# Cisco Umbrella DNS  Cisco Secure Access  - DNS

**Cisco Secure Access**
Updated October 7, 2026

# 제 1 장

:


- □□□□ □□□ □□
- Cisco Secure Access - DNS □□ □□
- □□□□□ □□ □□
- □□□□□ □□□□□
- Cisco Security Cloud Control □□□ □□□□□.
- Umbrella□□ □□□□□ □□□ □□□
- □□ □ □□ □□


Umbrella를 Secure Access - DNS 방어로 업그레이드하기 전에 업그레이드 가이드 전체를 읽어보십시오.

업그레이드 시간은 이전하는 데 필요한 정책 및 데이터 수에 따라 달라집니다. Umbrella는 이 프로세스 중에도 계속 작동하며 조직은 항상 보호됩니다.

전체 업그레이드 프로세스를 단계별로 보여주는 Umbrella에서 Secure Access DNS로 업그레이드 동영상을 시청할 수도 있습니다.

중요사항

보안 액세스로의 업그레이드를 시작하려면 전체 관리자 액세스 권한이 있어야 합니다.

- Cisco Secure Access - DNS 방어 시작
- 간편한 시작
- Cisco Security Cloud Control 계정을 생성합니다.
- Umbrella에서 업그레이드 관리자 생성
- 지침 및 제한 사항

이 오퍼는 Umbrella DNS Advantage, Umbrella DNS Essentials, MSP 및 다중 조직을 보유한 고객에게 제공됩니다.

이 오퍼는 Umbrella DNS Advantage, Umbrella DNS Essentials, MSP 및 다중 조직을 보유한 고객에게 제공됩니다.

> 주
>
> 이 업그레이드에서는 Secure Access 평가판 라이선스가 지원되지 않습니다. 업그레이드하려면 활성 상태의 유료 보안 액세스 구독이 필요합니다. 평가판 라이선스를 사용하면 만료되어 기존 Umbrella 대시보드 액세스가 중단될 수 있습니다.

현재 Umbrella 제품을 식별하려면 관리되는 조직 Umbrella 대시보드로 이동하여 **Admin(관리자) > Licensing(라이선싱)**을 선택합니다.

## Cisco Secure Access - DNS

Cisco Secure Access - DNS 방어로 향상된 보안을 경험하십시오.

단순한 DNS 레이어 보호 그 이상을 제공하도록 설계된 보안 액세스로 보안의 새로운 시대를 열어보십시오. 이 고급 솔루션은 최신 DNS Advantage 또는 Essentials 기능을 통합하여 사이버 위협에 한발 앞서 앞서 나가는 포괄적인 보호를 제공합니다. 사무실, 집, 또는 이동 중 어디서든 탁월한 가시성과 제어 기능을 갖추고 있다는 사실을 믿고 안심하고 연결하십시오.

> 주
>
> Umbrella에서 Secure Access - DNS 방어로 업그레이드를 시도하기 전에 업그레이드 가이드 전체를 읽어야 합니다.

Secure Access - DNS 방어를 선택하는 이유는 무엇입니까?

- 원활한 전환: 운영 중단 없이 향상된 보안 조치로 원활하게 업그레이드합니다.
- 언제 어디서나 연결 : 장소에 구애받지 않고 애플리케이션과 데이터에 안전하게 액세스할 수 있으므로 원격 작업이 수월합니다.
- Zero Trust 아키텍처: VPN 없이 회사 네트워크 외부의 리소스에 연결하므로 프라이빗 애플리케이션을 보호합니다.
- 세밀한 액세스 제어: 사용자 역할, 디바이스 컴플라이언스 및 기타 중요한 요소에 따라 액세스 권한을 맞춤화합니다.
- MFA(다단계 인증): 권한이 있는 액세스만 보장하도록 여러 확인 단계를 통해 보안을 강화합니다.
- 강력한 정책 시행: 자세한 보안 정책을 구현하여 사용자 액세스 및 활동을 효과적으로 관리합니다.

Secure Access는 기업 애플리케이션에 대한 안전하고 신뢰할 수 있는 액세스가 중요한 원격 작업 시나리오에 이상적인 파트너입니다. 사용자 액세스 및 활동에 대한 향상된 제어 기능을 통해 내부 리소스를 자신 있게 보호할 수 있습니다.

이 주제에서는 Cisco Umbrella에서 Secure Access로 전환하는 데 도움이 되는 모범 사례를 간략하게 설명합니다.

다음은 Cisco Umbrella에서 Secure Access로 전환하는 데 도움이 되는 모범 사례입니다.

- 업무 시간 외 업그레이드.
- 마이그레이션 툴을 사용하여 한 번에 디바이스 하위 집합을 마이그레이션합니다. 이 단계별 접근 방식은 전체 롤아웃으로 확장하기 전에 소규모 단말기 그룹을 통한 마이그레이션을 확인하는 데 도움이 됩니다.

  단계별로 마이그레이션하면 나머지 디바이스를 마이그레이션하기 전에 정책을 테스트하고, 성공적인 통합을 확인하고, 문제를 해결할 수 있습니다.
- 한 번에 ID의 하위 집합을 리디렉션하려면 트래픽 리디렉션 기능을 사용합니다. 다음을 수행할 수 있는 단계별 업그레이드 접근 방식을 권장합니다.
  - 소규모 ID 그룹으로 인터넷 액세스 규칙을 테스트합니다.
  - 인터넷 액세스 규칙이 성공적으로 통합되었는지 확인합니다.
  - 문제를 조기에 식별하고 해결합니다.

이는 업그레이드를 완료하는 데 필요한 단계에 대한 빠른 개요입니다.

1. Cisco Security Cloud Control(SCC) 계정을 생성합니다. Secure Access 계정을 Umbrella 인스턴스와 연결하려면 구독 클레임 코드가 포함된 환영 이메일을 받아야 합니다. Cisco Security Cloud Control 계정 생성의 단계를 따르십시오.

   자세한 내용은 기존 고객을 위한 Security Cloud Control 시작 가이드에서 구독 클레임을 참조하십시오.
2. 업그레이드 관리자를 활성화합니다.
3. Umbrella 대시보드에서 모든 사전 요건을 완료합니다.
   - 모든 사용자에 대해 Cisco Security Cloud 로그온을 활성화합니다.
   - 가상 어플라이언스 업데이트 및 Active Directory Connector 업데이트.
   - Chromebook 업데이트 및 모바일 디바이스 업데이트.
4. 업그레이드 시작

   Umbrella DNS 정책 및 구성 요소가 Secure Access 인터넷 액세스 정책 및 설정에 복사됩니다.
5. 트래픽 리디렉션

   조직의 ID 트래픽이 Secure Access를 통해 소스로 조정되도록 ID 트래픽을 리디렉션합니다.
6. 업그레이드 완료 및 Umbrella 닫기

   마지막 단계는 Umbrella 계정을 닫고 Secure Access - DNS 방어만 사용하는 것입니다.

# Cisco Security Cloud Control .

Cisco Security Cloud Control은 보안 제품을 관리하고 단일 통합 인터페이스에서 보안 성과를 달성할 수 있는 새로운 보안 플랫폼입니다.

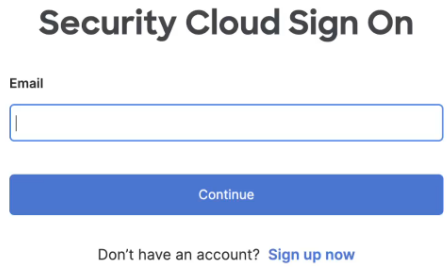
Cisco Security Cloud Control(SCC)은 Cisco 보안 제품에 대한 중앙 집중식 가시성과 관리를 제공합니다. Umbrella DNS에서 Secure Access - DNS 방어로 업그레이드하려면 클레임 코드가 포함된 환영 이메일을 받은 후 Security Cloud Control 계정을 생성해야 합니다. 자세한 내용은 Security Cloud Control에 로그인을 참조하십시오.

이 프로세스의 일부로 Security Cloud Sign On 계정을 생성합니다. Security Cloud Sign On은 하나의 자격 증명 집합으로 여러 Cisco 보안 및 클라우드 서비스에 액세스할 수 있는 솔루션입니다.

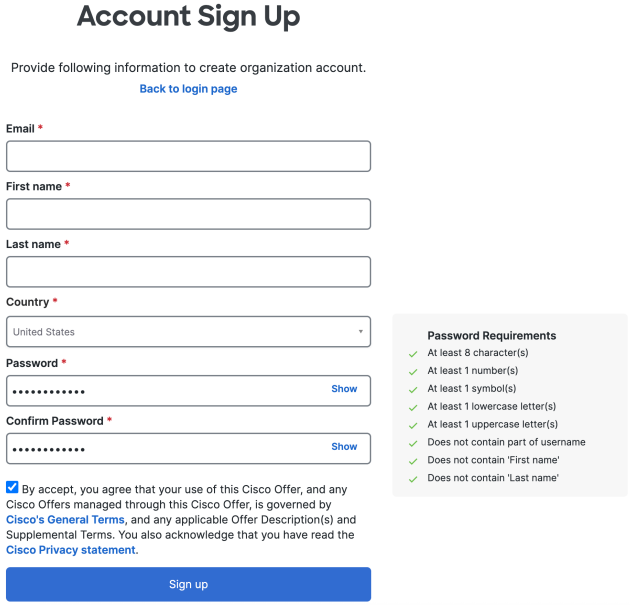
마지막으로, 보안 강화를 위해 다단계 인증을 설정해야 하며 Duo사용을 권장합니다.

---

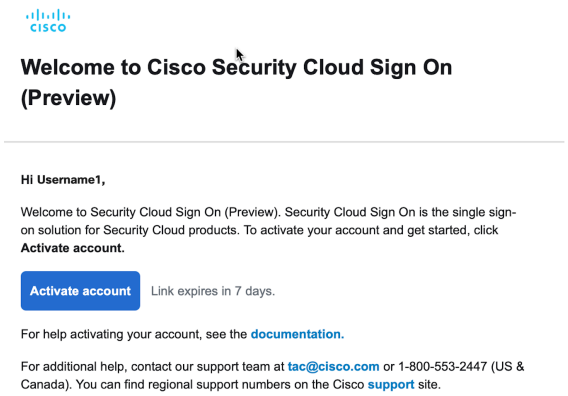
1. Security Cloud Sign On 계정을 생성하여 Security Cloud Control(SCC) 계정을 생성합니다.
2. **Sign up now(**지금 등록**)**를 클릭하여 Security Cloud Sign On 계정을 생성합니다.




