

# 与PEAP、ISE 2.1和WLC 8.3的802.1x验证

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[指定在WLC的RADIUS服务器](#)

[创建SSID](#)

[宣称在ISE的WLC](#)

[创建ISE的一个新用户](#)

[创建验证规则](#)

[创建授权配置文件](#)

[创建授权规则](#)

[终端设备的配置](#)

[验证](#)

[在WLC的认证过程](#)

[在ISE的认证过程](#)

## 简介

本文解释如何设置—WLAN (无线局域网)以802.1x安全和与PEAP (已保护可扩展的认证协议)的VLAN (虚拟局域网)覆盖作为EAP (可扩展的认证协议)。

## [先决条件](#)

思科推荐有基础知识：

- 802.1x
- PEAP
- 认证机构(CA)
- 证书

## [要求](#)

### 使用的组件

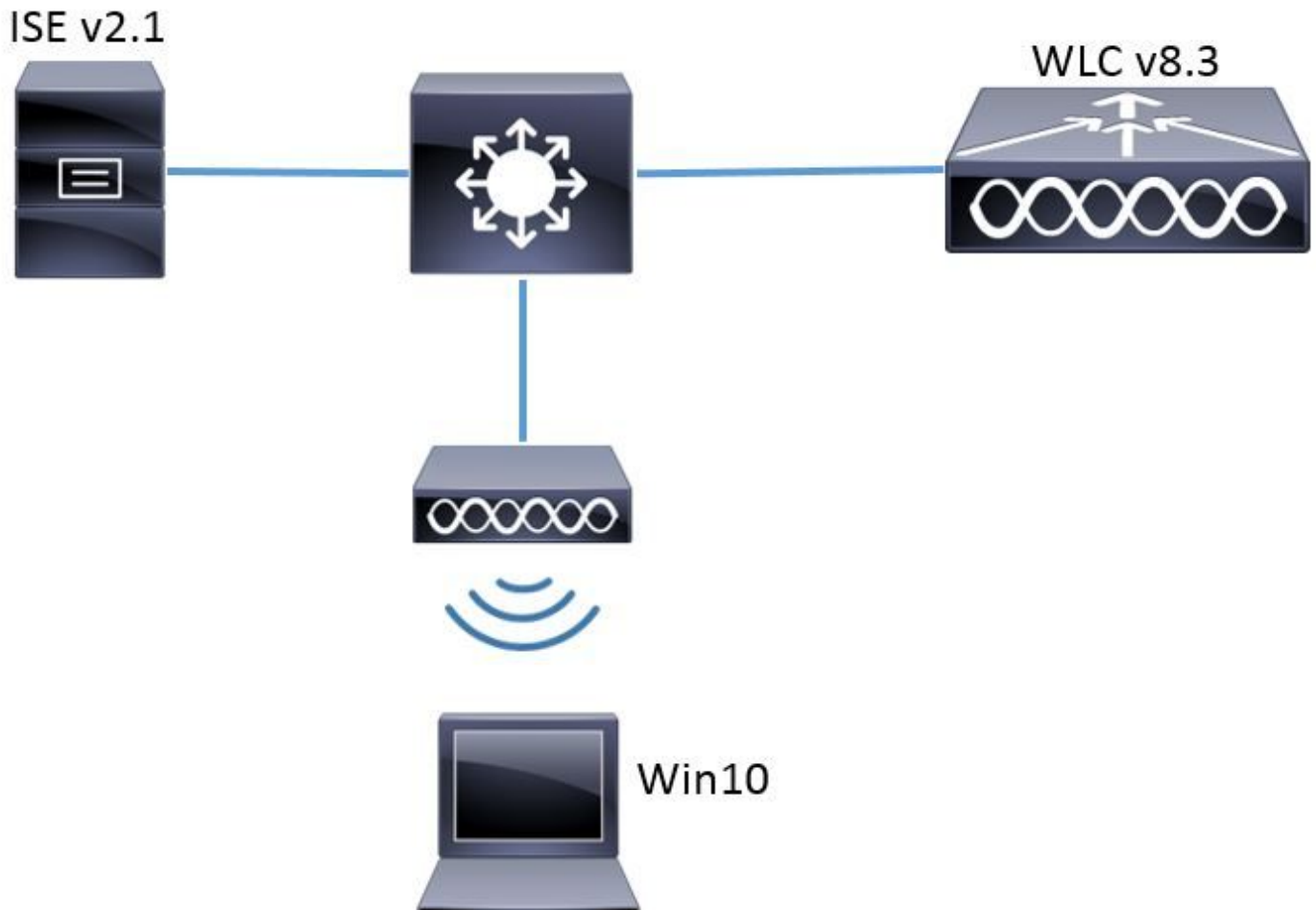
WLC v8.3.102.0

ISE v2.1

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：

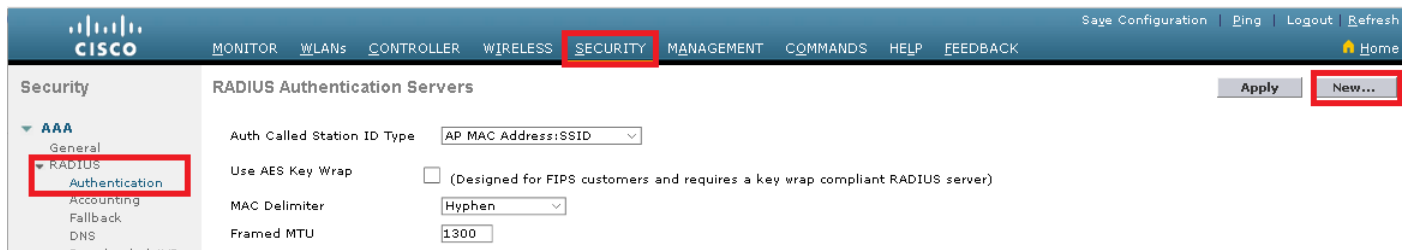
1. 指定RADIUS服务器(在本例中的ISE)在WLC反之亦然允许彼此的通信
