# 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 parapluie au SCC et demander un abonnement
- 4. Appliquer la licence à l'instance d'accès sécurisé

Vérification de la liaison d'accès sécurisé vers SCC

- 1. Statut 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

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

La migration vers Mutli-org et MSSP sort du cadre de cet article. Pour la migration multi-organisations et MSSP, veuillez vous référer à Umbrella Multi-org Console Upgrade to Secure Access Manager Organization.

## Conditions préalables

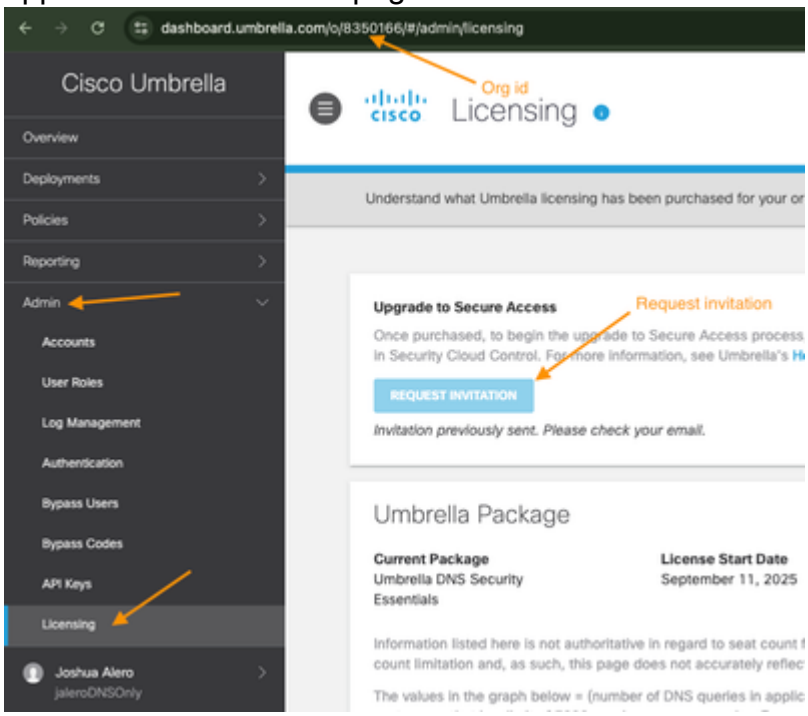
- Abonnement DNS ou SIG actuel
- Accès administrateur complet à Umbrella
- Accès au contrôle du cloud de sécurité

# Étapes de préparation

## 1. Préparer la migration

Assurez-vous de disposer d'un abonnement DNS ou SIG sur Umbrella :

1. Accédez à Admin > Licensing pour vérifier. La mise à niveau vers un accès sécurisé doit apparaître en haut de la page :




2. Notez l'ID d'organisation, dans cet exemple 8350166.
3. Sélectionnez l'option Demander une invitation sur la page de licence.

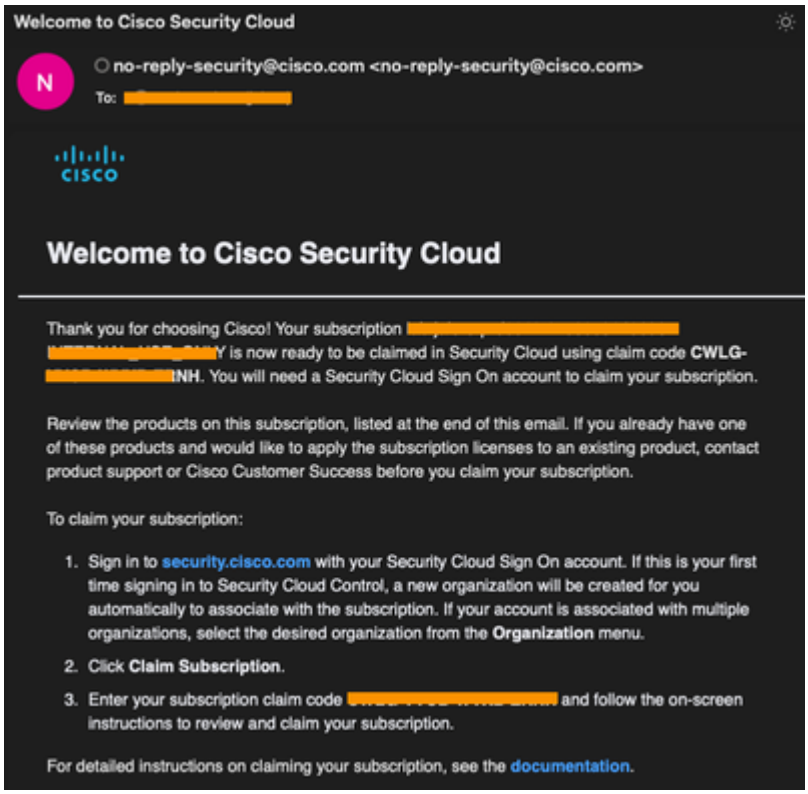
> Important : Le bouton Request Invitation sert d'invitation à rejoindre le locataire Umbrella pour SCC. Il ne génère pas de code de revendication. Un code de demande vous est fourni une fois votre commande d'accès sécurisé terminée. Cela fait partie du processus de migration vers un accès sécurisé.

> Remarque : La migration est un service payant disponible uniquement pour les clients ayant souscrit un abonnement Cisco Secure Access. L'invitation ne peut être demandée qu'après l'achat de l'abonnement Secure Access.

> Remarque : Si la mise à niveau vers un accès sécurisé n'est pas présente, assurez-

vous que le package Umbrella est DNS ou SIG.

4. En supposant que vous passez votre commande pour un accès sécurisé, attendez 3 à 4 jours ouvrables pour recevoir un e-mail avec votre code de demande d'abonnement (après avoir lancé l'invitation de votre locataire Umbrella). Exemple d'adresse :




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

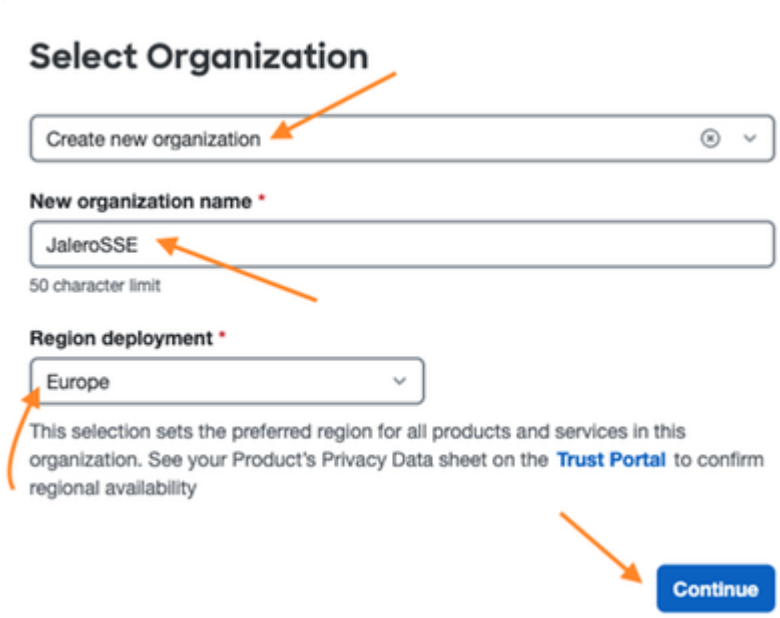
1. Accédez au portail Security Cloud Control et connectez-vous avec vos identifiants de connexion Cisco.

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

2. Sélectionnez Créer une nouvelle organisation (si vous n'en avez pas déjà une).
3. Saisissez le nom de la nouvelle organisation dans le champ Nom de la nouvelle organisation.
4. 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 :




5. Sélectionnez Continuer pour terminer la création de l'organisation.

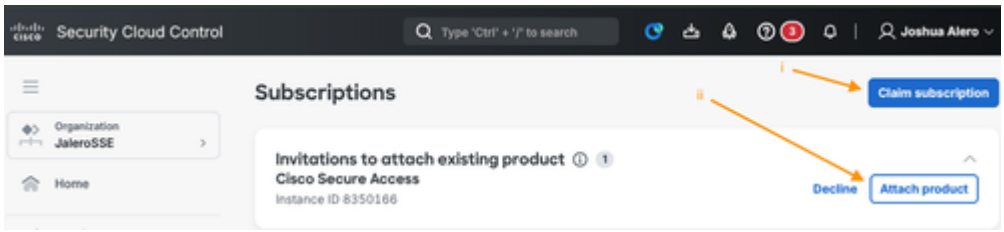
## 3. Lier l'organisation parapluie au SCC et demander un abonnement

1. Cliquez sur le bouton Demande d'abonnement pour la demander avec les codes fournis à l'étape 1 ci-dessus.
2. Votre ID d'organisation Umbrella doit être affiché sur la page Abonnements ainsi que sur l'invitation à le joindre au SCC.

