

Connexion à Secure Malware Analytics avec Cisco Security Cloud Sign-On (Cisco SCSO) - Comment lier des comptes

Table des matières

Introduction

[Création d'un utilisateur SMA](#)

[Lier un utilisateur existant](#)

[Plusieurs comptes Secure Malware Analytics liés à un seul compte SCSO](#)

[Connexion SCSO uniquement pour l'intégration](#)

[Soutien](#)

Introduction

Ce document décrit comment Secure Malware Analytics (SMA) passera à Security Cloud Sign On (SCSO) comme méthode d'authentification exclusive pour tous les utilisateurs. Cette modification vise à fournir une expérience de connexion centralisée et cohérente sur l'ensemble des produits de sécurité Cisco.

Ce document décrit les changements introduits par cette transition et explique comment les utilisateurs peuvent lier leur compte SCSO à Secure Malware Analytics. Cette fonctionnalité sera disponible à partir du 19 février 2026.

Après cette date, l'authentification utilisant des noms d'utilisateur et des mots de passe SMA natifs ne sera plus prise en charge.

Connexion au cloud de sécurité (SCSO)

Cisco Security Cloud Sign-On est un service de gestion centralisée des identités conçu pour offrir une expérience de connexion unifiée et hautement sécurisée à travers diverses applications de sécurité Cisco. Un seul compte SCSO peut être utilisé pour accéder à plusieurs services de sécurité Cisco.

Tous les utilisateurs doivent disposer d'un compte Cisco SCSO enregistré pour accéder à Secure Malware Analytics.

Pour vous inscrire à Cisco SCSO, accédez à : <https://sign-on.security.cisco.com/signin/register>

Création d'un utilisateur SMA

Le processus de création d'un nouvel utilisateur dans Secure Malware Analytics reste inchangé, notamment le fait qu'un e-mail d'invitation de liaison de compte est envoyé automatiquement

après la création de l'utilisateur.

Créer un nouvel utilisateur :

1. Connectez-vous à Secure Malware Analytics en tant qu'administrateur d'entreprise.

2. Accédez à Administration > Users > New User.

3. Saisissez les informations requises :

-Connexion

- Rôle

- Nom d'utilisateur

- Adresse e-mail

4. Cliquez sur Soumettre.

New User

Active User Quota: 4/10 ⓘ

Organization

SMA [REDACTED] Test_Org

Login *

test_user04

Role *

User

User Name *

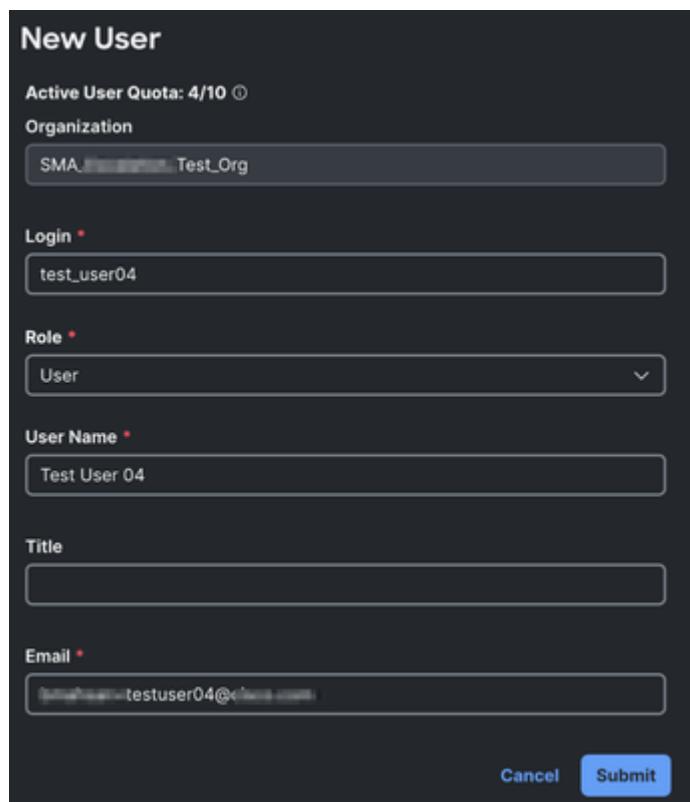
Test User 04

Title

Email *

testuser04@cisco.com

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



Liaison du nouveau compte utilisateur au compte SCSO :

Le compte utilisateur est créé et un e-mail d'invitation intitulé « Secure Malware Analytics (SMA) SCSO Link Request » est envoyé de noreply@cisco.com à l'adresse e-mail de l'utilisateur.

