使用思科身份服务引擎的网络访问设备配置文件

安全访问操作指南系列

目录

© 2015 思科系统公司

第 1 章网络访问设备配置文件

关于网络访问设备配置文件

思科身份服务引擎 (ISE) 引入了对某些非思科网络访问设备 (NAD) 的支持。ISE 使用*网络访问设备配置文件*表示 NAD 的功能和要求，ISE 使用这些功能和要求来启用 MAB、访客、自带设备和终端安全评估等流程。

ISE 2.0 随附许多位于“网络资源”(Network Resources) 下的内置 NAD 配置文件：

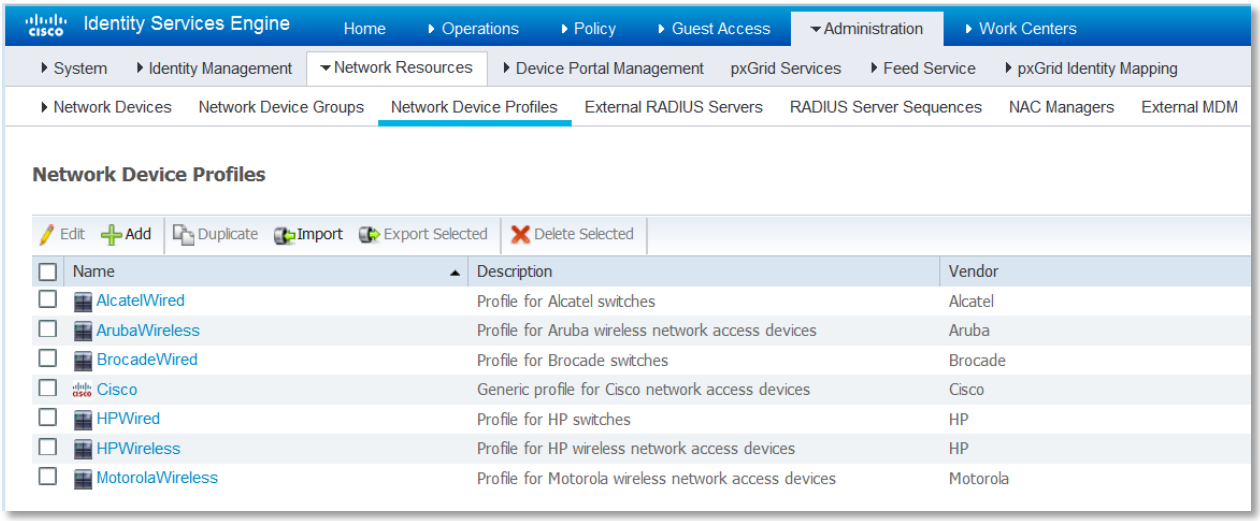

图 1. 内置 NAD 配置文件

自定义网络访问设备配置文件

本指南介绍在内置配置文件不足的情况下如何创建自定义 NAD 配置文件。NAD 将启用的 ISE 流程数取决于 NAD 的功能。

☞ 对于访客、自带设备和终端安全评估等复杂流程，设备需要支持 RFC 5176、“授权变更”(CoA) 以及能够重定向到 ISE 门户并将客户端身份（MAC 或 IP 地址）作为 URL 参数传入的 URL 重定向机制。如果 NAD 不支持这些功能，则这些流程将不起作用。

© 2015 思科系统公司

第 2 章自定义配置文件创建步骤

概述

需要先确定有关设备的某些信息，然后才能定义新的 NAD 配置文件。通常必须为设备导入新的 RADIUS 字典，然后才能创建 NAD 配置文件。您可能必须将设备固件升级到更新的版本才能获取 CoA/URL 重定向支持。通常还必须在设备上进行配置更改，以配置或启用特定功能，尤其对于 URL 重定向而言更是如此。一旦完成后，就请在 ISE 中创建新的 NAD 配置文件，并将其分配到相应的设备。最后，配置新的授权配置文件和 ISE 策略，以利用新的配置文件。

建议程序

收集信息

步骤 1 参阅 NAD 的《*管理手册*》（通常具有所寻求的信息）
步骤 2 确定所需的 RADIUS 字典（如果有），并将其导入到 ISE 中
步骤 3 确定用于 MAB、SSID、设置 VLAN、ACL 的属性（如果适当）
步骤 4 确定是否支持 RADIUS CoA 及其在 CoA 请求中需要哪些属性
步骤 5 确定是否支持 URL 重定向及其使用哪些属性和 URL 参数

设备配置

步骤 6 验证 NAD 固件的级别是否足够，如有必要，请进行升级
步骤 7 在 NAD 上进行任何所需的配置更改（对于 CoA/URL 重定向）

配置文件创建和分配

步骤 8 使用从上述内容获取的信息创建新的 NAD 配置文件
步骤 9 将新的配置文件分配到一个或多个 NAD

策略配置

创建 10 创建新的授权配置文件
步骤 11 配置 ISE 策略以利用新的 NAD 配置文件
步骤 12 验证预期行为

这些步骤将在后续章节中更详细地进行说明。

© 2015 思科系统公司

第 3 章 RADIUS 字典

确定是否需要导入字典

参考 NAD 文档以确定 NAD 使用的 RADIUS 字典。大多数 NAD 都具有供应商特定的 RADIUS 字典，除标准 IETF RADIUS 属性以外，该字典还提供许多供应商特定属性。诸如 MAB、CoA、URL 重定向、ACL、VLAN、SSID 等功能全都可能使用 RADIUS 属性，并且有时这些属性是供应商特定的 (VSA)，而不是 IETF。

导入 RADIUS 字典

如果您的设备使用 VSA，则通常需要先将其 RADIUS 字典安装到 ISE 中，然后才能将其分配到 NAD 配置文件。ISE 能够以 *freeradius* 格式导入 RADIUS 字典文件，可以在*策略元素 (Policy Elements)* →*字典 (Dictionaries)* →*系统 (System)* →*Radius* →*RADIUS 供应商 (RADIUS Vendors)* 中找到这些文件。