---

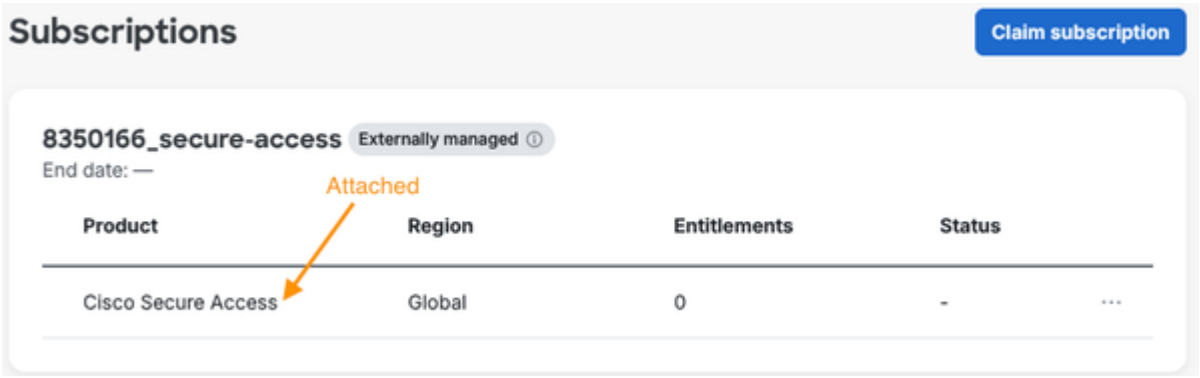
Remarque : L'ID de l'organisation parapluie doit être identique à celui figurant sur votre tableau de bord parapluie. Cela est important pour la migration et pour s'assurer que SCC et Umbrella ont été liés.

---

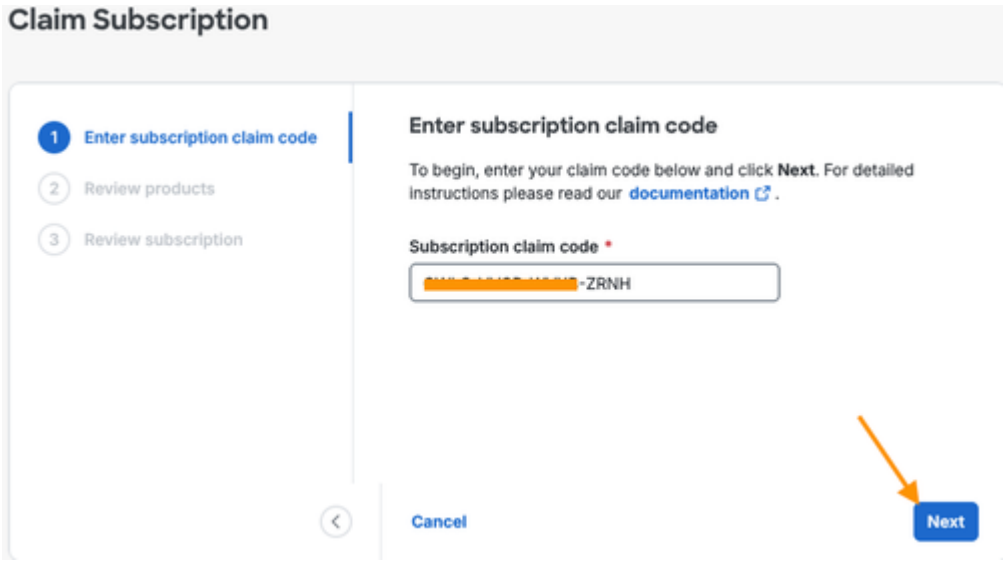



Sélectionnez Attach product pour attacher votre organisation-cadre à SCC.

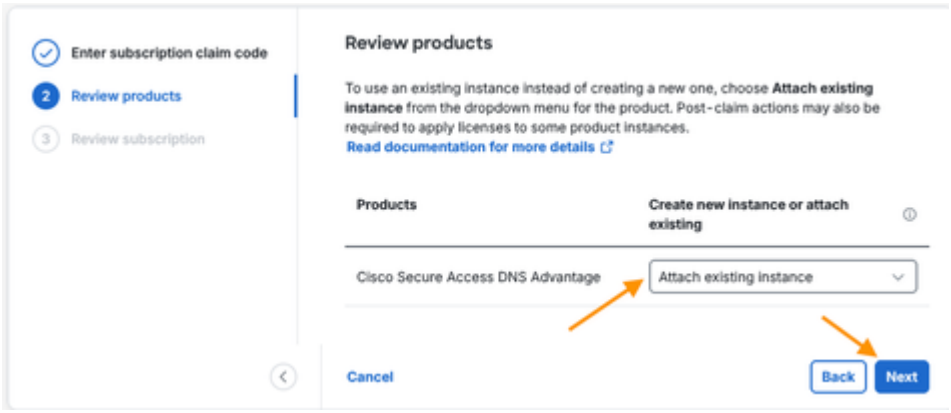
Une fois joint, vous devez voir le Cisco Secure Access en tant que produit dans la même page comme indiqué sur l'exemple ici :



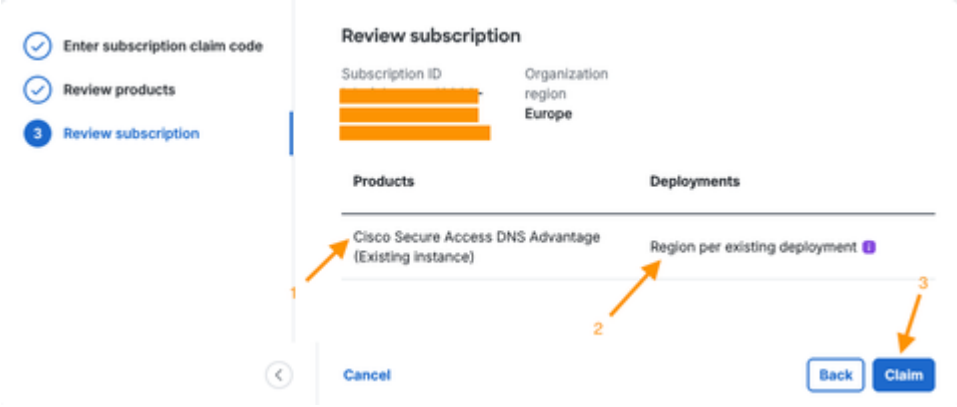

3. Entrez le code de demande et sélectionnez Next :



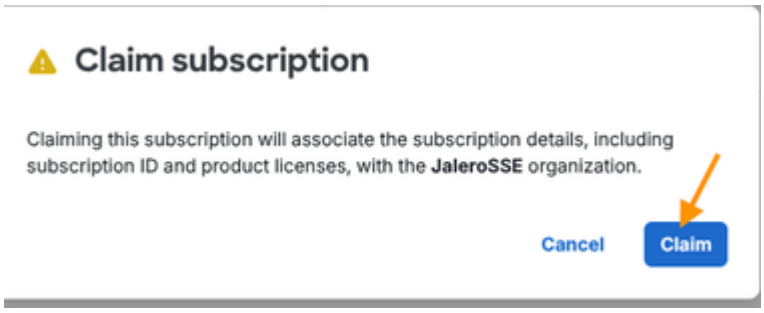

4. Sélectionnez Attacher une instance existante dans le menu déroulant Créer une nouvelle instance ou attacher une instance existante :