3. Account Sign Up(계정 등록) 페이지에 정보를 입력합니다.

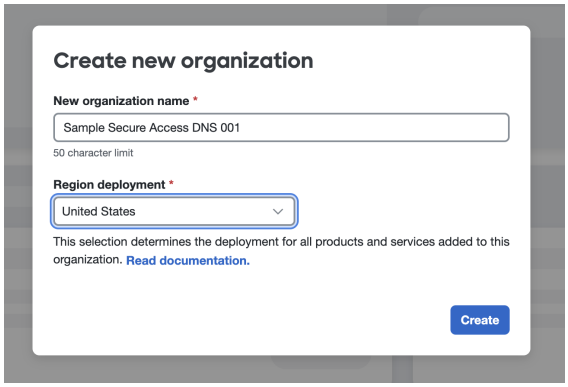



4. 계정을 활성화하기 위해 확인 이메일을 찾습니다. 링크는 7일 후에 만료됩니다.




5. 다단계 인증에 등록합니다. Duo를 사용하는 것이 좋습니다.
6. SCC에 사용자를 추가합니다. 조직의 역할 기반 액세스 제어를 참조하십시오.

   모든 Umbrella 관리자를 추가하여 Umbrella에서 잠기지 않도록 합니다. ID 서비스 제공자를 구성하지 않는 한 모든 사용자는 Duo에 등록해야 합니다.
7. ID 서비스 제공자를 통합하려면 다음 단계를 따르십시오.
8. 새 조직 이름을 생성합니다.




   새 Secure Access 조직의 이름은 Umbrella 조직과 동일해야 합니다. 조직 및 지역에 대한 자세한 내용은 조직 생성을 참조하십시오.

   드롭다운 메뉴에서 지역을 선택합니다. 제품은 전 세계적으로 사용 가능하므로 선택 사항은 기능에 영향을 주지 않습니다.

---

다음 단계에 따라 업그레이드 관리자를 Umbrella 대시보드에 추가합니다.

## Umbrella

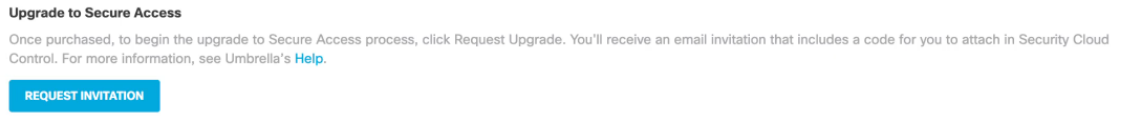
업그레이드 관리자를 활성화하는 방법을 설명합니다.

- **Umbrella**에서 업그레이드 관리자를 활성화하는 관리자는 동일한 이메일 주소를 사용하여 **SCC(Security Cloud Control)** 계정을 생성해야 합니다**.** 다른 이메일을 사용하면 Umbrella 조직을 올바른 SCC 계정에 연결할 수 없으므로 업그레이드가 실패하고 Umbrella 조직을 연결하지 않고 새 Secure Access 조직을 만들 수 있습니다.

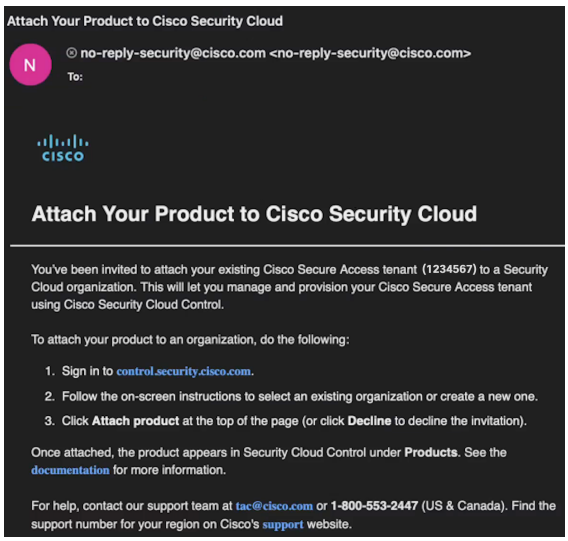
- 관리자가 Secure Access - DNS 방어로 업그레이드하려면 Cisco Security Cloud 로부터 고유한 구독 클레임 코드가 포함된 환영 이메일을 받아야 합니다.
- 구독 클레임 코드를 받은 관리자는 Umbrella에서 업그레이드 관리자를 활성화하기 위한 후속 단계를 완료할 책임이 있습니다.

---

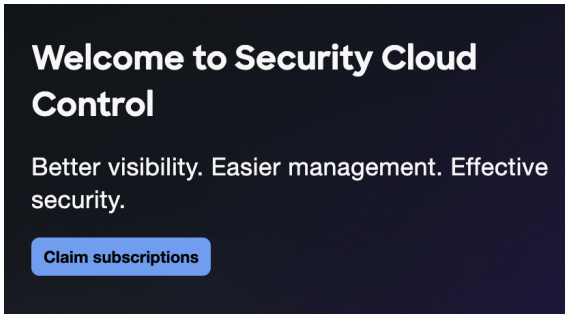
1. Umbrella 계정에 로그인합니다.
2. **Admin(관리) > Licensing(라이선싱) > Upgrade to Secure Access(보안 액세스로 업그레이드)**로 이동하여 **Request Invitation(초대 요청)**을 클릭합니다.



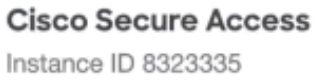

3. **Cisco Security Cloud**에 제품 첨부에 대한 초대 이메일을 확인하십시오.




4. 이메일에 있는 링크를 클릭하여 Security Cloud Control 계정에 로그인합니다. 업그레이드 관리자를 활성화하는 Umbrella 관리자는 동일한 이메일 주소를 사용하여 Security Cloud Control 계정을 생성해야 합니다.
5. **Claim subscription(구독 클레임)**을 클릭합니다.

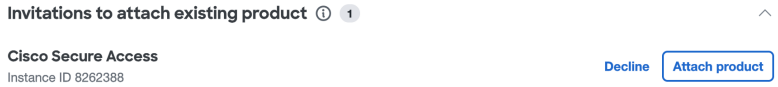



6. **Cisco Secure Access** 인스턴스 **ID**가 Umbrella 조직 ID와 동일한지 확인합니다.

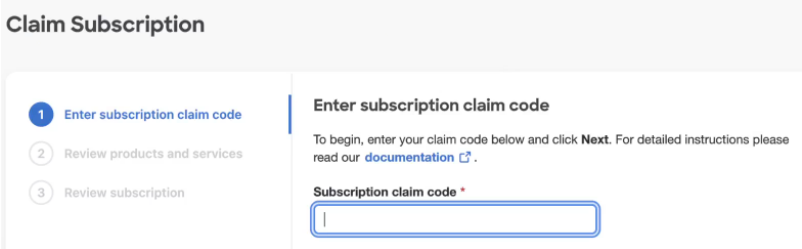


7. **Attach Product(**제품 연결**)**를 클릭한 다음 **Attach(**연결**)**를 클릭하여 Umbrella 조직을 Secure Access 인스턴스에 연결합니다.

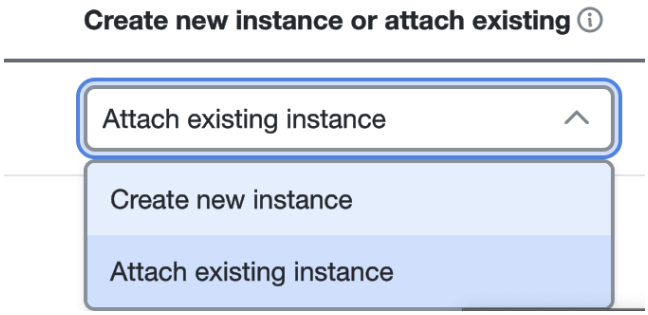
   본 작업은 완료되지 않은 상태로 둘 수 없습니다**.**




8. **Claim subscription(**구독 클레임**)**을 클릭하고 구독 클레임 코드를 입력합니다.



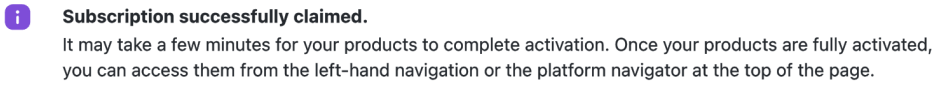

9. **Next(**다음**)**를 클릭하여 구독 클레임 워크플로를 시작합니다.
10. 드롭다운 목록에서 **Attach existing instance(**기존 인스턴스 연결**)**를 선택합니다.




   새 인스턴스 를 생성하지 마십시오. 새 조직은 Secure Access - DNS 방어로 업그레이드하지 않습니다.

11. **Claim(**클레임**)**을 클릭하여 구독 ID 및 제품 라이선스를 포함한 구독 세부 정보를 새 Secure Access 조직에 연결합니다.

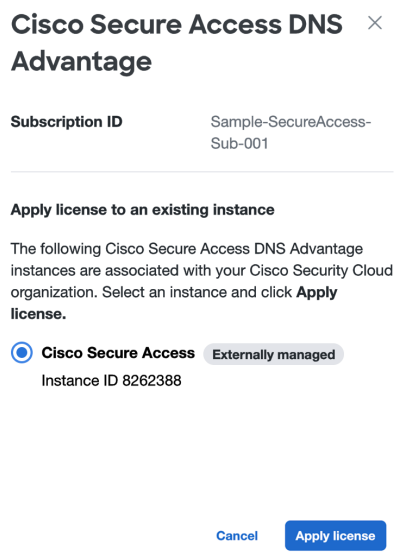
    구독이 청구되었습니다. 제품의 활성화를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 제품이 완전히 활성화되면 왼쪽 탐색 메뉴 또는 SCC 페이지 상단에 있는 플랫폼 탐색기에서 액세스할 수 있습니다.



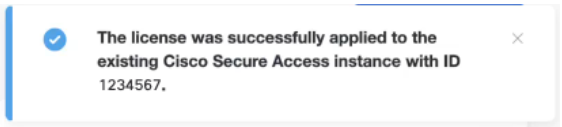

12. **Product and service activation status(**제품 및 서비스 활성화 상태**)**에서 **Action required(**작업 필요**)**를 클릭합니다.




