思科 BYOD+ISE 无线场景配置指南

目 录

1. 简介 2

2. 演示准备 2

- 需求说明 2
- 设备组件 2
- 网络拓扑 3

3. 在 ISE 上创建内部用户 3

4. 在 ISE 中添加 WLC 设备 5

5. 在 ISE 中配置无线认证 6

6. WLC 初始化配置 8

7. ISE 设备识别与授权配置 27

8. ISE 访客服务 47

9. BYOD 设备注册配置 57

1. 简介

思科 Identity Service Engine（ISE）是思科的下一代的身份服务引擎，为思科的TrustSec 解决方案提供了认证和授权的基础架构。此外 ISE 还提供了两个重要的服务：

- ISE 从多种方式获得的设备属性信息，提供了自动识别终端设备类型的一种方法。这种服务被称为设备识别 Profiler，与以前在 NAC Profiler 设备提供的功能是相同的。
- ISE 支持检查重点设备是否符合安全标准；例如，AV/AS 软件是否安装以及其特征库文件的有效期（也称为终端状态 Posture）。以是在 NAC 设备上提供了终端健康状态检查的功能。

思科 ISE 并且集成了 802.1X 认证，结合无线控制器（WLC）还实现了移动终端设备哦的识别功能，如 Apple 的设备（iPhone, iPad 和 iPod），Android 系统的智能手机等。对于 802.1X 用户而言，ISE 能够提供诸如设备识别 profiling 和终端状态检查 posture，访客服务 guest service。ISE 与无线控制器集成后，能够将 web authentication 的认证请求重定向到 ISE 上进行认证。

本文档介绍了对于 BYOD 的无线解决方案，如根据终端设备的类型和用户类型，提供不同的访问权限。本文档并没有提供 BYOD 的完整的解决方案，但是演示了一个简单用户场景的动态访问。此外还提供了一个配置举例，即通过 ISE 的 Sponsor Portal 页面，经过授权的 Sponsor 如何为一位访客如何无线访问的服务。

原文链接：Wireless BYOD with Identity Services Engine

2. 演示准备

• 需求说明

本文档的内容是针对一般性的用户需求，假定了一个 BYOD 在无线网络的访问场景，通过 ISE 实现认证和授权的配置过程。

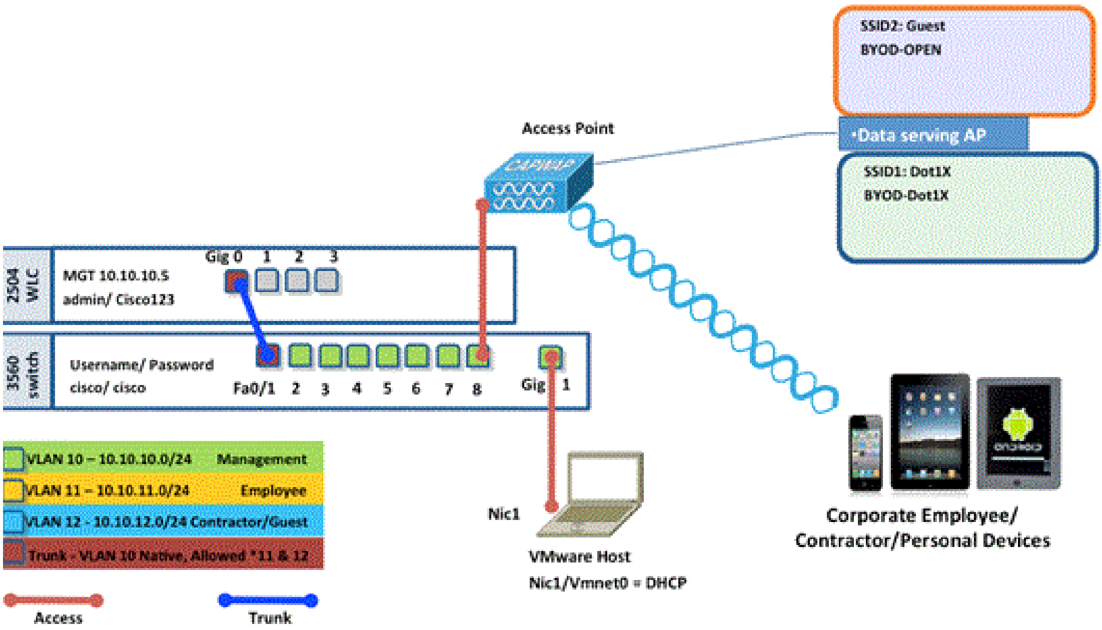
• 设备组件

以下是本文档用到的设备组件的硬件和软件信息：

- 思科无线控制器 2504 或 2106，软件版本 7.2.103
- 交换机 Catalyst3560-8 口
- ISE 1.0 MR(VMware server image version)
- Windows 2008 服务器(VMware 版) – 内存 512M，磁盘 20GB
  - Active Directory
  - DNS
  - DHCP
  - CA 证书服务器

- ## 网络拓扑

下图为整个演示用到的网络拓扑图，和 IP 地址分配信息：



设备 IP 地址配置信息：

设备名称	IP 地址	登录信息
VMware Host	10.10.10.2	安装 ISE 的虚拟机服务器
Wireless LAN Controller	10.10.10.5	无线控制器
Identity Service Engine	10.10.10.70	admin/default1A
AD/DNS/DHCP/CA Server	10.10.10.10	安装 AD/DNS/DHCP/CA 的 2008 服务器

3. 在 ISE 上创建内部用户

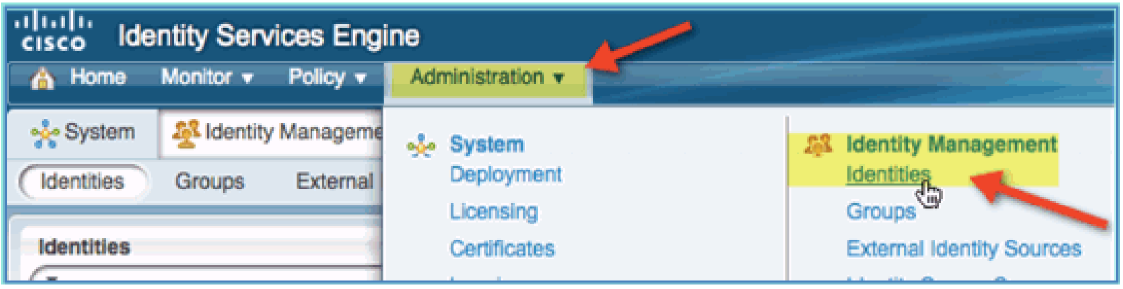
在简单的 PoC 测试中，Active Directory 不是必需的。ISE 可以单独用做身份验证数据库，用于对用户的访问控制和授权的策略控制。

在 ISE1.0 版本中，ISE 可以使用 AD 的组别的属性进行授权。如果使用内部用户（未集成 AD）进行授权，用户组别信息不能和设备组别信息同时使用（这个在 ISE1.1 中已经解决），因此仅可使用单个用户，比如 employees 或 contractors 可以和设备组别信息进行组合授权。

配置步骤如下：

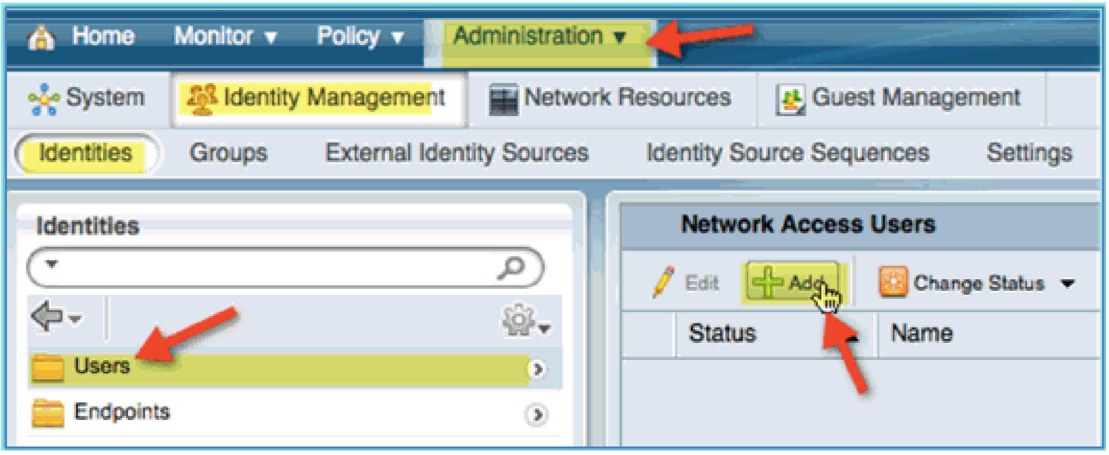
1). 通过浏览器访问 https://<ISE 的 IP 地址>。

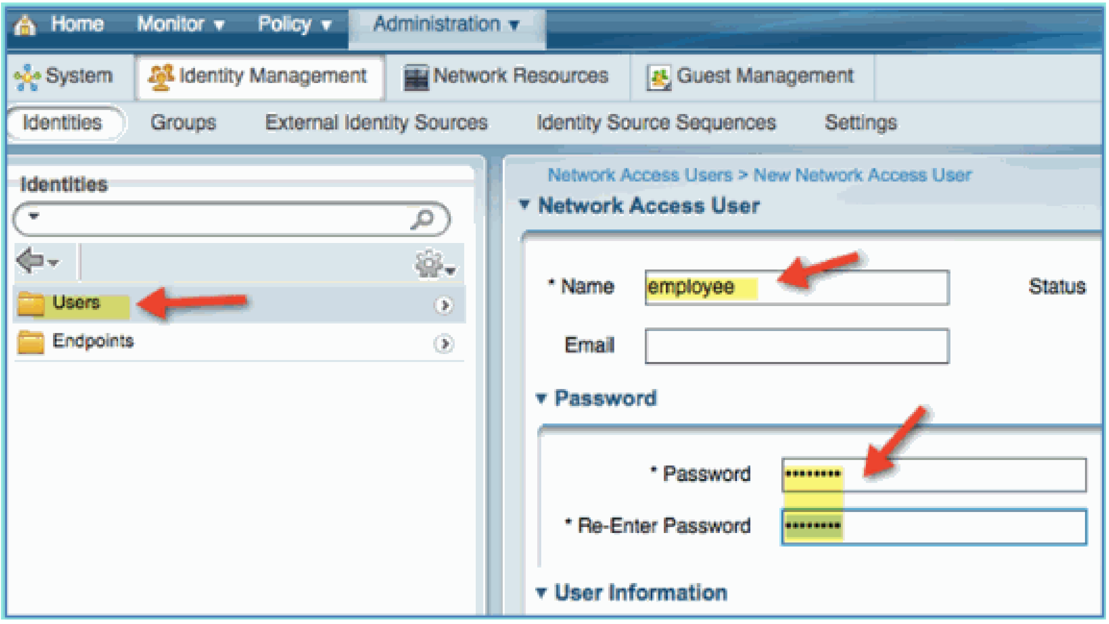
2). 进入 Administration > Identity Management > Identities



3). 选择 Users，再点击 Add（Network Access Users)。输入以下用户信息：

- Name: employee
- Password: XXXX





* Name: employee

Email:

* Password: ••••••••

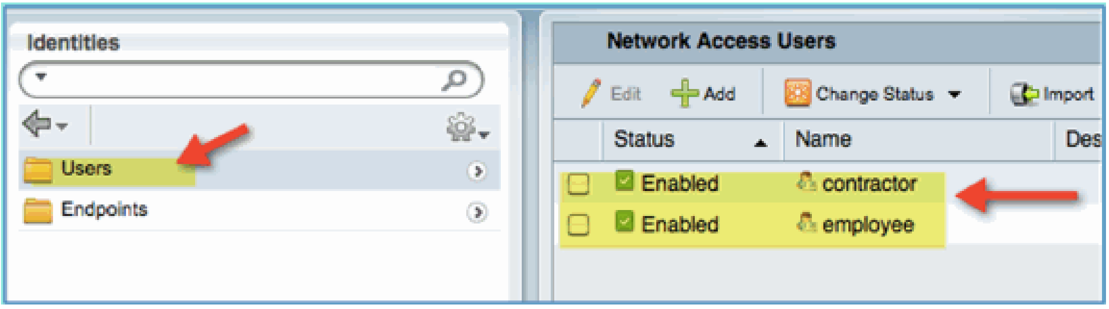
* Re-Enter Password: ••••••••

4) 点击 Submit。再点击 Add，添加另一个用户：

Name: contractor

Password: XXXX

5) 确认两个用户都已经创建。



Status	Name	Des
☑ Enabled	contractor	
☑ Enabled	employee	

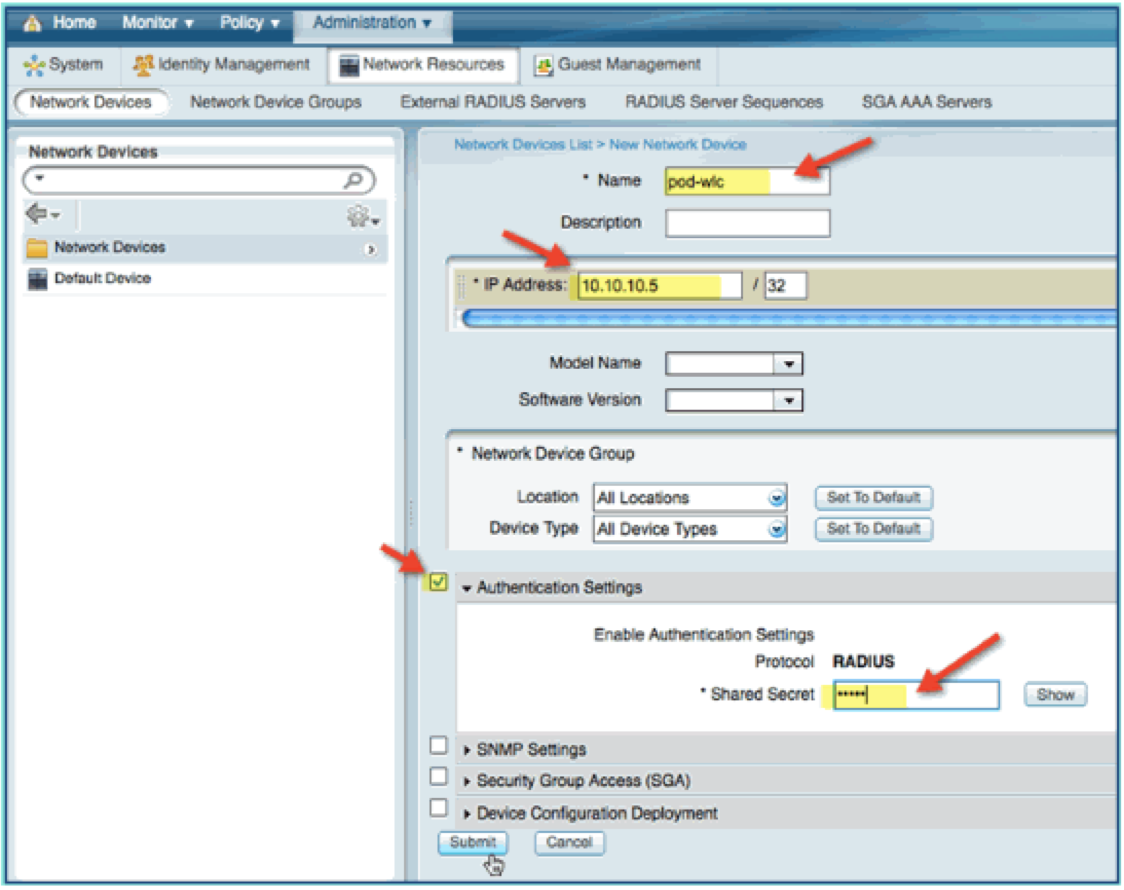
4. 在 ISE 中添加 WLC 设备

任何向 ISE 发起 RADIUS 请求的网络设备，必须事先添加到 ISE 中。这些定义到 ISE 上的设备都以 IP 地址进行区分。在 ISE 上添加网络设备，支持用 IP 地址范围表示多台实际设备。

除了必须的用于 RADIUS 通信需要以外，ISE 添加设备时还包含了 SNMP 和 SSH 等信息。另外，网络设备的定义还要进行适当的分组，这样就可以利用设备的分组信息来设置网络访问策略。

定义网络设备的步骤如下：

1) 进入 Administration > Network Resources > Network Devices.
2) 点击 Add，输入 IP 地址等信息，输入 cisco 作为共享密钥。



* Name: pod-wlc

Description:

* IP Address: 10.10.10.5 / 32

Model Name:

Software Version:

* Network Device Group

Location: All Locations

Device Type: All Device Types

☑ Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

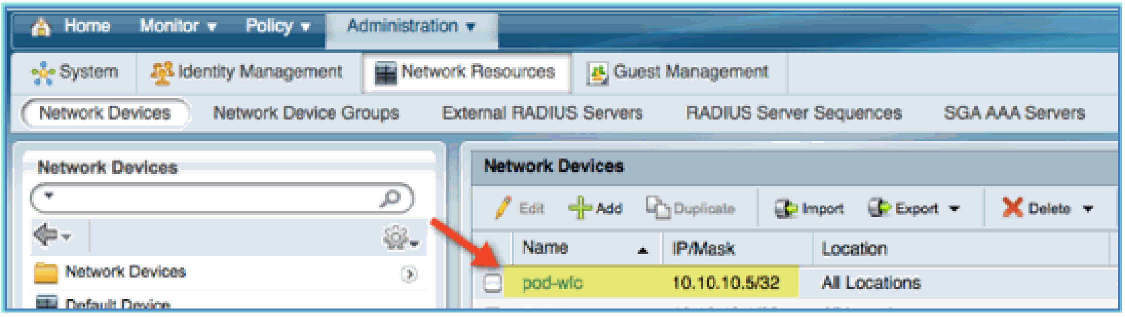
* Shared Secret: *****

□ SNMP Settings

□ Security Group Access (SGA)

□ Device Configuration Deployment

3) 保存 WLC 的添加，确认 WLC 已经在设备列表中。



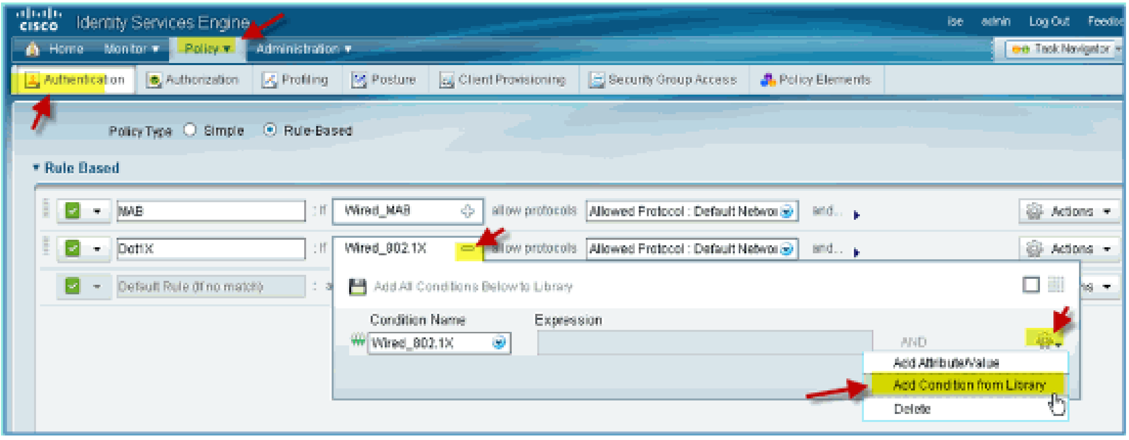
5. 在 ISE 中配置无线认证

ISE 需要配置 802.1X 无线客户端认证，并使用 AD 作为身份认证请求。配置步骤如下：

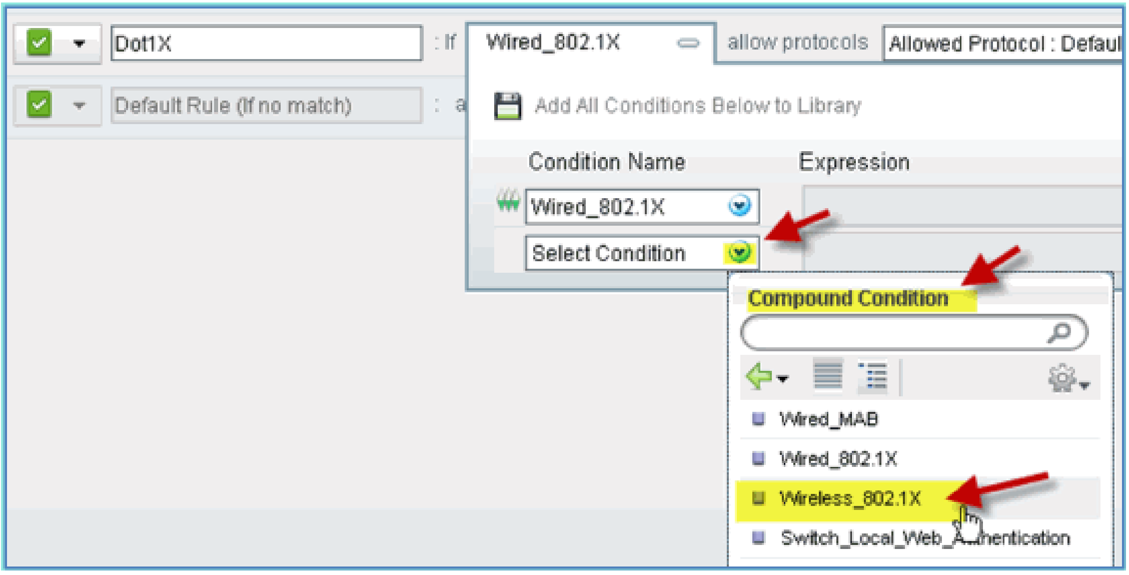
1) 进入 Policy > Authentication.

2) 在 Dot1X 所在的条目，点击 Wired_802.1X 后面的+号.

3) 点击齿轮标记，并选择 Add Condition from Library.



4) 从条件选择下拉式列表中，选择 Compound Condition > Wireless_802.1X



Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Defaul

Default Rule (If no match) : a

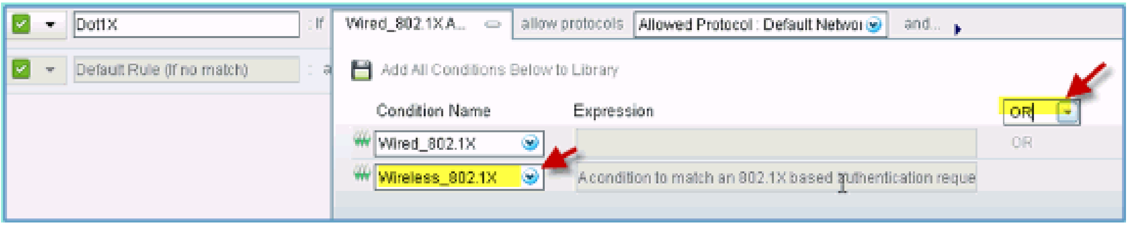
Add All Conditions Below to Library

Condition Name	Expression
Wired_802.1X	
Select Condition	

Compound Condition

- Wired_MAB
- Wired_802.1X
- Wireless_802.1X
- Switch_Local_Web_Authentication

5) 设置表达式条件为 OR



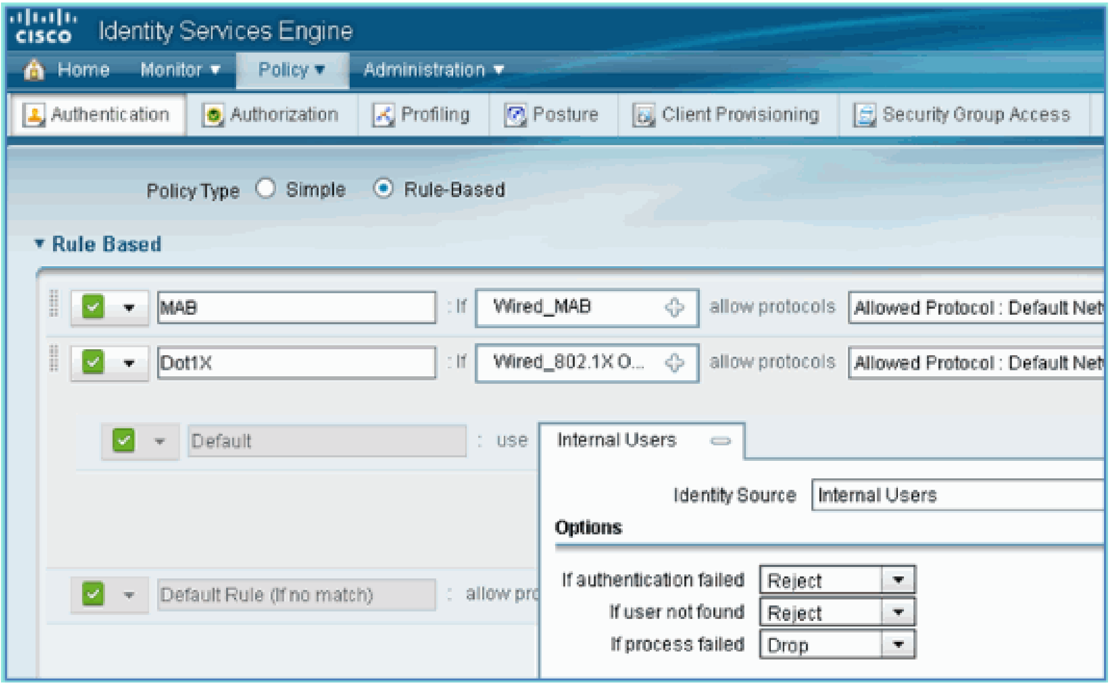
Dot1X : If Wired_802.1X A... allow protocols Allowed Protocol : Default Networ and ...

Default Rule (If no match) : a

Add All Conditions Below to Library

Condition Name	Expression	OR
Wired_802.1X		OR
Wireless_802.1X	A condition to match an 802.1X based authentication reque	

6) 展开“allow protocols”的箭头的选项，并接受缺省的身份认证 Internal Users



Policy Type ○ Simple ● Rule-Based

Rule Based

MAB : If Wired_MAB allow protocols Allowed Protocol : Default Net

Dot1X : If Wired_802.1X O... allow protocols Allowed Protocol : Default Net

Default : use Internal Users

Identity Source: Internal Users

Options

If authentication failed: Reject

If user not found: Reject

If process failed: Drop

Default Rule (If no match) : allow pro

7) 其他内容保持为默认值，点击 Save 保存设置。

6. WLC 初始化配置

思科 2500 系列无线控制器部署指南，请参考 2500 系列部署指南。

- WLC 初始配置向导

```
(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.
```

- 连接 WLC 的交换机端口配置

无线控制连接到交换机的端口 FastEthernet 0/1 上，该端口要配置为 802.1Q Trunk 链路，并允许所有的 VLAN 通过。接口的本地 VLAN 10，允许 WLC 的管理接口连上来。

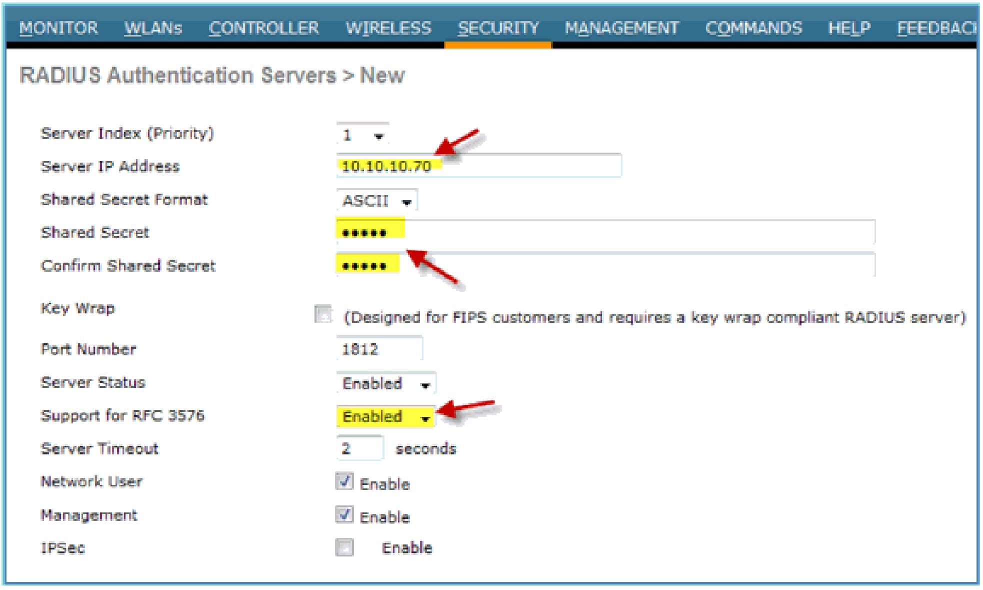
```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport trunk allowed vlan 11,12
switchport mode trunk
end
```

- 在 WLC 上增加认证服务器的配置

通过在 WLC 上添加 ISE，并启用无线终端设备的 802.1X 认证和授权变更(CoA)功能。

配置步骤如下：

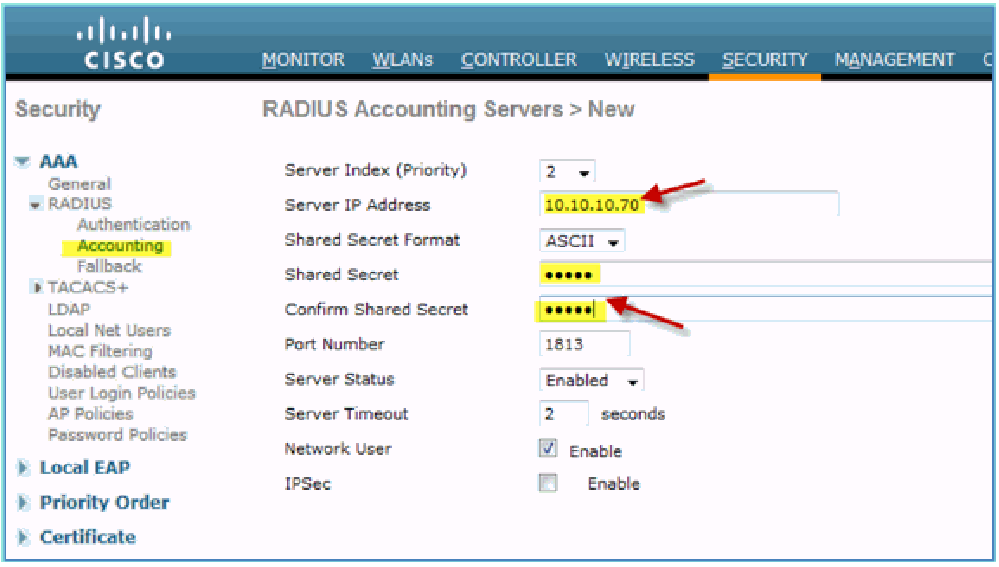
1) 打开浏览器，连接 WLC 的管理界面：http://<WLC 的管理 IP 地址>
2) 进入 Security > RADIUS > Authentication > New



RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address	10.10.10.70
Shared Secret Format	ASCII
Shared Secret	•••••
Confirm Shared Secret	•••••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	☑ Enable
IPSec	□ Enable

3) 输入以下数值：
   - Server IP Address：10.10.10.70
   - Shared Secret: cisco
   - Support for RFC 3576：Enabled(Default)
   - 其他选项：默认值
4) 点击 Apply，继续下面步骤
5) 选择 Security > RADIUS > Accounting > New



RADIUS Accounting Servers > New

Server Index (Priority)	2
Server IP Address	10.10.10.70
Shared Secret Format	ASCII
Shared Secret	●●●●●
Confirm Shared Secret	●●●●●
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
IPSec	□ Enable

