

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

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Vorbereitungsphasen](#)

[1. Vorbereitung auf die Migration](#)

[2. Melden Sie sich mit Ihren bestehenden Cisco Anmeldeinformationen bei SCC an.](#)

[3. Link Umbrella Org zu SCC und Anspruch Abonnement](#)

[4. Wenden Sie die Lizenz auf die Instanz für sicheren Zugriff an](#)

[Sichere Zugriffsverbindung mit SCC überprüfen](#)

[1. Produktaktivierungsstatus in "Abonnements"](#)

[2. Sicherer Zugriff in der Produktliste](#)

[Migration von Umbrella zu Secure Access](#)

[Migration überprüfen](#)

[Zugehörige Informationen](#)

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

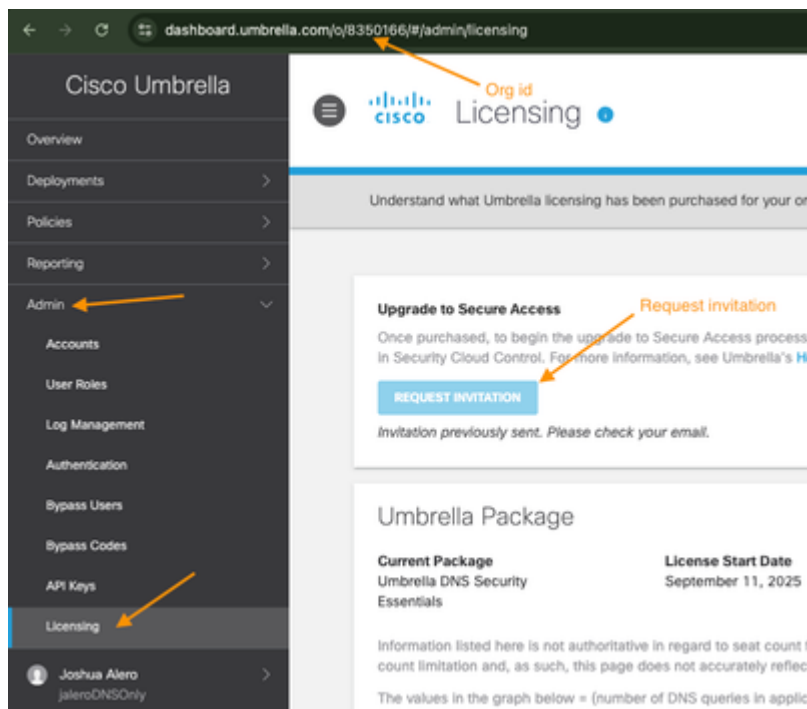
- Aktuelles DNS- oder SIG-Abonnement
- Vollständiger Administratorzugriff auf Umbrella
- Zugriff auf Cloud-Sicherheitskontrolle

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:



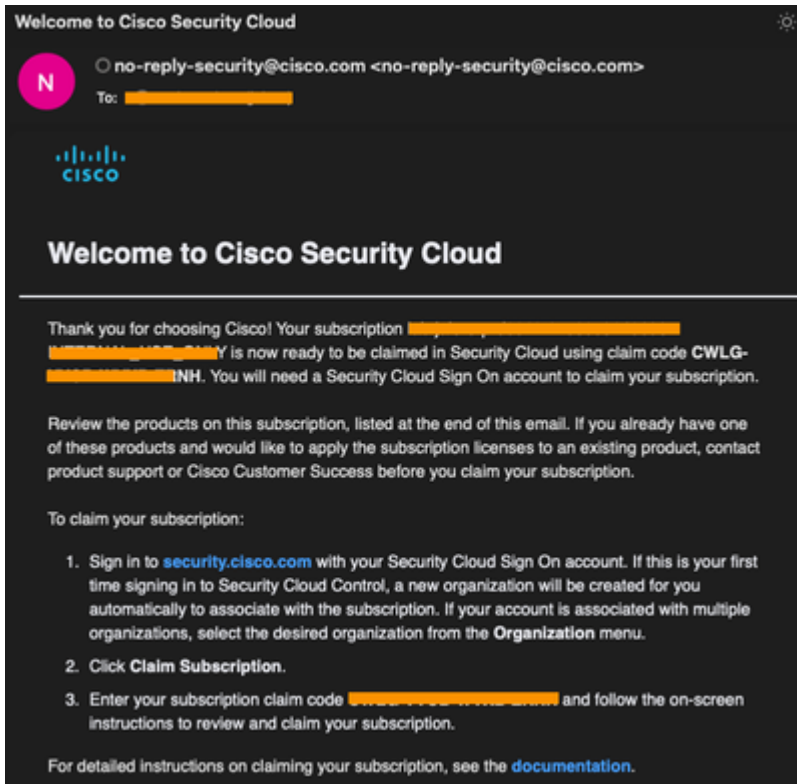
ii) Notieren Sie sich die Organisations-ID in diesem Beispiel 8350166.

