Lier des comptes Secure Malware Analytics Connexion avec Security Cloud Connexion

Table des matières

Introduction

Fond

Connexion au cloud de sécurité (SCSO)

Lier un utilisateur existant

- Prérequis

Créer un nouvel utilisateur SMA

- Lier un nouveau compte utilisateur à un compte SCSO

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) passe à Security Cloud Sign On (SCSO) comme méthode d'authentification exclusive pour tous les utilisateurs.

Fond

Cette modification vise à fournir une expérience de connexion centralisée et cohérente sur l'ensemble des produits de sécurité Cisco.

Il explique les mises à jour introduites par cette transition et fournit des conseils sur la façon de lier votre compte SCSO à Secure Malware Analytics. Cette fonctionnalité est disponible à partir du 24 février 2026. Après cette date, l'authentification utilisant des noms d'utilisateur et des mots de passe SMA natifs n'est plus prise en charge.



Remarque : Cette modification s'applique uniquement au service cloud Secure Malware Analytics (SMA). L'authentification de l'appliance Secure Malware Analytics reste inchangée. L'authentification API reste également inchangée.

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

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 24 février 2026, suivez cette procédure pour lier les comptes.

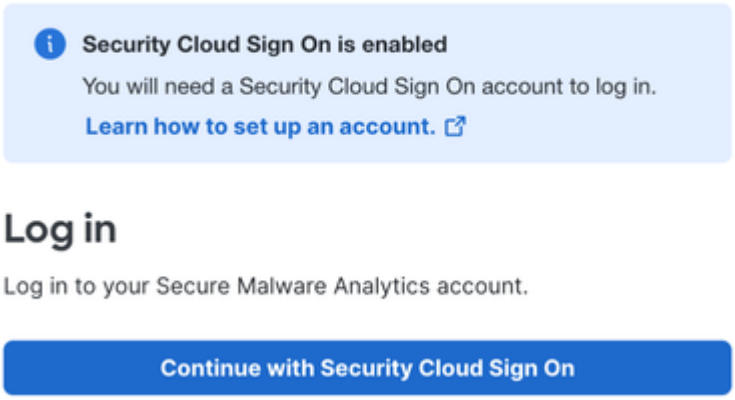
Prérequis

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

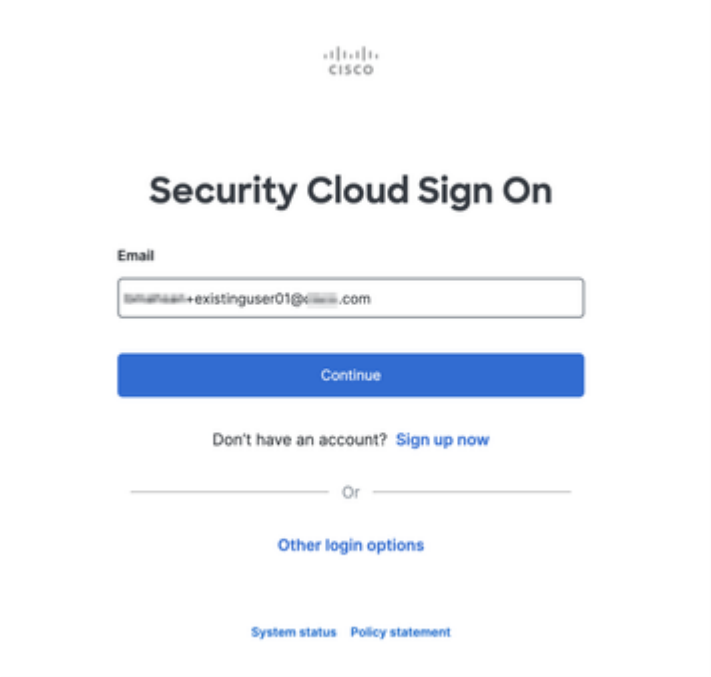
1. Accédez au portail Secure Malware Analytics approprié :