6) 输入以下数值：

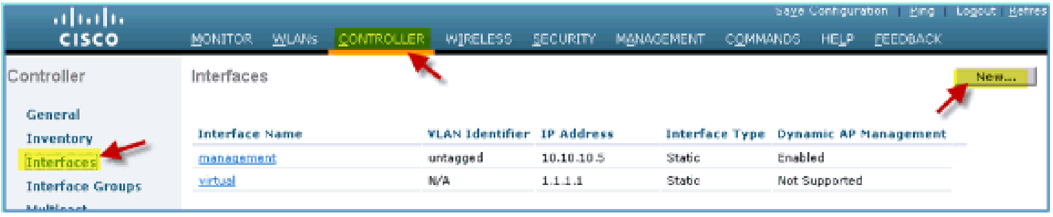
- o Server IP Address: 10.10.10.70
- o Shared Secret: cisco
- o 其他选项：默认值

7) 点击 Apply，然后点击 Save Configuration 保存所有配置。

- **在 WLC 上创建动态接口 Employee**

通过以下步骤在 WLC 上创建了一个动态接口，并将其映射到 Employee VLAN 中。

1) 在 WLC 上，进入 Controller > Interface > New

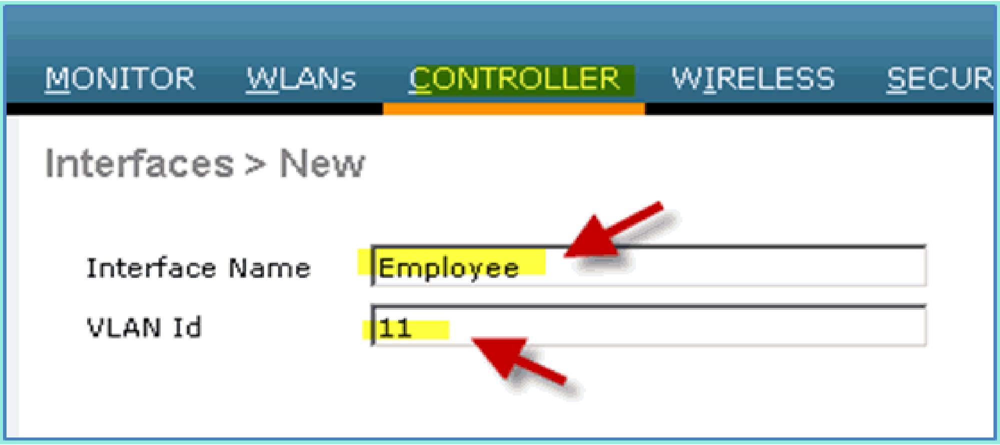


Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	untagged	10.10.10.5	Static	Enabled
virtual	N/A	1.1.1.1	Static	Not Supported

2) 在新建 Interface 上输入以下数值：

- o Interface Name: Employee
- o VLAN id: 11

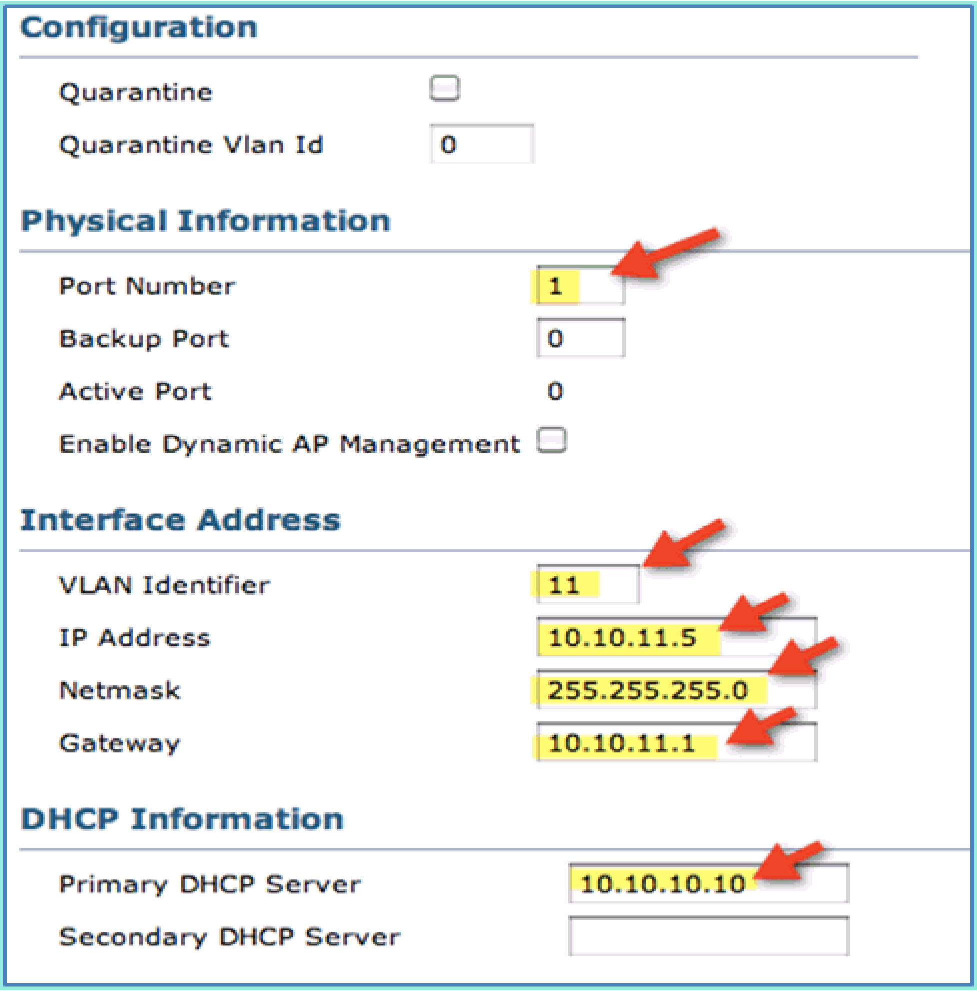


Interfaces > New

Interface Name	Employee
VLAN Id	11

3) 在新建接口 Employee 上输入以下数值：

- Port Number: 1
- VLAN Identifier: 11
- IP Address: 10.10.11.5
- Netmask: 255.255.255.0
- Gateway: 10.10.11.1
- DHCP: 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	□

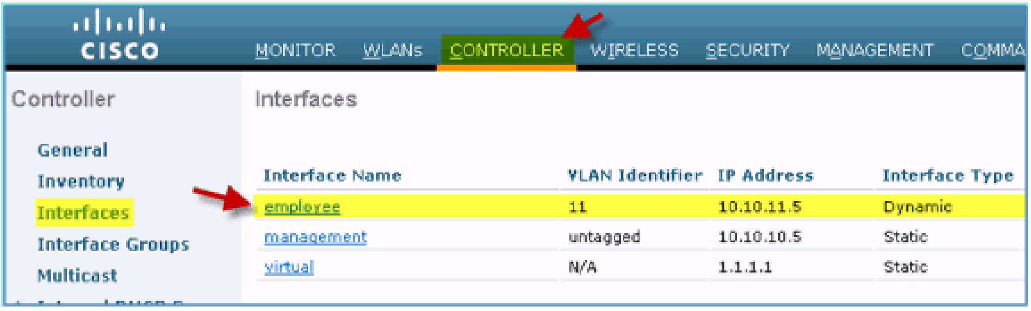
Interface Address

VLAN Identifier	11
IP Address	10.10.11.5
Netmask	255.255.255.0
Gateway	10.10.11.1

DHCP Information

Primary DHCP Server	10.10.10.10
Secondary DHCP Server	

4) 确认动态接口 Employee 已经创建完成：



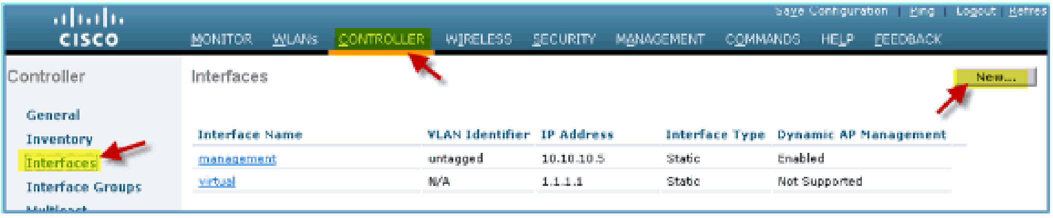
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

- **在 WLC 上创建动态接口 Guest**

通过以下步骤在 WLC 上创建了一个动态接口，并将其映射到 Guest VLAN 中。

1) 在 WLC 上，进入 Controller > Interfaces > New

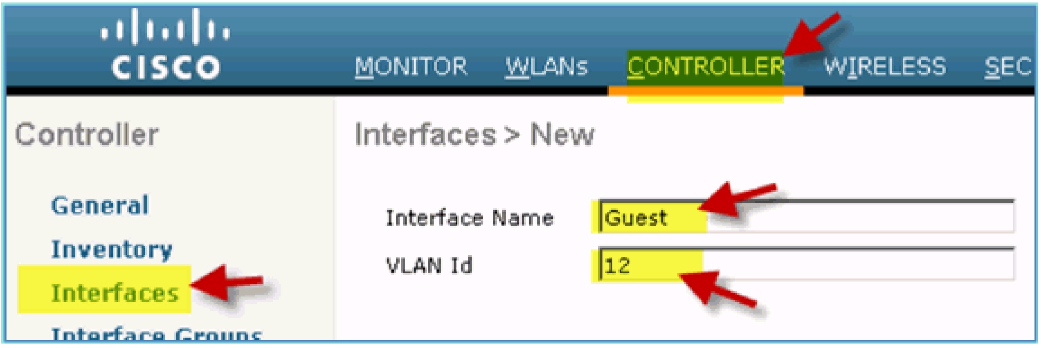

Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
New...

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	untagged	10.10.10.5	Static	Enabled
virtual	N/A	1.1.1.1	Static	Not Supported

2) 在新建 Interface 上，输入以下数值：

- Interface Name:
- VLAN Id:12



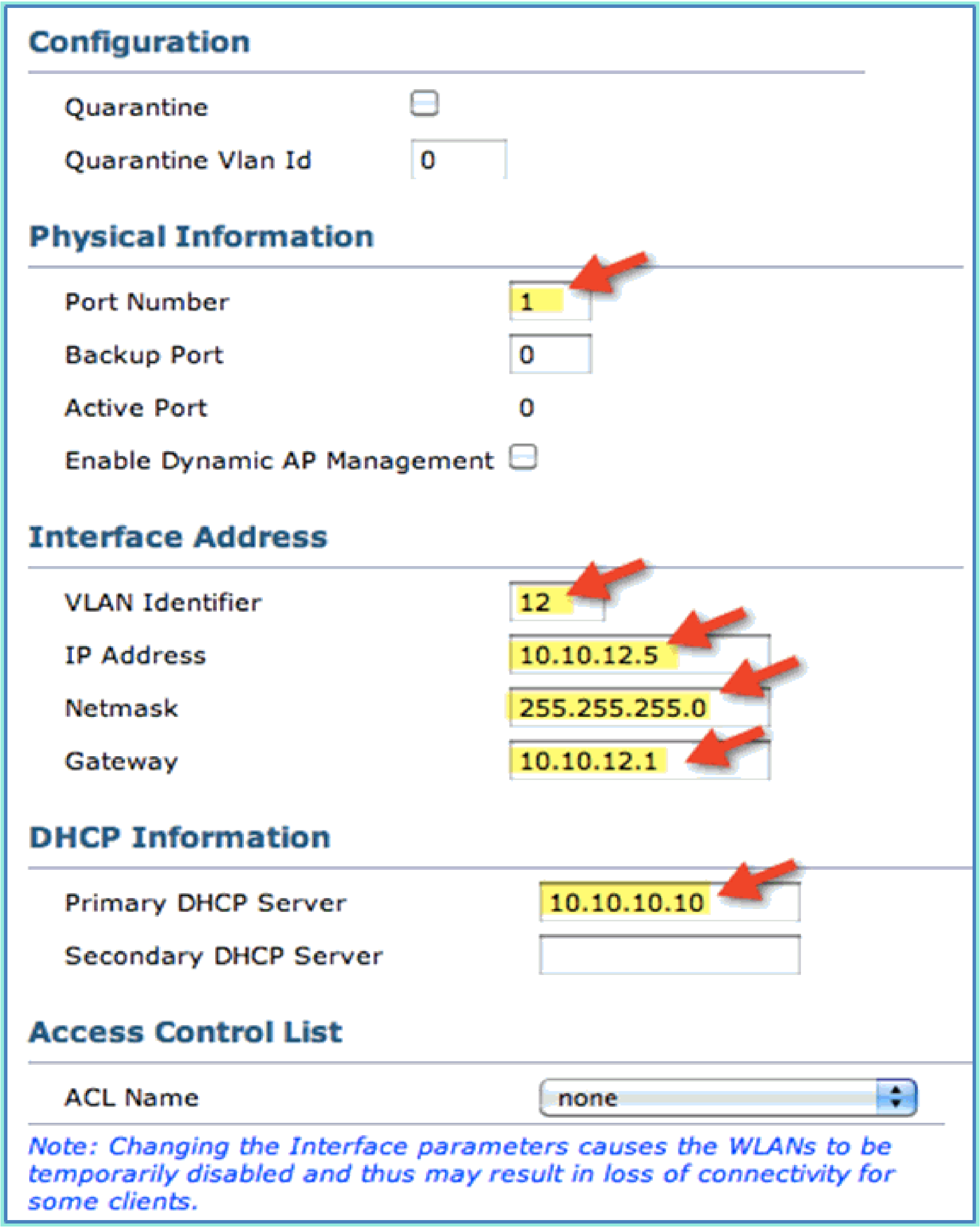
Interfaces > New

Interface Name: Guest

VLAN Id: 12

3) 在新建接口 Guest 上输入以下数值：

- Port Number: 1
- VLAN Identifier: 12
- IP Address: 10.10.12.5
- Netmask: 255.255.255.0
- Gateway: 10.10.12.1
- DHCP: 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

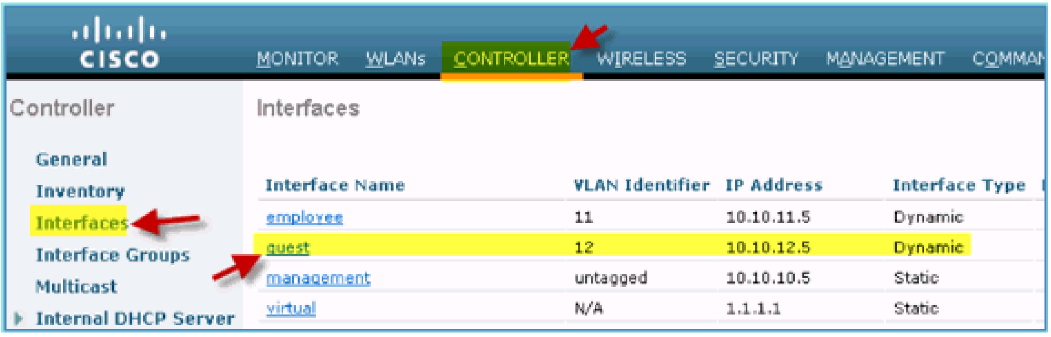
Secondary DHCP Server:

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.

3) 确认动态接口 Guest 已经完成添加：



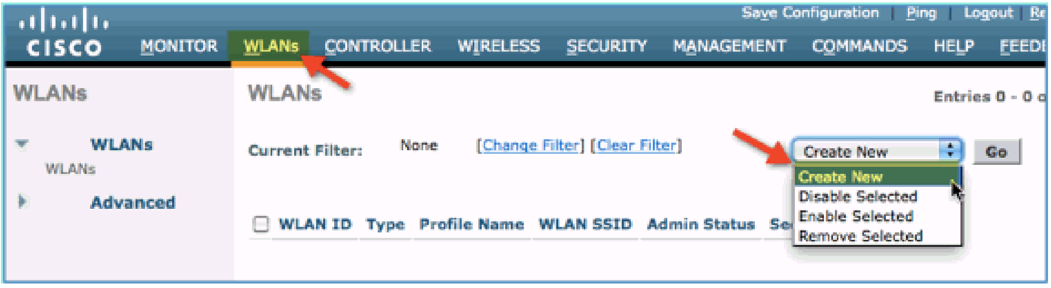
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
guest	12	10.10.12.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

- 新建 802.1X WLAN

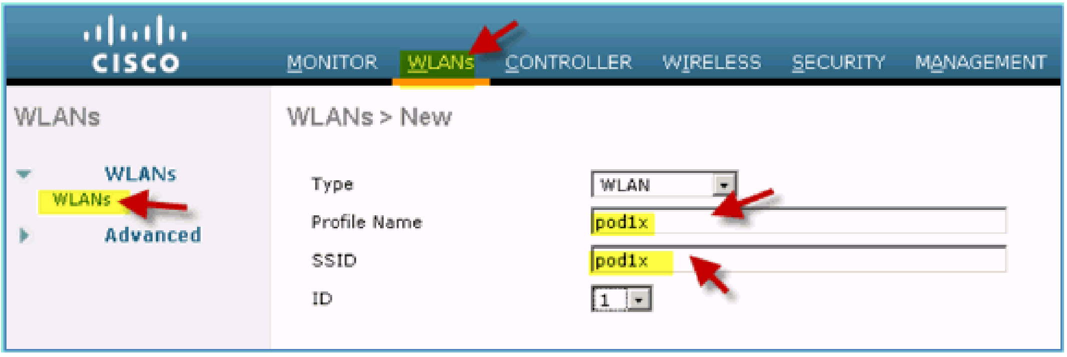
在 WLC 的初始配置中，可能已经有缺省的 WLAN 已经创建了。如果这样，可以修改或新建支持 802.1X 认证的 WLAN。

1) 在 WLC 上，进入 WLAN > Create New



2) 对于新建 WLAN，输入以下信息：

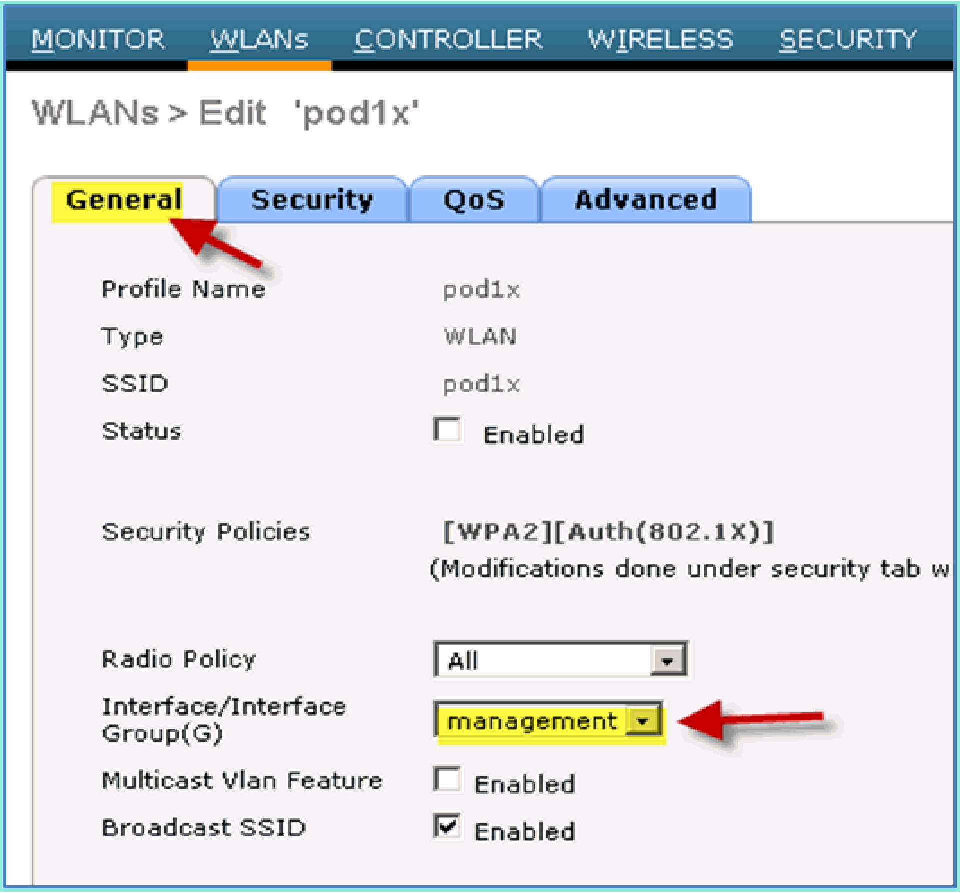
- Profile Name: pod1x
- SSID: pod1x



Type: WLAN
Profile Name: pod1x
SSID: pod1x
ID: 1

3) 进入 WLAN 设置 > General，修改以下配置：

- Radio Policy: All
- Interface/Group: management
- 其他配置：默认值

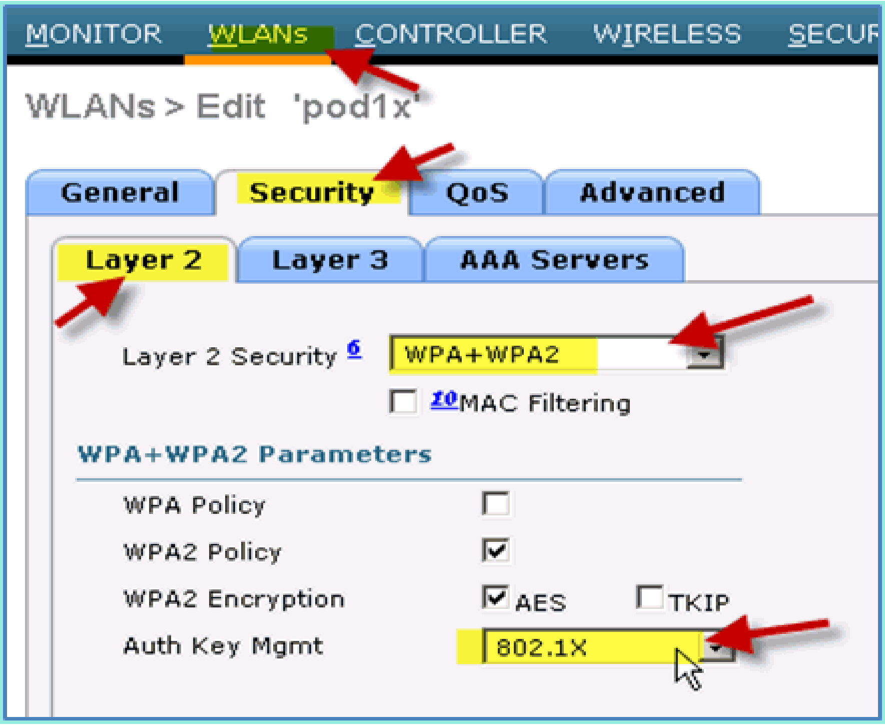


WLANs > Edit 'pod1x'

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	□ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab w
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled

4) 进入 WLAN > Security Tab > Layer 2，修改以下配置：

- Layer 2 Security: WPA+WPA2
- WPA2 Policy/Encryption: Enabled/AES
- Auth Key Mgmt: 802.1X



WLANs > Edit 'pod1x'

Layer 2 Security [6] WPA+WPA2

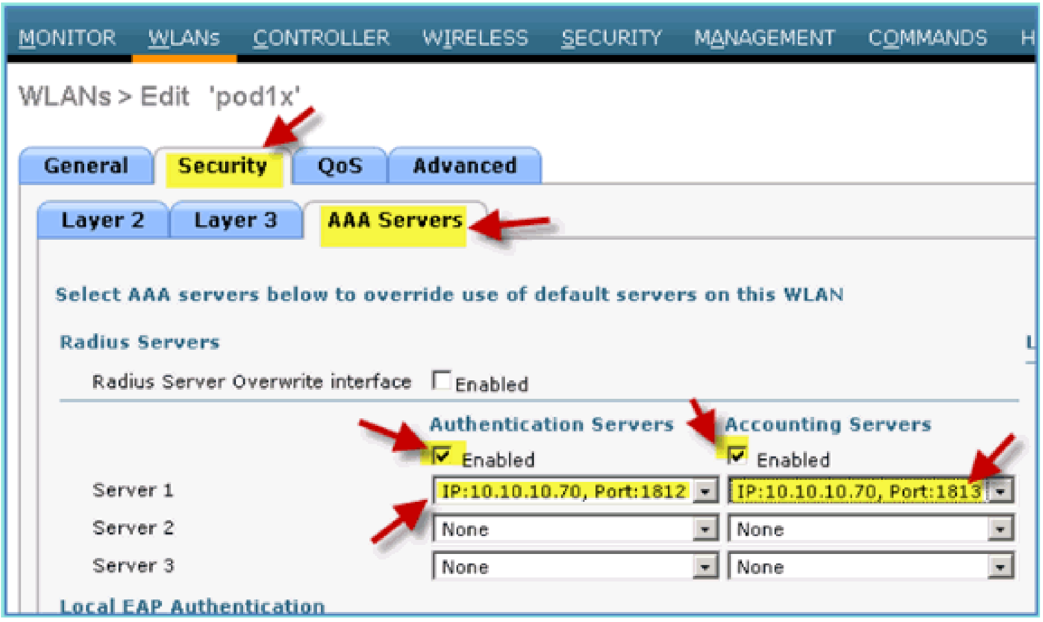
□ [10]MAC Filtering

WPA+WPA2 Parameters

WPA Policy	□	
WPA2 Policy	☑	
WPA2 Encryption	☑ AES	□ TKIP
Auth Key Mgmt	802.1X	

5) 进入 WLAN > Security Tab > AAA Servers，修改以下配置：

- Radius Server Overwrite interface: Disabled
- Authentication/Accountint Server: Enable
- Server1: 10.10.10.70



WLANs > Edit 'pod1x'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

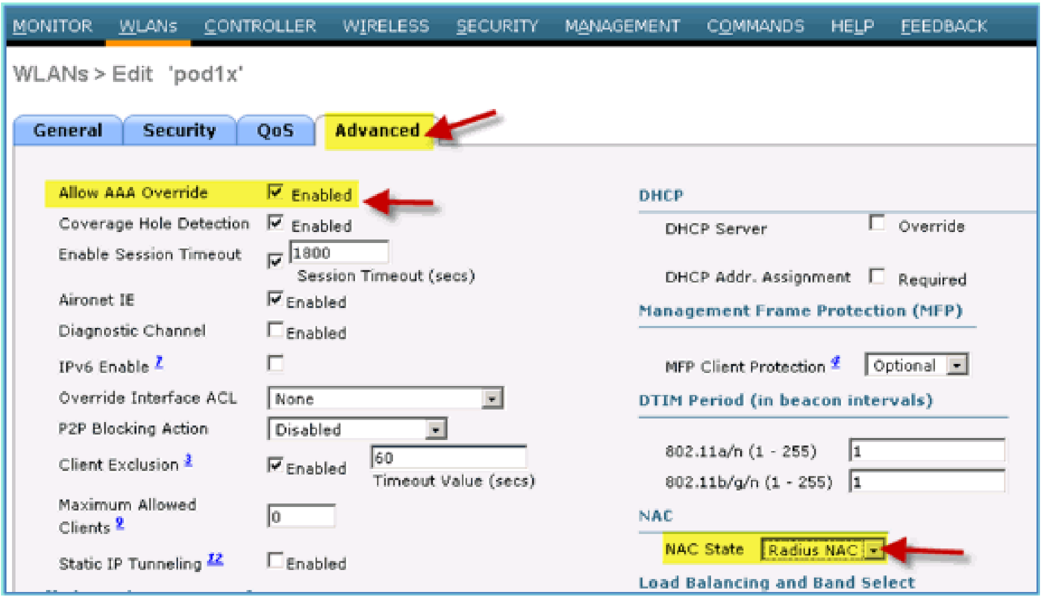
Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.10.10.70, Port:1812	IP:10.10.10.70, Port:1813
Server 2	None	None
Server 3	None	None

Local EAP Authentication

6) 进入 WLAN > Advanced Tab，修改以下配置：

- Allow AAA Override: Enabled
- NAC State: Radius NAC(selected)



WLANs > Edit 'pod1x'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel □ Enabled

IPv6 Enable □

Override Interface ACL None

P2P Blocking Action Disabled

Client Exclusion ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients 0

Static IP Tunneling □ Enabled

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

MFP Client Protection Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

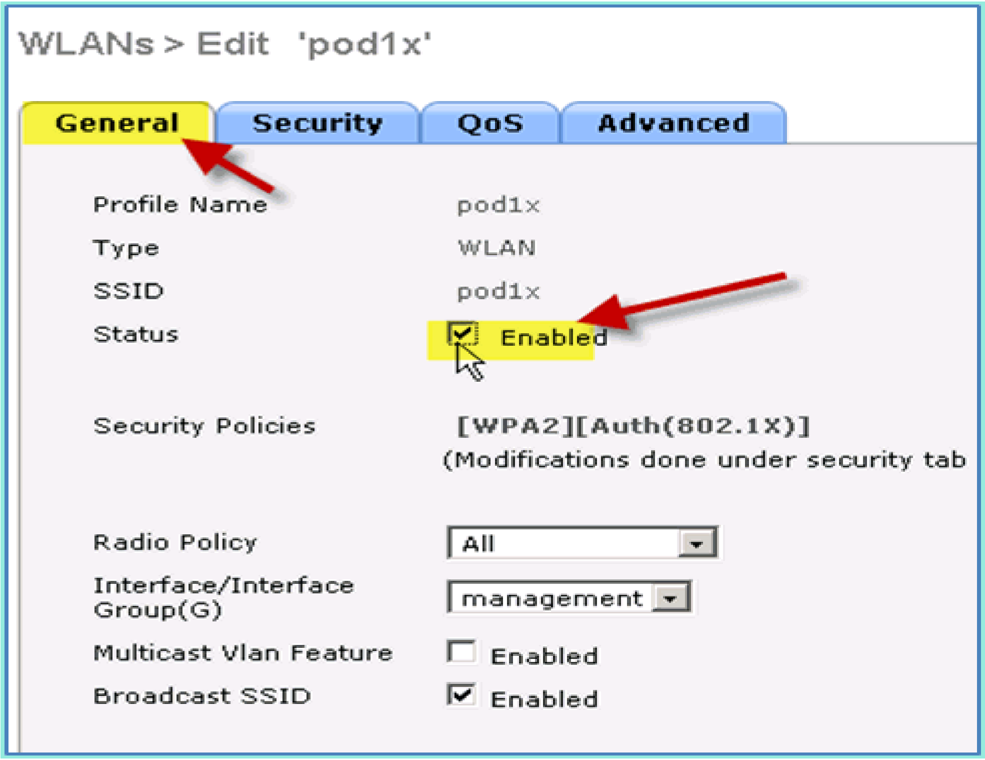
802.11b/g/n (1 - 255) 1

NAC

NAC State Radius NAC

Load Balancing and Band Select

7) 返回 WLAN > General Tab > Enabled WLAN：



WLANs > Edit 'pod1x'

