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

## Table des matières



## 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

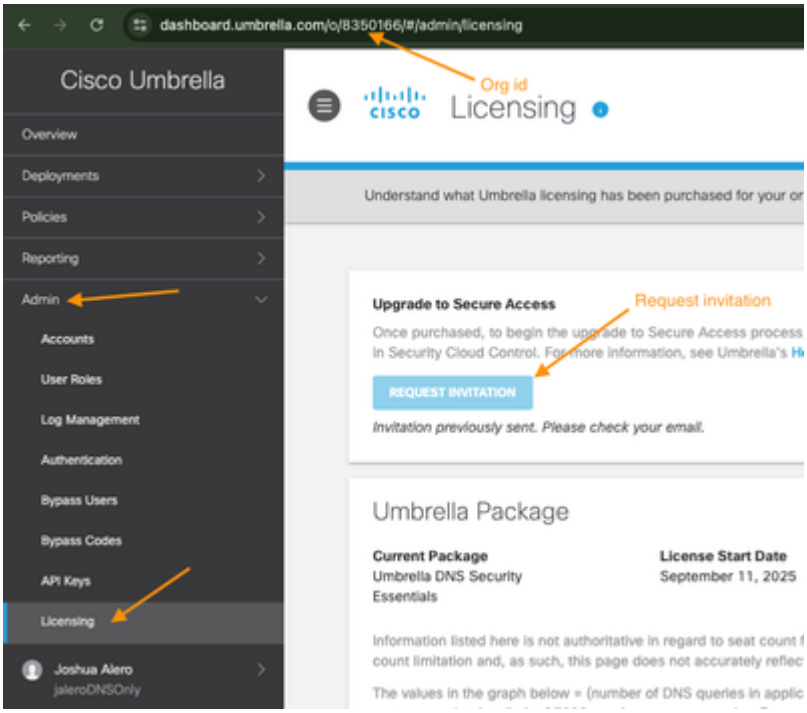
- Abonnement DNS ou SIG actuel
- Accès administrateur complet à Umbrella
- Accès au contrôle du cloud de sécurité

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.

---

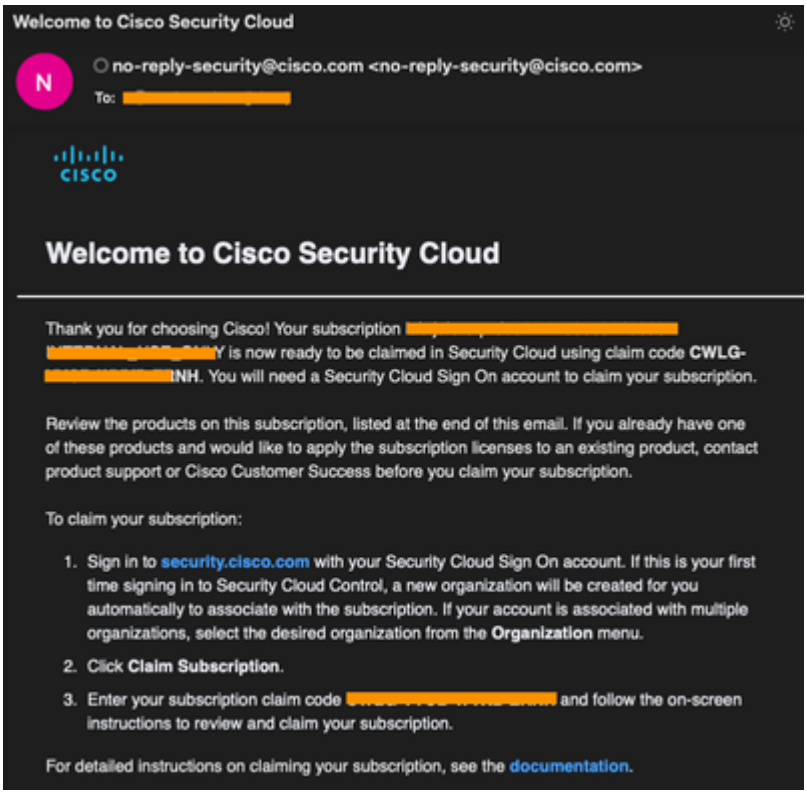
Important : Le bouton Request Invitation sert d'invitation à rejoindre le locataire Umbrella pour SCC. Il ne génère pas de code de revendication. Un code de demande vous sera fourni une fois votre commande d'accès sécurisé terminée. Cela fait partie du processus de migration vers un accès sécurisé.

---

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.

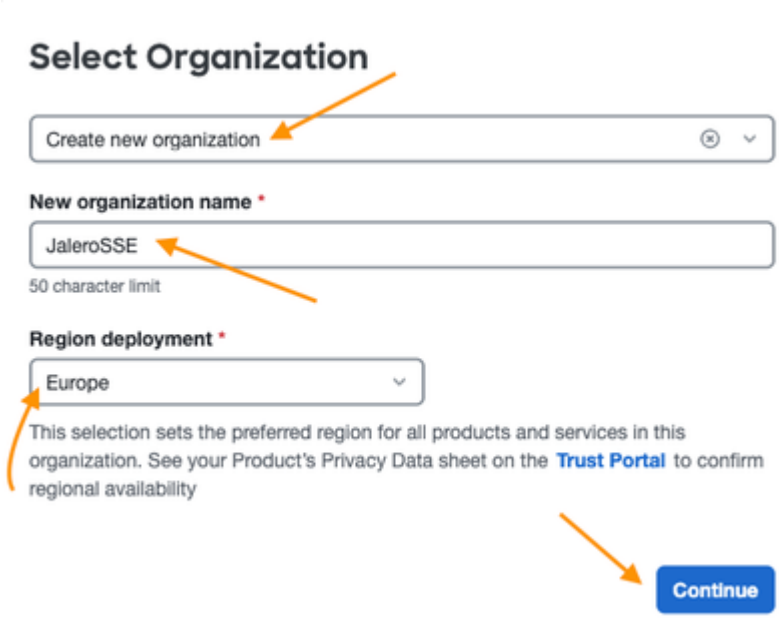
iv. Sélectionnez la région appropriée dans le menu déroulant Déploiement de la région.

---

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

---

Exemple ici :




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

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

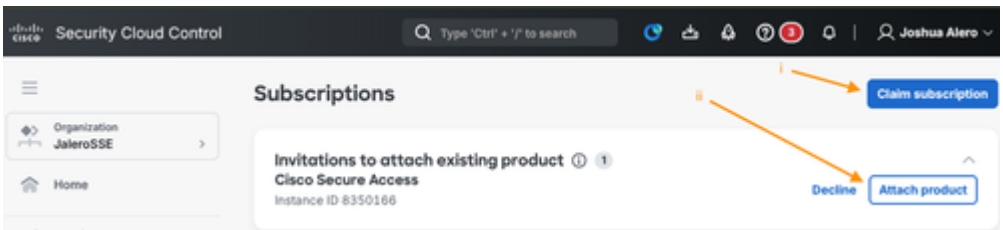
i. Cliquez sur le bouton Demande d'abonnement pour la demander avec les codes fournis à l'étape 1 ci-dessus.

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

---

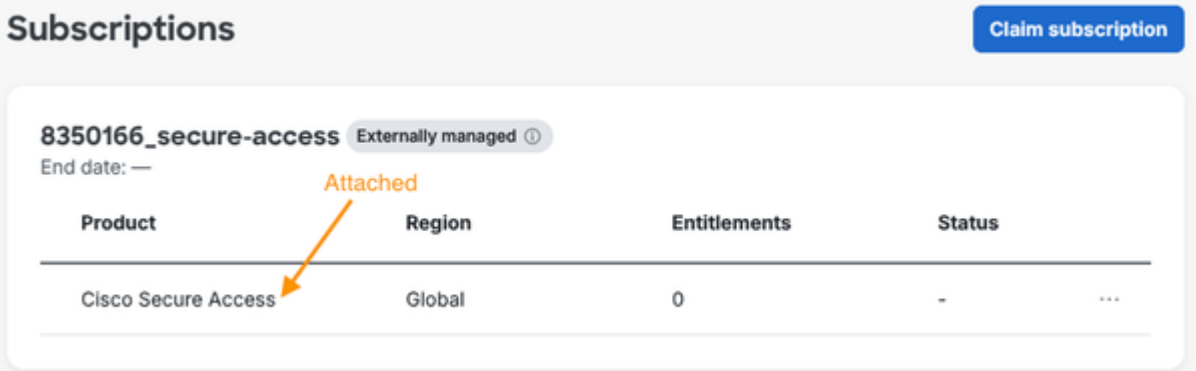
Remarque : L'ID d'organisation Umbrella doit être identique à celui figurant sur votre tableau de bord Umbella. Cela est important pour la migration et pour s'assurer que SCC et Umbrella ont été liés.

