排除ISE 3.2和Windows中的有线Dot1x问题

目录

简介

本文档介绍如何为身份服务引擎(ISE) 3.2和Windows本地请求方配置基本802.1X PEAP身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 受保护的扩展身份验证协议 (PEAP)
- PEAP 802.1x

使用的组件

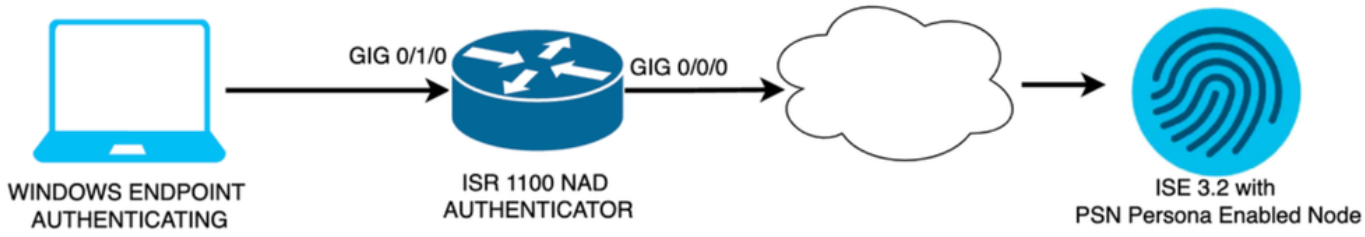
本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎(ISE)版本
- 思科C1117 Cisco IOS® XE软件，版本17.12.02
- 使用Windows 10的笔记本电脑

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



网络图

配置

执行以下步骤进行配置：

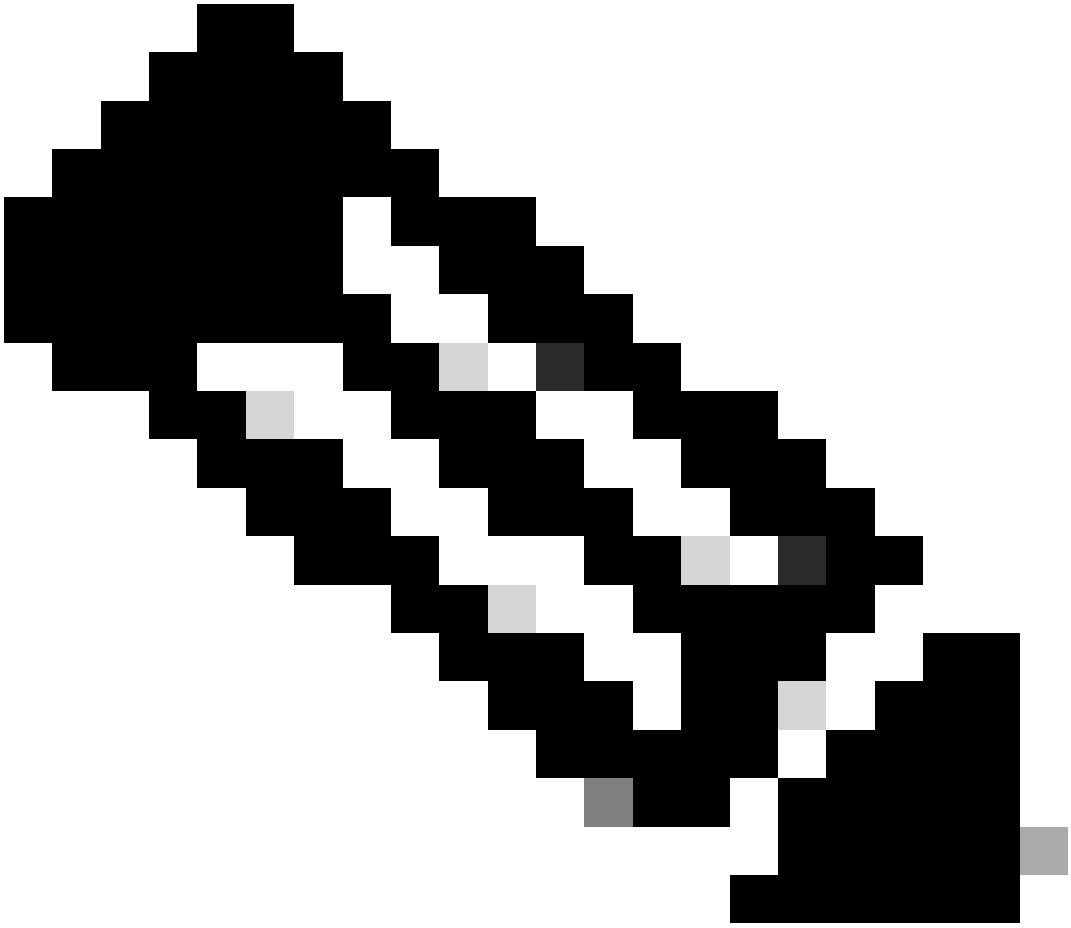
步骤1:配置ISR 1100路由器。

第二步：配置身份服务引擎3.2。

第三步：配置Windows本地请求方。

步骤1:配置ISR 1100路由器

本部分说明至少需要NAD才能使dot1x正常运行的基本配置。



注意：对于多节点ISE部署，请配置已启用PSN角色的节点的IP。您可以导航到Administration > System > Deployment选项卡下的ISE来启用此功能。

```
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>
!
!
```

