

# Solucionar problemas de Wired Dot1x no ISE 3.2 e no Windows

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

---

## Introdução

Este documento descreve como configurar uma autenticação PEAP 802.1X básica para o Identity Services Engine (ISE) 3.2 e o solicitante nativo do Windows.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo PEAP protegido
- PEAP 802.1x

### Componentes Utilizados

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

- Versão do Cisco Identity Services Engine (ISE)
- Software Cisco C1117 Cisco IOS® XE, versão 17.12.02
- Notebook com Windows 10

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.

## Configurar

### Diagrama de Rede

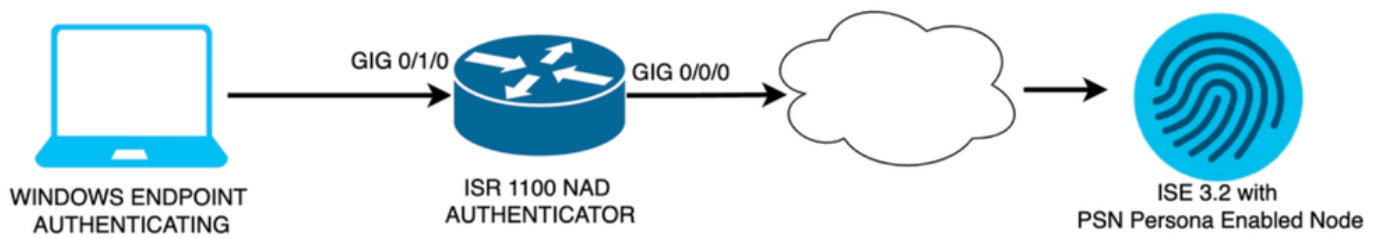


Diagrama de Rede

## Configurações

Execute estas etapas para configurar:

Etapa 1. Configure o roteador ISR 1100.

Etapa 2. Configure o Identity Service Engine 3.2.

Etapa 3. Configurar o Solicitante Nativo do Windows.

Etapa 1. Configurar o roteador ISR 1100

Esta seção explica a configuração básica que pelo menos o NAD deve ter para fazer o dot1x funcionar.

---

Observação: para implantação do ISE com vários nós, configure o IP do nó que tem a persona PSN habilitada. Isso pode ser ativado se você navegar até o ISE na guia Administração > Sistema > Implantação.