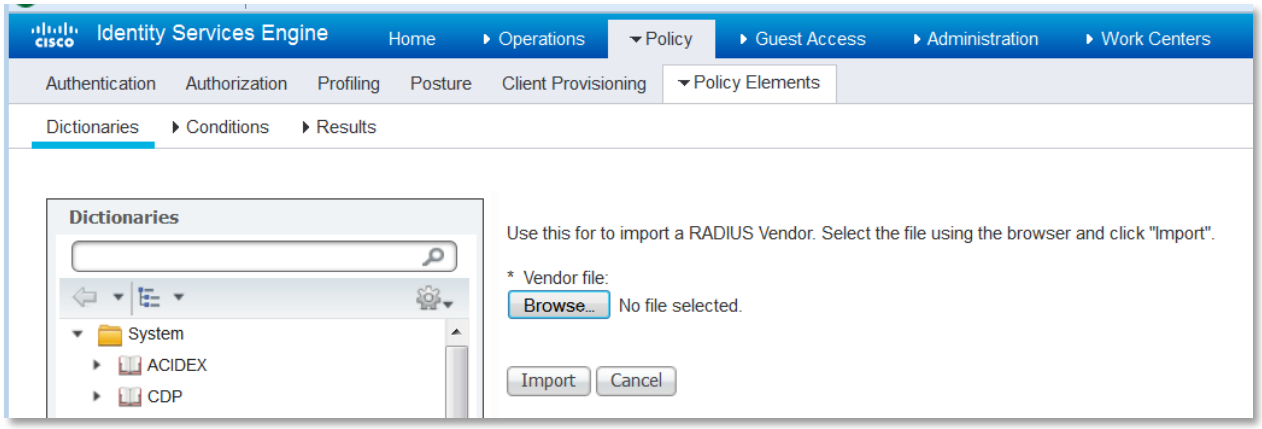

图 2. 导入 RADIUS 字典

© 2015 思科系统公司

成功导入后，新字典应该会显示在 RADIUS 字典供应商列表中：

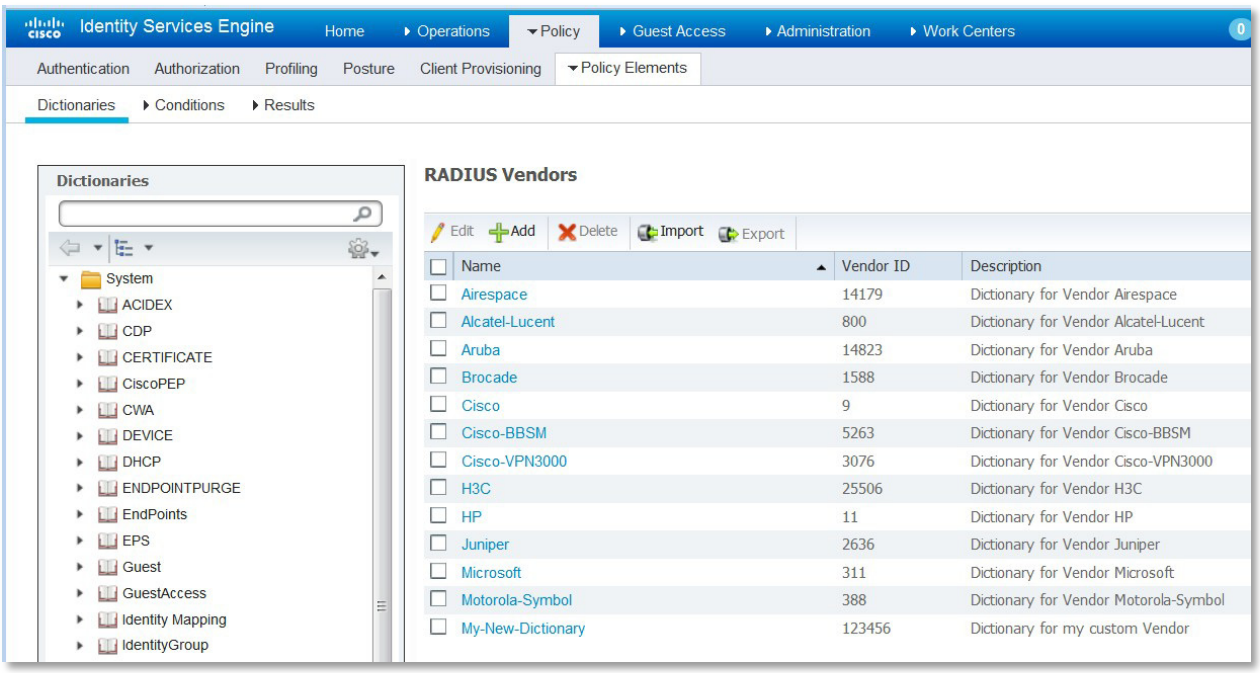

图 3. 新导入的词典

© 2015 思科系统公司

第 4 章定义自定义配置文件

创建新的配置文件条目

一旦您拥有所需的信息并已安装 RADIUS 字典，就请点击*新建网络设备配置文件 (New Network Device Profile)* 以创建新的 NAD 配置文件。为 NAD 配置文件创建新的名称和描述。名称在策略条件和故障排除中可能有用，并会显示在报告中。您可以为新的配置文件分配特定图标，从而更轻松地将其与其他配置文件区分开来。

