

使用思科身份服务引擎进行自注册和调配

安全访问操作指南系列

日期：2012 年 4 月

作者：Imran Bashir

目录

概述	3
方案概览	4
双 SSID 无线 BYOD 自行注册	4
单 SSID 无线 BYOD 自行注册	4
架构/图	5
组件	6
Cisco ISE 配置	6
识别 BYOD 流程用户	6
创建身份源序列	9
配置 My Devices Portal	11
配置访客门户序列	13
创建客户端调配策略	15
策略配置	18
配置身份验证策略	21
附录 A: Android 和 Play.Google.Com	33
Android 有何独特之处?	33
附录 B: BYOD 流程	34
附录 C: 参考	36
Cisco TrustSec 系统	36
设备配置指南:	36

概述

移动设备的激增，以及因支持自带设备 (BYOD) 现象对企业造成的压力已经对安全产生新的要求，只有满足这些要求才能保障网络服务，保护数据，以及在企业需要与用户需求之间实现平衡。本应用说明介绍一些内置于身份服务引擎的功能（例如设备注册和本地请求方调配），用户可以使用这些功能应对有关 BYOD 的一些要求。

本操作指南介绍设置系统进行自注册的过程，其中包括本地请求方调配、所推送的请求方配置文件的类型，以及如何编写用于差异化访问权限的策略。

表 1 列出支持的平台、请求方配置文件下载后的位置以及查看或清除配置文件的对应位置。

表 1. 支持的平台

设备	证书库	证书信息	版本
iPhone/iPad/iPod	设备证书库 (配置文件)	可以通过 Settings → General → Profile 进行查看	5.0 以及更高版本
Android	设备加密证书库	无法查看。但是可以通过 Settings → Location & Security → Clear Storage (清除所有设备证书和密码) 予以清除	3.2 以及更高版本
Windows	用户证书库	可以通过启动 Certificate Snap-In for MMC 进行查看	WindowsXP - SP3 Windows Vista - SP? Windows7 - 所有版本
MacOS-X	Keychain	可以通过启动 application → Utilities → Keychain Access 进行查看	MacOS-X 10.6 和 10.7

注：MACOS-X 10.8 具有以下注意事项

当在 Security & Privacy Preference 窗格中选择选项“MAC App Store and identified developers”时，系统不会安装 SPW (请求方 MAC)

当安装 SPW 配置文件/证书时，系统会多次显示弹出窗口

注：在本文档中，我们介绍了推荐的部署方法以及一些根据您的实际环境所需的安全级别而定的不同选项。这些方法是最佳实践规定的 Cisco TrustSec 部署的示例和分步说明，可确保成功部署项目。

如果您对调配证书以及请求方配置文件感兴趣，请参阅以下操作指南：“BYOD - 使用证书差异化访问权限” (BYOD-Using_Certificates_for_Differentiated_Access)

警告：用户必须始终遵循本文档执行相关操作，忽略某些章节可能会造成不良后果。

方案概览

本文档将介绍个人设备自注册过程，在自注册过程中，员工将注册新的设备，系统会自动为该用户和设备调配本地请求方，并且使用预配置为将设备连接到企业网络的请求方配置文件来安装本地请求方。Cisco ISE 策略还可以配置为根据用户、设备类型、位置和时间对用户/设备提供差异化访问权限。

进行无线自注册的设备可以设置为使用单 SSID 和/或双 SSID，每个用户用例的注册和激活流程如下。

我们将以 iPad 的本地请求方调配和授权为例，介绍本文档中所用的方案。

双 SSID 无线 BYOD 自行注册

客户网络设置有 2 个 SSID，一个是用于访客/BYOD (BYOD-Open) 的开放式 SSID，另一个是用于安全企业访问 (BYOD-Dot1x) 的 SSID。

员工与访客 SSID (BYOD-Open) 相关联。

打开浏览器，然后系统会将员工重定向至 Cisco ISE CWA（集中式 Web 身份验证）访客门户。

员工在标准访客门户中输入其企业用户名和密码。

Cisco ISE 根据企业 Active Directory 或其他企业身份库对用户进行身份验证，提供授权，如果接受授权策略则重定向至员工设备注册门户。

设备 MAC 地址已预先填入 DeviceID 的设备注册门户，并且员工可以输入可选描述，然后接受可接受的用户策略（如需要）。

员工选择接受并开始下载和安装请求方调配向导。

通过使用 OTA，Cisco ISE 策略服务节点向 iPad 发送新的配置文件，包括颁发的证书（如果已配置），其中嵌入 iPad 的 MAC 地址和员工的 AD 用户名，以及强制使用 MSCHAPv2 或 EAP-TLS 进行 802.1X 身份验证的 Wi-Fi 请求方配置文件。

现在，iPad 已配置为使用 MSCHAPv2 或 EAP-TLS 进行身份验证与企业无线网络进行关联，并且 Cisco ISE 授权策略将使用证书中的属性实施网访问控制（例如，提供有限访问权限，因为 iPad 并非企业资产）。

Cisco ISE 发起授权变更 (CoA)，员工与企业 SSID (BYOD-Dot1x) 重新关联（如果采用双 SSID，则员工必须手动连接到企业 SSID，而在采用单 SSID 的情况下，iPad 会使用 EAP-TLS 自动重新连接），并且通过 MSCHAPv2 或 EAP-TLS（为该请求方配置的身份验证方法）进行身份验证。

单 SSID 无线 BYOD 自行注册

1. 客户网络设置有一个 SSID (BYOD-Dot1x)，用于执行可同时支持 PEAP 和 EAP-TLS 的安全企业访问（当使用证书时）。
2. 员工与企业 SSID (BYOD-Dot1x) 相关联。
3. 输入请求方的用户名和密码（均为 EMPLOYEE）以进行 PEAP 身份验证。
4. Cisco ISE 根据企业 Active Directory 或其他企业身份库对用户进行身份验证，提供授权，如果接受授权策略则重定向至员工设备注册门户。
5. 员工打开浏览器，然后系统会将员工重定向至员工设备注册门户。

6. 设备 MAC 地址已预先填入 DeviceID 的设备注册门户，并且员工可以输入可选描述，然后接受可接受的用户策略（如需要）。
7. 员工选择接受并开始下载和安装请求方调配向导。
8. 通过使用 OTA，Cisco ISE 策略服务节点向 iPad 发送新的配置文件，包括颁发的证书（如果已配置），其中嵌入 iPad 的 MAC 地址和员工的 AD 用户名，以及强制使用 MSCHAPv2 或 EAP-TLS 进行 802.1X 身份验证的 Wi-Fi 请求方配置文件。
9. 现在，iPad 配置为使用 MSCHAPv2 或 EAP-TLS 进行身份验证与企业无线网络进行关联（如果采用双 SSID，则员工必须手动连接到企业 SSID，而在采用单 SSID 的情况下，iPAD 会使用 EAP-TLS 自动重新连接），并且 Cisco ISE 授权策略将使用证书中的属性实施网络访问控制（例如，提供有限访问权限，因为这并非企业资产）。
10. Cisco ISE 发起授权变更 (CoA)，员工与企业 SSID (BYOD-Dot1x) 重新关联，并且通过 MSCHAPv2 或 EAP-TLS（为该请求方配置的身份验证方法）进行身份验证。

架构/图

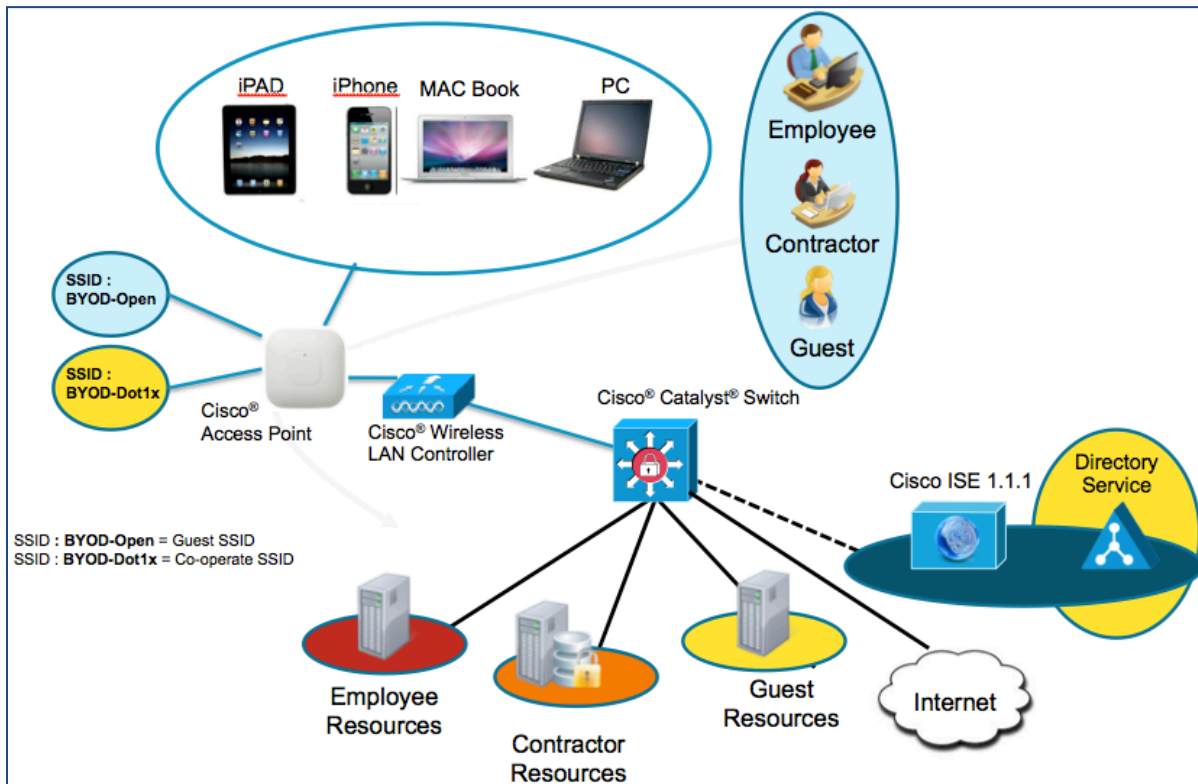


图 1. 网络图

组件

表 2: 本文档中使用的组件

组件	硬件	经过测试的功能	Cisco IOS® 软件版本
思科身份服务引擎 (ISE)	任意: 1121/3315、3355、3395、VMWare	集成 AAA、策略服务器和服务 (访客、分析器和安全状况)	ISE 1.1.1
无线 LAN 控制器 (WLC)	5500 系列 2500 系列 WLSM-2	分析和授权更改 (CoA)	统一无线 7.2.???
Apple iOS 和 Google Android	Apple 和 Google	N/A	Apple iOS 5.0 Google Android 2.3

注: 仅使用集中交换模式对无线进行了测试。

Cisco ISE 配置

在本节中, 我们将完成实施操作指南中所述的使用案例所需的步骤。这将包括基本配置, 例如创建高级配置的用户组、为 PEAP-MSCHAPv2 创建请求方配置文件, 以及相应地创建身份验证和授权策略。

识别 BYOD 流程用户

在用户自注册过程中 (“自注册” 一词是指注册资产并将该资产请求方调配为能够访问企业网络的过程), 我们可以选择身份库来定义要转发到自注册 (BYOD) 流程的资源。以下示例展示的是身份源序列包含的思科身份服务引擎以及 Active Directory 中的本地库内定义的用户。

作为最佳实践自注册程序的一部分, 我们将使用 Active Directory 作为身份源来确定允许自注册其设备的用户组。以下程序展示的是身份源序列包含的 Cisco ISE 本地用户数据库以及 Active Directory 中定义的用户。

用户组是单个用户或终端的集合, 这些用户或终端共享一组允许其访问特定 Cisco ISE 服务和功能集的权限。例如, 如果您属于 Change User Password 管理员组, 则可以为其其他用户更改管理密码。

