

# 适用于FlexConnect的无线BYOD部署指南

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[拓扑](#)

[设备注册和请求方调配](#)

[资产注册门户](#)

[自助注册门户](#)

[身份验证和调配](#)

[iOS调配\(iPhone/iPad/iPod\)](#)

[Android调配](#)

[双SSID无线BYOD自助注册](#)

[单SSID无线BYOD自助注册](#)

[功能配置](#)

[WLAN 配置](#)

[FlexConnect AP配置](#)

[ISE 配置](#)

[用户体验 — 调配iOS](#)

[双SSID](#)

[单SSID](#)

[用户体验 — 调配Android](#)

[双SSID](#)

[我的设备门户](#)

[参考 — 证书](#)

[相关信息](#)

## 简介

移动设备在计算能力上越来越强大，在消费者中越来越受欢迎。数以百万计的这些设备通过高速Wi-Fi销售给消费者，因此用户可以进行通信和协作。现在，消费者已经习惯了这些移动设备为他们的生活带来的工作效率提升，并正在寻求将他们的个人体验带入工作空间。这就产生了在工作场所使用自带设备(BYOD)解决方案的功能需求。

本文档提供BYOD解决方案的分支机构部署。员工使用新iPad连接到企业服务集标识符(SSID)，并被重定向到自助注册门户。思科身份服务引擎(ISE)根据公司Active Directory(AD)对用户进行身份验证，并将具有嵌入式iPad MAC地址和用户名的证书以及请求方配置文件下载到iPad，该请求方配置文件强制使用可扩展身份验证协议 — 传输层安全(EAP-TLS)作为dot1x连接的方法。根据ISE中的授权策略，用户可以使用dot1x连接并访问适当的资源。

早于7.2.110.0的思科无线局域网控制器软件版本中的ISE功能不支持通过FlexConnect接入点(AP)关联的本地交换客户端。版本7.2.110.0支持用于本地交换和集中身份验证客户端的FlexConnect AP的这些ISE功能。此外，与ISE 1.1.1集成的版本7.2.110.0提供 ( 但不限于 ) 以下无线自带设备解决方案功能：

- 设备分析和状态
- 设备注册和请求方调配
- 个人设备自注册 ( 调配iOS或Android设备 )

**注意：**虽然受支持，但本指南中不包括其他设备，例如PC或Mac无线笔记本电脑和 workstation。

## 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：

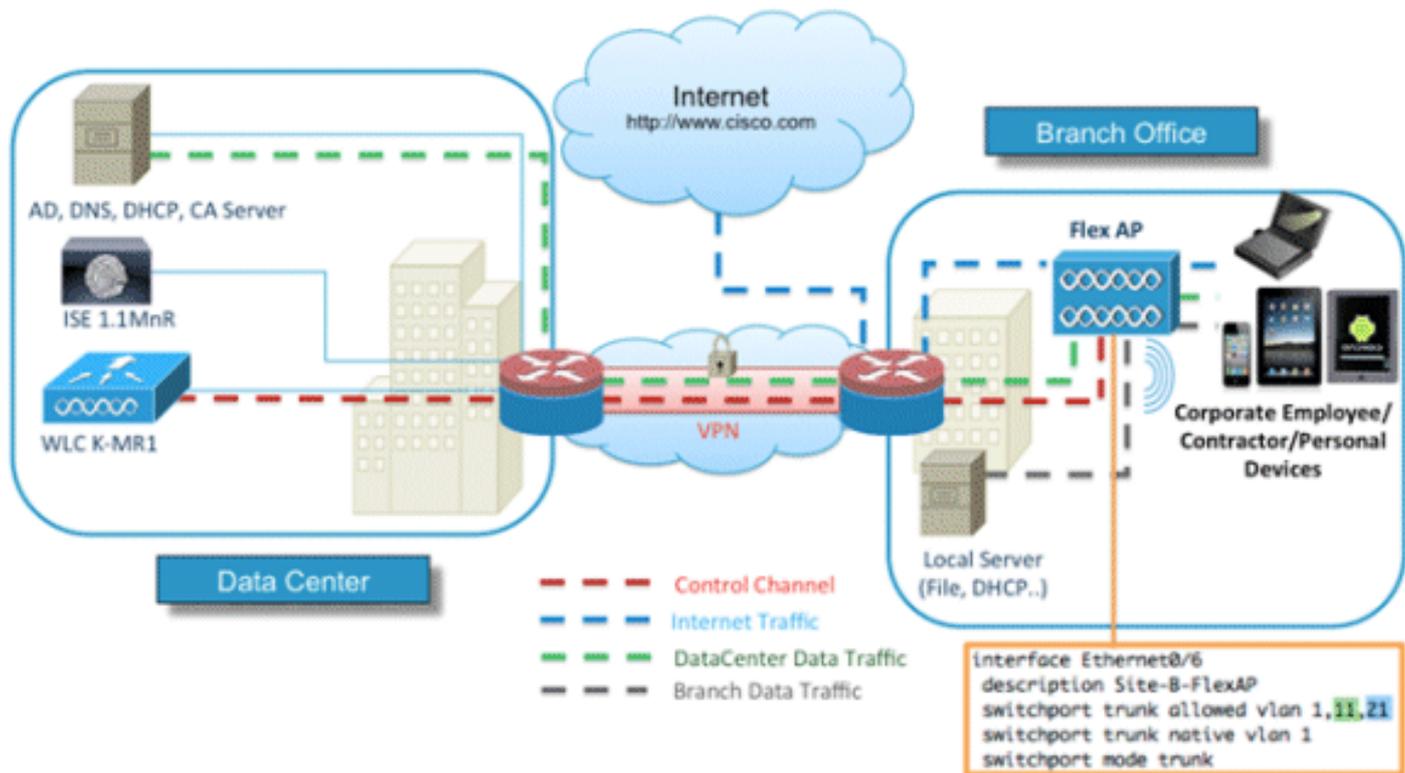
- Cisco Catalyst交换机
- 思科无线局域网(WLAN)控制器
- 思科WLAN控制器(WLC)软件版本7.2.110.0及更高版本
- FlexConnect模式下的802.11n AP
- Cisco ISE软件1.1.1版及更高版本
- 带证书颁发机构(CA)的Windows 2008 AD
- DHCP 服务器
- 域名系统 (DNS) 服务器
- 网络时间协议 (NTP)
- 无线客户端笔记本电脑、智能手机和平板电脑 ( Apple iOS、Android、Windows和Mac )

**注意：**有关此软件版本的重要信息，请参阅[版本7.2.110.0的思科无线LAN控制器和轻量接入点版本说明](#)。在加载和测试软件之前，请登录Cisco.com网站查看最新的版本说明。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 ( 默认 ) 配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### 拓扑

要正确实施和测试这些功能，需要最低限度的网络设置，如下图所示：



对于此模拟，您需要具有FlexConnect AP的网络、具有本地DHCP的本地/远程站点、DNS、WLC和ISE。FlexConnect AP连接到中继以测试多个VLAN的本地交换。

## 设备注册和请求方调配

必须注册设备，以便其本地请求方可以调配dot1x身份验证。根据正确的身份验证策略，用户被重定向到访客页面并通过员工凭证进行身份验证。用户将看到设备注册页面，该页面要求用户输入设备信息。然后开始设备调配过程。如果调配不支持操作系统(OS)，则用户将被重定向到资产注册门户，以将该设备标记为MAC身份验证绕行(MAB)访问。如果操作系统受支持，注册过程将开始并配置设备的本地请求方进行dot1x身份验证。

## 资产注册门户

资产注册门户是ISE平台的元素，允许员工通过身份验证和注册流程启动终端自注册。

管理员可以从终端身份页面删除资产。每位员工都可以编辑、删除已注册的资产并将其列入黑名单。列入黑名单的终端被分配到黑名单身份组，并且创建授权策略以阻止列入黑名单的终端访问网络。

## 自助注册门户

在中心Web身份验证(CWA)流程中，员工被重定向到允许他们输入其凭证、进行身份验证和输入他们希望注册的特定资产的细节的门户。此门户称为自助调配门户，类似于设备注册门户。它允许员工输入MAC地址以及有意义的终端描述。

## 身份验证和调配

一旦员工选择自助注册门户，他们便需要提供一组有效的员工凭证以继续进入调配阶段。身份验证成功后，终端可以调配到终端数据库中，并为终端生成证书。页面上的链接允许员工下载 Supplicant客户端引导向导(SPW)。

**注意：**请参阅Cisco的[FlexConnect功能矩阵](#)文章，以便查看BYOD的最新FlexConnect功能矩阵。

## iOS调配(iPhone/iPad/iPod)

对于EAP-TLS配置，ISE遵循Apple Over-the-Air(OTA)注册流程：

- 身份验证成功后，评估引擎将评估客户端调配策略，从而生成请求方配置文件。
- 如果请求方配置文件用于EAP-TLS设置，则OTA进程确定ISE是使用自签名还是由未知CA签名。如果其中一个条件为true，则要求用户下载ISE或CA的证书，然后才能开始注册过程。
- 对于其他EAP方法，ISE在身份验证成功后推送最终配置文件。

## Android调配

出于安全考虑，Android代理必须从Android市场网站下载，并且不能从ISE调配。思科通过Cisco Android marketplace发布者帐户将向导的候选版本上传到Android市场。

这是Android调配过程：

1. 思科使用软件开发套件(SDK)创建扩展名为.apk的Android软件包。
2. 思科将软件包上传到Android市场。
3. 用户使用适当的参数配置客户端调配中的策略。
4. 注册设备后，当dot1x身份验证失败时，最终用户将重定向到客户端调配服务。
5. 调配门户页面提供将用户重定向到Android市场门户的按钮，用户可以在该门户下载SPW。
6. Cisco SPW启动并执行请求方的调配：SPW发现ISE并从ISE下载配置文件。SPW为EAP-TLS创建证书/密钥对。SPW向ISE发出简单证书注册协议(SCEP)代理请求调用并获取证书。SPW应用无线配置文件。如果成功应用配置文件，SPW将触发重新身份验证。SPW退出。

## 双SSID无线BYOD自助注册

双SSID无线BYOD自注册过程如下：

1. 用户与访客SSID关联。
2. 用户打开浏览器并重定向到ISE CWA访客门户。
3. 用户在访客门户中输入员工用户名和密码。
4. ISE对用户进行身份验证，并根据他们是员工而不是访客的事实，将用户重定向到Employee Device Registration访客页面。
5. MAC地址预填充到设备ID的设备注册访客页面中。用户输入说明，并在需要时接受可接受的使用策略(AUP)。

6. 用户选择**Accept**并开始下载和安装SPW。
7. 该用户设备的请求方将与所有证书一起调配。
8. 发生CoA，设备重新关联到企业SSID(CORP)并使用EAP-TLS ( 或用于该请求方的其它授权方法 ) 进行身份验证。

## 单SSID无线BYOD自助注册

在此方案中，企业接入(CORP)使用单个SSID，同时支持受保护的可扩展身份验证协议(PEAP)和EAP-TLS。没有访客SSID。

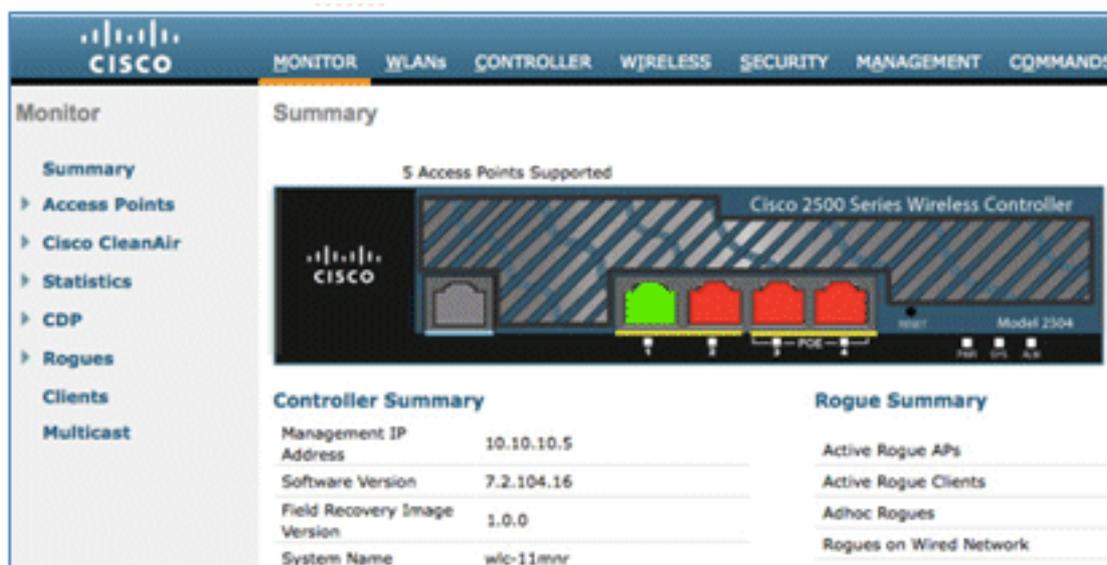
以下是单SSID无线BYOD自注册过程：

1. 用户与CORP关联。
2. 用户向PEAP身份验证的请求方输入员工用户名和密码。
3. ISE对用户进行身份验证，并根据PEAP方法，提供接受授权策略并重定向到Employee Device Registration访客页面。
4. 用户打开浏览器并重定向到Employee Device Registration guest页面。
5. MAC地址预填充到设备ID的设备注册访客页面中。用户输入说明并接受AUP。
6. 用户选择**Accept**并开始下载和安装SPW。
7. 该用户设备的请求方将与所有证书一起调配。
8. 发生CoA，设备重新关联到CORP SSID并使用EAP-TLS进行身份验证。

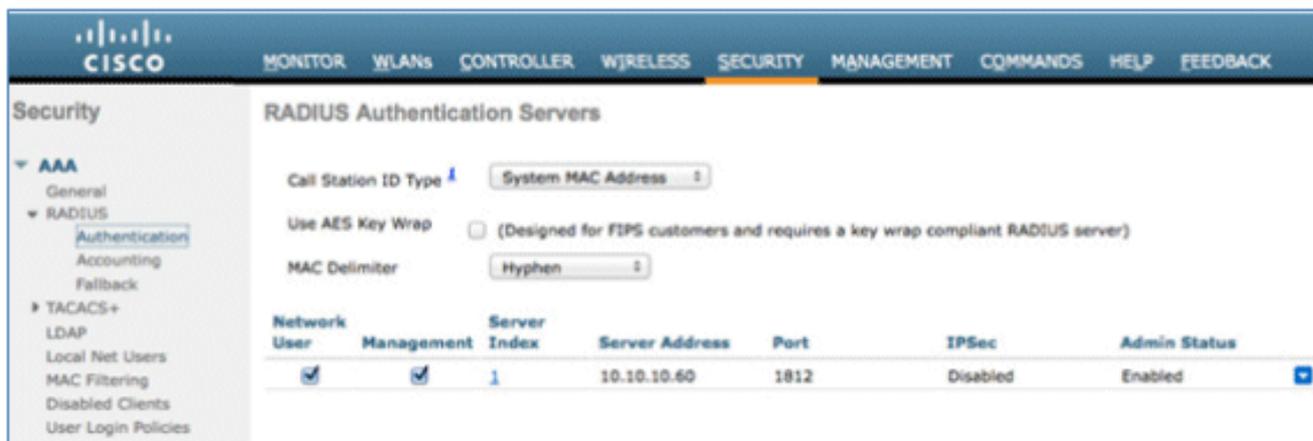
## 功能配置

完成以下步骤以开始配置：

1. 对于本指南，请确保WLC版本为7.2.110.0或更高版本。

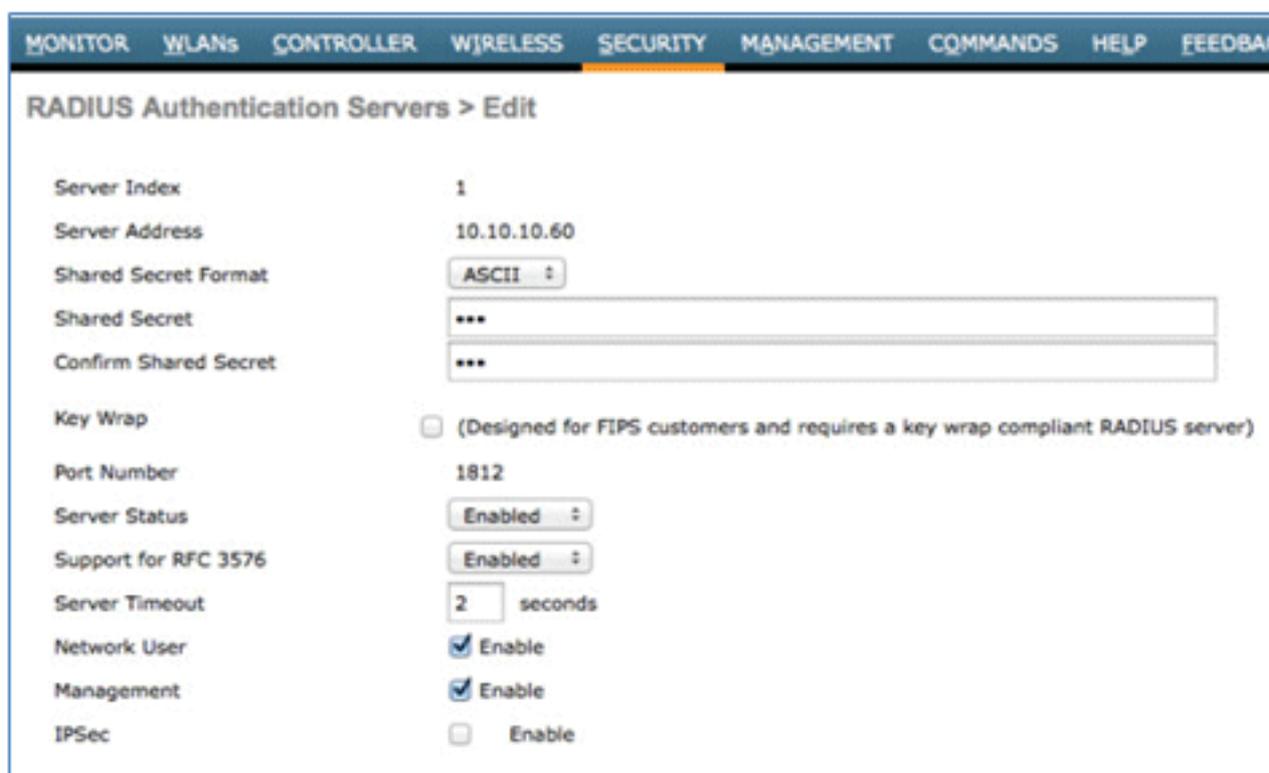


2. 导航到**Security > RADIUS > Authentication**，然后将RADIUS服务器添加到WLC。

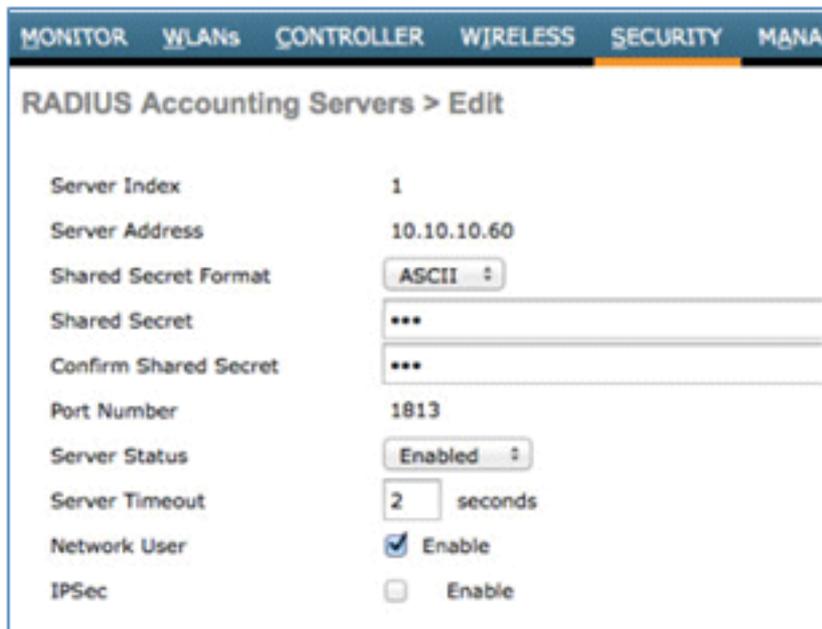


3. 将ISE 1.1.1添加到WLC:

输入共享密钥。将Support for RFC 3576 (对RFC 3576的支持) 设置为Enabled。



4. 添加与RADIUS记账服务器相同的ISE服务器。



5. 创建稍后在ISE策略中使用的WLC预身份验证ACL。导航到WLC > **Security** > Access Control Lists > **FlexConnect ACLs**，然后创建名为**ACL-REDIRECT**的新FlexConnect ACL（在本例中）。



6. 在ACL规则中，允许所有流入/流出ISE的流量，并在请求方调配期间允许客户端流量。

对于第一条规则（序列1）：

将Source设置为**Any**。设置IP（ISE地址）/网络掩码**255.255.255.255**。将Action设置为**Permit**。

Access Control Lists > Rules > Edit

Sequence:

Source:

Destination:  IP Address:  Netmask:

Protocol:

DSCP:

Direction:

Action:

对于第二个规则（序列2），将源IP（ISE地址）/掩码255.255.255.255设置为Any，将操作设置为Permit。

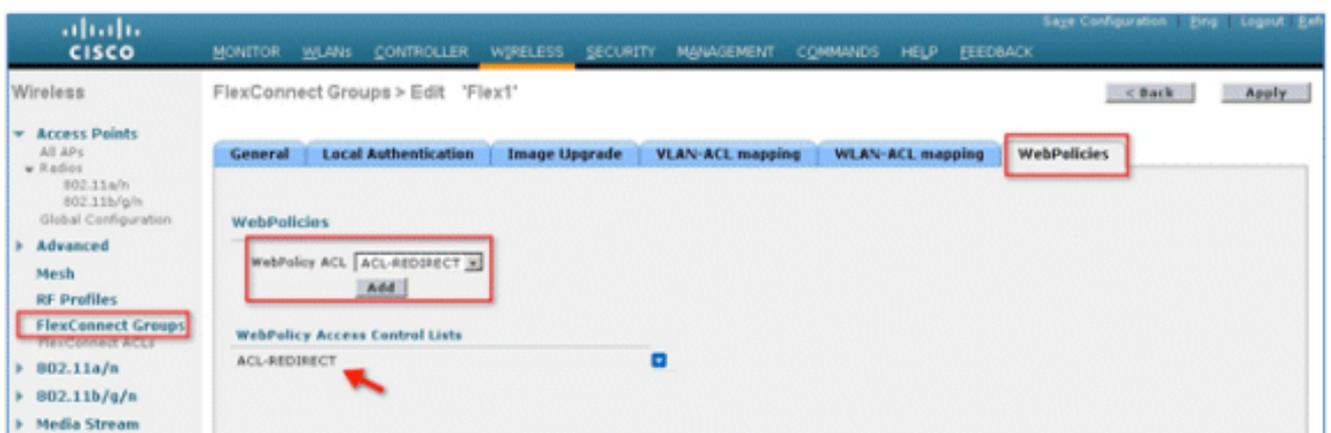
General

Access List Name: ACL-REDIRECT

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.60 / 255.255.255.255	Any	Any	Any	Any
2	Permit	10.10.10.60 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any

7. 创建名为Flex1的新FlexConnect组（在本例中）：

导航到FlexConnect Group > WebPolicies选项卡。在WebPolicy ACL字段下，单击Add，然后选择ACL-REDIRECT或之前创建的FlexConnect ACL。确认它填充了WebPolicy Access Control Lists 字段。



8. 单击Apply和Save Configuration。

## WLAN 配置

要配置WLAN，请完成以下步骤：

1. 创建双SSID的开放式WLAN SSID示例：

输入WLAN名称：**DemoCWA**（在本例中）。为Status选择**Enabled**选项。



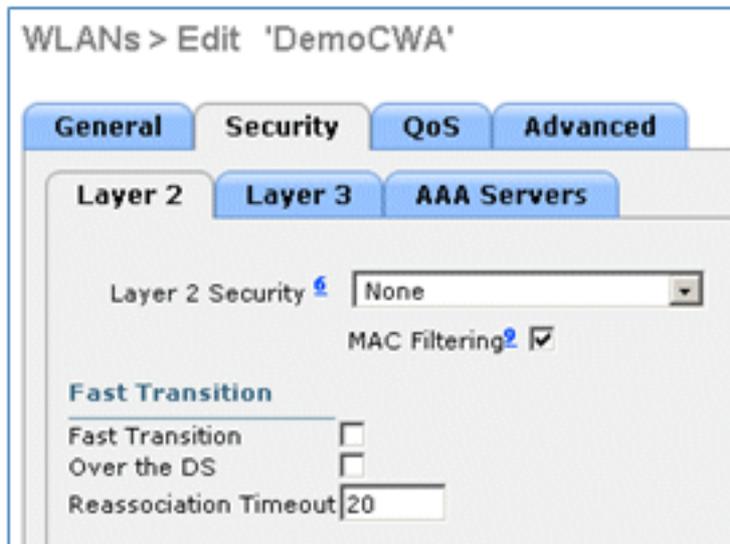
WLANs > Edit 'DemoCWA'

