美洲台：LDAP与ACS集成的配置示例

目录

简介

本文档提供的示例配置步骤将演示如何配置 Beacon 和 ACS，以使配置了 MAB 功能的 Cisco 设备能够在已通过身份验证的网络中对不支持 802.1x 的设备高效地执行有效验证。

Cisco 已在其交换机上实现 MAC 身份验证旁路 (MAB) 功能，并在 ACS 中提供了必要支持，以便无法通过 802.1X 身份验证的端点能够访问支持 802.1X 的网络。此功能可确保未配备 802.1X 功能（如没有有效的 802.1X 请求方）且尝试连接到支持 802.1X 的网络的端点可以在许可之前得到身份验证，并在其连接中强制执行基本网络使用策略。

通过 MAB 可将网络配置为当标识的设备无法参与 802.1X 协议时允许此设备将其 MAC 地址用作主要凭证。为了有效地部署和使用 MAB，环境必须能够标识环境中不支持 802.1X 身份验证的设备，并在发生设备移动、添加和更改时随时维护这些设备的最新数据库。需要在身份验证服务器 (ACS) 中手动填充和维护此列表，或者通过一些其他方法进行填充和维护，以确保基于 MAC 身份验证的设备随时完整有效。

信标终端仿形铣床能自动化非正在验证终端，那些，不用802.1X恳求者和这些终端正确性的维护的识别的进程在变化的缩放网络的在终端描出和行为监控功能的。通过标准 LDAP 接口，Beacon 系统可以用作端点的外部数据库或目录，以通过 MAB 进行验证。当接收到来自边缘基础架构的 MAB 请求时，ACS 可以查询 Beacon 系统，以根据 Beacon 已知的端点的最新相关信息确定是否应允许给定端点访问网络，从而避免手动配置的需要。

参考的美洲台：与ACS 5.x的LDAP集成及以后配置示例欲知更多信息和一相似的配置使用ACS

5.x和以后。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 12.2(25)SEE2 的 Cisco 交换机 3750
- 用于 Windows 4.1 的 Cisco 安全访问控制服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

MAB 是一项重要功能，可为打印机、IP 电话、传真机等设备以及 802.1X 之后的环境部署中不支持 802.1X 的其他设备提供动态支持。如果没有 MAB 功能，对于连接至不支持 802.1X 的端点的网络接入端口，必须进行静态设置以免尝试 802.1X 身份验证，或者通过使用提供极其有限的策略选项的其他功能来进行设置。显然，这样注定了无法在大型企业环境中进行扩展。如果在所有接入端口上同时启用 MAB 和 802.1X，那么不支持 802.1x 的已知端点可以移至环境中的任意位置，并且仍能可靠（安全）地连接到网络。由于允许访问网络的设备已通过身份验证，因此可以对不同设备应用不同策略。

此外，如有必要，还可以通过 MAB 向环境中不支持 802.1X 的未知端点（例如，访客或承包商的便携式计算机）提供对网络的有限访问权限。

顾名思义，MAC 身份验证旁路使用端点的 MAC 地址作为主要凭证。在接入端口上启用 MAC 身份验证旁路后，如果端点连接且无法响应 802.1X 身份验证要求，该端口将恢复为 MAB 模式。尝试对端点执行 MAB 的交换机使用站点的 MAC 向 ACS 发出标准 RADIUS 请求。在允许端点访问网络之前，该交换机会尝试连接到网络，并请求 ACS 对该端点进行身份验证。

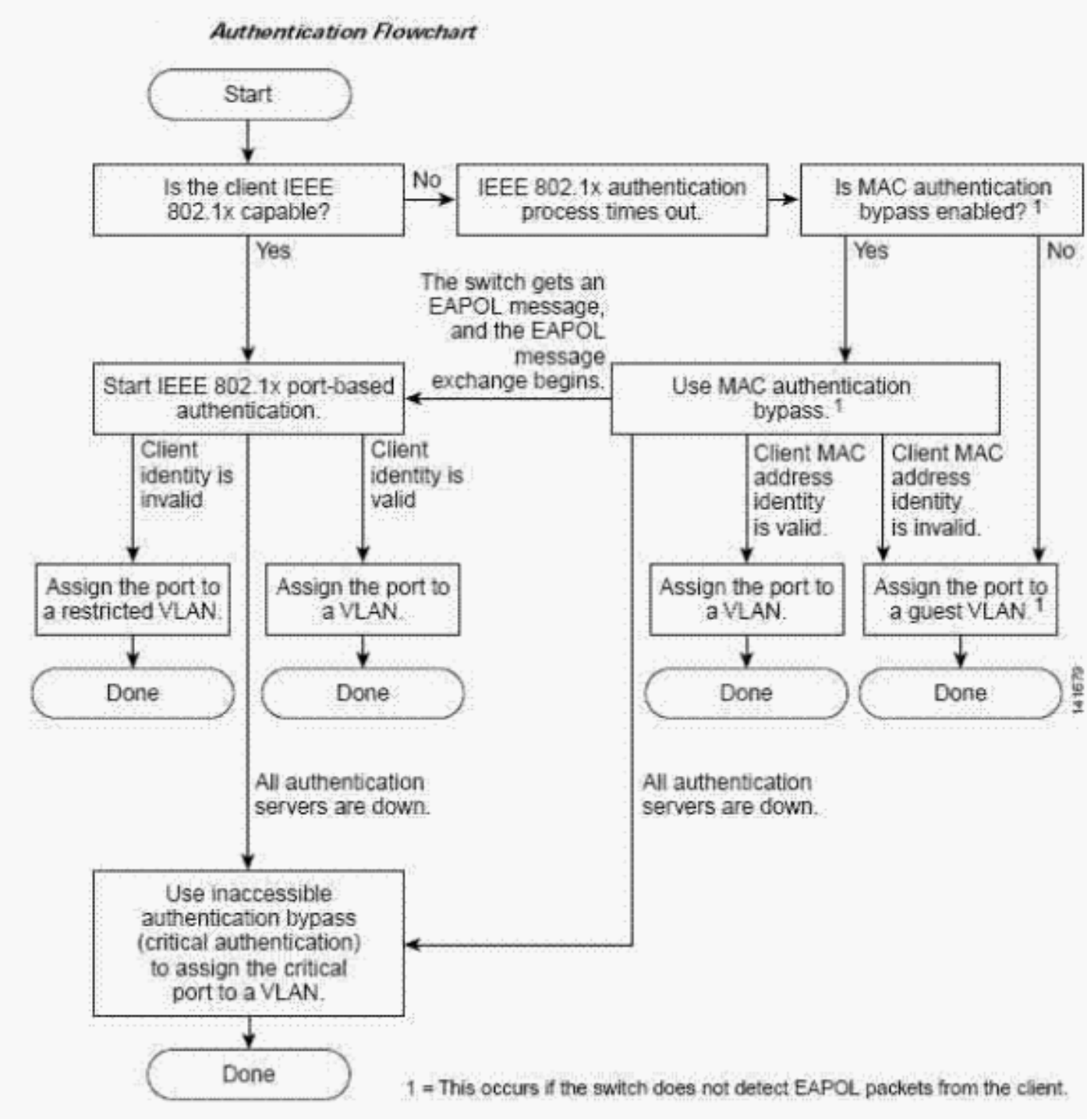
配置

流程图图表

以下流程图摘自 Cisco Systems 文档，该图说明当新的端点尝试连接到网络时，如何在 Cisco 边缘基础架构中配合使用 MAB 和 802.1X 身份验证。

本文档使用以下流程图工作流：

图 1：身份验证流程



可以对 ACS 进行配置，使其使用自己的内部数据库或外部 LDAP 服务器验证 MAC 地址用户请求。默认情况下，Beacon Endpoint Profiler 系统完全启用 LDAP，并且可供 ACS 使用，以通过标准 LDAP 功能验证 MAC 地址用户请求。由于 Beacon 能自动发现和分析网络上的所有端点，因此 ACS 可以通过 LDAP 查询 Beacon，以便确定是否应允许 MAC 访问网络，以及应将端点映射到哪个组。这会自动执行 MAC 身份验证旁路功能，并大幅提高此功能的性能，在大型企业环境中尤其如此。

通过 Beacon 提供的行为监视功能，如果被监视设备的行为与已启用 MAB 的配置文件不一致，则会将这些设备转至已启用 LDAP 的配置文件之外，从而使下次常规重新验证尝试失败。

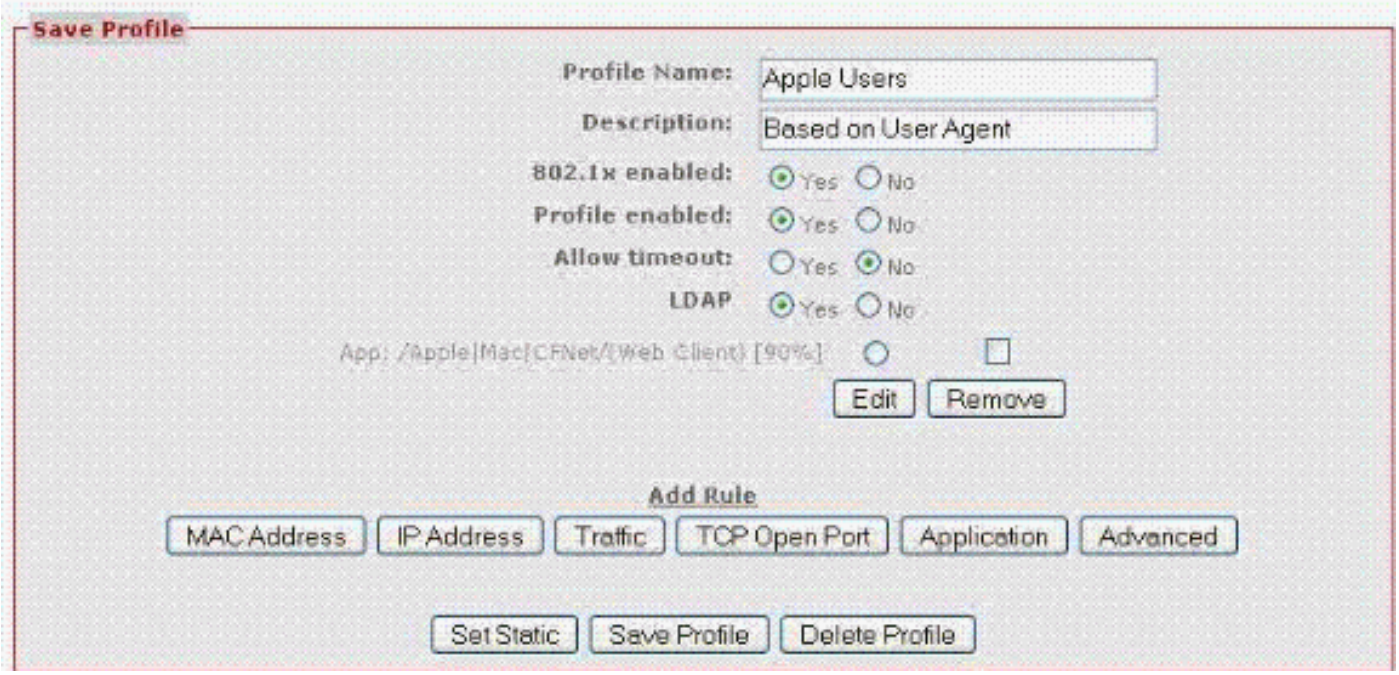
Beacon Endpoint Profiler 系统的 MAB 配置

为了支持 MAB 而配置 Beacon 系统来集成 ACS 的过程非常简单，因为在默认情况下已启用 LDAP

功能。主要配置任务是标识包含环境中要通过 MAB 身份验证的端点的配置文件，并对这些配置文件启用 LDAP。对于包含组织所拥有的设备的 Beacon 配置文件，如果在端口上看到的这些配置文件无法通过 802.1X 身份验证，通常应向这些配置文件提供网络访问权限。例如，这些配置文件通常包含打印机、IP 电话或可管理的 UPS。

