使用Microsoft Entra ID为SD-WAN配置SSO

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 使用单点登录的优势

配置

- 步骤1.获取Cisco SD-WAN Manager SAML元数据
- 步骤2.在Microsoft Entra ID中配置用于SSO的企业应用
- 步骤3.将用户或组帐户添加到企业应用程序
- 步骤4.为Microsoft Entra ID配置SAML组调配
- 步骤5.将Microsoft Entra ID SAML元数据文件导入到Cisco SD-WAN Manager

验证

相关信息

简介

本文档介绍如何使用Microsoft Entra ID为Cisco Catalyst软件定义的广域网(SD-WAN)配置单点登录(SSO)。

先决条件

要求

思科建议您了解以下主题的一般知识：

- 单一登录
- Cisco Catalyst SD-WAN解决方案

使用的组件

本文档中的信息基于：

- Cisco Catalyst SD-WAN Manager版本20.15.3.1
- Microsoft Entra ID

注意：以前称为Azure Active Directory(Azure AD)的解决方案现在称为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。

背景信息

单点登录是一种身份验证方法，允许用户使用一组凭证安全地访问多个独立应用或网站。使用SSO，用户不再需要单独登录到每个应用程序 — 经过身份验证后，即可无缝访问所有允许的资源。

一种实施SSO的常用方法是通过联合，即使用SAML 2.0、WS-Federation或OpenID Connect等协议在身份提供方(IdP)与服务提供商(SP)之间建立信任。联合通过集中身份验证提高安全性、可靠性和用户体验。

Microsoft Entra ID是一种广泛使用的基于云的身份提供程序，支持这些联合协议。在使用Cisco Catalyst SD-WAN的SSO设置中，Microsoft Entra ID充当IdP，Cisco SD-WAN Manager充当Service Provider。

集成工作如下：

1. 网络管理员尝试登录到Cisco SD-WAN Manager。
2. Cisco SD-WAN Manager向Microsoft Entra ID发送身份验证请求。
3. Microsoft Entra ID提示管理员使用其Entra ID(Microsoft)帐户进行身份验证。
4. 验证凭证后，Microsoft Entra ID会将安全响应发送回Cisco SD-WAN Manager，以确认身份验证。
5. Cisco SD-WAN Manager无需单独的凭证即可授予访问权限。

在此模型中：

- 身份提供程序(IdP) — 存储用户数据，验证凭证（例如，Microsoft Entra ID、Okta、PingID、ADFS）。
- 服务提供商 — 托管要访问的应用（例如，Cisco SD-WAN Manager）。
- Users — 在IdP目录中拥有帐户，并有权访问服务提供商。

Cisco Catalyst SD-WAN与任何符合SAML 2.0的IdP（根据行业标准配置）兼容。

使用单点登录的优势

- 通过身份提供程序集中凭据管理。
- 通过消除多个弱密码增强身份验证安全性。
- 简化管理员的安全访问。
- 支持对Cisco Catalyst SD-WAN Manager和其他授权应用的一键访问。

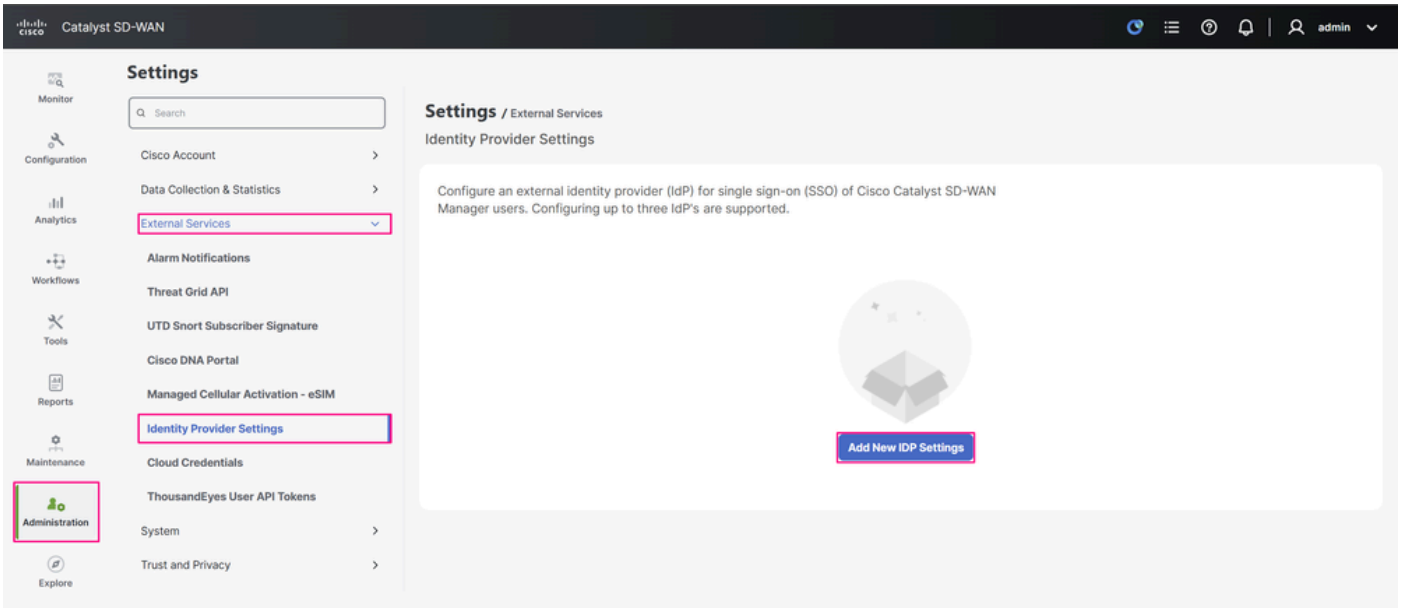
配置



注意：支持的最低版本：Cisco Catalyst SD-WAN Manager版本20.8.1。

步骤1.获取Cisco SD-WAN Manager SAML元数据

- 在Cisco SD-WAN Manager中，导航到管理>设置>外部服务>身份提供程序设置，然后单击添加新的IDP设置。



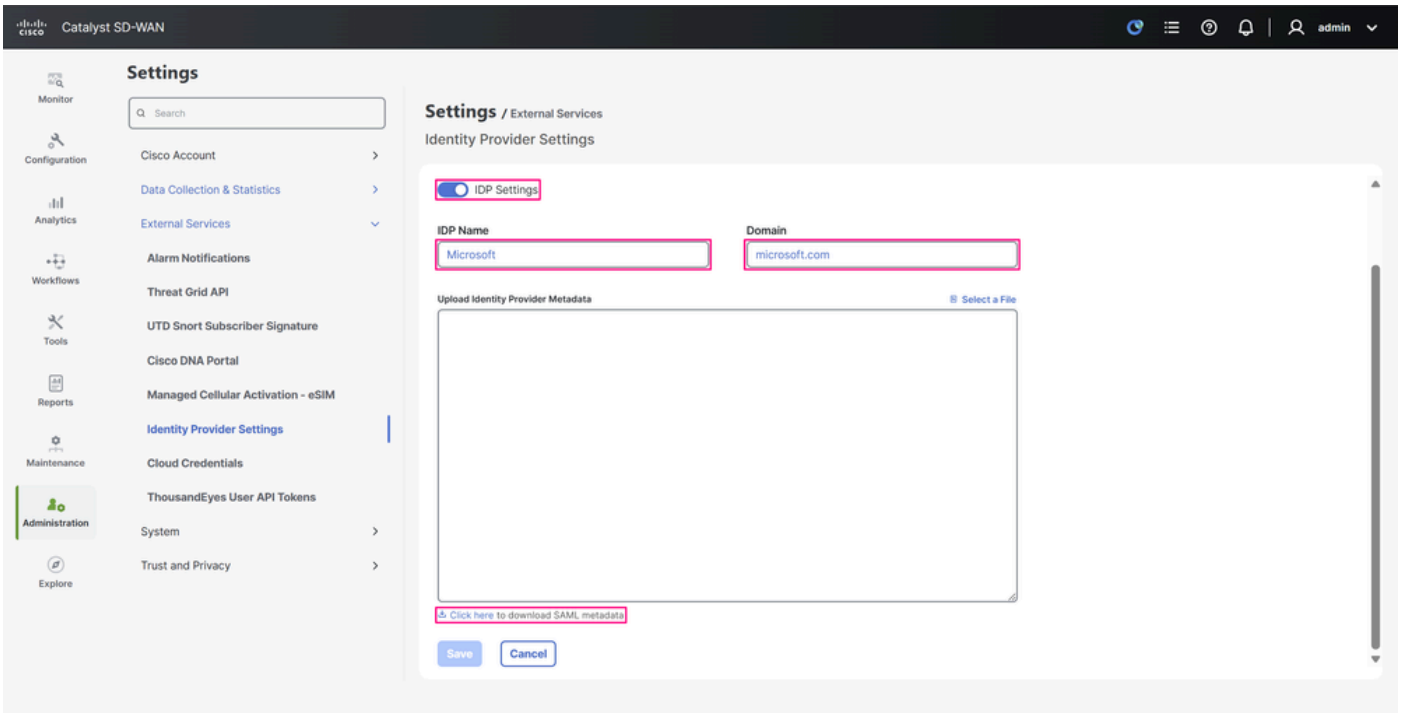
思科SD-WAN管理器UI

- 切换IDP设置以启用身份提供程序设置。在IDP Name字段中，输入引用您正在使用的IdP的name，然后在Domain字段中，输入与组织企业应用程序中的用户使用的域名匹配的domain。单击单击此处下载SAML元数据，并将元数据XML文件保存到您的计算机。在下一步中，此文件用于在Microsoft Entra ID中配置SSO。

注意：在本示例中，元数据XML文件直接指向Cisco SD-WAN Manager的IP地址，但在许多生产环境中，它指向其完全限定域名(FQDN)。 对于独立的思科SD-WAN管理器，元数据中包含的实体ID与下载时用于登录思科SD-WAN管理器的URL匹配。这意味着它可以与IP地址或FQDN配合使用，因为它是单节点设置。

对于Cisco SD-WAN Manager集群，同样的原理是FQDN指向其中一个集群节点，并且元数据包括此域作为实体ID。不同之处在于，无论是将元数据与集群的FQDN配合使用，还是从使用其IP地址的特定节点使用元数据，一旦成功完成与Microsoft Entra ID的SSO集成，其他节点也会重定向到IdP登录提示。

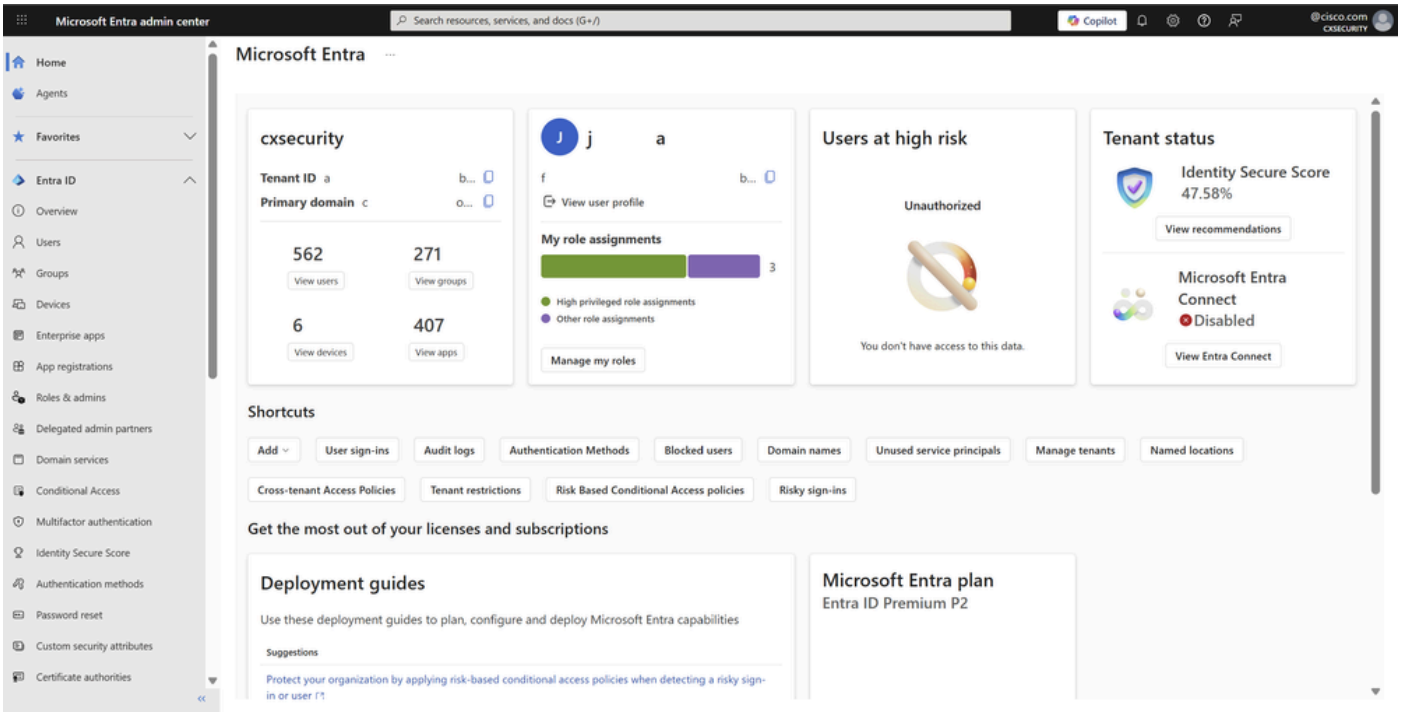
两种方案的主要要求是，您在Cisco SD-WAN Manager中使用的实体ID（无论是IP地址还是FQDN）与IdP端上配置的标识符匹配。



"IdP设置配置"页

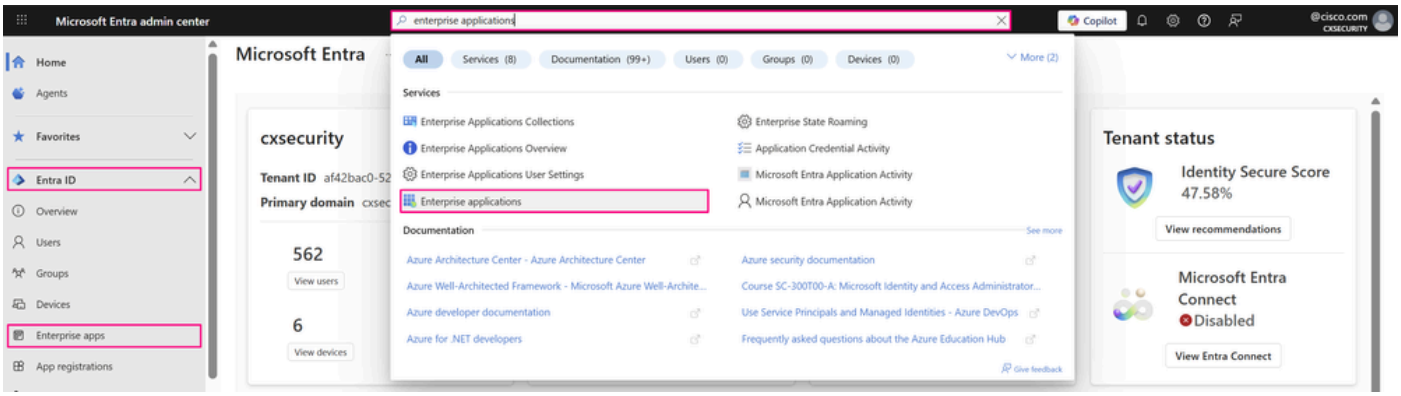
步骤2.在Microsoft Entra ID中配置用于SSO的企业应用

- 使用以下角色之一登录Microsoft Entra管理中心门户：云应用管理员、应用管理员或服务主体的所有者。



Microsoft Entra管理中心门户

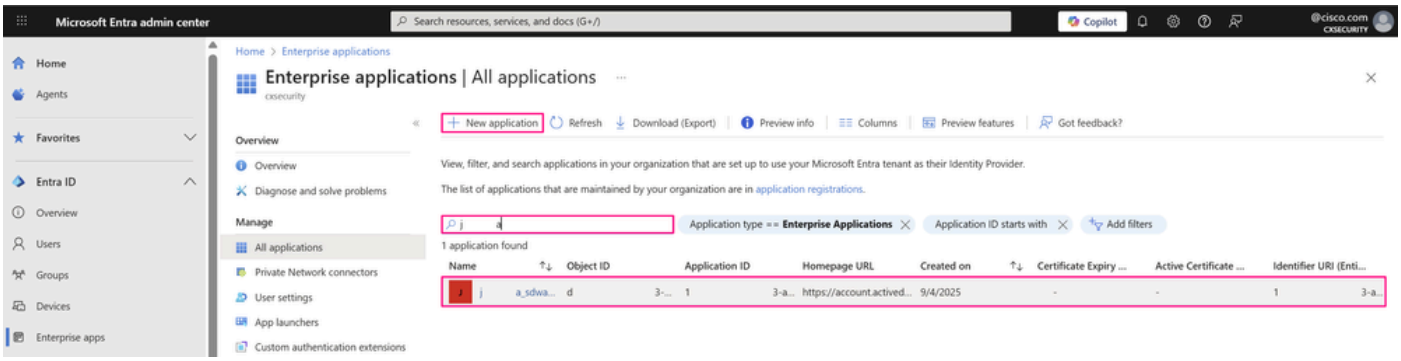
- 导航到Entra ID > Enterprise apps，或者当您在门户顶部的搜索栏中输入enterprise applications，然后选择Enterprise Applications时，也可以访问此服务。



