

配置Umbrella以迁移到安全访问和安全云控制

目录

[简介](#)

[背景信息](#)

[先决条件](#)

[准备阶段](#)

[1.为迁移做好准备](#)

[2.使用您现有的思科登录凭证登录SCC](#)

[3.将Umbrella组织链接到SCC并申请订阅](#)

[4.将许可证应用于安全访问实例](#)

[验证到SCC的安全访问链路](#)

[1.订用中的产品激活状态](#)

[2.产品列表中的安全访问](#)

[从Umbrella迁移到安全访问](#)

[验证迁移](#)

[相关信息](#)

简介

本文档介绍如何使用安全云控制(SCC)从Umbrella迁移至安全访问。

背景信息

我们鼓励Umbrella客户从Umbrella迁移至安全访问，并要求使用这些更改中的一部分使用Security Cloud Control管理其所有云安全产品。这样，您就可以通过单一管理平台管理包括思科安全访问在内的云安全产品。

当前不支持多组织和MSSP (创建本文时)。

先决条件

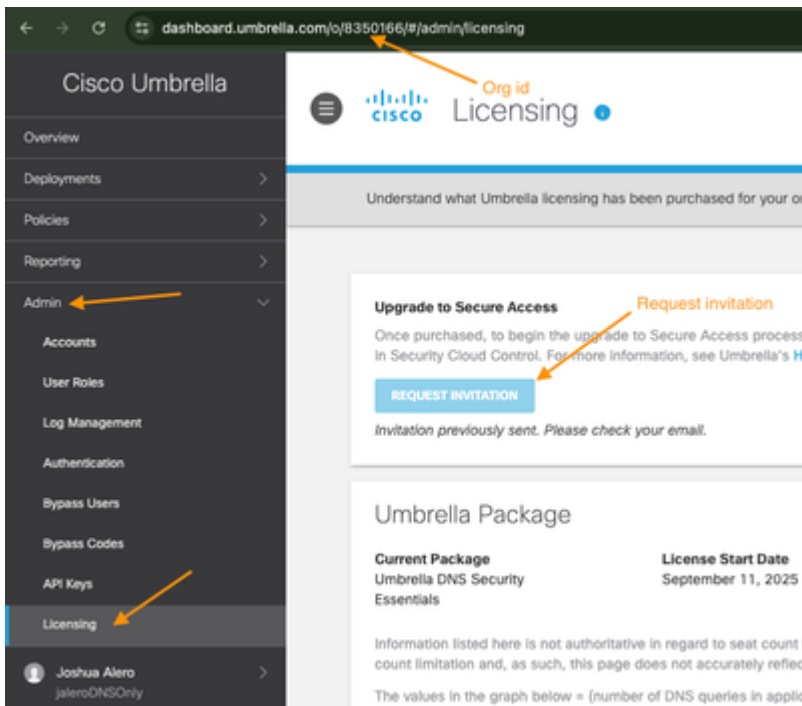
- 当前DNS或SIG订用
- 对Umbrella的完全管理员访问权限
- 访问安全云控制

