通过协调集成ISE和SecureX OnPremises

目录

简介

本文档介绍通过协调将身份服务引擎和SecureX与来自Cisco Secure GitHub的工作流程集成的步骤。

先决条件

思科建议您了解以下主题：

- Cisco ISE配置体验
- ISE API知识
- SecureX协调知识

要求

您必须在网络中部署思科ISE并具有活动的SecureX帐户。协调工作流程通过SecureX浏览器扩展触发。

在我们的示例中，要使用的工作流程是从Cisco Secure GitHub页面导入的，此过程也适用于自定义工作流程。

使用的组件

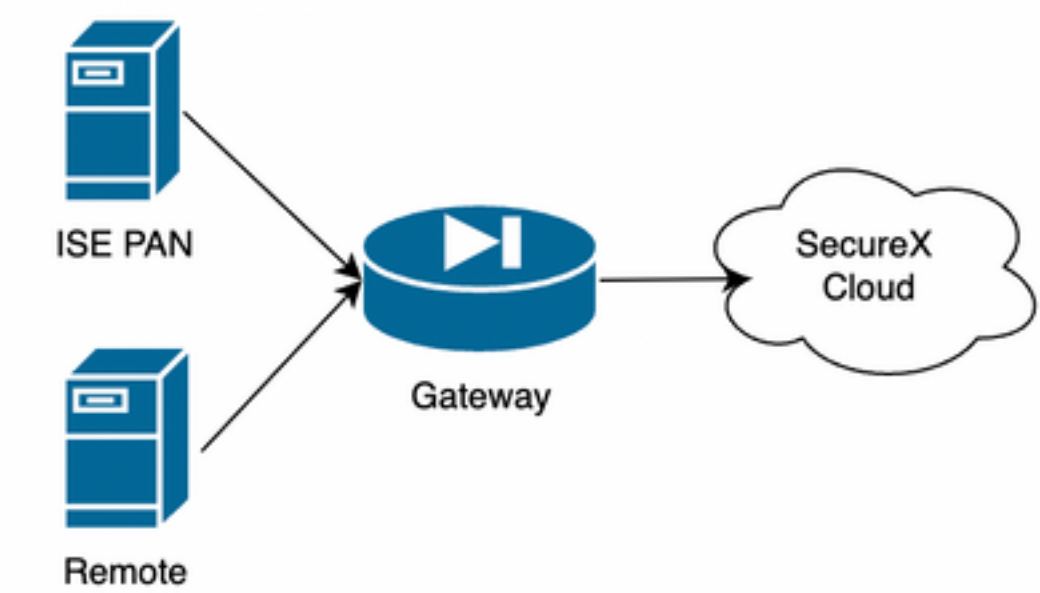
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

