

Secure Malware Analytics Login with Cisco Security Cloud Sign-On (Cisco SCSO) - How to link Accounts

Contents

Introduction

[Creating New SMA User](#)

[Link Existing User](#)

[Multiple Secure Malware Analytics accounts linked to single SCSO account](#)

[SCSO-only login for Integration](#)

[Support](#)

Introduction

This document describes how Secure Malware Analytics (SMA) will transition to **Security Cloud Sign On (SCSO)** as the exclusive authentication method for all users. This change is intended to provide a centralized and consistent login experience across Cisco Security products.

This document describes the changes introduced by this transition and explains how users can link their SCSO account to Secure Malware Analytics. This feature will be available beginning **February 19, 2026**.

After this date, authentication using native SMA usernames and passwords will no longer be supported.

Security Cloud Sign On (SCSO)

Cisco Security Cloud Sign-On is a centralized identity management service designed to provide a unified and highly secure login experience across various Cisco Security applications. A single SCSO account can be used to access multiple Cisco Security services.

All users must have a registered Cisco SCSO account to access Secure Malware Analytics.

To register for Cisco SCSO, navigate to: <https://sign-on.security.cisco.com/signin/register>

Creating New SMA User

The process for creating a new user in Secure Malware Analytics remains unchanged, including that an **account-linking invitation email** is sent automatically after user creation.

Create new user:

1. Log in to Secure Malware Analytics as an Organization Administrator.
2. Navigate to **Administration > Users > New User**.
3. Enter the required information:
 - Login

- Role
- User Name
- Email Address

4. Click Submit.

New User

Active User Quota: 4/10 ⓘ

Organization

SMA [REDACTED] Test_Org

Login *

test_user04

Role *

User

User Name *

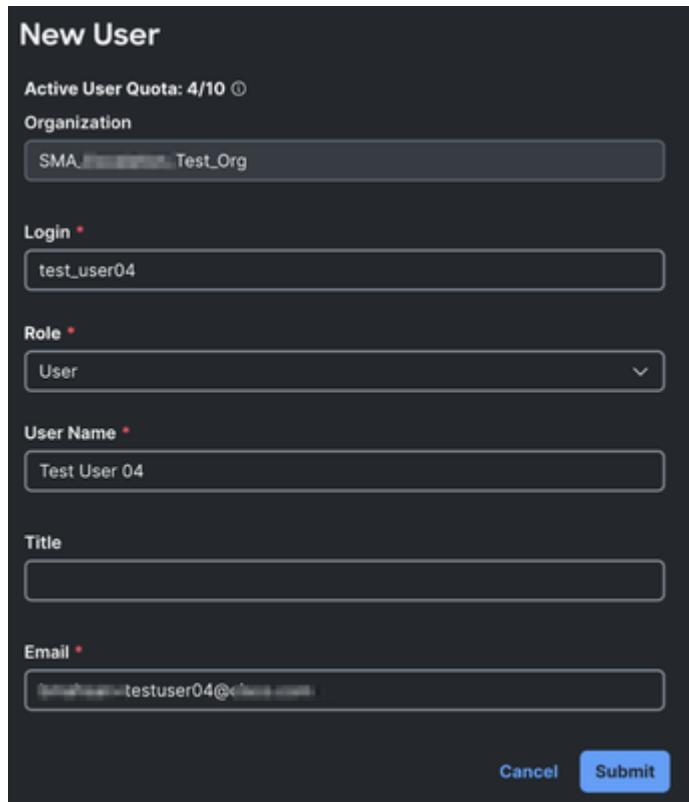
Test User 04

Title

Email *

[REDACTED] testuser04@cisco.com

Cancel Submit



Linking new user account to SCSO account:

The user account is created, and an invitation email titled **“Secure Malware Analytics (SMA) SCSO Link Request”** is sent from **noreply@cisco.com** to the user’s email address.

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.

When user click on the URL or open it in their browser, user will be redirected to Security Cloud Sign On (SCSO) login page.

If the user has already signed up for SCSO account, they authenticate using their registered email address and link their SMA account.

If the user does not have an SCSO account, they select **Sign up now** to start the registration process.

Security Cloud Sign On

Email

Continue

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



Or

[Other login options](#)

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

Enter account information to sign up for an SCSO account. The user receives an email to activate the new SCSO account. Follow the instructions in the email to **Activate the account** and **enable multi-factor authentication**.

Account Sign Up

Provide following information to create organization account.

[Back to login page](#)

Email *

First name *

Last name *

Country *

Please select *

Password *

Show

Confirm Password *

Show



Security Cloud Sign On

Activate Account

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](#)

Once the user has successfully signed up for an SCSO account, return to the previously received **Secure Malware Analytics (SMA) SCSO Link Request** email and open the URL in a browser.

