身份源：pxGrid Cloud 身份（ISE 3.3 及更低版本）

以下主题讨论如何配置和使用包含 Cisco ISE 3.3 及更早版本的 pxGrid 云身份源。

关于 pxGrid 云身份源

思科身份服务引擎 (Cisco ISE) pxGrid 云身份源 允许您在 Secure Firewall Management Center 访问控制规则中使用来自 的 服务器或集群 的订阅和用户数据。此外，身份源在 Secure Firewall Management Center的访问控制策略中使用来自 的不断变化的动态对象。

pxGrid 云身份源 还使用：

- Cisco Platform Exchange Grid (pxGrid)，可在安全监控和检测系统、网络策略平台、资产和配置管理、身份和访问管理等领域实现多供应商跨平台网络系统协作。 pxGrid 云是 Cisco ISE 的基于云的接口。

  有关 pxGrid 的更多信息可以在 devnet 上的“什么是 PxGrid？”等资源中找到。

- 思科全数字化网络架构 (Cisco DNA) 可提供自动化、安全性、预测性监控和策略驱动方法。它能够提供端到端网络可视性，利用网络洞察优化网络性能并提供最佳的用户和应用体验。

  要将 pxGrid 云身份源 和 Secure Firewall Management Center配合使用，您必须 创建一个思科帐户。

- devnet 上的什么是 pxGrid?
- devnet 上的思科平台交换架构云

相关主题

如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）
如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 3 页

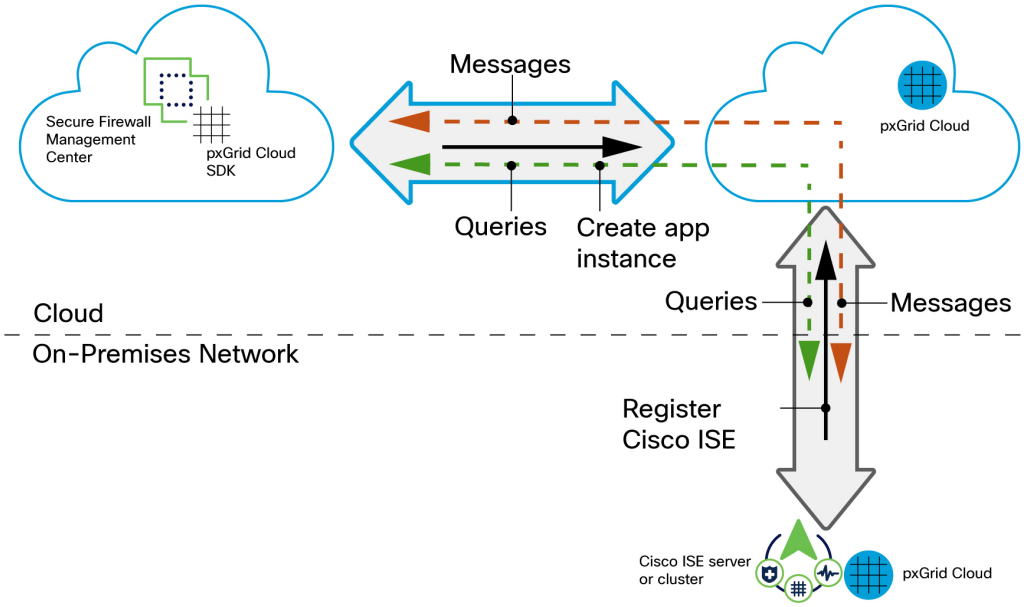
pxGrid 云身份源 的限制

在设置 pxGrid 云身份源 之前，请注意以下事项：

- pxGrid 云 支持以下区域：`us-west-2`、`eu-central-1` 和 `ap-southeast-1`。
- 有关 Cisco ISE 版本和查询大小的信息，请参阅 GitHub 上 pxGrid 云 SDK 中的查询限制。

pxGrid 云身份源 工作原理

下图显示了身份源的工作原理。



您的 Secure Firewall Management Center 使用 pxGrid 云 SDK 以编程方式从本地 Cisco ISE 服务器或集群 检索用户信息，以便可以在 Secure Firewall Management Center 上的身份策略中使用这些用户。

要授权和验证此数据交换，您必须：

1. 在 Cisco ISE 中，启用 pxGrid 云。
2. 在 pxGrid 云中将 Cisco ISE 注册为产品，这将对 Cisco ISE 和 pxGrid 云进行身份验证，并使它们能够相互通信。

身份验证过程要求您将一次性密码 (OTP) 从 pxGrid 云粘贴到 Cisco ISE 中。

3. 在 pxGrid 云中，创建一个“应用实例”，用于生成 OTP，以供您在 Secure Firewall Management Center 中用于对彼此进行身份验证。
4. 完成上述所有任务后，Secure Firewall Management Center（包括 pxGrid 云 SDK）可以使用 pxGrid 云查询 Cisco ISE 并检索包含用户信息、SGT、终端配置文件和其他详细信息的会话。
5. 可以过滤许多类型的动态对象，并将其作为要在访问控制规则中使用的动态对象发送到 Secure Firewall Management Center。其中包括：SGT、终端配置文件、终端安全评估状态和计算机身份验证。

   我们会从 Cisco ISE 检索用户信息，并从 Microsoft Active Directory 或 Azure Active Directory 检索组信息。

相关主题

如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）
如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 3 页

如何配置 pxGrid 云身份源

这些主题总结了如何为 ISE 3.3 及更早版本或 ISE 3.4 及更高版本配置 pxGrid 云身份源。步骤不同，因此请确保完全按照步骤操作。

相关主题

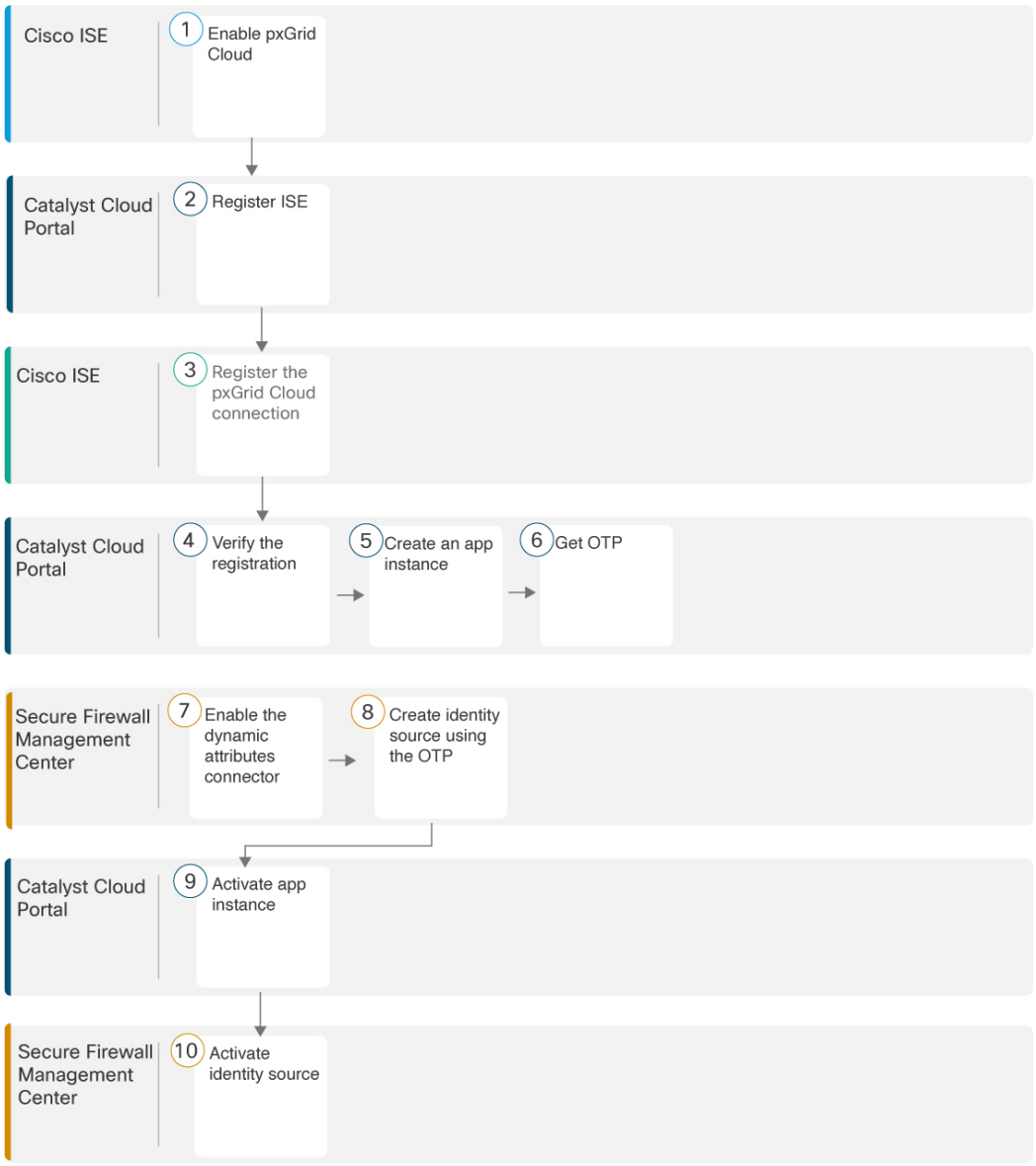
如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）
如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本），第 3 页
在 Cisco ISE 中启用 pxGrid 云 服务
创建应用实例
创建身份源，第 12 页
激活应用实例，第 13 页
激活 pxGrid 云身份源，第 16 页