---

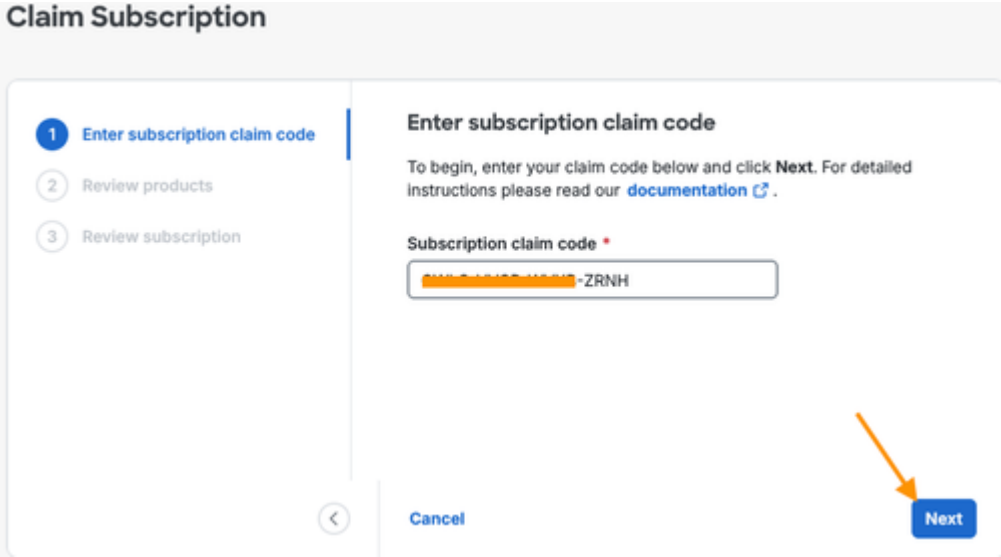



- Sélectionnez Joindre un produit pour joindre votre organisation-cadre au SCC.

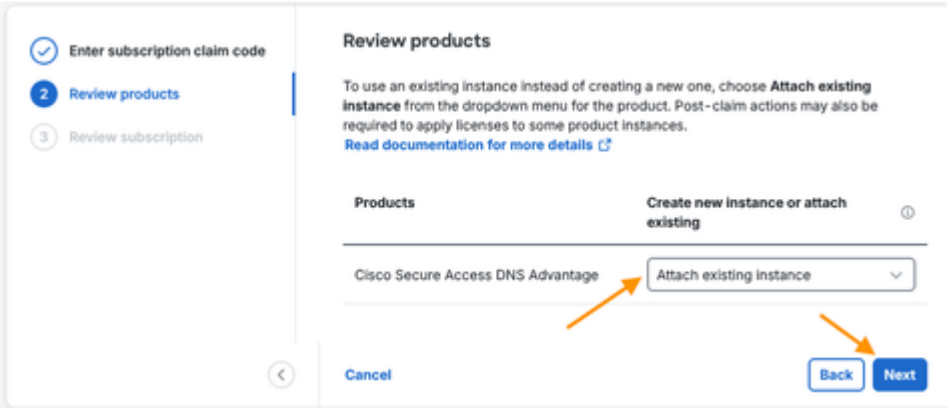
- Une fois joint, vous devez voir le Cisco Secure Access en tant que produit dans la même page comme indiqué sur l'exemple ici :




iii. Entrez le code de demande et sélectionnez Next :

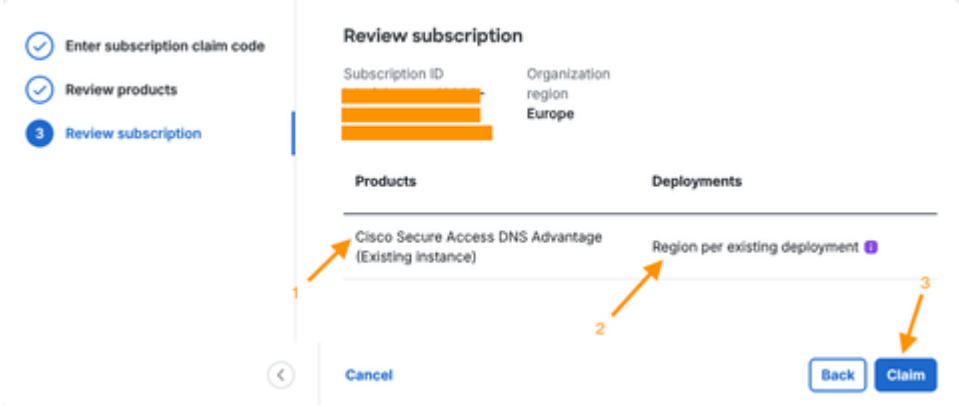



iv. Sélectionnez Attacher une instance existante dans le menu déroulant Créer une nouvelle instance ou attacher une instance existante :

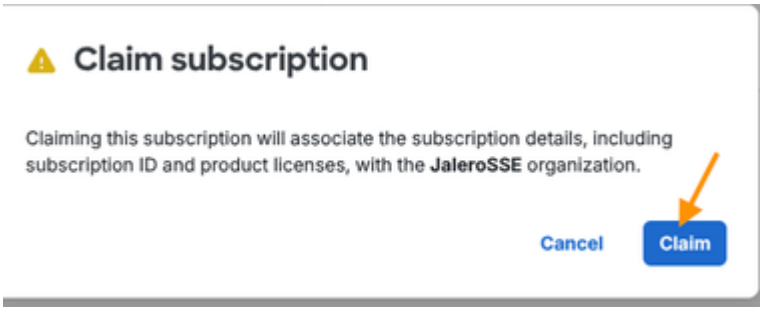



v. Vérifiez les paramètres :

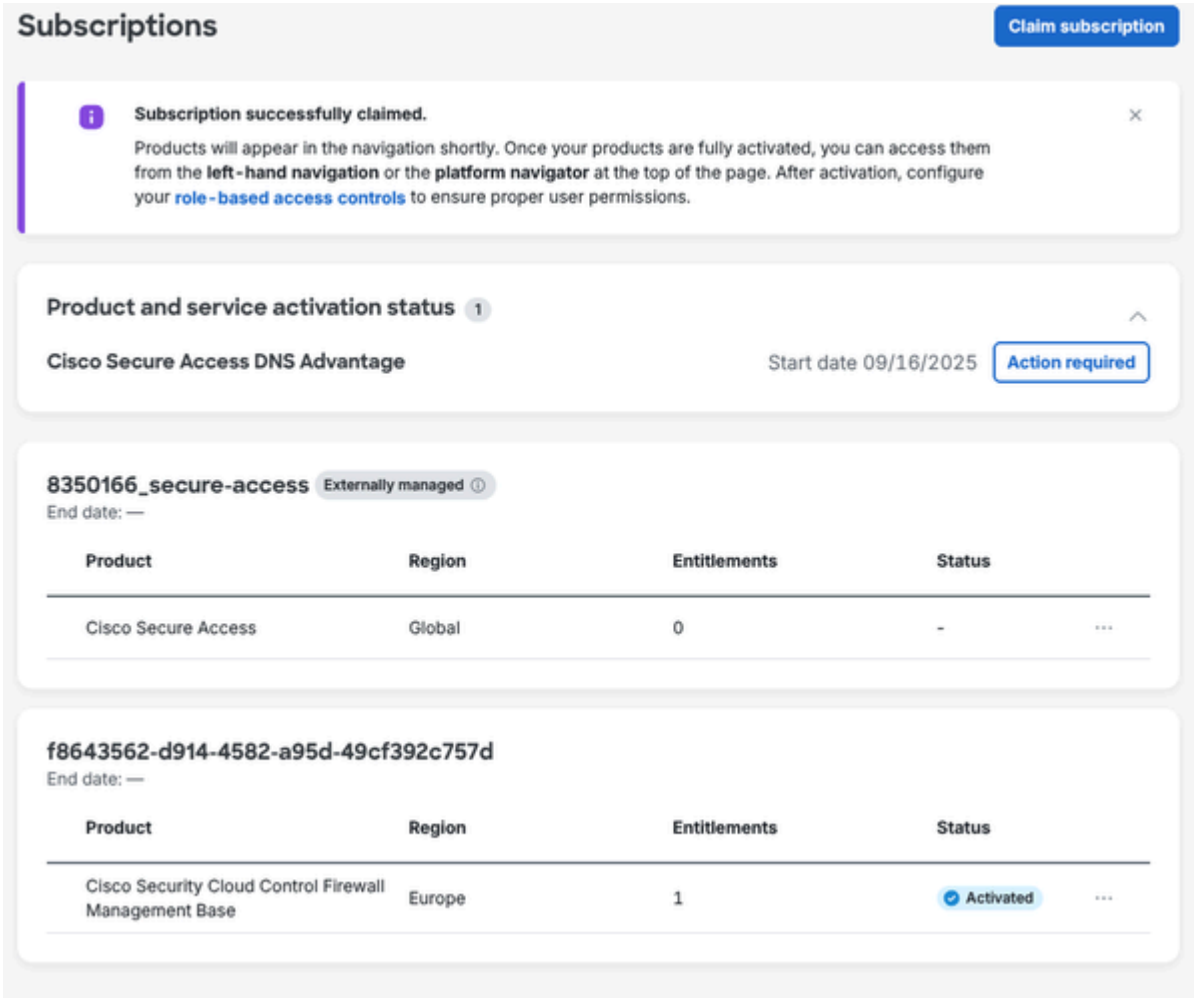
- Assurez-vous que le (instance existante) fait partie du nom du produit
- La région doit être définie sur la région existante de l'instance d'accès sécurisé connectée
- Sélectionnez Déplacer la demande pour passer à la page suivante




