



Cisco Security Cloud Control: Cisco Meraki

Cisco Security Cloud Control
Updated July 12, 2026



© 2021–2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

제

1

장

:

- Security Cloud Control Meraki
- Cisco Security Cloud Control
- Security Cloud Control
- Security Cloud Control Firewall Management
- Firewall Management

Security Cloud Control Firewall Management (이전 Cisco Defense Orchestrator)는 시스코 방화벽 및 기타 디바이스에서 정책을 간소화하고 통합하는 클라우드 기반 보안 정책 플랫폼입니다. 정책 일관성을 간소화하고 직관적이면서도 고급 인터페이스를 제공하며, 여러 디바이스 관리자 간 구성 변경 사항을 조정합니다.

Security Cloud Control Meraki

지원되는 Meraki MX 활용 사례와 기본 설정 및 구성 작업을 포함하여 Security Cloud Control의 Cisco Meraki 관리에 대한 개요입니다.

Meraki 디바이스를 Security Cloud Control에 온보딩하면 Security Cloud Control은 Meraki 대시보드와 통신하여 해당 디바이스를 관리합니다. Security Cloud Control은 MX 디바이스와 직접 통신하지 않습니다.

Security Cloud Control은 구성 요청을 Meraki 대시보드로 안전하게 전송하며, Meraki 대시보드는 새 구성을 디바이스에 적용합니다. 자세한 내용은 [Security Cloud Control가 Meraki와 통신하는 방법](#) 페이지 5를 참조하십시오.

Security Cloud Control은 개체 및 정책의 문제를 식별하고 가능한 수정 또는 대체 옵션을 생성하여 Meraki 환경을 최적화하는 데 도움이 됩니다. 이는 디바이스 및 템플릿 모두에 연결된 정책에 적용됩니다. Security Cloud Control 사용 방법:

- 하나 이상의 Meraki 디바이스에서 정책을 동시에 관리합니다.
- 포괄적인 환경에서 FTD 및 ASA 디바이스와 함께 Meraki 정책 또는 템플릿을 모니터링하고 관리합니다.
- Meraki 템플릿을 사용하여 여러 네트워크를 관리합니다.
- FTD 및 ASA 디바이스와 같이 지원되는 다른 플랫폼에서 호환되는 개체로 액세스 규칙을 맞춤화합니다.

Meraki MX

Security Cloud Control에 디바이스를 온보딩하기 전에 Meraki 대시보드에서 어카운트를 생성하고 대시보드에 디바이스 또는 템플릿을 온보딩해야 합니다. 조직의 Meraki 대시보드에 어카운트가 없는 경우 API 토큰을 생성할 수 없으며 디바이스가 Security Cloud Control과 통신하지 않습니다.

[Meraki MX 디바이스](#) 또는 [Meraki 템플릿](#)을 Security Cloud Control에 온보딩할 수 있습니다.

Security Cloud Control 콘솔을 통해 Meraki MX 로그인 자격 증명 및 권한을 처리합니다. 올바른 자격 증명 또는 권한이 없으면 Security Cloud Control가 Meraki 디바이스와 통신할 수 없습니다.

자세한 내용은 [Meraki MX 자격 증명 업데이트](#) 및 [Meraki API 키 생성 및 검색](#)을 참조하십시오.

Meraki 3 Security Cloud Control

현재 Security Cloud Control은 레이어 3 방화벽 규칙만 지원합니다. 레이어 3 규칙은 OSI 모델의 네트워크 레이어에서 정책을 적용합니다. 자세한 내용은 [레이어 3 방화벽 규칙 사용](#)을 참조하십시오.

Meraki 대시보드에서 레이어 3 아웃바운드 규칙을 생성할 수 있습니다. 디바이스를 Security Cloud Control에 온보딩하면 Security Cloud Control은 Meraki 대시보드에서 정의한 레이어 3 규칙을 읽습니다. 그런 다음 Security Cloud Control에서 FTD 또는 ASA 규칙을 관리하는 것처럼 이러한 규칙을 관리할 수 있습니다. 자세한 내용은 [Meraki 액세스 제어 정책 관리](#)를 참조하십시오.

개체를 사용하여 새 액세스 제어 정책을 세부적으로 조정합니다. Meraki 대시보드는 프로토콜과 IP 주소 또는 IP 주소 범위 그룹을 사용합니다. 반면 Security Cloud Control은 다양한 개체를 사용하여 규칙을 관리합니다. Security Cloud Control가 Meraki 프로토콜을 개체로 전송하는 방법에 대한 자세한 내용은 [Meraki 디바이스와 연결된 개체](#)를 참조하십시오. Security Cloud Control에서 다음 개체를 생성할 수 있으며, 이 개체는 Meraki 대시보드에서 IP 그룹으로 변환됩니다:

- 네트워크 개체 또는 개체 그룹
- 네트워크 서비스(포트) 개체

Meraki 대시보드에서 레이어 3 아웃바운드 규칙을 생성할 수 있습니다. Security Cloud Control은 Security Cloud Control에 디바이스를 온보딩할 때 Meraki 대시보드에서 정의한 레이어 3 규칙을 읽습니다. 그런 다음 Security

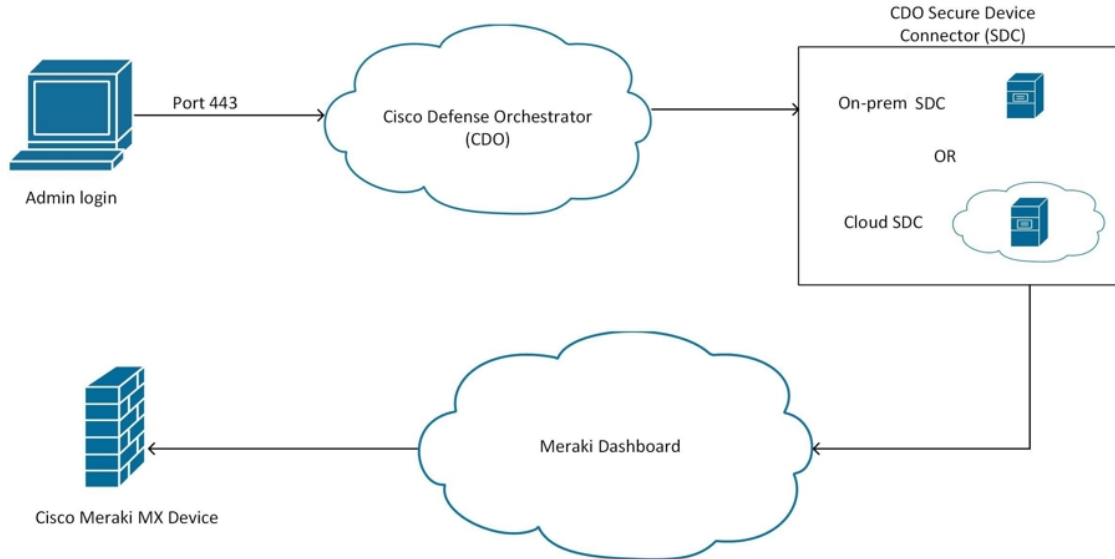
Cloud Control에서 FTD 또는 ASA 규칙을 관리하는 것처럼 이러한 규칙을 관리할 수 있습니다. Meraki 액세스 제어 정책에 대한 자세한 내용은 [Meraki Access 제어 정책 관리](#)를 참조하십시오.

Security Cloud Control Meraki

Security Cloud Control에서 Meraki 디바이스에 구축을 포함하여 Security Cloud Control가 Meraki와 어떻게 통신하는지에 대한 개요입니다. Security Cloud Control은 구성 변경 사항을 Meraki MX 디바이스에 직접 구축하지 않습니다.

Security Cloud Control에서 Meraki 디바이스에 구축

Security Cloud Control은 구성 변경 사항을 Meraki MX 디바이스에 직접 구축하지 않습니다. 구축은 여러 단계 프로세스입니다. 아래 다이어그램은 구축 프로세스를 보여줍니다.



Meraki MX 디바이스에 대해 Security Cloud Control에서 변경하는 구성은 구축을 결정할 때까지 Security Cloud Control에서 스테이징됩니다. 구성 변경 사항을 구축하면 Security Cloud Control은 해당 변경 사항을 Meraki 대시보드로 전달하고, Meraki 대시보드는 Meraki MX 디바이스에 변경 사항을 구현합니다. Security Cloud Control은 방화벽 정책을 관리하고 Meraki 대시보드는 정책이 적용되는 네트워크를 관리합니다. 두 작업 모두 Meraki MX 디바이스가 네트워크 트래픽을 관리하고 처리하는 방식에 영향을 미칩니다.

이전 테넌트가 있는 일부 고객은 SDC를 통해 Meraki MX 디바이스를 Security Cloud Control에 연결할 수 있습니다. 이러한 고객인 경우 이 방법을 계속 사용하거나 Meraki MX를 다시 온보딩하거나 연결 자격 증명을 업데이트하여 SDC를 제거할 수 있습니다. Security Cloud Control를 Meraki MX에 연결하는 데 SDC가 필요하지 않습니다.

Security Cloud Control과 Meraki 대시보드의 한 가지 차이점은 개체를 사용한다는 것입니다. Meraki 대시보드에서 생성된 규칙의 경우 Security Cloud Control은 Meraki IP 주소 그룹 또는 IP 주소 범위를 규칙 및 디바이스 정책에 연결하거나 연결할 수 있는 개체로 변환합니다. Security Cloud Control에서 생성된 개체를 Meraki 어플라이언스에 구축할 때 Meraki 대시보드는 해당 개체를 다시 IP 주소 그룹 또는 범위로 변환합니다. Security Cloud Control의 개체는 다른 디바이스 플랫폼과 호환되므로 고유하고 다양합니다. 다른 디바이스가 Security Cloud Control에 온보딩된 경우 모든 디바이스에 대해 단일 개체를 생성할 수 있습니다. Meraki 디바이스와 연결된 개체에 대한 자세한 내용은 [Meraki 디바이스와 연결된 개체](#) 페이지 84를 참조하십시오.

Cisco Security Cloud Control

통합된 Cisco 보안 제품의 온보딩, 관리 및 탐색을 위한 통합 플랫폼으로서 Cisco Security Cloud Control의 개요입니다.

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

보안 제품을 통합하는 것은 간소화된 경험입니다. 시스코 보안 제품에 대한 구독을 구매하고 나면 구매한 모든 구독에 대한 단일 클레임 코드가 포함된 단일 이메일을 받게 됩니다. 새 **Security Cloud Control** 조직에 클레임 코드를 입력하면 모든 제품이 **Security Cloud Control**로 동시에 프로비저닝됩니다.

Security Cloud 제어 내에서 사용자 및 그룹 관리가 플랫폼 수준에서 이루어집니다. **Security Cloud Control** 이러한 사용자 및 그룹에 역할을 할당하여 **Security Cloud Control** 및 통합 제품을 관리할 수 있는 권한을 정의합니다.

제품과 톨 간의 탐색은 직관적이며 모든 통합 제품에 대한 공통 플랫폼 메뉴 및 톨바 사용하여 표준화되었습니다.