如何配置 pxGrid 云身份源（Cisco ISE 3.3 或更早版本）

在开始之前，创建一个 Cisco 账户。

重要事项 本主题适用于 *Cisco ISE* 版本 *3.3* 或更早版本。如果您使用的是更高版本，另请参阅如何配置 pxGrid 云身份源（Cisco ISE 3.4 或更高版本）。

下图显示了使用 Cisco ISE、Catalyst 云门户 和 Secure Firewall Management Center 来配置 pxGrid 云身份源 的步骤。



1 在 Cisco ISE 中启用 pxGrid Cloud 服务， 第 6 页
2 使用 Catalyst 云门户 注册 Cisco ISE， 第 6 页
3 使用 Catalyst 云门户 注册 Cisco ISE， 第 6 页
4 创建应用实例， 第 11 页
5 启用 dynamic attributes connector
6 创建应用实例， 第 11 页
7 激活应用实例， 第 13 页
8 激活 pxGrid 云身份源， 第 16 页

表 *1:* 配置 *pxGrid* 云身份源

1	Cisco ISE	在 Cisco ISE 中启用 pxGrid Cloud。 pxGrid Cloud 使您能够订阅产品/服务，并注册应用（在此情况下为 Secure Firewall Management Center），以在云环境中进行安全数据交换。 有关详细信息，请参阅在 Cisco ISE 中启用 pxGrid Cloud 服务，第 6 页。
2	Catalyst 云门户	在 Catalyst 云门户 中注册 Cisco ISE，并对 Cisco ISE 与 Catalyst 云门户 之间的通信进行身份验证。 有关详细信息，请参阅使用 Catalyst 云门户 注册 Cisco ISE，第 6 页。
3, 4	Cisco ISE，Catalyst 云门户	向 Cisco ISE 注册 pxGrid Cloud 并验证注册。 有关详细信息，请参阅向 Cisco ISE 注册 pxGrid 云 连接，第 9 页。
5, 6	Catalyst 云门户，Secure Firewall Management Center	在 Catalyst 云门户 中创建一个应用实例并获取一次性密码 (OTP)。 应用实例使 Secure Firewall Management Center 能够使用 pxGrid Cloud 服务向 Cisco ISE 进行身份验证。 下一步所需的 OTP 将在 60 分钟后到期。
7	Secure Firewall Management Center	如果尚未启用，请启用 dynamic attributes connector。 使用 pxGrid 云身份源 需借助 dynamic attributes connector。 有关详细信息，请参阅启用 dynamic attributes connector。
8	Secure Firewall Management Center	使用您在上一步中获取的 OTP 创建 pxGrid 云身份源。 关联该应用后，可让 Secure Firewall Management Center 向 Cisco ISE 和 Catalyst 云门户进行身份验证，以便接收来自 Cisco ISE 的用户数据。 有关详细信息，请参阅创建身份源，第 12 页。
9	Catalyst 云门户	激活应用实例。 有关详细信息，请参阅激活应用实例，第 13 页。
10	Secure Firewall Management Center	激活 pxGrid 云身份源。 有关详细信息，请参阅激活 pxGrid 云身份源，第 16 页

完成所有前述任务后，您可以：

- 测试 pxGrid 云身份源 以确保其正常运行。

  有关详细信息，请参阅测试 pxGrid 云身份源，第 18 页。

- 创建动态属性过滤器，定义哪些动态对象发送到 Secure Firewall Management Center。

  有关详细信息，请参阅创建动态属性过滤器，第 24 页。

- 配置 pxGrid 云身份源 后，您可以在访问控制规则中使用以下任何内容：
  - 动态对象
  - Microsoft AD 用户和组
  - Azure AD 用户和组

相关主题

在 Cisco ISE 中启用 pxGrid Cloud 服务，第 6 页

在 Cisco ISE 中启用 pxGrid Cloud 服务

开始之前

- 确保在 Cisco ISE 部署中安装并激活 Advantage 许可证层。
- pxGrid Cloud 代理会创建与 Cisco pxGrid 云 的出站 HTTPS 连接。因此，如果客户网络使用代理访问互联网，则必须配置 Cisco ISE 代理设置。要在 Cisco ISE 中配置代理设置，点击**菜单**图标 (☰)，然后选择 **管理 > 系统 > 设置 > 代理**。
- 思科 ISE 受信任的证书储存必须包括验证 pxGrid 云 提供的服务器证书所需的根 CA 证书。确保已为此根 CA 证书启用 **信任思科服务的身份验证** 选项。要启用**信任对思科服务的身份验证**，请导航至**管理 > 系统 > 证书**。

过程

步骤 1 在思科 ISE GUI 中，点击**菜单** 图标 (☰)，然后选择 **管理 > 系统 > 部署**。

步骤 2 点击要在其上启用 pxGrid 云 服务的节点。

步骤 3 在**常规设置 (General Settings)** 选项卡中，启用 **pxGrid** 服务。

步骤 4 选中**启用 pxGrid 云 (Enable pxGrid Cloud)** 复选框。

为了实现高可用性，可在两个节点上启用 pxGrid 云服务。

注释

只有在该节点上启用了 **pxGrid** 服务后才能启用 **pxGrid 云 (pxGrid Cloud)** 选项。

使用 Catalyst 云门户 注册 Cisco ISE

此任务讨论如何在 Catalyst 云门户 中将 Cisco ISE 注册为应用，以及验证 Catalyst 云门户 与 Cisco ISE 之间的通信。

另请参阅《*pxGrid Cloud* 解决方案指南》中的注册 Cisco ISE。

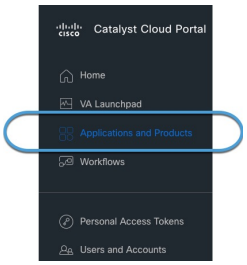
过程

步骤 1 登录到 Cisco Cloud Catalyst 门户。

步骤 2 如果出现提示，请选择要使用的账户。

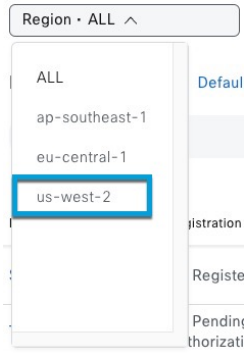
步骤 3 点击**注册 (Register)**。

步骤 4 在 Catalyst 云门户 中，点击☰ > **应用程序和产品**，如下图所示：

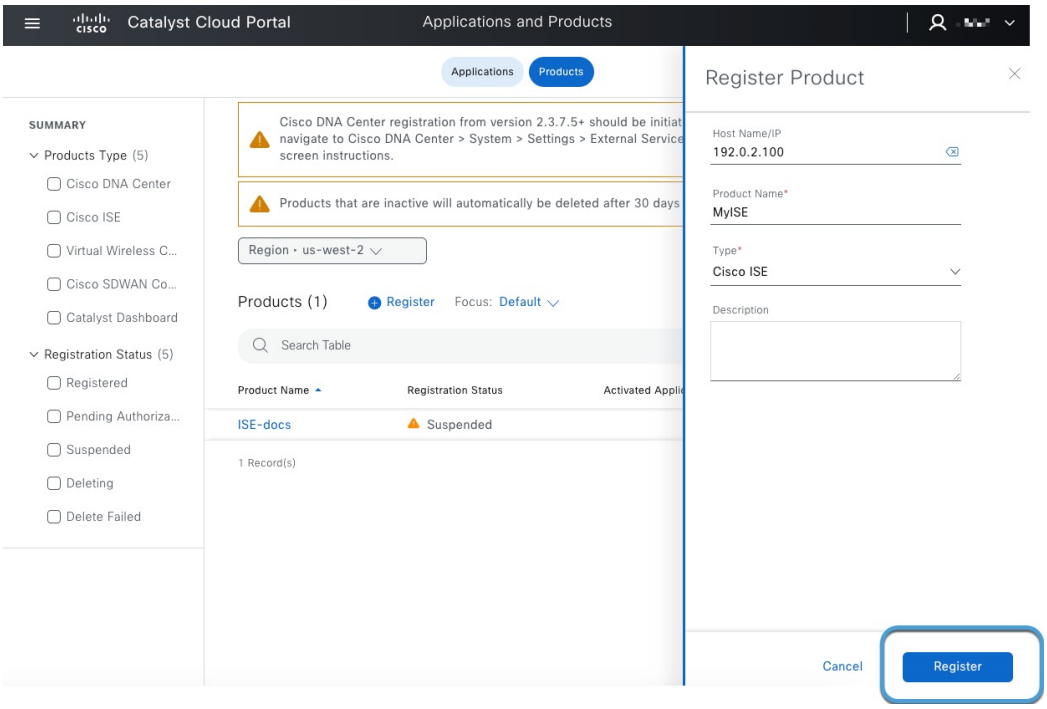


步骤 5 在页面顶部，点击**产品**。

步骤 6 从**区域**列表中，点击 **us-west-2**、**eu-central-1** 或 **ap-southeast-1**。



步骤 7 点击**注册 (Register)**。
下图显示了示例注册页面。



步骤 8 输入以下信息。

- **主机名/IP**：（可选）。输入 ISE 服务器的完全限定域名或 IP 地址。如果输入 IP 地址，请省略方案（例如 **https://**）和端口（如有）。
- **产品名称**：输入用于标识此服务器的唯一名称。
- **类型**：从列表中，点击 **Cisco ISE**。
- **说明**：输入可选说明。

步骤 9 点击**注册 (Register)**。

步骤 10 通过以下任一方式生成一次性密码 (OTP)：

- 如果您之前已注册 ISE 应用并在列表中看到您的应用，请点击**操作**列中的**生成 OTP**；您将在本过程的后续部分用到它。
- 如果您现在正在注册应用，将显示 OTP。点击 将其复制到剪贴板；您将在本过程的后续部分用到它。