准备阶段

1.为迁移做好准备

1. 确保您在Umbrella上具有DNS或SIG订用：

- 导航到Admin > Licensing进行验证
- 升级到安全访问必须显示在页面顶部：



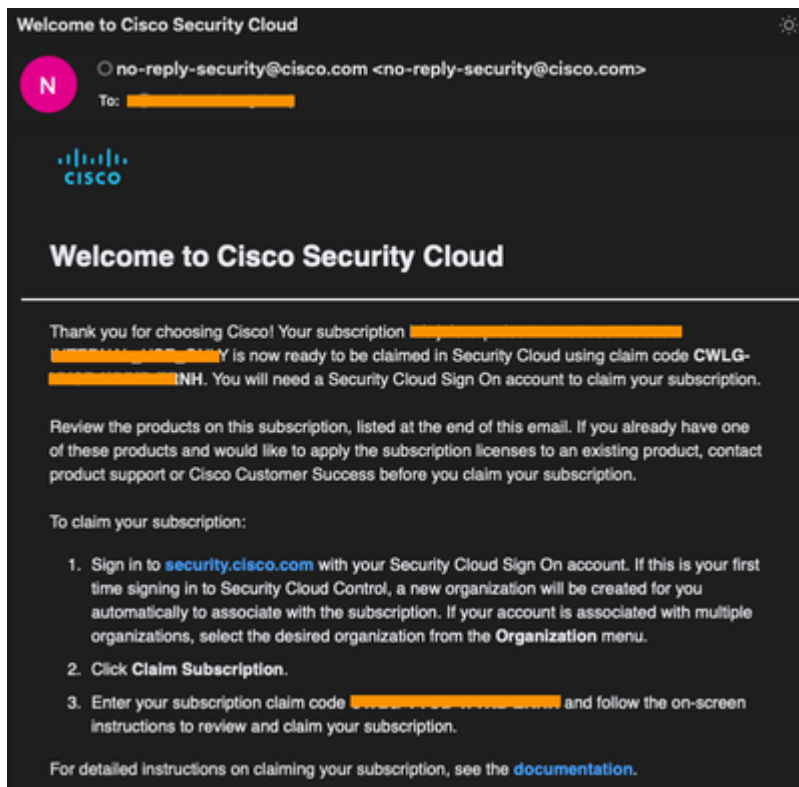
二、记下组织ID，在本例中为8350166。

三。选择许可页面上的Request Invitation选项。

重要信息： Request Invitation按钮用作加入SCC的Umbrella租户的邀请。它不会生成声明代码。完成安全访问的订单后，系统将向您提供申请代码。这是安全访问的迁移过程的一部分。

注意： 如果Upgrade to Secure Access不存在，请确保Umbrella软件包是DNS或SIG（在撰写本文时，当前不支持多组织或插件）。

四。假设您已为安全访问下单，请等待3-4个工作日，您必须收到一封包含订用申请代码的邮件(在从Umbrella租户发起请求邀请之后)。 请在此处查看示例电子邮件：



2.使用您现有的思科登录凭证登录SCC

i.导航到[安全云控制门户](#)，并使用您的思科登录凭证登录。



注意：用于访问您的Umbrella控制面板的相同思科登录凭证。

二、选择创建新组织（如果您没有现有组织）。

三。在“新组织名称”(New Organization name)字段中输入新组织名称。

四。从Region deployment下拉菜单中选择适当的区域。



注意：这必须是您的租户将部署到的地理区域。

示例如下：

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

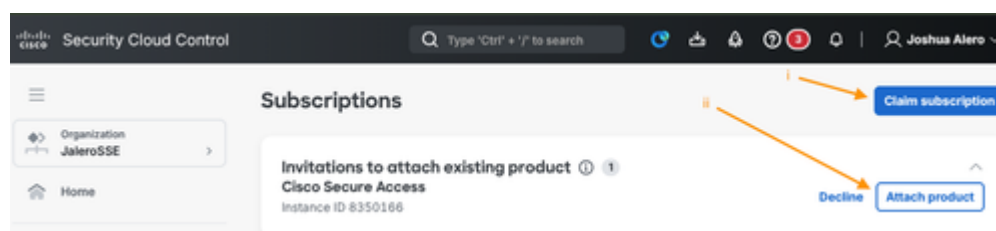
v.然后选择继续完成组织创建。

3.将Umbrella组织链接到SCC并申请订阅

i.选择Claim subscription按钮，以使用上述第1步中提供的代码进行领款申请。

二、必须在订用页面中看到您的Umbrella组织ID以及将其附加到SCC的邀请。

注意：伞状组织ID必须与Umbera控制面板上的相同。这对于迁移和确保SCC和Umbrella链接都非常重要。



— 选择Attach product将您的Umbrella组织附加到SCC。

— 附加时，您必须在同一页面中看到Cisco Secure Access作为产品，如以下示例所示：

Subscriptions				Claim subscription
8350166_secure-access Externally managed ⓘ				
End date: —				
Product	Region	Entitlements	Status	
Cisco Secure Access	Global	0	-	...

三。输入领款申请代码并选择下一步:

The screenshot shows the 'Claim Subscription' interface. On the left, a sidebar lists three 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 begin, enter your claim code below and click Next. For detailed instructions please read our [documentation](#).' Below this is a text input field labeled 'Subscription claim code *' containing the code '9NNH-2-1057-10510-ZRHH'. At the bottom, there are three buttons: a back arrow, a 'Cancel' button, and a 'Next' button. An orange arrow points to the 'Next' button.

