# 使用LAP配置ACS 5.2进行基于端口的身份验证

## 目录



## 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RADIUS服务器(例如访问控制服务器(ACS)5.2)进行身份验证。

## 先决条件

### 要求

尝试进行此配置之前，请确保满足以下要求：

- 了解无线LAN控制器(WLC)和LAP的基本知识。
- 了解 AAA 服务器的功能.
- 全面了解无线网络和无线安全问题.

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本 7.0.220.0 的 Cisco 5508 WLC
- Cisco 3502 系列 LAP
- 运行 5.2 版的 Cisco 安全 ACS
- Cisco 3560 系列交换机

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。

### 规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

## 背景信息

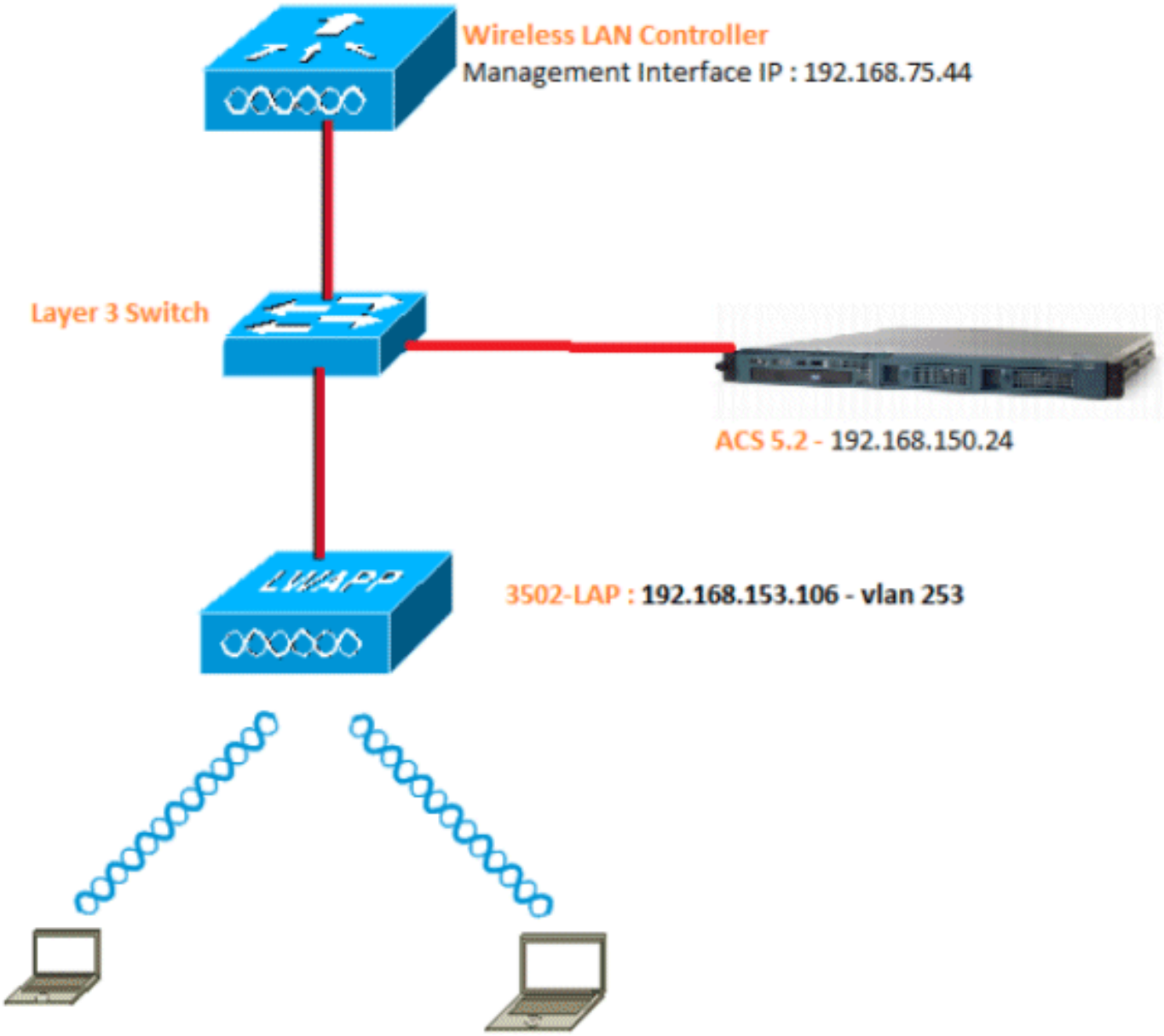
LAP在工厂安装了X.509证书（由私钥签名），这些证书在制造时烧录到设备中。LAP使用此证书以在加入过程中向WLC进行身份验证。此方法描述另一种验证LAP的方法。使用WLC软件，您可以在Cisco Aironet接入点(AP)和Cisco交换机之间配置802.1x身份验证。在此实例中，AP充当802.1x请求方，并由交换机针对使用带匿名PAC调配的EAP-FAST的RADIUS服务器(ACS)进行身份验证。一旦配置为802.1x身份验证，交换机将不允许除802.1x流量外的任何流量通过端口，直到连接到端口的设备成功进行身份验证。AP可以在加入WLC之前或加入WLC之后进行身份验证，在这种情况下，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：




下面是此图中使用的组件的配置详细信息：

- ACS (RADIUS) 服务器的 IP 地址为 192.168.150.24。
- WLC的管理和AP管理器接口地址为192.168.75.44。
- DHCP服务器地址为192.168.150.25。
- LAP位于VLAN 253中。
- VLAN 253:192.168.153.x/24。网关：192.168.153.10
- VLAN 75:192.168.75.x/24。网关：192.168.75.1

## 假设

- 所有第3层VLAN都配置了交换机。

- 为DHCP服务器分配了一个DHCP作用域。
- 网络中的所有设备之间都存在第3层连接。
- LAP已连接到WLC。
- 每个VLAN都有一个/24掩码。
- ACS 5.2已安装自签名证书。

# 配置步骤

此配置分为三类：

1. 配置LAP。
2. 配置交换机。
3. 配置 RADIUS 服务器。

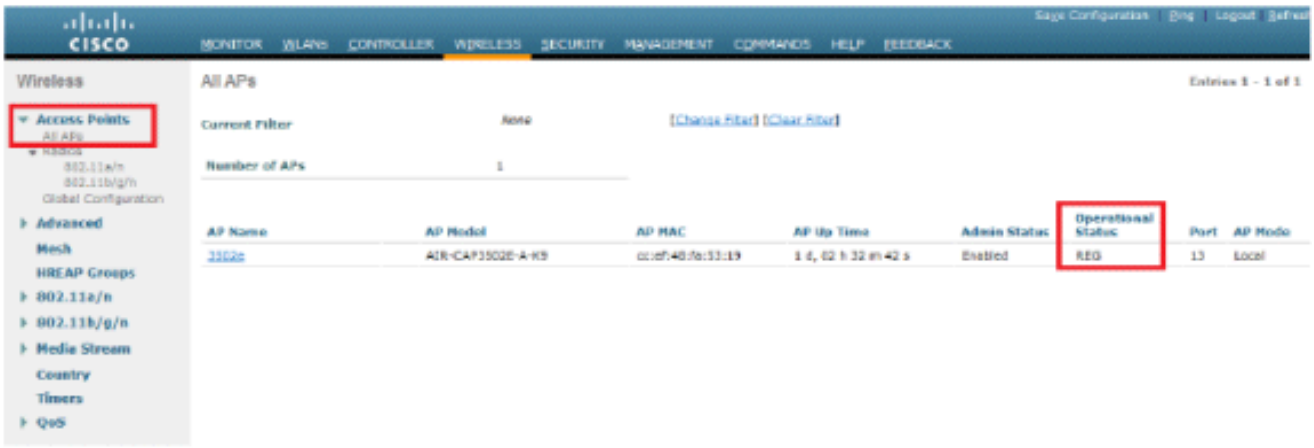
## 配置LAP

假设：

LAP已使用选项43、DNS或静态配置的WLC管理接口IP注册到WLC。

请完成以下步骤：

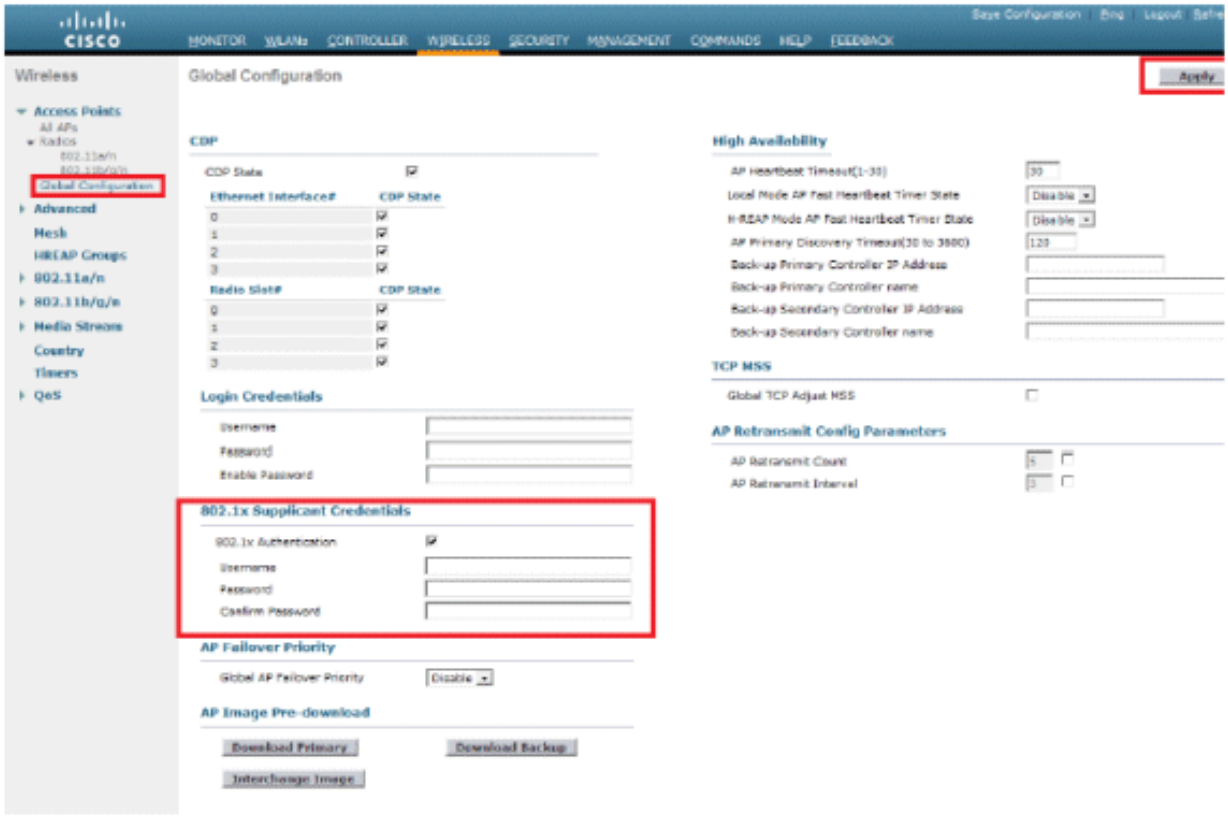
1. 转到Wireless > Access Points > All APs以验证WLC上的LAP注册。




