

# Configurazione di Umbrella per la migrazione a Secure Access e Security Cloud Control

## Sommario

---

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Fasi di preparazione](#)

[1. Preparare la migrazione](#)

[2. Accedere a SCC utilizzando le credenziali di accesso Cisco esistenti](#)

[3. Collegare Umbrella.org a SCC e richiedere l'abbonamento](#)

[4. Applicare la licenza all'istanza Secure Access](#)

[Verifica del collegamento di accesso sicuro a SCC](#)

[1. Stato di attivazione del prodotto nelle sottoscrizioni](#)

[2. Accesso sicuro nell'elenco dei prodotti](#)

[Migrazione da Umbrella a Secure Access](#)

[Verifica migrazione](#)

[Informazioni correlate](#)

---

## Introduzione

Questo documento descrive come eseguire la migrazione da Umbrella a Secure Access utilizzando Security Cloud Control (SCC).

### Premesse

I clienti Umbrella sono incoraggiati a migrare da Umbrella a Secure Access e sono obbligati a utilizzare Security Cloud Control per gestire tutti i loro prodotti di sicurezza cloud come parte di queste modifiche. Ciò consente di avere un'unica console per gestire i propri prodotti di sicurezza cloud, tra cui Cisco Secure Access.

Al momento della creazione di questo articolo, le organizzazioni multiple e i provider di servizi condivisi non sono attualmente supportati.

## Prerequisiti

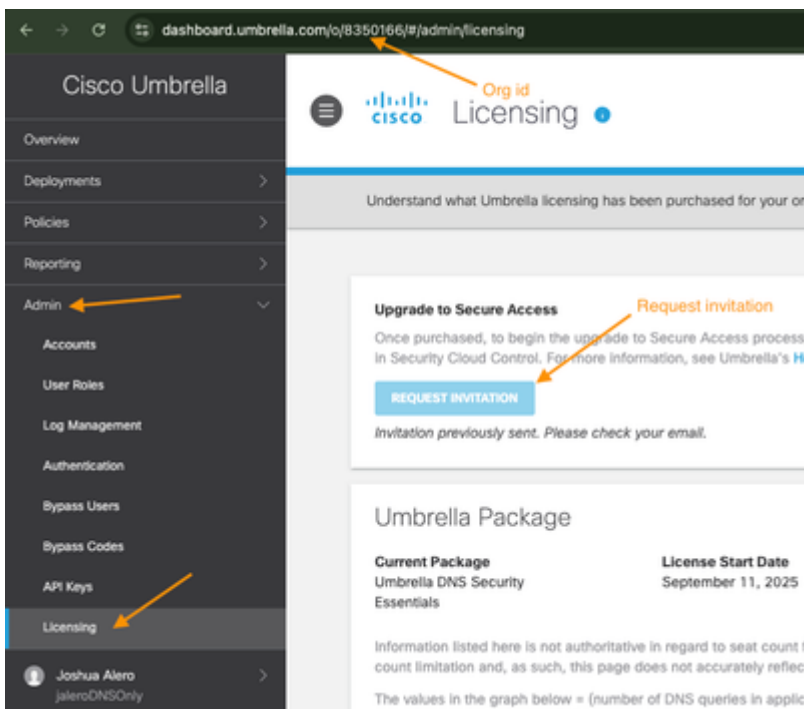
- Sottoscrizione DNS o SIG corrente
- Accesso amministrativo completo a Umbrella
- Accesso a Security Cloud Control

## Fasi di preparazione

### 1. Preparare la migrazione

1. Assicurati di disporre di un abbonamento DNS o SIG su Umbrella:

- Selezionare Admin > Licensing per verificare
- L'aggiornamento ad Accesso sicuro deve essere visualizzato nella parte superiore della pagina:



ii. Prendere nota dell'ID organizzazione, in questo esempio 8350166.


iii. Selezionare l'opzione Richiedi invito nella pagina delle licenze.

