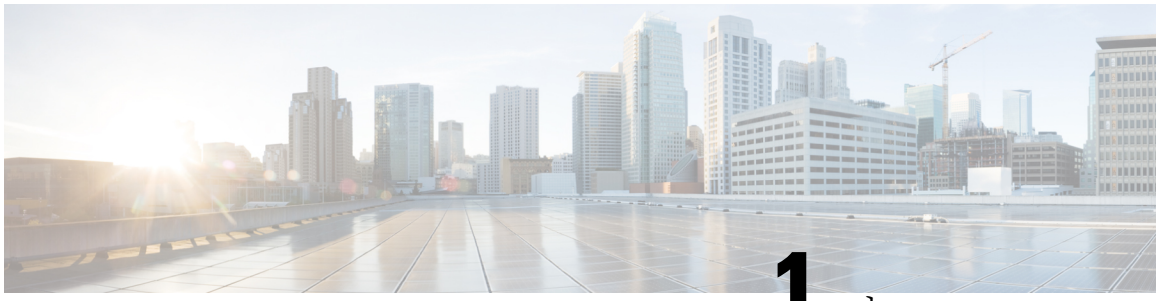
Cisco SecureX 로그인 빠른 시작 가이드

초판: 2019년 10월 1일

최종 변경: 2022년 6월 29일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



1 장

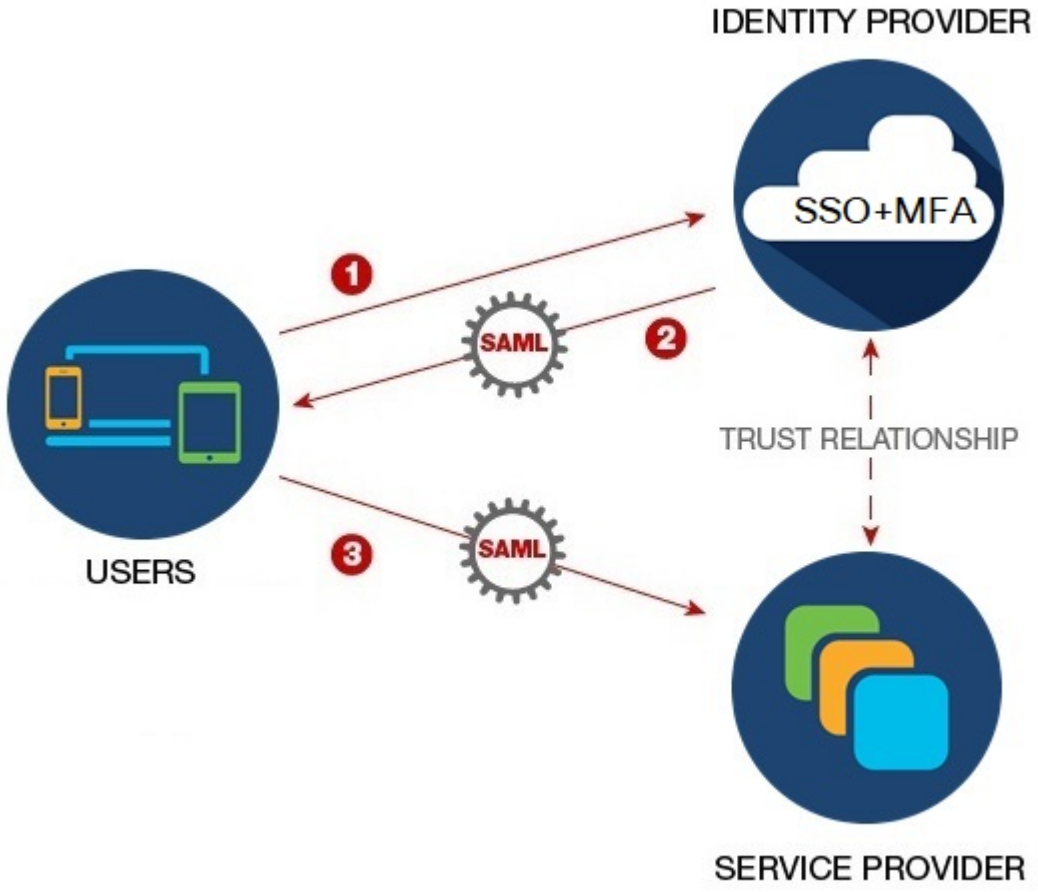
환영합니다.

개요

Cisco SecureX 로그인을 사용하면 모든 디바이스에서 하나의 자격증명 집합으로 모든 Cisco Security 제품에 쉽게 액세스할 수 있습니다. 사용자 이름과 비밀번호를 사용하여 로그인하면 모든 Cisco Security 제품이 맞춤형 대시보드에 앱으로 표시됩니다.