- Confirmez la demande d'abonnement :

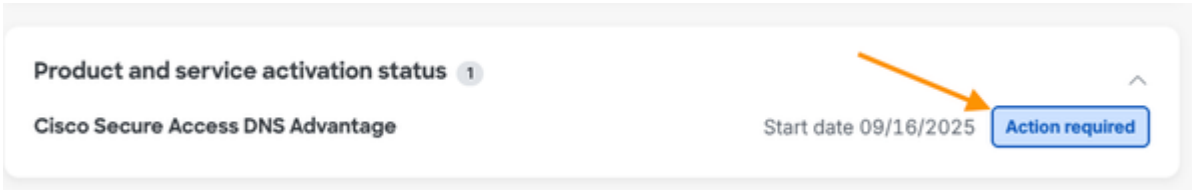



- Une fois la demande et le provisionnement réussis, vous devez obtenir une page Abonnements similaire à celle-ci, montrant tous vos produits activés :

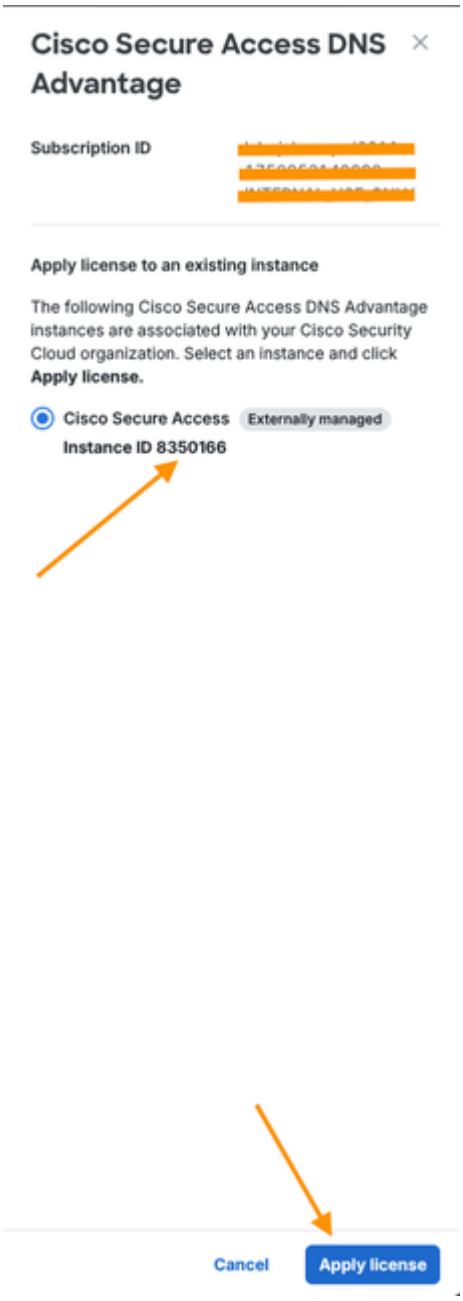



## 4. Appliquez la licence à Secure Access Instance

i. Sélectionnez l'option Action requise :




ii. Sélectionnez Appliquer la licence :

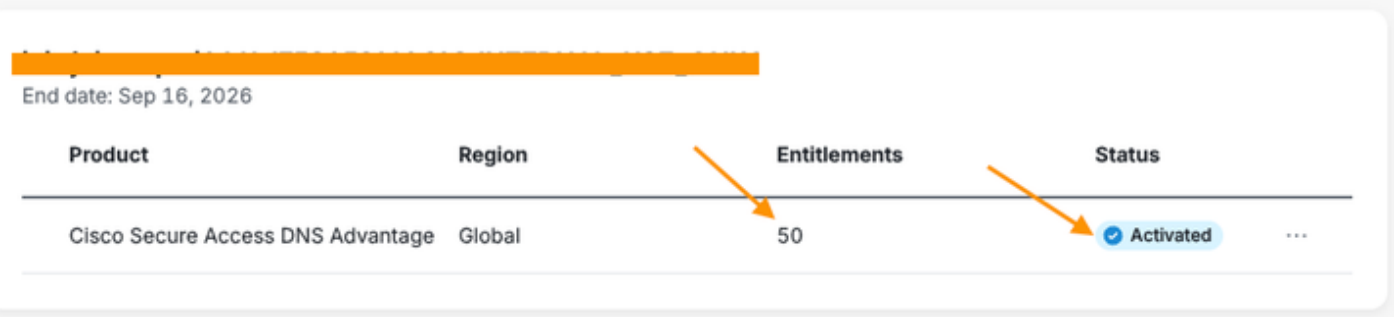



# Vérification de la liaison d'accès sécurisé vers SCC

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

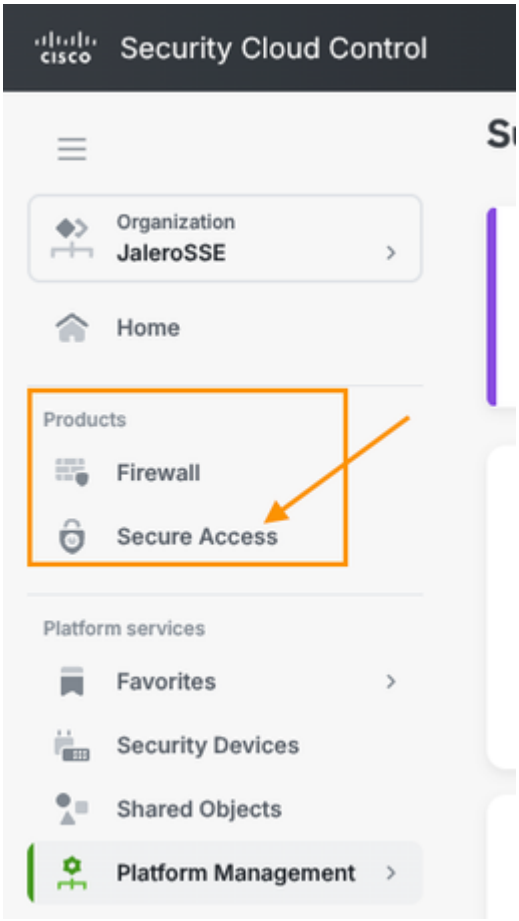
## 1. État d'activation du produit dans les abonnements

