



2025의 새로운 기능

2025 Security Cloud Control에 구축된 새로운 방화벽 기능입니다.

- [2025년 12월, 1 페이지](#)
- [2025년 11월, 2 페이지](#)
- [2025년 10월, 3 페이지](#)
- [2025년 9월, 4 페이지](#)
- [2025년 8월, 5 페이지](#)
- [2025년 7월, 6 페이지](#)
- [2025년 6월, 7 페이지](#)
- [2025년 4월, 8 페이지](#)
- [2025년 3월, 8 페이지](#)

2025년 12월

2025년 12월 18일

Security Cloud Control Firewall Management, 이제 아랍에미리트(UAE)에서 사용 가능

아랍에미리트 지역에서 Security Cloud Control Firewall Management(보안 클라우드 제어 방화벽 관리)를 사용할 수 있음을 알려드립니다. 이제 조직을 생성할 때 구축 지역으로 아랍에미리트를 선택할 수 있습니다.

2025년 12월 12일

클라우드 제공 **Firewall Management Center**로 업데이트

Security Cloud Control은 클라우드 제공 Firewall Management Center로 의 업데이트를 릴리스했습니다. 자세한 내용은 [클라우드 제공 Firewall Management Center 릴리스 노트](#)를 참조하십시오.

AIOps의 보안 인사이트 소개

이 릴리스에서는 조직 전체의 의심스러운 활동에 대한 가시성을 제공하기 위해 보안 인사이트를 도입했습니다. 이제 사용자 위협 급증과 같이 진화하는 보안 위협을 식별하고 대응할 수 있습니다. 이는 신뢰 수준과 기타 의심스러운 사용자 행동을 나타냅니다.

[보안 인사이트](#)를 참조하십시오.

2020년 12월 4일**MSSP** 포털용 새 상태 대시보드

이 릴리스에서는 Secure Firewall ASA 디바이스에 대한 상태 대시보드를 도입했습니다.

이 대시보드에는 CPU, 메모리, 디스크 사용량 및 인터페이스 통계와 같은 중요한 성능 메트릭이 표시됩니다. 이제 성능 병목 현상을 조기에 감지하고 최적의 운영 상태를 유지하기 위한 사전 조치를 취할 수 있습니다.

자세한 내용은 [MSSP 포털에서 상태 대시보드 정보](#)를 참조하십시오.

2025년 11월**2025년 11월 20일**클라우드 제공 **Firewall Management Center**에 업데이트

보안 클라우드 제어가 클라우드 제공 Firewall Management Center의 업데이트를 릴리스했습니다. 자세한 내용은 [클라우드 제공 Firewall Management Center 릴리스 노트](#)를 참조하십시오.

2020년 11월 13일공용 **API**를 사용한 **MSSP** 디바이스 업그레이드

Security Cloud Control Firewall Management는 이제 MSSP에 대한 새로운 API 엔드포인트를 제공하여 테넌트 전체에서 Cisco Secure Firewall Threat Defense 디바이스를 업그레이드합니다. 이를 위해서는 MSSP 포털이 필요합니다.

자세한 내용은 [Security Cloud Control 방화벽 API 문서 시작하기](#)를 참조하십시오.

2025년 11월 6일

Security Cloud Control 이제 **Catalyst SD-WAN NGFW** 기능을 관리합니다.

이제 Security Cloud Control가 Catalyst SD-WAN Manager와 통합되어 Catalyst SD-WAN Manager에서 관리하는 개체 및 보안 정책을 비롯한 NGFW(차세대 방화벽) 기능을 중앙에서 관리할 수 있습니다.

Security Analytics and Logging(보안 분석 및 로깅)을 사용하면 네트워크 활동에 대한 가시성을 확보하여 보안 이벤트를 쉽게 모니터링, 분석 및 대응할 수 있습니다. 네트워크에서 탐지된 허용 및 차단된 침입 및 멀웨어 이벤트를 볼 수도 있습니다.

자세한 내용은 [Security Cloud Control를 사용하는 Cisco Catalyst SD-WAN 방화벽 기능 관리](#)를 참조하십시오.

Cisco Security Analytics and Logging 대한 계층형 구독 모델 도입

이 릴리스에서는 새로운 계층형 구독 모델을 제공하도록 Cisco Security Analytics and Logging 라이선싱을 업데이트했습니다. 이 구조는 기본 보존 기간이 1년으로 더 길어지고, 스토리지 옵션이 최대 10TB로 증가합니다. Essentials, Advantage 또는 Premier 계층 중에서 특정 요구 사항에 맞게 선택할 수 있습니다. 이 업데이트는 가격을 간소화하고 방화벽 로그 관리에 있어 더 큰 유연성과 가치를 제공합니다.