13. **Apply license(**라이선스 적용**)**를 클릭하여 Cisco Secure Access를 기존 Umbrella 계정에 연결합니다.




Cisco Secure Access 인스턴스에 라이선스가 성공적으로 적용되었음을 알리는 알림이 표시됩니다.




14. 왼쪽 탐색 메뉴에 업그레이드 관리자를 표시하려면 Umbrella 대시보드에 로그인합니다.




15. 새 Secure Access 조직을 생성하기 전에 **Upgrade Manager(**업그레이드 관리자**)**를 클릭하여 필요한 사전 요건을 완료하는 프로세스를 시작합니다.

다음 단계, 사전 요건, 업그레이드 시작을 참조하여 새 Secure Access 조직을 생성합니다.

---

Cisco Secure Access - DNS 방어에서 지침 및 제한 사항에 대해 자세히 알아보십시오.

**Umbrella Secure Access**

업그레이드 시작 단계를 완료하면 Umbrella 애플리케이션 설정이 Secure Access 애플리케이션 목록이 됩니다. 애플리케이션 설정 및 애플리케이션 목록은 별도로 관리되며, 애플리케이션 범주에 대한 변경 사항은 두 대시보드 간에 반영되지 않습니다. 업그레이드 관리자의 마지막 단계를 완료하고 Umbrella 계정을 영구적으로 닫을 때까지 변경을 수행하지 않는 것이 좋습니다.

액세스 차단 및 허용이 있는 Umbrella의 애플리케이션 설정은 Secure Access에서 두 개의 애플리케이션 목록으로 분리됩니다. 애플리케이션 목록은 Secure Access 인터넷 액세스 규칙을 지원하도록 차단 또는 허용만 합니다.

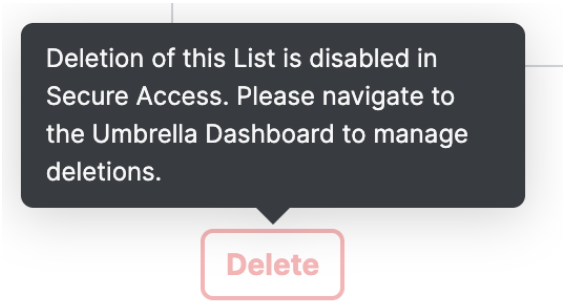
**Umbrella**

- ID가 포함되지 않은 Umbrella DNS 정책은 Secure Access에 복사되지 않습니다.
- 비활성화된 Umbrella DNS 정책은 Secure Access에 복사되며 비활성화된 상태로 유지됩니다.

- Secure Access는 인텔리전트 프록시를 지원하지 않습니다. 이 수준의 DNS 보안을 복제하려면 Secure Access 구독을 유사한 DNS 레이어 보호 수준인 Secure Access DNS Defense로 다운그레이드하거나 Secure Access로 업그레이드하고 Secure Access SWG(Secure Web Gateway)를 구현하는 것이 좋습니다. 여기서 더욱 포괄적인 보안 태세를 제공하는 전체 웹 프록시 기능을 구성할 수 있습니다.

### , SaaS Umbrella

업그레이드가 시작되면 업그레이드 관리자의 4단계를 완료하고 Umbrella 계정을 닫을 때까지 Secure Access에서 Umbrella 정책에 대한 삭제 기능이 비활성화됩니다. 또한 보안 프로파일과 인터넷 및 SaaS 리소스에 나열된 Umbrella 정책 구성 요소는 업그레이드 관리자가 활성인 동안에는 Secure Access에서 삭제할 수 없습니다.




차단 페이지 우회는 복사되지 않습니다. Secure Access 기능에 대한 자세한 내용은 알림 페이지 관리를 참조하십시오.

맞춤형 사용자 역할은 복사되지 않습니다. Secure Access에는 두 가지 역할만 있습니다.

- 전체 관리자
- 읽기 전용

자세한 내용은 새 계정 추가를 참조하십시오.

**Connect(연결) > End User Connectivity(최종 사용자 연결) > Internet Security(인터넷 보안) > Traffic Steering(트래픽 조정)**으로 이동하여 내부 도메인 허용 목록을 찾습니다.

### Secure Access ID

Secure Access 정책은 규칙 기반이며 각 규칙은 최대 **250**개의 고유한 소스 **ID**를 지원합니다. Umbrella 정책 **[%POLICY NAME%]**이 Secure Access로 변환할 때 결과 규칙이 이 제한을 초과할 수 있습니다. 마이그레이션을 계속할 수 있습니다. 그러나 Umbrella 정책에 250개 이상의 고유 소스 ID가 포함되어 있는 경우 마이그레이션이 실패할 수 있습니다.

정책에서 소스 ID로 **All(모두)**을 사용하는 경우 이 경고를 무시해도 됩니다. 예를 들어 **All Roaming Computers(모든 로밍 컴퓨터)**를 선택한 경우 Umbrella 정책에서 250보다 큰 개수가 표시될 수 있지만, 이 선택 사항은 단일 소스 ID로 변환됩니다.

### SaaS

인터넷 및 SaaS 리소스 페이지에는 인터넷 액세스 규칙을 설정할 때 대상으로 사용할 수 있는 재사용 가능한 구성 요소("개체"라고도 함)가 포함되어 있습니다. 인터넷 및 SaaS 리소스는 다음을 포함합니다.

- 대상 목록

> 주
>
> Cisco Secure Access는 이에 상응하는 기능을 제공하지 않으므로 SAML 우회 대상 목록은 Cisco Umbrella에서 Cisco Secure Access로 마이그레이션되지 않습니다.

- 애플리케이션 목록
- 콘텐츠 범주 목록

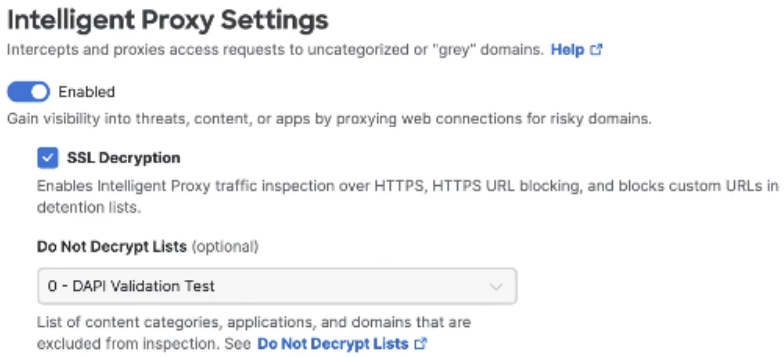
### Umbrella

레거시 Umbrella 콘텐츠 범주는 Secure Access에서 해당 범주로 업그레이드됩니다. 자세한 내용은 사용 가능한 콘텐츠 범주를 참조하십시오.

Cisco Secure Access Security 프로파일은 액세스 정책의 규칙에 사용할 수 있는 재사용 가능한 구성 요소입니다. 인터넷 액세스 규칙에 대한 보안 프로파일에는 보안 제어 및 허용 사용 제어와 같이 집합으로 구성하는 기타 설정이 포함됩니다. 자세한 내용은 인터넷 액세스용 보안 프로파일 추가를 참조하십시오. 보안 프로파일은 다음을 포함합니다.

- 위협 범주
- 파일 검사
- SafeSearch
- 암호 해독 안 함 목록
- 알림 페이지

Umbrella의 선택적 암호 해독이 보안 액세스의 암호 해독 안 함 목록으로 업그레이드됩니다. 업그레이드 관리자가 실행되는 동안에는 Umbrella에서 생성된 정책에 연결된 Do Not Decrypt(암호 해독 안 함) 목록을 변경할 수 없습니다. Umbrella 계정을 닫으면 이 옵션이 활성화됩니다. 자세한 내용은 인텔리전트 프록시 활성화 및 암호 해독 안 함 목록을 참조하십시오.



Secure Access에서 고정 키는Connect(연결) > Users(사용자), Groups(그룹) > Configuration Management(구성 관리) > Integrate Directories(디렉터리 통합) > IdP로 이동하여 찾을 수 있습니다. 자세한 내용은 ID 제공자용 프로비저닝 토큰을 참조하십시오.

### Umbrella API

Umbrella API가 2022년에 릴리스된 이후 레거시 API 키가 보안 액세스로 전송되지 않습니다. Secure Access에서는 API 키, KeyAdmin 키 및 고정 키를 계속 사용합니다. 자세한 내용은 API 키 관리 및 Secure Access API 인증을 참조하십시오.

# 제 2 장

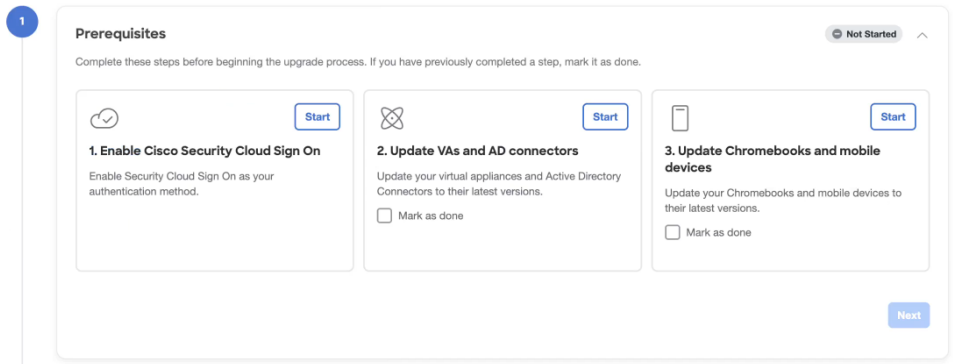
:


- Cisco Security Cloud □□□ □□□
- □□ □□□□□□ □□□□ □□
- Active Directory Connector □□□□ □□
- Chromebook □□□□
- □□□ □□□□ □□□□


Secure Access - DNS 방어로 업그레이드하기 전에 모든 사전 요건을 완료해야 합니다.

Secure Access - DNS 방어로 업그레이드하기 전에 모든 사전 요건이 완료되었는지 확인합니다.