配置用户组

步骤 1 导航至 Administration → Identity Management → Groups。

步骤 2 点击 ADD。

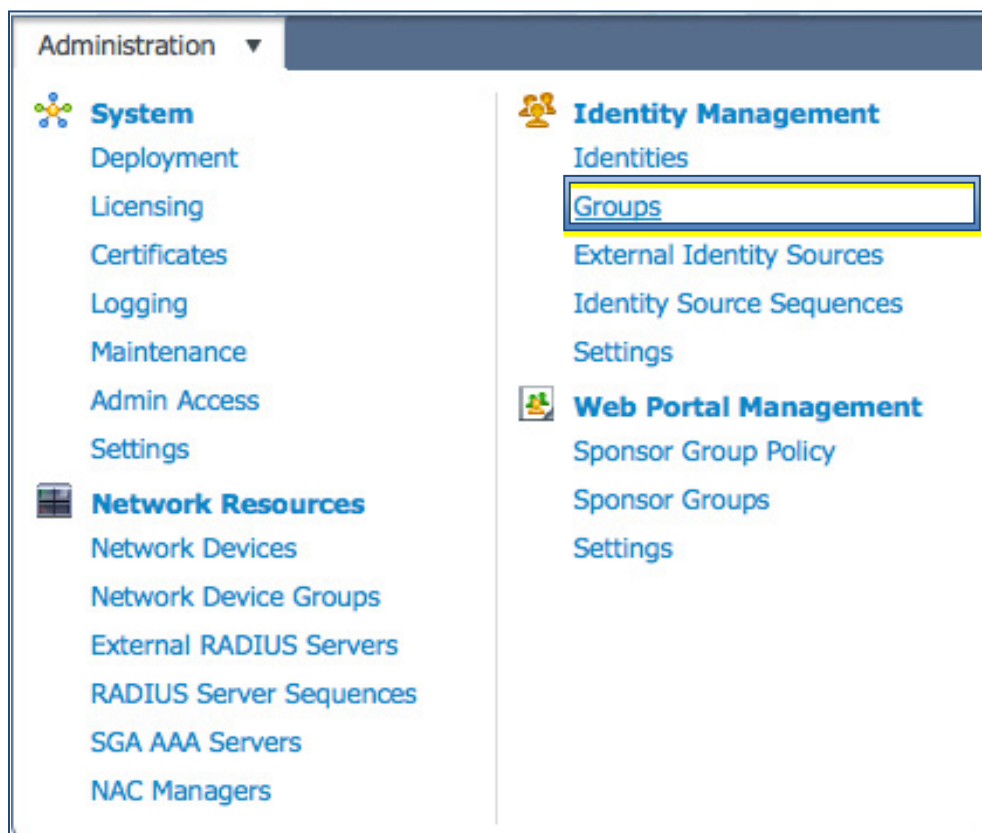


图 2. 身份组导航

步骤 3 创建身份组。

在本例中，我们将身份组命名为“Employee”。

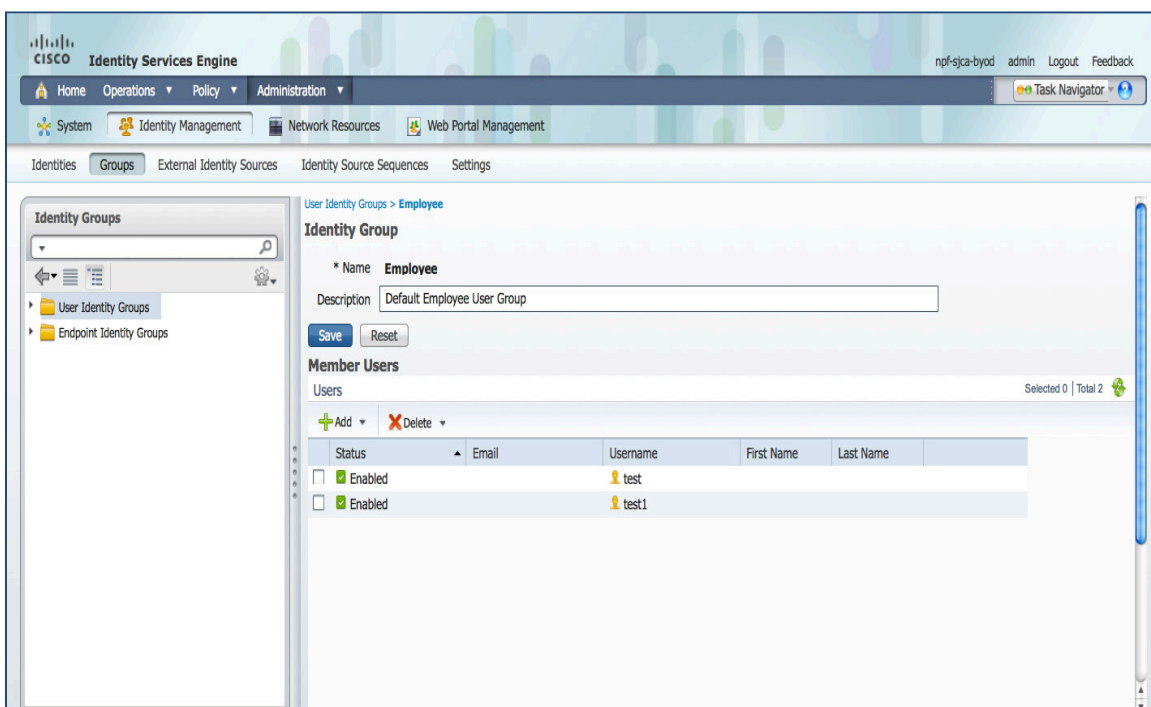
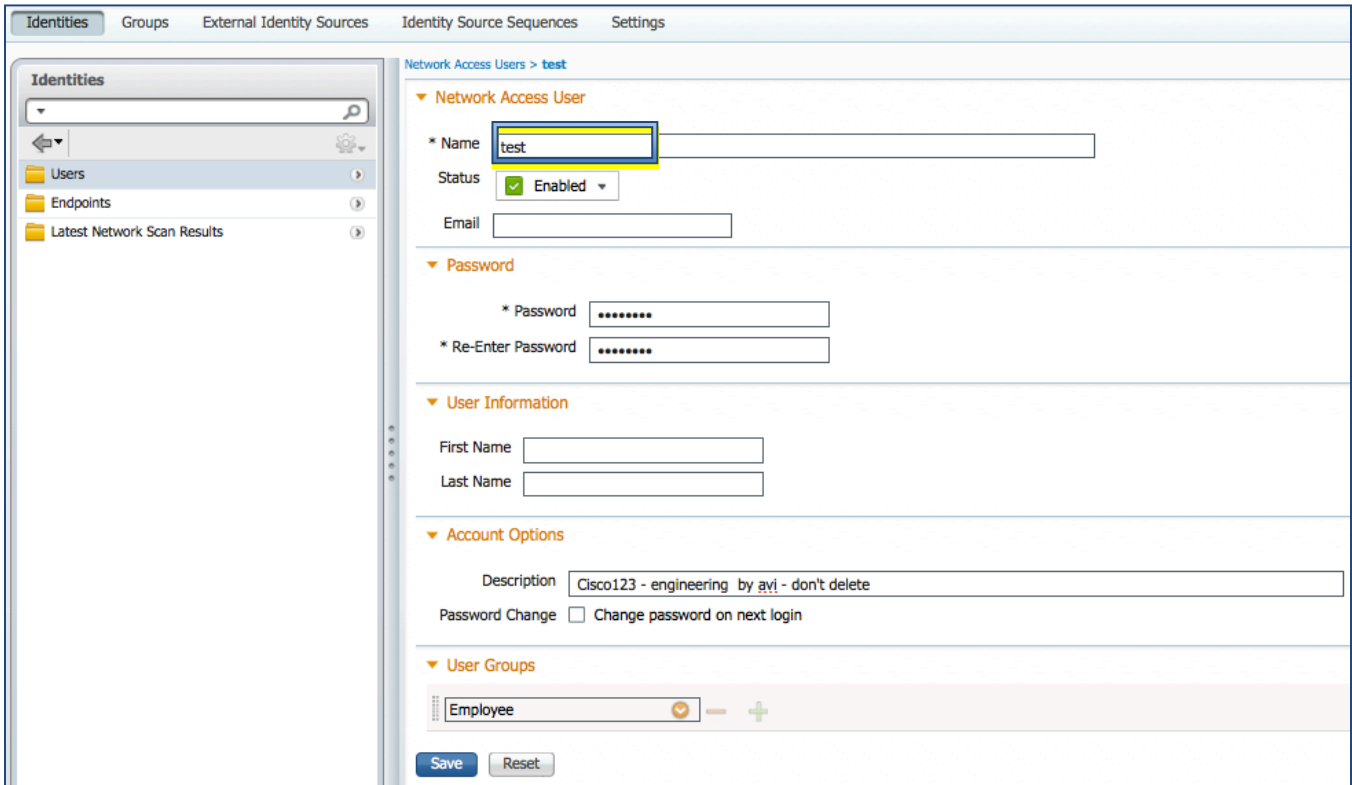


图 3. 用户身份组

在 Employee 组中创建用户

步骤 1 导航至 Administration → Identity Management → Identities → Users。

步骤 2 点击 ADD。



The screenshot shows the Cisco ISE user creation interface. The left sidebar shows the navigation menu with 'Users' selected. The main content area is titled 'Network Access Users > test'. The form fields are as follows:

- Name:** test (highlighted with a yellow box)
- Status:** Enabled (checked)
- Email:** (empty)
- Password:** (masked with dots)
- Re-Enter Password:** (masked with dots)
- User Information:**
 - First Name: (empty)
 - Last Name: (empty)
- Account Options:**
 - Description: Cisco123 - engineering by avj - don't delete
 - Password Change: Change password on next login
- User Groups:** Employee (selected)

Buttons for 'Save' and 'Reset' are visible at the bottom.

图 4. 用户帐户

创建身份源序列

身份源序列定义 Cisco ISE 在不同数据库中查找用户凭证将依照的顺序。Cisco ISE 支持以下数据库：Internal Users、Internal Endpoints、Active Directory、LDAP、RSA、RADIUS Token Servers 和 Certificate Authentication Profiles。

如果贵组织将凭证存储在多个身份库中，则您可以定义一个身份源序列，用于表明您希望 Cisco ISE 在这些数据库中查找用户信息所依照的顺序。找到匹配项之后，Cisco ISE 不再继续查找，但会评估凭证并将授权结果返回到网络访问设备。此策略是第一个匹配策略。

创建身份源序列。

步骤 1 Administration → Identity Source Sequence。

步骤 2 点击 ADD。

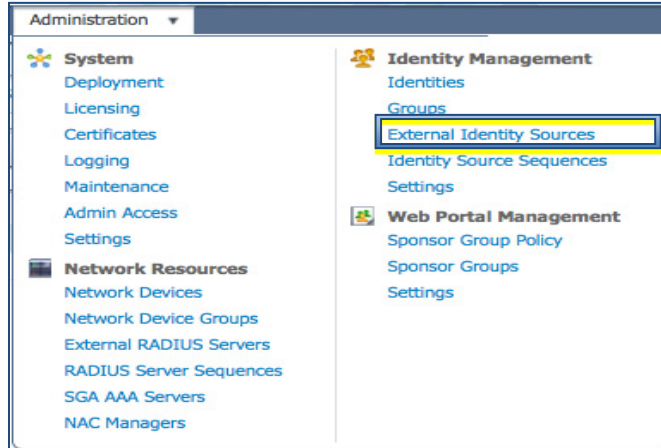


图 5. 身份源序列导航

- 步骤 3 对序列进行命名。在本例中，我们将序列命名为“Dot1x”。
- 步骤 4 在 **Authentication Search List** 中选择 Active Directory Server (AD1)、Internal Endpoints 和 Internal Users。

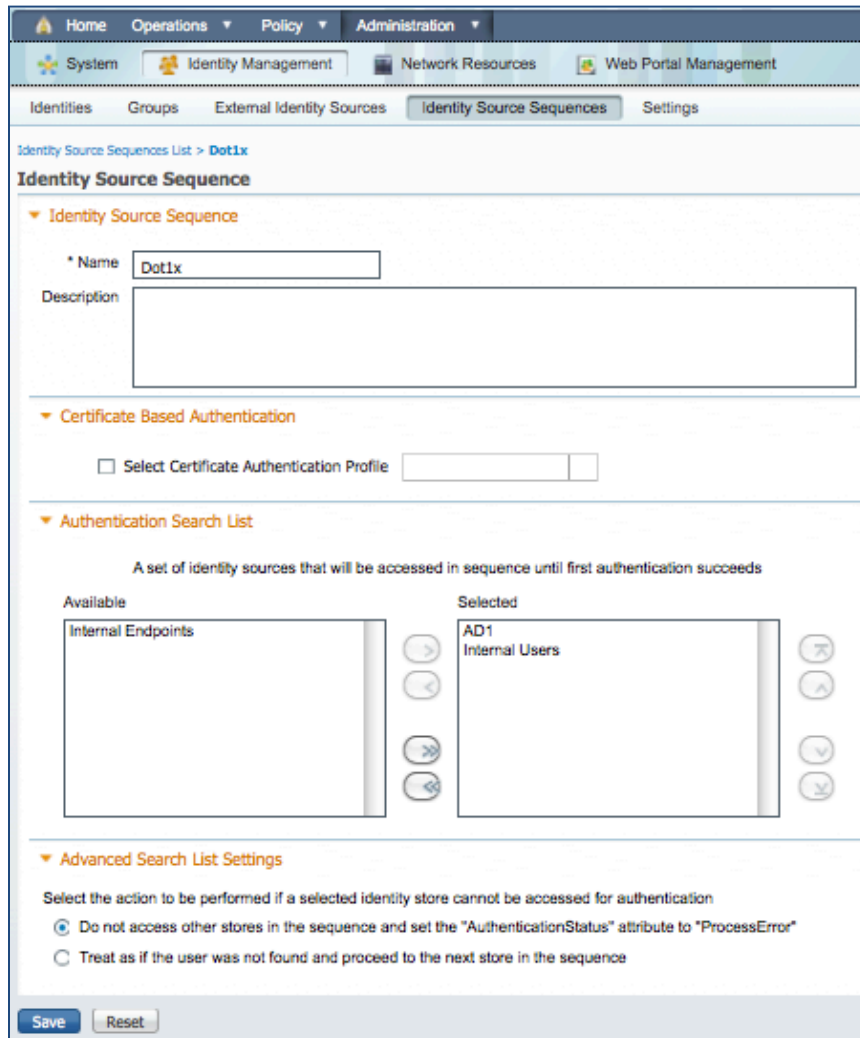


图 6. 身份源序列

配置 My Devices Portal

My Devices Portal 的主要用途是供最终用户自行将设备联网。虽然此门户可用于将任何设备输入 ISE 终端数据库中并因此使其联网，但是该门户面向的是没有用户或浏览器并因此无法完成自助调配流程的设备。这些设备可能包括点滴泵、打印机、游戏控制台等等。

