使用9800控制器配置接入点的802.1X请求方

目录

简介

本文档介绍如何将思科接入点(AP)配置为802.1x请求方，以便在交换机端口上针对RADIUS服务器进行授权。

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（轻量接入点）。
- 思科交换机和ISE上的802.1x
- 可扩展认证协议 (EAP)
- 远程用户拨入认证系统(RADIUS)

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、Cisco IOS® XE、15.2(3r)E2
- C9800-CL-K9、Cisco IOS® XE、17.6.1
- ISE 3.0

- AIR-CAP3702
- AIR-AP3802

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。

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ISE使用EAP方法EAP-FAST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。

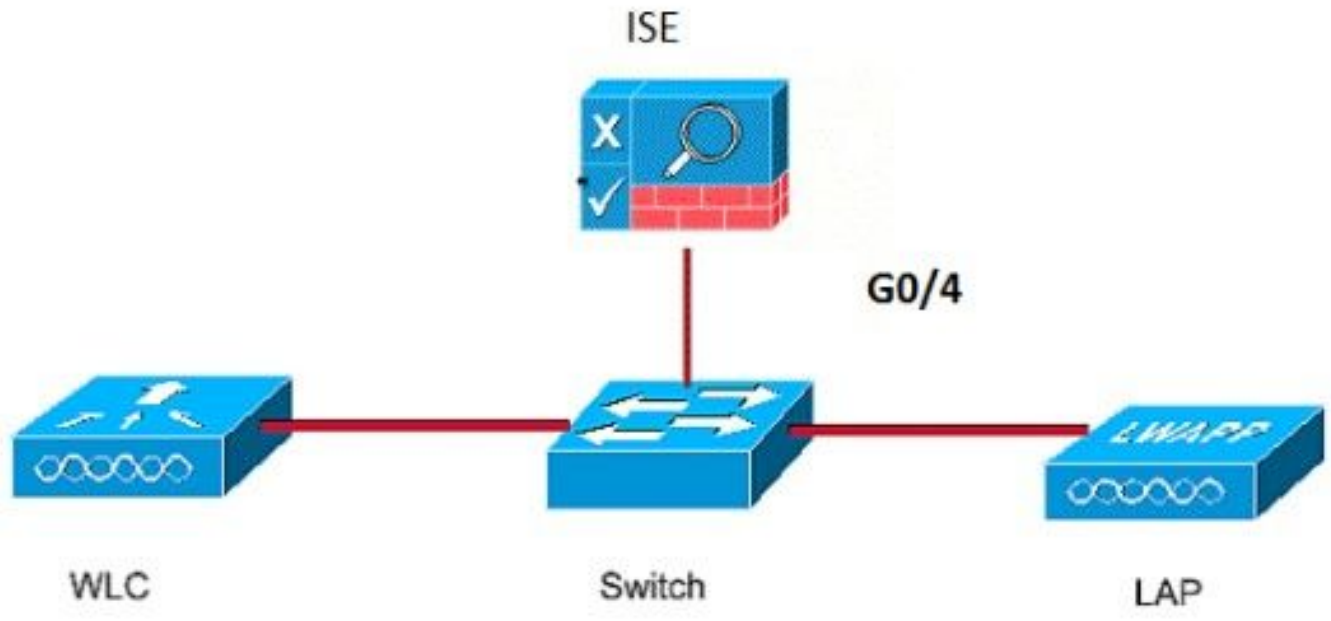
AP可以在加入WLC之前或加入WLC之后进行身份验证，在这种情况下，您可以在LAP加入WLC之后在交换机上配置802.1X。

