使用思科安全云登录（思科SCSO）安全恶意软件分析登录 — 如何链接帐户

目录

简介

- 链接现有用户
- 创建新的SMA用户
- 多个安全恶意软件分析帐户链接到单个SCSO帐户
- 仅用于SCSO的集成登录
- 支持

简介

本文档概述安全恶意软件分析(SMA)如何过渡到安全云登录(SCSO)，作为所有用户的独占身份验证方法。此更改旨在跨思科安全产品提供集中且一致的登录体验。

它解释了此过渡引入的更新，并指导用户如何将其SCSO帐户链接到安全恶意软件分析。此功能将于2026年2月24日起提供。

在此日期之后，将不再支持使用本地SMA用户名和密码进行身份验证。

注意：

此更改仅适用于安全恶意软件分析(SMA)云服务。安全恶意软件分析设备的身份验证保持不变。

API身份验证也保持不变。

安全云登录(SCSO)

思科安全云登录是一项集中式身份管理服务，旨在跨各种思科安全应用提供统一且高度安全的登录体验。单个SCSO帐户可用于访问多个思科安全服务。

所有用户必须拥有已注册的Cisco SCSO帐户才能访问安全恶意软件分析。

要注册思科SCSO，请导航至：https://sign-on.security.cisco.com/signin/register

链接现有用户

如果现有安全恶意软件分析(SMA)帐户在仅SCSO登录功能于2026年2月24日生效之前尚未链接到安全云登录(SCSO)，请完成以下步骤以链接这些帐户。

前提条件

需要注册的安全云登录(SCSO)帐户。

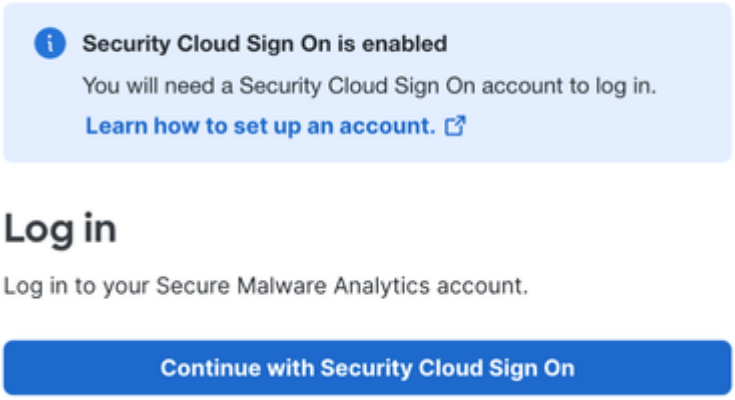
如果尚未创建SCSO帐户，请在以下位置注册：https://sign-on.security.cisco.com/signin/register

步骤

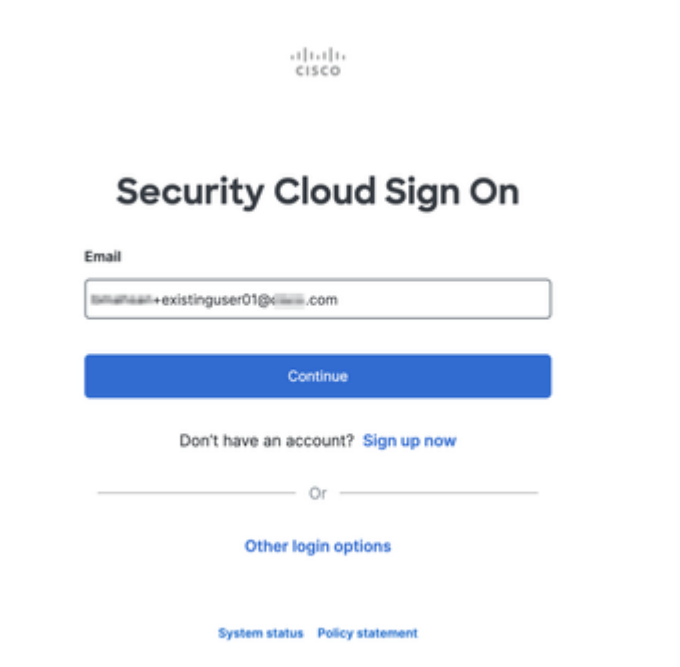
导航到相应的安全恶意软件分析门户：

- 美国 — https://panacea.threatgrid.com
- 欧盟 — https://panacea.threatgrid.eu
- 澳大利亚 — https://panacea.threatgrid.com.au
- 加拿大 — https://panacea.threatgrid.ca
- 印度 — https://panacea.threatgrid.in