下一步做什么

请参阅向 Cisco ISE 注册 pxGrid 云 连接，第 9 页。

向 Cisco ISE 注册 pxGrid 云 连接

此任务讨论如何向 Cisco ISE 注册 pxGrid 云 连接，这将使 pxGrid 云 能够在 pxGrid 云身份源 中将用户数据发送到 Security Cloud Control。

开始之前

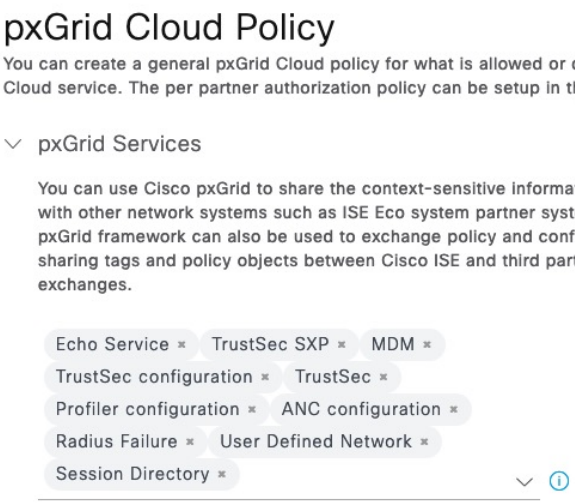
完成 使用 Catalyst 云门户 注册 Cisco ISE，第 6 页中讨论的任务。

过程

步骤 1 以管理员身份登录 Cisco ISE。

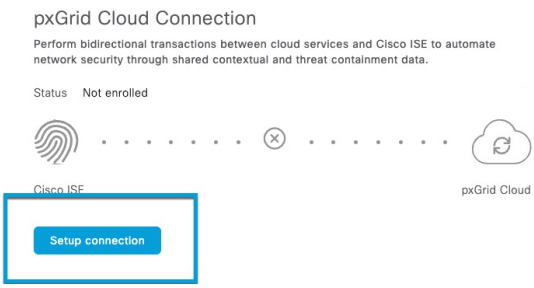
步骤 2 点击 ☰ > **管理** > **pxGrid 服务** > **客户端管理** > **pxGrid Cloud 连接**。

步骤 3 确保所有服务均已启用并具有读/写权限。
下图显示了一个示例。



步骤 4 在左侧导航栏中，点击 **pxGrid Cloud 连接**。

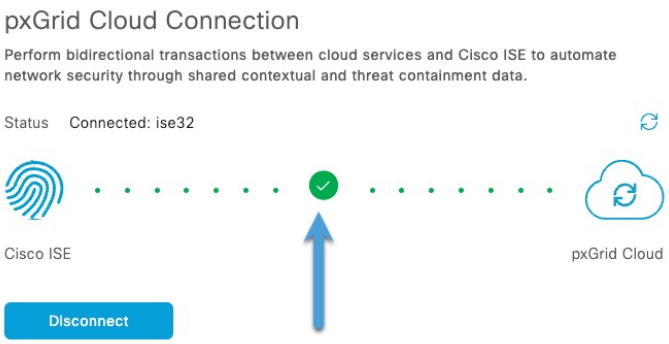
步骤 5 点击**设置连接**，如下图所示。



步骤 6 将 OTP 值粘贴到提供的字段中。

步骤 7 点击**连接 (Connect)**。

如下所示的绿色复选标记确认连接已成功。

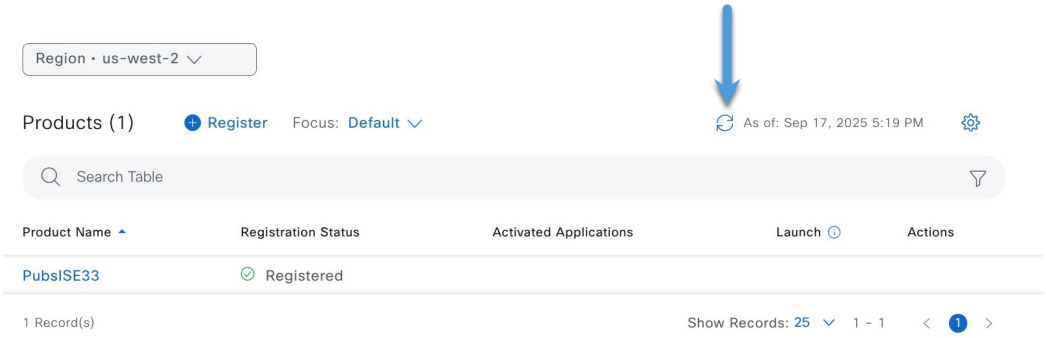


步骤 8 确认到目前为止设置已成功：

a) 登录Catalyst 云门户。

b) 点击 **产品** 选项卡。

c) 点击**刷新**，如下图所示。



d) 验证**已注册**显示为您的产品的状态。

下一步做什么

继续执行创建身份源，第 12 页。

创建一个 pxGrid 云身份源

以下任务讨论如何使用 Cisco ISE、Catalyst 云门户 和 Security Cloud Control 来创建 pxGrid 云身份源。您必须按所示顺序完成所有任务；在某些情况下，由于所需一次性密码 (OTP) 的过期，存在时间限制。

相关主题

创建应用实例，第 11 页
创建身份源，第 12 页
激活应用实例，第 13 页
激活 pxGrid 云身份源，第 16 页
测试 pxGrid 云身份源，第 18 页

创建应用实例

此任务是您必须执行的多项任务之一，目的是创建一个 pxGrid 云身份源，以便将用户会话数据发送到 Secure Firewall Management Center。

输入一次性密码 (OTP) 的时间限制为一小时，请在此时间内完成此程序。您无需登录到 Cisco ISE。

开始之前

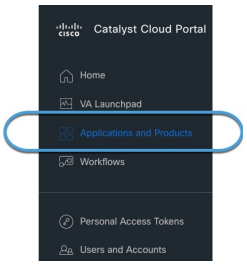
首先完成以下所有任务：

- 在 Cisco ISE 中启用 pxGrid Cloud 服务，第 6 页
- 使用 Catalyst 云门户 注册 Cisco ISE，第 6 页
- 向 Cisco ISE 注册 pxGrid 云 连接，第 9 页

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 在 Catalyst 云门户 中，点击☰ > **应用程序和产品**，如下图所示：



步骤 3 在页面顶部，点击**应用**。

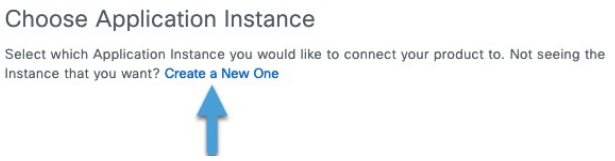
步骤 4 从**区域**列表中，点击 **us-west-2**、**eu-central-1** 或 **ap-southeast-1**。

步骤 5 点击 **Firepower 管理中心**旁边的**管理**（或**激活**）。

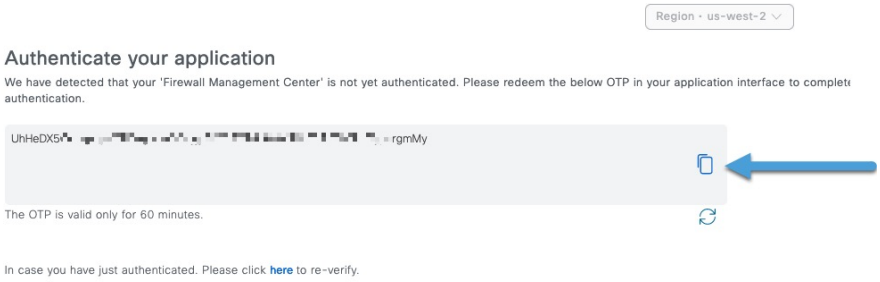
步骤 6 点击**添加 (Add)**。

步骤 7 点击**创建一个新的**。

下图显示了一个示例。



步骤 8 点击显示的 OTP 旁边的复制按钮，如下图所示：



步骤 9 将 OTP 复制到文本文件；它会在 60 分钟后过期。

步骤 10 继续执行创建身份源，第 12 页。

创建身份源

此任务是创建 pxGrid 云身份源 以将用户会话数据发送到 Secure Firewall Management Center 的多项任务之一。

开始之前

完成 创建应用实例，第 11 页中讨论的任务。

过程

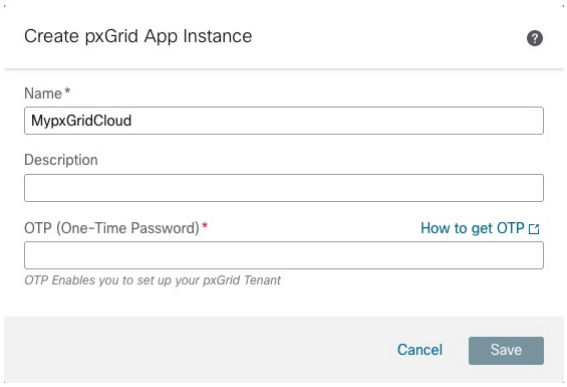
步骤 1 登录至 Secure Firewall Management Center

步骤 2 点击 **集成** > **身份** > **身份源**

步骤 3 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 4 点击**创建 pxGrid 应用实例**。