四。从Create new instance or attach existing下拉菜单中选择Attach existing instance:

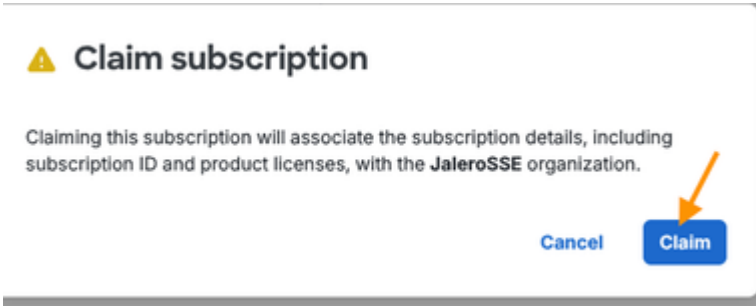
The screenshot shows the 'Review products' step. The sidebar indicates the current step is 2. The main content area is titled 'Review products' and includes instructions: 'To use an existing instance instead of creating a new one, choose **Attach existing instance** from the dropdown menu for the product. Post-claim actions may also be required to apply licenses to some product instances. [Read documentation for more details](#).' Below this is a table with two columns: 'Products' and 'Create new instance or attach existing'. The first row shows 'Cisco Secure Access DNS Advantage' in the 'Products' column and a dropdown menu with 'Attach existing instance' selected in the 'Create new instance or attach existing' column. An orange arrow points to the dropdown menu. At the bottom, there are three buttons: a back arrow, a 'Cancel' button, and 'Back' and 'Next' buttons. An orange arrow points to the 'Next' button.

v.检查设置：

- 确保(现有实例)是产品名称的一部分
- 必须将区域设置为所连接的安全访问实例的现有区域
- 选择Claim move以移至下一页

The screenshot shows the 'Review subscription' step. The sidebar indicates the current step is 3. The main content area is titled 'Review subscription' and includes fields for 'Subscription ID' (three orange bars) and 'Organization region' (Europe). Below this is a table with two columns: 'Products' and 'Deployments'. The first row shows 'Cisco Secure Access DNS Advantage (Existing instance)' in the 'Products' column and a dropdown menu with 'Region per existing deployment' selected in the 'Deployments' column. An orange arrow points to the dropdown menu. At the bottom, there are three buttons: a back arrow, a 'Cancel' button, and 'Back' and 'Claim' buttons. An orange arrow points to the 'Claim' button.

- 确认订阅声明：



- 申请和调配成功后，您必须获得一个类似于此处的Subscriptions页面，其中显示您激活的所有产品：

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	- ...

