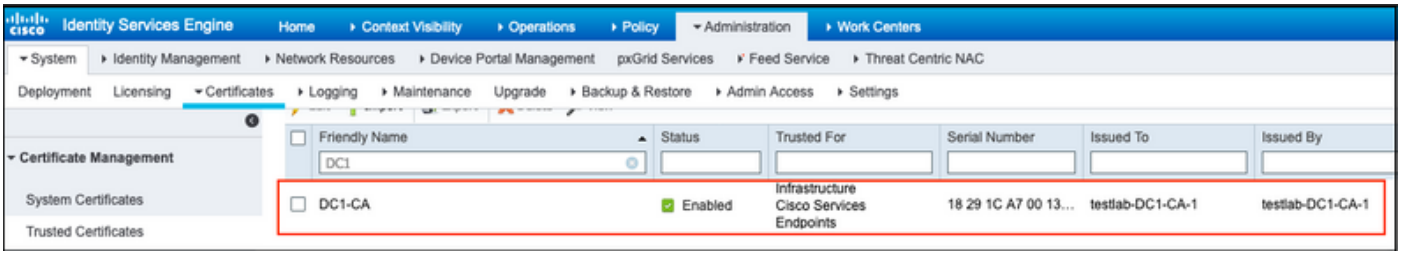
2. Para simplificar, crie uma unidade organizacional (OU) chamada **ISE OU** no AD e deve ter um grupo chamado **UserGroup**. Crie dois usuários (**user1** e **user2**) e torne-os membros do grupo **UserGroup**.

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



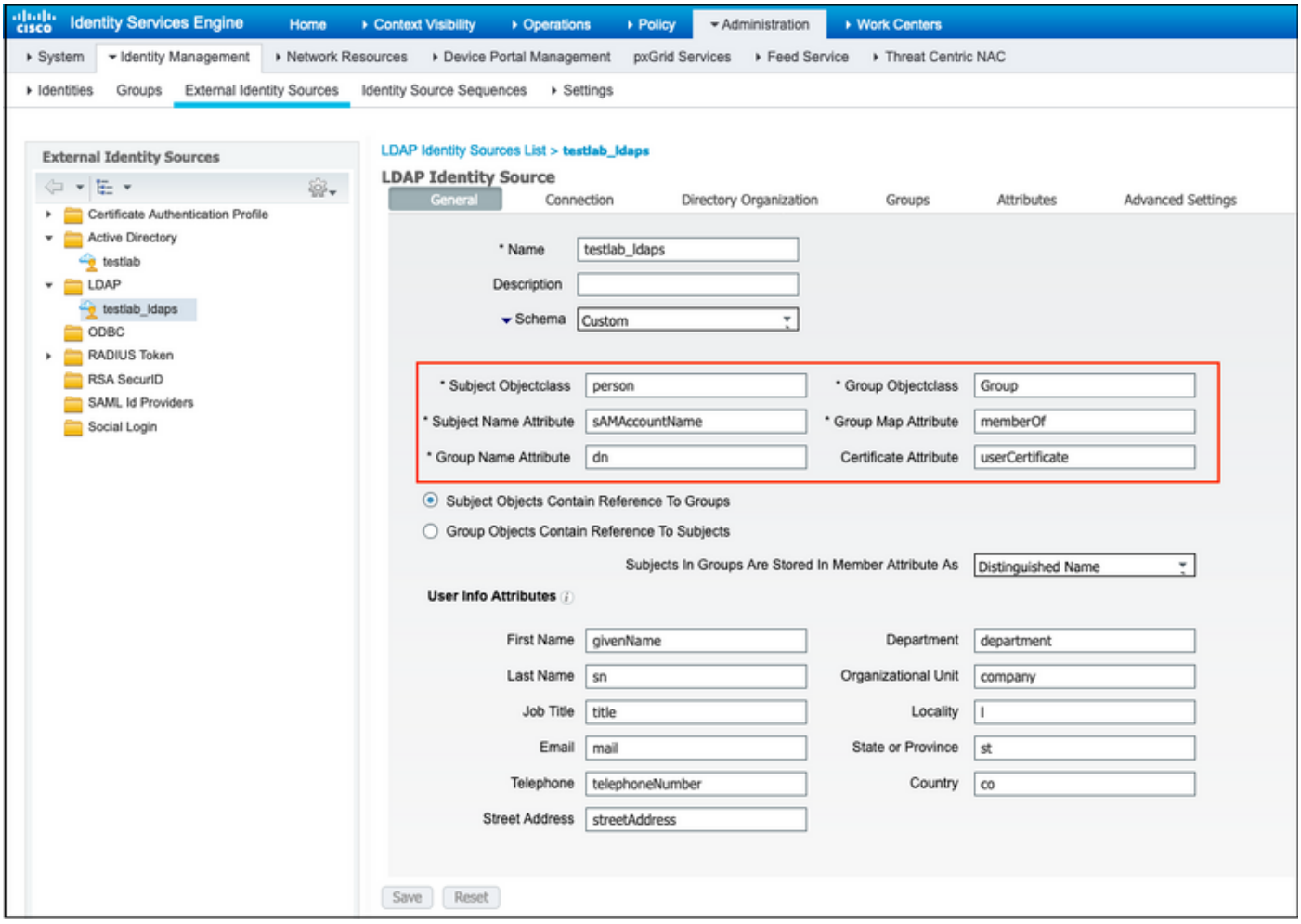
Integre o ISE ao servidor LDAPS

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



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.

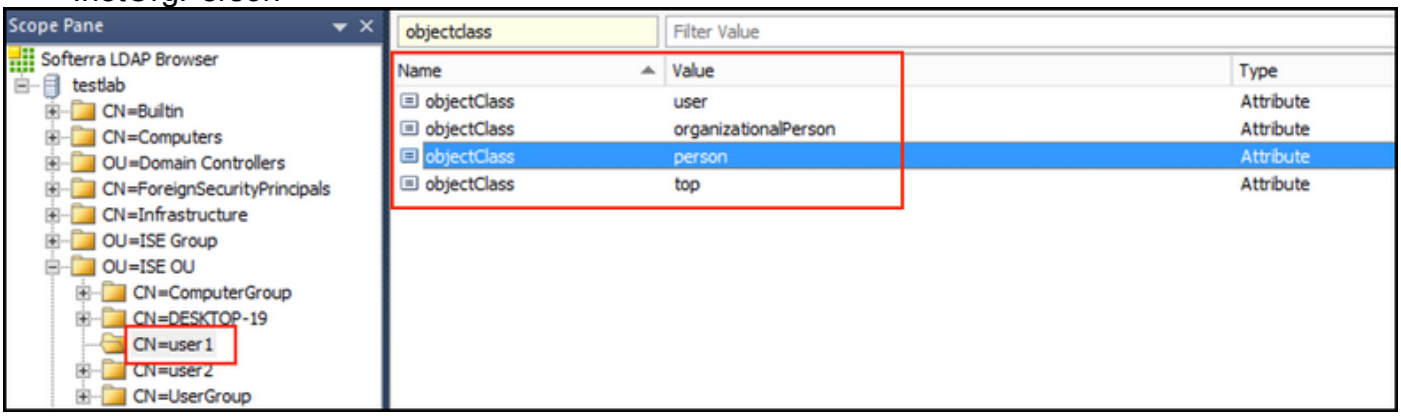
3. Para integrar o servidor LDAPS, use os diferentes atributos LDAP do diretório LDAPS. Navegue até **Administração > Gerenciamento de identidade > Fontes de identidade externas > Fontes de identidade LDAP > Adicionar**.