자세한 내용은 [Cisco 보안 분석 및 기록](#)을 참조하십시오.

2025년 10월

2025년 10월 23일

클라우드 제공 **Firewall Management Center**에서 관리하는 **Firewall Threat Defense** 디바이스에 대한 **CLI** 지원

이제 Security Cloud Control 인터페이스를 통해 클라우드 제공 Firewall Management Center에서 관리하는 Firewall Threat Defense 디바이스의 CLI에 액세스할 수 있습니다. **Security Devices > FTD(보안 디바이스 FTD)** 로 이동하여 **FTD**를 선택하고 오른쪽 창에서 **Command Line Interface(명령줄 인터페이스)**를 선택합니다.

자세한 내용은 [Security Cloud 제어 명령줄 인터페이스를 사용하여](#) 참조하십시오.

2025년 9월

2025년 9월 18일

새로운 AIOps 기능 소개

AIOps는 방화벽 관리에 AI 기반 인텔리전스를 제공하여 사전 대응적 인사이트와 실행 가능한 지침을 제공하여 운영을 간소화하고 보안을 강화합니다.

Webex Control Hub의 새로운 기능을 소개합니다.

- **AIOps 요약 대시보드**: 통찰력을 통합하는 통합 보기로, 디바이스의 성능에 대한 명확한 스냅샷을 제공합니다.
- **모범 사례 및 권장 사항**: 모범 사례와의 편차를 강조 표시하고 교정 지침을 제공하는 자세한 평가입니다.
- **기능 도입**: 라이선스별로 분류된 활발하게 사용되는 기능에 대한 가시성, 테넌트 전체의 도입률 및 사용자 개선을 위한 지침입니다.
- **소프트웨어 업그레이드 플래너**: 해결된 버그 및 보안 취약점에 대한 가시성을 포함하여 Secure Firewall Threat Defense 디바이스에 가장 적합한 업그레이드 버전에 대한 제안을 통해 업그레이드 결정을 간소화합니다.

이러한 개선 사항은 **Policy Analyzer & Optimizer**와 같은 기존 기능에 추가되어 AIOps를 사전적이고 효율적인 방화벽 관리를 위한 중앙 허브로 포지셔닝합니다.

Secure Firewall ASA 디바이스에 대한 디바이스 상태 메트릭 도입

이 릴리스에서는 Secure Firewall ASA 디바이스에 대한 디바이스 상태 메트릭을 도입했습니다. CPU, 메모리, 디스크 사용량, 팬 상태, 인터페이스 통계 등의 중요한 성능 메트릭을 표시합니다. 이러한 가시성을 통해 성능 병목 현상을 감지하고 최적의 운영 상태를 유지하기 위한 사전 조치를 취할 수 있습니다.

자세한 내용은 **디바이스 상태 메트릭**을 참조하십시오.

2025년 8월

2025년 8월 28일

Security Cloud Control에서 CLI 템플릿 사용 가능

이제 새 디바이스를 구성하기 위해 CLI 템플릿을 .txt 파일로 관리하고 내보낼 수 있습니다. CLI 템플릿에 액세스하려면 왼쪽 창에서 **Administration(관리)**를 클릭하고 **Integrations(통합) > CLI Templates(통합 CLI 템플릿)**를 선택합니다.

자세한 내용은 [CLI 템플릿 관리](#)를 참조하십시오.

하드웨어 단종 필터

이제 **Security Devices(보안 디바이스)** 페이지에서 디바이스를 필터링하여 마지막 지원 날짜가 임박하거나 지난 하드웨어를 식별할 수 있습니다. 상세 보기에는 라이프사이클 계획에 도움이 되는 권장 교체 디바이스도 제공됩니다.

자세한 내용은 [Security Devices\(보안 디바이스\)](#)를 참조하십시오.

2025년 8월 21일

Microsoft Teams에서 Security Cloud Control 알림

Microsoft Teams에서 Security Cloud Control 알림을 수신하려면 Teams에서 수신 Webhook을 생성하고 Security Cloud Control에 Webhook URL을 입력하십시오(**Administration(관리) > Notification Settings(알림 설정)**).

자세한 내용은 [Microsoft Teams용 수신 Webhook](#)을 참조하십시오.

2025년 8월 14일

클라우드 제공 Firewall Management Center로 업데이트

Security Cloud Control은 클라우드 제공 Firewall Management Center로 의 업데이트를 릴리스했습니다. 자세한 내용은 [클라우드 제공 Firewall Management Center 릴리스 노트](#)를 참조하십시오.