---

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
  client A.B.C.D server-key <Your shared secret>
!
!
radius server ISE-PSN-1
  address ipv4 A.B.C.D auth-port 1645 acct-port 1646
  timeout 15
  key <Your shared secret>
```

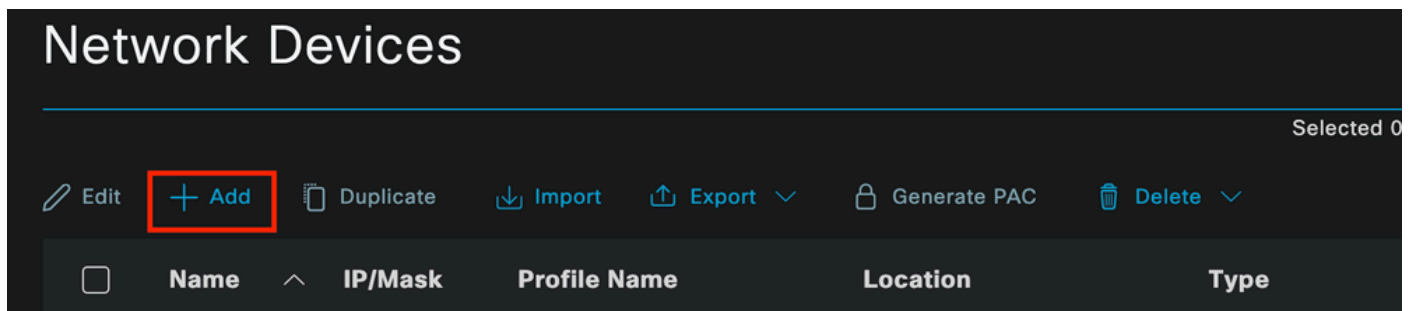
```
!  
!  
aaa group server radius ISE-CLUSTER  
  server name ISE-PSN-1  
!  
interface GigabitEthernet0/1/0  
  description "Endpoint that supports dot1x"  
  switchport access vlan 15  
  switchport mode access  
  authentication host-mode multi-auth  
  authentication order dot1x mab  
  authentication priority dot1x mab  
  authentication port-control auto  
  dot1x pae authenticator  
  spanning-tree portfast
```

Etapa 2. Configure o Identity Service Engine 3.2.

2. a. Configure e adicione o dispositivo de rede a ser usado para a autenticação.

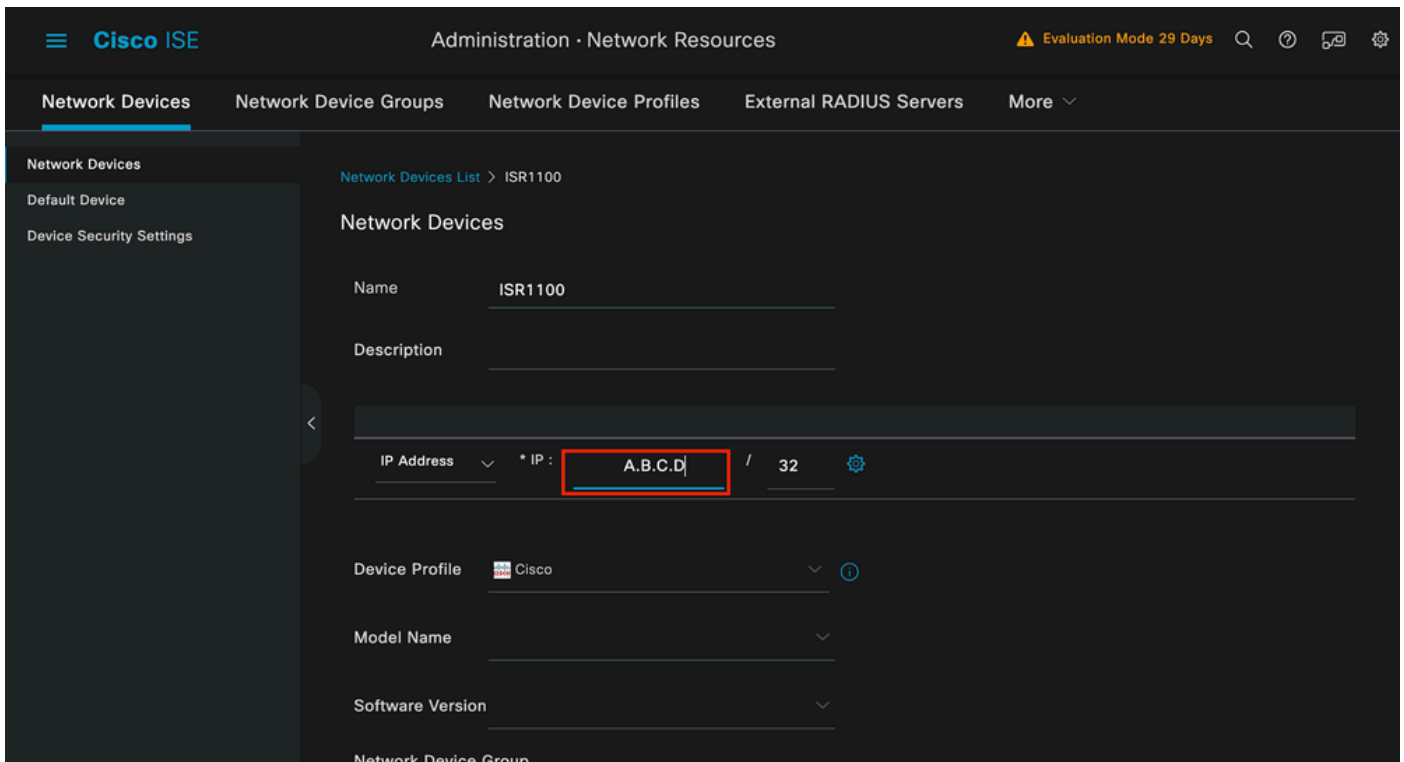
Adicione o dispositivo de rede à seção Dispositivos de rede do ISE.

Clique no botão Add para iniciar.



Dispositivos de rede ISE

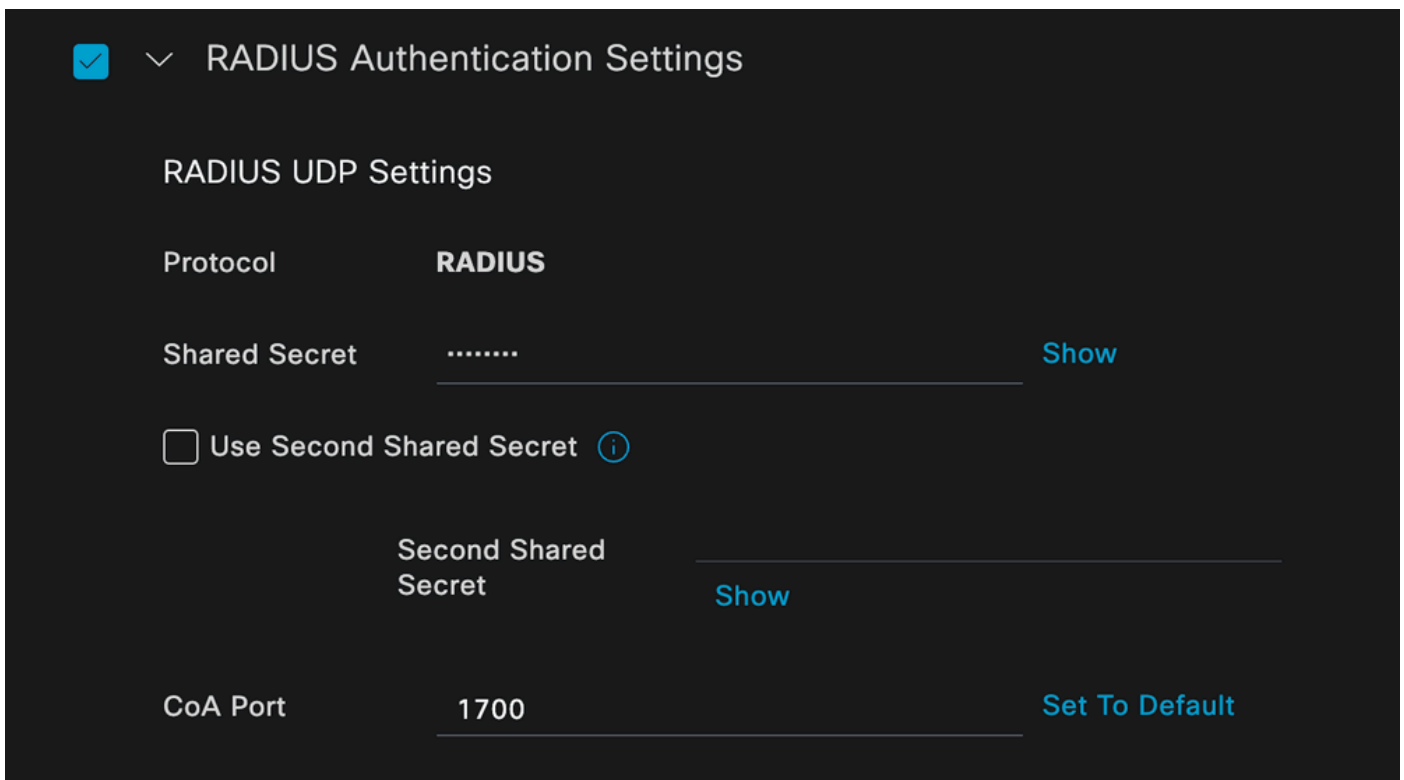
Insira os valores, atribua um nome ao NAD que você está criando e adicione também o IP que o dispositivo de rede usa para entrar em contato com o ISE.



Página Network Device Creation

Nesta mesma página, role para baixo para encontrar as configurações de autenticação RADIUS. Como mostrado na próxima imagem.

Adicione o Shared Secret que você usou na sua configuração NAD.

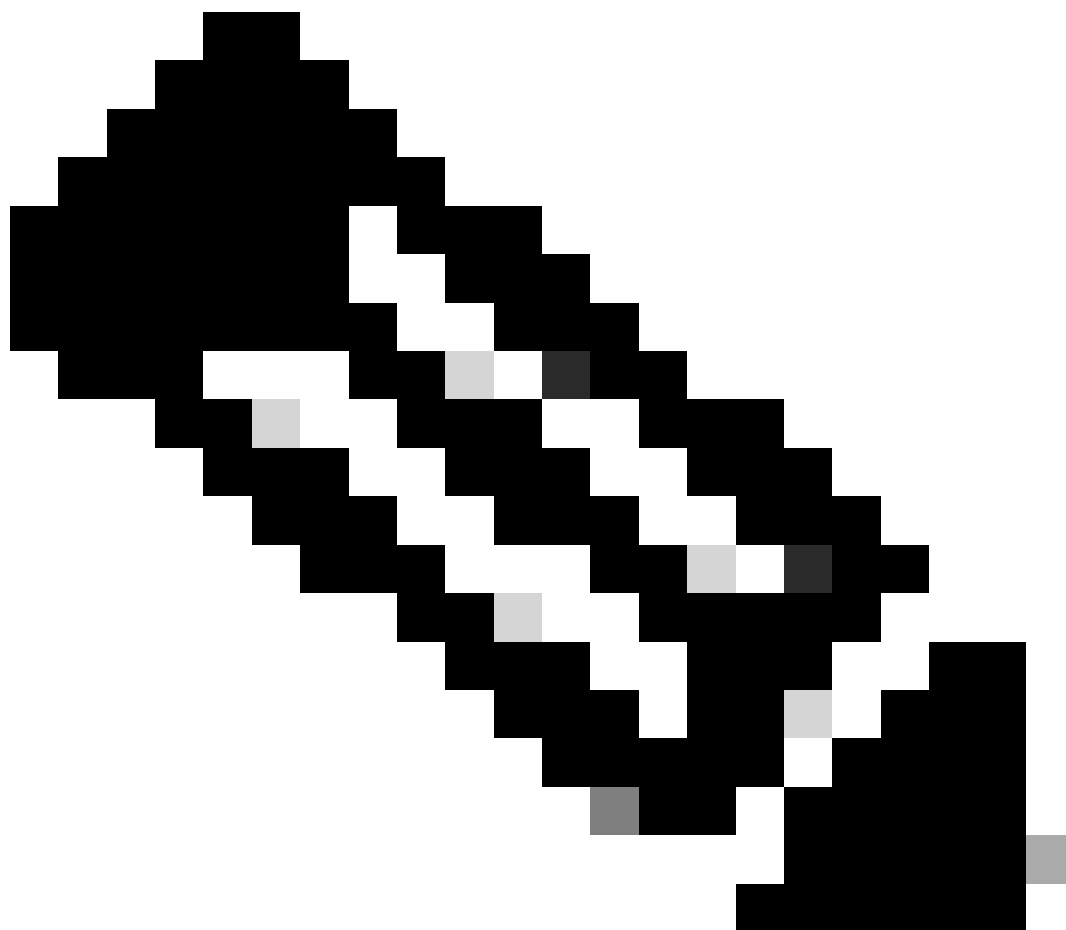


Configuração de RADIUS

Salve as alterações.

2. b. Configure a identidade que é usada para autenticar o ponto final.

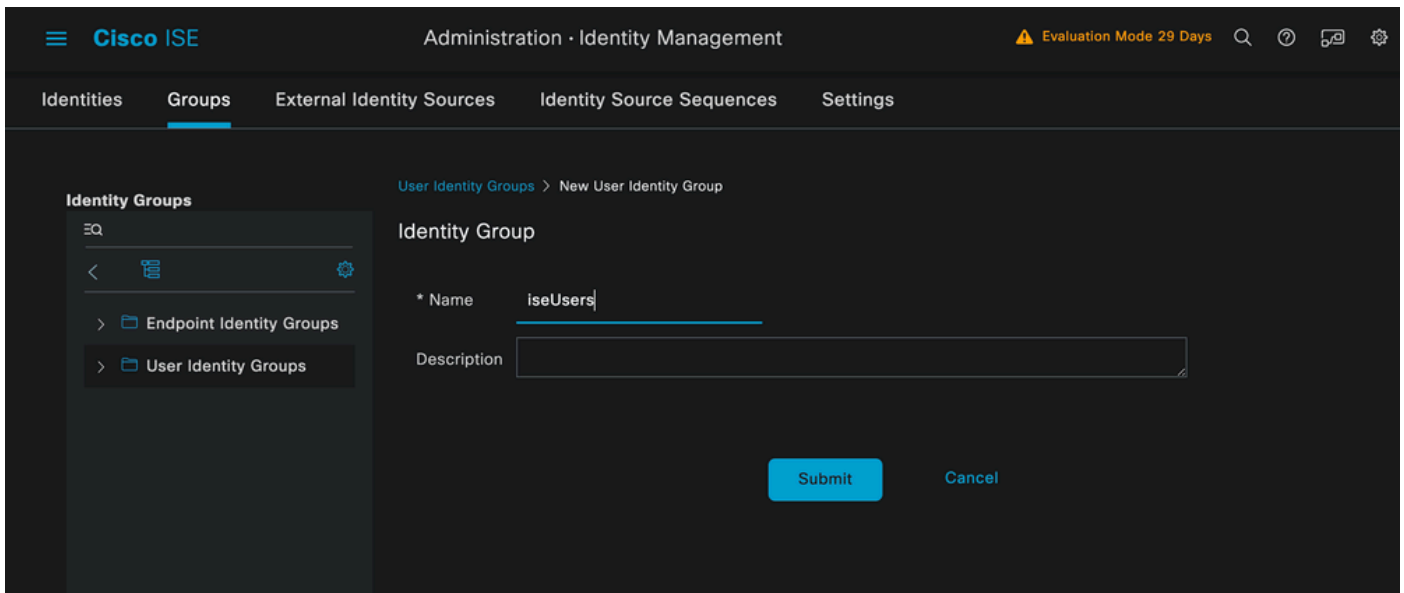
---



Observação: com o objetivo de manter este guia de configuração simples, a autenticação local do ISE é usada.

---

Navegue até a guia Administração > Gerenciamento de identidades > Grupos. Crie o grupo e a identidade, o grupo criado para esta demonstração é iseUsers.

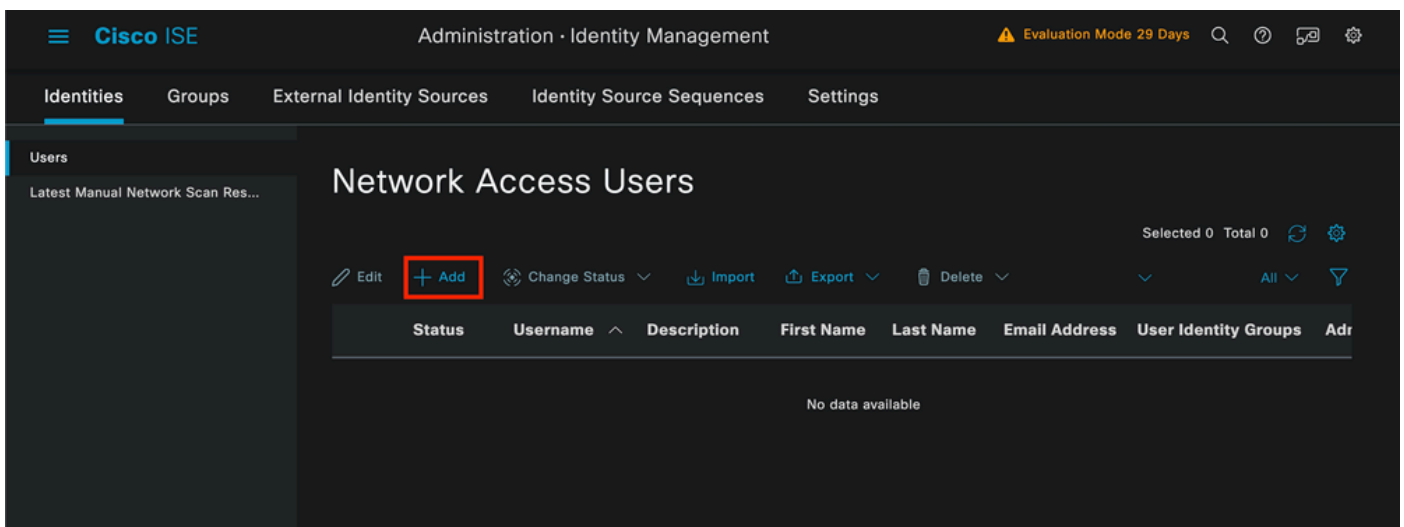


*Página Criação do Grupo de Identidade*

Clique no botão Submit.

Em seguida, navegue até a guia Administração > Gerenciamento de identidades > Identidade.

Clique em Add.



*Página Criação de Usuário*

Como parte dos campos obrigatórios, comece com o nome do usuário. O nome de usuário isiscool é usado neste exemplo.

### Network Access User

\* Username

Status  Enabled ⌵

Account Name Alias  ⓘ

Email

Nome atribuído ao nome de usuário

A próxima etapa é atribuir uma senha ao nome de usuário criado. O VainillaSE97 é usado nesta demonstração.

### Passwords

Password Type:  ⌵

Password Lifetime:

- With Expiration ⓘ  
Password will expire in 60 days
- Never Expires ⓘ

	Password	Re-Enter Password	
* Login Password	<input type="password" value="....."/>	<input type="password" value="....."/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Generate Password"/> ⓘ

Criação de Senha

Atribua o usuário ao grupo iseUsers.

### User Groups

ⓘ

Atribuição do grupo de usuários

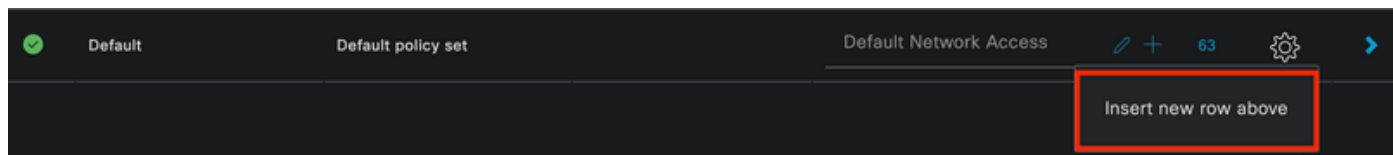


## 2. c. Configurar o Conjunto de Políticas

Navegue até o menu do ISE > Política > Conjuntos de políticas.

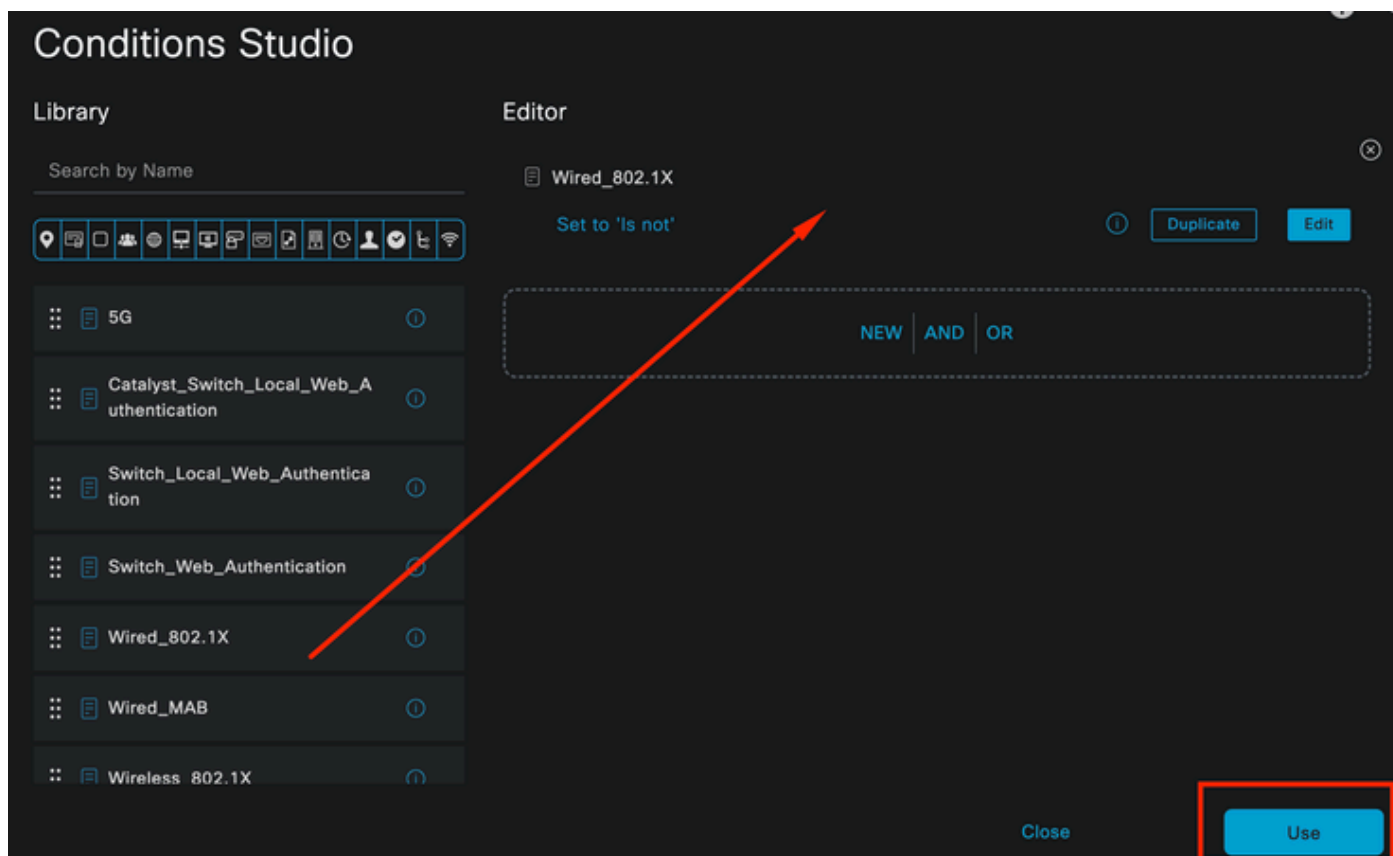
O conjunto de políticas padrão pode ser usado. No entanto, neste exemplo, um conjunto de políticas é criado e é chamado de Wired. Classificar e diferenciar os conjuntos de políticas ajuda na solução de problemas,

Se o ícone de adição ou adição não estiver visível, é possível clicar no ícone de engrenagem de qualquer conjunto de diretivas. Selecione o ícone de engrenagem e depois selecione Inserir nova linha acima.



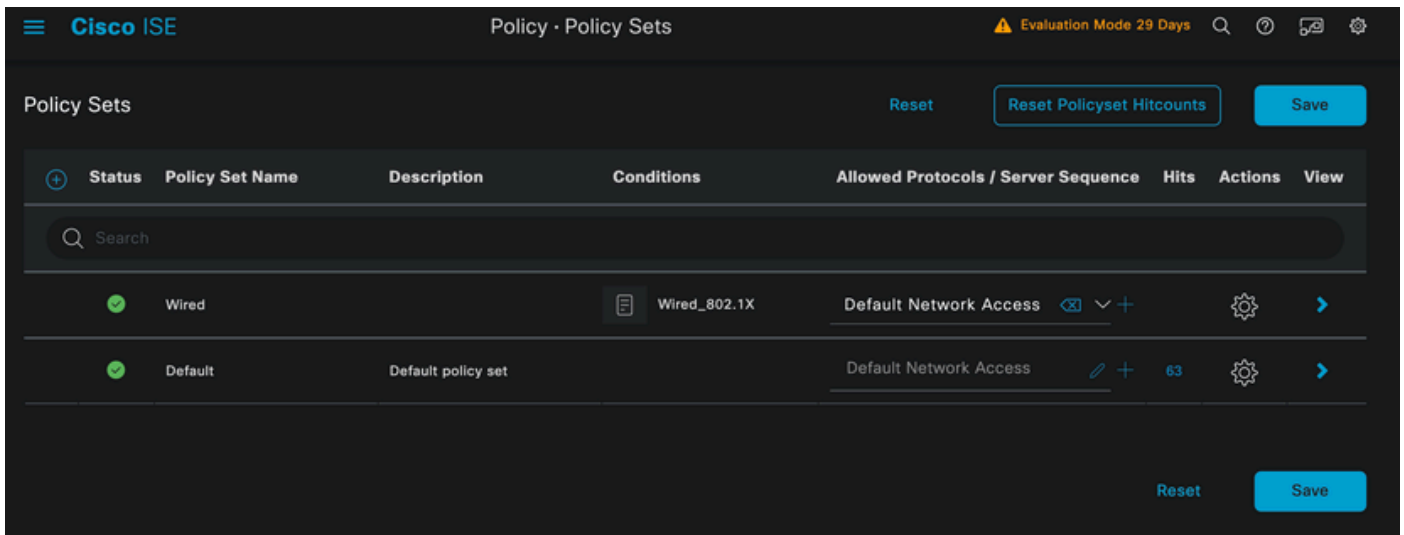
Criação de política

A condição configurada neste exemplo é Wired 802.1x, que é uma condição pré-configurada em novas implantações do ISE. Arraste-o e clique em Usar.



Estúdio de Condição

Por fim, selecione Default Network Access preconfigured allowed protocols service.

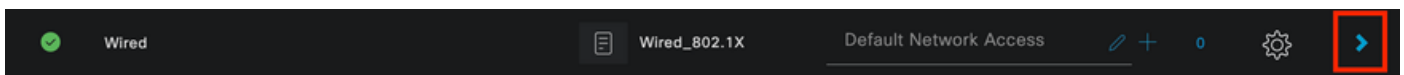


Exibição do conjunto de políticas

Click Save.

2. d. Configure as Políticas de Autenticação e Autorização.

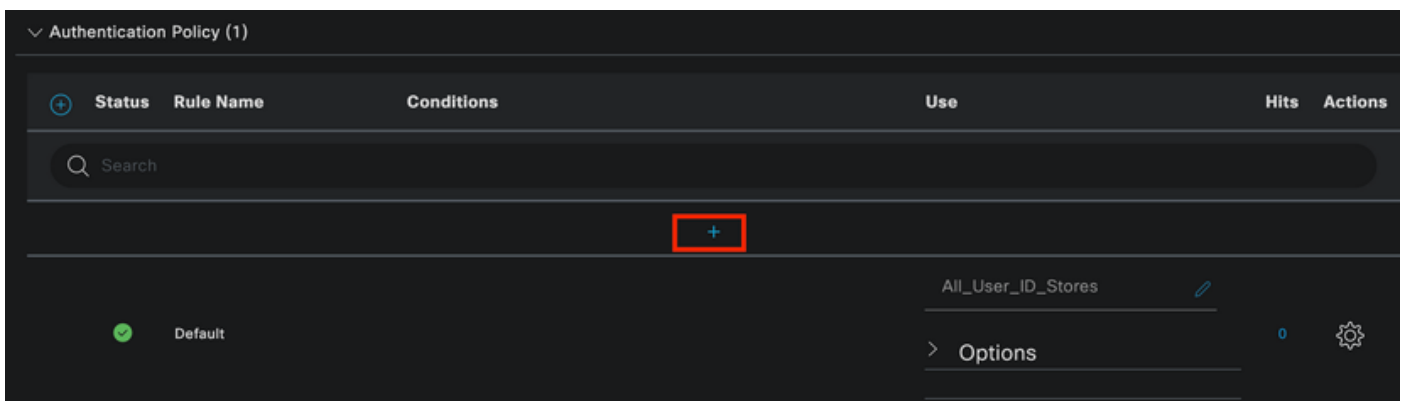
Clique na seta à direita do conjunto de políticas recém-criado.



Conjunto de políticas com fio

Expanda a política de autenticação

Clique no ícone +.



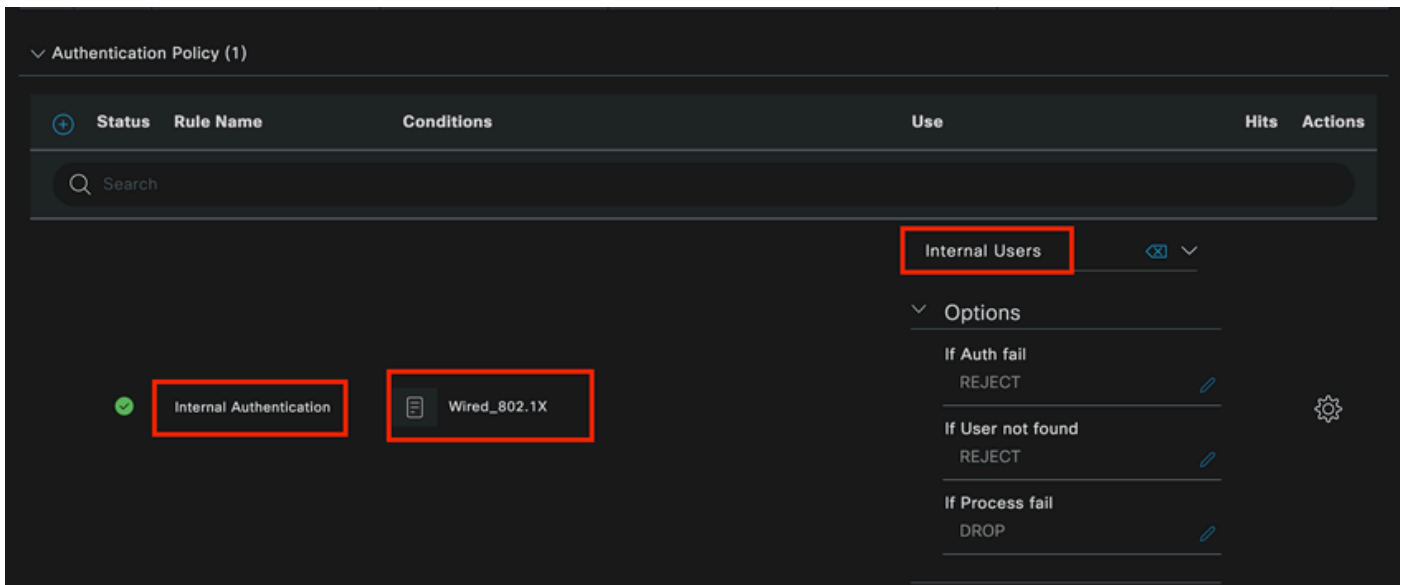
Adicionar política de autenticação

Atribua um nome à política de autenticação; neste exemplo, Internal Authentication é usado.

Clique no ícone + na coluna condições para esta nova Política de autenticação.

A condição pré-configurada Wired Dot1x ISE vem com pode ser usada.

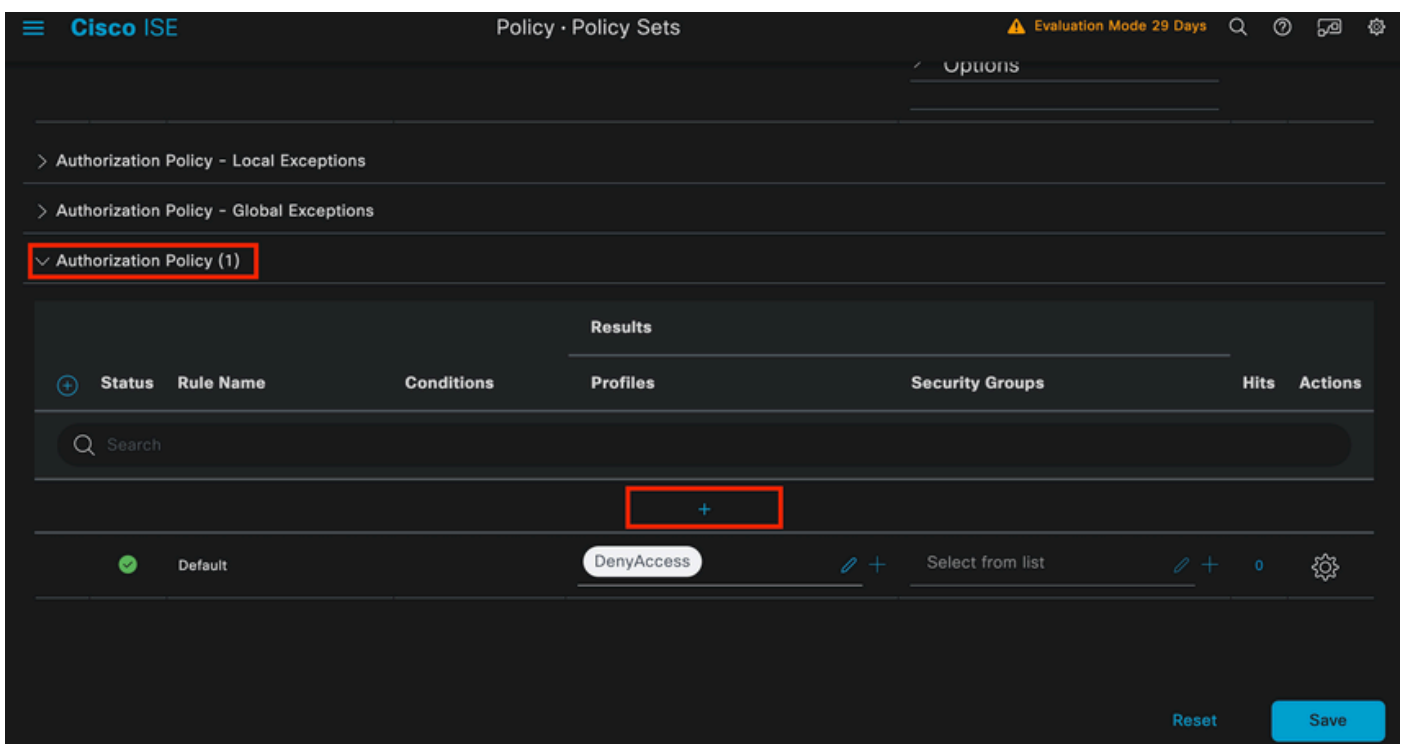
Por fim, na coluna Use, selecione Internal Users na lista suspensa.



Política de autenticação

## Política de Autorização

A seção Política de autorização está na parte inferior da página. Expanda-o e clique no ícone +.



Política de Autorização

Nomeie a política de autorização que você acabou de adicionar. Neste exemplo de configuração, o nome Internal ISE Users é usado.

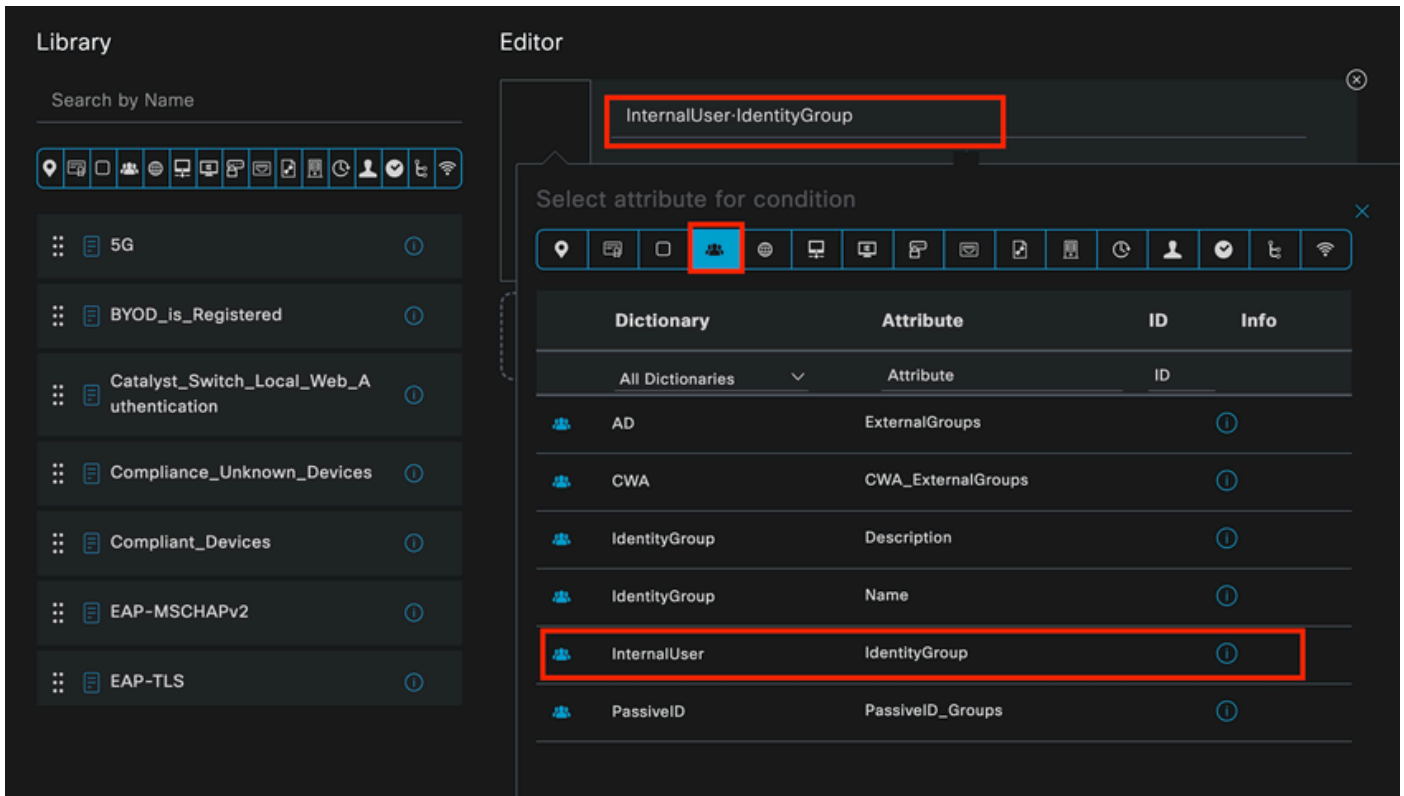
Para criar uma condição para esta Diretiva de autorização, clique no ícone + sob a coluna Condições.

O usuário criado anteriormente faz parte do grupo IseUsers.

No editor, clique na seção Clique para adicionar um atributo.

Selecione o ícone Grupo de identidade.

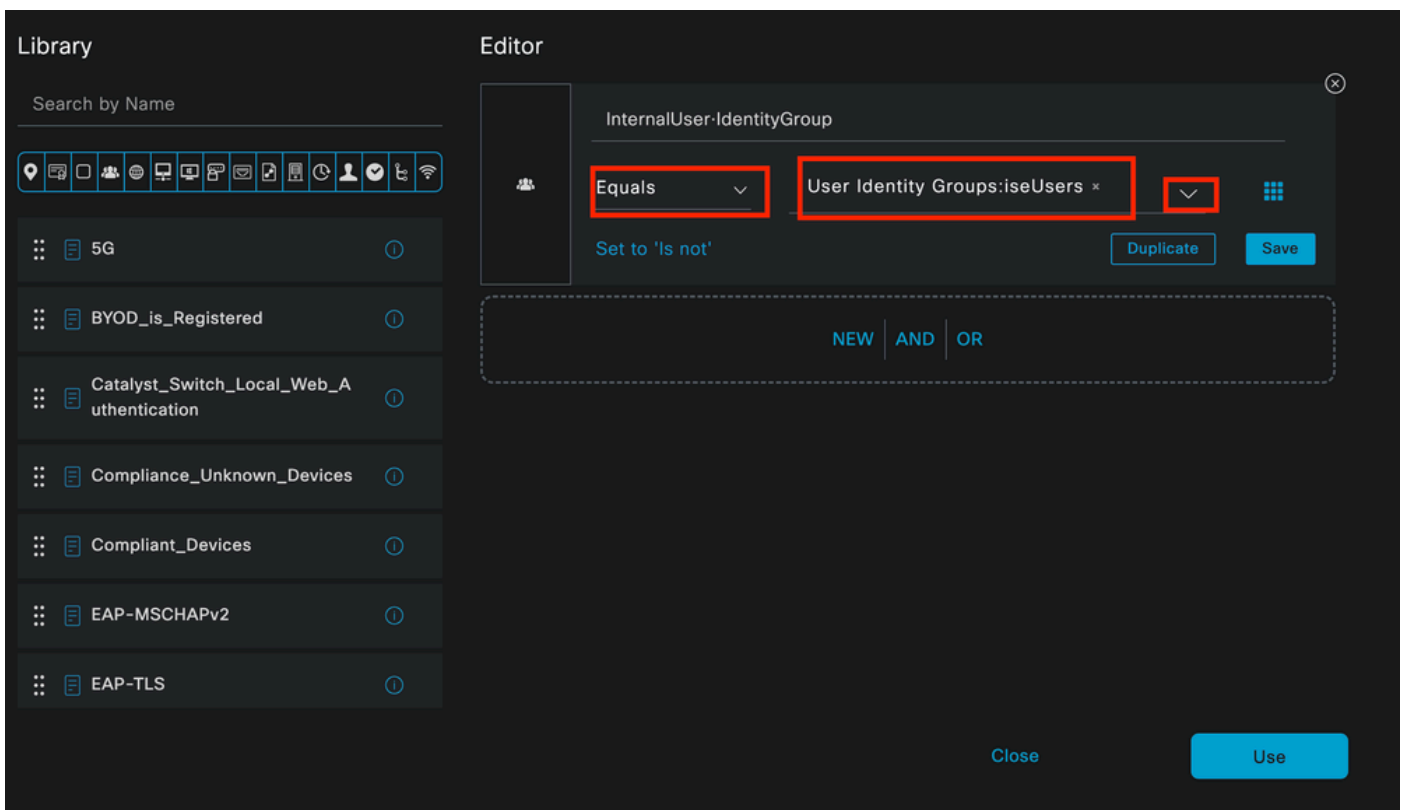