例如，如果将 Beacon 分析的打印机放在名为 *Printers* 的配置文件中，并将 IP 电话放置在名为 IP Phones 的配置文件中，则需要对这些配置文件启用 LDAP，以便在环境中通过 MAB 将这些配置文件中的端点作为已知 IP 电话和打印机进行成功身份验证。若要对配置文件启用 LDAP，则需要在端点配置文件配置中选中 LDAP 单选按钮，如下例所示：

图 2：对配置文件启用 LDAP



当 ACS 通过 LDAP 委托 Beacon 执行 MAC 身份验证时，查询包括二个子查询，这两个子查询必须返回有效的非空结果。对 Beacon 的首个查询是 Beacon 是否已知 MAC，例如是否已发现 MAC 并将其添加到 Beacon 数据库中。如果 Beacon 尚未发现此端点，此端点则视为未知。如果 Beacon 尚未发现端点，且该端点不在 Beacon 数据库中，则不必执行第二个查询。如果该端点已被发现且位于 Beacon 数据库中，下一个查询将确定该端点的当前配置文件。如果该端点尚未经过分析，或者当前位于未启用 LDAP 的配置文件中，则会向 ACS 返回未知结果，并且 Beacon 对该端点的身份验证将失败。这取决于 ACS 的配置方式，并且可能导致完全拒绝设备对网络的访问权限，或者向该设备指定适用于未知设备或来宾设备的策略。

仅当 MAC 端点已被 Beacon 发现且位于已启用 LDAP 的配置文件中时，才会向 ACS 返回 Beacon 已知且已分析该端点，并以此作为响应。最重要的是 Beacon 会为这些端点提供当前配置文件名称，这使得 ACS 可以将已知端点映射到 Cisco SecureAccess 组。这可以精确确定策略，如有必要，可以为已启用 LDAP 的每个 Beacon 配置文件精确确定一个单独的策略。

为 ACS 配置 MAB 以及使用 Beacon 作为外部用户数据库

为 ACS 配置 MAB 以及使用 Beacon 作为外部用户数据库需要执行三个不同步骤。本文档说明的顺序遵循用于执行 MAB 完整配置的高效工作流，对于已配置其他身份验证模式的系统，可能有所不同。

配置 Cisco SecureGroup

当对试图连接到网络中的特定端点尝试执行 MAB 时，ACS 会基于 LDAP 查询 Beacon，以确定

Beacon 是否已发现此 MAC 地址，以及 Beacon 当前已将其置于哪个配置文件中，如前文所述。

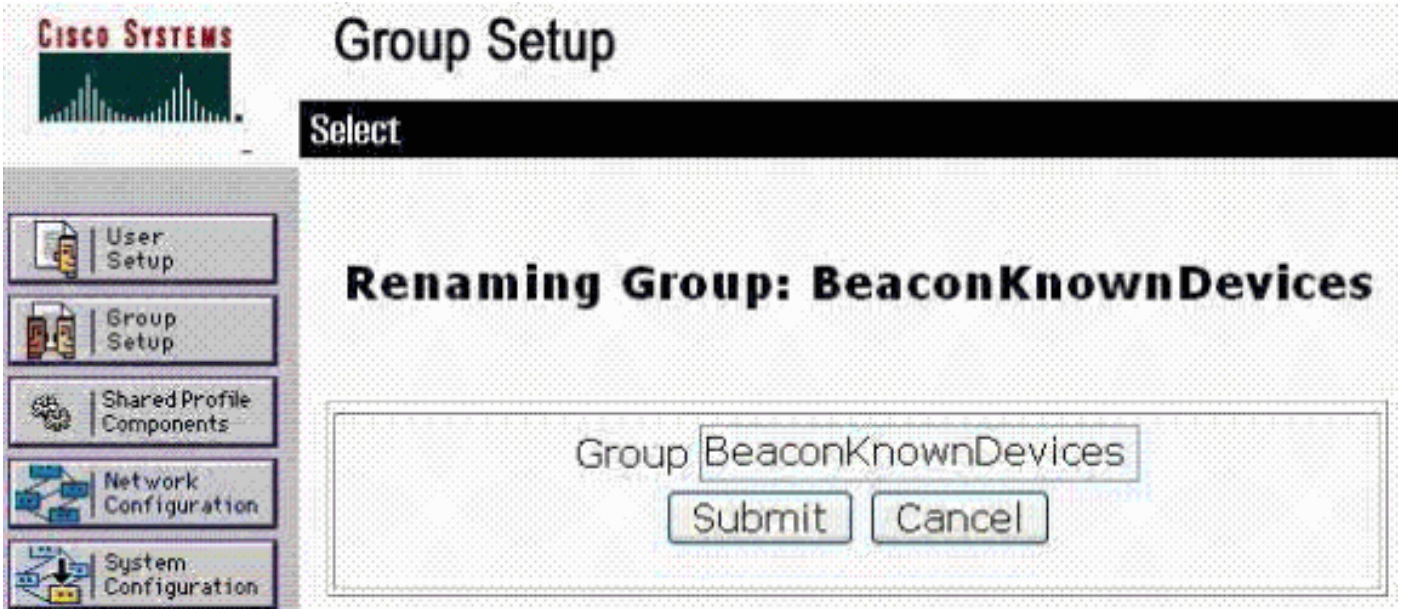
ACS 的 Cisco SecureGroup 机制可用于验证 Beacon 通过 MAB 发现和分析的端点以及验证失败的端点（即 Beacon 未知的设备或当前尚未经过 Beacon 分析的设备），并向这些端点应用策略。

例如，可以在 Beacon 发现和分析的端点的 ACS 配置中添加一个名为 *BeaconKnownDevices* 的组，并为 Beacon 当前未知的设备添加另一个组 BeaconUnknownDevices。Beacon 可能尚未发现这些未知设备的 MAC，或者当前未将其分析到已启用 LDAP 的配置文件中。如下文所示，在端点尝试加入到网络中时，该组允许对这些端点应用策略。

请注意，在本文档概述的示例中，只配置了 BeaconKnown 和 BeaconUnknown 这两个组。但是可以为 Beacon 发现和分析的端点配置多个 SecureGroup（可为 Beacon 中已启用 LDAP 的每个配置文件均配置一个 SecureGroup），其中每个 SecureGroup 均采用不同的策略参数（例如，VLAN 分配）。此外，还可以配置 BeaconUnkown 设备组，以拒绝对 Beacon 尚未发现的端点或尚未放置在已启用 LDAP 的配置文件中的端点的所有访问。如果在 BeaconUnknownDevices 组配置窗口的参数中选中了 Group Disabled 复选框，则可以实现上述功能。

使用 ACS 用户界面中的 Group Setup 按钮，可以开始在 ACS 中创建组。选择其中一个可用组，并选择 **Rename Group** 按钮以将 Group Name 更改为 KnownBeaconDevices，如以下示例所示。单击 **Submit** 以保存更改。

图 3：编辑 CiscoSecure 组

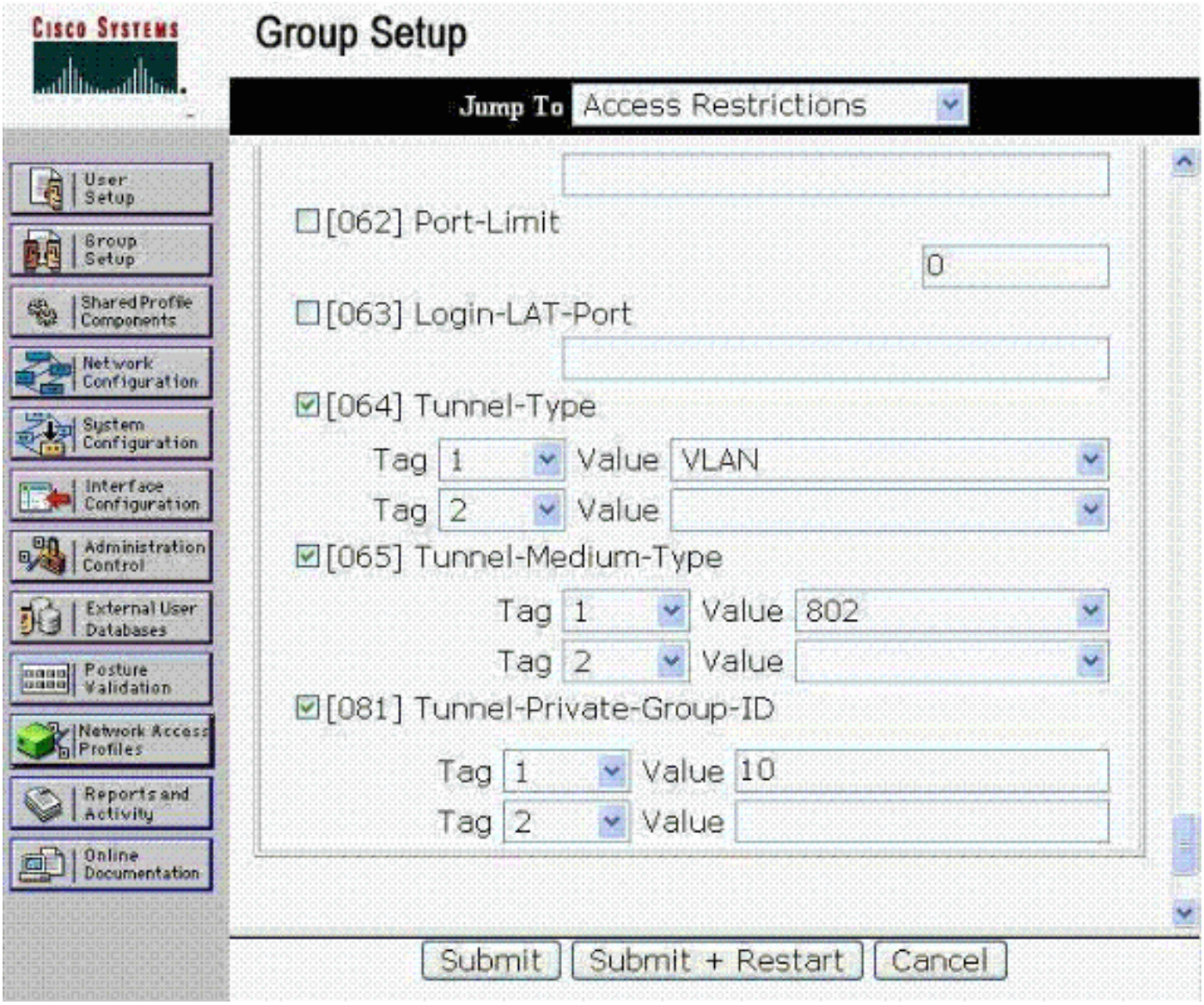


选择 **Edit Settings** 以编辑组设置。根据需要编辑 BeaconKnownDevices 组的参数。对于本文档中的示例而言，更改的组参数仅包括页面底部的 IETF RADIUS 属性。

具体而言，您需要将已通过身份验证的设备指定到此组，Beacon 已分析到配置文件（已选择 MAB 并启用 LDAP）中的 MAC 地址会将策略参数返回到验证的交换机，该交换机允许端点在适当的 VLAN 上访问网络。为此，将设置 RADIUS 属性 064 Tunnel-Type、065 Tunnel-Medium-Type 和 081 Tunnel- Private-Group-ID，以便将端点放置到所需 VLAN 中，如图 4 所示。