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

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

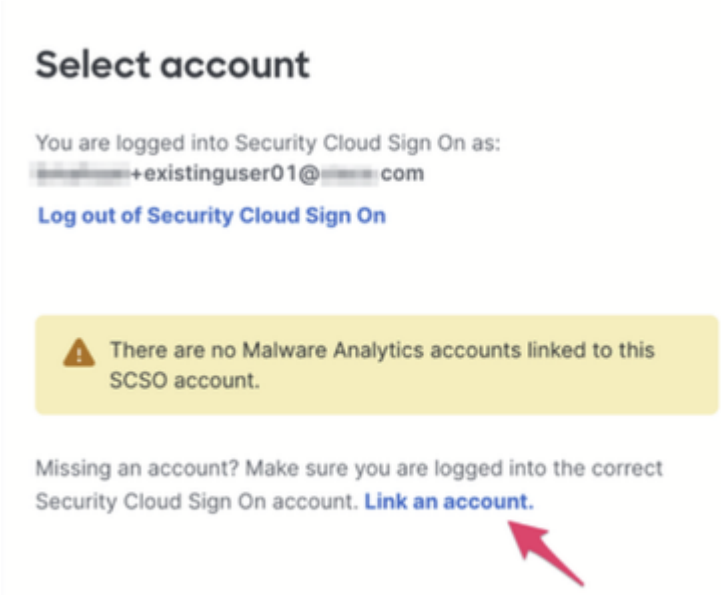


3. Connectez-vous à Security Cloud Sign On (SCSO) à l'aide du compte précédemment créé.



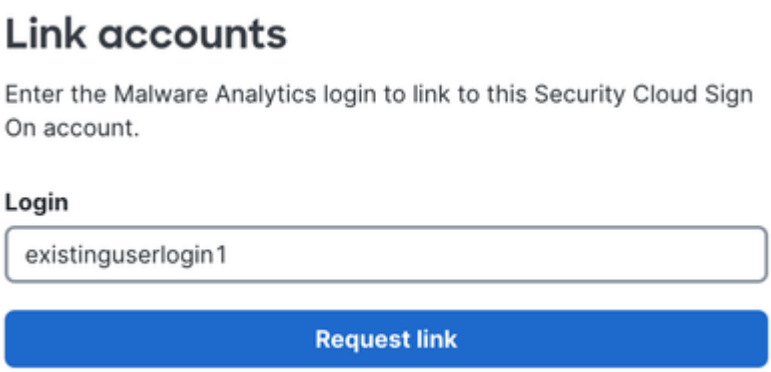
Une fois l'authentification réussie, un message indiquant « Aucun compte Malware Analytics n'est lié à ce compte SCSO » s'affiche. s'affiche, ainsi que l'option permettant de lier un compte.

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

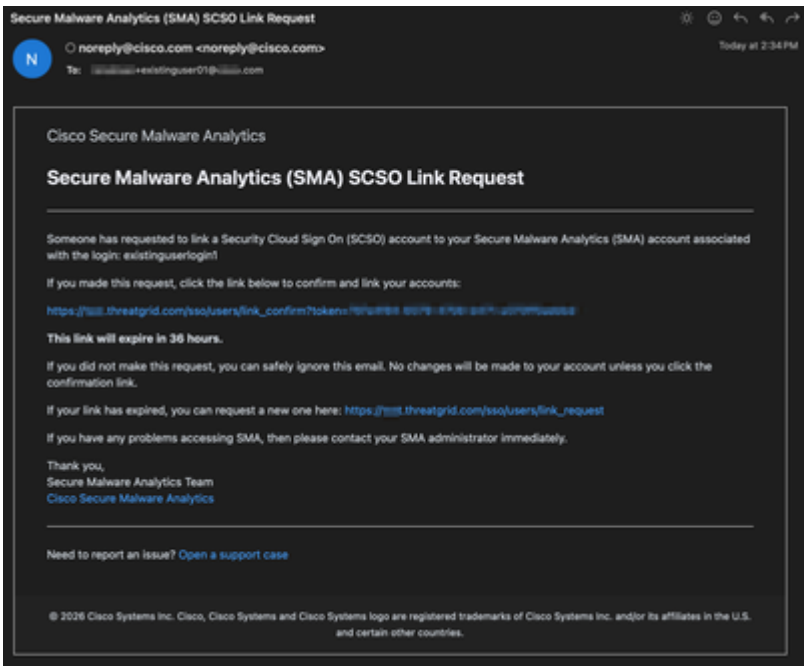


Sur la page suivante, une option permettant de lier des comptes s'affiche.

5. Saisissez la connexion existante et sélectionnez le lien Demander.

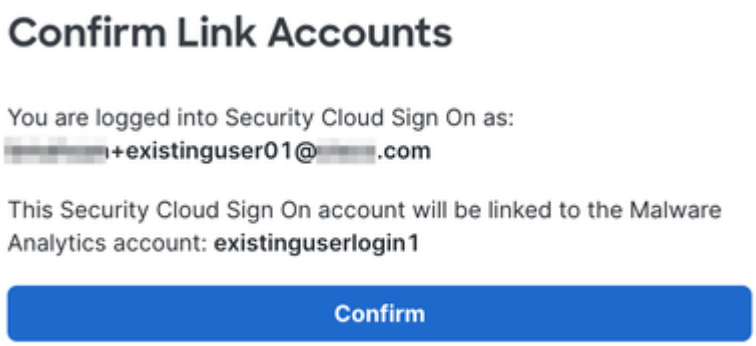


Un e-mail d'invitation est envoyé à l'adresse e-mail associée au compte SMA existant.
Dans la plupart des cas, cette adresse e-mail correspond à celle du compte SCSO. Si l'adresse e-mail doit être mise à jour, contactez l'administrateur de l'entreprise ou l'assistance Cisco.



