用PEAP、ISE 2.1和WLC 8.3配置802.1x认证

Contents

Introduction

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)。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 802.1x
- PEAP
- 认证机构(CA)
- 证书

Components Used

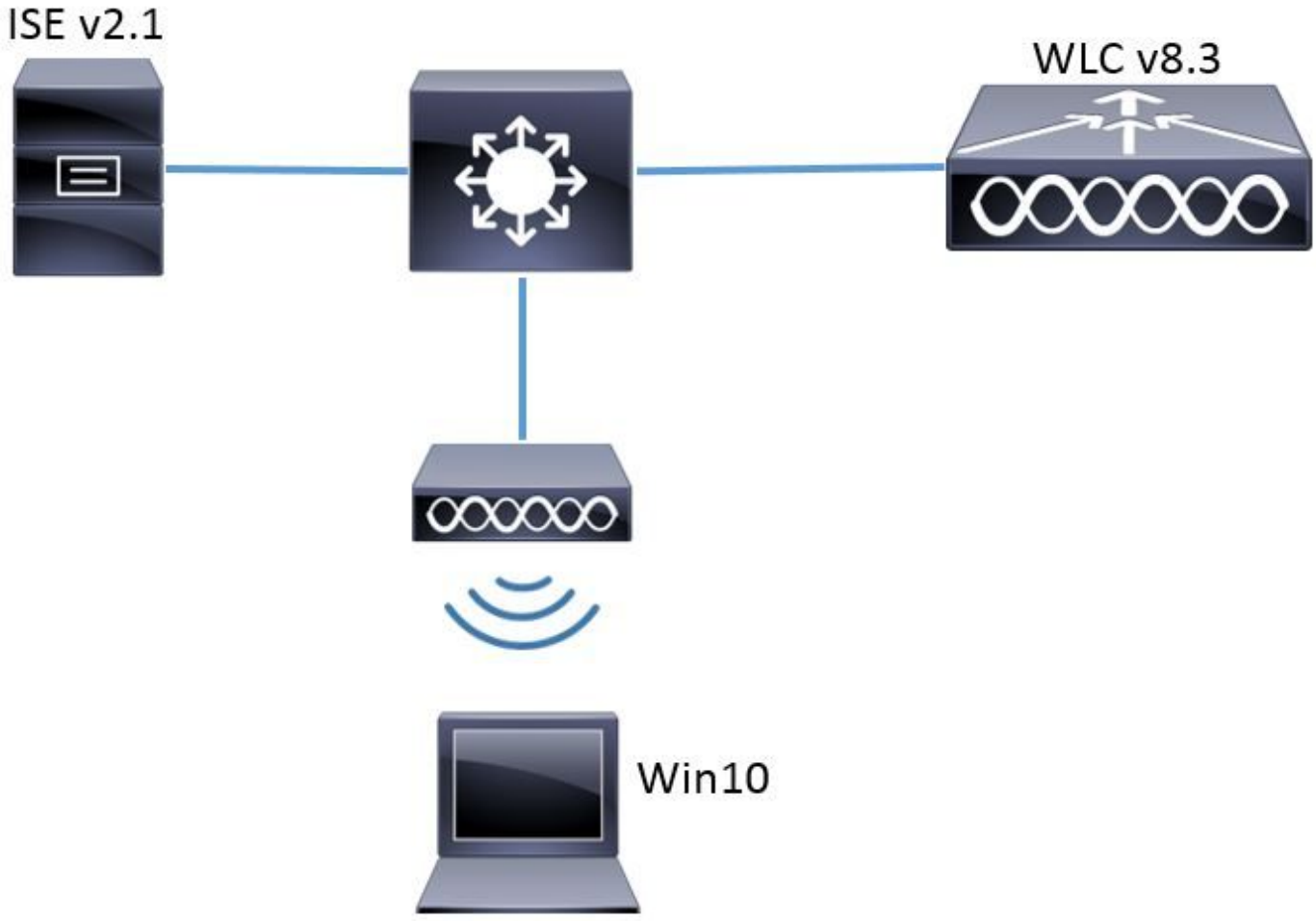
本文档中的信息基于以下软件和硬件版本：

- WLC v8.3.102.0
- 身份服务引擎(ISE) v2.1
- Windows 10膝上型计算机

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Configure

Network Diagram



配置

一般步骤是：

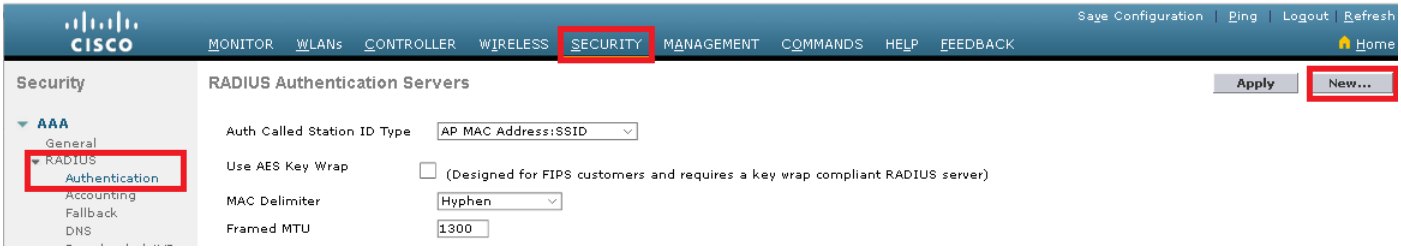
1. 指定在WLC的RADIUS服务器反之亦然允许彼此的通信。
2. 创建在WLC的服务集标识(SSID)。
3. 创建在ISE的认证规则。
4. 创建在ISE的授权配置文件。
5. 创建在ISE的授权规则。
6. 配置终端。

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并且连接对**SECURITY>RADIUS >认证>New**。



