

보안 액세스 및 보안 클라우드 제어로 마이그레이션하기 위한 Umbrella 구성

목차

[소개](#)

[배경 정보](#)

[사전 요구 사항](#)

[준비 단계](#)

[1. 마이그레이션 준비](#)

[2. 기존 Cisco 로그인 자격 증명을 사용하여 SCC에 로그인합니다.](#)

[3. Umbrella 조직을 SCC에 연결하고 서브스크립션 청구](#)

[4. Secure Access 인스턴스에 라이선스 적용](#)

[SCC에 대한 보안 액세스 링크 확인](#)

[1. 서브스크립션의 제품 활성화 상태](#)

[2. 제품 목록의 보안 액세스](#)

[Umbrella에서 보안 액세스로 마이그레이션](#)

[마이그레이션 확인](#)

[관련 정보](#)

소개

이 문서에서는 SCC(Security Cloud Control)를 사용하여 Umbrella에서 Secure Access로 마이그레이션하는 방법에 대해 설명합니다.

배경 정보

Umbrella 고객은 Umbrella에서 Secure Access로 마이그레이션하는 것이 좋으며, 이러한 변경의 일환으로 Security Cloud Control을 사용하여 모든 클라우드 보안 제품을 관리해야 합니다. 이를 통해 단일 창에서 Cisco Secure Access가 포함된 클라우드 보안 제품을 관리할 수 있습니다.

다중 조직은 현재 지원되지 않습니다(이 문서 작성 시).

사전 요구 사항

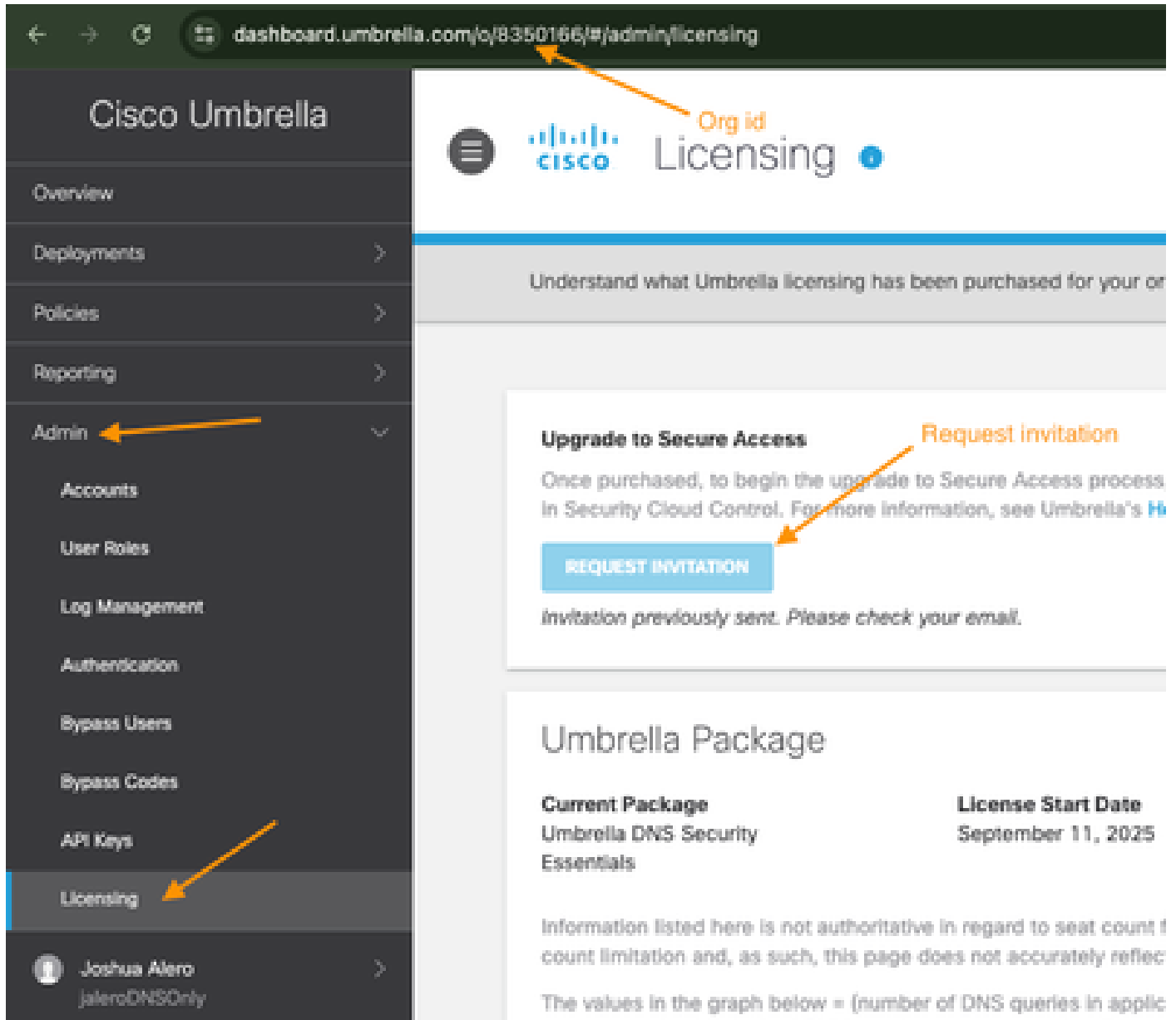
- 현재 DNS 또는 SIG 서브스크립션
- Umbrella에 대한 전체 관리자 액세스
- 보안 클라우드 제어에 액세스

