配置与PEAP、ISE 2.1和WLC 8.3的802.1x验证

目录

简介

本文描述如何设置一个无线局域网(WLAN)以802.1x安全和与Protected Extensible Authentication Protocol (PEAP)的虚拟局域网覆盖作为可扩展的认证协议(EAP)。

先决条件

要求

Cisco 建议您了解以下主题：

- 802.1x
- PEAP
- 认证机构(CA)
- 证书

使用的组件

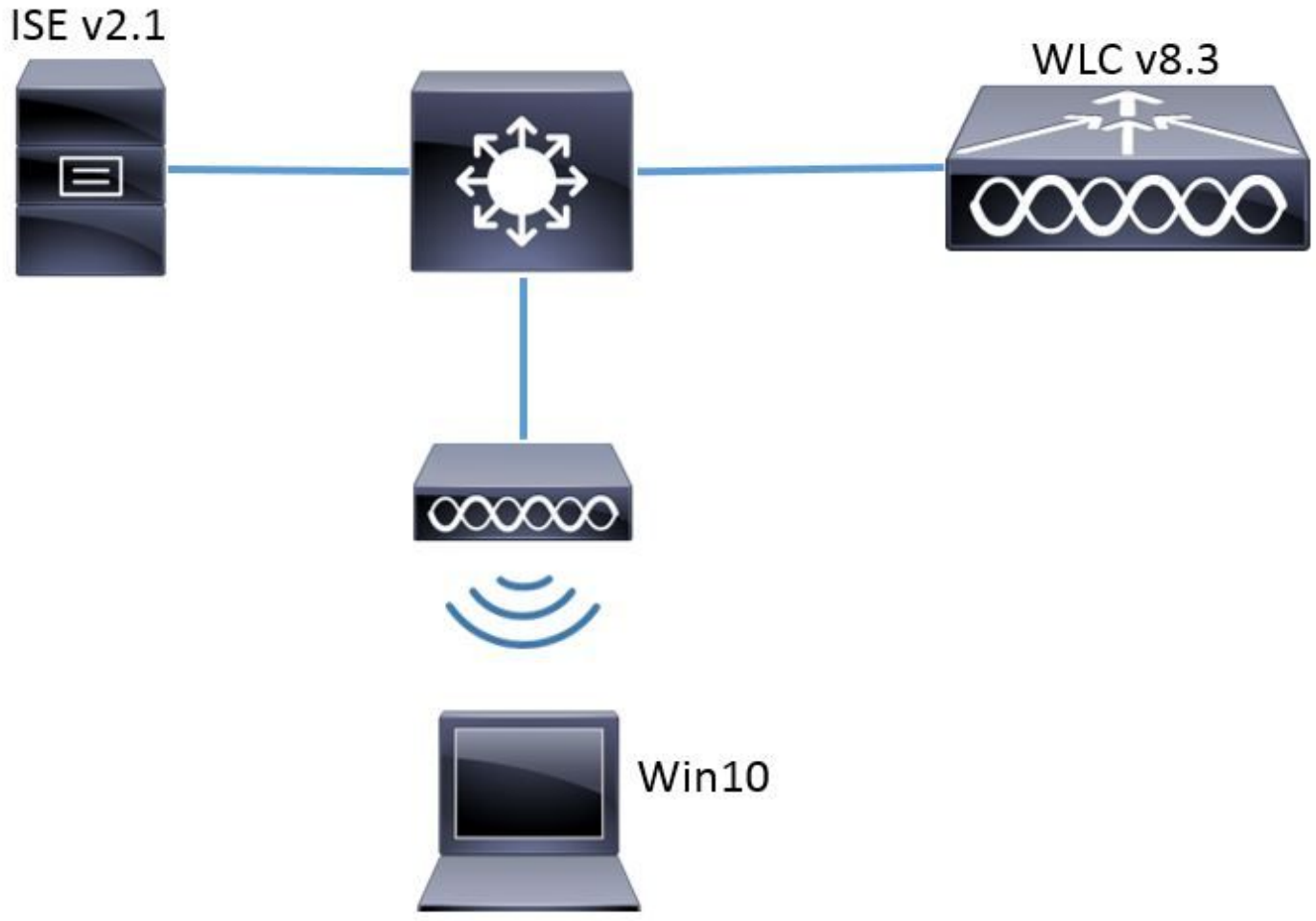
本文档中的信息基于以下软件和硬件版本：

- WLC v8.3.102.0
- 身份服务引擎(ISE) v2.1
- Windows 10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。

配置

网络图



配置

一般步骤是：

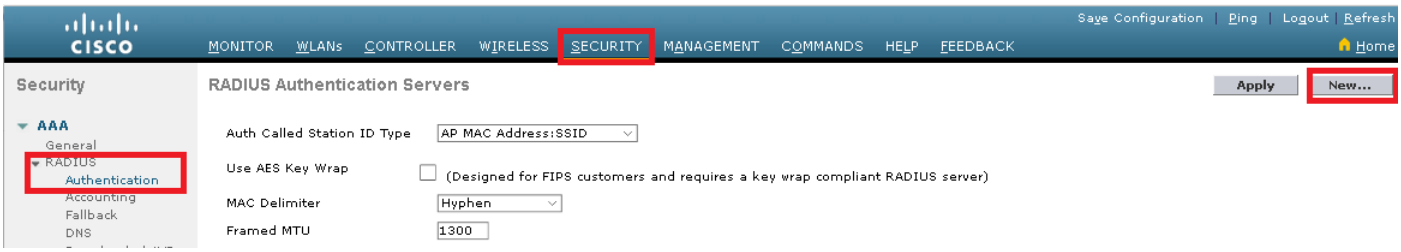
1. 指定在WLC的RADIUS服务器反之亦然允许彼此的通信。
2. 创建在WLC的服务集标识(SSID)。
3. 创建在ISE的验证规则。
4. 创建在ISE的授权配置文件。
5. 创建在ISE的授权规则。
6. 配置终端。