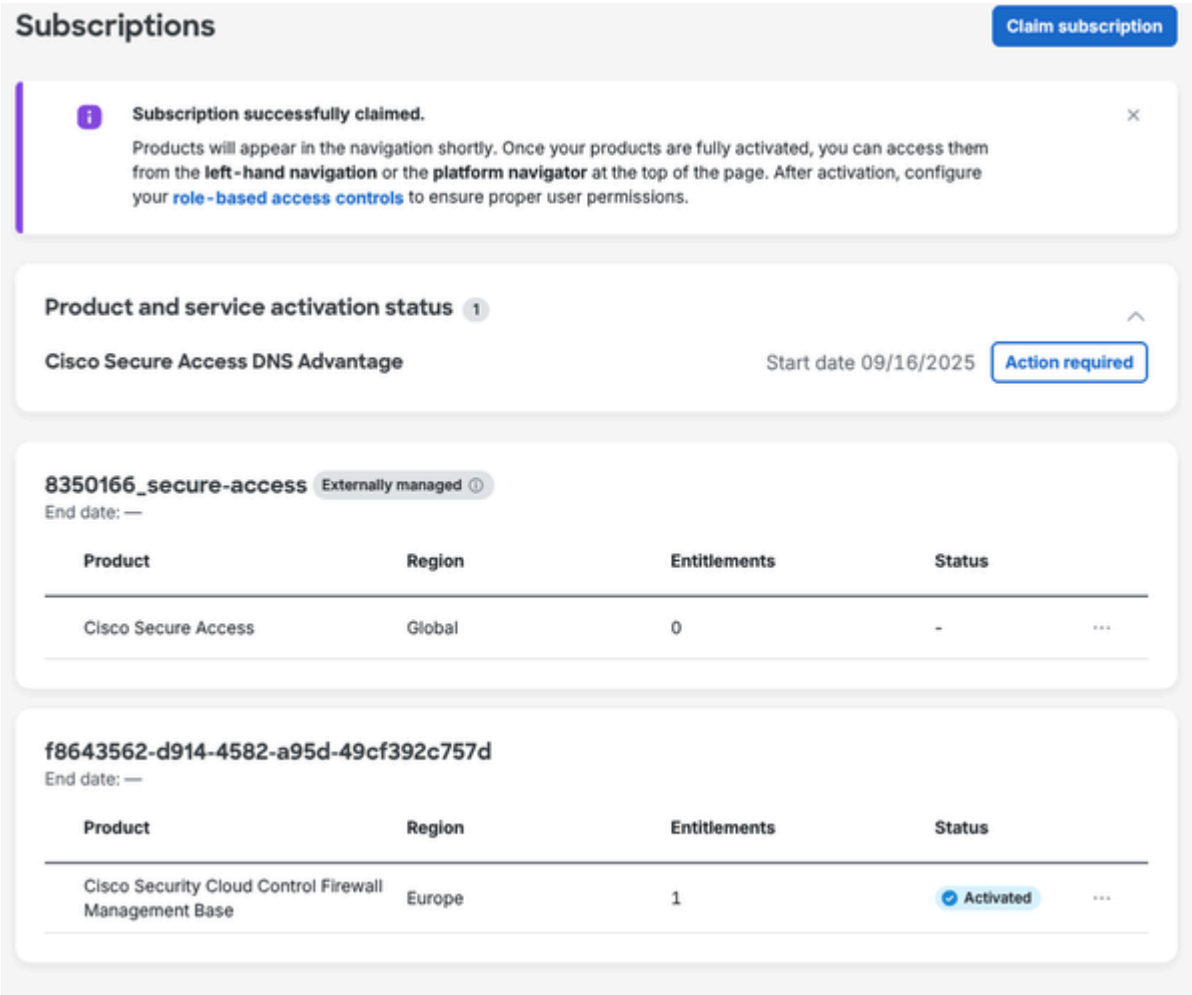

5. Vérifiez les paramètres :
    1. Assurez-vous que (instance existante) fait partie du nom du produit.
    2. Définissez la région sur la région existante de l'instance d'accès sécurisé connectée.
    3. Sélectionnez Déplacer la demande pour passer à la page suivante.




4. Confirmez la demande d'abonnement.

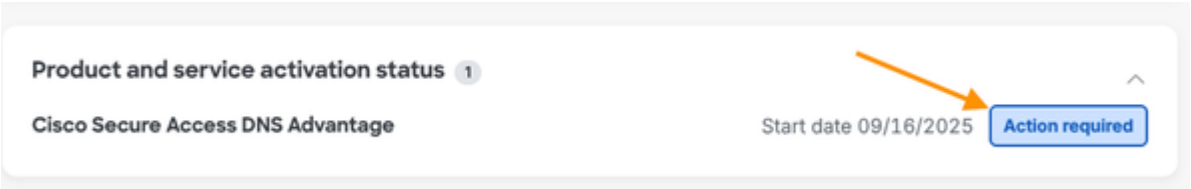



5. Une fois la demande et la mise en service réussies, recherchez une page Abonnements affichant tous vos produits activés :

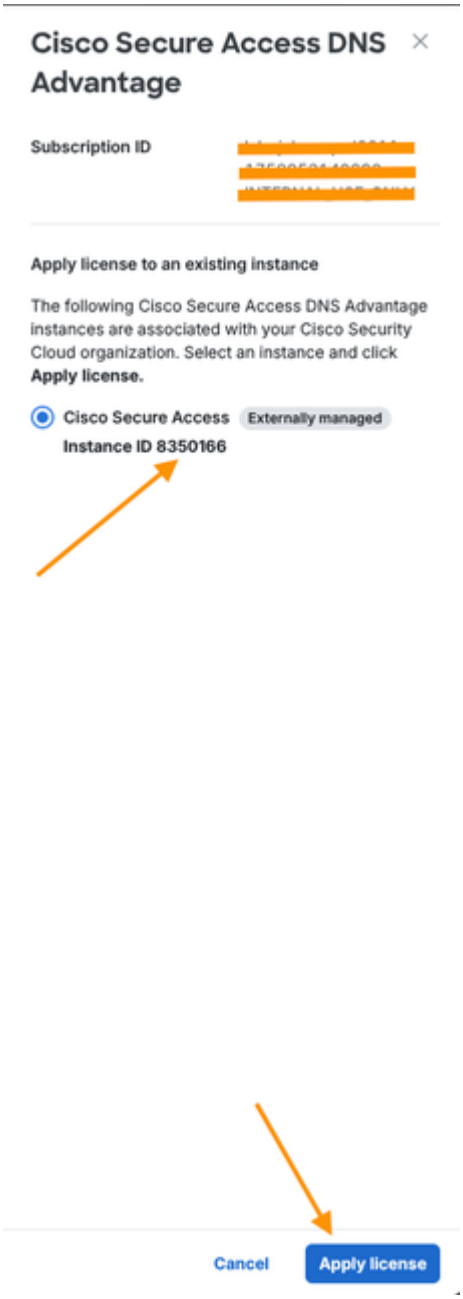


4. Appliquer la licence à l'instance d'accès sécurisé

1. Sélectionnez l'option Action requise.




2. Sélectionnez Appliquer la licence.

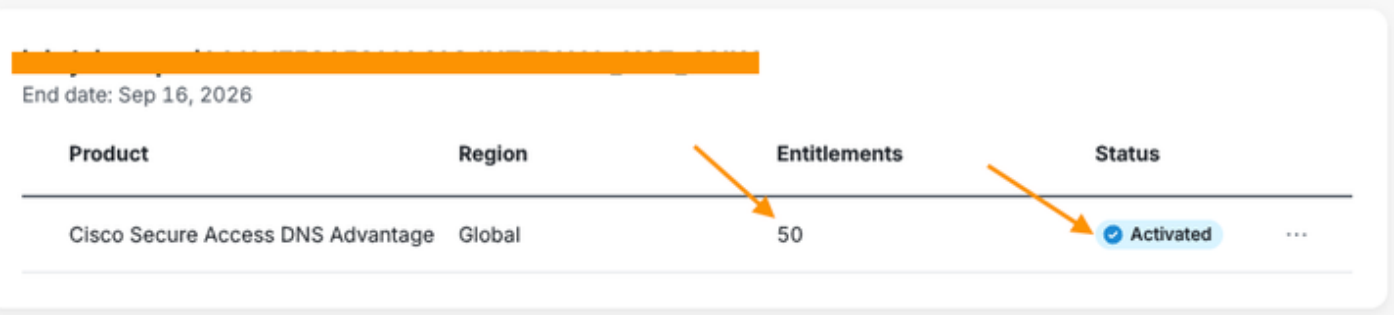



# Vérification de la liaison d'accès sécurisé vers SCC

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

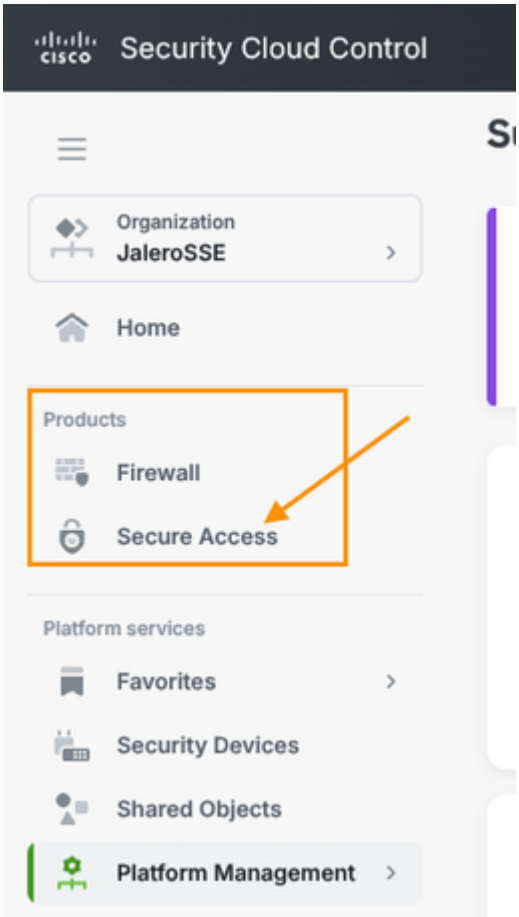
## 1. Statut d'activation du produit dans les abonnements

