使用Web用户界面配置Catalyst 1300中的授权更改

目标

本文的目的是向您展示如何使用Web用户界面(UI)在Catalyst 1300交换机中配置授权更改(CoA)。

适用的设备和软件版本

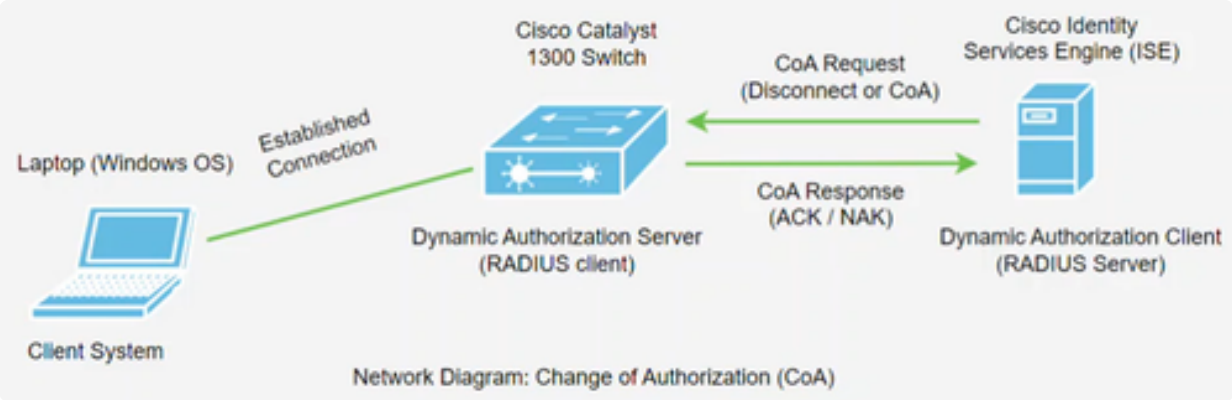
- Catalyst 1300 交换机 |4.1.6.53

简介

授权更改(CoA)是RADIUS协议的扩展，允许您在身份验证、授权和记帐(AAA)或dot1x用户会话后更改其属性。当AAA中用户或组的策略更改时，管理员可以从AAA服务器（例如思科身份服务引擎[ISE]）传输RADIUS CoA数据包，以重新初始化身份验证并应用新策略。

思科身份服务引擎（或ISE）是一个功能齐全的基于网络的访问控制和策略实施引擎。它提供安全分析和实施、RADIUS和TACACS服务、策略分发等。Cisco ISE目前是Catalyst 1300交换机唯一支持的CoA动态授权客户端。有关详细信息，请参阅ISE管理员指南。

此功能需要在动态授权客户端（RADIUS服务器）和动态授权服务器（Catalyst交换机）之间进行通信。 如下面的网络图所示，动态授权服务器向动态授权服务器发送断开连接或CoA消息，交换机提供响应。



Network Diagram: Change of Authorization (CoA)

CoA支持已添加到固件版本4.1.3.36中的Catalyst 1300交换机。这包括支持断开用户连接以及更改适用于用户会话的授权。设备支持以下CoA操作：

- 断开会话
- 禁用主机端口CoA命令
- 退回主机端口CoA命令
- 重新验证主机CoA命令

要使用命令行界面(CLI)配置CoA，请参阅使用CLI在Catalyst 1300交换机中配置授权更改。

目录

在ISE上配置Catalyst 1300 RADIUS客户端

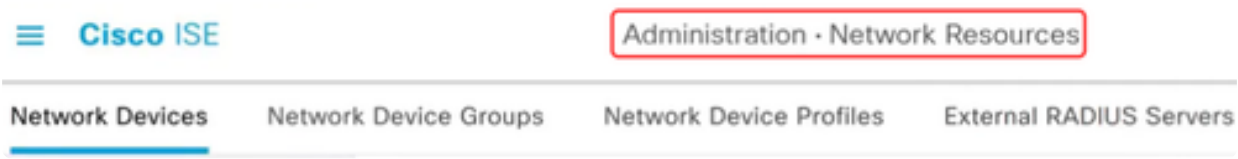
在本示例中，使用Cisco ISE服务器版本3.2。有关ISE的概述，请查看Cisco Identity Services Engine产品页面。