指定在WLC的RADIUS服务器

为了允许RADIUS服务器和WLC之间的通信，它是需要的注册在WLC的RADIUS服务器反之亦然。

GUI ：

步骤1.如镜像所显示，打开WLC的GUI并且导航对**SECURITY>RADIUS >验证>New。**



步骤2.如镜像所显示，输入RADIUS服务器信息。

CLI ：

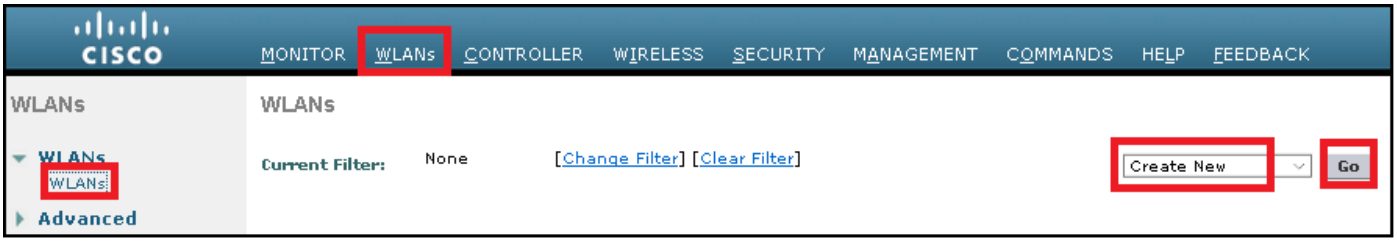
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

