Konfigurieren von Umbrella für die Migration zu Secure Access und Security Cloud Control

Inhalt

Einleitung

In diesem Dokument wird die Migration von Umbrella zu Secure Access mithilfe von Security Cloud Control (SCC) beschrieben.

Hintergrundinformationen

Umbrella-Kunden wird empfohlen, von Umbrella zu Secure Access zu migrieren und Security Cloud Control zu verwenden, um all ihre Cloud-Security-Produkte im Rahmen dieser Änderungen zu verwalten. Sie erhalten somit eine zentrale Oberfläche für das Management der Cloud-Sicherheitsprodukte, zu denen auch Cisco Secure Access gehört.

Multi-Org und MSSP werden derzeit (zum Zeitpunkt der Erstellung dieses Artikels) nicht unterstützt.

Voraussetzungen

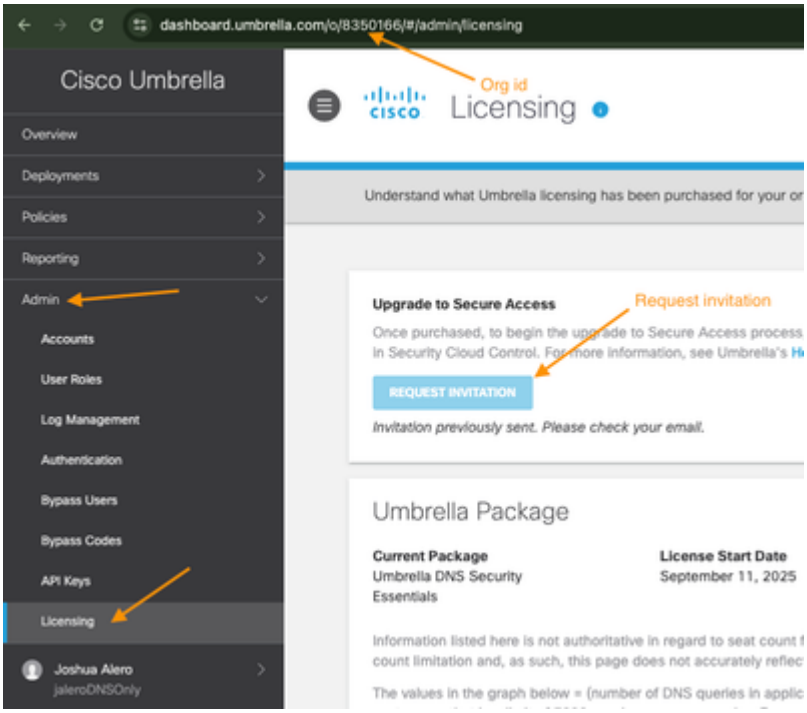
- Aktuelles DNS- oder SIG-Abonnement
- Vollständiger Administratorzugriff auf Umbrella
- Zugriff auf Cloud-Sicherheitskontrolle

Vorbereitungsphasen

1. Vorbereitung auf die Migration

1. Stellen Sie sicher, dass Sie über ein DNS- oder SIG-Abonnement bei Umbrella verfügen:

- Navigieren Sie zu Admin > Licensing, um die
- Upgrade auf sicheren Zugriff muss oben auf der Seite angezeigt werden:



ii) Notieren Sie sich die Organisations-ID in diesem Beispiel 8350166.

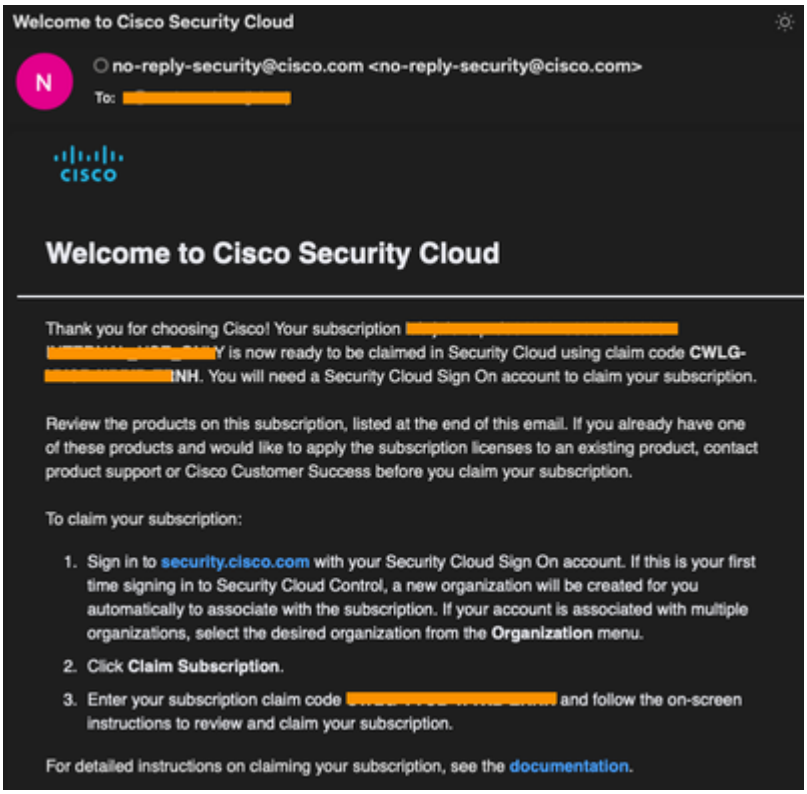
iii. Wählen Sie auf der Lizenzierungsseite die Option Einladung anfordern aus.

Wichtig: Die Schaltfläche Request Invitation (Einladung anfordern) dient als Einladung, dem Umbrella-Tenant für SCC beizutreten. Es wird kein Anspruchscode generiert. Sobald Ihre Bestellung für Secure Access abgeschlossen ist, erhalten Sie einen Antragscode. Dies ist Teil des Migrationsprozesses zu Secure Access.

Anmerkung: Wenn das Upgrade auf sicheren Zugriff nicht vorhanden ist, stellen Sie sicher, dass das Umbrella-Paket DNS oder SIG ist (mehrere Organisationen oder Add-ons werden derzeit zum Zeitpunkt der Erstellung dieses Artikels nicht unterstützt).

---

iv. Angenommen, Sie haben Ihre Bestellung für sicheren Zugriff aufgegeben, warten Sie 3-4 Werktage, und Sie müssen eine E-Mail mit Ihrem Abonnement-Antragscode (nach Initiierung der Anforderungseinladung von Ihrem Umbrella Tenant) erhalten. Siehe Beispiel-E-Mail:



2. Melden Sie sich mit Ihren bestehenden Cisco Anmeldeinformationen bei SCC an.

i. Navigieren Sie zum Security Cloud Control-Portal, und melden Sie sich mit Ihren Cisco Anmeldeinformationen an.

Anmerkung: Die Cisco Anmeldedaten für den Zugriff auf Ihr Umbrella Dashboard.

---

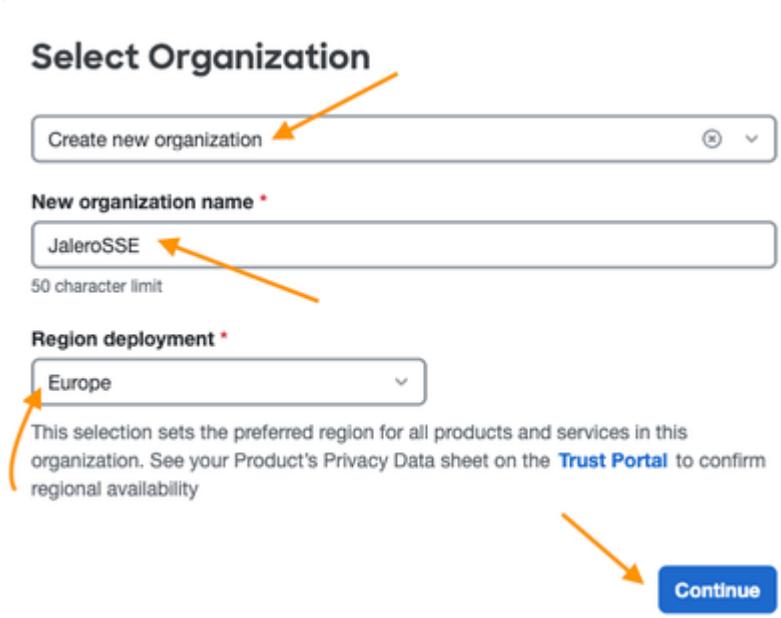
ii) Wählen Sie Neue Organisation erstellen (wenn noch keine vorhanden ist).

iii. Geben Sie den neuen Organisationsnamen in das Feld Neuer Organisationsname ein.

iv. Wählen Sie im Dropdown-Menü Region deployment (Bereitstellung der Region) die entsprechende Region aus.

Hinweis: Dies muss die grafische Region sein, in der der Tenant bereitgestellt wird.

Beispiel:



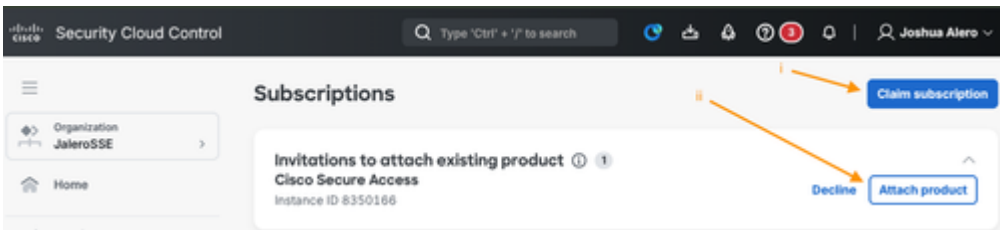
v. Wählen Sie dann Weiter, um die Erstellung der Organisation abzuschließen.