> Note:
> ISE版本2.7及更高版本支持CoA。

部署思科ISE服务器后，登录以访问Web UI。

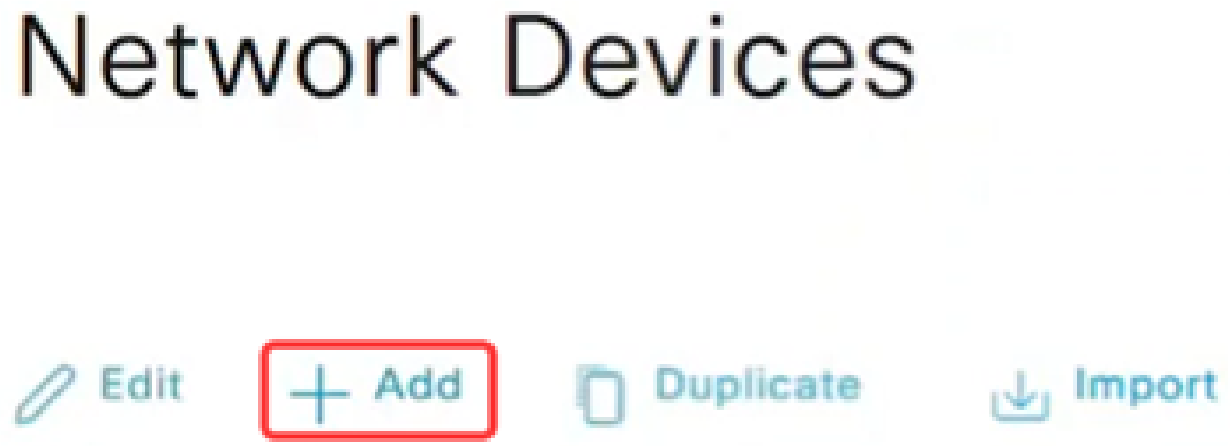
第 1 步

要添加网络设备，请导航到管理>网络资源菜单。



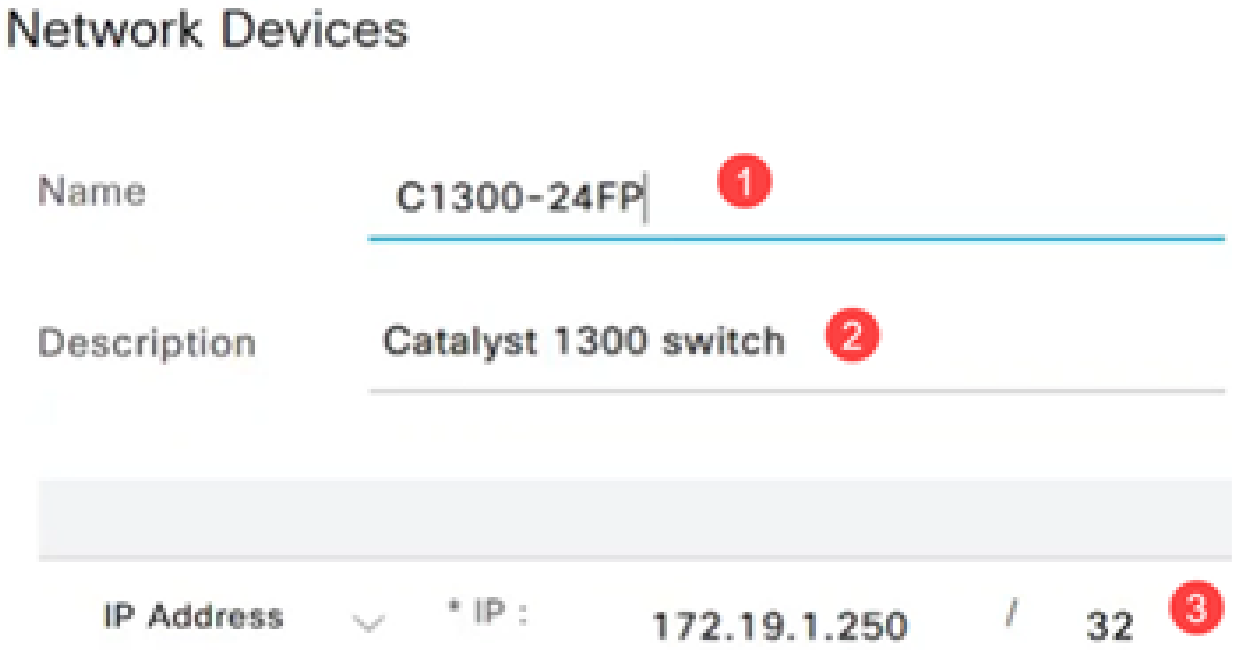
第 2 步

点击+添加按钮。



第 3 步

输入Catalyst交换机的名称、描述和IP地址。

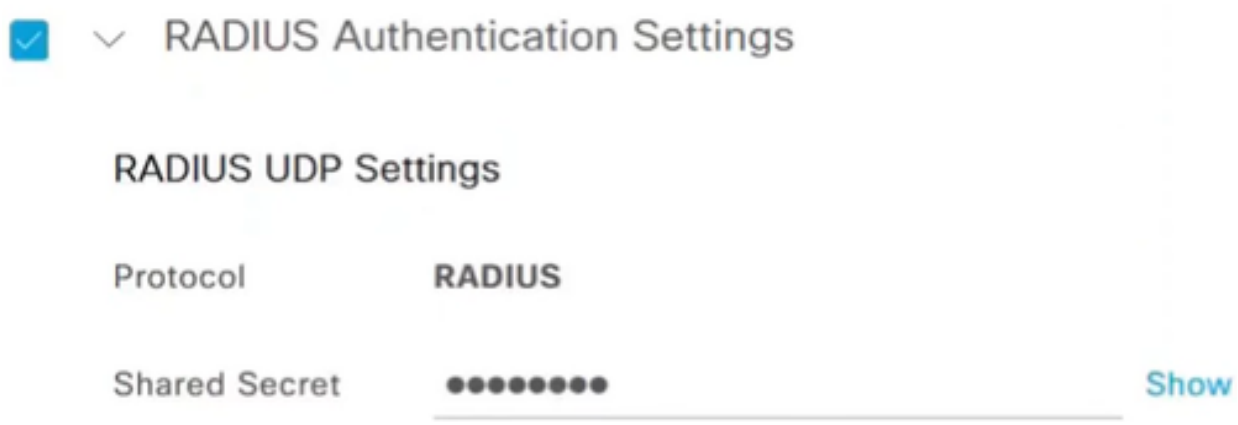


第 4 步

从Device Profile下拉菜单中，选择Cisco。

步骤 5

通过输入Shared Secret配置RADIUS身份验证设置。

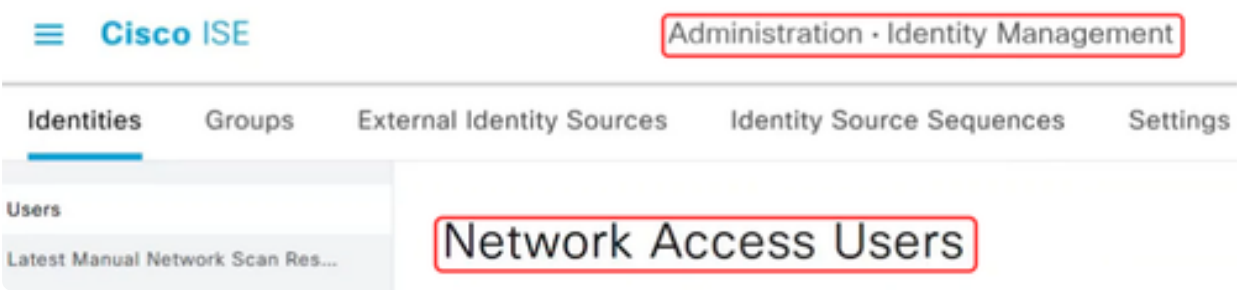


第 6 步

输入CoA端口号。默认端口为 1700。

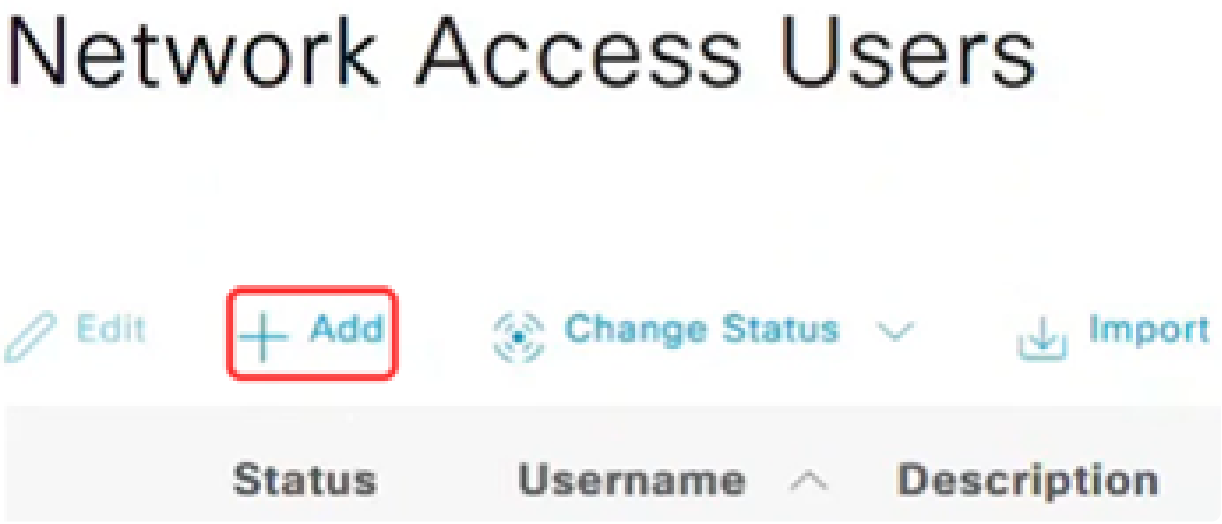
第 7 步

接下来，导航到Administration > Identity Management，然后选择Network Access Users。



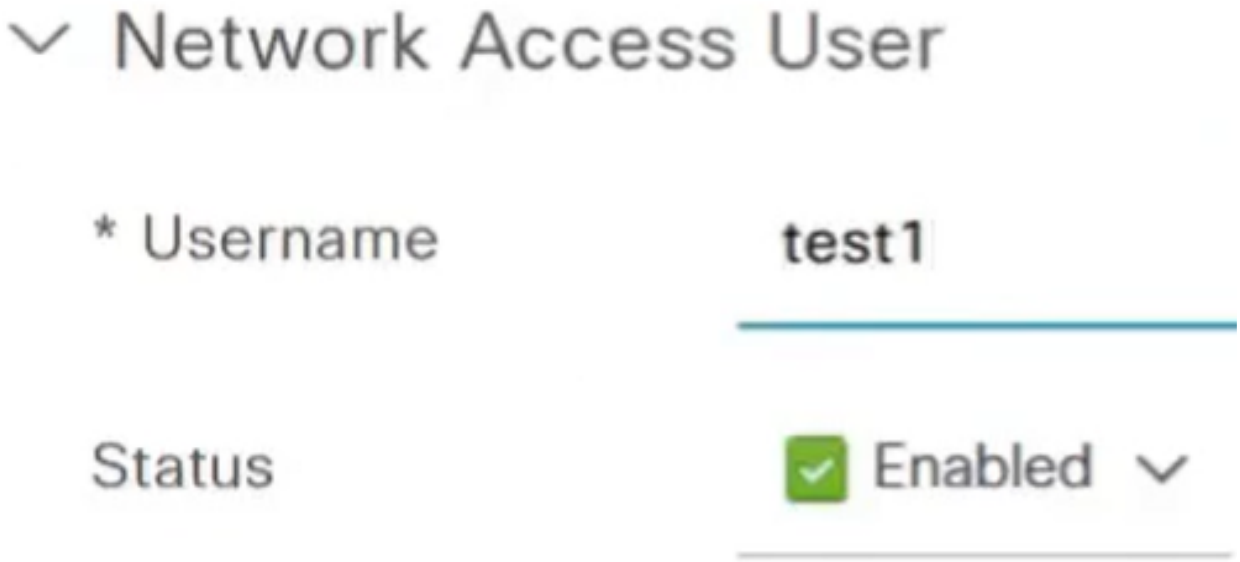
步骤 8

要定义用户名和密码，请点击+Add符号。