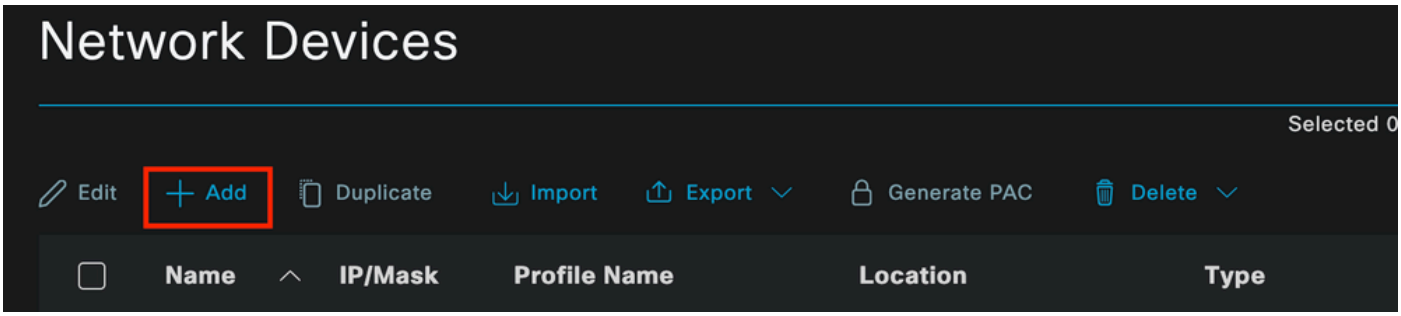
```
aaa group server radius ISE-CLUSTER
 server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
 description "Endpoint that supports dot1x"
 switchport access vlan 15
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication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

第二步：配置身份服务引擎3.2。

2. a.配置并添加用于身份验证的网络设备。

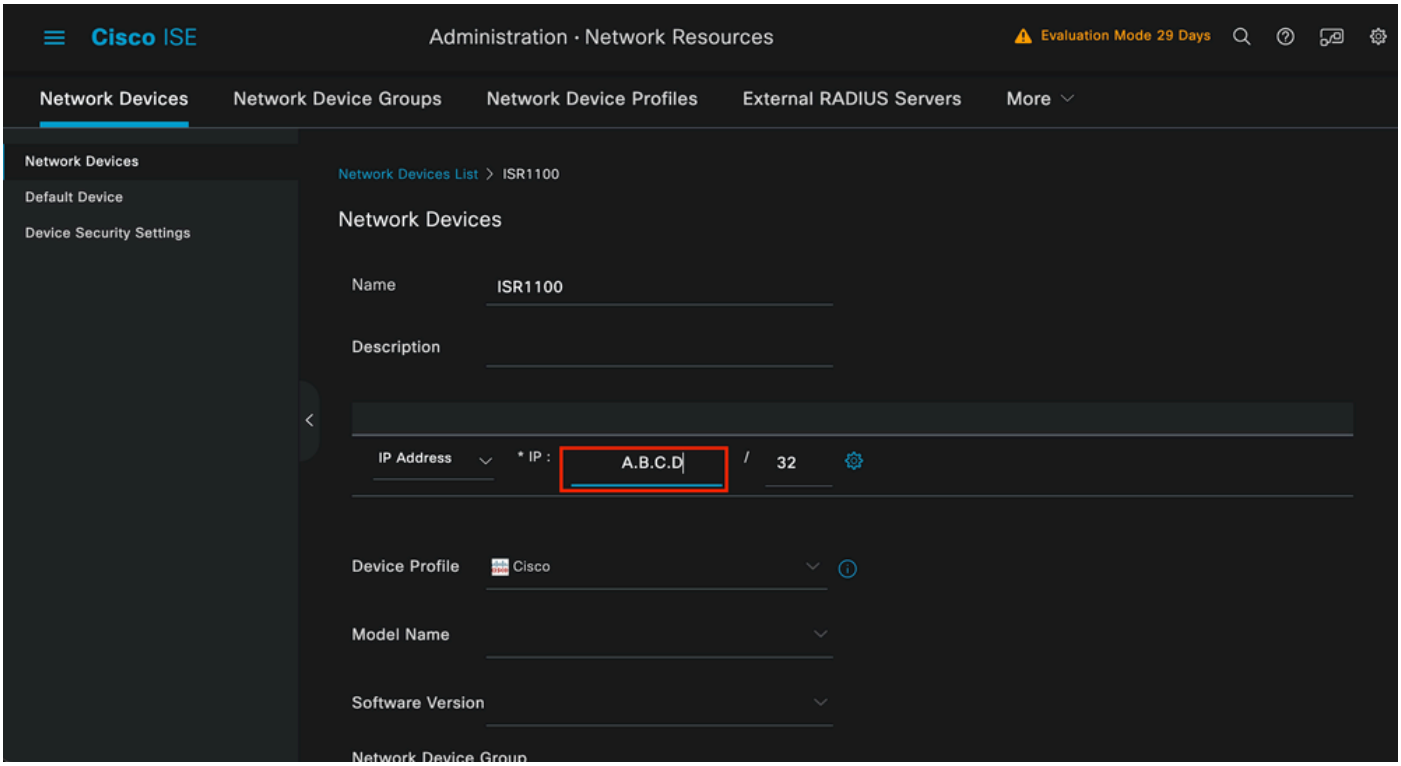
Add the Network Device to ISE Network Devices部分。

单击Add按钮开始。



ISE网络设备

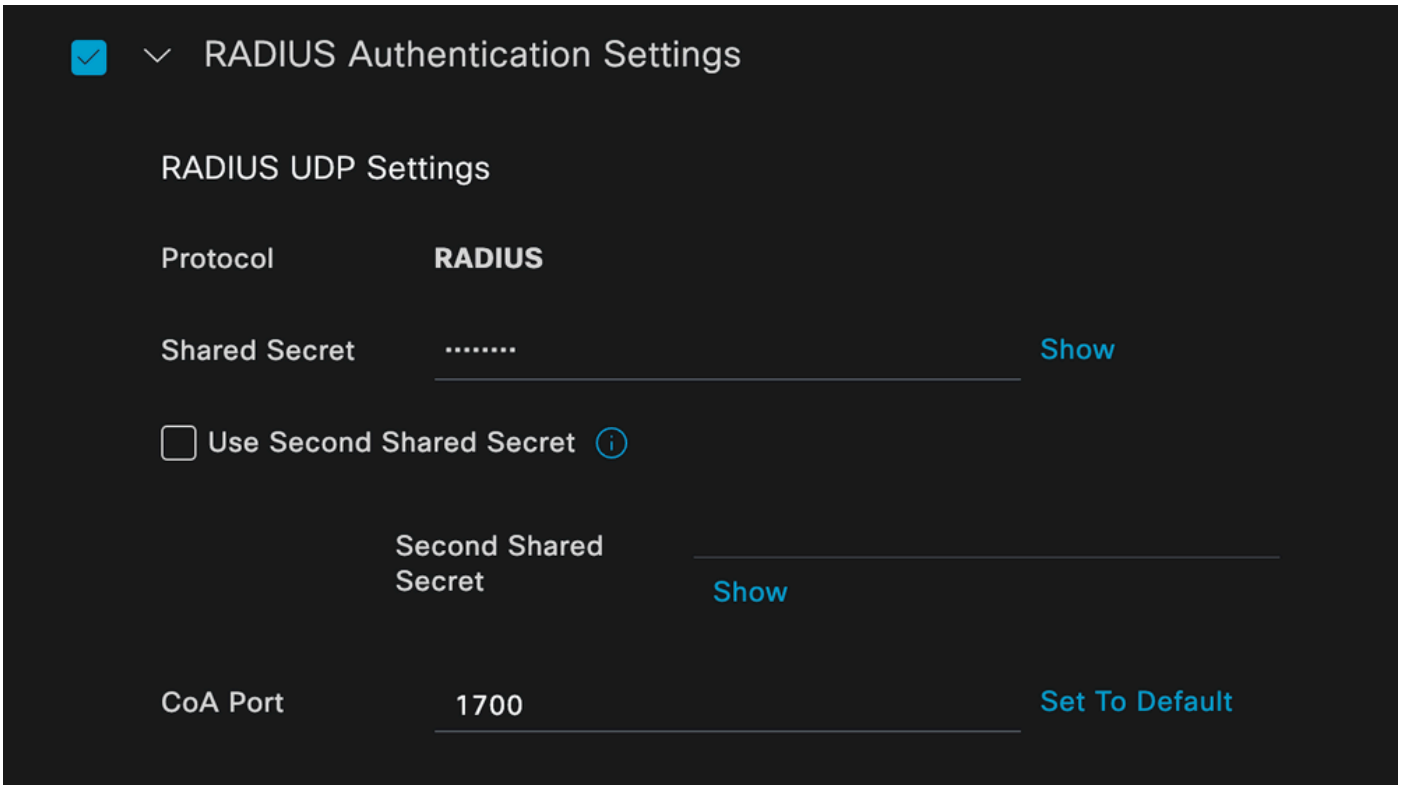
输入值，为您创建的NAD指定名称，并添加网络设备用于联系ISE的IP。



网络设备创建页面

在同一页中，向下滚动以查找Radius Authentication Settings。如下图所示。

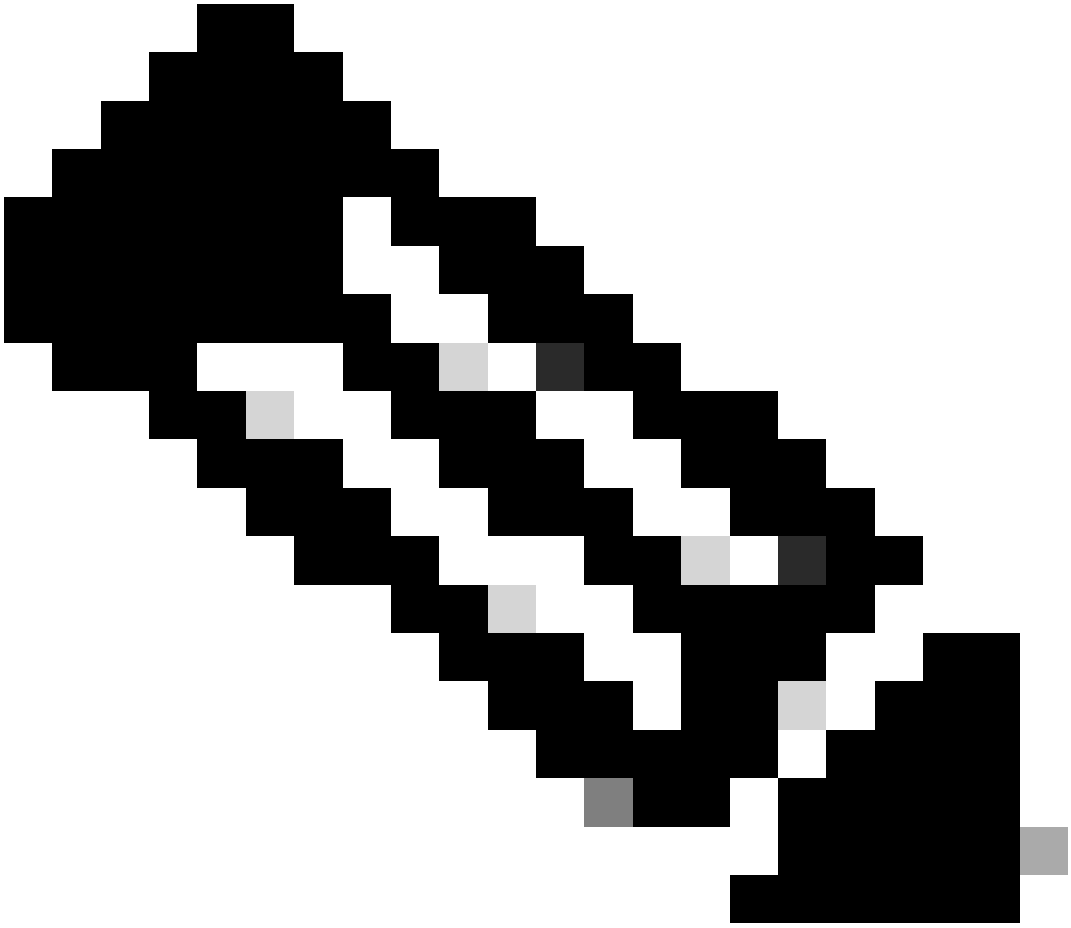
添加您在NAD配置下使用的共享密钥。



RADIUS 配置

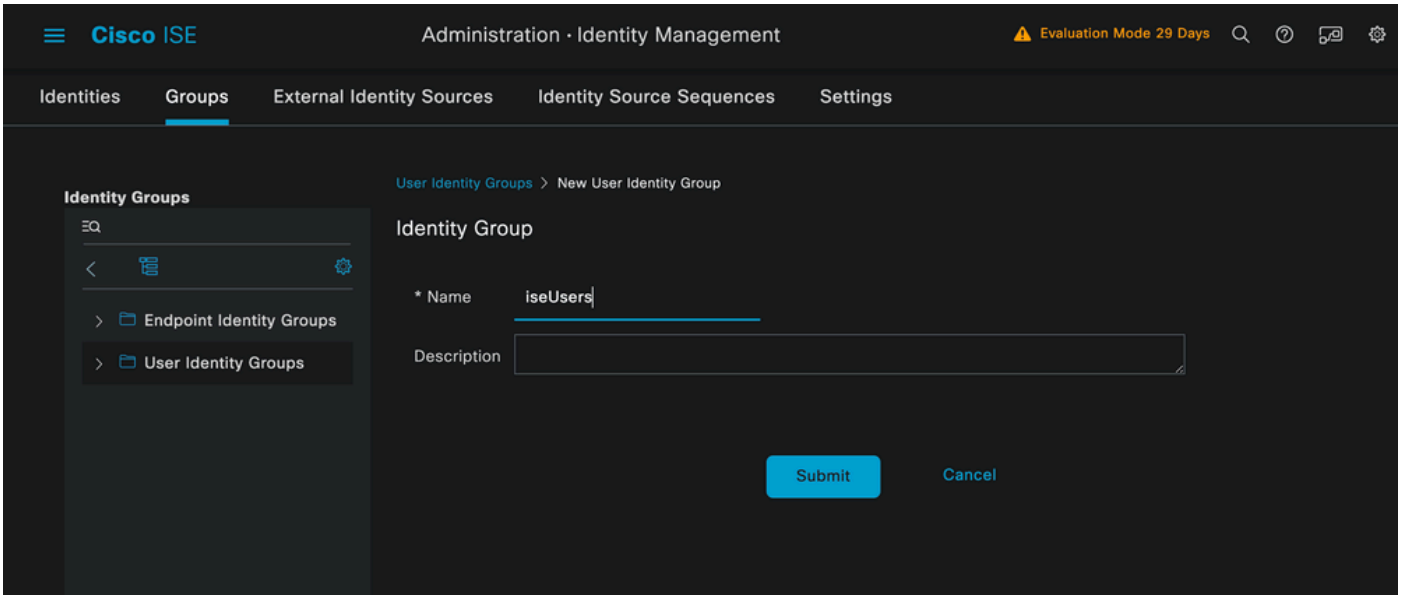
保存更改。

2. b.配置用于对终端进行身份验证的身份。



注意：为了保持本配置指南的不变，将使用简单的ISE本地身份验证。

导航到管理>身份管理>组选项卡。创建组和身份，为此演示创建的组为iseUsers。

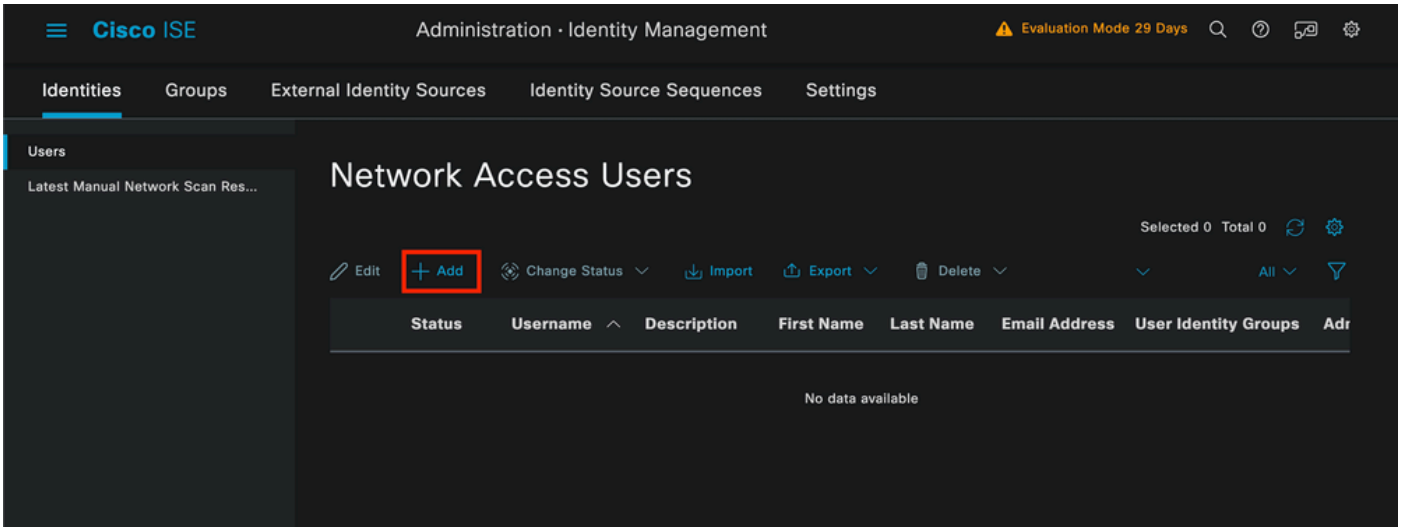


“身份组创建”页

单击Submit按钮。

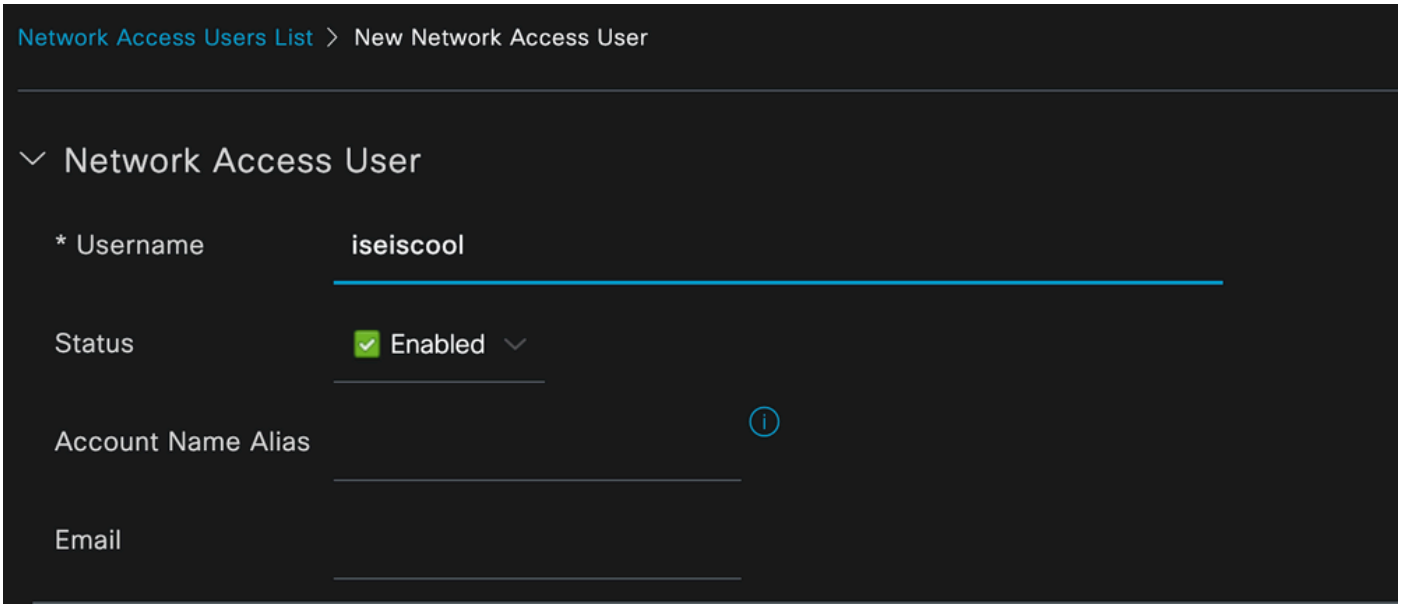
接下来，导航到Administration > Identity Management > Identity选项卡。

单击Add。



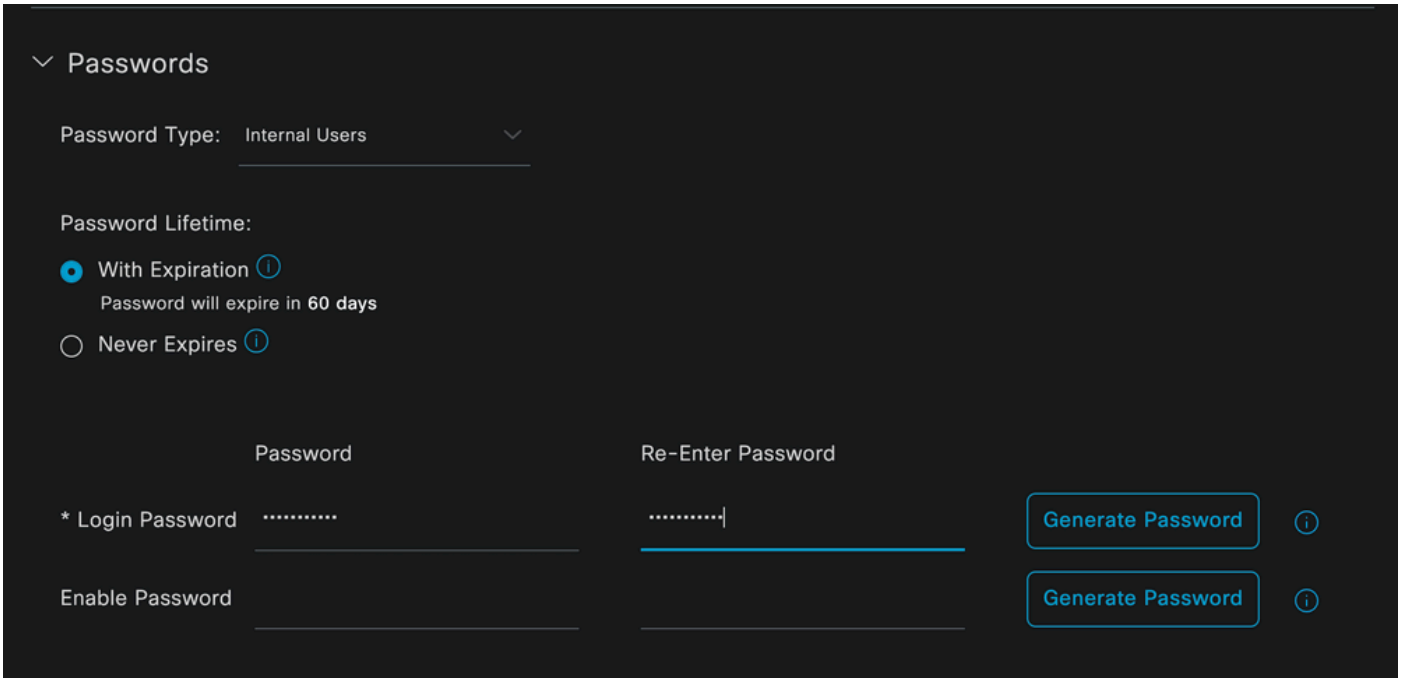
“用户创建”页

作为必填字段的一部分，以用户的名称开头。此示例中使用用户名iseiscool。



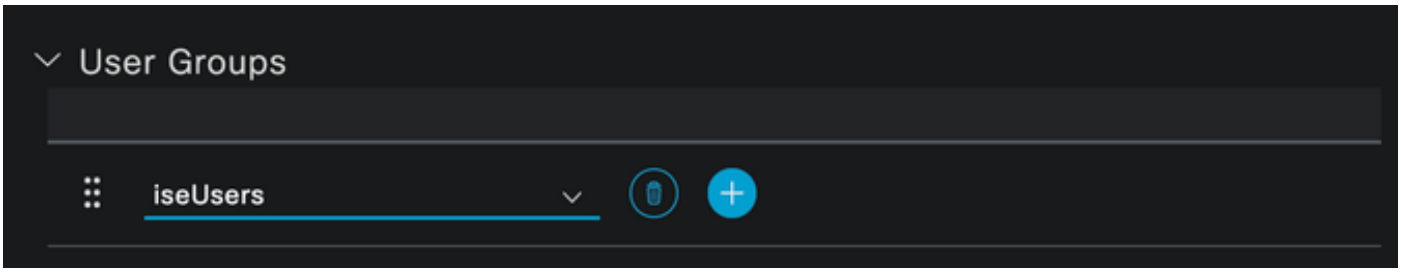
分配给用户名的名称

下一步是为创建的用户名指定密码。 VainillaISE97用于此演示。



密码创建

将用户分配到iseUsers组。



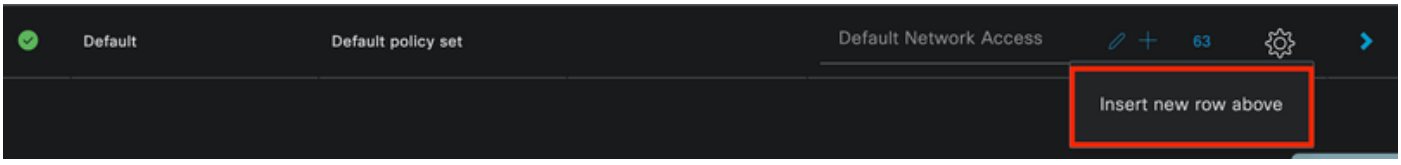
用户组分配

2. c.配置策略集

导航至ISE菜单>策略>策略集。

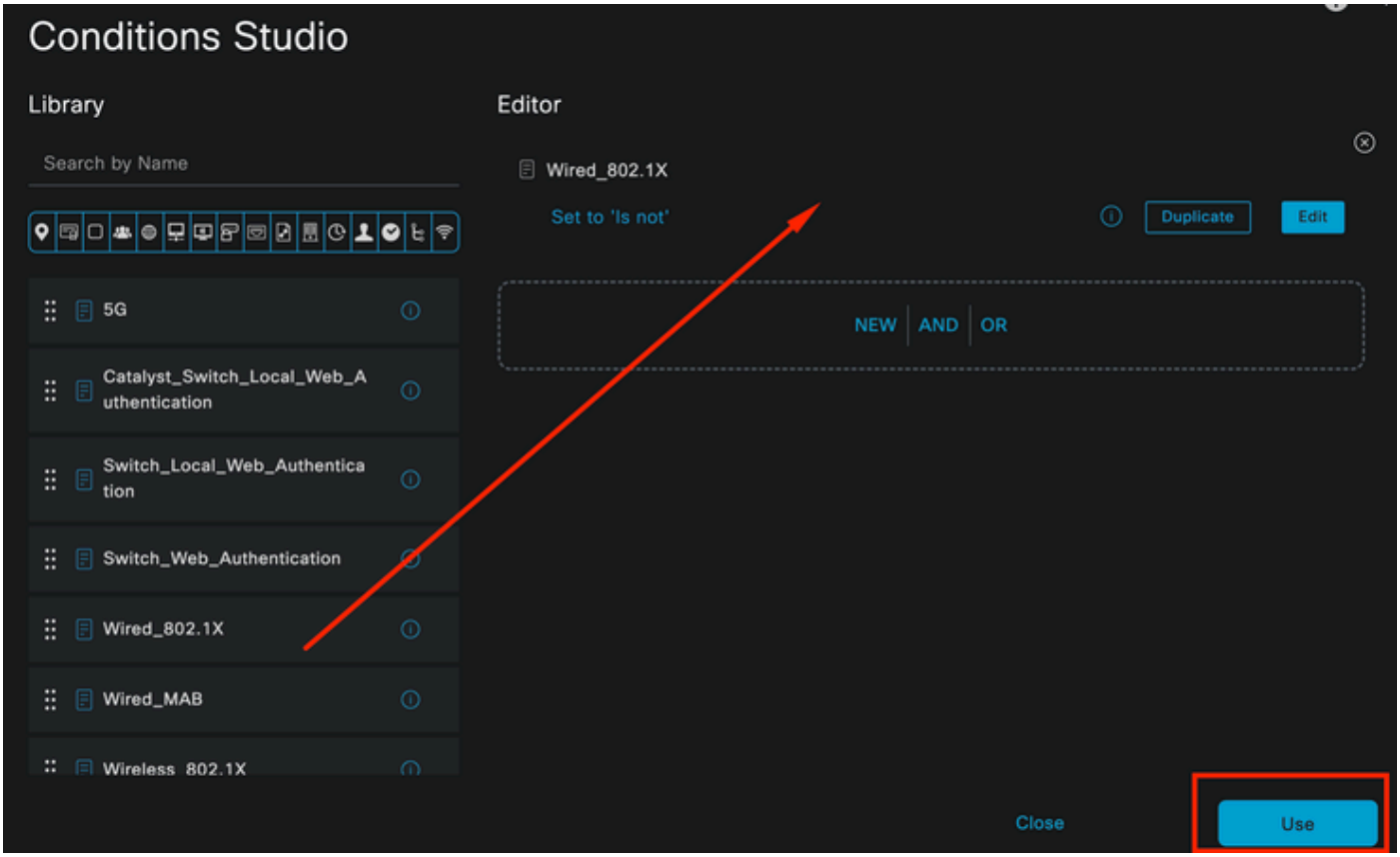
可以使用默认策略集。然而，在本示例中，创建了策略集，称为有线。 对策略集进行分类和区分有助于排除故障，

如果看不到添加或加号图标，则可以点击任何策略集的齿轮图标。选择齿轮图标，然后选择“在上方插入新行”。



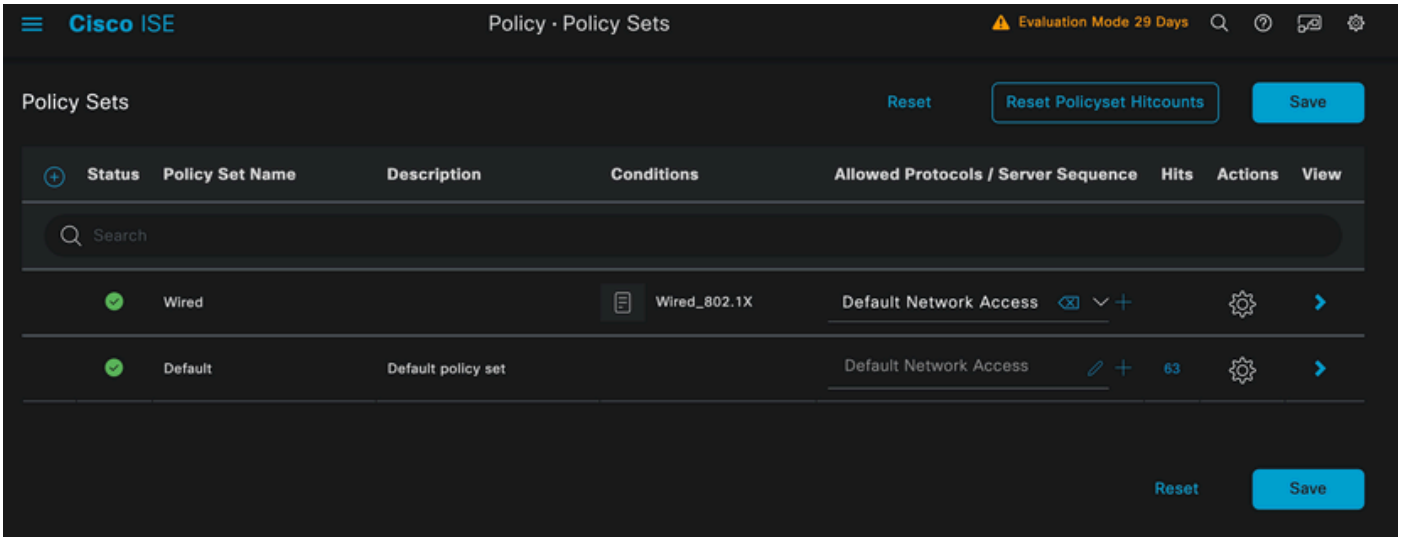
策略创建