After successful authentication, the user is presented with the option to link the SMA account with the signed-in SCSO account.

Confirm Link Accounts

You are logged into Security Cloud Sign On as:

testuser04@company.com

This Security Cloud Sign On account will be linked to the Malware Analytics account: **test_user04**

Confirm

Confirm the action. A success message stating “**Your accounts have been linked**” is displayed. Select **Continue with Security Cloud Sign On** to log in to the Secure Malware Analytics (SMA) account, and accept the End User License Agreement (EULA) to complete account setup.

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

Link Existing User

If an existing Secure Malware Analytics (SMA) account has not been linked to Security Cloud Sign On (SCSO) before the SCSO-only login feature becomes effective on **February 19, 2026**, complete the following procedure to link the accounts.

Prerequisite

A registered Security Cloud Sign On (SCSO) account is required.

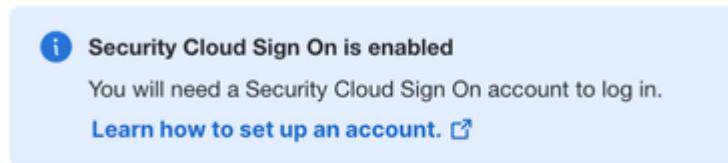
If an SCSO account has not been created, register at: <https://sign-on.security.cisco.com/signin/register>

Procedure

Navigate to the appropriate Secure Malware Analytics portal:

- US - <https://panacea.threatgrid.com>
- EU - <https://panacea.threatgrid.eu>
- Australia - <https://panacea.threatgrid.com.au>
- Canada - <https://panacea.threatgrid.ca>

On the login screen, select **Continue with Security Cloud Sign On** to log in using SCSO.

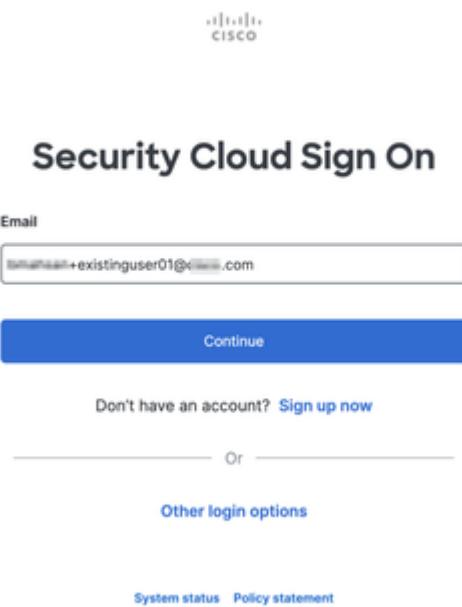


Log in

Log in to your Secure Malware Analytics account.

[Continue with Security Cloud Sign On](#)

Log in to **Security Cloud Sign On (SCSO)** using the account that was previously created.



After successful authentication, a message stating **“There are no Malware Analytics accounts linked to this SCSO account.”** is displayed, along with the option to **link an account**.

Select **Link an account** to begin linking the existing Secure Malware Analytics (SMA) account to the

SCSO account.

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.](#)



On the next page, an option to link accounts is displayed. Enter the existing **Username** and select **Request link**.

Link accounts

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

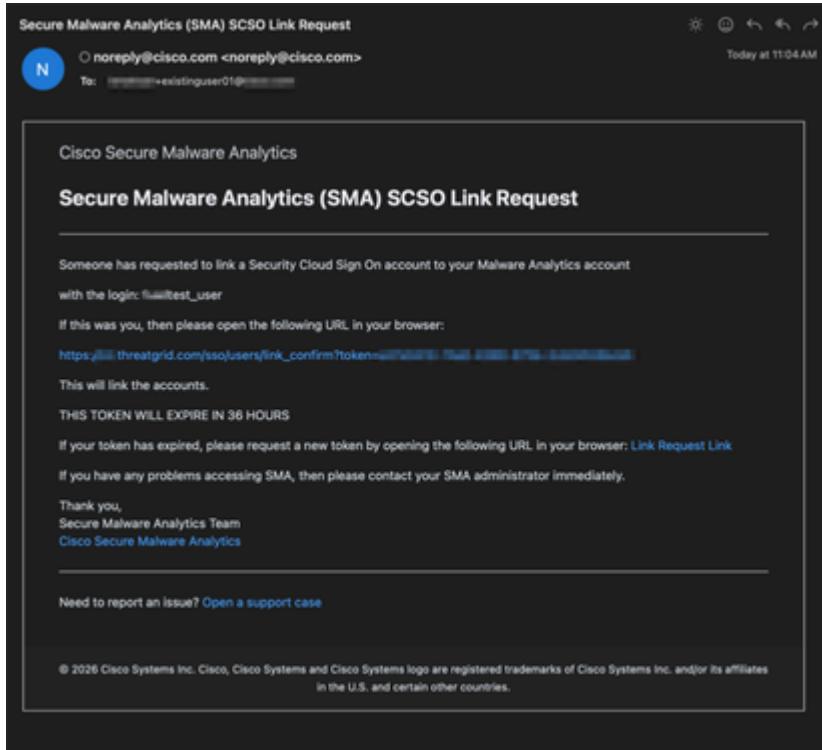
Username

[Request link](#)



An **invitation email** is sent to the email address configured for the existing account.