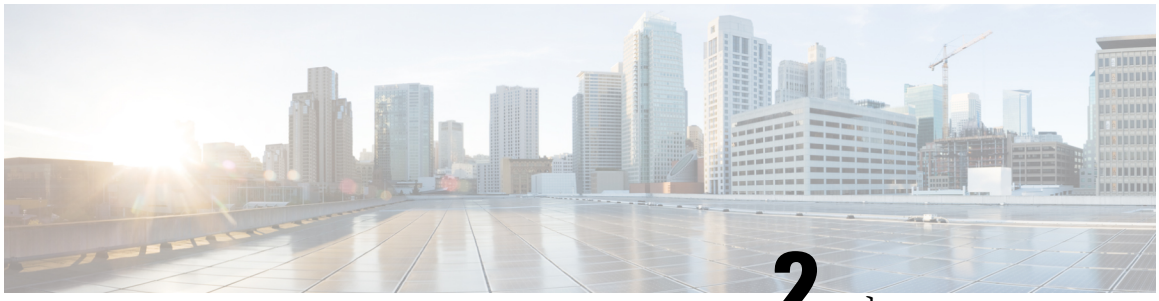
- 앱을 클릭하면 Cisco Security 제품 전반에서 원활한 워크플로를 위해 자동으로 로그인됩니다. 더 이상 여러 비밀번호를 기억하고 복잡하게 사용할 필요가 없습니다.
- Duo MFA(Multi-Factor Authentication) 통합은 적응형, 계층화된, 간소화된 인증을 의미합니다. 푸시 알림 한 번, 탭 한 번으로 즉시 액세스

운영 방식



SAML(Security Assertion Markup Language)은 ID 제공자(IdP)와 SP(통신 사업자) 간에 인증 및 권한 데이터를 교환하기 위한 XML 기반의 개방형 표준입니다. SP와 IdP 간 교환을 하면 사용자의 ID와 권한을 확인합니다. 이렇게 하면 단일 자격 증명 집합을 사용하여 다른 애플리케이션에 로그인할 수 있게 됩니다. 각 애플리케이션 모두에 대해 별도의 SSO(Single Sign-On, 단일 인증)를 관리하는 것보다 사용자당 SSO(Single Sign-On, 단일 인증)를 관리하는 것이 더 쉽습니다.

1. 사용자는 Duo의 MFA와 통합된 Cisco SecureX 로그인인 SSO IdP에 로그인합니다.
2. IdP와 SP 사이에 신뢰 관계가 있습니다. IdP는 SP에 신뢰할 수 있는 사용자 관련 정보가 포함된 SAML 속성 어설션을 전달할 수 있습니다.
3. 사용자가 다른 애플리케이션을 실행하면, SP가 IdP에서 사용자 권한 부여 및 인증을 요청합니다. IdP에 대한 SSO가 성공했기 때문에, 사용자는 이제 추가 자격 증명을 기억하고 입력할 필요 없이 다른 모든 애플리케이션에 액세스할 수 있습니다.



2 장

새로운 기능

새 포털

새 포털에서 Cisco SecureX 로그인의 외관, 느낌 및 사용 편의성이 개선되었습니다. 지역을 선택하고, 향상된 포털에서 SecureX 또는 기타 Cisco Security 제품을 시작합니다.

Cisco SecureX

Cisco Secure Sign-On을 사용하여 **Cisco SecureX**에 로그인

이제 Cisco Secure Sign-On 계정을 사용하여 Cisco SecureX에 로그인할 수 있습니다. 이제부터는 Cisco Secure Sign-On을 Cisco SecureX 로그인이라고 합니다.

Microsoft Azure

Microsoft Azure 계정을 사용하여 **Cisco Secure Sign-On**에 로그인

이제 Microsoft Azure 계정을 사용하여 Cisco Secure Sign-On에 로그인할 수 있습니다.

- 누가 이 방법을 사용할 수 있습니까?

  Microsoft Azure를 조직의 IdP(Identity Provider)로 사용하는 고객입니다.

- 이 방법을 활성화하려면 어떻게 해야 합니까?

고객의 Microsoft Azure 구성에 따라 조직에 대해 투명하게 작동합니다. 그렇지 않은 경우 첫 번째 사용자가 액세스를 시도하면 관리자가 Azure 포털에서 이를 승인해야 합니다. 구성 세부 사항은 Microsoft Docs 웹사이트로 이동하여 다음 주제에 대한 Azure 설명서에서 참조하십시오.

- 엔터프라이즈 앱에 사용자 또는 그룹 할당
- 앱에 테넌트 전체 관리자 동의를 부여합니다.
- 관리자 동의 워크플로 구성

- 이렇게 하면 고객의 Microsoft Azure AD(Active Directory) 프로파일에서 사용자 ID 특성을 가져옵니까?

  예, 이름, 성, 표시 이름, 직함, 휴대폰 및 조직을 가져옵니다.

- 이렇게 하면 Azure 그룹 정보를 가져와 Cisco Secure Sign-On으로 보호되는 애플리케이션에서 해당 정보를 인식하고 사용할 수 있습니까?

  아니요, 그룹 할당 및 역할 권한은 각 Cisco 애플리케이션에서 개별적으로 처리됩니다.

- 이렇게 하면 Cisco Secure Sign-On을 사용하는 애플리케이션에 액세스하는 방법이 변경됩니까?

  아니요. 동일한 사용자 이름을 사용하는 한 이전과 마찬가지로 애플리케이션에 매핑된 상태로 유지됩니다. 인증 방법만 변경됩니다.

- 두 계정을 모두 유지하고 사용할 수 있습니까?

  예, 그렇습니다.

