

# 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

[创建新的SMA用户](#)

[链接现有用户](#)

[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

本文档介绍安全恶意软件分析(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。

本文档介绍此过渡引入的更改，并解释用户如何可以将其SCSO帐户链接到安全恶意软件分析。此功能将于2026年2月19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。

### 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>

### 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。

**New User**

Active User Quota: 4/10 ⓘ

Organization

SMA [REDACTED] Test\_Org

Login \*

test\_user04

Role \*

User

User Name \*

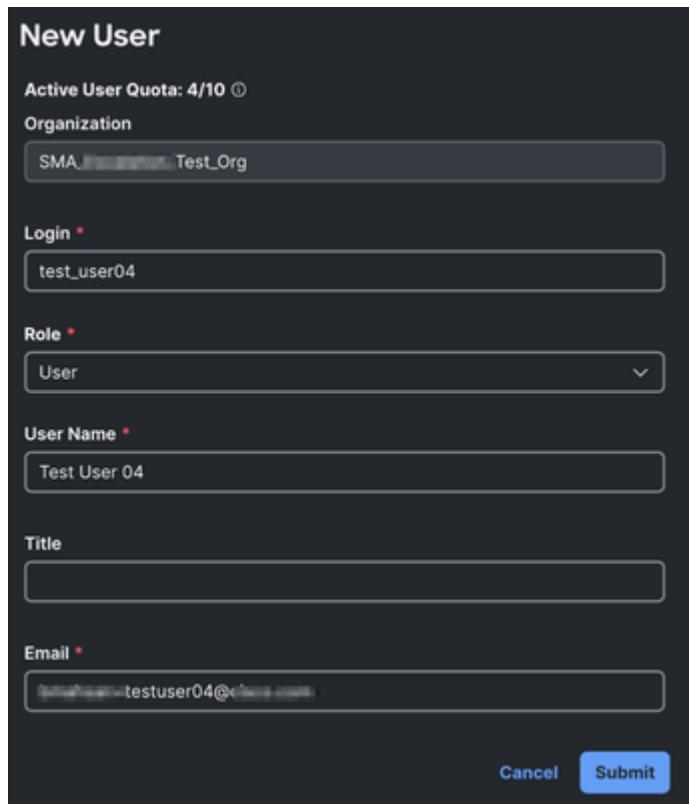
Test User 04

Title

Email \*

[REDACTED] testuser04@cisco.com

[Cancel](#) [Submit](#)



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。

Secure Malware Analytics (SMA) SCSO Link Request

N

○ noreply@cisco.com <noreply@cisco.com>

To: [REDACTED] testuser04@[REDACTED]

Today at 10:32 AM

Cisco Secure Malware Analytics

## Secure Malware Analytics (SMA) SCSO Link Request

Someone has requested to link a Security Cloud Sign On account to your Malware Analytics account with the login: test\_user04

If this was you, then please open the following URL in your browser:

[https://\[REDACTED\].threatgrid.com/sso/users/link\\_confirm?token=\[REDACTED\]](https://[REDACTED].threatgrid.com/sso/users/link_confirm?token=[REDACTED])

This will link the accounts.

THIS TOKEN WILL EXPIRE IN 36 HOURS

If your token has expired, please request a new token by opening the following URL in your browser: [Link Request Link](#)

If you have any problems accessing SMA, then please contact your SMA administrator immediately.

Thank you,  
Secure Malware Analytics Team  
Cisco Secure Malware Analytics

---

Need to report an issue? [Open a support case](#)

© 2026 Cisco Systems Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems Inc. and/or its affiliates in the U.S. and certain other countries.

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子邮件地址进行身份验证，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。

## Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)



Or

[Other login options](#)

[System status](#) [Policy statement](#)

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。

### Account Sign Up

Provide following information to create organization account.

[Back to login page](#)

Email \*

First name \*

Last name \*

Country \*

Password \*  [Show](#)

Confirm Password \*  [Show](#)

By accept, you agree that your use of this Cisco Offer, and any Cisco Offers managed through this Cisco Offer, is governed by Cisco's General Terms, and any applicable Offer Description(s) and Supplemental Terms. You also acknowledge that you have read the Cisco Privacy statement.

