Cisco TrustSec 操作指南：监控模式

文档版本 3.0

2012 年 8 月 6 日

目录

简介

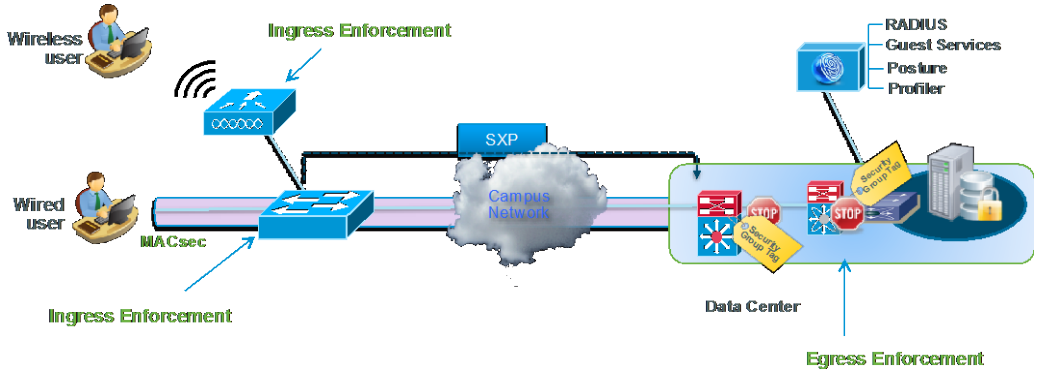
什么是 TrustSec 系统?

Cisco TrustSec® 是 Cisco SecureX Architecture™ 的一个核心组件，是一种智能访问控制解决方案。TrustSec 通过全面了解正在整个网络基础设施进行连接的用户和设备并控制其可以访问的内容和位置来降低安全风险。

TrustSec 构建于您现有的身份感知访问层基础设施（交换机、无线控制器等）之上。该解决方案及其内部所有组件都已作为一个集成系统经过了彻底的检查和严格的测试。

除了结合 IEEE 802.1X 与 VLAN 控制等基于标准的身份和实施模式外，TrustSec 系统还包括高级身份和实施功能，例如灵活的身份认证、可下载的访问控制列表 (dACL)、安全组标记 (SGT)、设备分析、安全状态评估等。

图 1：TrustSec 架构概览

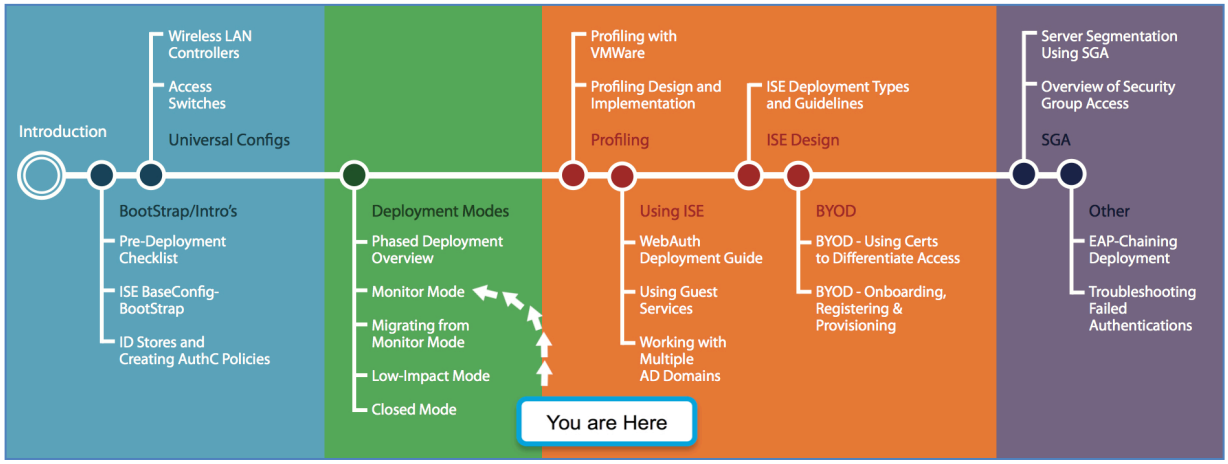


关于 TrustSec 操作指南

本系列操作指南文档由 TrustSec 团队编制，旨在介绍 TrustSec 部署的最佳实践。本系列文档相辅相成，引导读者成功实施 TrustSec 系统。您可以使用这些文档按照规定的路径部署整个系统，也可以只选择满足您特定需求的单独的使用案例。

此系列的每个指南都随附地铁式“定位”地图，帮助您确定文档所论述的阶段并准确描述您在 TrustSec 部署流程中所处的位置（图 2）。

图 2：操作指南导航图



“TrustSec 认证”意味着什么?

每个 TrustSec 版本（例如，TrustSec 版本 2.0、版本 2.1 等）都是通过认证的设计或架构。组成架构的所有技术都已通过彻底的架构设计开发和实验室测试。操作指南要获得“TrustSec 认证”标记，其文档中论述的所有元素都必须符合以下条件：

- 设计中包含的产品必须为稳定版本。
- 系统中组件的部署、操作和管理必须表现为可重复的流程。
- 设计中使用的所有配置和产品均必须作为集成解决方案经过充分测试。

可能有许多功能有益于您的部署，但如果经过测试的解决方案中不包括它们，则不会标记为“TrustSec 认证”。TrustSec 团队会努力为这些文档提供定期更新，以及时包括新功能，并集成到 TrustSec 测试计划、试点部署和系统修订中。（如 TrustSec 2.2 认证）。

此外，许多功能和方案虽已经过测试，但并不是最佳实践，因此不包括在这些文档中。例如，某些 IEEE 802.1X 计时器和本地网络身份验证功能不包含在内。

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，有助于确保成功部署项目。

监控模式

监控模式概述

通过采用监控模式，企业能够在整个有线基础架构中启用身份验证，不会对有线用户或设备产生影响。您可以将其看做一种“审核模式”。在用于验证的日志记录数据的帮助下，管理员使用监控模式帮助确保所有设备都使用 802.1X 或 MAC 身份验证绕行正确进行身份验证。如果设备配置错误或缺少 802.1X 客户端，则访问会被拒绝并直接记录。部署监控模式后，多数企业会吃惊地发现，有些设备连接至网络而自己之前并未察觉。

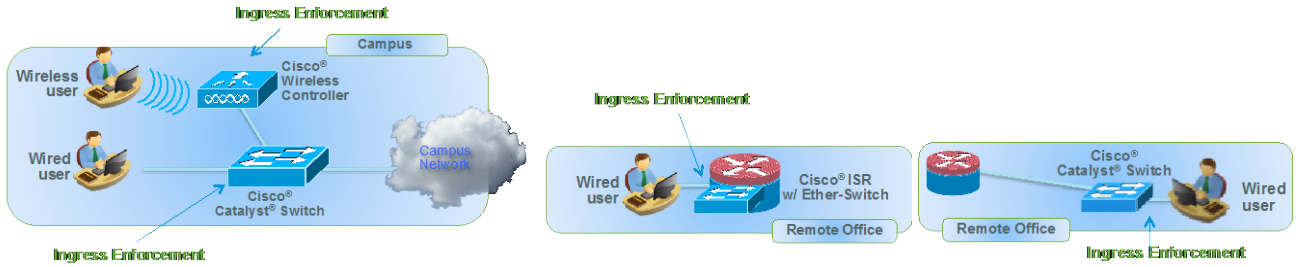
采用 802.1X 的无线环境为二进制（802.1X 专为此而设计），因此如果用户无法进行身份验证，则不能访问无线网络。多数用户能够接受此行为，并且愿意寻找有物理网络连接（有线连接）的位置来实现网络访问。尽管最终用户大多能够接受无法加入无线环境的情况，但如果出现无法访问有线网络端口的情形，他们会变得不太理解这种情况。