Profile Name pod1x

Type WLAN

SSID pod1x

Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab

Radio Policy All

Interface/Interface Group(G) management

Multicast Vlan Feature □ Enabled

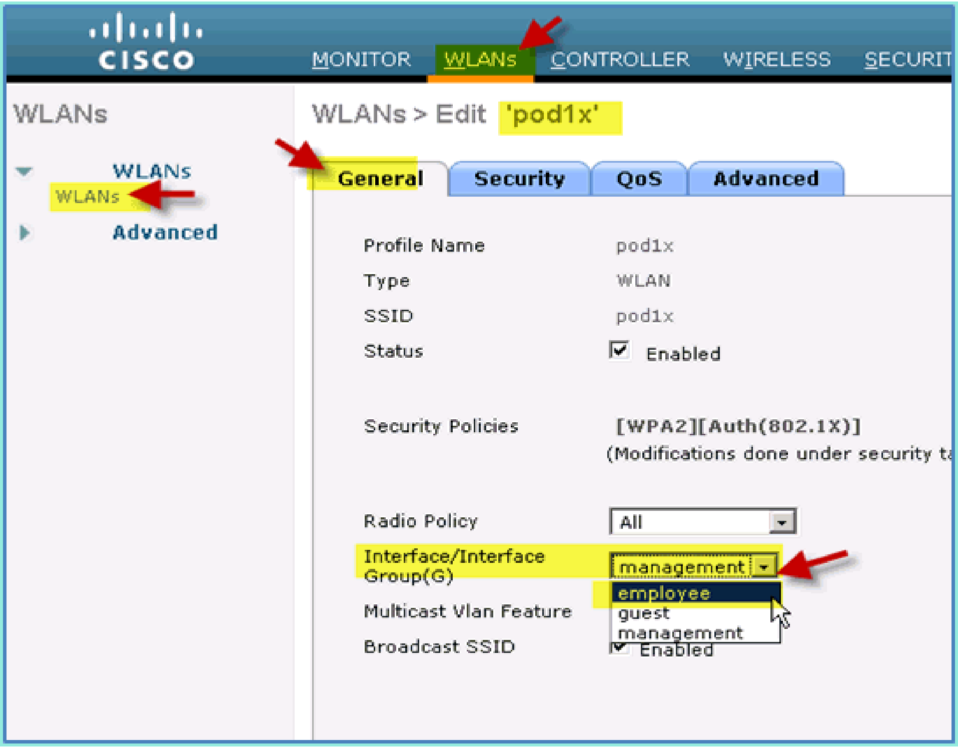
Broadcast SSID ☑ Enabled

- **测试 WLC 动态接口的配置**

快速检查动态接口 Employee 和 Guest。通过任意设备连接到 WLAN，分别分配 Employee 和 Guest 接口，验证设备分配的 VLAN。

1) 在 WLC 上，进入 WLAN > WLANs，点击并编辑之前创建的 SSID。

2) 把 Interface/Interface Group 对应的接口修改为 Employee，点击 Apply。



WLANs > Edit 'pod1x'

Profile Name pod1x

Type WLAN

SSID pod1x

Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security ta

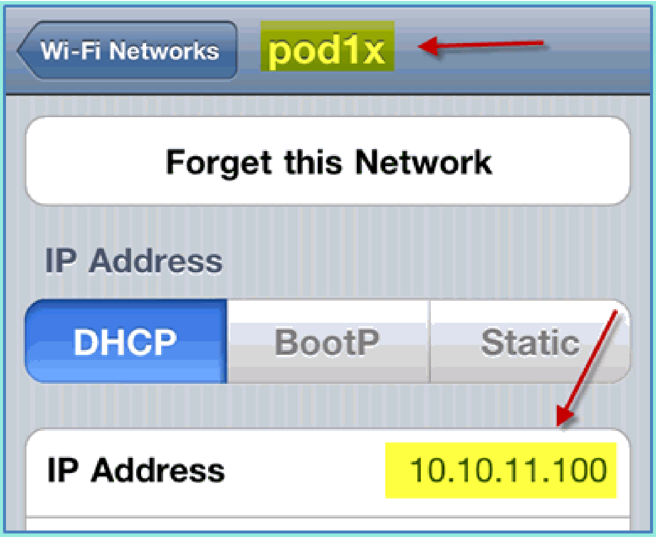
Radio Policy All

Interface/Interface Group(G) management
employee
guest
management

Multicast Vlan Feature

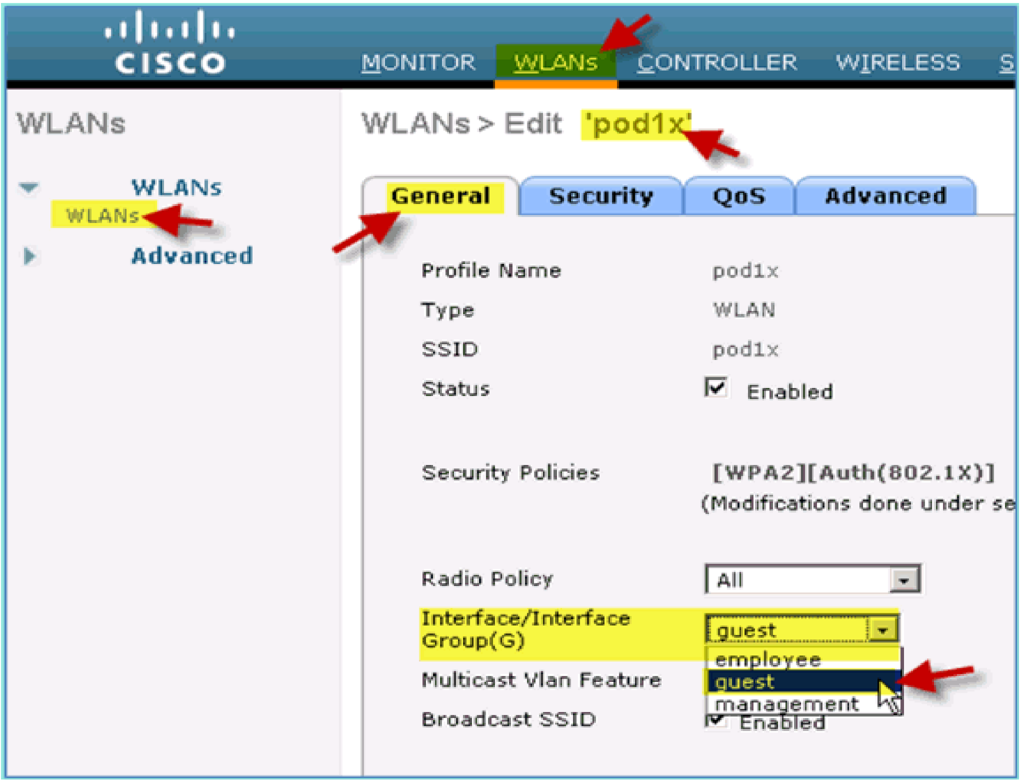
Broadcast SSID ☑ Enabled

3) 如果配置正确，设备会获得一个 Employee VLAN(10.10.11.0/24)的地址。下图显示一台 iPhone 设备获得了一个 VLAN 11 的地址。



IP Address 10.10.11.100

4) 验证接口 Employee 后，修改 WLAN 分配的接口为 Guest 接口，点击 Apply。



Profile Name pod1x

Type WLAN

SSID pod1x

Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under se

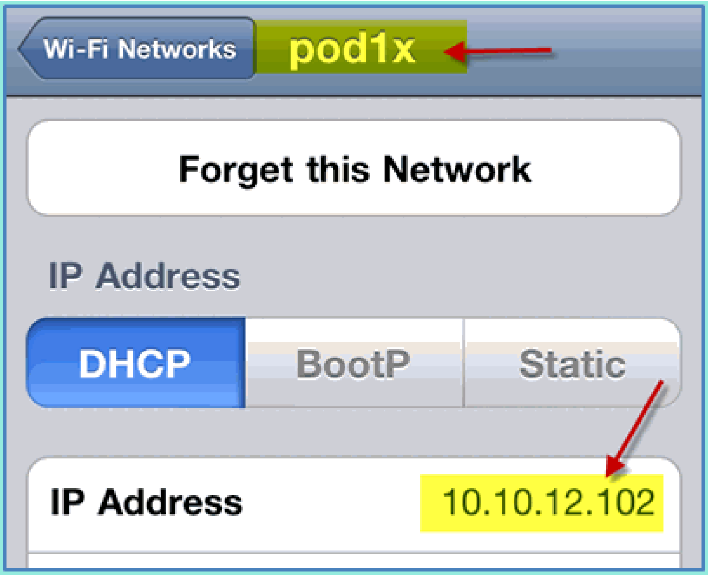
Radio Policy All

Interface/Interface Group(G) guest

Multicast Vlan Feature

Broadcast SSID ☑ Enabled

5) 如果配置正确，连接 WLAN 的设备会获得 Guest VLAN（10.10.12.0/24）的 IP 地址，如下图所示，获得了 VLAN 12 的地址。



IP Address 10.10.12.102

6) **重要步骤**：把 WLAN 分配的接口改回到接口 Management。

7) 点击 Apply 和 Save Configuration，保存 WLC 的配置。

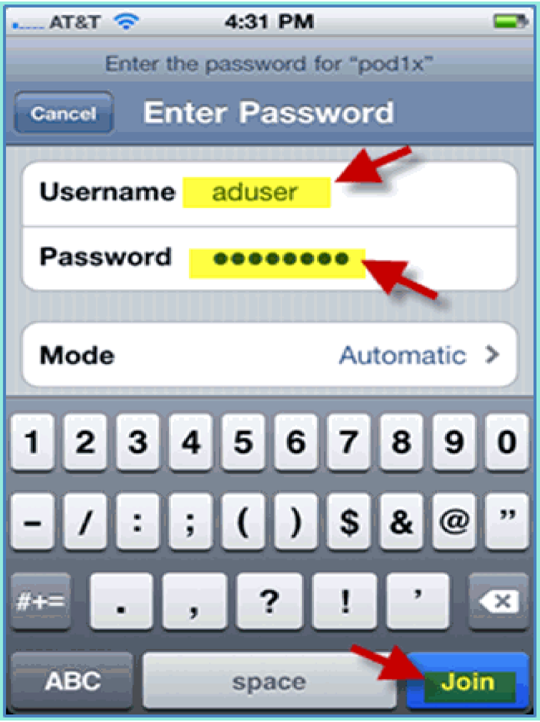
- **针对 iOS 设备(iPhone/iPad)的无线认证**

使用移动终端设备，如 iPhone，iPad 或 iPod 等运行 iOS 的设备，用内部用户或 AD 用户作为认证帐号，连接到需要认证的 SSID。

1) 在 iOS 设备上，进入 WLAN 设置，启用 Wifi，然后选择连接在 WLC 上创建的需要 802.1X 认证的 SSID。

2) 提供以下信息连接到 SSID：pod1x

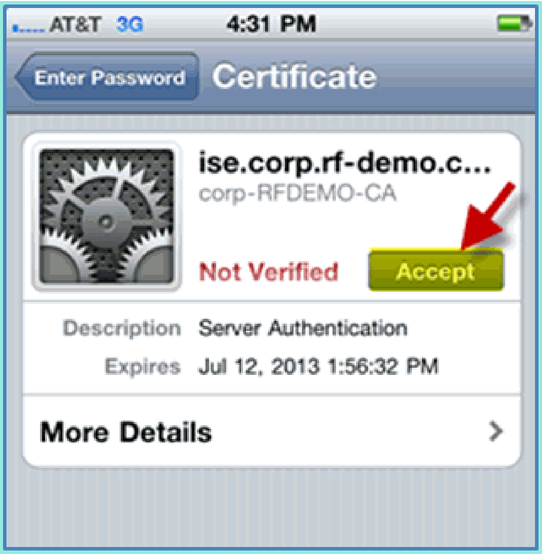
- 用户名：employee 或 contractor
- 密码：XXXX



Username aduser

Password ●●●●●●●●●

3) 点击 Accept，接受 ISE 的证书



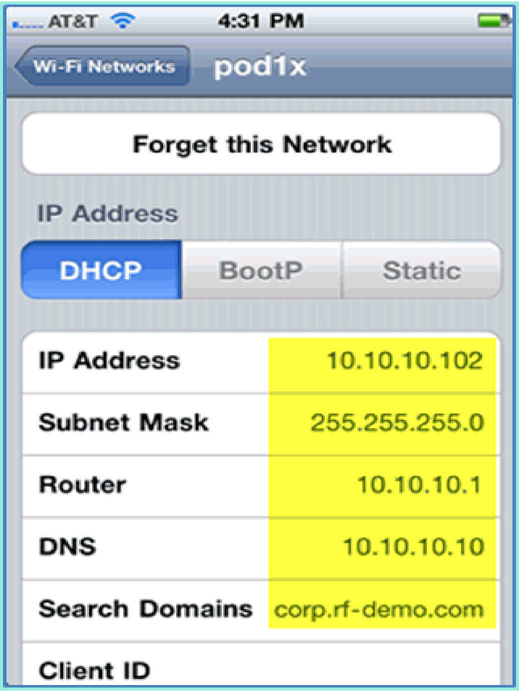
ise.corp.rf-demo.c...

corp-RFDEMO-CA

Description Server Authentication

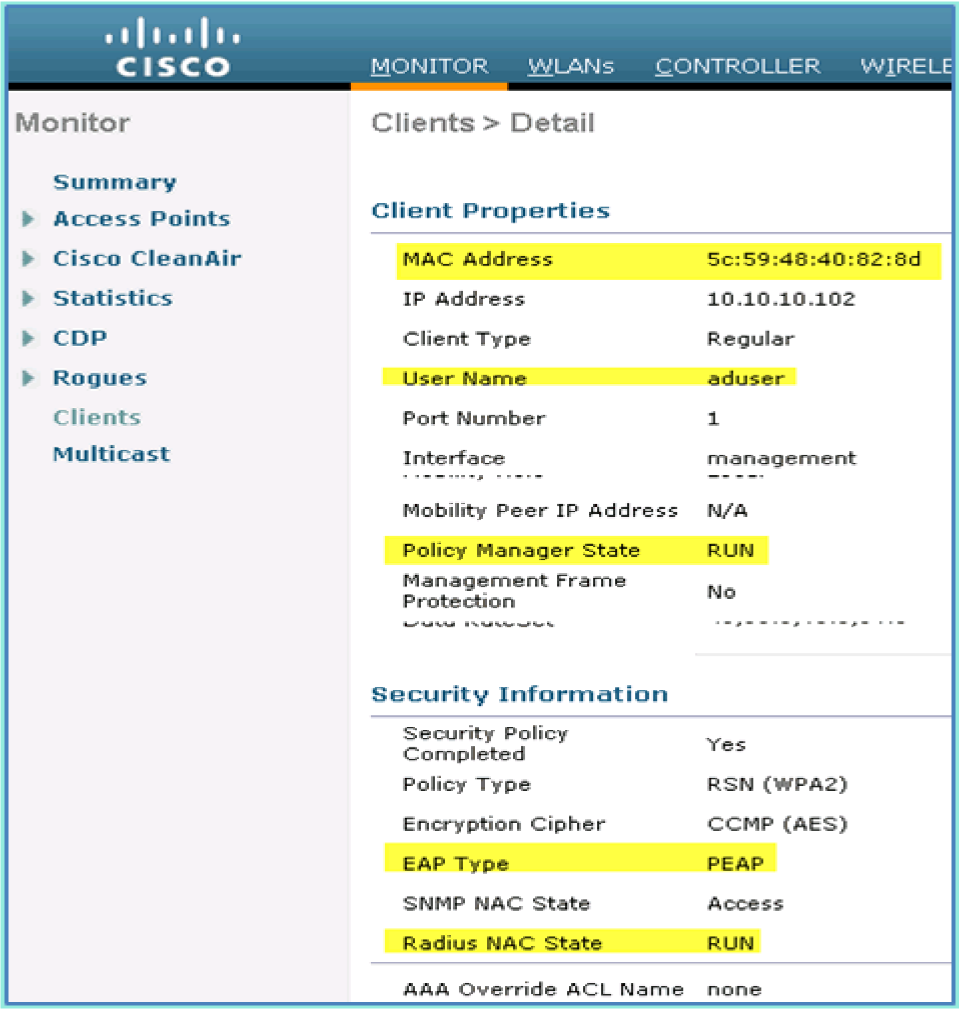
Expires Jul 12, 2013 1:56:32 PM

4) 确认设备获得了接口 Management（VLAN10）的 IP 地址



IP Address	10.10.10.102
Subnet Mask	255.255.255.0
Router	10.10.10.1
DNS	10.10.10.10
Search Domains	corp.rf-demo.com
Client ID	

5) 在 WLC 上，进入 Monitor > Clients，验证终端设备信息，包括 User Name，Radius NAC State 和 EAP type。



Clients > Detail

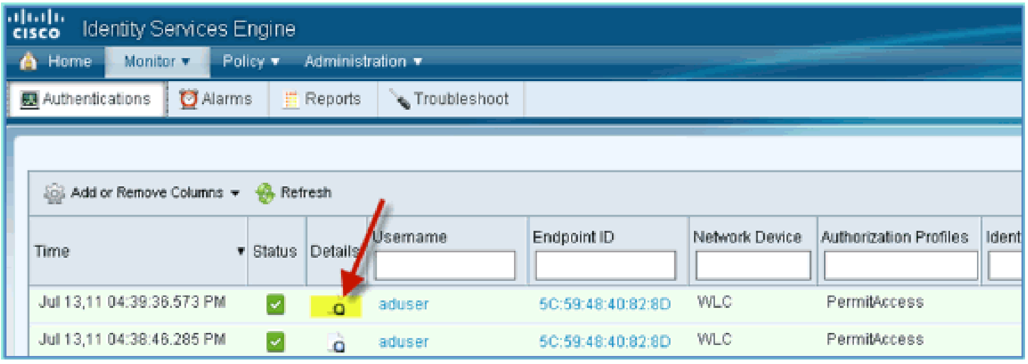
Client Properties

MAC Address	5c:59:48:40:82:8d
IP Address	10.10.10.102
Client Type	Regular
User Name	aduser
Port Number	1
Interface	management
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

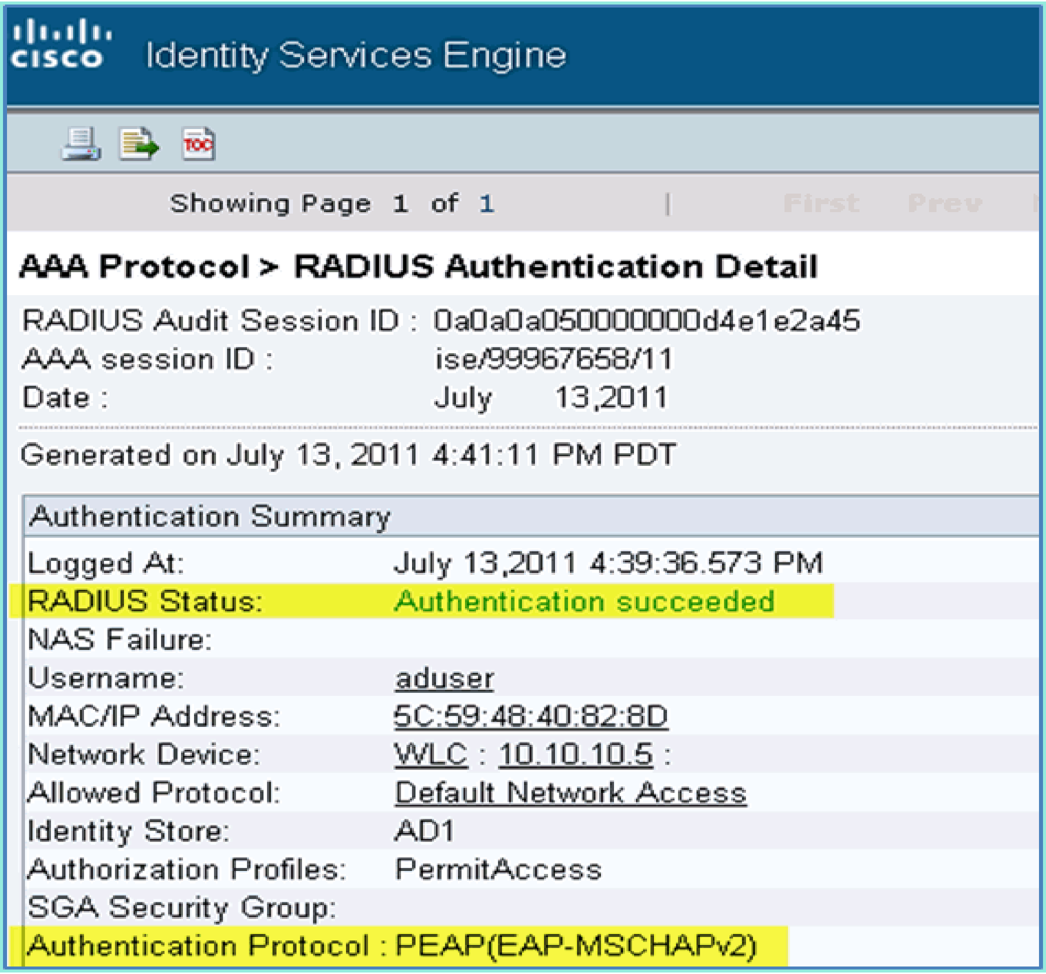
Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN
AAA Override ACL Name	none

6) 类似地，在 ISE 上，进入 Monitor > Authentications 页面查看终端设备认证信息。



Time	Status	Details	Username	Endpoint ID	Network Device	Authorization Profiles	Ident
Jul 13,11 04:39:38.573 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	
Jul 13,11 04:38:46.285 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	

7) 点击 Details 图标，查看认证会话的详细信息。



AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : 0a0a0a050000000d4e1e2a45
AAA session ID : ise/99967658/11
Date : July 13,2011

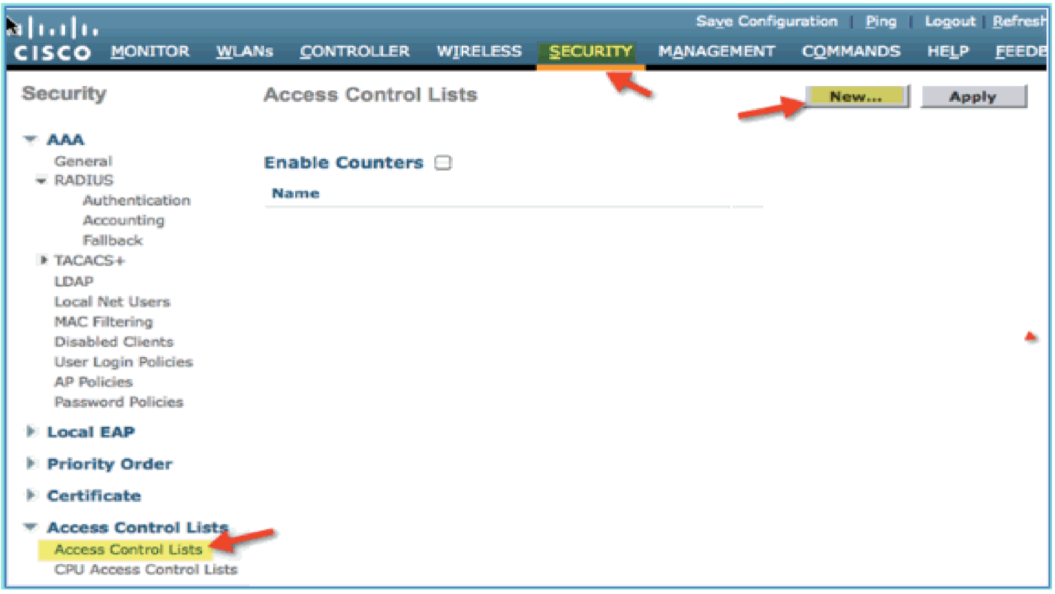
Generated on July 13, 2011 4:41:11 PM PDT

Authentication Summary	
Logged At:	July 13,2011 4:39:36.573 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	aduser
MAC/IP Address:	5C:59:48:40:82:8D
Network Device:	WLC : 10.10.10.5 :
Allowed Protocol:	Default Network Access
Identity Store:	AD1
Authorization Profiles:	PermitAccess
SGA Security Group:	
Authentication Protocol :	PEAP(EAP-MSCHAPv2)

- **在 WLC 创建重定向 ACL**

通过在 WLC 上配置重定向 ACL，ISE 就可以利用 ACL 限制终端设备进行健康状态检查。ACL 的最低要求是放行终端设备的流量到 ISE 上。其他 ACL 规则也可以根据情况增加。

1) 进入 Security > Access Control Lists > Access Control Lists，点击 New

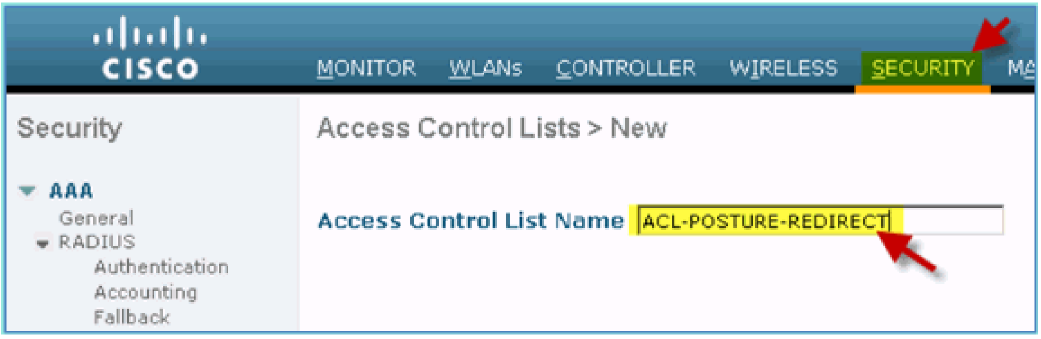


Access Control Lists

Enable Counters □

Name

2) 定义 ACL 的名字：ACL-POSTURE-REDIRECT

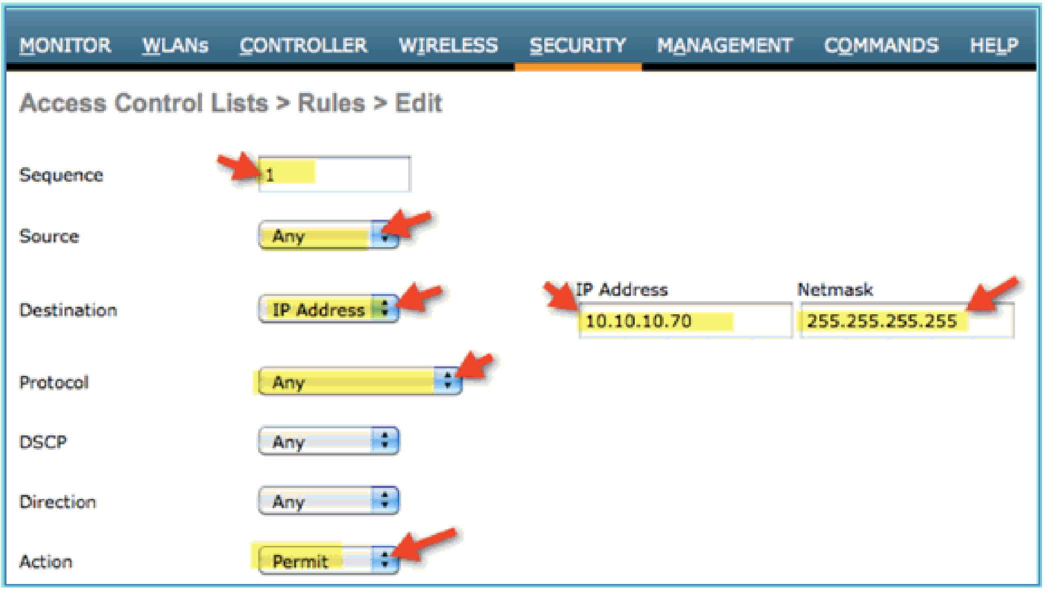


Access Control Lists > New

Access Control List Name: ACL-POSTURE-REDIRECT

3) 点击 Add New Rule，并设置 ACL 的顺序号为 1，并输入以下数值。完成后点击 Apply。

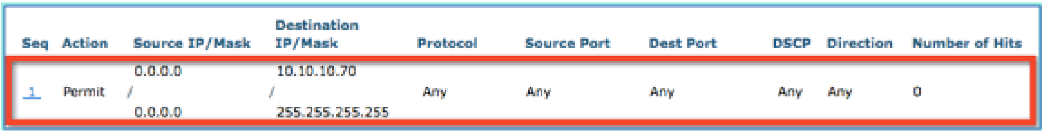
- Source: Any
- Desitnation: IP Address 10.10.10.70 255.255.255.255
- Protocol: Any
- Action: Permit



Access Control Lists > Rules > Edit

Sequence: 1
Source: Any
Destination: IP Address — IP Address: 10.10.10.70 — Netmask: 255.255.255.255
Protocol: Any
DSCP: Any
Direction: Any
Action: Permit

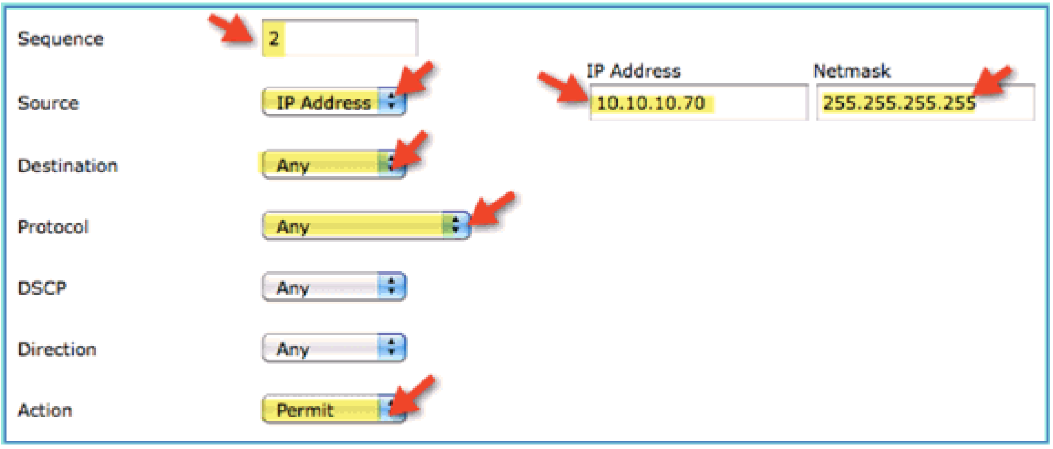
4) 确认顺序号 1 已经完成添加。



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) 点击 Add New Rule。添加顺序号为 2 的 ACL 条目，输入以下数值。完成后点击 Apply.