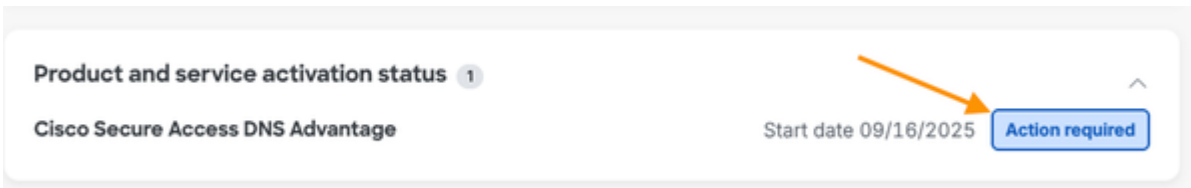
f8643562-d914-4582-a95d-49cf392c757d

End date: —

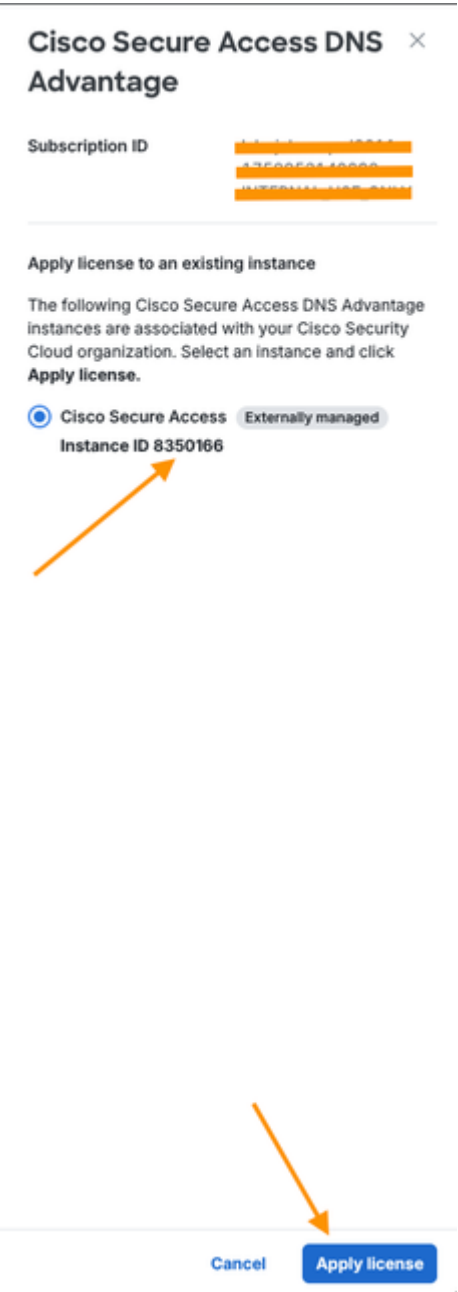
Product	Region	Entitlements	Status
Cisco Security Cloud Control Firewall Management Base	Europe	1	Activated ...

4.将许可证应用于安全访问实例

- i.选择Action required选项：



二、选择App许可证：



验证到SCC的安全访问链路

使用此部分验证您的安全访问租户是否已链接到SCC。

1. 订用中的产品激活状态

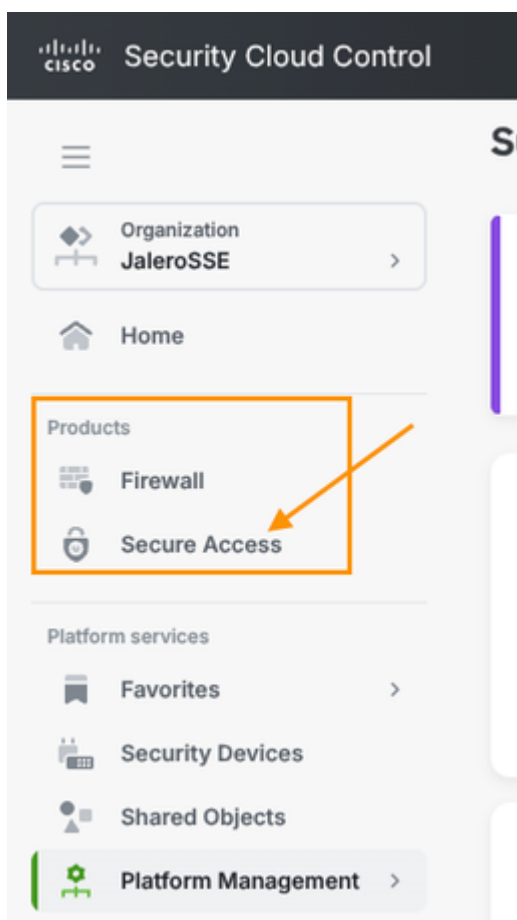
验证Cisco Secure Access <License Type>产品实例已激活：