**General** Security QoS Advanced

Profile Name	DemoCWA
Type	WLAN
SSID	DemoCWA
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	MAC Filtering (Modifications done under se
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

2. 导航到**Security**选项卡> **Layer 2**选项卡，并设置以下属性：

第2层安全：无MAC过滤：启用（复选框为选中状态）快速过渡：禁用（未选中框）



WLANs > Edit 'DemoCWA'

General **Security** QoS Advanced

Layer 2 **Layer 3** AAA Servers

Layer 2 Security <sup>6</sup> None

MAC Filtering <sup>2</sup>

**Fast Transition**

Fast Transition

Over the DS

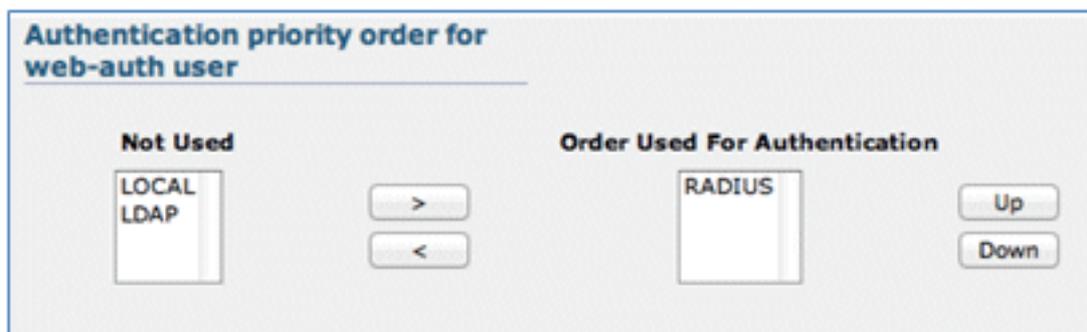
Reassociation Timeout 20

3. 转至**AAA Servers**选项卡，并设置以下属性：

身份验证和帐户服务器：已启用服务器1:<ISE IP地址>

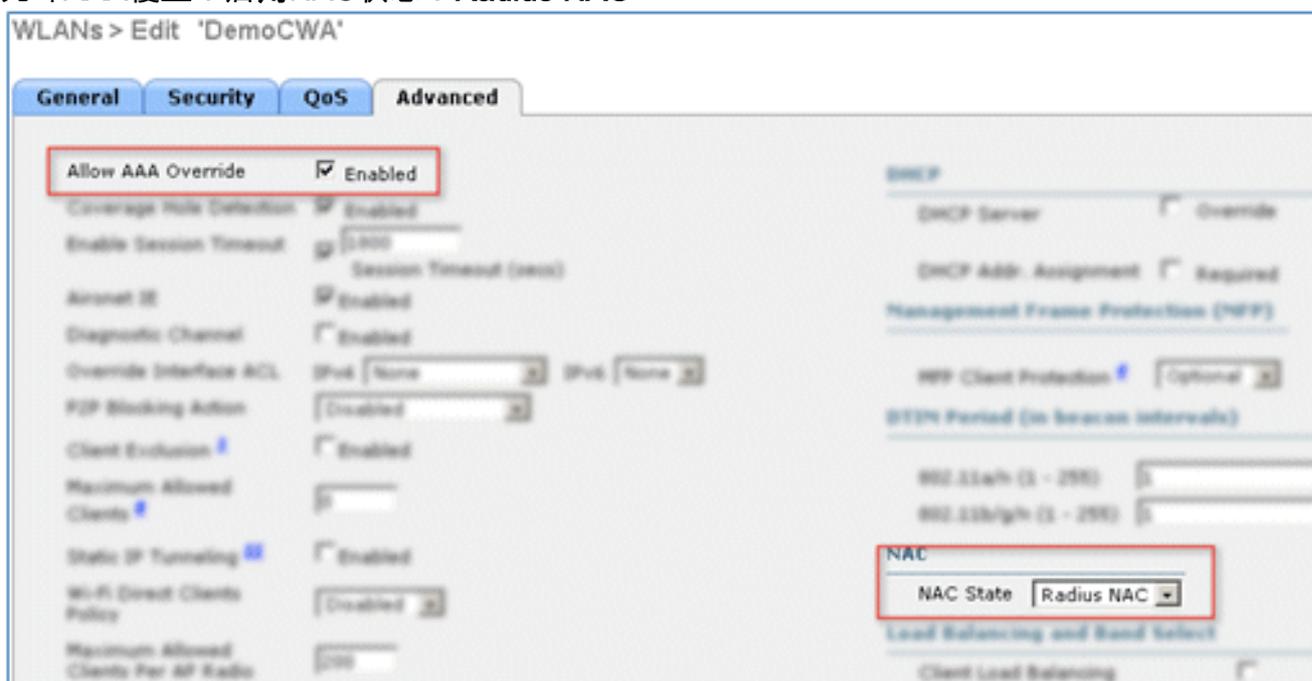


4. 从AAA Servers选项卡向下滚动。在Web-auth用户的Authentication priority order下，确保将RADIUS用于身份验证，而不使用其他身份验证。



5. 转到Advanced选项卡，并设置以下属性：

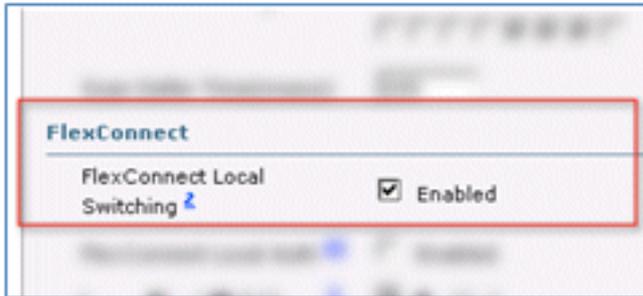
允许AAA覆盖：启用NAC状态：Radius NAC



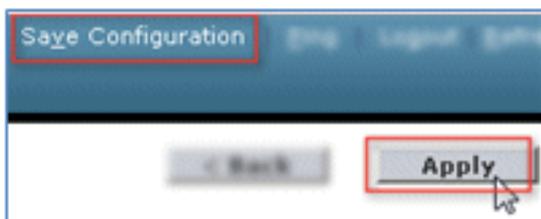
注意：当FlexConnect AP处于断开模式时，不支持RADIUS网络准入控制(NAC)。因此，如果

FlexConnect AP处于独立模式且失去与WLC的连接，所有客户端都会断开连接，并且不再通告SSID。

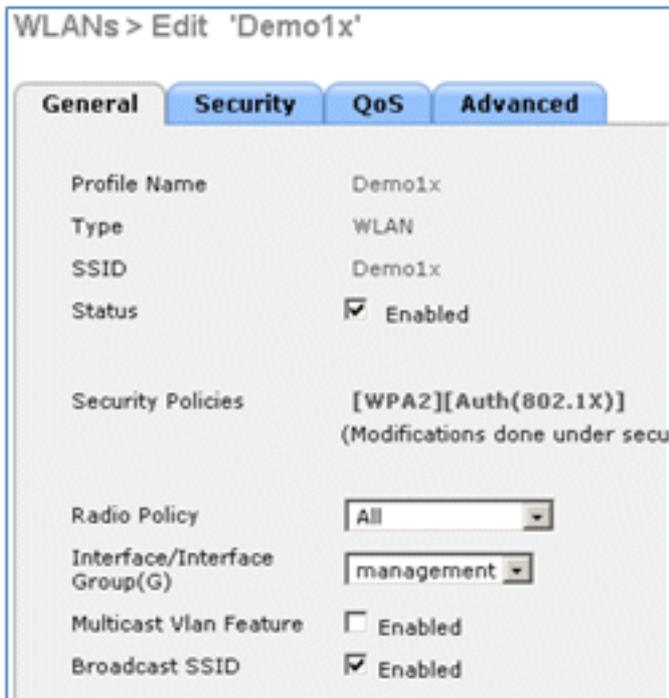
6. 在Advanced (高级) 选项卡中向下滚动，并将FlexConnect Local Switching ( FlexConnect本地交换 ) 设置为**Enabled**。



7. 单击**Apply**和**Save Configuration**。

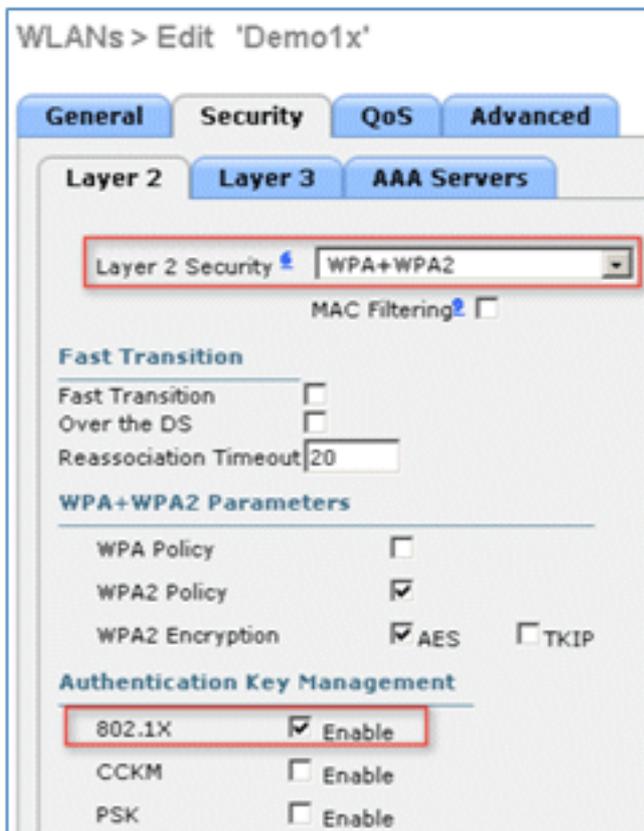


8. 为单和双SSID场景创建名为**Demo1x** ( 在本例中 ) 的802.1X WLAN SSID。



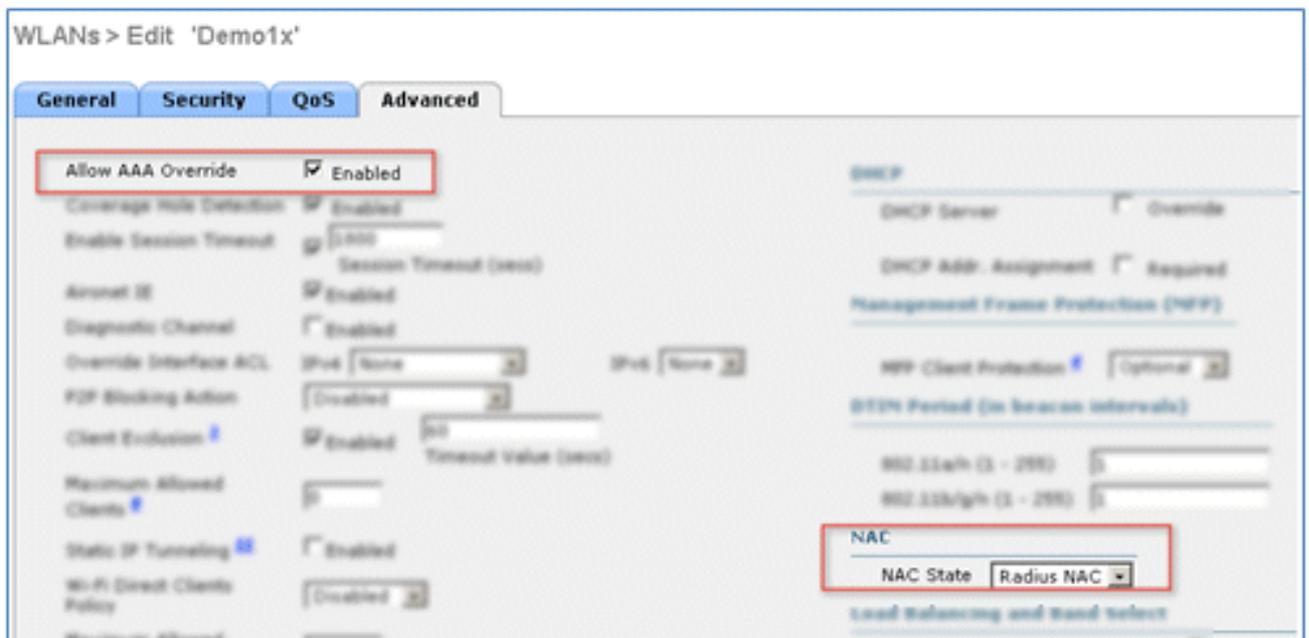
9. 导航到**Security**选项卡> **Layer 2**选项卡，并设置以下属性：

第2层安全:WPA+WPA2快速过渡：禁用 ( 未选中框 ) 身份验证密钥管理：802.IX：启用

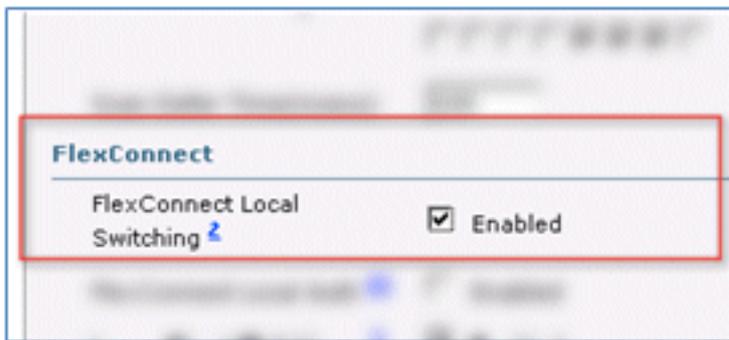


10. 转到**Advanced**选项卡，并设置以下属性：

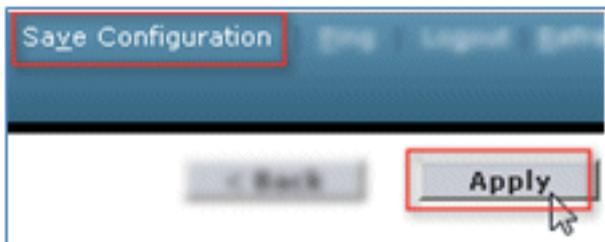
允许AAA覆盖：启用NAC状态：Radius NAC



11. 在**Advanced**选项卡中向下滚动，并将FlexConnect Local Switching设置为**Enabled**。



12. 单击Apply和Save Configuration。



13. 确认已创建两个新WLAN。

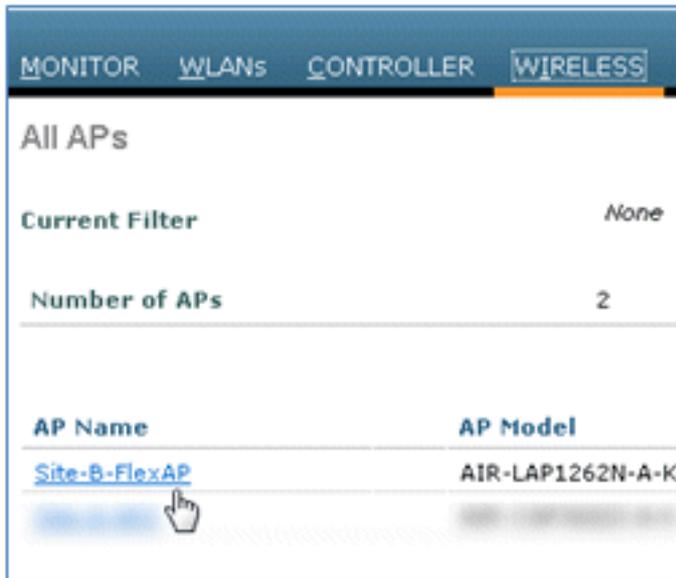
The screenshot shows the 'WLANs' configuration page. A table lists several WLANs. A red box highlights the two newly created WLANs: 'Demo1x' and 'DemoCWA'.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	SSX	SSX	Disabled	[WPA2][Auth(802.1X)]
2	WLAN	B	B	Enabled	[WPA2][Auth(PSK)]
3	WLAN	Demo1x	Demo1x	Enabled	[WPA2][Auth(802.1X)]
4	WLAN	DemoCWA	DemoCWA	Enabled	MAC Filtering
5	WLAN	Sec	Sec	Disabled	Web-Auth

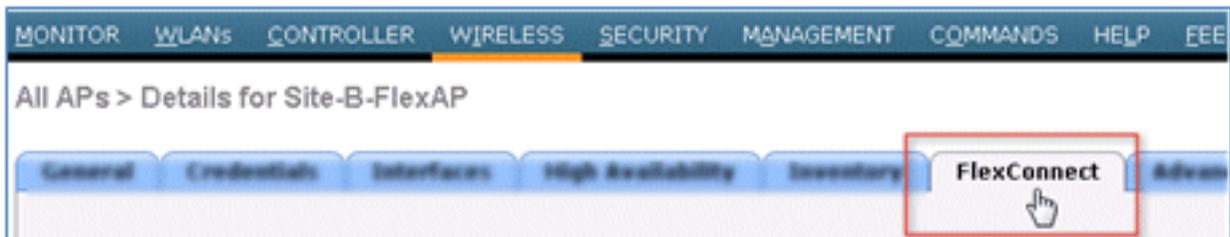
## FlexConnect AP配置

要配置FlexConnect AP，请完成以下步骤：

1. 导航到WLC > Wireless，然后单击目标FlexConnect AP。



2. 单击FlexConnect选项卡。



3. 启用VLAN支持（选中此框），设置本地VLAN ID，然后单击VLAN映射。



4. 将SSID的VLAN ID设置为21（在本例中）以用于本地交换。

MONITOR			WLANs			CONTROLLER			WIRELESS			SECURITY			M...		
All APs > Site-B-FlexAP > VLAN Mappings																	
AP Name						Site-B-FlexAP											
Base Radio MAC						e8:04:62:0a:68:80											
WLAN Id		SSID		VLAN ID													
3		Demo1x		21													
4		DemoCWA		21													

5. 单击Apply和Save Configuration。

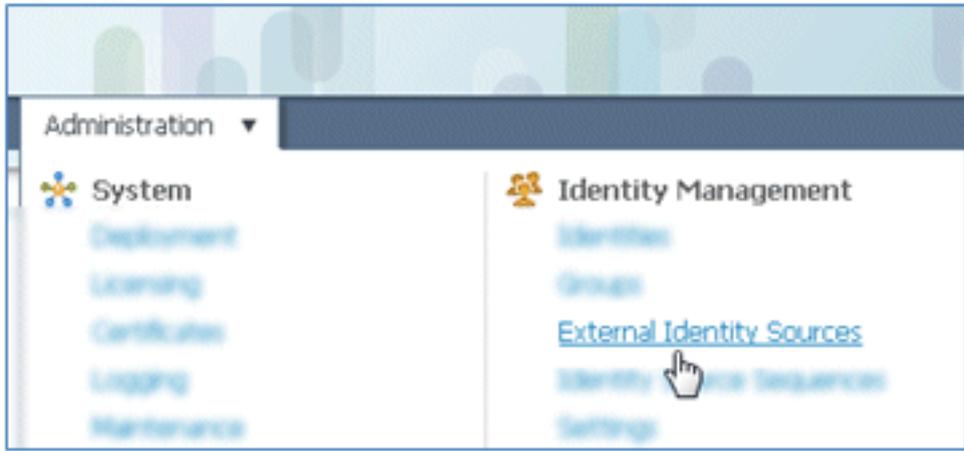
## ISE 配置

完成以下步骤以配置ISE:

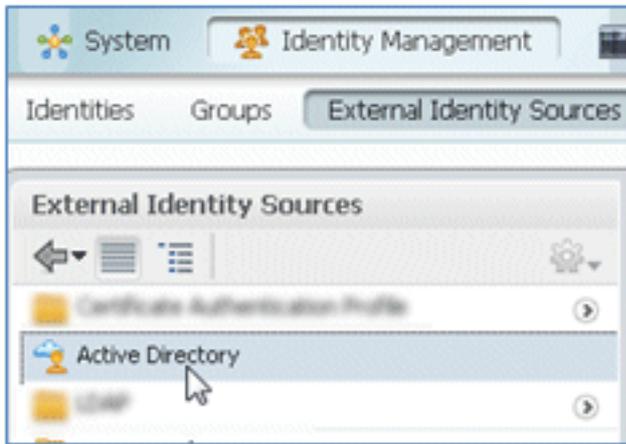
1. 登录ISE服务器 : <<https://ise>>。



2. 导航到管理 > 身份管理 > 外部身份源。



3. 单击Active Directory。

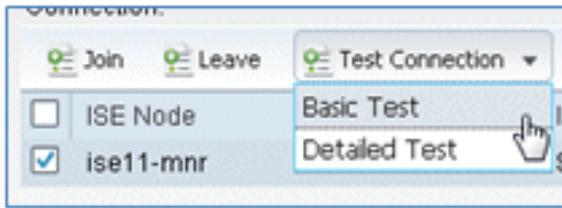


4. 在Connection选项卡中：

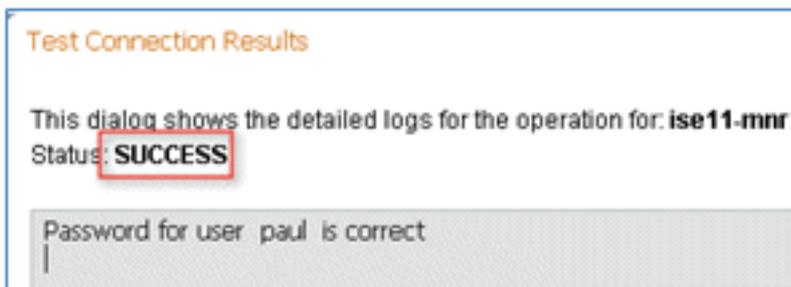
添加corp.rf-demo.com的域名（在本例中），并将身份库名称默认为AD1。单击Save Configuration。单击Join，并提供加入所需的AD管理员帐户用户名和密码。“状态”必须为绿色。启用Connected to:（复选框处于选中状态）。



5. 使用当前域用户对AD执行基本连接测试。

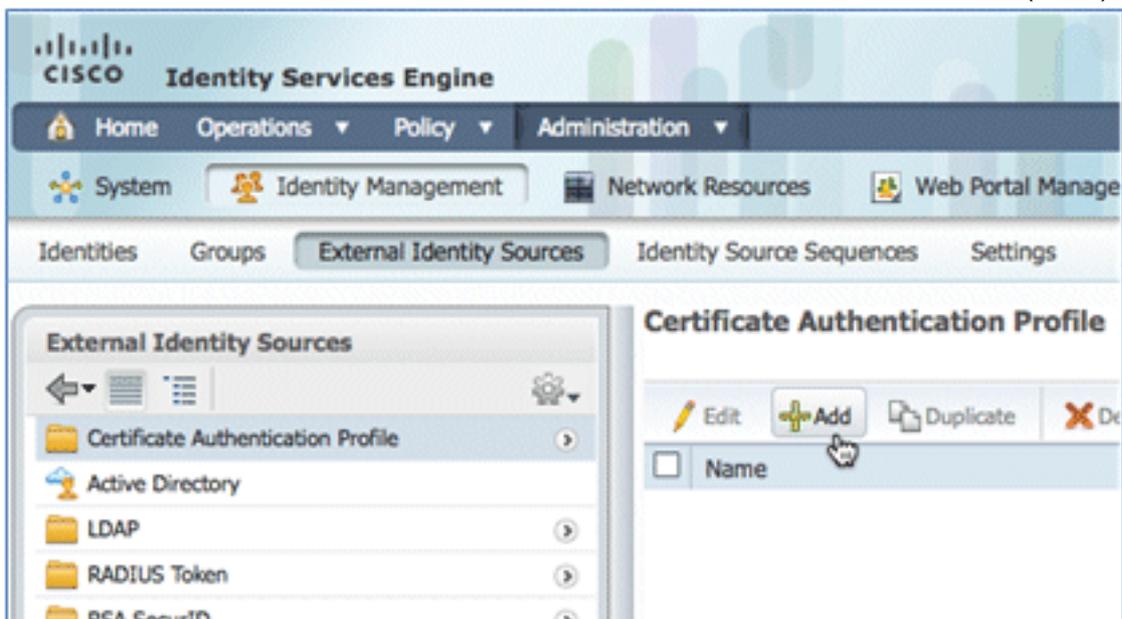


6. 如果成功连接到AD，则会显示一个对话框，确认密码正确。



7. 导航到管理 > 身份管理 > 外部身份源:

点击证书身份验证配置文件。单击Add以获取新的证书身份验证配置文件(CAP)。



8. 为CAP输入名称**CertAuth**（在本例中）；对于Principal Username X509 Attribute，选择**Common Name**；然后单击Submit。

Certificate Authentication Profiles List > New Certificate Authentication Profile