In most cases, this email address matches the SCSO account email address. If the email address must be updated, contact the Organization Administrator or Cisco Support.



Open the **URL** provided in the invitation email in a browser. After successful authentication, the user is prompted to confirm account linking.

Verify the account details and select **Confirm**.

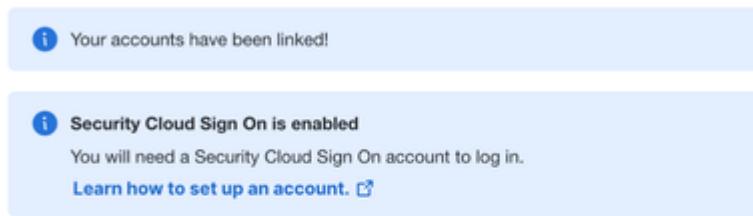
Confirm Link Accounts

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

A confirmation message is displayed indicating that the accounts have been linked. Select **Continue with Security Cloud Sign On** to log in to the existing Secure Malware Analytics account using SCSO.



Log in

Log in to your Secure Malware Analytics account.

Continue with Security Cloud Sign On

On the next page, **select the user** account to log in to.

Select account

You are logged into Security Cloud Sign On as:

existinguser01@.com

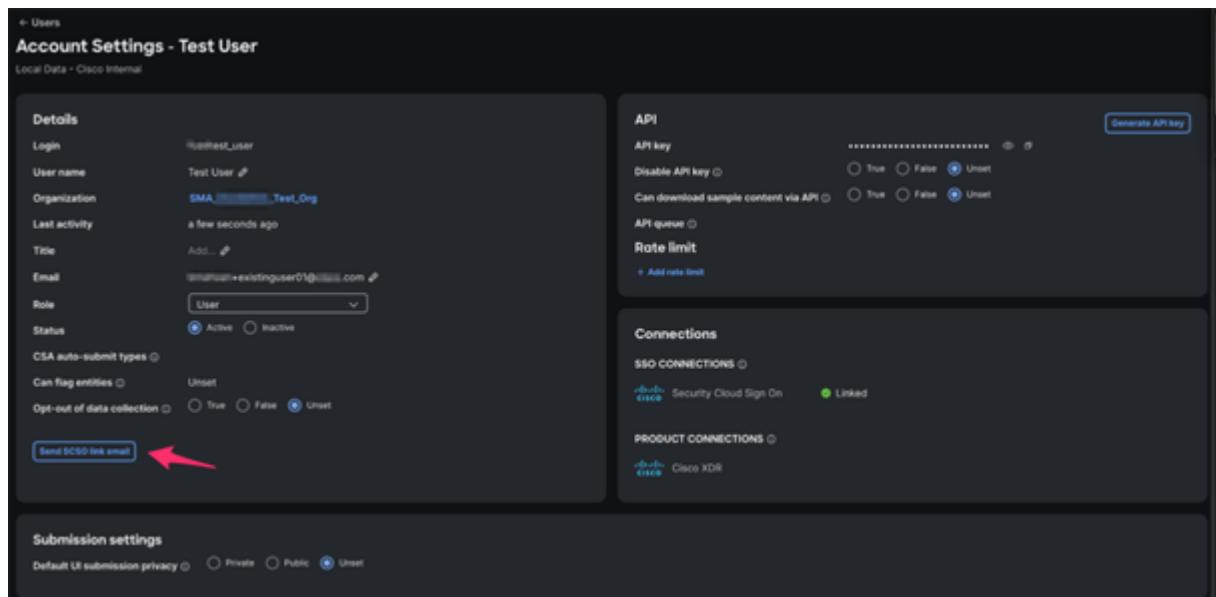
[Log out of Security Cloud Sign On](#)

User

test_user

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

Note: Organization Administrators can also send the SCSO account linking invitation email from the User Management page.