注：无线网络无法实施监控模式。因此，我们会在低影响模式阶段介绍无线方式。

监控模式是一个过程，而不只是交换机上的一个命令。在此过程中，系统会在您的思科基础架构上综合使用 RADIUS 记帐数据包、开放式身份验证和多重身份验证功能，同时结合设备分析，让管理员了解正在连接至网络的用户和设备及其接入网络的位置。如果由于种类配置错误，设备应该却无法进行身份验证，那么管理员会得到通知并进行更正，不会拒绝用户访问网络。

此操作指南涵盖园区和远程办公室的有线访问（图 3）。如前所述，不存在采用无线访问的监控模式的概念，因此，在此指南中将不讨论无线访问。

图 3 - 园区和远程办公室中的有线场景



在部署之前了解流程

检查 Cisco® 身份服务引擎 (ISE) 默认配置或在思科 ISE 中进行任何新配置之前，您必须充分了解网络访问的功能和网络访问处理流程，这一点非常重要。

RADIUS 控制的网络访问采用传统的身份验证、授权和记帐 (AAA) 模式。

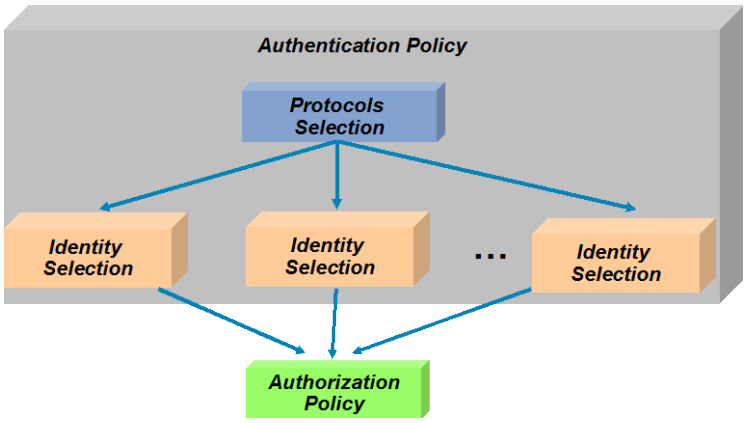
简而言之，身份验证就是验证凭证是否有效，就是这样。身份验证可以用于验证客户端证书的有效性，也可以用于确认用户名/密码组合是否有效。但是，身份验证自身无法提供任何访问权限。

授权即确定通过身份验证的用户或设备的访问级别。其中会进行大量的网络访问控制工作。

思科 ISE 图形用户界面逻辑分出了身份验证和授权策略。身份验证策略会根据传入的身份验证请求决定要检查的身份库。例如，来自 VPN 的身份验证请求可能会配置为通过检查一次性密码 (OTP) 服务器对凭证进行验证。同时，使用相同的思科 ISE 安装，来自思科无线 LAN 控制器的身份验证请求可能会使系统使用 Active-Directory 验证凭证。思科 ISE 能够提供非常强大、灵活的身份验证策略。

如图 4 所述，身份验证策略会将传入协议与配置的规则进行比较，选择分配的身份库，然后交给授权策略接管。

图 4 身份验证策略

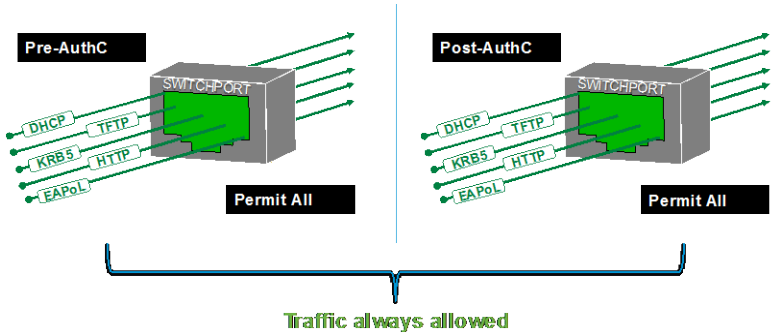


ISE 部署

部署策略

监控模式是一种部署战略，无论身份验证状态如何均会提供完全访问权限（图 5）。在每台适用设备上配置身份验证时，思科 ISE 会显示哪些设备身份验证成功，哪些设备身份验证失败。此操作指南仅包含适用于 ISE 的配置。对于交换机端口配置，请参阅《TrustSec 操作指南：全局交换机配置》。

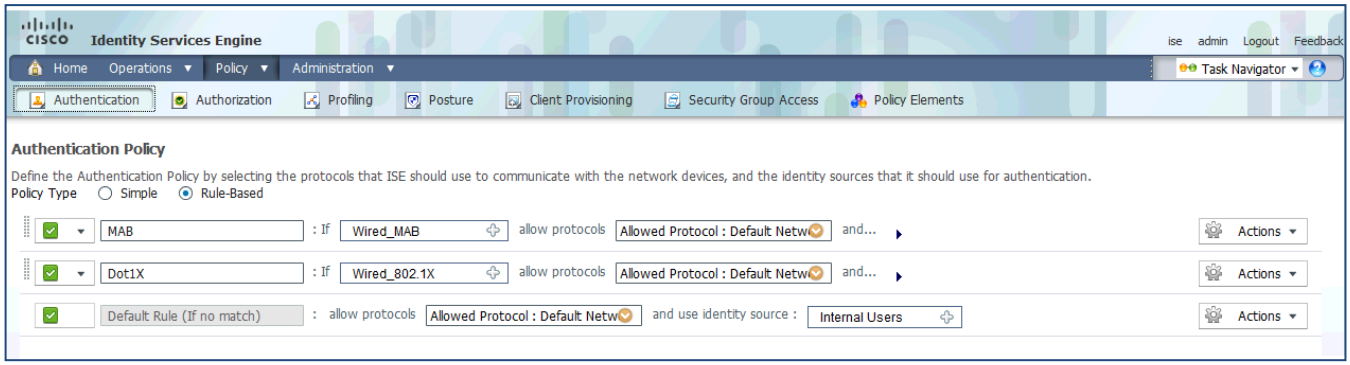
图 5 监控模式端口行为



程序 1　检查默认思科 ISE 身份验证策略

步骤 1　导航至 Policy → Authentication（图 6）。

图 6 添加身份验证策略



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。

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。

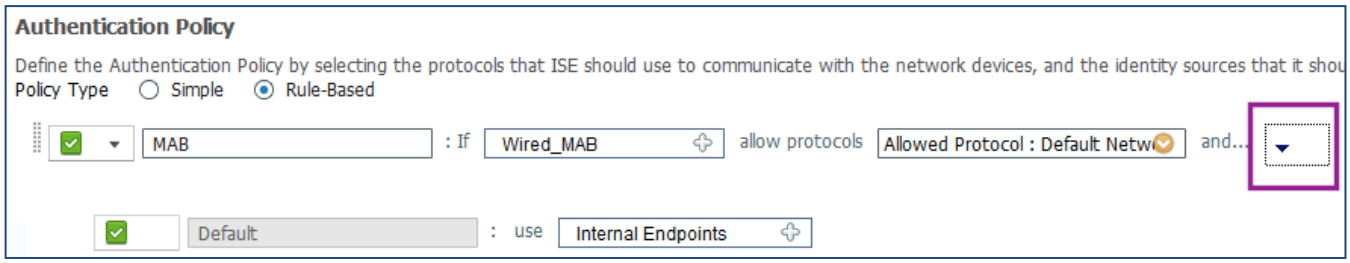
思科 ISE 策略采用逻辑 IF-THEN 格式。请注意显示为 Wired_MAB 的“选择器”前面的 IF。此行说明：“如果 RADIUS 请求是 Wired_MAB，则允许使用默认网络协议。”例如：