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



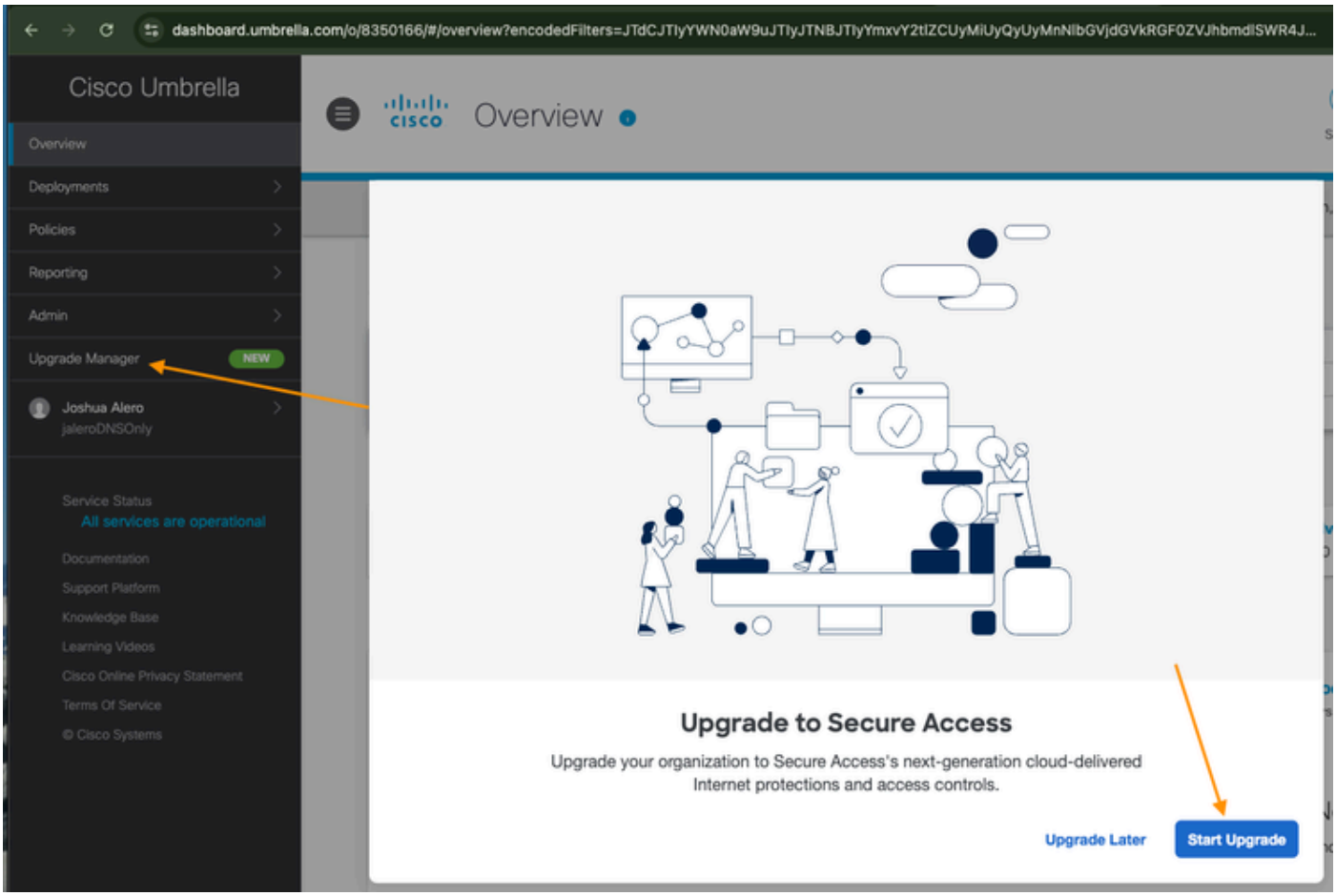

### 2. Accès sécurisé dans la liste des produits

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

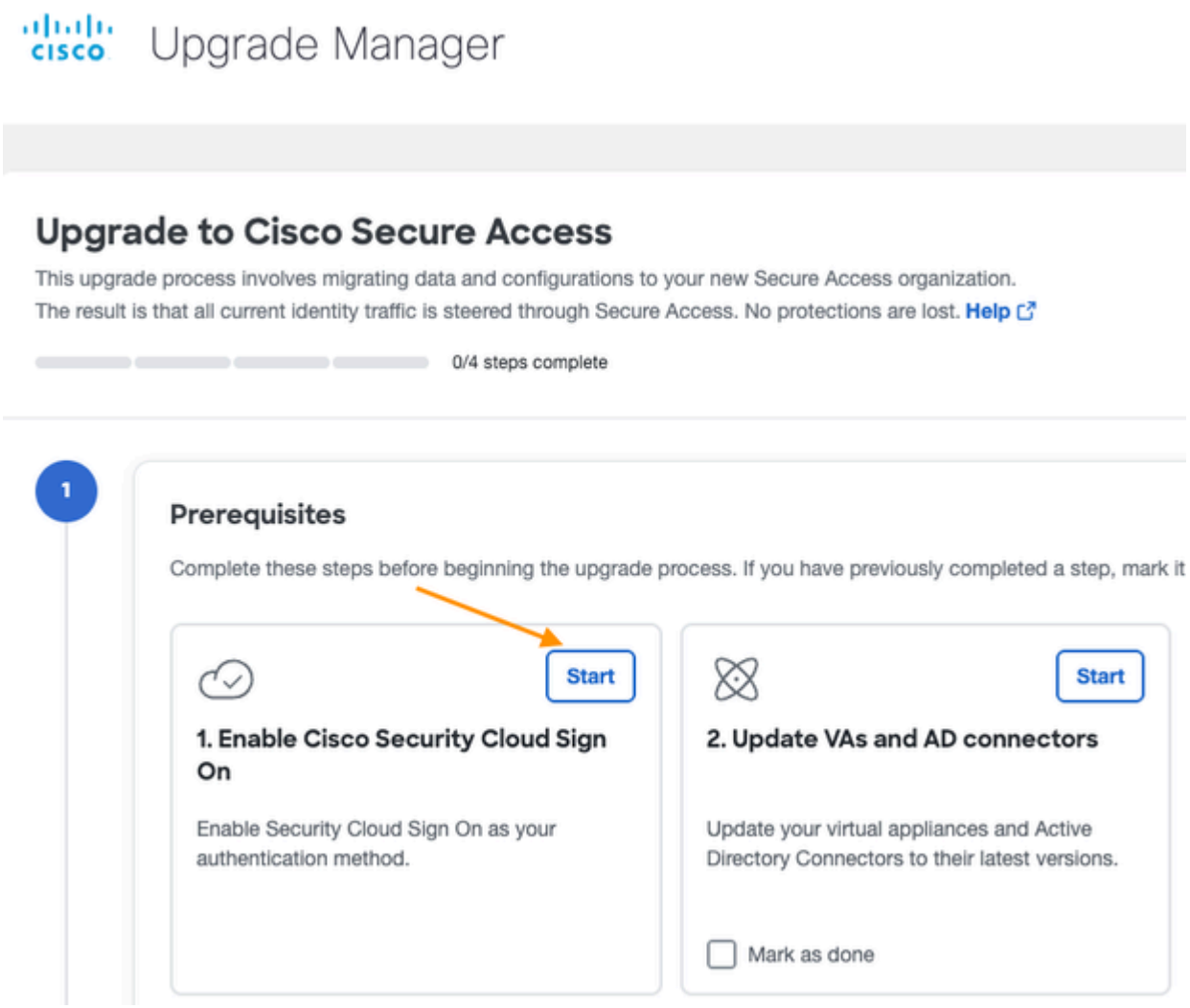



## Migration d'Umbrella vers un accès sécurisé

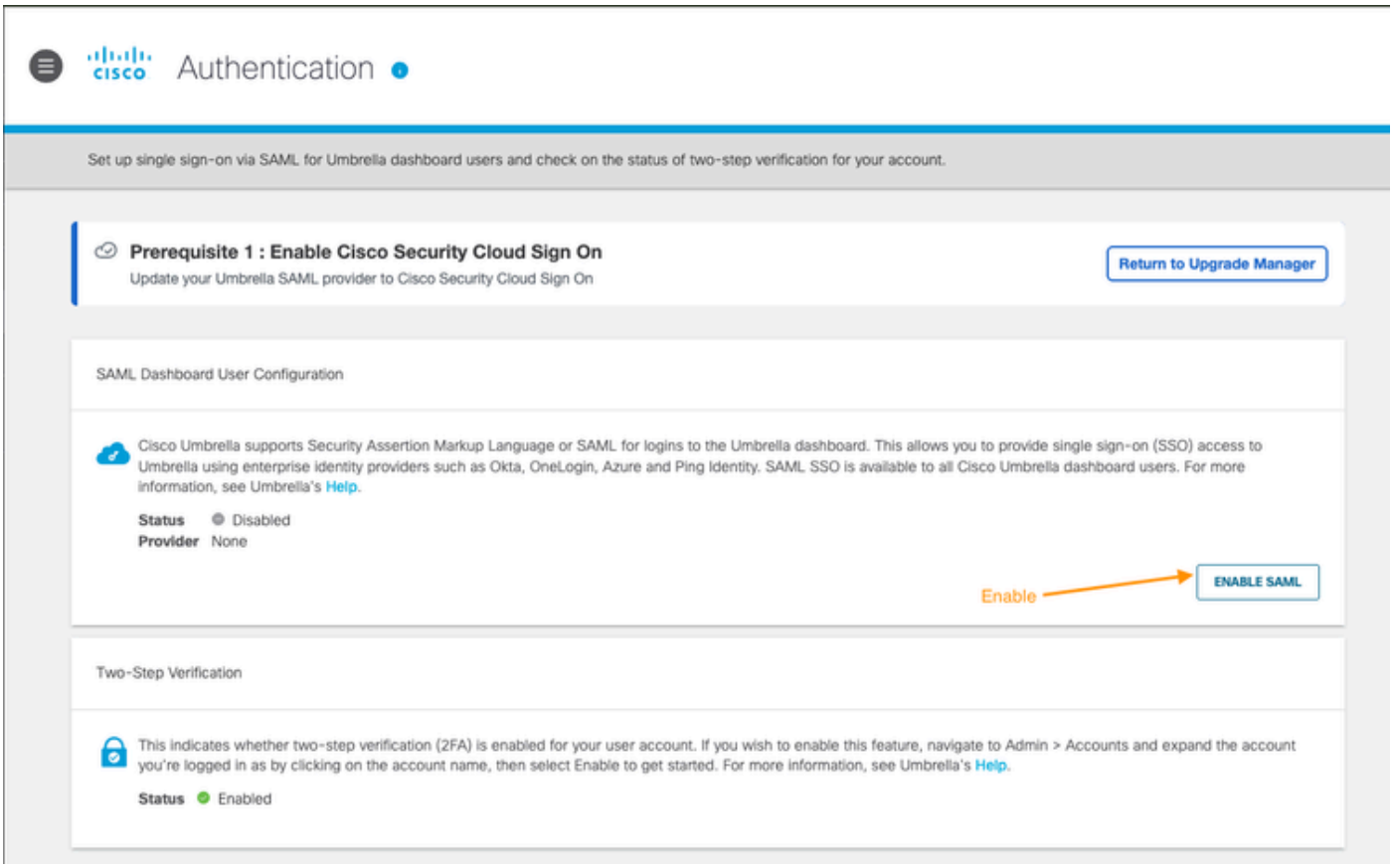
1. Reconnectez-vous à Umbrella avec le même compte que ci-dessus.
2. Accédez au nouvel élément de menu Gestionnaire de mise à niveau :