Microsoft Entra管理中心门户

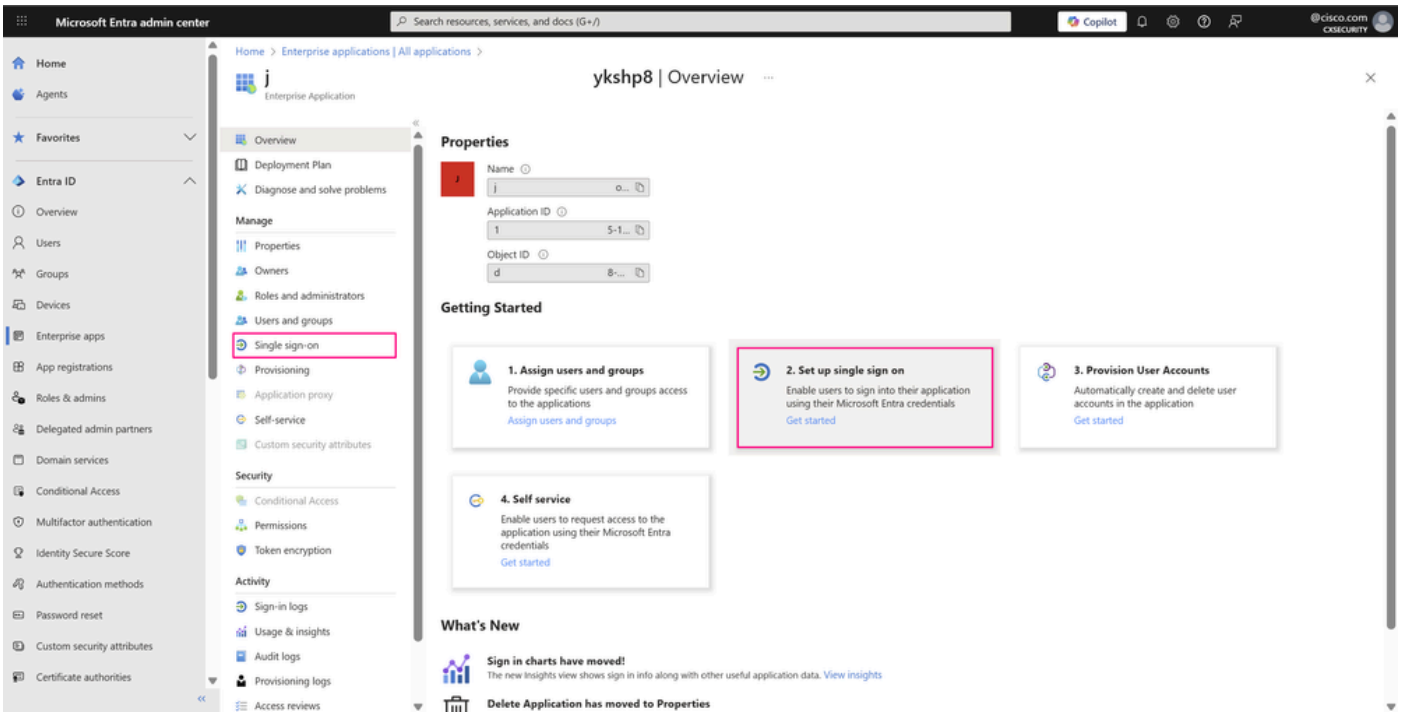
- 将打开所有应用页面。在搜索框中输入现有应用的名称，然后从搜索结果中选择应用。

注意：在此页面上，您可以根据贵组织的要求创建自定义企业应用，如果尚未使用，请在点击New application时使用SSO身份验证对其进行配置。



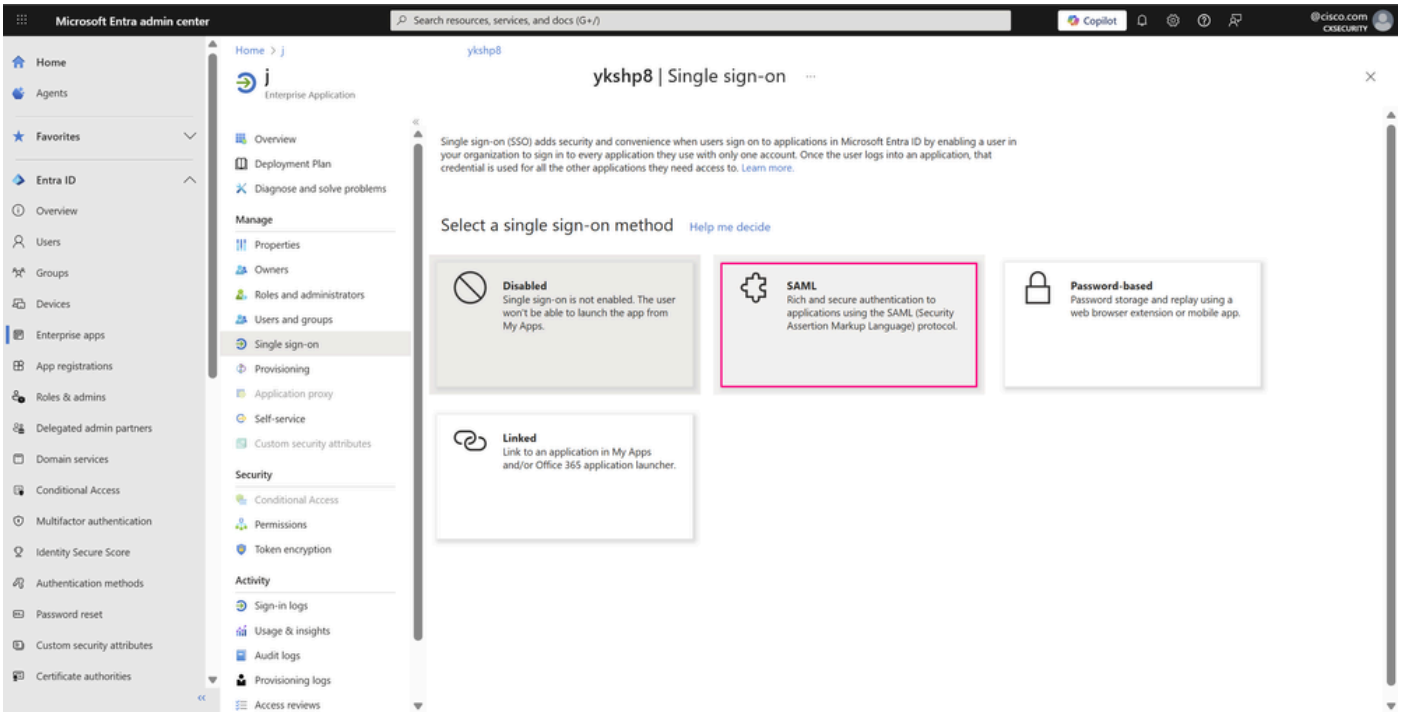
企业应用控制面板

- 在左侧菜单的“管理”(Manage)部分，单击“单点登录”(Single sign-on)，或在“概述”(Overview)部分的“入门”(Getting Started)窗格中，单击2.设置单点登录(2.Set up single sign-on)以打开单点登录(Single sign-on)窗格进行编辑。



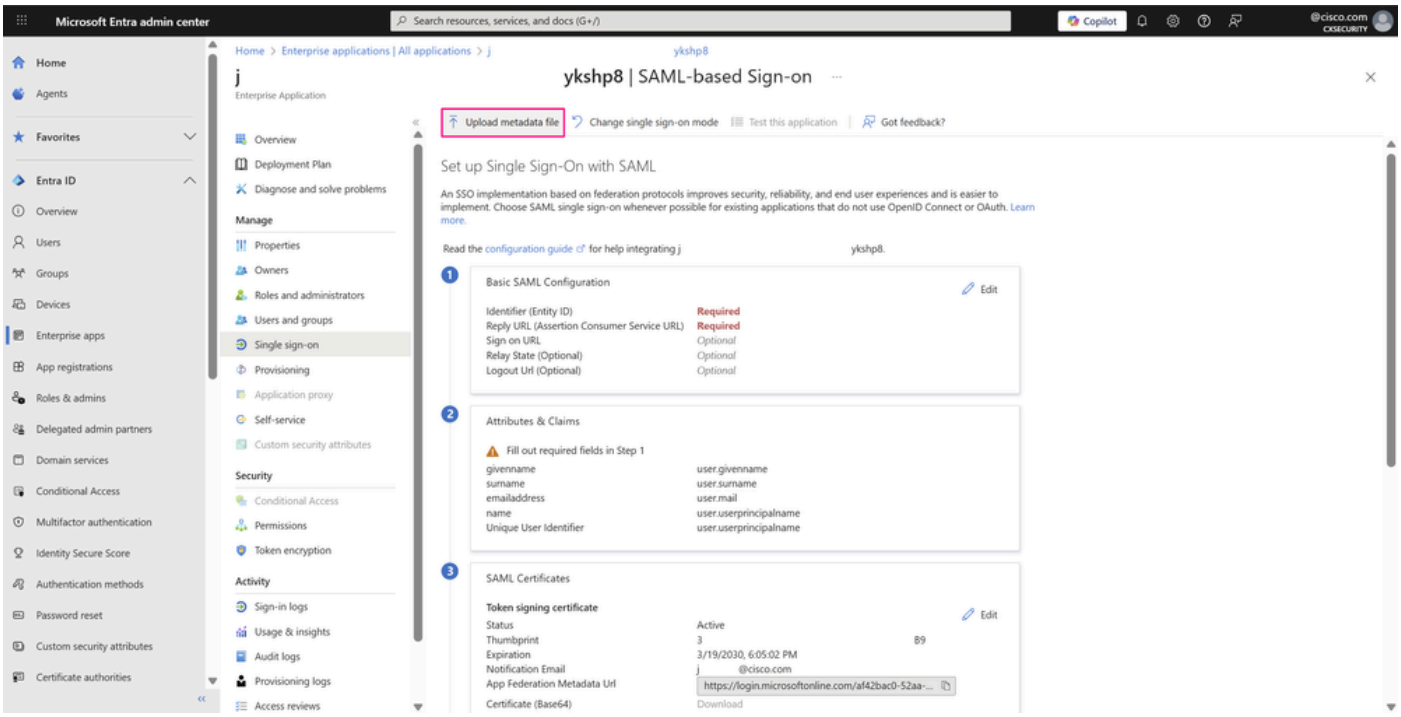
企业应用概述

- 选择SAML以打开SSO配置页。



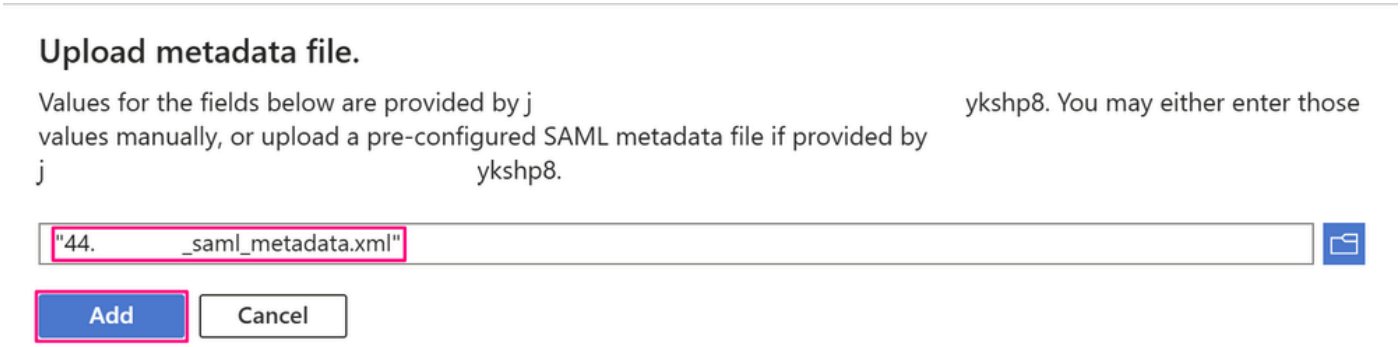
单一登录窗格

- 在“使用SAML设置单一登录”页上，单击上传元数据文件。



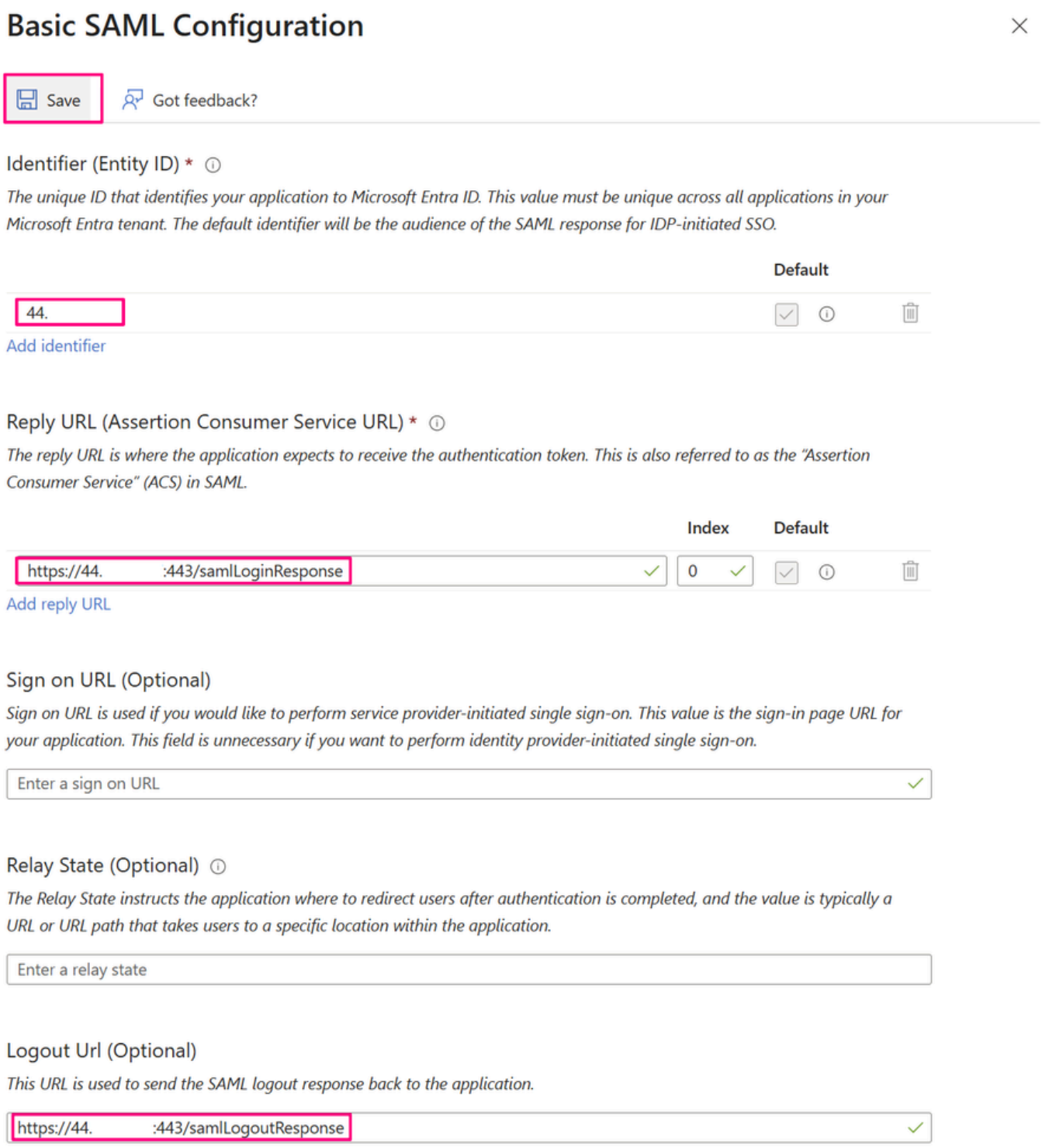
“使用SAML的SSO配置”页

- 在Upload metadata file窗口中，浏览并点击之前下载的元数据XML文件，然后单击Add。



上载元数据文件窗口

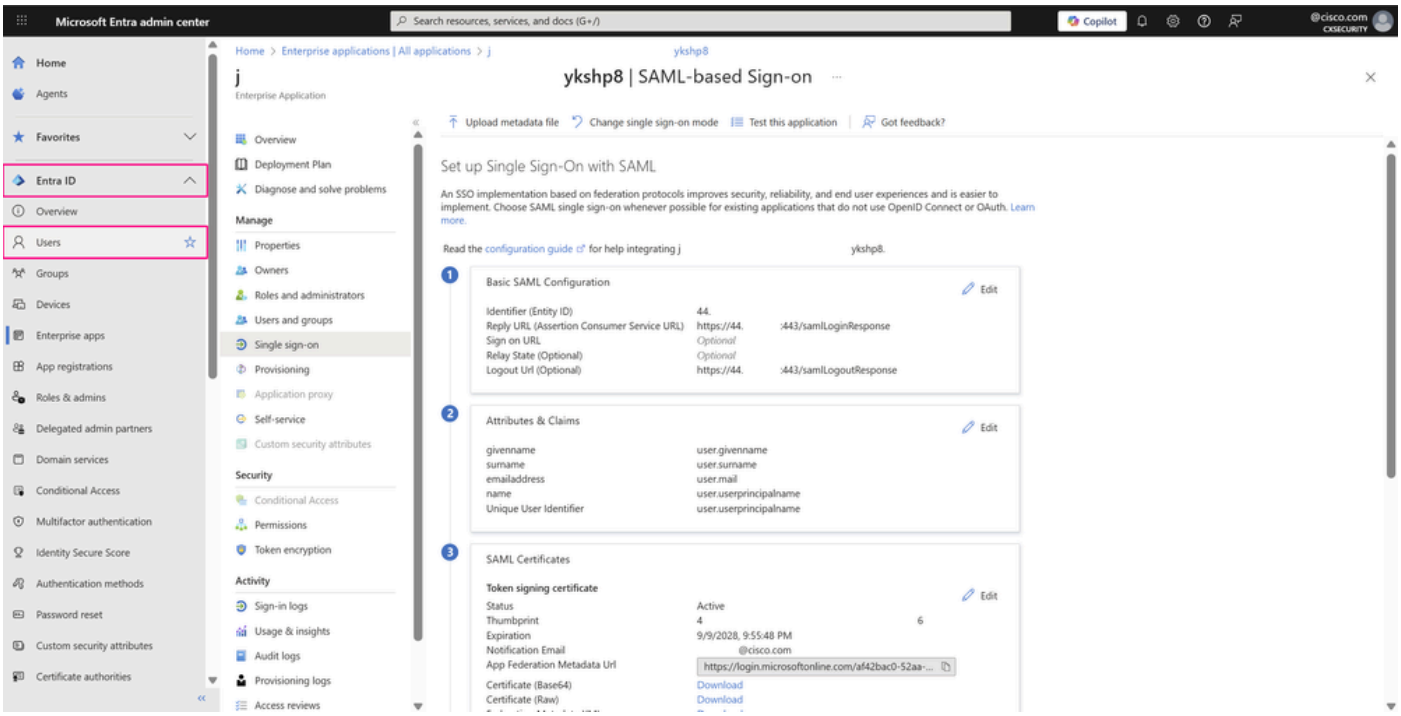
- 在Basic SAML Configuration窗口中，Identifier(Entity ID)通常是应用程序特定的URL（在本例中为Cisco SD-WAN Manager），您正与集成（如上一步所述）。 成功上传文件后，系统将自动填充回复URL和注销URL值。要继续，请单击Save。