[Sign up](#)

Cancel

## Security Cloud Sign On

[Activate Account](#)



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。

## Confirm Link Accounts

You are logged into Security Cloud Sign On as:

████████+testuser04@████████.com

This Security Cloud Sign On account will be linked to the Malware Analytics account: test\_user04

**Confirm**

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。

**i** Your accounts have been linked!

**i** Security Cloud Sign On is enabled

You will need a Security Cloud Sign On account to log in.

[Learn how to set up an account.](#)

## Log in

Log in to your Secure Malware Analytics account.

**Continue with Security Cloud Sign On**

## 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19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。

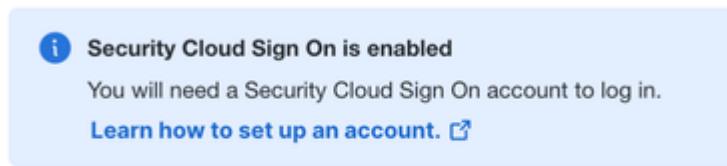
如果尚未创建SCSO帐户，请在以下位置注册：<https://sign-on.security.cisco.com/signin/register>

## 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>

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

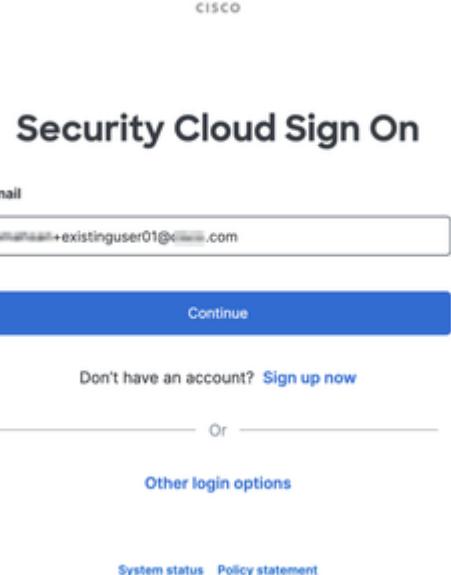


## Log in

Log in to your Secure Malware Analytics account.

[Continue with Security Cloud Sign On](#)

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。

## Select account

You are logged into Security Cloud Sign On as:

████████+existinguser01@████.com

[Log out of Security Cloud Sign On](#)

 There are no Malware Analytics accounts linked to this SCSO account.

Missing an account? Make sure you are logged into the correct Security Cloud Sign On account. [Link an account.](#)



在下一页上，将显示链接帐户的选项。输入现有用户名并选择请求链接。

### Link accounts

Enter the Malware Analytics username to link to this Security Cloud Sign On account.

