带身份服务引擎的无线BYOD

目录

简介

思科身份服务引擎(ISE)是思科的下一代策略服务器，为Cisco TrustSec解决方案提供身份验证和授权基础设施。它还提供另外两项关键服务：

- 第一项服务是提供一种方法，根据思科ISE从各种信息源接收的属性自动分析终端设备类型。此服务（称为Profiler）提供与思科之前通过Cisco NAC Profiler设备提供的相同功能。
- 思科ISE提供的另一项重要服务是扫描终端合规性；例如，AV/AS软件安装及其定义文件有效性（称为状态）。思科之前仅通过Cisco NAC设备提供此确切的安全评估功能。

思科ISE提供同等级别的功能，并与802.1X身份验证机制集成。

与无线局域网控制器(WLC)集成的思科ISE可提供移动设备(例如Apple iDevices（iPhone、iPad和iPod）、基于Android的智能手机和其他设备的分析机制。对于802.1X用户，思科ISE可提供相同级别的服务，例如分析和状态扫描。思科ISE上的访客服务也可通过将Web身份验证请求重定向到思科ISE进行身份验证而与思科WLC集成。

本文档介绍自带设备(BYOD)的无线解决方案，例如根据已知终端和用户策略提供差异化接入。本文档不提供BYOD的完整解决方案，但用于演示动态访问的简单使用案例。其他配置示例包括使用ISE发起人门户，特权用户可以发起访客调配无线访客接入。

先决条件

要求

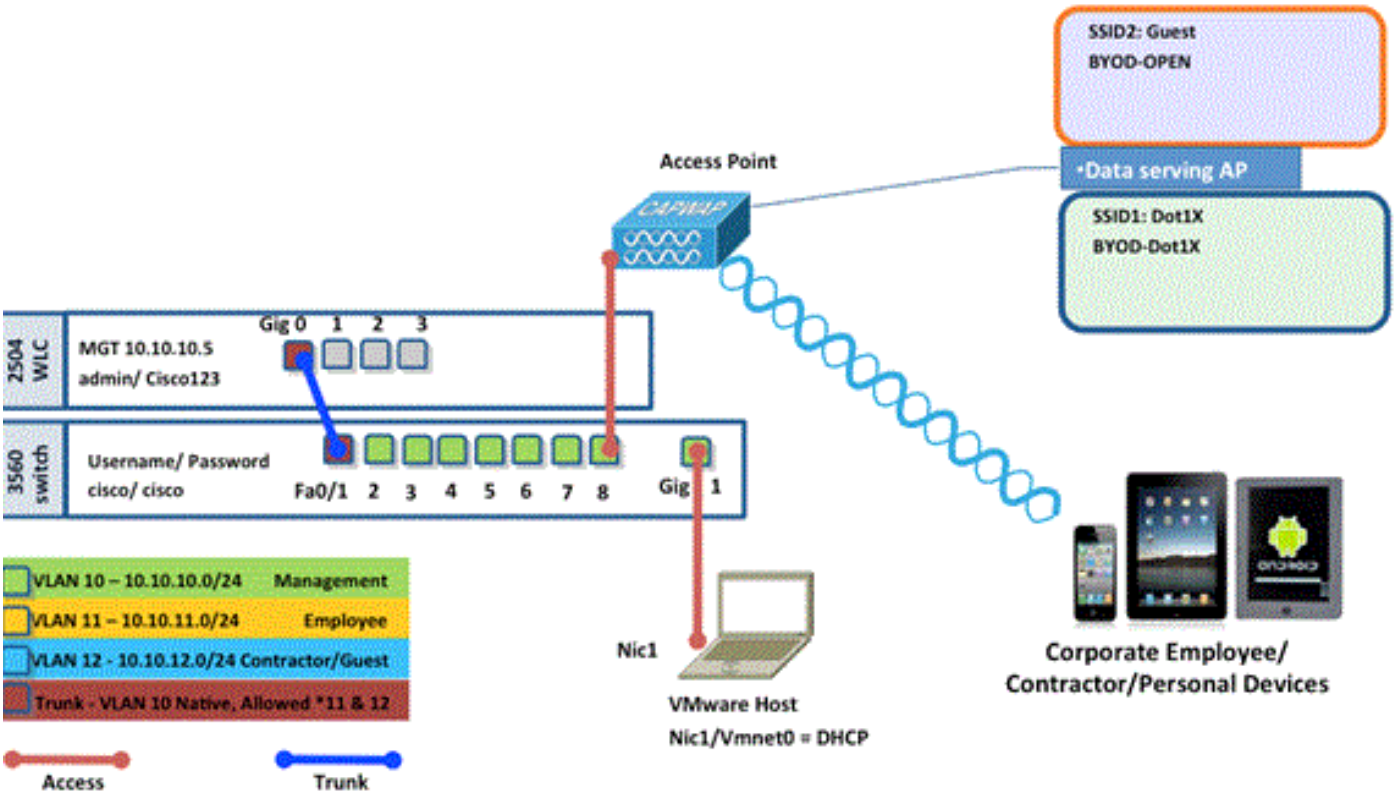
本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 软件版本为7.2.103的思科无线局域网控制器2504或2106
- Catalyst 3560 - 8端口
- WLC 2504
- 身份服务引擎1.0MR（VMware服务器映像版本）
- Windows 2008 Server（VMware映像） — 512M，20GB磁盘Active DirectoryDNSDHCP证书服务

拓扑



Name	IP Address	Credential
Vmware Host	10.10.10.2	*(Machine used to host the ISE 1.0 MR vmware server files)*
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	*(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)*

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

无线LAN控制器RADIUS NAC和CoA概述

此设置使WLC能够查找来自ISE RADIUS服务器的URL重定向AV对。这仅适用于绑定到启用了RADIUS NAC设置的接口的WLAN。当收到用于URL重定向的Cisco AV-Pair时，客户端将进入POSTURE_REQD状态。这基本上与控制器内部的WEBAUTH_REQD状态相同。

当ISE RADIUS服务器认为客户端符合安全评估时，它会发出CoA ReAuth。Session_ID用于将其连接在一起。使用此新的AuthC（重新身份验证）时，它不会发送URL-Redirect AV-Pairs。由于没有URL重定向AV对，因此WLC知道客户端不再需要安全评估。

如果未启用RADIUS NAC设置，WLC将忽略URL重定向VSA。

CoA-ReAuth：这通过RFC 3576设置启用。ReAuth功能已添加到以前支持的现有CoA命令中。

RADIUS NAC设置与此功能互斥，但CoA需要它才能工作。

Pre-Posture ACL：当客户端处于POSTURE_REQ状态时，WLC的默认行为是阻止除DHCP/DNS之外的所有流量。Pre-Posture ACL（在url-redirect-acl AV-Pair中称为）应用于客户端，该ACL中允许的内容是客户端可以到达的内容。

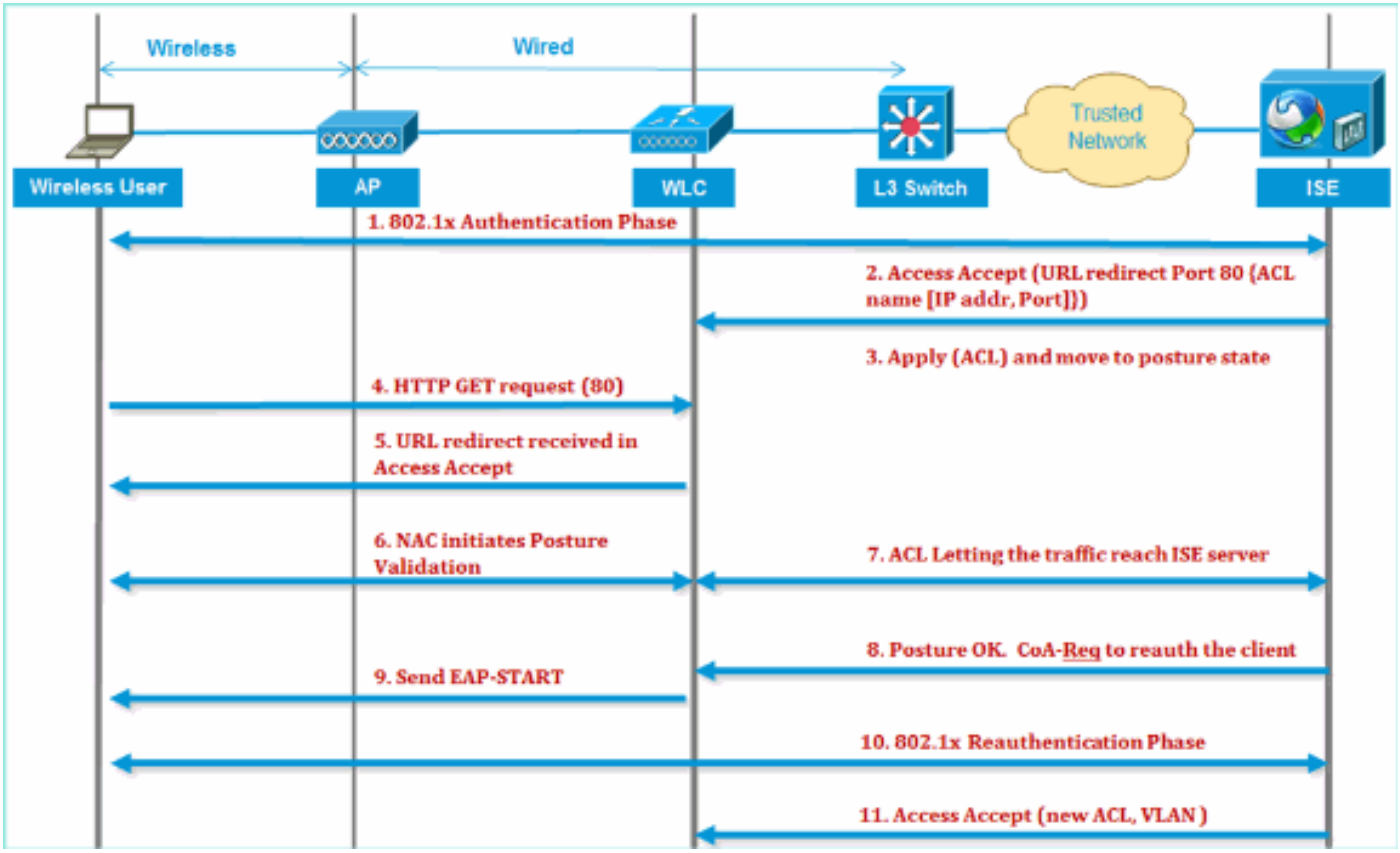
Pre-Auth ACL与VLAN覆盖：7.0MR1不支持与接入VLAN不同的隔离或AuthC VLAN。如果从策略服务器设置VLAN，它将成为整个会话的VLAN。首次授权后无需更改VLAN。

无线LAN控制器RADIUS NAC和CoA功能流

以下图提供了客户端通过后端服务器身份验证和NAC状态验证时消息交换的详细信息。

1. 客户端使用dot1x身份验证进行身份验证。
2. RADIUS Access Accept传输端口80的重定向URL和包括允许IP地址和端口或隔离VLAN的预身份验证ACL。
3. 客户端将重定向到access accept中提供的URL，并进入新状态，直到完成状态验证。处于此状态的客户端与ISE服务器通信，并根据ISE NAC服务器上配置的策略验证自身。
4. 客户端上的NAC代理启动状态验证（到端口80的流量）：代理向端口80发送HTTP发现请求，控制器重定向到访问接受中提供的URL。ISE知道客户端尝试访问并直接响应客户端。这样，客户端即可了解ISE服务器IP，从现在起，客户端将直接与ISE服务器进行通信。
5. 由于ACL配置为允许此流量，因此WLC允许此流量。如果发生VLAN覆盖，流量会桥接以便到达ISE服务器。
6. ISE客户端完成评估后，RADIUS CoA-Req with reauth service将发送到WLC。这将启动客户端的重新身份验证（通过发送EAP-START）。重新身份验证成功后，ISE会发送包含新ACL（如果有）和无URL重定向或访问VLAN的访问接受。
7. 根据RFC 3576,WLC支持CoA-Req和Disconnect-Req。根据RFC 5176,WLC需要支持重新身份验证服务的CoA-Req。
8. WLC上使用的是预配置的ACL，而不是可下载的ACL。ISE服务器仅发送ACL名称，该名称已在控制器中配置。
9. 此设计适用于VLAN和ACL两种情况。如果发生VLAN覆盖，我们只需重定向端口80，并允许（桥接）隔离VLAN上的其余流量。对于ACL，应用访问接受中收到的预身份验证ACL。

此图直观地显示了此功能流：



ISE分析概述

思科ISE分析器服务提供发现、定位和确定网络上所有连接的终端的功能，无论其设备类型如何，以确保和维护对企业网络的适当访问。它主要收集网络上所有终端的一个属性或一组属性，并根据其配置文件对它们进行分类。

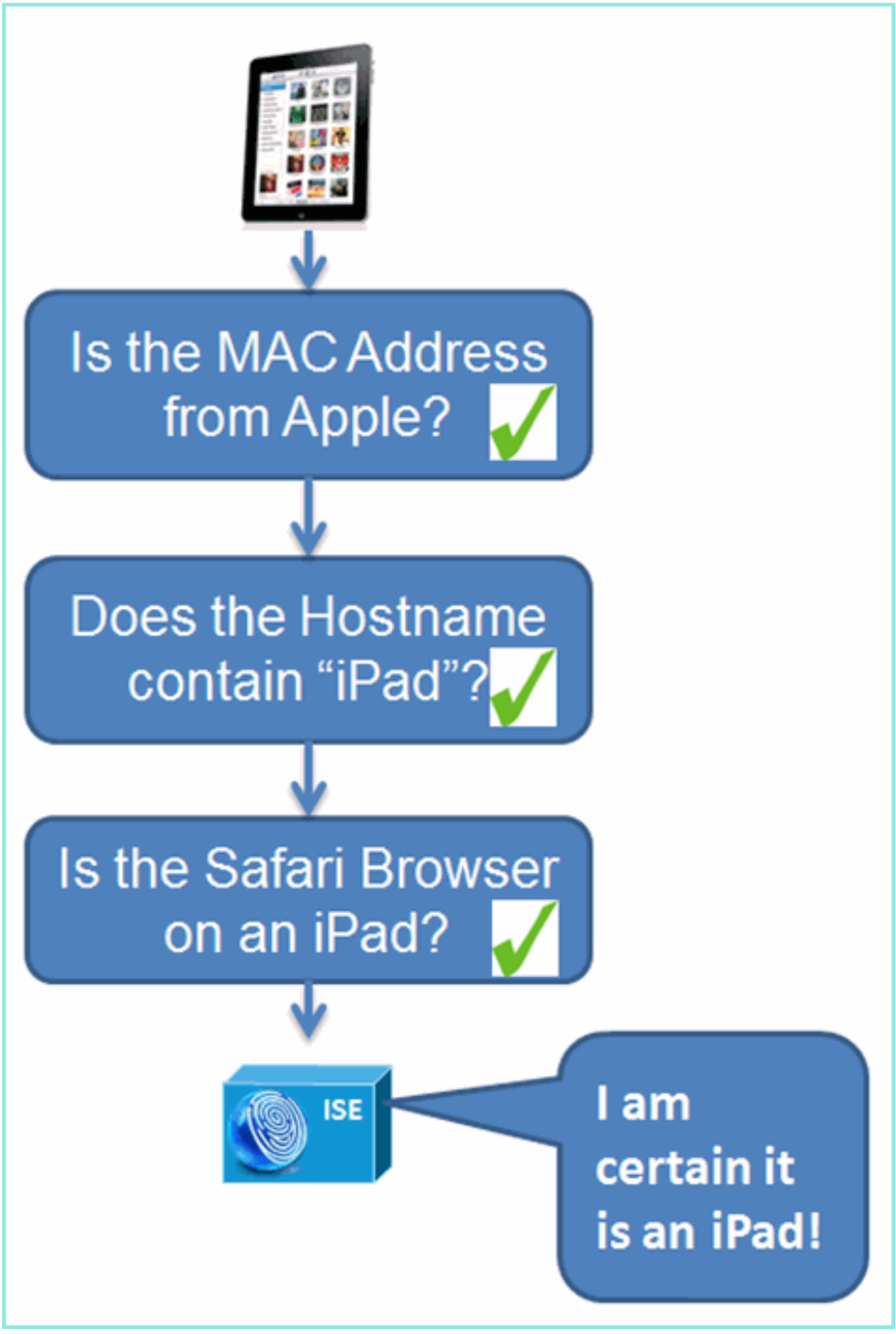
分析器由以下组件组成：

- 传感器包含许多探针。探测功能通过查询网络接入设备来捕获网络数据包，并将从终端收集的属性及其属性值转发到分析器。
- 分析器使用配置的策略和身份组评估终端以匹配所收集的属性及其属性值，将终端分类到指定组并将具有匹配配置文件的终端存储在思科ISE数据库中。

对于移动设备检测，建议结合使用以下探针正确识别设备：

- RADIUS（呼叫站ID）：提供MAC地址(OUI)
- DHCP（主机名）：主机名 — 默认主机名可以包括设备类型；例如：jsmith-ipad
- DNS（反向IP查找）：FQDN — 默认主机名可以包括设备类型
- HTTP（用户代理）：有关特定移动设备类型的详细信息

在iPad的此示例中，分析器从User-Agent属性捕获网络浏览器信息，从请求消息捕获其他HTTP属性，并将它们添加到终端属性列表中。


Is the MAC Address from Apple?
Does the Hostname contain “iPad”?
Is the Safari Browser on an iPad?
ISE
I am certain it is an iPad!

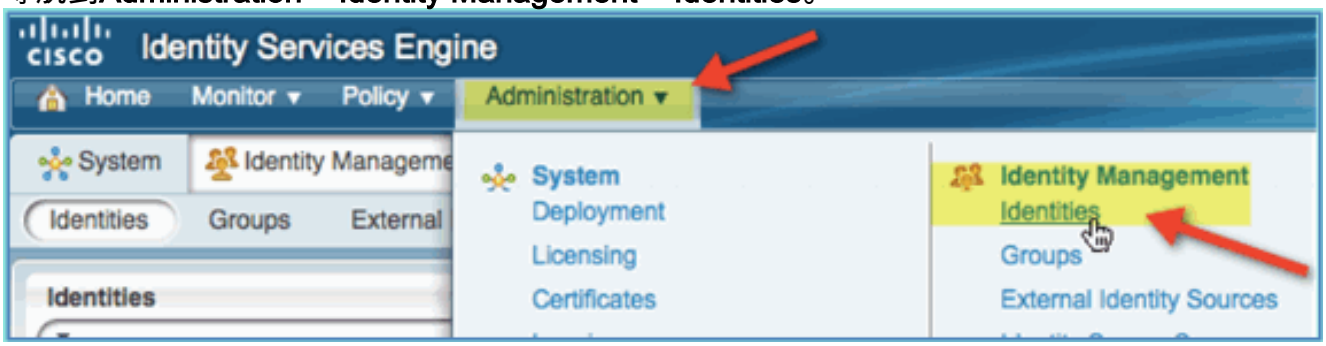
[创建内部身份用户]

简单概念验证不需要MS Active Directory(AD)。ISE可用作唯一的身份库，其中包括区分用户访问权限以进行访问和精细策略控制。

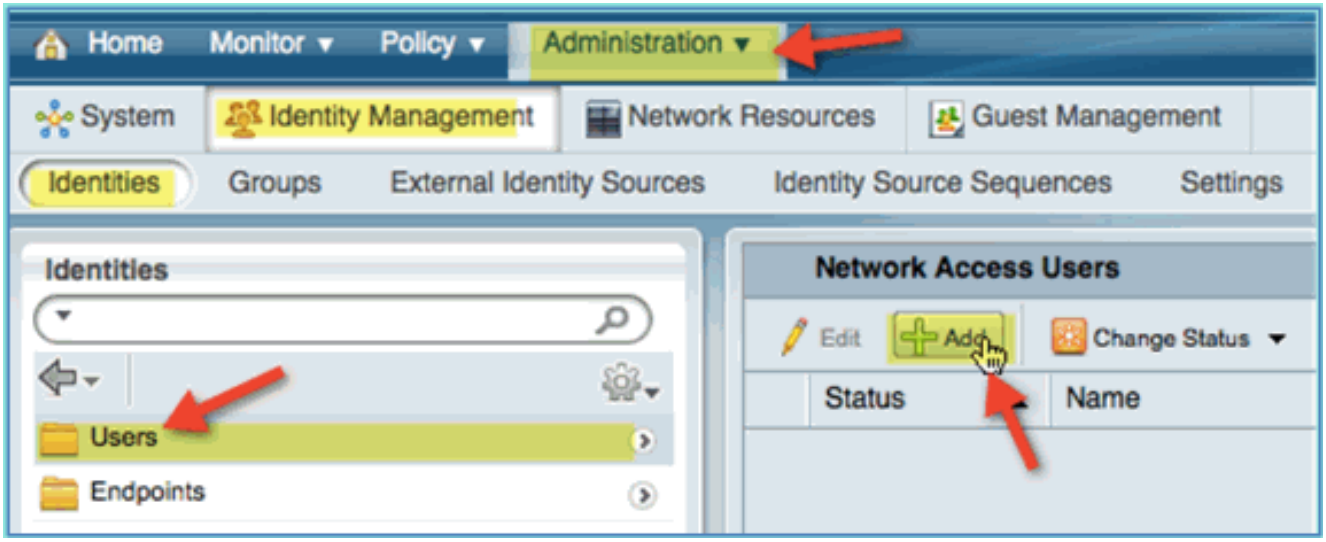
在ISE 1.0版本中，使用AD集成，ISE可以在授权策略中使用AD组。如果使用ISE内部用户存储（无AD集成），则不能在策略中与设备身份组一起使用组（已在ISE 1.1中确定需要解决的漏洞）。因此，除了设备身份组外，使用时只能区分个人用户，例如员工或承包商。

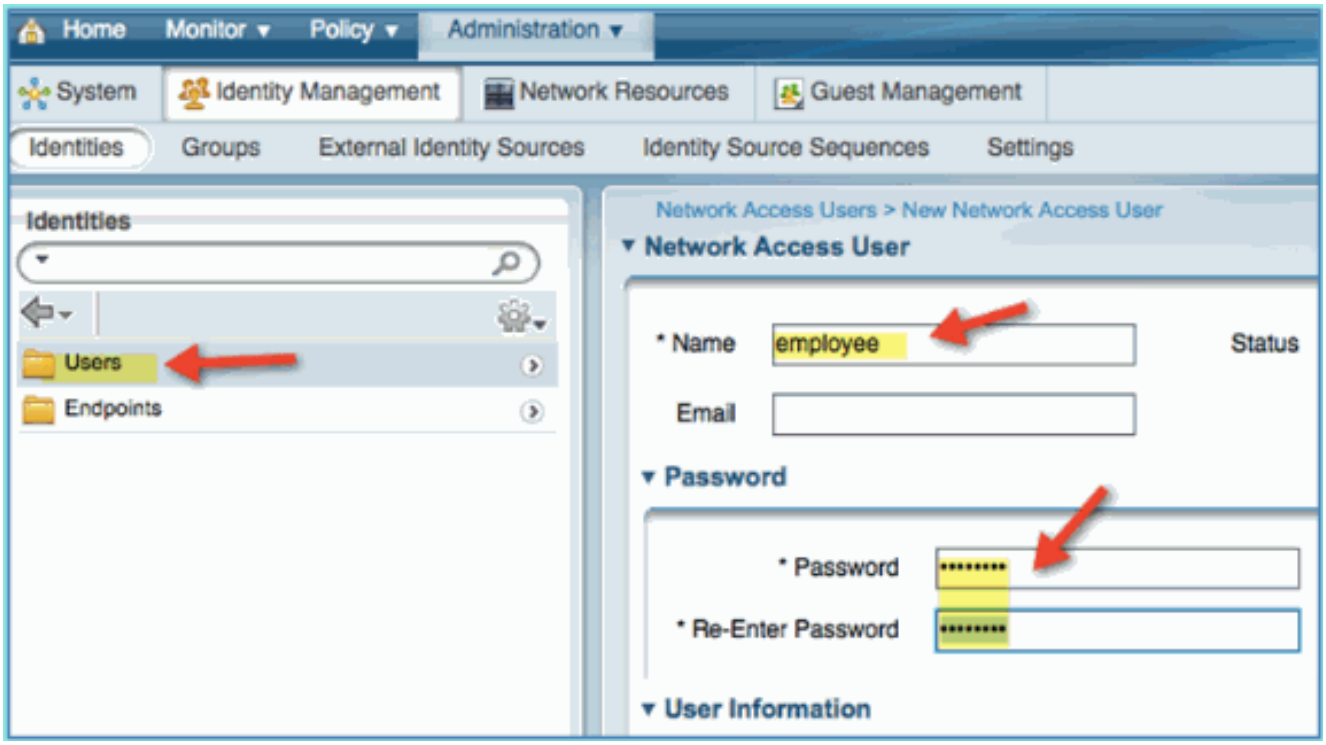
请完成以下步骤：

1. 打开浏览器窗口访问https://ISEip地址。
2. 导航到**Administration > Identity Management > Identities**。

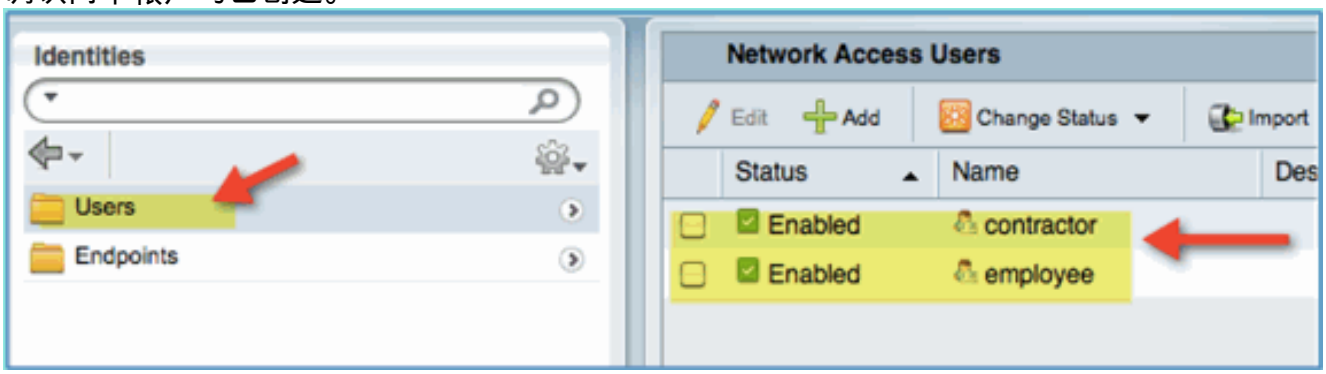


3. 选择**Users**，然后单击**Add**（网络访问用户）。输入以下用户值并分配给Employee组：姓名：employee密码：XXXX





4. 单击“Submit”。姓名：承包商密码：XXXX
5. 确认两个帐户均已创建。



向ISE添加无线LAN控制器

向ISE发起RADIUS请求的任何设备都必须在ISE中有定义。这些网络设备是根据其IP地址定义的。ISE网络设备定义可以指定IP地址范围，从而允许定义代表多个实际设备。

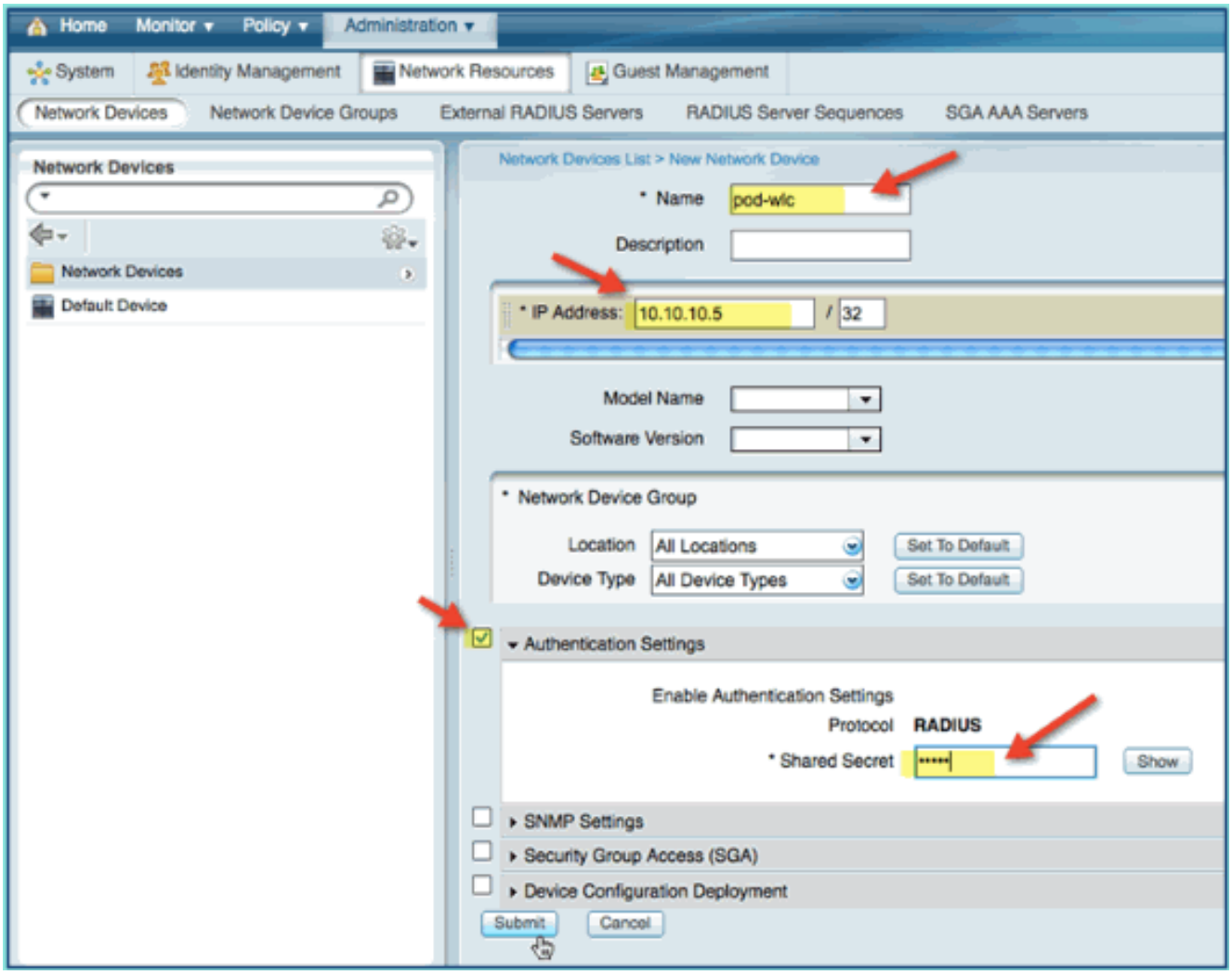
除了RADIUS通信所需的设置，ISE网络设备定义还包含其他ISE/设备通信的设置，例如SNMP和SSH。

网络设备定义的另一个重要方面是对设备进行适当分组，以便可以在网络访问策略中使用此分组。

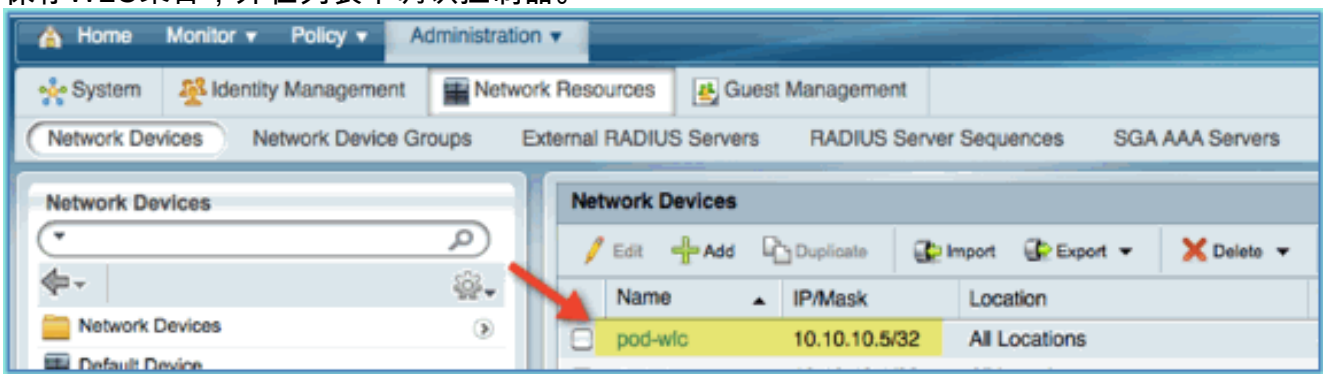
本练习将配置实验所需的设备定义。

请完成以下步骤：

1. 从ISE转至**Administration > Network Resources > Network Devices**。



2. 在Network Devices（网络设备）中，单击**Add**。输入IP地址，掩码检查Authentication Setting，然后输入cisco作为共享密钥。
3. 保存WLC条目，并在列表中确认控制器。

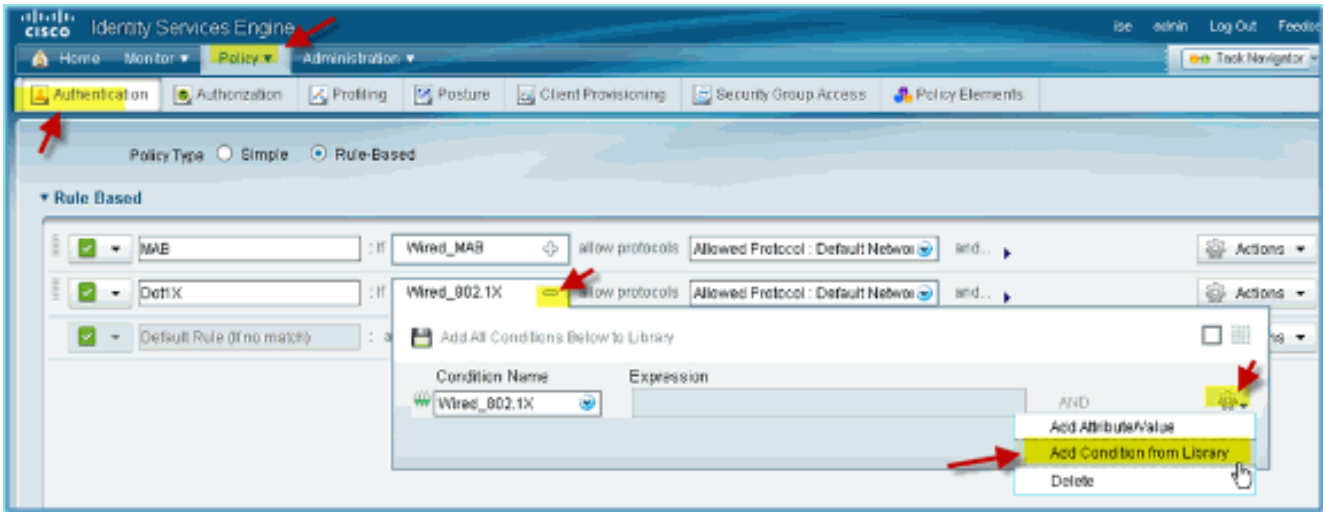


配置ISE进行无线身份验证

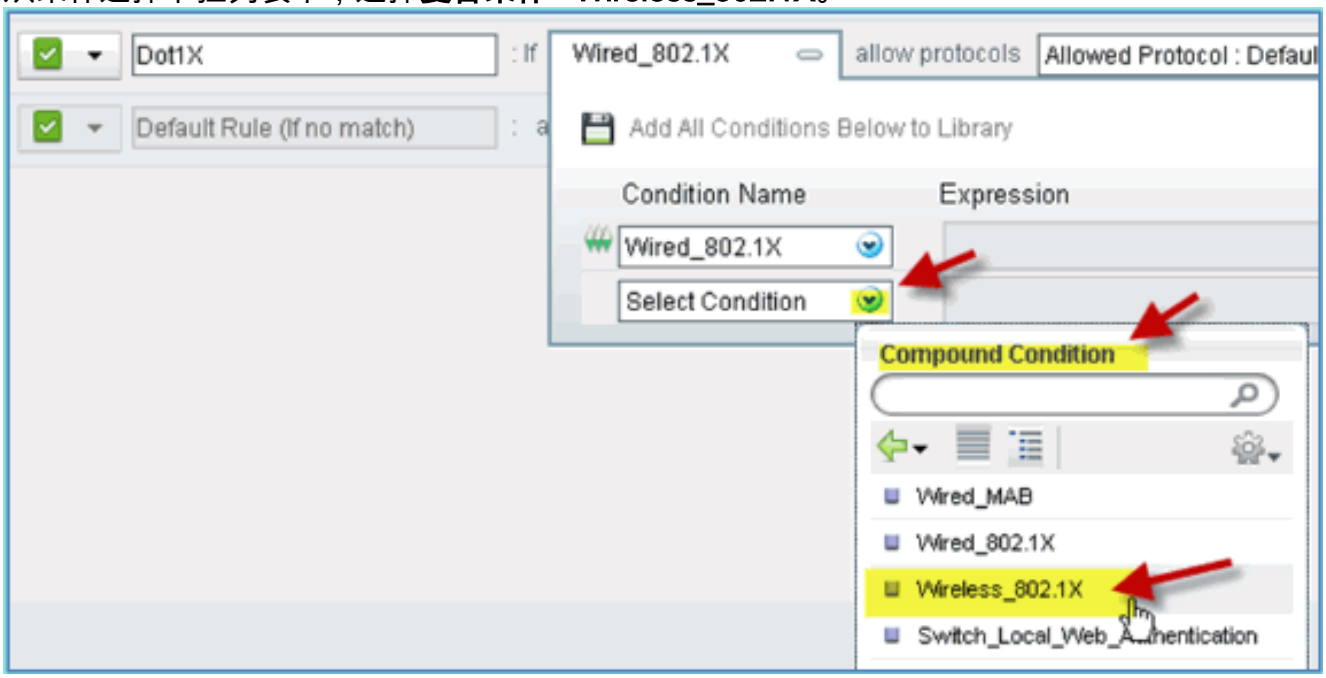
需要配置ISE以对802.1x无线客户端进行身份验证，并使用Active Directory作为身份库。

请完成以下步骤：

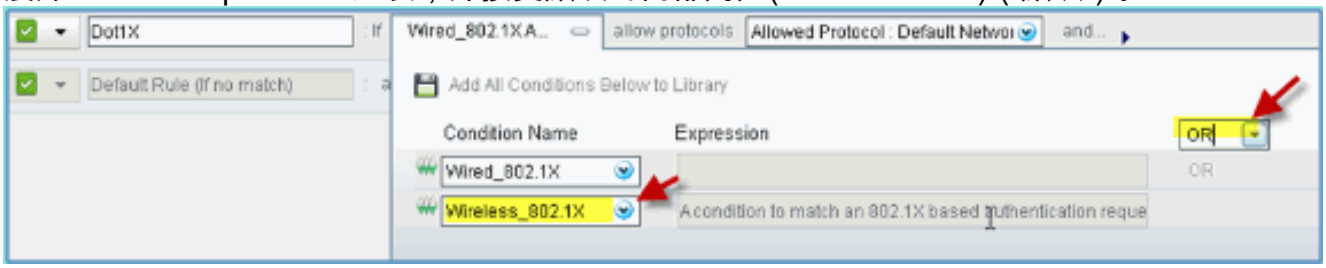
1. 从ISE导航到**策略>身份验证**。
2. 单击展开Dot1x > Wired_802.1X(-)。
3. 单击齿轮图标以从库**中添加条件**。

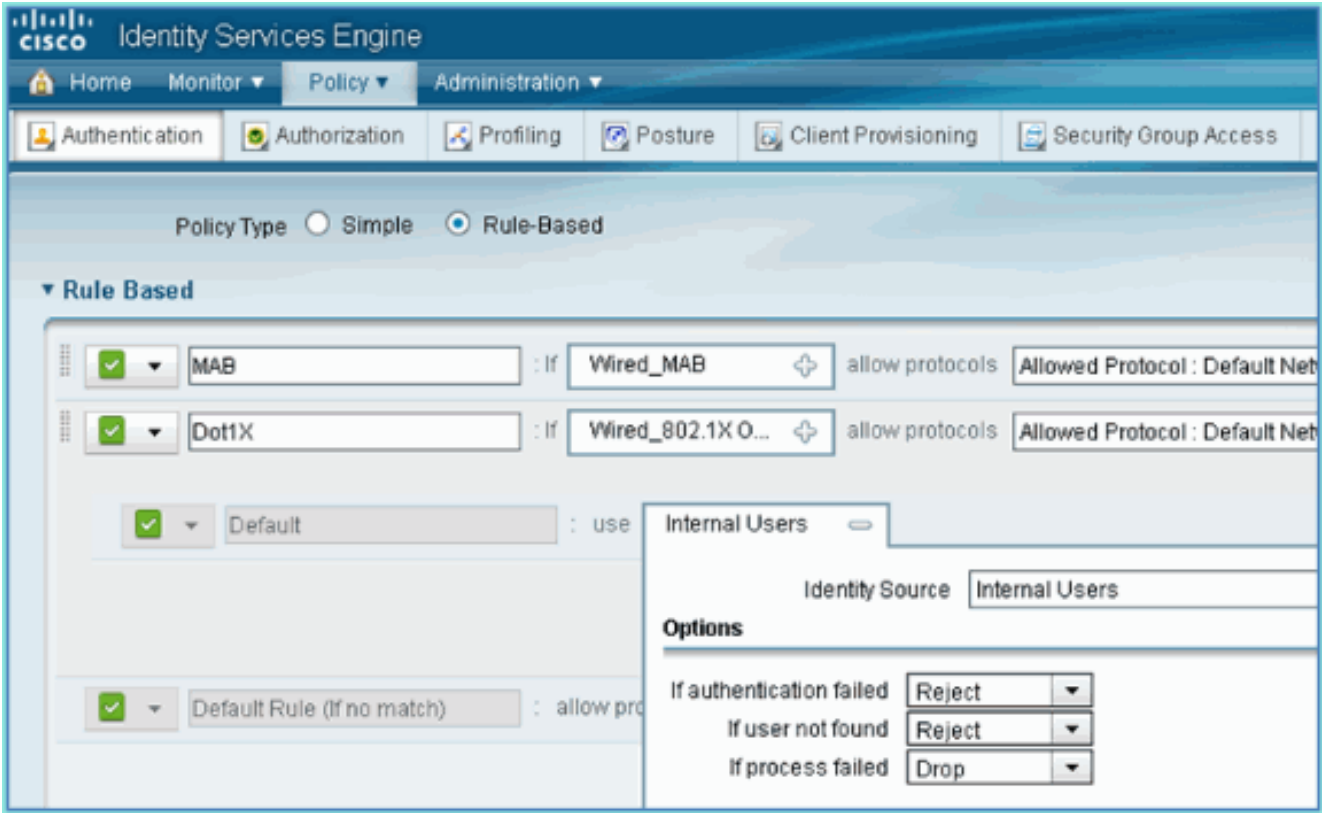


4. 从条件选择下拉列表中，选择**复合条件> Wireless_802.1X**。



5. 将Express条件设置为**OR**。
6. 展开after allow protocols选项，并接受默认的内部用户(Internal Users)（默认）。





7. 保留其他所有设置。单击**Save**完成这些步骤。

Bootstrap无线LAN控制器

将WLC连接到网络

Cisco 2500 Series Wireless Controller Deployment Guide中还提供了Cisco 2500无线LAN控制器部署指南。

使用启动向导配置控制器

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
 Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
```

```
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

邻居交换机配置

控制器连接到相邻交换机(Fast Ethernet 1)的以太网端口。邻居交换机端口配置为802.1Q中继并允许中继上的所有VLAN。本征VLAN 10允许连接WLC的管理接口。