步骤2.如镜像所显示，输入RADIUS服务器信息。

CLI ：

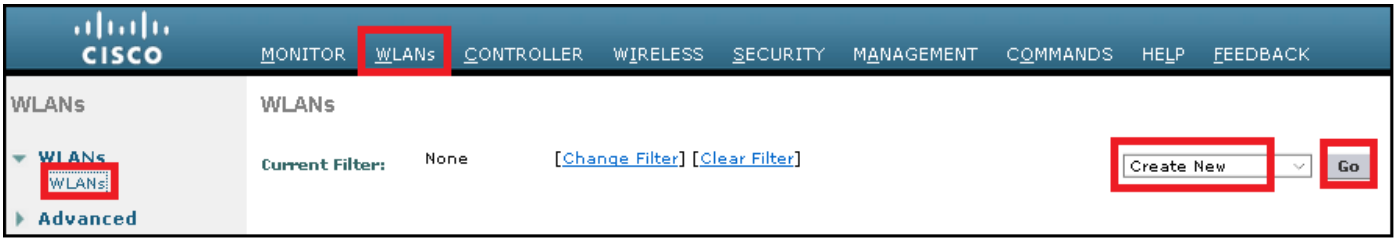
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

<a.b.c.d>对应于RADIUS服务器。

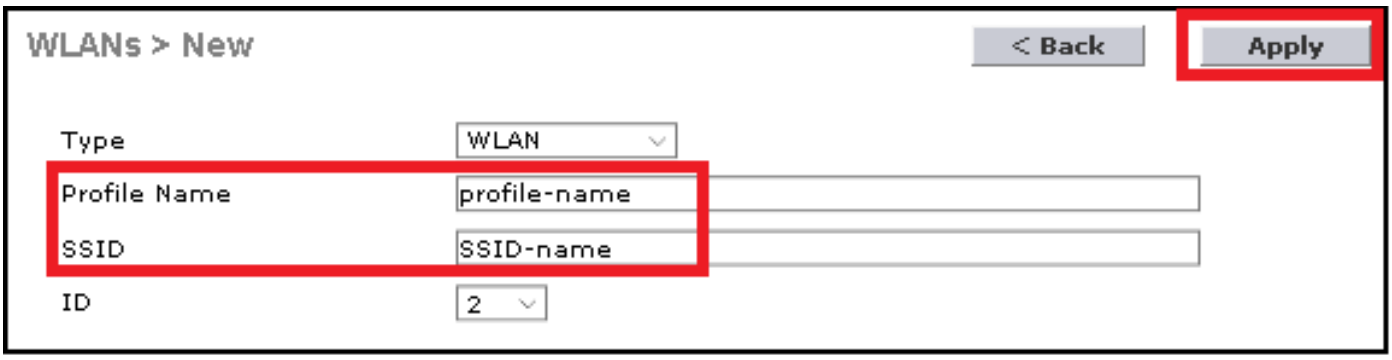
创建SSID

GUI ：

步骤1.如镜像所显示，打开WLC的GUI并且连接对**WLANs >创建新>去**。



步骤2.如镜像所显示，选择一个名字对于SSID和配置文件，然后点击**适用**。



CLI ：