### Certificate Authentication Profile

\* Name

Description

Principal Username X509 Attribute

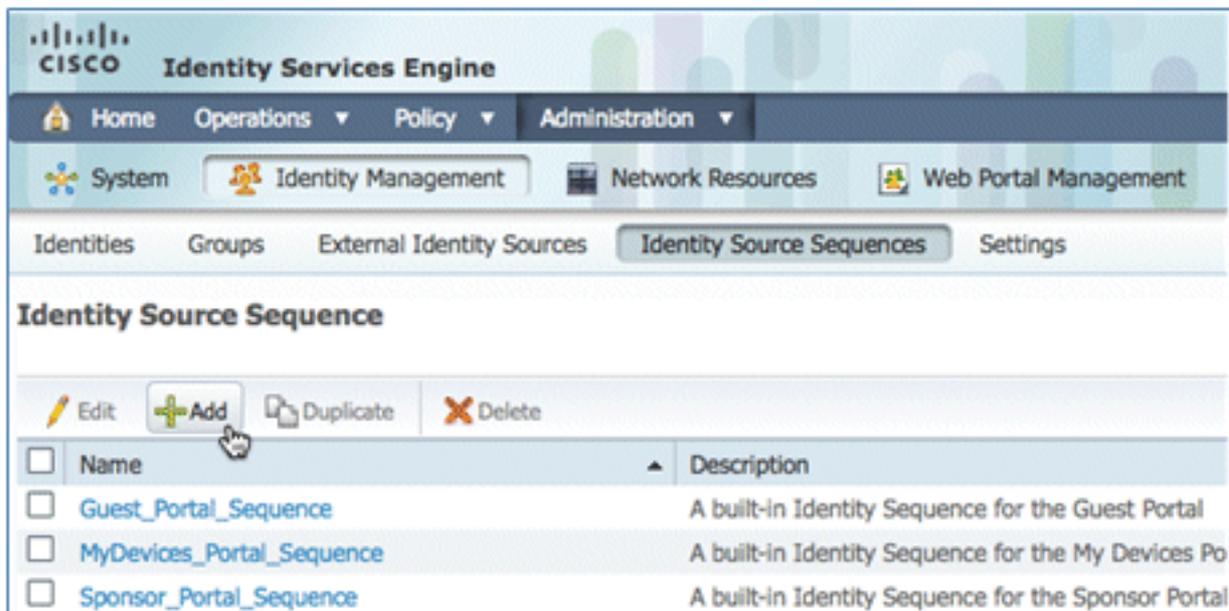
Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

LDAP/AD Instance Name

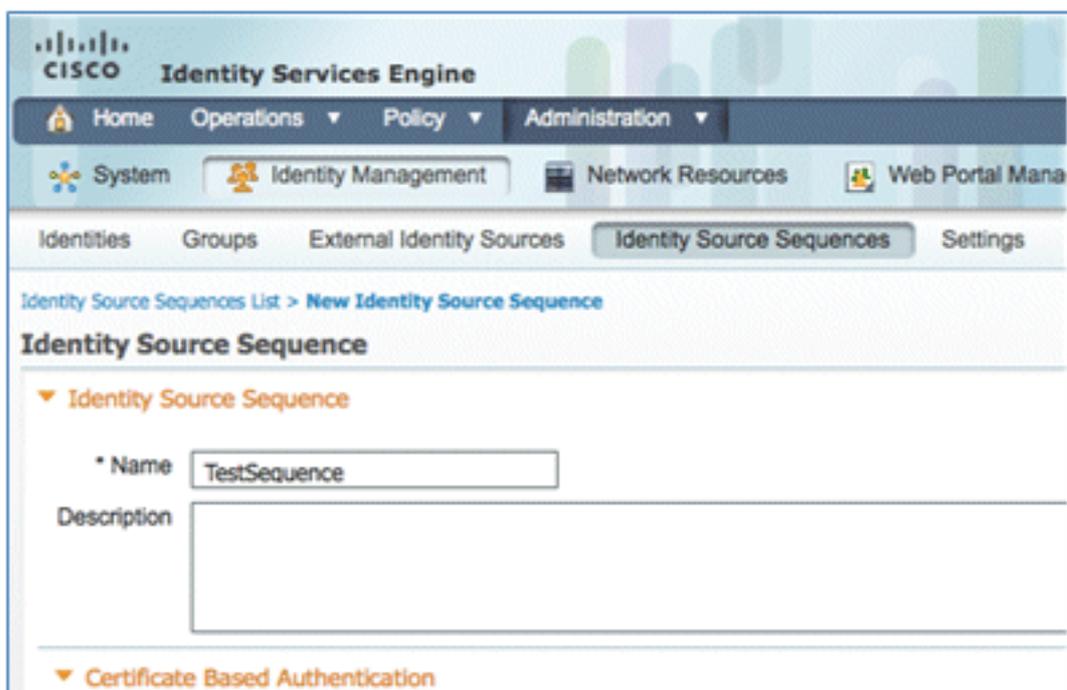
9. 确认已添加新的CAP。

The screenshot shows the Cisco Identity Services Engine Administration interface. The breadcrumb navigation is Administration > Identity Management > External Identity Sources > Certificate Authentication Profile. The left sidebar shows a tree view of External Identity Sources with 'Certificate Authentication Profile' selected. The main content area displays the configuration for the 'Certificate Authentication Profile'. At the top, there are buttons for Edit, Add, Duplicate, and Delete. Below these, there is a list of fields with checkboxes. The 'Name' field is checked and highlighted in blue, and a red arrow points to the text 'CertAuth' in the field.

10. 导航到Administration > Identity Management > Identity Source Sequences，然后单击Add。

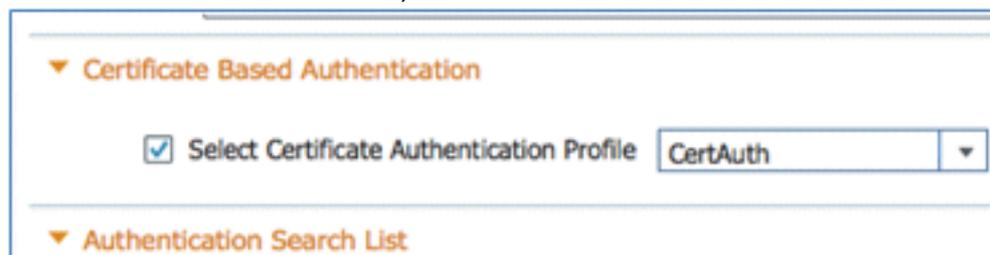


11. 为序列指定名称**TestSequence**（在本例中）。



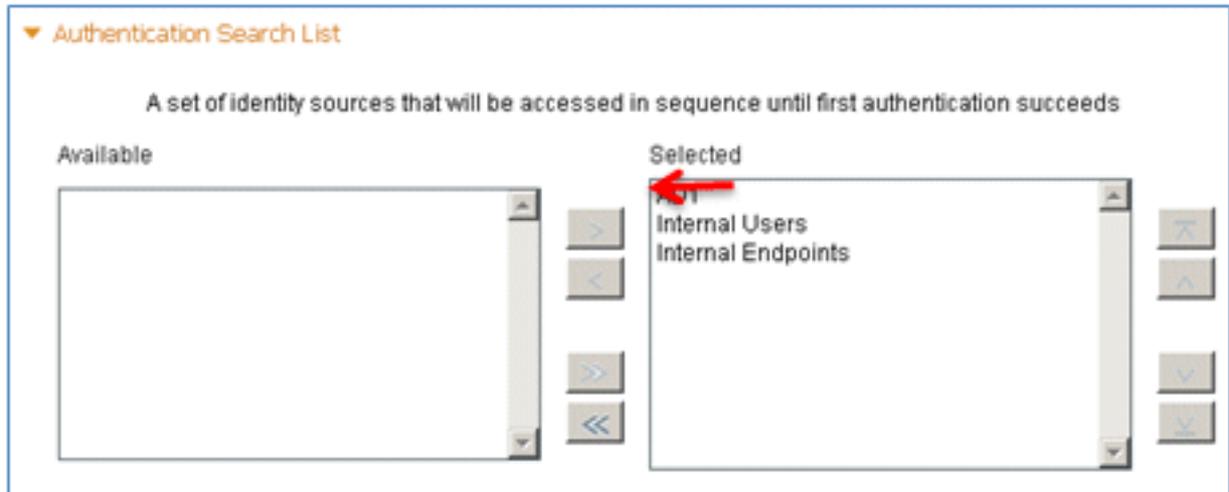
12. 向下滚动到**Certificate Based Authentication**:

启用**Select Certificate Authentication Profile**（复选框处于选中状态）。选择**CertAuth**（或之前创建的其他CAP配置文件）。

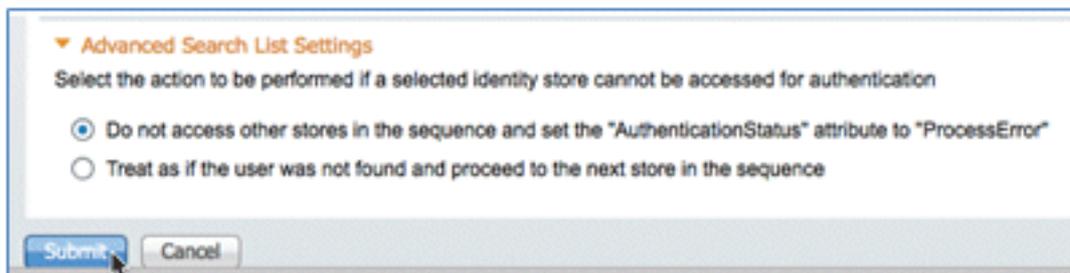


13. 向下滚动到**Authentication Search List**:

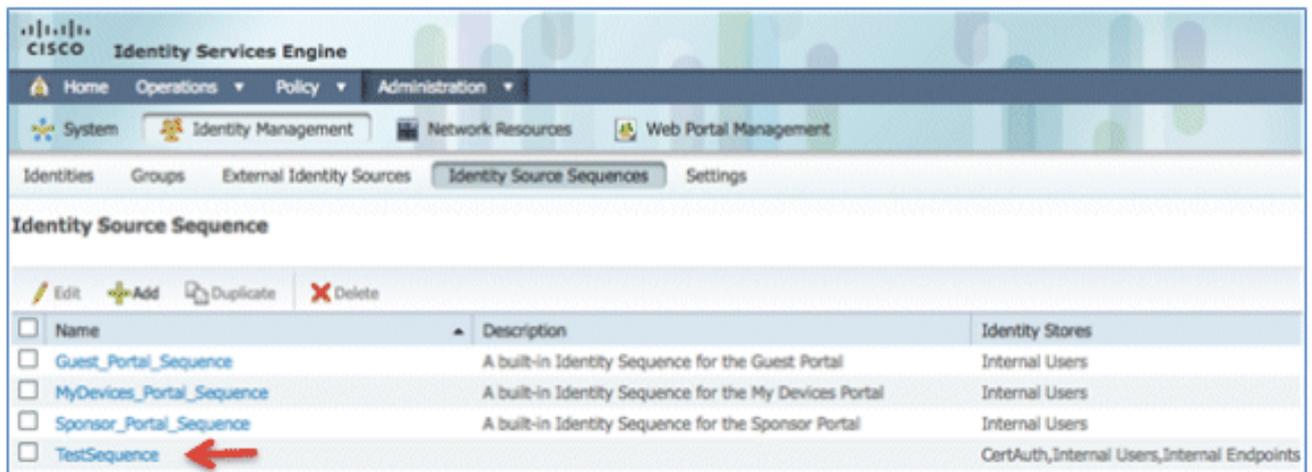
将AD1从“可用”移动到“选定”。点击向上按钮将AD1移至最高优先级。



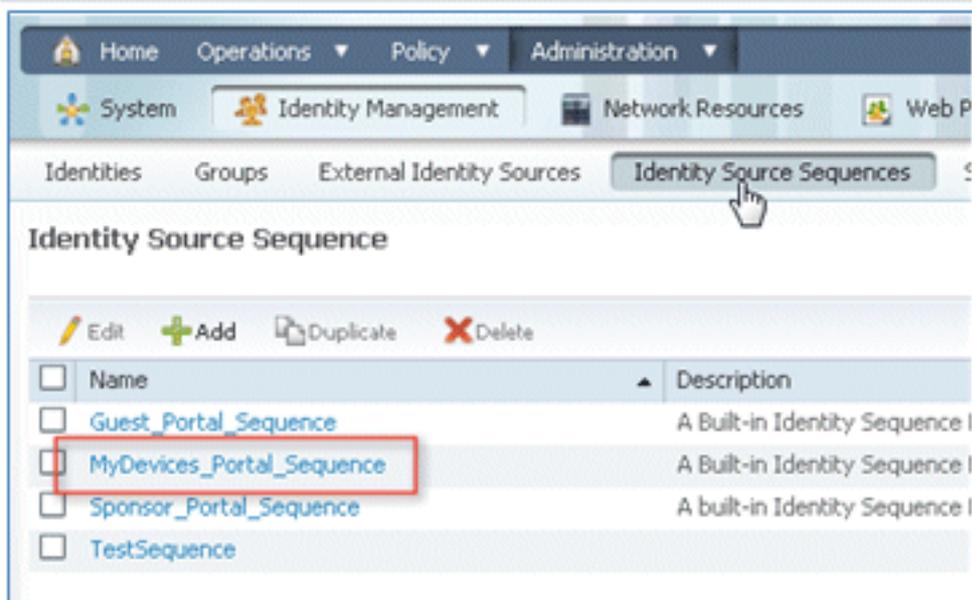
14. 单击Submit进行保存。



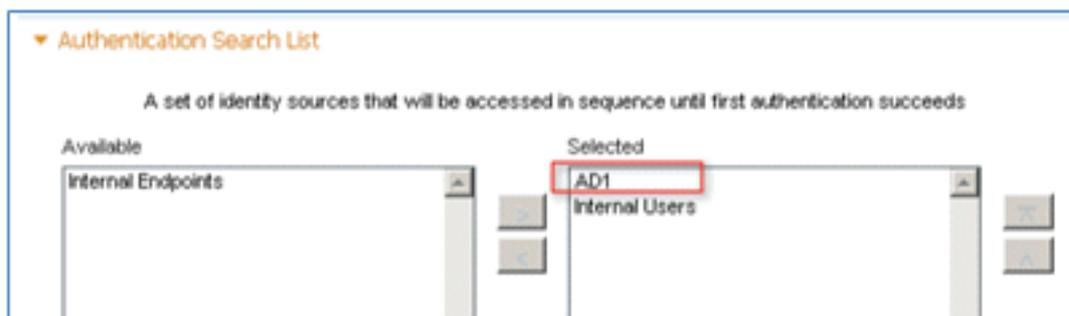
15. 确认已添加新的身份源序列。



16. 使用AD验证我的设备门户。导航到ISE > Administration > Identity Management > Identity Source Sequence，然后编辑MyDevices\_Portal\_Sequence。



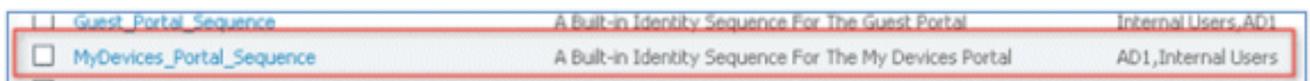
17. 将AD1添加到Selected列表，然后单击up按钮将AD1移动到最高优先级。



18. Click **Save**.



19. 确认MyDevices\_Portal\_Sequence的身份库序列包含AD1。



20. 重复步骤16-19以添加Guest\_Portal\_Sequence的AD1，然后单击**Save**。



21. 确认Guest\_Portal\_Sequence包含AD1。

Name	Description	Identity Stores
Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users,AD1

22. 要将WLC添加到网络接入设备(WLC)，请导航到**管理 > 网络资源 > 网络设备**，然后单击添加。



23. 添加WLC名称、IP地址、子网掩码等。

Network Devices List > New Network Device

### Network Devices

\* Name

Description

---

\* IP Address:  /

---

Model Name

Software Version

---

\* Network Device Group

Location

Device Type

24. 向下滚动到Authentication Settings，然后输入Shared Secret。这必须与WLC RADIUS的共享密钥匹配。

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

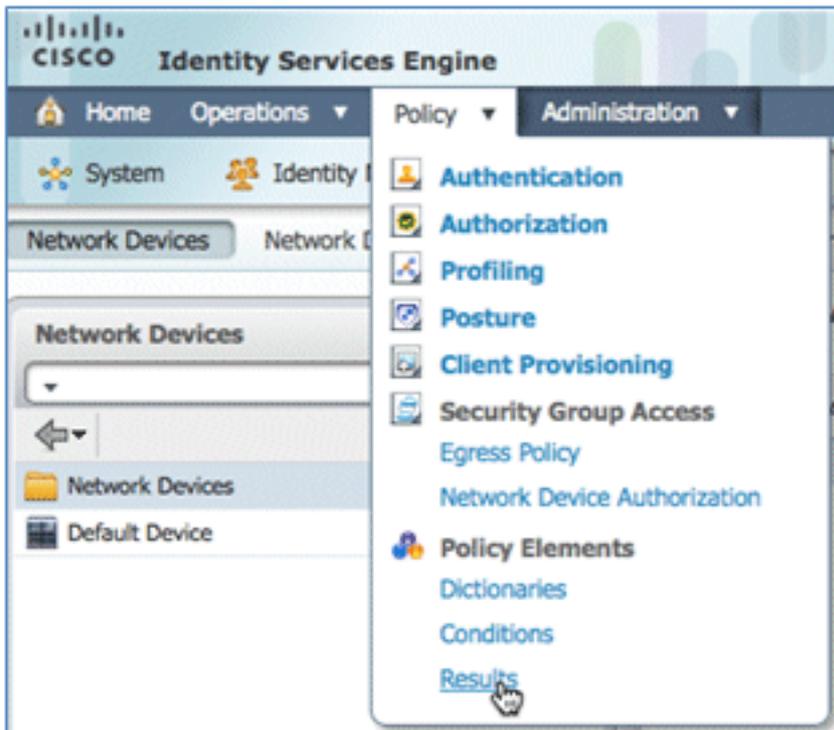
Key Input Format  ASCII  HEXADECIMAL

SNMP Settings

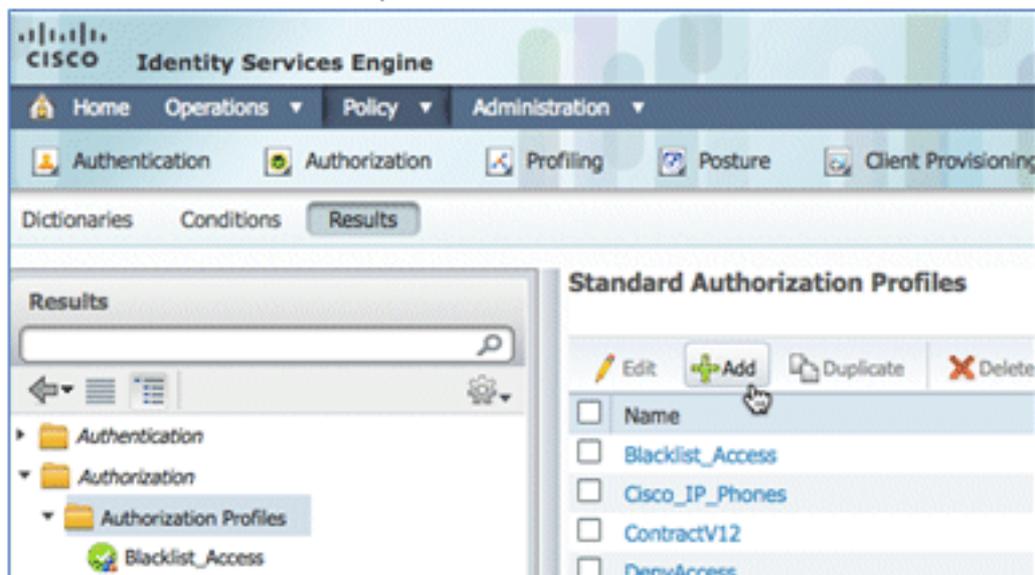
SGA Attributes

25. 单击“Submit”。

26. 导航到ISE > Policy > Policy Elements > Results。



27. 展开Results和Authorization，单击Authorization Profiles，然后单击Add以获取新的配置文件。



28. 为此配置文件指定以下值：

名称：CWA

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name

Description

\* Access Type

启用Web身份验证（选中此框）：

Web身份验证：集中ACL:ACL-REDIRECT（必须与WLC预身份验证ACL名称匹配。）重定向：默认

Common Tasks

DACL Name

VLAN

Voice Domain Permission

Web Authentication  ACL  Redirect

29. 单击Submit，并确认已添加CWA授权配置文件。

### Standard Authorization Profiles

Edit Add Duplicate Delete

<input type="checkbox"/>	Name
<input type="checkbox"/>	Blacklist_Access
<input type="checkbox"/>	CWA
<input type="checkbox"/>	Cisco_IP_Phones

30. 单击Add以创建新的授权配置文件。

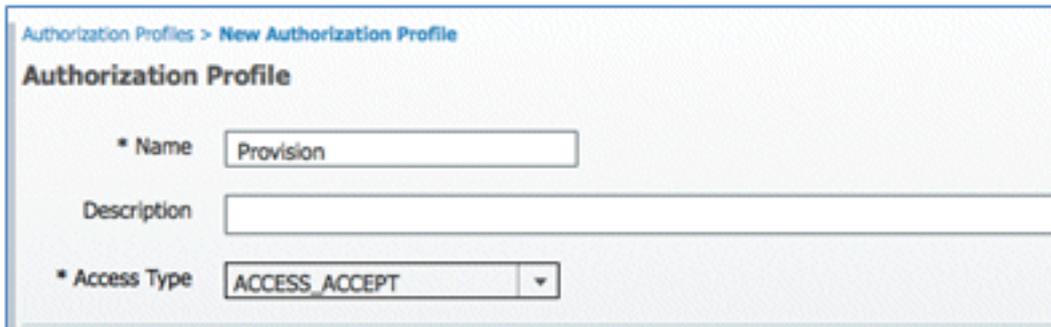
### Standard Authorization Profiles

Edit Add Duplicate Delete

<input type="checkbox"/>	Name
<input type="checkbox"/>	Blacklist_Access
<input type="checkbox"/>	CWA
<input type="checkbox"/>	Cisco_IP_Phones