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：

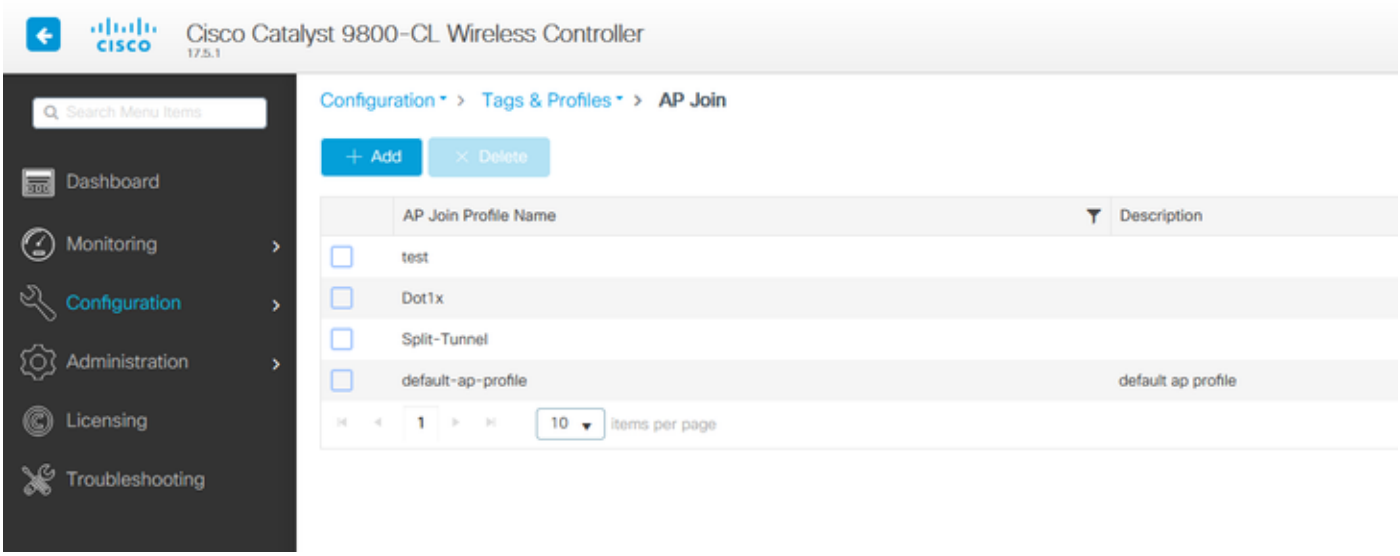


将LAP配置为802.1x请求方

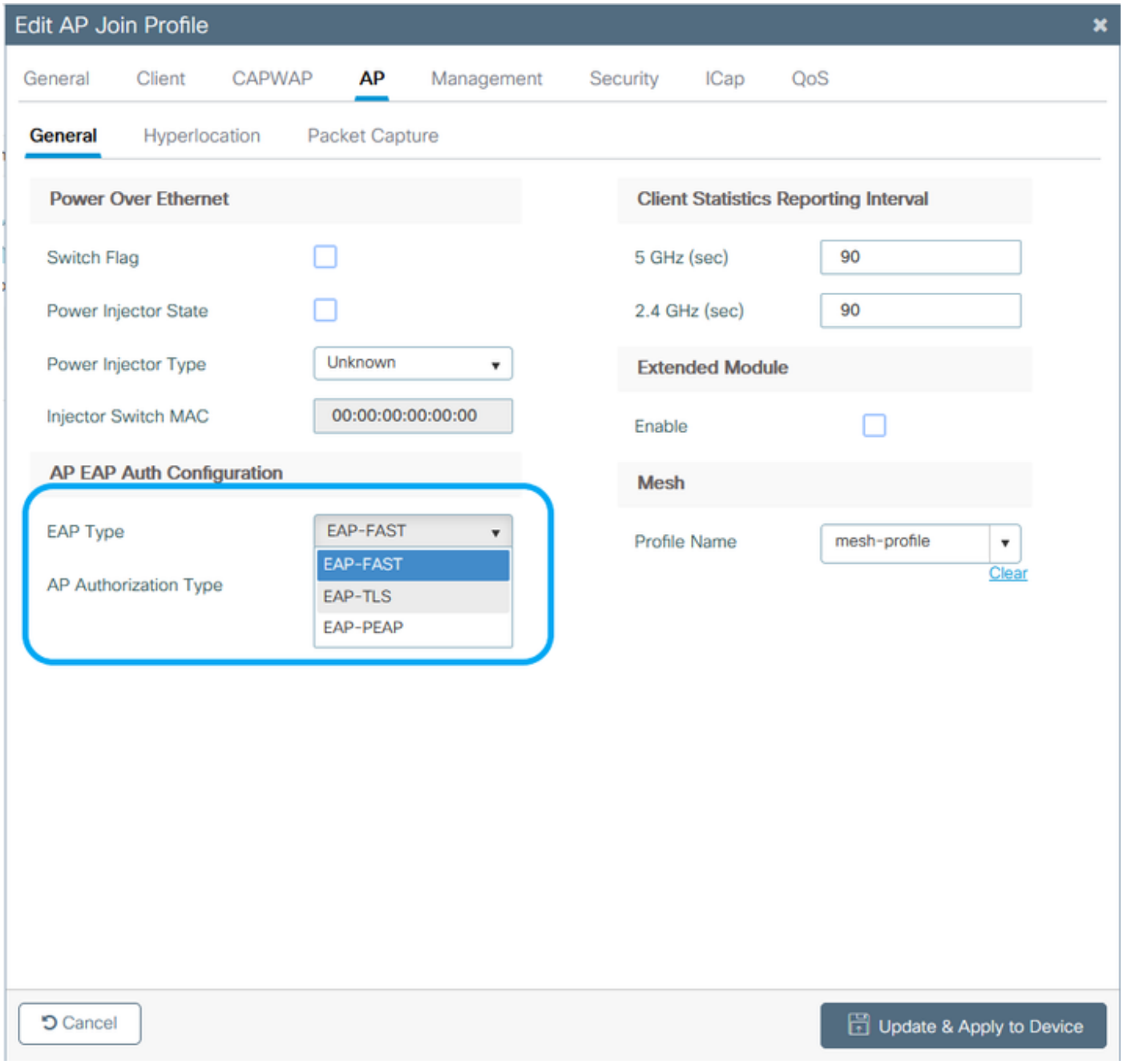
如果AP已加入WLC:

配置802.1x身份验证类型和本地重要证书(LSC)AP身份验证类型：

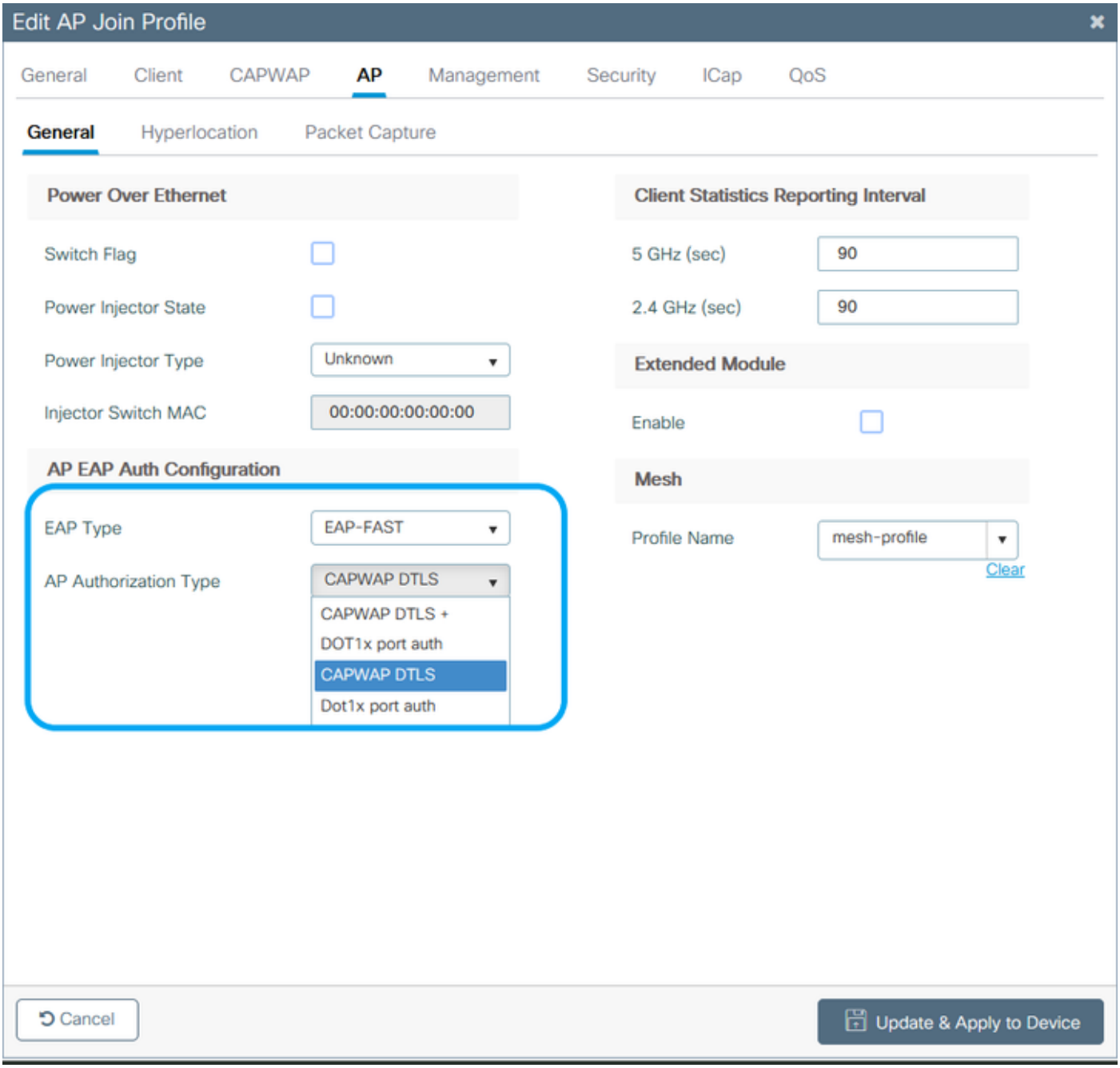
步骤1:在**AP Join Profile**页面上，导航至Configuration > **Tags & Profiles** > AP Join > On AP Join Profile上，点击**Add**以添加新的加入配置文件，或在点击AP加入配置文件名称时编辑该加入配置文件。



第二步：在AP Join Profile页面中，从**AP > General**导航到**AP EAP Auth Configuration**部分。 从**EAP Type**下拉列表中，选择EAP类型作为EAP-FAST、EAP-TLS或EAP-PEAP，以配置dot1x身份验证类型。

