配置轻量级接入点作为802.1x请求方

简介

本文档介绍如何将轻量接入点(LAP)配置为802.1x请求方，以便根据身份服务引擎(ISE)服务器进行身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 无线局域网控制器(WLC)和LAP
- 思科交换机上的802.1x
- ISE
- 可扩展身份验证协议(EAP) — 通过安全隧道的灵活身份验证(FAST)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- WS-C3560CX-8PC-S，15.2(4)E1
- AIR-CT-2504-K9,8.2.141.0
- ISE 2.0

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

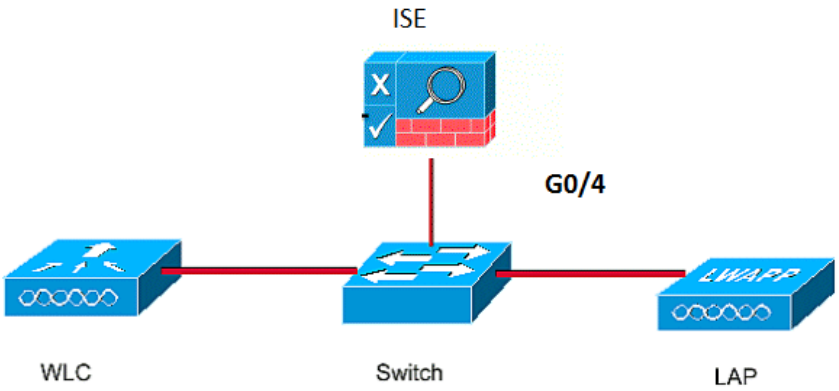
在此设置中，接入点(AP)充当802.1x请求方，并由交换机根据使用匿名保护访问凭证(PAC)调配的EAP-FAST的ISE进行身份验证。一旦端口配置为802.1x身份验证，交换机将不允许除802.1x流量外的任何流量通过该端口，直到连接到该端口的设备成功进行身份验证。AP可以在加入WLC之前或加入WLC之后进行身份验证，在这种情况下，您可以在LAP加入WLC之后在交换机上配置802.1x。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：



