# 为Microsoft Entra ID SSO配置SNA Manager

## 目录



## 简介

本文档介绍如何配置安全网络分析(SNA)以使用Microsoft Entra ID进行单点登录(SSO)。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Microsoft Azure
- 安全网络分析

### 使用的组件

- SNA Manager v7.5.2
- Microsoft Entra ID

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。

## 配置步骤

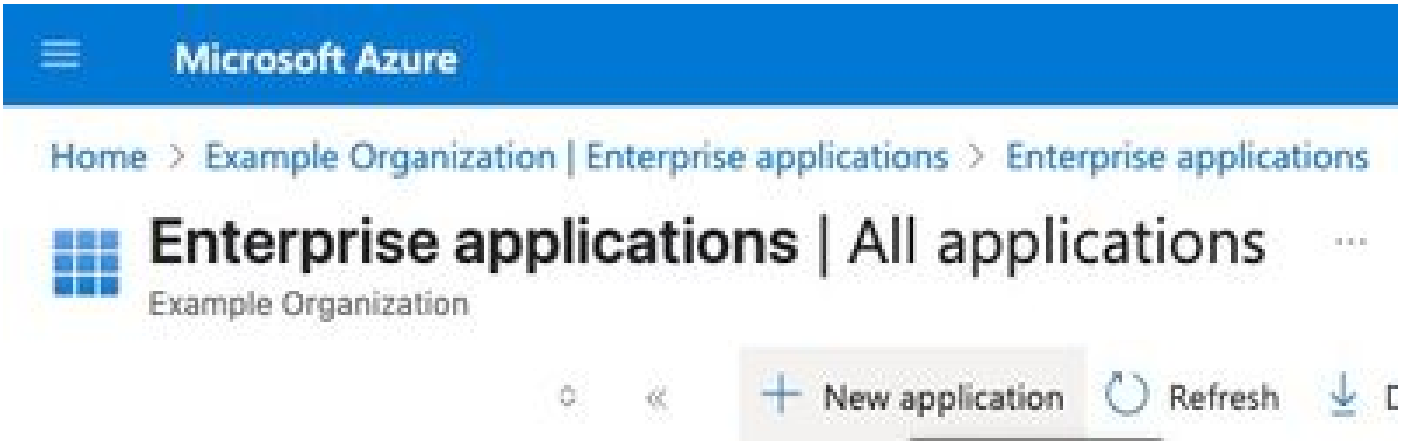
### 在Azure中配置企业应用程序

1.登录到Azure云门户。

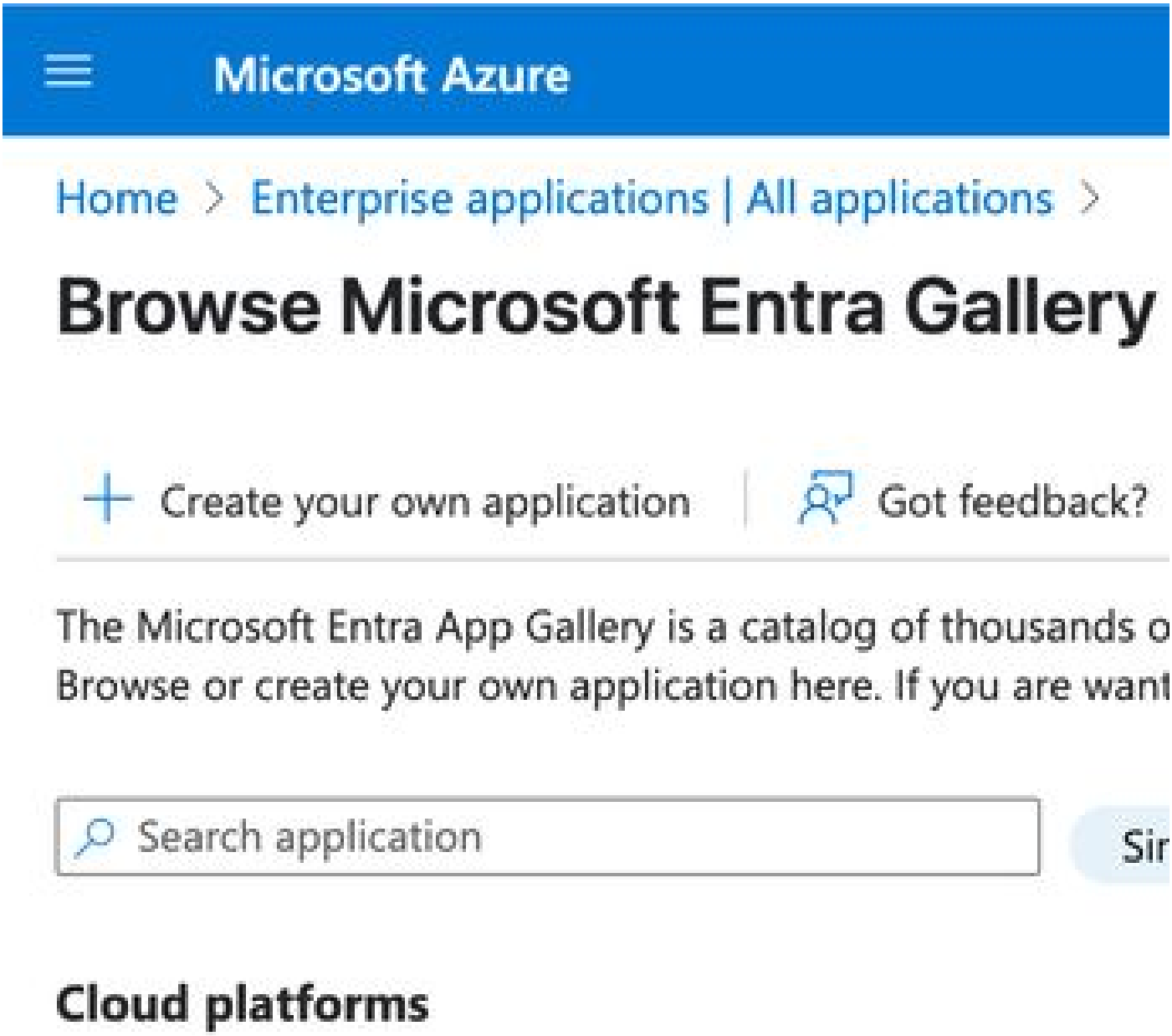
2.在搜索框中搜索Entra ID服务，然后选择Microsoft Entra ID。