<a.b.c.d>对应于RADIUS服务器。

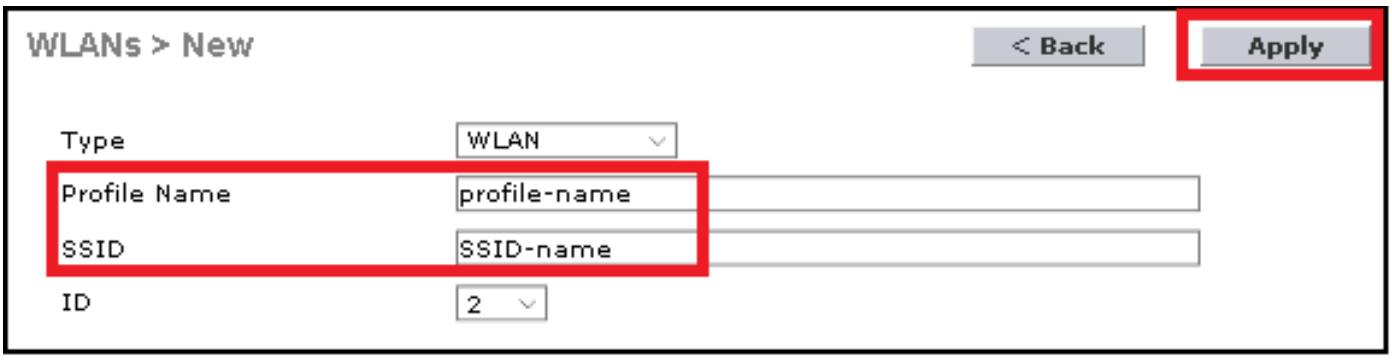
创建SSID

GUI ：

步骤1.如镜像所显示，打开WLC的GUI并且导航对**WLAN >创建新>去。**



步骤2.如镜像所显示，选择一名称对于SSID和配置文件，然后单击**应用**。



CLI ：

```
> config wlan create <id> <profile-name> <ssid-name>
```

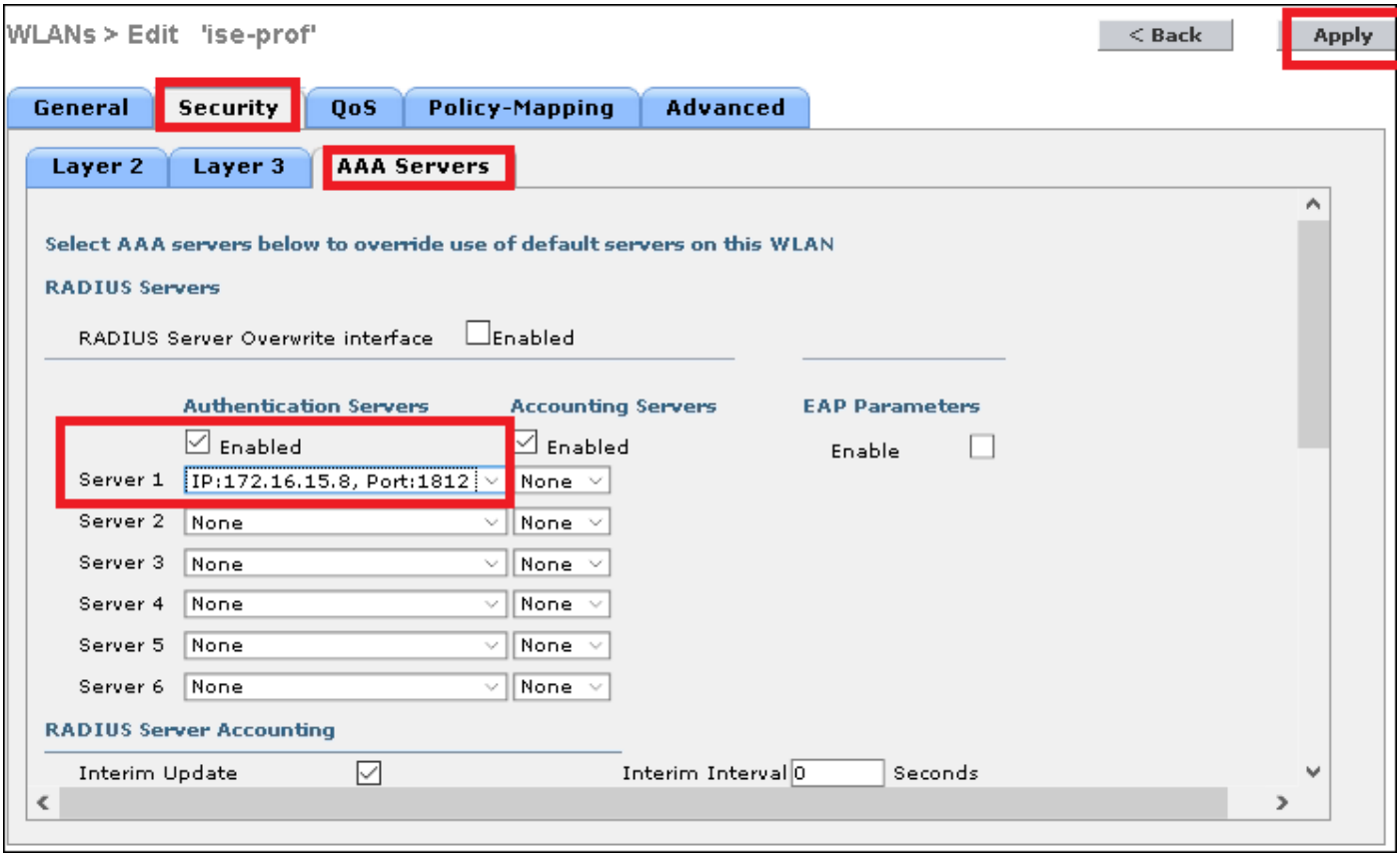
步骤3.分配RADIUS服务器到WLAN。

CLI ：