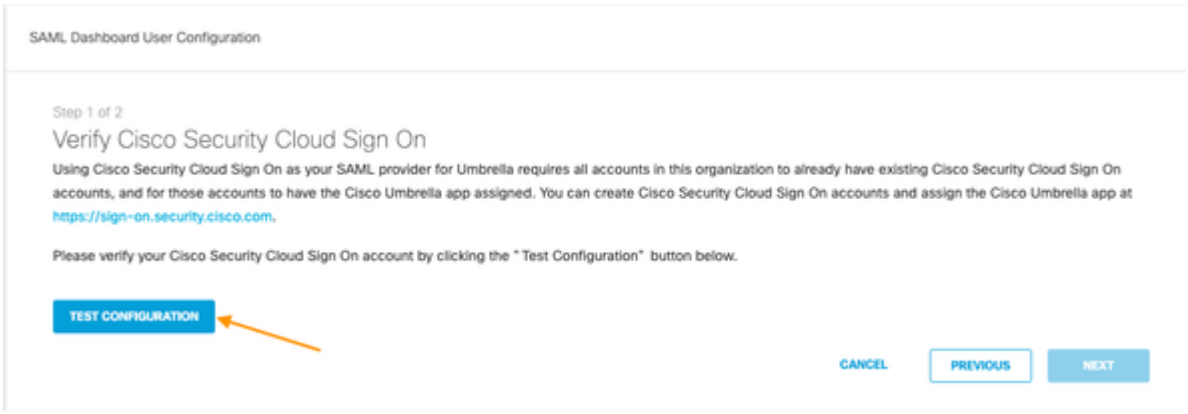

3. Dans la page Gestionnaire de mise à niveau, sélectionnez Démarrer sous Activer la connexion au cloud de sécurité Cisco




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 :

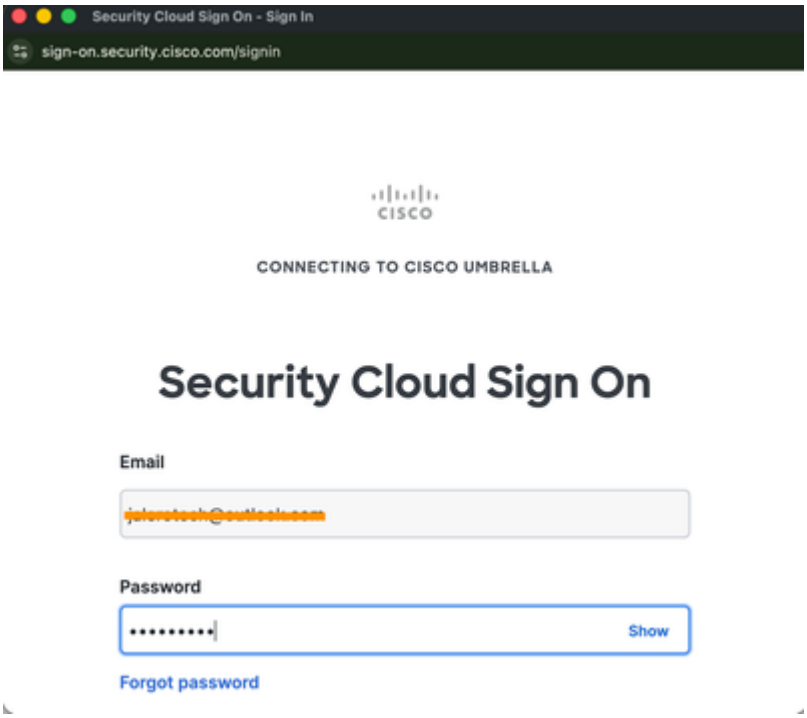


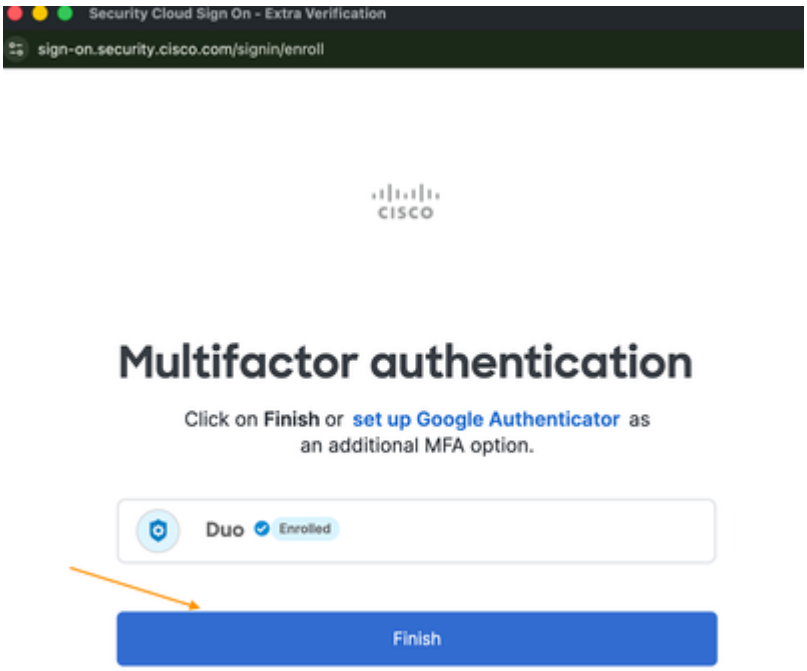

5. Testez la configuration SAML avec l'option TEST CONFIGURATION :



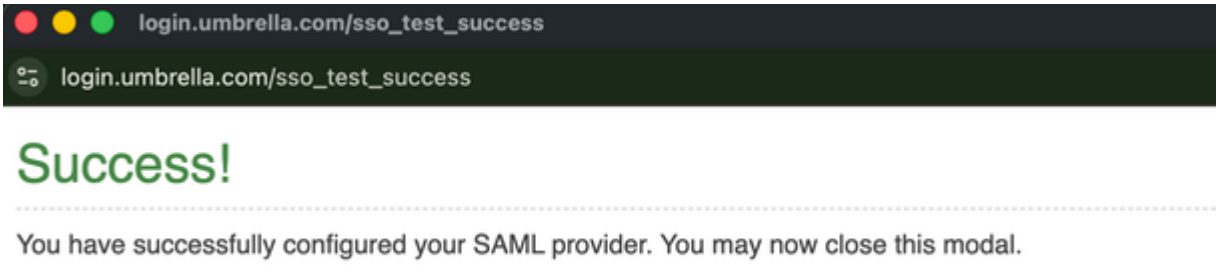

6. La page de connexion de SCC doit apparaître dans une autre fenêtre contextuelle (assurez-vous que le bloqueur de fenêtres contextuelles est désactivé) :

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



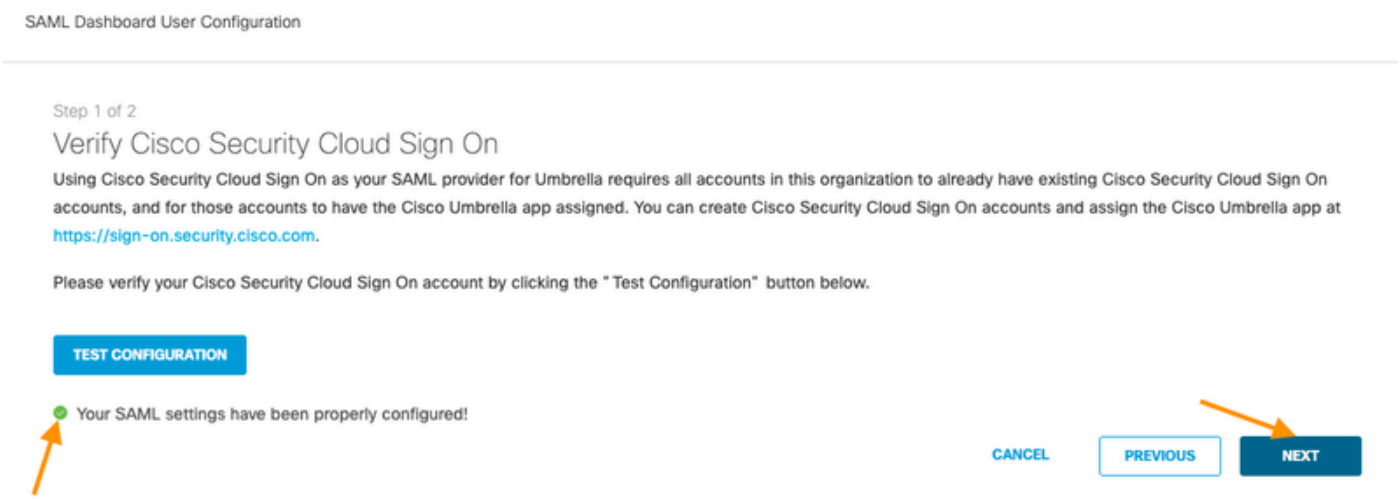




Lorsque la connexion a été vérifiée, vous devez obtenir le message ici, le confirmant. À ce stade, la partie SAML est presque terminée :