在登录屏幕上，选择Continue with Security Cloud Sign On以使用SCSO登录。



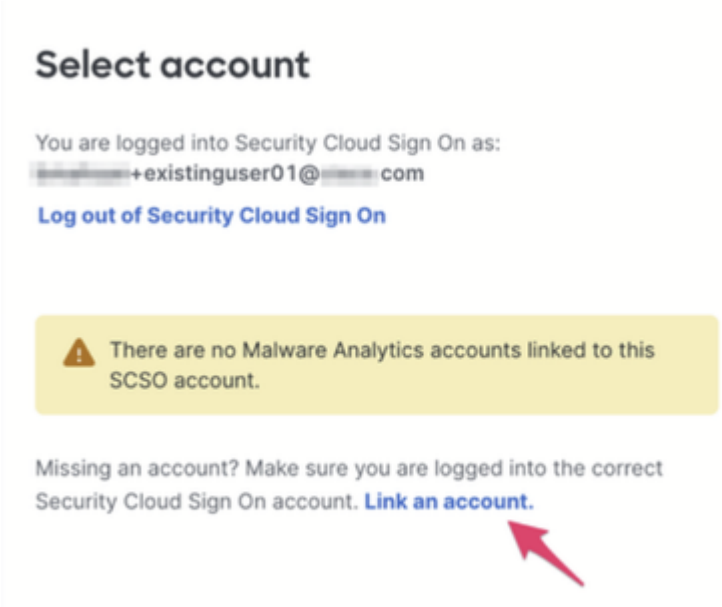
使用先前创建的帐户登录到安全云登录(SCSO)。



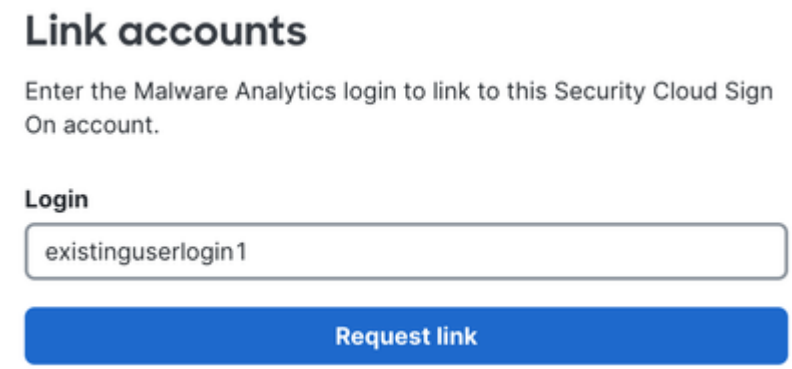
身份验证成功后，出现一条消息“没有恶意软件分析帐户链接到此SCSO帐户”。 以及链接帐户的选

项。

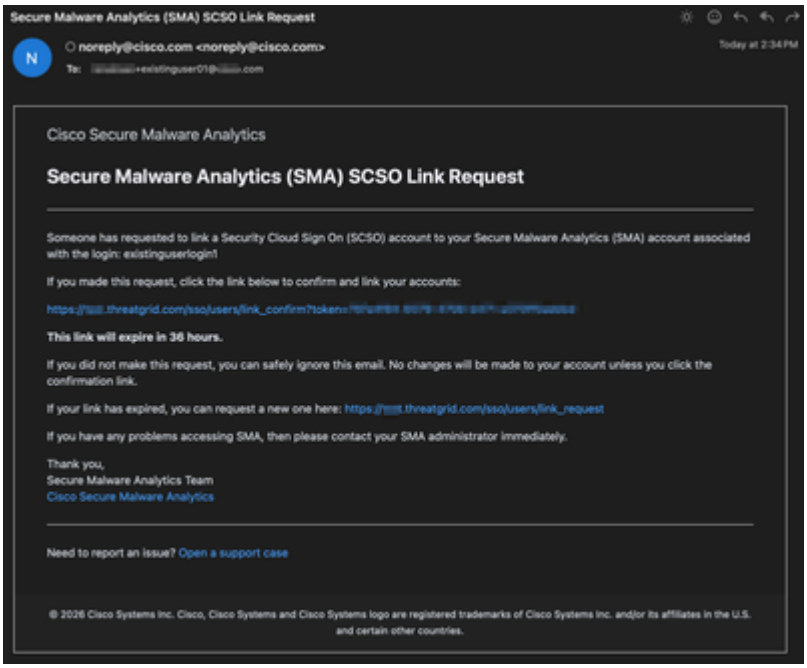
选择链接帐户，开始将现有安全恶意软件分析(SMA)帐户链接到SCSO帐户。



在下一页上，将显示链接帐户的选项。输入现有的Login并选择Request链接。

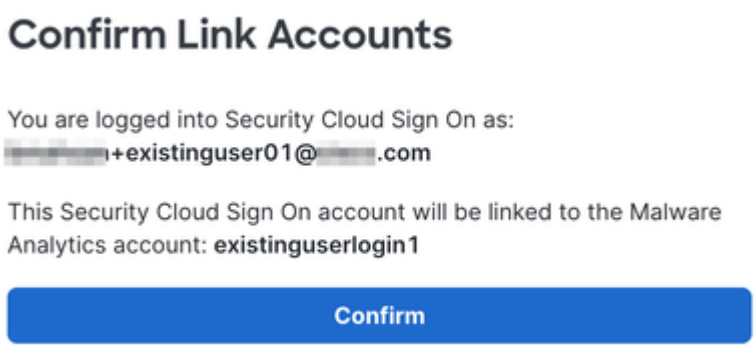


系统会向与现有SMA帐户关联的电子邮件地址发送一封邀请邮件。
在大多数情况下，此电子邮件地址与SCSO帐户电子邮件地址匹配。如果必须更新电子邮件地址，请联系组织管理员或思科支持部门。