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



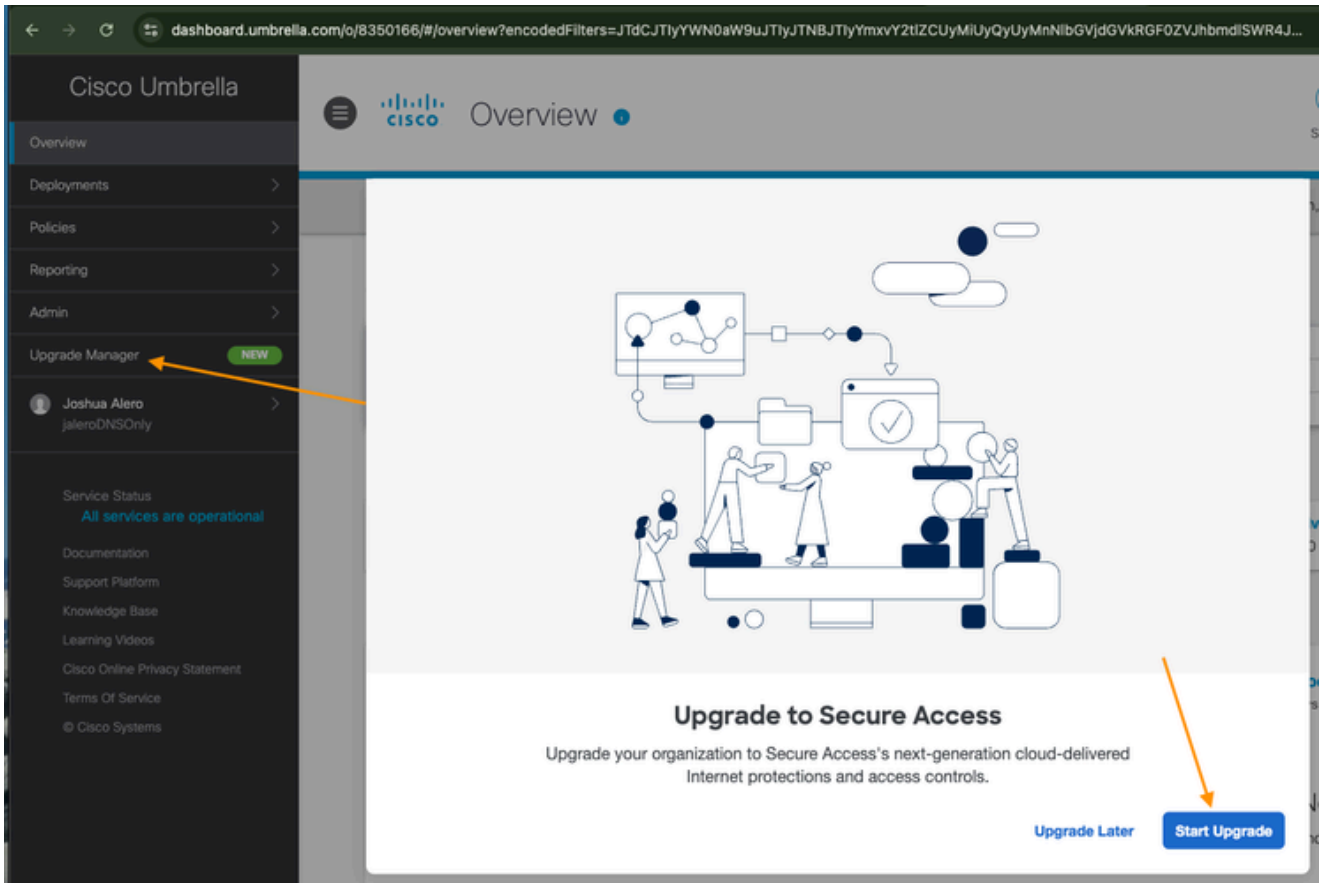

## 2. Accès sécurisé dans la liste des produits

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

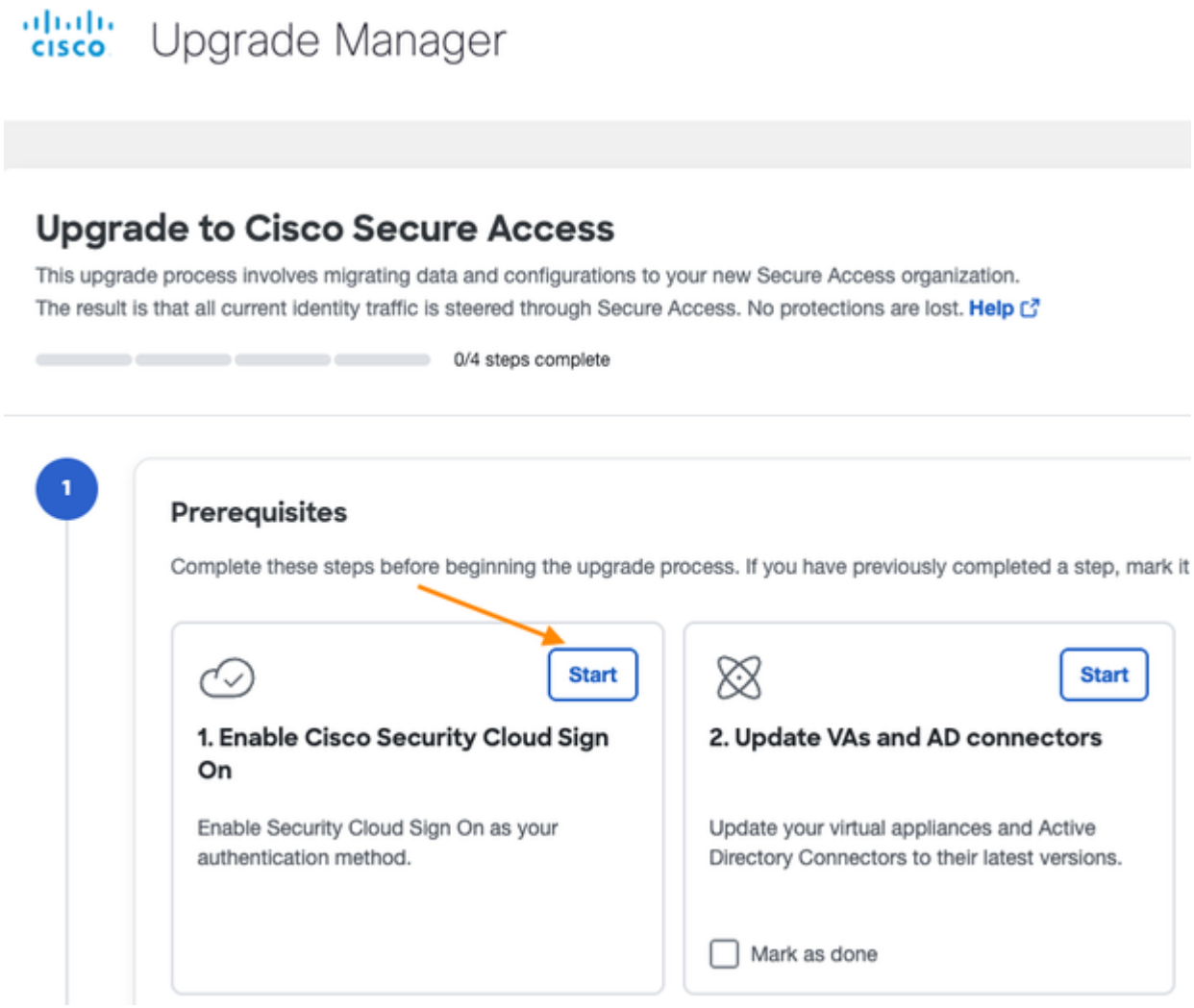


# Migration d'Umbrella vers un accès sécurisé

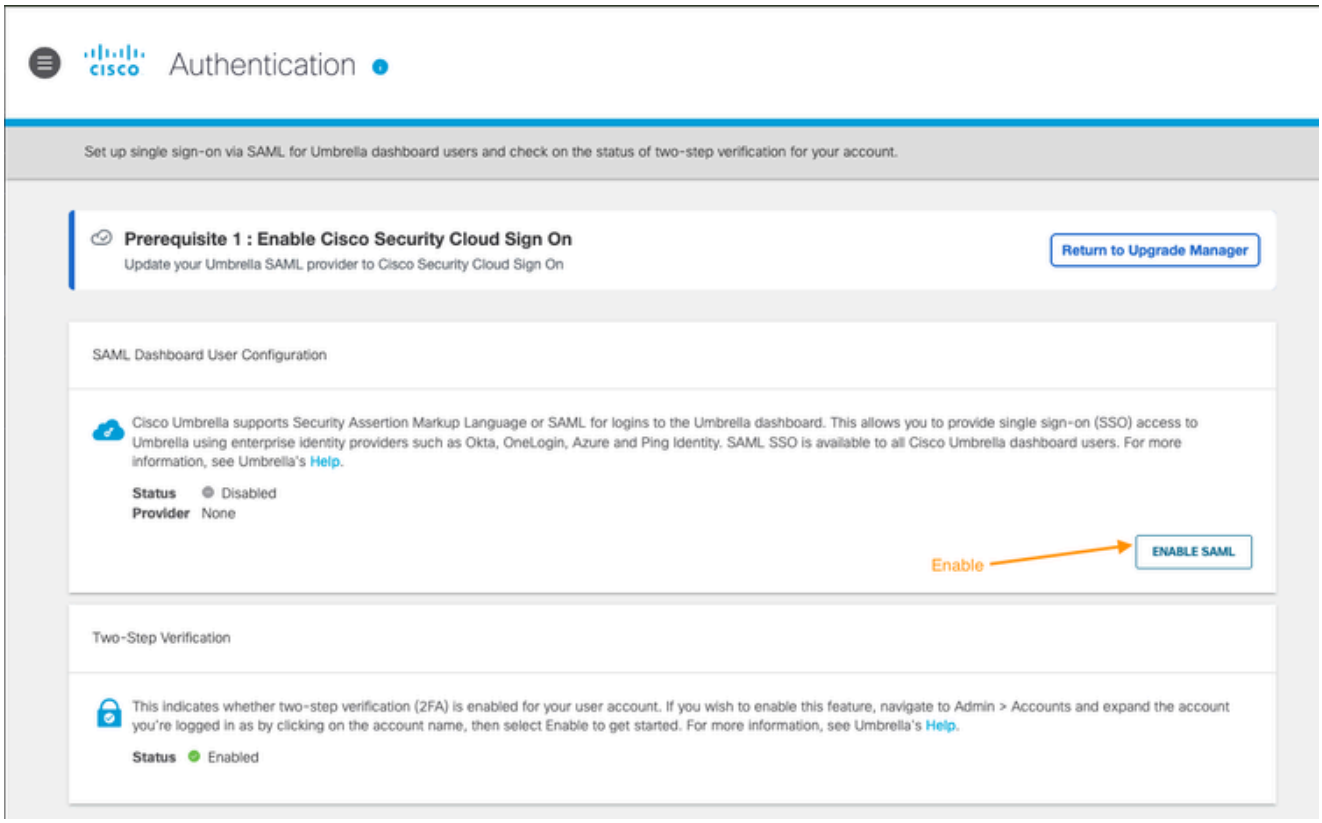
1. Reconnectez-vous à Umbrella avec le même compte que ci-dessus.
2. Accédez au nouvel élément de menu Gestionnaire de mise à niveau.



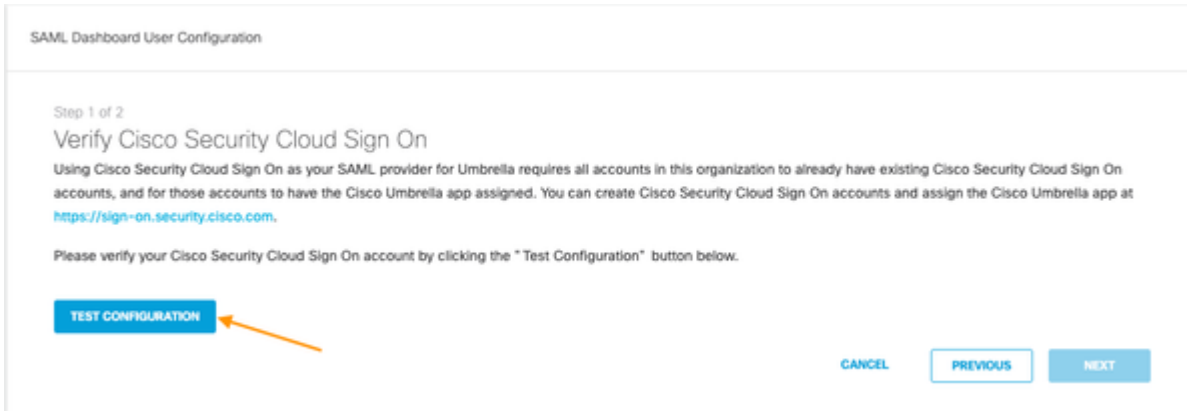

3. Dans la page Gestionnaire de mise à niveau, sélectionnez Démarrer sous Activer la connexion au cloud de sécurité Cisco.