2. 您可以通过两种方式为所有LAP配置802.1x凭证（即用户名/密码）：

   - 全局

     对于已加入的LAP，您可以全局设置凭证，以便加入WLC的每个LAP都将继承这些凭证。

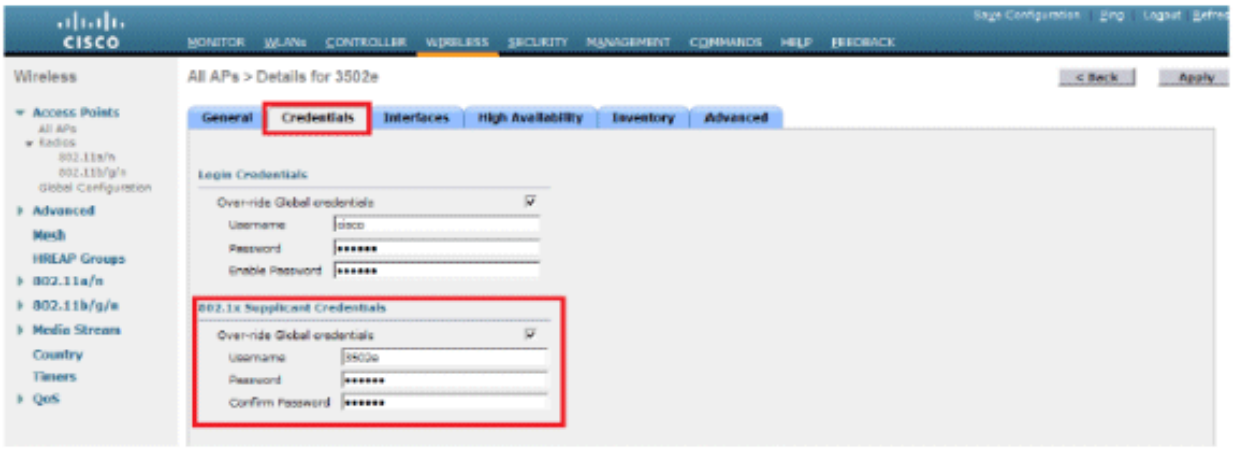



- 单独

  配置每个AP的802.1 x配置文件。在我们的示例中，我们将配置每个AP的凭证。

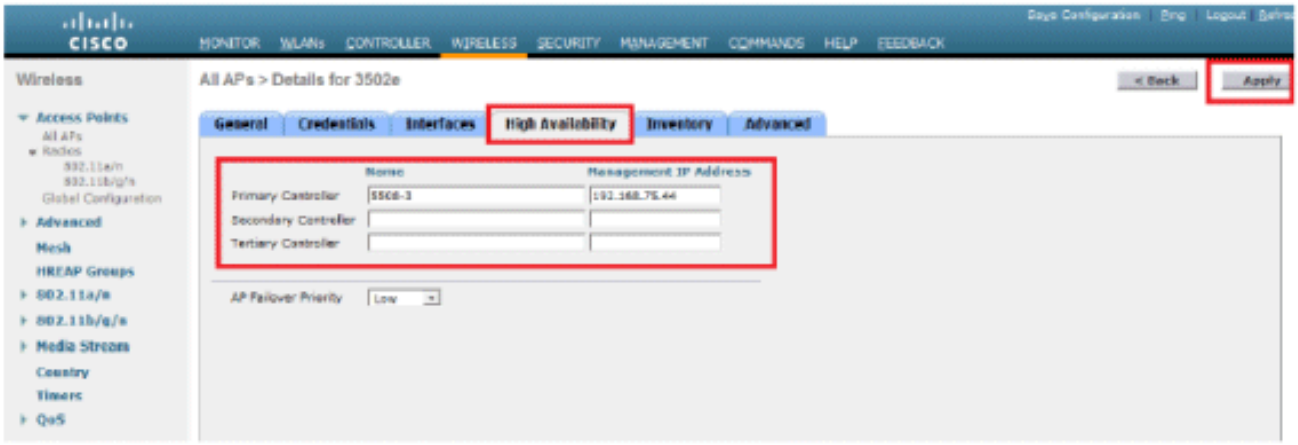
  a. 转至Wireless > All APs，然后选择相关的AP。

  b. 在802.1x Supplicant Credentials字段中添加用户名和密码。




  注意：登录凭证用于通过Telnet、SSH或控制台登录到AP。

3. 配置High Availability部分，然后单击Apply。




注意：保存后，这些凭证在WLC中保留并重新启动AP。仅当LAP加入新的WLC时，凭证才会更改。LAP采用在新WLC上配置的用户名和密码。

如果AP尚未加入WLC，则必须通过控制台连接到LAP以设置凭证。在启用模式下发出以下CLI命令：

LAP#lwapp ap dot1x username <username> password <password>

或

LAP#capwap ap dot1x username <username> password <password>

注意：此命令仅适用于运行恢复映像的AP。

LAP的默认用户名和密码分别为cisco和Cisco。

## 配置交换机

交换机充当LAP的身份验证器，并根据RADIUS服务器对LAP进行身份验证。如果交换机没有兼容的软件，请升级交换机。在交换机CLI中，发出以下命令以在交换机端口上启用802.1x身份验证：

```
<#root>

switch#

configure terminal

switch(config)#

dot1x system-auth-control

switch(config)#

aaa new-model

!--- Enables 802.1x on the Switch.

switch(config)#

aaa authentication dot1x default group radius
```

```
switch(config)#
radius server host 192.168.150.24 key cisco

!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x information

switch(config)#
ip radius source-interface vlan 253

!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.

switch(config)interface gigabitEthernet 0/11
switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253
switch(config-if)mls qos trust dscp
switch(config-if)spanning-tree portfast

!--- gig0/11 is the port number on which the AP is connected.

switch(config-if)dot1x pae authenticator

!--- Configures dot1x authentication.

switch(config-if)dot1x port-control auto

!--- With this command, the switch initiates the 802.1x authentication.
```

注意：如果同一交换机上有其他AP，并且您不希望它们使用802.1x，您可以保留未为802.1x配置的端口或发出以下命令：

```
<#root>
switch(config-if)authentication port-control force-authorized
```

## 配置RADIUS服务器

使用EAP-FAST对LAP进行身份验证。如果您未使用Cisco ACS 5.2，请确保您使用的RADIUS服务器支持此EAP方法。

RADIUS服务器配置分为四个步骤：

1. 配置网络资源。
2. 配置用户.
3. 定义策略元素。
4. 应用访问策略。

ACS 5.x是基于策略的ACS。换句话说，ACS 5.x使用基于规则的策略模型，而不是4.x版本中使用的基于组的模型。

ACS 5.x基于规则的策略模型提供比旧的基于组的方法更强大、更灵活的访问控制。

在旧的基于组的模型中，一个组定义策略，因为它包含三种类型的信息并将它们关联在一起：

- 身份信息 — 此信息可以基于AD或LDAP组中的成员资格或内部ACS用户的静态分配。
- 其他限制或条件 — 时间限制、设备限制等。
- 权限 — VLAN或Cisco IOS®权限级别。

