



使用证书区分思科身份服务引擎的访问

安全访问操作指南系列

作者：Imran Bashir

日期：2013 年 9 月

目录

概述.....	3
数字证书	3
证书调配	3
方案概览	4
架构图	5
组件	6
思科身份服务引擎配置.....	7
确定 BYOD 流程的用户	7
创建证书身份验证配置文件	10
创建身份源序列	11
创建客户端调配策略	13
为 BYOD 自行激活准备 WLC	18
配置身份验证策略.....	21
简单证书注册协议 (SCEP) 设置.....	33
附录 A: 配置 SCEP 服务器	34
设置 SCEP 服务器	34
配置 SCEP 注册	36
分配新的颁发模板.....	45
附录 B: Android 和 Play.Google.Com	50
为什么 Android 与众不同.....	50
附录 C: BYOD 流程.....	51
附录 D: 参考	53
Cisco TrustSec 系统:	53
设备配置指南:	53

概述

本操作指南说明如何使用证书区分企业设备与非企业设备，以及如何根据这种区分来应用不同的授权策略。本操作指南还介绍如何设置系统自行激活，包括本机请求方调配、所推送的证书类型，以及可将证书内的哪些字段用于编写策略从而区分访问。

数字证书

虽然分析可作为一种终端识别和分类方法，但数字证书也可用于提供类似使用数字证书并结合分析可以进一步提供更加准确的终端指纹识别机制。

通过公钥加密实现的数字签名为设备和用户提供了一种身份验证方法。在 RSA 加密系统等公钥加密中，每位用户都有一个包含公钥和私钥的密钥对。这一对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密。

简言之，使用私钥加密数据时会形成一个签名。此签名附加在数据中并发送给接收者，接收者对数据应用发送者的公钥，如果随数据一起发送的签名与对数据应用公钥的结果一致，就会确立消息的有效性。此过程的前提是接收者拥有发送者的公钥副本而且非常确定此密钥属于发送者，而不是伪装成发送者的其他人。

证书调配

思科身份服务引擎请求方调配支持部署请求方配置文件。调配 EAP-TLS 配置文件还包括调配数字证书。在这种情况下，思科身份服务引擎策略服务节点 (PSN) 充当发起 SCEP 请求的终端的注册机构。

表 1 列出支持的平台、下载之后证书的位置和查看或清除证书的相应位置。

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（配置配置文件）	查看路径为：Settings → General → Profile	5.0 及以上
Android	设备加密的证书库	无法查看。但是可以清除，路径为：Settings → Location & Security → Clear Storage（清除所有设备证书和密码）	3.2 及以上

设备	证书库	证书信息	版本
Windows	用户证书库	可以通过启动 MMC 证书管理单元进行查看。	WindowsXP – SP3 Windows Vista – SP? Windows7 – 全部版本
MacOS-X	密钥链	可以通过启动应用查看，路径为：→ Utilities → Keychain Access	MacOS-X 10.6 和 10.7

注：MACOS-X 10.8 有以下警告

当我们在 Security & Privacy Preference 窗格中选择“MAC App Store and identified developers”选项时，无法安装 SPW（请求方 MAC）。

安装 SPW 配置文件/证书时，会多次弹出信息。

调配的证书将具有以下属性：

Common Name (CN) of the Subject:
用于身份验证的用户身份

Subject Alternative Name: 终端的 MAC 地址。

PERMIT if (Wireless_802.1X AND Radius:Calling-Station-ID EQUALS then PermitAccess
CERTIFICATE:Subject Alternative Name) Edit

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

警告：应从头到尾遵从本文档的指导，略过其中的内容可能会造成不良后果。

方案概览

本文档将讨论个人设备的自行激活，其中员工将自行激活一台新设备，并且系统将自动为该用户和设备调配证书，此证书将随预配置为使用该证书并将该设备连接至企业网络的请求方配置文件一起安装。思科 ISE 策略还将配置为根据证书为用户/设备提供差异化访问。

为了解释本文档中使用的场景，我们不妨来看一下 iPad 的本机请求方调配和授权的一个示例：

1. 某员工使用自己的新 iPad 连接企业无线 SSID。
2. iPad Web 浏览器将重定向到托管于思科 ISE 策略服务节点 (PSN) 上的自助注册门户。
3. 该员工需要在 Web 门户中输入其凭证。

4. 系统将按照企业 Active Directory 或其他企业身份库对该员工的凭证进行身份验证。
5. PSN 将向下发送生成证书签名请求 (CSR) 的 Apple Over-the-Air (OTA) 调配配置文件。
6. iPad 将 CSR 发送至充当注册机构的策略服务节点，此节点将此请求发送至 Active-Directory 证书颁发机构 (CA)。
7. Active Directory 证书颁发机构将颁发证书并将其发送回思科 ISE 策略服务节点。
8. 利用 OTA，思科 ISE PSN 向此 iPad 发送一个新配置文件，其中包含所颁发的嵌入了该 iPad 的 MAC 地址及此员工 AD 用户名的证书，同时还将发送一个强制将 EAP-TLS 用于 802.1X 身份验证的 Wi-Fi 请求方配置文件。
9. iPad 即已配置为通过身份验证 EAP-TLS 与企业无线网络关联（以防双 SSID 员工需要手动连接至企业 SSID；在单 SSID 情况下，iPad 会自动通过 EAP-TLS 重新连接），并且思科 ISE 授权策略将使用证书中的属性强制实施网络访问（例如，提供有限访问，因为这不属于企业资产）。

架构图

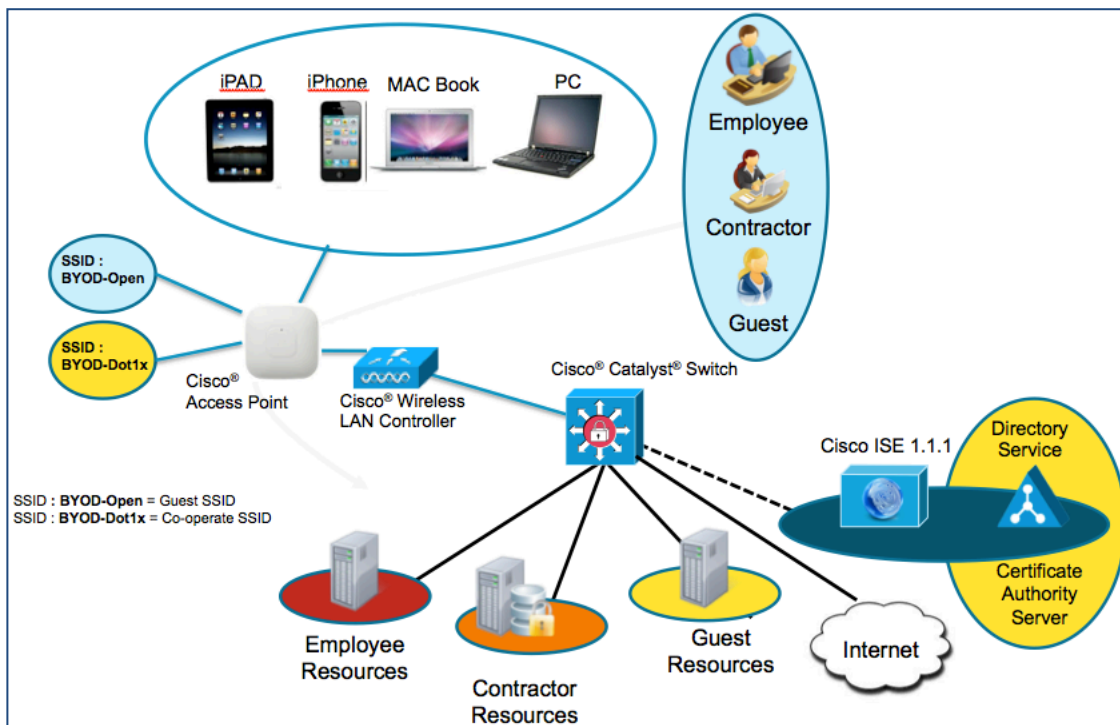


图 1. 架构图

组件

表 2. 本文中使用的组件

组件	硬件	经过测试的特性	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
证书颁发机构服务器	任意，依据 Microsoft 的规范 (Windows 2008 R2 Enterprise SP2)	SCEP，证书颁发机构服务器	N/A
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：无线接入仅针对集中交换模式进行了测试。

思科身份服务引擎配置

本节介绍实施操作指南中描述的使用案例所需执行的步骤。这包括从基本配置（如创建用户组）到高级配置（例如创建用于 EAP-TLS 的请求方配置文件，以及创建用于检查证书的身份验证策略）的全部内容。

确定 BYOD 流程的用户

在用户自行激活过程中（自行激活一词是指注册某个资产并将该资产请求方调配为能够访问企业网络的一个过程），我们可以选择身份库来定义要转发至自行激活 (BYOD) 流程的资源。以下示例说明在思科身份服务引擎的本地库中以及在 Active Directory 中定义的用户，这是身份源序列的组成部分。

作为最佳实践自行激活程序的一部分，我们将 Active Directory 作为身份源来确定允许哪一组（哪些组）用户自行激活其设备。以下程序说明在思科 ISE 本地用户数据库中以及在 Active Directory 中定义的用户，这是身份源序列的组成部分。

用户组是具有相同权限，可允许其访问特定思科 ISE 服务和功能的个人用户或终端的集合。例如，如果您属于 Change User Password 管理员组，就可以更改其他用户的管理密码。

配置用户组

步骤 1. 导航至 Administration → Identity Management → Groups。

步骤 2. 点击 ADD。

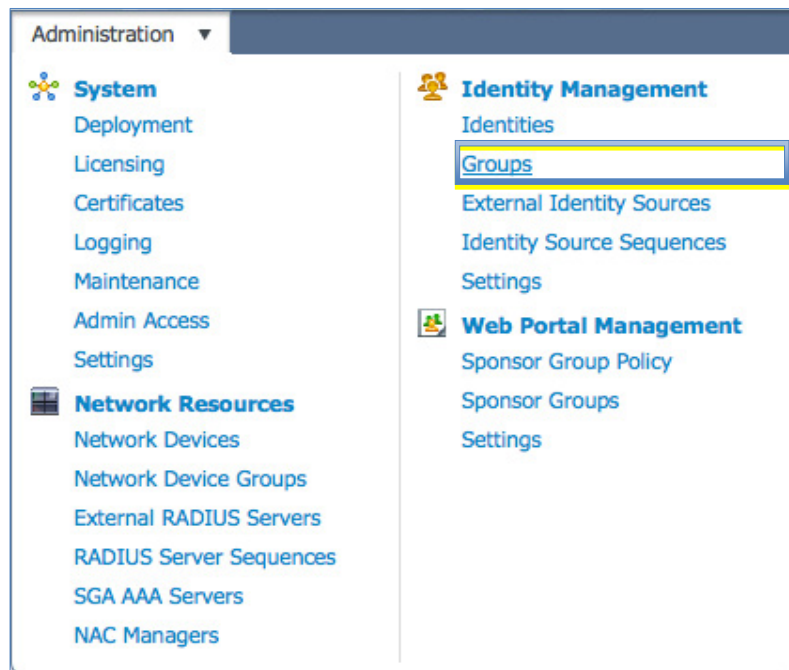


图 2. 身份组导航

步骤 3. 创建身份组。

在本示例中我们将自己的身份组命名为“Employee”。

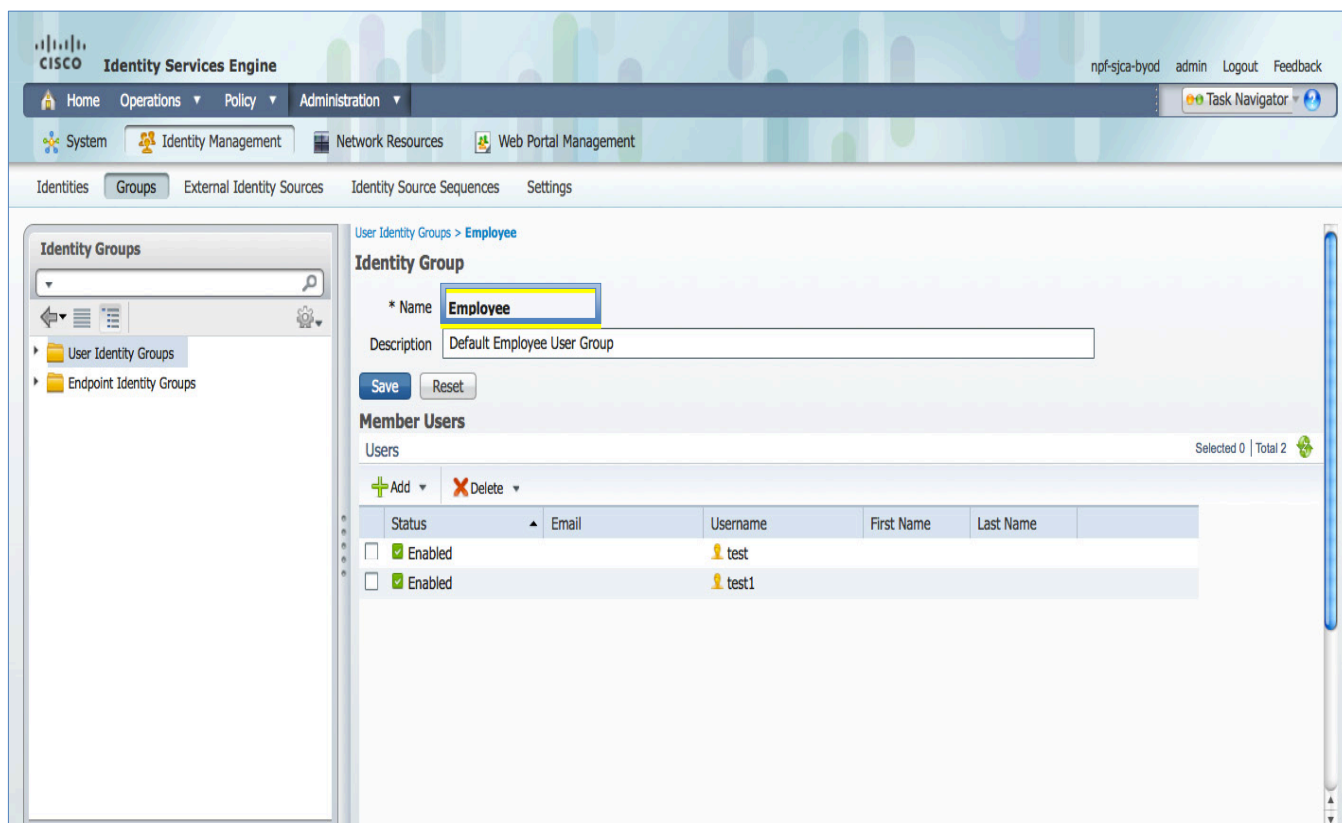
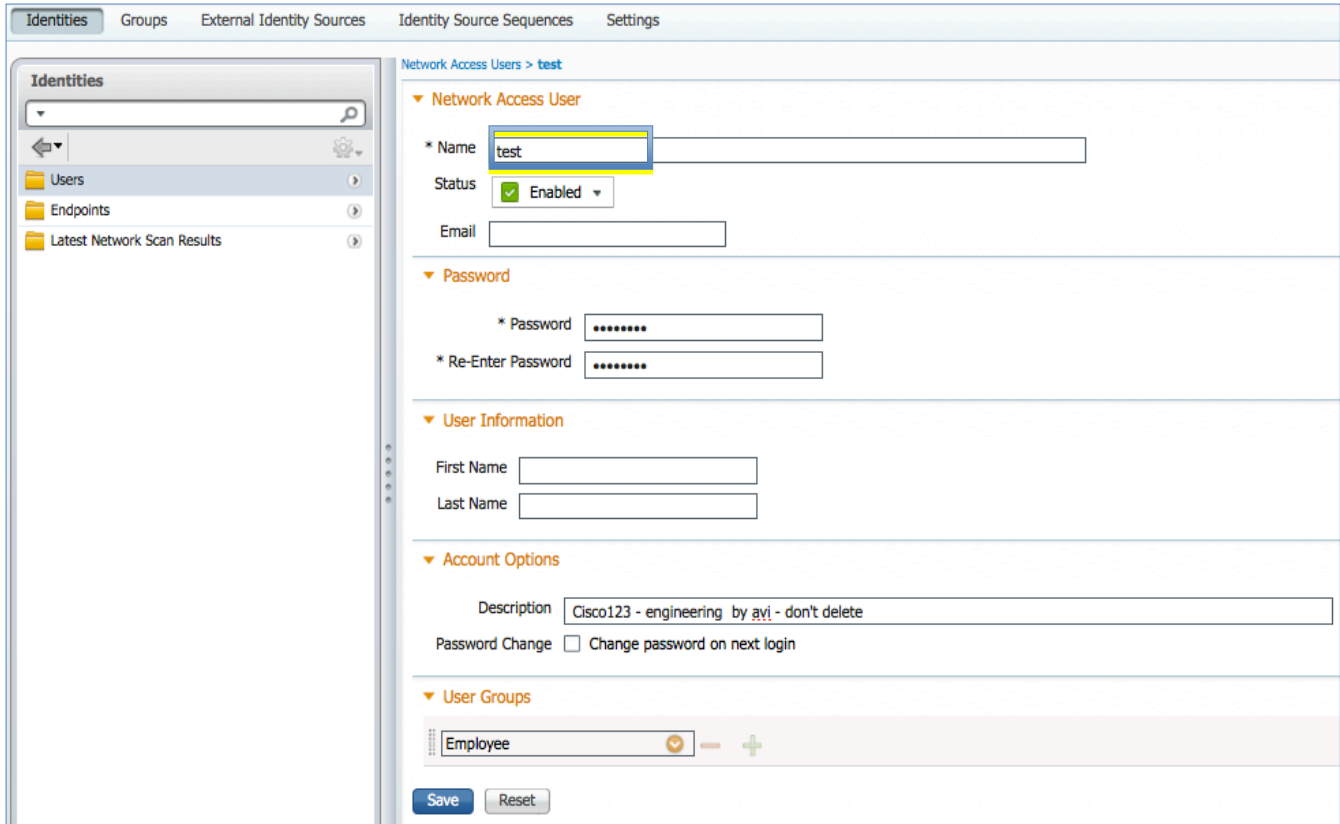