基本SAML配置窗口

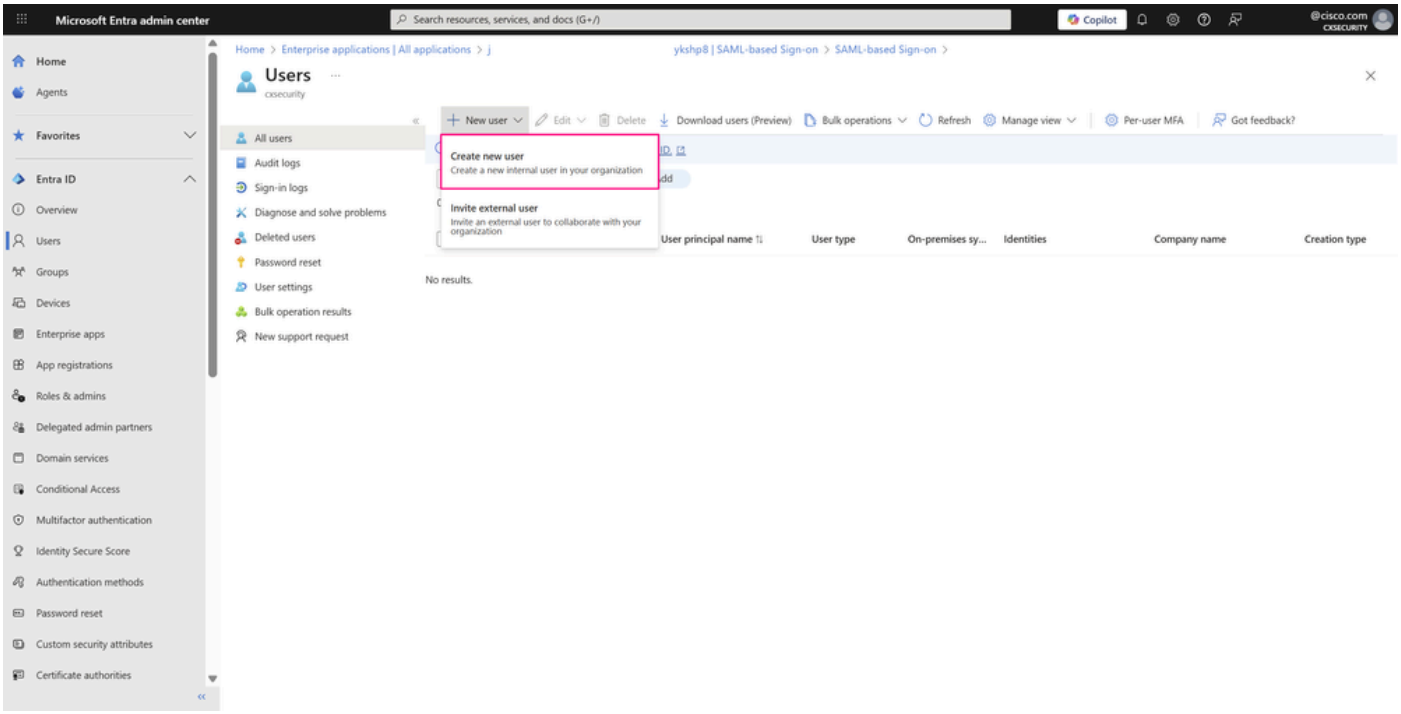
步骤3.将用户或组帐户添加到企业应用程序

- 定义应用的SAML配置参数后，您将继续在企业应用中添加登录到应用的用户或组。为此，请首先导航到Entra ID > Users，或在门户顶部的搜索栏中搜索服务名称时也可以访问此服务，如上一步所示。



“使用SAML的SSO配置”页

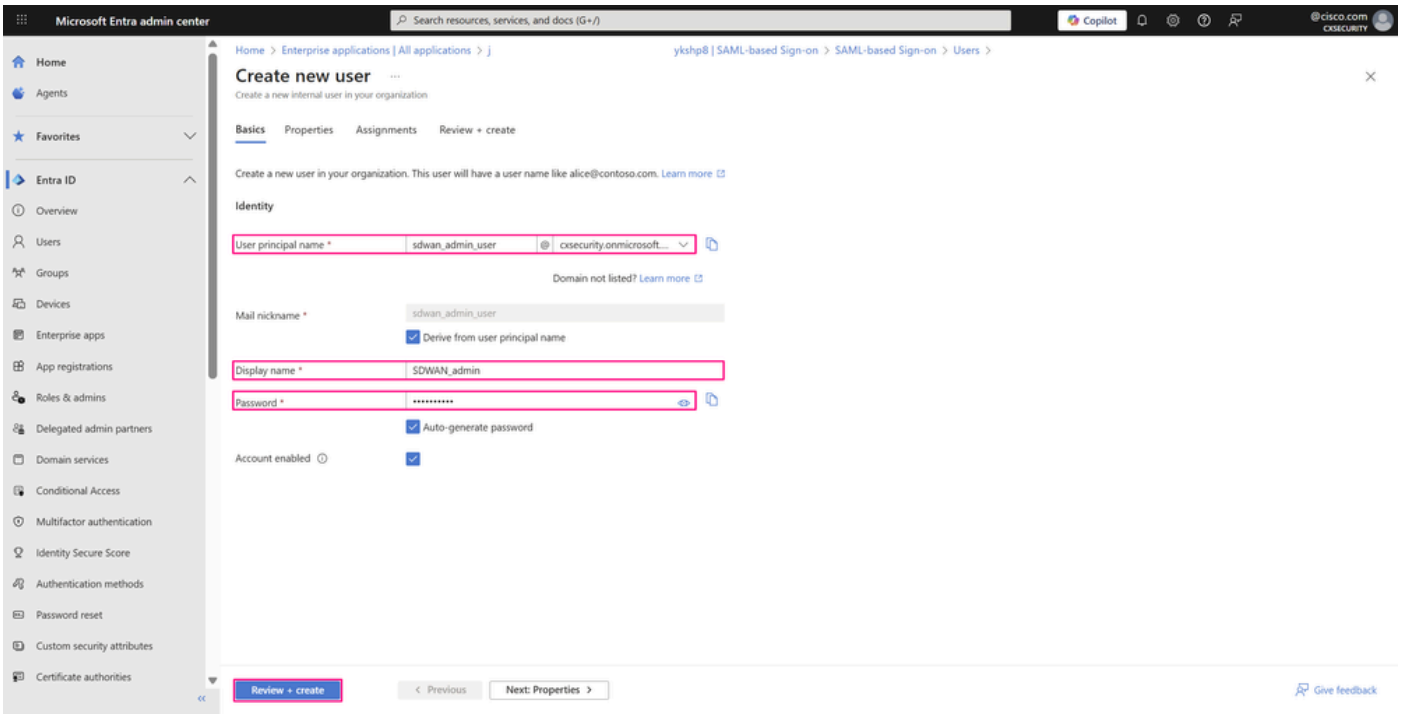
- 创建与组关联的用户，以说明使用Cisco SD-WAN Manager及其用户组之一netadmin（在生产环境中最常见）进行SSO身份验证。为此，请定位至Entra ID > Users。然后，单击New user，然后选择Create new user。



用户控制面板

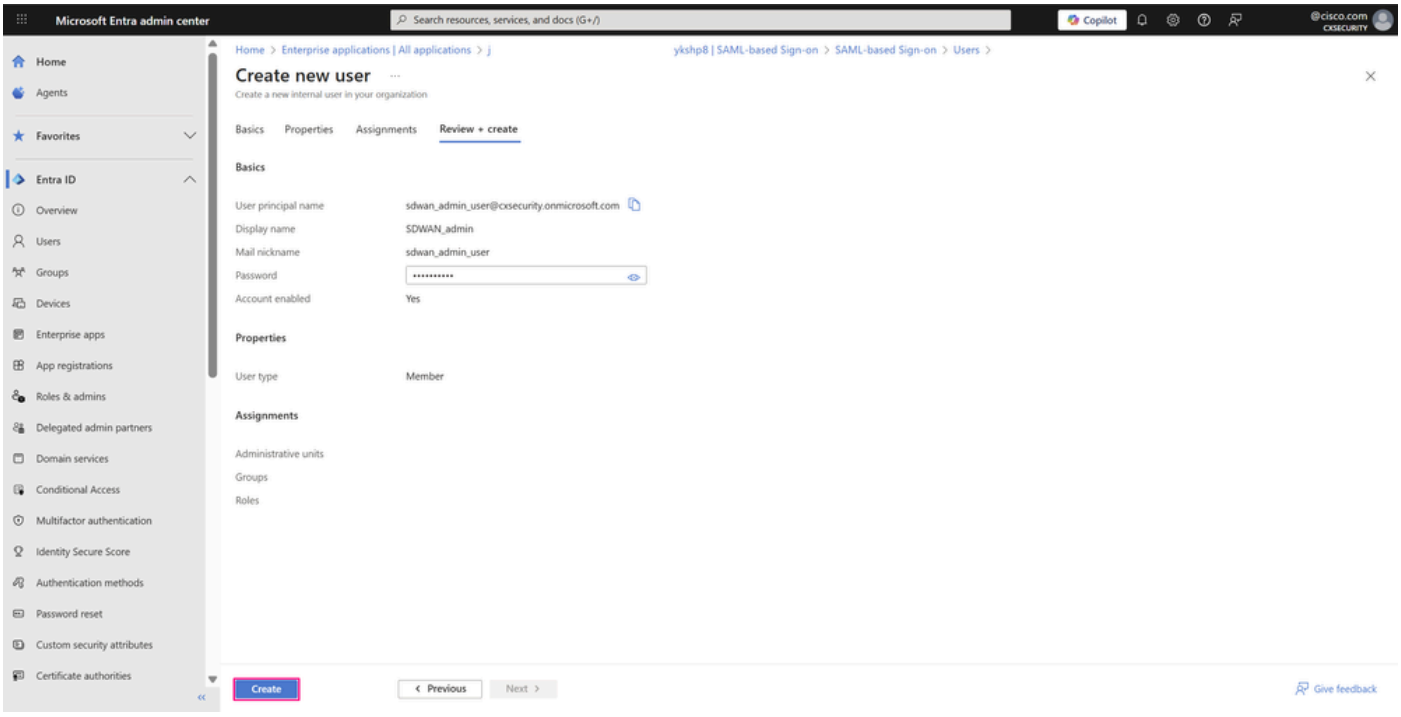
- Basics选项卡包含创建新用户所需的核心字段。
  - 对于User principal name，输入唯一的用户名，然后从组织中的可用域下拉列表中选择域。
  - 输入用户的Display name。

- 如果要输入自定义密码，请取消选中Auto-generate password，或保留选中此选项以自动生成密码。
- 您可以在Assignments选项卡中将用户添加到组，但由于尚未创建组成员资格，请单击Review + create。



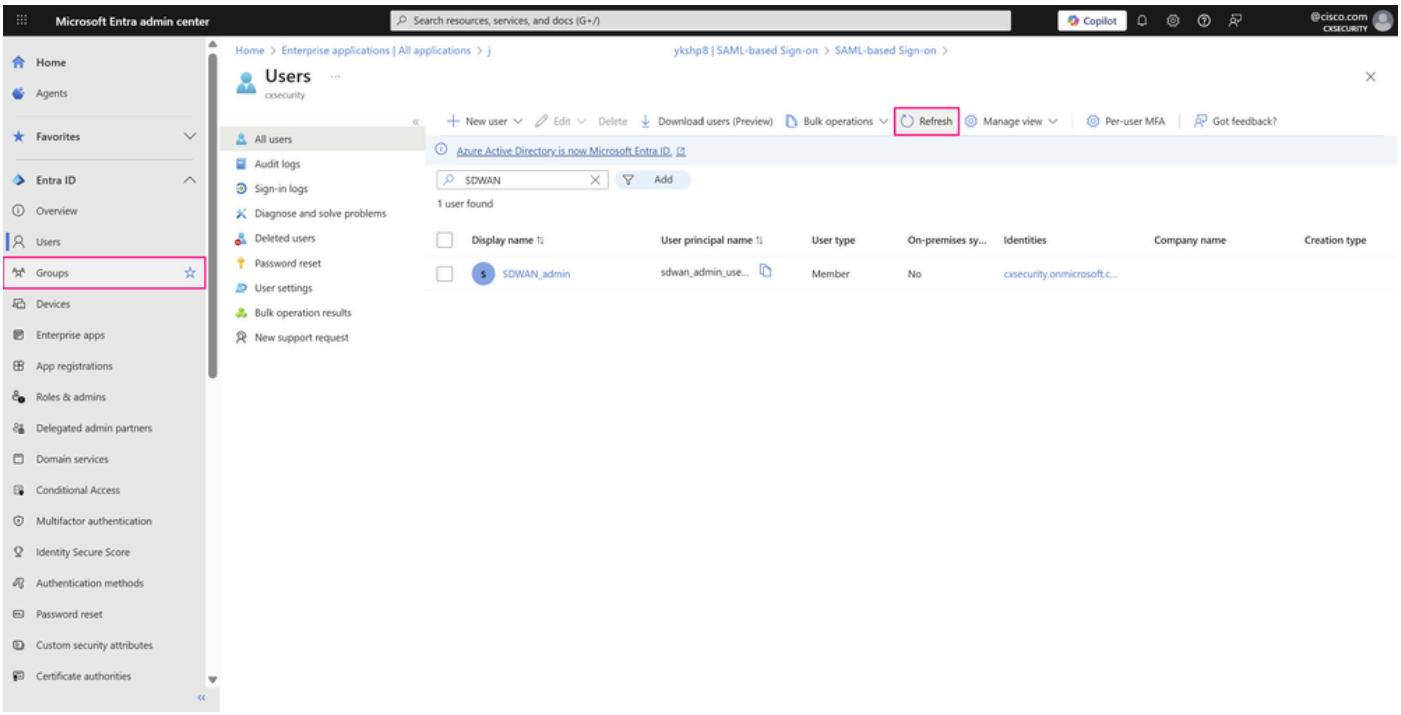
“用户创建”页

- 最后一个选项卡显示用户创建工作流程中的关键详细信息。查看详细信息，然后单击Create完成此过程。



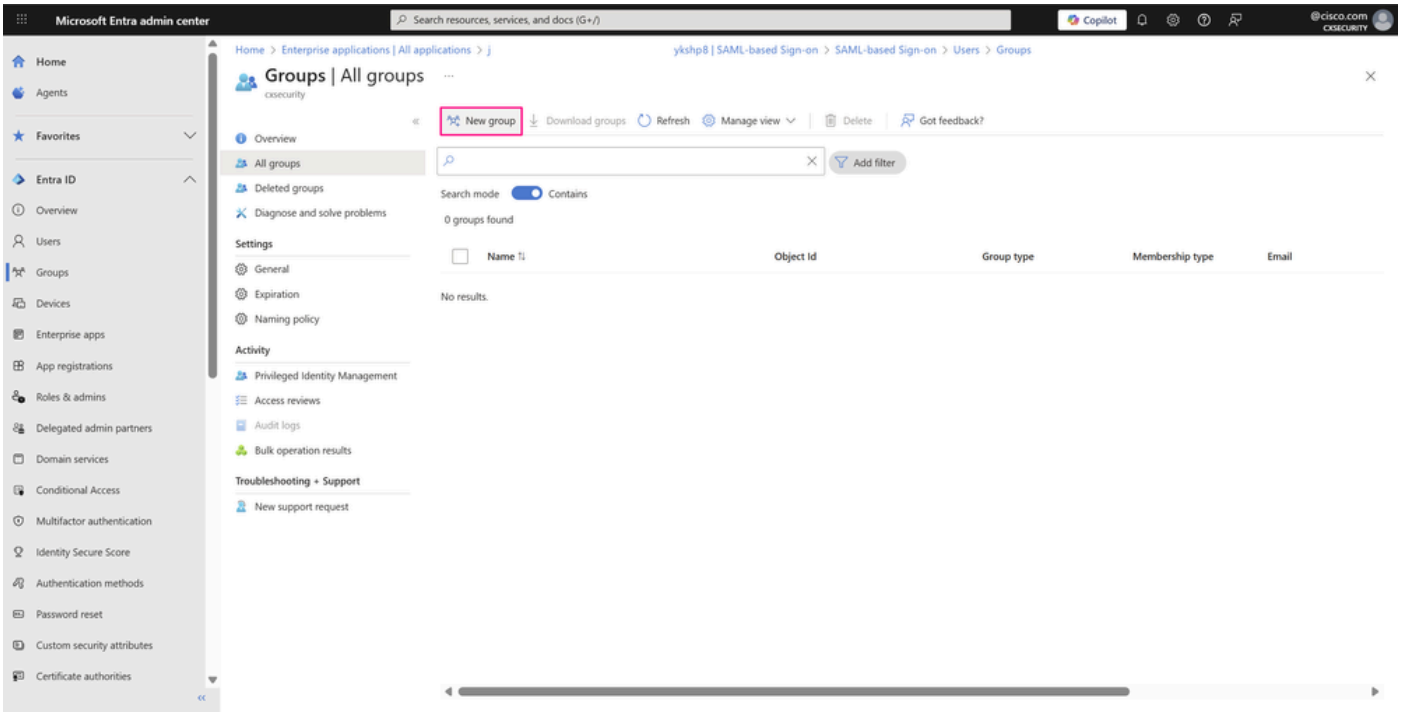
“用户创建”页

- 新用户将在稍后显示。如果没有，请单击Refresh并使用服务中的搜索栏搜索用户。接下来，导航到Entra ID > Groups > All groups以创建新组。