ACS 5.x策略模型基于以下形式的规则：

如果condition，则结果

例如，我们使用为基于组的模型描述的信息：

如果为identity-condition、restriction-condition，则为authorization-profile。

因此，我们可以灵活地限制允许用户访问网络的条件，以及在满足特定条件时允许的授权级别。

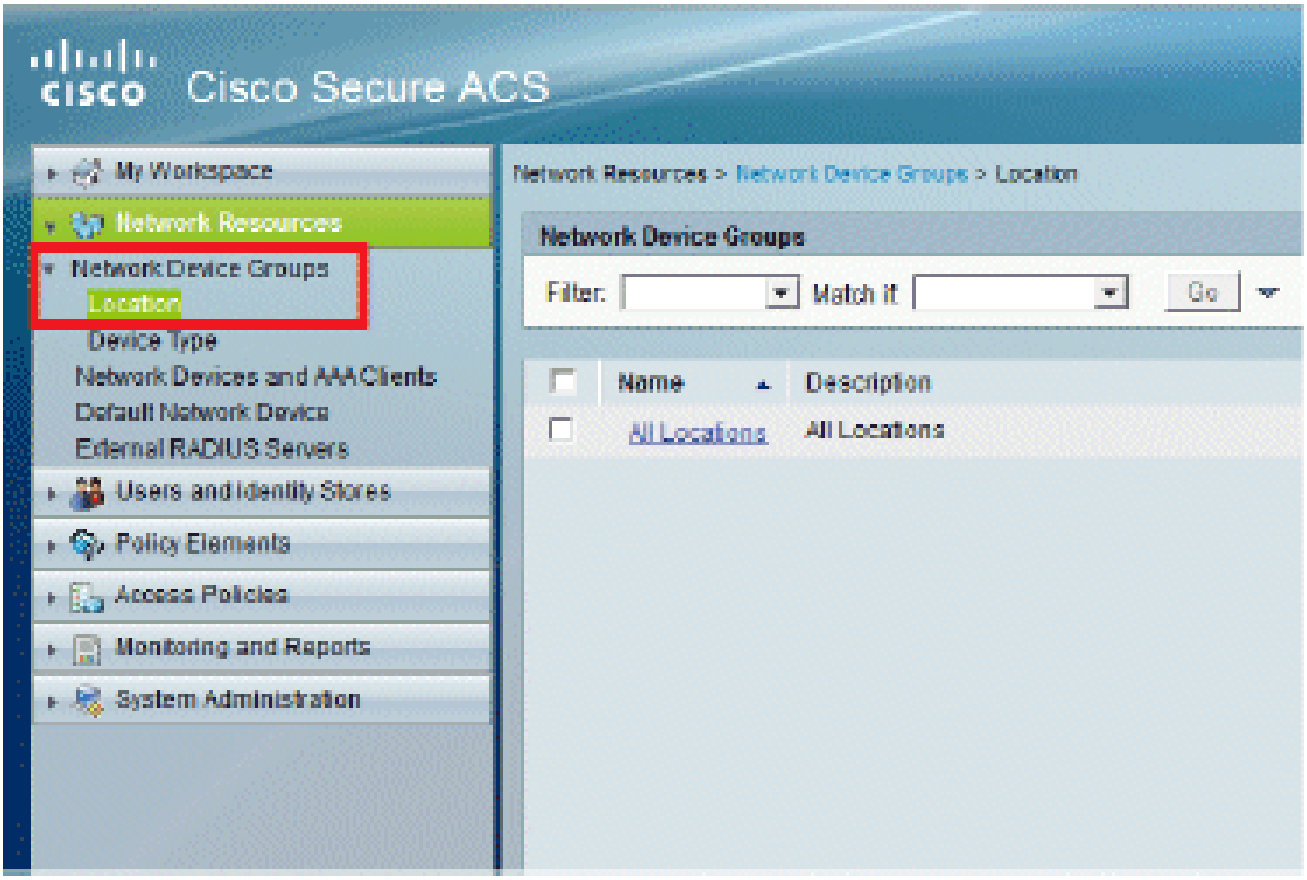
## 配置网络资源

在本节中，我们将为RADIUS服务器上的交换机配置AAA客户端。

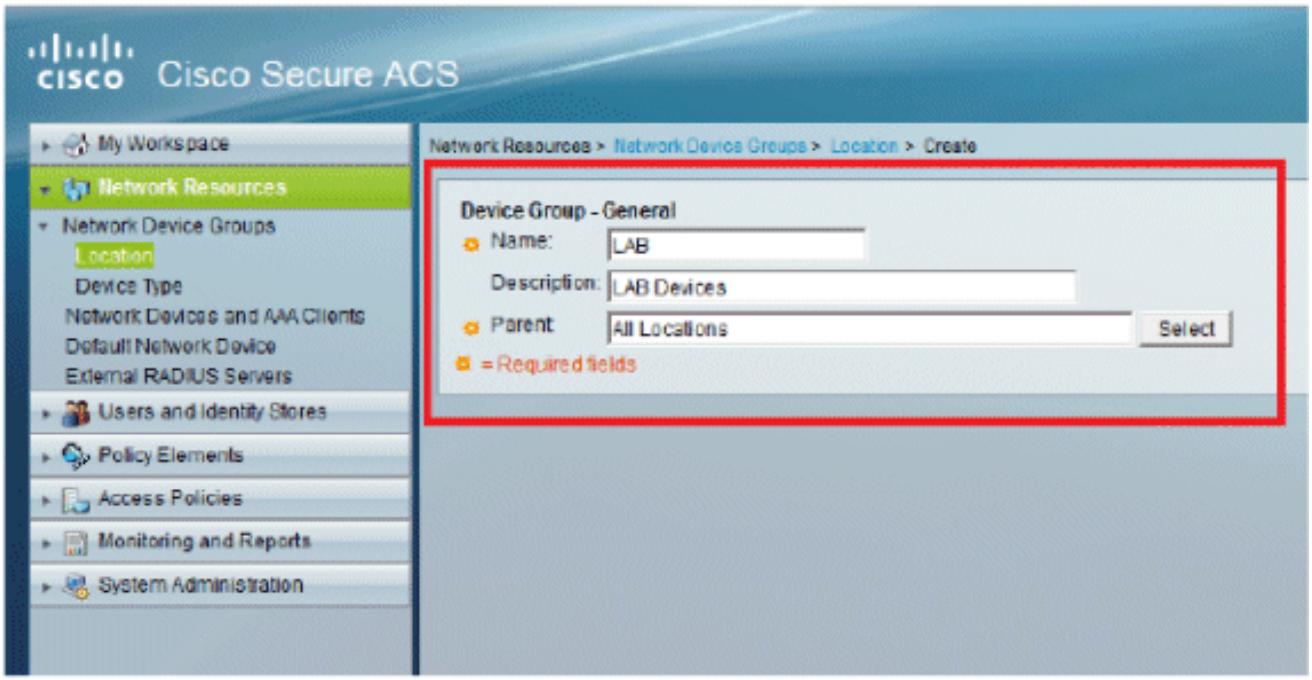
此过程说明如何将交换机添加为RADIUS服务器上的AAA客户端，以便交换机可以将LAP的用户凭证传递到RADIUS服务器。

请完成以下步骤：

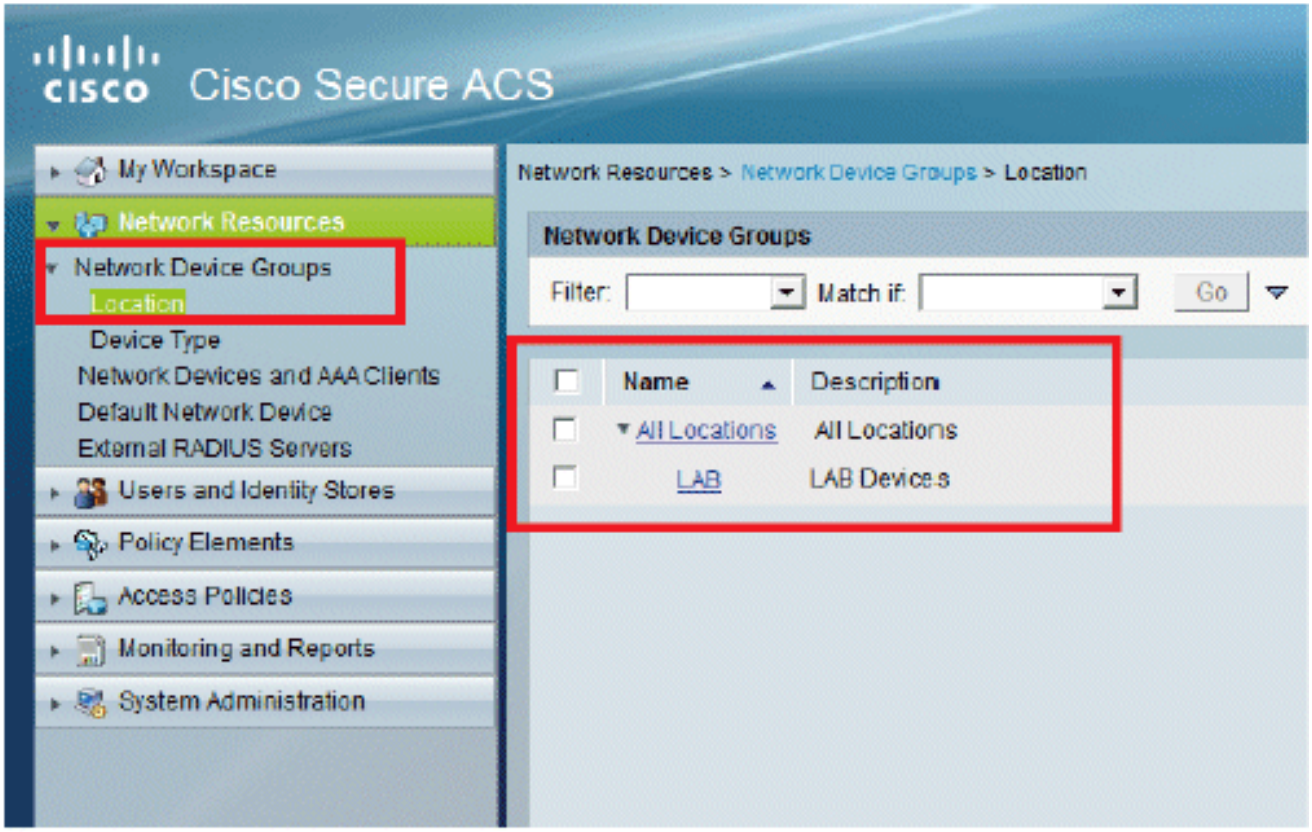
1. 在ACS GUI中，单击Network Resources。
2. 单击Network Device Groups。
3. 转至Location > Create（位于底部）。