3.在左侧窗格中，展开Manage，然后选择Enterprise Applications。

4.单击New Application。



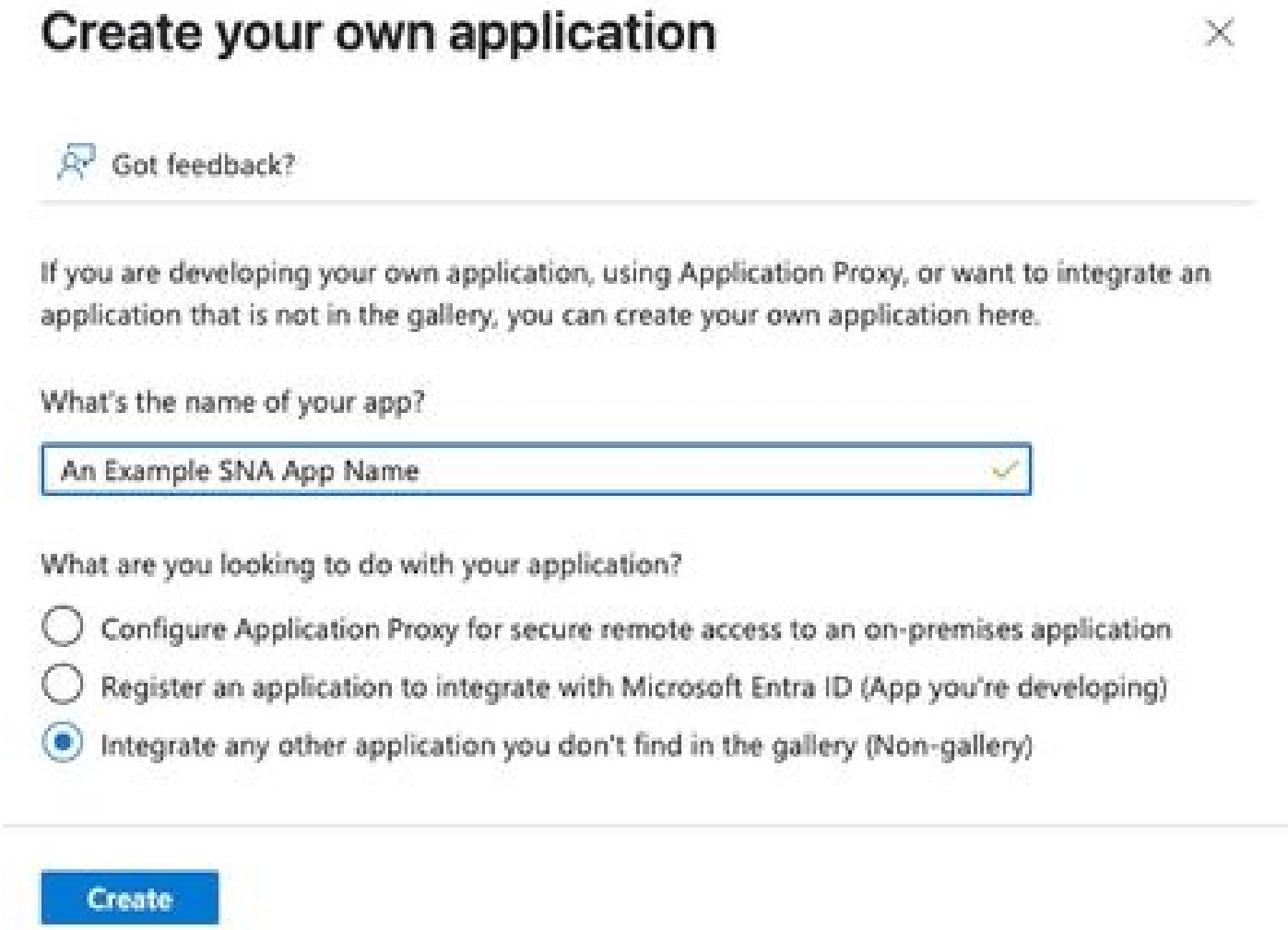

5.在加载的新页面上，选择“创建自己的应用程序”。



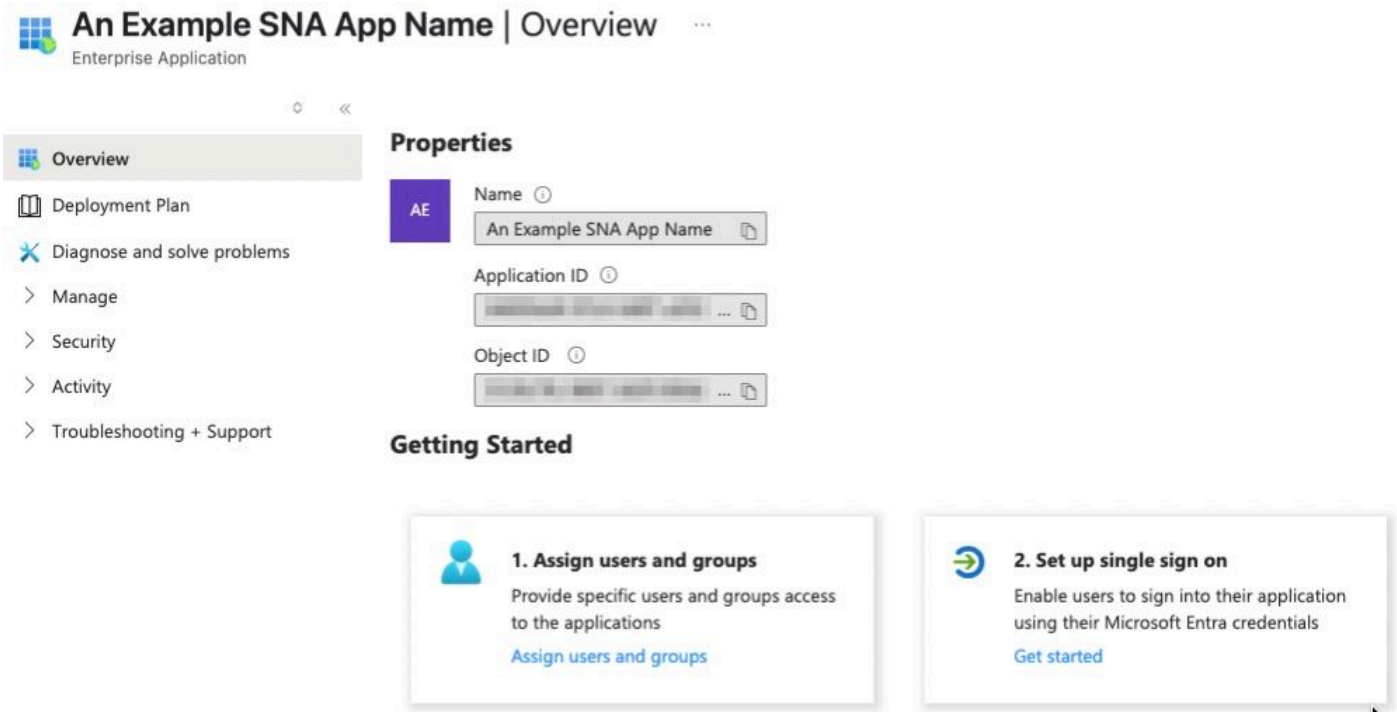

Azure-UI

6.在What’s name of your app（您的应用名称是什么？）中为应用提供名称。字段。

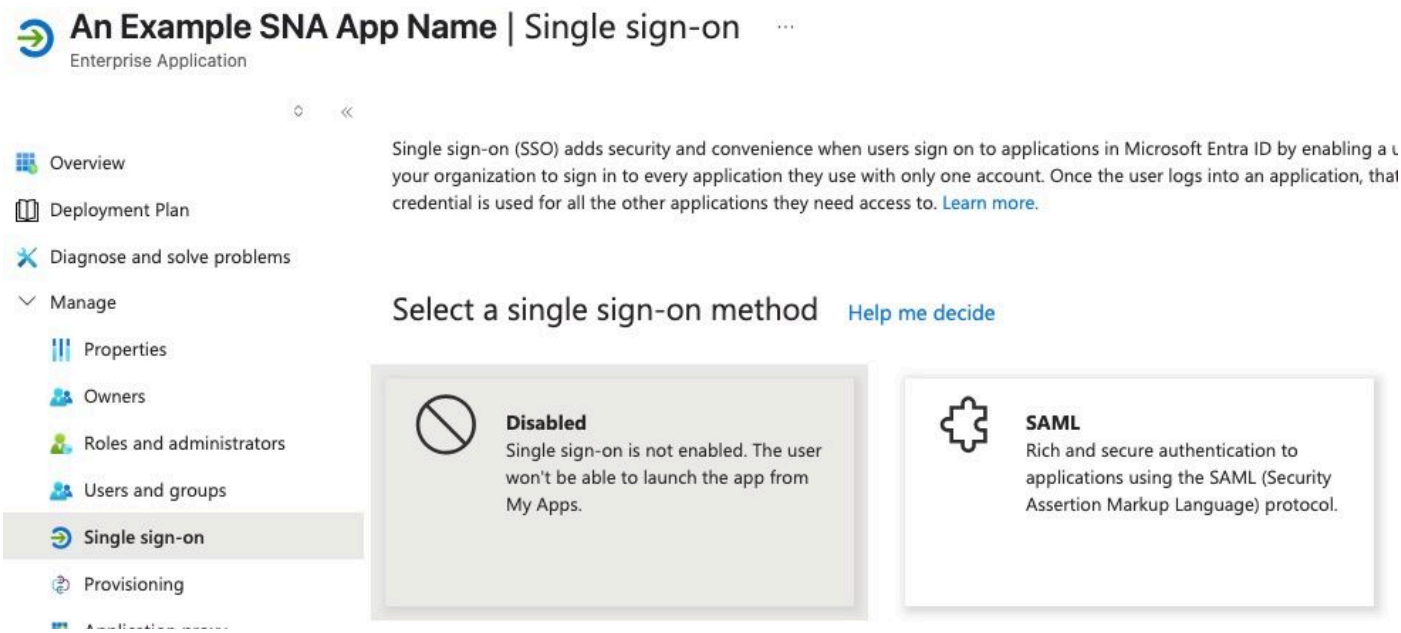
7.选择单选按钮“集成在图库（非图库）中找不到的所有其他应用程序”，然后单击“创建”。