确保选中每个 RADIUS 属性旁边的复选框。

图 4：组 VLAN 属性

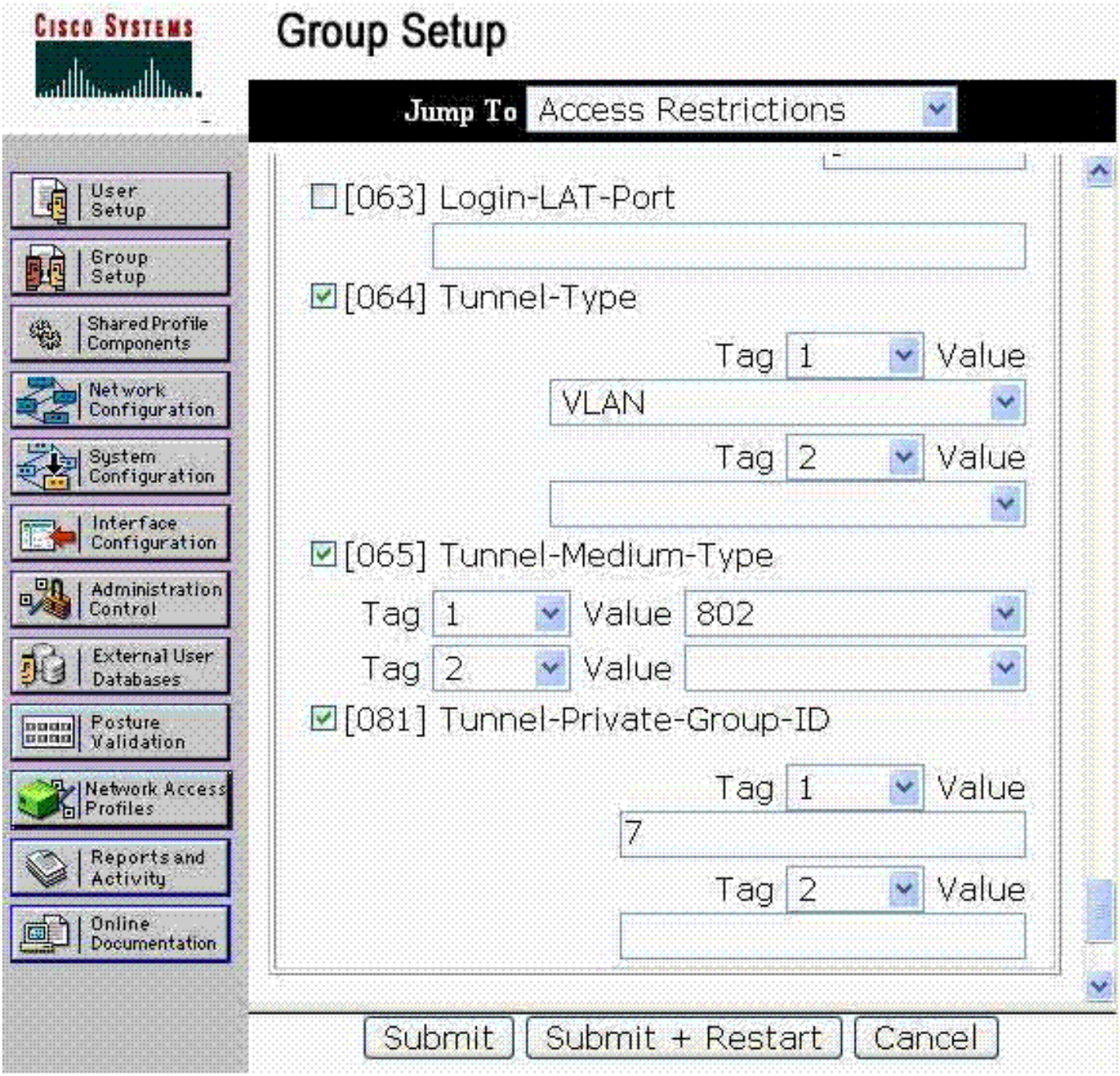


在显示的示例中，通过将 Beacon 用作外部用户数据库，已成功通过 Beacon 验证并随后分配到 ACS BeaconKnownDevices 组中的端点将在连接到网络并基于 MAB 成功通过 ACS 验证时放置到 VLAN 10（即网络配置示例中的授权 VLAN）中。

同样，将按照所示内容为 Beacon 当前未知的设备创建 BeaconUnknownDevices 组。同样，如果这些设备不应获取对网络的访问权限，您只需选中窗体顶部的 **Group Disabled** 复选框即可。对于 Beacon 未发现的端点或 Beacon 当前未分析到已启用 LDAP 的配置文件中的端点，将在执行 MAB 时失败，且被禁止访问网络。

此图显示在不选中 Group Disabled 复选框时的示例。在这种情况下，无法通过 Beacon 验证的端点被分配到已启用的组中，但其策略不同于已知端点的策略。请参阅图 5。

图 5：BeaconUnknownDevices 的 VLAN 参数



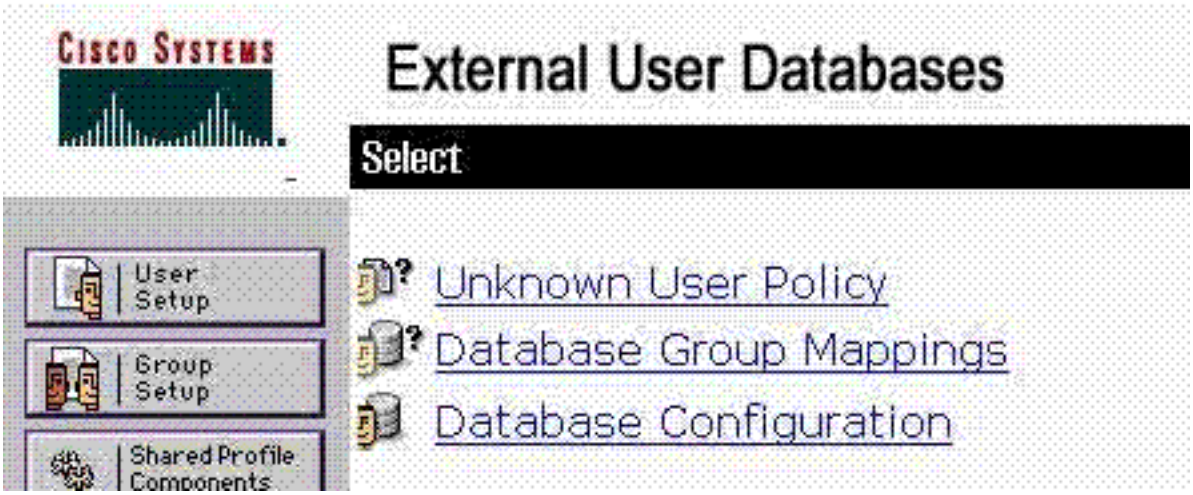
请注意，尽管本示例中的未知设备可以访问网络，但将被归类到来宾或受限 VLAN（即 VLAN 7）中。在此示例网络中，VLAN 7 为来宾 VLAN，它仅允许端点访问 Internet，而禁止其访问内部资源。

当 ACS 请求 Beacon 验证 Beacon 尚未发现或分析的端点的 MAC 时，ACS 会将 MAC 放置在此组中，并将结果返回到已启用 MAB 的验证交换机。

ACS 外部用户数据库配置

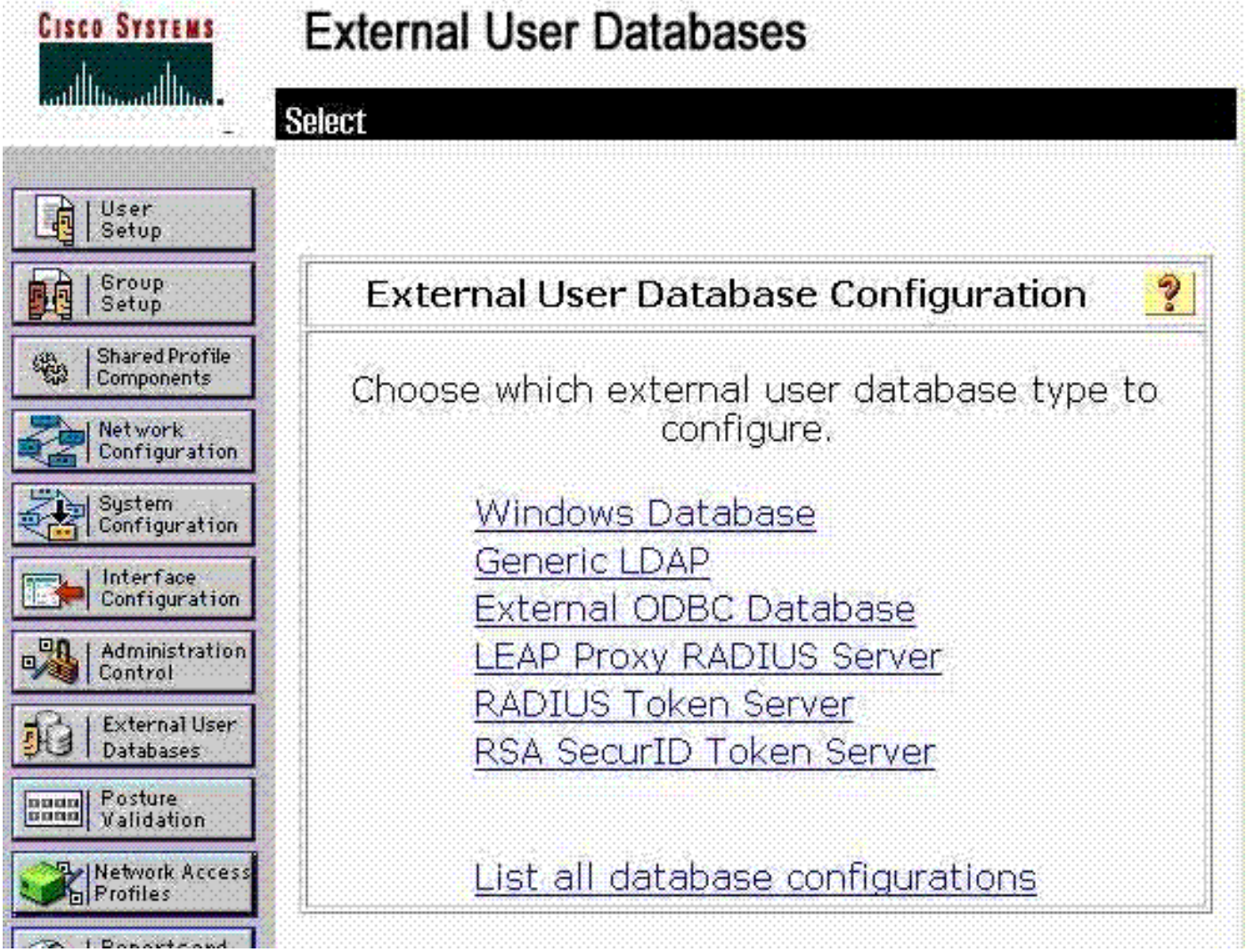
必须配置 ACS，以便通过 LDAP 将来自接入交换机的 MAB 请求委托给 Beacon。这要求 ACS 配置中包含 Beacon 系统并将其作为通用 LDAP 外部用户数据库。本部分概述的步骤说明如何将 Beacon Endpoint Profiler 系统添加为外部用户数据库，以供 ACS 在接收 MAB 请求时查询。在全局导航窗格中选择 **External User Database**，以便显示图 6 所示的 External User Database 窗口。

