

Configuración de un marco para la migración al acceso seguro y el control de seguridad en la nube

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Etapas de preparación](#)

[1. Preparación para la migración](#)

[2. Inicie sesión en SCC con sus credenciales de inicio de sesión de Cisco existentes](#)

[3. Enlace Umbrella.org a SCC y suscripción de reclamación](#)

[4. Aplique la licencia a la instancia de Secure Access](#)

[Verificación del enlace de acceso seguro a SCC](#)

[1. Estado de activación del producto en Suscripciones](#)

[2. Acceso seguro en la lista de productos](#)

[Migrar de Umbrella a Secure Access](#)

[Verificar migración](#)

[Información Relacionada](#)

Introducción

En este documento se describe cómo migrar de Umbrella a Secure Access mediante Security Cloud Control (SCC).

Antecedentes

Se recomienda a los clientes de Umbrella que migren de Umbrella a Secure Access y se les exige que utilicen Security Cloud Control para gestionar todos sus productos de seguridad en la nube como parte de estos cambios. Esto le permite disponer de un único panel de acceso para gestionar sus productos de seguridad para la nube, que incluye Cisco Secure Access.

Actualmente no se admite Multi-org (en el momento de la creación de este artículo).

Prerequisites

- Suscripción actual a DNS o SIG
- Acceso de administrador completo a Umbrella

- Acceso al control de seguridad en la nube

Etapas de preparación

1. Preparación para la migración

1. Asegúrese de que dispone de una suscripción DNS o SIG en Umbrella:

- Vaya a Admin > Licensing para verificar
- La actualización a Secure Access debe aparecer en la parte superior de la página:

The screenshot shows the Cisco Umbrella dashboard. The left sidebar contains the navigation menu with 'Admin' selected. The 'Admin' dropdown menu is open, showing 'Accounts', 'User Roles', 'Log Management', 'Authentication', 'Bypass Users', 'Bypass Codes', 'API Keys', and 'Licensing'. The 'Licensing' option is highlighted. The main content area shows the 'Licensing' page. At the top, the URL is 'dashboard.umbrella.com/o/8350166/#/admin/licensing'. The page title is 'Licensing'. Below the title, there is a section titled 'Upgrade to Secure Access' with a 'REQUEST INVITATION' button. Below this, there is a section titled 'Umbrella Package' with a table showing the current package and license start date.

Current Package	License Start Date
Umbrella DNS Security Essentials	September 11, 2025

ii. Anote el ID de organización, en este ejemplo 8350166.

iii. Seleccione la opción Solicitar invitación en la página de licencias.