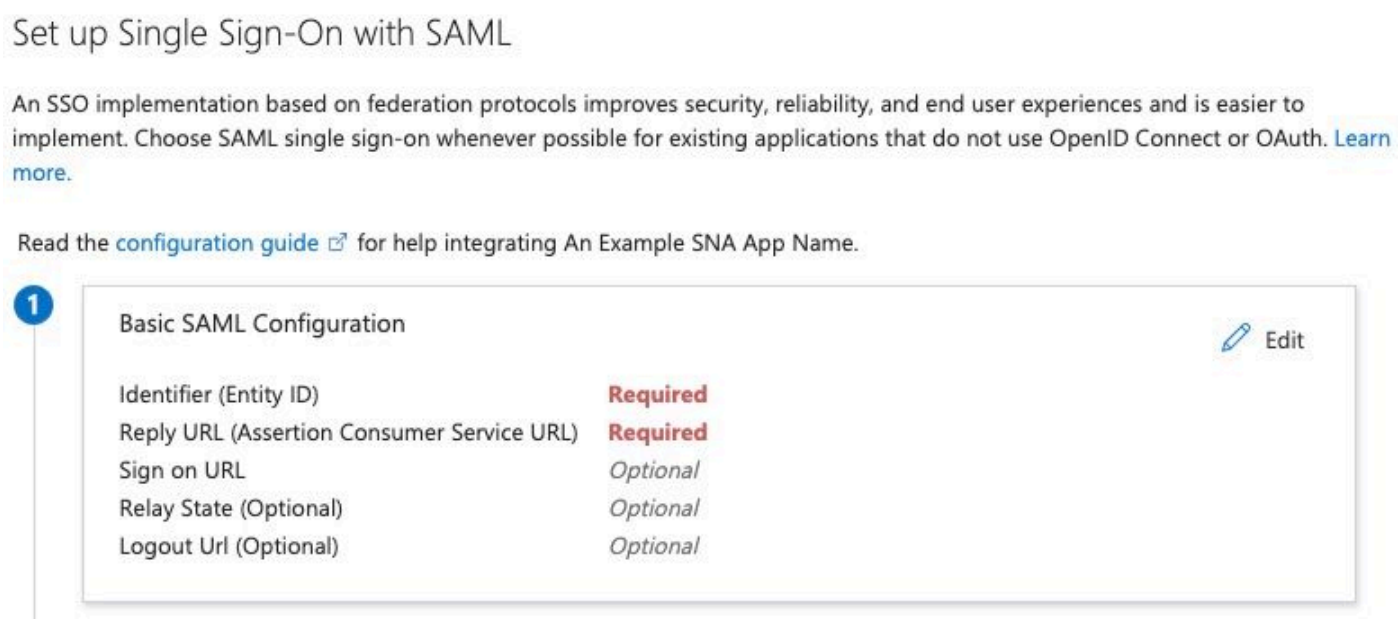

8.在新配置的应用控制面板上，单击设置单点登录。



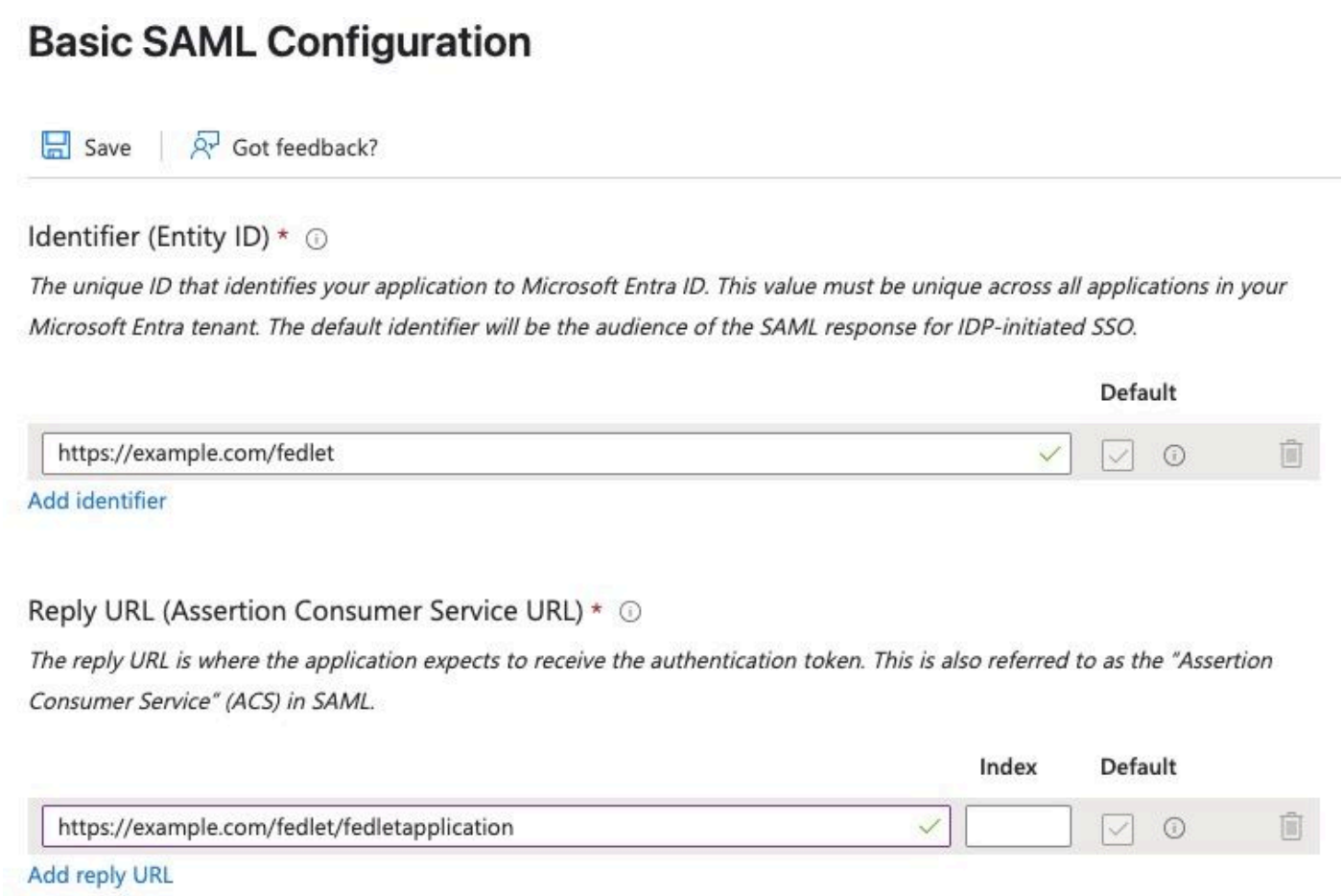
9.选择SAML。



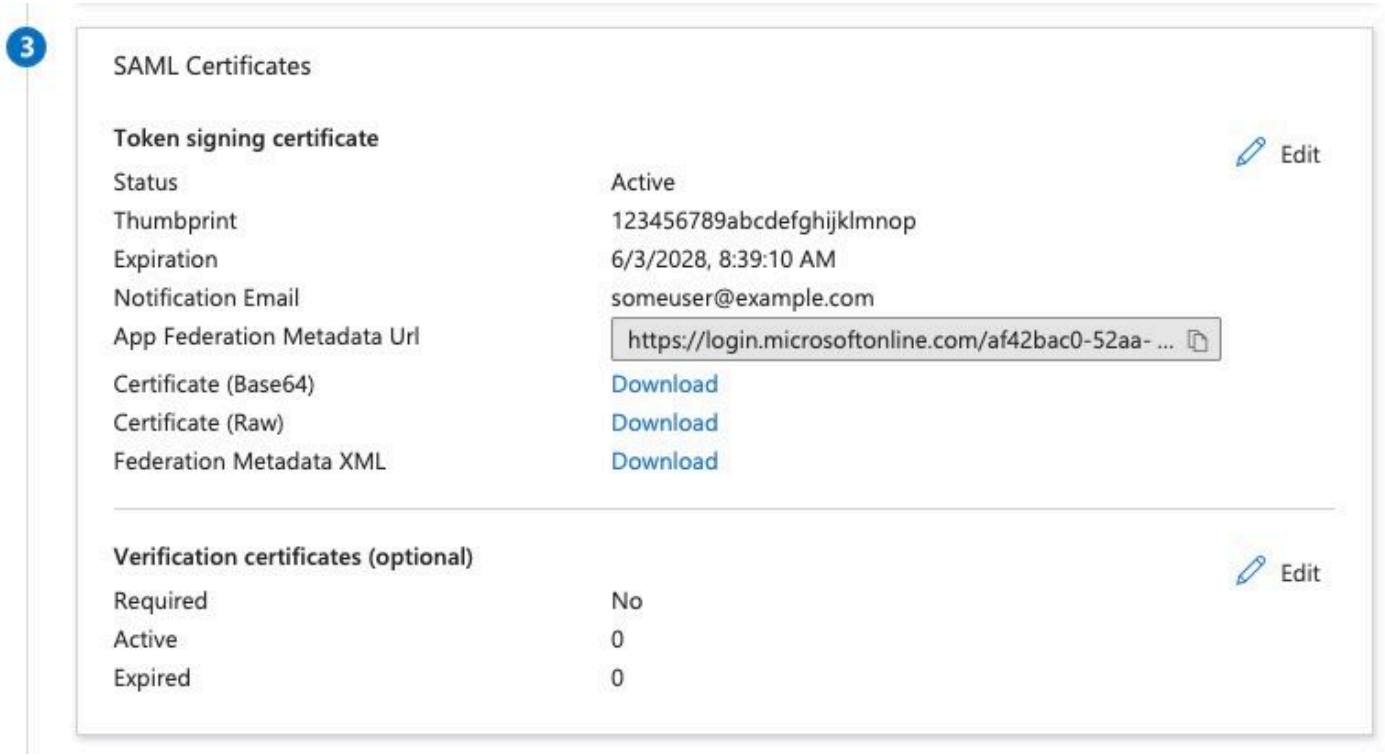

10.在“使用SAML设置单一登录”页面上，单击“基本SAML配置”下的编辑。




11.在Basic SAML Configuration窗格下，将Add Reply URL配置到 https://example.com/fedlet/fedletapplication，用SNA Manager的FQDN替换example.com，然后单击save。