图 3. 用户身份组

在 Employee 组中创建一个用户

步骤 4. 导航至 Administration → Identity Management → Identities → Users。

步骤 5. 点击 ADD。



The screenshot shows the Cisco ISE user configuration interface. The top navigation bar includes 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The left sidebar shows a tree view with 'Identities' selected, containing 'Users', 'Endpoints', and 'Latest Network Scan Results'. The main content area is titled 'Network Access Users > test'. It features several sections: 'Network Access User' with fields for Name (test), Status (Enabled), and Email; 'Password' with fields for Password and Re-Enter Password; 'User Information' with fields for First Name and Last Name; 'Account Options' with a Description field (Cisco123 - engineering by avi - don't delete) and a checkbox for 'Change password on next login'; and 'User Groups' with a dropdown menu showing 'Employee'. At the bottom, there are 'Save' and 'Reset' buttons.

图 4. 用户帐户

创建证书身份验证配置文件

证书身份验证配置文件 (CAP) 在身份验证策略中用于基于证书的身份验证。CAP 在证书中定义特定属性，以便作为额外的身份源进行查看和使用。例如，如果用户名在证书的 CN= 字段，您将创建用来检查 CN= 字段的 CAP。然后，系统将按照 Active Directory 等其他身份源使用和检查那些数据。证书身份验证配置文件允许您指定以下项目：

- 应作为主要用户名的证书字段
- 是否应对证书执行二进制比较

注： Certificate Authentication Profiles 页会列出您已添加的配置文件。

创建证书授权配置文件

步骤 1. 导航至 Administration → External Identity Sources → Certificate Authorization Profile。

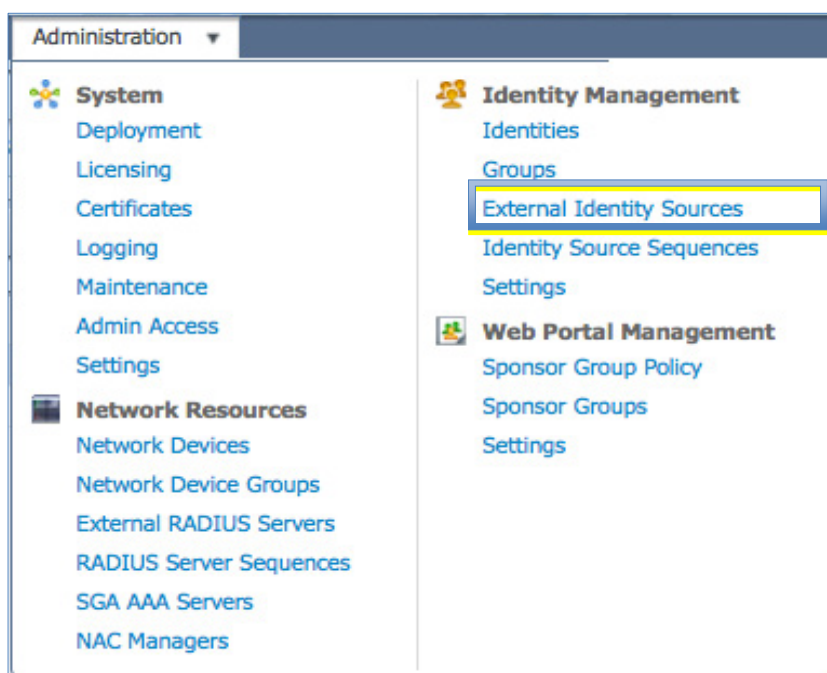


图 5. 导航

步骤 2. 点击 ADD 并给该配置文件命名，本示例中将其命名为“Cisco_CAP”。

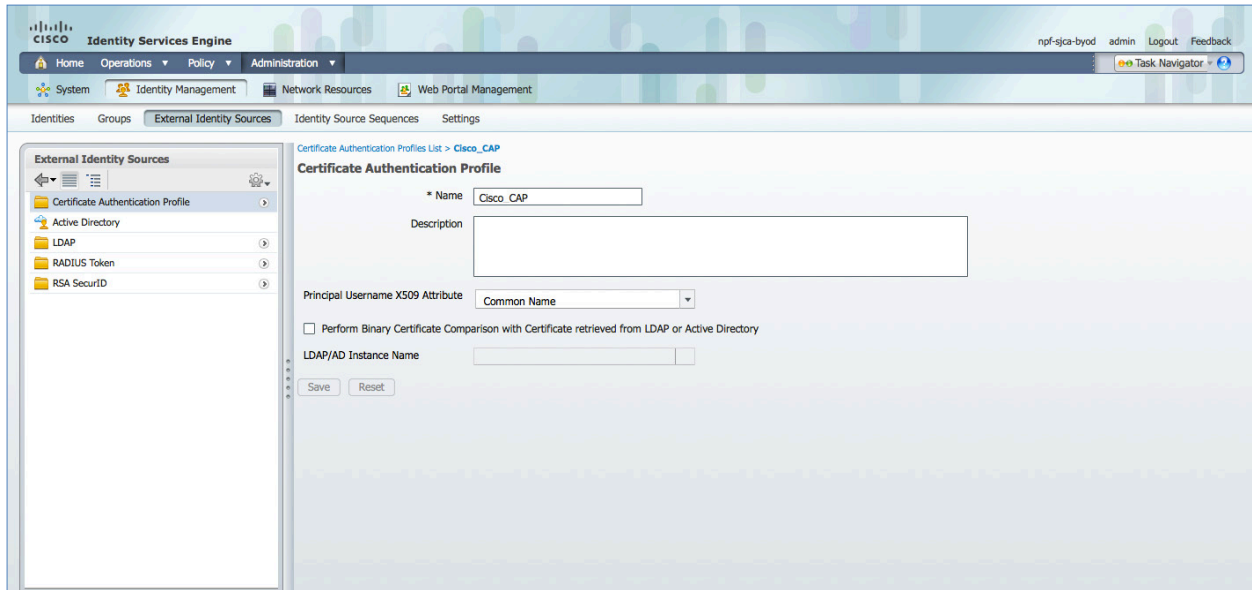


图 6. 证书身份验证配置文件

创建身份源序列

身份源序列用于定义思科 ISE 在不同数据库中查找用户凭证的顺序。思科 ISE 支持以下数据库：内部用户、内部终端、Active Directory、LDAP、RSA、RADIUS 令牌服务器和证书身份验证配置文件。

如果贵组织将凭证存储于以下多个身份库中，那么您可以定义身份源序列，指定您希望思科 ISE 在这些数据库中查找用户信息的顺序。当检索到匹配项后，思科 ISE 将停止查找，但是会评估凭证并将授权结果返回至网络接入设备。此策略是第一个匹配策略。

创建身份源序列。

步骤 1. 导航至：Administration → Identity Source Sequence。

步骤 2. 点击 ADD。



图 7. 管理→身份源序列

步骤 3. 为序列命名。

在本例中我们将此序列命名为“Dot1x”。

步骤 4. 选择在本节中前面部分创建的名为“Cisco_CAP”的证书身份验证配置文件。

步骤 5. 在 **Authentication Search List** 中选择 Active Directory 服务器 (AD1)、内部终端和内部用户。

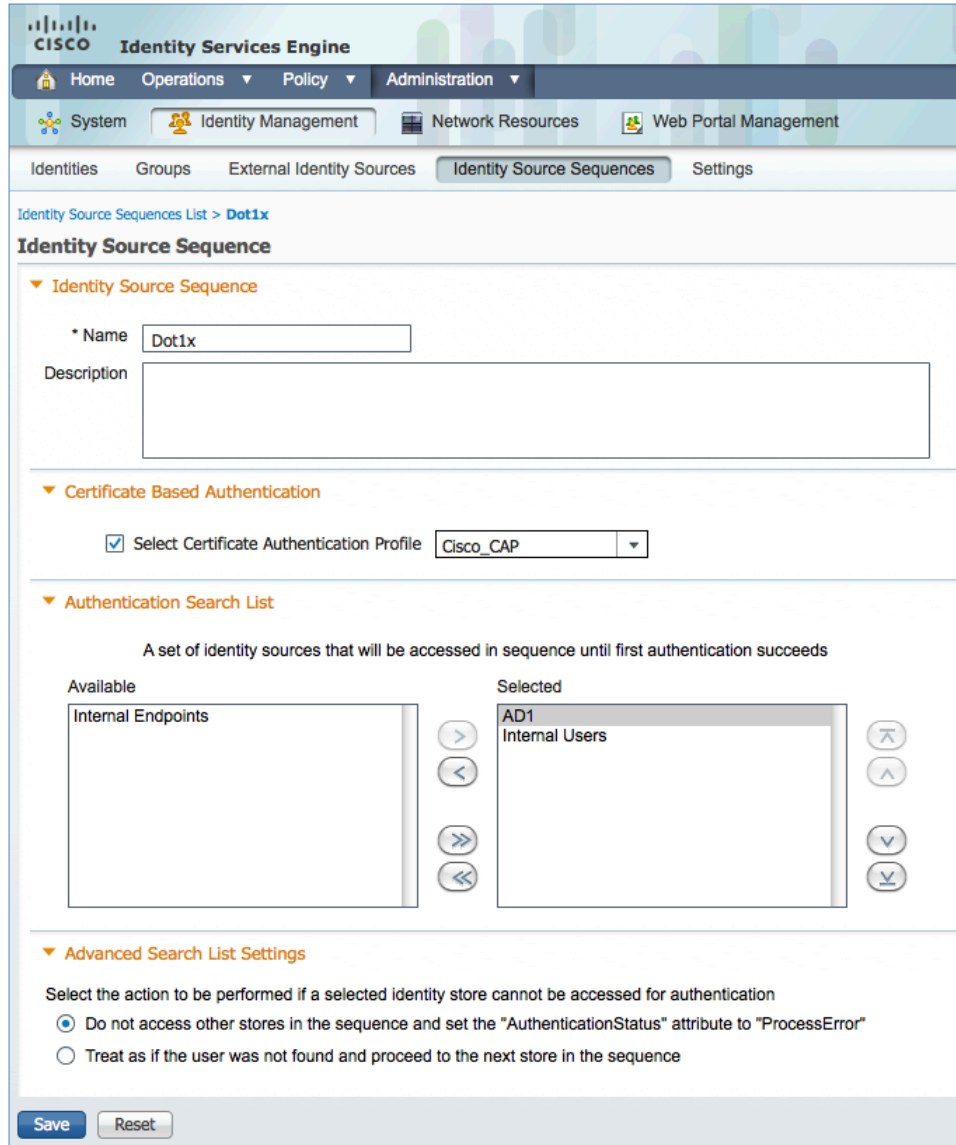


图 8. 身份源序列

创建客户端调配策略

思科身份服务引擎在划分用户访问内部网络的登录会话类型时会考虑各种元素。我们可以利用客户端调配策略创建请求方配置文件，以便配置终端（例如 iPhones、iPad、Windows、MAC OSx。）

利用本机请求方调配 (NSP)，思科 ISE 会对不同操作系统采用不同调配策略。每个策略都将包含一个“本机请求方配置文件”，此文件指示是使用 PEAP 还是 EAP-TLS、所要连接的无线 SSID 等信息。此外，客户端调配策略还会涉及所要使用的调配向导。当然，iPad 的请求方调配不同于 Android 设备的调配。为了确定为终端调配哪个数据包，我们按照操作系统利用思科 ISE 中的客户端调配策略，将请求方配置文件与调配向导绑定。

创建本机请求方配置文件

- 步骤 1. 转至 Policy → Policy Elements → Results。
- 步骤 2. 点击 Client Provisioning → Resources。
- 步骤 3. 点击 ADD。

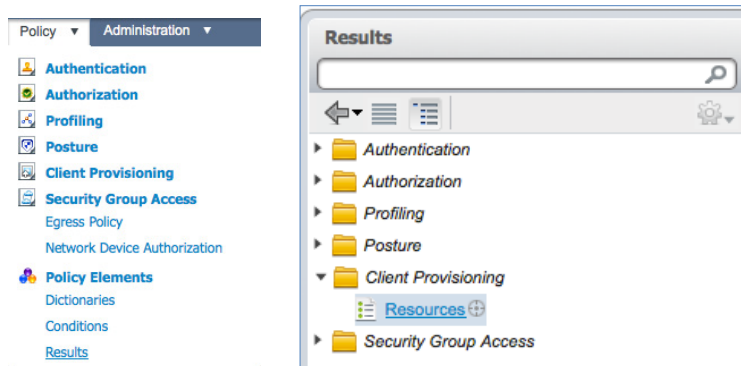


图 9. 客户端调配资源导航

为本机请求方配置文件命名

- 步骤 1. 选择操作系统。

注：我们可以为所有操作系统配置同一个请求方配置文件。但是，下文中我们将按照操作系统指定不同的调配方法。

- 步骤 2. 选择 Connection Type: **Wired** 和/或 **Wireless**。
- 步骤 3. 按照无线局域网控制器上的配置，键入贵公司无线 SSID。
- 步骤 4. 选择 Allowed Protocols，在本示例中因为使用的是证书，所以要选择“**TLS**”。
- 步骤 5. 选择密钥大小：**1024**。