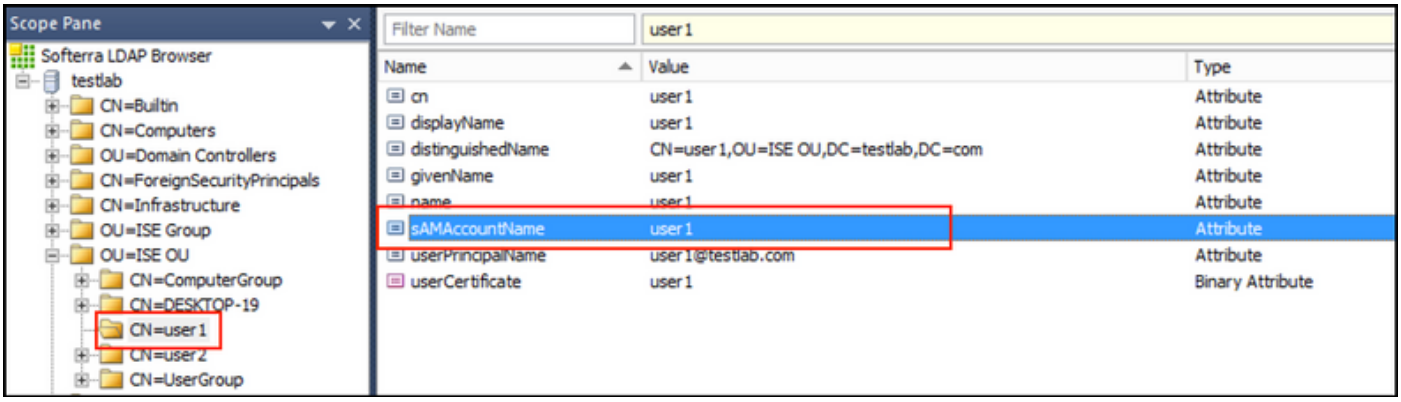
4. Configure estes atributos na **guia Geral**:

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

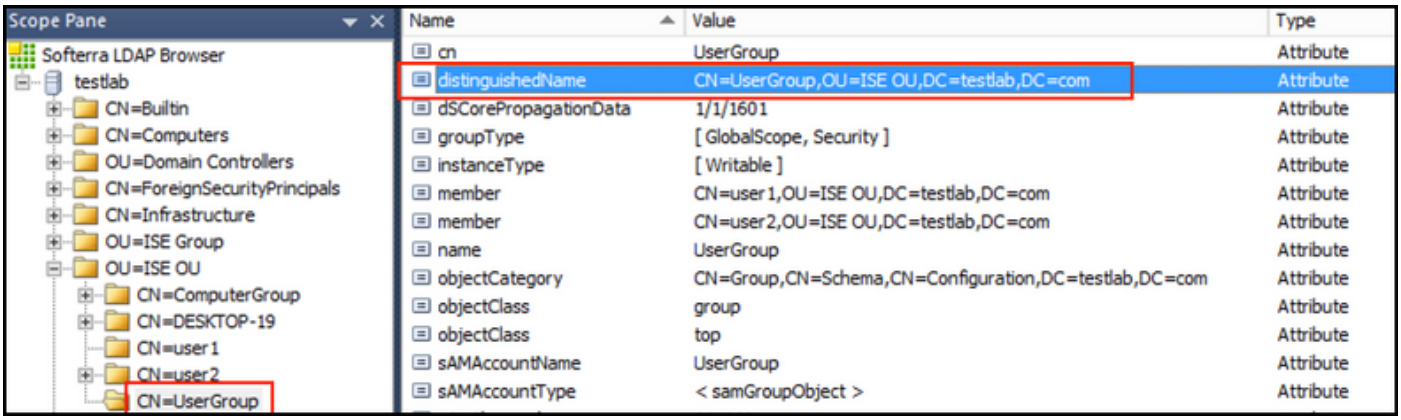
- Superior
- Pessoa
- PessoaOrganizacional
- InetOrgPerson



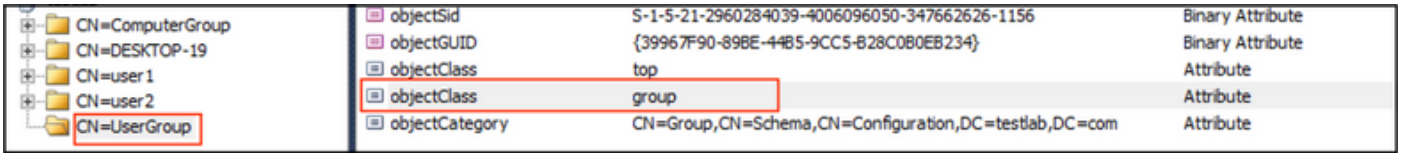
Atributo do nome do assunto: este campo é o nome do atributo que contém o nome de usuário da solicitação. Este atributo é recuperado do LDAPS quando o ISE pergunta um nome de usuário específico no banco de dados LDAP (você pode usar cn, sAMAccountName etc.). Nesse cenário, é usado o nome de usuário user1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



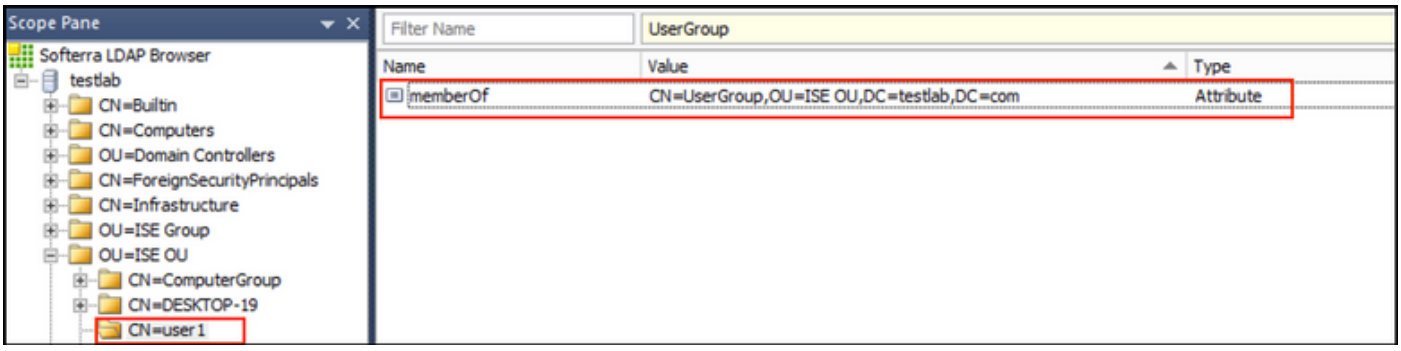
Atributo do nome do grupo: Este é o atributo que contém o nome de um grupo. Os valores dos **atributos do nome do grupo** no diretório LDAP devem corresponder aos nomes dos grupos LDAP na página **Grupos de usuários**



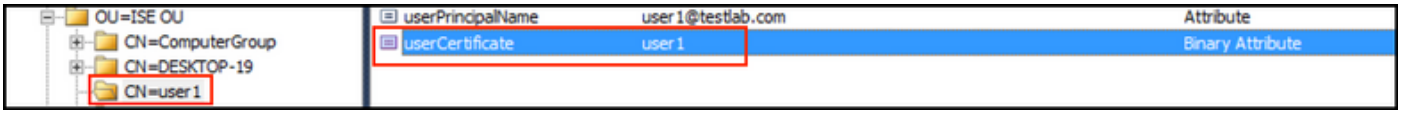
Classe de objeto do grupo: esse valor é usado em pesquisas para especificar os objetos reconhecidos como grupos.