Security Cloud Control는 플랫폼의 모든 통합 제품에 다음과 같은 추가 핵심 서비스를 제공합니다:

- **플랫폼 관리:** 역할 기반 액세스 제어 관리, 구독 클레임 및 제품 인스턴스의 표준화된 지역 구축과 같은 공통 서비스를 **Security Cloud Control**에서 제공합니다. **Security Cloud Control**는 이러한 기능을 중앙 집중화하여 플랫폼에서 관리되는 모든 **Cisco** 보안 제품에서 액세스를 프로비저닝하고 관리하는 데 있어 일관된 사용자 경험을 보장합니다. **Security Cloud Control**의 기본 내비게이션 바에 있는 플랫폼 관리 메뉴에서 이러한 공통 서비스에 접근할 수 있습니다.
- **AI Assistant:** **Security Cloud Control**의 **Cisco AI Assistant** AI 기반 인사이트, 자동화 및 상황별 지침을 제공하여 보안 운영을 간소화 하도록 설계되었습니다. 방화벽, **Duo**, 및 **Secure Access**를 비롯한 **Cisco** 보안 제품 전반에서 보안 정책을 관리하고, 문제를 해결하고, 설정을 최적화하는 데 도움이 됩니다. 어시스턴트는 자연어 처리 및 플랫폼 간 인텔리전스를 활용하여 효율성을 높이고 사고 대응을 가속화하며 보안 워크플로우를 간소화합니다.
- **Global Search(전역검색):** 플랫폼의 제품 전체에서 값을 검색할 수 있는 기능입니다.
- **Shared Objects(공유 개체):** 디바이스 및 정책 전체에서 공유할 수 있는 개체를 생성하고 관리합니다.
- **Unified documentation portal(통합문서 포털):** 하나의 포털에서 모든 문서에 액세스할 수 있는 문서 "도움말" 환경입니다.

Security Cloud Control

Security Cloud Control에서 다음 모든 보안 제품을 관리할 수 있습니다.

- AI Defense
- Security Cloud Control Firewall Management
- Multicloud Defense
- Secure Access

Security Cloud Control

Security Cloud Control에서 이러한 보안 제품을 실행할 수 있습니다. 이러한 제품은 출시 후에는 독립형 제품으로 작동하며 **Security Cloud Control**를 통해 관리할 수 없습니다. **Security Cloud Control**에서 그러한 제품의 라이선스를 요청하거나 비활성화만 할 수 있습니다.

Security Cloud Control 톨바에서 9개의 점으로 이루어진 메뉴 를 클릭하여 다음 제품을 실행합니다.

- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Cisco Duo
- Cisco XDR

Security Cloud Control

Security Cloud Control에서 지원하는 제품 및 솔루션과 플랫폼에서 통합하거나 실행하는 방법에 대해 알아봅니다.

현재 Security Cloud Control와 통합할 수 있는 제품은 다음과 같습니다.

AI Defense: AI Defense는 AI 사용자 및 제공자의 위험을 해결합니다. Security Cloud Control, AI Defense 에서 네트워크 가시성 및 시행 지점을 사용하여 분산형 클라우드 환경에서 승인된 AI 워크로드, 승인되지 않은 AI 워크로드, 애플리케이션, 모델, 데이터 및 사용자 액세스를 검색하기 위한 탐지 및 시행 조치를 추가합니다. AI 기반 서비스를 개발하고 제공하는 조직을 위해 AI Defense는 AI 모델이 제공되기 전에 취약점을 탐지합니다. 실행 중인 AI 애플리케이션의 경우 AI Defense 가드레일은 신속한 주입, 서비스 거부, 데이터 유출 등 빠르게 진화하는 위협을 차단합니다. 자세한 내용은 [AI Defense 문서](#)를 참조하십시오.

Security Cloud Control Firewall Management: Security Cloud Control Firewall Management (이전 Cisco Defense Orchestrator)는 Cisco 방화벽 및 기타 디바이스에서 정책을 간소화하고 통합하는 클라우드 기반 보안 정책 관리 자입니다. 자세한 내용은 [보안 클라우드의 방화벽 제어 설명서](#)를 참조하십시오.

Multicloud Defense: Multicloud Defense 는 멀티 클라우드 보안에 대한 간소화된 고도로 자동화된 접근 방식을 제공합니다. 이 솔루션을 사용하면 조직은 단일 SaaS 제공 컨트롤 플레인 및 중앙 집중식 또는 분산형 PaaS 제공 데이터 플레인 아키텍처를 사용하여 멀티 클라우드 환경을 관리하고 보호할 수 있습니다. Multicloud Defense 는 모든 주요 클라우드 제공자에 걸쳐 지속적인 가시성, 통합 보호 및 유동 정책 업데이트를 제공하므로 각 클라우드 제공자를 위한 솔루션에 대해 별도의 포인트 솔루션이 필요하지 않습니다. 자세한 내용은 [Multicloud Defense 설명서](#)를 참조하십시오.

Secure Access: Cisco Secure Access는 인터넷 기반 위협에 대한 여러 수준의 방어를 제공하는 클라우드 기반 플랫폼입니다. 조직의 네트워크 또는 로밍 오프네트워크 상태에서 인터넷, SaaS 애플리케이션 및 사설 디지털 리소스에 안전하게 연결합니다. 정책 규칙을 사용하여 리소스, 사용자, 디바이스 모음에 대해 보안 제어를 구성하고 시행합니다. 자세한 내용은 [Secure Access 설명서](#)를 참조하십시오. Secure Access 구독에는 추가 비용 없이 Security Cloud Control를 통한 ID 인텔리전스 통합이 포함되며, 독립형 ID 인텔리전스 대시보드에 대한 액세스는 포함되지 않습니다. 자세한 내용은 [Cisco Identity Intelligence와 Secure Access 통합](#)을 참조하십시오.

Cisco XDR(Extended Detection and Response): Cisco XDR는 보안 운영을 간소화하고 사고 대응을 가속화하도록 설계된 클라우드 네이티브, 확장 가능한 보안 솔루션입니다. 엔드포인트, 네트워크, 방화벽, 이메일, ID, DNS 등 여러 소스의 텔레메트리 수집 및 분석하여 Cisco Talos의 강화된 컨텍스트 및 위협 인텔리전스를 통해 정교한 위협을 탐지합니다.

Cisco XDR는 잠재적인 위협과 영향을 기반으로 위협의 우선순위를 지정하고 오탐을 줄이며 AI 기반 지침 및 자동화를 제공하여 조사 및 대응 절차를 간소화합니다. 이 통합 접근 방식을 통해 Security Operations Center(SOC) 팀은 멀티 벡터, 멀티 벤더 환경에서 Cisco 및 서드파티 보안 툴을 모두 통합하여 더 빠르게 행동하고 생산성을 향상하며 보안 탄력성을 구축할 수 있습니다. 자세한 내용은 [Cisco XDR 도움말 센터](#)를 참조하십시오.

Security Cloud Control Firewall Management

방화벽 디바이스, 정책, 개체 및 구성 일관성을 관리하는 데 사용되는 Security Cloud Control Firewall Management의 개요입니다.

Security Cloud Control Firewall Management(이전 명칭은 Cisco Defense Orchestrator)은 분산 환경에서 보안 정책 관리를 간소화합니다. 매니지드 방화벽 및 디바이스 전체에서 정책을 일관된 상태로 유지하는 데 도움이 됩니다. Security Cloud Control에서는 **Products(제품)** 아래에 **Firewall(방화벽)**이 나타납니다.

Security Cloud Control Firewall Management는 보안 정책의 불일치를 식별하고 해결 도구를 제공하여 보안 정책을 최적화하는 데 도움이 됩니다. 또한 개체 공유, 정책 공유 및 설정 템플릿을 지원하므로 디바이스 전체에 일관된 설정을 적용할 수 있습니다.

Security Cloud Control Firewall Management는 ASDM(Adaptive Security Device Manager)과 같은 로컬 디바이스 관리자 와 함께 사용할 수 있습니다. 다른 관리자가 수행한 구성 변경 사항을 추적하고 필요한 경우 차이점을 조정합니다.

이 플랫폼에는 Threat Defense 디바이스를 온프레미스 방화벽 Management Center 또는 클라우드 제공 Firewall Management Center에 연결할 수 있도록 도와주는 안내형 'Day 0' 경험이 포함되어 있습니다. 주요 기능을 강조 표시하고 해당 기능을 활성화 및 구성하는 데 도움이 됩니다.

디바이스를 온보딩하기 전에 다음 사전 요건을 완료합니다.

- 설치 마법사를 완료합니다.
- 디바이스에 라이선스를 할당합니다.

이러한 사전 요건을 완료한 후, Security Cloud Control Firewall Management 온보딩 마법사를 사용하여 디바이스를 온보딩합니다.

다음 제한 사항에 유의하십시오.

- 조직에 연결된 Security Cloud Control Firewall Management에 디바이스를 온보딩한 후에는 한 조직에서 다른 조직으로 디바이스를 마이그레이션할 수 없습니다.
- 디바이스를 새 조직으로 이동하려면 새 조직에 다시 온보딩해야 합니다.

Cisco

Cisco Systems, Inc. 및 자회사("Cisco"로 통칭)에서는 개인 정보를 보호하고 사용자가 Cisco 웹사이트에서 그리고 시스코 제품 및 서비스("솔루션")의 사용에서 유익한 경험을 할 수 있도록 최선을 다하고 있습니다. [Cisco 온라인 개인정보 보호정책](#)을 주의 깊게 읽고 Cisco에서 개인 정보를 수집, 사용, 공유 및 보호하는 방법을 명확하게 이해하십시오.

Firewall Management

방화벽 관리 대시보드를 사용하여 테넌트 수준 인사이트, 알림, 작업, 재고 목록, VPN 활동, 변경 로그 및 보안 이벤트를 보는 방법을 알아봅니다.

Firewall 대시보드는 다양한 범주에서 테넌트 레벨 세부 정보를 모니터링하고 관리하기 위한 중앙 허브입니다. 로그인하면 중요한 인사이트와 보안 및 운영 효율성 최적화하기 위한 작업을 제공하는 맞춤형 대시보드에 액세스할 수 있습니다.

왼쪽 창에서 **Dashboard**(대시보드)를 클릭합니다.

대시보드 사용자 맞춤화

표시되는 위젯을 맞춤 설정하여 대시보드를 특정 요구 사항에 맞게 조정합니다.

1. Home 페이지에서 **Customize**(맞춤화)를 클릭합니다.
2. 대시보드에 표시할 위젯을 선택하거나 선택을 해제합니다.
3. 위젯을 끌어다 놓아 원하는 대로 정렬할 수 있습니다.

대시보드는 **Top Insights & Alerts**(주요 인사이트 및 알림), **Top Actions**(주요 조치) 및 **Top Information**(주요 정보)의 세 가지 주요 섹션으로 나뉩니다. 각 섹션은 최적의 보안 및 운영 통제를 유지하는 데 도움이 되는 다양한 범주의 통찰력을 제공합니다.

인사이트 및 알림

테넌트에 **AgenticOps**인사이트가 활성화된 경우에만 이 섹션이 표시됩니다. Elephant 플로우로 인한 높은 트래픽, RA VPN 예측, 액세스 제어 정책 이상, 높은 CPU 및 메모리 사용량, 스노트 CPU 및 메모리 사용량과 관련된 인사이트를 확인할 수 있습니다.