下图显示了一个示例。



步骤 5 输入以下信息。

值	说明
名称	输入名称以唯一标识此连接器。
说明	可选说明。
OTP（一次性密码）	输入的 OTP。

步骤 6 点击**创建 (Create)**。

步骤 7 在该页面顶部，点击**保存**。

步骤 8 继续执行激活应用实例，第 13 页。

激活应用实例

本任务讨论如何创建 pxGrid 云身份源 向 Secure Firewall Management Center 发送用户会话数据。

输入一次性密码 (OTP) 的时间限制为一小时，请在此时间内完成此程序。您无需登录到 Cisco ISE。

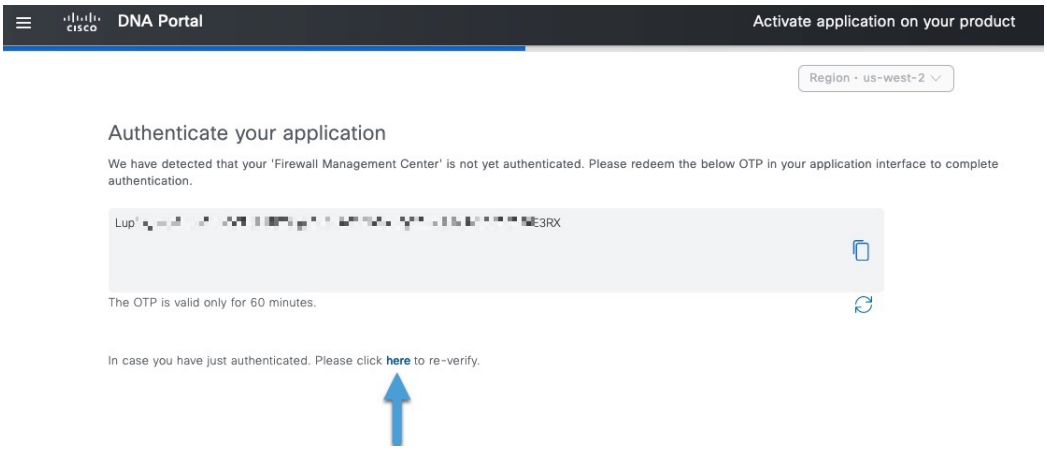
开始之前

完成创建身份源，第 12 页中讨论的任务。

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

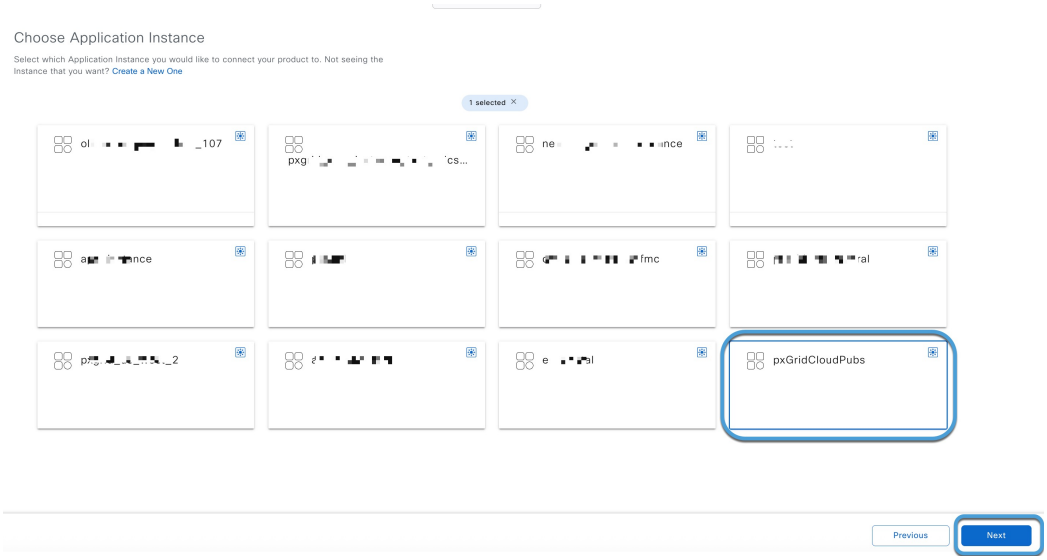
步骤 2 点击下图所示的单词**此处**，重新验证应用。



步骤 3 点击您刚刚在 Secure Firewall Management Center 中创建的应用实例的名称。

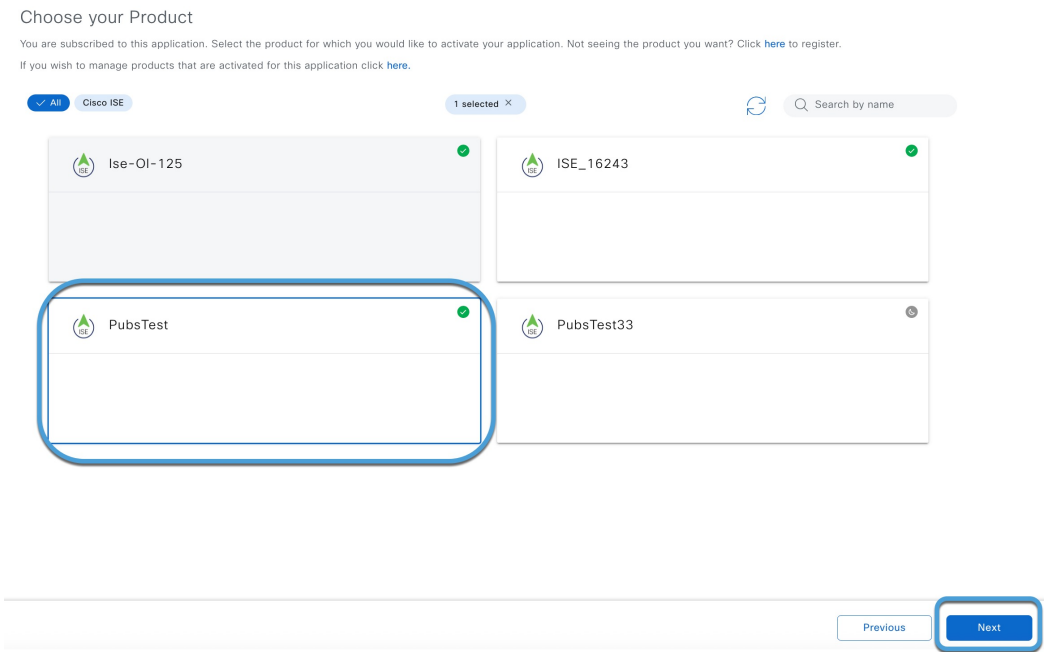
步骤 4 点击**下一步 (Next)**。

示例：



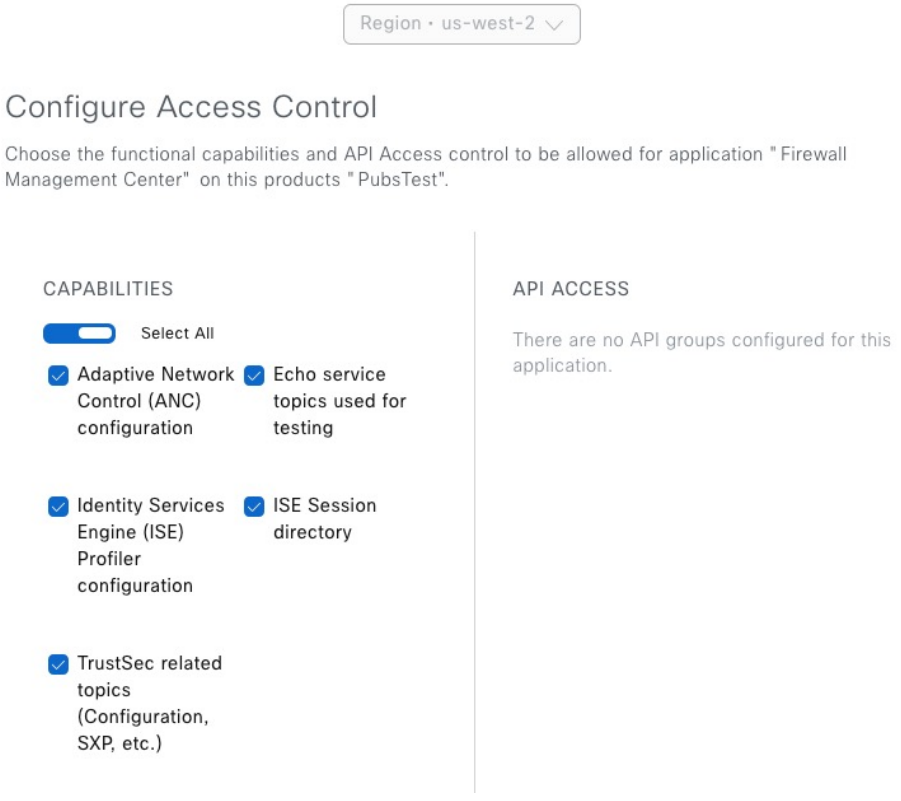
步骤 5 在“选择产品”页面上，点击 Cisco ISE 产品的名称，然后点击**下一步**。