2. 创建SSID (服务集标识符)在WLC
3. 创建在ISE的验证规则
4. 创建在ISE的授权配置文件
5. 创建在ISE的授权规则
6. 配置终端

### 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.打开WLC的GUI并且导航对**SECURITY>RADIUS >验证>New**。



步骤2.填装RADIUS服务器信息。



CLI :

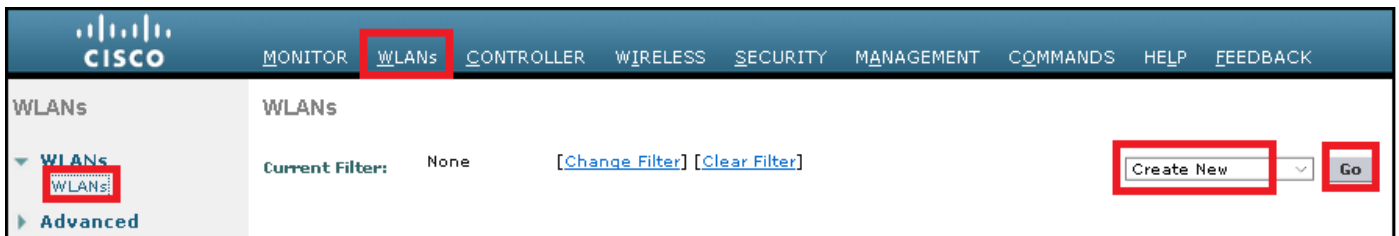
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>> config radius auth disable <index>> config radius auth retransmit-timeout <index> <timeout-seconds>> config radius auth enable <index>
```

<a.b.c.d>对应于RADIUS服务器。

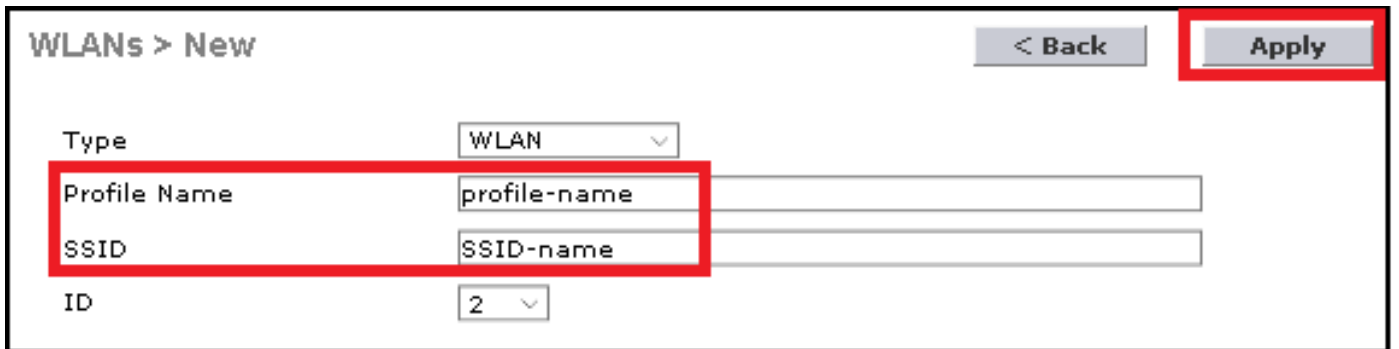
## 创建SSID

GUI :

步骤1.打开WLC的GUI并且导航对**WLAN >创建新>去**。



步骤2.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>
```