My Devices Portal 设置

步骤 1 要启用 My Devices Portal，请依次点击 Administration → Web Portal Management → Settings → My Devices → Portal Configuration。

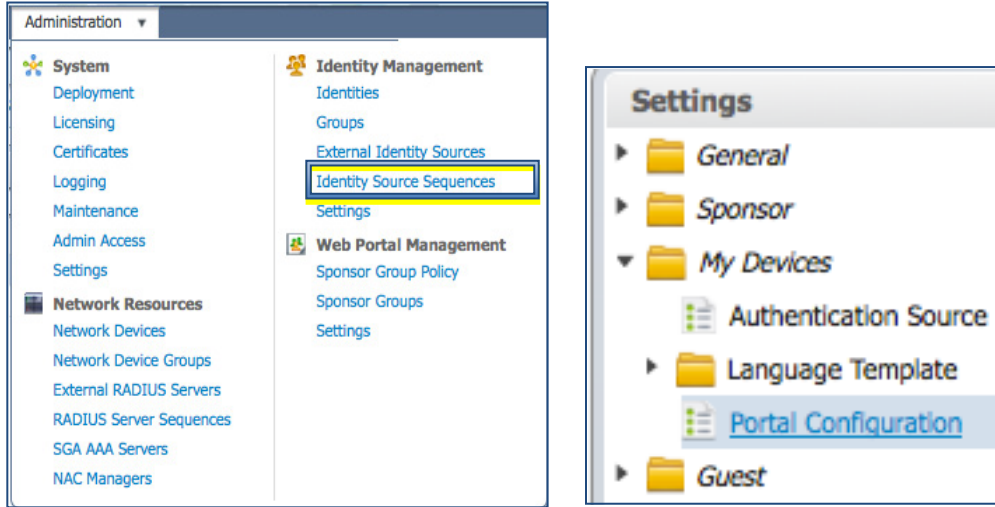


图 7. My Devices Portal 导航

步骤 2 默认情况下，系统会启用 My Devices Portal，但是，请导航至 My Devices 的门户管理页面并验证其是否已启用。

步骤 3 点击 ADD。

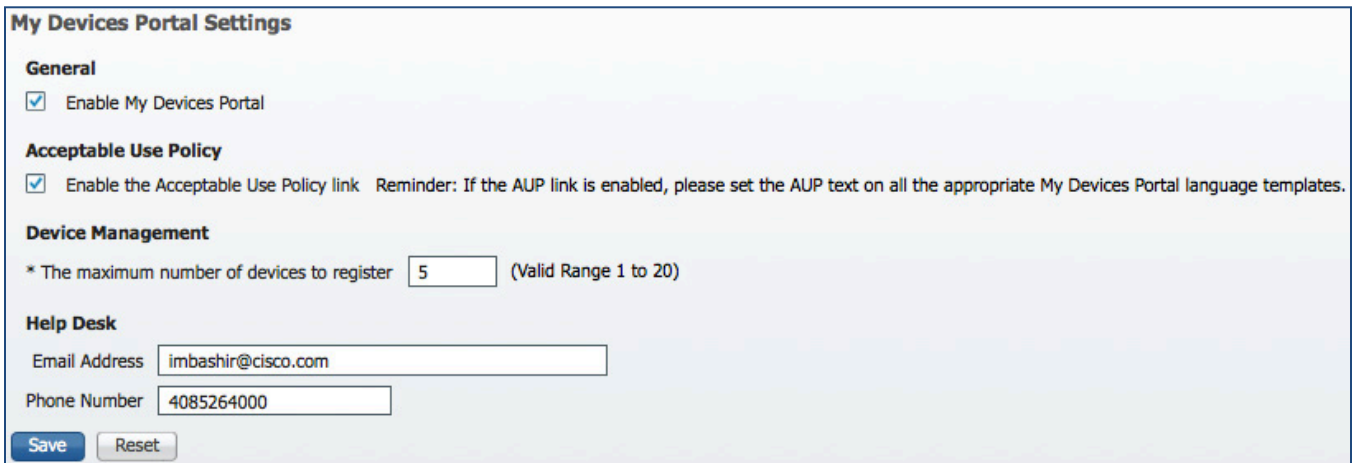


图 8. My Devices Portal 设置

为 MyDevices Portal 创建身份源序列

配置身份源序列，其中定义用于登录到 My Devices Portal 的身份验证请求。

步骤 1 转至 Administration → Identity Management → Identity Source Sequence。

步骤 2 点击 **ADD**。

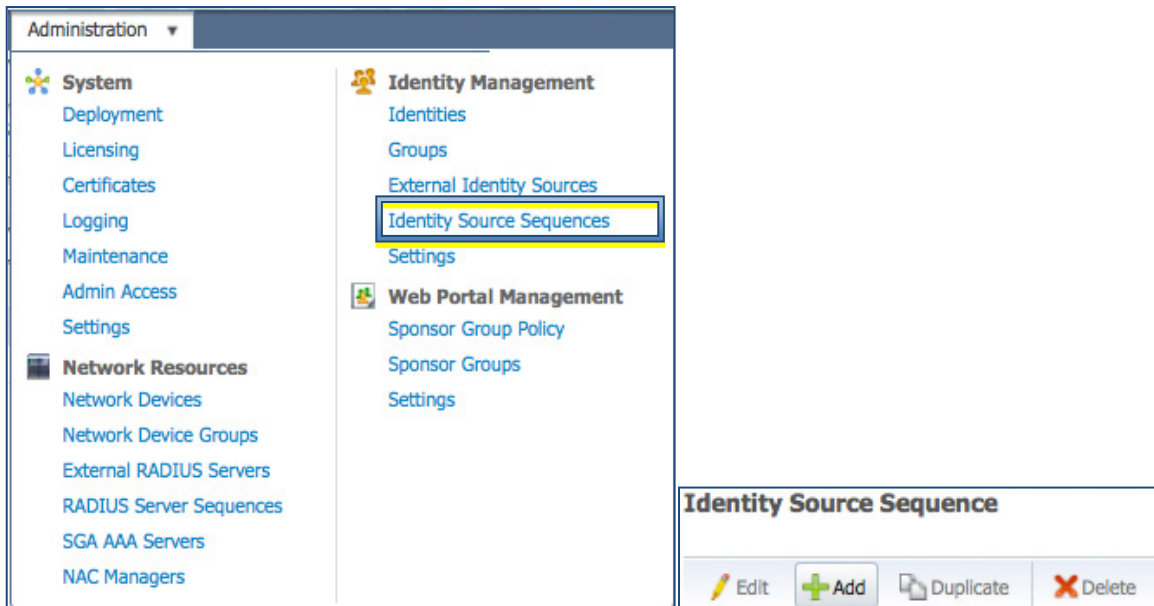


图 9. 身份源序列导航

步骤 3 定义 MyDevices Portal 的身份源序列

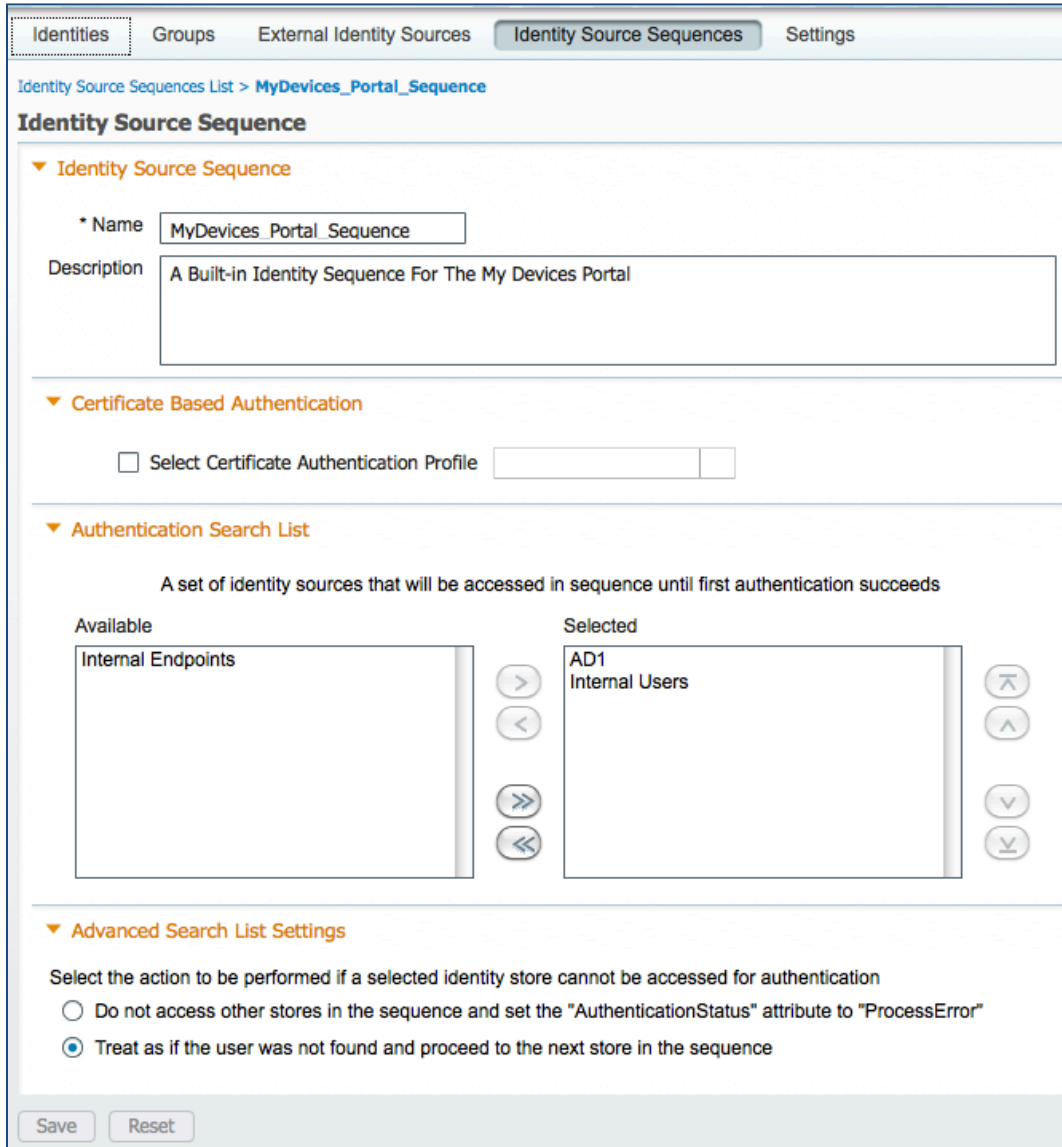


图 10. 身份源序列设置

配置访客门户序列

访客门户还将用于对企业用户进行身份验证，因此务必将 Active Directory 添加到默认访客门户序列中。

配置访客门户序列

步骤 1 转至 Administration → Identity Management → Identity Source Sequence。

步骤 2 编辑 “Guest_Portal_Sequence”。

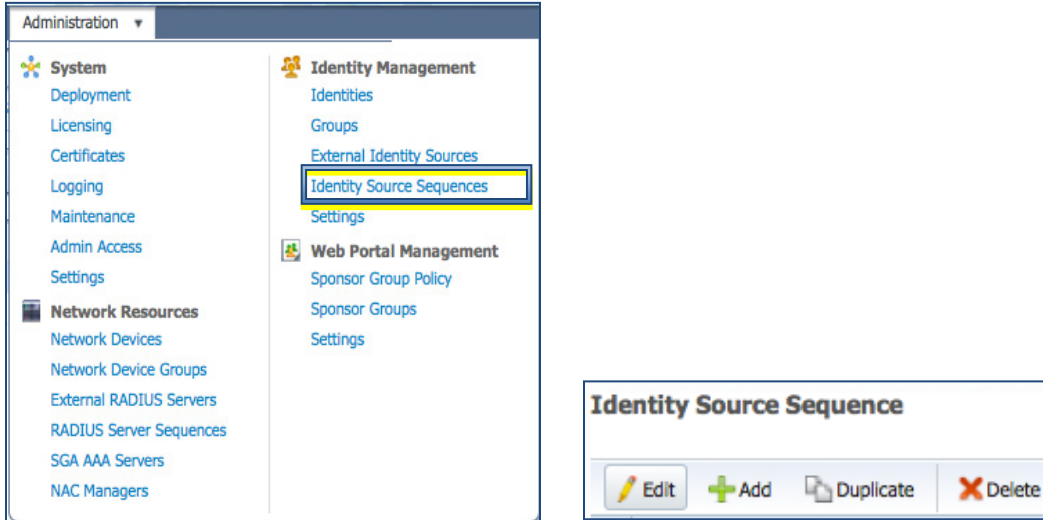


图 11. 身份源序列导航

步骤 3 将 Active Directory 添加到 “Guest_Portal_Sequence”。

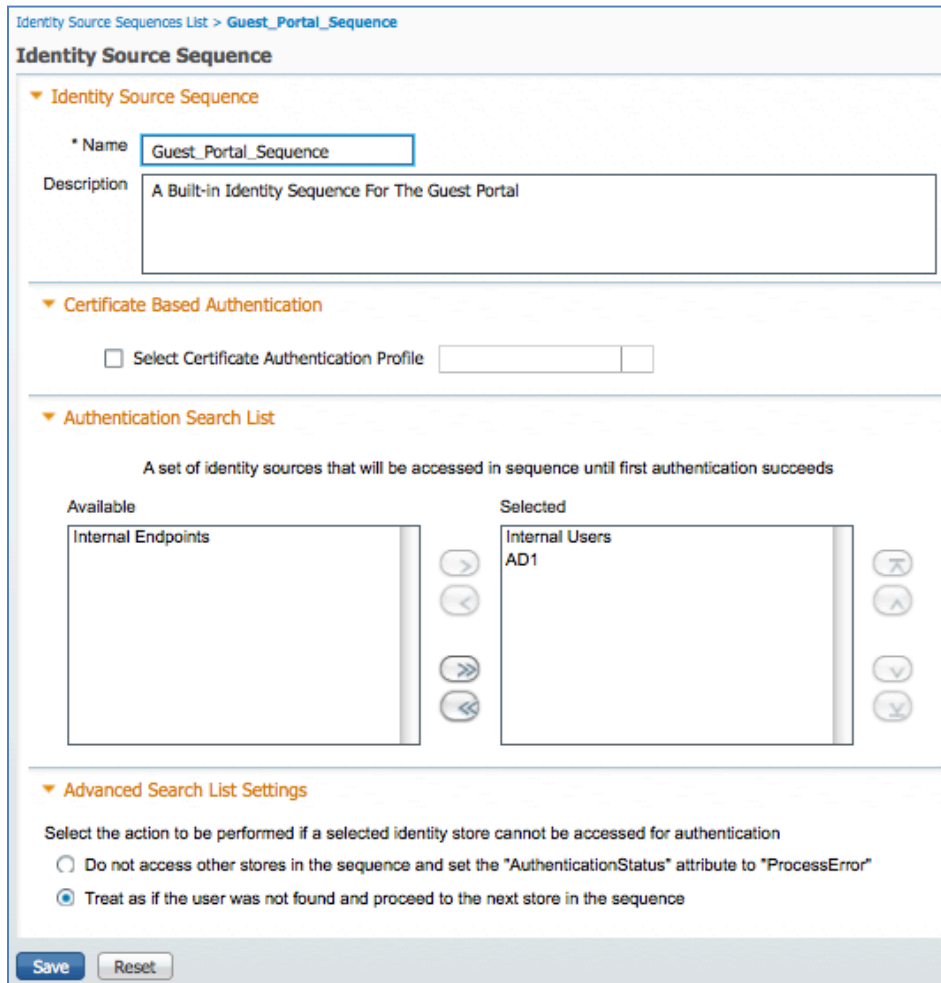


图 12. 身份源序列设置 - 访客门户

创建客户端调配策略

思科身份服务引擎在对登录会话（用户通过其访问内部网络）的类型进行分类时会查看各种元素。我们可以利用客户端调配策略创建请求方配置文件来配置终端（例如 iPhone、iPad、Windows、MAC OSx 等等）。

通过本地请求方调配 (NSP)，Cisco ISE 根据操作系统将具有不同的调配策略。每个策略都将包含“本地请求方配置文件”，其中规定使用 PEAP 还是 EAP-TLS 以及要连接到的无线 SSID 等等。此外，客户端调配策略还将指明要使用的调配向导。自然而然，iPad 的请求方调配将不同于 Android 设备的请求方调配。为确定要向终端调配的包，我们根据操作系统利用 Cisco ISE 中的客户端调配策略将请求方配置文件绑定到调配向导。

创建客户端调配策略

- 步骤 1** 创建本地请求方配置文件。转至 **Policy** → **Policy Elements** → **Results**。
- 步骤 2** 点击 Client Provisioning → Resources。
- 步骤 3** 点击 **ADD**。

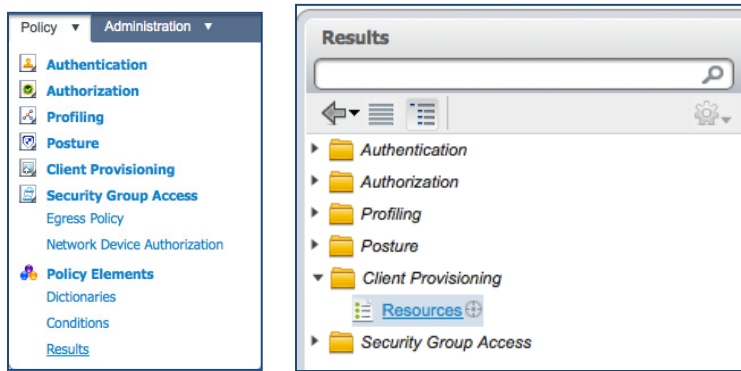


图 13. 客户端调配资源导航

对本地请求方配置文件进行命名

- 步骤 1** 选择操作系统。

注：我们可以为所有操作系统配置一个请求方配置文件。但是，我们将在本文档后续部分依照操作系统指定不同的调配方法。

- 步骤 2** 选择连接类型：**Wired** 和/或 **Wireless**。
- 步骤 3** 按照无线局域网控制器上的配置，键入企业无线 SSID。
- 步骤 4** 选择 Allowed Protocols，在本例中为“**PEAP**”。

Native Supplicant Profile > PEAP-MSCHAPv2

Native Supplicant Profile

* Name: PEAP-MSCHAPv2

Description: PEAP-MSCHAPv2

* Operating System: ALL

* Connection Type: Wired, Wireless

* SSID: BYOD-Dot1x

Security: WPA2 Enterprise

* Allowed Protocol: PEAP

Optional Settings

Save Reset

图 14. 客户端调配资源导航

创建客户端调配策略 (CPP)

在此程序中，我们会创建客户端调配策略来配置 iOS 和 Android 设备的本地请求方。此外，也可以为 Windows 和 Mac OSx 请求方创建 CPP。

- 步骤 1 下载 Windows 和 MAC OSx 的请求方向导。
- 步骤 2 转至 Policy → Policy Elements → Results → Client Provisioning → Resources。
- 步骤 3 在右侧，点击 ADD。
- 步骤 4 选择“Agent resources from Cisco site”。

在本例中，我们选择的是 WinSPWizard 1.0.0.15 和 MacOsXSPWizard 1.0.0.999。

Download Remote Resources...			
<input type="checkbox"/>	Name	Type	Version
<input type="checkbox"/>	MacOsXAgent 4.9.0.652	MacOsXAgent	4.9.0.652
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.3	MacOsXSPWizard	1.0.0.3
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.6	MacOsXSPWizard	1.0.0.6
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.7	MacOsXSPWizard	1.0.0.7
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.998	MacOsXSPWizard	1.0.0.998
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.999	MacOsXSPWizard	1.0.0.999
<input type="checkbox"/>	NACAgent 4.9.0.27	NACAgent	4.9.0.27
<input type="checkbox"/>	NACAgent 4.9.0.28	NACAgent	4.9.0.28
<input type="checkbox"/>	NACAgent 4.9.0.40	NACAgent	4.9.0.40