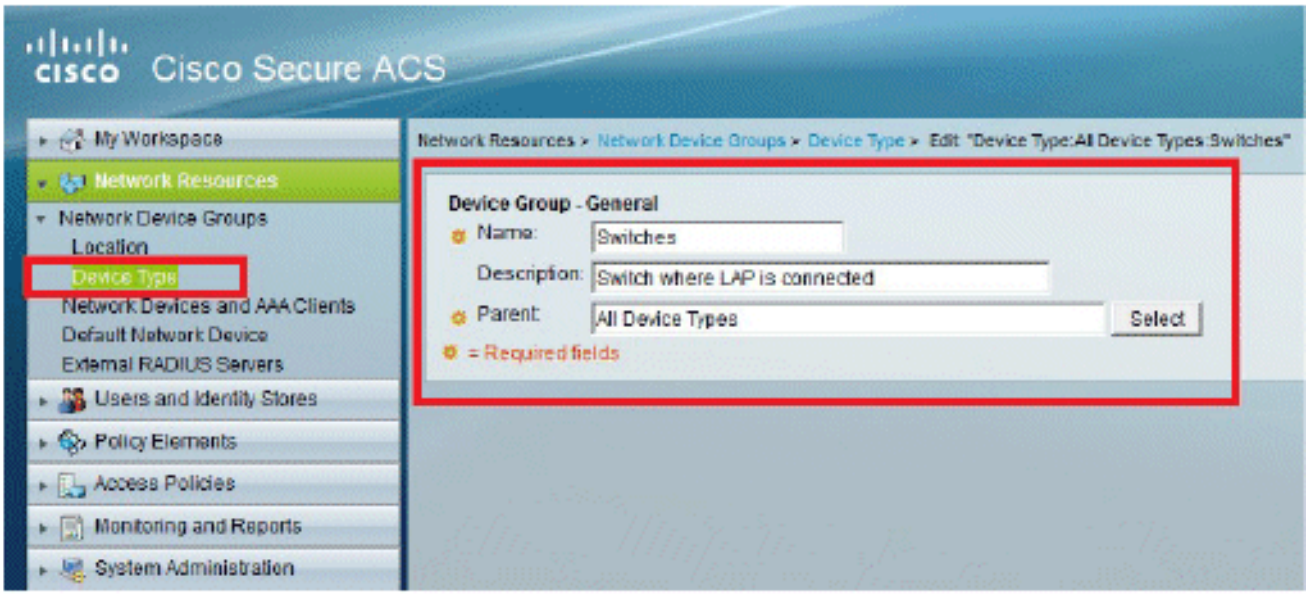

4. 添加必填字段，然后单击Submit。




5. 窗口将刷新：



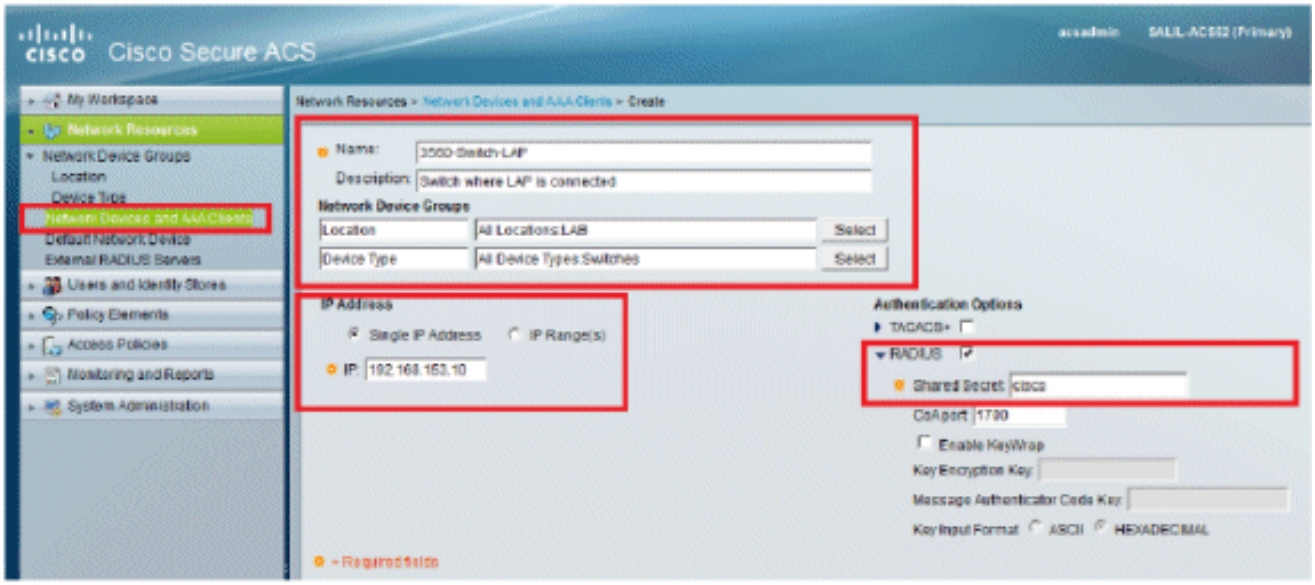

6. 单击Device Type > Create。



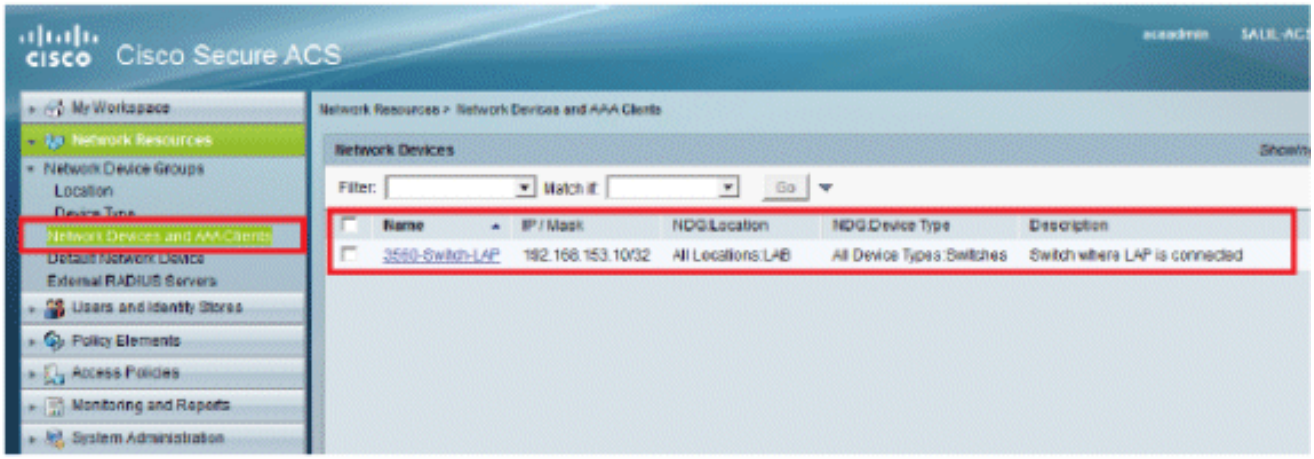

7. 单击“Submit”。完成后，窗口将刷新：


8. 转至Network Resources > Network Devices and AAA Clients。

9. 单击Create，并填写如下所示的详细信息：




10. 单击“Submit”。窗口将刷新：

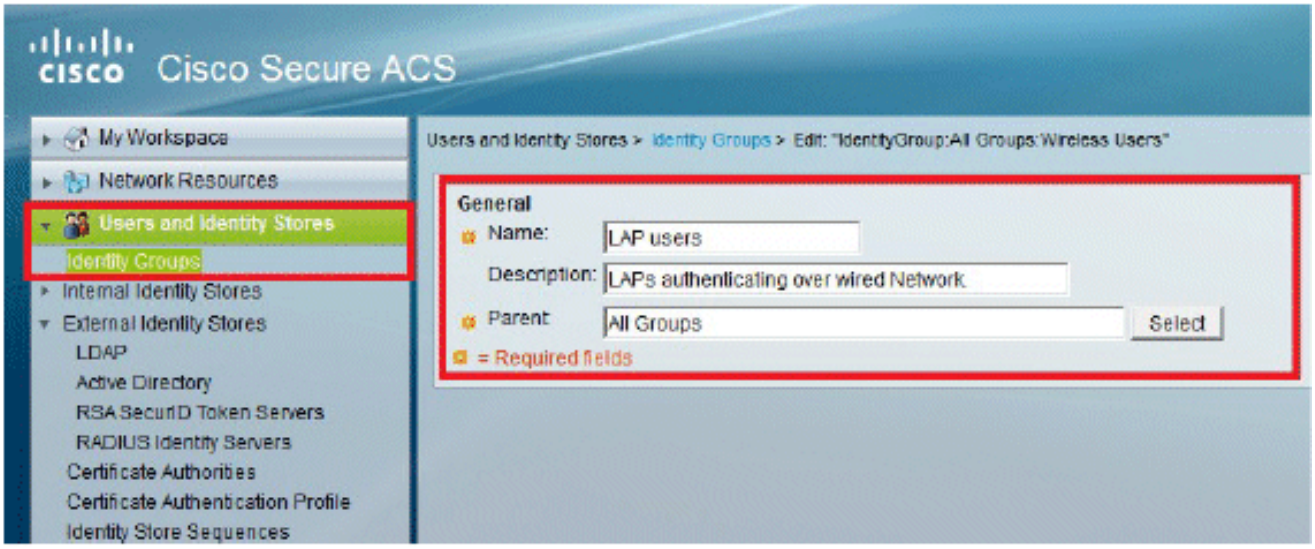



## 配置用户

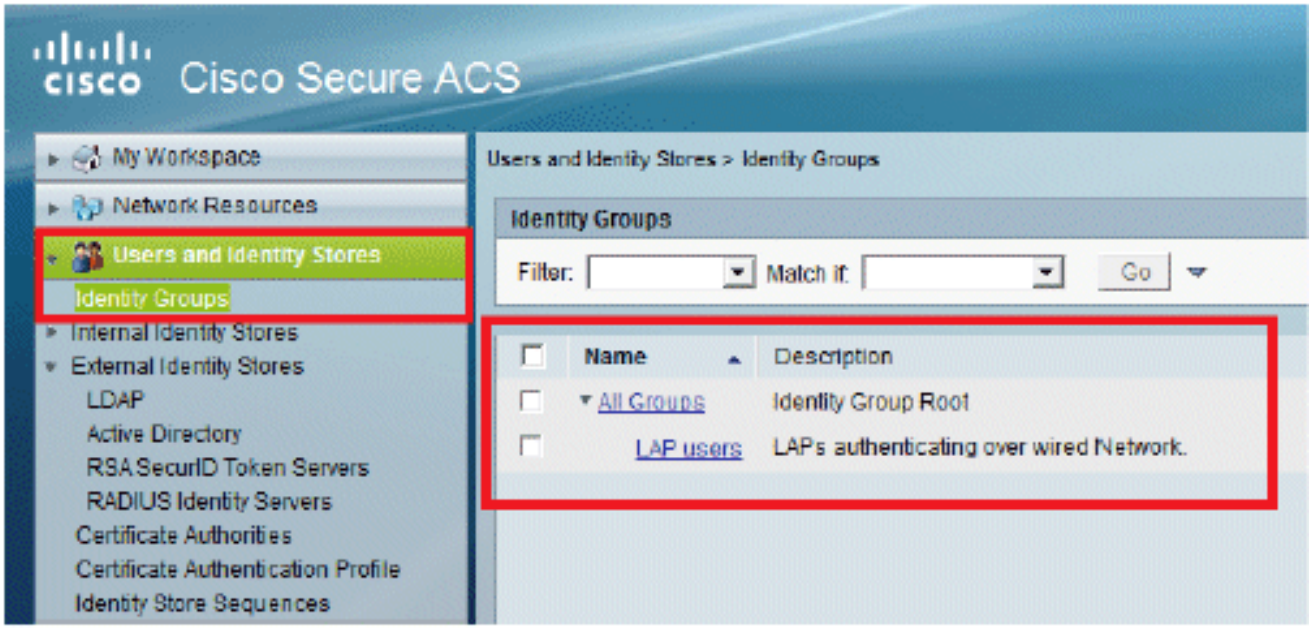
在本节中，您将看到如何在之前配置的ACS上创建用户。您将将该用户分配到名为“LAP用户”的组。