配置

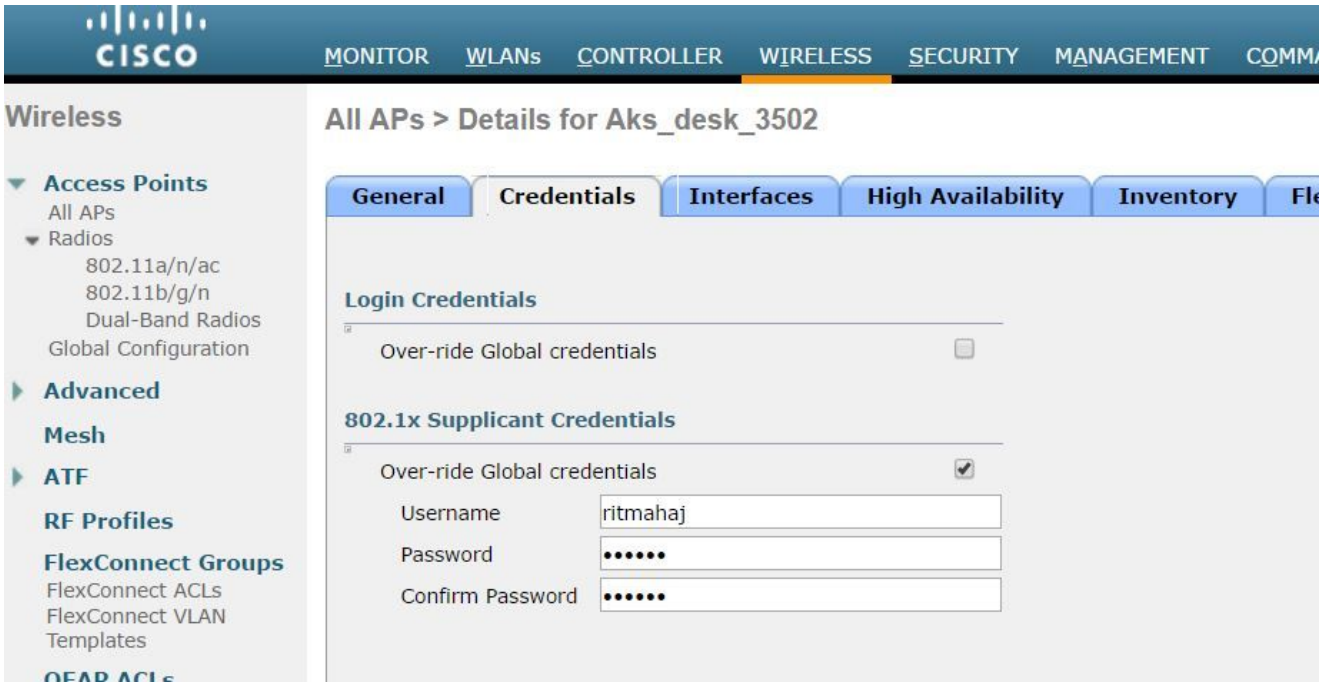
本文档使用以下IP地址：

- 交换机的IP地址为10.48.39.141
- ISE服务器的IP地址为10.48.39.161
- WLC的IP地址是10.48.39.142

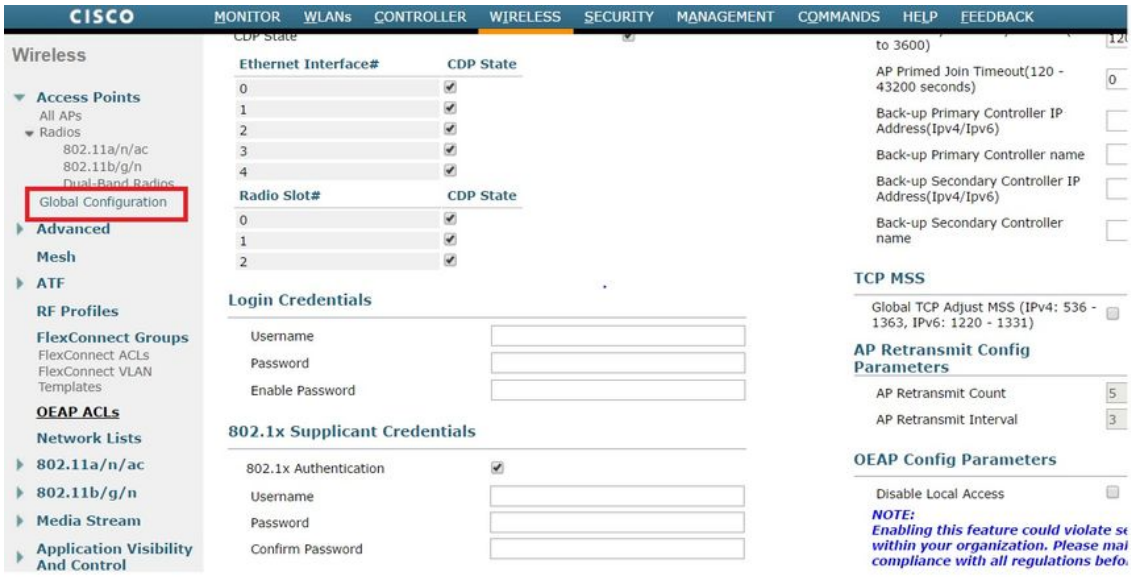
配置LAP

在本节中，您将了解将LAP配置为802.1x请求方的信息。

1. 如果AP已加入WLC，请转到Wireless（无线）选项卡，然后点击AP，转到Credentials（凭证）字段，并在802.1x Supplicant Credentials（802.1x请求方凭证）标题下，选中Over-ride Global credentials复选框，以设置此AP的802.1x用户名和密码。



您还可以通过Global Configuration菜单为加入到WLC的所有AP设置公用用户名和密码。



2. 如果AP尚未加入WLC，则必须通过控制台连接到LAP，以便设置凭证并使用以下CLI命令：<#root>

LAP#

debug capwap console cli

LAP#

capwap ap dot1x username

```
          password
```

配置交换机

1. 在交换机上全局启用dot1x并将ISE服务器添加到交换机。
   <#root>

```
aaa new-model

!

aaa authentication dot1x default group radius

!

dot1x system-auth-control

!

radius server ISE

address ipv4 10.48.39.161 auth-port 1645 acct-port 1646

  key 7 123A0C0411045D5679
```