준비 단계

1. 마이그레이션 준비

1. Umbrella에 DNS 또는 SIG 가입이 있는지 확인합니다.

- Admin(관리) > Licensing(라이센싱)으로 이동하여 확인합니다.
- Upgrade to Secure Access(보안 액세스로 업그레이드)가 페이지 상단에 표시되어야 합니다.



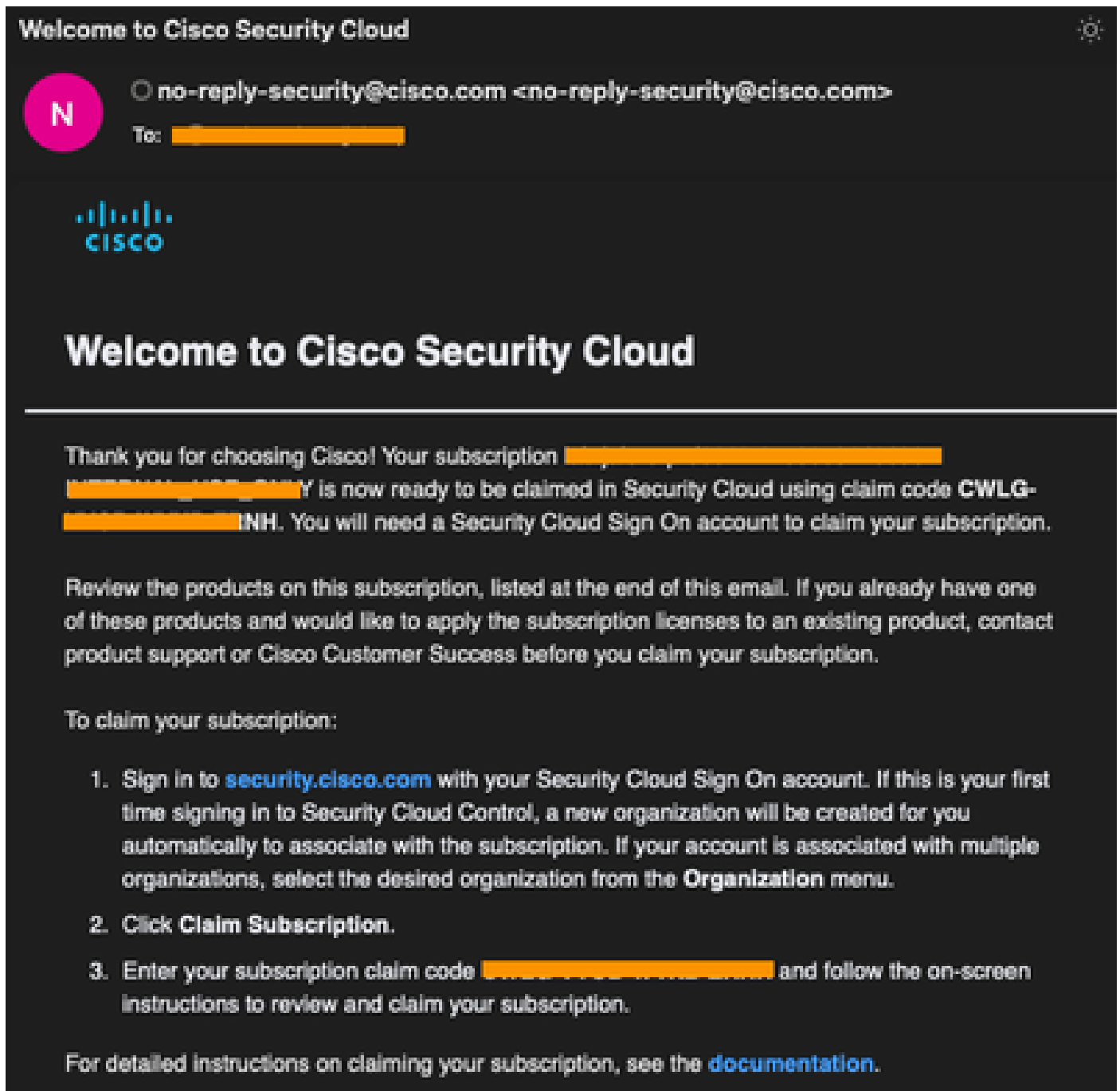
나. 이 예에서 조직 ID를 기록해 8350166.