802.1Q交换机端口配置如下：

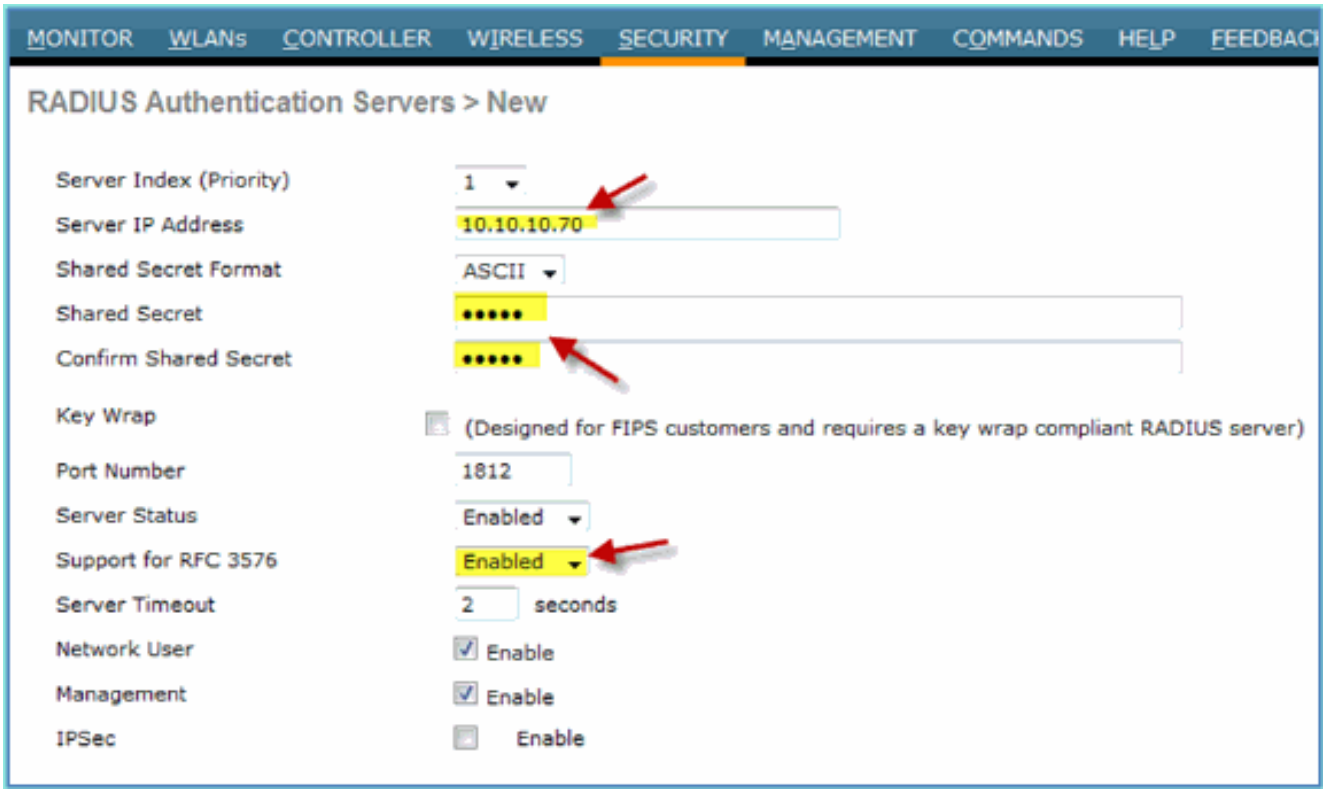
```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

将身份验证服务器(ISE)添加到WLC

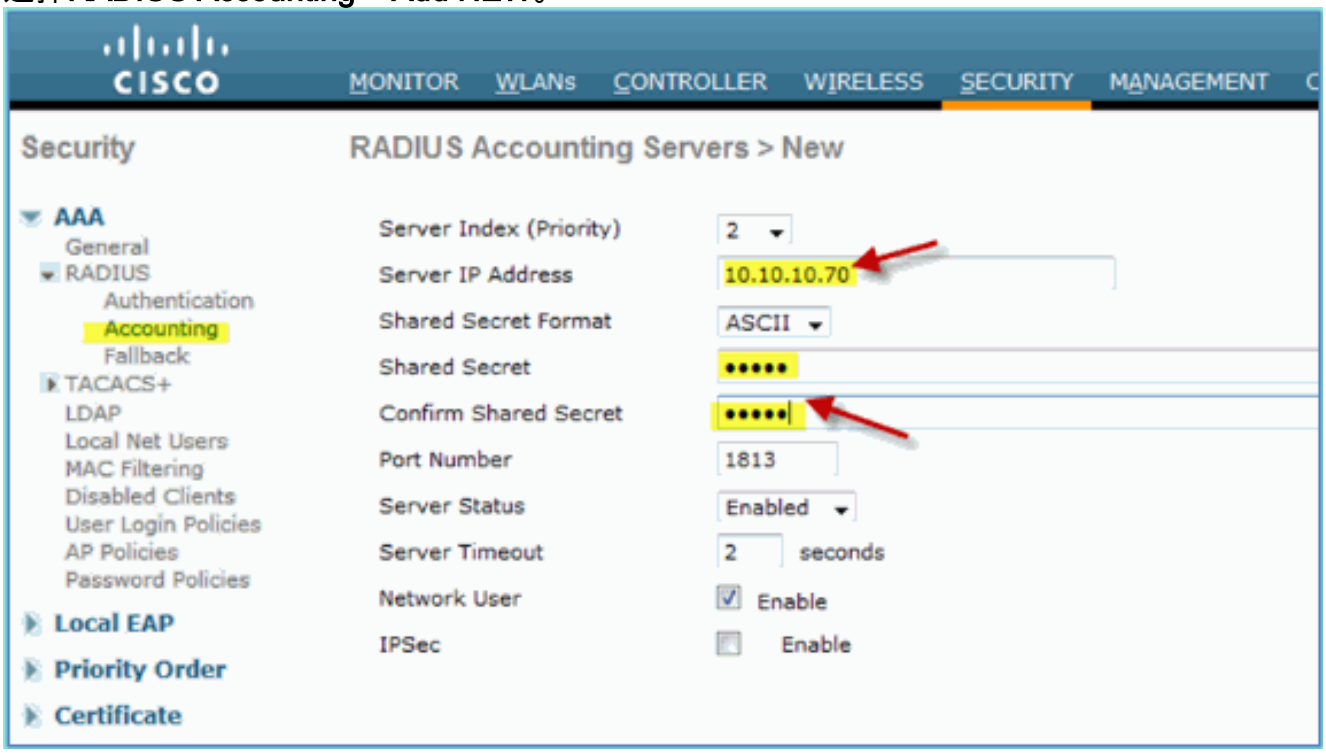
需要将ISE添加到WLC，以便为无线终端启用802.1X和CoA功能。

请完成以下步骤：

1. 打开浏览器，然后连接到Pod WLC（使用安全HTTP）> https://wlc。
2. 导航到**安全>身份验证>新建**。



3. 输入以下值：服务器IP地址：10.10.10.70（检查分配）共享密钥：cisco支持RFC 3576(CoA)：启用（默认）其他所有内容：默认
4. 单击**Apply**继续。
5. 选择**RADIUS Accounting > Add NEW**。

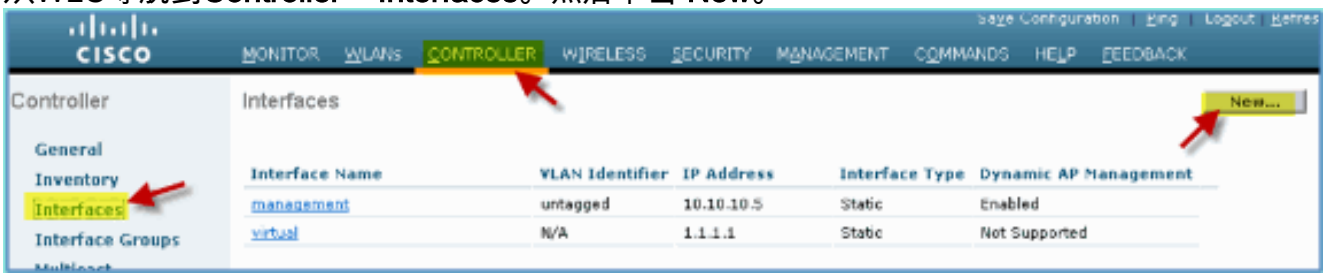


6. 输入以下值：服务器IP地址：10.10.10.70共享密钥：cisco其他所有内容：默认
7. 单击**Apply**，然后保存WLC的配置。

创建WLC员工动态接口

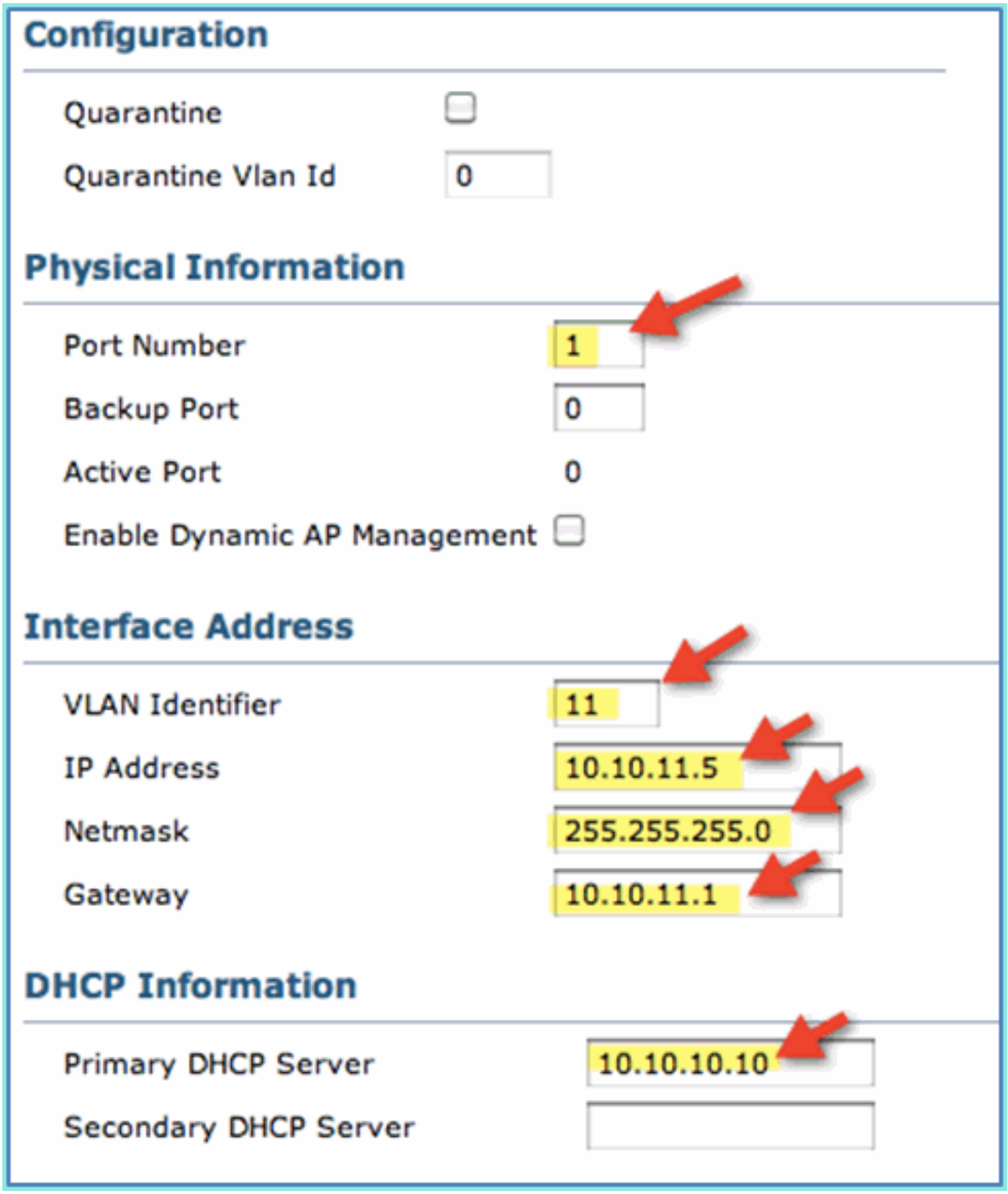
完成以下步骤，以便为WLC添加新的动态接口并将其映射到Employee VLAN:

1. 从WLC导航到**Controller > Interfaces**。然后单击 **New**。



2. 从WLC导航到**Controller > Interfaces**。输入以下内容：接口名称：EmployeeVLAN ID:11

3. 为员工界面输入以下内容：端口号：1VLAN标识符：11IP地址：10.10.11.5网络掩码：255.255.255.0网关：10.10.11.1DHCP:10.10.10.10

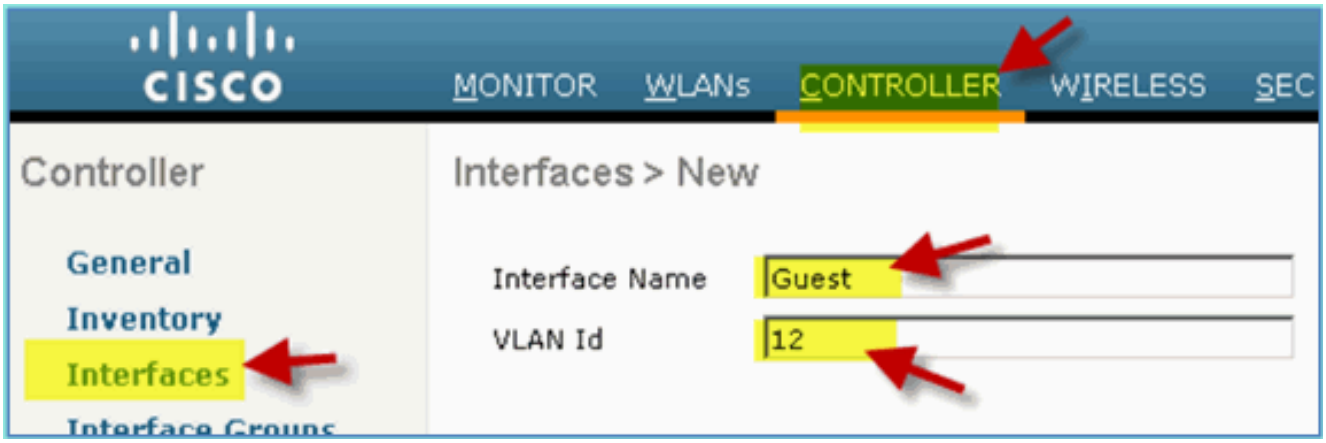


4. 确认已创建新的员工动态接口。

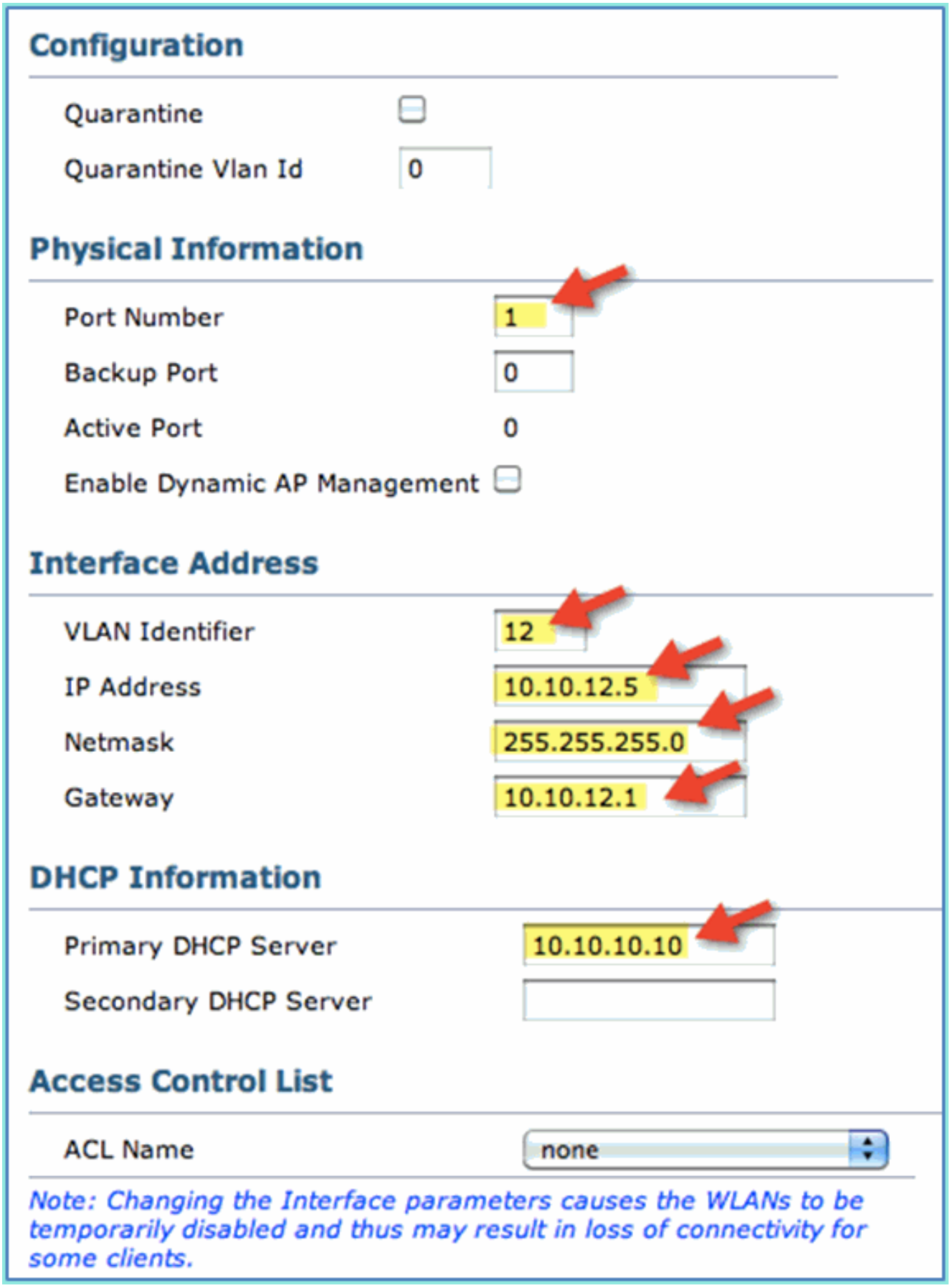
创建WLC访客动态接口

完成以下步骤，以便为WLC添加新的动态接口并将其映射到访客VLAN:

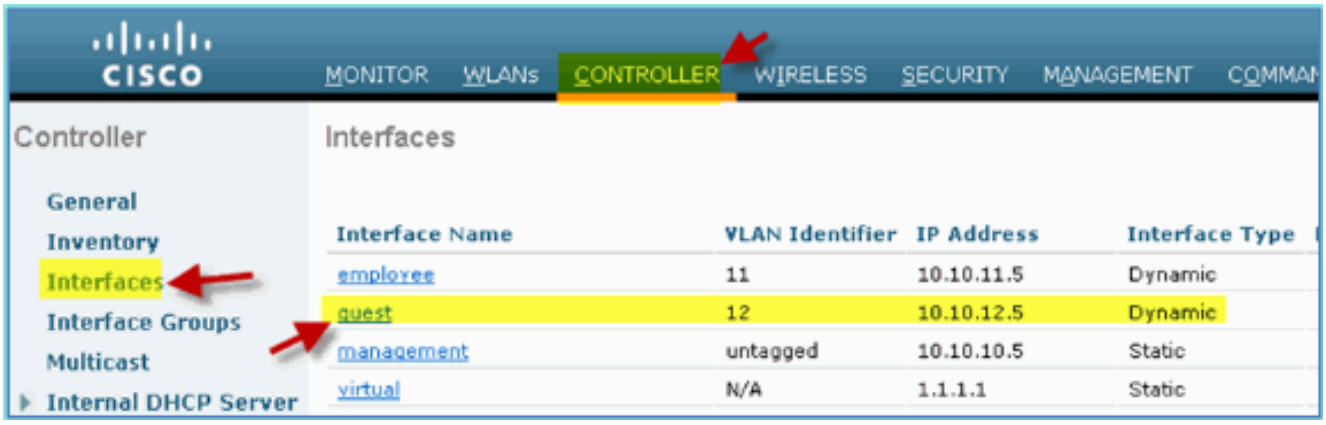
1. 从WLC导航到**Controller > Interfaces**。然后单击 **New**。
2. 从WLC导航到**Controller > Interfaces**。输入以下内容：接口名称：访客VLAN ID:12



3. 为访客接口输入以下内容：端口号：1VLAN标识符：12IP地址：10.10.12.5网络掩码：255.255.255.0网关：10.10.12.1DHCP:10.10.10.10


Configuration
Quarantine
Quarantine Vlan Id
0
Physical Information
Port Number
1
Backup Port
0
Active Port
0
Enable Dynamic AP Management
Interface Address
VLAN Identifier
12
IP Address
10.10.12.5
Netmask
255.255.255.0
Gateway
10.10.12.1
DHCP Information
Primary DHCP Server
10.10.10.10
Secondary DHCP Server
Access Control List
ACL Name
none
Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

4. 确认已添加访客接口。



添加802.1x WLAN

从WLC的初始引导中，可能已创建默认WLAN。如果是，请按照指南中的说明修改它或创建一个新的WLAN以支持无线802.1X身份验证。

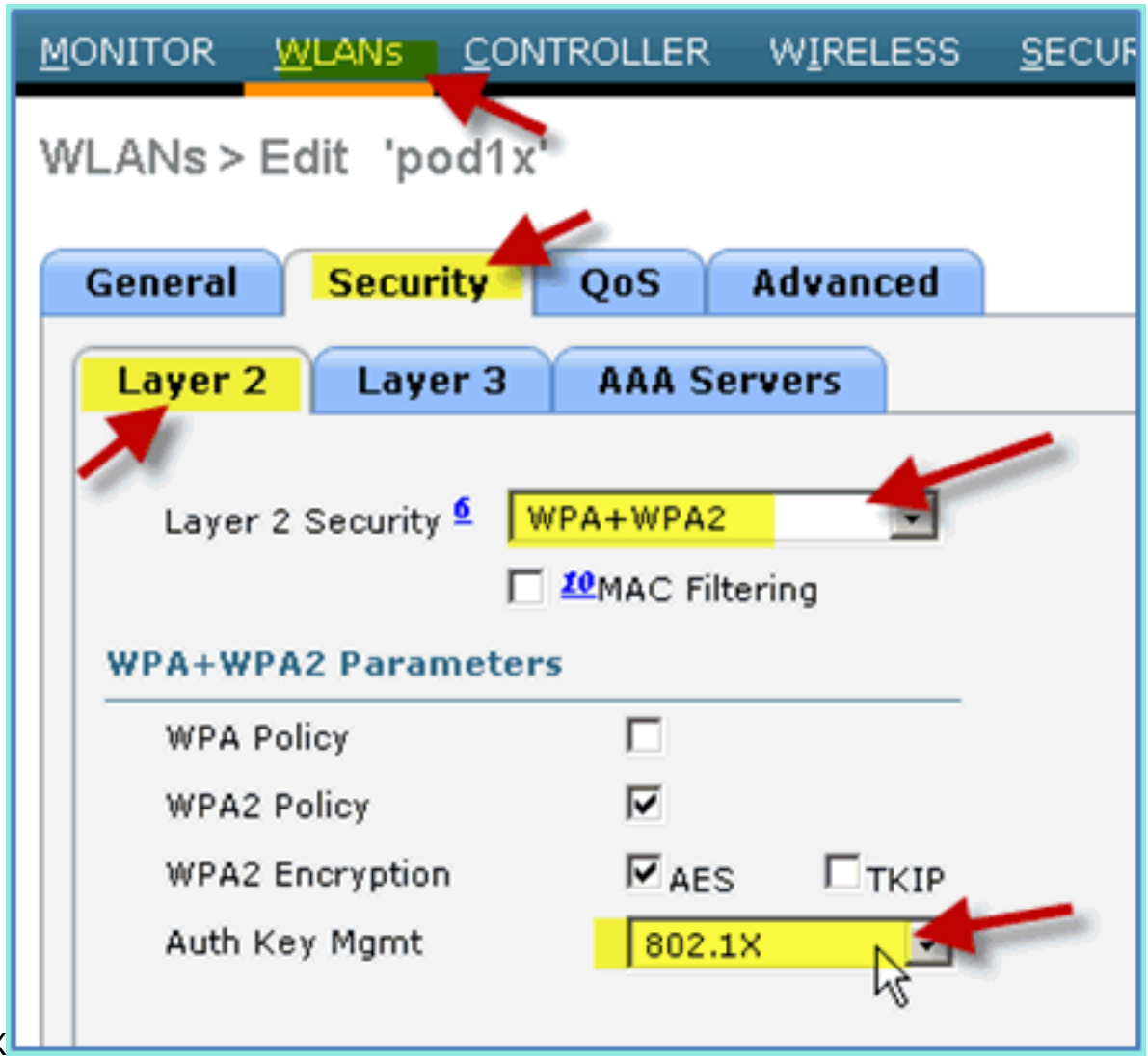
请完成以下步骤：

1. 从WLC导航到**WLAN > Create New**。

2. 对于WLAN，请输入以下命令：配置文件名称：pod1xSSID：相同

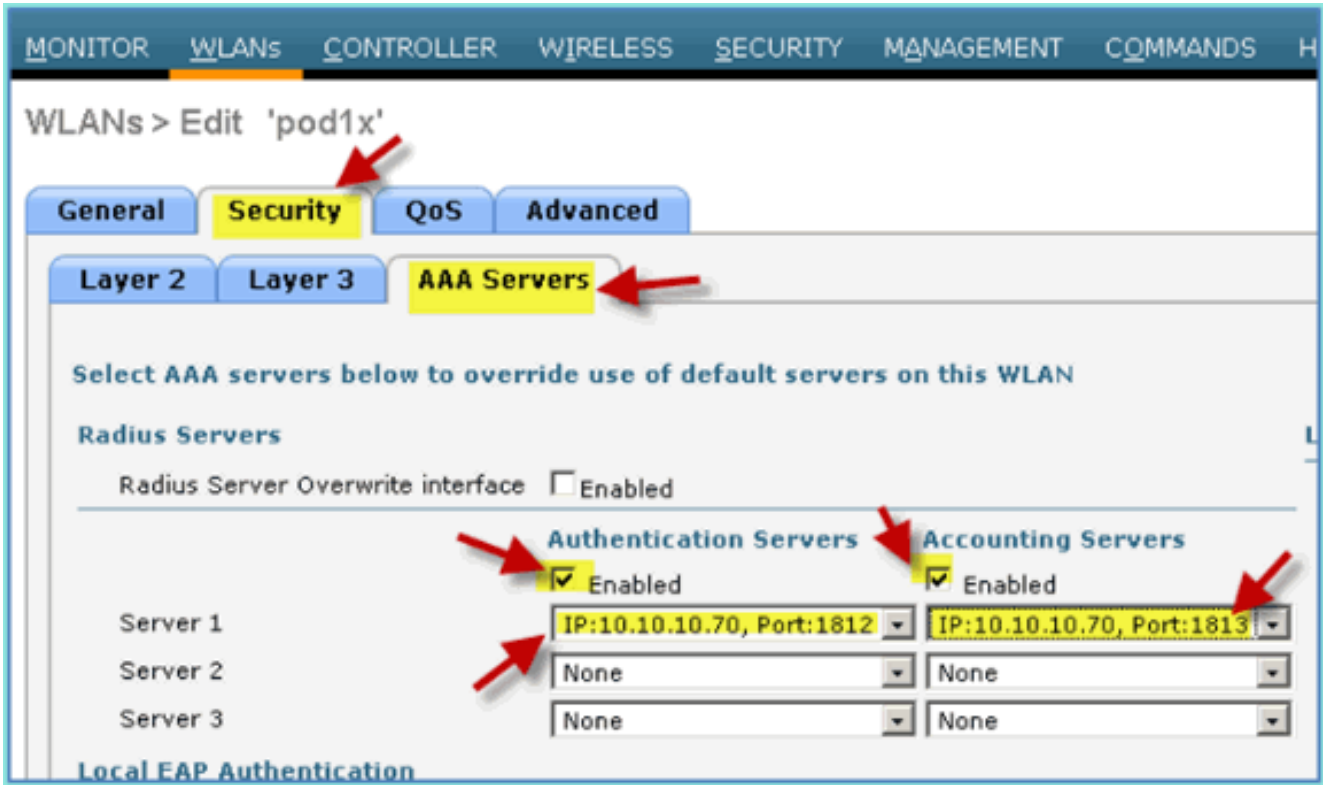
3. 对于WLAN settings > General选项卡，请使用以下命令：无线电策略：全部接口/组：管理其他所有内容：默认

4. 对于WLAN > Security选项卡> Layer 2，请设置以下内容：第2层安全：WPA+WPA2WPA2策略/加密：启用/AES身份验证密钥管理



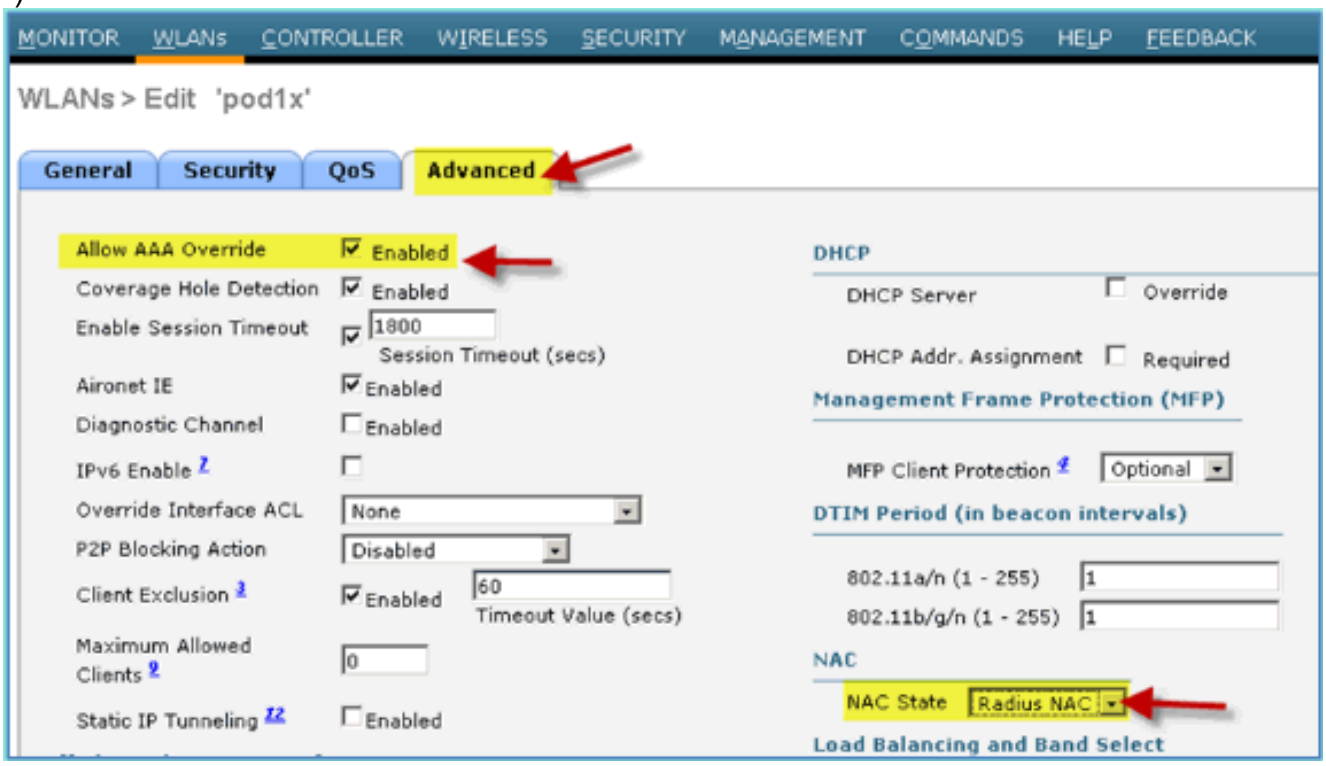
：802.1X

5. 对于WLAN > Security选项卡> AAA Servers，请设置以下内容：无线电服务器覆盖接口：已禁用身份验证/记帐服务器：已启用服务器
1:10.10.10.70

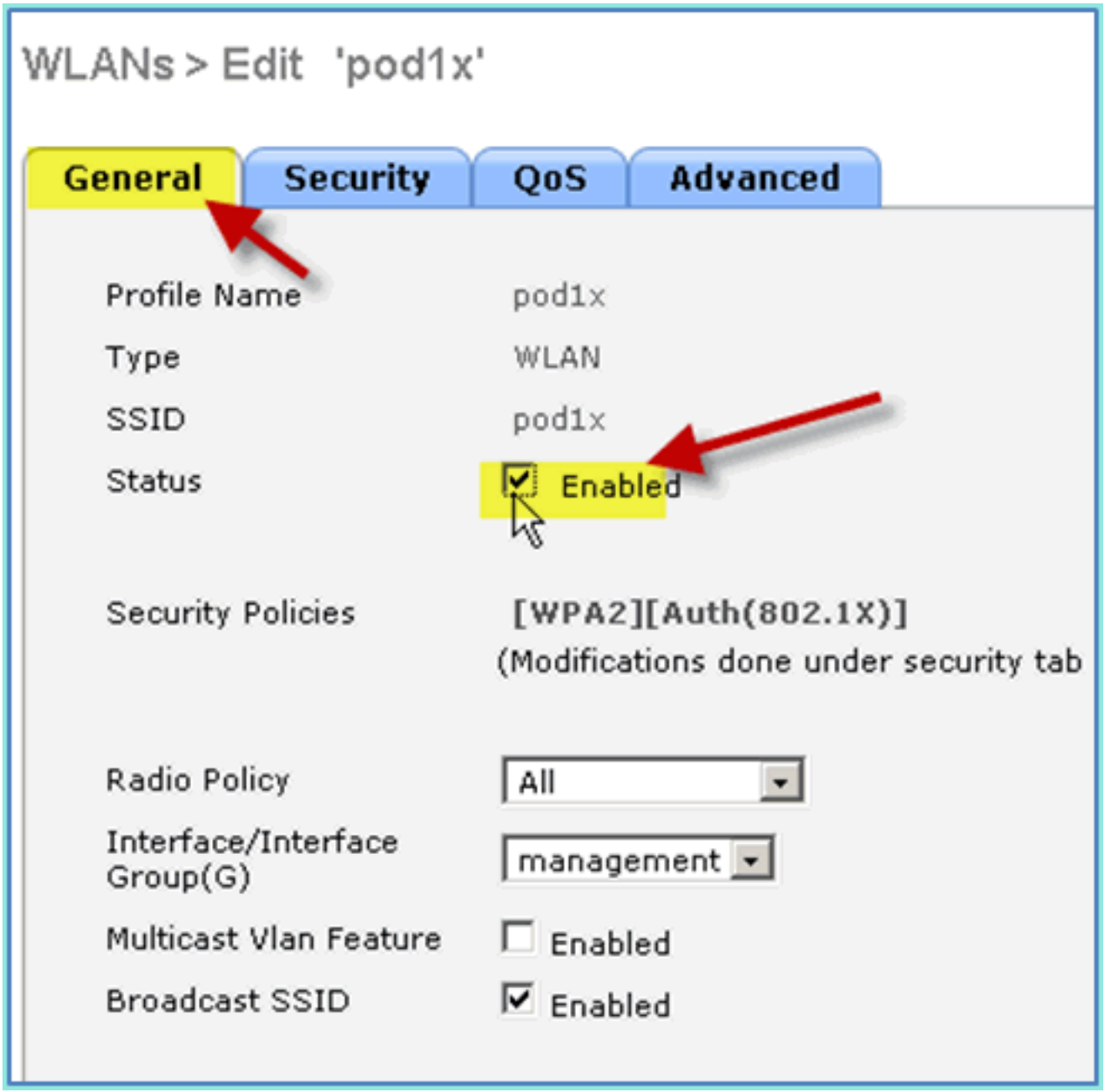


6. 对于WLAN > Advanced选项卡，请设置以下内容：允许AAA覆盖：已启用NAC状态：Radius

NAC（选中
）



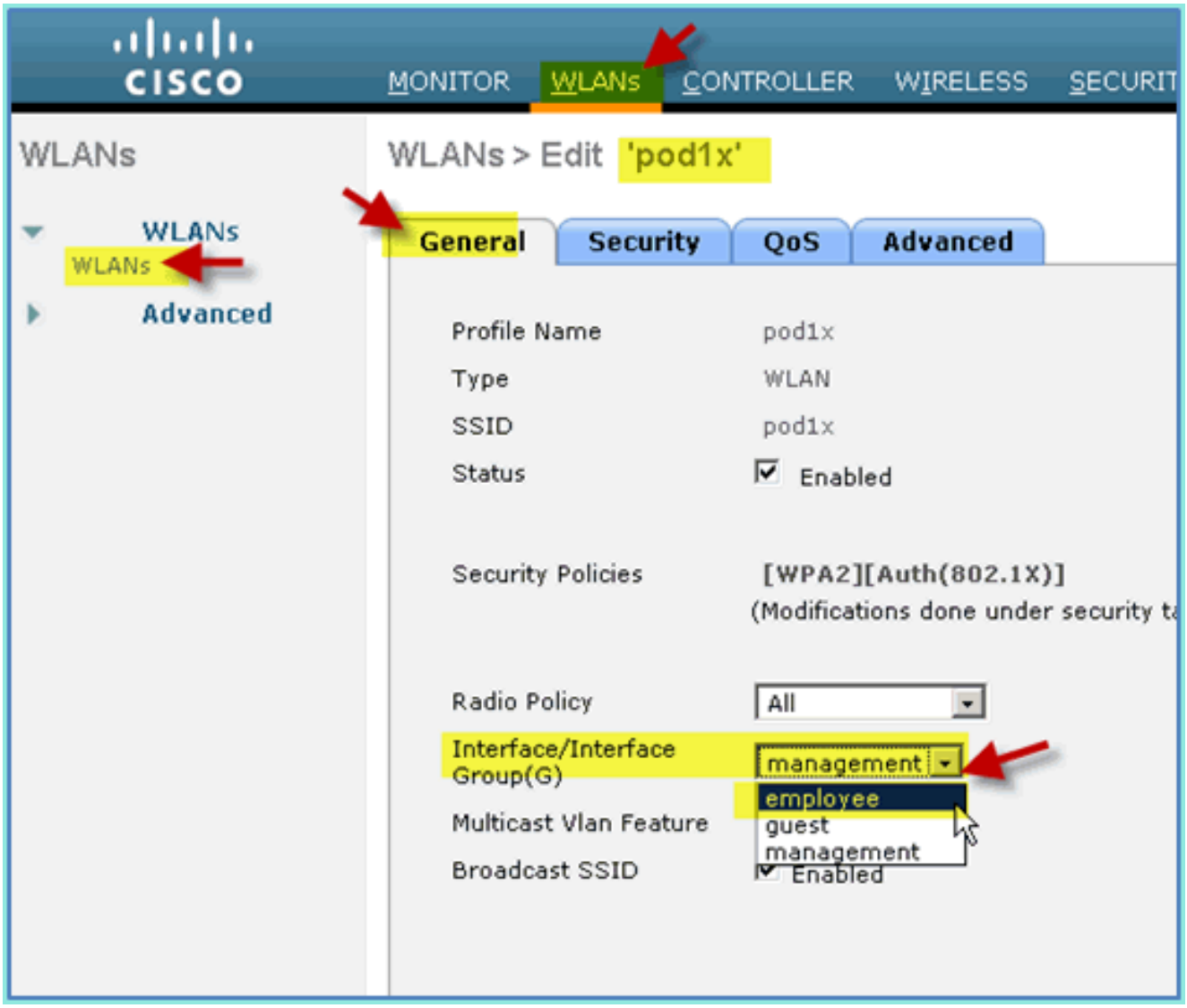
7. 返回WLAN > General选项卡> Enable WLAN（复选框）。



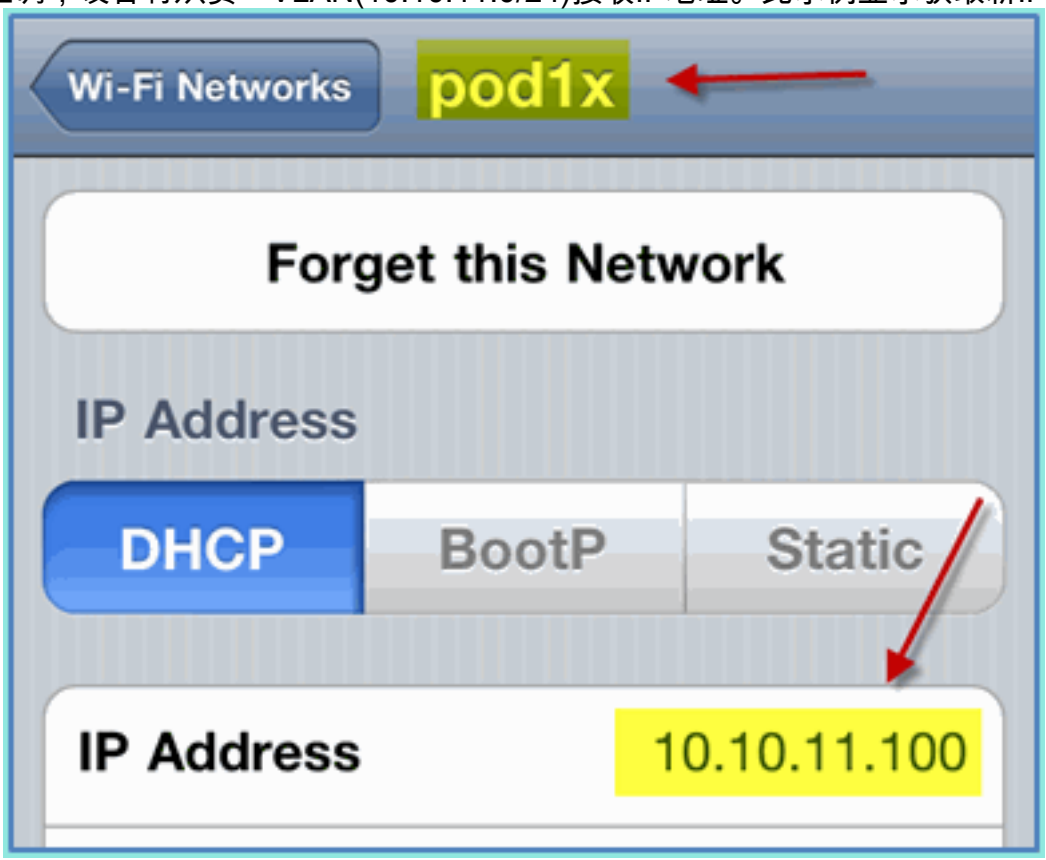
测试WLC动态接口

您需要快速检查有效的员工和访客接口。使用任何设备与WLAN关联，然后更改WLAN接口分配。

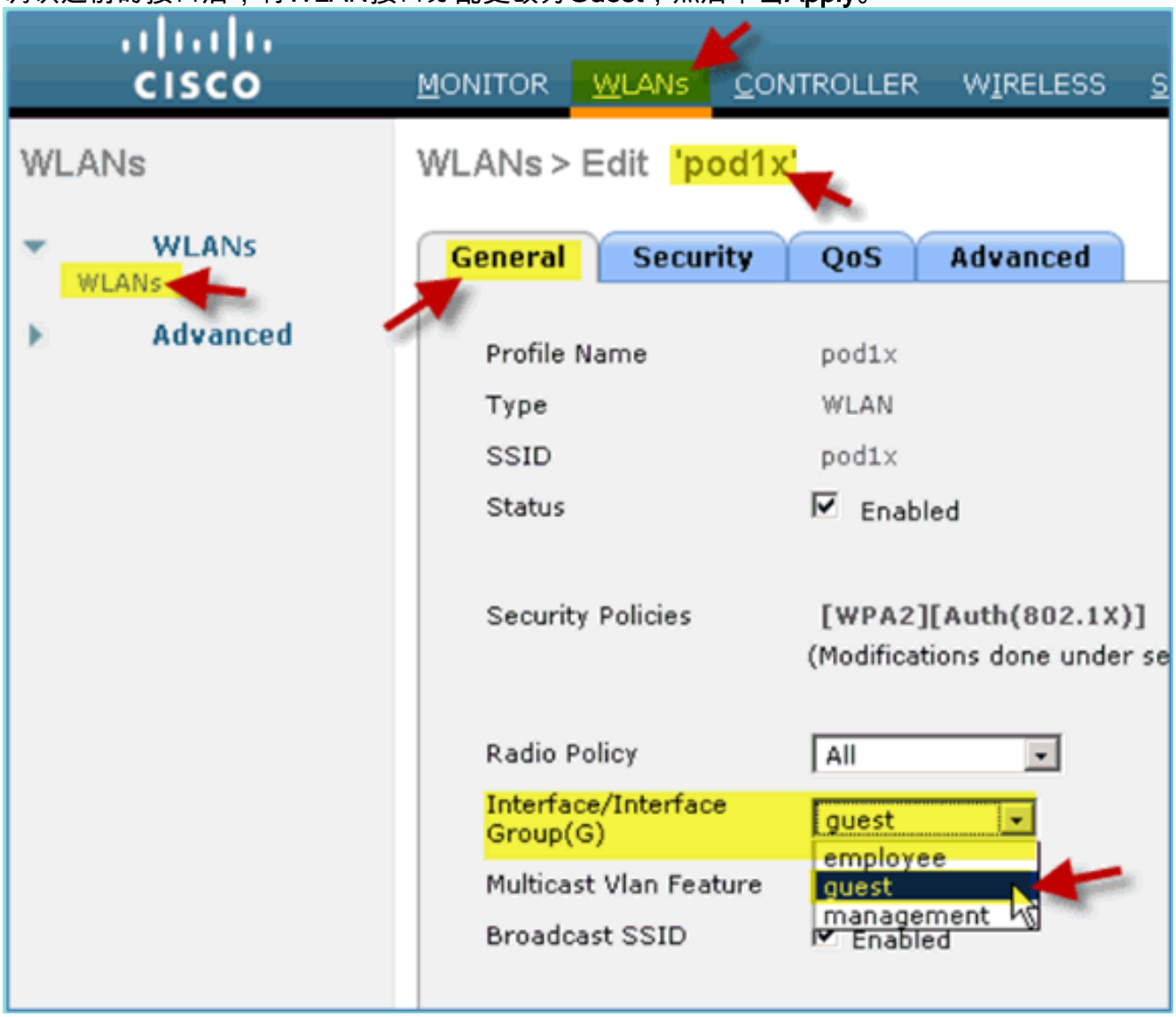
1. 从WLC导航到**WLAN > WLANs**。单击以编辑在前面的练习中创建的安全SSID。
2. 将Interface/Interface Group更改为**Employee**，然后单击**Apply**。



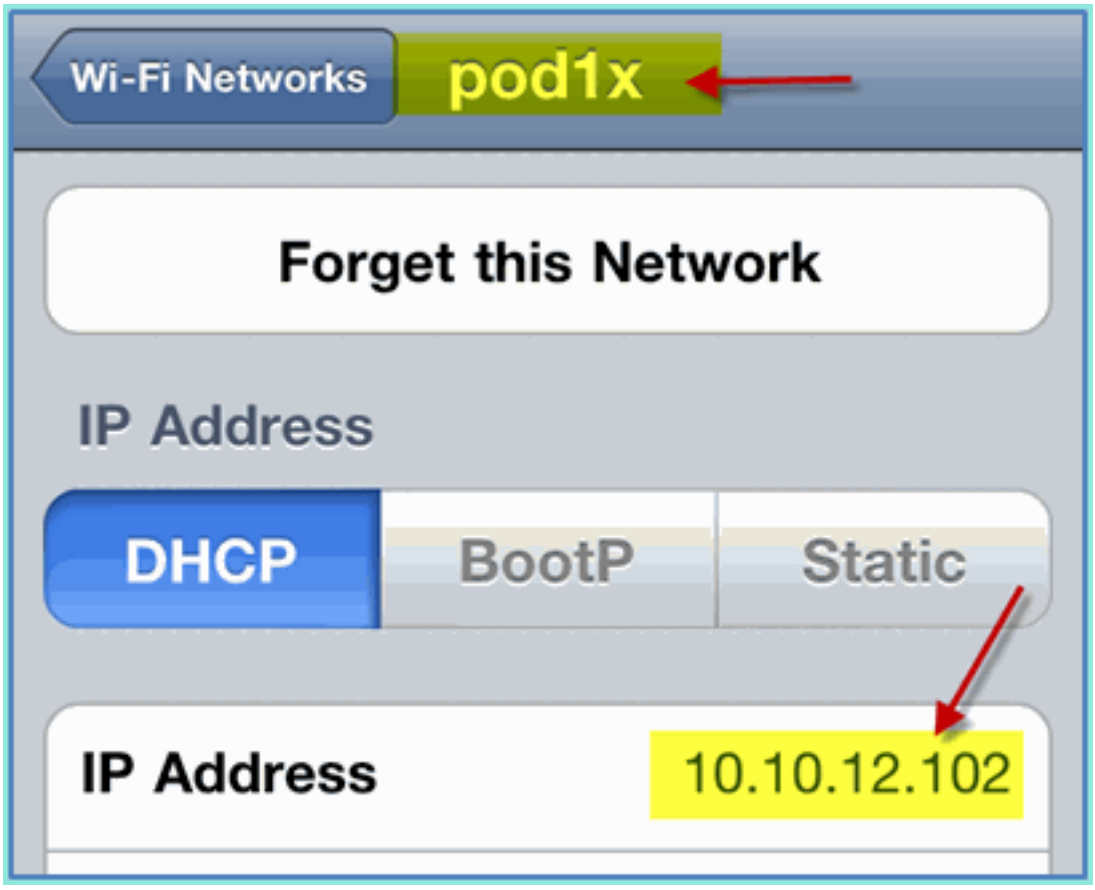
3. 如果配置正确，设备将从员工VLAN(10.10.11.0/24)接收IP地址。此示例显示获取新IP地址的iOS设备。



4. 确认之前的接口后，将WLAN接口分配更改为**Guest**，然后单击**Apply**。



5. 如果配置正确，设备将从访客VLAN(10.10.12.0/24)接收IP地址。此示例显示获取新IP地址的



iOS设备。

6. **重要信息**：将接口分配更改回原始管理。
7. 单击Apply并保存WLC的配置。

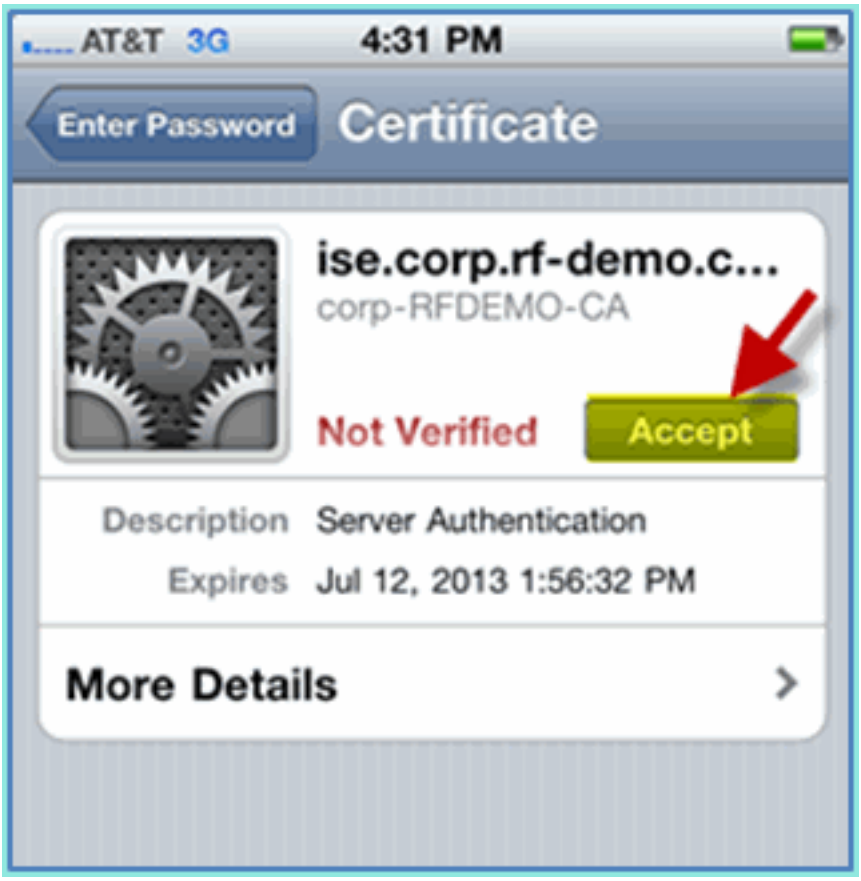
iOS无线身份验证(iPhone/iPad)

使用iPhone、iPad或iPod等iOS设备，通过经过身份验证的SSID与内部用户（或集成的AD用户）关联到WLC。如果不适用，请跳过这些步骤。

1. 在iOS设备上，转到WLAN设置。启用WIFI，然后选择上一节中创建的启用802.1X的SSID。
2. 提供以下信息以连接：用户名：员工（内部 — 员工）或承包商（内部 — 承包商）密码