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.

Lorsque l'utilisateur clique sur l'URL ou l'ouvre dans son navigateur, il est redirigé vers la page de connexion de Security Cloud Sign On (SCSO).

Si l'utilisateur s'est déjà inscrit à un compte SCSO, il s'authentifie à l'aide de son adresse e-mail enregistrée et établit un lien vers son compte SMA.

Si l'utilisateur ne dispose pas d'un compte SCSO, il sélectionne Sign up now pour démarrer le processus d'inscription.

Security Cloud Sign On

Email

Continue

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



Or

[Other login options](#)

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

Saisissez les informations de compte pour vous inscrire à un compte SCSO. L'utilisateur reçoit un e-mail pour activer le nouveau compte SCSO. Suivez les instructions dans l'e-mail pour activer le compte et activer l'authentification multifacteur.

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](#)



Une fois que l'utilisateur s'est inscrit avec succès à un compte SCSO, retournez à l'e-mail de demande de lien SCSO Secure Malware Analytics (SMA) précédemment reçu et ouvrez l'URL dans un navigateur.

Une fois l'authentification réussie, l'utilisateur a la possibilité de lier le compte SMA au compte SCSO connecté.

Confirm Link Accounts

You are logged into Security Cloud Sign On as:

~~XXXXXXXXXX~~+testuser04@~~XXXXXX~~.com

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

Confirm

Confirmez l'action. Un message de réussite indiquant « Vos comptes ont été liés » s'affiche. Sélectionnez Continue with Security Cloud Sign On pour vous connecter au compte Secure Malware Analytics (SMA) et accepter le Contrat de licence utilisateur final (CLUF) pour terminer la configuration du compte.

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

Lier un utilisateur existant

Si un compte Secure Malware Analytics (SMA) existant n'a pas été lié à Security Cloud Sign On (SCSO) avant que la fonctionnalité de connexion SCSO-only ne prenne effet le 19 février 2026,

procédez comme suit pour lier les comptes.

Prérequis

Un compte SCSO (Security Cloud Sign On) enregistré est requis.

Si aucun compte SCSO n'a été créé, inscrivez-vous à l'adresse : <https://sign-on.security.cisco.com/signin/register>

Procédure

Accédez au portail Secure Malware Analytics approprié :

- États-Unis - <https://panacea.threatgrid.com>
- UE - <https://panacea.threatgrid.eu>
- Australie - <https://panacea.threatgrid.com.au>
- Canada - <https://panacea.threatgrid.ca>

Dans l'écran de connexion, sélectionnez Continue with Security Cloud Sign On pour vous connecter à l'aide de SCSO.

 **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](#)

Connectez-vous à Security Cloud Sign On (SCSO) à l'aide du compte précédemment créé.

Security Cloud Sign On

Email

Continue

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

Or

[Other login options](#)

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

Une fois l'authentification réussie, un message indiquant « Aucun compte Malware Analytics n'est lié à ce compte SCSO » s'affiche. s'affiche, ainsi que l'option permettant de lier un compte.

Sélectionnez Lier un compte pour commencer à lier le compte Secure Malware Analytics (SMA) existant au compte SCSO.

Select account

You are logged into Security Cloud Sign On as:

existinguser01@cisco.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.](#)



Sur la page suivante, une option permettant de lier des comptes s'affiche. Saisissez le nom d'utilisateur existant et sélectionnez le lien Demander.