1. Cisco Security Cloud 로그온 활성화
2. 가상 어플라이언스 업데이트 및 Active Directory Connector 업데이트
3. Chromebook 업데이트 및 모바일 디바이스 업데이트




주

업그레이드하기 전에 레거시 API를 사용하여 등록된 네트워크 디바이스를 추가합니다. 레거시 API로 네트워크 디바이스를 설정하는 방법에 대한 지침은 https://securitydocs.cisco.com/docs/umbrella-sig/olh/152032.dita에서 하드웨어 통합 섹션을 참조하십시오.

주

Umbrella DNS 전용 패키지에서 **Secure Access - DNS** 방어 대신 **Secure Access - Essentials**또는 **Secure Access - Advantage**로 업그레이드하는 경우 마이그레이션 전에 기존 Umbrella DNS 정책에서 인텔리전트 프록시를 비활성화합니다.

DNS 전용에서 전체 보안 액세스로 마이그레이션하는 동안 Umbrella DNS 인텔리전트 프록시는 DNS 전용 구축에 사용되는 선택적 프록시가 아닌 전체 프록시로 업그레이드됩니다. 마이그레이션 후 예기치 않은 프록시 동작을 방지하기 위해 미리 인텔리전트 프록시를 비활성화하는 것이 좋습니다.

## Cisco Security Cloud

이 주제에서는 Cisco Security Cloud 로그인을 활성화하고 Umbrella 관리자용 Security Cloud Control 계정을 생성하는 방법을 설명합니다.

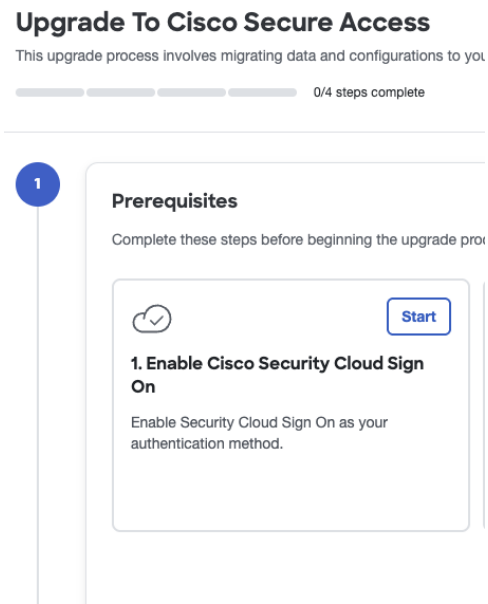
Cisco Security Cloud Sign On(SCSO)을 사용하면 모든 디바이스에서 하나의 자격증명 집합으로 모든 Cisco Security 제품에 액세스할 수 있습니다. Security Cloud Control은 Cisco Security Cloud Sign On이 제품 전반에서 원활한 인증을 제공하는 반면, 단일 통합 인터페이스를 통해 이러한 제품을 관리하고 보안 결과를 달성하는 플랫폼입니다.

- 전체 관리자 사용자 역할이 필요합니다.
- 기존 **SAML** 구성**:** 조직에서 이미 Umbrella와 함께 ID 공급자(IdP)를 사용하는 경우 이 기능을 활성화하기 전에 Security Cloud 제어에서 동일한 IdP를 구성해야 합니다. 이렇게 하면 기존 인증 플로우가 그대로 유지되고 관리자 잠금이 방지됩니다. 명시적으로 필요한 경우가 아니면 기존 Umbrella IdP 구성을 제거하지 마십시오.
- 사용자 계정 확인**:** Umbrella 관리자 계정이 Security Cloud Control에 수동으로 생성된 사용자로 또는 IdP를 통해 프로비저닝된 사용자로 존재하는지 확인합니다. 액세스 문제를 방지하려면 Umbrella와 Security Cloud Control 모두에서 동일한 관리자 이메일 주소를 사용합니다.

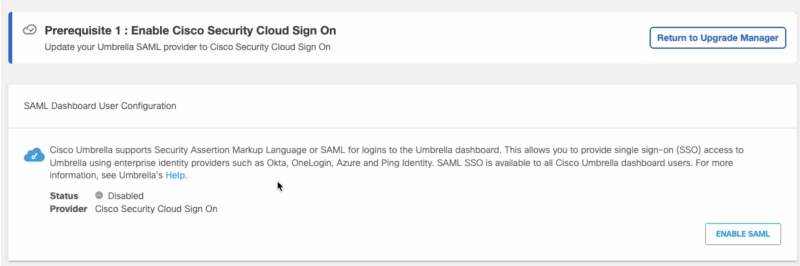
  자세한 내용은 기존 고객을 위한 Security Cloud Control 시작 가이드에서 Security Cloud Sign On 개요를 참조하십시오.

---

1. 업그레이드 관리자로 이동합니다. **Enable Cisco Security Cloud Sign On(Cisco Security Cloud Sign On 활성화)** 사전 요건 단계에서**Start(**시작**)**를 클릭합니다.

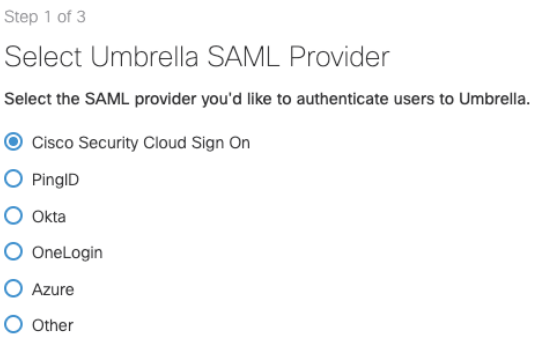



2. **Enable SAML(SAML** 활성화**)**을 클릭합니다.



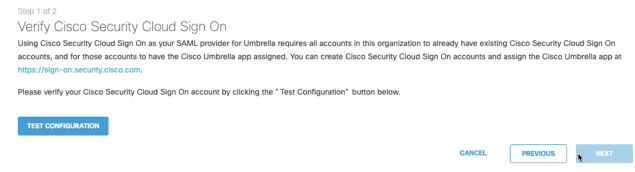

3. 현재 구성에 따라 다음 작업 중 하나를 수행합니다.

   - **SAML**을 구성하지 않은 경우Cisco Security Cloud Sign On을 클릭하여 모든 Umbrella 대시보드 사용자에 대한 Security Cloud Sign On 계정을 생성합니다. 다음 창에서 **Sign up now(**지금 등록**)**를 클릭합니다. 계정 생성에 대한 자세한 내용은 사용자 초대를 참조하십시오.

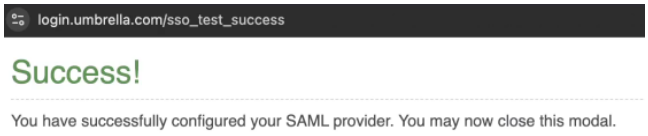
   - **SAML**을 이미 구성한 경우**:** 기존 IdP가 Security Cloud Control에 구성되어 있는지 확인하고 계정 연결을 진행합니다.

4. 계정이 생성되면 **Upgrade Manager(**업그레이드 관리자**) > Prerequisite(**사전 요건**) > Enable Cisco Security Cloud Sign On(Cisco Security Cloud Sign On** 활성화**) > Start(**시작**)**로 이동합니다. **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다.

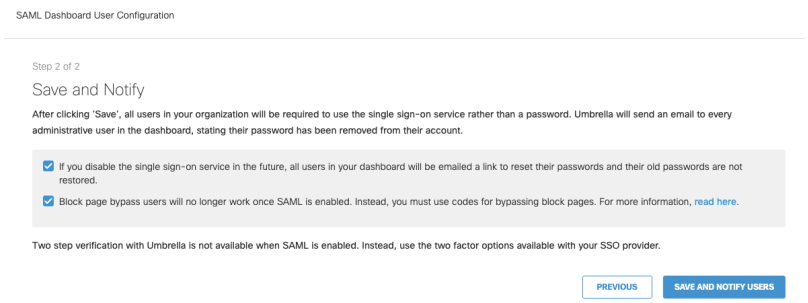
   
   

   설정을 완료하려면 테스트 구성을 수행하고 성공해야 합니다.

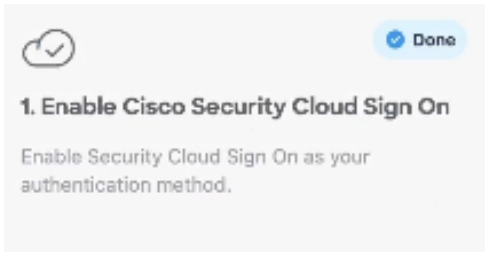
   인증이 완료되면 성공 모달이 표시됩니다.

5. **Next(**다음**)**를 클릭합니다. 두 확인란을 모두 선택하여 정보를 승인하고 **Save and Notify Users(**저장 및 사용자에게 알리기**)**를 클릭합니다.




6. **Return to Upgrade Manager(**업그레이드 관리자로 돌아가기**)** 및 **Cisco Security Cloud Sign On**활성화 단계가 Start(시작)에서 **Done(** 완료**)**으로 변경됩니다.




---

다음 단계에 따라 가상 어플라이언스 및 Active Directory 커넥터가 최신 상태인지 확인합니다.

Cisco Security Cloud Sign On을 활성화한 후:

- 앞으로 Cisco Security Cloud Sign On은 Umbrella 대시보드 사용자의 필수 로그인 방법이 됩니다.
- Umbrella가 모든 대시보드 사용자(최종 사용자 제외)에게 이메일을 전송하여 필수 SSO(Single Sign-On)와 비밀번호가 더 이상 허용되지 않음을 알립니다.
- 나중에 SSO가 비활성화되면 이전 암호가 더 이상 유효하지 않으므로 모든 사용자가 암호 재설정 링크가 포함된 이메일을 받게 됩니다.
- SAML이 활성화되어 있으면 차단 페이지 우회 사용자가 더 이상 작동하지 않습니다.

---

가상 어플라이언스가 업데이트되었는지 확인합니다.

새로운 VA(가상 어플라이언스) 소프트웨어 버전은 자동으로 제공되며, 일반적으로 어떤 개입 없이 적용됩니다. DNS 서비스의 고가용성을 보장하고 자동 업데이트가 수행되도록 하려면 두 개의 VA가 실행 중이어야 합니다.

커넥터와 VA 모두 자동 업데이트를 지원합니다. 업데이트를 다운로드하려면 이러한 구성 요소에서 다음 URL에 액세스할 수 있어야 합니다.