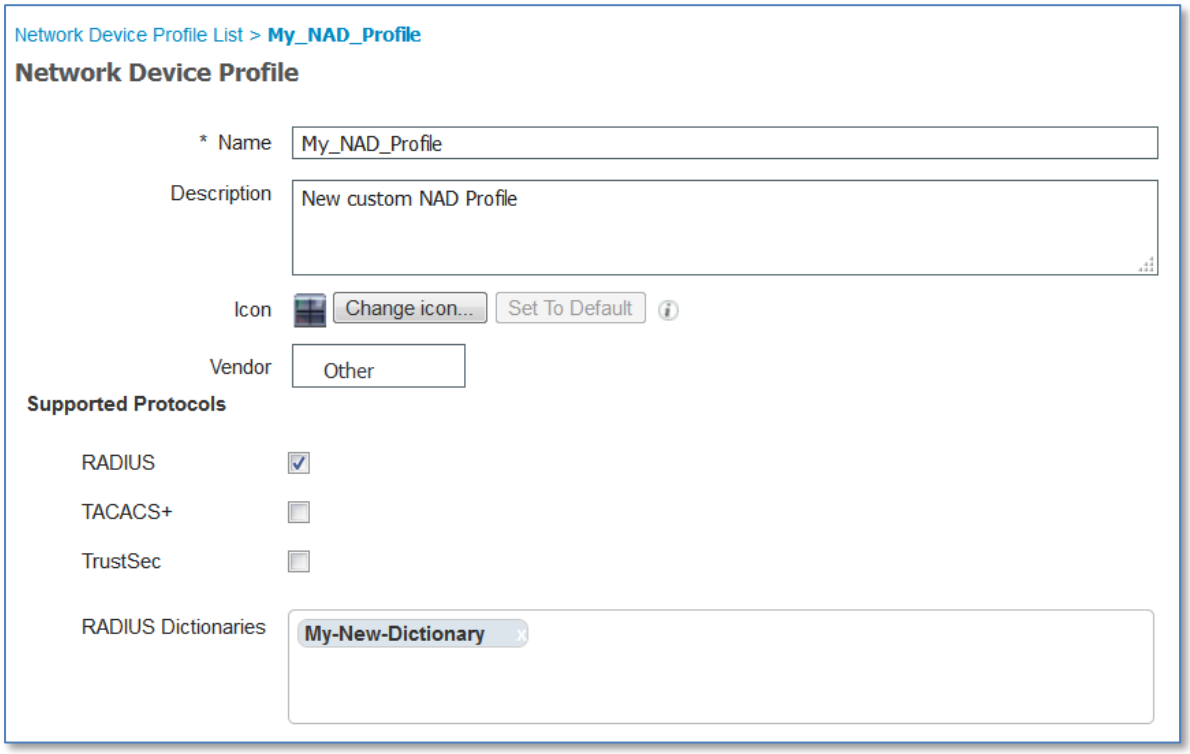

图 4. 新 NAD 配置文件

对于*供应商 (Vendor)*，如果您是为设备创建与其中一个内置配置文件类似的 NAD 配置文件（即，供应商相同，但是型号因某些差异而不同），则最好是克隆现有 NAD 配置文件并对其进行自定义。克隆的配置文件将具有原始配置文件的设置的副本，因此您只需对其进行调整即可，而不必重头开始定义。如果当前 RADIUS 字典足够，您可能不必定义新的 RADIUS 字典。

但是，如果您的 NAD 供应商与任何现有供应商都不匹配，则应将*供应商 (Vendor)* 字段设置为“其他”(Other) 并输入其所有特征。

© 2015 思科系统公司

支持的协议

如果您的设备支持 RADIUS、TACACS+ 和/或 TrustSec，请选中每个框。只需选中实际要使用的协议即可。

RADIUS 字典

分配设备支持的 RADIUS 字典（通常是您在某个步骤中事先导入的字典）。注意：您可以分配多

个字典，原因是某些设备确实支持多个供应商字典。

流程类型条件

在“流程类型条件”(Flow Type Conditions) 部分中（“身份验证/授权”[Authentication/Authorization] 下）输入设备针对各种流程（例如有线 MAB 和 802.1x）使用的属性和值。这对于使 ISE 根据设备使用的属性来为该设备检测适当的流程类型是必需的。对于 MAB 而言没有任何 IETF 标准，不同的供应商使用不同的 Service-Type 值。如果此处的值未记录在设备的《管理指南》中，则可能必须使用嗅探器跟踪来确定这些值。

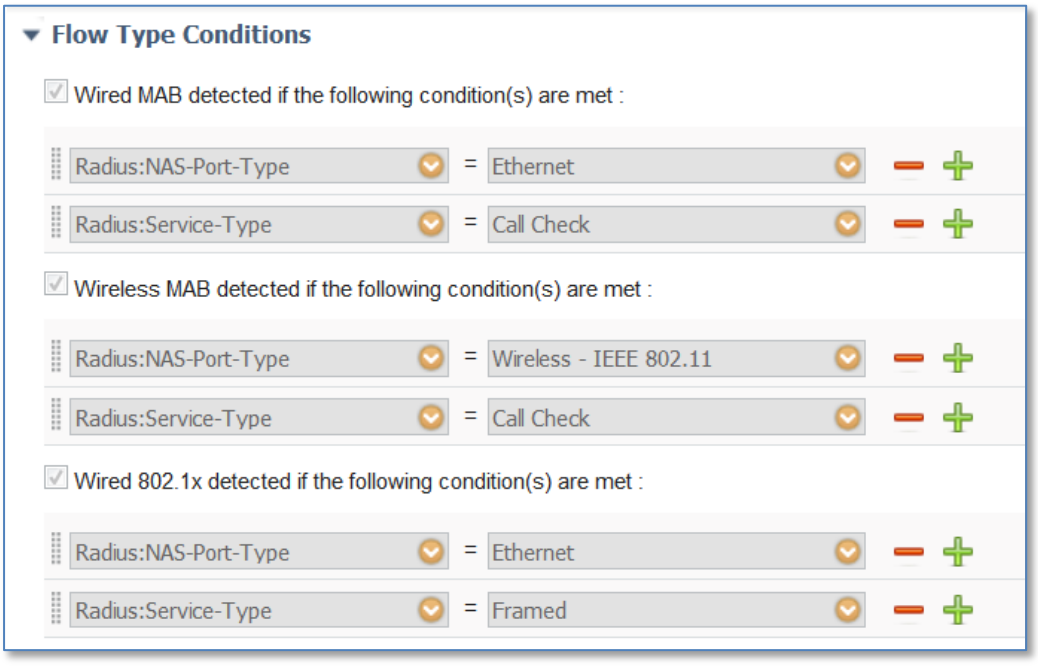

图 5. 流程类型条件

© 2015 思科系统公司

属性别名

本节允许您将设备特定属性名称映射到通用名称以简化策略规则。目前，仅定义了“SSID”。如果您的设备具有无线 SSID 的概念，则将此设置为其使用的属性。

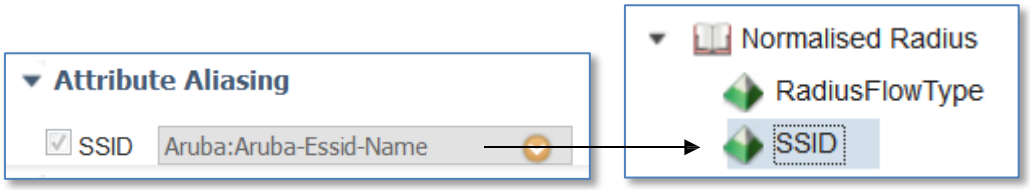

图 6. 属性别名 (SSID)