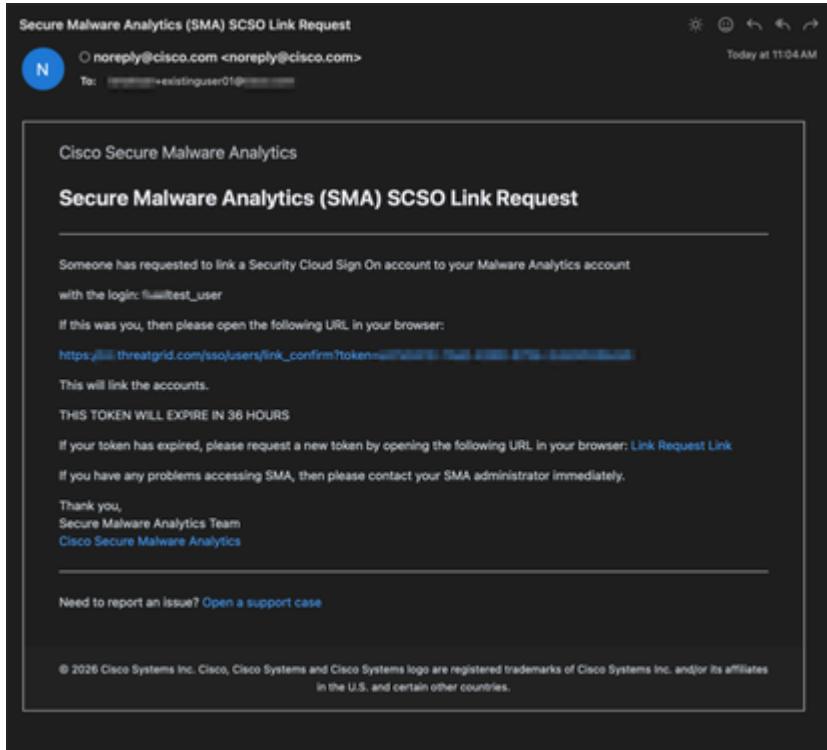
Username

[Request link](#)



系统会将邀请邮件发送到为现有帐户配置的邮件地址。

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。

## Confirm Link Accounts

You are logged into Security Cloud Sign On as: [REDACTED]+existinguser01@[REDACTED].com

This Security Cloud Sign On account will be linked to the Malware Analytics account:  
[REDACTED]test\_user

**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。

**i** Your accounts have been linked!

**i** Security Cloud Sign On is enabled

You will need a Security Cloud Sign On account to log in.

[Learn how to set up an account.](#)

## Log in

Log in to your Secure Malware Analytics account.

**Continue with Security Cloud Sign On**

在下一页上，选择要登录到的用户帐户。

## Select account

You are logged into Security Cloud Sign On as:

\*\*\*\*\*+existinguser01@\*\*\*\*\*.com

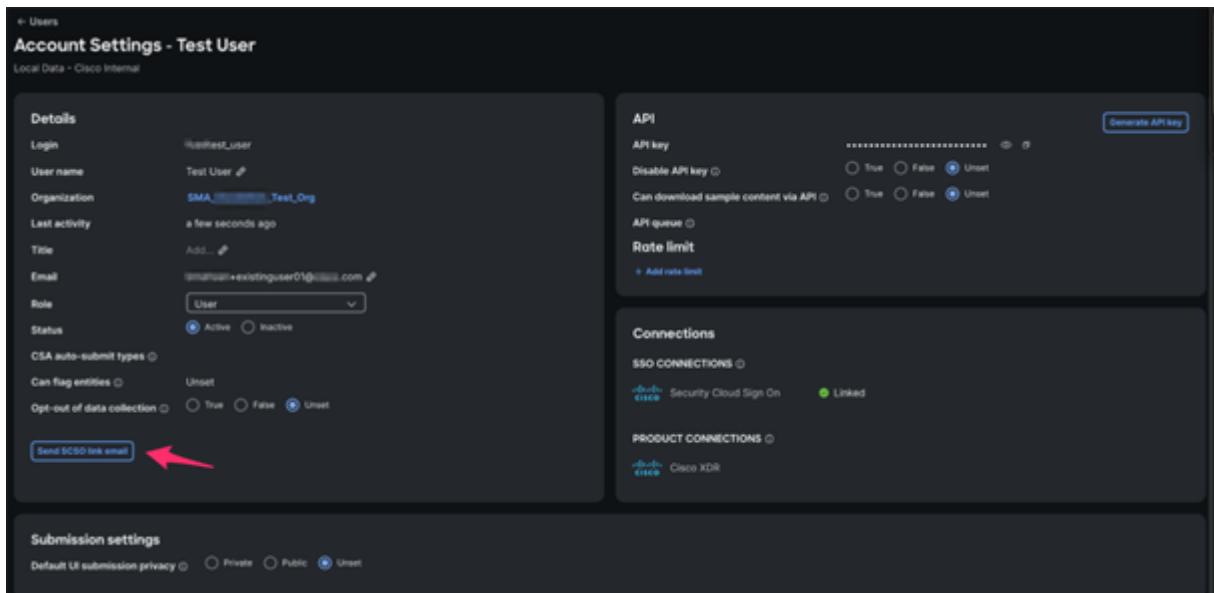
[Log out of Security Cloud Sign On](#)

User

Test\_user

Missing an account? Make sure you are logged into the correct Security Cloud Sign On account. [Link an account](#).