- 443 (TCP) - disthost.opendns.com
- 443 (TCP) - disthost.umbrella.com

릴리스 노트를 포함하여 예정된 버전에 대한 자세한 내용은 서비스 업데이트를 참고하십시오. 업데이트 알림을 받으려면 **Follow(**팔로우**)**를 클릭하십시오.

가상 어플라이언스 업데이트는 일반적으로 자동으로 업데이트되지만 수동으로 업데이트할 수도 있습니다.

VA를 v3.7.1 이상으로 업데이트하고 인증 향상을 구성하는 것이 좋습니다.

새 버전을 VA에 자동으로 설치하려면 최소 두 개의 **VA**를 설치해야 합니다. 업데이트 프로세스가 진행되는 동안 다운타임이나 서비스 중단이 발생하지 않도록 VA가 두 개 있어야 합니다.

VA의 "현재 위치" 수동 업데이트를 수행하면 최대 **15**분의 다운타임이 발생합니다. 이 시간 동안에는 네트워크에서 DNS 쿼리를 수행할 수 없으며 인터넷 서비스를 효과적으로 유지할 수 없습니다.

가상 어플라이언스를 업데이트하려면 다음 단계를 따르십시오.

- 가상 어플라이언스 업데이트
- 가상 어플라이언스 인증 구성

## Active Directory Connector

Active Directory Connector가 업데이트되었는지 확인하십시오.

Cisco AD(Active Directory) Connector는 Umbrella와 통합되어 조직에서 사용자 및 그룹을 프로비저닝합니다. LDIF(LDAP Interchange Format) 소스 파일을 사용하여 사용자 및 그룹을 프로비저닝하도록 AD 커넥터를 설치하고 구성할 수 있습니다. 서버에 LDIF 파일을 구축하면 AD Connector가 조직의 사용자 및 그룹을 Umbrella와 동기화합니다.

### Active Directory Connector

다음은 AD Connector용 자동 업데이트를 설정하는 단계입니다.

Umbrella가 구축된 AD Connector에서 Cisco AD Connector 소프트웨어를 업데이트하는 날짜와 시간을 예약합니다. Umbrella는 예약된 경우 AD Connector에 최신 버전의 소프트웨어가 설치되어 있는지 확인합니다. 새 버전을 사용할 수 있는 경우 Umbrella는 설치된 AD Connector 소프트웨어를 시스템에서 제거하고 최신 버전의 AD Connector를 구축합니다.

Umbrella에서 전체 관리자 액세스 권한이 있어야 합니다.

1. **Deployments(**구축**) > Configurations(**구성**) > Sites and Active Directory(**사이트 및 **Active Directory)**로 이동하고 **Settings(**설정**)**를 클릭합니다.
2. **Active Directory Connector Auto-Upgrades(Active Directory Connector** 자동 업그레이드**)**로 이동하여 **Edit(**편집**)**을 클릭합니다.
3. **Day(**요일**)**에서 AD Connector 소프트웨어를 업데이트할 요일을 선택합니다.

> 주
>
> 기본값 **Day(**요일**)**는 **Any day(**모든 요일**)**임 - 소프트웨어 업데이트가 사용 가능한 경우 Umbrella는 최신 버전의 소프트웨어로 AD Connector를 재구축하려고 시도합니다.

4. **Time Range(**시간 범위**)**에서 4시간 기간을 선택하여 예약된 날짜에 AD 커넥터를 업데이트합니다.

> 주
>
> 기본 **Time Range(**시간 범위**)**는 오전 **2:00~**오전 **6:00(PST)**입니다.

### Active Directory Connector

Active Directory Connector를 수동으로 업그레이드하려면 이 절차를 사용하십시오.

Umbrella에서 전체 관리자 액세스 권한이 있어야 합니다.

1. **Deployments(**구축**) > Configurations(**구성**) > Sites and Active Directory(**사이트 및 **Active Directory)**로 이동합니다.
2. **Version(**버전**)** 필드에서 버전이 오래된 AD 커넥터에 대한 빨간색 느낌표 기호를 클릭합니다.

   AD 커넥터 업그레이드 중에 업그레이드할 수 있는 AD 커넥터 버전을 나타내는 확인 메시지 및 몇 분의 다운타임에 대한 경고가 표시됩니다.
3. **Upgrade(**업그레이드**)**를 클릭합니다.

   진행 중인 수동 업그레이드는 **Version(**버전**)** 필드에서 실행 중인 시계 기호로 표시됩니다.

## Chromebook

모든 Chromebook 및 Cisco Chromebook 클라이언트가 업데이트되었는지 확인합니다.

모든 Chromebook 운영 체제 및 Chromebook 클라이언트가 업데이트되었는지 확인합니다. Chromebook에서 소프트웨어를 업데이트하는 작업은 Google에서 진행합니다. Cisco가 Chrome 웹 저장소에서 Chromebook 클라이언트를 위한 Cisco Security를 업데이트하면 Google에서 모든 Chromebook으로 업그레이드를 자동으로 푸시합니다. 이 프로세스에는 몇 시간 정도 걸릴 수 있습니다. 자세한 내용은 Chromebook 클라이언트 FAQ를 참고하십시오.

- Chromebook 운영 체제를 버전 122 이상으로 업데이트합니다.
- Chromebook 클라이언트용 Cisco Security 2.1.1 이상으로 업데이트합니다.

업그레이드를 시도하기 전에 모든 모바일 디바이스 및 클라이언트가 최신 버전인지 확인합니다.

업그레이드를 시도하기 전에 모든 모바일 디바이스 및 클라이언트가 최신 상태인지 확인합니다. 설정된 모바일 디바이스나 클라이언트가 없는 경우 다음 단계로 진행할 수 있습니다.

자세한 내용은 관리되는 Android 디바이스를 참조하십시오.

자세한 내용은 관리되는 iOS 디바이스를 참조하십시오.

자세한 내용은 관리되지 않는 모바일 디바이스 보호를 참조하십시오.

# 제 3 장

:


- Secure Access - DNS □□ □□□□□
- □□□ □□□ □□ □□□□
- □□□ □□ □□ □□: Secure Web Gateway □□□


이 단계에서는 새 Secure Access 조직을 생성하고 Umbrella 구성에 복사합니다.

업그레이드 프로세스를 시작하면 새 보안 액세스 - DNS 방어 조직이 생성됩니다. Umbrella는 이 프로세스 중에도 계속 작동하며 조직은 항상 보호됩니다.

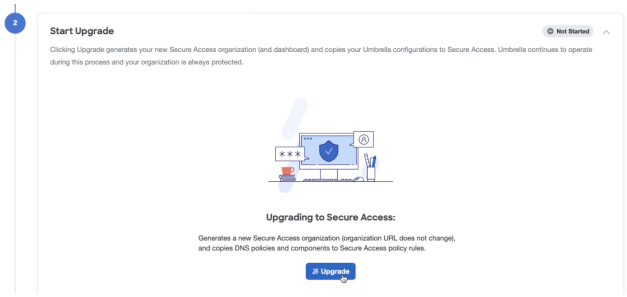
Umbrella DNS 정책 및 구성 요소는 인터넷 액세스 규칙, 설정, 인터넷 및 SaaS 리소스로 보안 액세스에 복사됩니다. 업그레이드 후 보안 액세스에서 Umbrella DNS 정책을 여러 규칙으로 분할할 수 있습니다. 규칙과 테스트의 순서를 검토하여 원하는 트래픽 처리 방식인지 확인해야 합니다.

## Secure Access - DNS

업그레이드를 클릭하면 새 Secure Access 조직이 생성되고 Umbrella 구성이 복사됩니다.

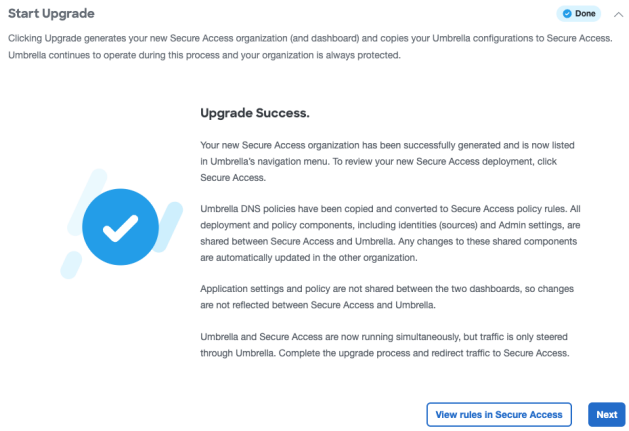
Umbrella에서 Secure Access로의 업그레이드가 진행되는 동안에는 정책을 변경하지 않는 것이 좋습니다. 정책이 의도하지 않게 변경되는 것을 방지하려면 업그레이드가 완료될 때까지 기존 보안 프로파일을 편집하거나 삭제하지 마십시오. Umbrella 사후 변환에서 생성된 정책은 Secure Access에 동기화되지 않습니다. 새 정책 구성 요소 매핑에 대한 내용은 인터넷 액세스 정책 시작하기를 참조하십시오.

1. 시작하려면 **Upgrade(**업그레이드**)**를 클릭합니다. 업그레이드 중에는 페이지를 종료하지 마십시오. 모든 변경 사항이 손실되며 처음부터 다시 시작해야 합니다. 업그레이드 시간은 Umbrella에서 Secure Access로 복사된 정책의 수에 따라 다릅니다.



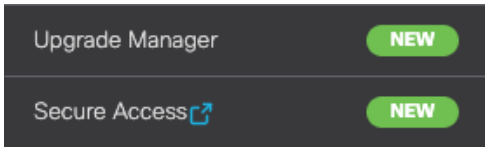

2. 업그레이드가 완료되면 **Upgrade Success(**업그레이드 성공**)**가 표시됩니다.

   새 Secure Access 조직이 성공적으로 생성되었습니다.




3. **View rules in Secure Access(Secure Access**에서 규칙 보기**)**를 클릭하여 새 Secure Access 대시보드로 이동하거나 **Next(**다음**)**를 클릭하여 **Redirect Traffic(**트래픽 리디렉션**)**으로 이동합니다.

   Secure Access 바로가기는 다음에 Umbrella에 로그인 때 왼쪽 탐색 창에 나타납니다.




   Umbrella 정책이 Secure Access의 규칙으로 복사되었는지 확인합니다. 새로운 매핑에 대한 자세한 내용은 인터넷 액세스 규칙을 참조하십시오.

규칙을 생성하는 방법에 대한 자세한 내용은 인터넷 액세스 규칙 시작하기를 참조하십시오.