- 身份服务引擎ISE版本3.1
- SecureX帐户

- SXO远程设备版本1.7

配置

网络图



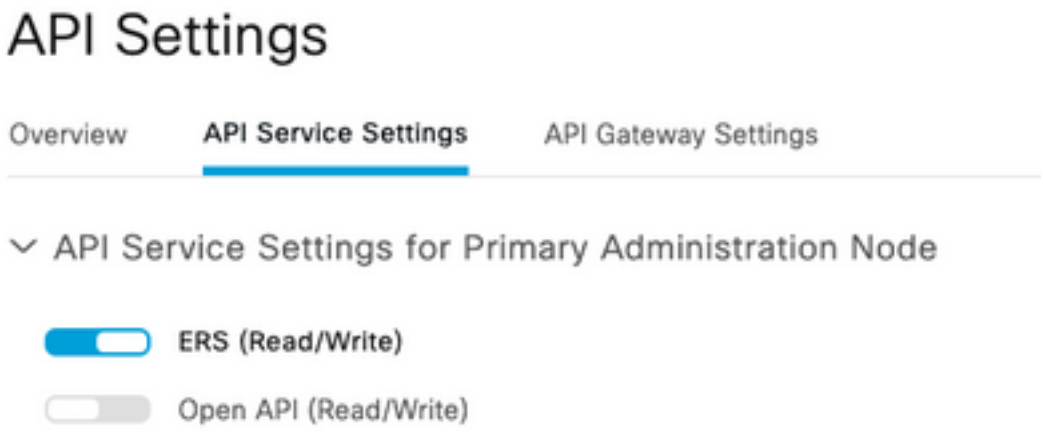
在我们的示例中，ISE PAN和远程服务器位于同一子网中以实现直接连接。

由于ISE是内部设备，远程服务器与Secure-X云联系并将信息转发到ISE PAN

配置

ISE PAN配置

1.导航到**管理>系统>设置> API设置> API服务设置**并启用**ERS（读/写）**

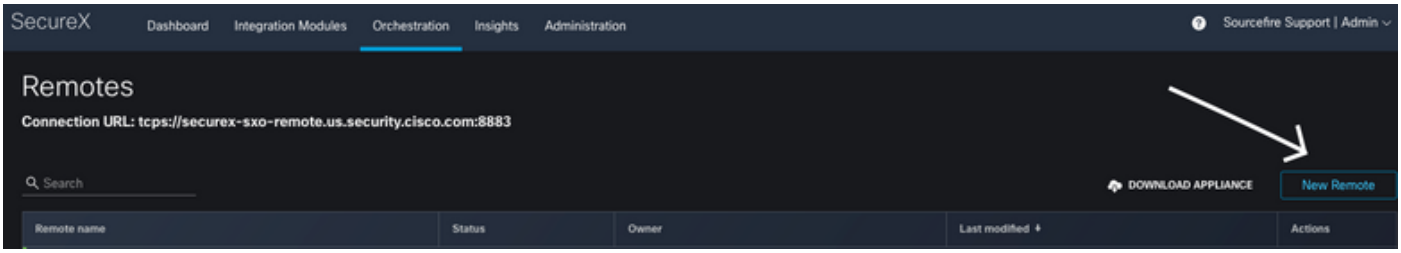


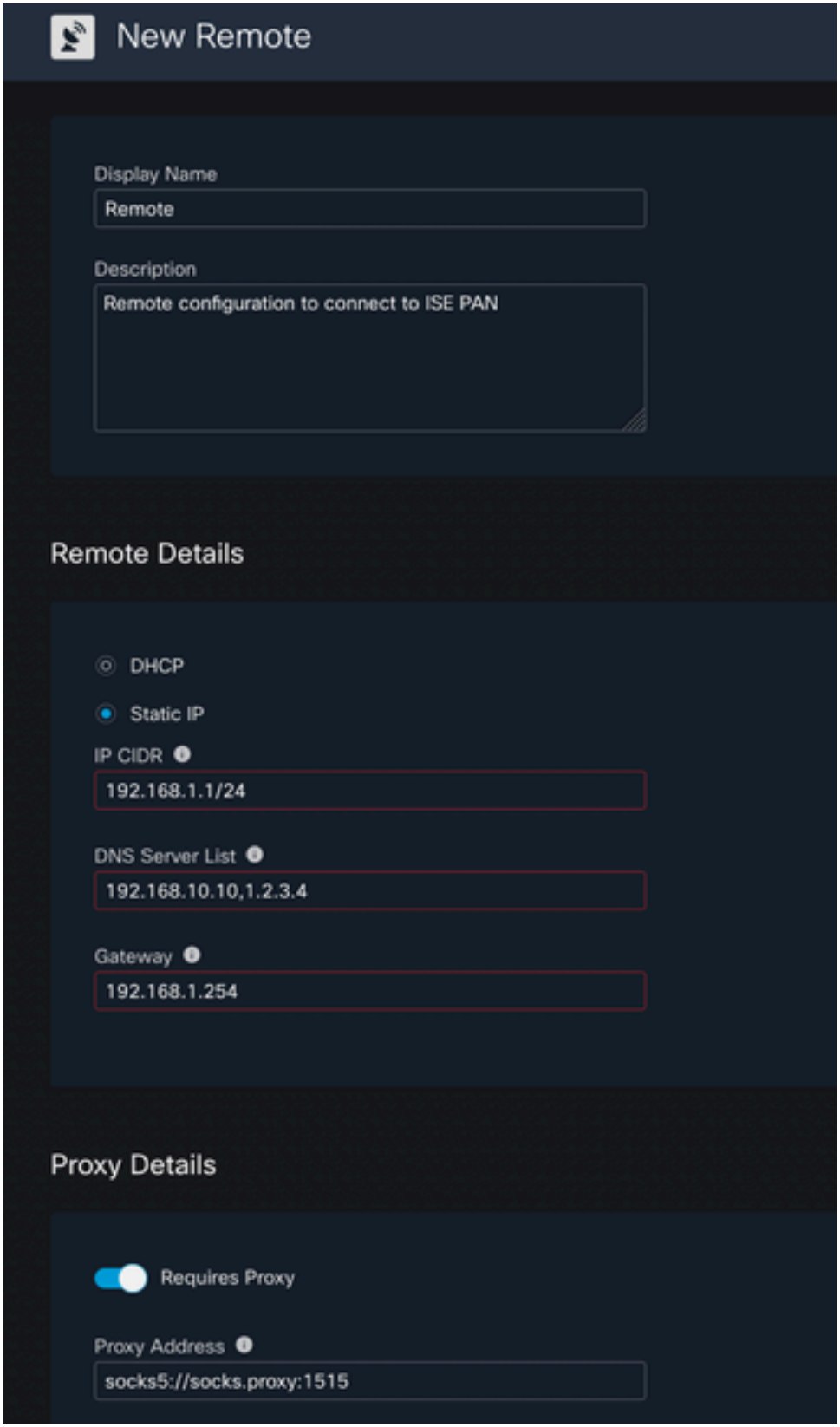
2.（可选）为Secure-X连接创建新用户，导航到**Administration > System > Admin Access > Administrator > Admin Users**并创建新用户，此新用户必须具有“ERS Admin”权限，或者它可以是超级管理员用户。