iii. 라이선스 페이지에서 초대 요청 옵션을 선택합니다.

 참고: Upgrade to Secure Access(보안 액세스로 업그레이드)가 없는 경우 Umbrella 패키지가 DNS 또는 SIG인지 확인합니다(이 문서 작성 시 다중 조직 또는 애드온은 현재 지원되지 않음).

iv. 영업일 기준 3~4일 정도 기다리시면 서브스크립션 클레임 코드가 포함된 이메일을 받으셔야 합

니다. 이메일 예시는 여기를 참조하십시오.



2. 기존 Cisco 로그인 자격 증명을 사용하여 SCC에 로그인합니다.

i. [Security Cloud Control 포털](#)로 [이동하여](#) Cisco 로그인 크리덴셜을 사용하여 로그인합니다.



참고: Umbrella 대시보드에 액세스하는 데 사용하는 것과 동일한 Cisco 로그인 자격 증명

나. 기존의 조직이 없는 경우 Create new organization을 선택합니다.

iii. New Organization name(새 조직 이름) 필드에 새 조직 이름을 입력합니다.

iv. Region deployment 드롭다운 메뉴에서 해당 지역을 선택합니다.

 참고: 테넌트를 배포할 지역 그룹이어야 합니다.

예:

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

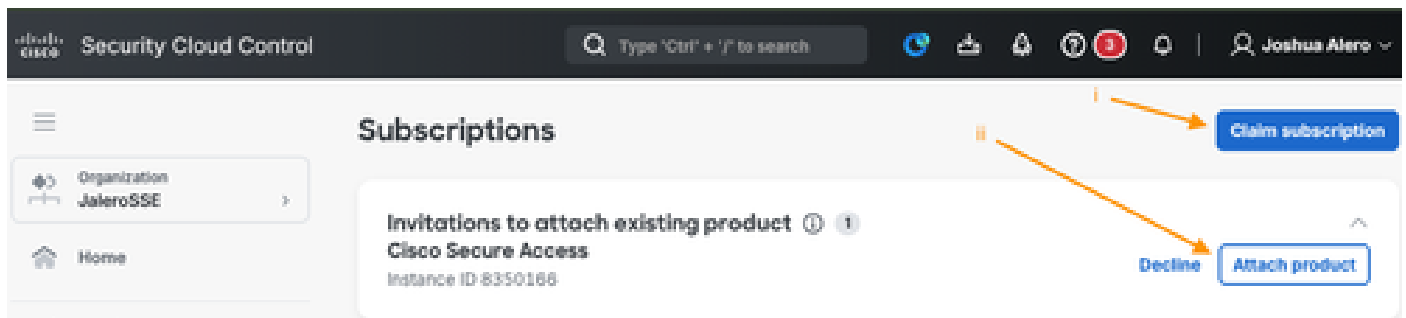
v. 그런 다음 계속을 선택하여 조직 생성을 완료합니다.