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。



The screenshot shows the 'Account Settings - Test User' page. The 'Details' section includes fields for Login (TestedUser), User name (Test User), Organization (SMA\_\*\*\*\*\*\_Test\_Org), Last activity (a few seconds ago), Title (Add...), Email (\*\*\*\*\*+existinguser01@\*\*\*\*\*.com), Role (User), Status (Active), and several checkboxes for CSA auto-submit types, Can flag entities, and Opt-out of data collection. The 'API' section contains fields for API key, Disable API key, Can download sample content via API, and Rate limit. The 'Connections' section shows SSO CONNECTIONS (Security Cloud Sign On, Linked) and PRODUCT CONNECTIONS (Cisco XDR). At the bottom, there are 'Submission settings' with a 'Default UI submission privacy' dropdown set to 'Unset'. A red arrow points to the 'Send SCSO link email' button in the 'Details' section.

## 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。

## Select account

You are logged into Security Cloud Sign On as:

100@.com

[Log out of Security Cloud Sign On](#)

## User

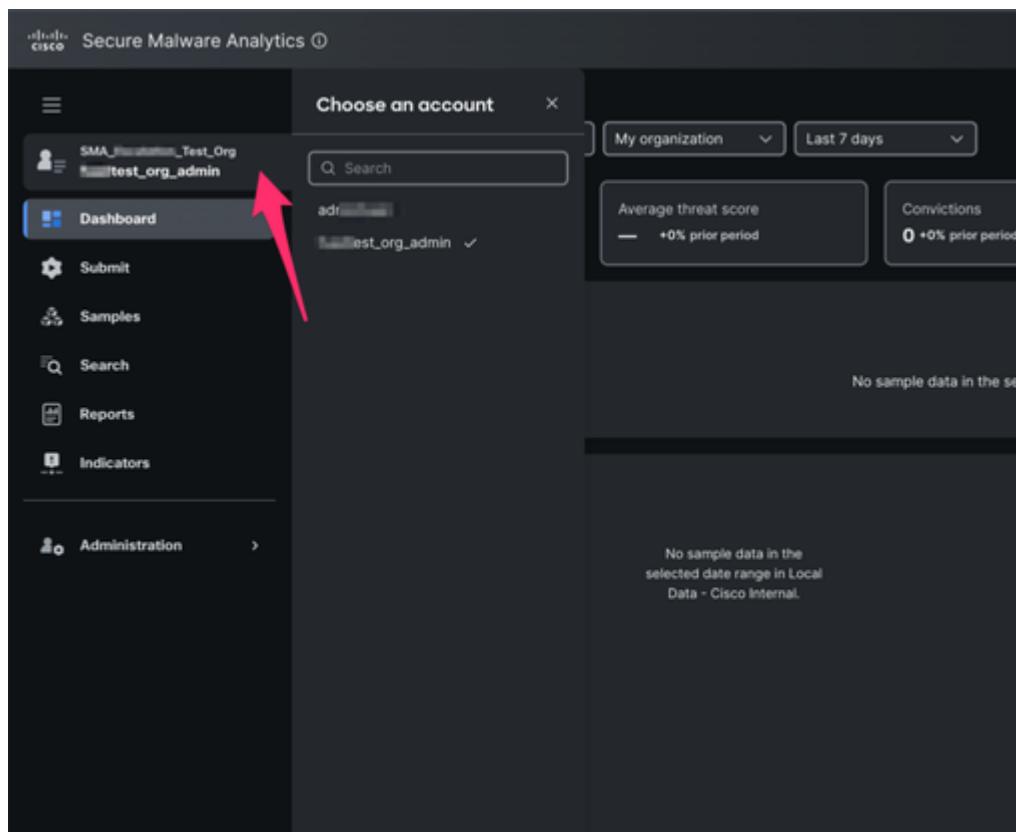
test\_org\_admin

10 of 10



Missing an account? Make sure you are logged into the correct Security Cloud Sign On account. [Link an account.](#)

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

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）。