<input type="checkbox"/>	NativeSPPProfile 1.0.0.0	NativeSPPProfile	1.0.0.0
<input type="checkbox"/>	NativeSPPProfile 1.0.0.1	NativeSPPProfile	1.0.0.1
<input type="checkbox"/>	NativeSPPProfile 1.0.0.2	NativeSPPProfile	1.0.0.2
<input type="checkbox"/>	WebAgent 4.9.0.13	WebAgent	4.9.0.13
<input type="checkbox"/>	WebAgent 4.9.0.14	WebAgent	4.9.0.14
<input type="checkbox"/>	WebAgent 4.9.0.22	WebAgent	4.9.0.22
<input type="checkbox"/>	WinSPWizard 1.0.0.12	WinSPWizard	1.0.0.12

图 15. 本地请求方向导 A

步骤 5 选择最新的请求方向导。

Resources				
Edit + Add Duplicate Delete				
<input type="checkbox"/>	Name	Type	Version	Last Update
<input type="checkbox"/>	NACAgent 4.9.0.37	NACAgent	4.9.0.37	2012/04/14 06:38:31
<input type="checkbox"/>	MacOsXAgent 4.9.0.650	MacOsXAgent	4.9.0.650	2012/04/14 06:38:37
<input type="checkbox"/>	ComplianceModule 3.5.526.2	ComplianceModule	3.5.526.2	2012/04/14 06:38:41
<input type="checkbox"/>	WebAgent 4.9.0.20	WebAgent	4.9.0.20	2012/04/14 06:38:49
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.999	MacOsXSPWizard	1.0.0.999	2012/04/13 01:15:21
<input type="checkbox"/>	PEAP	Native Supplicant Profile	Not Applicable	2012/04/12 23:21:35
<input type="checkbox"/>	WinSPWizard 1.0.0.15	WinSPWizard	1.0.0.15	2012/04/18 00:58:10
<input type="checkbox"/>	EAP_TLS	Native Supplicant Profile	Not Applicable	2012/04/18 01:49:07

图 16. 本地请求方向导 B

为 Apple iOS 创建客户端调配策略

- 步骤 1** 转至 Policy → Client Provisioning。
- 步骤 2** 在右侧，点击 Actions → Insert new Policy above。
- 步骤 3** 创建 Apple iOS CPP 策略。

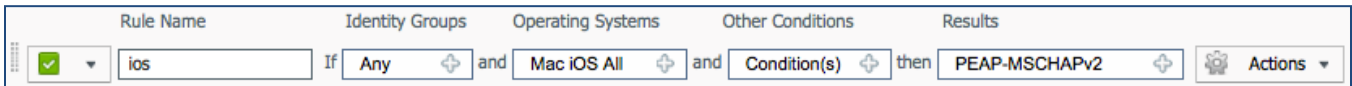


图 17. Apple iOS 客户端调配策略

步骤 4 创建 Android CPP 策略。



图 18. Android 客户端调配策略

步骤 5 (可选)：创建 MAC OSx CPP 策略。

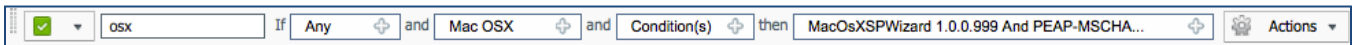


图 19. OSx 客户端调配策略

步骤 6 (可选)：创建 Windows CPP 策略。

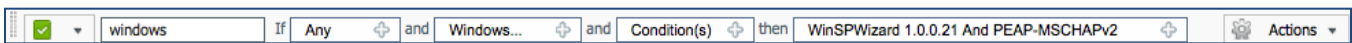


图 20. Windows 客户端调配策略

注： Windows 和 OSx 具有其他请求方调配配置文件，这些配置文件是用于执行请求方和证书调配的基于 Java 的向导，并且可以作为更新的一部分从 cisco.com 下载。

策略配置

在此配置部分中，我们将在无线局域网控制器中创建多个 ACL，它们稍后会在策略中用于重定向为 BYOD 请求方和证书调配选择的客户端，从而在将设备列入黑名单等情况之后拒绝流量。

```
The Cisco Identity Services Engine IP address = 10.35.50.165
Internal Corporate Networks = 192.168.0.0, 172.16.0.0 (to redirect)
```

配置请求方调配 ACL

在此配置部分中，我们将在无线局域网控制器中创建一个 ACL，它稍后会在策略中用于重定向为 BYOD 请求方和证书调配选择的客户端。

步骤 1 导航至 Security → Access Control Lists。

步骤 2 添加名为“NSP-ACL”的新 ACL。

图 1: 用于将客户端重定向至 BYOD 流程的访问控制列表

Access Control Lists > Edit											< Back	Add New Rule
General												
Access List Name		NSP-ACL										
Deny Counters		0										
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	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0	<input checked="" type="checkbox"/>		
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>		
3	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>		
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0	<input checked="" type="checkbox"/>		
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0	<input checked="" type="checkbox"/>		
6	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>		
7	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>		
8	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>		
9	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	<input checked="" type="checkbox"/>		

图 21.

