添加身份库和创建身份验证策略

安全访问操作指南系列

作者：Aaron Woland

日期：2012 年 8 月

目录

添加身份库和创建身份验证策略

概述

思科® 身份服务引擎 (ISE) 可提供内部数据库，对用户和终端进行身份验证。通常，内部数据库用于以下两种情况：通过 Web 身份验证对访客用户进行身份验证，或通过 MAC 身份验证绕行 (MAB) 对终端进行身份验证。不过，思科 ISE 也可通过集成外部身份源对用户或终端凭证进行验证，并检索与用户或设备相关联的安全组成员和其他属性，以便用于授权策略。外部身份源不仅可用于进行 802.1x/MAB/Web 身份验证的用户和终端的身份验证与授权，也可用于 ISE 管理员和访客发起人的身份验证与授权。身份验证过程通过将终端或用户的凭证转发到正确的身份源来验证其有效性。为此，思科 ISE 会处理来自网络接入设备 (NAD) 的 RADIUS 请求，在身份数据库中查询凭证，然后将请求转发到授权策略进行进一步处理，进而为用户和终端分配不同的权限。这样，ISE 就可以使用不同的身份数据库处理不同的身份请求。

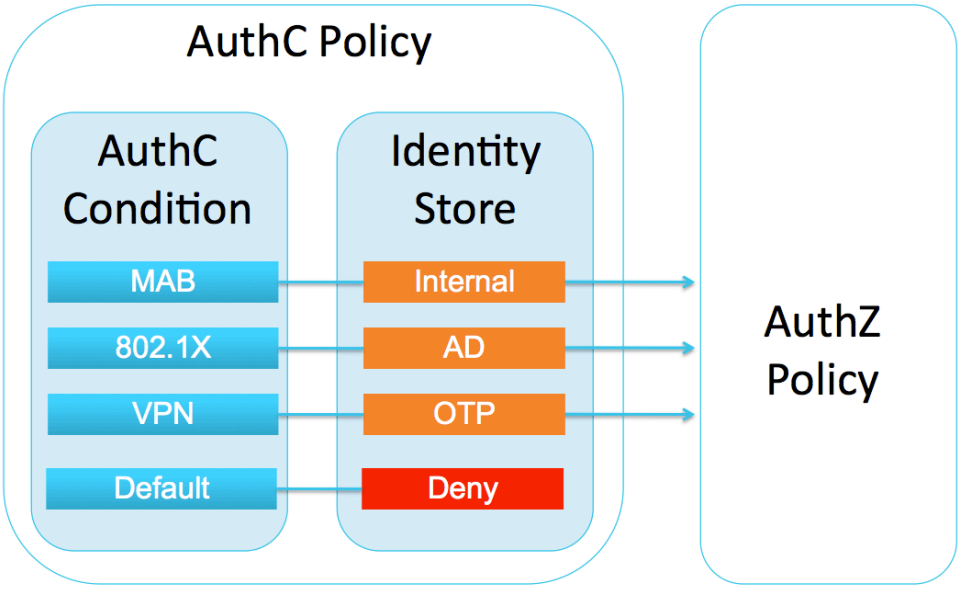
当 NAD 向思科 ISE 发送身份验证请求时，该请求将作为 RADIUS 请求发送（NAD 可能包括 VPN 集中器、无线局域网控制器和局域网交换机）。RADIUS 请求包含多个属性，其中包括用户名/密码、服务类型和类属性等。身份验证策略将传入的 RADIUS 请求与配置的身份验证条件进行比较，使用协议允许的过滤器过滤出协议和可扩展身份验证协议 (EAP) 类型，选择分配的身份库，并处理身份库发送回来的响应。然后，交给授权 (AuthZ) 策略接管。

例如，当终端通过受保护的可扩展身份验证协议 (PEAP) 与 Microsoft 质询握手身份验证协议版本 2 (PEAP-MSCHAPv2) 进行身份验证时，ISE 身份验证策略可使用身份验证条件将请求定向到 Active Directory (AD) 身份源。但是，如果 ISE 接收的是 MAB 请求，则可以将请求定向到内部终端数据库。另一种场景是将 VPN 请求转发到一次性密码 (OTP) 服务器进行身份验证，而将 WLAN 和 LAN 802.1X 请求转发到 AD 进行身份验证。

注：为便于阅读和区分术语，我们通常将身份验证策略称为 AuthC 策略，将授权策略称为 AuthZ 策略。

ISE 图形用户界面逻辑可帮助区分 AuthC 策略和 AuthZ 策略（图 3）。AuthC 策略会根据传入的身份验证请求决定要查询的身份库。例如，来自 VPN 网关的身份验证请求可能会配置为通过检查 OTP 服务器对凭证进行验证。同时，如果使用相同的 ISE 安装，来自思科无线局域网控制器 (WLC) 的身份验证请求则会使用 Active Directory 验证凭证。ISE 能够提供非常强大灵活的身份验证策略功能。

图 3 IES 身份验证和授权策略结构



您必须先在 ISE 中配置包含您的用户信息的外部身份源，然后才能使用外部身份源来配置 AuthC 策略。本操作指南提供有关 EAP 方法的基本介绍，并示范如何使用 Microsoft AD 和轻量级目录访问协议 (LDAP) 来处理身份库。

了解 EAP 方法和身份源

并非所有身份源都支持所有 EAP 方法。在选择身份源时，请务必验证其是否支持您要部署的 EAP 方法。反之，如果已经决定了要使用的身份源，则务必要选择该身份源支持的 EAP 方法。例如，使用 MSCHAPv2 作为内部方法的 EAP 类型（例如 PEAP-MSCHAPv2）可以将 Active Directory 用作后端数据库，但不能使用通用 LDAP 服务器。表 1 显示各种身份源平台及其支持的 EAP 方法。

表 1 主要身份源平台支持的 EAP 类型

EAP-Type	Win 7 Native	Vista Native	Win XP Native	AC 3.0	Apple SL (10.6)	Ubuntu	RHL	ACS 5.2	ISE 1.0	AD	LDAP
EAP-TLS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EAP-TTLS	No	No	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes
PEAP MSCHAPv2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
PEAP EAP-GTC	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PEAP EAP-TLS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
EAP-FAST MSCHAPv2	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
EAP-FAST EAP-GTC	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Active Directory 配置

思科 ISE 使用 Active Directory 连接器，因此 TrustSec 部署中的每个思科 ISE 节点都可以加入 AD 域并访问 AD 资源，正如任何其他 Windows 域成员一样。这种场景在 Active Directory 与 TrustSec 安全解决方案搭配使用时，能够大幅提高速度、易用性和灵活性。ISE AD 集成支持多个 AD 域，只要这些域之间已配置双向信任关系即可。如果要设法将 ISE 集成到不可能在域之间建立双向信任关系的环境中，请参阅《TrustSec 多 Active Directory 操作指南》。

思科最佳实践： 时间同步和域名系统 (DNS) 对与 Active Directory 集成具有重要作用。因此，请务必使用网络时间协议 (NTP) 并始终确保为所有 Active Directory 服务器正确配置 DNS 的反向 DNS 指针。

思科 ISE 配置和 Active Directory 集成

程序 1　加入域

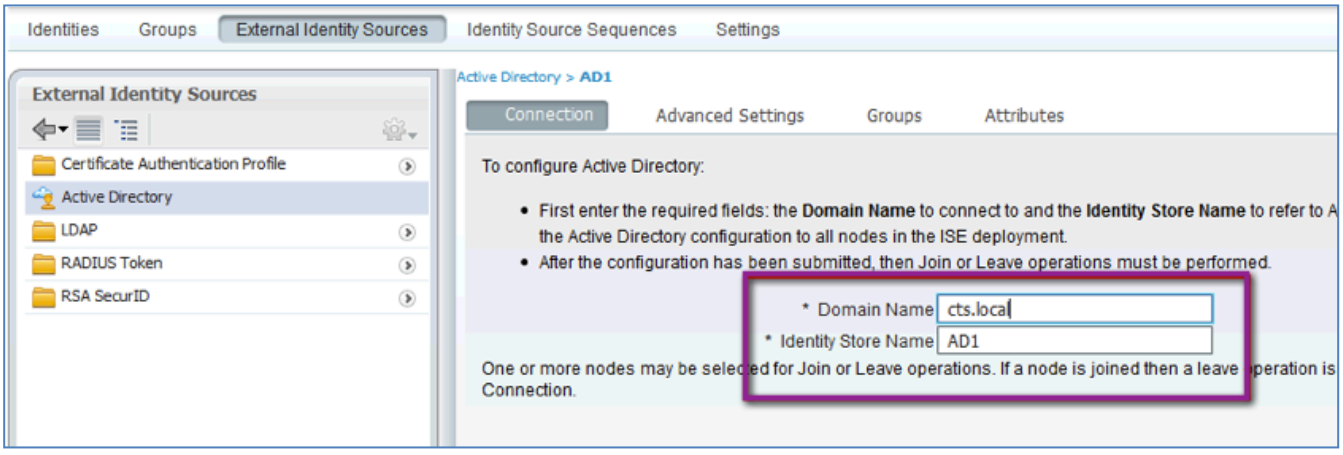
分别将每个思科 ISE 节点加入域。以下是所有思科 ISE 节点与 Active Directory 之间必须开放的端口的列表：

- SMB (TCP/445)
- KDC (TCP/88)
- 全局编录（TCP/3268 和 3289）
- KPASS (TCP/464)
- NTP (UDP/123)
- LDAP（TCP 和 UDP/389）
- LDAPS (TCP/636)

步骤 1　在思科 ISE GUI 中，选择 Administration → Identity Management → External Identity Sources → Active Directory。

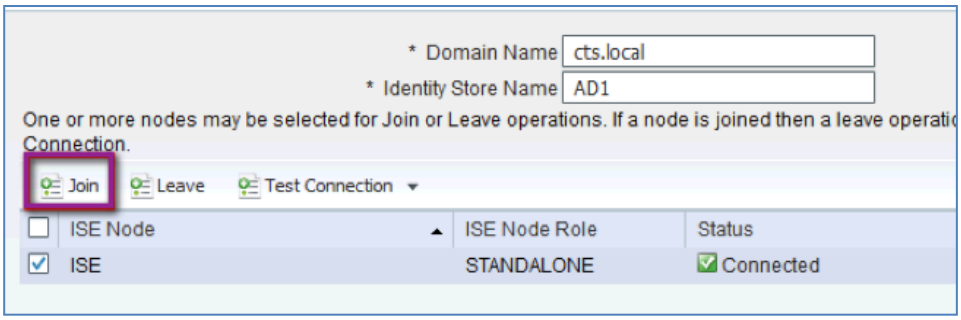
步骤 2　输入 AD Domain Name（在本示例中为 cts.local），然后点击 Save Configuration（图 4）。

图 4 AD 外部身份源：配置 AD 连接器



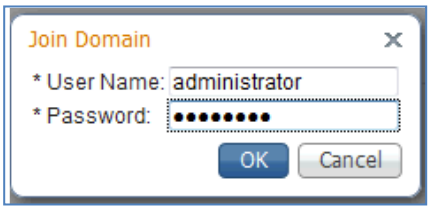
步骤 3　点击 ISE 复选框，然后点击 Join（图 5）。

图 5 AD 外部身份源：加入操作



系统将显示 Join Domain 弹出窗口。输入有权将工作站加入该域的 AD 帐户的用户名和密码 - 例如 administrator（图 6）。

图 6 AD 外部身份源：帐户信息



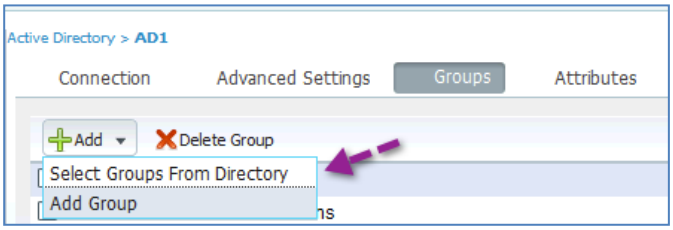
注：上一步操作所用的用户帐户至少必须具有添加和删除计算机的权限。

注：用于将 ISE 节点添加到域的凭证并非保存在 ISE 中。

步骤 4　选择 Administration → Identity Management → External Identity Sources → Active Directory → Groups。

步骤 5　选择选项 Select Groups From Directory（图 7）。

图 7 AD 外部身份源 - 组

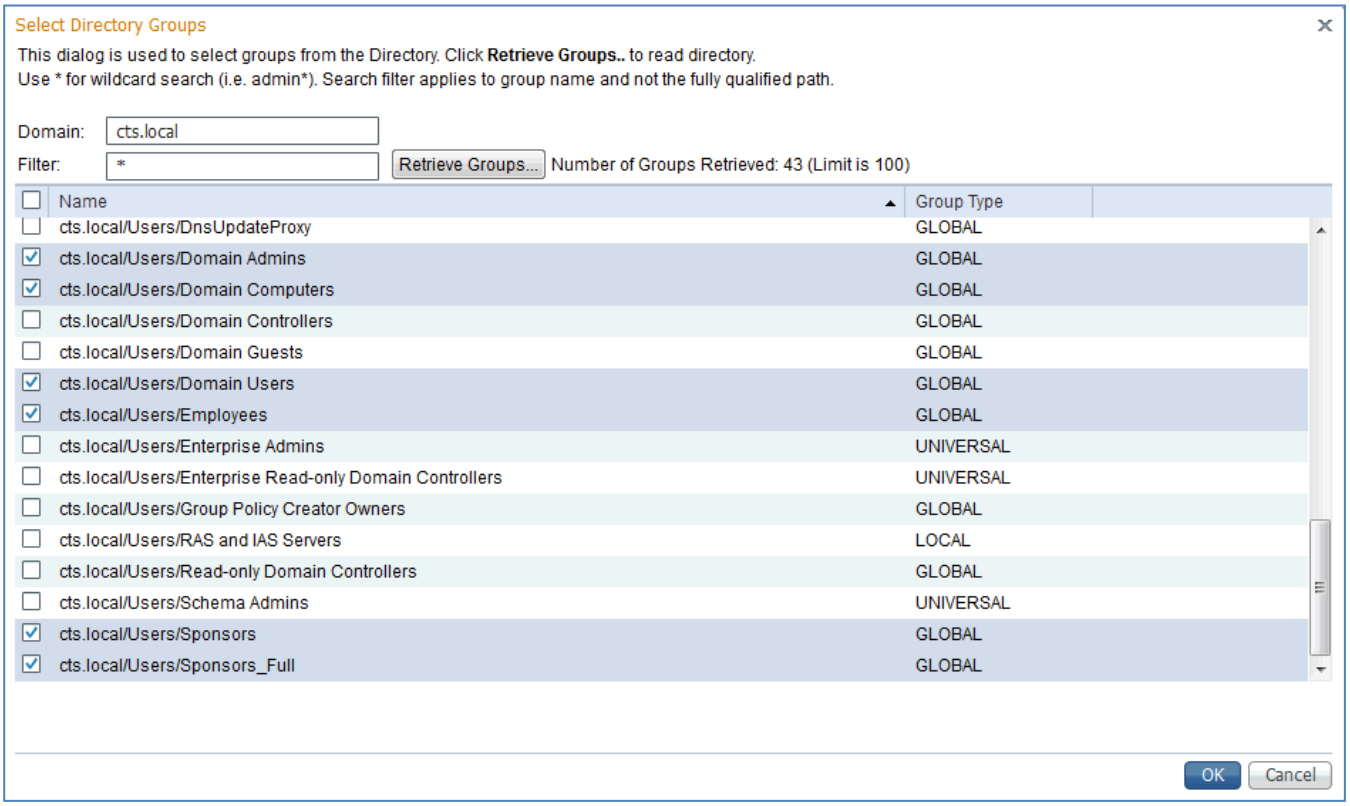


思科 ISE 允许网络管理员从 Active Directory 中选择特定的组和属性。这样便可以在根据 AD 对用户进行身份验证时缩短查找时间。它还有助于确保在管理员构建与 AD 组相关的策略时，管理员只需要浏览比较短的列表而无需查看 Active Directory 中的每个组。