---


 **Importante:** Il pulsante Richiedi invito consente di partecipare al tenant Umbrella per SCC.

---


---

 Non viene generato un codice attestazione. Una volta completato l'ordine per l'accesso sicuro, riceverai un codice di richiesta. Questa operazione fa parte del processo di migrazione verso l'accesso protetto.

---

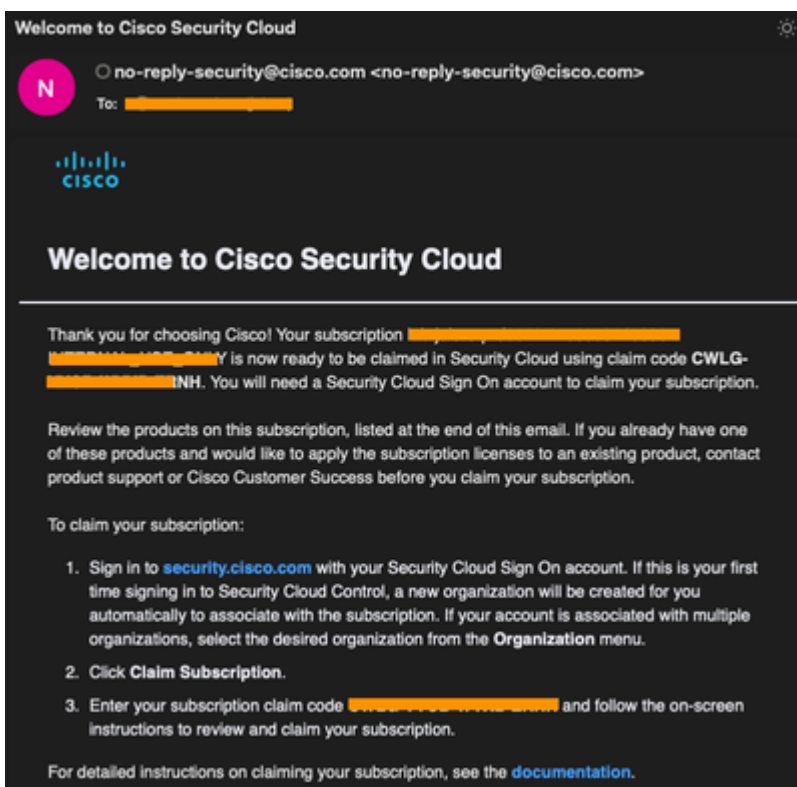
 Nota: La migrazione è un servizio a pagamento disponibile solo per i clienti che hanno acquistato un abbonamento Cisco Secure Access. L'invito può essere richiesto solo dopo l'acquisto della sottoscrizione Accesso sicuro.

---

 Nota: Se l'aggiornamento all'accesso sicuro non è presente, verificare che il pacchetto Umbrella sia DNS o SIG (più organizzazioni o componenti aggiuntivi non sono attualmente supportati al momento della scrittura di questo articolo).

---

iv. Supponendo di aver effettuato l'ordine per Secure Access, attendere 3-4 giorni lavorativi e ricevere un'e-mail con il codice di richiesta di abbonamento (dopo aver avviato la richiesta di invito dal tenant Umbrella). Vedere l'esempio di e-mail:



## 2. Accedere a SCC utilizzando le credenziali di accesso Cisco esistenti

i. Passare al [portale Security Cloud Control](#) e accedere con le credenziali di accesso Cisco.

---

 Nota: Le stesse credenziali di accesso Cisco usate per accedere al dashboard Umbrella.