本示例中配置的条件是有线8021x，这是在ISE新部署中预配置的条件。拖动它，然后单击使用。



条件工作室

最后，选择Default Network Access preconfigured allowed protocols service。

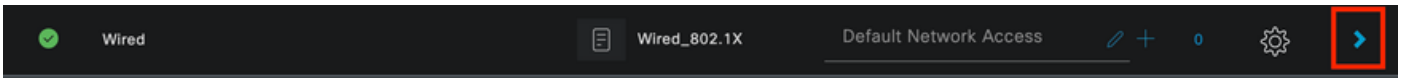


策略集视图

Click Save.

2. d.配置身份验证和授权策略。

点击刚创建的策略集右侧的箭头。



有线策略集

展开身份验证策略

点击+图标。

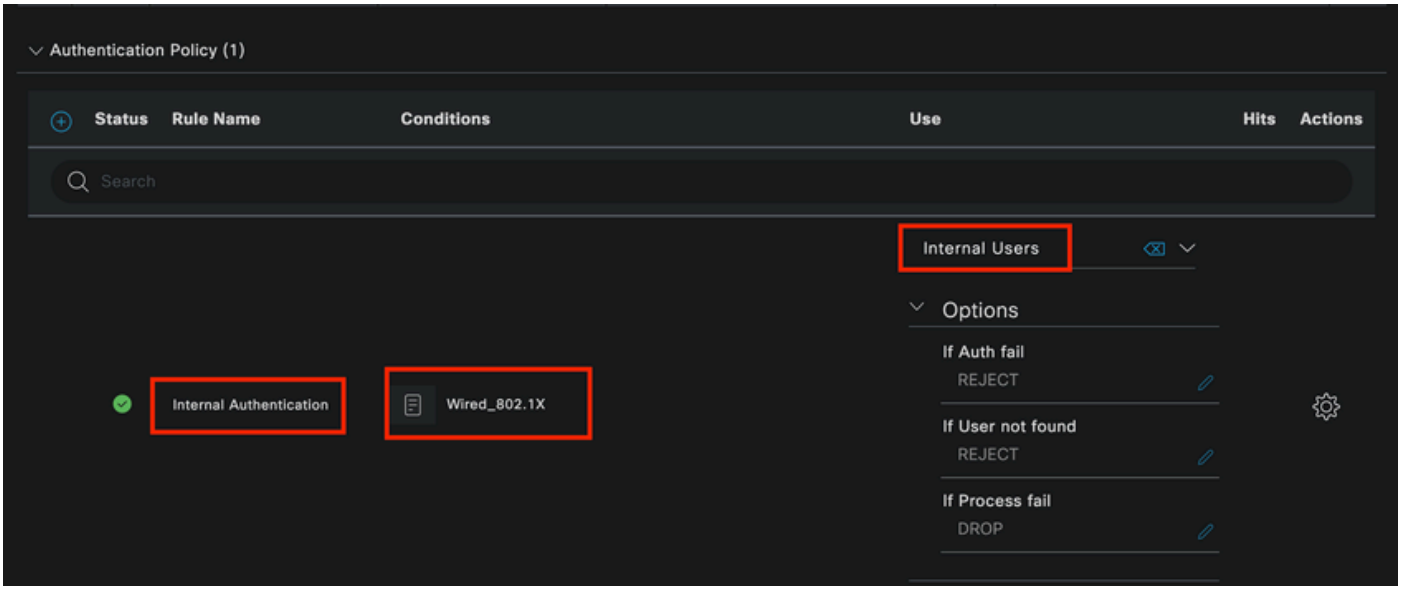
添加身份验证策略

为身份验证策略分配名称，例如使用内部身份验证。

点击此新身份验证策略的条件列上的+图标。

可以使用随附的预配置条件Wired Dot1x ISE。

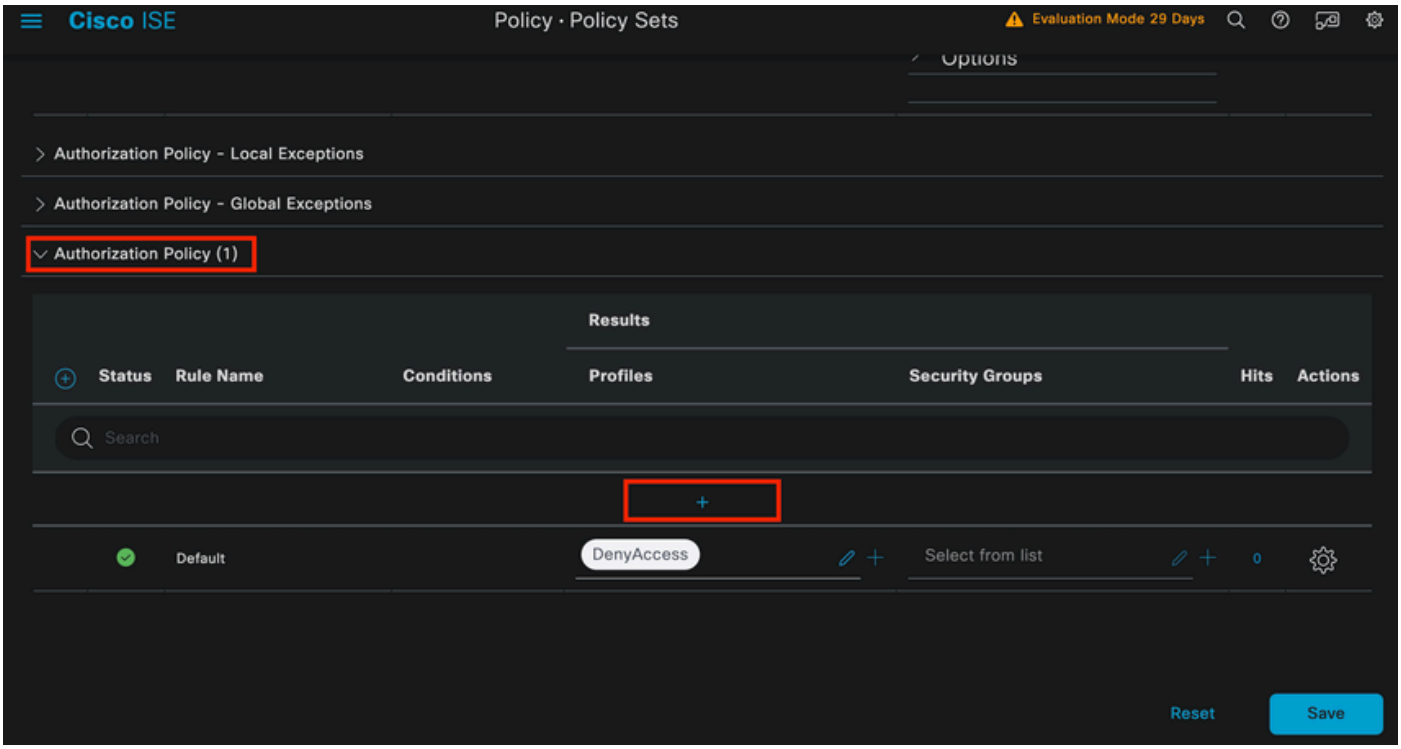
最后，在使用列下，从下拉列表中选择“内部用户”。



身份验证策略

授权策略

授权策略部分位于页面底部。 展开并单击+图标。



授权策略

为您刚添加的授权策略命名，在此配置示例中使用内部ISE用户名称。

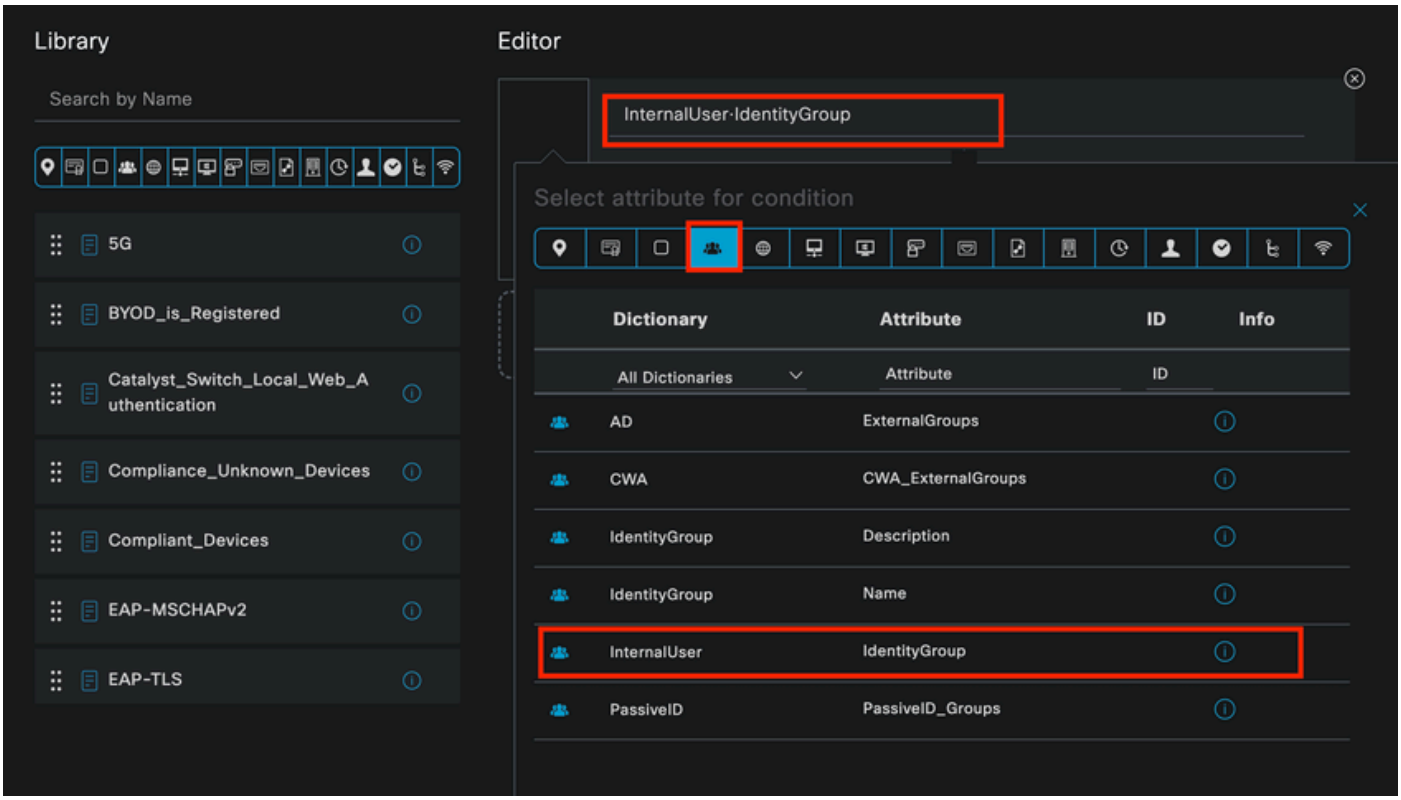
要为此授权策略创建条件，请点击条件列下的+图标。

先前创建的用户是IseUsers组的一部分。

在编辑器中，单击Click to add an attribute部分。

选择身份组图标。

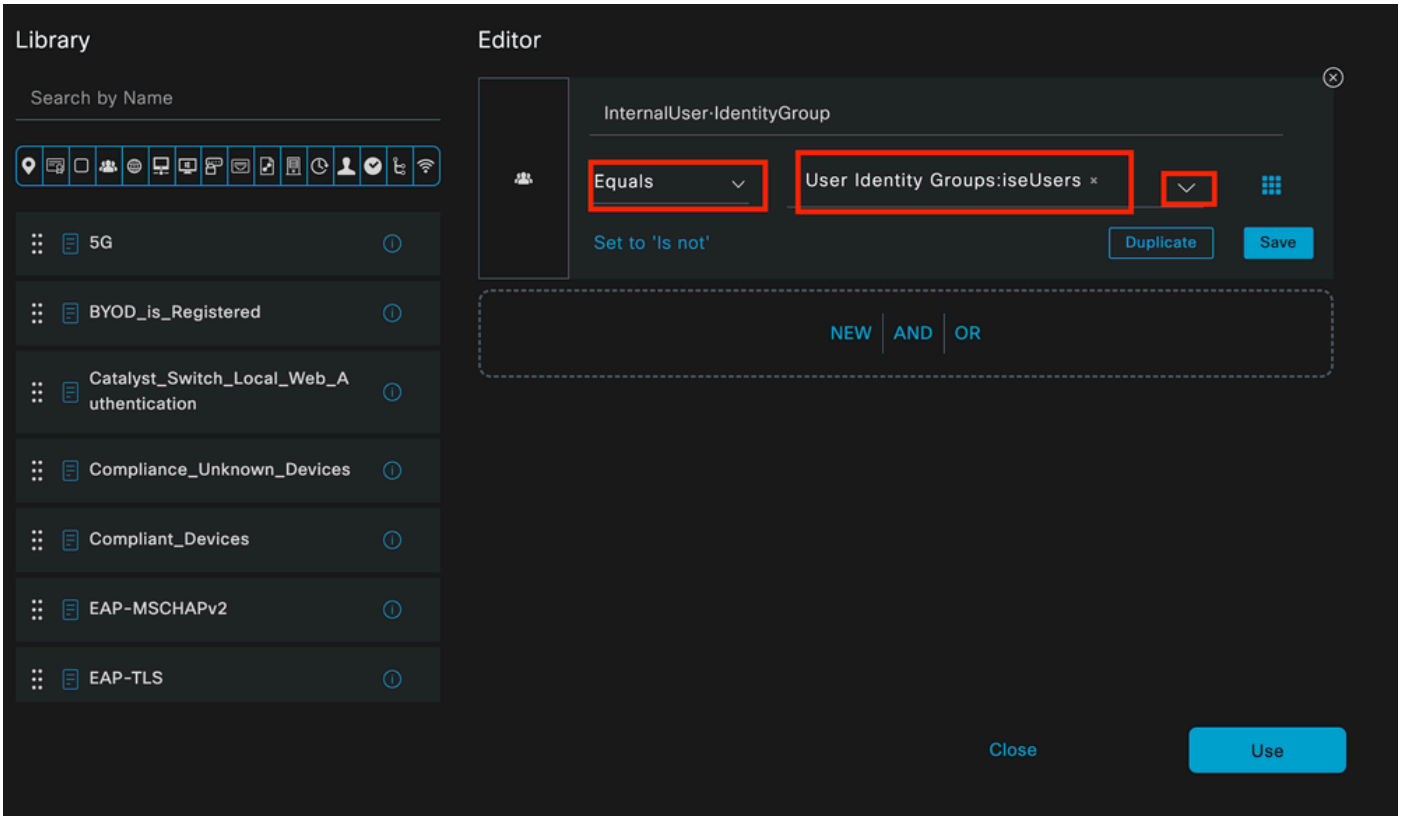
从词典中，选择带有身份组属性的InternalUser词典。



授权策略的Condition Studio

选择Equals运算符。

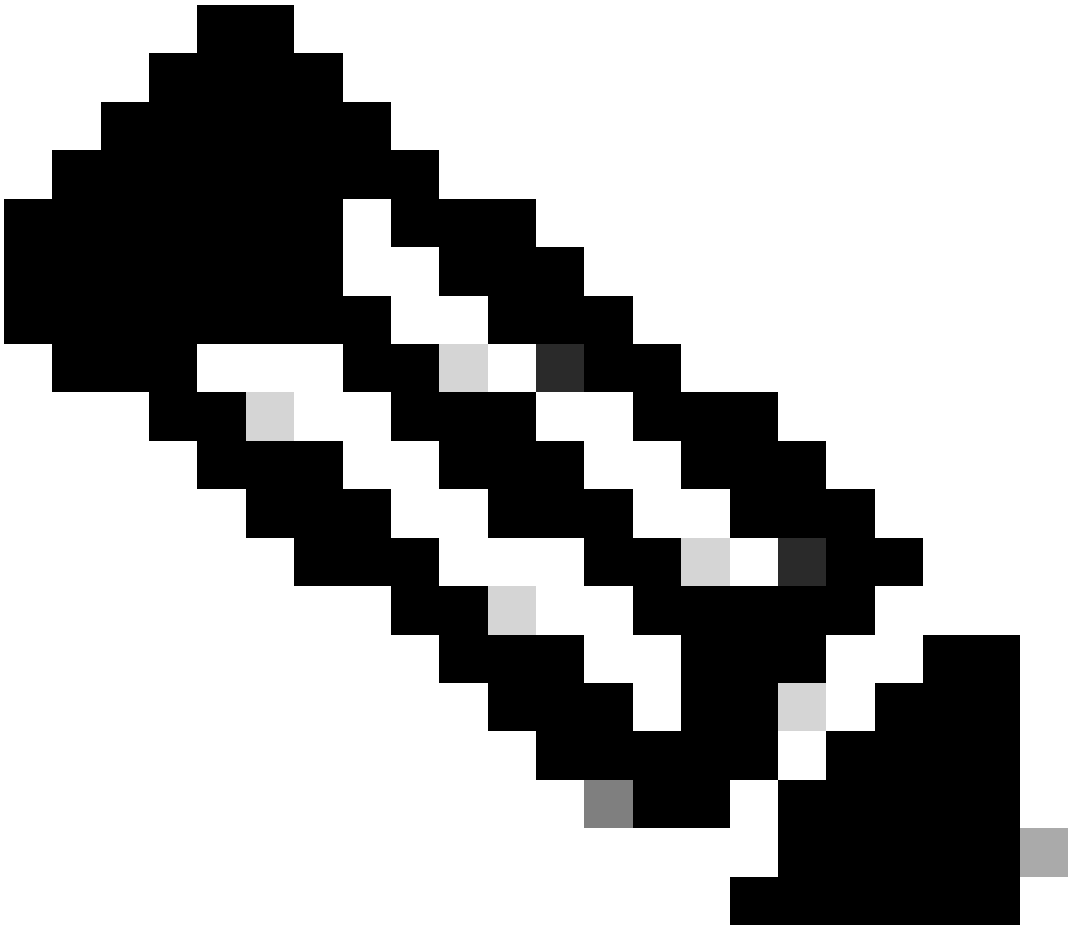
从User Identity Groups下拉列表中，选择组IseUsers。



授权策略条件已完成

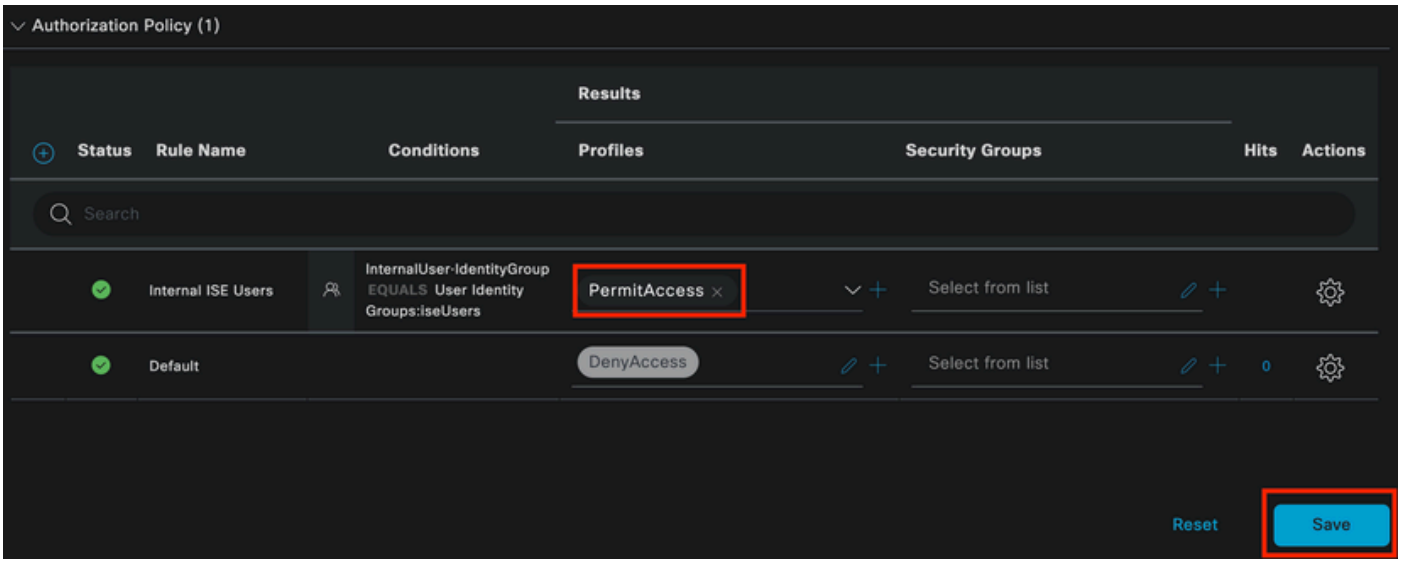
单击Use。

最后，选择接收此身份组的身份验证部分的Result Authorization Profile。



注意：请注意，到达ISE的身份验证将触发此并非用户身份组ISEUsers一部分的有线Dot1x策略集，此时按的是默认授权策略。配置文件结果为DenyAccess。

ISE已通过允许访问配置文件进行预配置。选择它。



授权策略已完成

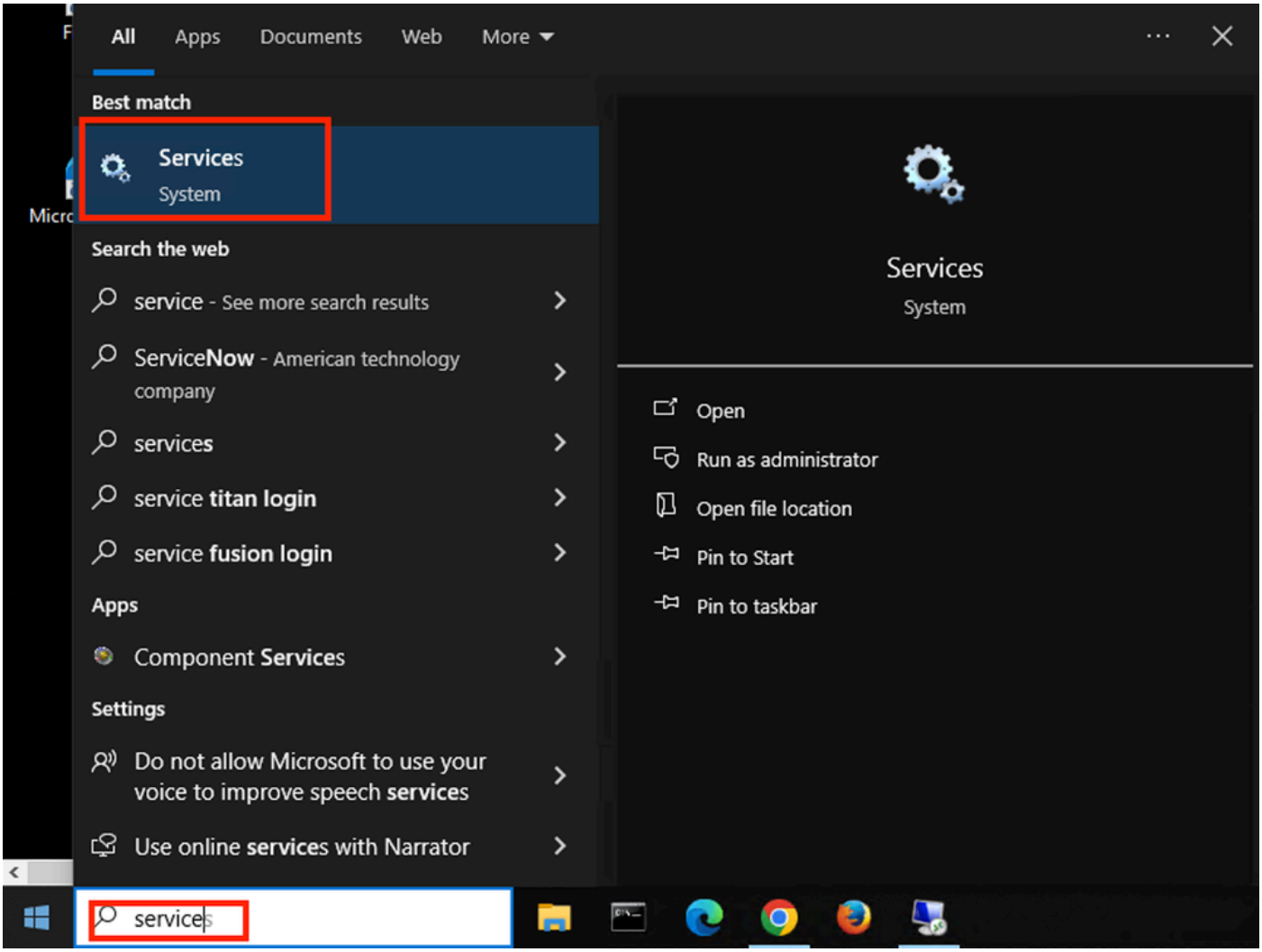
Click Save.

ISE的配置已完成。

第三步：Windows本机请求方配置

3. a.在Windows上启用有线dot1x。

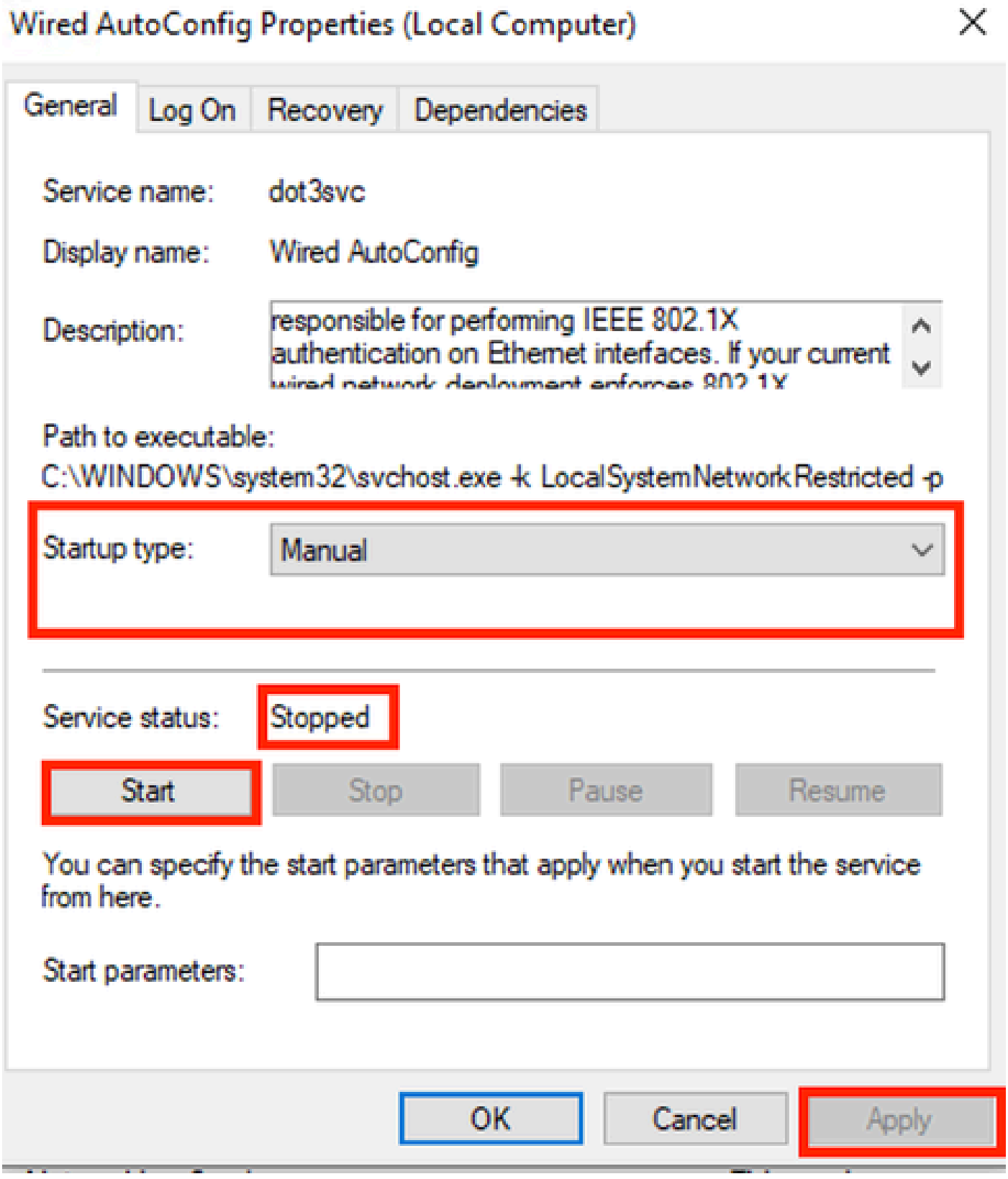
从Windows搜索栏打开Services。



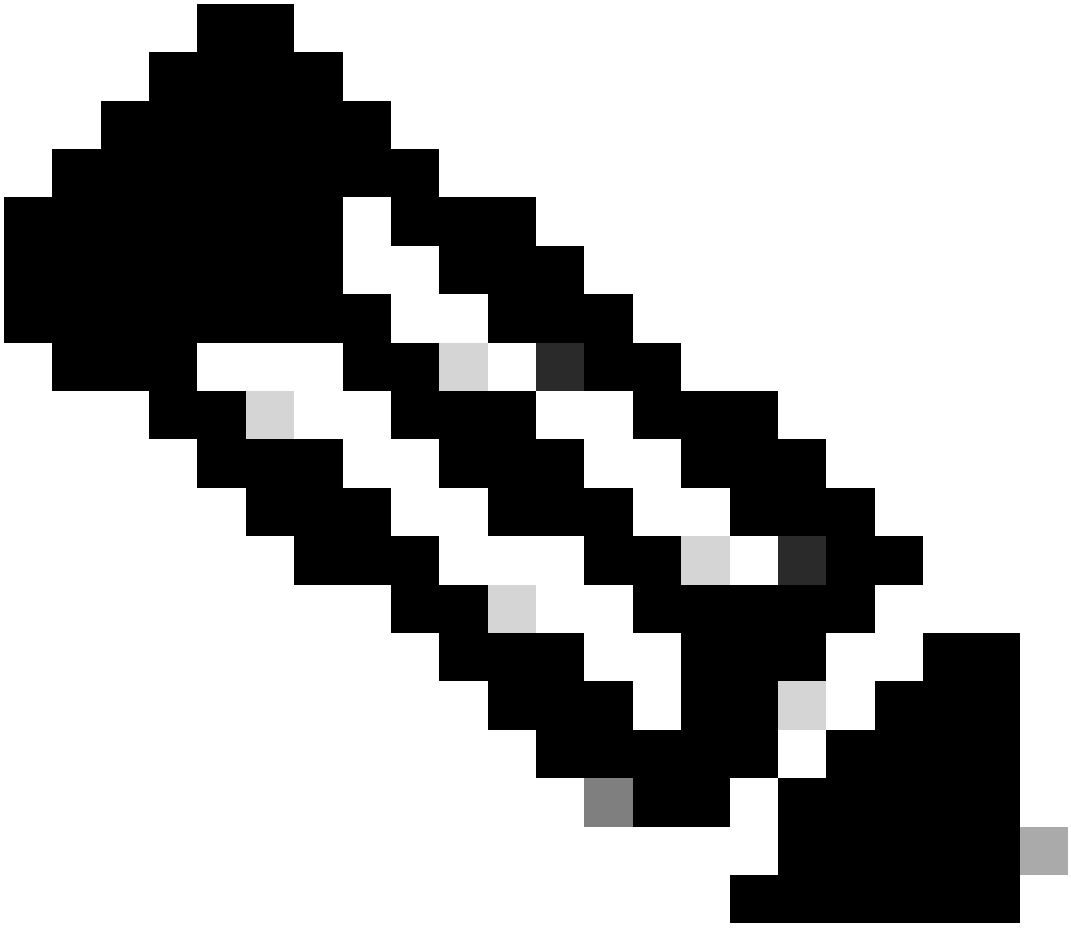
Windows搜索栏

在Services列表的底部，找到Wired Autoconfig。

右键单击“Wired AutoConfig”并选择属性。


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
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