Link accounts

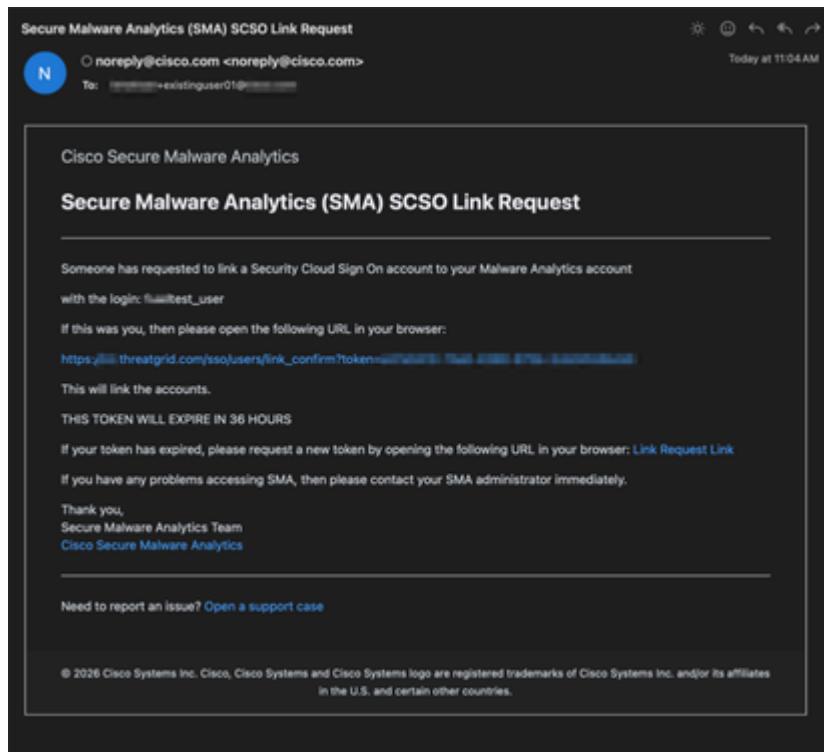
Enter the Malware Analytics username to link to this Security Cloud Sign On account.

Username

Request link



Un e-mail d'invitation est envoyé à l'adresse e-mail configurée pour le compte existant. Dans la plupart des cas, cette adresse e-mail correspond à celle du compte SCSO. Si l'adresse e-mail doit être mise à jour, contactez l'administrateur de l'entreprise ou l'assistance Cisco.



Ouvrez l'URL fournie dans l'e-mail d'invitation dans un navigateur. Une fois l'authentification réussie, l'utilisateur est invité à confirmer la liaison du compte.

Vérifiez les détails du compte et sélectionnez Confirm.

Confirm Link Accounts

You are logged into Security Cloud Sign On as: existinguser01@.com

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

Confirm

Un message de confirmation s'affiche pour indiquer que les comptes ont été liés. Sélectionnez

Continuez avec Security Cloud Sign On pour vous connecter au compte Secure Malware Analytics existant à l'aide de SCSO.

- Your accounts have been linked!

Log in

Log in to your Secure Malware Analytics account.

Continue with Security Cloud Sign On

Sur la page suivante, sélectionnez le compte utilisateur auquel vous souhaitez vous connecter.

Select account

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

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

1100

Best user

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

Remarque : Les administrateurs de l'organisation peuvent également envoyer le compte SCSO liant l'e-mail d'invitation depuis la page Gestion des utilisateurs.

← Users

Account Settings - Test User

Local Data • Cisco Internal

Details

Login:

User name: Test User 

Organization:

Last activity: a few seconds ago

Title: 

Email: 

Role:

Status: Active Inactive

CSA auto-submit types: 

Can flag entities:  Unset

Opt-out of data collection: True False Unset

Send SSO link email 

Submission settings

Default UI submission privacy: Private Public Unset

API

API key:  

Disable API key: True False Unset

Can download sample content via API: True False Unset

API quota: 

Rate limit: 

Connections

SSO CONNECTIONS 

PRODUCT CONNECTIONS 

Plusieurs comptes Secure Malware Analytics liés à un seul compte SCSO

Les utilisateurs peuvent lier plusieurs comptes Secure Malware Analytics (SMA) au même compte Security Cloud Sign On (SCSO) à l'aide de la méthode Create New SMA User ou Link an Existing User.

Une fois l'authentification SCSO réussie, l'utilisateur se voit proposer une option lui permettant de sélectionner le compte Secure Malware Analytics auquel il doit accéder.