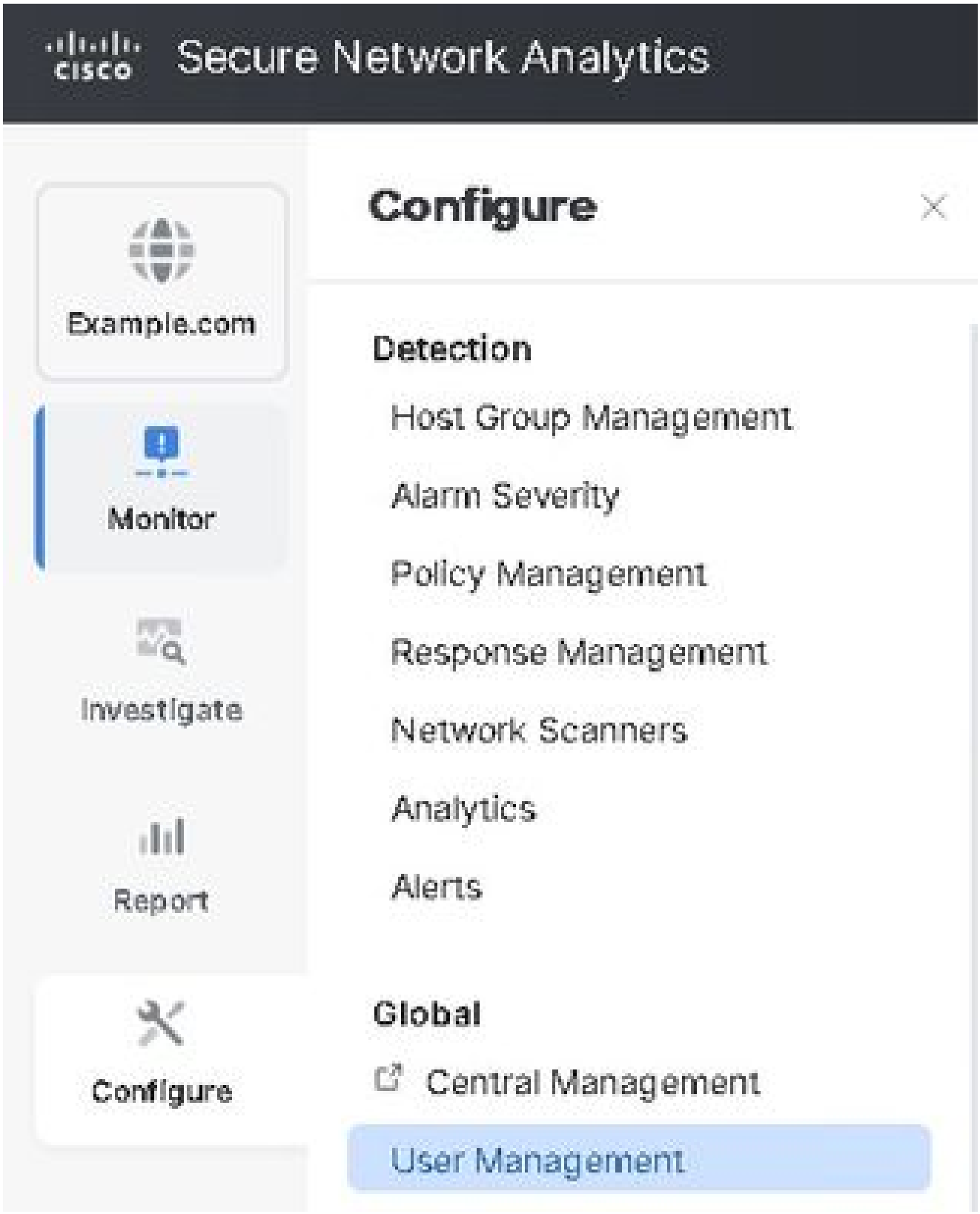



12.找到SAML Certificates卡并保存App Federation Metadata URL字段值，然后下载Federation Metadata XML。

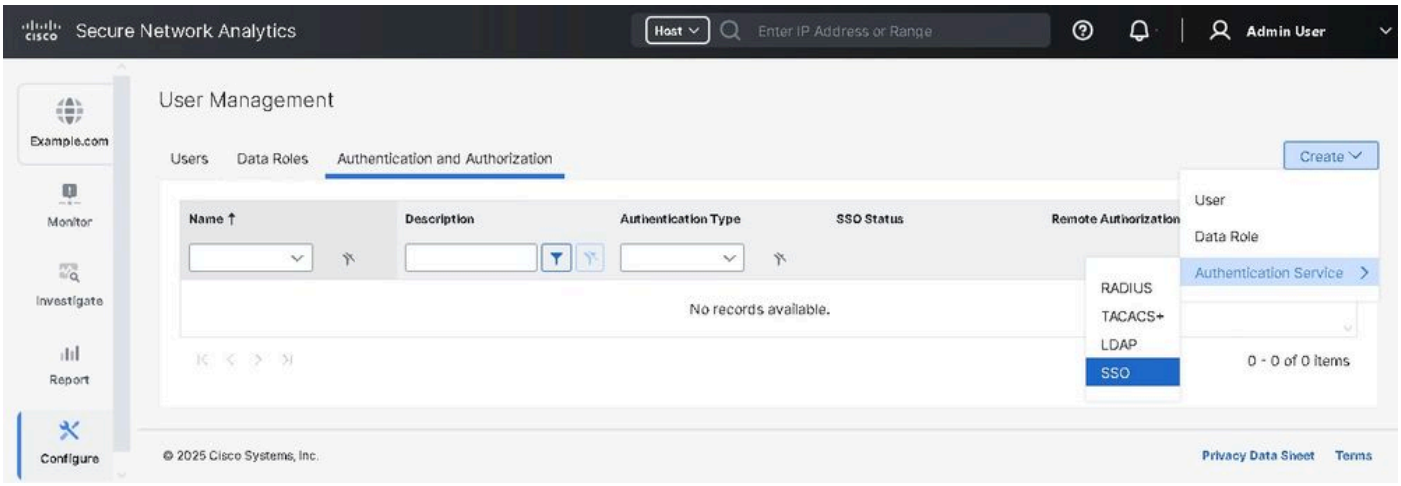



在SNA中配置和下载服务提供商XML文件

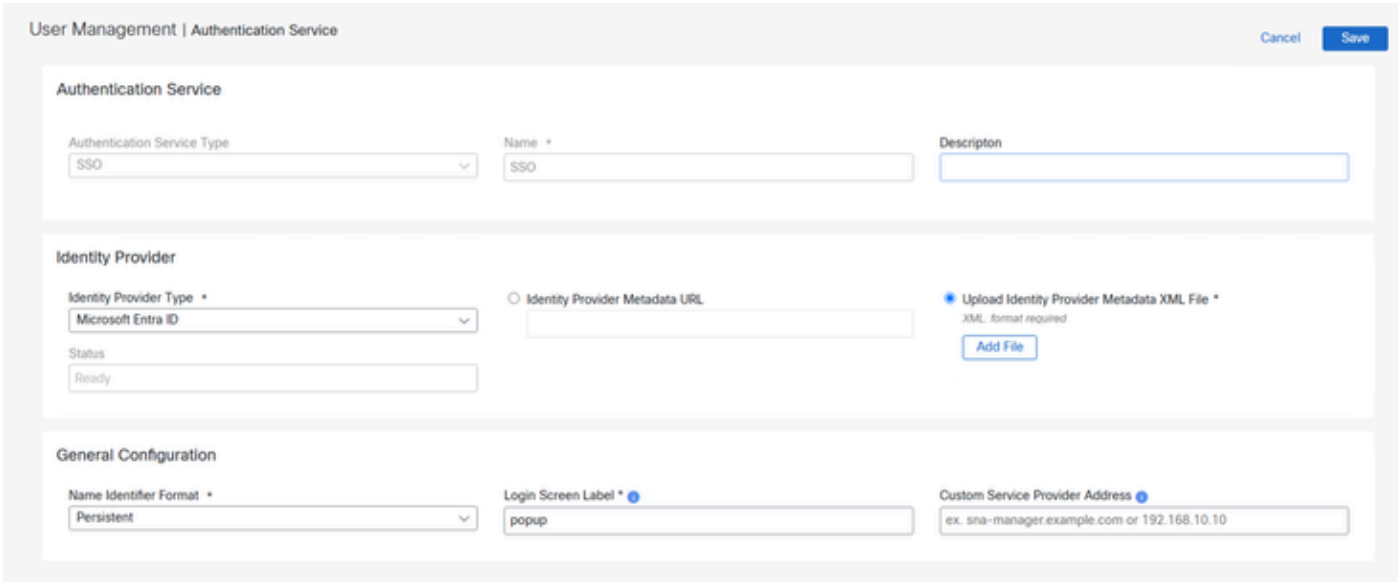
1. 登录到SNA Manager UI。
2. 导航到配置>全局>用户管理。

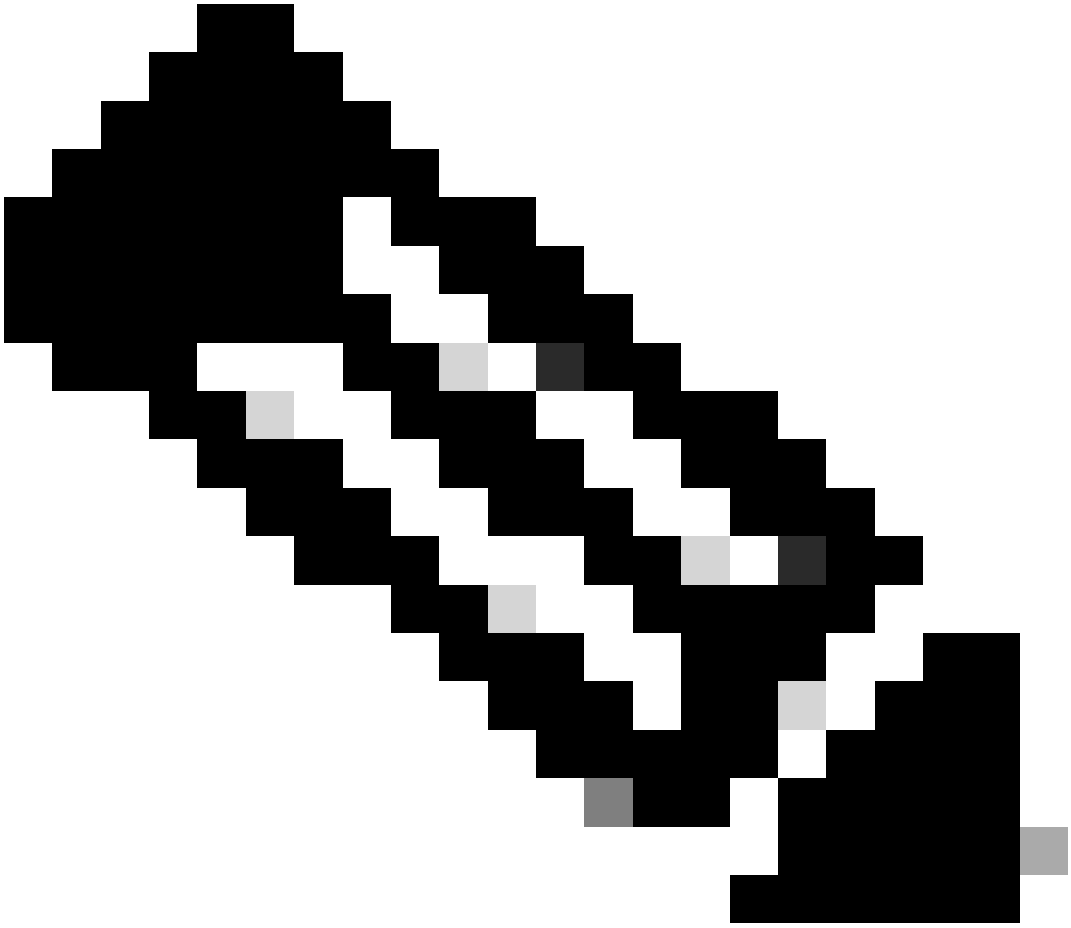



3. 在Authentication and Authorization选项卡下，单击Create > Authentication Service > SSO。