상위 작업

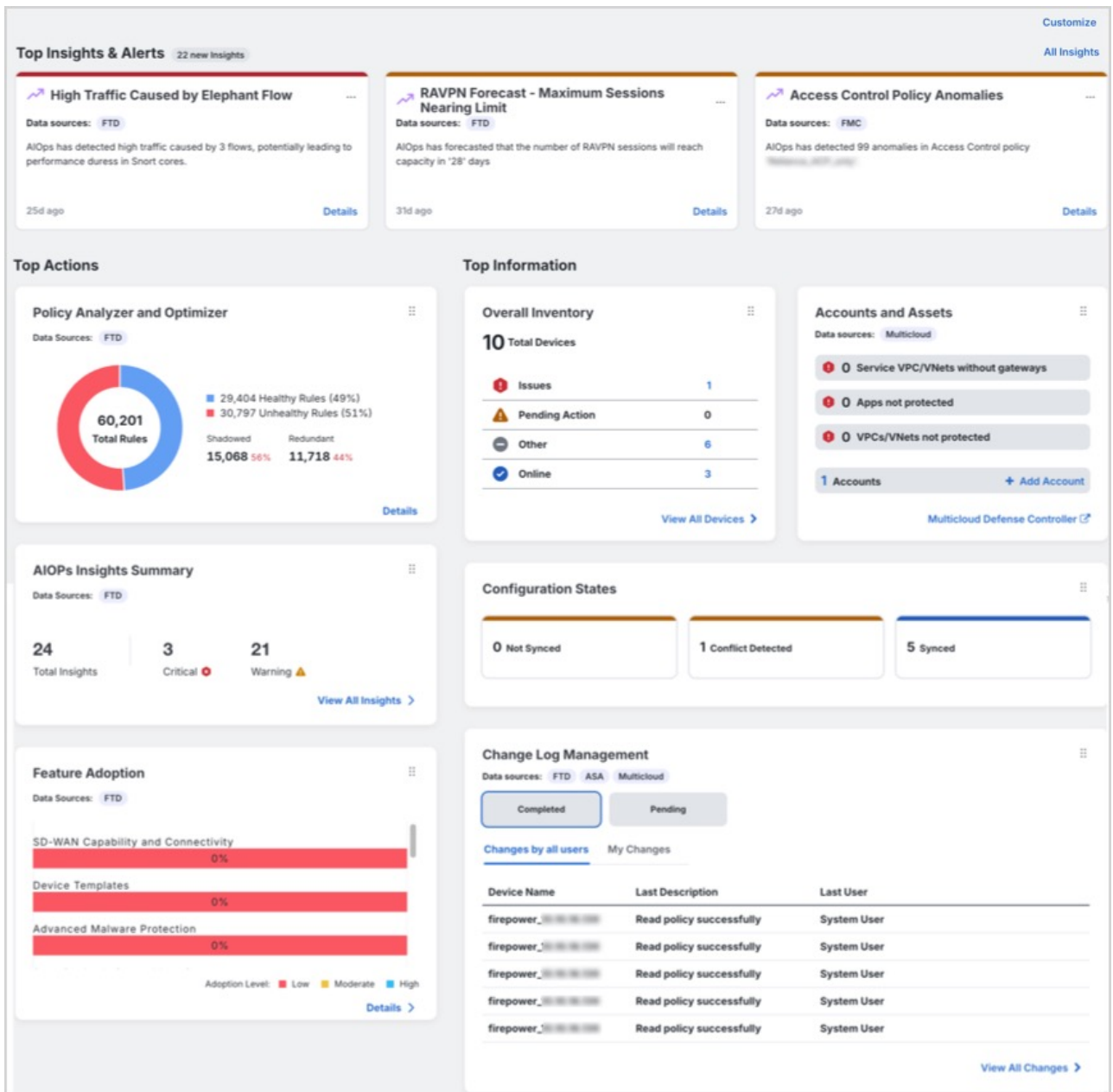
테넌트에 **AgenticOps** 인사이트가 활성화된 경우에만 이 섹션이 표시됩니다. 활성화된 경우 다음 위젯을 볼 수 있습니다.

- **Policy Analyzer and Optimizer**(정책 분석기 및 옵티마이저): 방화벽 성능을 개선하기 위한 보안 정책을 분석하고 이상 징후를 탐지하며 최적화 권장 사항을 제공합니다.
자세한 내용은 [Policy Analyzer and Optimizer\(정책 분석기 및 옵티마이저\)](#)를 참조하십시오.
- **AgenticOps** 인사이트: 구성, 상태 및 운영, 트래픽 및 용량 등 범주별로 활성 인사이트와 추세를 표시합니다.
자세한 내용은 [AgenticOpsInsights\(인사이트\)](#)를 참조하십시오.
- 기능 채택: 사용량을 평가하고 개선할 수 있도록 기능 채택률을 표시합니다.
자세한 내용은 [기능 채택 평가 및 개선](#)을 참조하십시오.

상위 정보

이 섹션에서는 다양한 테넌트 수준 메트릭에 대한 상세한 인사이트를 제공합니다. 테넌트에 대해 활성화된 기능에 따라 다음 위젯을 볼 수 있습니다.

- **Configuration Status**(구성 상태): 불일치 또는 충돌을 식별할 수 있도록 디바이스 구성을 Security Cloud Control에서 유지 관리하는 구성과 비교합니다.
자세한 내용은 [디바이스 관리](#)를 참조하십시오.
- **Change Log Management**(변경 로그 관리): 운영 변경 사항을 추적할 수 있도록 완료된 변경 로그와 보류 중인 변경 로그를 표시합니다. 위젯에 **Completed**(완료됨) 및 **Pending**(보류 중) 변경 로그가 표시됩니다.
자세한 내용은 [Change Logs\(변경 로그\)](#)를 참조하십시오.
- **RA VPN Sessions**(RA VPN 세션): 원격 액세스 VPN 세션 활동을 표시합니다.
자세한 내용은 [RA VPN 세션](#)을 참조하십시오.
- **Overall Inventory**(전체 재고 목록): 총 디바이스 수를 표시하고 Issues(문제), Pending Actions(보류 중인 작업), Other(기타) 및 Online(온라인)별로 그룹화합니다.
자세한 내용은 [All Devices\(모든 디바이스\)](#)를 참조하십시오.
- **Site-to-Site VPN**(사이트 간 VPN): 총 VPN 터널 수와 Active(활성) 및 Idle(유휴) 상태인 터널의 비율을 표시합니다. 위젯에 총 VPN 터널 수와 **Active**(활성) 및 **Idle**(유휴)의 비율이 표시됩니다.
자세한 내용은 [사이트 간 VPN](#)을 참조하십시오.
- **어카운트 및 자산**:
 - 멀티 클라우드 어카운트 및 리소스를 효과적으로 추적하고 관리할 수 있습니다. 여기에서 **Multicloud Defense** 컨트롤러를 실행할 수 있습니다.
 - **+Add Account**(+어카운트 추가)를 클릭하여 새 어카운트를 추가합니다.
 자세한 내용은 [Multicloud Defense Controller](#)를 참조하십시오.
- **Top Risky Destinations**(상위 위험한 대상): 액세스 권한이 부여된 상위 위험한 대상을 식별하고 모니터링하는 데 도움이 됩니다. 위젯은 애플리케이션 및 URL 범주를 나열하며, 지난 90일, 60일 또는 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 트래픽(기본값)과 차단된 트래픽 사이에서 필터링할 수 있습니다.
- **Top Intrusion and Malware Events**(상위 침입 및 멀웨어 이벤트): 상위 침입 및 멀웨어 이벤트를 모니터링하고 대응할 수 있습니다. 위젯은 침입 이벤트와 멀웨어 이벤트를 표시하며, 지난 90일, 60일, 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 이벤트(기본값)와 차단된 이벤트 사이에서 필터링할 수 있습니다.



발표

최신 **Security Cloud Control** 기능 및 업데이트를 보려면 알림 아이콘을 클릭합니다. 목록에 있는 항목에 대한 추가 정보가 필요할 경우 관련 문서 링크가 제공됩니다.

제

2 Security Cloud Control Firewall Management

장

:

- Cisco Security Cloud Control □□
- Security Cloud Control Firewall Management □□
- □□□□ □□ Firewall Management Center □□
- Security Cloud Control Firewall Management □□□□□
- Security Cloud Control Firewall Management □□
- Firewall Management □□□□

조직에 대한 방화벽 관리를 프로비저닝하고, 방화벽 애플리케이션을 연 다음, 환경을 모니터링 및 관리하는 데 도움이 되는 대시보드 섹션을 검토합니다.

이 장에서는 **Security Cloud Control Firewall Management** 내에서 방화벽 관리를 프로비저닝하는 단계와 액세스 방법을 설명합니다. 또한 방화벽 대시보드의 개요를 제공합니다.

Cisco Security Cloud Control

통합된 Cisco 보안 제품의 온보딩, 관리 및 탐색을 위한 통합 플랫폼으로서 Cisco Security Cloud Control의 개요입니다.

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

보안 제품을 통합하는 것은 간소화된 경험입니다. 시스코 보안 제품에 대한 구독을 구매하고 나면 구매한 모든 구독에 대한 단일 클레임 코드가 포함된 단일 이메일을 받게 됩니다. 새 Security Cloud Control 조직에 클레임 코드를 입력하면 모든 제품이 Security Cloud Control로 동시에 프로비저닝됩니다.

Security Cloud 제어 내에서 사용자 및 그룹 관리가 플랫폼 수준에서 이루어집니다. Security Cloud Control 이러한 사용자 및 그룹에 역할을 할당하여 Security Cloud Control 및 통합 제품을 관리할 수 있는 권한을 정의합니다.

제품과 툴 간의 탐색은 직관적이며 모든 통합 제품에 대한 공통 플랫폼 메뉴 및 툴바 사용하여 표준화되었습니다.

Security Cloud Control는 플랫폼의 모든 통합 제품에 다음과 같은 추가 핵심 서비스를 제공합니다:

- **플랫폼 관리:** 역할 기반 액세스 제어 관리, 구독 클레임 및 제품 인스턴스의 표준화된 지역 구축과 같은 공통 서비스를 Security Cloud Control에서 제공합니다. Security Cloud Control은 이러한 기능을 중앙 집중화하여 플랫폼에서 관리되는 모든 Cisco 보안 제품에서 액세스를 프로비저닝하고 관리하는 데 있어 일관된 사용자 경험을 보장합니다. Security Cloud Control의 기본 내비게이션 바에 있는 플랫폼 관리 메뉴에서 이러한 공통 서비스에 접근할 수 있습니다.
- **AI Assistant:** Security Cloud Control의 Cisco AI Assistant AI 기반 인사이트, 자동화 및 상황별 지침을 제공하여 보안 운영을 간소화 하도록 설계되었습니다. 방화벽, Duo, 및 Secure Access를 비롯한 Cisco 보안 제품 전반에서 보안 정책을 관리하고, 문제를 해결하고, 설정을 최적화하는 데 도움이 됩니다. 어시스턴트는 자연어 처리 및 플랫폼 간 인텔리전스를 활용하여 효율성을 높이고 사고 대응을 가속화하며 보안 워크플로우를 간소화합니다.
- **Global Search(전역검색):** 플랫폼의 제품 전체에서 값을 검색할 수 있는 기능입니다.
- **Shared Objects(공유 개체):** 디바이스 및 정책 전체에서 공유할 수 있는 개체를 생성하고 관리합니다.
- **Unified documentation portal(통합문서 포털):** 하나의 포털에서 모든 문서에 액세스할 수 있는 문서 "도움말" 환경입니다.

Security Cloud Control

Security Cloud Control에서 다음 모든 보안 제품을 관리할 수 있습니다.