End date: Sep 16, 2026

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

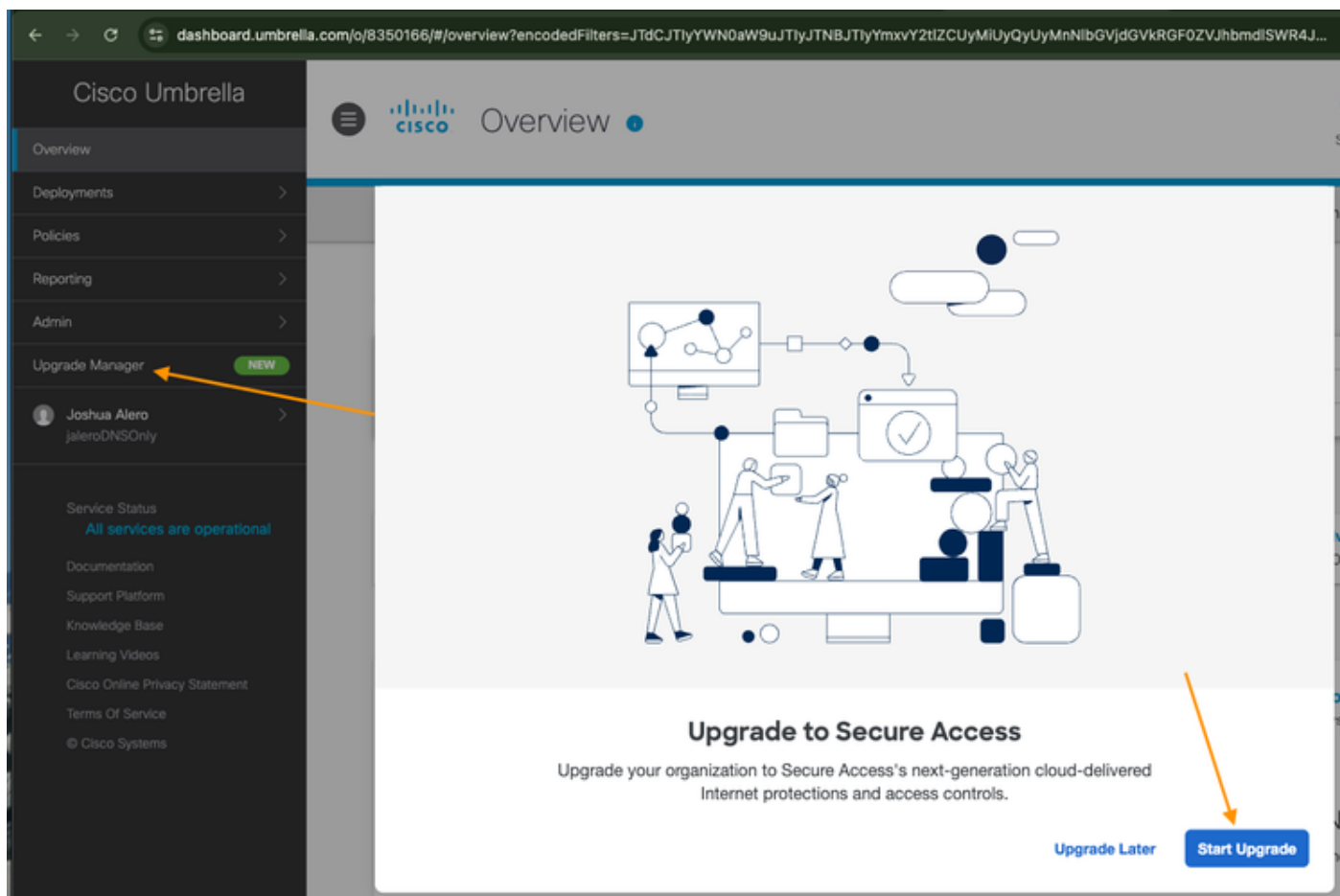
2.产品列表中的安全访问

安全访问现在还必须列在产品下：



从Umbrella迁移到安全访问

1. 使用与上述相同的帐户重新登录Umbrella。
2. 导航到新菜单项Upgrade Manager:



3.在Upgrade Manager页面中，选择Enable Cisco Security Cloud Sign on下的Start

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



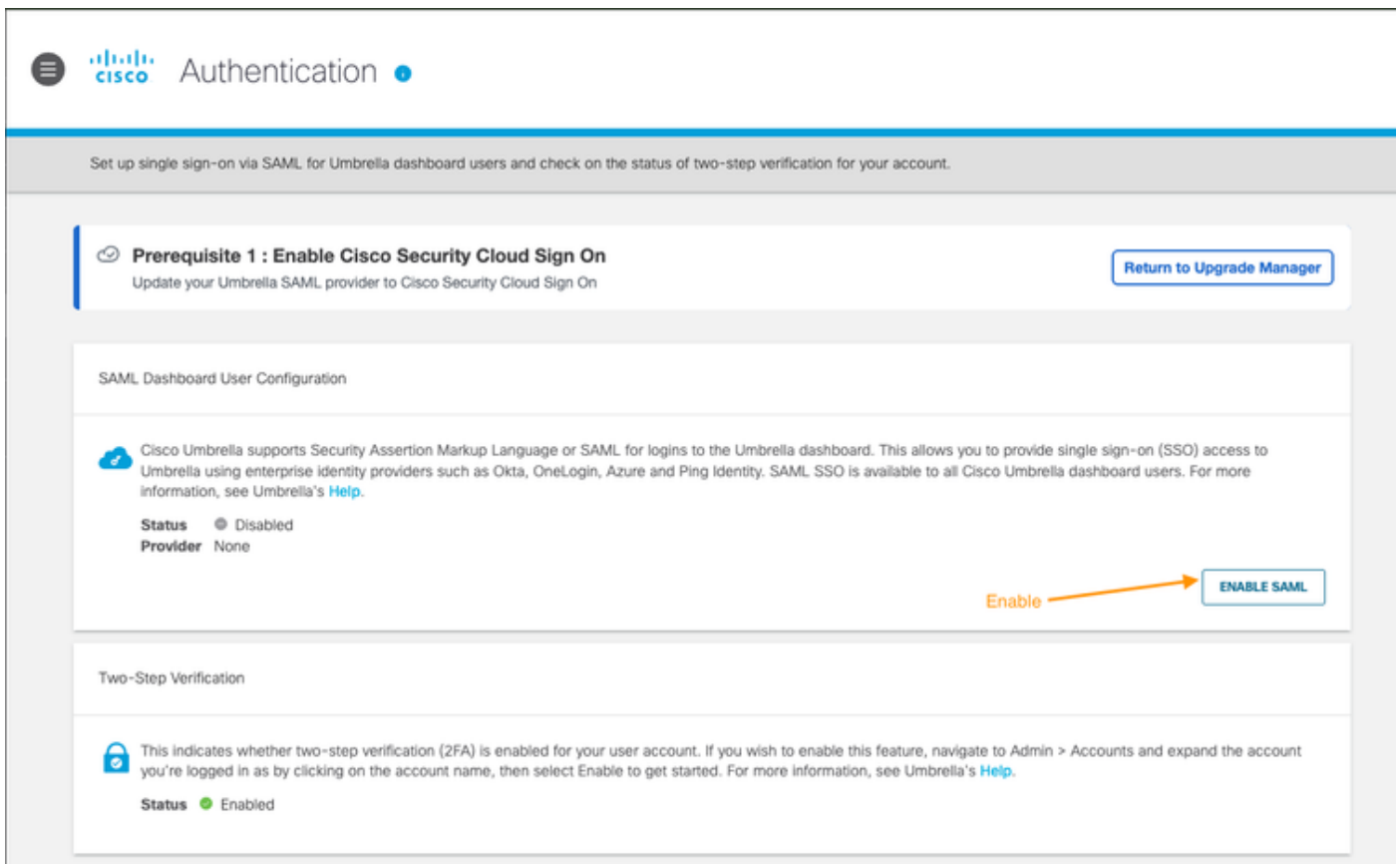
2. Update VAs and AD connectors

Update your virtual appliances and Active Directory Connectors to their latest versions.