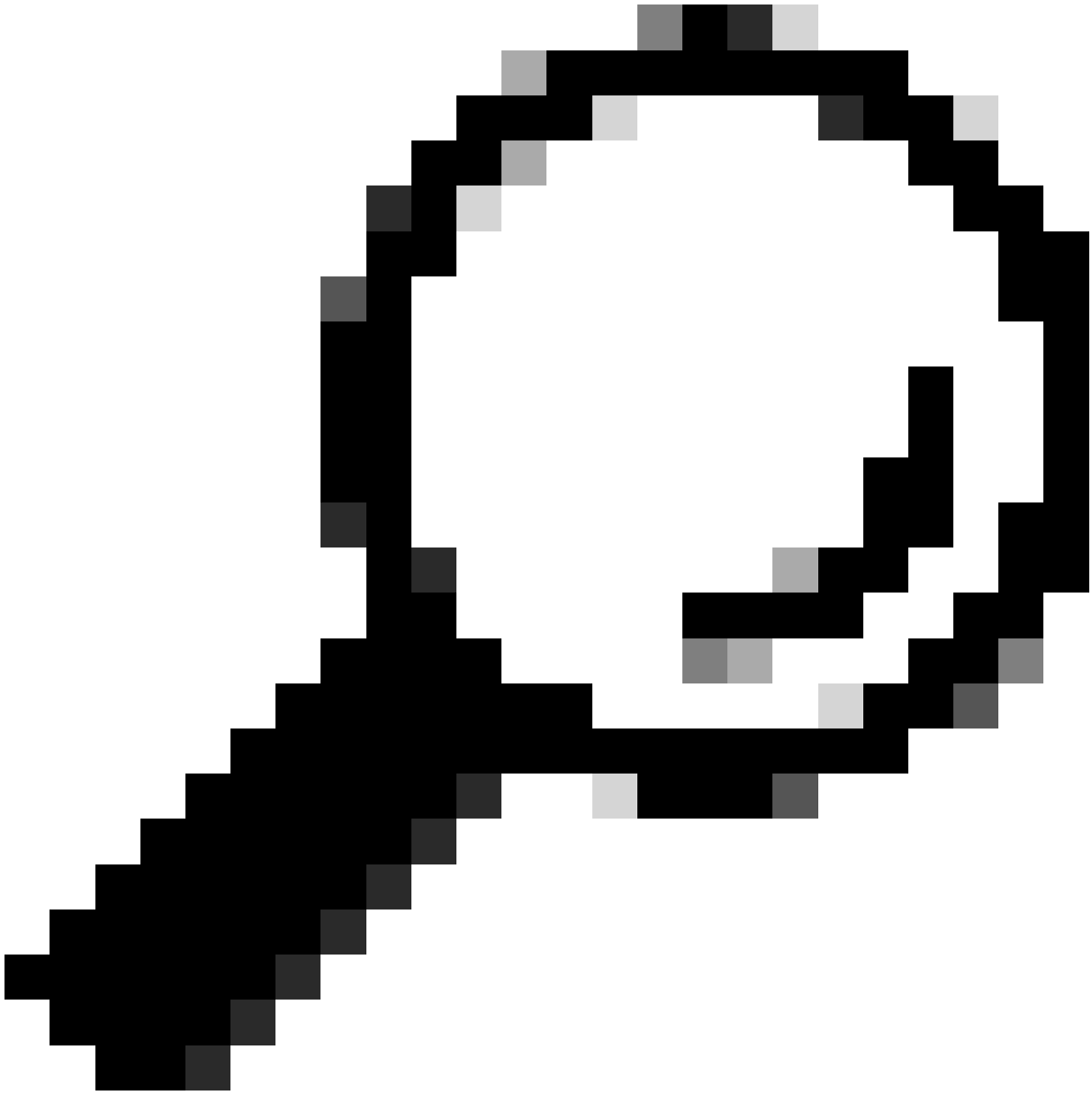

4.为身份提供程序元数据URL或上传身份提供程序元数据XML文件选择相应的单选按钮。





注意：在此演示中，已选择上传身份提供程序元数据XML文件。

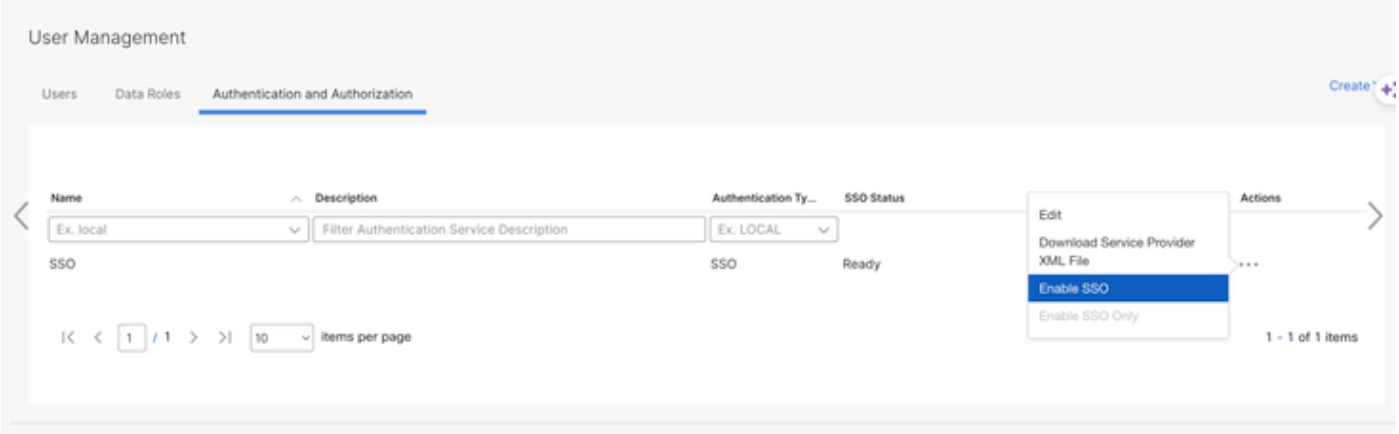
5.将“身份提供程序类型”字段配置为Microsoft Entra ID，将名称标识符格式配置为Persistent，键入登录屏幕标签。



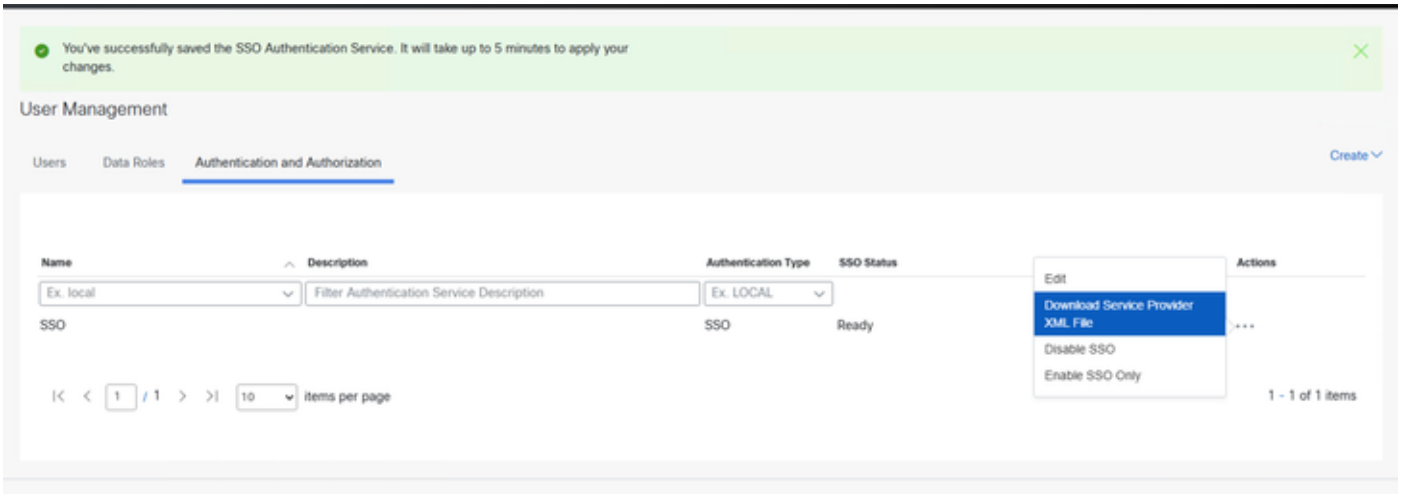
提示：配置的登录屏幕标签（名称/文本）显示在“使用SSO登录”按钮上方，不应留空。

6.单击Save，返回到Authentication and Authorization选项卡。

7.等待状态变为READY，然后从操作菜单中选择Enable SSO。




8.在Authentication and Authorization选项卡下，单击Actions列中的三个点，然后单击Download Service Provider XML File。