3. Link Umbrella Org zu SCC und Anspruch Abonnement

i. Wählen Sie die Schaltfläche für das Anspruchsabonnement, um es mit den Codes aus Schritt 1 oben zu beantragen.

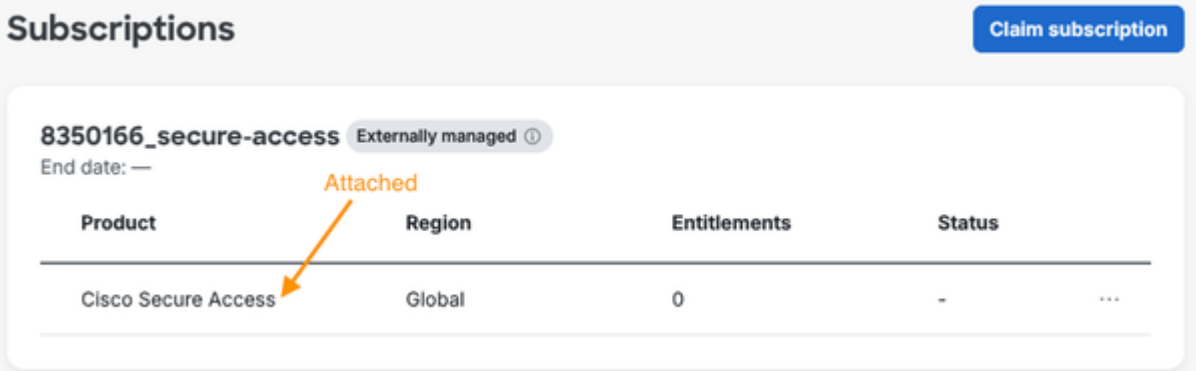
ii) Ihre Umbrella-Org-ID muss auf der Seite "Subscriptions" (Abonnements) sowie auf der Einladung zum Anhängen an SCC angezeigt werden.

Anmerkung: Die Umbrella-Org-ID muss mit der ID auf Ihrem Umbella-Dashboard übereinstimmen. Dies ist wichtig für die Migration und um sicherzustellen, dass sowohl SCC als auch Umbrella miteinander verknüpft wurden.

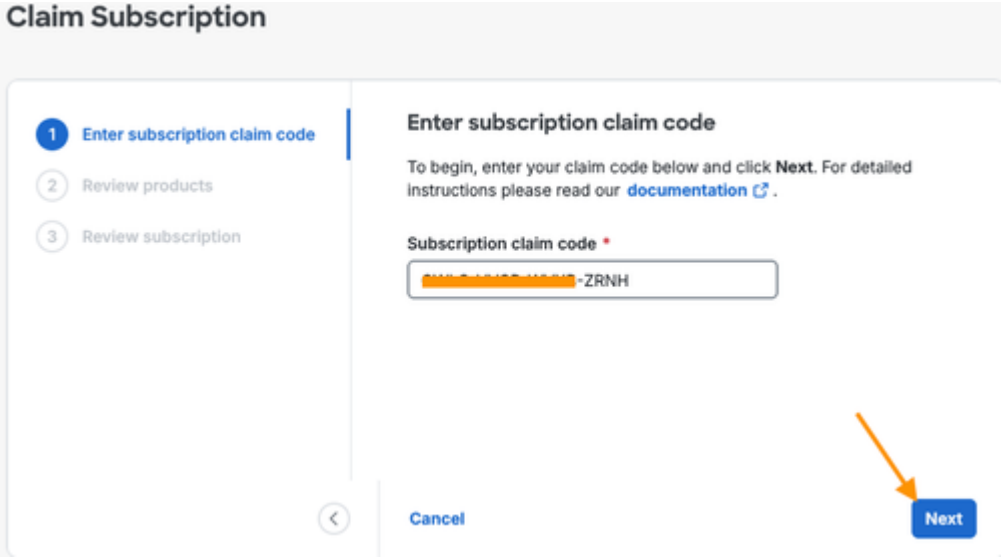


- Wählen Sie Produkt anhängen, um Ihre Umbrella Org an SCC anzuhängen.

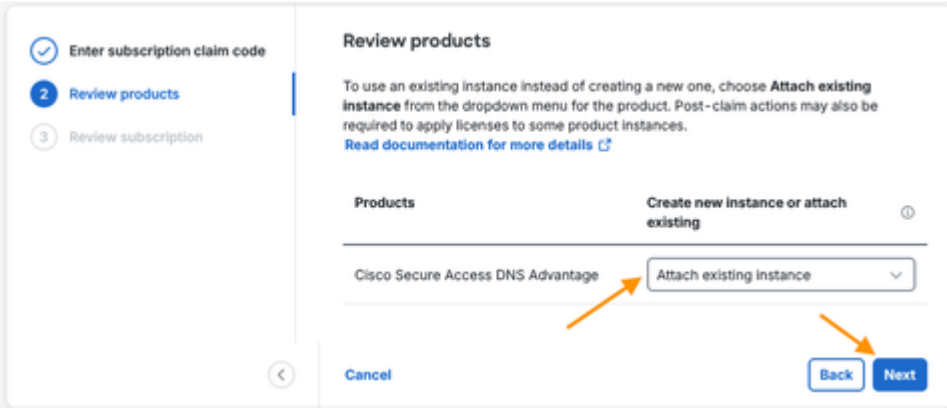
- Wenn das Dokument angehängt ist, muss Cisco Secure Access als Produkt auf derselben Seite wie im folgenden Beispiel angezeigt werden:



iii. Geben Sie den Anspruchscode ein, und wählen Sie Weiter aus:

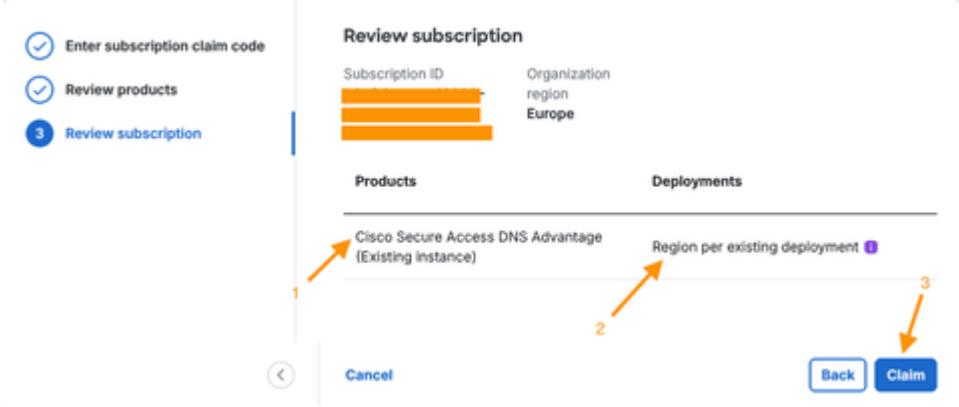


iv. Wählen Sie Vorhandene Instanz anhängen im Dropdown-Menü Neue Instanz erstellen oder Vorhandene anhängen aus:

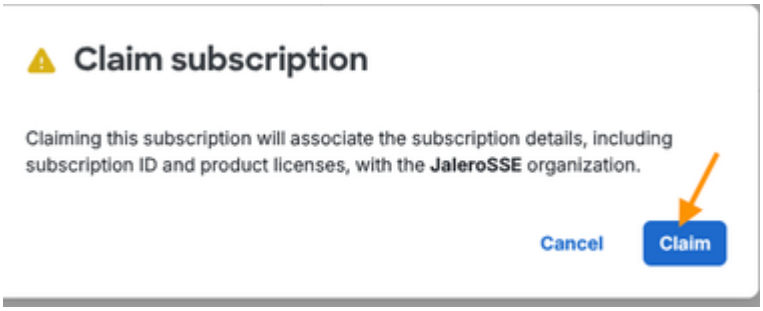


v. Überprüfen Sie die Einstellungen:

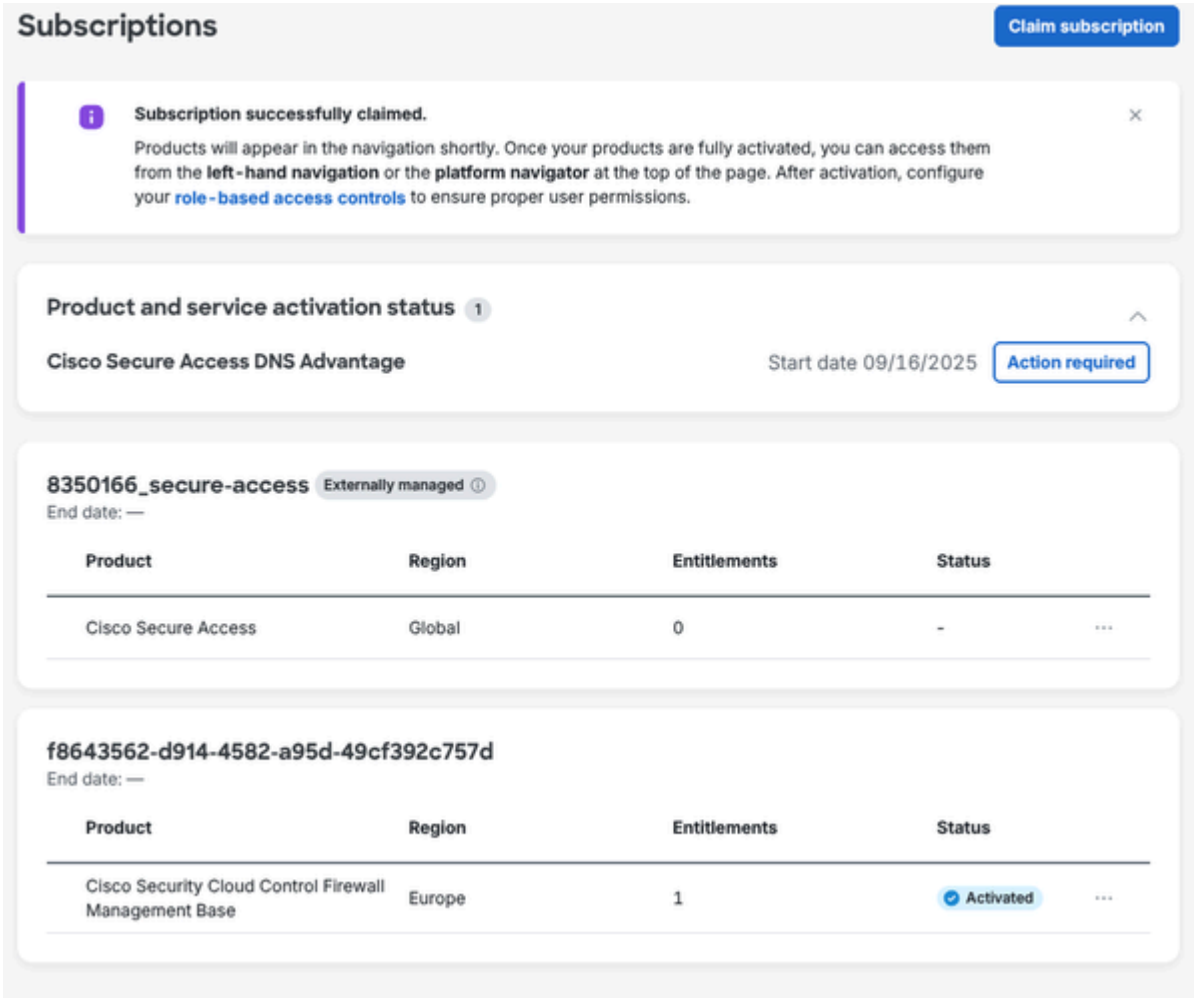
- Stellen Sie sicher, dass die (vorhandene Instanz) Teil des Produktnamens ist.
- Für die Region muss die vorhandene Region der angefügten Secure Access-Instanz festgelegt werden.
- Wählen Sie Forderungsverschiebung, um zur nächsten Seite zu gelangen.



- Bestätigen Sie den Abonnementanspruch:

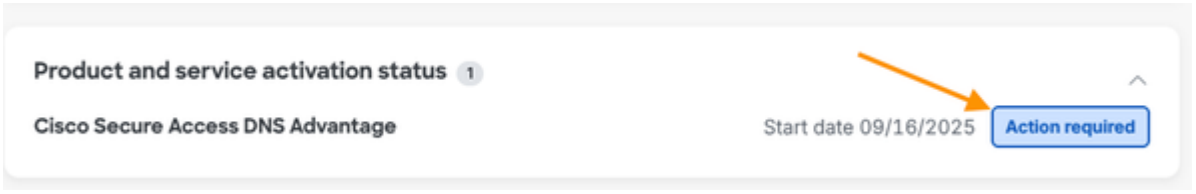


- Nach erfolgreicher Antragstellung und Bereitstellung müssen Sie eine Seite für Abonnements erhalten, die der hier gezeigten Seite ähnelt und auf der alle aktivierten Produkte angezeigt werden:

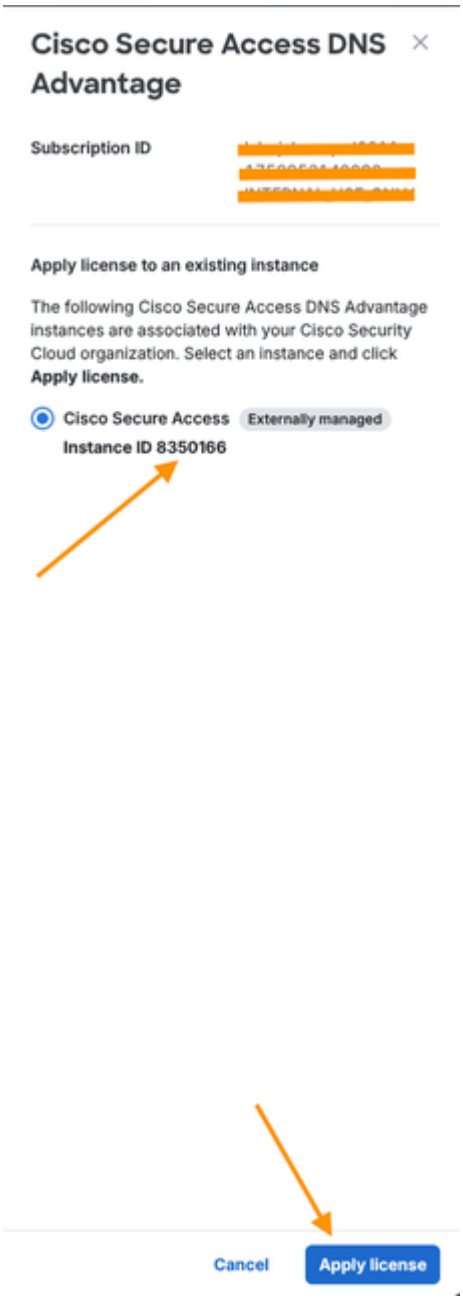


4. Wenden Sie die Lizenz auf die Instanz für sicheren Zugriff an

i. Wählen Sie die Option "Aktion erforderlich":



ii) Wählen Sie Lizenz anwenden:

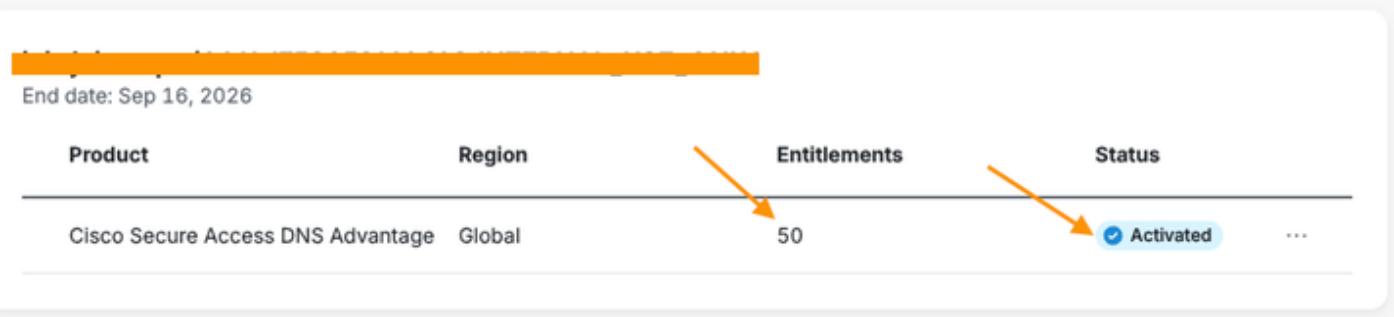


Sichere Zugriffsverbindung mit SCC überprüfen

Überprüfen Sie in diesem Abschnitt, ob Ihr Secure Access-Tenant mit SCC verknüpft wurde.

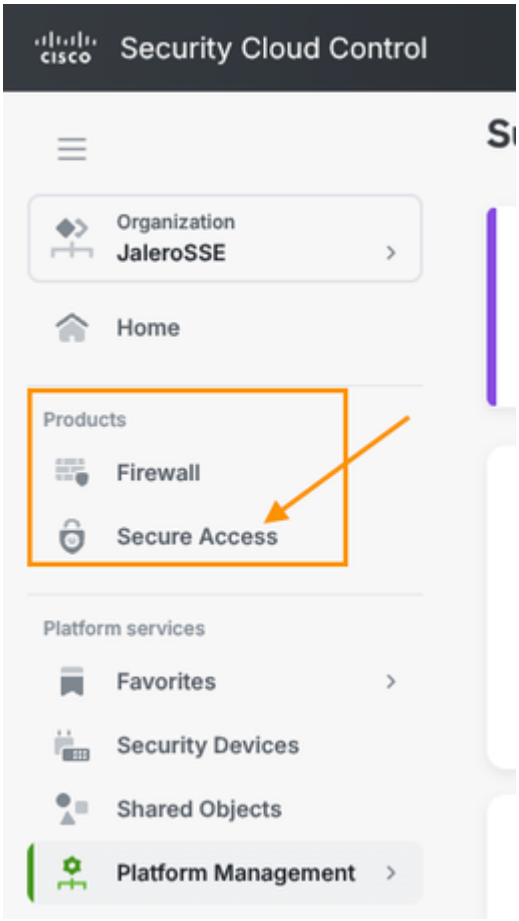
1. Produktaktivierungsstatus in "Abonnements"

Vergewissern Sie sich, dass die Produktinstanz Cisco Secure Access <Lizenztyp> aktiviert wurde:



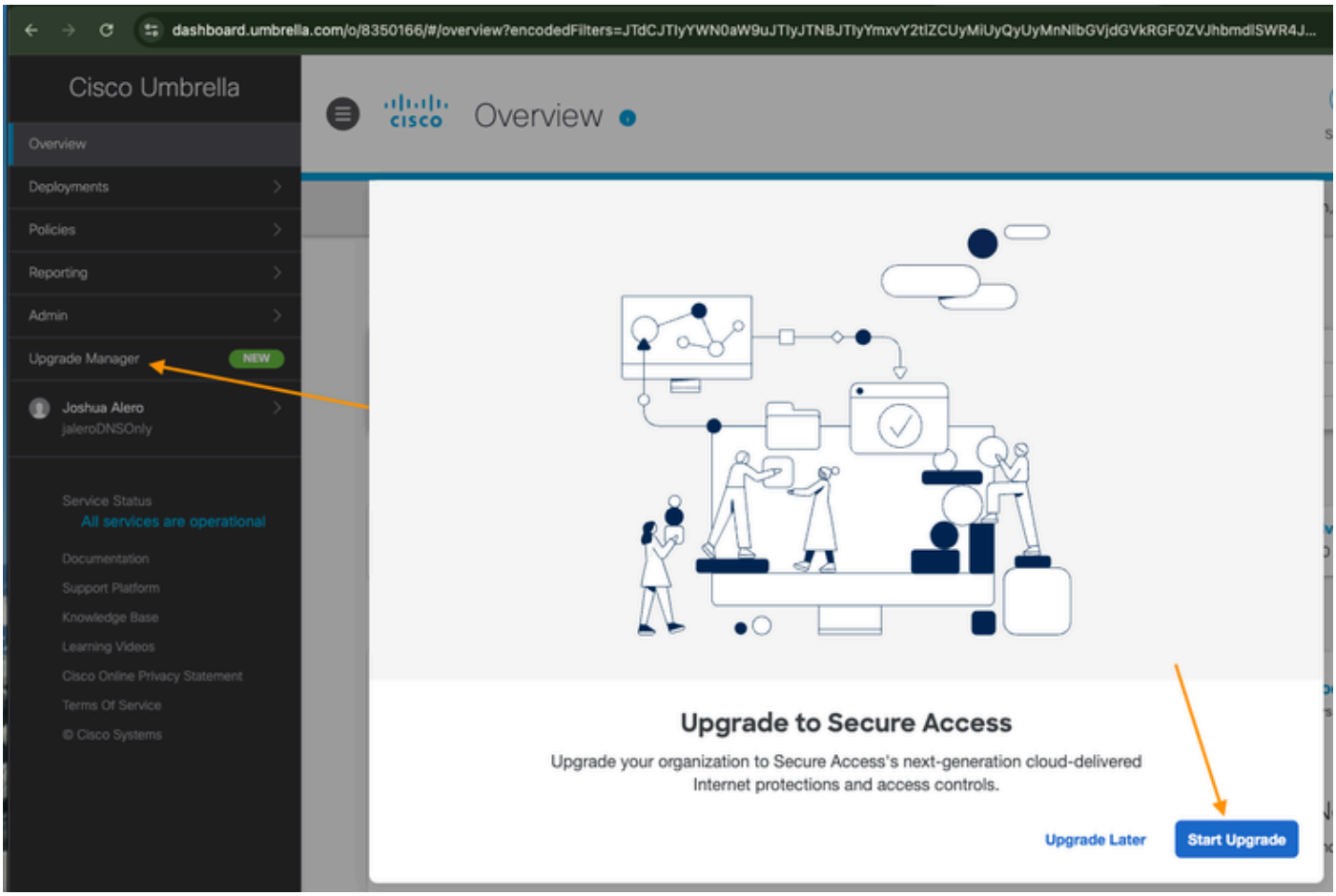
2. Sicherer Zugriff in der Produktliste

Secure Access muss jetzt auch unter Produkte aufgeführt werden:

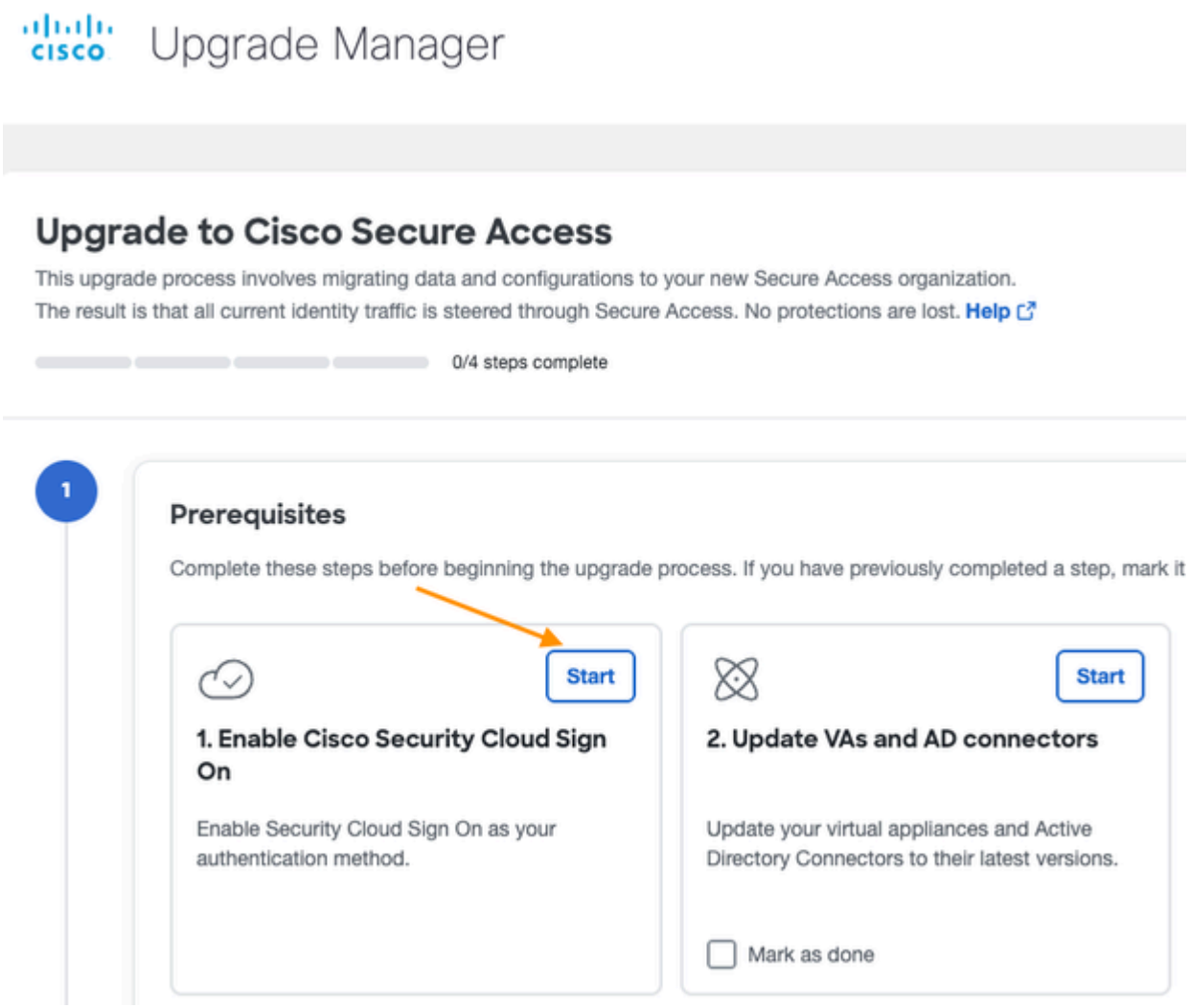


Migration von Umbrella zu Secure Access

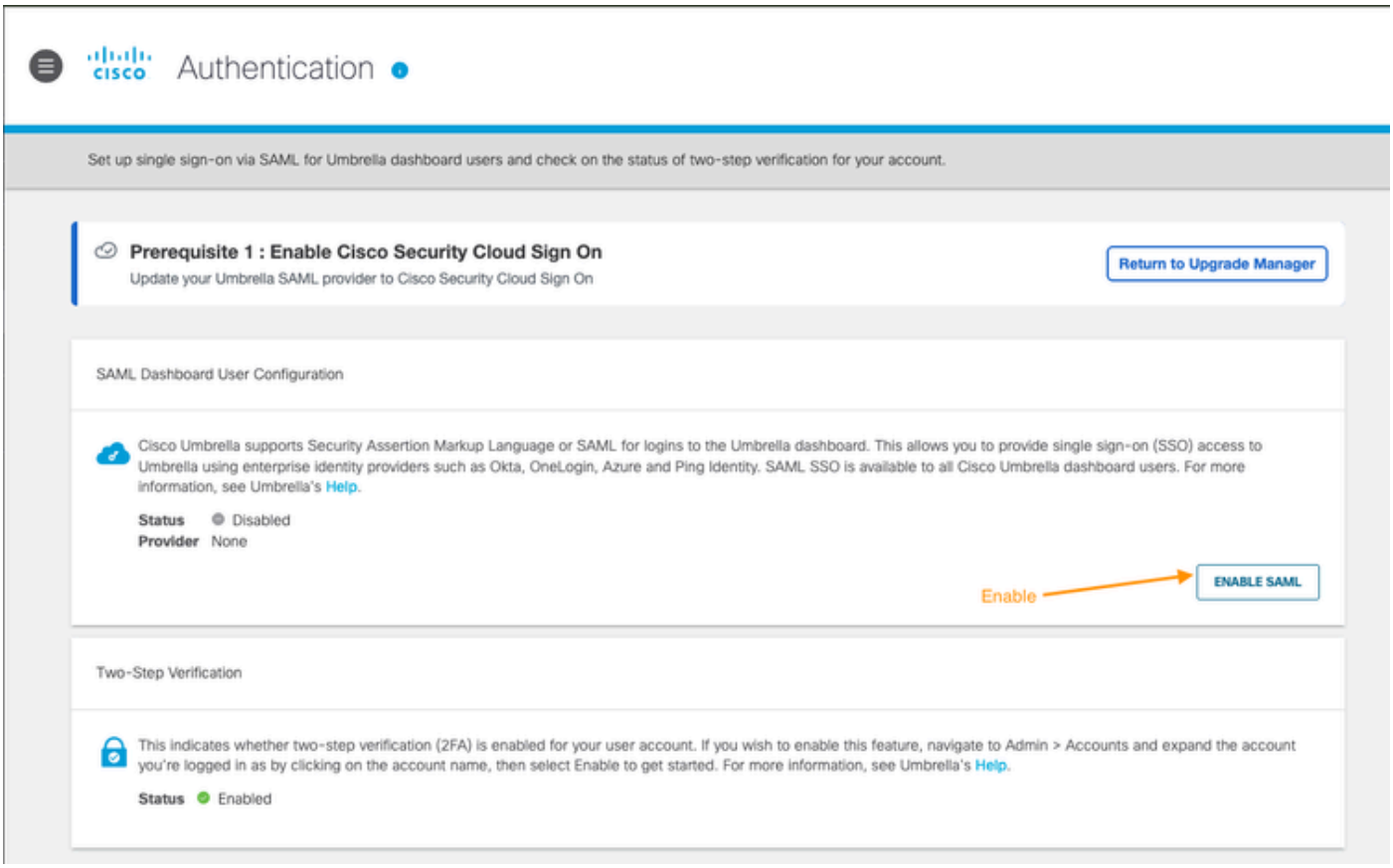
1. Melden Sie sich mit dem gleichen Konto wie oben wieder bei Umbrella an.
2. Navigieren Sie zum neuen Menüpunkt Upgrade Manager:



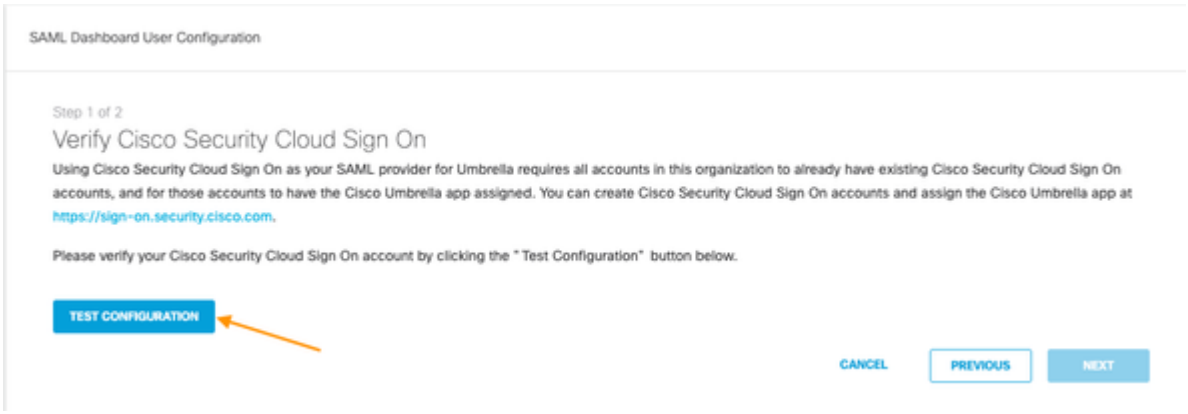
3. Wählen Sie auf der Seite Upgrade Manager unter Cisco Security Cloud aktivieren die Option Start aus.



4. Wählen Sie SAML AKTIVIEREN unter SAML Dashboard Benutzerkonfiguration, um Ihr SCC als SAML-Anbieter für die Dashboard-Anmeldung zu verknüpfen:

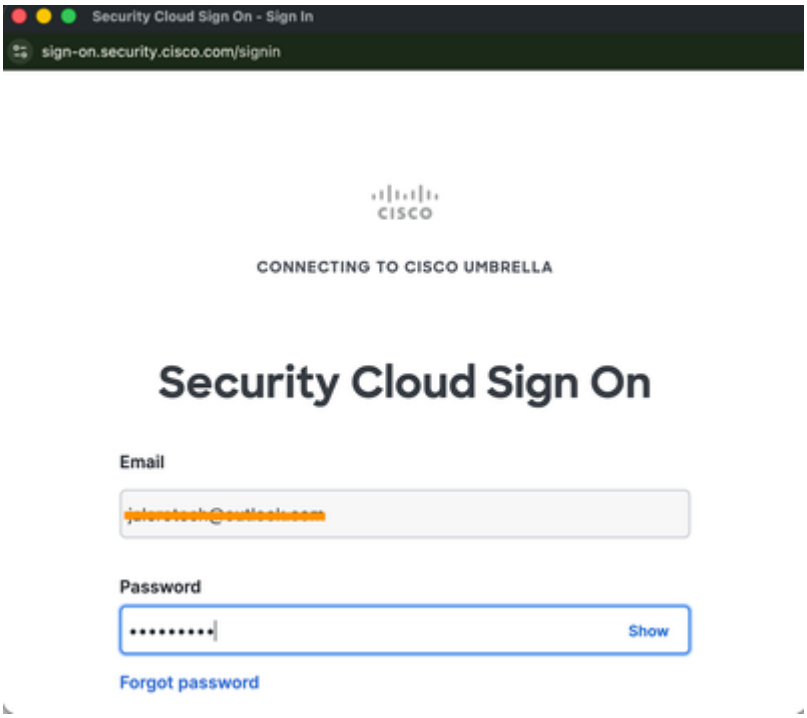


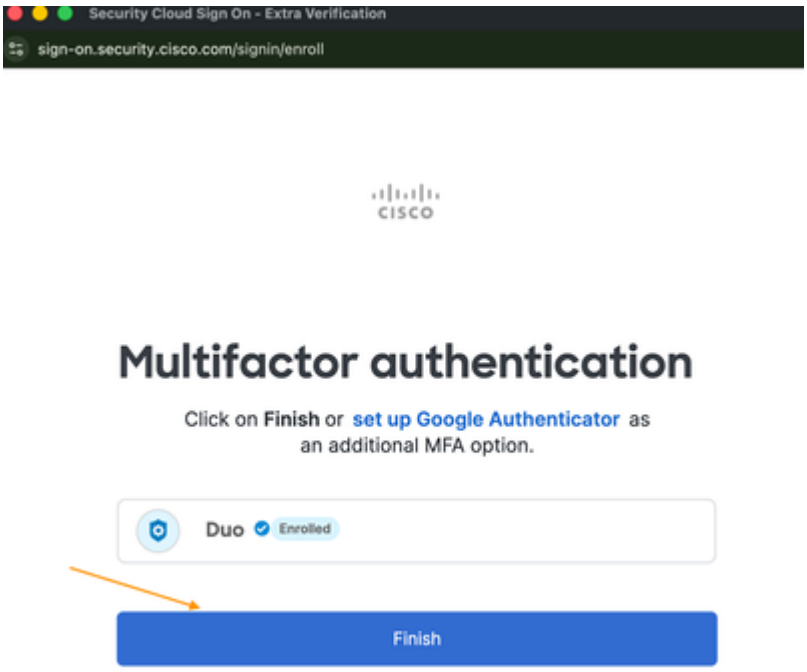
5. Testen Sie die SAML-Konfiguration mit der Option TEST CONFIGURATION:



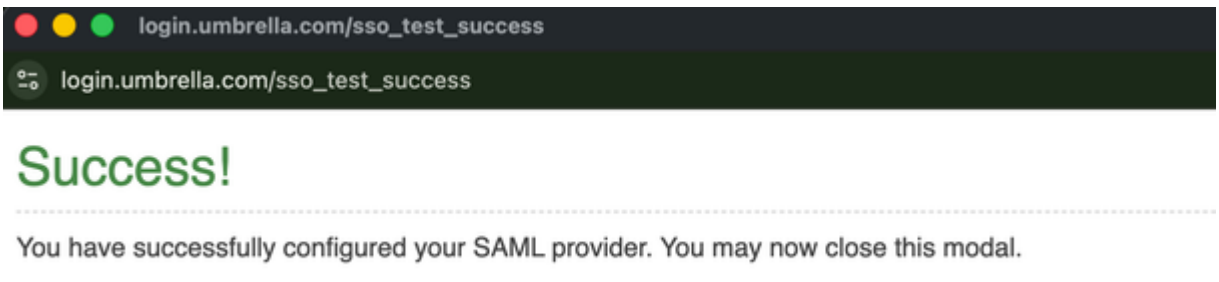
6. Die Anmeldeseite von SCC muss in einem anderen Popup-Fenster angezeigt werden (sicherstellen, dass der Popupblocker deaktiviert ist):

Melden Sie sich mit Ihren SCC-Anmeldeinformationen an, wenn Sie dazu aufgefordert werden.



