

Configurar o Umbrella para migração para proteger o acesso e o controle de segurança na nuvem

Contents

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

[Etapas de Preparação](#)

- [1. Preparar-se para a migração](#)
- [2. Faça login no SCC usando suas credenciais de login da Cisco existentes](#)
- [3. Vincular a Umbrella.org ao SCC e solicitar assinatura](#)
- [4. Aplicar a licença à Instância de Acesso Seguro](#)

[Verificar o link de acesso seguro ao SCC](#)

- [1. Status de ativação do produto em Assinaturas](#)
- [2. Acesso seguro na lista de produtos](#)

[Migre do Umbrella para o acesso seguro](#)

[Verificar Migração](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como migrar do Umbrella para o Secure Access usando o Security Cloud Control (SCC).

Informações de Apoio

Os clientes da Umbrella são incentivados a migrar do Umbrella para o Secure Access e obrigados a usar o Security Cloud Control para gerenciar todos os seus produtos de segurança de nuvem como parte dessas alterações. Isso permite que você tenha um único painel para gerenciar seus produtos de segurança de nuvem, que inclui o Cisco Secure Access.

Multi-org e MSSP não são suportados no momento da criação deste artigo.

Pré-requisitos

- Assinatura DNS ou SIG atual
- Acesso administrativo completo ao Umbrella

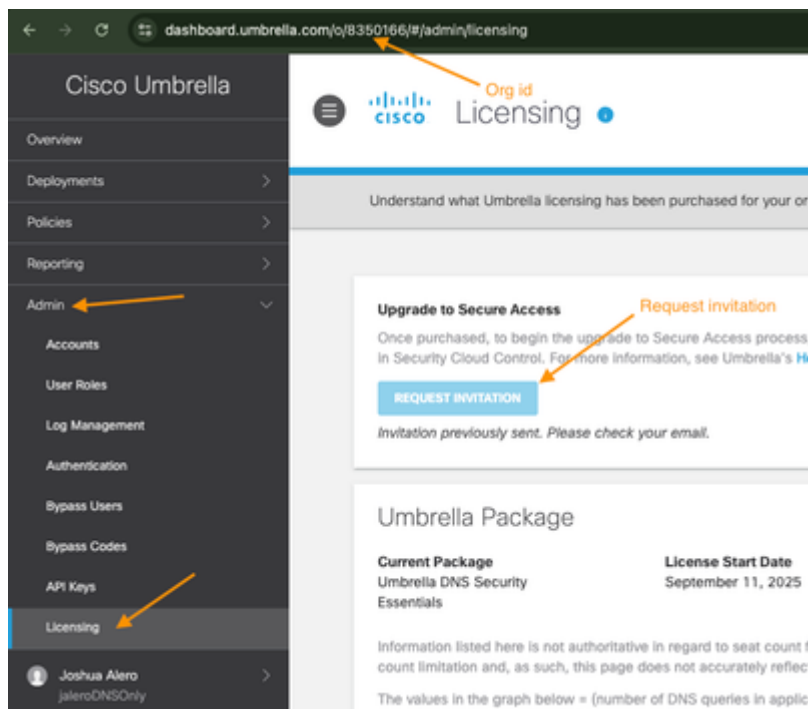
- Acesso ao controle de segurança na nuvem

Etapas de Preparação

1. Preparar-se para a migração

1. Verifique se você tem uma assinatura DNS ou SIG no Umbrella:

- Navegue até Admin > Licenciamento para verificar
- Atualizar para Acesso Seguro deve ser exibido na parte superior da página:



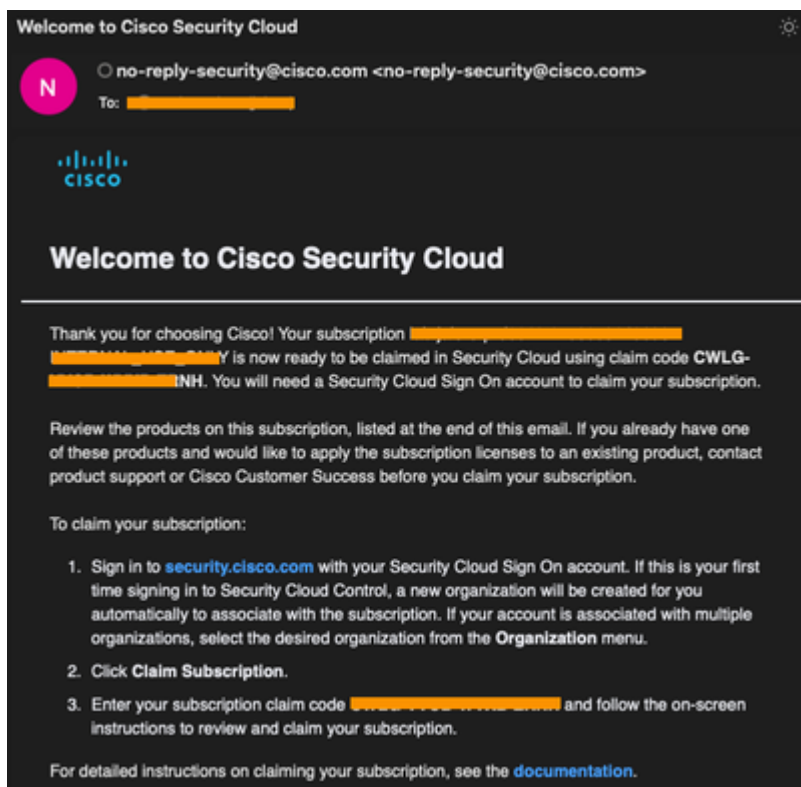
ii) Anote a ID da organização, neste exemplo 8350166.

iii) Selecione a opção Solicitar Convite na página de licenciamento.

⚠ Importante: O botão Request Invitation serve como um convite para participar do espaço do Umbrella para o SCC. Ele não gera um código de declaração. Um código de solicitação será fornecido a você assim que seu pedido de acesso seguro for concluído. Isso faz parte do processo de migração para o Secure Access.

✍ Note: Se a atualização para acesso seguro não estiver presente, verifique se o pacote Umbrella é DNS ou SIG (não há suporte para multiorganizações ou complementos no momento da elaboração deste artigo).

iv) Supondo que você tenha feito seu pedido do Secure Access, aguarde 3 a 4 dias úteis e você deverá receber um e-mail com seu código de solicitação de assinatura (depois de iniciar o convite de solicitação do seu Umbrella Tenant). Veja um exemplo de e-mail aqui:



2. Faça login no SCC usando suas credenciais de login da Cisco existentes

i. Navegue até o [portal Security Cloud Control](#) e faça login com suas credenciais de login da Cisco.

 Note: As mesmas credenciais de login da Cisco usadas para acessar o painel do Umbrella.

ii) Selecione Criar nova organização (se você não tiver uma existente).

iii) Insira o nome da nova organização no campo Nome da nova organização.

iv) Selecione a região apropriada no menu suspenso Implantação da região.

 Observação: esta deve ser a região geográfica na qual seu espaço será implantado.

Exemplo aqui:

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

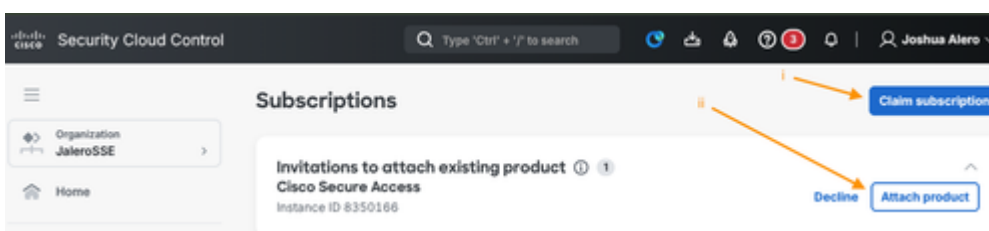
Continue

v. Em seguida, selecione Continue para concluir a criação da organização.

3. Vincular a Umbrella org ao SCC e solicitar assinatura

- i. Selecione o botão Solicitar assinatura para solicitá-lo com os códigos fornecidos na etapa 1 acima.
- ii) Sua ID da empresa Umbrella deve ser vista na página Assinaturas, bem como no convite para anexá-la ao SCC.

 Note: A ID da organização do Umbrella deve ser a mesma do seu Painel Umbrella. Isso é importante para a migração e para garantir que o SCC e o Umbrella estejam vinculados.



