为CRES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，以便对思科安全邮件加密服务进行身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全邮件加密服务（注册信封）
- 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

- 安全邮件加密服务（注册信封）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。

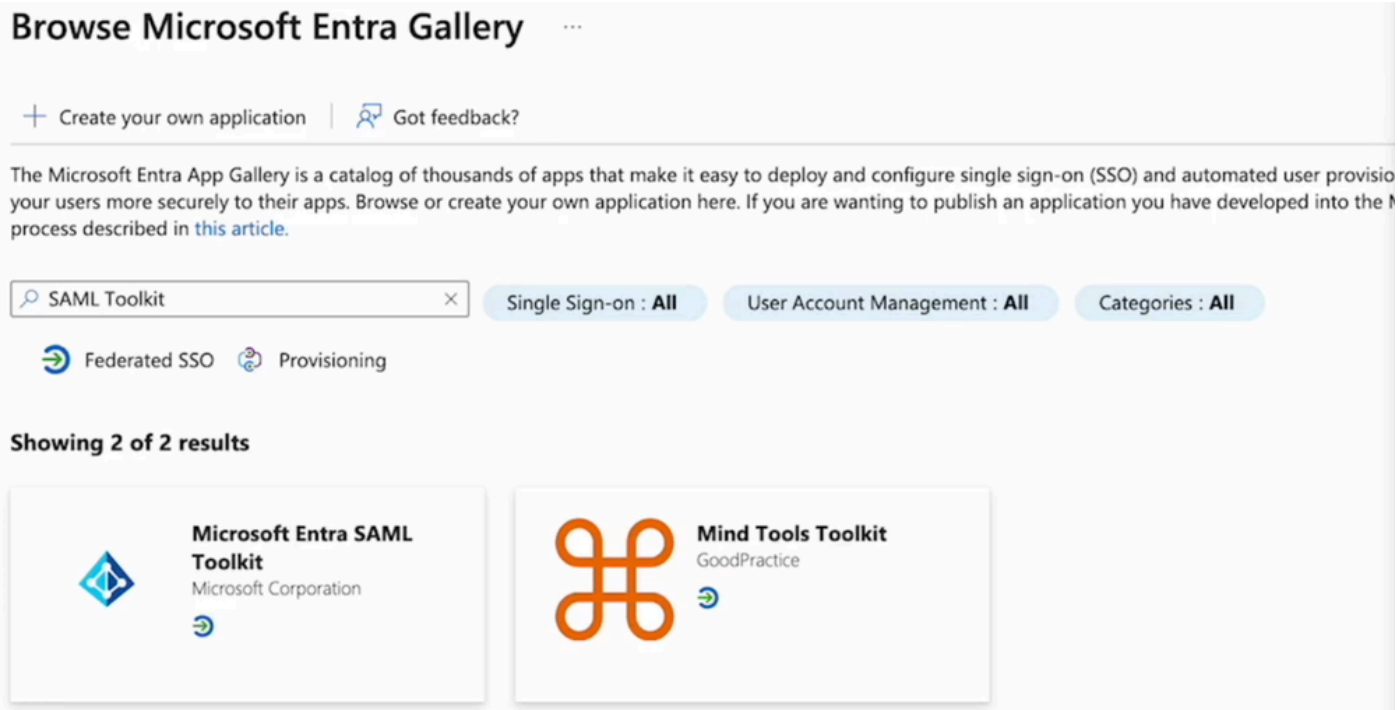
背景信息

- 注册信封为使用SAML的最终用户启用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。
- 注册信封可以设置为通过身份验证方法连接到Microsoft Entra的托管身份应用，这些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