用户控制面板

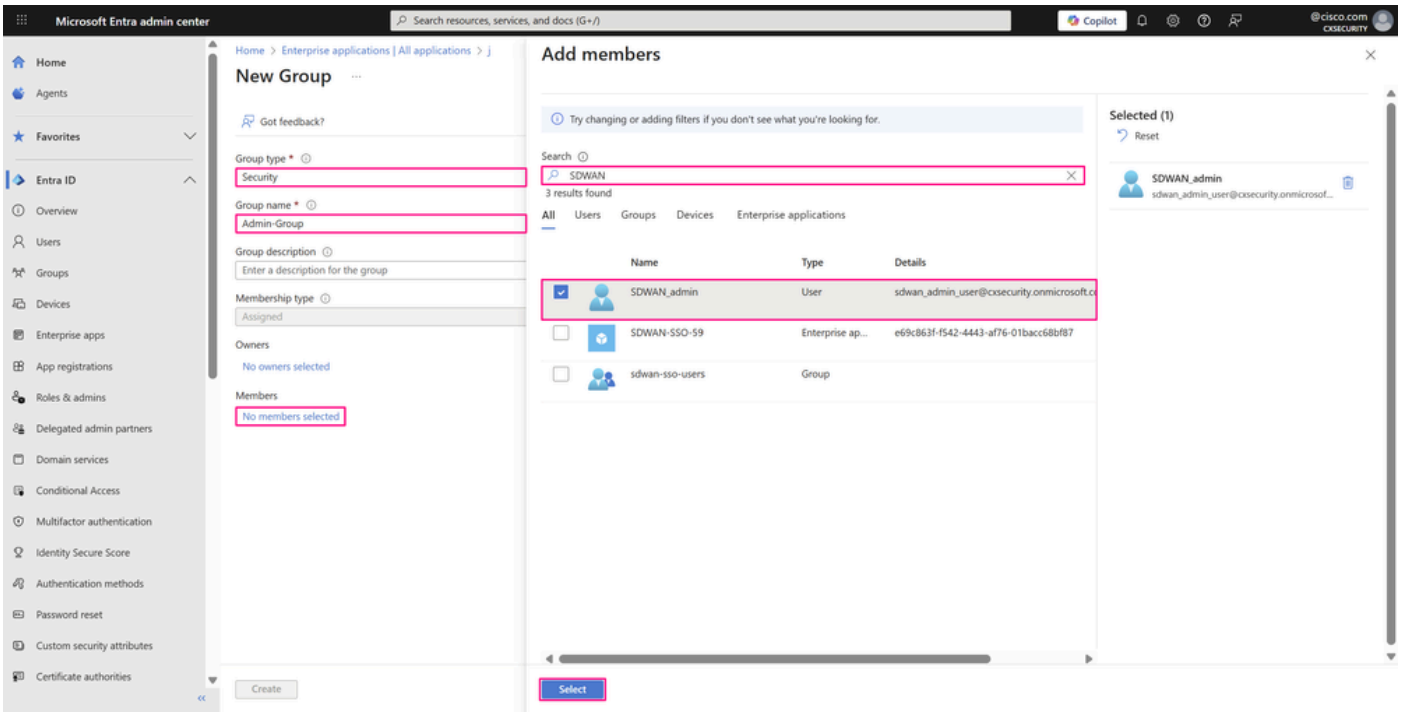
- 在此页上，可以管理组织中的不同组及其权限。单击新建组可创建具有网络管理员权限的组。



“所有组”页

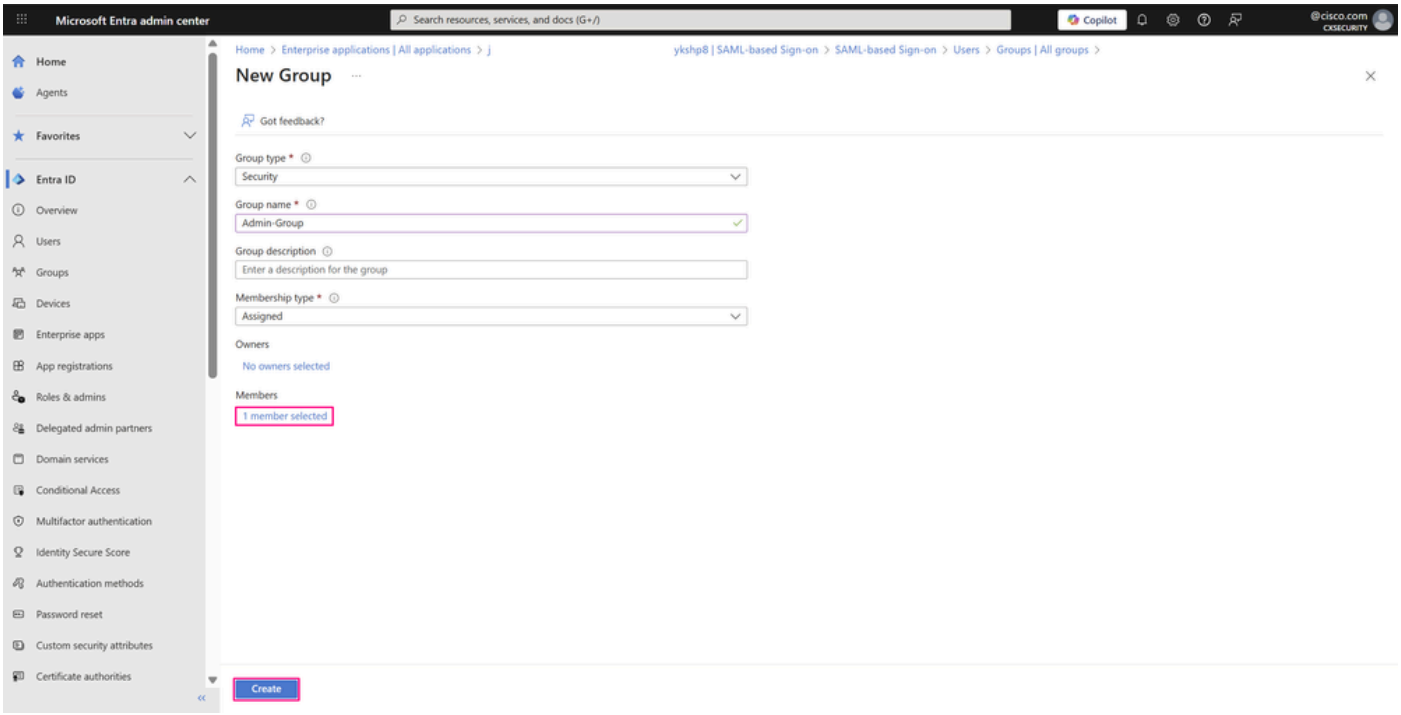
- 从下拉列表中选择Group type — 在本例中为Security，因为只需要访问共享资源。输入您选择的引用组角色或权限的组名称。此时，当您点击Members字段中的选定成员时，请将用户与该组关联。

- 在Add members窗口中，浏览并选择要添加的用户（在本例中是刚刚创建的用户），然后单击Select。



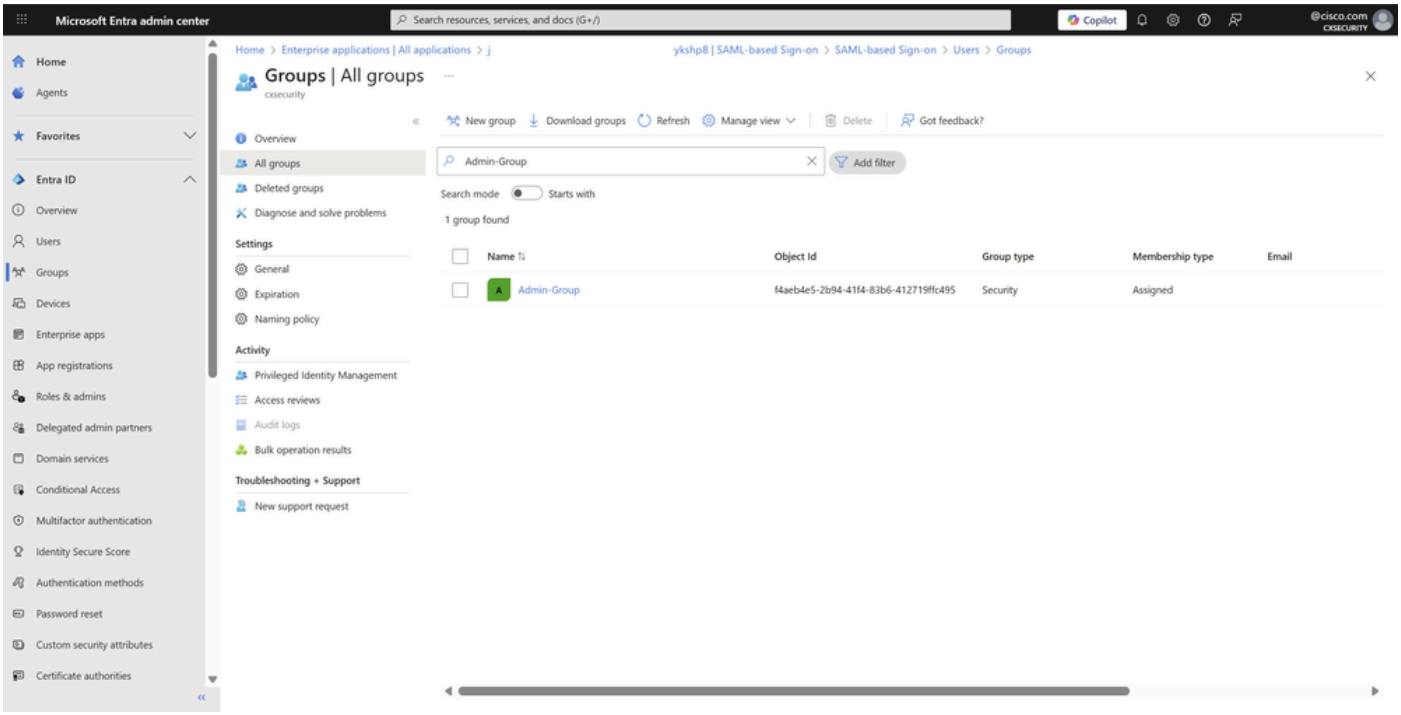
“组创建”页

- 单击Create以创建组。



“组创建”页

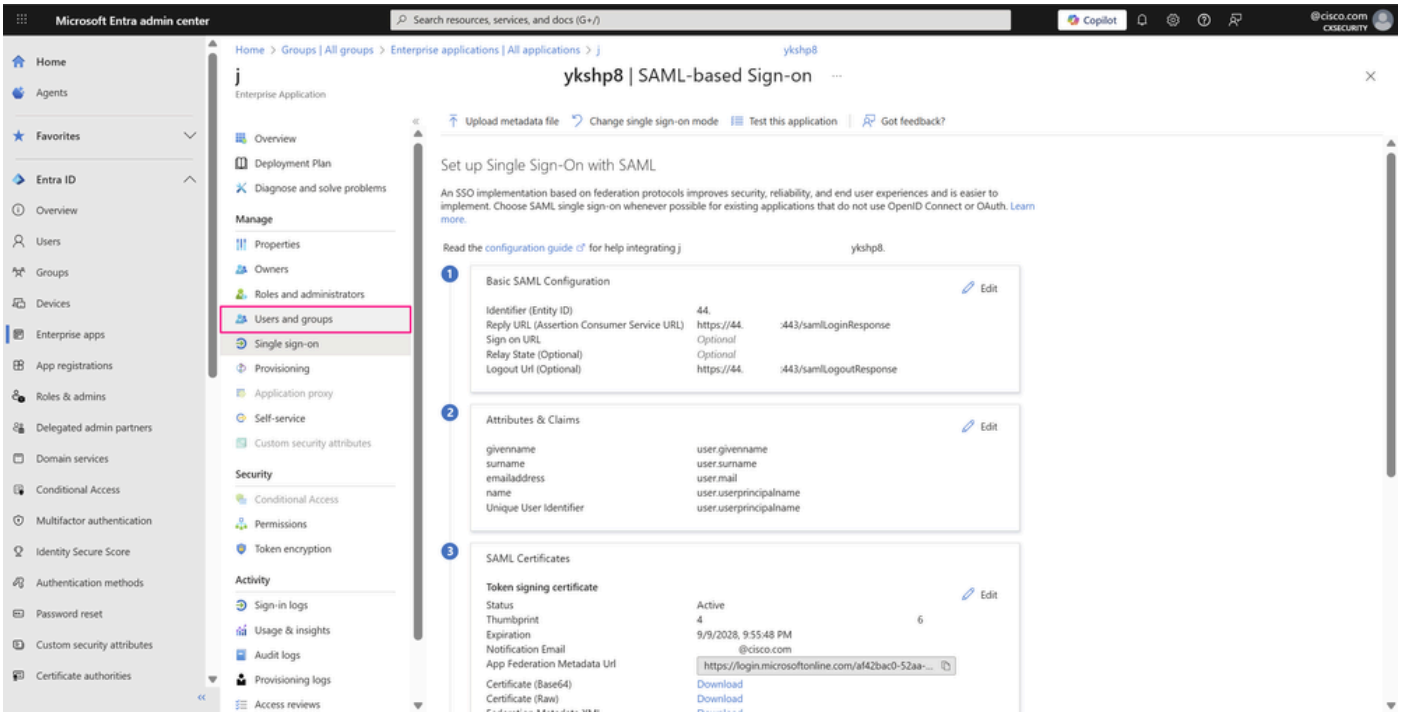
- 新组将在稍后显示。如果没有，请单击Refresh，使用服务中的搜索栏搜索组名。重复上述步骤以创建其他用户，并将其添加到其他组成员身份，以验证应用程序及其其他用户组（如操作员）的SSO登录。



“所有组”页

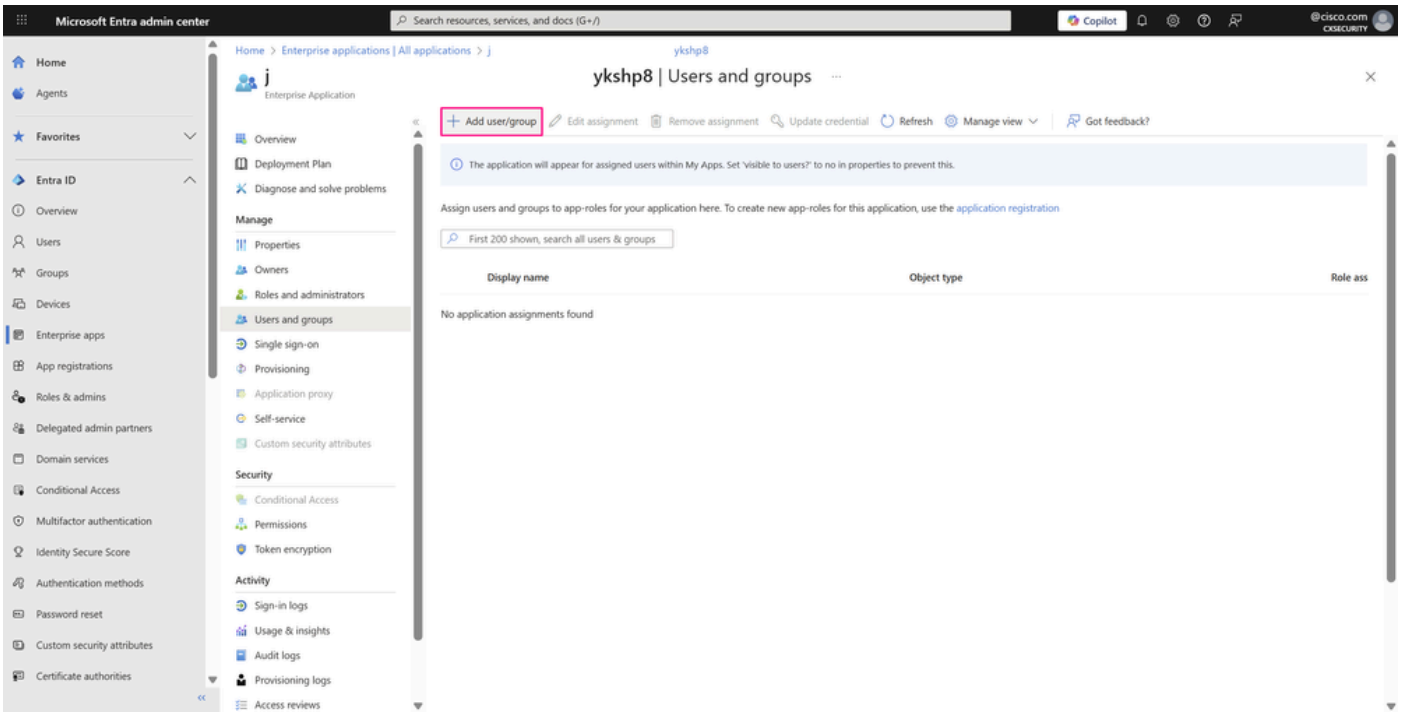
步骤4.为Microsoft Entra ID配置SAML组调配

- 要在SAML配置中调配与其关联的组或用户，需要将其分配到企业应用，以便他们拥有您的应用（例如Cisco SD-WAN Manager）的登录权限。导航回Entra ID > Enterprise apps并打开您的企业应用。在左侧菜单的Manage部分中，单击Users and groups。