示例：



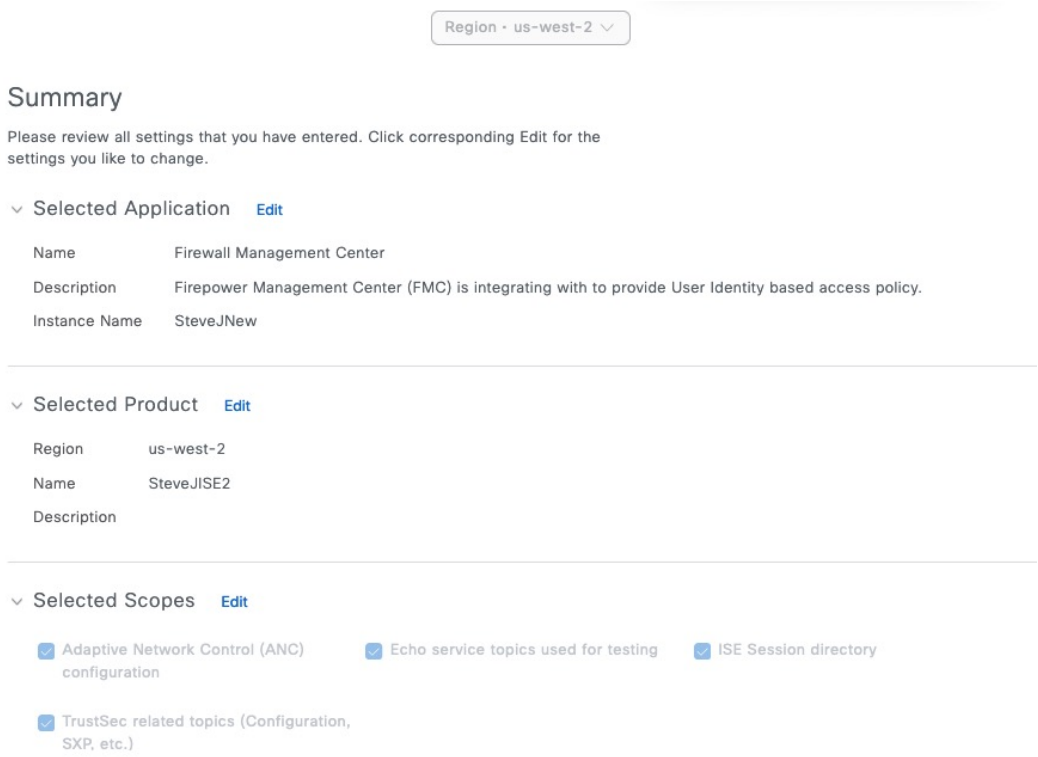
步骤 6 选中每个范围旁边的复选框。

下图显示了一个示例。



步骤 7 点击下一步 **(Next)**。

步骤 8 查看所显示信息的准确性。确保选中所有范围。
下图显示了一个示例。



步骤 9 点击**激活**。

激活应用实例可能需要几分钟时间。

步骤 10 继续执行激活 pxGrid 云身份源，第 16 页。

激活 pxGrid 云身份源

此任务说明如何在 Secure Firewall Management Center 中激活 pxGrid 云身份源。

开始之前

完成激活应用实例，第 13 页中讨论的任务。

注释 每次只能有一个 pxGrid 云身份源 处于活动状态。

过程

步骤 1 登录至 Secure Firewall Management Center

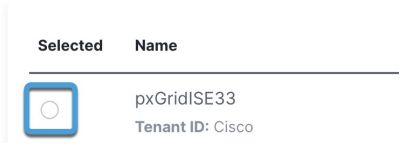
步骤 2 点击 **集成** > **身份** > **身份源**

步骤 3 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 4 点击页面顶部的**保存**。

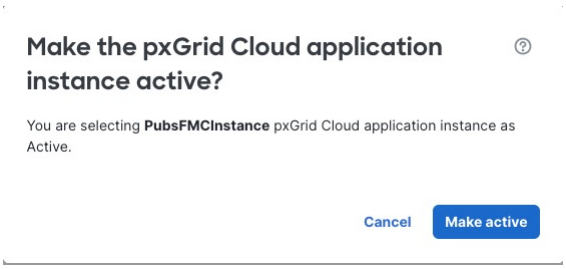
步骤 5 如果身份源名称旁边未显示绿色复选标记，请将其选中。

示例：



步骤 6 点击**设为主用**。

示例：



步骤 7 （可选。）如果需要，请选择以下选项：

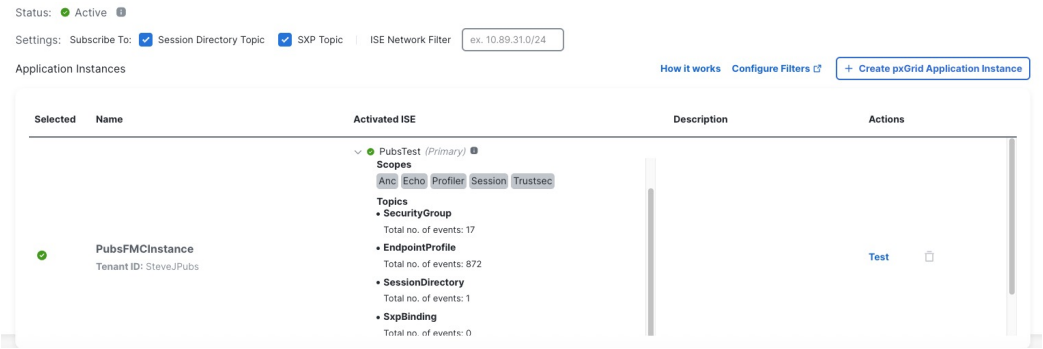
- **会话目录主题**：选中此复选框可从 Cisco ISE 服务器接收 ISE 用户会话信息。
- **SXP 主题**：选中此复选框，以便在 ISE 服务器提供 SGT 到 IP 映射的更新时接收更新。要在访问控制规则中使用目标 SGT 标记，需要使用此选项。
- **ISE 网络过滤器**：您可以设置可选筛选条件来限制 Cisco ISE 报告的数据。如果提供网络过滤器，Cisco ISE 会报告来自该过滤器中的网络的数据。

  您有以下选择：

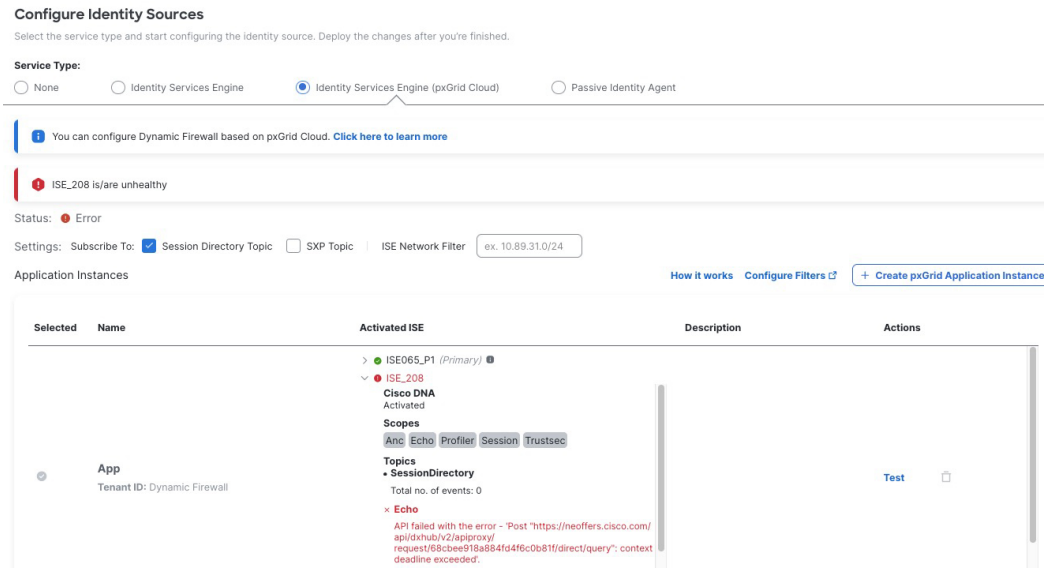
  - 将此字段留空以指定**任意 (any)** 值。
  - 使用 CIDR 符号输入单一 IPv4 地址块。
  - 使用由逗号分隔的 CIDR 符号输入 IPv4 地址块列表。

步骤 8 在已激活的 ISE 下，展开身份源。

正常结果示例：



错误结果示例：



如有错误，请参阅测试 pxGrid 云身份源，第 18 页。

步骤 9 验证状态是否为活动，以及是否已显示所有范围和主题。

步骤 10 等待几分钟以便下载数据。

下一步做什么

请参阅测试 pxGrid 云身份源，第 18 页。

测试 pxGrid 云身份源

本主题讨论您可以使用 Secure Firewall Management Center 执行的诊断，以确定身份源是否正常工作。错误可能包括与 Cisco ISE 的通信，或与 Catalyst 云门户 的 Cisco ISE 配置问题。

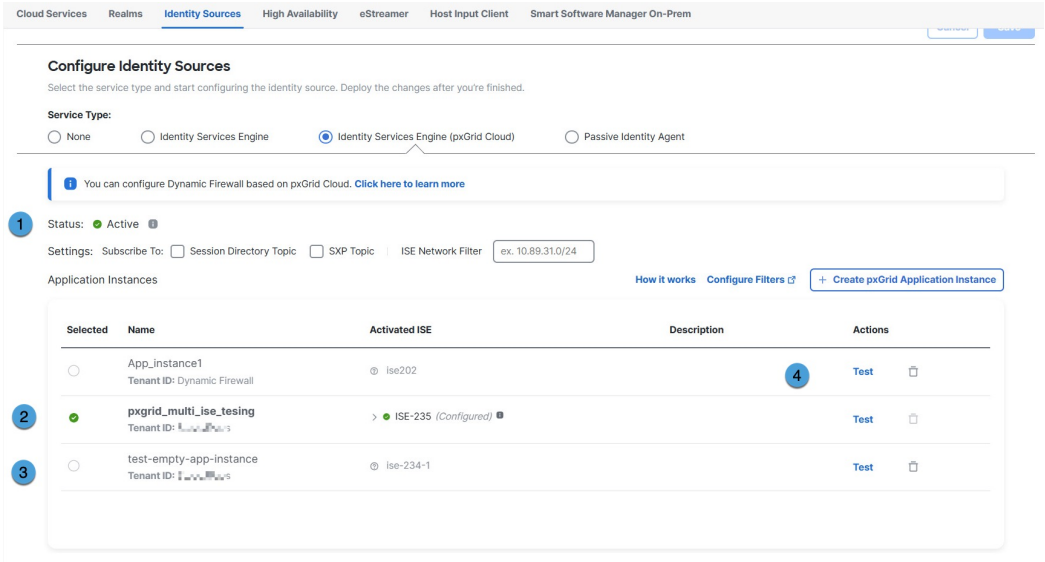
查看当前配置

如需了解入门信息：

1. 登录Secure Firewall Management Center。
2. 点击 **集成** > **身份** > **身份源**
3. 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