请完成以下步骤：

1. 转至Users and Identity Stores > Identity Groups > Create。

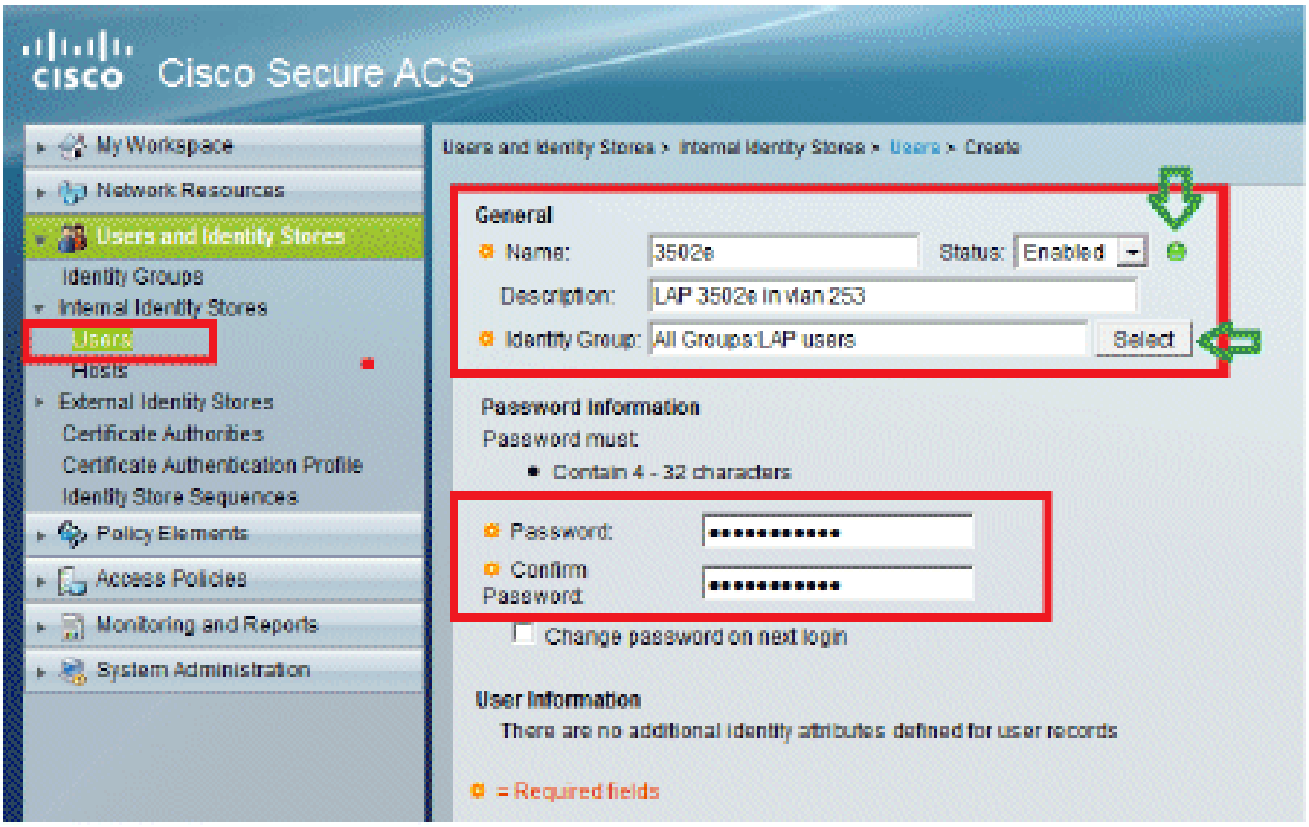



2. 单击“Submit”。

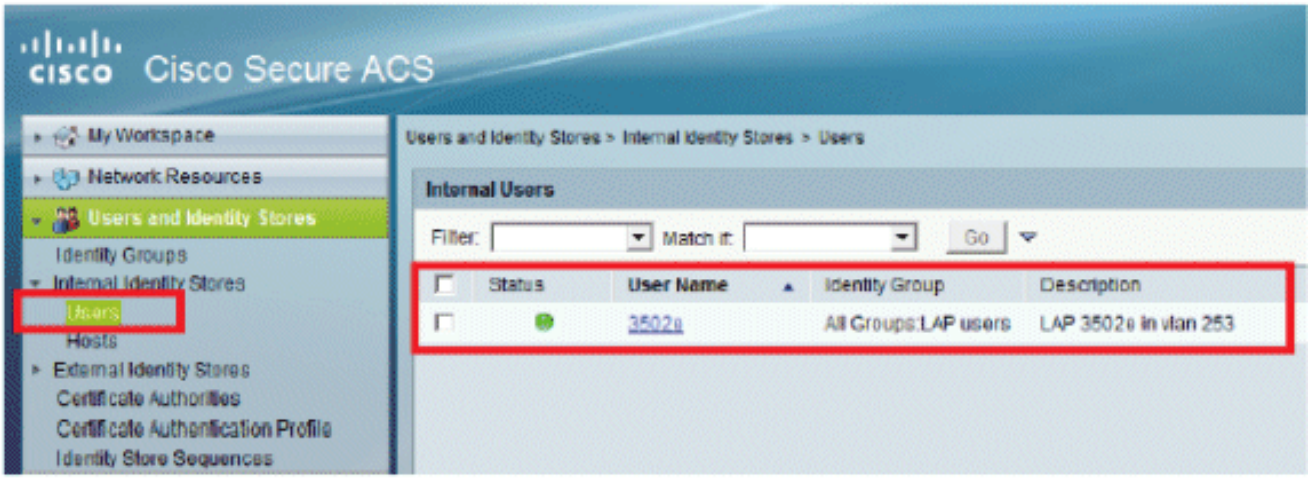



3. 创建3502e并将其分配到组“LAP用户”。

4. 转至Users and Identity Stores > Identity Groups > Users > Create。