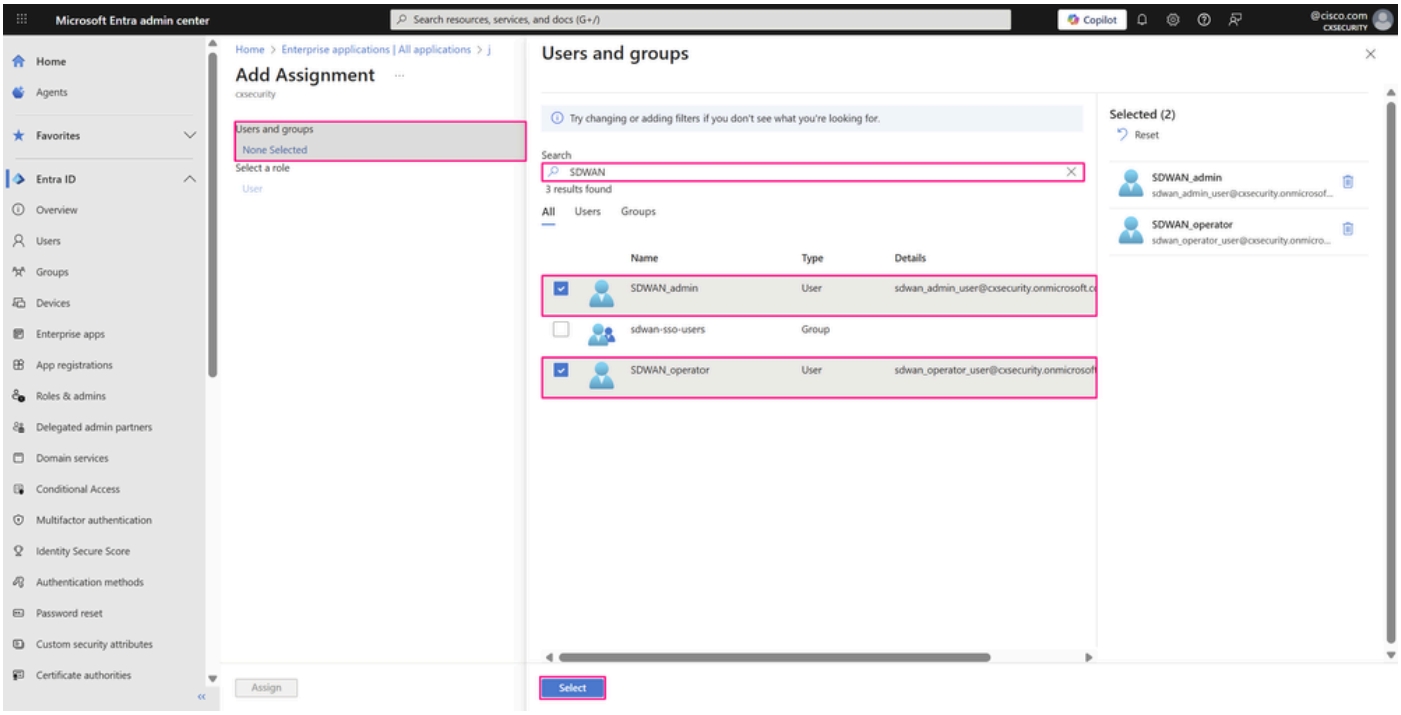
“使用SAML的SSO配置”页

- 接下来，单击Add user/group。



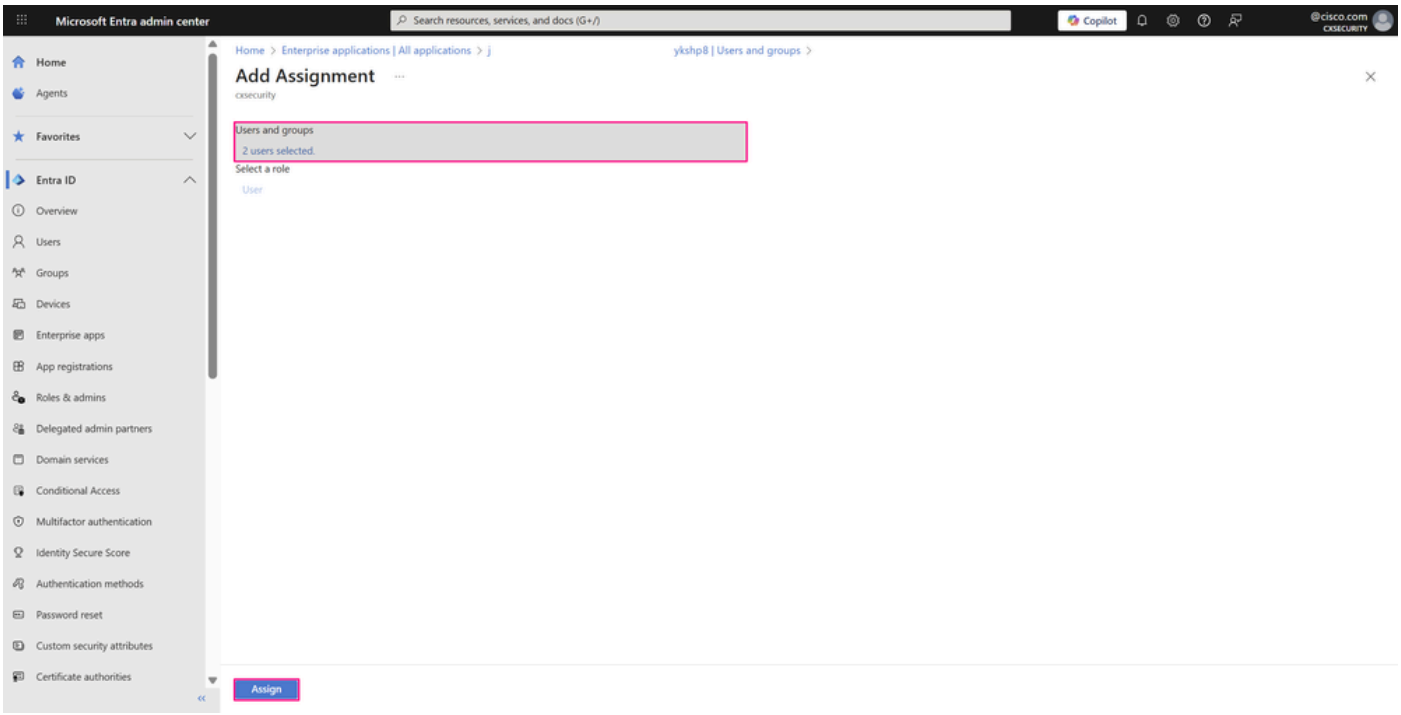
“用户和组”页

- 在Add Assignment窗格中，点击Users and groups字段下的None Selected。搜索并选择要分配给应用程序的用户或组(在本例中，为前面步骤中创建的两个用户)，然后单击选择。



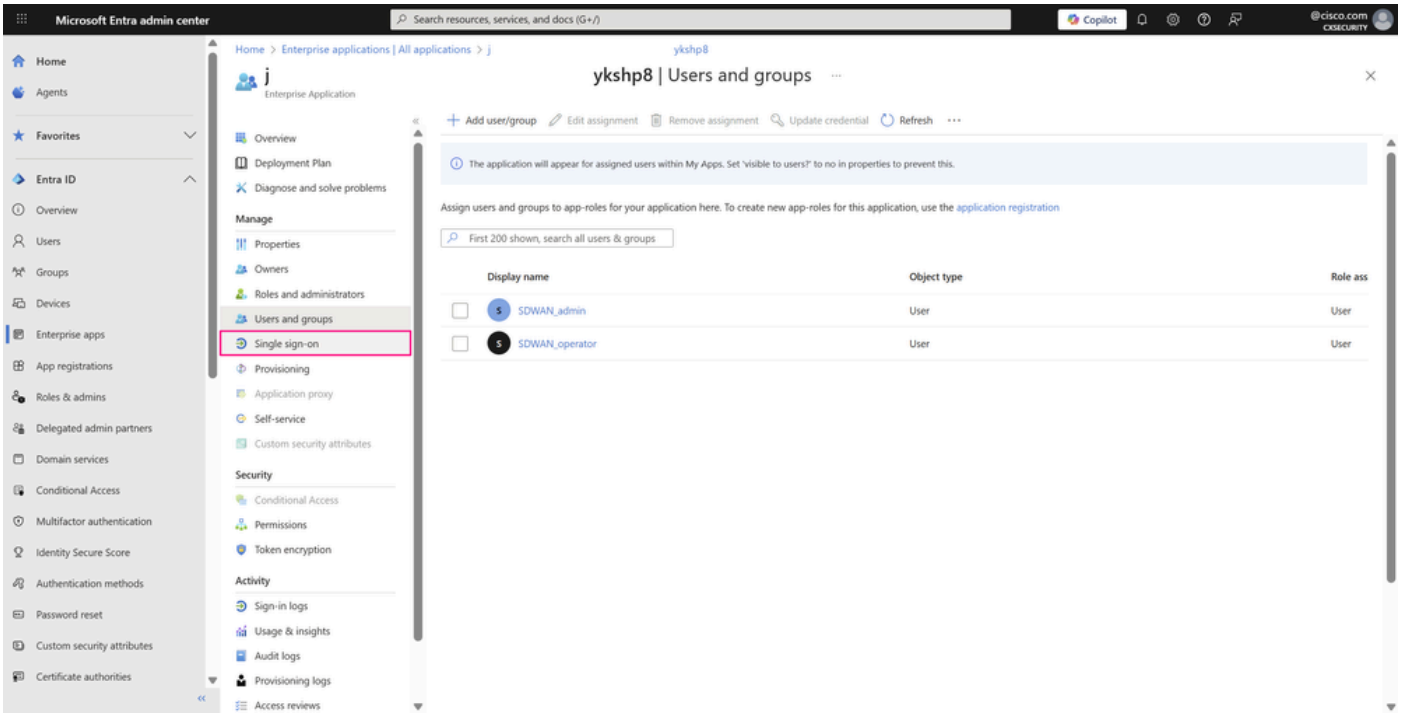
用户/组分配窗格

- 单击Assign将用户或组分配给应用程序。



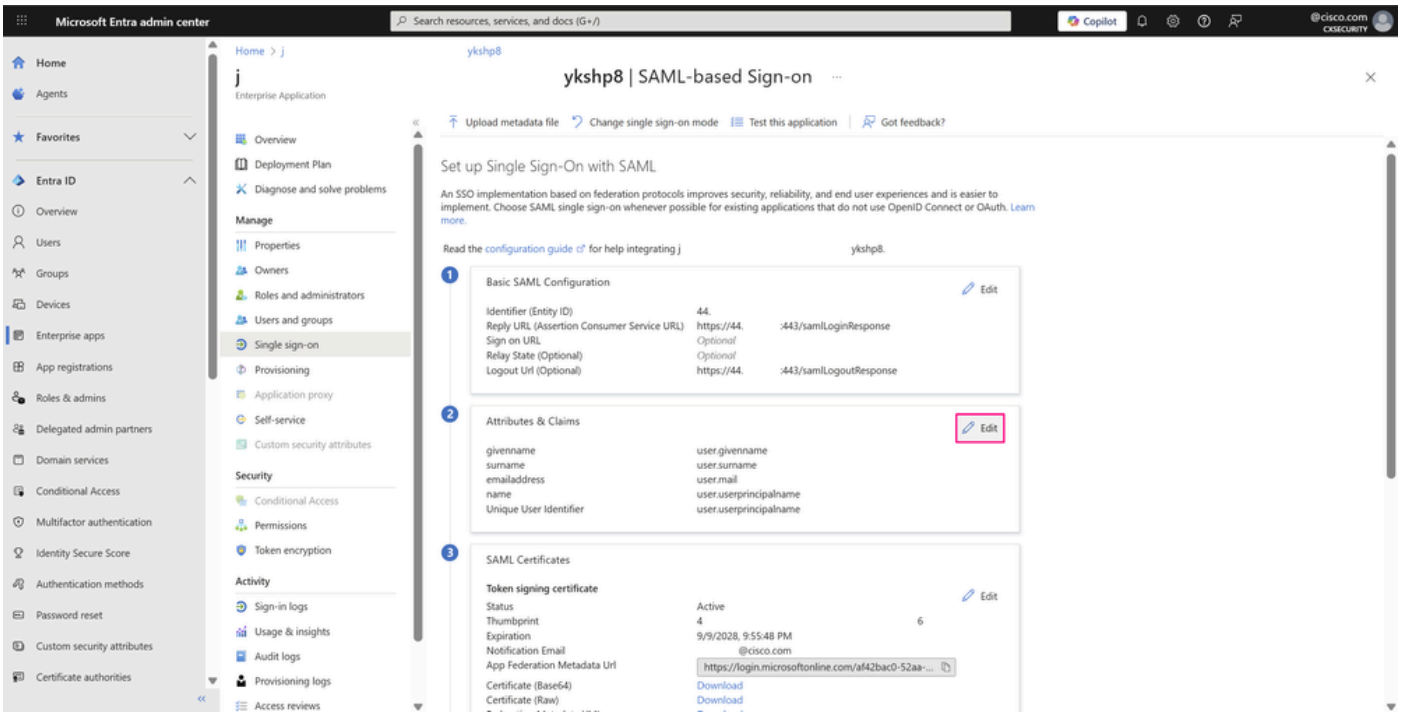
用户/组分配窗格

- 分配给企业应用的用户会在分配后立即列出。在左侧菜单的Manage部分中单击Single sign-on可访问应用的SSO SAML配置并完成其余所需的配置。



“用户和组”页

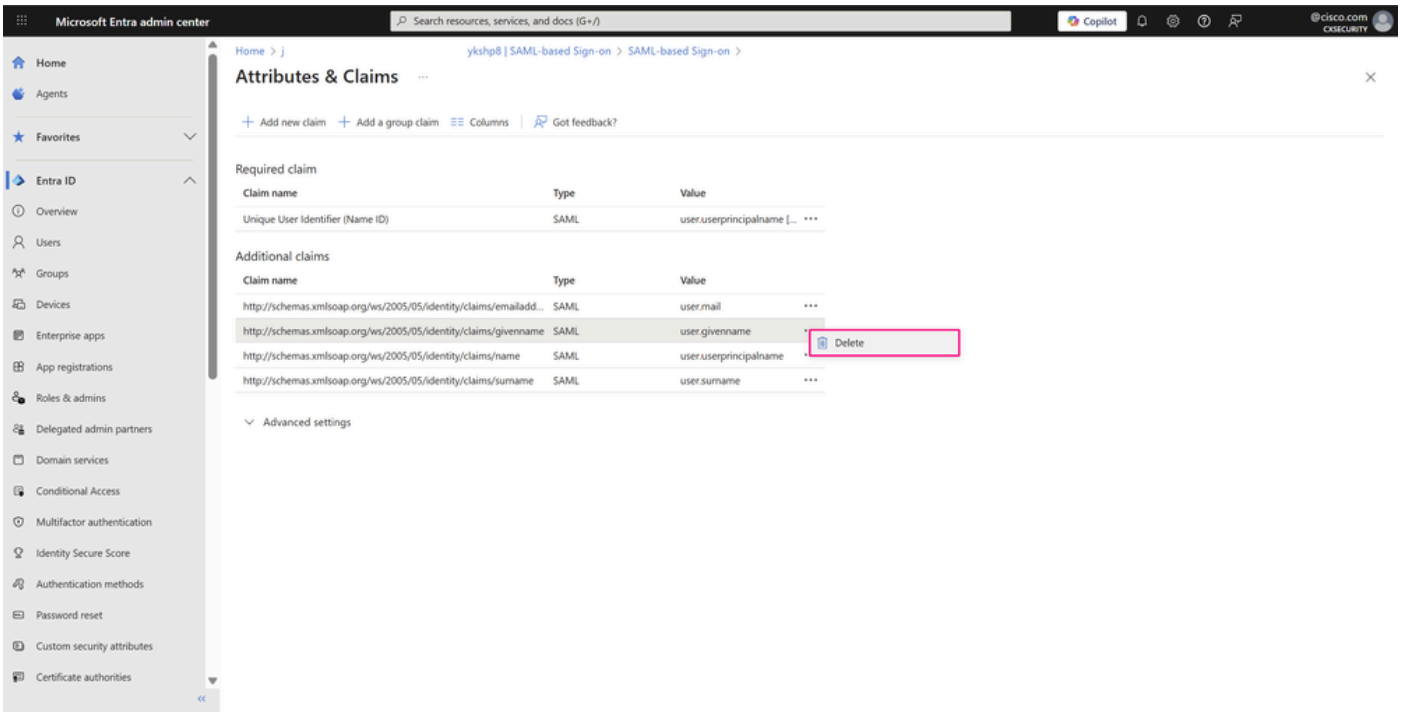
- 在Set Single Sign-On with SAML页面的Attributes & Claims下，单击Edit。



“使用SAML的SSO配置”页

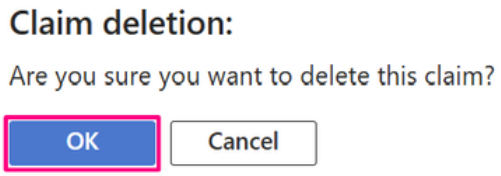
- 在“属性和领款申请”(Attributes & Claims)页面上，点击三点图标，然后点击删除以删除值为user.givenname的领款申请和值为user.surname的领款申请，因为本示例不需要这些领款申请。只有以下领款申请对于您的应用程序进行基本SSO身份验证是必需的：
    - user-user.mail的电子邮件地址
    - user-user.userprincipalname的用户主体名(UPN)