The screenshot shows the 'Account Settings - Test User' page. The left sidebar contains 'Details' with fields like Login (test_user), User name (Test User), Organization (SMA_Test_Org), and Email (existinguser01@.com). The right sidebar contains 'API' settings with 'Generate API key' and 'Connections' showing 'SSO CONNECTIONS' (Security Cloud Sign On, Linked). A red arrow points to the 'Send SCSO link email' button in the bottom-left corner of the left sidebar.

Multiple Secure Malware Analytics accounts linked to single SCSO account

Users can link multiple Secure Malware Analytics (SMA) accounts to the same Security Cloud Sign On (SCSO) account using either the **Create New SMA User** or **Link an Existing User** method.

After successful SCSO authentication, the user is presented with an option to select the Secure Malware Analytics account to access.

Select account

You are logged into Security Cloud Sign On as:

[REDACTED]@[REDACTED].com

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

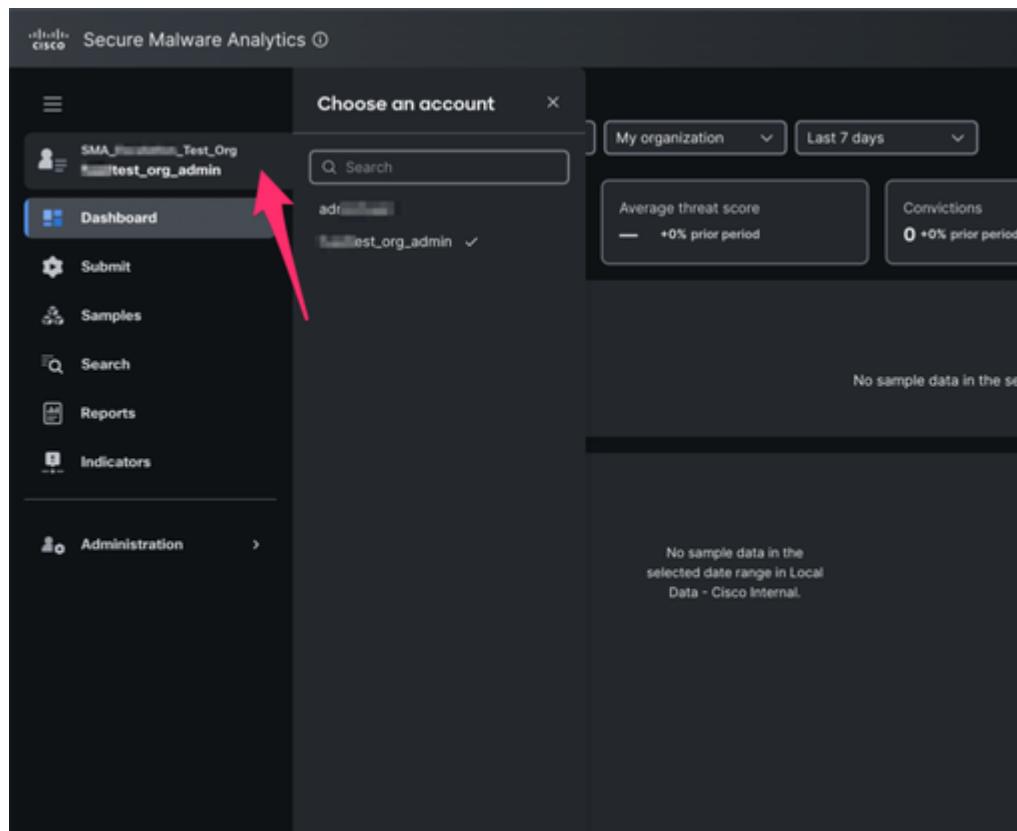
User

[REDACTED]test_org_admin



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

Users can also **switch between accounts** after logging in using the menu in the left-hand navigation.



The screenshot shows the Cisco Secure Malware Analytics interface. On the left, a vertical navigation menu lists 'Dashboard', 'Submit', 'Samples', 'Search', 'Reports', and 'Indicators'. A red arrow points to the 'Dashboard' item. In the center, a modal window titled 'Choose an account' is open. It displays a search bar with 'Search' placeholder text, a dropdown for 'My organization' set to 'Last 7 days', and two summary boxes: 'Average threat score' (unchanged from prior period) and 'Convictions' (unchanged from prior period). The main dashboard area shows a message: 'No sample data in the selected date range in Local Data - Cisco Internal.'

SCSO-only login for Integration

Integrations such as **Umbrella SIG**, **Secure Access**, **Meraki**, and **Email Threat Defense (ETD)** automatically provision either an **Organization Administrator** or **Device Administrator** account when they register with Secure Malware Analytics.

An invitation email is sent to the email address provided by the integrating device or service to complete account linking using Security Cloud Sign On (SCSO).

Support

For assistance or additional information, contact the [**Cisco Technical Assistance Center \(TAC\)**](#).