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

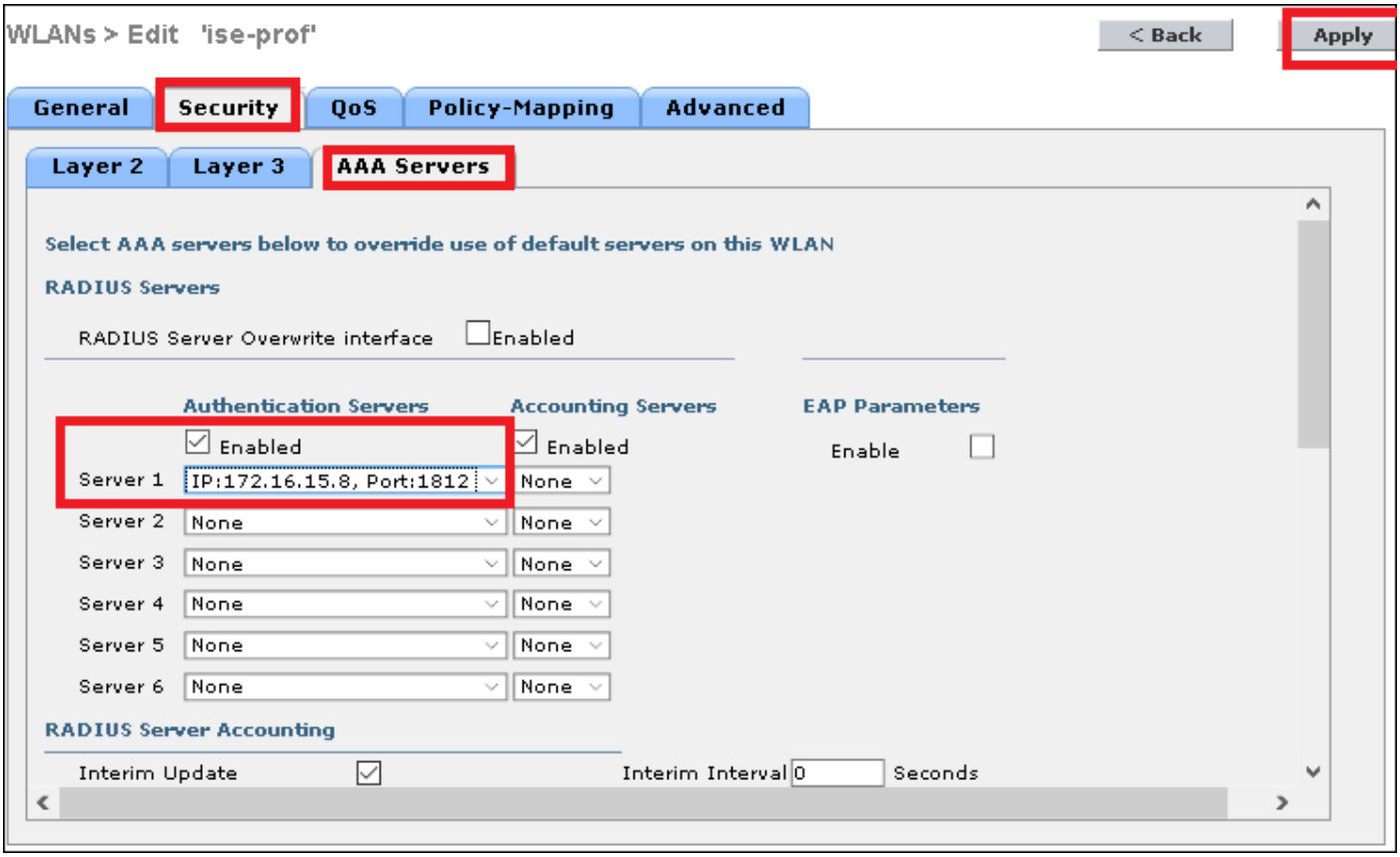
步骤3.分配RADIUS服务器到WLAN。

CLI ：

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

GUI ：

连接到**安全>AAA服务器**并且选择期望RADIUS服务器，如镜像所显示，然后命中**适用**。



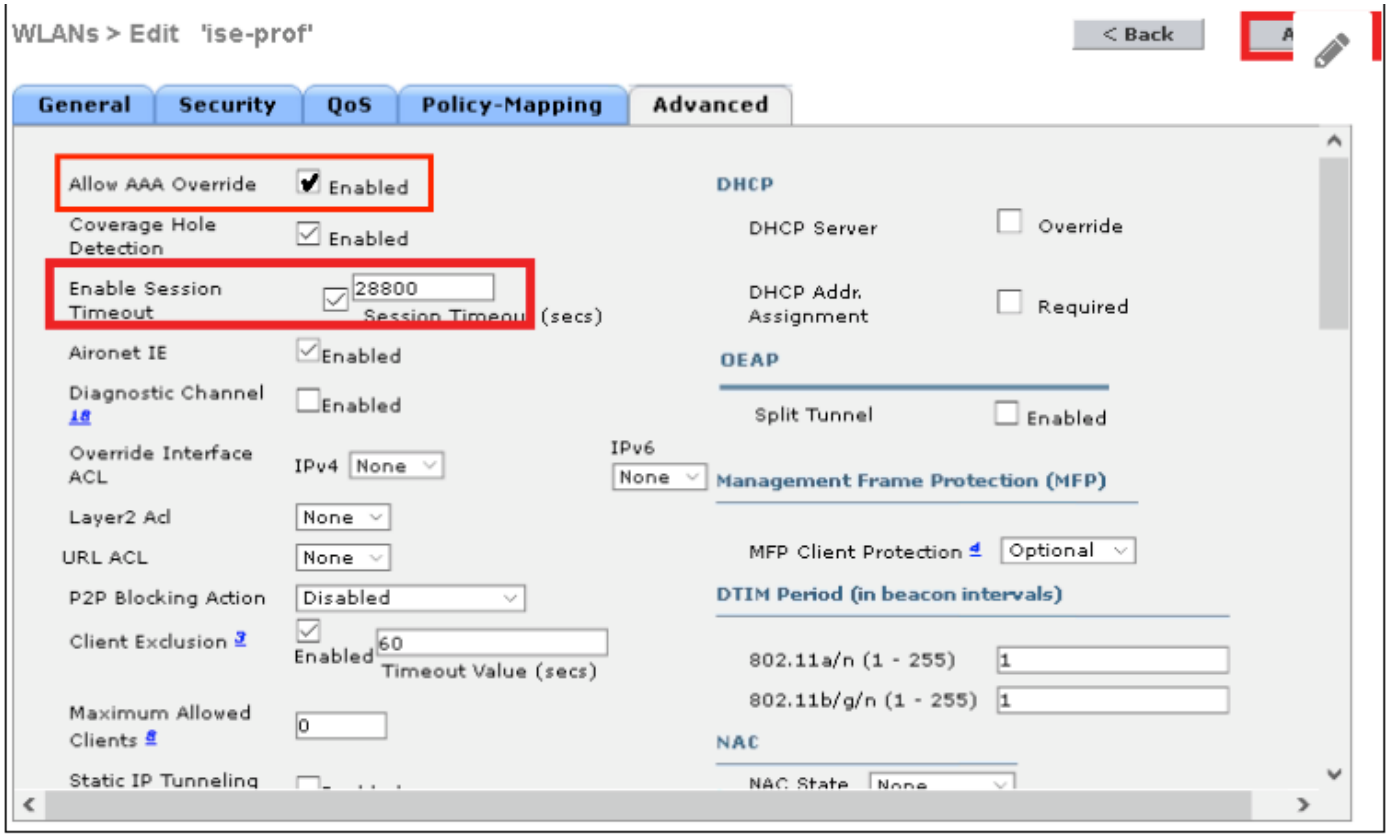
步骤4. Enable (event)**允许AAA覆盖**和可选地增加会话超时