- AI Defense
- Security Cloud Control Firewall Management
- Multicloud Defense
- Secure Access

Security Cloud Control

Security Cloud Control에서 이러한 보안 제품을 실행할 수 있습니다. 이러한 제품은 출시 후에는 독립형 제품으로 작동하며 Security Cloud Control를 통해 관리할 수 없습니다. Security Cloud Control에서 그러한 제품의 라이선스를 요청하거나 비활성화만 할 수 있습니다.

Security Cloud Control 툴바에서 9개의 점으로 이루어진 메뉴 를 클릭하여 다음 제품을 실행합니다.

- Cisco Secure Email Threat Defense

- Cisco Secure Endpoint
- Cisco Duo
- Cisco XDR

Security Cloud Control

Security Cloud Control에서 지원하는 제품 및 솔루션과 플랫폼에서 통합하거나 실행하는 방법에 대해 알아보니다.

현재 Security Cloud Control과 통합할 수 있는 제품은 다음과 같습니다.

AI Defense: AI Defense는 AI 사용자 및 제공자의 위험을 해결합니다. Security Cloud Control, AI Defense 에서 네트워크 가시성 및 시행 지점을 사용하여 분산형 클라우드 환경에서 승인된 AI 워크로드, 승인되지 않은 AI 워크로드, 애플리케이션, 모델, 데이터 및 사용자 액세스를 검색하기 위한 탐지 및 시행 조치를 추가합니다. AI 기반 서비스를 개발하고 제공하는 조직을 위해 AI Defense는 AI 모델이 제공되기 전에 취약점을 탐지합니다. 실행 중인 AI 애플리케이션의 경우 AI Defense 가드레일은 신속한 주입, 서비스 거부, 데이터 유출 등 빠르게 진화하는 위협을 차단합니다. 자세한 내용은 [AI Defense 문서](#)를 참조하십시오.

Security Cloud Control Firewall Management: Security Cloud Control Firewall Management (이전 Cisco Defense Orchestrator)는 Cisco 방화벽 및 기타 디바이스에서 정책을 간소화하고 통합하는 클라우드 기반 보안 정책 관리 자입니다. 자세한 내용은 [보안 클라우드의 방화벽 제어 설명서](#)를 참조하십시오.

Multicloud Defense: Multicloud Defense 는 멀티 클라우드 보안에 대한 간소화된 고도로 자동화된 접근 방식을 제공합니다. 이 솔루션을 사용하면 조직은 단일 SaaS 제공 컨트롤 플레인 및 중앙 집중식 또는 분산형 PaaS 제공 데이터플레인 아키텍처를 사용하여 멀티 클라우드 환경을 관리하고 보호할 수 있습니다. Multicloud Defense 는 모든 주요 클라우드 제공자에 걸쳐 지속적인 가시성, 통합 보호 및 유동 정책 업데이트를 제공하므로 각 클라우드 제공자를 위한 솔루션에 대해 별도의 포인트 솔루션이 필요하지 않습니다. 자세한 내용은 [Multicloud Defense 설명서](#)를 참조하십시오.

Secure Access: Cisco Secure Access는 인터넷 기반 위협에 대한 여러 수준의 방어를 제공하는 클라우드 기반 플랫폼입니다. 조직의 네트워크 또는 로밍 오프네트워크 상태에서 인터넷, SaaS 애플리케이션 및 사설 디지털 리소스에 안전하게 연결합니다. 정책 규칙을 사용하여 리소스, 사용자, 디바이스 모음에 대해 보안 제어를 구성하고 시행합니다. 자세한 내용은 [Secure Access 설명서](#)를 참조하십시오. Secure Access 구독에는 추가 비용 없이 Security Cloud Control를 통한 ID 인텔리전스 통합이 포함되며, 독립형 ID 인텔리전스 대시보드에 대한 액세스는 포함되지 않습니다. 자세한 내용은 [Cisco Identity Intelligence와 Secure Access 통합](#)을 참조하십시오.

Cisco XDR(Extended Detection and Response): Cisco XDR는 보안 운영을 간소화하고 사고 대응을 가속화하도록 설계된 클라우드 네이티브, 확장 가능한 보안 솔루션입니다. 엔드포인트, 네트워크, 방화벽, 이메일, ID, DNS 등 여러 소스의 텔레메트리 수집 및 분석하여 Cisco Talos의 강화된 컨텍스트 및 위협 인텔리전스를 통해 정교한 위협을 탐지합니다.

Cisco XDR는 잠재적인 위협과 영향을 기반으로 위협의 우선순위를 지정하고 오탐을 줄이며 AI 기반 지킴 및 자동화를 제공하여 조사 및 대응 절차를 간소화합니다. 이 통합 접근 방식을 통해 Security Operations Center(SOC) 팀은 멀티 벡터, 멀티 벤더 환경에서 Cisco 및 서드파티 보안 툴을 모두 통합하여 더 빠르게 행동하고 생산성을 향상하며 보안 탄력성을 구축할 수 있습니다. 자세한 내용은 [Cisco XDR 도움말 센터](#)를 참조하십시오.

Security Cloud Control Firewall Management

방화벽 디바이스, 정책, 개체 및 구성 일관성을 관리하는 데 사용되는 Security Cloud Control Firewall Management의 개요입니다.

Security Cloud Control Firewall Management(이전 명칭은 Cisco Defense Orchestrator)은 분산 환경에서 보안 정책 관리를 간소화합니다. 매니지드 방화벽 및 디바이스 전체에서 정책을 일관된 상태로 유지하는 데 도움이 됩니다. Security Cloud Control에서는 **Products(제품)** 아래에 **Firewall(방화벽)**이 나타납니다.

Security Cloud Control Firewall Management는 보안 정책의 불일치를 식별하고 해결 도구를 제공하여 보안 정책을 최적화하는 데 도움이 됩니다. 또한 개체 공유, 정책 공유 및 설정 템플릿을 지원하므로 디바이스 전체에 일관된 설정을 적용할 수 있습니다.

Security Cloud Control Firewall Management는 ASDM(Adaptive Security Device Manager)과 같은 로컬 디바이스 관리자와 함께 사용할 수 있습니다. 다른 관리자가 수행한 구성 변경 사항을 추적하고 필요한 경우 차이점을 조정합니다.

이 플랫폼에는 Threat Defense 디바이스를 온프레미스 방화벽 Management Center 또는 클라우드 제공 Firewall Management Center에 연결할 수 있도록 도와주는 안내형 'Day 0' 경험이 포함되어 있습니다. 주요 기능을 강조 표시하고 해당 기능을 활성화 및 구성하는 데 도움이 됩니다.

디바이스를 온보딩하기 전에 다음 사전 요건을 완료합니다.

- 설치 마법사를 완료합니다.
- 디바이스에 라이선스를 할당합니다.

이러한 사전 요건을 완료한 후, Security Cloud Control Firewall Management 온보딩 마법사를 사용하여 디바이스를 온보딩합니다.

다음 제한 사항에 유의하십시오.

- 조직에 연결된 Security Cloud Control Firewall Management에 디바이스를 온보딩한 후에는 한 조직에서 다른 조직으로 디바이스를 마이그레이션할 수 없습니다.
- 디바이스를 새 조직으로 이동하려면 새 조직에 다시 온보딩해야 합니다.

Cisco

Cisco Systems, Inc. 및 자회사("Cisco"로 통칭)에서는 개인 정보를 보호하고 사용자가 Cisco 웹사이트에서 그리고 시스코 제품 및 서비스("솔루션")의 사용에서 유익한 경험을 할 수 있도록 최선을 다하고 있습니다. [Cisco 온라인 개인정보 보호정책](#)을 주의 깊게 읽고 Cisco에서 개인 정보를 수집, 사용, 공유 및 보호하는 방법을 명확하게 이해하십시오.

Security Cloud Control Firewall Management

Security Cloud Control Firewall Management는 매주 목요일 09:00~12:00 UTC에 주간 플랫폼 업데이트를 받아 새로운 기능과 품질 개선 사항을 제공합니다. 유지 보수 중에도 액세스는 계속 사용할 수 있지만, 중단 없는 정책 시행과 안정적인 디바이스 관리를 위해 구성 변경 사항을 구축하지 않아도 됩니다.

Security Cloud Control Firewall Management은 새로운 기능과 품질 개선으로 매주 플랫폼을 업데이트합니다. 이 일정에 따라 업데이트가 3시간 동안 이루어집니다.

요일	시각 (24시간제, UTC)
목요일	09:00 UTC - 12:00 UTC

Security Cloud Control Firewall Management 업그레이드 기간 동안 조직 및 클라우드 제공 Firewall Management Center에 계속 액세스할 수 있습니다. 또한 Security Cloud Control Firewall Management에 온보딩한 디바이스가 보안 정책을 계속 적용합니다.



- Security Cloud Control Firewall Management의 유지 관리 기간 동안에는 관리하는 디바이스에 구성을 생성하거나 구축하지 마십시오.
- Security Cloud Control Firewall Management의 통신을 중단시키는 문제가 발생하면 Cisco는 유지 관리 기간이 아니더라도 영향을 받는 모든 테넌트에서 최대한 신속하게 해당 문제를 해결합니다.

Security Cloud Control Firewall Management

Security Cloud Control Firewall Management에 방화벽 및 지원되는 디바이스를 관리하려면 기본 구독 및 디바이스 라이선스가 필요합니다. 구축 요구사항에 맞게 기간제 요금제를 선택하고, 소프트웨어 업데이트에 액세스하고, Cisco TAC 지원을 받으십시오. Catalyst SD-WAN는 추가 라이선스가 필요하지 않습니다. Cisco DNA(Cisco Digital Network Architecture) 또는 WAN Essentials 라이선스를 사용하는 고객은 Security Cloud Control Firewall Management와 통합할 수 있습니다.

Security Cloud Control Firewall Management는 조직 자격에 대한 기본 구독과 디바이스 관리를 위한 디바이스 라이선스가 필요합니다. 필요한 테넌트 수에 따라 하나 이상의 Security Cloud Control Firewall Management 기본 구독을 구입하고 디바이스 모델 번호 및 수량에 따라 디바이스 라이선스를 구입할 수 있습니다. 즉, 기본 구독을 구매하면 Security Cloud Control Firewall Management 조직이 제공됩니다. Security Cloud Control Firewall Management를 사용하여 관리하도록 선택하는 모든 디바이스에 대해 별도의 디바이스 라이선스가 필요합니다.

Security Cloud Control Firewall Management에서 디바이스를 온보딩하고 관리하려면, 관리하려는 디바이스에 따라 기본 구독 및 디바이스별 기간 기반 구독을 구매해야 합니다.

Security Cloud Control Firewall Management 구독은 기간 기반입니다.

- **Base(기본):** 1년, 3년 및 5년 구독을 제공하며 Security Cloud Control Firewall Management 조직에 액세스하고 적절하게 라이선스가 부여된 디바이스를 온보딩할 수 있는 자격을 제공합니다.
- **Device License(디바이스 라이선스):** 관리하기로 선택한 모든 지원 디바이스에 대해 1년, 3년 및 5년 구독을 제공합니다. 예를 들어 Cisco Firepower 1010 디바이스에 대한 3년 소프트웨어 구독을 구매한 경우, 3년 동안 Security Cloud Control Firewall Management를 사용하여 Cisco Firepower 1010 디바이스를 관리하도록 선택할 수 있습니다.