步骤 6　选择策略决策中要使用的组（图 8）。

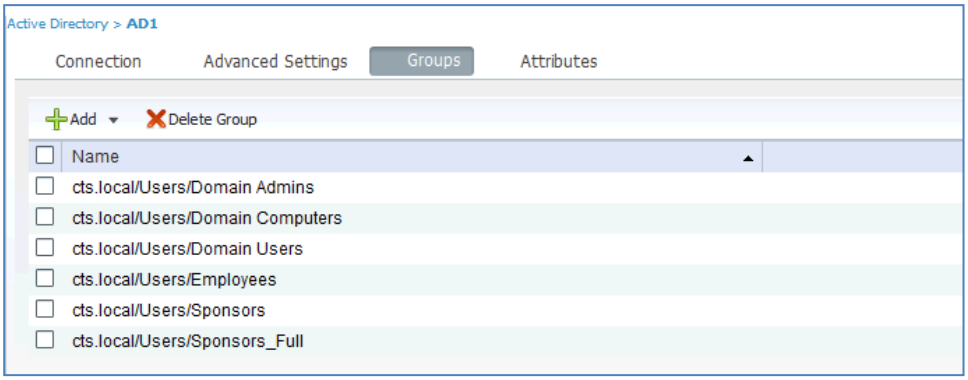
选择网络访问策略中稍后要使用的组。常见的组可能包括：Domain Computers、Contractors、Employees、Domain Users 等。您可以随时添加和删除组。

图 8 AD 外部身份源 - 搜索组



步骤 7　选择所有必要的组之后，点击 OK（图 8）。

图 9 AD 外部身份源：选择组



步骤 8　点击 Save Configuration（图 10）。

图 10 保存配置

LDAP 配置

思科 ISE 支持使用符合 LDAP v3 的 LDAP 服务器进行身份验证。尽管 LDAP 服务器需要通过策略管理节点 (PAN) GUI 添加，但每个策略服务节点 (PSN) 却直接连接到为身份验证请求配置的 LDAP 服务器。

AuthZ 的配置过程中也要使用 LDAP，这与终端是否通过 LDAP 进行身份验证无关。换言之，您可以将身份验证配置为使用证书身份验证配置文件 (CAP)，并在配置的 LDAP 服务器中执行终端组成员查找，查看有无其他授权条件。

有关如何使用 LDAP 查找配置 CAP 的详细信息，请参阅《TrustSec 多 Active Directory 操作指南》。

当您在思科 ISE 中设置 LDAP 服务器时，您会发现系统中已有适用于 Microsoft Active Directory、Sun directory server 和 Novell eDirectory 的预定义架构。对于其他符合 LDAPv3 的服务器，可以使用自定义选项来配置架构设置。下一节将举例说明如何将 ISE 配置为连接到 Microsoft Active Directory 服务器进行 LDAP 身份验证。

程序 1　添加 LDAP 服务器

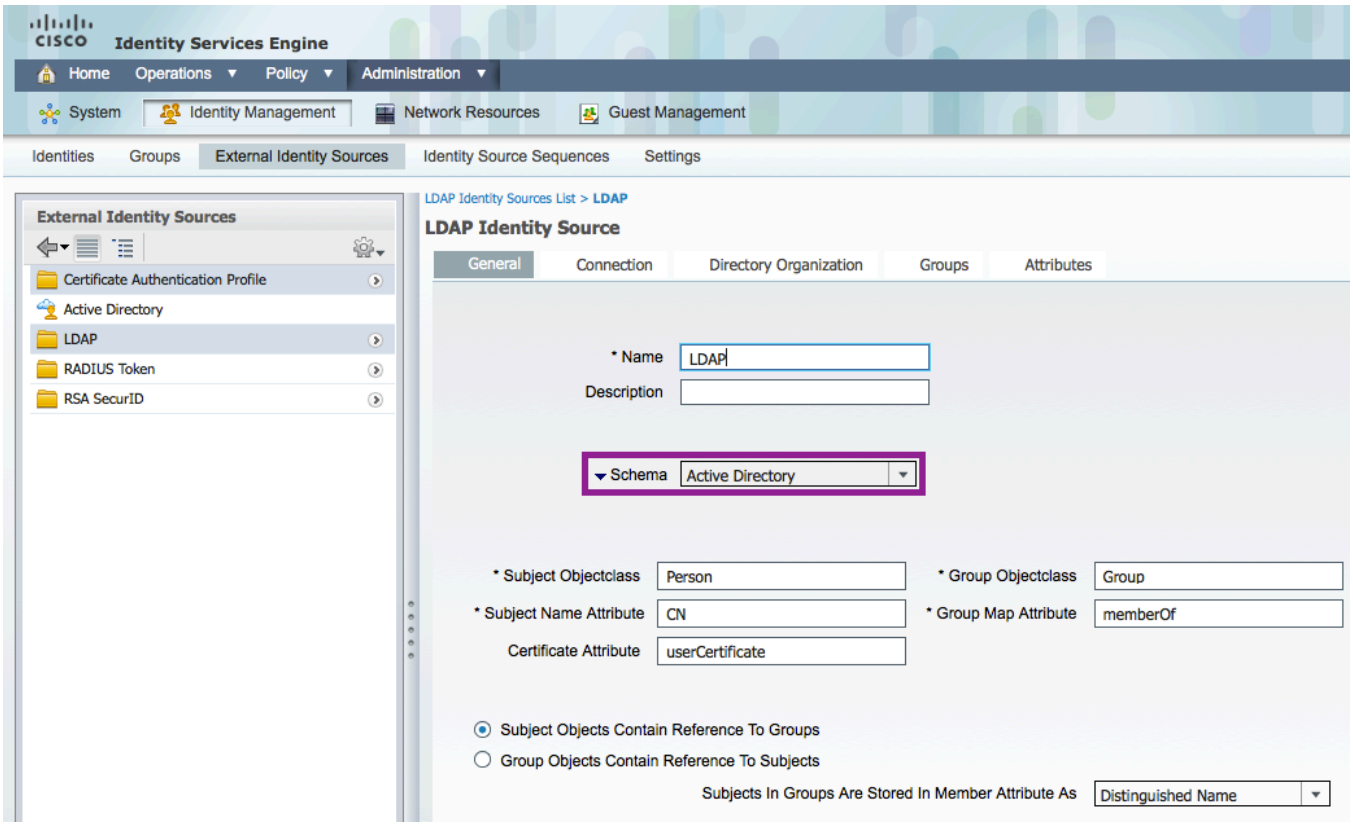
步骤 **1**　导航至 Administration → Identity Management → External Identity Sources → LDAP。

步骤 **2**　点击 Add。

步骤 **3**　输入 LDAP 身份源的名称。

步骤 **4**　选择 Active Directory 作为 Schema。点击向下箭头查看 Active Directory Schema 的详细信息（图 11）。

图 11 LDAP 外部身份源：架构



步骤 5　点击 Connection 选项卡。

步骤 6　输入 Hostname/IP（请参阅图 12）。

步骤 7　输入 Port 号。在本示例中，此编号为 389。

步骤 8　对 Access 类型选择 Authenticated Access。

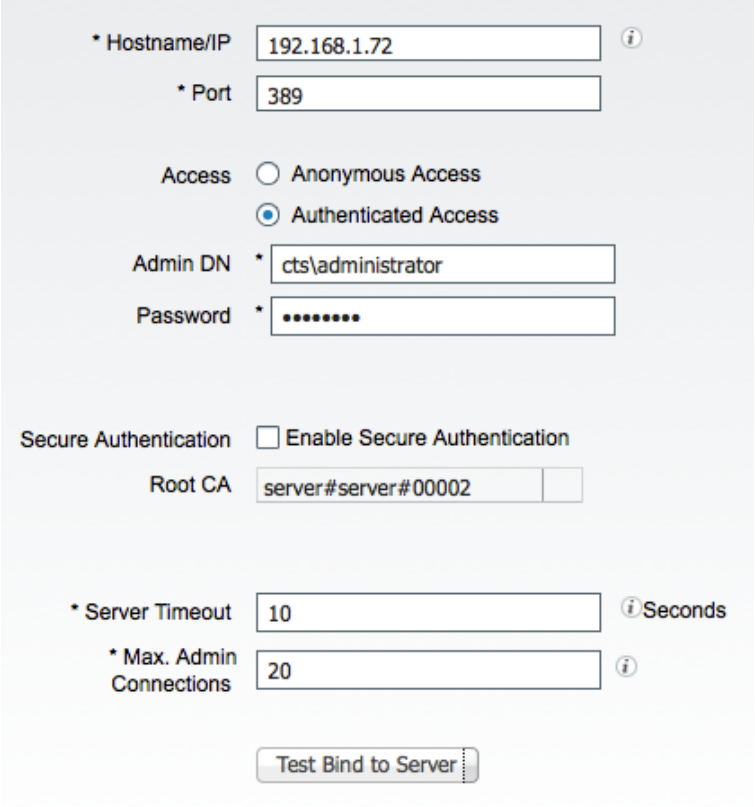
步骤 9　输入 Admin DN - 在本示例中为 cts\administrator。这是在 Active Directory 中具有 Schema Admin Group 成员身份的用户的可分辨名称。例如：cn=SchemaAdmin, cn=Users, dc=demo, dc=local。

步骤 10 输入 Admin DN 的密码。

最佳实践：思科 ISE 最多允许使用两台 LDAP 服务器来实现冗余。我们建议您使用两台服务器，以防主服务器发生故障。

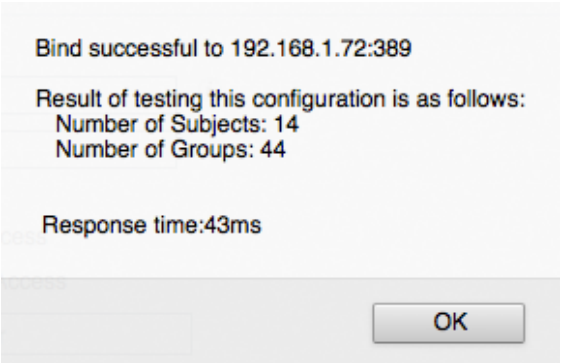
最佳实践：建议您通过启用安全身份验证来使用 SSL。LDAP 设置可能需要使用不同端口。

图 12 LDAP 外部身份源：配置



步骤 11 点击 Test Bind to Server 验证配置。此时应显示确认消息，如图 13 所示。

图 13 LDAP 外部身份源：测试绑定验证

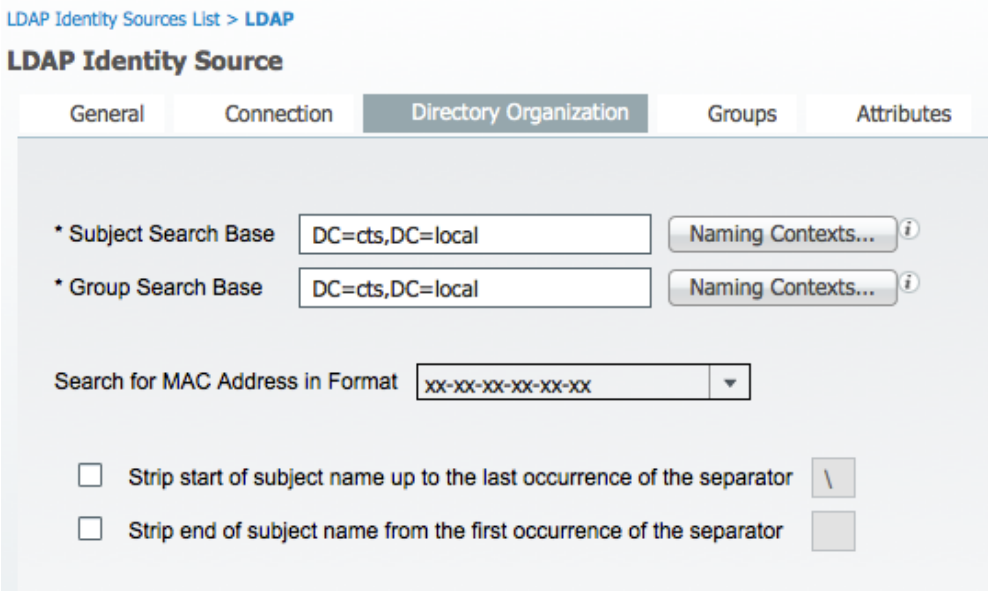


步骤 12 点击 Directory Organization 选项卡。

步骤 13 将 Subject Search Base 和 Group Search Base 配置为 DC=cts, DC=local（图 14）。

最佳实践：最好尽量具体地定义搜索库。如果是标准的 Active Directory 服务器配置，用于主题和组搜索的搜索库为 **CN=Users, <Domain Component>**。(CN=Users, DC=demo, DC=local)

图 14 LDAP 外部身份源：目录组织

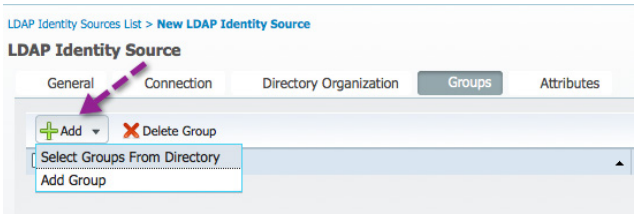


步骤 **14** 导航至 Groups 选项卡。

步骤 **15** 选择 Groups → Add →Select Groups From Directory（图 15）。

思科 ISE 允许网络管理员从 Active Directory 中选择特定的组和属性。此情景可以在对用户进行身份验证时缩短查找时间。此外，它还可确保管理员在构建与 AD 组相关的策略时，只需要浏览比较短的列表而无需查看 AD 中的每个组。

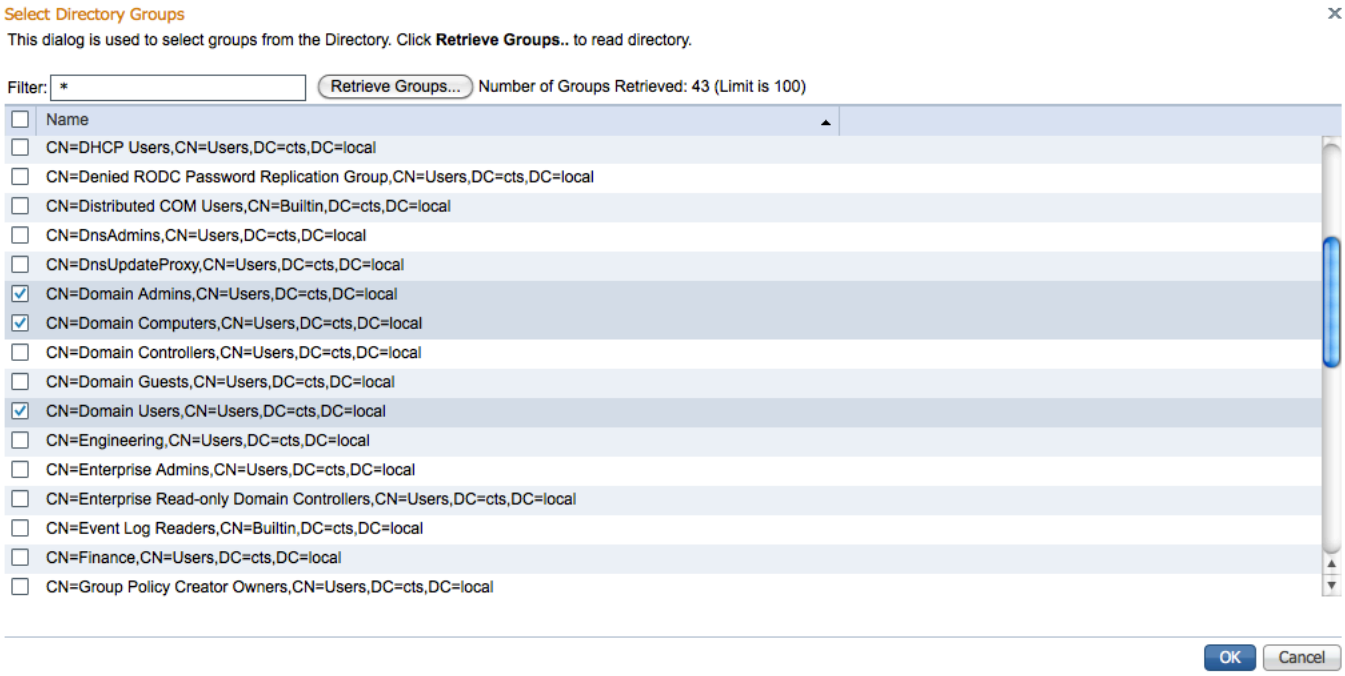
图 15 LDAP 外部身份源：外部组



注：找到的组是根据您在 LDAP Identity Source 常规页面（图 11）中配置的 **memberOf** 属性进行搜索所返回的值的结果。

步骤 **16** 从检索到的组中，选择要用于定义 AuthC 策略和 AuthZ 策略的特定组（图 16）。

图 16 LDAP 外部身份源：搜索组



步骤 17 点击 Save。

内部数据库/证书授权配置文件 (CAP)/RADIUS 令牌/RADIUS 代理

除 AD 和 LDAP 外，思科 ISE 还支持内部数据库、证书、将 RADIUS 令牌服务器用作 OTP 服务器，以及通过本地集成将 RSA SecurID 令牌服务器用于身份验证。ISE 提供三种类型的内部数据库：用户、终端和访客。用户和访客身份数据库通常在使用 802.1x 或 Web 身份验证进行身份验证时用于终端身份验证。终端身份数据库则用于根据自动分析、设备注册以及手动创建的 MAC 地址白名单或黑名单对终端进行分类。终端身份源可用于对终端进行简单的 MAB 身份验证，也可在授权过程中与其他条件搭配用于企业 BYOD 策略。

