为DMP配置Microsoft Entra ID SSO外部身份验证

目录

简介

本文档介绍如何配置Microsoft Entra ID单点登录以向思科域保护门户进行身份验证。

先决条件

要求

思科建议您了解以下主题：

- 思科域保护
- Microsoft Entra ID
- PEM格式的自签名或CA签名（可选）X.509 SSL证书

使用的组件

- Cisco Domain Protection管理员访问权限
- Microsoft Entra ID管理中心管理员访问权限

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

- 思科域保护通过SAML 2.0协议为最终用户启用SSO登录。
- Microsoft Entra SSO允许和控制通过单点登录从任何地点访问软件即服务(SaaS)应用、云应

用或本地应用。

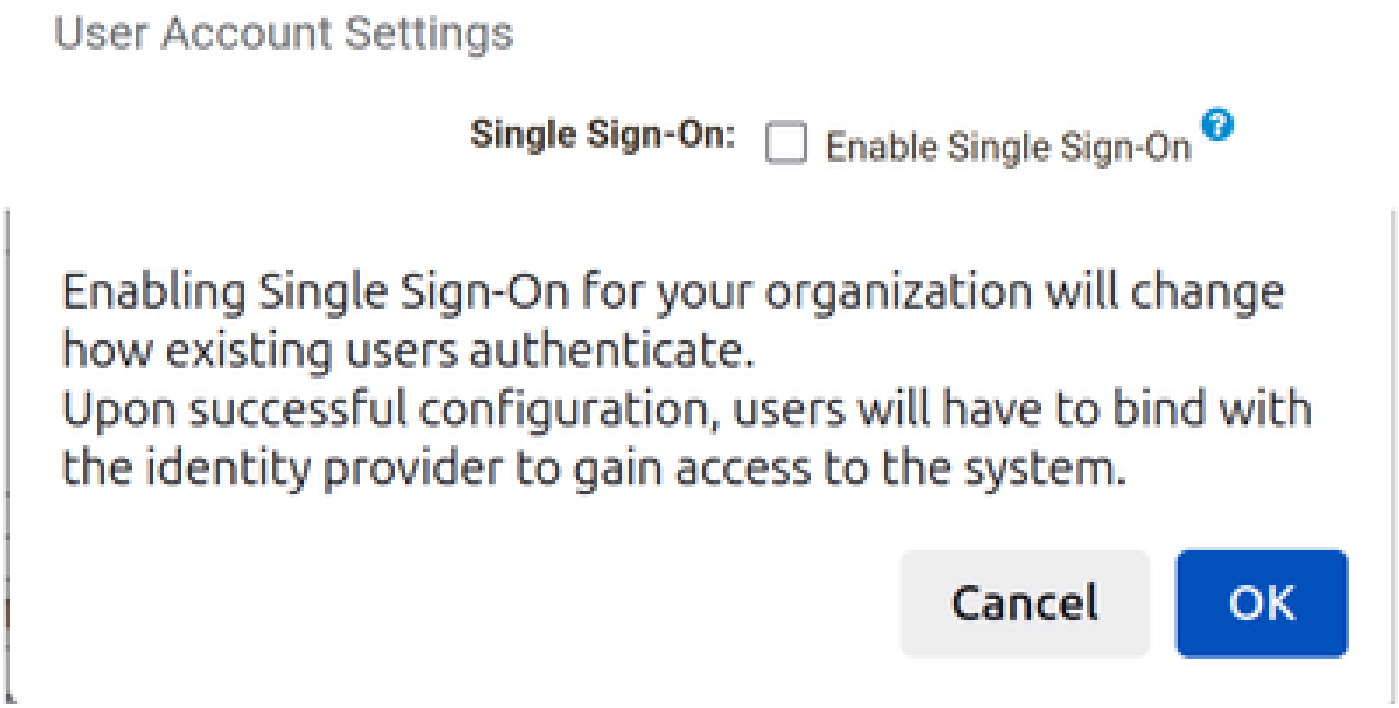
- Cisco Domain Protection可以设置为连接到Microsoft Entra的托管身份应用，其身份验证方法包括多重身份验证，因为纯密码身份验证不安全，也不建议使用。
- SAML是基于XML的开放标准数据格式，使管理员能够在登录其中一个应用后无缝访问一组已定义的应用。
- 要了解有关SAML的更多信息，请参阅：什么是SAML?