범용 Zero Trust 네트워크 액세스(범용 ZTNA)

Security Cloud Control은 범용 Zero Trust 네트워크 액세스(범용 ZTNA) 기능을 출시했습니다. 범용 ZTNA는 사용자 ID, 신뢰 및 보안 태세 기반으로 내부 네트워크 리소스에 대한 보안 액세스를 제공하는 포괄적인 솔루션입니다. 이는 원격 액세스 VPN과 같이 하나의 애플리케이션에 대한 접근 권한이 암묵적으로 전체 네트워크에 대한 접근 권한을 부여하지 않도록 보장합니다. **Policies(정책) > Zero Trust Application(Zero Trust 애플리케이션)**을 사용하여 범용 ZTNA를 활성화합니다. 자세한 내용은

Security Cloud Control에서 클라우드 제공 Firewall Management Center로 Firewall Threat Defense 관리를 참조하십시오.

2025년 7월

2025년 7월 24일

MSSP 포털: 보안 디바이스의 향상된 페이지 매김 및 정렬

이제 MSSP 포털의 **Security Devices**(보안 디바이스) 페이지에 **Devices**(디바이스), **Cloud Services**(클라우드 서비스), **Templates**(템플릿) 및 **Firewall Managers**(방화벽 관리자) 전용 탭이 포함됩니다. 이러한 개선 사항은 페이지 성능을 개선하고 페이지화 및 필터링을 간소화하여 보안 자산을 보다 효율적으로 관리할 수 있도록 합니다.

자세한 내용은 [Security Devices Details](#)(보안 디바이스 세부 정보)를 참조하십시오.

Security Cloud Control Firewall Manager API 업데이트

Security Cloud Control Firewall Manager API가 업데이트되어 ASA 디바이스에 대한 상태 메트릭을 수집 및 확인하고 MSSP 포털 재고 목록을 볼 수 있는 여러 개의 새 API 엔드포인트가 추가되었습니다.

이벤트 로그 검색 기능 업데이트

Event Logging(이벤트 로깅) 페이지의 **Background Search**(백그라운드 검색) 버튼 이름이 **Reports**(보고서)로 변경되었습니다. 버튼의 기능은 동일하게 유지되므로 백그라운드에서 이벤트 로그 검색을 수행하고 생성된 보고서를 관리할 수 있습니다.

자세한 내용은 [백그라운드에서 기록 이벤트 검색](#)을 참조하십시오.

클라우드 제공 Firewall Management Center 디바이스 백업 업데이트

클라우드 제공 Firewall Management Center의 다음 업그레이드부터 가장 최근의 Firewall Threat Defense 백업 5개만 보존됩니다. 이전 백업은 자동으로 삭제됩니다.

2025년 5월 1일 발표 이후 프라이빗 환경에 필요한 백업을 다운로드하지 않은 경우 2025년 7월 31일 이전에 필요한 백업을 다운로드하여 데이터에 지속적으로 액세스할 수 있습니다.

디바이스 백업을 다운로드하는 방법에 대한 자세한 내용은 [방화벽 Firewall Threat Defense 디바이스 복원](#)을 참조하십시오.

2025년 7월 3일

클라우드 제공 Firewall Management Center에 업데이트

Security Cloud Control은 클라우드 제공 Firewall Management Center로 의 업데이트를 릴리스했습니다. 자세한 내용은 [클라우드 제공 Firewall Management Center 릴리스 노트](#)를 참조하십시오.

샘플 필터를 사용한 강화된 이벤트 검색

이 릴리스에서는 검색 환경을 개선하기 위해 이벤트 로깅 페이지에 샘플 필터를 도입했습니다. 이러한 필터는 일반적인 검색 쿼리로 검색 창을 즉시 채웁니다. 이렇게 하면 검색 쿼리를 수동으로 입력할 필요가 줄어듭니다. 샘플 필터를 선택하고 특정 요구에 맞게 검색 파라미터를 수정하면 됩니다.

자세한 내용은 [사용하여 Sample Filters to Search Events 검색에 샘플 필터 사용하여](#)를 참조하십시오.

Firewall 마이그레이션 툴에 대한 업데이트

Security Cloud Control가 Firewall 마이그레이션 툴의 업데이트된 버전을 호스팅합니다. 업데이트에는 Firewall Threat Defense로의 Azure Firewall 마이그레이션, Multicloud Defense로의 Checkpoint 및 fortinet 방화벽 마이그레이션, 간소화된 정책 관리 등이 포함됩니다. 자세한 정보는 [Cisco Secure Firewall 마이그레이션 툴 릴리스 노트](#)를 참조하십시오.