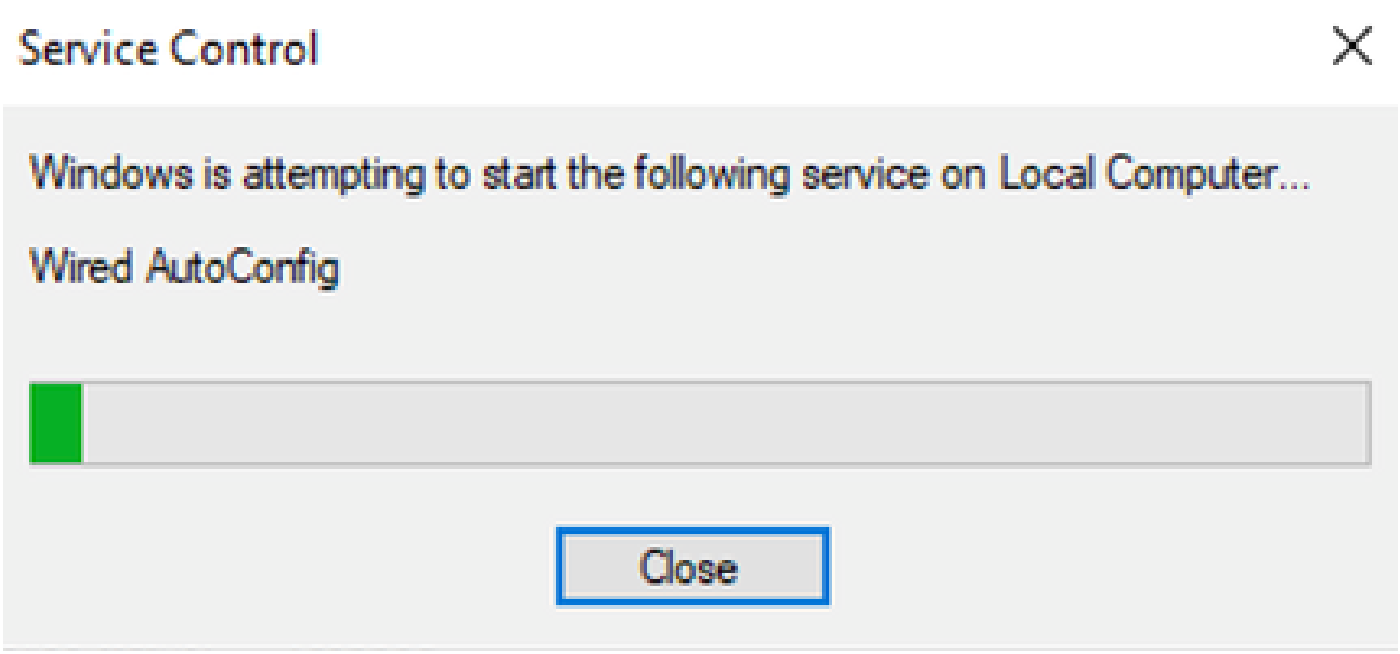
“属性”窗口



注意：有线AutoConfig (DOT3SVC)服务负责在以太网接口上执行IEEE 802.1X身份验证。

已选择手动启动类型。

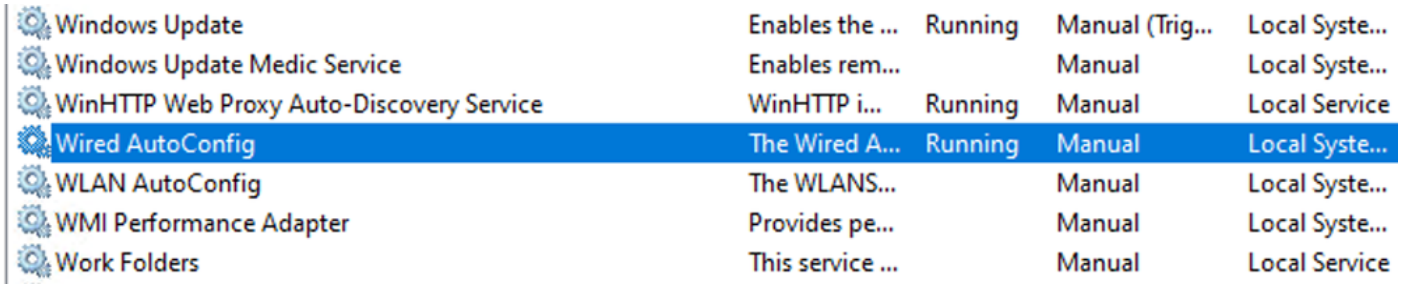
因为服务状态为Stopped。单击开始。



服务控制

然后，单击OK。

之后服务正在运行。



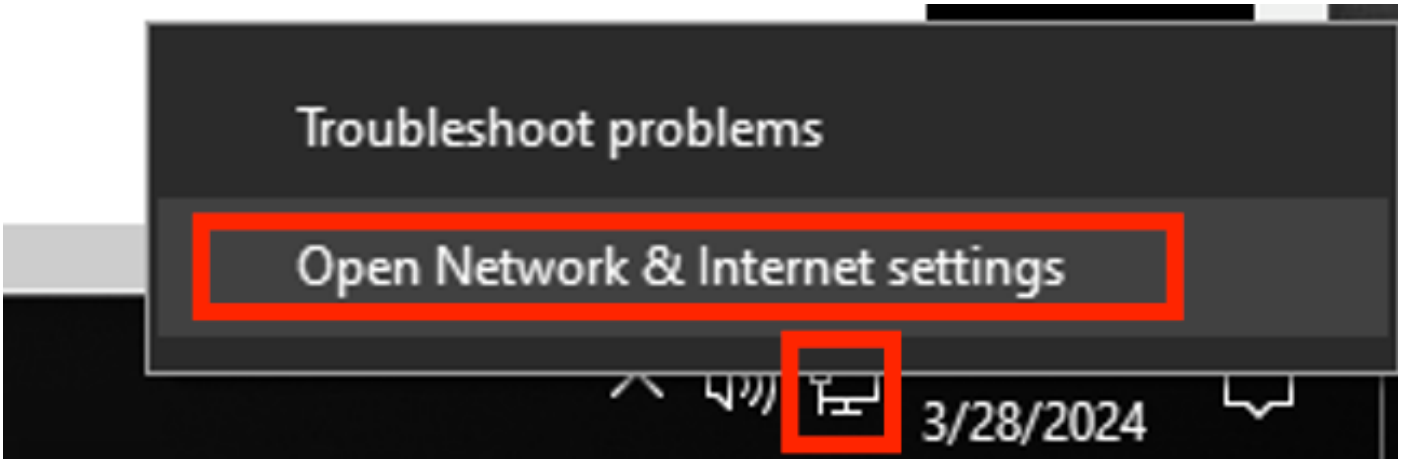
有线自动配置服务

3. b.配置连接到NAD身份验证器(ISR 1100)的Windows笔记本电脑接口。

在任务栏中，找到右角，然后使用计算机图标。

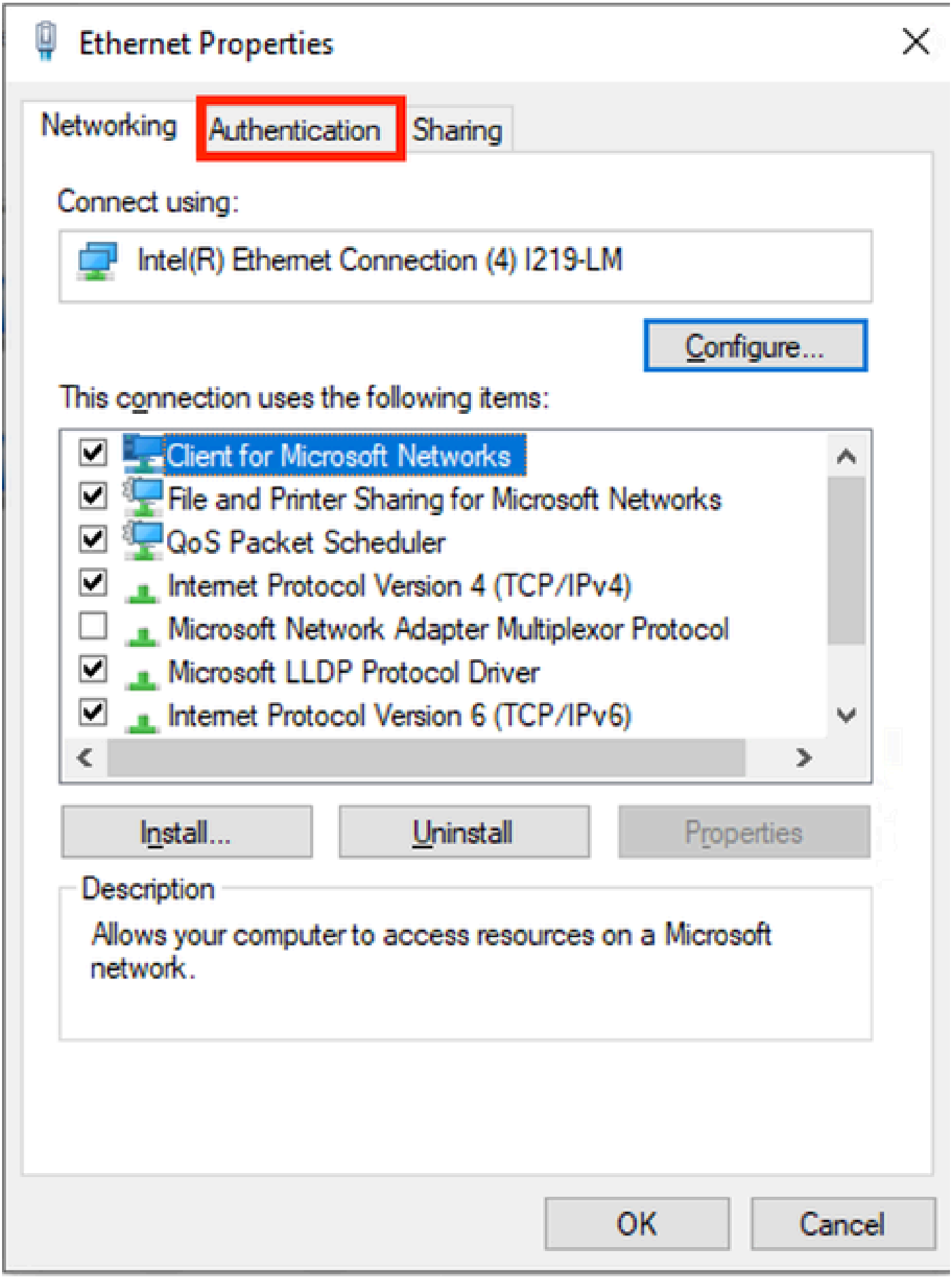
双击计算机图标。

选择打开网络和 Internet 设置。



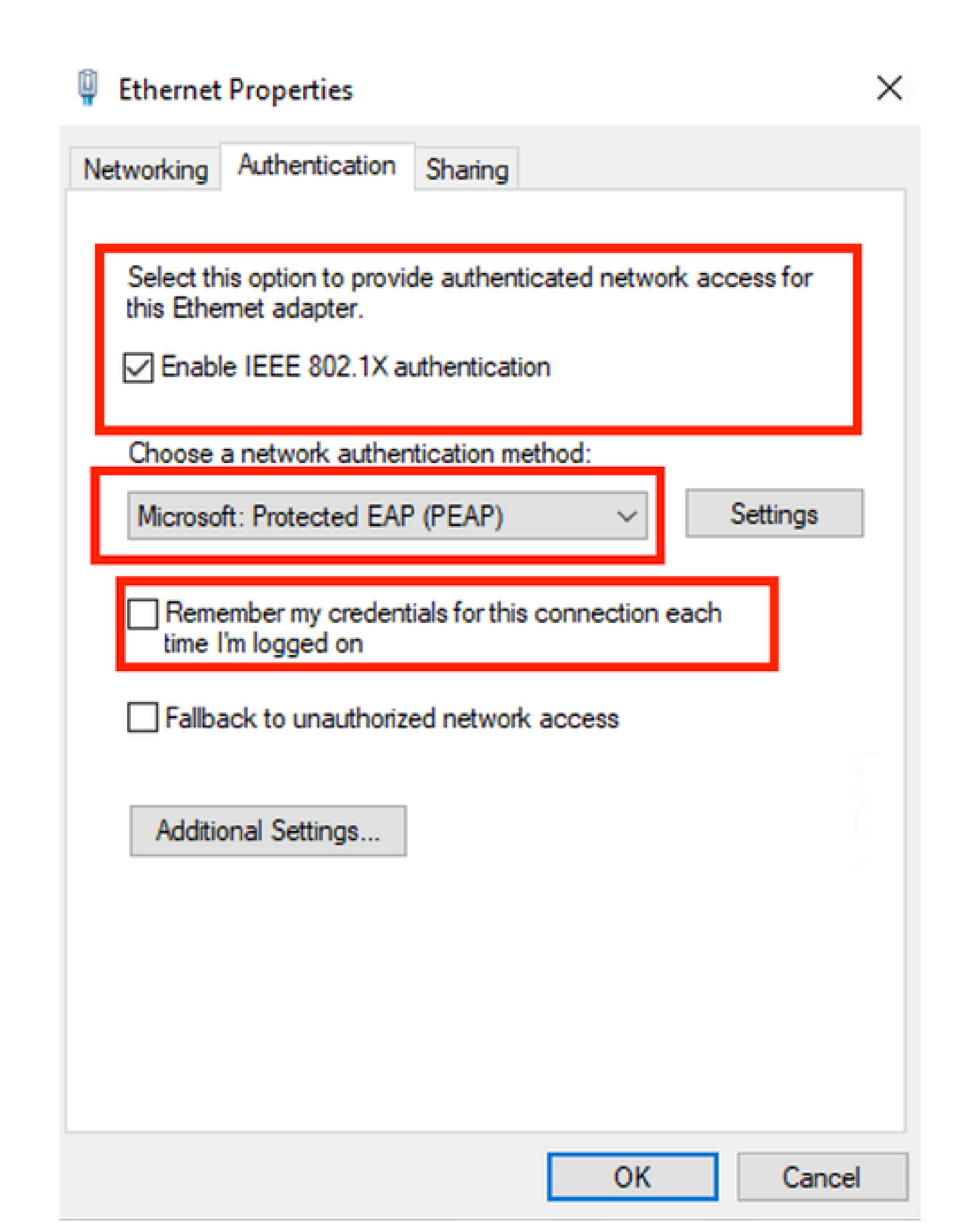
打开网络连接窗口后，右键单击连接到ISR Gig 0/1/0的以太网接口。单击Properties选项。

单击 Authentication 选项卡。



接口以太网属性

选中Enable IEEE 802.1X authentication复选框。

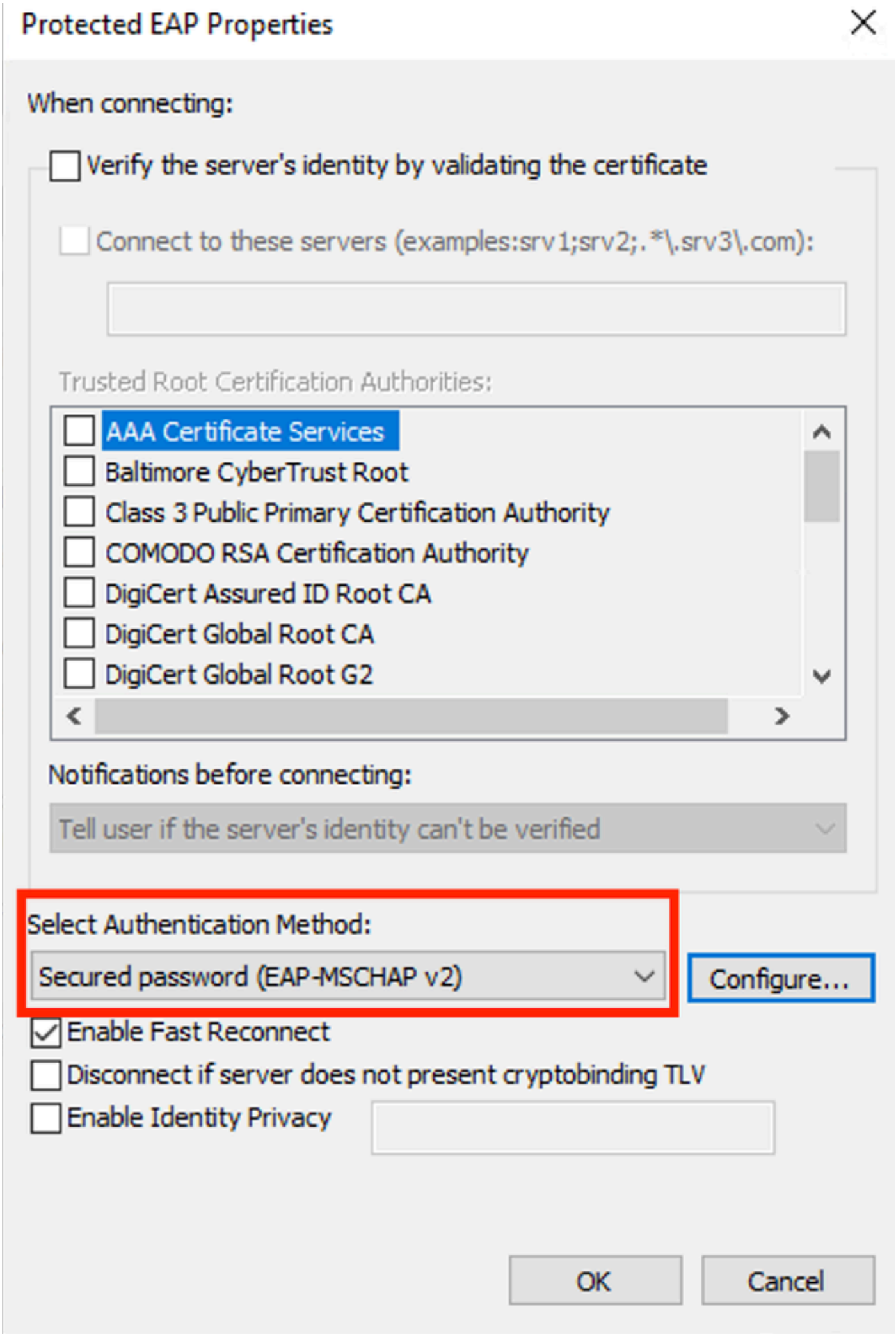

Ethernet Properties
Networking
Authentication
Sharing
Select this option to provide authenticated network access for this Ethernet adapter.
Enable IEEE 802.1X authentication
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Fallback to unauthorized network access
Additional Settings...
OK
Cancel

身份验证以太网属性

选择Protected EAP (PEAP)。

取消选中Remember my credentials for this connection each time I'm logged on选项。

单击设置。


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

PEAP属性

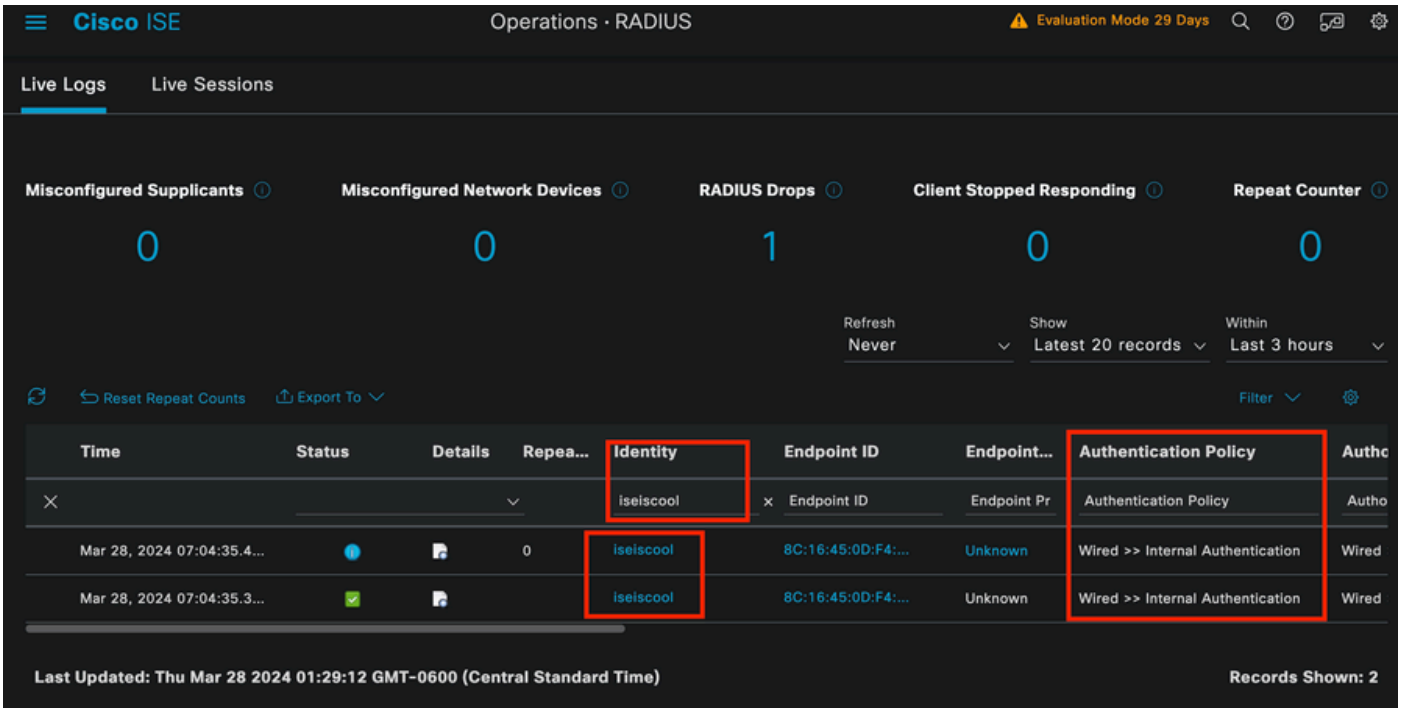
```
            Interface:  GigabitEthernet0/1/0
                IIF-ID:  0x08767C0D
           MAC Address:  8c16.450d.f42b
          IPv6 Address:  Unknown
          IPv4 Address:  Unknown
             User-Name:  iseiscool <--------- The username configured for Windows Native Supplicant
                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 authenticati
```