---

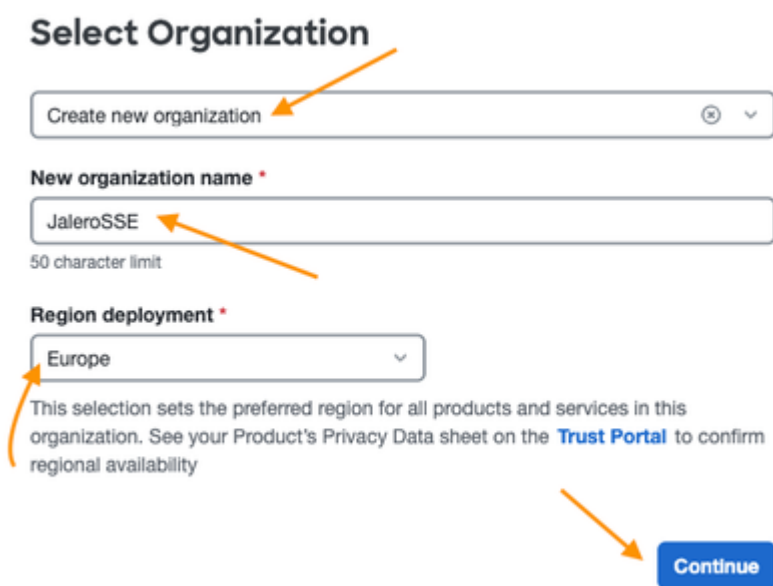
- ii. Selezionare Crea nuova organizzazione (se non ne esiste una esistente).
- iii. Inserire il nuovo nome dell'organizzazione nel campo Nuovo nome organizzazione.
- iv. Selezionare l'area appropriata dal menu a discesa Distribuzione area.

---

 Nota: questa deve essere l'area grafica in cui il tenant verrebbe distribuito.

---

Esempio:



**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. Quindi selezionare Continua per completare la creazione dell'organizzazione.

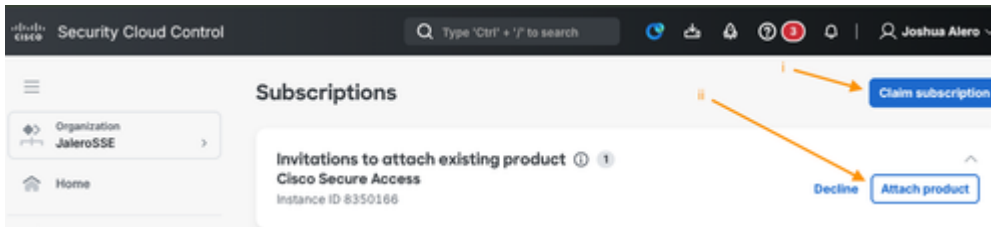
### 3. Collegare Umbrella org a SCC e richiedere l'abbonamento

- i. Selezionare il pulsante Richiedi sottoscrizione per richiederlo con i codici forniti dal passaggio 1 precedente.
- ii. L'ID organizzazione Umbrella deve essere visualizzato nella pagina Sottoscrizioni insieme all'invito ad allegarlo a SCC.

---

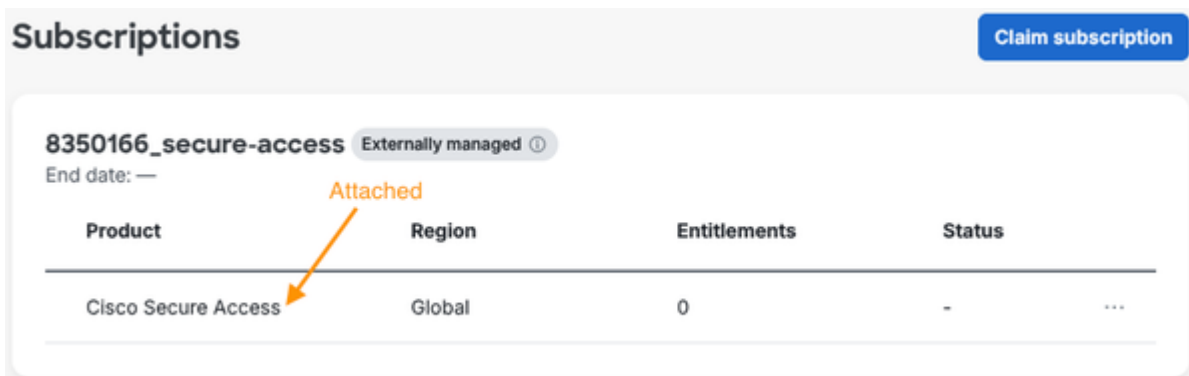
 Nota: L'ID organizzazione Umbrella deve corrispondere a quello del dashboard Umbrella. Ciò è importante per la migrazione e per garantire che sia SCC che Umbrella siano state collegate.