属性别名允许 NAD 配置文件将供应商特定属性映射到通用属性，以便策略规则可以使用友好名称。这样可以简化属性选择，减少不同供应商设备所需的身份验证/授权策略规则数，并降低容易出错的可能性。例如，在某个流程中涉及的无线 SSID 可能包含在 Airespace-Wlan-ID、Aruba-ESSID-Name 或 Called-Station-ID 中，具体取决于所涉及的 NAD 的类型。您可以将此映射到“规范化 Radius”(Normalised Radius) 字典（策略 [Policy] > 策略元素 [Policy Elements] > 字典 [Dictionaries] > 规范化 Radius [Normalised Radius] > SSID）中提供的“SSID”属性。

主机查询

本节允许您定义设备用于 MAB 的属性和协议。在 2.0 之前的版本中，通过*允许的协议 (Allowed Protocols)* 页面中的复选框的各种不明确组合来完成此任务，并且其可能需要多个“允许的协议”(Allowed Protocol) 条目。主机查询现在封装在 NAD 配置文件中，并可简化配置。

当在“允许的协议”(Allowed Protocols) 页面中启用“处理主机查询”(Process Host Lookup) 选项时，将会根据 NAD 配置文件配置（具体是指主机查询 [MAB] 设置）处理主机查询请求。

不同的（非思科）供应商在执行 MAB 身份验证时以不同方式填充 RADIUS *Calling-Station-ID* 和密码属性。对于执行 MAB 的思科 NAD 而言，启用“处理主机查询”(Process Host Lookup) 选项即足够。但是，对于其他供应商设备，则必须在“主机查询 (MAB)”(Host Lookup [MAB]) 部分中启用相应的选项，同时创建 NAD 配置文件。

如上所述，对于 MAB 而言没有任何标准，因此其使用的属性和协议根据供应商而异。请参阅您的设备的《管理指南》或 MAB 身份验证的嗅探器跟踪，以确定此部分的正确设置。

© 2015 思科系统公司

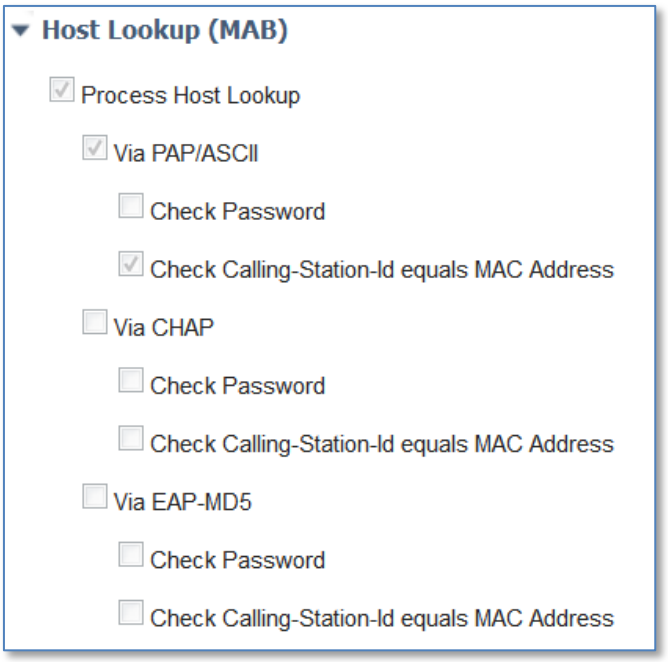

图 7. 主机查询 (MAB)

权限

本节定义设备用于设置 VLAN 或 ACL 的属性。它们可以是 IETF 标准属性，也可以是供应商特定属性。这些属性通常发布在设备的《管理指南》中。

对于 VLAN 权限，可以指定多个 RADIUS 属性/值对，也可以指定单个 RADIUS 属性（例如 Aruba-User-VLAN）。

对于 ACL 权限，可以指定单个 RADIUS 属性，以用于在与当前 NAD 配置文件相关的 NAD 上设置指定 ACL。

注意：“授权配置文件”(Authorization Profile) 页面的“常见任务”(Common Tasks) 部分中显示的选项根据您在“NAD 配置文件权限”(NAD Profile Permission) 部分中配置的属性而异。

© 2015 思科系统公司

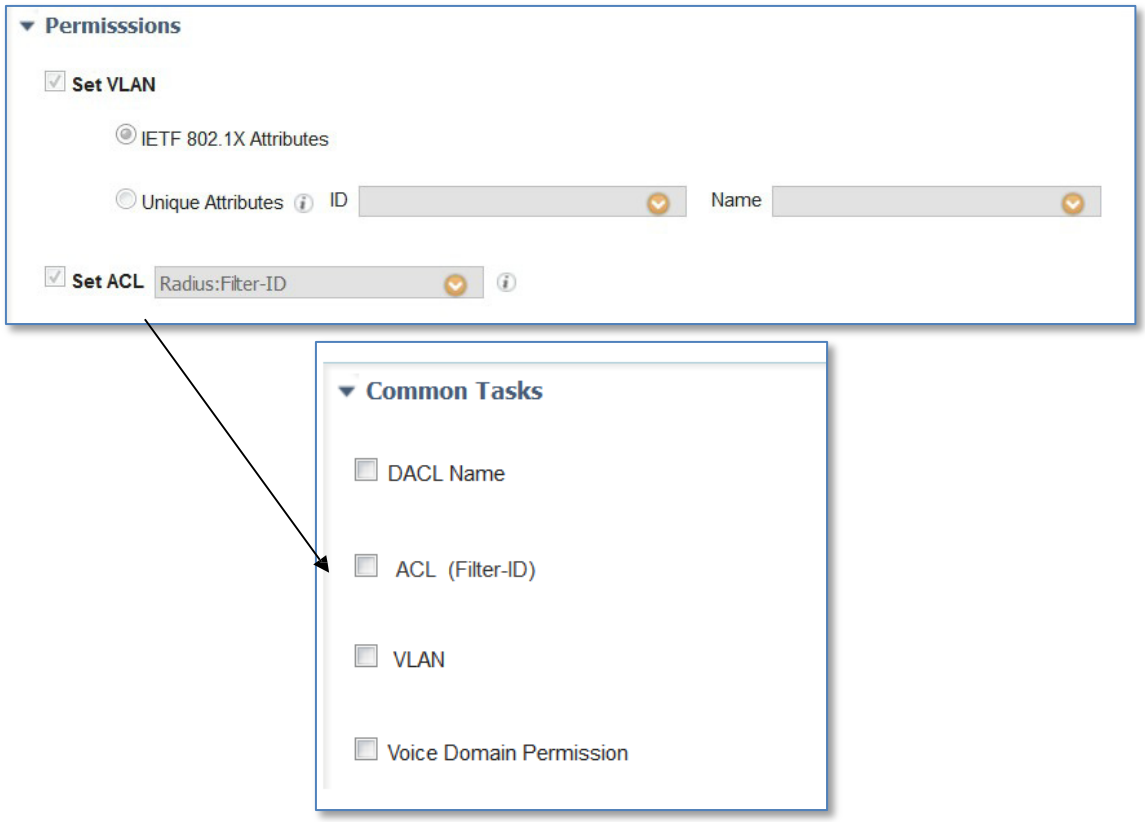

图 8. 权限以及与常见任务的关系

授权变更 (CoA)