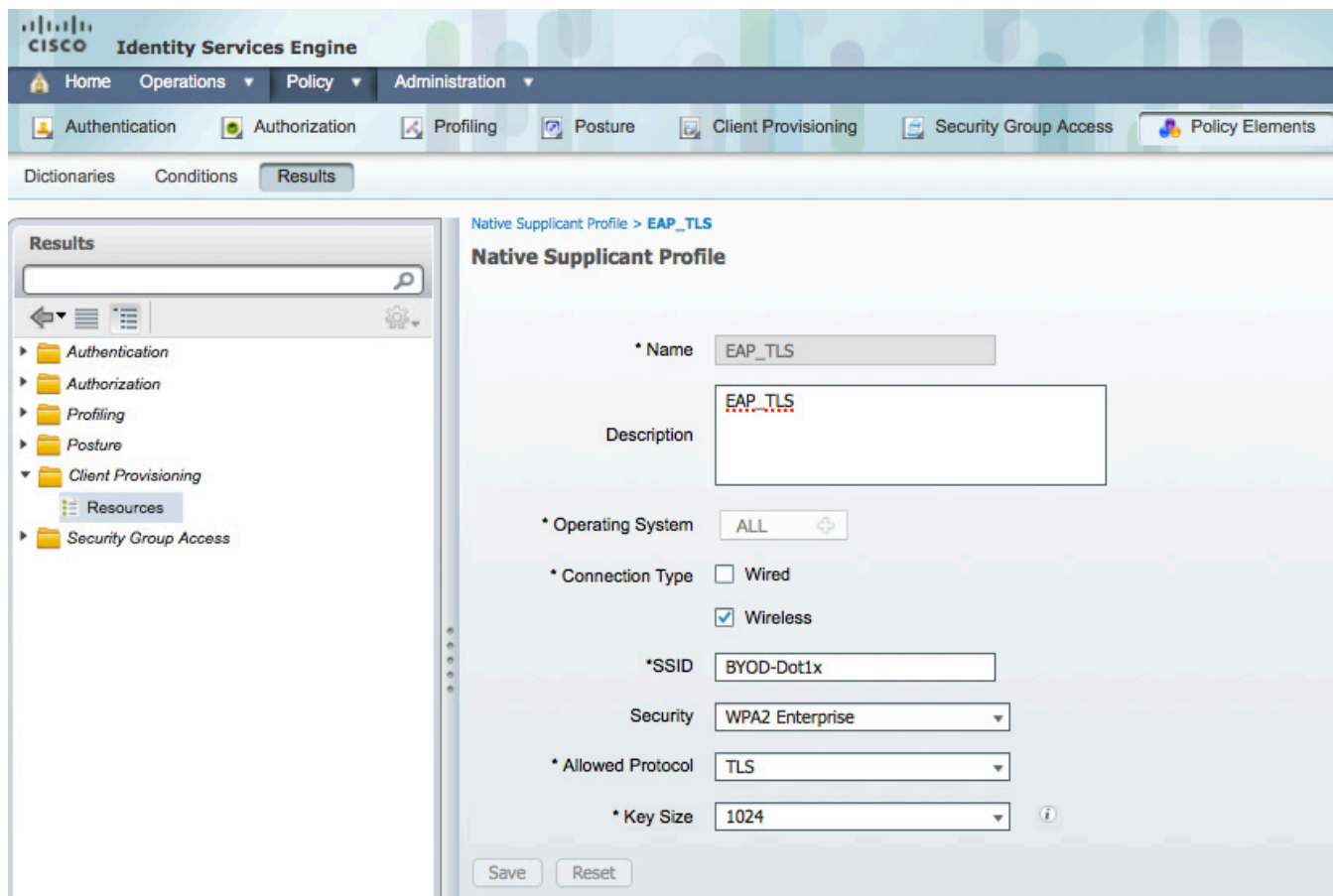


图 10. 本机请求方配置文件

下载适用于 Windows 和 MAC OSx 的请求方向导

- 步骤 6. 转至 Policy → Policy Elements → Results → Client Provisioning → Resources。
- 步骤 7. 在右侧点击 ADD。
- 步骤 8. 选择“Agent resources from Cisco site”。

在本例中我们选择了 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 11. 本机请求方向导 A

步骤 9. 选择最新的请求方向导。

Resources				
<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 3.5.528.2	ComplianceModule	3.5.528.2	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 12. 本机请求方向导 B

为 Apple iOS 创建客户端调配策略

步骤 10. 转至 Policy → Client Provisioning。

步骤 11. 在右侧点击 Actions → Insert new Policy above。

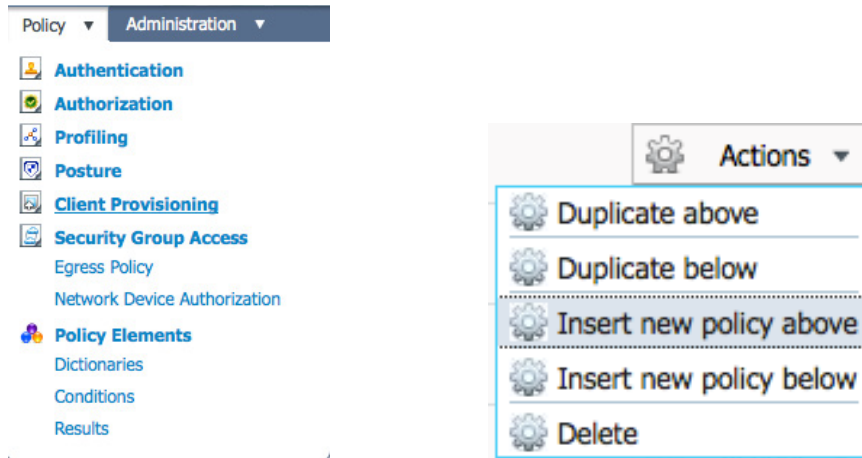


图 13. 客户端调配策略

步骤 12. 创建 Apple iOS CPP 策略。

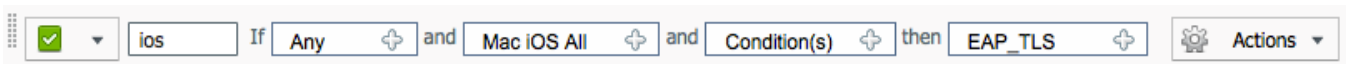


图 14. Apple iOS 客户端调配策略

步骤 13. 创建 Android CPP 策略。

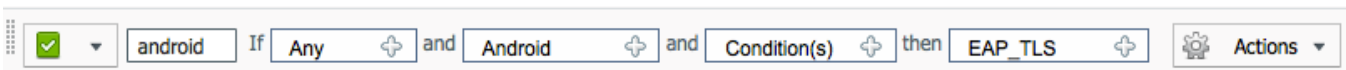


图 15. Android 调配策略

步骤 14. (可选)：创建 MAC OSx CPP 策略。

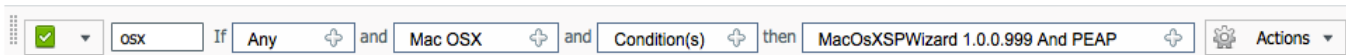


图 16. MacOS-X 调配策略

步骤 15. (可选)：创建 Windows CPP 策略。

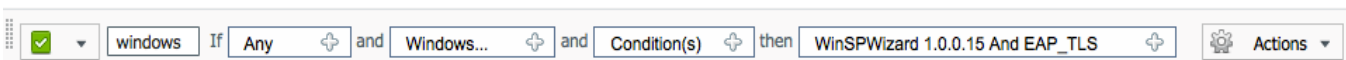


图 17. Windows 客户端调配策略

注： 请注意，Windows 和 OSx 具有额外的请求方调配配置文件，这些配置文件是基于 Java 的向导，用于执行请求方和证书调配，在更新过程中从 cisco.com 下载。

为 BYOD 自行激活准备 WLC

为无线局域网控制器准备访问控制列表

在此过程中，我们将在无线局域网控制器中创建多个 ACL，后面在策略中将会使用这些 ACL 来重定向为 BYOD 请求方和证书调配选择的客户端。

思科身份服务引擎 IP 地址 = 10.35.50.165

公司内部网络 = 192.168.0.0, 172.16.0.0 (需重定向)

步骤 16. 创建一个类似于下文描述的 ACL，将其命名为“NSP-ACL”。

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 18. 用于将客户端重定向至 BYOD 流程的 ACL

图 17 中 NSP-ACL 的解释如下

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（根据公司策略）
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（根据公司策略）
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（根据公司策略）
9. 允许其余所有流量（可选）

步骤 17. 在无线局域网控制器中创建一个名称为“**BLACKLIST-ACL**”的 ACL，后面在策略中会将其用于限制对列入黑名单的设备的访问。

Access Control Lists > Edit < Back Add New Rule

General

Access List Name BLACKLIST-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	Deny	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 19. 黑名单 ACL

图 18 中 **BLACKLIST-ACL** 的解释如下

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. 对于 Blacklist Web Portal 页面，允许从客户端到服务器再到 ISE 的所有“入站”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 18. 在无线局域网控制器中创建一个名称为“**NSP-ACL-Google**”的 ACL，后面在策略中会将其用于调配 Android 设备。

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	<input checked="" type="checkbox"/>
		0.0.0.0 /	255.255.255.255 /							
2	Permit	10.35.50.165 /	0.0.0.0 /	Any	Any	Any	Any	Outbound	114	<input checked="" type="checkbox"/>
		255.255.255.255 /	0.0.0.0 /							
3	Deny	0.0.0.0 /	10.0.0.0 /	Any	Any	Any	Any	Inbound	5	<input checked="" type="checkbox"/>
		0.0.0.0 /	255.0.0.0 /							
4	Deny	0.0.0.0 /	192.168.0.0 /	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
		0.0.0.0 /	255.255.0.0 /							
5	Deny	0.0.0.0 /	172.16.0.0 /	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
		0.0.0.0 /	255.240.0.0 /							
6	Deny	0.0.0.0 /	171.71.181.0 /	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
		0.0.0.0 /	255.255.255.0 /							
7	Permit	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	3449	<input checked="" type="checkbox"/>
		0.0.0.0 /	0.0.0.0 /							

图 20. 用于 Google 访问的 ACL

上图中 **NSP-ACL-Google** 的解释如下

1. 允许流向 ISE 的所有“入站”流量（此步骤可选）
2. 允许来自 ISE 的所有“出站”流量（此步骤可选）
3. 拒绝流向企业内部子网的所有“入站”流量（可以根据公司策略配置）
4. 拒绝流向企业内部子网的所有“入站”流量（可以根据公司策略配置）
5. 拒绝流向企业内部子网的所有“入站”流量（可以根据公司策略配置）
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不同）

注：有关如何只允许 play.google.com 的详细信息，请查阅附录 B。如有必要，可添加额外的线路进行故障排除，例如 ICMP。

配置身份验证策略

复合身份验证策略配置。

查看复合身份验证条件，稍后在策略配置中会用到。我们查看这些内置策略是为了确保其存在而且未被修改，因为在我们的新策略中将会引用它们。

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

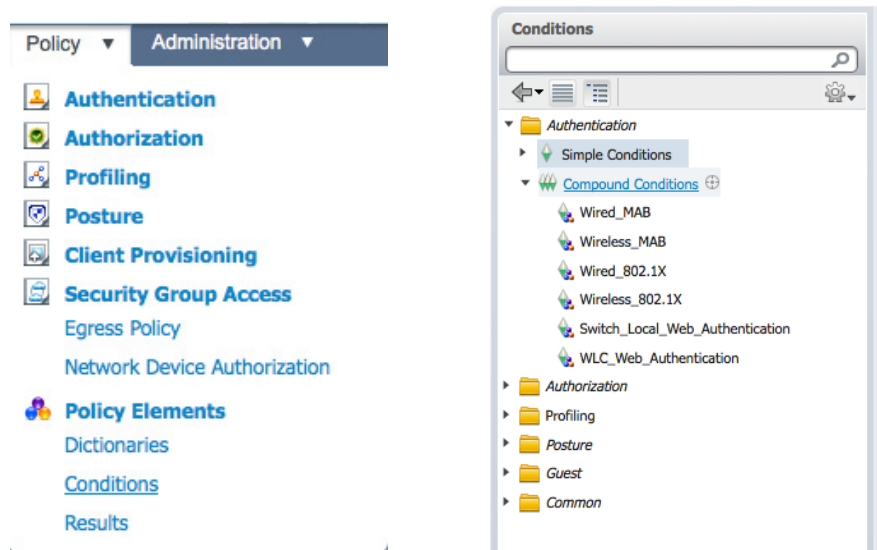


图 21. 复合条件导航

步骤 2. 查看名为“Wireless_MAB”的复合条件。

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

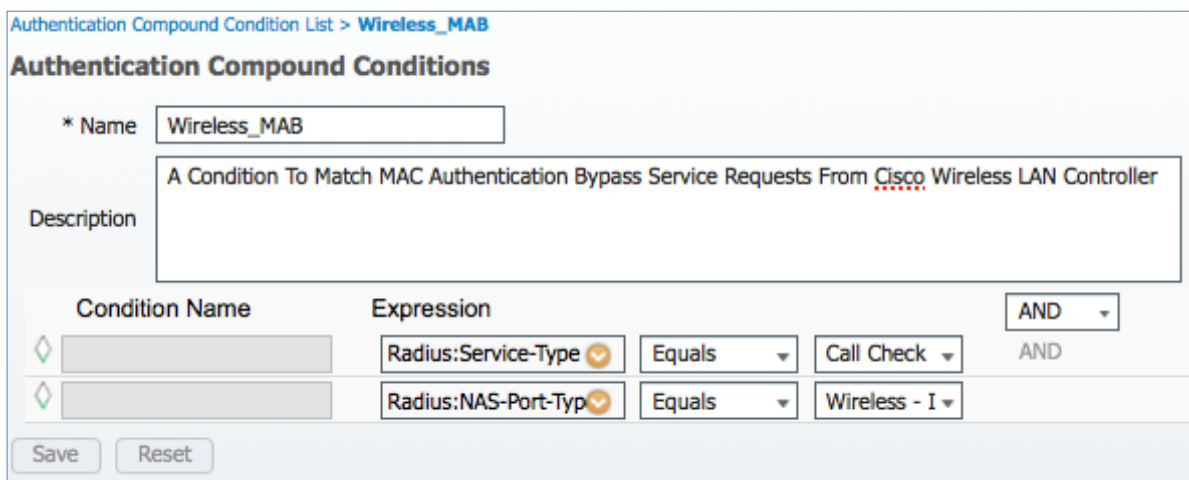


图 22. 无线 MAB

步骤 3. 查看名为“**Wired_MAB**”的复合条件。

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

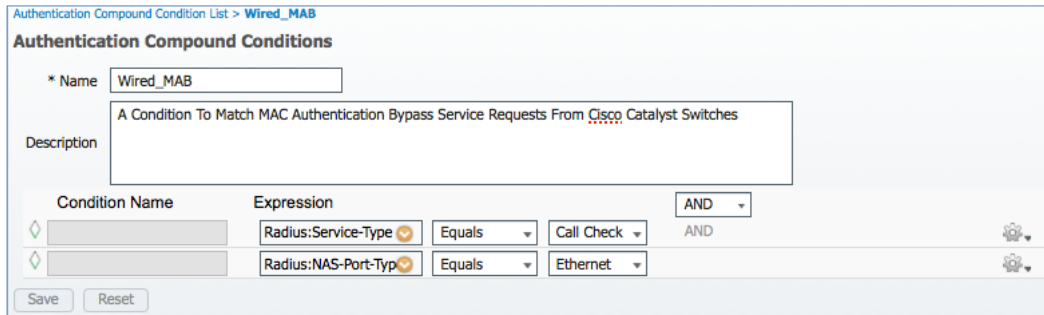


图 23. 有线 MAB

确定默认网络接入结果

此程序说明“**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。

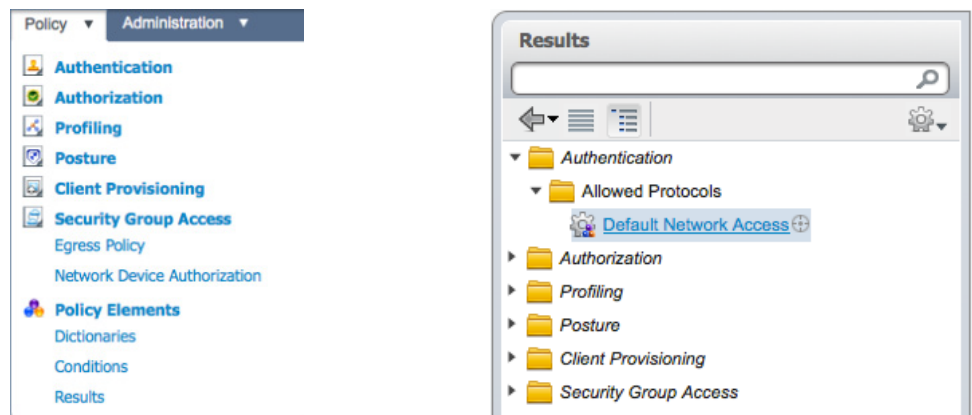


图 24. 默认网络接入导航

注：请根据以下屏幕截图确定协议设置，因为我们会将预置 Default Network Access 对象用于允许的协议。请确保默认对象未更改而且配置与以下截图一致。

