

配置Umbrella以便遷移至安全訪問和安全雲控制

目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[準備階段](#)

[1.為遷移做準備](#)

[2.使用您現有的思科登入憑證登入到SCC](#)

[3.將Umbrella組織連結到SCC並申請訂閱](#)

[4.將許可證應用於安全訪問例項](#)

[驗證到SCC的安全訪問鏈路](#)

[1.訂閱中的產品啟用狀態](#)

[2.產品清單中的安全訪問](#)

[從Umbrella遷移至安全訪問](#)

[驗證遷移](#)

[相關資訊](#)

簡介

本檔案介紹如何使用安全雲控制(SCC)從Umbrella遷移至安全存取。

背景資訊

Umbrella客戶被鼓勵從Umbrella遷移到Secure Access，並需要使用Security Cloud Control管理其所有雲安全產品，作為這些更改的一部分。這樣，您就可以通過一個單一平台來管理其雲安全產品，包括思科安全訪問。

目前不支援多組織和MSSP (在本文建立時)。

必要條件

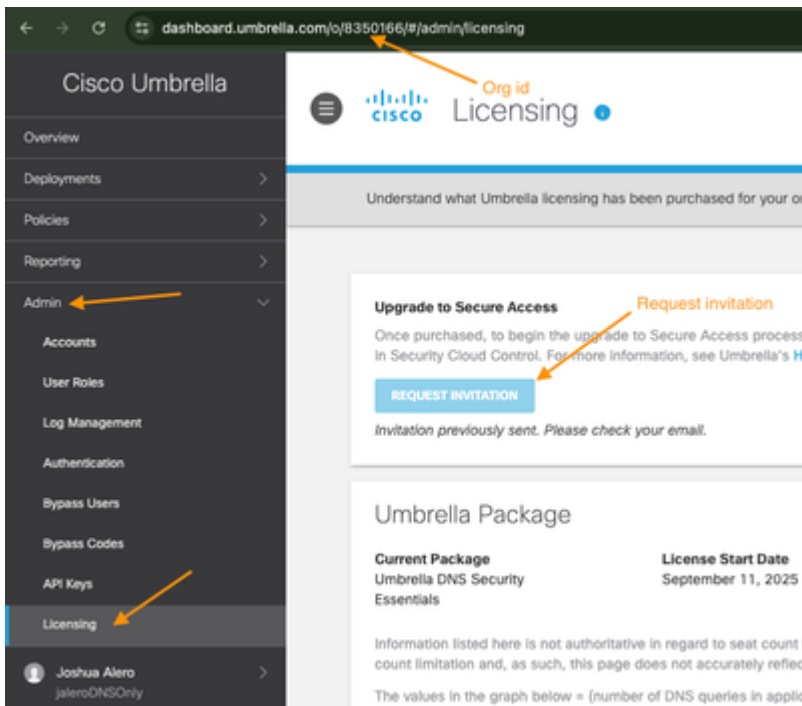
- 當前DNS或SIG訂閱
- 對Umbrella的完全管理員訪問許可權
- 訪問安全雲控制