步骤 9

输入用户名、密码并点击页面底部的Save。



Catalyst 1300交换机中的配置

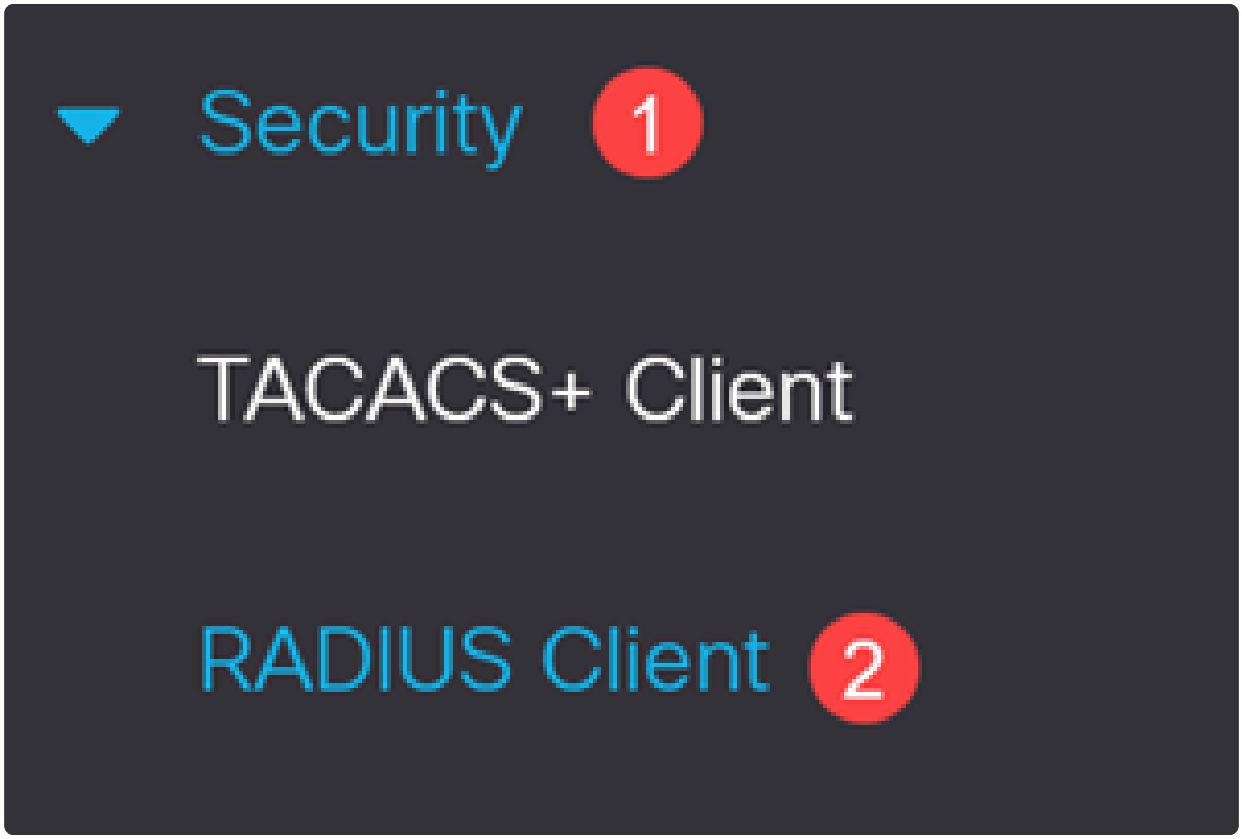
第 1 步

登录您的Catalyst 1300交换机并选择Advanced模式。本例中使用C1300-24FP-4X。

> Note:
> CoA支持已添加到固件版本4.1.3.36中的Catalyst 1300交换机。

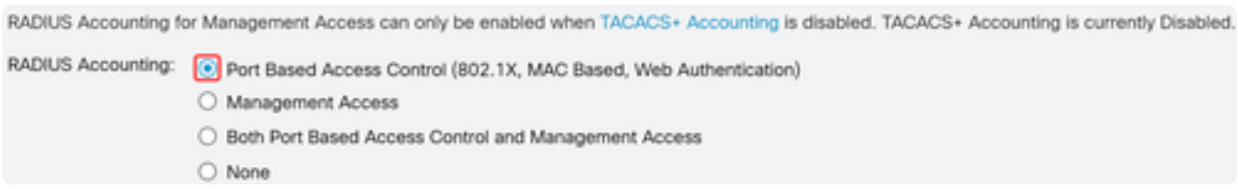
第 2 步

导航到导航窗格中的Security > RADIUS Client。



第 3 步

将RADIUS Accounting设置为基于端口的访问控制。



第 4 步

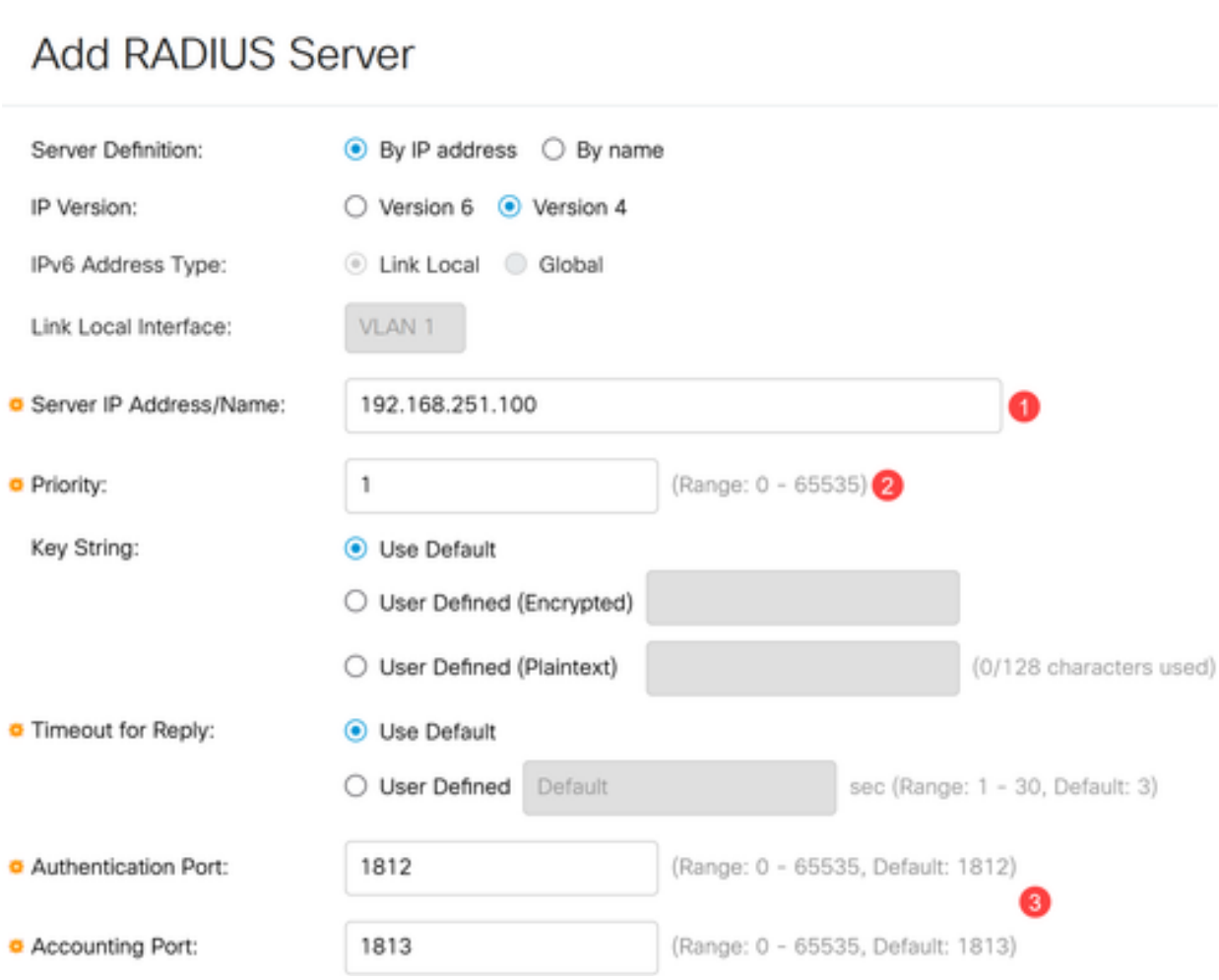
要添加ISE服务器，请向下滚动到RADIUS表，然后点击加号图标。

步骤 5

配置RADIUS服务器设置。

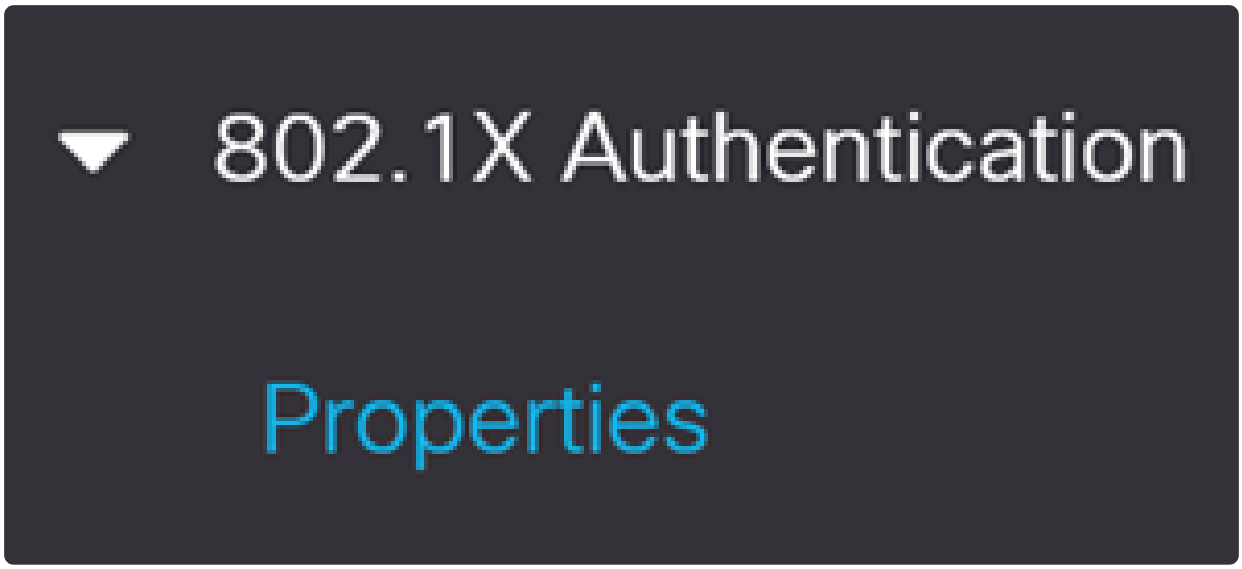
- 选择服务器定义。在本示例中，By IP address处于选中状态。在服务器IP地址/名称字段中输入IP地址。
- 设置RADIUS优先级。
- 身份验证和记帐端口设置为默认值。
- 使用类型为802.1x。

