

Configuration d'un cadre pour la migration vers un accès sécurisé et un contrôle cloud sécurisé

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Étapes de préparation](#)

[1. Préparer la migration](#)

[2. Connectez-vous à SCC en utilisant vos identifiants de connexion Cisco existants](#)

[3. Lier l'organisation-cadre à SCC et demander un abonnement](#)

[4. Appliquez la licence à Secure Access Instance](#)

[Vérification de la liaison d'accès sécurisé vers SCC](#)

[1. État d'activation du produit dans les abonnements](#)

[2. Accès sécurisé dans la liste des produits](#)

[Migration d'Umbrella vers un accès sécurisé](#)

[Vérifier la migration](#)

[Informations connexes](#)

Introduction

Ce document décrit comment migrer d'Umbrella vers un accès sécurisé à l'aide du contrôle du cloud de sécurité (SCC).

Informations générales

Les clients Umbrella sont encouragés à migrer d'Umbrella vers Secure Access et doivent utiliser Security Cloud Control pour gérer tous leurs produits de sécurité cloud dans le cadre de ces changements. Cela vous permet de disposer d'une interface unique pour gérer leurs produits de sécurité cloud, notamment Cisco Secure Access.

Multi-org et MSSP ne sont pas pris en charge actuellement (au moment de la création de cet article).

Conditions préalables

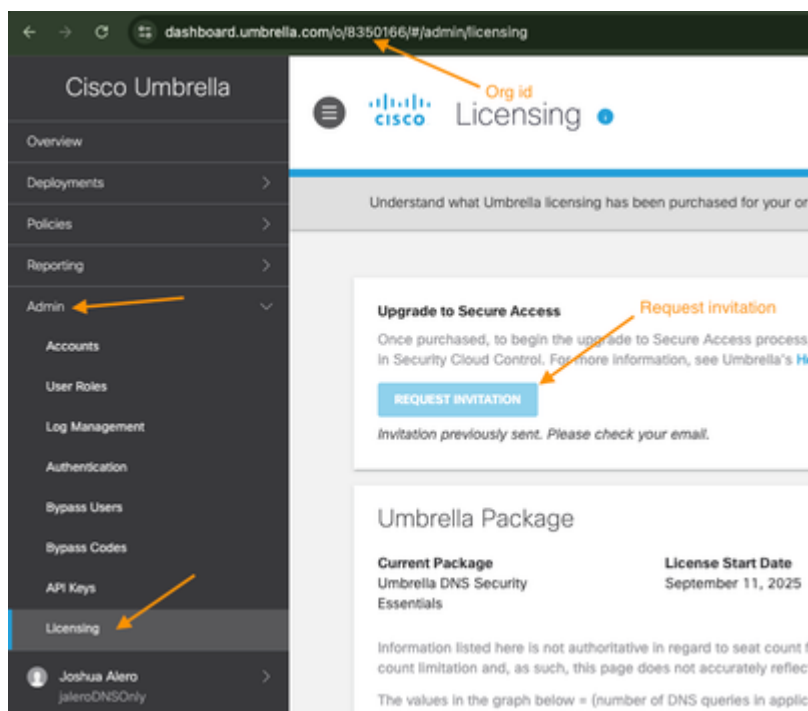
- Abonnement DNS ou SIG actuel
- Accès administrateur complet à Umbrella
- Accès au contrôle du cloud de sécurité

Étapes de préparation

1. Préparer la migration

1. Assurez-vous que vous disposez d'un abonnement DNS ou SIG sur Umbrella :

- Accédez à Admin > Licensing pour vérifier
- La mise à niveau vers un accès sécurisé doit être affichée en haut de la page :