: XXXX

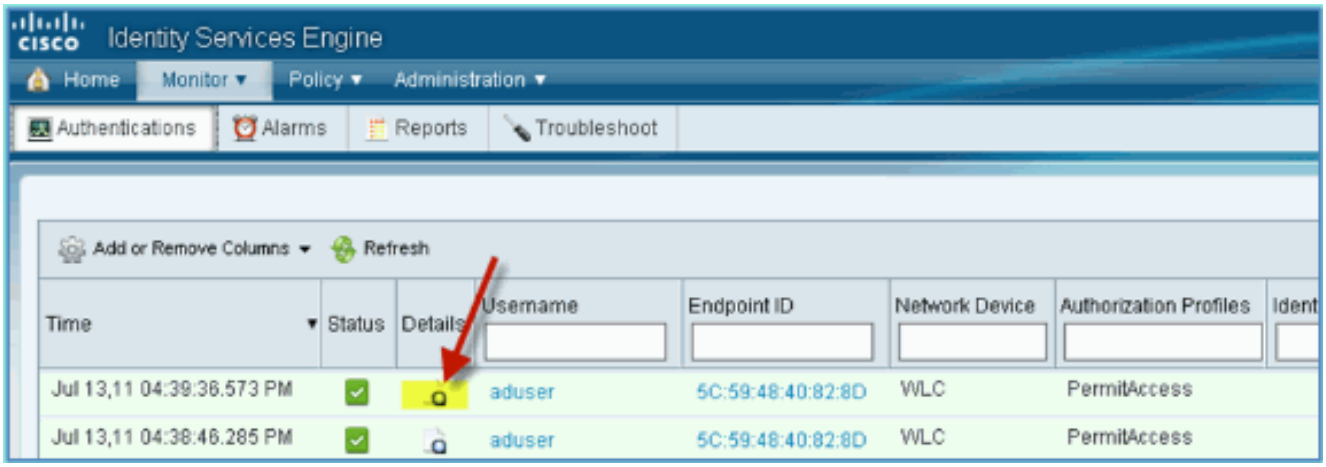

AT&T
4:31 PM
Enter the password for "pod1x"
Cancel
Enter Password
Username
aduser
Password
Mode
Automatic
1 2 3 4 5 6 7 8 9 0
- / : ; ( ) $ & @ "
#+= . , ? ! '
ABC
space
Join



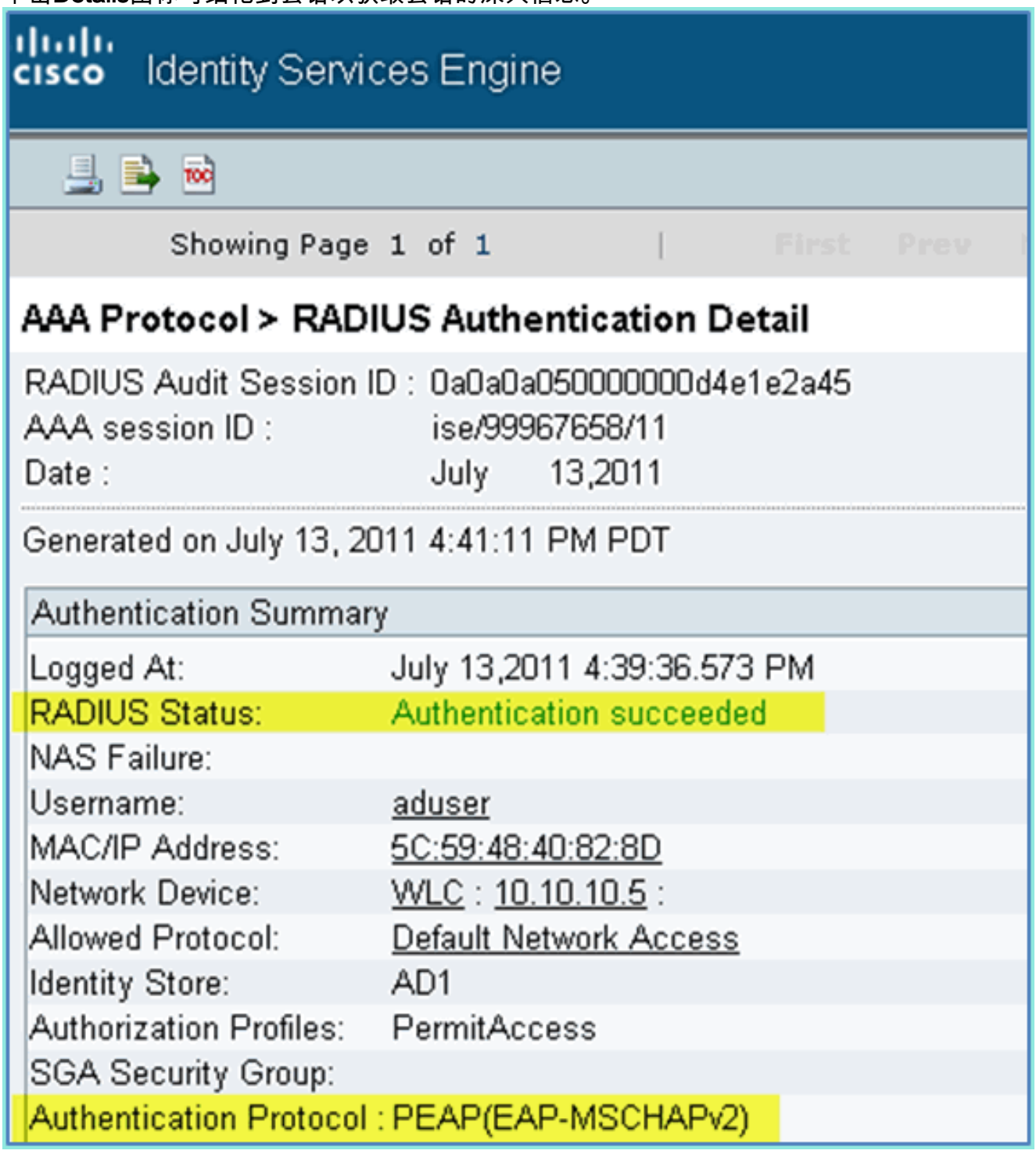
3. 单击以接受ISE证书。
4. 确认iOS设备正在从管理(VLAN10)接口获取IP地址。

5. 在WLC > Monitor > Clients上，验证终端信息，包括使用、状态和EAP类型。

6. 同样，客户端信息可以由ISE > Monitor > Authentication页面提供。



7. 单击**Details**图标可细化到会话以获取会话的深入信息。

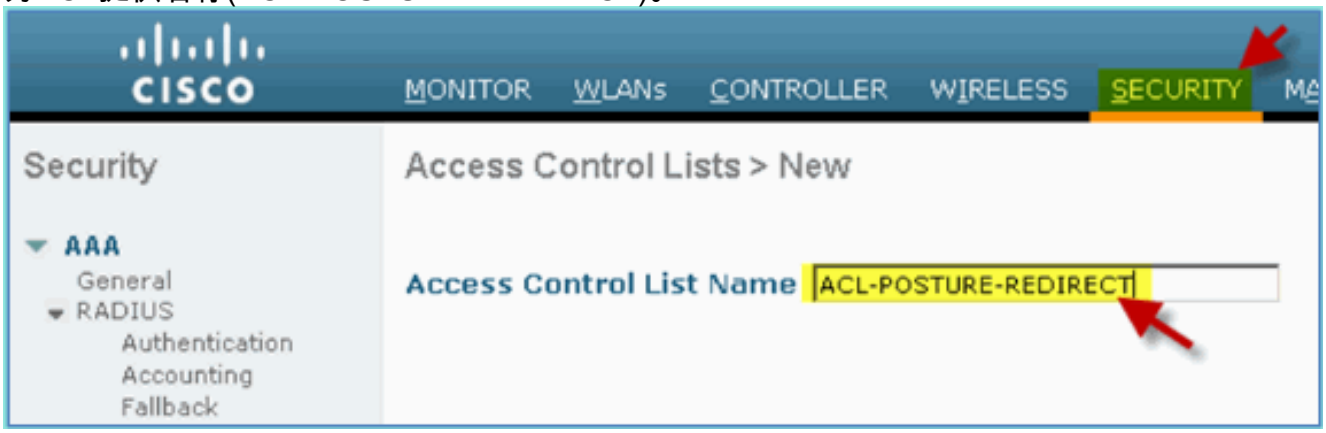


将状态重定向ACL添加到WLC

在WLC上配置终端安全评估重定向ACL，ISE将用于限制客户端的终端安全评估。ACL至少有效地允许ISE之间的流量。如果需要，可以在此ACL中添加可选规则。

1. 导航到**WLC > Security > Access Control Lists > Access Control Lists**。单击 **New**。

2. 为ACL提供名称(ACL-POSTURE-REDIRECT)。

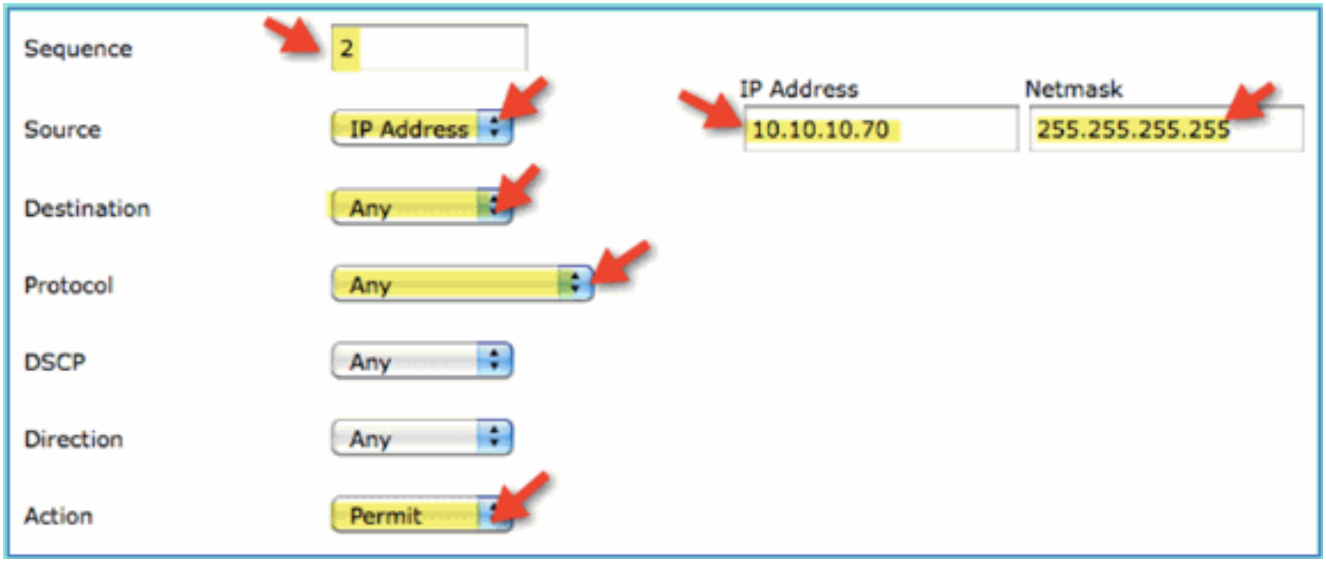


3. 单击**Add New Rule**以添加新ACL。将以下值设置为ACL序列#1。完成后单击**Apply**。来源：任意目的：IP地址10.10.10.70、255.255.255.255协议：任意操作：允许

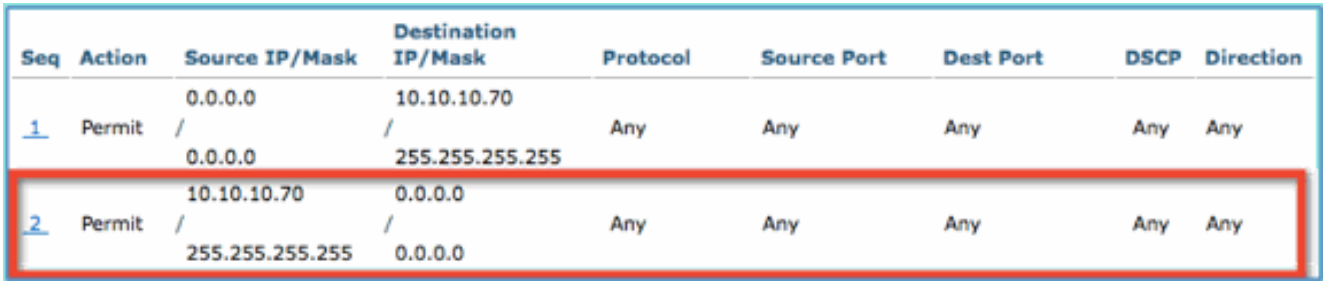
4. 已添加确认序列。

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

5. 单击 **Add New Rule**。将以下值设置为ACL序列#2。完成后单击**Apply**。来源：IP地址10.10.10.70、255.255.255.255目标：任意协议：任意操作：允许

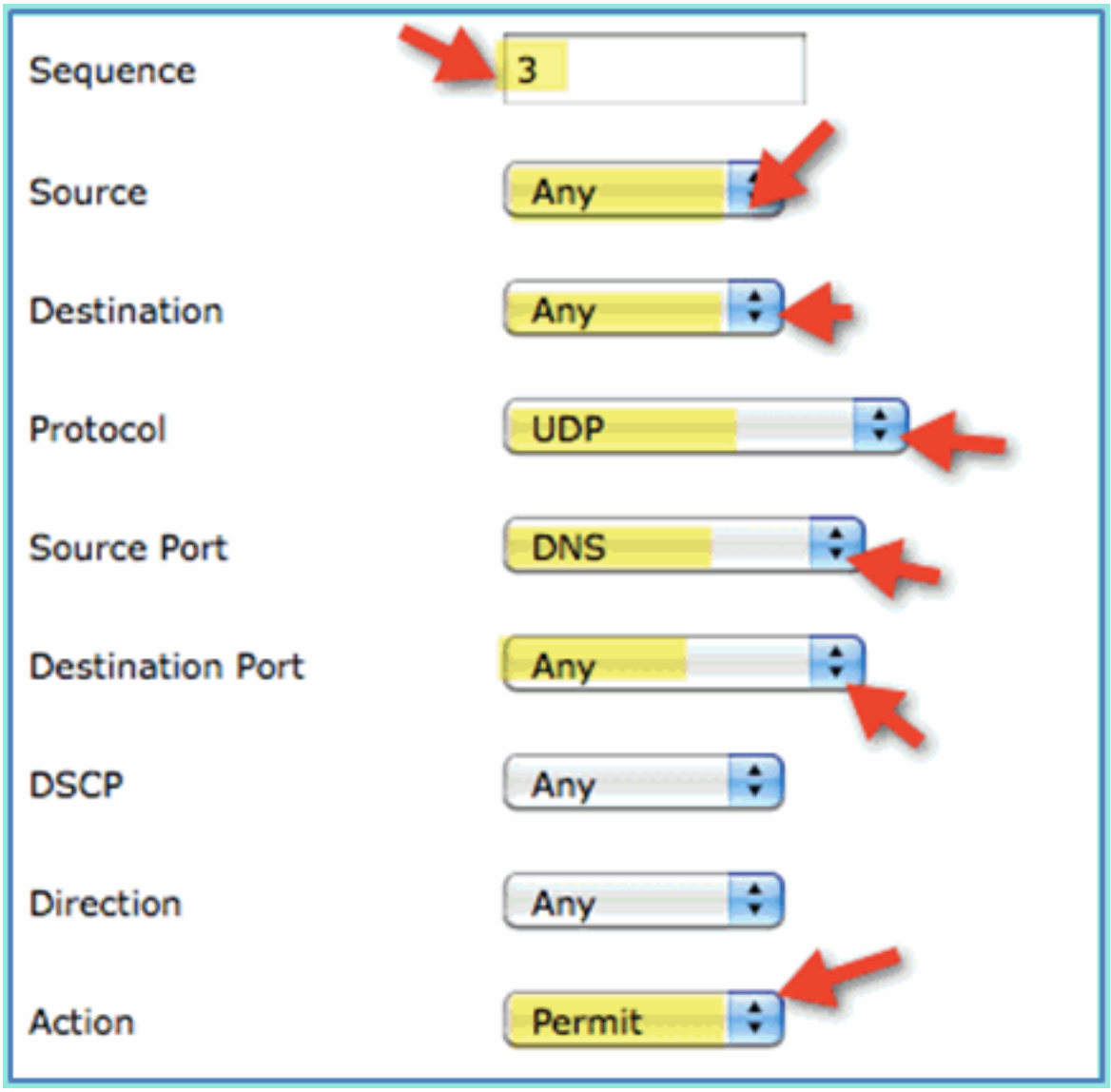


6. 已添加确认序列。



Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any

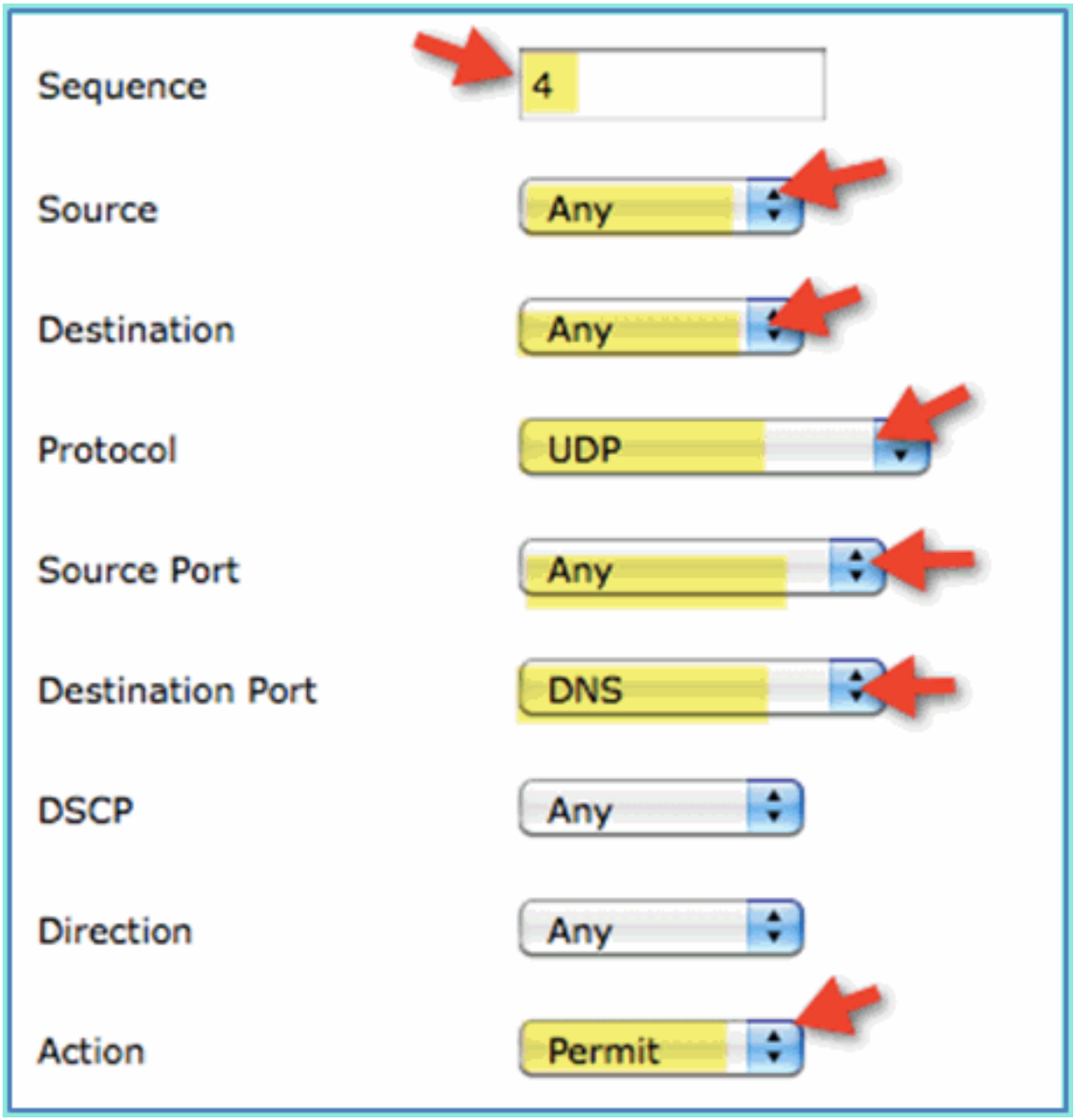
7. 将以下值设置为ACL序列#3。完成后单击**Apply**。来源：任意目标：任意协议：UDP源端口：DNS目标端口：任意操作：允许



8. 已添加确认序列。

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any

9. 单击 **Add New Rule**。将以下值设置为ACL序列#4。完成后单击**Apply**。来源：任意目标：任意协议：UDP源端口：任意目标端口：DNS操作：允许



10. 已添加确认序列。

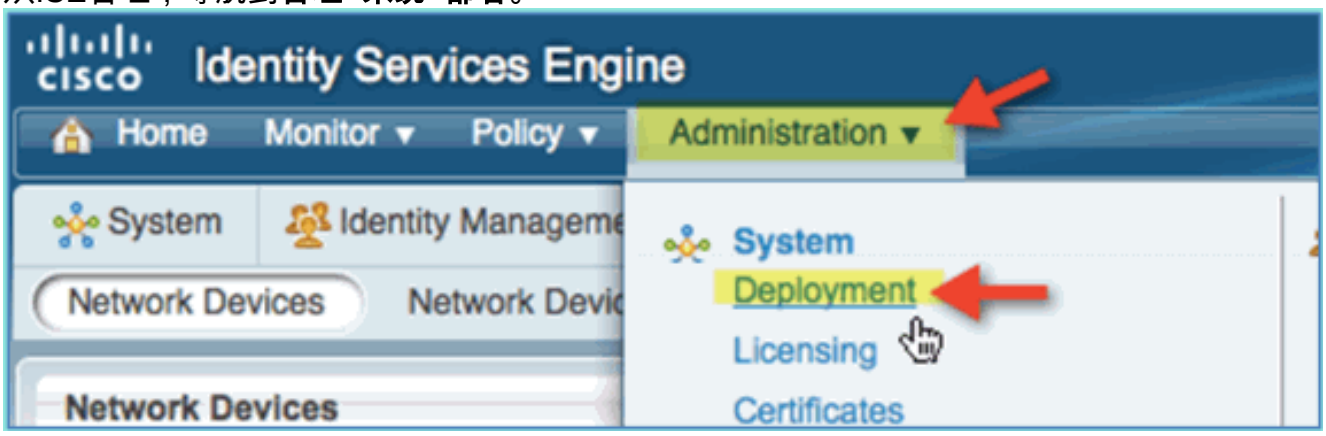
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any

11. 保存当前WLC配置。

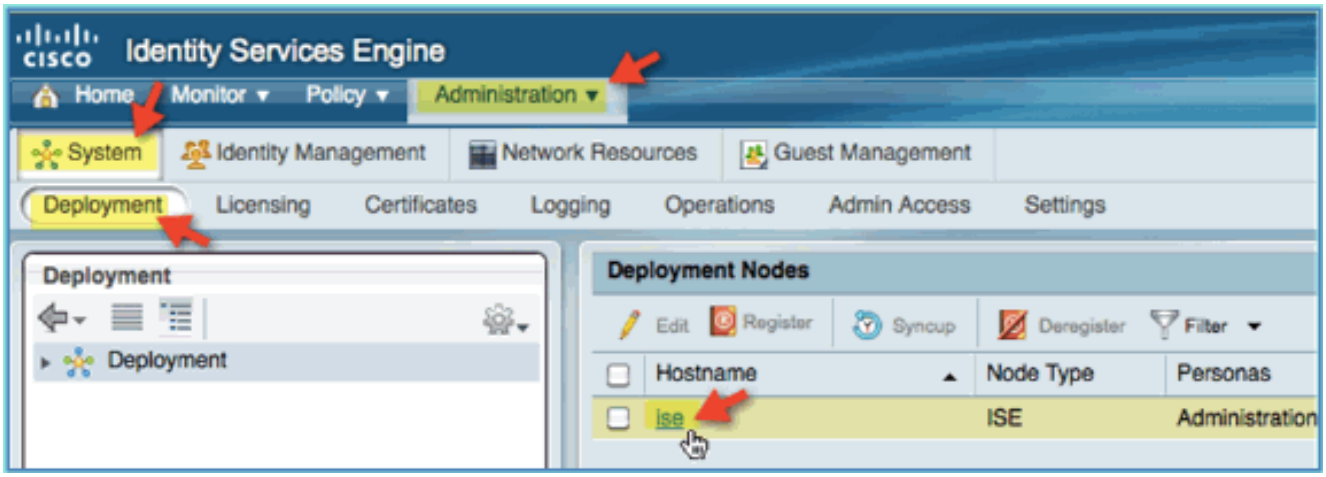
在ISE上启用分析探测

需要将ISE配置为探测功能以有效地分析终端。默认情况下，这些选项处于禁用状态。本节介绍如何将ISE配置为探测功能。

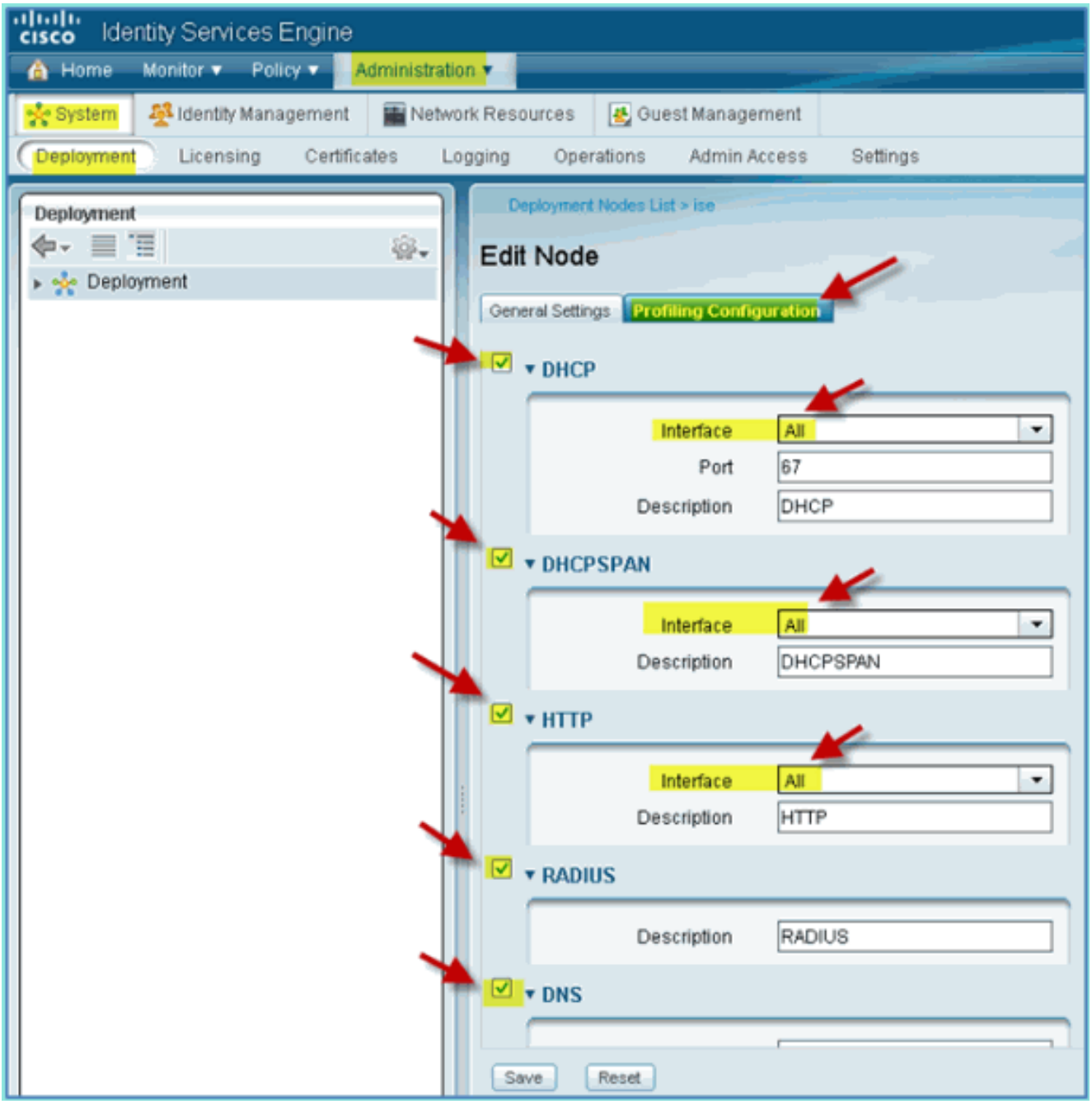
1. 从ISE管理，导航到**管理>系统>部署**。



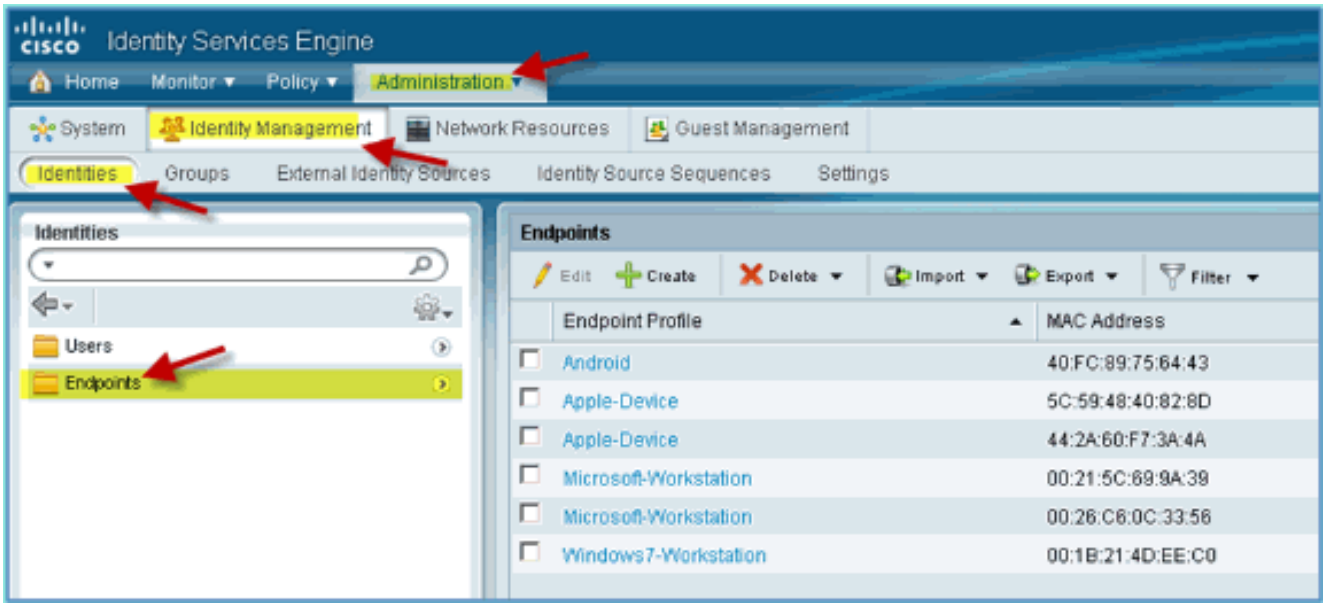
2. 选择**ISE**。单击**Edit ISE host**。



3. 从Edit Node页中，选择Profiling Configuration并配置以下内容：DHCP：启用、全部（或默认）DHCPSPAN：启用、全部（或默认）HTTP：启用、全部（或默认）RADIUS：已启用，不适用DNS：已启用，不适用



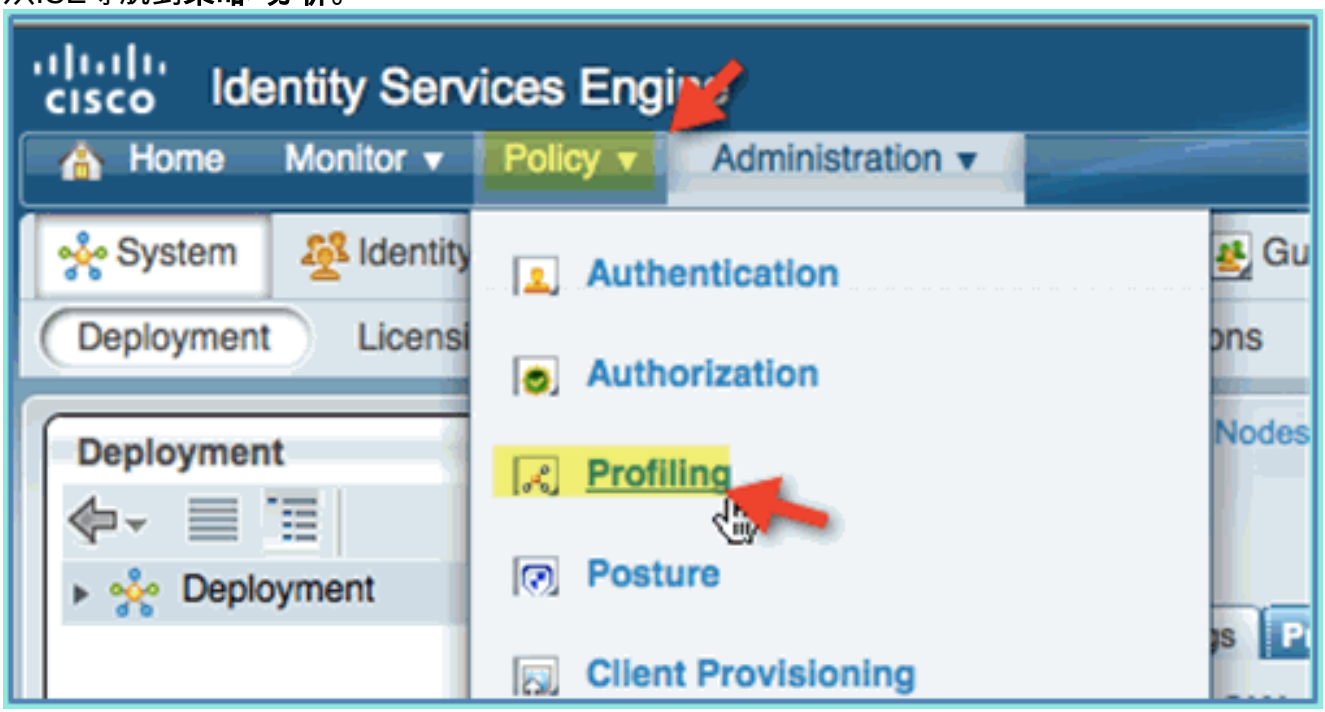
4. 重新关联设备（iPhone/iPad/Droids/Mac等）。
5. 确认ISE终端身份。导航到**Administration > Identity Management > Identities**。点击Endpoints以列出已分析的内容。**注意**：初始分析来自RADIUS探测器。



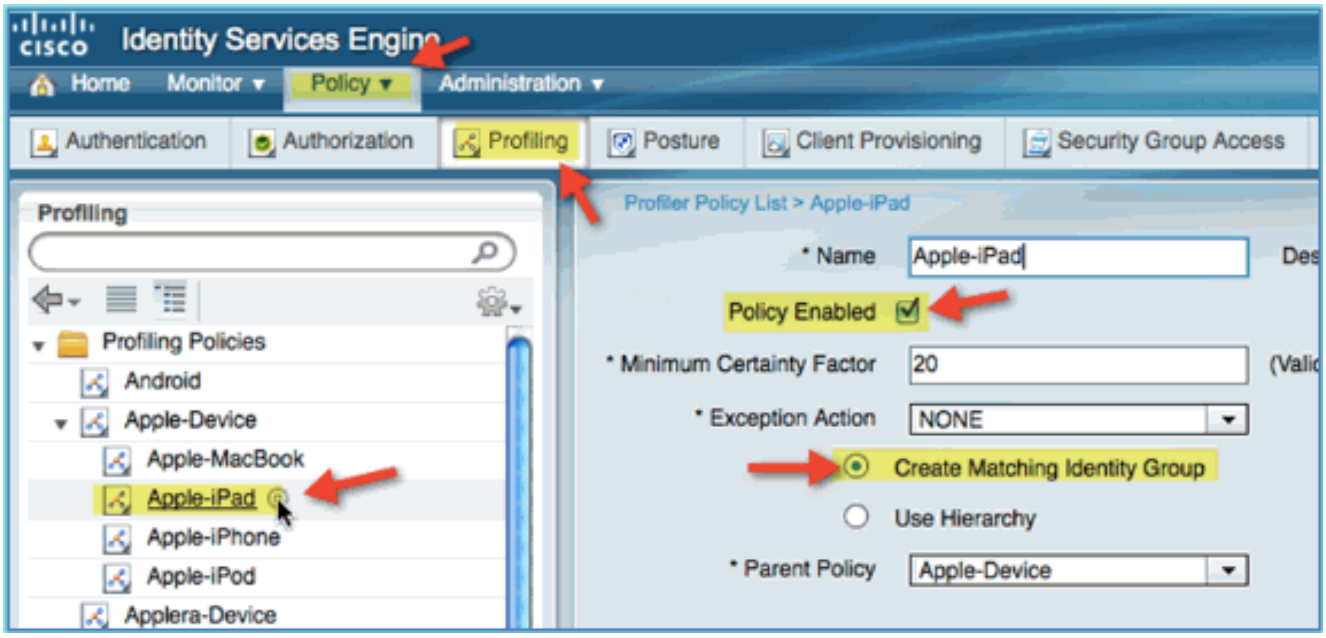
为设备启用ISE配置文件策略

ISE开箱即用提供各种终端配置文件库。要启用设备的配置文件，请完成以下步骤：

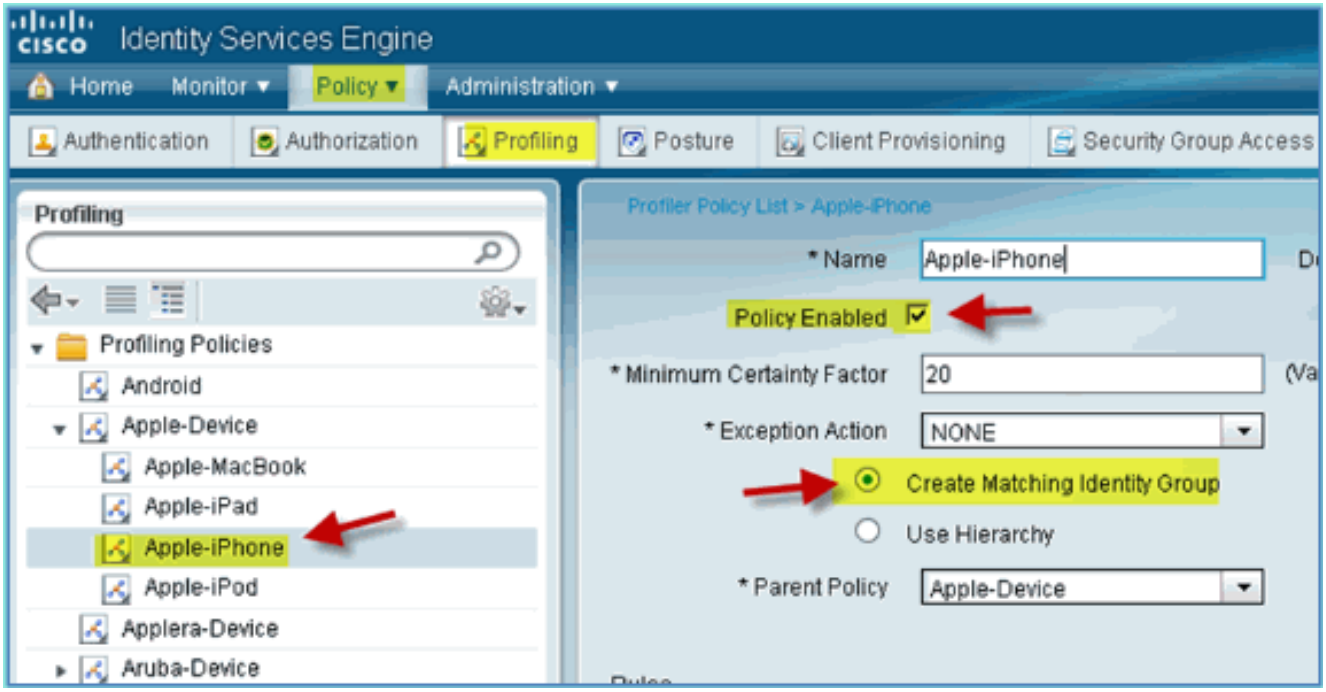
1. 从ISE导航到**策略>分析**。



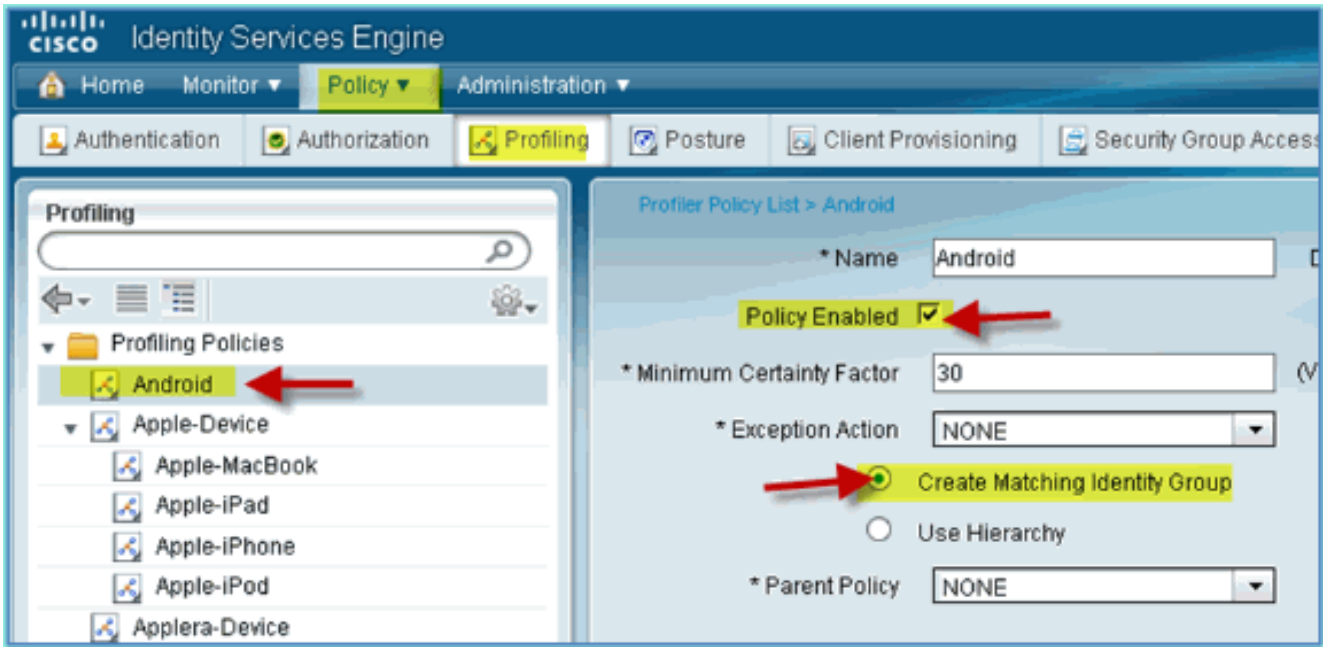
2. 在左侧窗格中，展开**分析策略**。
3. 单击**Apple Device > Apple iPad**，然后设置以下项：策略已启用：已启用创建匹配的身份组：已选择



4. 单击**Apple Device > Apple iPhone**，设置以下项：策略已启用：已启用创建匹配的身份组：已选择



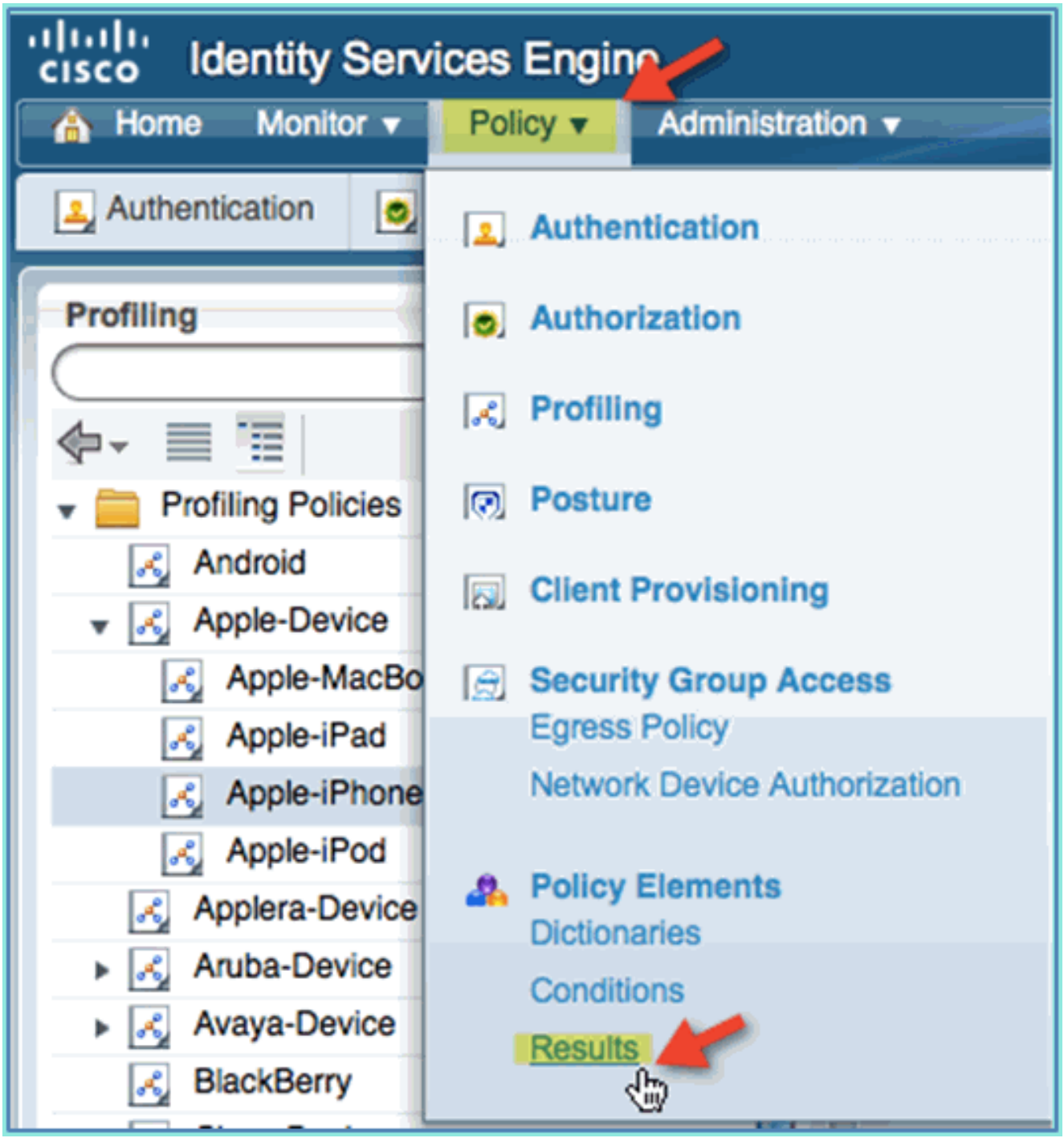
5. 单击**Android**，设置以下项：策略已启用：已启用创建匹配的身份组：已选择



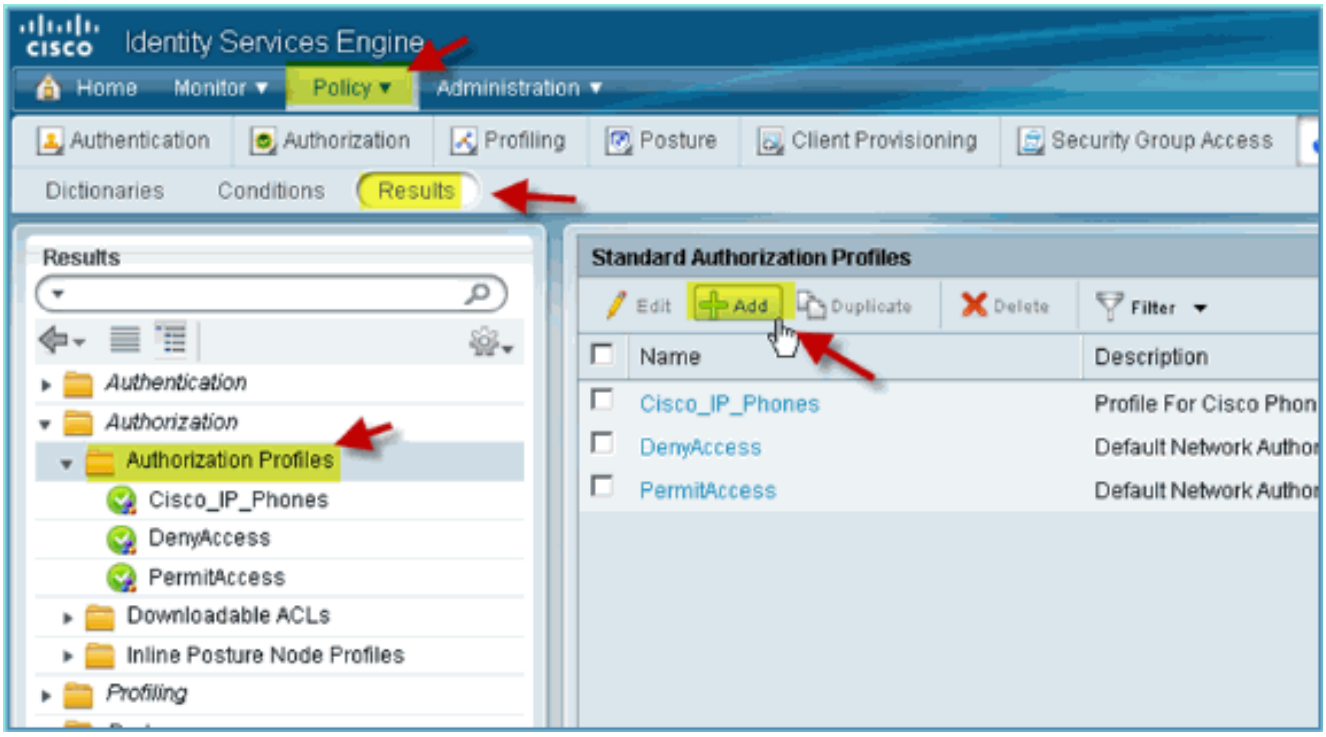
终端安全评估发现重定向的ISE授权配置文件

完成以下步骤以配置授权策略状态重定向，允许将新设备重定向到ISE进行适当的发现和分析：

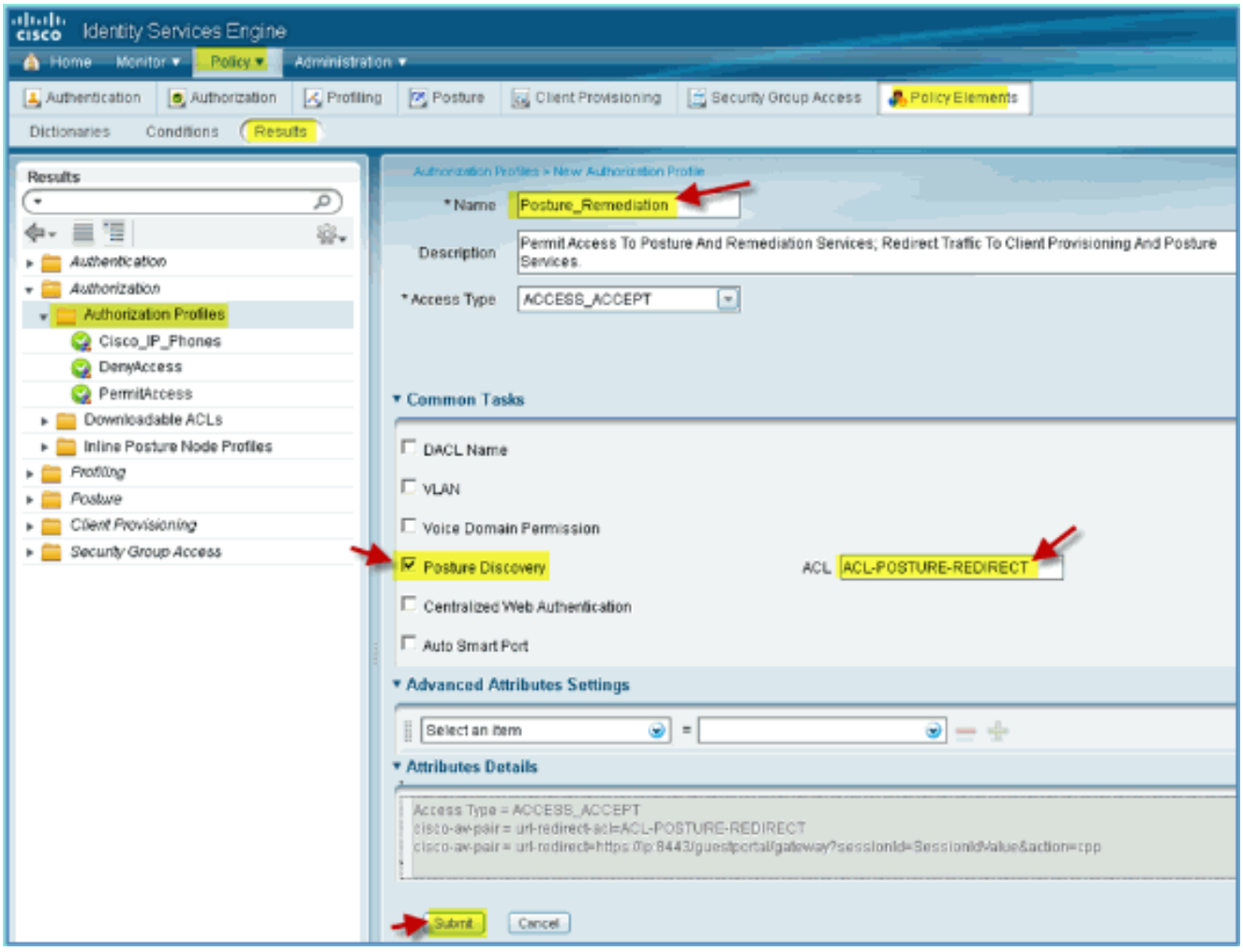
1. 从ISE，导航到**策略>策略元素>结果**。



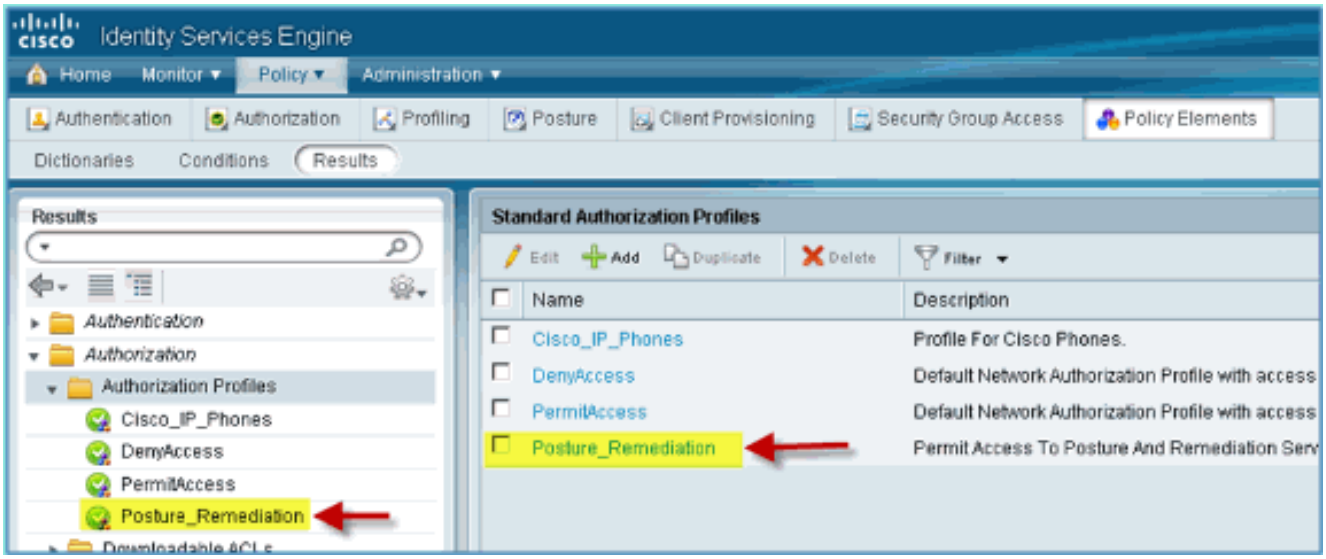
2. 展开**授权**。单击**Authorization Profiles**（左窗格），然后单击**Add**。



3. 使用以下内容创建授权配置文件：名称：Posture_Remediation访问类型：Access_Accept常用工具：状态发现，已启用状态发现、ACL ACL-POSTURE-REDIRECT



4. 单击**Submit**完成此任务。
5. 确认已添加新的授权配置文件。

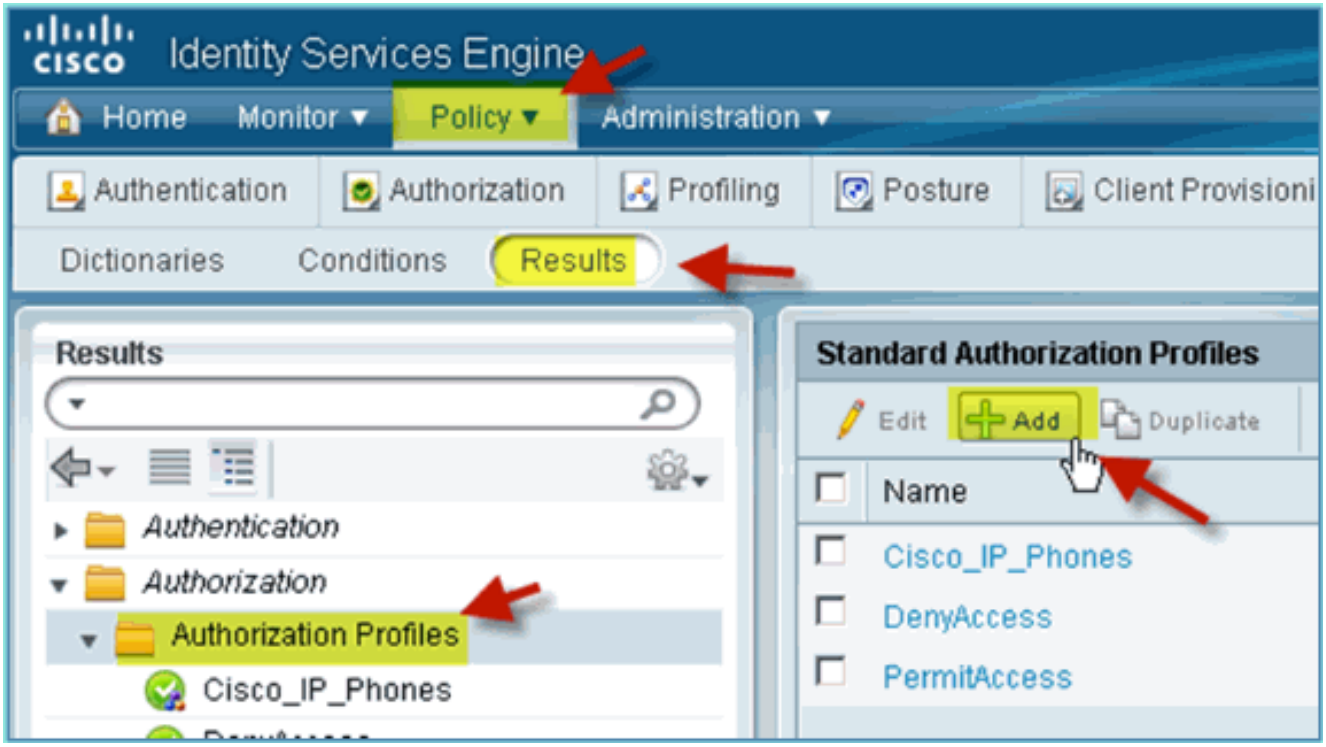


为员工创建ISE授权配置文件