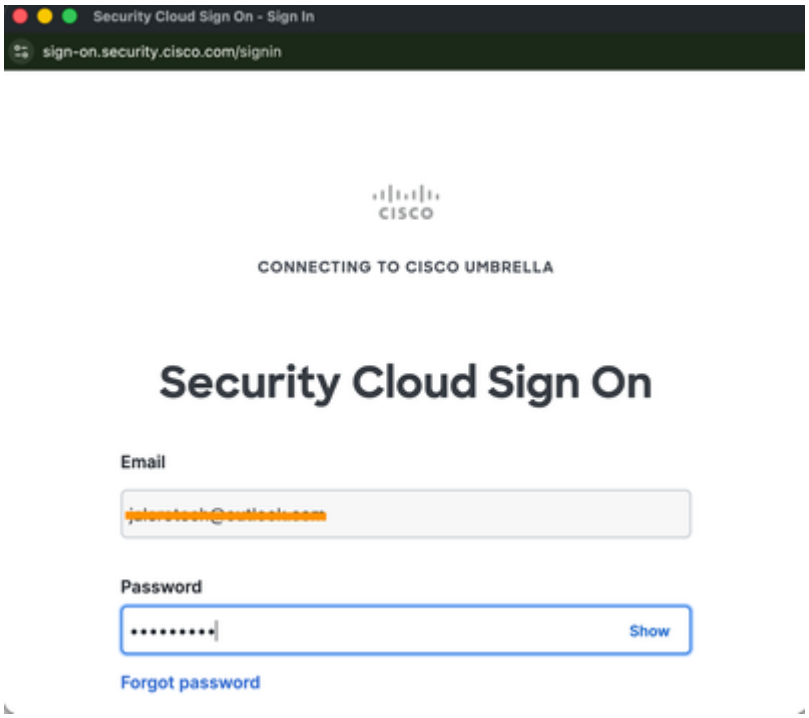

4. Sélectionnez ENABLE SAML sous SAML Dashboard User Configuration pour lier votre SCC comme fournisseur SAML pour la connexion au tableau de bord.

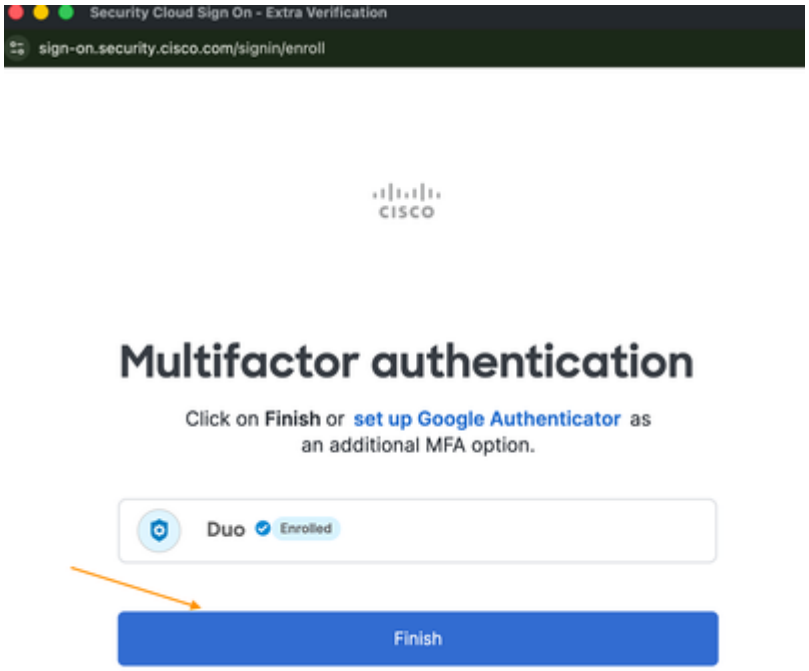



5. Testez la configuration SAML avec l'option TEST CONFIGURATION.

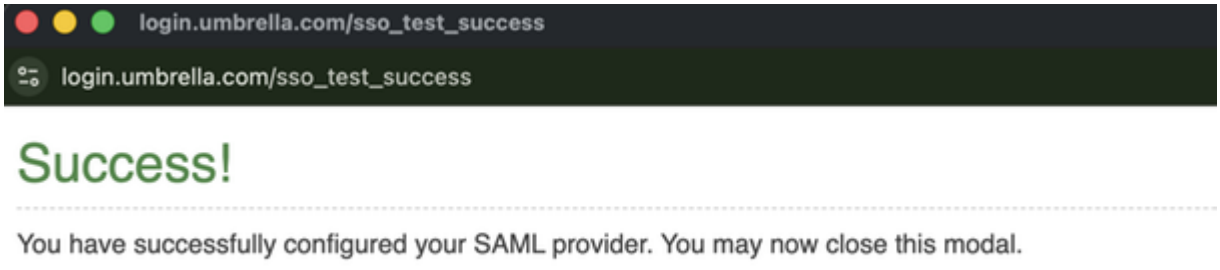



6. La page de connexion de SCC doit apparaître dans une autre fenêtre contextuelle (assurez-vous que le bloqueur de fenêtres contextuelles est désactivé). Lorsque vous y êtes invité, connectez-vous avec vos informations d'identification SCC.