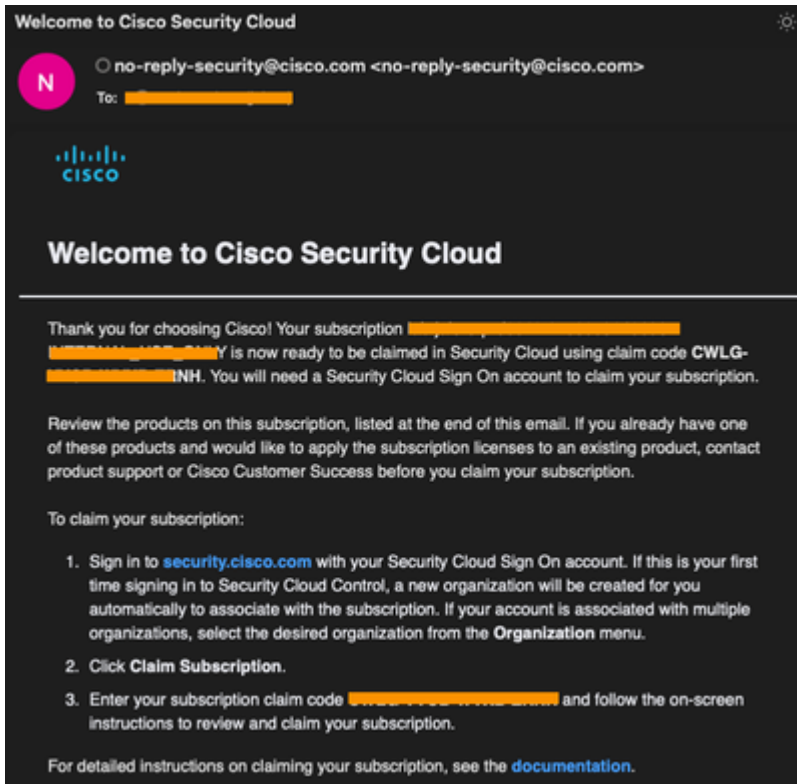
ii. Notez l'ID d'organisation, dans cet exemple 8350166.

iii. Sélectionnez l'option Demander une invitation sur la page de licence.

⚠ Important : Le bouton Request Invitation sert d'invitation à rejoindre le locataire Umbrella pour SCC. Il ne génère pas de code de revendication. Un code de demande vous sera fourni une fois votre commande d'accès sécurisé terminée. Cela fait partie du processus de migration vers un accès sécurisé.

✍ Remarque : Si la mise à niveau vers un accès sécurisé n'est pas présente, alors assurez-vous que le paquet Umbrella est DNS ou SIG (multi-org ou les modules complémentaires ne sont pas actuellement pris en charge au moment de la rédaction de cet article).

iv. En supposant que vous avez passé votre commande pour un accès sécurisé, attendez 3 à 4 jours ouvrables et vous devez recevoir un e-mail avec votre code de demande d'abonnement (après avoir lancé l'invitation de votre locataire Umbrella). Veuillez consulter l'exemple d'e-mail ici :



2. Connectez-vous à SCC en utilisant vos identifiants de connexion Cisco existants

i. Accédez au [portail Security Cloud Control](#) et connectez-vous avec vos identifiants de connexion Cisco.

 Remarque : Identifiants de connexion Cisco utilisés pour accéder à votre tableau de bord Umbrella.

ii. Sélectionnez Créer une organisation (si vous n'en avez pas déjà une).

iii. Saisissez le nom de la nouvelle organisation dans le champ Nom de la nouvelle organisation.

iv. Sélectionnez la région appropriée dans le menu déroulant Déploiement de la région.

 Remarque : il doit s'agir de la région géographique dans laquelle votre locataire sera déployé.

