

Paraplu configureren voor migratie naar veilige toegang en cloudbeveiliging

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vorbereidingsfasen](#)

[1. Vorbereiden op migratie](#)

[2. Meld u aan bij SCC met uw bestaande Cisco-aanmeldingsreferenties](#)

[3. Paraplu-organisatie koppelen aan SCC en claimabonnement](#)

[4. De licentie toepassen op Secure Access Instance](#)

[Beveiligde toegangskoppeling naar SCC verifiëren](#)

[1. Productactiveringsstatus in Abonnementen](#)

[2. Veilige toegang in de lijst met producten](#)

[Migreren van paraplu naar beveiligde toegang](#)

[Migratie controleren](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u kunt migreren van Umbrella naar Secure Access met Security Cloud Control (SCC).

Achtergrondinformatie

Umbrella-klanten worden aangemoedigd om van Umbrella naar Secure Access te migreren en moeten Security Cloud Control gebruiken om al hun cloudbeveiligingsproducten te beheren als onderdeel van deze wijzigingen. Hiermee kunt u één venster gebruiken om hun cloudbeveiligingsproducten te beheren, waaronder Cisco Secure Access.

Multi-org en MSSP worden momenteel niet ondersteund (ten tijde van het aanmaken van dit artikel).

Voorwaarden

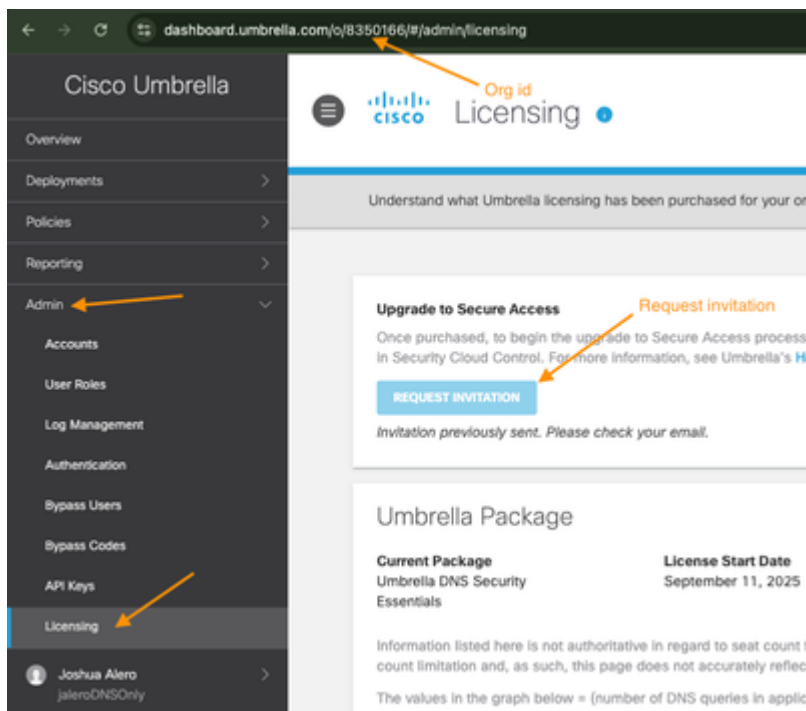
- Huidig DNS- of SIG-abonnement
- Volledige toegang tot de paraplu
- Toegang tot Cloud Security Control

Vorbereidingsfasen

1. Vorbereiden op migratie

1. Zorg ervoor dat je een DNS- of SIG-abonnement hebt op Umbrella:

- Navigeer naar Beheer > Licenties om te controleren
- Upgrade naar Secure Access moet bovenaan de pagina worden weergegeven:



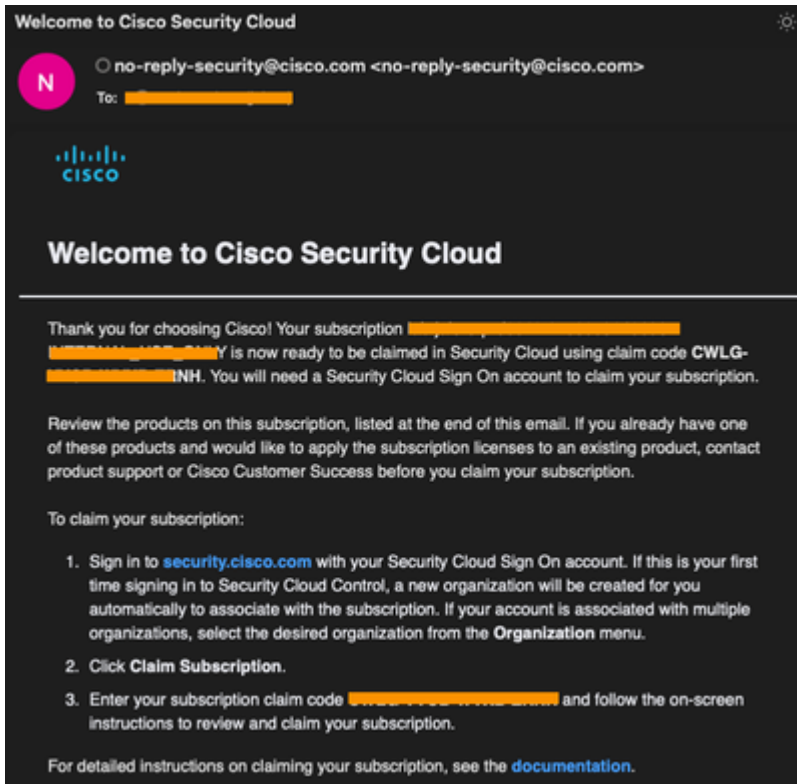
ii. Noteer de org ID, in dit voorbeeld 8350166.

iii. Selecteer de optie Uitnodiging aanvragen op de licentiepagina.

 **Belangrijk:** de knop Uitnodiging aanvragen dient als uitnodiging om lid te worden van de Umbrella-huurder voor SCC. Er wordt geen claimcode gegenereerd. Een claimcode wordt aan u verstrekt zodra uw bestelling voor beveiligde toegang is voltooid. Dit maakt deel uit van het migratieproces naar Secure Access.

 **Opmerking:** als de upgrade naar Secure Access niet aanwezig is, moet u ervoor zorgen dat het paraplu-pakket DNS of SIG is (multi-org of ad-ons worden momenteel niet ondersteund op het moment dat dit artikel wordt geschreven).

iv. Ervan uitgaande dat u uw bestelling voor Secure Access hebt geplaatst, wacht 3-4 werkdagen en u moet een e-mail ontvangen met uw abonnementsclaimcode (na het initiëren van de uitnodiging van uw Umbrella Tenant). Zie voorbeeld e-mail hier:



2. Meld u aan bij SCC met uw bestaande Cisco-aanmeldingsreferenties

i. Navigeer naar het [Security Cloud Control-portaal](#) en log in met uw Cisco-inloggegevens.



Opmerking: dezelfde Cisco-aanmeldingsreferenties die worden gebruikt om toegang te krijgen tot uw Umbrella-dashboard.

ii. Selecteer Nieuwe organisatie maken (als u geen bestaande organisatie hebt).

iii. Voer de nieuwe organisatienaam in het veld Nieuwe organisatienaam in.

iv. Selecteer de juiste regio in het vervolgkeuzemenu Regio-implementatie.



Opmerking: Dit moet de geografische regio zijn waar uw huurder naartoe wordt gestuurd.

Voorbeeld hier:

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

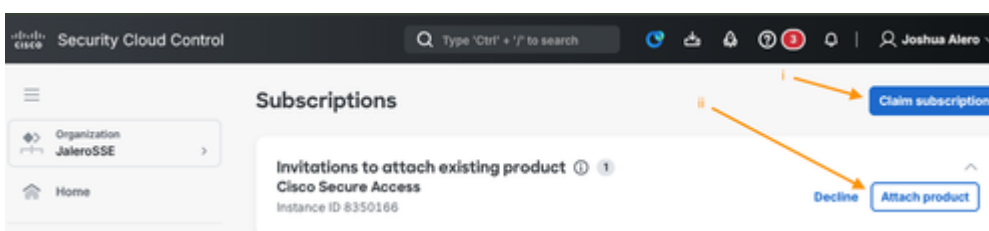
v. Selecteer vervolgens Doorgaan om het maken van de organisatie te voltooien.