No dicionário, selecione o dicionário InternalUser que vem com o atributo Identity Group.



Estúdio de Condição para Diretiva de Autorização

Selecione o operador Equals.

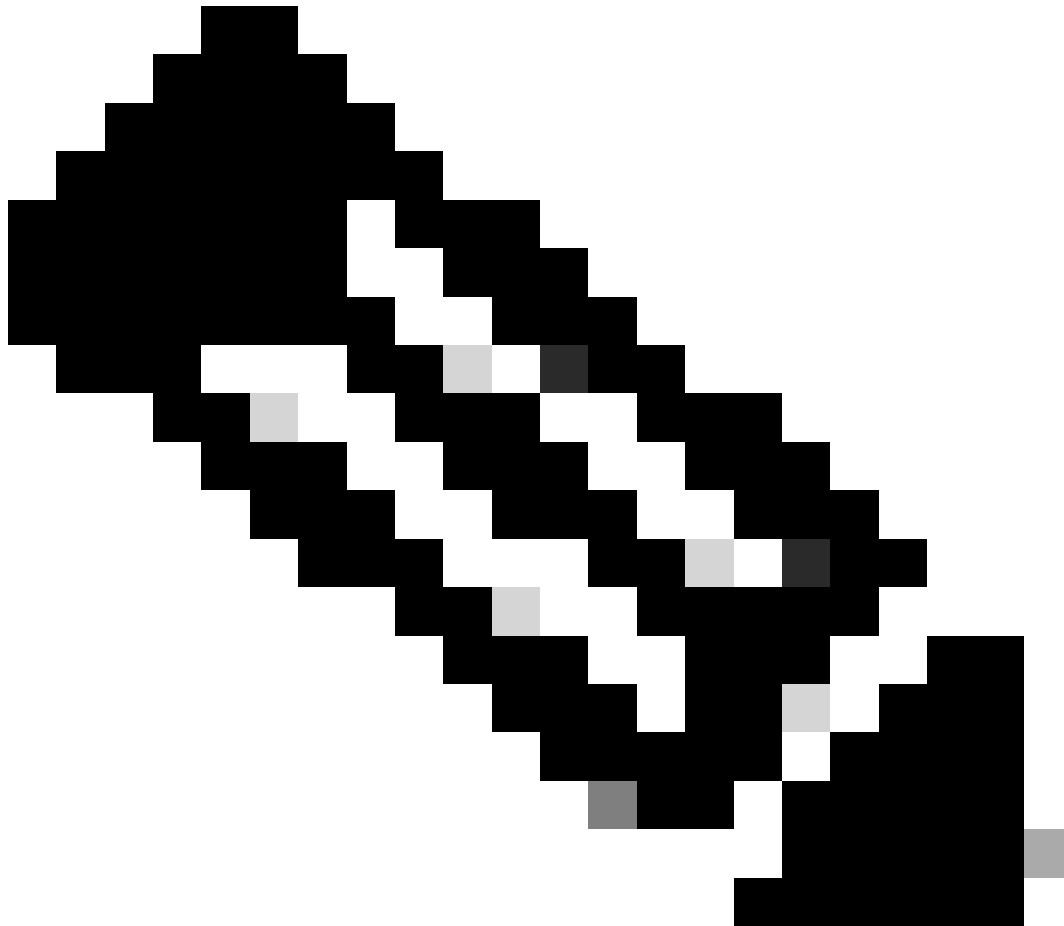
Na lista suspensa User Identity Groups, selecione o grupo IseUsers.



Clique em Usar.

Por fim, selecione o Result Authorization Profile que recebe a parte de autenticações deste grupo de identidade.

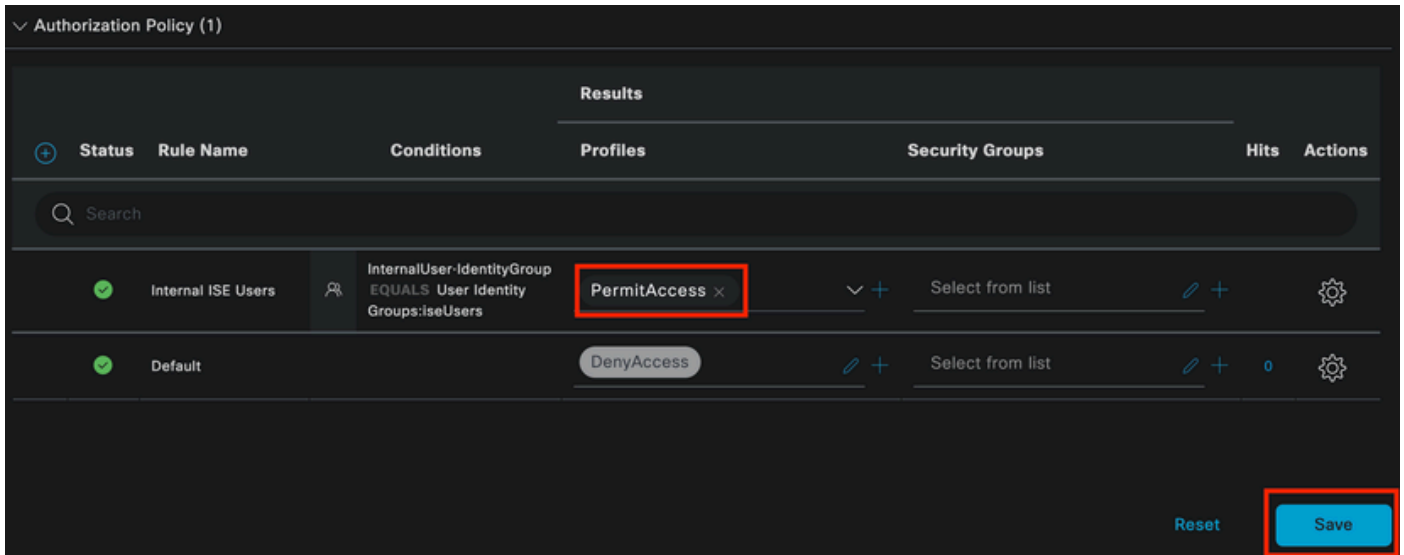
---



Observação: observe que as autenticações que chegam ao ISE e estão atingindo esse conjunto de políticas Wired Dot1x que não fazem parte do Users Identity Group ISEUsers, agora atingem a política padrão AuthorizationPolicy. Isso tem o resultado do perfil DenyAccess.

---

O ISE é pré-configurado com o perfil Permit Access. Selecione-o.



Política de Autorização Concluída

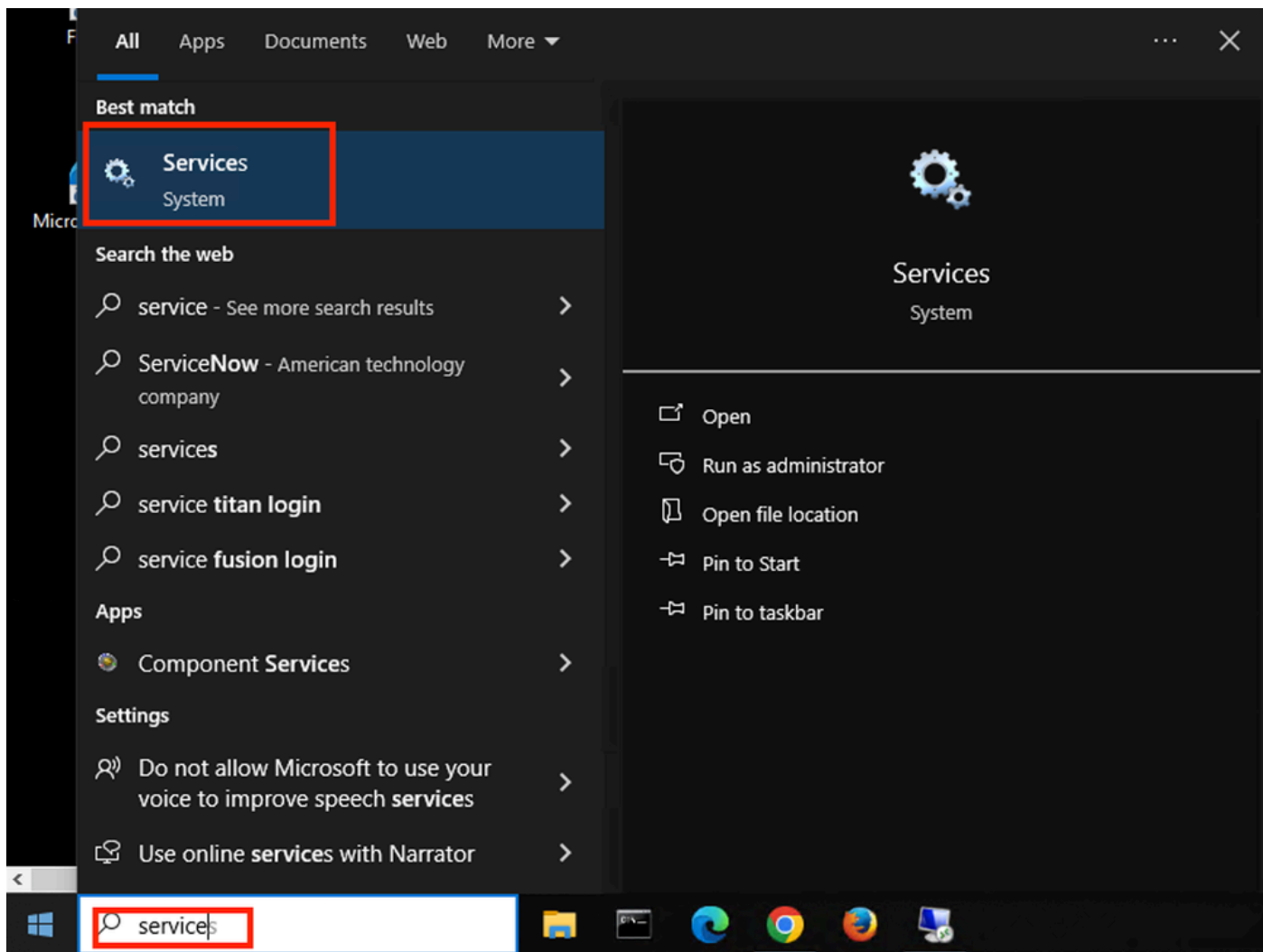
Click Save.

A configuração do ISE está concluída.

Etapa 3. Configuração do Solicitante Nativo do Windows

3. a. Ative Wired dot1x no Windows.

Na Barra de Pesquisa do Windows, abra Serviços.



Barra de Pesquisa do Windows

Na parte inferior da lista Serviços, localize Wired Autoconfig.

Clique com o botão direito em Wired AutoConfig e selecione Properties.

## Wired AutoConfig Properties (Local Computer)



General Log On Recovery Dependencies

Service name: dot3svc

Display name: Wired AutoConfig

Description: responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X

Path to executable:

C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p

Startup type: Manual

Service status: Stopped

Start

Stop

Pause

Resume

You can specify the start parameters that apply when you start the service from here.

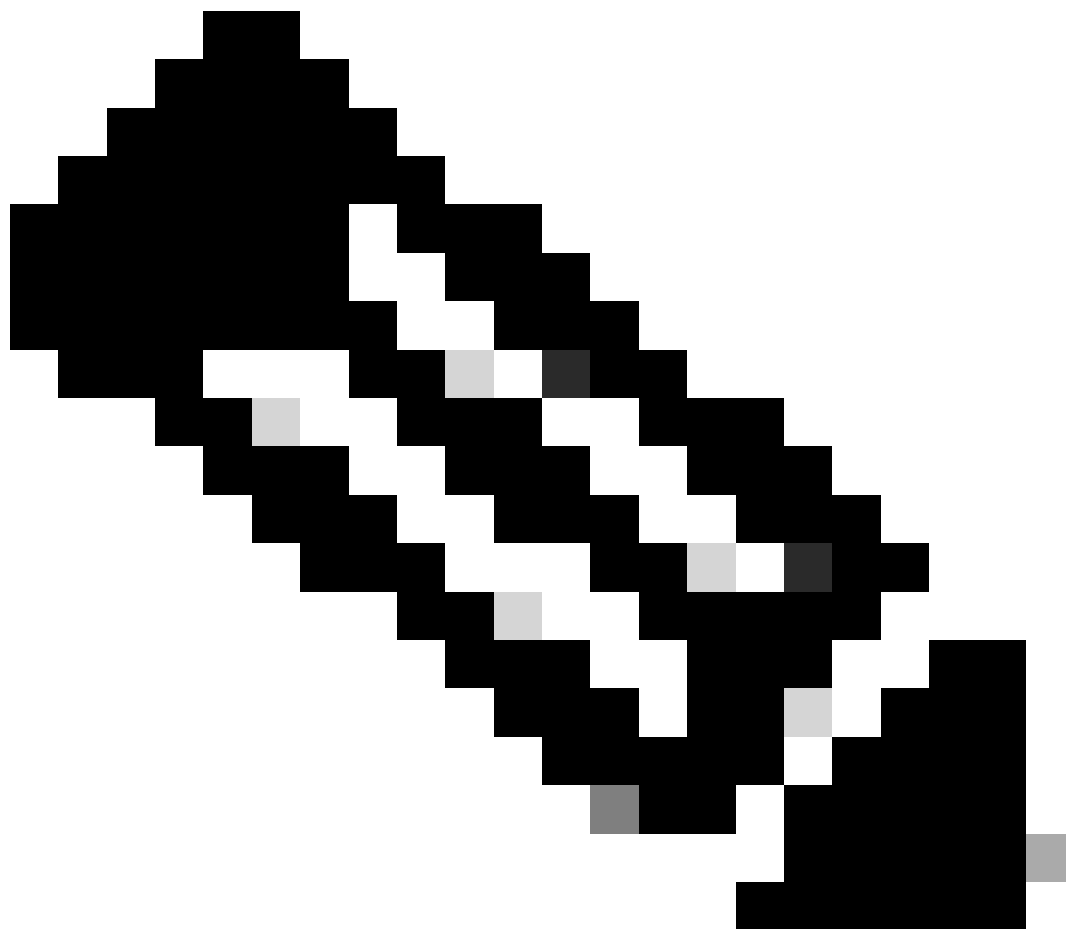
Start parameters:

OK

Cancel

Apply





Observação: o serviço Wired AutoConfig (DOT3SVC) é responsável por executar a autenticação IEEE 802.1X em interfaces Ethernet.

---

O tipo de inicialização Manual é selecionado.

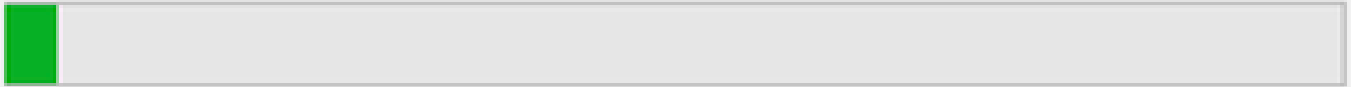
Como o status do serviço é Parado. Clique em Iniciar.

## Service Control



Windows is attempting to start the following service on Local Computer...

Wired AutoConfig



Close

*Controle de serviços*

Em seguida, clique em OK.

O serviço está em execução depois disso.

	Windows Update	Enables the ...	Running	Manual (Trig...	Local Syste...
	Windows Update Medic Service	Enables rem...		Manual	Local Syste...
	WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Running	Manual	Local Service
	Wired AutoConfig	The Wired A...	Running	Manual	Local Syste...
	WLAN AutoConfig	The WLANS...		Manual	Local Syste...
	WMI Performance Adapter	Provides pe...		Manual	Local Syste...
	Work Folders	This service ...		Manual	Local Service

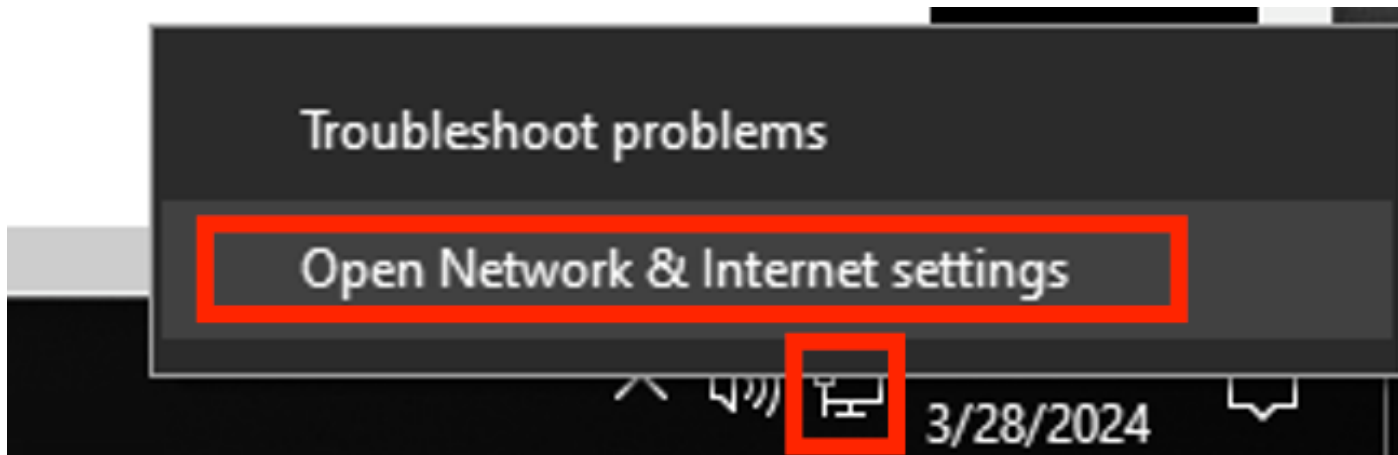
*Serviço de configuração automática com fio*

3. b. Configure a interface do laptop Windows que está conectada ao NAD Authenticator (ISR 1100).

Na barra de tarefas, localize o canto direito e use o ícone do computador.

Clique duas vezes no ícone do computador.

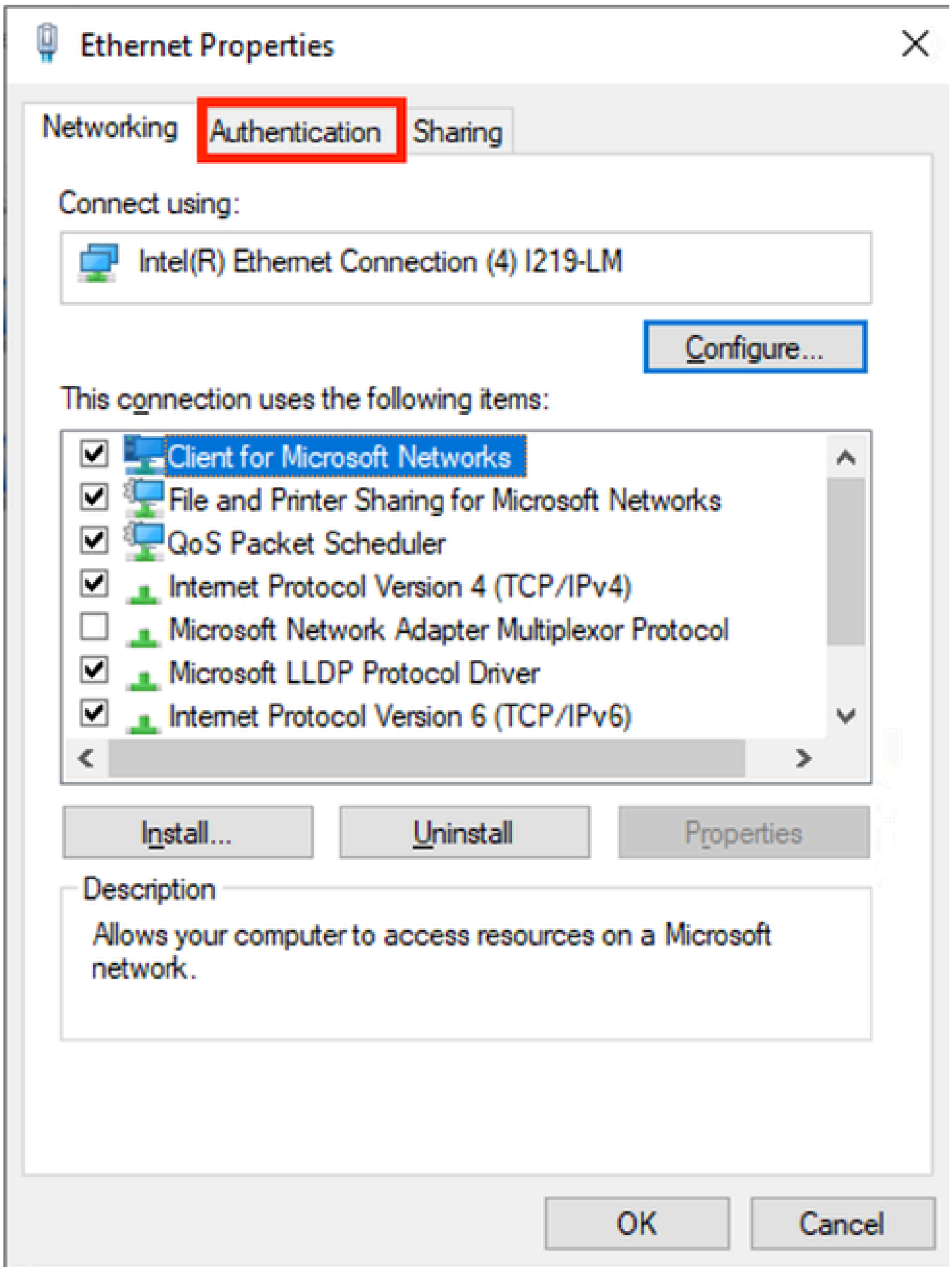
Selecione Open Network & Internet settings.



*Barra de Tarefas do Windows*

Quando a janela Conexões de rede for aberta, clique com o botão direito do mouse na interface Ethernet que está conectada ao ISR Gig 0/1/0. Clique na opção Properties.

Clique na guia Authentication.



Propriedades Ethernet da interface

Marque a caixa de seleção Enable IEEE 802.1X authentication.



## Ethernet Properties



Networking

Authentication

Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) ▾

Settings

Remember my credentials for this connection each time I'm logged on

Fallback to unauthorized network access

Additional Settings...

OK

Cancel

Propriedades Ethernet de Autenticação

Selecione EAP protegido (PEAP).

Desmarque a opção Lembrar minhas credenciais para esta conexão sempre que eu fizer logon.

Clique em Configurações.

## Protected EAP Properties



When connecting:

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1;srv2;. \*\.srv3\.com):

Trusted Root Certification Authorities:

- AAA Certificate Services
- Baltimore CyberTrust Root
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert Global Root G2

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Configure...

Enable Fast Reconnect

Disconnect if server does not present cryptobinding TLV

Enable Identity Privacy

OK

Cancel

Interface: GigabitEthernet0/1/0  
IIF-ID: 0x08767C0D  
MAC Address: 8c16.450d.f42b  
IPv6 Address: Unknown  
IPv4 Address: Unknown  
User-Name: iseiscool <----- The username configured for Windows Native Supplicant  
Status: Authorized <----- An indication that this session was authorized by the PSN  
Domain: DATA  
Oper host mode: multi-auth  
Oper control dir: both  
Session timeout: N/A  
Common Session ID: 22781F0A0000000C83E28461  
Acct Session ID: 0x00000003  
Handle: 0xc6000002  
Current Policy: POLICY\_Gi0/1/0

Local Policies:

Service Template: DEFAULT\_LINKSEC\_POLICY\_SHOULD\_SECURE (priority 150)  
Security Policy: Should Secure

Server Policies:

Method status list:

Method	State
dot1x	Authc Success <----- An indication that dot1x is used for this authentication



Router#

Logs ISE

Navegue até a guia Operations > Radius > Live logs.