2. 现在，配置AP交换机端口。
   <#root>

```
interface GigabitEthernet0/4
```

```
switchport access vlan 231

switchport mode access

authentication order dot1x

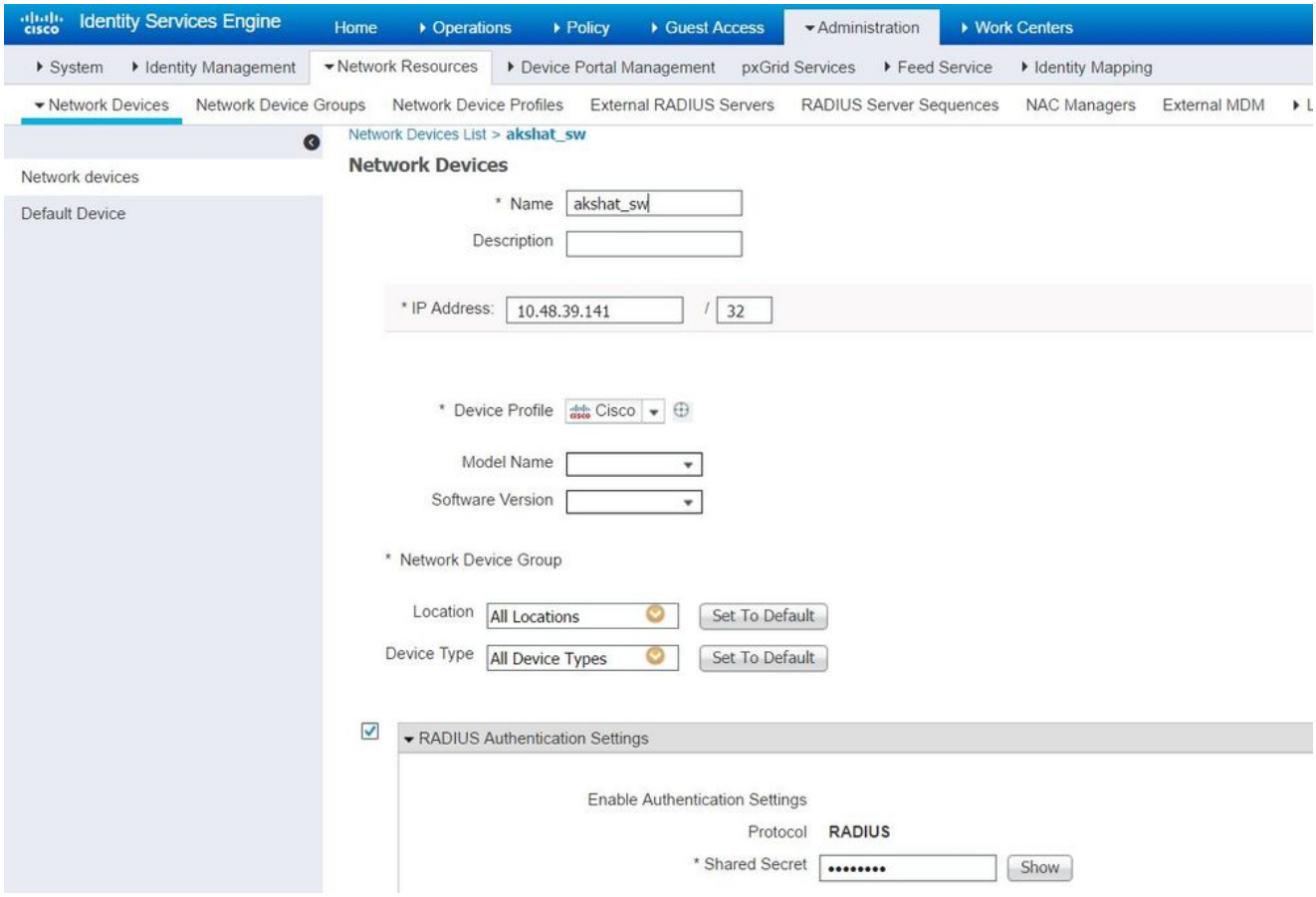
authentication port-control auto

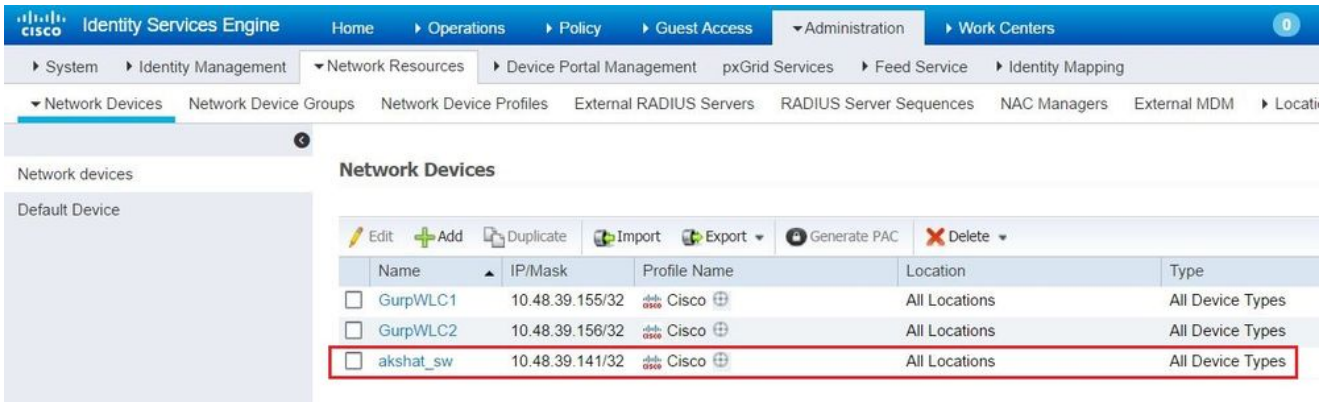
dot1x pae authenticator

spanning-tree portfast edge
```