本节允许您定义设备具有的 CoA 功能。请参阅您的设备文档以获取信息 - 查找对“RFC 5176”、“授权变更”或“CoA”等术语的引用。具有 RFC 5176 支持的大多数非思科设备都将支持“推送”和“断开连接”，但不支持重新进行身份验证，因此如果不确定，请尝试启用标记为“RFC 5176”的两个复选框。

© 2015 思科系统公司

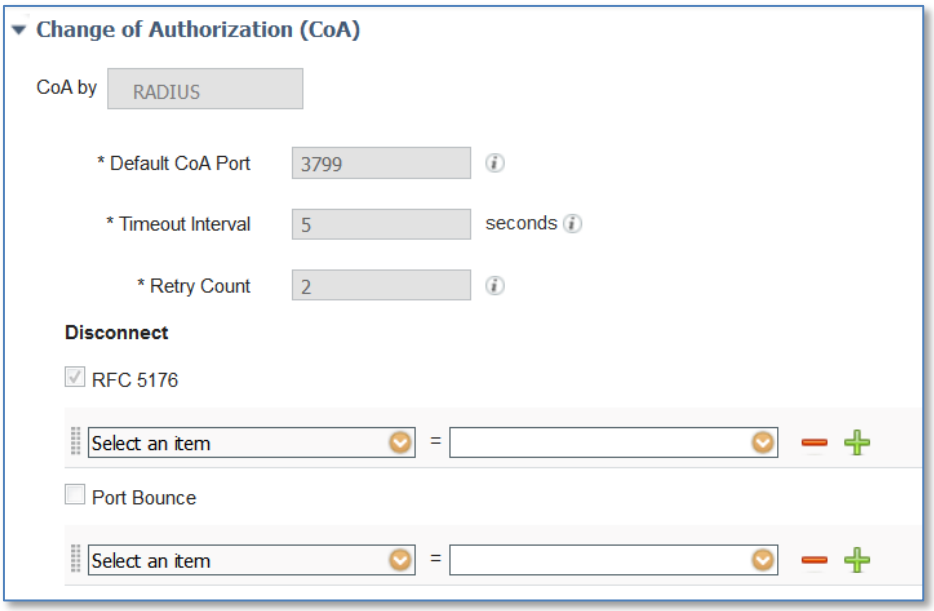

图 9. CoA 配置

虽然 RFC 5176 会定义 CoA 请求的类型，但是请求中的必需属性根据设备而异。某些设备对于 CoA 请求中发送的属性非常讲究。

如果您的 CoA 请求从设备获取的是 CoA“NAK”，请检查下列某些提示：

- 某些设备要求在 CoA 请求中包含来自 access-request 的 RADIUS User-Name 属性
- 某些设备不同时接受同一请求中发送的 Calling-Station-ID 和 Acct-Session-ID（请仅发送一项）
- 某些设备在请求中不接受其他供应商 VSA
- 某些设备可以配置为应该（或不应）具有 Event-Timestamp 属性，并且上述 CoA 配置必须匹配

虽然某些《管理指南》确实会发布属性，但某些则不发布，并且其需要一定的试用或错误来确定适当的属性集。

注意：请确保在*支持的协议 (Supported Protocols)* 部分中选择 RADIUS 选项，然后再配置 RADIUS CoA。

URL 重定向

本节定义设备的 RUL 重定向功能。URL 重定向对于访客、自带设备和终端状态评估等复杂流程是必需的。它需要能够重定向到 ISE 门户，即*本地 Web 身份验证*不够。

在设备上有两种通用类型的 URL 重定向：静态和动态。静态意味着必须将 URL 配置到设备中（手动）。它不支持通过 RADIUS 属性获知要动态重定向到的位置。通常，您将 ISE 门户 URL 复制并粘贴到设备的配置中。

© 2015 思科系统公司

另一种类型是动态 URL，ISE 可以在此类 URL 中使用 RADIUS 属性指示设备要动态重定向到的位置。不必手动配置设备。如果设备支持动态 URL，则应使用该设备，因为它可简化配置。

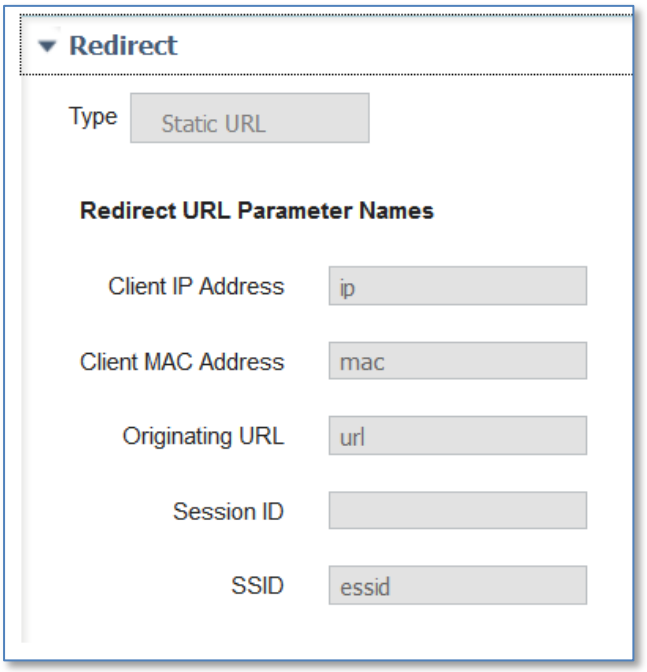

图 10. URL 重定向

“参数名称”(Parameter Names) 包含设备在重定向 URL 中传递的参数。ISE 需要获知这些参数的名称，从而可以从 URL 正确提取这些参数。它使用这些参数识别客户端和会话，以及客户端尝试访问的原始 URL，以便可以将其重定向。