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

步骤 2　在图 7 中，请注意黑色下拉三角形（其概览见图 7）。

步骤 3　点击下图标记出来的三角形。

图 7：添加身份验证策略



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“内部端点”数据存储。内部端点数据存储是 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。

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，然后在内部端点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
```

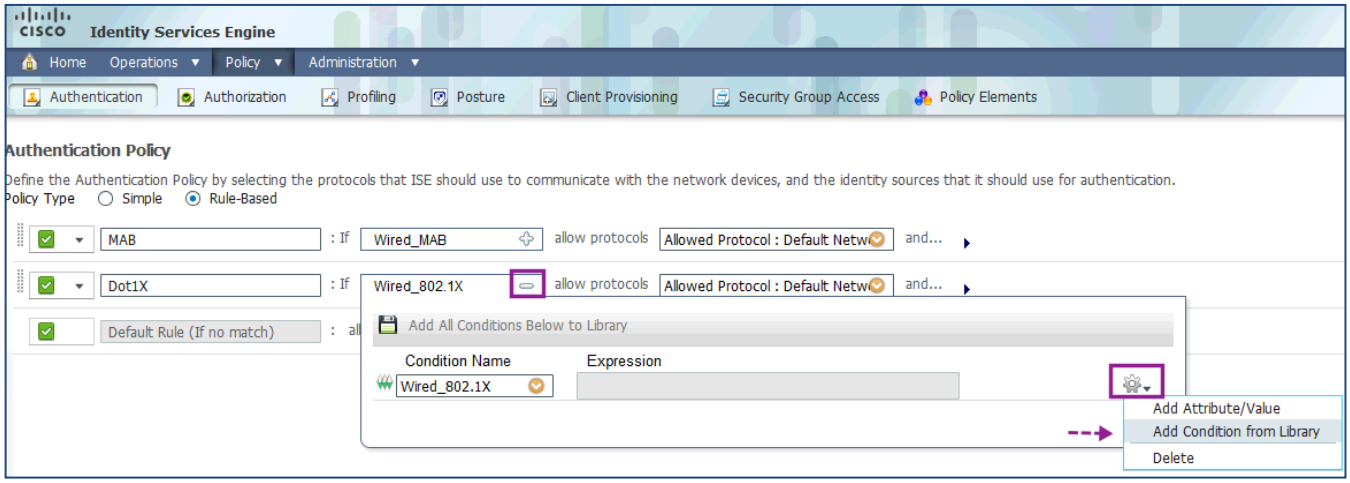
注：Wired_MAB 是预构建条件，用来匹配 RADIUS 属性：**service-type = call-check** 和 **nas-port-type = ethernet**。

程序 2　启用无线身份验证

步骤 1　导航至 Policy → Authentication。

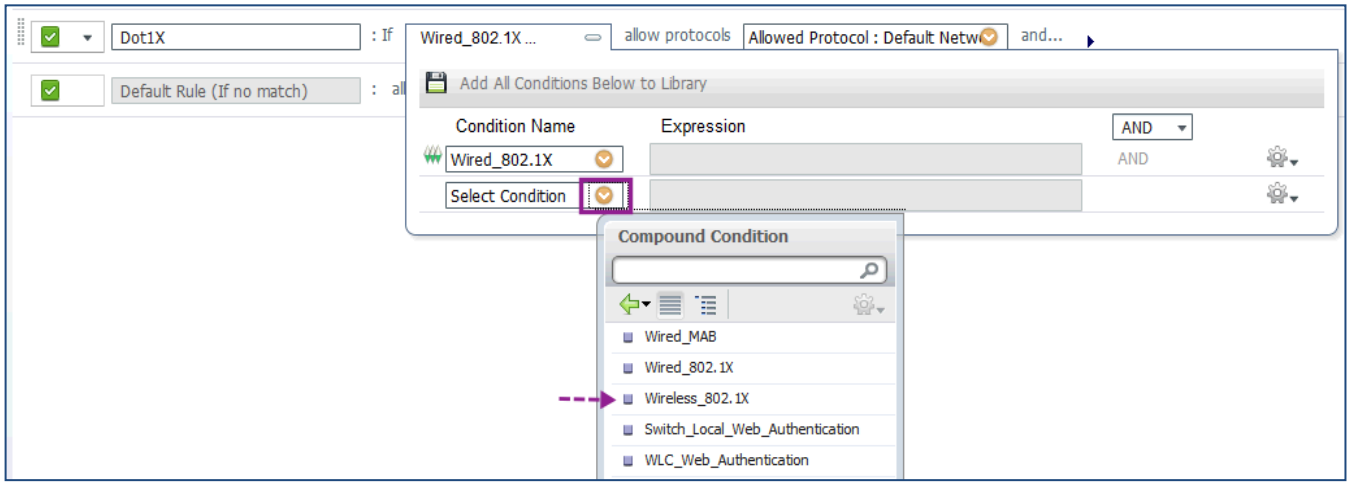
步骤 2　展开 Dot1X 规则的 IF 条件，并选择 Add Condition from Library（图 8）。

图 8 添加身份验证策略



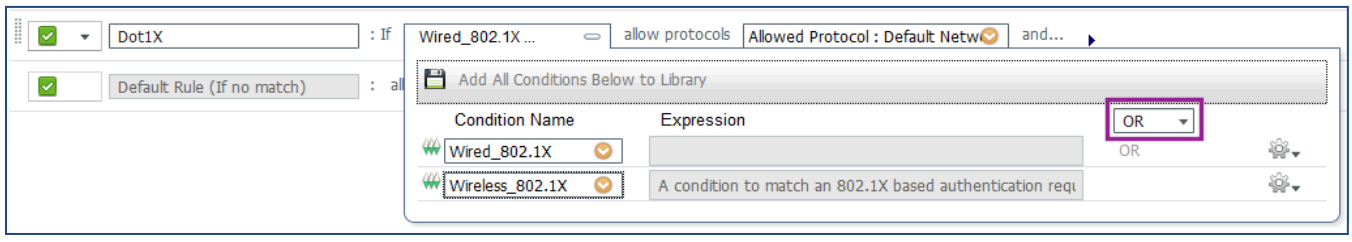
步骤 3　从 Select Condition 下拉菜单，转至 Compound Condition → Wireless_802.1X（图 9）。

图 9 选择条件



步骤 4　确保运算符指定为 OR 而不是 AND（图 10）。

图 10 选择运算符