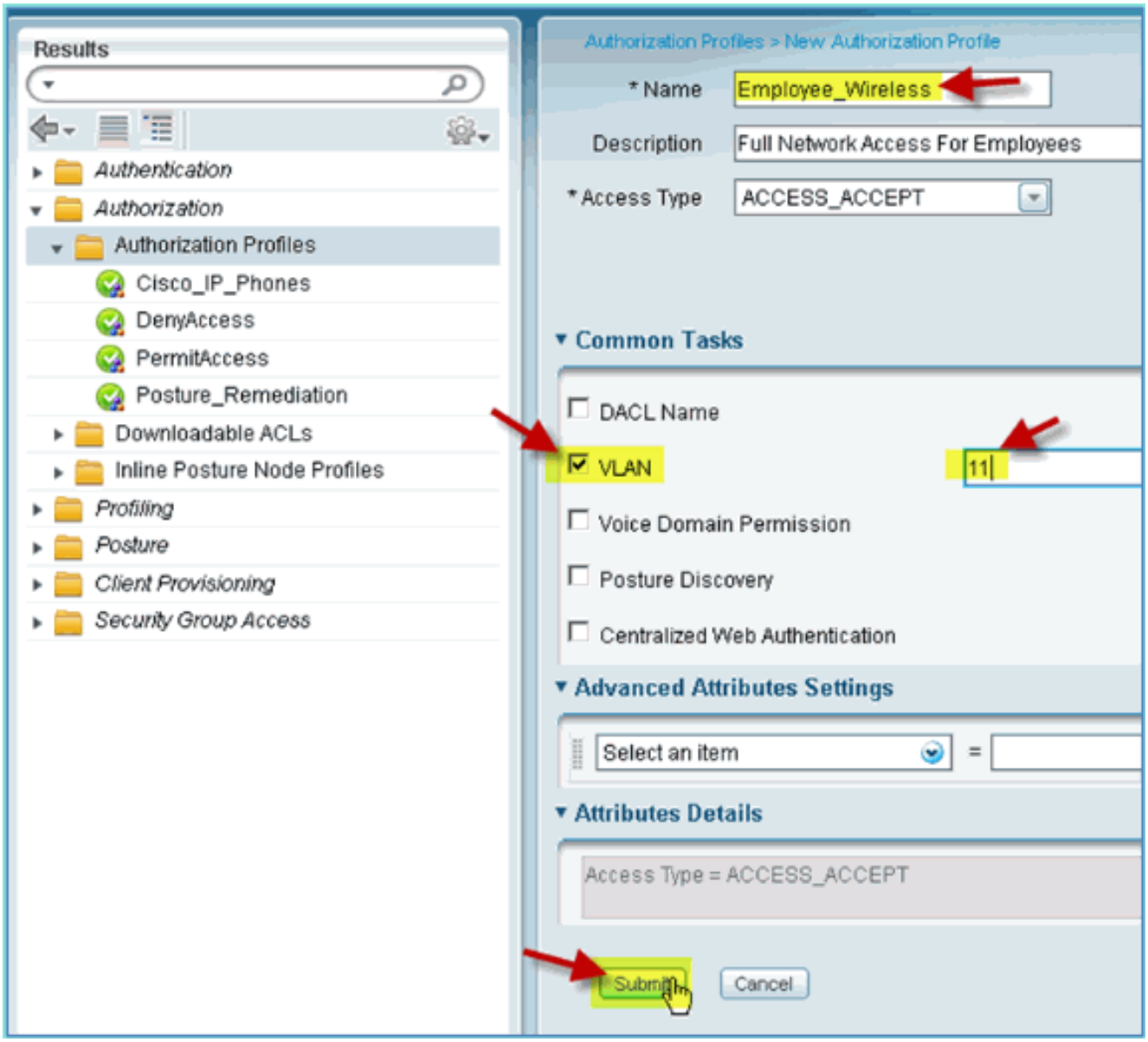
添加员工的授权配置文件允许ISE授权和允许具有已分配属性的访问。本例中分配了员工VLAN 11。

请完成以下步骤：

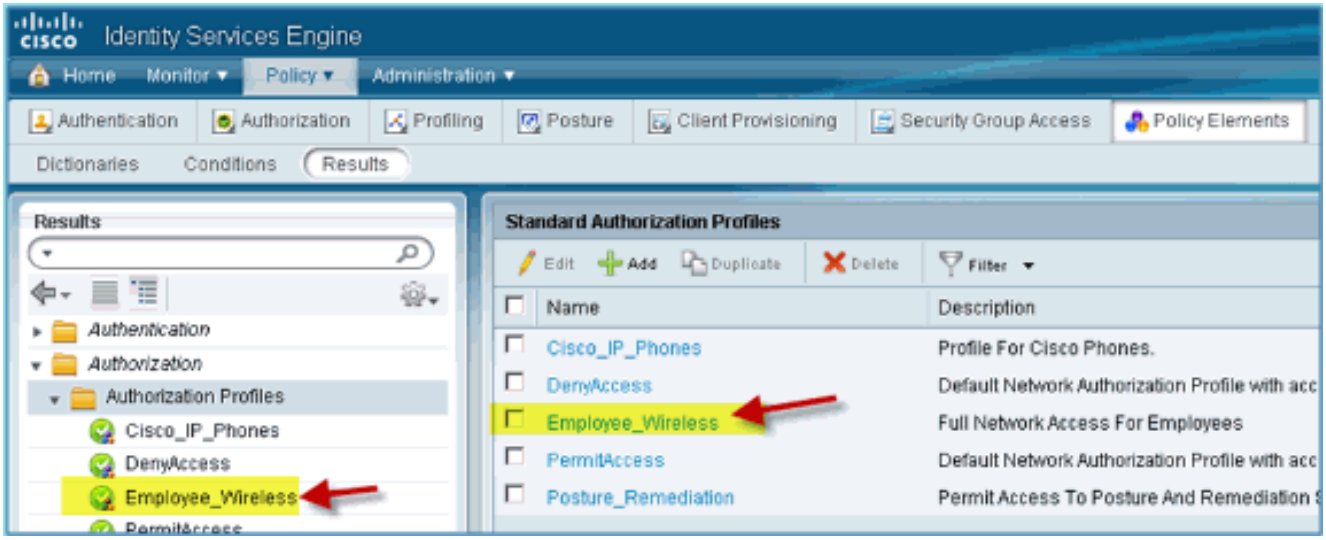
1. 从ISE导航到**策略>结果**。展开**Authorization**，然后单击**Authorization Profiles**，然后单击**Add**。



2. 为员工授权配置文件输入以下内容：名称：Employee_Wireless常见任务:VLAN，已启用VLAN，子值11
3. 单击**Submit**完成此任务。



4. 确认已创建新的员工授权配置文件。

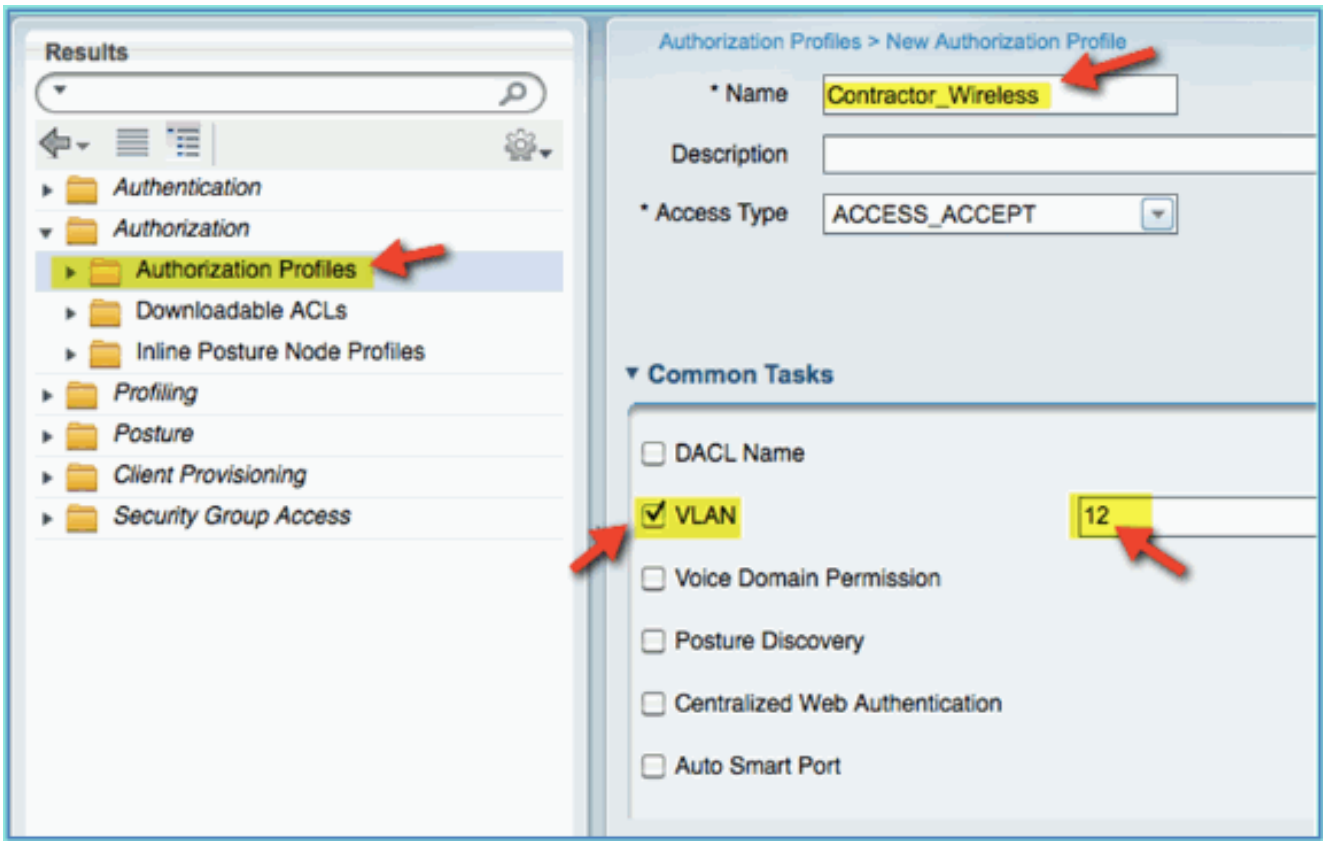


为承包商创建ISE授权配置文件

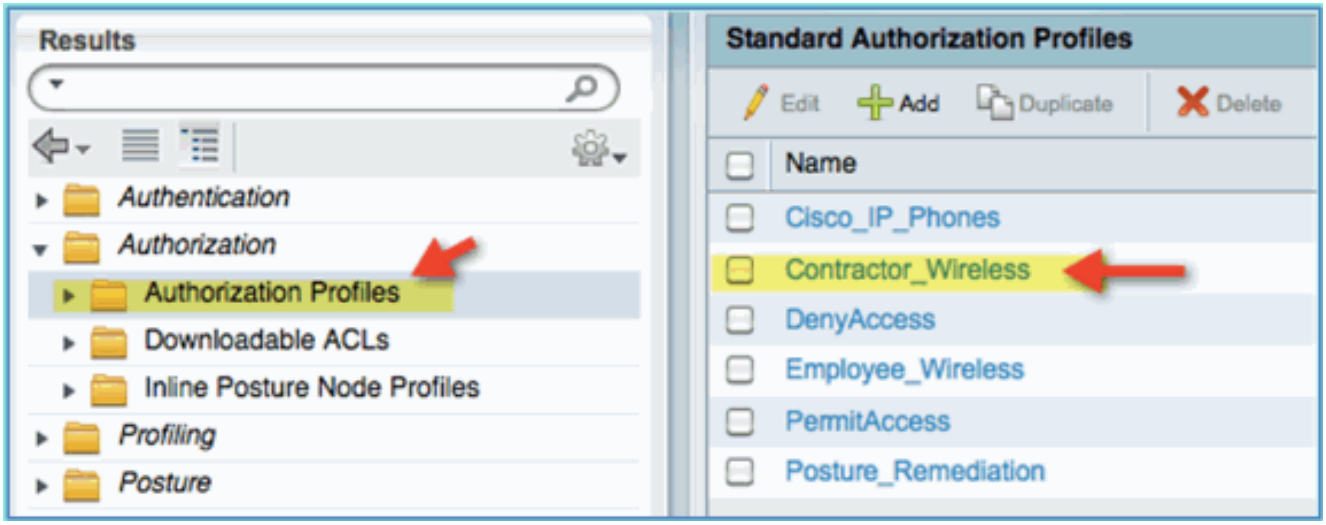
为承包商添加授权配置文件允许ISE授权和允许具有已分配属性的访问。在本例中，分配了承包商VLAN 12。

请完成以下步骤：

1. 从ISE导航到**策略>结果**。展开**Authorization**，然后单击**Authorization Profiles**，然后单击**Add**。
2. 为员工授权配置文件输入以下内容：名称：Employee_Wireless常见任务:VLAN，已启用VLAN，子值
   12



3. 单击**Submit**完成此任务。
4. 确认已创建承包商授权配置文件。

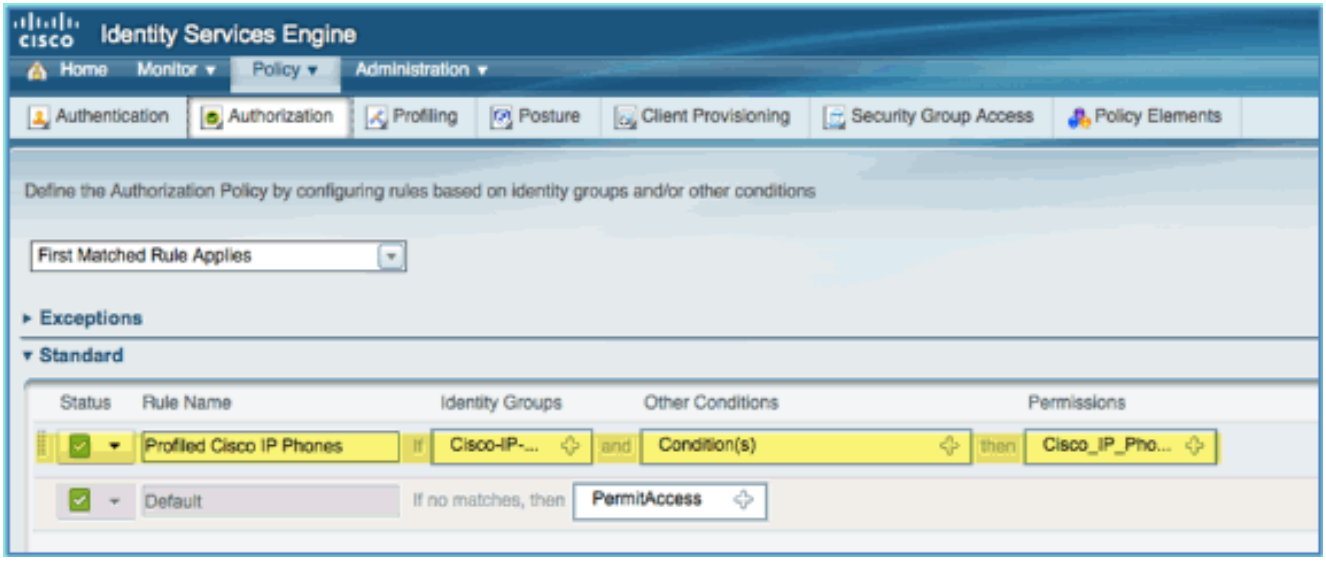


设备状态/分析的授权策略

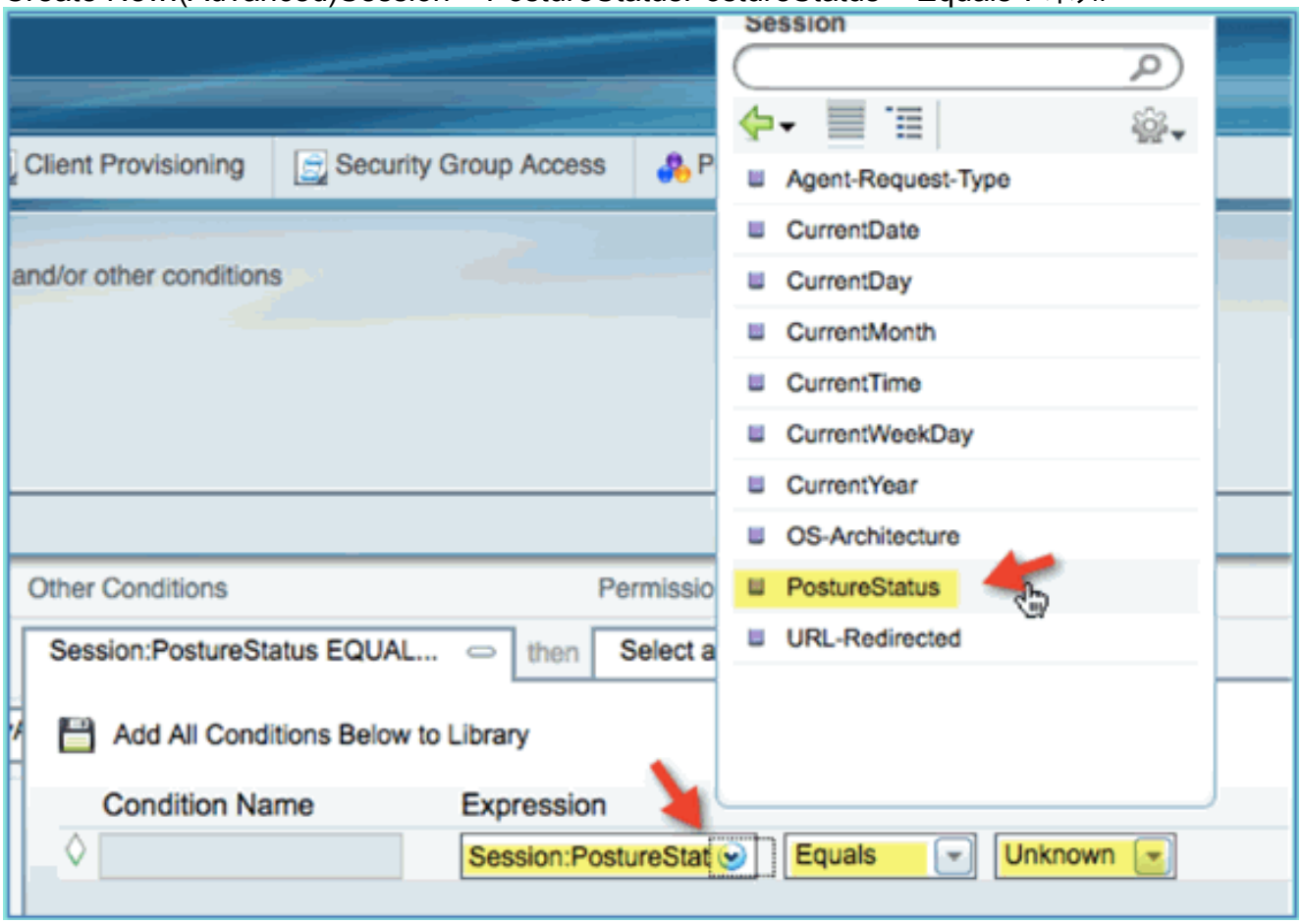
新设备首次进入网络时，其相关信息很少，管理员会创建适当的策略，以允许未知终端在允许访问之前被识别。在本练习中，将创建授权策略，以便将新设备重定向到ISE进行终端安全评估（对于无代理的移动设备，因此仅分析相关）；终端将重定向到ISE强制网络门户并识别。

请完成以下步骤：

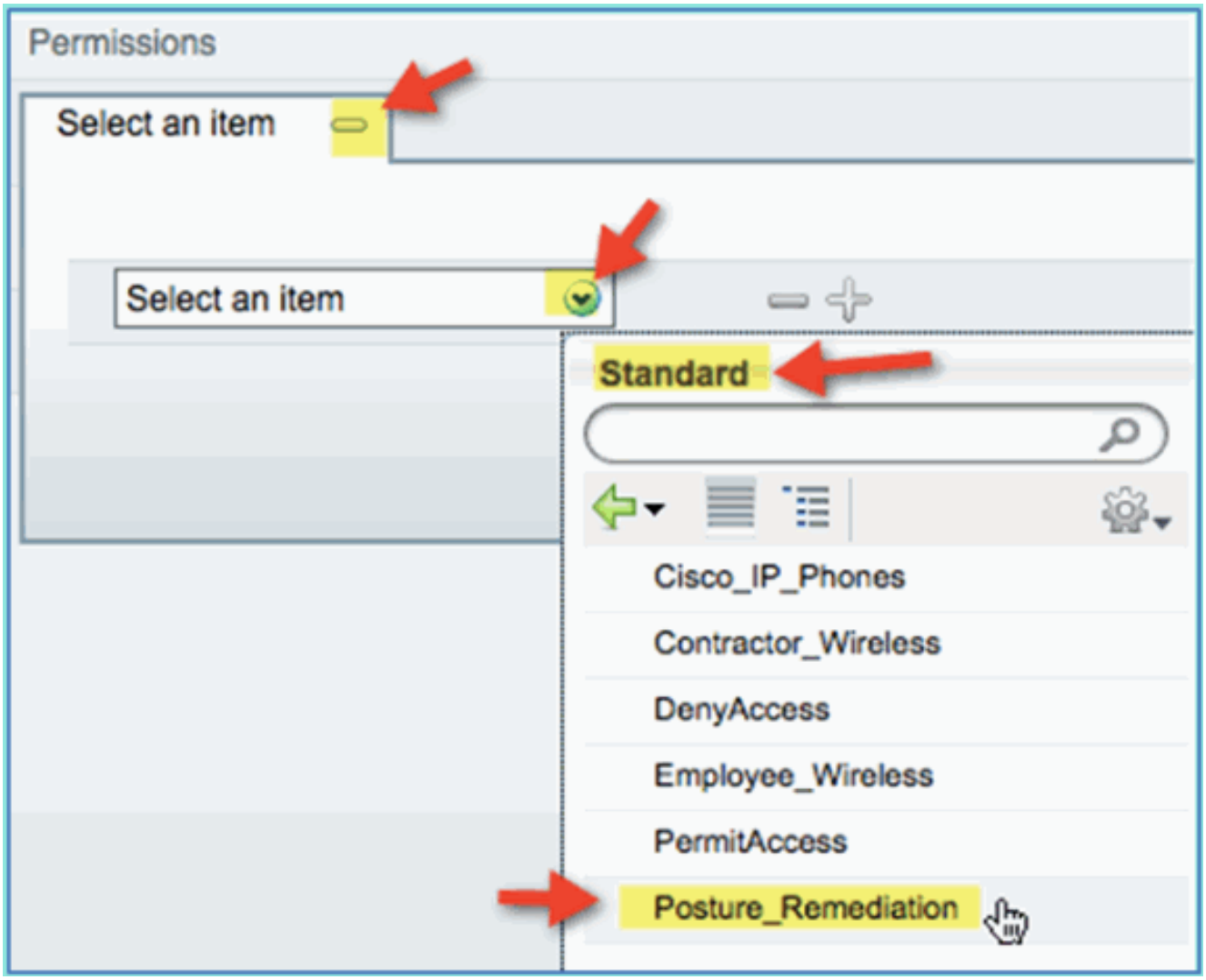
1. 从ISE导航到**策略>授权**。



2. 有一个策略用于分析的Cisco IP电话。这是开箱即用的。将此编辑为状态策略。
3. 为此策略输入以下值：规则名称：Posture_Remediation身份组：任意Other Conditions > Create New:(Advanced)Session > PostureStatusPostureStatus > Equals：未知



4. 设置以下权限：Permissions > Standard: Posture_Remediation

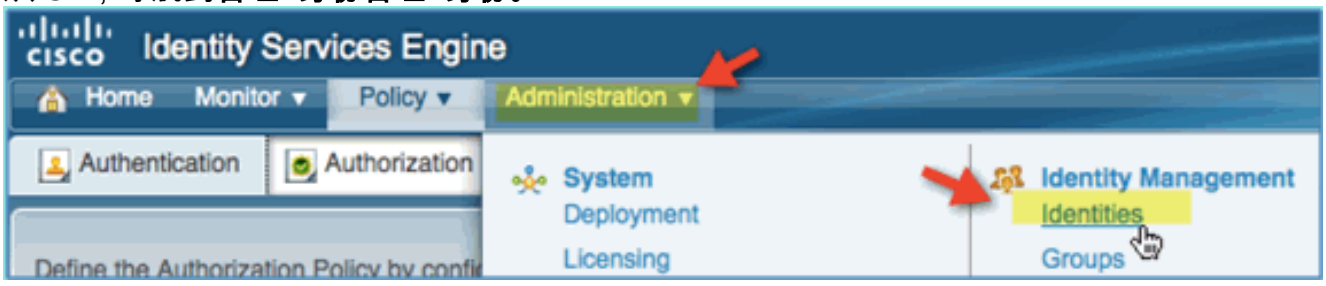


5. Click **Save**.**注意：**或者，可以创建自定义策略元素来增加易用性。

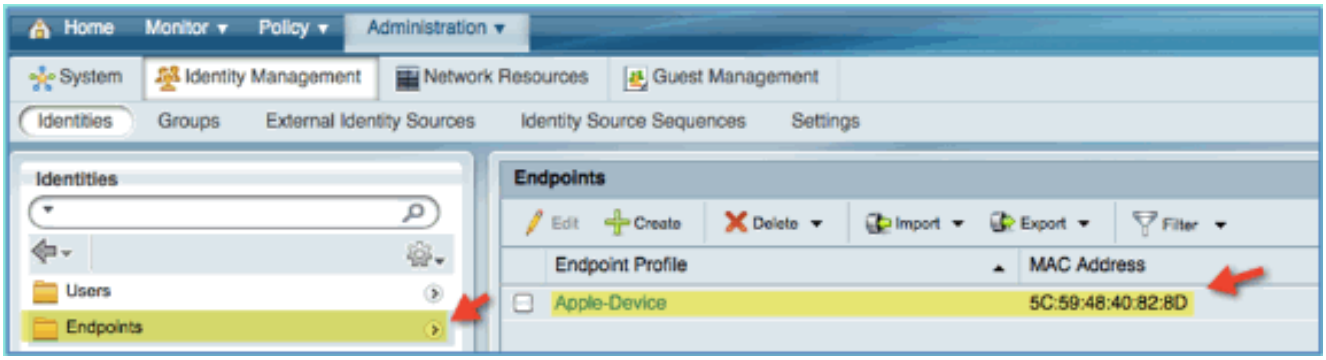
测试状态补救策略

可以执行简单演示，以显示ISE正根据终端安全评估策略正确分析新设备。

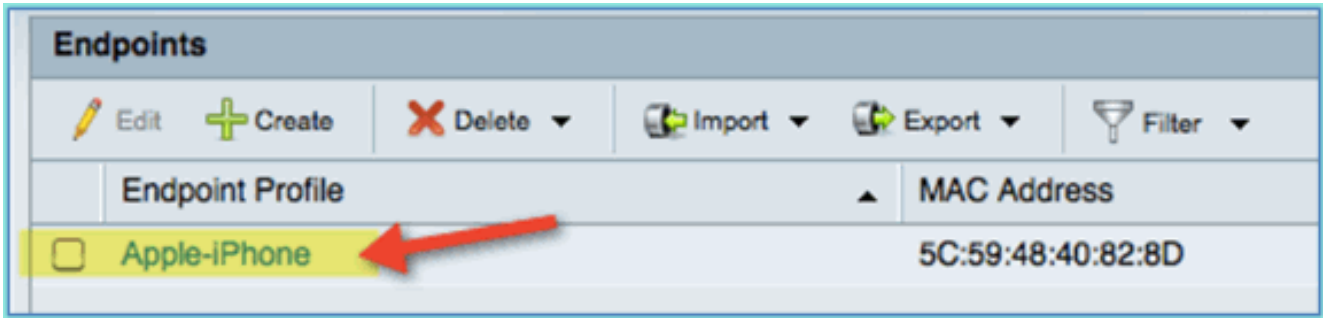
1. 从ISE，导航到**管理>身份管理>身份**。



2. 点击**终端**。关联并连接设备（本示例中为iPhone）。



3. 刷新终端列表。观察给出的信息。
4. 从终端设备浏览到：URL:http://www（或10.10.10.10）设备被重定向。接受证书的任何提示。
5. 移动设备完全重定向后，从ISE再次刷新终端列表。观察变化。上一个终端（例如，Apple-Device）应更改为“Apple-iPhone”等。原因是HTTP探测功能在重定向到强制网络门户的过程中有效地获取用户代理信息。

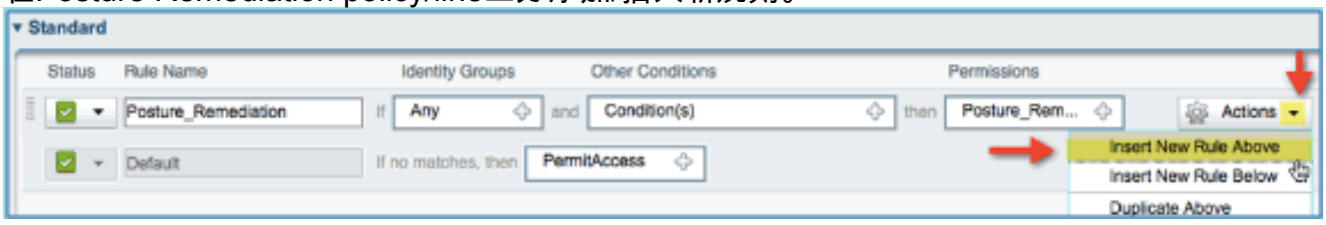


差异化访问的授权策略

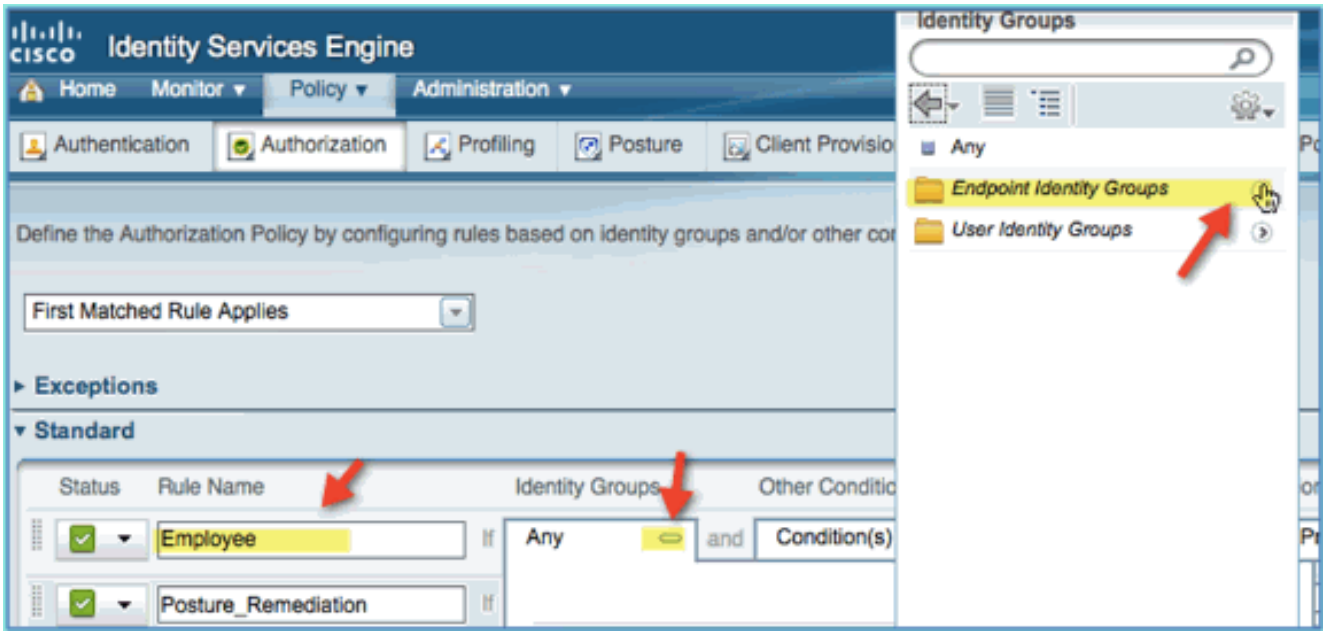
成功测试安全评估授权后，继续构建策略，以支持员工和承包商的差异化访问，包括已知设备和特定于用户角色的不同VLAN分配（在此场景中，员工和承包商）。

请完成以下步骤：

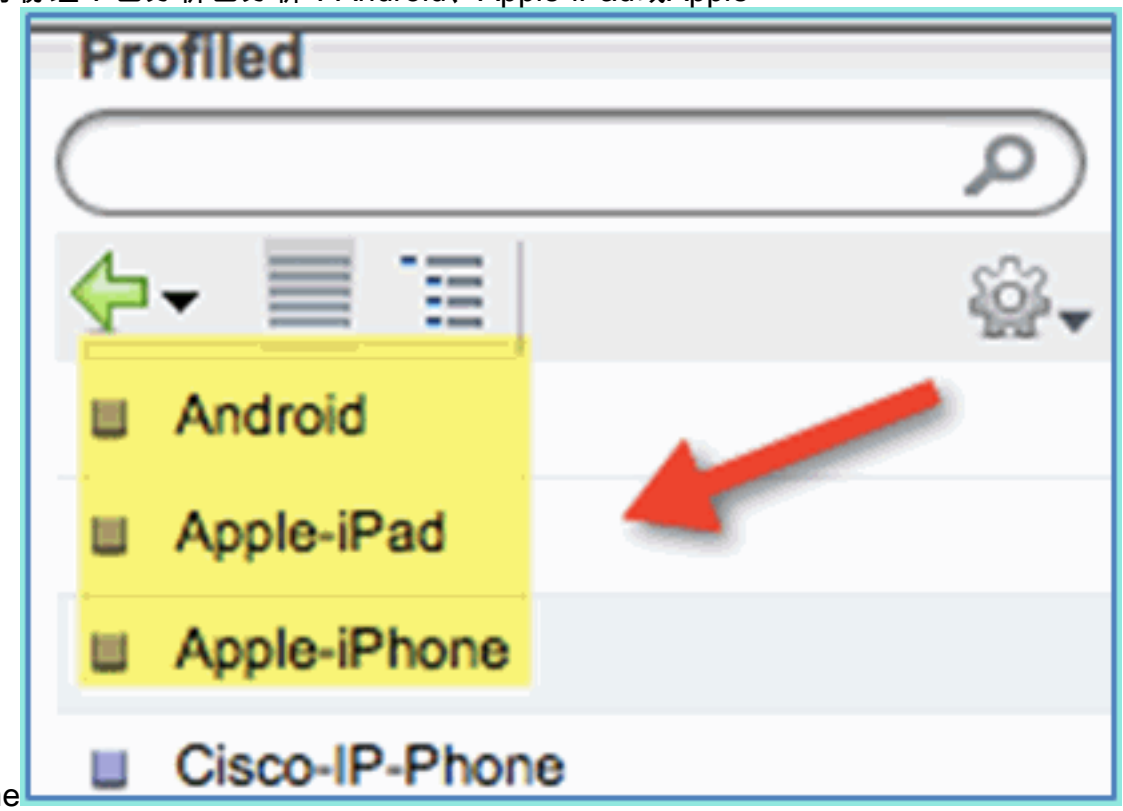
1. 导航到**ISE > Policy > Authorization**。
2. 在Posture Remediation policy/line上方添加/插入新规则。



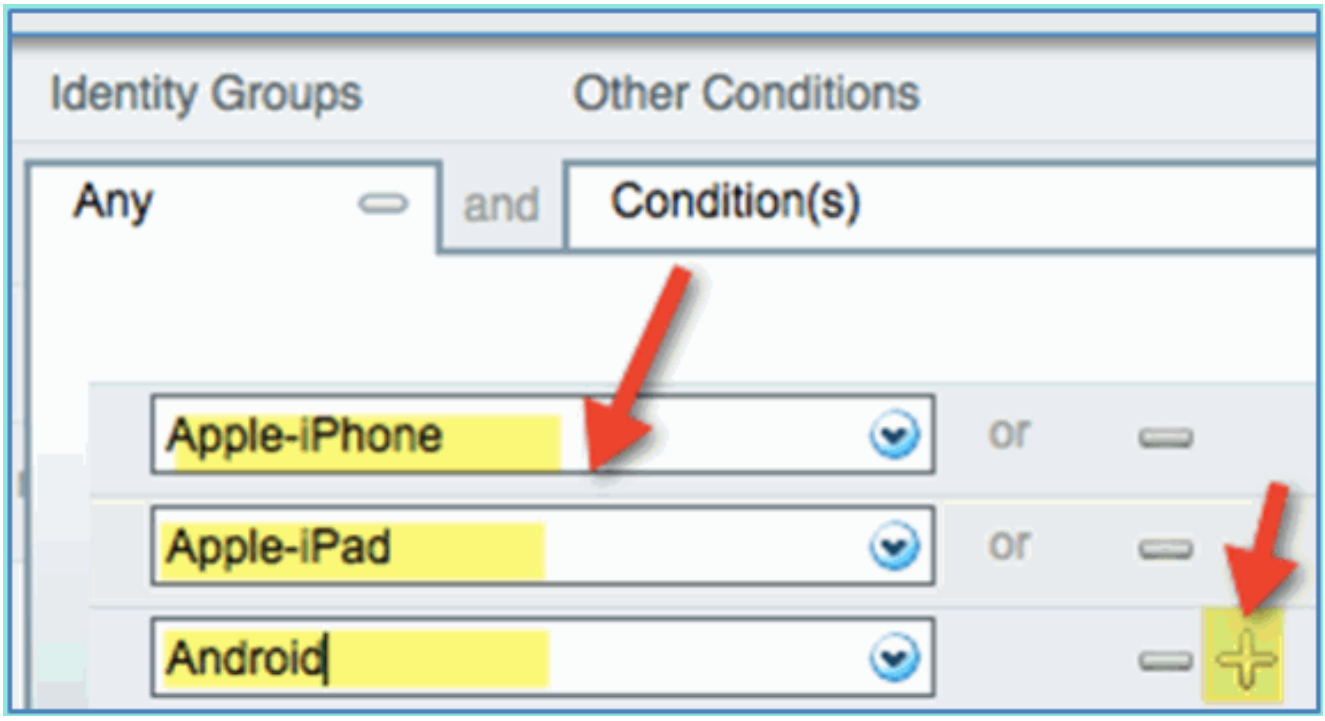
3. 为此策略输入以下值：规则名称：员工身份组（扩展）：终端身份组



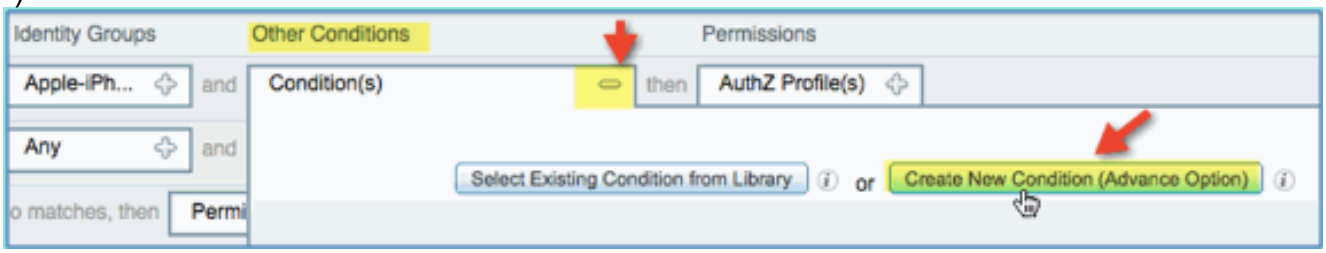
终端身份组：已分析已分析：Android、Apple-iPad或Apple-iPhone



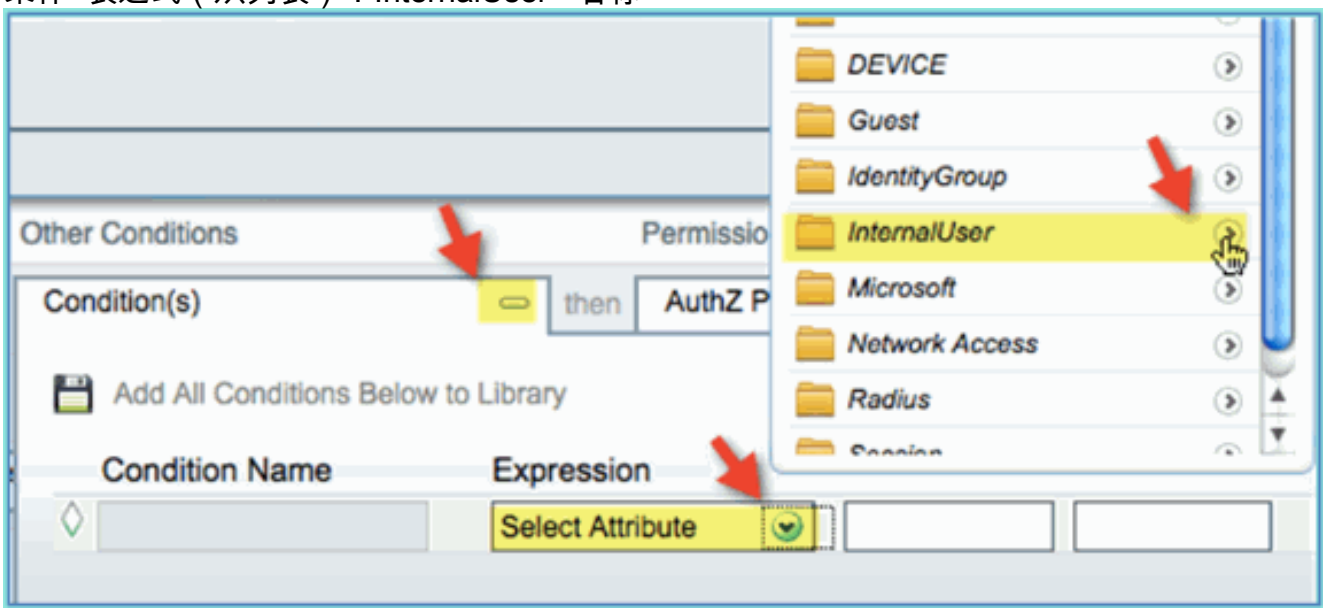
4. 要指定其他设备类型，请点击+并添加更多设备（如果需要）：终端身份组：已分析已分析：Android、Apple-iPad或Apple-iPhone



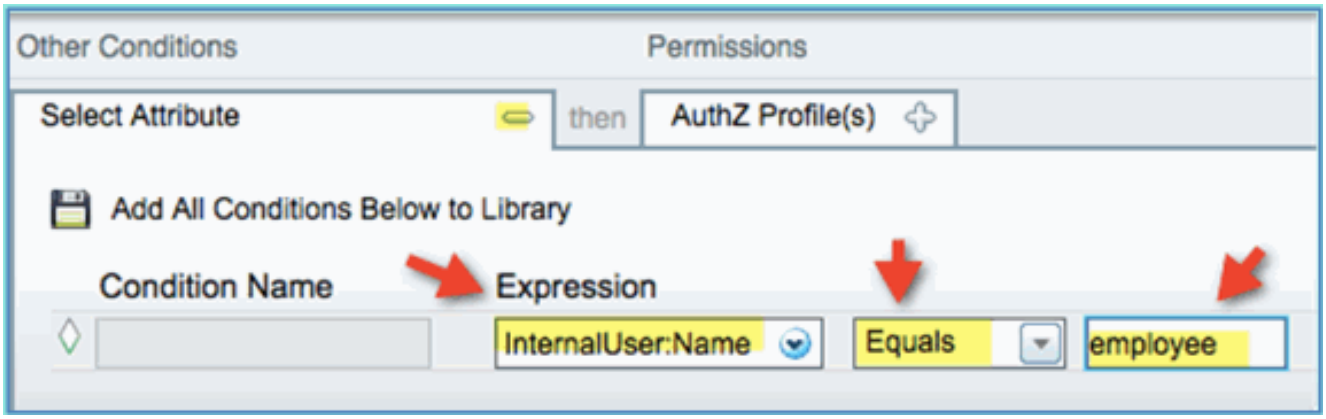
5. 为此策略指定以下“权限”值：其他条件（展开）：创建新条件（高级选项）



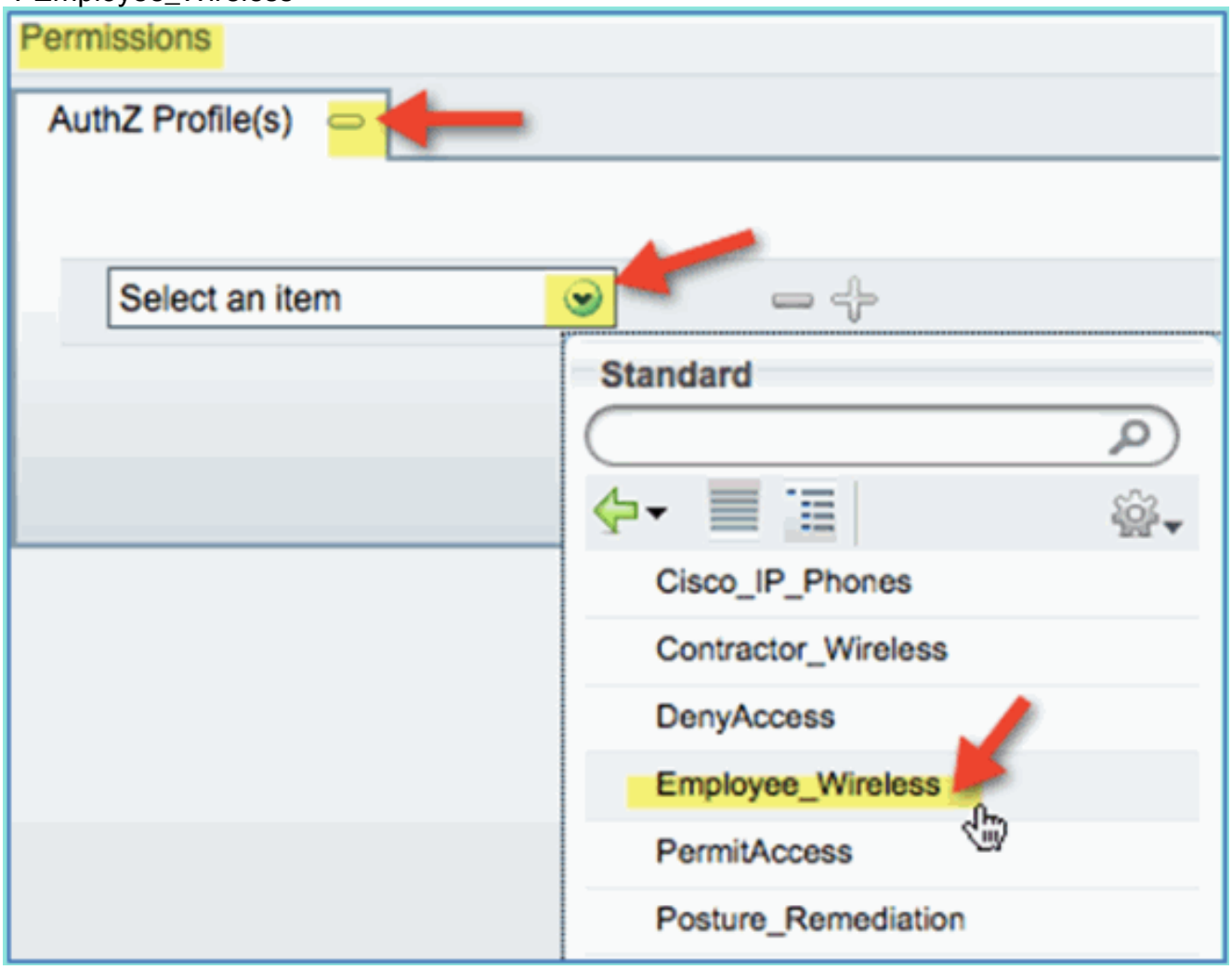
条件>表达式（从列表）：InternalUser >名称



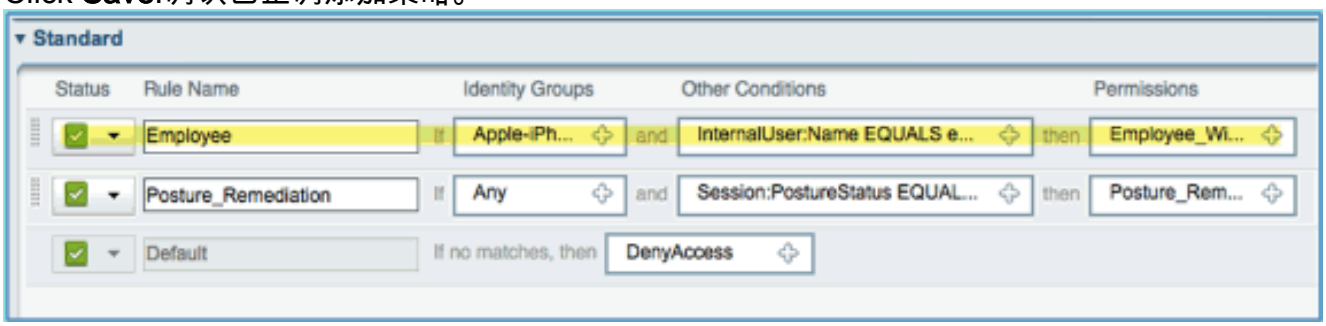
InternalUser >
Name:employee



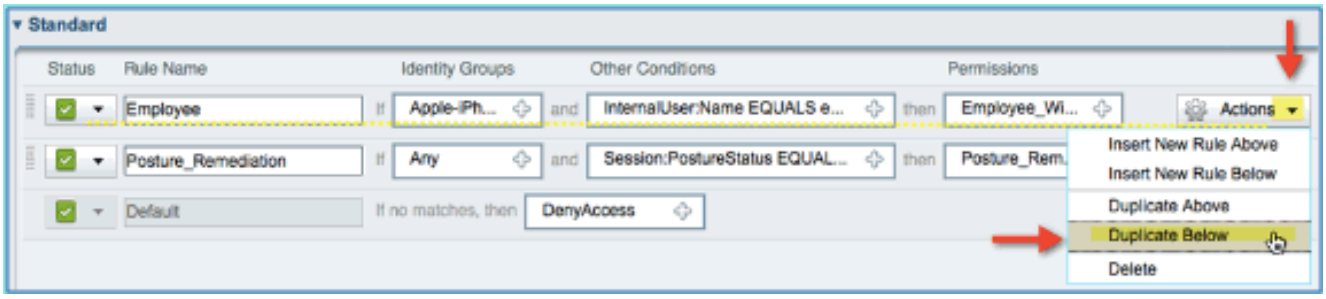
6. 为安全评估会话合规添加条件：权限>配置文件>标准：Employee_Wireless



7. Click **Save**.确认已正确添加策略。

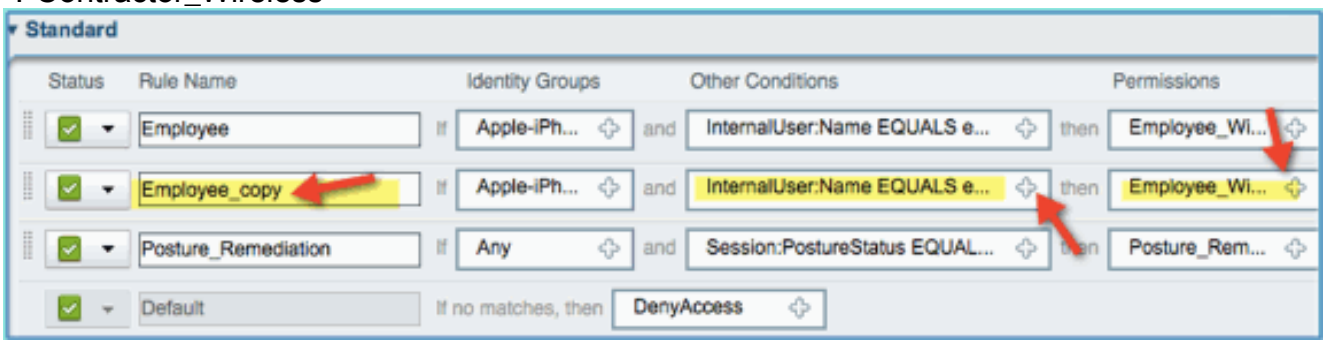


8. 继续添加承包商策略。在本文档中，复制了之前的策略以加快流程（或者，您可以手动配置以实现良好实践）。从Employee policy > Actions中，单击**Duplicate Below**。

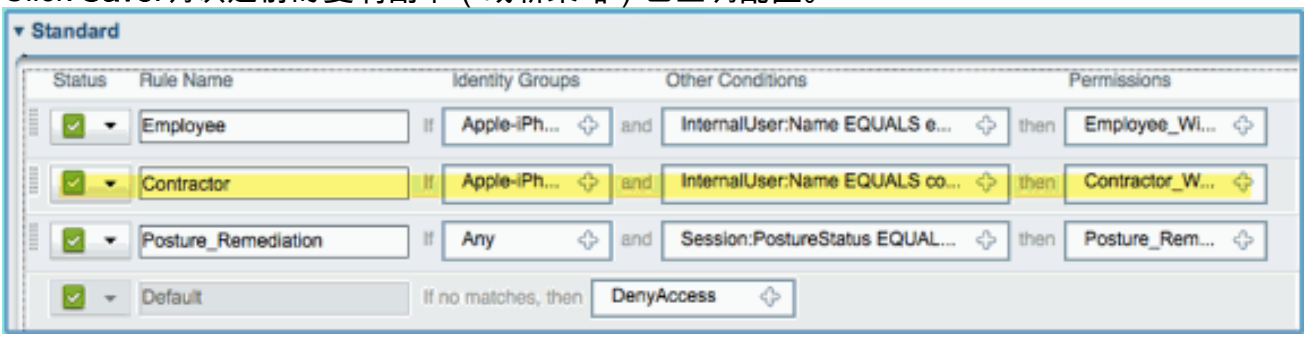


9. 编辑此策略的以下字段（复制副本）：规则名称：承包商其它条件>内部用户>姓名：承包商权限

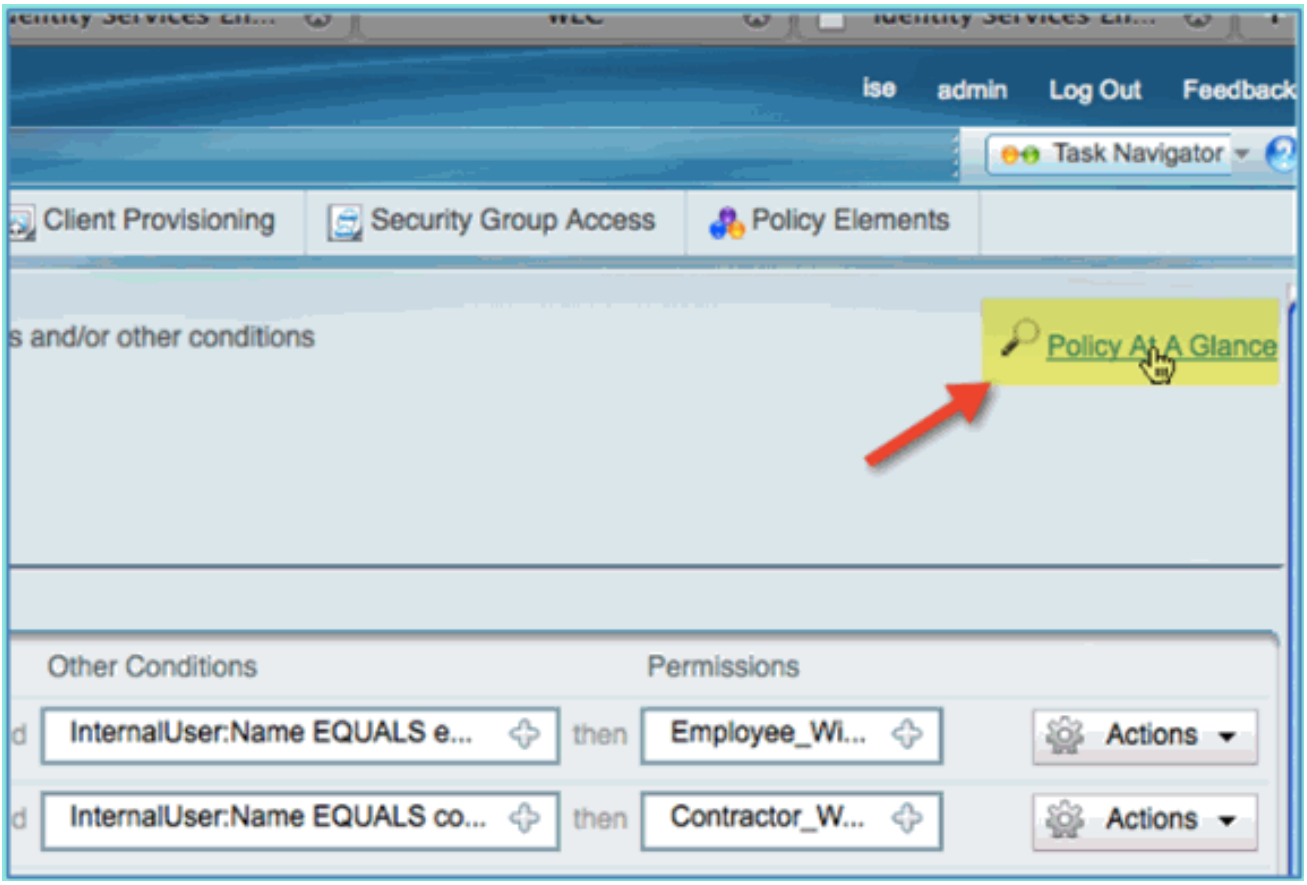
   ：Contractor_Wireless



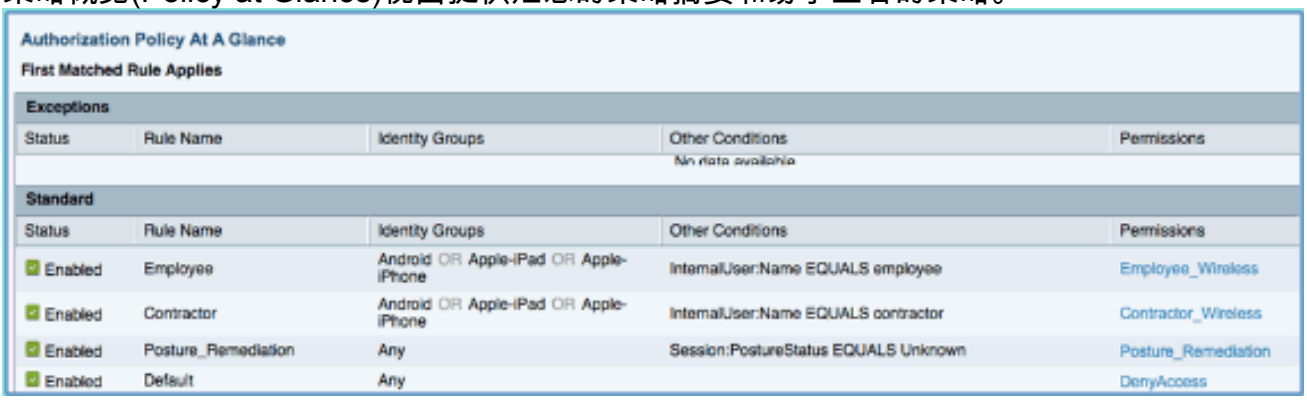
10. Click **Save**.确认之前的复制副本（或新策略）已正确配置。



11. 要预览策略，请单击**Policy-at-a-Glance**。



策略概览(Policy at Glance)视图提供汇总的策略摘要和易于查看的策略。



Authorization Policy At A Glance

First Matched Rule Applies