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI ：

导航到**安全>AAA服务器**并且选择希望的RADIUS服务器，如镜像所显示，然后命中数**应用**。



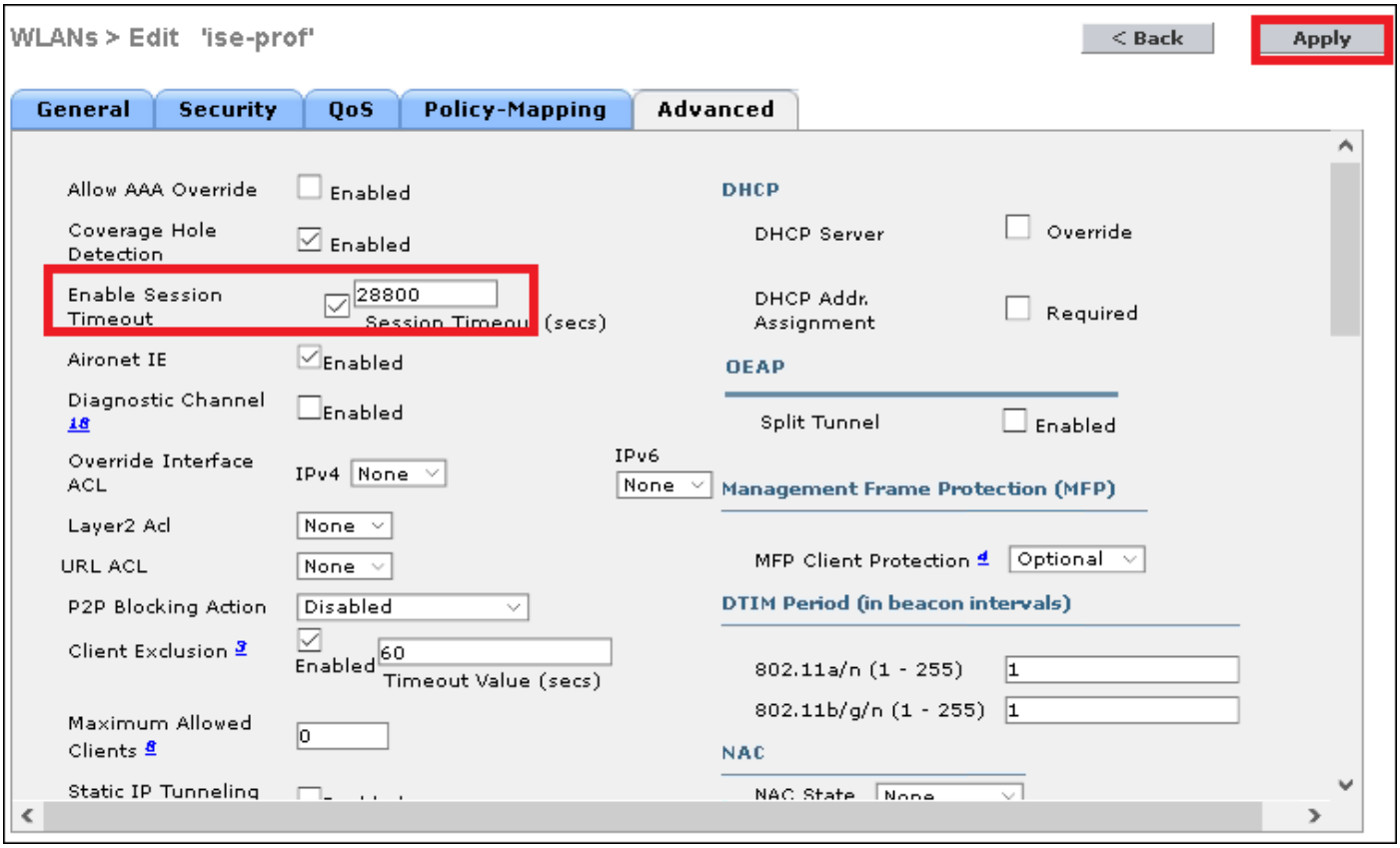
步骤4.随意地请增加会话超时

CLI ：

```
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI ：

如镜像所显示，导航对**WLAN >提前的WLAN ID>**并且指定会话超时。



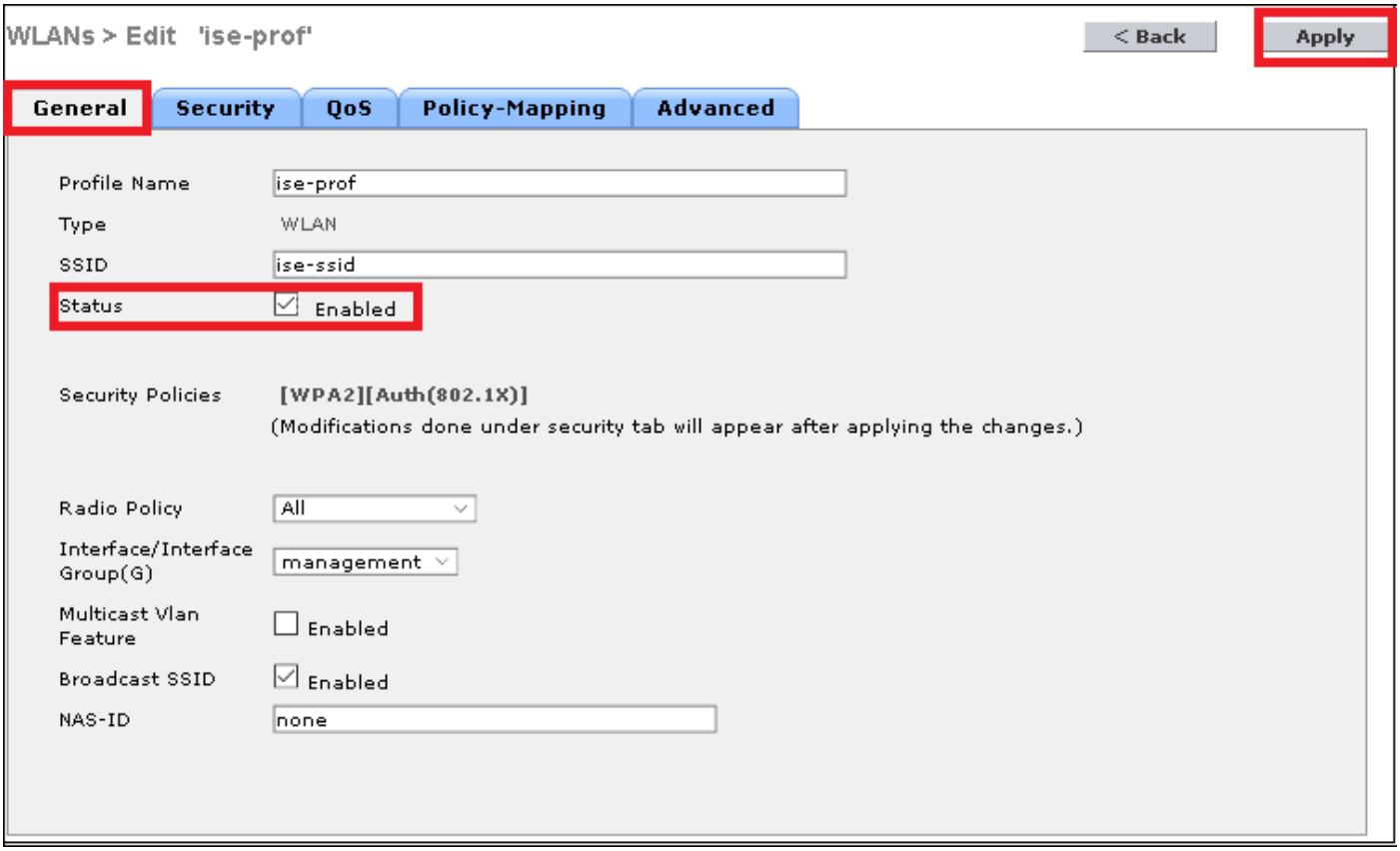
步骤5.启用WLAN。

CLI ：