步骤 5　保存设置。

程序 3　更改身份库

如果采用预配置规则，MAB 会使用内部端点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。

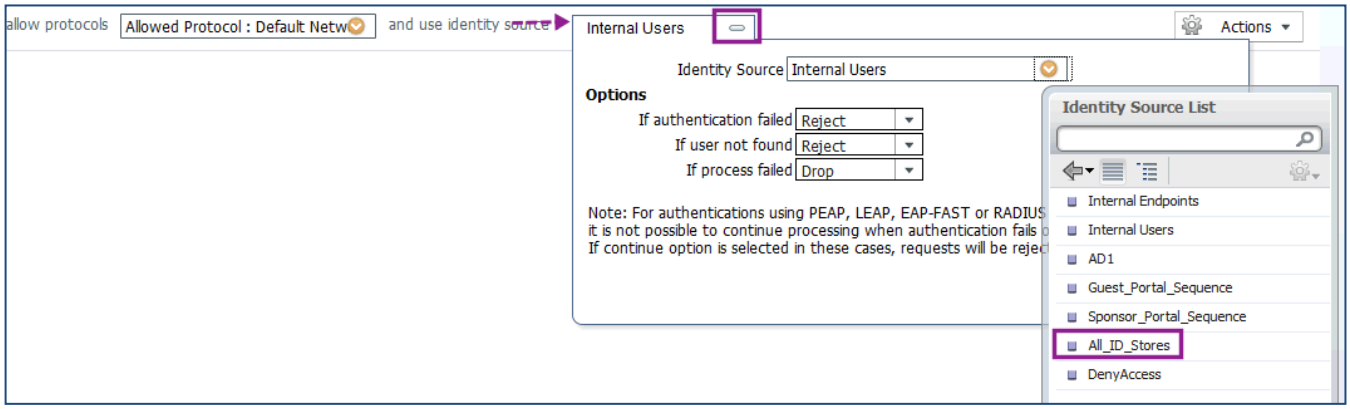
如果是其他类型的身份验证（例如 WebAuth），则不会与任何一条预配置规则相匹配，最终会使用默认规则。默认规则预配置为检查内部用户数据存储。

多数企业不愿对用户帐户使用默认的本地数据存储。绝大多数企业使用 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　在默认规则中，点击 Internal Users 旁边的减号，打开身份源选择器。

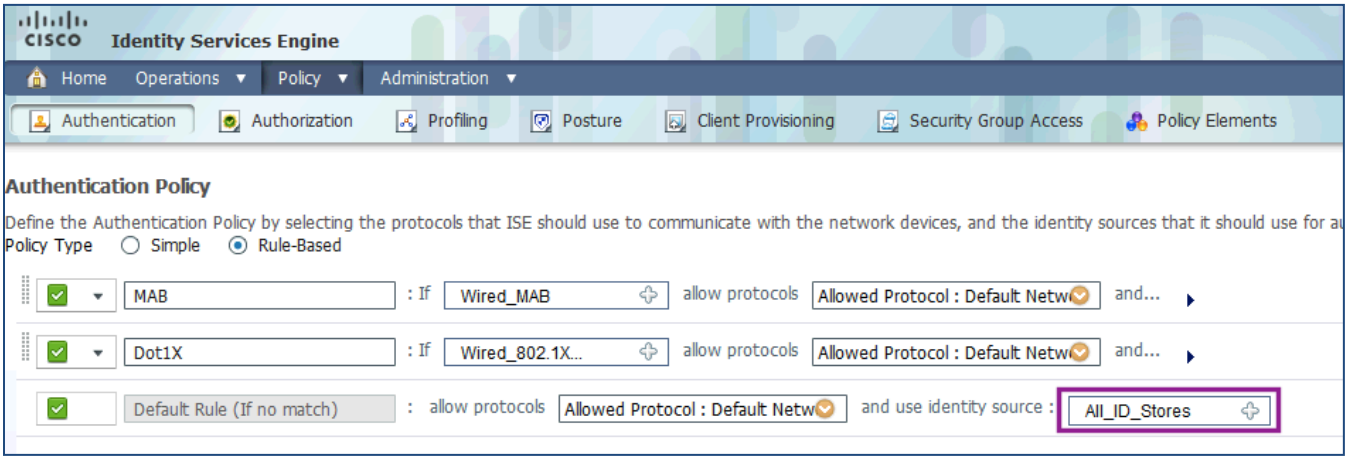
步骤 2　如图 11 所示，点击 Identity Source 列表，选择 All_ID_Stores 身份序列。该身份序列是在《TrustSec 操作指南：添加身份库和创建身份验证策略》中的“创建身份序列”程序中创建。

图 11：更改身份库



步骤 3　点击 Save 按钮。如图 12 所示，基于规则的策略即已修改。

图 12 更改身份库



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。表 1 中列出的三个选项以及表 2 中列出的其各自操作都对每个身份验证策略规则可用，包括默认规则。

表 1 身份验证策略选项

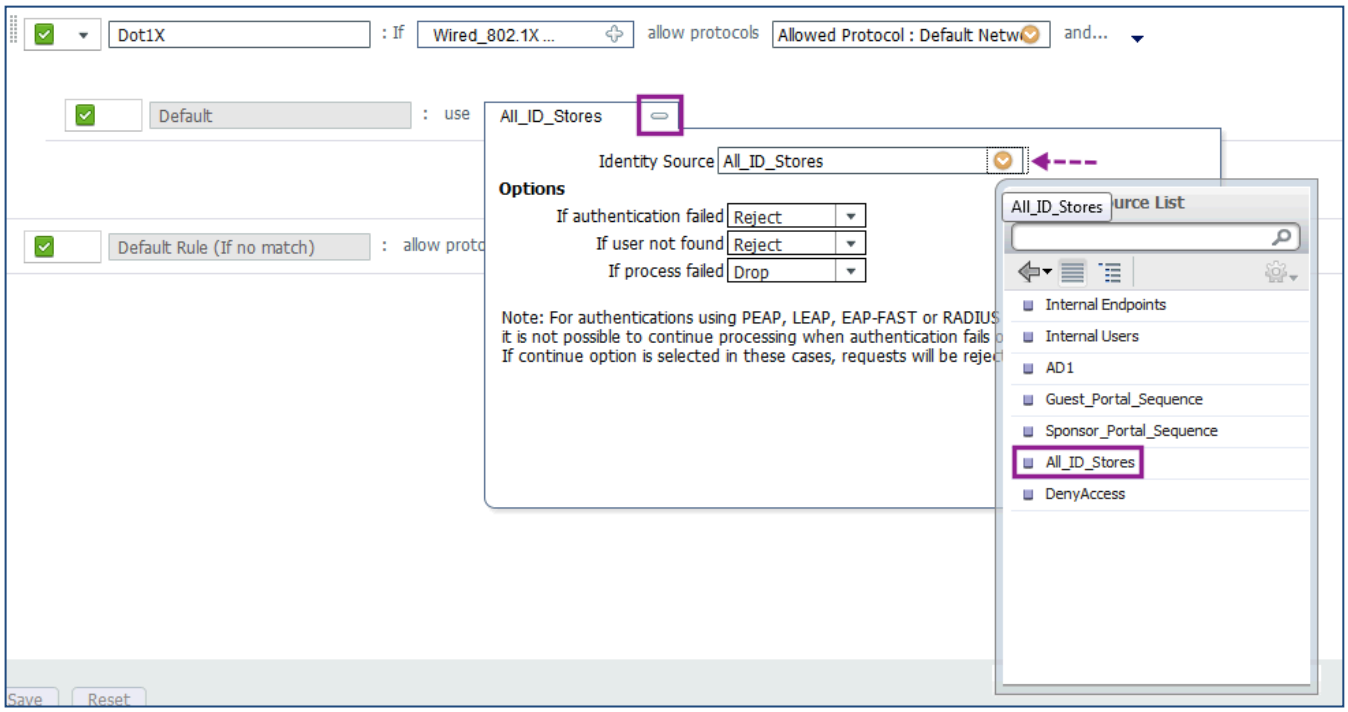
选项	描述
身份验证失败	收到身份验证已失败的明确回应，例如错误凭证、禁用的用户等。默认操作是“拒绝”。
未找到用户	在任何身份数据库中均未找到此用户。默认操作是“拒绝”。
处理失败	无法访问身份数据库。默认操作是“丢弃”。

表 2 身份验证策略操作