- Source: IP Address 10.10.10.70 255.255.255.255
- Destination: Any
- Protocol: Any
- Action: Permit



Sequence: 2

Source: IP Address — IP Address: 10.10.10.70 — Netmask: 255.255.255.255

Destination: Any

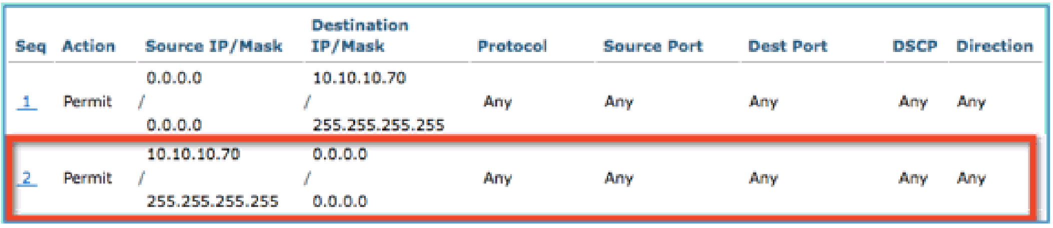
Protocol: Any

DSCP: Any

Direction: Any

Action: Permit

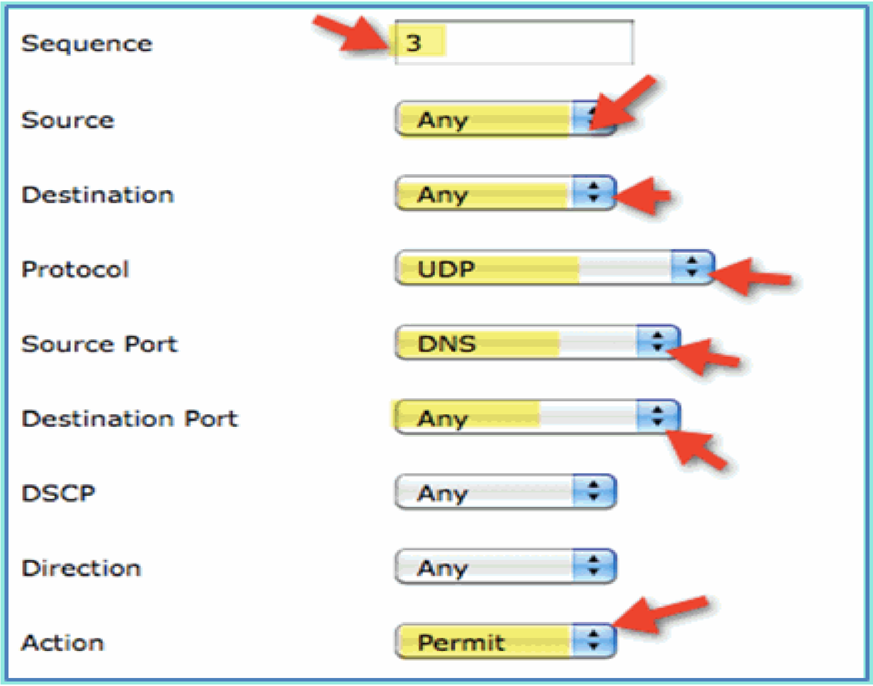
6) 确认 ACL 顺序号 2 已经完成添加。



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) 设置 ACL 条目 3 的输入如下，完成后点击 Apply。

- Source： Any
- Destination： Any
- Protocol： UDP
- Source Port： DNS
- Destination Port： Any



Sequence: 3

Source: Any

Destination: Any

Protocol: UDP

Source Port: DNS

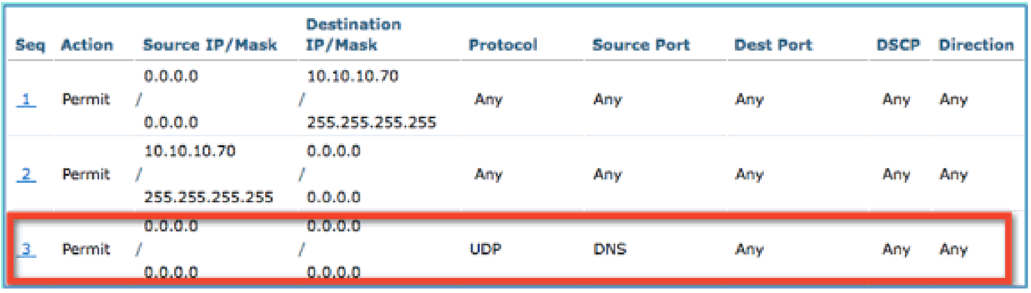
Destination Port: Any

DSCP: Any

Direction: Any

Action: Permit

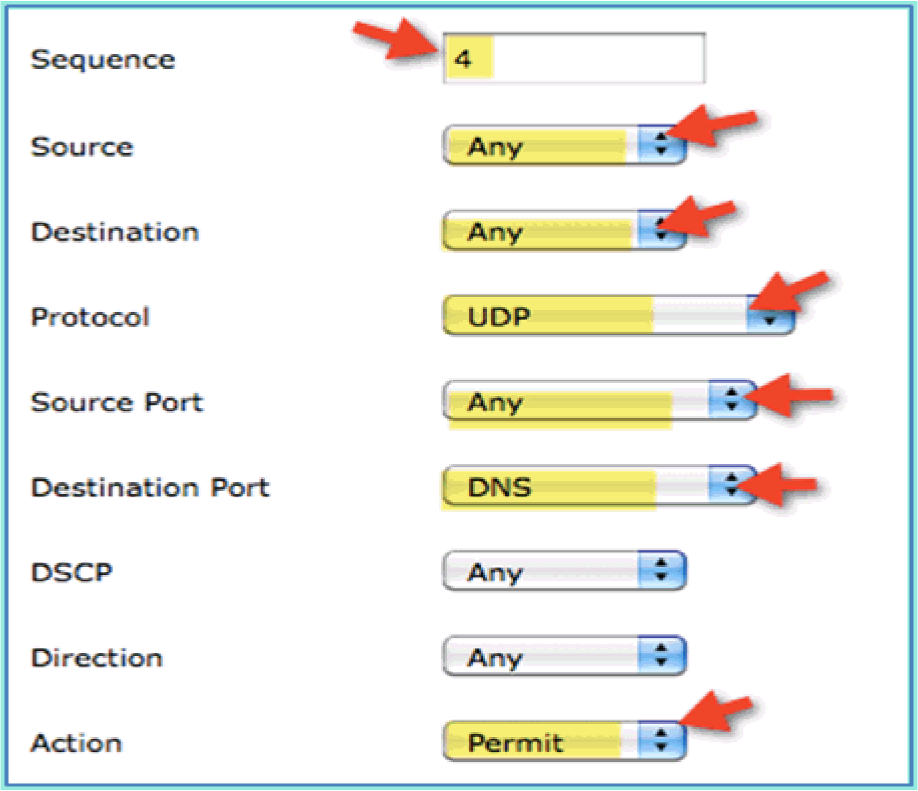
8) 确认 ACL 条目 3 已经添加完成。



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

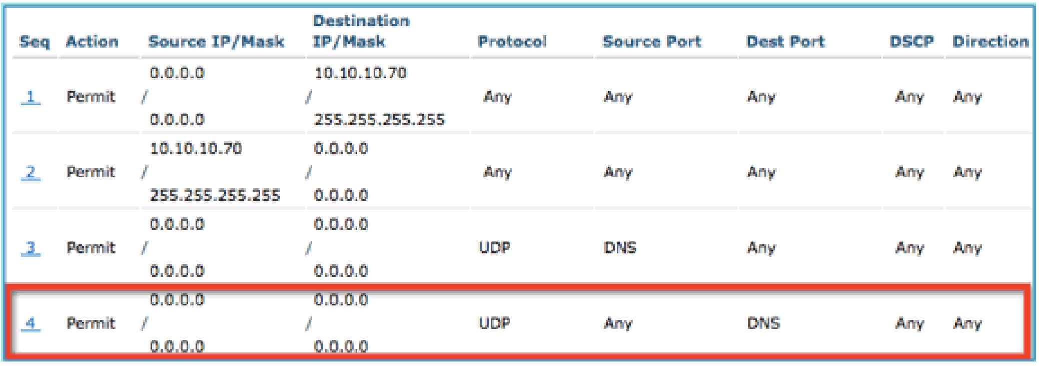
9) 点击 Add New Rule，添加 ACL 条目 4，并输入以下值，完成后点击 Apply。

- Source: Any
- Destination: Any
- Protocol: UDP
- Source Port: Any
- Destination Port: DNS
- Action: Permit



Sequence	4
Source	Any
Destination	Any
Protocol	UDP
Source Port	Any
Destination Port	DNS
DSCP	Any
Direction	Any
Action	Permit

10) 确认以下条目已经完成添加。



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

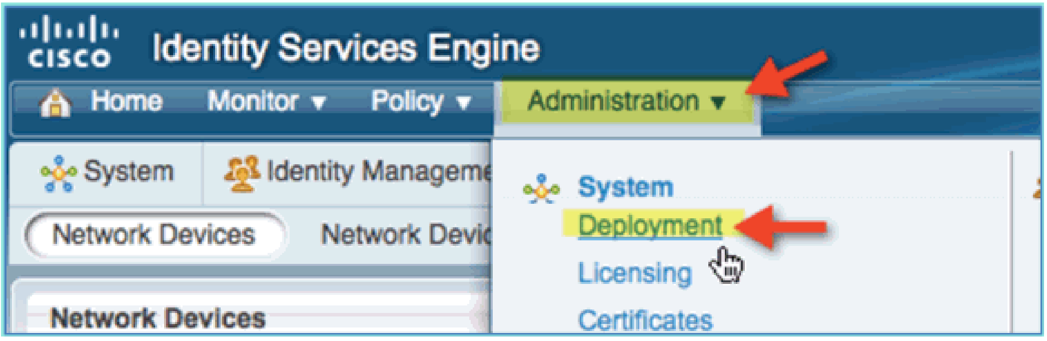
11) 保持 WLC 配置。

7. ISE 设备识别与授权配置

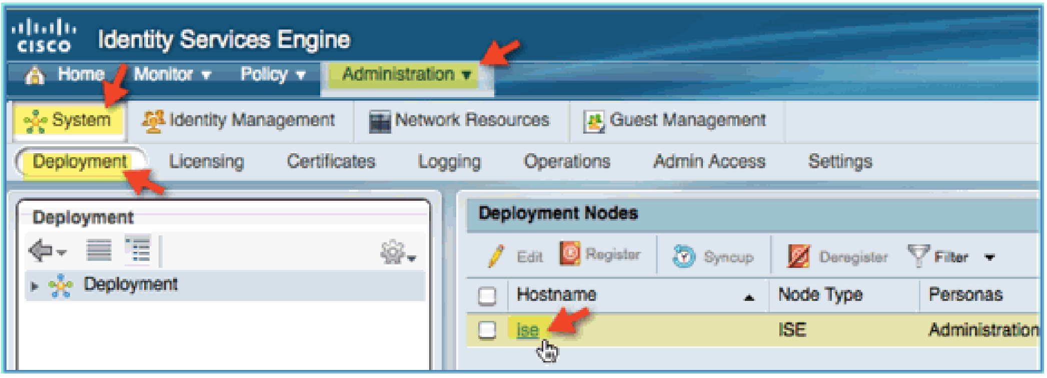
- **在 ISE 上启用设备探测**

ISE 需要配置为启用设备探测，识别终端设备的类型。默认情况下，这些选项是关闭的。以下部分介绍了如何启用 ISE 的设备识别。

1) 在 ISE 管理界面上，进入 Administration > System > Deployment。

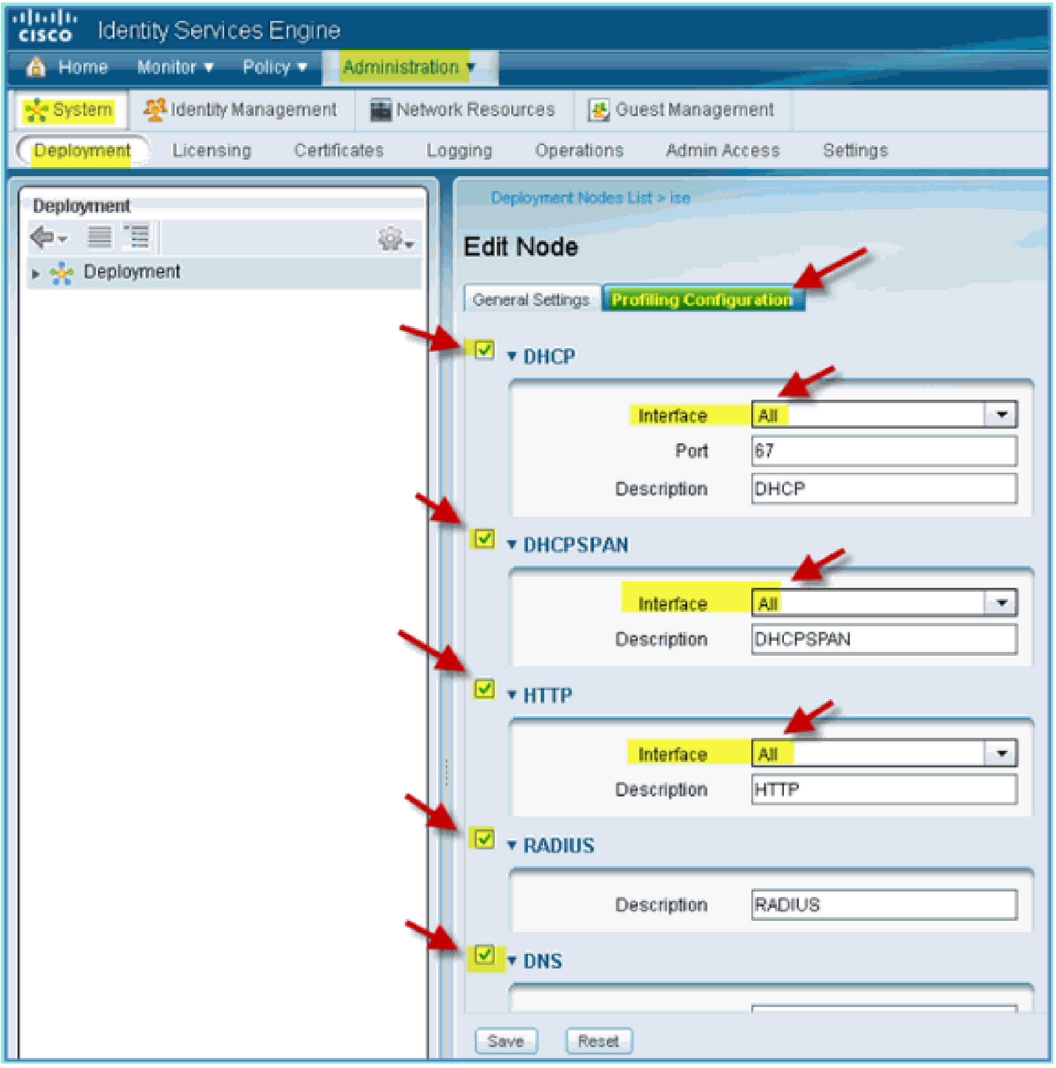


2) 选中主机名 ise，然后点击 Edit。



3) 在 Edit Node 页面，设置一下设备识别的属性值：

- DHCP: Enabled, All(or default)
- DHCPSPAN: Enabled,All(or default)
- HTTP: Enabled, All(or default)
- RADIUS: Enabled, N/A
- DNS: Enabled, N/A



☑ DHCP

Interface: All
Port: 67
Description: DHCP

☑ DHCPSPAN

Interface: All
Description: DHCPSPAN

☑ HTTP

Interface: All
Description: HTTP

☑ RADIUS

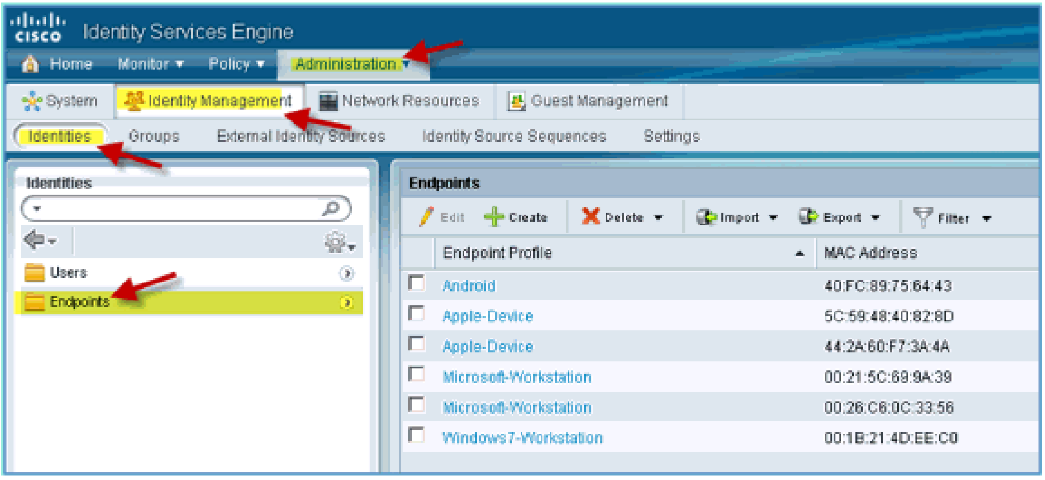
Description: RADIUS

☑ DNS

4) 断开连接无线的终端设备，再重新连接无线(iPhone/iPad/Android/Mac 等)。

5) 确认终端设备的身份。进入 Administration > Identity Management > Identities。点击 Endpoints 查看哪些设备已经被识别了。

注意：最初的识别是通过 RADIUS 探测。

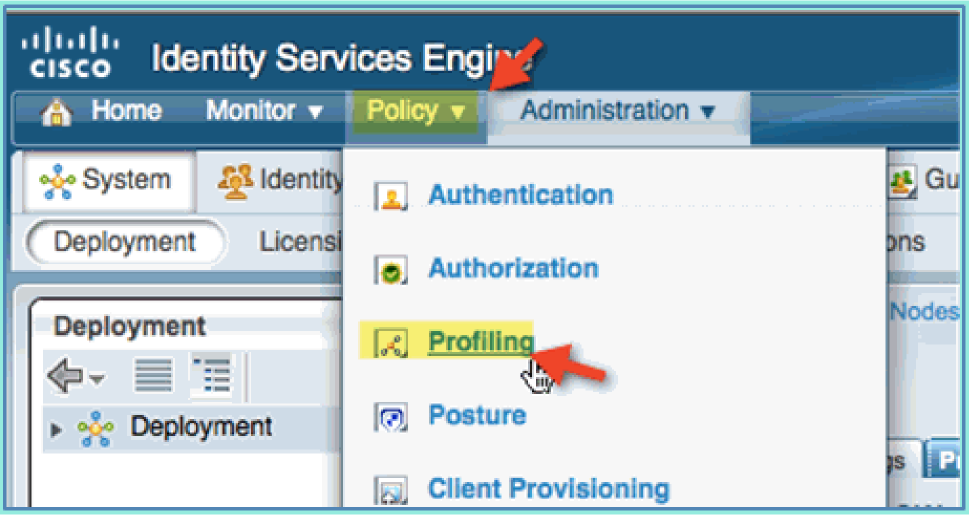


	Endpoint Profile	MAC Address
□	Android	40:FC:89:75:64:43
□	Apple-Device	5C:59:48:40:82:8D
□	Apple-Device	44:2A:60:F7:3A:4A
□	Microsoft-Workstation	00:21:5C:69:9A:39
□	Microsoft-Workstation	00:26:C6:0C:33:56
□	Windows7-Workstation	00:1B:21:4D:EE:C0

- **在 ISE 上配置设备识别策略**

ISE 提供了一个终端设备识别库，以下步骤启用了设备识别策略。

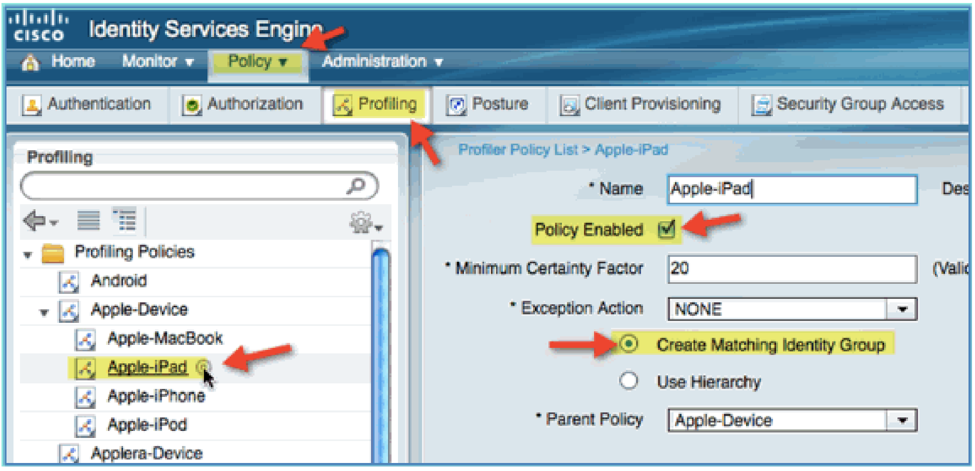
1) 在 ISE 管理界面上，进入 Policy > Profiling。



2) 在左侧面板，展开 Profiling Policies。

3) 点击 Apple-Device > Apple-iPad，并设置以下值：

- Policy Enabled: Enabled
- Creating Matching Identity Group: Selected



* Name: Apple-iPad

Policy Enabled ☑

* Minimum Certainty Factor: 20

* Exception Action: NONE

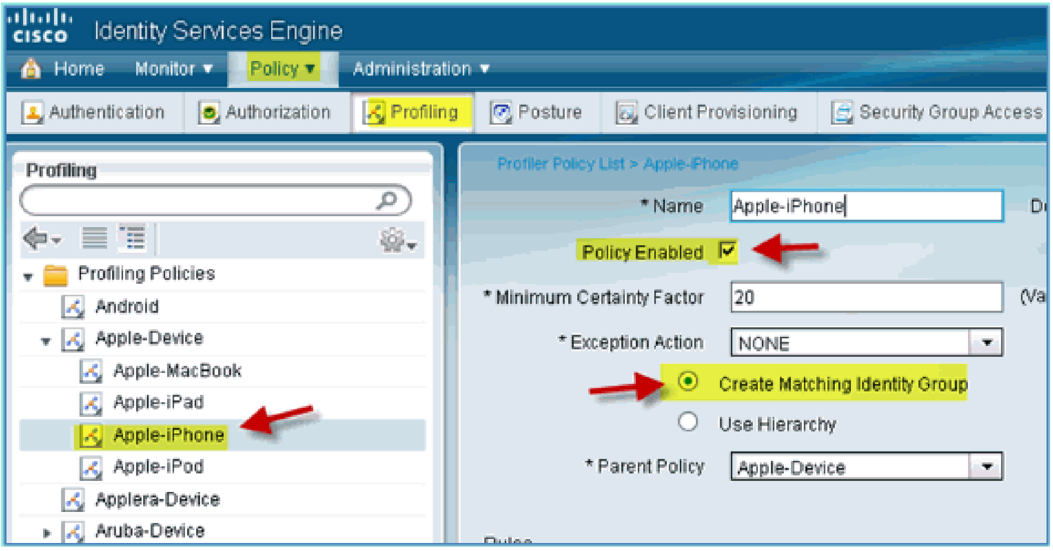
● Create Matching Identity Group

○ Use Hierarchy

* Parent Policy: Apple-Device

4) 点击 Apple-Device > Apple-iPhone，并设置以下值：

- Policy Enabled: Enabled
- Create Matching Identity Group: Selected



* Name Apple-iPhone

Policy Enabled ☑

* Minimum Certainty Factor 20

* Exception Action NONE

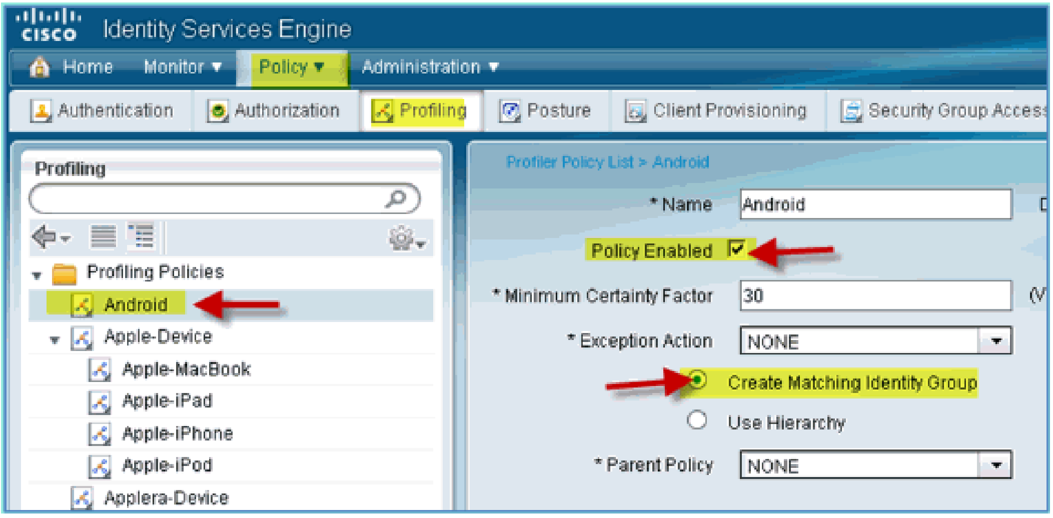
● Create Matching Identity Group

○ Use Hierarchy

* Parent Policy Apple-Device

5) 点击 Android，并设置以下值：

- Policy Enabled: Enabled
- Create Matching Identity Group: Selected



* Name Android

Policy Enabled ☑

* Minimum Certainty Factor 30

* Exception Action NONE

● Create Matching Identity Group

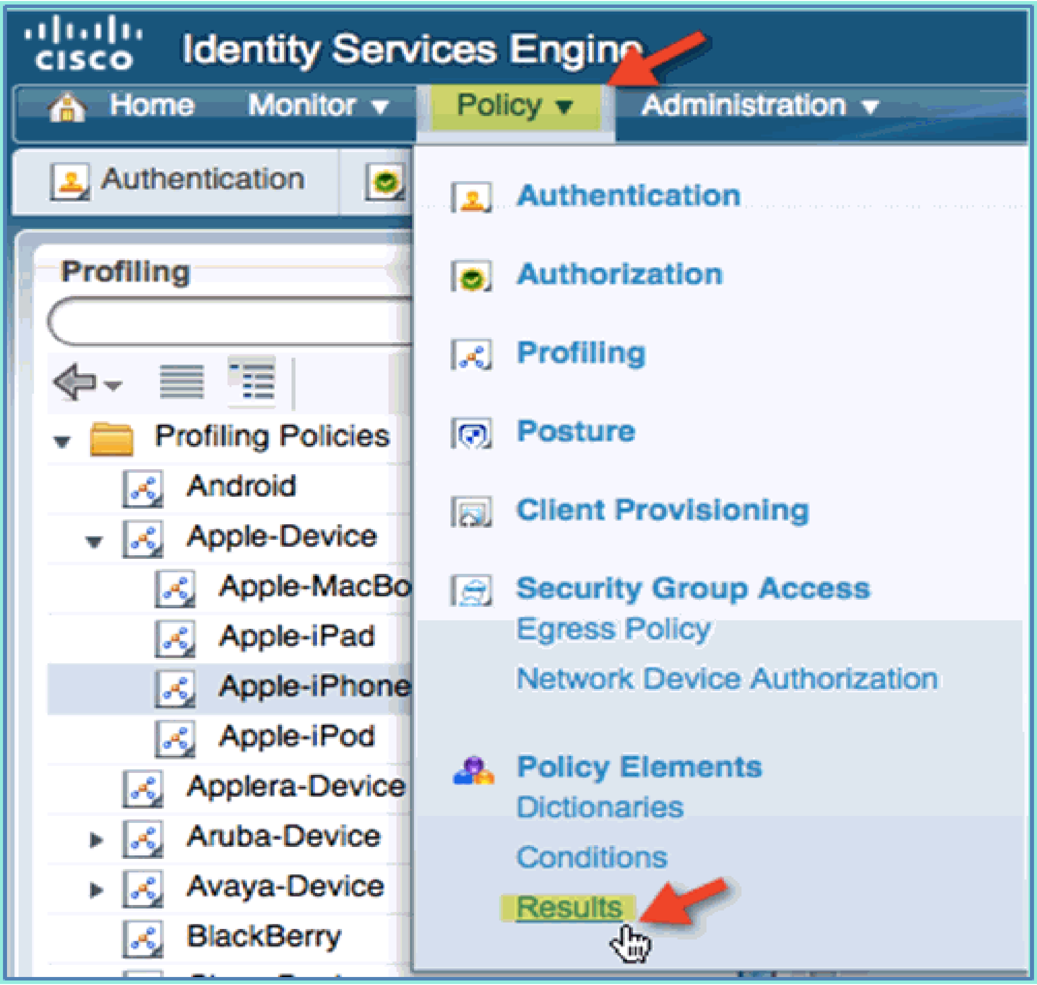
○ Use Hierarchy

* Parent Policy NONE

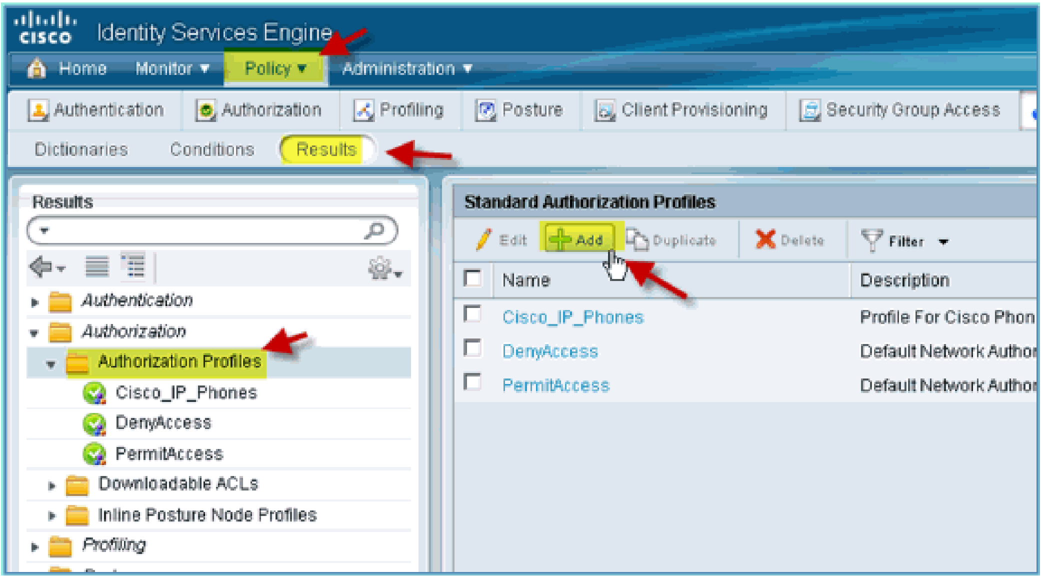
- **在 ISE 上创建用于认证后重定向的 Authorization Profile**

通过以下步骤创建一个授权策略，用于将新设备重定向到 ISE 上并进行终端设备的检测和识别。

1) 在 ISE 管理界面上，进入 Policy > Policy Elements > Results.



2) 展开 Authorization。点击 Authorization Profiles(左侧面板)并点击 Add。

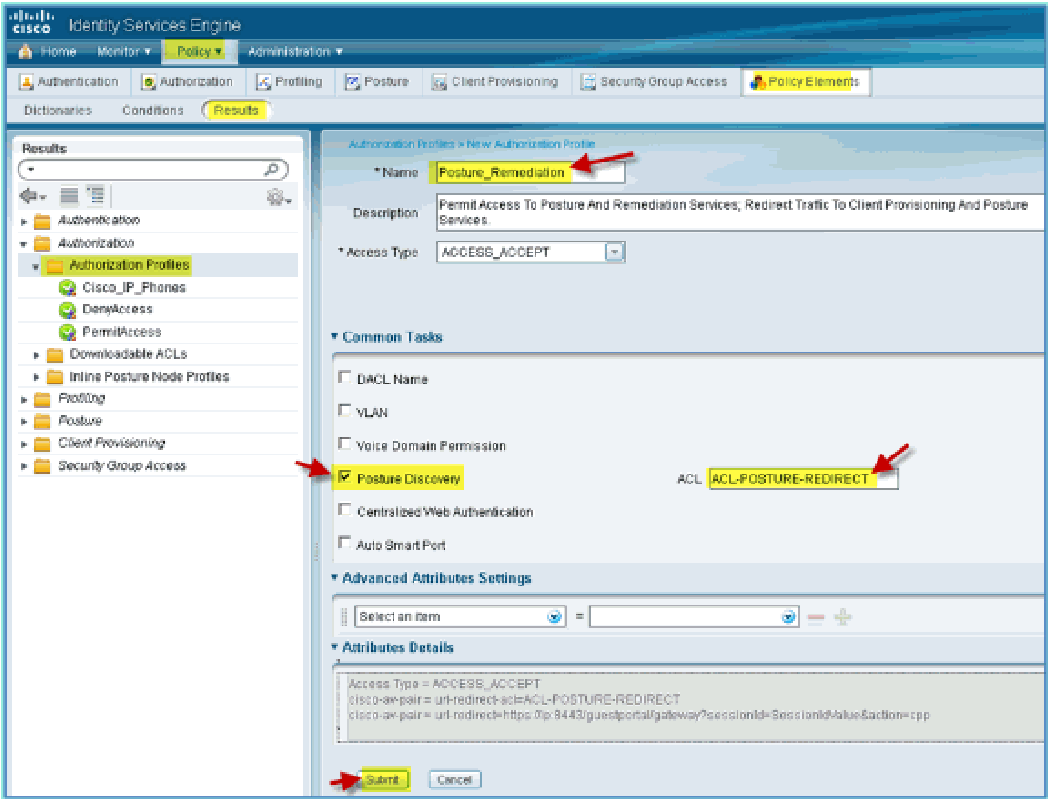


□	Name	Description
□	Cisco_IP_Phones	Profile For Cisco Phon
□	DenyAccess	Default Network Author
□	PermitAccess	Default Network Author

3) 展开 Authorization。点击 Authorization Profiles(左侧面板)并点击 Add。

- Name: Posture_Remediation
- Access Type: Access_Accept
- Common Tools:
  - Posture Discovery, Enabled

- Posture Discovery, ACL: ACL-POSTURE-REDIRECT



Authorization Profiles > New Authorization Profile

* Name: Posture_Remediation

Description: Permit Access To Posture And Remediation Services; Redirect Traffic To Client Provisioning And Posture Services.