单击 Apply。



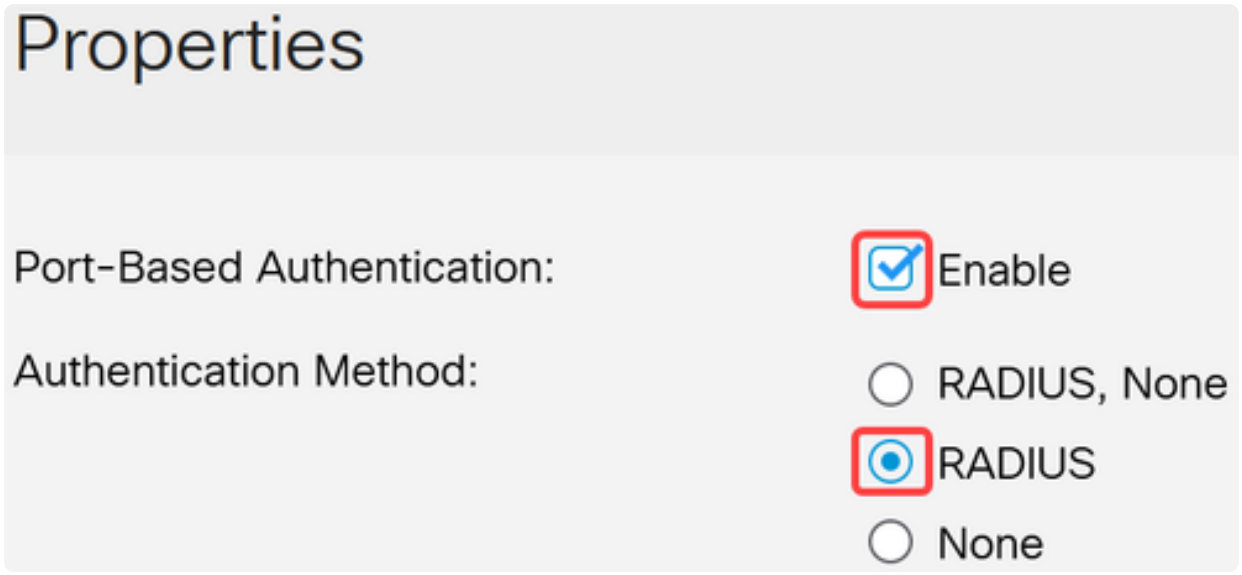
第 6 步

要配置802.1x身份验证，请导航至安全> 802.1X身份验证>属性菜单。



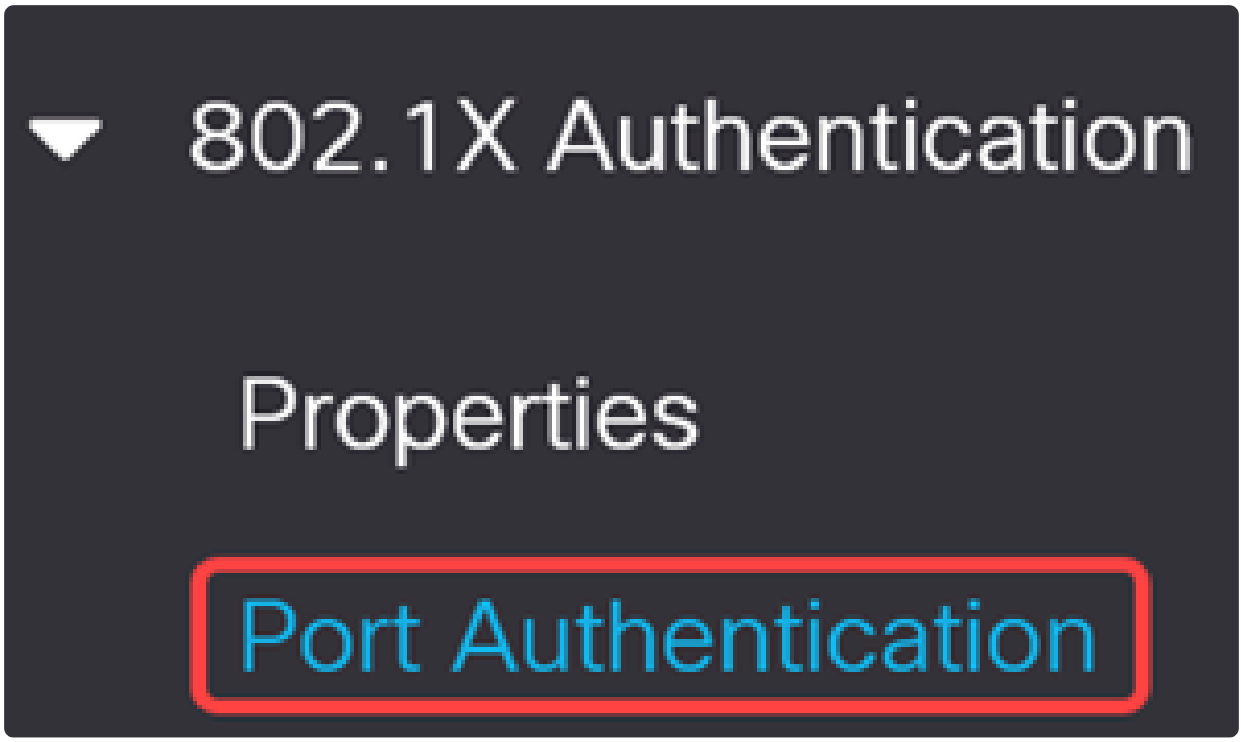
第 7 步

确保Port-Based Authentication已启用，且Authentication Method设置为RADIUS。



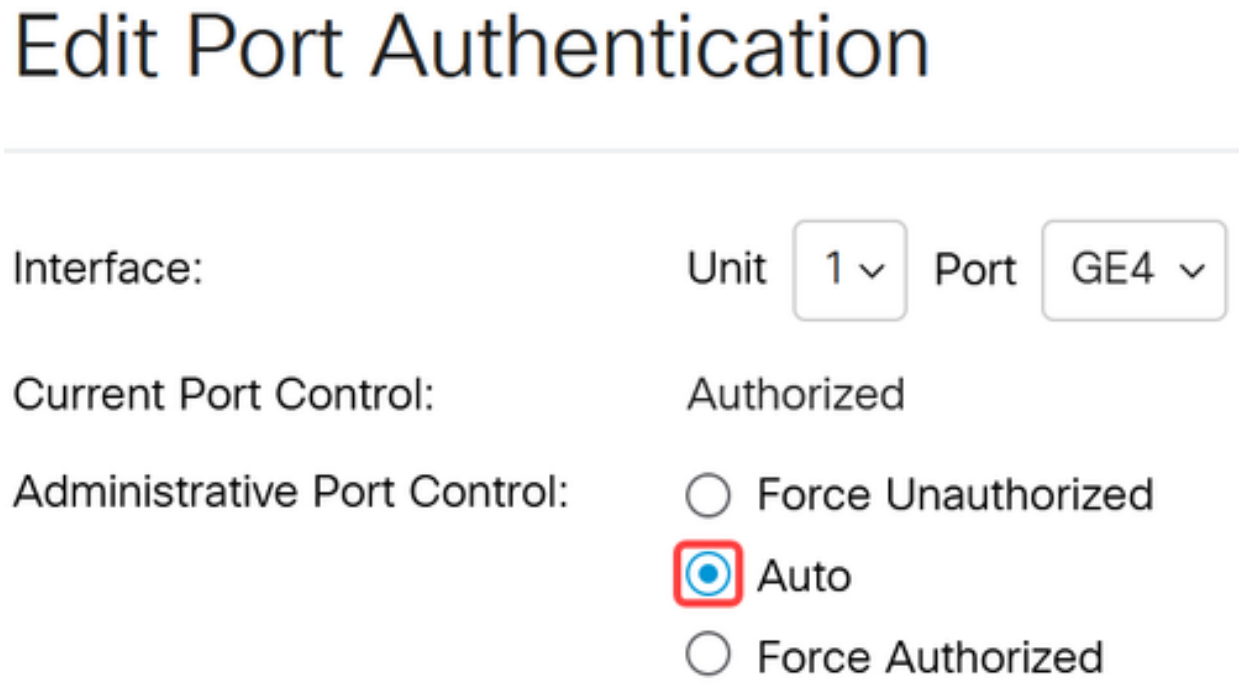
步骤 8

导航到Port Authentication菜单，选择所需的端口，然后单击edit。



步骤 9

对于Administrative Port Control，选择Auto选项，该选项将根据RADIUS响应在授权和未经授权状态之间切换端口。

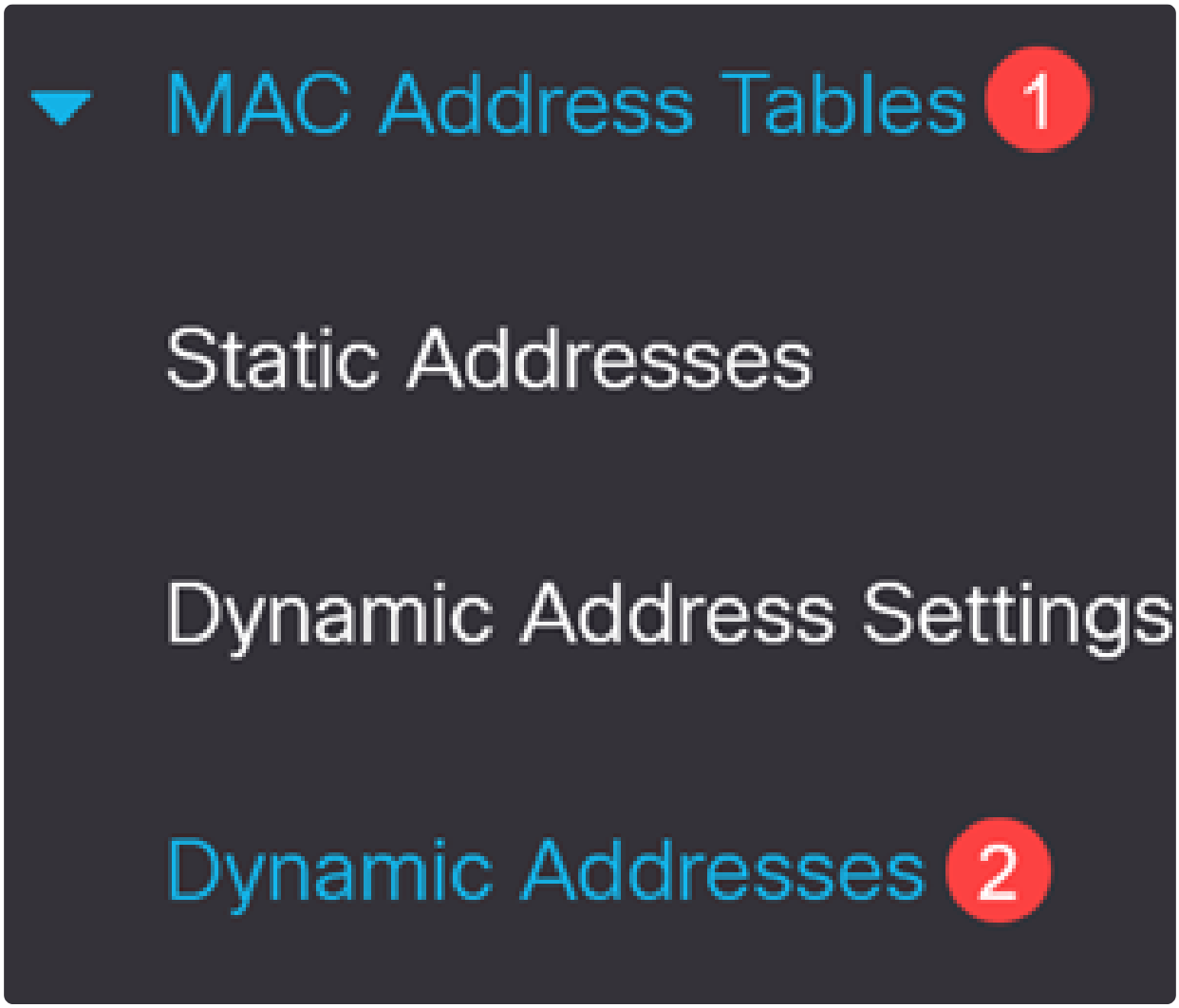