Filtre pela identidade do nome de usuário, neste exemplo, o nome de usuário isisicool é usado.

The screenshot shows the Cisco ISE Operations - RADIUS Live Logs interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (1), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). A table below displays log entries. The table has columns: Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint Name, Authentication Policy, and Authn. Two entries are shown, both with 'Isisicool' in the Identity column and 'Wired >> Internal Authentication' in the Authentication Policy column. The 'Identity' and 'Authentication Policy' columns are highlighted with red boxes. At the bottom, it says 'Last Updated: Thu Mar 28 2024 01:29:12 GMT-0600 (Central Standard Time)' and 'Records Shown: 2'.

Livlogs do ISE

The screenshot shows the Cisco ISE Operations - RADIUS Live Logs interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (1), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). A table below displays log entries. The table has columns: Authorization Policy, Authoriz..., IP Address, Network De..., Device Port, Identity Group, Posture..., and Server. Two entries are shown. The first entry has 'Wired >> Internal ISE Users' in the Authorization Policy column, 'PermitAcc...' in the Authoriz... column, 'ISR1100' in the Network De... column, 'GigabitEthernet0/1/0' in the Device Port column, 'User Identity Groups:iseUsers' in the Identity Group column, and 'PSN01' in the Server column. The second entry has 'Wired >> Internal ISE Users' in the Authorization Policy column, 'PermitAcc...' in the Authoriz... column, 'ISR1100' in the Network De... column, 'GigabitEthernet0/1/0' in the Device Port column, 'User Identity Groups:iseUsers' in the Identity Group column, and 'PSN01' in the Server column. The 'Authorization Policy', 'Authoriz...', 'Network De...', 'Device Port', 'Identity Group', and 'Server' columns are highlighted with red boxes. At the bottom, it says 'Last Updated: Thu Mar 28 2024 01:34:19 GMT-0600 (Central Standard Time)' and 'Records Shown: 2'.

Livlogs do ISE

Observe que, nessa visualização rápida, os logs dinâmicos fornecem informações importantes:

- Carimbo de data/hora da autenticação.
- Identidade usada.
- Endereço MAC do ponto final.
- Política definida e Política de Autenticação atingida.
- Política definida e Política de Autorização atingida.
- Resultado do Perfil de Autorização.
- O dispositivo de rede que envia a solicitação Radius ao ISE.
- A interface à qual o ponto de extremidade está conectado.
- O Grupo de Identidade do usuário que foi autenticado.
- O Nó do Servidor de Políticas (PSN) que tratou a autenticação.

## Troubleshooting

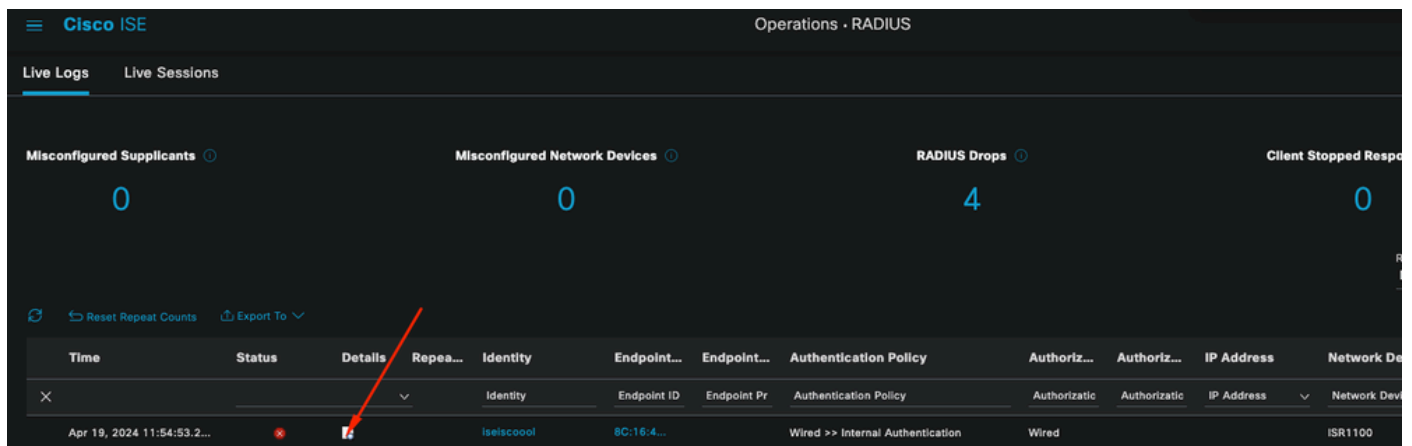
### 1 - Lendo detalhes do Live Log do ISE

Navegue até a guia Operations > Radius > Live logs, filtre por Auth status: Failed OU pelo nome de usuário usado OU pelo endereço MAC OU pelo Network Access Device usado.

Acesse Operations > Radius > Live logs > Desired authentication > Live log details.

Na mesma página, depois que a autenticação for filtrada, clique no ícone Pesquisar.

Primeiro cenário: o usuário digita seu nome de usuário com um erro de digitação.



Abrindo Detalhes do Live Log

Uma vez que o detalhe do registro em tempo real é aberto, você pode ver que a autenticação falhou e também o nome de usuário usado é listado.

Overview	
Event	5400 Authentication failed
Username	iseiscool
Endpoint Id	<ENDPOINT MAC ADDRESS>#
Endpoint Profile	
Authentication Policy	Wired >> Internal Authentication
Authorization Policy	Wired
Authorization Result	

#### Seção Visão Geral

Em seguida, nos mesmos detalhes do registro em tempo real, na seção Authentication Details (Detalhes de autenticação), pode ser encontrado o Failure Reason, Root Cause (Motivo da falha) e Resolution do erro.

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resolution settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).
Username	iseiscool

#### Detalhes da autenticação

Nesse cenário, o motivo da falha da autenticação é porque o nome de usuário tem um erro de digitação, no entanto, esse mesmo erro seria apresentado se o usuário não fosse criado no ISE ou se o ISE não fosse capaz de validar se o usuário existe em outros armazenamentos de identidade, por exemplo, LDAP ou AD.

#### Seção Etapas

15041 Evaluating Identity Policy

15013 Selected Identity Source - Internal Users ←

24210 Looking up User in Internal Users IDStore - iseiscoool ←

24216 The user is not found in the internal users identity store ←

22056 Subject not found in the applicable identity store(s) ←

22058 The advanced option that is configured for an unknown user is used

22061 The 'Reject' advanced option is configured in case of a failed authentication request ←

11815 Inner EAP-MSCHAP authentication failed ←

11520 Prepared EAP-Failure for inner EAP method

22028 Authentication failed and the advanced options are ignored

12305 Prepared EAP-Request with another PEAP challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12304 Extracted EAP-Response containing PEAP challenge-response

61025 Open secure connection with TLS peer

12307 PEAP authentication failed ←

11504 Prepared EAP-Failure

11003 Returned RADIUS Access-Reject ←

Seção Etapa de Detalhes do Log ao Vivo