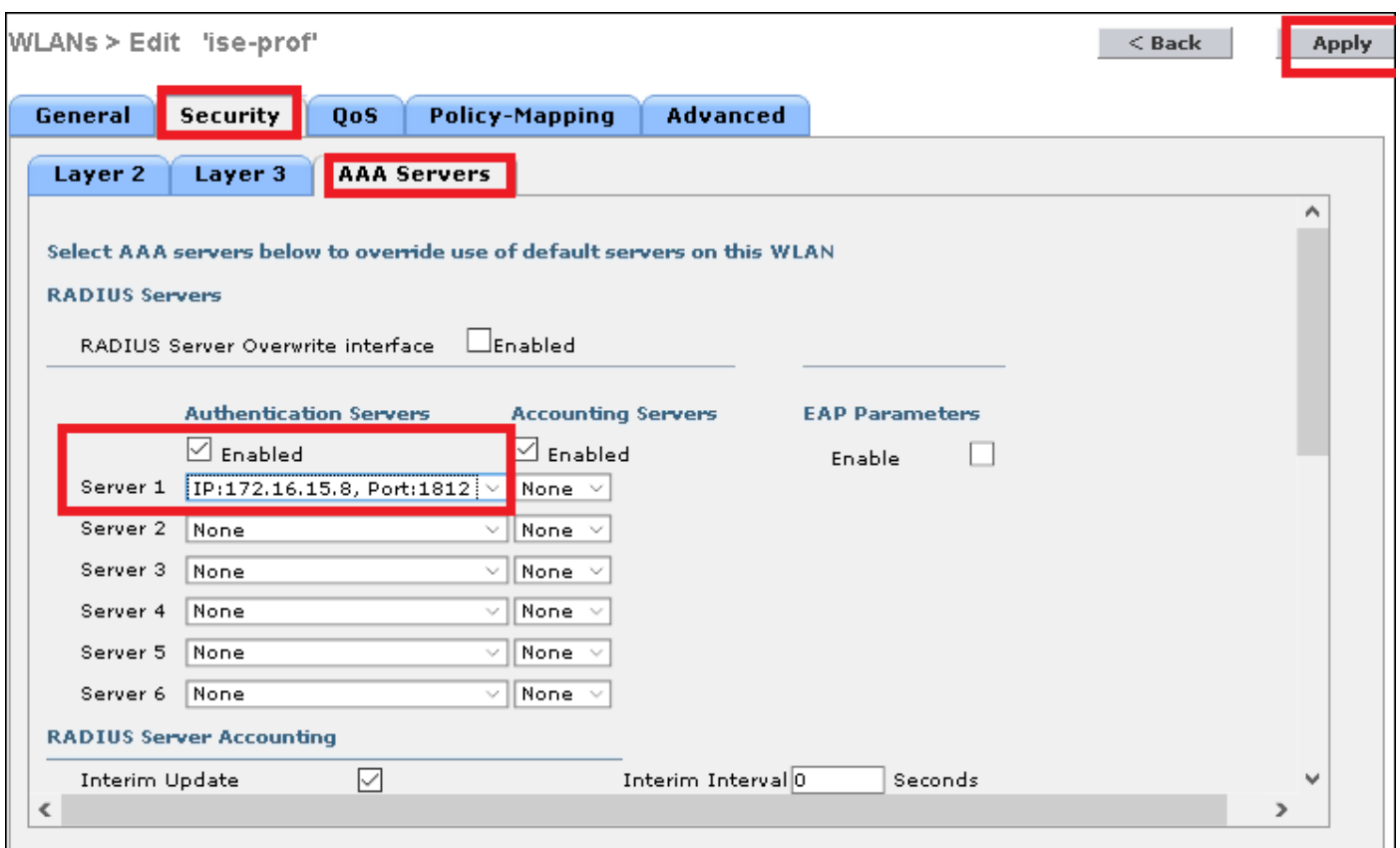
步骤3.分配RADIUS服务器到WLAN。

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，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 :