配置和部署远程服务器

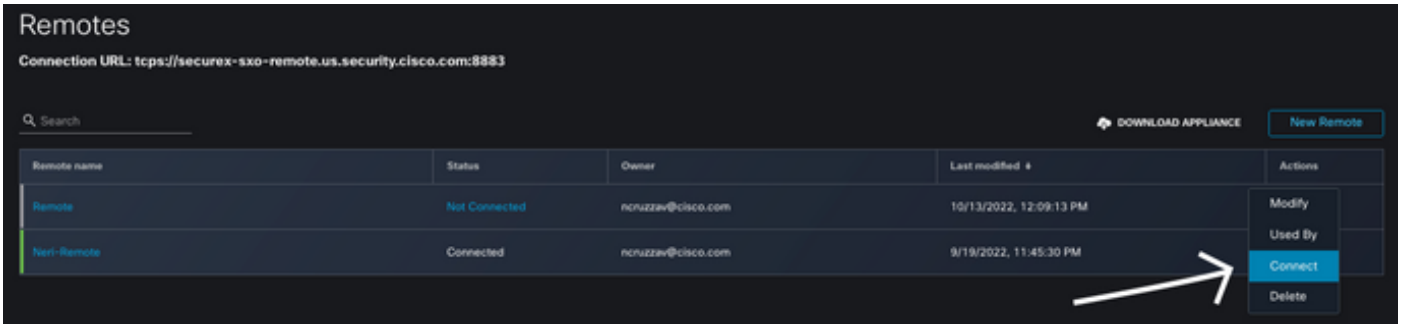
1.配置远程服务器，在Secure-X控制台上，导航到**Orchestration > Admin > Remote Configuration**并选择选项**New Remote**,IP地址信息是创建VM时使用的信息，并且它必须位于部署ISE PAN的同一子网中。