注意：《管理员指南》通常不发布这些参数名称。某些指南会发布，但是大多数都不发布。少数参数实际可编程。无论什么情况，URL 参数名称都必须与设备发送的参数名称（如果未发布，则可能必须使用浏览器来确定这些参数名称）匹配。

注意：有线设备通常无法重定向 URL。

生成策略元素

通常，不必创建其他身份验证/授权条件或修改内置身份验证/授权条件（例如 *有线/无线 MAB* 或 *有线/无线 802.1X*），因为这些条件将在运行时自动使用适当的 NAD 配置文件。同样，内置 *允许的协议* 将使用现有 NAD 配置文件中的正确属性来检测 MAB。

但是，如果必须创建自定义条件、协议或配置文件，则可以使用 *策略元素生成 (Policy Element Generation)* 向导帮助您执行操作。它可以根据能够在策略中进一步自定义或使用的 NAD 配置文件创建各种可编辑元素。

© 2015 思科系统公司

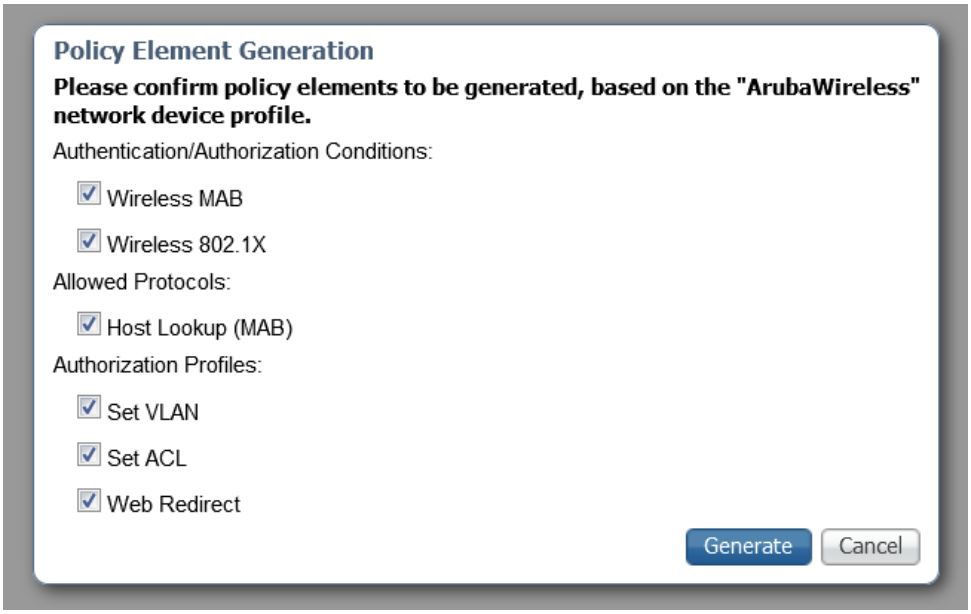

图 11. 生成策略元素

Summary

“摘要”(Summary) 部分显示 NAD 配置文件配置将启用的流程和服务。

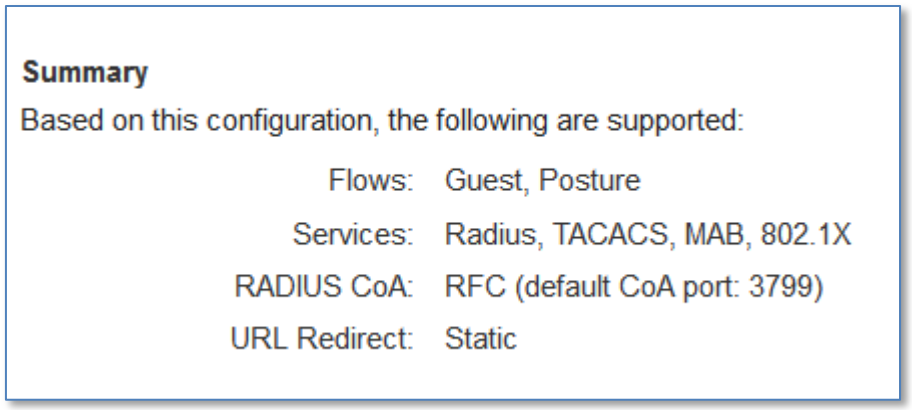

图 12. NAD 配置文件摘要

© 2015 思科系统公司

第 5 章使用网络设备配置文件

分配 NAD 配置文件