Exemple ici :

Select Organization

Create new organization

New organization name *

JaleroSSE

50 character limit

Region deployment *

Europe

This selection sets the preferred region for all products and services in this organization. See your Product's Privacy Data sheet on the [Trust Portal](#) to confirm regional availability

Continue

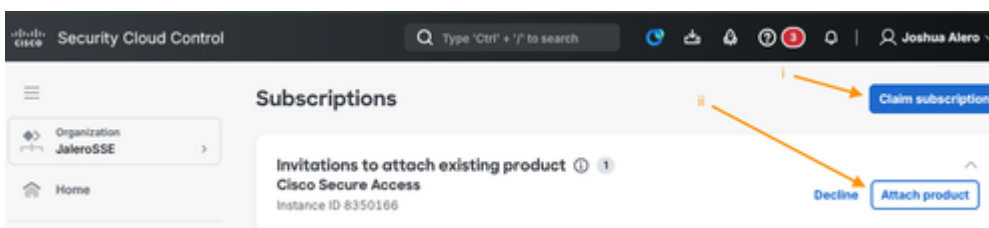
v. Sélectionnez ensuite Continuer pour terminer la création de l'organisation.

3. Lier l'organisation-cadre à SCC et demander un abonnement

i. Cliquez sur le bouton Demande d'abonnement pour la demander avec les codes fournis à l'étape 1 ci-dessus.

ii. Votre ID d'organisation Umbrella doit être affiché sur la page Abonnements ainsi que sur l'invitation à le joindre au SCC.

 Remarque : L'ID d'organisation Umbrella doit être identique à celui figurant sur votre tableau de bord Umbrella. Cela est important pour la migration et pour s'assurer que SCC et Umbrella ont été liés.



- Sélectionnez Joindre un produit pour joindre votre organisation-cadre au SCC.

- Une fois joint, vous devez voir le Cisco Secure Access en tant que produit dans la même page comme indiqué sur l'exemple ici :

Subscriptions

Claim subscription

8350166_secure-access

Externally managed ⓘ

End date: —

Product	Region	Entitlements	Status
Cisco Secure Access	Global	0	- ...

iii. Entrez le code de demande et sélectionnez Next :

Claim Subscription

1 Enter subscription claim code

2 Review products

3 Review subscription

Enter subscription claim code

To begin, enter your claim code below and click **Next**. For detailed instructions please read our [documentation](#).

Subscription claim code *

-ZRNH

<

Cancel

Next

iv. Sélectionnez Attacher une instance existante dans le menu déroulant Créer une nouvelle instance ou attacher une instance existante :

✓ Enter subscription claim code

2 Review products

3 Review subscription

Review products

To use an existing instance instead of creating a new one, choose **Attach existing instance** from the dropdown menu for the product. Post-claim actions may also be required to apply licenses to some product instances. [Read documentation for more details](#)

Products	Create new instance or attach existing ⓘ
Cisco Secure Access DNS Advantage	Attach existing instance

<

Cancel

Back

Next

v. Vérifiez les paramètres :

- Assurez-vous que le (instance existante) fait partie du nom du produit
- La région doit être définie sur la région existante de l'instance d'accès sécurisé connectée
- Sélectionnez Déplacer la demande pour passer à la page suivante

Review subscription

Subscription ID: [Redacted]
 Organization region: Europe

Products	Deployments
Cisco Secure Access DNS Advantage (Existing instance)	Region per existing deployment 1

Buttons: Cancel, Back, Claim

- Confirmez la demande d'abonnement :

Claim subscription

Claiming this subscription will associate the subscription details, including subscription ID and product licenses, with the **JaleroSSE** organization.

Buttons: Cancel, Claim

- Une fois la demande et le provisionnement réussis, vous devez obtenir une page Abonnements similaire à celle-ci, montrant tous vos produits activés :

Subscriptions

[Claim subscription](#)

Subscription successfully claimed.



Products will appear in the navigation shortly. Once your products are fully activated, you can access them from the **left-hand navigation** or the **platform navigator** at the top of the page. After activation, configure your **role-based access controls** to ensure proper user permissions.

Product and service activation status 1



Cisco Secure Access DNS Advantage

Start date 09/16/2025

[Action required](#)

8350166_secure-access Externally managed ⓘ

End date: —

Product	Region	Entitlements	Status
Cisco Secure Access	Global	0	- ...

f8643562-d914-4582-a95d-49cf392c757d

End date: —

Product	Region	Entitlements	Status
Cisco Security Cloud Control Firewall Management Base	Europe	1	Activated ...