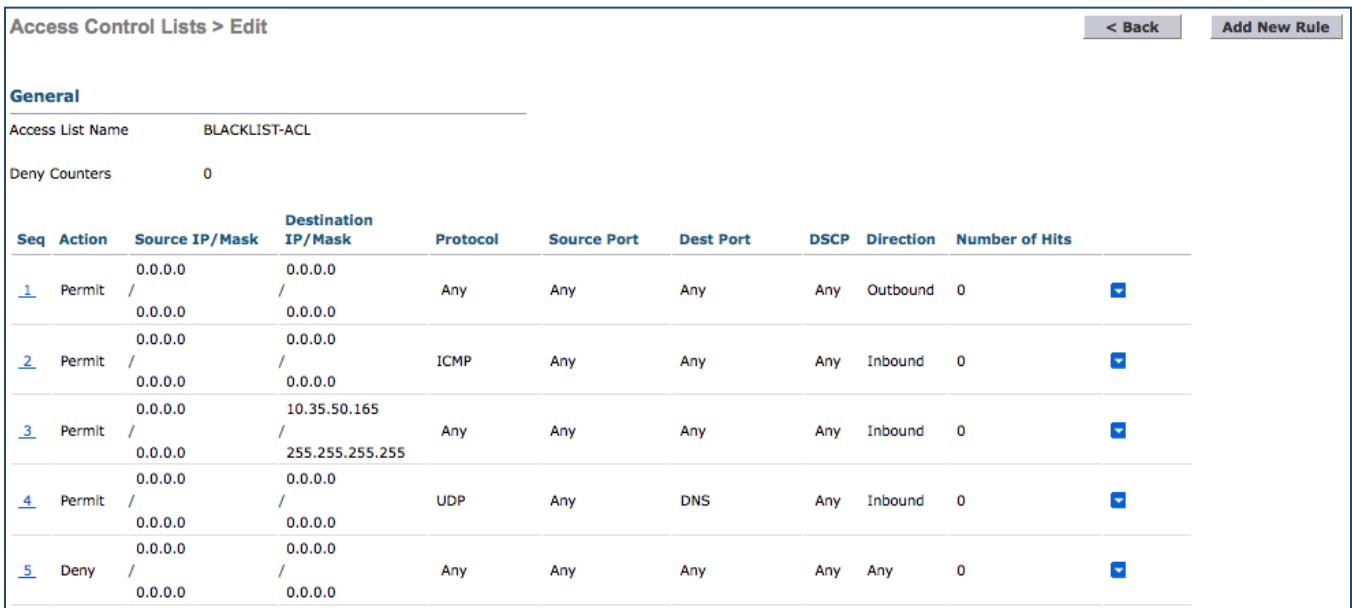
图 17 中 **NSP-ACL** 的说明如下

1. 允许从服务器到客户端的所有“出站”流量。
2. 对于故障排除，允许从客户端到服务器的“入站”ICMP 流量，这是可选的。
3. 允许从客户端到服务器再到 ISE 的所有“入站”流量以执行网络门户和请求方以及证书调配流程。
4. 允许从客户端到服务器的“入站”DNS 流量以进行名称解析。
5. 允许从客户端到服务器的“入站”DHCP 流量以获取 IP 地址。
6. 拒绝从客户端到服务器再到用于重定向至 ISE 的企业资源的所有“入站”流量（根据企业策略）。
7. 拒绝从客户端到服务器再到用于重定向至 ISE 的企业资源的所有“入站”流量（根据企业策略）。
8. 拒绝从客户端到服务器再到用于重定向至 ISE 的企业资源的所有“入站”流量（根据企业策略）。
9. 允许其余所有流量（可选）。

创建黑名单 ACL

在无线局域网控制器中创建一个名为“**BLACKLIST-ACL**”的 ACL，稍后在策略中用于限制对已列入黑名单的设备的访问。

图 2: 黑名单 ACL



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 /	Any	Any	Any	Any	Outbound	0
2	Permit	0.0.0.0 /	0.0.0.0 /	ICMP	Any	Any	Any	Inbound	0
3	Permit	0.0.0.0 /	10.35.50.165 /	Any	Any	Any	Any	Inbound	0
		0.0.0.0 /	255.255.255.255 /						
4	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DNS	Any	Inbound	0
5	Deny	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	0

图 22.

图 18 中 **BLACKLIST-ACL** 的说明如下

1. 允许从服务器到客户端的所有“出站”流量。
2. 对于故障排除，允许从客户端到服务器的“入站”ICMP 流量，这是可选的。
3. 允许从客户端到服务器到黑名单 Web 门户页面的所有“出站”流量。
4. 允许从客户端到服务器的“入站”DNS 流量以进行名称解析。
5. 拒绝其余所有流量。

步骤 3 在无线局域网控制器中创建名为“NSP-ACL-Google”的 ACL，它稍后会在策略中用于调配 Android 设备。

图 3: Google 访问 ACL

Access Control Lists > Edit

General

Access List Name NSP-ACL-Google

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 /	10.35.50.165 /	Any	Any	Any	Any	Inbound	110
		0.0.0.0 /	255.255.255.255 /						
2	Permit	10.35.50.165 /	0.0.0.0 /	Any	Any	Any	Any	Outbound	114
		255.255.255.255 /	0.0.0.0 /						
3	Deny	0.0.0.0 /	10.0.0.0 /	Any	Any	Any	Any	Inbound	5
		0.0.0.0 /	255.0.0.0 /						
4	Deny	0.0.0.0 /	192.168.0.0 /	Any	Any	Any	Any	Inbound	0
		0.0.0.0 /	255.255.0.0 /						
5	Deny	0.0.0.0 /	172.16.0.0 /	Any	Any	Any	Any	Inbound	0
		0.0.0.0 /	255.240.0.0 /						
6	Deny	0.0.0.0 /	171.71.181.0 /	Any	Any	Any	Any	Inbound	0
		0.0.0.0 /	255.255.255.0 /						
7	Permit	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	3449
		0.0.0.0 /	0.0.0.0 /						

图 23.

上图中 NSP-ACL-Google 的说明如下

1. 允许到 ISE 的所有“入站”流量（此步骤为可选）。
2. 允许来自 ISE 的所有“出站”流量（此步骤为可选）。
3. 拒绝到企业内部子网的所有“入站”流量（可以根据企业策略进行配置）。
4. 拒绝到企业内部子网的所有“入站”流量（可以根据企业策略进行配置）。
5. 拒绝到企业内部子网的所有“入站”流量（可以根据企业策略进行配置）。
6. 允许其余所有流量（这可能仅限于 Google Play 子网，但请注意，Google Play 子网可能根据位置而异）。

注：如果需要，可以添加其他行以进行故障排除，例如 ICMP。

注：有关如何仅允许访问 play.google.com 的详细信息，请查阅“附录 B”。如果需要，可以添加其他行以进行故障排除，例如 ICMP。

配置身份验证策略

复合身份验证策略配置。

请审查复合身份验证条件，这些条件稍后将用于策略配置。我们通过审查这些内置策略来确保其存在且未修改，因为在新策略中将对其进行引用。

步骤 1 点击 Policy → Conditions → Authentication → Compound Conditions。

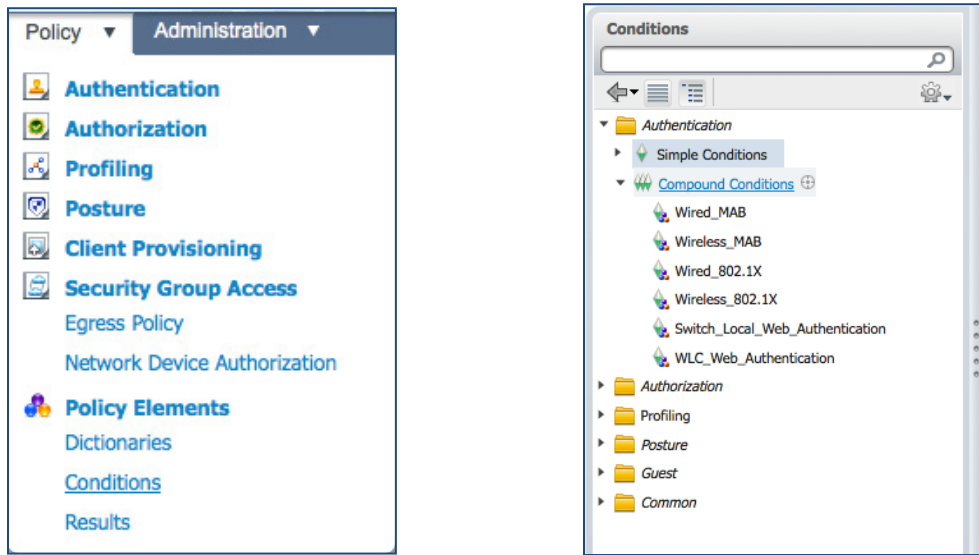


图 24. 注：仅使用集中交换模式对无线进行了测试。

步骤 2 审查名为“Wireless_MAB”的复合条件。

```
“Radius:Service-Type Equals Call Check AND Radius:NAS-Port-Type Equals Wireless - IEEE 802.11”
```

图 4 无线 MAB

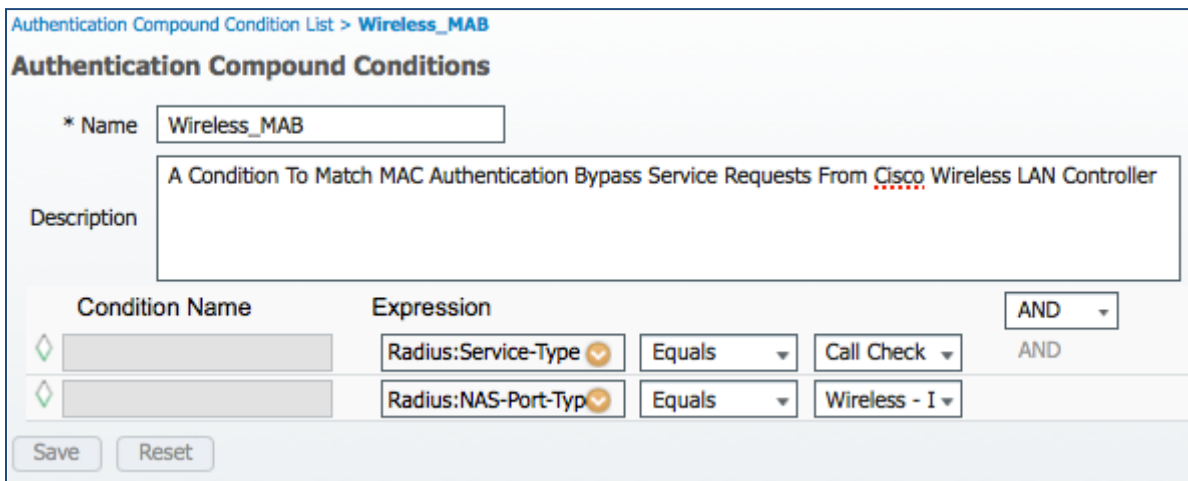
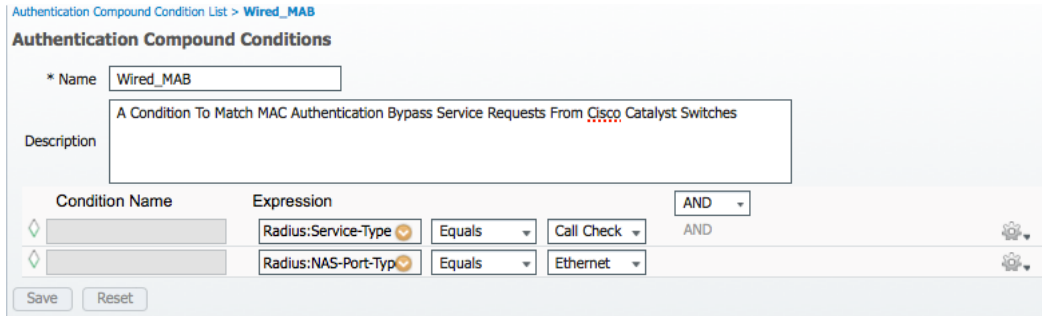


图 25.

步骤 3 审查名为 “Wired_MAB” 的复合条件。

```
“Radius:Service-Type Equals Call Check AND Radius:NAS-Port-Type Equals Ethernet”
```