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:

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

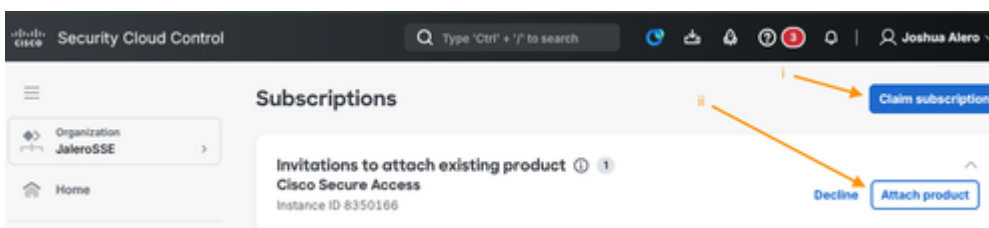
v. Wählen Sie dann Weiter, um die Erstellung der Organisation abzuschließen.

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 Umbrella-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:

Subscriptions

[Claim subscription](#)

8350166_secure-access

Externally managed ⓘ

End date: —

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

Attached

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

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 *

8350166_secure-access-ZRNH

Cancel

Next

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

1 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. 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.

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

- Bestätigen Sie den Abonnementanspruch:

Claim subscription

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

Buttons: Cancel, Claim

- 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:

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 1

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

i. Wählen Sie die Option "Aktion erforderlich":

Product and service activation status 1



Cisco Secure Access DNS Advantage

Start date 09/16/2025

[Action required](#)

ii) Wählen Sie Lizenz anwenden:

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



Sichere Zugriffsverbindung mit SCC überprüfen

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

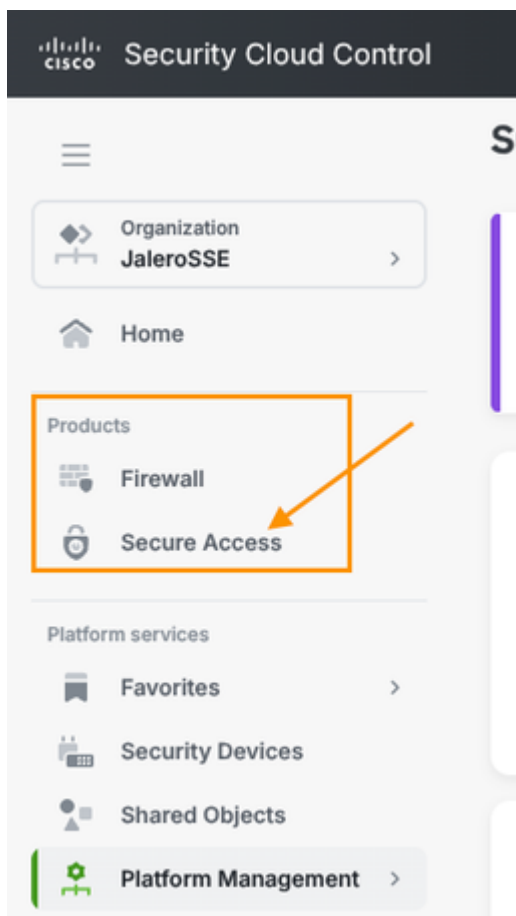
1. Produktaktivierungsstatus in "Abonnements"

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

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

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:

dashboard.umbrella.com/o/8350166/#/overview?encodedFilters=JTdCJTlYWN0aW9uJTlYJTlYmXvY2t1ZCUyMiUyQyUyMnNlbGVjdGVkRGF0ZVJhbmdlSWR4J...

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

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

 **Authentication**

Set up single sign-on via SAML for Umbrella dashboard users and check on the status of two-step verification for your account.

 **Prerequisite 1 : Enable Cisco Security Cloud Sign On**
Update your Umbrella SAML provider to Cisco Security Cloud Sign On [Return to Upgrade Manager](#)

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  Disabled
Provider None

Enable  [ENABLE SAML](#)

Two-Step Verification

 This indicates whether two-step verification (2FA) is enabled for your user account. If you wish to enable this feature, navigate to Admin > Accounts and expand the account you're logged in as by clicking on the account name, then select Enable to get started. For more information, see Umbrella's [Help](#).

Status  Enabled

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

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](#) 

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

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

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



CONNECTING TO CISCO UMBRELLA

Security Cloud Sign On

Email

Password

 [Show](#)

[Forgot password](#)



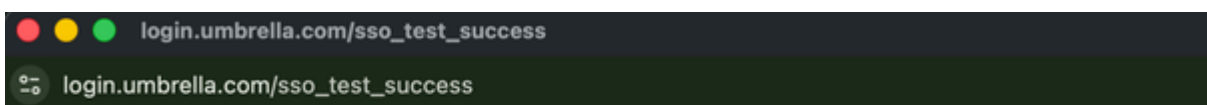
Multifactor authentication

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



[Finish](#)

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



Success!