> **注意**：如果通过代理连接到云，则目前仅支持SOCKS5代理用于此目的。

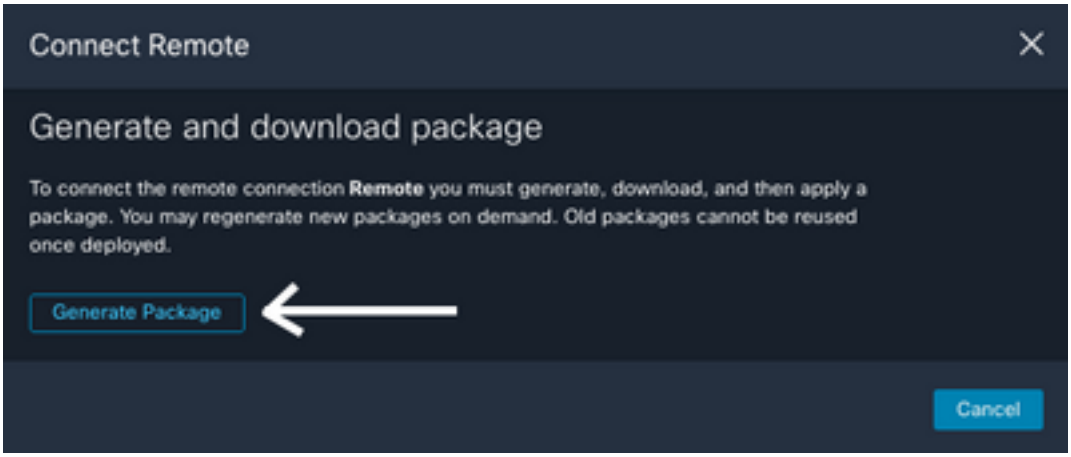




2.下载要用于VM部署的已配置设置，保存信息后，远程将显示为“**Not Connected”，在“操作”下导航，然后选择“连**接”。



选择**Generate Package**，此操作将下载一个.zip文件，其中包含刚刚配置为在部署虚拟机时使用的信息。



3.下载并安装VM，在**New Remote** 选择**DOWNLOAD APPLIANCE**旁，此操作将下载用于部署远程服务器的OVA映像。

有关远程VM规格，请参阅SecureX Remote Setup指南

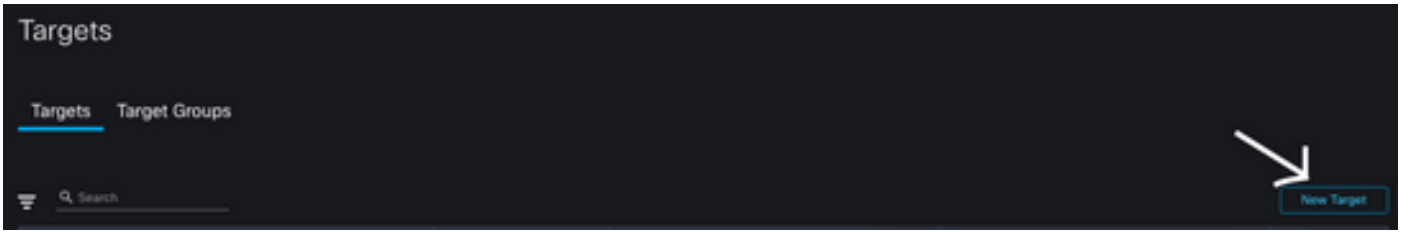
创建VM时，必须在**编码用户数据**上使用ZIP文件内的下载信息，这会在服务器启动后将配置的远程信息填充到服务器中。

4.虚拟机启动后，它会自动连接到SecureX帐户，以验证连接是否已启动，在“远程”配置下，您必须看到状态更改为“已连接”(**Connected)**

在SecureX上配置目标

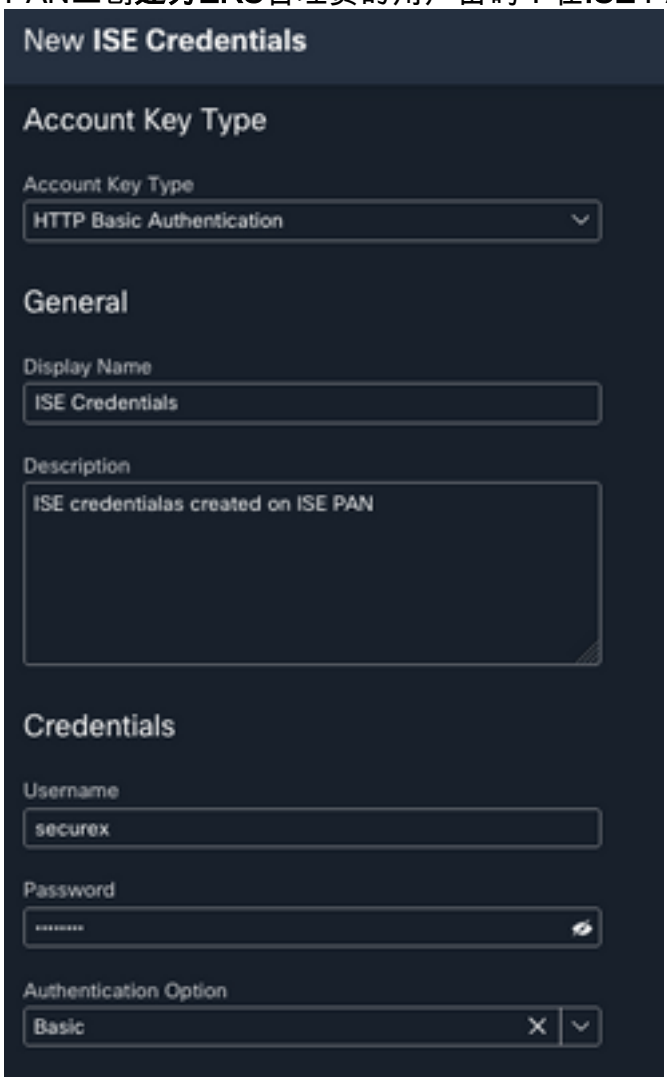
对于协调与设备配合使用而言，配置**Target**非常重要，Secure X使用此目标发送API调用，并通过协调与设备交互