The screenshot shows the 'WLANs > Edit 'ise-prof'' configuration page. The 'Advanced' tab is selected. In the 'Session Timeout (secs)' section, the 'Enable Session Timeout' checkbox is checked, and the value '28800' is entered in the adjacent text box. The 'Apply' button in the top right corner is highlighted with a red border. Other settings visible include 'Coverage Hole Detection' (checked), 'Aironet IE' (checked), 'Diagnostic Channel 18' (unchecked), 'Override Interface ACL' (IPv4: None, IPv6: None), 'Layer2 Ad' (None), 'URL ACL' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (checked, 60 seconds), 'Maximum Allowed Clients' (0), and 'Static IP Tunneling' (unchecked). On the right side, 'DHCP' settings (DHCP Server, DHCP Addr. Assignment) and 'OEAP' (Split Tunnel) are shown as disabled. 'Management Frame Protection (MFP)' is set to 'Optional', and 'DTIM Period' is set to 1 for both 802.11a/n and 802.11b/g/n. 'NAC State' is set to 'None'.

#### 步骤5.启用WLAN

CLI :

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

GUI :

WLANs > Edit 'ise-prof' [< Back](#) [Apply](#)

**General** Security QoS Policy-Mapping Advanced

Profile Name: ise-prof

Type: WLAN

SSID: ise-ssid

Status:  Enabled

Security Policies: [WPA2][Auth(802.1X)]  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): management