準備階段

1.為遷移做準備

1. 確保您在Umbrella上具有DNS或SIG訂閱：

- 導航到Admin > Licensing進行驗證
- 升級至Secure Access必須顯示在頁面頂部：



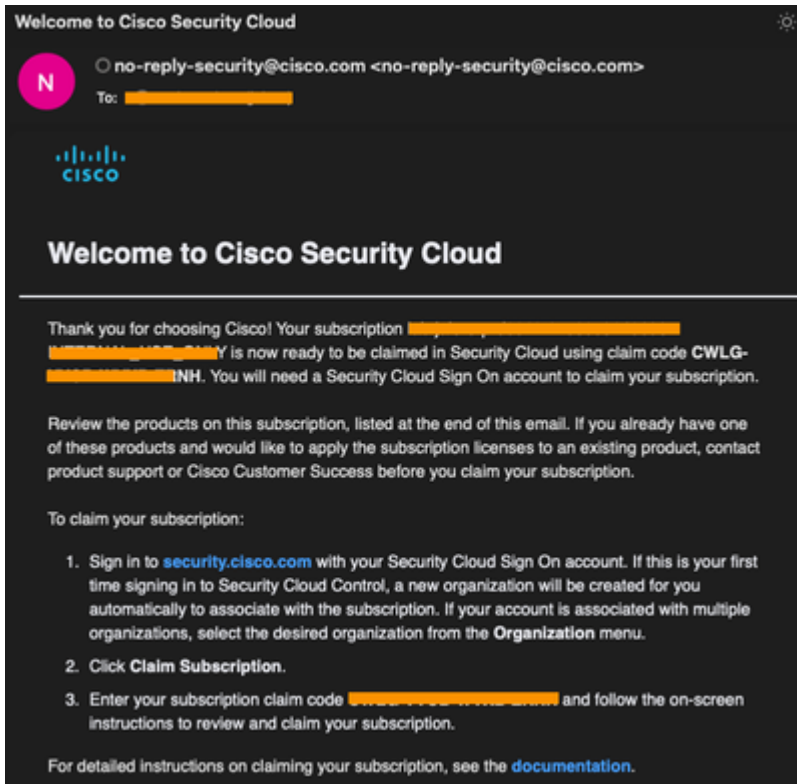
二。記下組織ID，在本例中為8350166。

三。在許可頁面上選擇Request Invitation選項。

重要: Request Invitation按鈕用作加入SCC的Umbrella租戶的邀請。它不會生成宣告代碼。完成安全訪問的訂單後，系統將向您提供索賠代碼。這是安全訪問的遷移過程的一部分。

附註： 如果沒有Upgrade to Secure Access，請確保Umbrella軟體包是DNS或SIG（撰寫本文時當前不支援多組織或外掛）。

四。假設您已訂購Secure Access，請等待3-4個工作日，然後您必須收到一封包含訂閱宣告代碼的電子郵件(在從Umbrella租戶啟動請求邀請後)。請在此處檢視示例電子郵件：