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

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.

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**

Speichern und Benutzer über die Änderungen informieren:

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**

SAML-Konfiguration abgeschlossen:

SAML Dashboard User Configuration

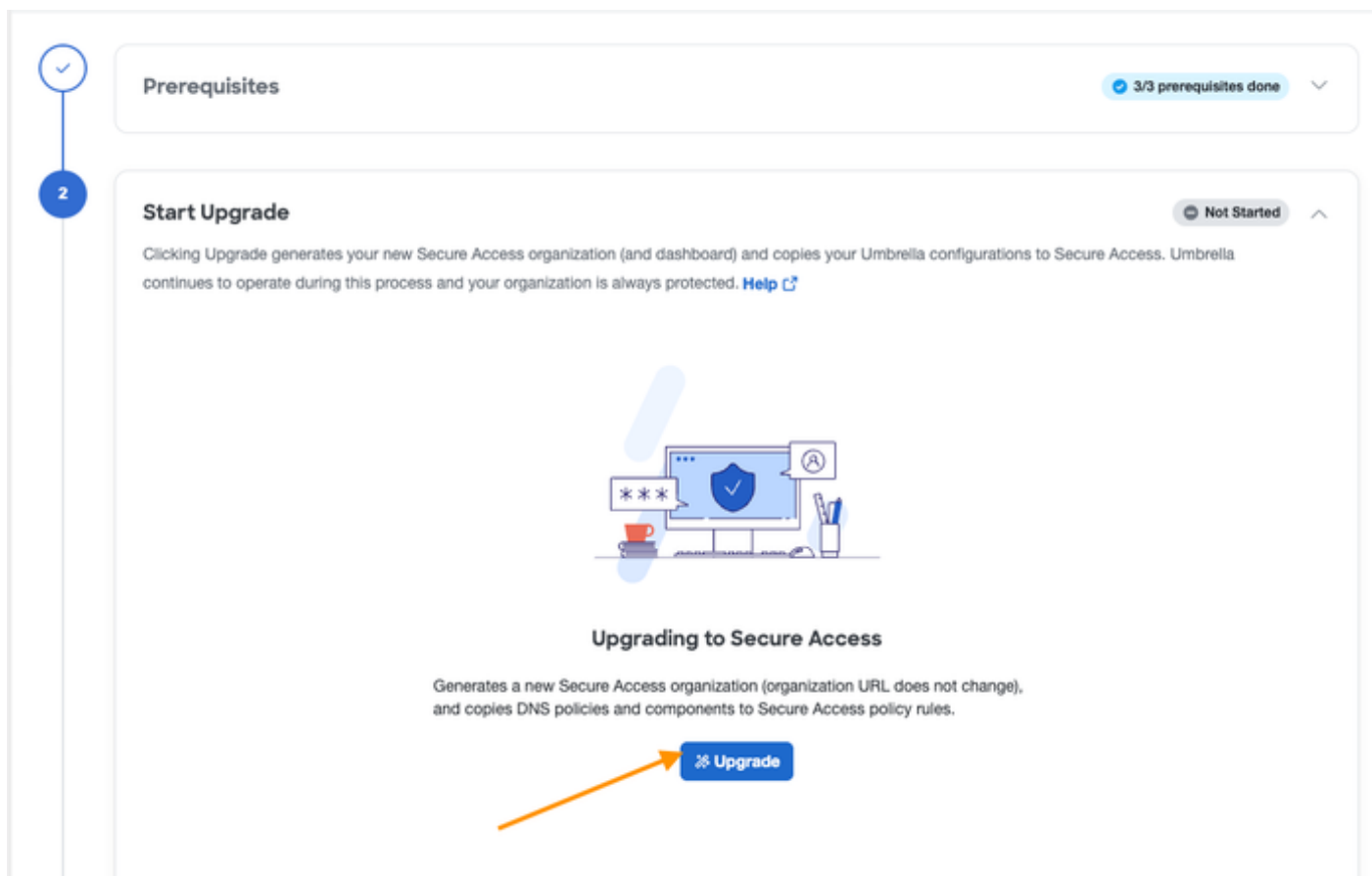
Cisco Umbrella supports Security Assertion Markup Language or SAML for logins to the Umbrella dashboard. This allows you to provide single sign-on (SSO) access to Umbrella using enterprise identity providers such as Okta, OneLogin, Azure and Ping Identity. SAML SSO is available to all Cisco Umbrella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