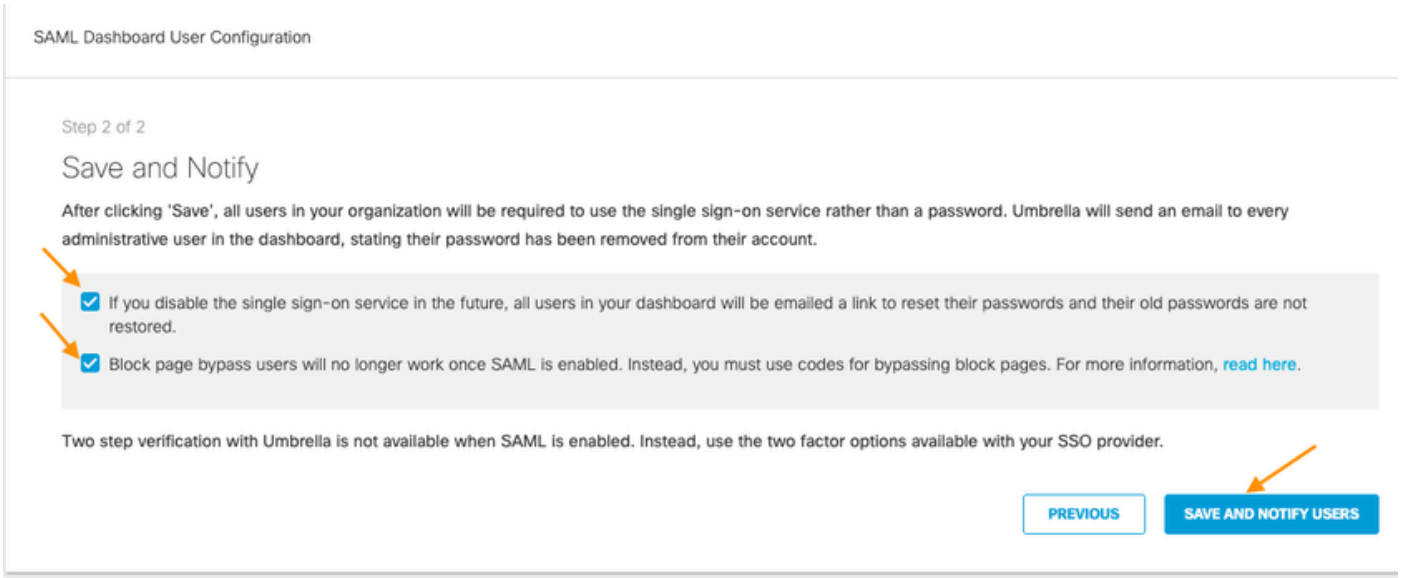


Vous devez ensuite revenir à la partie SAML Dashboard User Configuration :

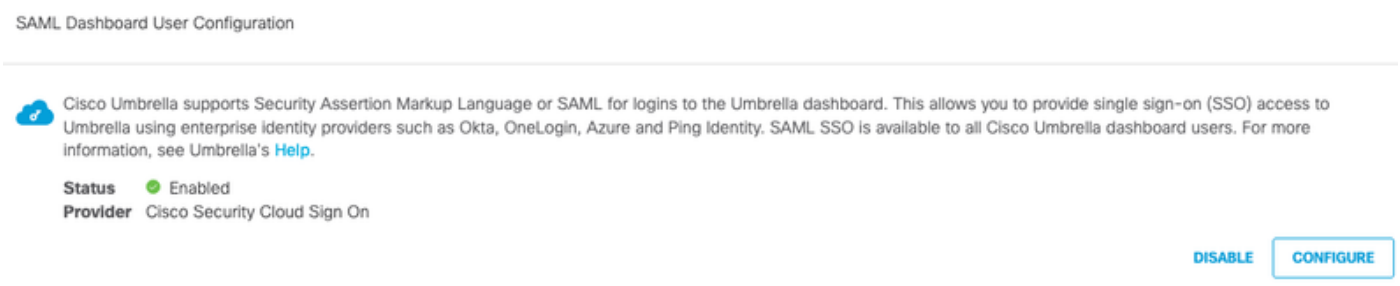
- La coche verte indique que les paramètres SAML ont été correctement configurés
- Sélectionnez NEXT pour continuer




Enregistrez les modifications et avertissez les utilisateurs :

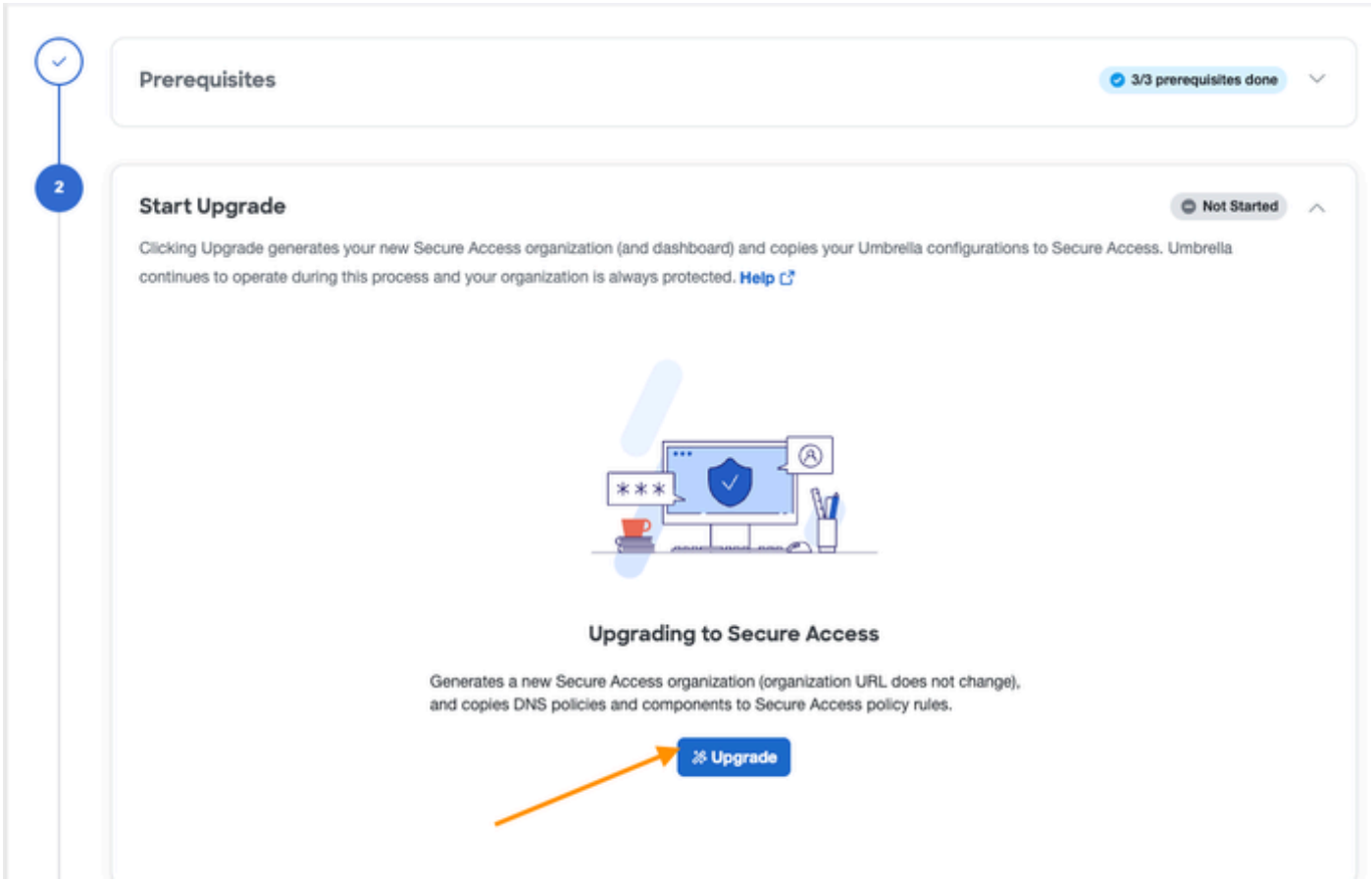



Configuration SAML terminée :