```
Router#
```

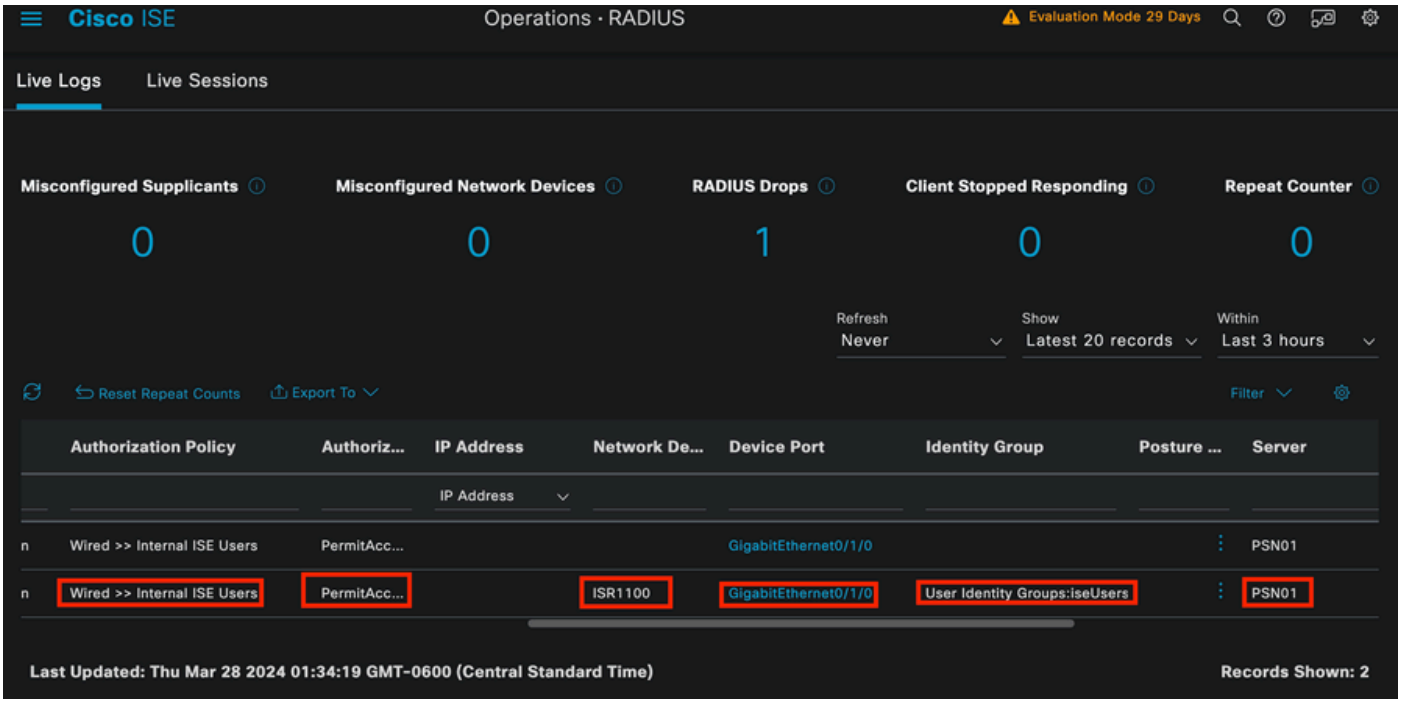
ISE日志

导航到操作> Radius >实时日志选项卡。

按用户名标识过滤，本示例中使用用户名iseiscool。



*ISE*实时日志



*ISE*实时日志

请注意，在此快速视图中，实时日志提供关键信息：

- 身份验证的时间戳。
- 使用的标识。
- 终端mac地址。
- 已命中的策略集和身份验证策略。
- 已命中的策略集和授权策略。
- 授权配置文件结果。
- 向ISE发送RADIUS请求的网络设备。
- 终端所连接的接口。
- 通过身份验证的用户的身份组。
- 处理身份验证的策略服务器节点(PSN)。

故障排除

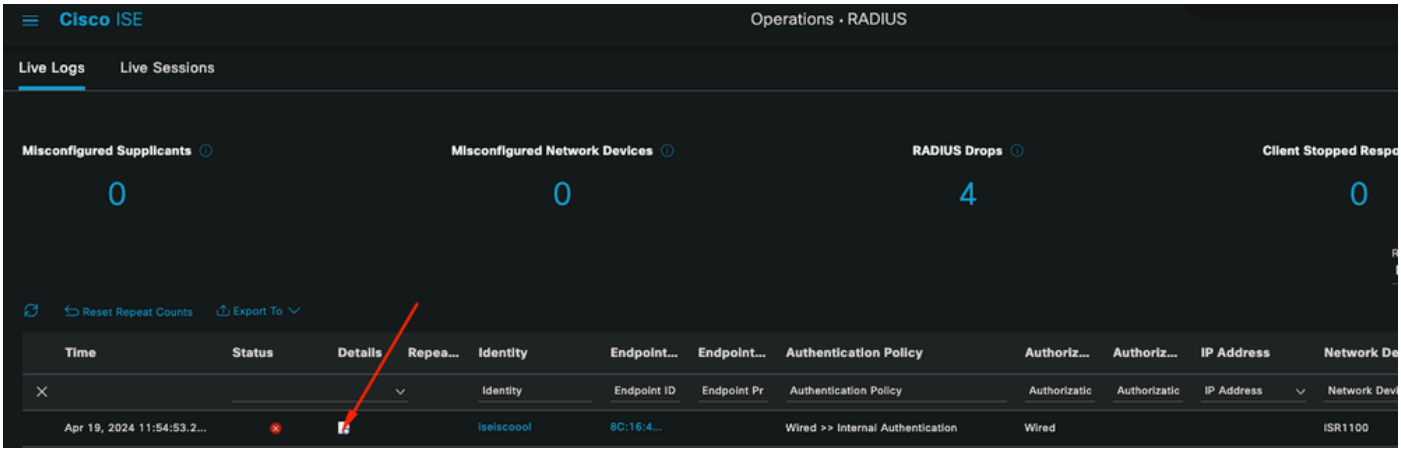
1 -读取ISE实时日志详细信息

导航到操作> Radius >实时日志选项卡，按身份验证状态：失败过滤，按使用的用户名过滤，按MAC地址过滤，按使用的网络接入设备过滤。

访问Operations > Radius > Live logs > Desired authentication > Live log details。

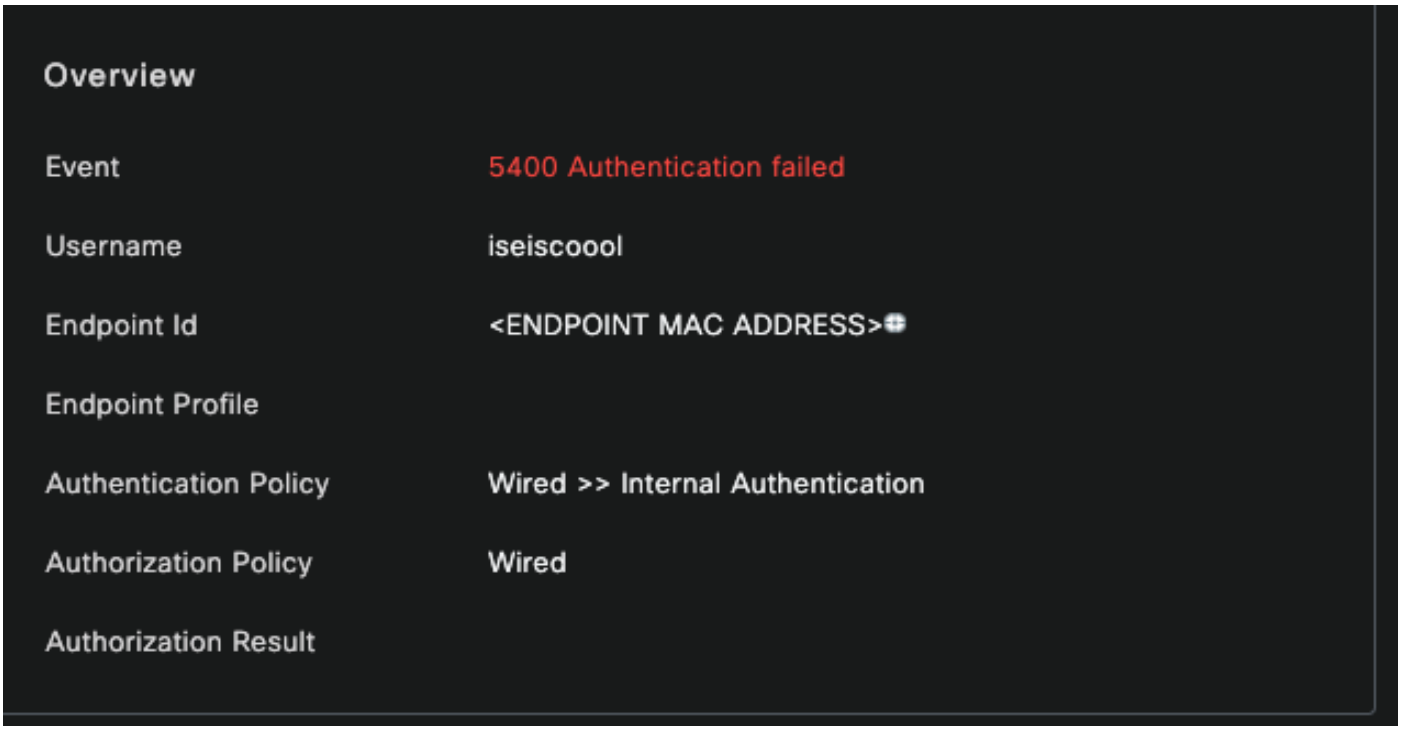
在同一页中，一旦过滤了身份验证，请点击搜索图标。

第一种情况：用户输入其用户名时输入拼写错误。



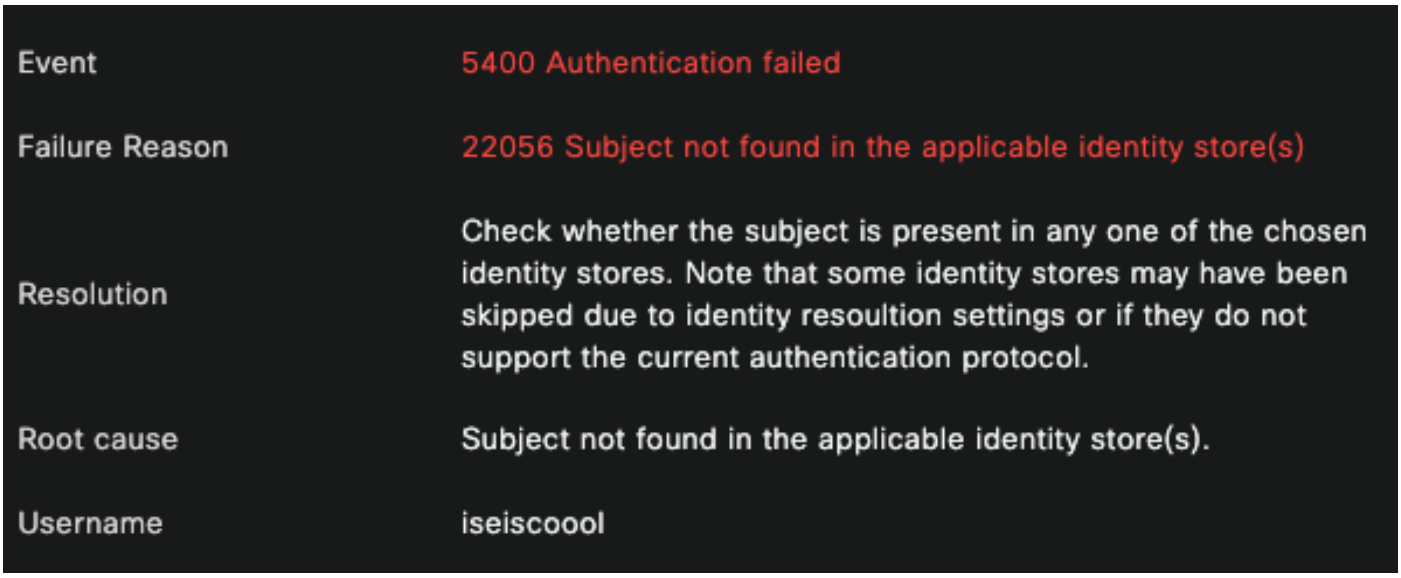
打开实时日志详细信息

打开实时日志详细信息后，您会看到身份验证失败，还会列出使用的用户名。



概述部分

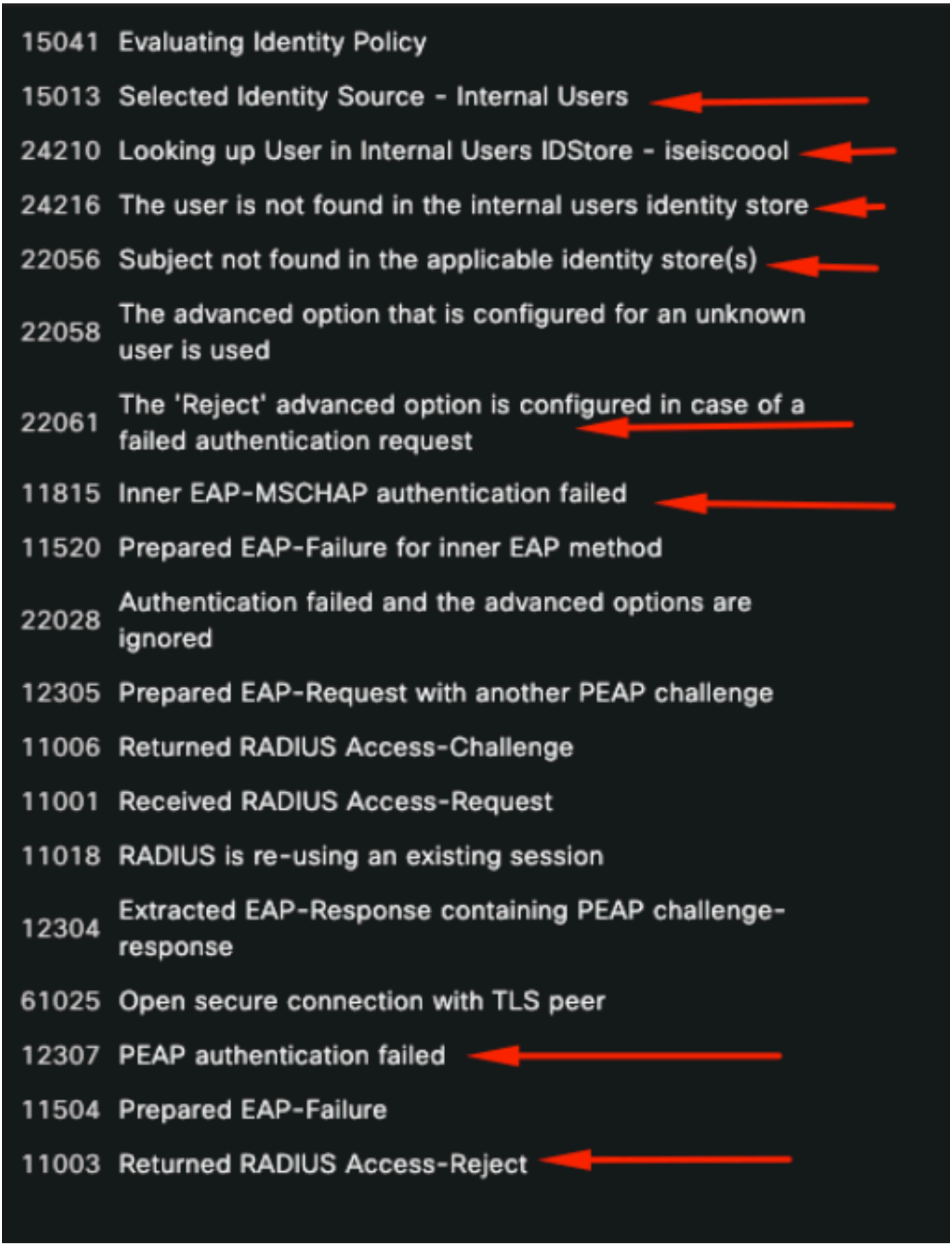
然后，在同一实时日志详细信息中，在“身份验证详细信息”部分中可以找到错误的故障原因、根本原因和解决方案。



身份验证详细信息

在此场景中，身份验证失败的原因是由于用户名拼写错误，但是，如果用户不是在ISE中创建，或者ISE无法验证用户存在于其他身份库（例如LDAP或AD）中，也会出现此错误。

Steps部分



Live Log Details步骤部分

步骤部分详细介绍ISE在RADIUS会话期间运行的过程。

您可以在此处找到以下信息：

- 对话是如何开始的。
- SSL握手过程。
- 协商的EAP方法。
- EAP方法进程。

在此示例中，可以看到ISE刚刚签入了此身份验证的内部身份。未找到用户，因此，ISE作为响应发送了Access-Reject。

第二个场景：ISE管理员从策略集允许(Policy Set Allowed)协议禁用PEAP。

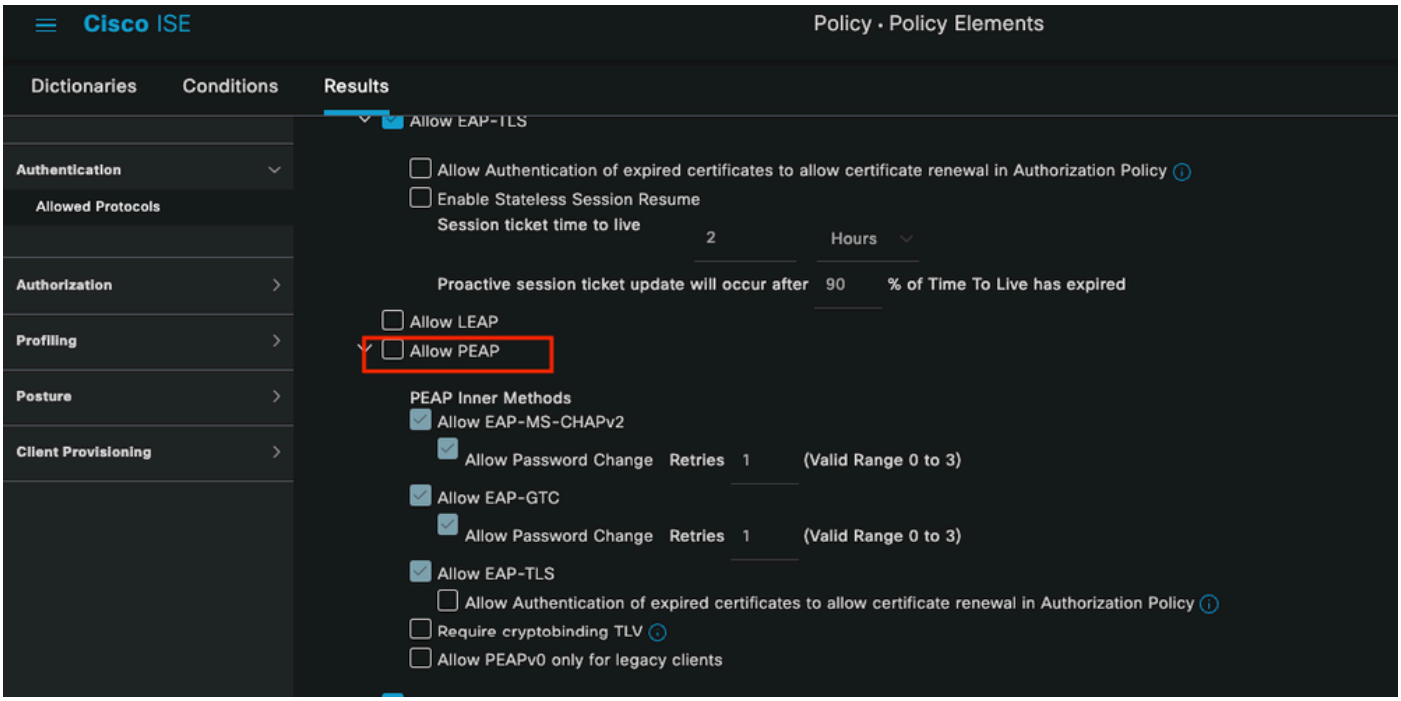
2 -已禁用PEAP

打开会话失败的实时日志详细信息后，系统会显示错误消息“PEAP is not allowed in the Allowed Protocols”（允许的协议中不允许PEAP）。

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

实时日志详细信息报告

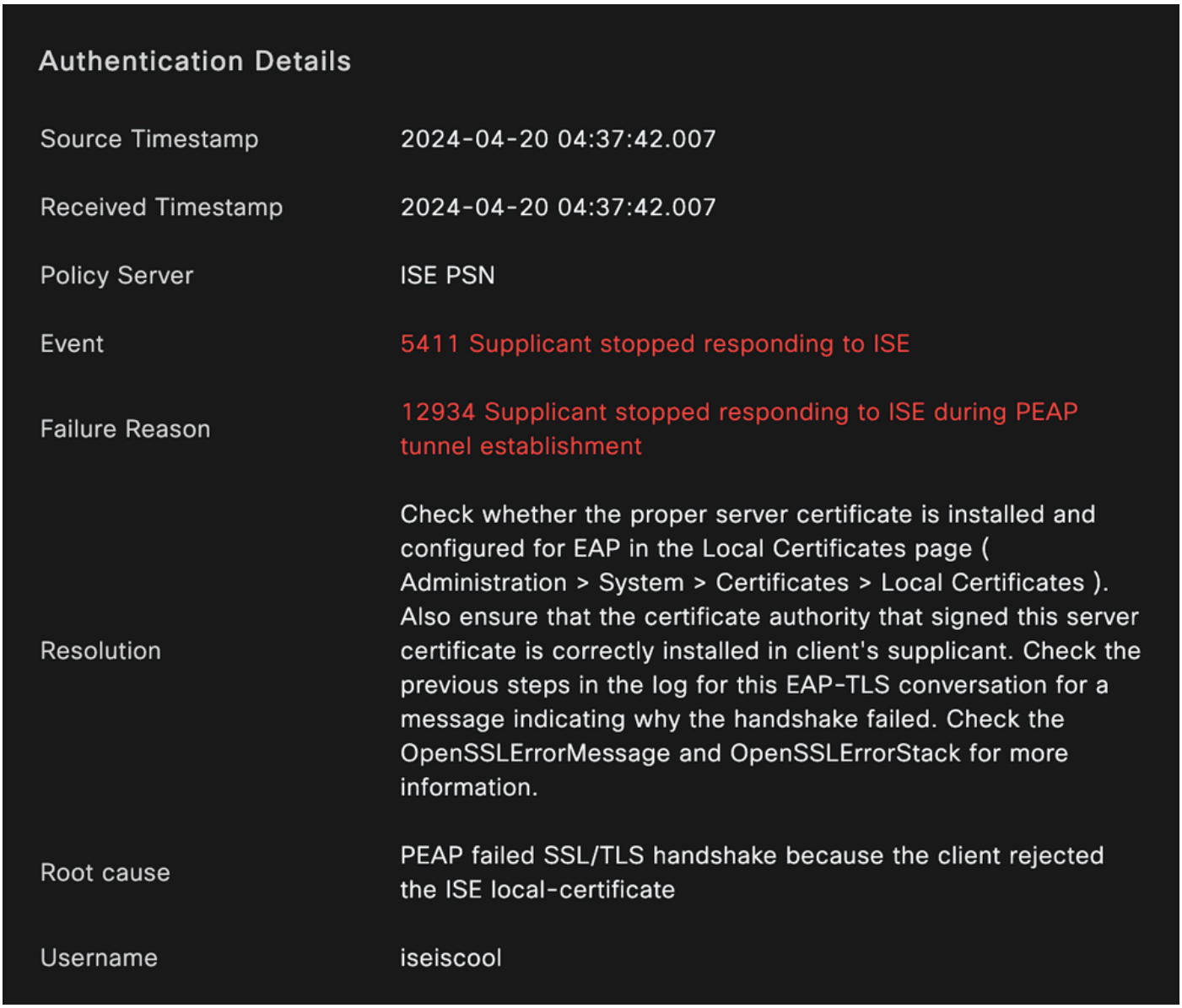
此错误很容易解决，解决方法是导航到策略>策略元素>身份验证>允许的协议。 验证是否已禁用选项Allow PEAP。



Allowed Portocols部分

第三种情况：身份验证失败，因为终端不信任ISE证书。

导航到实时日志详细信息。查找失败的身份验证的记录，并检查实时日志详细信息。

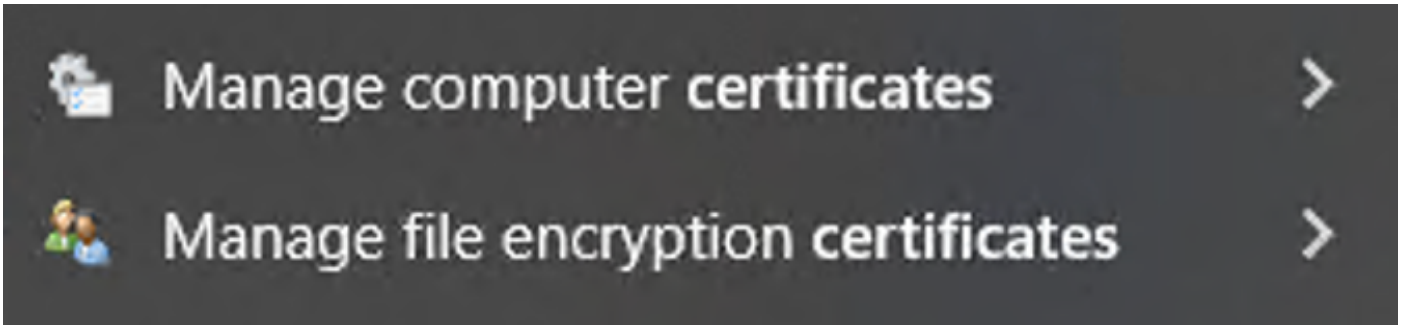


实时日志详细信息

终端拒绝用于建立PEAP隧道的证书。

要解决此问题，请在存在问题的Windows终端中验证签署ISE证书的CA链位于管理用户证书>受信任的根证书颁发机构部分或管理计算机证书>受信任的根证书颁发机构部分中。

通过在Windows搜索栏中搜索配置，可以在Windows设备上访问配置部分。

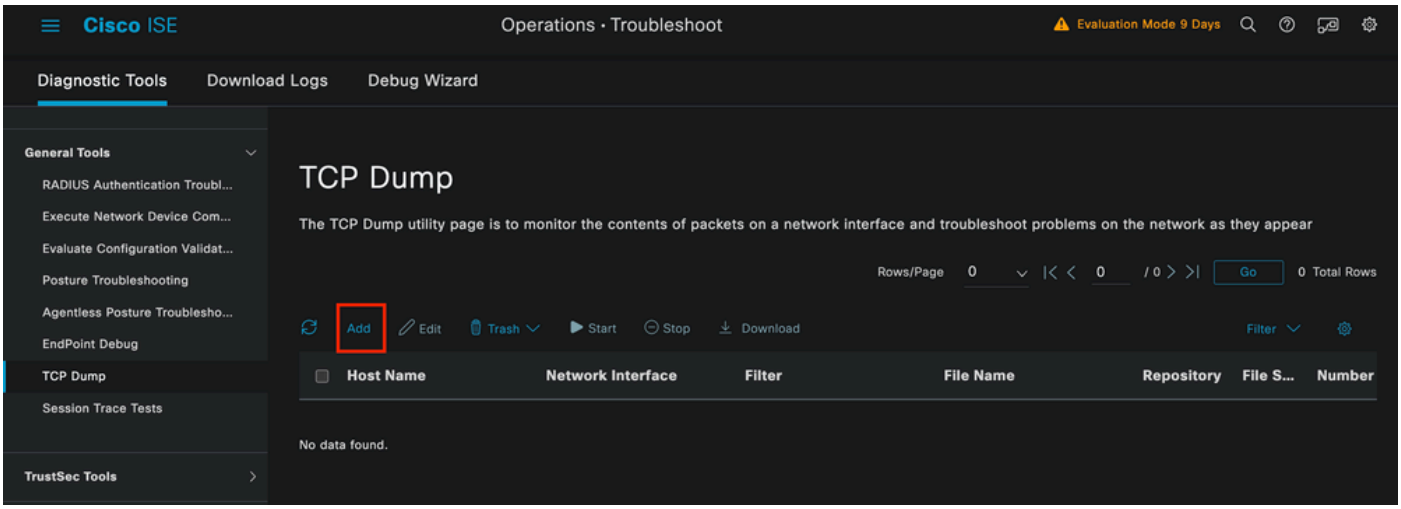


Windows搜索栏结果