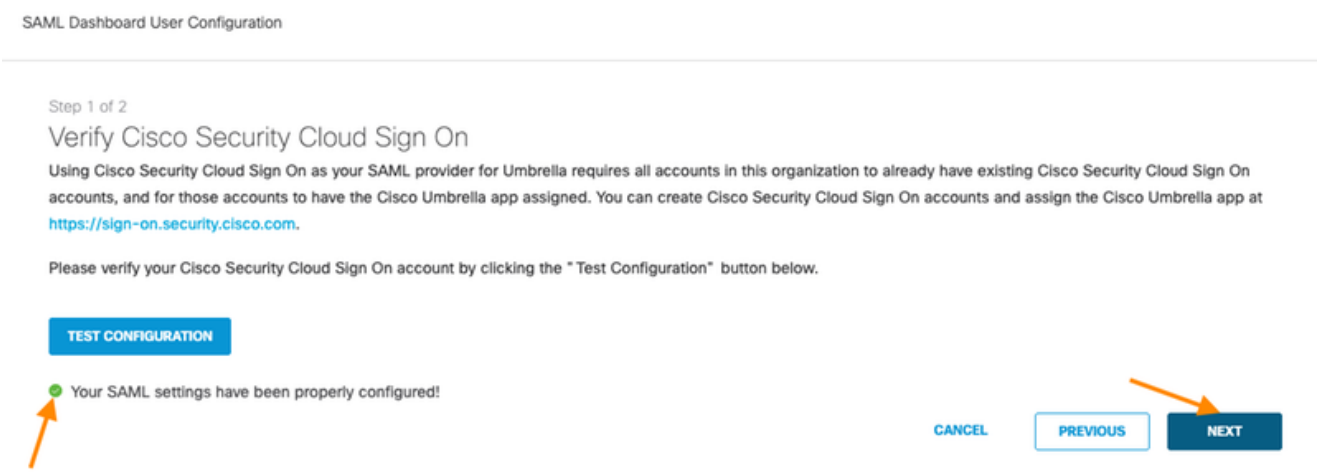


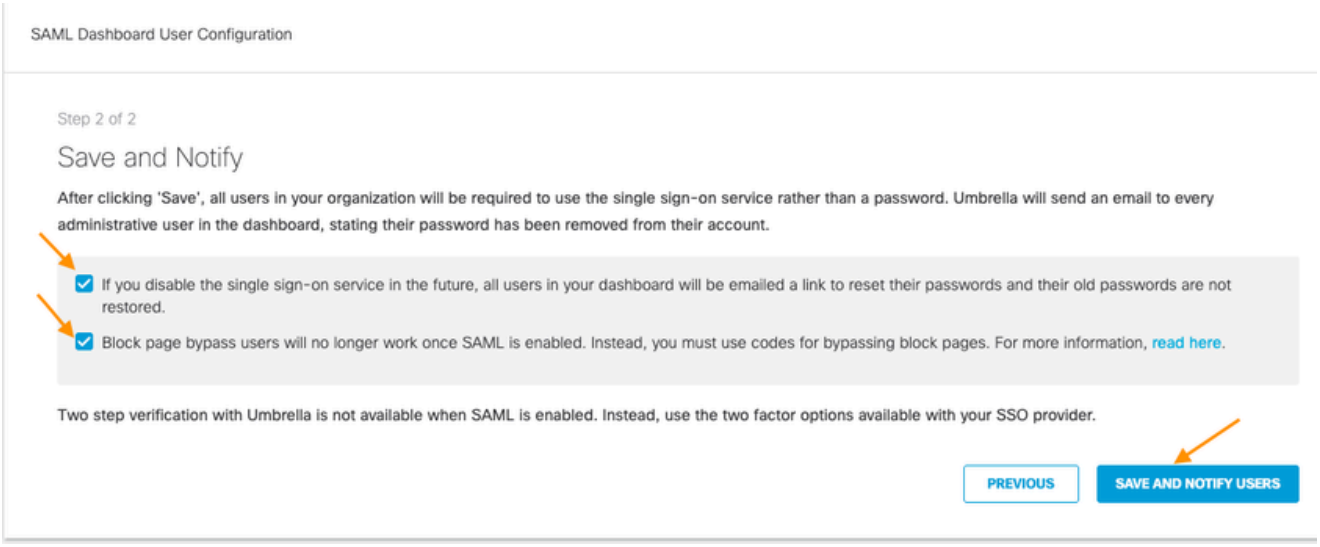

7. Lorsque la connexion a été vérifiée, recherchez ce message de confirmation, auquel point la partie SAML est presque terminée :



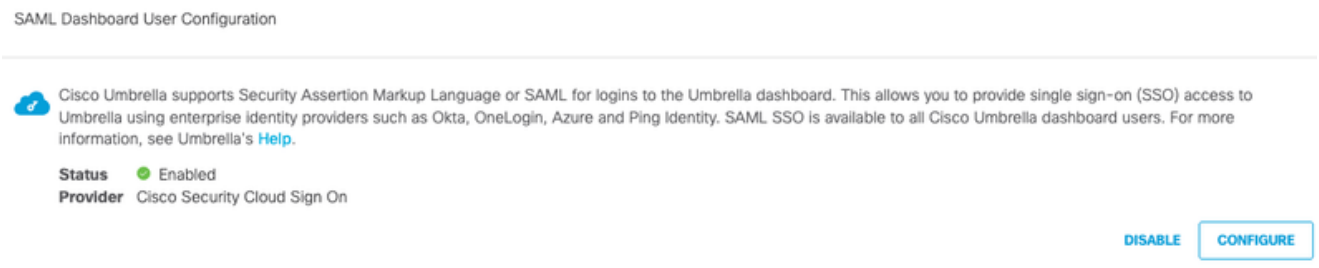
8. Revenez à la partie Configuration utilisateur du tableau de bord SAML. La puce verte indique que les paramètres SAML ont été correctement configurés. Sélectionnez SUIVANT.