4. Appliquez la licence à Secure Access Instance

i. Sélectionnez l'option Action requise :

Product and service activation status 1



Cisco Secure Access DNS Advantage

Start date 09/16/2025

[Action required](#)

ii. Sélectionnez Appliquer la licence :

Cisco Secure Access DNS Advantage ×

Subscription ID

XXXXXXXXXXXX
XXXXXXXXXXXX
XXXXXXXXXXXX

Apply license to an existing instance

The following Cisco Secure Access DNS Advantage instances are associated with your Cisco Security Cloud organization. Select an instance and click **Apply license**.

☒ Cisco Secure Access Externally managed
Instance ID 8350166



Cancel

Apply license

Vérification de la liaison d'accès sécurisé vers SCC

Utilisez cette section pour vérifier que votre locataire d'accès sécurisé a été lié à SCC.

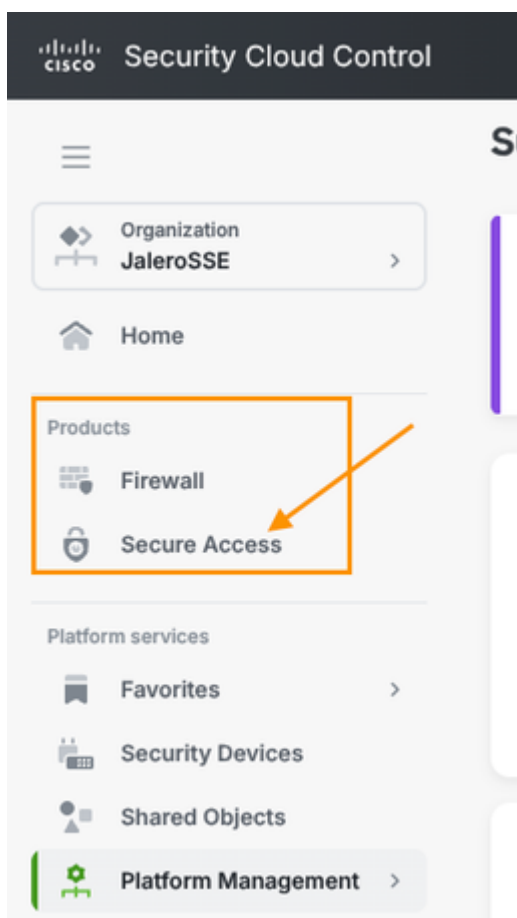
1. État d'activation du produit dans les abonnements

Vérifiez que l'instance de produit Cisco Secure Access <License Type> a été activée :

End date: Sep 16, 2026			
Product	Region	Entitlements	Status
Cisco Secure Access DNS Advantage	Global	50	Activated

2. Accès sécurisé dans la liste des produits

L'accès sécurisé doit désormais être répertorié sous Produits également :



Migration d'Umbrella vers un accès sécurisé

1. Reconnectez-vous à Umbrella avec le même compte que ci-dessus.
2. Accédez au nouvel élément de menu Gestionnaire de mise à niveau :

← → ↻ dashboard.umbrella.com/o/8350166/#/overview?encodedFilters=JTdCJTlyYWN0aW9uJTlyJTNBJTlyYmxvY2t1ZCUyMiUyQyUyMnNlbGVjdGVkRGF0ZVJhbmdlSWR4J...

Cisco Umbrella

Overview

Deployments >

Policies >

Reporting >

Admin >

Upgrade Manager **NEW**

Joshua Alero
jaleroDNSOnly >

Service Status
All services are operational

Documentation

Support Platform

Knowledge Base

Learning Videos

Cisco Online Privacy Statement

Terms Of Service

© Cisco Systems

Overview



Upgrade to Secure Access

Upgrade your organization to Secure Access's next-generation cloud-delivered Internet protections and access controls.

Upgrade Later **Start Upgrade**

3. Dans la page Gestionnaire de mise à niveau, sélectionnez Démarrer sous Activer la connexion au cloud de sécurité Cisco



Upgrade to Cisco Secure Access

This upgrade process involves migrating data and configurations to your new Secure Access organization.