图 5 有线 MAB



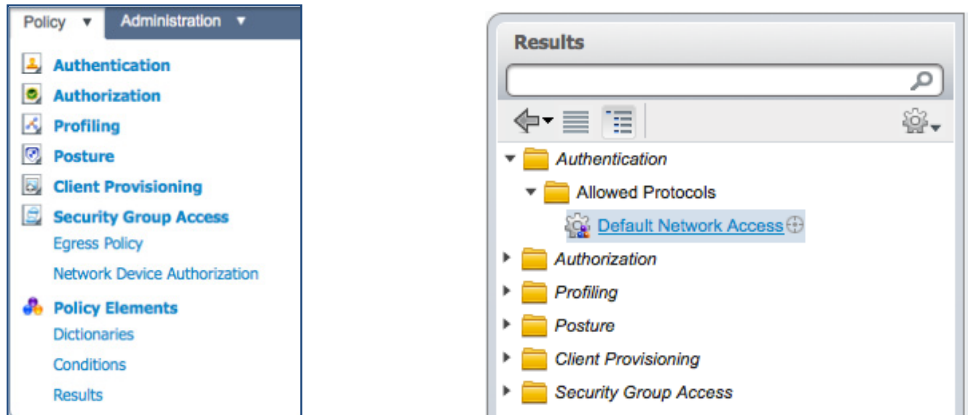
验证默认网络访问结果

本程序介绍 “Default Network Access” 下的当前协议设置。

步骤 1 点击 Policy → Policy Elements → Results。

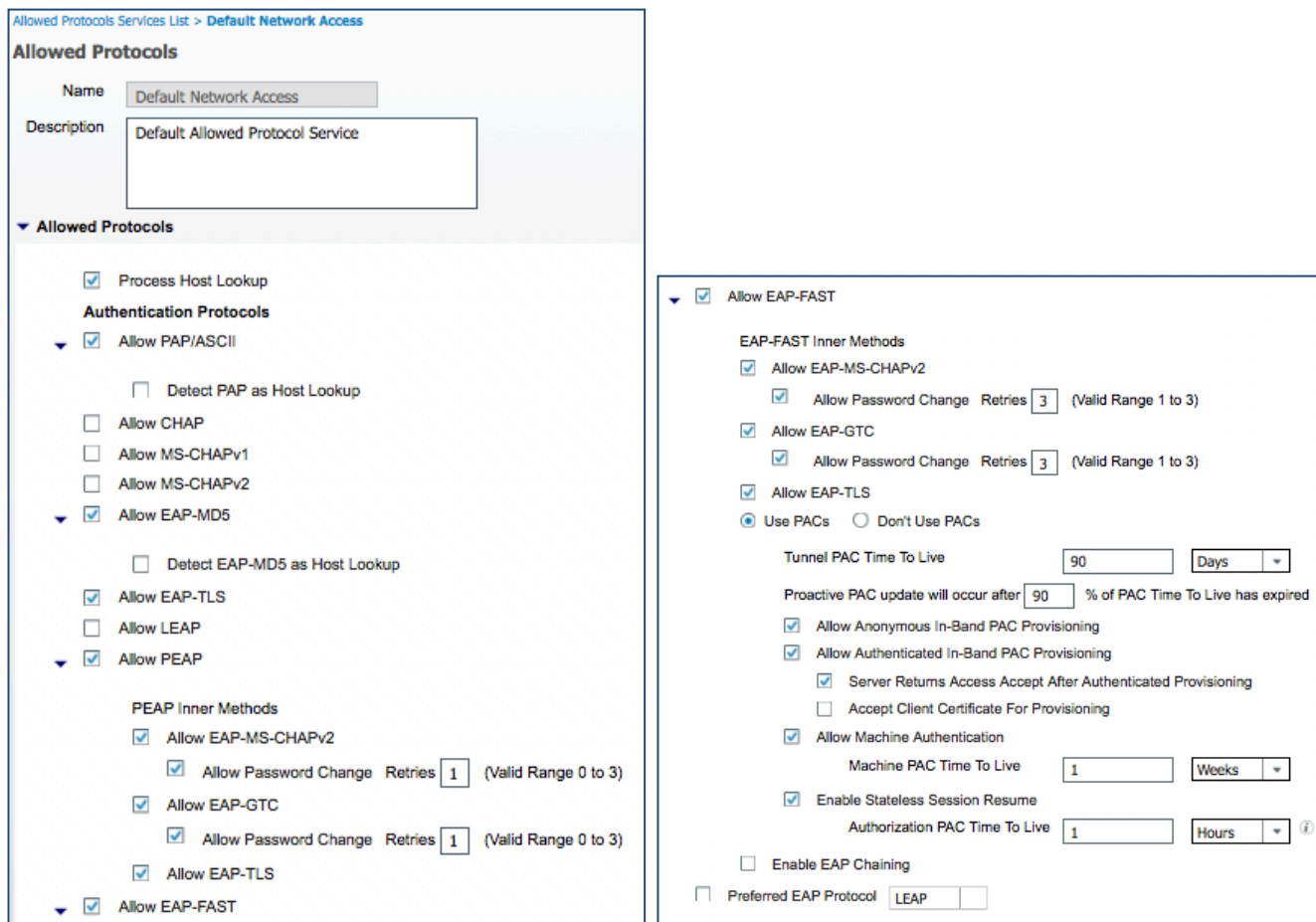
步骤 2 点击 Authentication → Allowed Protocols → Default Network Access。

图 6 默认网络访问导航



注：请根据以下屏幕截图验证协议设置，因为我们将对允许的协议使用预构建默认网络访问对象... 请确保默认对象未更改，并且配置与以下屏幕截图相匹配。

图 7 默认网络访问策略



Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

▼ Allowed Protocols

- Process Host Lookup
- Authentication Protocols**
 - ▼ Allow PAP/ASCII
 - Detect PAP as Host Lookup
 - Allow CHAP
 - Allow MS-CHAPv1
 - Allow MS-CHAPv2
 - ▼ Allow EAP-MD5
 - Detect EAP-MD5 as Host Lookup
 - Allow EAP-TLS
 - Allow LEAP
 - ▼ Allow PEAP
 - PEAP Inner Methods**
 - Allow EAP-MS-CHAPv2
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-GTC
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-TLS
 - ▼ Allow EAP-FAST
 - Allow EAP-FAST
 - EAP-FAST Inner Methods**
 - Allow EAP-MS-CHAPv2
 - Allow Password Change Retries (Valid Range 1 to 3)
 - Allow EAP-GTC
 - Allow Password Change Retries (Valid Range 1 to 3)
 - Allow EAP-TLS
 - Use PACs Don't Use PACs
 - Tunnel PAC Time To Live: Days
 - Proactive PAC update will occur after % of PAC Time To Live has expired
 - Allow Anonymous In-Band PAC Provisioning
 - Allow Authenticated In-Band PAC Provisioning
 - Server Returns Access Accept After Authenticated Provisioning
 - Accept Client Certificate For Provisioning
 - Allow Machine Authentication
 - Machine PAC Time To Live: Weeks
 - Enable Stateless Session Resume
 - Authorization PAC Time To Live: Hours
 - Enable EAP Chaining
 - Preferred EAP Protocol:

图 26.

步骤 3 审查身份验证策略配置，以下屏幕截图是供参考的完整策略视图，各个策略将在后续步骤中进行配置。

图 8 身份验证策略配置

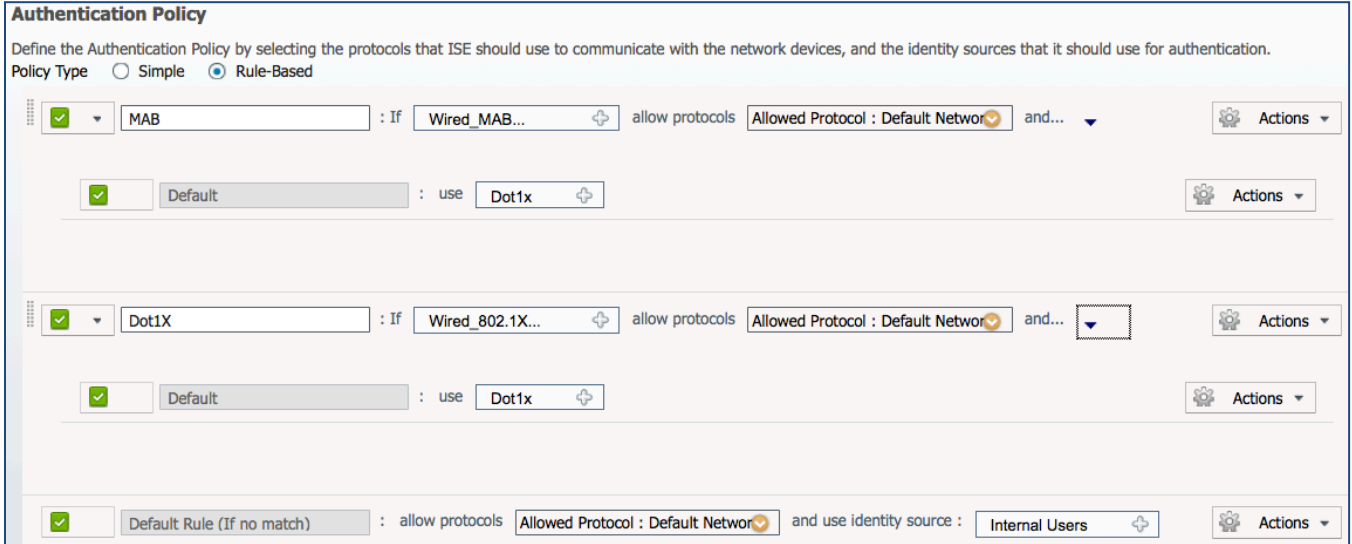
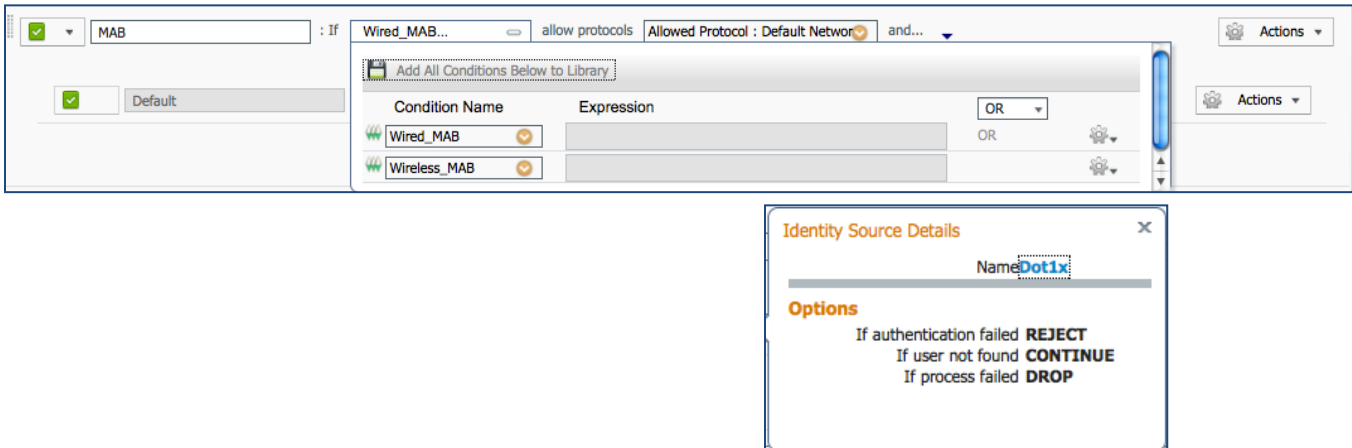


图 27.

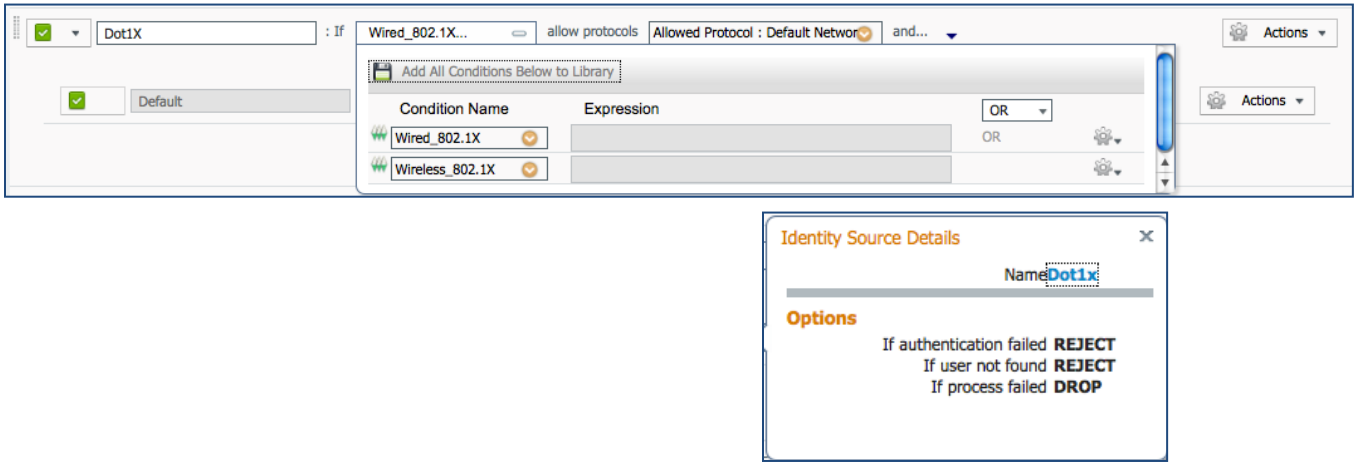
步骤 4 MAB 的身份验证策略，请添加条件 (Wired_MAB OR Wireless_MAB)。

图 9 MAC 身份验证绕行策略



步骤 5 Dot1x 的身份验证策略，请添加条件 (Wired_802.1X OR Wireless_802.1X)。

图 10 802.1X 策略



步骤 6 默认身份验证策略。

图 11 默认身份验证策略

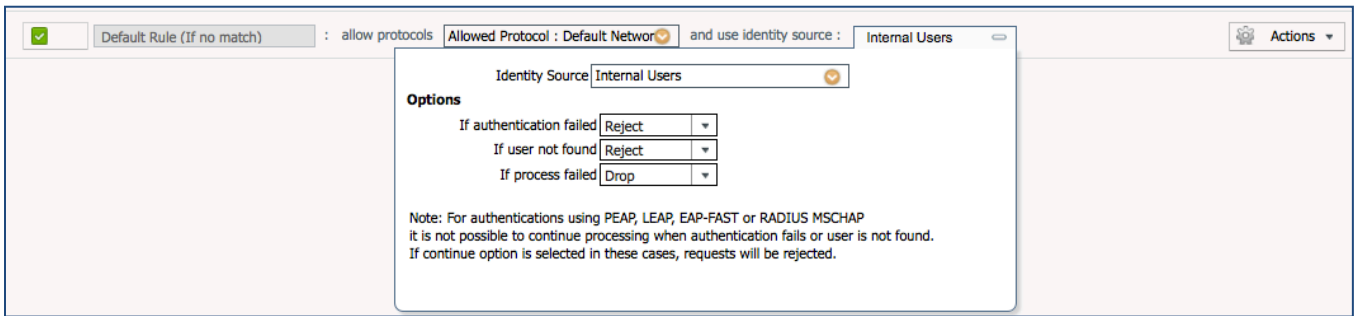


图 28.