A seção de etapas descreve em detalhes o processo que o ISE executou durante a conversação

do RADIUS.

Você pode encontrar informações aqui como:

- Como a conversa foi iniciada.
- processo de handshake SSL.
- O método EAP foi negociado.
- Processo do método EAP.

Neste exemplo, pode-se ver que o ISE acabou de fazer check-in das identidades internas para essa autenticação. O usuário não foi encontrado e, por esse motivo, o ISE enviou como resposta um Access-Reject.

Segundo cenário: o administrador do ISE desabilitou o PEAP dos protocolos Policy Set Allowed.

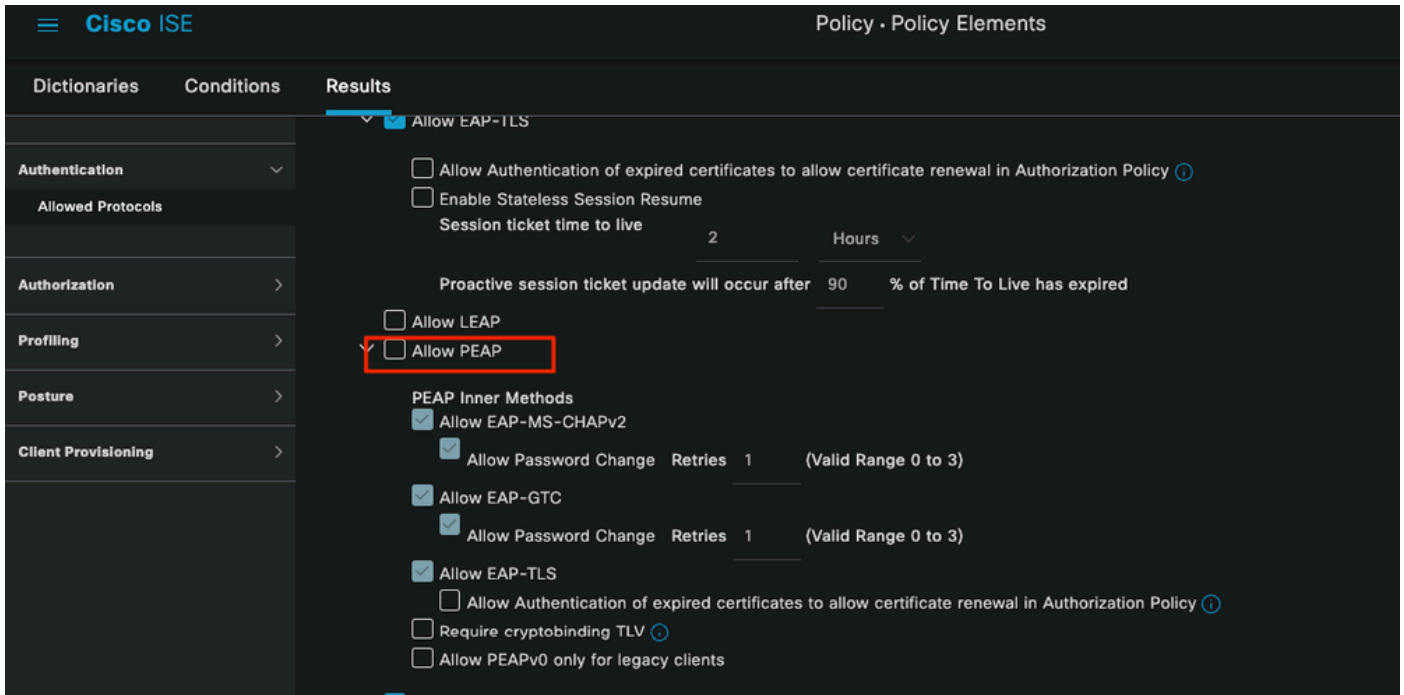
## 2 - PEAP desativado

Quando o detalhe do registro ao vivo da falha da sessão é aberto, a mensagem de erro "PEAP não é permitido nos protocolos permitidos" é exibida.

Event	5400 Authentication failed
Failure Reason	12303 Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols
Resolution	Ensure that the PEAP protocol is allowed by ISE in Allowed Protocols.
Root cause	The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use PEAP instead. However, PEAP is not allowed in Allowed Protocols.
Username	iseiscool

Relatório de Detalhes do Log ao Vivo

Esse erro é fácil de resolver, a resolução é navegar para Policy > Policy Elements > Authentication > Allowed Protocols. Verifique se a opção Allow PEAP está desativada.



Seção de protocolos permitidos

Terceiro cenário: a autenticação falha porque o ponto de extremidade não confia no certificado ISE.

Navegue até os detalhes do log ao vivo. Localize o registro da autenticação que falhar e verifique os detalhes do log ao vivo.

## Authentication Details

Source Timestamp 2024-04-20 04:37:42.007

Received Timestamp 2024-04-20 04:37:42.007

Policy Server ISE PSN

Event 5411 Supplicant stopped responding to ISE

Failure Reason 12934 Supplicant stopped responding to ISE during PEAP tunnel establishment

Resolution Check whether the proper server certificate is installed and configured for EAP in the Local Certificates page ( Administration > System > Certificates > Local Certificates ). Also ensure that the certificate authority that signed this server certificate is correctly installed in client's supplicant. Check the previous steps in the log for this EAP-TLS conversation for a message indicating why the handshake failed. Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information.

Root cause PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

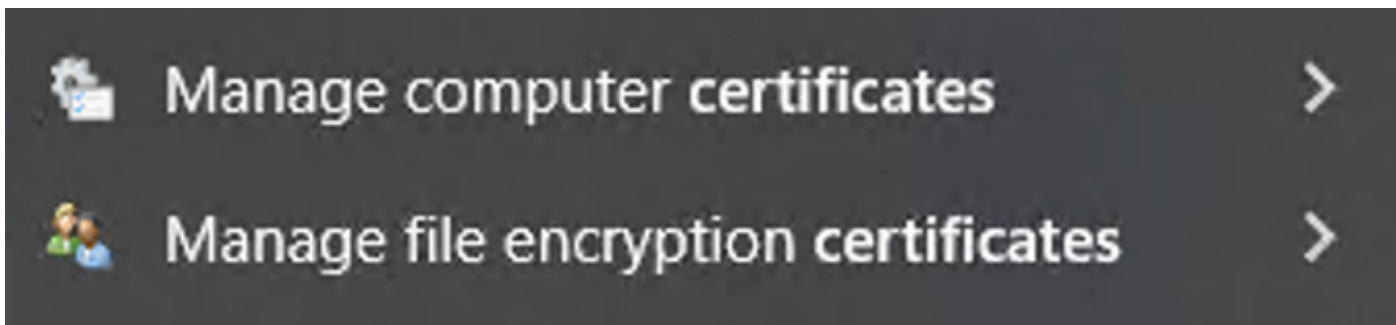
Username iseiscool

### Detalhes do Log ao Vivo

O ponto de extremidade está rejeitando o certificado usado para o estabelecimento de túnel PEAP.

Para resolver esse problema, no endpoint do Windows onde você tem o problema, verifique se a cadeia de CA que assinou o certificado ISE está na seção do Windows Gerenciar certificados de usuário > Autoridades de certificação raiz confiáveis OU Gerenciar certificados de computador > Autoridades de certificação raiz confiáveis.

Você pode acessar esta seção de configuração em seu dispositivo Windows pesquisando-os na barra de pesquisa do Windows.

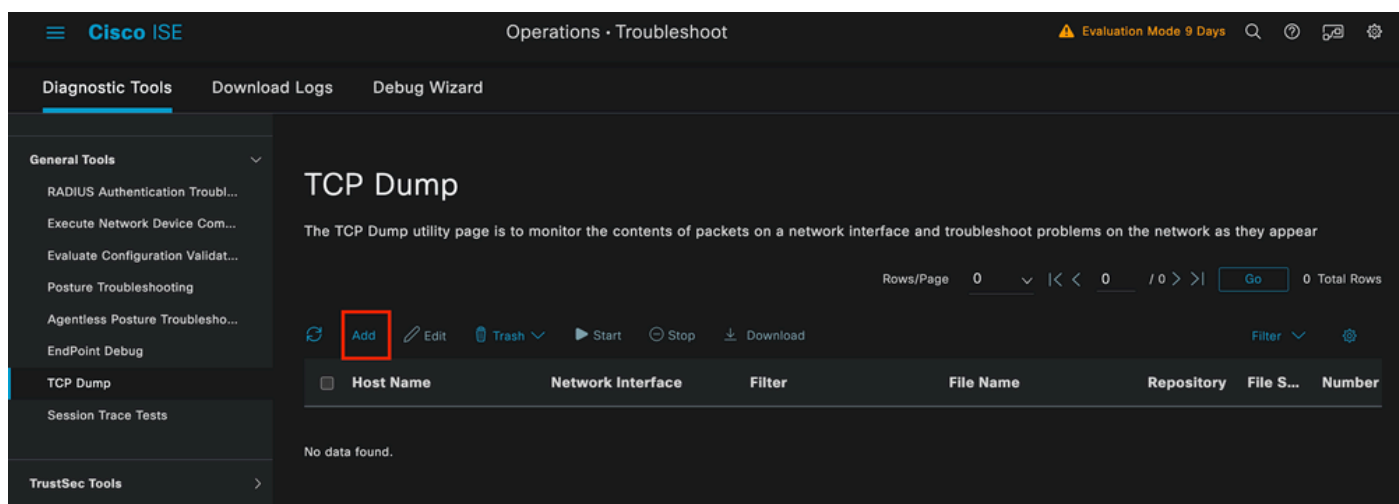


Resultados da Barra do Windows Search

### 3 - Ferramenta de despejo TCP do ISE (captura de pacotes)

A análise de captura de pacotes é essencial ao solucionar problemas. As capturas de pacotes diretamente do ISE podem ser feitas em todos os nós e em qualquer interface dos nós.

Para acessar essa ferramenta, navegue para Operações > Ferramentas de diagnóstico > Ferramentas gerais > Despejo TCP.



Seção Despejo TCP

Clique no botão Add para iniciar a configuração de um pcap.



### Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name\*

ISE PSN

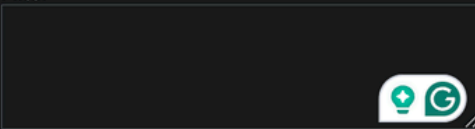


Network Interface\*

GigabitEthernet 0 [Up, Running]



Filter





E.g: ip host 10.77.122.123 and not  
10.177.122.119

File Name

ISEPCAP

Criação de despejo TCP

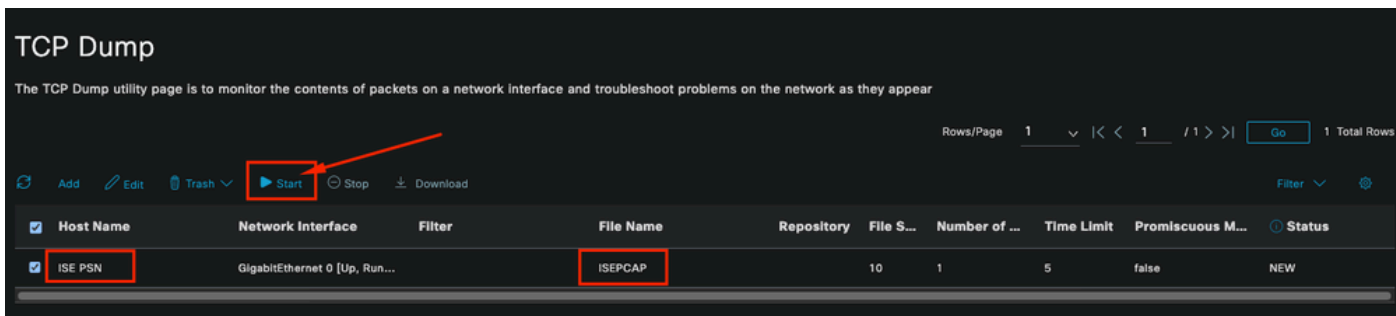
The screenshot shows a configuration window with a dark background. At the top left, there is a 'Repository' dropdown menu with a downward arrow and an information icon. Below it are three input fields: 'File Size' with the value '10' and unit 'Mb', 'Limit to' with the value '1' and unit 'File(s)', and 'Time Limit' with the value '5' and unit 'Minute(s)'. Each of these fields has an information icon to its right. At the bottom left, there is a checkbox labeled 'Promiscuous Mode' which is currently unchecked. At the bottom right, there are three buttons: 'Cancel', 'Save' (highlighted with a red border), and 'Save and Run'.

#### Seção Despejo TCP

Para criar um pcap no ISE, estes são os dados que você deve inserir:

- Selecione o nó no qual você precisa pegar o pcap.
- Selecione a interface do nó ISE que é usada para o pcap.
- Caso você precise capturar determinado tráfego, use os filtros, o ISE fornece alguns exemplos.
- Nomeie o pcap. Neste cenário, usamos ISEPCAP.
- Selecione o repositório, se nenhum repositório for selecionado, a captura será salva no disco local do ISE e poderá ser baixada da GUI.
- Além disso, se necessário, modifique o tamanho do arquivo pcap.
- Se necessário, use mais de 1 arquivo, portanto, se o pcap exceder o tamanho do arquivo, um novo arquivo será criado posteriormente.
- Estenda o tempo de captura de tráfego para o pcap, se necessário.