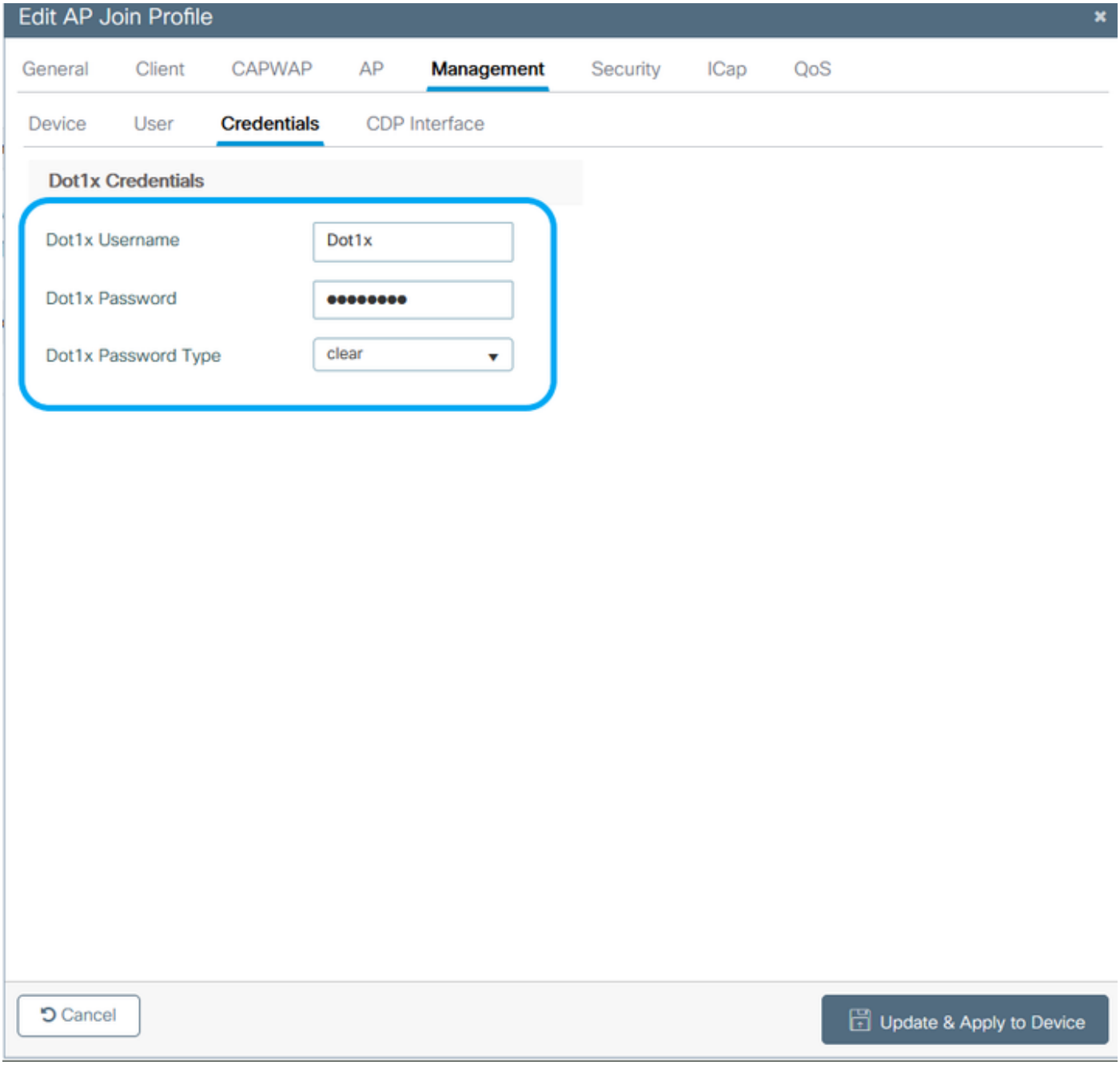


第三步：从**AP Authorization Type**下拉列表中，选择类型为CAPWAP DTLS +或CAPWAP DTLS >点击**Update & Apply to Device**。



配置802.1x用户名和密码：

步骤1:从**管理>凭证> 输入Dot1x用户名和密码详细信息**>选择适当的802.1x密码类型>单击**更新并应用到设备**



如果AP尚未加入WLC:

您必须通过控制台连接到LAP才能设置凭证并使用以下CLI命令：(适用于Cheetah OS和Cisco IOS® AP)

CLI：

```
LAP# debug capwap console cli
LAP# capwap ap dot1x username
```

清除AP上的Dot1x凭证（如果需要）

对于Cisco IOS® AP，重新加载AP后：

CLI：

```
LAP# clear capwap ap dot1x
```

对于Cisco COS AP，重新加载AP后：

CLI：

```
LAP# capwap ap dot1x disable
```

配置交换机

在交换机上全局启用dot1x并将ISE服务器添加到交换机。

CLI：

```
Enable
Configure terminal
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control
Radius-server host
```

配置AP交换机端口

CLI：

```
configure terminal
interface GigabitEthernet
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
end
```

如果AP处于Flex Connect模式（本地交换），则必须在交换机接口上进行额外配置，以允许端口上有多个MAC地址，因为客户端流量在AP级别释放：

```
authentication host-mode multi-host
```

