

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 n'est pas pris en charge actuellement (au moment de la création de cet article).

Conditions préalables

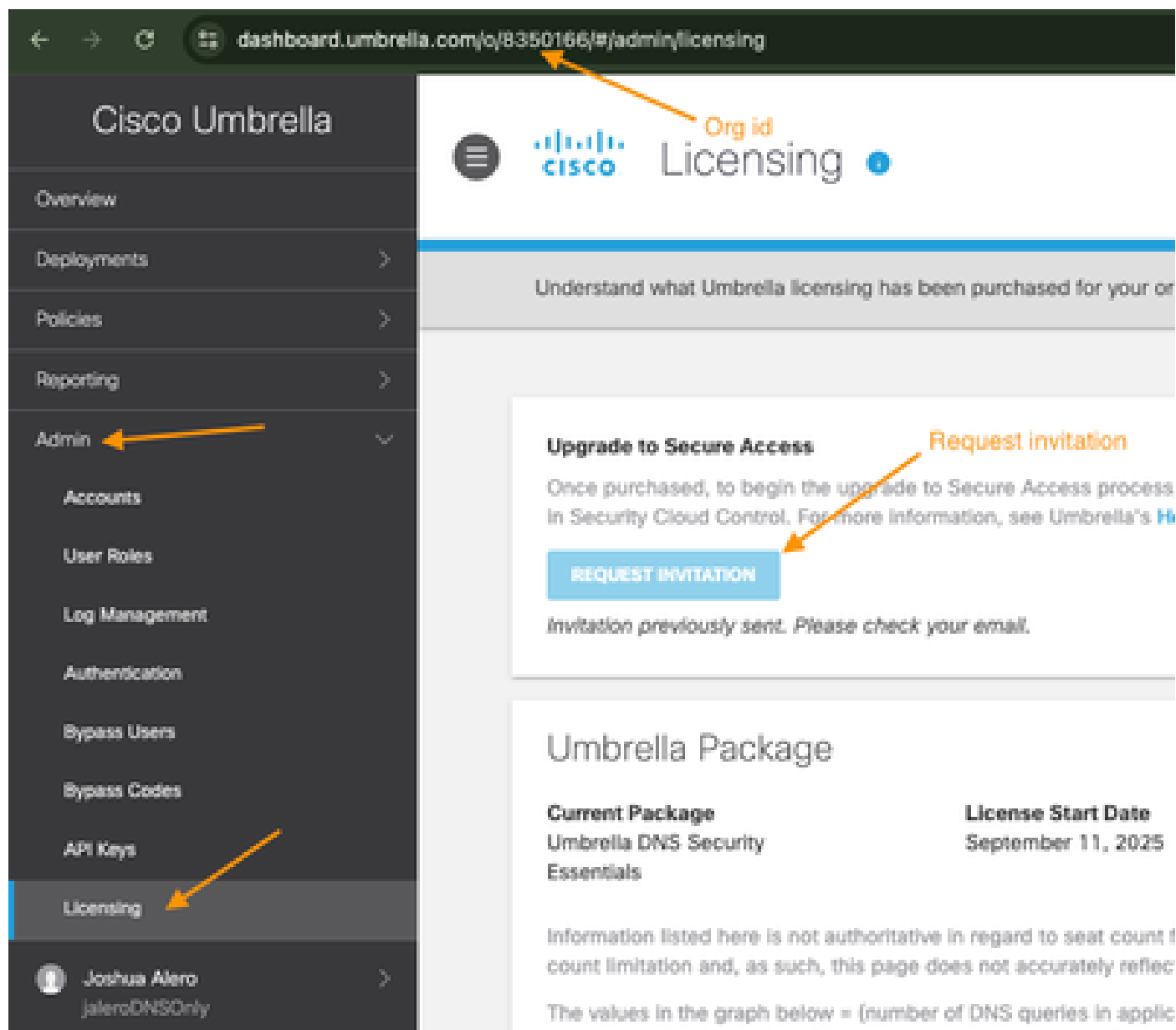
- Abonnement DNS ou SIG actuel
- Accès administrateur complet à Umbrella
- Accès au contrôle du cloud de sécurité

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 :