- 이는 @cisco.com 사용자 이름을 사용하는 Cisco 직원에게 어떤 영향을 미칩니까?

  Cisco에서 @cisco.com 계정에 대해 Microsoft 로그인을 활성화하지 않았으므로 이 방법을 사용하여 로그인하려고 하면 실패 메시지가 표시됩니다.

- **Sign in with Microsoft(Microsoft**로 로그인**)** 옵션을 사용하지만 Cisco Secure Sign-On 어카운트가 없으면 어떻게 됩니까?

  이렇게 하면 투명하게 작동하며 별도의 계정을 만들 필요 없이 직접 로그인할 수 있습니다.

Cisco.com

Cisco.com 계정을 사용하여 **Cisco Secure Sign-On**에 로그인

이제 Cisco.com 계정을 사용하여 Cisco Secure Sign-On에 로그인할 수 있습니다.

- 내 Cisco Secure Sign-On 계정과 어떻게 다릅니까?

  이는 표준 cisco.com 계정(이전의 CCO)으로, 지원에 액세스하고 소프트웨어를 다운로드하는 데 사용된 것과 동일한 계정입니다.

- 이렇게 하면 Cisco Secure Sign-On을 사용하는 애플리케이션에 액세스하는 방법이 변경됩니까?

아니요. 동일한 사용자 이름을 사용하는 한 이전과 마찬가지로 애플리케이션에 매핑된 상태로 유지됩니다. 인증 방법만 변경됩니다.

- 두 계정을 모두 유지하고 사용할 수 있습니까?

  예, 그렇습니다.

- 이는 @cisco.com 사용자 이름을 사용하는 Cisco 직원에게 어떤 영향을 미칩니까?

  Cisco 직원은 **Cisco.com**으로 로그인 옵션을 사용하는 것이 좋습니다. 그러면 Cisco에서 직원을 메트릭에서 직원으로 인식하고 하나의 MFA 프롬프트만 수신할 수 있습니다.

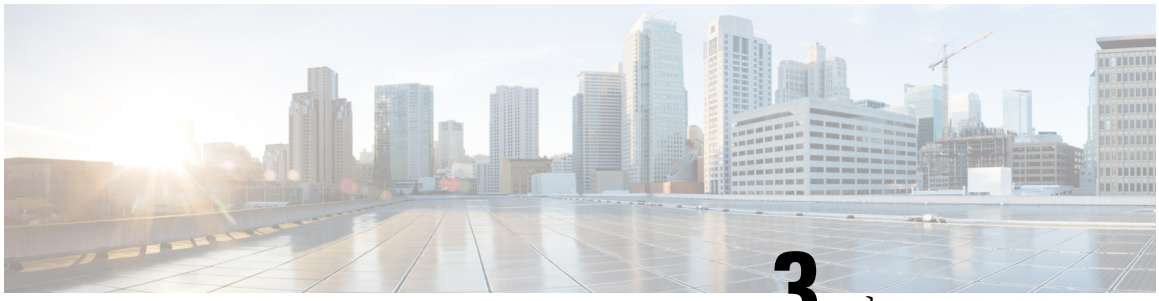
- **Sign in with Cisco.com(Cisco.com**으로 로그인**)** 옵션을 사용하지만 Cisco Secure Sign-On 계정이 없으면 어떻게 됩니까?

  이렇게 하면 투명하게 작동하며 별도의 계정을 만들 필요 없이 직접 로그인할 수 있습니다.

URL 변경

URL 변경

2020년 3월 24일, Cisco Secure Sign-On 도메인은 Cisco SecureX를 수용하기 위해 security.cisco.com에서 sign-on.security.cisco.com으로 이동했습니다. 즐겨찾기 및 비밀번호 관리자(예: LastPass, 1Password 또는 DashLane)를 업데이트하여 새 URL을 참조합니다.



3 장

절차

시작하기

시작하기 전에

지원되는 제품의 경우, 제품별 세부사항은 마이그레이션 및 옵트인 가이드에서 참고하십시오.

단계 **1** https://sign-on.security.cisco.com을 방문하십시오.

단계 **2** SecureX 로그인 계정이 있는 경우:

a) 사용자 이름을 입력하고 **Next(**다음**)**를 클릭합니다.

b) 비밀번호를 입력하고 로그인을 클릭합니다.

c) Duo MFA 프롬프트에서 등록된 디바이스에 알림을 푸시하고 승인을 탭하여 인증합니다.

단계 **3** 또는 대체 계정을 사용하여 계속 진행하도록 선택할 수 있습니다. **Other login options(**기타 로그인 옵션**)**를 클릭하여 **Cisco** 또는 **Microsoft**와 같은 다른 IdP를 선택합니다.

단계 **4** SecureX 로그인 계정이 없는 경우:

a) **Sign up(**등록하기**)**을 클릭합니다.

b) 양식을 작성하고 **Create Account(**계정 생성**)**를 클릭합니다.

중요 공용 도메인 이메일 주소는 SecureX에서 조직을 생성하는 데 사용할 수 없습니다. 따라서 비즈니스 도메인 이메일 주소를 사용하여 로그인 계정을 생성하는 것이 좋습니다. 이렇게 하면 Cisco에서 조직 정보를 검증하고 온보딩 프로세스를 간소화하는 데 도움이 됩니다.

