보안 이메일 위협 방어: 다단계 인증 및 액세스 제어

목차

소개

이 문서에서는 Cisco ETD(Email Threat Defense)에서 관리 콘솔에 대한 관리자 액세스를 제어하는 기능을 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Duo를 사용하여 ETD 인증을 구성하려면 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco ETD 서브스크립션
- Cisco SCC(Security Cloud Control) 액세스
- 보안 강화를 위한 인증 솔루션(이 경우 Cisco Duo)입니다.

사용되는 구성 요소

이 문서는 Email Treat Defense 및 Secure Cloud Control로 제한됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 Cisco ETD가 Cisco SCC를 활용하고 Cisco Duo와 통합되어 보안 인증 및 세분화된 액세스 제어를 제공하는 방법에 대해 중점적으로 설명합니다.

최신 클라우드 기반 솔루션에서 액세스 제어는 데이터 보안, 규정 준수 및 운영 무결성을 보장하는 데 가장 중요한 구성 요소 중 하나입니다. 무단 액세스 - 특히 관리자 계정에 대한 액세스는 시스템 손상, 데이터 유출, 서비스 중단과 같은 심각한 결과를 초래할 수 있습니다.

Cisco는 Cisco ETD와 같은 서비스의 필수적인 부분인 MFA(Multifactor Authentication) 기술을 비롯한 클라우드 포트폴리오 전반에 걸쳐 강력한 보안 기능을 제공합니다. MFA는 기존 비밀번호 외에 중요한 확인 단계를 추가하여 사용자가 모바일 애플리케이션 승인, 보안 토큰 또는 생체 인식 확인과 같은 추가 요소를 통해 인증하도록 요구합니다.

관리자 인증 프로세스를 간소화하고 강화하기 위해 ETD는 중앙 집중식 인증 및 정책 관리 서비스인 Cisco SCC를 활용합니다.

ETD는 SCC를 통해 다음과 같은 다양한 보안 기능에 액세스할 수 있습니다.

- 자격 증명 도난 위험을 완화하기 위한 MFA 시행.
- Cisco Duo, Microsoft Entra ID, Okta 등과 같은 타사 ID 공급자와 통합하여 유연한 인증 워크플로 및 엔터프라이즈 ID 연합을 지원합니다.
- 중앙 집중화된 정책 관리를 통해 Cisco 클라우드 서비스 전반에 걸쳐 일관된 액세스 규칙 제공

특히 Cisco Duo는 고급 정책 기반 액세스 관리를 추가하여 이러한 기능을 확장합니다. ETD는 SCC를 통합 채널로 사용하여 소스 IP 제한, 디바이스 상태 확인, 사용자 그룹 기반 규칙 등 Duo의 세분화된 제어를 관리자 액세스에 직접 적용할 수 있습니다.

예를 들어, 조직은 신뢰할 수 있는 특정 네트워크 범위에서만 액세스를 허용하는 정책을 정의할 수 있습니다. 승인된 IP 목록 이외의 모든 연결 시도는 첨부된 다이어그램에 표시된 것처럼 자동으로 차단될 수 있습니다. 이러한 MFA + 컨텍스트 정책의 조합을 통해 심층 방어 접근 방식을 사용할 수 있으므로, 자격 증명이 손상되더라도 추가 보안 기준을 충족하지 않는 한 공격자가 시스템에 액세스하지 못하도록 할 수 있습니다.

Cisco ETD, Cisco SCC 및 Cisco Duo를 통합함으로써 기업은 안전하고 확장 가능하며 사용자 친화적인 액세스 제어 모델을 구현하여 업계 모범 사례에 부합하면서 중요한 클라우드 서비스에 대한 보호를 강화할 수 있습니다.

시나리오

관리 액세스를 보호하기 위해 ETD를 사용하여 여러 인증 및 액세스 제어 시나리오를 구현할 수 있습니다.

1. 내장형 MFA - Cisco의 내장형 MFA를 사용하거나 Microsoft MFA를 통합합니다.

2. Cisco SCC with Cisco Duo - Cisco SCC의 중앙 집중식 인증과 Duo의 고급 MFA 기능을 결합합니다.

3. 외부 ID 공급자(예: Microsoft Entra ID)가 있는 Cisco SCC - 엔터프라이즈 ID 솔루션과 통합하

여 인증 정책을 확장합니다.

이 문서에서는 시나리오 2의 컨피그레이션 단계에 대해 설명합니다. Cisco Duo가 포함된 Cisco SCC(다른 기술에 맞게 프로세스를 조정할 수 있음)

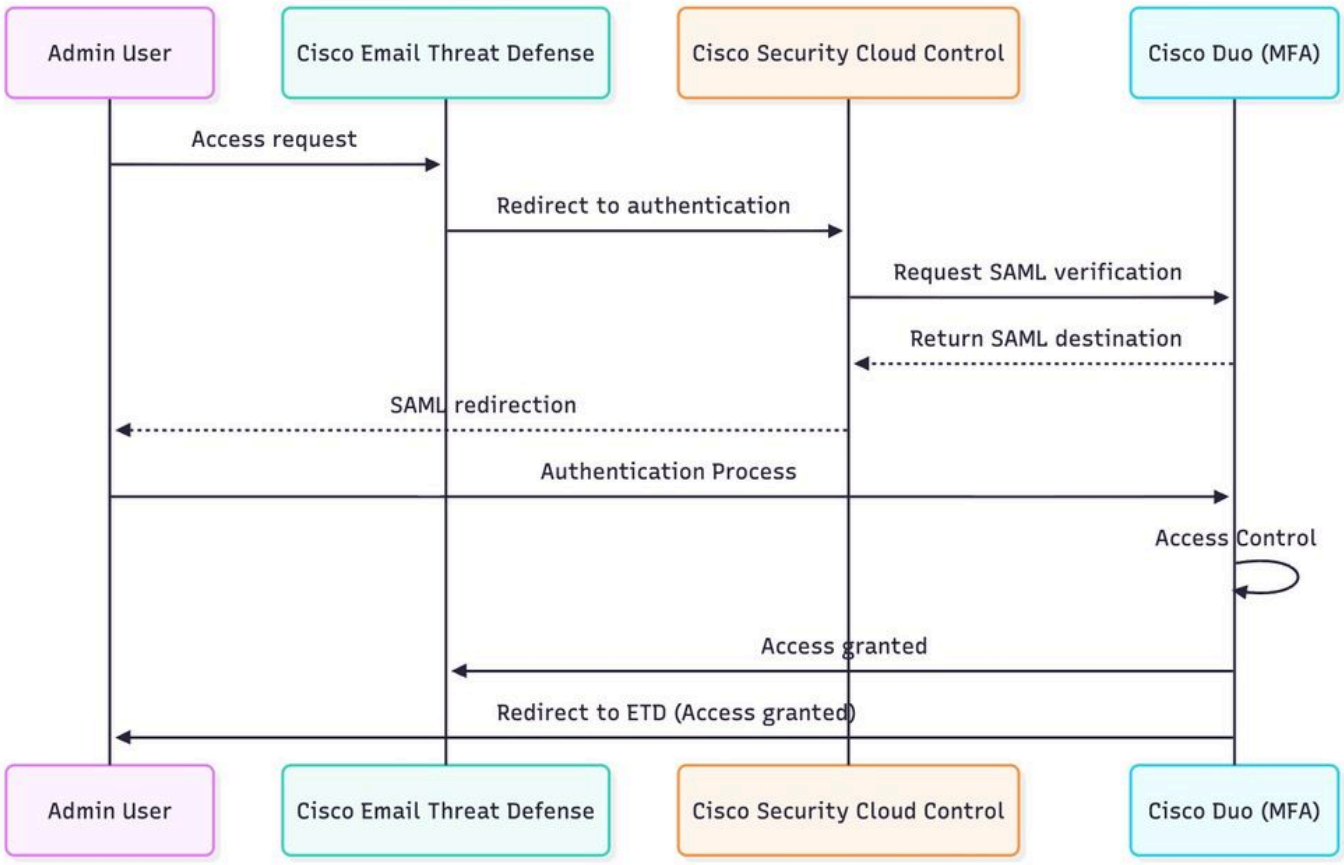
참고: 이 문서에서는 Cisco Duo의 다단계 인증 기능을 사용하여 ETD(Email Threat Defense)에서 액세스 제어를 활성화하는 데 필요한 기본 단계를 개략적으로 설명합니다. Duo 통합을 구현하면 인증된 사용자만 플랫폼에 액세스할 수 있도록 하여 보안을 강화할 수 있습니다. 포괄적인 지침, 컨피그레이션 옵션 및 고급 구축 시나리오에 대해서는 공식 제품 설명서를 참조하십시오.

- 중앙 집중식 보안 정책 및 액세스 관리.

Cisco Duo- 다단계 인증 설정 및 모범 사례에 대한 자세한 지침을 제공합니다.