The result is that all current identity traffic is steered through Secure Access. No protections are lost. [Help](#)

0/4 steps complete

1

Prerequisites

Complete these steps before beginning the upgrade process. If you have previously completed a step, mark it



1. Enable Cisco Security Cloud Sign On

Enable Security Cloud Sign On as your authentication method.

Start



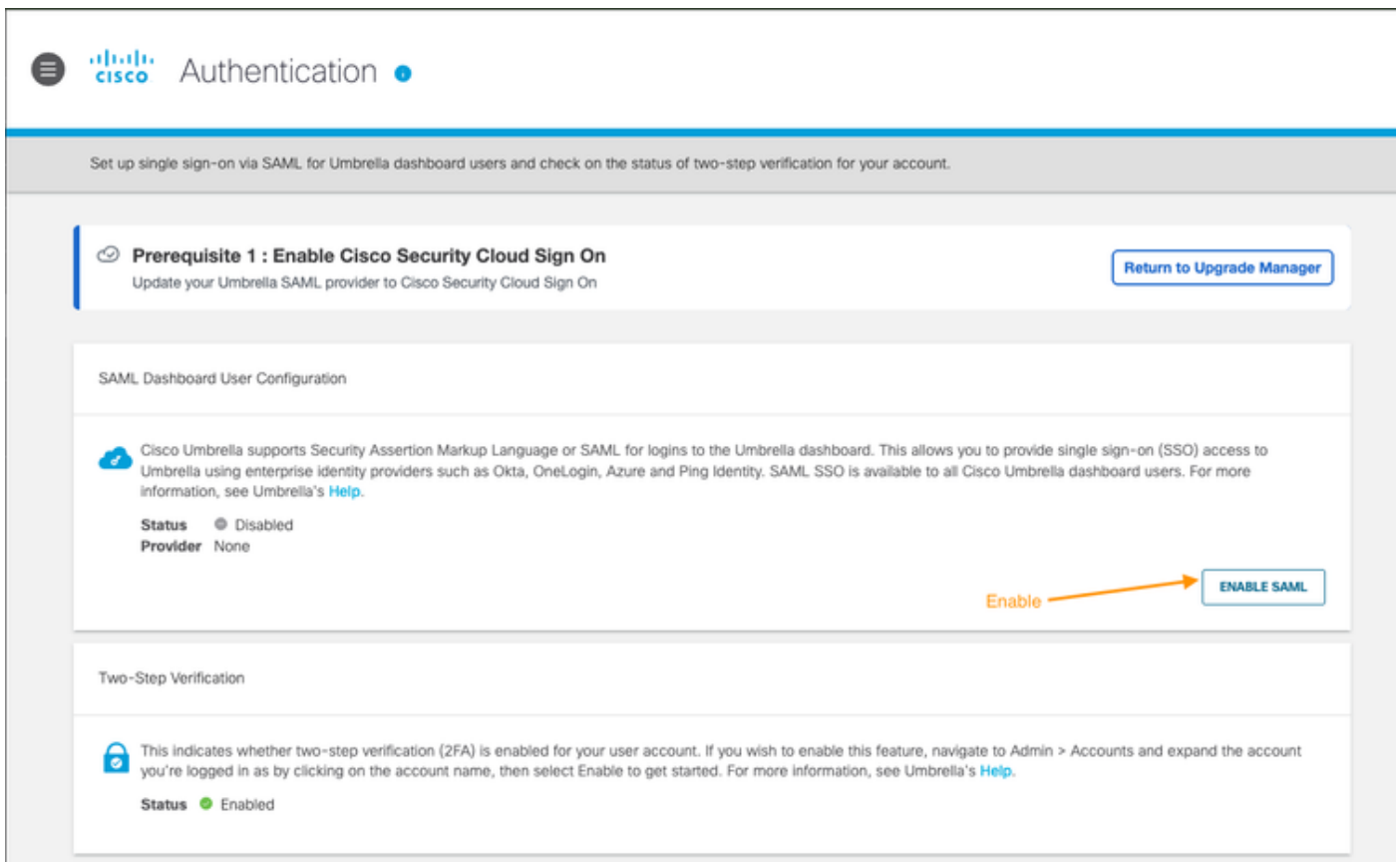
2. Update VAs and AD connectors

Update your virtual appliances and Active Directory Connectors to their latest versions.