注：只有在登录发起人门户页面后，访客身份数据库才可见。

证书身份验证配置文件 (CAP) 可用于对以数字证书标识自己身份的终端进行身份验证。在要求使用数字证书进行相互身份验证的环境中，就会使用此方法。你可以选择使用哪一个 X.509 字段作为终端身份，例如 CN= 字段的主题或 SAN 的邮箱地址。

如果要与一次性密码 (OTP) 服务器集成，思科 ISE 支持 RADIUS 令牌服务器和本地 SecurID 集成。当 OTP 服务器在本地运行 RADIUS 并且 ISE 将 RADIUS 请求转发到 OTP RADIUS 服务器时，使用 RADIUS 令牌服务器。如果思科 ISE 在本地终止 RADIUS 并通过安全设备调配 (SDP) 功能将 OTP 请求转发到 SecurID 服务器，则使用 SecurID。

CAP 和 OTP 的配置不属于本文档的讨论范围。有关详细信息，请参阅 ESS 1.1 用户手册文档。

身份源序列

身份序列在 ISE 中用来提供单个“对象”，该对象实际上是仅供 ISE 在验证凭证时进行查询的身份库的序列。如果存在多个身份数据库，而且无法在处理身份验证请求期间确定用户是哪个身份源的成员，则此序列非常有用。在我们的配置示例中，我们创建的是按顺序查询以下身份库的身份序列：Active Directory → Internal Users。

最佳实践：尽量避免使用身份源序列。反之，应该使用身份验证条件将身份验证请求转发到正确的身份源。

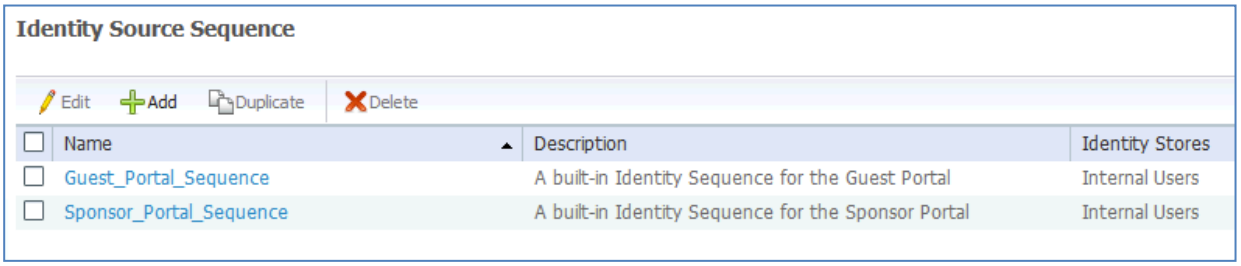
添加身份源序列

程序 1　创建身份序列

步骤 1　导航至 Administration → Identity Management → Identity Source Sequences。

步骤 2　默认情况下有两个身份源序列（图 17）。

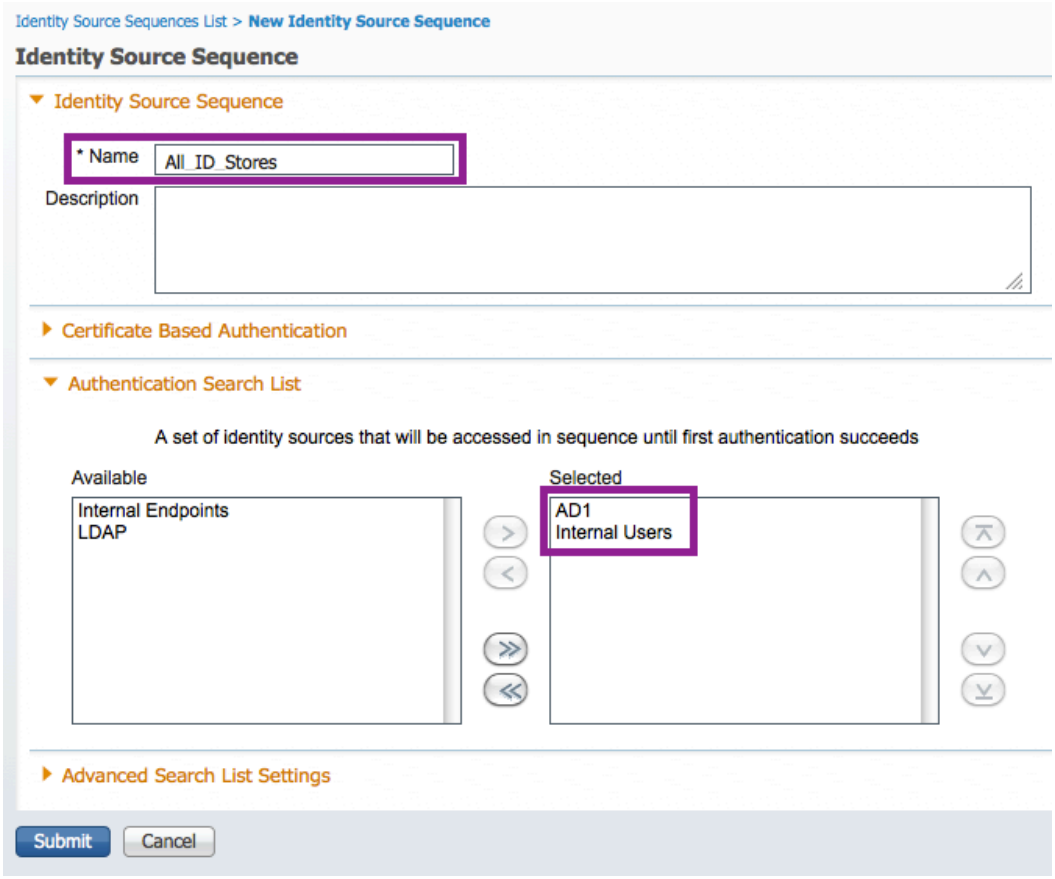
图 17 添加身份源序列



步骤 3　点击 Add。

步骤 4　将身份序列命名为 All_ID_Stores。从左侧窗格选择身份库 AD1 并将其添加到右侧窗格。然后，选择并添加 Internal Users（图 18）。

图 18 配置身份源序列



步骤 5　滚动到窗口底部，然后点击 Submit。

创建身份验证策略

在我们的配置示例中，我们将创建执行以下操作的身份验证策略：

- 将所有 MAB 请求转发到内部终端数据库
- 将有线和无线 802.1x 请求转发到 AD
- 将所有未知请求转发到上一节中配置的 All_ID_Store 序列

配置身份验证策略

程序 1　检查默认 ISE 身份验证策略

步骤 1　导航至 Policy → Authentication。

身份验证策略中有两条预配置规则以及一条默认规则。策略规则表与访问列表一样，从上向下进行处理，采用第一条匹配的规则。

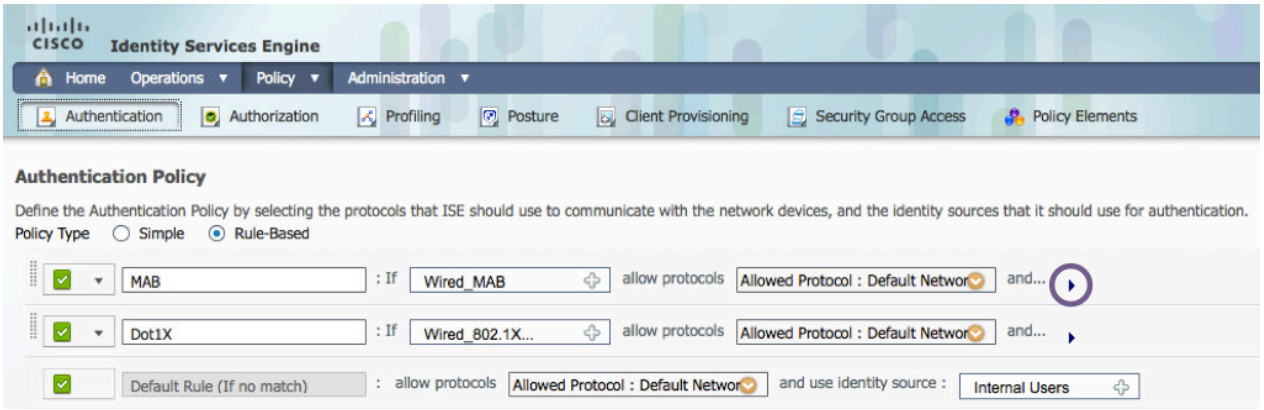
注： 页面顶部有 Policy Type 选项，可用于选择简单策略还是基于规则的策略。如果使用 Simple 选项，只能将所有身份验证请求都转发到一个身份源或身份源序列。对于大多数部署而言，建议使用基于规则选项，以便将身份验证请求有效地路由到正确的身份源。

身份验证请求与规则行按照一定条件进行匹配。为详细说明，我们将具体介绍一下第一条预配置规则 MAB，这是交换机中用于 MAC 身份验证绕行的规则。

思科 ISE 策略采用逻辑 IF-THEN 格式。请注意显示为 Wired_MAB 的“选择器”前面的 IF。此行说明：“如果 RADIUS 请求是 Wired_MAB，则允许使用默认网络协议。”

```
IF Wired_MAB
THEN Allow the default protocols
ELSE
Move to next Line in Authentication Policy Table
```

图 19 身份验证策略

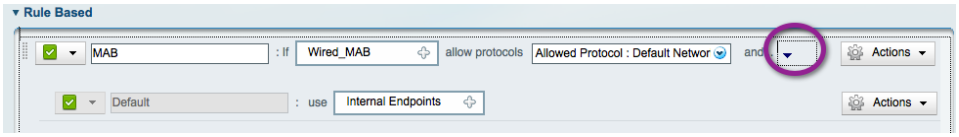


步骤 2　在图 19 中，请注意 Allowed Protocol 框后的 "and..."。在 "and..." 这个词旁边是黑色的下拉三角形（在图 19 中标有圆圈）

步骤 3　点击此三角形。

此操作的结果如图 20 所示。身份验证策略表中的各规则均含有第二部分。此行用于选择凭证库。默认情况下，会将 MAC 身份验证绕行的此预配置规则配置为使用内部终端数据存储。内部终端数据存储是 ISE 内部已知设备的数据库，此数据库可以进行手动填充或动态填充。

图 20 身份验证策略：MAB



注：手动填充示例：管理员从 Cisco Unified Communications Manager 界面导出已知思科统一 IP 电话 MAC 地址列表，然后将该列表导入 ISE。
动态填充示例：ISE 分析通过一个或多个分析探针发现此设备，然后在内部终端数据存储中创建此设备条目。

IF-THEN 语句显示如下：

```
IF Wired_MAB
THEN Allow the default protocols
  AND  Check Credentials with the Internal Endpoints Data Store
ELSE
Move to next Line in Authentication Policy Table
```

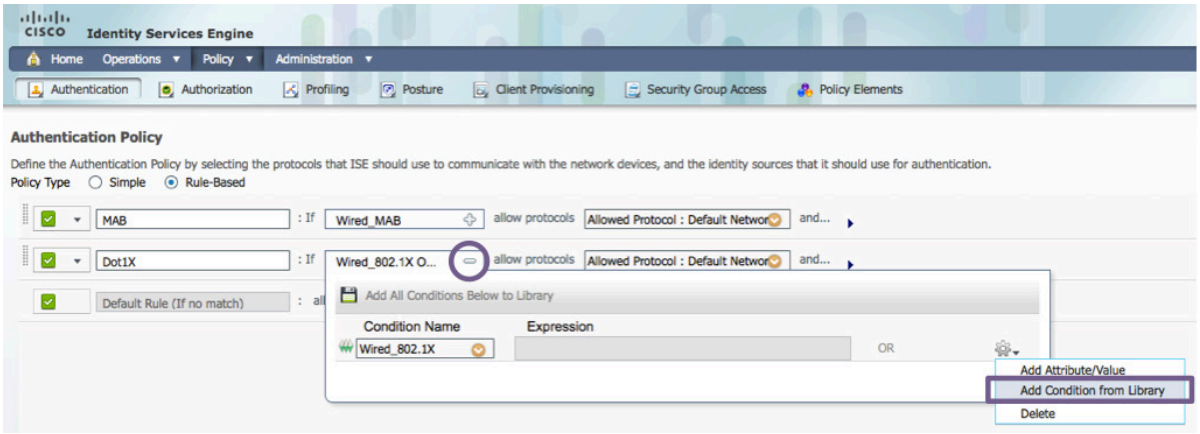
注：Wired_MAB 是预构建条件，用来匹配 RADIUS 属性 **service-type = call-check** 和 **nas-port-type = ethernet**。

程序 2　启用无线身份验证

步骤 1　导航至 Policy → Authentication。

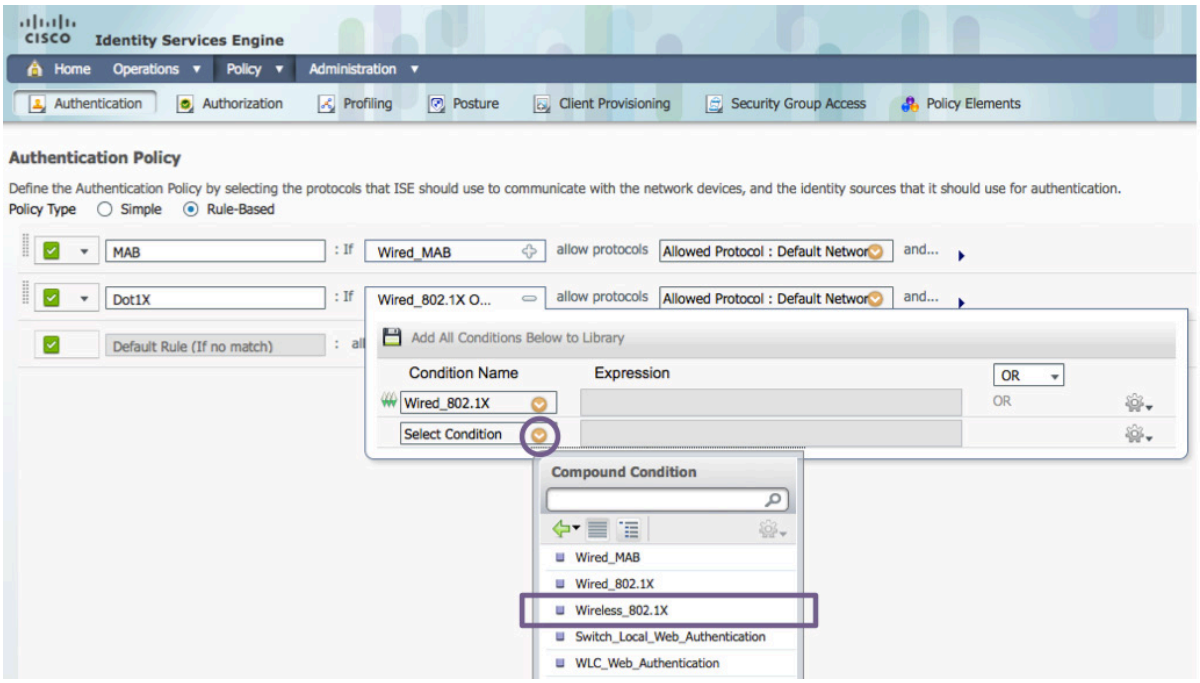
步骤 2　展开 Dot1X 规则的 IF 条件，并选择 Add Condition from Library（图 21）。