2. 使用您現有的思科登入憑證登入到SCC

i. 導覽至 [Security Cloud Control portal](#)，然後使用您的思科登入憑證登入。



附註：用於訪問您的Umbrella控制面板的相同思科登入憑證。

二。選擇建立新組織（如果您沒有現有組織）。

三。在「新組織名稱」(New Organization name)欄位中輸入新組織名稱。

四。從Region deployment下拉選單中選擇適當的區域。



注意：這必須是您的租戶將部署到的基本區域。

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

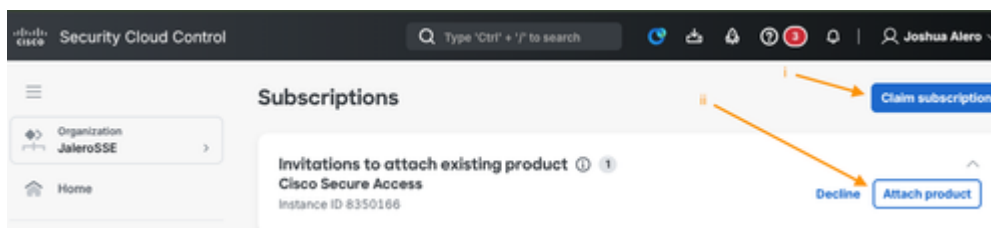
v. 然後選擇繼續以完成組織建立。

3. 將Umbrella組織連結到SCC並申請訂閱

i. 選擇Claim subscription按鈕以使用上面第1步中提供的代碼進行索賠。

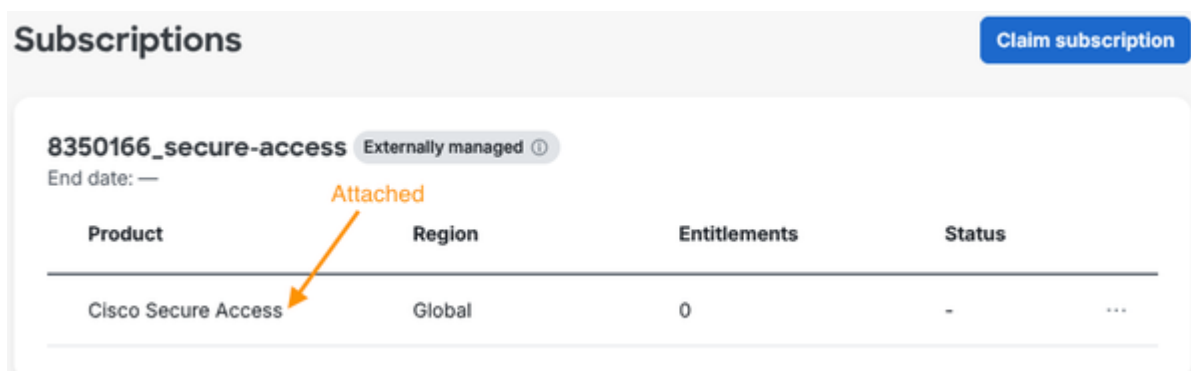
二。必須在訂用頁面中看到您的Umbrella組織ID，以及將其附加到SCC的邀請。

 附註：Umberla控制面板上的Umberla組織ID必須相同。這對遷移和確保SCC和Umbrella連結都很重要。



— 選擇Attach product，將您的Umbrella組織附加到SCC。

— 附加時，您必須在同一頁面中看到Cisco Secure Access產品，如以下示例所示：



三。輸入領款申請代碼並選擇下一步：

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-241057-100010-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。從Create new instance or attach existing下拉選單中選擇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 four buttons: a back arrow, a 'Cancel' button, a 'Back' button, and a 'Next' button. Another orange arrow points to the 'Next' button.

v.檢查設定：

- 確保(Existing instance)是產品名稱的一部分
- 必須將區域設定為所連線的Secure Access例項的現有區域
- 選擇Claim move以移至下一頁

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 'Region per existing deployment 1' in the 'Deployments' column. An orange arrow points to the 'Products' column. Another orange arrow points to the 'Deployments' column. At the bottom, there are four buttons: a back arrow, a 'Cancel' button, a 'Back' button, and a 'Claim' button. An orange arrow points to the 'Claim' button.