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

步骤 5 展开 Dot1X 行，重复上面的步骤 1 和 2，将身份源更改为 All_ID_Stores，如图 13 所示。

图 13 修改身份源



步骤 6 点击 Save。

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。

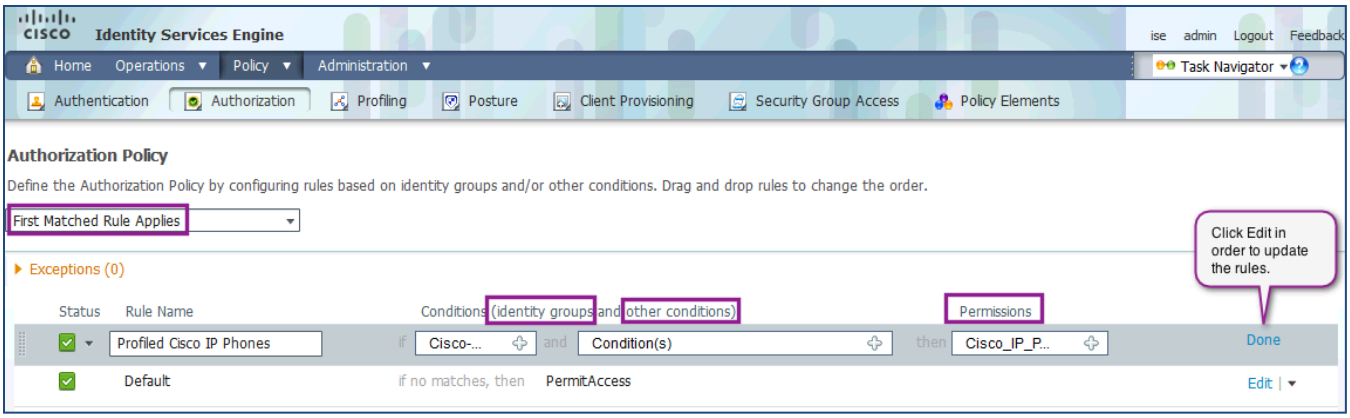
开始授权配置

程序 1　检查默认思科 ISE 授权策略

如前所述，身份验证只是确认用户凭证。所有的实施和访问控制都发生在网络访问的授权阶段。

步骤 1　导航至 Policy → Authorization，然后点击 Edit 以更新规则（图 14）。

图 14 编辑授权策略



授权策略中有一项预配置规则，还有默认规则。就像在身份验证策略中一样，在默认情况下，授权规则表的处理与访问列表相似：按从上到下的顺序进行处理，并且使用的是第一项符合条件的规则。

注：授权表能够匹配多项规则，可以得到非常复杂的授权结果，但此主题不属于本文档范围。

思科最佳实践：使用默认设置 First Matched Rule Applies。

就像在身份验证策略中一样，授权请求与规则行进行匹配的方式是基于条件而定的。说得更明白一点，我们将检查预配置规则 Profiled Cisco IP Phones。顾名思义，此规则用于授权在分析过程中确定的思科统一 IP 电话。

表 3：身份验证策略

选项	描述
身份组	手动或动态创建的特殊组，例如 guest 和 Whitelist。
其他条件	所有其他条件，例如 Group Membership。
权限	授权配置文件结果。

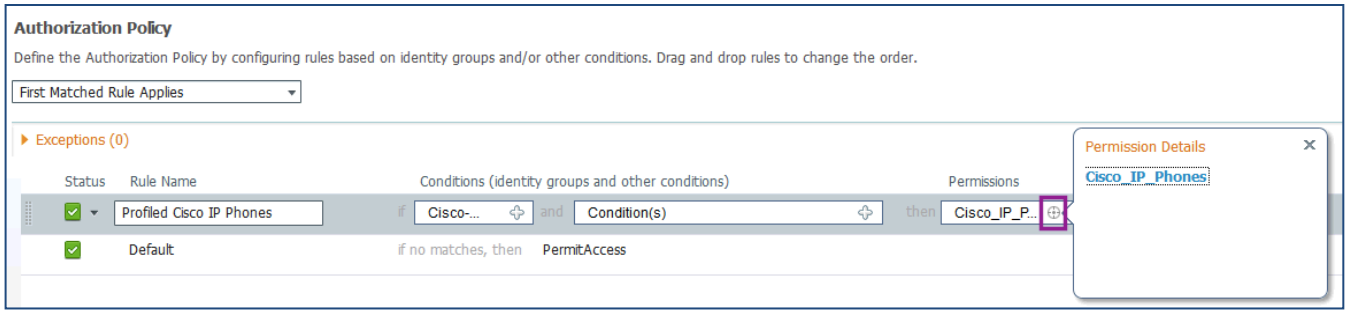
思科 ISE 策略采用逻辑 IF-THEN 格式。通过检查此规则，我们发现：