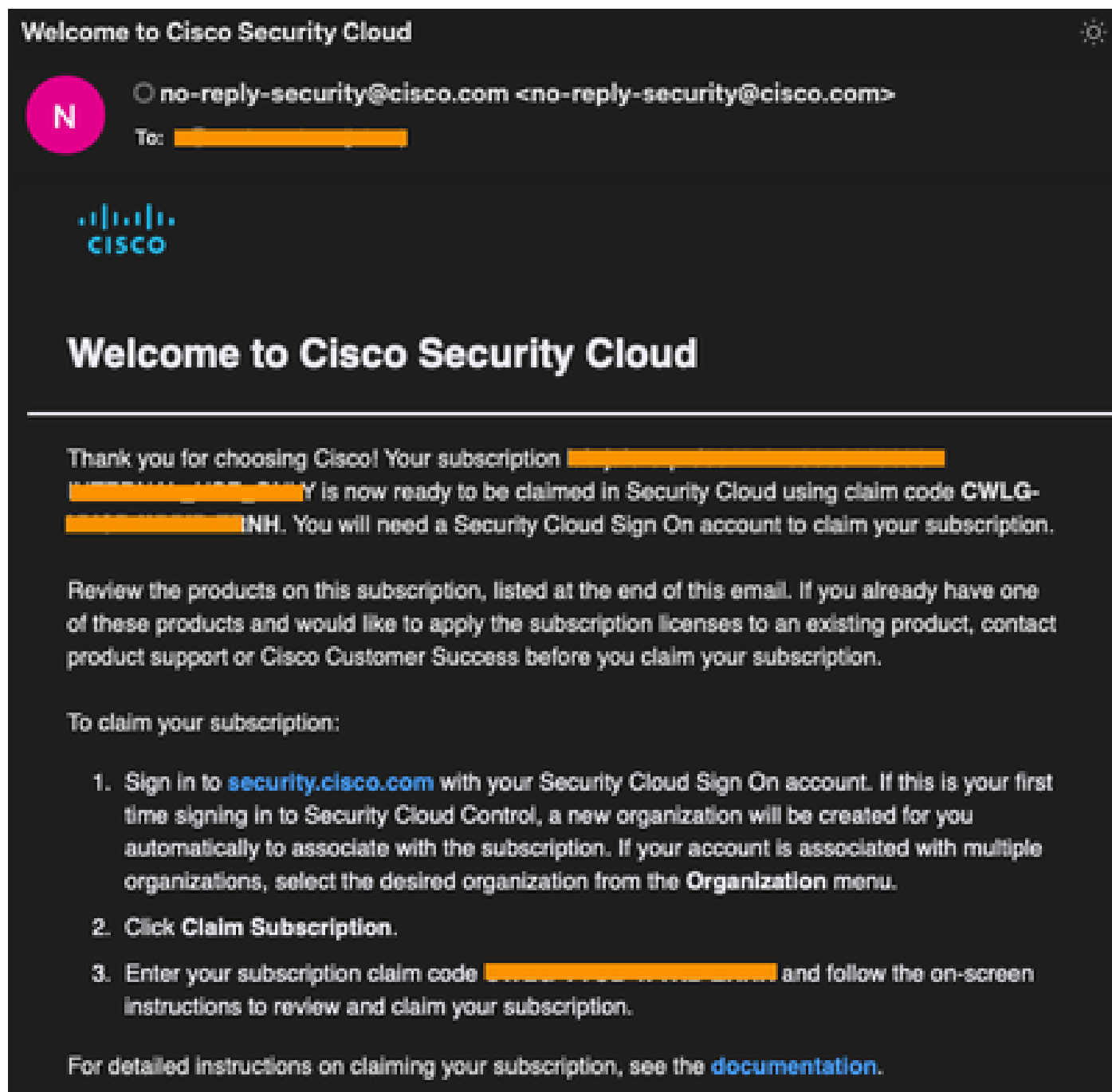


Nota: Si el Upgrade to Secure Access no está presente, asegúrese de que el paquete



Umbrella sea DNS o SIG (actualmente no se soportan multi-org o complementos en el momento de escribir este artículo).

iv. Espere 3-4 días hábiles y debe recibir un correo electrónico con su código de reclamación de suscripción. Consulte el ejemplo de correo electrónico aquí:



2. Inicie sesión en SCC con sus credenciales de inicio de sesión de Cisco existentes

i. Navegue hasta el [portal Security Cloud Control](#) e inicie sesión con sus credenciales de inicio de sesión de Cisco.



Nota: Las mismas credenciales de inicio de sesión de Cisco utilizadas para acceder a su

 panel de Umbrella.

- ii. Seleccione Crear nueva organización (si no tiene una existente).
 - iii. Introduzca el nuevo nombre de la organización en el campo Nombre de la nueva organización.
 - iv. Seleccione la región adecuada en el menú desplegable Region deployment.
-

 Nota: Debe ser la región geográfica en la que se implementaría el arrendatario.

Ejemplo aquí:

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

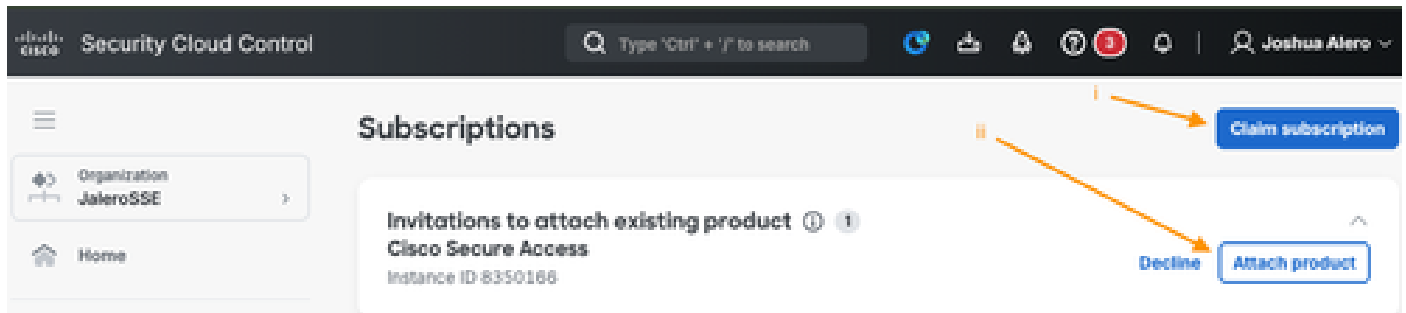
- v. A continuación, seleccione Continuar para completar la creación de la organización.