- 確認訂閱宣告：

Claim subscription

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

Cancel

Claim 

- 成功申請和調配後，您必須獲得一個類似於此處的Subscriptions頁面，其中顯示您所有已啟用的產品：

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.將許可證應用於安全訪問例項

i.選擇Action required選項：

Product and service activation status ¹

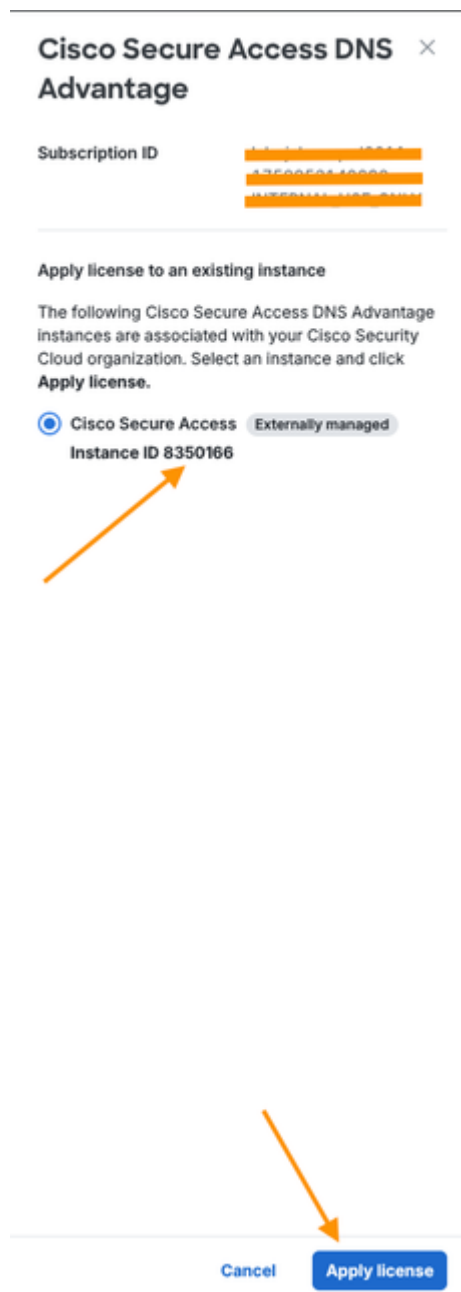


Cisco Secure Access DNS Advantage

Start date 09/16/2025

Action required 

二。選擇App license:



驗證到SCC的安全訪問鏈路

使用此部分驗證您的Secure Access租戶是否已連結到SCC。

1.訂閱中的產品啟用狀態

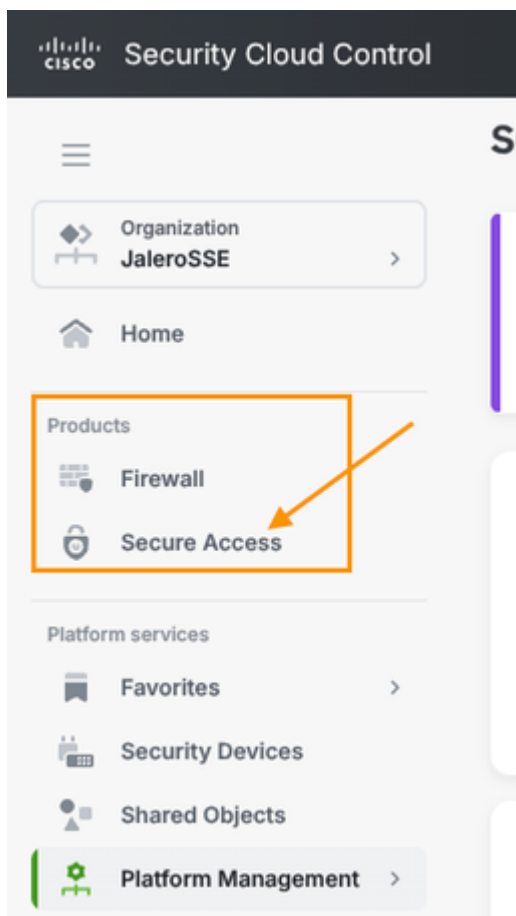
驗證Cisco Secure Access <License Type>產品例項是否已啟用：