Cisco SCC 컨피그레이션

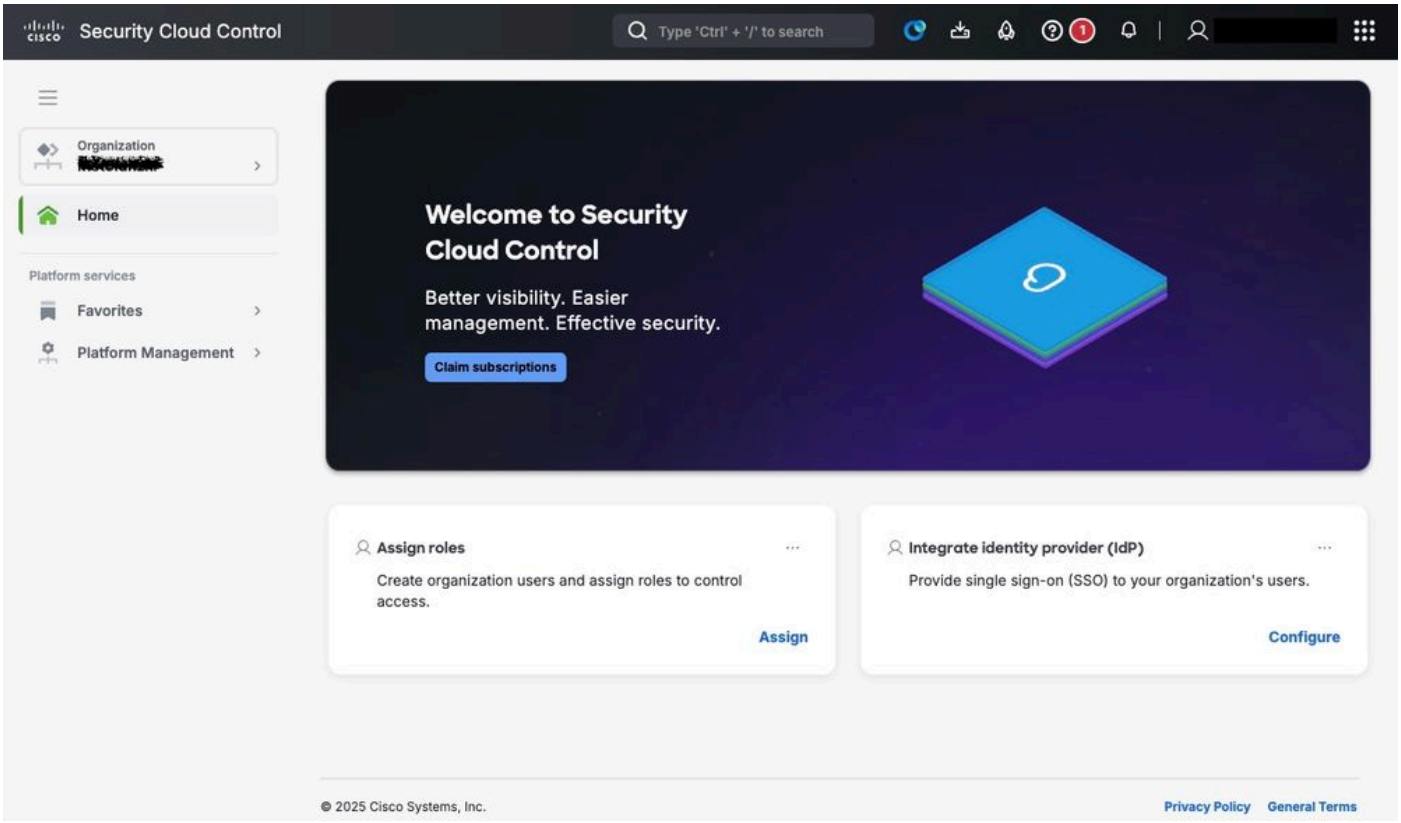
Cisco ETD를 Cisco Duo와 통합하기 위해 첫 번째 단계는 Cisco SCC에서 인증 도메인을 구성하는 것입니다. 이렇게 하면 Cisco SCC가 외부 ID 및 MFA 제공자와 작동할 수 있는 신뢰 관계가 설정됩니다.



다이어그램

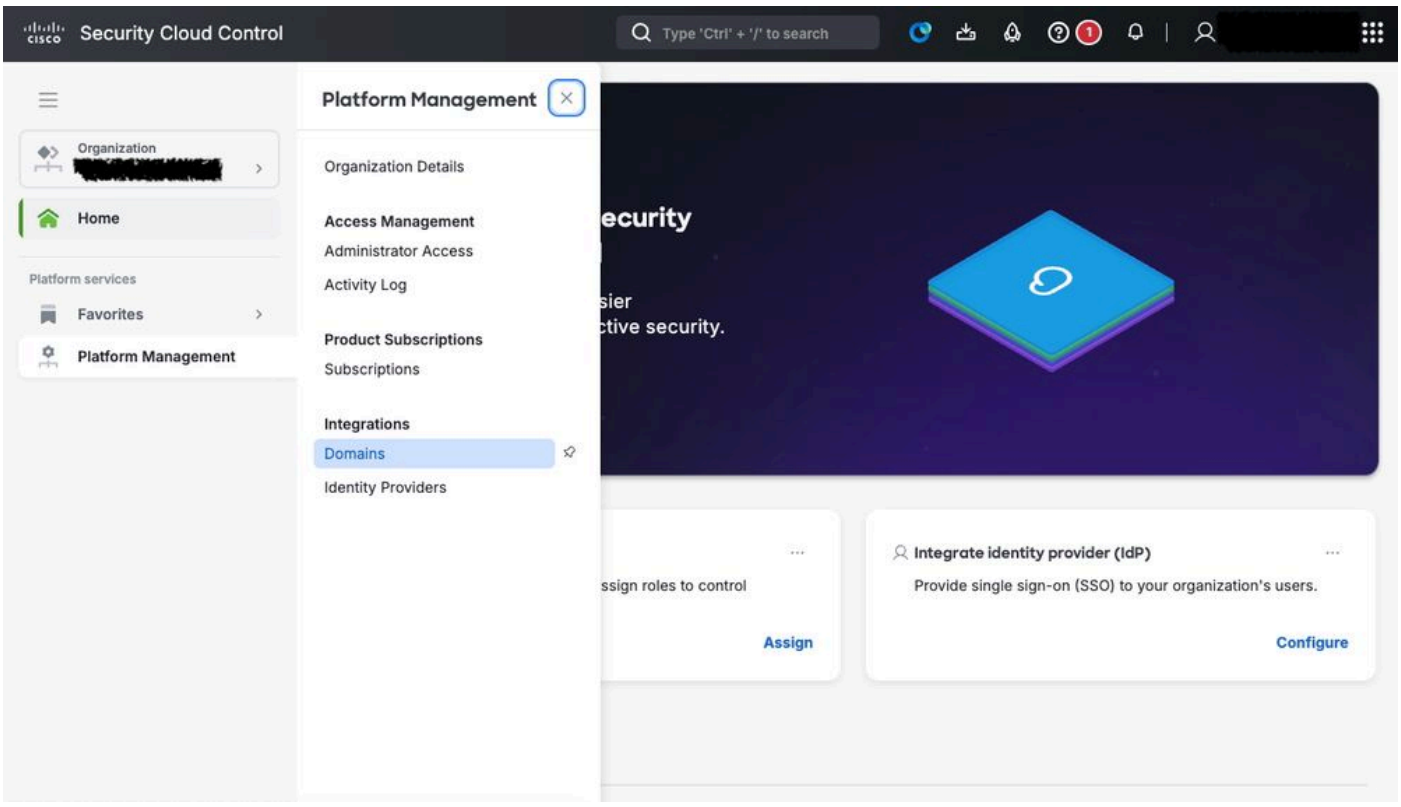
1단계. Cisco SCC 콘솔에 액세스합니다.

Cisco SCC 포털 https://security.cisco.com/에 로그인합니다.



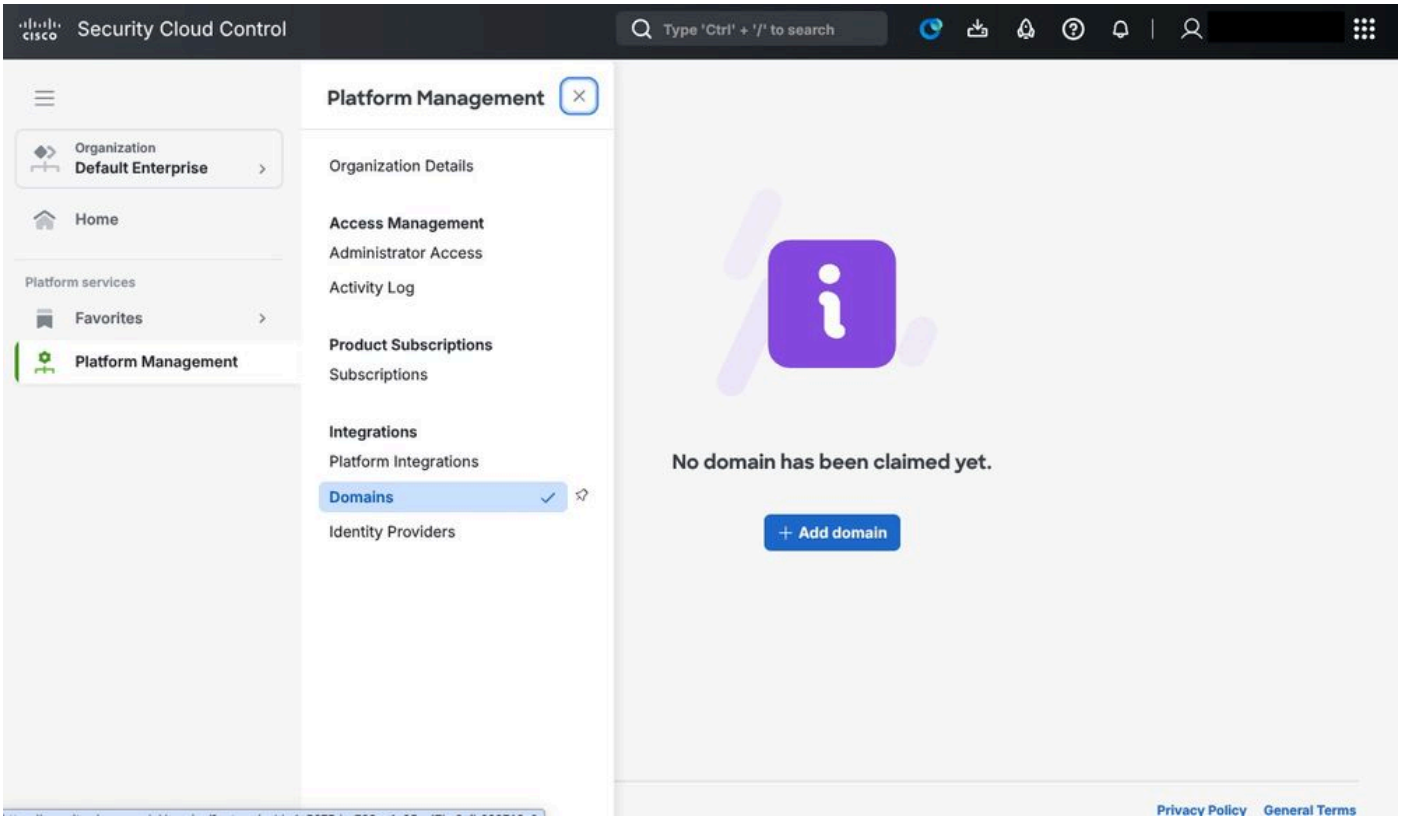
2단계. Domain Management(도메인 관리)로 이동합니다.