注意：您的组织可能根据自身的特定需求要求其他申请。



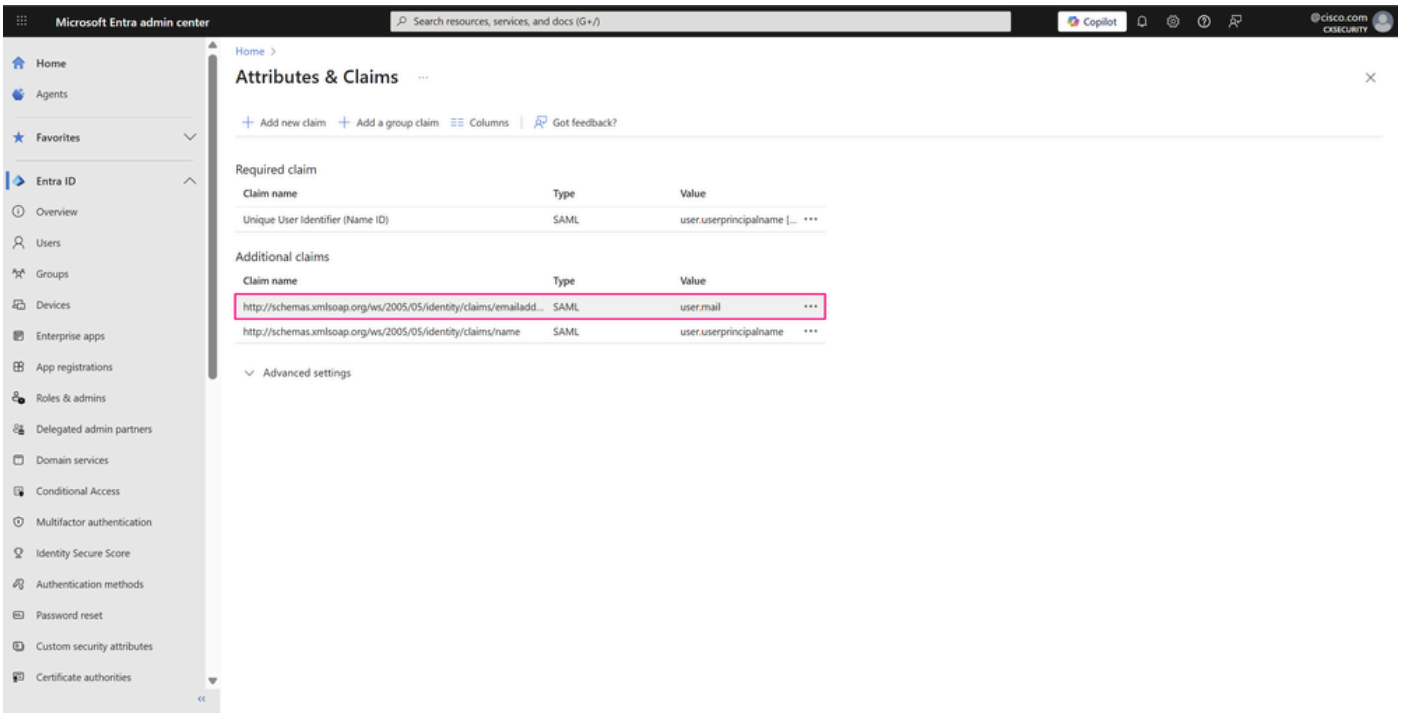
“属性和领款申请”页

- 在Claim deletion窗口中，单击OK以删除领款申请。



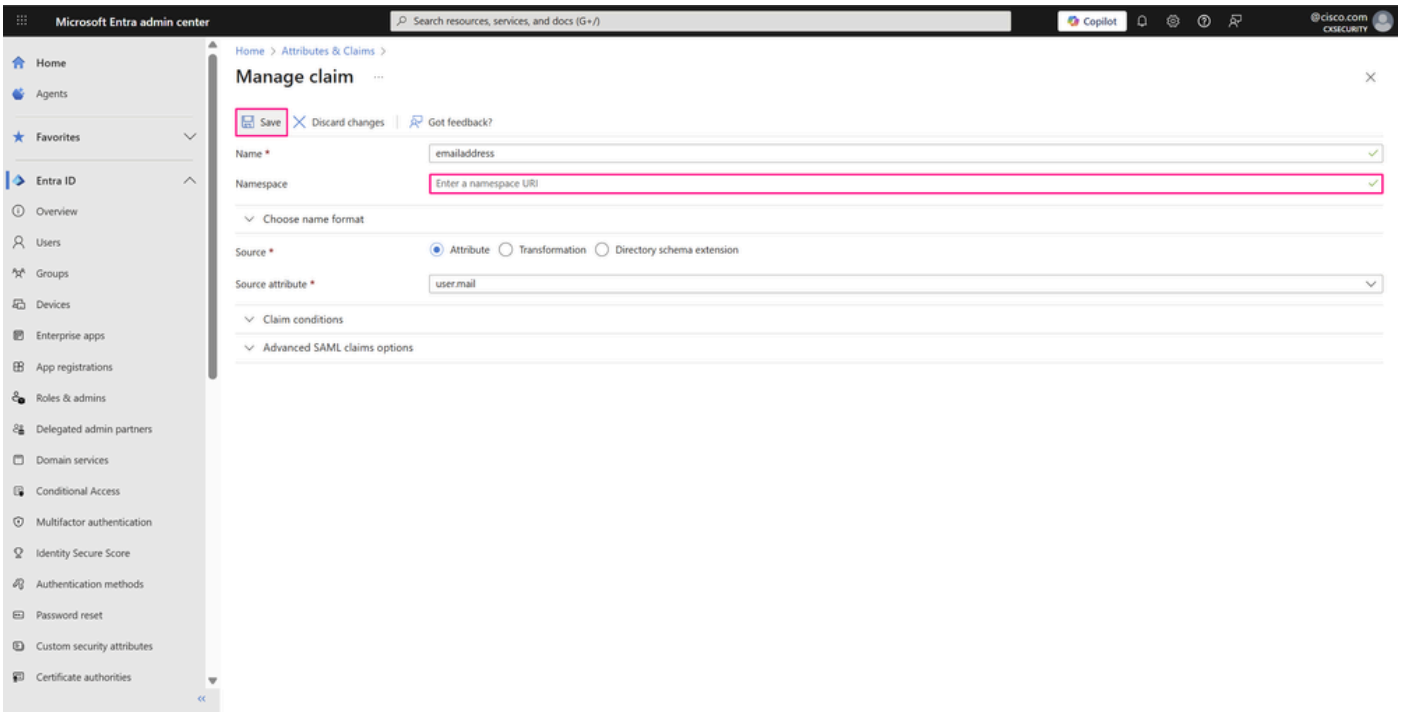
领款申请删除窗口

- 接下来，从其余两个领款申请的领款申请名称中删除命名空间，因为此字段是可选的。此更改允许在此页面上显示每个的实际名称，以便于识别。将鼠标悬停在每个声明上，然后单击它以访问其设置。



“属性和领款申请”页

- 在Manage claim页面上，删除Namespace字段，然后单击Save以应用更改。

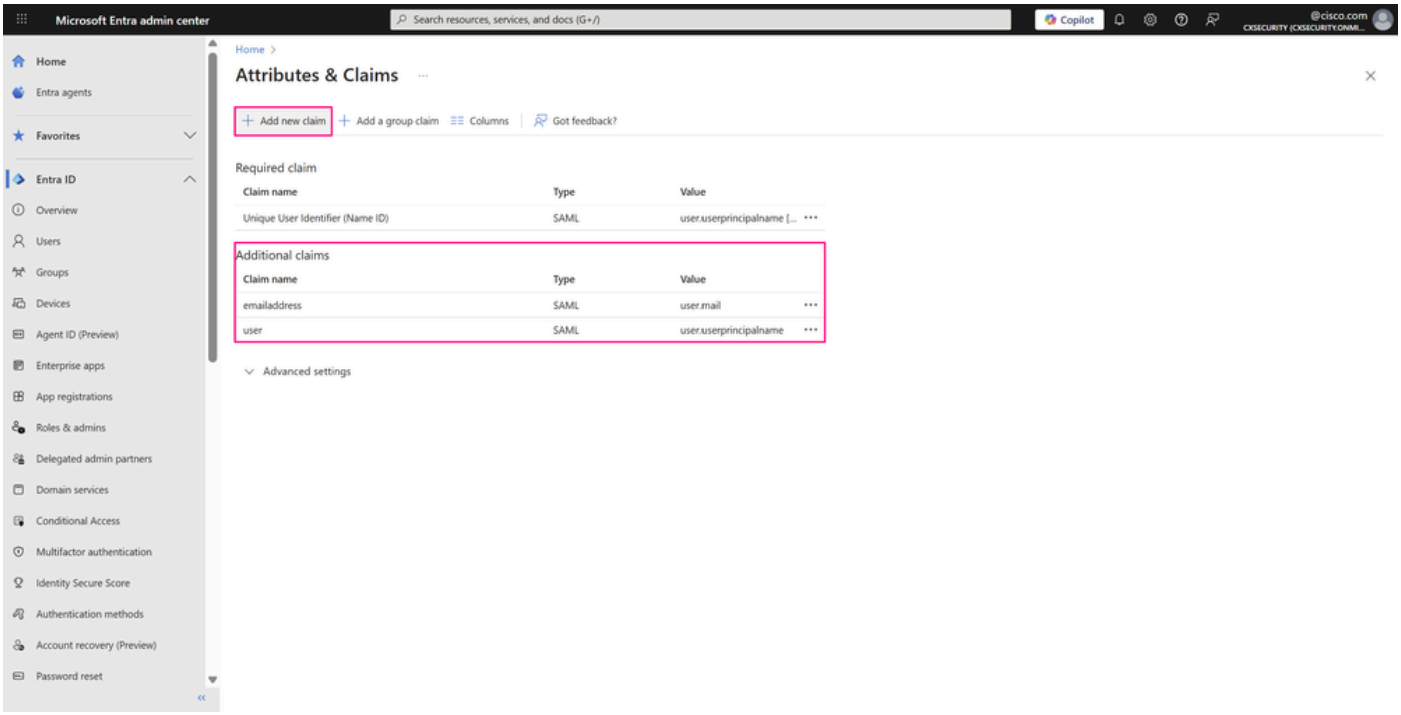


管理领款申请页面

- 现在可以看到两个所需求的名称。但是，还需要一个附加声明，以定义用户所属的组和授权访问应用程序资源的组。为此，请单击Add new claim。

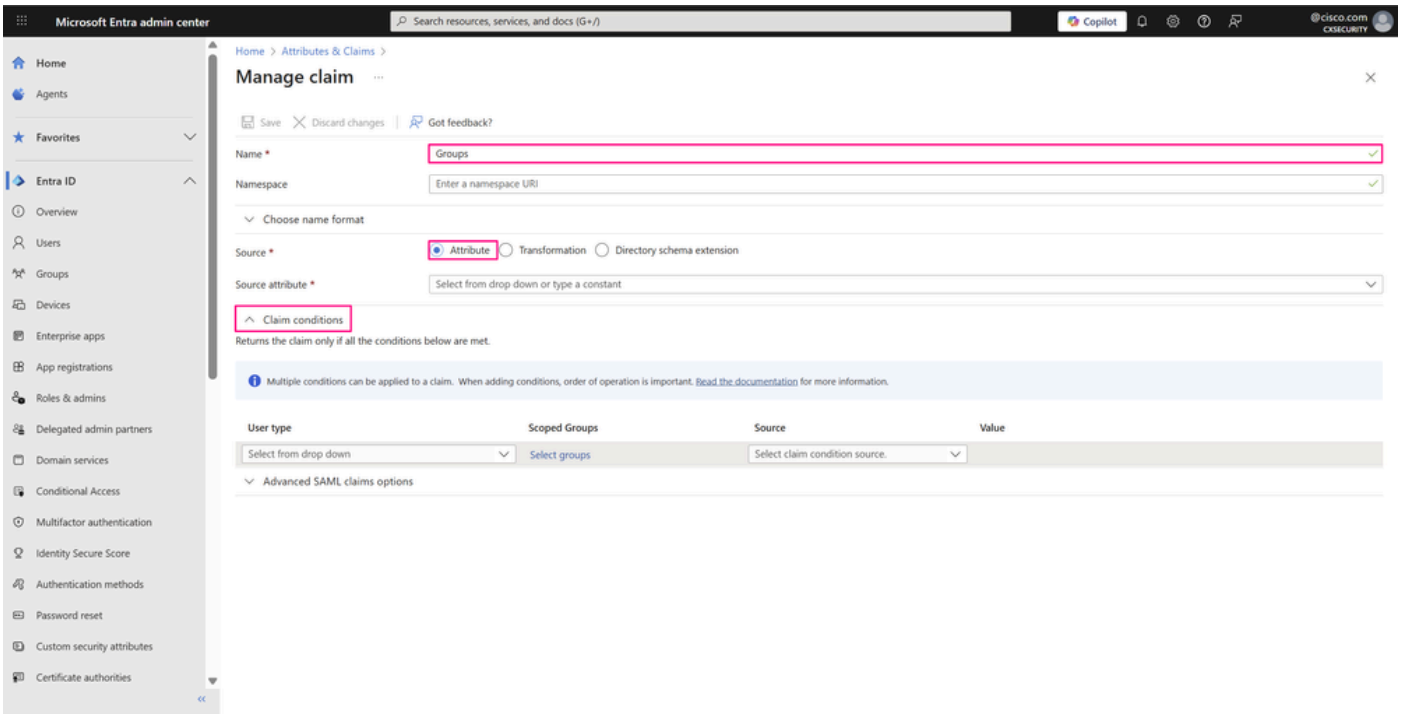
注意：在本例中，选择user作为UPN Claim name，以便在Cisco SD-WAN Manager UI中

的配置文件详细信息中显示用户的邮件地址，而不是SAML NameID格式。



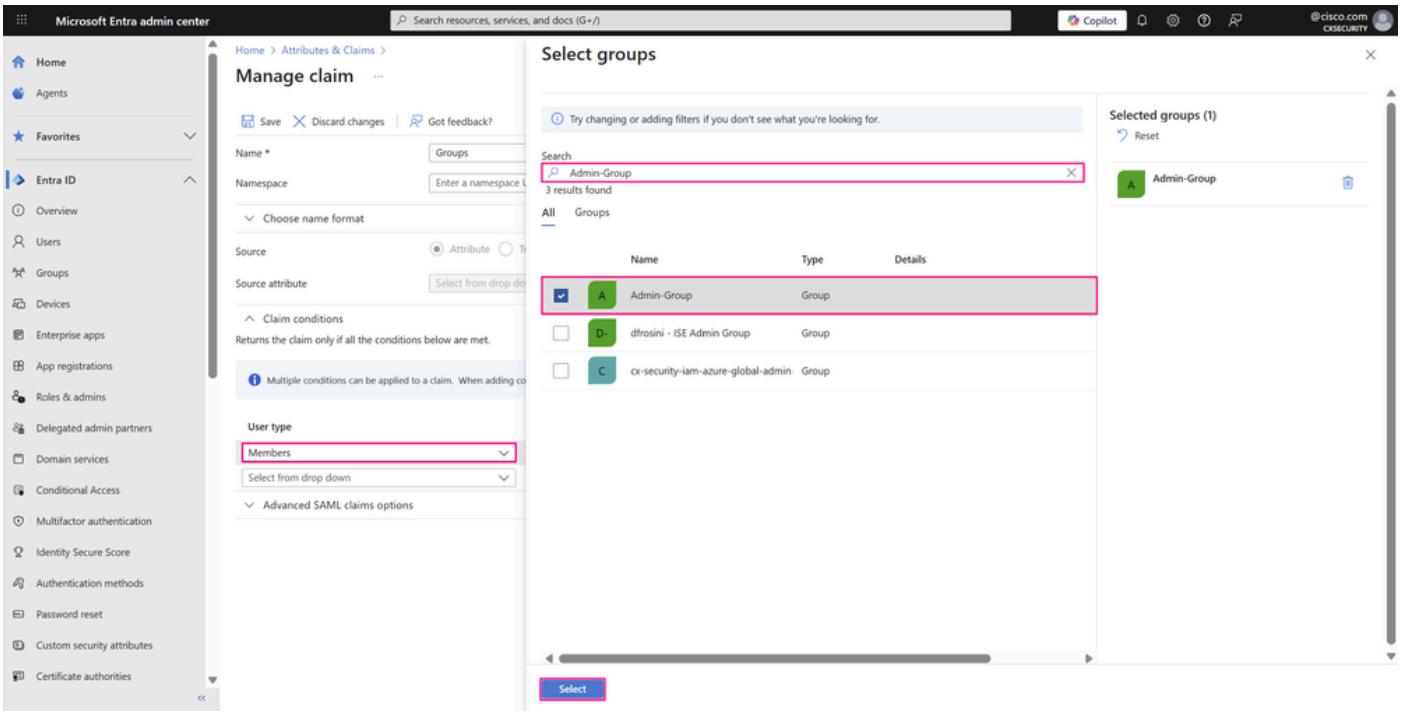
“属性和领款申请”页

- 输入Name以标识此领款申请。在Source旁边，选择Attribute。然后单击Claim conditions展开选项并配置多个条件。



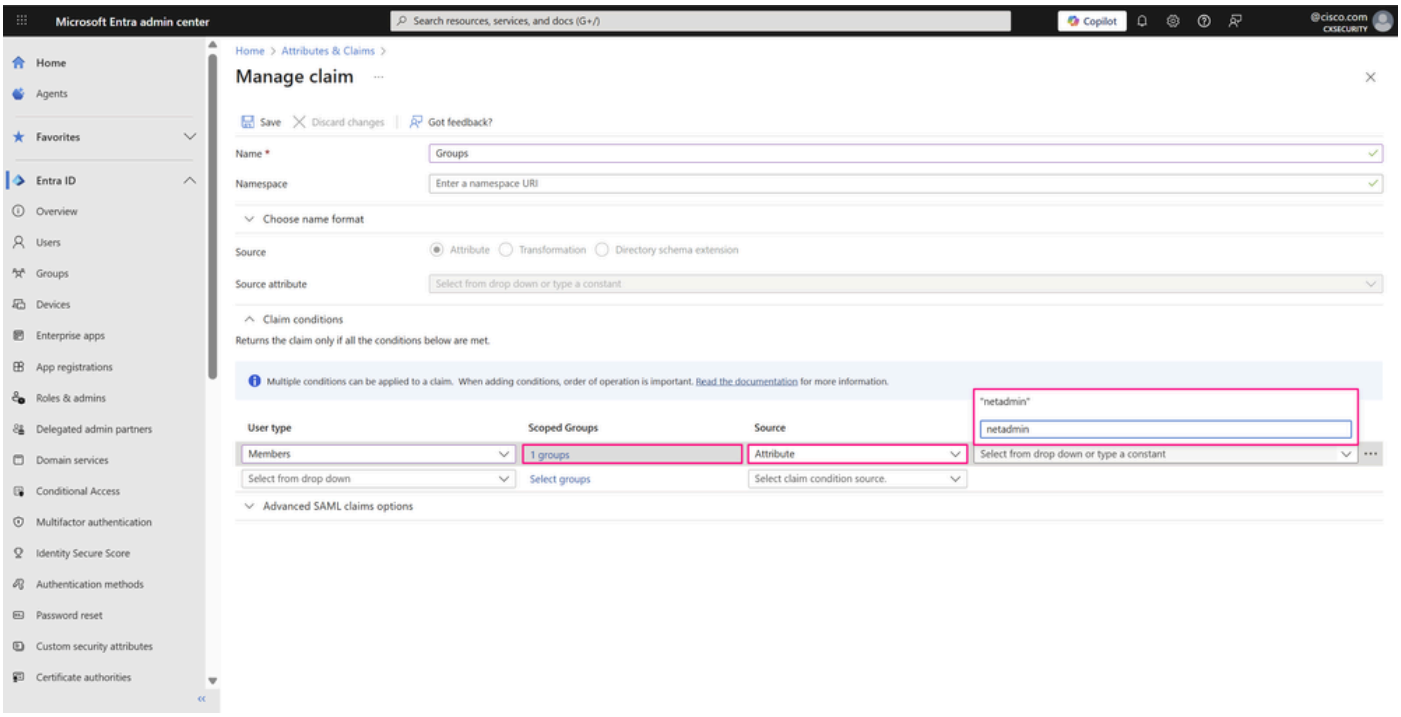
管理领款申请页面

- 在声明条件中，从User type下拉列表中选择Members，然后单击Select Groups以选择用户必须所属的组，然后单击Select。



管理领款申请页面

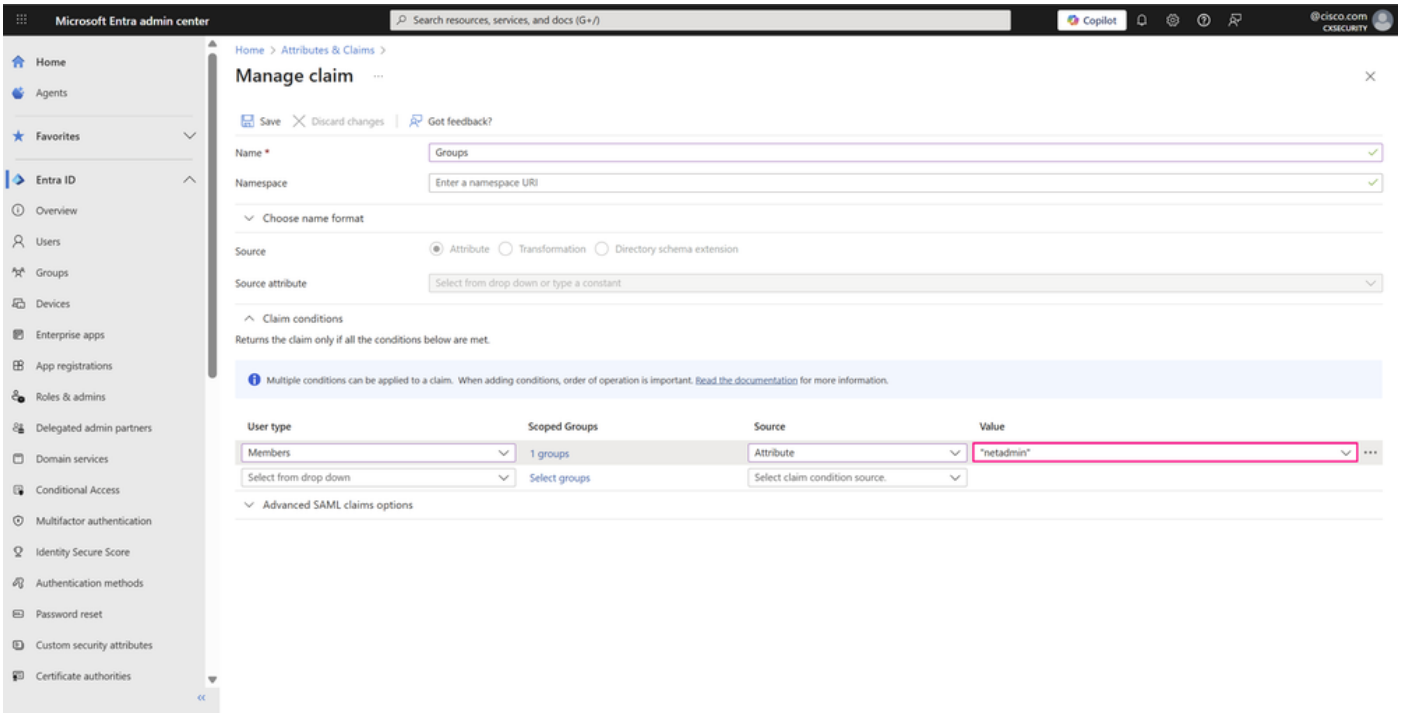
- 从Source下拉列表中选择Attribute，声明将在其中检索其值。在值字段中，输入引用应用程序中所定义的用户组的自定义属性。在本例中，netadmin是Cisco SD-WAN Manager中的标准用户组之一。输入不带引号的属性值，然后按Enter。