配置

思科域保护（第1部分）

1.登录到Cisco Domain Protection管理员门户，然后导航到Admin > Organization。单击Edit Organization Details按钮，如图所示：

2.导航到用户帐户设置部分，然后单击启用Single Sign-On复选框。此时将显示如下图所示的消息：



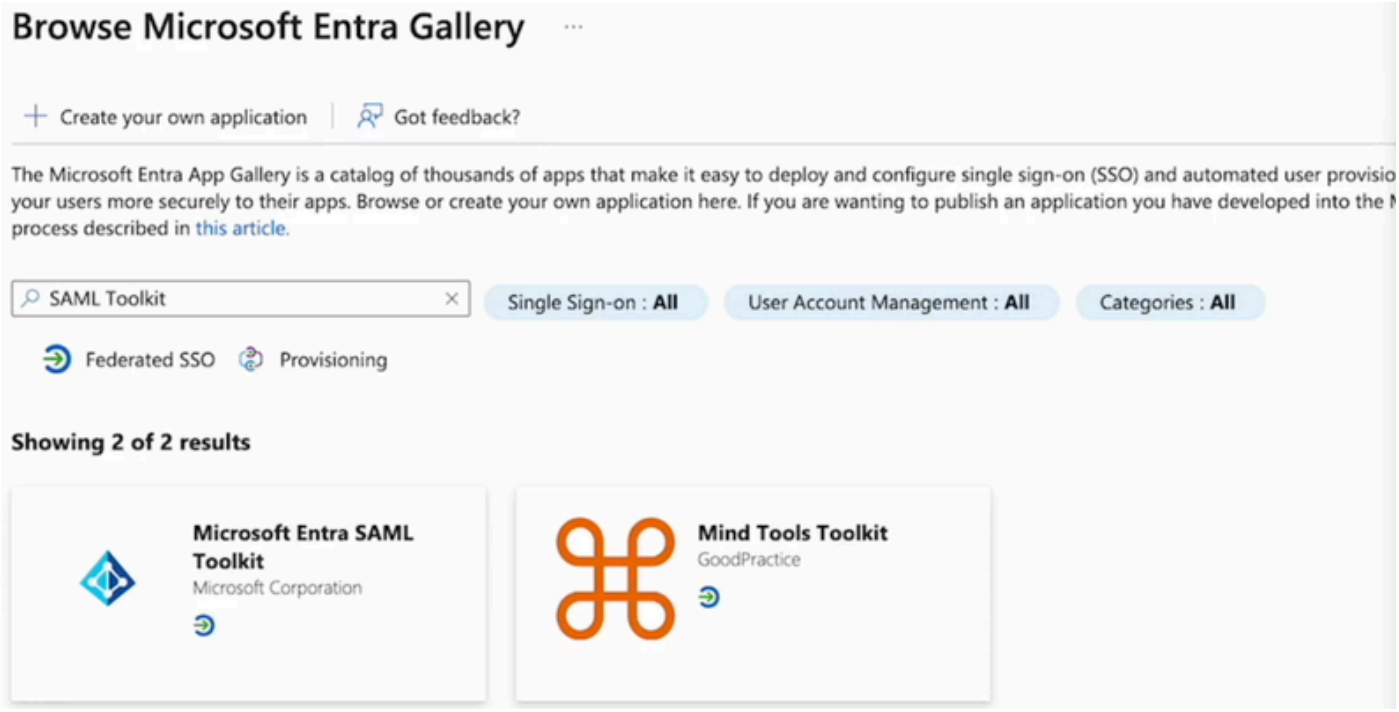
3.单击OK按钮并复制实体ID和断言消费者服务(ACS)URL参数。必须在Microsoft Entra ID基本SAML身份验证中使用这些参数。稍后返回以设置名称标识符格式、SAML 2.0终端和公共证书参数。