步骤 10

启用基于802.1x的身份验证，然后单击Apply。

步骤 11

您将需要端口上设备的MAC地址。ISE上的CoA操作将应用到该MAC地址。在本例中，它是端口9。要获取该端口，请导航到MAC地址表>动态地址。

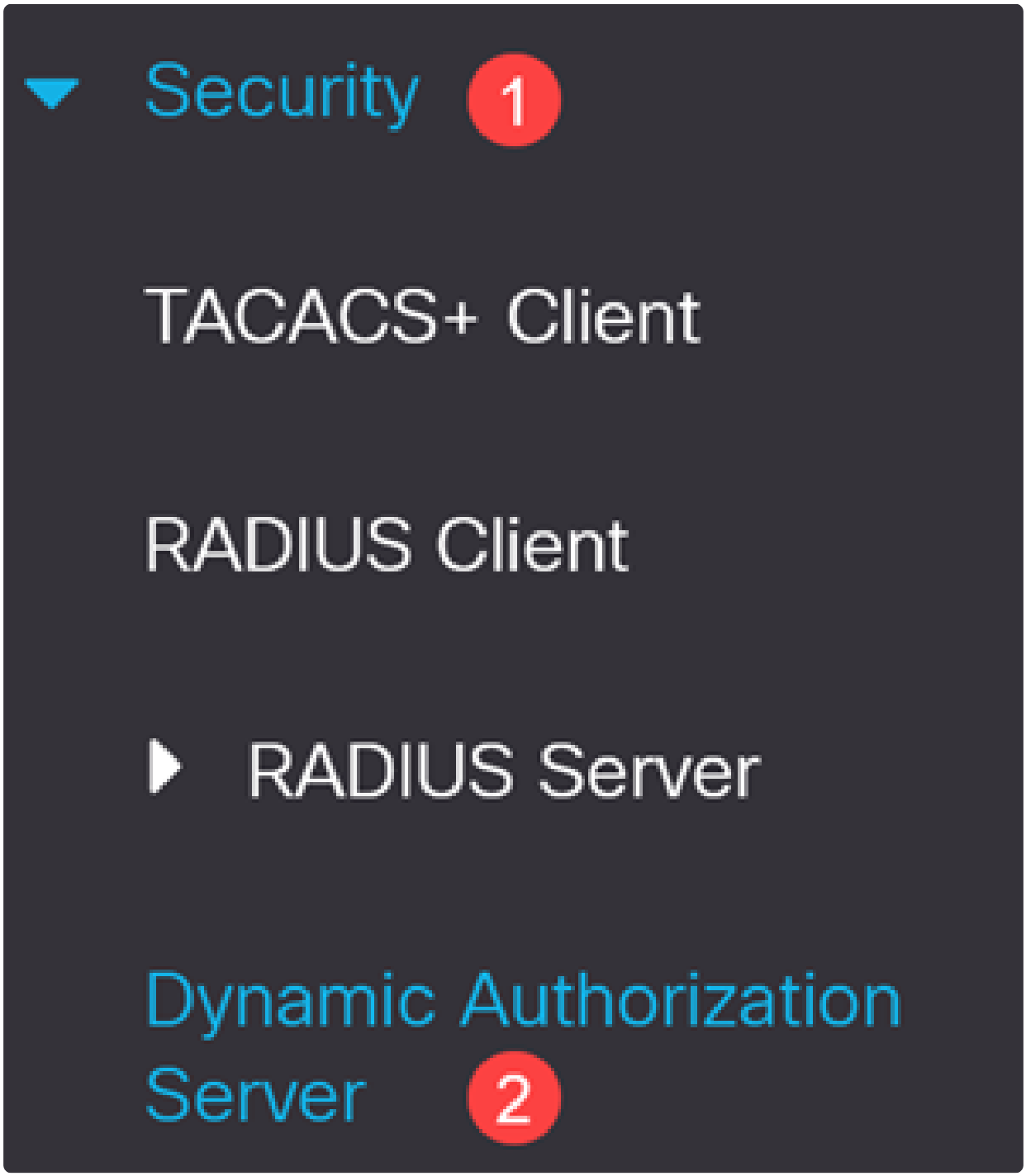


步骤 12

向下滚动到端口并记录MAC地址。

步骤 13

导航到安全>动态授权服务器。

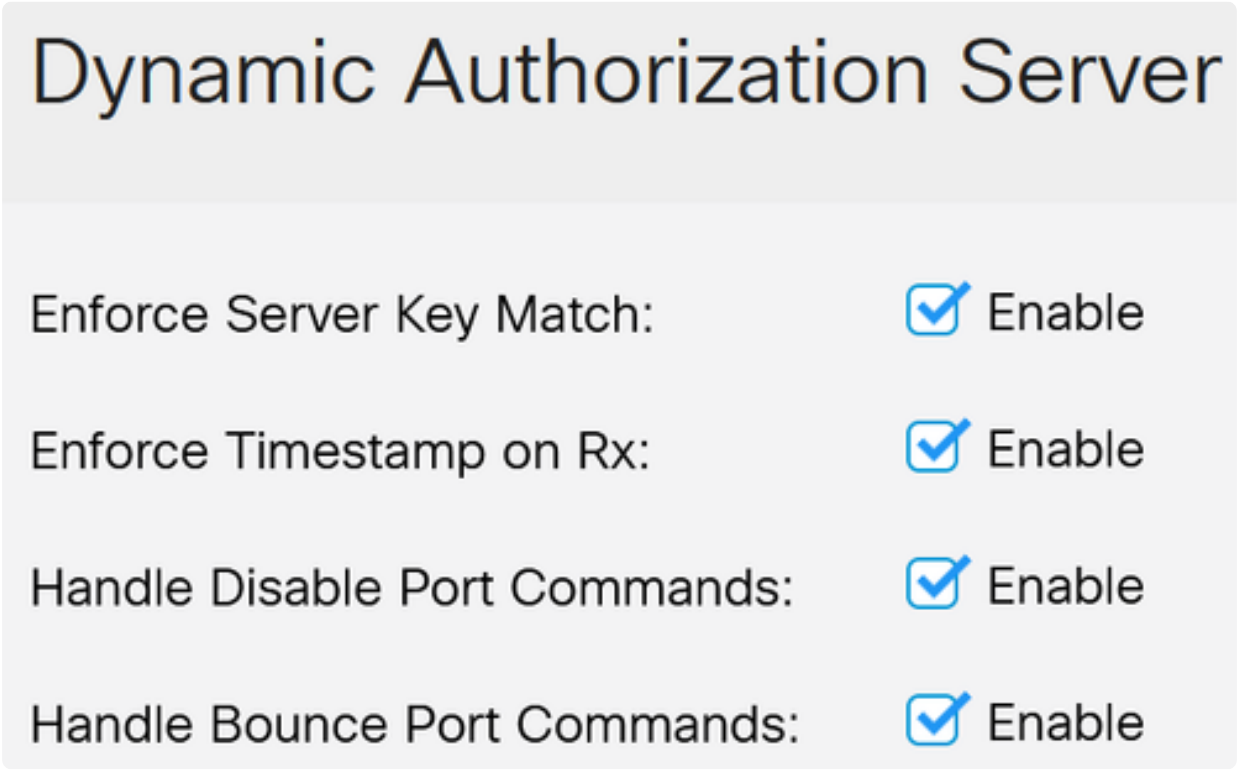


步骤 14

启用以下功能：

- 强制服务器密钥匹配

- 在Rx上实施时间戳
- 处理Disable端口命令
- 处理退回端口命令

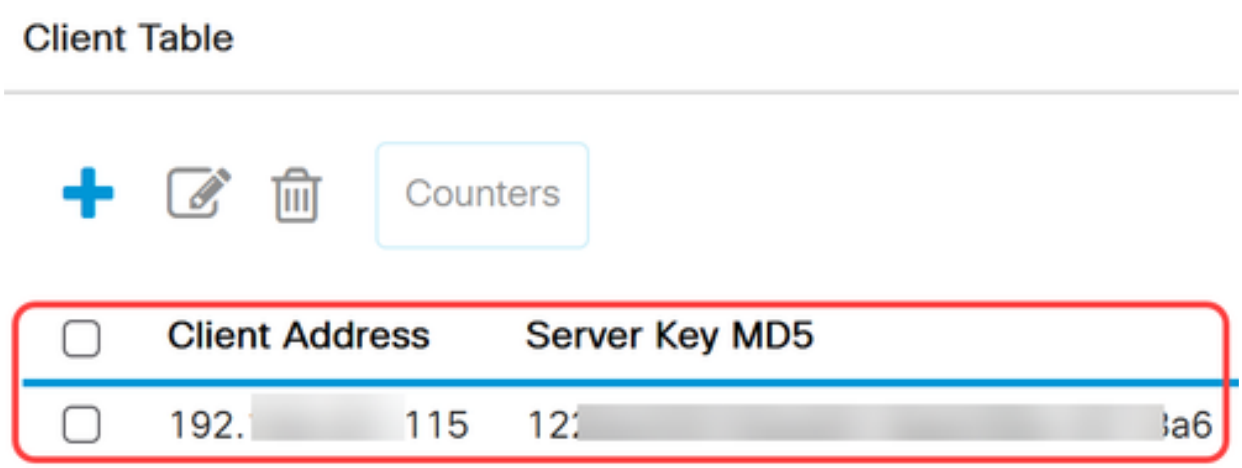


步骤 15

将UDP Port保留为默认值1700。