Select account

You are logged into Security Cloud Sign On as:

1@123.com

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

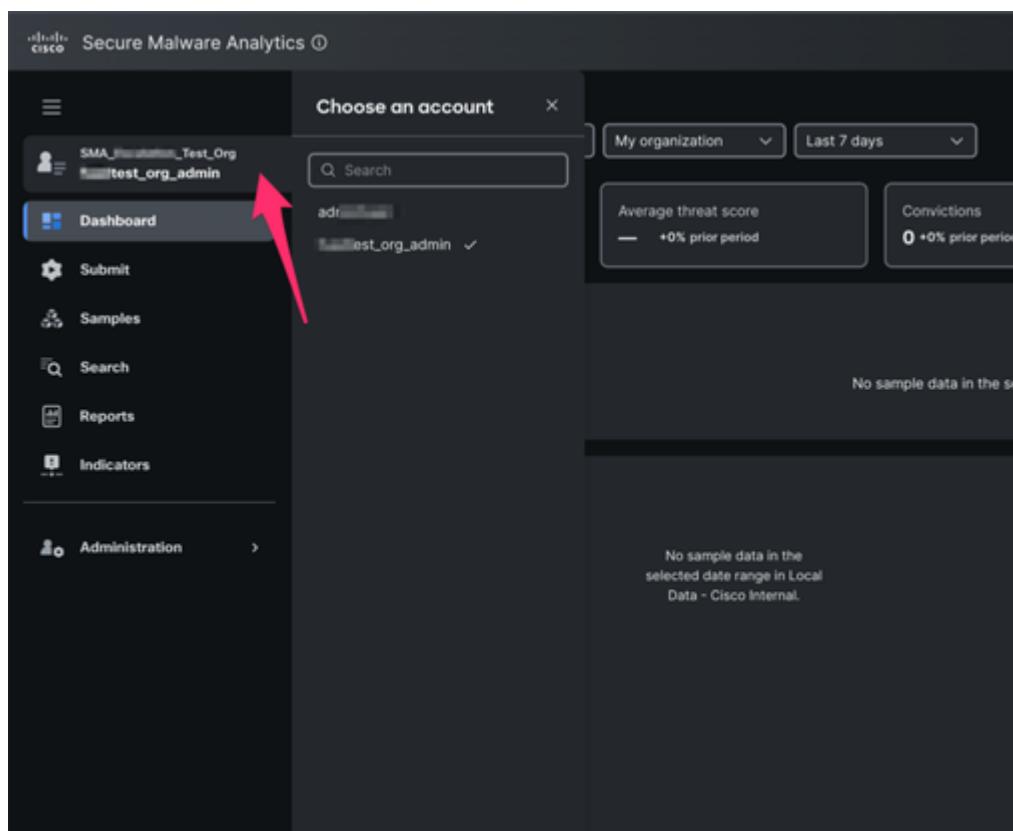
User

test_org_admin



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

Les utilisateurs peuvent également passer d'un compte à l'autre après s'être connectés à l'aide du menu de navigation de gauche.



The screenshot shows the Secure Malware Analytics interface. On the left, a navigation menu is visible with items: SMA_123_Test_Org, test_org_admin, Dashboard (which is currently selected and highlighted in blue), Submit, Samples, Search, Reports, Indicators, Administration, and a link to Cisco.com. A red arrow points to the 'Dashboard' item in the menu. In the center, a modal window titled 'Choose an account' is open. It contains a search bar with the placeholder 'Search' and a dropdown menu showing 'adri' and 'test_org_admin'. Below the search bar are two boxes: 'Average threat score' (showing '+0% prior period') and 'Convictions' (showing '0 +0% prior period'). At the bottom of the modal, it says 'No sample data in the selected date range in Local Data - Cisco Internal.'

Connexion SCSO uniquement pour l'intégration

Les intégrations telles que Umbrella SIG, Secure Access, Meraki et Email Threat Defense (ETD) provisionnent automatiquement un compte d'administrateur d'entreprise ou d'administrateur de périphérique lorsqu'elles sont enregistrées auprès de Secure Malware Analytics.

Un e-mail d'invitation est envoyé à l'adresse e-mail fournie par le périphérique ou le service d'intégration pour terminer la liaison du compte à l'aide de la connexion au cloud de sécurité (SCSO).

Soutien

Pour obtenir de l'aide ou des informations supplémentaires, contactez le [Centre d'assistance technique Cisco \(TAC\)](#).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.