주 메뉴에서 Platform Management(플랫폼 관리) > Domains(도메인)로 이동합니다.



3단계. 새 도메인을 추가합니다.

인증 도메인 등록 프로세스를 시작하려면 Add Domain을 클릭합니다.

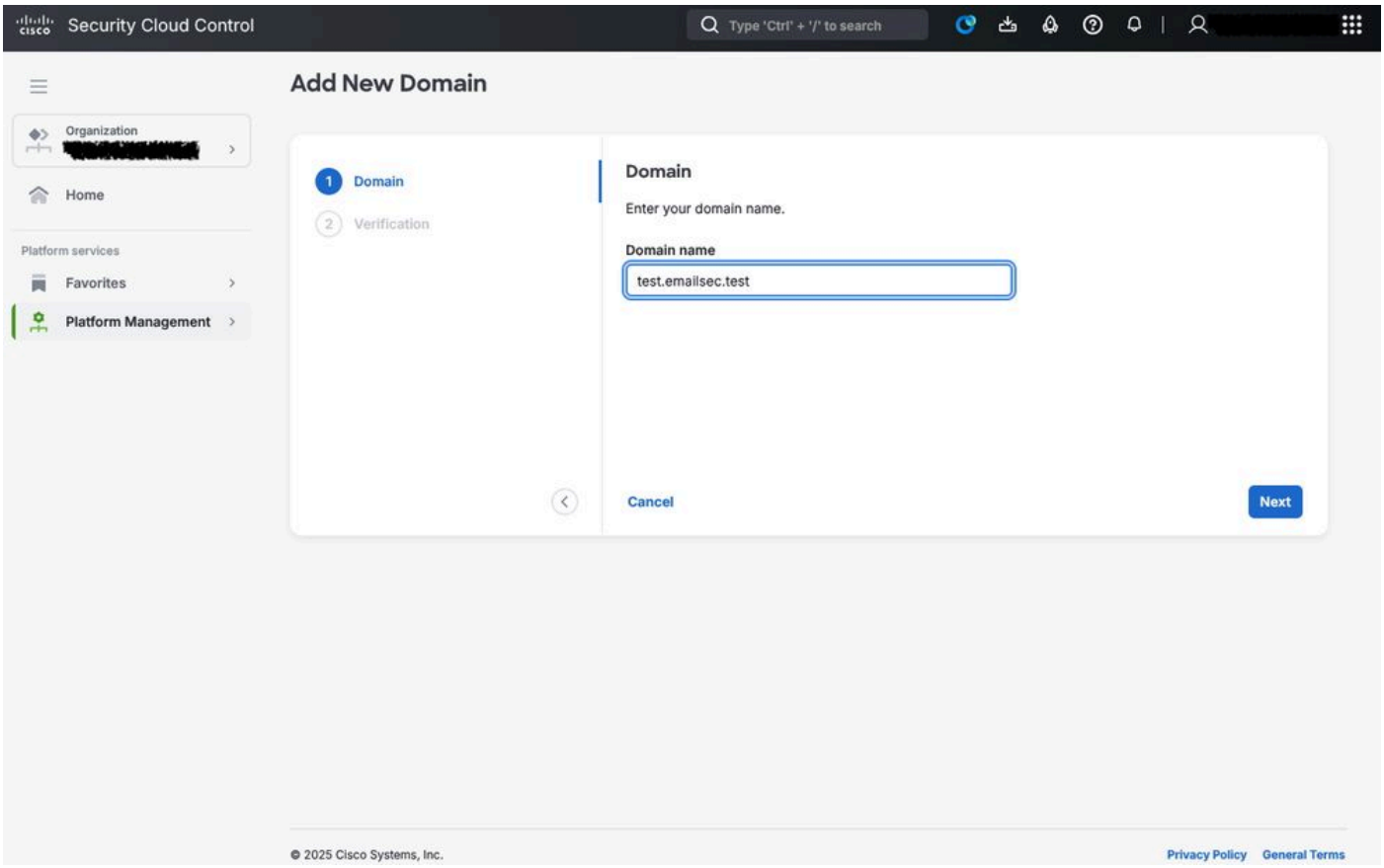


보안 클라우드 제어: 도메인

4단계. 도메인 정보를 제공합니다.

인증에 사용되는 도메인에 대한 세부 정보가 포함된 양식을 작성합니다. 여기에는 일반적으로 다음이 포함됩니다.

- 도메인 이름(예: test.emailsec.test)
- 연락처 정보(관리 및 기술)
- 선택한 ID 제공자에 따라 인증 매개변수

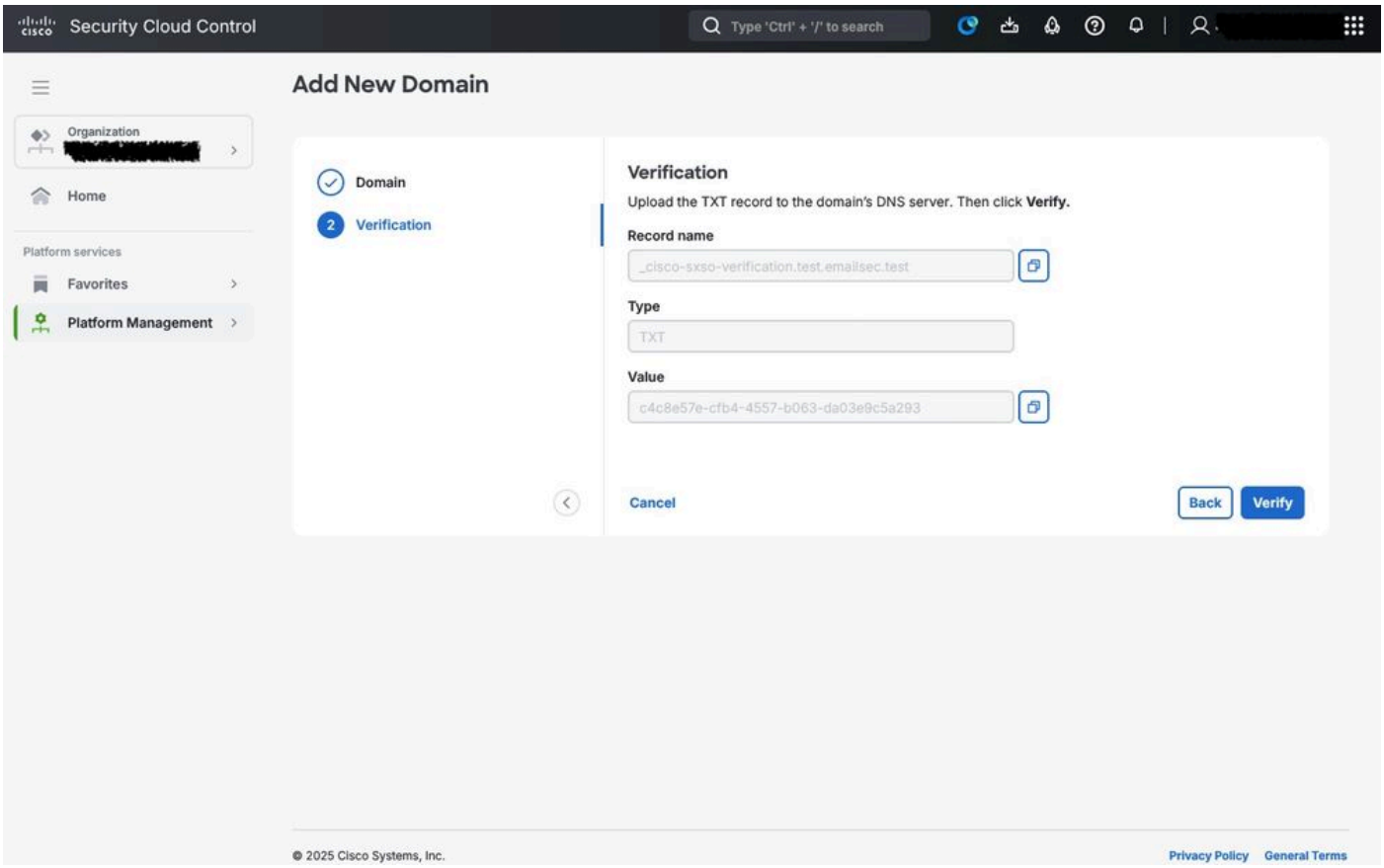


5단계. DNS를 통한 도메인 확인

도메인이 등록되면 Cisco는 소유권 증명을 필요로 합니다.