* Access Type: ACCESS_ACCEPT

▾ Common Tasks

□ DACL Name

□ VLAN

□ Voice Domain Permission

☑ Posture Discovery   ACL: ACL-POSTURE-REDIRECT

□ Centralized Web Authentication

□ Auto Smart Port

▾ Advanced Attributes Settings

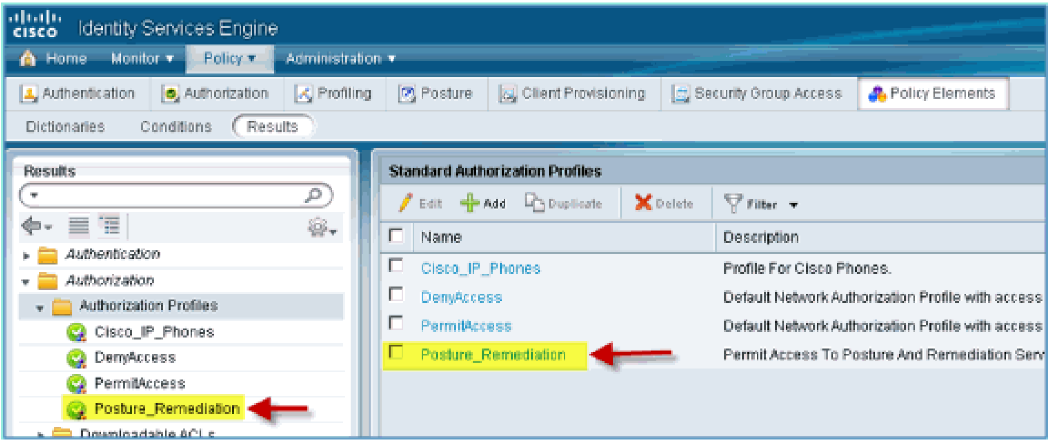
Select an item =

▾ Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL-POSTURE-REDIRECT
cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp
```

4) 点击 Submit 完成配置。

5) 确认新的 Authorization Profile 已经创建完成。



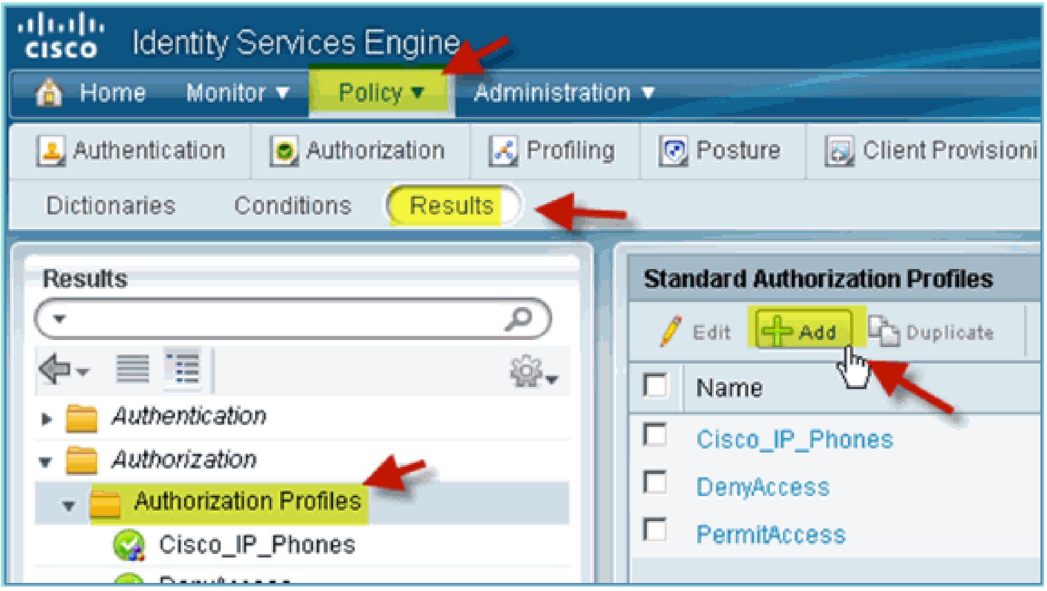
Standard Authorization Profiles

□	Name	Description
□	Cisco_IP_Phones	Profile For Cisco Phones.
□	DenyAccess	Default Network Authorization Profile with access
□	PermitAccess	Default Network Authorization Profile with access
□	Posture_Remediation	Permit Access To Posture And Remediation Serv

- **在 ISE 上为用户 Employee 创建 Authorization Profile**

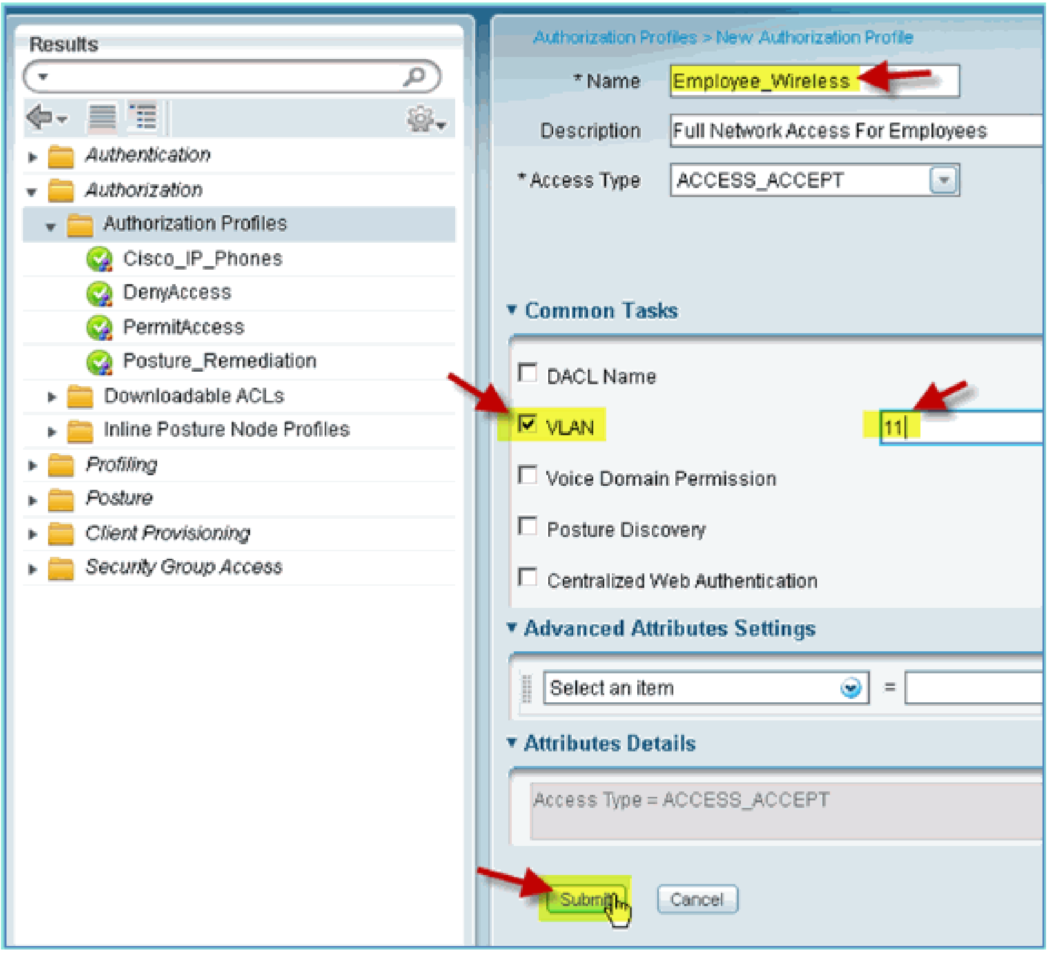
在 ISE 上为用户 Employee 创建一个 Authorization Profile，对其授权和允许访问，并将 Employee 分配到 VLAN 11 上。

1) 在 ISE 上，进入 Policy > Results. 展开 Authorization，然后点击 Authorization Profile，再点击 Add。



2) 在 Employee 的 Authorization Profile 中输入以下数值：

- Name: Employee_Wireless
- Common Tasks:
  - VLAN: Enabled
  - VLAN, sub value 11



* Name: Employee_Wireless

Description: Full Network Access For Employees

* Access Type: ACCESS_ACCEPT

☐ DACL Name

☑ VLAN 11

☐ Voice Domain Permission

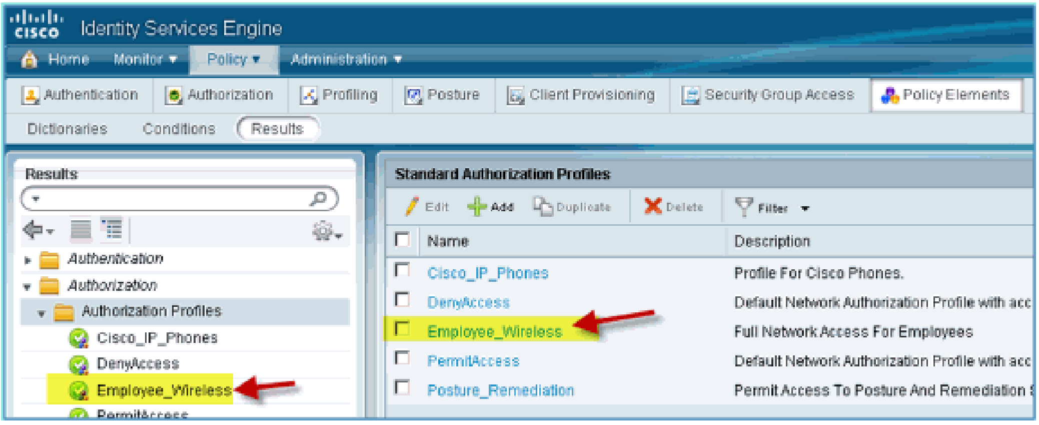
☐ Posture Discovery

☐ Centralized Web Authentication

Access Type = ACCESS_ACCEPT

3) 点击 Submit。

4) 确认 Employee 的 Authorization Profile 完成了创建。

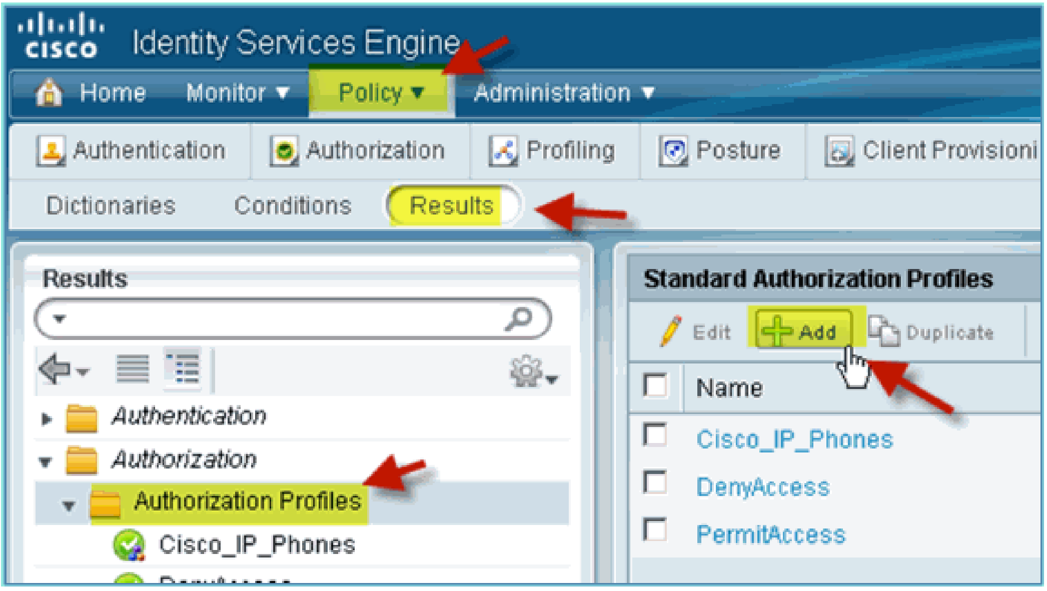


Name	Description
Cisco_IP_Phones	Profile For Cisco Phones.
DenyAccess	Default Network Authorization Profile with acc
Employee_Wireless	Full Network Access For Employees
PermitAccess	Default Network Authorization Profile with acc
Posture_Remediation	Permit Access To Posture And Remediation

- **在 ISE 上为用户 Contractor 创建 Authorization Profile**

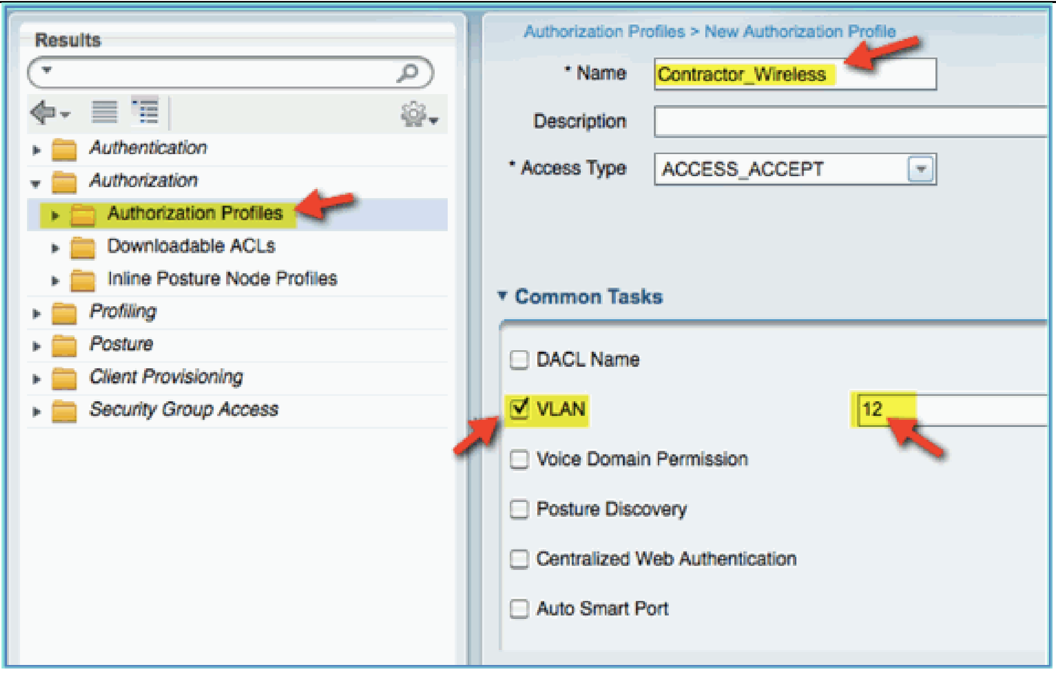
在 ISE 上为用户 Contractor 创建一个 Authorization Profile，对其授权和允许访问，并将 Contractor 分配到 VLAN 11 上。

1) 在 ISE 上，进入 Policy > Results. 展开 Authorization，然后点击 Authorization Profile，再点击 Add.



2) 在 Contractor 的 Authorization Profile 中输入以下数值：

- Name: Contractor_Wireless
- Common Tasks:
  - VLAN: Enabled
  - VLAN, sub value 12



Authorization Profiles > New Authorization Profile

* Name: Contractor_Wireless

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

□ DACL Name

☑ VLAN 12

□ Voice Domain Permission

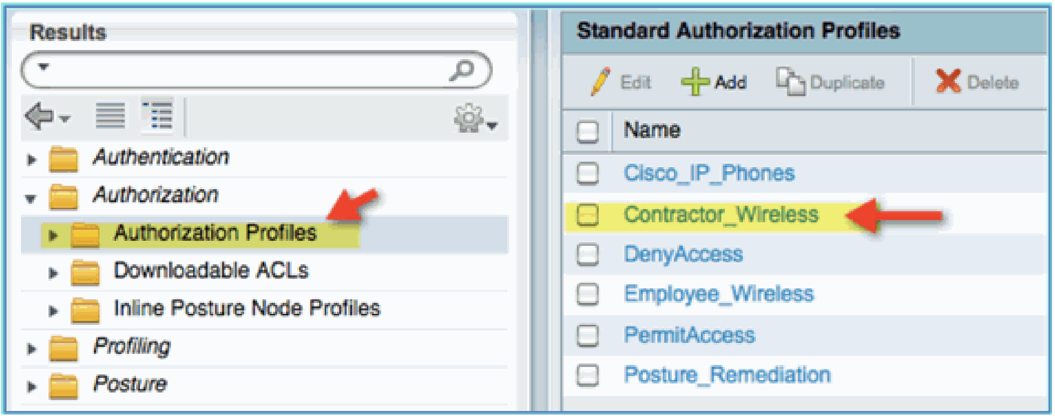
□ Posture Discovery

□ Centralized Web Authentication

□ Auto Smart Port

3) 点击 Submit。

4) 确认 Contractor 的 Authorization Profile 完成了创建。



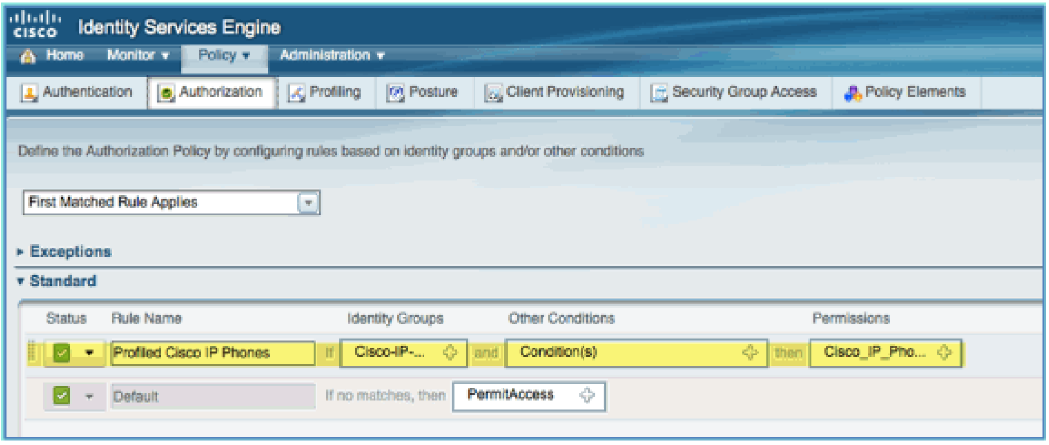
Standard Authorization Profiles

□	Name
□	Cisco_IP_Phones
□	Contractor_Wireless
□	DenyAccess
□	Employee_Wireless
□	PermitAccess
□	Posture_Remediation

- **创建设备检测和识别的授权策略**

当终端设备首次接入到网络中时，ISE 能够得到的设备信息很少，因此需要创建一些策略允许这些未知设备在获得访问权限之前，能够被识别出来。在下面配置中，要创建一个重定向的授权策略，使新接入网络的终端设备会被重定向到 ISE 上进行设备的健康状态检查（由于移动终端设备不支持客户端 Agent 安装，因此只执行设备的识别），终端设备将被重定向到 ISE 的门户页面，并被识别出设备类型。

1) 在 ISE 上，进入 Policy > Authorization。



Define the Authorization Policy by configuring rules based on identity groups and/or other conditions

First Matched Rule Applies

▸ Exceptions

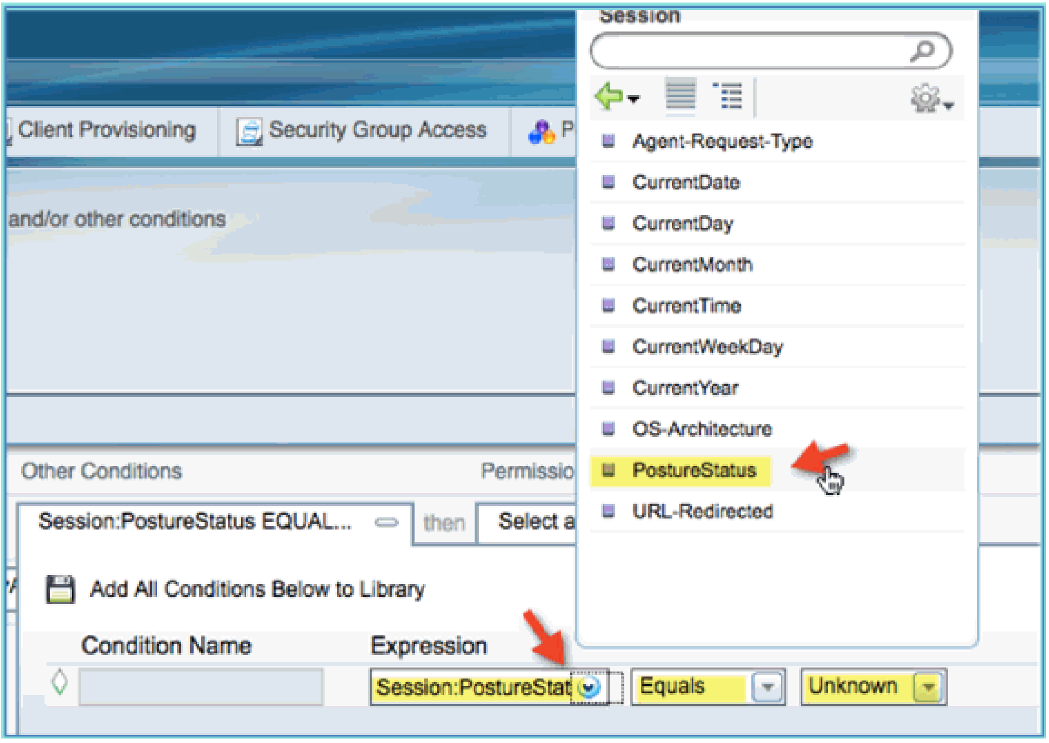
▾ Standard

Status	Rule Name		Identity Groups		Other Conditions		Permissions
☑	Profiled Cisco IP Phones	if	Cisco-IP-...	and	Condition(s)	then	Cisco_IP_Pho...
☑	Default	If no matches, then	PermitAccess				

2) ISE 上预配置了一个策略 Profiled Cisco IP Phones，将其修改为终端设备检查策略。

3) 编辑该策略，输入以下参数：

- Rule Name: Posture_Remediation
- Identity Groups: Any
- Other Conditions > Create New: (Advanced)Session > PostureStatus
- PostureStatus > Equals: Unknown

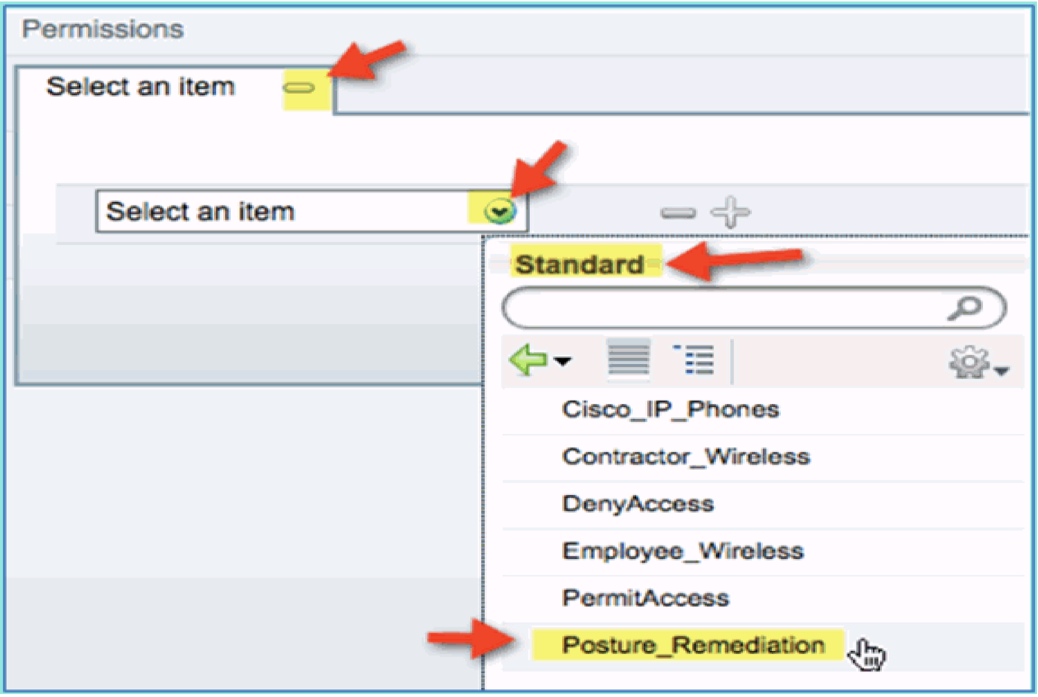


Session:PostureStatus EQUAL...

Condition Name	Expression		
	Session:PostureStat	Equals	Unknown

4) 在 Permission 配置，设置为如下值：

- Permissions > Standard: Posture_Remediation



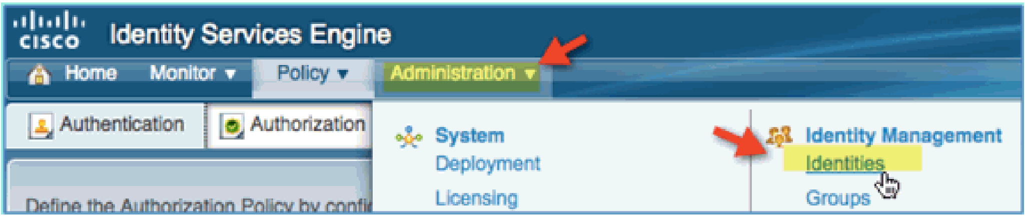
5) 点击 Save 保持配置。

注意：授权策略可以根据需要自定义内容，以方便使用。

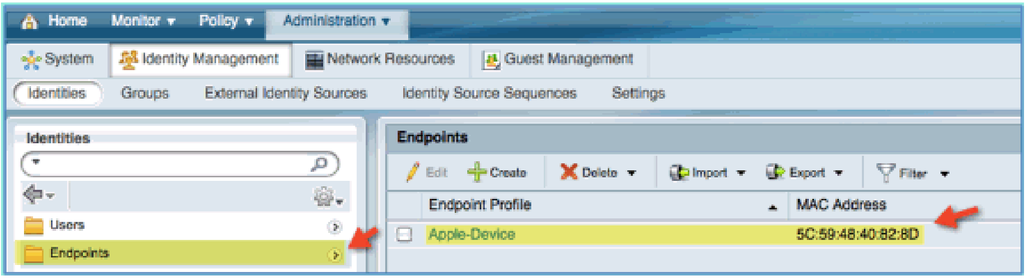
- **测试终端设备的检测修复策略**

下面的操作，简单地显示了 ISE 基于终端检查的策略，识别出新终端设备的类型。

1) 在 ISE 上，进入 Administration > Identity Management > Identities。



2) 点击 Endpoints，查看 ISE 记录的终端设备列表。



	Endpoint Profile	MAC Address
□	Apple-Device	5C:59:48:40:82:8D

3) 刷新终端设备列表，查看有哪些更新的信息。

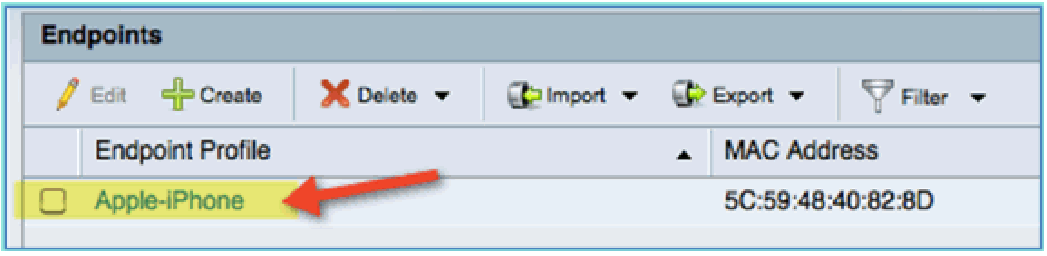
4) 在终端设备上，通过浏览器访问以下 URL：

- URL：http://10.10.10.10

结果页面被重定向到 ISE 的门户页面。接受提示的证书。

5) 在终端设备被重定向后，再次刷新 ISE 终端设备列表。查看发生了哪些改变。之前设备被识别为 Apple-Device，现在应该变为了 Apple-iPhone。改变的原

因是，在访问页面被重定向时，ISE 通过 HTTP Probe 获得了浏览器的 http user-agent 信息。（通常，这需要过一段时间设备列表才会更新）



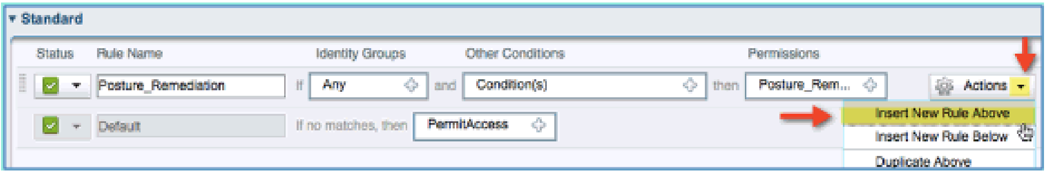
	Endpoint Profile	MAC Address
□	Apple-iPhone	5C:59:48:40:82:8D

- **对应不同访问的授权策略**

完成终端类型的检测测试后，接下来创建对应不同的用户 Employee 和 Contractor 的访问的授权策略，为指定用户分配不同的 VLAN。