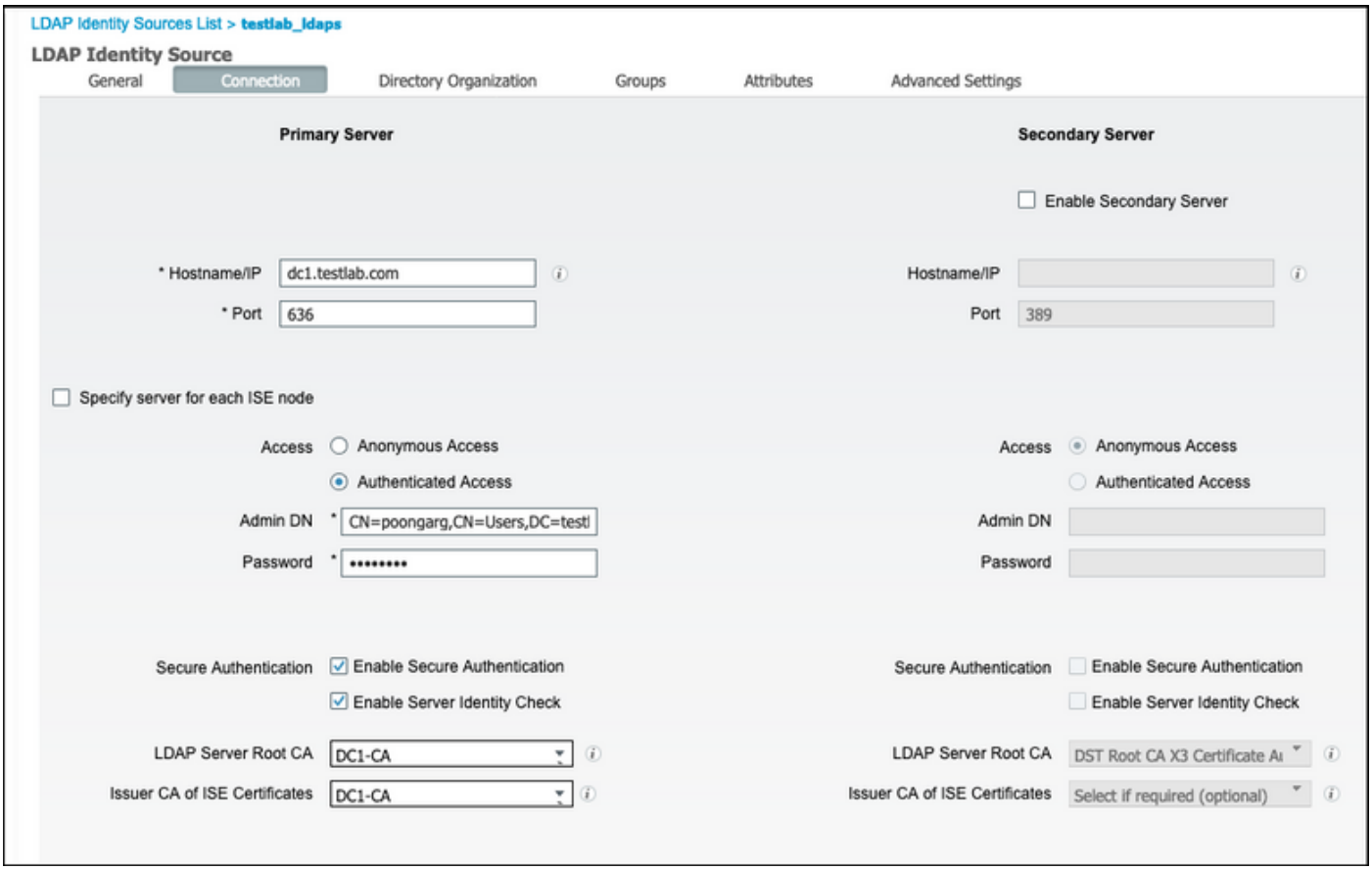
Atributo do mapa de grupo: Este atributo define como os usuários são mapeados para os grupos.

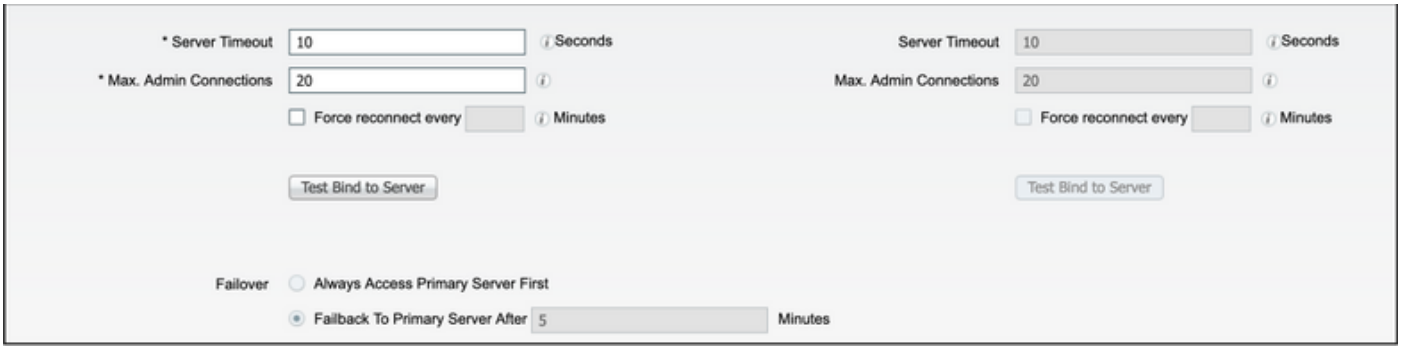


Atributo do certificado: Insira o atributo que contém as definições do certificado. Opcionalmente, essas definições podem ser usadas para validar certificados apresentados por clientes quando eles são definidos como parte de um perfil de autenticação de certificado. Nesses casos, uma comparação binária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



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





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.

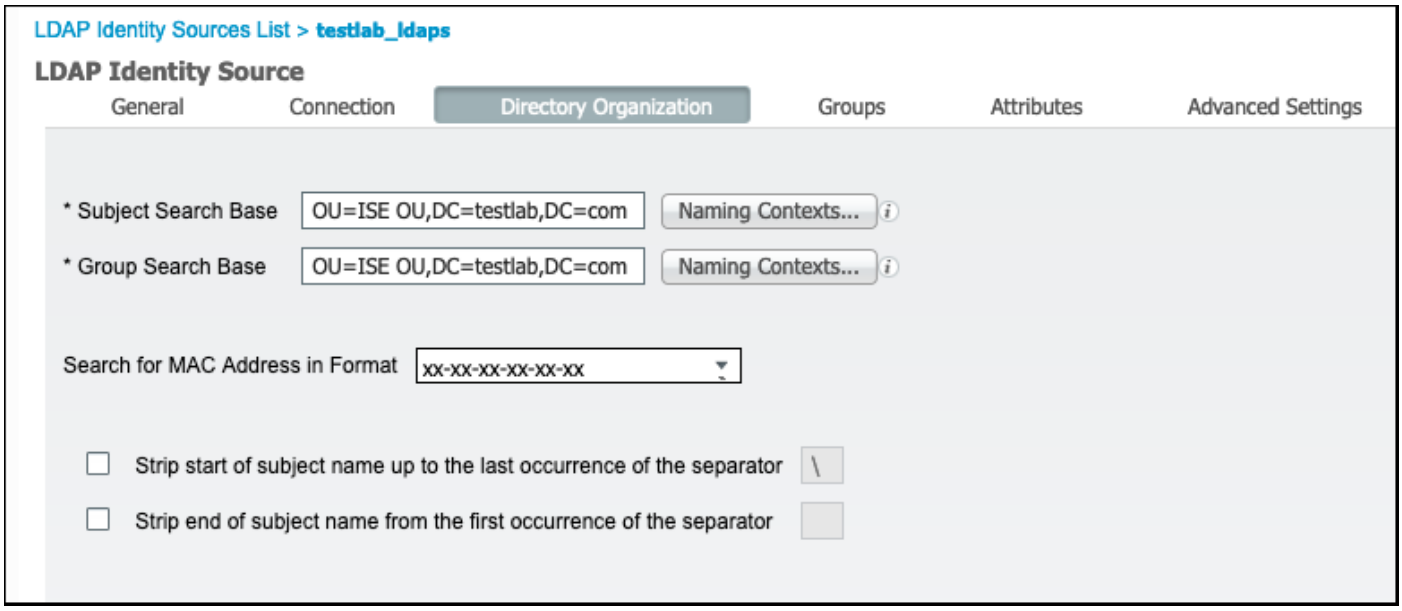
Etapa 2. Ativar a opção Autenticação segura e Verificação de identidade do servidor.

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

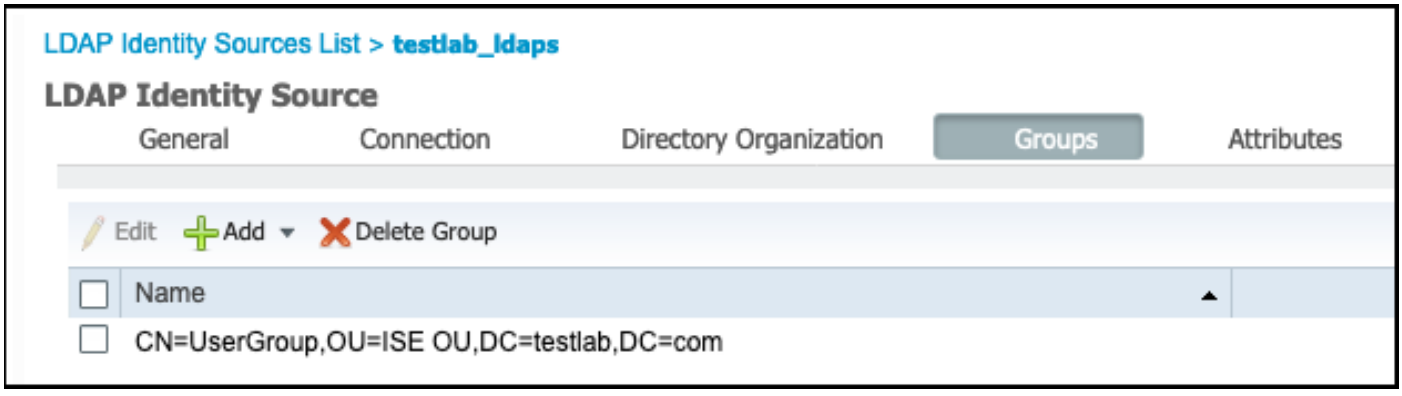
administrador ISE Isser CA certificado (também usamos autoridade de certificado, instalada no mesmo servidor LDAP para emitir o certificado de administrador ISE),