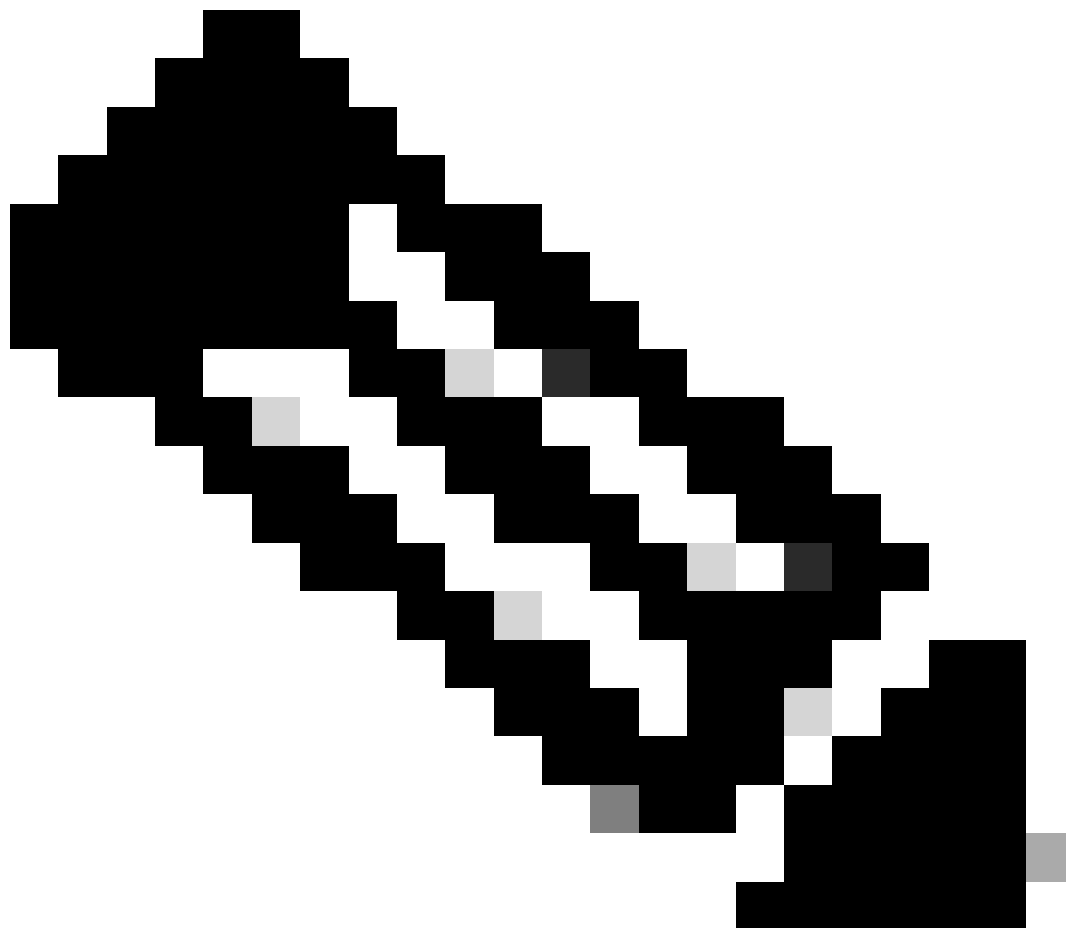
Por fim, clique no botão Save.



## Seção Despejo TCP

Em seguida, quando estiver pronto, selecione o pcap e clique no botão Start.

Depois de clicar em Iniciar, a coluna Status é alterada para o estado EXECUTANDO.



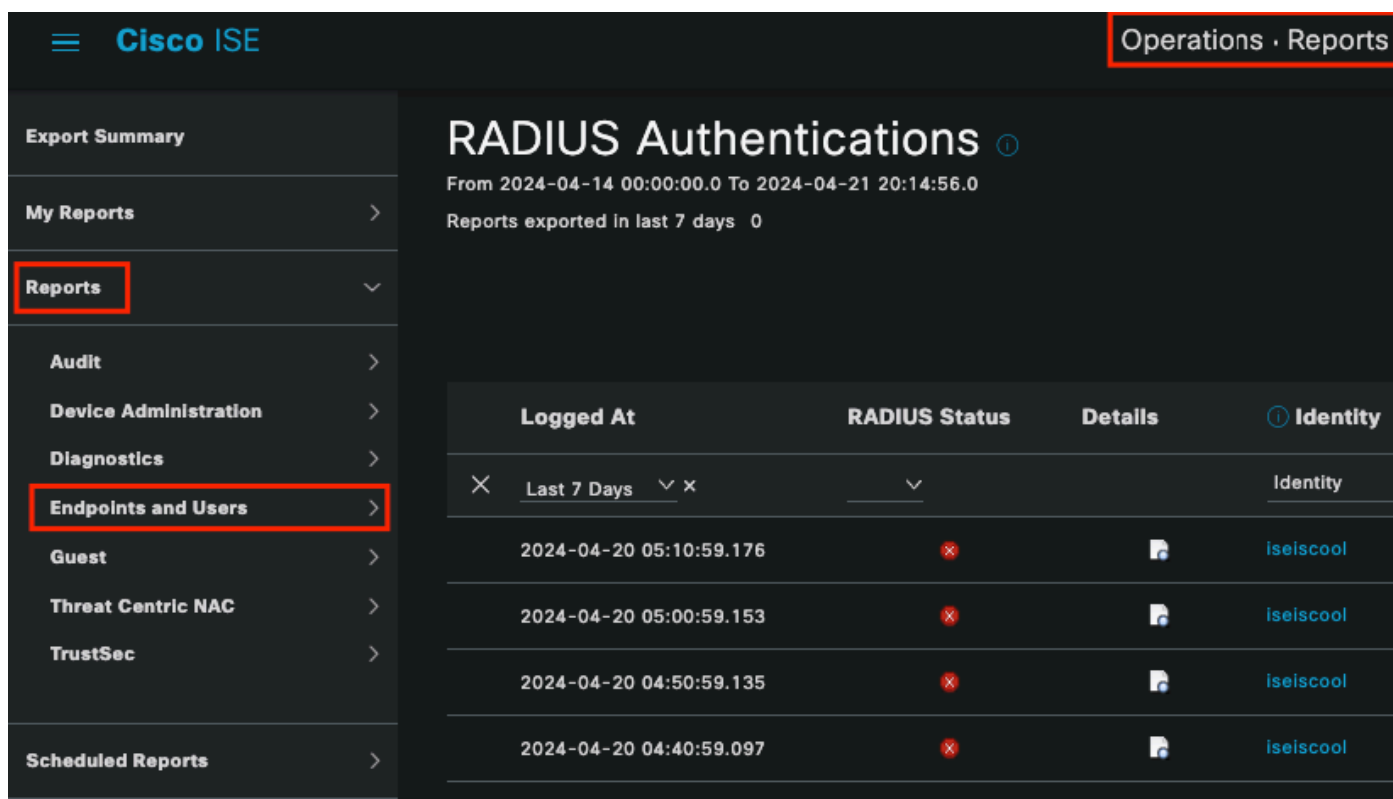
Observação: enquanto o PCAP estiver no estado RUNNING, replique o cenário de falha ou o comportamento que você precisa capturar. Uma vez concluídos, os detalhes do RADIUS, a conversação são visíveis no PCAP.

Quando os dados necessários forem capturados enquanto o PCAP estiver em execução, conclua a coleta do pcap. Selecione-a novamente e clique em Parar.

### 3 a 1 relatórios do ISE

Caso seja necessária uma análise mais profunda, o ISE oferece relatórios úteis para investigar eventos passados.

Para localizá-los, navegue até Operações > Relatórios > Relatórios > Endpoints e Usuários



The screenshot displays the Cisco ISE web interface. The top right corner shows 'Operations · Reports'. The left sidebar contains a navigation menu with 'Reports' and 'Endpoints and Users' highlighted. The main content area is titled 'RADIUS Authentications' and shows a table of authentication events. The table has columns for 'Logged At', 'RADIUS Status', 'Details', and 'Identity'. The data shows four failed authentication attempts for the user 'iseiscool' on 2024-04-20.

Logged At	RADIUS Status	Details	Identity
2024-04-20 05:10:59.176	×		iseiscool
2024-04-20 05:00:59.153	×		iseiscool
2024-04-20 04:50:59.135	×		iseiscool
2024-04-20 04:40:59.097	×		iseiscool

Seção Relatórios do ISE

## Endpoints and Users



Agentless Posture

Authentication Summary

Client Provisioning

Current Active Sessions

Endpoint & Logical Profi...

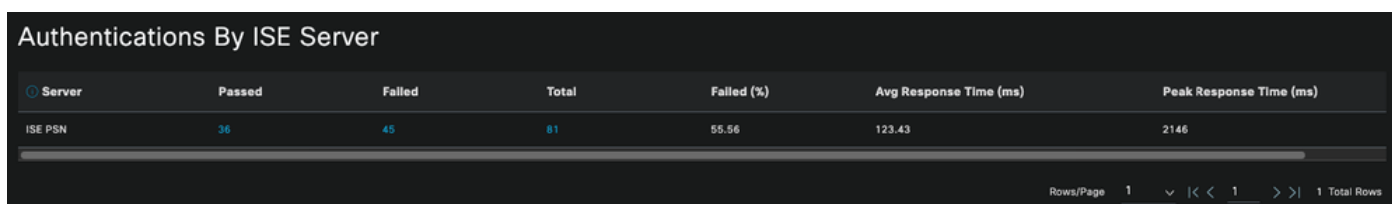
Endpoint Scripts Provisi...

External Mobile Device ...

Manual Certificate Provi...

PassiveID

: na implantação usada para este documento, apenas uma PSN foi usada; no entanto, para implantações maiores, esses dados são úteis para ver se o balanceamento de carga é necessário.



Server	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak Response Time (ms)
ISE PSN	36	45	81	55.56	123.43	2146

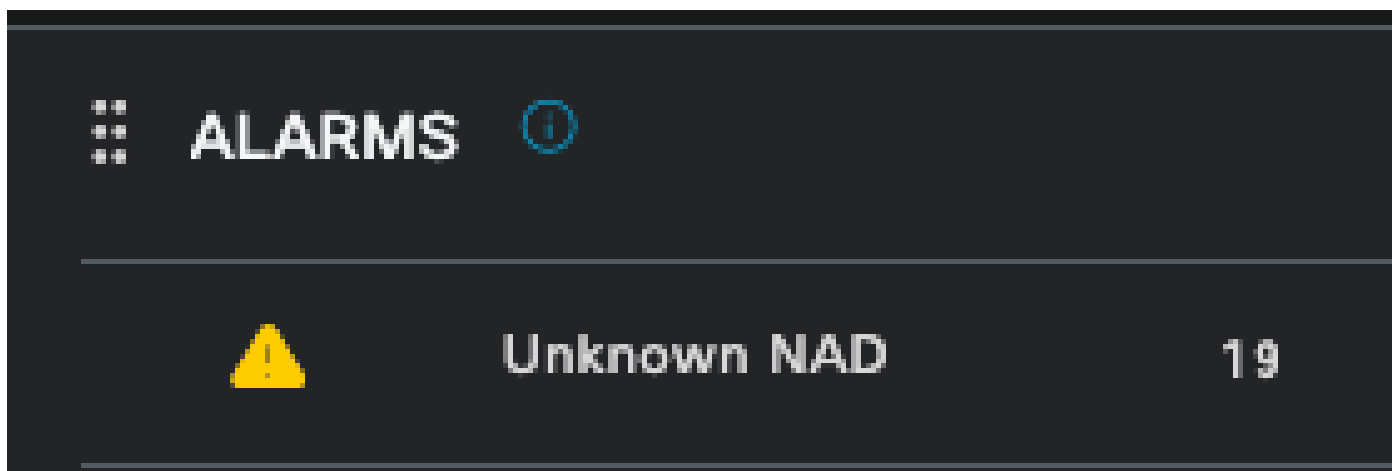
Autenticações pelo servidor ISE

#### 4 - Alarmes ISE

No Painel do ISE, a seção Alarmes exibe os problemas de implantação.

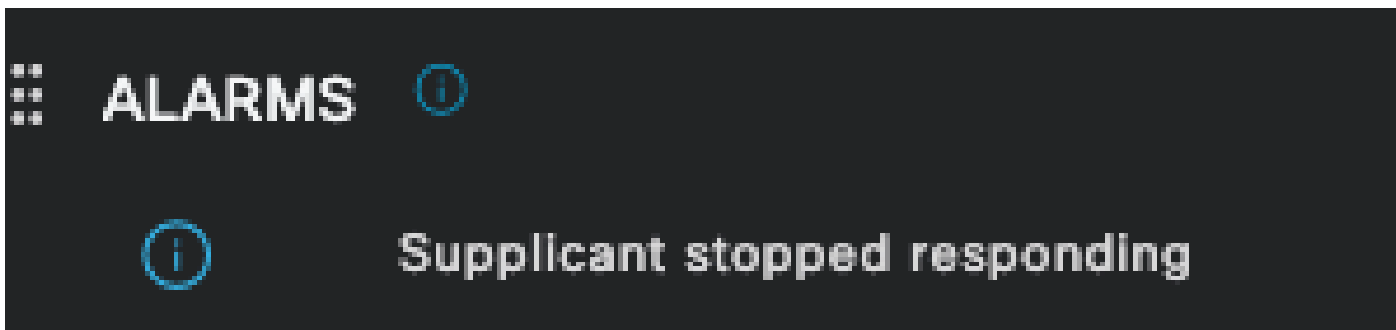
Aqui estão vários alarmes ISE que ajudam na solução de problemas.

NAD desconhecido — Esse alarme é mostrado quando há um dispositivo de rede que autentica um endpoint e acessa o ISE. Mas o ISE não confia nele e desconecta a conexão RADIUS. Os motivos mais comuns são que o dispositivo de rede não foi criado ou o IP que o dispositivo de rede está usando não é o mesmo que o ISE registrou.



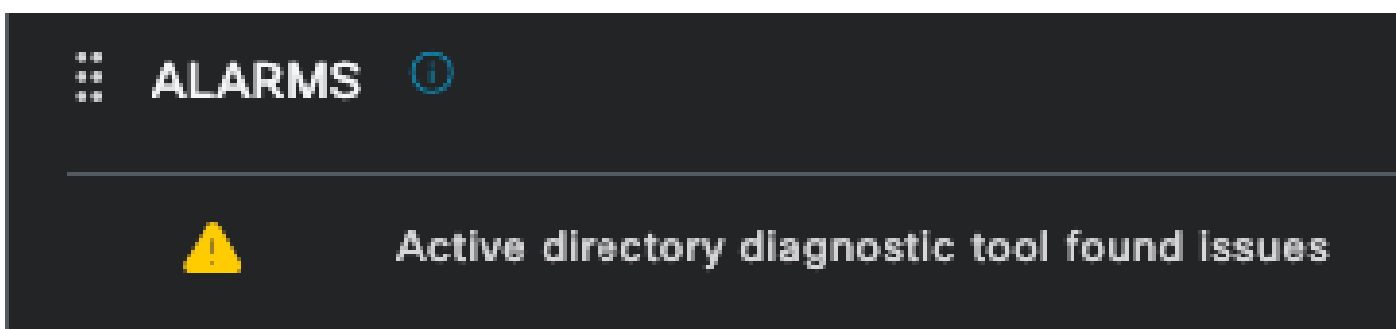
NAD desconhecido

Supplicant Stopped Responding — Este alarme ocorre quando há um problema com a comunicação do suplicante, na maioria das vezes devido a um erro de configuração no suplicante que precisa ser verificado e investigado no lado do endpoint.



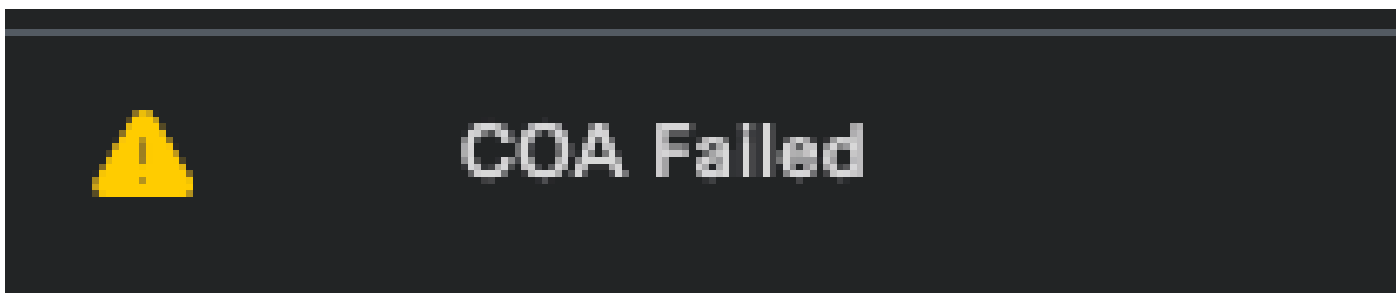
O Requerente Parou de Responder

A ferramenta de diagnóstico do Ative Directory encontrou problemas — quando o Ative Directory é usado para validar a identidade do usuário, se começar a ter problemas com o processo de comunicação ou se a conexão for interrompida, você verá este alarme. Em seguida, você perceberia por que as autenticações de que a identidade existe no AD falham.



Falha no diagnóstico do AD

Falha no COA (Change of Authorization) — Vários fluxos no ISE usam CoA; esse alarme informa se foram encontrados problemas durante a comunicação da porta de CoA com qualquer dispositivo de rede.



Falha de Coa

## 5 - Configuração de depuração do ISE e coleta de logs

Para continuar com os detalhes do processo de autenticação, você deve habilitar os próximos componentes em DEBUG para problemas de mab e dot1x:

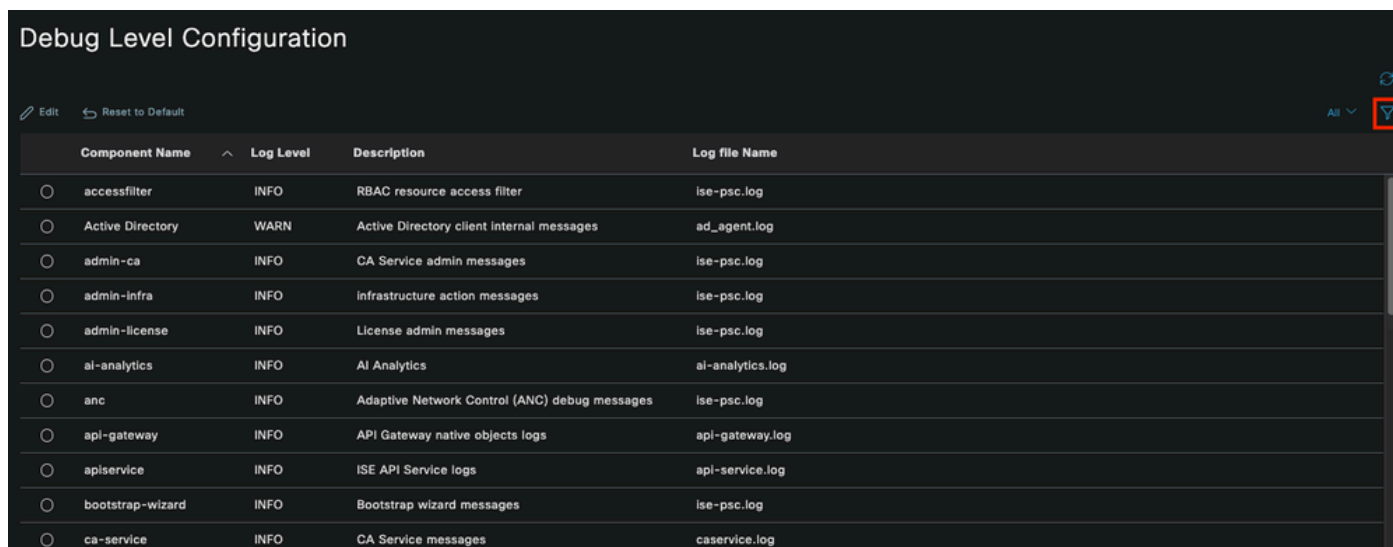
Problema: dot1x/mab

Atributos a serem definidos para o nível de depuração.

- runtime-AAA (prrt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

Para habilitar os componentes para o nível DEBUG, primeiro é necessário identificar qual é a PSN que recebe a autenticação que está falhando ou precisa ser investigada. Essas informações podem ser obtidas nos logs ao vivo. Depois disso, você deve ir para o menu ISE > Solução de problemas > Assistente de depuração > Configuração do log de depuração > Selecionar o PSN > Clique no botão Editar.

O próximo menu é exibido. Clique no ícone de filtro:



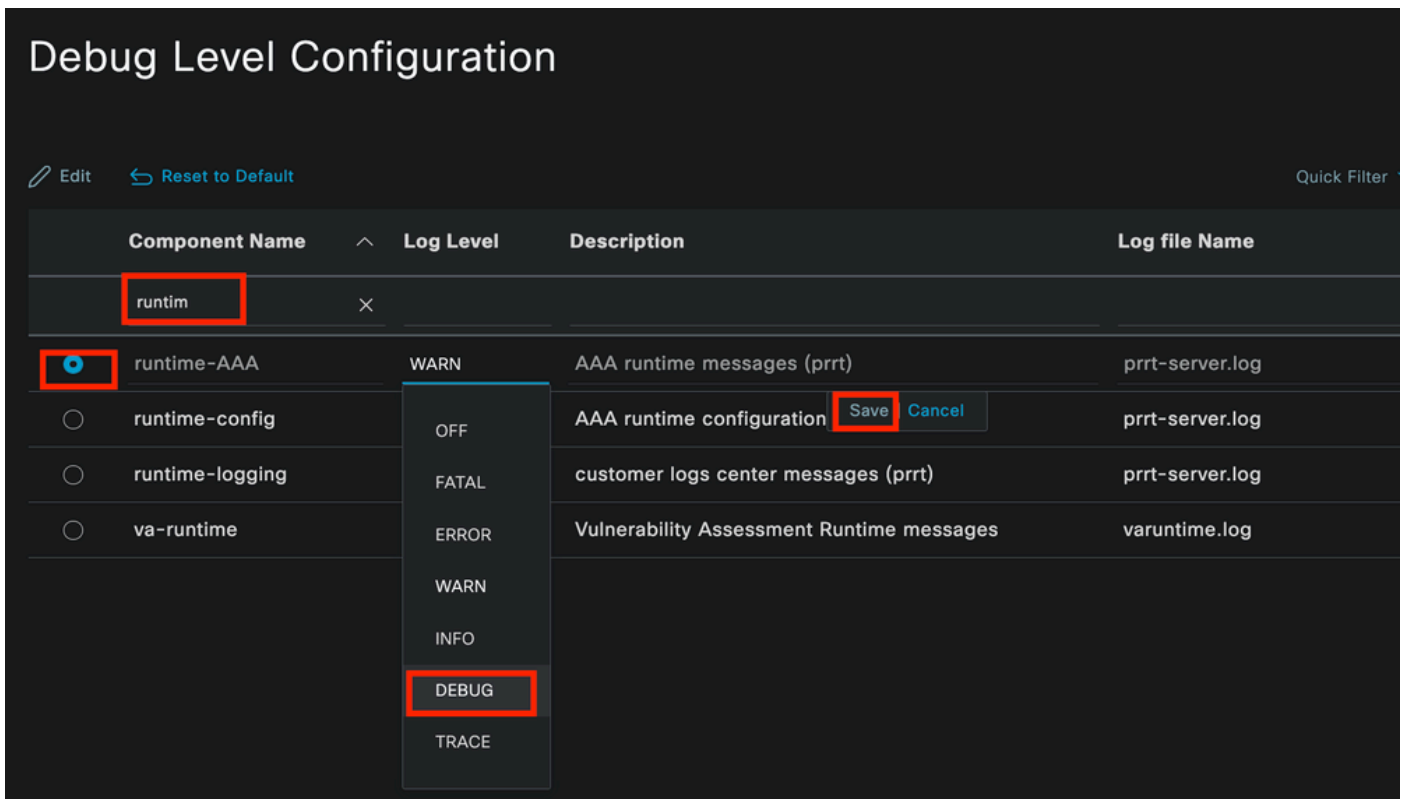
The screenshot shows the 'Debug Level Configuration' page with a table of components. The table has columns for Component Name, Log Level, Description, and Log file Name. A red box highlights the filter icon in the top right corner of the table.

Component Name	Log Level	Description	Log file Name
<input type="radio"/> accessfilter	INFO	RBAC resource access filter	ise-psc.log
<input type="radio"/> Active Directory	WARN	Active Directory client internal messages	ad_agent.log
<input type="radio"/> admin-ca	INFO	CA Service admin messages	ise-psc.log
<input type="radio"/> admin-Infra	INFO	infrastructure action messages	ise-psc.log