참고 비밀번호는 180일 후에 만료됩니다. 비밀번호 요구 사항:

- 최소 8자
- 최소 1개의 숫자
- 최소 1개의 기호
- 최소 1개의 소문자
- 최소 1개의 대문자
- 사용자 이름의 일부를 포함하지 않음
- 이름을 포함하지 않음
- 성을 포함하지 않음
- 최근 10개의 비밀번호를 재사용할 수 없음

c) Cisco의 no-reply-security에서 온 '계정 활성화' 이메일을 찾아 **Activate Account(**계정 활성화**)**를 클릭합니다.

참고 활성화 링크는 7일 후에 만료됩니다.

d) 프롬프트에 따라 Duo 보안을 구성하여 다단계 인증(MFA)을 설정합니다. 이중 인증(MFA의 한 유형)은 보조 디바이스를 사용하여 ID를 확인함으로써 계정의 보안을 강화합니다. 이렇게 하면 다른 사람이 사용자의 비밀번호를 알고 있더라도 사용자 이외의 사용자가 계정에 액세스할 수 없습니다.

e) 추가할 디바이스를 선택하고 프롬프트에 따라 디바이스를 등록합니다. 자세한 내용은 Duo MFA 및 디바이스 등록 가이드에서 참고하십시오. 디바이스에 이미 Duo 앱이 있는 경우 이 어카운트에 대한 활성화 코드를 받게 됩니다. Duo는 하나의 디바이스에서 여러 계정을 지원합니다.

f) 추가 보안을 위해 최소 2개의 서로 다른 디바이스를 등록하는 것이 좋습니다. **+Add another device(**다른 디바이스 추가**)**를 클릭하고 프롬프트에 따라 다른 디바이스를 등록합니다. 자세한 내용은 Duo MFA 및 디바이스 관리 가이드에서 참고하십시오.

g) **Continue to Login(**로그인 계속**)**을 클릭하고 디바이스가 계정과 페어링되면 **Finish(**마침**)**를 클릭합니다.

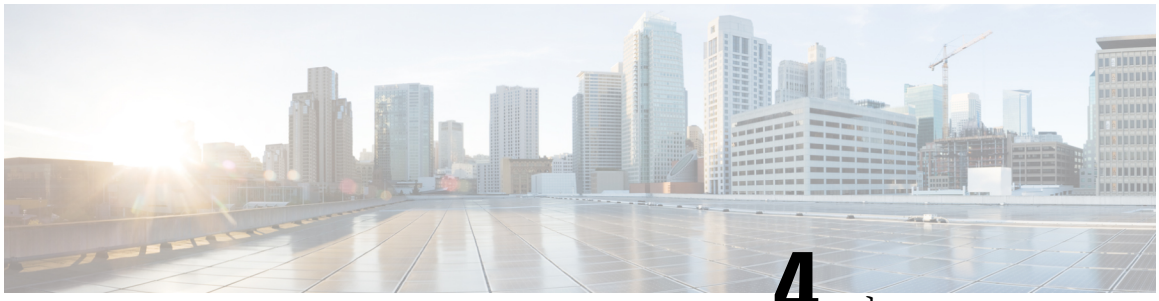
참고 선택적으로, MFA용 Google Authenticator의 기존 사용자는 **Setup** Google Authenticator(Google Authenticator 설정)를 클릭하고 프롬프트에 따라 백업 요소로 추가할 수 있습니다.

다음에 수행할 작업

SecureX 로그인 애플리케이션 포털에 오신 것을 환영합니다.

- 지역을 선택하고 SecureX를 실행합니다.
- 타일을 클릭하여 해당 앱을 실행합니다. 비밀번호는 필요하지 않습니다.
- 여기에서 SSO 포털로 애플리케이션을 내보내려면 오른쪽 상단의 사용자 프로파일 메뉴에서 **Export Applications(**애플리케이션 내보내기**)**를 선택합니다.

- 이전 포털로 돌아가려면 오른쪽 상단의 사용자 프로파일 메뉴에서 **Legacy Portal(**레거시 포털**)**을 선택합니다.



4 장

지원되는 제품

지원되는 제품

제품	설명	이 제품을 원하십니까?	지원
Cisco Cloudlock	Cisco Cloudlock은 안전한 클라우드 사용을 가속화하는 API 기반 CASB(Cloud Access Security Broker)입니다. Cloudlock은 ID, 데이터 및 앱을 보호하여 계정 보안 침해, 보안 침해 및 클라우드 앱 에코시스템 위험을 방지합니다. Cloudlock의 API 기반 접근 방식은 건전한 클라우드 도입을 활성화하고 클라우드 앱 에코시스템에서 위험을 관리할 수 있는 간단하고 개방적인 방법을 제공합니다. Cisco Umbrella + Cloudlock 솔루션 개요를 보십시오.	견적 요청	옵트인 가이드 설명서 보기 이메일 지원