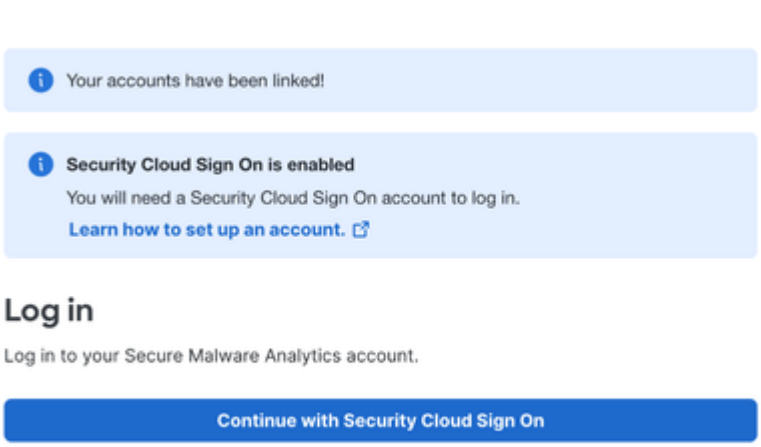


在浏览器中打开邀请邮件中提供的URL。身份验证成功后，系统将提示用户确认帐户链接。

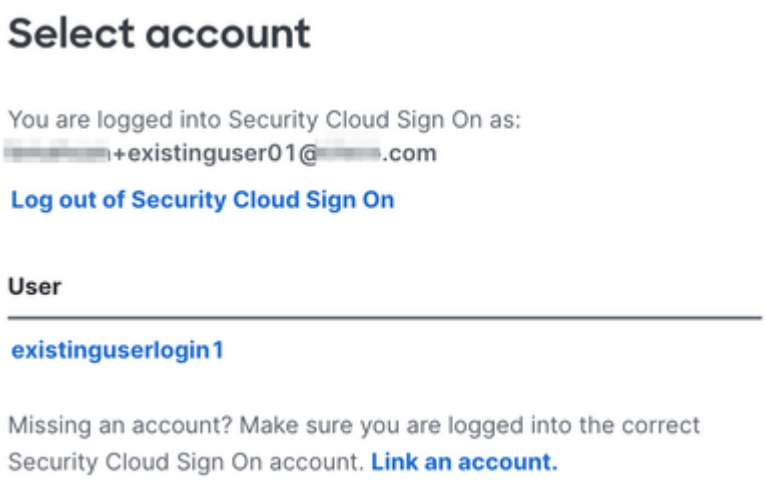
验证帐户详细信息并选择Confirm。



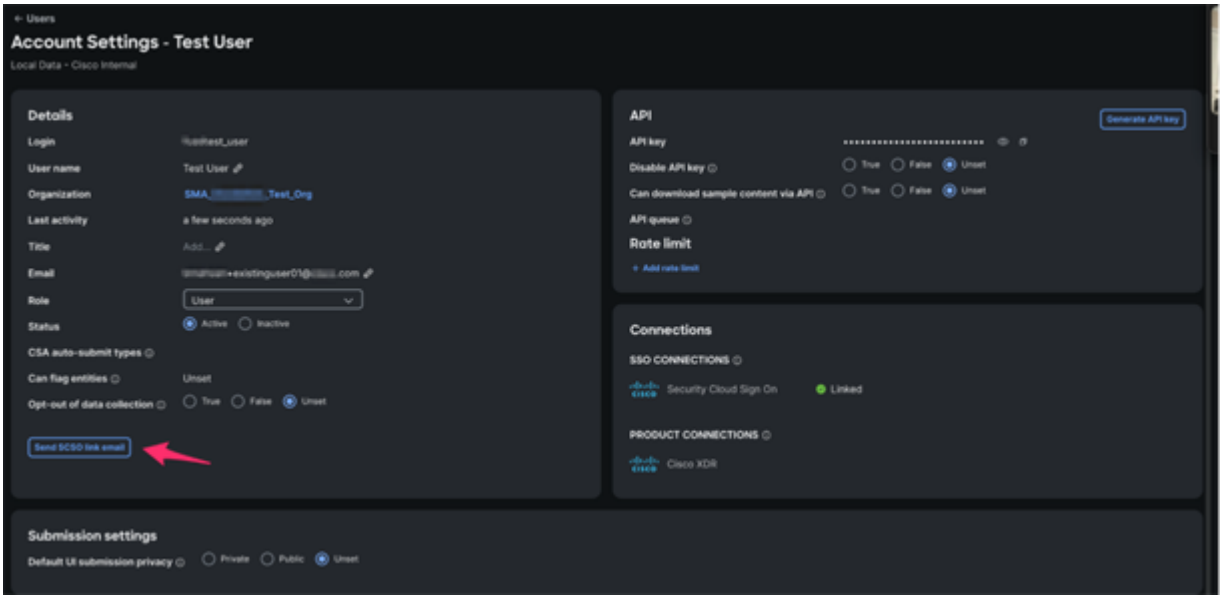
系统将显示确认消息，指示帐户已链接。选择Continue with Security Cloud Sign On以使用SCSO登录到现有安全恶意软件分析帐户。