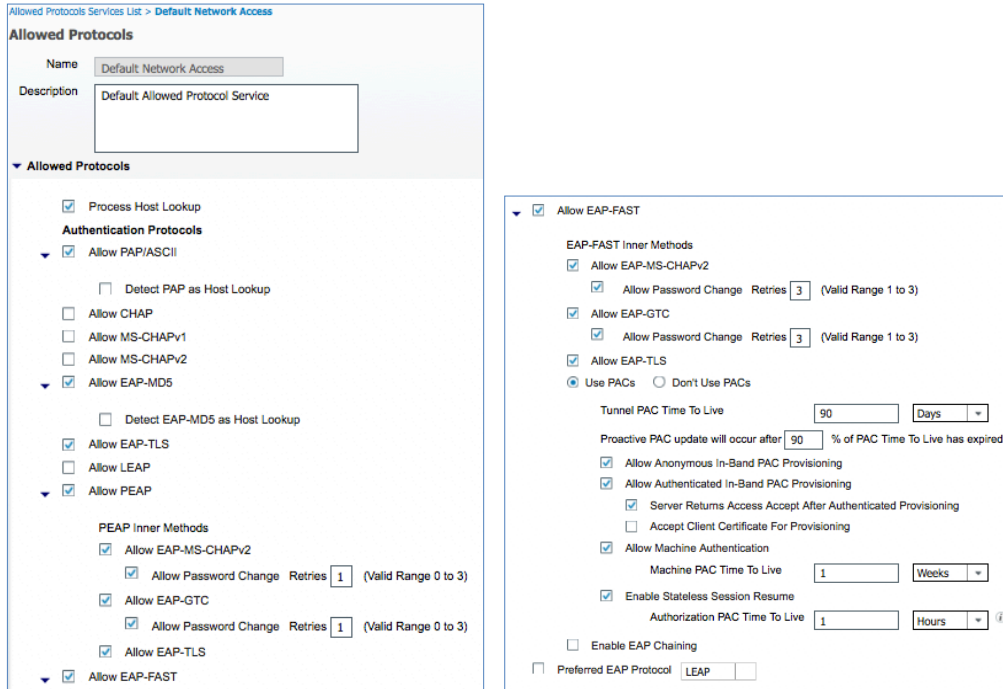


图 25. 默认网络接入策略

步骤 3. 查看身份验证策略配置，以下截图是完整的策略视图，以供参考，后续步骤中将逐一配置各策略。

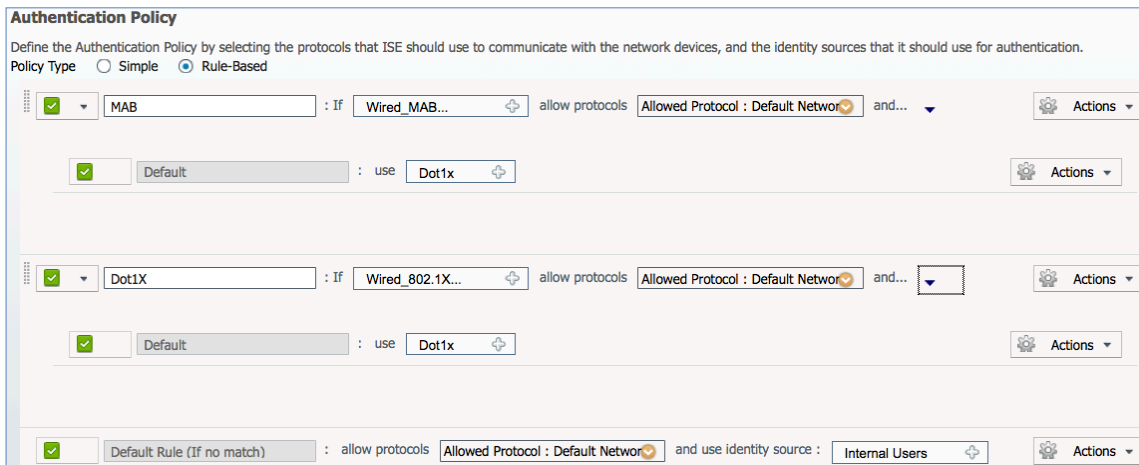


图 26. 身份验证策略配置

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

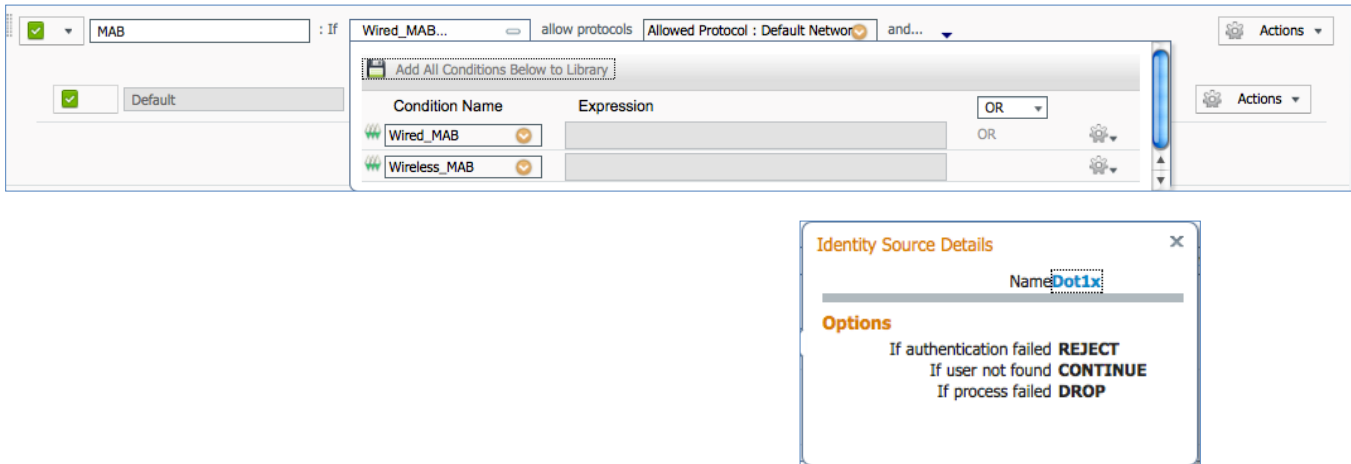


图 27. MAC 身份验证绕行策略

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

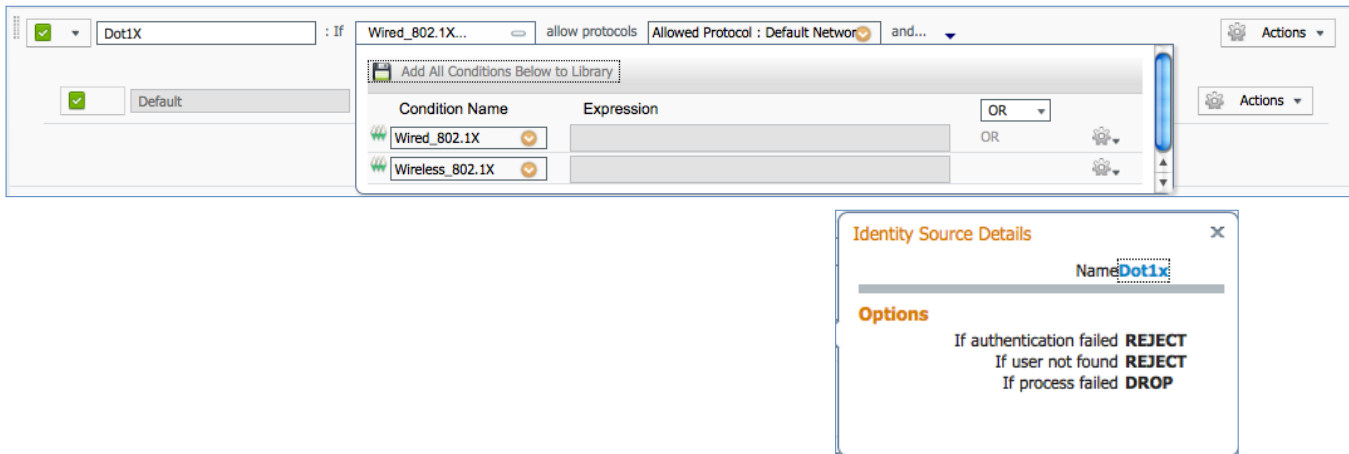


图 28. 802.1X 策略

步骤 6. 默认身份验证策略。

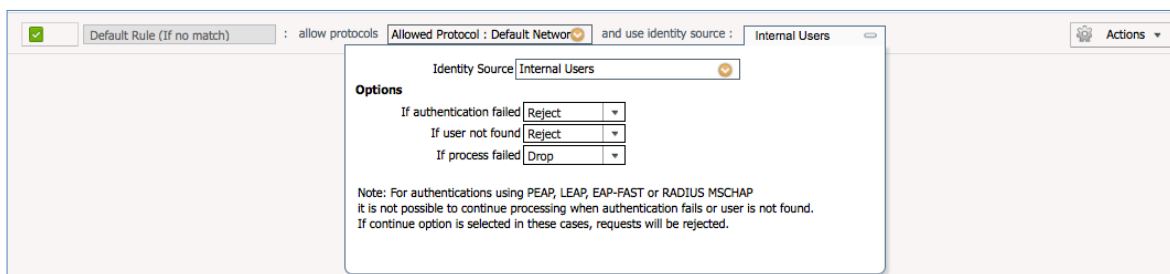


图 29. 默认身份验证策略

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”。

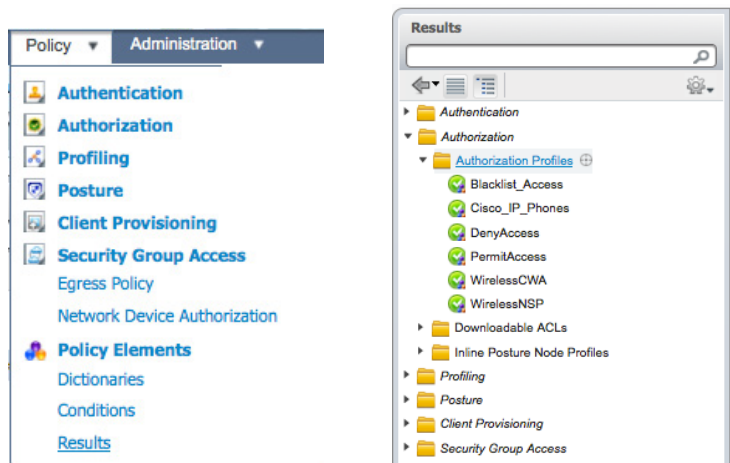


图 30. 授权配置文件导航

- 步骤 4. 添加名为“CWA”的授权配置文件。

集中 Web 身份验证 (CWA) 为将集中设备用做 Web 门户（此例中即思科身份服务引擎）提供了可能性。集中 Web 身份验证客户端与 mac/dot1x 身份验证一起转至第 2 层，然后思科身份服务引擎返回一条向交换机指示已发生 Web 重定向的特殊属性。从全局范围看，如果 RADIUS 服务器不知道客户端站的 MAC 地址（但是也可以使用其他条件），服务器会返回重定向属性而且交换机会向该站授权（通过 MAB），但会设置一个访问列表以将 Web 流量重定向至此门户。

用户登录访客门户之后，可能会通过授权更改 (CoA) 退回交换机端口，从而发生新的第 2 层 MAB 身份验证。然后 ISE 将记住这是一个 WebAuth 用户并向该用户应用第 2 层属性（就像动态 VLAN 分配）。activeX 组件也可以强制客户端 PC 刷新其 IP 地址。

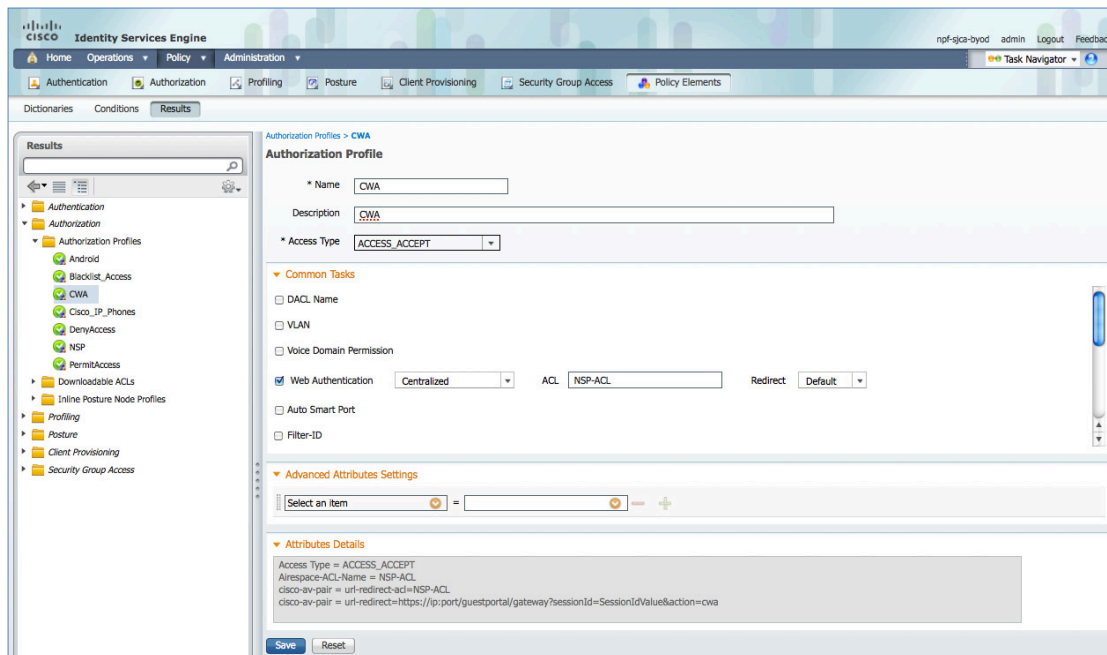


图 31. CWA 授权配置文件

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，以便下载“思科网络设置助理”。

Authorization Profile

* Name

Description

* Access Type

▼ Common Tasks

DACL Name

VLAN

Voice Domain Permission

Web Authentication ACL Redirect

Auto Smart Port

Filter-ID

▼ Advanced Attributes Settings

Select an item = - +

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = NSP-ACL-Google
cisco-av-pair = url-redirect-acl=NSP-ACL-Google
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

图 32. 用于 Android 访问 Google 的 CWA 授权配置文件

查看 Authorization Profiles 下的策略条件

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

Authorization Profiles > Blacklist_Access

Authorization Profile

* Name

Description

* Access Type

▼ Common Tasks

- DAACL Name
- VLAN
- Voice Domain Permission
- Web Authentication
- Auto Smart Port
- Filter-ID

▼ Advanced Attributes Settings

<input type="text" value="Cisco:cisco-av-pair"/>	=	<input type="text" value="url-redirect=https://ip:port/mydev"/>
<input type="text" value="Cisco:cisco-av-pair"/>	=	<input type="text" value="url-redirect-acl=BLACKLIST-ACL"/>