图 6：外部数据库配置主屏幕



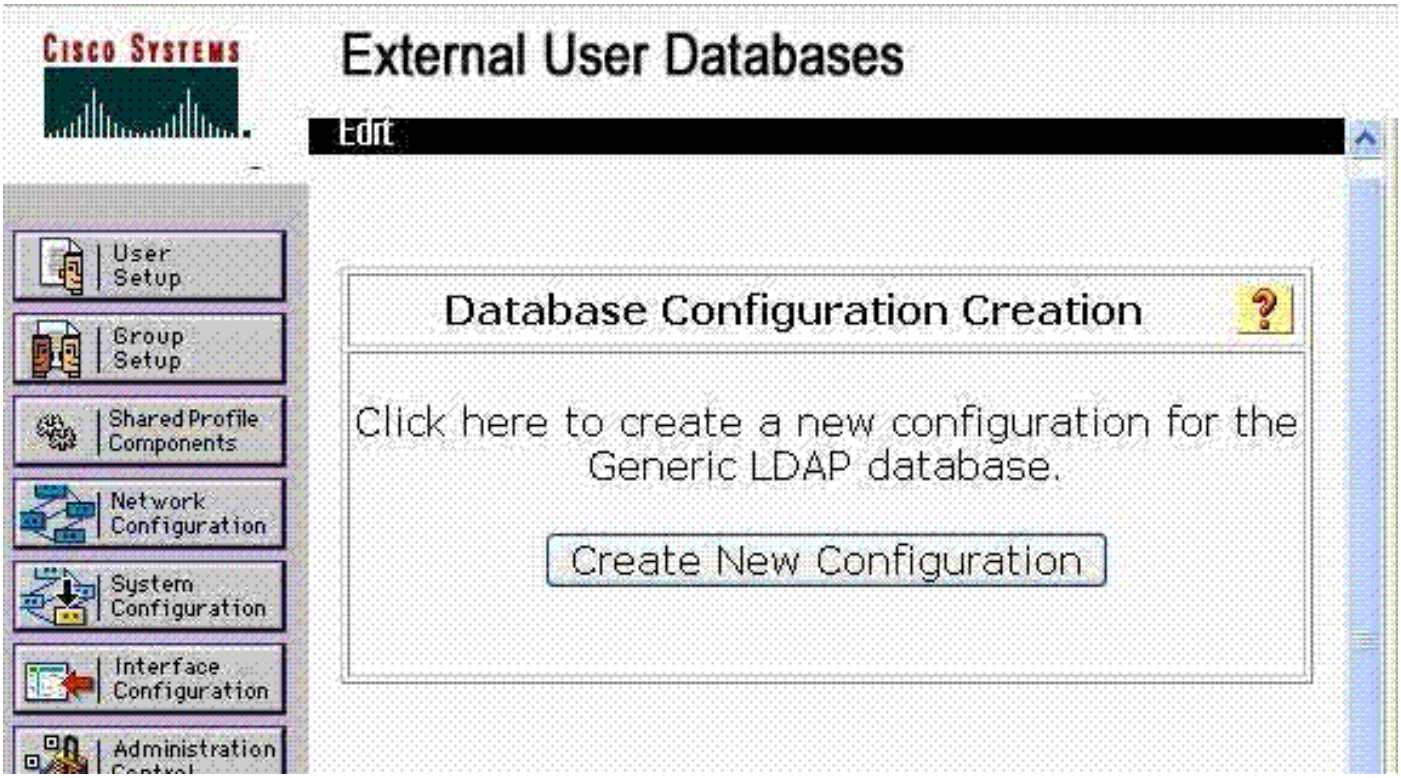
将 Beacon 配置为外部用户数据库的首要任务是将 Beacon 系统添加为通用 LDAP 外部用户数据库。选择 **Database Configuration** 以显示如图 7 所示的窗口。

图 7：ACS 外部用户数据库配置



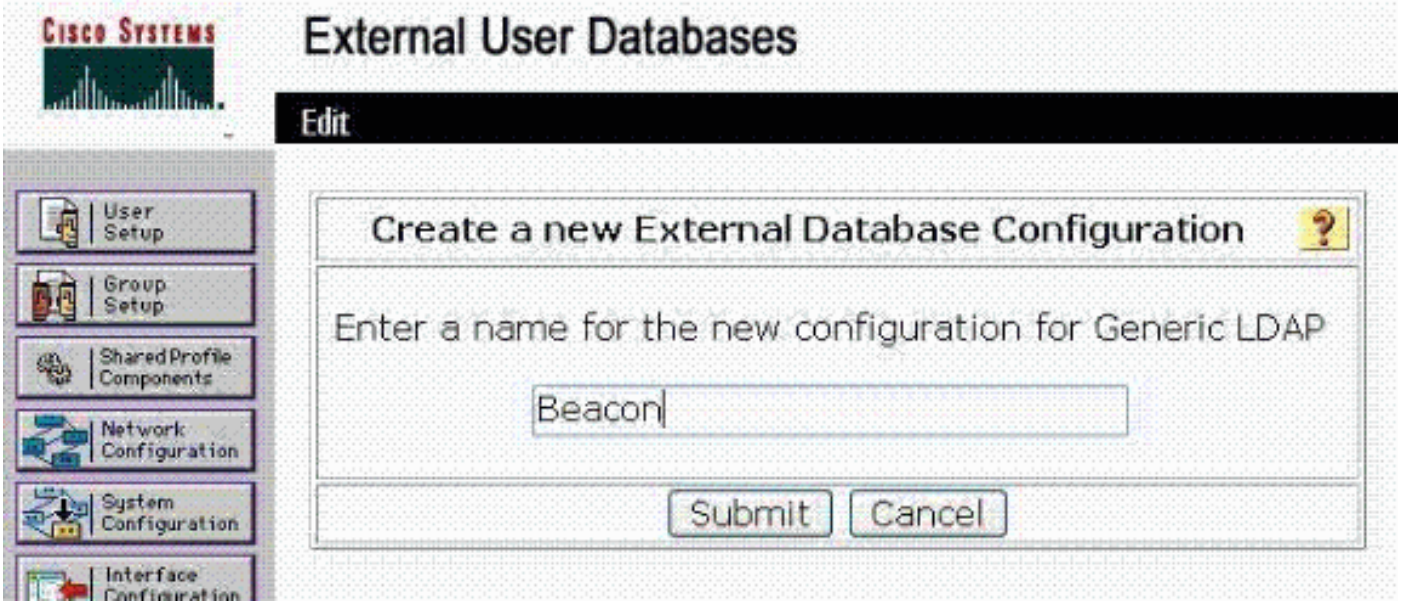
选择 **Generic LDAP** 以打开相关窗体，从而在 ACS 配置中将 Beacon Endpoint Profiler 系统添加为外部用户数据库。此时将显示以下窗口，您可以在该窗口中新建通用 LDAP 类型的外部用户数据库配置。

图 8：创建数据库配置



选择 **Create New Configuration** 按钮以便为 Beacon 创建通用 LDAP 数据库。此时将显示以下窗口，您可以在该窗口中命名新的外部数据库。

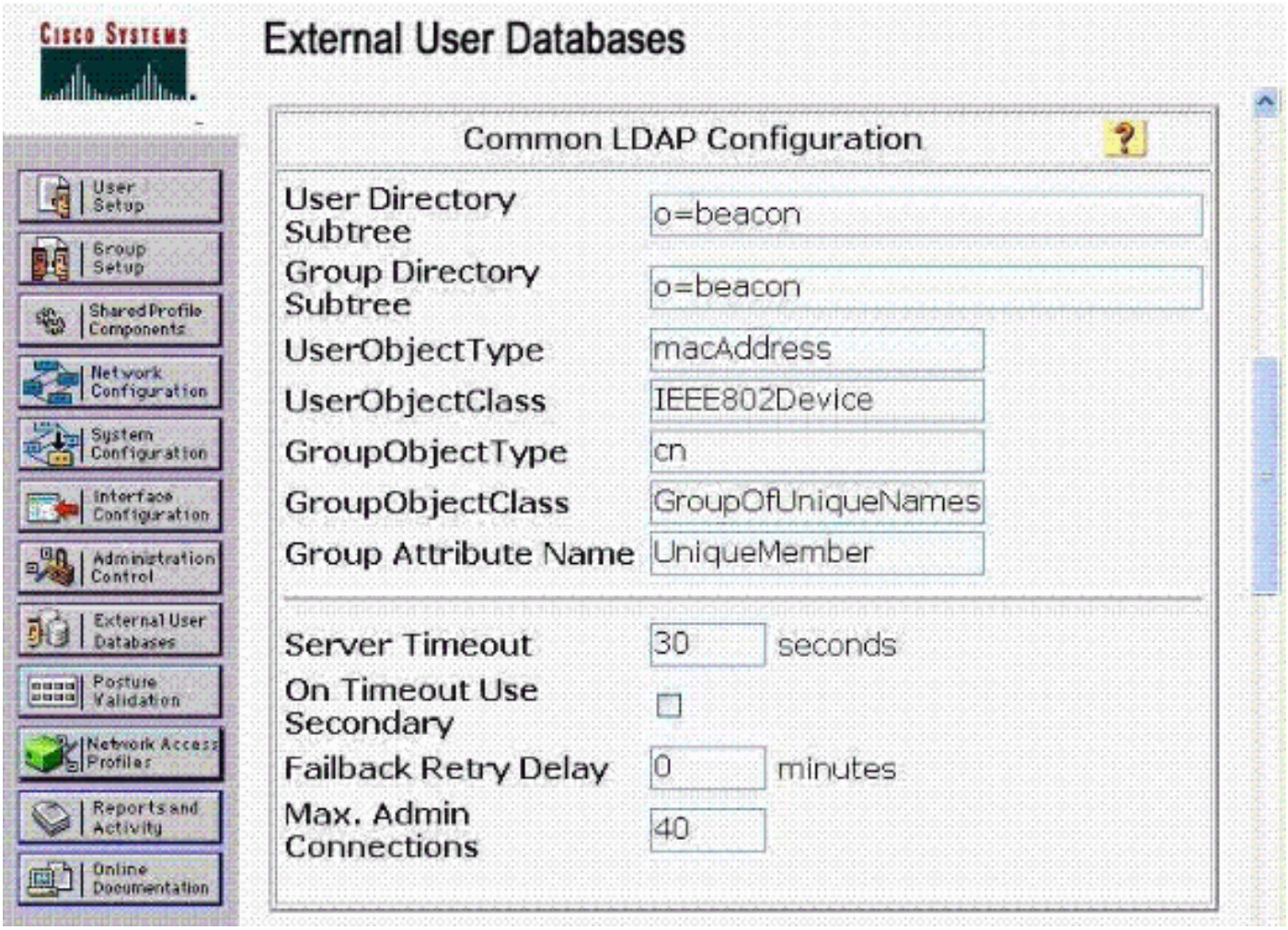
图 9：命名 Beacon 外部用户数据库



输入 Beacon 通用 LDAP 外部数据库的名称，将其与配置中的其他外部数据库轻松区分开来。选择 **Submit** 以继续输入所需的 LDAP 参数，使用这些参数可以在 ACS 和 Beacon 之间通信，以便使用 Beacon 数据库信息验证 MAC 地址。