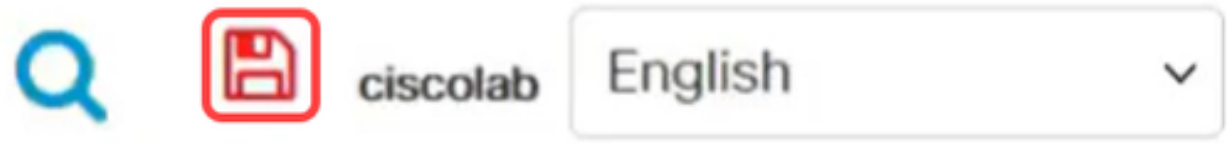
步骤 16

在客户端表下，确保使用正确的服务器密钥添加ISE服务器。单击 Apply。



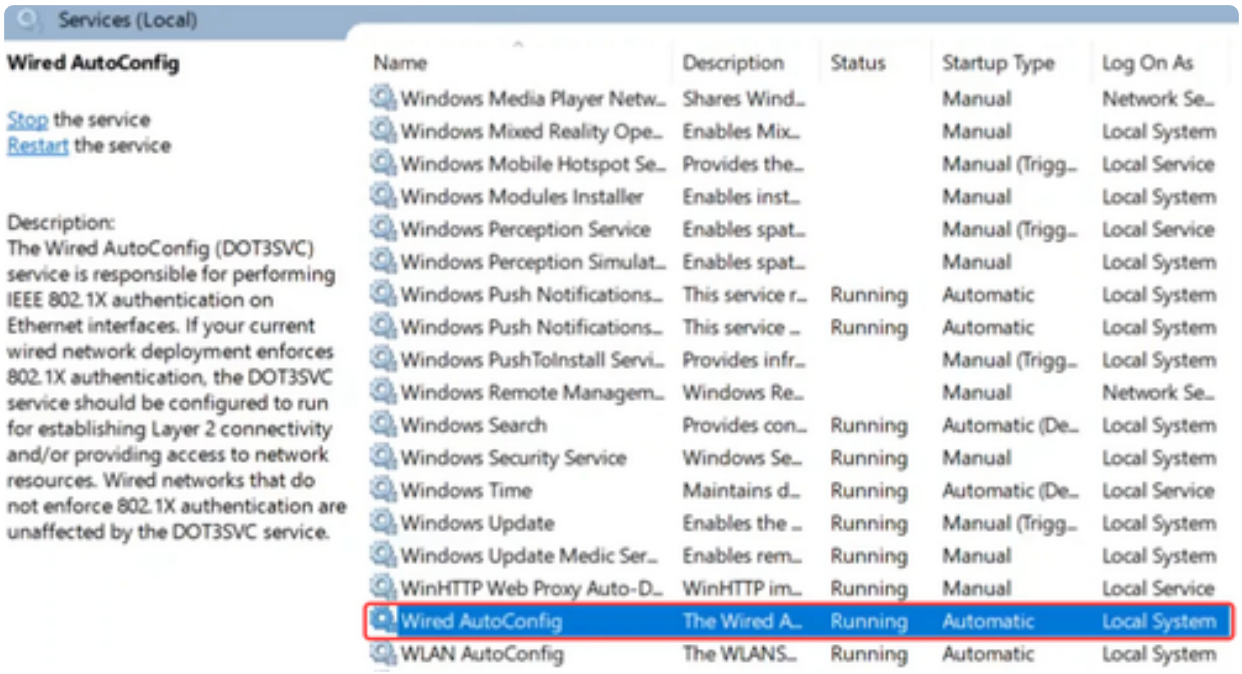
步骤 17

单击红色闪烁的Save图标以保存配置。



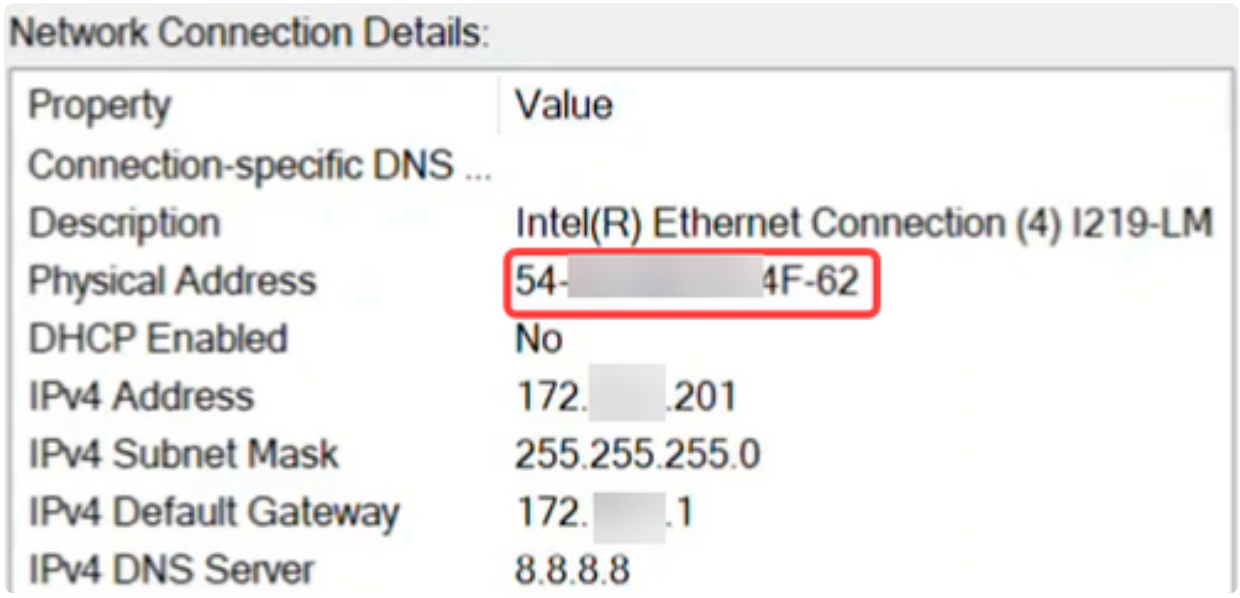
步骤 18

在连接到端口9的客户端笔记本电脑上，验证是否已为802.1 X身份验证启用有线自动配置服务。



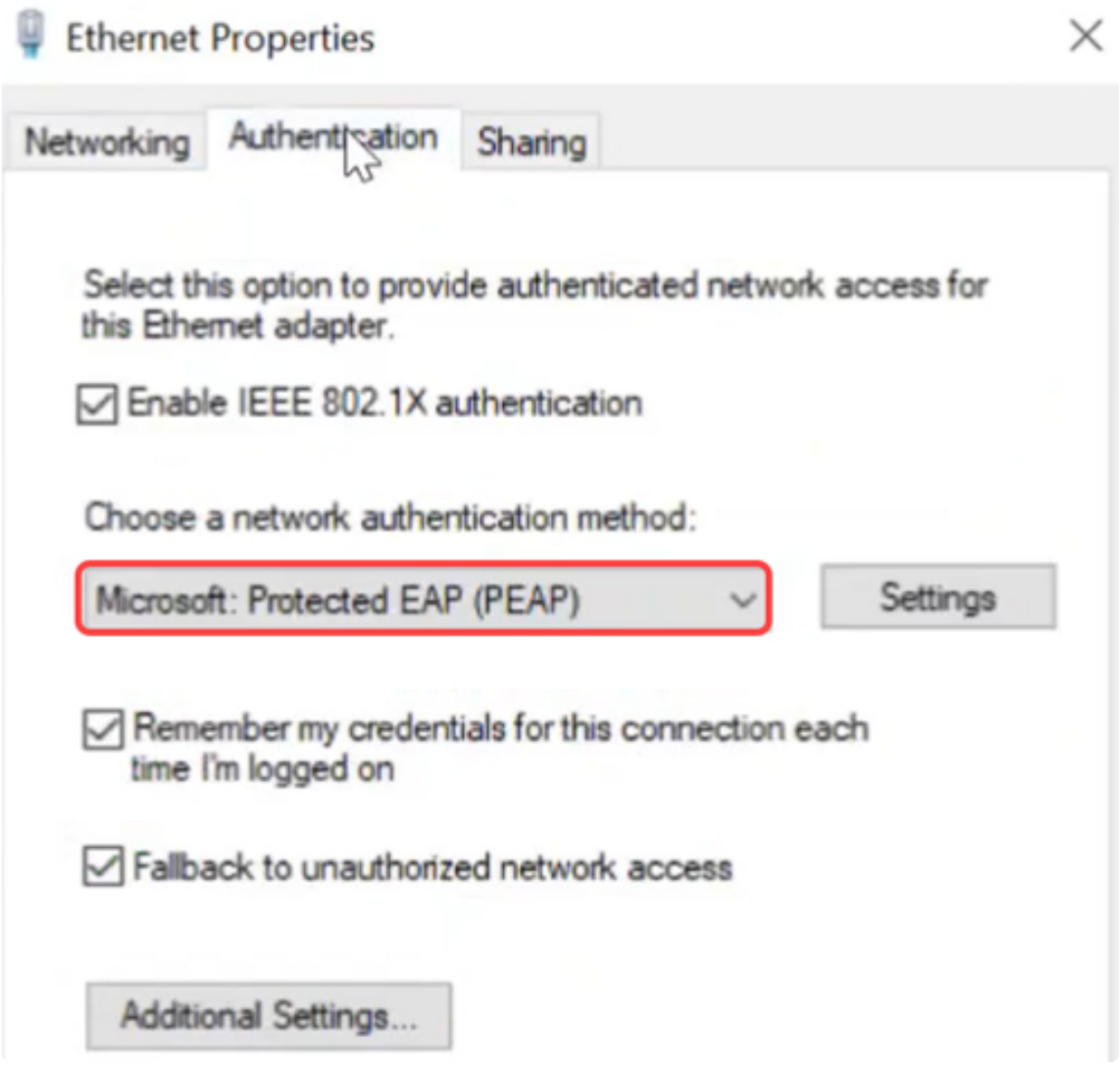
步骤 19

在以太网适配器设置上，验证MAC地址是否匹配。



步骤 20

单击Ethernet settings下的Properties按钮，然后在Authentication选项卡下确保启用复选框。此外，请确保身份验证方法是受保护的EAP(PEAP)。