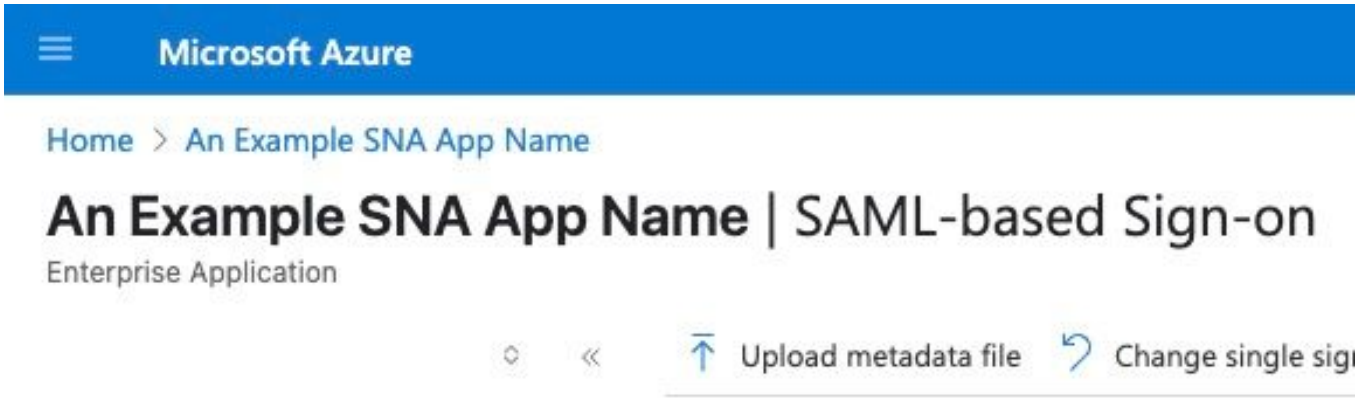

## 在Azure中配置SSO

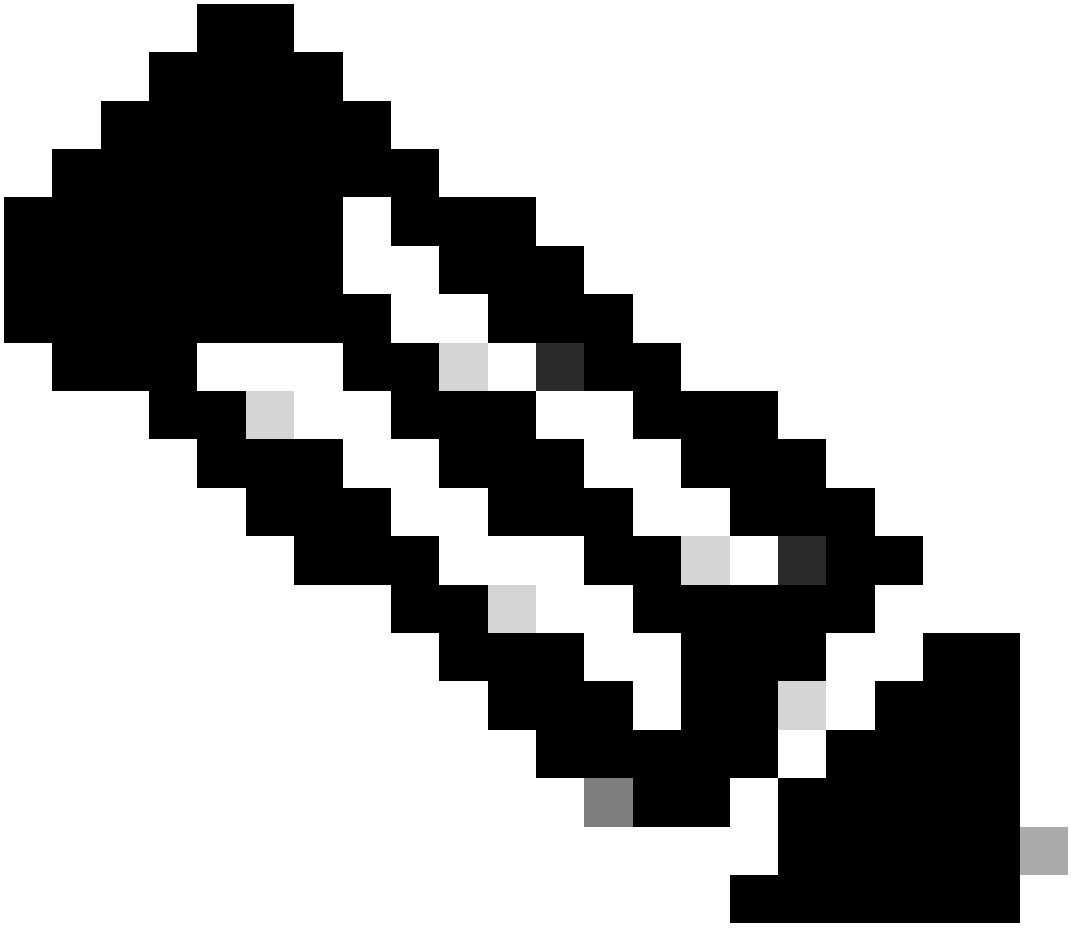
1.登录Azure门户。

2.从搜索栏导航至企业应用程序>选择已配置企业应用程序>单击设置单点登录。

3.单击页面顶部的上传元数据文件，并上传从SNA Manager下载的sp.xml文件。

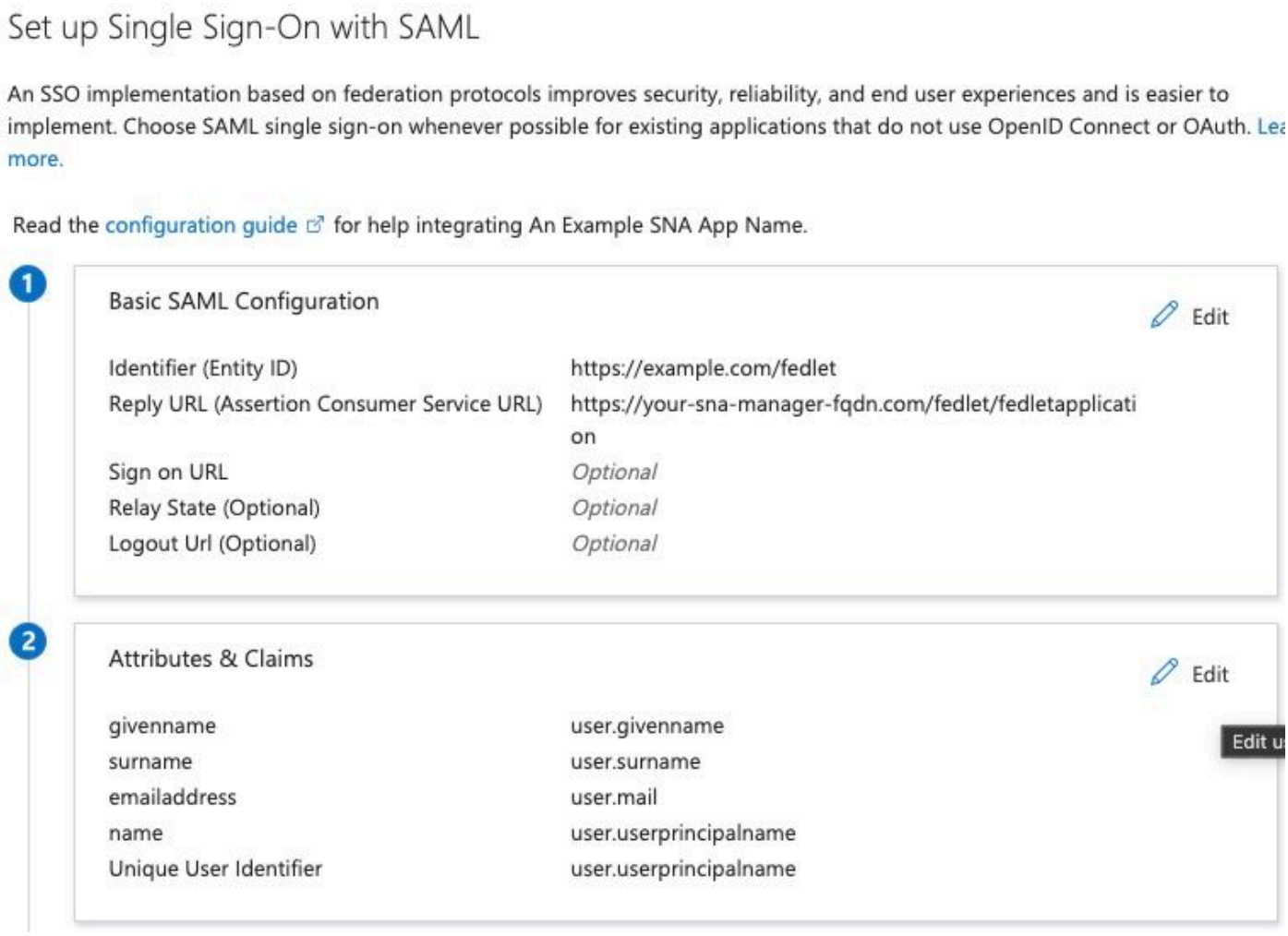
4.打开“基本SAML配置”屏幕并将各种设置设置为正确的值，单击“保存”。





注意：确保Entra ID中的Name ID Format正确。

5.找到Attributes & Claims部分，然后点击Edit。




6.单击Claim Name部分下的user.userprincipalname值。


7.在Manage Claim页面Verify下选择name identifier format。

Microsoft Azure

Search

Home > An Example SNA App Name | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >

# Manage claim ...

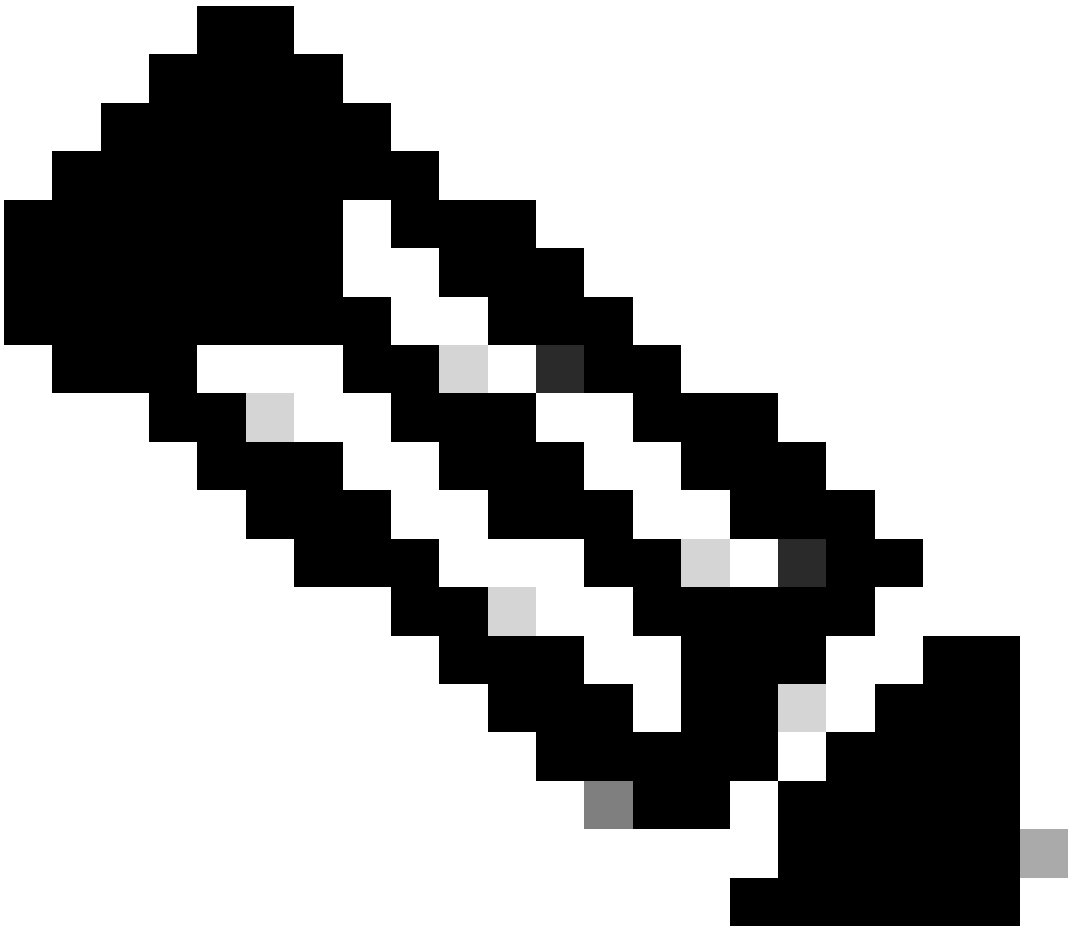
Save | Discard changes | Got feedback?

Name: nameidentifier

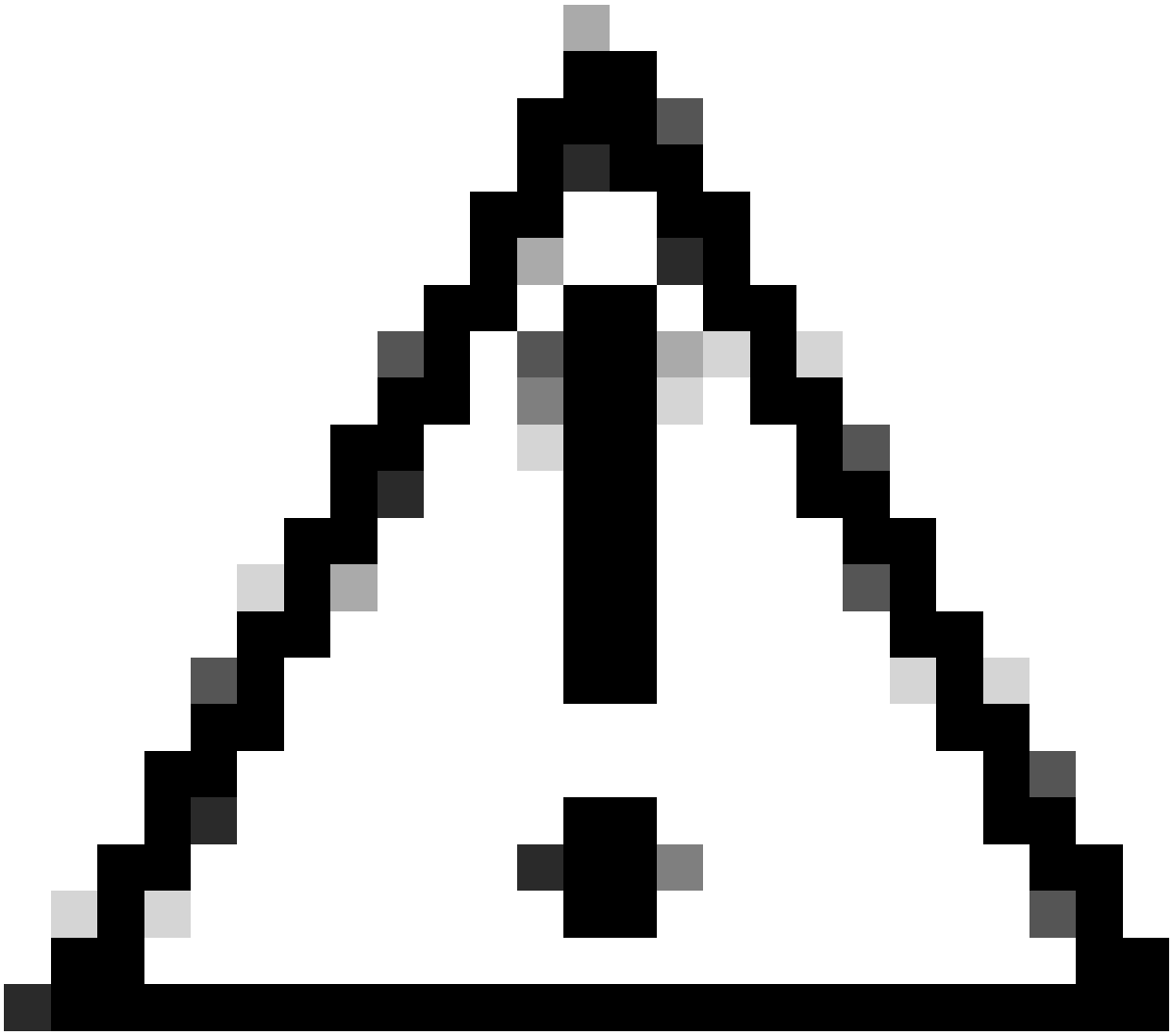
Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Persistent



注意：名称标识符格式字段设置为“持续”(Persistent)（如果不是），则从下拉菜单中选择该字段。如果进行了更改，请单击“保存”。

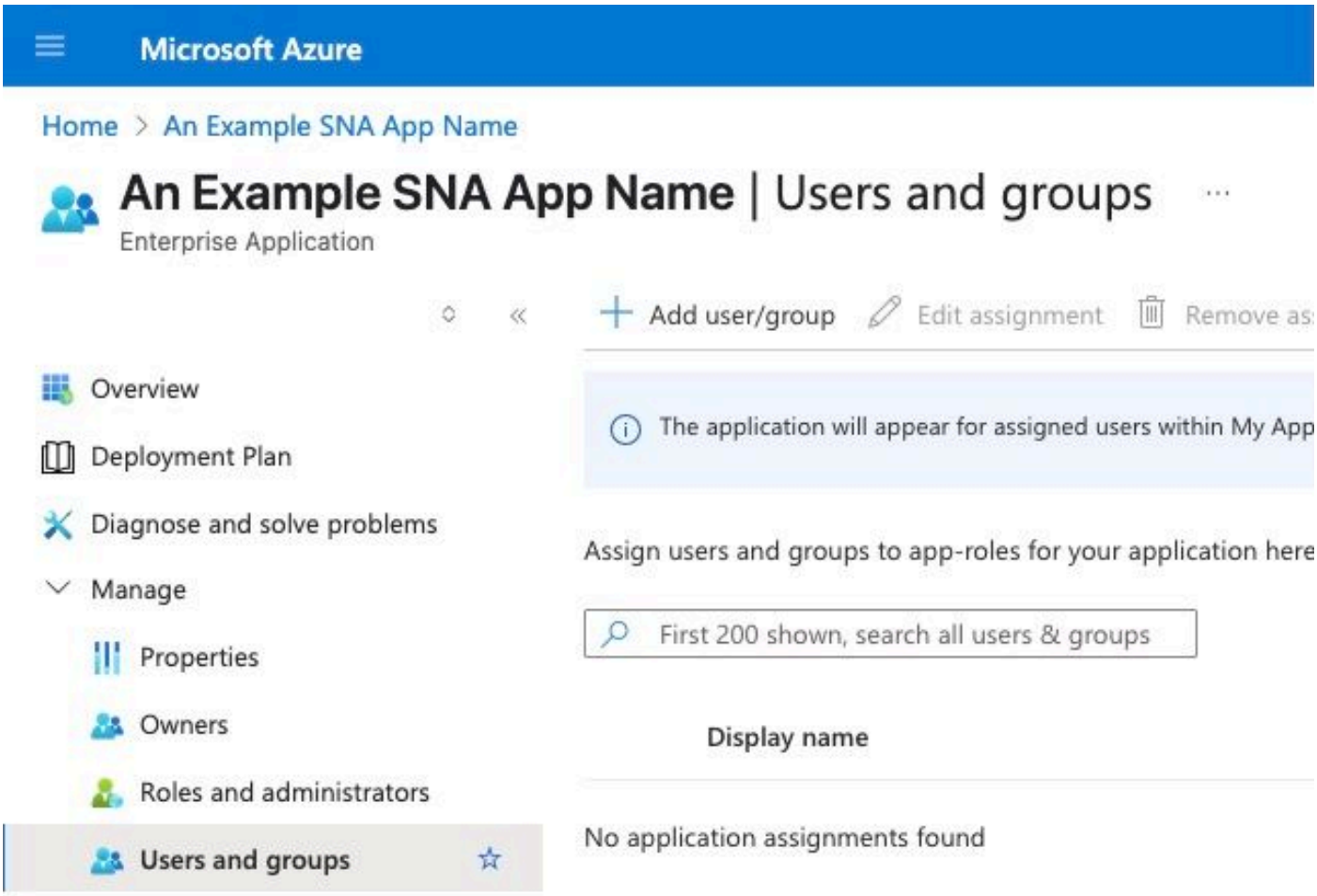


警告：这是最常见的问题所在。SNA Manager和Microsoft Azure上的设置必须匹配。如果您选择在SNA中使用“emailAddress”格式，则此处的格式也必须是“Email Address”。