3 - ISE TCP转储工具（数据包捕获）

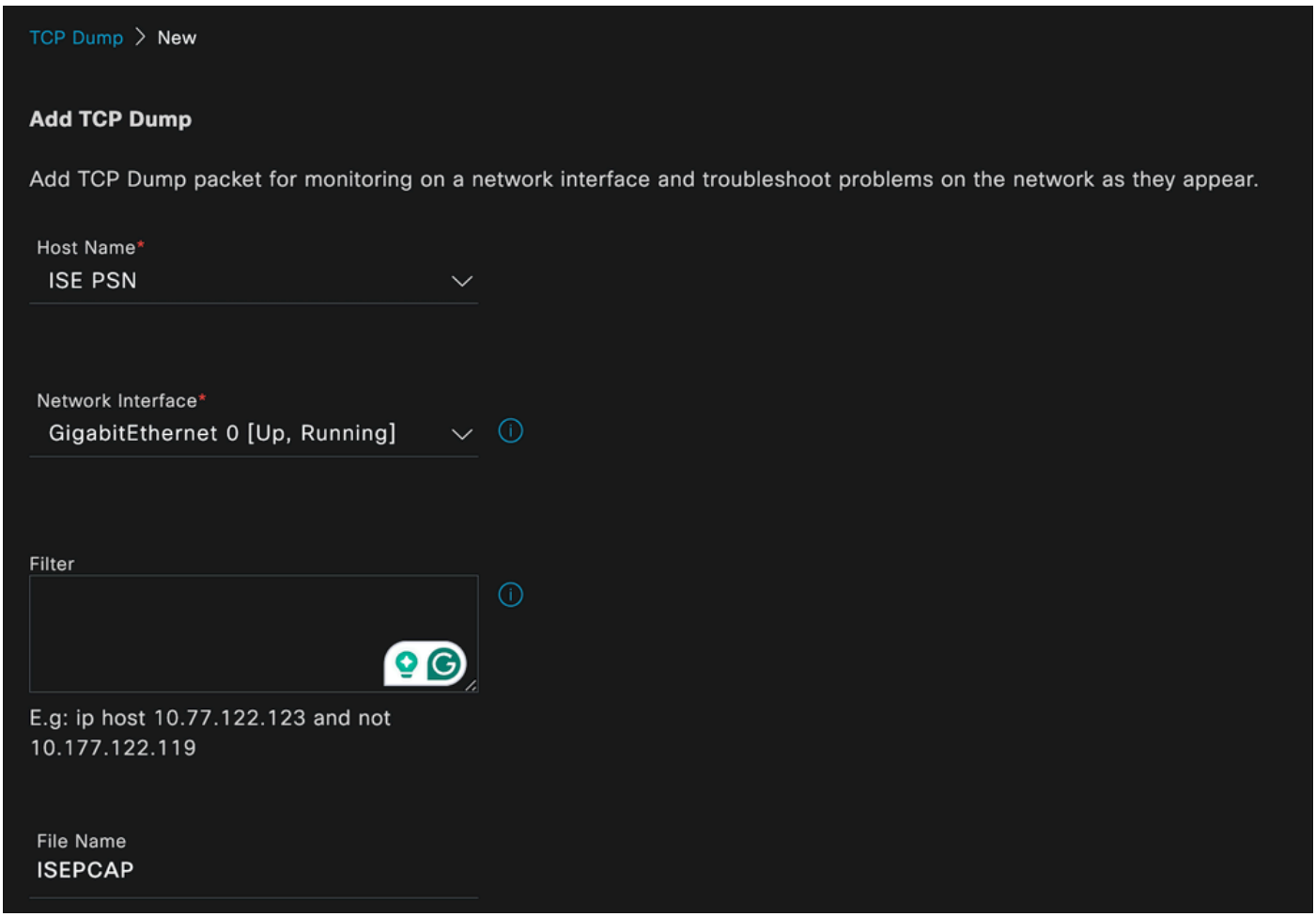
在故障排除时，数据包捕获分析必不可少。直接从ISE数据包捕获可在所有节点和节点的任何接口上进行。

要访问此工具，请导航到操作>诊断工具>General Tools> TCP转储。

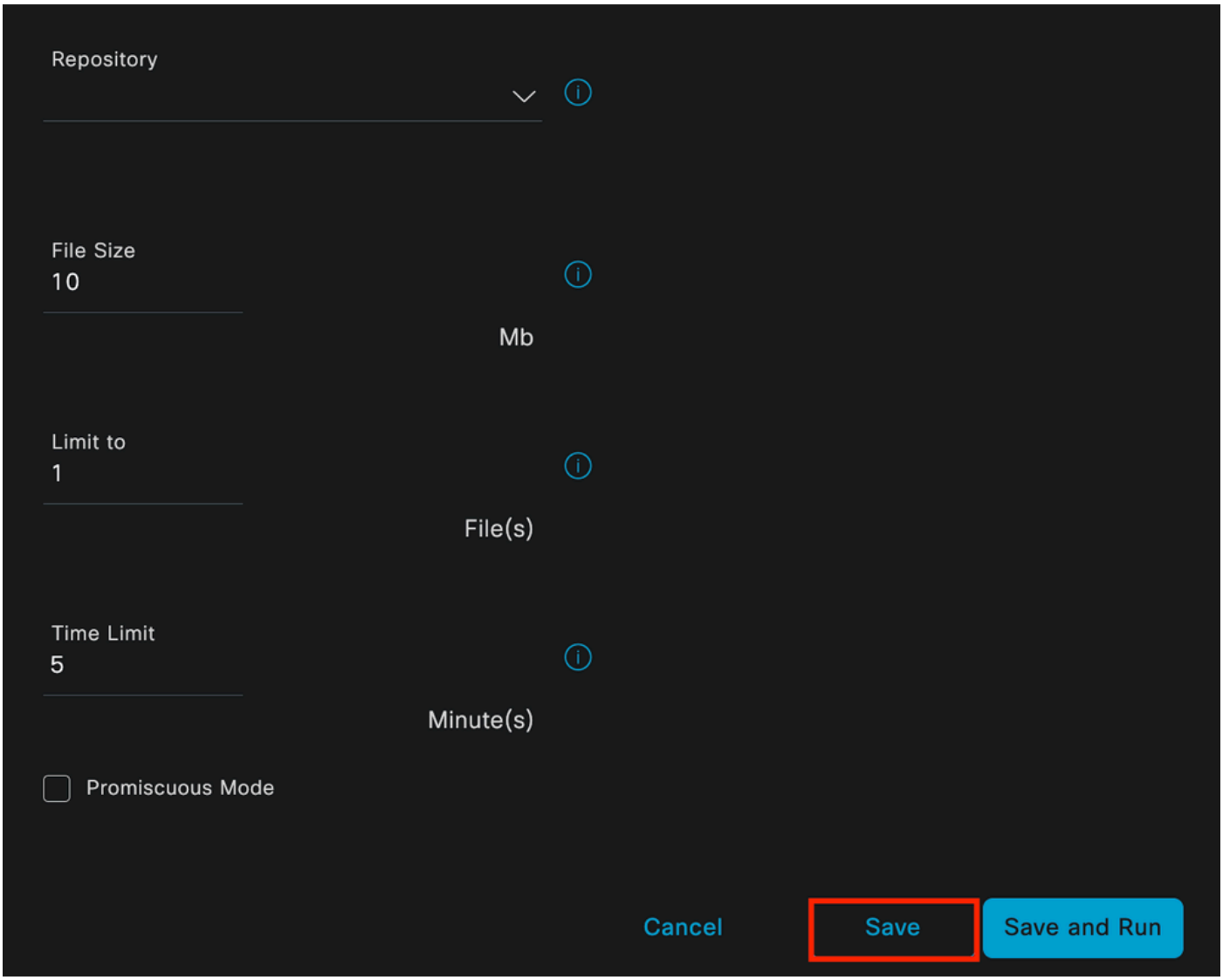


TCP Dump部分

单击Add按钮开始配置pcap。



TCP转储创建

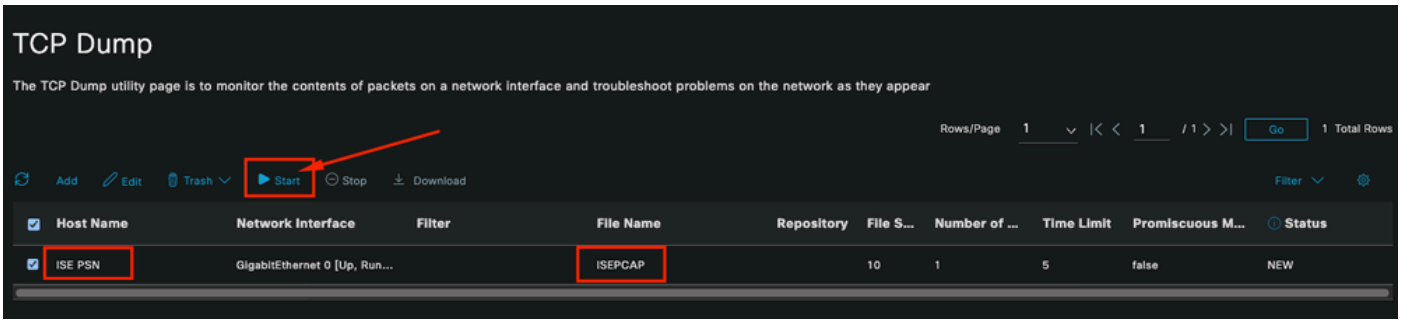


TCP Dump部分

要在ISE中创建pcap，您必须输入以下数据：

- 选择需要获取pcap的节点。
- 选择用于pcap的ISE节点接口。
- 如果需要捕获特定流量，请使用过滤器，ISE会提供一些示例。
- 为pcap命名。在此场景中，我们使用了ISEPCAP。
- 选择存储库，如果未选择存储库，则捕获保存在ISE本地磁盘上并可从GUI下载。
- 此外，如有必要，请修改pcap文件大小。
- 如有必要，使用超过1个文件，因此如果pcap超过文件大小，随后将创建一个新文件。
- 如果需要，可以延长pcap的流量捕获时间。

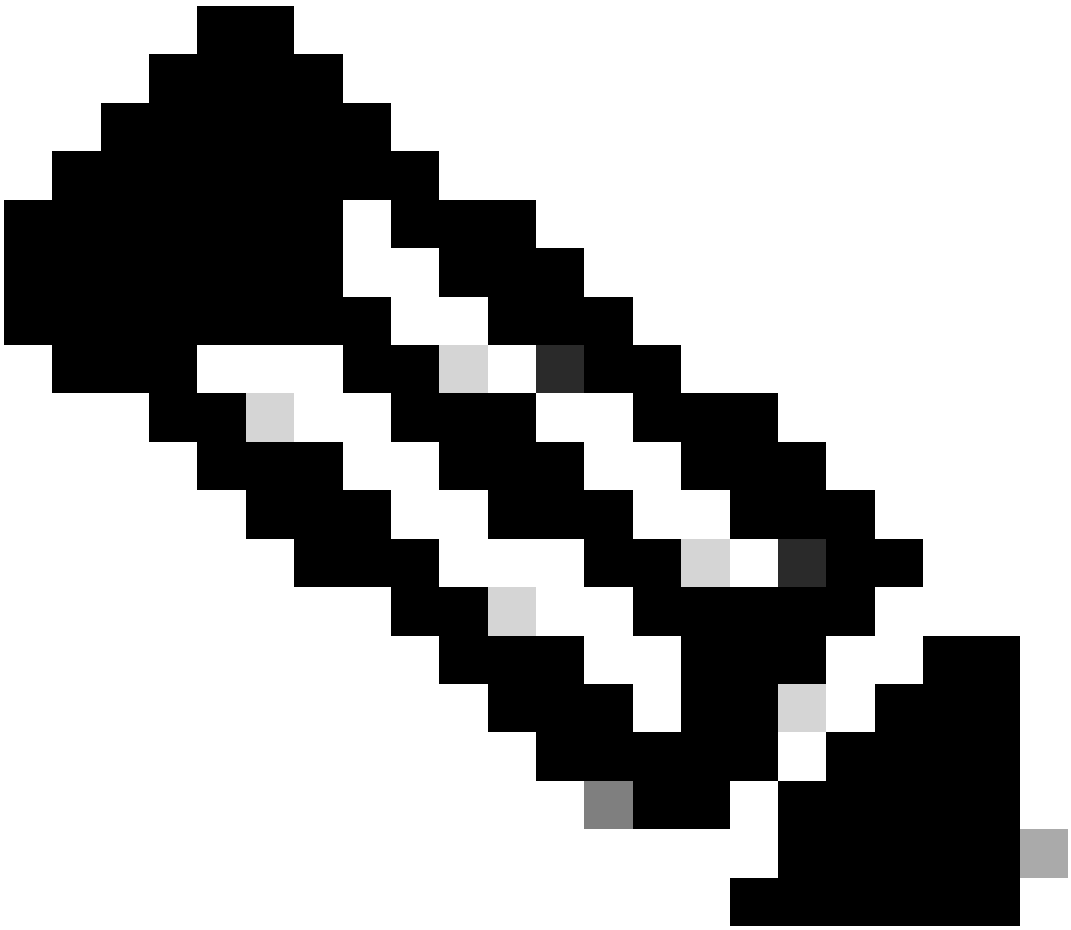
最后，单击Save 按钮。



TCP Dump部分

然后，选择pcap准备就绪后，单击开始按钮。

单击Start后，Status列将更改为RUNNING状态。



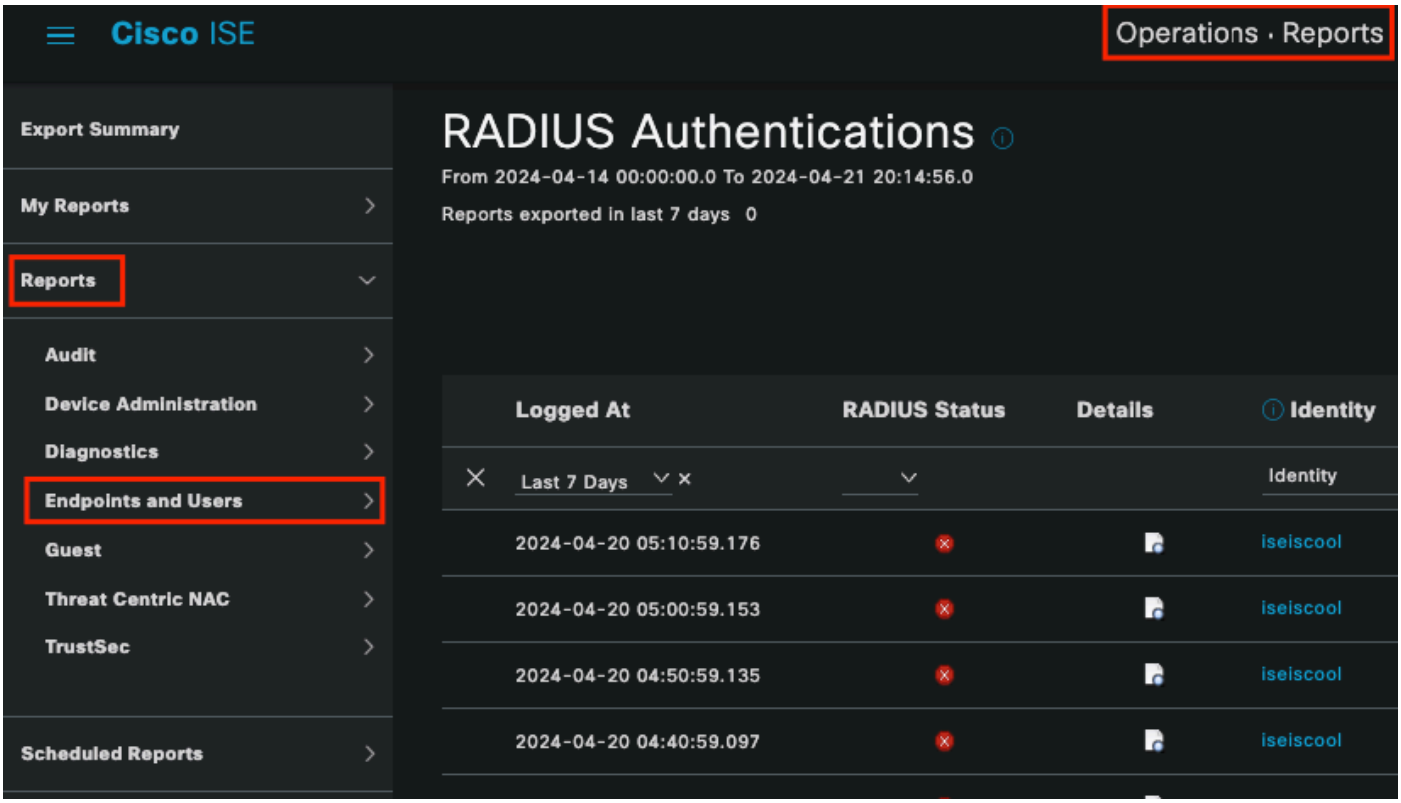
注意：当PCAP处于运行状态时，会复制失败场景或需要捕获的行为。完成后，即可在PCAP中看到RADIUS、会话的详细信息。

在PCAP运行时捕获所需的数据后，完成pcap收集。再次选择它并单击Stop。

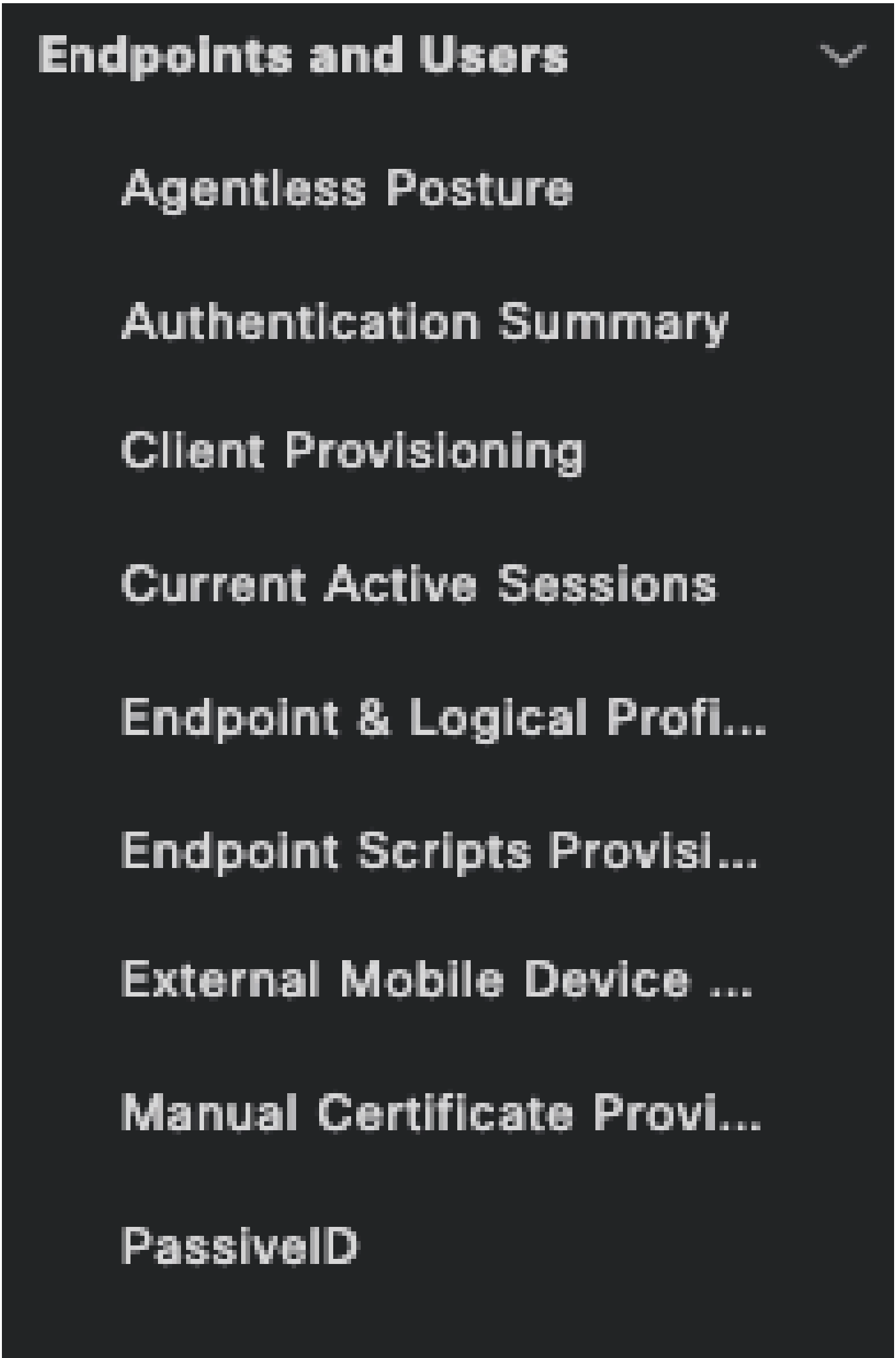
3 – 1个ISE报告

如果需要更深入的分析，ISE会提供有用的报告来调查过去的事件。

要找到这些报告，请导航到操作>报告>报告>端点和用户

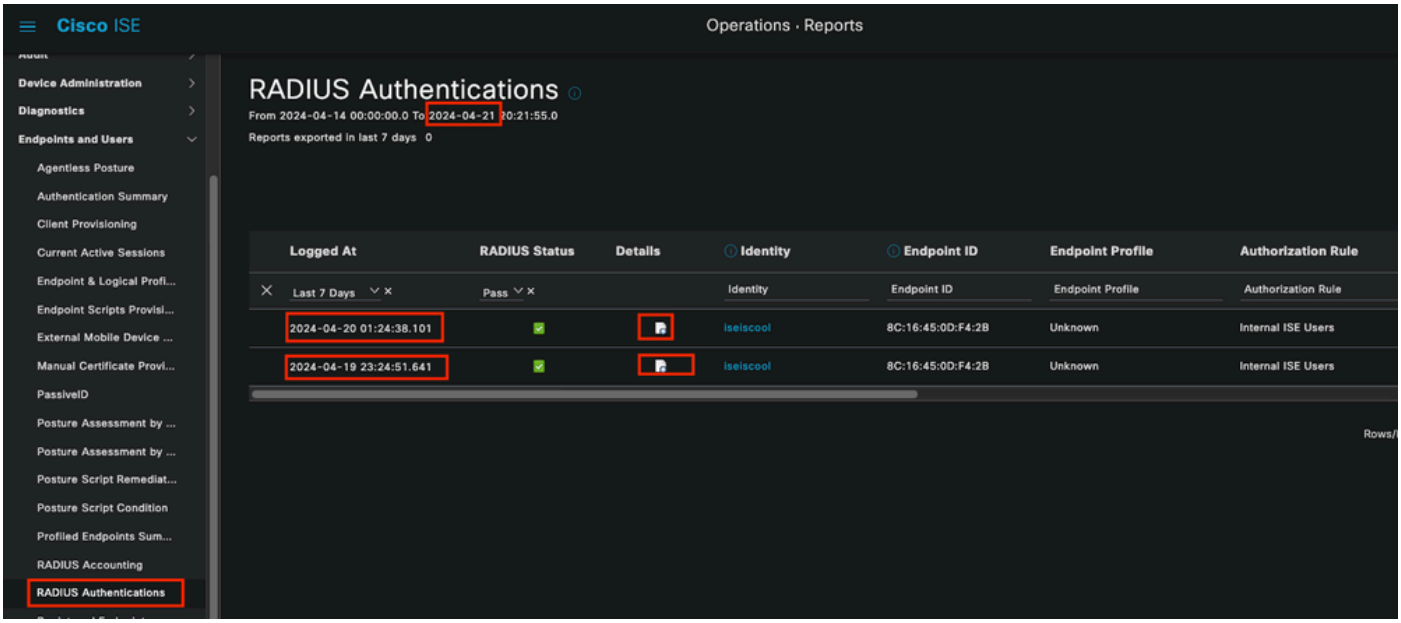


ISE报告部分


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

实时日志部分，您可以选择最长24小时的过去数据。有时需要进行旧的身份验证。如果过去正常运行的身份验证突然开始失败，您必须将过去正常运行的身份验证与过去正常运行的身份验证进行比较。您可以使用RADIUS身份验证报告实现此目的。

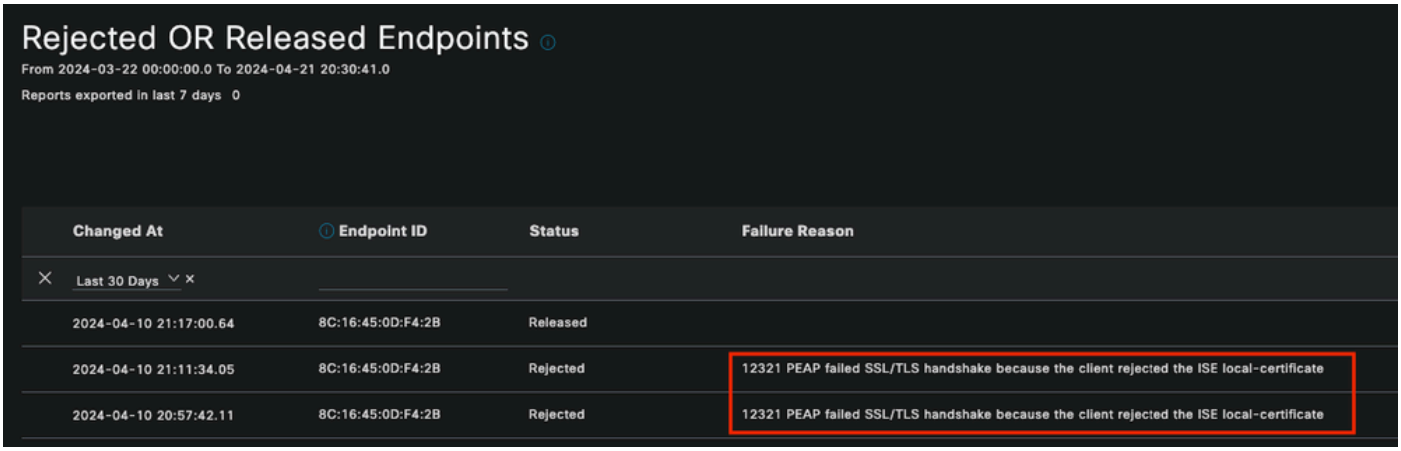
该报告允许您选择最长30天的时间范围。此外，保留每个身份验证的实时日志详细信息报告。



身份验证报告

3-3个被拒绝或释放的终端

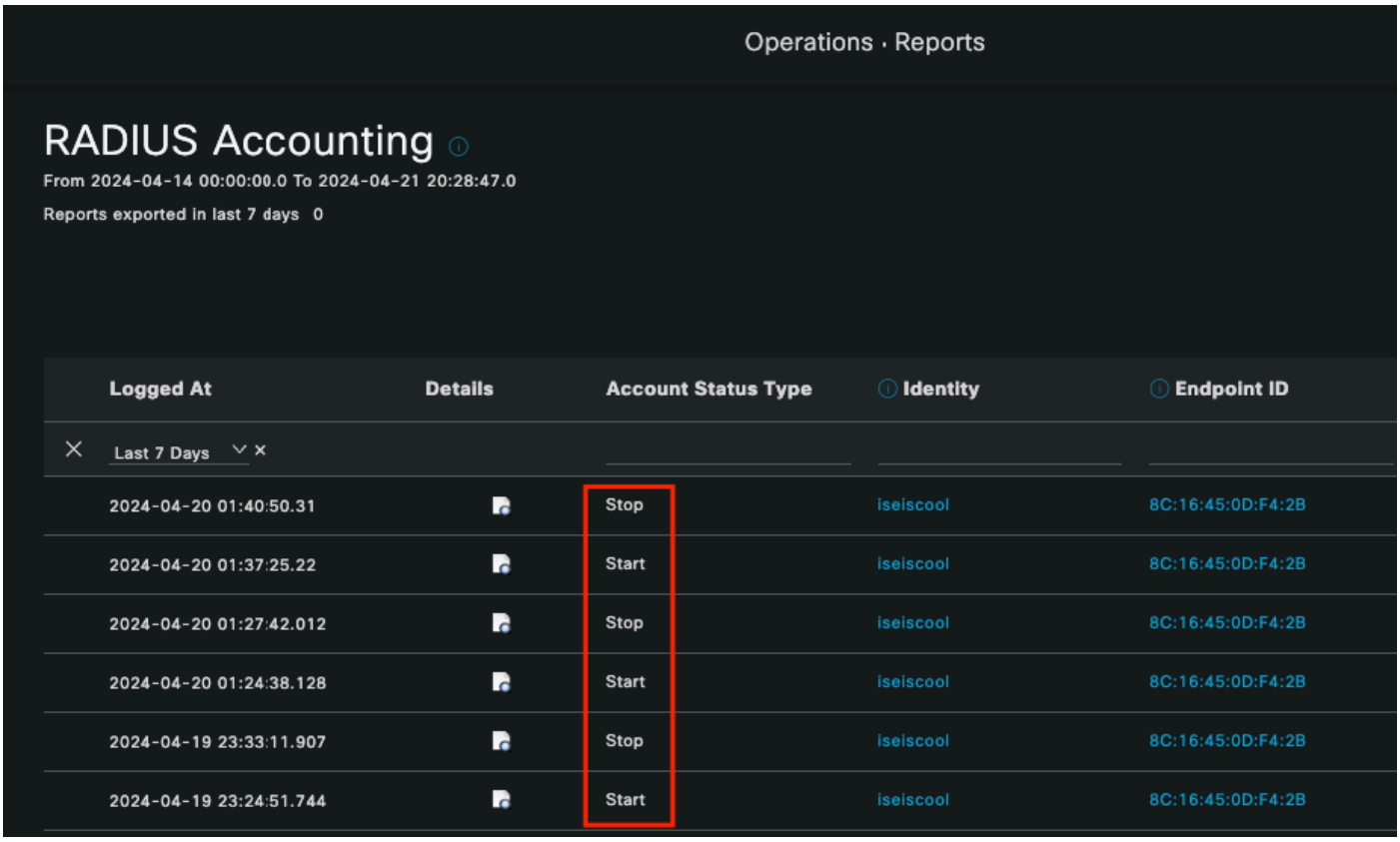
验证拒绝端点的故障原因。您可以检查“已拒绝(Rejected)”或“已释放(Released)”终端报告。在ISE部署中的所有PSN节点上更新EAP证书，然后PEAP身份验证开始失败整个区域的方案中。可以检查此报告，而不检查实时日志详细信息，您会知道客户端拒绝且不信任ISE证书。



拒绝的终端报告

3-4 RADIUS记帐报告

当发现过度许可使用问题时，通常使用此方法。 在这些情况下，ISE不会释放许可证，因为它无法确定会话是否完成。ISE使用网络设备发送的记帐数据包来确定这一点。当记账从网络设备正确共享到ISE时，情况如下：



RADIUS记帐报告

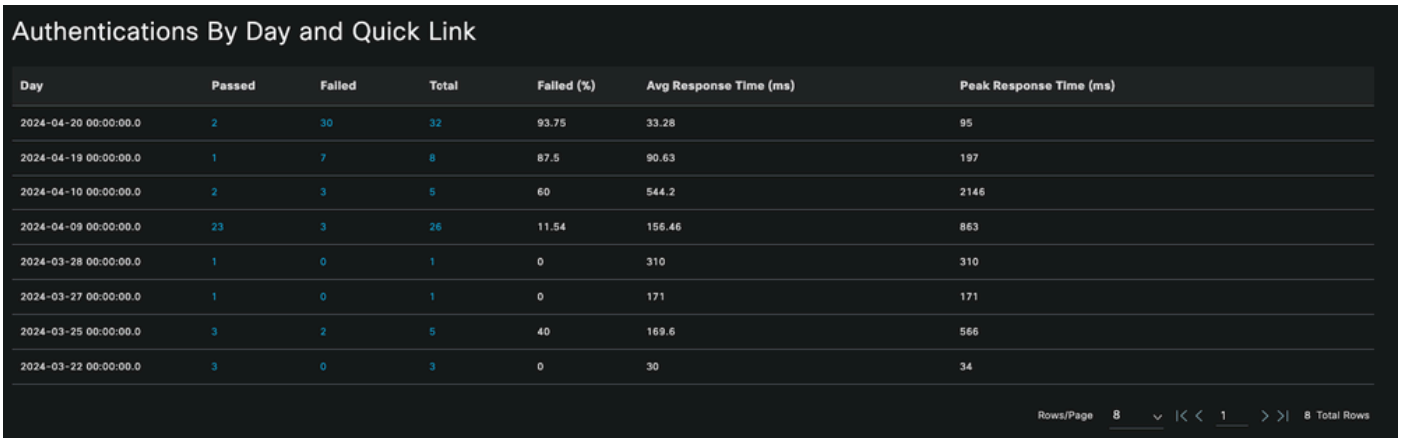
3-5身份验证摘要报告

这些是ISE提供的常用和有用报告。它允许您选择最多30天的旧数据。在此报告中，您可以看到以下信息：

- 按天列出的通过身份验证和失败身份验证的百分比。

图表：按天传递的身份验证

- 每天的身份验证次数，在图表中，并且可以选择单击蓝色值查看详细数据。

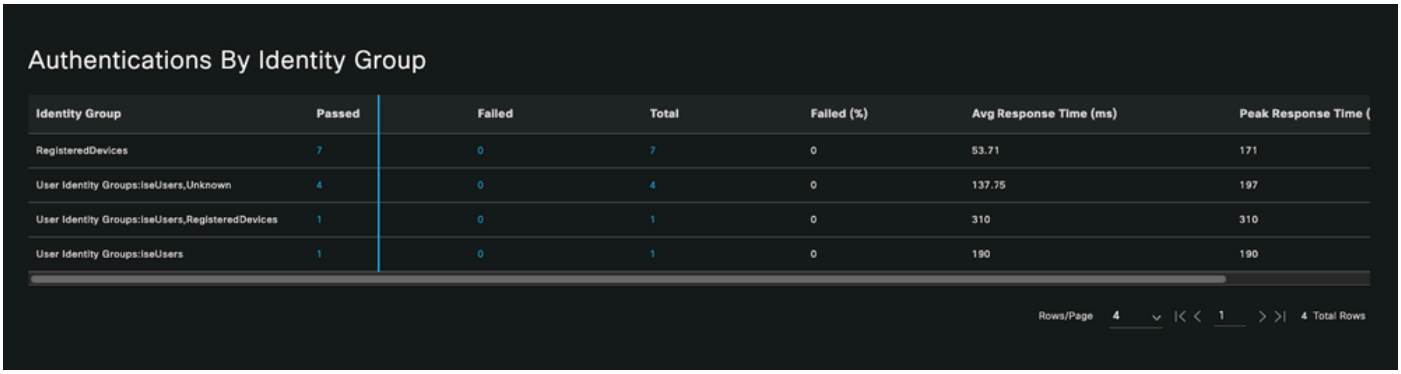