- CSCC에서 확인 레코드를 제공합니다.
- 이 레코드는 도메인의 DNS 컨피그레이션에 추가해야 합니다(일반적으로 TXT 레코드)
- Cisco Secure Cloud는 DNS 항목을 자동으로 검증하여 도메인이 조직에 속해 있는지 확인합니다

⚠ 주의: 통합을 진행하려면 먼저 확인 프로세스를 성공적으로 완료해야 합니다. DNS 전파에 따라 검증에는 몇 분에서 몇 시간이 소요됩니다.



Cisco SCC를 사용하여 ETD를 Cisco Duo와 연결

관리자의 도메인이 성공적으로 구성되면(더 엄격한 액세스 제어 적용 및 권한 관리의 기반이 됨), 다음 단계는 계약된 MFA 서비스를 통합하는 것입니다.

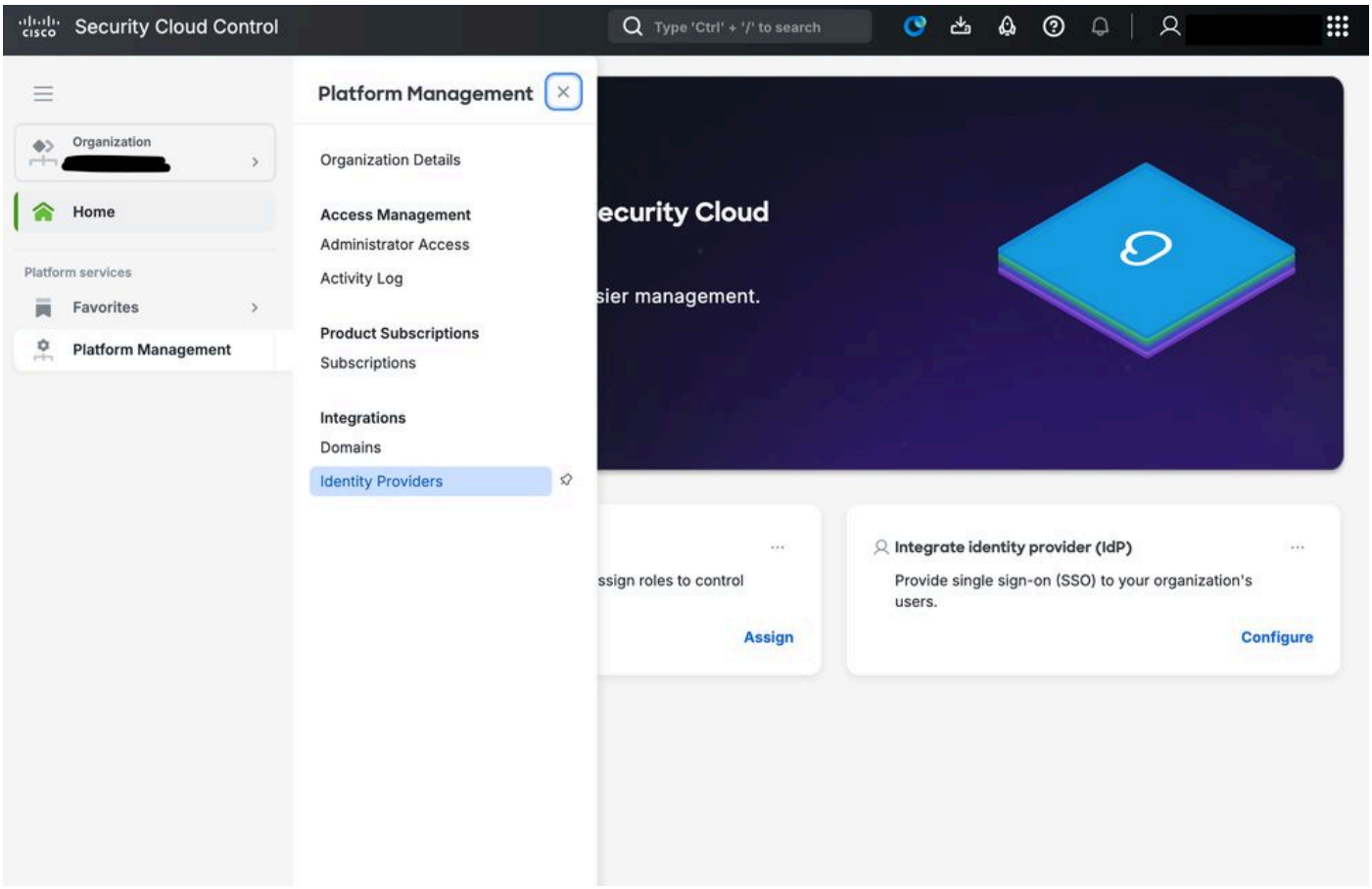
이 시나리오에서 Cisco Duo는 액세스 제어, 보안 로그인 및 MFA 확인을 위한 기본 솔루션으로 구현됩니다. 이러한 통합은 관리자가 여러 확인 단계를 통해 ID를 인증하도록 함으로써 환경의 보안 상태를 개선하고 무단 액세스의 위험을 줄이며 조직의 보안 정책을 준수하도록 합니다.

Cisco Duo 및 Cisco Cloud Control 통합

1단계. Cisco SCC Console 액세스

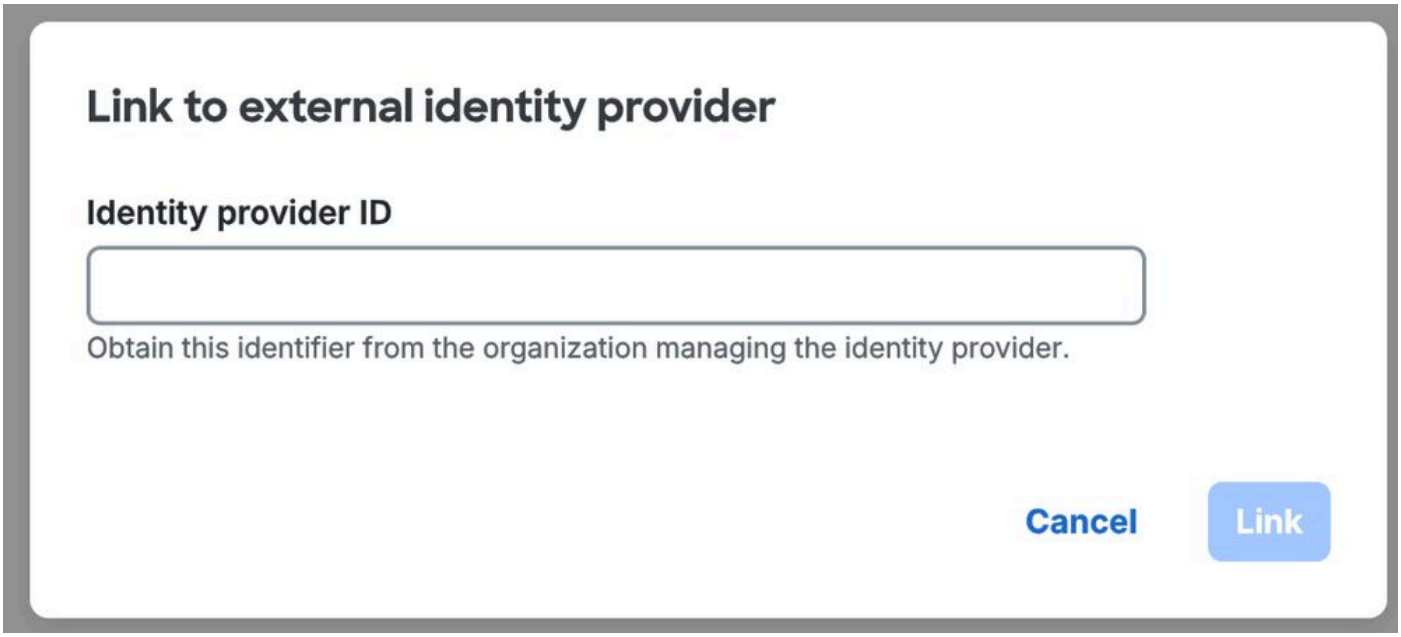
Cisco Security Cloud Control 포털 https://security.cisco.com/에 로그인합니다.

Platform Management(플랫폼 관리)로 이동하고 Identity Providers(ID 제공자)를 클릭합니다.