Exceptions

Status	Rule Name	Identity Groups	Other Conditions	Permissions
			No data available	

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Employee	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS employee	Employee_Wireless
Enabled	Contractor	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS contractor	Contractor_Wireless
Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
Enabled	Default	Any		DenyAccess

测试CoA以区分访问

利用为区分访问而准备的授权配置文件和策略，是时候进行测试了。如果使用单个安全WLAN，则员工将被分配员工VLAN，承包商将被分配为承包商VLAN。下一个示例中使用的是Apple iPhone/iPad。

请完成以下步骤：

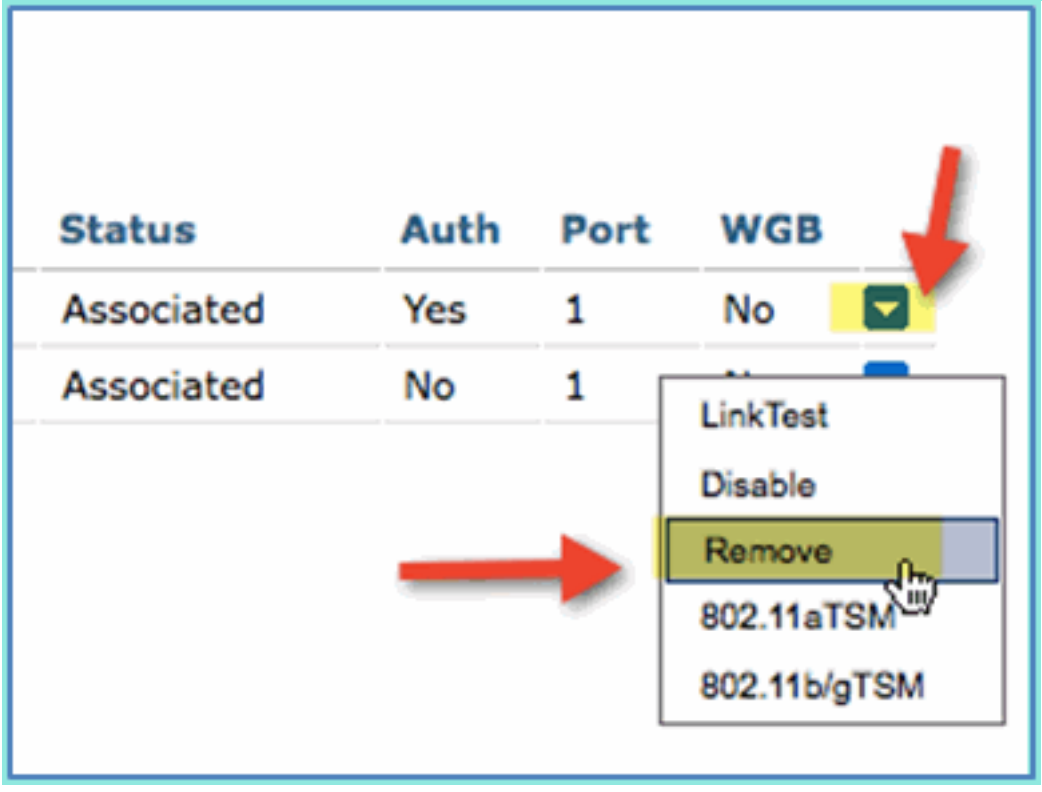
1. 使用移动设备连接到安全的WLAN(POD1x)并使用以下凭证：用户名：employee密码：XXXXX

2. 单击**Join**。确认已为员工分配了VLAN 11（员工VLAN）。

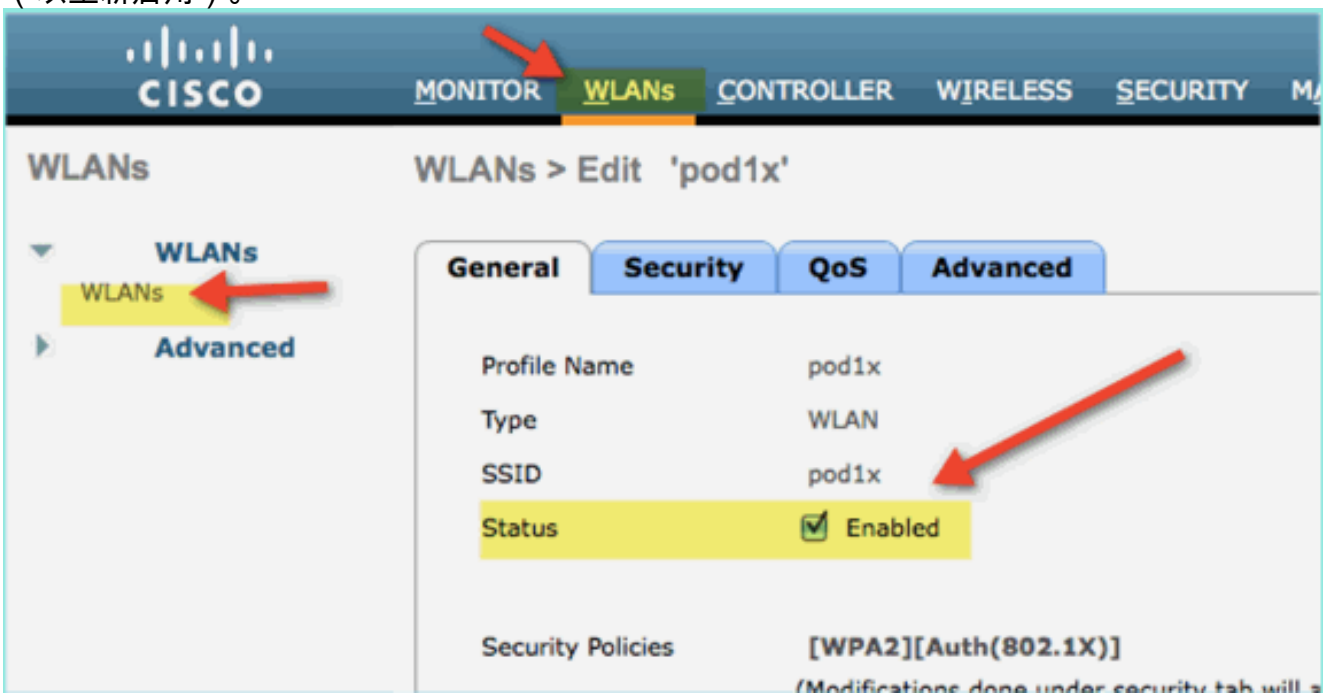
3. 单击Forget this Network。单击Forget进行确认。

4. 转到WLC并删除现有的客户端连接（如果在前面的步骤中使用了相同的连接）。导航到**监控>客户端> MAC地址**，然后单击**删除**。


CISCO
MONITOR
WLANs
Monitor
Clients
Summary
Current Filter
Access Points
Cisco CleanAir
Client MAC Addr
Statistics
44:2a:60:f7:3a:4a
CDP
5c:59:48:40:82:8d
Rogues
Clients
Multicast


Status
Auth
Port
WGB
Associated
Yes
1
No
Associated
No
1
LinkTest
Disable
Remove
802.11aTSM
802.11b/gTSM

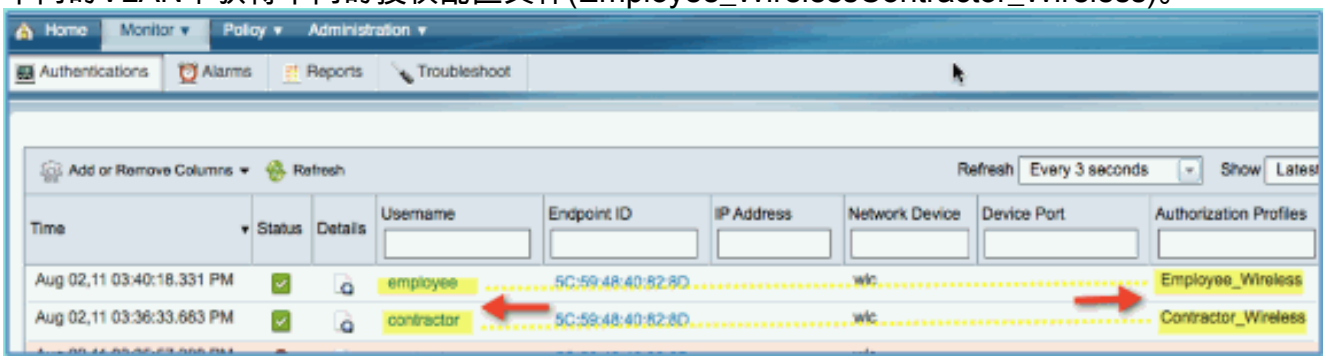
5. 另一种清除以前客户端会话的可靠方法是禁用/启用WLAN。转到**WLC > WLANs > WLAN**，然后单击要编辑的WLAN。取消选中**Enabled > Apply**（以禁用）。选中**Enabled > Apply**复选框（以重新启用）。



6. 返回移动设备。使用以下凭证重新连接到同一WLAN:用户名：contractor密码：XXXX

7. 单击**Join**。确认为承包商用户分配了VLAN 12（承包商/访客VLAN）。

8. 您可以在**ISE >监控>授权**中查看ISE实时日志视图。您应该看到个人用户（员工、承包商）在不同的VLAN中获得不同的授权配置文件(Employee_WirelessContractor_Wireless)。



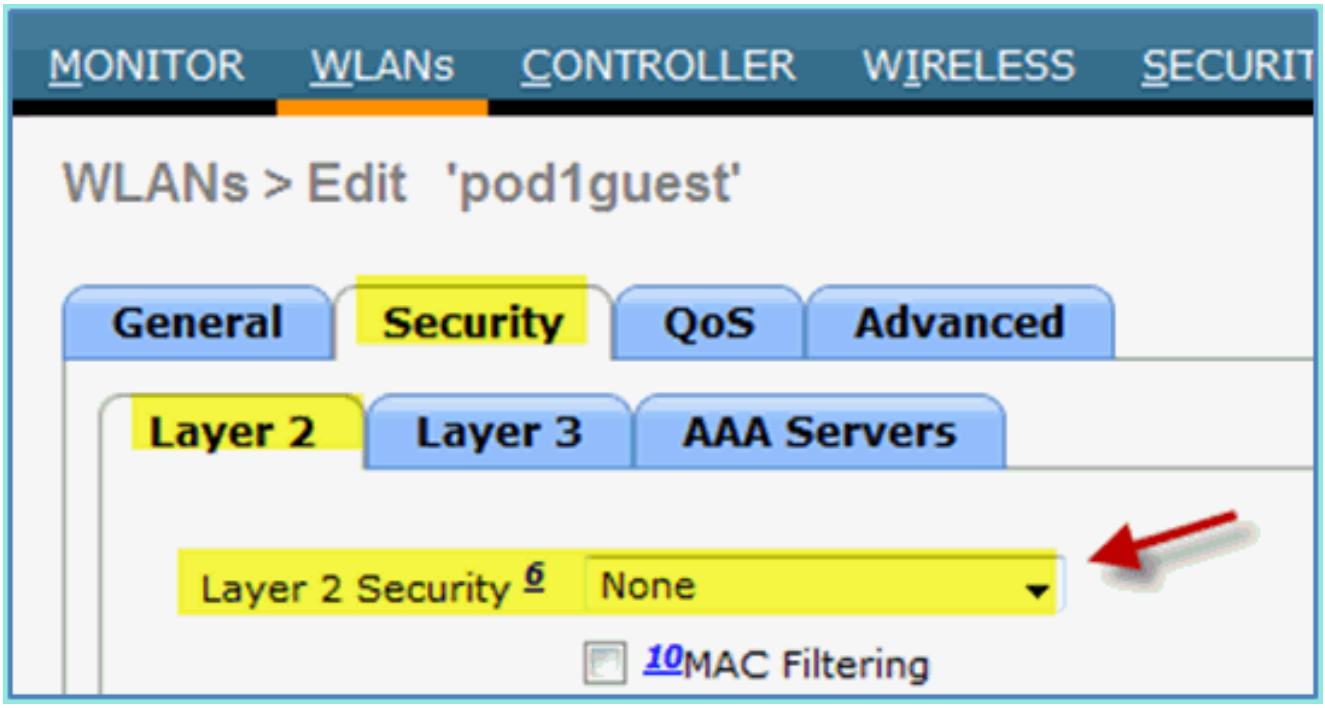
WLC访客WLAN

完成以下步骤以添加访客WLAN以允许访客访问ISE保证人访客门户：

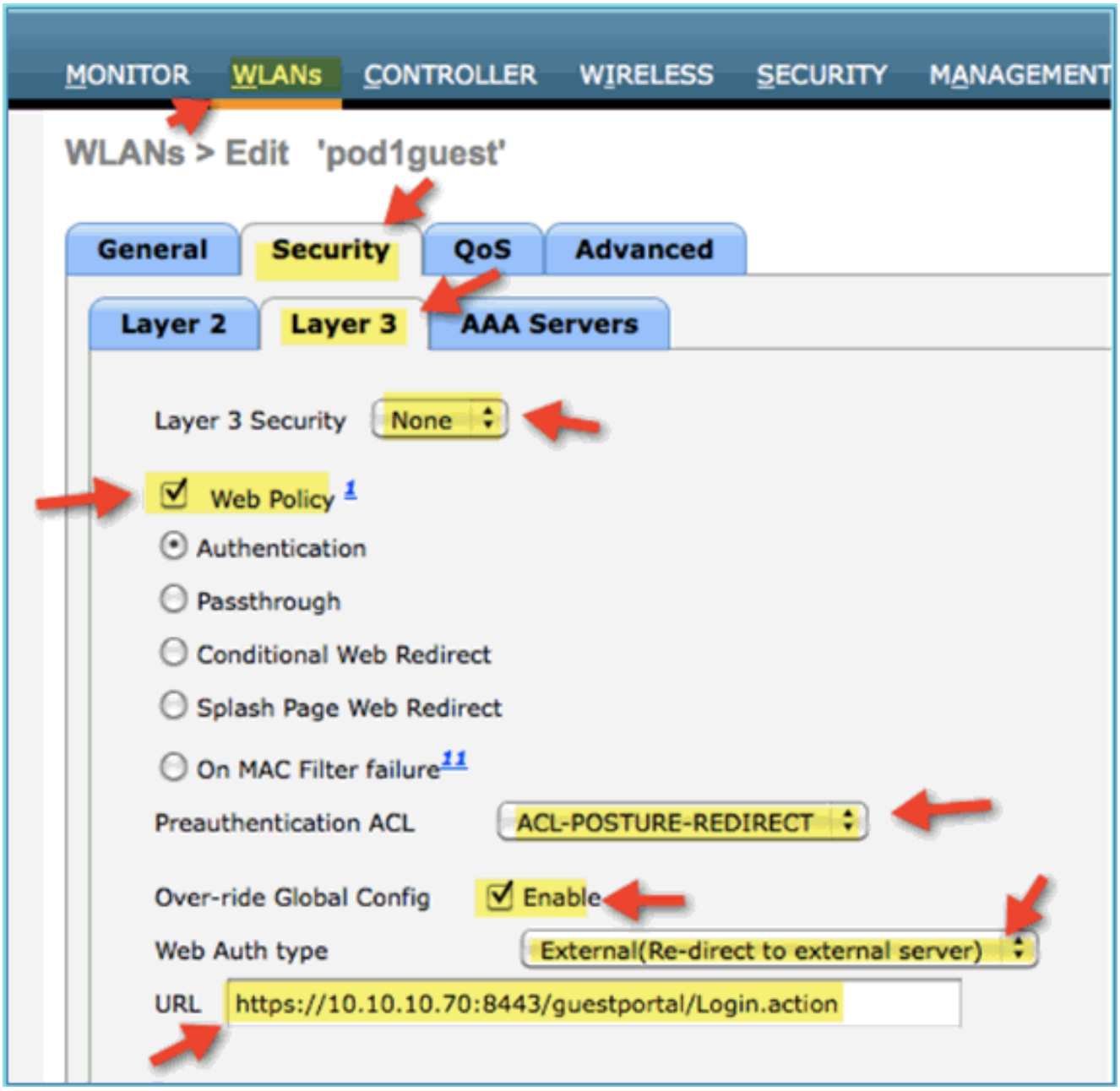
1. 从WLC导航到**WLANs > WLANs > Add New**。
2. 为新的访客WLAN输入以下命令：配置文件名称
   ：pod1guestSSID:pod1guest

3. 单击 **Apply**。
4. 在访客WLAN > General选项卡下输入以下命令：状态：已禁用接口/接口组：访客

5. 导航到访客**WLAN > Security > Layer2**，然后输入以下内容：第2层安全：无



6. 导航到访客**WLAN > Security > Layer3**选项卡，然后输入以下内容：第3层安全：无Web策略：已启用Web策略子值：身份验证预身份验证ACL:ACL-POSTURE-REDIRECTWeb身份验证类型：外部（重定向到外部服务器）URL:https://10.10.10.70:8443/guestportal/Login.action



7. 单击 **Apply**。
8. 确保保存**WLC配置**。

测试访客WLAN和访客门户

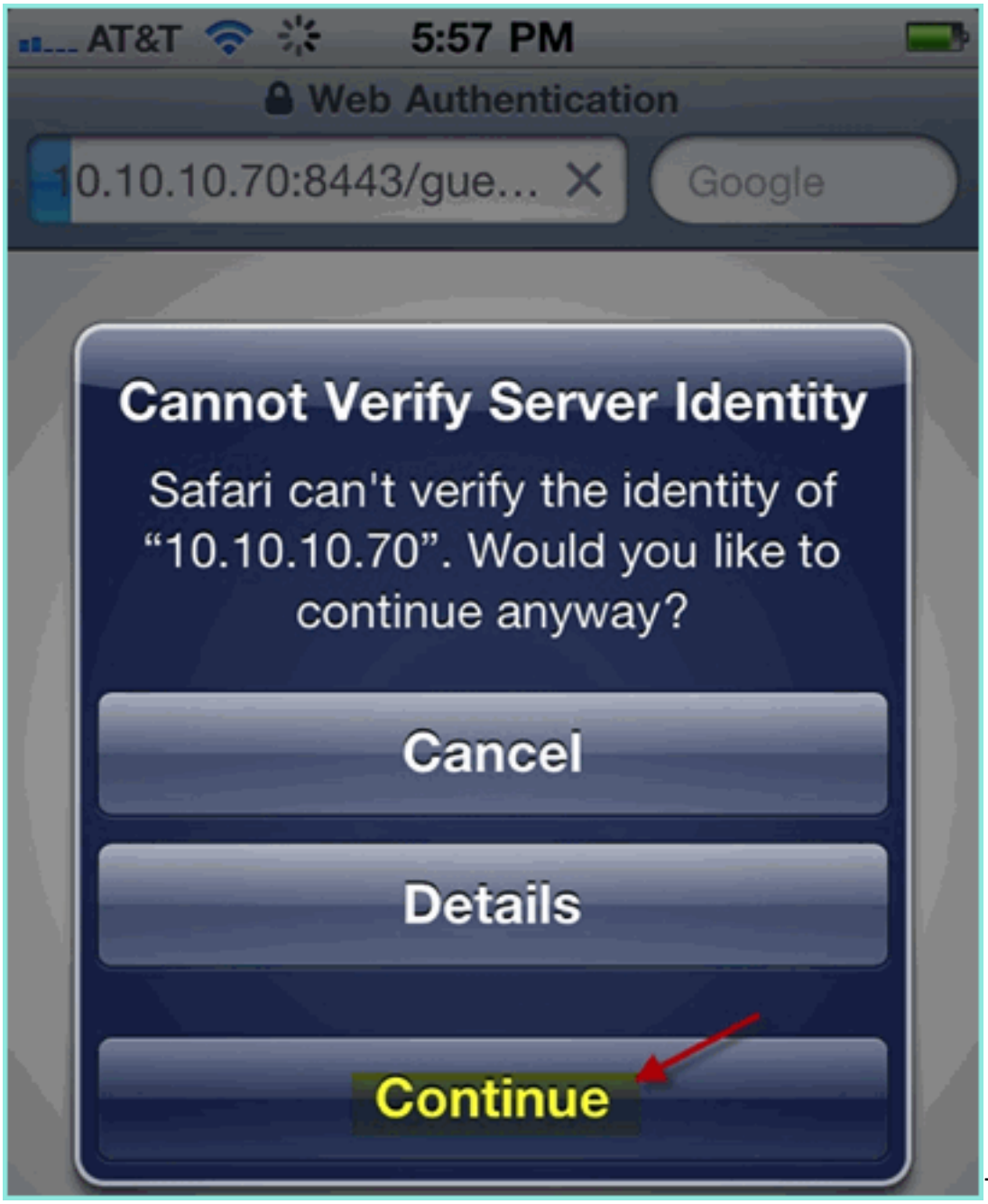
现在，您可以测试访客WLAN的配置。它应将访客重定向到ISE访客门户。

请完成以下步骤：

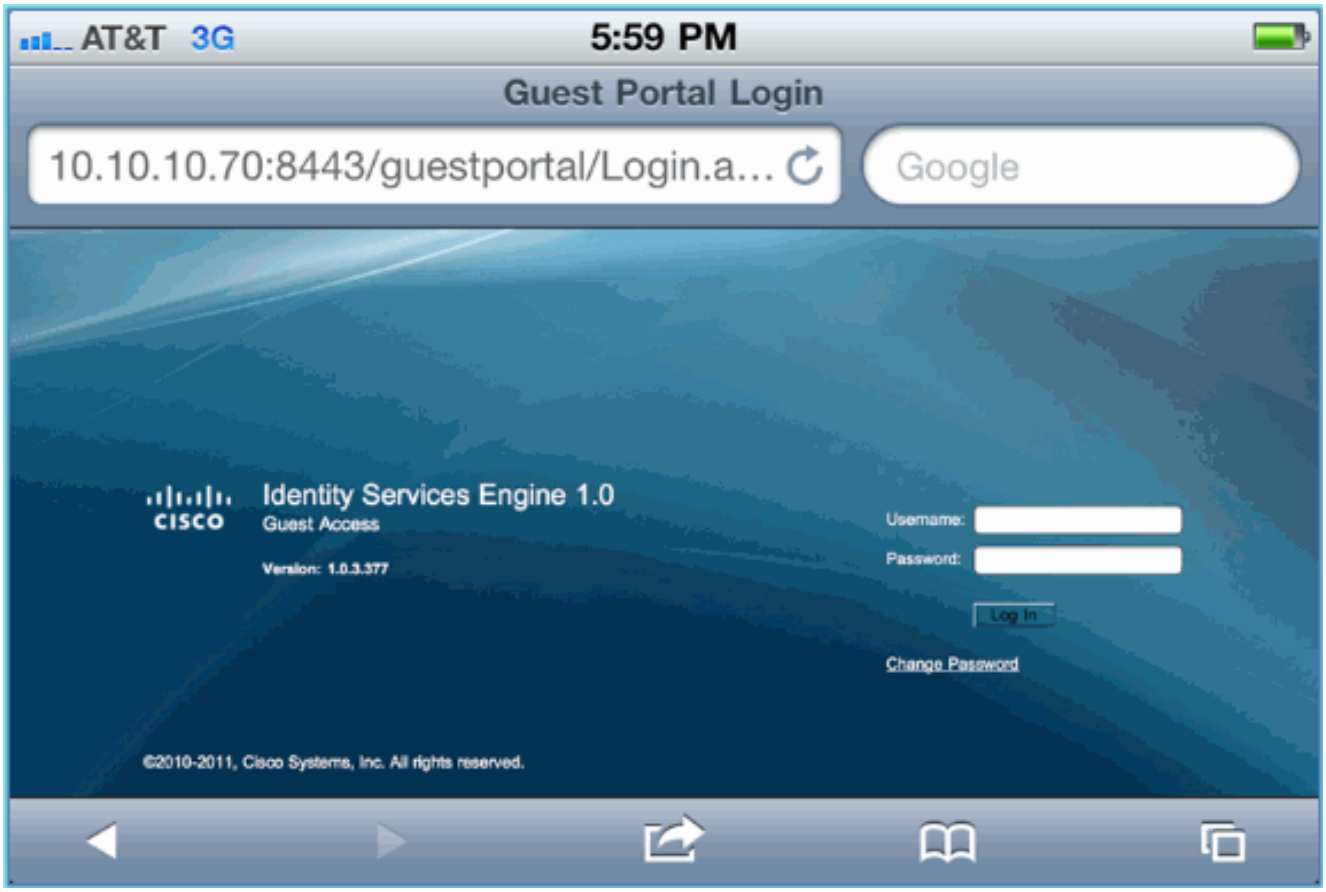
1. 从iPhone等iOS设备导航到**Wi-Fi Networks > Enable**。然后，选择POD访客网络。

2. 您的iOS设备应显示来自访客VLAN(10.10.12.0/24)的有效IP地址。

3. 打开Safari浏览器并连接到：URL:http://10.10.10.10系统将显示Web身份验证重定向。
4. 点击**继续**，直到您到达ISE访客门户页面。



下一个示例屏幕截图显示访客门户登录上的iOS设备。这可以确认WLAN和ISE访客门户的正确设置处于活动状态。

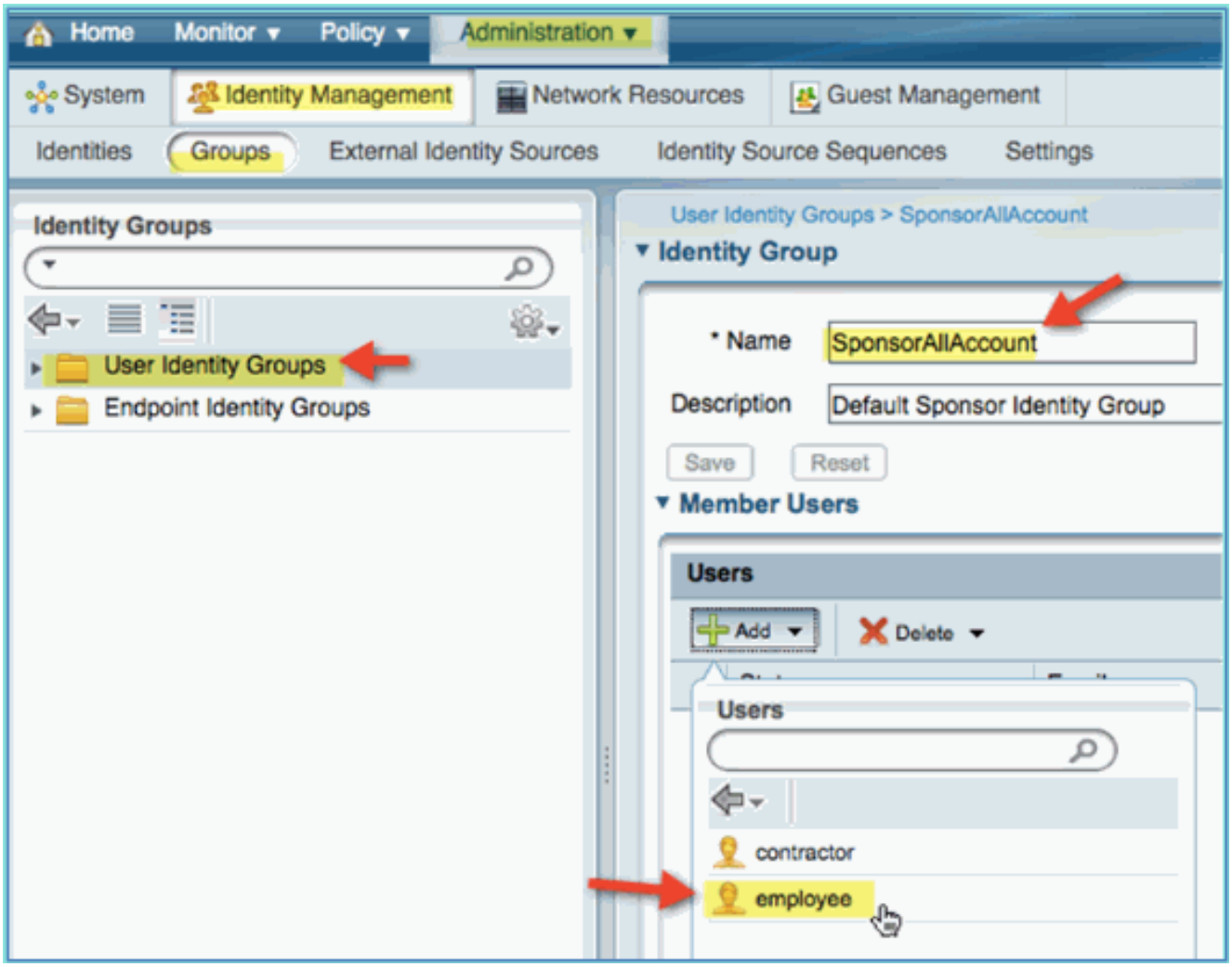


ISE无线发起访客接入

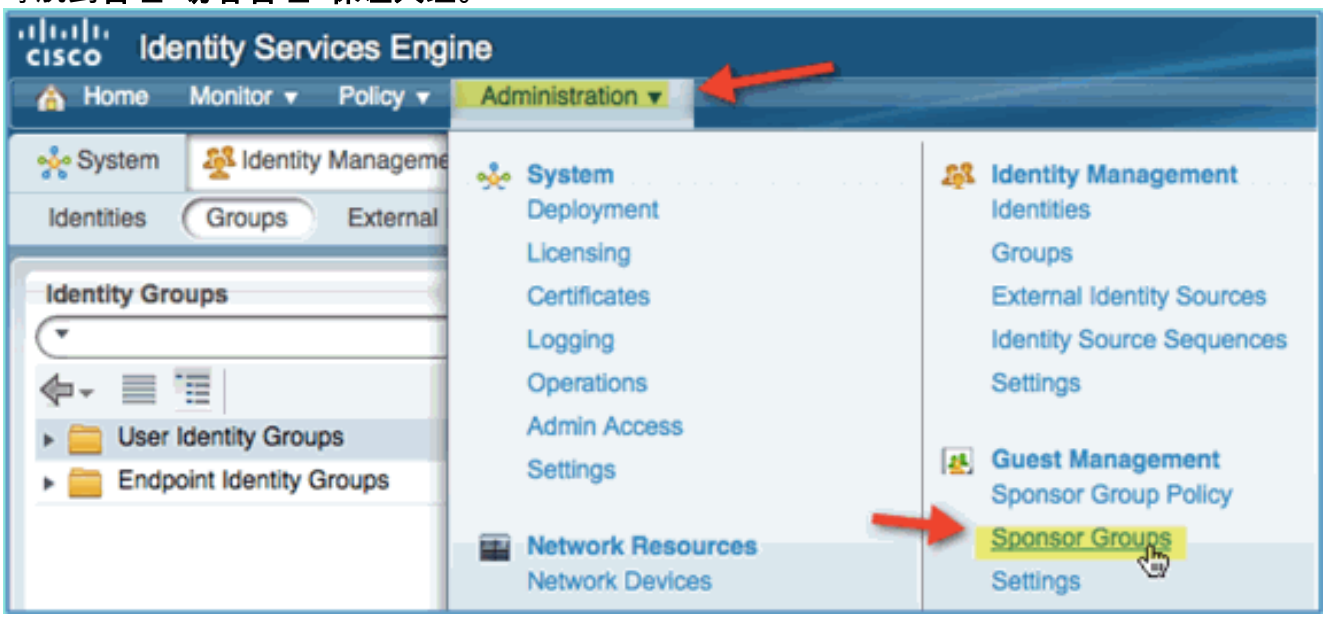
可以将ISE配置为允许发起访客。在这种情况下，您将配置ISE访客策略以允许内部或AD域（如果集成）用户发起访客访问。您还将配置ISE以允许发起人查看访客密码（可选），这对本实验很有帮助。

请完成以下步骤：

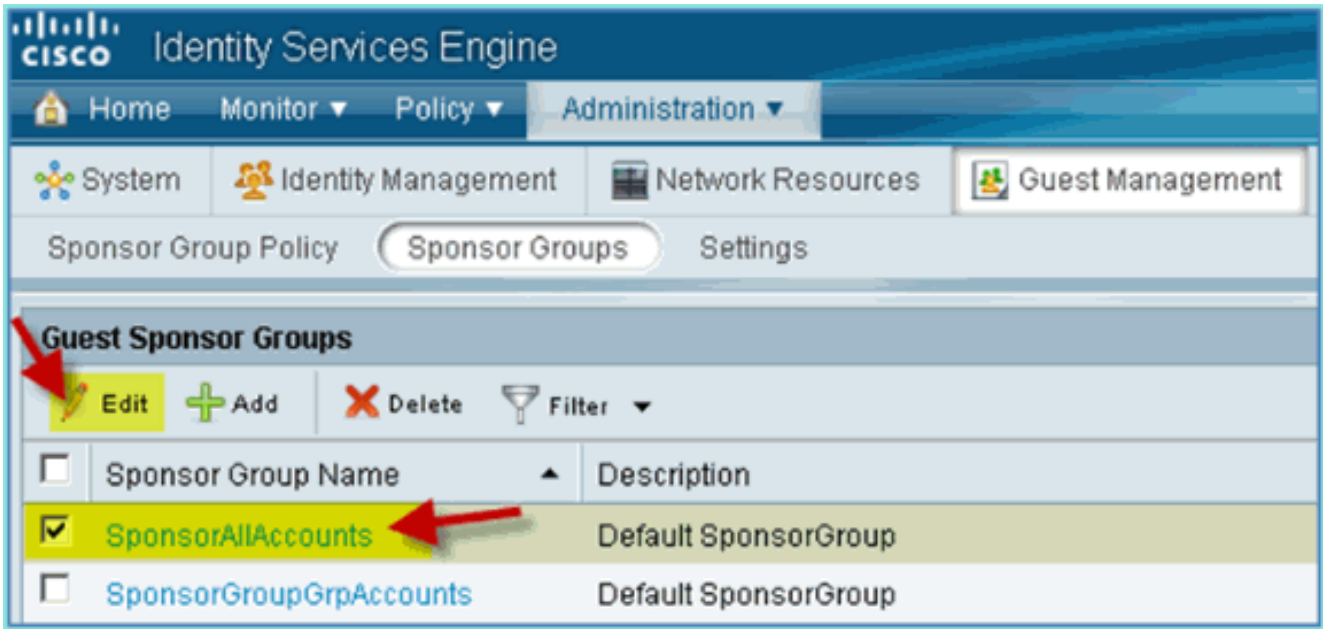
1. 将员工用户添加到SponsorAllAccount组。有不同的方法可以执行此操作：直接转到组，或编辑用户并分配组。在本示例中，导航到**管理>身份管理>组>用户身份组**。然后，单击SponsorAllAccount并添加员工用户。



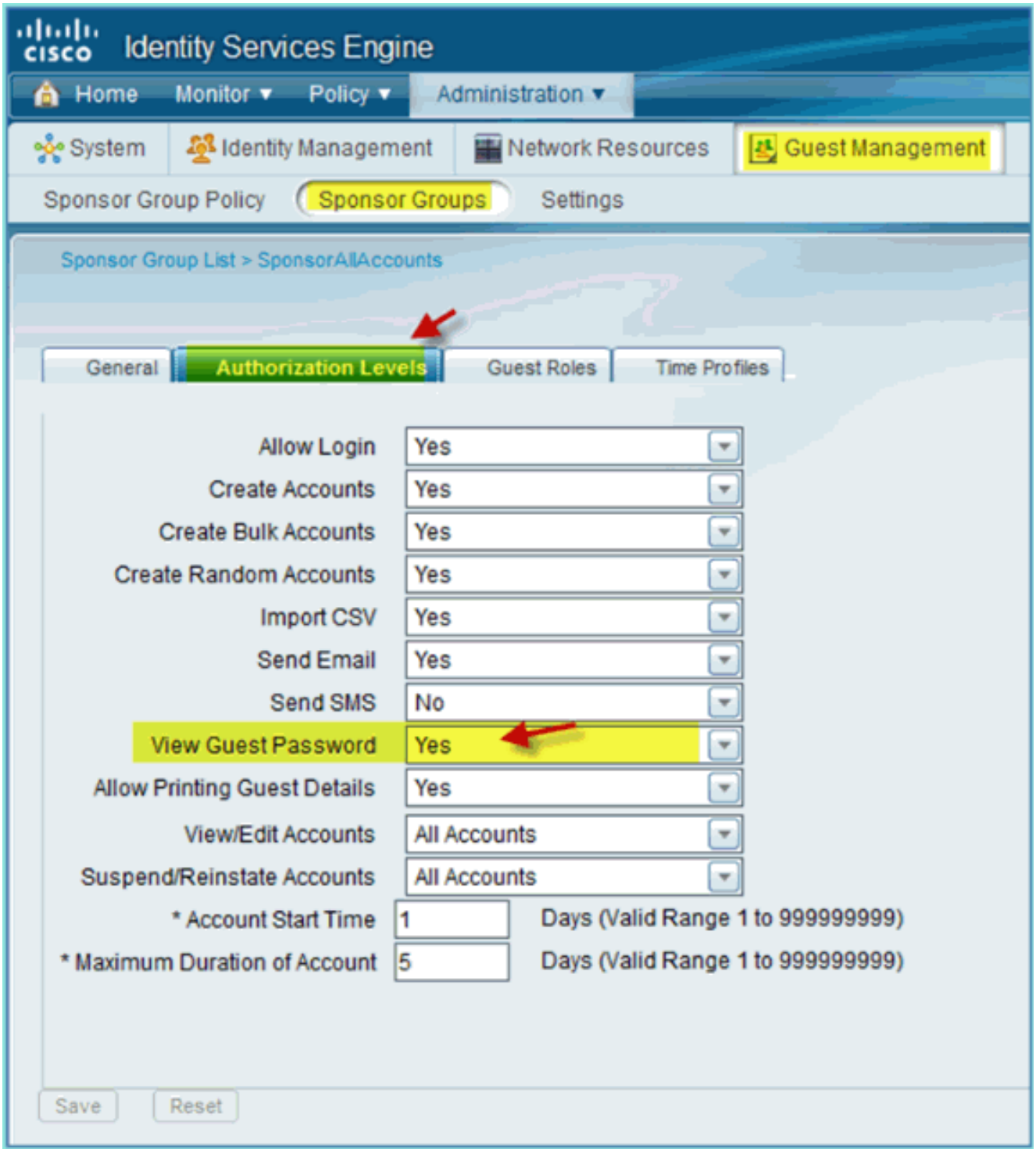
2. 导航到**管理>访客管理>保证人组**。



3. 点击**编辑**，然后选择**发起人所有帐户**。



4. 选择Authorization Levels并设置以下内容：查看访客密码：是



5. 单击**Save**以完成此任务。

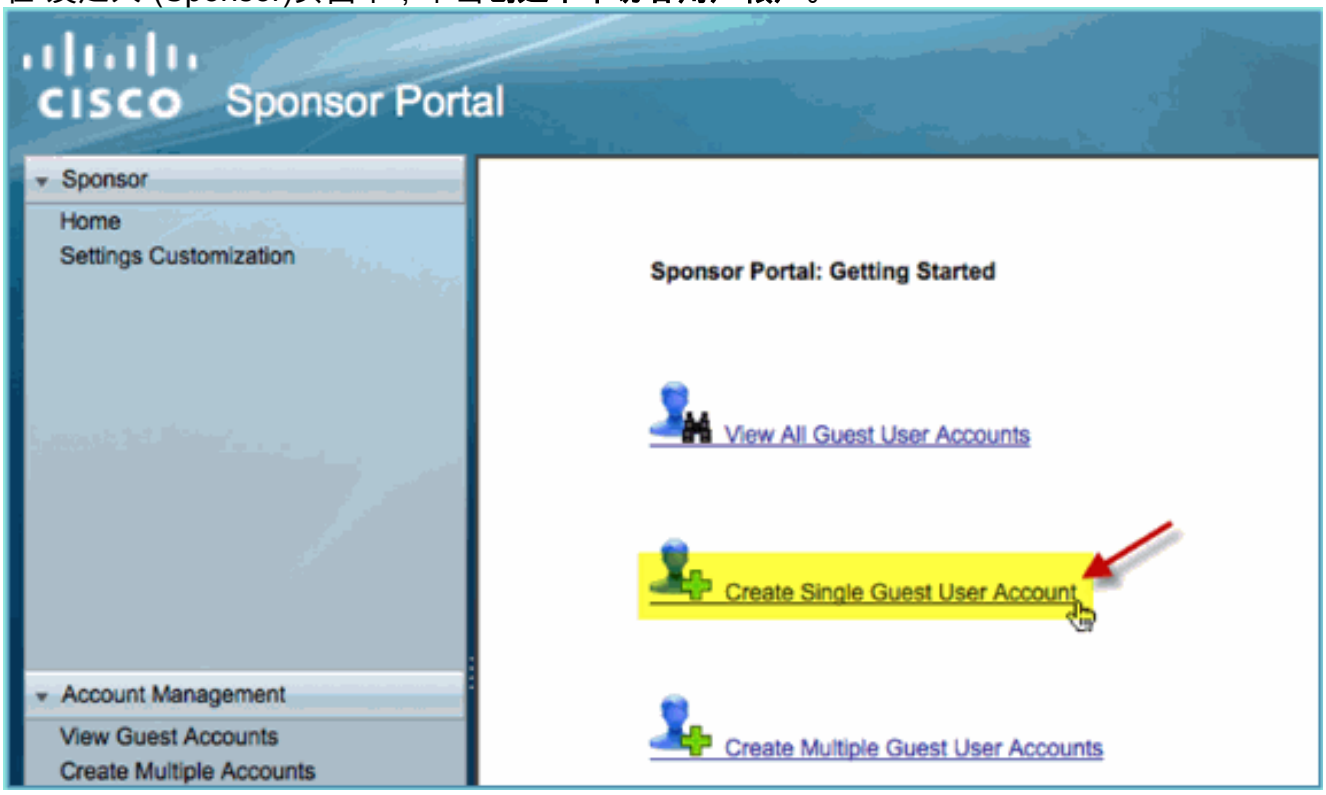
赞助访客

以前，您已配置相应的访客策略和组，以允许AD域用户发起临时访客。接下来，您将访问发起人门户并创建临时访客访问权限。

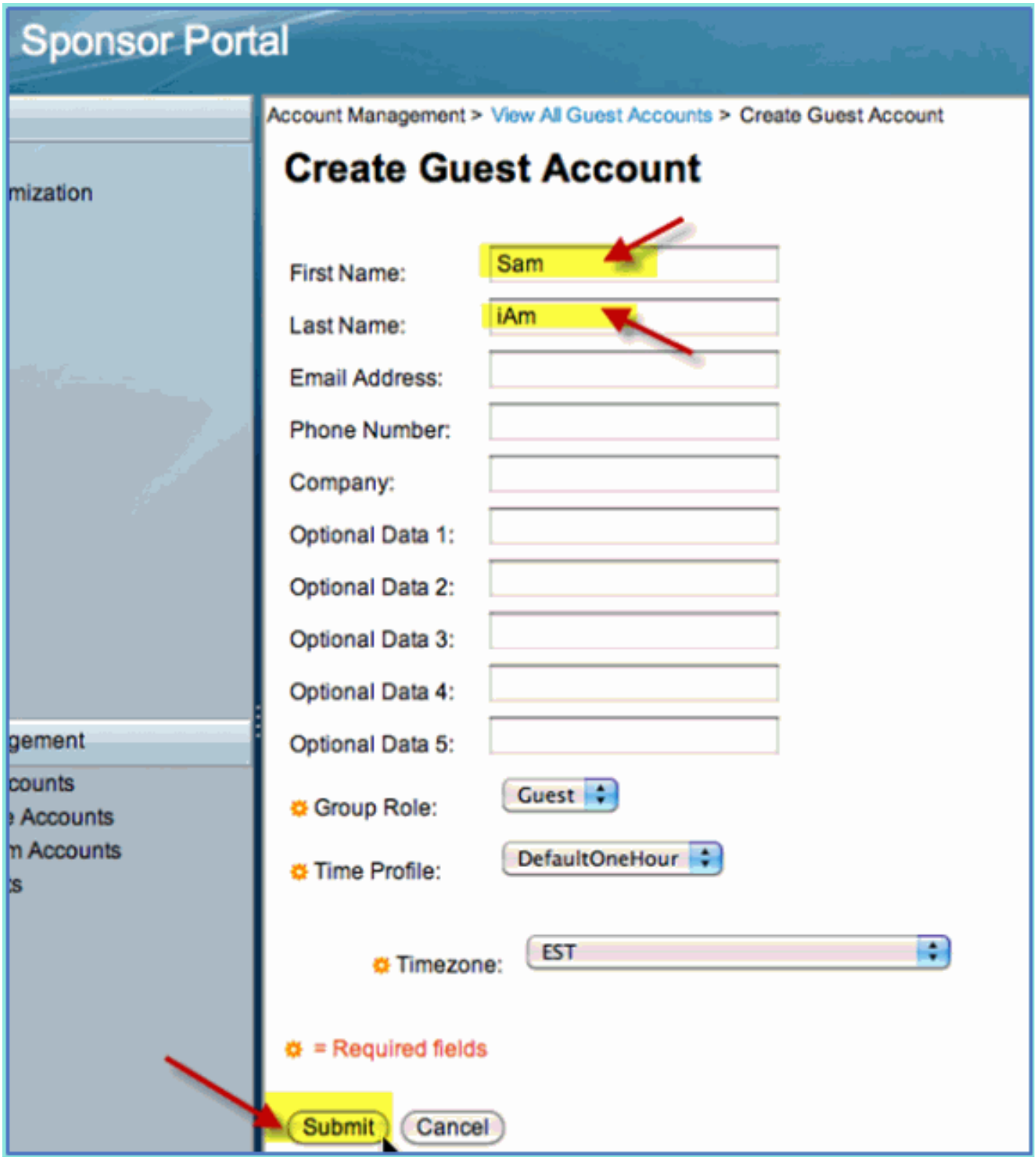