配置名为“CWA”的授权策略

- 步骤 1 点击 Policy → Policy Elements → Results。
- 步骤 2 选择 Authorization → Authorization Profiles。
- 步骤 3 点击“ADD”。

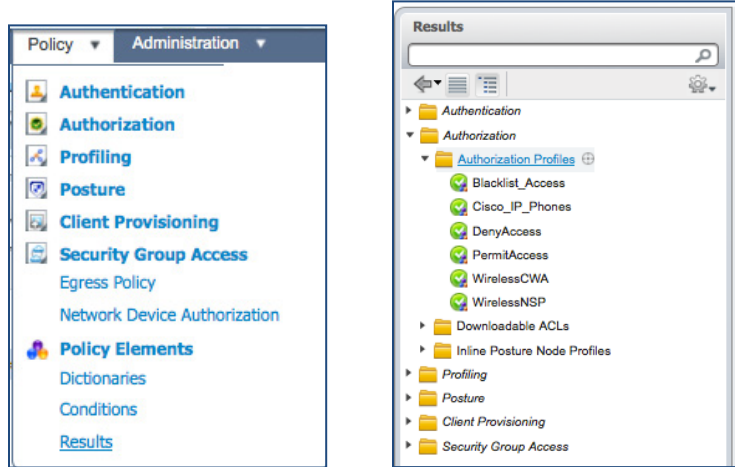


图 29. 授权配置文件导航

步骤 4 添加名为“CWA”的授权配置文件。

集中式 Web 身份验证 (CWA) 使得中央设备充当 Web 门户（此处为思科身份服务引擎）成为可能。在集中式 Web 身份验证中，客户端转向第 2 层以及 Mac/dot1x 身份验证，思科身份服务引擎之后会返回一个特殊属性，向交换机表明必须进行 Web 重定向。全局而言，如果 RADIUS 服务器不知道客户端工作站的 MAC 地址（但还可以使用其他条件来获知），则服务器会返回重定向属性，并且交换机将对该工作站进行授权（通过 MAB），但会采用访问列表将网络流量重定向至该门户。

用户登录访客门户后，可通过授权变更 (CoA) 退回交换机端口，从而进行新的第 2 层 MAB 身份验证。然后，ISE 可以记住其为 webauth 用户，并将第 2 层属性（如动态 VLAN 分配）应用于该用户。ActiveX 组件还可以强制客户端 PC 刷新其 IP 地址。

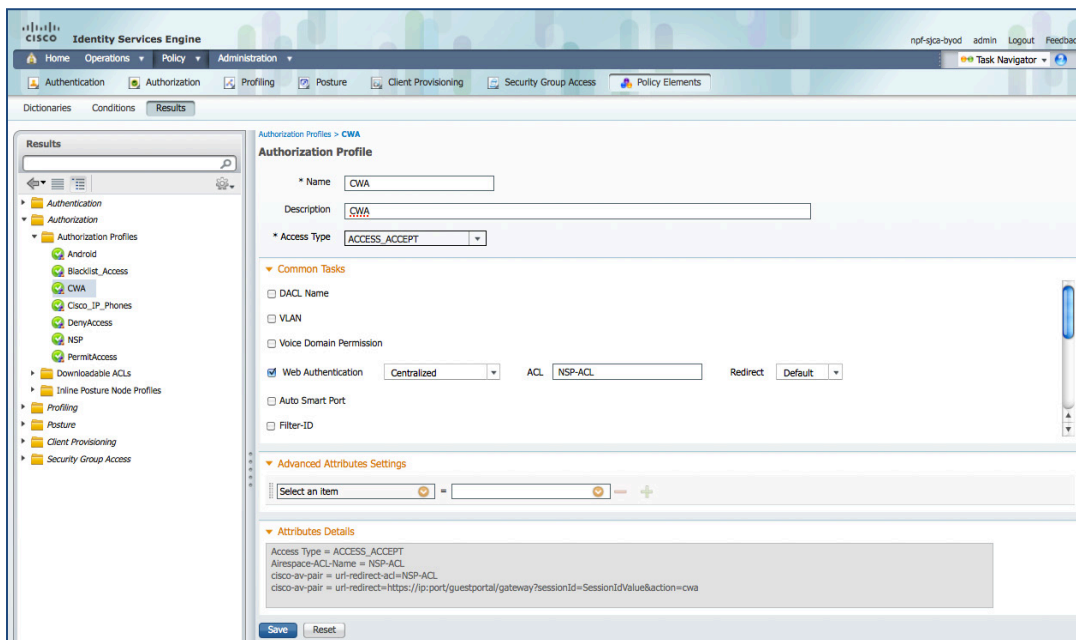


图 30. CWA 授权配置文件

步骤 5 添加名为“CWA_GooglePlay”的授权配置文件。

Android 设备将使用此配置文件允许访问 Google Play，以下载“Cisco Network Setup Assistant”。

The screenshot shows the 'Authorization Profile' configuration interface. The profile name is 'CWA_GooglePlay' and the description is 'CWA'. The access type is set to 'ACCESS_ACCEPT'. Under 'Common Tasks', 'Web Authentication' is checked and configured with 'Centralized' authentication, 'NSP-ACL-Google' ACL, and 'Default' redirect. Under 'Advanced Attributes Settings', there is a configuration entry: 'Select an item' = [dropdown] - +. The 'Attributes Details' section shows the following values: Access Type = ACCESS_ACCEPT, Airespace-ACL-Name = NSP-ACL-Google, cisco-av-pair = url-redirect-ad=NSP-ACL-Google, and cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa. At the bottom, there are 'Save' and 'Reset' buttons.

图 31. 供 Android 用于访问 Google 的 CWA 授权配置文件

审查 Authorization Profiles 下的策略条件

- 步骤 1 点击 Policy → Policy Elements → Results → Authorization → Authorization Profiles。
- 步骤 2 审查名为 “Blacklist_Access” 的配置文件。

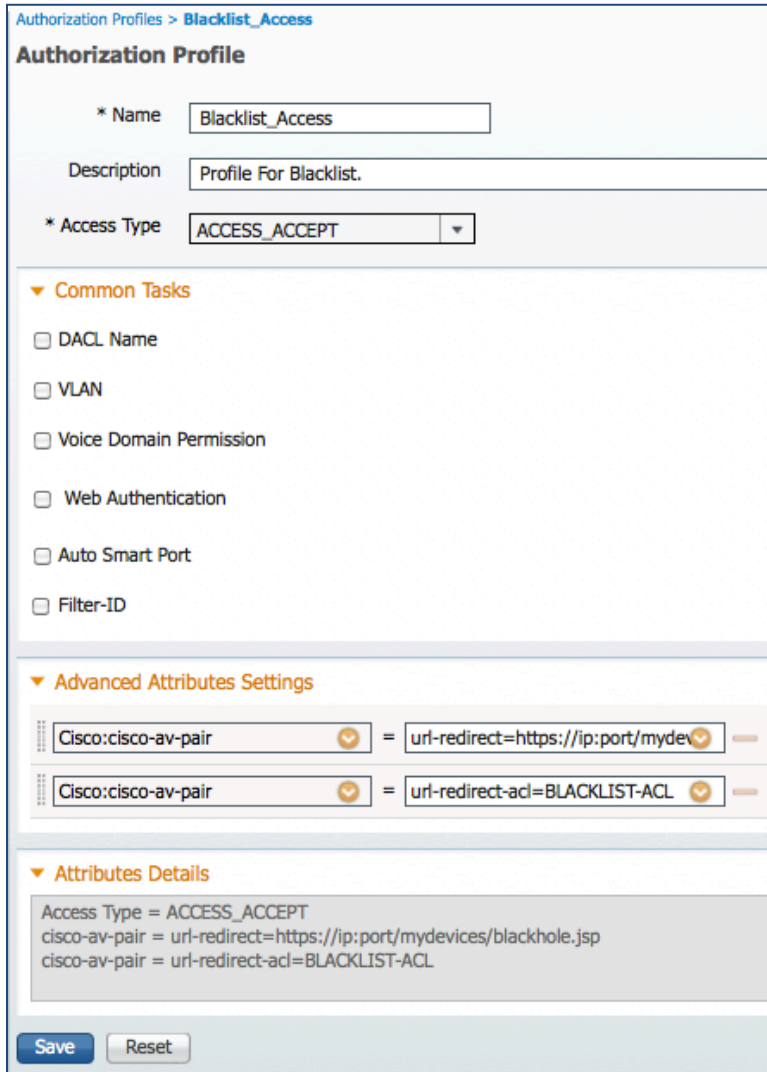


图 32. 黑名单授权配置文件

高级属性设置

```
Cisco:cisco-av-pair = url-redirect=https://ip:port/mydevices/blackhole.jsp  
Cisco:cisco-av-pair = url-redirect-acl=BLACKLIST-ACL
```