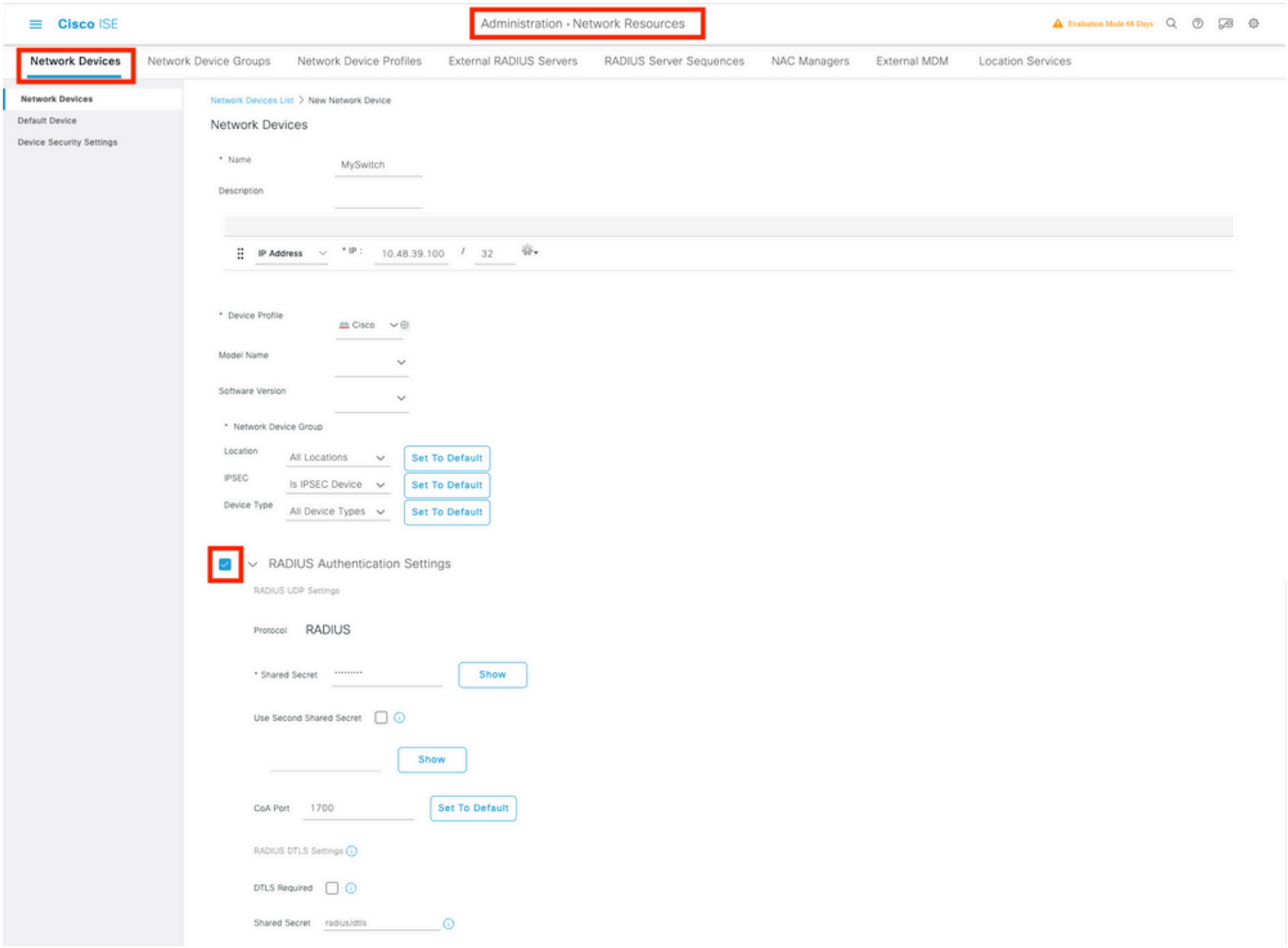
注意：意味着读者需要注意。注释包含有用的建议或文档未涵盖的材料的引用。

> **注意**：多主机模式对第一个MAC地址进行身份验证，然后允许无限数量的其他MAC地址。如果已连接的AP配置了本地交换模式，请在交换机端口上启用主机模式。它允许客户端的流量通过交换机端口。如果需要安全流量路径，则在WLAN上启用dot1x以保护客户端数据