1.定位至**协调>目标>新目标**

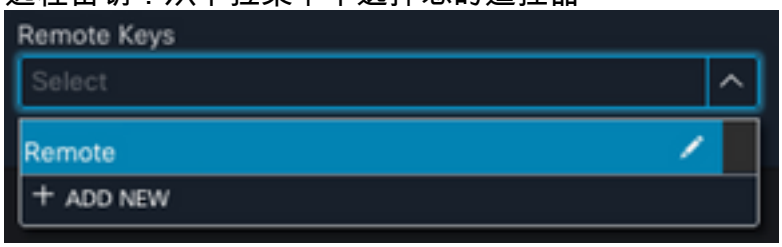


2.使用下一条准则填写目标信息

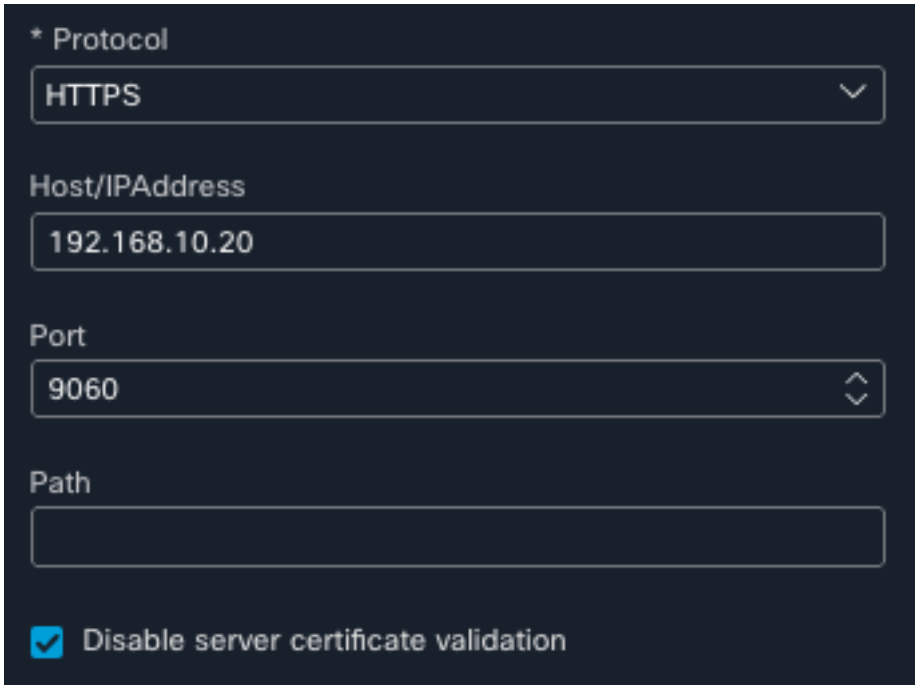
- 显示姓名：目标识别器
- 描述:确定目标用途的小说明
- 帐户密钥：您需要在此配置用户/密码以通过API访问ISE 无帐户密钥：**错误**默认帐户密钥：选择**新增** 帐户密钥类型：**HTTP基本身份验证**显示姓名：帐户密钥标识符username：在**ISE** PAN上创**建为ERS**管理员的用户密码：在**ISE** PAN上创建的用户**的密码**身份验证选项：**基本**



- 远程:此处，您需要选择以前配置的远程连接
  远程密钥：从下拉菜单中选择您的遥控器



- HTTP:此处，您需要配置**ISE** PAN的API**信息** 协议：**HTTPS**主机/IP地址：**ISE PAN专用IP**端口：**9060**路径：将其留空禁用服务器证书验证：**选中此框**