在下一页上，选择要登录到的用户帐户。



注意：组织管理员还可以从“用户管理”(User Management)页面发送SCSO帐户链接邀请邮件。



创建新的SMA用户

在安全恶意软件分析中创建新用户的流程保持不变，包括在用户创建后自动发送帐户链接邀请电子邮件。

创建新用户：

1.以组织管理员身份登录安全恶意软件分析。

2.定位至管理>用户>新用户。

3.输入所需信息：

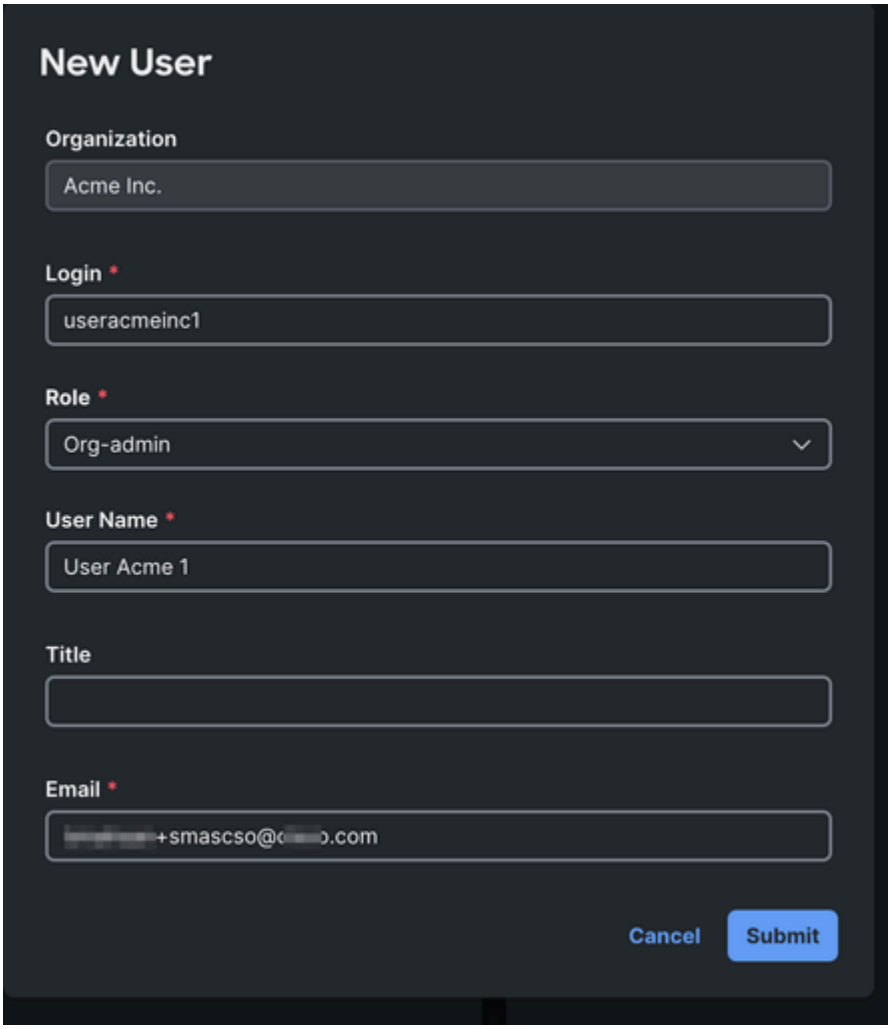
-登录

— 角色

-用户名

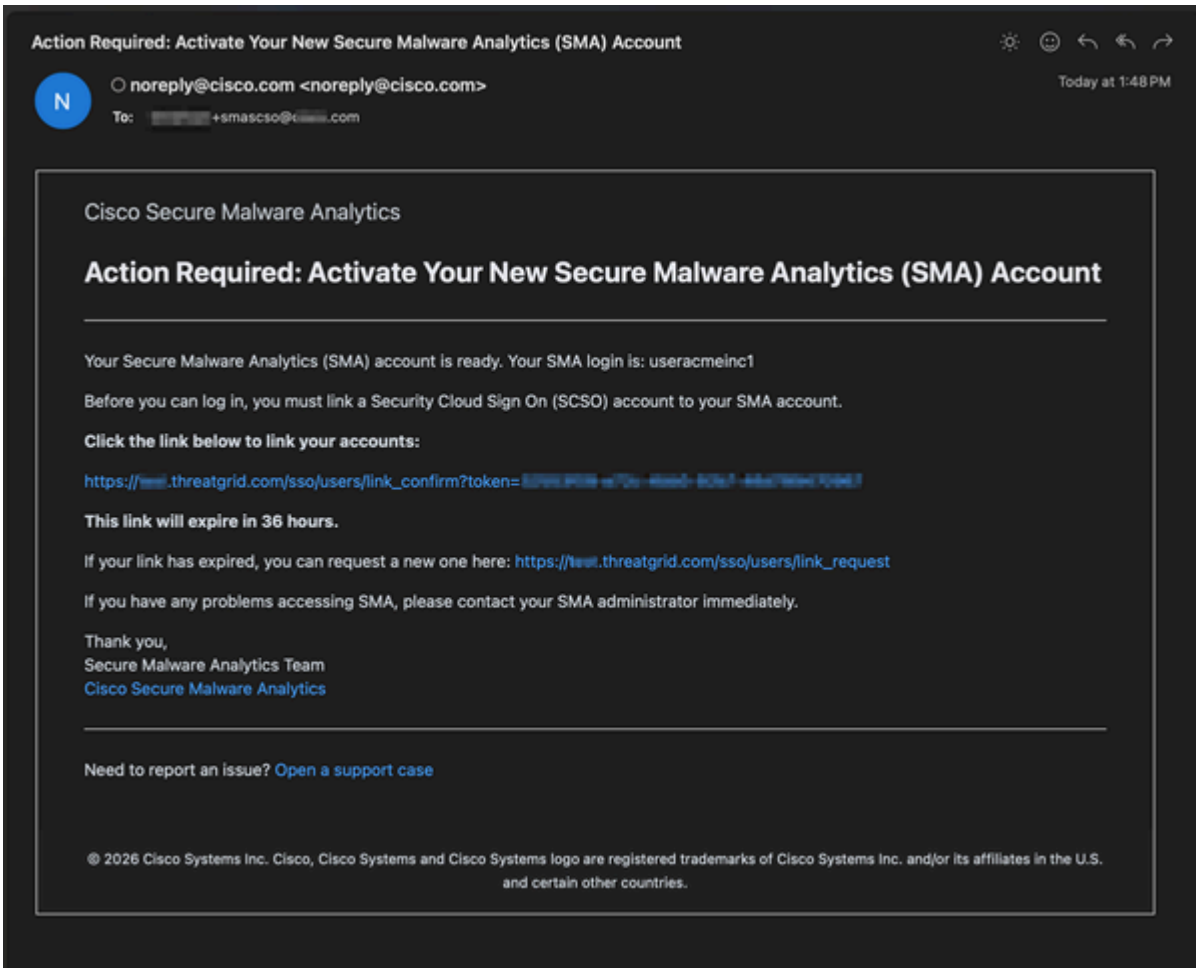
- 电子邮件地址

4.单击提交。



将新用户帐户链接到SCSO帐户：

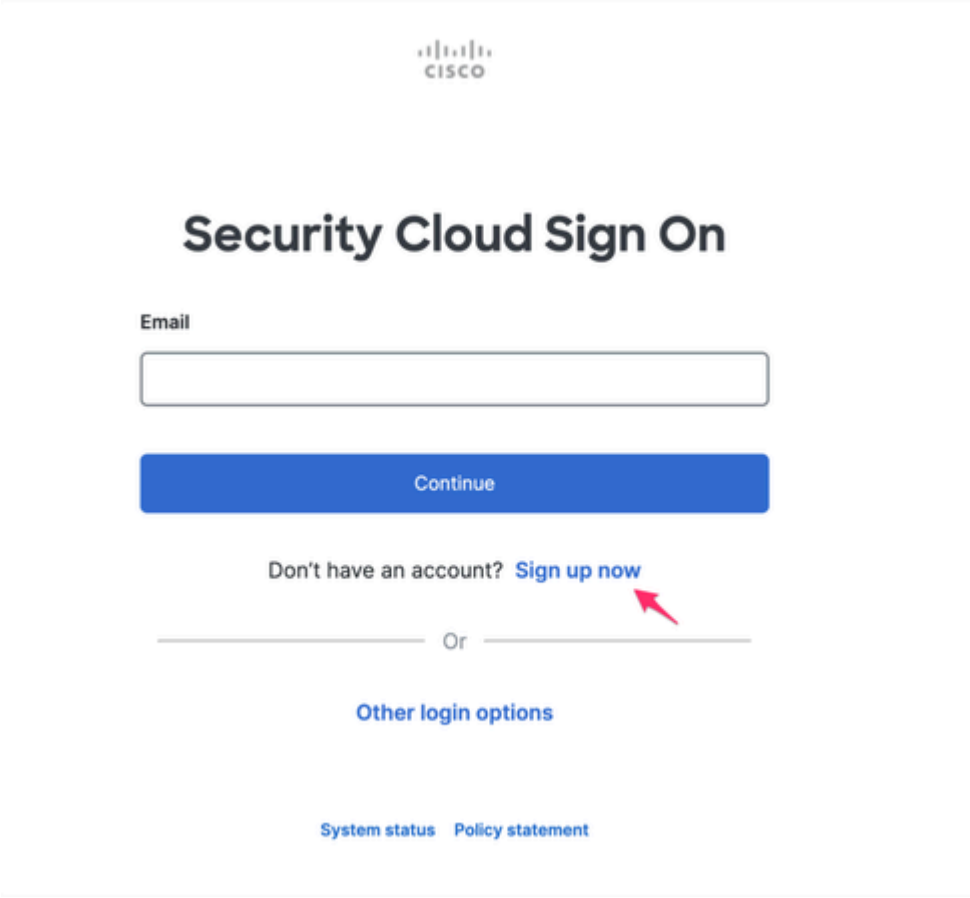