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 **Diretory 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

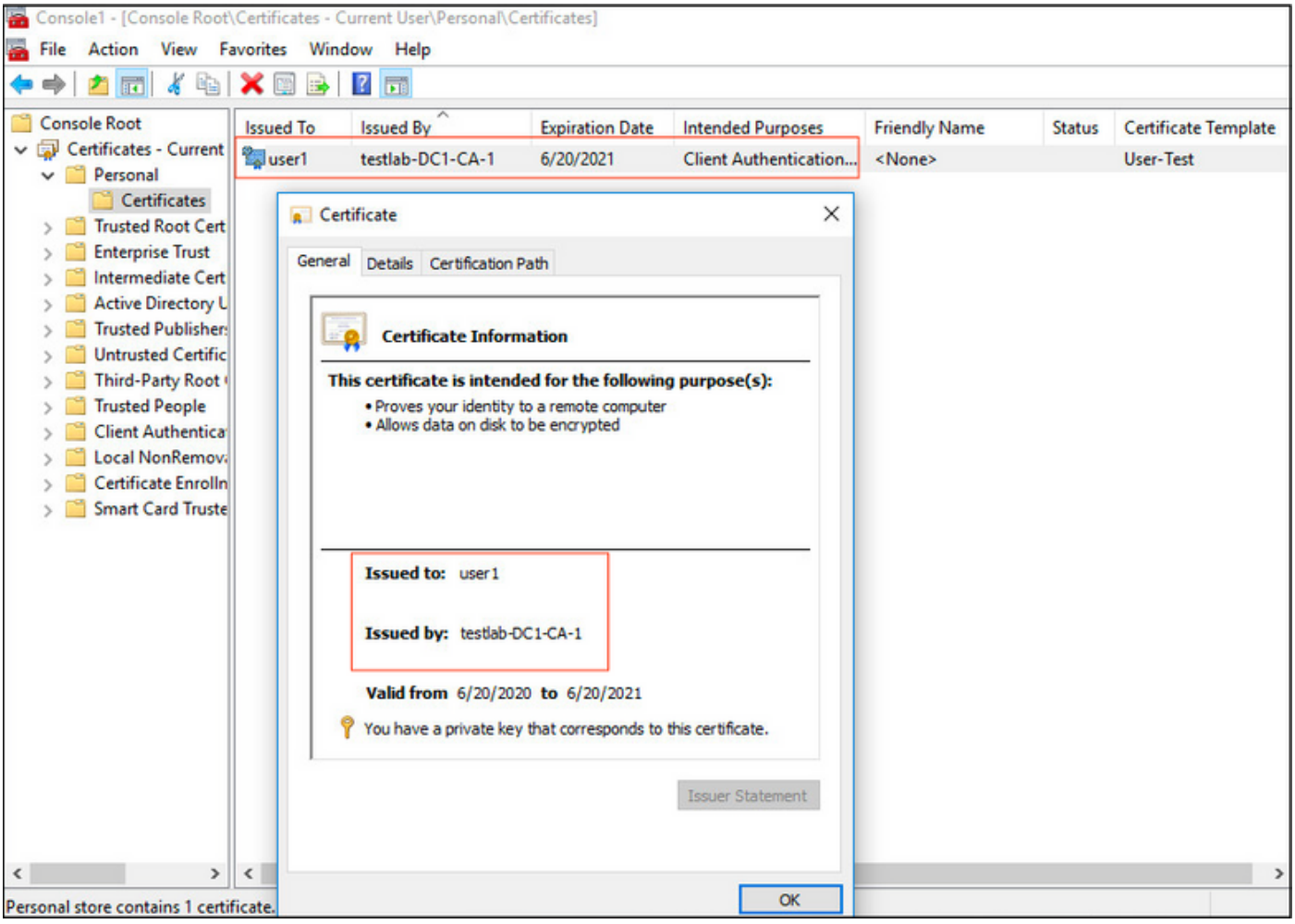
```
aaa new-model radius server ISE address ipv4 x.x.x.x auth-port 1812 acct-port 1813 key xxxxxx
aaa group server radius ISE_SERVERS server name ISE ! aaa server radius dynamic-author client
x.x.x.x server-key xxxxxx ! aaa authentication dot1x default group ISE_SERVERS local aaa
authorization network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