4. **Upgrade Failed(**업그레이드 실패**)**가 표시되는 경우 **Upgrade(**업그레이드**)**를 다시 클릭하거나 지원팀에 문의합니다.

---

다음 단계에서 Umbrella ID를 보안 액세스로 리디렉션하기 시작합니다.

업그레이드 중 보안 액세스를 위한 중요 로그인 지침

업그레이드 관리자가 활성인 동안에는 Umbrella 대시보드를 통해서만 Secure Access에 액세스할 수 있습니다.

Cisco Secure Access에서 직접 로그인 리디렉션 루프가 발생할 수 있으며 지원되지 않습니다. 4단계: 업그레이드 완료 및 Umbrella 닫기가 완료될 때까지 Umbrella 대시보드만 로그인 방법으로 지원됩니다.

---

Umbrella DNS 정책은 이제 액세스 정책의 Secure Access 인터넷 액세스 규칙입니다.

Umbrella에서 Secure Access로 업그레이드하면 정책 구조화 방식이 변경됩니다. 정책이 여러 차단 및 허용 구성 요소를 포함할 수 있는 Umbrella와 달리 Secure Access는 통합 정책 모델을 사용합니다. 이 모델의 각 규칙은 트래픽을 차단하거나 허용하도록 구성할 수 있습니다. 전환 과정에서 Umbrella 정책은 보안 액세스에서 다음과 같은 특정 순서에 따라 최대 3개의 고유한 규칙으로 변환됩니다.

1. 허용 규칙(기본): 첫 번째 규칙은 원래 Umbrella 정책에 지정된 대로 트래픽을 허용하는 허용 규칙입니다.
2. 차단 규칙(보조): 두 번째 규칙은 원래 Umbrella 정책에 정의된 대로 트래픽 제한을 적용하는 차단 규칙입니다.
3. 허용 규칙(기본값): 정책 평가가 Umbrella의 정책 모델과 일치하는지 확인하기 위해 세 번째 규칙을 암시적 허용 규칙으로 도입할 수 있습니다. 이 규칙은 대상에 대해 명시적으로 일치하는 항목이 없어 의도하지 않은 트래픽 중단을 방지하는 시나리오를 설명합니다.

> 주
>
> 규칙과 규칙 집합이 동일한 ID를 사용하는 경우 암시적 허용 규칙은 생성되지 않습니다.

비 터미널 허용: 암시적 허용 규칙을 지원하기 위해 Secure Access는 비 터미널 허용 기능을 도입했습니다. 이 기능은 기본 규칙이 다음을 보장합니다.

- 시행 측에서 규칙 평가를 종료하지 않으므로 트래픽을 추가로 분석할 수 있습니다.
- 기본적으로 안전한 웹사이트 및 악의적이 아닌 웹사이트에 대한 일반 액세스를 허용합니다. Cisco의 위협 인텔리전스에서 악의적으로 명시적으로 플래그가 지정되지 않은 웹사이트는 허용됩니다.
- 기본 규칙은 맞춤형 규칙이 구성될 때까지 원래 Umbrella 정책의 모든 소스에 적용됩니다.
- Destination(대상)은 Any(모두)로 설정됩니다.

기본 규칙의 작동 방식**:**

- 비 터미널 허용 규칙이 일치할 경우, 동일한 쿼리 주기 동안 그 이상에서는 어떤 규칙도 평가되지 않습니다.

- 하지만 이 규칙은 다음과 같은 특정 상황에서 동일한 쿼리에 대한 후속 평가를 허용합니다. CNAME 레코드를 분석할 때 그리고 DNS 확인에서 확인된 IP 주소를 검색한 후.

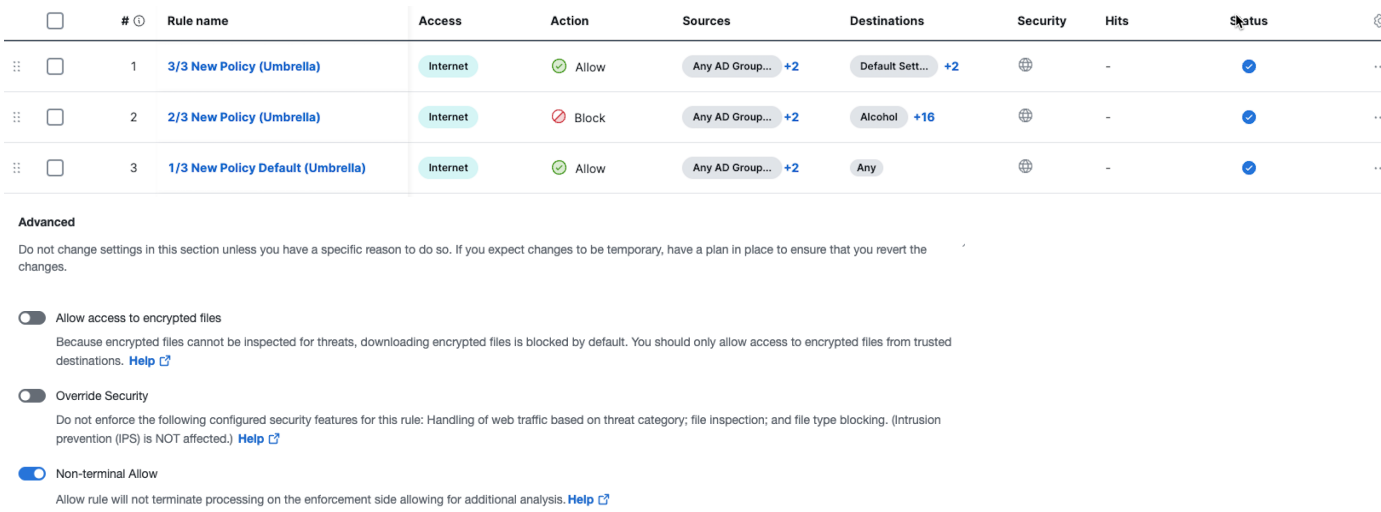
> 주
>
> 소스는 이렇게 새로 분리된 규칙에서 동일하게 유지됩니다.

**Umbrella** 정책을 **Secure Access** 규칙으로 업그레이드

예: 이름이 "새 정책"인 Umbrella 정책은 AD 그룹, AD 사용자, AD 컴퓨터를 ID로 하고, 콘텐츠 범주는 모든 성인 관련 웹사이트 및 불법 활동을 차단하며, 애플리케이션 설정은 박스 클라우드 스토리지를 허용합니다.

Secure Access의 액세스 정책에 Umbrella 정책이 표시됩니다.

1. 첫 번째 규칙의 이름, **3/3** 새 정책**(Umbrella)**. 소스: AD 그룹, AD 사용자, AD 컴퓨터. 애플리케이션 목록 허용: 박스 클라우드 스토리지.
2. 두 번째 규칙의 이름은 **2/3** 새 정책**(Umbrella)**입니다. 소스: AD 그룹, AD 사용자, AD 컴퓨터. 차단 콘텐츠 범주 목록: 모든 성인 관련 웹사이트 및 불법 행위를 차단합니다.
3. 세 번째 규칙의 이름은 **1/3** 새 정책 기본값**(Umbrella)**입니다. 소스: AD 그룹, AD 사용자, AD 컴퓨터. Any(모두) 허용. 비 터미널 허용을 확인하려면 **Secure(**보안**) > Access Policy(**액세스 정책**)**으로 이동 **> Default (Umbrella)** 규칙 옆에 있는 **Edit(**편집**)** 클릭 **> Configure Security(**보안 구성**) > Next(**다음**) > Advanced(**고급**) > Non-terminal Allow(**비 터미널 허용**)** 클릭.




자세한 내용은 인터넷 액세스 규칙 시작하기 및 액세스 정책 관리를 참조하십시오.

**1:**

| **Umbrella** 정책 구성 요소 | 안전한 액세스 인터넷 액세스 규칙 |
|---|---|
| 정책 | 인터넷 액세스 정책 |
| 애플리케이션 설정 | 애플리케이션 목록 |
| 차단 페이지 표시 | 알림 페이지 |
| 콘텐츠 범주 | 콘텐츠 범주 |
| 대상 목록 | 대상 목록 |

| **Umbrella** 정책 구성 요소 | 안전한 액세스 인터넷 액세스 규칙 |
|---|---|
| ID | 출처 |
| 모바일 디바이스 및 로밍 컴퓨터 | 로밍 디바이스 |
| 보안 설정 | 위협 범주 |
| 선택적 암호 해독 | 암호 해독 안 함 목록 |

## : Secure Web Gateway

SWG가 활성화된 경우 규칙 시행에 대해 설명합니다.

> 주
>
> 여기에 설명된 기능 중 일부는 Secure Access 패키지에 제공되지 않을 수도 있습니다. 현재 패키지를 확인하려면 Admin(관리) → Subscription(구독)으로 이동합니다. 자세한 내용은 현재 패키지 확인을 참조하십시오.
>
> 여기에 설명된 기능에 액세스할 수 없는 경우 영업 담당자에게 자세한 내용을 문의하십시오. Cisco Umbrella 및 Cisco Secure Access 패키지를 참조하십시오.

Cisco Umbrella에서 Cisco Secure Access로 업그레이드하면 조직에 대해 SWG(Secure Web Gateway)가 활성화된 경우 규칙 시행이 변경됩니다. 보안 액세스에서 SWG 프록시는 URL을 포함하는 대상이 있는 규칙(example.com/login)에 대한 최종 시행을 수행합니다.

차단 규칙이 URL과 일치하는 경우, DNS 확인자는 전체 URL 경로를 평가할 수 없으며 도메인 (example.com)만 식별할 수 있습니다. 이 경우 Secure Access는 SWG로 시행을 연기합니다.

1. **DNS Evaluation(DNS** 평가**)**: 대상(example.com/login)을 평가하기 위한 요청입니다. DNS 리졸버는 도메인(example.com)만 확인하고 SWG에 따라 시행합니다.
2. **SWG**로 지연된 시행: 보안 액세스는 차단 페이지(알림 페이지)를 반환하는 대신 대상 IP 주소를 반환하고, SWG가 웹 트래픽을 차단하고 HTTP 또는 HTTPS 계층에서 차단을 적용할 것으로 기대합니다.
3. **SWG**가 트래픽 경로에 있어야 함: 차단을 적용하려면 네트워크 터널 그룹, PAC 파일 또는 Cisco Secure Client를 사용하여 SWG를 통해 사용자 트래픽을 조정해야 합니다.
4. **SWG** 미적용 결과: 트래픽이 DNS 전용 경로를 따르고 SWG를 통과하지 않는 경우 차단이 시행되지 않고 트래픽이 허용됩니다.