按天和快速链接进行身份验证

- 按失败原因进行身份验证，列在顶部列表中，重复次数最多，重复次数较少。

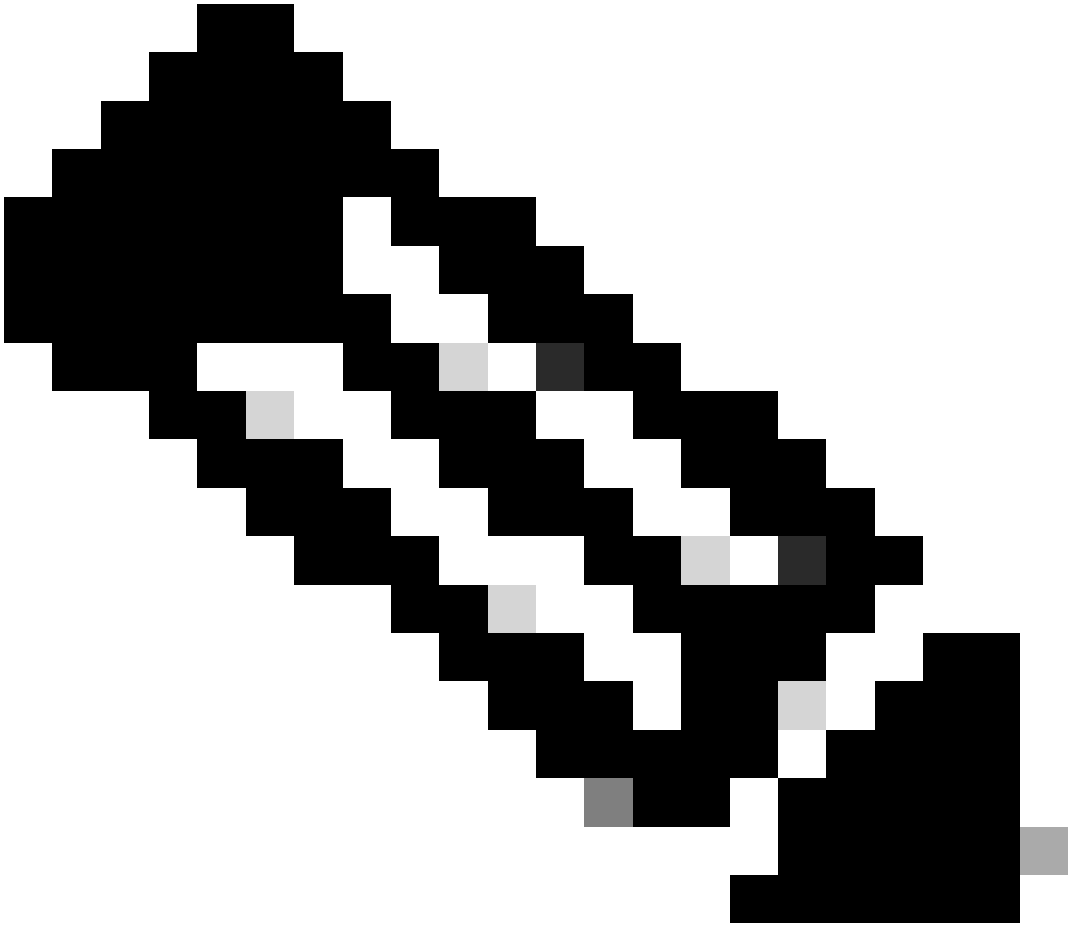
按故障原因进行的身份验证

- 选项用于查看部署身份验证中常用的身份组。

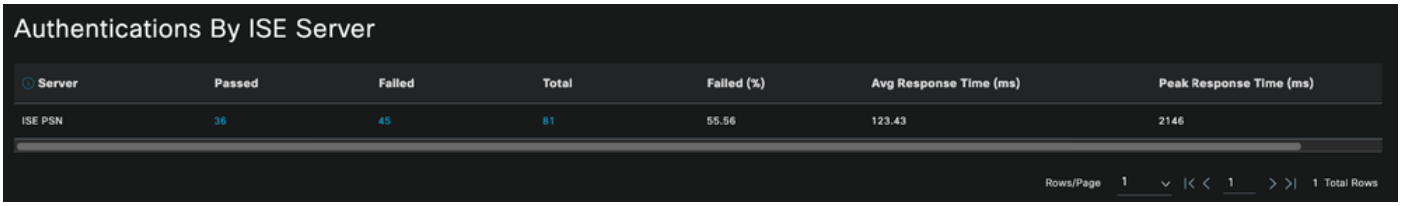


按身份组进行身份验证

- 哪个PSN接收更多身份验证。



注意：在用于本文档的部署中，仅使用了一个PSN；但是，对于较大的部署，此数据对于查看是否需要负载均衡十分有用。



通过ISE服务器进行身份验证

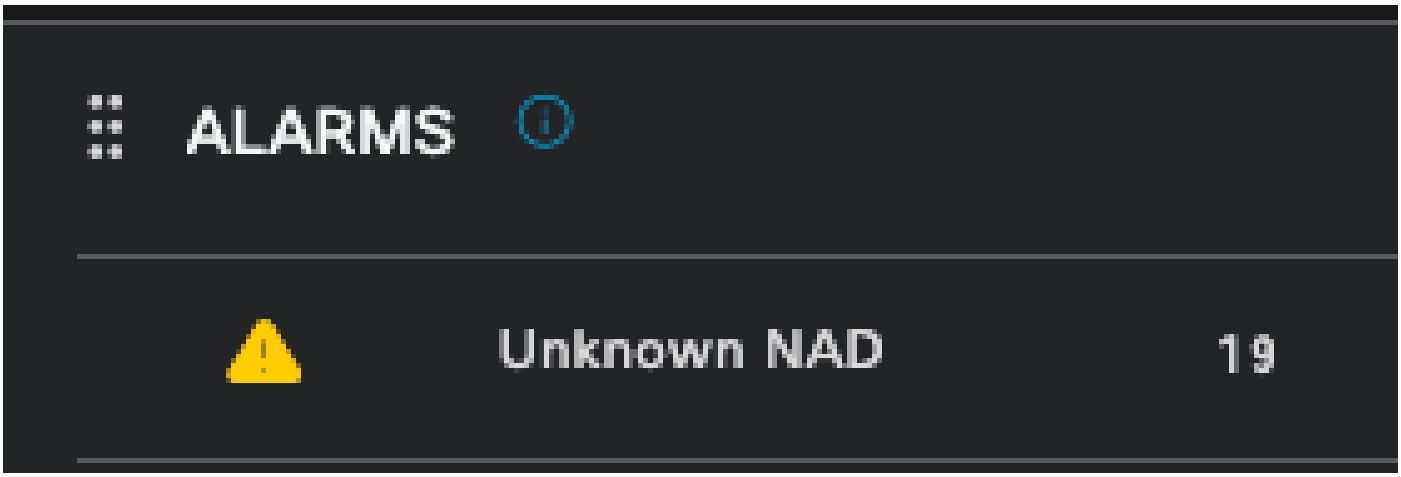
4 - ISE警报

在ISE Dashboard下，Alarms部分显示部署问题。

以下是有助于故障排除的几个ISE警报。

Unknown NAD —当存在网络设备对终端进行身份验证并访问ISE时，会显示此警报。但是，ISE不信任它，它会丢弃RADIUS连接。最常见的原因是，未创建网络设备或网络设备使用的IP与ISE注册

的IP不同。

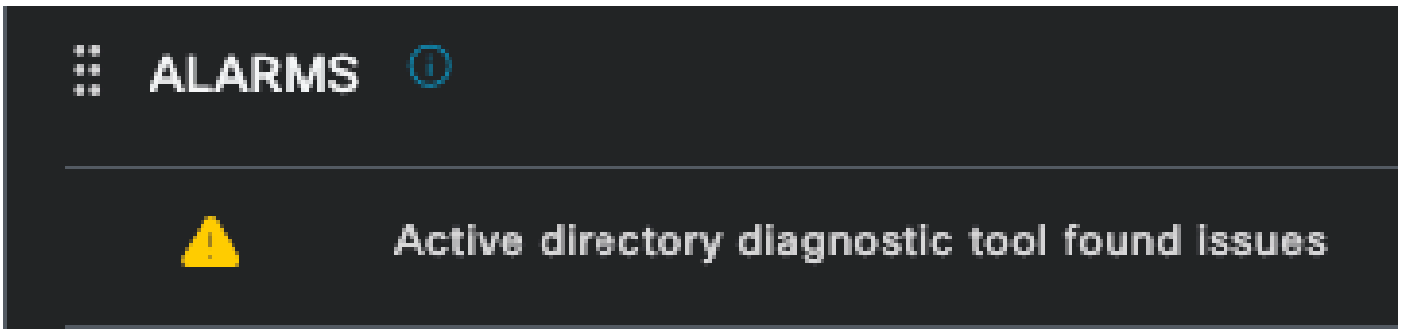


未知NAD

Supplicant客户端停止响应 —当请求方通信存在问题时，会发生此警报，大多数时间是因为请求方配置错误，需要在终端端检查和调查。

请求方停止响应

Active directory诊断工具发现问题— 使用Active Directory验证用户身份时，如果通信进程开始出现问题，或者连接中断，您将看到此警报。然后，您会了解AD上存在该身份的身份验证失败的原因。



AD诊断失败

COA（授权更改）失败 - ISE中的多个流使用CoA，此警报会在与任何网络设备的CoA端口通信期间出现问题时通知您。

Coa失败

5 - ISE调试配置和日志收集

要继续了解身份验证过程的详细信息，必须启用调试中有关mab和dot1x问题的以下组件：

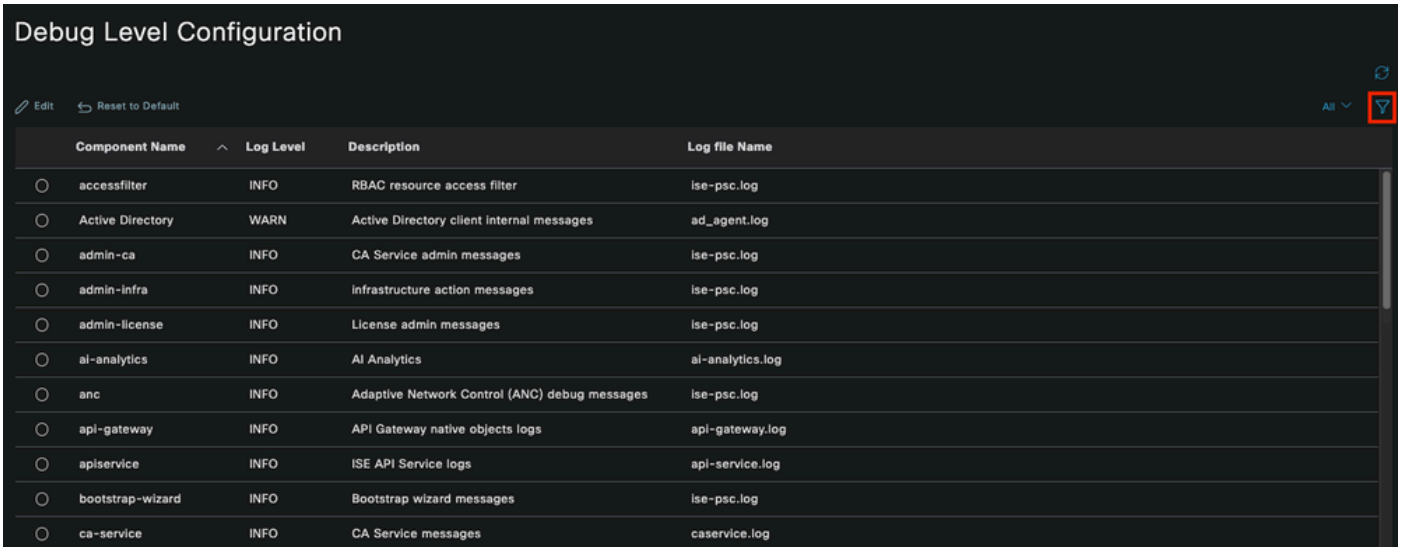
问题：dot1x/mab

要设置为调试级别的属性。

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

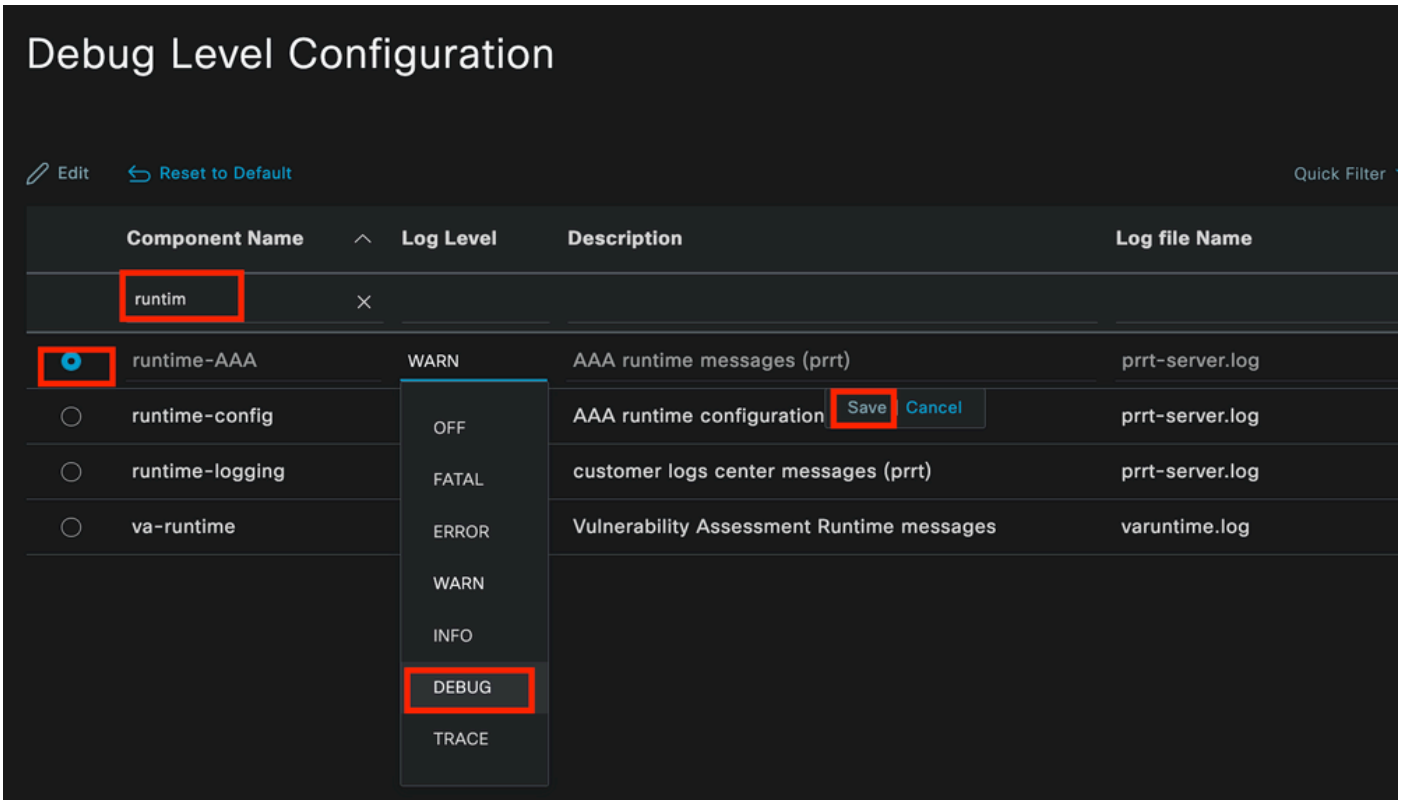
要使组件达到调试级别，首先需要确定哪个PSN接收了失败的身份验证或需要进行调查。您可以从实时日志中获取此信息。之后，您必须转至ISE菜单>故障排除>调试向导>调试日志配置>选择PSN>单击Edit按钮。

将显示下一个菜单。点击过滤器图标：



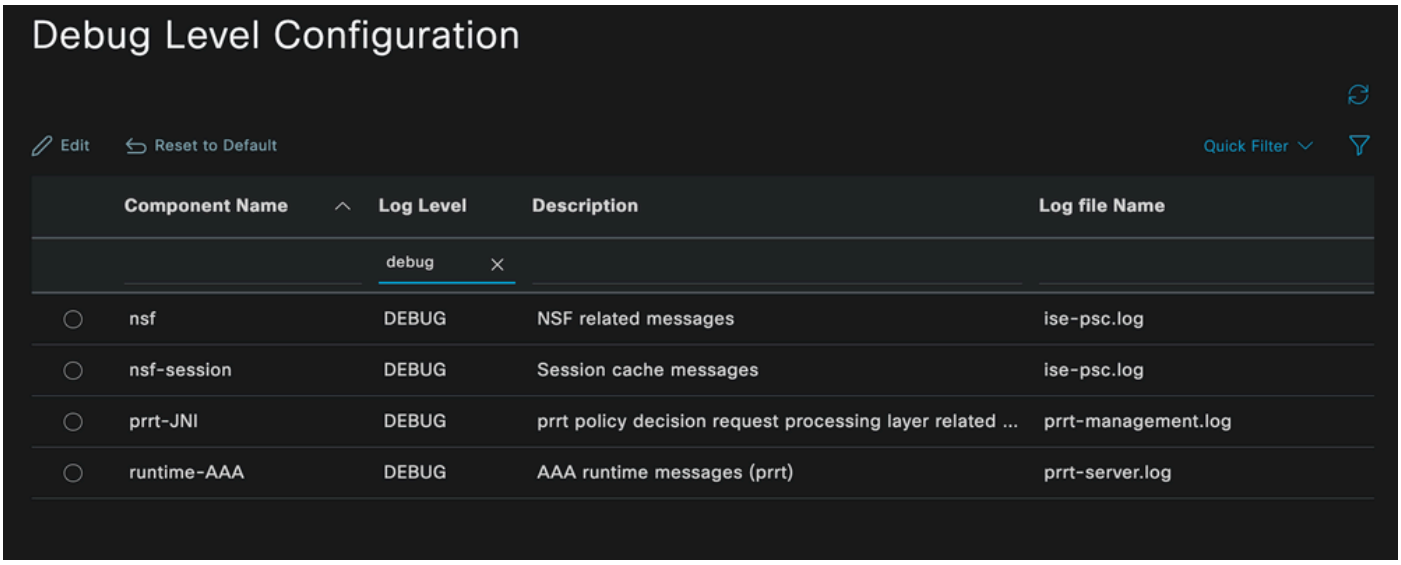
调试日志配置

在组件名称列中，搜索以前列出的属性。选择每个日志级别并将其更改为DEBUG。保存更改。



运行时AAA组件设置

完成每个组件的配置后，请使用DEBUG对其进行过滤，以便查看是否所有组件都配置正确。

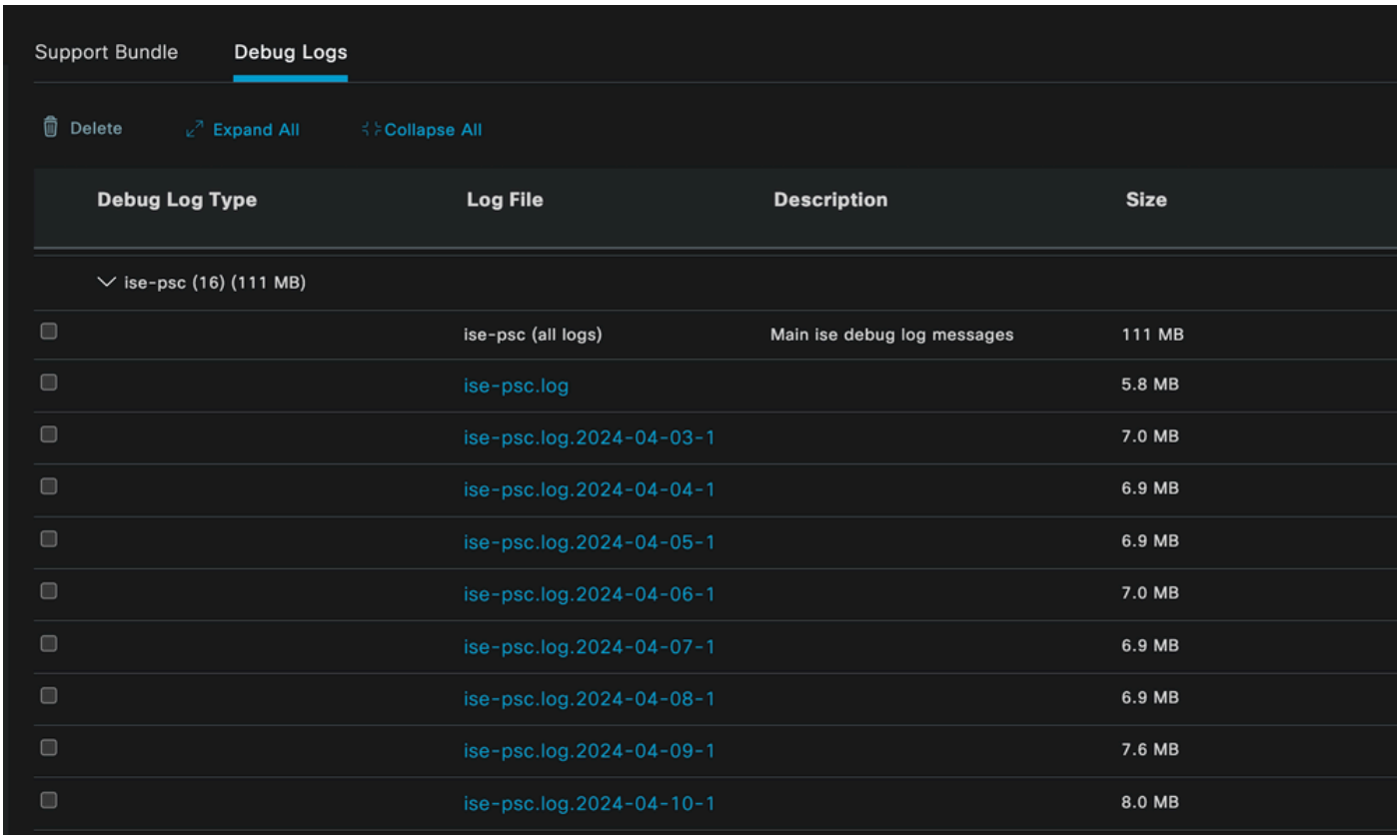


调试日志配置

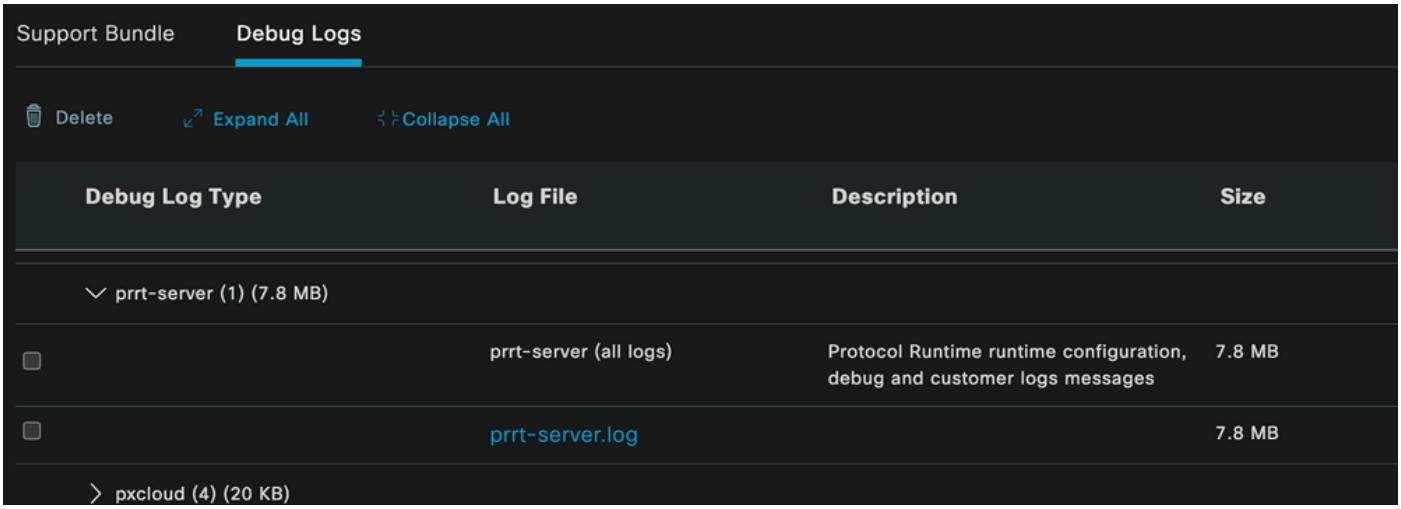
如果需要立即分析日志，您可以导航到路径ISE Menu > Operations > Troubleshoot > Download Logs > Appliance node list > PSN并启用DEBUGS > Debug Logs以下载日志。

在这种情况下，您必须在prrt-server.log和ise-psc.log中下载dot1x和mab问题。您必须下载的日志是包含上次测试日期的日志。

只需单击此图像中所示的日志文件并下载它（以蓝色文本显示）。



从PSN节点调试日志

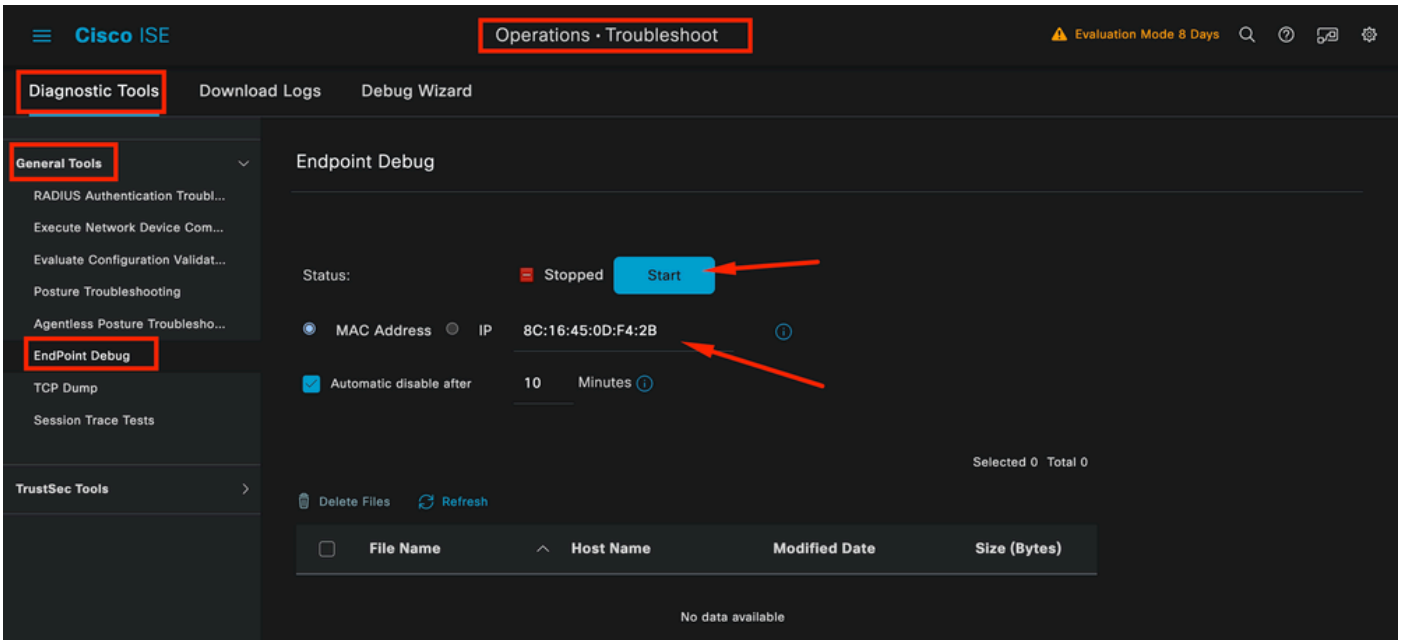


Debug Logs部分

6 -每个终端的ISE调试

还有另一个选项可用于根据MAC地址或IP为每个终端获取DEBUG日志。您可以使用端点调试ISE工具。

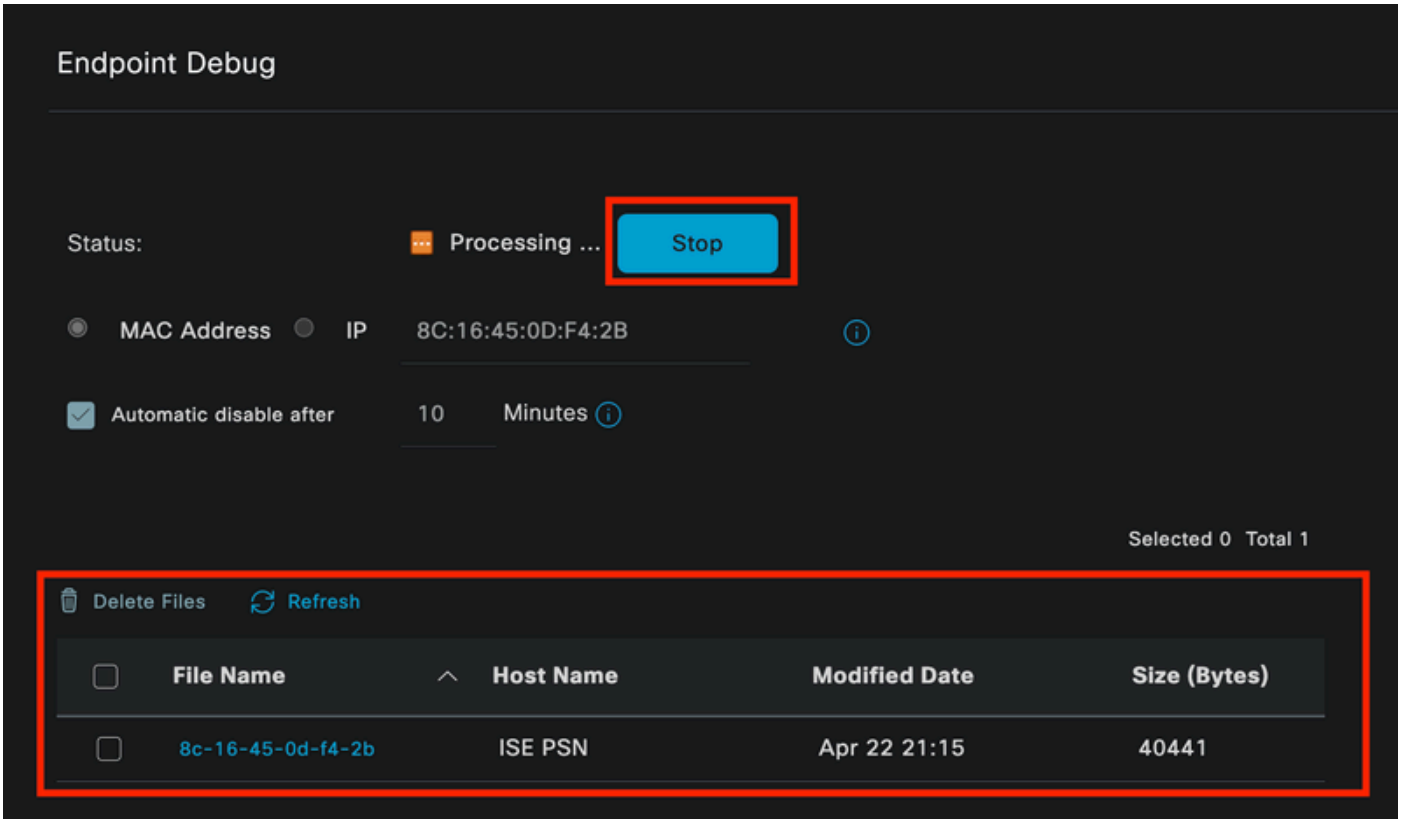