一旦创建 NAD 配置文件后，就请在“网络设备”(Network Devices) 中将其分配到您的设备。

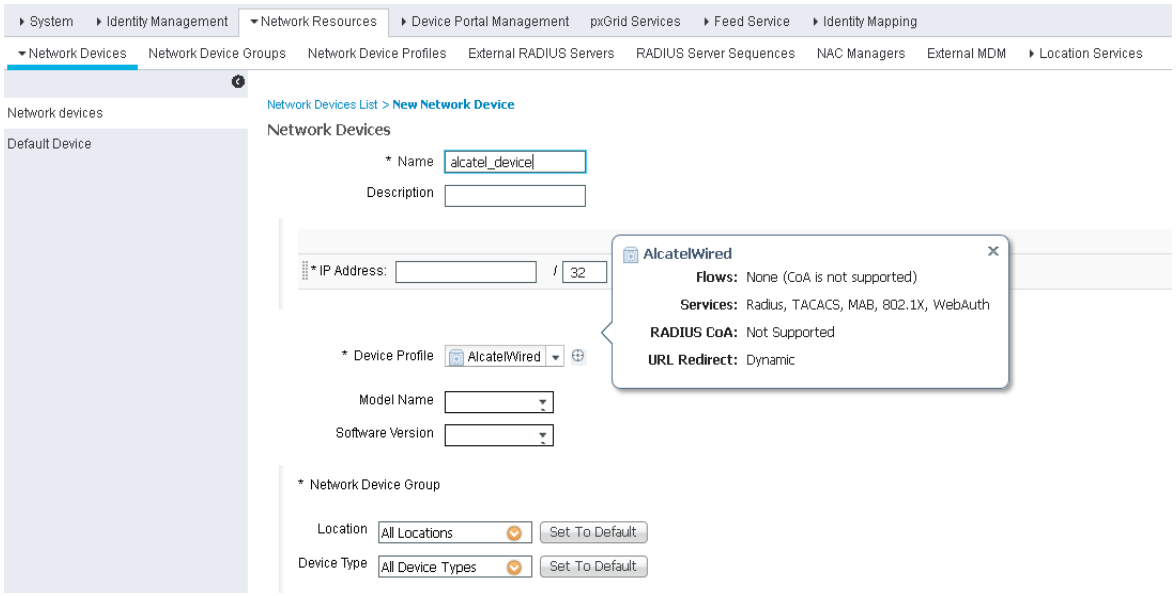

图 13. 分配 NAD 配置文件

© 2015 思科系统公司

身份验证/授权条件

ISE 具有许多内置身份验证和授权条件（有线/无线 MAB 和 802.1x），可以智能选择适当的基础条件进行评估。它通过确定在运行时分配到 NAD 的 NAD 配置文件，然后参考其 NAD 配置文件中的信息来进行此选择。借此可以显著减少您的身份验证/授权条件。通常，您可以定义新的 NAD 配置文件，并且不必自定义内置智能条件。

如果您检查其中一个现有条件，则可以了解哪些 NAD 配置文件将被其纳入考虑，哪些不予考虑。

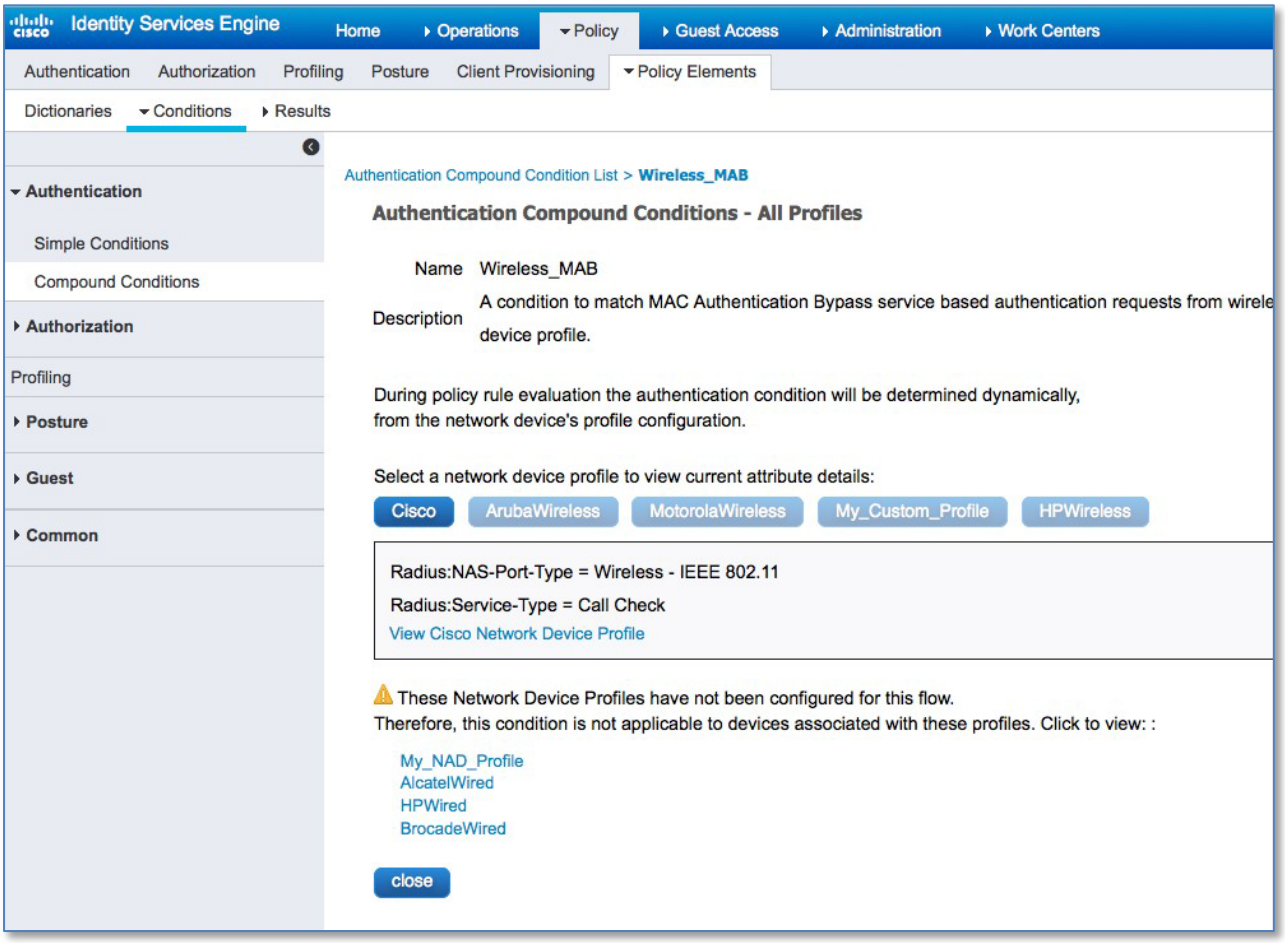

图 14. 智能身份验证条件

有时，您可能希望为新设备定义自定义条件。您可以使用 NAD 配置文件中的*生成策略元素 (Generate Policy Elements)* 功能来帮助生成具有条件中的正确属性/值的策略元素。

© 2015 思科系统公司

授权配置文件

您通常需要为新设备创建一个或多个授权配置文件。当创建配置文件时，请将*网络设备配置文件 (Network Device Profile)* 框设置为新 NAD 配置文件的名称。这使“智能”授权能够根据设备的所分配 NAD 配置文件自动选择适当的配置文件。