- 代理：由于代理配置包含在远程配置中，因此您可以将此部分留空
- 选择**提交**

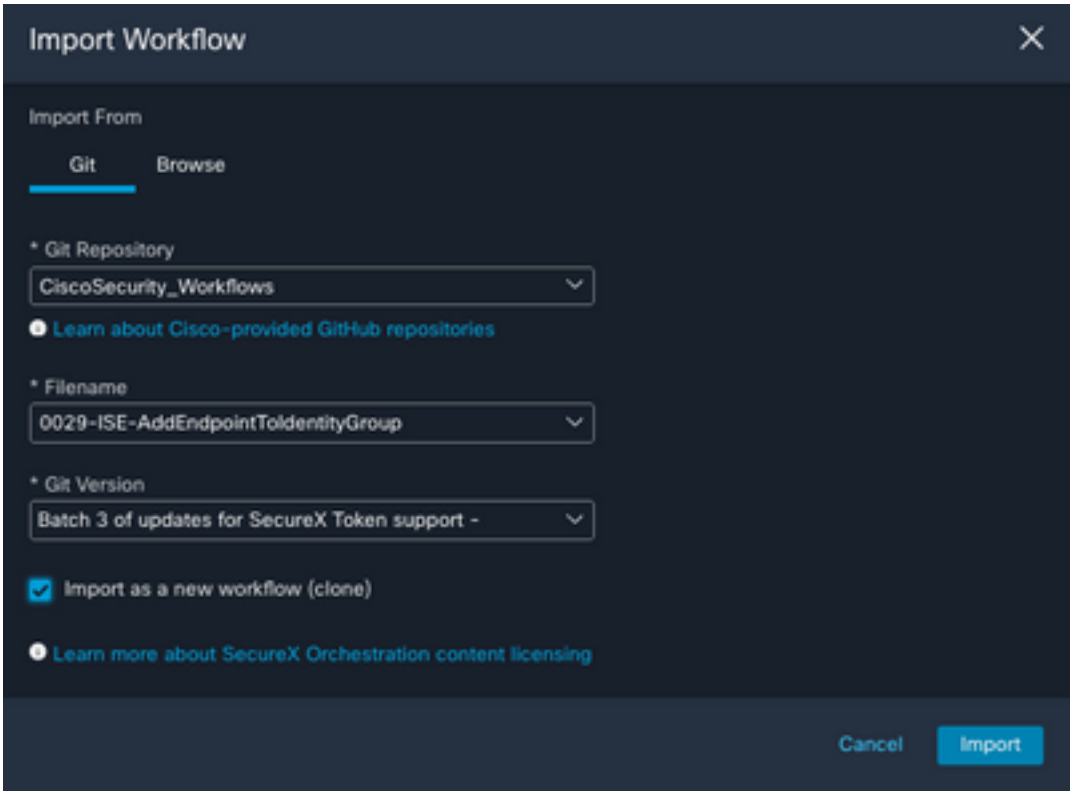
从Cisco Secure GitHub导入工作流程

对于此示例，要使用的工作流程是“将终端添加到身份组”，您可以使用Cisco Secure GitHub页面上列出的任何工作流程，也可以创建自定义工作流程。

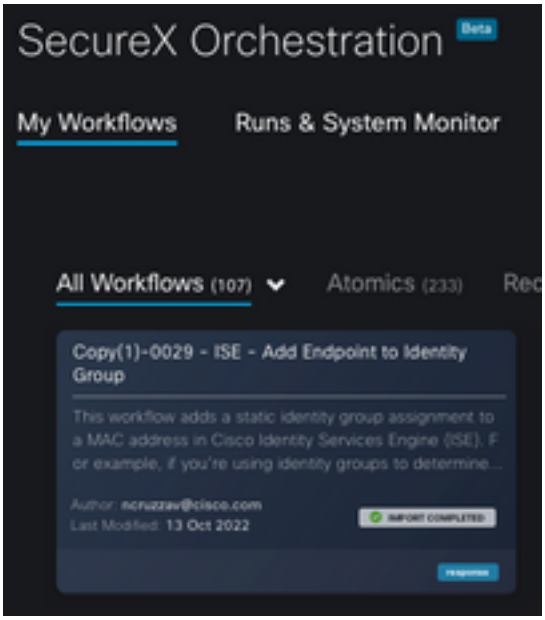
1.定位至**协调>我的工作流>导入工作流**

2.要导入工作流，请填写以下信息并选择“导**入**”；要标识要导入的工作流，可以按名称或按工作流编号进行搜索

- Git存储库：**CiscoSecurity_Workflows**（工作流程所在位置）
- 文件名：**0029-ISE-AddEndpointToIdentityGroup**（选择要使用的工作流数量）
- Git版本：**SecureX令牌支持的第3批更新**（最新版本）
- 作为新工作流程导入（克隆）：选中（此操作将导入工作流并创建工作流的克隆）