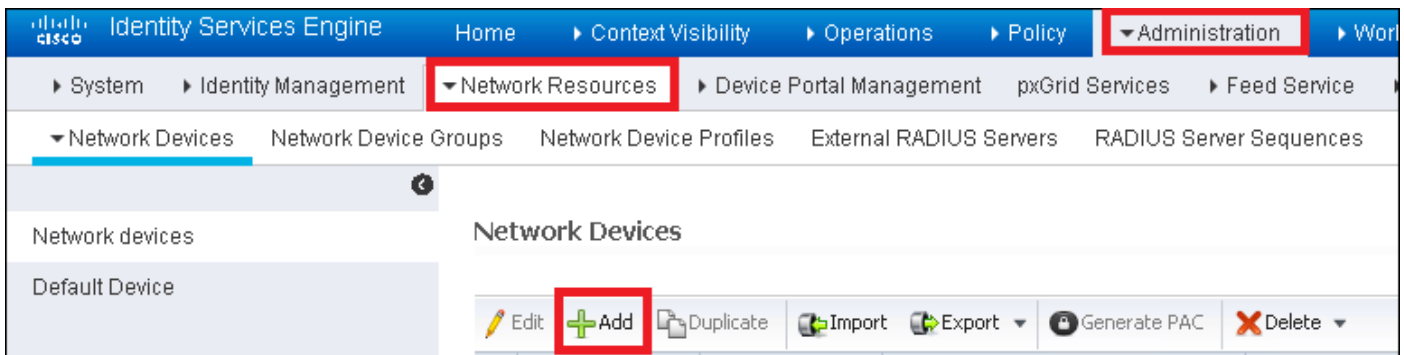
Multicast Vlan Feature:  Enabled

Broadcast SSID:  Enabled

NAS-ID: none

## 宣称在ISE的WLC

步骤1. 开放ISE控制台和导航对Administration > 网络资源 > 网络设备 > Add。



步骤2. 填装信息

随意地它能指定模型名称，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。默认情况下它是管理接口。

## Network Devices

\* Name

Description

\* IP Address:  /

\* Device Profile

Model Name

Software Version

### \* Network Device Group

Device Type

Location

WLCs

### **RADIUS Authentication Settings**

#### Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

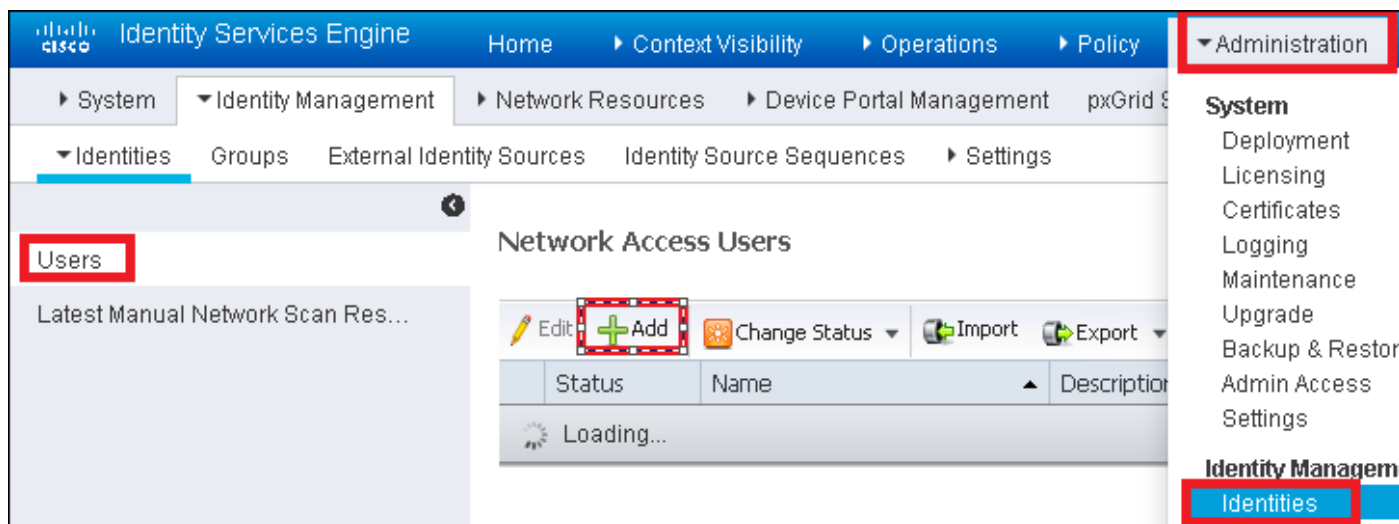
CoA Port

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.导航对Administration >身份管理>标识> Users >Add