▼ Attributes Details

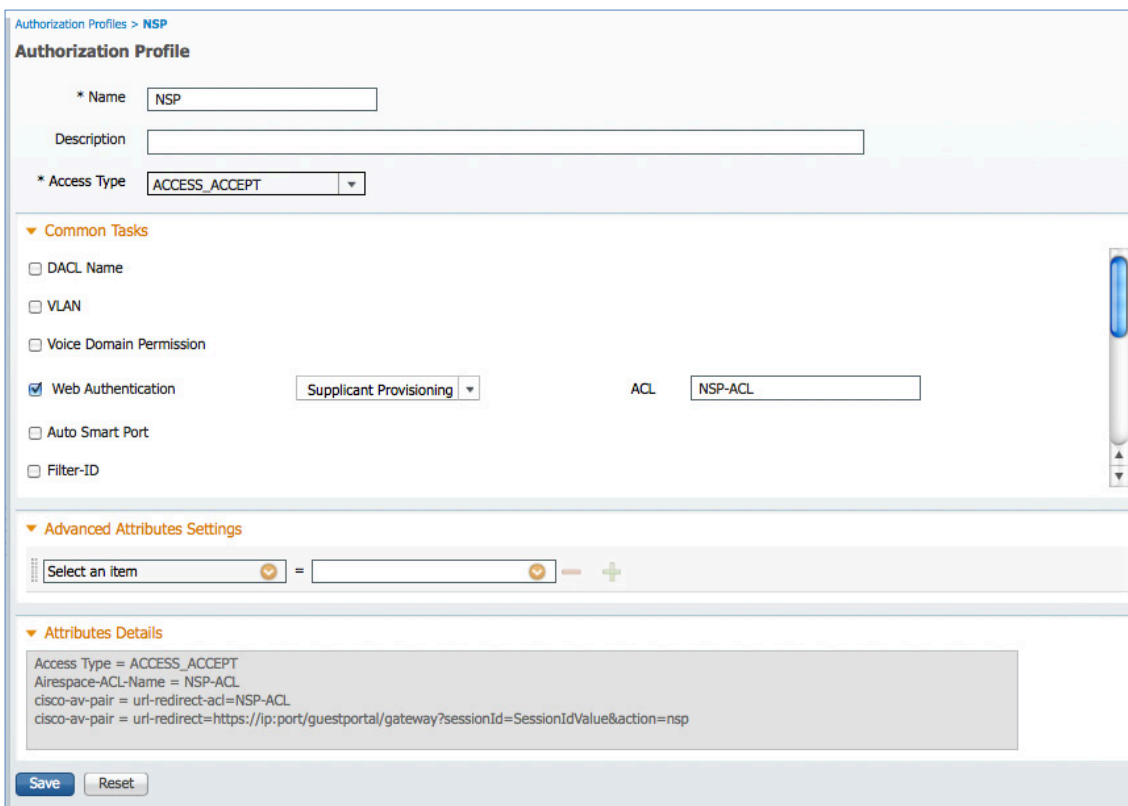
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect=https://ip:port/mydevices/blackhole.jsp
cisco-av-pair = url-redirect-acl=BLACKLIST-ACL

图 33. 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 1. 创建名为“NSP”的授权配置文件。

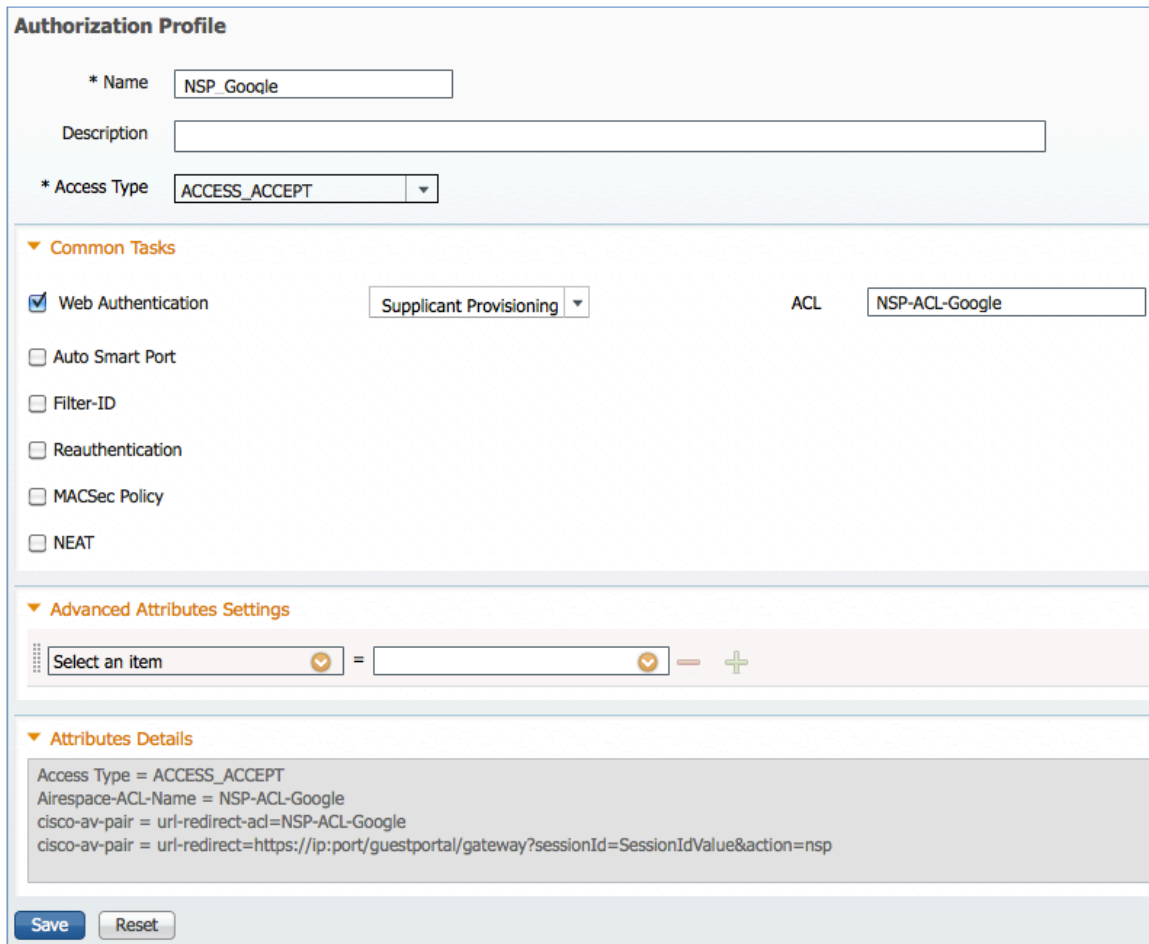


The screenshot shows the configuration page for an Authorization Profile named "NSP". The "Name" field is set to "NSP" and the "Access Type" is set to "ACCESS_ACCEPT". Under "Common Tasks", "Web Authentication" is checked and configured with "Supplicant Provisioning" and "ACL NSP-ACL". The "Attributes Details" section shows the following configuration: Access Type = ACCESS_ACCEPT, Airespace-ACL-Name = NSP-ACL, cisco-av-pair = url-redirect-acl=NSP-ACL, and cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp. There are "Save" and "Reset" buttons at the bottom.

图 34. 本机请求方调配授权配置文件

注：也请点击 Airespace ACL Name 。

步骤 2. 创建名为“NSP_Google”的授权配置文件。



Authorization Profile

* Name

Description

* Access Type

▼ **Common Tasks**

Web Authentication ACL

Auto Smart Port

Filter-ID

Reauthentication

MACSec Policy

NEAT

▼ **Advanced Attributes Settings**

Select an item = - +

▼ **Attributes Details**

Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = NSP-ACL-Google
cisco-av-pair = url-redirect-ac=NSP-ACL-Google
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp

图 35. NSP_Google 授权配置文件

注：也请点击 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” 。

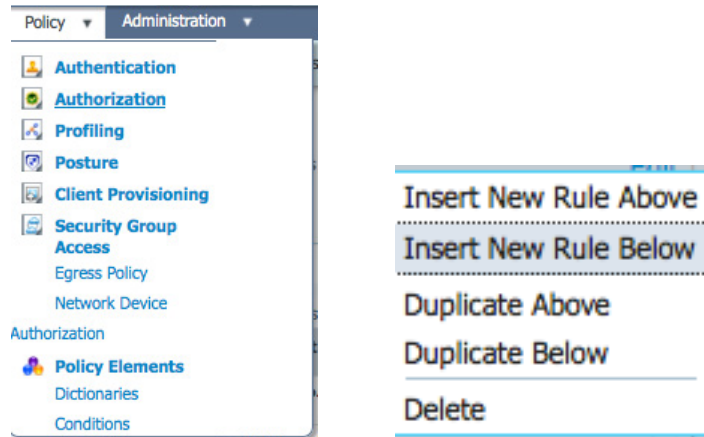


图 36. 插入新规则

步骤 3. 请添加以下授权策略。

Black List Default = 这是将设备列入黑名单的默认授权规则，可以根据公司策略自定义，其中设备可以重定向至限制网页，甚至不允许其在列入黑名单之后出现在网络上。

Profiled Cisco IP Phones = 思科 IP 电话的默认授权规则。

Corp_Owned = 当要绕过 BYOD 请求方和证书调配流程的设备被划分为企业资产“Corp_Assets”并且利用协议 MSCHAPV2 通过使用 802.1x 的企业无线 SSID 接入时，向这些设备添加此授权规则。

Android_SingleSSID = 对于 Android 设备，要添加此授权规则，因为这些设备要求下载思科网络设置助理才能完成调配。此规则特定于单 SSID 设置。一旦 Android 设备在设备注册期间命中“Register”按钮，ISE 将向控制器发送 Re-Auth COA。Android 重新连接网络时，会话 ID 保留不变，因为 ISE 发出的 COA 为 Ra-Auth 而不是终止会话。然后 ISE 会应用 NSP_Google 权限，继续执行调配流程。

Android_DualSSID = 对于 Android 设备，要添加此授权规则，因为这些设备要求下载思科网络设置助理才能完成调配。此规则特定于双 SSID 设置。一旦 Android 设备在设备注册期间命中“Register”按钮，ISE 将向控制器发送 Re-Auth COA。Android 重新连接网络时，会话 ID 保留不变，因为 ISE 发出的 COA 为 Ra-Auth 而不是终止会话。然后 ISE 会应用 NSP_Google 权限，继续执行调配流程。

CWA = 针对集中 Web 身份验证添加的授权规则。

NSP = 对于在利用 MSCHAPV2 协议通过使用 802.1x 的企业无线 SSID 接入时经过 BYOD 请求方和证书调配流程的设备，要添加此授权规则。

PERMIT = 设备如果已通过使用 EAP-TLS 进行身份验证的证书完成 BYOD 请求方和证书调配，并且通过企业无线 SSID 接入，则归属于此授权策略。

Default = 默认授权策略，设置为 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 37. 授权策略

简单证书注册协议 (SCEP) 设置

在此程序中，我们将配置用于客户端上证书调配的 SCEP 配置文件。此注册过程要求证书颁发机构 (CA) 使用简单证书注册协议 (SCEP) 颁发证书。ISE 会充当注册机构 (RA) 并与 CA 通信以在客户端上调配证书。

添加 SCEP CA 配置文件

步骤 1. 点击 Administration → Certificates → SCEP CA Profiles。

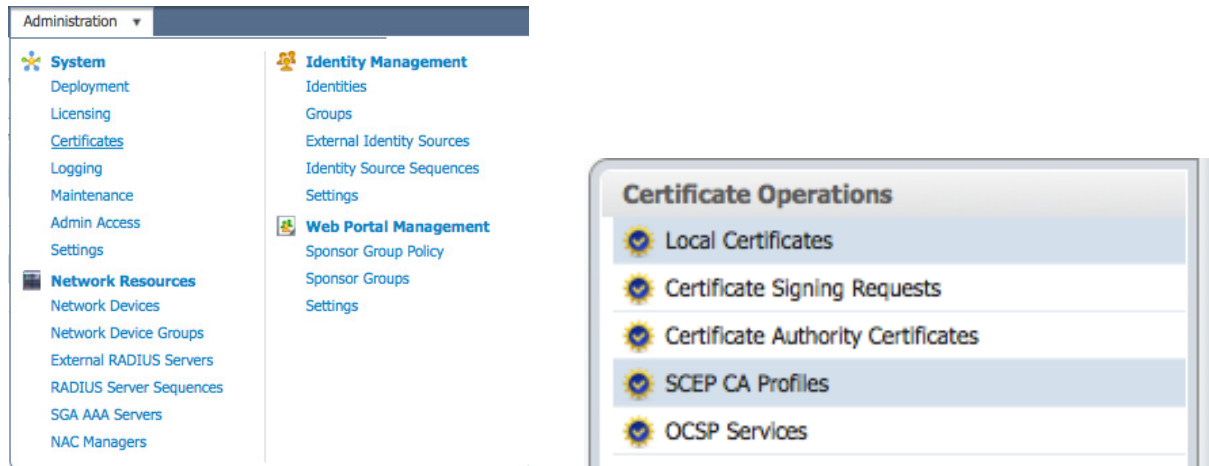


图 38. 导航至 SCEP CA Profiles

步骤 2. 点击 Add。

步骤 3. 添加 SCEP CA 配置文件。

CA 服务器 IP = 172.21.77.24。

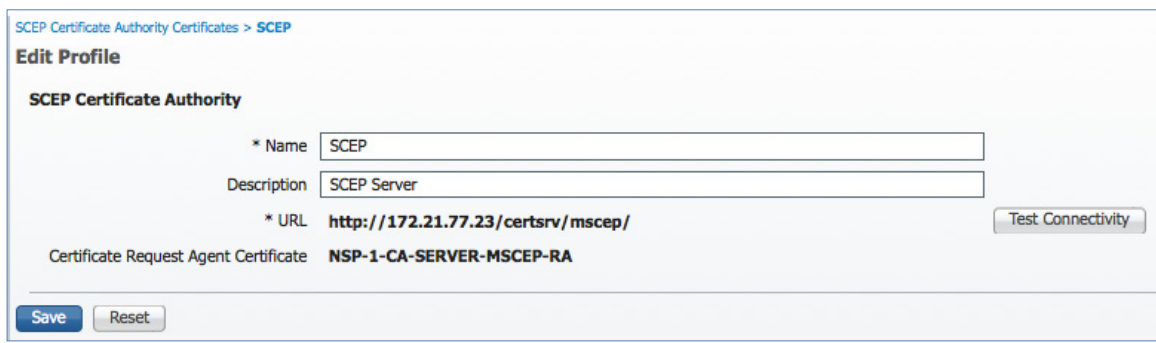


图 39. SCEP CA 配置文件



您已完成！

有关详细信息，请参阅 TrustSec “自行激活” 操作指南。

附录 A：配置 SCEP 服务器

本节介绍将 Microsoft 2008 R2 Enterprise SP2 配置为 SCEP 服务器的详细过程，以下是设置 SCEP 需要完成的任务。

设置 SCEP 服务器

针对 SCEP 服务器的 Microsoft 2008 R2 Enterprise SP2 设置

- 步骤 1. 安装 Windows Server 2008 R2 Enterprise 服务器。
- 步骤 2. 安装完成后，请运行 Microsoft 更新，获取所有必要的更新。
- 步骤 3. 激活 Windows 许可证。
- 步骤 4. 在命令提示符窗口运行 dcpromo。这会将 Active Directory Domain Services 安装至服务器。
- 步骤 5. 检查 Active Directory Domain Services 的安装。
 - a. 选择“advanced”模式复选框
 - b. 在森林中创建一个新域
 - c. 为森林 root 域插入名称
 - d. 安装 DNS 服务器
 - e. 等待 Active Domain Services 完成安装
 - f. 服务器将重新启动
- 步骤 6. 向 IIS_IUSRS 组添加管理员或 SCEP_User。

安装角色：Active Directory 证书服务

- 步骤 1. AD CS：点击 Next。
 - a. 角色服务：
 - i. 证书颁发机构
 - ii. 证书颁发机构 Web 注册
 - b. Setup Type：选择“Enterprise”
 - c. CA Type：Root CA
 - d. Private Key：创建新私钥
 - i. Cryptography：默认值，但请选择 SHA256 哈希算法
 - ii. CA Name：保留默认值
 - iii. Validity Period：保留默认值
 - e. Certificate Database：保留默认值
- 步骤 2. Web Server (IIS)：点击 Next。
 - a. Role Services：保留默认值，点击 Next
- 步骤 3. Confirmation：点击 Install。