Security Cloud Control Firewall Management가 지원하는 Cisco 보안 디바이스에 대한 자세한 내용은 [Security Cloud Control Firewall Management에서 지원하는 소프트웨어 및 하드웨어](#)를 참조하십시오.

중요사항

Security Cloud Control Firewall Management에서 고가용성 디바이스 쌍을 관리하기 위해 두 개의 별도 디바이스 라이선스가 필요하지 않습니다. ASA(고가용성 쌍이 있는 경우, Security Cloud Control Firewall Management는 고가용성 디바이스 쌍을 하나의 단일 디바이스로 간주하므로 하나의 디바이스 라이선스를 구입하는 것으로 충분합니다.



- Catalyst SD-WAN는 Security Cloud Control Firewall Management와의 통합을 위해 추가 라이선스가 필요하지 않습니다. Cisco Digital Network Architecture DNA(Digital Network Architecture) 또는 WAN Essentials 라이선스가 있는 고객은 다른 라이선스 없이 이러한 기존 라이선스를 통합에 사용할 수 있습니다.
-



Cisco 스마트 라이선스 포털을 통해 Security Cloud Control Firewall Management 라이선스를 관리할 수 없습니다.

Security Cloud Control Firewall Management 기본 구독에는 구독 기간 동안 유효한 소프트웨어 구독 지원이 포함되며 추가 비용 없이 소프트웨어 업데이트, 주요 업그레이드 및 Cisco TAC(Technical Assistance Center)에 대한 액세스를 제공합니다. 소프트웨어 지원이 기본적으로 선택되어 있지만 요구 사항에 따라 Security Cloud Control Firewall Management 솔루션 지원을 활용할 수도 있습니다.

클라우드 제공 Firewall Management Center, Security Cloud Control를 통해 Secure Firewall Threat Defense 디바이스를 지원하는 것 외에도 다음 디바이스도 관리합니다.

- Cisco Secure Firewall ASA
- 온프레미스 Cisco Secure Firewall Management Center
- Cisco Meraki 보안 어플라이언스
- Cisco IOS 디바이스
- SSH를 사용하여 액세스할 수 있는 디바이스
- Amazon Web Services(AWS) 가상 프라이빗 클라우드(VPC)
- Umbrella 조직

Security Cloud Control 기본 인타이틀먼트 라이선스와 관리하려는 디바이스에 특정한 라이선스가 필요합니다.

Firewall Management Center

Threat Defense 관리, 마이그레이션, 온보딩, 고가용성, 보안 애널리틱스, 라이선싱이 포함된 클라우드 제공 Firewall Management Center의 개요입니다.

클라우드 제공 Firewall Management Center는 Security Cloud Control Firewall Management을 통해 Secure Firewall Threat Defense 디바이스를 관리하는 SaaS(서비스형 소프트웨어) 제품입니다. 이 기능은 온프레미스 방화벽 Management Center과 동일한 기능을 다수 제공합니다.

클라우드 제공 Firewall Management Center은 온프레미스 방화벽 Management Center와 외관과 동작이 동일하며, 동일한 FMC API를 사용합니다.

SaaS 제품이므로 Security Cloud Control Firewall Management 운영 팀에서 클라우드 제공 Firewall Management Center 소프트웨어를 구축하고 유지 관리합니다. 새로운 기능이 도입되면 운영 팀이 Security Cloud Control Firewall Management 조직의 클라우드 제공 Firewall Management Center를 업데이트합니다.

마이그레이션 마법사를 사용하면 Threat Defense 디바이스를 온프레미스 방화벽 Management Center에서 클라우드 제공 Firewall Management Center로 마이그레이션할 수 있습니다.

마이그레이션하기 전에 디바이스에서 다음 Threat Defense 소프트웨어 릴리스 중 하나를 실행해야 합니다.

- 최소 온프레미스 방화벽 Management Center: 7.2
- 최소 Threat Defense: 7.2.x(버전 7.1에서는 지원되지 않음)

Threat Defense 7.1 릴리스는 마이그레이션이 지원되지 않습니다.

일련 번호를 입력하거나 등록 키를 포함하는 CLI 명령을 사용하는 등의 친숙한 방법을 사용하여 Security Cloud Control Firewall Management에서 Threat Defense 디바이스를 온보딩합니다.

온보딩 후:

- 디바이스가 Security Cloud Control Firewall Management와 클라우드 제공 Firewall Management Center 모두에 표시됩니다.
- 클라우드 제공 Firewall Management Center에서 디바이스를 구성합니다.
- Security Cloud Control Firewall Management에서 버전, 구성 상태, 연결성, 상태 및 노드 상태와 같은 디바이스 관련 정보를 볼 수 있습니다.
- Security Cloud Control Firewall Management에서 상태를 클릭하면 플랫폼이 클라우드 제공 Firewall Management Center 사용자 인터페이스에서 디바이스 상태 모니터링 페이지를 엽니다.

Security Cloud Control Firewall Management는 데이터 인터페이스를 통해 관리하는 Threat Defense 디바이스에서 고가용성 지원을 제공합니다. 이 기능은 소프트웨어 버전 7.2 이상에서 실행되는 디바이스에서 지원됩니다.

Security Analytics and Logging(SaaS) 또는 Security Analytics and Logging(온프레미스)을 사용하여 온보딩된 Threat Defense 디바이스의 보안 이벤트를 분석할 수 있습니다:

- Security Analytics and Logging(SaaS)는 클라우드에 이벤트를 저장하고, 사용자는 해당 이벤트를 Security Cloud Control Firewall Management에서 볼 수 있습니다.
- Security Analytics and Logging(온프레미스)은 온프레미스 Secure Network Analytics 어플라이언스에 이벤트를 저장하고, 분석은 온프레미스 방화벽 Management Center에서 발생합니다.

두 경우 모두 방화벽에서 원하는 로그 컬렉터로 로그를 직접 전송할 수 있습니다.

클라우드 제공 Firewall Management Center의 라이선스는 디바이스별 매니지드 라이선스이며 클라우드 제공 Firewall Management Center 자체에는 라이선스가 필요하지 않습니다. 기존 Secure Firewall Threat Defense 디바이스는 기존 스마트 라이선스를 재사용하며, 새 Secure Firewall Threat Defense 디바이스는 Secure Firewall Threat Defense에서 구현된 각 기능에 대해 새 스마트 라이선스를 프로비저닝합니다. 자세한 내용은 [클라우드 제공 Firewall Management Center 라이선스](#)를 참조하십시오.

기존 고객은 Security Cloud Control를 계속 사용하여 Secure Firewall ASA, Meraki, Cisco IOS 디바이스, Umbrella 및 AWS 가상 프라이빗 클라우드와 같은 다른 디바이스 유형을 관리할 수 있습니다. Firepower Device Manager에서 로컬 관리용으로 구성된 Secure Firewall Threat Defense 디바이스를 Security Cloud Control를 사용하여 관리하는 경우 Security Cloud Control로도 계속 관리할 수 있습니다.

테넌트에 클라우드 제공 Firewall Management Center을(를) 프로비저닝하는 방법을 알아보려면 [Security Cloud Control 테넌트에서 클라우드 제공 Firewall Management Center 활성화](#)를 참조하십시오.

클라우드 제공 Firewall Management Center에 대한 전체 관리자 가이드는 [클라우드 제공 Firewall Management Center로 Cisco Secure Firewall Threat Defense 관리](#)를 참조하십시오.

Firewall Management Center

Security Cloud Control 테넌트에 대해 클라우드 제공 Firewall Management Center을(를) 활성화하고, 프로비저닝 상태를 추적하고, 준비 알림을 수신하고, 라이선싱 및 디바이스 온보딩을 준비하는 방법을 알아봅니다.

Secure Firewall Threat Defense 디바이스를 관리하려는 경우 테넌트에서 클라우드 제공 Firewall Management Center를 활성화할 수 있습니다. 이 작업을 수행하려면 관리자 또는 슈퍼 관리자 사용자 역할이 있어야 합니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. Security Cloud Control 메뉴에서 **Administration(관리) > Integration(통합) > Firewall Management Center**를 클릭하고 **Enable Cloud-Delivered FMC(클라우드 제공 FMC 활성화)**를 클릭합니다.

Security Cloud Control는 백그라운드에서 클라우드 제공 Firewall Management Center 인스턴스 프로비저닝을 시작합니다. 이 작업을 완료하는 데 일반적으로 15~30분이 소요됩니다. **Cloud-Delivered FMC(클라우드 제공 FMC)**의 **Status(상태)** 열에서 프로비저닝 진행 상황을 추적할 수 있습니다.

프로비저닝이 완료되면 상태가 **Active(활성)**로 변경됩니다. 또한 수신 webhook을 구성한 애플리케이션 및 Security Cloud Control 알림 패널에서 클라우드 제공 **Firewall Management Center is Ready(준비됨)** 알림을 받게 됩니다. 자세한 내용은 [알림 설정](#)을 참조하십시오.

주

클라우드 제공 **Firewall Management Center is Ready(준비됨)** 알림을 수신한 후 테넌트에서 로그아웃했다가 로그인하여 **Actions(작업)**, **Management(관리)**, **System(시스템)**과 같은 **Cloud-Delivered FMC(클라우드 제공 FMC)** 오른쪽 창 옵션을 확인하십시오.

다음 작업:

- a. CSSM(Cisco Smart Software Manager)에 클라우드 제공 Firewall Management Center을(를) 등록하여 스마트 라이선스를 활성화합니다. 자세한 단계는 [Smart Software Manager에 클라우드 제공 Firewall Management Center 등록](#)을 참조하십시오.
- b. Firewall Threat Defense 디바이스를 클라우드 제공 Firewall Management Center에 온보딩하고 관리합니다.

Security Cloud Control Firewall Management

Firewall Management Center

클라우드 제공 Firewall Management Center 버전 정보는 주로 마이그레이션 계획 수립, 기능 지원 확인, 문제 해결, 라이선스 관리 및 운영 관리를 위해 필요합니다.

이 절차를 사용하여 Security Cloud Control Firewall Management에서 클라우드 제공 Firewall Management Center의 현재 버전을 확인합니다.

조직에서 [클라우드 제공 Firewall Management Center](#)를 활성화합니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Administration(관리) > Integrations(통합) > Firewall Management Center**를 클릭합니다.
3. FMC 탭에서 버전이 **Version(버전)** 옆에 표시됩니다.

Name	Version	Devices	Type	Status	Last heartbeat
Cloud-Delivered FMC	20250825	2	Cloud-Delivered FMC	Active	10/10/2025, 19:22:48
OnPrem_FMC_1	7.6.0-build 1526	1	On-Prem FMC	Synced	10/10/2025, 19:22:39
OnPrem_FMC_2	7.7.0-build 91	1	On-Prem FMC	Synced	10/10/2025, 19:22:39

클라우드 제공 Firewall Management Center 버전에 대한 자세한 내용은 [클라우드 제공 Firewall Management Center 릴리스 노트](#)를 참조하십시오.

Firewall Management Center

스마트 라이선싱을 위해 Cisco Smart Software Manager에 클라우드 제공 Firewall Management Center을(를) 등록하는 방법을 알아봅니다. 등록하면 내보내기 제어 기능이 활성화되고 평가 기간 후 구축 중단을 방지하는 데 도움이 됩니다.

온프레미스 방화벽 Management Center와 동일한 방법으로 Cisco Smart Licensing에 클라우드 제공 Firewall Management Center을(를) 등록합니다.