조직 전체에서 일관된 규칙을 시행하려면 다음 단계를 따르십시오.

1. 명시적 도메인 이름 사용: 전체 도메인에 시행을 적용하려면 대상 목록에 도메인(example.com)을 추가합니다. 특정 URL(example.com/login)을 사용하는 경우 URL 기반의 시행에는 웹 레이어 검사가 필요하므로 해당 트래픽은 SWG를 통해 평가됩니다.
2. **SWG** 커버리지 확인: URL 기반 차단이 필요한 경우 SWG 프록시 특정 소스 또는 네트워크의 데이터 경로에서 활성 상태인지 확인합니다. Secure Access에서 이 작업을 수행하려면 Cisco Secure Client, PAC 파일 또는 네트워크 터널 그룹을 사용하여 Secure Access 프록시 통해 인터넷 보안을 구성하고 트래픽을 라우팅합니다.

3. 규칙 감사: 특정 URL 경로를 사용하는 모든 차단 규칙을 식별합니다. 규칙 설정을 네트워크 아키텍처에 맞게 조정하면 예기치 않은 허용 동작을 방지하고 보안 규칙이 의도한 대로 시행될 수 있습니다.

SWG 시행을 설정하는 다양한 방법에 대해서는 Cisco Secure Access 도움말 가이드북에서 다음 항목을 참조하십시오.

- 로밍 디바이스에 대한 Cisco Secure Client 설정 구성.
- PAC 파일 관리.
- DNS 및 웹 보안 구성 (웹 보안 포트 80/443 트래픽만 활성화).
- 사이트, 브랜치 또는 네트워크 기반 트래픽의 네트워크 터널 그룹 관리.

추가 리소스는 다음을 참조하십시오.

- 인터넷 액세스 규칙 문제 해결.
- 맞춤형 URL에 대한 액세스 제어.
- 예.
- 대상 목록 관리.

# 제 4 장

:

- □□□ □□□□ □□

보안 액세스를 통해 조직의 트래픽을 리디렉션하는 방법을 설명합니다.

이 단계에서는 트래픽을 Secure Access로 리디렉션할 Umbrella ID를 선택합니다. 리디렉션 후에는 이러한 ID의 트래픽이 Secure Access를 통해서만 라우팅됩니다. Secure Access에서는 ID를 소스라고 합니다.

업그레이드 관리자가 활성화된 상태에서는, Secure Access에서 등록된 네트워크나 로밍 디바이스와 같은 새로운 소스를 직접 생성하더라도, Umbrella의 업그레이드 관리자로 돌아가서 3단계: 트래픽 리디렉션을 완료해야 합니다.

이는 업그레이드 관리자 기능 새 소스 및 기존 소스가 리디렉션될 때까지 Umbrella 계정에 연결된 상태를 유지하기 때문에 필요합니다.

Secure Access 대시보드로 완전히 전환하려면 다음 단계를 완료하십시오.

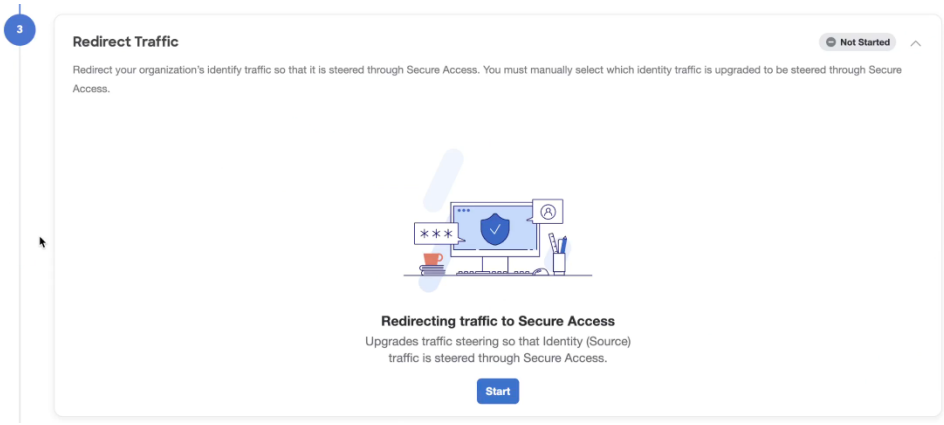
- 3단계: 트래픽 리디렉션 - Umbrella ID를 Secure Access 소스로 리디렉션합니다.
- 4단계: 업그레이드 완료 및 Umbrella 닫기 - Umbrella 계정을 비활성화하고 영구적으로 닫습니다.

## Secure Access Umbrella

Secure Access를 통해 조정을 시작하도록 Umbrella의 ID 트래픽을 리디렉션합니다.

이 단계에서는 Umbrella에서 Secure Access로 트래픽을 전환합니다. 업그레이드를 완료하고 Umbrella 계정을 닫을 때까지 언제든지 이 단계에서 트래픽을 되돌릴 수 있습니다. 원하는 경우 Umbrella에서 새 ID를 생성하여 Secure Access에서 기능을 테스트할 수도 있습니다.

1. **Redirect Traffic**(트래픽 리디렉션)에서 **Start**(시작)를 클릭합니다.

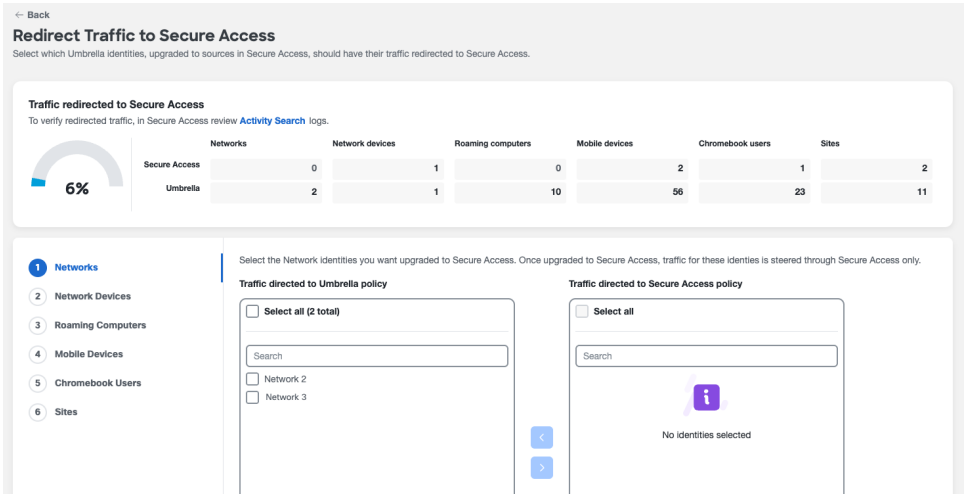



**Redirect Traffic to Secure Access**(**Secure Access**로 트래픽 리디렉션) 페이지에는 보안 액세스로 리디렉션할 수 있는 트래픽 및 다음 ID 유형이 표시됩니다.

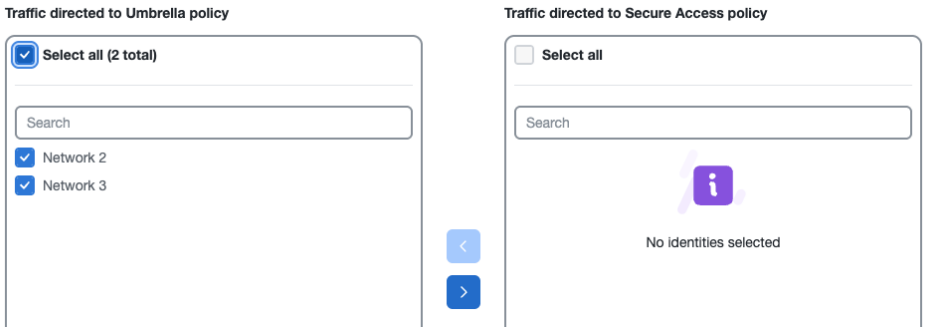
- 네트워크
- 네트워크 디바이스
- 로밍 컴퓨터
- 모바일 장치
- Chromebook 사용자
- 사이트

2. ID 유형을 클릭합니다.

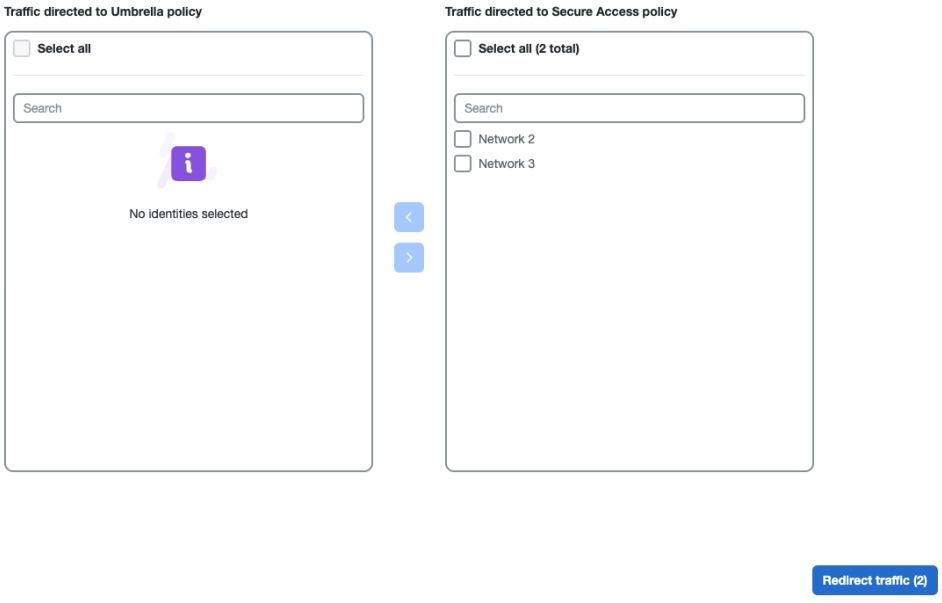
   해당 ID 유형의 사용 가능한 ID 목록이 **Umbrella**로 리디렉션된 트래픽 정책에 나타납니다.