图 21 身份验证策略：添加 WLAN 条件 1



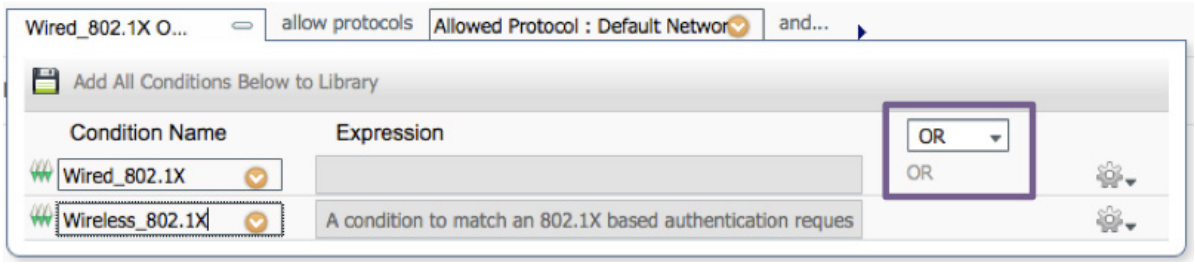
步骤 3　从 Select Condition 下拉菜单中，选择 Compound Condition → Wireless_802.1X（图 22）。

图 22 身份验证策略：添加 WLAN 条件 2



步骤 4　确保运算符指定为 OR 而不是 AND（图 23）。

图 23 身份验证策略：添加 WLAN 条件 3



步骤 5　保存设置。

Dot1X 规则的 IF-THEN 语句显示如下：

```
IF Wired_802.1X or Wireless_802.1X
THEN Allow the default protocols
  AND  Check Credentials with the Internal Users Data Store
ELSE
Move to next Line in Authentication Policy Table
```

注：Wired_802.1X 是预构建条件，用来匹配下列 RADIUS 属性：**service-type = Framed** 和 **nas-port-type = Ethernet**。相反，Wireless_802.1X 是用来匹配以下 RADIUS 属性的预构建条件：**service-type = call-check** 和 **nas-port-type = Wireless – IEEE 802.11**。

程序 3　更改身份库

如果采用预配置规则，MAB 会使用内部终端存储来查询已知设备的 MAC 地址。如果传入的身份验证请求是 802.1X 身份验证，那么 ISE 会使用“内部用户”数据存储来检查用户名和密码有效性。

如果是其他类型的身份验证（例如 WebAuth），则不会与任何一条预配置规则相匹配，最终会使用默认规则。默认规则预配置为检查内部用户数据存储。

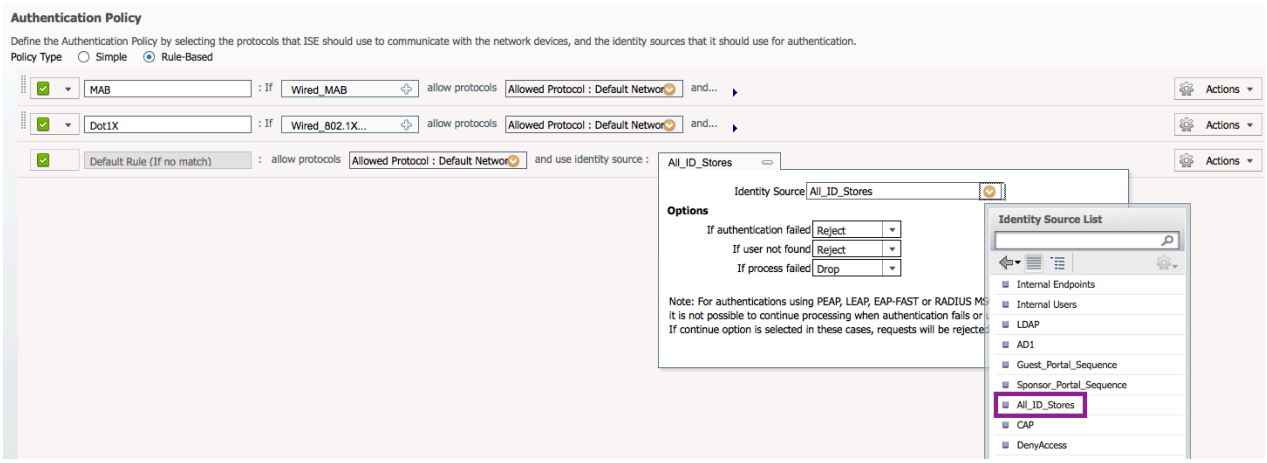
多数组织不愿对用户帐户使用默认的本地数据存储。绝大多数组织使用 Active Directory 作为主要的用户身份数据源。因此，我们会将默认规则改为使用 All_ID_Stores 并且将 Dot1X Rules 改为仅使用 Active Directory。

步骤 1　在 Default Rule 中，点击 Internal Users 旁边的加号。

此操作会打开身份源选择器。

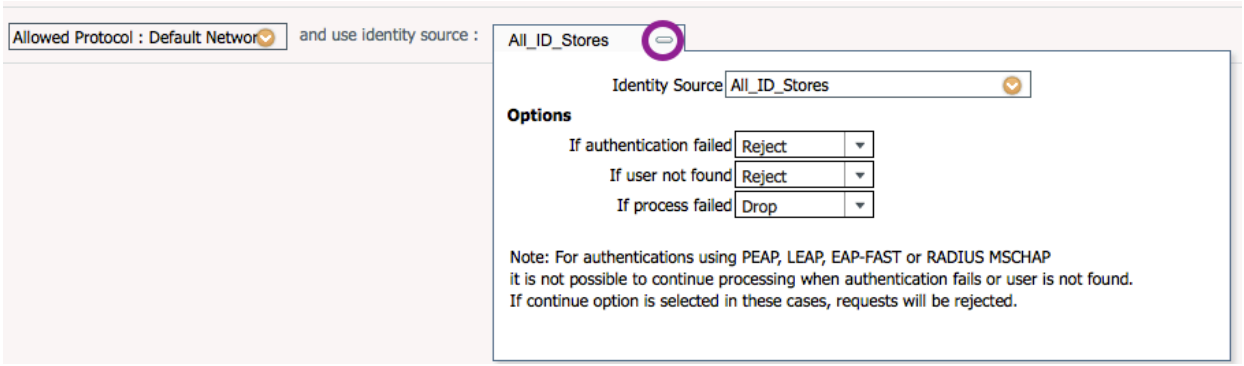
步骤 2　选择先前构建的 All_ID_Stores 身份源序列（图 24）。

图 24 身份验证策略：修改默认规则 1



步骤 3　点击减号关闭身份源选择器（图 25）。

图 25 身份验证策略：修改默认规则 2



步骤 **4** 记下身份源下面的选项。

各选项的操作为：拒绝、丢弃或继续。这三个选项及其相应的选择可用于每个身份验证策略规则，包括默认规则。表 2 介绍这三个选项。表 3 介绍其可配置的操作。

表 2 身份验证选项

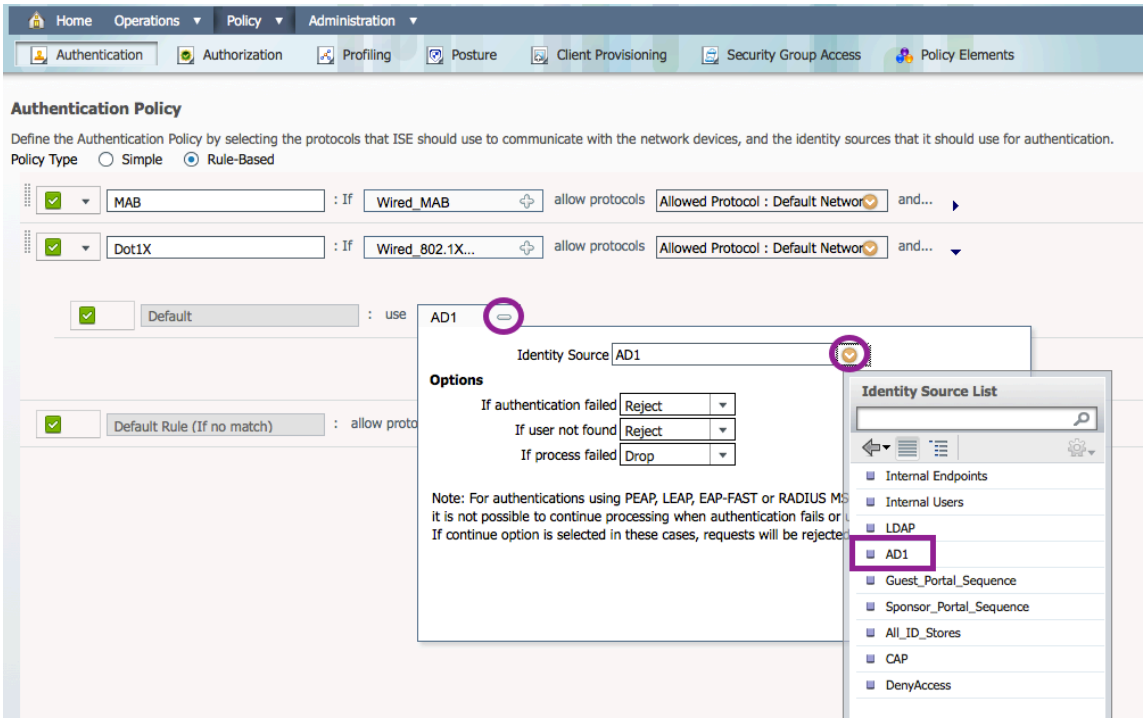
选项	描述
身份验证失败	收到身份验证已失败的明确响应，例如错误凭证、禁用的用户等。默认操作是拒绝。
未找到用户	在任何身份数据库中均未找到此用户。默认操作是拒绝。
处理失败	无法访问身份数据库。默认操作是丢弃。

表 3 身份验证操作

操作	描述
拒绝	向 NAD 发送“RADIUS 访问被拒绝”响应。
丢弃	丢弃访问请求，不发送响应。
继续	继续应用授权策略。

步骤 5　展开 Dot1X 行，重复步骤 1 和 2，将身份源更改为 AD1（图 26）。

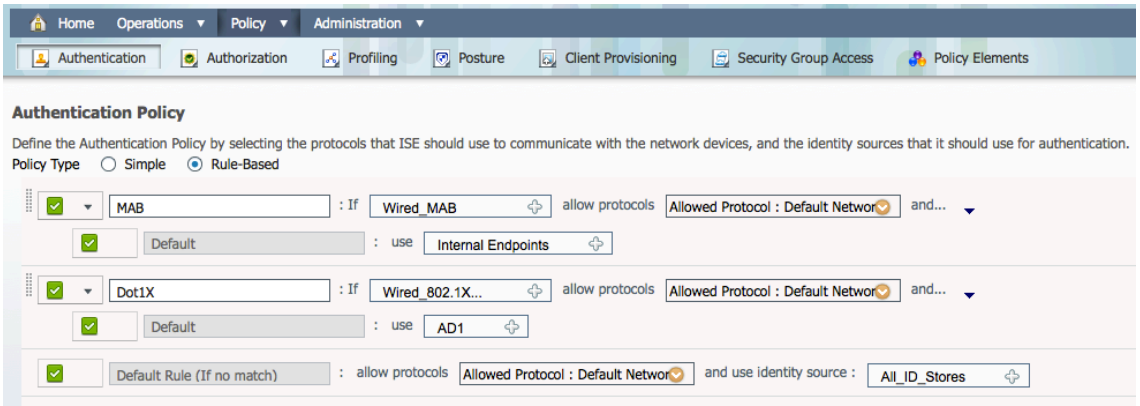
图 26 身份验证策略：802.1X 规则



步骤 6　点击 Save。

身份验证规则应该如图 27 所示。

图 27 最终的身份验证策略



ISE 身份验证策略规则的 IF-THEN 语句显示如下：

```
IF Wired_MAB
THEN Allow the default protocols
  AND  Check Credentials with the Internal Endpoints Data Store
ELSE IF Wired_802.1X or Wireless_802.1X
THEN Allow the default protocols
  AND  Check Credentials with the AD1 Data Store
ELSE IF No Match
THEN Allow the default protocols
  AND  Check Credentials with the All_ID_Stores Data Store
```

注： 您可以广泛地自定义身份验证规则。在这些示例中，我们已使用默认网络访问权限作为我们的允许协议。这能够支持绝大多数身份验证类型，但是使用默认设置不会将访问限制为某类 EAP 方法。

要配置一组可自定义的身份验证协议（例如仅使用 EAP-TLS），请转至 Policy → Policy Elements → Results → Authentication → Allowed Protocols。

附录 A：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/7.2/configuration/guide/cg.html

初始安装和设置

概述

本指南介绍如何运行思科身份服务引擎 (ISE) 安装程序来配置思科 ISE 硬件设备和虚拟机环境。虽然思科 ISE 在订购时已预先安装到物理设备上，但有时候可能需要重新安装物理设备（或重置映象）。本操作指南可用作参考；我们将在稍后一节中示范分步配置。

完成设置对话

需要在虚拟机中全新安装 ISE。安装包括两个程序。

- 程序 1 - 从 ISE ISO 映像引导
- 程序 2 - 启动安装操作系统和 ISE 应用的安装过程

有关如何设置 VMware 的详细信息，请参阅《思科身份服务引擎硬件安装指南》中的“在 VMware Virtual 虚拟机中安装思科 ISE 系统软件”。

完成步骤 1 和 2 后，安装暂停，必须完成设置对话后才能继续并完成安装。

程序 1

要完成设置对话，请执行以下步骤。

步骤 1 登录 ise-1 虚拟机控制台。

```
**********************************************
Please type ‘setup’ to configure the appliance
localhost login:
**********************************************
```

步骤 2 在登录提示符后输入 setup 启动设置对话。

```
Enter hostname[]: ise
Enter IP address []: 10.1.100.21
Enter IP default netmask[]: 255.255.255.0 Enter IP default gateway[]: 10.1.100.1 Enter default DNS
domain[]: demo.local Enter Primary nameserver[]: 10.1.100.10 Add/Edit another nameserver? Y/N : n
Enter Primary NTP server[time.nist.gov]: ntp.demo.local Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC]: <return> Enter username[admin]: <return> Enter password: default1A
Enter password again: default1A Bringing up network interface... Pinging the gateway...
Pinging the primary nameserver ...
Do not use 'Ctrl-C' from this point on... Appliance is configured
Installing applications... Installing ise ...
Generating configuration...

=== Initial Setup for Application: ise ===
Welcome to the ISE initial setup. The purpose of this setup is to provision the internal ISE
database. This setup is non-interactive, and will take roughly 15 minutes to complete. Please be
patient.

Running database cloning script...
Running database network config assistant tool... Extracting ISE database content...
Starting ISE database processes... Restarting ISE database processes... Creating ISE M&T session
directory... Performing ISE database priming...
Generating configuration... Rebooting...
```

虽然没有明确地说明密码策略，但可以用 default1A 作为密码。完成设置对话后，大概需要 45 分钟才能完成安装。主机名和 DNS 域名最好（但不是必须）全部小写。如果打算将此 ISE 加入 Active Directory 域，主机名应限制在 15 个字符以内。

步骤 3 完成设置对话后，安装将继续并在完成后重新启动。显示以下登录提示符时，即表示安装完毕：

```
ise-1 login:
```

此时程序 1 完成。

程序 2

要完成设置对话，请执行以下步骤：

步骤 4 使用您在设置期间提供的凭证登录。

注：您可以继续使用 VM 控制台界面访问 ISE CLI，也可以使用安全外壳 (SSH) 协议。在物理设备上，可以使用串行端口或键盘和视频来访问 ISE CLI。