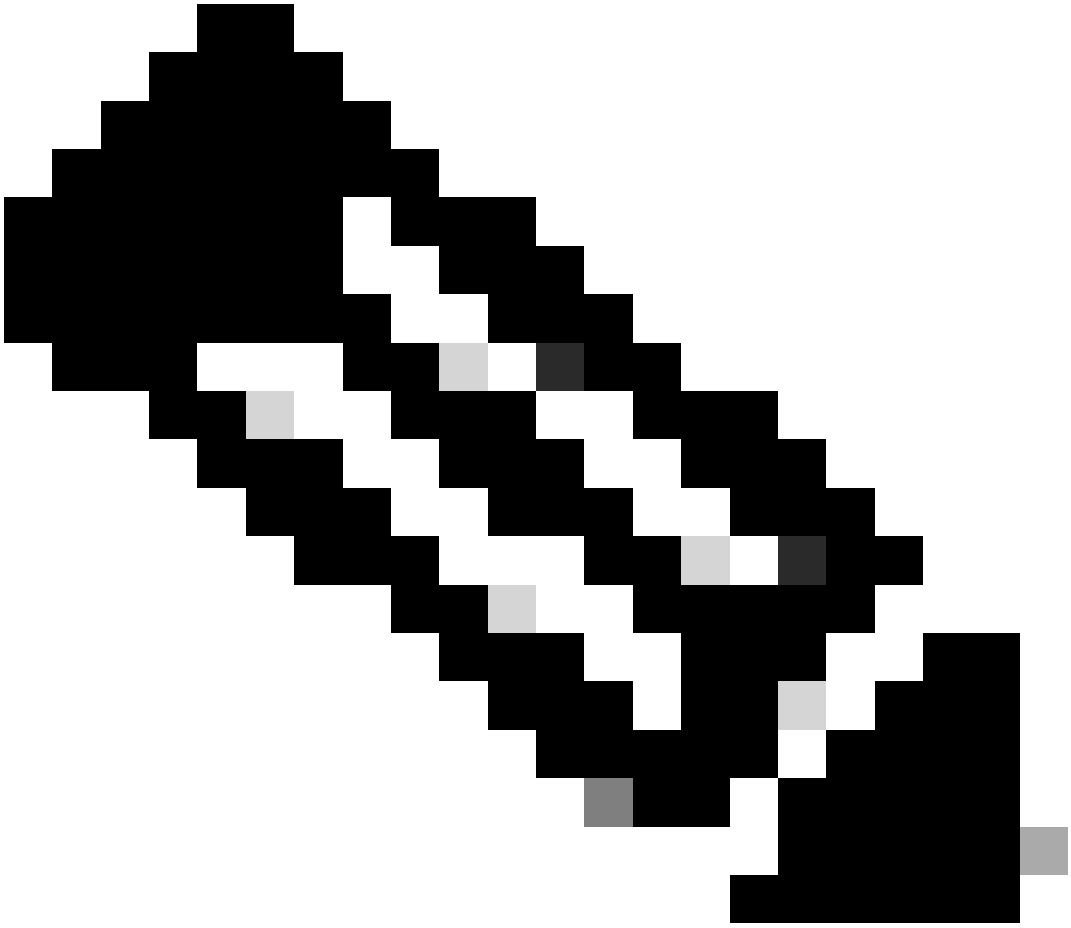
Microsoft Entra ID

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



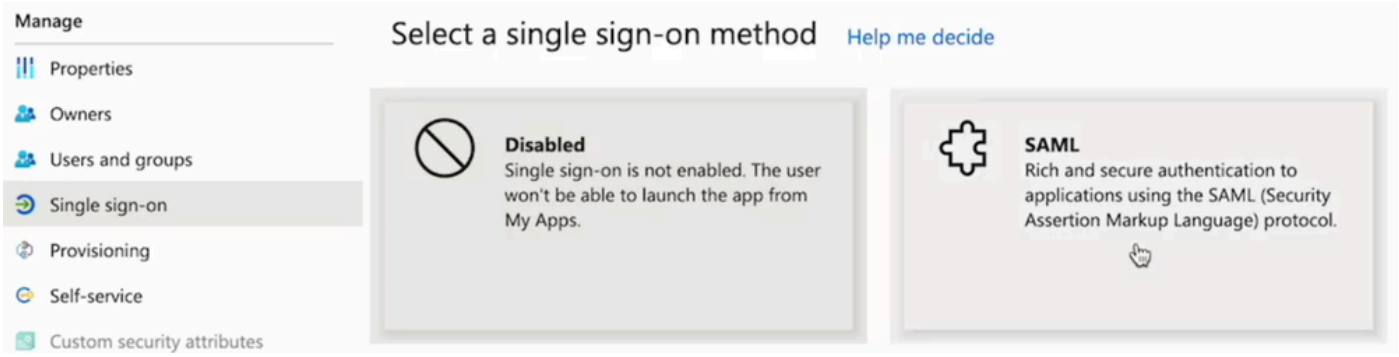
浏览Microsoft Entra库

2.使用有意义的值命名它，然后单击Create。例如，CRES单点登录。



注意：要允许所有用户登录CRES门户，您需要在CRES Sign On(SAML toolkit)属性下手动禁用Required Assignment，对于Assignment Required，请选择No。