步骤2.填装信息

在本例中此用户属于组呼叫ALL\_ACCOUNTS，但是可以调节当必要时。



▼ Network Access User

\* Name

Status  Enabled ▼

Email

▼ Passwords

Password Type:  ▼

Password

Re-Enter Passw

\* Login Password

Enable Password

▼ User Information

First Name

Last Name

▼ Account Options

Description

Change password on next login

▼ Account Disable Policy

Disable account if date exceeds

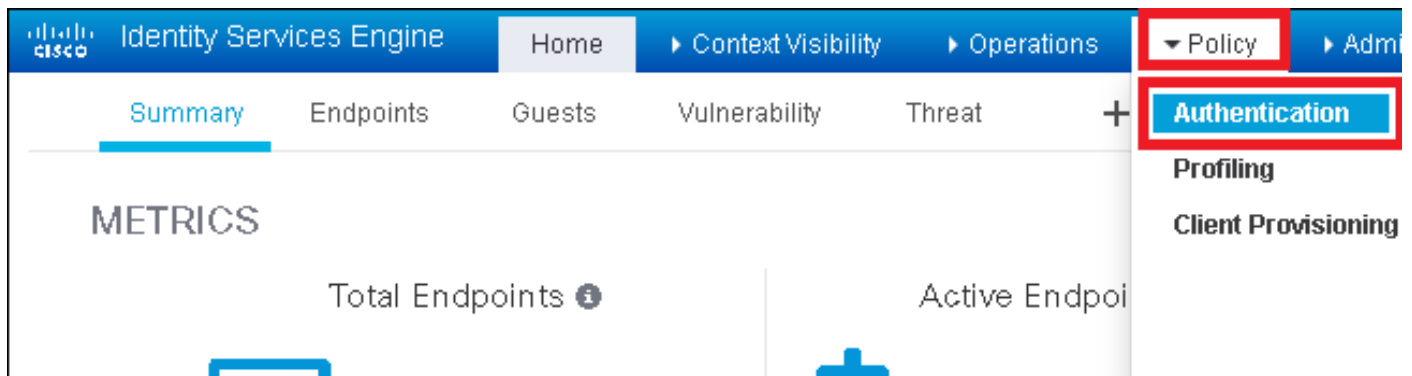
▼ User Groups

+