## 在Entra ID中设置用户。

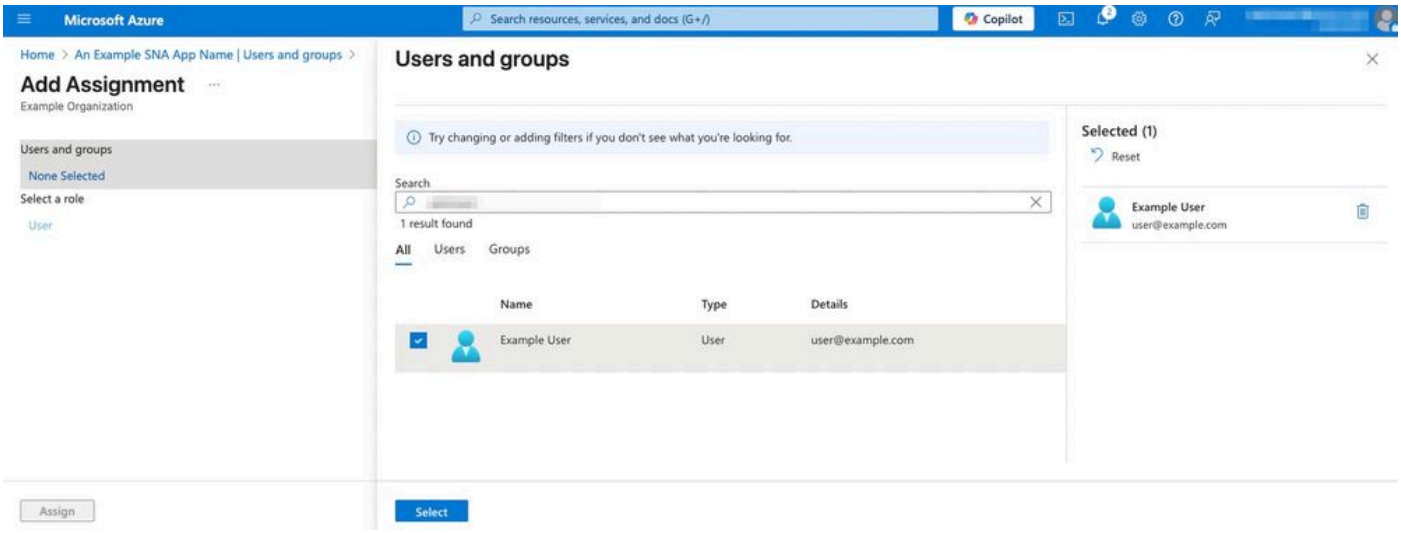
1.登录Azure门户。

2.从搜索栏导航到“企业应用”>“选择已配置的企业应用”>选择左侧的“用户和组”>单击“添加用户/组”。




3.在左侧窗格中，单击None Selected。

4.搜索所需的用户并将其添加到应用程序。

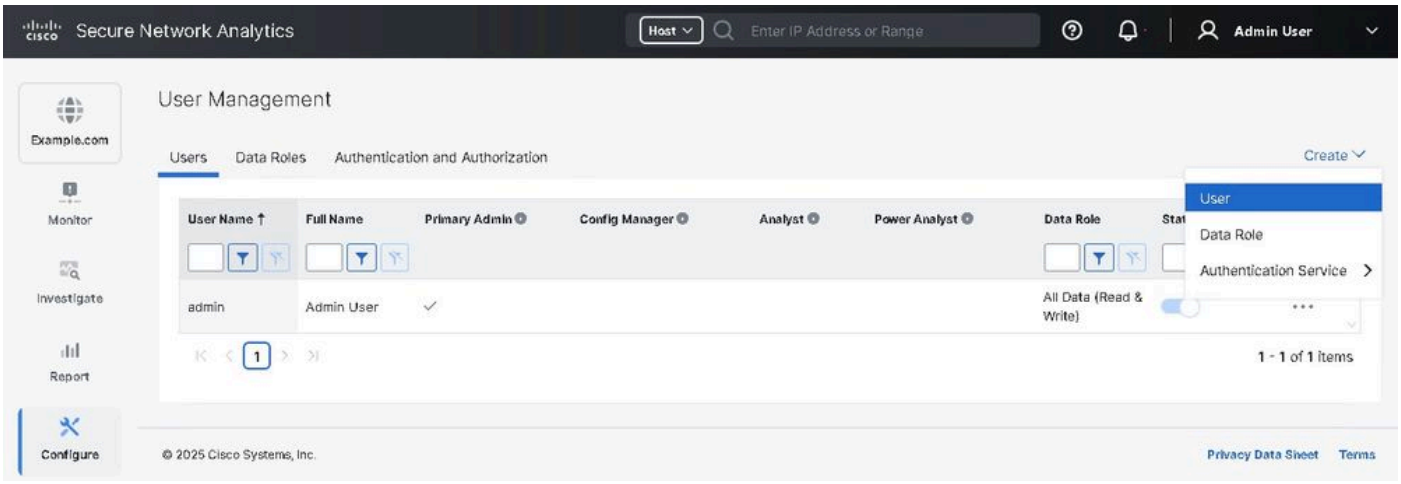



## 在SNA中配置SSO

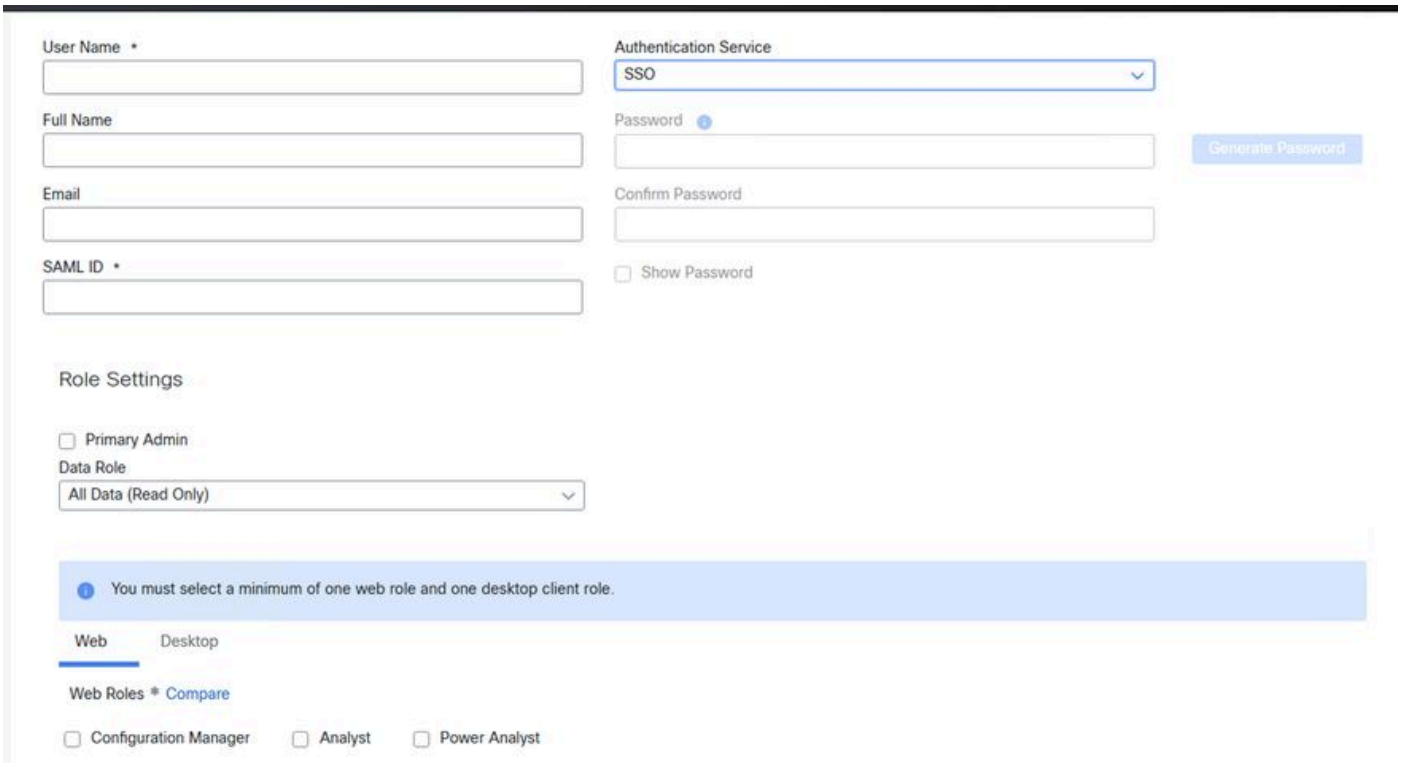
1.登录到SNA Manager UI。

2.定位至配置>全局>用户管理。

3.单击创建>用户。




4.通过提供与选为SSO的身份验证服务相关的详细信息来配置用户，然后单击Save。




在SNA-UI中创建SAML用户

# 故障排除

如果用户无法登录到SNA Manager，则可以使用SAML跟踪器进行进一步调查。

如果需要进一步协助调查SNA Manager，可以提出TAC案例。

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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）。