导航到ISE菜单>操作>故障排除>诊断工具>常规工具>终端调试。



终端调试

然后输入所需的终端信息以开始捕获日志。单击开始。

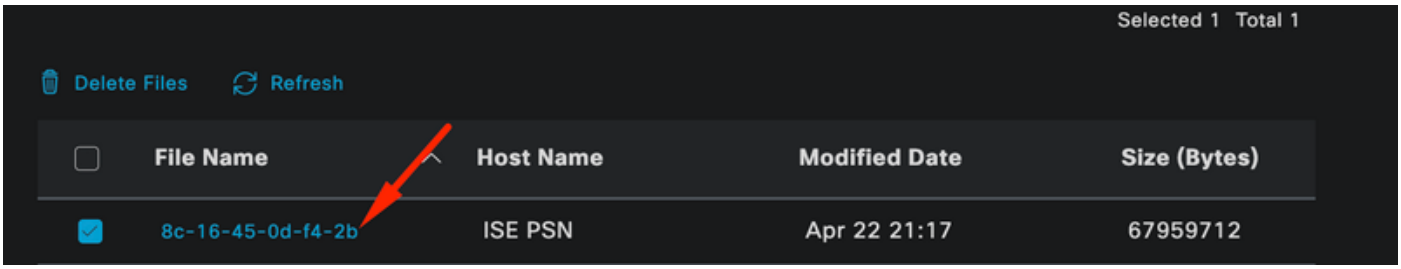
然后，在警告消息中单击Continue。



终端调试

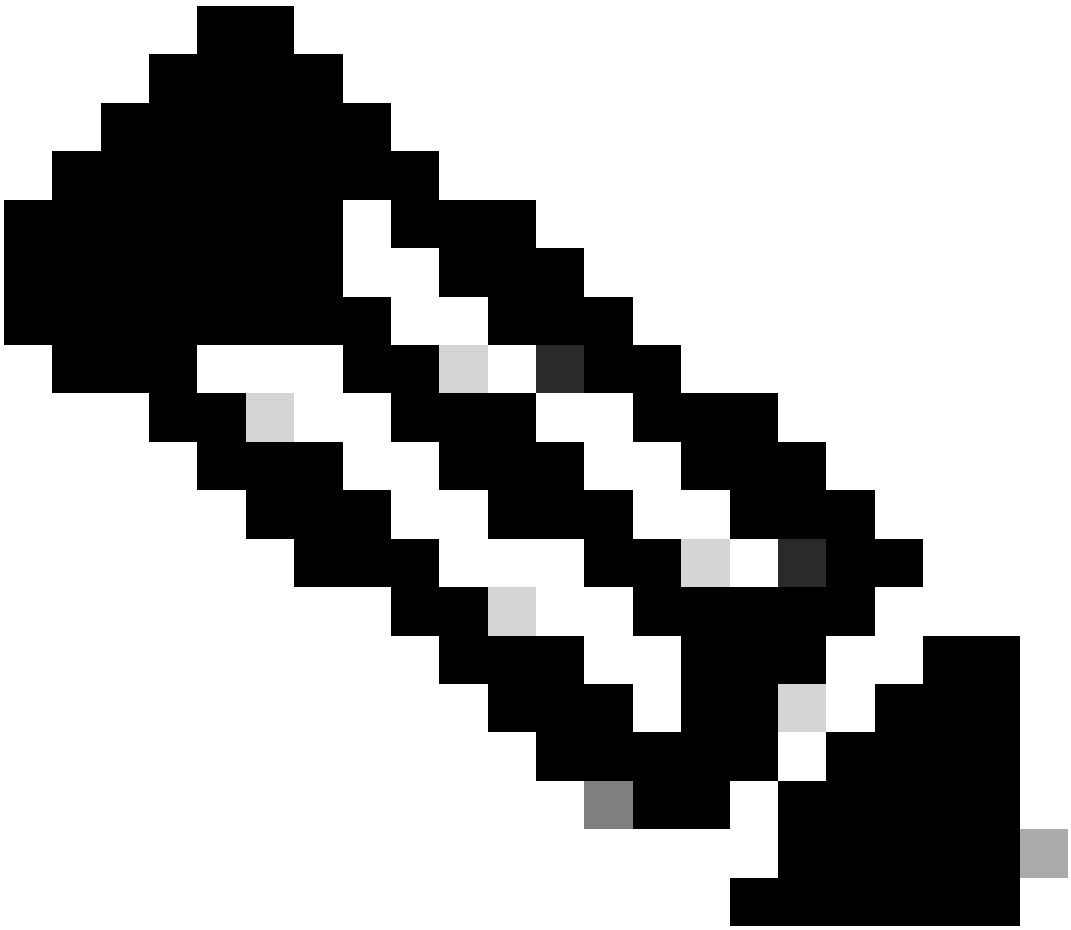
捕获信息后，单击Stop。

单击此图中显示为蓝色的文件名。



终端调试

您必须能够查看带DEBUG日志的身份验证日志，而无需直接从Debug Log Configuration启用它们。

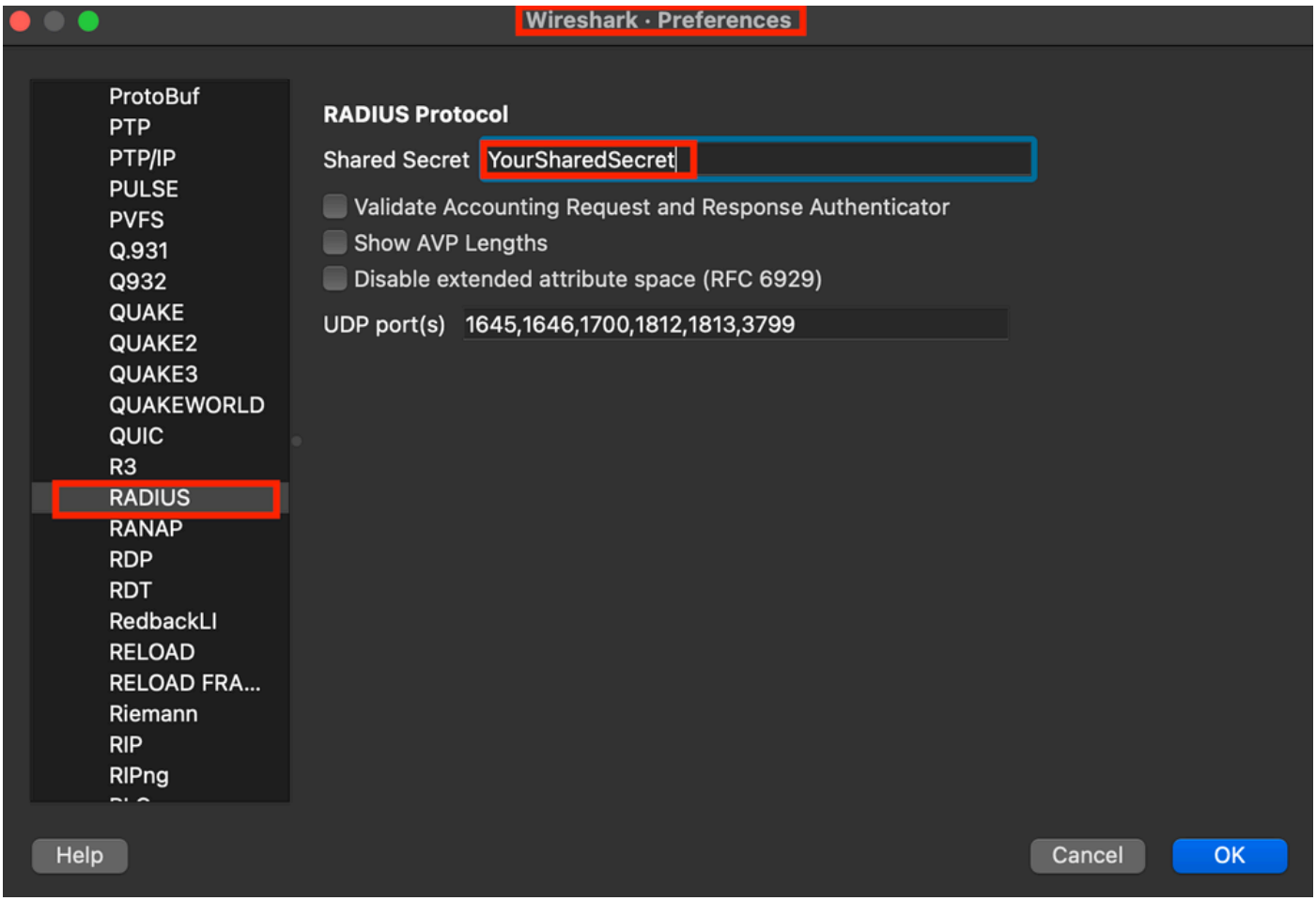


注意：由于终端调试输出中可能会忽略某些内容，因此您将获得一个更完整的日志文件，通过调试日志配置生成该文件并从任何需要的文件下载所有必需的日志。如前面的ISE调试配置和日志收集部分所述。

---

7 -解密RADIUS数据包

除user password字段外，Radius数据包不加密。但是，您需要验证发送的密码。导航到Wireshark > Preferences > Protocols > RADIUS，然后添加ISE和网络设备使用的RADIUS共享密钥，即可查看用户发送的数据包。之后，解密显示RADIUS数据包。



Wireshark Radius选项

8 -网络设备故障排除命令

下一命令有助于排除ISR 1100或有线NAD设备上的问题。

8 – 1使用show aaa servers查看AAA服务器或ISE是否可用以及是否可从网络设备访问。

```
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
        WNCD 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
        WNCD 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要查看端口状态、详细信息、应用于会话的ACL、身份验证方法和更有帮助的信息，请使用命令show authentication sessions interface <interface where the laptop is attached>详细信息。

```
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: 22781F0A0000000C0777AECD
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要验证全局配置中是否有aaa的所有必需命令，请运行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 COHVSRADISE01-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 COHVSRADISE01-NEW
!
!
!
!
aaa new-model
aaa session-id common
!
!

Router#
```

8-4另一个有用命令是test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy。

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

Router#
```

9 -网络设备相关的调试

- debug dot1x all - 显示所有dot1x EAP消息
- debug aaa authentication -显示来自AAA应用程序的身份验证调试信息
- debug aaa authorization -显示AAA授权的调试信息
- debug radius authentication -提供仅用于身份验证的协议级别活动的详细信息
- debug radius -提供协议级别活动的详细信息

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。