添加角色服务

- 步骤 1. 导航至：Server Manager → Roles → Active Directory Certificate Services。
- 步骤 2. 选择“Network Device Enrollment Service”。
- 步骤 3. 选择“Certificate Enrollment Web Service”。

用户帐户

指定用户帐户（选择用户）。这可能是管理员帐户或 SCEP 服务帐户（即添加至 IIS_USERS 组的那个帐户）

- 步骤 4. RA Information - 保留默认值。
- 步骤 5. Cryptography - 保留默认值。
- 步骤 6. CA for CES - 保留默认值。
- 步骤 7. Authentication Type - 保留默认值。
- 步骤 8. Service Account - 保留默认值并选择管理员帐户。
- 步骤 9. Server Authentication Certificate。
- 步骤 10. 为 SSL 加密选择现有证书 - 请选择以“客户端身份验证”作为指定用途的证书。
- 步骤 11. Web Server (IIS) - 点击 **Next**。
- 步骤 12. Role Servers - 保留默认值。
- 步骤 13. Confirmation: 点击 **Install**。

修改注册表

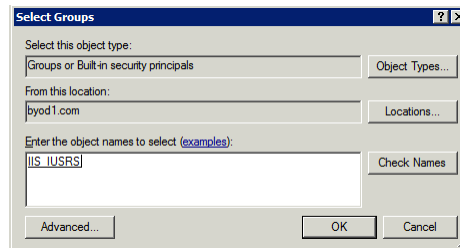
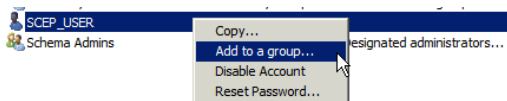
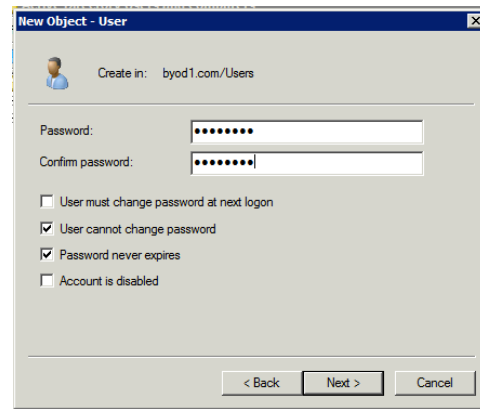
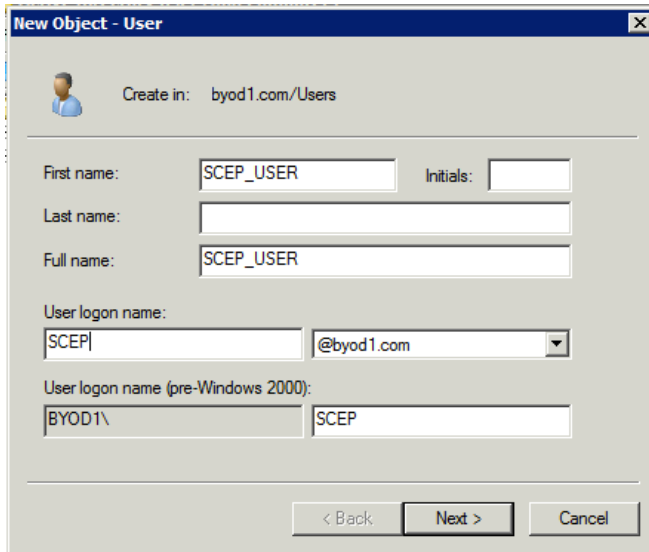
- 步骤 1. 从“Start”菜单键入 regedit。
- 步骤 2. 在注册表编辑器中转至：HKEY_LOCAL_MACHINE → Software → Microsoft → Cryptography → MSCEP。
- 步骤 3. 单击标记为 Enforce Password 的密钥。
- 步骤 4. 将 EnforcePassword 的值从 1 改为 0。
- 步骤 5. 重新启动服务器。

配置 SCEP 注册

创建 SCEP 服务帐户

安装 CA 服务器和服务之后，请将服务器配置为执行 SCEP 注册。

步骤 1. 创建新帐户。



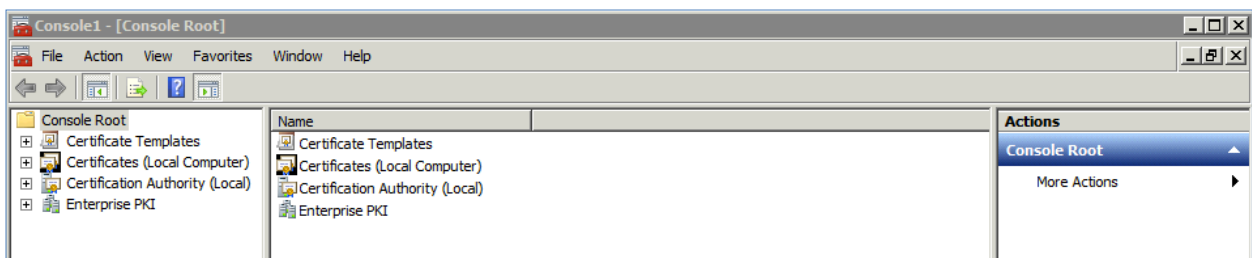
参考：<http://technet.microsoft.com/en-us/library/ff955646%28v=ws.10%29.aspx>

创建并保存与证书一起使用的 MMC

步骤 1. 导航至：Start → Run → mmc。

步骤 2. 为 Certificate Templates、Certificates (Local Computer)、Certification Authority (Local) 和 Enterprise PKI 添加证书管理单元。

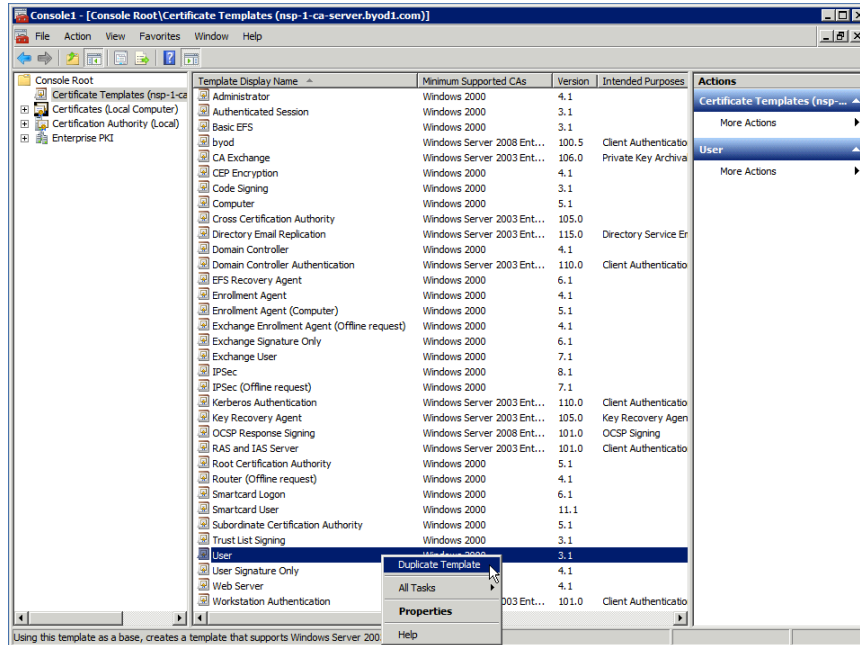
步骤 3. 完成后，点击“OK”。（快照如下所示）。



步骤 4. 保存 mmc 控制台，便于以后轻松访问。

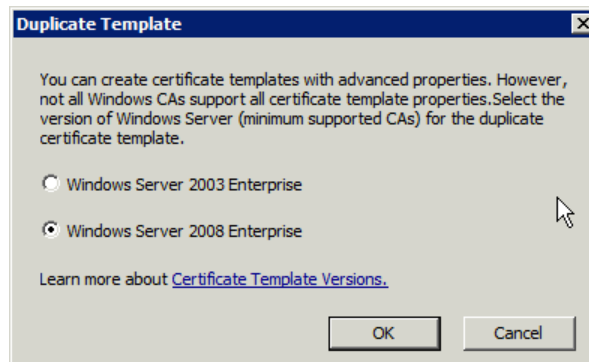
创建新的证书模板

步骤 1. 选择 Certificate Templates 并复制 “User” 模板。



步骤 2. 选择 “Windows Server 2008 Enterprise”（在本文档示例中，还可以使用 Windows Server 2003 Enterprise）。

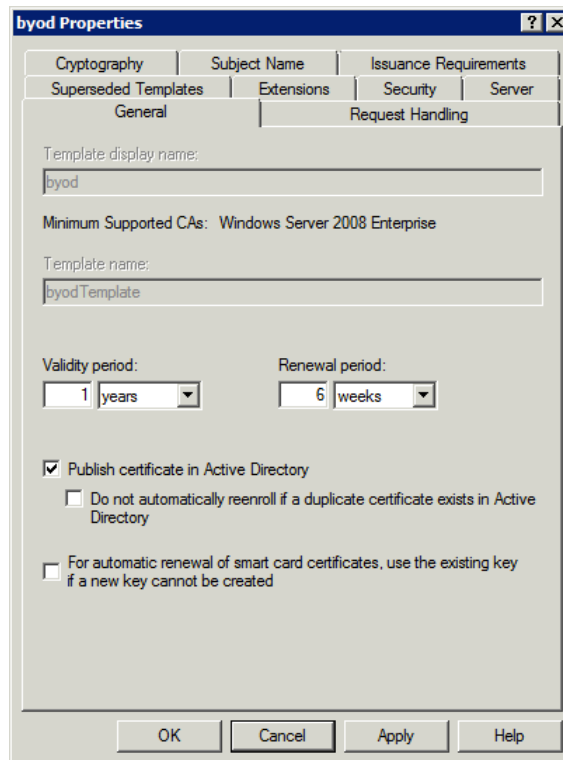
步骤 3. 点击 OK。



步骤 4. 为模板命名（在本示例中将其命名为 “byod”）。

General 选项卡

步骤 1. 在 Active Directory 中发布证书，Active Directory 会将其与所有域控制器同步。



byod Properties [?] [X]

Cryptography	Subject Name	Issuance Requirements	
Superseded Templates	Extensions	Security	Server
General	Request Handling		

Template display name:
byod

Minimum Supported CAs: Windows Server 2008 Enterprise

Template name:
byodTemplate

Validity period: 1 years
Renewal period: 6 weeks

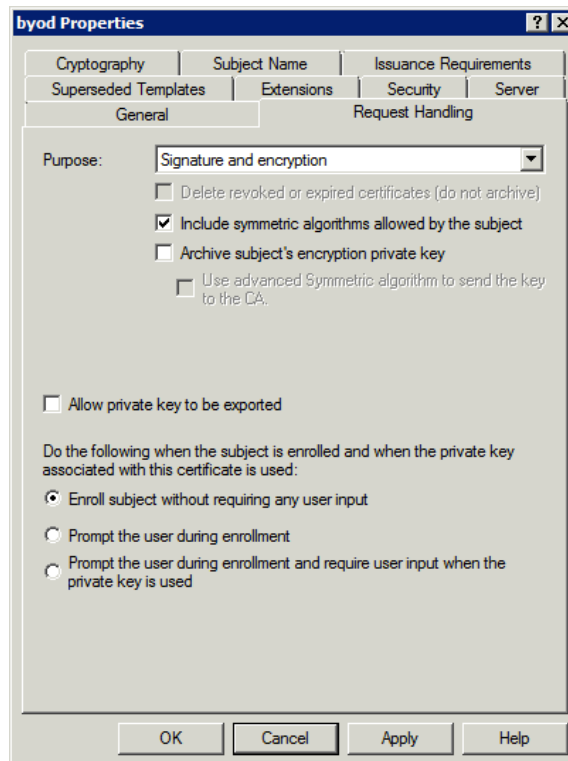
Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory
 For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

OK Cancel Apply Help

Request Handling 选项卡

此选项卡指定将用于签名和加密的证书。

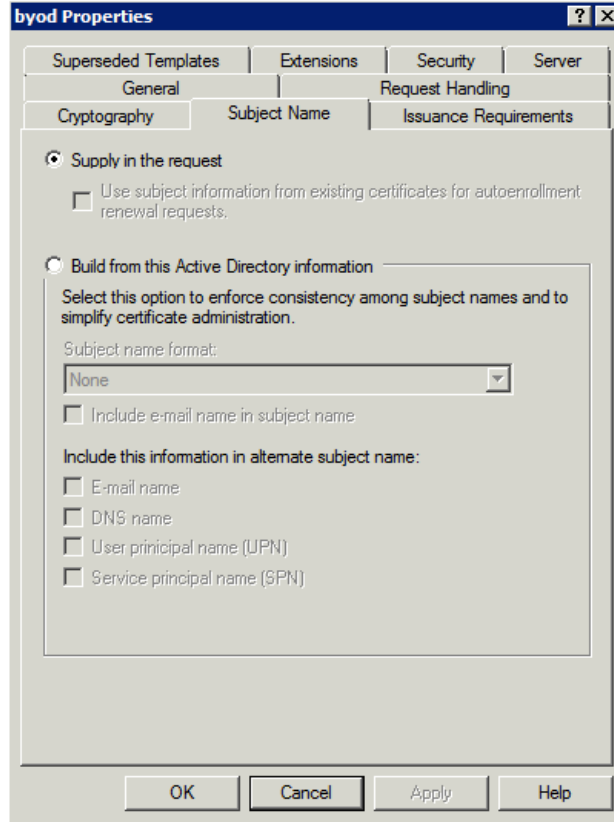
- 步骤 1.** 请取消选中 “**allow private key to be exported**”，视需要将其标记为 “on-exportable”。
- 步骤 2.** 系统通过将自动化流程的 BYOD 调配流程请求证书，因此请确保选择 “**enroll subject without requiring any user input**”。



Subject Name 选项卡

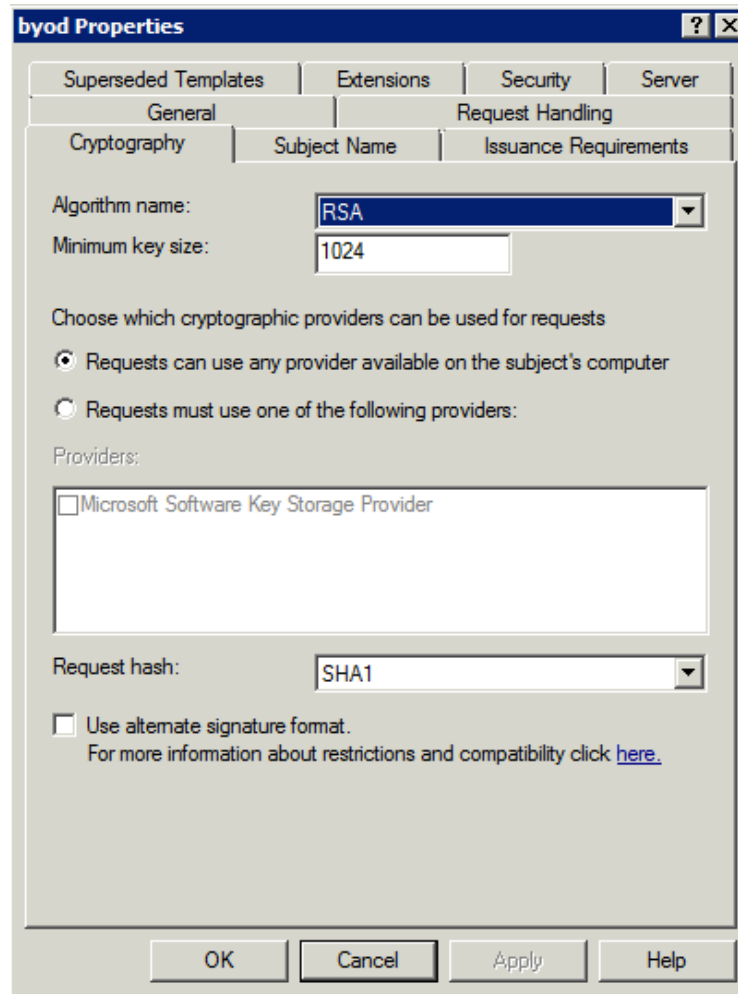
步骤 1. 选择“Supply in Request”。

因为证书不是 Active Directory 成员而是通过 SCEP 创建的，所以这是必选项。



Cryptography 选项卡

步骤 1. 选择 “Requests can use any provider available on the subject’s computer”。



The screenshot shows the 'byod Properties' dialog box with the 'Cryptography' tab selected. The 'Algorithm name' is set to 'RSA' and the 'Minimum key size' is '1024'. The 'Request hash' is set to 'SHA1'. The option 'Requests can use any provider available on the subject's computer' is selected. The 'Providers' list is empty. The 'Use alternate signature format' checkbox is unchecked. The dialog box has 'OK', 'Cancel', 'Apply', and 'Help' buttons at the bottom.