3. Paraplu-organisatie koppelen aan SCC en claimabonnement

i. Selecteer de knop Abonnement claimen om het te claimen met de codes uit stap 1 hierboven.

ii. Uw Paraplu-ID moet worden gezien op de pagina Abonnementen en met de uitnodiging om deze aan SCC toe te voegen.

 **Opmerking:** de ID van de paraplu-organisatie moet hetzelfde zijn als op het dashboard van de paraplu. Dit is belangrijk voor de migratie en om ervoor te zorgen dat zowel SCC als Umbrella aan elkaar zijn gekoppeld.



- Selecteer Product bevestigen om uw paraplu-org aan SCC te bevestigen.

- Als u de Cisco Secure Access als een product ziet op dezelfde pagina als in het onderstaande voorbeeld:

Subscriptions Claim subscription

8350166_secure-access Externally managed ⓘ

End date: —

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

Note: An orange arrow points to 'Cisco Secure Access' with the label 'Attached'.

iii. Voer de claimcode in en selecteer Volgende:

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 *

Cancel Next

Note: An orange arrow points to the 'Next' button.

iv. Selecteer Bestaande instantie koppelen in de keuzelijst Nieuwe instantie maken of Bestaande instantie toevoegen:

- 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

Note: An orange arrow points to the 'Attach existing instance' dropdown menu.

v. Controleer de instellingen:

- Zorg ervoor dat de (bestaande instantie) deel uitmaakt van de productnaam
- De regio moet worden ingesteld op de bestaande regio van de gekoppelde Secure Access-instantie
- Selecteer Claim verplaatsen naar de volgende pagina

Enter subscription claim code

Review products

3 Review subscription

Review subscription

Subscription ID
Organization
region
Europe

Products	Deployments
Cisco Secure Access DNS Advantage (Existing instance)	Region per existing deployment 1

Cancel Back Claim

- De claim op het abonnement bevestigen:

Claim subscription

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

Cancel Claim

- Na succesvolle claim en levering moet u een pagina met abonnementen krijgen die vergelijkbaar is met de pagina hier, met al uw geactiveerde producten:

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. De licentie toepassen op Secure Access Instance

i. Selecteer de optie Actie vereist:

Product and service activation status 1



Cisco Secure Access DNS Advantage

Start date 09/16/2025

[Action required](#)

ii. Selecteer Licentie toepassen:

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



Beveiligde toegangskoppeling naar SCC verifiëren

Gebruik dit gedeelte om te controleren of uw Secure Access-tenant is gekoppeld aan SCC.

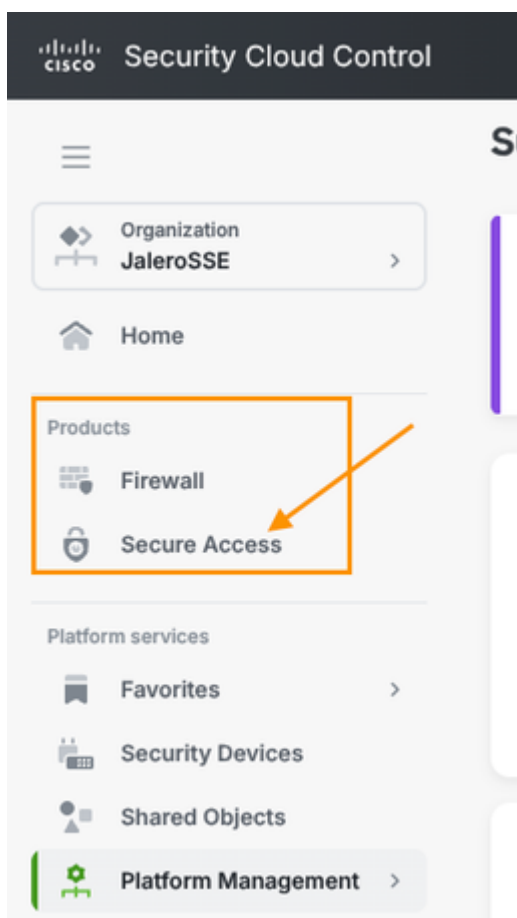
1. Productactiveringsstatus in Abonnementen

Controleer of de productinstantie Cisco Secure Access <Licentietype> is geactiveerd:

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

2. Veilige toegang in de lijst met producten

Veilige toegang moet nu ook worden vermeld onder Producten:



Migreren van paraplu naar beveiligde toegang

1. Log terug in bij Umbrella met hetzelfde account als hierboven.
2. Navigeer naar het nieuwe menu-item Upgrade Manager:

dashboard.umbrella.com/o/8350166/#/overview?encodedFilters=JTdCJTlYWN0aW9uJTlYJTlYJTlYmXvY2tZCUyMiUyQyUyMnNlbGVjdGVkRGF0ZVJhbmdlSWR4J...