CLI ：

```
> config wlan aaa-override enable <wlan-id>
>config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI ：

连接对**提前的WLANs > WLAN ID>**如镜像所显示，并且enable (event)**允许AAA覆盖**，可选地指定会话超时。



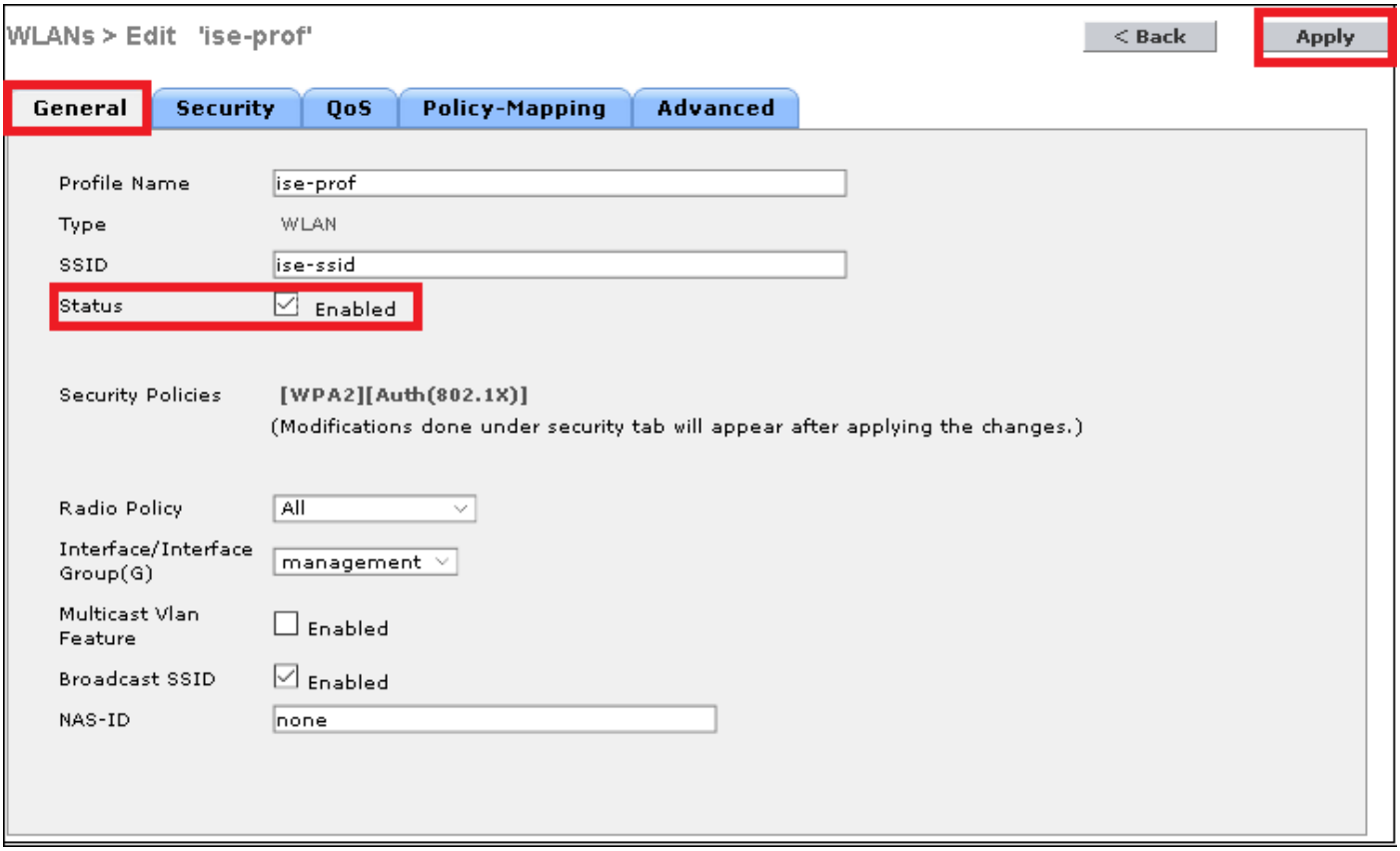
步骤5. Enable (event) WLAN。

CLI ：

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

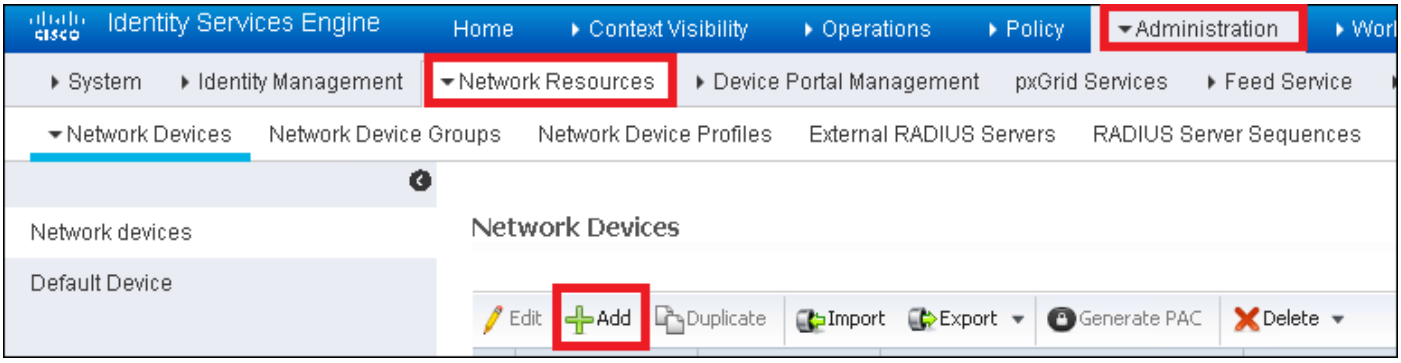