```
IF Device is member of ISE ID Group = Cisco-IP-Phone
AND (no other conditions in this line)
  THEN Assign the Cisco_IP_Phone Authorization Profile
ELSE Move to next Line in Authentication Policy Table
```

步骤 2 查看 Cisco_IP_Phone 授权配置文件的详细信息。

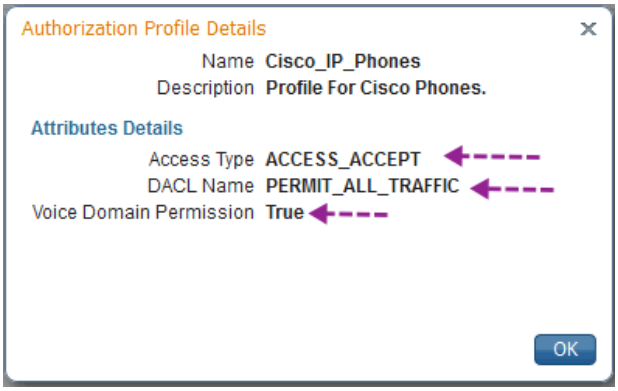
要查看 Cisco_IP_Phone 授权配置文件的详细信息，请将鼠标光标放在权限选择器上，屏幕上将弹出 Permission Details 窗口，点击 Cisco_IP_Phones 的链接（图 15）。

图 15：编辑授权策略



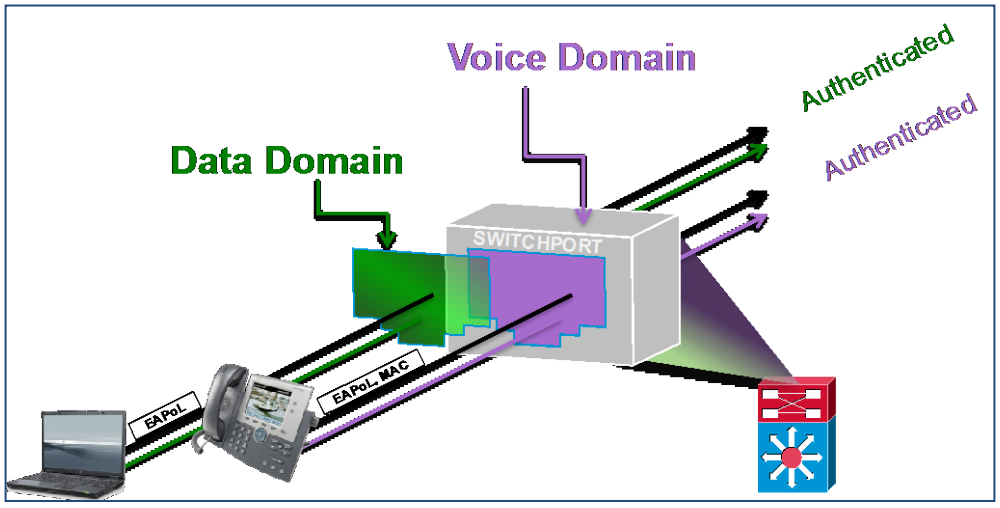
如图 16 中“授权配置文件详细信息”所示，Cisco_IP_Phones 发送 RADIUS Access-Accept 消息，发送名为 PERMIT_ALL_TRAFFIC 的可下载 ACL (dACL)，并允许设备加入语音域（语音 VLAN）。

图 16：授权配置文件详细信息



如图 17 所示，IP 电话需要一个特别的 RADIUS 属性才能在授权结果中发送，从而授予该设备加入语音 VLAN 的权限。

图 17 多域身份验证 (MDA)



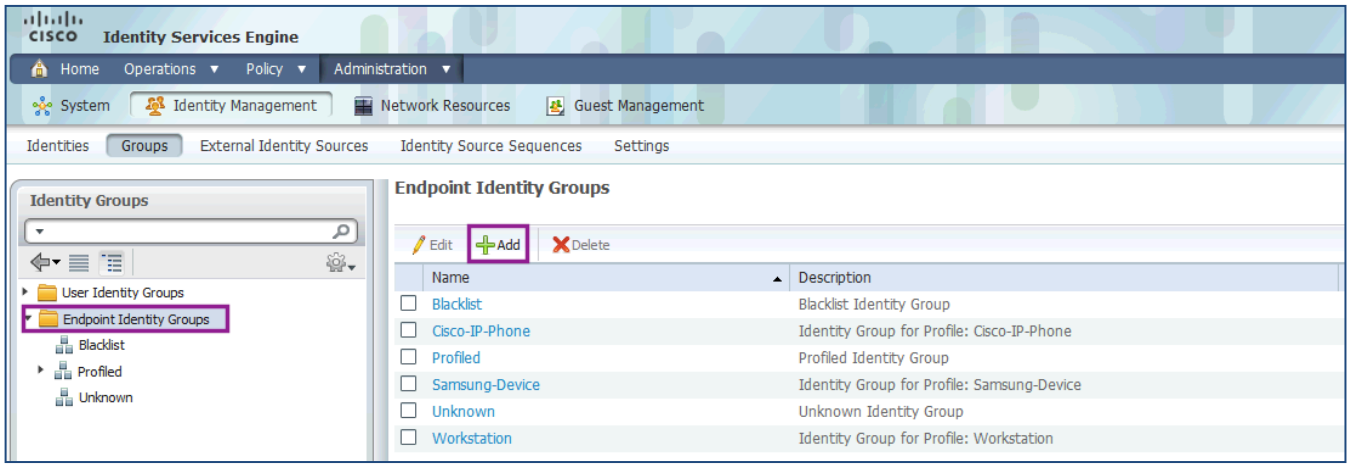
程序 2　为端点创建白名单

我们将手动创建一个白名单身份组。管理员可以向此组添加设备，以便授予该设备对网络的完全访问权限。建议仅在特殊情况下授予此权限。

步骤 1　导航至 Administration → Identities → Groups → Endpoint Identity Groups。

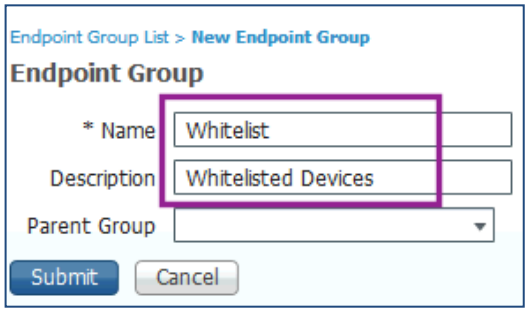
步骤 2　点击 Add（图 18）。

图 18 添加身份组



步骤 3　将新组命名为 **Whitelist**，然后将 Parent Group 下拉字段留空（图 19）。

图 19 新终端组

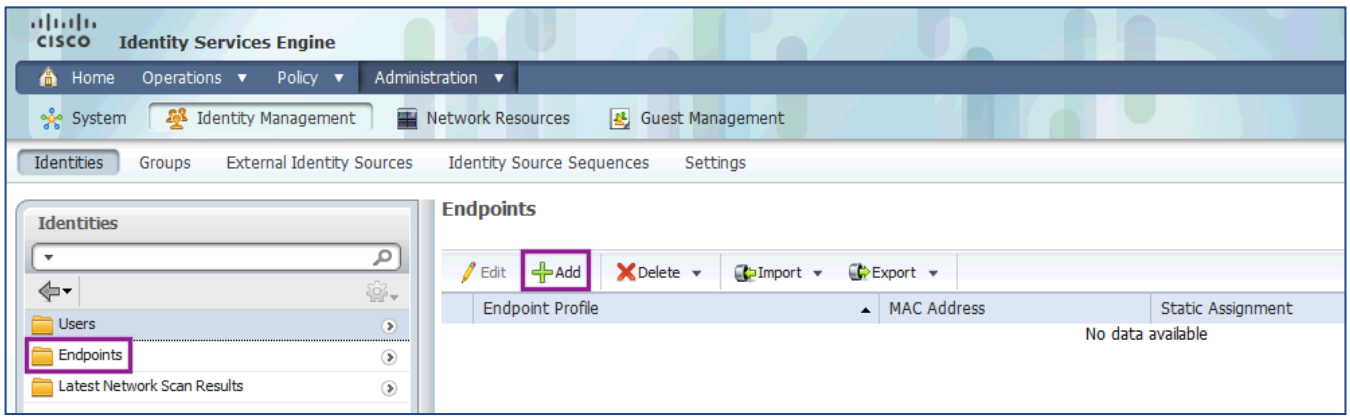