Superseded Templates	Extensions	Security	Server
General	Request Handling		
Cryptography	Subject Name	Issuance Requirements	

Algorithm name:

Minimum key size:

Choose which cryptographic providers can be used for requests

Requests can use any provider available on the subject's computer

Requests must use one of the following providers:

Providers:

Microsoft Software Key Storage Provider

Request hash:

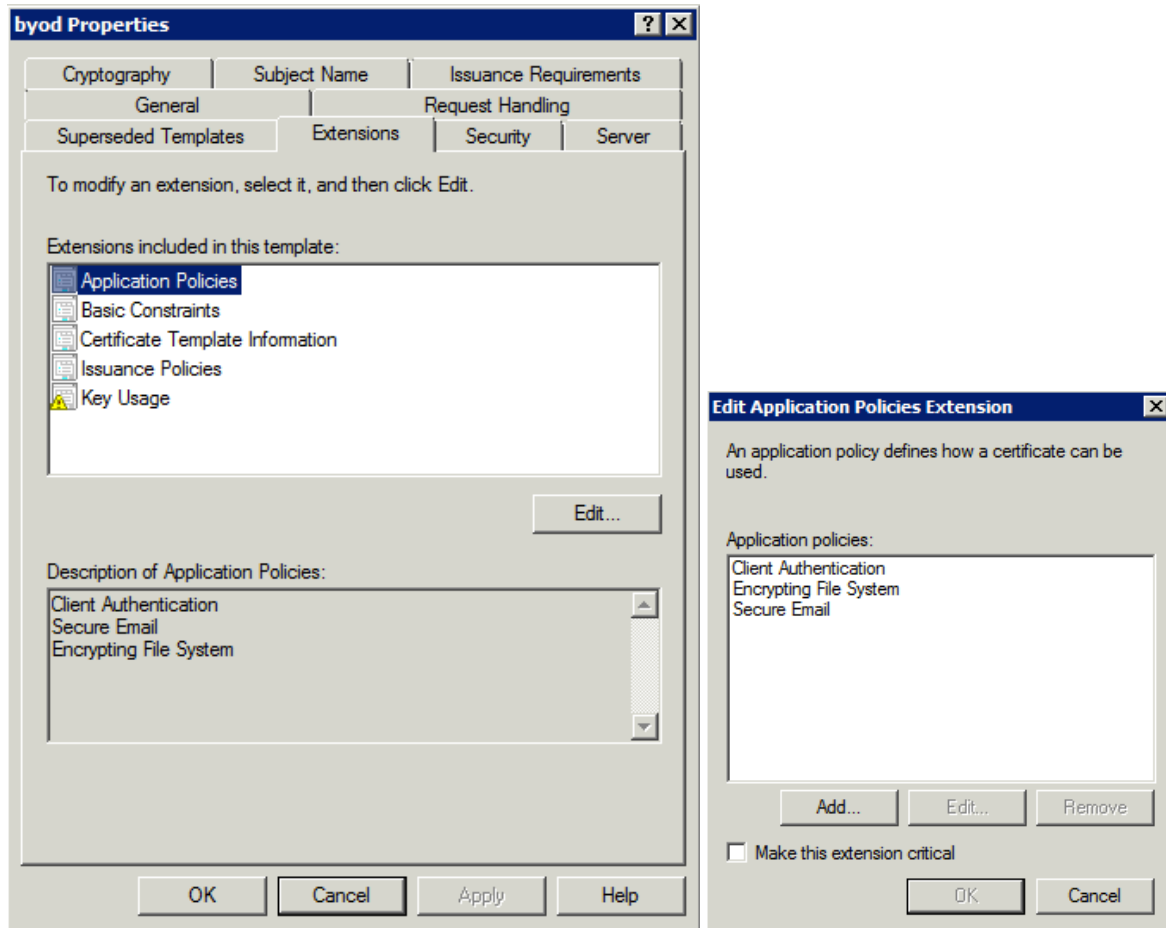
Use alternate signature format.
For more information about restrictions and compatibility click [here](#).

OK Cancel Apply Help

Extensions 选项卡

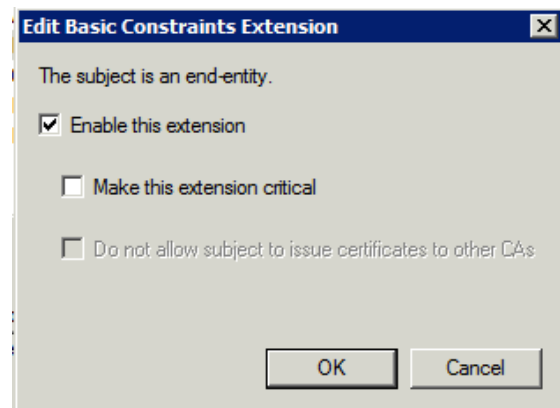
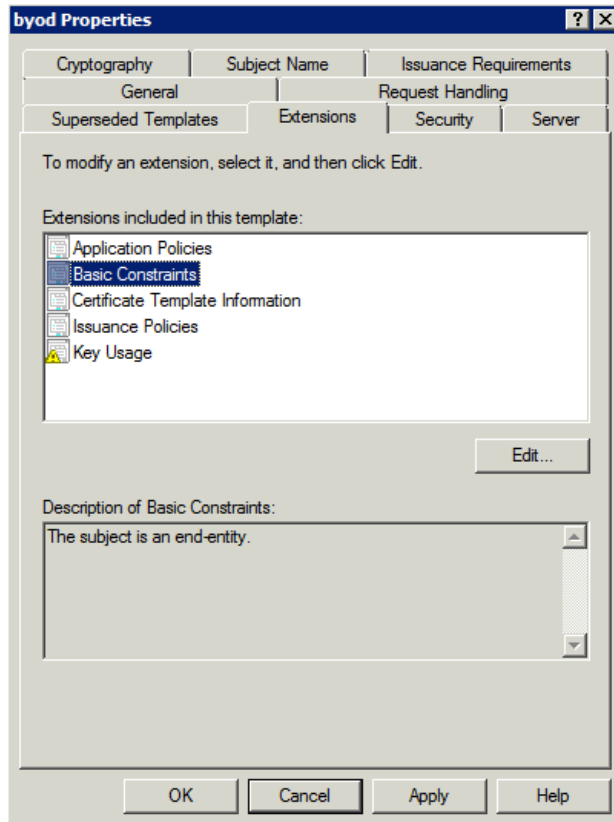
步骤 1. Applications Policies:

如果 Application Policies 的说明与快照所示内容不一致，可以点击 Application Policies 的“Edit”和“Add”选项。



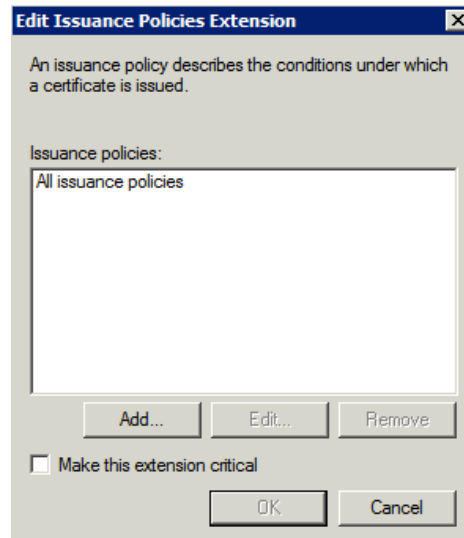
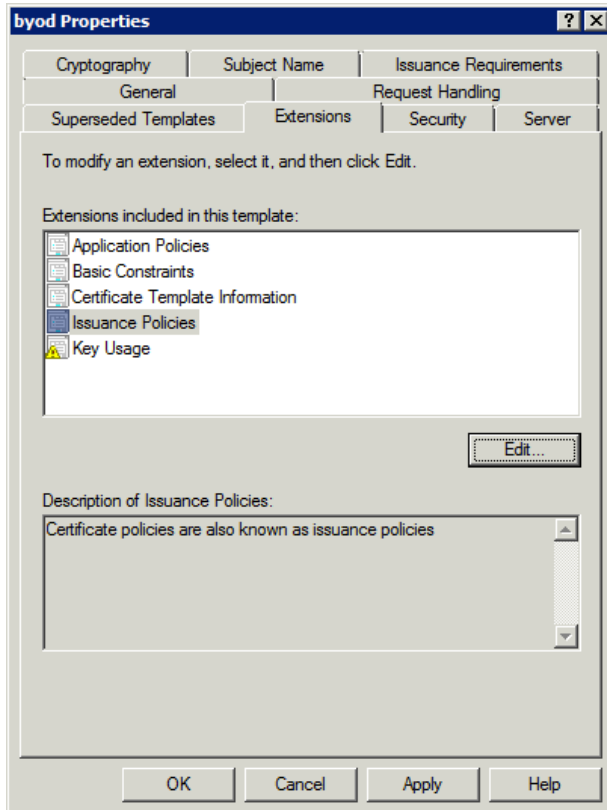
步骤 2. Basic Constraints

此选项将证书设置为属于终端而不属于后续签名者。



步骤 3. Issuance Policies

必须配置 Issuance Policies，允许 CA 实际颁发证书。请选择 “All issuance policies”。

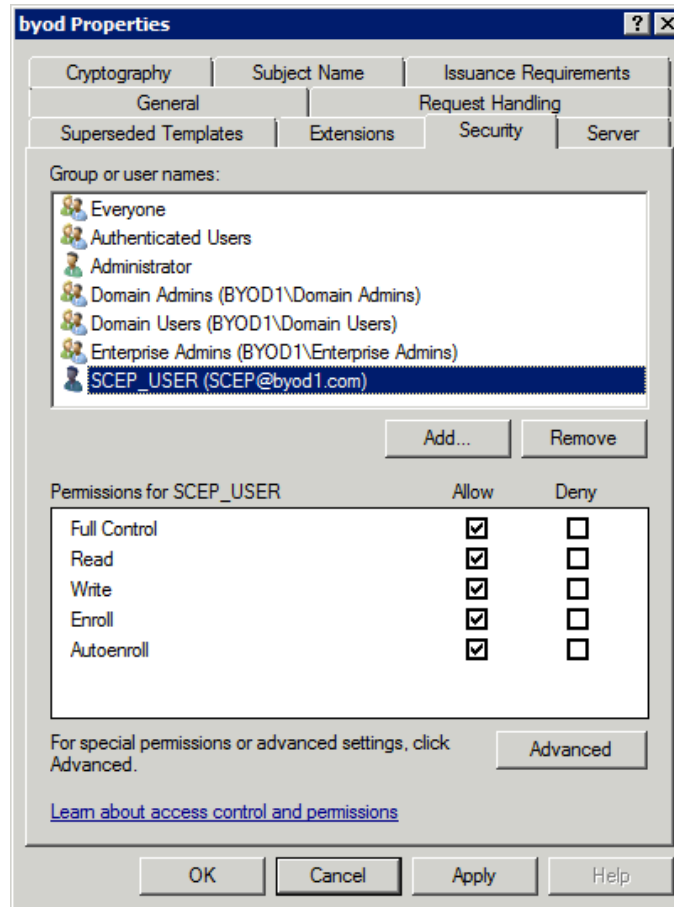


Security 选项卡

在此部分我们将添加“**Service Account User**”，使其具有对证书模板的 Full Control 权限。之前运行 SCEP 服务的步骤中已创建此帐户。

步骤 1. 点击 Add。

步骤 2. SCEP_USER。



分配新的颁发模板

此时，我们已经完成复制模板流程，接下来我们必须将其选择为要颁发的模板。

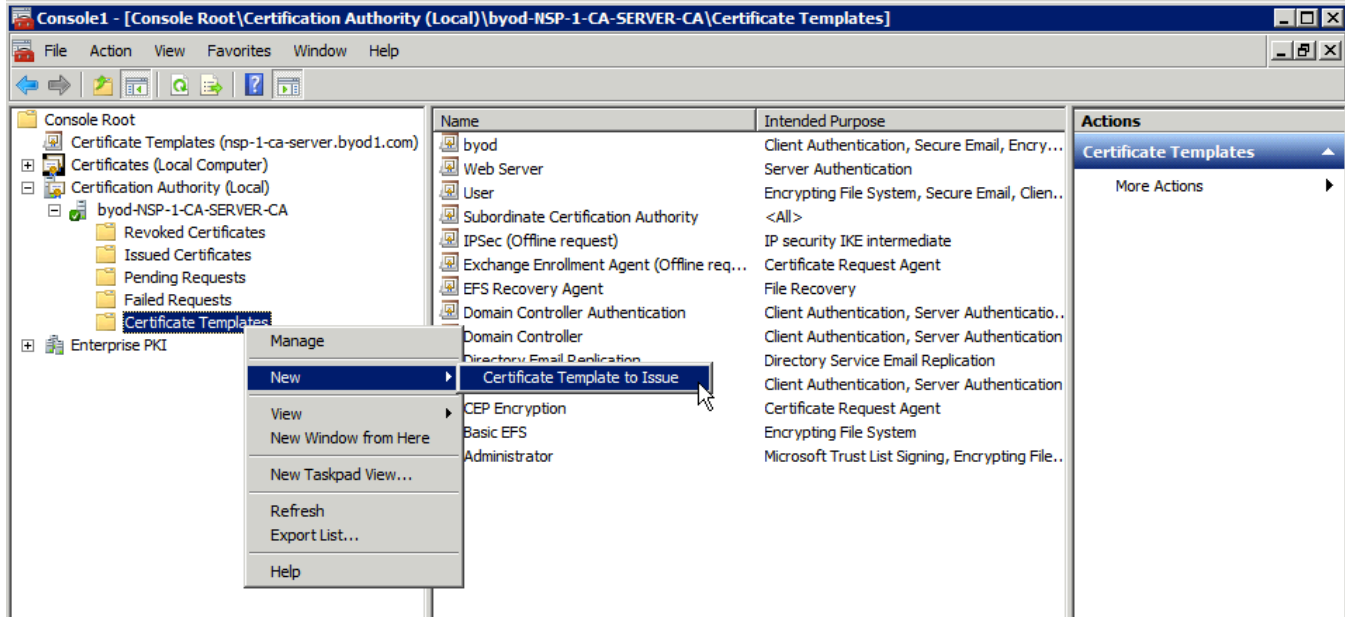
分配新的颁发模板

步骤 1. 导航至：Server Manager → Roles → AD Certificate Authority → <your CA → Certificate Templates。