步骤 5 输入 show run 确认安装设置。

步骤 6 配置存储库。

ISE 存储库是一个文件存储位置，您可以在它与 ISE 之间复制文件。这些存储库可用于各种不同的操作，例如为 ISE 安装补丁或升级。您还可以备份或恢复配置，以及创建支持套件。

不同的存储库类型如下表所示。

表 1. ISE 存储库类型

ISE 存储库	存储库类型
CDROM	只读
FTP	
HTTP	只读
HTTPS	只读
NFS	

步骤 7 在 ISE 中配置 FTP 存储库。

```
ise-1/admin# config t
Enter configuration commands, one per line. End with CNTL/Z. ise-1/admin(config)# repository myFTP
ise-1/admin(config-Repository)# url ftp ftp.demo.local/
ise-1/admin(config-Repository)# user anonymous password plain admin@demo.local
ise-1/admin(config-Repository)# end
ise-1/admin# copy running-config startup-config
Generating configuration... ise-1/admin#
```

步骤 8 使用 show repository 命令确认 ISE 可与该存储库通信。

步骤 **4** 系统将显示来自 FTP 服务器的目录列表。

```
ise-1/admin# show repository myFTP
<file list>
ise-1/admin#
```

步骤 **5** 注：在此示例设置中，FTP 服务器位于 admin PC 上，而 FTP 主目录为 <local directory>:\Configs

步骤 9 确认时间同步正常。

步骤 10 刚配置完网络时间协议 (NTP) 主服务器时，您会发现 ISE 处于未同步状态。

```
ise-pap-1/admin# show ntp
Primary NTP : ntp.demo.local unsynchronized
time server re-starting polling server every 64 s
remote      refid   st t when poll reach   delay   offset jitter
==============================================================================
Warning: Output results may conflict during periods of changing synchronization.
```

步骤 11 几分钟后，ISE 应与 NTP 主服务器同步。星号指出其同步的是哪一台时间服务器。

```
ise-pap-1/admin# show ntp
Primary NTP : ntp.demo.local
synchronised to NTP server (128.107.220.1) at stratum 5 time correct to within 459 ms
polling server every 64 s
remote              refid     st   t    when    poll   reach   delay    offset     jitter
==============================================================================
127.127.1.0     .LOCL.          10  1       5      64      377    0.000    0.000      0.001
127.107.220.1   .LOCL.      4   u     1026   1026   377    0.478   -866.81     60.476

Warning: Output results may conflict during periods of changing synchronization.
```

注：可能无法立即与 NTP 服务器同步。您可能需要等待 10 至 15 分钟，让 ISE 越过本地时钟选择 NTP 服务器。

步骤 12 如果看到 ISE 已经同步到本地计算机（如下所示），这表示 NTP 时间同步未正常工作。

```
ise-pap-1/admin# show ntp
Primary NTP : ntp.demo.local synchronised to local net at stratum 11
time correct to within 10 ms polling server every 1024 s
remote             refid     st t     when    poll    reach    delay     offset     jitter
==============================================================================
127.127.1.0    .LOCL.     10 1        5       64     377     0.000       0.000       0.001
127.127.220.1 .LOCL.      4 u     1026     1024     377     0.478     -866.61      60.476

Warning: Output results may conflict during periods of changing synchronization.
```

注：可能无法立即与 NTP 服务器同步。您可能需要等待 10 至 15 分钟，让 ISE 越过本地时钟选择 NTP 服务器。

ISE Web GUI 访问

概述

首次登录思科 ISE 基于网络的界面时，需要使用预先安装的评估许可证。您只能使用 ISE 支持并启用 HTTPS 的浏览器，之前的章节中已列出这些浏览器。在按照本指南所述安装思科 ISE 后，即可登录思科 ISE 基于网络的界面。

启动与 ISE 之间的 Web 会话

要登录并启动与 ISE 之间的 Web 会话，请执行以下步骤：

步骤 1 打开启用 HTTP 的浏览器窗口，浏览到 http://ise.demo.local。

注：此 URL 根据上一节中的实验设置而定。使用 http://<host name>.<domain name> 访问浏览器。启用 HTTPS 的浏览器包括：Mozilla Firefox 2.6 和 9 以及 Microsoft Internet Explorer 8 和 9。

会话将被重定向到安全的思科 ISE 登录页面：https://ise.demo.local/admin。

步骤 2 在登录页面，输入您在设置过程中定义的用户名和密码。

步骤 3 点击 Login，系统将显示思科 ISE 控制面板，如图 2 所示。

注：默认的 Web UI 凭证为 admin/cisco。首次登录时，系统会提示您更改默认密码。

图 1. ISE Web 登录

证书和证书颁发机构

概述

本指南介绍如何生成 ISE 证书，证书颁发机构 (CA) 如何向 ISE 颁发证书，以及如何将证书安装到 ISE。在安装思科 ISE 时，会生成默认的自签名证书。尽管此证书用于实验和演示已经足够，但是将使用自签名证书的思科 ISE 用于生产环境却不是一个好办法。为了确保与 ISE 的通信，无论通信与身份验证相关还是用于 ISE 管理（例如使用 ISE Web 界面进行配置），都需要配置 X.509 证书和证书信任链以启用非对称加密。

注：时间同步对于证书操作非常重要。请确保您已配置 NTP 并已设定正确时间。

思科 ISE 配置 - 证书和信任 CA

注：对于证书链：应成功导入整个证书链后再创建证书请求

步骤 1 登录思科身份服务引擎，然后点击 **Administration** 选项卡。
步骤 2 点击菜单栏中的 **System** 链接，然后选择 **Certificates**。

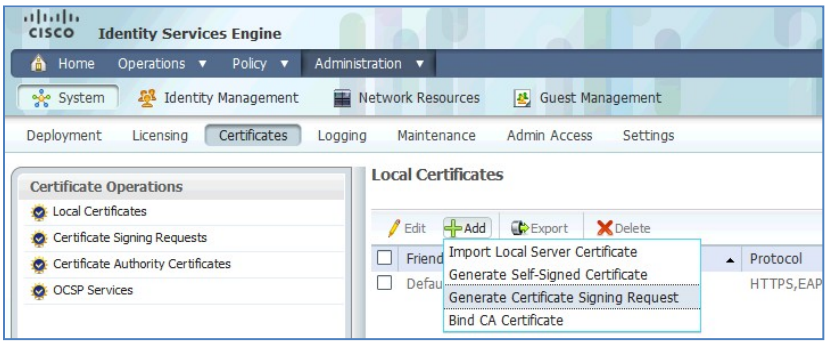


图 2. 证书

步骤 3 点击 **Add** 按钮。
步骤 4 从下拉菜单中选择 Generate Certificate Signing Request。

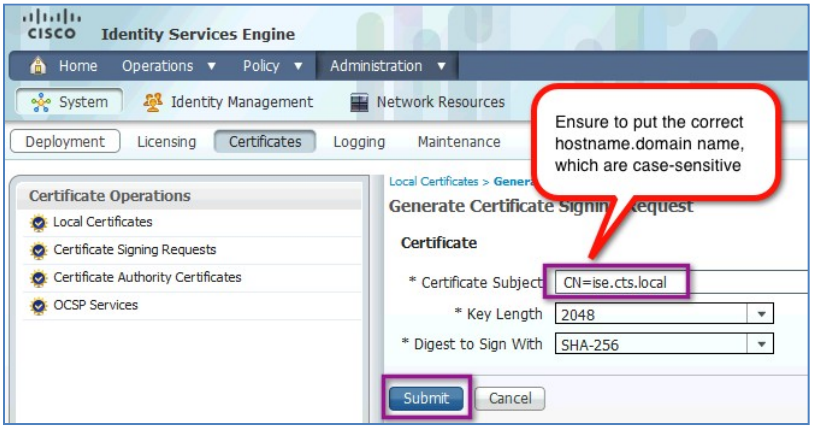


图 3. Generate Certificate Signing Request 面板

步骤 5 在 Certificate Subject 字段中输入思科 ISE 节点的完全限定域名 (FQDN)。

步骤 6 点击 **Submit** 按钮。

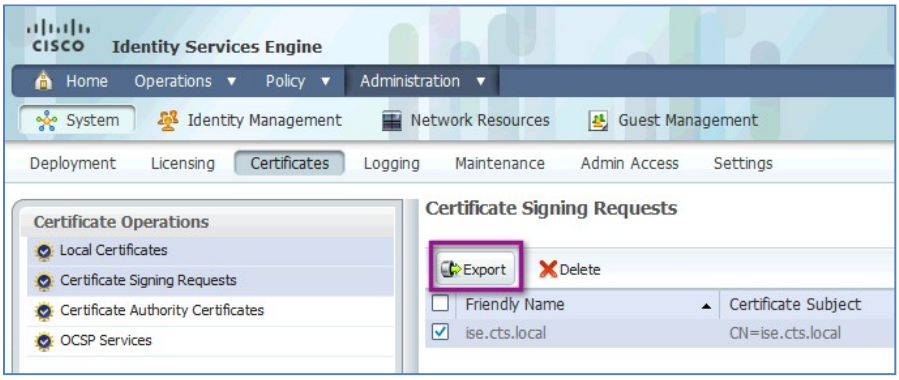


图 4.

步骤 7 点击 **Export** 链接。

步骤 8 将 .pem 文件保存在适当的位置，以便方便地进行访问。

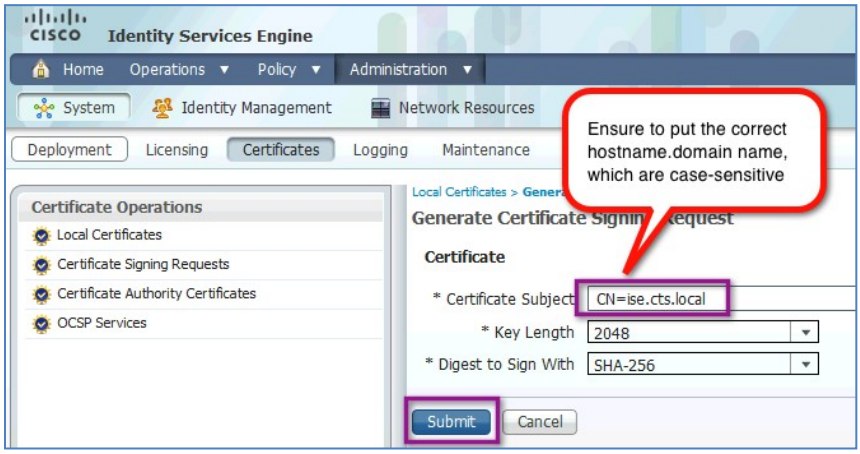


图 5. Generate Certificate Signing Request 面板

下载 CA 根证书并颁发证书

步骤 1 浏览至您的 CA。

步骤 2 点击标题为 "Download a CA certificate, certificate chain, or CRL" 的链接。

注：我们使用的是 Microsoft CA；因此，需要浏览至 http://ad.cts.local/certsrv/。根据贵组织的 CA，证书请求可能需要遵循不同的程序。使用 Microsoft CA 时，我们发现使用 Internet Explorer 体验更佳。