1) 在 ISE 上，进入 Policy > Authorization。

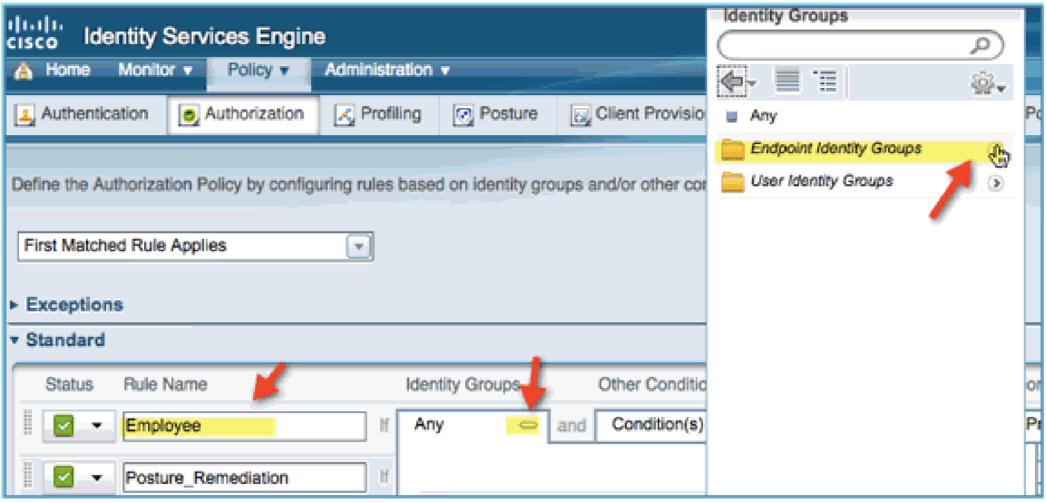
2) 点击 Action，插入一条位于 Posture_Remediation 策略上面的授权规则。



Status	Rule Name		Identity Groups		Other Conditions		Permissions
☑	Posture_Remediation	if	Any	and	Condition(s)	then	Posture_Rem...
☑	Default				If no matches, then		PermitAccess

3) 在这条策略中输入以下内容：

- Rule Name: Employee
- Identity Group(expand): Endpoint Identity Groups

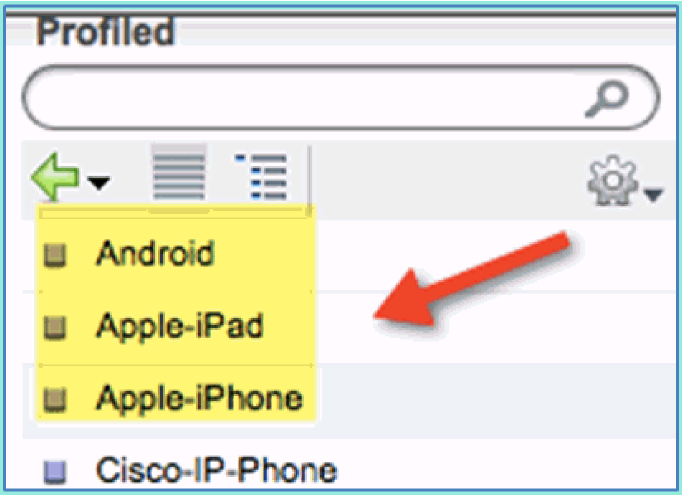


Define the Authorization Policy by configuring rules based on identity groups and/or other cor

First Matched Rule Applies

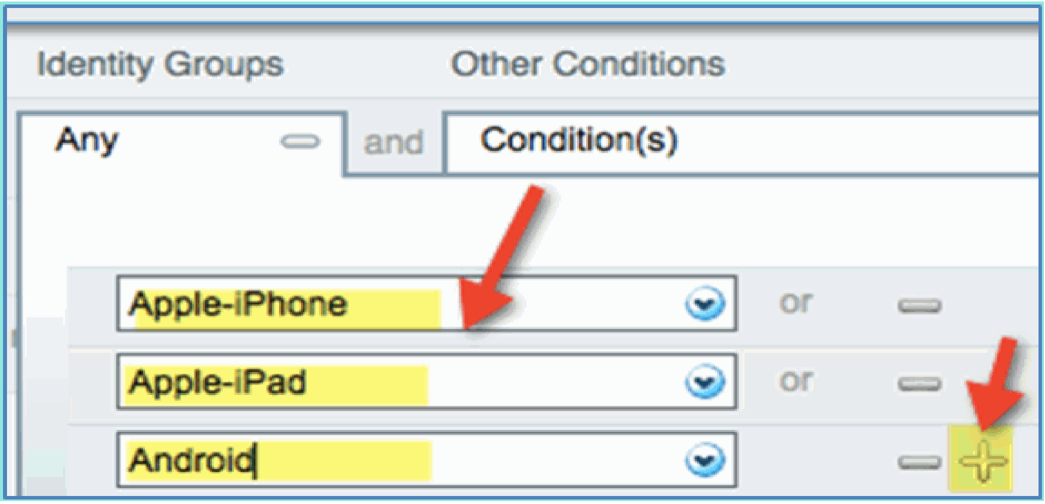
Status	Rule Name		Identity Groups		Other Conditic
☑	Employee	If	Any	and	Condition(s)
☑	Posture_Remediation	If			

- Endpoint Identity Groups: Profiled
- Profiled: Android, Apple-iPad or Apple-iPhone



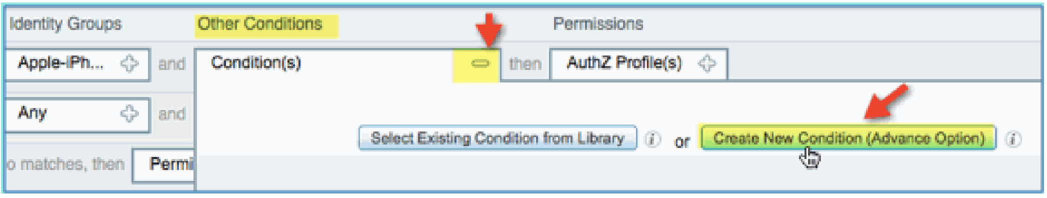
4) 要添加其他设备类型，点击+然后增加更多的设备(如果需要)：

- o Endpoint Identity Groups: Profiled
- o Profiled: Android, Apple-iPad or Apple-iPhone

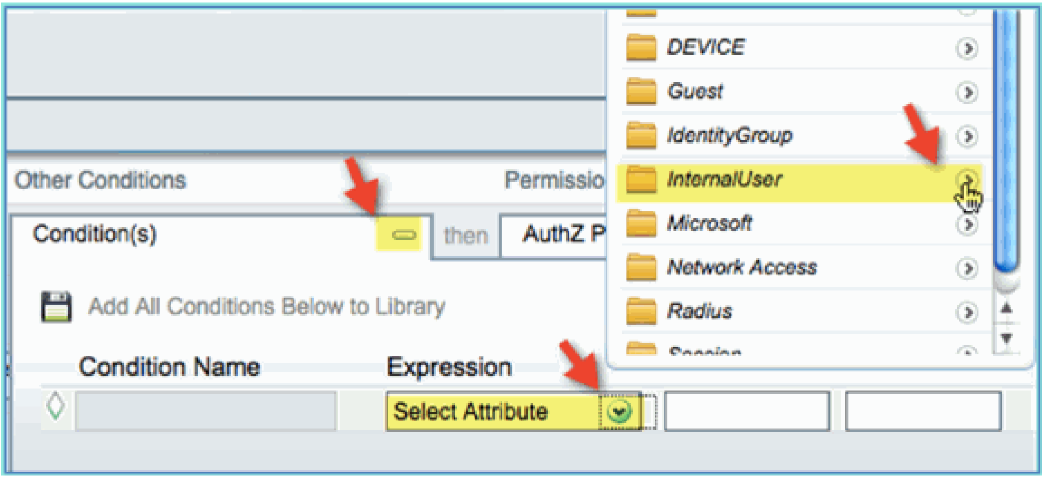


5) 设定以下允许访问权限：

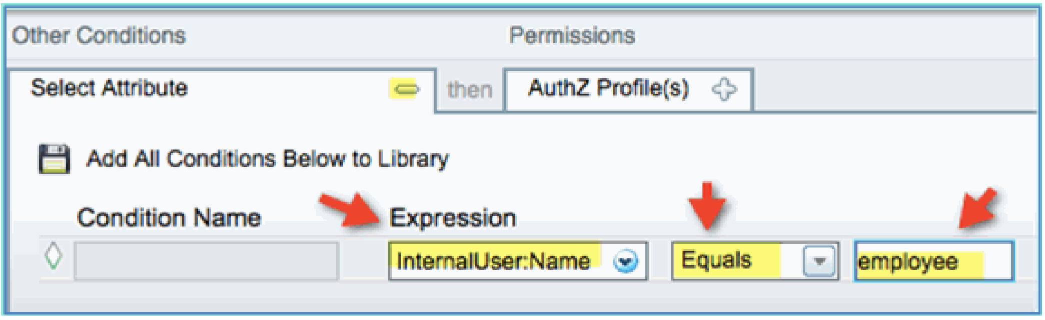
- o Other Conditions(expand): Create New Condition(Advanced Option)



- o Condition > Expression(from list): InternalUser > Name



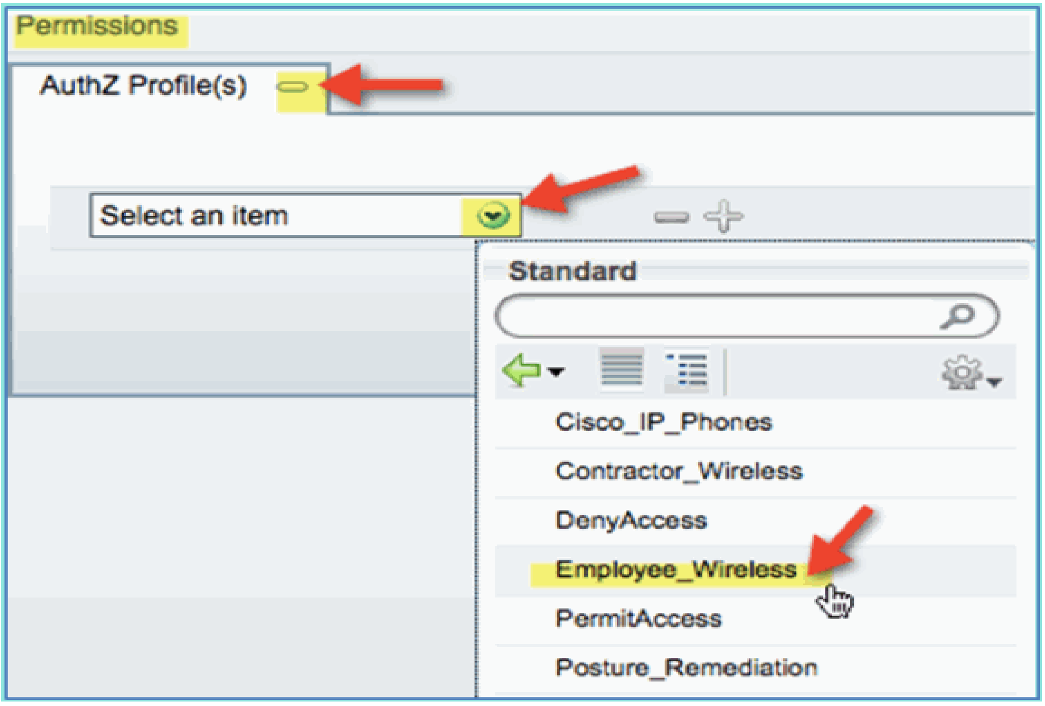
- InternalUser > Name: employee



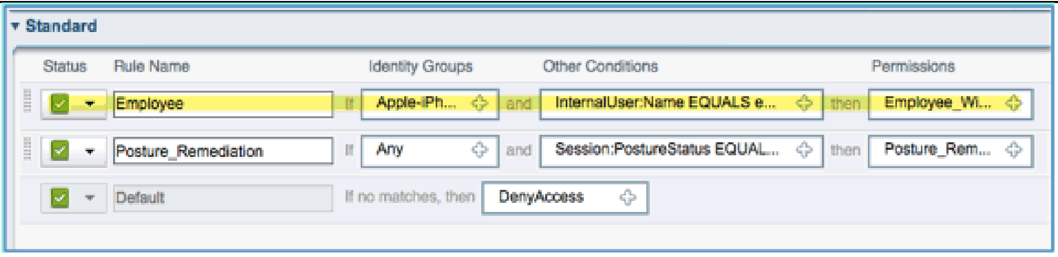
InternalUser:Name | Equals | employee

6) 增加访问权限的授权描述：

- Permissions > Profiles > Standard: Employee_Wireless



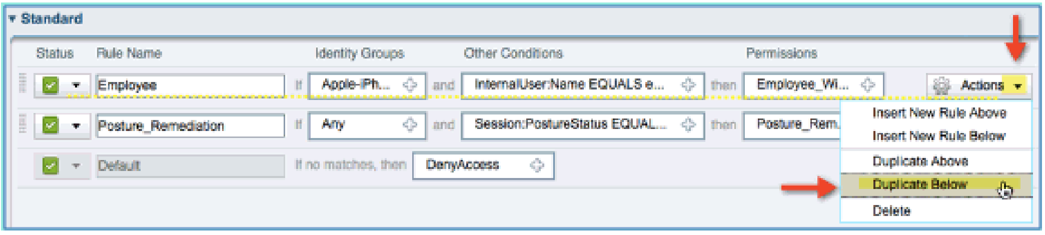
7) 点击 Save。确认策略已经完成添加。



Standard

Status	Rule Name		Identity Groups		Other Conditions		Permissions
☑	Employee	If	Apple-iPh...	and	InternalUser:Name EQUALS e...	then	Employee_Wi...
☑	Posture_Remediation	If	Any	and	Session:PostureStatus EQUAL...	then	Posture_Rem...
☑	Default	If no matches, then	DenyAccess				

8) 继续添加针对用户 Contractor 的策略。通过复制前面创建的 Employee 的策略，加快创建过程。进入 Employee Policy > Actions，点击 Duplicate Below。

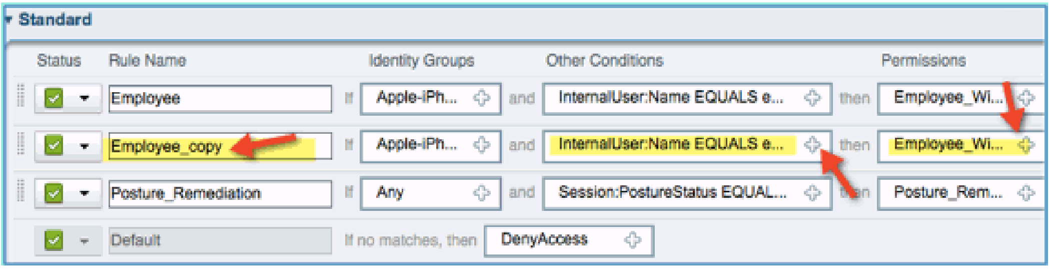


Standard

Status	Rule Name		Identity Groups		Other Conditions		Permissions	
☑	Employee	If	Apple-iPh...	and	InternalUser:Name EQUALS e...	then	Employee_Wi...	Actions
☑	Posture_Remediation	If	Any	and	Session:PostureStatus EQUAL...	then	Posture_Rem...	
☑	Default	If no matches, then	DenyAccess					

9) 在复制的策略中，编辑以下内容：

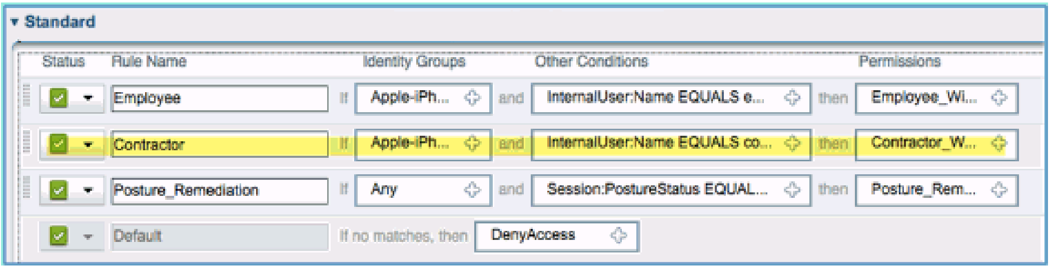
- Rule Name: Contractor
- Other Conditions > InternalUser > Name: contractor
- Permissions: Contractor_Wireless



Standard

Status	Rule Name		Identity Groups		Other Conditions		Permissions
☑	Employee	If	Apple-iPh...	and	InternalUser:Name EQUALS e...	then	Employee_Wi...
☑	Employee_copy	If	Apple-iPh...	and	InternalUser:Name EQUALS e...	then	Employee_Wi...
☑	Posture_Remediation	If	Any	and	Session:PostureStatus EQUAL...	then	Posture_Rem...
☑	Default	If no matches, then	DenyAccess				

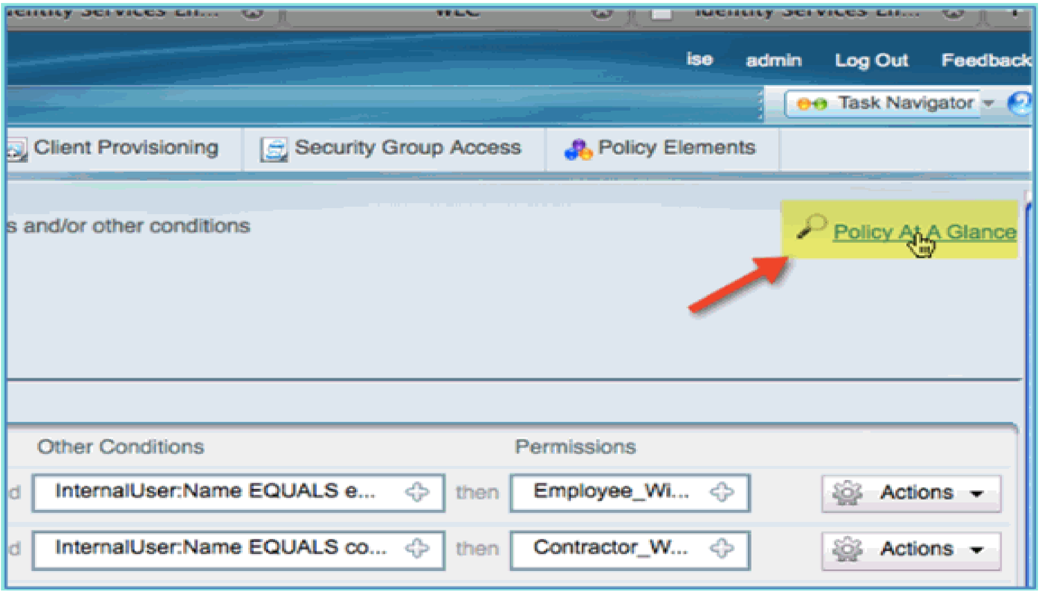
10) 点击 Save。确认复制的策略已经被编辑完成。



Standard

Status	Rule Name		Identity Groups		Other Conditions		Permissions
☑	Employee	If	Apple-iPh...	and	InternalUser:Name EQUALS e...	then	Employee_Wi...
☑	Contractor	If	Apple-iPh...	and	InternalUser:Name EQUALS co...	then	Contractor_W...
☑	Posture_Remediation	If	Any	and	Session:PostureStatus EQUAL...	then	Posture_Rem...
☑	Default	If no matches, then	DenyAccess				

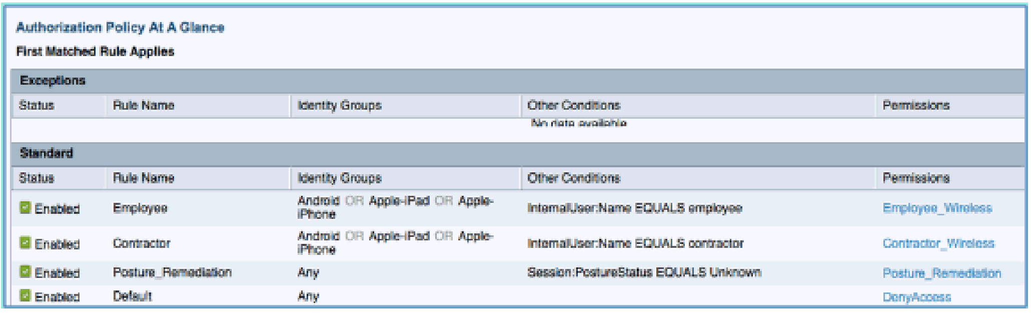
11) 要预览策略，点击 Policy-at-a-Glance。



InternalUser:Name EQUALS e... then Employee_Wi...

InternalUser:Name EQUALS co... then Contractor_W...

通过 Policy-at-a-Glance 视图，查看完整的策略内容。


Authorization Policy At A Glance

First Matched Rule Applies

Exceptions

Status	Rule Name	Identity Groups	Other Conditions	Permissions
			No data available	

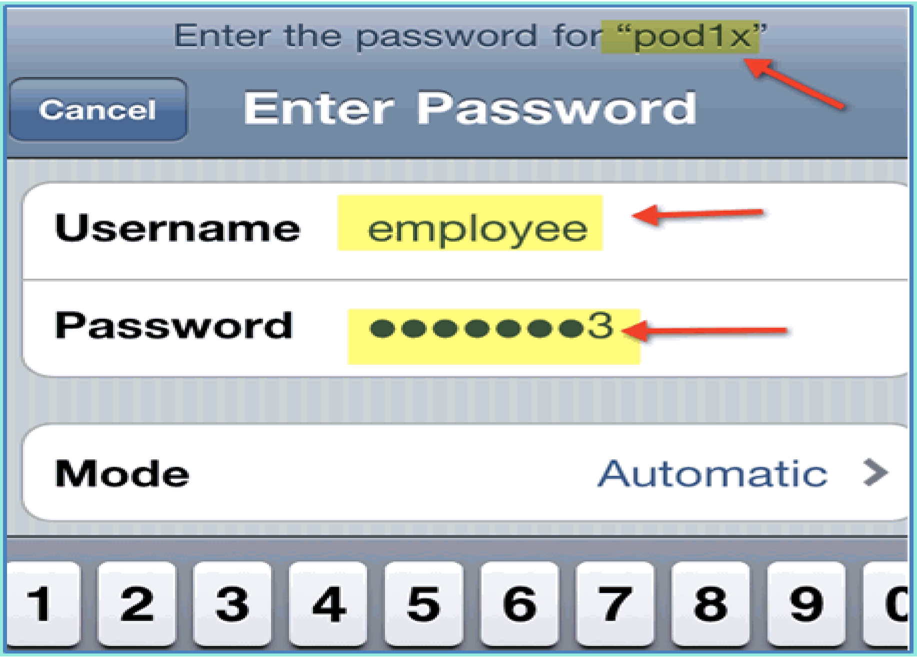
Standard

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

- **测试不同访问的策略变更(CoA)**

完成了对不同访问的授权描述和授权策略的配置后，下面对其进行测试。去连接启用身份验证的 WLAN，Employee 被分配到 employee 的 VLAN，Contractor 被分配到 contractor 的 VLAN。下一例子测试 iPhone/iPad。

1) 通过移动终端设备连接到 WLAN（pod1x），用下面信息做身份验证：
   - Username: employee
   - Password: XXXXX



Enter the password for "pod1x"

Cancel

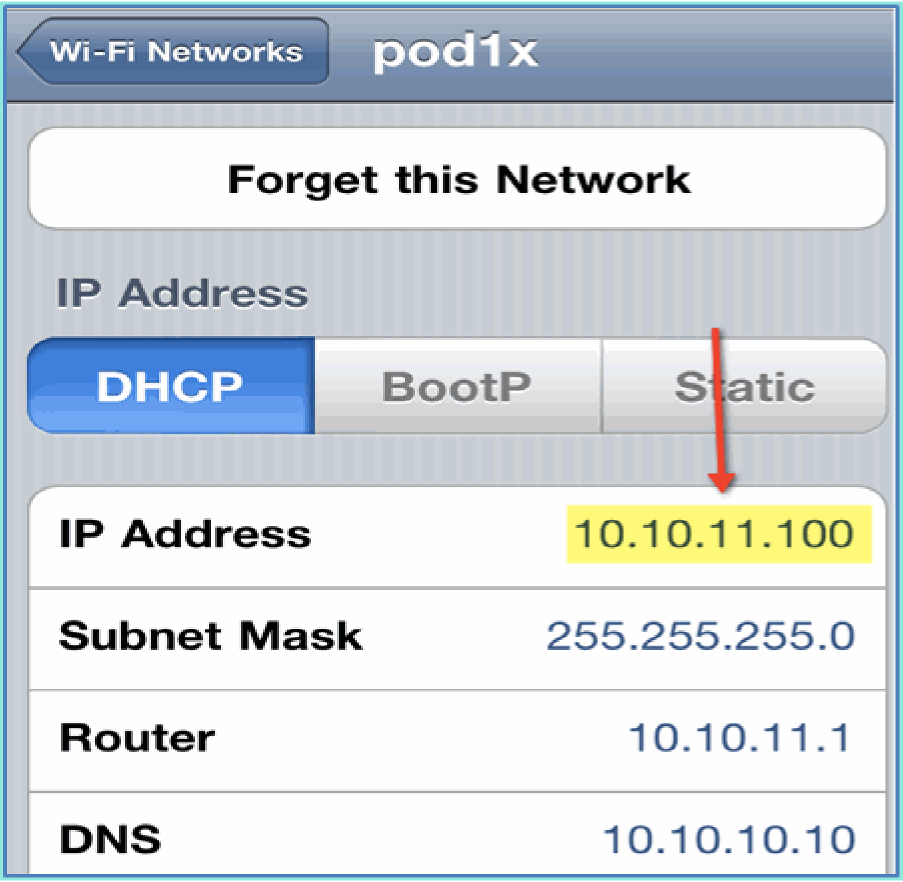
Enter Password

Username employee

Password ●●●●●●●3

Mode Automatic

2) 点击 Join。确认 employee 被分配到了 VLAN11（Employee VLAN）.



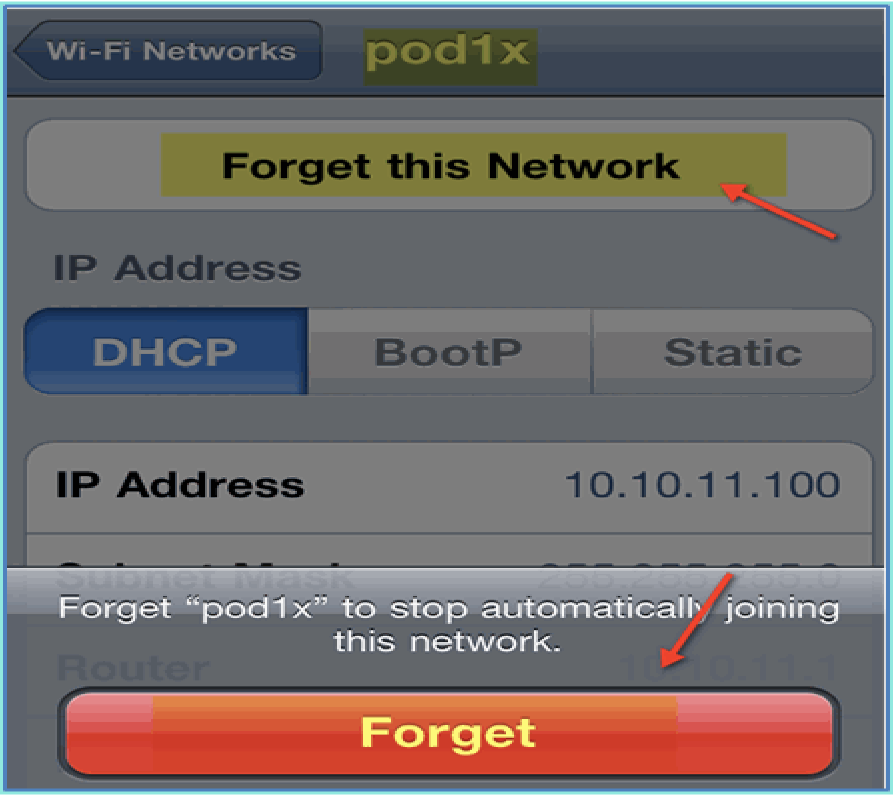
IP Address 10.10.11.100

Subnet Mask 255.255.255.0

Router 10.10.11.1

DNS 10.10.10.10

3) 点击 Forget this Network 断开 WLAN 的连接，并点击 Forget 确认。



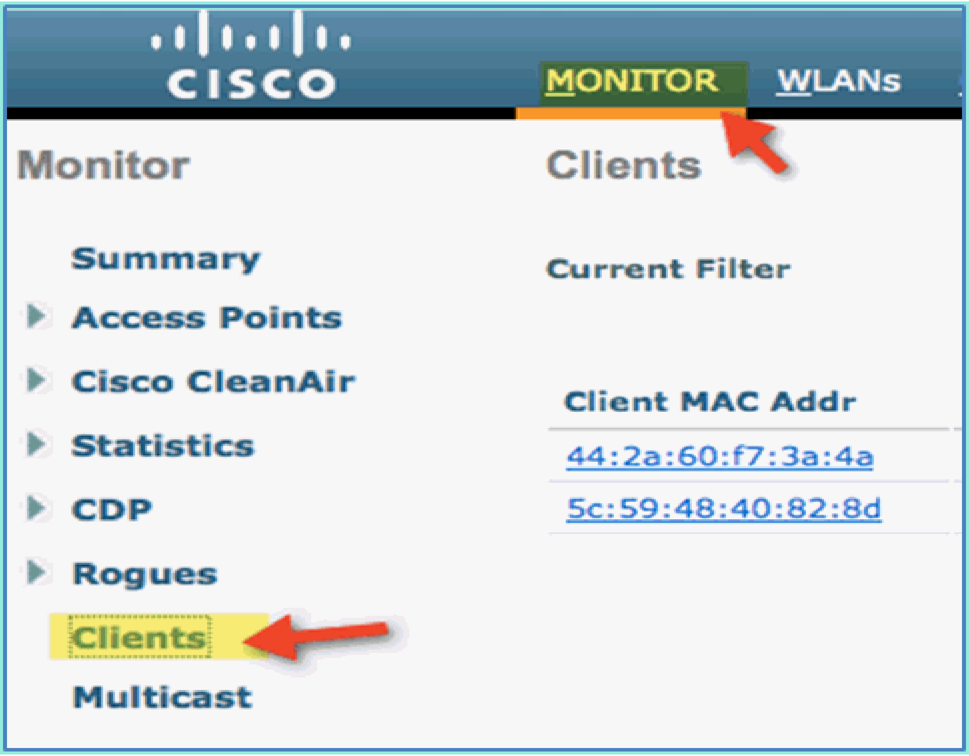
IP Address 10.10.11.100

Subnet Mask 255.255.255.0

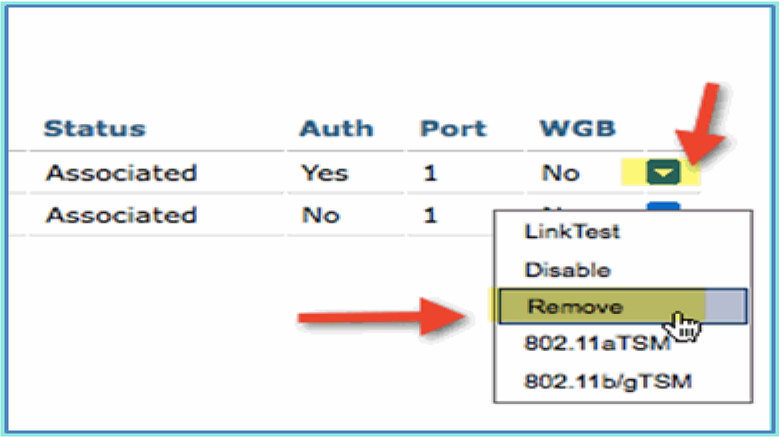
Router 10.10.11.1

Forget “pod1x” to stop automatically joining this network.

4) 在 WLC 管理界面，删除客户端的连接。进入 Monitor > Clients > MAC address，然后点击 Remove.



Client MAC Addr
44:2a:60:f7:3a:4a
5c:59:48:40:82:8d



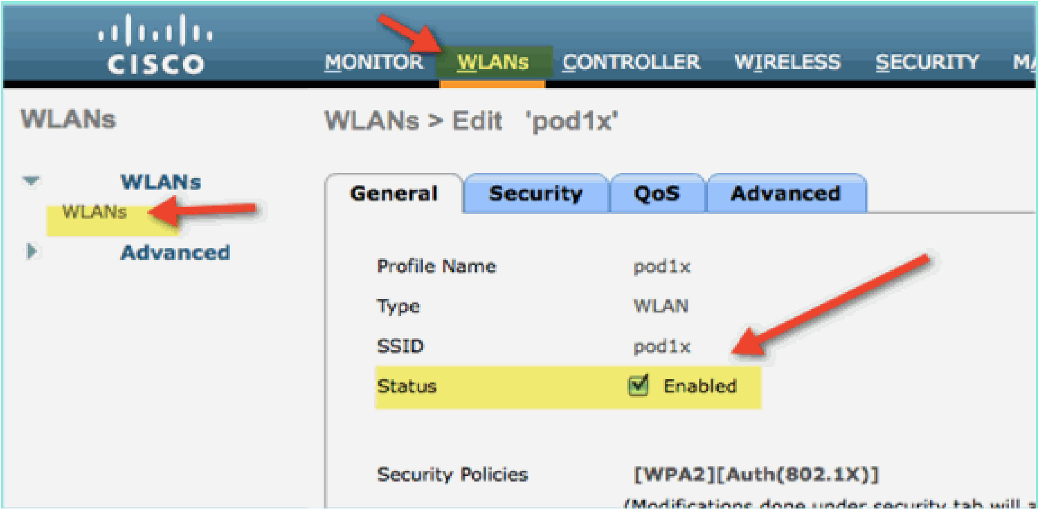
Status	Auth	Port	WGB
Associated	Yes	1	No