GUI ：

如镜像所显示，连接对**WLANs > WLAN ID>常规**和enable (event) SSID。



宣称在ISE的WLC

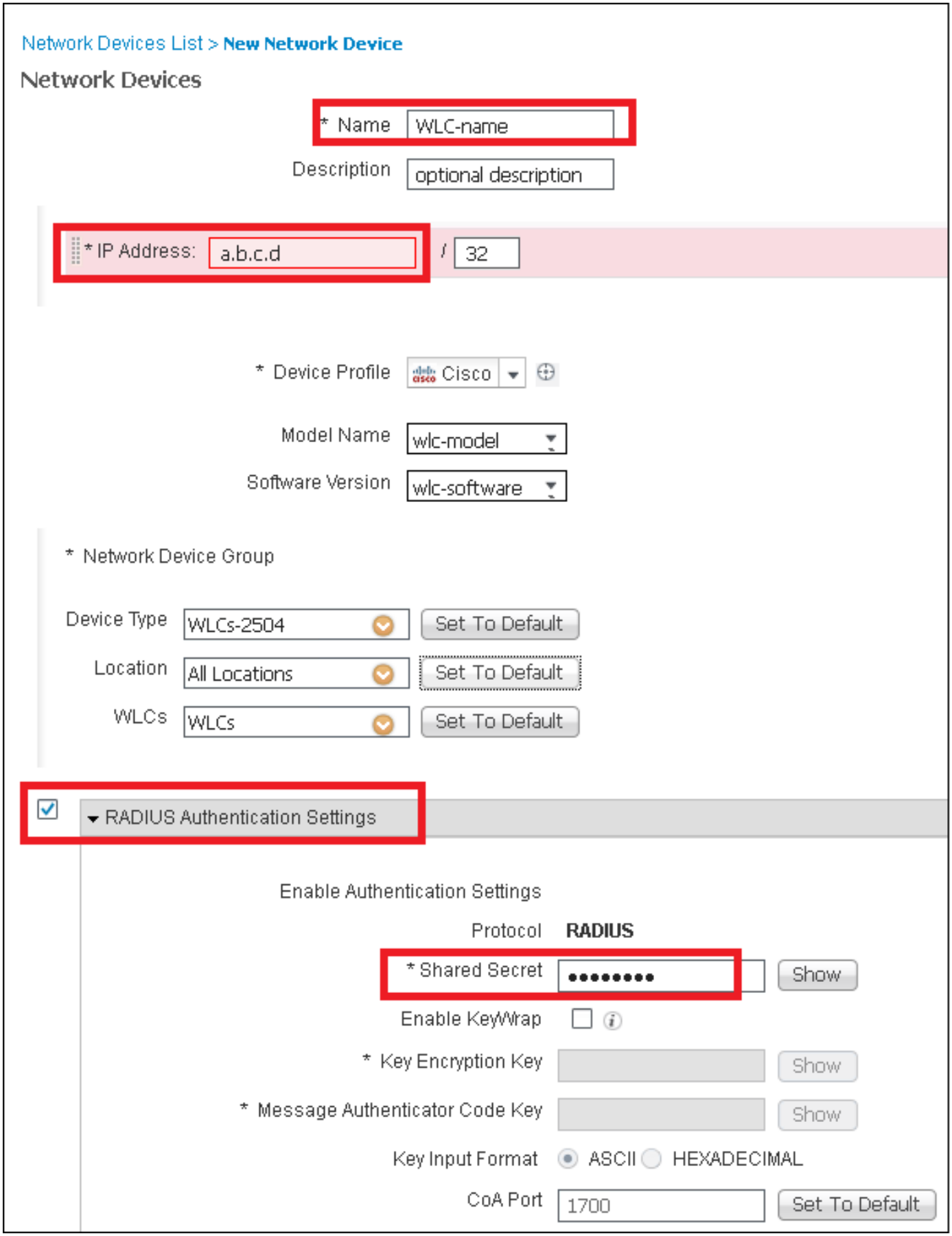
步骤1.如镜像所显示，打开ISE控制台并且连接对**Administration >网络资源>网络Devices > Add**。



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对应于发送被请求的认证的WLC's接口。如镜像所显示，默认情况下它是管理接口。

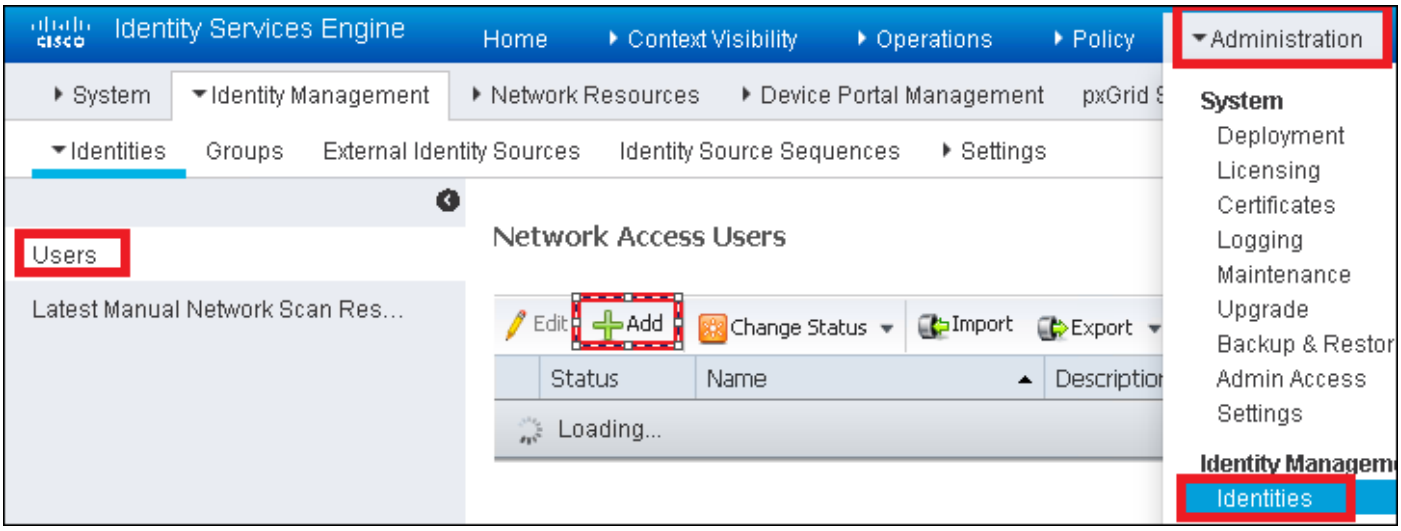