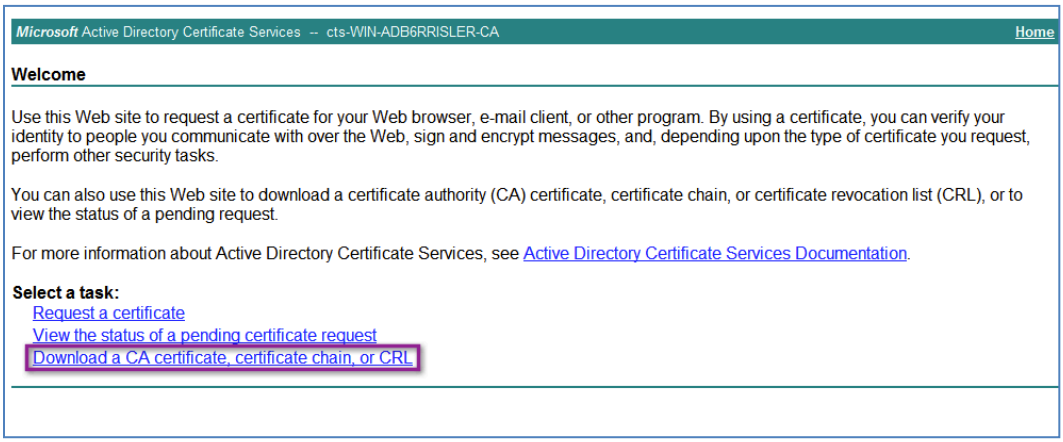


图 6. 下载 CA 证书

步骤 3 点击 Download CA certificate。

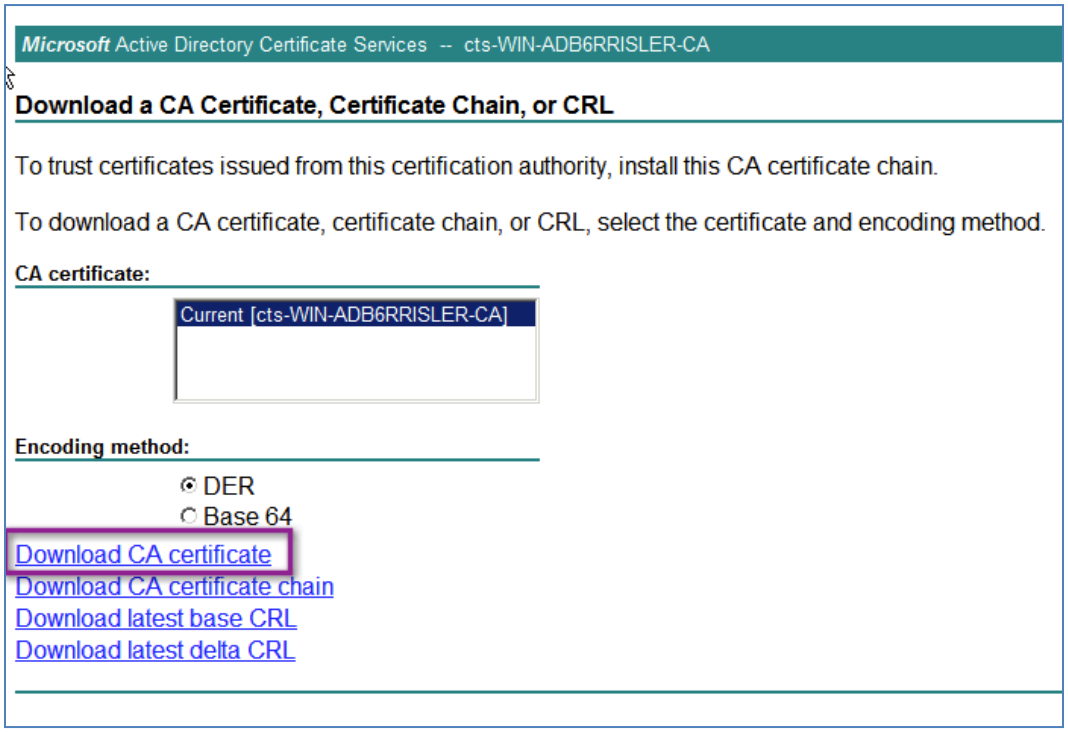


图 7. 选择证书和编码方法

步骤 4 将得到的 .cer 文件保存到适当的位置，以便方便地进行访问。

思科最佳实践：文件的命名应该独特，例如 RootCert.cer。

步骤 5 点击右上角的 Home。

步骤 6 点击 Request a certificate。

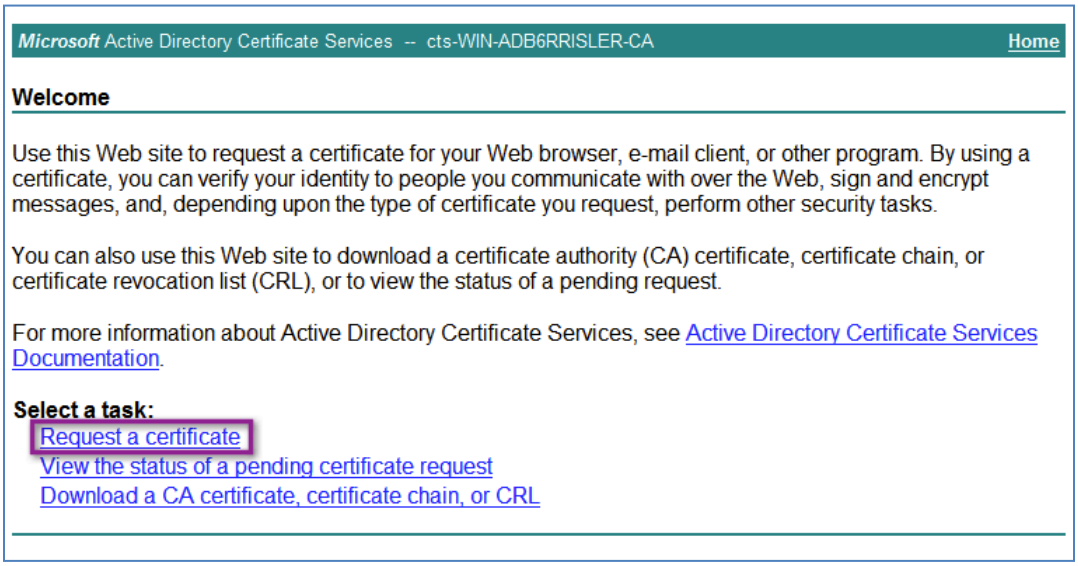


图 8. 申请证书

步骤 7 点击 advanced certificate request。

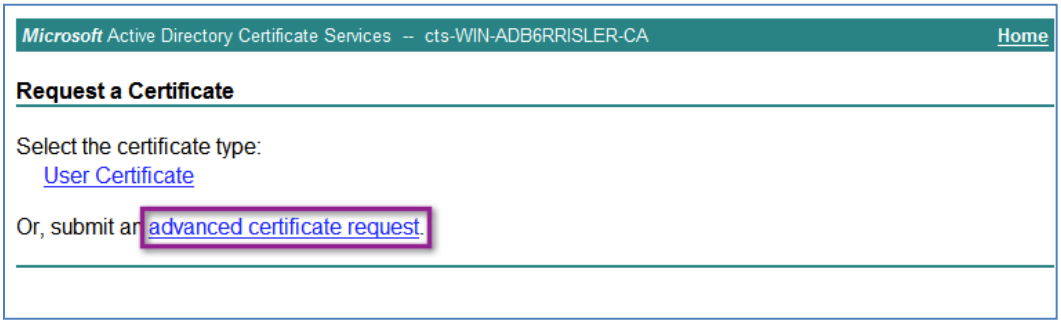


图 9. 申请高级证书

步骤 8 选择标题为 "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoder PKCS #7 file" 的选项。

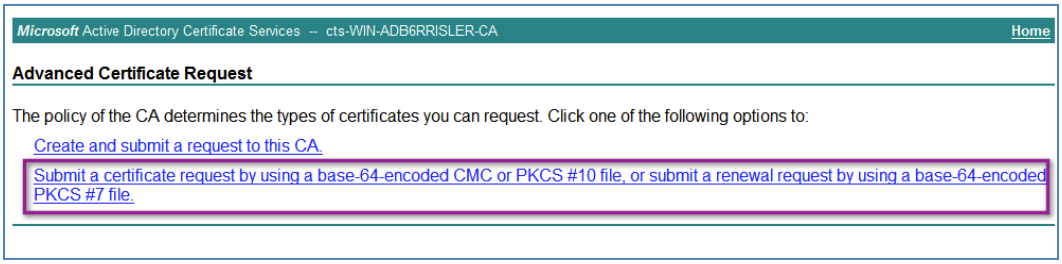


图 10. 选择证书请求选项

步骤 9 使用记事本或其他文本编辑器打开程序 2 中保存的 .pem 文件。

步骤 10 突出显示整个文件内容，然后选择 Edit → Copy。

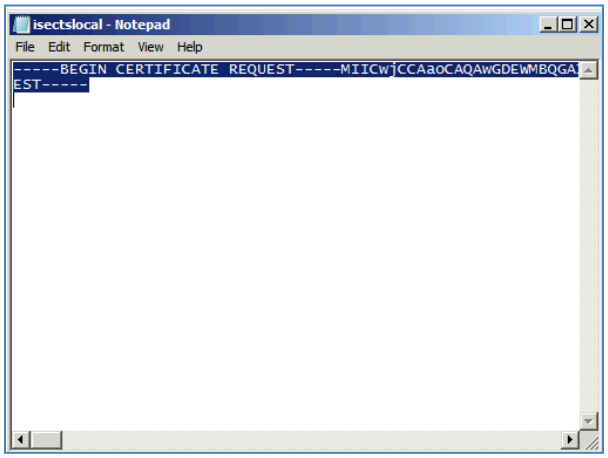


图 11. 复制证书

步骤 11 在 CA 窗口中，将证书请求 .pem 文件的内容粘贴到 Saved Request 文本框中。Certificate Template 应设置为 Web Server。

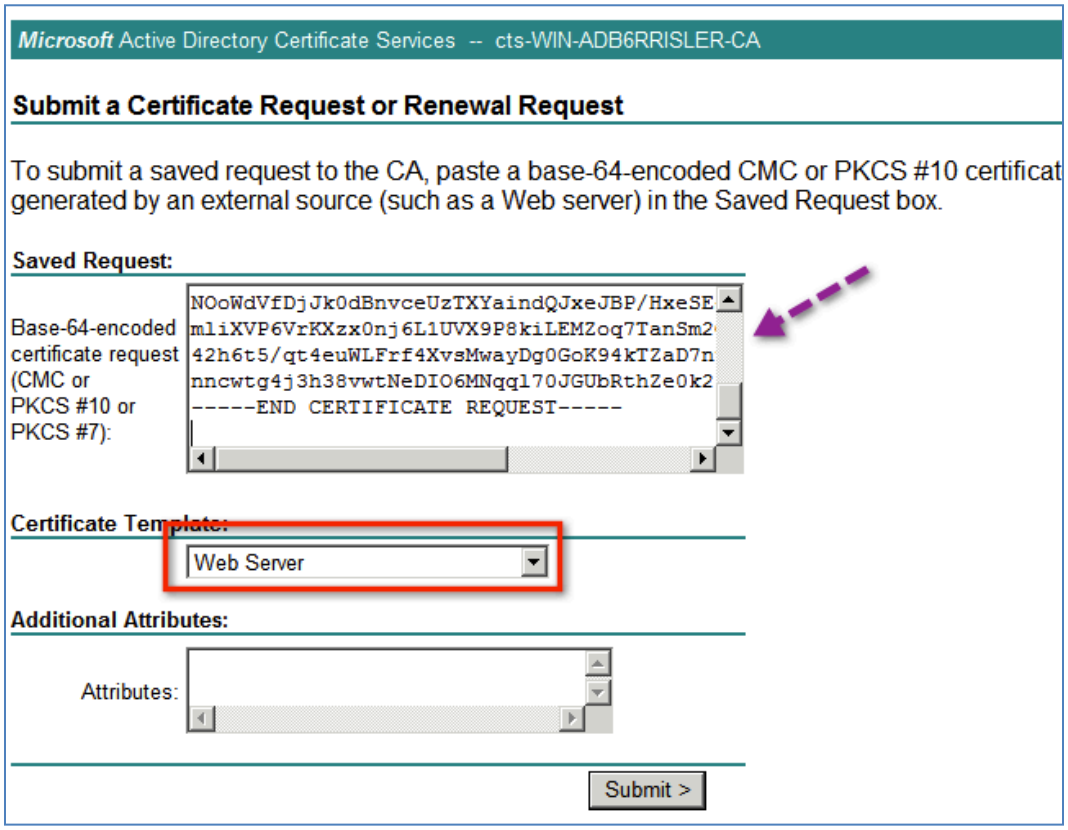


图 12. 提交证书请求

步骤 12 在思科 ISE 管理界面中，导航至 Administration → System → Certificates → Certificate Authority Certificates。

步骤 13 点击 Import。

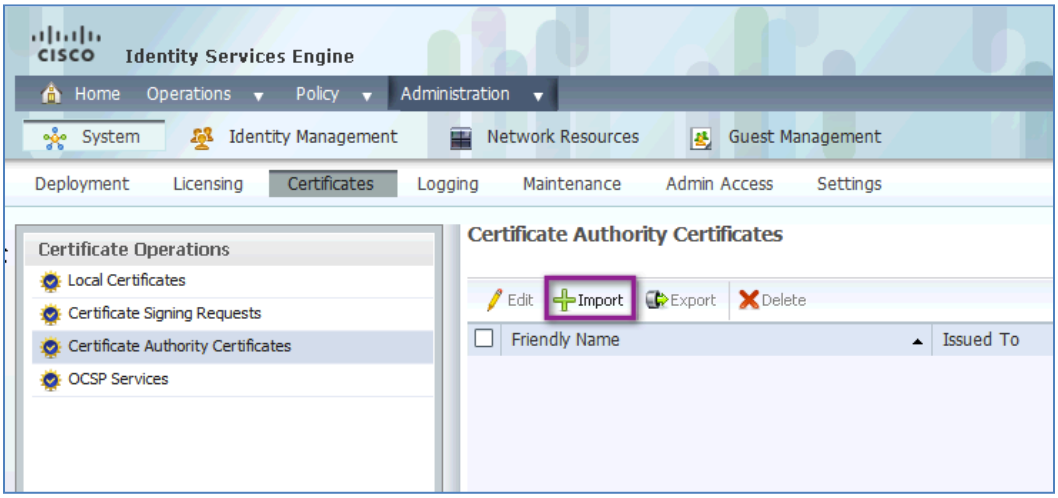


图 13. 导入证书

步骤 14 浏览找到程序 3 步骤 3 中保存的 CA 根证书。

步骤 15 选中标题为 "Trust for client authentication" 的复选框，然后选中标题为 "Enable Validation of Certificate Extensions" 的复选框。

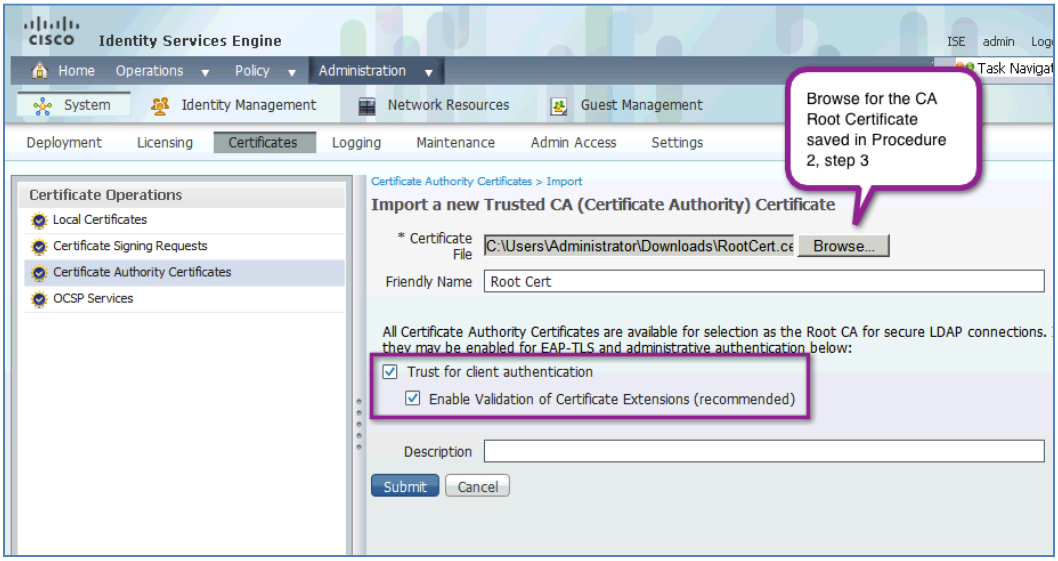


图 14. 信任 EAP-TLS

步骤 16 点击 Submit。

安装新的本地证书

现在，CA 根证书已受到信任，您可以使用 CA 颁发的证书替换自签名证书，并删除已完成的证书签名请求 (CSR)。

步骤 1 从 Administration → System → Certificates → Local Certificates，点击 Add → Bind CA Certificate。

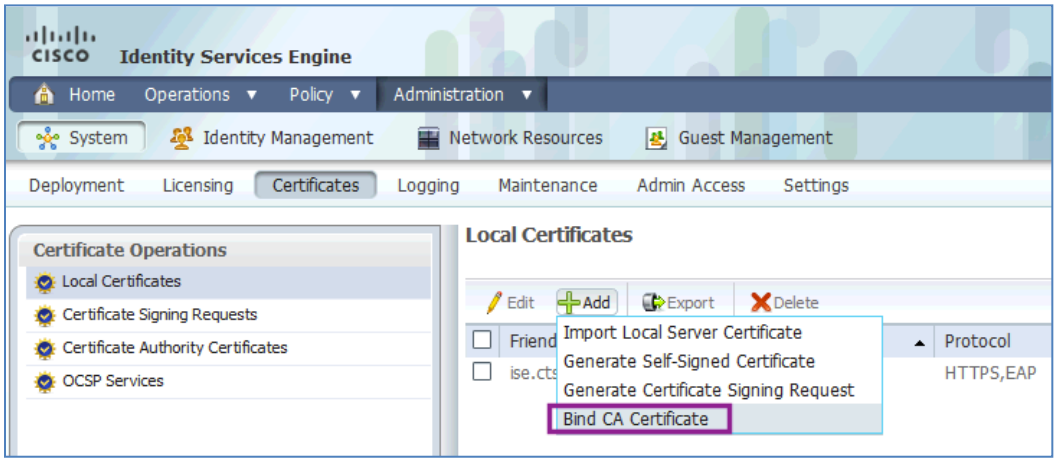


图 15. 绑定 CA 证书

步骤 2 浏览找到 CA 为思科 ISE 颁发的证书。选中 EAP 和 Management Interface 复选框。

步骤 3 点击 **Submit**。

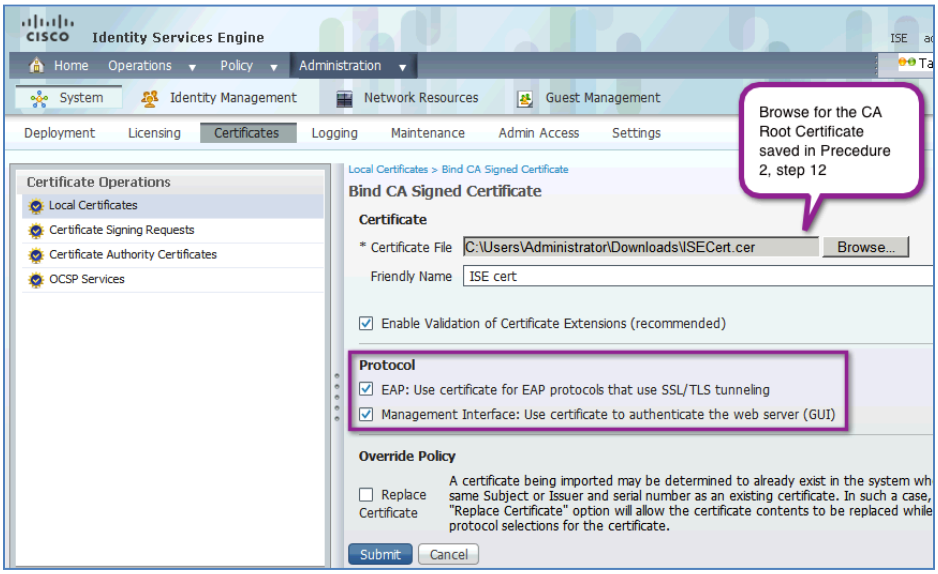


图 16. 绑定 CA 签名的证书选择

注：如果创建证书签名请求 (CSR) 时没有使用与思科 ISE 服务器相同的主机名（或没有使用相同的域名），则会收到错误消息。删除旧的 CSR 或直接更改主机名并重新启动。