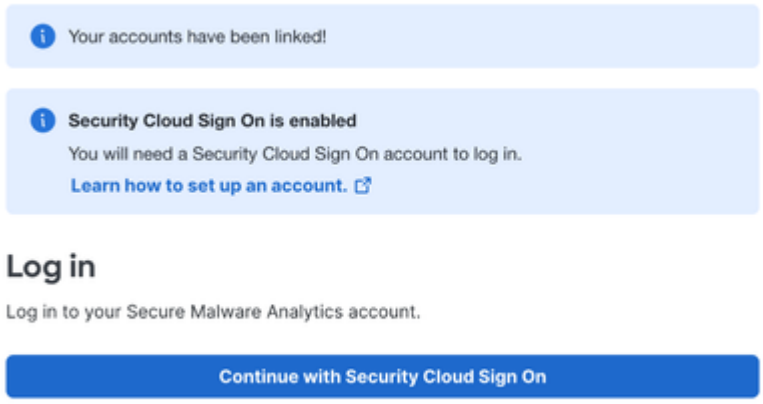
6. Ouvrez l'URL fournie dans l'e-mail d'invitation dans un navigateur. Une fois l'authentification réussie, vous êtes invité à confirmer la liaison du compte.

7. Vérifiez les détails du compte et sélectionnez Confirmer.

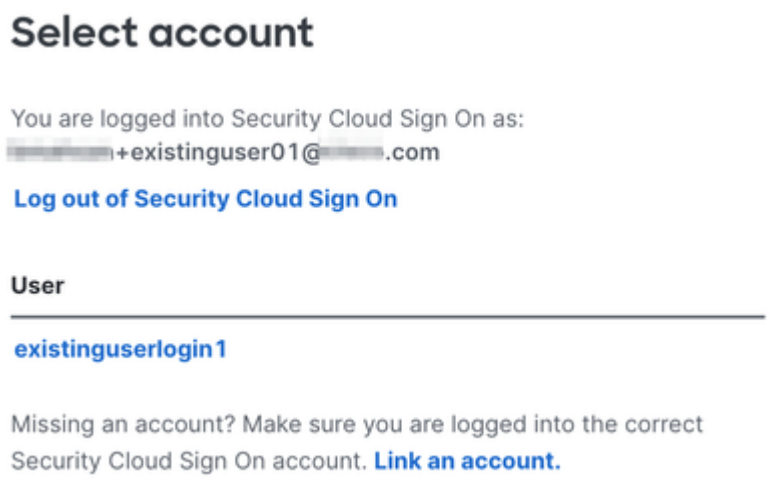


Un message de confirmation s'affiche pour indiquer que les comptes ont été liés.

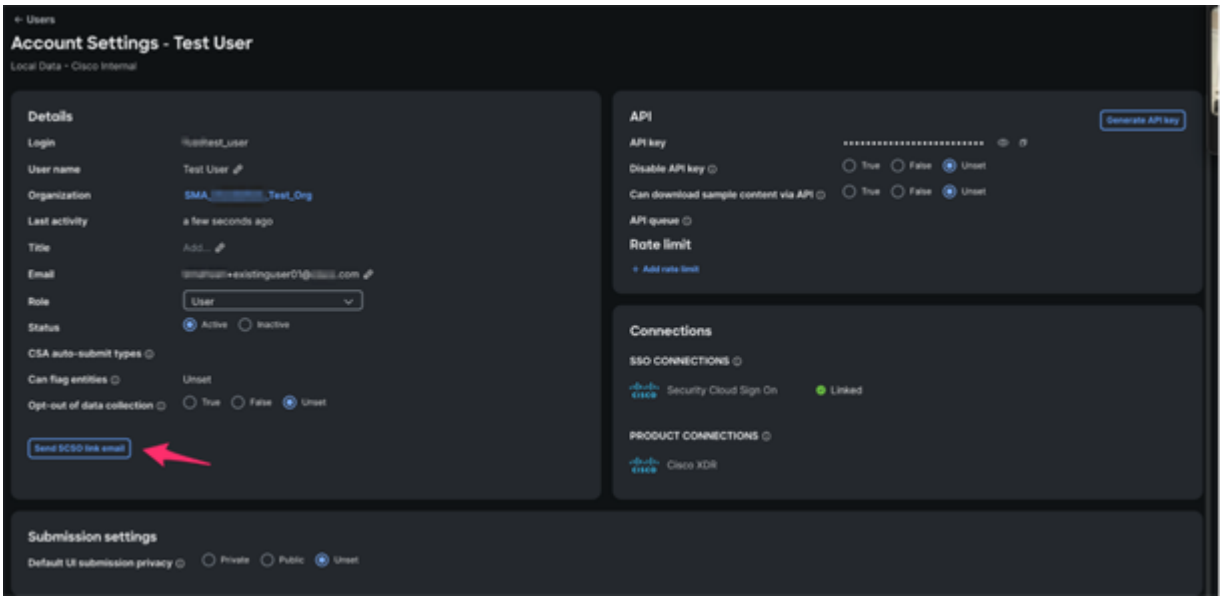
8. Sélectionnez Continue with Security Cloud Sign On pour vous connecter au compte Secure Malware Analytics existant à l'aide de SCSO.