管理领款申请页面

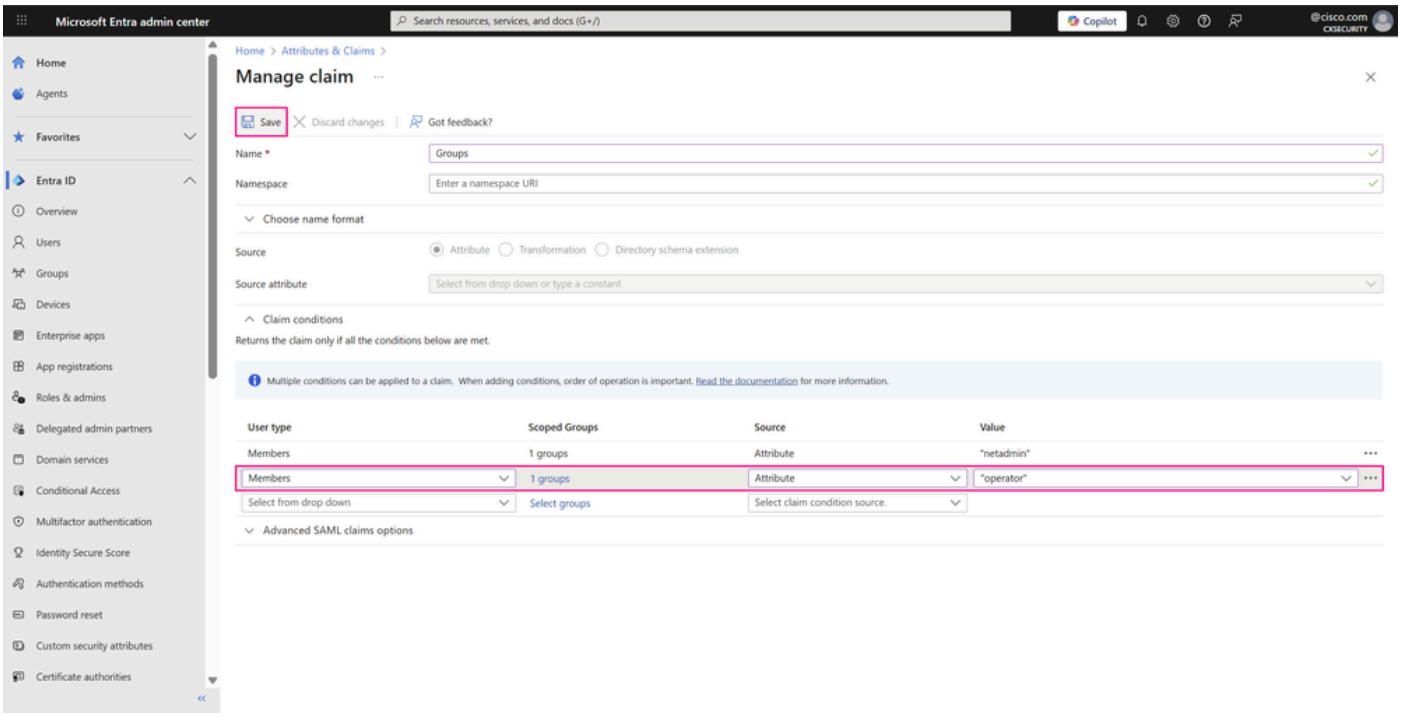
- 紧接之后，属性值会随引号一起显示，因为Microsoft Entra ID将此值作为字符串来处理。

注意：声明条件中的这些参数与企业应用的SSO SAML配置高度相关，因为这些自定义属性必须始终与Cisco SD-WAN Manager中定义的用户组匹配。此匹配项根据用户所属的Microsoft Entra ID组确定授予用户的权限或权限。



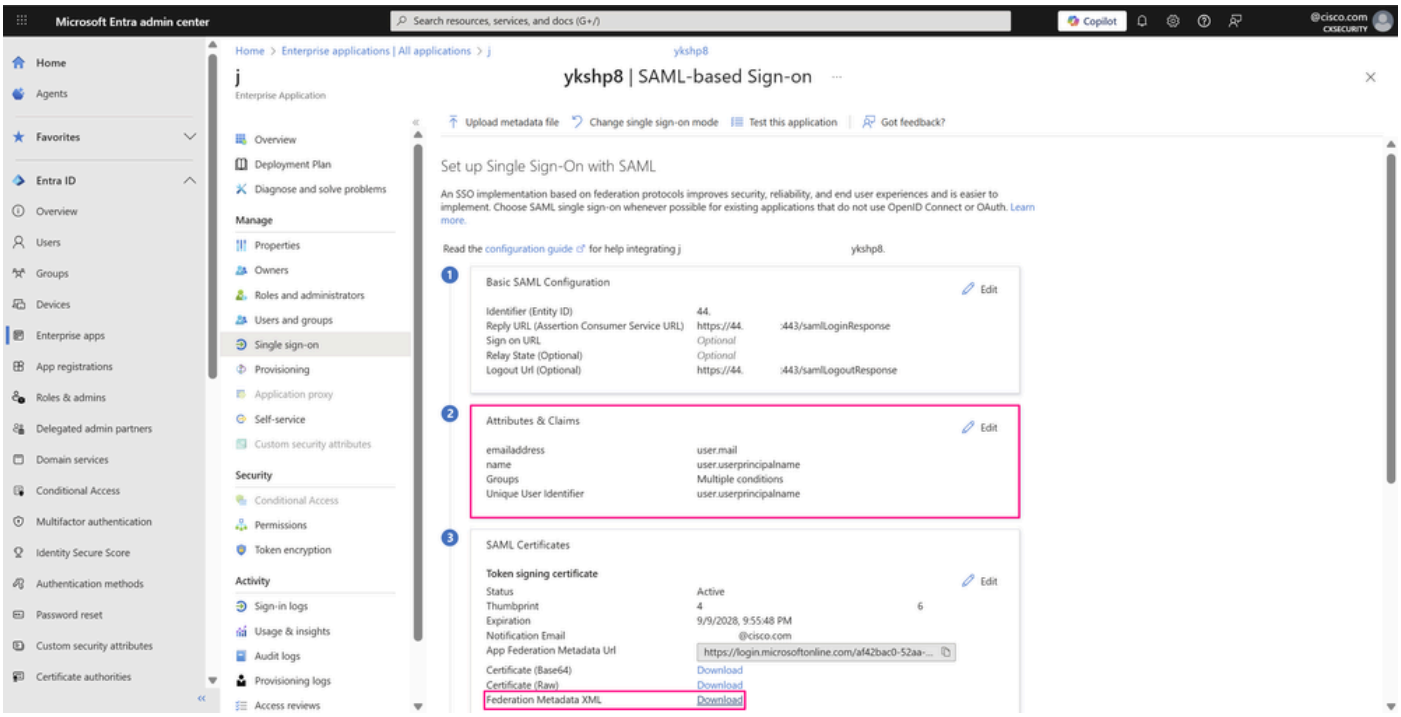
管理领款申请页面

- 为所创建的第二个组(映射到Cisco SD-WAN Manager中的operator用户组)重复相同的步骤。每个具有要登录到应用程序的特定权限的不同组都需要此过程。您也可以在一个条件中添加多个组。单击Save保存更改。



管理领款申请页面

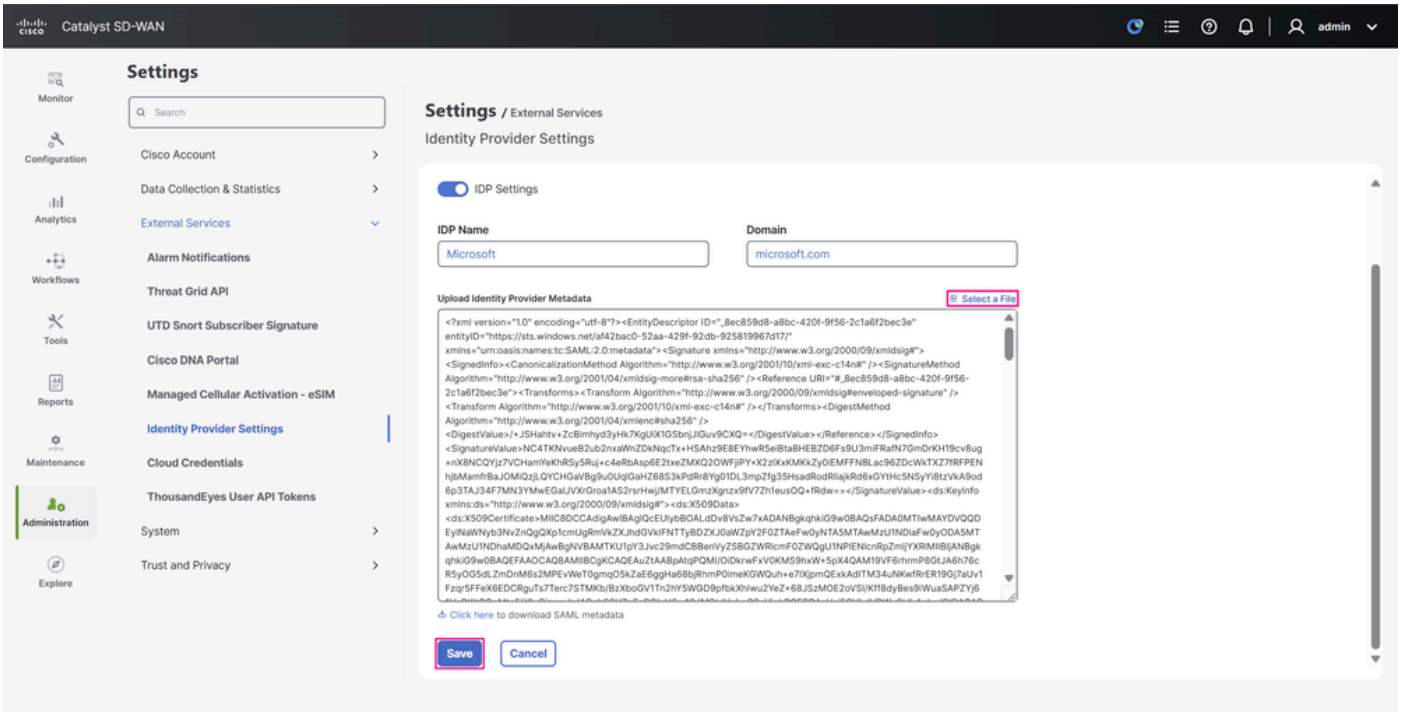
- 在使用SAML设置单点登录页面上，属性和领款申请部分显示所做的新更改。要完成Microsoft Entra ID中的配置，请在SAML Certificates下，点击Federation Metadata XML旁边的Download，将提供身份服务的XML文件下载到应用程序。



"使用SAML的SSO配置"页

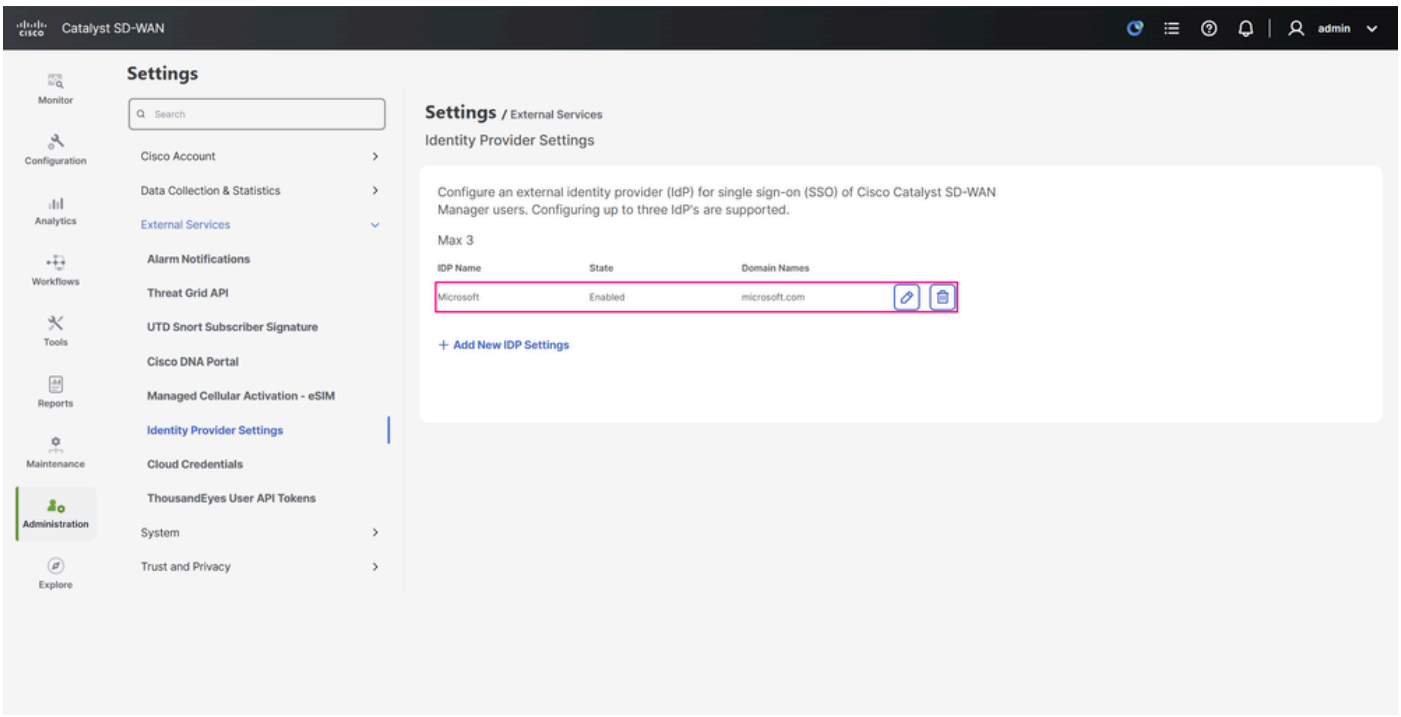
步骤5.将Microsoft Entra ID SAML元数据文件导入到Cisco SD-WAN Manager

- 要将联合元数据上传到Cisco SD-WAN Manager，请导航到Administration > Settings > External Services > Identity Provider Settings，然后单击Select a file。选择刚从Microsoft Entra ID下载的文件，然后单击Save。