3. Umbrella 조직을 SCC에 연결하고 서브스크립션 청구

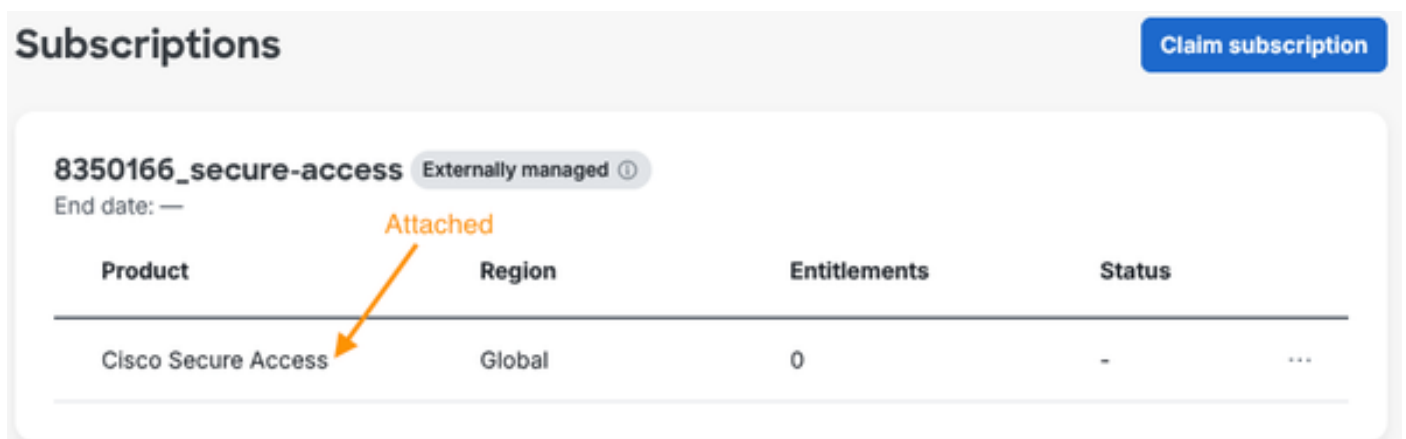
i. Claim subscription(서브스크립션 클레임) 버튼을 선택하여 위의 1단계에서 제공된 코드로 클레임합니다.

나. Umbrella 조직 ID는 Subscriptions(서브스크립션) 페이지와 함께 SCC에 어태치할 수 있는 초대 메시지도 표시되어야 합니다.

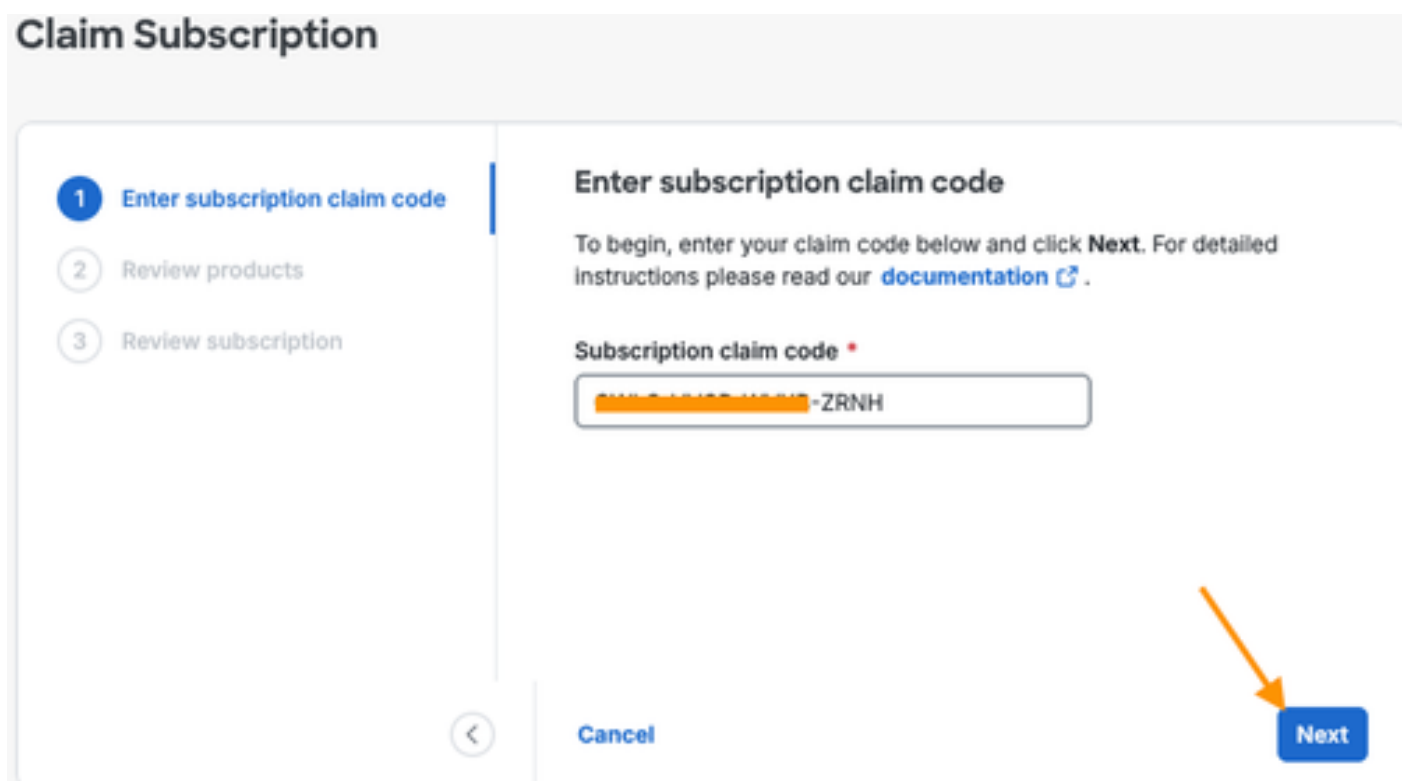
 참고: Umbrella 조직 ID는 Umbrella 대시보드와 동일해야 합니다. 이는 마이그레이션에 중요하며 SCC와 Umbrella가 모두 연결되었는지 확인하는 데 중요합니다.