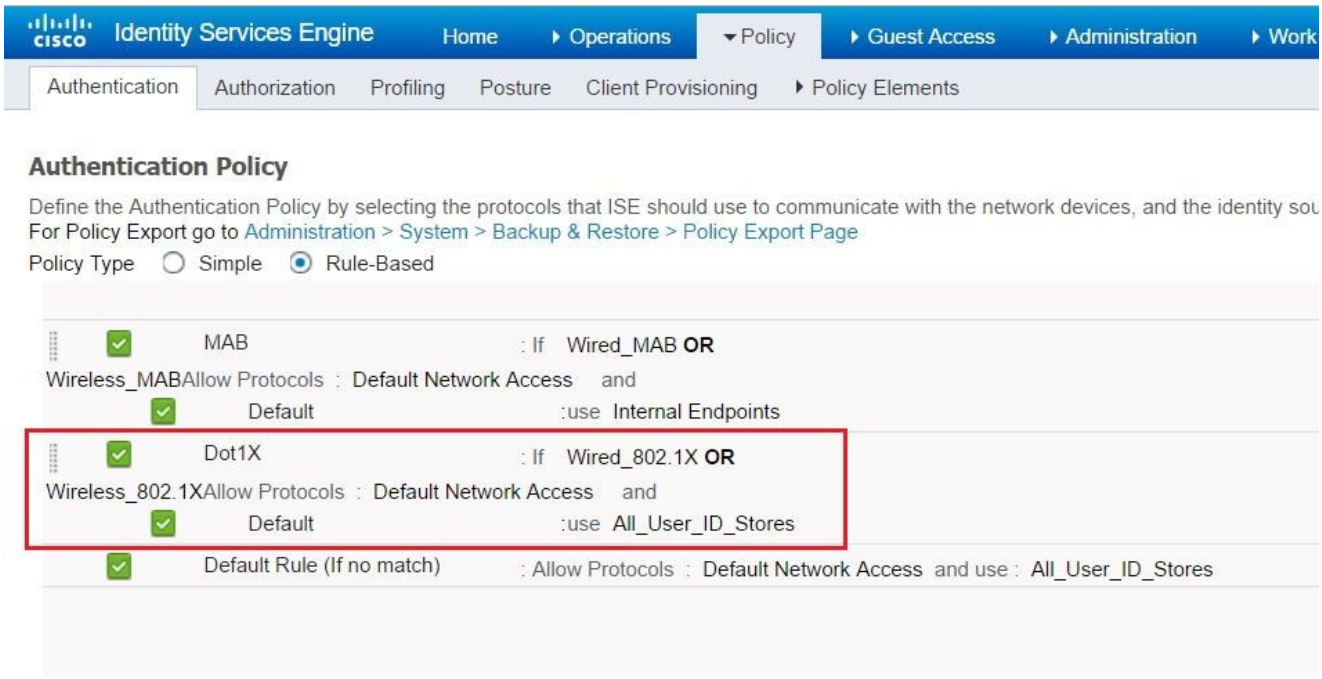
配置ISE服务器

1. 将交换机添加为ISE服务器上的身份验证、授权和记帐(AAA)客户端。

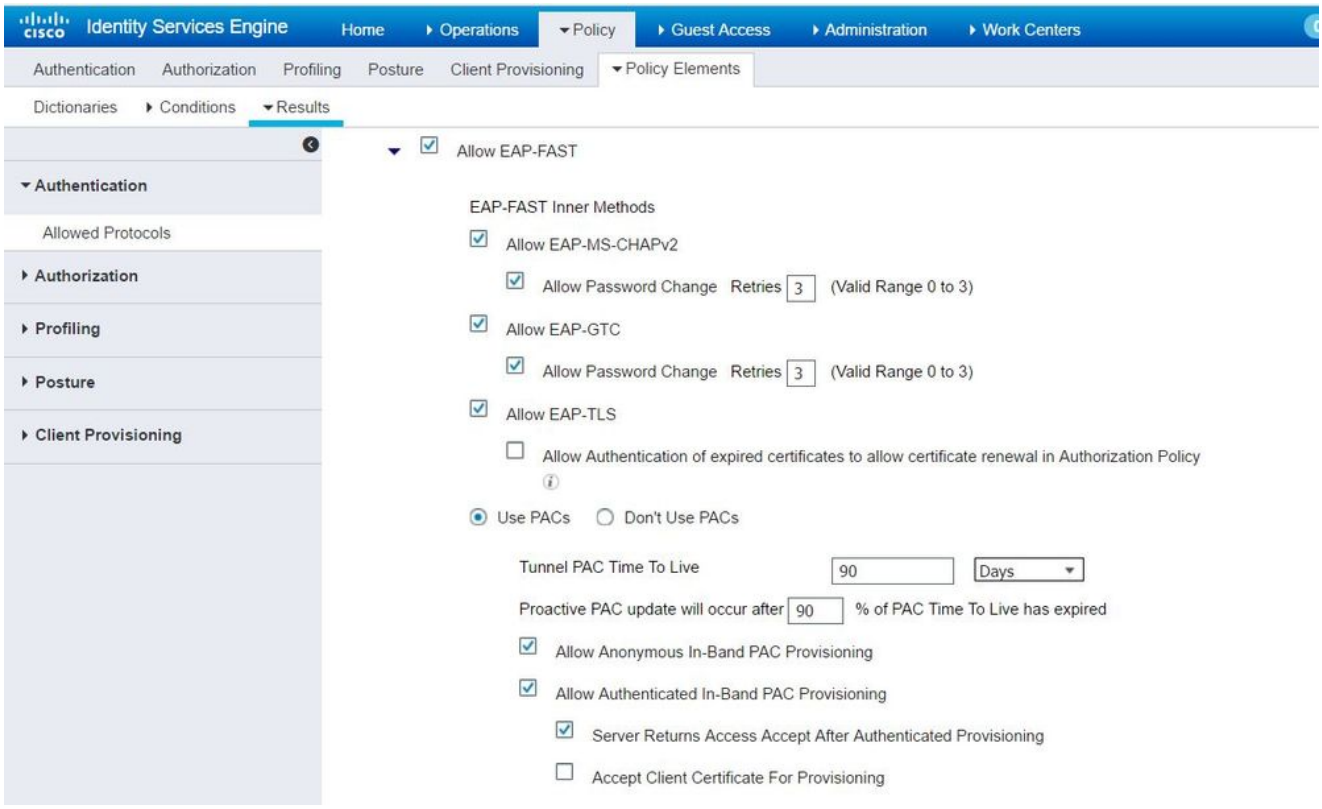