Security Cloud Control Firewall Management의 기본 구독 및 평가판에는 클라우드 제공 Firewall Management Center가 포함되어 있습니다. 클라우드 제공 Firewall Management Center에 대한 별도의 라이선스를 구매할 필요가 없습니다. 기본 구독 또는 평가판에는 클라우드 제공 Firewall Management Center가 포함되며, 클라우드를 통해 Firewall Threat Defense 디바이스를 관리할 수 있습니다.

클라우드 제공 Firewall Management Center은(는) 구축 시 90일 평가 라이선스와 함께 프로비저닝됩니다.

중요사항

RAVPN 및 SSL VPN과 같이 내보내기 암호화에 필요한 기능을 비롯한 모든 기능에 액세스하려면 구축 후 즉시 Cisco Smart Software Manager에 클라우드 제공 Firewall Management Center을(를) 등록하는 것이 좋습니다. 조기 등록을 통해 기능 제한 및 구축 중단을 방지할 수 있습니다.

- 원격 액세스 VPN, SSL VPN 및 기타 암호화 종속 옵션과 같이 내보내기 암호화가 필요한 기능은 CSSM(Cisco Smart Software Manager)에 클라우드 제공 Firewall Management Center을(를) 등록할 때까지 비활성화된 상태로 유지됩니다.

- 90일 평가 기간이 끝난 후에도 **Firewall Threat Defense** 디바이스를 계속 온보딩할 수 있습니다. 그러나 수동으로 트리거하거나 예약한 구축은 **CSSM** 등록이 완료될 때까지 차단됩니다.
- **Security Cloud Control Firewall Management**에서는 평가 라이선스가 만료에 가까워지면 경고 알림을 보냅니다.

주

평가판 라이선스가 만료되면 스마트 라이선스 필드에 경고가 표시됩니다.

Cloud-Delivered
FMC

Hostname	amallio.app.staging.cdo.cisco.com
Version	20260213
Smart license	Evaluation period (expires in 89 days)

평가 기간이 끝나면 클라우드 제공 **Firewall Management Center**의 등록이 취소됩니다. **Cisco Smart Software Manager**에 클라우드 제공 **Firewall Management Center**을(를) 등록하면 평가 모드에서 전체 라이선스 상태로 전환됩니다.

평가 경고 링크를 클릭하여 스마트 라이선싱 등록 페이지를 열고 **Cisco Smart Software Manager**에 클라우드 제공 **Firewall Management Center**을(를) 등록합니다.

CSSM(Cisco Smart Software Manager)

- 온프레미스 방화벽 **Management Center**와 동일한 프로세스를 따라 스마트 라이선싱 계정에 클라우드 제공 **Firewall Management Center**을(를) 연결합니다. 이 섹션에서는 개략적인 절차를 제공합니다.
- 클라우드 제공 **Firewall Management Center**은 별도의 라이선스 구매가 필요하지 않습니다. 라이선스는 등록 시 자동으로 적용됩니다.
- 스마트 라이선싱에 등록하면 암호화 내보내기 기능이 활성화됩니다.
- 등록은 컴플라이언스를 보장하고 구축 문제를 방지합니다.

Security Cloud Control 테넌트에서 프로비저닝된 클라우드 제공 **Firewall Management Center**를 가져오는 방법을 알아보려면 [Security Cloud Control 테넌트용 클라우드 제공 Firewall Management Center 요청](#)을 참조하십시오.

Firewall Threat Defense

- 클라우드 제공 **Firewall Management Center**의 경우 별도의 라이선스를 구매할 필요가 없습니다.
- 클라우드 제공 **Firewall Management Center**에서 관리하는 **Firewall Threat Defense** 디바이스에는 개별 라이선스가 필요합니다.
- **CSSM**에 클라우드 제공 **Firewall Management Center**을(를) 등록한 후, 관리자는 보안 디바이스에 기능 라이선스를 적용할 수 있습니다.

여기에서는 개략적인 절차를 제공합니다. 자세한 단계는 [Smart Software Manager에 Management Center 등록](#)을 참조하십시오.

1. 스마트 어카운트 생성 또는 액세스:

Cisco Smart Software Manager 어카운트가 있는지 확인합니다. 없는 경우 [Smart Software Manager](#)에서 생성합니다.

2. 등록 토큰 생성 또는 등록 토큰 사용:

Smart Software Manager에서 기존의 유효한 등록 토큰을 사용하거나 클라우드 제공 Firewall Management Center 을(를) 등록하려는 가상 어카운트에 대해 등록 토큰을 생성합니다.

a. Inventory(재고 목록) → New Token(새 토큰)으로 이동합니다.

b. 설명을 입력하고 만료를 설정합니다(Cisco는 30일 권장).

c. 토큰을 생성하고 복사합니다.

3. 클라우드 제공 Firewall Management Center을(를) 토큰으로 등록합니다.

a. 클라우드 제공 Firewall Management Center 인터페이스에 로그인합니다.

b. System(시스템) > Licenses(라이선스) > Smart Licenses(스마트 라이선스)로 이동합니다.

c. Register(등록)를 클릭하고 Product Instance Registration Token(제품 인스턴스 등록 토큰) 필드에 등록 토큰을 붙여넣습니다.

d. 토큰 전후에 추가 공백이나 빈 줄이 없는지 확인합니다.

e. Apply Changes(변경 사항 적용)를 클릭합니다.

4. 등록을 확인합니다.

등록 후 **System(시스템) > Licenses(라이선스) > Smart Licenses(스마트 라이선스)**에서 라이선스 상태를 확인하여 등록, 라이선스 적용이 성공적으로 완료되었는지 그리고 "Export-Controlled Features(내보내기 제어 기능)"가 활성화되었는지 확인합니다.

Firewall Management Center

클라우드 제공 Firewall Management Center의 유지보수 일정에 대한 자세한 내용을 확인하세요. 여기에는 조직 내에 클라우드 제공 Firewall Management Center를 배포한 고객들에게 Security Cloud Control이 클라우드 제공을 업데이트하기 약 1주일 전에 알림이 전송된다는 내용도 포함됩니다.

조직에 클라우드 제공 Firewall Management Center이(가) 구축된 고객은 Security Cloud Control가 클라우드 제공 Firewall Management Center 환경을 업데이트하기 약 1주일 전에 알림을 받습니다.

테넌트의 슈퍼 관리자 및 관리자 사용자에게는 이메일 알림이 전송됩니다. Security Cloud Control 는 또한 모든 사용자에게 향후 업데이트를 알리는 배너를 홈페이지에 표시합니다.



- 클라우드 제공 **Firewall Management Center**의 유지 관리 기간 동안에는 관리하는 디바이스에 구성을 생성하거나 구축하지 마십시오.
- **Security Cloud Control** 또는 클라우드 제공 **Firewall Management Center**와 통신이 중단되는 문제가 발생하면 유지보수 기간이 아니더라도 영향을 받는 모든 테넌트에게 최대한 신속하게 장애를 해결합니다.

Security Cloud Control Firewall Management

Security Cloud Control Firewall Management를 프로비저닝하는 방법을 알아봅니다. 조직을 설정하고, 방화벽 관리를 활성화하고, 구독을 클레임하고, 보안 정책 구성 및 구축을 위한 환경을 준비합니다.

이 항목에서는 **Security Cloud Control** 내에서 방화벽을 프로비저닝하는 데 필요한 대략적인 단계를 제공합니다. 방화벽 프로비저닝에는 조직에 대해 방화벽 기능 활성화, 구독 및 보안 네트워크 관리를 위한 환경 준비 작업이 포함됩니다. 이 프로세스를 통해 조직의 방화벽 서비스가 올바르게 설정되고 설정 및 정책 구축을 위한 준비가 완료되었는지 확인합니다.

1. **Security Cloud Sign On** 어카운트를 사용하여 **Security Cloud Control**에 로그인합니다. 계정이 없는 경우 계정을 생성합니다.

Security Cloud Sign On 계정을 생성하려면 계정 활성화 이메일이 발송될 이메일 주소를 제공해야 합니다. **Duo MFA**(다단계 인증)를 사용하려면 모든 **Security Cloud Sign On** 사용자 계정이 필요합니다. **Duo MFA**는 **Security Cloud Sign On** 계정에 무료로 포함되어 있습니다.

Security Cloud Sign On 어카운트를 생성하는 방법에 대한 자세한 내용은 [Security Cloud Sign On](#)을 참조하십시오..



이미 **Security Cloud Sign on** 계정이 있는 경우 [Security Cloud Control](#)에 **로그인**을 참조하십시오.

2. 조직을 생성하고 기본 지역을 설정합니다. [조직 생성](#)을 참조하십시오.
3. (선택 사항) **Security Cloud Control**에서 방화벽 관리를 활성화합니다.

새로운 **Security Cloud Control** 조직을 보유하고 있으며 **Security Cloud Control**에서 방화벽 사용 권한이 있지만 아직 구독 코드를 받지 못한 경우, 이 절차를 통해 방화벽 애플리케이션을 활성화할 수 있습니다. 자세한 내용은 [Security Cloud Control Firewall Management](#) **활성화**를 참조하십시오.

4. 구독 코드를 수신한 후 제품 인스턴스에 대한 구독을 클레임할 수 있도록 **Security Cloud Control** 환영 이메일로 수신된 클레임 코드를 입력합니다. 자세한 내용은 [제품 구독 클레임](#)을 참조하십시오. 새 제품 인스턴스를 활성화합니다.



클레임 구독 프로세스를 이해해야 하는 경우 [클레임 구독 개요](#)를 참조하십시오.

5. 제품 조직에 도메인을 추가합니다. 자세한 내용은 [도메인 추가 및 클레임](#)을 참조하십시오.
6. ID 공급자를 Security Cloud Sign On 계정과 통합합니다. 자세한 내용은 [ID 공급자 통합](#)을 참조하십시오.
7. 사용자 및 그룹을 생성합니다. 정확한 제품 관리 및 제어를 위해 역할을 할당합니다. 역할 기반 액세스에 대한 자세한 내용은 [역할 기반 액세스 제어](#)를 참조하십시오.

Security Cloud Control Firewall Management

어카운트와 방화벽 관리 서비스가 프로비저닝된 후 Security Cloud Control Firewall Management에서 방화벽 애플리케이션을 여는 방법을 알아봅니다.

이 주제에서는 Security Cloud Control에서 방화벽 애플리케이션으로 이동하는 단계를 설명합니다.

Cisco Security Cloud Sign-On 어카운트가 있고 방화벽 조직의 Security Cloud Control에 프로비저닝되었는지 확인합니다. 자세한 내용은 [프로비저닝 Security Cloud Control Firewall Management](#)을 참조하십시오.

1. <https://security.cisco.com/>에서 Security Cloud Control을(를) 엽니다.
2. 어카운트를 생성할 때 설정한 Security Cloud Sign On 자격 증명 및 MFA(다단계 인증) 옵션을 사용하여 로그인합니다.
3. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.

Firewall Management

방화벽 관리 대시보드를 사용하여 테넌트 수준 인사이트, 알림, 작업, 재고 목록, VPN 활동, 변경 로그 및 보안 이벤트를 보는 방법을 알아봅니다.

Firewall 대시보드는 다양한 범주에서 테넌트 레벨 세부 정보를 모니터링하고 관리하기 위한 중앙 허브입니다. 로그인하면 중요한 인사이트와 보안 및 운영 효율성 최적화하기 위한 작업을 제공하는 맞춤형 대시보드에 액세스할 수 있습니다.