31. 为此配置文件指定以下值：

名称：调配



Authorization Profiles > New Authorization Profile

### Authorization Profile

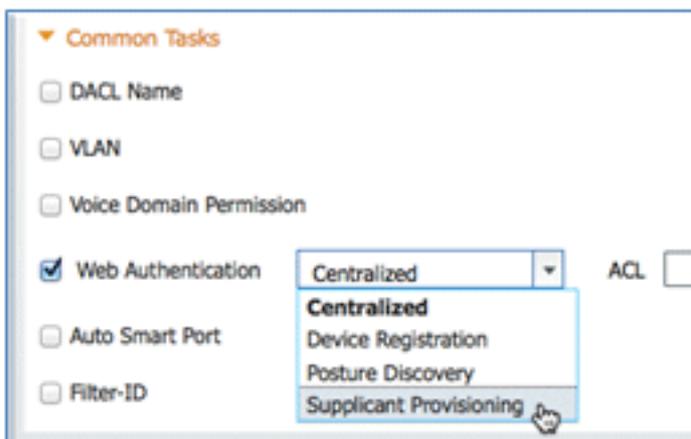
\* Name

Description

\* Access Type

启用Web身份验证（选中此框）：

Web身份验证值：请求方调配



Common Tasks

DACL Name

VLAN

Voice Domain Permission

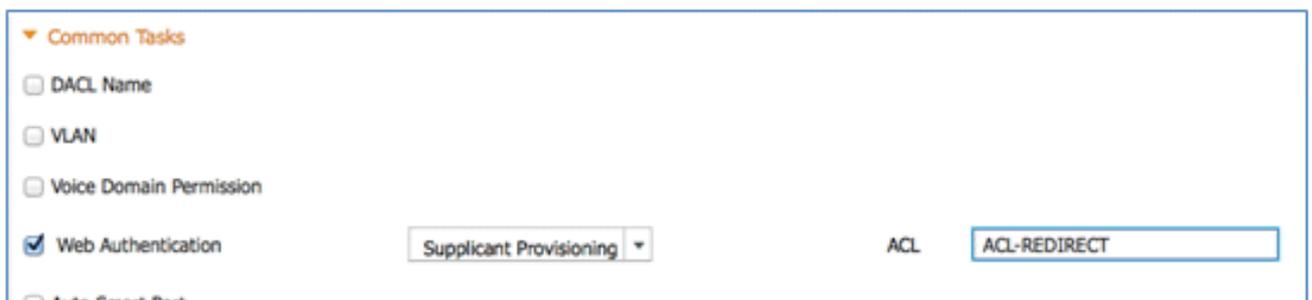
Web Authentication  ACL

Auto Smart Port

Filter-ID

Centralized  
Device Registration  
Posture Discovery  
Supplicant Provisioning

ACL:ACL-REDIRECT（必须与WLC预身份验证ACL名称匹配。）



Common Tasks

DACL Name

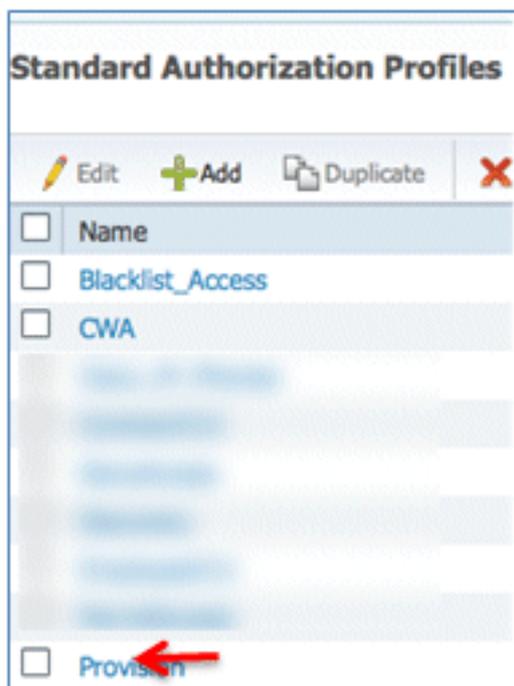
VLAN

Voice Domain Permission

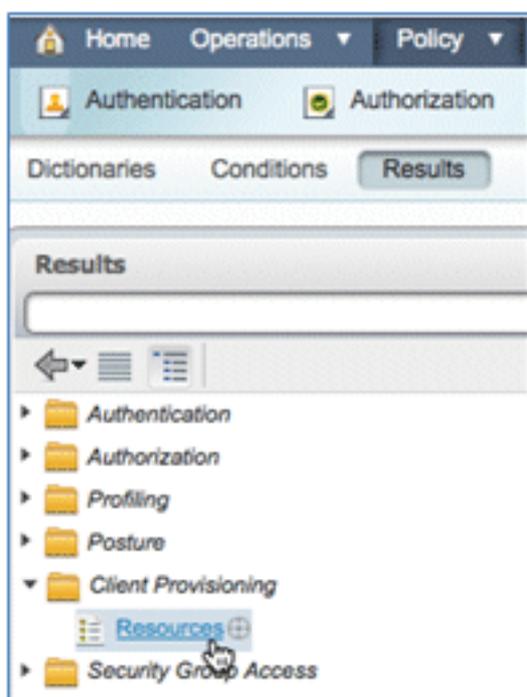
Web Authentication  ACL

Auto Smart Port

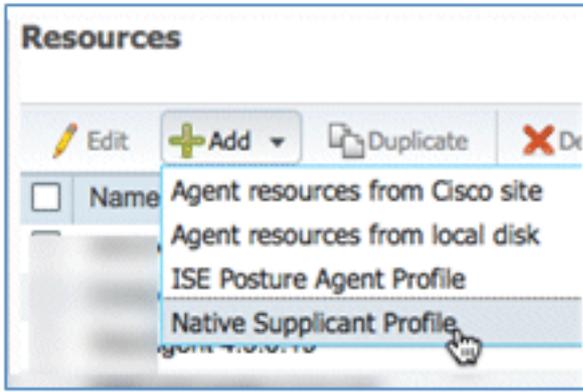
32. 单击Submit，并确认已添加调配授权配置文件。



33. 在Results ( 结果 ) 中向下滚动 , 展开Client Provisioning , 然后单击Resources。



34. 选择Native Supplicant Profile。



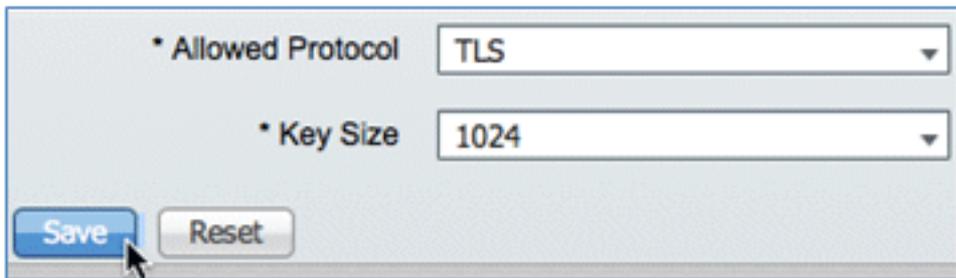
35. 为配置文件指定名称**WirelessSP**（在本例中）。

36. 输入以下值：

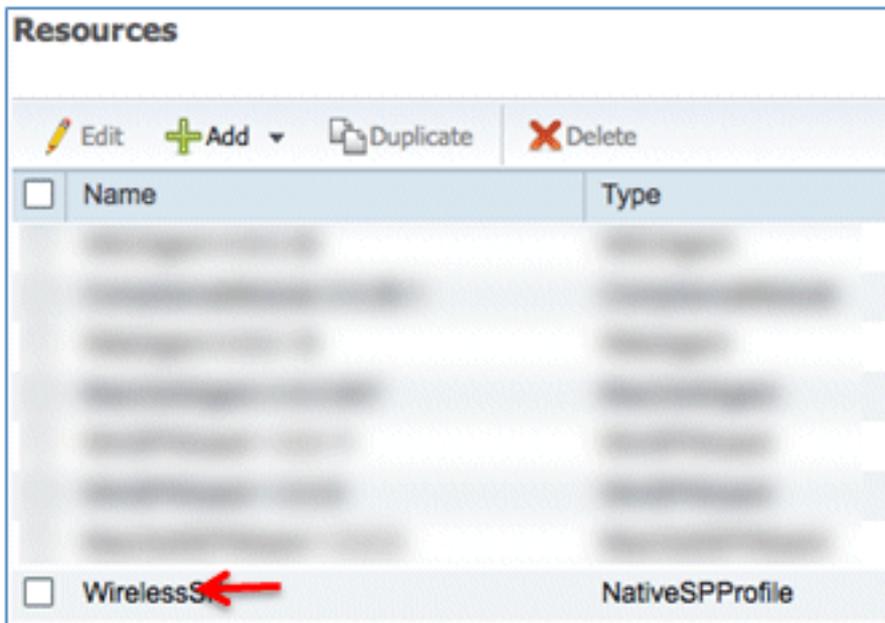
连接类型：无线 SSID: **Demo1x**（此值来自 WLC 802.1x WLAN 配置）允许的协议：**TLS** 密钥大小：**1024**

37. 单击“Submit”。

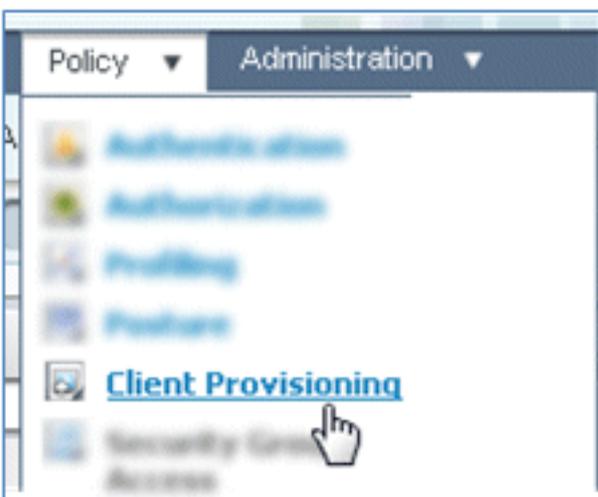
38. Click **Save**.



39. 确认已添加新配置文件。

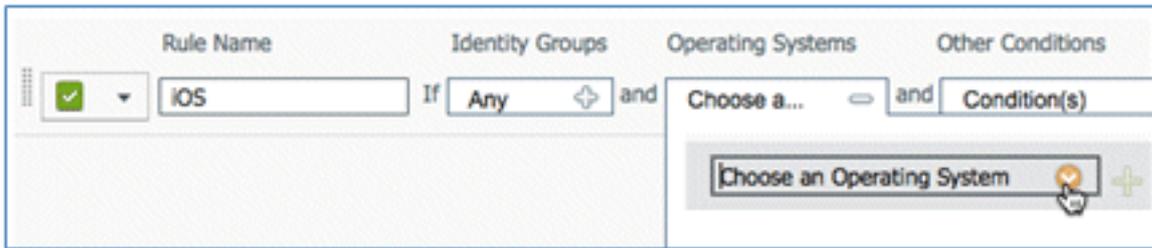


40. 导航到策略 > 客户端调配。



41. 为iOS设备的调配规则输入以下值：

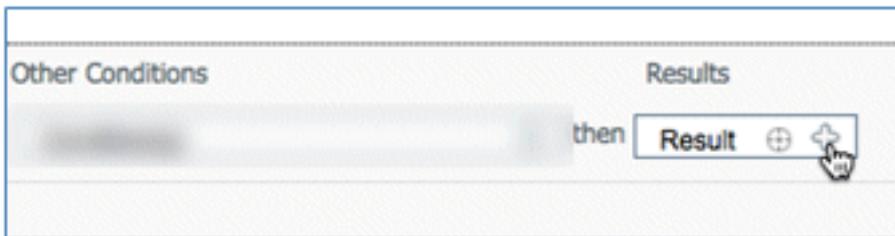
规则名称：iOS身份组：任意



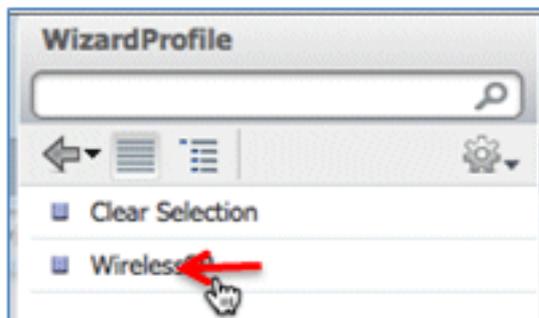
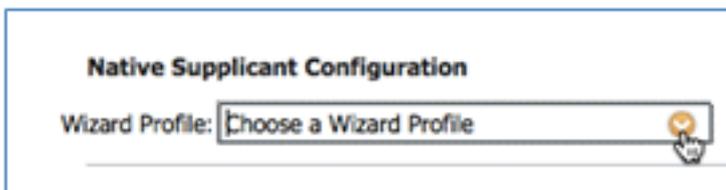
操作系统：Mac iOS All



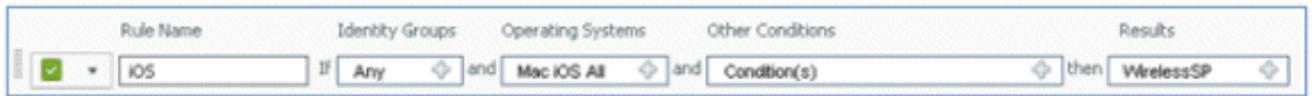
结果：WirelessSP（这是之前创建的本地请求方配置文件）



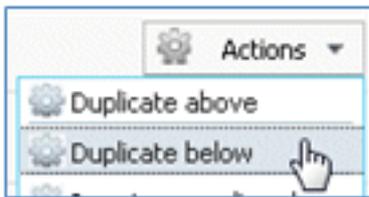
导航到结果 > 向导配置文件（下拉列表）> WirelessSP。



42. 确认已添加iOS调配配置文件。



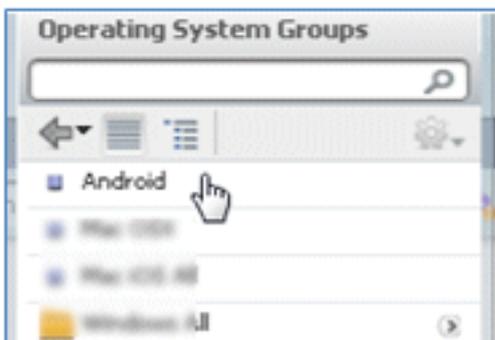
43. 在第一个规则的右侧，找到Actions下拉列表，然后选择**Duplicate below**(或above)。



44. 将新规则的名称更改为**Android**。

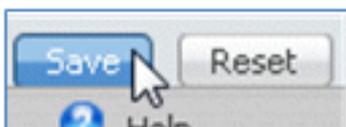


45. 将操作系统更改为**Android**。

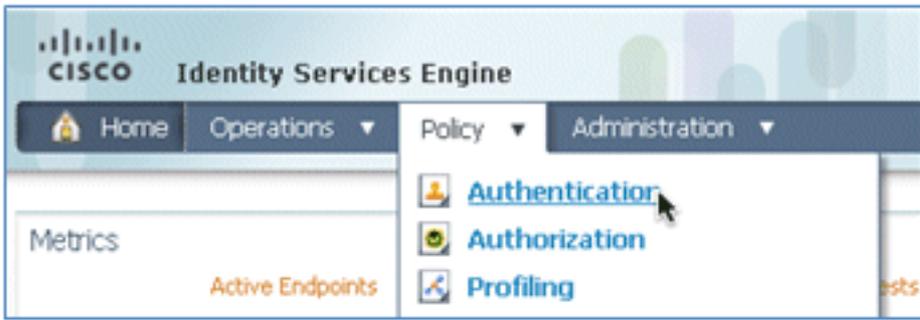


46. 保留其他值不变。

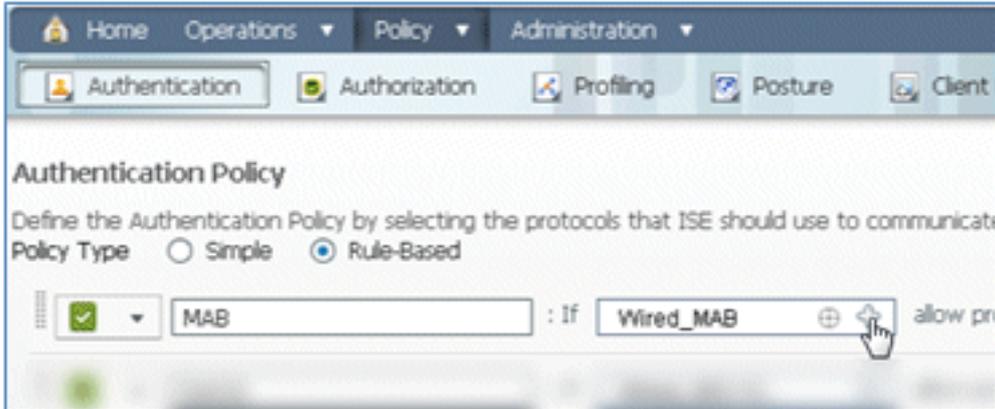
47. 单击**Save** ( 左下屏幕 ) 。



48. 导航到**ISE > Policy > Authentication**。



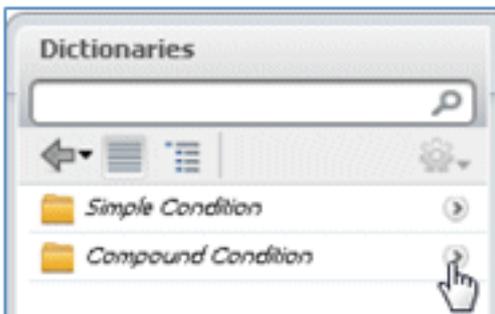
49. 修改条件以包括Wireless\_MAB，然后展开Wired\_MAB。



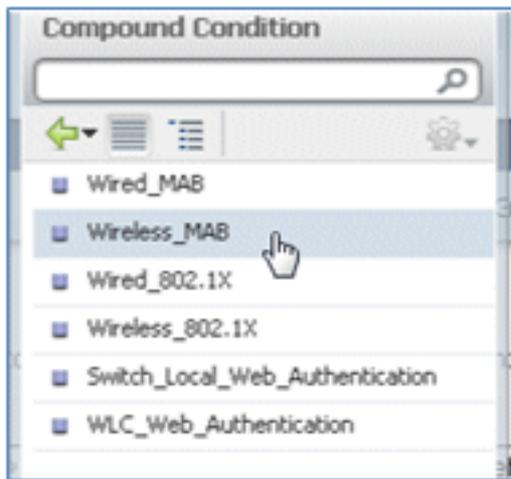
50. 单击Condition Name下拉列表。



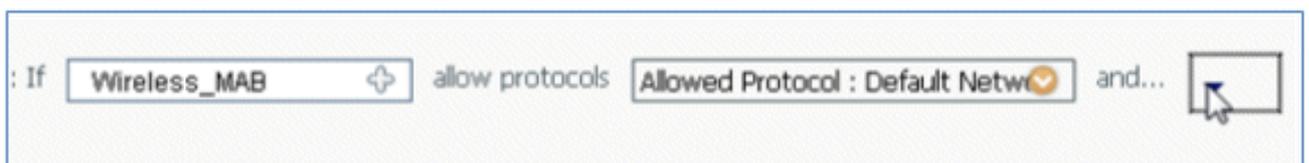
51. 选择Dictionaries > Compound Condition。



52. 选择Wireless\_MAB。

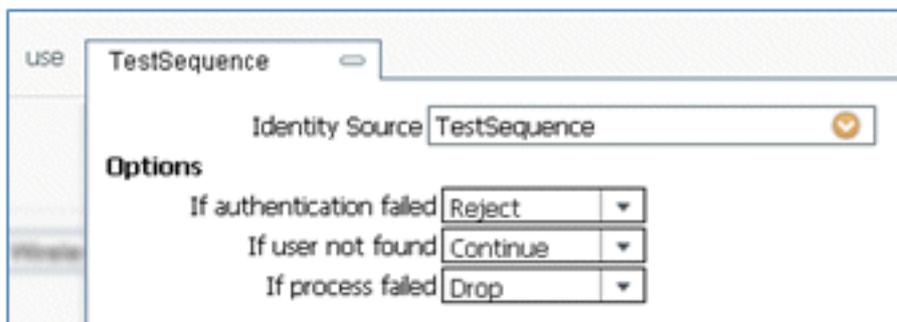


53. 在规则右侧，选择要展开的箭头。

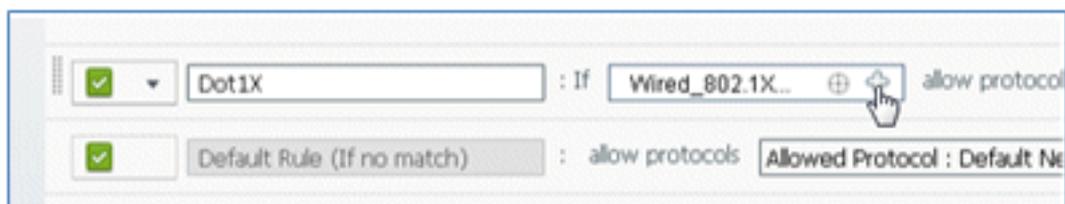


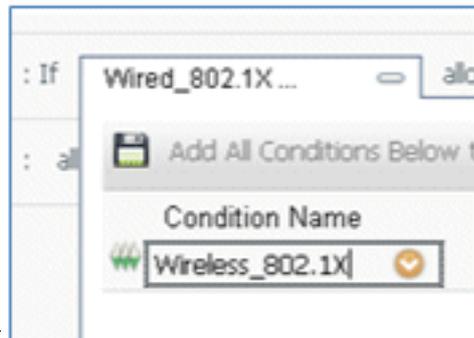
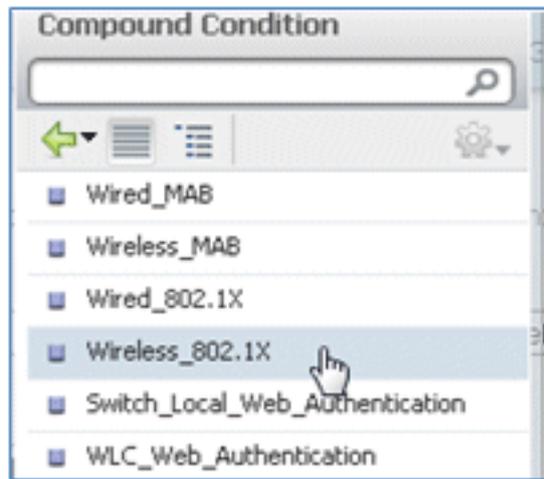
54. 从下拉列表中选择以下值：

身份源：**TestSequence**（这是之前创建的值）如果身份验证失败：**拒绝**如果找不到用户：**继续**如果进程失败：**丢弃**



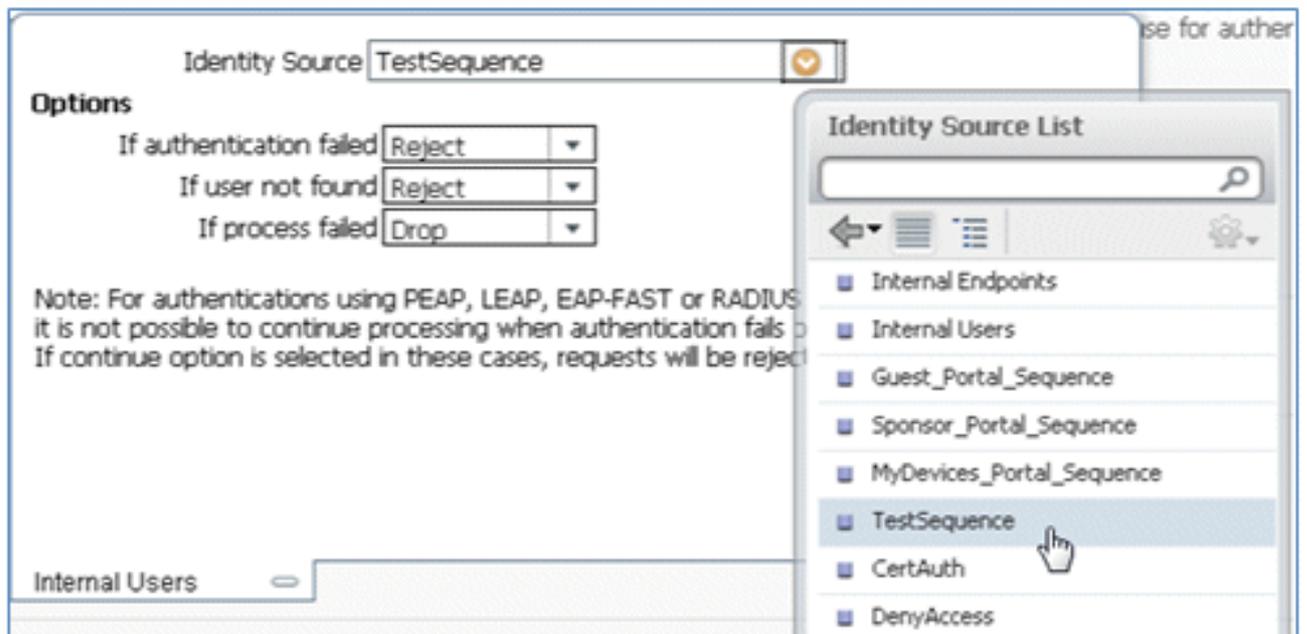
55. 转到Dot1X规则，然后更改以下值：





条件:Wireless\_802.1X

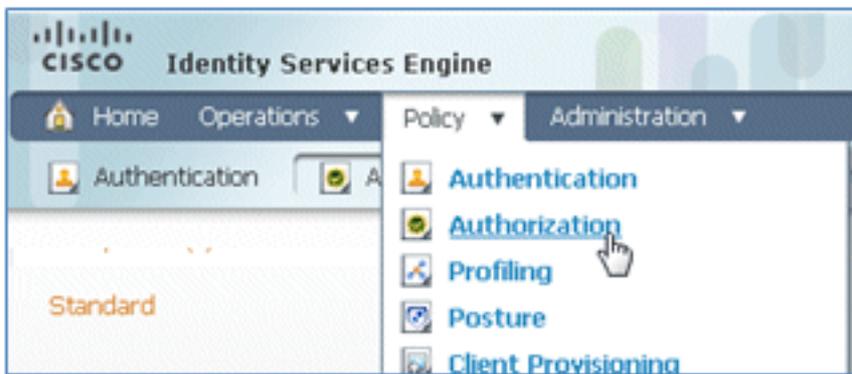
身份源 : TestSequence



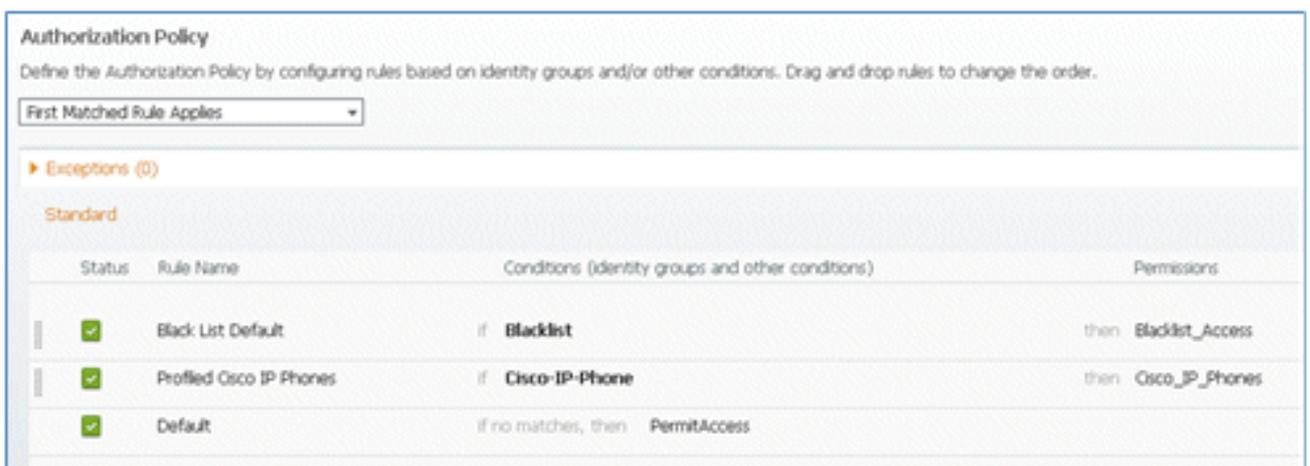
56. Click **Save**.