- 实体ID:dmp.cisco.com

- 断言消费者服务URL:https://<dmp_id>.dmp.cisco.com/auth/saml/callback

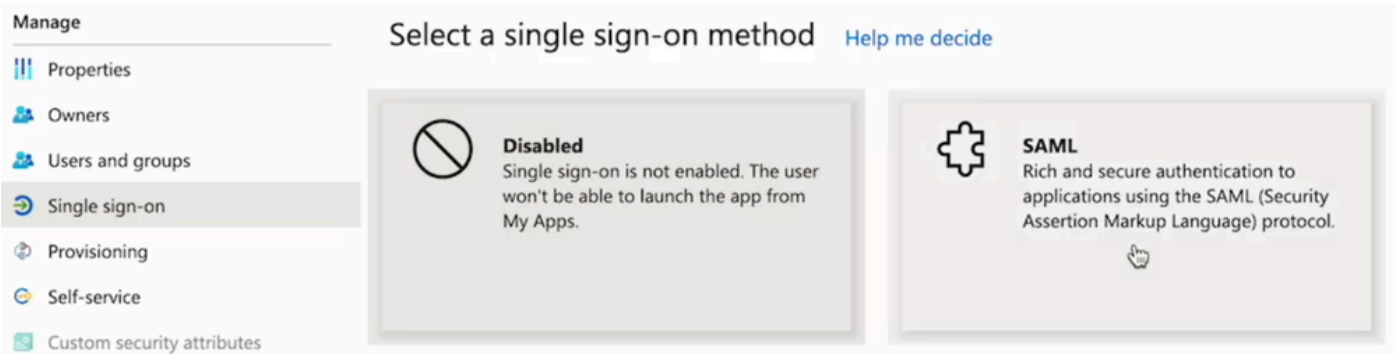
Microsoft Entra ID

1.导航到Microsoft Entra ID管理中心，然后单击Add按钮。选择Enterprise Application，然后搜索Microsoft Entra SAML Toolkit，如图所示：



2.使用有意义的值命名它，然后单击Create。例如，域保护登录。

3.导航至管理部分下的左侧面板。单击Single sign-on，然后选择SAML。



4.在“基本SAML配置”面板中，单击编辑，然后填写参数：

- 标识符（实体ID）：dmp.cisco.com
- 回复URL（断言消费者服务URL）：https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- 登录URL:https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- Click Save.

5.在“属性和领款申请”面板中，单击编辑。

在Required claim下，点击Unique User Identifier(Name ID)声明进行编辑。

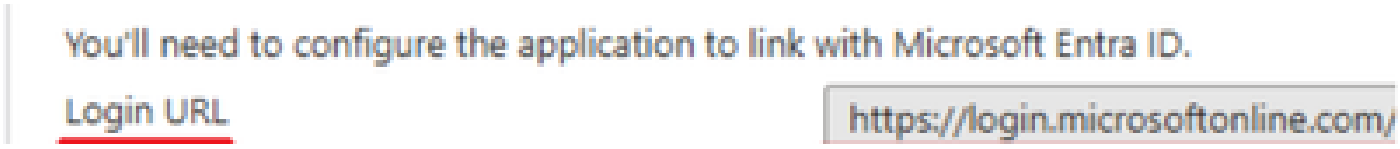
- 将Source attribute字段设置为user.userprincipalname。这假定user.userprincipalname的值代表有效的邮件地址。否则，请将Source设置为user.primaryauthoritiveemail。
- 在Additional Claims面板下，单击Edit并创建Microsoft Entra ID用户属性和SAML属性之间的映射。

名称	命名空间	源属性
电邮地址	无值	user.userprincipalname
名字	无值	user.givenname
姓氏	无值	user.surname