<input type="radio"/> admin-license	INFO	License admin messages	ise-psc.log
<input type="radio"/> ai-analytics	INFO	AI Analytics	ai-analytics.log
<input type="radio"/> anc	INFO	Adaptive Network Control (ANC) debug messages	ise-psc.log
<input type="radio"/> api-gateway	INFO	API Gateway native objects logs	api-gateway.log
<input type="radio"/> apiservice	INFO	ISE API Service logs	api-service.log
<input type="radio"/> bootstrap-wizard	INFO	Bootstrap wizard messages	ise-psc.log
<input type="radio"/> ca-service	INFO	CA Service messages	caservice.log

#### Configuração do Log de Depuração

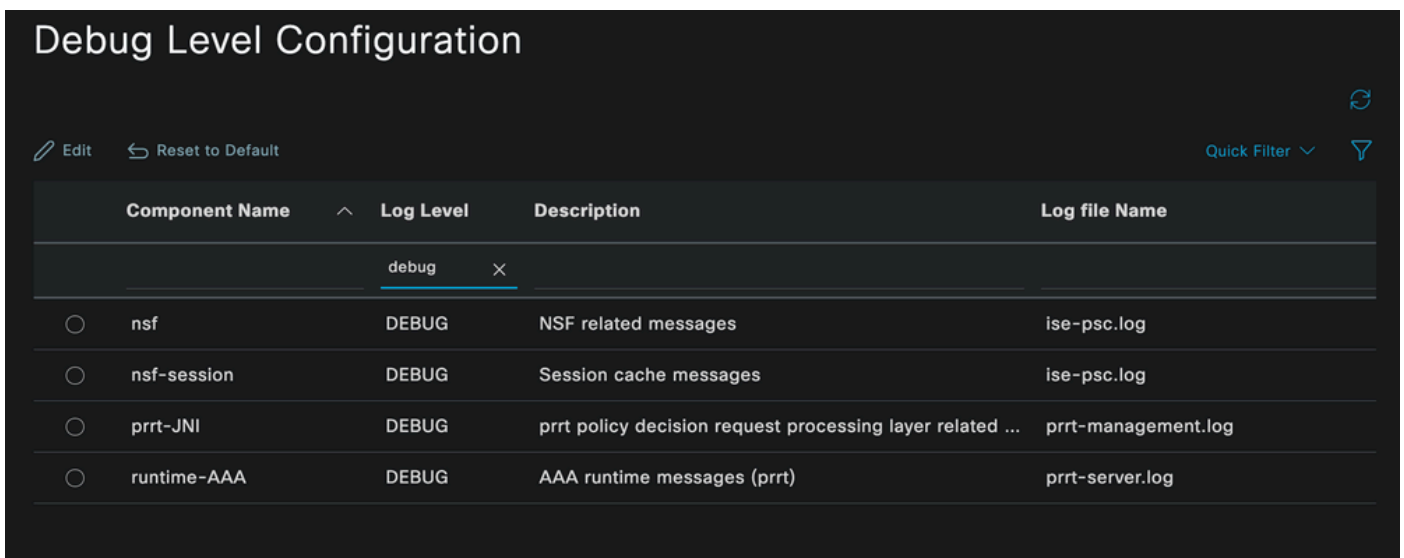
Na coluna Nome do Componente, procure os atributos listados anteriormente. Selecione cada nível de log e altere-o para DEBUG. Salve as alterações.





Configuração de Componente AAA de Tempo de Execução

Quando terminar de configurar cada componente, filtre-os com DEBUG para que você possa ver se todos os componentes foram configurados corretamente.



Configuração do Log de Depuração

Caso haja necessidade de analisar imediatamente os registros, você pode baixá-los navegando até o caminho ISE Menu > Operações > Solução de problemas > Download Logs > Lista de nós do dispositivo > PSN e ativando o DEBUGS > Debug Logs.

Nesse caso, você deve fazer o download para problemas de dot1x e mab nos arquivos prrt-server.log e ise-psc.log. O log que você deve baixar é aquele com a data do último teste.

Basta clicar no arquivo de registro mostrado nesta imagem e baixá-lo (exibido em texto azul).

Support Bundle		Debug Logs	
Debug Log Type	Log File	Description	Size
<input type="checkbox"/> Delete <input type="checkbox"/> Expand All <input type="checkbox"/> Collapse All			
<input checked="" type="checkbox"/> ise-psc (16) (111 MB)			
<input type="checkbox"/>	ise-psc (all logs)	Main ise debug log messages	111 MB
<input type="checkbox"/>	<a href="#">ise-psc.log</a>		5.8 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-03-1</a>		7.0 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-04-1</a>		6.9 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-05-1</a>		6.9 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-06-1</a>		7.0 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-07-1</a>		6.9 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-08-1</a>		6.9 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-09-1</a>		7.6 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-10-1</a>		8.0 MB

Logs de depuração do nó PSN

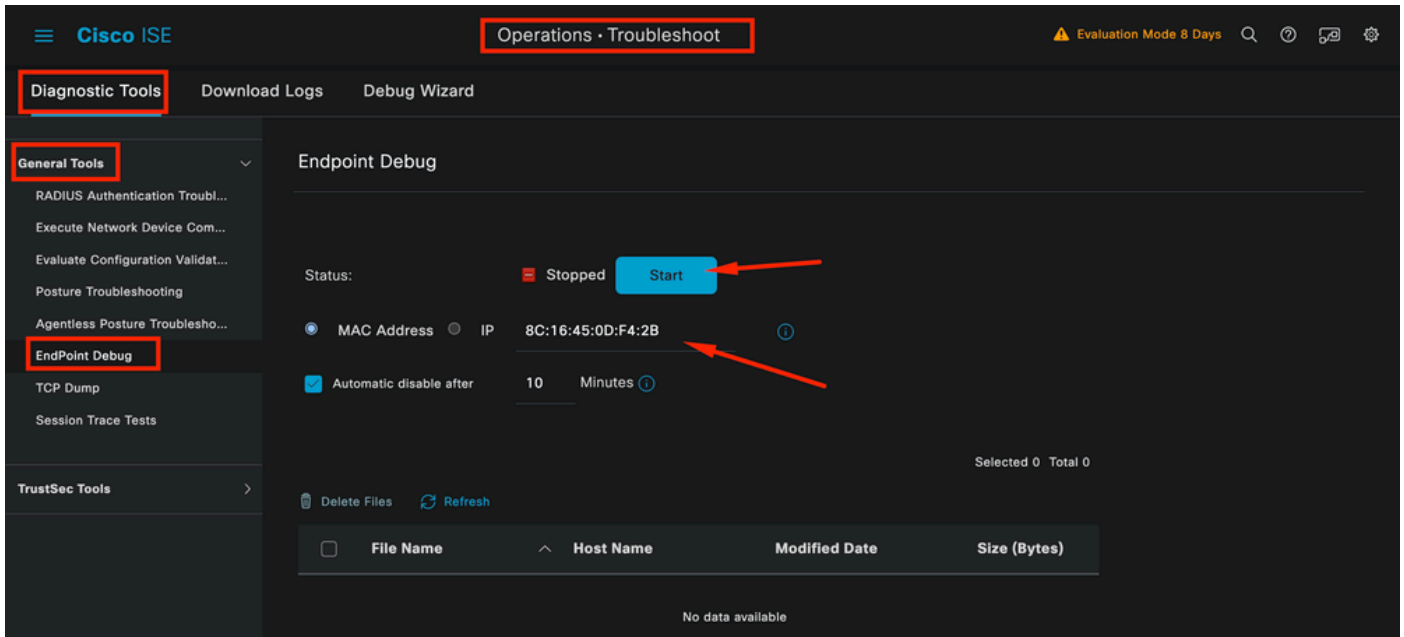
Support Bundle		Debug Logs	
Debug Log Type	Log File	Description	Size
<input type="checkbox"/> Delete <input type="checkbox"/> Expand All <input type="checkbox"/> Collapse All			
<input checked="" type="checkbox"/> prrt-server (1) (7.8 MB)			
<input type="checkbox"/>	prrt-server (all logs)	Protocol Runtime runtime configuration, debug and customer logs messages	7.8 MB
<input type="checkbox"/>	<a href="#">prrt-server.log</a>		7.8 MB
<input type="checkbox"/> pxcloud (4) (20 KB)			

Seção Logs de Depuração

## 6 - Depuração do ISE por endpoint

Há também outra opção para obter logs de DEBUG, por logs de depuração de endpoint com base no endereço MAC ou IP. Você pode usar a ferramenta Depuração de endpoint do ISE.

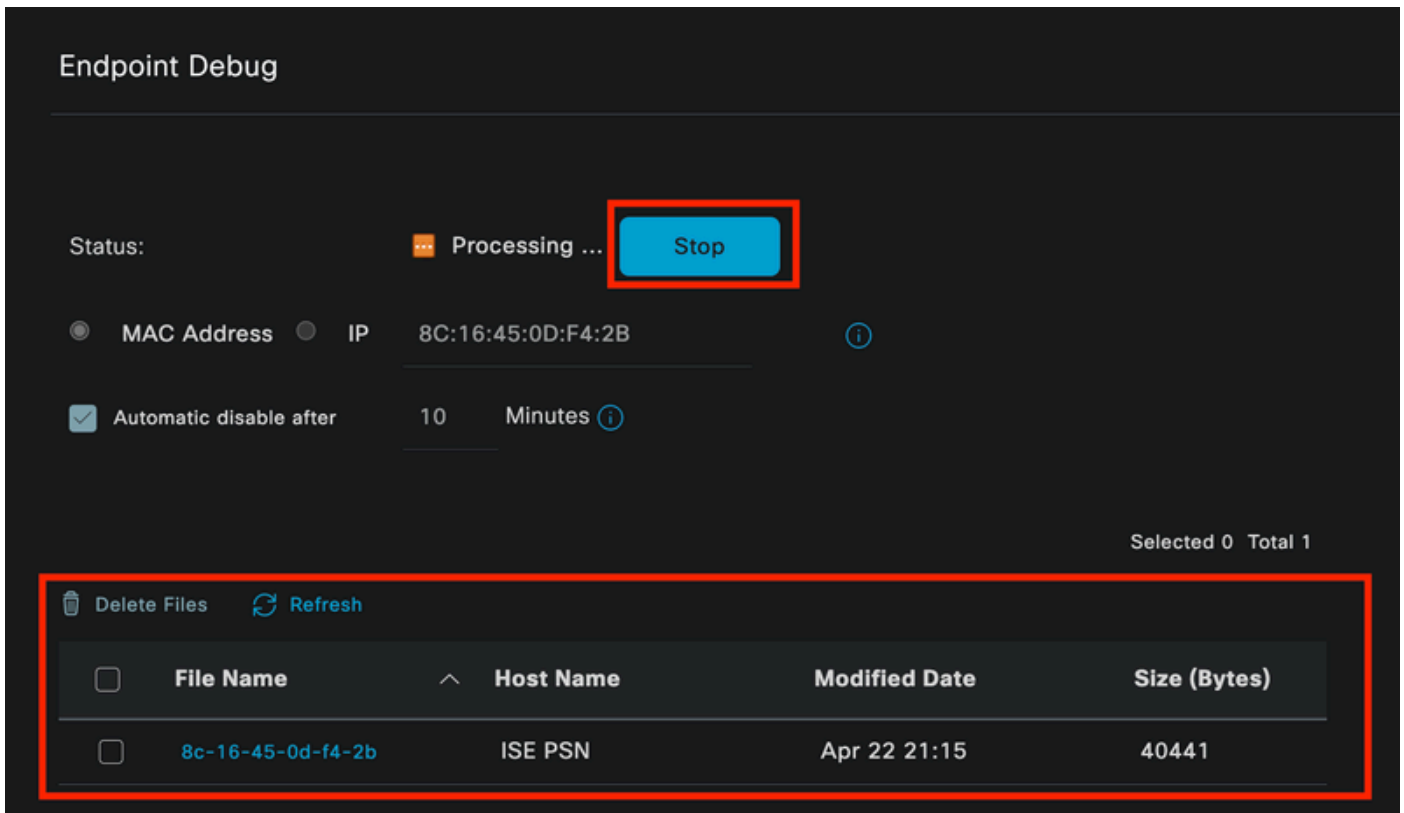
Navegue até o menu ISE > Operações > Solução de problemas > Ferramentas de diagnóstico > Ferramentas gerais > Depuração de endpoint.



Depuração de Ponto Final

Em seguida, insira as informações de endpoint desejadas para iniciar a captura de logs. Clique em Iniciar.

Em seguida, clique em Continuar na mensagem de aviso.



Depuração de Ponto Final

Depois que as informações forem capturadas, clique em Stop.

Clique no nome de arquivo mostrado em azul nesta imagem.

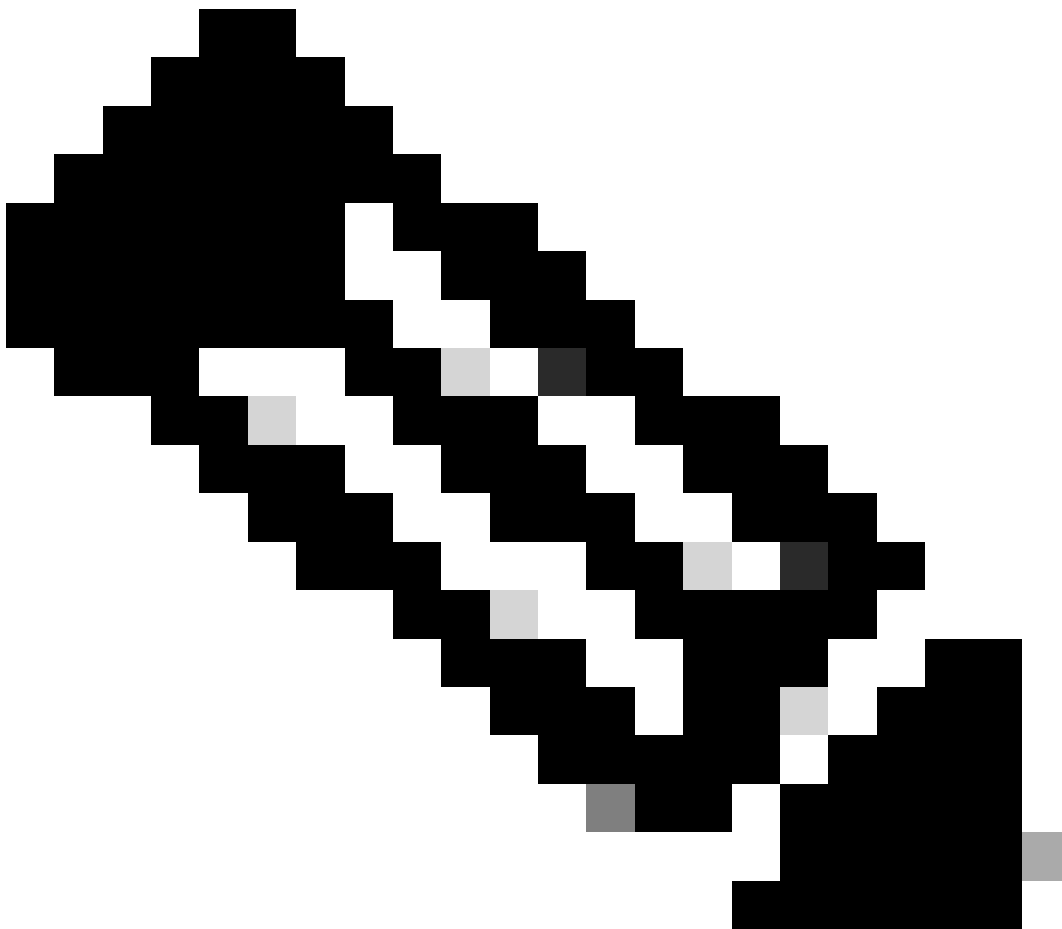
Selected 1 Total 1

Delete Files Refresh

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input checked="" type="checkbox"/>	8c-16-45-0d-f4-2b	ISE PSN	Apr 22 21:17	67959712

### Depuração de Ponto Final

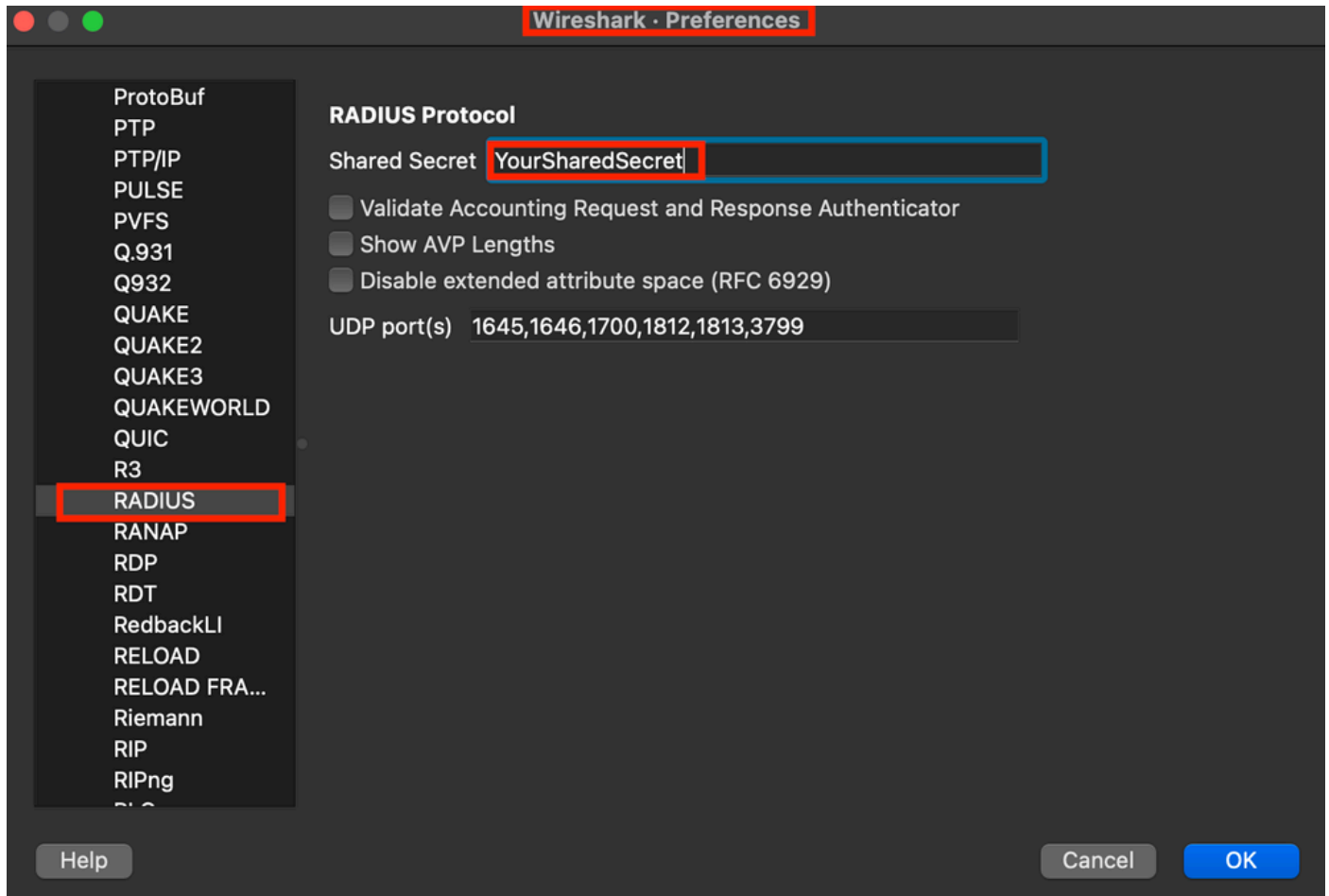
Você deve ser capaz de ver os logs de autenticação com os logs de DEBUG sem ativá-los diretamente da Configuração do Log de Depuração.



Observação: como algumas coisas podem ser omitidas na saída de Depuração de Ponto Final, você obterá um arquivo de log mais completo gerando-o com a Configuração de Log de Depuração e fazendo download de todos os logs necessários de qualquer arquivo que você precise. Conforme explicado na seção anterior Configuração de depuração do ISE e Coleta de logs.

## 7 - Criptografar pacotes RADIUS

Os pacotes Radius não são criptografados, exceto pelo campo de senha do usuário. No entanto, você precisa verificar a senha enviada. Você pode ver o pacote que o usuário enviou navegando para Wireshark > Preferências > Protocolos > RADIUS e adicionar a chave compartilhada RADIUS usada pelo ISE e o dispositivo de rede. Depois disso, os pacotes RADIUS são exibidos criptografados.



Opções de raio do Wireshark

## 8 - Comandos de identificação e solução de problemas do dispositivo de rede

O comando a seguir ajuda a solucionar problemas no ISR 1100 ou em dispositivos com fio NAD.

8 - 1 Para ver se o servidor AAA ou ISE está disponível e acessível a partir do dispositivo de rede, use show aaa servers.