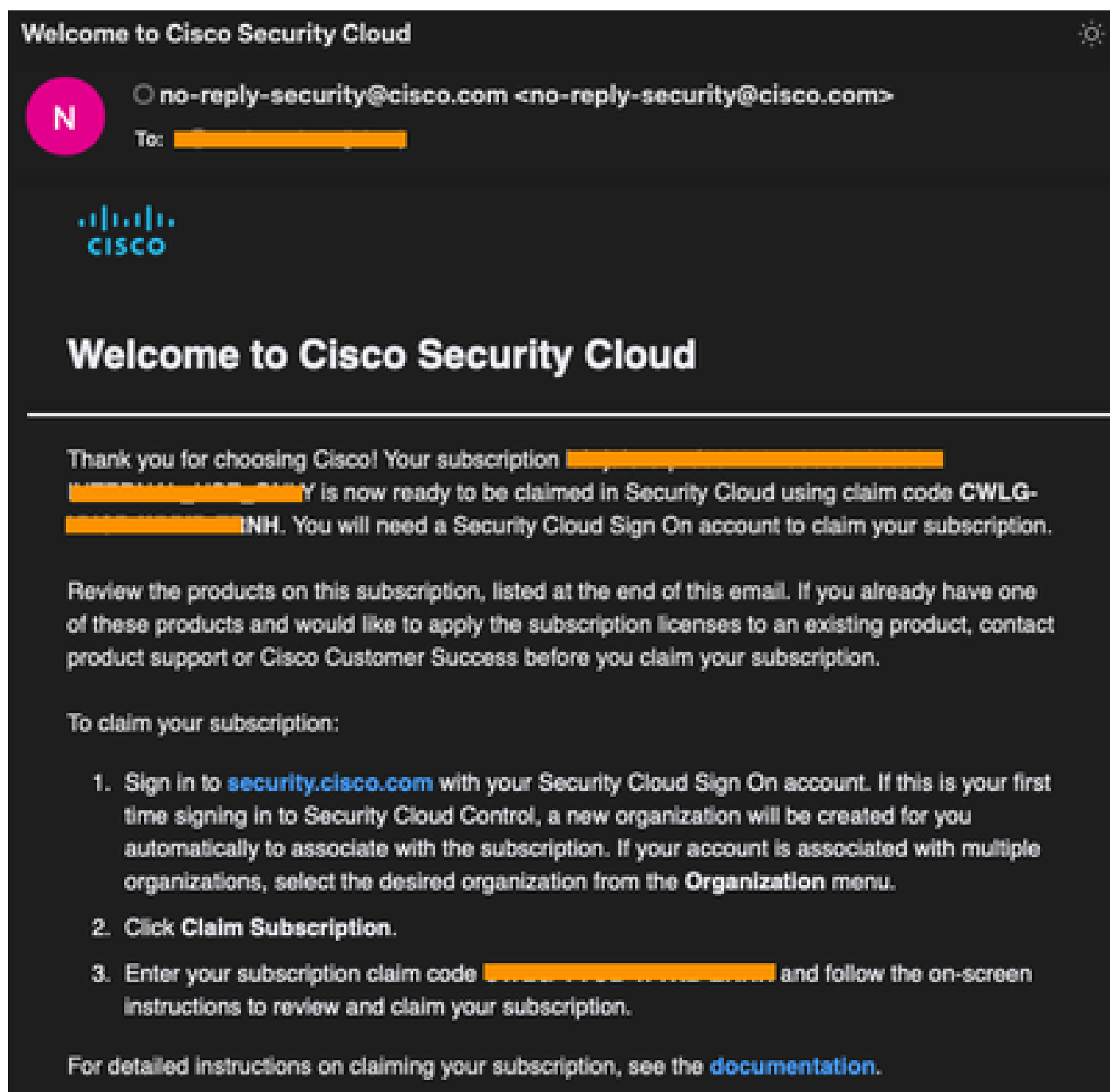


ii. Notez l'ID d'organisation, dans cet exemple 8350166.

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

 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. Attendez 3 à 4 jours ouvrables et vous devez recevoir un e-mail avec votre code de demande d'abonnement. 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

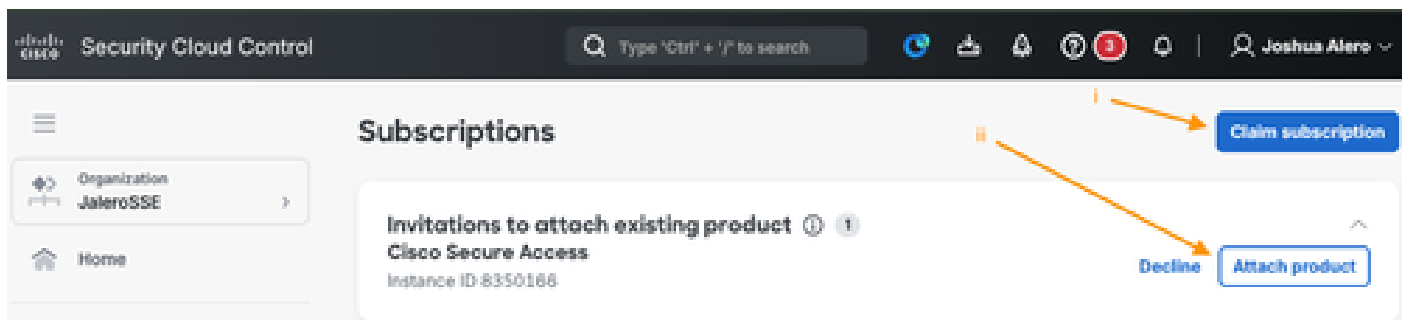
i. Cliquez sur le bouton Demande d'abonnement pour la demander avec les codes fournis à l'étape 1 ci-dessus.