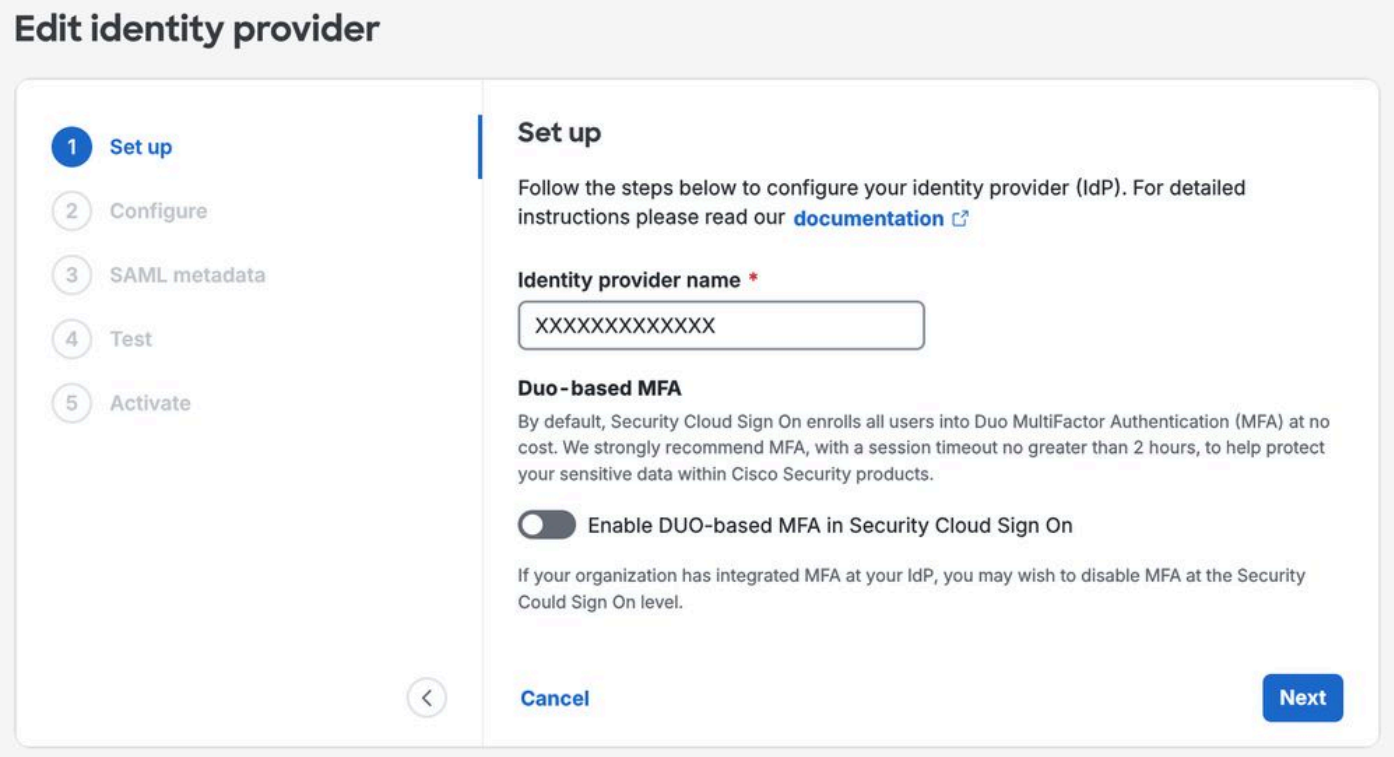
SCC IDP 컨피그레이션

ID 제공자를 식별하기 위해 사용자 지정 이름을 사용합니다.



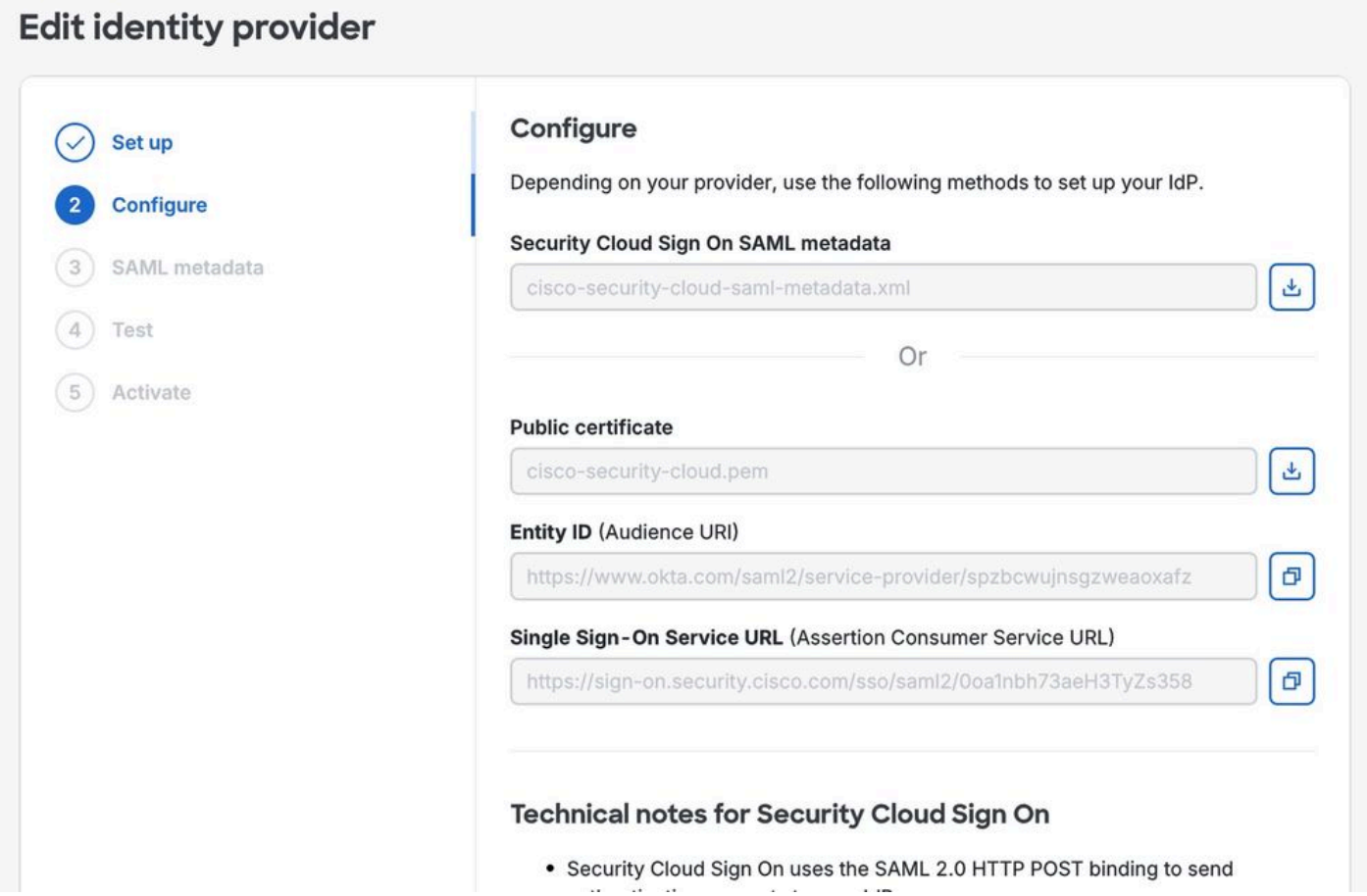
이제 설치가 시작됩니다. 이제 Cisco SCC 및 Cisco Duo에 액세스할 수 있습니다.

2단계. SCC에서 그림과 같이 Enable DUO-based MFA in Security Cloud Sing On(보안 클라우드에서 DUO 기반 MFA 활성화)을 비활성화하고 Next(다음)를 클릭합니다.

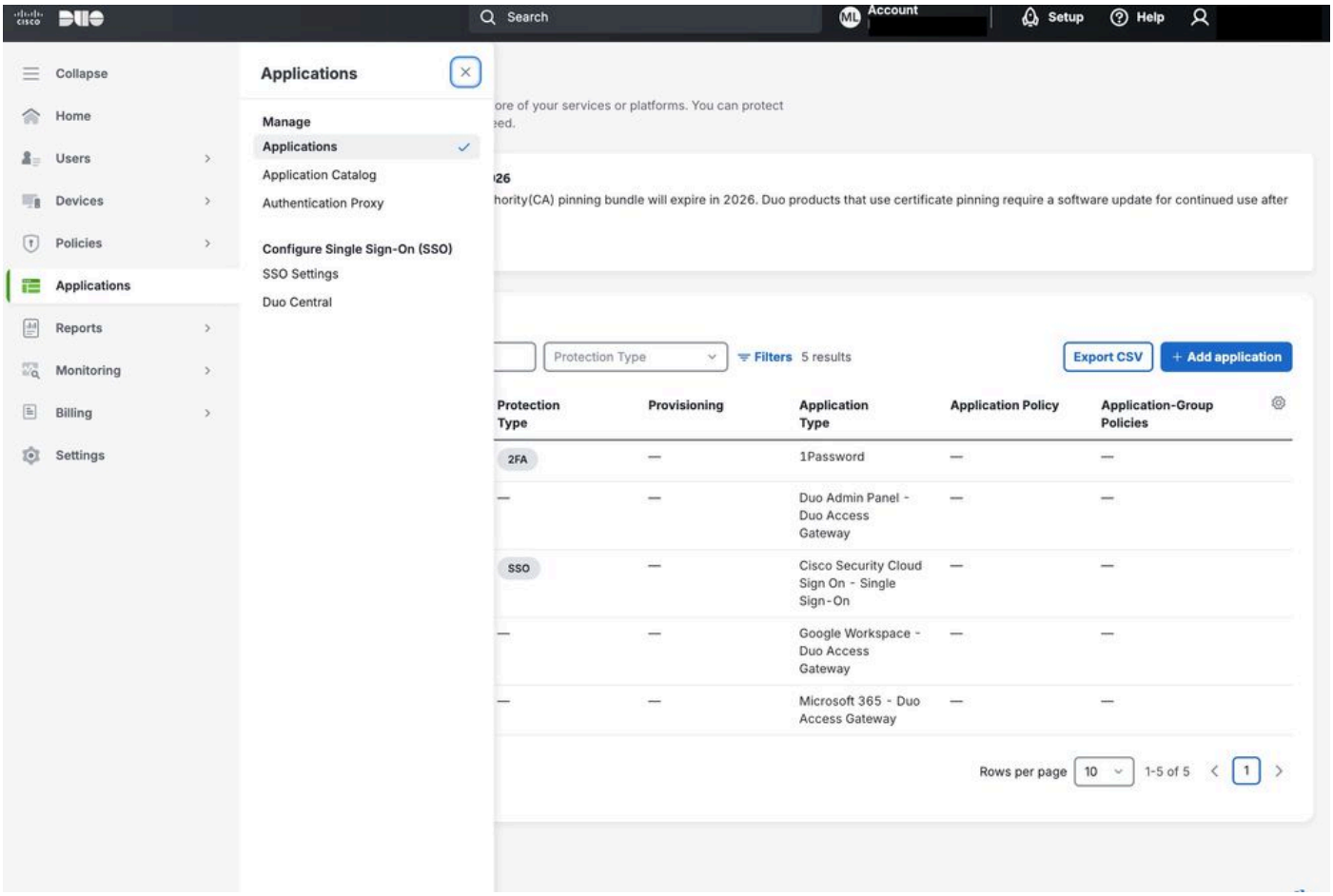


ID 공급자 컨피그레이션

3단계. 관련 데이터가 생성되고 이는 Cisco Duo 컨피그레이션 중에 사용됩니다.
모든 필수 값 및 관련 데이터를 복사하고 안전한 위치에 저장해야 합니다.
이러한 세부 정보는 향후 통합 단계에서 반드시 필요하므로, 권한이 있는 담당자에게만 액세스하고 조직의 보안 정책에 따라 보호되도록 해야 합니다.