请完成以下步骤：

1. 从浏览器导航至以下URL:http://<ise ip>:8080/sponsorportal/**或**https://<ise ip>:8443/sponsorportal/。然后，使用以下内容登录：用户名：aduser(Active Directory)、employee（内部用户）密码
   ：XXXX

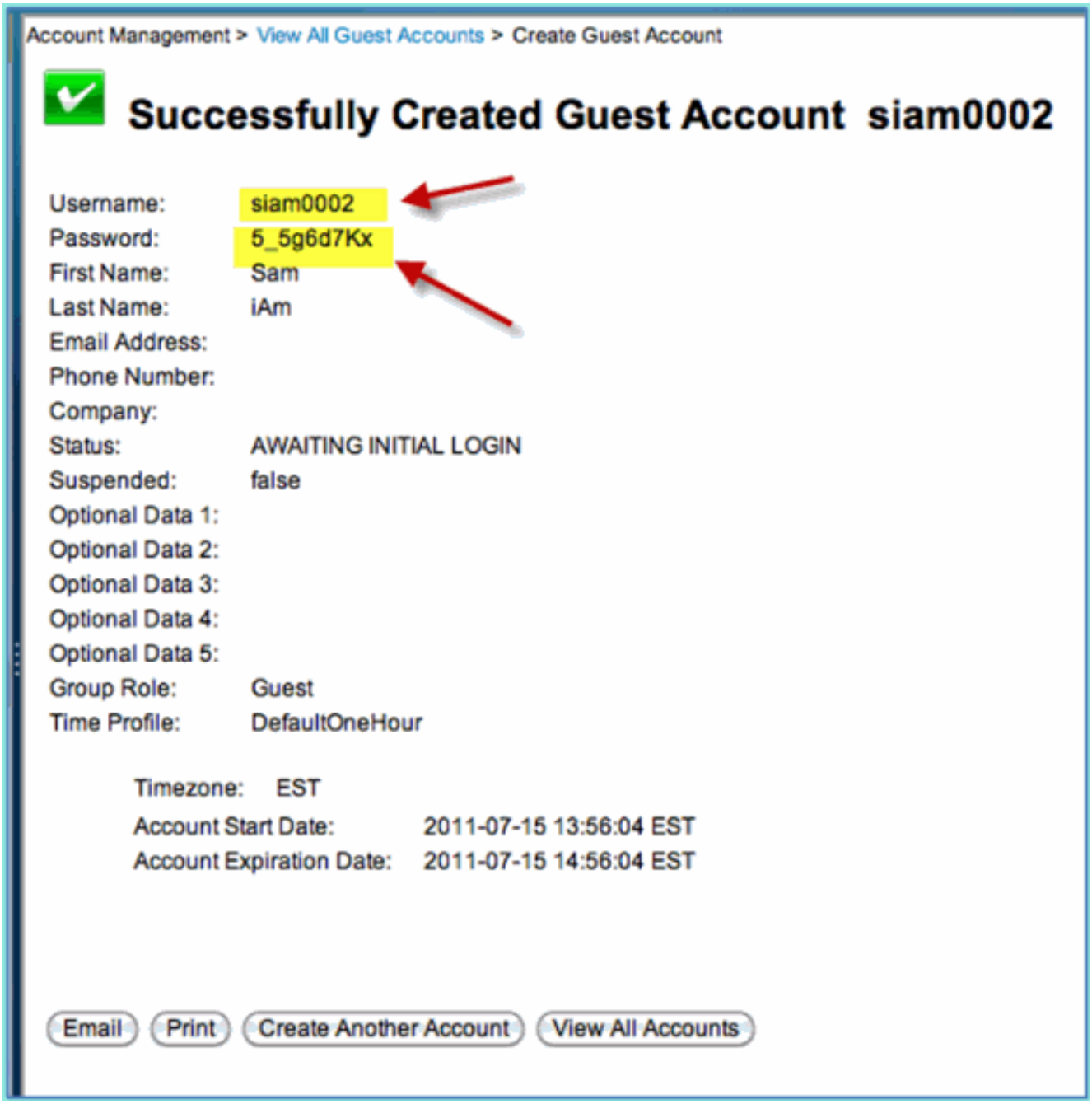
2. 在“发起人”(Sponsor)页面中，单击**创建单个访客用户帐户**。



3. 对于临时访客，添加以下内容：名字：必填（例如，Sam）姓氏：必填（例如，Jones）组角色：访客时间配置文件：DefaultOneHour时区：任意/默认



4. 单击“Submit”。
5. 访客帐户根据您之前的输入创建。请注意，密码可见（从上一个练习中），与散列密码相***。
6. 保持此窗口打开，显示访客的用户名和密码。您将使用它们测试访客门户登录（下一步）。



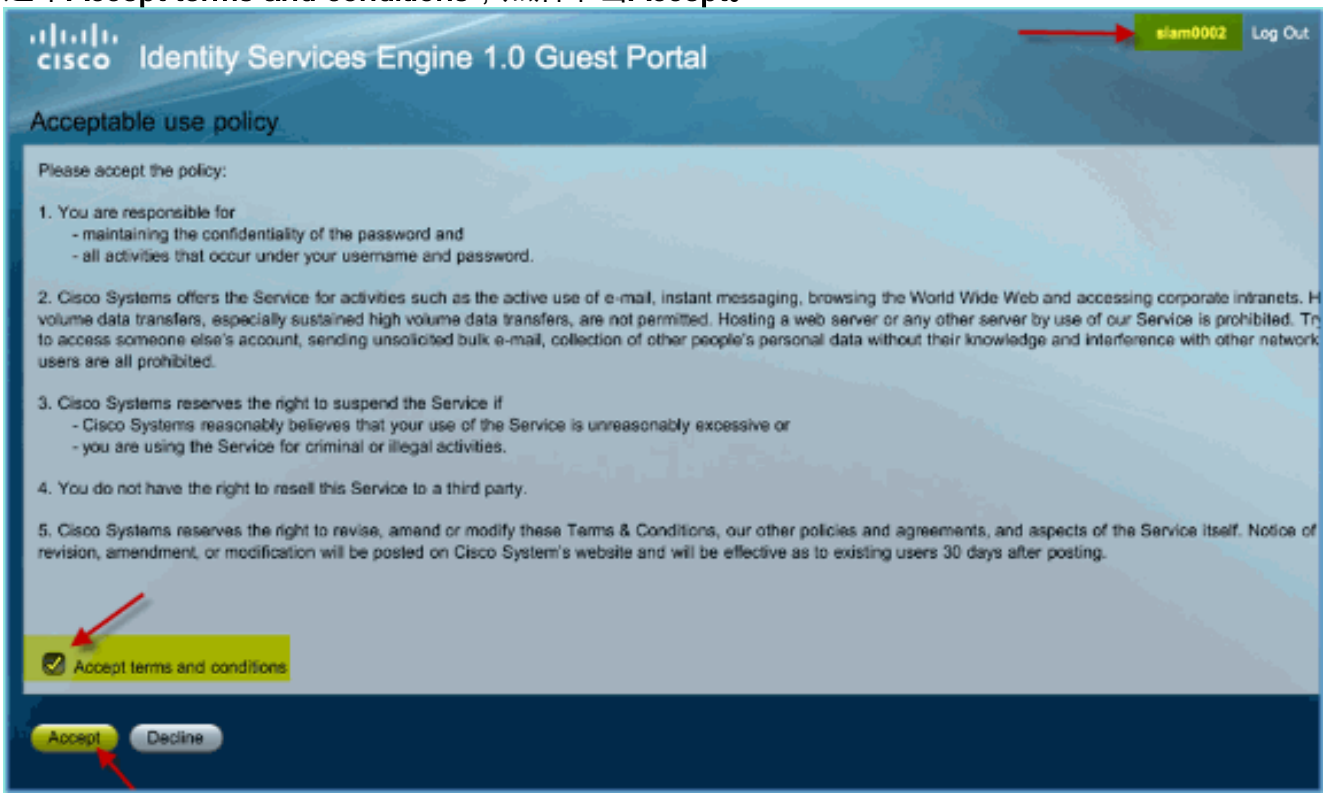
测试访客门户访问

使用AD用户/发起人创建的新访客帐户，测试访客门户和访问权限的时机到了。

请完成以下步骤：

1. 在首选设备（本例中为Apple iOS/iPad）上，连接到Pod访客SSID并检查IP地址/连接。
2. 使用浏览器并尝试导航至http://www。您将重定向到“访客门户登录”页面。

3. 使用在上一个练习中创建的访客帐户登录。如果成功，系统将显示Acceptable use policy页面。
4. 选中**Accept terms and conditions**，然后单击**Accept**。



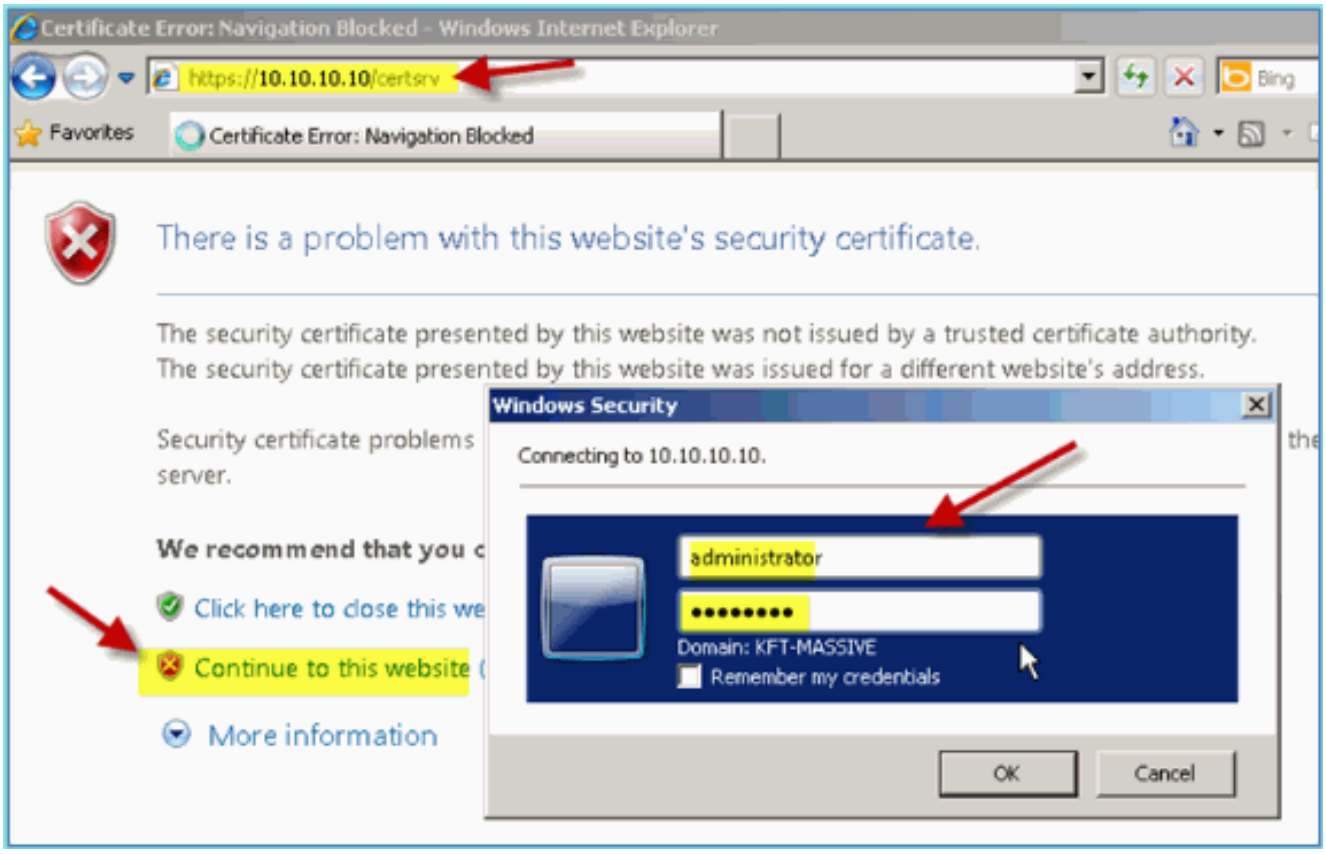
原始URL已完成，并且允许终端作为访客访问。

证书配置

要保护与ISE的通信，请确定该通信是身份验证相关还是用于ISE管理。例如，对于使用ISE Web UI的配置，需要配置X.509证书和证书信任链以启用非对称加密。

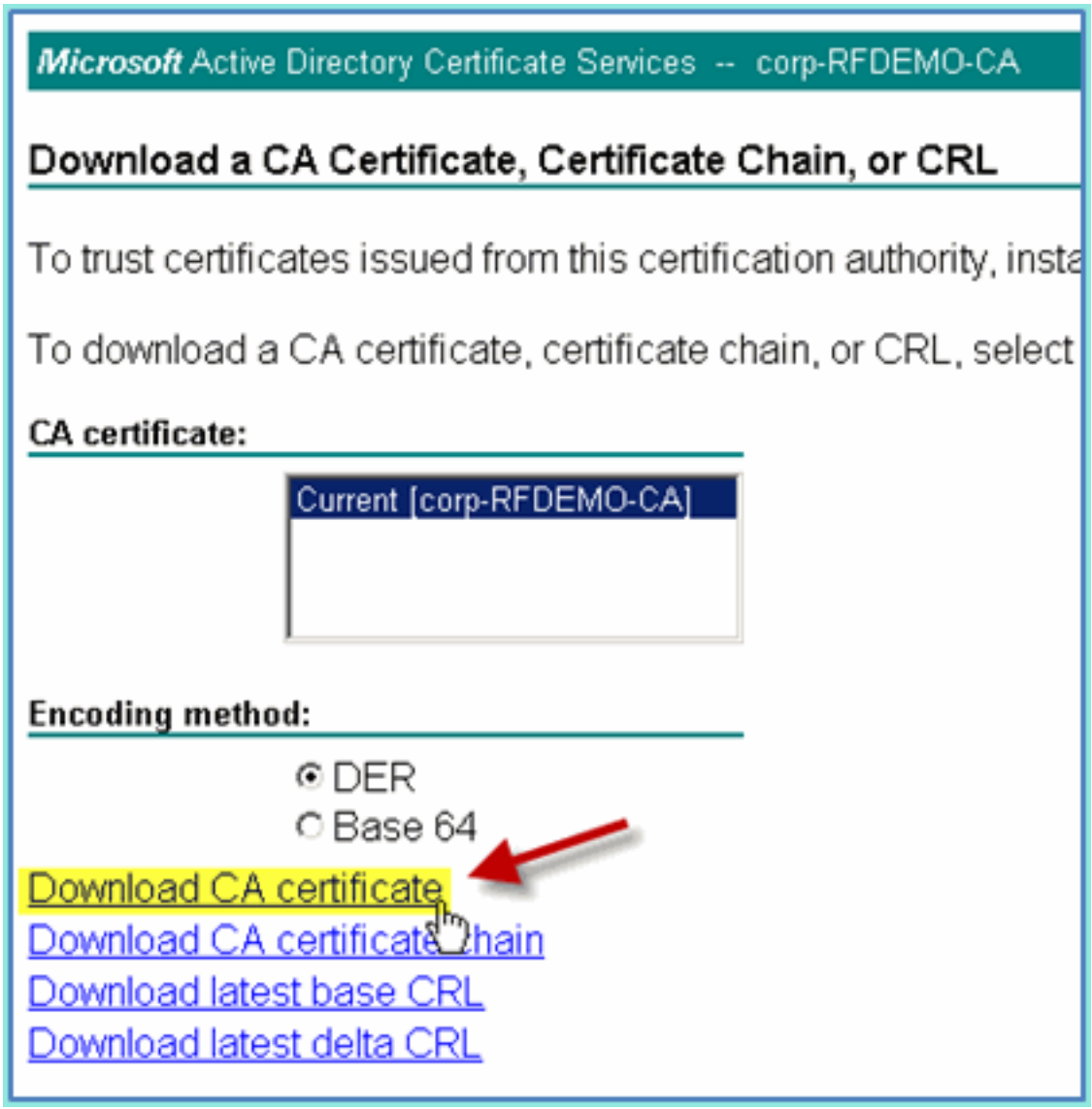
请完成以下步骤：

1. 从有线连接的PC上，打开一个浏览器窗口，转到https://AD/certsrv。**注意**：使用安全HTTP。**注**：请使用Mozilla Firefox或MS Internet Explorer访问ISE。
2. 以管理员/Cisco123身份登录。

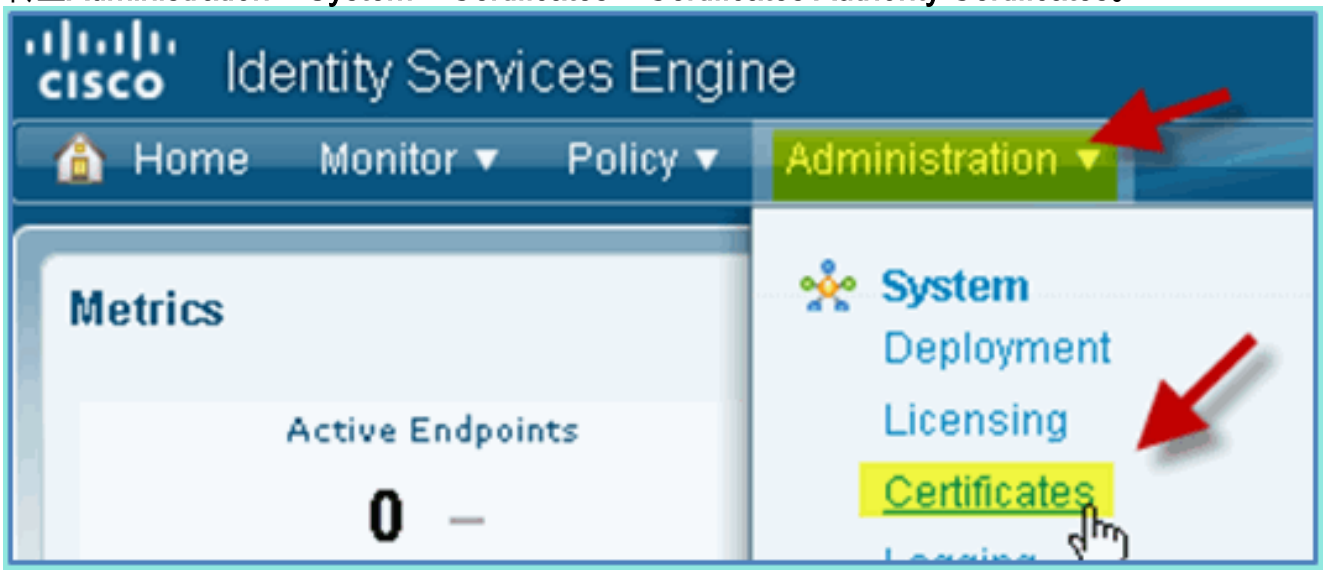


3. 单击 Download a CA certificate, certificate chain, or CRL。

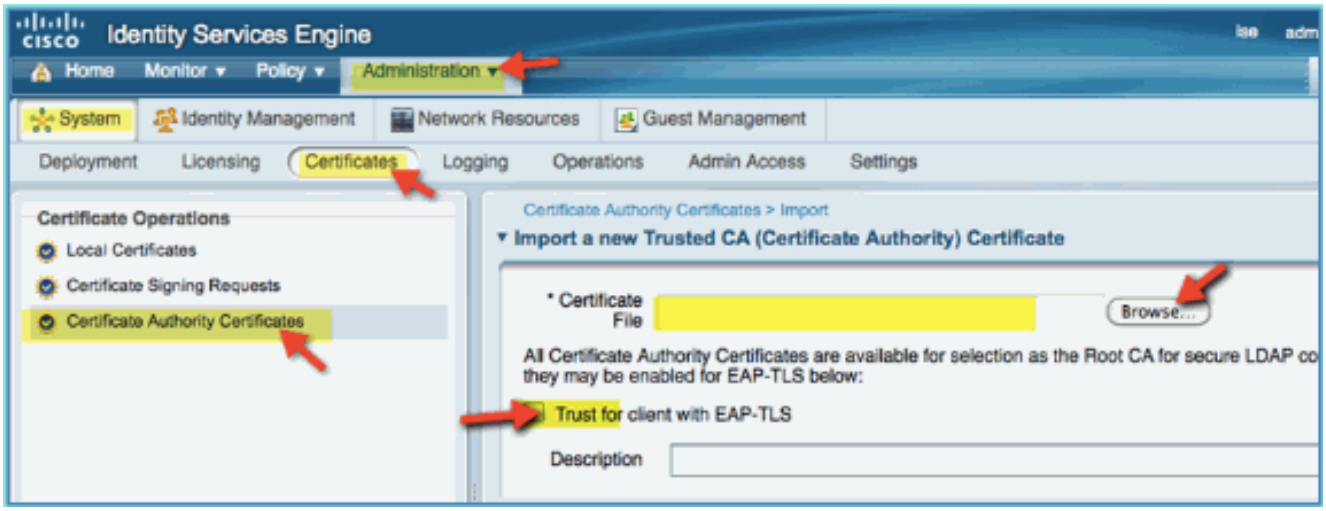
4. 单击Download CA certificate并保存它（注意保存位置）。



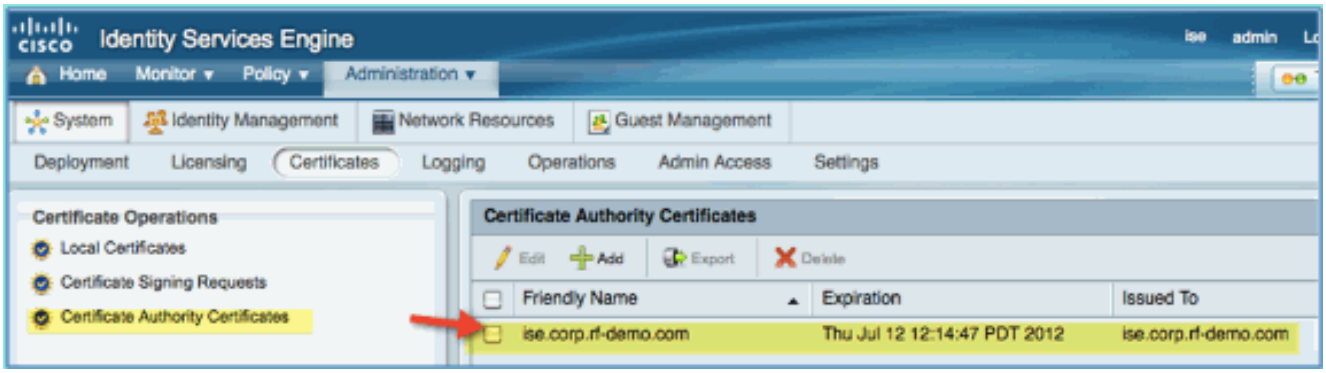
5. 打开浏览器窗口访问https://<Pod-ISE>。
6. 转至**Administration > System > Certificates > Certificates Authority Certificates**。



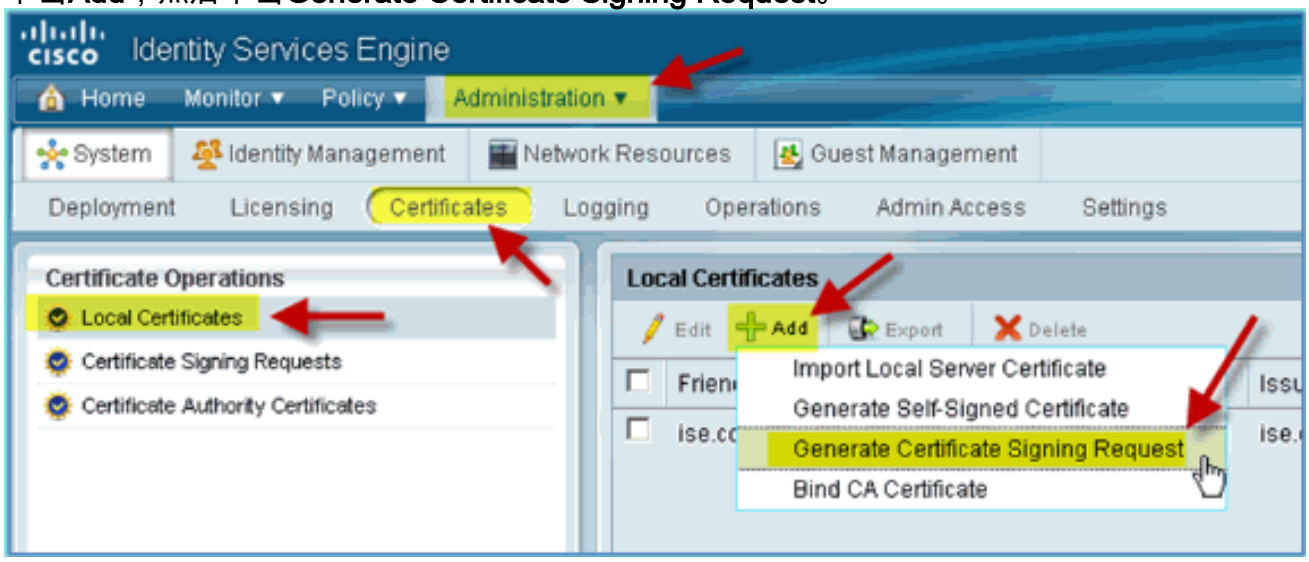
7. 选择**Certificate Authority Certificates**操作并浏览到以前下载的CA证书。
8. 选择**Trust for client with EAP-TLS**，然后提交。



9. 确认已将CA添加为受信任的根CA。



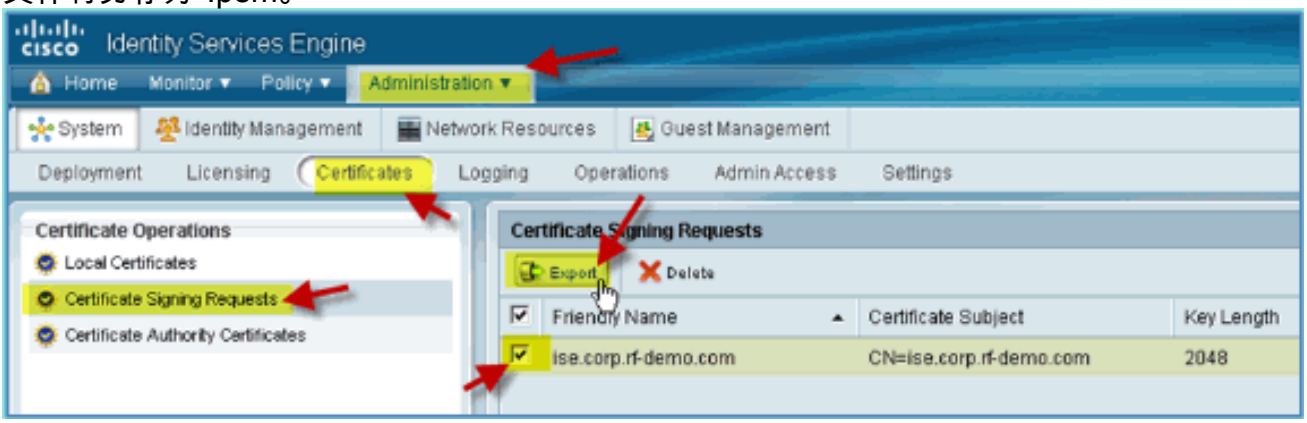
10. 从浏览器转到**Administration > System > Certificates > Certificates Authority Certificates**。
11. 单击**Add**，然后单击**Generate Certificate Signing Request**。



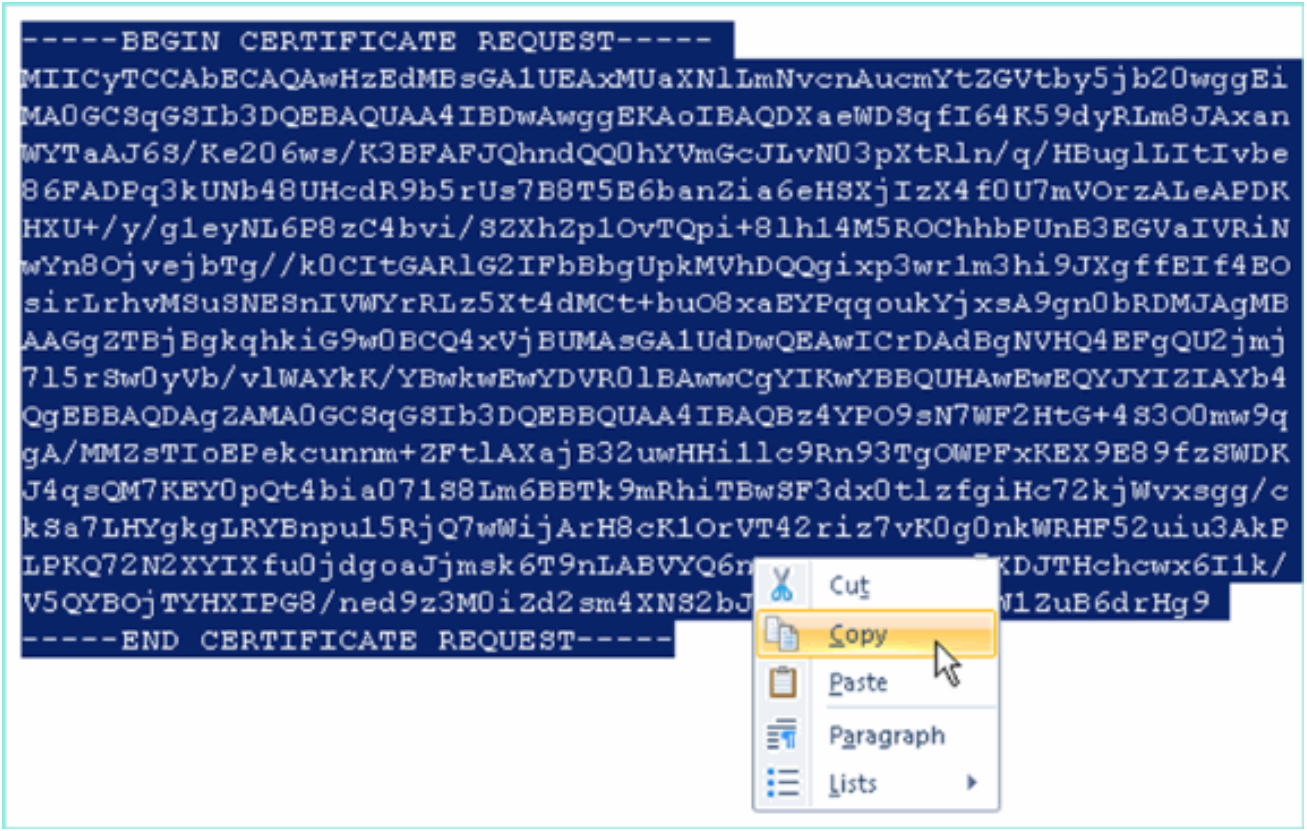
12. 提交以下值：证书主题：CN=ise.corp.rf-demo.com密钥长度：2048

13. ISE提示在CSR页面中提供CSR。Click OK.

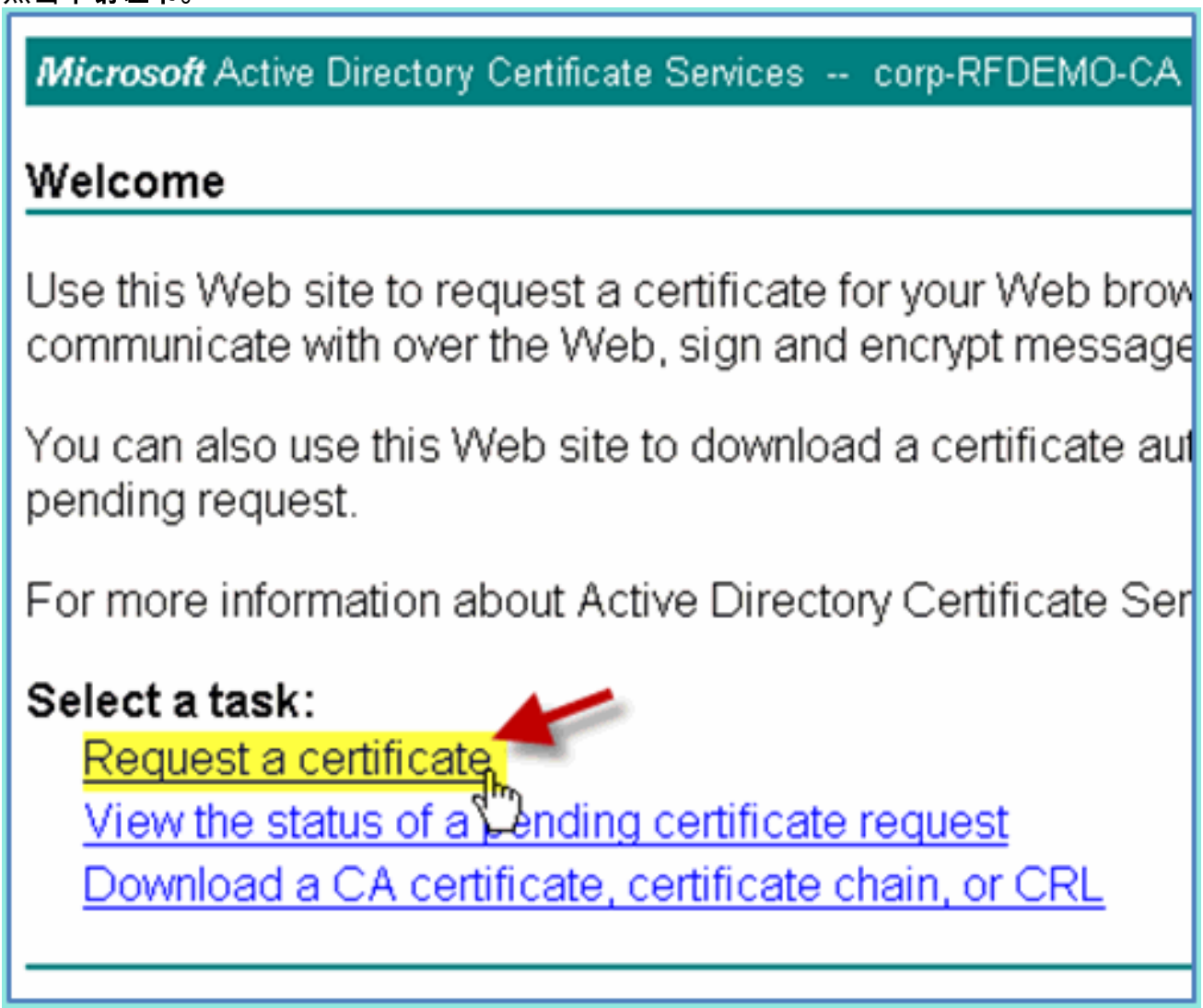
14. 从ISE CSR页面选择CSR并点击**导出**。
15. 将文件保存到任何位置（例如，下载等）
16. 文件将另存为*.pem。



17. 找到CSR文件并使用记事本/写字板/文本编辑进行编辑。
18. 复制内容（“全选”>“复制”）。

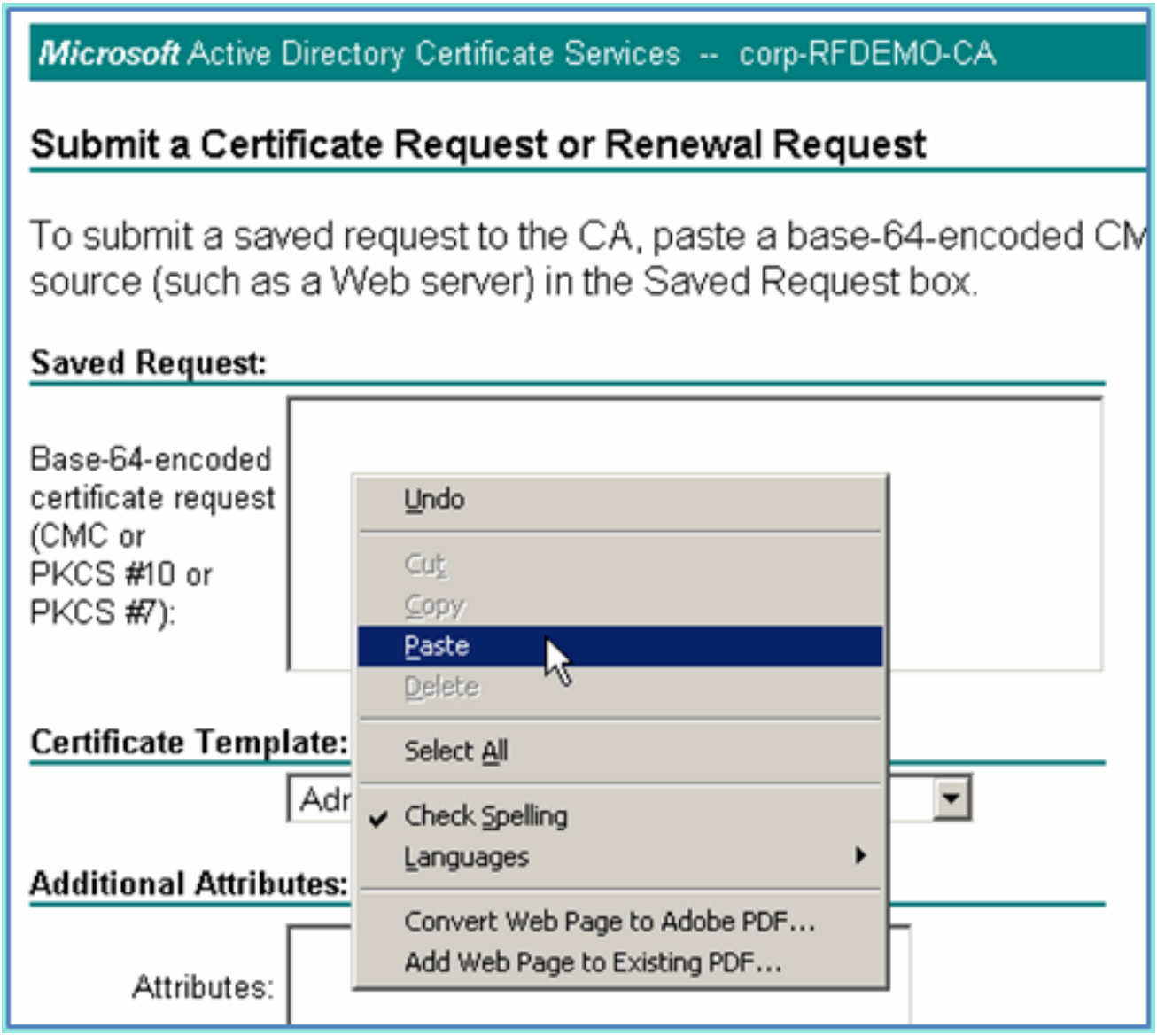


19. 打开浏览器窗口访问https://<Pod-AD>/certsrv。
20. 点击**申请证书**。

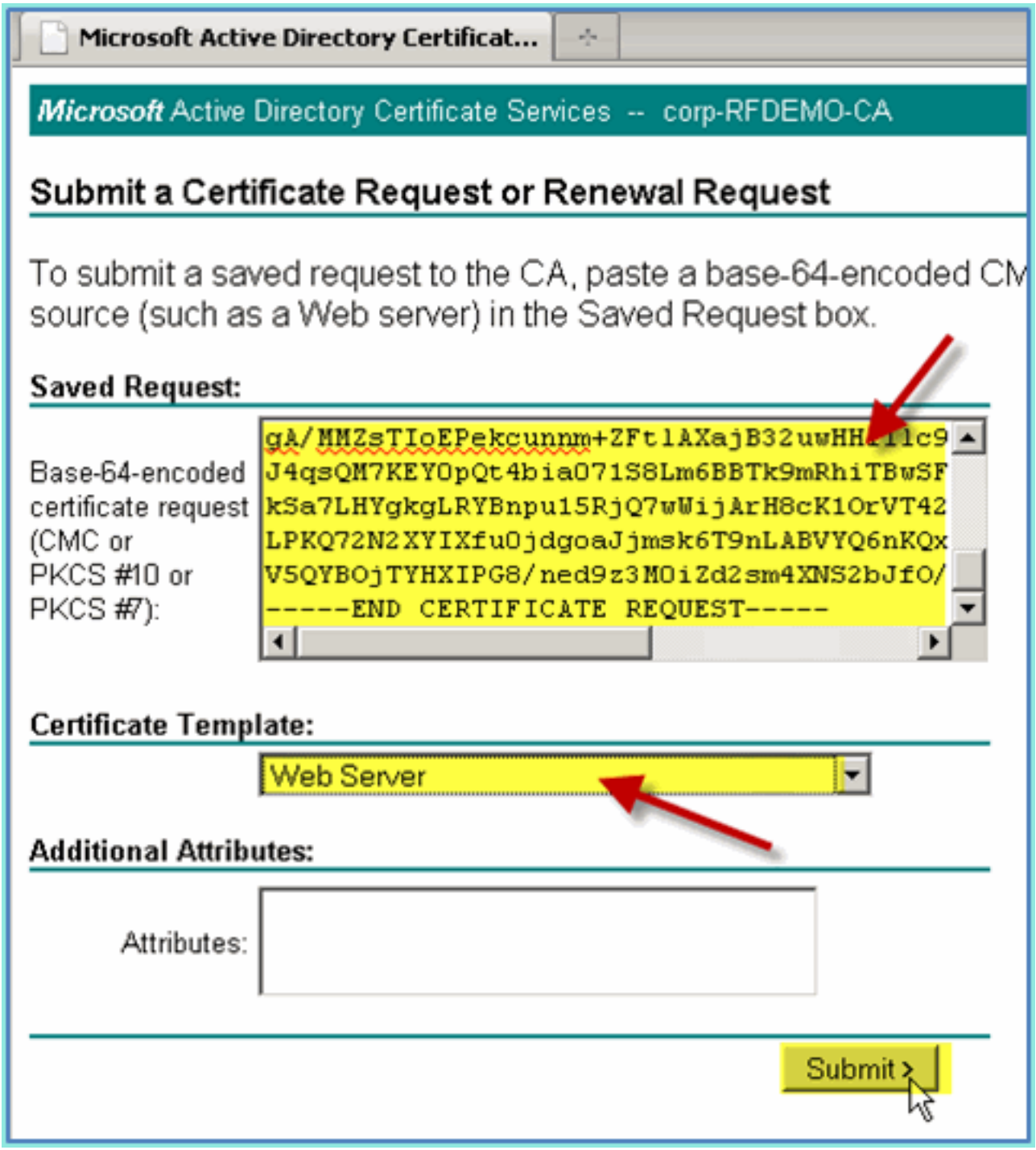


21. 单击以提交**高级证书申请**。

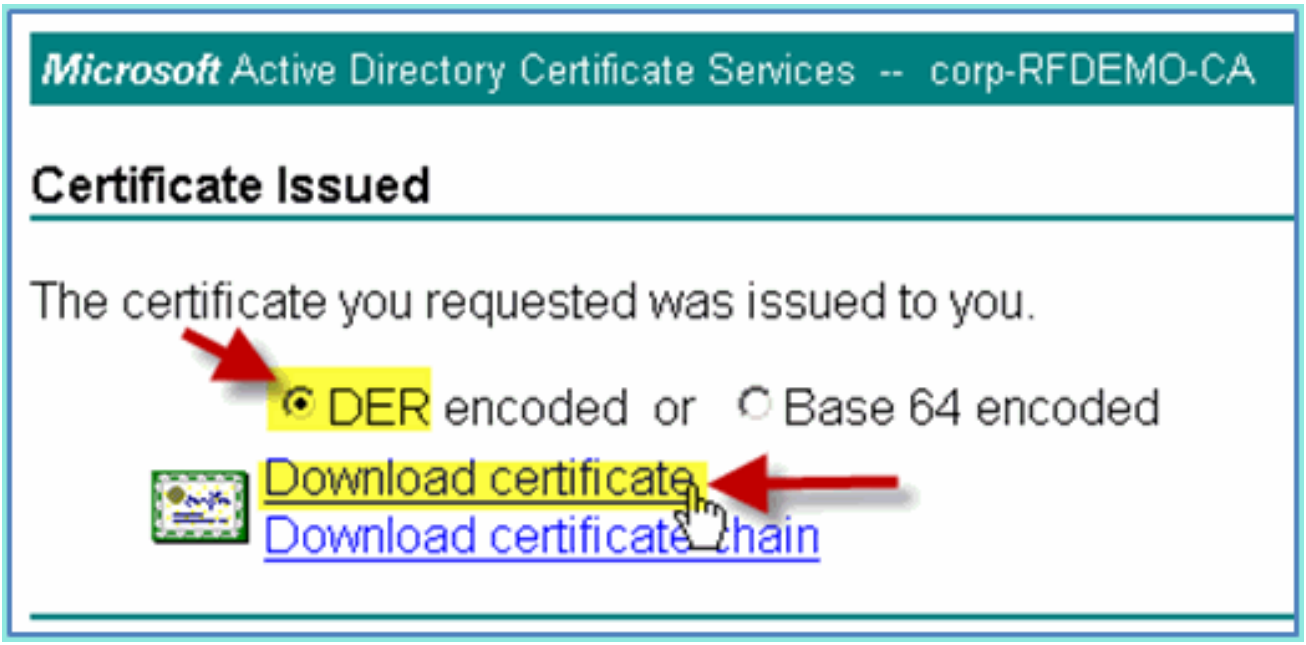
22. 将CSR内容粘贴到已保存请求字段中。



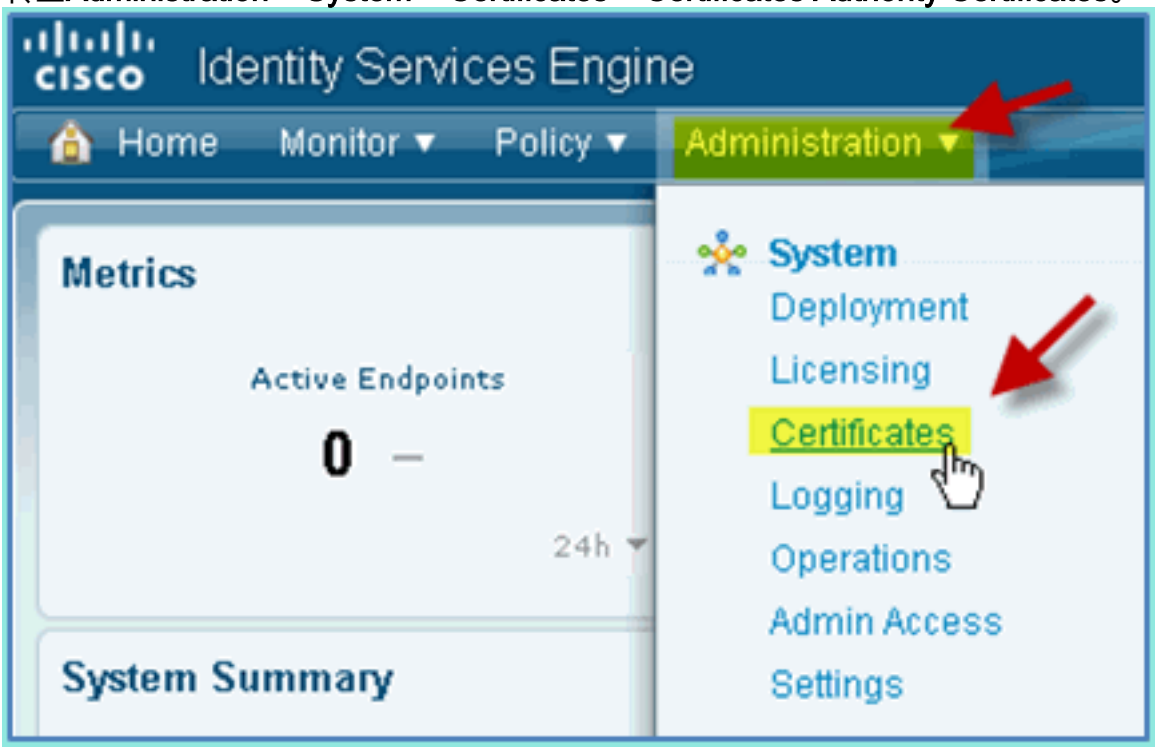
23. 选择**Web Server**作为证书模板，然后单击**Submit**。



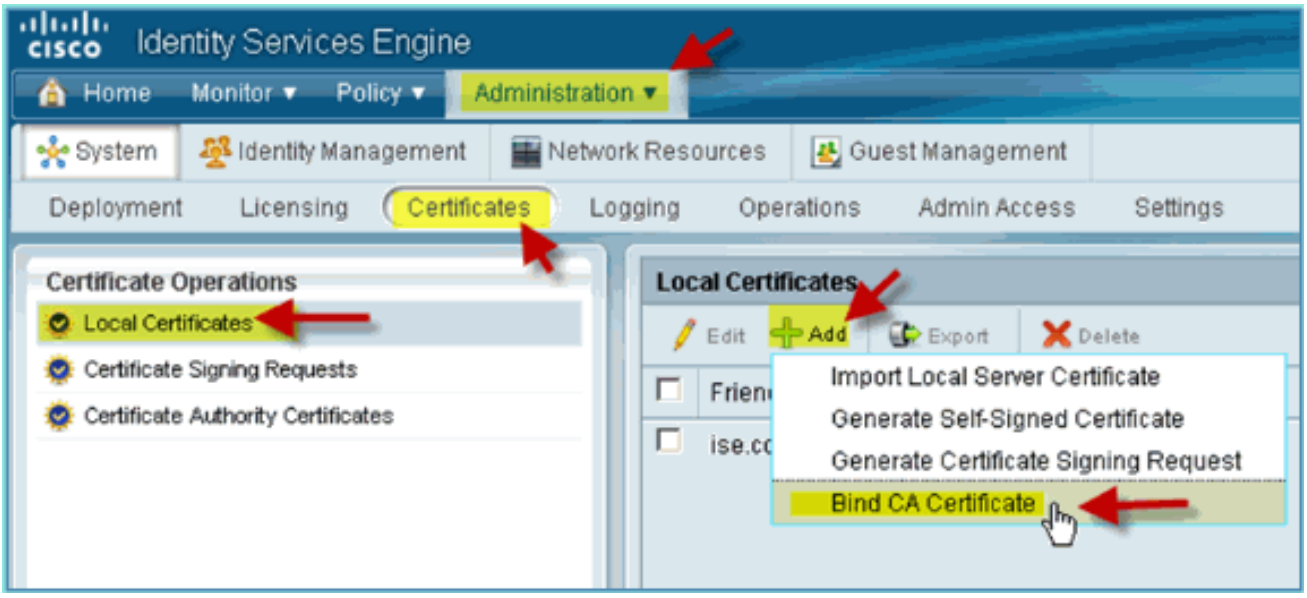
24. 选择DER encoded，然后单击Download certificate。



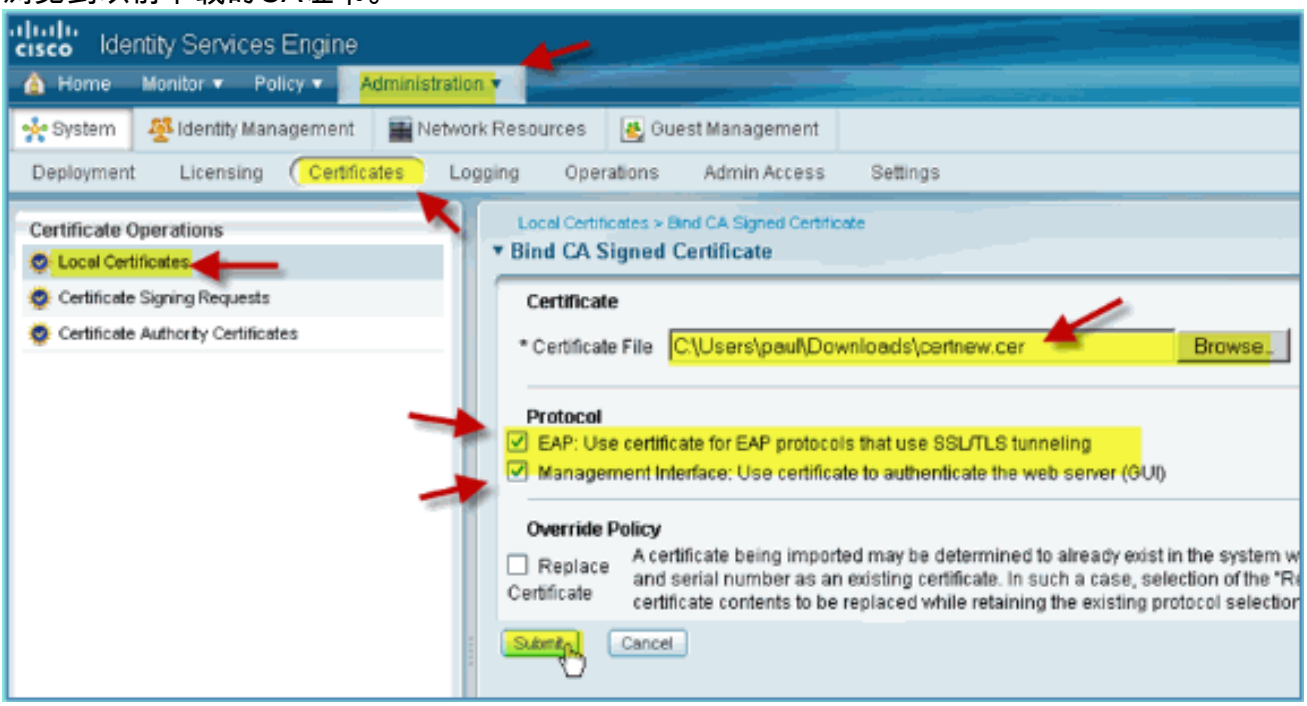
25. 将文件保存到已知位置（例如，下载）
26. 转至**Administration > System > Certificates > Certificates Authority Certificates**。



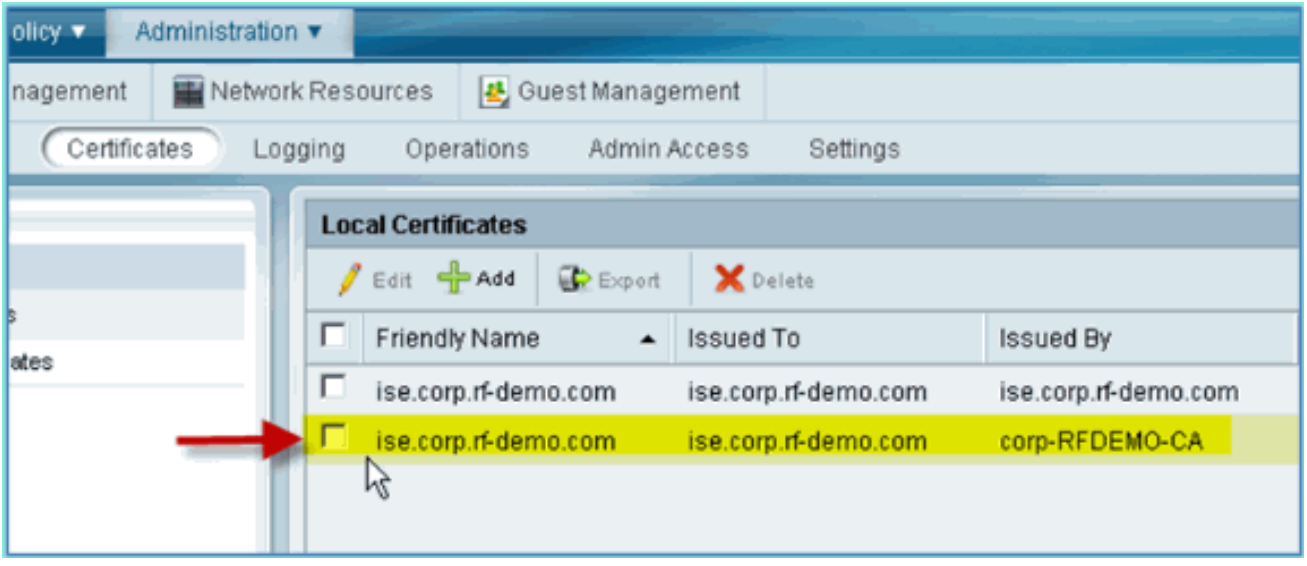
27. 单击**Add > Bind CA Certificate**。



28. 浏览到以前下载的CA证书。



29. 选择**Protocol EAP**和**Management Interface**，然后单击**Submit**。
30. 确认已将CA添加为受信任的根CA。

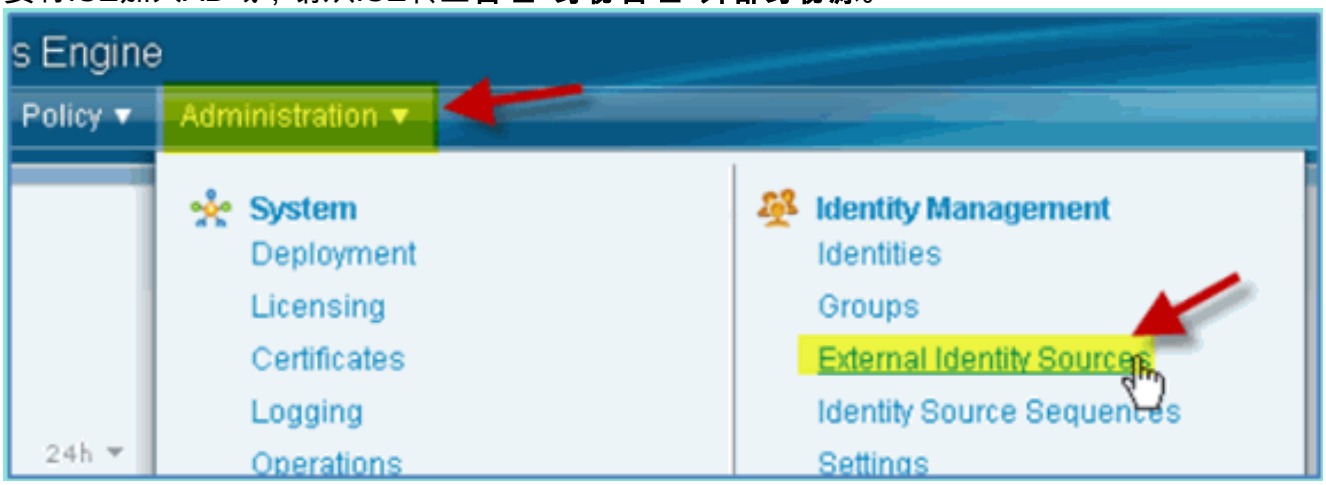


Windows 2008 Active Directory集成

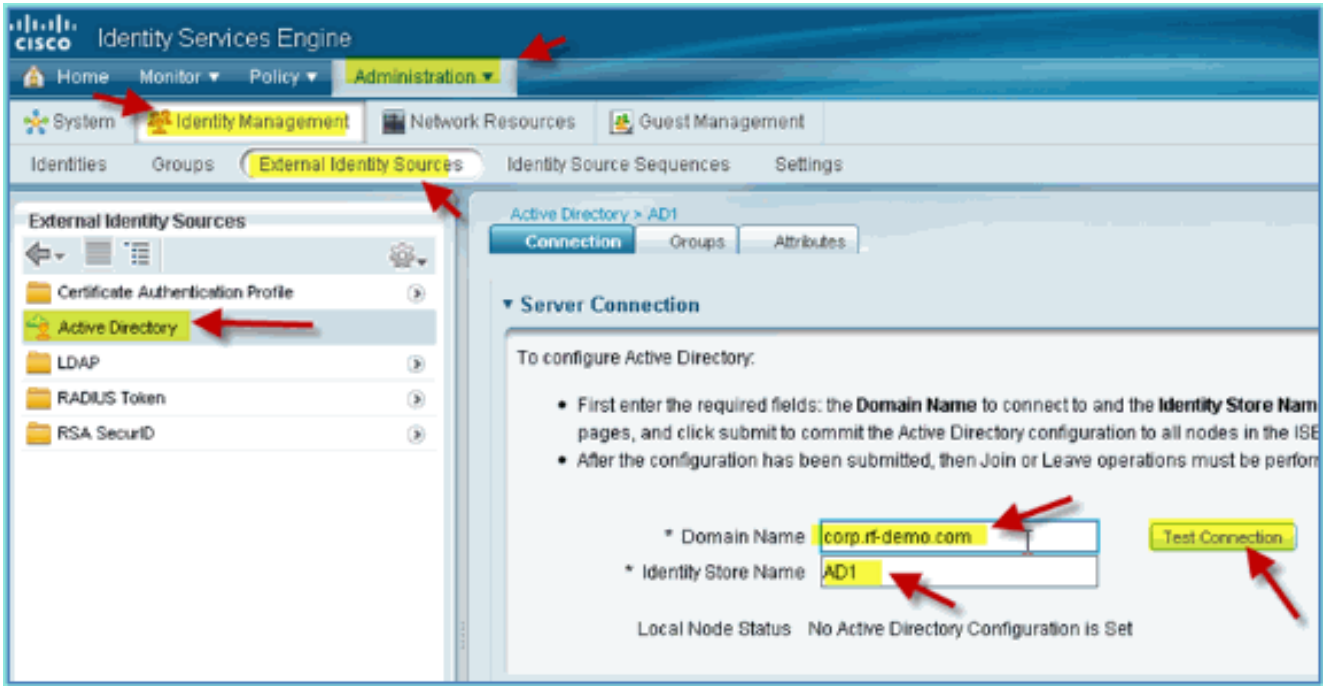
ISE可以直接与Active Directory(AD)进行通信，以进行用户/机器身份验证或检索授权信息用户属性。为了与AD通信，ISE必须“加入”到AD域。在本练习中，您将将ISE加入AD域，并确认AD通信是否正常工作。

请完成以下步骤：

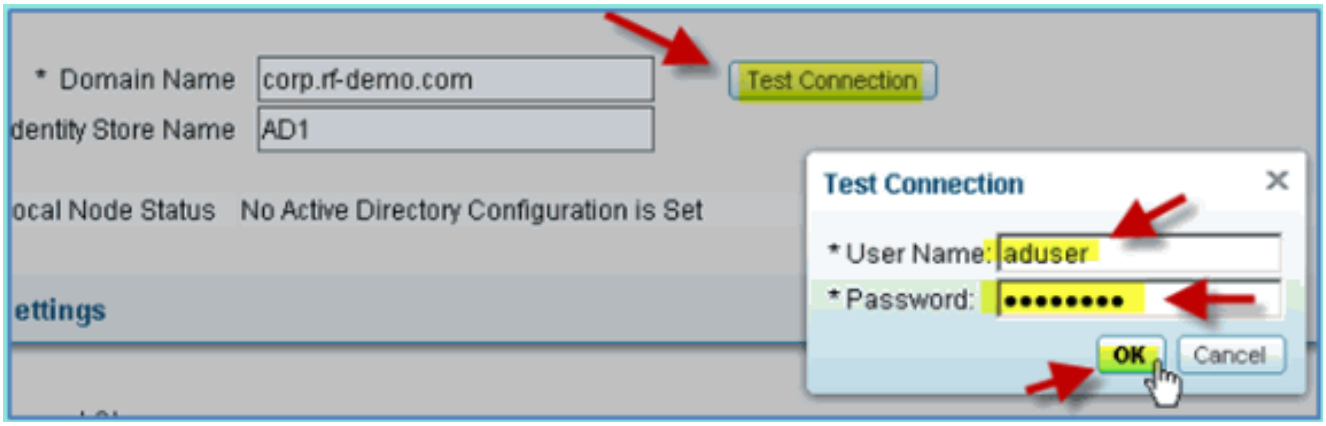
1. 要将ISE加入AD域，请从ISE转至**管理>身份管理>外部身份源**。