清除旧的证书和 CSR

步骤 1 选中标题为 "Default self-signed server certificate" 的复选框。

步骤 2 点击 Delete。

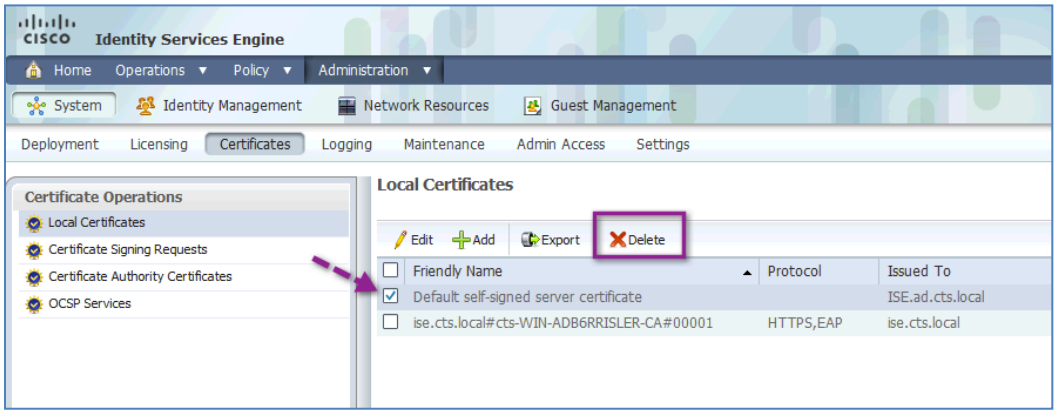


图 17. 删除旧的证书

步骤 3 点击 Certificate Signing Requests。

步骤 4 选择 CSR。

步骤 5 点击 Delete。

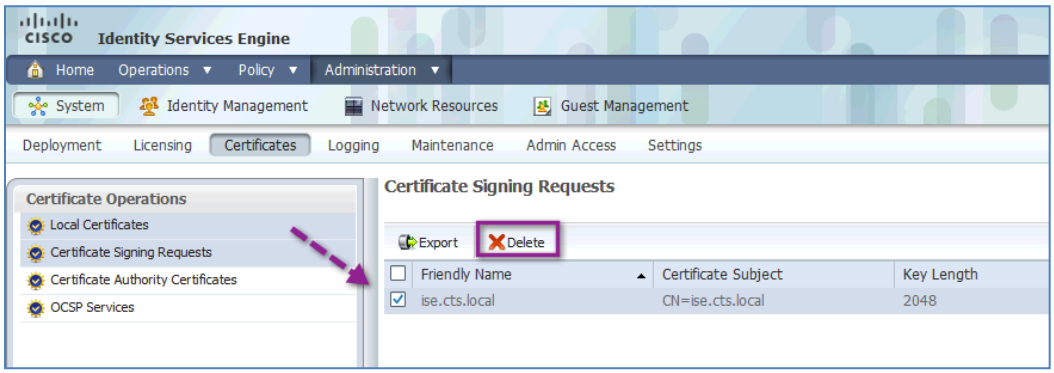


图 18. 删除旧的签名请求

添加网络设备

概述

任何交换机或无线局域网控制器 (WLC) 如果需要将 RADIUS 请求发送到思科 ISE 进行身份验证和网络客户端授权，都应添加到思科 ISE。思科 ISE 提供一台默认设备，可配置为允许任何网络设备发送 RADIUS 请求，但是使用此功能并不是一个安全的好办法。

为了提供全面的策略创建和详细的报告，建议将所有设备逐一添加到思科 ISE，并使用网络设备组 (NDG) 来组织这些网络设备。

注：思科 ISE 提供导入/导出机制，用于批量导入网络设备并将这些设备分配到相应的 NDG。有关详细说明，请参阅思科 ISE 用户手册 (http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_admin.html)。

配置网络设备组

如果使用得当，NDG 是功能很强大的工具。思科 ISE 在进行策略决策时能够使用任意数量的属性。NDG 成员就是可用作策略条件的属性之一。例如，可以为交换机创建一个 NDG，再为 VPN 设备创建一个，然后为 WLC 创建第三个组。

思科最佳实践：至少要按照设备类型和位置创建相应的 NDG。

步骤 1　转至 Administration → Network Resource → Network Device Groups。

默认情况下，最高一级的 NDG 类型有两个：All Device Types 和 All Locations。大多数部署都可以从这两个类型开始。您的部署可能需要创建多个位置的子组。其可能性几近无限（请参阅随后的层次结构示例）

组采用分层结构。以组结构 "All Locations → North America → US → SJC → Building M → 1st Floor" 为例，您可以在策略中使用组层次结构的任意级别。换言之，您可以在策略中选择 "US" 并获得 "US" 下面每个组中的每台设备。

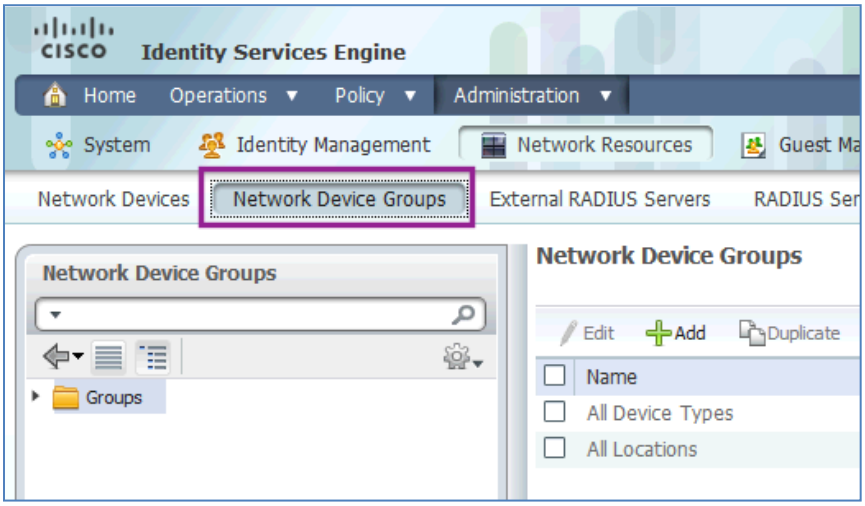


图 19. 网络设备组

步骤 2 选择 Network Devices，点击 Add。

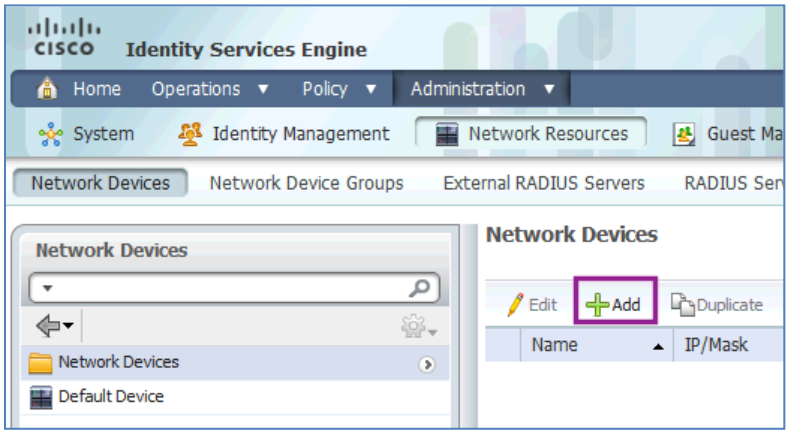


图 20. 添加网络设备

步骤 3 在 Name 字段中输入名称 **Switch**，然后点击 Submit。

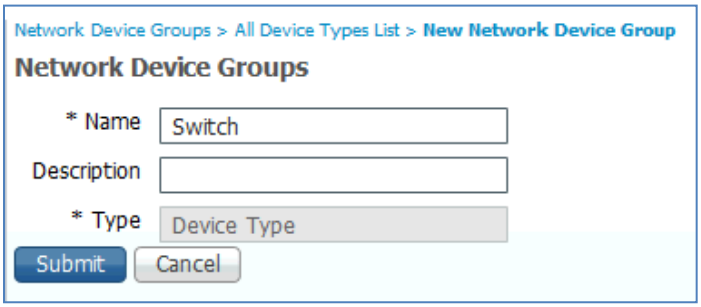


图 21. 添加交换机

步骤 4 重复此过程，创建所需的 NDG 层次结构。图 24 所示为层次结构示例。

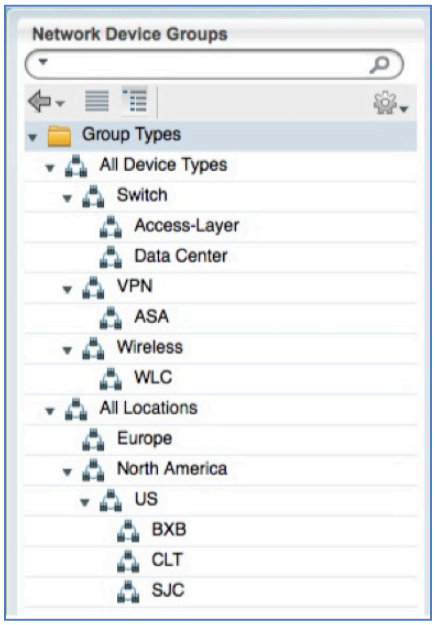


图 22. 组类型

添加网络设备

步骤 1 转至 Administration → Network Resources → Network Devices，然后点击 Add。

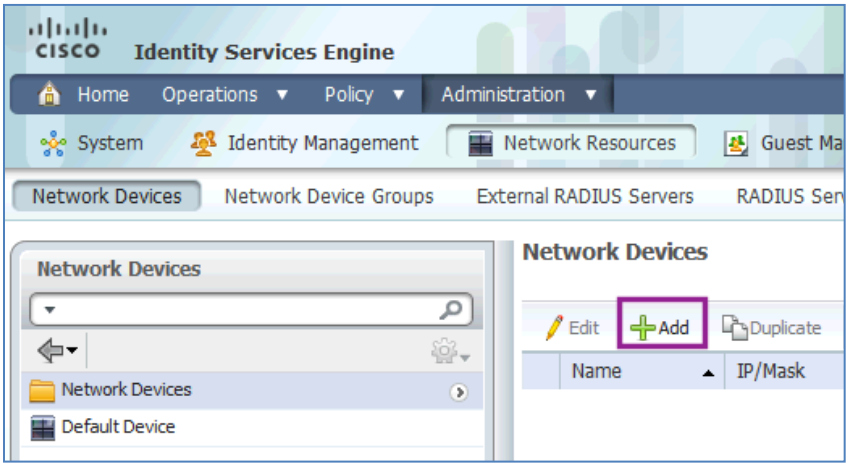


图 23. 网络设备

步骤 2 填写 Name、IP Address 和 Network Device Group 字段。

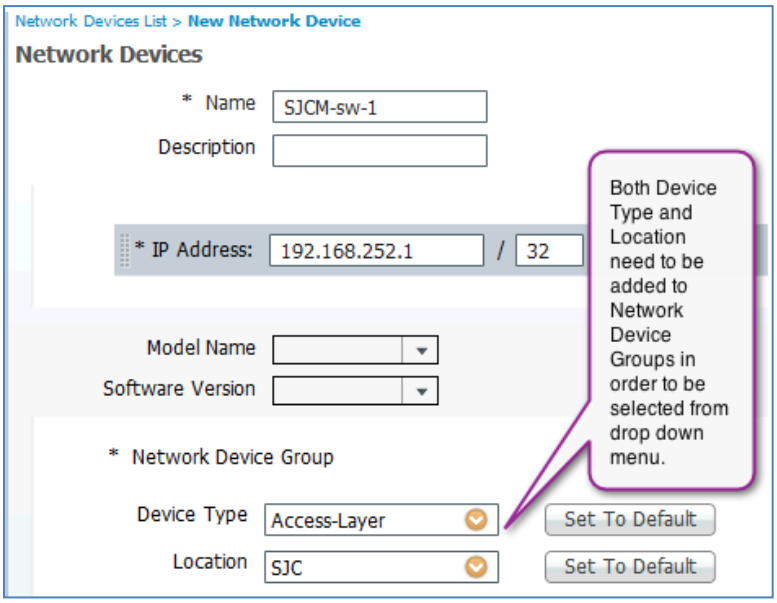


图 24. 网络设备详细信息

步骤 3 对所有网络设备（也称为“策略实施点”）重复此步骤。

注：如果是批量管理，可通过 CSV 文件导入网络设备。有关详细信息，请参阅思科 ISE 用户手册 (http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_admin.html)。

表 2. 网络设备

项	目的
常规设置	
名称	请使用便于日后进行区分的名称。该名称将显示于所有监控、控制面板和报告中。
描述	可选
IP 地址	必须与在交换机配置部分所选的 RADIUS 通信源接口相匹配。最佳实践是使用环回接口进行管理。
型号名称	可选
软件版本	可选
网络设备组	
位置	请尽量具体一些。
设备类型	请尽量具体一些。
身份验证设置	
协议	将预先填充为 RADIUS。
共享密钥	必须与交换机上配置的 RADIUS 密钥相匹配。
SNMP 设置（用于设备分析）	
SNMP 版本	请选择您的组织中使用的版本。
SNMP RO 社区	SNMP 仅用于设备分析用途。思科 ISE 将探测交换机，查找思科发现协议表和链路层发现协议 (LLDP) 表的内容。
SNMP 用户名	用于 SNMPv3 - 必须与交换机上的配置相匹配。
安全级别	用于 SNMPv3 - 必须与交换机上的配置相匹配。
身份验证协议	用于 SNMPv3 - 必须与交换机上的配置相匹配。
隐私协议	用于 SNMPv3 - 必须与交换机上的配置相匹配。
轮询间隔	建议不要更改默认轮询间隔：3,600 秒

项	目的
链路陷阱查询	将思科 ISE 配置为接受来自交换机的 Linkup 和 Linkdown SNMP 陷阱。保留此复选框被选中。
MAC 陷阱查询	将思科 ISE 配置为接受来自交换机的 mac-address-table 类型的陷阱。保留此复选框被选中。
安全组访问 (SGA)：在本部署指南的此阶段无需使用。我们将在 SGA 部分重新访问此项。	
设备配置部署：在本部署指南的此阶段无需使用。我们将在 SGA 部分重新访问此项。	

设备分析

概述

思科 ISE 分析器负责 ISE 平台上的终端检测和分类。它使用一系列探针（传感器）来收集有关终端的属性，并使用基于策略的机制来评估属性，以便将终端与预定义的配置文件相匹配。随后，分析器的收集和分类结果将用作身份验证和授权策略中的条件。分析的分类结果可以用来调用其他授权结果。有关探针的更多详情，请参阅*操作指南-30-分析设计指南*。

下图举例说明基于分析的有区别的设备策略。

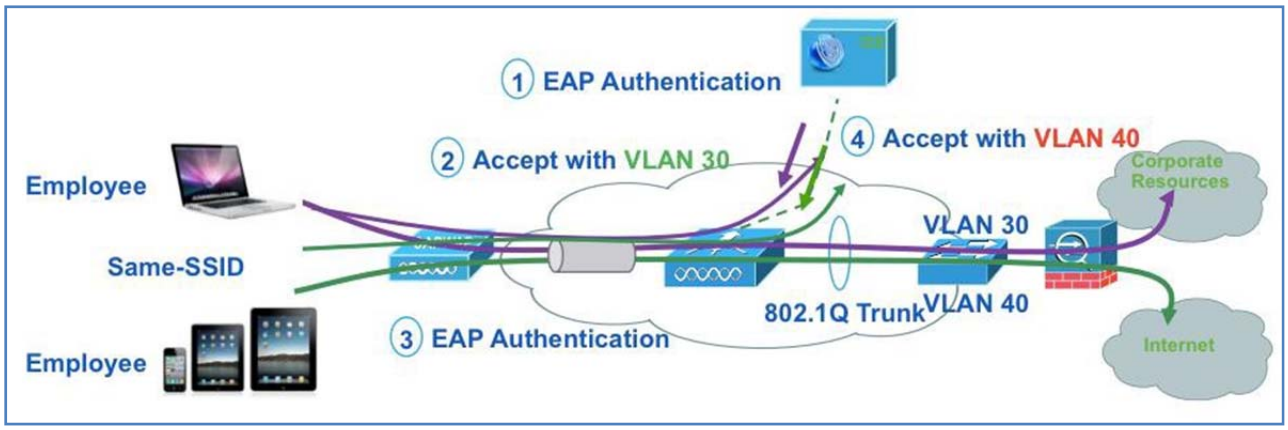


图 25. 基于分析的设备策略

EAP 身份验证完成后，使用相同 SSID 的用户可与不同的有线 VLAN 接口相关联。

- 使用企业手提电脑的员工，其 AD 用户 ID 被分配到 VLAN 30，可获得完全访问网络的权限
- 使用个人 iPad/iPhone 的员工，其 AD 用户 ID 被分配到 VLAN 40，只能访问互联网