配置状态示例

下图所示为一个配置示例。

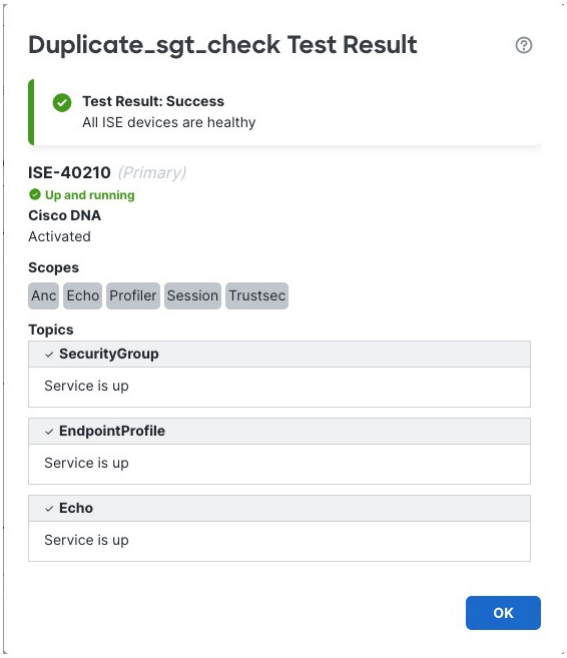


下表提供了有关图中编号区域的详细信息。

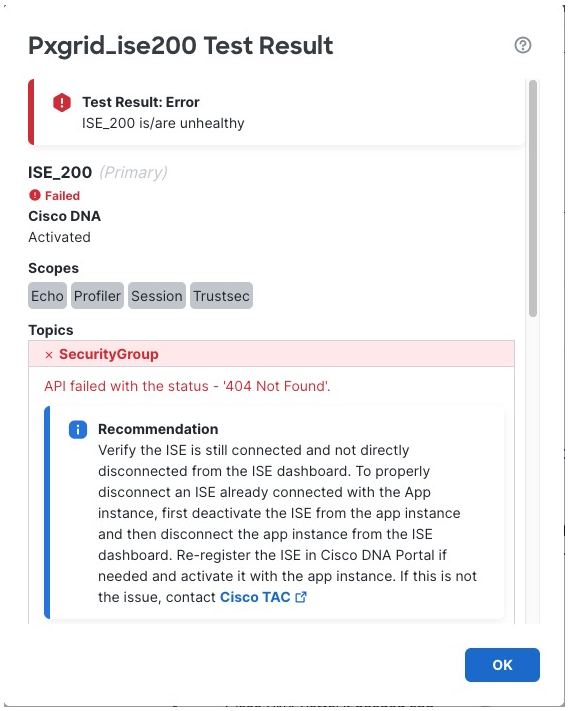
数字	含义
1	总体状态 系统会显示 Cisco ISE 应用实例的整体状态中的任何错误。在这种情况下，请滚动到该实例，然后展开错误消息或点击**测试**以了解更多信息。
2	主用 绿色复选标记表示应用处于活动状态。
3	非活动 灰显的应用实例处于非活动状态。您可以通过选中其名称旁边的复选框，然后点击**设为主用**来将其激活。

数字	含义
4	**测试**按钮 点击**测试**以执行显示更详细的应用实例状态的诊断测试。有关详细信息，请参阅下一节。

下图显示了一条示例成功消息。



下图为搜索结果的示例。



以下部分提供可能的错误的参考。

错误代码参考

提供以下信息可帮助您诊断和解决 Cisco ISE、pxGrid 云 和 Catalyst 云门户 的问题。如果这些建议不起作用，或者您遇到其他问题，请联系思科 TAC。

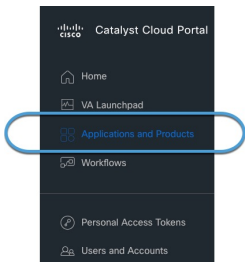
403 – Forbidden

请验证 Cisco ISE 产品在 Catalyst 云门户 中未处于**待处理**或**已中止**状态。如果设备已暂停，请按照在 Cisco ISE 中启用 pxGrid Cloud 服务并注册设备的步骤，验证 Cisco ISE 是否已注册。

此外，请验 pxGrid 云 证服务是否公开可用。

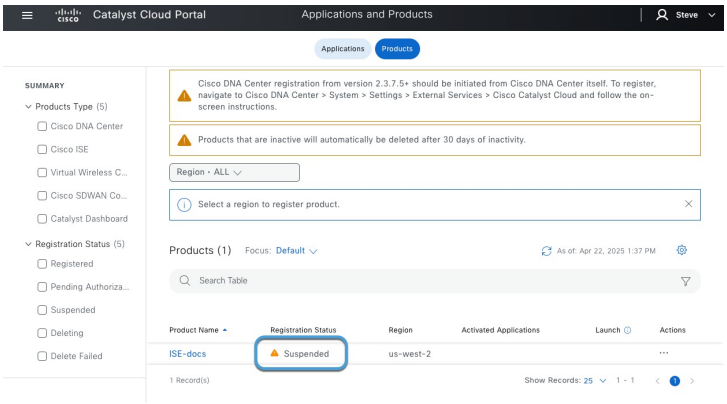
要验证您的产品是否处于活动状态，请执行以下操作：

1. 登录Catalyst 云门户。
2. 在 Catalyst 云门户 中，转到☰ > **应用程序和产品**，如下图所示：



3. 点击 **产品** 选项卡。

下图显示了已终止产品的示例。



4. 要更正此问题，请在操作列中点击 ***，然后点击**生成 OTP**。
5. 按照创建身份源，第 12 页中所述使用 OTP。

404 – Not Found

验证 Cisco ISE 服务器未直接与 Cisco ISE 控制面板断开。要正确断开已与应用实例连接的 Cisco ISE，请先从应用实例停用 Cisco ISE，然后断开应用实例与 Cisco ISE 控制面板的连接。

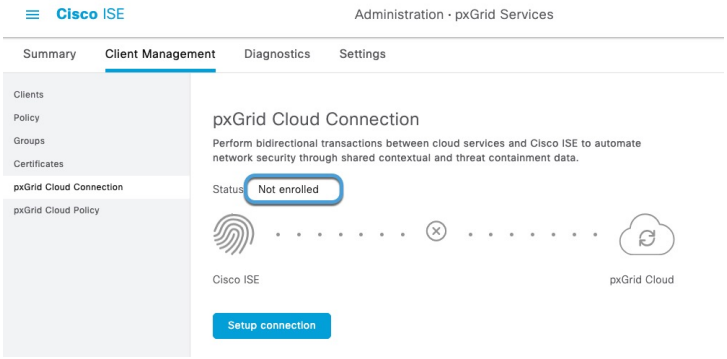
408 – Request Timeout

一般连接

检查 Cisco ISE是否存在任何常规连接问题，并在 ISE 面板中的 ☰ > **管理** > **pxGrid 服务** > **客户端管理** > **pxGrid Cloud 连接** 下验证 pxGrid 云 连接状态是否为**已连接**。

下图显示了已连接的系统示例。

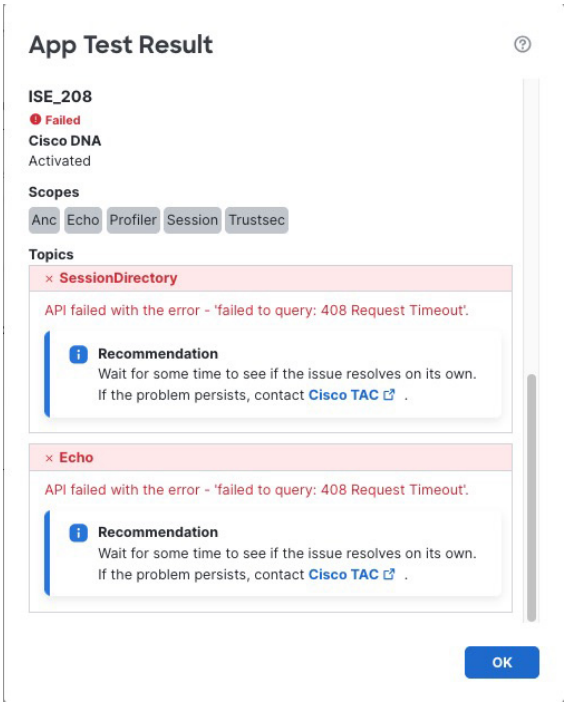
下图显示的是未注册（即未连接）的系统示例。



验证 Cisco ISE 服务器未直接与 Cisco ISE 控制面板断开。要正确断开已与应用实例连接的 Cisco ISE，请先从应用实例停用 Cisco ISE，然后断开应用实例与 Cisco ISE 控制面板的连接。

集群成员无法访问

如果无法访问 Cisco ISE 集群的一个成员，系统将显示如下页面：



要查找无法访问的节点，请以管理员身份登录 Cisco ISE 主管理节点，然后点击 点击**菜单**图标 (☰)，然后选择 **管理** > **系统** > **部署**，查看 Cisco ISE 部署中的节点状态。

413 – 内容过大

我们建议您查看 GitHub 上的 pxGrid Cloud API 限制。如果需要，请考虑升级您的 Cisco ISE 版本，以充分利用 pxGrid 云 支持。