关于的更多信息**网络设备组**查看此链路：

[ISE -网络设备组]

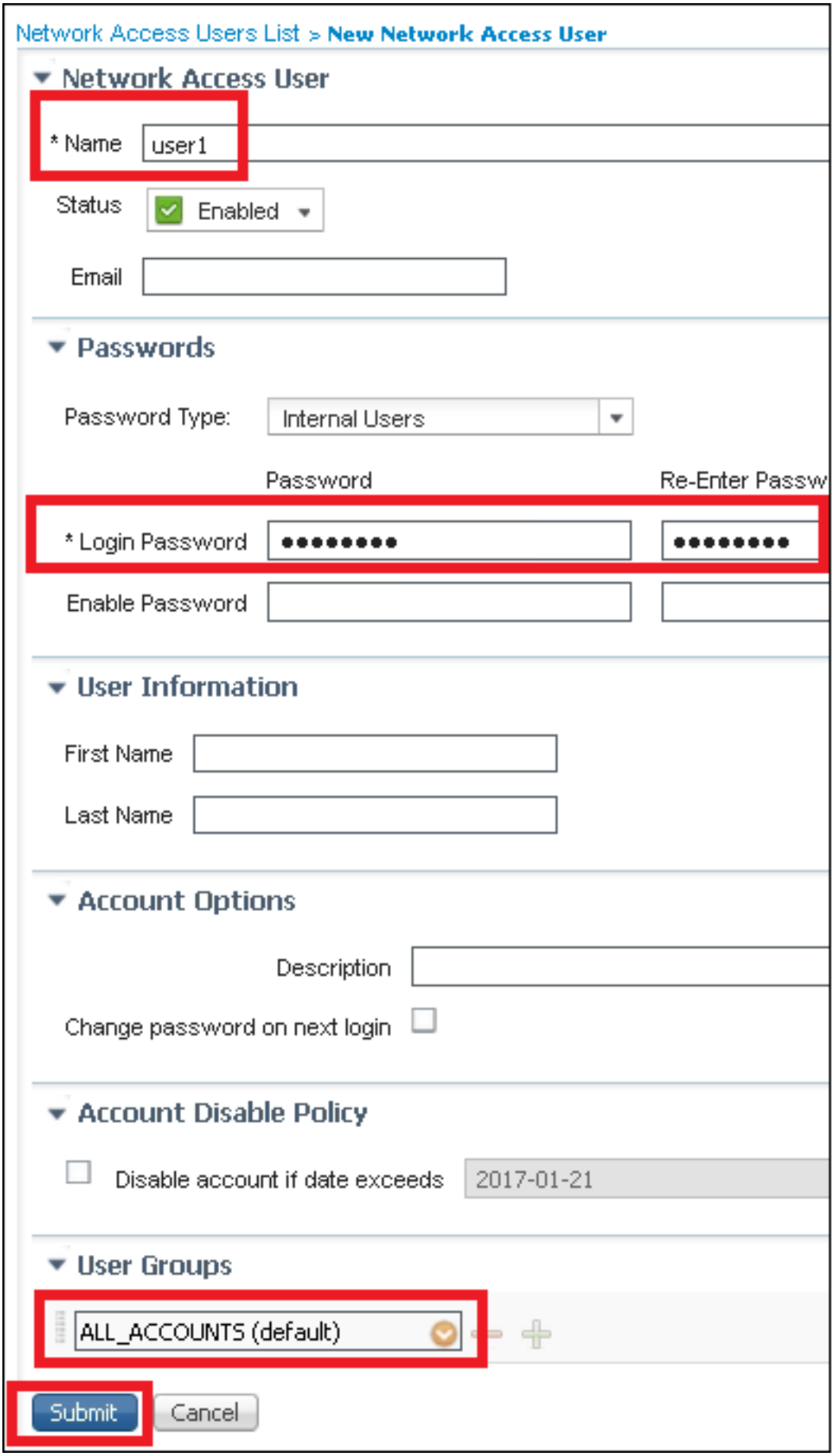
创建ISE的新用户

步骤1.如镜像所显示，连接对**Administration >身份管理>身份> Users >Add**。



步骤2.输入信息。

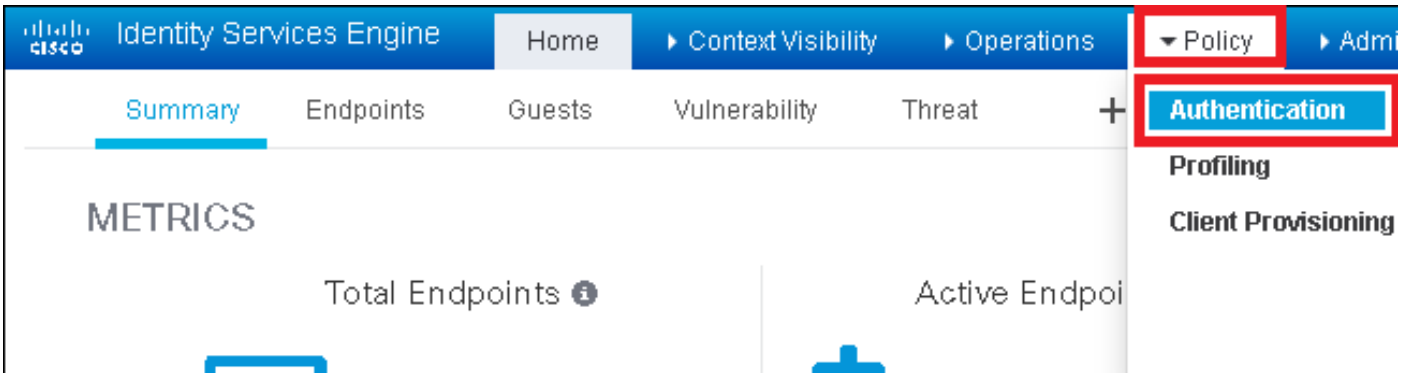
在本例中，此用户属于告诉ALL_ACCOUNTS的组，但是可以被调整当必要时如镜像所显示。



创建认证规则

认证规则用于验证用户的证件是否是合适的(请验证用户确实是否是谁说是)和限制允许由它使用的认证方法。

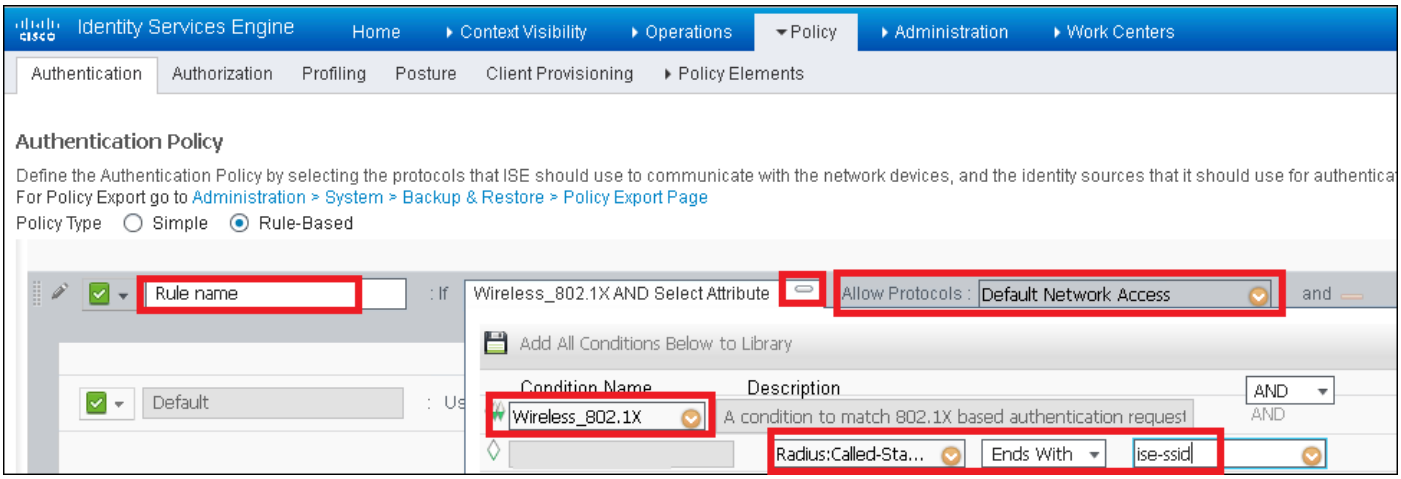