- Attach product를 선택하여 Umbrella 조직을 SCC에 연결합니다.
- 연결할 경우 다음 예제와 같은 페이지에서 Cisco Secure Access가 제품으로 표시되어야 합니다.



- iii. 청구 코드를 입력하고 다음을 선택합니다.



- iv. Create new instance(새 인스턴스 생성)에서 Attach existing instance(기존 인스턴스 첨부)를 선택하거나 드롭다운 메뉴에서

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. 설정을 검토합니다.

- (기존 인스턴스)가 제품 이름의 일부인지 확인합니다
- 해당 영역은 연결된 Secure Access 인스턴스의 기존 영역으로 설정되어야 합니다
- 다음 페이지로 이동하려면 청구 이동을 선택합니다.

Review subscription

Subscription ID: [Redacted]
 Organization: region
 Europe

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

Cancel Back Claim

- 구독 클레임을 확인합니다.

Claim subscription

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

Cancel

Claim

- 클레임 및 프로비저닝을 성공적으로 완료한 후에는 활성화된 모든 제품을 표시하는 여기와 유사한 서브스크립션 페이지를 가져와야 합니다.

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	- ...

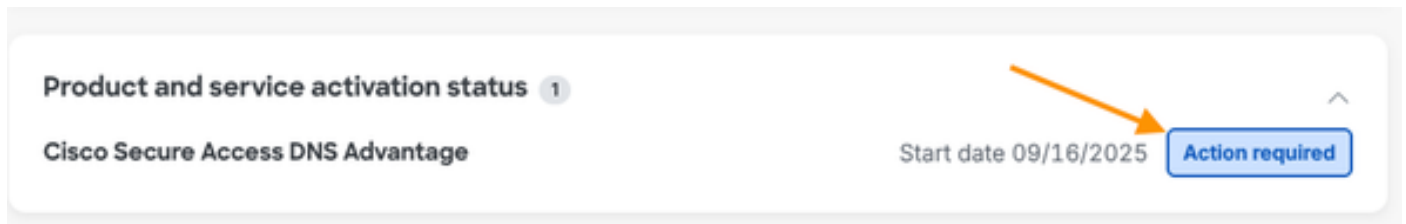
f8643562-d914-4582-a95d-49cf392c757d

End date: —

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

4. Secure Access 인스턴스에 라이선스 적용

i. 작업 필요 옵션을 선택합니다.



나. Apply license 선택:

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



의 로그인 페이지는 다른 팝업 창에 표시되어야 합니다(팝업 차단 기능이 비활성화되어 있는지 확인).

프롬프트가 표시되면 SCC 자격 증명으로 로그인합니다.