步骤 3 创建名为“NSP”的授权配置文件。

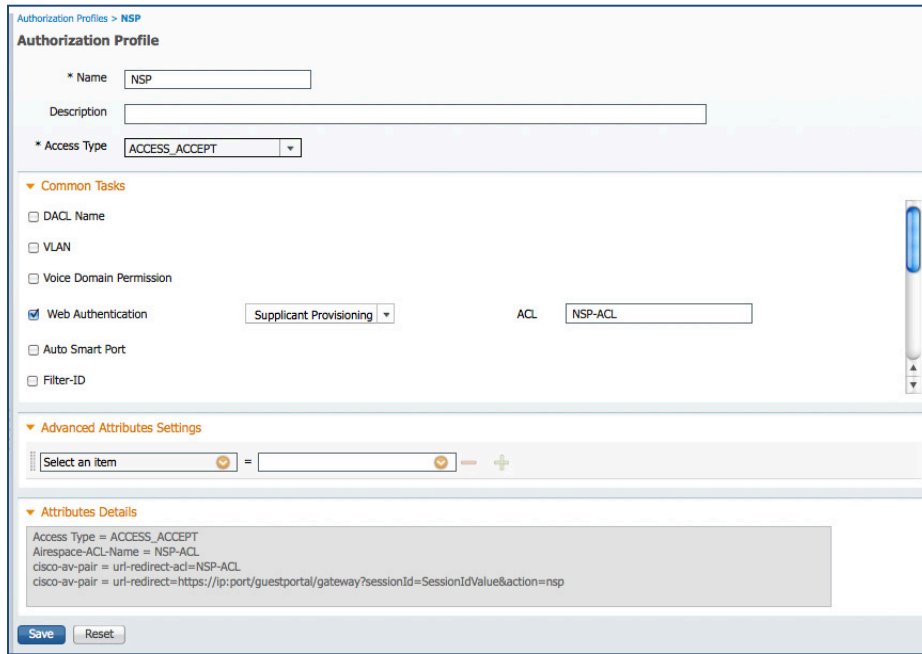


图 33. 本地请求方调配授权配置文件

注：另请点击 Airespace ACL Name 。

步骤 4 创建名为“NSP_Google”的授权配置文件。

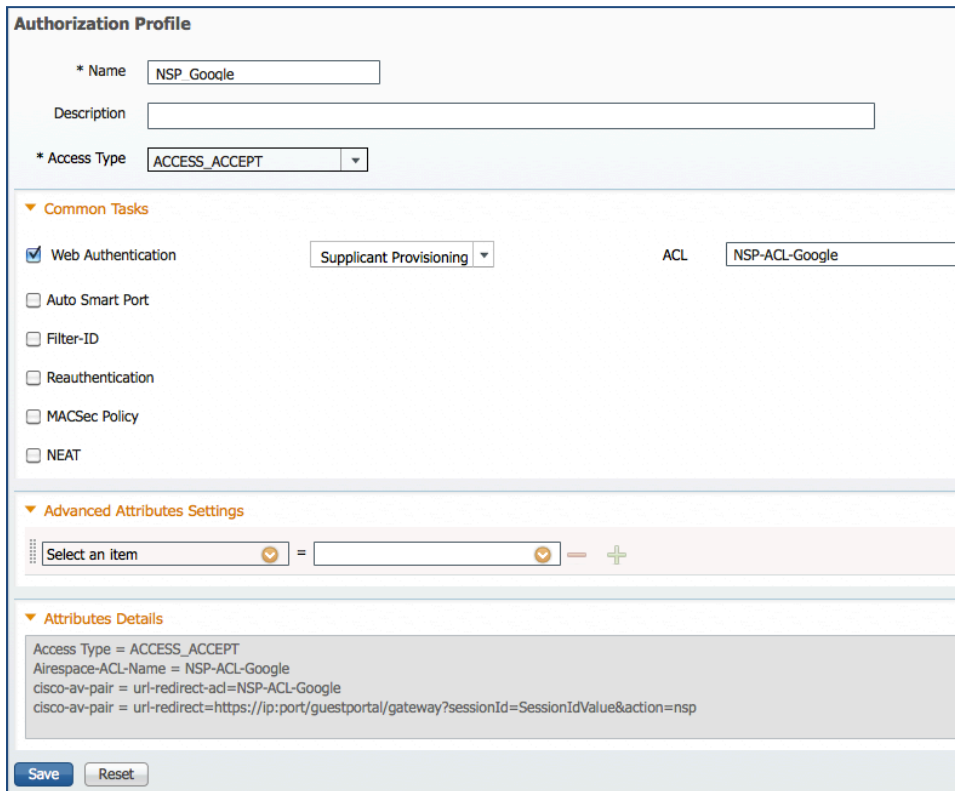


图 34. NSP_Google 授权配置文件

注：另请点击 Airespace ACL Name 。

添加授权策略

步骤 1 点击 Policy → Authorization。

步骤 2 点击 “Insert New Rule Below”。

图 12 插入新规则

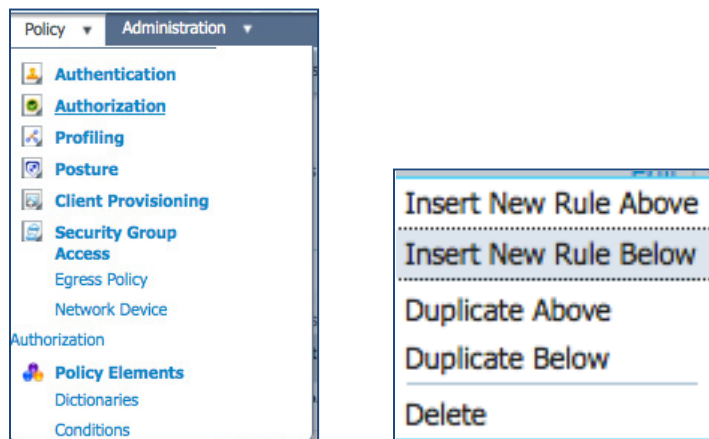


图 35. 插入新规则

步骤 3 请添加以下授权策略。

Black List Default = This is the Default Authorization rule for blacklisting the devices, it could be customized as per company policy where devices could either be redirected to a restricted web page or even not allowed to be on the network once blacklisted.

Profiled Cisco IP Phones = Default Authorization rule for Cisco IP Phones.

Corp_Owned = This Authorization Rule is added for devices which would by-pass BYOD supplicant and certificate provisioning flows when they are classified as corporate assets "Corp_Assets" and coming over Corporate Wireless SSID using 802.1x using protocol MSCHAPV2.

Android_SingleSSID = This Authorization Rule is added for Android devices since they require to download the Cisco Network Setup Assistant to complete the provisioning. The rule is specific to Single SSID setup. Once the Android device hits the "Register" button during device registration, ISE sends a Re-Auth COA to the controller. When the Android connects back to the network the session ID remains same since COA issued from ISE was Ra-Auth and NOT Session Terminate. ISE then applies the NSP_Google permission to continue with the provisioning process

Android_DualSSID = This Authorization Rule is added for Android devices since they require to download the Cisco Network Setup Assistant to complete the provisioning. The rule is specific to Dual SSID setup. Once the Android device hits the "Register" button during device registration, ISE sends a Re-Auth COA to the controller. When the Android connects back to the network the session ID remains same since COA issued from ISE was Ra-Auth and NOT Session Terminate. ISE then applies the NSP_Google permission to continue with the provisioning process

CWA = Authorization rule added for Central Web Authentication.

NSP = This Authorization Rule is added for devices which will go through the BYOD supplicant and certificate provisioning flows when coming over Corporate Wireless SSID using 802.1x using protocol MSCHAPV2.

PERMIT = Devices which have completed BYOD Supplicant and Certificate provisioning, with a certificate using EAP-TLS for authentication and coming over Corporate Wireless SSID will fall under this Authorization Policy.

Default = Default Authorization Policy set as Deny Access.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✔	Wireless Black List Default	if Blacklist AND Wireless_802.1X	then Blacklist_Access Edit ▼
✔	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones Edit ▼
✔	Corp_Owned	if Corp_Assets AND (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then PermitAccess Edit ▼
✔	Android_SingleSSID	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	then NSP_Google Edit ▼
✔	Android_DualSSID	if (Wireless_MAB AND Session:Device-OS EQUALS Android)	then CWA_GooglePlay Edit ▼
✔	CWA	if Wireless_MAB	then CWA Edit ▼
✔	NSP	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then NSP Edit ▼
✔	PERMIT	if Wireless_802.1X	then PermitAccess Edit ▼
✔	Default	if no matches, then	DenyAccess Edit ▼

图 36. 授权策略



您已完成！

如果您对调配证书以及请求方配置文件感兴趣，请参阅操作指南“BYOD-使用证书进行差异化访问”。

附录 A: Android 和 Play.Google.Com

Android 有何独特之处？

用户需要将 Android 设备与 iOS 设备和/或 Windows 区别对待。这一方面是因为没有两个 Android 设备是完全相同的，另一方面是因为要求使用请求方调配应用来为 Android 调配请求方和证书。

默认情况下，Android 设备不会接受来自任意来源的应用；应用必须来自受信任的应用商店，例如“play.google.com”。虽然可以将 Cisco ISE 配置为托管请求方调配向导 (SPW) 应用，但是最终用户的 Android 设备将不会配置为以 Cisco ISE 作为受信任的应用商店。因此，与 Windows、MAC 和 iOS 不同；Android 设备必须有权访问互联网才能参与 BYOD 和本地请求方调配。

在 TrustSec 测试期间，发现 Google Play 在许多情况下会使用 TCP 和 UDP 端口 5228。但是，这并不足以使所有经过测试的 Android 设备都正常工作。互联网搜索（请参阅“附录 C：参考”）结果表明，还可能需打开端口 8880。根据 Android 的配置，系统可能会提示最终用户输入“Internet”或“Play Store”选项。

实验室测试：

Android 选项	要打开的网络范围	TCP 和 UDP 端口
Google Play 选项	74.125.00/16 173.194.0.0/16	TCP/UDP: 5228 TCP/UDP: 8889
Internet 选项	74.125.00/16 173.194.0.0/16	UDP: 5228 TCP: 所有端口

附录 B: BYOD 流程

本节涵盖 iOS 和 Android 设备的 BYOD 流程。

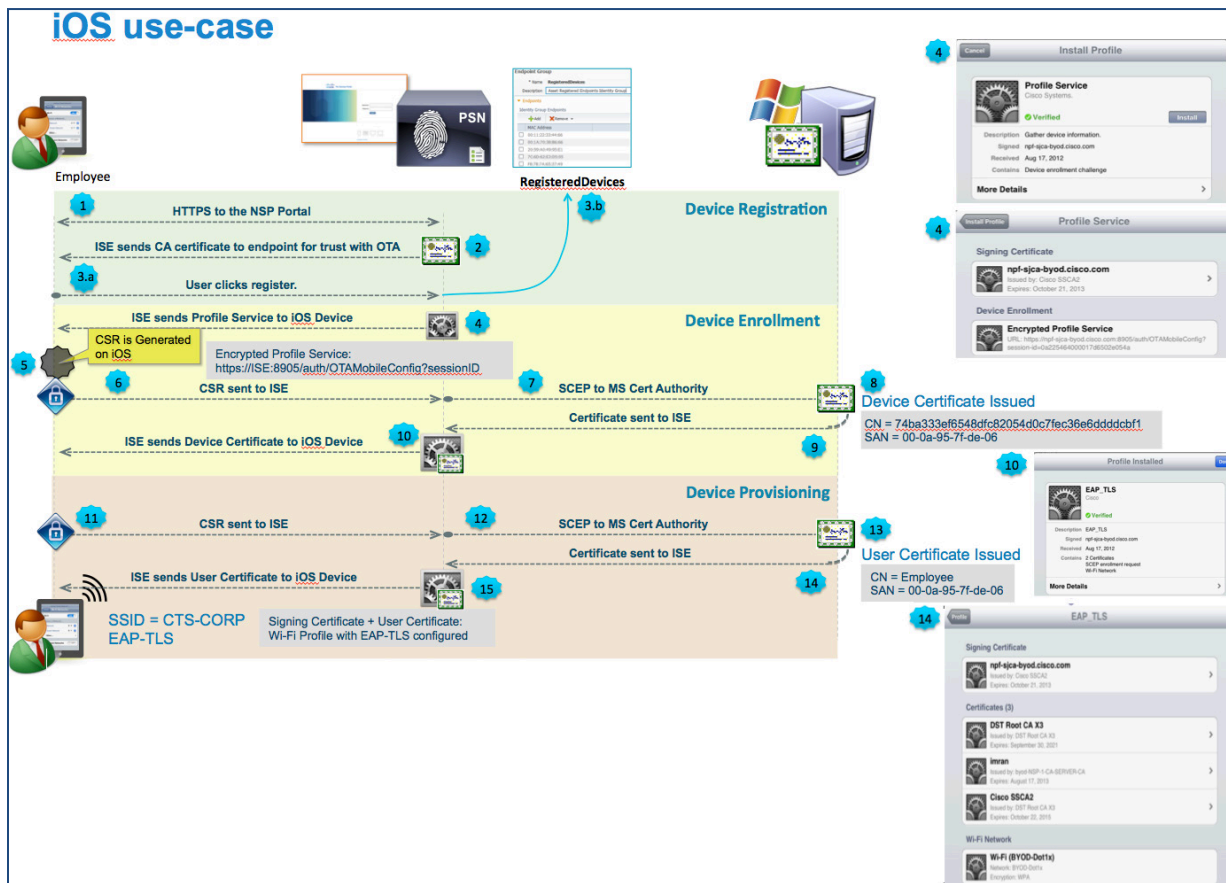


图 37. iOS 和 Android 设备的 BYOD 流程

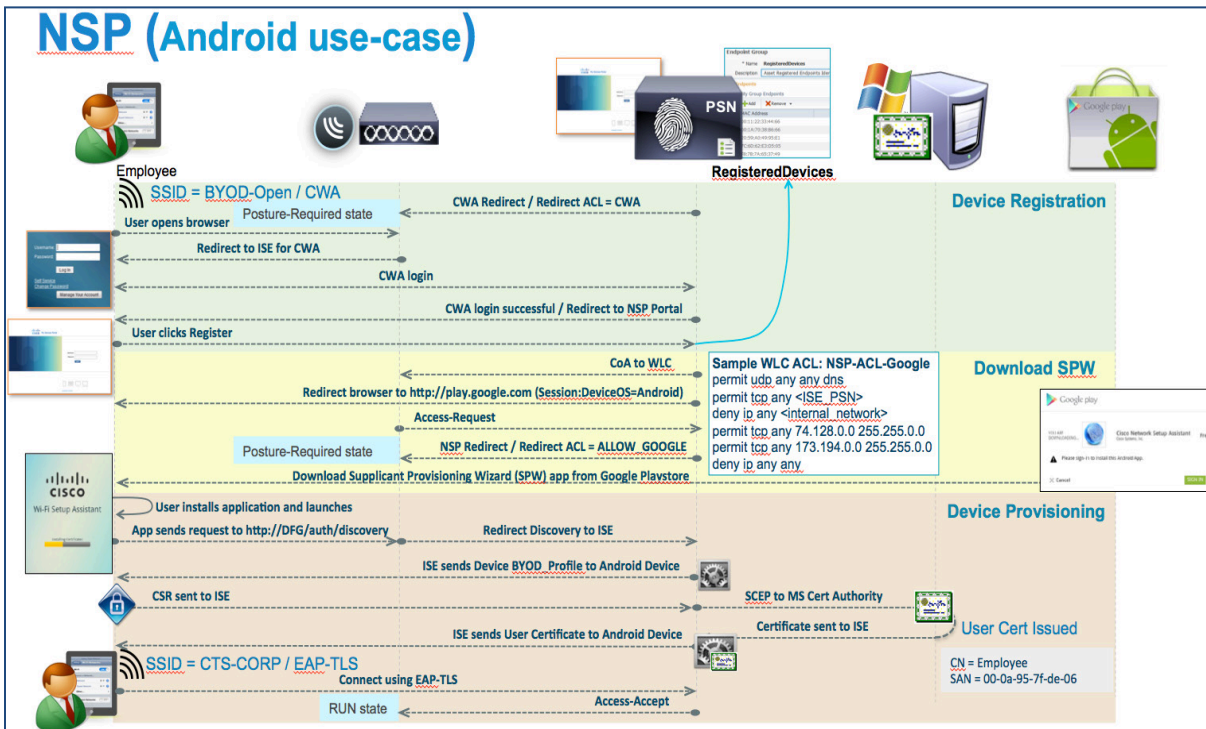


图 38. Android 使用案例

附录 C：参考

Cisco TrustSec 系统

<http://www.cisco.com/go/trustsec>

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

设备配置指南：

思科身份服务引擎用户指南：

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

有关思科 IOS 软件、思科 IOS XE 软件和思科 NX-OS 软件版本的更多信息，请参阅以下 URL：

对于 Cisco Catalyst 2900 系列交换机：

http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000 系列交换机：

http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000-X 系列交换机：

http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 4500 系列交换机：

http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 6500 系列交换机：

http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

对于 Cisco ASR 1000 系列路由器：

http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

对于思科无线局域网控制器：

http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html