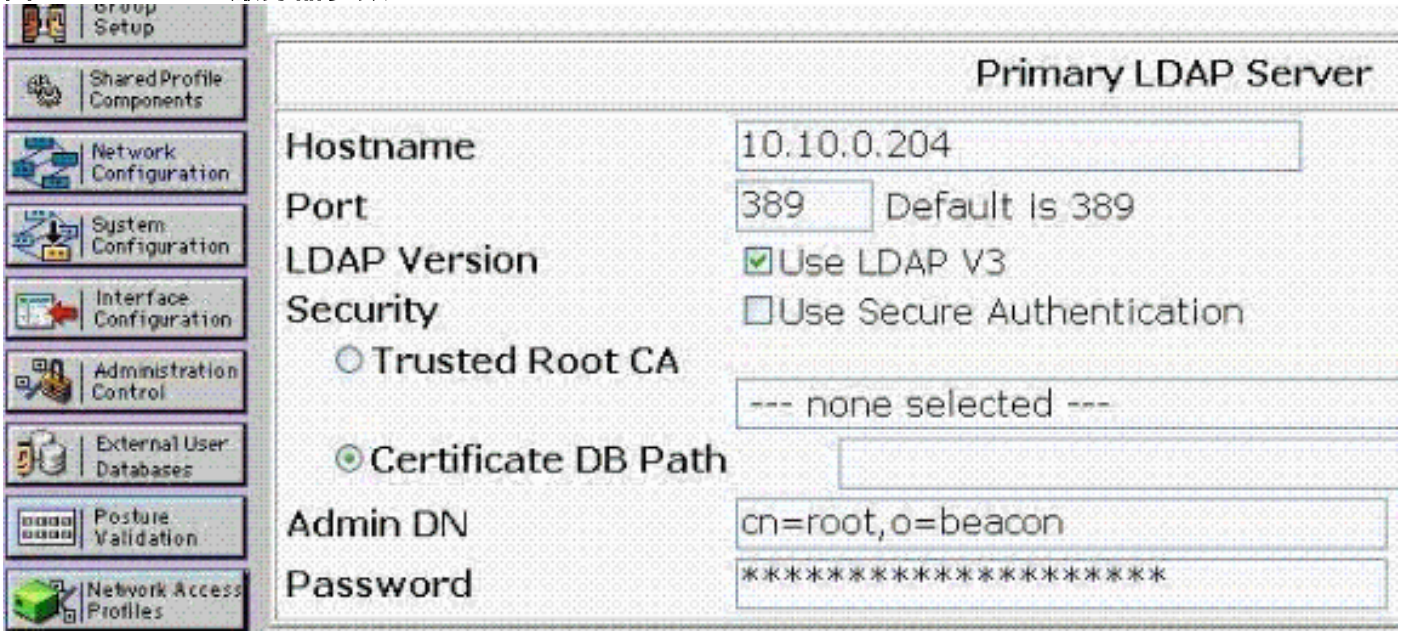
图 10 说明必须为 ACS 配置中添加的 Beacon 通用 LDAP 外部用户数据库输入的常见 IDAP 配置参数。请注意，这些参数向 ACS 提供通过 LDAP 查询 Beacon 时所需的信息。应按照该图所示内容正确输入这些参数，以便在 ACS 和 Beacon Endpoint Profiler 之间通信。

图 10：常见 Beacon IDAP 配置



注意： 请使用口令 **GBSbeacon** 作为 LDAP 绑定口令。请在图 11 所示的窗体底部输入该口令。

图 11：Beacon 服务器参数



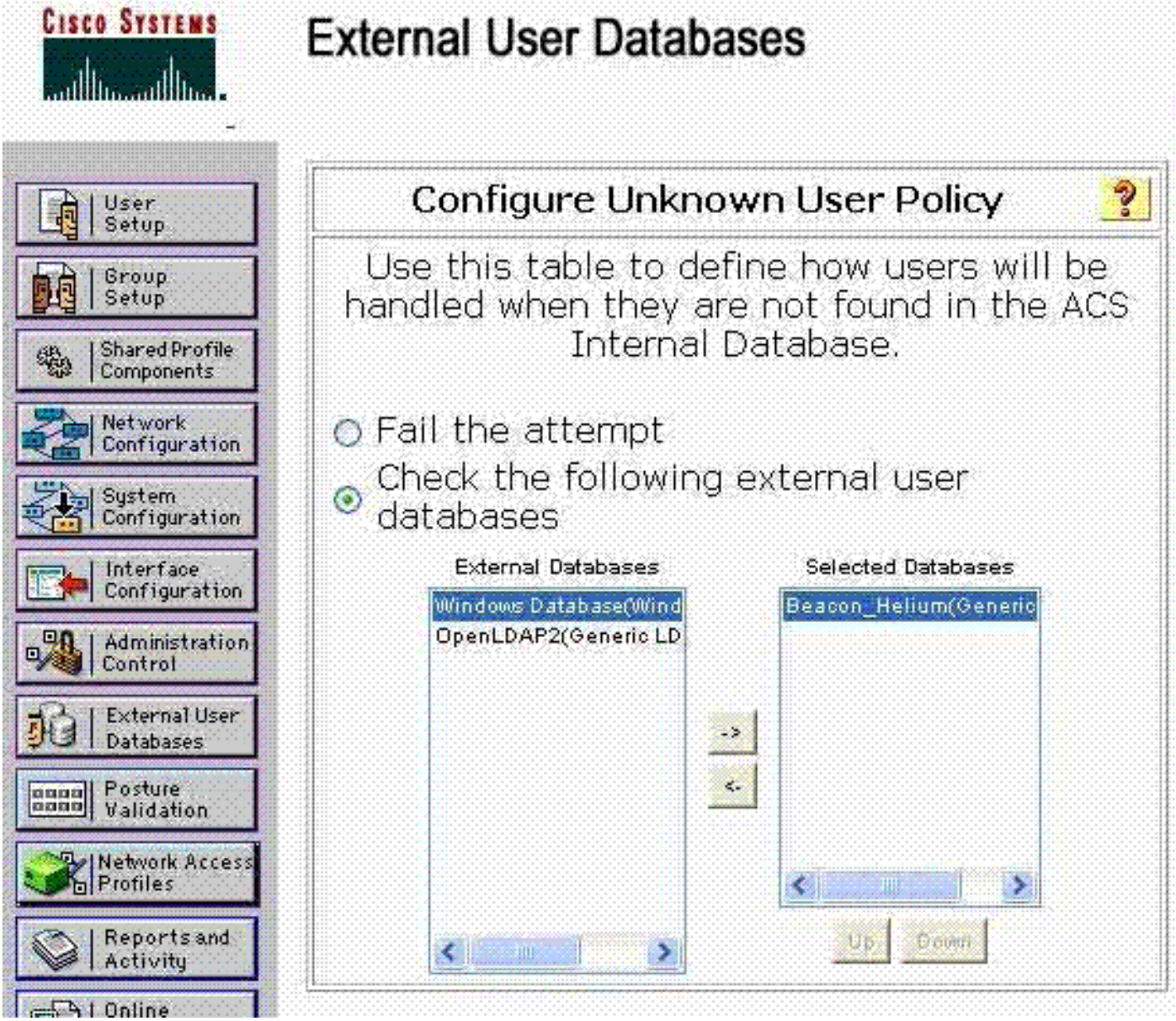
将 Beacon 配置为外部用户数据库的第二个相关配置任务是配置未知用户策略。当 ACS 收到用户的验证请求（如果为 MAB，则为 MAC 地址）时，如果在自己的数据库中没有有关此请求的信息，未知用户策略将指示 ACS 查询 Beacon 数据库。

请注意，在典型的 ACS 部署中，可能已配置了现成的外部用户数据库，并且可能已将该部署配置为在提交未知用户凭证时查询这些数据库。必须将 Beacon 外部用户数据库添加到此列表中，以便

在交换机请求对各 MAC 地址执行 MAB 时查询该数据库。

下列各图概述未知用户策略的配置工作流，以及如何将 Beacon 添加为外部用户数据库以供查询。在图 6 所示的 External User Database 主页上选择 **Unknown User Policy** 链接以便开始此工作流。

图 12：配置未知用户策略

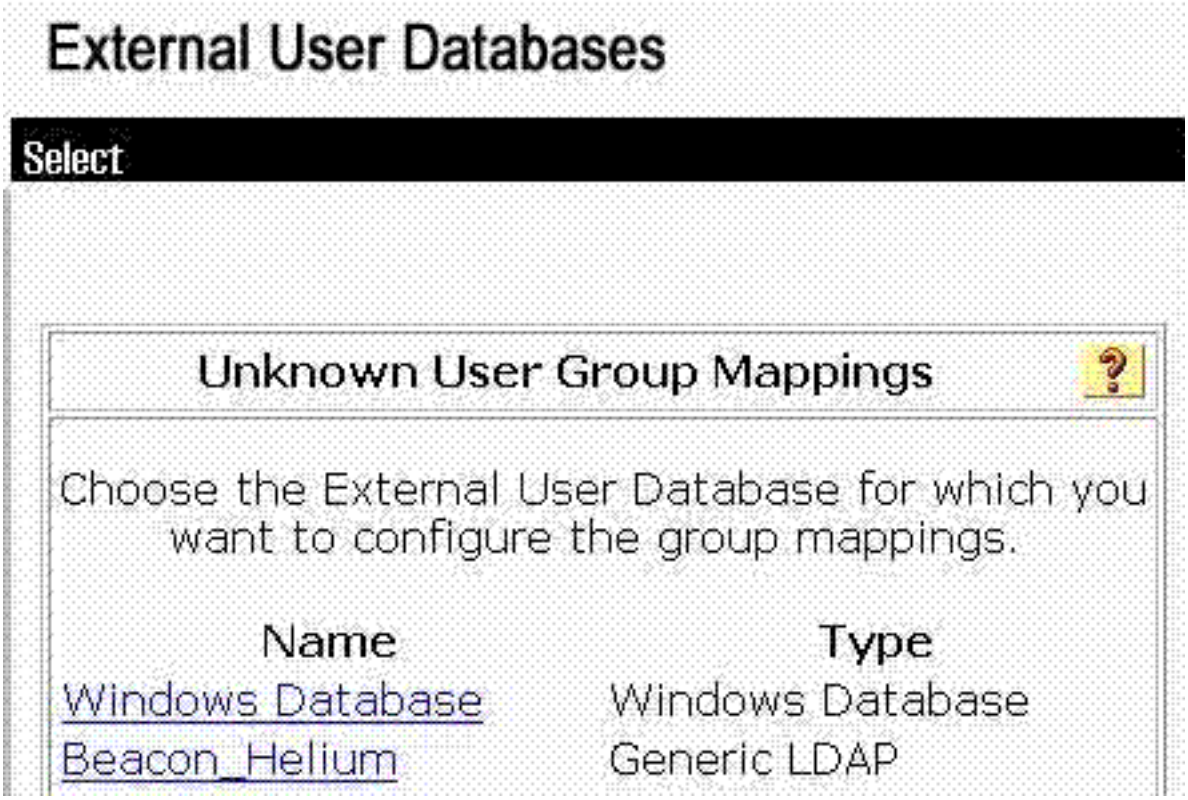


从示例左侧的 External Databases 列表中选择在上一步骤中添加到 ACS 配置的 Beacon 通用 LDAP 数据库 (Beacon_Helium)。使用 **- >** 将其移至 Selected Databases。确保选中 **Check the following external user databases** 单选按钮。这可以确保当交换机向 ACS 提交要验证的 MAC 地址时，ACS 会查询 Beacon 以确定相应端点是否是已知的，以及是否具有最新的配置文件（如果有）。

将 Beacon 添加为外部用户数据库的最终配置任务是完成数据库组映射。从本质上而言，此映射会将创建的 CiscoSecure 组（如 BeaconKnownDevices 和 BeaconUnknownDevices）绑定到对 Beacon 执行的成功和失败的 LDAP 查询，以使交换机尝试的每次 MAB 都会导致 ACS 将端点分配到 CiscoSecure 组中。这样，ACS 便可以对交换机发出的是否应允许端点访问网络的询问做出响应，并在允许的情况下指示应采用何种策略（如 VLAN 属性）。