请务必清除每个声明的Namespace字段，如下所示：

6.填写属性和索赔部分后，系统将填写SAML签名证书的最后一部分。

- 保存登录URL。

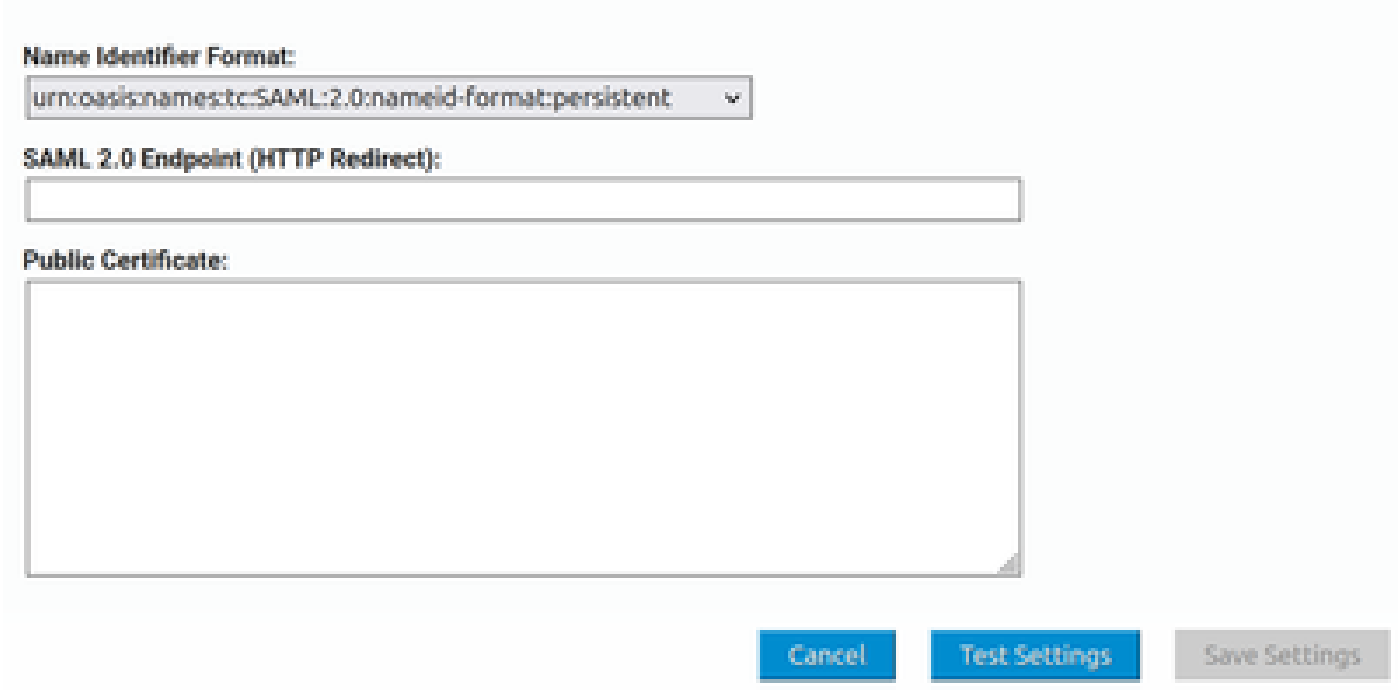


- 保存证书(Base64)。

思科域保护（第2部分）

返回Cisco Domain Protection > Enable Single Sign-On部分。

- 名称标识符格式: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- SAML 2.0终端（HTTP重定向）：Microsoft Entra ID提供的登录URL
- 公共证书:Microsoft Entra ID提供的证书(Base64)



验证

单击测试设置。它将您重定向到身份提供程序的登录页。使用您的SSO凭证登录。

成功登录后，您可以关闭窗口。单击 Save Settings。

故障排除

```
Error - Error parsing X509 certificate
```

- 确保证书在Base64中。

```
Error - Please enter a valid URL
```

- 确保Microsoft Entra ID提供的登录URL正确。

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）。