2. 从左侧窗格（外部身份源）中选择**Active Directory**。
3. 在右侧，选择**Connection**选项卡并输入以下内容：域名：corp.rf-demo.com身份库名称：AD1

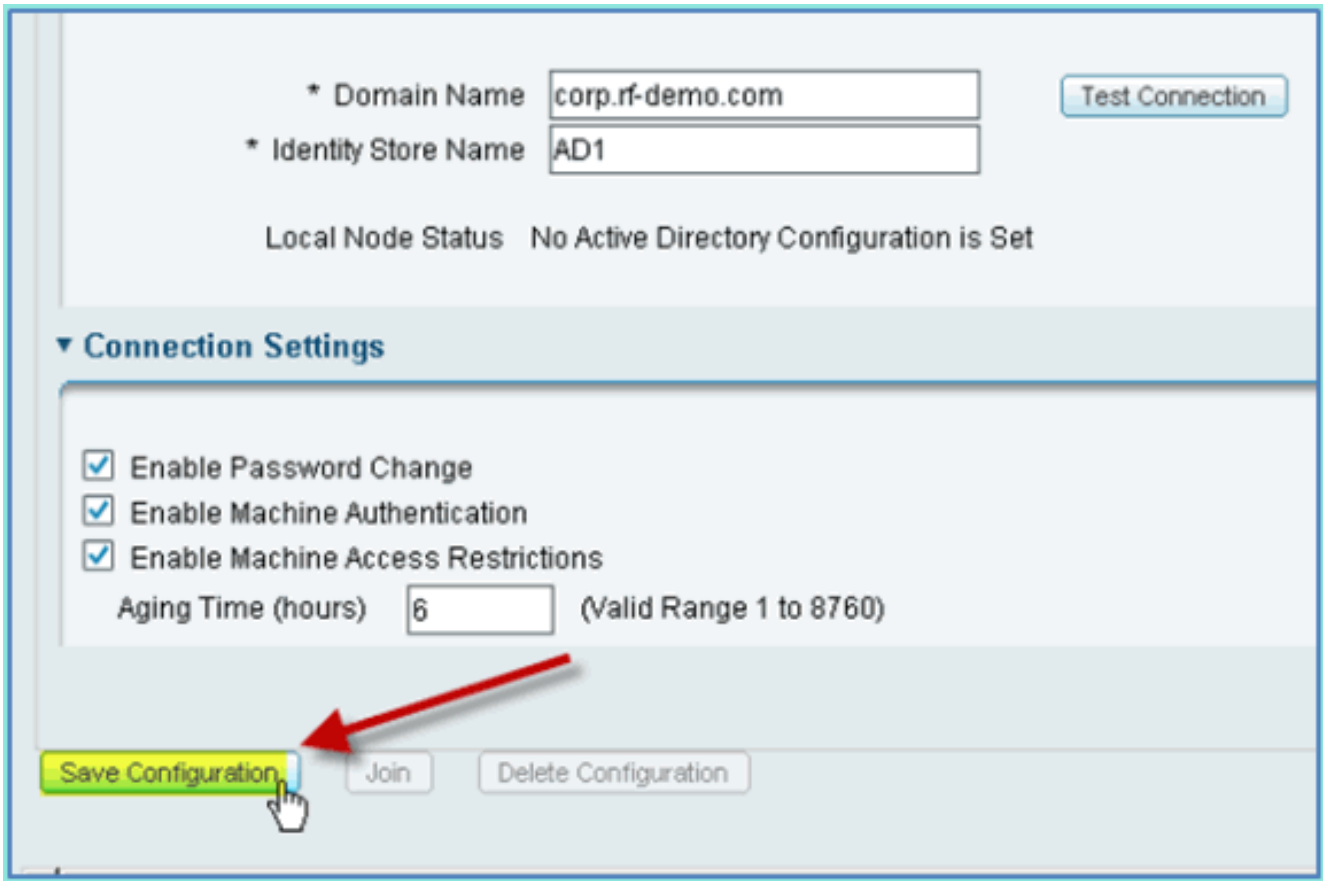


4. 单击**Test Connection**。输入AD用户名(aduser/Cisco123)，然后单击**OK**。

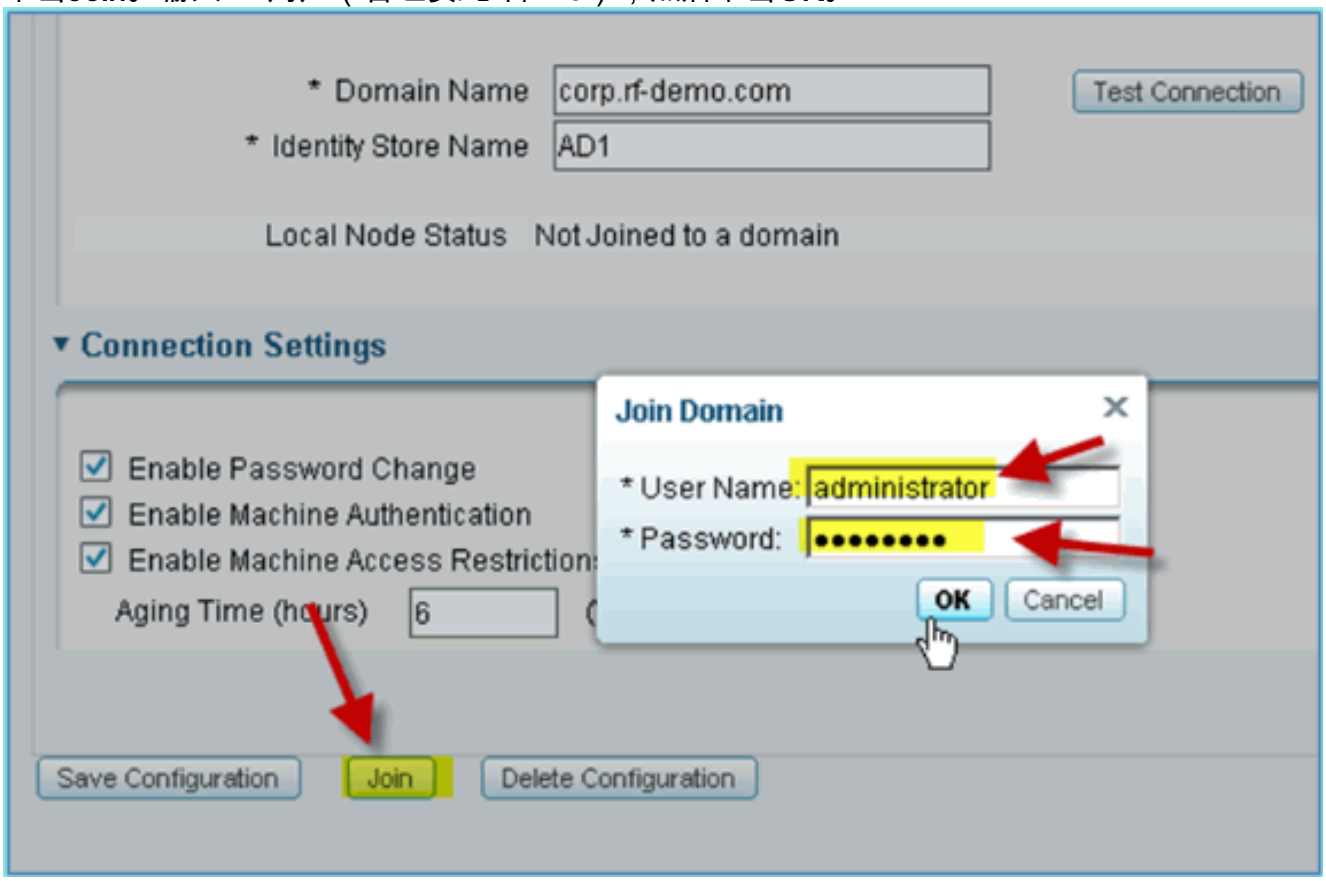


5. 确认“测试状态”显示测试成功(**Test Succeeded**)。
6. 选择Show Detailed Log并观察对故障排除有用的详细信息。单击 **OK 继续。**

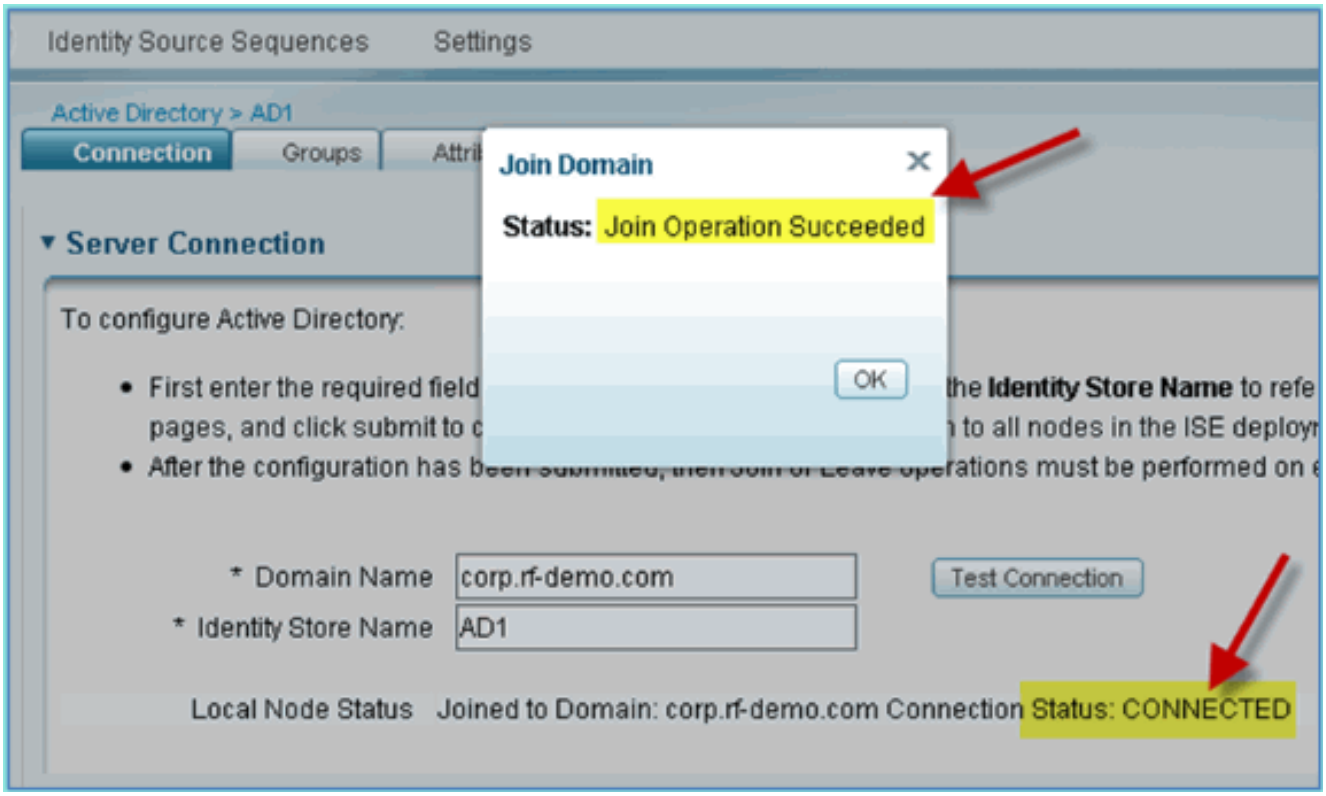
7. 单击**Save Configuration**。



8. 单击**Join**。输入AD用户（管理员/思科123），然后单击**OK**。



9. 确认Join Operation Status显示为**Succeeded**，然后单击**OK**继续。服务器连接状态显示**CONNECTED**。如果此状态随时更改，测试连接将帮助排除AD操作问题。



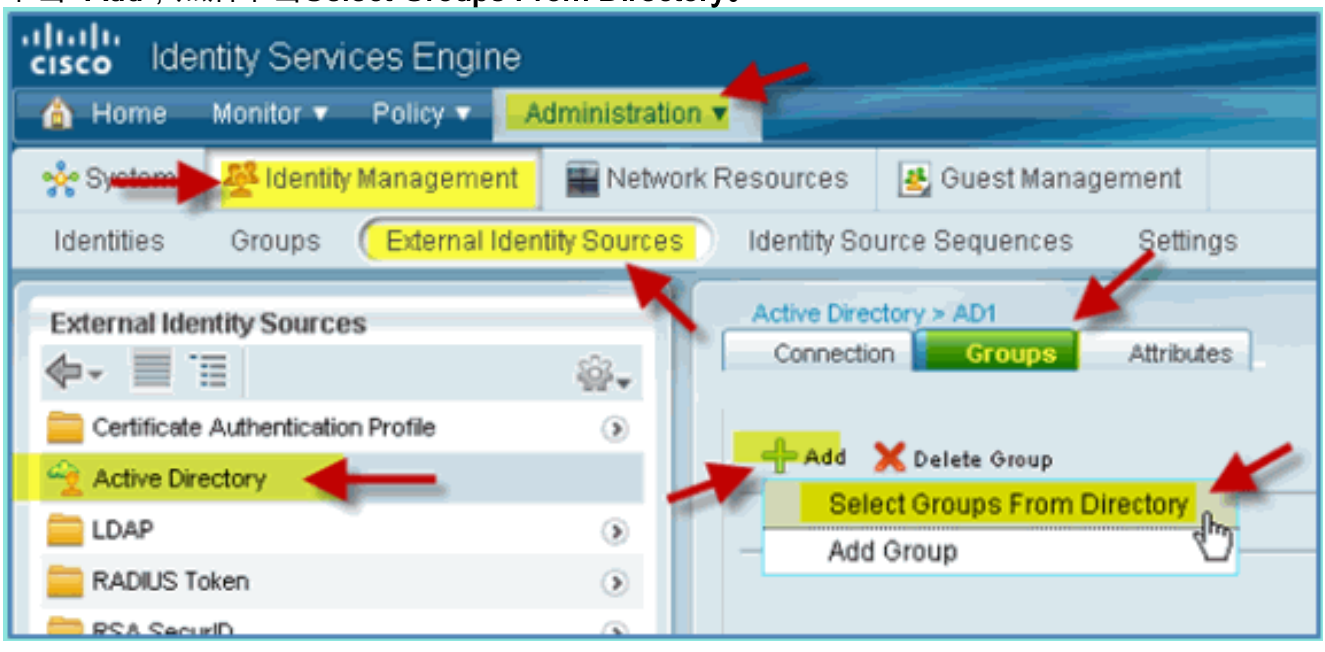
添加Active Directory组

添加AD组时，允许对ISE策略进行更精细的控制。例如，AD组可以按功能角色（如员工或承包商组）区分，而不会在以前的ISE 1.0练习中遇到相关漏洞，在此练习中，策略仅限于用户。

在本实验中，仅使用Domain Users和/或Employee组。

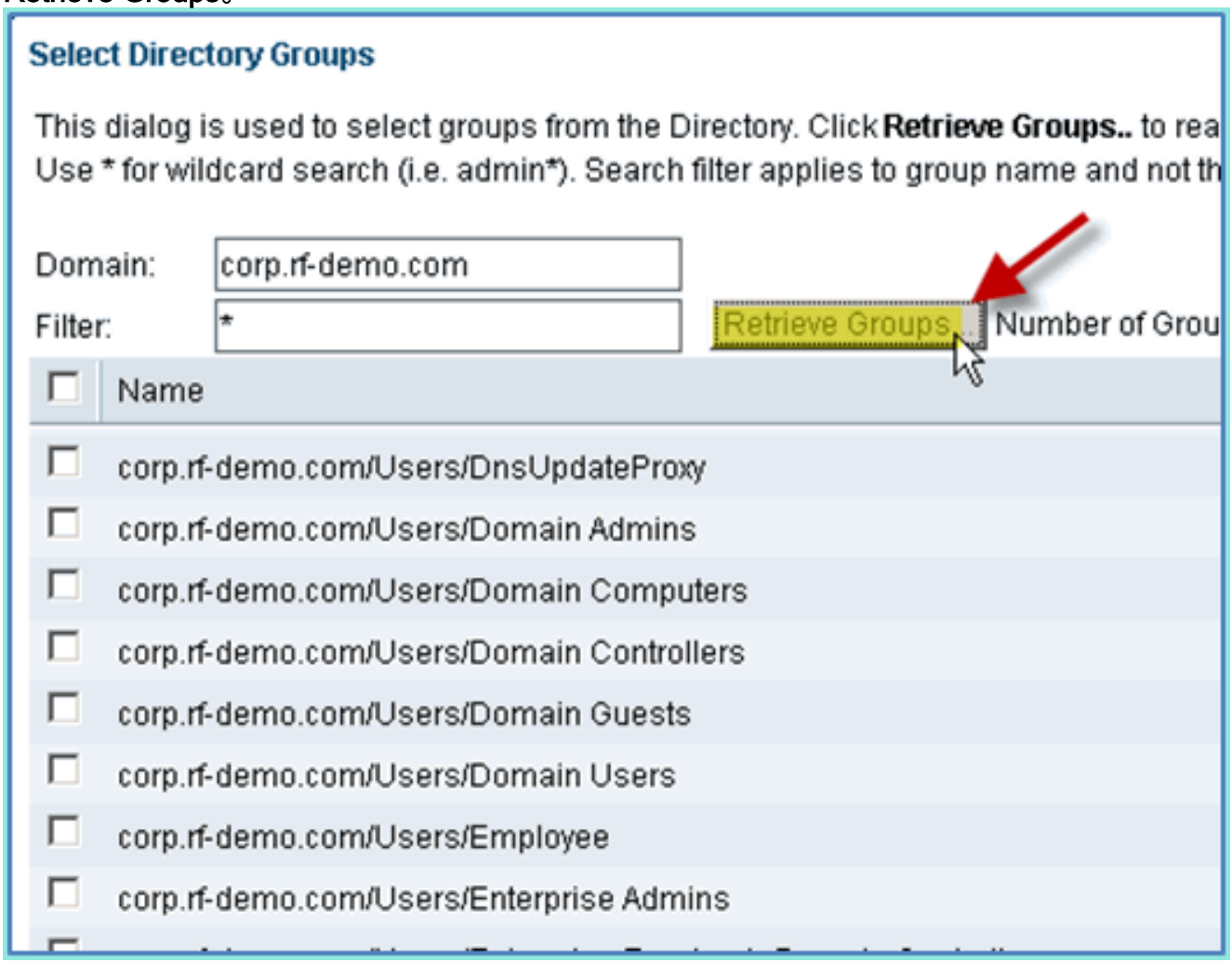
请完成以下步骤：

1. 从ISE，转至**管理>身份管理>外部身份源**。
2. 选择**Active Directory > Groups**选项卡。
3. 单击**+Add**，然后单击**Select Groups From Directory**。

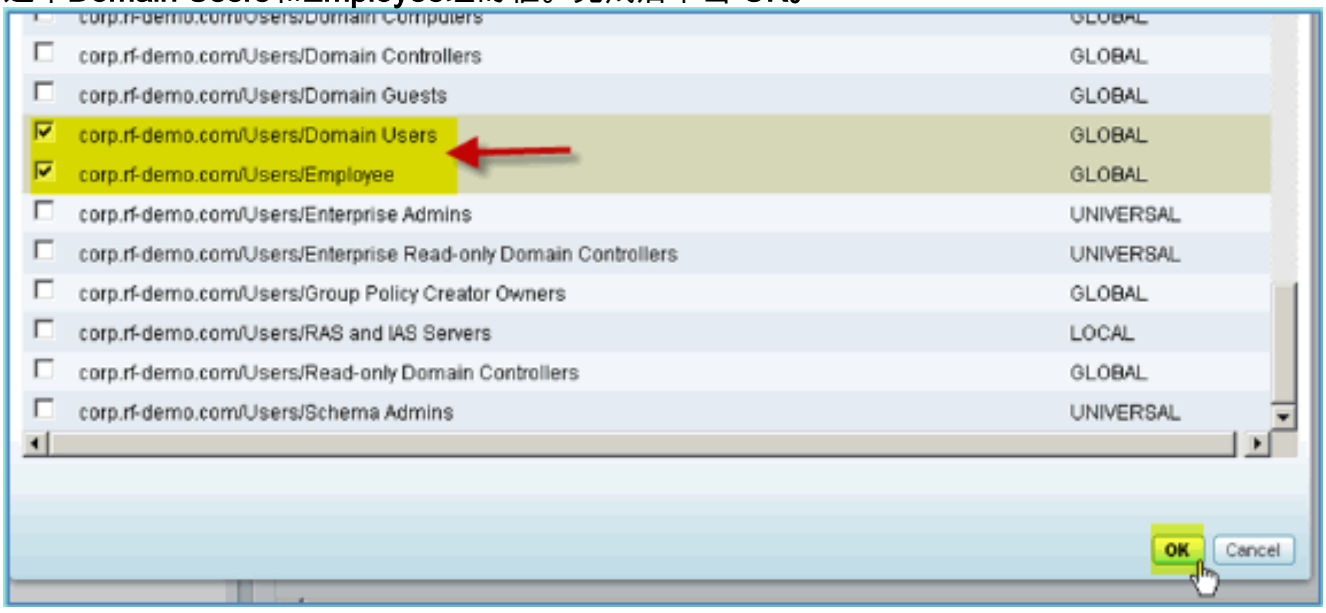


4. 在后续窗口（选择目录组）中，接受域(corp-rf-demo.com)和过滤器(*)的默认值。然后，单击

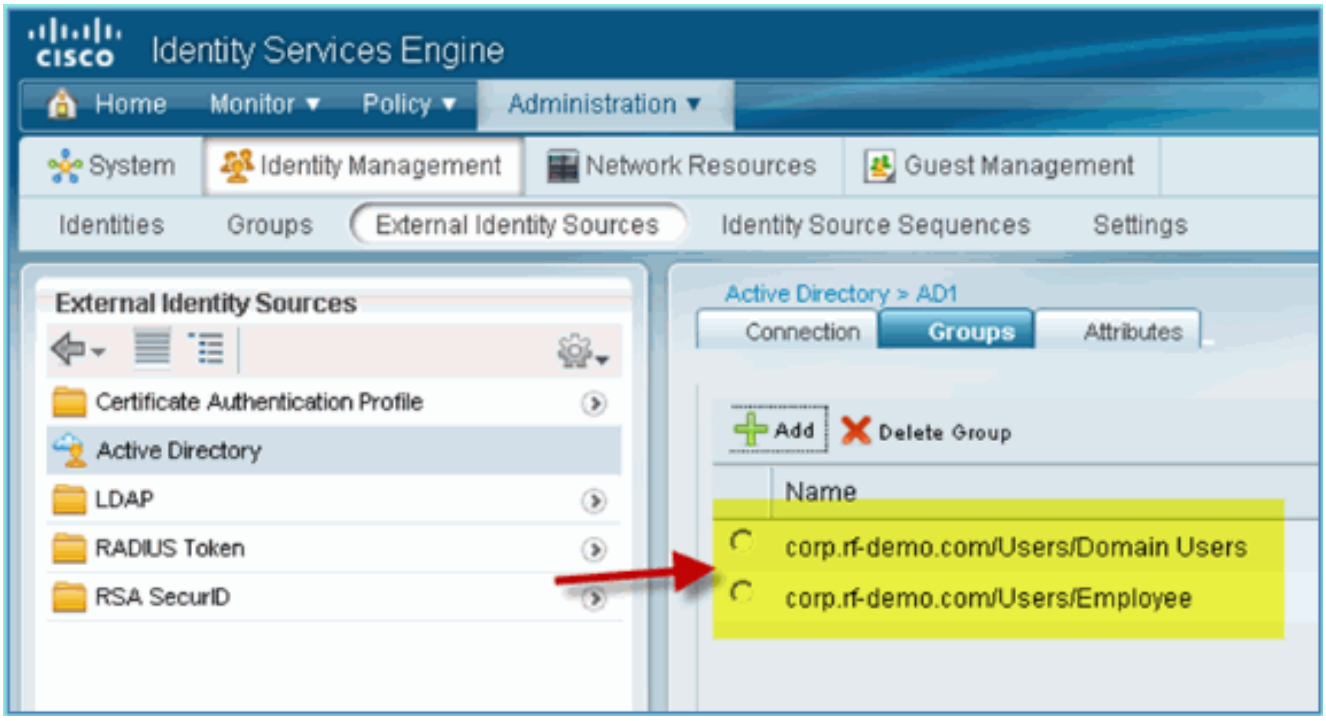
Retrieve Groups。



5. 选中Domain Users和Employee组的框。完成后单击 OK。



6. 确认已将组添加到列表中。

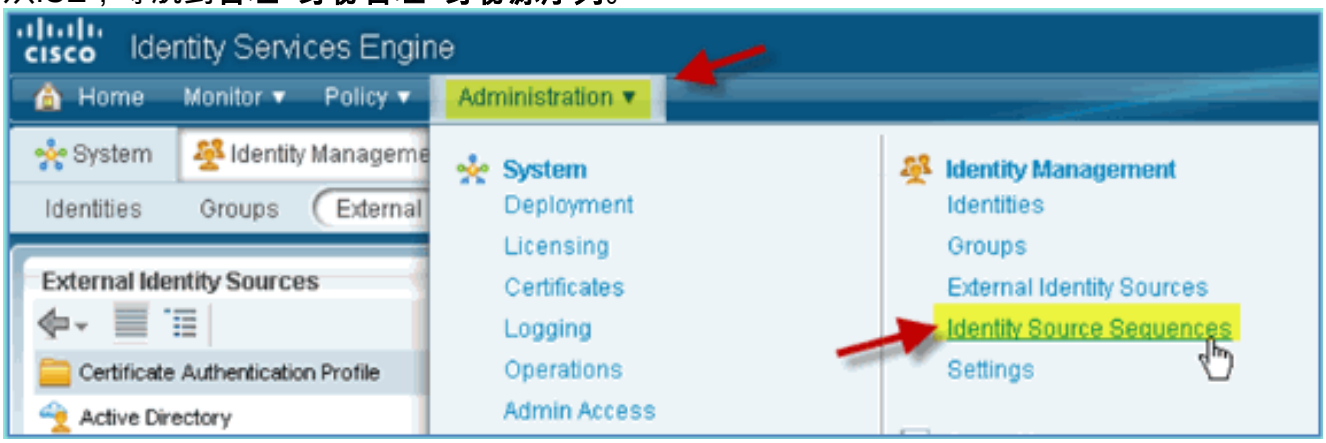


添加身份源序列

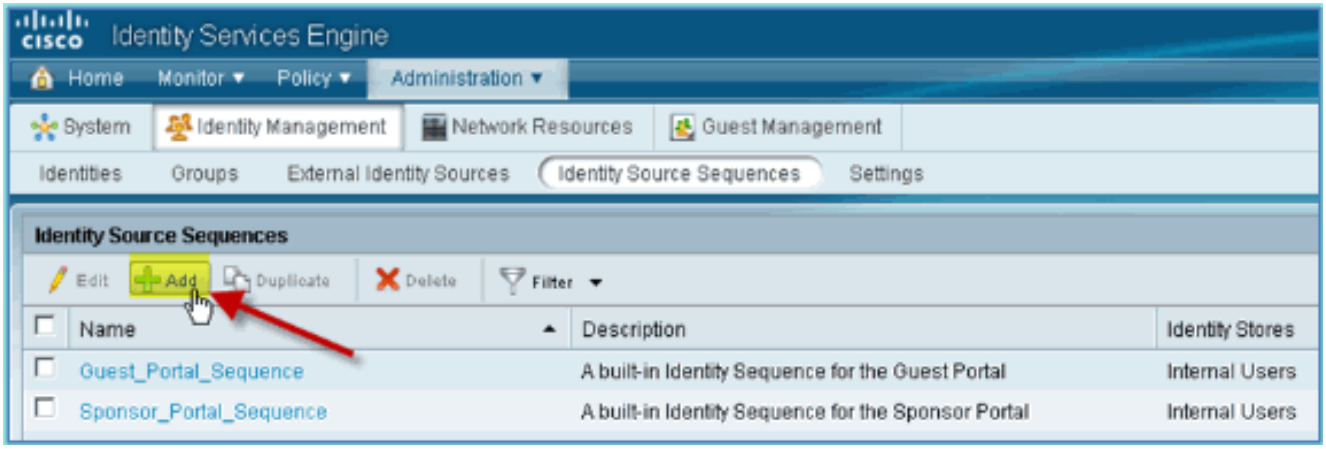
默认情况下，ISE设置为使用内部用户进行身份验证存储。如果添加AD，可以创建优先级顺序以包括ISE将用于检查身份验证的AD。

请完成以下步骤：

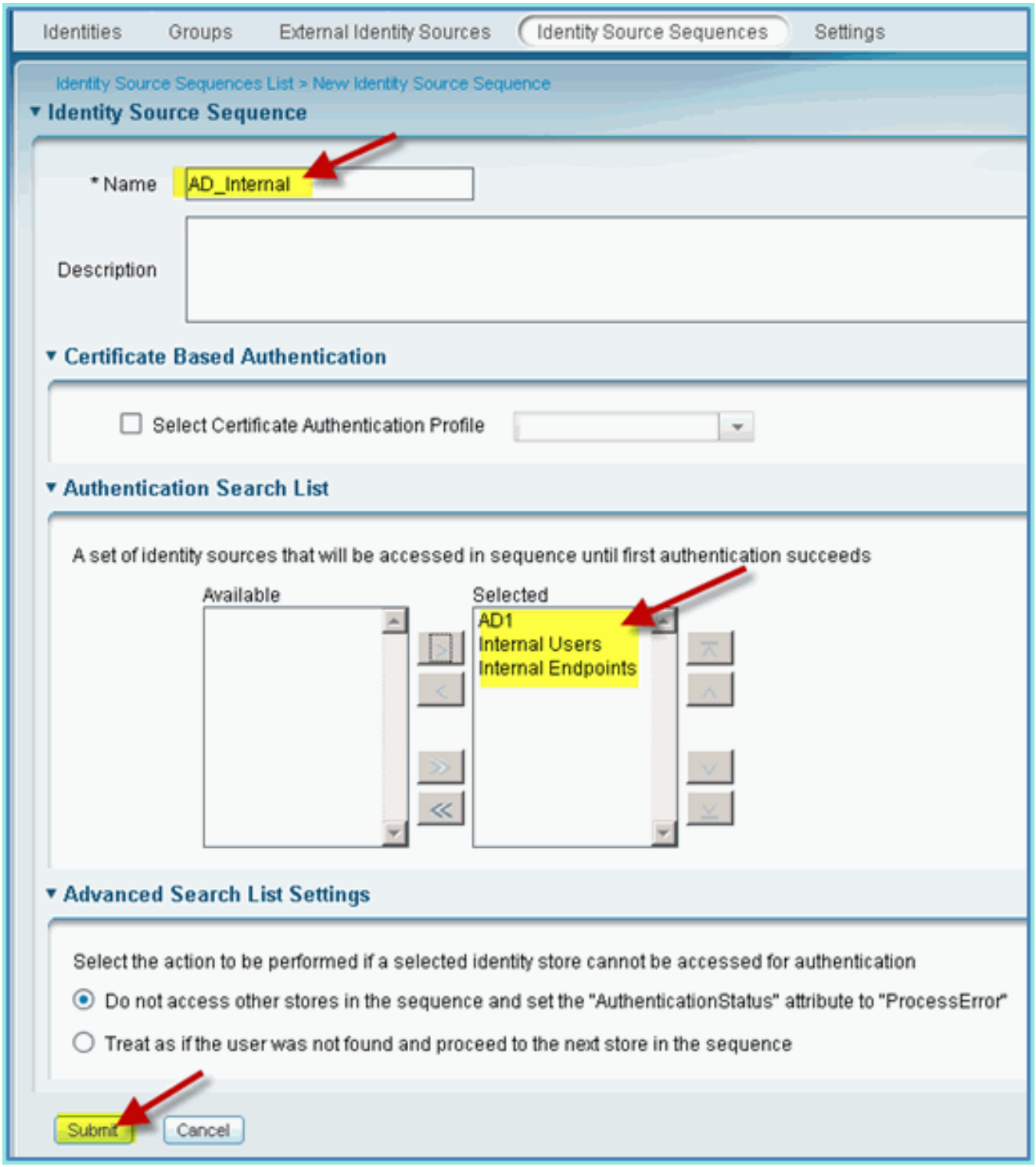
1. 从ISE，导航到**管理>身份管理>身份源序列**。



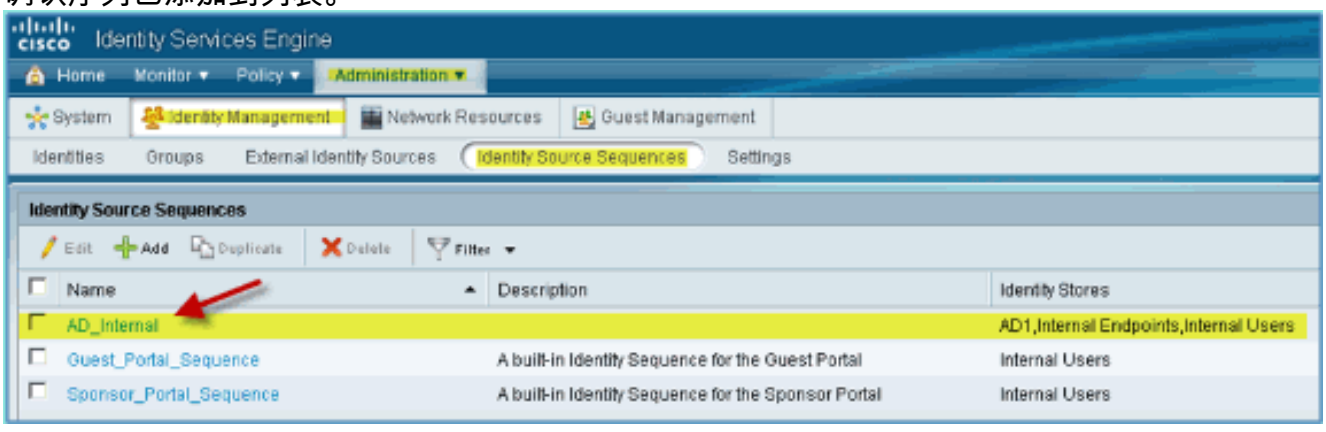
2. 单击**+Add**以添加新序列。



3. 输入新名称:**AD_Internal**。将所有可用源添加到Selected字段。然后，根据需要重新排序，将AD1移至列表顶部。单击“Submit”。



4. 确认序列已添加到列表。

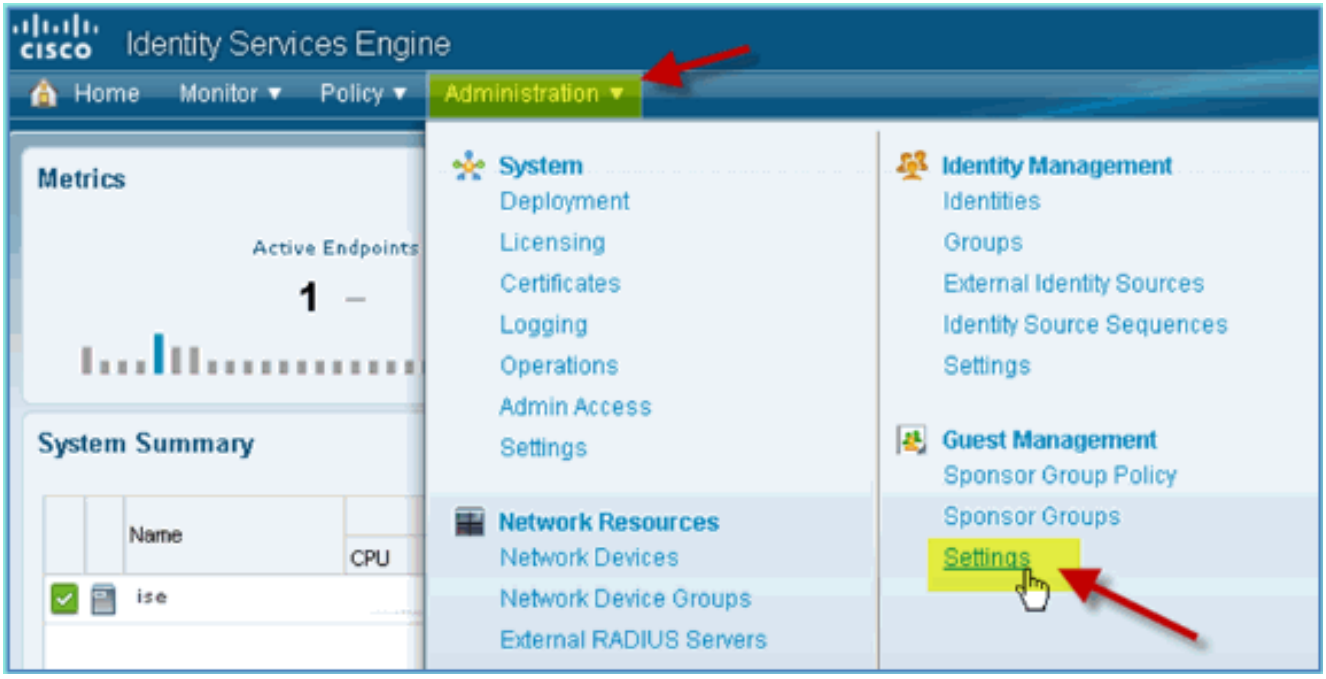


集成AD的ISE无线赞助访客接入

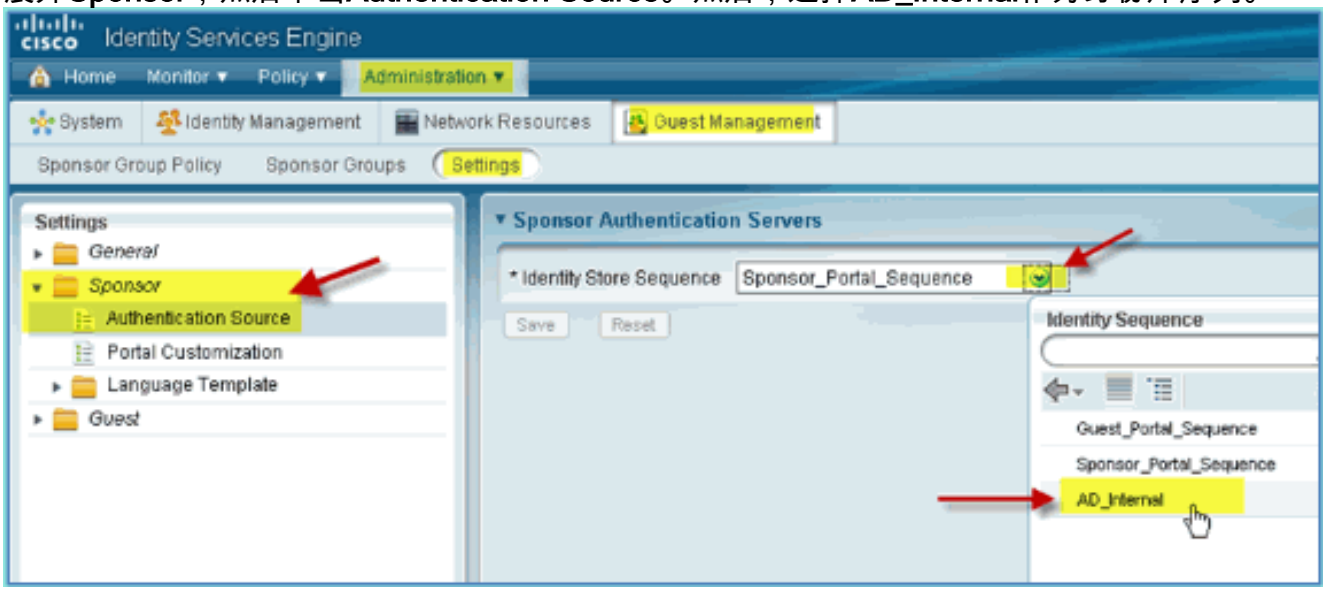
ISE可配置为允许使用策略发起访客，以允许AD域用户发起访客访问。

请完成以下步骤：

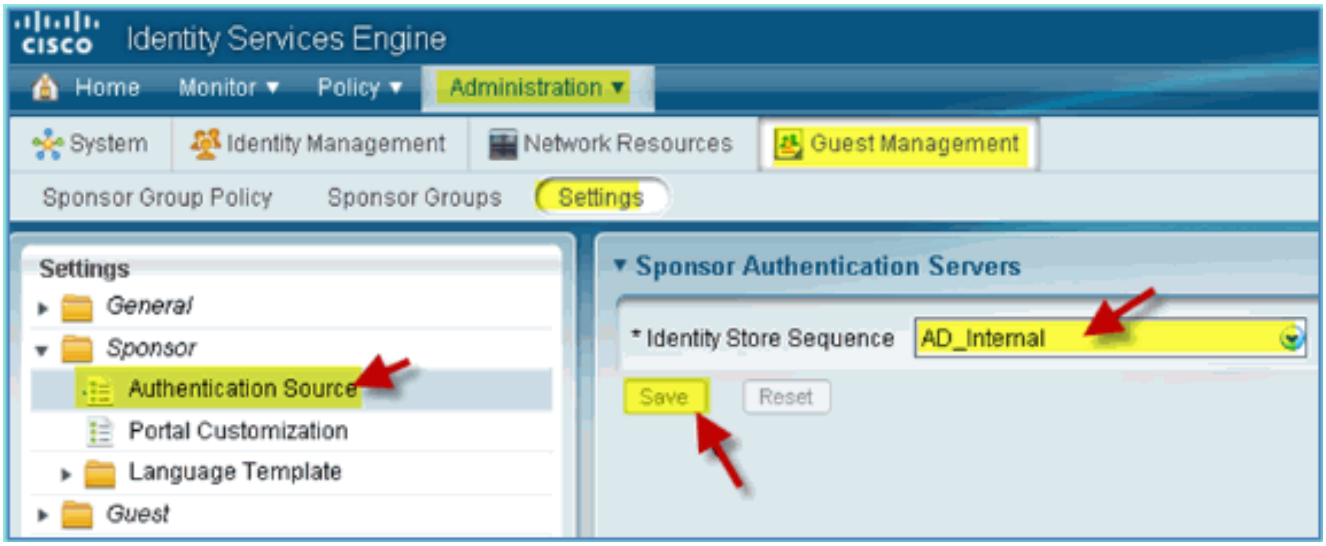
1. 从ISE导航到**管理>访客管理>设置**。



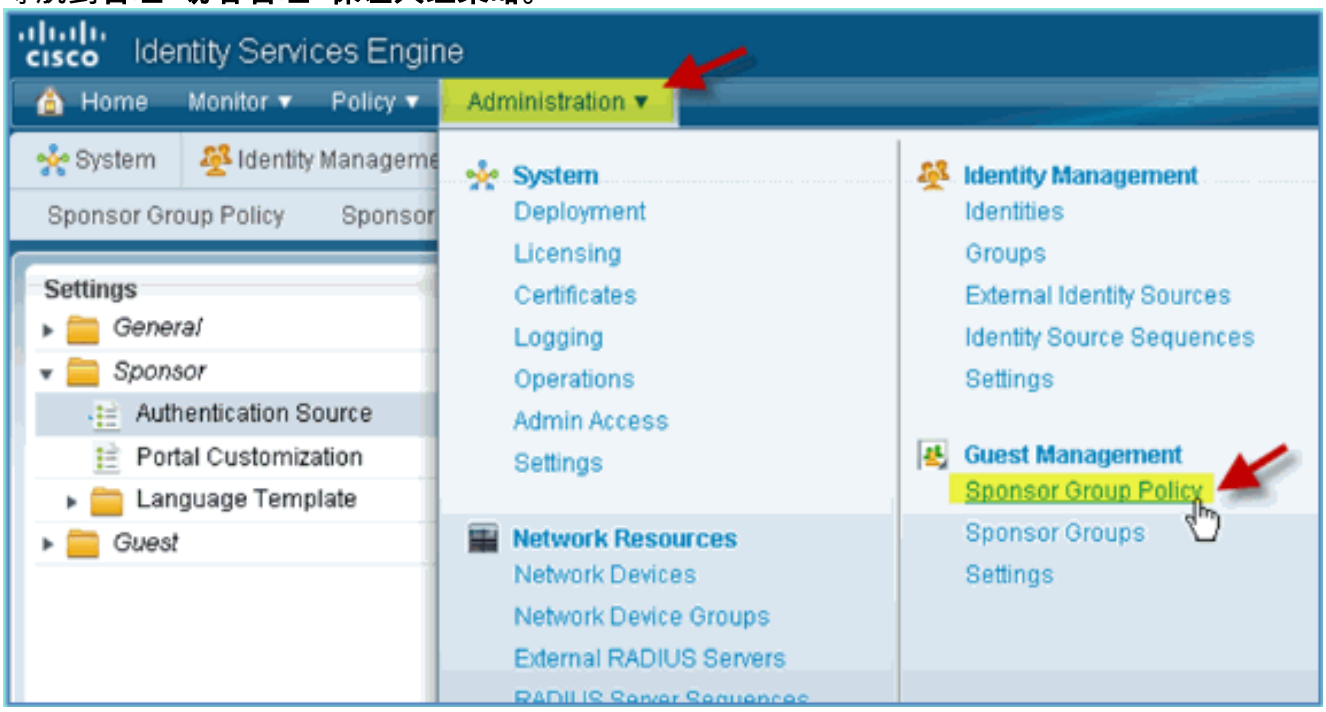
2. 展开**Sponsor**，然后单击**Authentication Source**。然后，选择**AD_Internal**作为身份库序列。



3. 确认AD_Internal作为身份库序列。Click **Save**.

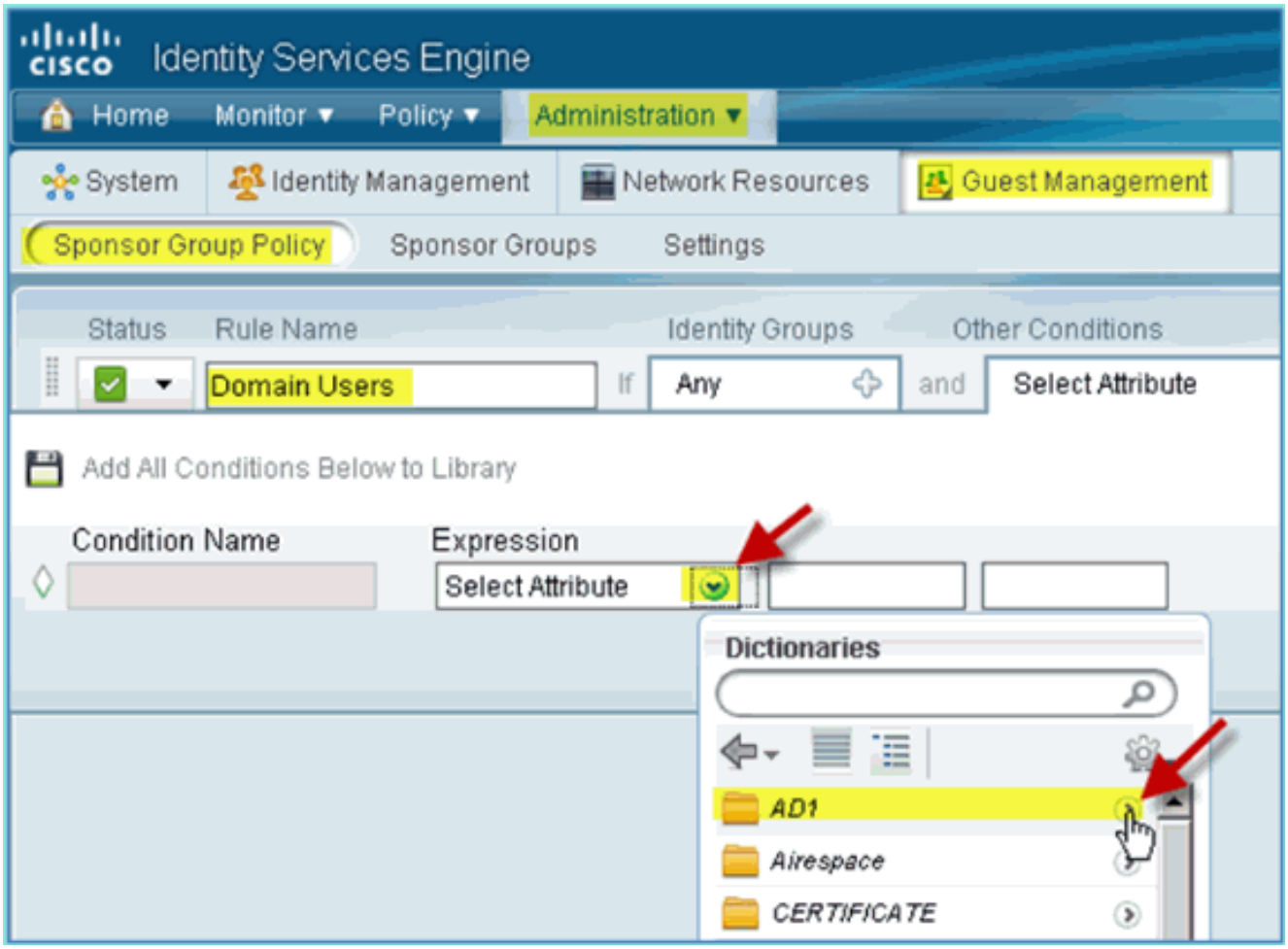


4. 导航到**管理>访客管理>保证人组策略**。

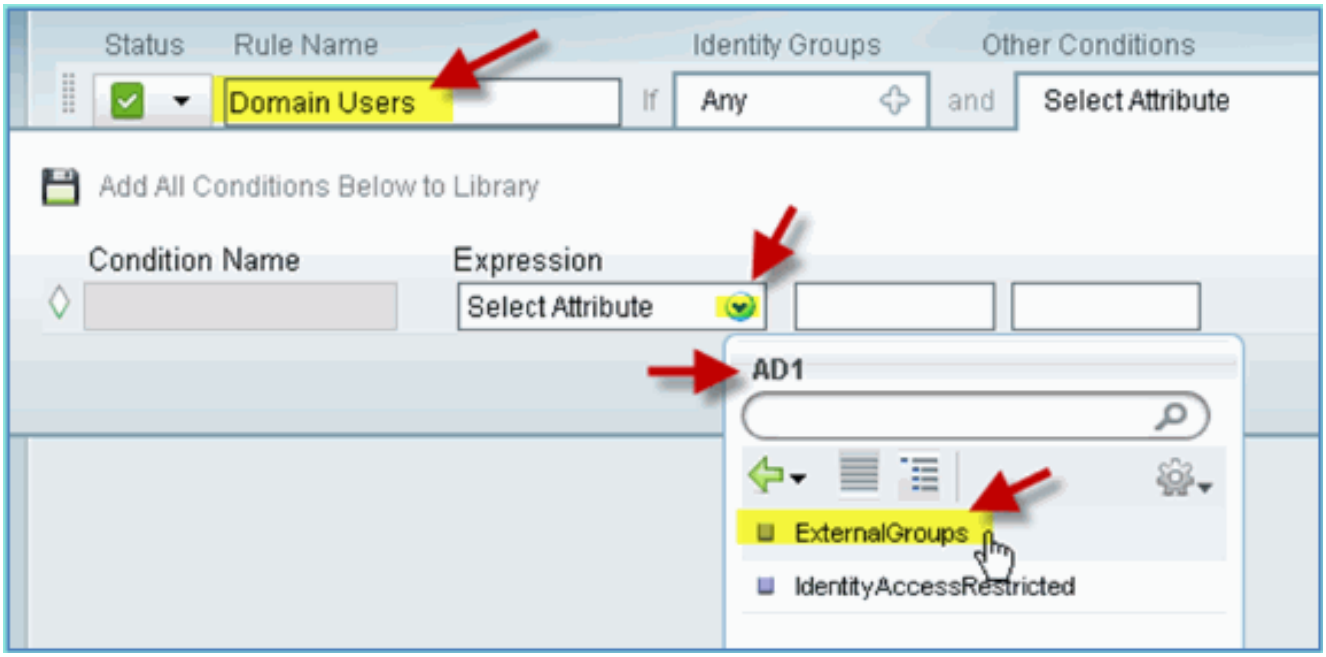


5. 在第一个规则上方插入新策略(点击右侧的**操作**图标)。

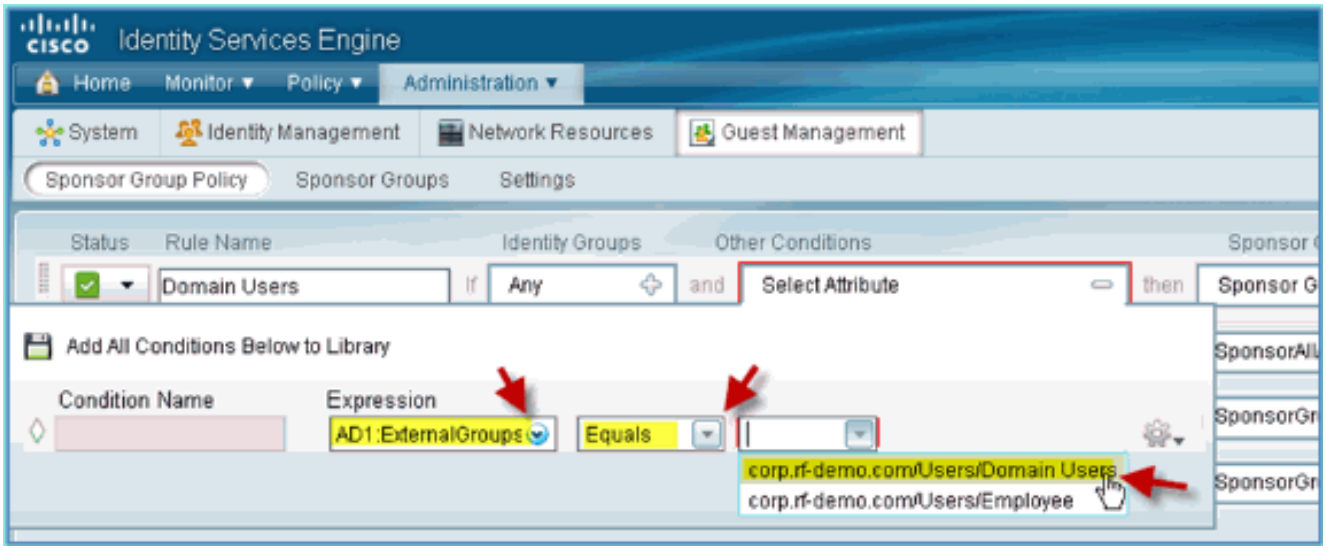
6. 对于新的发起人组策略，请创建以下内容：规则名称：域用户身份组：任意其他条件：（新建/高级）>
AD1



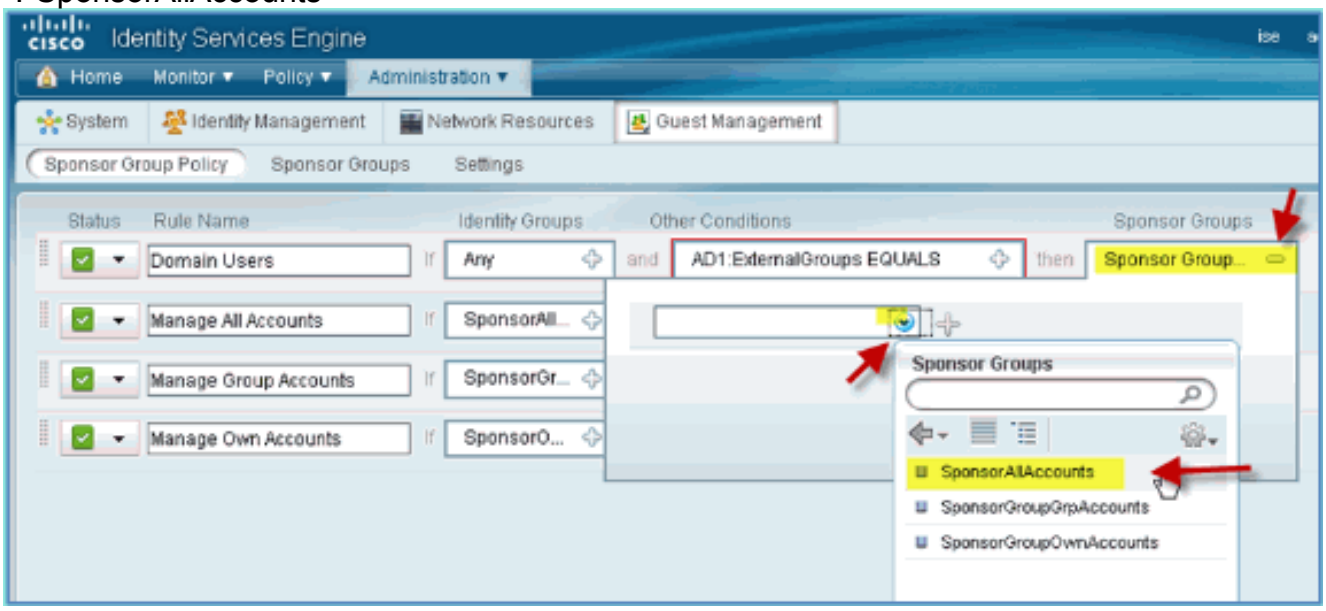
AD1：外部组



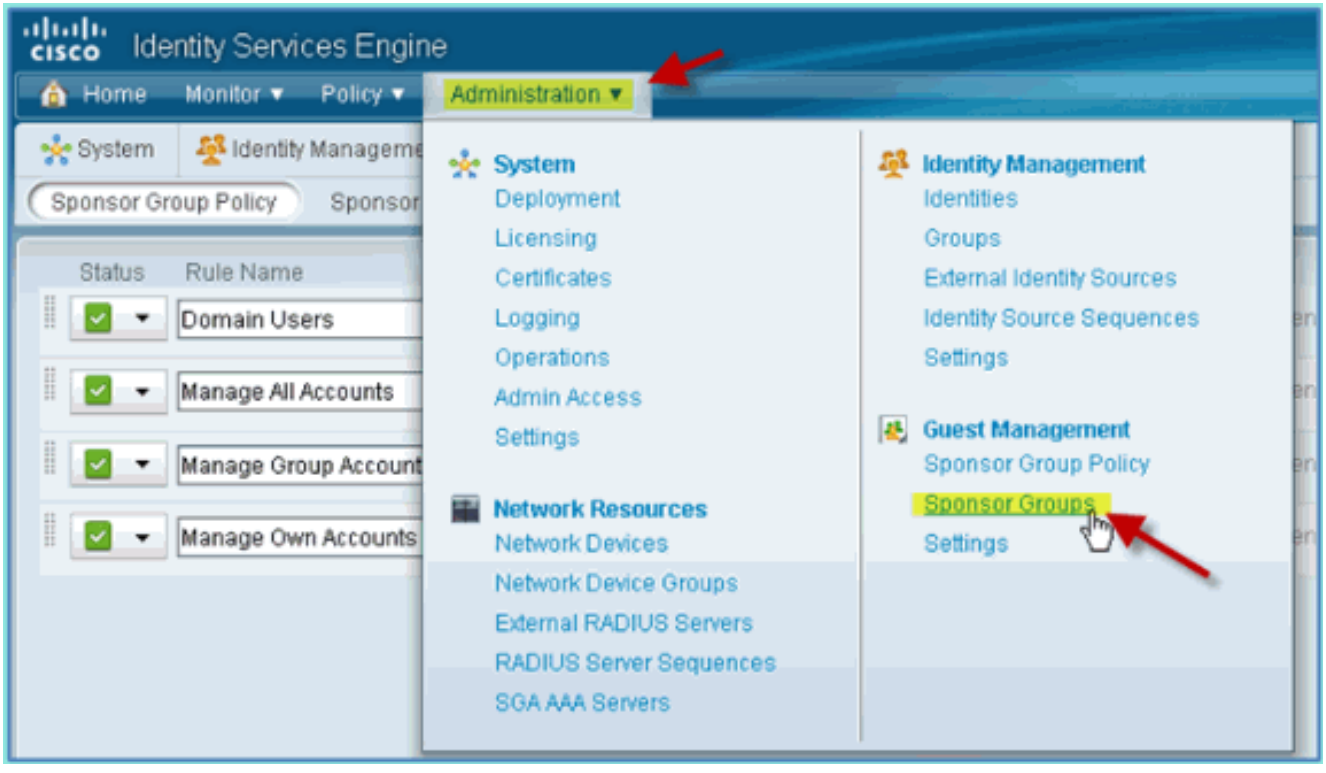
AD1外部组>等于> corp.rf-demo.com/Users/Domain用户



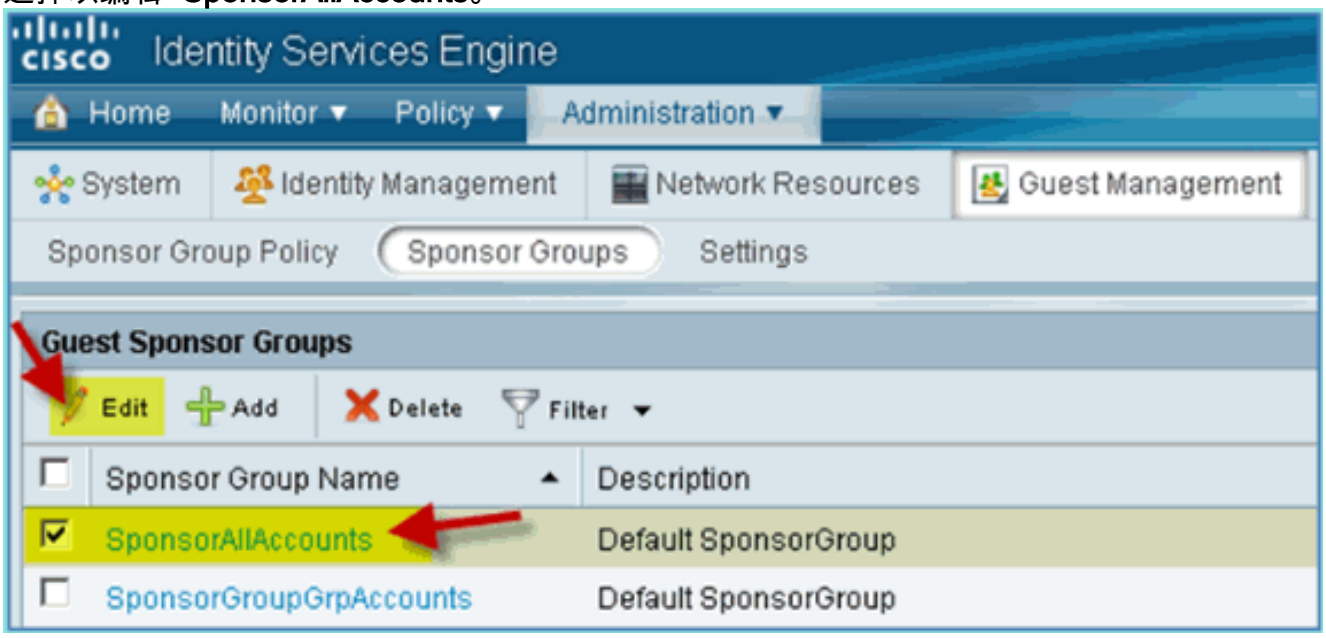
7. 在保证人组中，设置以下内容：保证人组
：SponsorAllAccounts



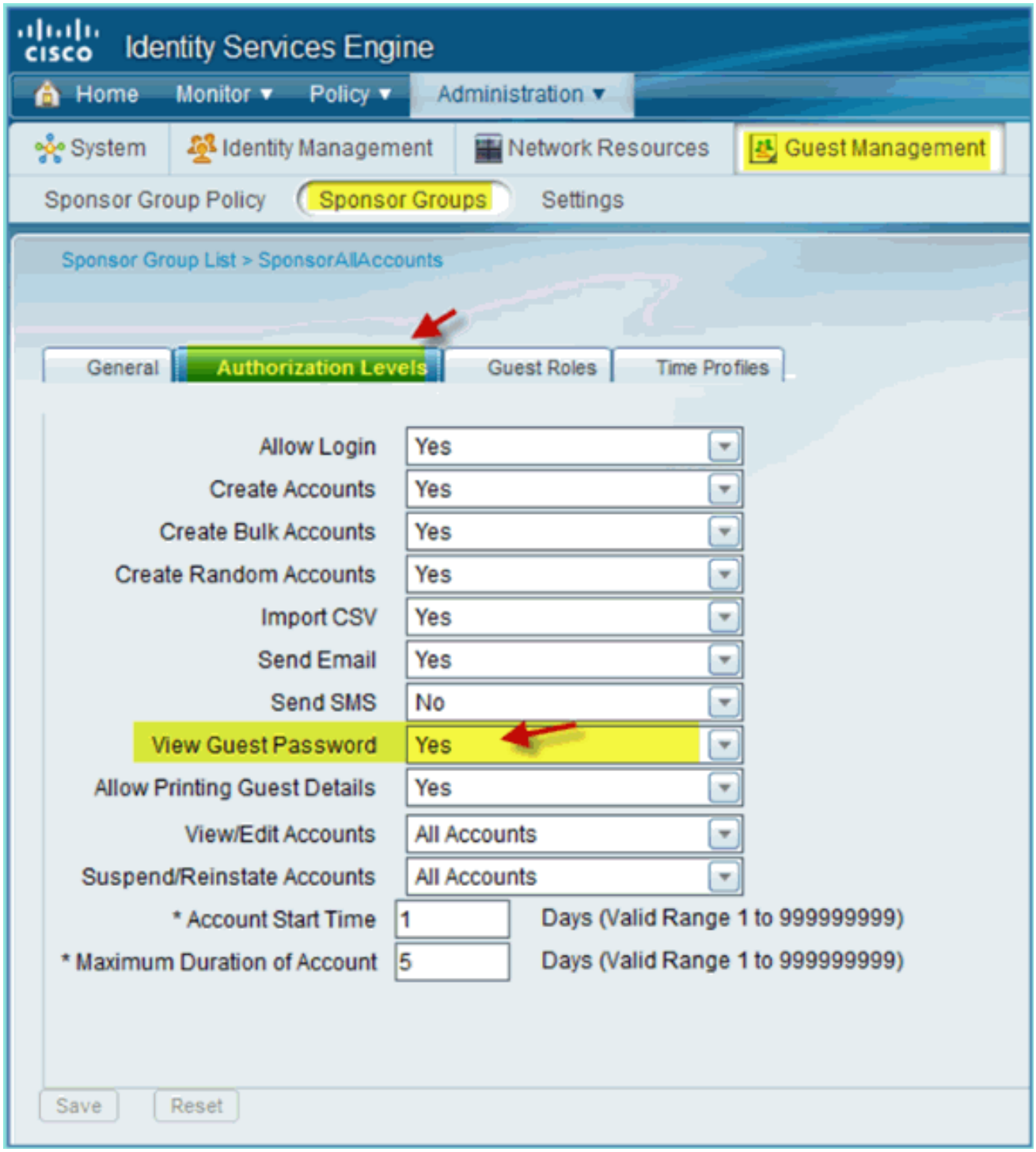
8. 导航到**管理>访客管理>保证人组。**



9. 选择以编辑>SponsorAllAccounts。



10. 选择Authorization Levels并设置以下内容：查看访客密码：是



在交换机上配置SPAN

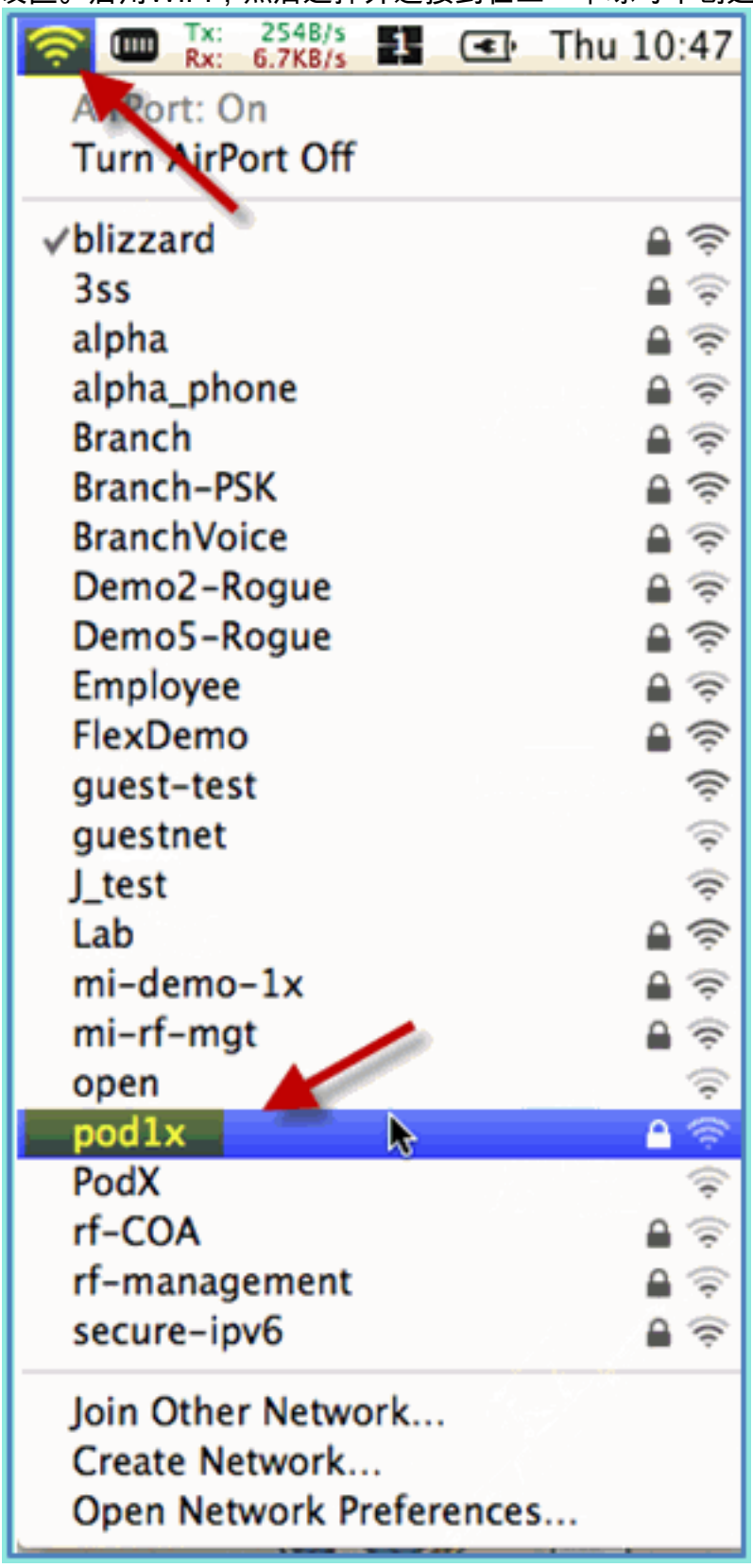
配置SPAN - ISE管理/探测接口与WLC管理接口相邻的第2层。交换机可配置为SPAN和其他接口，例如员工和访客接口VLAN。

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

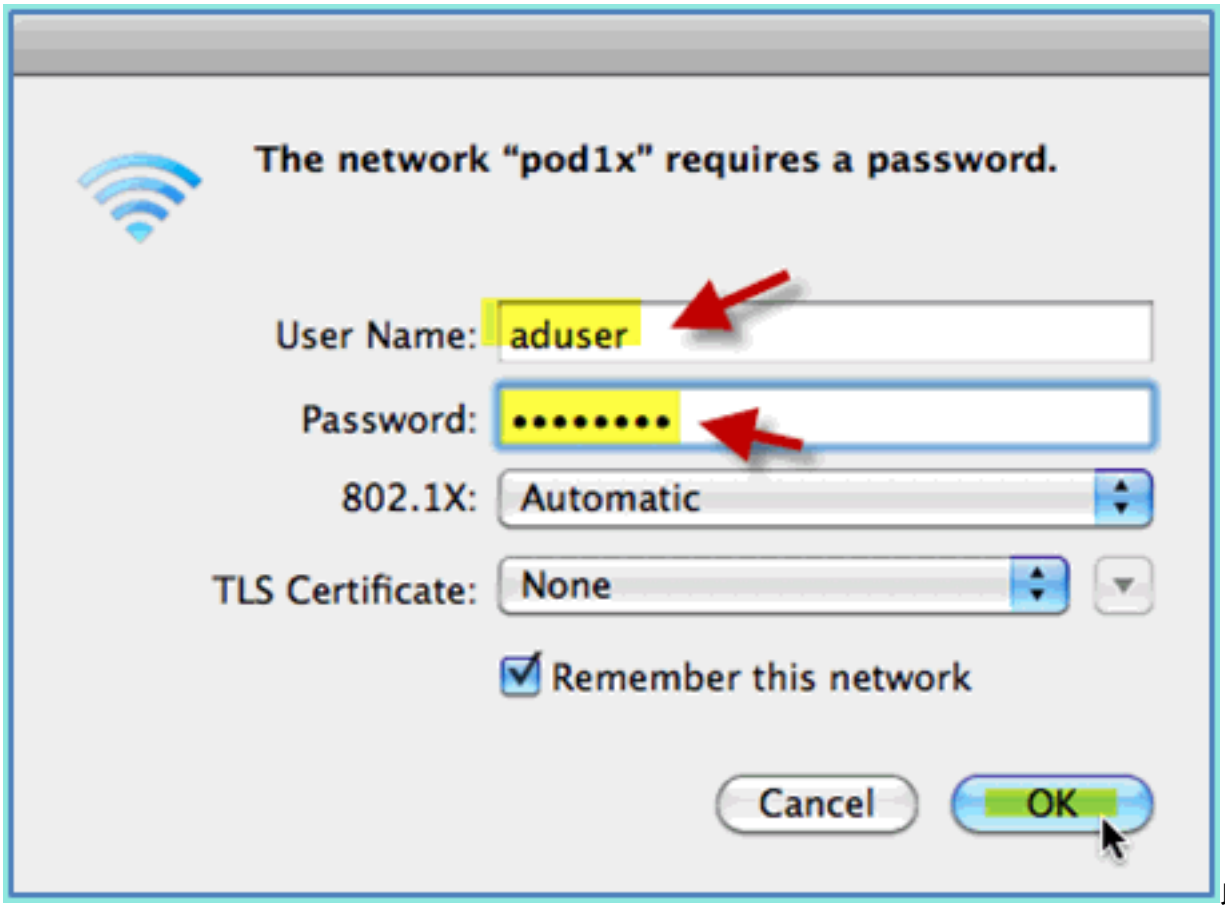
参考：Apple MAC OS X的无线身份验证

使用Apple Mac OS X无线笔记本电脑，通过经过身份验证的SSID作为内部用户（或集成的AD用户）关联到WLC。如果不适用，请跳过。

1. 在Mac上，转到WLAN设置。启用WIFI，然后选择并连接到在上一个练习中创建的启用802.1X的POD SSID。



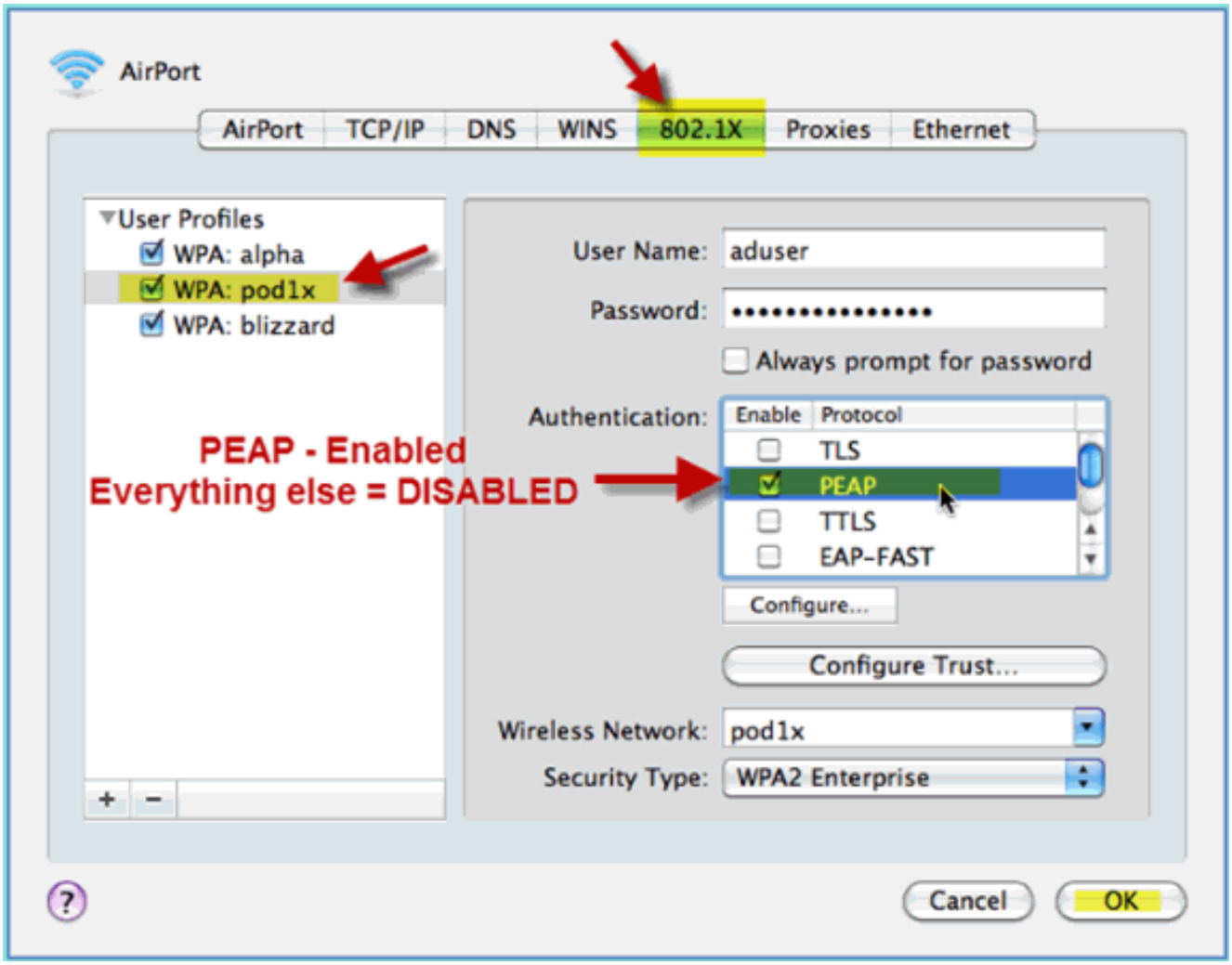
2. 提供以下连接信息：用户名：aduser（如果使用AD）、employee（内部 — 员工）、contractor（内部 — 承包商）密码：XXXX802.1X：自动TLS证书：无



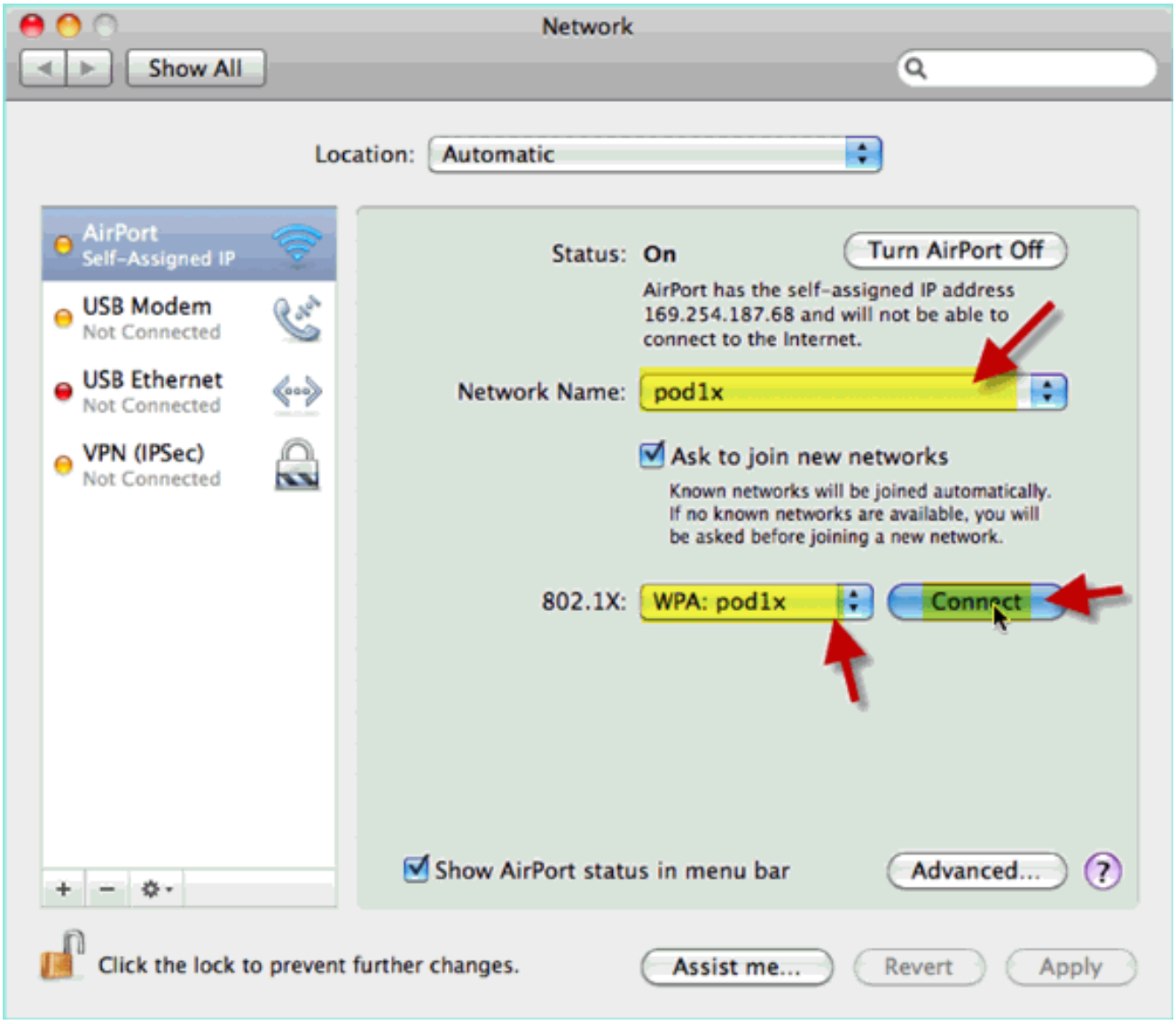
此时，笔记本电脑可能无法连接。此外，ISE可以引发失败事件，如下所示：