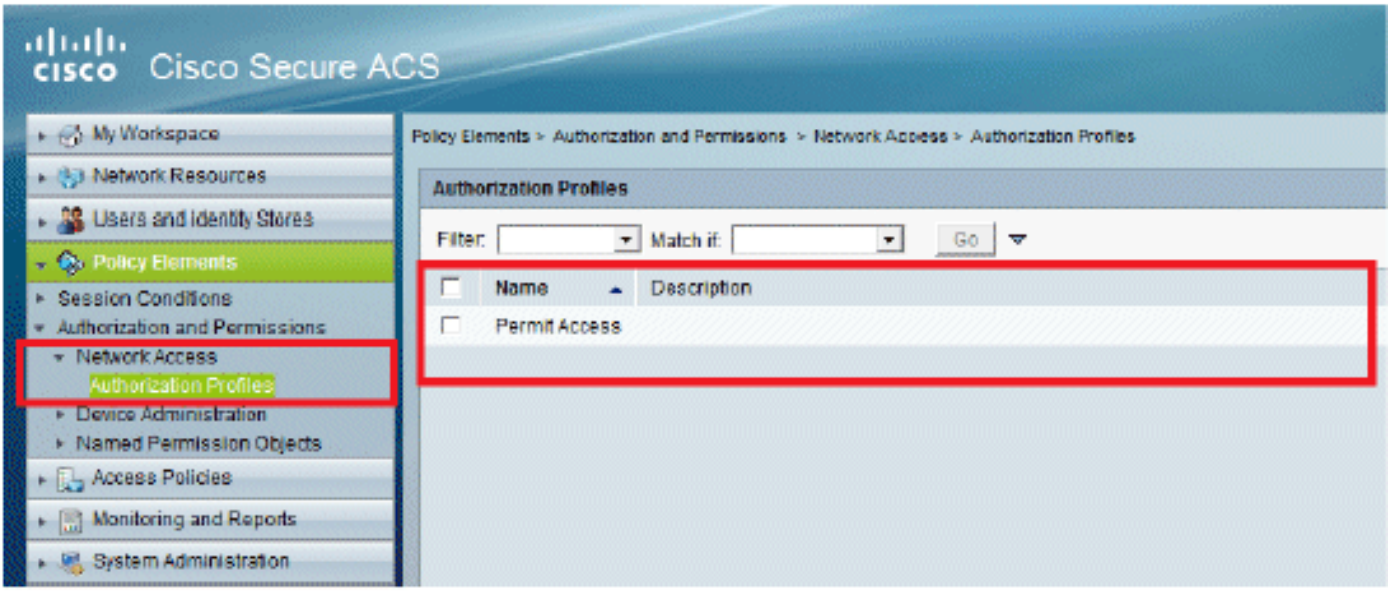



5. 您将看到更新的信息：




## 定义策略元素

验证Permit Access已设置。

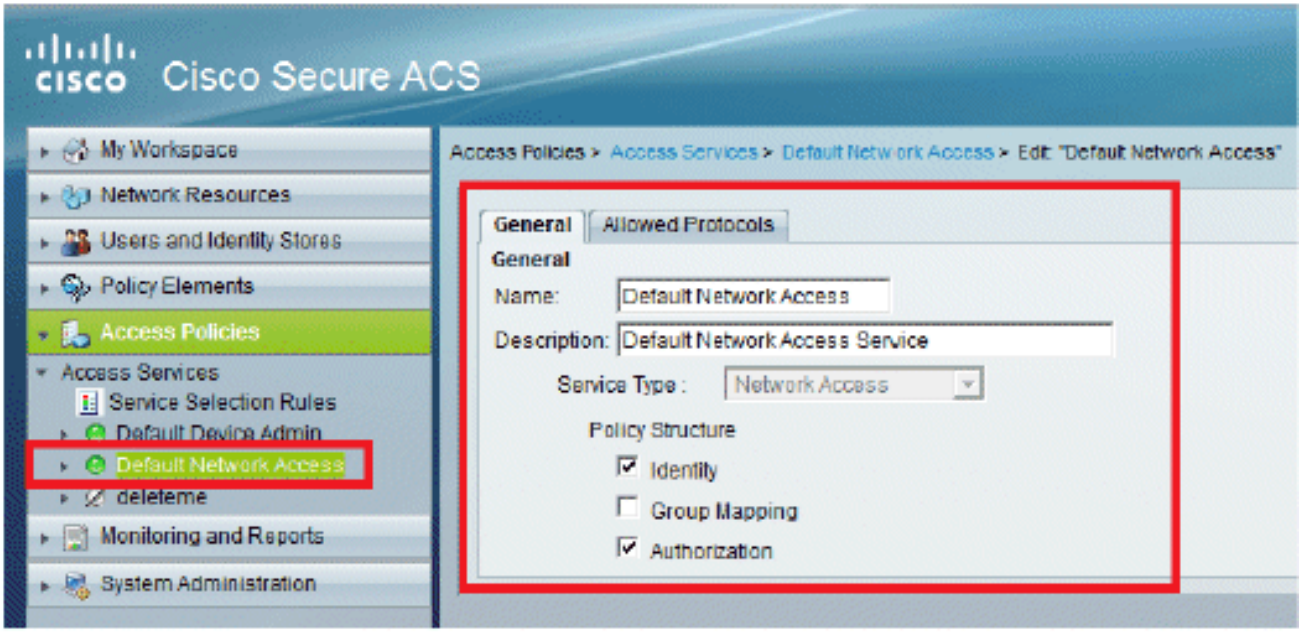



## 应用访问策略

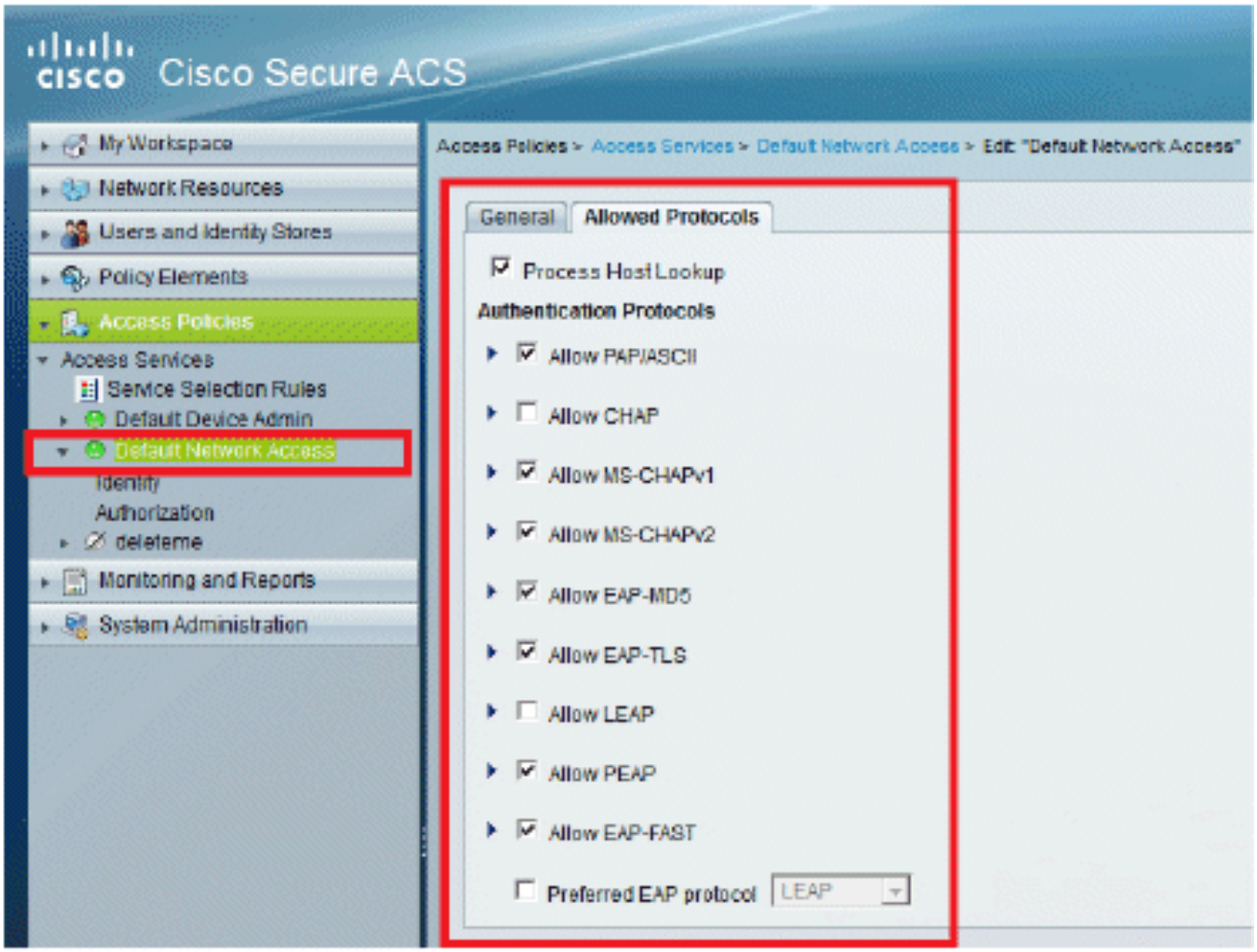
在本部分中，您将选择EAP-FAST作为LAP的身份验证方法，以便进行身份验证。然后，您将基于上述步骤创建规则。