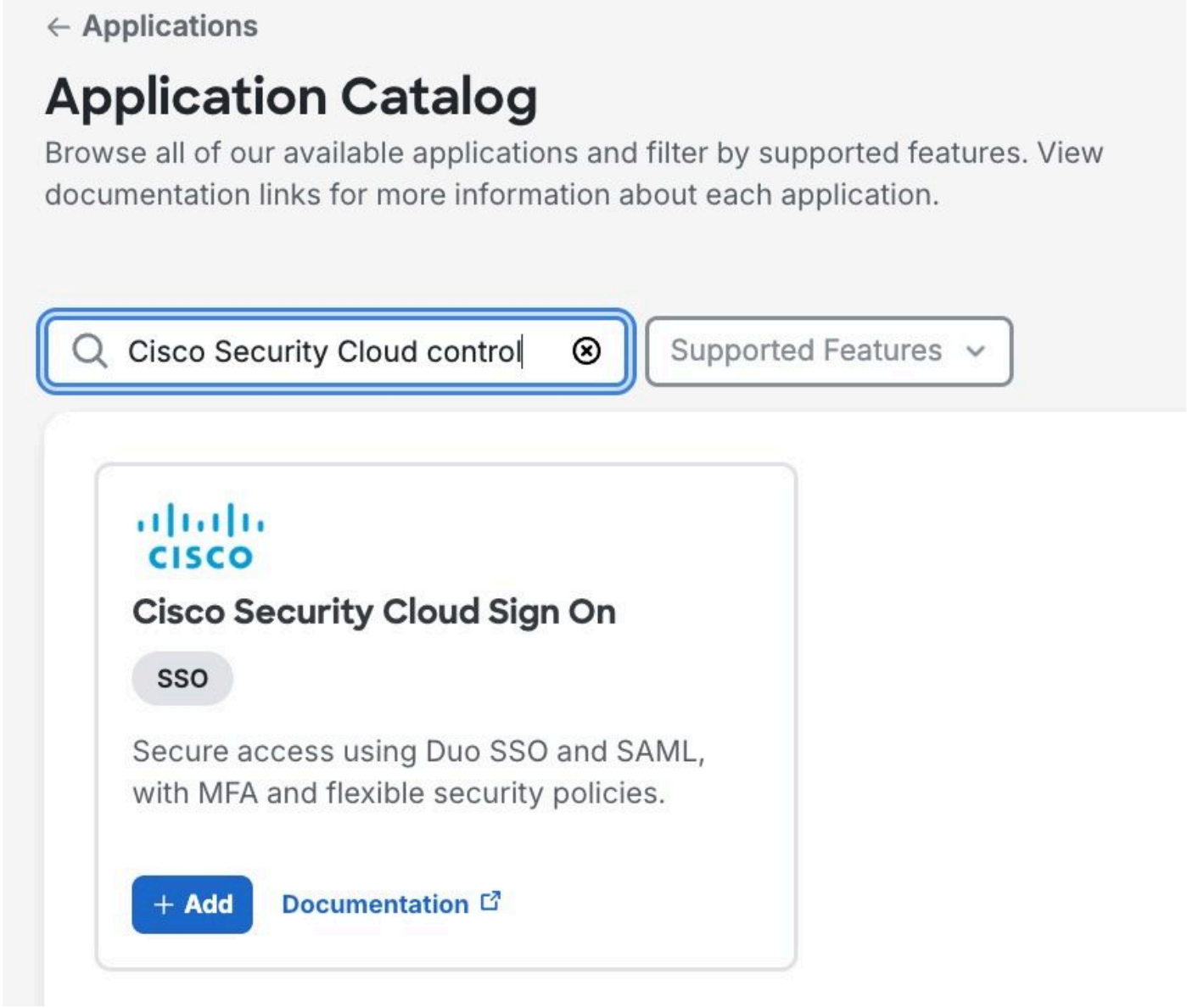


4단계. Cisco Duo를 열고 Applications(애플리케이션) 섹션으로 이동한 후 Add application(애플리케이션 추가)을 클릭합니다.



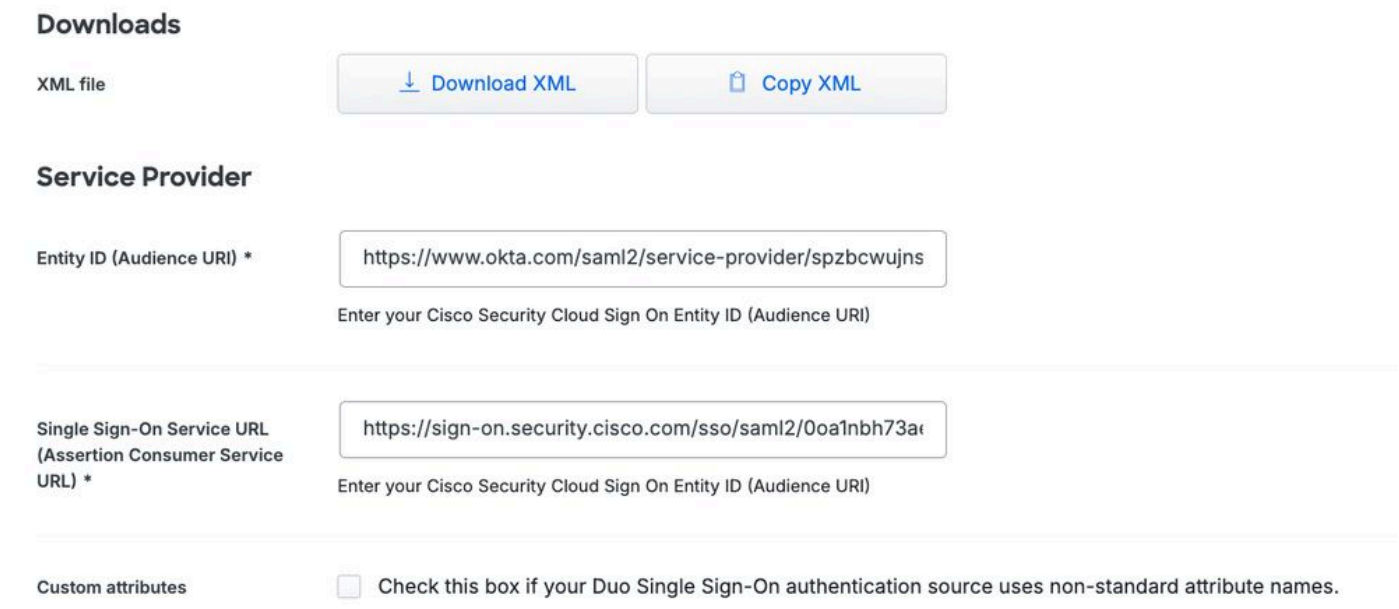
Cisco DUO 애플리케이션

메뉴에서 Cisco Security Cloud를 검색하고 Add(추가)를 클릭하여 통합을 시작합니다.