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



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



Créer un nouvel 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.

Pour créer un nouvel utilisateur :

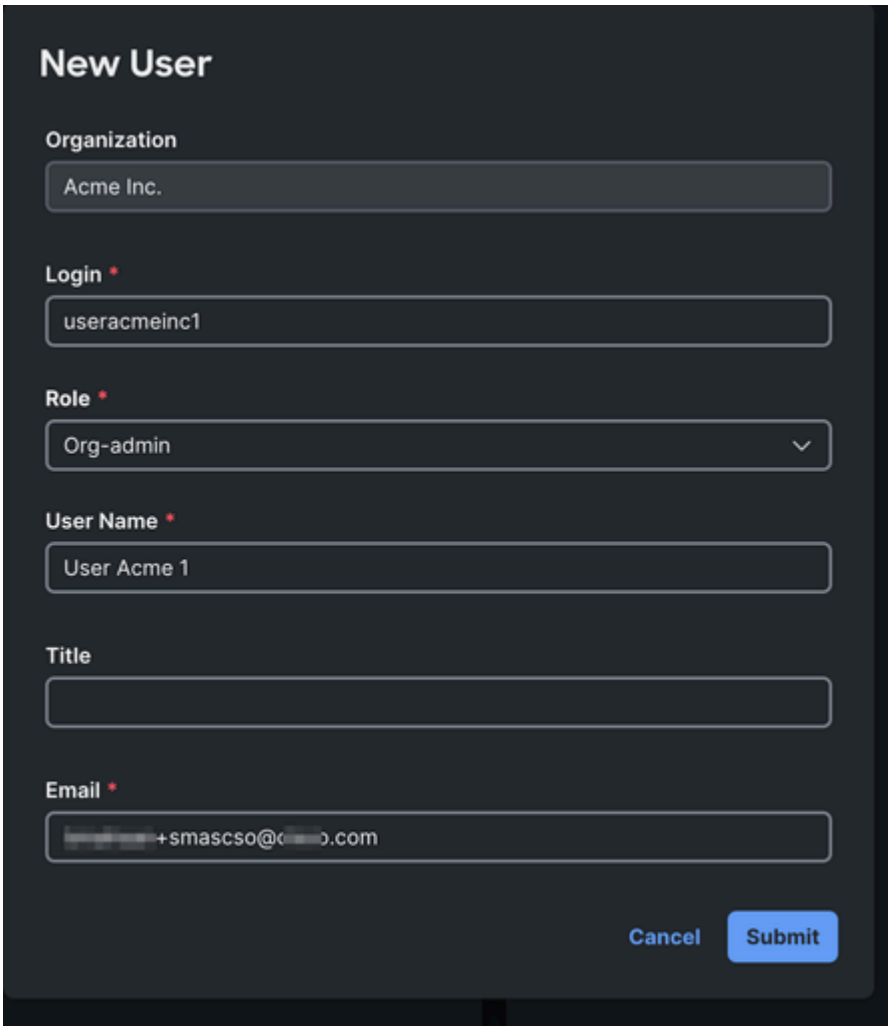
1. Connectez-vous à Secure Malware Analytics en tant qu'administrateur d'entreprise.