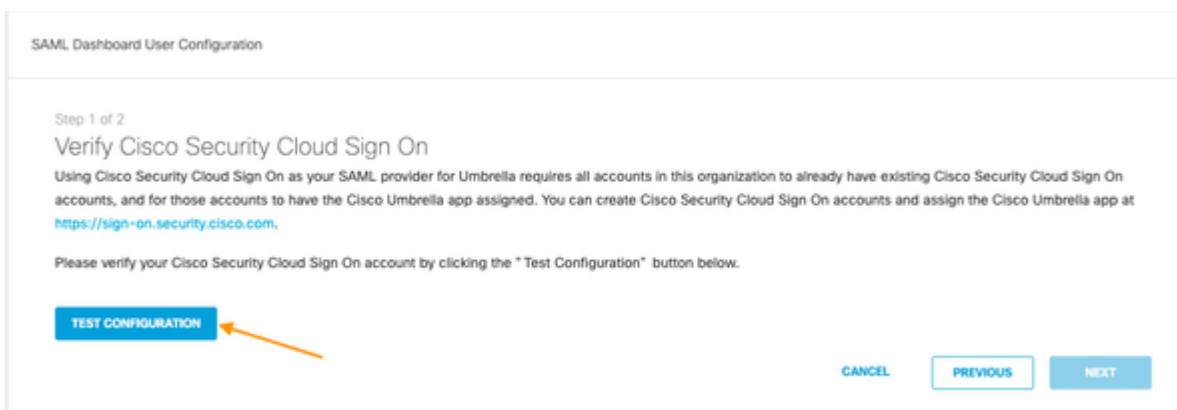
Start

☐ Mark as done

4. Sélectionnez ENABLE SAML sous SAML Dashboard User Configuration pour lier votre SCC en tant que fournisseur SAML pour la connexion au tableau de bord :



5. Testez la configuration SAML avec l'option TEST CONFIGURATION :



6. La page de connexion de SCC doit apparaître dans une autre fenêtre contextuelle (assurez-vous que le bloqueur de fenêtres contextuelles est désactivé) :

Lorsque vous y êtes invité, connectez-vous avec vos identifiants SCC.



CONNECTING TO CISCO UMBRELLA

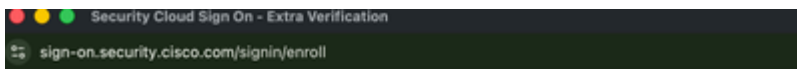
Security Cloud Sign On

Email

Password

 [Show](#)

[Forgot password](#)



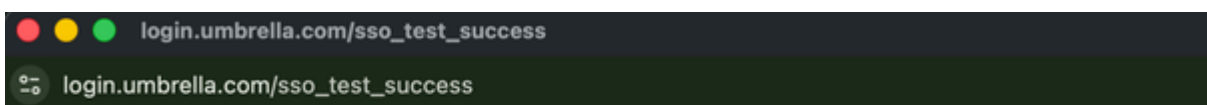
Multifactor authentication

Click on **Finish** or [set up Google Authenticator](#) as an additional MFA option.



[Finish](#)

Lorsque la connexion a été vérifiée, vous devez obtenir le message ici, le confirmant. À ce stade, la partie SAML est presque terminée :



Success!

You have successfully configured your SAML provider. You may now close this modal.