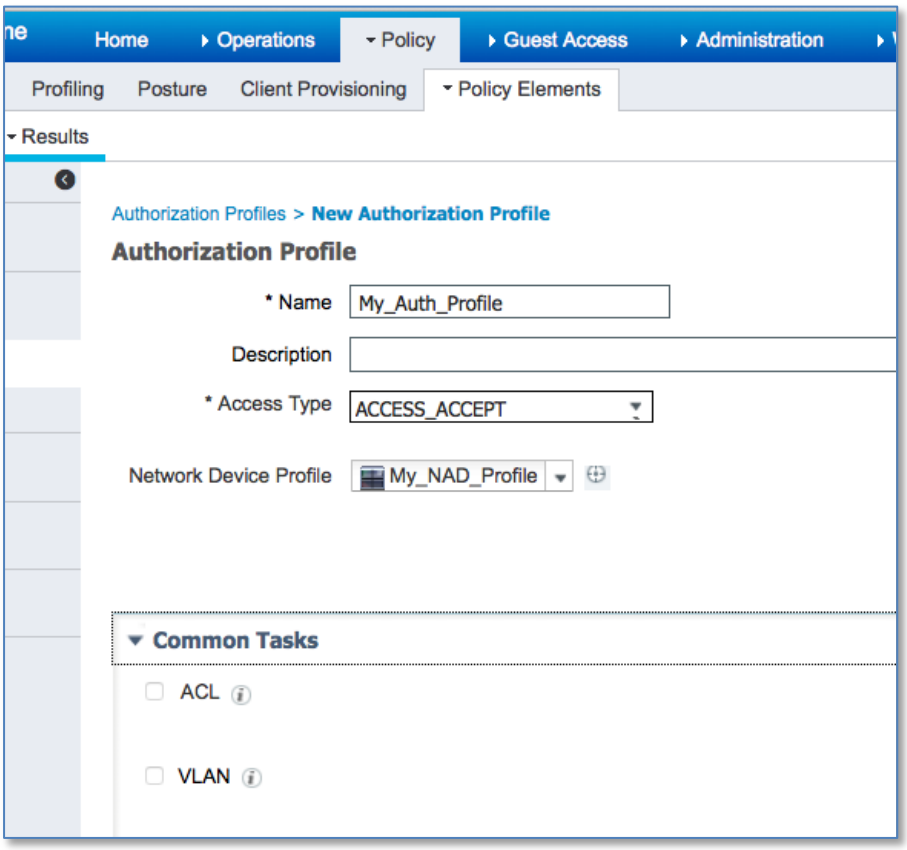

图 15. 新建授权配置文件

© 2015 思科系统公司

当配置策略规则时，授权配置文件应显式设置为您分配到该设备的 NAD 配置文件；如果您使用的只是 VLAN 或 ACL，则应设置为“Any”。

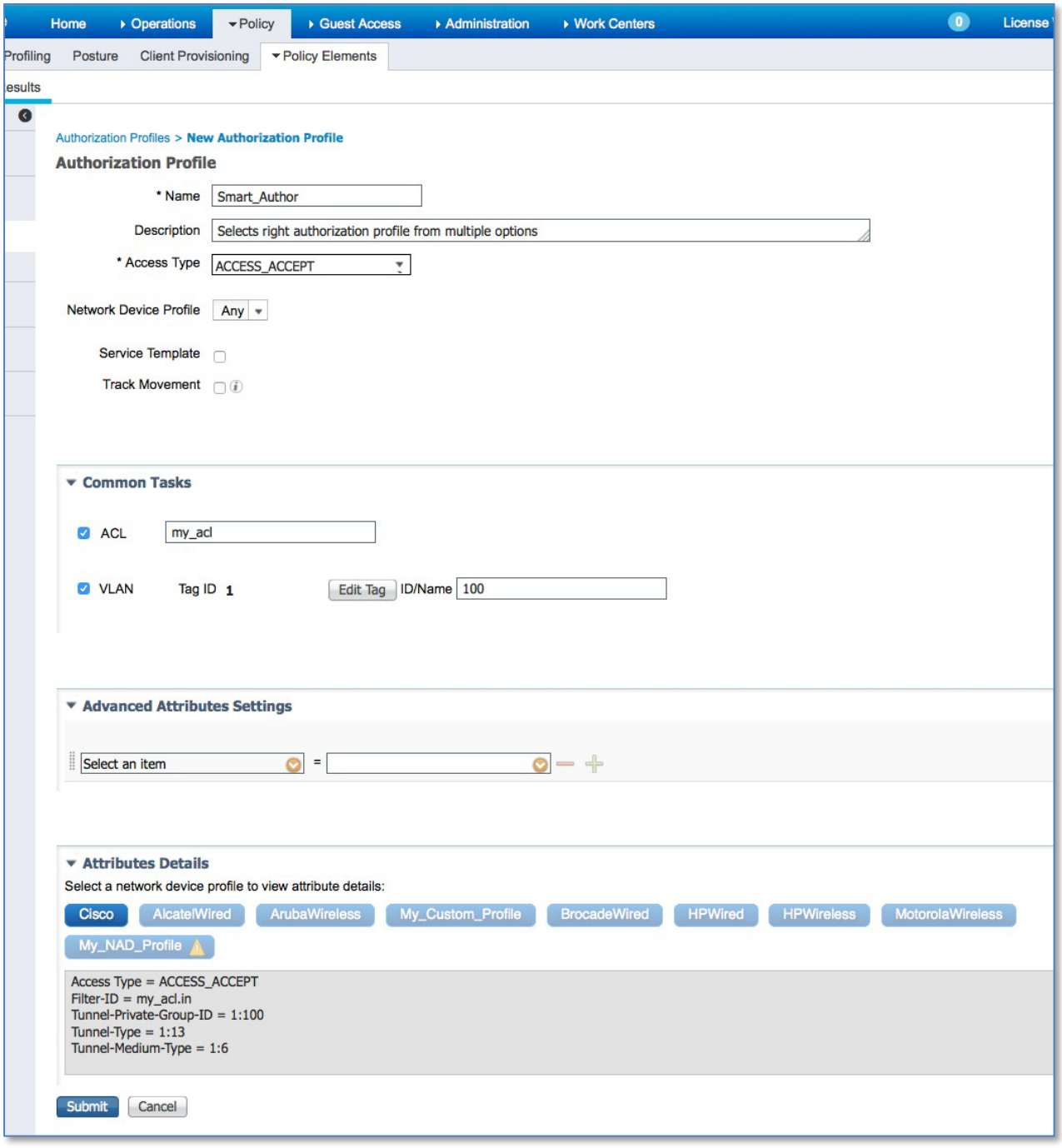

图 16. 智能授权配置文件

© 2015 思科系统公司

验证行为

一旦您已创建新的 NAD 配置文件并将 ISE 的策略配置为使用该配置文件，就应验证相关流程是否按预期工作。此外，建议验证使用其他 NAD 配置文件的设备是否仍然按预期工作。ISE 的监控/报告中的“步骤”(STEPS) 详细信息具有 ISE 2.0 中的附加信息，可帮助您了解使用的是哪个 NAD 配置文件，以及检测到的可帮助故障诊断的流程类型。

© 2015 思科系统公司