왼쪽 창에서 **Dashboard**(대시보드)를 클릭합니다.

대시보드 사용자 맞춤화

표시되는 위젯을 맞춤 설정하여 대시보드를 특정 요구 사항에 맞게 조정합니다.

1. **Home** 페이지에서 **Customize**(맞춤화)를 클릭합니다.
2. 대시보드에 표시할 위젯을 선택하거나 선택을 해제합니다.
3. 위젯을 끌어다 놓아 원하는 대로 정렬할 수 있습니다.

대시보드는 **Top Insights & Alerts**(주요 인사이트 및 알림), **Top Actions**(주요 조치) 및 **Top Information**(주요 정보)의 세 가지 주요 섹션으로 나뉩니다. 각 섹션은 최적의 보안 및 운영 통제를 유지하는 데 도움이 되는 다양한 범주의 통찰력을 제공합니다.

인사이트 및 알림

테넌트에 **AgenticOps** 인사이트가 활성화된 경우에만 이 섹션이 표시됩니다. **Elephant** 플로우로 인한 높은 트래픽, **RA VPN** 예측, 액세스 제어 정책 이상, 높은 **CPU** 및 메모리 사용량, 스노트 **CPU** 및 메모리 사용량과 관련된 인사이트를 확인할 수 있습니다.

상위 작업

테넌트에 **AgenticOps** 인사이트가 활성화된 경우에만 이 섹션이 표시됩니다. 활성화된 경우 다음 위젯을 볼 수 있습니다.

- **Policy Analyzer and Optimizer**(정책 분석기 및 옵티마이저): 방화벽 성능을 개선하기 위한 보안 정책을 분석하고 이상 징후를 탐지하며 최적화 권장 사항을 제공합니다.
자세한 내용은 [Policy Analyzer and Optimizer\(정책 분석기 및 옵티마이저\)](#)를 참조하십시오.
- **AgenticOps** 인사이트: 구성, 상태 및 운영, 트래픽 및 용량 등 범주별로 활성 인사이트와 추세를 표시합니다.
자세한 내용은 [AgenticOpsInsights\(인사이트\)](#)를 참조하십시오.
- 기능 채택: 사용량을 평가하고 개선할 수 있도록 기능 채택률을 표시합니다.
자세한 내용은 [기능 채택 평가 및 개선](#)을 참조하십시오.

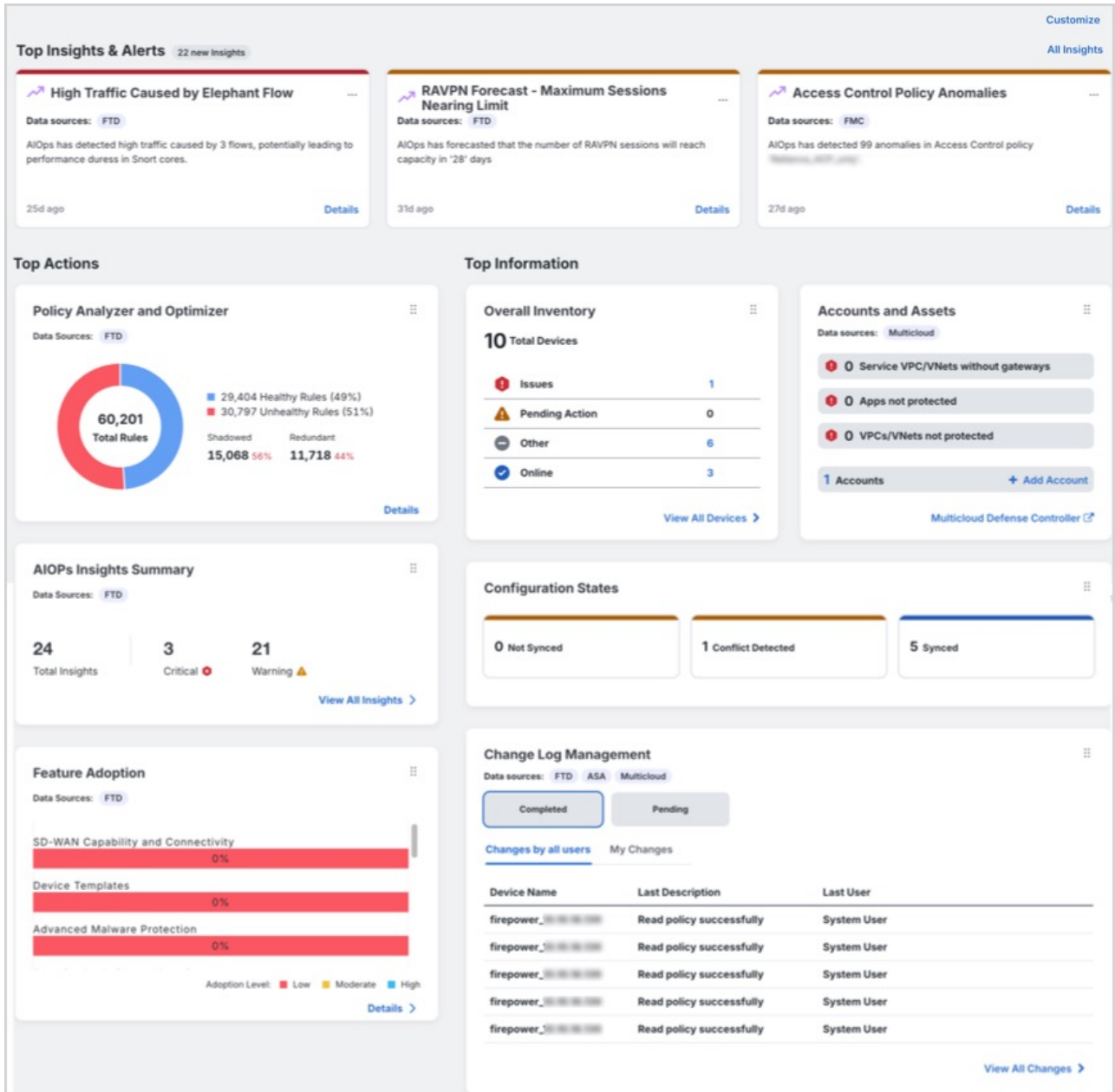
상위 정보

이 섹션에서는 다양한 테넌트 수준 메트릭에 대한 상세한 인사이트를 제공합니다. 테넌트에 대해 활성화된 기능에 따라 다음 위젯을 볼 수 있습니다.

- **Configuration Status**(구성 상태): 불일치 또는 충돌을 식별할 수 있도록 디바이스 구성을 **Security Cloud Control**에서 유지 관리하는 구성과 비교합니다.
자세한 내용은 [디바이스 관리](#)를 참조하십시오.
- **Change Log Management**(변경 로그 관리): 운영 변경 사항을 추적할 수 있도록 완료된 변경 로그와 보류 중인 변경 로그를 표시합니다. 위젯에 **Completed**(완료됨) 및 **Pending**(보류 중) 변경 로그가 표시됩니다.
자세한 내용은 [Change Logs\(변경 로그\)](#)를 참조하십시오.
- **RA VPN Sessions**(RA VPN 세션): 원격 액세스 VPN 세션 활동을 표시합니다.
자세한 내용은 [RA VPN 세션](#)을 참조하십시오.
- **Overall Inventory**(전체 재고 목록): 총 디바이스 수를 표시하고 **Issues**(문제), **Pending Actions**(보류 중인 작업), **Other**(기타) 및 **Online**(온라인)별로 그룹화합니다.
자세한 내용은 [All Devices\(모든 디바이스\)](#)를 참조하십시오.
- **Site-to-Site VPN**(사이트 간 VPN): 총 VPN 터널 수와 **Active**(활성) 및 **Idle**(유휴) 상태인 터널의 비율을 표시합니다. 위젯에 총 VPN 터널 수와 **Active**(활성) 및 **Idle**(유휴)의 비율이 표시됩니다.
자세한 내용은 [사이트 간 VPN](#)을 참조하십시오.
- **어카운트 및 자산**:
 - 멀티 클라우드 어카운트 및 리소스를 효과적으로 추적하고 관리할 수 있습니다. 여기에서 **Multicloud Defense** 컨트롤러를 실행할 수 있습니다.
 - **+Add Account**(+어카운트 추가)를 클릭하여 새 어카운트를 추가합니다.

자세한 내용은 [Multicloud Defense Controller](#)를 참조하십시오.

- **Top Risky Destinations(상위 위험한 대상):** 액세스 권한이 부여된 상위 위험한 대상을 식별하고 모니터링하는 데 도움이 됩니다. 위젯은 애플리케이션 및 URL 범주를 나열하며, 지난 90일, 60일 또는 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 트래픽(기본값)과 차단된 트래픽 사이에서 필터링할 수 있습니다.
- **Top Intrusion and Malware Events(상위 침입 및 멀웨어 이벤트):** 상위 침입 및 멀웨어 이벤트를 모니터링하고 대응할 수 있습니다. 위젯은 침입 이벤트와 멀웨어 이벤트를 표시하며, 지난 90일, 60일, 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 이벤트(기본값)와 차단된 이벤트 사이에서 필터링할 수 있습니다.



발표

최신 **Security Cloud Control** 기능 및 업데이트를 보려면 알림 아이콘을 클릭합니다. 목록에 있는 항목에 대한 추가 정보가 필요할 경우 관련 문서 링크가 제공됩니다.

제

3 Security Cloud Control Firewall Management Firewall

장

:

- [□□ □□ □□](#)
- [Security Cloud Control □□ □ □□□ □□ □□ □□](#)
- [Security Cloud Control Firewall Management□ API □□ □□□ □□](#)
- [Security Cloud Control □□ □□](#)
- [□□ □□ □□](#)
- [Security Cloud Control Firewall Management□ □□□ □□ □□](#)
- [□□ □□□□, □□ □ □□ □□□□ □□](#)

방화벽 관리 설정이 관리되는 조직 전체에 적용되고 여러 디바이스 및 사용자에게 어떤 영향을 미칠 수 있는지 알아봅니다.

조직의 **Security Cloud Control Firewall Management**을(를) 관리하는 경우 이 장을 사용하십시오. 조직 전체의 방화벽 설정, 사용자 액세스, 알림, 로그 조회 권한, 필터 및 역할 권한을 관리하는 방법을 알아봅니다.

이 섹션에서는 다음 정보를 제공합니다.

- [General Settings\(일반 설정\)](#)
- [API 사용자 관리](#)
- [로그 설정](#)

방화벽 관리 설정은 관리되는 조직 전체에 적용되며 여러 디바이스 및 사용자에게 영향을 미칠 수 있습니다. 일부 토글 버튼은 관리되는 조직에 대해 관련 기능이 활성화된 경우에만 표시됩니다.

Security Cloud Control 방화벽 관리에서 여러 매니지드 디바이스 및 사용자에게 영향을 미치는 조직 전체 설정을 구성하는 방법을 알아봅니다.

매니지드 조직의 여러 매니지드 디바이스 및 사용자에게 영향을 미치는 조직 차원의 설정을 관리하려면 **Administration(관리) > General Settings(일반 설정)**을 사용합니다.



주

관리되는 조직에 대해 활성화되지 않은 기능에 대한 토글 버튼은 표시되지 않습니다.