```
Router>show aaa servers
```

```
RADIUS: id 1, priority 1, host 10.88.240.80, auth-port 1645, acct-port 1646, hostname  
State: current UP, duration 2876s, previous duration 0s  
Dead: total time 0s, count 0
```

```
Platform State from SMD: current UP, duration 2876s, previous duration 0s  
SMD Platform Dead: total time 0s, count 0
```

Platform State from WNCD (1) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCD (2) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCD (3) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCD (4) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCD (5) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCD (6) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCD (7) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCD (8) : current UP, duration 3015s, previous duration 0s

WNCD Platform Dead: total time 0s, count 0UP

Quarantined: No

Authen: request 11, timeouts 0, failover 0, retransmission 0

Response: accept 1, reject 0, challenge 10  
Response: unexpected 0, server error 0, incorrect 0, time 33ms  
Transaction: success 11, failure 0  
Throttled: transaction 0, timeout 0, failure 0  
Malformed responses: 0  
Bad authenticators: 0  
Dot1x transactions:

Response: total responses: 11, avg response time: 33ms  
Transaction: timeouts 0, failover 0  
Transaction: total 1, success 1, failure 0

MAC auth transactions:  
Response: total responses: 0, avg response time: 0ms  
Transaction: timeouts 0, failover 0  
Transaction: total 0, success 0, failure 0

Author: request 0, timeouts 0, failover 0, retransmission 0

Response: accept 0, reject 0, challenge 0  
Response: unexpected 0, server error 0, incorrect 0, time 0ms  
Transaction: success 0, failure 0

Throttled: transaction 0, timeout 0, failure 0  
Malformed responses: 0  
Bad authenticators: 0  
MAC author transactions:

Response: total responses: 0, avg response time: 0ms  
Transaction: timeouts 0, failover 0  
Transaction: total 0, success 0, failure 0

Account: request 6, timeouts 4, failover 0, retransmission 3

Request: start 1, interim 0, stop 0  
Response: start 1, interim 0, stop 0

Response: unexpected 0, server error 0, incorrect 0, time 27ms  
Transaction: success 2, failure 1  
Throttled: transaction 0, timeout 0, failure 0  
Malformed responses: 0  
Bad authenticators: 0

Elapsed time since counters last cleared: 47m  
Estimated Outstanding Access Transactions: 0  
Estimated Outstanding Accounting Transactions: 0  
Estimated Throttled Access Transactions: 0  
Estimated Throttled Accounting Transactions: 0  
Maximum Throttled Transactions: access 0, accounting 0

Consecutive Response Failures: total 0

```
SMD Platform : max 0, current 0 total 0
WNCN Platform: max 0, current 0 total 0
IOSD Platform : max 0, current 0 total 0

Consecutive Timeouts: total 3
SMD Platform : max 0, current 0 total 0
WNCN Platform: max 0, current 0 total 0
IOSD Platform : max 3, current 0 total 3

Requests per minute past 24 hours:
high - 0 hours, 47 minutes ago: 4
low  - 0 hours, 45 minutes ago: 0
average: 0
```

Router>

8-2 Para ver o status da porta, os detalhes, as ACLs aplicadas à sessão, o método de autenticação e informações mais úteis, use o comando show authentication sessions interface <interface where the laptop is attached> details.

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
Interface: GigabitEthernet0/1/0
IIF-ID: 0x01D9BEFB
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781FOA0000000C0777AECD
Acct Session ID: 0x00000003
Handle: 0x0a000002
Current Policy: POLICY_Gi0/1/0
```

```
Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
```

```
Server Policies:
```

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

Router#

8-3 Para verificar se você tem todos os comandos necessários para aaa na configuração global, execute show running-config aaa.

```
Router#sh run aaa
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
client <A.B.C.D> server-key Cisc0123
!
!
radius server COHVSRAISE01-NEW
address ipv4 <A.B.C.D> auth-port 1645 acct-port 1646
timeout 15
key Cisc0123
!
!
aaa group server radius ISE-CLUSTER
server name COHVSRAISE01-NEW
!
!
!
!
aaa new-model
aaa session-id common
!
!

Router#
```

8-4 Outro comando útil é test aaa group radius server <A.B.C.D> isiscool VainillaISE97 legacy.

```
Router#test aaa group radius server <A.B.C.D> isiscool VainillaISE97 legacy
User was successfully authenticated.

Router#
```

## 9 - Depurações relevantes do dispositivo de rede

- debug dot1x all - Exibe todas as mensagens EAP dot1x
- debug aaa authentication - Exibe informações de depuração de autenticação de aplicativos AAA
- debug aaa authorization - Exibe informações de depuração para autorização AAA
- debug radius authentication - Fornece informações detalhadas sobre atividades no nível de protocolo apenas para a autenticação
- debug radius - Fornece informações detalhadas sobre as atividades em nível de protocolo

## Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)



## 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.