2. Accédez à Administration > Users > New User.

3. Saisissez les informations requises :

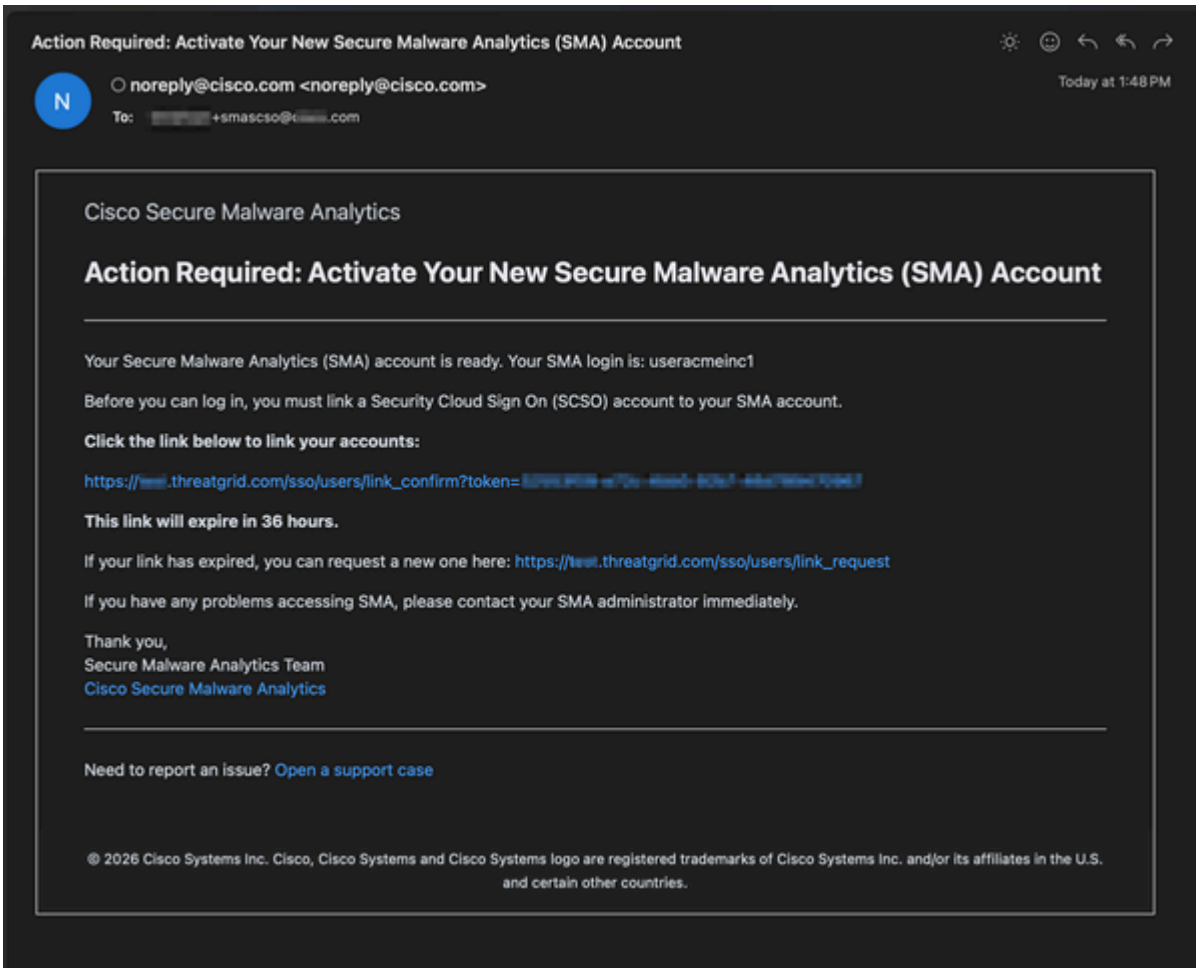
- Connexion
- Rôle
- Nom d'utilisateur
- Adresse électronique

4. Cliquez sur Soumettre.



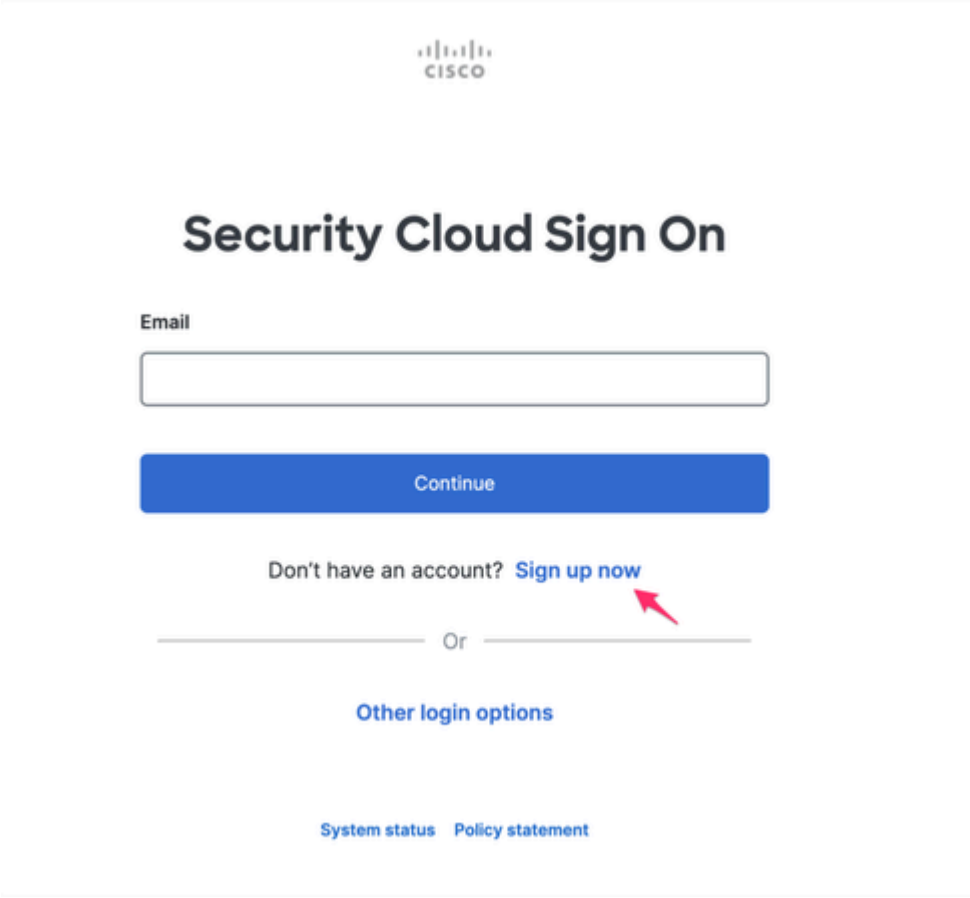
Lier un nouveau compte utilisateur à un compte SCSO