3.导航到左侧面板，在Manage部分下，单击Single sign-on，然后选择SAML。



4.在“基本SAML配置”面板中，单击编辑，然后按如下方式填写属性：

- 标识符（实体ID）：https://res.cisco.com/

- 回复URL（断言消费者服务URL）：https://res.cisco.com/websafe/ssourl
- 登录URL:https://res.cisco.com/websafe/ssourl
- 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。

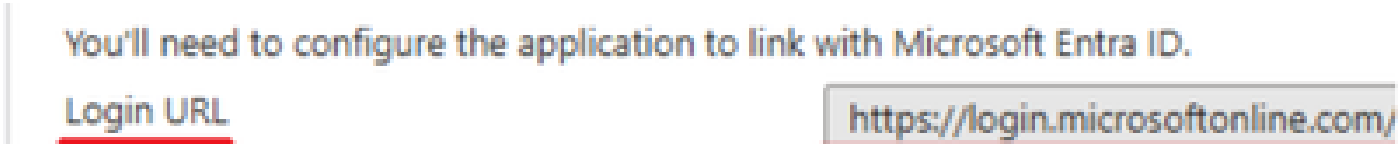
- 将Source 属性字段设置为user.userprincipalname。这假定user.userprincipalname的值代表有效的邮件地址。否则，请将Source设置为user.primaryauthoritiveemail。
- 在Additional Claims面板下，单击Edit并创建Microsoft Entra ID用户属性和SAML属性之间的映射。

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。按照CRES门户中的要求保存下一个值:

- 保存登录URL。



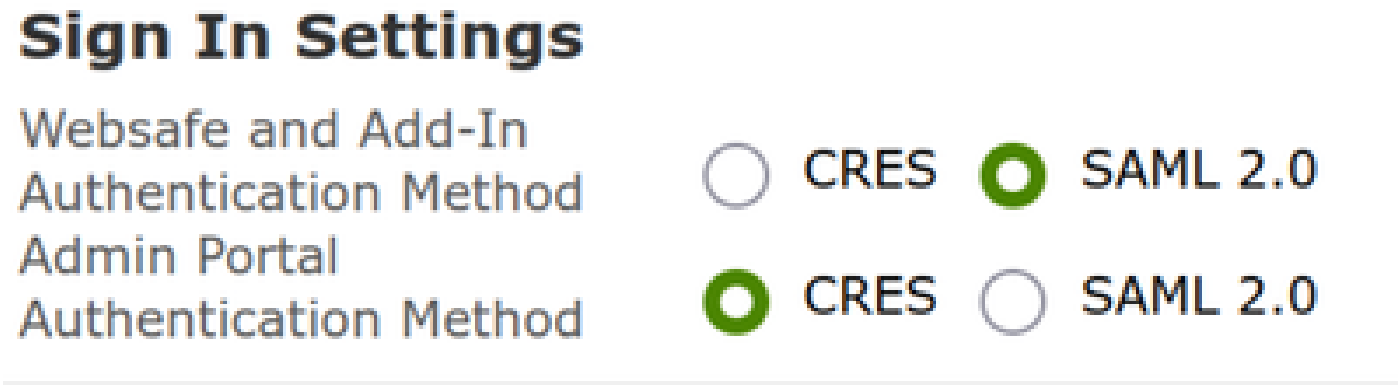
- 选择Certificate(Base64)Download链接。

思科邮件加密服务

1.以管理员身份登录到安全邮件加密服务组织门户。

2.在Accounts选项卡上，选择Manage Accounts选项卡，然后单击Account Number。

3.在Details选项卡中，滚动到Authentication Method并选择SAML 2.0。



4. — 填写属性，如下所示：

- SSO备用电子邮件属性名称：电邮地址
- SSO服务提供商实体ID*:https://res.cisco.com/
- SSO客户服务URL*:此链接由Entra ID提供，位于
- SSO注销URL:留空

5. — 单击激活SAML。

验证

系统将显示一个新窗口，确认在成功登录后启用了SAML身份验证。单击下一步。它会将您重定向到身份提供程序的登录页。使用您的SSO凭据登录。成功登录后，可以关闭窗口。Click Save.

故障排除

如果窗口未将您重定向到身份提供程序的登录页，则会返回一个回溯，为您提供错误。请复查属性和声明，确保它配置有与CRES身份验证方法部分相同的名称。SAML登录中使用的用户电子邮件地址必须与CRES中的电子邮件地址匹配。请勿使用别名。

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）。