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

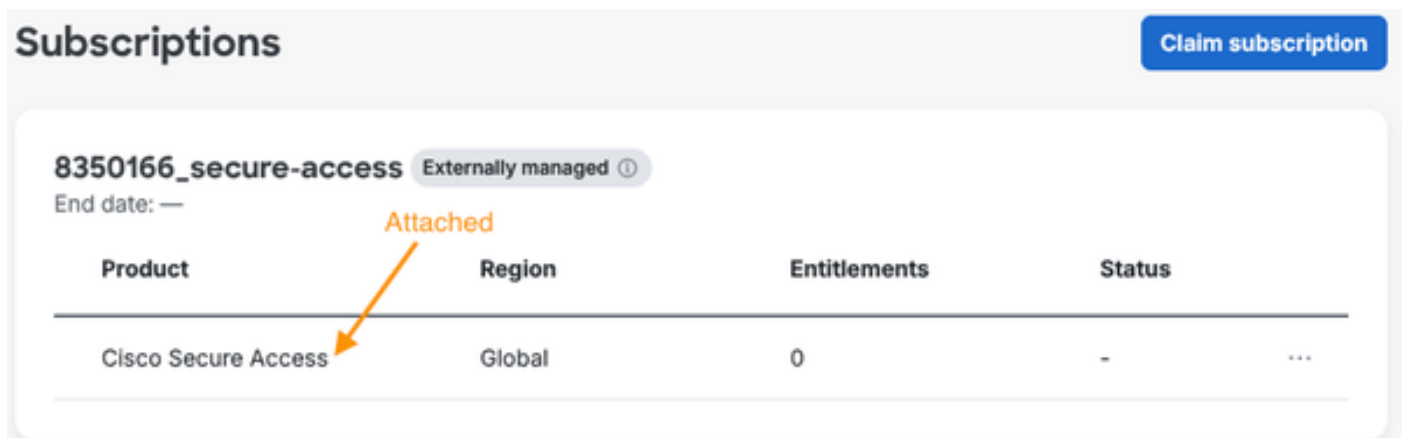
 Remarque : L'ID d'organisation Umbrella doit être identique à celui figurant sur votre tableau



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 :



- iii. Entrez le code de demande et sélectionnez Next :

Claim Subscription

The screenshot shows the first step of a three-step process. On the left, a sidebar lists the steps: 1. Enter subscription claim code (active), 2. Review products, and 3. Review subscription. The main area is titled 'Enter subscription claim code' and contains instructions to enter a claim code and click 'Next'. A text input field is labeled 'Subscription claim code *' and contains the text 'ZRNH'. At the bottom, there are three buttons: a back arrow, a 'Cancel' button, and a 'Next' button. An orange arrow points to the 'Next' button.

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 :

The screenshot shows the second step of the process. The sidebar now has '2 Review products' as the active step. The main area is titled 'Review products' and contains instructions to choose 'Attach existing instance' from a dropdown menu. A table lists products, with 'Cisco Secure Access DNS Advantage' selected. The dropdown menu for this product is open, showing 'Attach existing instance'. At the bottom, there are four buttons: a back arrow, a 'Cancel' button, a 'Back' button, and a 'Next' button. Two orange arrows point to the 'Attach existing instance' dropdown and the 'Next' button.

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
Organization
region
Europe

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

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.

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

1. 2010年10月1日起，凡在中华人民共和国境内销售货物或者提供加工、修理修配劳务以及进口货物的单位和个人，均应按照《中华人民共和国增值税暂行条例》及实施细则缴纳增值税。

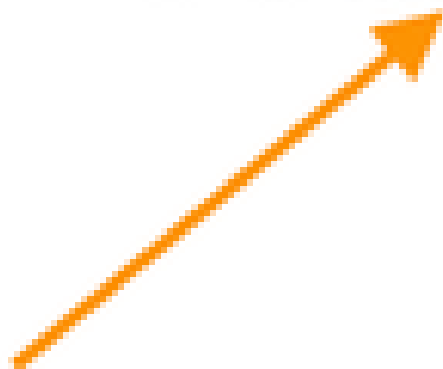
2. 2010年10月1日起，凡在中华人民共和国境内销售货物或者提供加工、修理修配劳务以及进口货物的单位和个人，均应按照《中华人民共和国增值税暂行条例》及实施细则缴纳增值税。

3. 2010年10月1日起，凡在中华人民共和国境内销售货物或者提供加工、修理修配劳务以及进口货物的单位和个人，均应按照《中华人民共和国增值税暂行条例》及实施细则缴纳增值税。

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



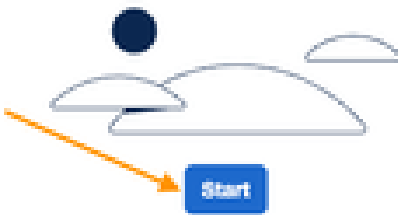
 : Cela supprime complètement votre organisation Umbrella et n'est pas réversible donc assurez-vous que tous les éléments ont été complètement migrés avant d'effectuer cette étape.

4

Complete Upgrade and Close Umbrella

Not Started

Umbrella has been successfully upgraded and selected traffic is now being steered through Secure Access. The last step in the Upgrade process is to permanently shut down Umbrella and cancel your Umbrella subscription. [Help](#)



- 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.