---

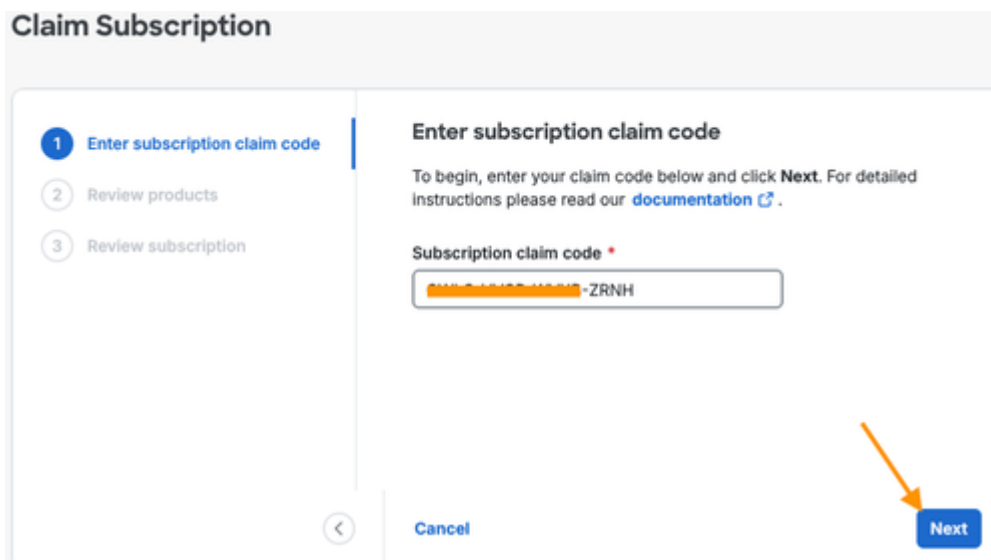


- Selezionare Attach product (Allega prodotto) per collegare l'organizzazione Umbrella a SCC.

- Se collegato, Cisco Secure Access deve essere visualizzato come prodotto nella stessa pagina come mostrato nell'esempio seguente:



iii. Immettere il codice attestazione e selezionare Avanti:



iv. Selezionare Attach existing instance dal menu a discesa Create new instance or attach existing:

v. Controllare le impostazioni:

- Verificare che (Istanza esistente) sia parte del nome del prodotto
- L'area deve essere impostata sull'area esistente dell'istanza di accesso protetto collegata
- Selezionare Sposta richiesta di rimborso per passare alla pagina successiva

- Confermare l'attestazione di sottoscrizione:

- Dopo aver completato con successo la richiesta di rimborso e il provisioning, è necessario ottenere una pagina Subscription (Sottoscrizioni) simile a quella riportata di seguito, in cui sono elencati tutti i prodotti attivati:

**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** ^

Cisco Secure Access DNS Advantage Start date 09/16/2025 Action required

---

**8350166\_secure-access** Externally managed ⓘ  
 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	<span style="color: blue;">✔ Activated</span> ...

#### 4. Applicare la licenza all'istanza Secure Access

i. Selezionare l'opzione Azione richiesta:

**Product and service activation status** ^

Cisco Secure Access DNS Advantage Start date 09/16/2025 Action required



ii. Selezionare Applica licenza:

## 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

## Verifica del collegamento di accesso sicuro a SCC

Utilizzare questa sezione per verificare che il tenant Secure Access sia stato collegato a SCC.