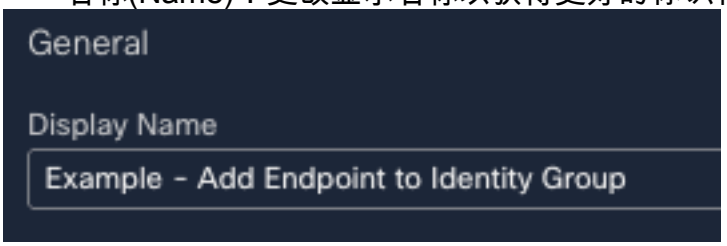


3.导入后，新模板将显示在**My Workflows**下，选择新创建的工作流程以编辑参数，使其与ISE配合使用

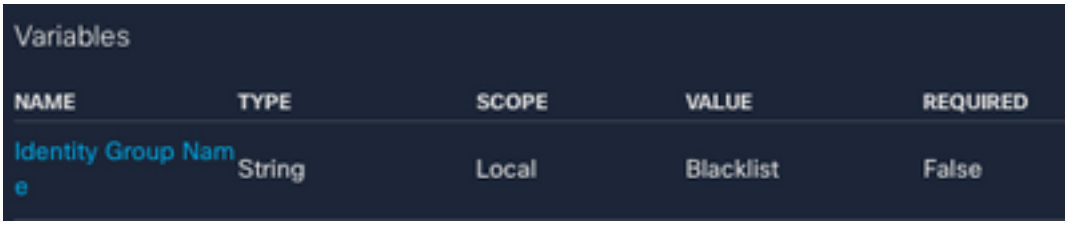


4.由于这是一个预构建工作流，因此只需修改工作流的3个部分：

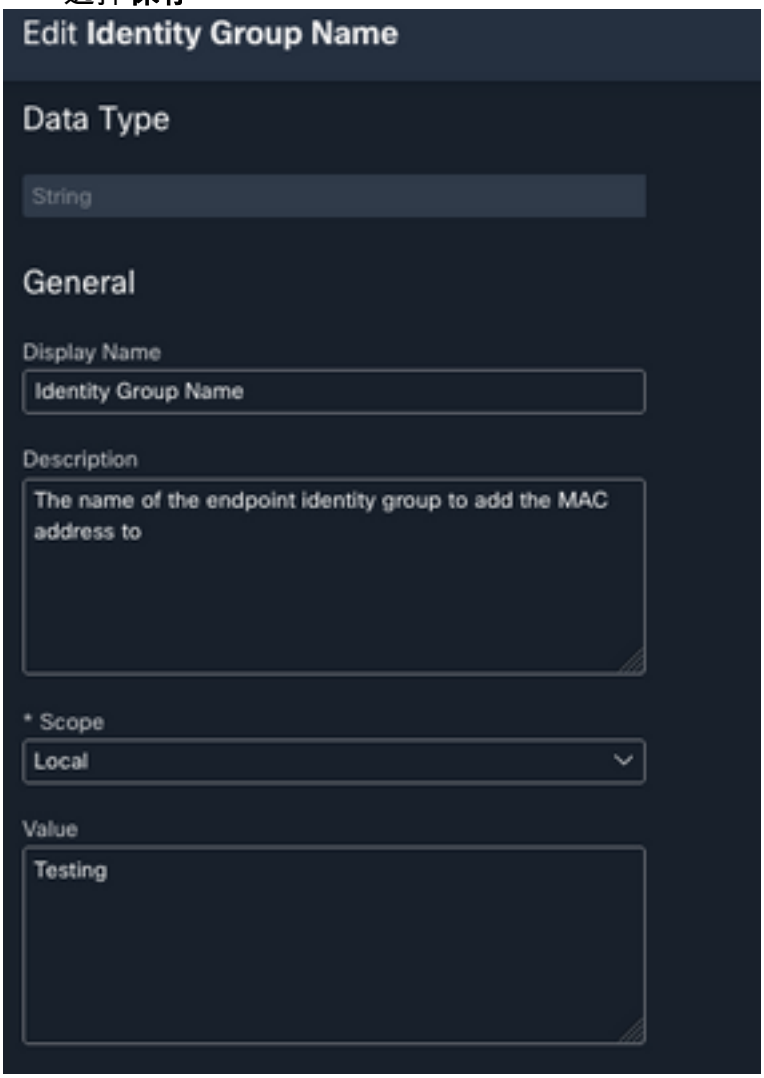
- 名称(Name)：更改显示名称以获得更好的标识符



- 身份组变量 在Variables下，编辑**Identity Group Variable**，默认情况下为**Balcklist**，选择变量并配置要通过业务流程修改的身份组名称



- 选择**保存**



- 目标：配置之前配置的**Target** 目标类型：**HTTP终端**目标：**已配置目标的名称**

验证

完成所有配置后，就到了测试工作流程的时候了

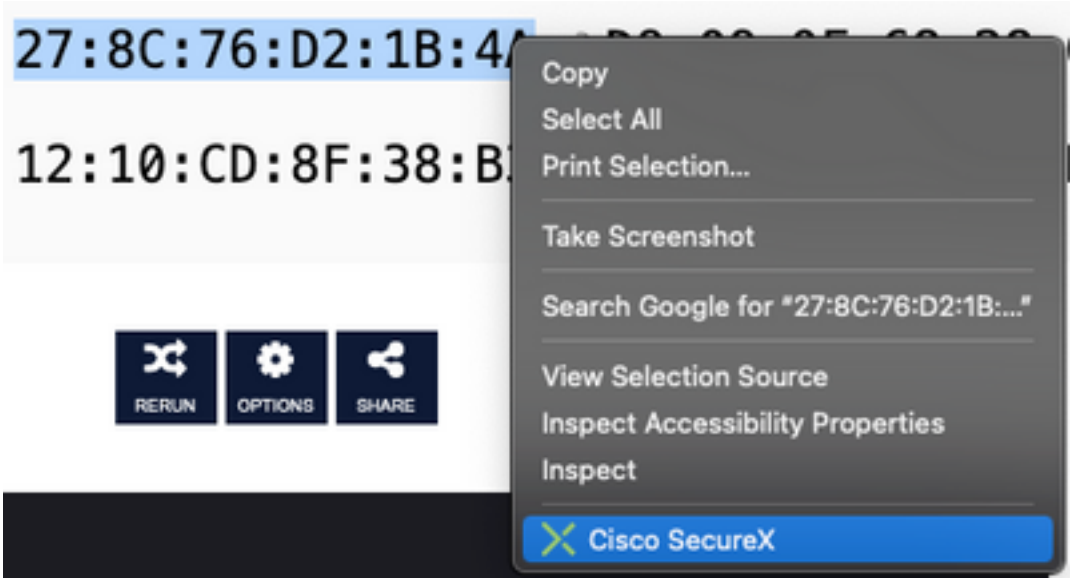
测试的工作流程将执行以下操作：如果您在网页中找到MAC地址，它可能位于ISE本身或其他网页（如威胁响应）；通过SecureX浏览器扩展，工作流程通过API在ISE数据库中查找该MAC地址，如果MAC不存在，可观察将添加到终端身份组中，而无需复制值并访问ISE。