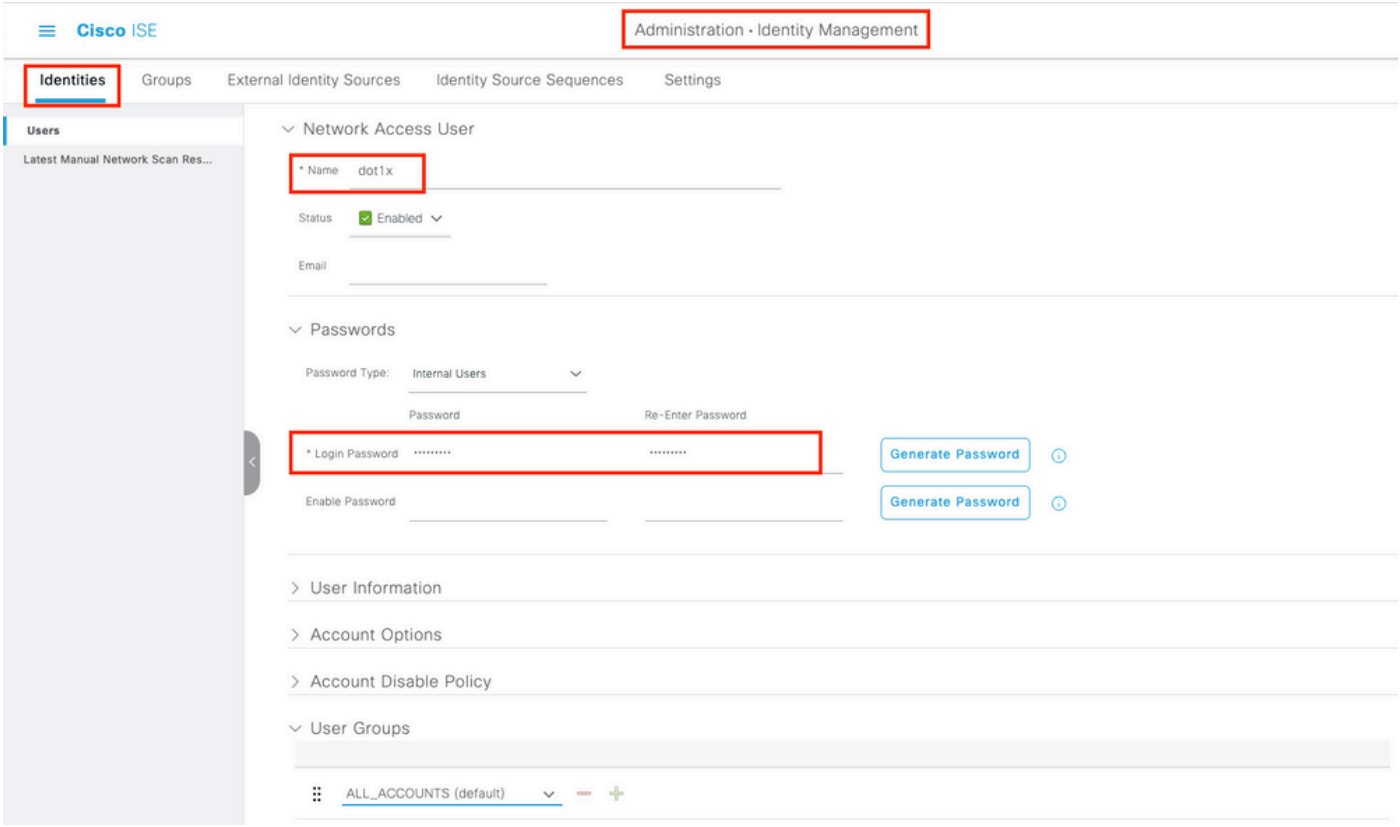
配置ISE服务器

步骤1: **将交换机添加为ISE服务器上的网络设备。**导航到Administration > Network Resources >

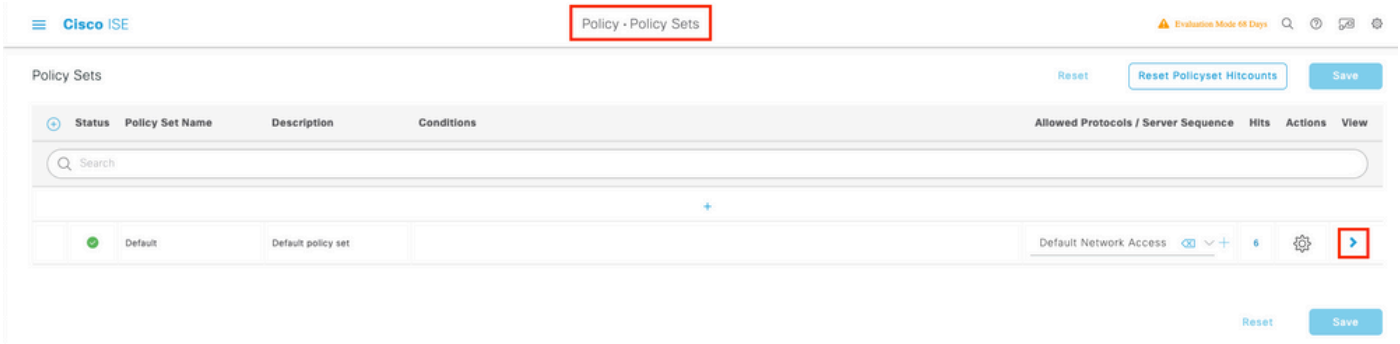
Network Devices > Click **Add** > Enter Device name， IP address， enable RADIUS Authentication Settings， Specify Shared Secret Value， COA port（或保留为默认值）> **Submit**。



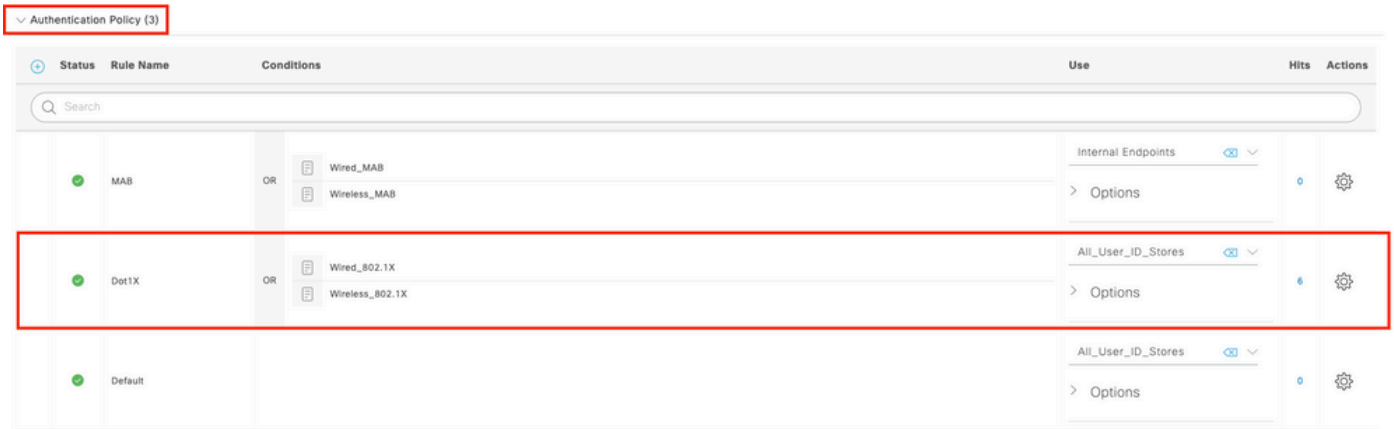
第二步：**将AP凭证添加到ISE**。导航到**Administration > Identity Management > Identities > Users**，然后单击**Add**按钮添加用户。您需要在此处输入在WLC上的AP加入配置文件中配置的凭证。请注意，用户被置于此处的默认组中，但可根据要求进行调整。