```
> config wlan enable <wlan-id>
```

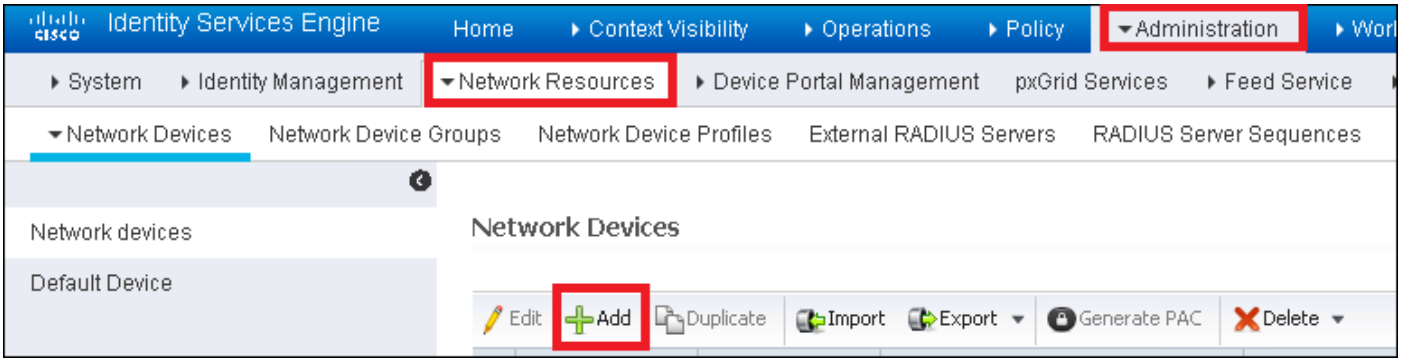
GUI ：

如镜像所显示，导航对**WLAN > WLAN ID>常规**并且启用SSID。



宣称在ISE的WLC

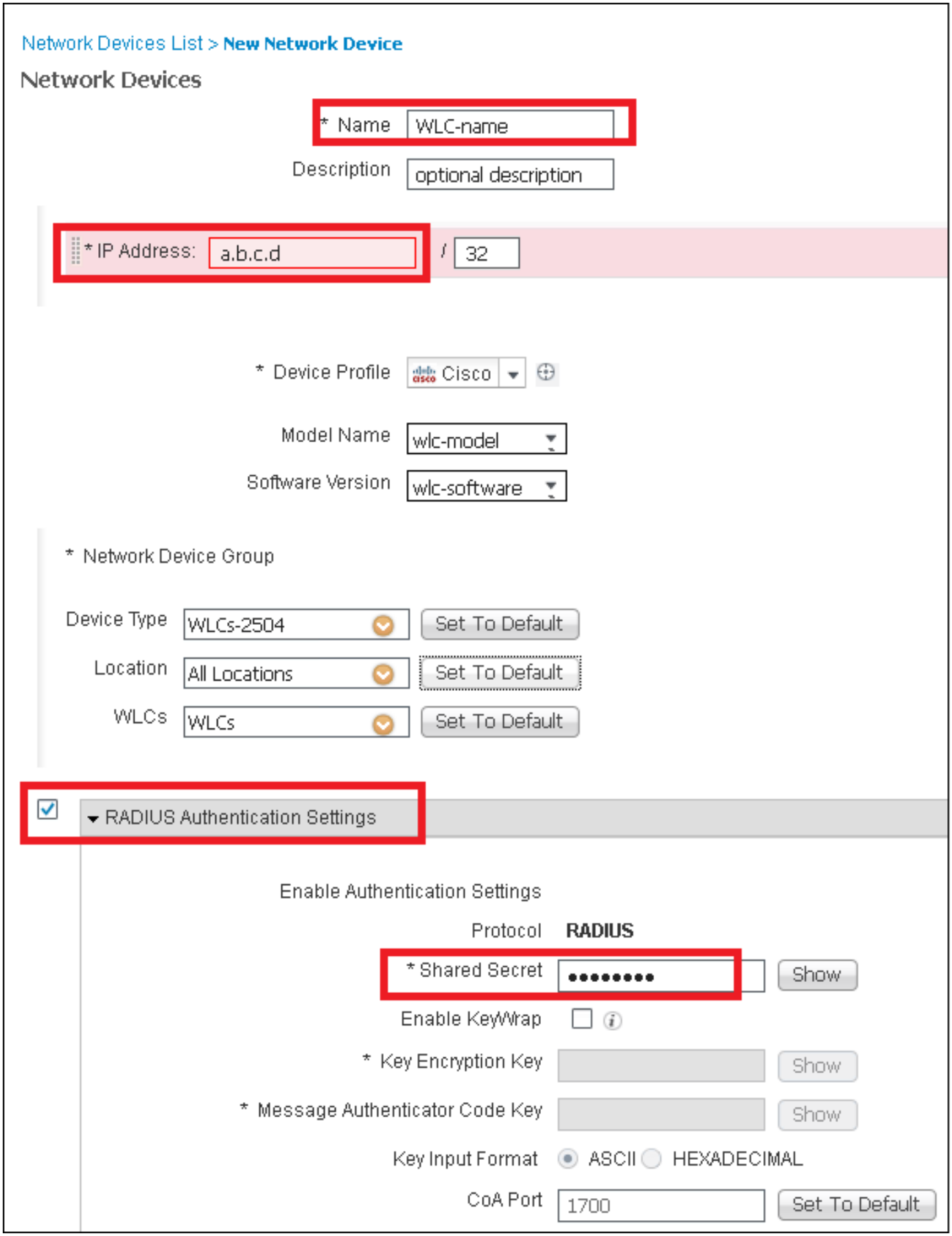
步骤1.如镜像所显示，开放ISE控制台和导航对**Administration >网络资源>网络设备>Add**。



步骤2.输入值。

随意地，它能是一指定的模型名称，软件版本，说明和分配根据设备类型、位置或者WLCs的网络设备组。

a.b.c.d对应于发送验证请求的WLC's接口。如镜像所显示，默认情况下它是管理接口。