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.



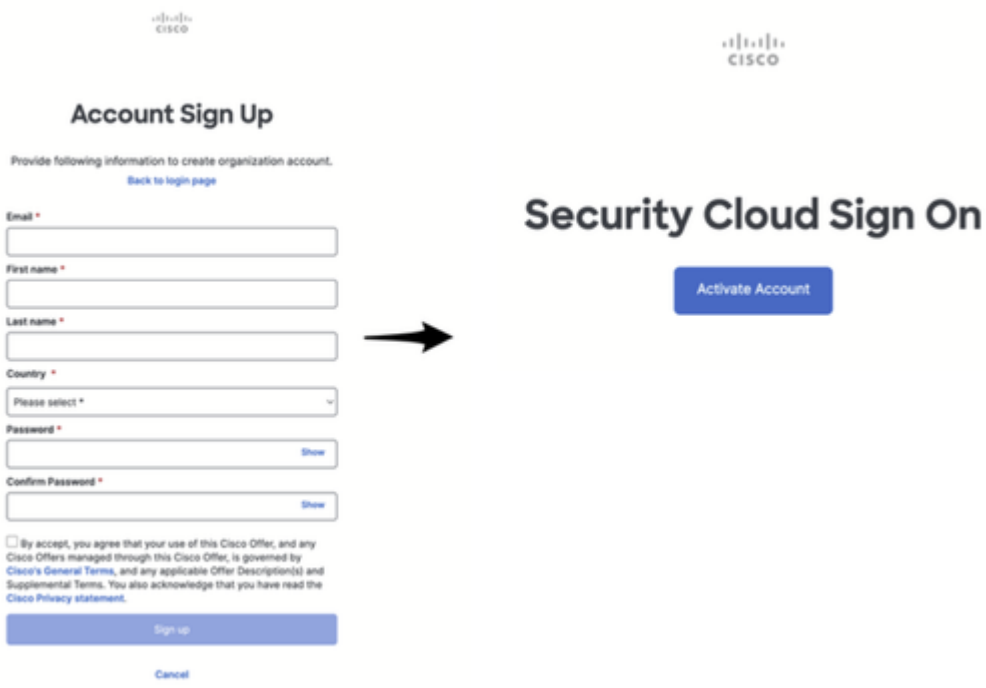
Lorsque le nouvel utilisateur clique sur l'URL ou l'ouvre dans son navigateur, il est redirigé vers la page de connexion SCSO (Security Cloud Sign On).

- 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 doit sélectionner Sign up now pour démarrer le processus d'inscription.



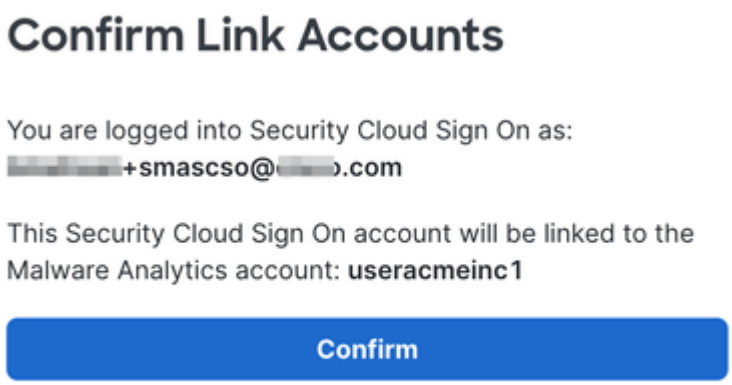
1. Saisissez les informations de compte pour vous inscrire à un compte SCSO. L'utilisateur reçoit un e-mail pour activer le nouveau compte SCSO.