3. Enlace Umbrella org a SCC y suscripción de reclamación

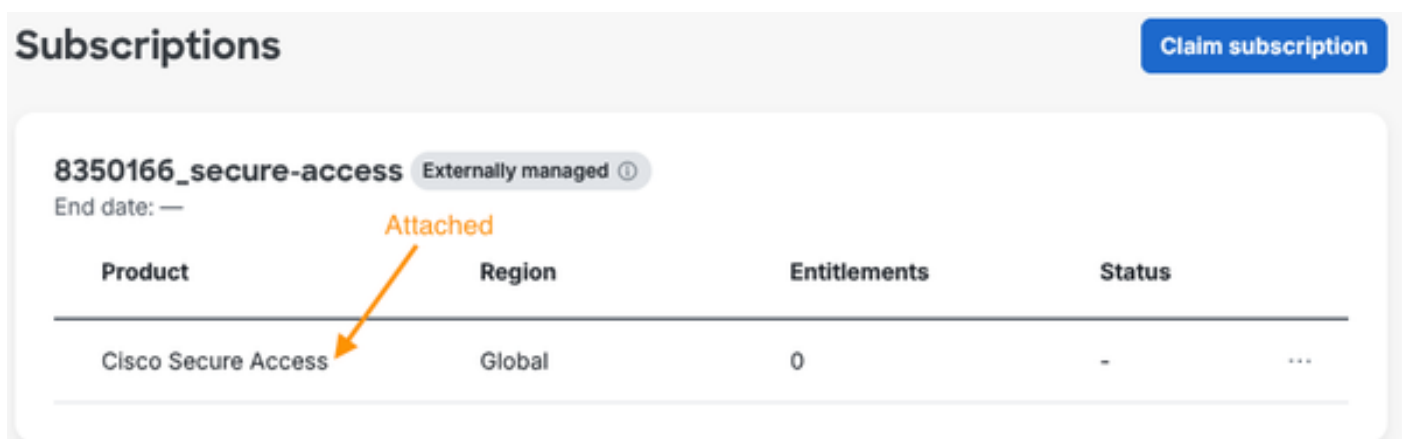
- i. Seleccione el botón Claim subscription para reclamarlo con los códigos proporcionados en el paso 1 anterior.

ii. Su ID de organización de Umbrella debe aparecer en la página Suscripciones, junto con la invitación para adjuntarlo a SCC.

 Nota: El ID de organización de Umbrella debe ser el mismo que el del panel de Umbrella. Esto es importante para la migración y para garantizar que tanto SCC como Umbrella estén vinculados.



- Seleccione Adjuntar producto para adjuntar su organización de Umbrella a SCC.
- Cuando se adjunta, debe ver Cisco Secure Access como producto en la misma página que se muestra en el ejemplo siguiente:



iii. Introduzca el código de reclamación y seleccione Next:

Claim Subscription

The screenshot shows the first step of a three-step process. On the left, a sidebar lists the steps: 1. Enter subscription claim code (active), 2. Review products, and 3. Review subscription. The main content area is titled 'Enter subscription claim code' and includes instructions to enter a claim code and click 'Next'. A text input field contains a masked code 'XXXXXXXXXXXX-ZRNH'. At the bottom, there are navigation buttons: a back arrow, a 'Cancel' button, and a 'Next' button. An orange arrow points to the 'Next' button.

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 *

XXXXXXXXXXXX-ZRNH

< Cancel Next

iv. Seleccione Attach existing instance en el menú desplegable Create new instance o attach existing:

The screenshot shows the second step of the process. The sidebar now has 'Review products' as the active step. The main content area is titled 'Review products' and provides instructions on how to use an existing instance. It features a table with two columns: 'Products' and 'Create new instance or attach existing'. The first row shows 'Cisco Secure Access DNS Advantage' with a dropdown menu set to 'Attach existing instance'. At the bottom, there are navigation buttons: a back arrow, a 'Cancel' button, a 'Back' button, and a 'Next' button. Two orange arrows point to the 'Attach existing instance' dropdown and the 'Next' button.