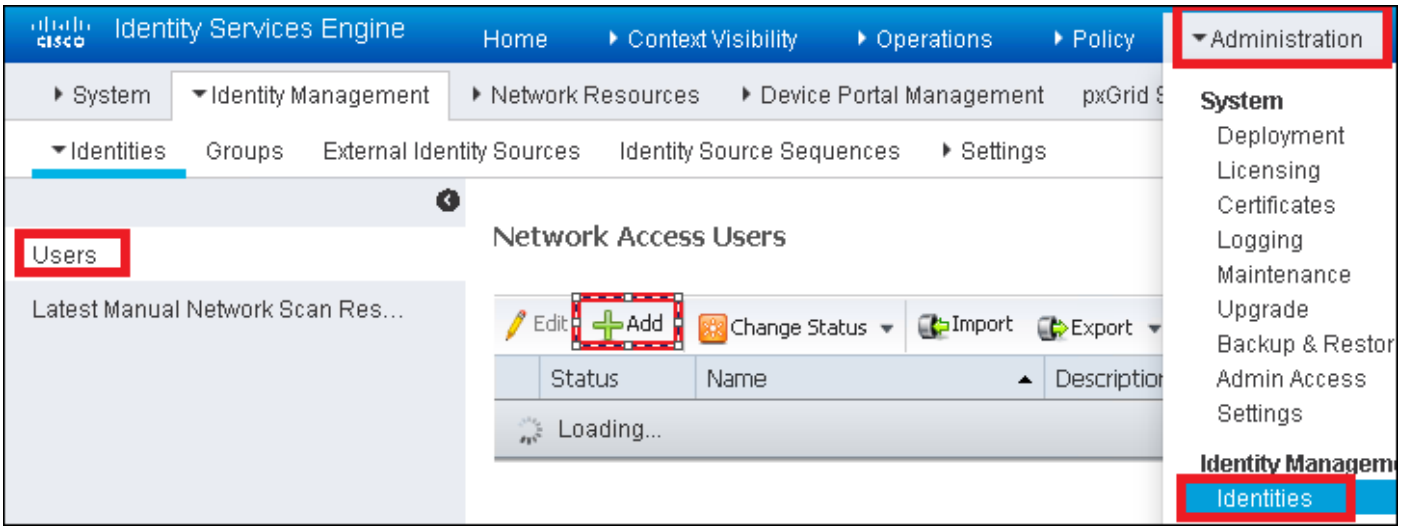


关于**网络设备组的更多信息请**查看此链路：

[ISE -网络设备组]

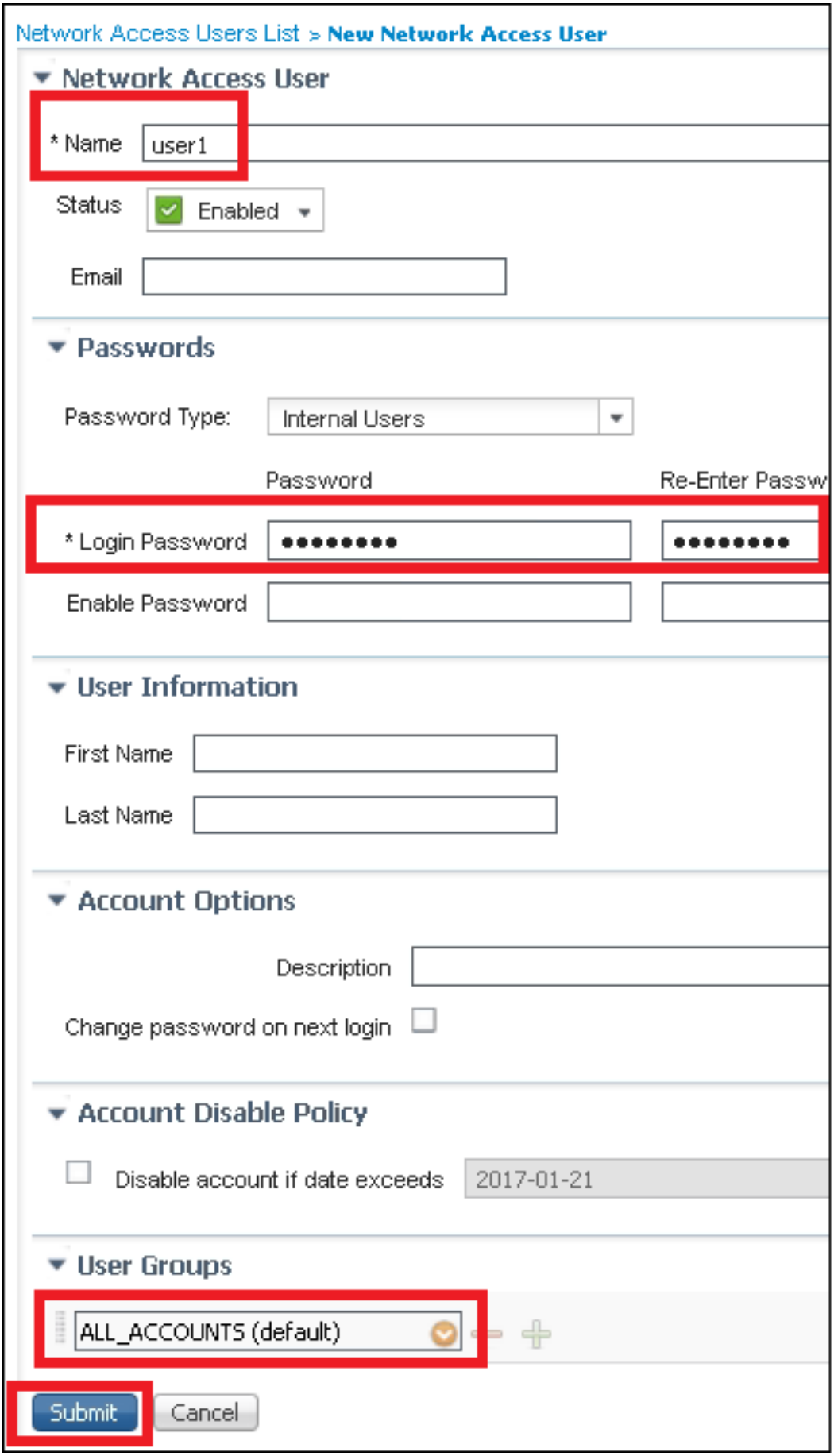
创建ISE的新用户

步骤1.如镜像所显示，导航对**Administration >身份管理>标识> Users >Add**。



步骤2.输入信息。

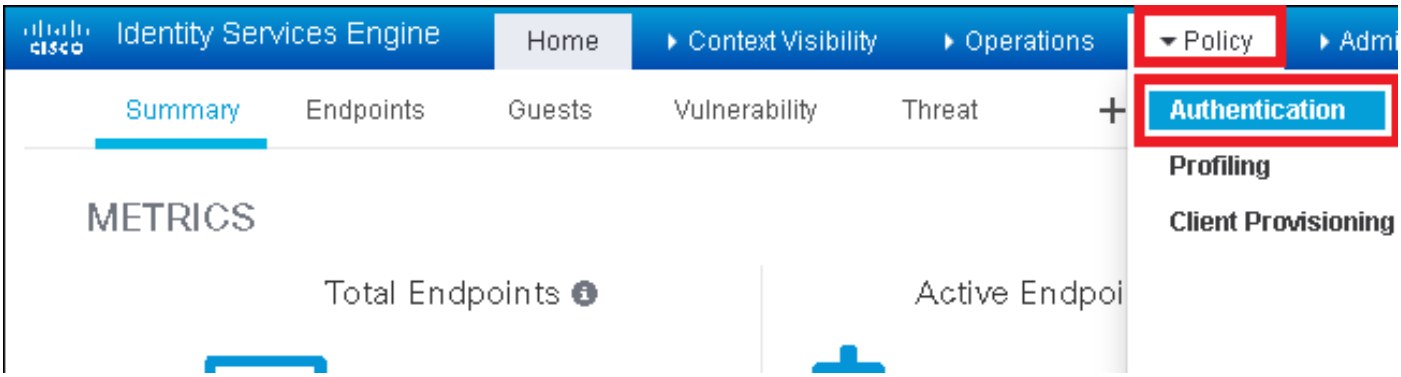
在本例中，此用户属于组呼叫ALL_ACCOUNTS如镜像所显示，但是可以调节作为需要。



创建验证规则

验证规则用于验证，如果用户的凭证是合适的(请验证，如果用户确实是谁说是)和限制允许由它使用的认证方法。