End date: Sep 16, 2026

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

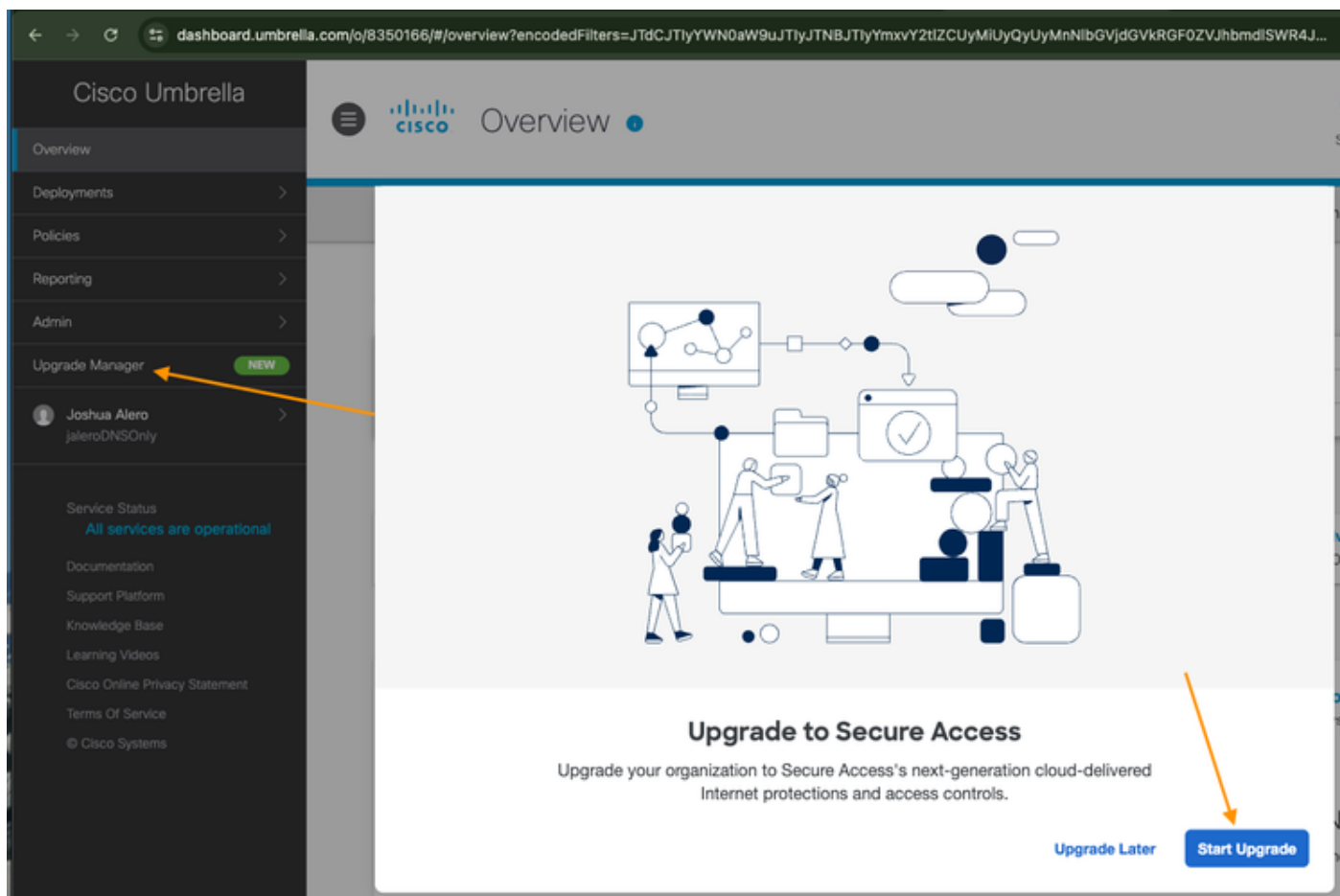
2. 產品清單中的安全訪問

安全訪問現在還必須列在產品下：



從Umbrella遷移至安全訪問

1. 使用與上面相同的帳戶重新登入到Umbrella。
2. 導航到新選單項Upgrade Manager:



3.在Upgrade Manager頁面中，選擇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



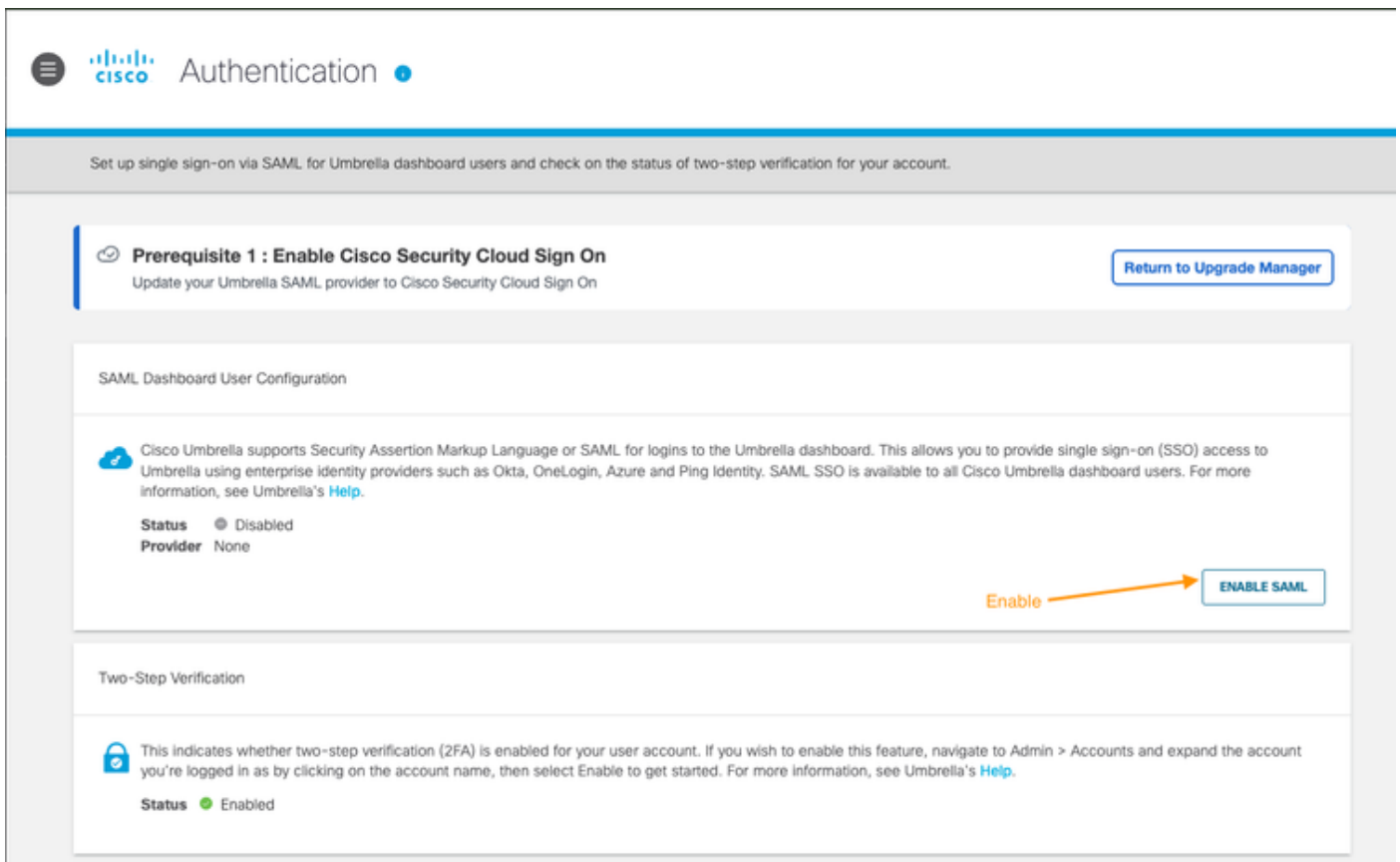
2. Update VAs and AD connectors

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

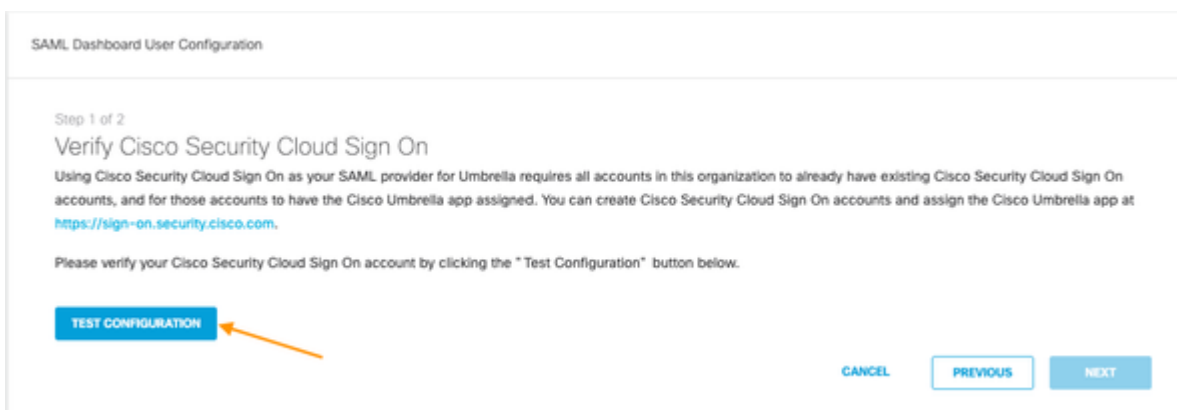
Start

☐ Mark as done

4.在SAML儀表板使用者配置下選擇啟用SAML，以將SCC作為SAML提供程式連結以進行儀表板登入：



5.使用TEST CONFIGURATION選項測試SAML配置：



6. SCC的登入頁面必須出現在另一個彈出視窗中（確保已禁用彈出視窗阻止程式）： 出現提示時，使用您的SCC憑證登入。



CONNECTING TO CISCO UMBRELLA

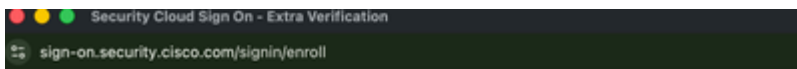
Security Cloud Sign On

Email

Password

 [Show](#)

[Forgot password](#)



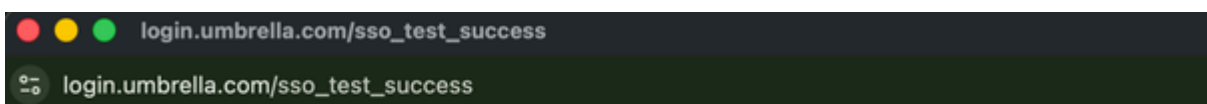
Multifactor authentication

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



[Finish](#)

驗證登入後，您必須在此處獲取消息，並進行確認。此時SAML部分幾乎完成：



Success!

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

然後，必須再次返回到SAML儀表板使用者配置部分：

- 綠色勾選顯示已正確配置SAML設定
- 選擇NEXT繼續

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**

儲存更改並通知使用者：

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.在開始升級部分中選擇升級，以升級到安全訪問：