2. Suivez les instructions de l'e-mail pour activer le compte et activer l'authentification multifacteur.



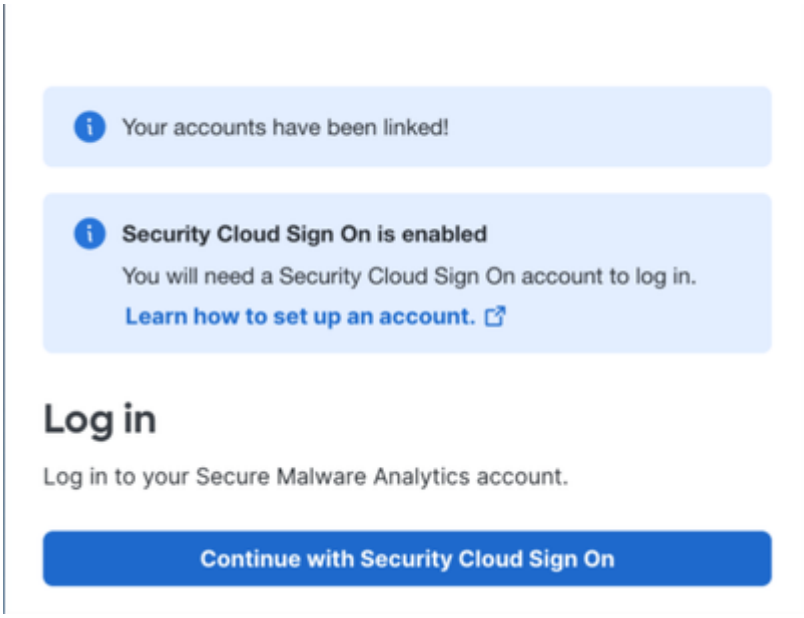
3. Une fois que l'utilisateur s'est inscrit avec succès à un compte SCSO, retournez à l'e-mail de demande de lien SCSO Secure Malware Analytics (SMA) précédemment reçu et ouvrez l'URL dans un navigateur.

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

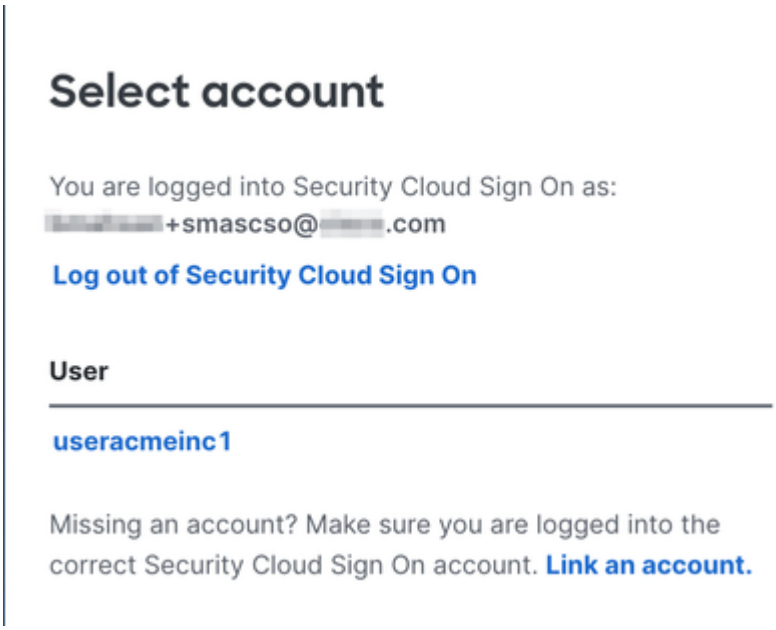


4. Confirmez l'action. Un message de réussite indiquant « Vos comptes ont été liés » s'affiche.

5. Sélectionnez Continue with Security Cloud Sign On pour vous connecter au compte Secure Malware Analytics (SMA) et accepter le Contrat de licence de l'utilisateur final (CLUF) pour terminer la configuration du compte.