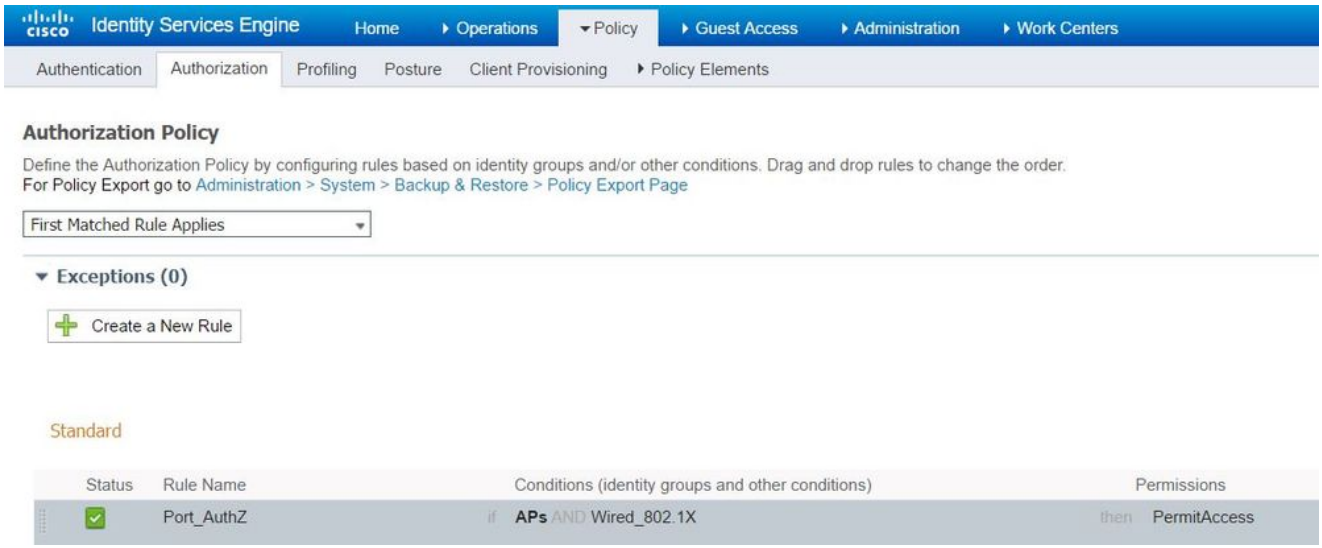
2. 在ISE上，配置身份验证策略和授权策略。在这种情况下，使用的是默认身份验证规则，即有线dot.1x，但可以根据要求自定义该规则。