步骤1.如镜像所显示，连接对**策略>认证**。



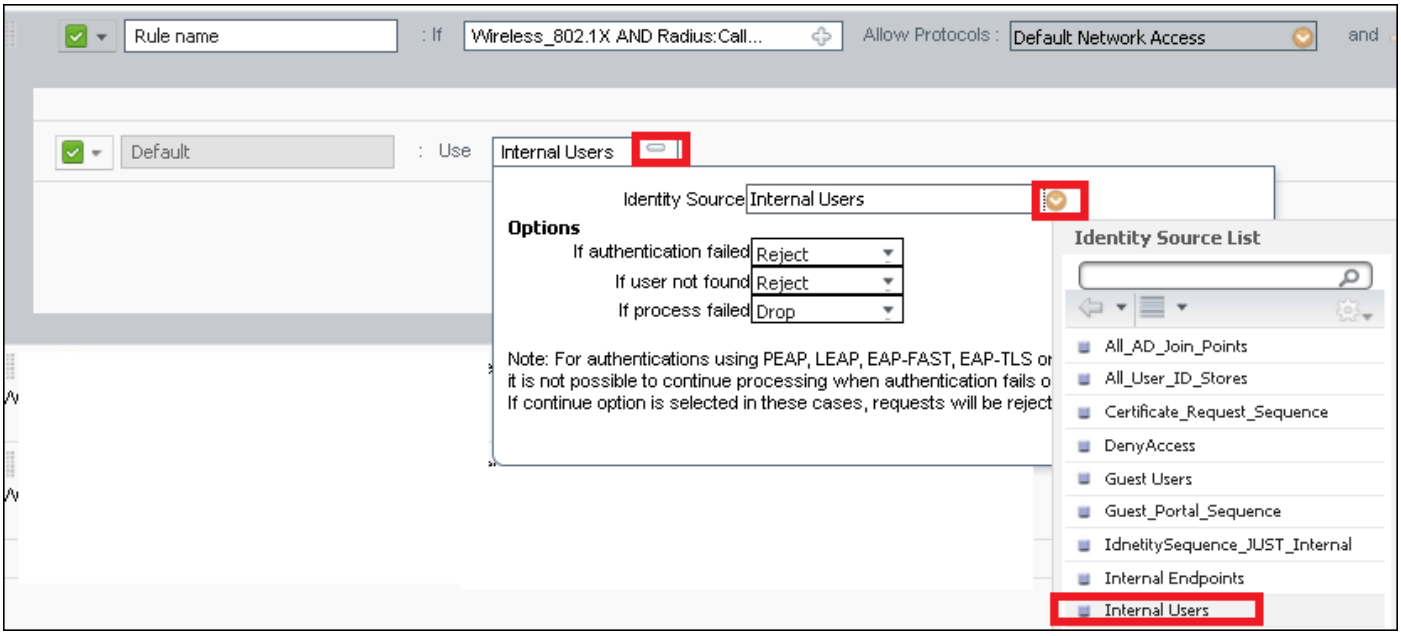
步骤2.如镜像所显示，插入新证书规则。

步骤3.输入值。

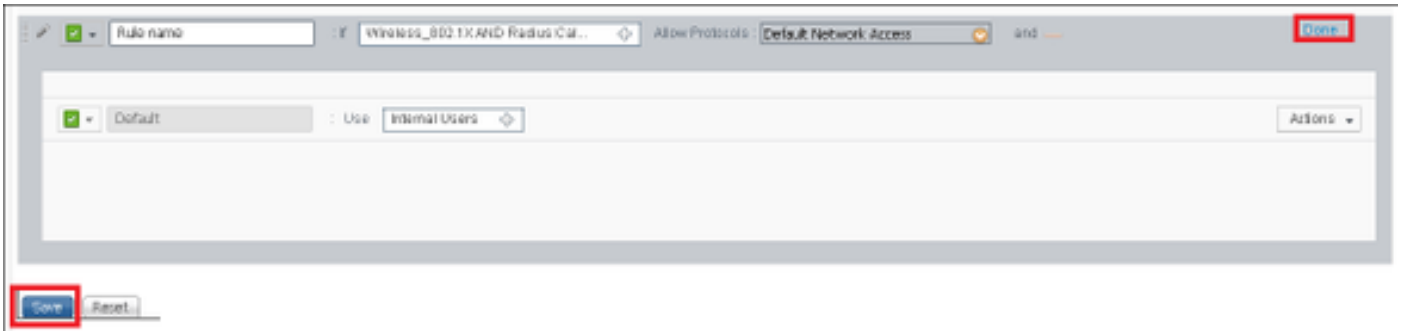
此认证规则允许所有协议列出在**默认网络访问列表下**，如镜像所显示，这适用于认证请求无线802.1x客户端的和与呼叫位置ID和末端与ISE **ssid**。



并且，请选择匹配此认证规则客户端的身份来源。如镜像所显示，此示例使用**内部用户**身份源列表。



如镜像所显示，一旦完成，请点击**执行**并且**保存**。



关于的更多信息请允许策略参见此链路的协议：

[允许的协议服务]