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. Selecteer op de pagina Upgrade Manager de optie Start onder Aanmelden Cisco Security Cloud inschakelen

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. Selecteer SAML INSCHAKELEN onder Gebruikersconfiguratie SAML-dashboard om uw SCC te koppelen als SAML-provider voor aanmelding bij het dashboard:

 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. Test de SAML-configuratie met de optie TESTCONFIGURATIE:

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. De aanmeldingspagina van SCC moet in een ander pop-upvenster worden weergegeven (zorg ervoor dat pop-upblokkering is uitgeschakeld):

Meld u desgevraagd aan met uw SCC-referenties.



CONNECTING TO CISCO UMBRELLA

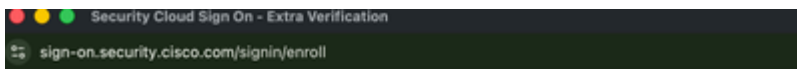
Security Cloud Sign On

Email

Password

 [Show](#)

[Forgot password](#)



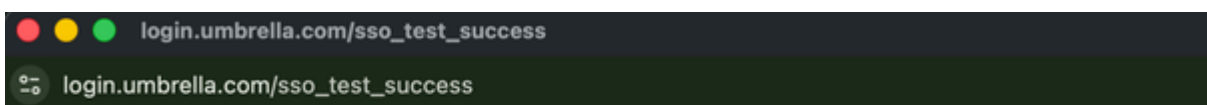
Multifactor authentication

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



[Finish](#)

Wanneer de login is geverifieerd, moet u het bericht hier krijgen, bevestigend. Op dat punt is het SAML-onderdeel bijna voltooid:



Success!

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

U moet dan opnieuw worden teruggestuurd naar het gedeelte Gebruikersconfiguratie SAML Dashboard:

- Groen vinkje geeft aan dat de SAML-instellingen correct zijn geconfigureerd
- Selecteer VOLGENDE om door te gaan

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**

Sla de wijzigingen op en stel de gebruikers op de hoogte:

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-configuratie voltooid:

SAML Dashboard User Configuration

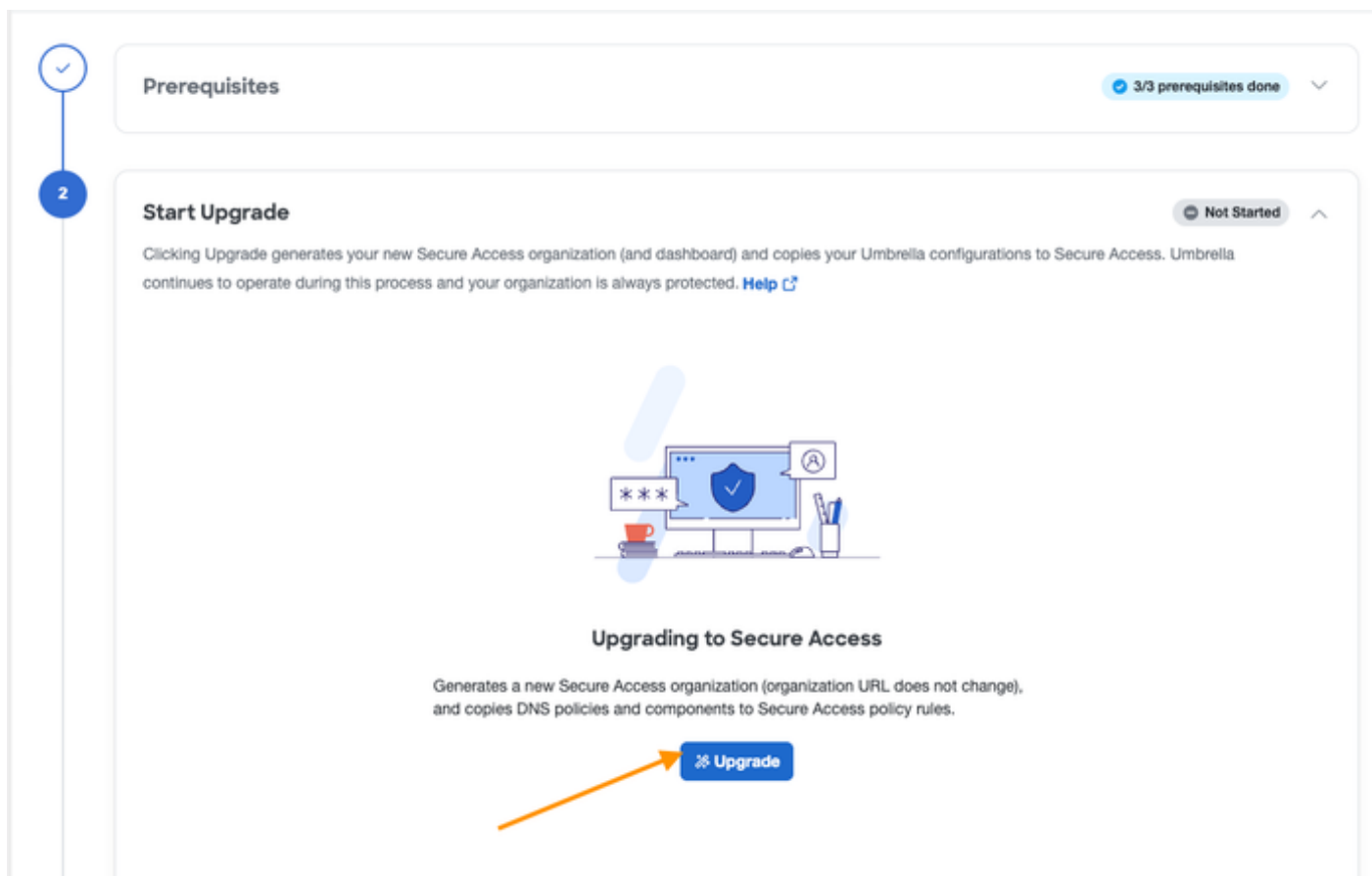
 Cisco Umbrella supports Security Assertion Markup Language or SAML for logins to the Umbrella dashboard. This allows you to provide single sign-on (SSO) access to Umbrella using enterprise identity providers such as Okta, OneLogin, Azure and Ping Identity. SAML SSO is available to all Cisco Umbrella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

Status  Enabled

Provider Cisco Security Cloud Sign On

DISABLE **CONFIGURE**

7. Upgrade naar Beveiligde toegang door in het gedeelte Upgrade starten de optie Upgrade te selecteren:



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](#)