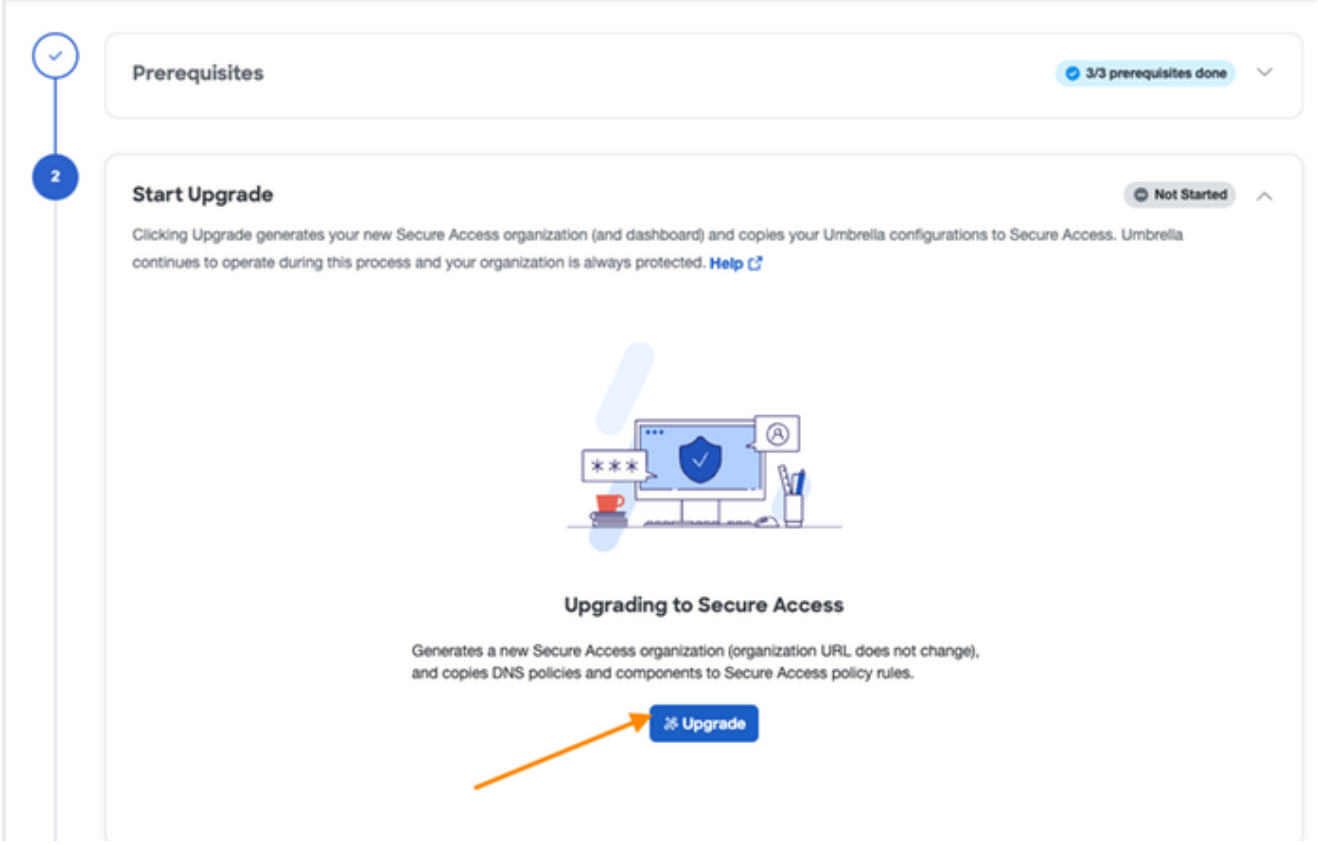

9. Enregistrez les modifications et avertissez les utilisateurs.



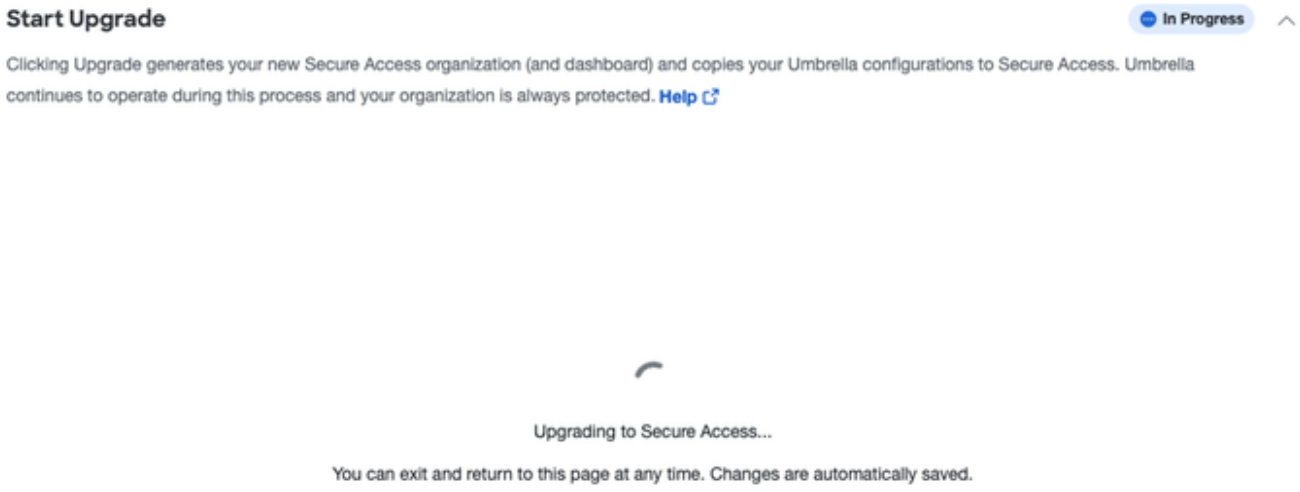

10. Configuration SAML terminée :



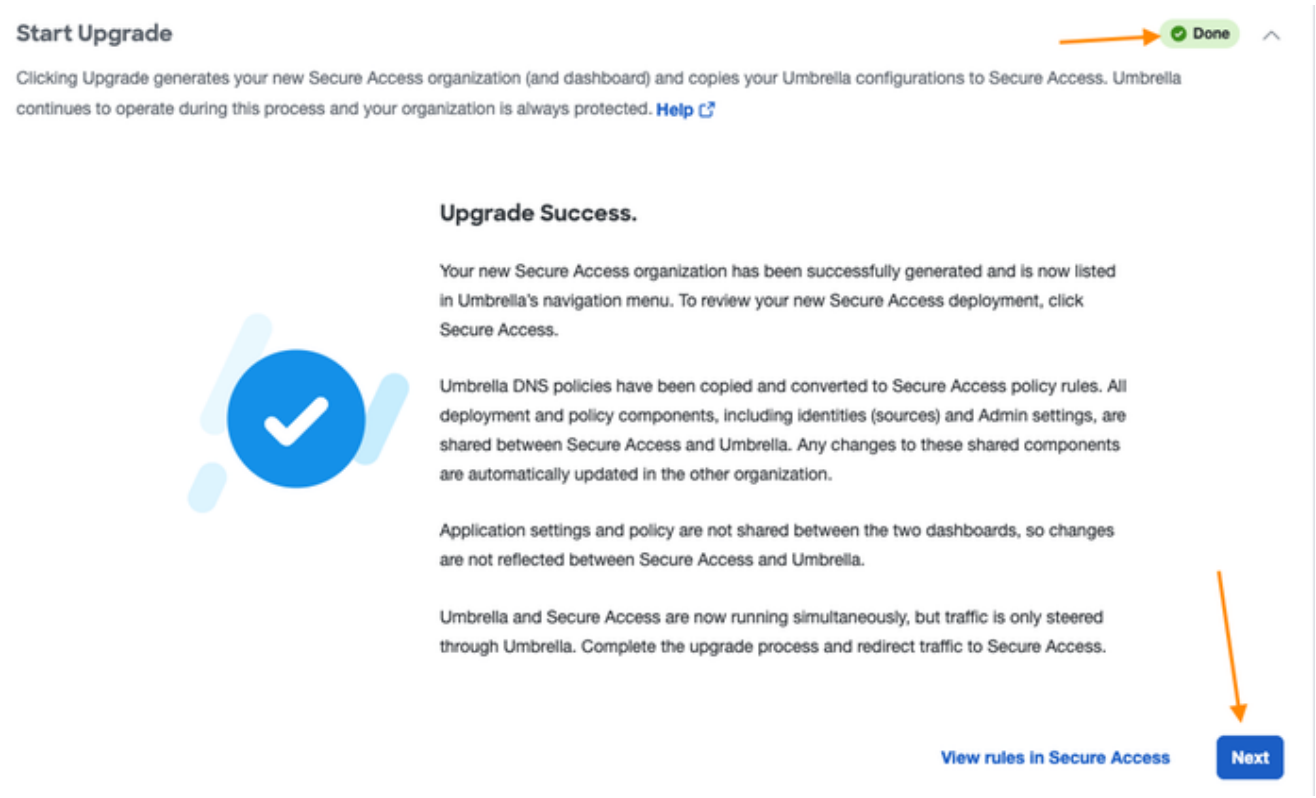

11. Effectuez la mise à niveau vers un accès sécurisé en sélectionnant Mise à niveau dans la section Démarrer la mise à niveau :