500 – Internal Server Error

检查 Cisco ISE 服务器是否正常运行以及 pxGrid 云 服务是否处于活动状态（验证 MNT、SXP、pxGrid 节点等）。

有关更多信息，请参阅《思科身份识别服务引擎管理员指南》中 Cisco pxGrid 章节的“监控和调试”。

创建动态属性过滤器

使用 Dynamic Attributes Connector 定义的动态属性过滤器会在 Secure Firewall Management Center 中显示为可在访问控制策略中使用的动态对象。例如，您可以将财务部门对 AWS 服务器的访问权限限制为 Microsoft Active Directory 中定义的财务组成员。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

有关访问控制规则或DNS规则的详细信息，请参阅使用动态属性过滤器来创建访问控制规则或 DNS 规则，第 25 页。

开始之前

创建连接器

过程

步骤 1 登录Secure Firewall Management Center。

步骤 2 请点击 **集成** > **动态属性连接器** > **动态属性筛选器**。

步骤 3 执行以下任一操作：

- 添加新过滤器：点击 **添加** (+)。
- 编辑或删除过滤器：点击 **更多**（⋮），然后点击行末尾的**编辑 (Edit)** 或**删除 (Delete)**。

步骤 4 输入以下信息。

项目	说明
名称	用于在策略和 Secure Firewall Management Center 对象管理器（**外部属性** > **动态对象**）中标识动态过滤器（作为动态对象）的唯一名称。
连接器	在列表中点击要使用的连接器的名称。

项目	说明
查询	请点击 添加  。

步骤 5 要添加或编辑查询，请输入以下信息。

项目	说明
密钥	点击列表中的一个键。密钥会从连接器获取。
操作	点击以下选项之一： • **等于 (Equals)** 会将密钥与值完全匹配。 • **包含 (Contains)** 会将键与值匹配（如果值的任何部分匹配）。
值	点击**任意 (Any)** 或**全部 (All)**，然后点击列表中的一个或多个值。点击**添加其他值 (Add another value)** 以便向查询中添加值。

步骤 6 点击**显示预览 (Show Preview)** 以便显示查询返回的网络或 IP 地址的列表。

步骤 7 完成后，点击**保存**。

步骤 8 （可选。）验证 Secure Firewall Management Center 中的动态对象。

a) 至少要以具有网络管理员角色的用户身份登录 Secure Firewall Management Center 。

b) 请点击 **对象 (Objects)** > **外部属性 (External Attributes)** > **动态对象 (Dynamic Object)**。

您创建的动态属性查询应显示为动态对象。

使用动态属性过滤器来创建访问控制规则或 DNS 规则

本主题讨论如何使用动态对象（这些动态对象以您之前创建的动态属性过滤器来命名）创建访问控制规则。

要向 DNS 策略添加动态属性过滤器，请参阅创建基本 DNS 策略。

要将动态属性过滤器添加到 DNS 策略，请参阅创建基本 DNS 策略。

开始之前

按照创建动态属性过滤器， 第 24 页中所述，创建动态属性筛选器。

注释 您不能为 通用文本、Office 365Azure Service Tags、Webex 或 Zoom 创建动态属性过滤器。这些类型的云对象会提供自己的 IP 地址。

过程

步骤 1 登录至 Secure Firewall Management Center

步骤 2 请点击 策略 > 安全策略 > 访问控制。

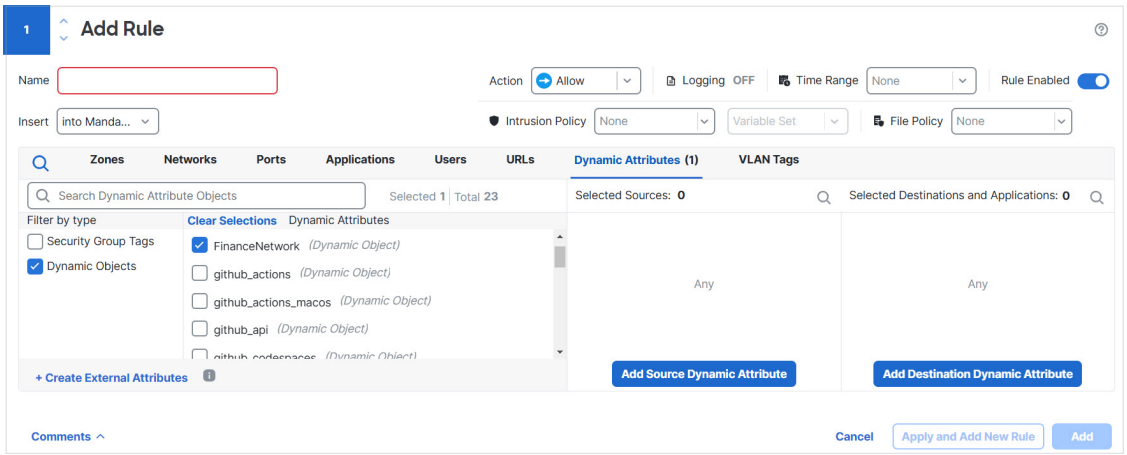
步骤 3 点击访问控制策略旁边的 编辑（ ）。

步骤 4 点击添加规则 (Add Rule)。

步骤 5 点击动态属性 (Dynamic Attributes) 选项卡。

步骤 6 在“可用属性”(Available Attributes) 部分中，点击列表中的动态对象 (Dynamic Objects)。

下图显示了一个示例。



本示例显示一个名为 APIC 动态属性的动态对象，它对应于 dynamic attributes connector 中创建的动态属性筛选器。

步骤 7 将所需对象添加到源或目标属性。

步骤 8 如果需要，向规则中添加其他条件。

下一步做什么

请参阅动态属性规则条件。

pxGrid 云身份源 故障排除

这些主题介绍如何对 pxGrid 云身份源 进行故障排除。

相关主题

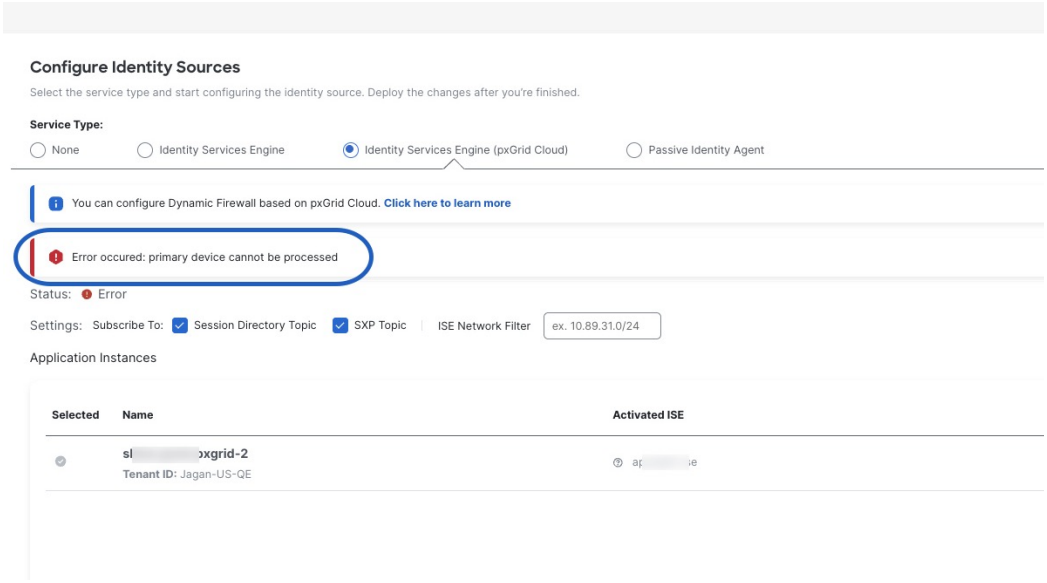
无法处理主设备，第 27 页

无法处理主设备

每个 Cisco ISE 集群必须与且仅与一个应用实例相关联，且通常位于一个专用租户中。

如果将一个 Cisco ISE 与多个应用实例相关联，身份源将显示错误，例如`错误：无法处理主设备`或 `ISE 运行状况不正常。`

示例：



解决方案是，在将该租户用于任何其他租户或应用实例之前，先从该租户的其他应用实例中正确停用 ISE。

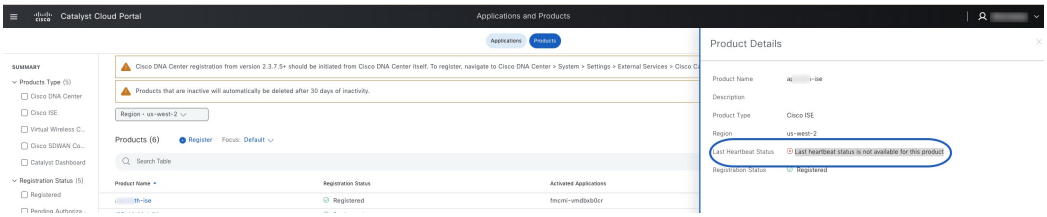
过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 在页面顶部，点击**应用**。

步骤 3 找到一款已激活的 Cisco ISE 产品，并确认是该产品导致了相关问题。

示例：



步骤 4 等待产品被删除。

步骤 5 停用应用实例，如停用 pxGrid 云 应用实例，第 28 页中所述。

停用并删除 pxGrid 云身份源

这些主题讨论了如何选择性地：

- 在 Catalyst 云门户 中停用 FMC 应用实例。

  您可以执行此可选任务来排除 Cisco ISE 集成问题。

- 从 Secure Firewall Management Center 中删除 pxGrid 云身份源。

  只有在确定不再使用身份源时，才应将其删除。

相关主题

停用 pxGrid 云 应用实例，第 28 页
删除 pxGrid 云身份源，第 31 页

停用 pxGrid 云 应用实例

（可选。）此任务介绍如何使用 Catalyst 云门户 停用 pxGrid 云 应用实例。只有当您的 Cisco ISE 或 pxGrid 云 停止工作或您需要更新时，才应执行此操作。