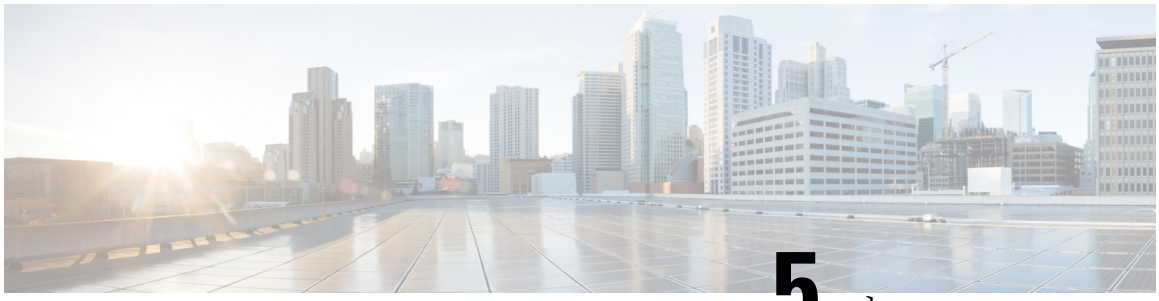
지원되는 제품

제품	설명	이 제품을 원하십니까?	지원
Cisco Defense Orchestrator	CDO(Cisco Defense Orchestrator)를 사용하면 Cisco 보안 제품 전반에서 정책을 일관되게 관리할 수 있습니다. 복잡성을 없애고 시간을 절약하고 최신 위협으로부터 조직을 보호하는 클라우드 기반 애플리케이션입니다.	CDO 무료 체험	마이그레이션 가이드 설명서 보기 지원 케이스 열기 이메일 지원
Cisco Meraki	Cisco Meraki에서는 업계 최대 규모의 클라우드 네트워킹 서비스를 운영합니다. Cisco Meraki 클라우드 서비스는 전 세계 수만 개의 네트워크를 지원하며 수백만 개의 디바이스를 연결합니다. Cisco Meraki 클라우드 네트워킹 플랫폼은 기업에서 병원, 은행 및 소매점에 이르기까지 수천 명의 IT 전문가가 신뢰합니다.	Cisco Meraki 무료 체험	옵트인 가이드 설명서 보기 지원 케이스 열기
Cisco Secure Cloud Analytics(이전 이름 Stealthwatch Cloud)	Cisco Secure Cloud Analytics는 사무실에서 공용 클라우드에 이르기까지 분산형 네트워크 전반의 보안을 강화하고 사고 대응 역량을 높여 줍니다. 실시간으로 위협을 탐지합니다. 오탐 감소 보안 팀의 효율성을 높이기 위해 실행 가능한 보안 인텔리전스를 확보합니다.	Secure Cloud Analytics 무료 체험	마이그레이션 가이드 설명서 보기 지원 케이스 열기 이메일 지원

제품	설명	이 제품을 원하십니까?	지원
Cisco Secure Email Cloud Mailbox(이전 Cloud Mailbox Defense)	Cisco Secure Email Cloud Mailbox는 간편한 구축, 손쉬운 공격 복구, 탁월한 가시성에 더해 최고의 유용성을 자랑하는 Cisco Talos의 위협 정보까지 갖춘 Microsoft 365용 통합 클라우드 네이티브 보안 솔루션입니다. Cloud Mailbox는 검증된 Cisco Secure Email 기술을 활용하여 랜섬웨어, BEC, 피싱, 스푸핑 및 스팸과 같은 고급 이메일 위협을 차단하여 Microsoft 365 보안의 허점을 해결합니다.	Cloud Mailbox 무료 체험	사용 설명서 FAQ 이메일 지원
Cisco Secure Endpoint(이전 명칭 Advanced Malware Protection for Endpoints)	Cisco Secure Endpoint는 글로벌 위협 인텔리전스, 지능형 샌드박스, 실시간 악성코드 차단으로 보안 위반을 예방합니다. 예방만으로는 충분하지 않은 만큼 Cisco Secure Endpoint에서는 확장 네트워크 전반의 파일 활동을 지속적으로 분석하여 지능형 악성코드를 신속하게 탐지, 억제, 제거할 수 있게 합니다.	Cisco Secure Endpoint 무료 체험	옵트인 가이드 설명서 보기 지원 케이스 열기

지원되는 제품

제품	설명	이 제품을 원하십니까?	지원
Cisco Secure Malware Analytics (이전의 Threat Grid)	Cisco Secure Malware Analytics는 고급 샌드박싱과 위협 인텔리전스를 하나의 통합 솔루션으로 결합하여 악성코드로부터 조직을 보호합니다. 악성코드에 대한 강력하고 풍부한 상황별 정보를 통해 악성코드의 활동 또는 목적, 위협 규모, 방어 방법을 파악하게 됩니다.	Secure Malware Analytics 무료 체험	옵트인 가이드(로그인 필요) 지원 케이스 열기
Cisco SecureX	Cisco SecureX는 간소화된 플랫폼 환경입니다. Cisco 보안 포트폴리오를 통합해 하나의 가시성과 자동화로 네트워크, 엔드포인트, 클라우드 및 애플리케이션 전반의 보안을 강화하고 일관된 경험을 제공합니다.	SecureX 무료 체험	로그인 가이드 설명서 보기 지원 케이스 열기
Cisco Umbrella	Cisco Umbrella는 네트워크, 지점 및 로밍 사용자 전반에 걸쳐 인터넷 액세스를 보호하고 클라우드 앱 사용을 제어하는 데 도움이 됩니다. 몇 분 만에 쉽게 구축할 수 있는 클라우드 보안 플랫폼이며, 심층 검사 및 제어를 제공하여 컴플라이언스를 지원하고 위협을 차단합니다.	Cisco Umbrella 무료 체험	옵트인 가이드 설명서 보기 지원 케이스 열기