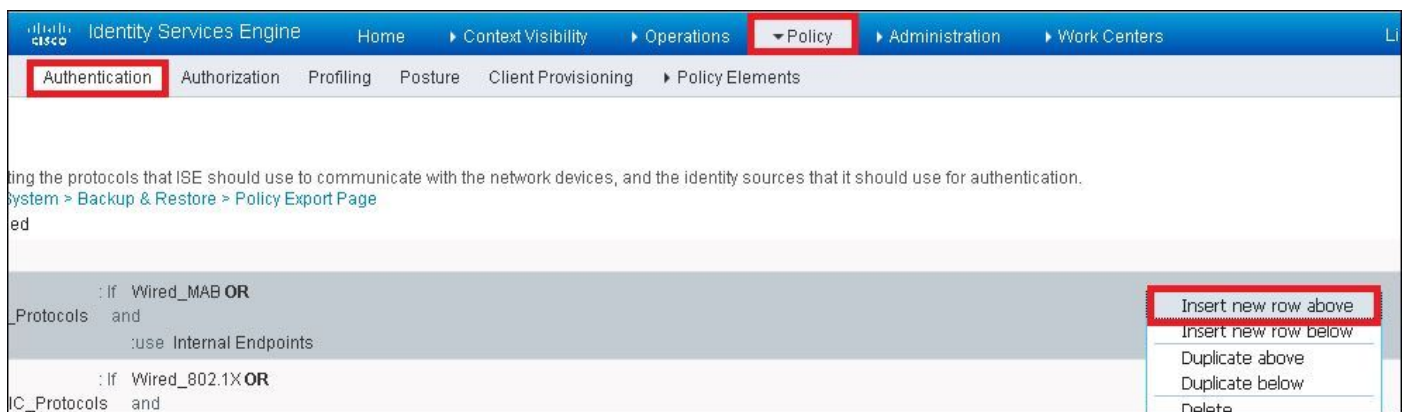
## 创建验证规则

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.导航对策略>验证。

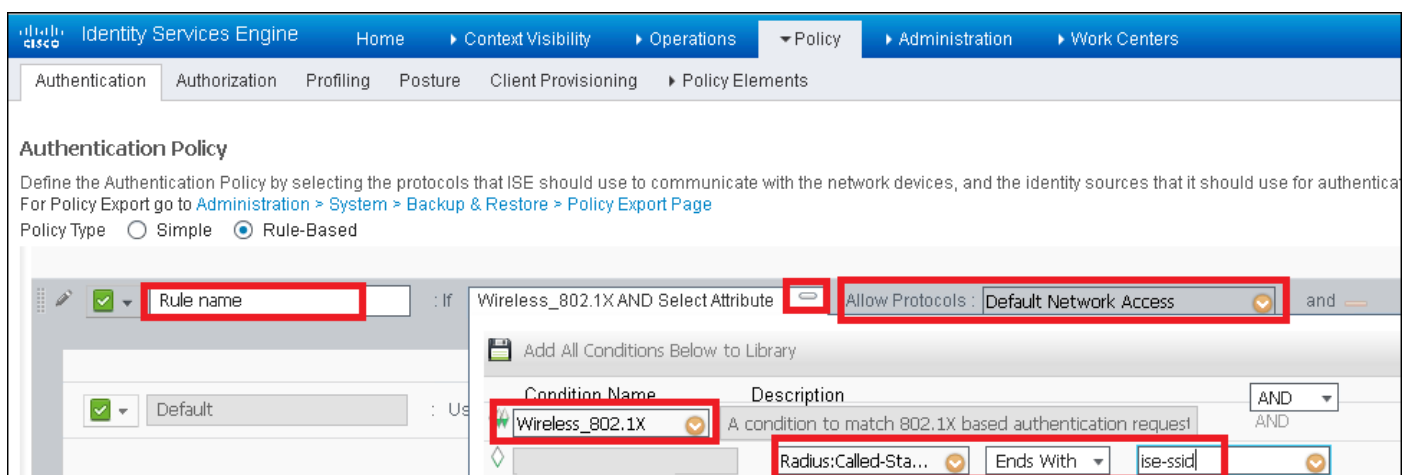


步骤2.插入新证书规则。

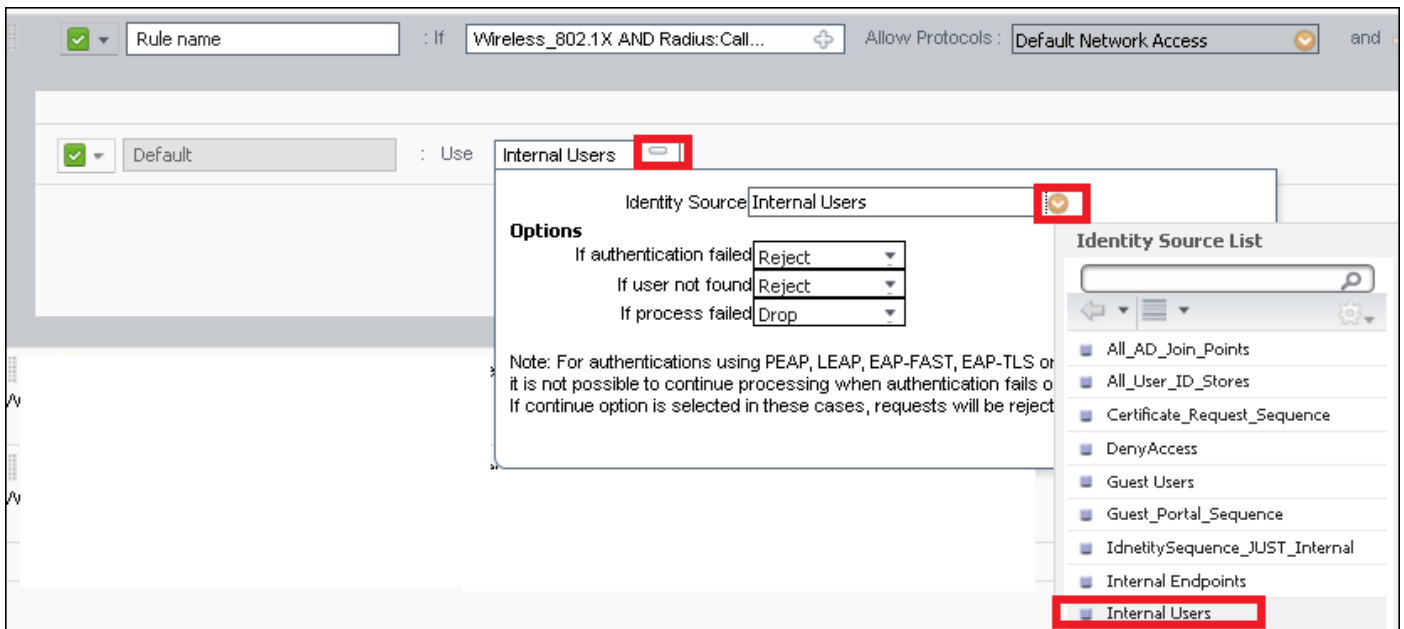


步骤3.输入值。

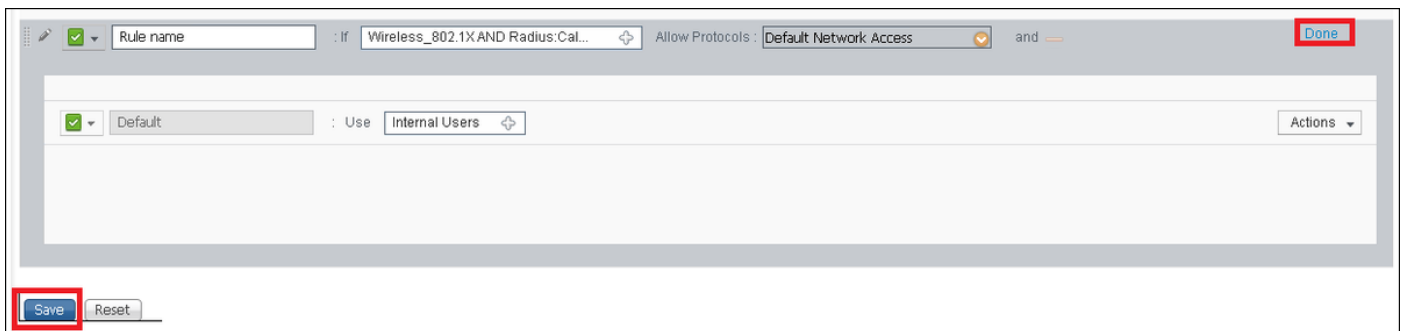
此验证规则允许所有协议列出在默认网络访问列表下，这适用于认证请求为无线802.1x客户端和与被呼叫状态ID和末端与ISE ssid。



并且请选择匹配此验证规则客户端的标识来源，此示例用途内部用户标识源列表



一旦它完成请点击完成和“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](#)