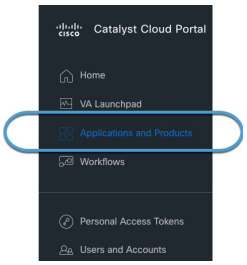
开始之前

如激活 pxGrid 云身份源，第 16 页中所述，请确保当前的 pxGrid 云身份源 处于活动状态。

过程

步骤 1 登录 Cisco Catalyst Cloud Portal。

步骤 2 在 Catalyst 云门户 中，点击☰ > **应用程序和产品**，如下图所示：

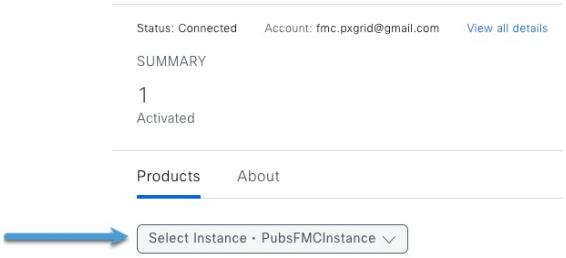


步骤 3 点击 **应用**。

步骤 4 点击防火墙管理中心的**管理**。

步骤 5 从**选择实例**列表中，点击您之前创建的防火墙应用的名称。

示例：



步骤 6 在“操作”列中，点击更多图标 （ ··· ）> **停用**。

步骤 7 等待直至移除产品。

如有必要，您可以点击 **刷新** (↻) 以查看更新后的状态。

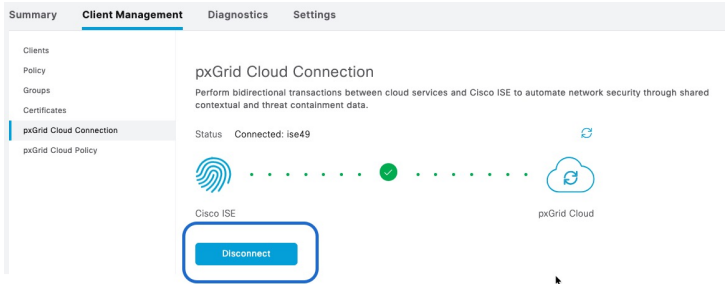
步骤 8 ISE 3.3 或更低版本：断开应用实例的连接：

a) 以管理员身份登录 Cisco ISE。

b) 点击**管理** > **pxGrid 服务** > **客户端管理** > **pxGrid Cloud 连接**。

c) 点击**断开连接**。

示例：



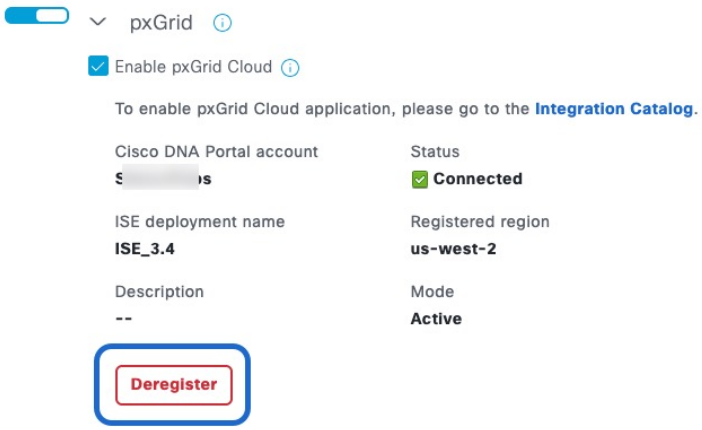
步骤 9 ISE 3.4 或更高版本：取消注册应用实例：

a) 以管理员身份登录 Cisco ISE。

b) 点击**管理** > **系统** > **部署**。

c) 展开**部署**。
d) 点击 ISE 节点的名称。
e) 在**常规设置**选项卡页面中，滚动至找到 **pxGrid**。
f) 点击**取消注册**。

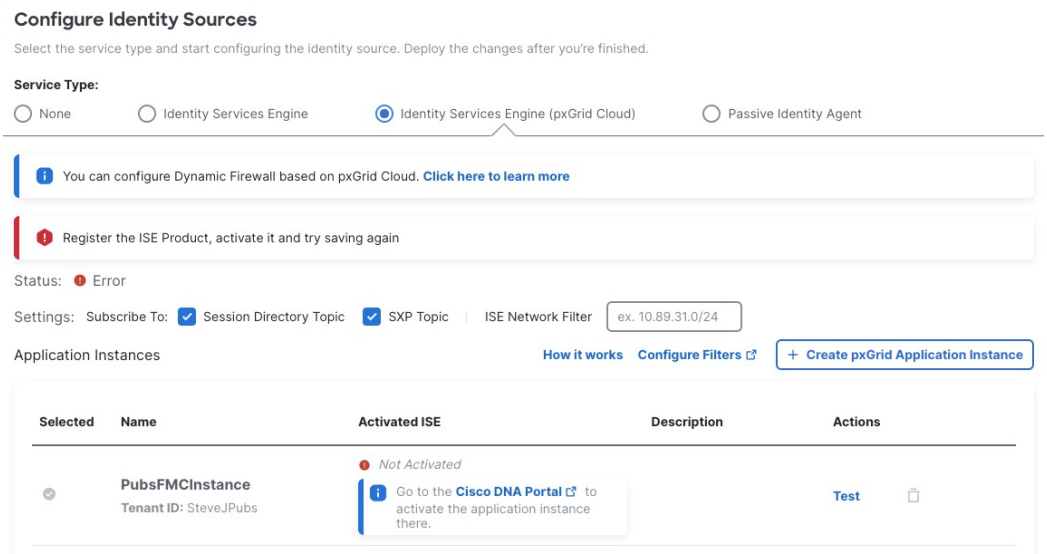
示例：



步骤 10 要验证已在 Secure Firewall Management Center 中停用应用实例：

a) 登录 Secure Firewall Management Center。
b) 点击 **集成** > **身份** > **身份源**
c) 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。
d) 验证已激活 ISE 列中是否显示**未激活**。

示例：



下一步做什么

- 要向 pxGrid 云 注册 Cisco ISE 并激活应用实例，请参阅：
  - ISE 3.3 及更早版本：使用 Catalyst 云门户 注册 Cisco ISE，第 6 页。
  - ISE 3.4 及更高版本：创建应用实例。
- 要彻底删除身份源，请参阅删除 pxGrid 云身份源，第 31 页。

删除 pxGrid 云身份源

（可选。）此任务说明如何从 Secure Firewall Management Center 中删除不想再次使用的 pxGrid 云身份源。

开始之前

按照停用 pxGrid 云 应用实例，第 28 页中所述，从 Catalyst 云门户 中停用 FMC 应用实例。

过程

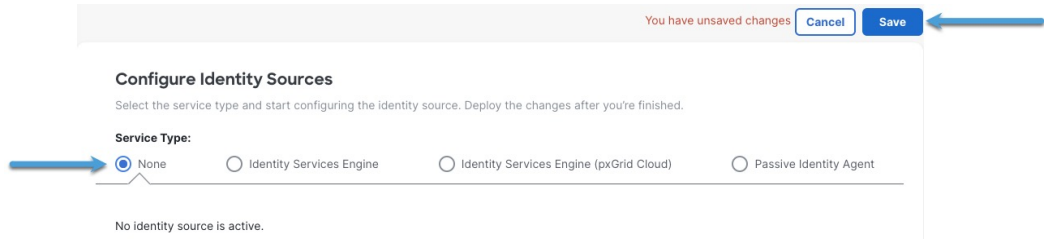
步骤 1 登录至 Secure Firewall Management Center

步骤 2 点击 **集成** > **身份** > **身份源**

步骤 3 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 4 对于服务类型，请点击**无**。

示例：



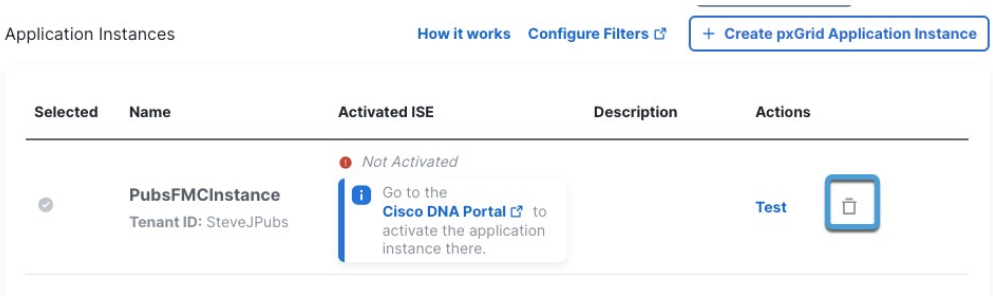
步骤 5 点击**保存**。

步骤 6 您需要确认您的选择。

步骤 7 点击**身份服务引擎（pxGrid 云）(Identity Services Engine [pxGrid Cloud])**。

步骤 8 请点击 删除 ()。

示例：


Application Instances
How it works
Configure Filters
+ Create pxGrid Application Instance
Selected
Name
Activated ISE
Description
Actions
Not Activated
PubsFMCInstance
Tenant ID: SteveJPubs
Go to the
Cisco DNA Portal
to activate the application instance there.
Test

步骤 9 您需要确认操作。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。