```
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of
an unknown CA in the client certificates chain
```

3. 转到**System Preference > Network > Airport > 802.1X**设置并将新的POD SSID/ WPA配置文件身份验证设置为：TLS：已禁用PEAP：已启用TTLS：已禁用EAP-FAST：已禁用

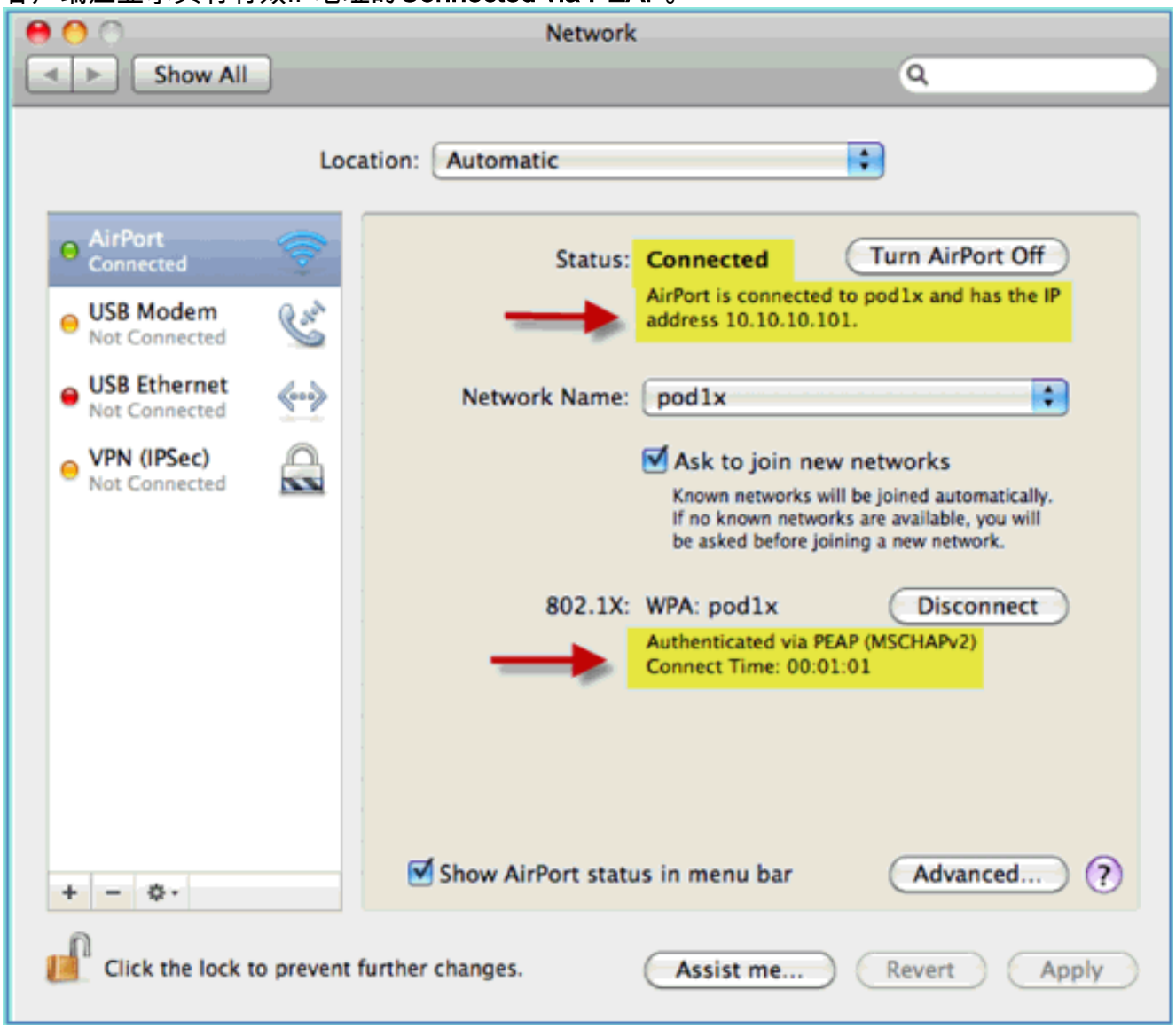


4. 单击**OK**继续并允许保存设置。
5. 在Network屏幕上，选择适当的SSID + 802.1X WPA配置文件，然后单击**Connect**。



6. 系统可能会提示输入用户名和密码。输入AD用户和密码(aduser/XXXX)，然后单击**OK**。

客户端应显示具有有效IP地址的Connected via PEAP。

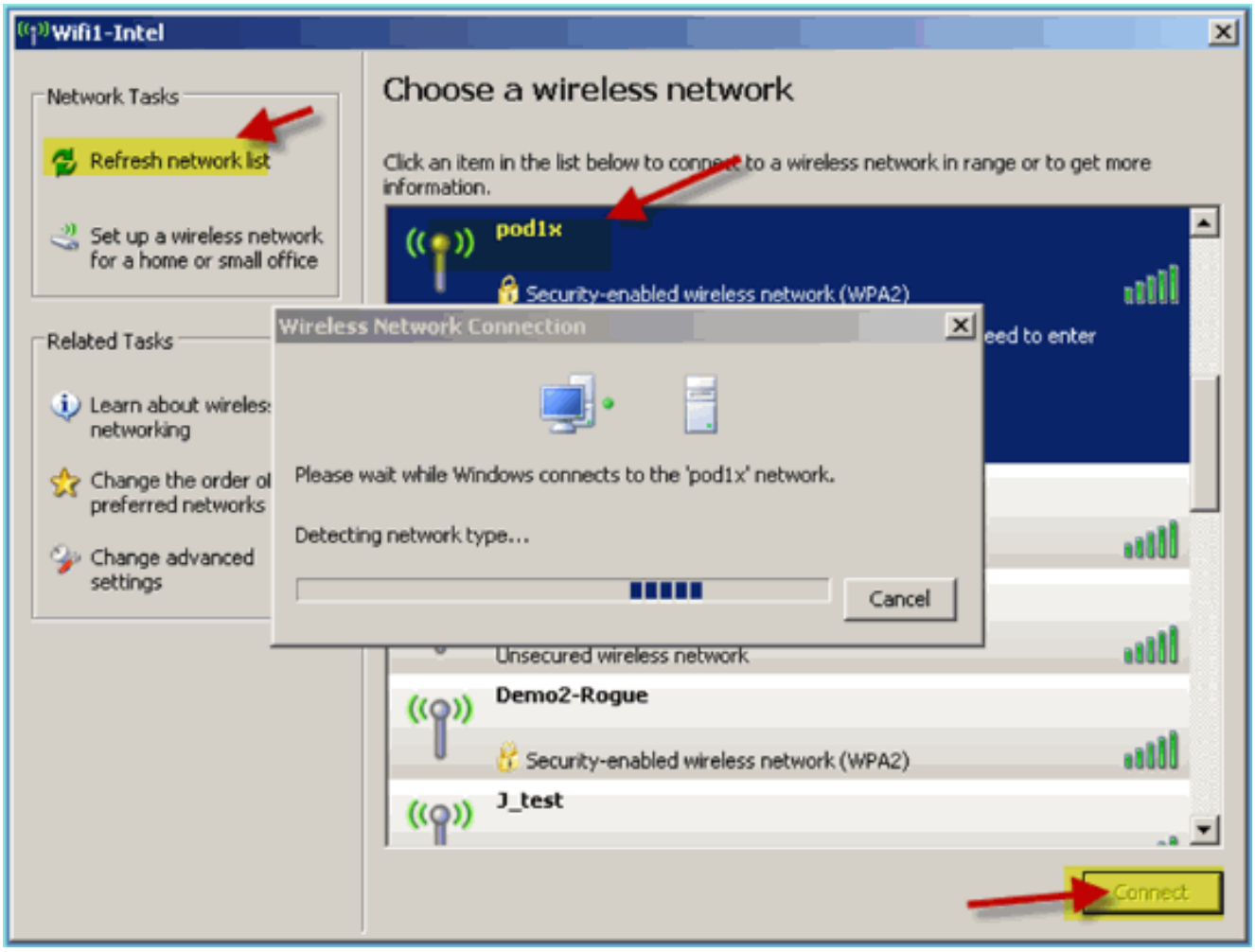


参考：Microsoft Windows XP的无线身份验证

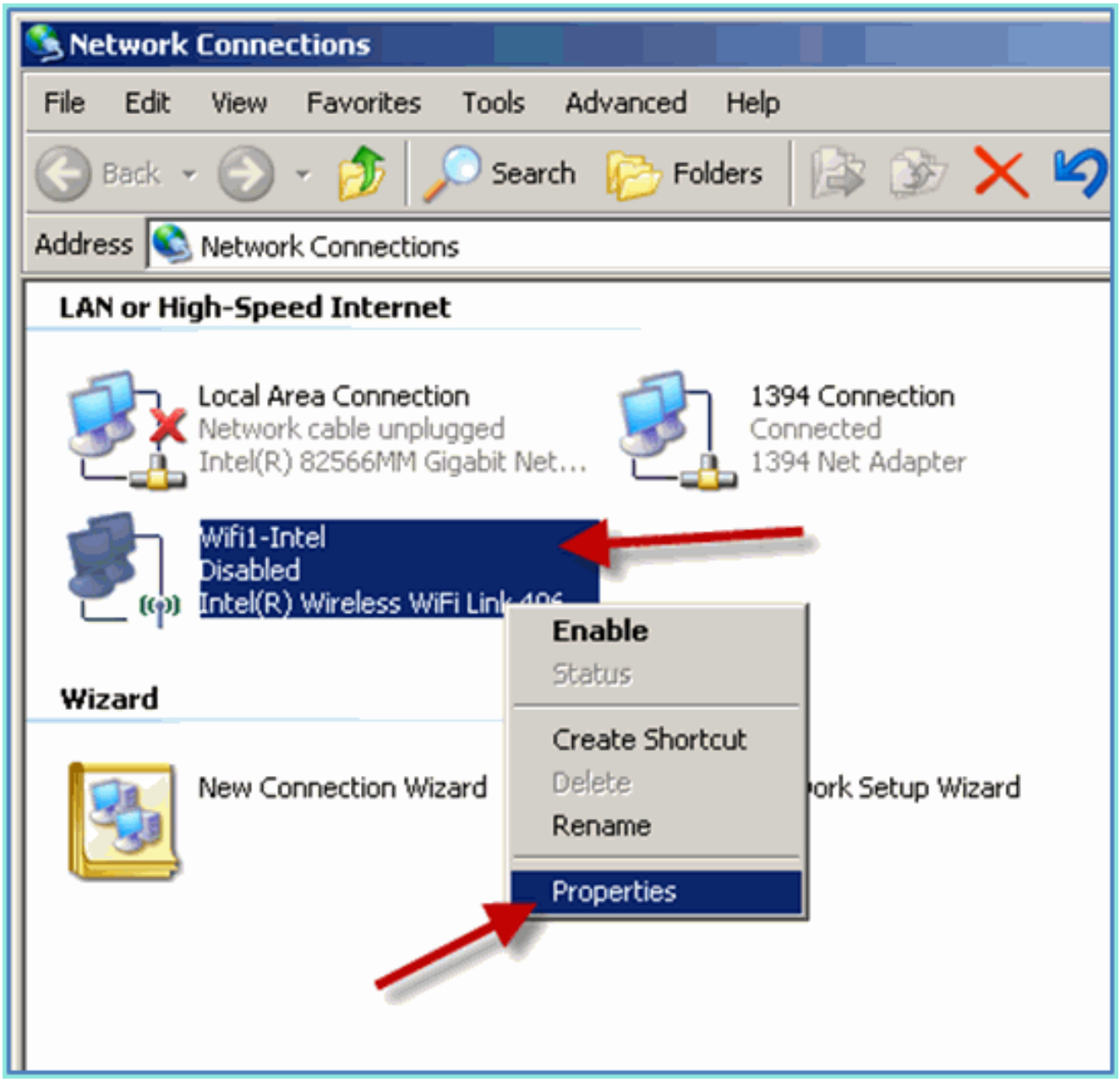
使用Windows XP无线笔记本电脑通过经过身份验证的SSID作为内部用户（或集成AD用户）关联到WLC。如果不适用，请跳过。

请完成以下步骤：

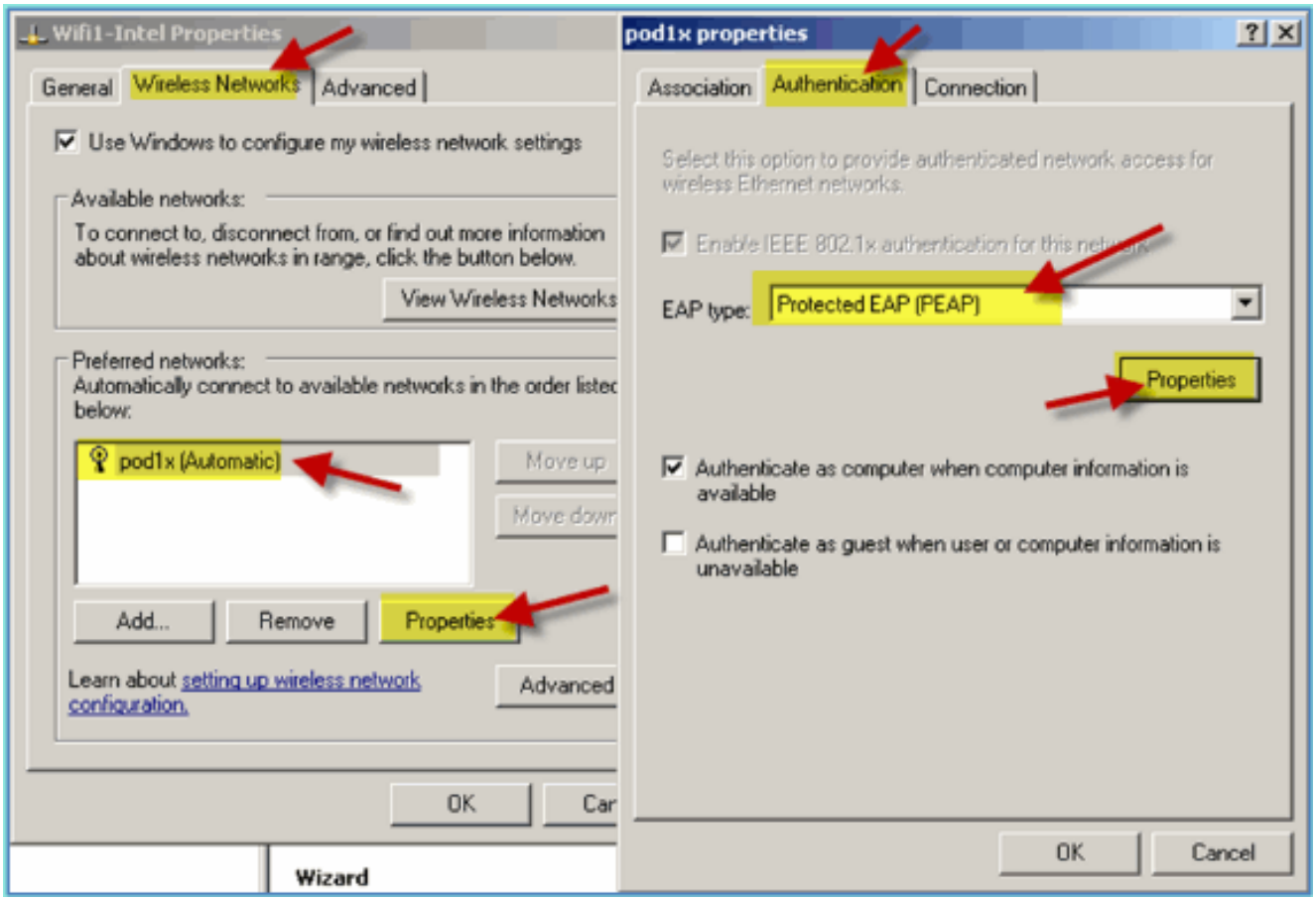
1. 在笔记本电脑上，转到WLAN设置。启用WIFI并连接到在上一个练习中创建的启用802.1X的POD SSID。



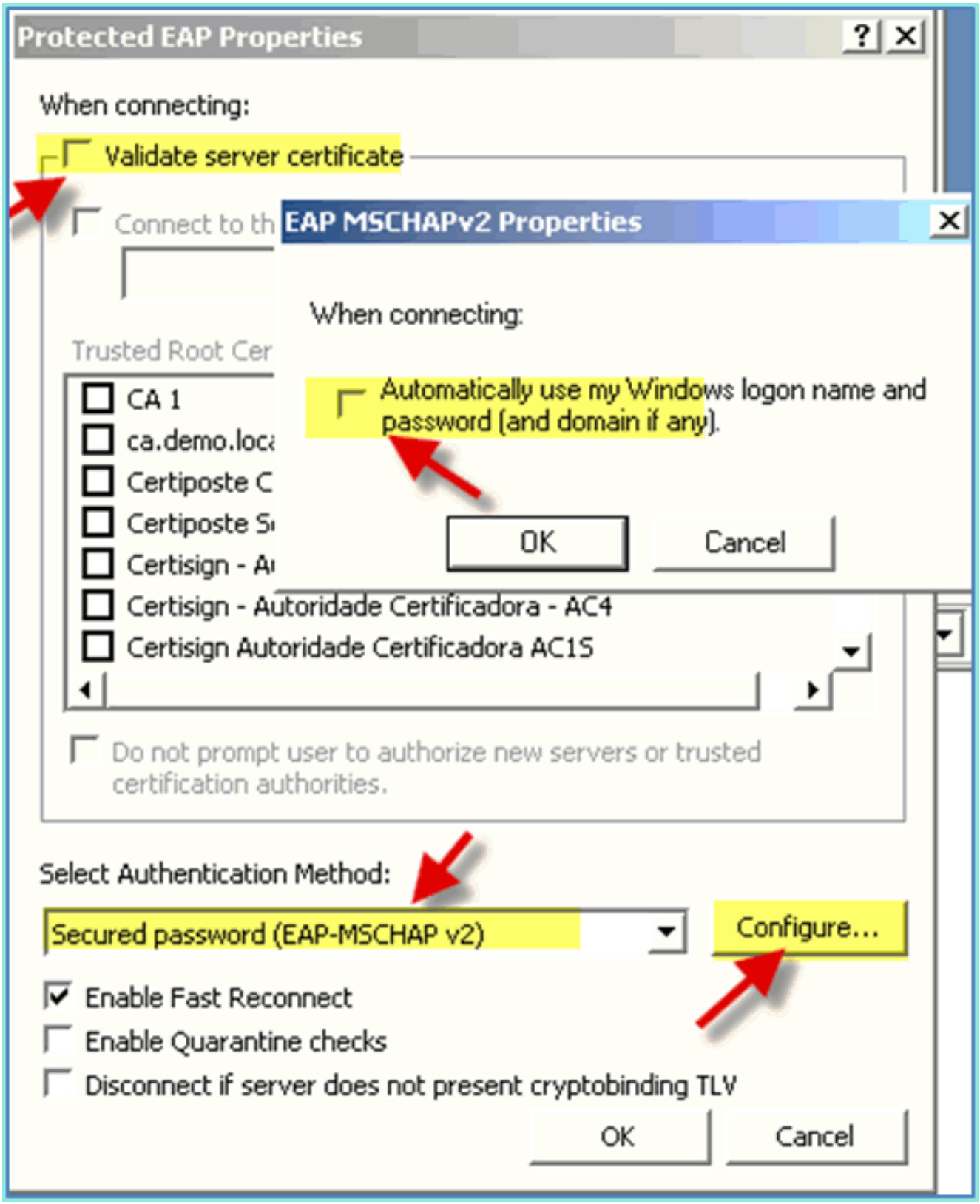
2. 访问WIFI接口的网络属性。



3. 导航到**无线网络**选项卡。选择Pod SSID网络属性>身份验证选项卡> EAP类型=受保护的EAP(PEAP)。



4. 点击EAP属性。
5. 设置以下项：验证服务器证书：已禁用身份验证方法：安全密码(EAP-MSCHAP v2)

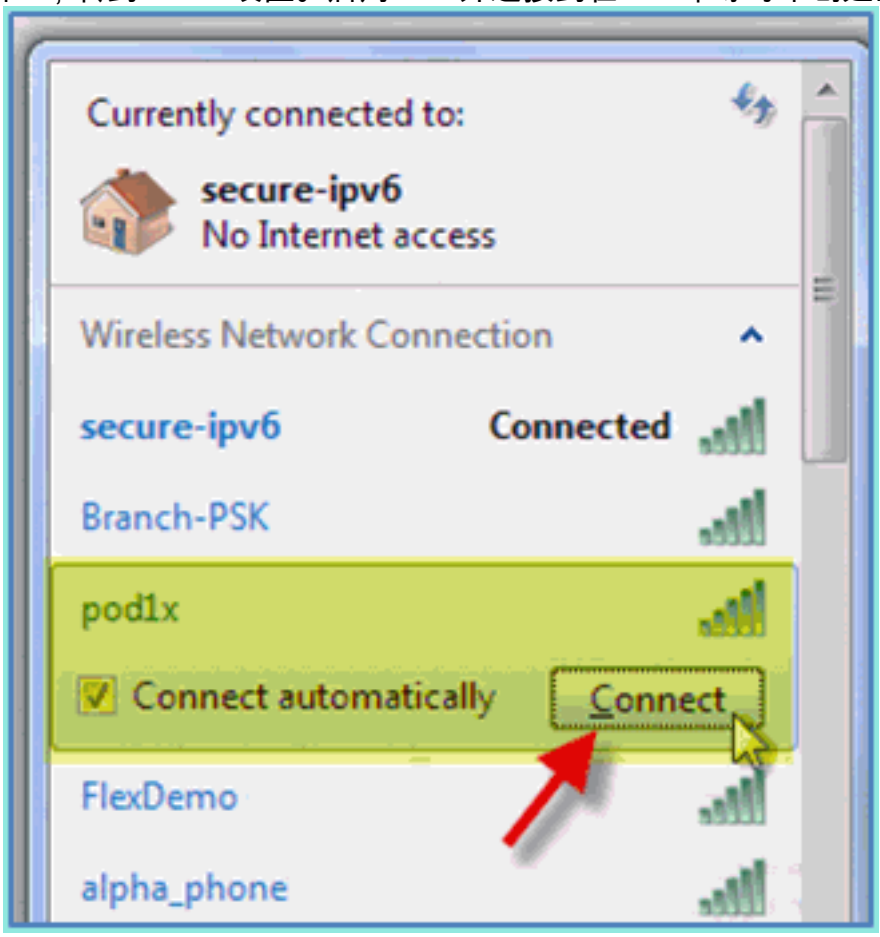


6. 在所有窗口中单击**OK**以完成此配置任务。
7. Windows XP客户端提示输入用户名和密码。在本例中，它是aduser/XXXX。
8. 确认网络连通性、IP编址(v4)。

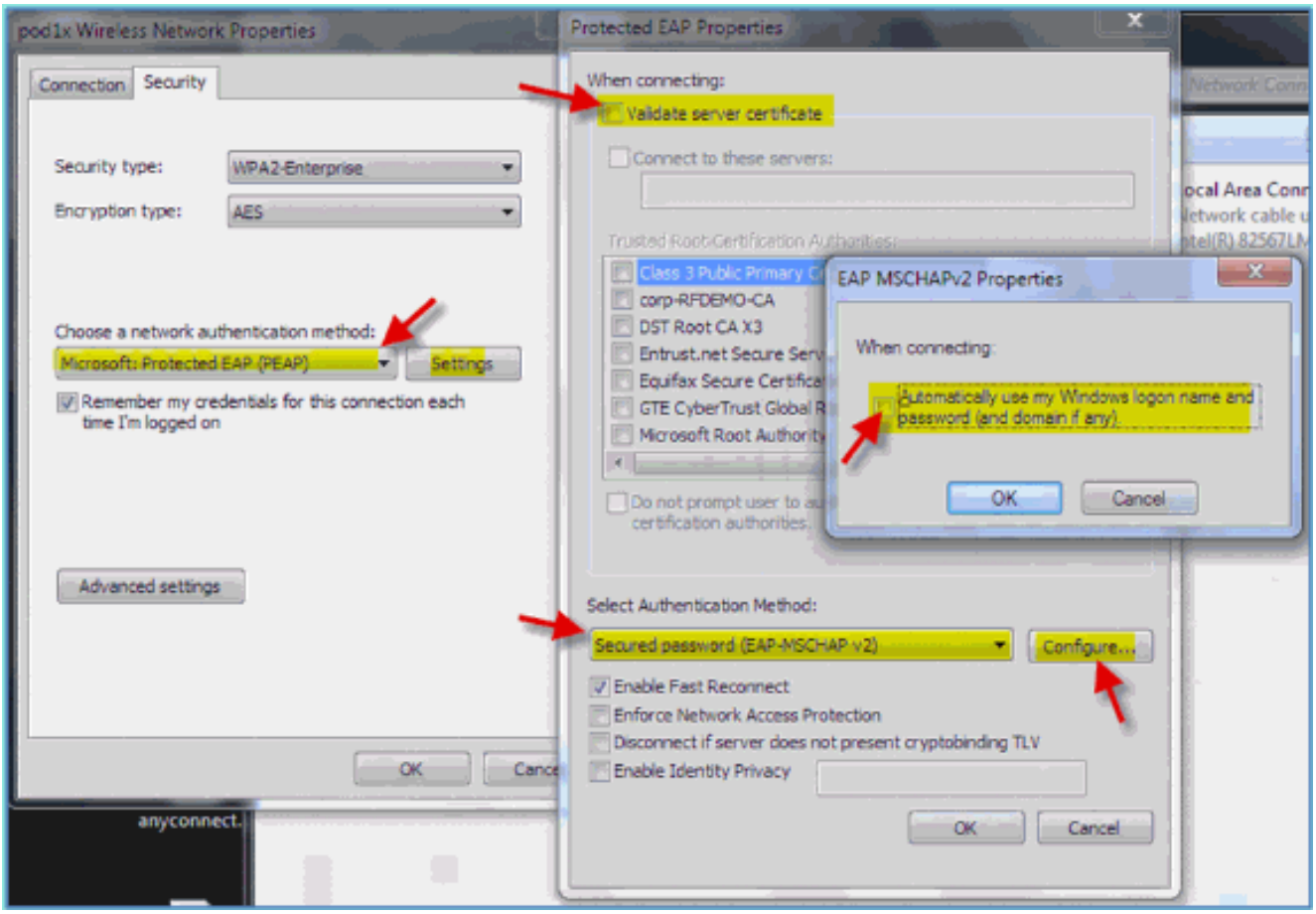
参考：Microsoft Windows 7的无线身份验证

使用Windows 7无线笔记本电脑通过经过身份验证的SSID作为内部用户（或集成AD用户）关联到WLC。

1. 在笔记本电脑上，转到WLAN设置。启用WIFI并连接到在上一个练习中创建的启用802.1X的 POD SSID。



2. 访问Wireless Manager并编辑新的POD无线配置文件。
3. 设置以下项：身份验证方法：PEAP记住我的凭据……：已禁用验证服务器证书（高级设置）：已禁用身份验证方法（高级设置）：EAP-MSCHAP v2自动使用我的Windows登录……：已禁用



相关信息

- 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）。