### 1. Stato di attivazione del prodotto nelle sottoscrizioni

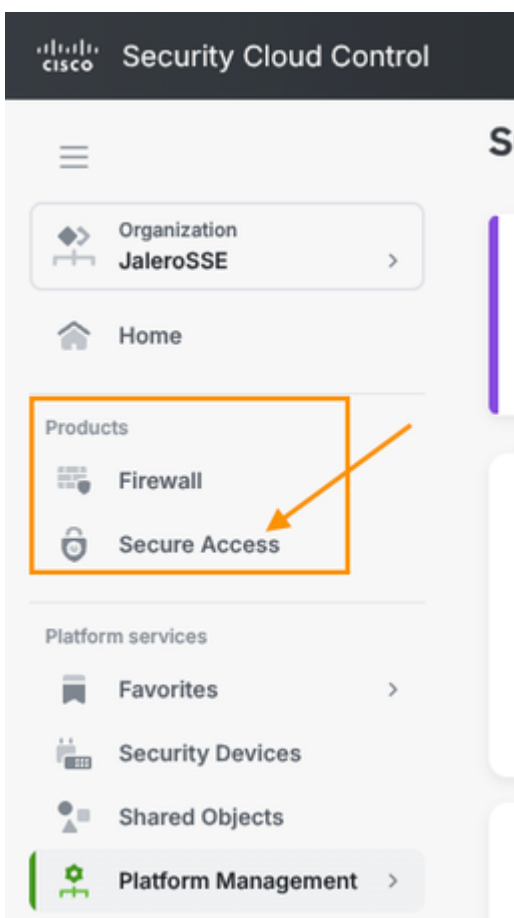
Verificare che l'istanza del prodotto Cisco Secure Access <License Type> sia stata attivata:

End date: Sep 16, 2026

Product	Region	Entitlements	Status
Cisco Secure Access DNS Advantage	Global	50	Activated

## 2. Accesso sicuro nell'elenco dei prodotti

Secure Access deve ora essere elencato anche in Prodotti:



## Migrazione da Umbrella a Secure Access

1. Accedere nuovamente a Umbrella con lo stesso account indicato sopra.
2. Passare alla nuova voce di menu Upgrade Manager:

dashboard.umbrella.com/o/8350166/#/overview?encodedFilters=JTdCJTlyYWN0aW9uJTlyJTNBJTlyYmxvY2t1ZCUyMiUyQyUyMnNlbGVjdGVkRGF0ZVJhbmdlSWR4J...

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. Nella pagina Upgrade Manager, selezionare Start (Avvia) in Enable Cisco Security Cloud Sign on (Abilita accesso a Cisco Security Cloud)

## 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.

Mark as done

[Start](#)

4. Selezionare ENABLE SAML in Configurazione utente dashboard SAML per collegare il SCC come provider SAML per l'accesso al dashboard:

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. Verificare la configurazione SAML con l'opzione 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](#)

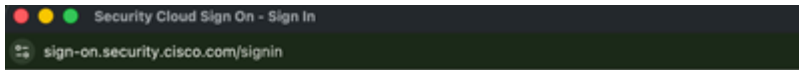
[CANCEL](#)

[PREVIOUS](#)

[NEXT](#)

6. La pagina di login di SCC deve essere visualizzata in una finestra popup diversa (accertarsi che il blocco popup sia disabilitato):

Quando richiesto, eseguire l'accesso con le credenziali SCC.