5 장

FAQ(자주 묻는 질문)

FAQ(자주 묻는 질문)

현재 **OneLogin**을 사용하고 있습니다. **Cisco SecureX** 로그인으로 마이그레이션하는 방법은 무엇입니까**?**

Cisco SecureX 로그인 페이지로 이동하여 **SecureX** 로그인 생성을 클릭하고 자가 등록 절차를 시작합니다.

계정 활성화 이메일은 언제까지 유효합니까**?**

계정 활성화 이메일은 전송일부터 7일 동안 유효합니다.

어떻게 보안 이미지를 변경합니까**?**

Security 이미지를 변경하려면 로그인하고 상단 메뉴에서 사용자 이름을 클릭한 다음 설정을 선택합니다. **Security** 이미지 섹션에서 편집을 클릭합니다. 새 security 이미지를 선택하고 저장을 클릭합니다.

어떻게 계정 비밀번호를 변경합니까**?**

계정 비밀번호를 변경하려면 로그인하고 상단 메뉴에서 사용자 이름을 클릭한 다음 설정을 선택합니다. 비밀번호 변경 섹션에서 편집을 클릭합니다. 기존 비밀번호와 새 비밀번호를 입력하고 비밀번호 변경과 저장을 차례로 클릭합니다.

비밀번호 분실 질문을 변경하는 방법은 무엇입니까**?**

비밀번호 분실 질문을 변경하려면 로그인하여 상단 메뉴에서 사용자 이름을 클릭한 다음 설정을 선택합니다. 비밀번호 분실 질문 섹션에서 편집을 클릭합니다. 새 질문을 선택하고 답변을 입력한 후 저장을 클릭합니다.

FAQ(자주 묻는 질문)

현재 **MFA**에 **Google Authenticator**를 사용하고 있습니다**.** 내 **ID**가 마이그레이션됩니까**?**

아니요, Google Authenticator MFA는 마이그레이션되지 않습니다. 모든 Cisco SecureX 로그인 계정은 Duo의 MFA를 사용해야 합니다. 하드웨어 및 소프트웨어 솔루션에 대한 통화 및 텍스트를 허용하기 때문입니다. Google OTP를 계속 사용하려면 계정의 백업 요소로 추가할 수 있습니다. 계정을 활성화하는 동안 Duo(기본)를 사용하여 MFA를 설정합니다. 그런 다음 Google Authenticator(백업)를 사용하여 추가 MFA를 설정합니다.

내 **Duo MFA**에 조직의 **Duo** 정책 및 설정을 사용할 수 있나요**?**

아직 아닙니다. Duo MFA가 조직의 Duo 정책 및 설정을 가리키도록 하는 "bring your own(사용자 고유의 방식)" 기능을 추가할 예정입니다.

비밀번호를 잊어버린 경우 어떻게 해야 합니까**?**

Cisco SecureX 로그인 페이지에서 로그인에 도움이 필요하십니까**?**와 비밀번호를 잊어버리셨습니까**?**를 클릭합니다. 비밀번호를 재설정할 수 있는 세 가지 옵션이 있습니다(기본 설정 순서대로).

- **Reset via Duo(Duo**를 통해 재설정**)**를 클릭하고 인증하여 ID를 확인한 다음 새 비밀번호를 입력합니다.
- 계정 설정에 추가한 휴대폰 번호를 입력하고 **Reset via SMS(SMS**로 재설정**)**를 클릭합니다. SMS 메시지를 찾아 프롬프트를 따릅니다.
- 이메일 또는 사용자 이름을 입력하고 **Reset via Email(**이메일로 재설정**)**을 클릭합니다. 이메일을 찾아 프롬프트를 따릅니다.

이러한 옵션을 사용할 수 없는 경우 지원되는 제품 팀에 문의하십시오.

내 비밀번호는 안전합니까**?**

예, Cisco는 귀하의 정보를 보호하기 위해 엄격한 보안 조치 및 제어를 제공합니다. 이러한 제어는 SOC2 보고서에서 감사 및 증명됩니다.

사용자 이름과 비밀번호는 어디에 어떻게 저장됩니까**?**

강력한 암호화를 사용하여 데이터를 보호하는 것처럼 사용자 이름 및 비밀번호 자격 증명에도 강력한(256비트 AES) 암호화를 사용합니다.

Duo로 내 신원을 확인하는 데 사용한 전화를 분실한 경우 어떻게 해야 하나요**?**

전화를 분실한 경우에도 사용자 이름과 비밀번호로 로그인할 수 있다면 Duo 확인 페이지에서 **Settings(**설정**)**를 클릭합니다. **Add a new device(**새 디바이스 추가**)**를 선택하고 프롬프트에 따라 새 교체 전화를 등록합니다. 자세한 내용은 Duo 새 디바이스 추가 가이드에서 참고하십시오.