57. 导航到ISE > Policy > Authorization。



58. 默认规则（例如Black List Default、Profiled和Default）已在安装中配置；前两个规则可以忽略；默认规则将在以后进行编辑。



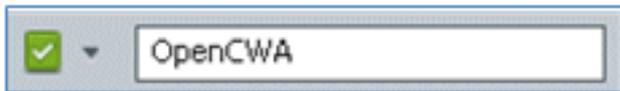
59. 在第二条规则（已分析的思科IP电话）的右侧，点击编辑旁边的向下箭头，然后选择**Insert New Rule Below**。



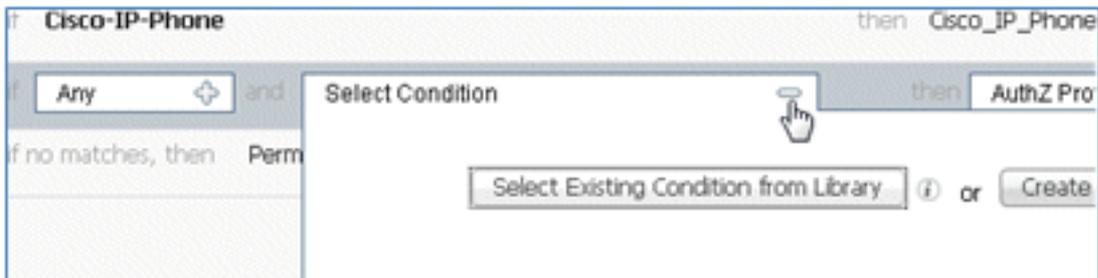
添加新的标准规则编号。



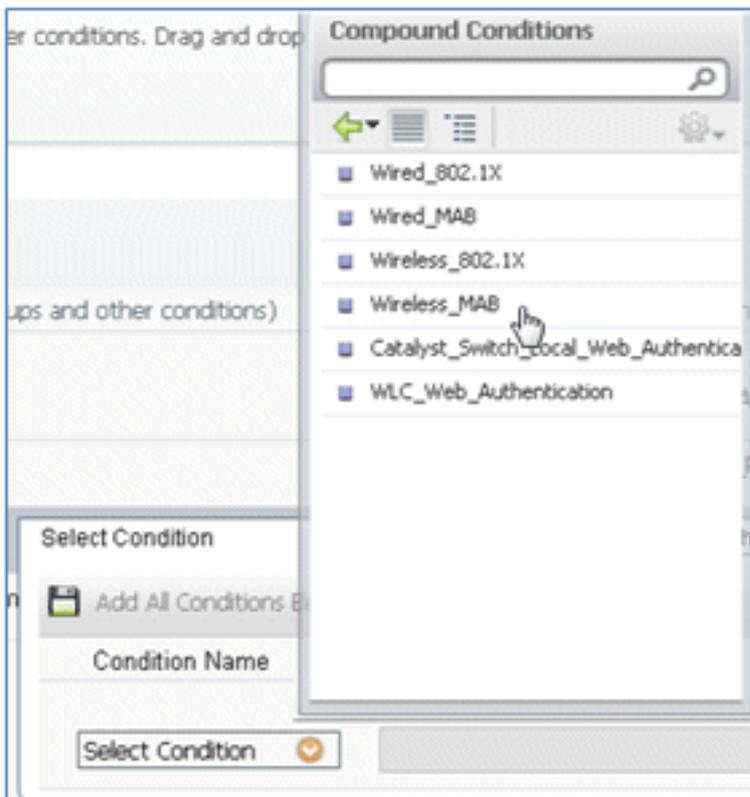
60. 将Rule Name从Standard Rule #更改为**OpenCWA**。此规则在开放式WLAN（双SSID）上为进入访客网络的用户启动注册过程，以便调配设备。



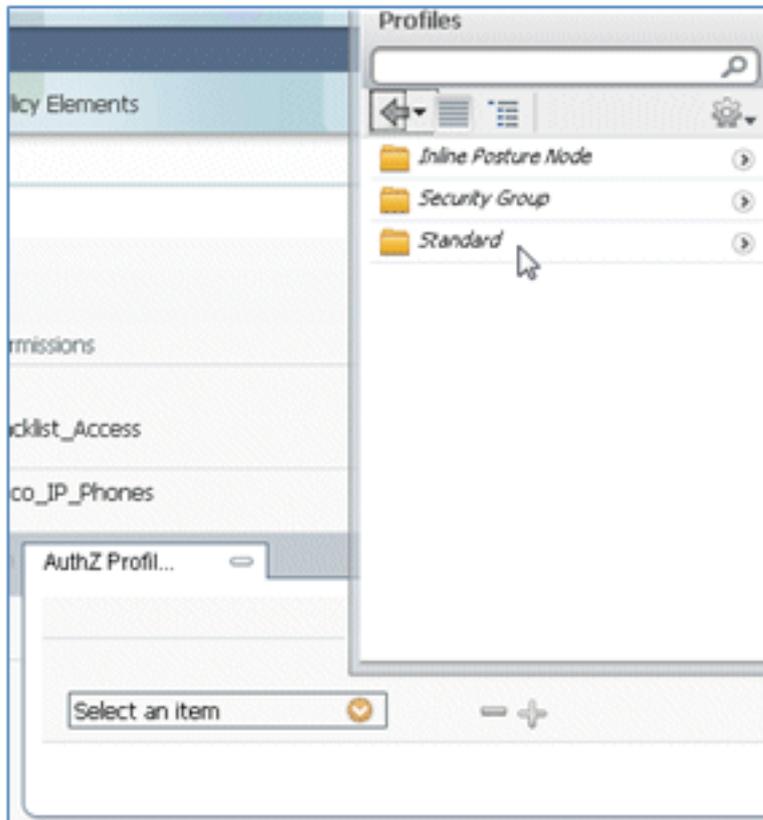
61. 单击“条件”的加号(+), 然后单击“从库中选择现有条件”(Select Existing Condition from Library)。



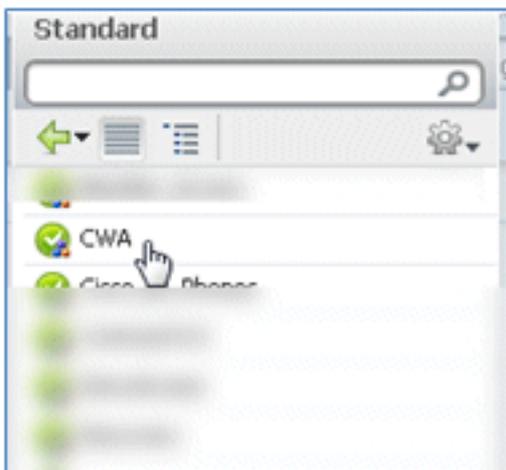
62. 选择复合条件 > Wireless\_MAB。



63. 在AuthZ配置文件中，点击加号(+), 然后选择Standard。



64. 选择标准CWA ( 这是之前创建的授权配置文件 ) 。



65. 确认添加的规则具有正确的条件和授权。



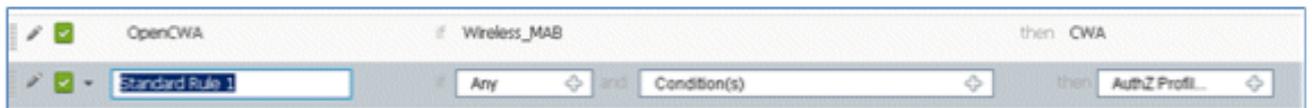
66. 单击Done ( 在规则的右侧 ) 。



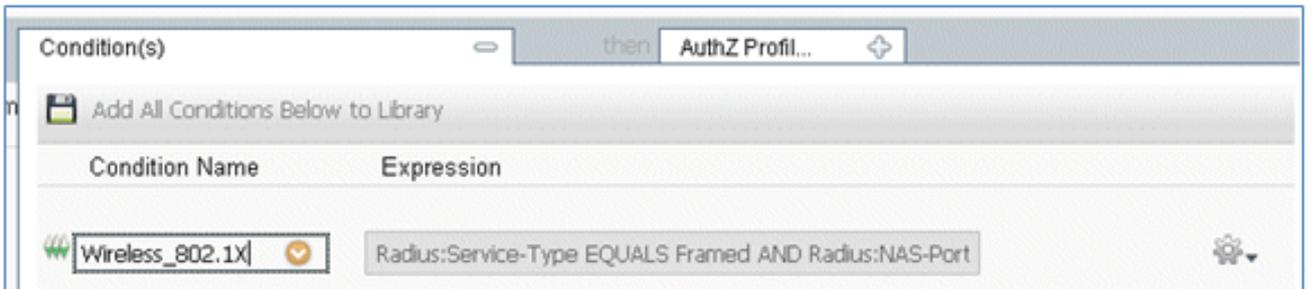
67. 在同一规则的右侧，点击Edit旁边的向下箭头，然后选择Insert New Rule Below。



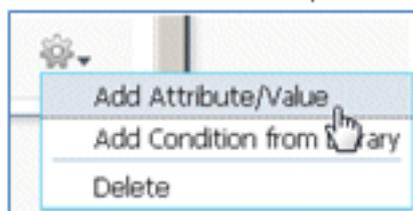
68. 将Rule Name从Standard Rule #更改为**PEAPrule** ( 在本例中 )。此规则用于PEAP ( 也用于单SSID方案 ) 检查没有传输层安全(TLS)的802.1X身份验证，并且网络请求方调配由之前创建的调配授权配置文件启动。



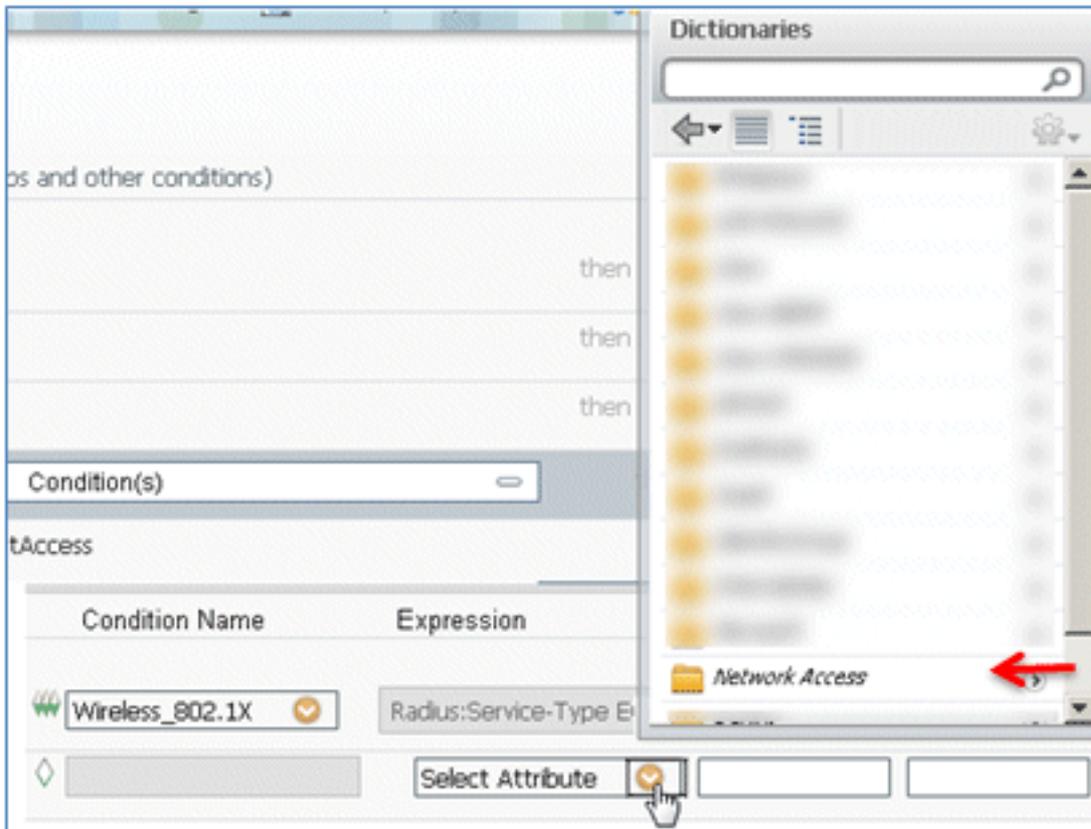
69. 将Condition ( 条件 ) 更改为**Wireless\_802.1X**。



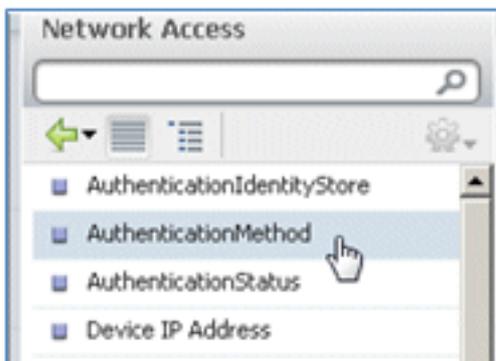
70. 单击条件右侧的齿轮图标，然后选择**添加属性/值**。这是一个“and”条件，而不是“or”条件。



71. 找到并选择**Network Access**。



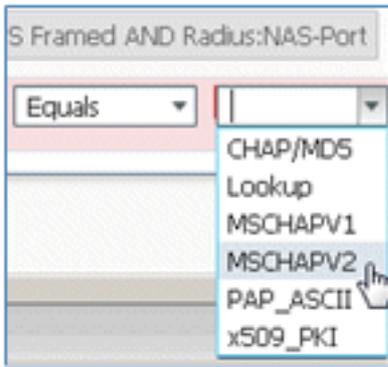
72. 选择**AuthenticationMethod**，然后输入以下值：



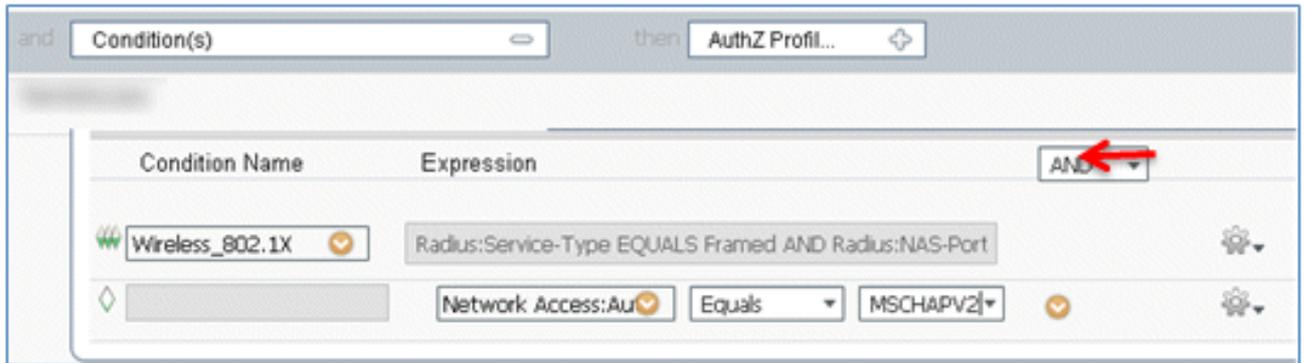
AuthenticationMethod:等于



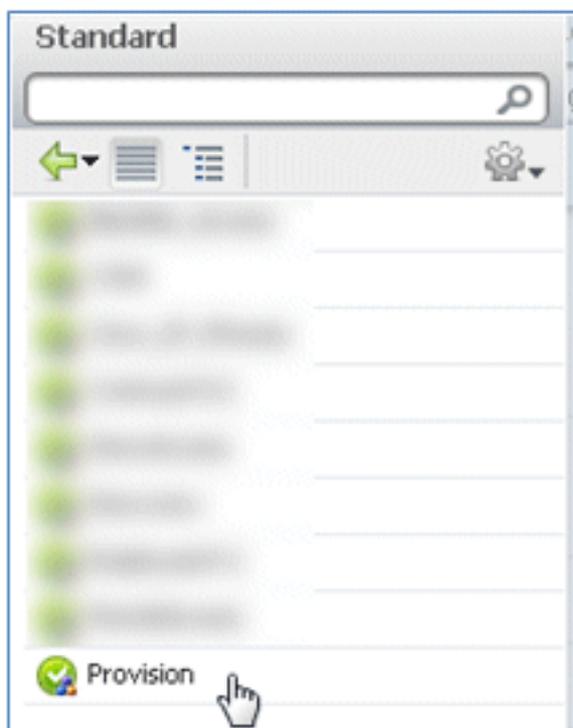
选择**MSCHAPV2**。



这是规则的示例；请务必确认Condition为AND。



73. 在AuthZ Profile中，选择**Standard > Provision**（这是之前创建的授权配置文件）。



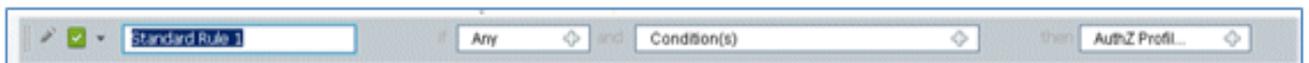
74. 单击**Done**。



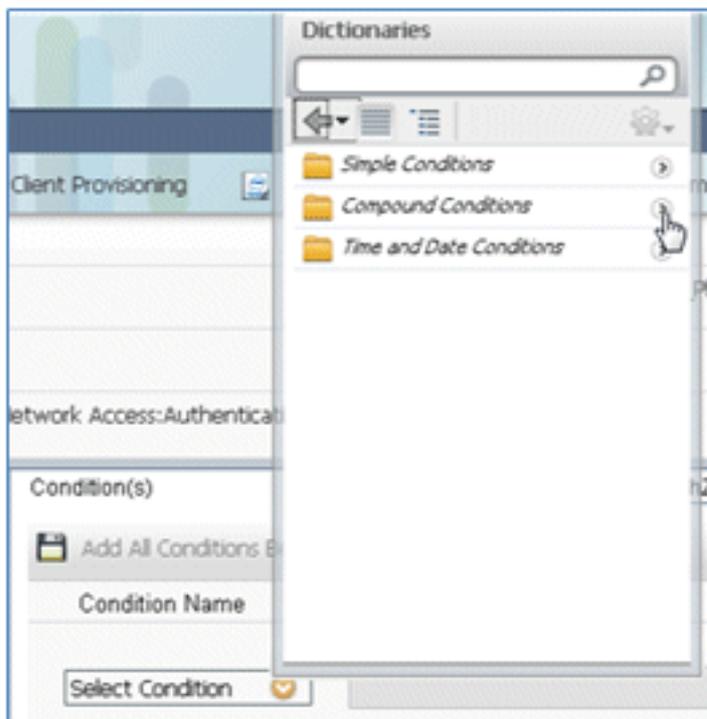
75. 在PEAPrule的右侧，点击Edit旁边的向下箭头，然后选择**Insert New Rule Below**。



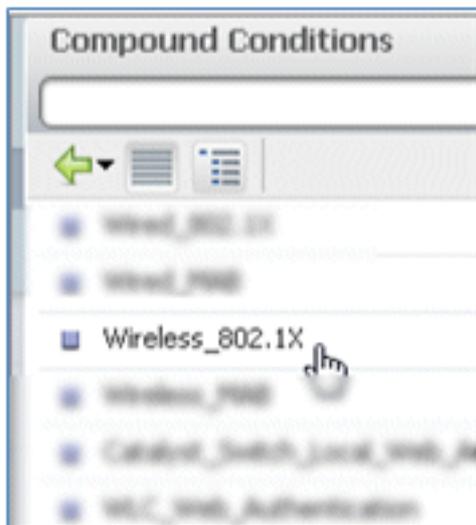
76. 将Rule Name从Standard Rule #更改为**AllowRule**（在本例中）。此规则将用于允许访问安装了证书的已注册设备。



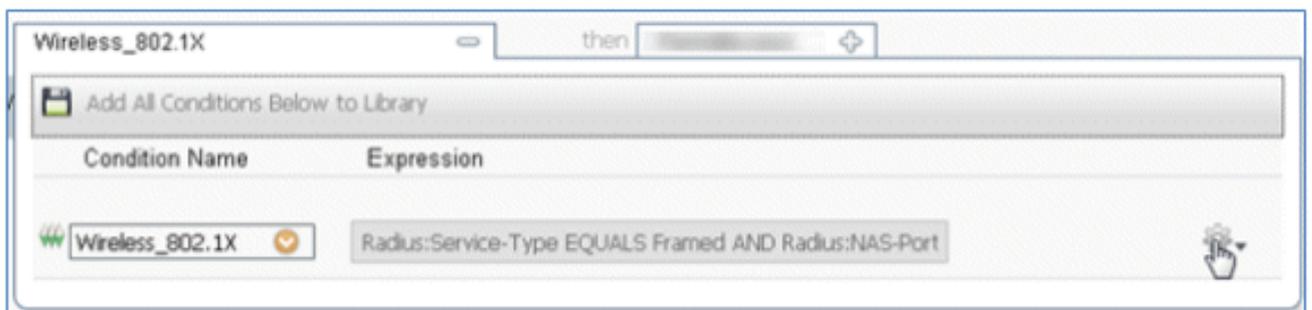
77. 在Conditions(s)下，选择**Compound Conditions**。