要演示这一点，请查看下一个示例：

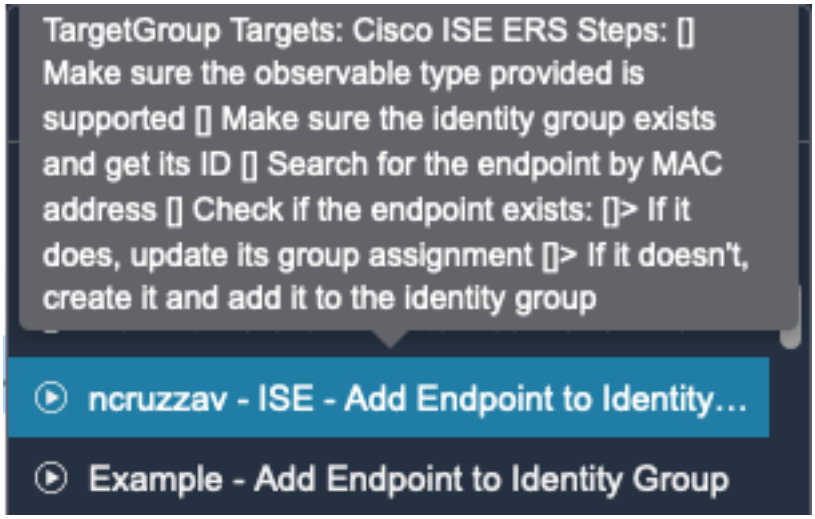
1.所选工作流程使用可观察类型“**MAC地址**”

2.在网页上查找MAC地址，然后右键点击。

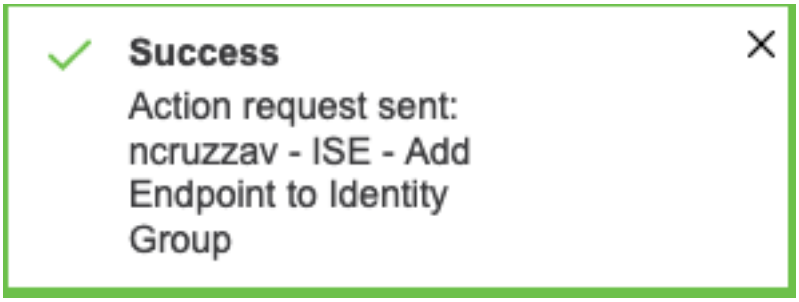
3.选择**SecureX**选项



4.选择之前创建的**工作流**

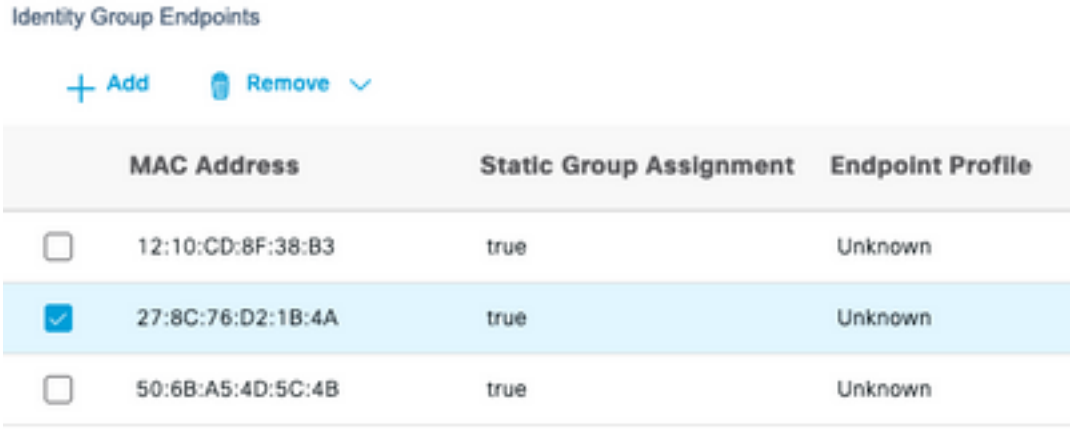


5.确认任务已成功执行



6.在ISE PAN上，导航到**管理>身份管理>组>终端身份组>（在工作流中配置的组）**

7.打开工作流程上配置的**终端身份组**，并确认所选的MAC地址已添加到该MAC地址列表中



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。