Vous devez ensuite revenir à la partie SAML Dashboard User Configuration :

- La coche verte indique que les paramètres SAML ont été correctement configurés
- Sélectionnez NEXT pour continuer

SAML Dashboard User Configuration

Step 1 of 2

Verify Cisco Security Cloud Sign On

Using Cisco Security Cloud Sign On as your SAML provider for Umbrella requires all accounts in this organization to already have existing Cisco Security Cloud Sign On accounts, and for those accounts to have the Cisco Umbrella app assigned. You can create Cisco Security Cloud Sign On accounts and assign the Cisco Umbrella app at <https://sign-on.security.cisco.com>.

Please verify your Cisco Security Cloud Sign On account by clicking the "Test Configuration" button below.

TEST CONFIGURATION

 Your SAML settings have been properly configured!

CANCEL

PREVIOUS

NEXT

Enregistrez les modifications et avertissez les utilisateurs :

SAML Dashboard User Configuration

Step 2 of 2

Save and Notify

After clicking 'Save', all users in your organization will be required to use the single sign-on service rather than a password. Umbrella will send an email to every administrative user in the dashboard, stating their password has been removed from their account.

- ☒ If you disable the single sign-on service in the future, all users in your dashboard will be emailed a link to reset their passwords and their old passwords are not restored.
- ☒ Block page bypass users will no longer work once SAML is enabled. Instead, you must use codes for bypassing block pages. For more information, [read here](#).

Two step verification with Umbrella is not available when SAML is enabled. Instead, use the two factor options available with your SSO provider.

PREVIOUS

SAVE AND NOTIFY USERS

Configuration SAML terminée :

SAML Dashboard User Configuration

 Cisco Umbrella supports Security Assertion Markup Language or SAML for logins to the Umbrella dashboard. This allows you to provide single sign-on (SSO) access to Umbrella using enterprise identity providers such as Okta, OneLogin, Azure and Ping Identity. SAML SSO is available to all Cisco Umbrella dashboard users. For more information, see Umbrella's [Help](#).

Status  Enabled

Provider Cisco Security Cloud Sign On

DISABLE

CONFIGURE

7. Effectuez la mise à niveau vers Secure Access en sélectionnant Upgrade dans la section Start

Upgrade :

Prerequisites 3/3 prerequisites done

Start Upgrade

Clicking Upgrade generates your new Secure Access organization (and dashboard) and copies your Umbrella configurations to Secure Access. Umbrella continues to operate during this process and your organization is always protected. [Help](#)

Upgrading to Secure Access

Generates a new Secure Access organization (organization URL does not change), and copies DNS policies and components to Secure Access policy rules.

Upgrade

- Autorisez la poursuite de la mise à niveau :

Start Upgrade

Clicking Upgrade generates your new Secure Access organization (and dashboard) and copies your Umbrella configurations to Secure Access. Umbrella continues to operate during this process and your organization is always protected. [Help](#)

Upgrading to Secure Access...

You can exit and return to this page at any time. Changes are automatically saved.

- Une fois terminé, vous devez obtenir une page comme sur l'image ici :

Start Upgrade

Done

Clicking Upgrade generates your new Secure Access organization (and dashboard) and copies your Umbrella configurations to Secure Access. Umbrella continues to operate during this process and your organization is always protected. [Help](#)

Upgrade Success.

Your new Secure Access organization has been successfully generated and is now listed in Umbrella's navigation menu. To review your new Secure Access deployment, click Secure Access.



Umbrella DNS policies have been copied and converted to Secure Access policy rules. All deployment and policy components, including identities (sources) and Admin settings, are shared between Secure Access and Umbrella. Any changes to these shared components are automatically updated in the other organization.

Application settings and policy are not shared between the two dashboards, so changes are not reflected between Secure Access and Umbrella.

Umbrella and Secure Access are now running simultaneously, but traffic is only steered through Umbrella. Complete the upgrade process and redirect traffic to Secure Access.

[View rules in Secure Access](#)

Next

8. Rediriger le trafic vers un accès sécurisé

Redirect Traffic

Not Started

[Help](#)

Redirect your organization's identify traffic so that it is steered through Secure Access. You must manually select which identity traffic is upgraded to be steered through Secure Access.