“IdP设置配置”页

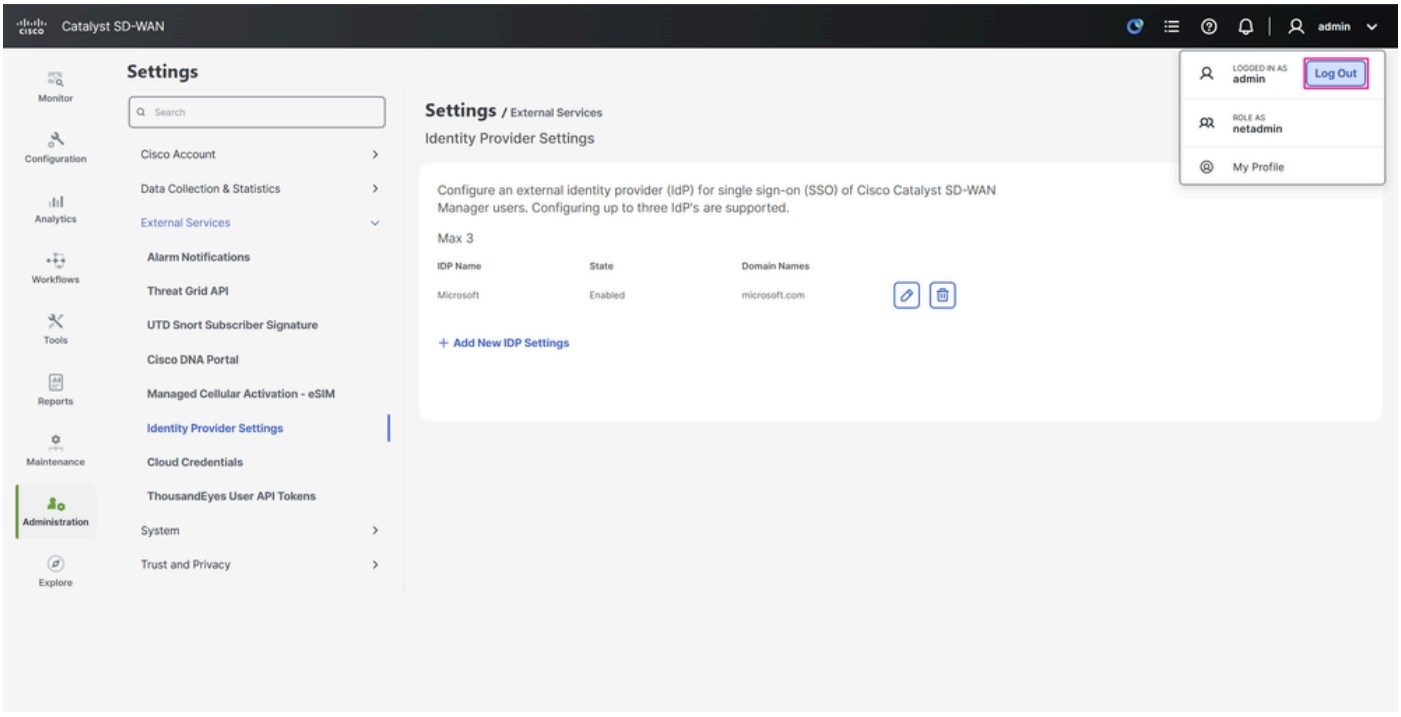
- IdP设置和元数据现在已保存。



“IdP设置配置”页

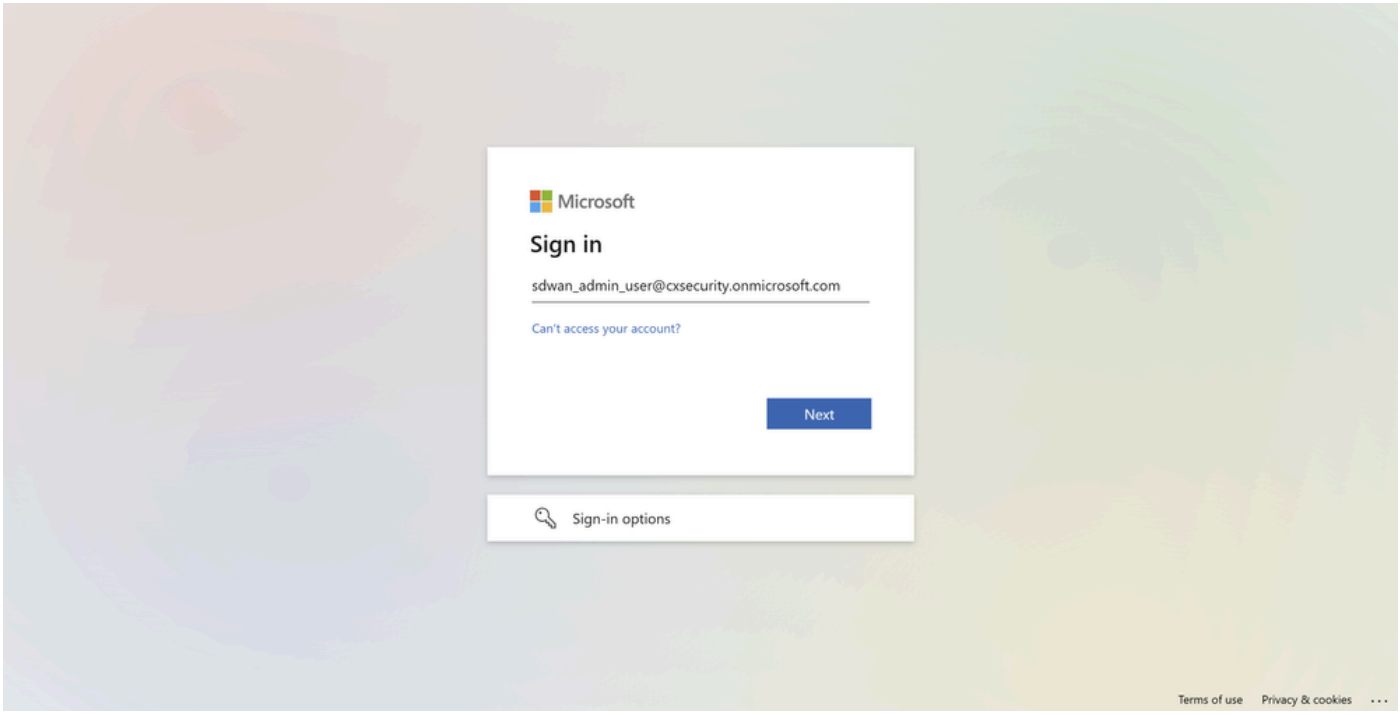
验证

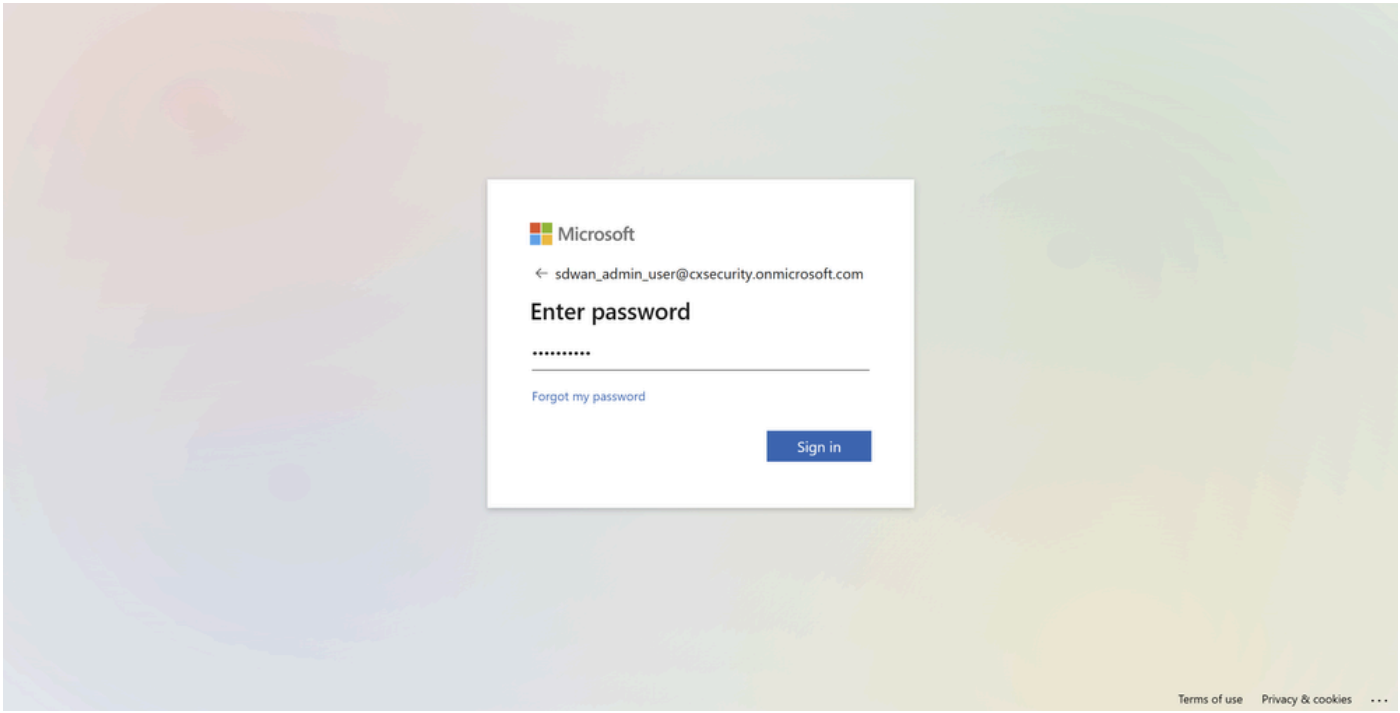
- 在UI的右上角点击您的配置文件名称以展开选项，从那里点击注销以注销门户。



配置文件菜单

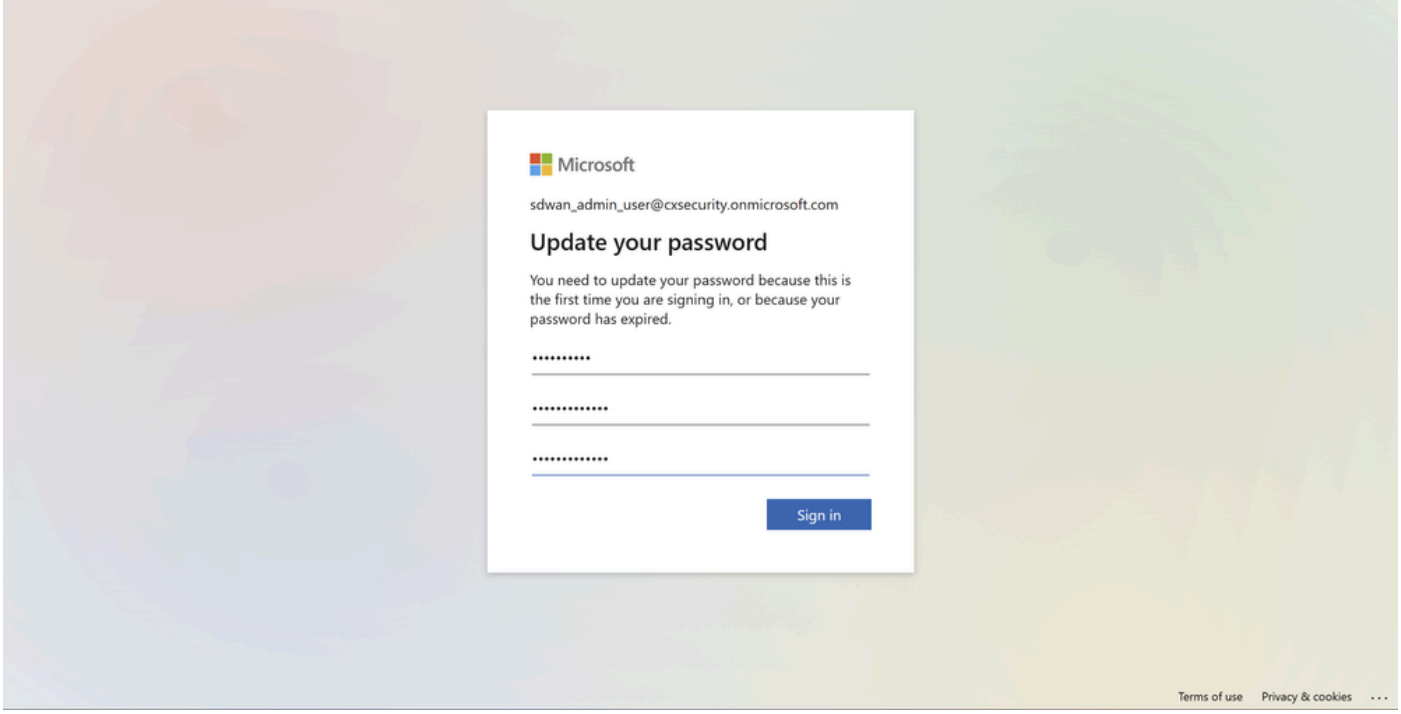
- 您将立即重定向到Microsoft身份验证屏幕，在该屏幕使用Microsoft Entra ID SSO用户的凭证登录。





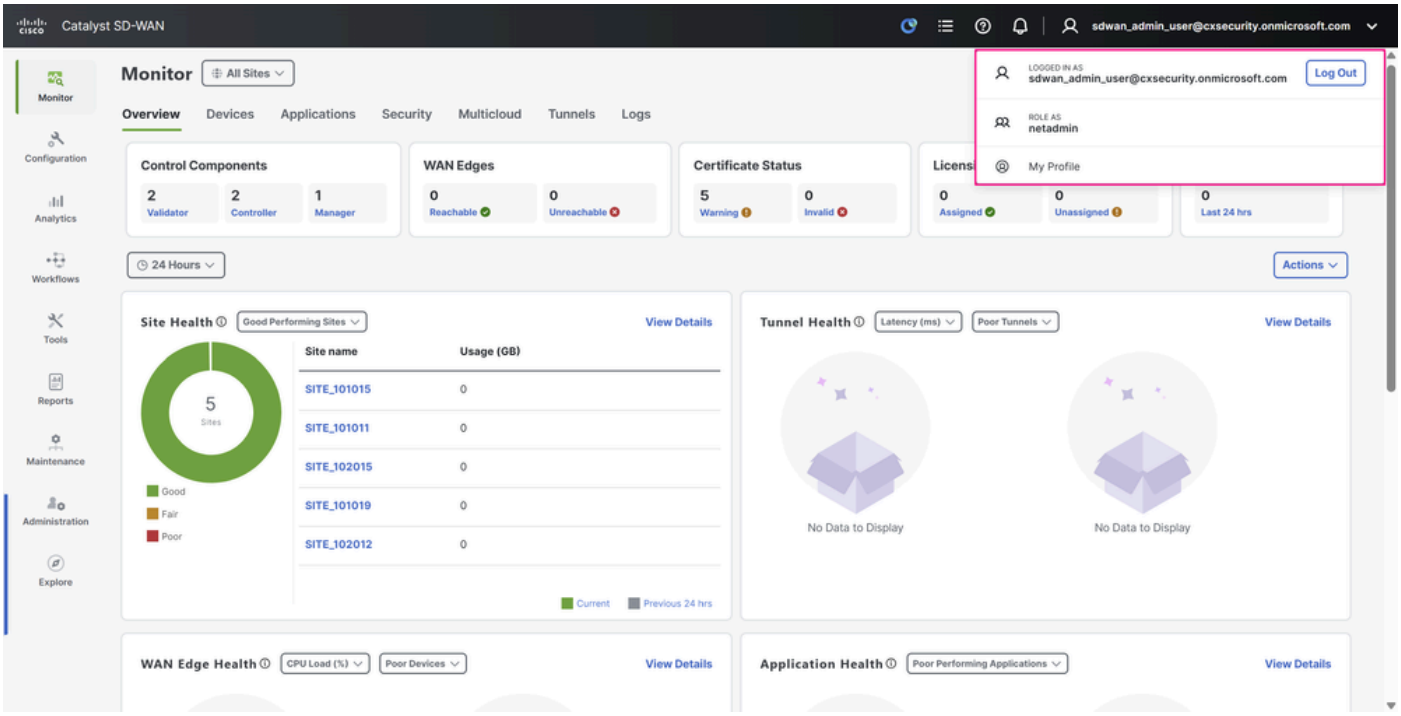
Microsoft登录屏幕

- 由于这是SSO用户首次登录，提示符会请求更改密码。



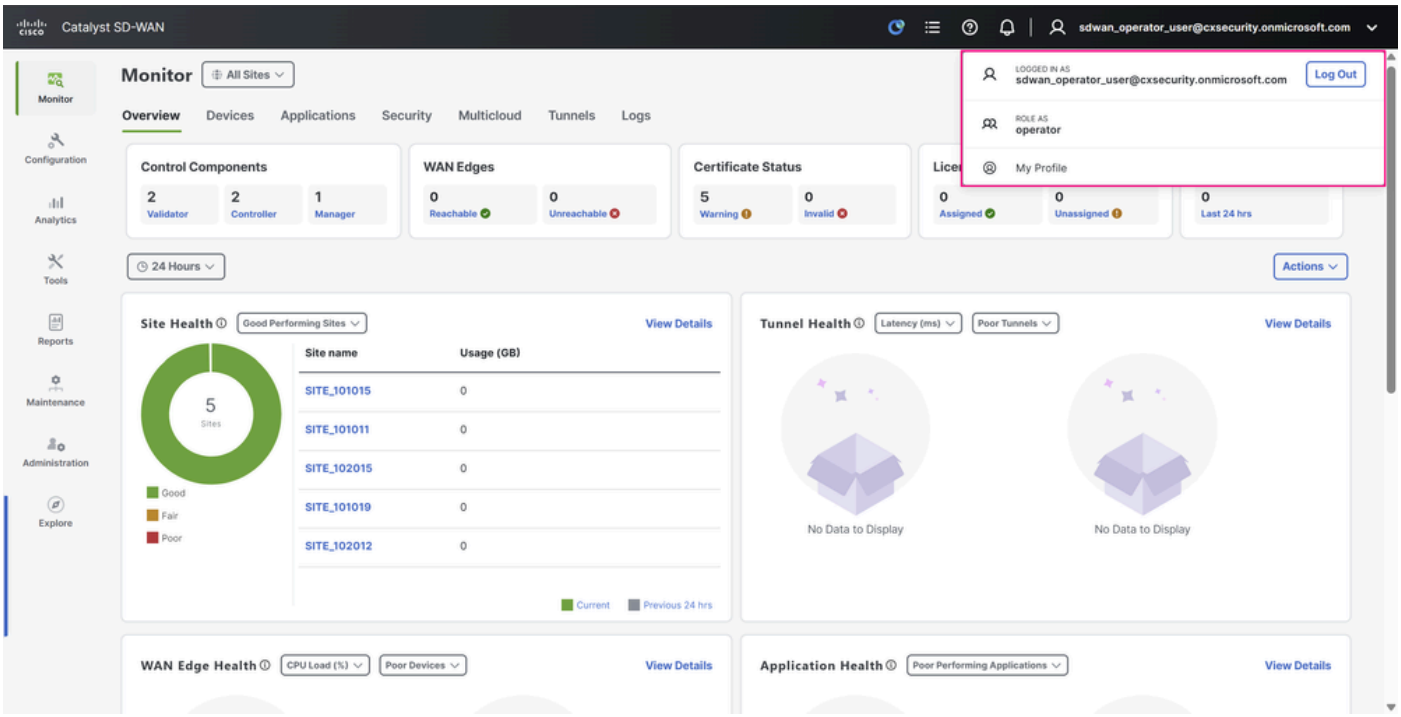
Microsoft登录屏幕

- 成功登录后，在控制面板右上角再次展开您的配置文件的详细信息，您可以确认检测到用户具有netadmin角色，与Microsoft Entra ID中配置的完全相同。



思科SD-WAN管理器UI

- 最后，与其他用户执行相同的登录测试。您看到相同的行为 — 用户现在以operator角色标识。



思科SD-WAN管理器UI

相关信息

- [在Cisco IOS XE Catalyst SD-WAN上配置单点登录]

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）。