步骤 4　点击 Submit。

注：在排除故障时或者特定情况下，可以在此列表中添加设备，添加的设备将可以访问网络。

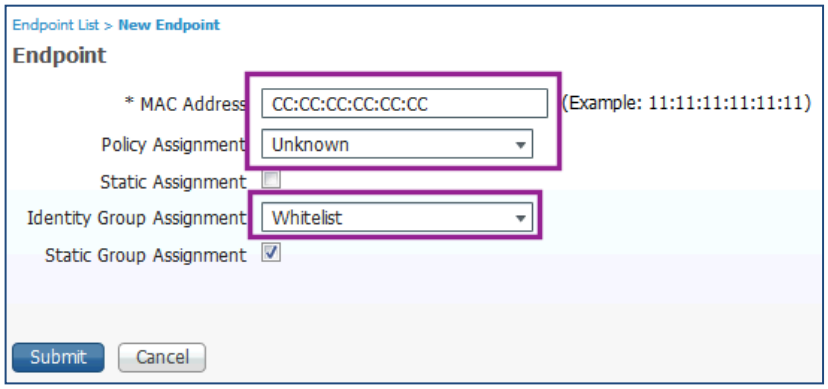
步骤 5　要向 Whitelist 组添加设备，请导航至 Administration → Identities → Endpoints，然后点击 Add（图 20）。

图 20 添加终端



步骤 6 以 nn:nn:nn:nn:nn:nn 的格式添加设备 MAC 地址，然后从 Identity Group Assignment 下拉列表中选择 Whitelist（图 21）。

图 21 新终端

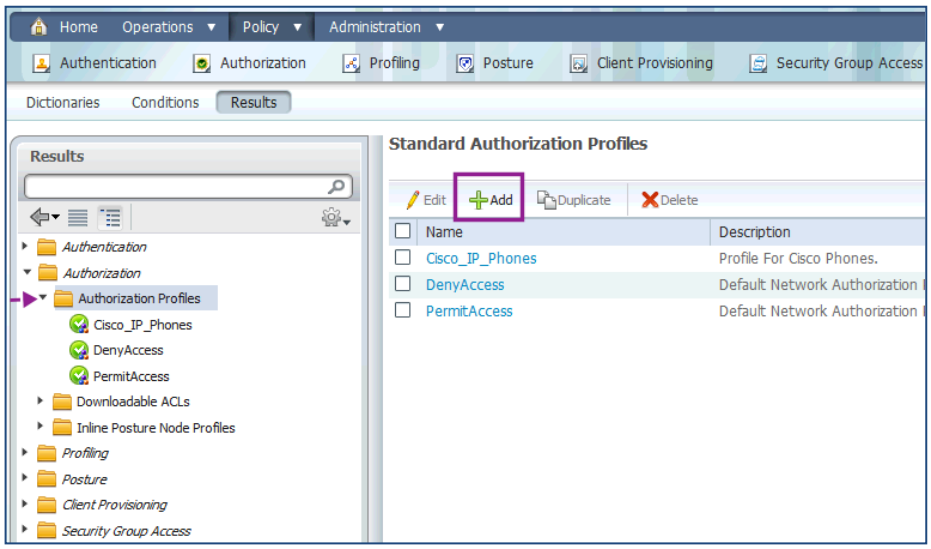


注：如果是已知设备类型（例如 Android），则可以从 Policy Assignment 下拉列表中进行选择。

程序 3　为列入白名单的设备创建授权配置文件

步骤 1 导航至 Policy → Policy Elements → Results → Authorization → Authorization Profiles（图 22）。

图 22 为列入白名单的设备添加授权配置文件

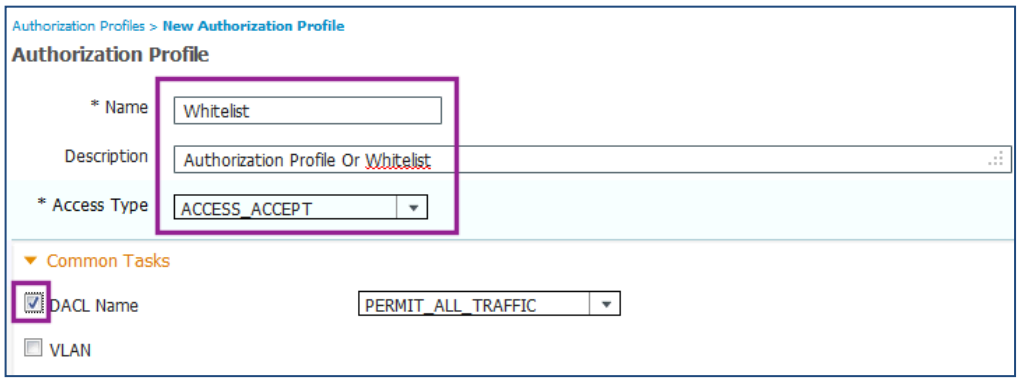


步骤 2 点击 Add。

步骤 3 如下所述，配置新的授权配置文件。

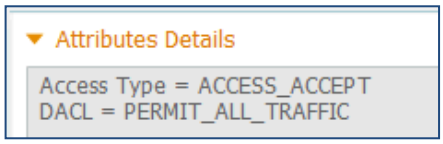
Name = Whitelist
Description = Authorization Profile for Whitelist
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ **DACL Name =** PERMIT_ALL_TRAFFIC

图 23：新授权配置文件



属性详细信息如图 24 所示。

图 24 属性详细信息



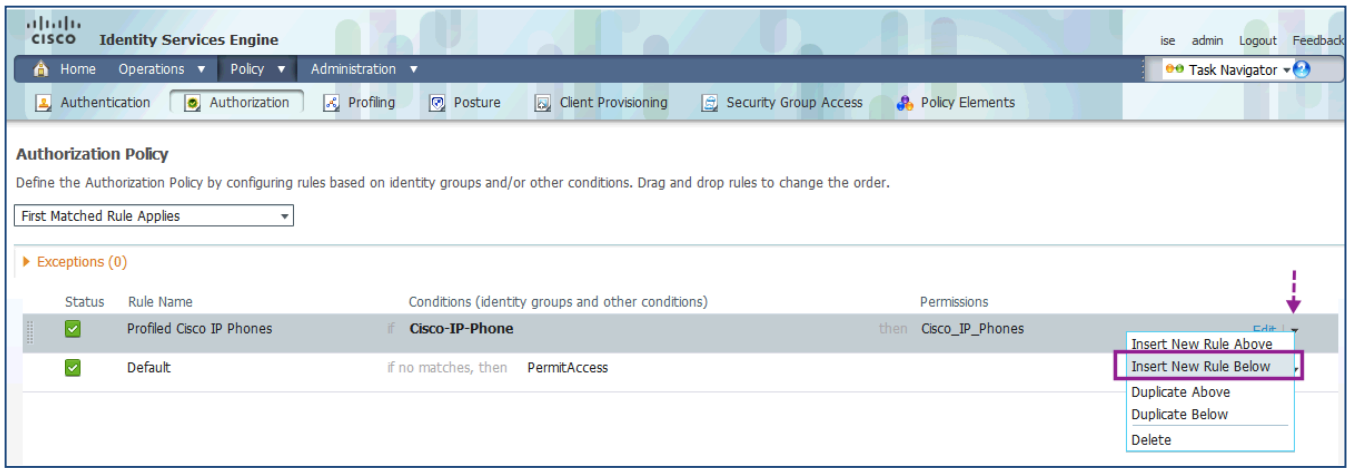
步骤 4 点击 Submit。

程序 4　为列入白名单的设备创建授权配置规则

步骤 1 导航至 Policy → Authorization。

步骤 2 点击 IP 电话授权规则末尾的 Actions（图 25）。

图 25 为列入白名单的设备创建授权策略