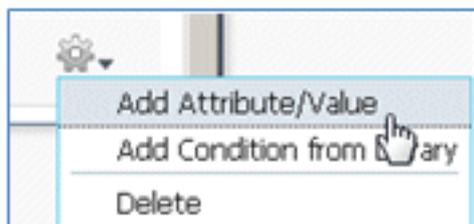
78. 选择**Wireless\_802.1X**。



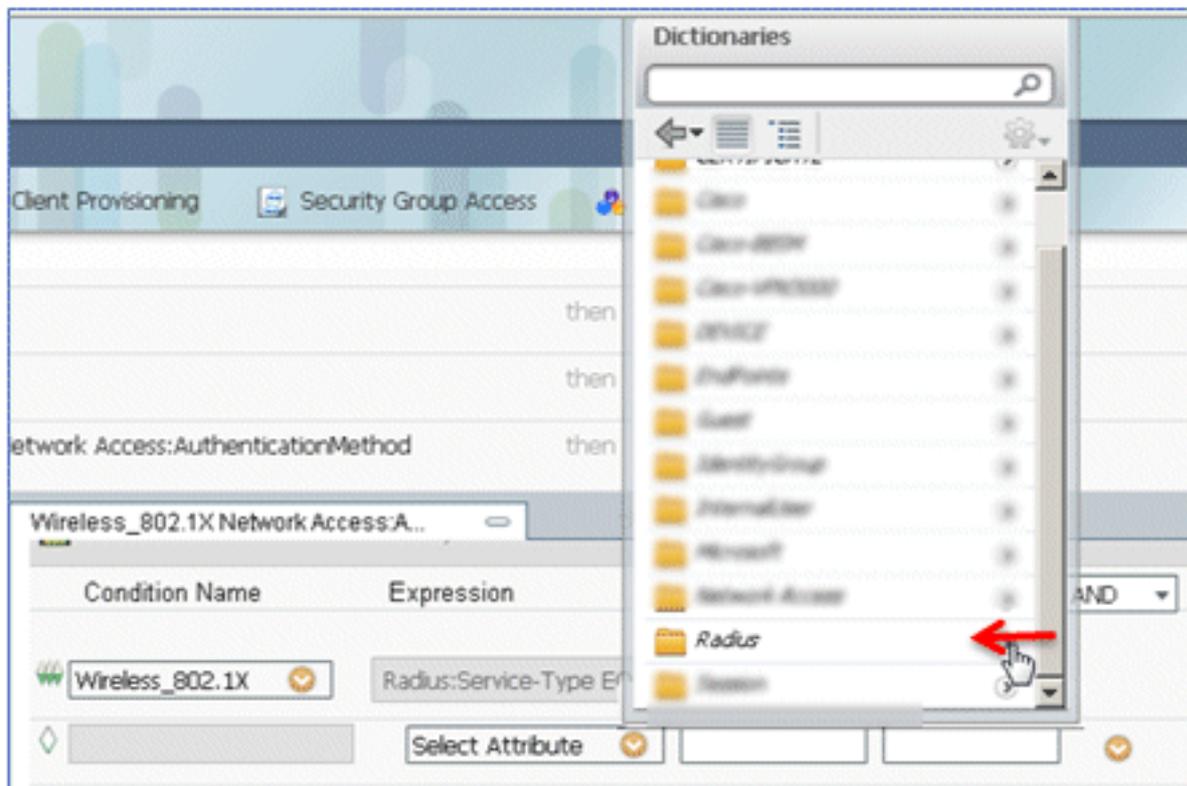
79. 添加AND属性。



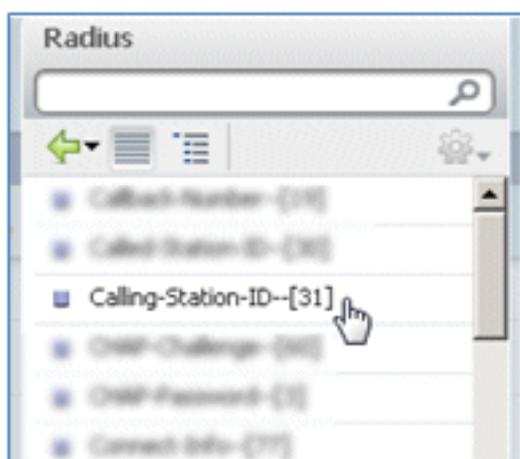
80. 单击条件右侧的齿轮图标，然后选择添加属性/值。



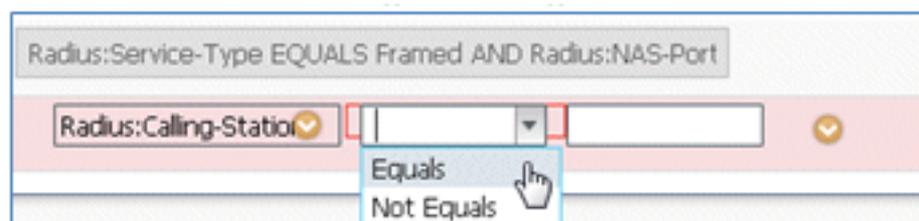
81. 找到并选择Radius。



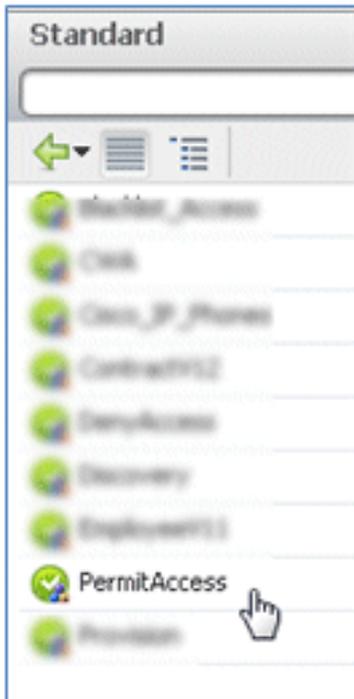
82. 选择Calling-Station-ID--[31]。



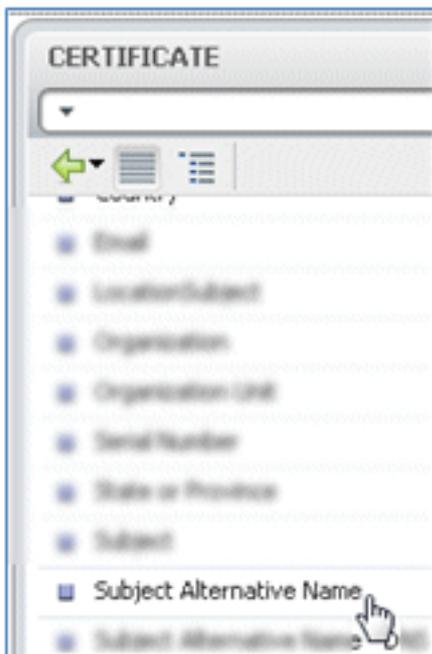
83. 选择Equals。



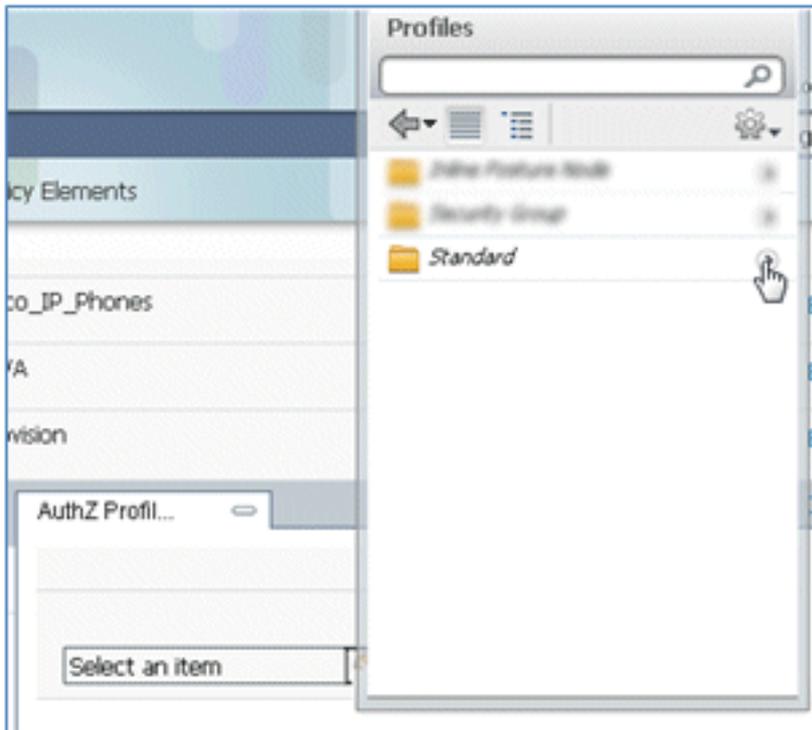
84. 转到CERTIFICATE，然后单击向右箭头。



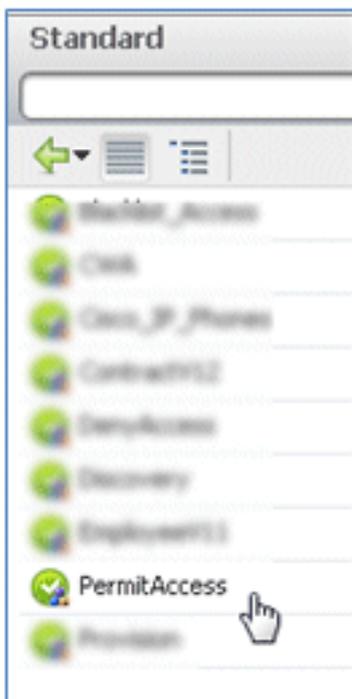
85. 选择Subject Alternative Name。



86. 对于授权配置文件，请选择标准。



87. 选择允许访问。



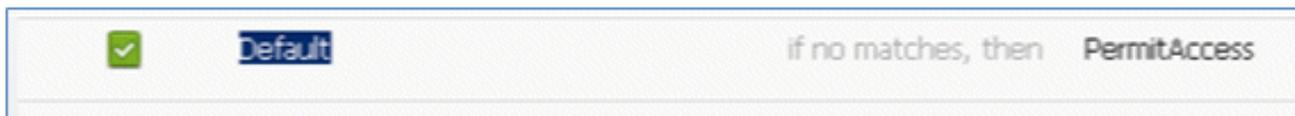
88. 单击Done。



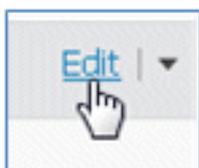
以下是规则示例：

	OpenCMA	Wireless_M40	then: Deny
	PermitRule	Wireless_802.1X (1): Network Access:AuthenticationMethod EQUALS RADIUS(2)	then: Permit
	AllowRule	Wireless_802.1X Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name	then: PermitAccess

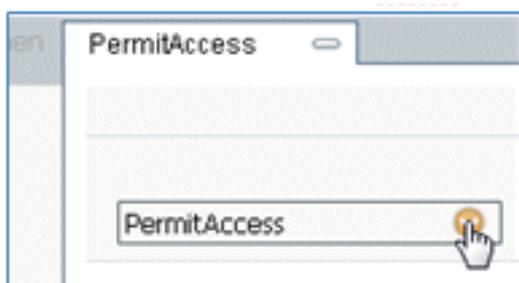
89. 找到Default规则以将PermitAccess更改为DenyAccess。



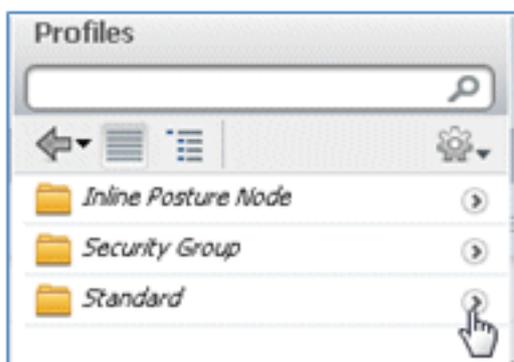
90. 单击Edit以编辑Default规则。



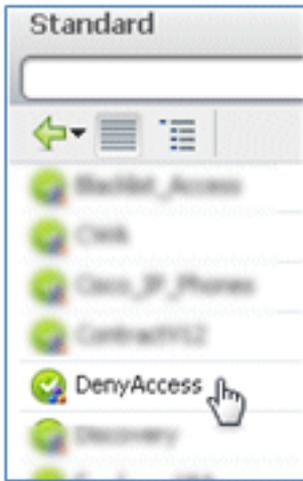
91. 转到PermitAccess的现有授权配置文件。



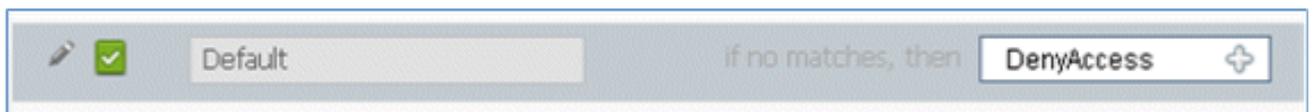
92. 选择Standard。



93. 选择DenyAccess。



94. 如果找不到匹配项，请确认Default规则具有DenyAccess。



95. 单击Done。



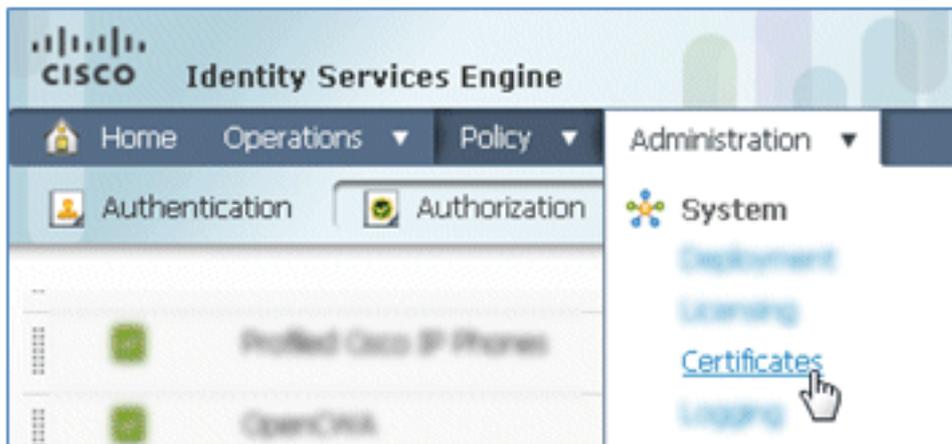
这是此测试所需的主要规则的示例；适用于单SSID或双SSID场景。

<input checked="" type="checkbox"/>	OpenCWA	if Wireless_MAB	then CWA
<input checked="" type="checkbox"/>	PEAPRule	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 )	then Provision
<input checked="" type="checkbox"/>	AllowRule	if (Wireless_802.1X AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name )	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

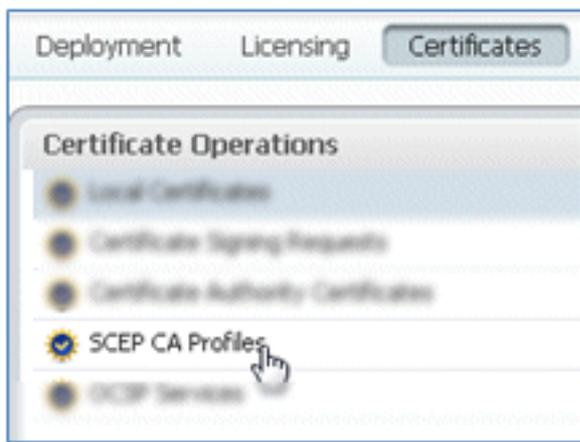
96. Click **Save**.



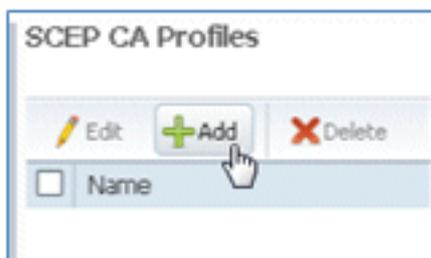
97. 导航到ISE > Administration > System > Certificates，以便使用SCEP配置文件配置ISE服务器。



98. 在Certificate Operations中，单击SCEP CA Profiles。



99. 单击 Add。



100. 为此配置文件输入以下值：

名称：mySCEP（在本示例中）URL: <https://<ca-server>/CertSrv/mscep/>（请检查CA服务器配置中的正确地址。）

SEP Certificate Authority Certificates > New SCEP Profile

Edit Certificate

SEP Certificate Authority

\* Name

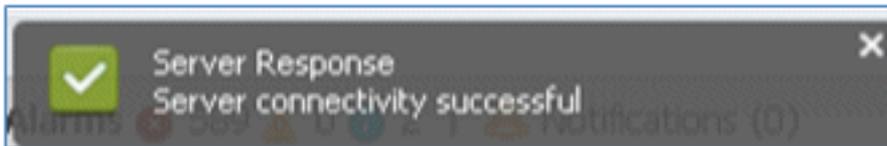
Description

\* URL

101. 单击**测试连接**以测试SCEP连接的连接。



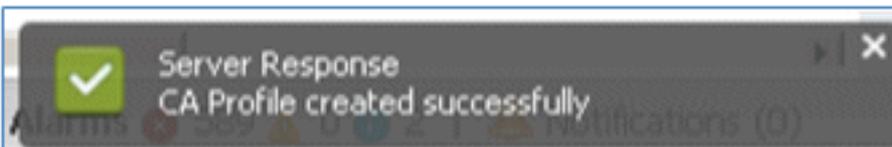
102. 此响应显示服务器连接成功。



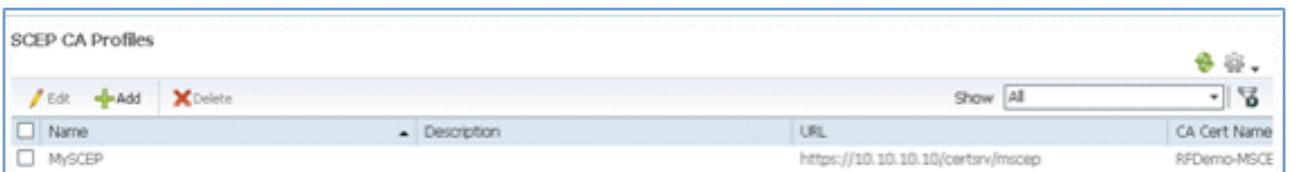
103. 单击“Submit”。



104. 服务器响应已成功创建CA配置文件。



105. 确认已添加SCEP CA配置文件。



## 用户体验 — 调配iOS

### 双SSID

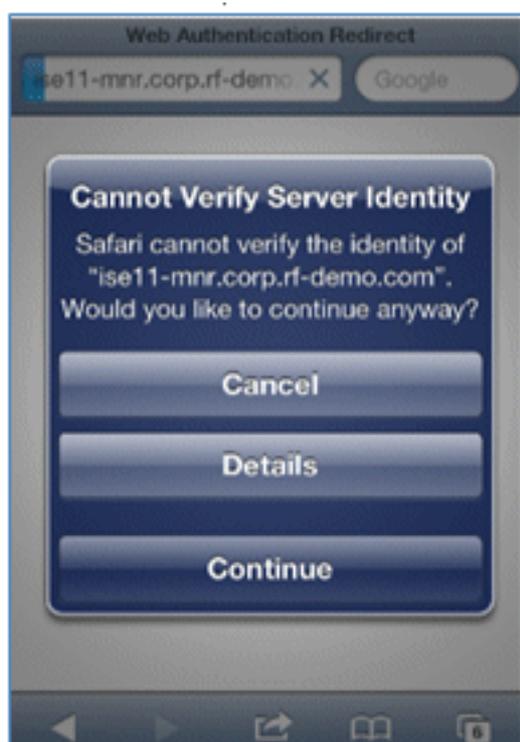
本节介绍双SSID，并介绍如何连接到要调配的访客，以及如何连接到802.1x WLAN。

完成以下步骤，以便在双SSID场景中调配iOS:

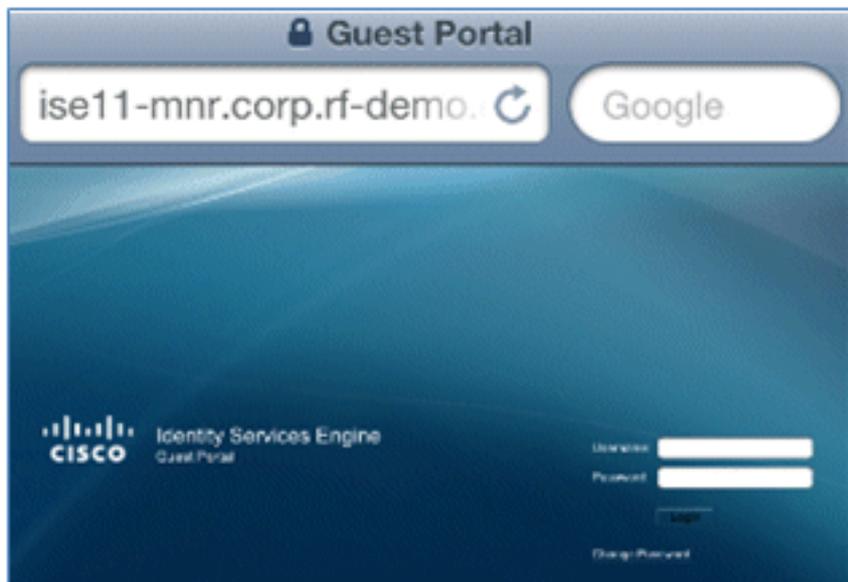
1. 在iOS设备上，转到**Wi-Fi Networks**，然后选择**DemoCWA**（在WLC上配置了开放式WLAN）。



2. 在iOS设备上打开Safari浏览器，并访问可访问的URL（例如，内部/外部Web服务器）。ISE会将您重定向到门户。单击 **Continue**。



3. 您将重定向到访客门户进行登录。



4. 使用AD用户帐户和密码登录。出现提示时，安装CA配置文件。



5. 单击Install CA服务器的受信任证书。



6. 配置文件安装完成后，单击Done。



7. 返回浏览器，然后单击**Register**。记下包含设备MAC地址的设备ID。



8. 单击**Install**以安装已验证的配置文件。



9. 单击Install Now。



10. 完成此过程后，WirelessSP配置文件确认已安装该配置文件。单击Done。



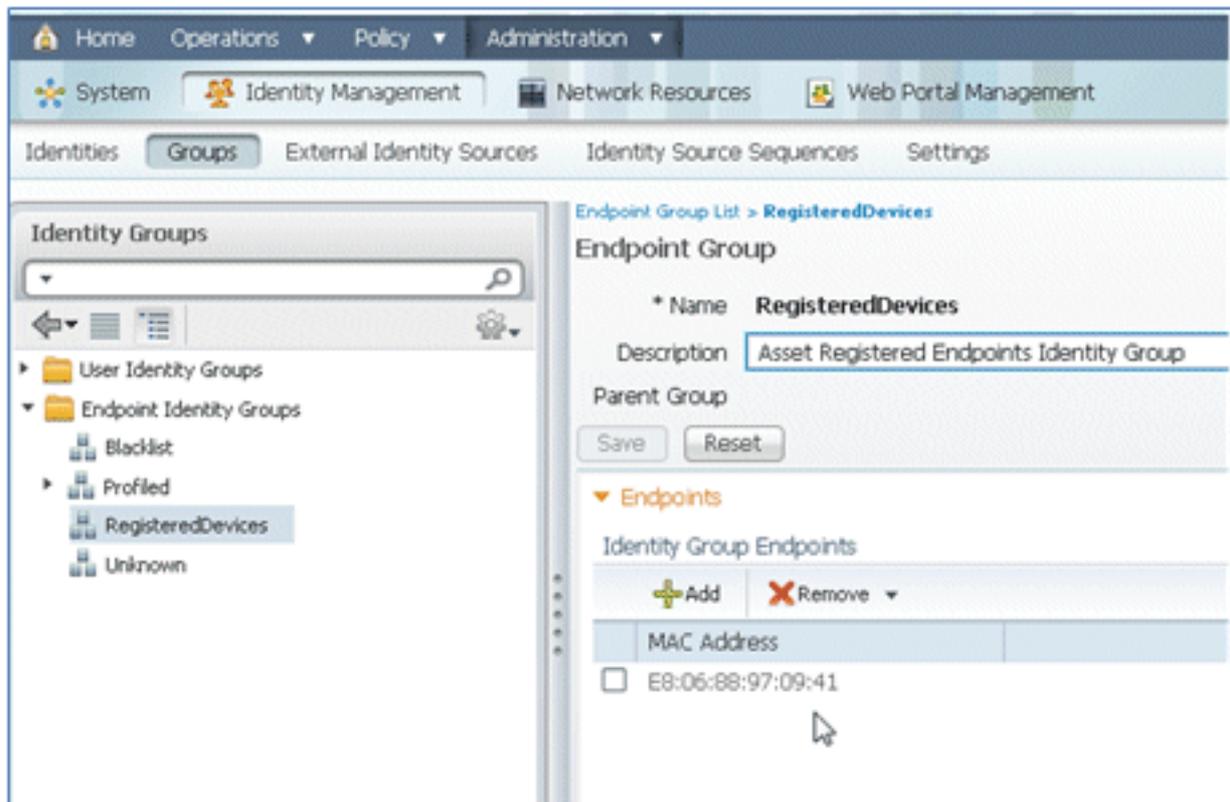
11. 转到Wi-Fi网络，将网络更改为**Demo1x**。您的设备现已连接并使用TLS。



12. 在ISE上，导航到**操作 > 身份验证**。事件显示设备连接到开放访客网络的过程，通过请求方调配完成注册过程，并在注册后允许访问。

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12 12:27:57.052 AM	✓	🔒	paul	EE-06-80-97-09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12 12:27:21.714 AM	✓	🔒	EE-06-80-97-09-41	EE-06-80-97-09-41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12 12:27:20.438 AM	✓	🔒			WLC				Dynamic Authorization succeeded
Mar 25, 12 12:26:56.187 AM	✓	🔒	paul	EE-06-80-97-09-41	WLC	CWA	Any-Profiled-Apple-iPad	Pending	

13. 导航至ISE >管理>身份管理> **Groups > Endpoint Identity Groups > RegisteredDevices**。MAC地址已添加到数据库。

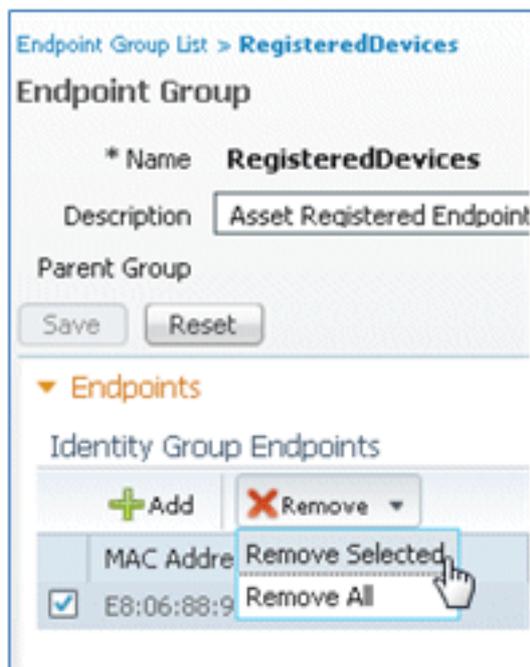


## 单SSID

本节介绍单SSID，并介绍如何直接连接到802.1x WLAN、提供AD用户名/密码进行PEAP身份验证、通过访客帐户调配以及重新连接TLS。

完成以下步骤，以便在单SSID场景中调配iOS：

1. 如果使用同一iOS设备，请从已注册设备中删除终端。



2. 在iOS设备上，导航到设置 > General > Profiles。删除本示例中安装的配置文件。



3. 单击Remove以删除以前的配置文件。



4. 使用现有 (已清除) 设备或新iOS设备直接连接到802.1x。

5. 连接到Dot1x，输入用户名和密码，然后单击加入。



6. 从[ISE配置](#)部分重复第90步和第页直到完全安装适当的配置文件。

7. 导航到ISE > Operations > Authentications以监控进程。此示例显示使用TLS调配、断开并重新连接到同一WLAN时直接连接到802.1X WLAN的客户端。

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12 12:40:03.593 AM	✔	🔒	paul	EB-06-98-97-09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12 12:39:53.353 AM	✔	🔒	EB-06-98-97-09-41	EB-06-98-97-09-41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12 12:39:08.967 AM	✔	🔒	paul	EB-06-98-97-09-41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