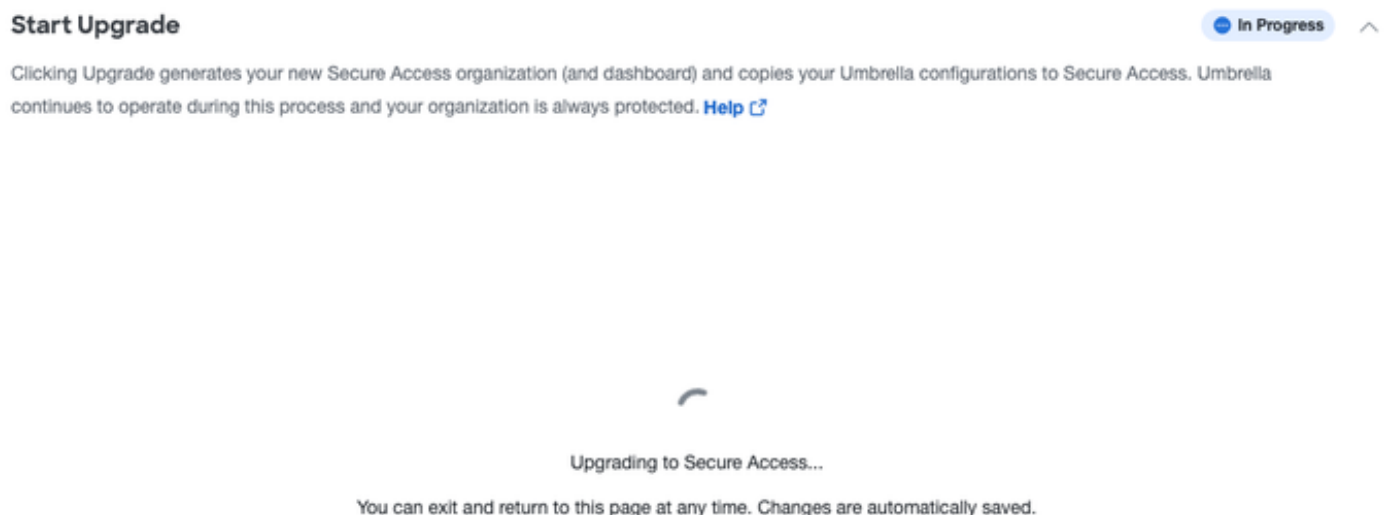


Upgrading to Secure Access

Generates a new Secure Access organization (organization URL does not change), and copies DNS policies and components to Secure Access policy rules.

[Upgrade](#)

- Laat de upgrade doorgaan:



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.

- Als je klaar bent, moet je een pagina zoals op de afbeelding hier te krijgen:

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. Verkeer omleiden naar beveiligde toegang

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.



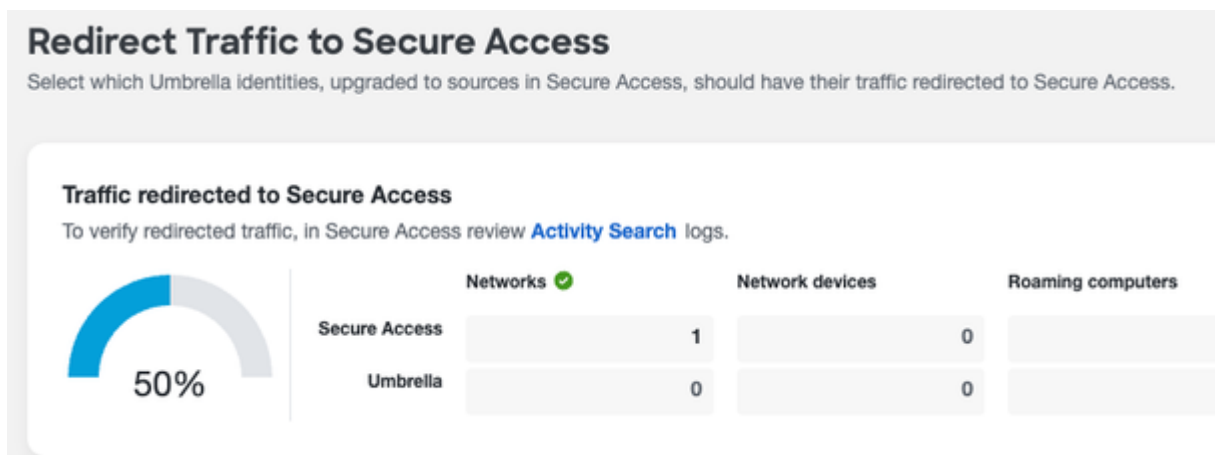
Redirecting traffic to Secure Access

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

Start

- Bevestiging van de omleiding wordt voltooid. In het voorbeeld is alleen de netwerkidentiteit

van Umbrella naar Secure Access gemigreerd:



9. Voltooi de upgrade en migratie naar Secure Access

 Let op: Dit verwijdert uw paraplu-org volledig en is niet omkeerbaar, dus zorg ervoor dat alle items volledig zijn gemigreerd voordat u deze stap uitvoert.



- Wanneer u hier Paraplu sluiten op de afbeelding selecteert, verliest u de toegang tot uw paraplu als deze wordt verwijderd:



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](#)

Migratie controleren

1. Meld u aan bij [Secure Access](#) met uw aanmeldingsgegevens
2. Navigeer naar Beveiligd > Toegangsbeleid om de gemigreerde regels weer te geven, zoals in het voorbeeld hier. De organisatie-ID moet hetzelfde zijn als in het gedeelte Voorbereiden op migratie hierboven.

← → ↻ 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

Gerelateerde informatie

- [overkoepelende documentatie](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.