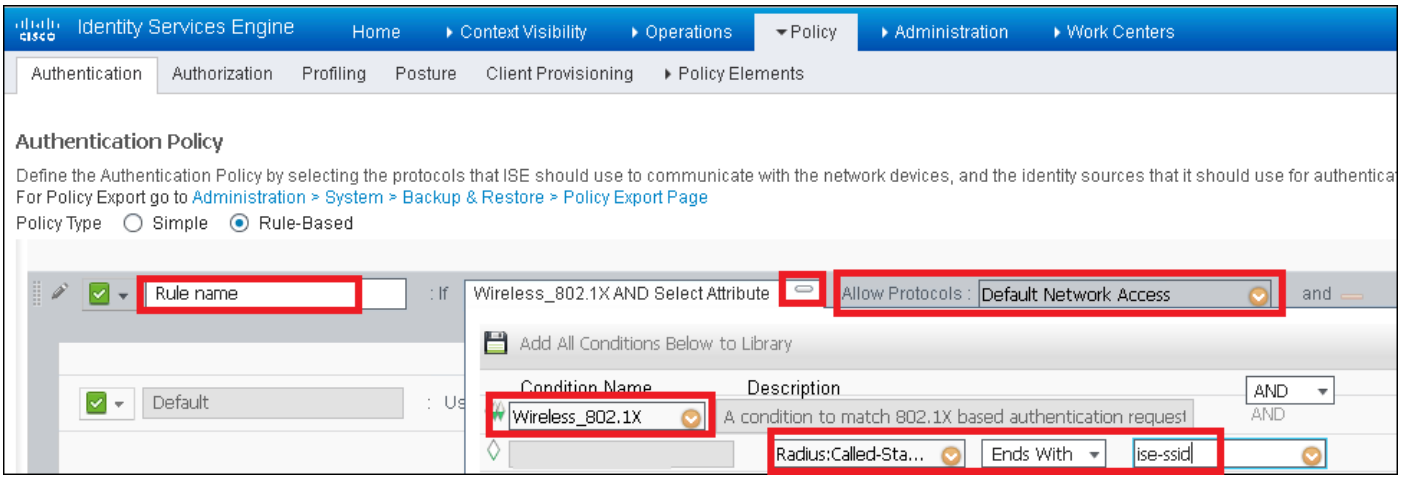
步骤1.如镜像所显示，导航对**策略>验证**。



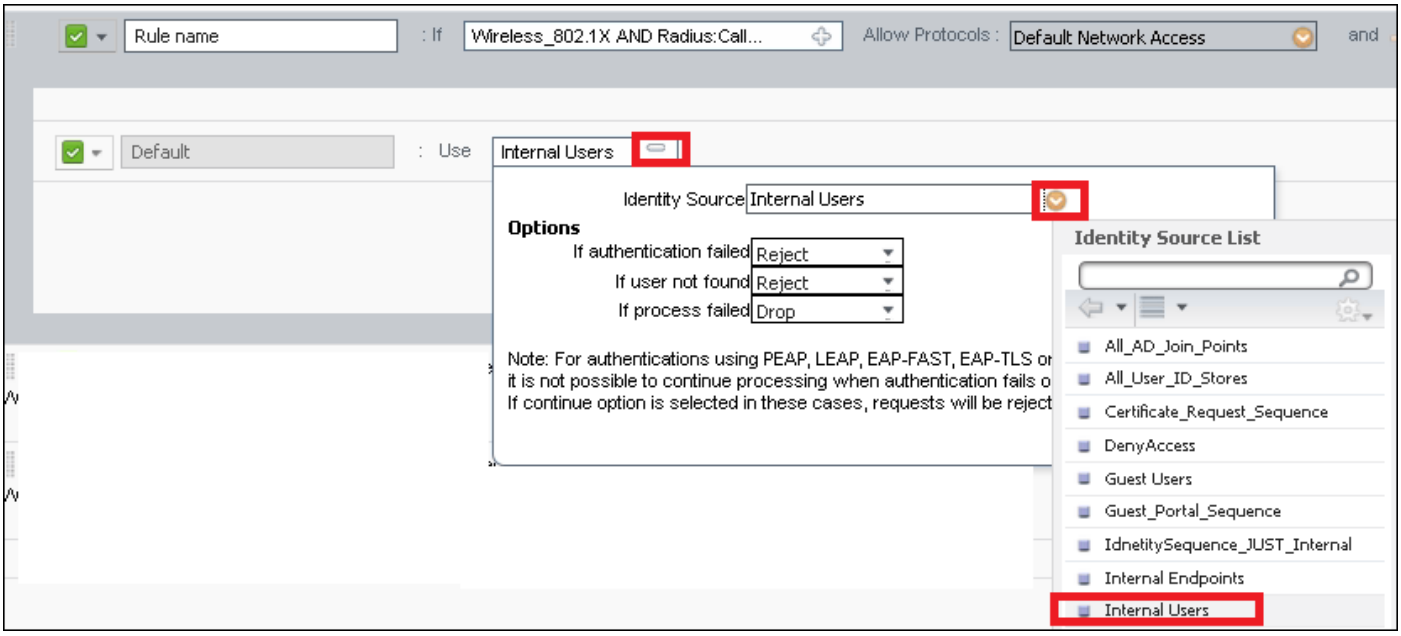
步骤2.如镜像所显示，插入新证书规则。

步骤3.输入值。

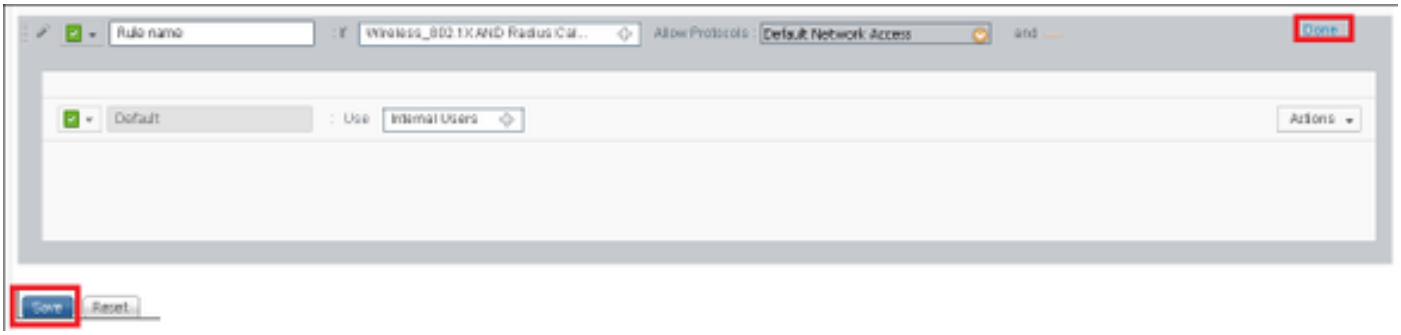
此验证规则允许所有协议列出在**默认网络访问列表下**，如镜像所显示，这适用于认证请求为无线802.1x客户端和与被呼叫状态ID和末端与ISE **ssid**。



并且，请选择匹配此验证规则客户端的标识来源。如镜像所显示，此示例使用**内部用户**标识源列表。



如镜像所显示，一旦完成，请单击**完成**和**"Save"**。