ISE 配置 - 启用设备分析探针

在此阶段，我们将在思科 ISE 设备上启用分析探针。在分布式部署中，通常会在所有策略服务节点（PSN，有时也称为策略决策点或 PDP）上启用分析探针。具体要启用何种探针（以及在何处启用）可能比较复杂，应该在概要设计过程中解决。

注：本指南不介绍如何启用 NetFlow 探针。NetFlow 是一款强大的工具，但是否实施该工具必须经过慎重考虑。在某些思科安全访问实施中，NetFlow 非常关键。但是，NetFlow 的一个重要方面是确定要发送哪些基础设施数据。

要启用分析探针，请执行以下步骤：

步骤 1 导航至 Administration > System > Deployment。
步骤 2 选择策略服务节点。

此节点可以是单个的思科 ISE 节点，如图 26 所示。如果您的思科安全访问部署是分布式部署，应选择为策略服务配置的节点之一。对部署中的每个 PSN 重复上述步骤。

步骤 3 选中 **Enable Session Services**。

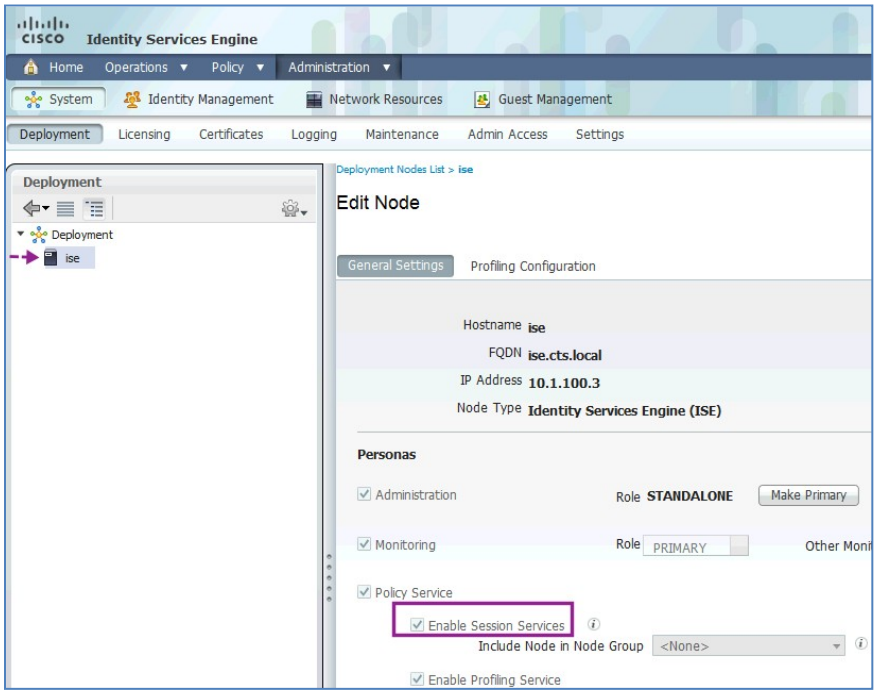


图 26. 策略服务节点

步骤 4 步骤 4 点击 Profiling Configuration 选项卡。

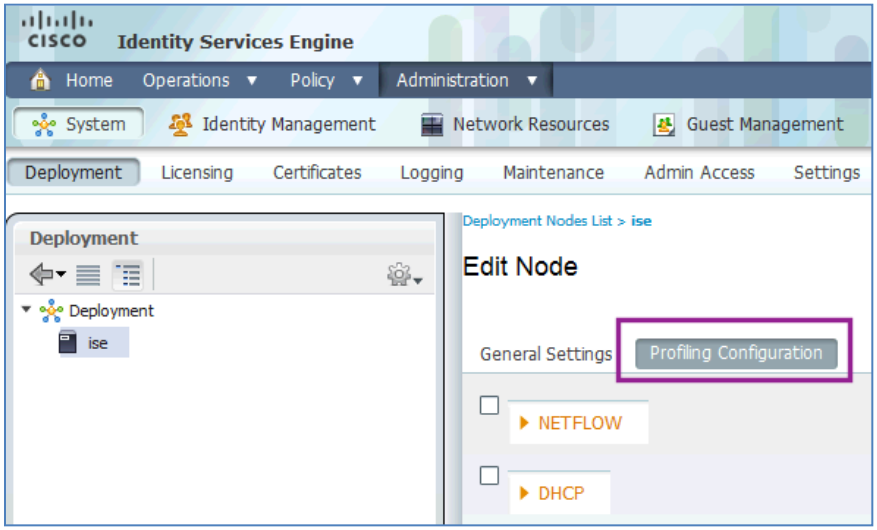


图 27. 分析配置

步骤 5 启用 DHCP 所对应的复选框。

这是 DHCP IP Helper 探针。它侦听从交换机或其他第 3 层设备上配置的 DHCP IP Helper 向它转发的数据包。DHCP IP Helper 探针只侦听从 DHCP 客户端到服务器的流量（DHCPDISCOVER 和 DHCPREQUEST）。

步骤 6 在特定接口或所有接口上启用此探针。

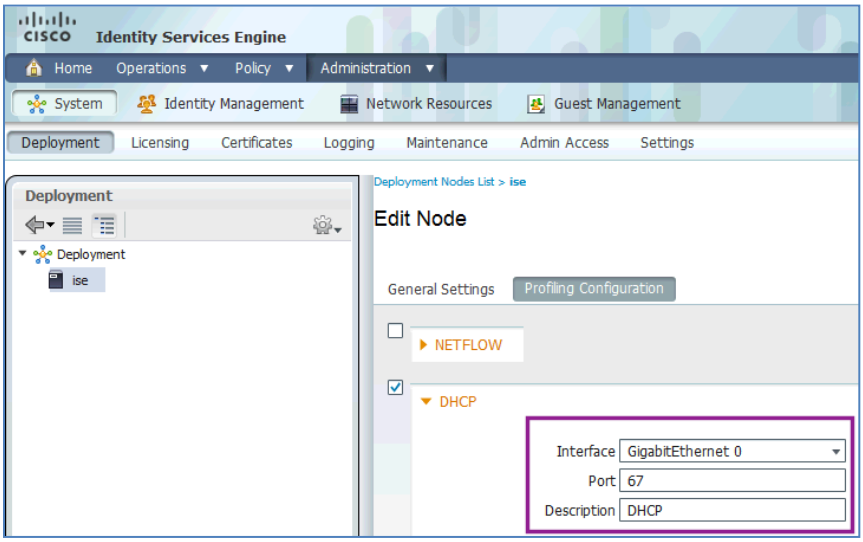


图 28. 启用 DHCP

步骤 7 启用 DHCPSPAN 所对应的复选框。

DHCP Span 探针侦听从交换机上配置的交换机端口分析器 (SPAN) 会话向它转发的数据包。此探针会侦听所有 DHCP 流量。

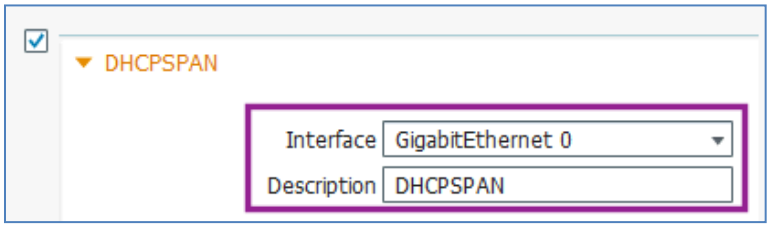


图 29. 启用 DHCPPSAN

当交换机端口被配置为 SPAN 目标时，该端口不能再正常工作。连接到 SPAN 目标端口的接口应为“混合模式”，表示该接口应该捕获进入该端口的所有流量，但不会响应定向通信。

了解这些之后，我们建议将一个或多个思科 ISE 服务器接口设置为适用于 DHCPSPAN 和 HTTP 探针的混合模式。在本指南中，我们将 GigabitEthernet 1 接口专用于 SPAN 目标。

注：使用思科 ISE 上除 GigabitEthernet 0 以外的接口时，应进入 CLI 并在接口配置模式下输入 **no shutdown** 启用该接口。有关交换机配置，请参阅“添加网络设备”程序。要在交换机端口上配置 SPAN（监控会话），请参阅“在交换机上配置 SPAN 会话”程序。

步骤 8 启用 HTTP 所对应的复选框。

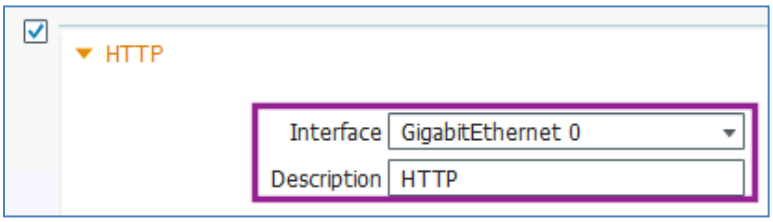


图 30. 启用 HTTP

HTTP Span 探针侦听指定接口上的 HTTP 数据包并解析他们，从而为终端补充 HTTP 属性。HTTP 探针捕获从终端发往端口 80 的流量，检测 HTTP 请求中存在哪些用户代理和其他 HTTP 属性。

在识别移动设备方面，HTTP 数据是重要因素之一。HTTP 的使用还需要考虑一些设计上的因素，而且应该在概要设计过程中考虑。

步骤 9 启用 RADIUS 所对应的复选框。

RADIUS 探针根据 RADIUS 信息帮助检测终端。此外，它还用于接收来自思科 IOS 路由器和 WLC 中的设备传感器的分析数据。

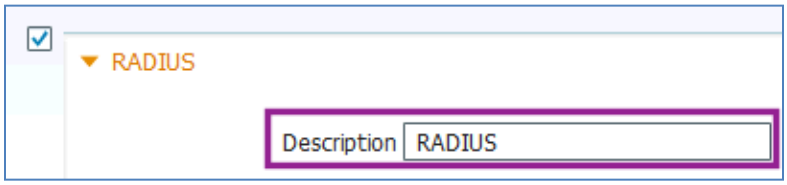


图 31. 启用 RADIUS

表 3 列出了已知由 RADIUS 探针收集的属性。RADIUS 探针根据 RADIUS 信息帮助检测终端。

表 3. RADIUS 探针收集的属性

User-Name	Framed-IP-Address	Acct-Session-Time
NAS-IP Address	Calling-Station-ID	Acct-Terminate-Cause
NAS-Port	Acct-Session-ID	

注：RADIUS 探针可能还会触发 DNS 和 SNMP 查询收集事件（如果已启用）。

步骤 10 启用 DNS 所对应的复选框。

使用思科 ISE 部署中的 DNS 探针，分析器能够查找终端并获取该终端的完全限定域名 (FQDN)。

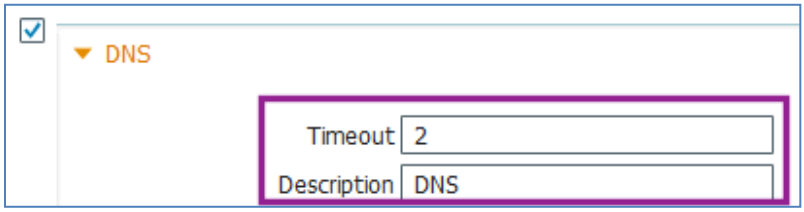


图 32. 启用 DNS

只有当 DHCP、RADIUS、 HTTP 和 SNMP 探针检测到的终端包含表 4 中列出的相应属性时，才会完成反向 DNS 查找。因此，对于 DNS 查找来说，除 DNS 探针之外，至少还需要启用表 4 中所列的一个探针。

表 4. 需要启用的探针

需要启用的探针
DHCP IP Helper、DHCP Span - "dhcp-requested-address"
RADIUS 探针 – "Framed-IP-Address"
SNMP 探针 – "cdpCacheAddress"
HTTP 探针 – “源 IP”

步骤 11 启用 SNMPQUERY 所对应的复选框。

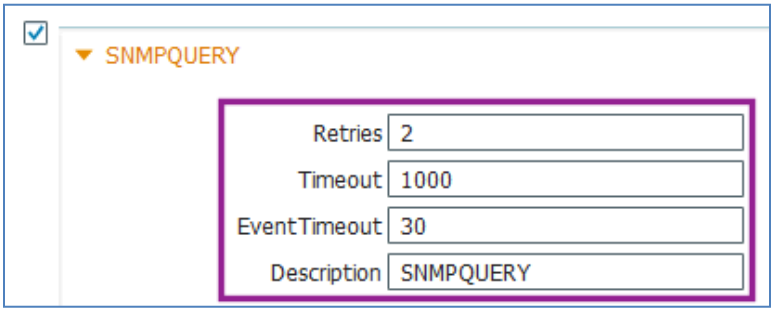


图 33. 启用 SNMPQUERY

注：在网络设备上配置 SNMP 设置时，还需要确保网络设备的所有端口上均启用了思科发现协议。如果在其中任意端口上禁用思科发现协议，您可能会因为缺少有关所有已连接终端的思科发现协议信息而无法进行正确的分析。

SNMPQuery 探针按照配置的轮询间隔轮询所有启用 SNMP 的网络设备。此功能需要完成“添加网络设备”一节中介绍的 SNMP 参数配置。

SNMPQuery 探针查询以下 MIBS：

- System
- cdpCacheEntry
- cLApEntry（如果设备是 WLC）
- cldcClientEntry（如果设备是 WLC）

LinkUp/MAC 通知/RADIUS 计费开始事件查询：

- 接口数据（ifIndex、ifDesc 等）
- 端口和 VLAN 数据
- 会话数据（如果接口类型是以太网接口）
- 思科发现协议数据（如果设备是思科设备）

在分布式部署中，NAD 轮询分布于已启用的 SNMP 查询探针中。

注：SNMPTrap 触发的查询进入与 SNMP 查询探针相同的节点的队列中。如果未启用本地 SNMP 查询探针，则会丢弃这些查询。

步骤 12 启用 SNMPTRAP 所对应的复选框。

SNMP 陷阱能够接收来自经过配置且支持 MAC 通知、Linkup、Linkdown 和通知的 NAD 的信息。要让 SNMPTrap 发挥全部功能，还必须启用 SNMPQuery 探针。SNMPTrap 探针能够在端口连接或中断以及终端与您的网络断开连接或进行连接时接收来自特定 NAD 的信息。要让此功能正常运行，您必须将 NAD 配置为发送 SNMP 陷阱。从 SNMP 陷阱接收的信息不会在思科 ISE 中创建新的终端，但可用于分析。

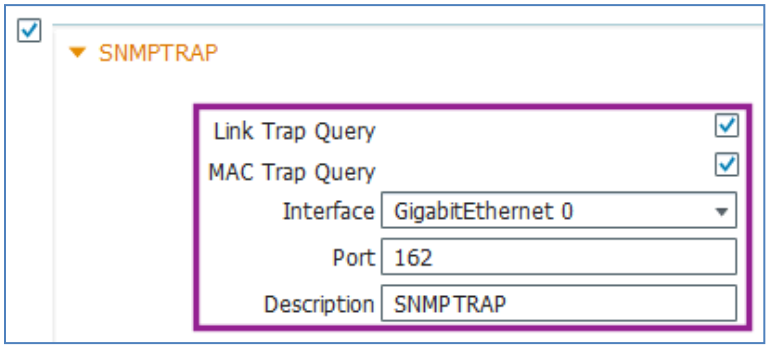


图 34. 启用 SNMPTRAP

注：支持 SNMP 通知。

步骤 13 确保已启用 Link Trap Query 和 MAC Trap Query 选项，然后点击 Save。

注：如果使用 VMware 进行分析，请参阅《ISE 基本配置操作指南》。

附录 A

思科安全访问系统

- http://www.cisco.com/en/US/products/ps11640/products_implementation_design_guides_list.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

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