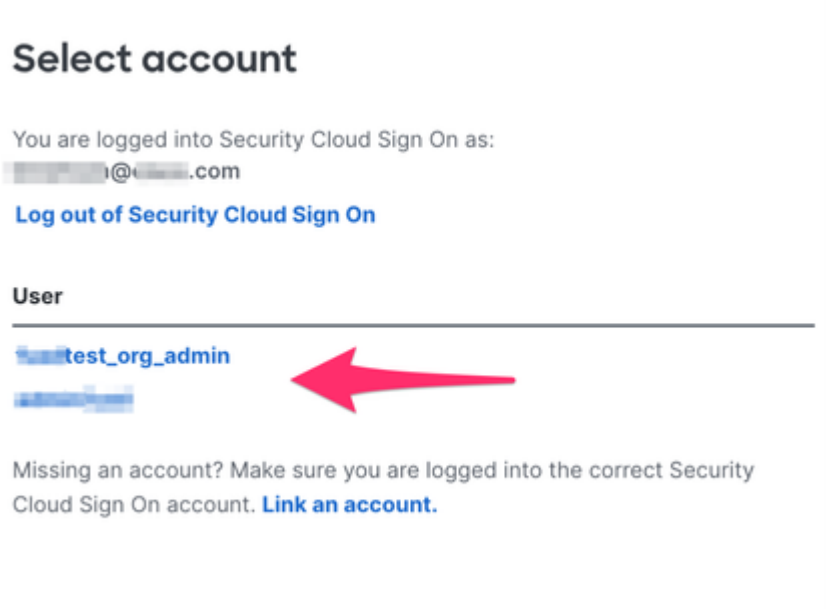
6. Sur la page suivante, sélectionnez le compte utilisateur auquel vous souhaitez vous connecter.



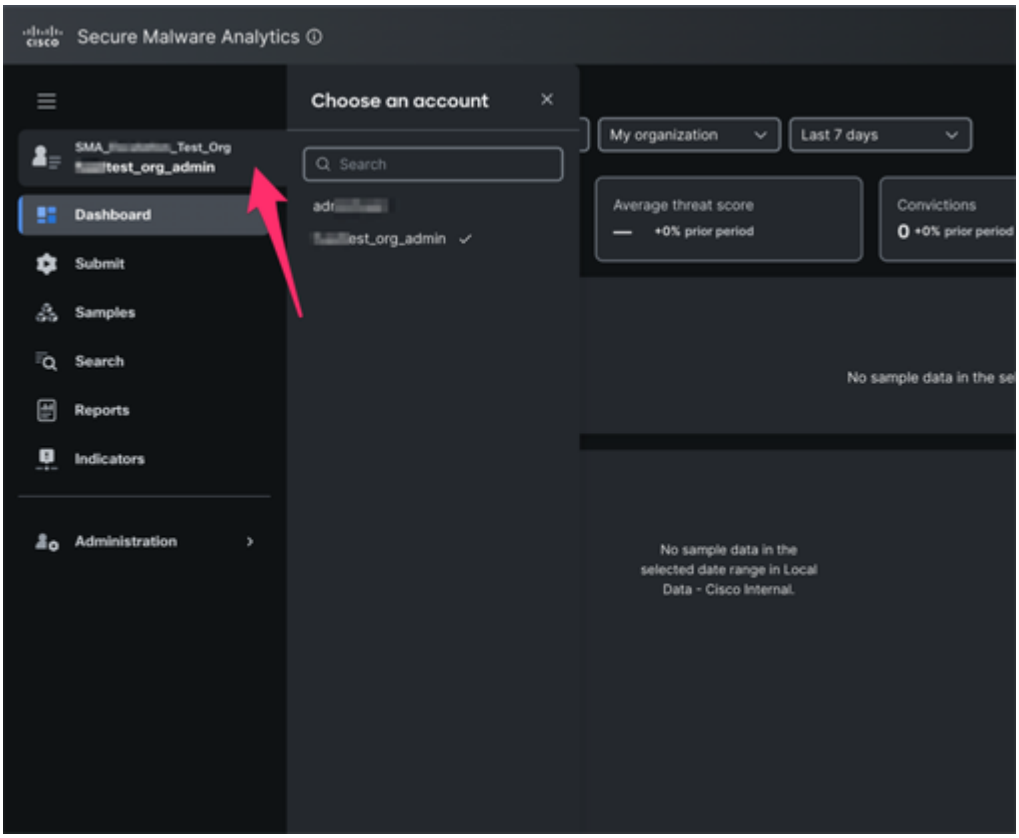
Plusieurs comptes Secure Malware Analytics liés à un seul compte SCSO

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.



Vous pouvez également basculer entre les comptes après vous être connecté à l'aide du menu de la navigation de gauche.



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 les problèmes d'authentification à deux facteurs Duo Mobile, veuillez consulter la section Réinitialiser Duo Mobile sur Security Cloud Sign-On et ajouter un document Périphérique d'authentification supplémentaire.
- Pour plus d'informations sur SCSO, consultez la page Security Cloud Sign On Documents.
- 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.