일부 앱의 경우 비밀번호를 입력해야 하는 이유는 무엇입니까**?**

Cisco SecureX 로그인을 사용하면 단일 통합 대시보드를 통해 애플리케이션에 액세스할 수 있습니다. 이러한 앱에 대한 액세스는 SAML(Security Assertion Markup Language)을 사용하는 SSO(Single Sign-On)

기술을 통해 제공됩니다. SAML을 사용하면 Cisco SecureX 로그인에서 토큰을 통해 액세스를 자동으로 전달하므로 앱에 업데이트가 필요할 때 수동으로 변경할 필요가 없습니다.

기존 앱의 사용자 이름과 비밀번호를 변경하려면 어떻게 해야 합니까?

기존 비밀번호를 변경하려면 앱의 타일 위에 마우스 포인터를 올려놓습니다. 타일의 오른쪽 상단에 기어 아이콘이 있습니다. 기어 아이콘을 클릭하여 설정을 열고 현재 사용자 이름과 비밀번호를 입력하여 ID를 확인합니다. 확인이 완료되면 새 비밀번호를 입력할 수 있습니다.

관리자가 내 로그인 정보를 볼 수 있습니까?

관리자는 사용자 이름을 볼 수 있지만 비밀번호에 액세스할 수는 없습니다.

내 계정이 잠긴 경우 어떻게 해야 합니까?

계정이 잠긴 경우 로그인하는 데 도움이 필요하십니까?를 클릭합니다. Cisco SecureX Sign-On(Cisco SecureX 로그인) 페이지에서 **Unlock Account(**계정 잠금 해제**)**를 클릭합니다. 이러한 옵션을 사용할 수 없는 경우 지원되는 제품 팀에 문의하십시오.

때때로 보안 이미지가 표시되지 않는 이유는 무엇입니까?

보안 이미지는 로그인할 때 설정되는 쿠키입니다. 브라우저의 쿠키가 지워지면 다음에 로그인할 때까지 보안 이미지가 표시되지 않을 수 있습니다.

세션은 만료되지만 일부 앱은 여전히 열려 있는 이유는 무엇입니까?

Cisco SecureX 로그인 세션에서는 로그아웃될 수 있지만 Cisco SecureX 로그인은 앱에서 로그아웃되지 않습니다.

SecureX 세션 토큰이 만료되는 데 얼마나 걸립니까?

SecureX 세션 토큰(JWT)은 24시간 후에 만료됩니다.

Cisco SecureX 로그인이 중단되면 어떻게 됩니까?

Cisco SecureX 로그인은 "Always-On" 아키텍처를 기반으로 합니다. 서비스가 중단된 경우 SSO(Single Sign-On)를 사용하여 로그인하고 앱에 액세스할 수 없습니다. 그러나 직접 링크를 통해 일부 앱에 계속 액세스할 수 있습니다. Cisco SecureX 로그인에 액세스할 수 없으며 서비스 중단으로 인한 것인지 확인하려면 지원되는 제품 팀에 문의하십시오.

기존 **Cisco SecureX** 로그인 계정을 삭제하려면 어떻게 해야 합니까?

제품 관리자가 계정을 삭제하여 개별 제품 앱에 대한 액세스 권한을 제거할 수는 있지만, Cisco SecureX 로그인 엔지니어링 팀이 대신 계정을 삭제하도록 하려면 지원되는 제품을 통해 Cisco TAC에 문의해야 합니다.

FAQ(자주 묻는 질문)

조직에서 이미 **SSO(Single Sign-On)**에 **IdP**를 사용하고 있습니다. 이를 **SecureX** 로그인과 통합하려면 어떻게 해야 합니까**?**

"사용자 고유의 IdP"를 가져와 SecureX 로그인과 통합할 수 있습니다. 그러면 모든 사용자 계정을 수동으로 다시 생성할 필요 없이 Cisco 보안 애플리케이션에 액세스할 수 있습니다. 자세한 내용은 Cisco SecureX Sign-On 서드파티 IdP 통합 설명서에서 참조하십시오.

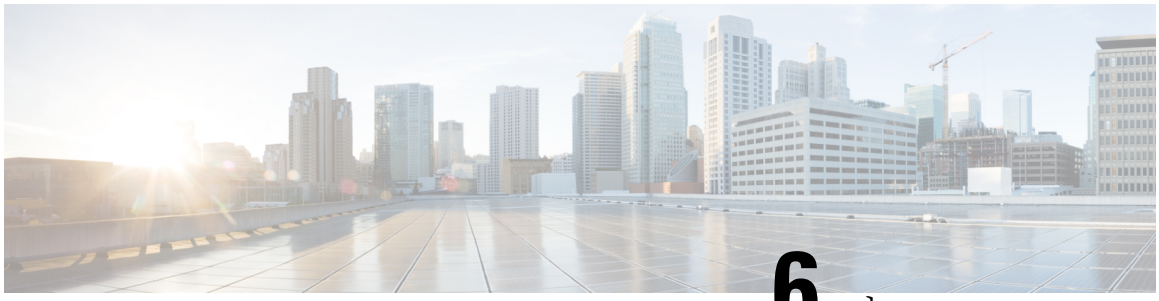
추가 자료가 필요하십니까**?**

추가 정보는 다음 리소스에서 참고하십시오.