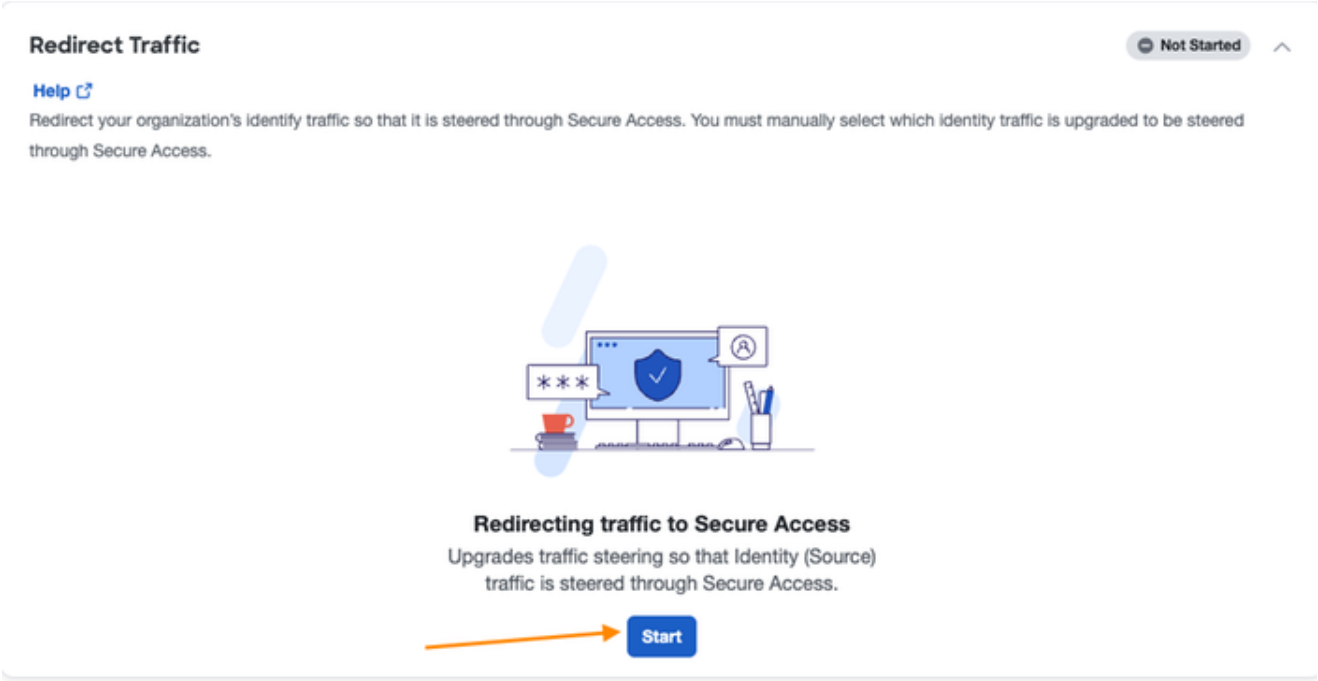

12. Autorisez la poursuite de la mise à niveau :



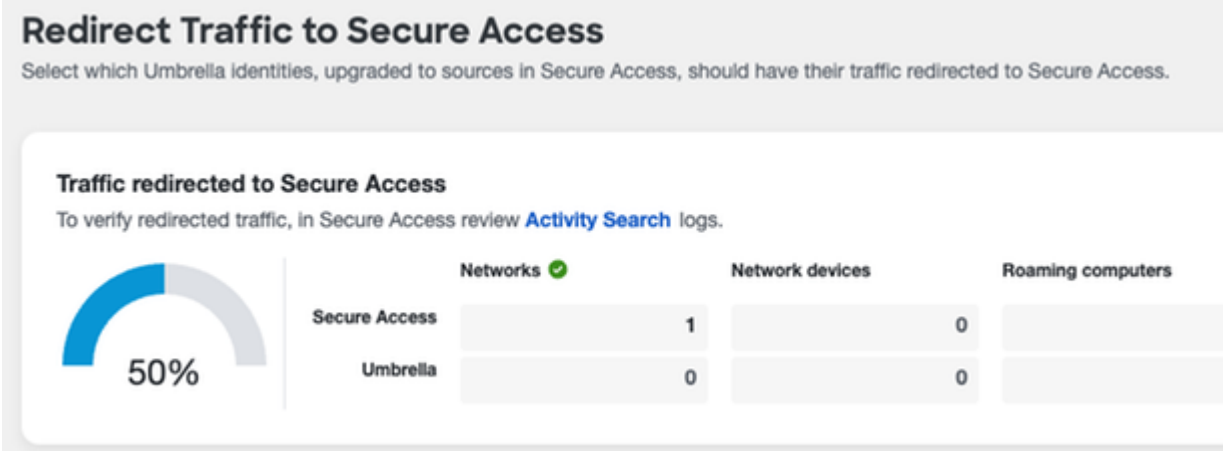

13. Lorsque vous avez terminé, recherchez cette page :




14. Rediriger le trafic vers Secure Access :




15. Confirmation de la redirection en cours. Dans l'exemple, seule l'identité réseau a été migrée d'Umbrella vers Secure Access :




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

---

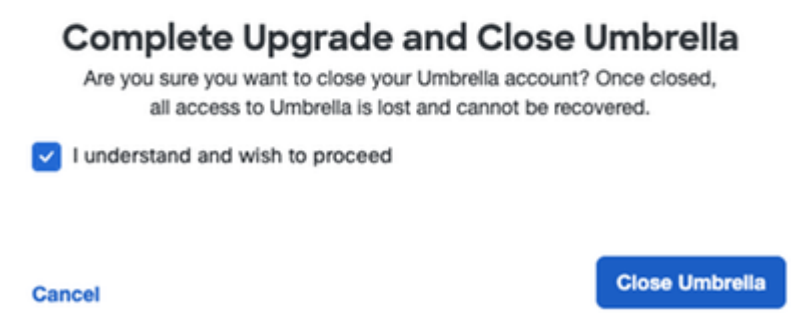
⚠ Mise en garde : Cela supprime complètement votre organisation Umbrella et n'est pas réversible donc assurez-vous que tous les éléments ont été complètement migrés avant d'effectuer cette étape.

---



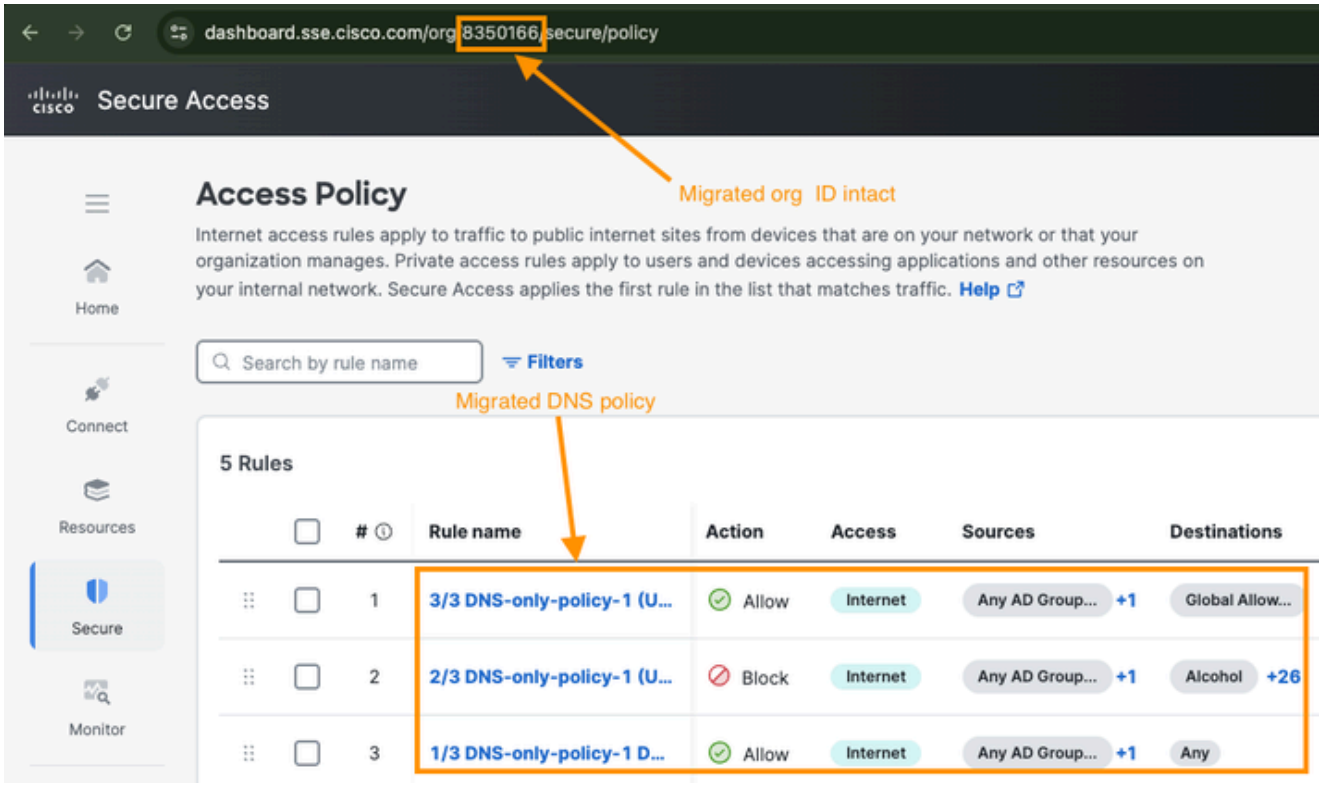

17. Lorsque vous sélectionnez Close Umbrella sur cette image, vous perdez l'accès à votre organisation parapluie dès qu'elle est supprimée.





# 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 Préparer la migration ci-dessus.




# Informations connexes

- Documentation générale
- documentation d'accès sécurisé
- Guide de mise à niveau DNS Defense
- 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.