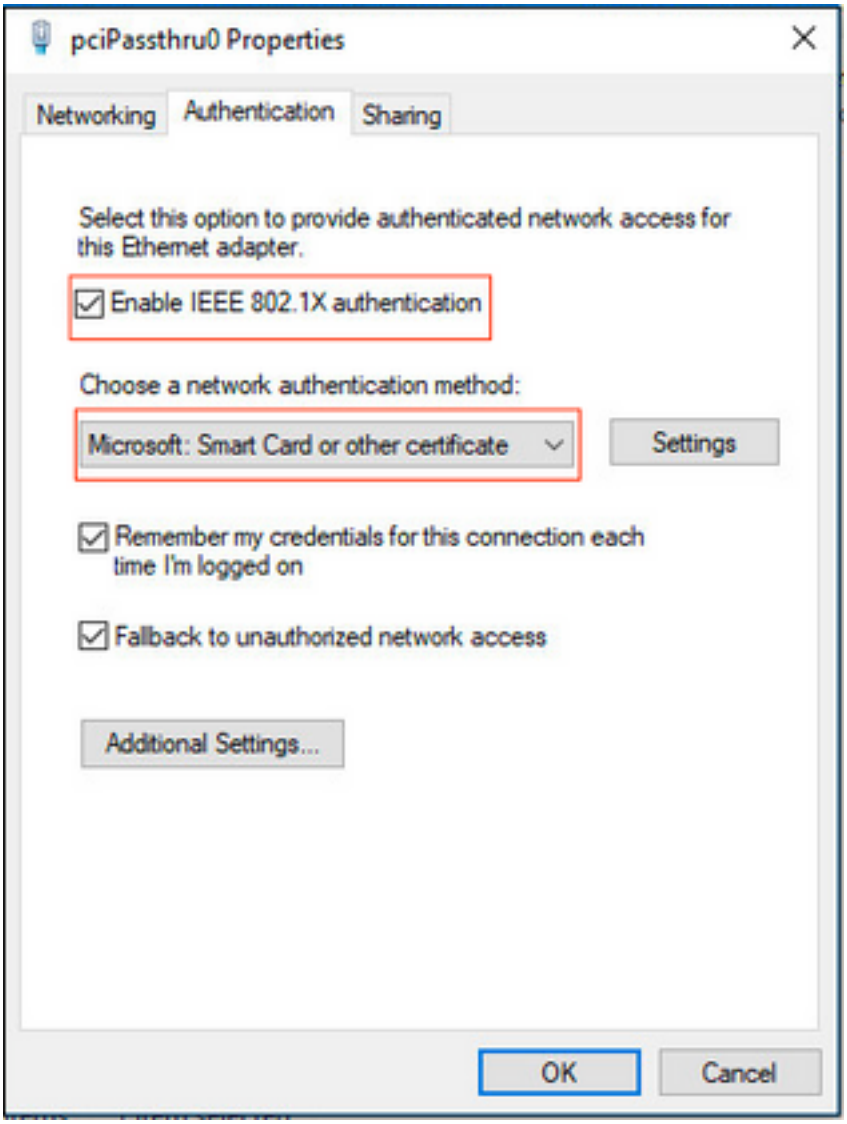
Configurar o endpoint

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

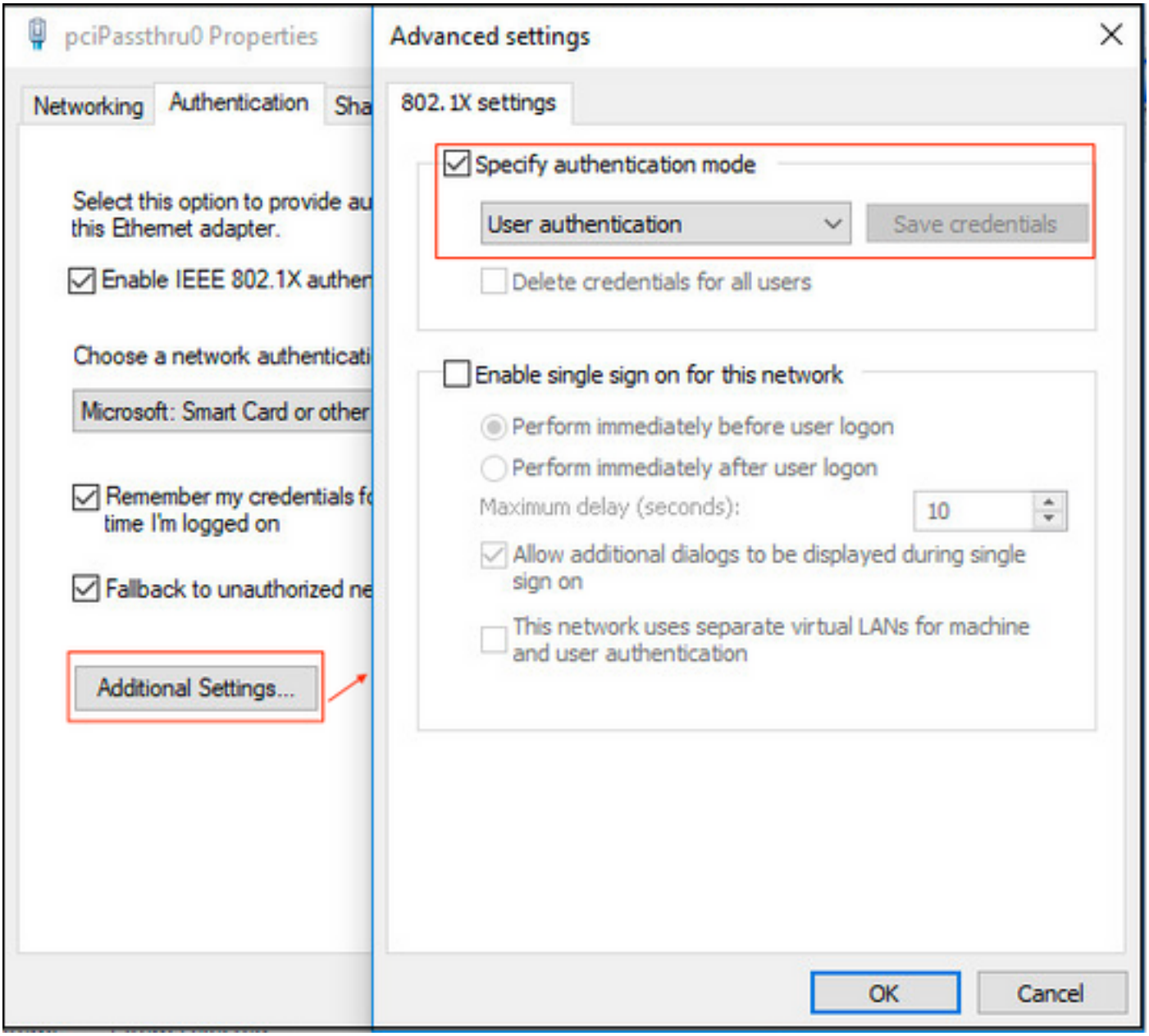
1. Certifique-se de que o PC esteja equipado com certificado de usuário (para usuário1) e tenha uma finalidade específica como Autenticação de cliente e, nas Autoridades de Certificação de Raiz Confiável, a cadeia de certificados do emissor está presente no PC.



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

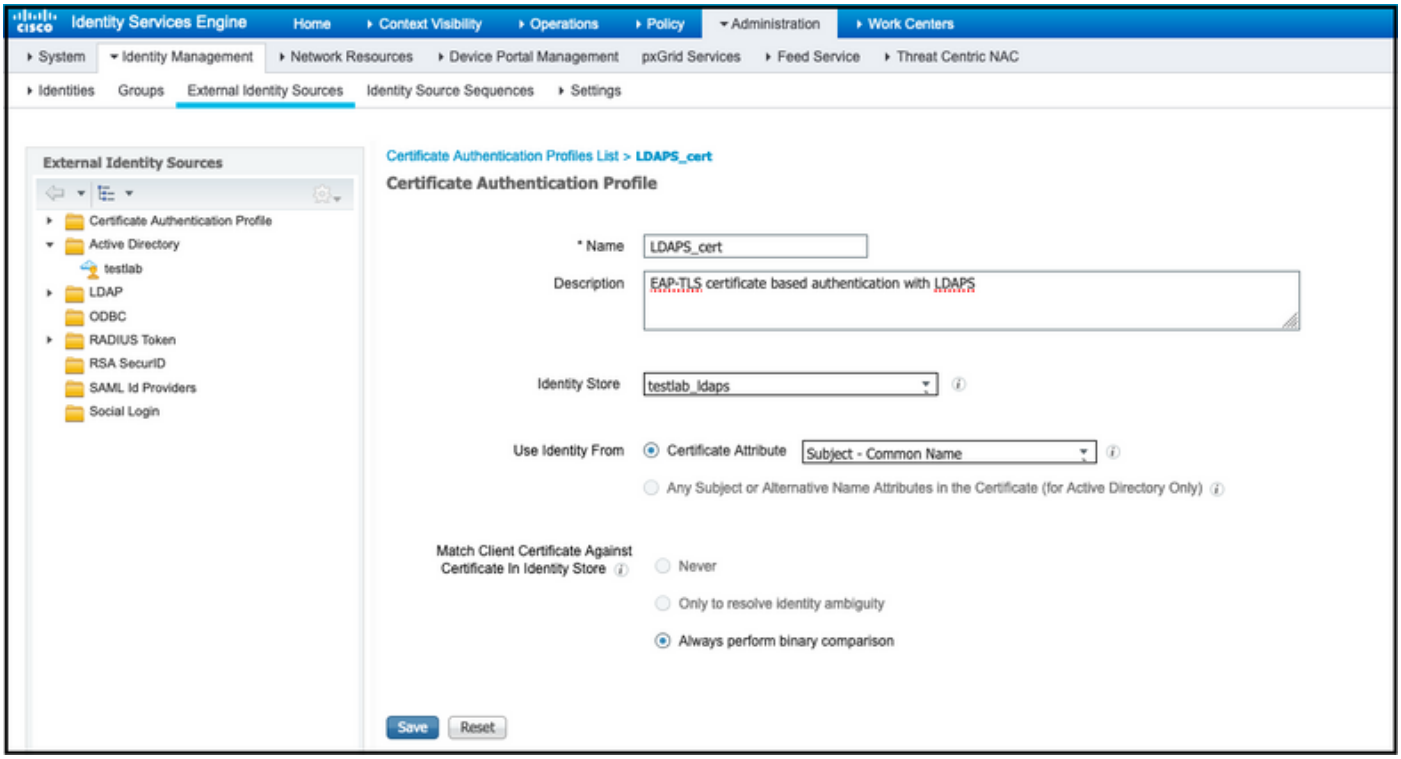