步骤 21

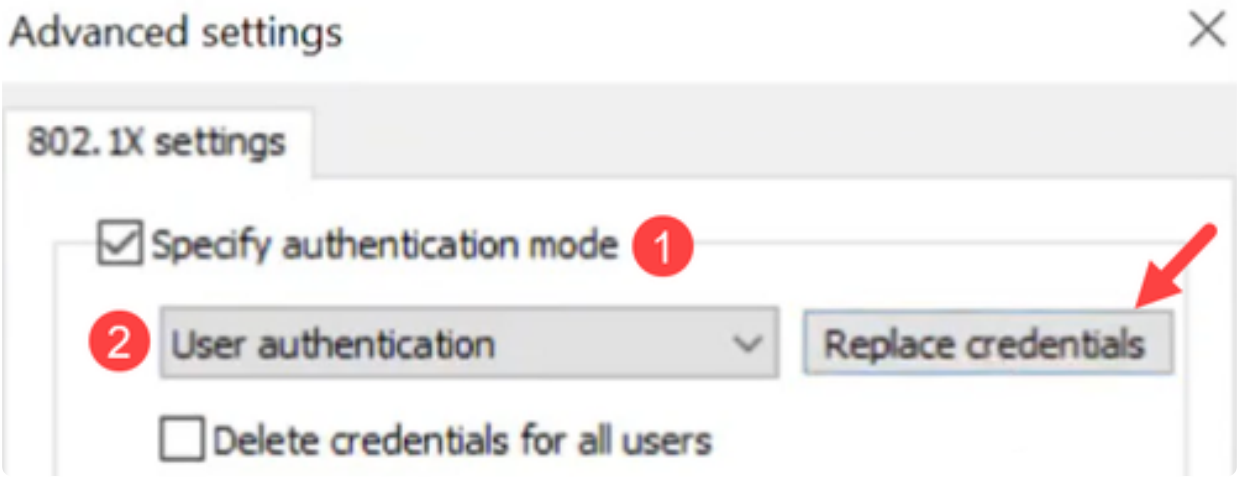
单击Settings按钮，确保取消选中Verify the server’s identity by validating the certificate旁边的复选框。

步骤 22

应选中Enable Fast Reconnect（启用快速重新连接）框。

步骤 23

在Additional settings下，确保已启用Specify authentication mode，并从下拉菜单中选择User authentication。您可以保存在ISE上创建的凭证，也可以使用替换凭证按钮替换它。



CoA操作

在启动CoA操作之前，请在交换机上启用数据包捕获。

第 1 步

在PuTTY上，使用命令monitor capture cap1 buffer size 20 circular登录到Catalyst交换

机，并指定缓冲区大小和捕获模式。

第 2 步

使用命令monitor capture cap1 control-plane both将控制平面指定为两者。

第 3 步

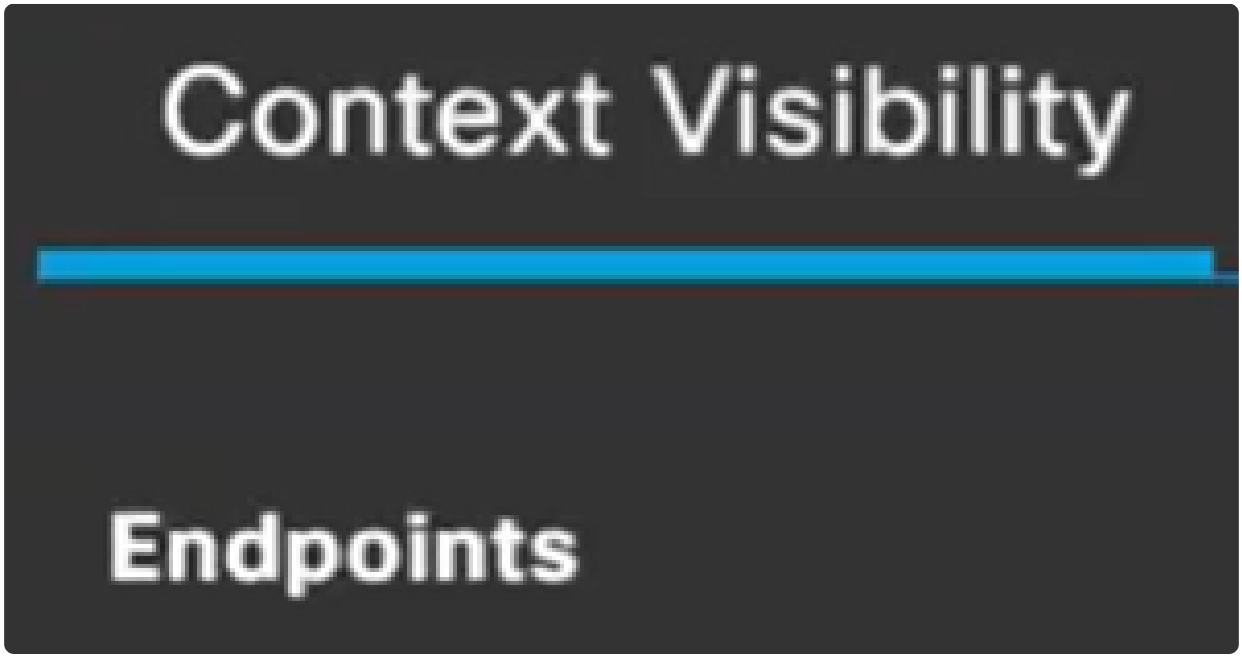
输入任意匹配条件。此命令为monitor capture cap1 match any。

第 4 步

开始数据包捕获。

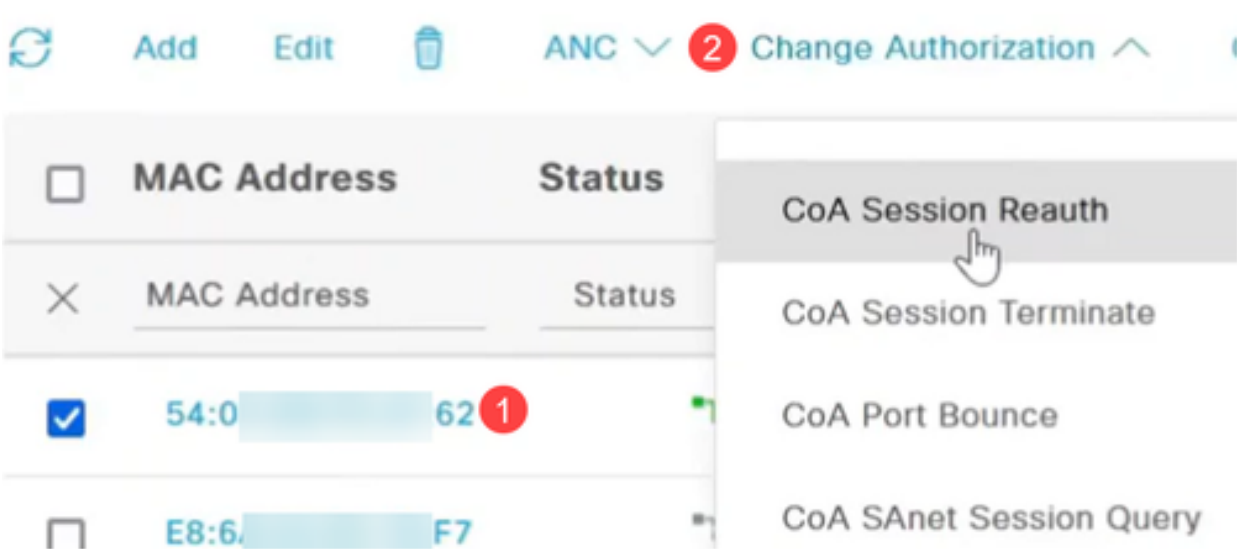
步骤 5

在ISE界面上，导航到情景可视性下的终端选项。



第 6 步

选择MAC地址，然后从Change of Authorization下拉菜单中选择CoA操作。在本示例中，CoA Session Reauth已选中。这通过使用reauthenticate命令发送CoA数据包来强制在端口上重新进行身份验证。



第 7 步

返回PuTTY终端检查CoA操作是否成功。

```
Started capture point : capl
Cat1300-1#04-Jul-2024 20:49:45 %SEC-W-COAREAUTHSESSN: 802.1x re-authentication initiated for host 5
4:  62 by CoA Request "reauthenticate"
```