✓

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

- 允許升級繼續：

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.

- 完成後，您必須在以下影象上獲得一個這樣的頁面：

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.將流量重定向到安全訪問

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

- 確認重新導向已完成。在示例中，只有網路身份從Umbrella遷移到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.



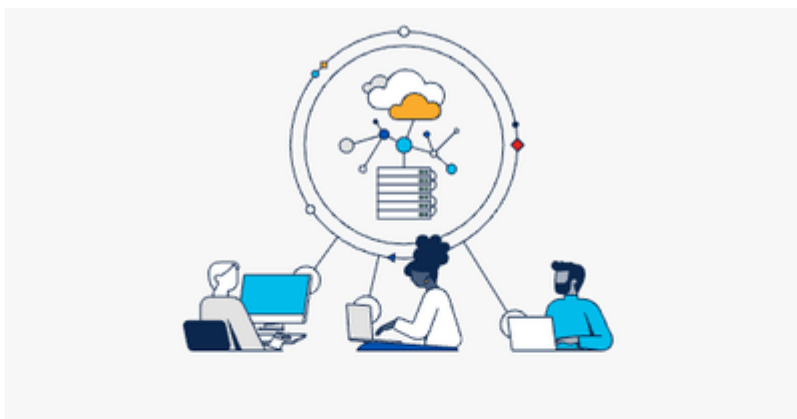
	Networks ✓	Network devices	Roaming computers
Secure Access	1	0	
Umbrella	0	0	

9.完成向Secure Access的升級和遷移

⚠ 注意：這將完全刪除您的Umbrella組織，並且不可撤銷，因此在執行此步驟之前，請確保所有專案都已完全遷移。



- 當您在此處的影象上選擇Close Umbrella時，您將在umbrella組織被刪除時失去對其的訪問許可權：



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](#)

驗證遷移

1. 使用登入憑據登入 [Secure Access](#)
2. 導航到安全>訪問策略以顯示遷移的規則，如下面的示例所示。組織ID必須與上面準備遷移部分的相同。

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](#)

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

相關資訊

- [Umbrella檔案](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。