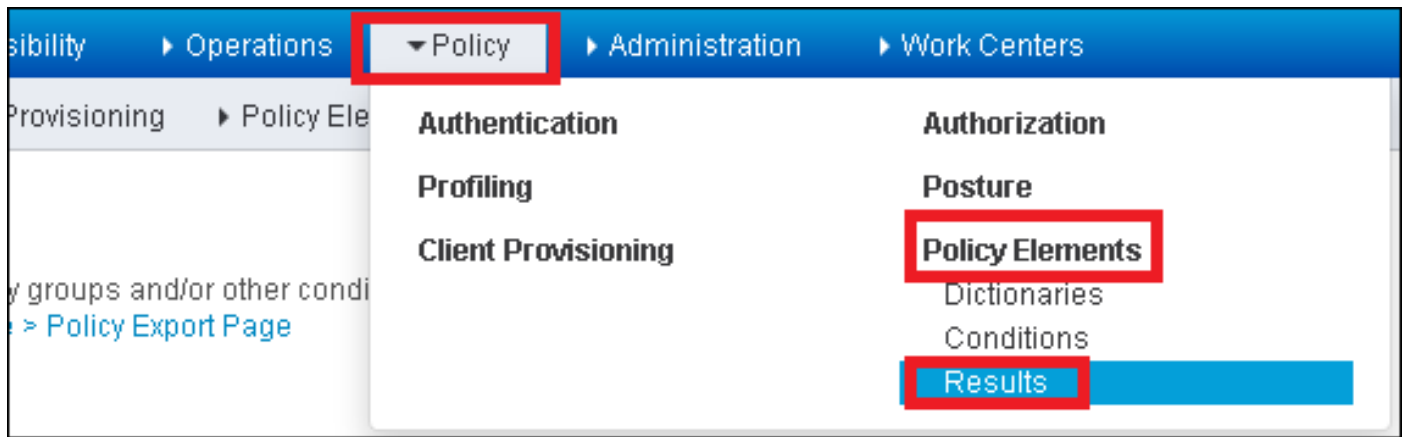
关于标识的更多信息来源参见此链路：

[创建用户标识组](#)

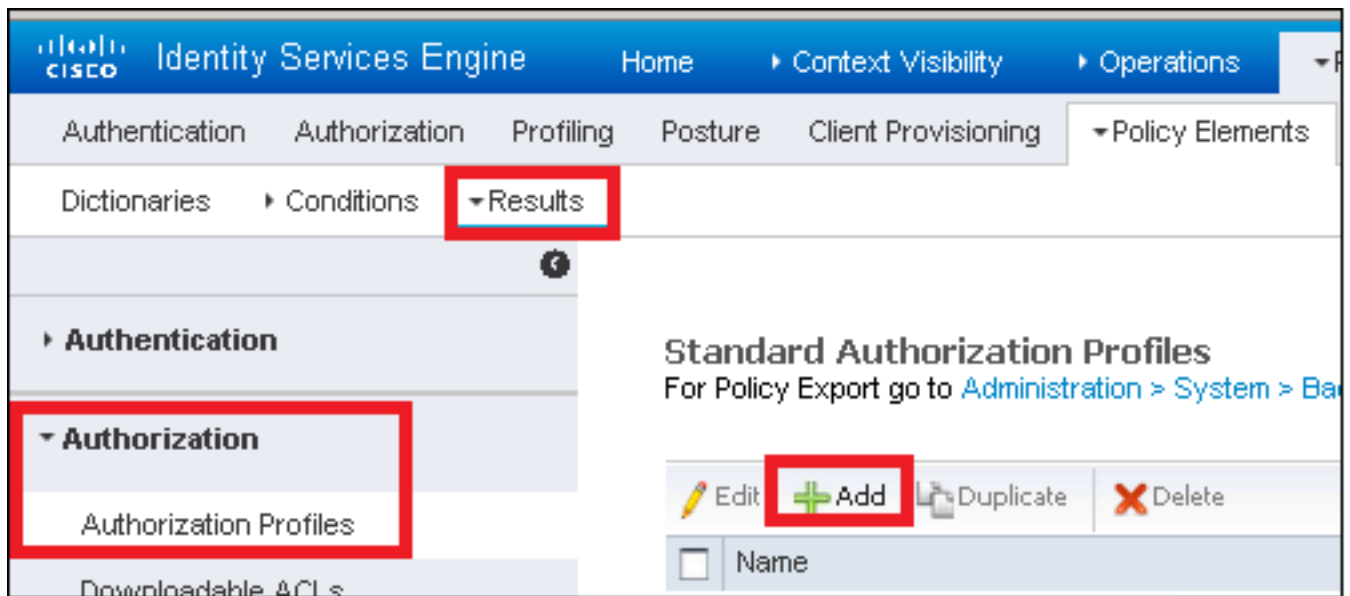
## 创建授权配置文件

授权配置文件确定客户端是否访问或不网络、推送ACL (访问控制列表)， VLAN (虚拟局域网)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.导航对策略>Policy元素>结果



步骤2.添加一新的授权配置文件。导航对授权>授权Profiles>添加



步骤3.填装值。