CONNECTING TO CISCO UMBRELLA

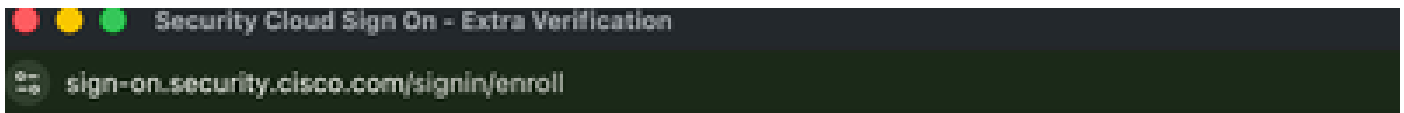
Security Cloud Sign On

Email

Password

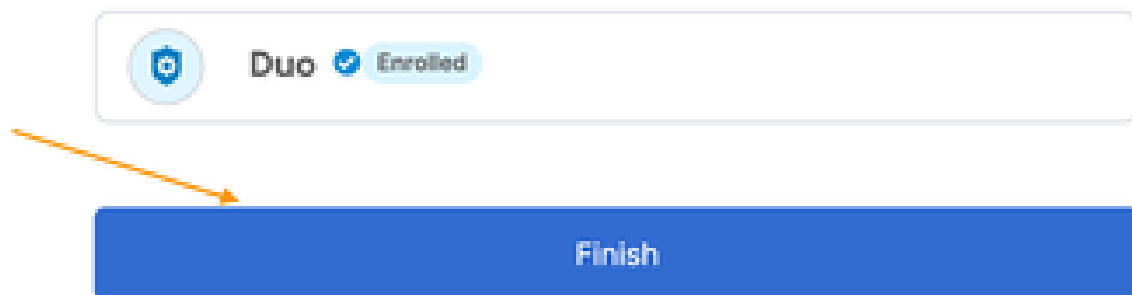
 [Show](#)

[Forgot password](#)

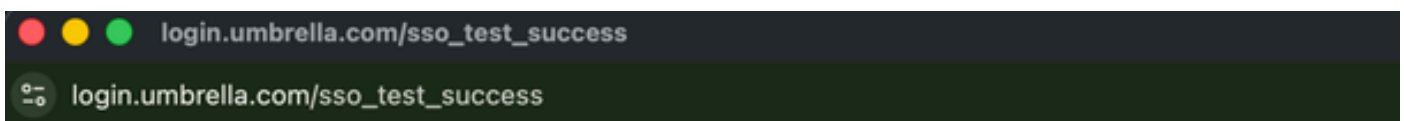


Multifactor authentication

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



로그인이 확인되면 여기서 확인 메시지를 받아야 합니다. SAML 부품이 거의 완성되는 지점입니다.



Success!

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

그런 다음 SAML Dashboard User Configuration(SAML 대시보드 사용자 컨피그레이션) 부분으로 다시 돌아가야 합니다.

- 녹색 선택 표시는 SAML 설정이 올바르게 구성되었음을 나타냅니다.

- 계속하려면 다음을 선택하십시오.

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

변경 사항을 저장하고 사용자에게 알립니다.

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 컨피그레이션 완료:

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. 업그레이드 시작 섹션에서 업그레이드를 선택하여 보안 액세스로 업그레이드 :

✓

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

- 업그레이드를 계속할 수 있습니다.

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.

- 완료되면 다음 그림과 같은 페이지를 가져와야 합니다.

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. 트래픽을 보안 액세스로 리디렉션

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

- 리디렉션 완료 확인 이 예에서는 네트워크 ID만 Umbrella에서 Secure Access로 마이그레이

선되었습니다.

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. Secure Access로의 업그레이드 및 마이그레이션 완료

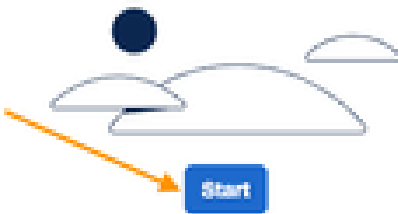
 주의: 이렇게 하면 Umbrella 조직이 완전히 제거되고 되돌릴 수 없으므로 이 단계를 수행하기 전에 모든 항목이 완전히 마이그레이션되었는지 확인하십시오.

4

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](#)



The diagram shows a stylized cloud with a dark blue circle above it. An orange arrow points from the cloud area down to a blue button labeled 'Start'.

- 여기 이미지에서 Close Umbrella를 선택하면 삭제되는 Umbrella 조직에 대한 액세스 권한이 손실됩니다.



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](#)

마이그레이션 확인

1. 로그인 자격 [증명](#)을 사용하여 [Secure Access](#)에 로그인합니다.
2. 여기 예와 같이 보안 > 액세스 정책으로 이동하여 마이그레이션된 규칙을 표시합니다. 조직 ID는 위의 마이그레이션 준비 섹션과 동일해야 합니다.

← → ↺ dashboard.sse.cisco.com/org8350166/secure/policy

Secure Access

☰

Home

🔗

Connect

📁

Resources

🛡️

Secure

🔍

Monitor

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

Migrated org ID intact

Migrated DNS policy

관련 정보

- [Umbrella 설명서](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.