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. Revise la configuración:

- Asegúrese de que (Instancia existente) forma parte del nombre del producto
- La región debe establecerse en la región existente de la instancia de Secure Access asociada
- Seleccione Reclamar mover para pasar a la página siguiente

Review subscription

Subscription ID
Organization
region
Europe

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

Cancel Back Claim

- Confirme la reclamación de suscripción:

Claim subscription

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

Cancel

Claim

- Después de realizar correctamente la reclamación y el aprovisionamiento, debe obtener una página de suscripciones similar a la que se muestra aquí, en la que se muestren todos los productos activados:

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 ⓘ

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. Aplique la licencia a la instancia de Secure Access

i. Seleccione la opción Acción requerida:

Product and service activation status 1



Cisco Secure Access DNS Advantage

Start date 09/16/2025

[Action required](#)

ii. Seleccione Aplicar licencia:

Cisco Secure Access DNS Advantage

Subscription ID

1. 2010年10月1日起，凡在中华人民共和国境内销售货物或者提供加工、修理修配劳务以及进口货物的单位和个人，均应按照《中华人民共和国增值税暂行条例》及实施细则缴纳增值税。

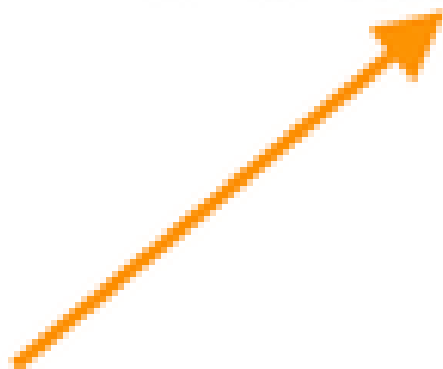
2. 2010年10月1日起，凡在中华人民共和国境内销售货物或者提供加工、修理修配劳务以及进口货物的单位和个人，均应按照《中华人民共和国增值税暂行条例》及实施细则缴纳增值税。

3. 2010年10月1日起，凡在中华人民共和国境内销售货物或者提供加工、修理修配劳务以及进口货物的单位和个人，均应按照《中华人民共和国增值税暂行条例》及实施细则缴纳增值税。

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



- Seleccione NEXT para continuar

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

Guarde los cambios y notifíquelos a los usuarios:

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

Configuración de SAML completada:

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. Actualice a Secure Access seleccionando Upgrade en la sección Iniciar Upgrade:

✓

2

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

- Permitir que la actualización continúe:

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.

- Cuando haya terminado, debe obtener una página como en la imagen aquí:

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. Redirección del tráfico a Secure Access

Redirect Traffic

Not Started

[Help](#)

Redirect your organization's identify 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

- Confirmación de la redirección que se está completando. En el ejemplo, solo se migró la

identidad de red de Umbrella a 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.



50%

	Networks 	Network devices	Roaming computers
Secure Access	1	0	
Umbrella	0	0	

9. Finalice la actualización y migración a Secure Access

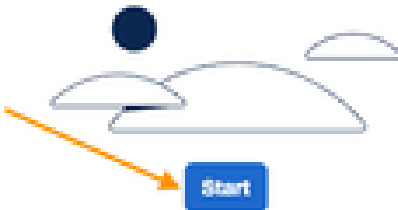
 **Precaución:** Esto elimina por completo la organización de Umbrella y no es reversible, por lo que debe asegurarse de que todos los elementos se han migrado por completo antes de realizar este paso.



Complete Upgrade and Close Umbrella

Not Started

Umbrella has been successfully upgraded and selected traffic is now being steered through Secure Access. The last step in the Upgrade process is to permanently shut down Umbrella and cancel your Umbrella subscription. [Help](#)



- Cuando seleccione Close Umbrella en la imagen, perderá el acceso a su organización paraguas a medida que se borre:



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](#)

Verificar migración

1. Inicie sesión en [Secure Access](#) con sus credenciales de inicio de sesión
2. Navegue hasta Secure > Access Policy para mostrar las reglas migradas, como en el ejemplo aquí. El ID de organización debe ser el mismo que en la sección Prepare for Migration arriba.

← → ↻ 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

Información Relacionada

- [Documentación general](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).