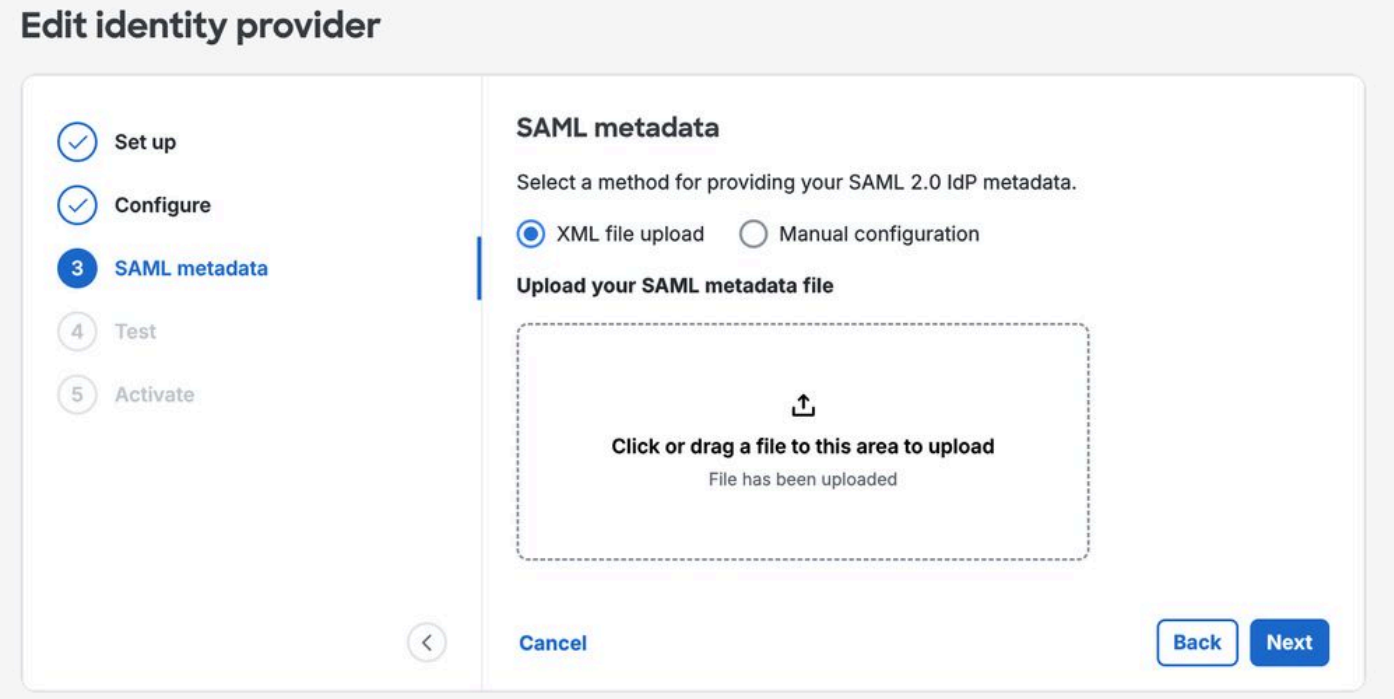


5단계. Cisco Duo 애플리케이션에서 관련 정보를 구성합니다.

Cisco SCC에서 Cisco Duo로 엔터티 ID 및 단일 로그인 서비스 URL을 복사합니다.



6단계. XML을 다운로드하고 파일을 Cisco SCC에 업로드합니다.



참고: Cisco Duo 콘솔에서 애플리케이션에 구성할 수 있는 나머지 매개변수는 특정 요구 사항에 따라 조정해야 합니다. 이러한 각 설정에 대한 자세한 설명은 공식 Cisco Duo 문서에서 확인할 수 있습니다. 구성 가능한 매개변수의 예로는 할당된 애플리케이션 이름, 정책이 적용되는 사용자 집합, 조직의 요구 사항을 충족하기 위해 보안 제어를 맞춤화할 수 있는 기타 사용자 지정 옵션 등이 있습니다.

Cisco ETD용 Cisco Duo의 정책 컨피그레이션

이 단계에서는 모든 구성 요소가 연결되며, 다음 단계는 Cisco ETD 콘솔 내에서 관리자의 인증 프로세스에 적용되는 정책을 구성하는 것입니다.

이 예에서는 특히 IP 주소를 기반으로 한 액세스 제어에 중점을 둡니다. 그러나 Cisco Duo는 다른 많은 액세스 제어 옵션을 제공합니다.

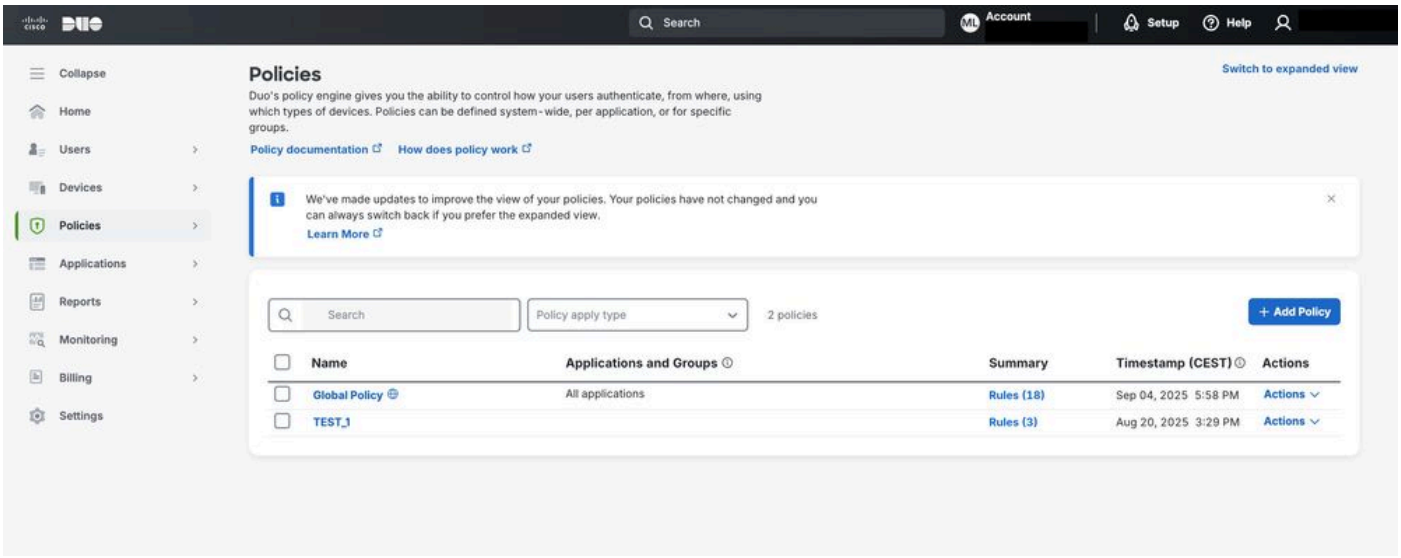
새 정책을 생성하고 애플리케이션에 할당하여 원하는 인증 규칙을 적용하고 관리자 로그인에 대한 보안 제한을 활성화할 수 있습니다.

Cisco Duo에서 사용 가능한 모든 제어 및 컨피그레이션 옵션에 대한 자세한 내용은 공식 Cisco Duo 설명서를 참조하십시오.

이 리소스는 보안 정책을 최적화하는 데 도움이 되도록 설정, 사용자 지정 및 모범 사례에 대한 포괄적인 지침을 제공합니다.

Cisco Duo의 Policies(정책) 섹션으로 이동하면 Cisco Duo를 통해 정책을 생성하고 Cisco ETD 연결에 할당할 수 있습니다.

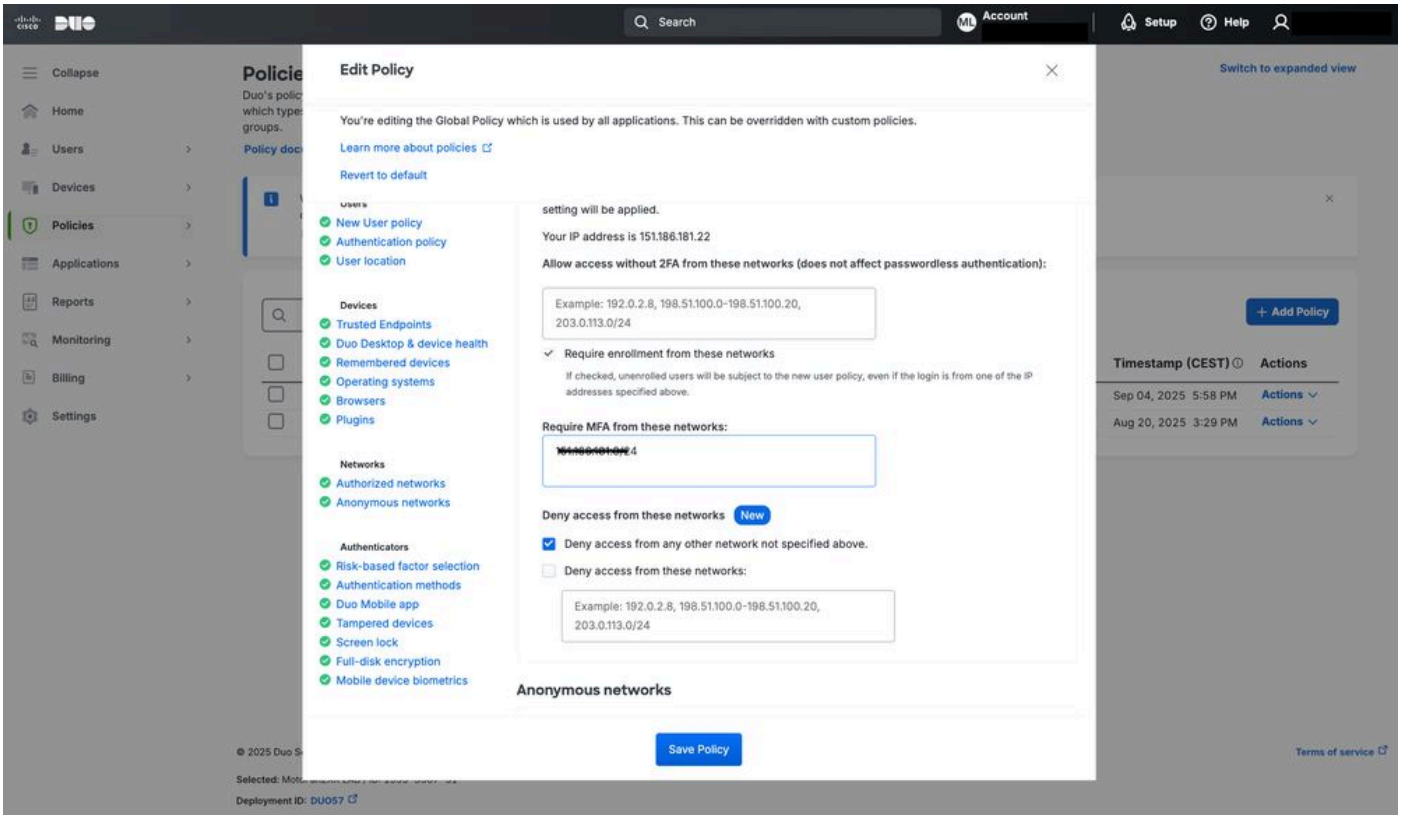
이 정책은 액세스 요구 사항에 따라 사용자 또는 그룹별로 적용할 수 있습니다.