创建用户帐户，并将标题为“安全恶意软件分析(SMA)SCSO链接请求”(Secure Malware Analytics(SMA)SCSO Link Request)的邀请邮件从noreply@cisco.com发送到用户的邮件地址。



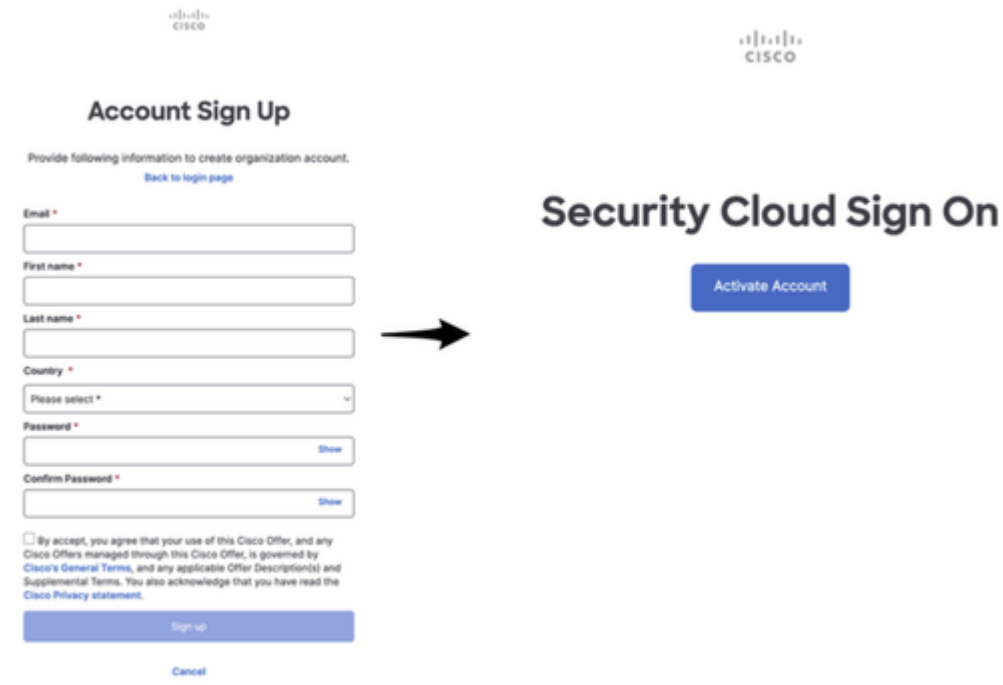
当用户点击该URL或在浏览器中打开该URL时，用户将被重定向到安全云登录(SCSO)登录页面。