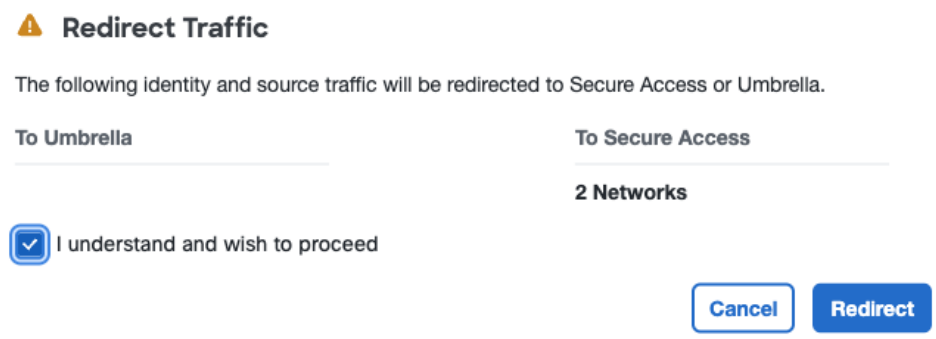

3. Secure Access로 트래픽 전송을 시작하려면 ID를 선택합니다.




4. 화살표를 클릭하여 선택한 ID를 **Secure Access** 정책으로 이동한 트래픽으로 이동합니다.

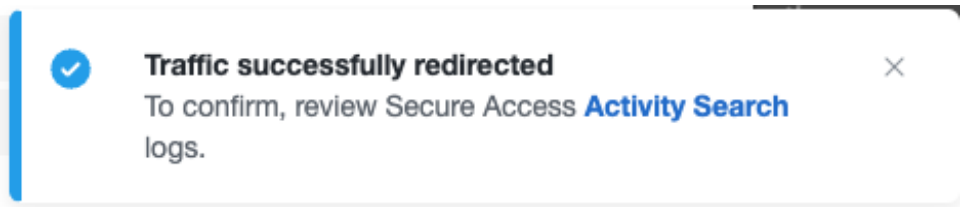



5. **Redirect Traffic(**트래픽 리디렉션**)**을 클릭합니다.
6. 다음 **ID** 및 소스 트래픽은 **Secure Access** 또는 **Umbrella**로 리디렉션됩니다**.** 팝업 메시지가 나타납니다.




7. 이해했으며, 계속하겠습니다.를 선택합니다.
8. **Redirect(**리디렉션**)**를 클릭합니다.

   인증이 완료되면 성공 모달인 **Traffic Successfully redirected(**트래픽이 성공적으로 리디렉션됨**)**가 표시됩니다.




---

Secure Access에서 활동 검색 보고서를 보고 소스 트래픽이 성공적으로 리디렉션되었는지 확인합니다. 왼쪽 탐색 메뉴에서 **Secure Access(**보안 액세스**) > Reports(**보고서**) > Activity Search(**활동 검색**)**를 클릭합니다. 자세한 내용은 활동 검색 보고서 보기 및 사용자 지정을 참조하십시오.

# 제 5 장

:


- Cisco Secure Access - DNS □□□ □ □□


Cisco Secure Access - DNS 방어로 업그레이드하여 전환하는 동안의 보고서에 대해 설명합니다.

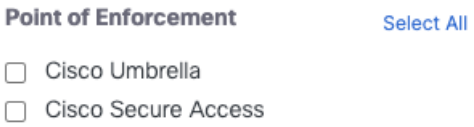
## Cisco Secure Access - DNS

모든 Umbrella 보고서는 Secure Access - DNS 방어에서 확인할 수 있습니다.

특정 기간에 대한 보고서를 생성할 수 있으며, 최대 범위는 지난 90일입니다.

자세한 내용은 보고서를 사용하여 Secure Access 모니터링을 참조하십시오.

Upgrade Manager가 실행되는 동안 보고서를 통해 시행 지점 필터를 통해 Secure Access 및 Umbrella 사용량을 모니터링할 수 있습니다. 시행 지점 필터를 사용하면 확인할 제품의 트래픽 경로를 선택할 수 있습니다.




중요사항

Umbrella를 영구적으로 종료하면 시행 지점 필터를 사용할 수 없습니다. 자세한 내용은 업그레이드 완료 및 Umbrella 닫기를 참조하십시오.

제

# 6 Umbrella

장

:

- Umbrella □□

업그레이드 프로세스를 완료하는 마지막 단계.

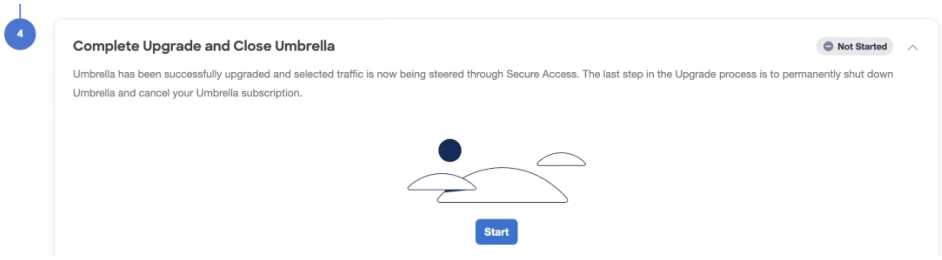
마지막 단계는 사전 요건을 완료하고 모든 정책 규칙을 업그레이드하고 모든 트래픽을 Secure Access로 리디렉션한 후 Umbrella 계정을 닫는 것입니다.

## Umbrella

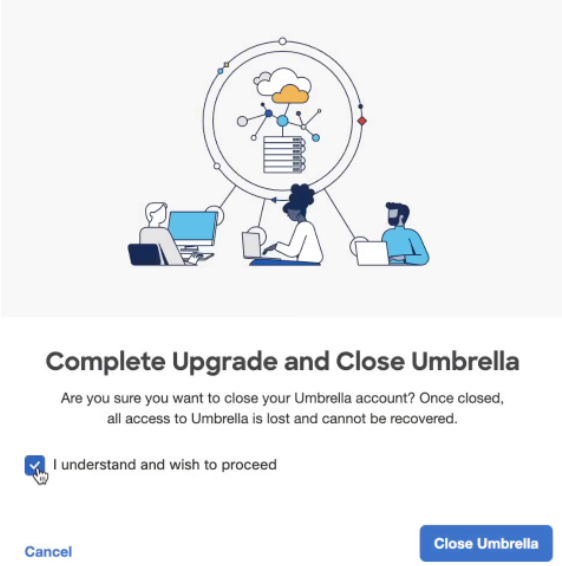
이 단계는 Umbrella를 종료하고 Umbrella 구독을 취소하기 위한 마지막 단계입니다.

Umbrella가 업그레이드되었으며 선택한 트래픽은 이제 Secure Access를 통해 조정됩니다. 업그레이드 관리자의 마지막 단계는 Umbrella를 영구적으로 종료하고 Umbrella 구독을 취소하는 것입니다.

1. **Start(**시작**)**를 클릭합니다.




2. 이해했으며**,** 계속하겠습니다**.**를 선택합니다.




3. **Close Umbrella(Umbrella** 닫기**)**를 클릭합니다.

   Umbrella 계정이 닫히고 조직은 보안 액세스 - DNS 방어를 통해 완전히 보호됩니다.

제

7

장

:

- □□□□□ □□□ □□ □□

Cisco Umbrella DNS에서 Cisco Secure Access - DNS 방어로 업그레이드할 때의 문제 해결 팁.

다음 주제에서는 업그레이드할 때 문제 해결해야 하는 가능한 시나리오에 대해 설명합니다.

업그레이드 중에 문제가 발생하는 경우 이 항목의 시나리오를 검토하십시오.

| 문제 | 해결책 |
| --- | --- |
| SCC(Security Cloud Control)의 구독 클레임 코드를 받지 못한 경우 어떻게 해야 합니까? | ● 스팸 편지함을 확인합니다.<br>● 사용자는 구매 시점의 계정에 연결된 관리자가 아닐 수 있습니다. 자세한 내용은 세일즈 담당자에게 문의하여 주십시오. |
| 2단계 **Start Upgrade**(업그레이드 시작)에 **Upgrade Failed**(업그레이드 실패)가 표시되면 어떻게 됩니까? | 업그레이드 프로세스 중에 다른 관리자가 정책을 편집하거나 추가하려고 하면 정책 변환이 실패할 수 있습니다. 업그레이드의 2단계를 다시 시도하기 전에 웹 브라우저 새로 고치거나 정책을 삭제해 보십시오. |
| 조직 이름을 변경할 수 있습니까? | ● Security Cloud Control에서 조직 이름을 변경하려면 왼쪽 열에서 해당 조직을 선택한 다음 > Platform management(플랫폼 관리) > Product Subscriptions(제품 구독) > Subscriptions(구독) > 연필 아이콘을 클릭하여 편집한 후 > Save(저장)를 클릭하면 됩니다.<br>● SCC에서 조직 이름을 변경해도 Secure Access에서는 이름이 변경되지 않습니다. 변경을 요청하려면 Secure Access 지원팀에 문의하십시오. |
| Umbrella 관리자는 Umbrella 대시보드에서 잠깁니다. | 고유한 Security Cloud Control 계정을 생성하려면 Umbrella 관리자에게 초대장을 보내야 합니다. 이제 인증이 Security Cloud Control을 통해 이루어집니다. 사용자 초대를 참조하십시오. |
| **Request Invitation**(초대 요청)을 클릭하여 Secure Access로 업그레이드했지만 제가 구독 클레임 코드가 포함된 초기 Security Cloud Control 이메일을 받은 관리자가 아닌 경우에는 어떻게 해야 합니까? | 최초 Security Cloud Control 이메일을 받은 관리자가 계정을 생성하고 귀하를 새 사용자로 추가하며, 사용자는 SCC에 구독 클레임 코드를 입력하여 보안 액세스 업그레이드를 활성화합니다. |
| 기존 Secure Access 인스턴스에 연결하는 대신 실수로 새 Secure Access 인스턴스를 생성한 경우 어떻게 해야 합니까? | Secure Access 지원에 문의 |
| 구독 클레임 코드를 잘못된 Umbrella 조직에 연결한 경우 어떻게 됩니까? | Secure Access 지원에 문의 |
| 기술적인 문제가 있는 경우 누구에게 문의해야 합니까? | Secure Access 지원에 문의 |

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.