Status ✔ Enabled

Provider Cisco Security Cloud Sign On

DISABLE **CONFIGURE**

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



Prerequisites 3/3 prerequisites done

Start Upgrade Not Started

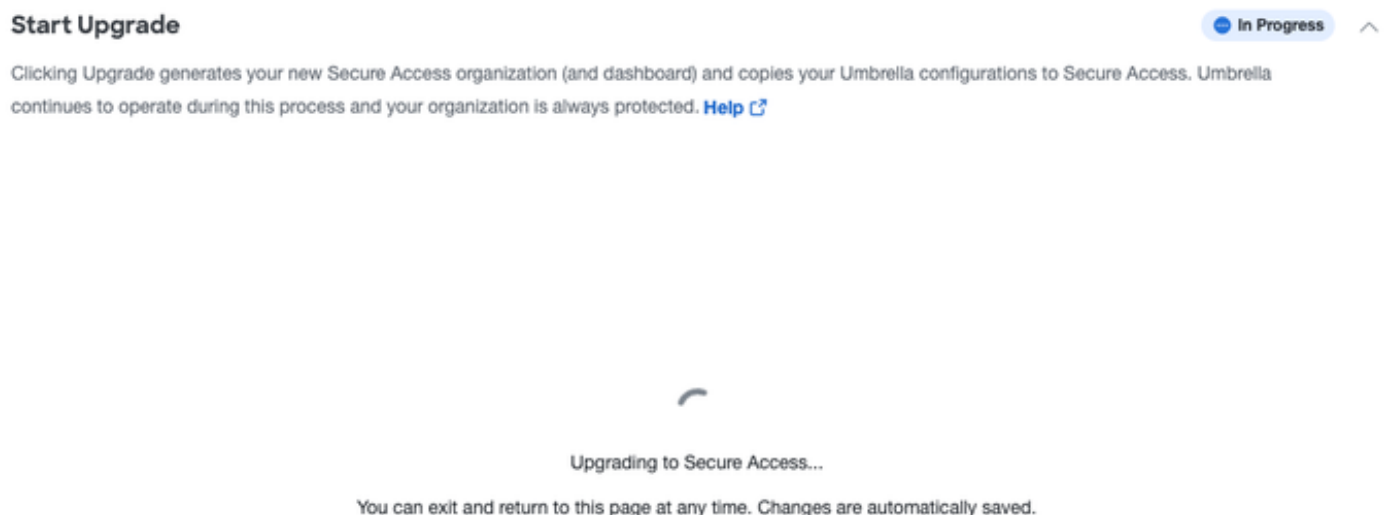
Clicking Upgrade generates your new Secure Access organization (and dashboard) and copies your Umbrella configurations to Secure Access. Umbrella continues to operate during this process and your organization is always protected. [Help](#)

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](#)

- Warten Sie, bis das Upgrade fortgesetzt wird:



Start Upgrade In Progress

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.

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

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. Datenverkehr an sicheren Zugriff umleiten

Redirect Traffic

Not Started

[Help](#)

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



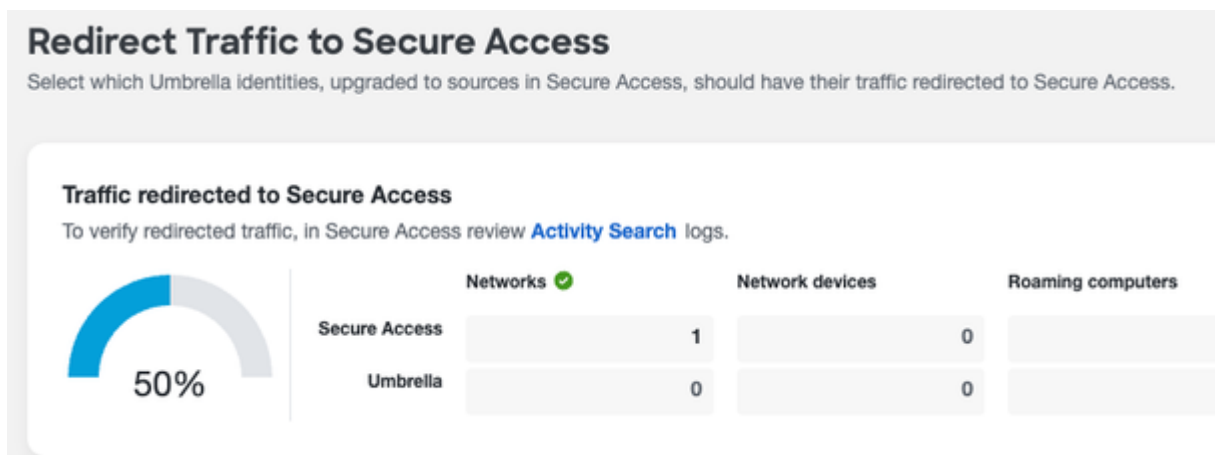
Redirecting traffic to Secure Access

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

Start

- 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:



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](#)

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.

← → ↻ 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

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.