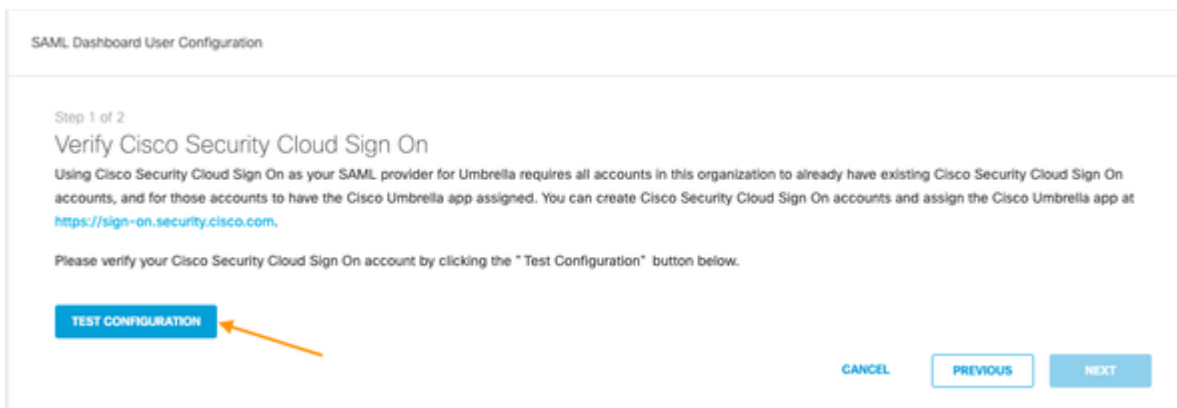
Start

☐ Mark as done

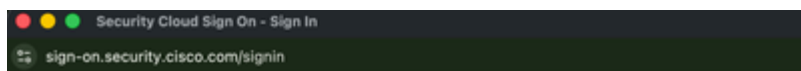
4.在SAML Dashboard User Configuration下选择ENABLE SAML，将SCC作为SAML提供程序链接以进行控制面板登录：



5.使用TEST CONFIGURATION选项测试SAML配置：



6. SCC的登录页必须出现在不同的弹出窗口中（确保已禁用弹出窗口阻止程序）： 出现提示时，使用您的SCC凭证登录。



CONNECTING TO CISCO UMBRELLA

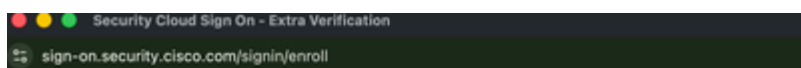
Security Cloud Sign On

Email

Password

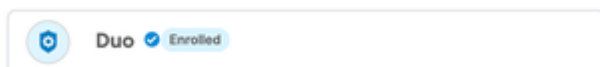
 [Show](#)

[Forgot password](#)



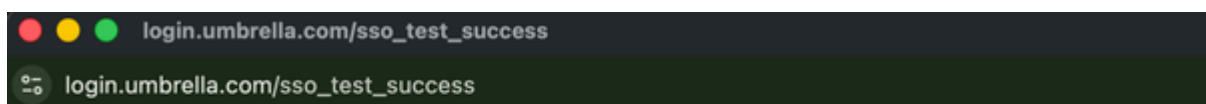
Multifactor authentication

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



[Finish](#)

验证登录后，您必须在此处收到消息，并进行确认。此时SAML部分几乎完成：



Success!

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

然后，必须再次返回到SAML控制面板用户配置部分：

- 绿色勾选表示已正确配置SAML设置
- 选择NEXT继续

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**

保存更改并通知用户：

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配置已完成：

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.选择开始升级部分中的升级，升级到Secure Access:

✓

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

- 允许继续升级：

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.

- 完成后，您必须在此处获得图像上的类似页面：

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.将流量重定向到安全访问

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

- 确认重定向已完成。在本示例中，仅网络身份从Umbrella迁移到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.完成升级和迁移至安全访问

警告：这将完全删除您的Umbrella组织，并且不可撤销，因此在执行此步骤之前，请确保所有项目都已完全迁移。

1

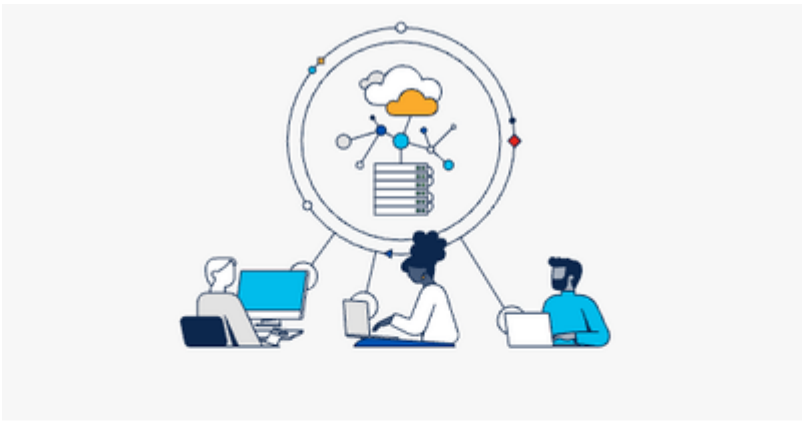
Complete Upgrade and Close Umbrella

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](#)

Start

- 当您在此处的图像上选择Close Umbrella时，您将无法在您的伞状组织被删除时对其进行访问：



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.