如果用户已注册SCSO帐户，则他们使用已注册的电邮地址进行身份验证，并链接其SMA帐户。

如果用户没有SCSO帐户，则选择Sign up now开始注册过程。

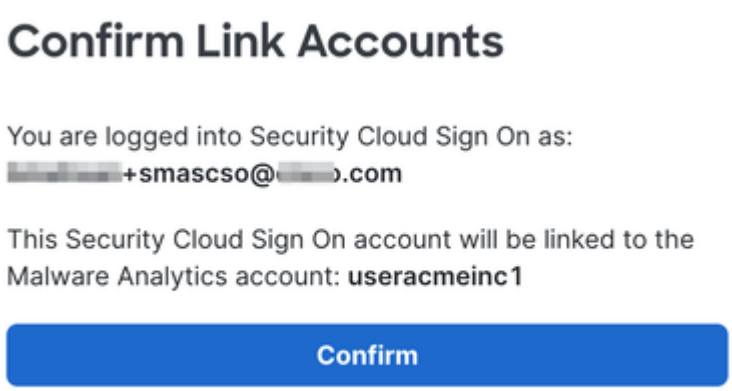


输入要注册SCSO帐户的帐户信息。用户收到一封邮件，用于激活新的SCSO帐户。按照邮件中的说明激活帐户并启用多重身份验证。

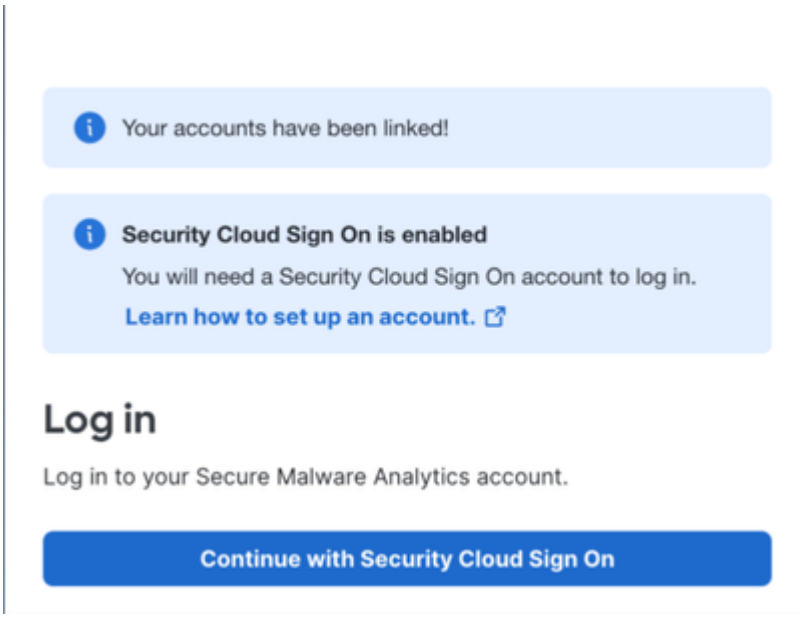


用户成功注册SCSO帐户后，返回之前收到的Secure Malware Analytics(SMA)SCSO Link Request邮件，并在浏览器中打开URL。

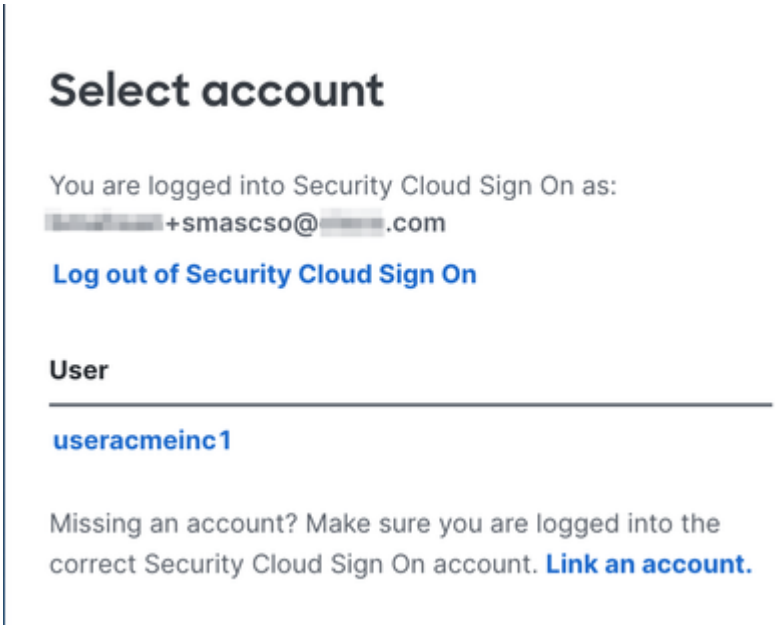
身份验证成功后，用户将可以选择将SMA帐户与已登录SCSO帐户关联。



确认操作。系统将显示一条“您的帐户已链接”的成功消息。选择Continue with Security Cloud Sign On以登录到安全恶意软件分析(SMA)帐户，并接受最终用户许可协议(EULA)以完成帐户设置。