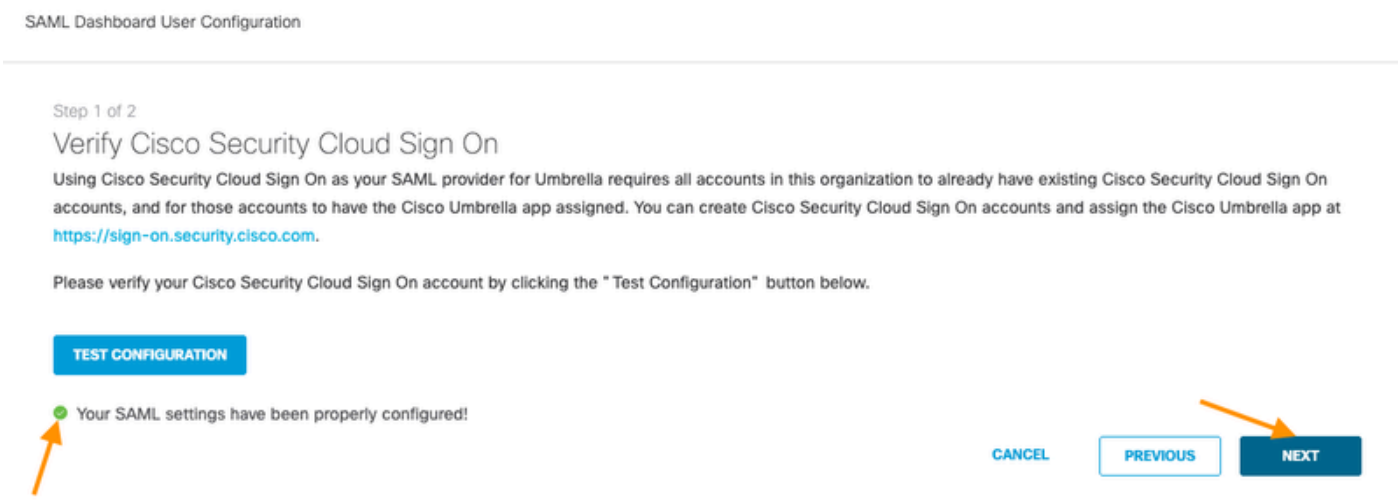


Wenn die Anmeldung verifiziert wurde, müssen Sie die Nachricht hier abrufen und bestätigen. An diesem Punkt ist der SAML-Teil fast abgeschlossen:

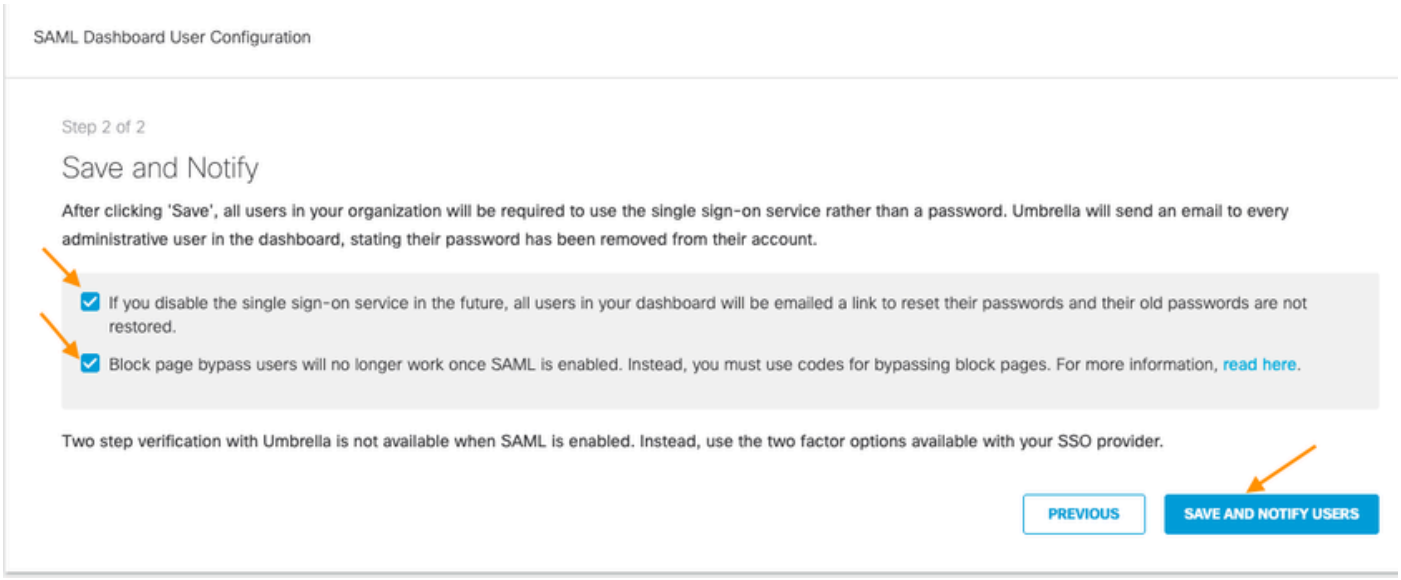


Anschließend müssen Sie erneut zum Abschnitt der SAML Dashboard-Benutzerkonfiguration zurückkehren:

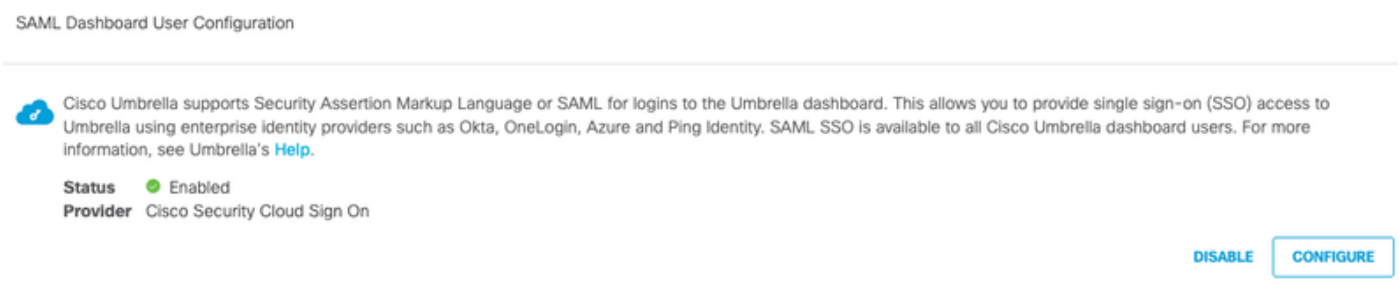
- Ein grünes Häkchen zeigt an, dass die SAML-Einstellungen korrekt konfiguriert wurden.
- Wählen Sie WEITER aus, um fortzufahren.



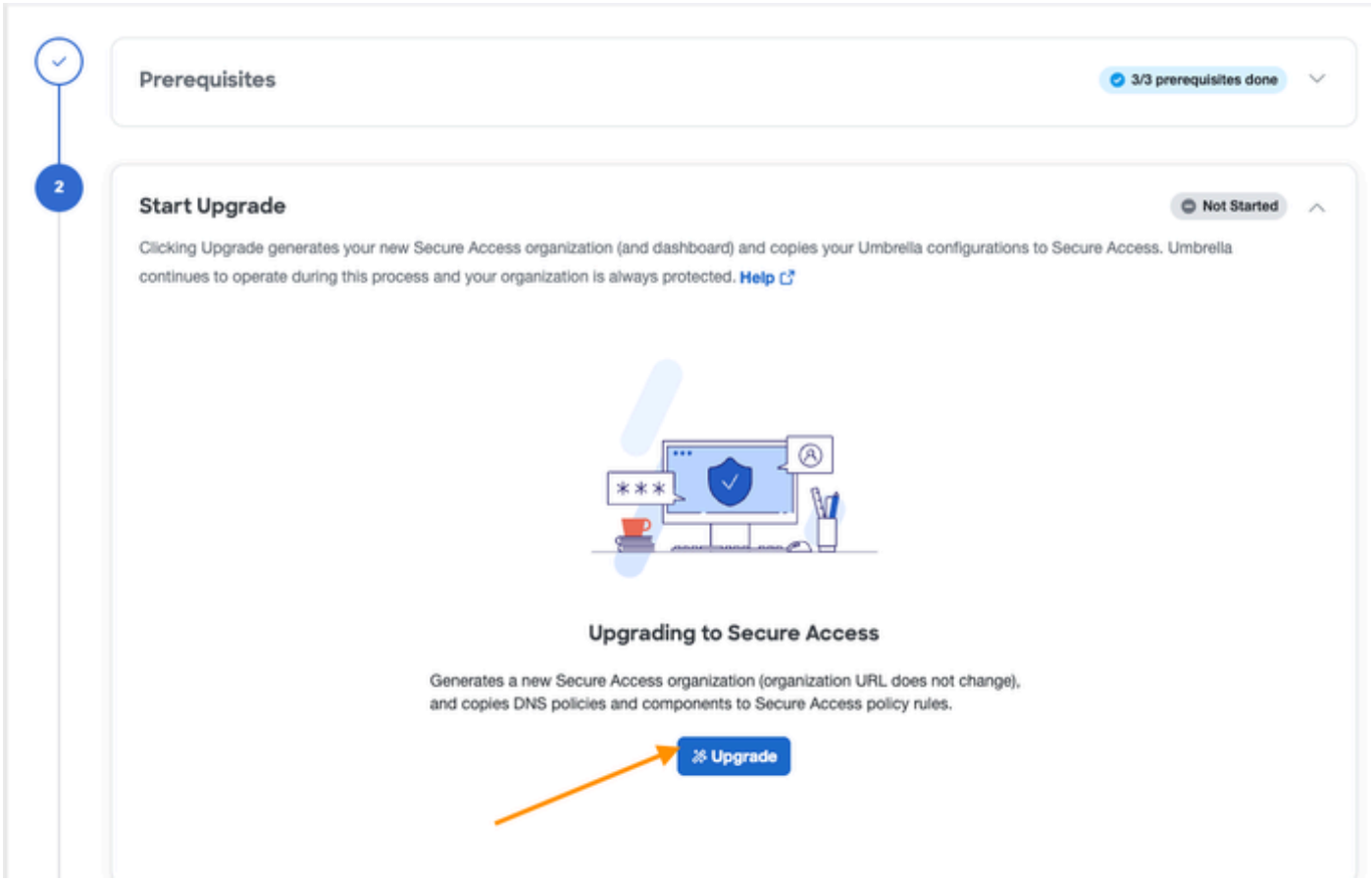
Speichern und Benutzer über die Änderungen informieren:



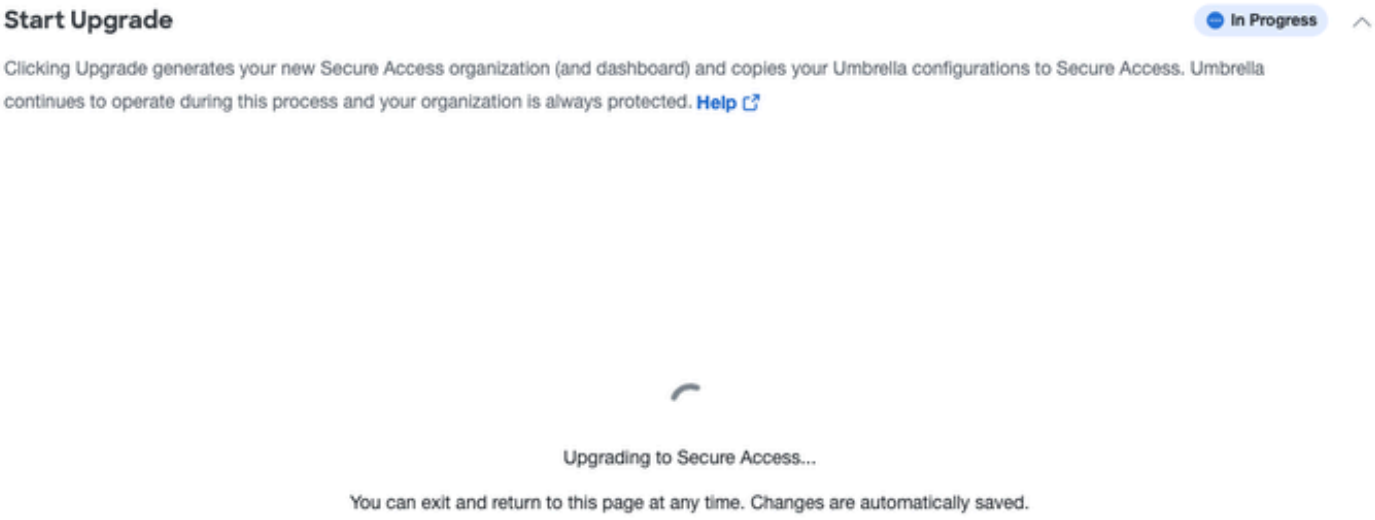
SAML-Konfiguration abgeschlossen:



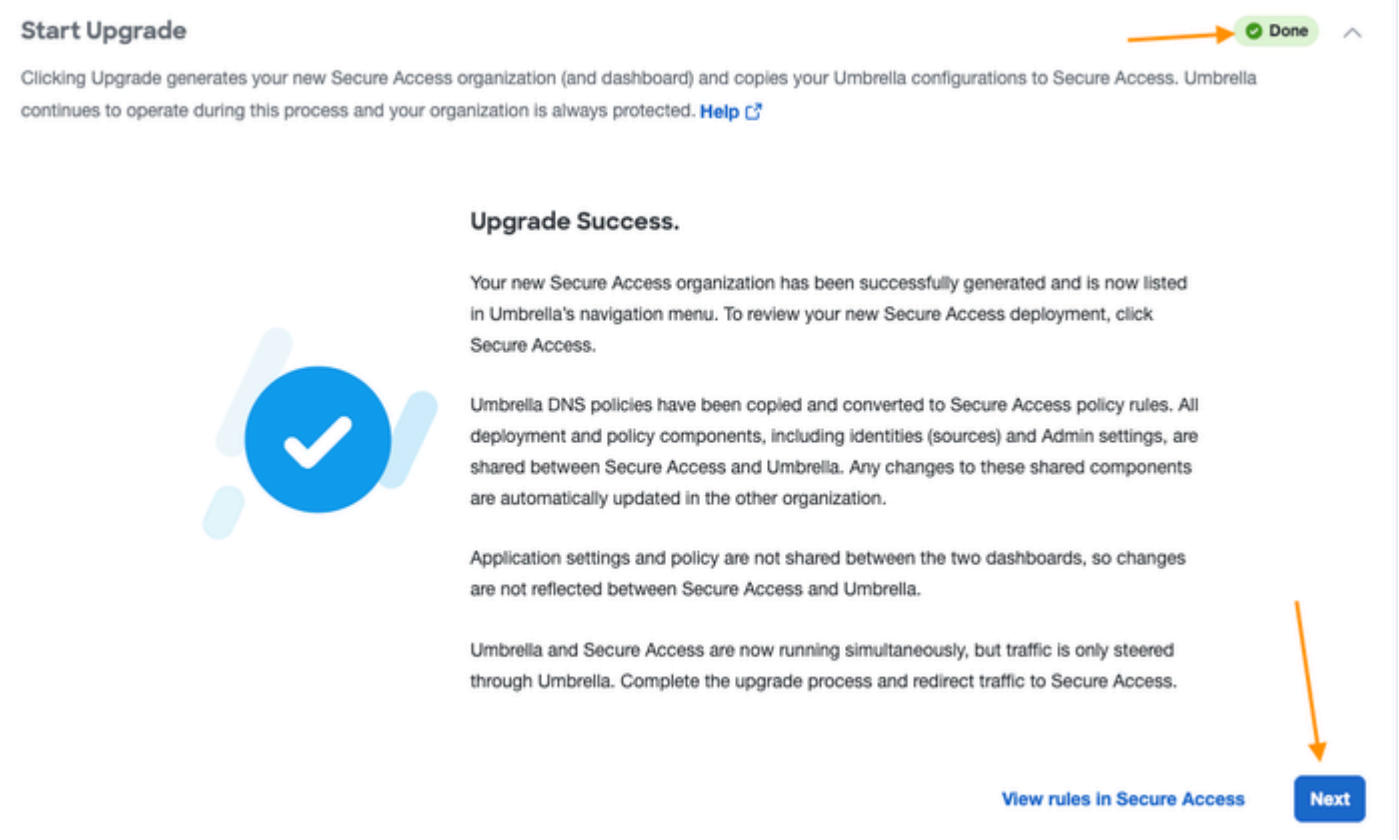
7. Führen Sie ein Upgrade auf sicheren Zugriff durch, indem Sie im Abschnitt Upgrade starten die Option Upgrade auswählen:



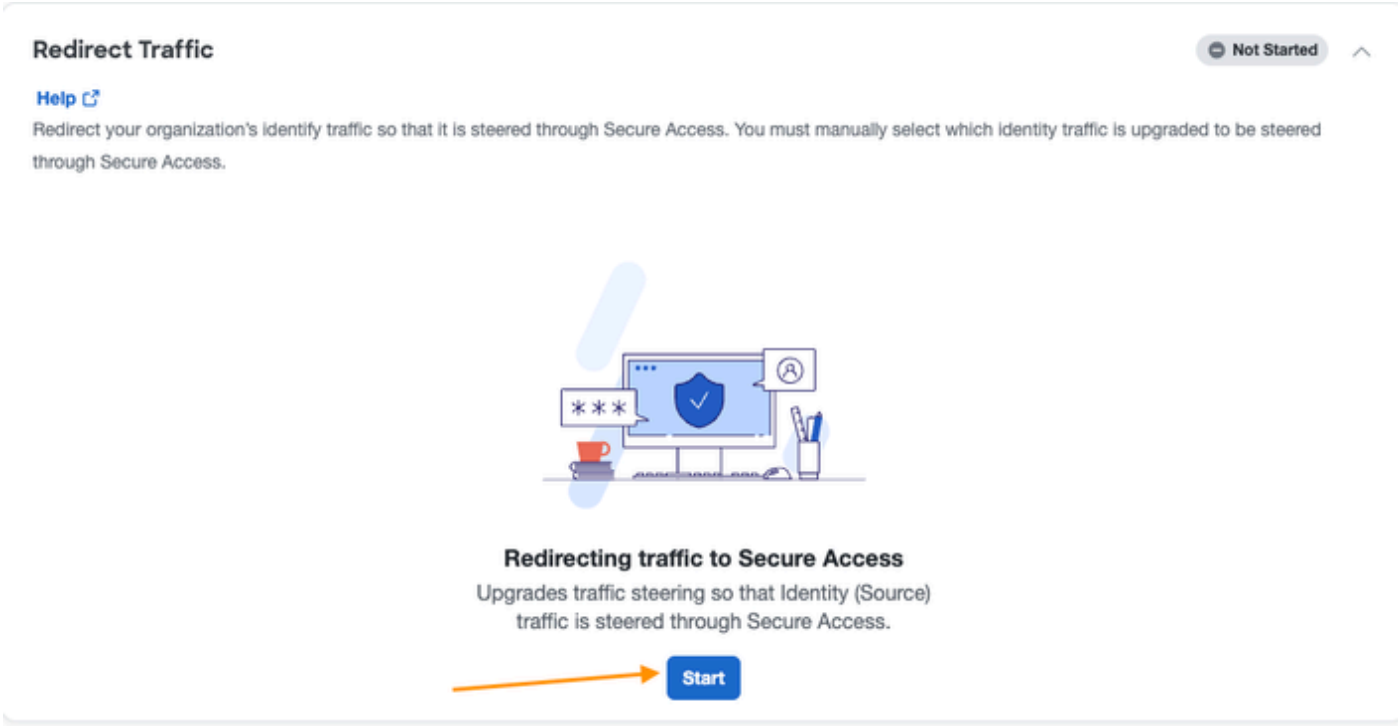
- Warten Sie, bis das Upgrade fortgesetzt wird:



- Wenn Sie fertig sind, müssen Sie eine Seite wie auf dem Bild hier:

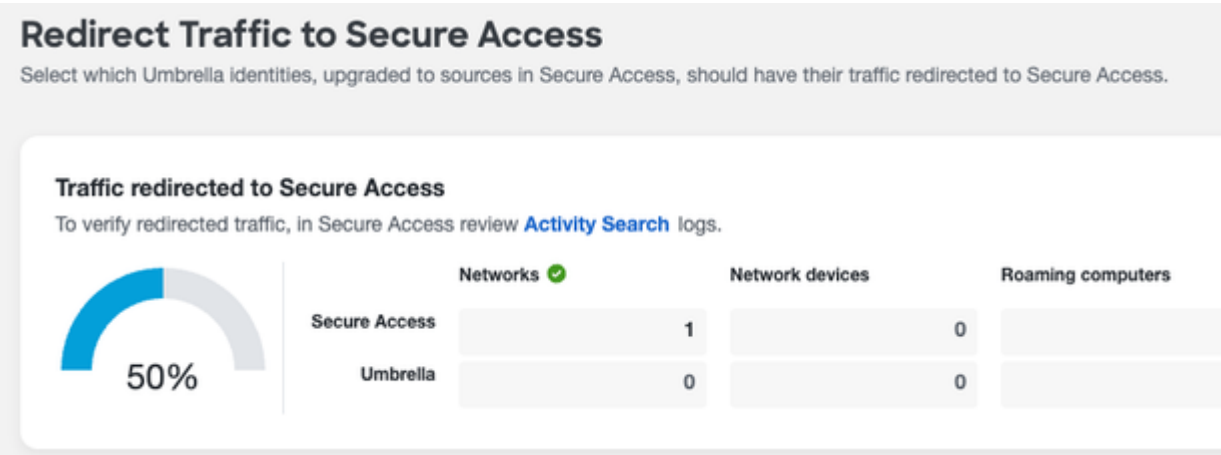


8. Datenverkehr an sicheren Zugriff umleiten



- Bestätigung, dass die Umleitung abgeschlossen wurde. In diesem Beispiel wurde nur die

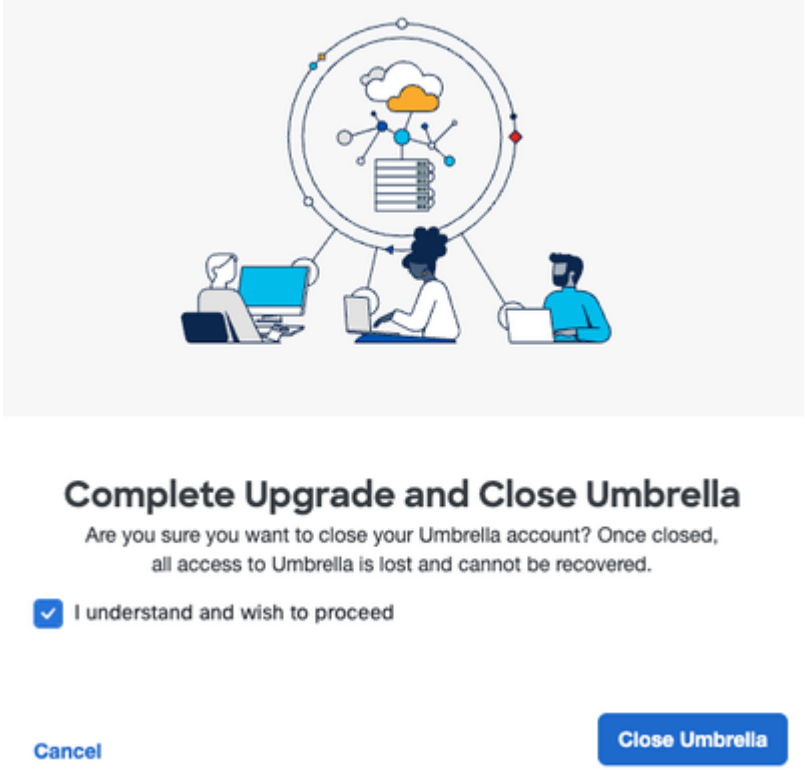
Netzwerkidentität von Umbrella zu Secure Access migriert:



9. Führen Sie das Upgrade und die Migration zu Secure Access durch.

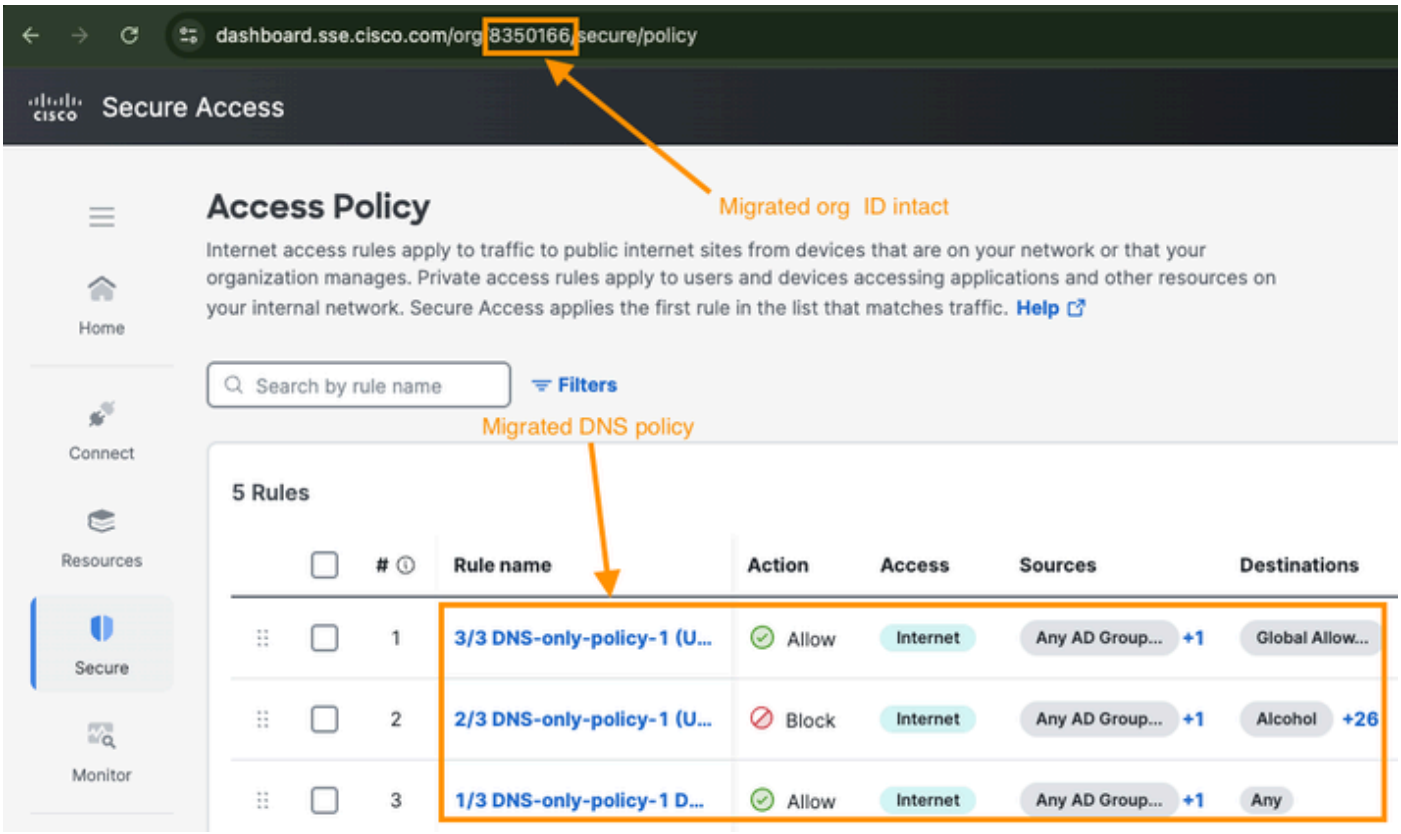
⚠ Vorsicht: Dies entfernt Ihre Umbrella Org vollständig und ist nicht reversibel. Stellen Sie deshalb sicher, dass alle Artikel vollständig migriert wurden, bevor Sie diesen Schritt durchführen.

- Wenn Sie auf dem Bild hier die Option Umbrella schließen auswählen, verlieren Sie beim Löschen den Zugriff auf Ihre Umbrella-Organisation:



Migration überprüfen

1. Melden Sie sich mit Ihren Anmeldeinformationen bei Secure Access an.
2. Navigieren Sie zu Sicher > Zugriffsrichtlinie, um die migrierten Regeln anzuzeigen, wie im Beispiel hier. Die Organisations-ID muss mit der ID im Abschnitt Vorbereitung der Migration oben übereinstimmen.



Zugehörige Informationen

- Umbrella-Dokumentation
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.