在图 6 所示的 External User Databases 主页上选择 **Database Group Mappings**，以便配置映射。

图 13：数据库组映射

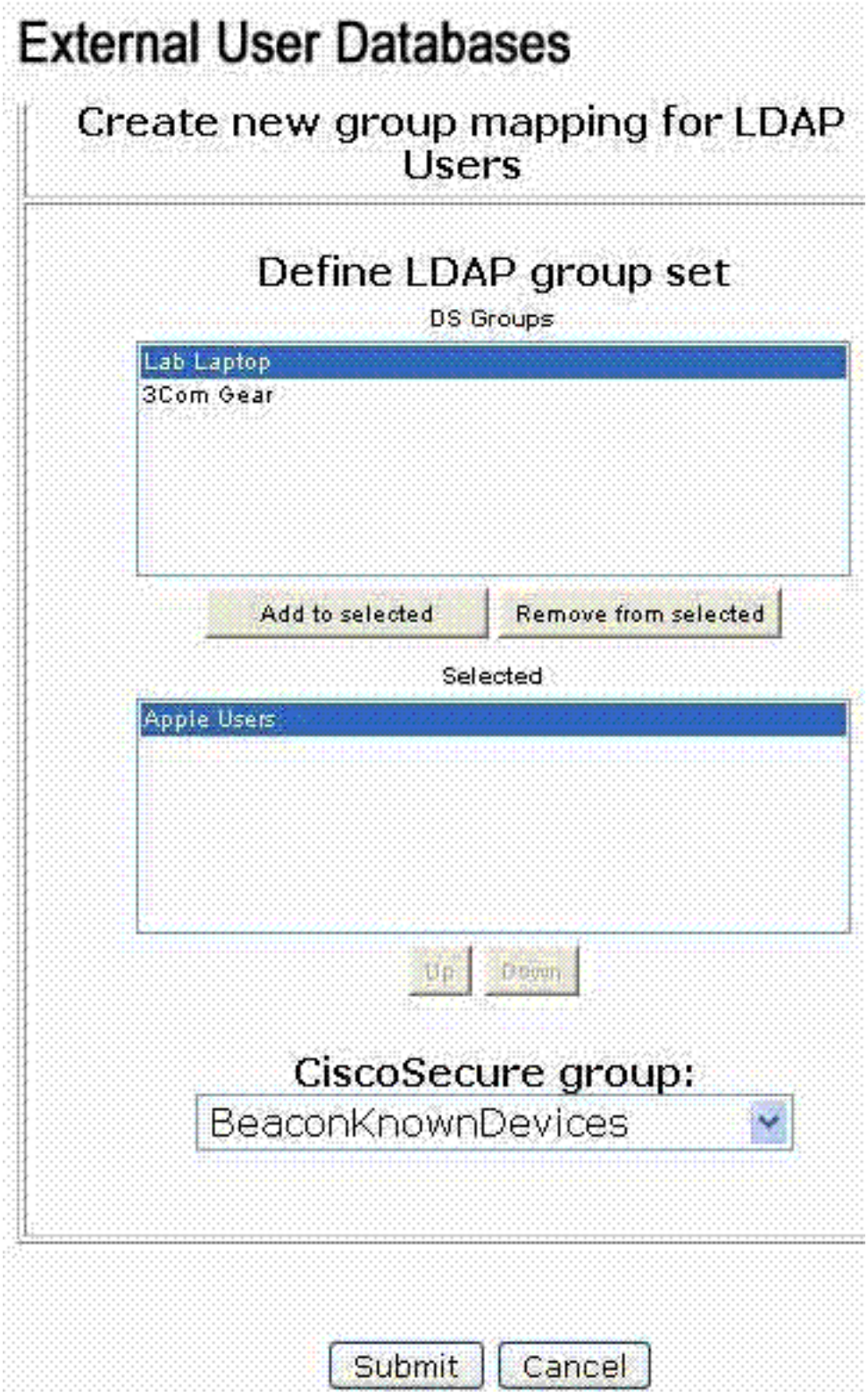


当通过选择上述示例中的 Beacon_Helium 链接来选择在此部分前面创建的 Beacon 外部用户数据库时，将显示图 14 所示的窗口。请注意，在 Beacon 系统配置中，按照上述配置说明第一部分中的介绍启用了 LDAP 的所有 Beacon 配置文件都会填充在 DS Groups 中，以供在 ACS 中创建映射时选择。如果 ACS 界面中未显示已启用 LDAP 的 Beacon 配置文件的名称，则表示 ACS IDAP 配置有问题。请参阅此部分前面概述的将 Beacon 配置为外部用户数据库的相关说明，特别是 LDAP 参数。

请注意，可通过此界面映射 Beacon 中已启用 LDAP 的各配置文件和在 ACS 中配置的 CiscoSecure 组。此界面允许将已启用 LDAP 的各 Beacon 配置文件映射到一个 CiscoSecure 组中。在本示例中，仅为已启用 LDAP 的 Beacon 配置文件中的已知设备创建了一个组：BeaconKnownDevices。但是，可以创建多个具有自身策略参数的组，以便根据设备当前的 Beacon 配置文件以不同方式进行成功的身份验证。

例如，可以为 BeaconKnownIPPhones 创建一个将返回 VLAN 属性的 CiscoSecure 组，当您加入到网络并通过 MAB 进行验证时，这些属性会将 Beacon IP Phone 配置文件中的端点分配到电话 VLAN。

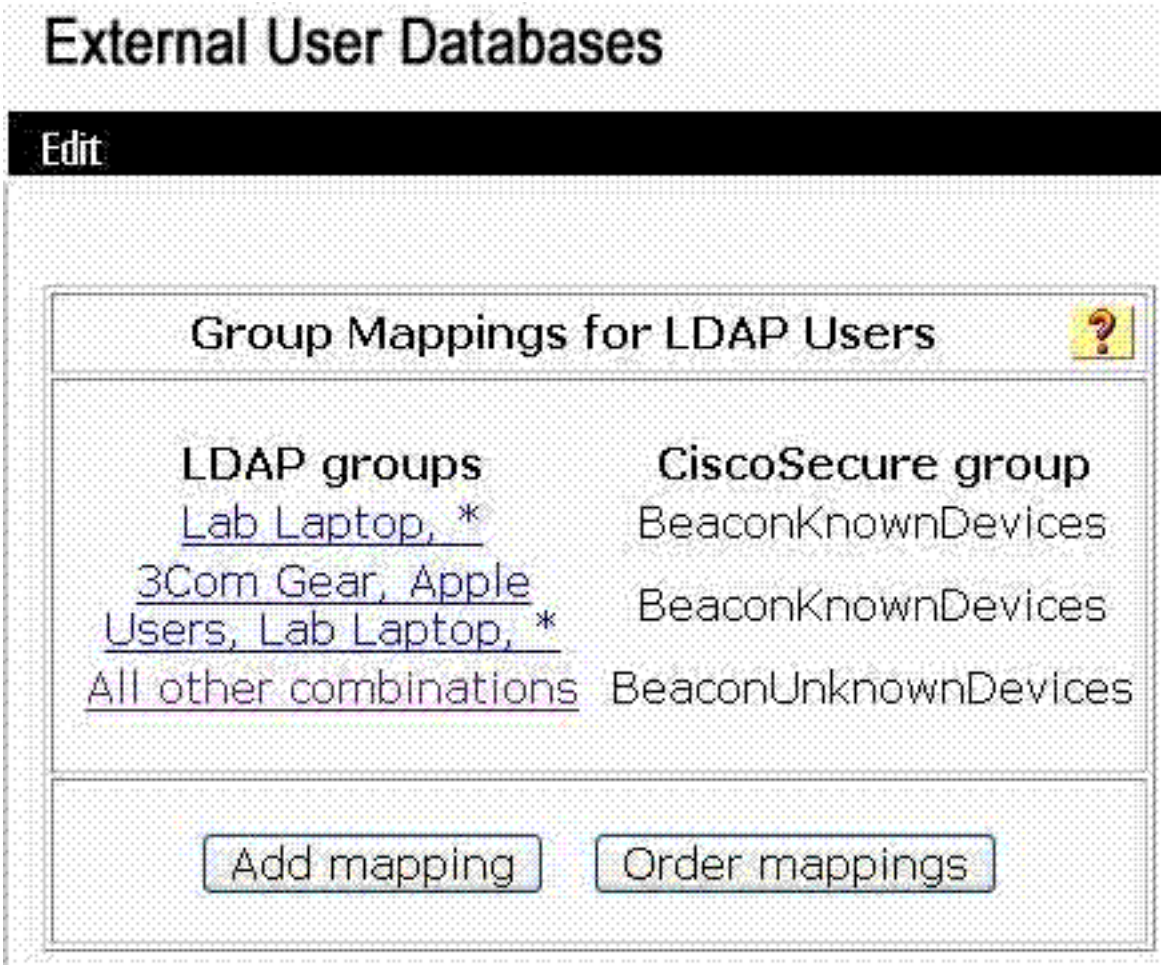
图 14：配置文件与组之间的映射



选择一个 DS 组（已启用 LDAP 的 Beacon 配置文件），并将该配置文件中的端点分配到下拉菜单中的所需 CiscoSecure 组中。在以上示例中，通过 MAB 验证当前位于 Beacon 的 Apple Users 配置文件中的 MAC 地址，并将其放置在 BeaconKnownDevices 中，这将导致验证成功，并在您加入到网络中时置入到用户 VLAN 中。

选择 Submit 将显示当在 Beacon 外部用户数据库中验证未知用户时 ACS 上的当前组映射列表。

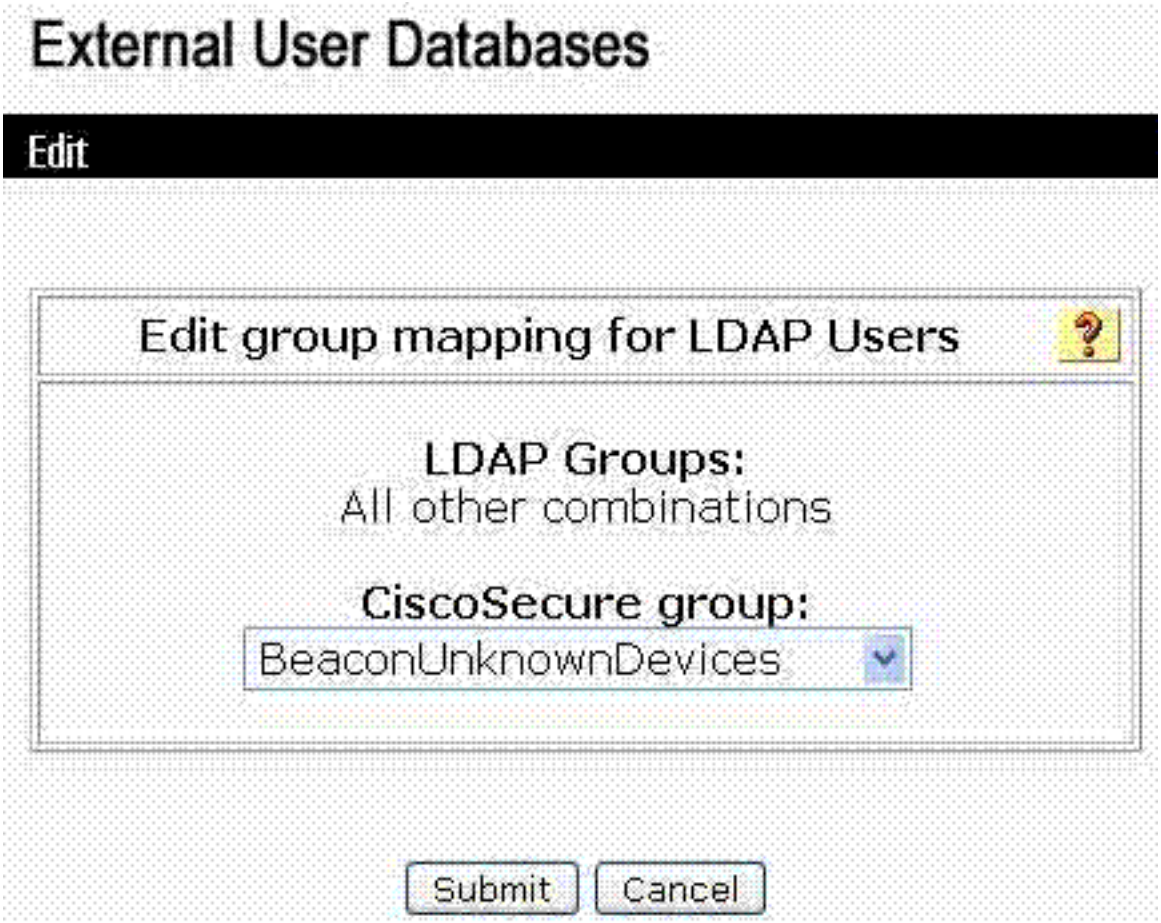
图 15：列出组映射



请注意，此视图中列出了通过前面介绍的过程显式执行的映射。对于 Beacon 尚未发现或尚未放置到已启用 LDAP 的配置文件中的端点所属的组，任何未显式映射到该组中的 DS 组（已启用 LDAP 的 Beacon 配置文件）都会纳入到 All other combinations 收集器中。从本质上而言，这允许将 Beacon 无法提供相关信息的端点纳入到 CiscoSecure 组（如 BeaconUnknownDevices）中。如前文所述，可以完全禁用该组，这会导致 MAB 失败，也可以按照上述示例将该组设计为仅提供对 Beacon 未知端点的有限连接。