8. 导航到WLC > Monitor > [Client MAC]。在客户端详细信息中，请注意客户端处于RUN状态，其数据交换被设置为本地，而身份验证被设置为中心。对于连接到FlexConnect AP的客户端而言，情况也是如此。

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12 12:40:03.593 AM	✔	🔒	paul	EB-06-98-97-09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12 12:39:53.353 AM	✔	🔒	EB-06-98-97-09-41	EB-06-98-97-09-41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12 12:39:08.967 AM	✔	🔒	paul	EB-06-98-97-09-41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

## 用户体验 — 调配Android

### 双SSID

本节介绍双SSID，并介绍如何连接到要调配的访客，以及如何连接到802.1x WLAN。

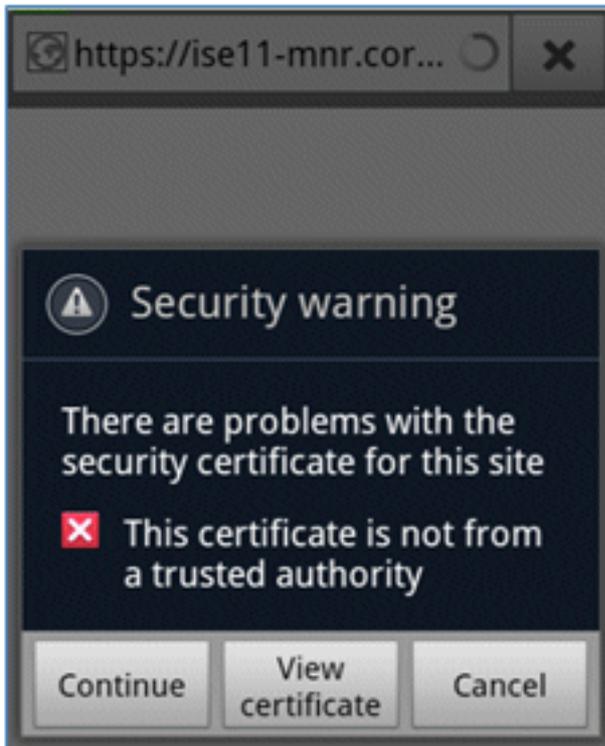
Android设备的连接过程与iOS设备的连接过程非常相似（单或双SSID）。但是，一个重要的区别是，Android设备需要访问Internet才能访问Google Marketplace（现为Google Play）和下载请求方代理。

完成以下步骤，以便在双SSID场景中调配Android设备（如本示例中的Samsung Galaxy）：

1. 在Android设备中，使用Wi-Fi连接到**DemoCWA**，然后打开访客WLAN。



2. 接受任何证书以连接到ISE。



3. 在访客门户输入用户名和密码以登录。

ne

Username: paul

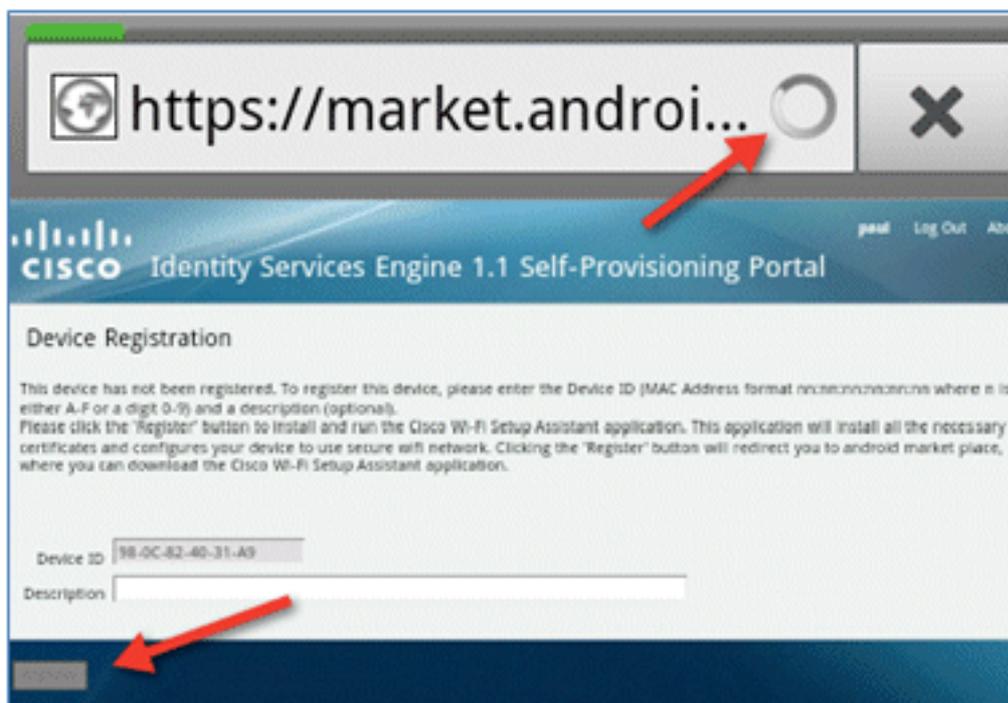
Password: [redacted]

Login

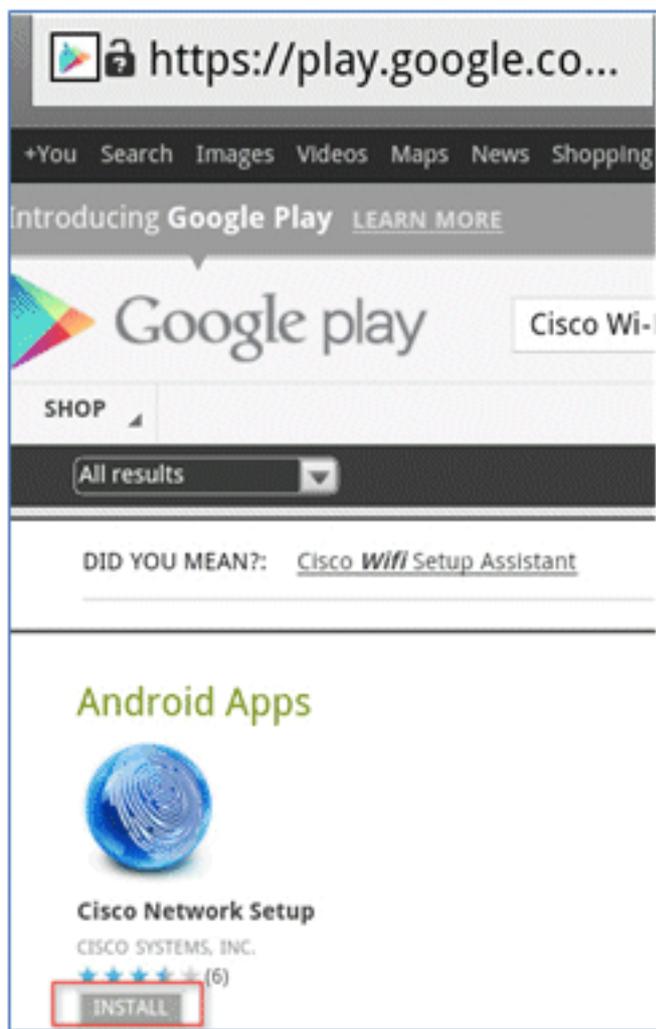
Prev. Next

1 2 3 4 5 6 7 8 9 0

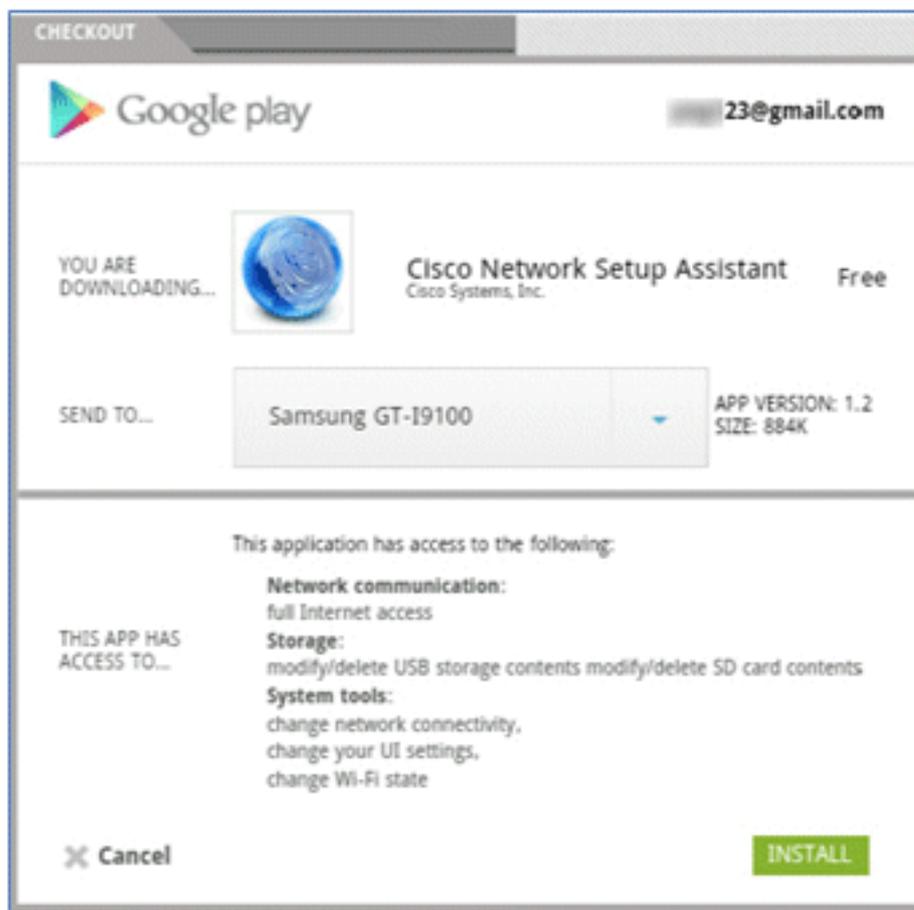
4. 单击**Register**。设备尝试访问Internet以访问Google市场。将任何其他规则添加到控制器中的预身份验证ACL（例如ACL-REDIRECT），以允许访问互联网。



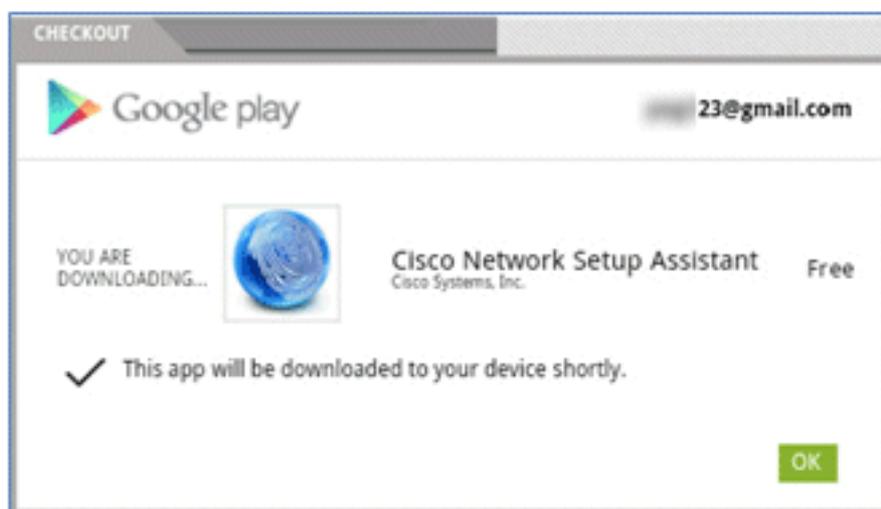
5. Google将思科网络设置列为Android应用。单击 **Install**。



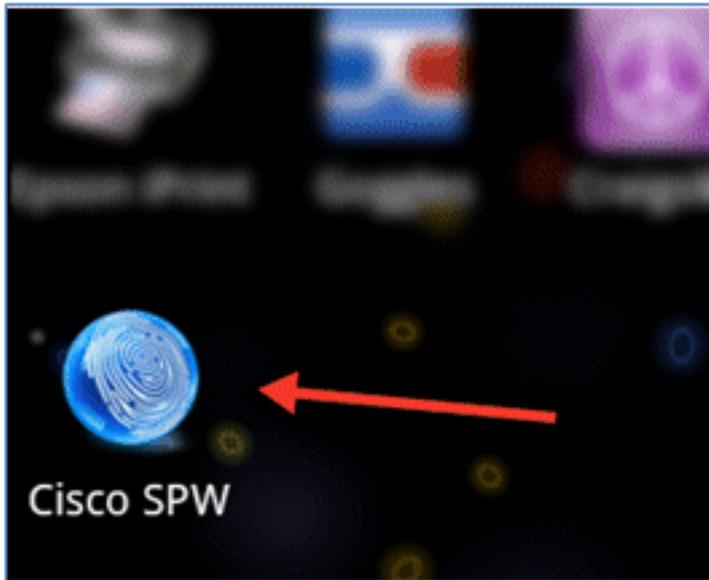
6. 登录Google，然后单击INSTALL。



7. Click OK.



8. 在Android设备上，找到已安装的思科SPW应用，然后将其打开。



9. 确保您仍然从Android设备登录到访客门户。

10. 单击**Start**以启动Wi-Fi设置助手。



11. Cisco SPW开始安装证书。



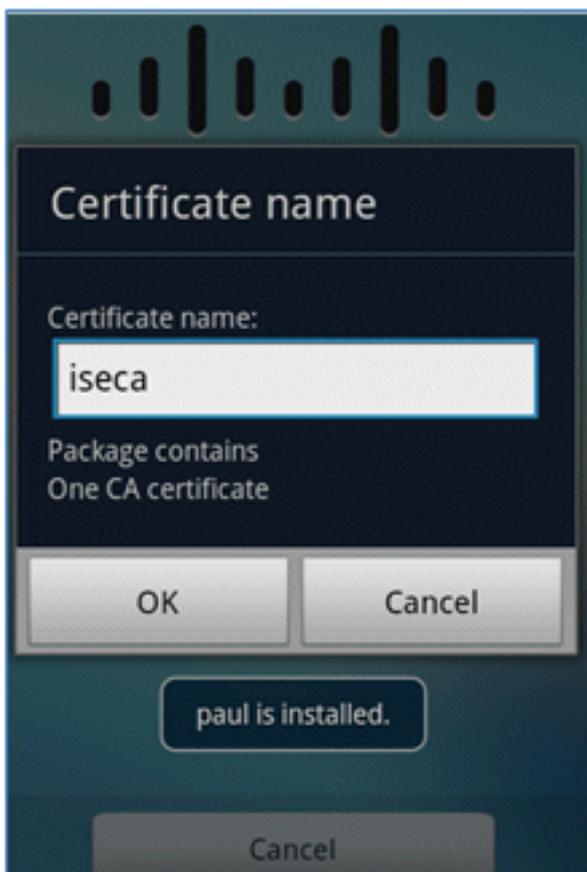
12. 出现提示时，设置凭据存储的密码。



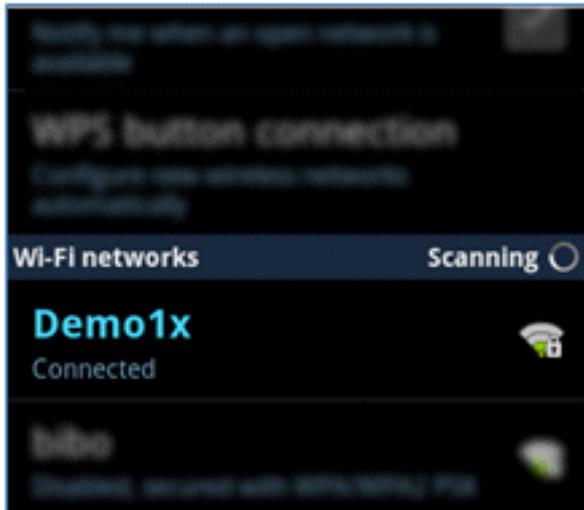
13. Cisco SPW返回证书名称，其中包含用户密钥和用户证书。点击**确定**以确认。



14. Cisco SPW继续并提示输入另一个包含CA证书的证书名称。输入名称**iseca**（在本例中），然后单击**OK**以继续。



15. Android设备现已连接。

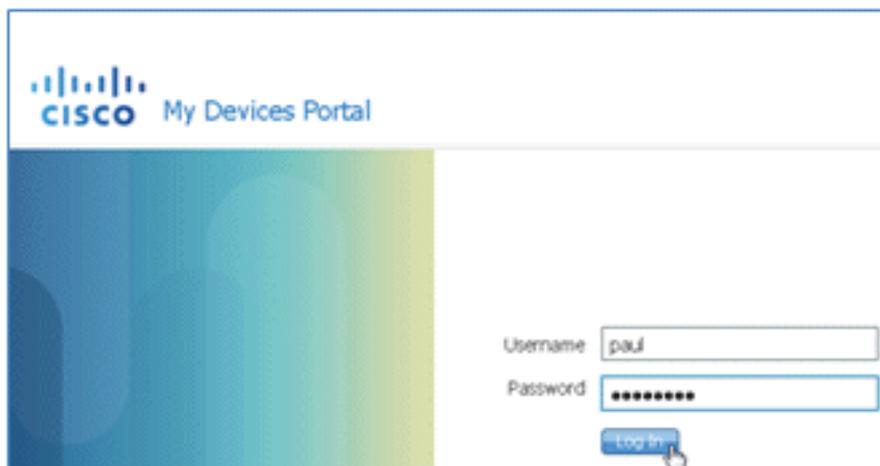


## 我的设备门户

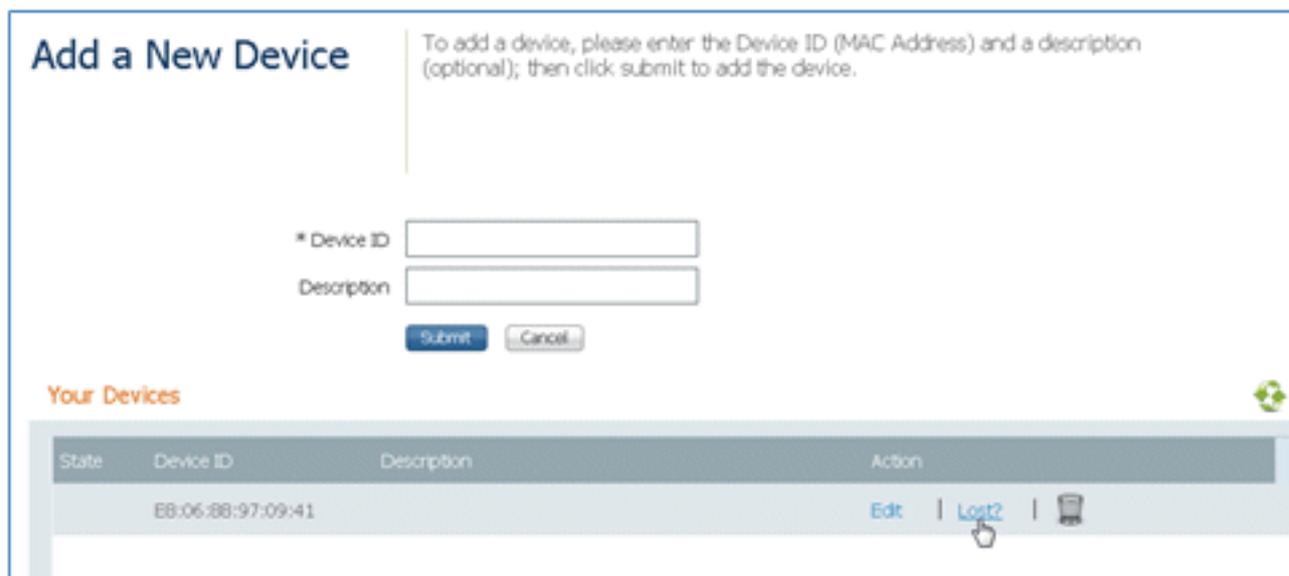
My Devices Portal允许用户在设备丢失或被盗的情况下将之前已注册的设备列入黑名单。它还允许用户在需要时重新登记。

完成以下步骤以将设备列入黑名单：

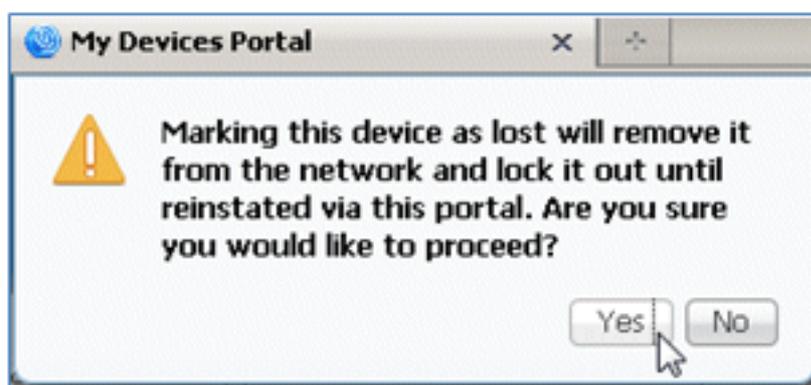
1. 要登录My Devices Portal，请打开浏览器，连接到<https://ise-server:8443/mydevices>（注意端口号8443），然后使用AD帐户登录。



2. 在Device ID（设备ID）下找到设备，然后单击Lost?以启动设备的黑名单。



3. 当ISE提示警告时，单击**Yes**以继续。



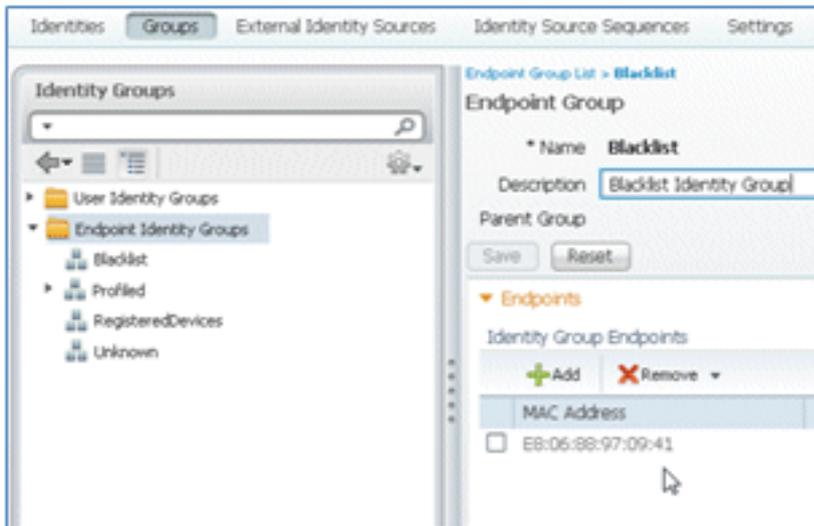
4. ISE确认设备已标记为**lost**。



5. 即使安装了有效的证书，使用之前注册的设备连接到网络的任何尝试现在都会被阻止。以下是身份验证失败的黑名单设备示例：

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12:49:07.851 AM			pa.j	E8:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:59.057 AM				E8:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:54.137 AM			pa.j	E8:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed

6. 管理员可以导航到ISE > Administration > Identity Management > **Groups**，点击**Endpoint Identity Groups** > **Blacklist**，然后看到设备已列入黑名单。