2025년 6월

2022년 6월 12일

Cisco Security Cloud Control 통합 플랫폼 사용 가능

APJ, 호주, 유럽연합, 인도 및 미국 지역의 Cisco Security Cloud Control 테넌트 고객을 Cisco Security Cloud Control 통합 플랫폼으로 마이그레이션을 기쁜 마음으로 알려드립니다.

Security Cloud Control 통합 플랫폼에 액세스하려면 <https://security.cisco.com/>으로 이동하여 홈페이지에서 **Products(제품)**> **Firewall(방화벽)** 로 이동합니다.

Security Cloud Control 통합 플랫폼의 방화벽 대시보드에서 현재의 모든 방화벽 설정 및 구성에 계속 액세스할 수 있습니다.

단순화된 사이트 간 VPN 마법사

Security Cloud Control에는 사이트 간 VPN 터널 생성을 간소화하고 가속화하도록 설계된 향상된 통합 마법사가 있습니다. 이 직관적인 단계별 마법사를 통해 클릭 몇 번으로 여러 VPN 연결을 원활하게 구성하고 관리할 수 있습니다. VPN 터널 생성은 Secure Firewall ASA, 클라우드 제공 Firewall Management Center 매니지드 Firewall Threat Defense, 멀티 클라우드 방어 및 엑스트라넷 디바이스에 대해 지원되어 VPN 관리에 대한 중앙 집중식 및 간소화된 접근 방식을 제공합니다.

자세한 정보는 [사이트 간 가상 프라이빗 네트워크](#)를 참조하십시오.

사용률 대시보드의 새 위젯

로깅 추세를 식별하고 스토리지를 효과적으로 관리하는 데 도움이 되는 새로운 위젯을 도입했습니다. 이러한 위젯은 최적화된 버전의 SAL 이벤트 로깅을 사용하는 경우에만 사용할 수 있습니다.

- 이벤트 수집 속도 추적을 위한 EPS Trends(EPS 동향).
- 사용 패턴 모니터링에서 이벤트 유형별 사용률 및 디바이스 유형 동향을 사용할 수 있습니다.

- 디바이스별 사용량 동향: 주요 디바이스의 스토리지 사용 현황을 보여줍니다.

자세한 내용은 [보안 분석 및 로깅 이벤트 스토리지](#)를 참조하십시오.

2025년 4월

2025년 4월 23일

클라우드 제공 **Firewall Management Center**에서 관리하는 **Secure Firewall Threat Defense** 디바이스 버전 **7.0.x** 지원 종료

2025년 10월 22일 이후 클라우드 제공 Firewall Management Center는 버전 7.0.x를 실행하는 Secure Firewall Threat Defense 디바이스의 관리를 더 이상 지원하지 않습니다. 지속적인 보호 및 최신 기능 이용을 보장하기 위해 2025년 10월 22일 이전에 버전 7.2.x 이상(Cisco 제안 버전은 7.4.2)으로 업그레이드해야 합니다.

2025년 10월 22일부터 업데이트 또는 등록 취소를 제외하고 버전 7.0.x를 실행하는 Secure Firewall Threat Defense 디바이스를 변경하거나 구축할 수 없습니다.

자세한 내용은 [FAQ\(자주 묻는 질문\)](#)를 참조하십시오.

2025년 4월 10일

AI0ps의 모범 사례 및 권장 사항

모범 사례 및 권장 사항 기능은 디바이스에서 평가를 실행하고, 실패한 확인을 강조 표시하며, 자세한 보고서를 생성합니다. Cisco Secure Firewall 모범 사례를 준수하고 전반적인 성능을 개선할 수 있는 수정 조치를 권장합니다.

자세한 내용은 [모범 사례 및 권장 사항 구현](#)을 참고하십시오.

2025년 3월

2025년 3월 13일

클라우드 제공 **Firewall Management Center**로 업데이트

Security Cloud Control는 클라우드 제공 Firewall Management Center의 업데이트를 릴리스했습니다. 자세한 내용은 [FTD를 클라우드 제공 Firewall Management Center로 마이그레이션](#)을 참조하십시오.

2025년 3월 6일

Firewall 마이그레이션 툴에 대한 업데이트

Security Cloud Control은 Firewall 마이그레이션 툴의 업데이트된 버전을 호스팅합니다. 새로운 기능에는 Secure Firewall ASA 및 Palo Alto Networks 방화벽에서 Multicloud Defense로 구성 마이그레이션이 포함됩니다.

자세한 정보는 [Cisco Secure Firewall 마이그레이션 툴 릴리스 노트](#)를 참조하십시오.

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.