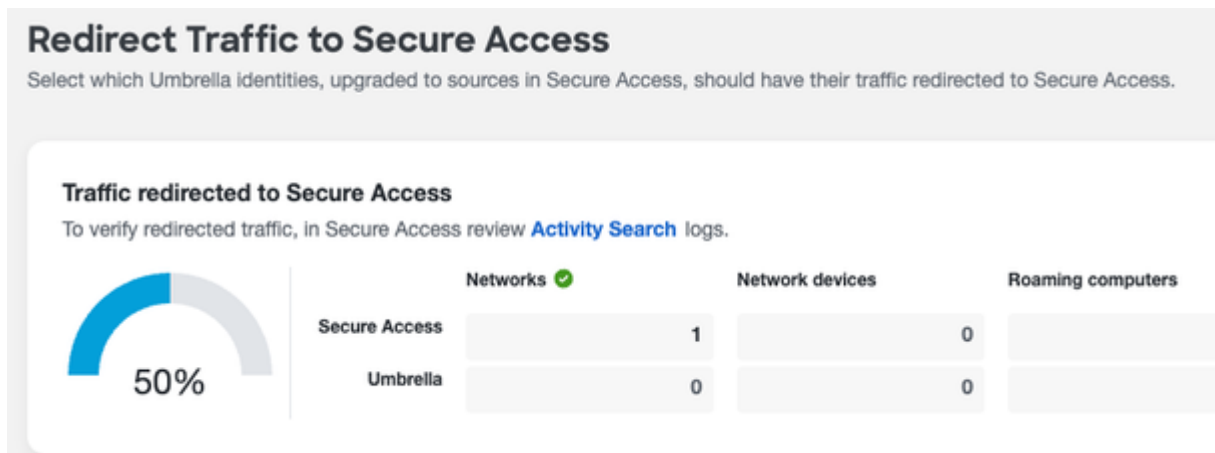
Redirecting traffic to Secure Access

Upgrades traffic steering so that Identity (Source) traffic is steered through Secure Access.

Start

- Confirmation de la redirection en cours. Dans l'exemple, seule l'identité réseau a été migrée

d'Umbrella vers Secure Access :



9. Terminez la mise à niveau et la migration vers Secure Access

 **Mise en garde :** Cela supprime complètement votre organisation Umbrella et n'est pas réversible donc assurez-vous que tous les éléments ont été complètement migrés avant d'effectuer cette étape.



- Lorsque vous sélectionnez Close Umbrella sur l'image ici, vous allez perdre l'accès à votre organisation parapluie comme il est supprimé :



Complete Upgrade and Close Umbrella

Are you sure you want to close your Umbrella account? Once closed, all access to Umbrella is lost and cannot be recovered.

☒ I understand and wish to proceed

[Cancel](#)

[Close Umbrella](#)

Vérifier la migration

1. Connectez-vous à [Secure Access](#) avec vos identifiants de connexion
2. Accédez à Secure > Access Policy pour afficher les règles migrées, comme dans l'exemple ci-dessous. L'ID d'organisation doit être identique à celui de la section Prepare for Migration ci-dessus.

← → ↻ dashboard.sse.cisco.com/org/8350166/secure/policy

Secure Access

Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. [Help](#)

Search by rule name [Filters](#)

Migrated org ID intact

Migrated DNS policy

5 Rules

	☐	# ⓘ	Rule name	Action	Access	Sources	Destinations
⋮	☐	1	3/3 DNS-only-policy-1 (U...	✓ Allow	Internet	Any AD Group... +1	Global Allow...
⋮	☐	2	2/3 DNS-only-policy-1 (U...	✗ Block	Internet	Any AD Group... +1	Alcohol +26
⋮	☐	3	1/3 DNS-only-policy-1 D...	✓ Allow	Internet	Any AD Group... +1	Any

Informations connexes

- [Documentation générale](#)
- [Assistance et documentation techniques - Cisco Systems](#)

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.