CONNECTING TO CISCO UMBRELLA

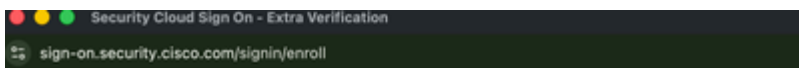
## Security Cloud Sign On

Email

Password


 [Show](#)

[Forgot password](#)



## Multifactor authentication

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

 Duo  Enrolled

[Finish](#)

Una volta verificato l'accesso, è necessario ricevere qui il messaggio di conferma. A questo punto la parte SAML è quasi completa:



# Success!

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

È quindi necessario tornare alla sezione Configurazione utente dashboard SAML:

- La spunta verde indica che le impostazioni SAML sono state configurate correttamente
- Selezionare NEXT (AVANTI) per continuare

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**

Salva e notifica le modifiche agli utenti:

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

## Configurazione SAML completata:

 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. Eseguire l'aggiornamento ad accesso sicuro selezionando **Aggiorna** nella sezione **Avvia aggiornamento**:


✓

Prerequisites 3/3 prerequisites done

2

### 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](#)

- Consenti il proseguimento dell'aggiornamento:

### 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.

- Al termine, è necessario ottenere una pagina simile a quella riportata nell'immagine:

## Start Upgrade



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](#)



## 8. Reindirizza il traffico verso l'accesso sicuro

## 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.



- Conferma del completamento del reindirizzamento. Nell'esempio solo l'identità di rete è stata migrata da Umbrella ad Secure Access:

## Redirect Traffic to Secure Access

Select which Umbrella identities, upgraded to sources in Secure Access, should have their traffic redirected to Secure Access.


### Traffic redirected to Secure Access

To verify redirected traffic, in Secure Access review [Activity Search](#) logs.



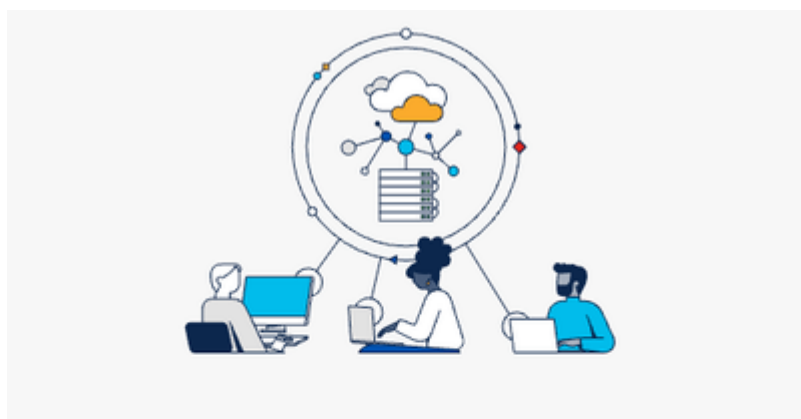
	Networks <span>✓</span>	Network devices	Roaming computers
Secure Access	1	0	
Umbrella	0	0	

## 9. Completare l'aggiornamento e la migrazione a Secure Access

 **Attenzione:** Questo rimuove completamente la vostra organizzazione Umbrella e non è reversibile, quindi assicurarsi che tutti gli elementi sono stati completamente migrati prima di eseguire questo passaggio.



- Quando selezioni Chiudi Umbrella sull'immagine qui, perderai l'accesso alla tua organizzazione ombrello mentre viene eliminata:



## 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

## Verifica migrazione

1. Accedere a [Secure Access](#) con le credenziali di accesso
2. Passare a Protetto > Criteri di accesso per visualizzare le regole migrate, come nell'esempio qui. L'ID organizzazione deve essere lo stesso della sezione Prepara per la migrazione sopra riportata.

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
<input type="checkbox"/>	1	3/3 DNS-only-policy-1 (U...	Allow	Internet	Any AD Group... +1	Global Allow...
<input type="checkbox"/>	2	2/3 DNS-only-policy-1 (U...	Block	Internet	Any AD Group... +1	Alcohol +26
<input type="checkbox"/>	3	1/3 DNS-only-policy-1 D...	Allow	Internet	Any AD Group... +1	Any

## Informazioni correlate

- [Documentazione Umbrella](#)
- [Documentazione sull'accesso sicuro](#)
- [Guida all'aggiornamento della difesa DNS](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).