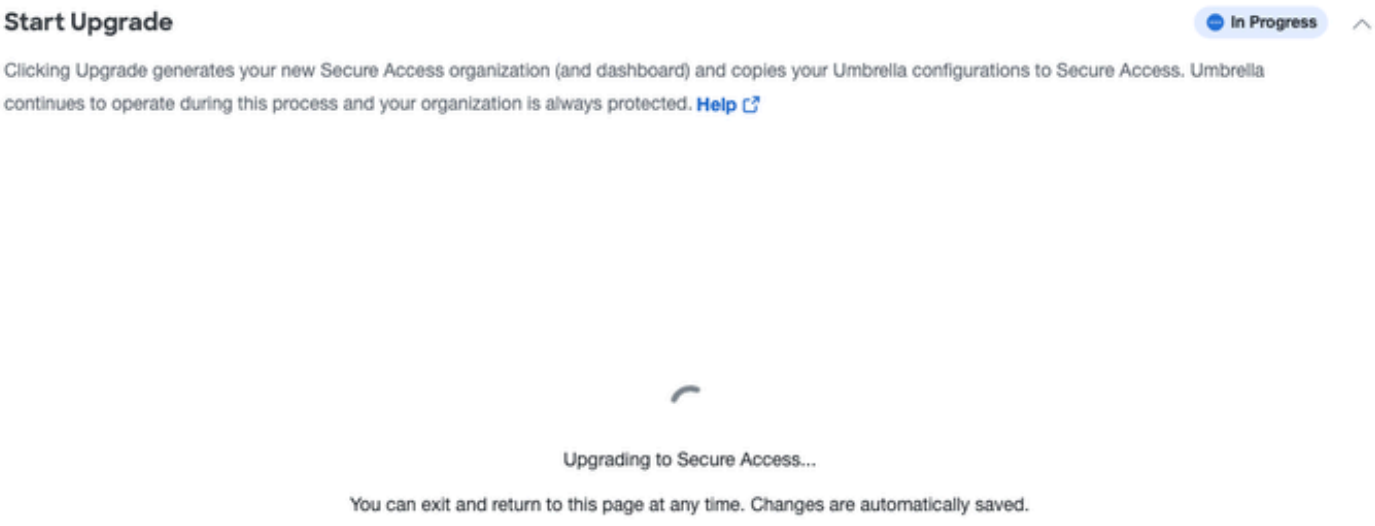



7. Effectuez la mise à niveau vers Secure Access en sélectionnant Upgrade dans la section Start

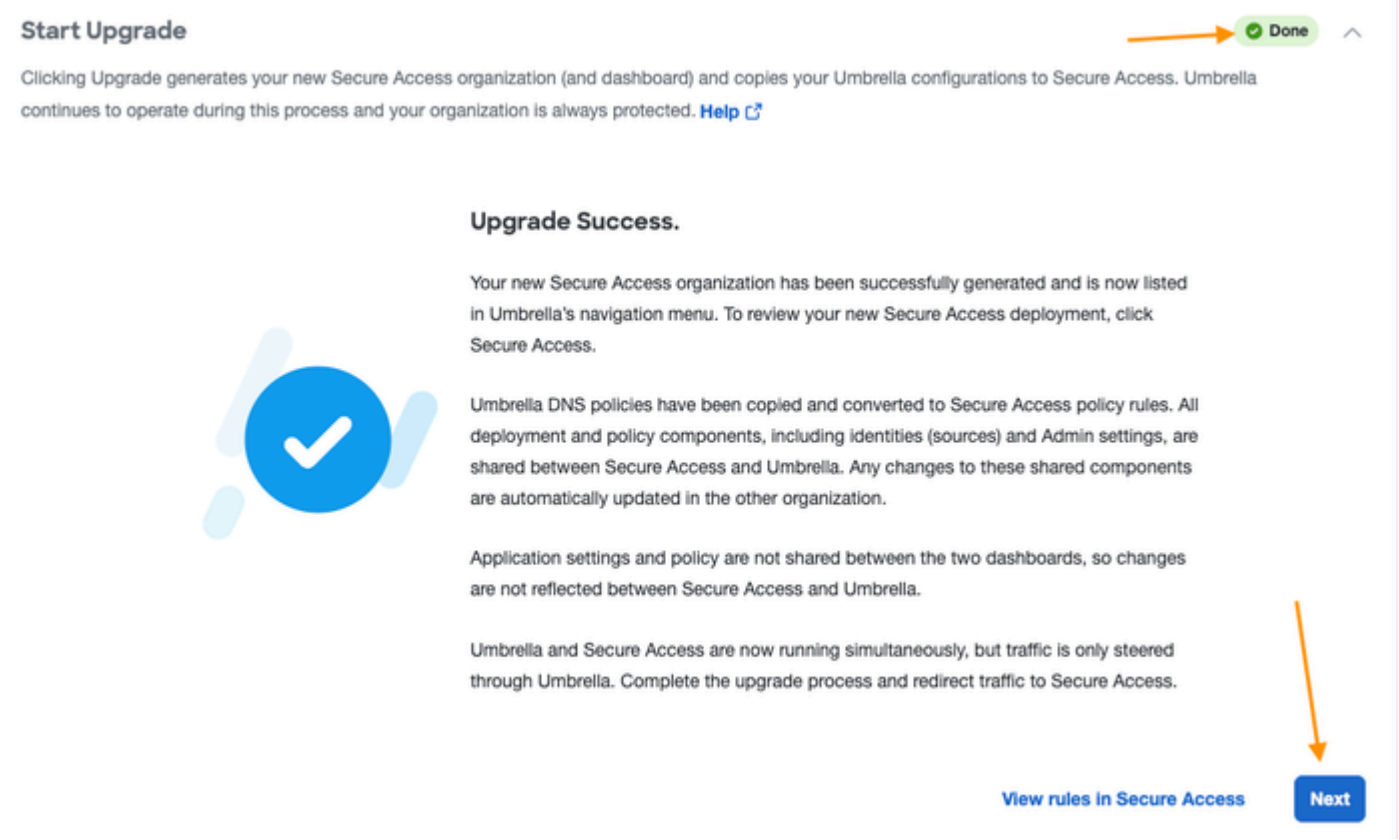
Upgrade :



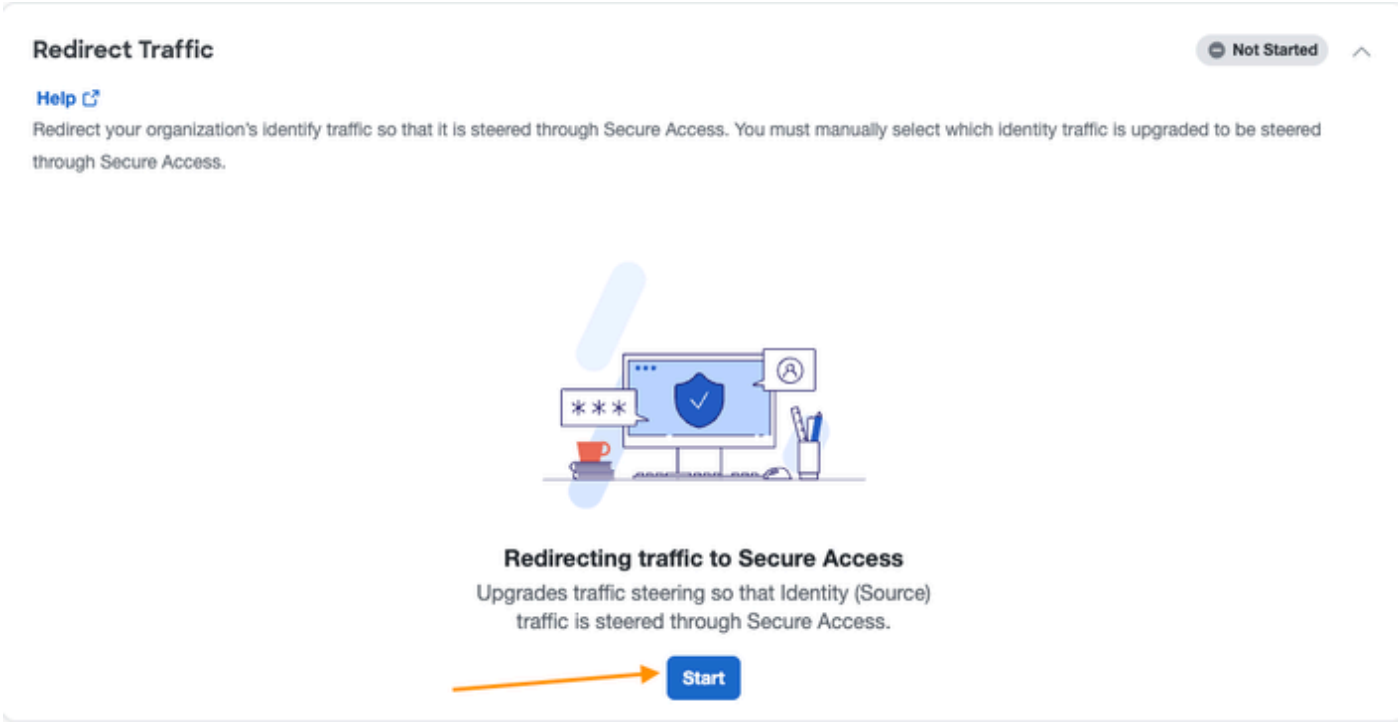

- Autorisez la poursuite de la mise à niveau :