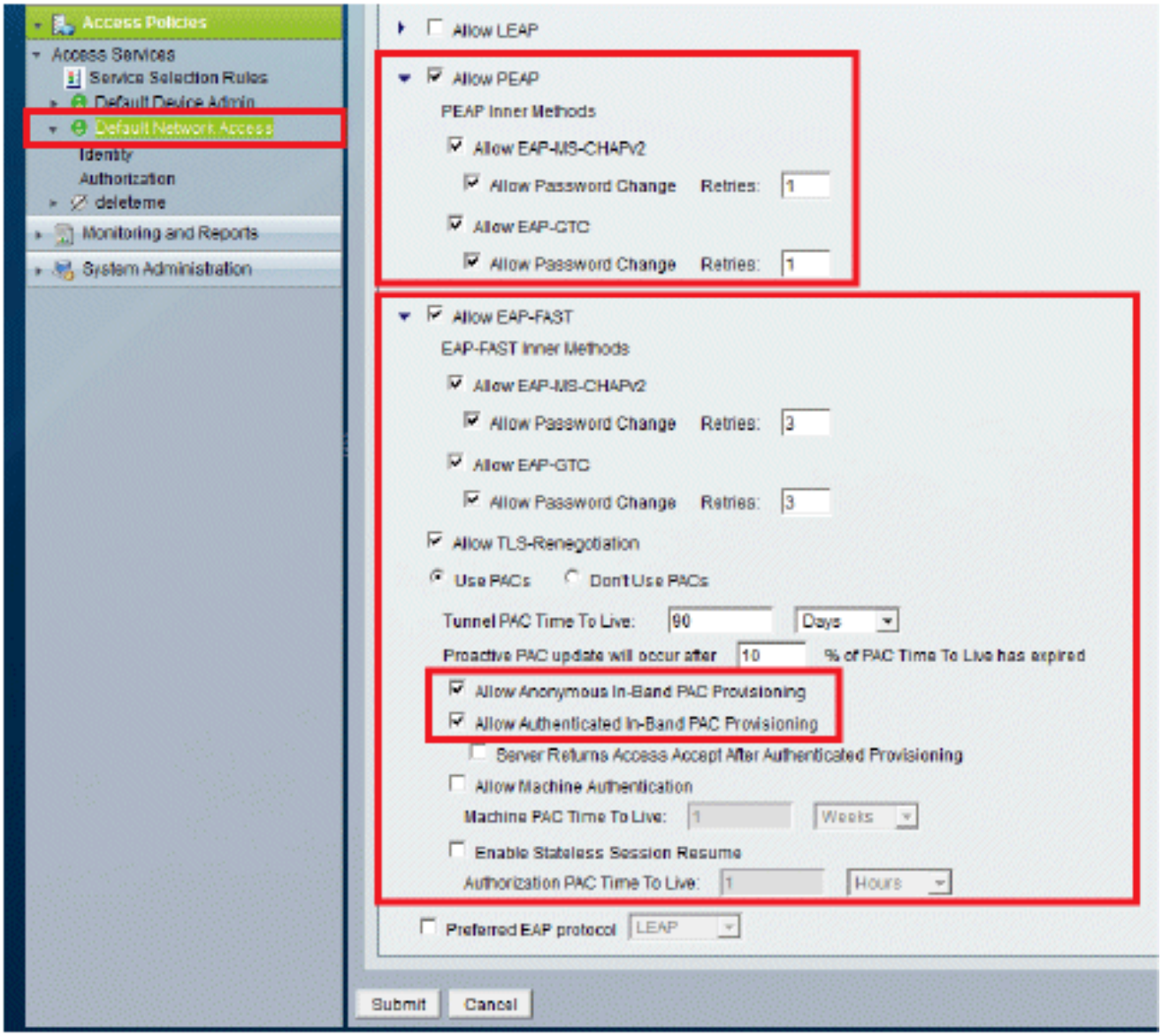
请完成以下步骤：

1. 转至Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"。



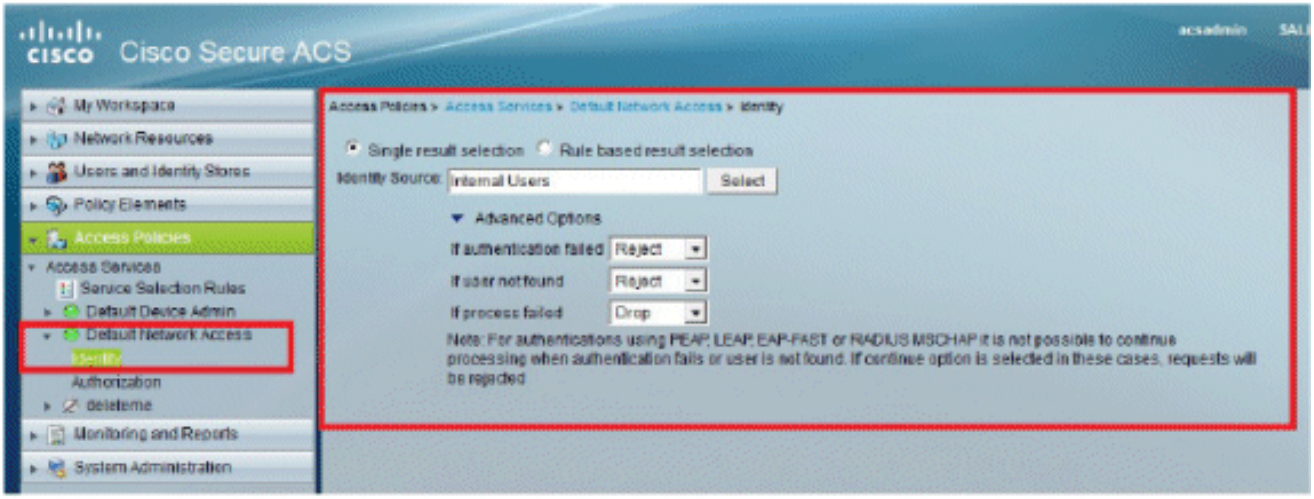

2. 确保已启用EAP-FAST和匿名带内PAC调配。






3. 单击“Submit”。

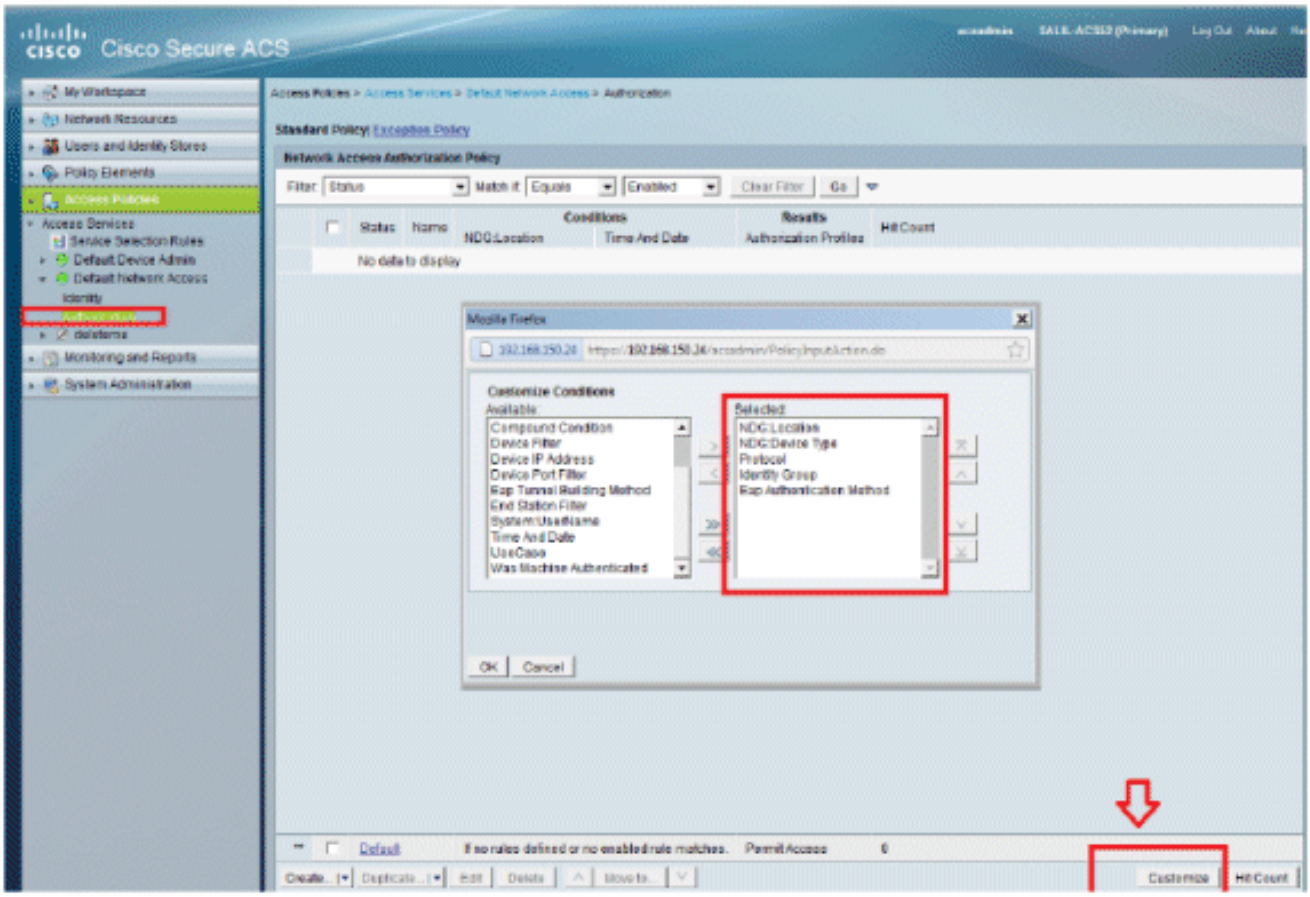
4. 验证您选择的身份组。在本示例中，使用Internal Users（在ACS上创建）并保存更改。




5. 转至Access Policies > Access Services > Default Network Access > Authorization以验证授

权配置文件。

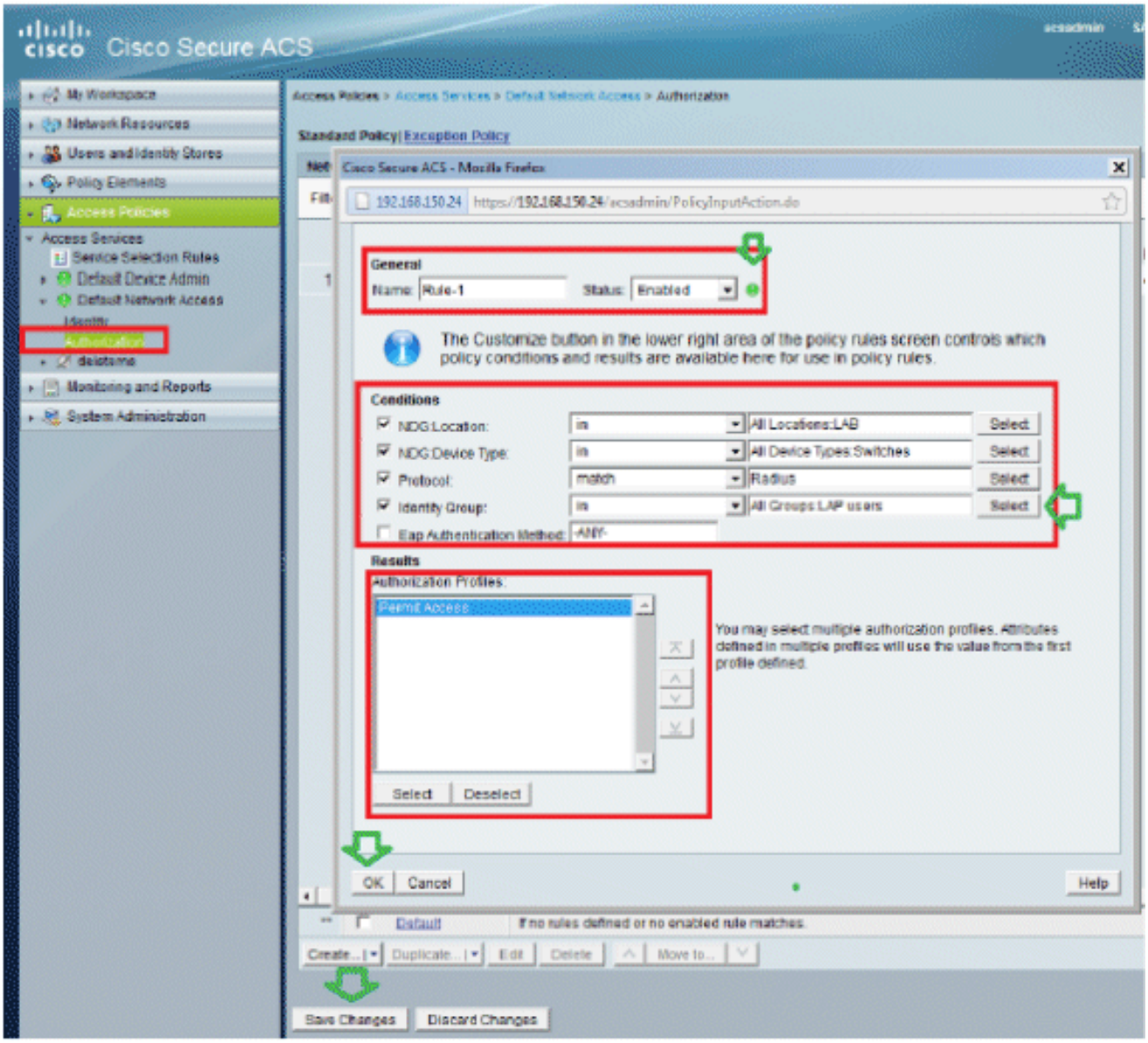
您可以自定义在什么条件下允许用户访问网络，以及经过身份验证后通过什么授权配置文件（属性）。此精细度仅在ACS 5.x中可用。在本示例中，选择Location、Device Type、Protocol、Identity Group和EAP Authentication Method。