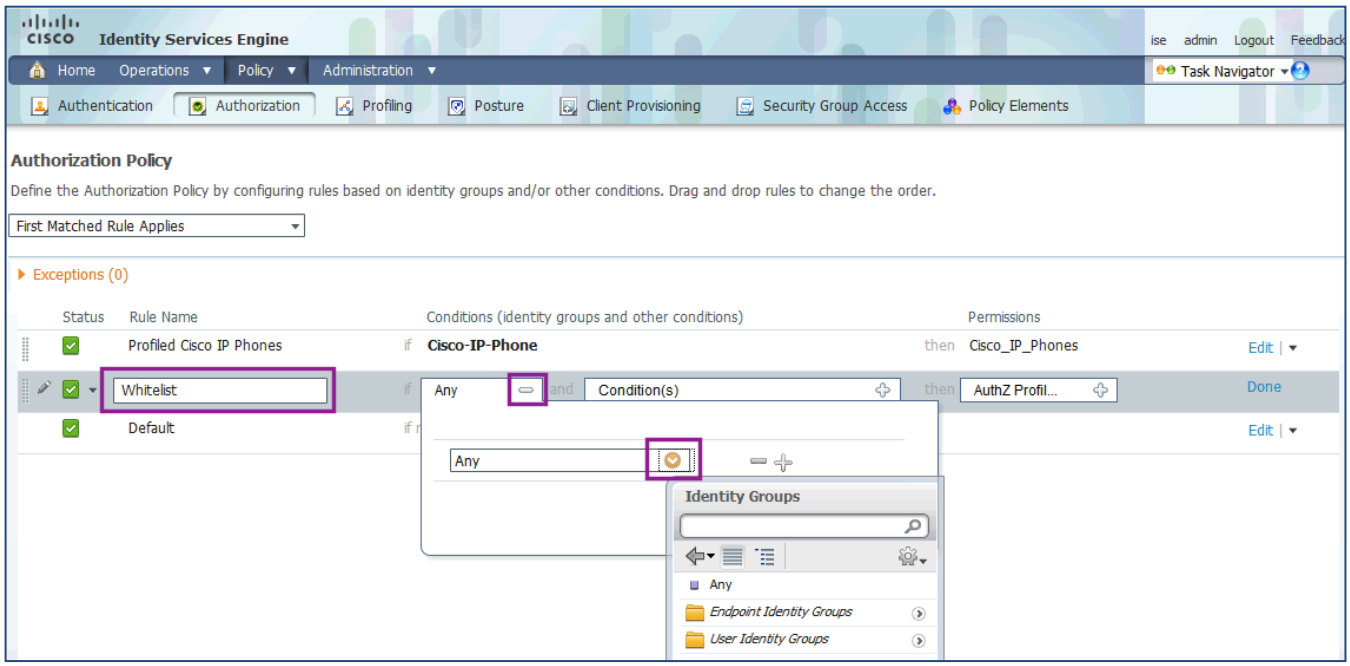


步骤 3 选择 Insert New Rule Below。

步骤 4 将新规则命名为 **Whitelist**。

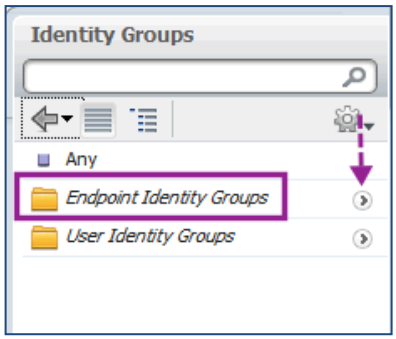
步骤 5 点击 Identity Group 列中 Any 旁边的 + 号（图 26）。

图 26 选择身份组



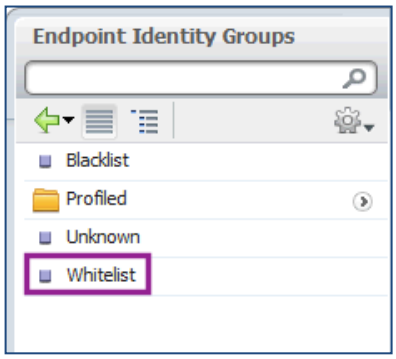
步骤 6 选择 Endpoint Identify Groups（图 27）。

图 27 终端身份组



步骤 7 从选择器选择 Whitelist Identity Group（图 28）。

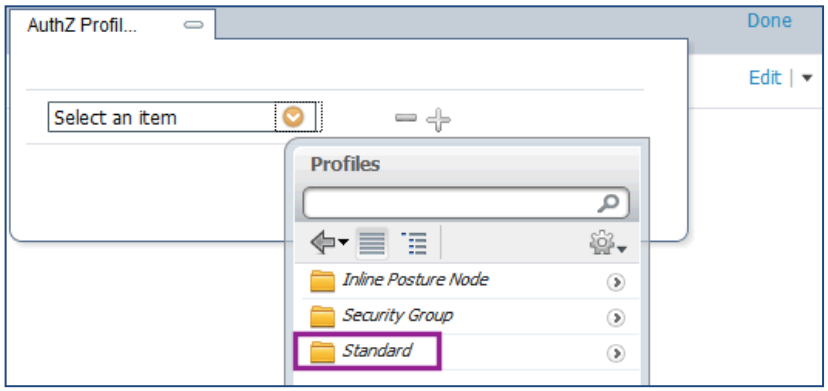
图 28 白名单身份组



步骤 8 请勿更改 Other Conditions 列。

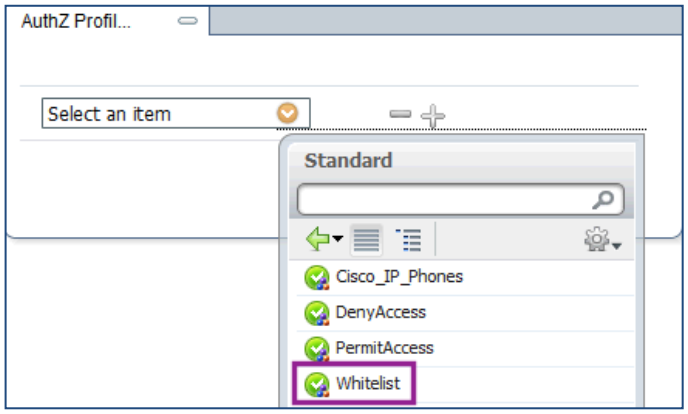
步骤 9 在 Permissions 列下选择加号，然后选择 Standard（图 29）。

图 29 授权配置文件



步骤 10 选择名为 Whitelist 的授权配置文件（图 30）。

图 30 选择白名单配置文件



步骤 11 点击 Save。

在监控模式下进行监控

此时，在监控模式配置中，所有设备无论是否成功通过身份验证，都仍可访问网络。这样，对最终用户就没有任何影响。但在此阶段期间所有交换机端口都会尝试对已连接的设备进行身份验证。端口将交替尝试通过 EAP (802.1X) 进行身份验证和通过 MAB 绕过身份验证。

在此阶段期间，我们将使用思科 ISE 中的监控和报告引擎查看所有失败的身份验证，并借此机会更正网络基础架构、甚至是用于托管资产的客户端配置流程中的任何错误配置。有关日志记录和故障排除详细信息，请参阅《操作指南-81-对失败的身份验证配置进行故障排除》。特别是，请检查以下两节。

- 22056 在适用的身份库未找到主题
- 11007 无法找到网络设备或 AAA 客户端

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 LAN 控制器：
http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html