关于的更多信息请允许策略参见此链路的协议：

[允许协议服务]

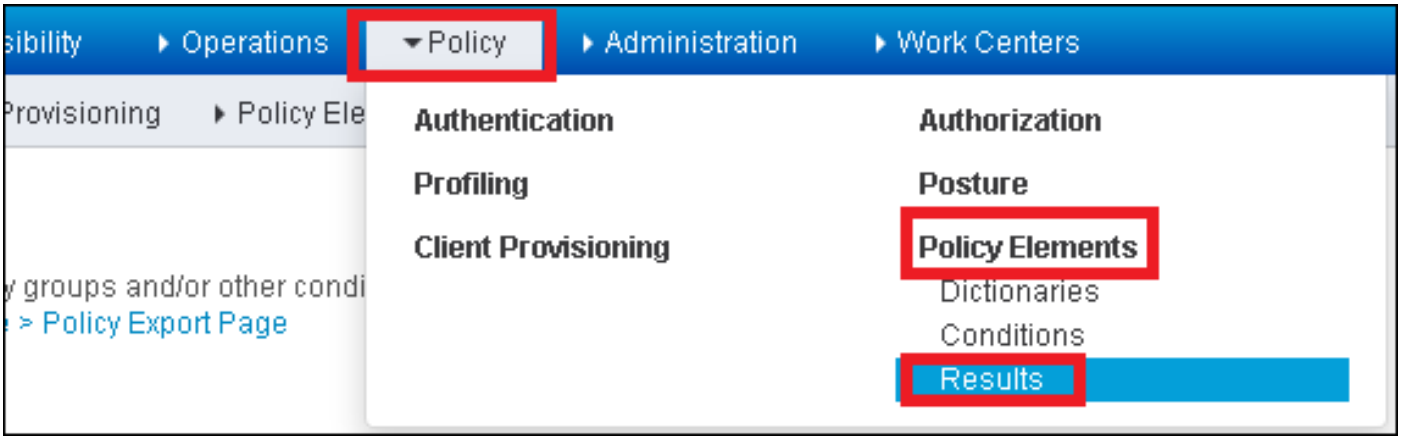
关于标识的更多信息来源参见此链路：

[创建用户标识组]

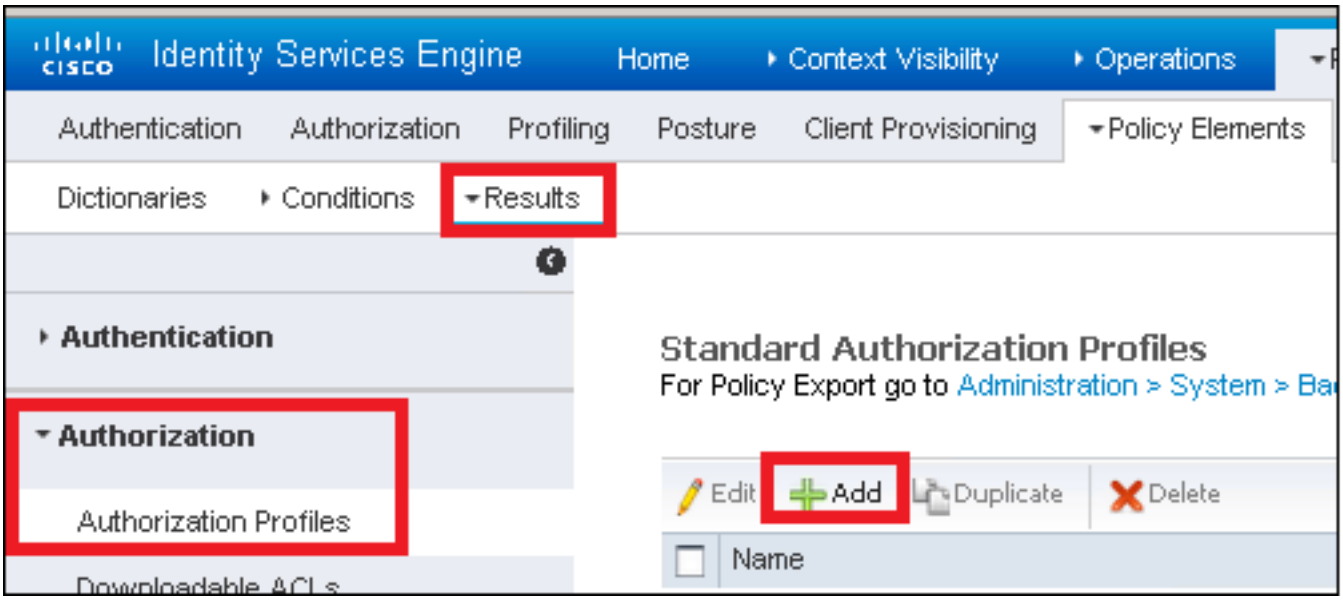
创建授权配置文件

授权配置文件确定客户端是否访问或不网络、推送访问控制列表(ACL)、VLAN覆盖或者其他参数。在本例中显示的授权配置文件发送访问为客户端接受并且分配客户端到VLAN 2404。

步骤1.如镜像所显示，导航对**策略>Policy元素>结果**。



步骤2.添加一新的授权配置文件。如镜像所显示，导航对**授权>授权Profiles>添加**。



步骤3.如镜像所显示，输入值。