Associated	No	1	

5) 另外清除客户端连接的方式，是先关闭/启用 WLAN。

   a. 进入 WLC > WLANs > WLAN，然后点击 WLAN 进行编辑。

   b. 取消选择 Enabled > Apply（关闭 WLAN）

   c. 选择 Enabled > Apply（打开 WLAN）

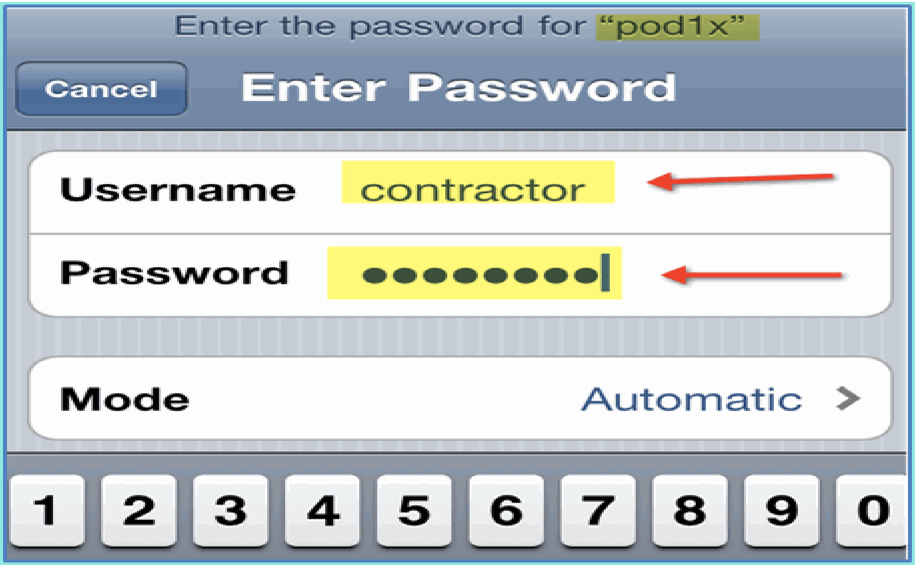


WLANs > Edit 'pod1x'

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)]
	(Modifications done under security tab will a

6) 在移动终端上，使用下面的认证信息，重新连接相同的 WLAN：

- Username: contractor
- Password: XXXXX



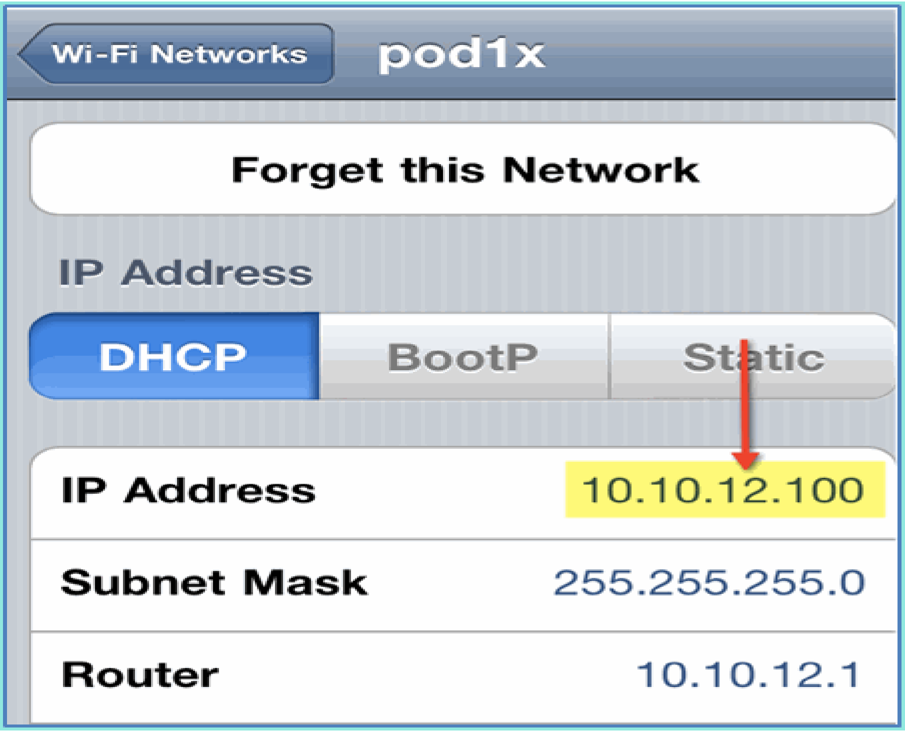
Enter the password for "pod1x"

Username contractor

Password ●●●●●●●●●●

Mode Automatic >

7) 点击 Join。确认用户 contractor 被分配给了 VLAN 12（Contractor 和 Guest VLAN）。

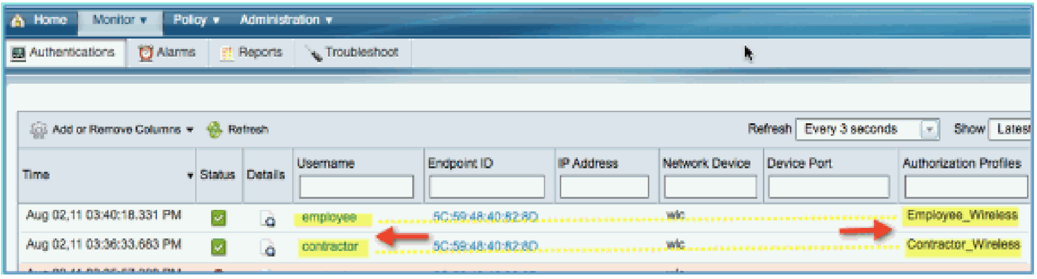


IP Address 10.10.12.100

Subnet Mask 255.255.255.0

Router 10.10.12.1

8) 在 ISE 上查看实施的认证记录，进入 Monitor > Authorizations。查看用户 employee 和 contractor 获得了不同的认证描述，分别为 Employee_Wireless 和 Contractor_Wireless，分配到了不同的 VLAN 中。



Refresh Every 3 seconds Show Latest

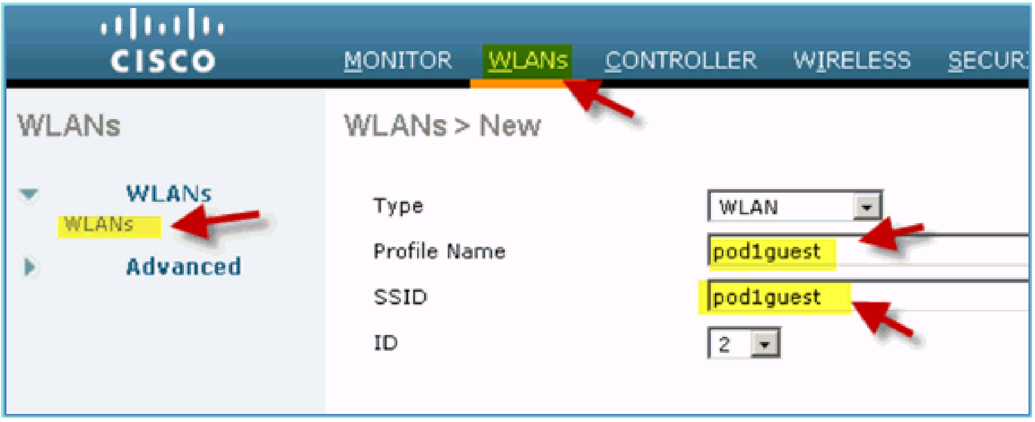
Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Aug 02,11 03:40:18.331 PM	✓		employee	5C:59:48:40:82:8D		wlc		Employee_Wireless
Aug 02,11 03:36:33.683 PM	✓		contractor	5C:59:48:40:82:8D		wlc		Contractor_Wireless

8. ISE 访客服务

- **在 WLC 上创建 Guest WLAN**

通过以下步骤创建一个 Guest WLAN，用于访客来接入网络时，通过 ISE 的门户页面进行认证。

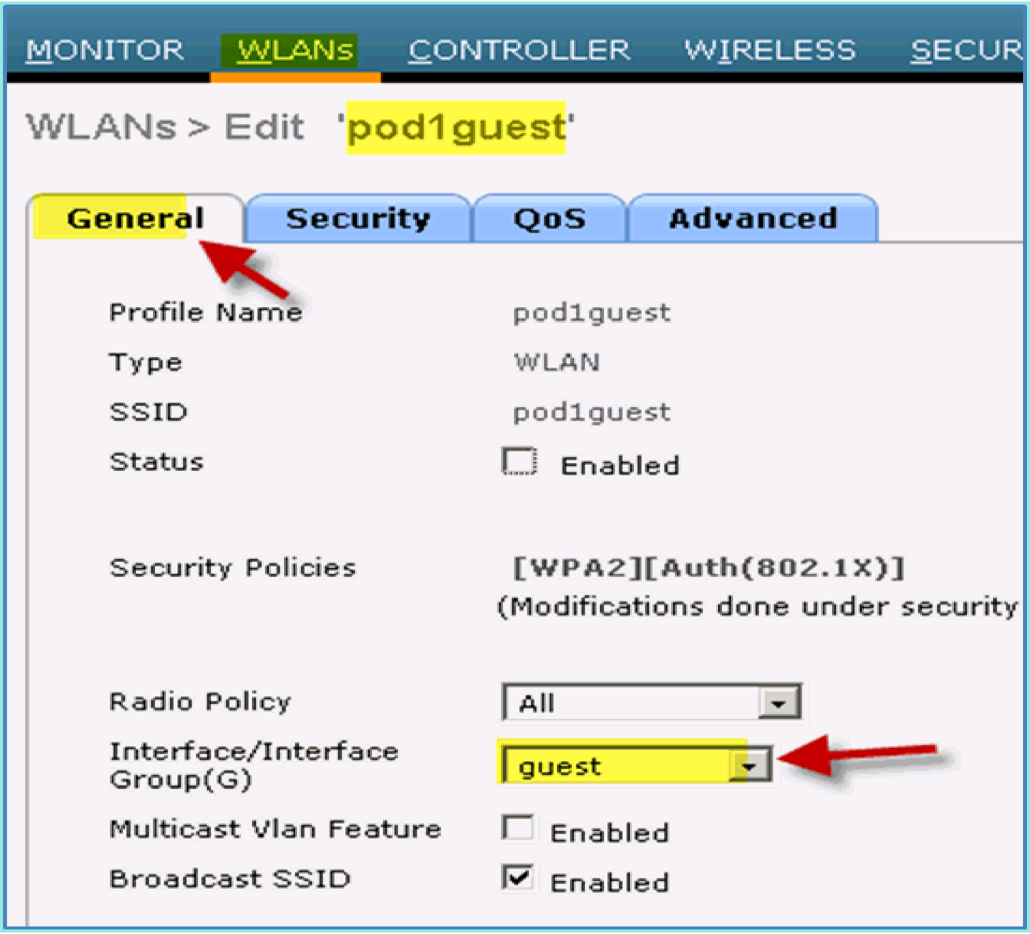
1) 在 WLC 上，进入 WLAN > WLANs > Add New.
2) 输入以下信息创建 Guest WLAN：
   - o Profile Name: pod1guest
   - o SSID: pod1guest



WLANs > New

Type: WLAN
Profile Name: pod1guest
SSID: pod1guest
ID: 2

3) 点击 Apply。
4) 在 guest WLAN > General 下，输入以下配置：
   - o Status: Disabled
   - o Interface/Interface Group: Guest



WLANs > Edit 'pod1guest'

Profile Name pod1guest

Type WLAN

SSID pod1guest

Status □ Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security

Radio Policy All

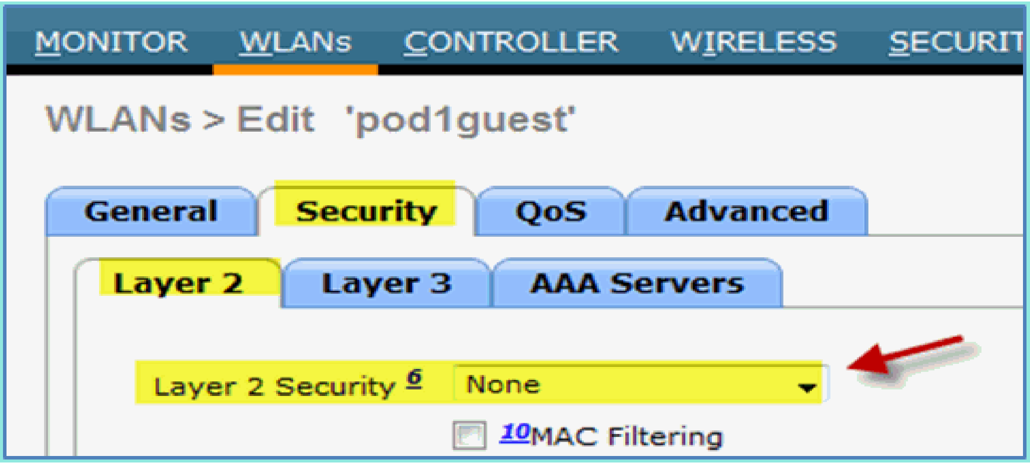
Interface/Interface Group(G) guest

Multicast Vlan Feature □ Enabled

Broadcast SSID ☑ Enabled

5) 进入 WLAN > Security > Layer2，输入以下配置：

- Layer2 Security: None



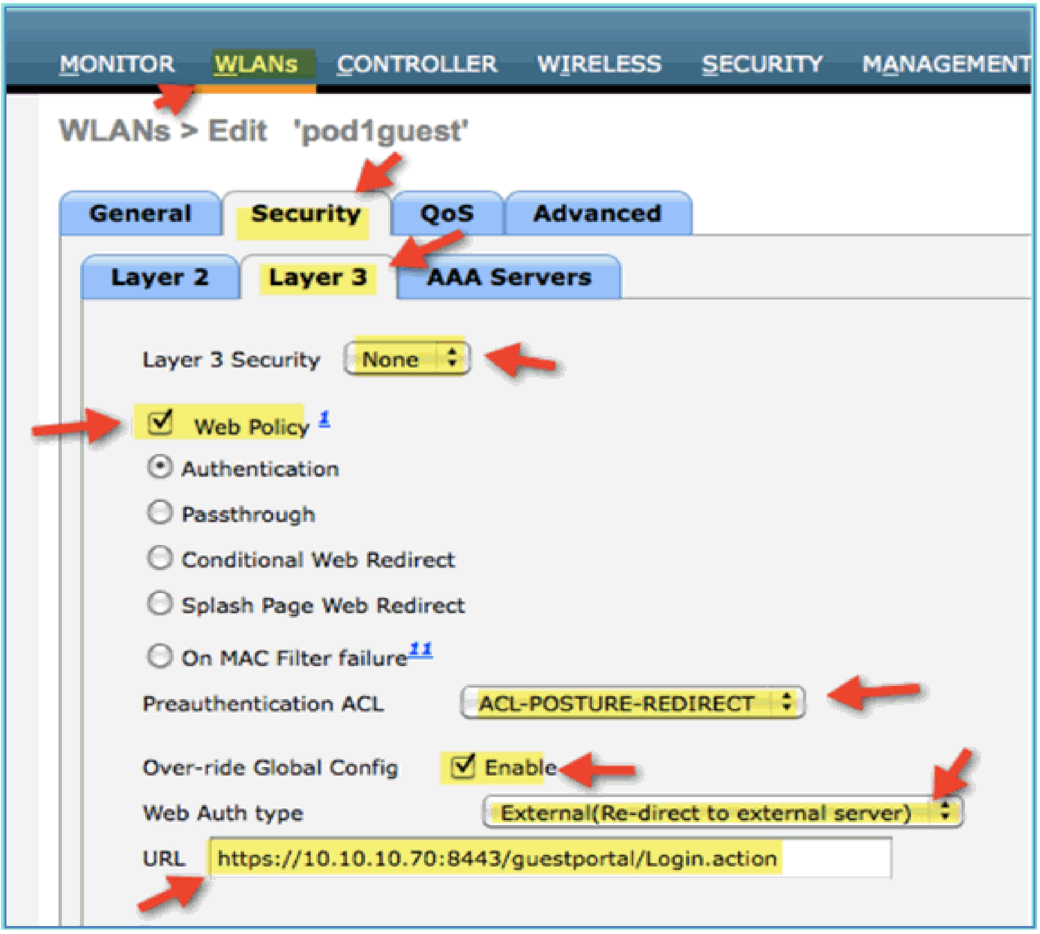
WLANs > Edit 'pod1guest'

Layer 2 Security 6 None

□ 10MAC Filtering

6) 进入 WLAN > Security > Layer3，输入以下配置：

- Layer3 Security: None
- Web Policy: Enabled
- Web Policy sub value: Authentication
- Preauthentication ACL: ACL-POSTURE-REDIRECT
- Web Auth type: External(Re-direct to external server)
- URL: https://10.10.10.70:8443/guestportal/Login.action



WLANs > Edit 'pod1guest'

Layer 3 Security None

☑ Web Policy [1]

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[11]

Preauthentication ACL ACL-POSTURE-REDIRECT

Over-ride Global Config ☑ Enable

Web Auth type External(Re-direct to external server)

URL https://10.10.10.70:8443/guestportal/Login.action

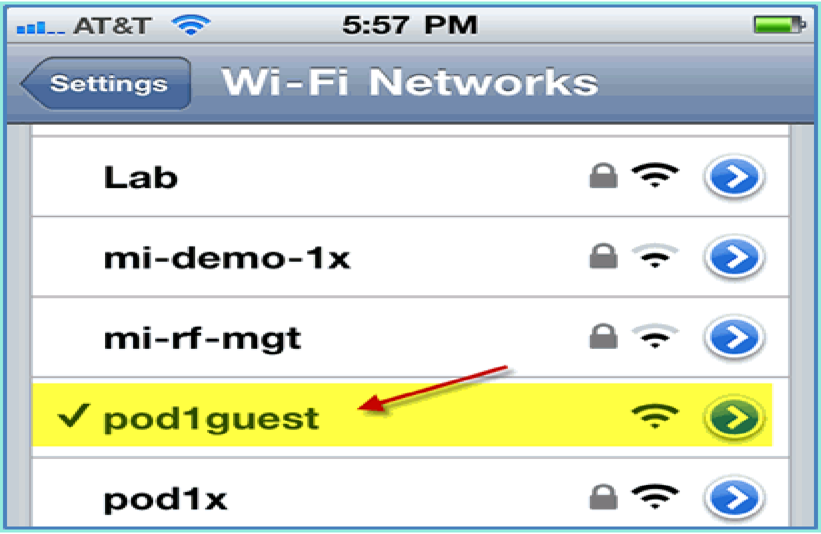
7) 点击 Apply。

8) 点击 Save Configuration 保存 WLC 的配置。

- **测试 Guest WLAN 和 Guest 门户页面**

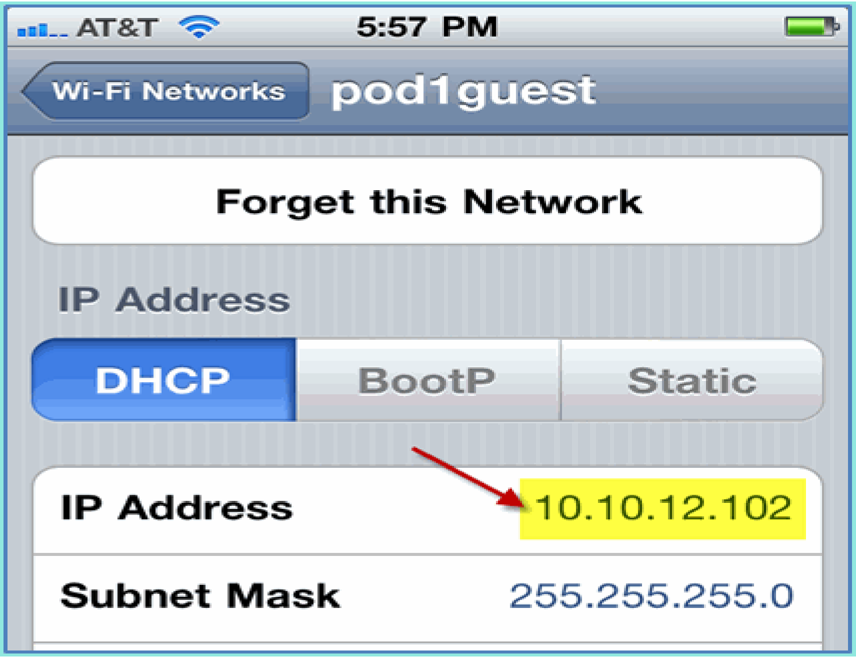
通过下面步骤验证 Guest WLAN 的配置，期望结果是重定向到 ISE 的 Guest 门户页面。

1) 在 iPhone 设备上，进入 Wi-Fi Networks > Enable，并选择连接 pod1guest。



2) 在 iPhone 连接 pod1guest 成功后，获得了 Guest VLAN 的 IP 地址

（10.10.12.0/24）。


AT&T 5:57 PM

Wi-Fi Networks pod1guest

Forget this Network

IP Address

DHCP BootP Static

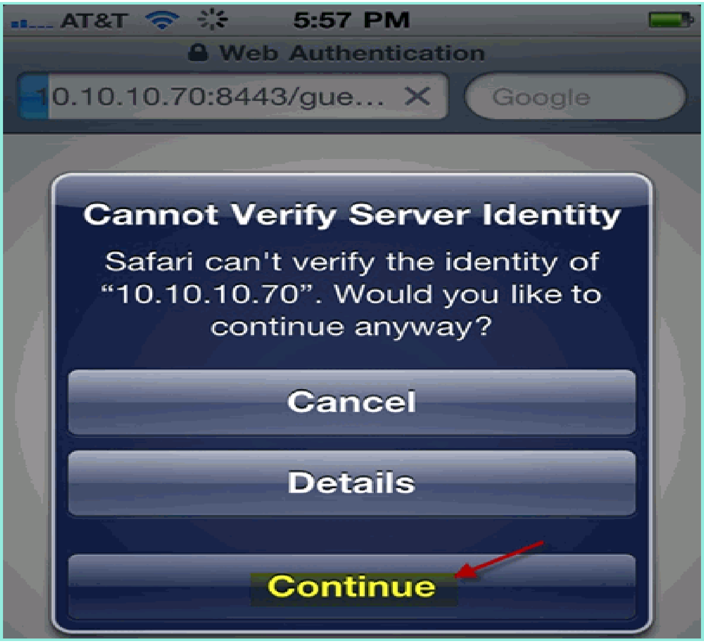
IP Address 10.10.12.102

Subnet Mask 255.255.255.0

3) 在 iPhone 上打开 Safari 浏览器，并访问以下 URL，页面被重定向到 ISE 的 Gueest 门户页面。

- URL：http://10.10.10.10

4) 在弹出的服务器证书验证窗口上，点击 Continue，直到访问到 ISE 的 Guest 门户页面。


AT&T 5:57 PM

Web Authentication

10.10.10.70:8443/gue... Google

Cannot Verify Server Identity

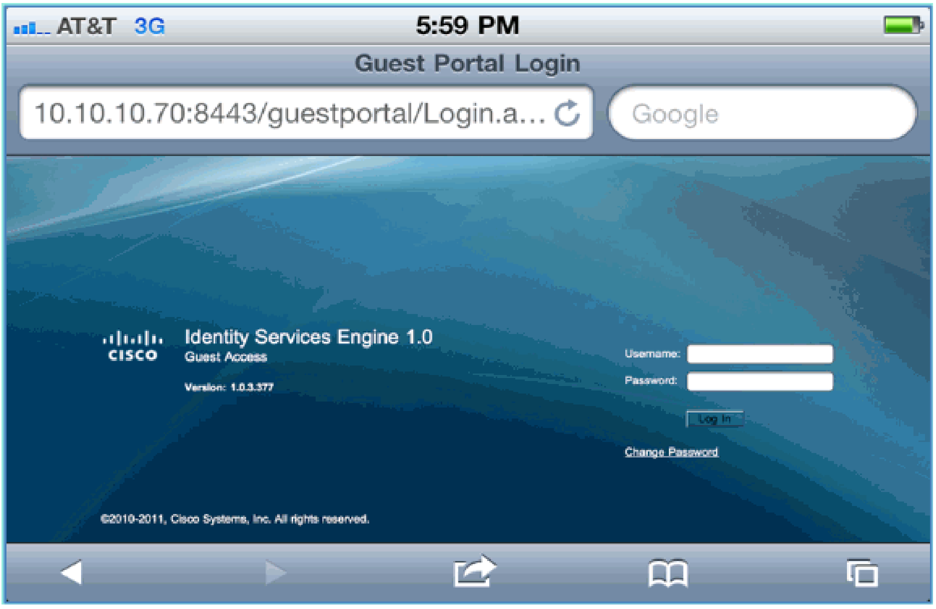
Safari can't verify the identity of "10.10.10.70". Would you like to continue anyway?

Cancel

Details

Continue

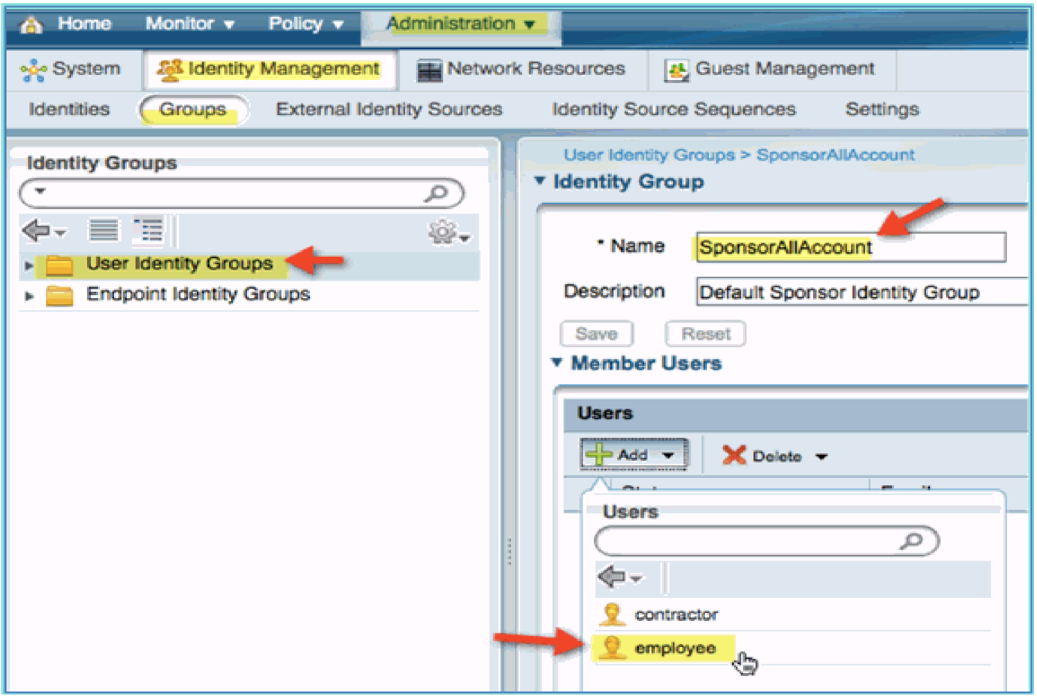
下面的截屏显示了 Guest 的门户页面。这表明 WLAN 和 ISE 的 Guest 门户配置都已经生效了。


AT&T 3G
5:59 PM
Guest Portal Login
10.10.10.70:8443/guestportal/Login.a…
Google
Identity Services Engine 1.0
Guest Access
Version: 1.0.3.377
Username:
Password:
Log In
Change Password
©2010-2011, Cisco Systems, Inc. All rights reserved.

- **ISE 无线访客服务配置**

通过 ISE 配置允许访客获取接待人 Sponsor 提供临时的网络访问权限。下面配置步骤，在 ISE 上增加访客授权策略，允许 ISE 内部用户或 AD 域的用户为访客创建临时访问帐号。ISE 还可配置接待人查看访客的密码（可选项），这样做的目的是为了方便测试。

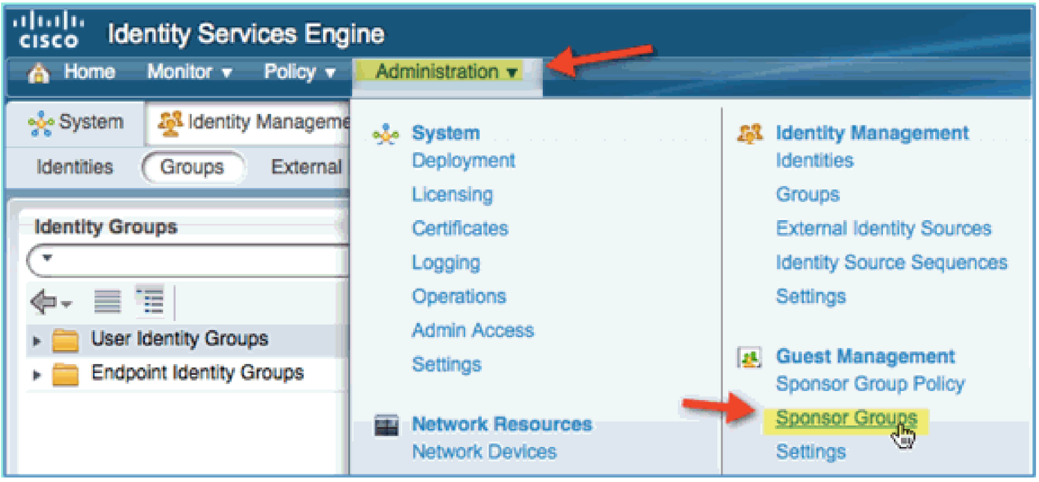
1) 在 ISE 上将用户 employee 加入到组 SponsorAllAccount 中。这里有不同的方法来完成：直接编辑 Group 添加某个用户，或者编辑用户，将其分配到某个组。进入 Administration > Identity Management > Groups > User Identity Groups。点击 SponsorAllAccount，然后增加用户 employee。



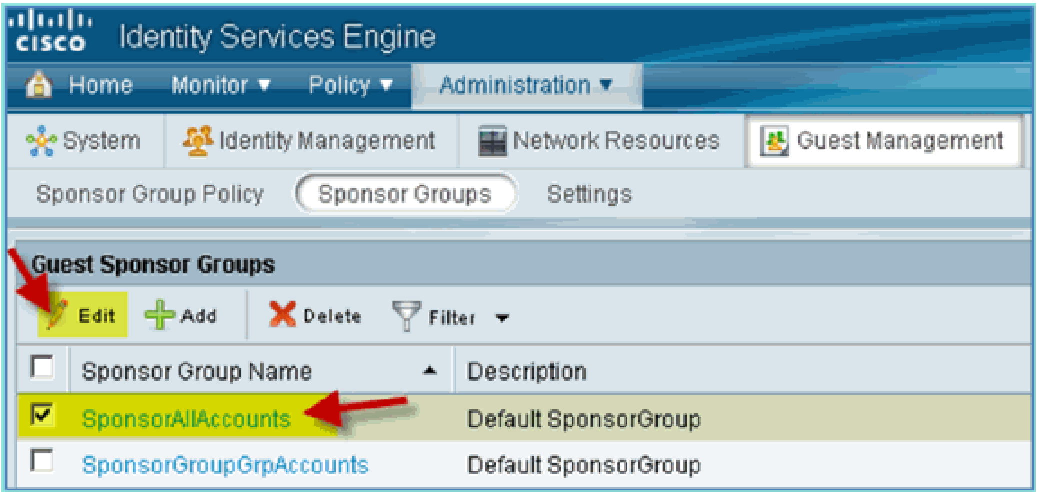
* Name: SponsorAllAccount

Description: Default Sponsor Identity Group

2) 进入 Administration > Guest Management > Sponsor Groups。



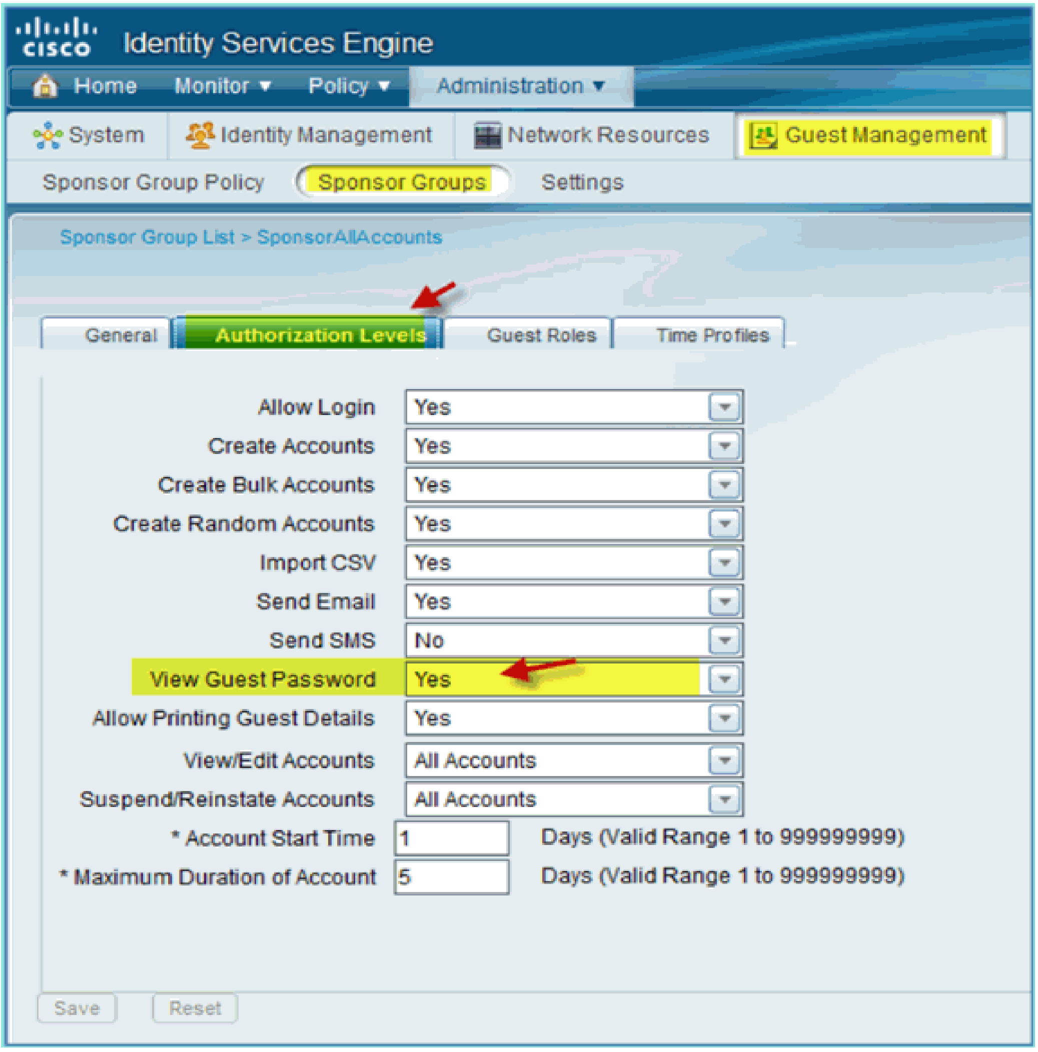
3) 选中 SponsorAllAccounts，点击 Edit。



	Sponsor Group Name	Description
☑	SponsorAllAccounts	Default SponsorGroup
□	SponsorGroupGrpAccounts	Default SponsorGroup

4) 选择 Authorization Levels，并设置以下选项：

- View Guest Password: Yes



Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

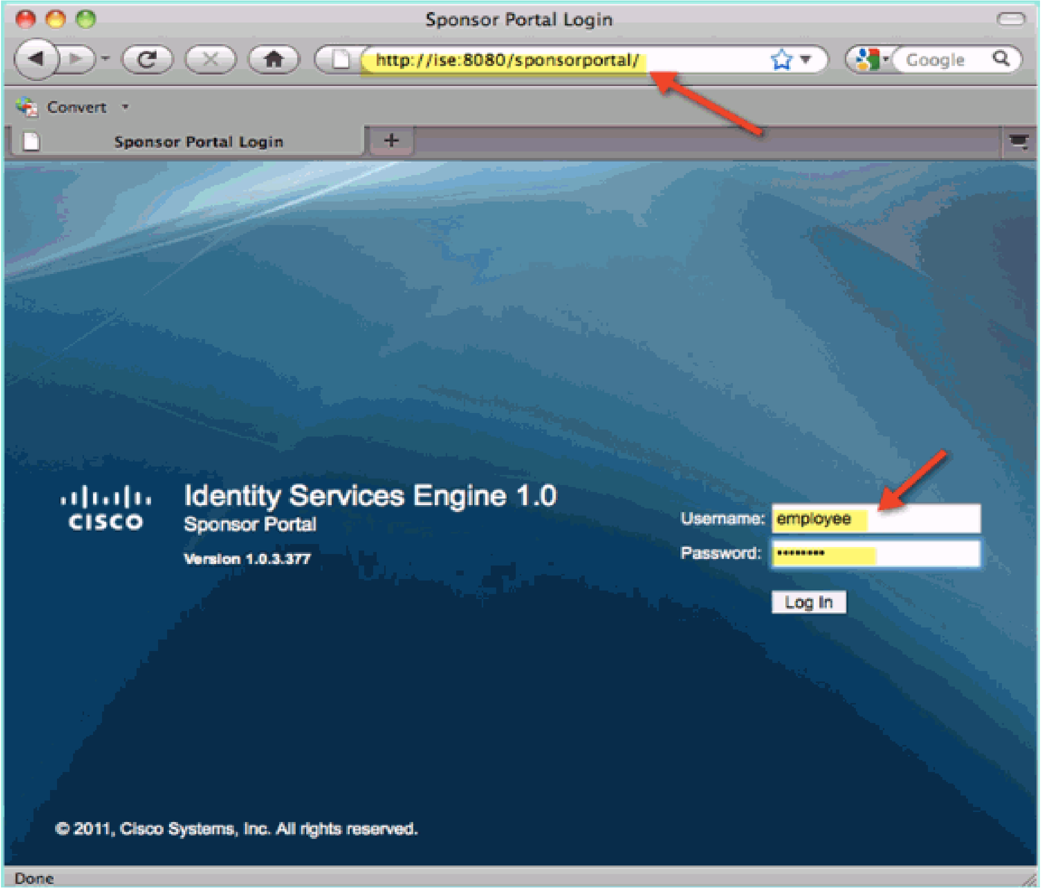
5) 点击 Save，保持所有配置。

- **接待人创建访客帐号**

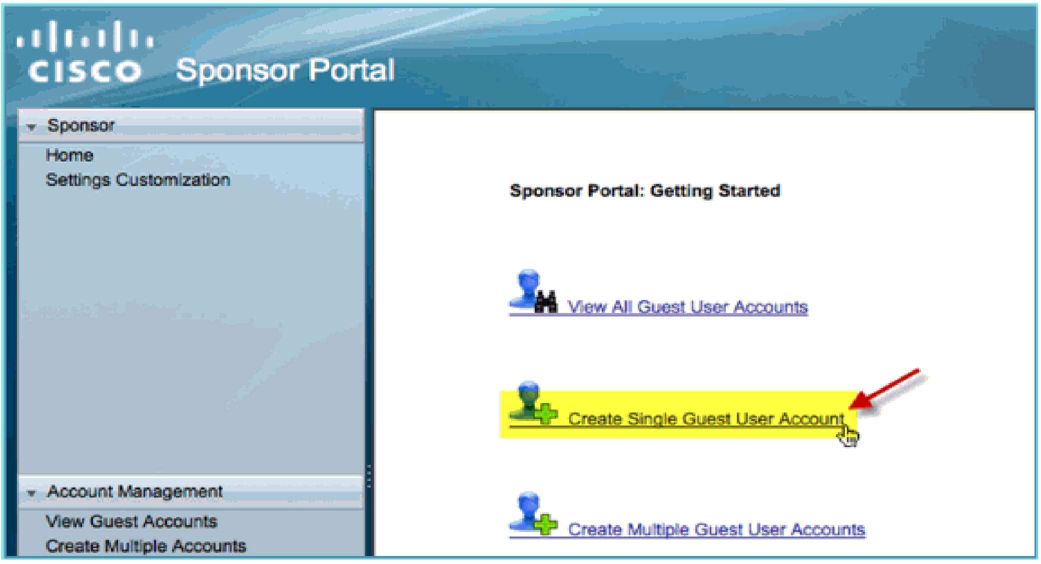
前面的步骤配置了访客的策略和组别，并为 AD 域的用户分配权限，允许其创建临时访客。

1) 通过浏览器访问 URL：http://<ise ip>:8080/sponsorportal 或 https://<ise ip>:8443/sponsorportal，并用以下用户登录：

  - Username: aduser(AD 用户),employee(内部)
  - Password: XXXXX



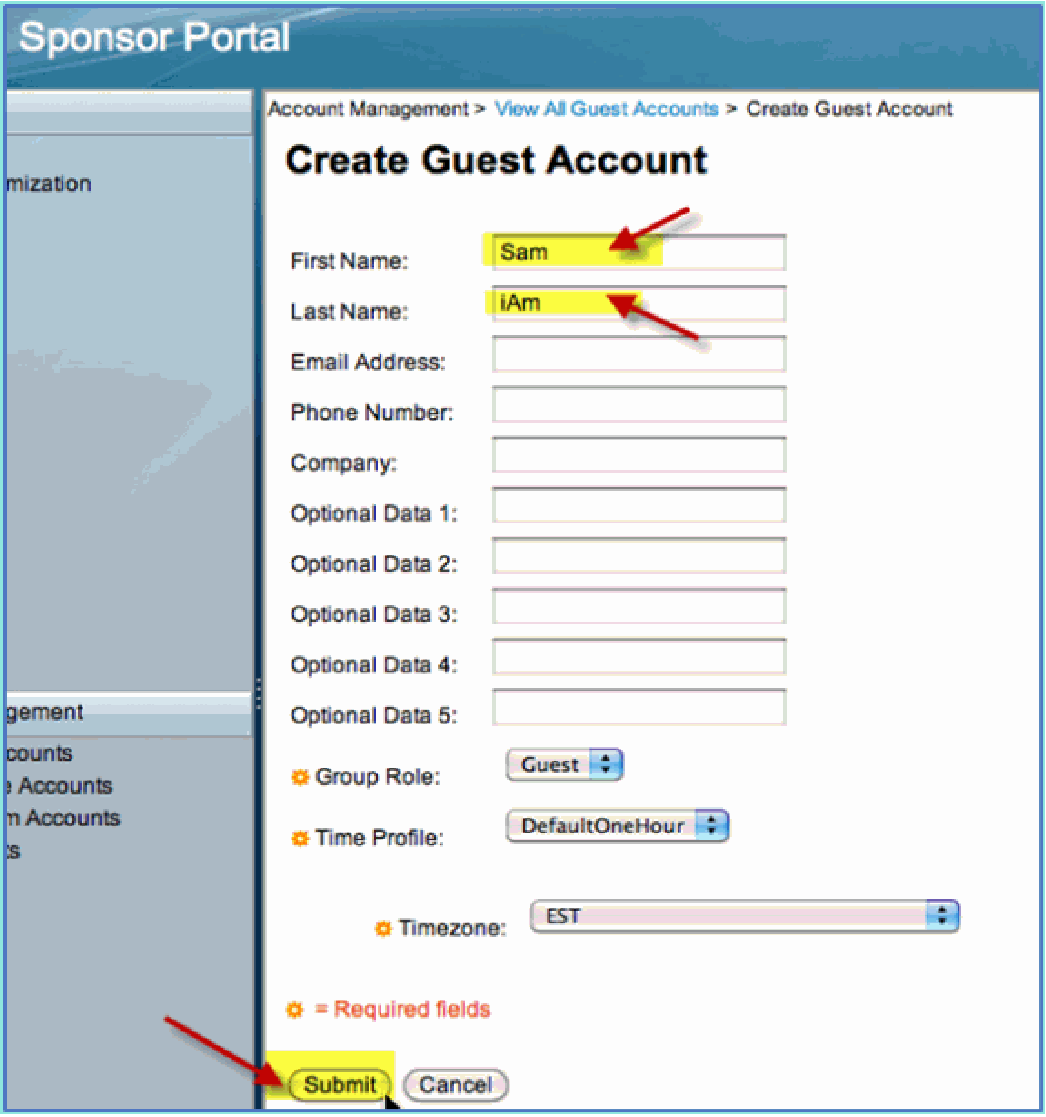
2) 在下面页面，点击 Create Single Guest User Account



cisco Sponsor Portal
Sponsor
Home
Settings Customization
Account Management
View Guest Accounts
Create Multiple Accounts
Sponsor Portal: Getting Started
View All Guest User Accounts
Create Single Guest User Account
Create Multiple Guest User Accounts

3) 创建临时访客帐号：

- First Name: Required
- Last Name: Required
- Group Role: Guest
- Time Profile: DefaultOneHour
- Time Zone: Any/Default


Sponsor Portal

Account Management > View All Guest Accounts > Create Guest Account

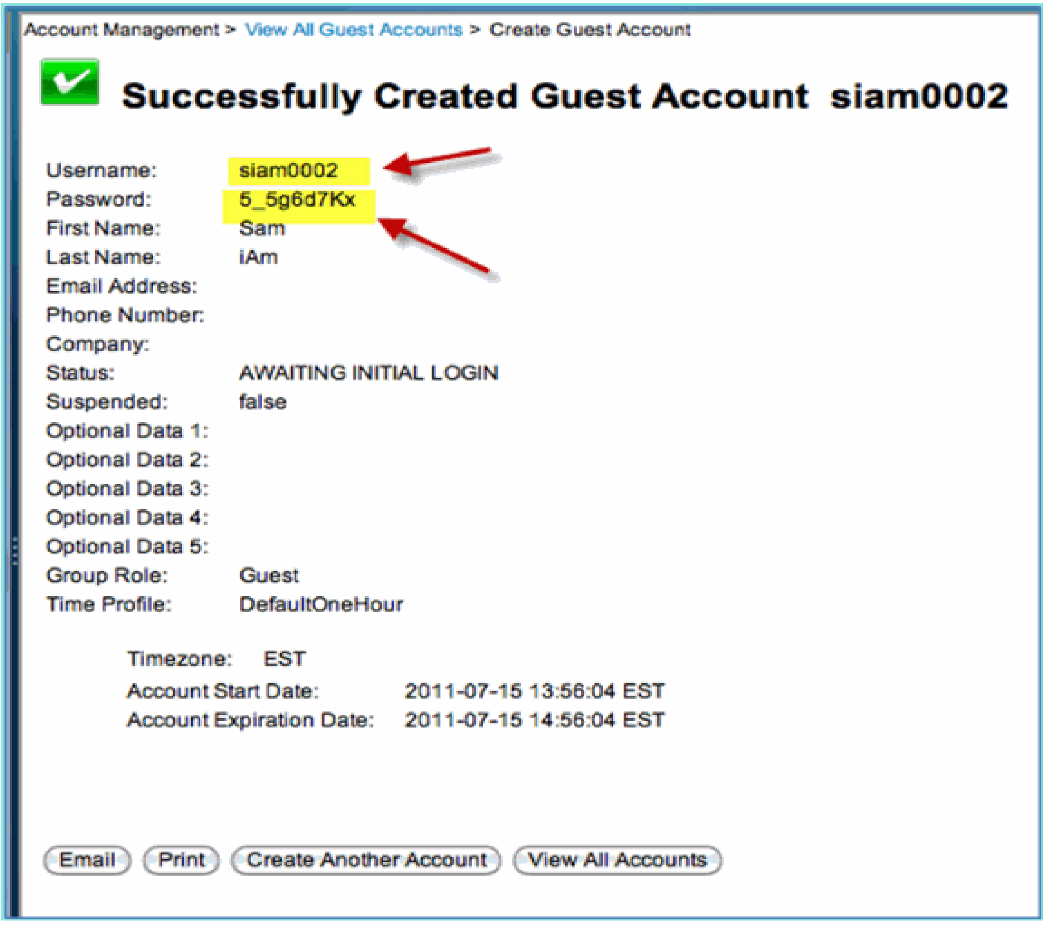
Create Guest Account

First Name:	Sam
Last Name:	iAm
Email Address:	
Phone Number:	
Company:	
Optional Data 1:	
Optional Data 2:	
Optional Data 3:	
Optional Data 4:	
Optional Data 5:	
✲ Group Role:	Guest
✲ Time Profile:	DefaultOneHour
✲ Timezone:	EST

✲ = Required fields

4) 点击 Submit

5) 访客帐号已经完成创建。注意密码是可见的。



Account Management > View All Guest Accounts > Create Guest Account

Successfully Created Guest Account siam0002

Username:	siam0002
Password:	5_5g6d7Kx
First Name:	Sam
Last Name:	iAm
Email Address:	
Phone Number:	
Company:	
Status:	AWAITING INITIAL LOGIN
Suspended:	false
Optional Data 1:	
Optional Data 2:	
Optional Data 3:	
Optional Data 4:	
Optional Data 5:	
Group Role:	Guest
Time Profile:	DefaultOneHour

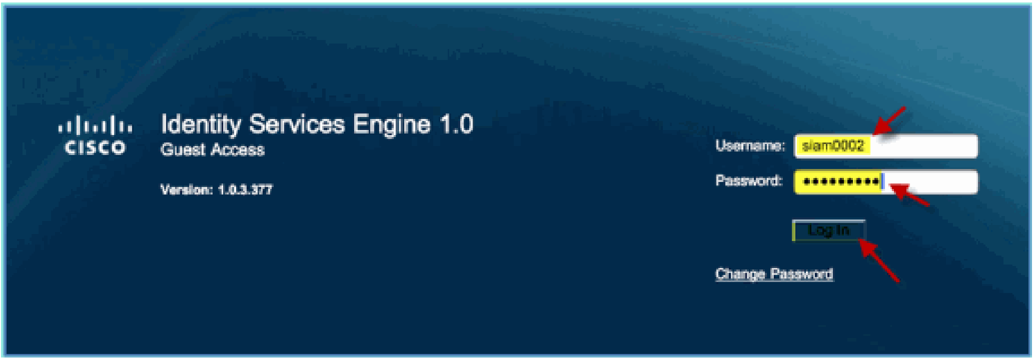
Timezone:	EST
Account Start Date:	2011-07-15 13:56:04 EST
Account Expiration Date:	2011-07-15 14:56:04 EST

- **测试访客登录和授权**

现在新的访客帐号已经由接待人创建完成，下面步骤测试访客的访问。

1) 测试设备（如 iPhone/iPad）连接到无线的 SSID pod1guest 上。

2) 通过浏览器去访问 http://10.10.10.10 或其他网站，结果被重定向到 Guest 门户登录页面上。



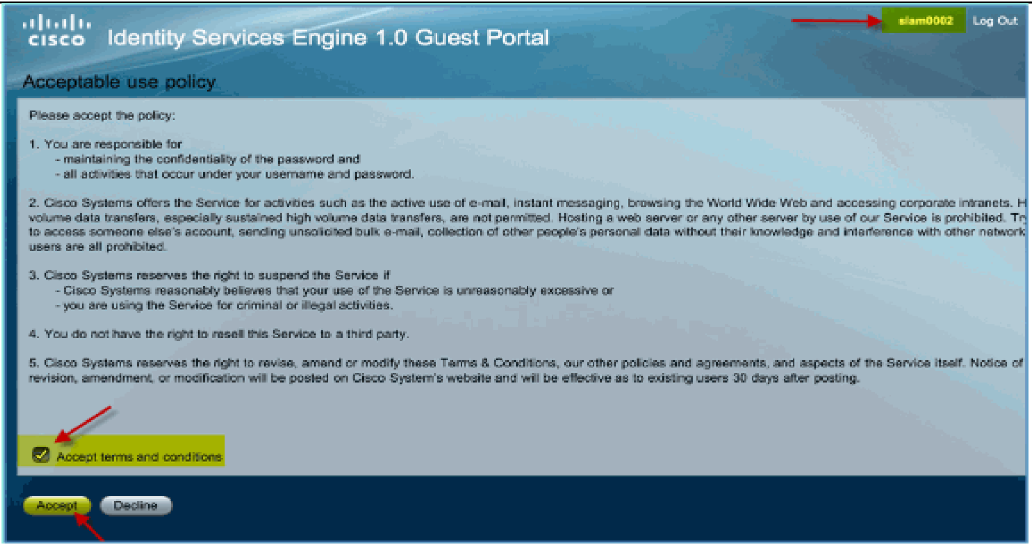
Identity Services Engine 1.0
Guest Access

Version: 1.0.3.377

Username: siam0002
Password: ••••••••••

3) 使用前面创建的访客帐号登录。

4) 登录后，出现了 Acceptable use policy 页面，选择接受 Accepterms and conditions，并点击 Accept 按钮。



Acceptable use policy

Please accept the policy:

1. You are responsible for
   - maintaining the confidentiality of the password and
   - all activities that occur under your username and password.

2. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. H volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Tr to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.

3. Cisco Systems reserves the right to suspend the Service if
   - Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or
   - you are using the Service for criminal or illegal activities.

4. You do not have the right to resell this Service to a third party.

5. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

☑ Accept terms and conditions

9. BYOD 设备注册

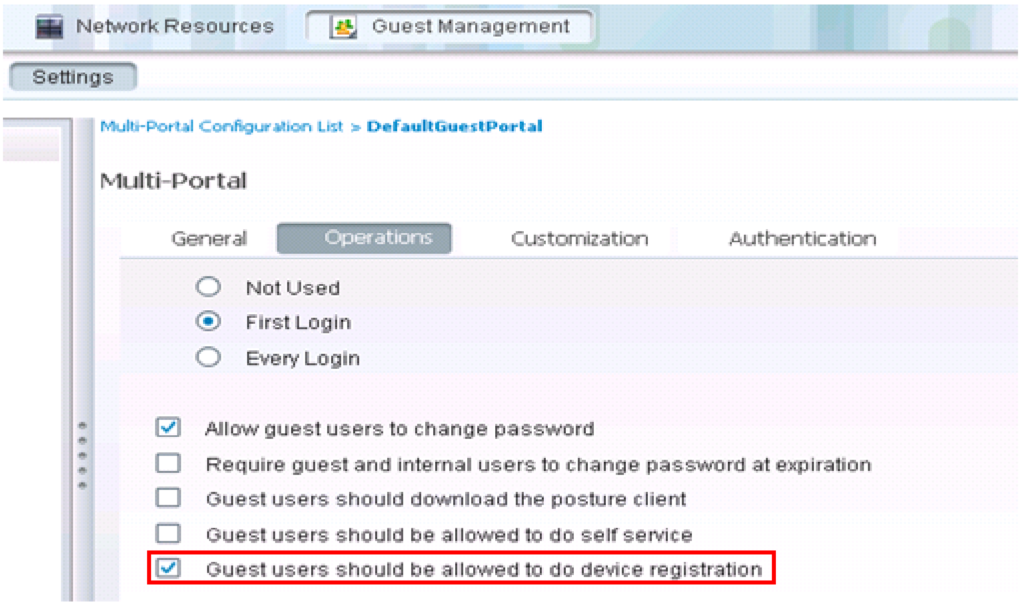
- **测试 BYOD 设备注册**

通过 ISE 的设备注册功能，可以实现员工或访客在使用注册的设备访问无线网络时，不再需要 802.1X 认证。下面步骤描述了如何在 ISE 上开启 BYOD 设备的注册。

注意：以下配置是在 ISE1.1FCS 版本上的步骤。

1) 在 ISE 上，进入 Administration > Guest Management > Guest > Multi-Portal Configurations > DefaultGuestPortal。

2) 进入 Operations 标签，选择“Guest user should be allowed to do device registration”。

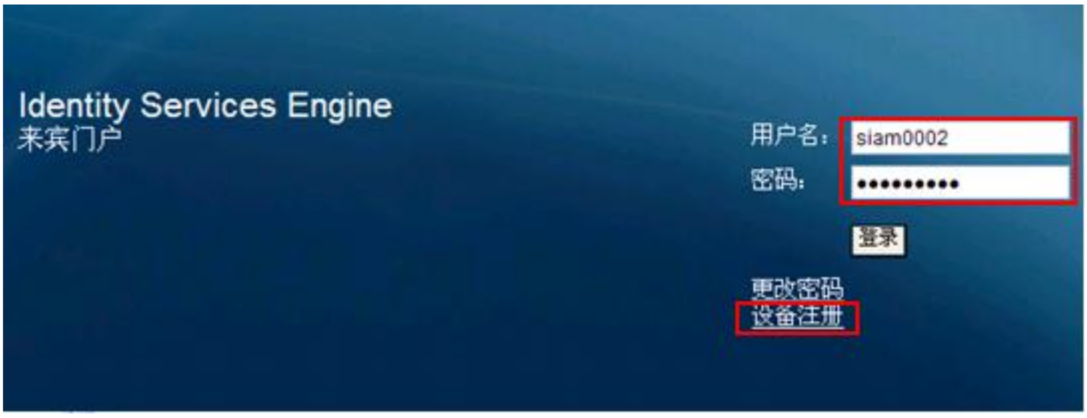


Multi-Portal

○ Not Used
● First Login
○ Every Login

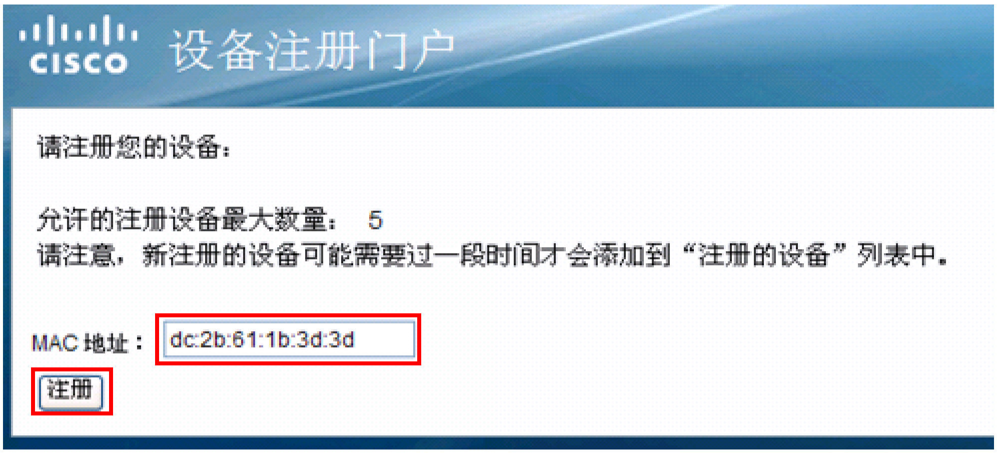
☑ Allow guest users to change password
□ Require guest and internal users to change password at expiration
□ Guest users should download the posture client
□ Guest users should be allowed to do self service
☑ Guest users should be allowed to do device registration

3) 使用移动终端设备连接 SSID pod1guest，输入前面创建的访客帐号，并点击“设备注册”。


Identity Services Engine
来宾门户

用户名：siam0002
密码：●●●●●●●●●

4) 在设备注册页面上，填写移动终端设备的 MAC 地址，并点击“注册”。

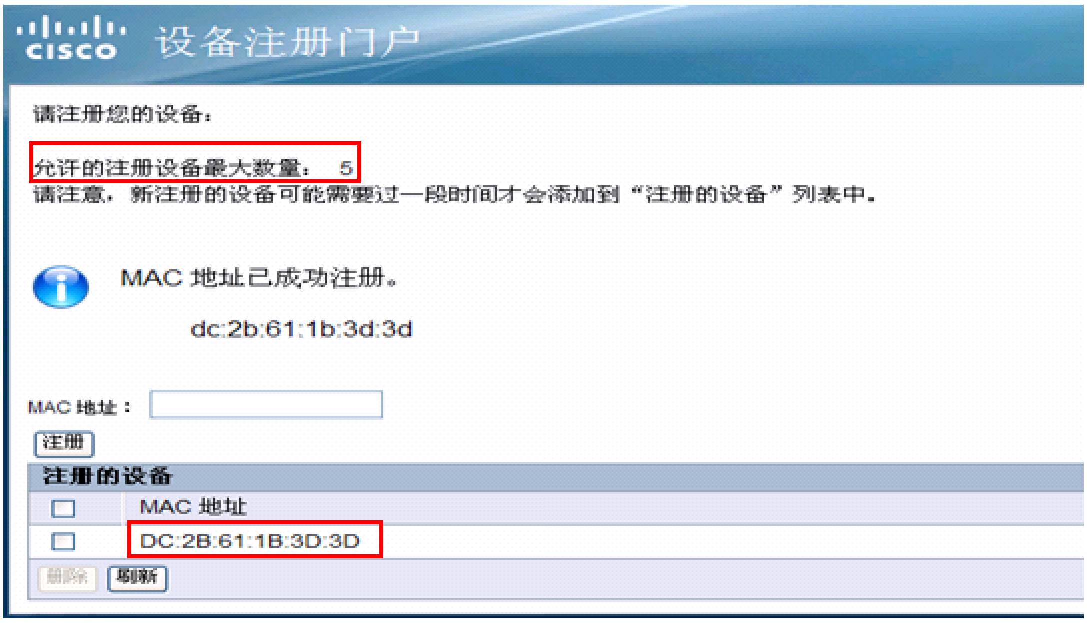

设备注册门户

请注册您的设备：

允许的注册设备最大数量： 5
请注意，新注册的设备可能需要过一段时间才会添加到“注册的设备”列表中。

MAC 地址：dc:2b:61:1b:3d:3d

5) 注册成功后，显示已经完成注册的设备的 MAC 地址。允许最大注册的设备数量为 5。



设备注册门户

请注册您的设备：

允许的注册设备最大数量： 5

请注意，新注册的设备可能需要过一段时间才会添加到“注册的设备”列表中。

MAC 地址已成功注册。

dc:2b:61:1b:3d:3d

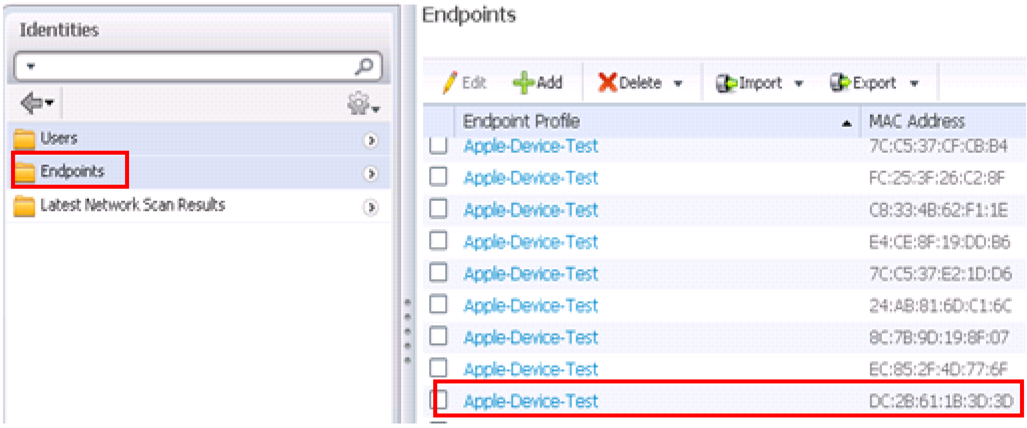
MAC 地址：

注册

注册的设备

□	MAC 地址
□	DC:2B:61:1B:3D:3D

6) 在 ISE 上，进入 Adminstration > Identity Management > Identities > Endpoints，查看注册成功的终端设备的 MAC 地址已经列入了 Endpoints 中。



Endpoints

	Endpoint Profile	MAC Address
□	Apple-Device-Test	7C:C5:37:CF:CB:B4
□	Apple-Device-Test	FC:25:3F:26:C2:8F
□	Apple-Device-Test	C8:33:4B:62:F1:1E
□	Apple-Device-Test	E4:CE:8F:19:DD:B6
□	Apple-Device-Test	7C:C5:37:E2:1D:D6
□	Apple-Device-Test	24:AB:81:6D:C1:6C
□	Apple-Device-Test	8C:7B:9D:19:8F:07
□	Apple-Device-Test	EC:85:2F:4D:77:6F
□	Apple-Device-Test	DC:2B:61:1B:3D:3D