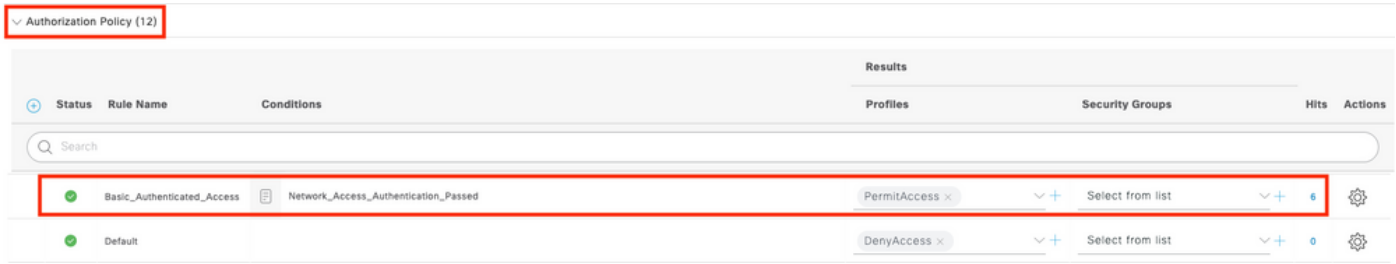


第三步：在ISE上，配置身份**验证策**略和**授权策略**。 转至**Policy > Policy Sets**，选择要配置的策略集和右侧的蓝色箭头。在这种情况下，将使用默认策略集，但可以根据要求自定义该策略集。