步骤 2. 右键点击。

步骤 3. 导航至：New → Certificate Template to Issue。

步骤 4. 选择新的证书模板。



步骤 5. 选择在上一步中创建的模板。

完成此步骤之后，您应该可以看见在右侧显示了此模板。

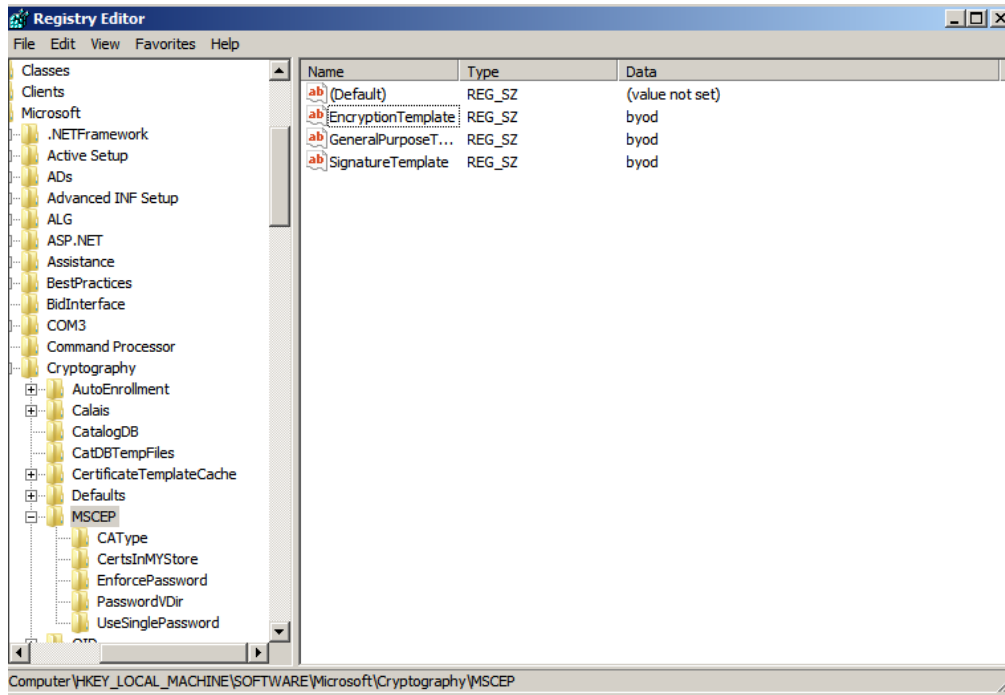
修改颁发的默认证书

SCEP 颁发的默认证书模板为 IPSEC 模板。必须将此改为使用新的用户模板：

步骤 1. 运行 regedit。

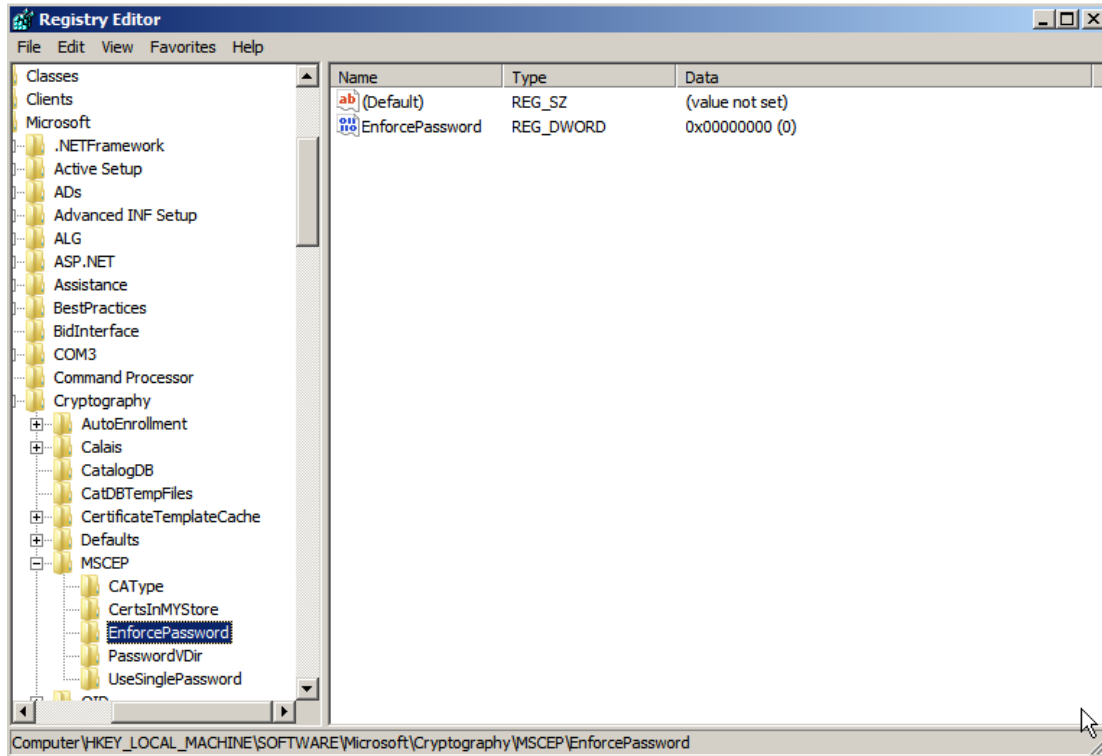
步骤 2. 导航至：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP。

步骤 3. 将 **EncryptionTemplate**、**GeneralPurposeTemplate** 和 **SignatureTemplate** 改为以上所创建的模板的名称 确定名称拼写与创建时的拼写一致。

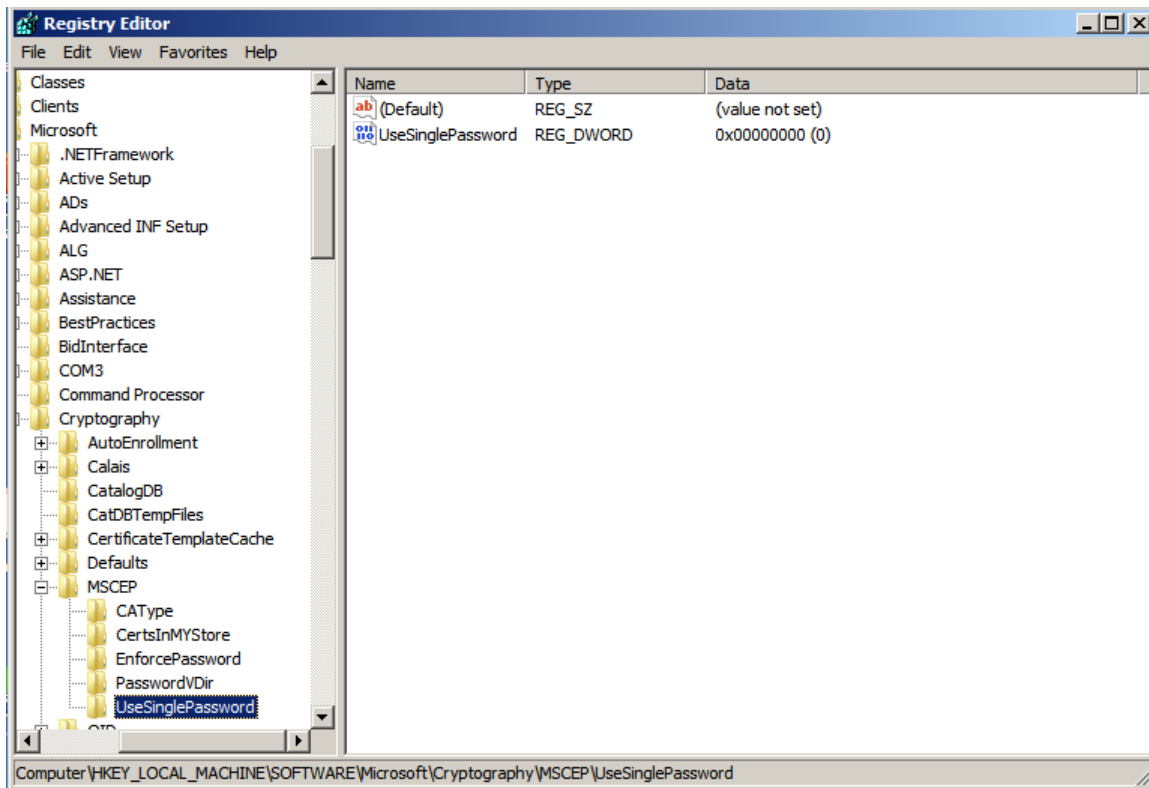


将 EnforcePassword 设置为零并禁用 “UseSinglePassword” 设置：

- 步骤 1. 运行 regedit。
- 步骤 2. 导航至：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword。
- 步骤 3. 将该值改为 0，UseSinglePassword 即被设置为零“0”。
- 步骤 4. 导航至：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\ EnforcePassword。
- 步骤 5. 将该值改为 0，EnforcePassword 即被设置为零“0”。



UseSinglePassword:



步骤 6. 如果您尚未保存上面创建的 mmc 控制台，请保存。

步骤 7. 重新启动整个服务器。



您已完成！

附录 B: Android 和 Play.Google.Com

为什么 Android 与众不同

Android 设备需要以不同于 iOS Devices 和/或 Windows 的方式对待。其部分原因是，由于要求使用请求方调配应用来为 Android 设备配置请求方和证书，所以没有两台 Android 设备是完全相同的。

默认情况下，Android 设备不会接受来自任何来源的应用，必须是来自受信任应用商店的应用，例如“play.google.com”。虽然可以将思科 ISE 配置为托管请求方调配向导 (SPW) 应用，但是最终用户的 Android 设备不会配置为像应用商店一样信任思科 ISE。因此，与 Windows、MAC 和 iOS 不同，Android 设备必须能够访问互联网，才能参与 BYOD 和本机请求方调配。

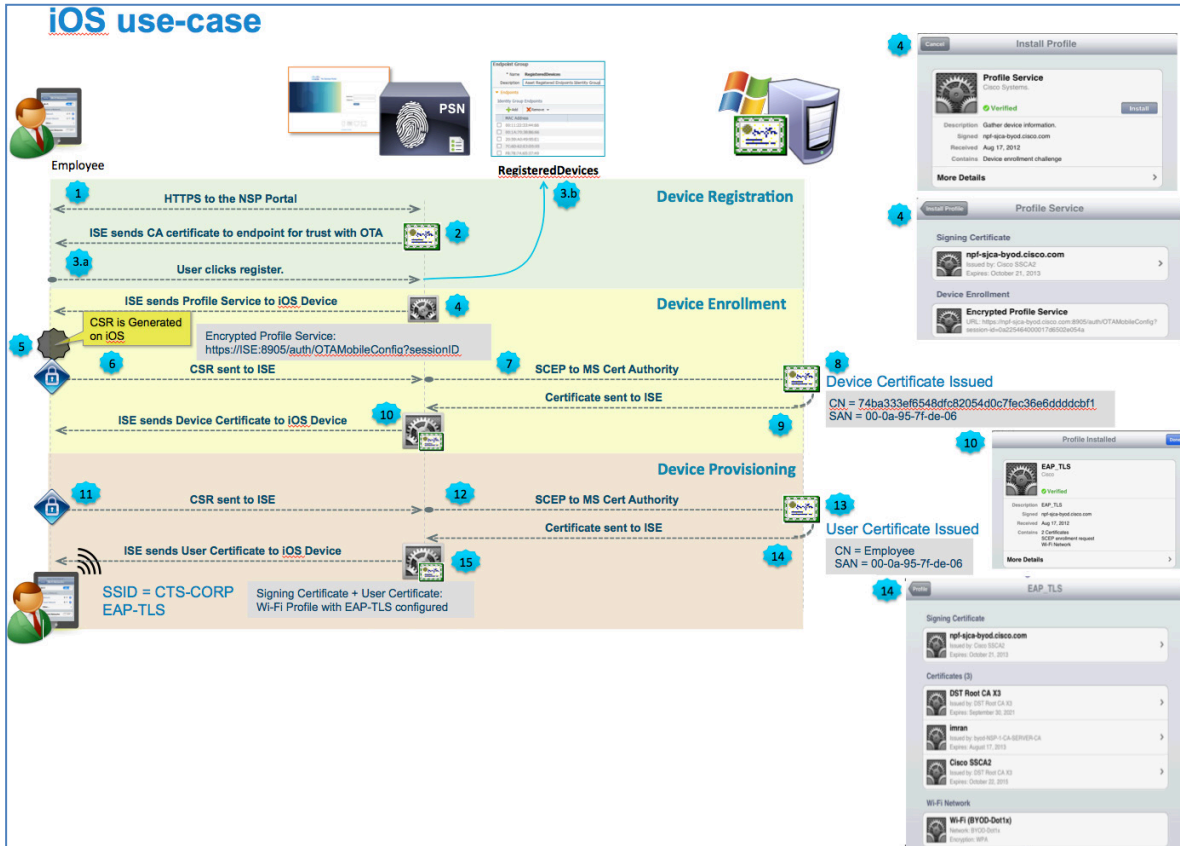
在 TrustSec 测试期间，我们发现在很多情况下 Google Play 使用的是 TCP 和 UDP 端口 5228。但是，要确保所有受测 Android 设备正常运行，这还不够。可能还需要打开产生该端口 8880 的互联网搜索（请参阅附录 C：参考）。根据 Android 的配置，系统可能会提示最终用户选择“Internet”或“Play Store”选项。

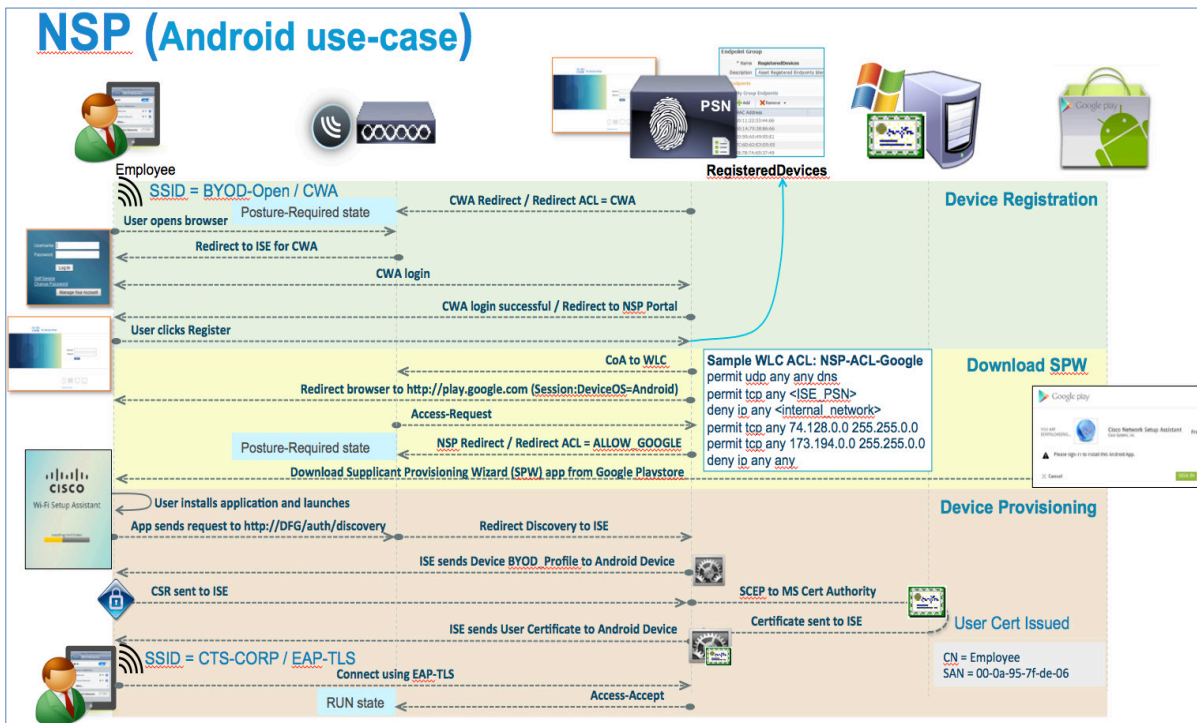
表 3. 测试实验室中有效的网络和端口

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
互联网选项	74.125.00/16 173.194.0.0/16	UDP: 5228 TCP: 所有端口

附录 C: BYOD 流程

本节介绍 iOS 和 Android 设备的 BYOD 流程。





附录 D：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