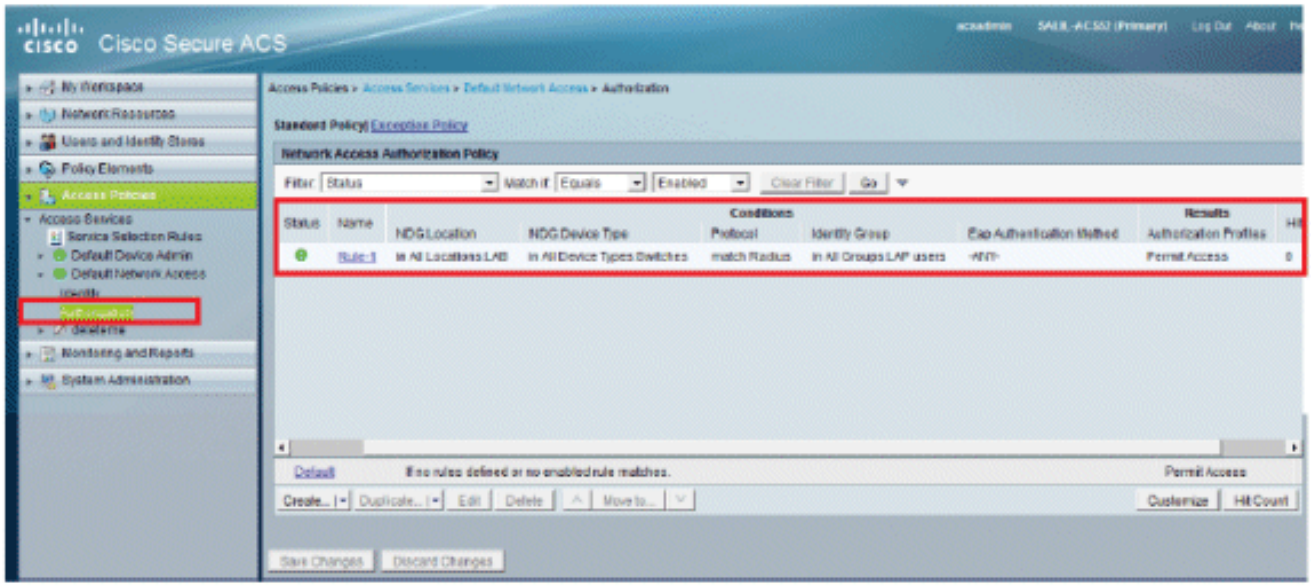

6. 单击确定，然后单击保存更改。

7. 下一步是创建规则。如果未定义规则，则允许LAP访问而不带任何条件。

8. 单击Create > Rule-1。此规则适用于组“LAP用户”中的用户。

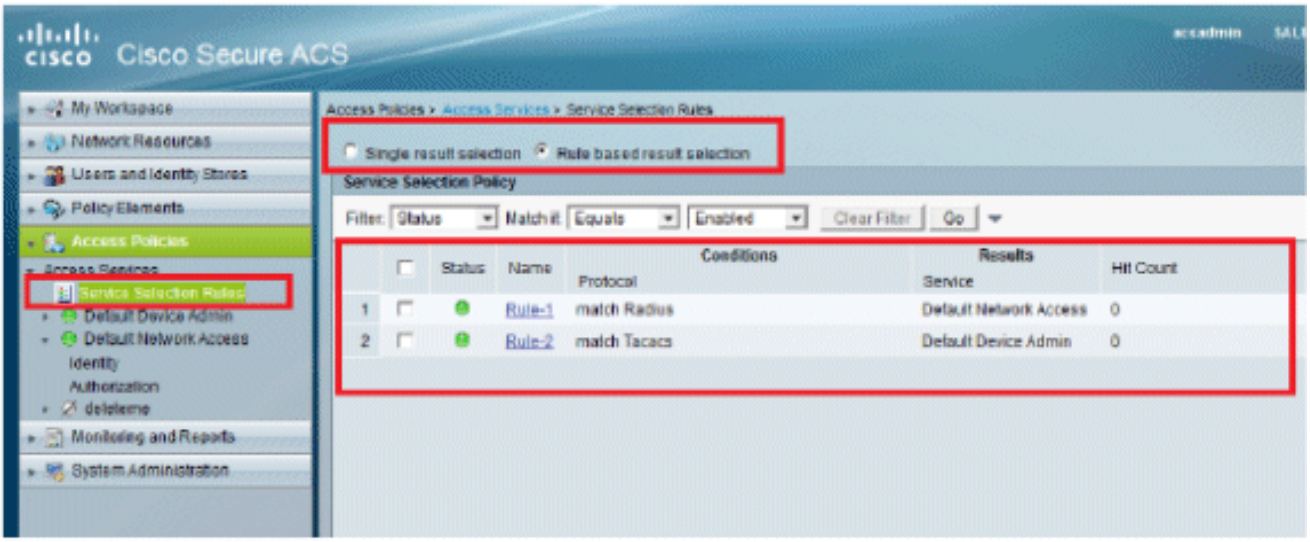



9. 点击Save Changes。如果希望拒绝不匹配条件的用户，请编辑默认规则以显示“拒绝访问”。




10. 最后一步是定义服务选择规则。使用此页可以配置简单策略或基于规则的策略，以确定将哪种

服务应用于传入请求。例如：




# 验证

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。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。

AP控制台：

<#root>

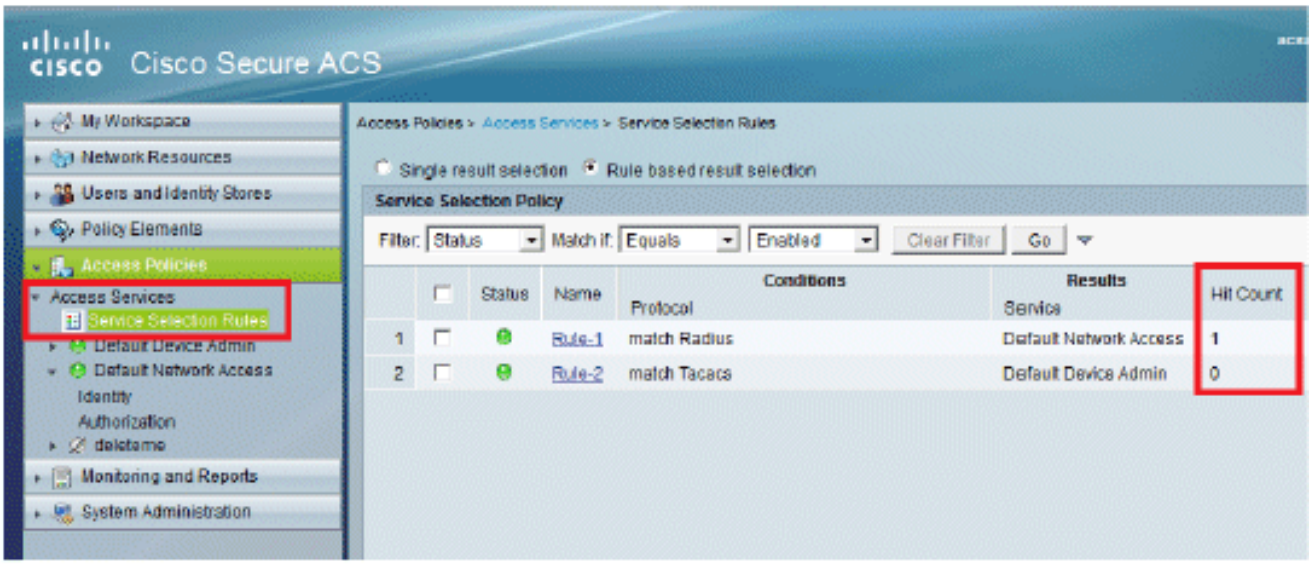
```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247

!--- AP disconnects upon adding dot1x information in the gig0/11.

*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   administratively down
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   administratively down
*Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)
*Jan 29 09:10:36.203: status of voice_diag_test from WLC is false

*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST] *Jan 29

!--- Authentication is successful and the AP gets an IP.
```

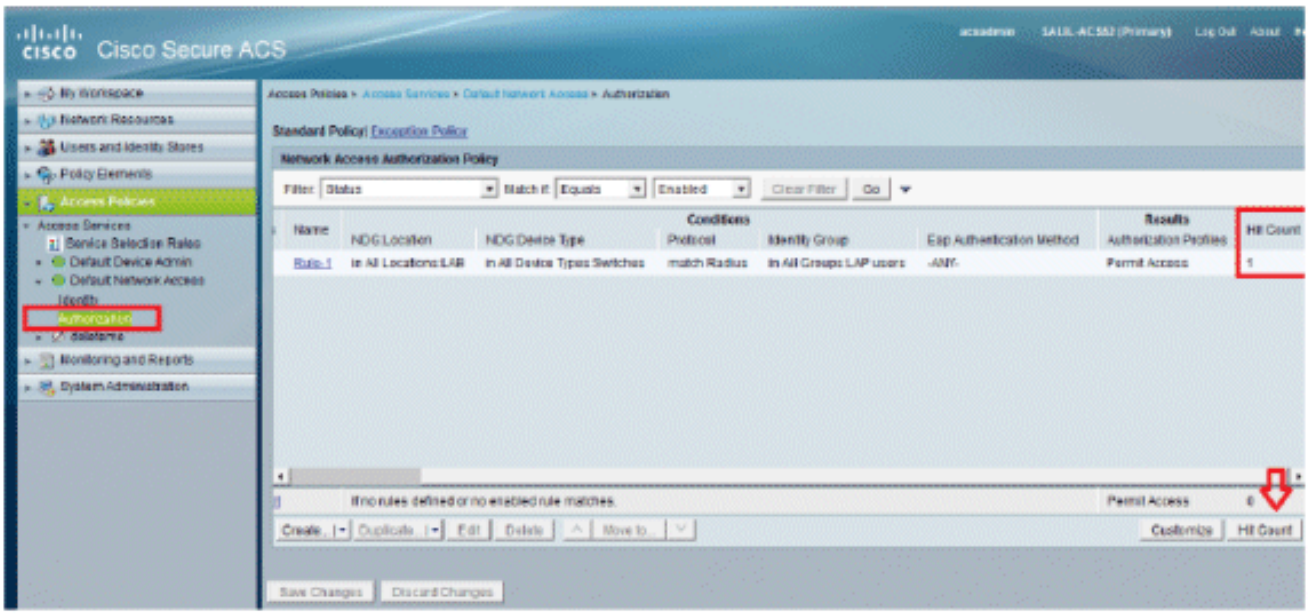
```
Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25)
*Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent
   peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
*Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created
   successfully peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44


*Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN


*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
   Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
   down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
   keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
   established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled

!--- AP joins the 5508-3 WLC.
```

ACS日志：

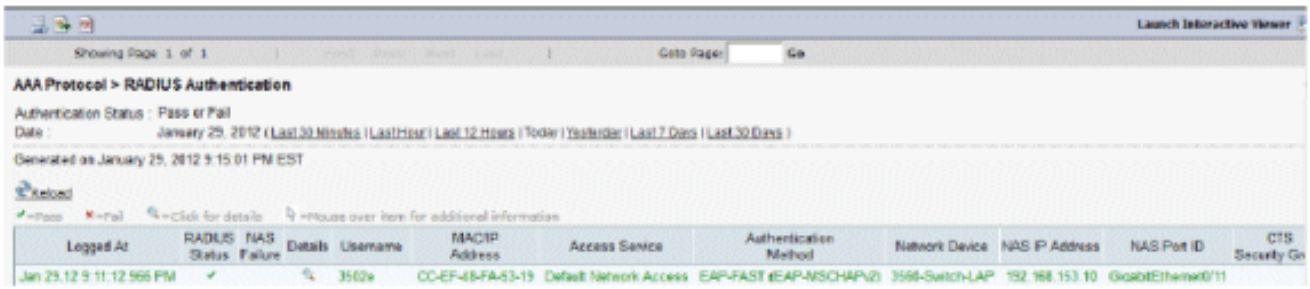
1. 查看命中次数：

   如果您在身份验证的15分钟内检查日志，请确保刷新命中计数。在同一页面底部有一个“点击计数”(Hit Count)选项卡。




2. 单击Monitoring and Reports，此时将显示一个新的弹出窗口。单击Authentications -RADIUS -Today。您也可以单击Details以验证应用了哪个服务选择规则。




# 故障排除

目前没有针对此配置的故障排除信息。

## 相关信息

- 思科安全访问控制系统
- 技术支持和文档 - Cisco Systems

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）。