- Cisco SecureX 로그인 제품 페이지
- Cisco SecureX 로그인 프라이버시 데이터 시트
- Cisco SecureX 로그인 상태 페이지

I 부

부록



6 장

애플리케이션 내보내기

개요

애플리케이션 내보내기 페이지(대시보드 페이지의 사용자 프로파일 메뉴에서 액세스)에는 SecureX 로그인에서 액세스할 수 있는 Cisco Security 제품 애플리케이션이 나열됩니다. 각 애플리케이션 옆에 있는 링크:

- 클립보드에 애플리케이션 이름 복사
- 클립보드에 애플리케이션의 URL 복사
- 컴퓨터에 애플리케이션의 로고 다운로드

여기에서 Cisco Security 제품 애플리케이션을 SSO(Single Sign-On, 단일 인증) 애플리케이션 포털로 내보낼 수 있습니다. 이는 단일 공통 로그인으로 액세스 가능한 애플리케이션 집합을 표시하는 랜딩 페이지입니다. 일반적인 SSO 애플리케이션에는 Duo Access Gateway, Microsoft Azure 및 Okta SSO가 있으며, 이를 통해 한 번 로그인한 다음 동일한 사용자 ID와 자격 증명으로 애플리케이션에 액세스할 수 있습니다. 애플리케이션 내보내기 페이지의 링크 및 해당 링크의 정보를 사용하여 SSO 애플리케이션에 애플리케이션을 추가 및 구성합니다. 이 장에서는 두 가지 예로 일반적인 절차를 설명합니다.

Duo Access Gateway로 애플리케이션 내보내기

Duo Access Gateway 런처에서 Cisco Security 제품 애플리케이션에 즐겨찾기를 추가하려면 다음 단계를 이행합니다.

시작하기 전에

- Cisco SecureX 로그인에서 애플리케이션에 액세스할 수 있어야 합니다.
- Duo Access Gateway에서 관리자 권한이 있어야 합니다.

- Duo Access Gateway 런처를 설정하고 활성화합니다. https://guide.duo.com/dag-launcher

단계 1 Duo Access Gateway 관리 콘솔에서 **Launcher**(런처)를 클릭합니다.

단계 2 **Bookmarks**(즐겨찾기)를 클릭합니다.

단계 3 **Add a Bookmark(**즐겨찾기 추가**)**를 클릭합니다.

단계 4 앱의 이름을 입력합니다(Export Applications 페이지의 애플리케이션에서 **Copy Name**).

단계 5 사용자가 애플리케이션에 액세스하는 데 사용할 **URL**을 입력합니다(Export Applications 페이지의 애플리케이션에서 **Copy URL**).

단계 6 (선택 사항) 앱의 로고 이미지를 업로드합니다(Export Applications 페이지의 앱에서 **Download Logo**).

단계 7 새 즐겨찾기는 기본적으로 모든 사용자에게 표시됩니다. Duo 그룹을 사용하여 즐겨찾기를 볼 사용자를 제어할 수 있습니다. **Only allow access from users in specific groups**(특정 그룹의 사용자만 액세스 허용) 또는 **Show this bookmark to only certain groups of users**(이 즐겨찾기를 특정 사용자 그룹에게만 표시) 확인란을 선택하고 그룹 선택 필드에 입력을 시작하여 Duo 그룹 목록을 검색합니다. 런처에서 새 즐겨찾기를 보려는 사용자가 포함된 각 그룹을 클릭합니다.

단계 8 **Add** 또는 **Save**를 클릭합니다.

Microsoft Azure로 애플리케이션 내보내기

Microsoft Azure 포털에 Cisco Security 제품 애플리케이션을 추가하려면 다음 단계를 따릅니다.

시작하기 전에

- Cisco SecureX 로그인에서 애플리케이션에 액세스할 수 있어야 합니다.
- Microsoft Azure에서 최고 관리자 권한이 있어야 합니다.

단계 1 최고 관리자 권한으로 https://portal.azure.com에 로그인합니다.

단계 2 **Azure Active Directory**를 클릭합니다.

단계 3 왼쪽 메뉴에서 엔터프라이즈 애플리케이션을 선택합니다.

단계 4 새 애플리케이션 → 비-갤러리 애플리케이션을 클릭합니다.

단계 5 앱의 이름을 입력합니다(Export Applications 페이지의 애플리케이션에서 **Copy Name**).

단계 6 (선택 사항) 앱의 로고 이미지를 업로드합니다(Export Applications 페이지의 앱에서 Download Logo).

단계 7 **SSO(Single Sign-On,** 단일 인증**)** 설정을 클릭합니다.

단계 8 연결됨을 선택합니다.

단계 9 Set 로그인 **URL**을 앱(애플리케이션 내보내기 페이지의 앱에서 **URL**복사)에 액세스하는 데 사용할 URL로 설정하고, 저장을 클릭합니다.

단계 10 앱의 왼쪽 메뉴에서 사용자 및 그룹을 클릭합니다.

단계 **11** 앱에 사용자 또는 그룹을 할당합니다. 할당된 사용자만 https://myapplications.microsoft.com에 액세스할 때 앱을 볼 수 있습니다.