3. Clique em **Additional Settings (Configurações adicionais**), uma janela será aberta, marque a caixa com **especificar modo de autenticação** e escolha **User authentication**, como mostrado nesta imagem.

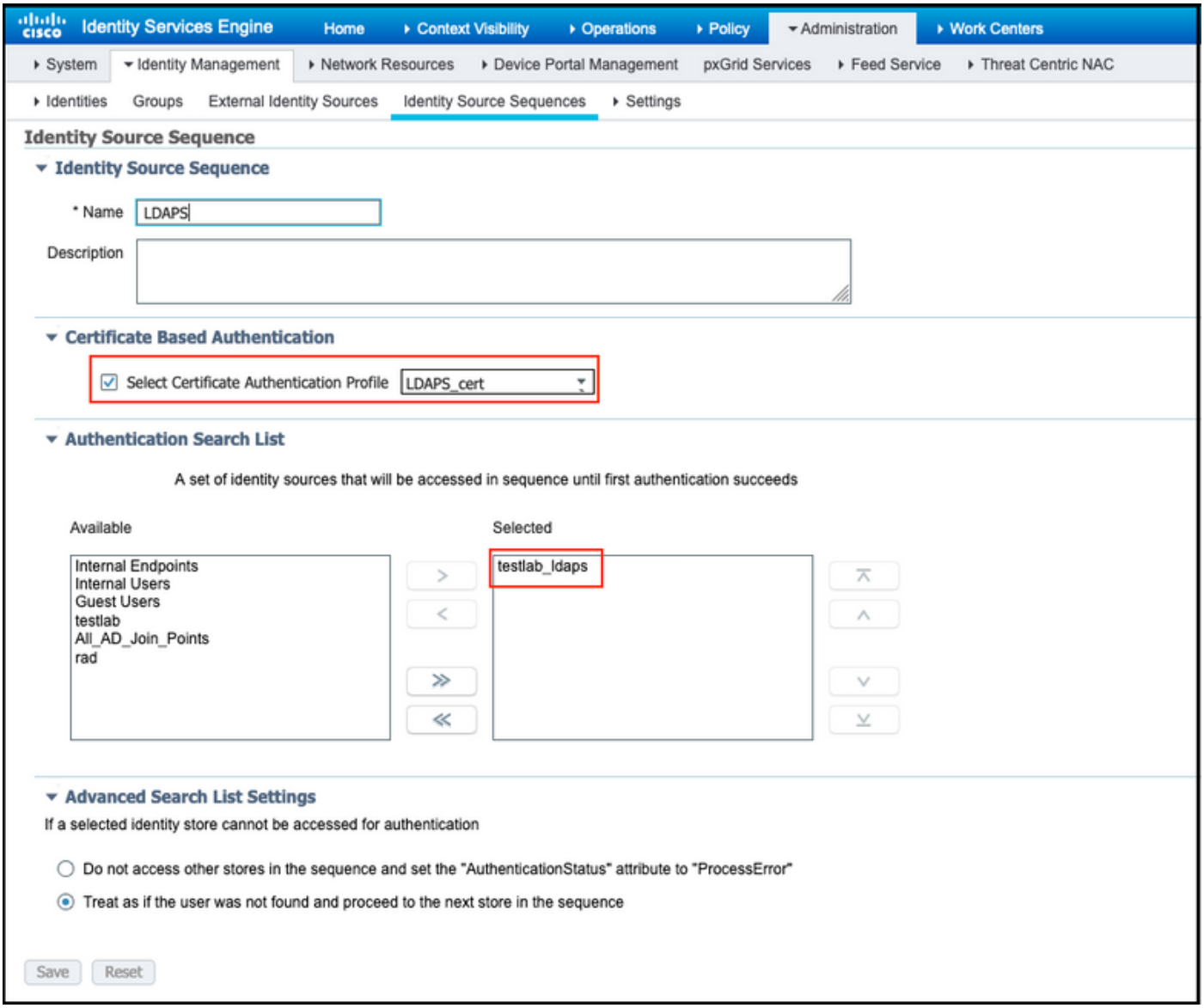


Configurar o conjunto de políticas no ISE

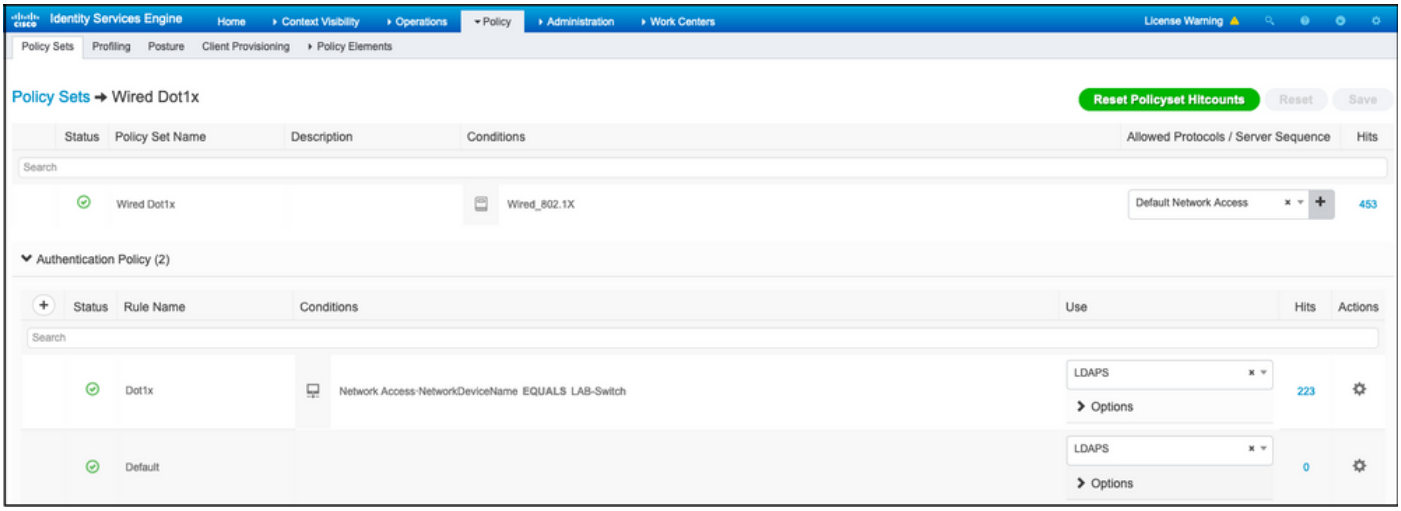
Como o protocolo EAP-TLS é usado, antes que o Conjunto de políticas seja configurado, o Perfil de autenticação do certificado precisa ser configurado e a sequência de origem da identidade será usada posteriormente na política de autenticação.