- Selecione Attach product (Anexar produto) para anexar sua Umbrella org ao SCC.
- Quando anexado, você deve ver o Cisco Secure Access como um produto na mesma página como mostrado no exemplo aqui:

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) Insira o código da reivindicação e selecione Avançar:

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 *

-ZRNH

[Cancel](#) [Next](#)

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

iv) Selecione Anexar instância existente no menu suspenso Criar nova instância ou anexar existente:

✓ 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. Revise as configurações:

- Certifique-se de que (Instância existente) faça parte do nome do produto
- A região deve ser definida como a região existente da instância do Secure Access anexada
- Selecione Mover reivindicação para ir para a próxima página

Review subscription

Subscription ID
[Redacted]

Organization region
Europe

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

Cancel Back Claim

- Confirme a declaração de assinatura:

Claim subscription

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

Cancel Claim

- Após receber com sucesso a solicitação e o provisionamento, você deve obter uma página de Assinaturas semelhante àquela aqui, mostrando todos os seus produtos ativados:

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. Aplicar a licença à Instância de Acesso Seguro

i. Selecione a opção Ação necessária:

Product and service activation status 1



Cisco Secure Access DNS Advantage

Start date 09/16/2025

[Action required](#)

ii) Selecione Aplicar licença:

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

Verificar o link de acesso seguro ao SCC

Use esta seção para verificar se o locatário do Secure Access foi vinculado ao SCC.

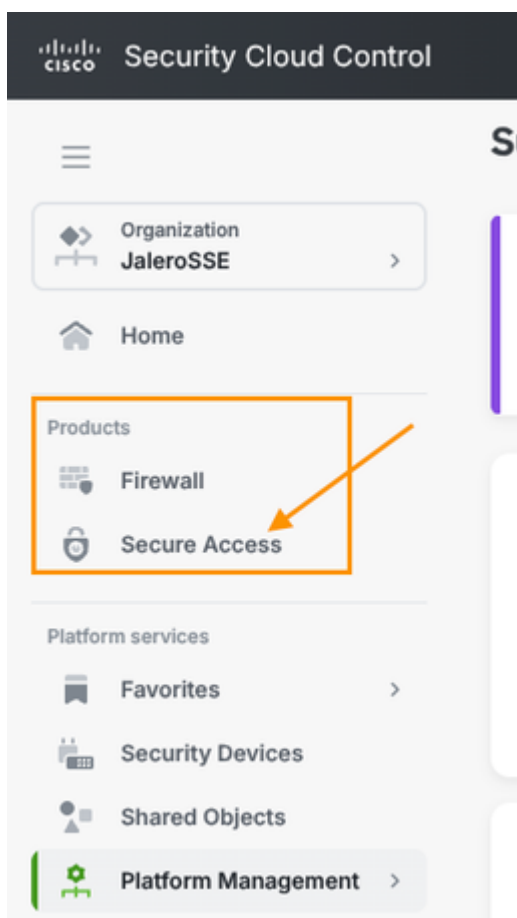
1. Status de ativação do produto em Assinaturas

Verifique se a instância do produto Cisco Secure Access <License Type> foi ativada:

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

2. Acesso seguro na lista de produtos

O acesso seguro agora deve estar listado em Produtos também:



Migre do Umbrella para o acesso seguro

1. Faça login novamente no Umbrella com a mesma conta acima.
2. Navegue até o novo item de menu Upgrade Manager:



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. Selecione ENABLE SAML em SAML Dashboard User Configuration para vincular seu SCC como provedor SAML para login no painel:

 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. Teste a configuração SAML com a opção 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](#)

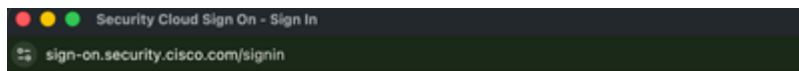
[CANCEL](#)

[PREVIOUS](#)

[NEXT](#)

6. A página de login do SCC deve aparecer em uma janela pop-up diferente (verifique se o bloqueador de pop-up está desativado):

Quando solicitado, faça login com suas credenciais SCC.