如果单击 All other combinations 链接显示以下窗口，则可以向 **All other combinations** 分配一个 CiscoSecure 组 (BeaconUnkownDevices)：

图 16：向 All other combinations 分配组

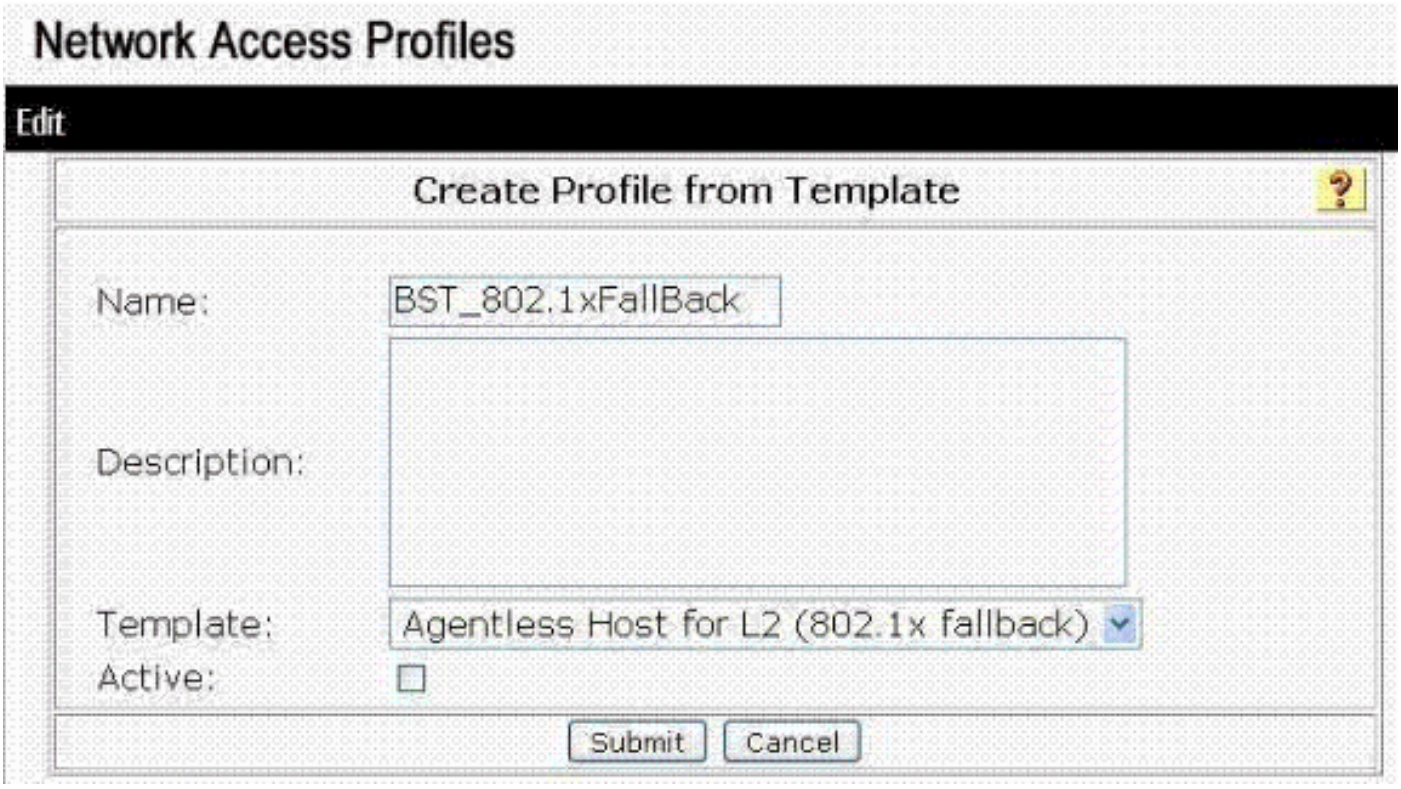


网络访问配置文件配置

在 ACS 的 MAB 配置中，将 Beacon Endpoint Profiler system 系统用作代理的最后一个必要步骤是为 802.1X Fallback 配置网络访问配置文件。请完成下面说明的步骤，配置所需网络访问配置文件以完成 ACS 配置，以便按照前面完成的配置来配置和运行 MAB。

要添加的网络访问配置文件是一个模板配置文件。请从全局导航页面中选择 **Network Access Profiles**。然后选择 **Add Template Profile** 以显示以下所示窗体。

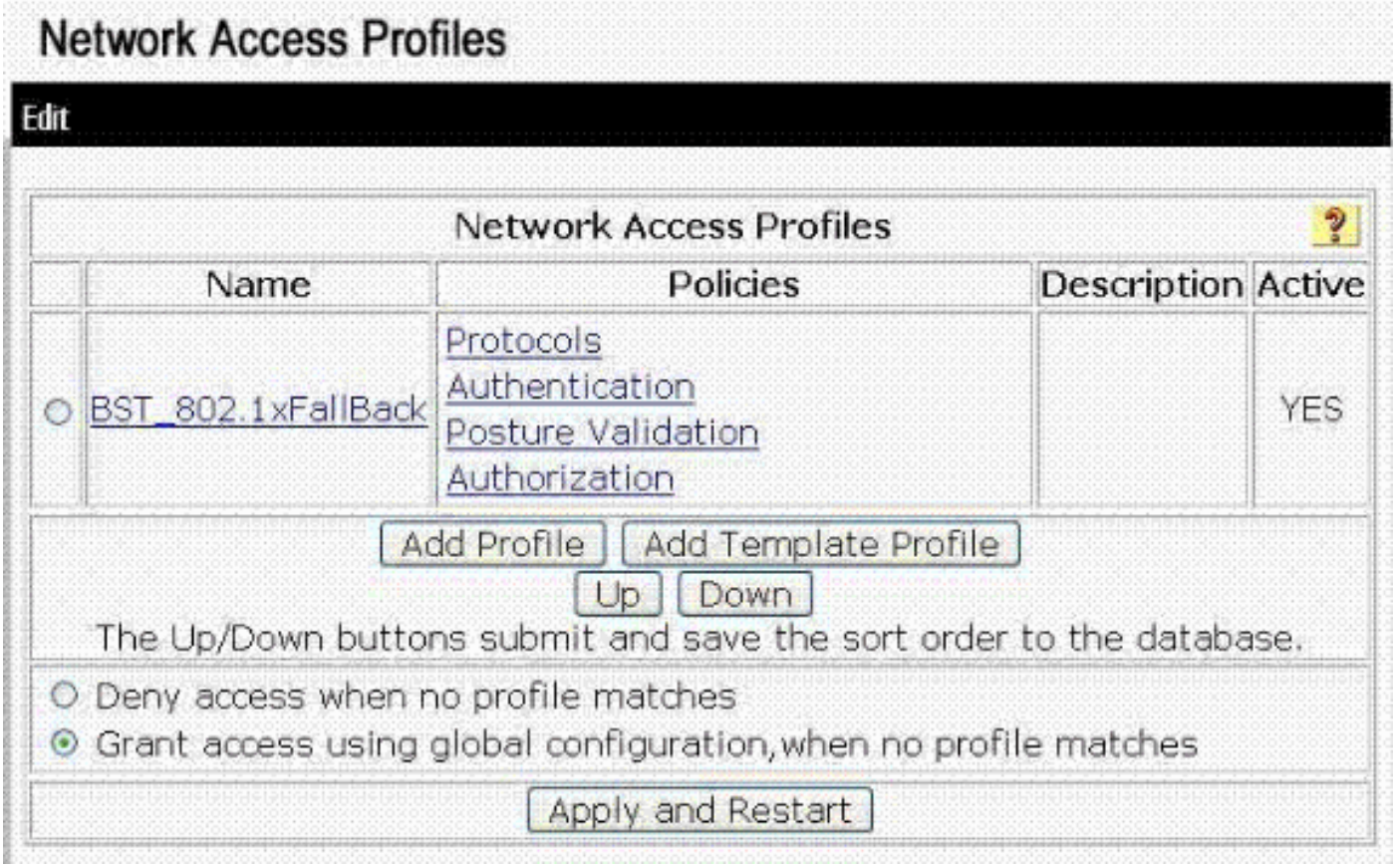
图 17：添加模板网络访问配置文件



命名网络访问配置文件，将其与其他配置文件区分开来，并根据需要添加说明。从下拉列表中选择此配置文件的模板。确保选择 **Agentless Host for L2 (802.1x Fallback)**，并选中 Active 复选框。完成后，请单击 **Submit** 按钮，以保存网络访问配置文件。