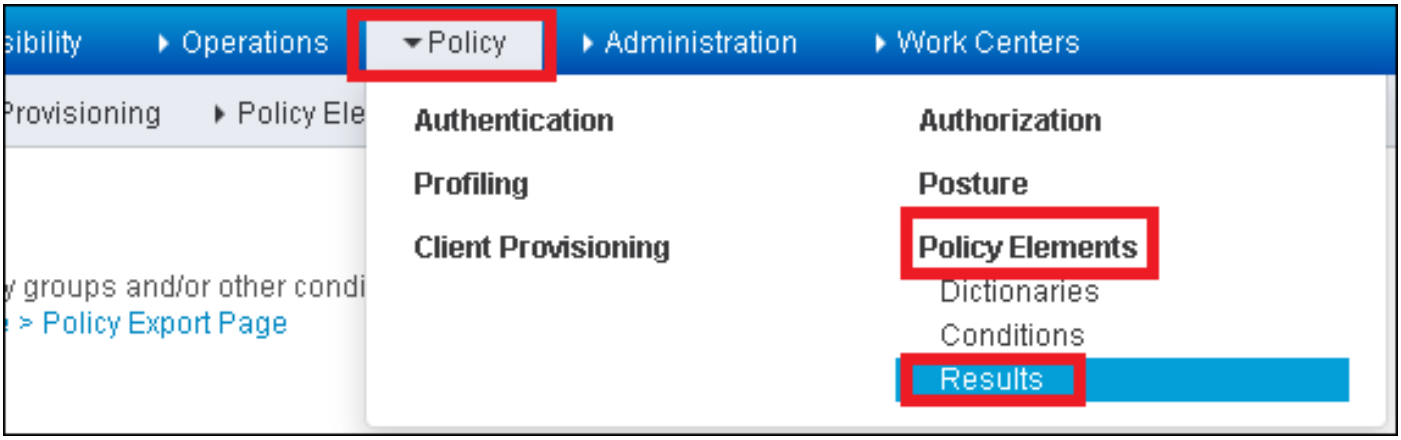
关于身份的更多信息来源参见此链路：

[创建一个用户身份组]

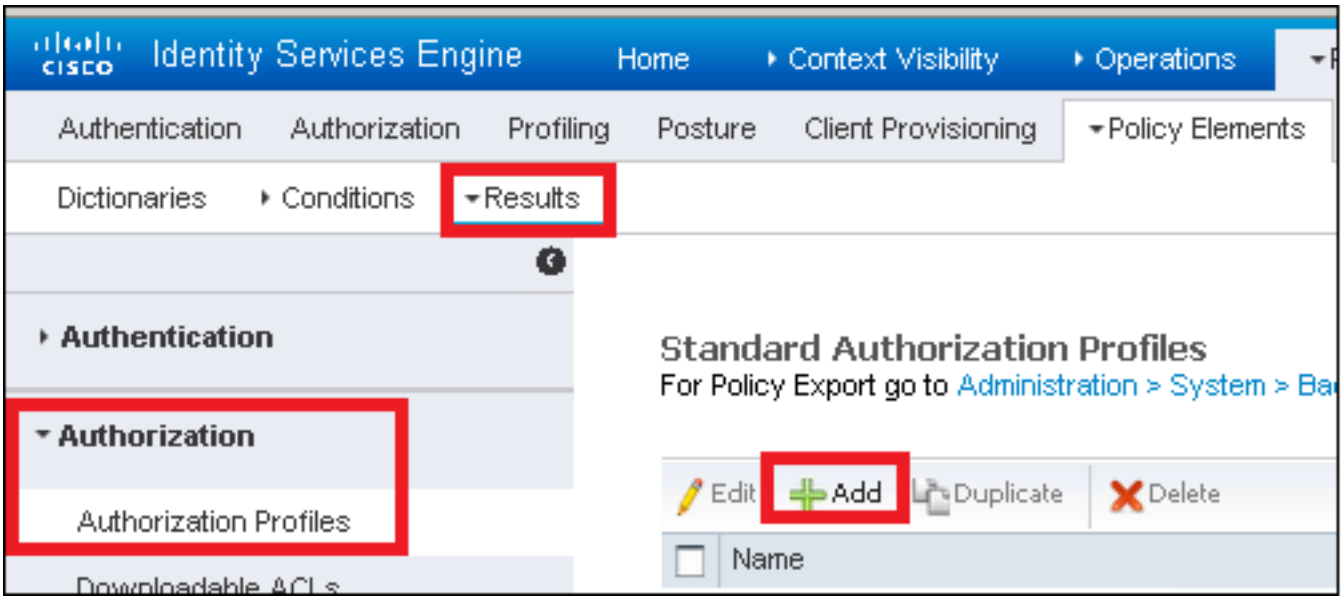
创建授权配置文件

授权配置文件确定客户端是否访问或不网络、推进访问控制列表(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一次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，连接对**策略>Policy元素>结果**。



步骤2.添加一个新的授权配置文件。如镜像所显示，连接对**授权>授权Profiles>添加**。



步骤3.如镜像所显示，输入值。