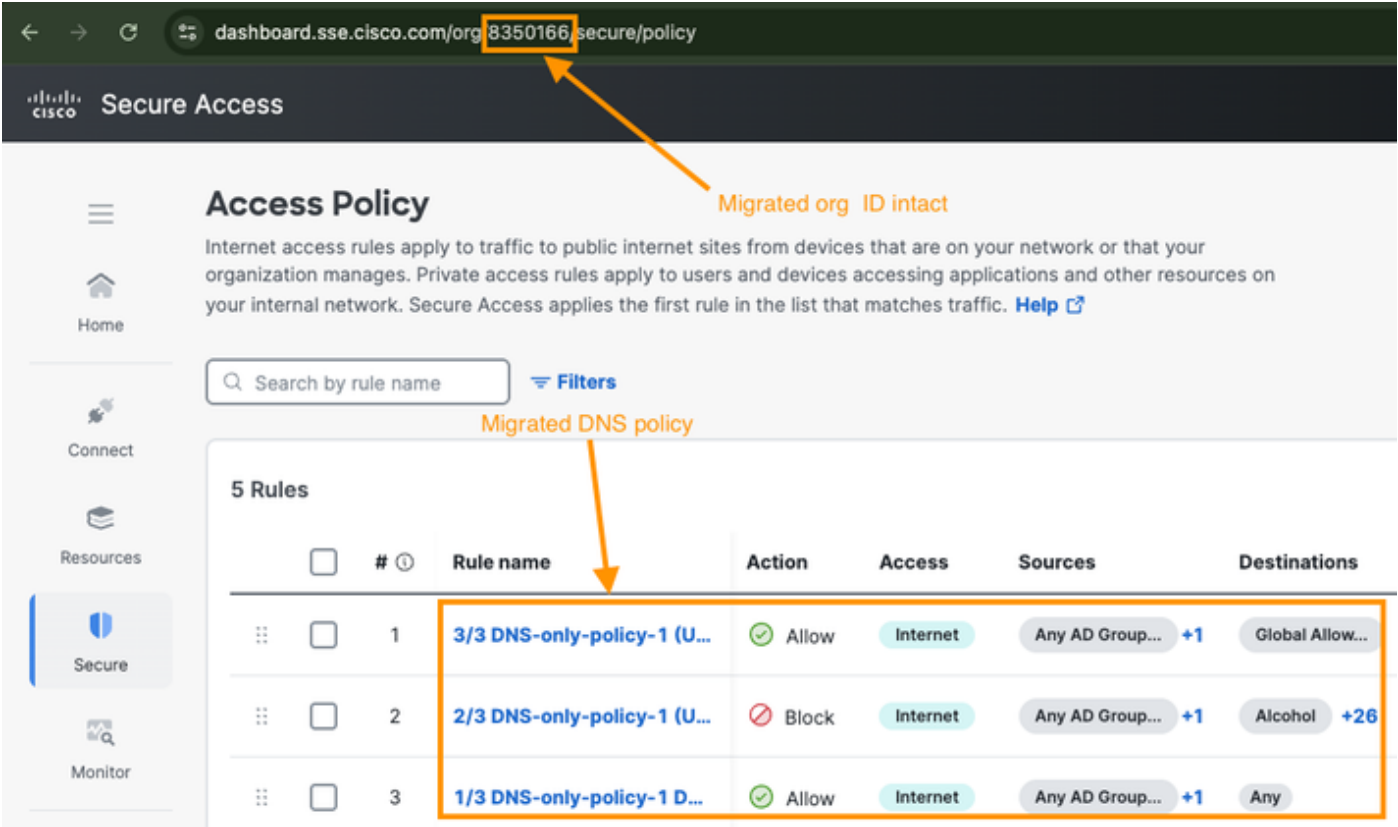
☒ I understand and wish to proceed

Cancel

Close Umbrella

验证迁移

- 1. 使用您的登录凭证登录[Secure Access](#)
- 2. 导航到安全>访问策略以显示迁移的规则，如以下示例所示。组织ID必须与上面准备迁移部分中的组织ID相同。



相关信息

- [Umbrella文档](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。