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

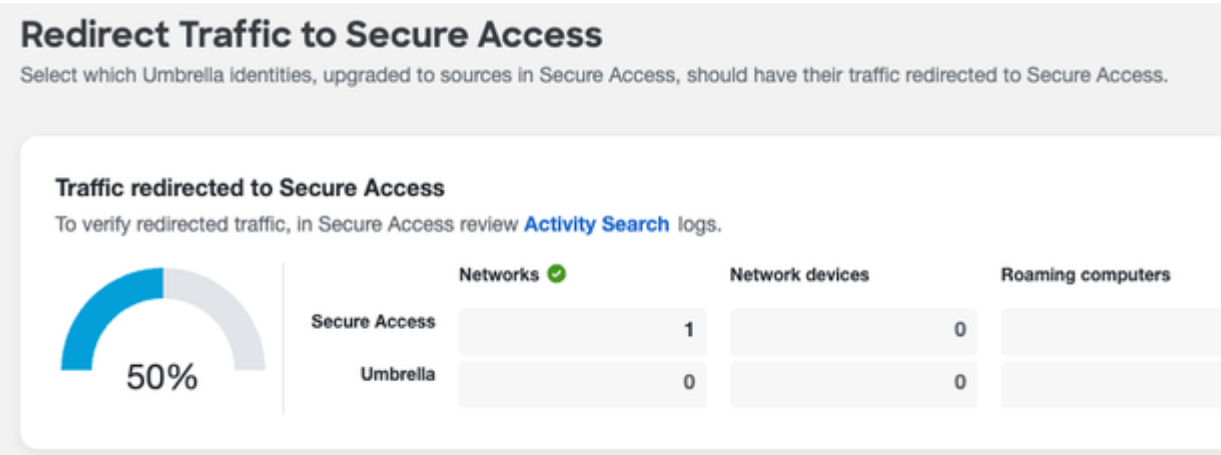



8. Rediriger le trafic vers un accès sécurisé




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

d'Umbrella vers Secure Access :



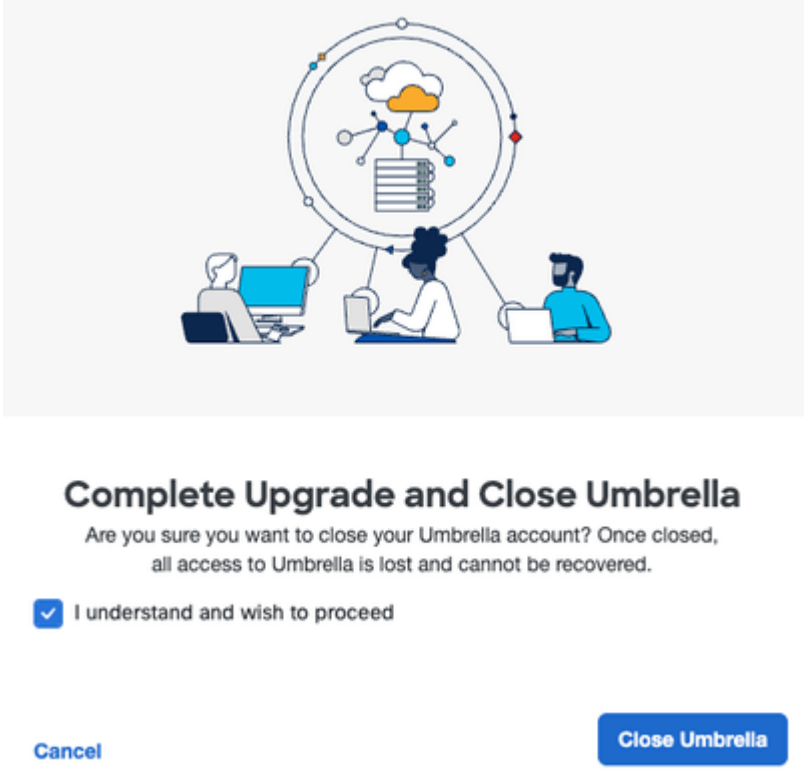

9. Terminez la mise à niveau et la migration vers Secure Access

---

⚠ 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.

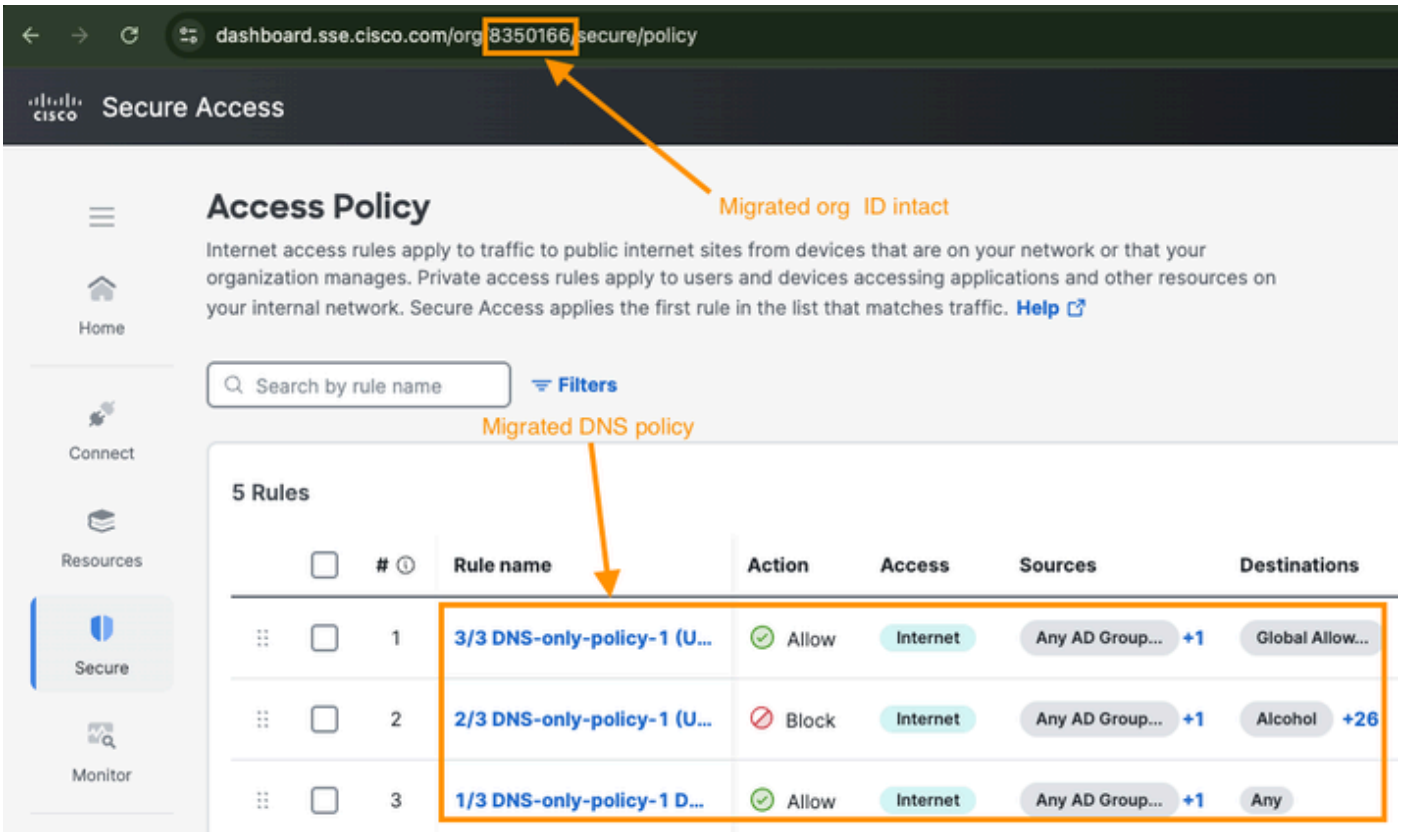
---


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




## 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.




## 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.