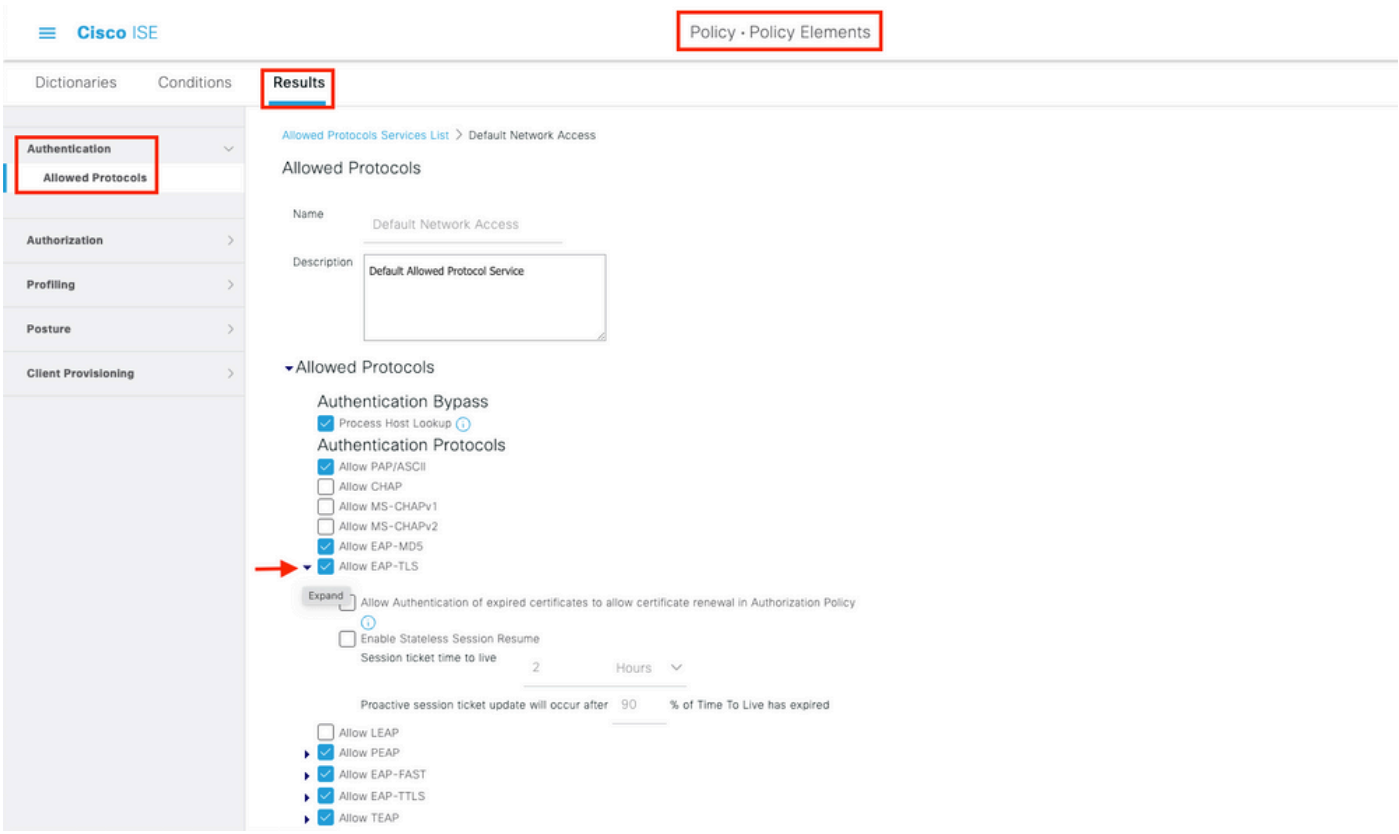


然后配置**身份验证策略和授权策略**。此处显示的策略是在ISE服务器上创建的默认策略，但可以根据需要进行修改和自定义。
在本示例中，配置可以转换为：“如果使用有线802.1X且用户在ISE服务器上已知，则我们允许访问身份验证成功的用户”。然后AP将根据ISE服务器获得授权。





第四步：确保在允许的“默认网络访问”协议中允许EAP-FAST。导航至Policy > Policy Elements > Authentication > Results > Allowed Protocols > Default Network Access > Enable EAP-TLS > Save。



验证

使用本部分可确认配置能否正常运行。

验证身份验证类型

show命令显示AP配置文件的身份验证信息：

CLI：

```
9800WLC#show ap profile name <profile-name> detailed
```

示例：

```
9800WLC#show ap profile name default-ap-profile detailed
 AP Profile Name        : Dot1x
```

```
 …
 Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
 LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

验证交换机端口上的802.1x

show命令显示交换机端口上802.1x的身份验证状态：

CLI：

```
Switch# show dot1x all
```

输出示例：

```
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for GigabitEthernet0/8
----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

验证端口是否已进行身份验证

CLI：

```
Switch#show dot1x interface <AP switch port number> details
```

输出示例：

```
Dot1x Info for GigabitEthernet0/8
----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
EAP Method                = FAST
Supplicant                = f4db.e67e.dd16
Session ID                = 0A30279E00000BB7411A6BC4
   Auth SM State         = AUTHENTICATED
   Auth BEND SM State    = IDLE
ED
Auth BEND SM State = IDLE
```

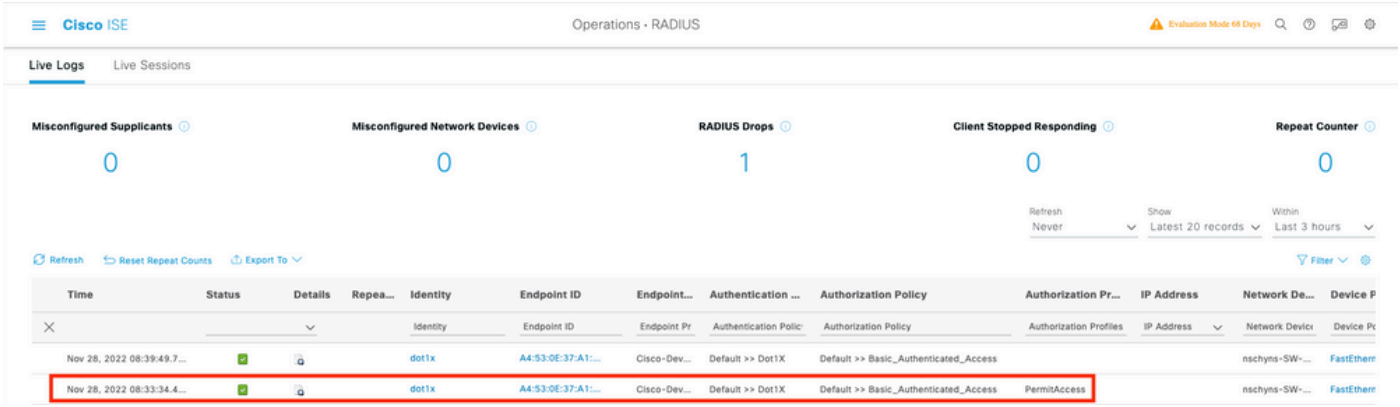
从CLI:

```
Switch#show authentication sessions
```

输出示例：

```
Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi0/8        f4db.e67e.dd16 dot1x   DATA    Auth      0A30279E00000BB7411A6BC4
```

在ISE中，选择**Operations > Radius Livelogs**，并确认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ISE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，且ISE服务器上的凭证相同。
   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**。

请注意，基于Cisco IOS的接入点(802.11ac wave 1)不支持TLS版本1.1和1.2。如果ISE或RADIUS服务器配置为仅允许802.1X内部的TLS 1.2身份验证，则可能导致问题。

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）。