Cisco 듀오

이 예에서는 이미지에 표시된 대로 Authorized Networks(인증된 네트워크) 섹션을 구성하여 소스 IP 액세스 제어가 활성화됩니다.

이 컨피그레이션은 지정된 신뢰할 수 있는 IP 범위에서만 액세스를 허용하여 Cisco ETD의 보안을 강화합니다.



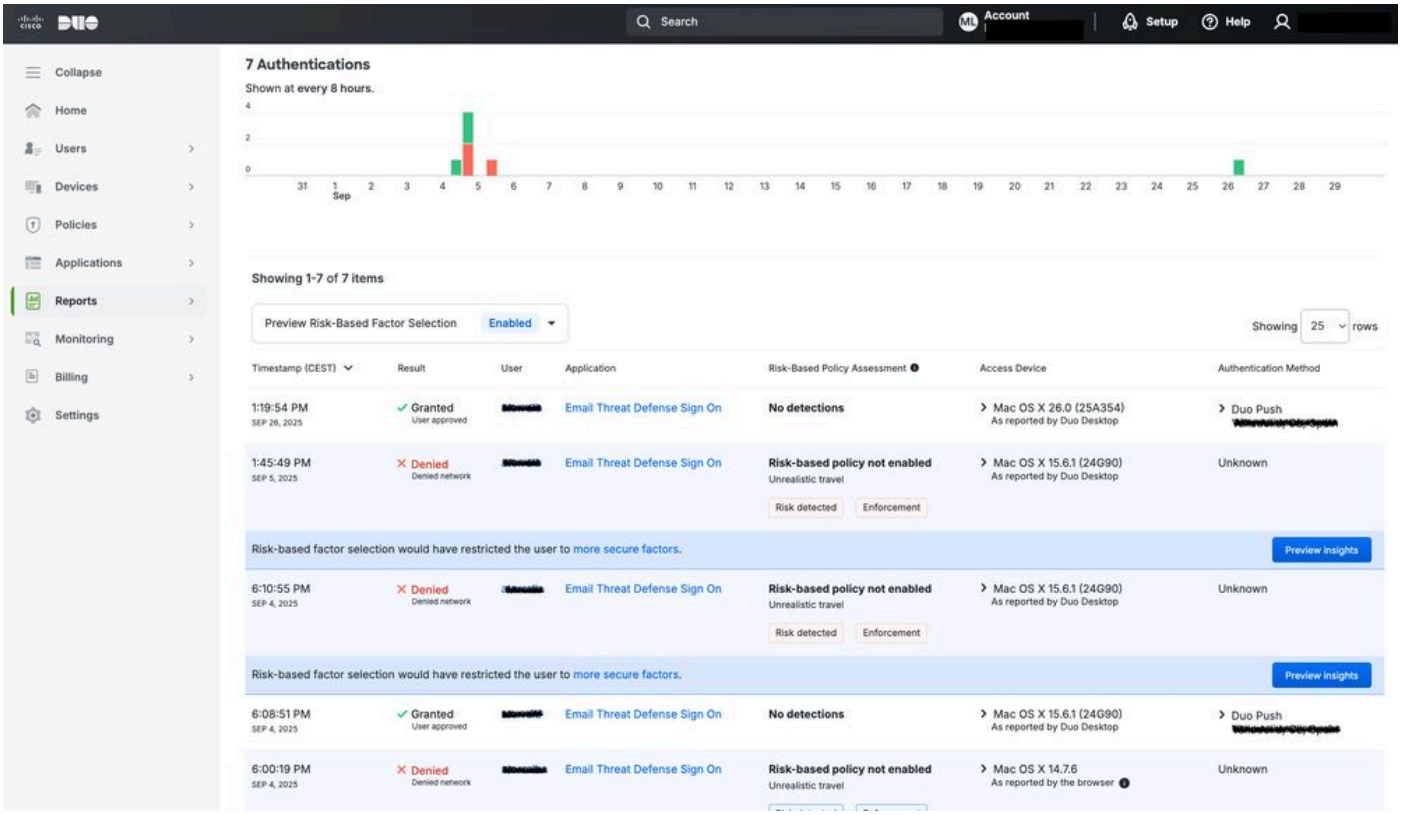
Cisco Duo 정책 컨피그레이션

결론

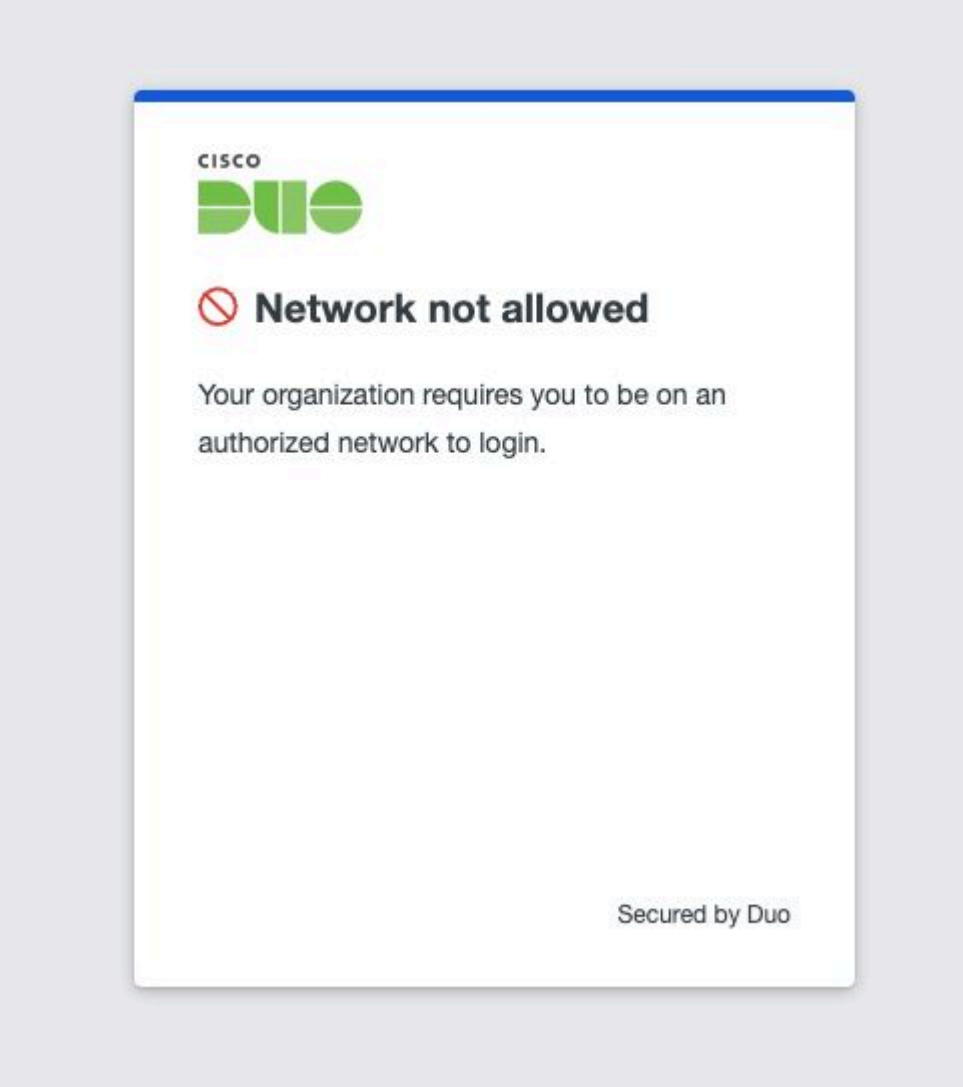
Cisco ETD는 MFA 및 ID 제공자와의 통합을 통해 관리자 액세스를 보호할 수 있는 유연한 옵션을 제공합니다.
Cisco SCC를 Cisco Duo와 결합함으로써 조직은 더 강력한 인증 정책을 구현하고, 무단 액세스의 위험을 줄이며, 안전한 클라우드 서비스 관리를 위한 업계 모범 사례에 부합할 수 있습니다.

MFA 외에도 관리자는 Cisco Duo의 정책 기반 제어를 활용하여 소스 IP 주소와 같은 특정 기준에 따라 액세스를 제한할 수 있습니다. 예를 들어, 다음 그림에서 볼 수 있듯이, 권한 있는 범위를 벗어난 IP 주소에서의 액세스 시도는 시스템에 의해 자동으로 차단됩니다. 이렇게 하면 신뢰할 수 있는 네트워크에서 시작된 요청만 허용되므로 잠재적인 공격에 대한 추가 보호 계층이 추가됩니다.

MFA와 함께 IP 기반 액세스 제어를 구현함으로써 조직은 심층 방어 접근 방식을 구현합니다. 즉, 클라우드에서 중요한 관리 인터페이스를 보호하기 위해 ID 검증과 네트워크 위치 검증을 결합합니다.



Cisco Duo 보고서



네트워크 제어 결과

경고: 이 변경 사항은 동일한 인증 도메인을 사용하는 모든 애플리케이션에 영향을 미친다는 것을 이해하는 것이 중요합니다. ETD뿐 아니라 Cisco Secure Access Console에 액세스하는 등 동일한 인증 프로세스를 사용하는 다른 제품도 포함됩니다.

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.