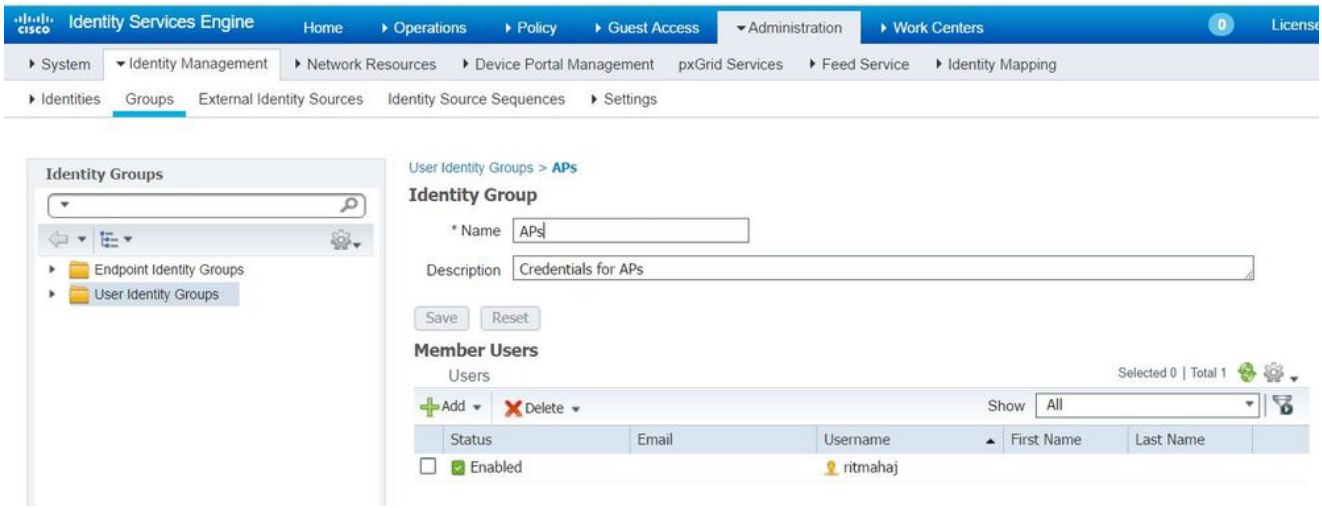


确保在允许的“默认网络访问”协议中允许EAP-FAST。



3. 对于授权策略(Port_AuthZ)，在这种情况下，AP凭证已添加到用户组(AP)。 使用的条件是“如果用户属于组AP并且执行有线dot1x，则推送默认授权配置文件允许访问”。 同样，可以根据需要进行自定义。





验证

使用本部分可确认配置能否正常运行。

一旦在交换机端口上启用了802.1x，除802.1x流量外的所有流量都会被阻塞通过该端口。如果已注册到WLC的LAP将取消关联。只有在802.1x身份验证成功后，其他流量才允许通过。在交换机上启用802.1x后，LAP成功注册到WLC表明LAP身份验证成功。您也可以使用这些方法来验证LAP是否经过身份验证。

1. 在交换机上，输入其中一个show命令以验证端口是否已进行身份验证。
   <#root>

```
akshat_sw#

show dot1x interface g0/4



Dot1x Info for GigabitEthernet0/4
-----------------------------------
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30


akshat_sw#

show dot1x interface g0/4 details



Dot1x Info for GigabitEthernet0/4
-----------------------------------
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
```

```
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30

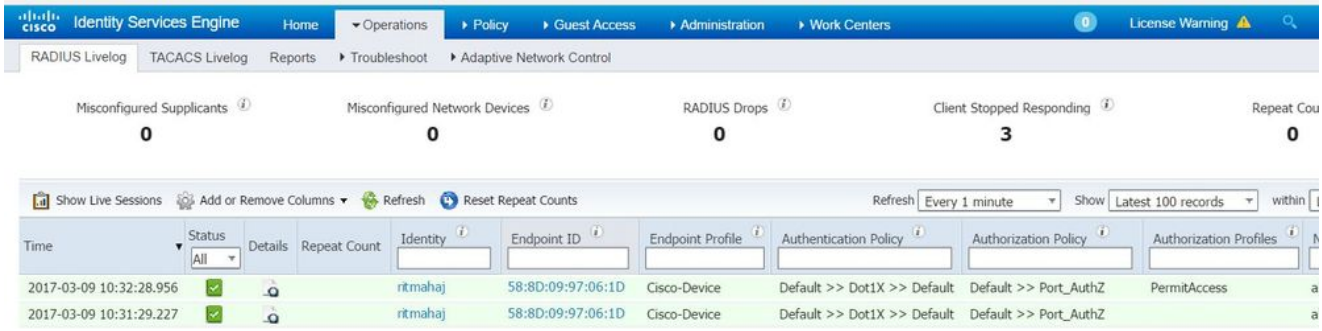

Dot1x Authenticator Client List
-------------------------------
EAP Method = FAST
Supplicant = 588d.0997.061d
Session ID = 0A30278D000000A088F1F604
 Auth SM State = AUTHENTICATED
 Auth BEND SM State = IDLE


akshat_sw#
```

```
show authentication sessions
```

```
Interface MAC Address Method Domain Status Fg Session ID
Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604
```

2. 在ISE中，选择Operations > Radius Livelogs，并查看身份验证成功且推送了正确的授权配置文件。



故障排除

本部分提供了可用于对配置进行故障排除的信息。

1. 输入ping命令以检查是否可从交换机访问ISE服务器。
2. 确保将交换机配置为ISE服务器上的AAA客户端。
3. 确保交换机和ACS服务器之间的共享密钥相同。
4. 检查ISE服务器上是否启用了EAP-FAST。
5. 检查是否为LAP配置了802.1x凭证并且在ISE服务器上配置相同。

> 注意：用户名和密码区分大小写。

6. 如果身份验证失败，请在交换机上输入以下命令：debug dot1x和debug authentication。

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）。