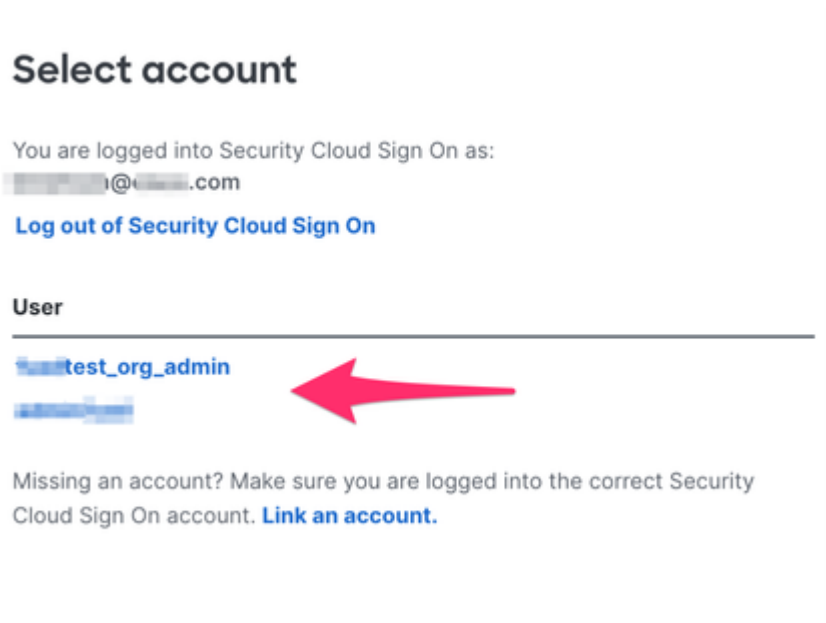
在下一页上，选择要登录到的用户帐户。



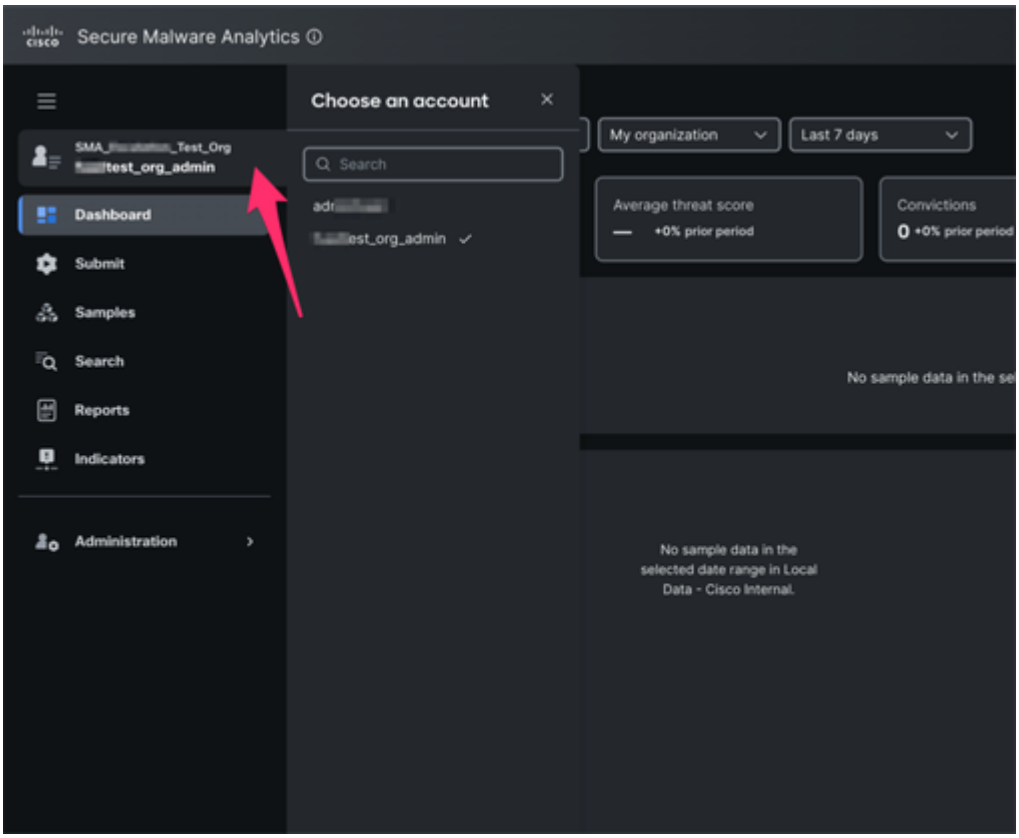
多个安全恶意软件分析帐户链接到单个SCSO帐户

用户可以使用创建新SMA用户或链接现有用户方法将多个安全恶意软件分析(SMA)帐户链接到同一安全云登录(SCSO)帐户。

在成功进行SCSO身份验证后，用户会看到一个选项，可选择要访问的Secure Malware Analytics帐户。



用户还可以使用左侧导航中的菜单登录后在帐户之间切换。



仅用于SCSO的集成登录

Umbrella　SIG、安全访问、Meraki和邮件威胁防御(ETD)等集成会在向安全恶意软件分析注册时自动调配组织管理员或设备管理员帐户。

邀请电邮发送到集成设备或服务提供的电邮地址，以使用安全云登录(SCSO)完成帐户链接。

支持

有关Duo Mobile双因素身份验证问题，请查看 — Reset Duo Mobile on Security Cloud Sign-On并添加其他身份验证设备文档。

安全云登录文档-

如需帮助或更多信息，请联系思科技术支持中心(TAC)。

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）。