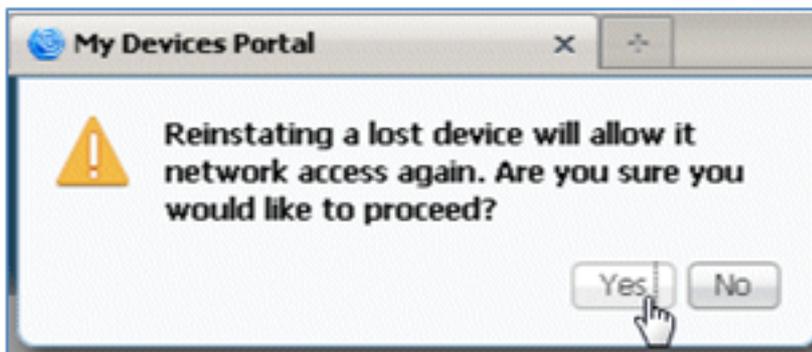


要恢复列入黑名单的设备，请完成以下步骤：

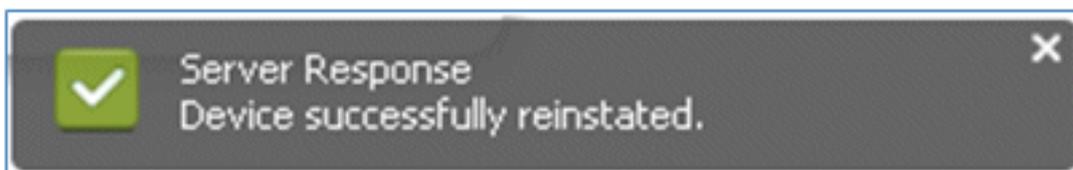
1. 从My Devices Portal中，点击该设备的Reinstate。



2. 当ISE提示警告时，单击Yes以继续。



3. ISE确认设备已成功恢复。将恢复后的设备连接到网络，以测试该设备现在是否被允许。

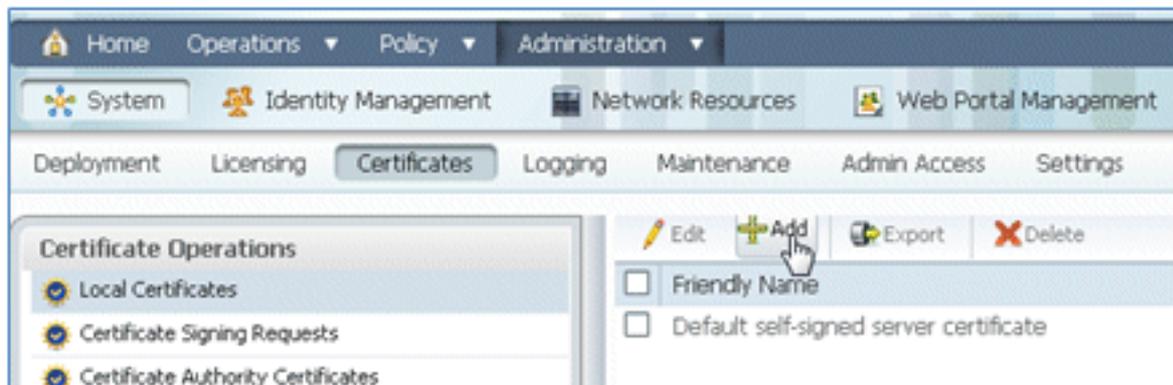


## 参考 — 证书

ISE不仅需要有效的CA根证书，还需要由CA签署的有效证书。

要添加、绑定和导入新的受信任CA证书，请完成以下步骤：

1. 导航到ISE > Administration > System > **Certificates** , 点击**Local Certificates** , 然后点击Add。



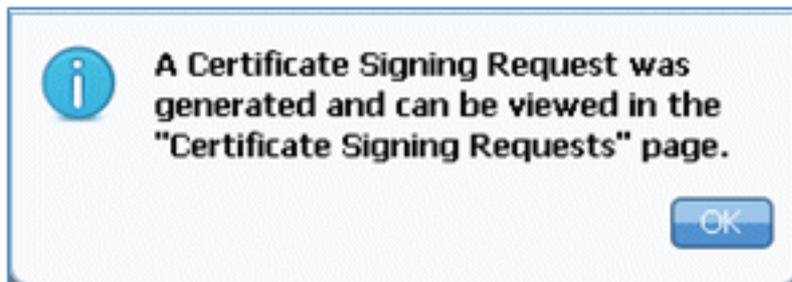
2. 选择**Generate Certificate Signing Request(CSR)**。



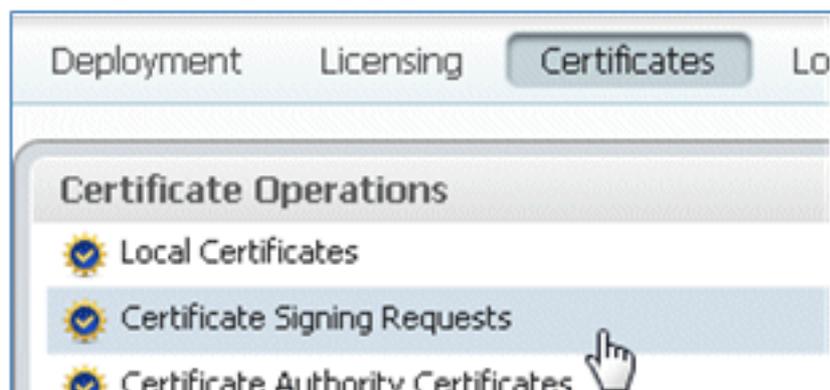
3. 输入证书主题**CN=<ISE-SERVER hostname.FQDN>**。对于其他字段，您可以使用CA设置所需的默认值或值。单击“Submit”。



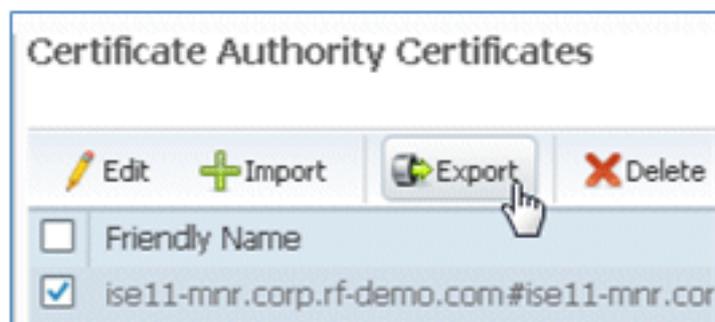
4. ISE验证已生成CSR。



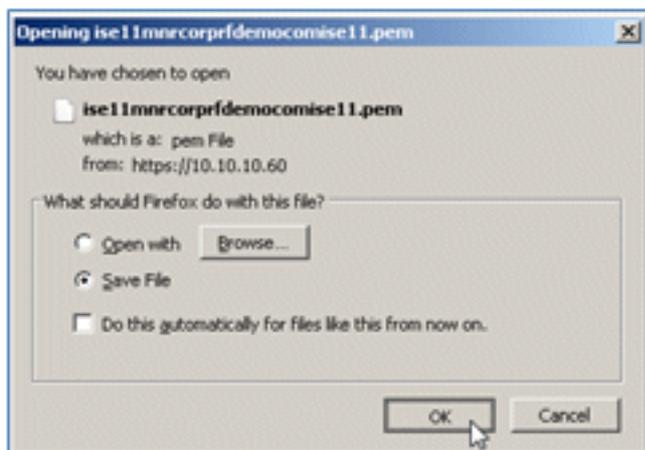
5. 要访问CSR，请点击**证书签名请求**操作。



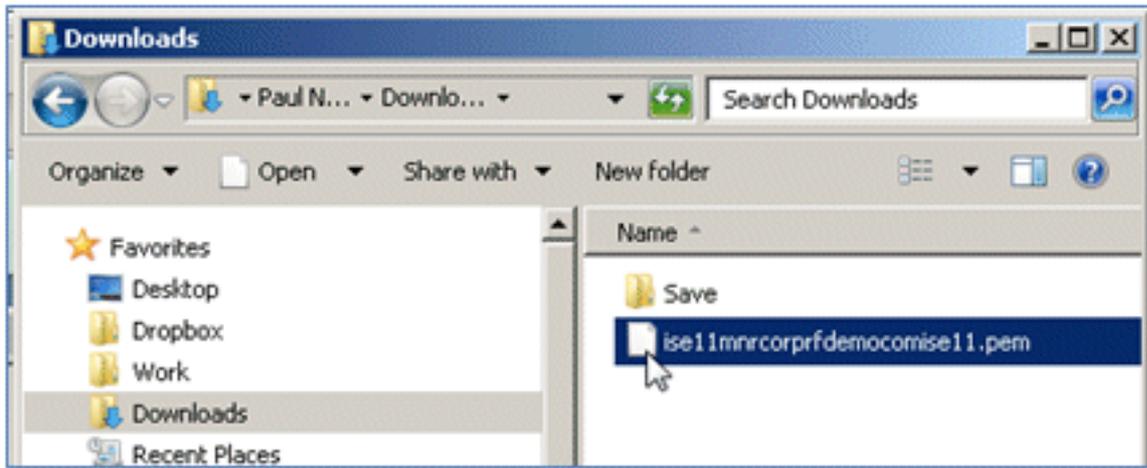
6. 选择最近创建的CSR，然后单击**Export**。



7. ISE将CSR导出到.pem文件。单击**Save File**，然后单击**OK**将文件保存到本地计算机。



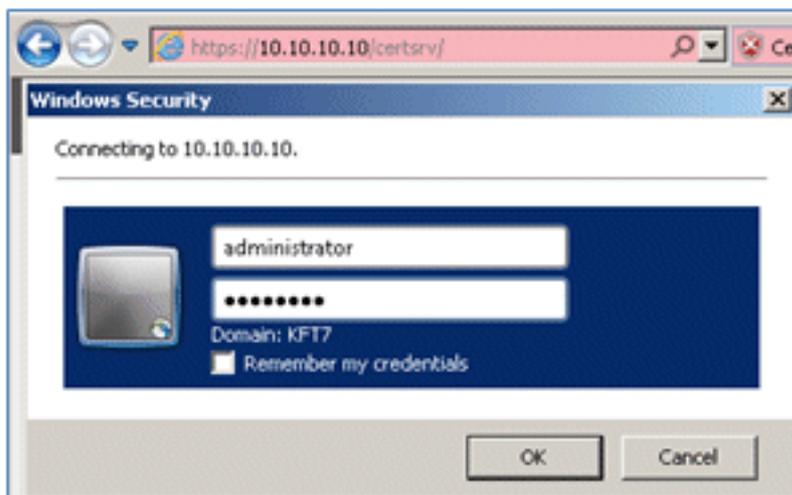
8. 使用文本编辑器查找并打开ISE证书文件。



9. 复制证书的全部内容。



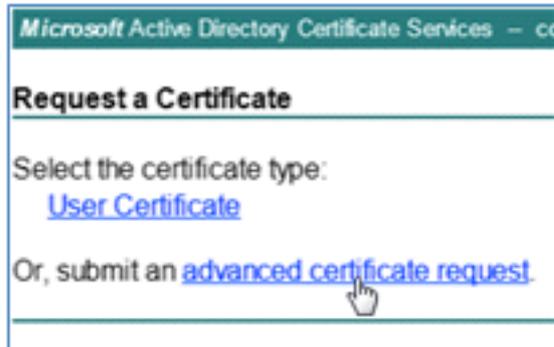
10. 连接到CA服务器，并使用管理员帐户登录。服务器是Microsoft 2008 CA，其地址为 <https://10.10.10.10/certsrv>（在本例中）。



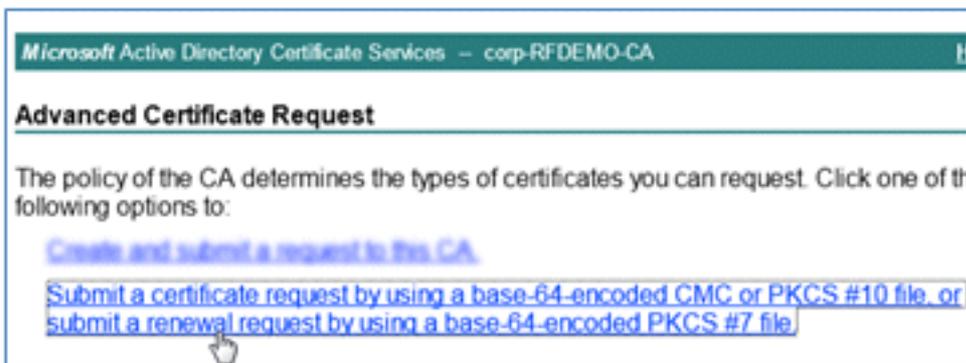
11. 点击申请证书。



12. 单击高级证书请求。



13. 单击第二个选项以使用base-64编码的CMC或.....提交证书请求。



14. 将ISE证书文件(.pem)中的内容粘贴到已保存请求字段，确保证书模板为Web Server，然后点击提交。

Microsoft Certificate Services -- labsrv.corp.rf-demo.com

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
MAAGAlUdDwQEAvICrDAdBgNVHQ4EFgQUBJa5qgBc
VRO1BAwvCgYIKwYBBQUHAWewEQYJYIZIAAyb4QgEB
BQUAA4GBAKS+tyTCZ1NKcXIyqxHTWjepfDqVdoS2
1/t6SUIOKQayBRUp21TpHf+o27eDTVwW83bCmbD1
oaMNBEmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pM
-----END CERTIFICATE-----
```

**Certificate Template:**

Web Server

**Additional Attributes:**

Attributes:

Submit >

15. 单击Download certificate。

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

 [Download certificate](#)

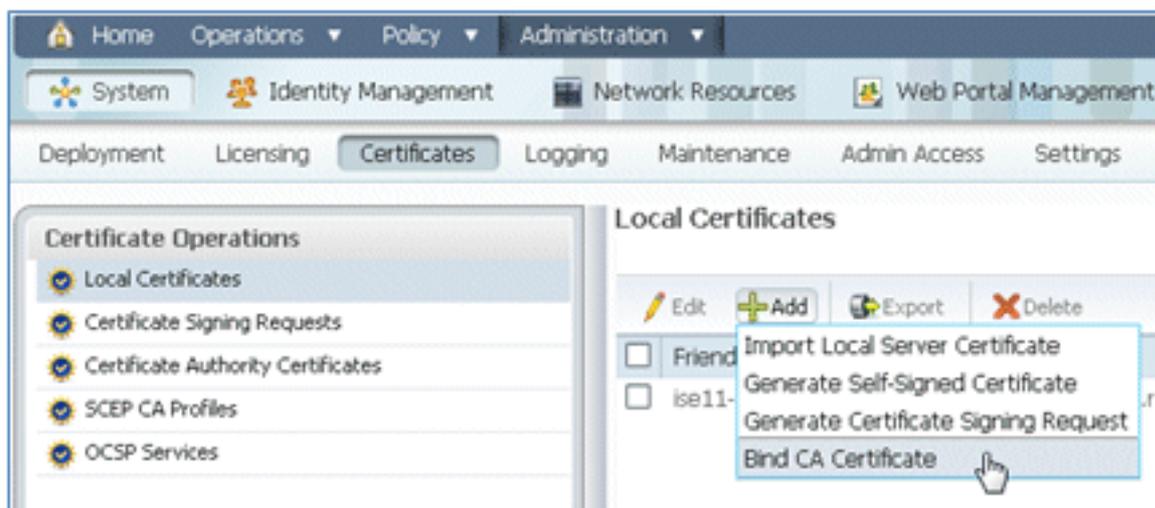
[Download certificate chain](#)

16. 保存certnew.cer文件；稍后将使用该文件与ISE绑定。

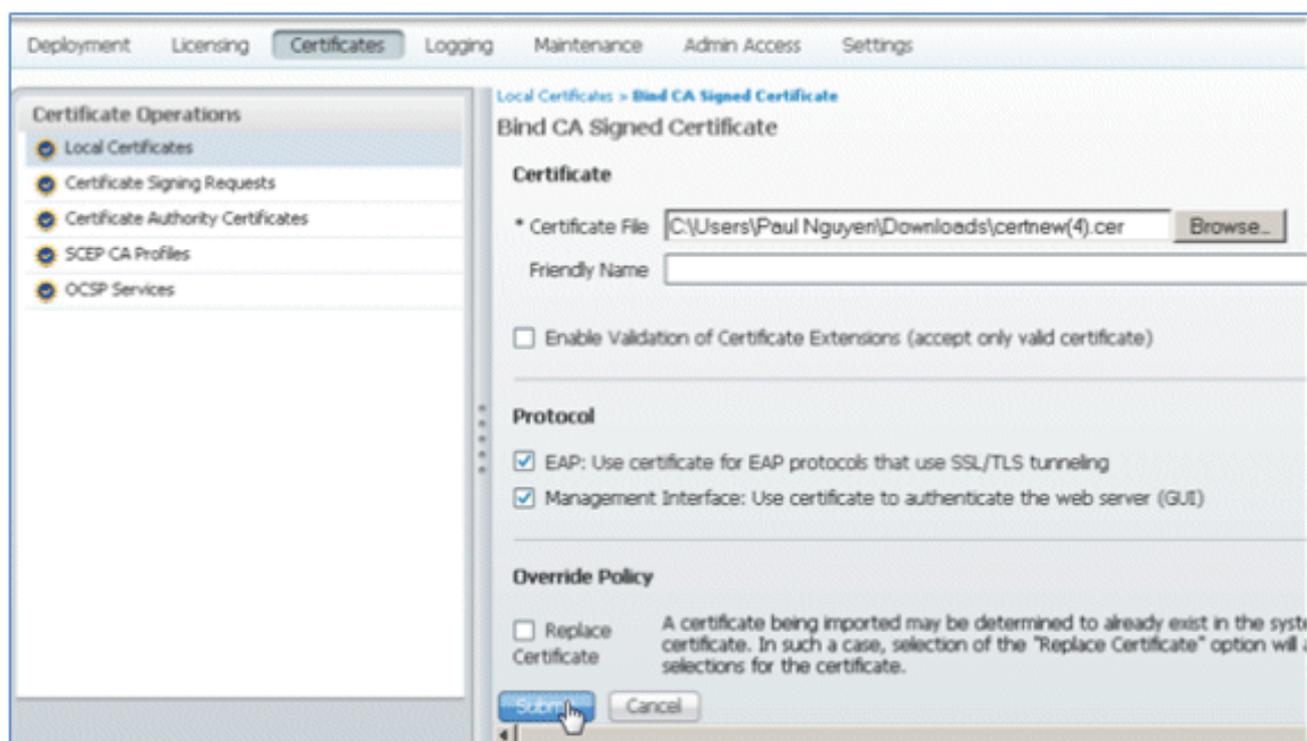
Do you want to open or save certnew.cer (921 bytes) from 10.10.10.10?

Open Save

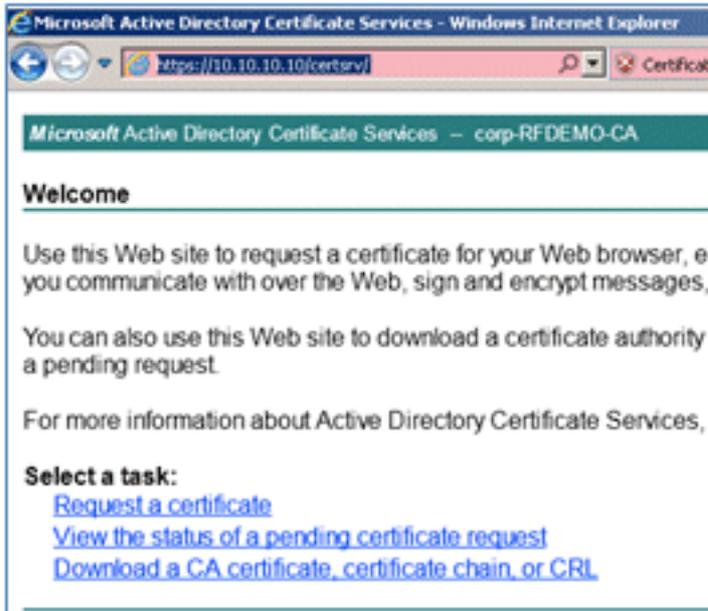
17. 从ISE Certificates，导航到Local Certificates，然后单击Add > Bind CA Certificate。



18. 浏览到在上一步中保存到本地计算机的证书，启用EAP和管理接口协议（复选框处于选中状态），然后点击提交。ISE可能需要几分钟或更长时间才能重新启动服务。



19. 返回CA的登录页(<https://CA/certsrv/>)，然后点击下载CA证书、证书链或CRL。



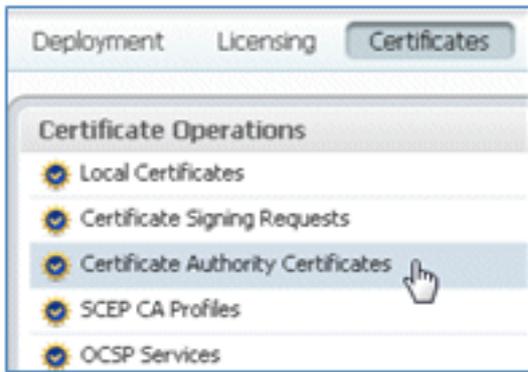
20. 单击下载 CA 证书。



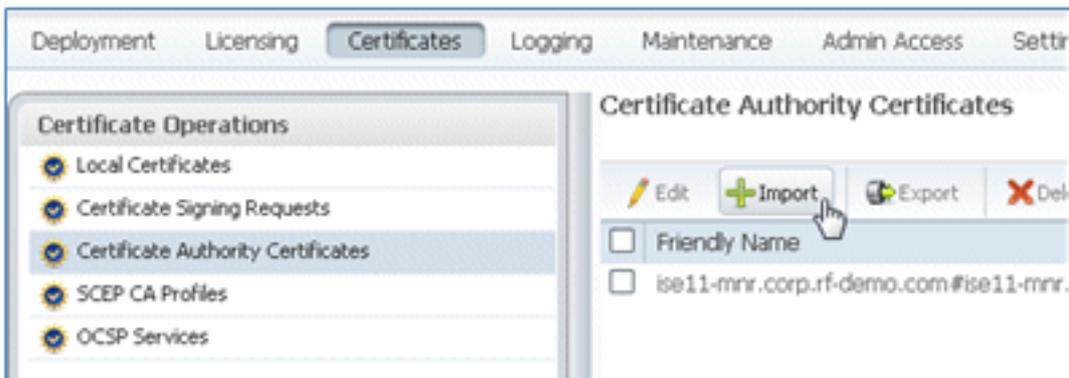
21. 将文件保存到本地计算机。



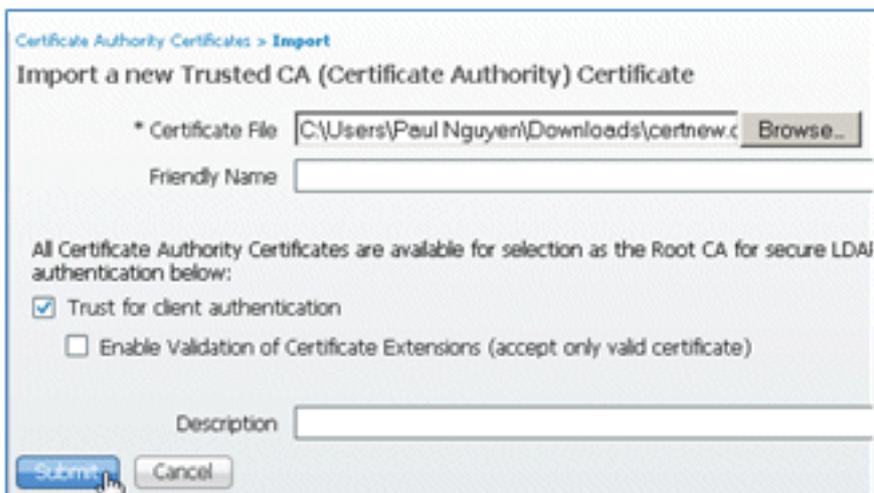
22. 在ISE服务器联机时，转到证书，然后单击证书颁发机构证书。



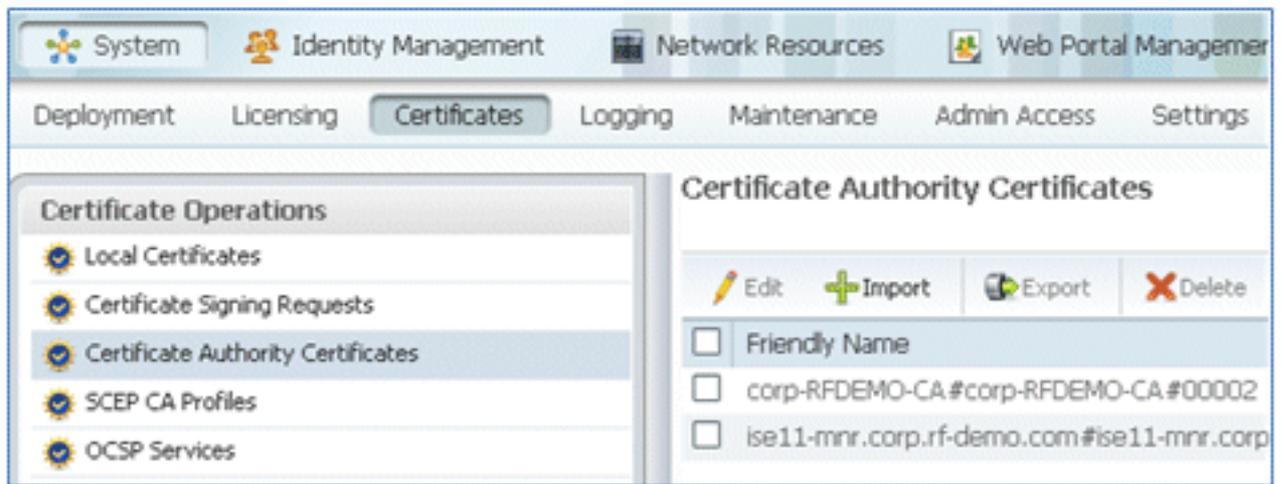
23. 单击 **Import**。



24. 浏览CA证书，启用Trust for client authentication（复选框为选中状态），然后单击Submit。



25. 确认已添加新的受信任CA证书。



## 相关信息

- [思科身份服务引擎硬件安装指南，版本1.0.4](#)
- [Cisco 2000 系列无线局域网控制器](#)
- [Cisco 4400 系列无线局域网控制器](#)
- [Cisco Aironet 3500 系列](#)
- [Flex 7500无线分支机构控制器部署指南](#)
- [自带设备 — 统一设备身份验证和一致的访问体验](#)
- [带身份服务引擎的无线BYOD](#)
- [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）。