CONNECTING TO CISCO UMBRELLA

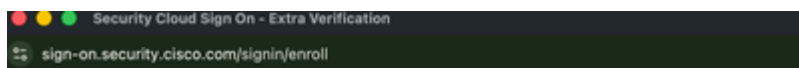
Security Cloud Sign On

Email

Password

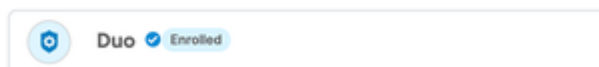
 [Show](#)

[Forgot password](#)



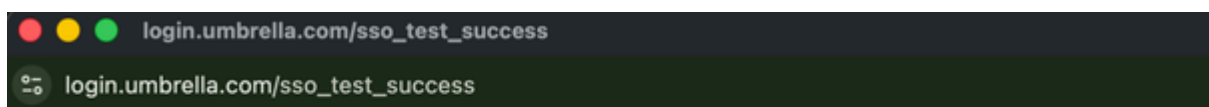
Multifactor authentication

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



[Finish](#)

Quando o login tiver sido verificado, você deverá receber a mensagem aqui, confirmando-a. Nesse ponto, a parte SAML está quase completa:



Success!

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

Em seguida, você deverá retornar à parte Configuração de usuário do painel SAML novamente:

- O tique verde mostra que as configurações de SAML foram configuradas corretamente
- Selecione 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**

Salve e notifique os usuários sobre as alterações:

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**

Configuração SAML concluída:

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. Atualize para o Secure Access selecionando Atualizar na seção Iniciar Atualização:

✓

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 a atualização continue:

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.

- Ao concluir, você deve obter uma página como na imagem aqui:

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. Redirecionar tráfego para Acesso Seguro

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.



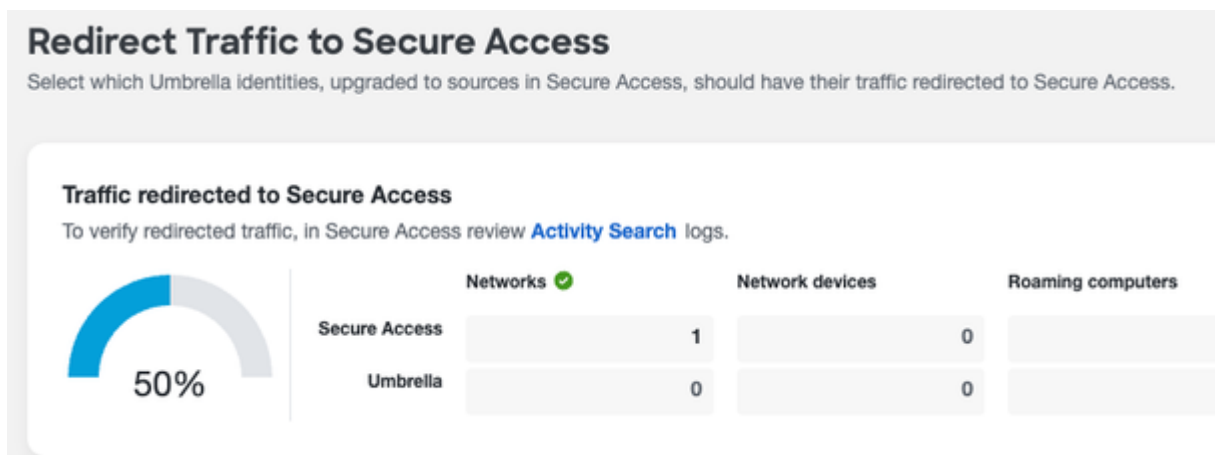
Redirecting traffic to Secure Access

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

Start

- Confirmação de conclusão do redirecionamento. No exemplo, apenas a identidade da rede

foi migrada do Umbrella para o Secure Access:



9. Concluir a atualização e a migração para o Secure Access

 **Caution:** Isso remove completamente sua organização Umbrella e não é reversível, portanto, certifique-se de que todos os itens tenham sido completamente migrados antes de executar esta etapa.



- Ao selecionar Fechar guarda-chuva na imagem aqui, você perderá o acesso à sua organização de guarda-chuva à medida que ela for excluída:



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 Migração

1. Faça login no [Secure Access](#) com suas credenciais de login
2. Navegue até Secure > Access Policy para exibir as regras migradas, como no exemplo aqui.
O ID da organização deve ser o mesmo da seção Prepare for Migration acima.

← → ↻ 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

Informações Relacionadas

- [Documentação do Umbrella](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.