步骤 8

如果选择CoA Session Terminate，它将根据管理请求发送带有终止命令的断开连接请求。

```
Cat1300-1#04-Jul-2024 20:50:02 %SEC-W-PORTUNAUTHORIZED: Port gil/0/9 is unAuthorized
04-Jul-2024 20:50:02 %SEC-W-COADISCSESSN: 802.1x session for host 54:  :62 on interface gi
1/0/9 has been terminated by Disconnect-Request. Authenticator state on the Interface will be re-in
itialized
04-Jul-2024 20:50:02 %SEC-I-PORTAUTHORIZED: Port gil/0/9 is Authorized
```

步骤 9

CoA Port Bounce选项将使用bounce host port命令发送CoA请求数据包，从而禁用并重新启用交换机上的端口。网络适配器离线了10秒，变为未授权状态。它将在线恢复，获得授权并可转发数据包。

```
Cat1300-1#04-Jul-2024 20:50:21 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:50:21 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:34 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:34 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:50:36 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:39 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:39 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized

Cat1300-1#04-Jul-2024 20:50:45 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

步骤 10

使用端口退回的CoA会话终止将终止现有会话，退回端口10秒，并变为未授权状态。然后，它会重新联机，获得授权并可转发数据包。

```
Cat1300-1#04-Jul-2024 20:51:04 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:          :62
04-Jul-2024 20:51:04 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:51:22 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:51:22 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:51:22 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized
04-Jul-2024 20:51:29 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

步骤 11

端口关闭的CoA会话终止将终止会话并管理性关闭端口。

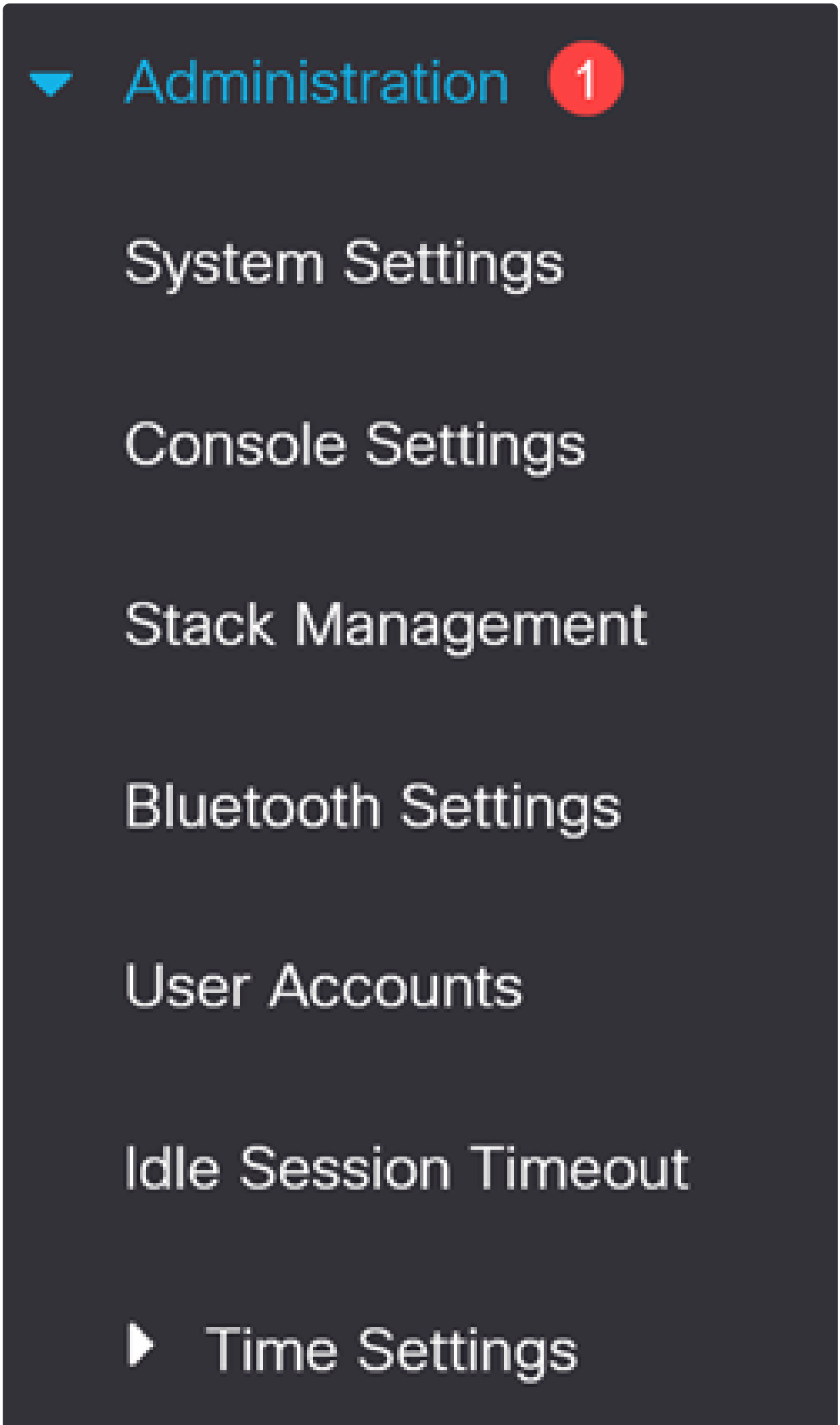
```
Cat1300-1#04-Jul-2024 20:51:47 %SEC-W-COADISPORT: Interface gi1/0/9 suspended by CoA Request "disab
le host port" for host 54:          :62
04-Jul-2024 20:51:47 %LINK-W-Down:  gi1/0/9
```

步骤 12

要停止数据包捕获，请使用命令monitor capture cap1 stop。

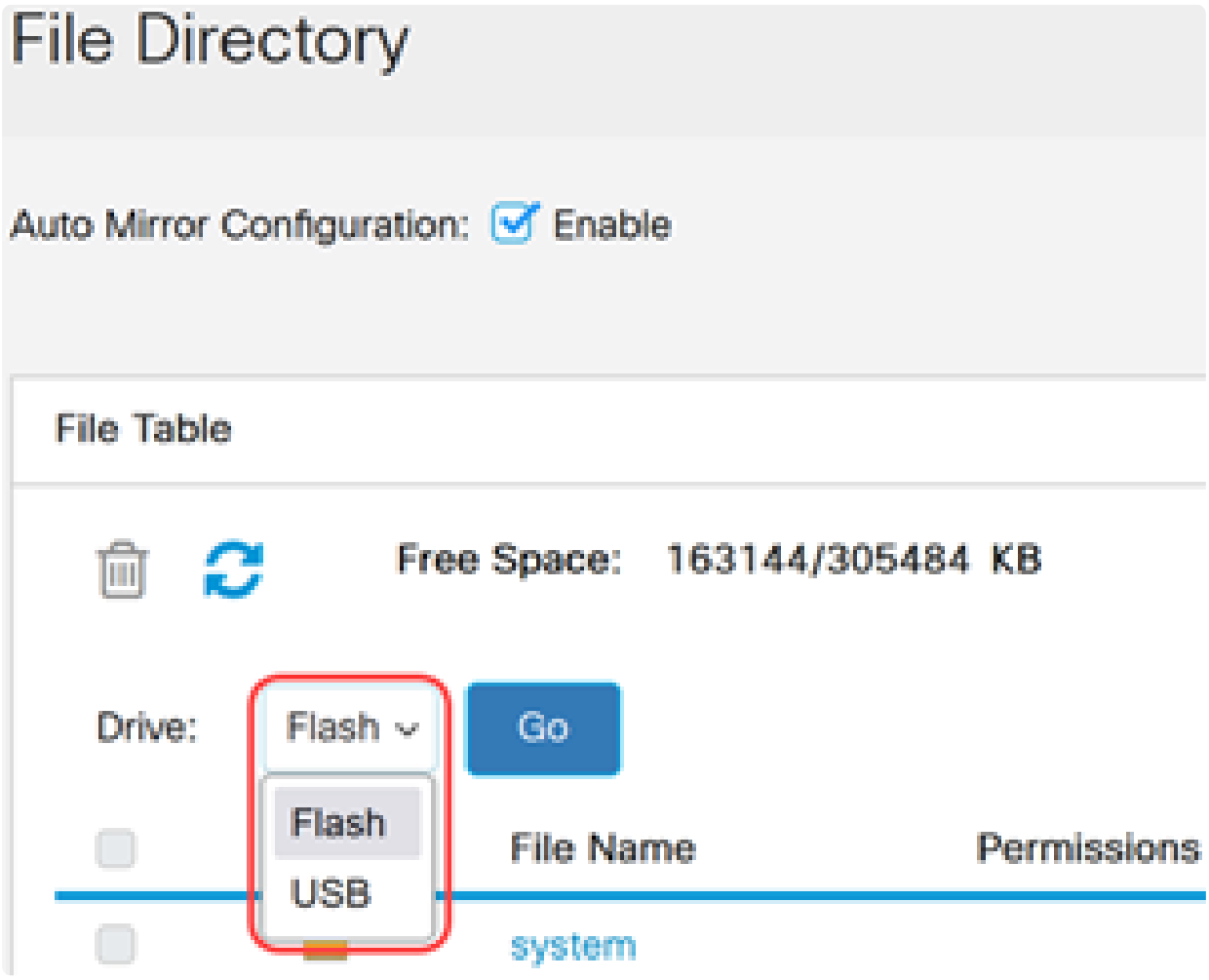
步骤 13

要复制文件，请导航到管理>文件管理>文件目录。


Administration
1
System Settings
Console Settings
Stack Management
Bluetooth Settings
User Accounts
Idle Session Timeout
Time Settings

步骤 14

默认的闪存可用。或者，可以从驱动器下拉菜单中选择USB。



结论

现在您已了解ISE以及如何在Catalyst 1300系列交换机中配置CoA。

有关详细信息，请查看以下视频。

观看与本文相关的视频...

点击此处查看思科的其他技术讲座

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）。