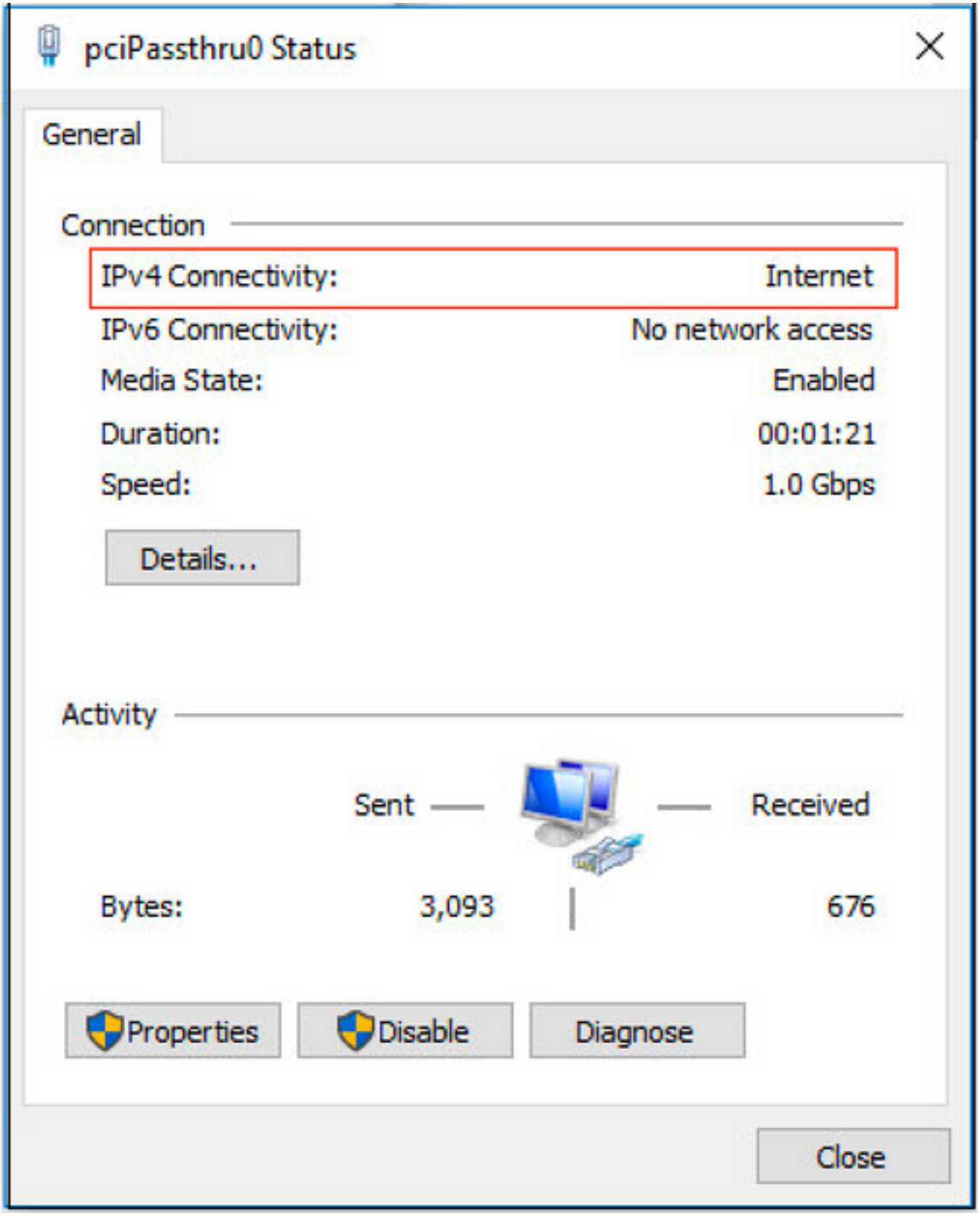
Consulte o Perfil de Autenticação de Certificado na Sequência de Origem da Identidade e defina a origem de identidade externa LDAPS na lista Pesquisa de Autenticação:



Agora configure a política definida para a autenticação Wired Dot1x:



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

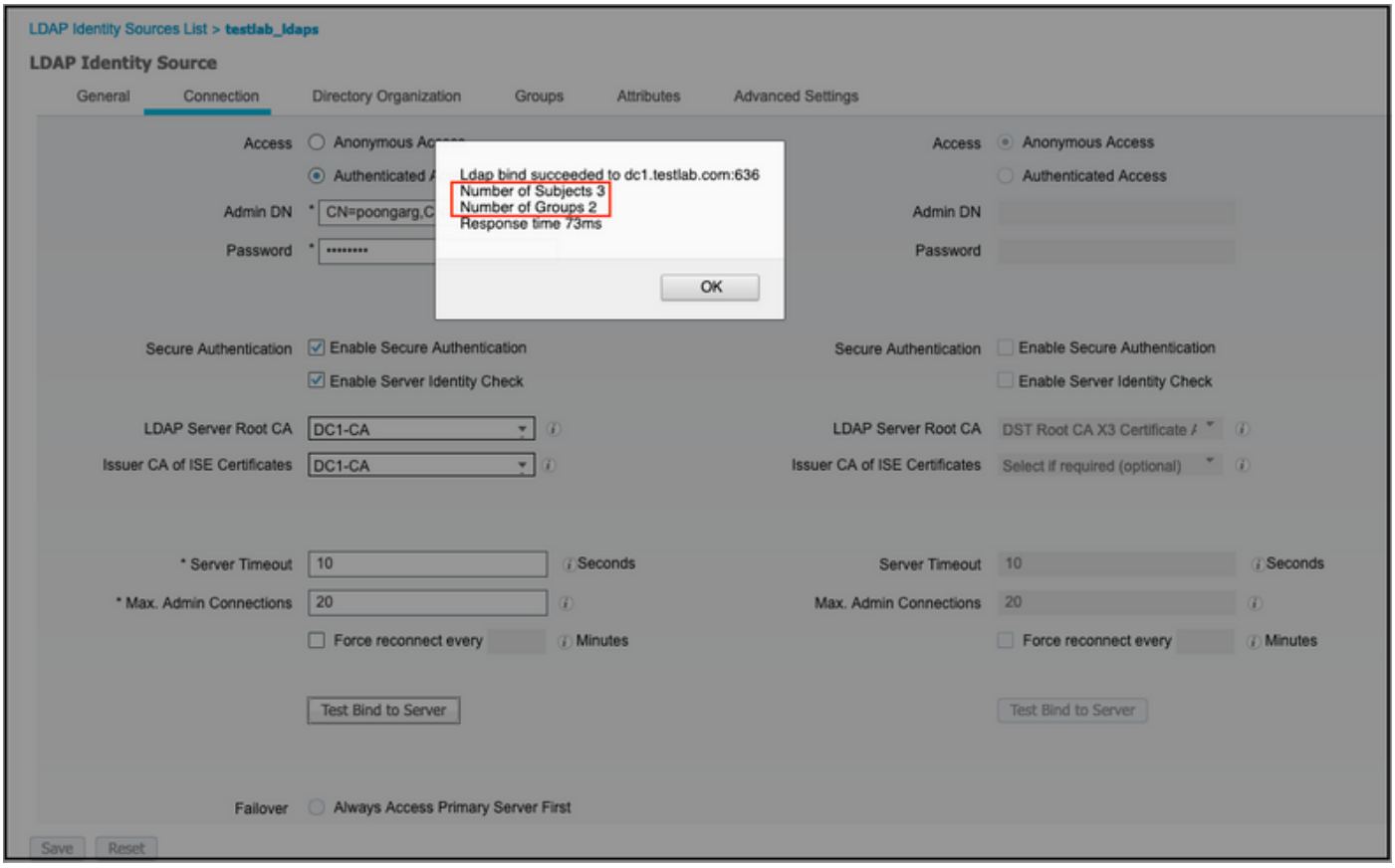


Verificar

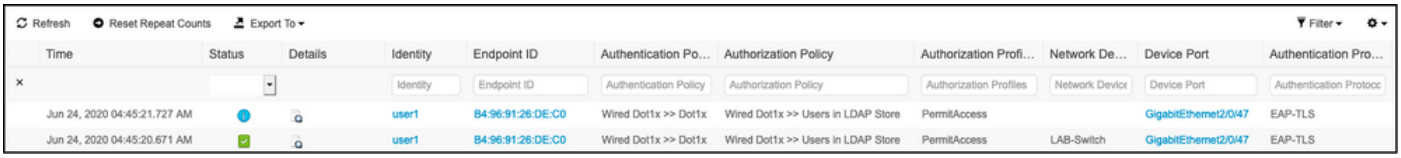
1. Verifique a sessão de autenticação na porta do switch conectada ao PC:

```
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:  0A6A263900000130798C66612
      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
```

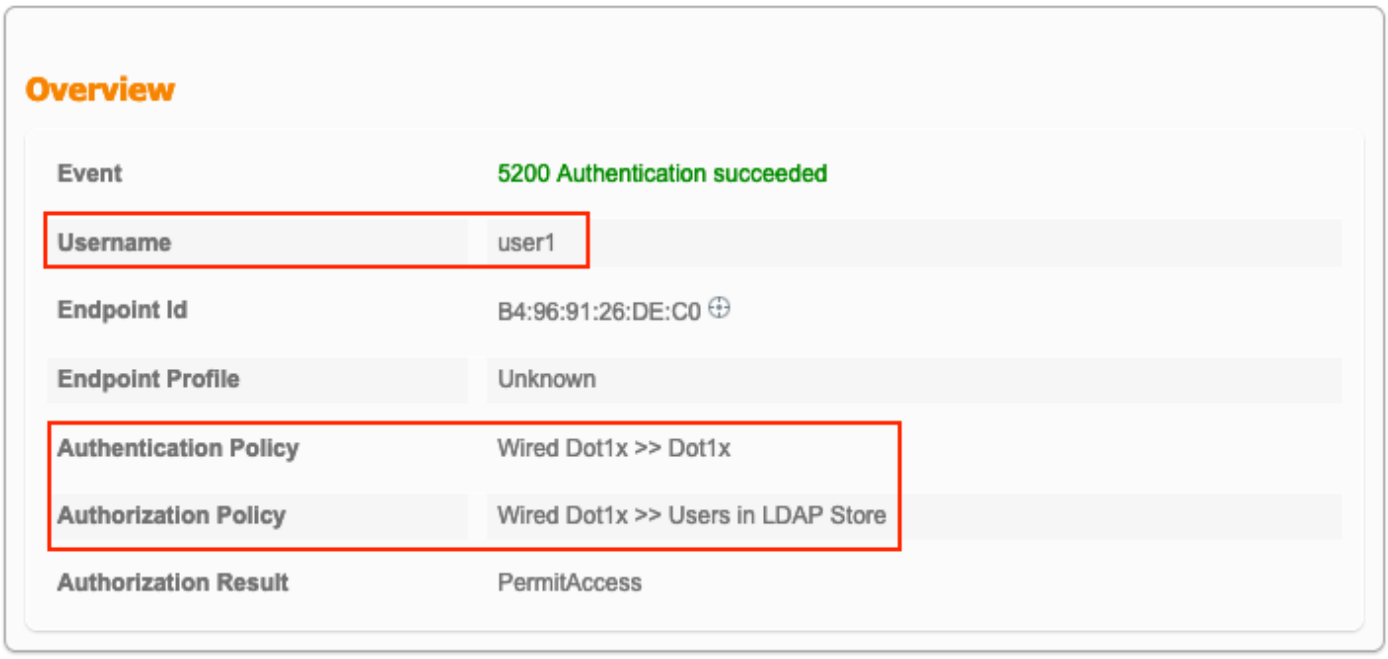
2. Para verificar as configurações de LDAPS e ISE, você pode recuperar os participantes e os grupos com uma conexão de teste com o servidor:



3. Verifique o relatório de autenticação do usuário:

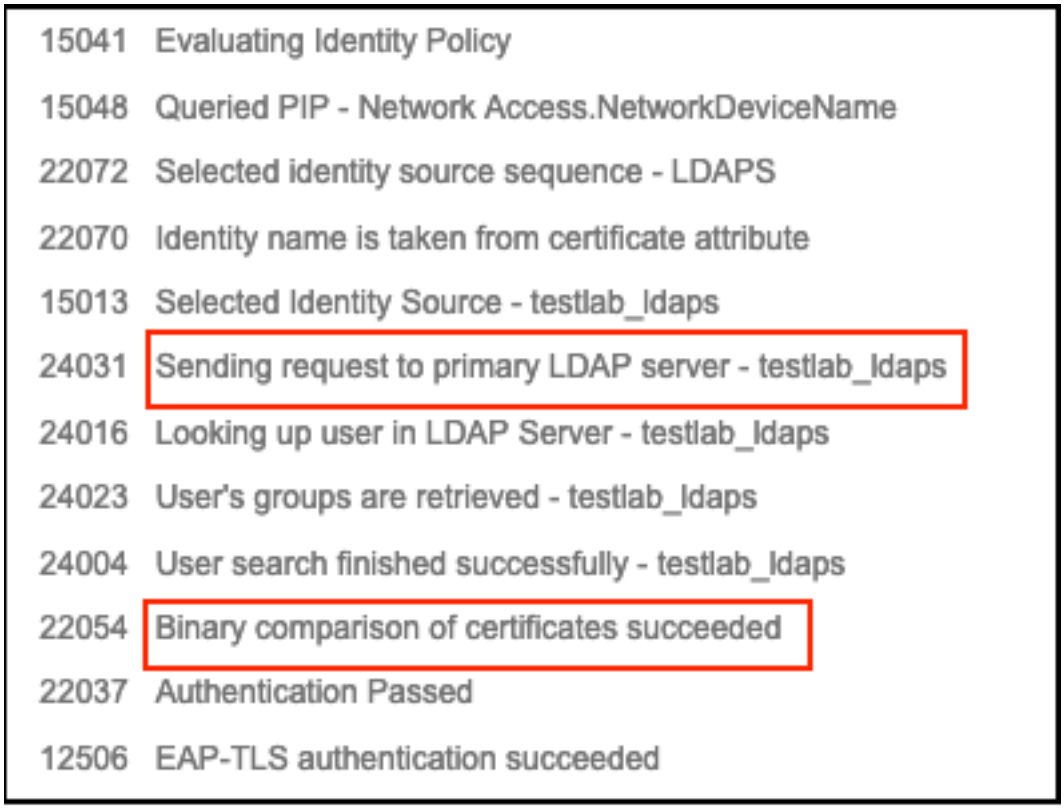


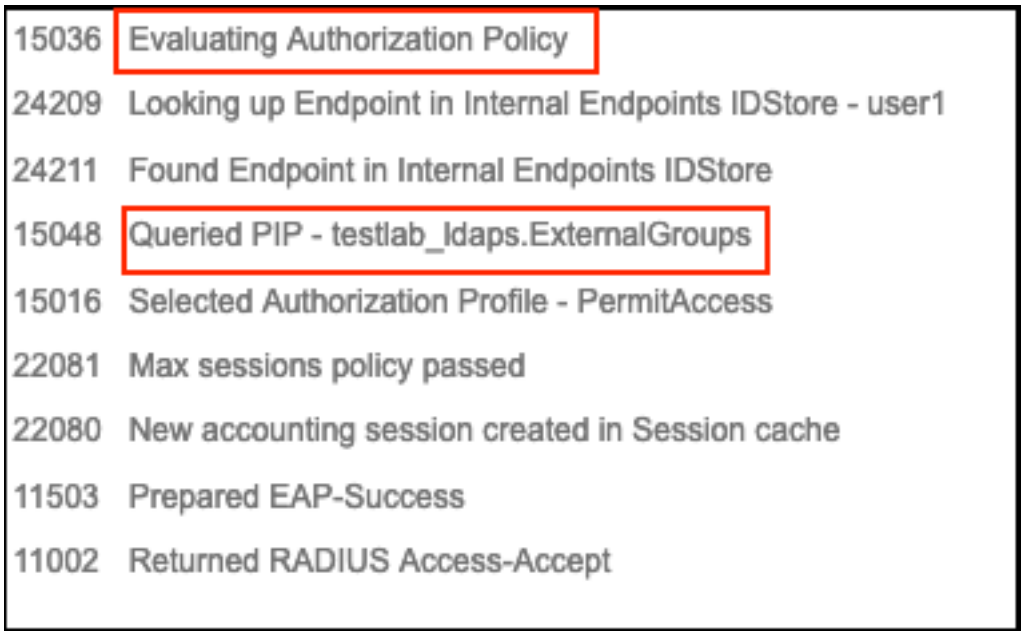
4. Verifique o relatório de autenticação detalhado para o endpoint:



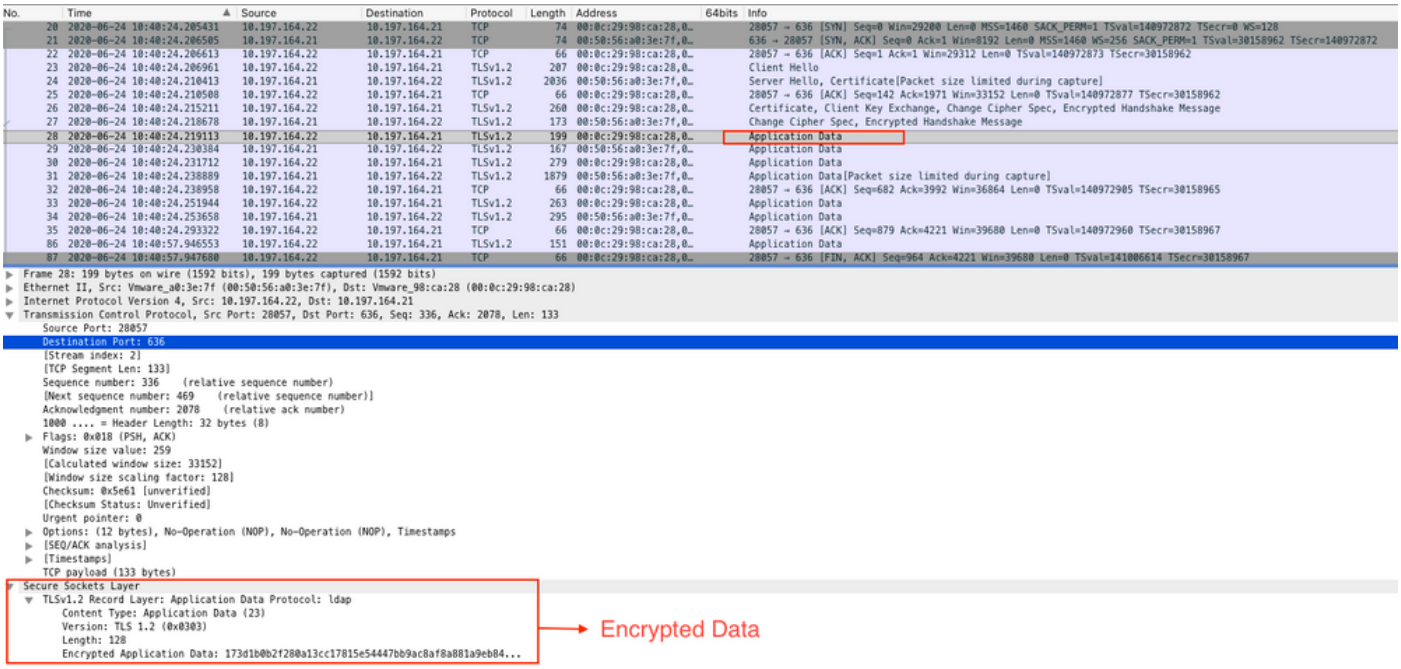
Authentication Details

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_ldaps
Identity Group	Unknown
Audit Session Id	0A6A26390000130C98CE6088
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	LAB-Switch





5. Valide se os dados estão criptografados entre o servidor ISE e LDAPS levando a captura de pacotes no ISE para o servidor LDAPS:



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, recrie 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_clnt.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