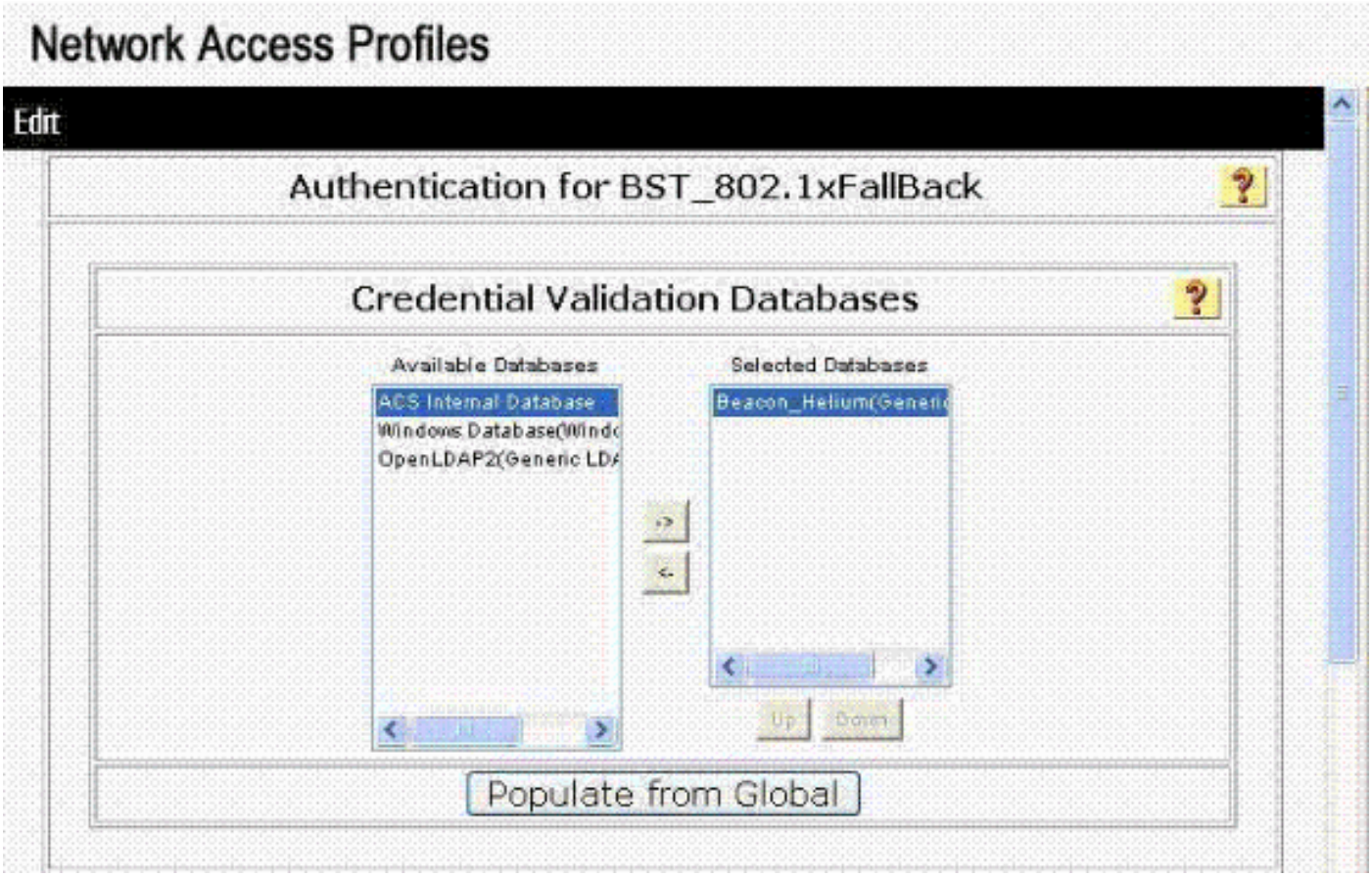
单击 Submit 后，将显示以下窗体，您可以按照显示内容在该窗体中编辑刚创建的配置文件的参数。

图 18：为 MAB 编辑 NAP



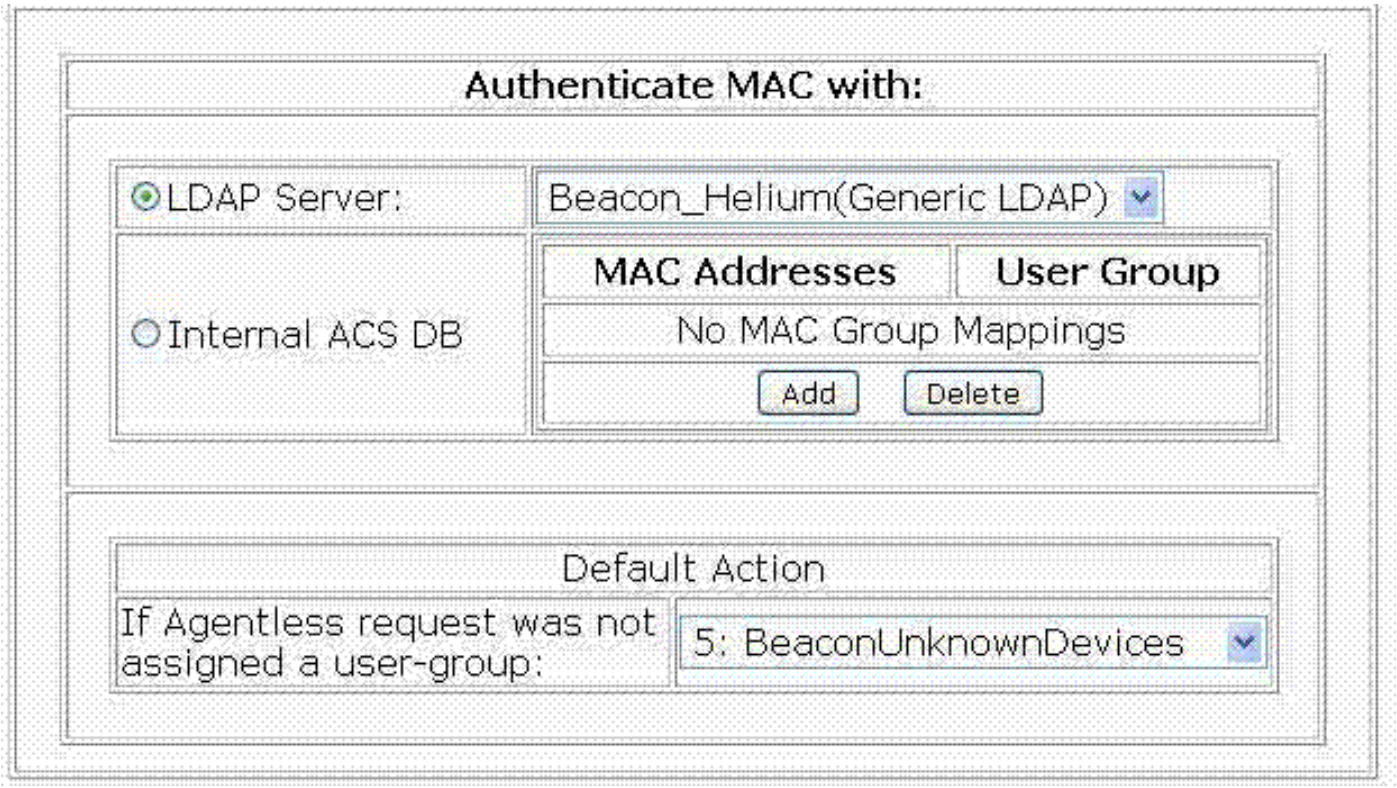
必须配置新配置的配置文件的 Authentication 策略，以便将 Beacon 系统用作凭证验证数据库。在新创建的网络访问配置文件（在本示例中为 802.1x FallBack）的 Policies 列中，选择 Authentication 链接。此时将显示以下窗体。

图 19：为 MAB 选择数据库



首先，从 Available Databases 表格中选择 Beacon 外部用户数据库，并使用 **- >** 按钮将其添加到 Selected Databases。往下滚动至此窗体的 Authenticate Mac 部分，并选择 **LDAP Server** 单选按钮。从下拉列表中选择 **Beacon** 数据库。最后，在 Default Action 中选择 **BeaconUnknownDevice** 组，如下图所示。

图 20：指定 Beacon LDAP 服务器



此步骤使用 Beacon 作为外部用户数据库完成 MAC 身份验证旁路的所需 ACS 配置。重新启动 ACS 服务，确保将所有配置更改提交到正在运行的配置。

如果交换机配置正确，应当可以使用该系统测试 MAB。通过为 BeaconKnownDevices 组指定 Policy 参数，当前位于已启用 LDAP 的 Beacon 配置文件中的端点在断开与网络之间的连接之后，可以重新允许该端点访问网络。

交换机的 MAC 身份验证旁路配置

以下交换机配置提供了 802.1X 验证的示例配置，该验证已启用 MAC 身份验证旁路，并需要重新分配动态 VLAN，以便应用从 ACS 返回的 RADIUS 属性。

交换机

```
switch#show running-config ! version 12.2 no service pad
service timestamps debug uptime service timestamps log
datetime service password-encryption service sequence-
numbers ! ! aaa new-model aaa authentication login
default line aaa authentication enable default enable
aaa authentication dot1x default group radius aaa
authorization network default group radius aaa
accounting dot1x default start-stop group radius ! aaa
session-id common switch 1 provision ws-c3750g-24ts ip
subnet-zero ip routing no ip domain-lookup ! ! ! ! ! !
dot1x system-auth-control no file verify auto spanning-
tree mode pvst spanning-tree extend system-id ! vlan
internal allocation policy ascending ! ! interface Port-
channel1 switchport trunk encapsulation dot1q switchport
trunk allowed vlan 5,7,9,10 ! interface Port-channel2
description LAG/trunk to einstein switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk ! interface Port-channel3
description "LAG to Edison" switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk ! interface
GigabitEthernet1/0/1 switchport trunk encapsulation
```

```
dot1q switchport trunk allowed vlan 5,7,9,10 channel-
group 1 mode passive ! interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,7,9,10 channel-group 1 mode passive !
interface GigabitEthernet1/0/3 switchport trunk
encapsulation dot1q switchport trunk allowed vlan
5,7,9,10 channel-group 1 mode passive ! interface
GigabitEthernet1/0/4 switchport access vlan 7 switchport
mode access ! interface GigabitEthernet1/0/5 switchport
access vlan 5 switchport mode access spanning-tree
portfast ! interface GigabitEthernet1/0/6 switchport
trunk encapsulation dot1q switchport trunk allowed vlan
5,7,9 switchport mode trunk switchport nonegotiate !
interface GigabitEthernet1/0/7 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/8 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/9 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/10 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/11 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/12 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/13 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/14 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/15 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/16 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/17 switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/18 switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/19 switchport mode access dot1x mac-
auth-bypass dot1x pae authenticator dot1x port-control
auto dot1x timeout quiet-period 10 dot1x timeout reauth-
period 60 dot1x timeout tx-period 10 dot1x timeout supp-
timeout 10 dot1x max-req 1 dot1x reauthentication dot1x
auth-fail max-attempts 1 spanning-tree portfast !
interface GigabitEthernet1/0/20 switchport mode access
dot1x mac-auth-bypass dot1x pae authenticator dot1x
port-control auto dot1x timeout quiet-period 10 dot1x
timeout reauth-period 60 dot1x timeout tx-period 10
dot1x timeout supp-timeout 10 dot1x max-req 1 dot1x
reauthentication dot1x auth-fail max-attempts 1
spanning-tree portfast ! interface GigabitEthernet1/0/21
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/22
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/23
switchport access vlan 10 spanning-tree portfast !
interface GigabitEthernet1/0/24 switchport access vlan
10 spanning-tree portfast ! interface
GigabitEthernet1/0/25 ! interface GigabitEthernet1/0/26
```

```
! interface GigabitEthernet1/0/27 ! interface
GigabitEthernet1/0/28 ! interface Vlan1 no ip address
shutdown ! interface Vlan5 ip address 10.1.1.10
255.255.255.0 ! interface Vlan9 ip address 10.9.0.1
255.255.0.0 ! interface Vlan10 ip address 10.10.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! interface Vlan11 ip address 10.11.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! ip default-gateway 10.1.1.1 ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1 ip route 10.30.0.0
255.255.0.0 10.10.0.2 ip route 10.40.0.0 255.255.0.0
10.10.0.2 ip http server ip http secure-server ! ! snmp-
server community public RW snmp-server host 10.1.1.191
public radius-server host 10.10.0.100 auth-port 1645
acct-port 1646 key 7 05090A1A245F5E1B0C0612 radius-
server source-ports 1645-1646 ! control-plane ! ! line
con 0 password 7 02020D550C240E351F1B line vty 0 4
password 7 00001A0803790A125C74 line vty 5 15 password 7
00001A0803790A125C74 ! end
```

验证

当前没有可用于此配置的验证过程。

相关信息

- Cisco NAC Appliance (Clean Access)
- 用于 Windows 的 Cisco 安全访问控制服务器
- 技术支持和文档 - Cisco Systems