AI Assistant

AI Assistant는 보안 정책 관리, 문제 해결, 설정 최적화를 통한 운영 효율성 향상에 대한 상황별 지침을 제공합니다. 테넌트 관리자는 일반 설정에서 이 설정을 관리하여 전체 조직에 대한 액세스를 제어해야 합니다.

AI Assistant는 보안 정책을 관리하고, 문제를 해결하며, 구성을 최적화하기 위한 상황별 지침과 인사이트를 제공하는 AI 기반 가상 컴패니언입니다. 자세한 내용은 [Cisco AI Assistant를 사용한 온보딩](#)을 참조하십시오.

기본적으로 AI Assistant이(가) 활성화되어 있습니다. AI Assistant를 활성화 또는 비활성화하면 변경 사항이 관리 조직의 모든 사용자에게 영향을 미칩니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
3. AI Assistant을 비활성화하려면 **Enable AI Assistant for Firewall(방화벽에 대해 활성화)** 토글 버튼을 끕니다.

디바이스 변경 사항에 대한 자동 수락을 활성화하여 업데이트를 자동으로 동기화하여 구성 관리를 간소화 하므로 충돌을 수동으로 검토할 필요가 없습니다. 매니지드 디바이스 전체에서 변경 동기화를 자동화하려는 경우 이 작업을 수행해야 합니다.

이 설정이 활성화된 경우, Security Cloud Control Firewall Management는 사용자가 디바이스에서 직접 수행한 변경 사항을 자동으로 수락합니다. 이 옵션을 비활성화된 상태로 두거나 나중에 비활성화하는 경우 수락하기 전에 각 디바이스 충돌을 검토해야 합니다.

디바이스 변경 사항 자동 수락을 활성화하려면 다음 단계를 따르십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
3. **Enable the option to auto-accept device changes(디바이스 변경 사항 자동 수락 옵션 활성화)** 토글 버튼을 켭니다.

Multicloud Defense SCC

특정 플랫폼 기능을 사용자 Security Cloud Control Firewall Management 환경에 직접 통합하려면 Multicloud Defense SCC 기능 활성화 옵션을 사용합니다. 기존 보안 관리 워크플로우 내에서 고급 멀티 클라우드 방어 기능을 활용해야 할 때마다 이 작업을 수행합니다.

이 기능을 활성화하면, Multicloud Defense과(와) ASA 및 Security Cloud Control Firewall Management에서 관리하는 Firewall Threat Defense 디바이스 사이에 사이트 간 IPsec VPN 터널을 구성할 수 있습니다. 기능을 활성화한 후에는 멀티클라우드 인프라 전반의 보안 연결성을 개선하기 위해 이러한 매니지드 디바이스 간에 VPN 구성을 설정 및 구축할 수 있습니다.

Multicloud Defense Security Cloud Control Firewall Management 기능을 활성화하려면 다음 단계를 수행합니다:

1. **Settings(설정) > General Settings(일반 설정)**를 선택합니다.
2. **Enable Multicloud Defense SCC Features(Multicloud Defense SCC 기능 활성화)** 토글 버튼을 켭니다.

Multicloud Defense

네트워크 개체를 원활하게 동기화하여 플랫폼 전반에 걸쳐 정책 일관성을 보장하려면 Multicloud Defense와의 개체 공유 활성화 옵션을 사용합니다. 운영 효율성 향상을 위해 Security Cloud Control Firewall Management과(와) Multicloud Defense 사이의 보안 개체를 통합해야 하는 경우 이 작업을 수행해야 합니다.

이 설정을 활성화하면 Security Cloud Control Firewall Management에서 Multicloud Defense 네트워크 개체를 공유할 수 있습니다.

다음 단계에 따라 Multicloud Defense과(와)의 개체 공유를 활성화합니다.

1. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
2. **Enable object sharing with Multicloud Defense(Multicloud Defense와 개체 공유 활성화)** 토글 버튼을 켭니다.

ASA

ASA 상태 모니터링을 활성화하여 대시보드 내에서 디바이스 상태 데이터를 수집하고 분석합니다. 시스템에서 관리하는 ASA 디바이스를 포괄적으로 모니터링하려면 테넌트 레벨에서 이 작업을 수행해야 합니다.

관리 조직 레벨에서 디바이스 상태 메트릭을 활성화해야 합니다. Secure Device Connector에서 관리하는 ASA 디바이스의 경우 개별 디바이스 레벨에서 이 기능을 활성화해야 합니다. 이러한 단계를 통해 상태 데이터가 수집되어 대시보드 내에서 분석에 사용할 수 있게 됩니다.

이 기능을 활성화하려면 슈퍼 관리자 사용자 역할이 있어야 합니다.

관리형 조직에 대한 ASA 상태 모니터링을 활성화하려면 다음 단계를 따르십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.

3. Enable ASA Health Monitoring(ASA 상태 모니터링 활성화) 토글 버튼을 켜서 관리 조직의 Device Health Metrics(디바이스 상태 메트릭) 기능을 활성화합니다.

디바이스 유형 고려 사항

- CDG(Cloud Device Gateway)로 관리되는 ASA 디바이스의 경우, 일반 설정에서 **Enable Device Health(상태) Metrics(디바이스 상태 지표 활성화)** 토글이 켜져 있을 때 상태 지표가 활성화됩니다.
- SDC(Secure Device Connector)에서 관리하는 ASA 디바이스의 경우 각 디바이스에 대한 상태 메트릭을 수동으로 활성화합니다.
 - a. **Security Devices(보안 디바이스)**를 선택합니다.
 - b. SDC 매니지드 ASA 디바이스를 선택합니다.
 - c. **Device Actions(디바이스 작업)** 창에서 **Opt-in to Health Metrics(상태 메트릭에 옵트인)**를 선택합니다.

이미 옵트인된 경우 상태 메트릭을 옵트아웃 할 수 있는 옵션이 대신 표시됩니다.



각 SDC는 최대 50개의 ASA 디바이스에 대한 상태 메트릭 수집을 지원할 수 있습니다.

기본 충돌 탐지 간격을 구성하여 구성 변경을 위해 온보딩된 디바이스를 폴링하는 빈도를 결정합니다. 시스템 성능과 가시성을 최적화하기 위해 관리 조직 전체에서 자동화된 모니터링의 주파수를 조정해야 할 때마다 이 작업을 수행해야 합니다.

이 간격은 Security Cloud Control가 변경 사항을 위해 온보딩된 디바이스를 폴링하는 빈도를 결정합니다. 선택 사항은 이 테넌트에서 관리되는 모든 디바이스에 적용됩니다. 언제든지 이 옵션을 변경할 수 있습니다.



하나 이상의 디바이스를 선택한 후 **Security Devices(보안 디바이스)** 페이지에서 사용 가능한 **Conflict Detection(충돌 탐지)** 옵션을 통해 이 선택 항목을 재정의할 수 있습니다.

기본 충돌 탐지 간격을 설정하려면 다음 단계를 따르십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
3. **Default Conflict Detection Interval(기본 충돌 탐지 간격)**의 드롭다운 메뉴를 클릭하고 시간 값을 선택합니다.

디바이스에 대한 단일 또는 반복 업데이트를 편리하게 계획할 수 있도록 자동 구축을 예약하는 옵션을 활성화합니다. 이 작업을 사용하여 구축 워크플로우를 자동화하고 최적의 시간에 업데이트가 발생하도록 합니다.

자동 구축을 예약하는 옵션을 활성화하면 편리한 날짜와 시간에 향후 구축을 예약할 수 있습니다. 이 옵션을 활성화하면 단일 자동 구축을 예약하거나 반복 자동 구축을 설정할 수 있습니다.

Security Cloud Control에서 디바이스에 대해 수행한 변경 사항은 디바이스에 보류 중인 변경 사항  이(가) 있는 경우 자동으로 구축되지 않습니다. 디바이스가 **Conflict Detected**(충돌 탐지됨) 또는 **Not Synced**(동기화되지 않음)와 같이 **Synced**(동기화됨) 상태가 아닌 경우 예약된 구축이 실행되지 않습니다. 예약된 구축이 실패한 모든 인스턴스가 작업 페이지에 나열됩니다.

Enable the Option to Schedule Automatic Deployments(자동 구축 예약 옵션 활성화)가 해제된 경우 예약된 모든 구축이 삭제됩니다.

중요사항

Security Cloud Control를 사용하여 디바이스에 대해 둘 이상의 예약된 구축을 생성하는 경우 새 구축이 기존 구축을 덮어씁니다. API를 사용하여 디바이스에서 둘 이상의 예약된 구축을 생성하는 경우, 새 구축을 예약하기 전에 기존 구축을 반드시 삭제해야 합니다.

예약된 자동 구축을 활성화하려면 다음 단계를 따르십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
3. **Enable the option to schedule automatic deployment**(자동 구축 옵션을 예약하는 옵션 활성화) 토글 버튼을 켜서 활성화합니다.

웹 애널리틱스를 활성화하거나 비활성화하여 익명의 제품 사용량 데이터를 Cisco와 공유함으로써 플랫폼의 기능과 성능을 개선할 수 있습니다. 필요에 따라 이 작업을 완료하여 익명 사용 정보 수집에 관한 개인정보 보호 기본 설정을 조정합니다.

웹 분석은 페이지 히트를 기반으로 익명의 제품 사용 정보를 Cisco에 제공합니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다.

웹 분석은 기본적으로 활성화됩니다. 웹 애널리틱스를 비활성화하거나 나중에 다시 활성화하려면 다음 단계를 완료하십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
3. **Web Analytics**(웹 애널리틱스) 토글 버튼을 켜서 활성화합니다.

FDM

모든 매니지드 FDM 디바이스에서 데이터 보호를 자동화하고 백업 간격을 표준화하도록 FDM 기본 반복 백업 일정을 구성합니다. 신뢰할 수 있는 데이터 복구를 위해 일관된 백업 시간을 설정하거나 업데이트해야 하는 경우 이 작업을 수행합니다.

이 설정을 사용하여 디바이스에 대한 기본 반복 백업 일정을 구성합니다. 디바이스에 대한 백업을 예약할 때 기본값을 사용하거나 사용자 지정할 수 있습니다. 기본 반복 백업 일정을 변경할 경우, 기존의 예약된 백업은 현재 반복 설정을 유지합니다.

FDM 기본 반복 백업 일정 설정하려면 다음 단계를 따르십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
3. **FDM Default Recurring Backup Schedule(FDM 기본 반복 백업 일정)** 섹션의 **Frequency(빈도)** 드롭다운에서 매일, 매주 또는 매월 백업을 선택합니다.
4. 백업 시간을 선택합니다. UTC(Coordinated Universal Time)로 24시간 형식을 사용하여 시간을 입력합니다. 예: 22:00(오후 10:00 UTC).
5. 매주 백업의 경우, 백업 요일을 선택합니다. 월별 백업의 경우, **Days of Month(월의 일)** 필드를 선택하고 백업을 실행할 날짜를 추가합니다. 일수가 31일 미만인 달에 대해 31일을 입력하면 해당 월에 대해서는 백업이 실행되지 않습니다. 백업 일정의 이름과 설명을 입력합니다.
6. **Save(저장)**를 클릭합니다.

Cisco Security Cloud FMC

인증된 디바이스만 추가되도록 하여, Cisco Security Cloud에서 Security Cloud Control 테넌트에 온프레미스 Firewall Management Center의 자동 온보딩을 비활성화하는 방법을 알아봅니다. 이 절차는 슈퍼 관리자 및 관리자가 사용할 수 있습니다.

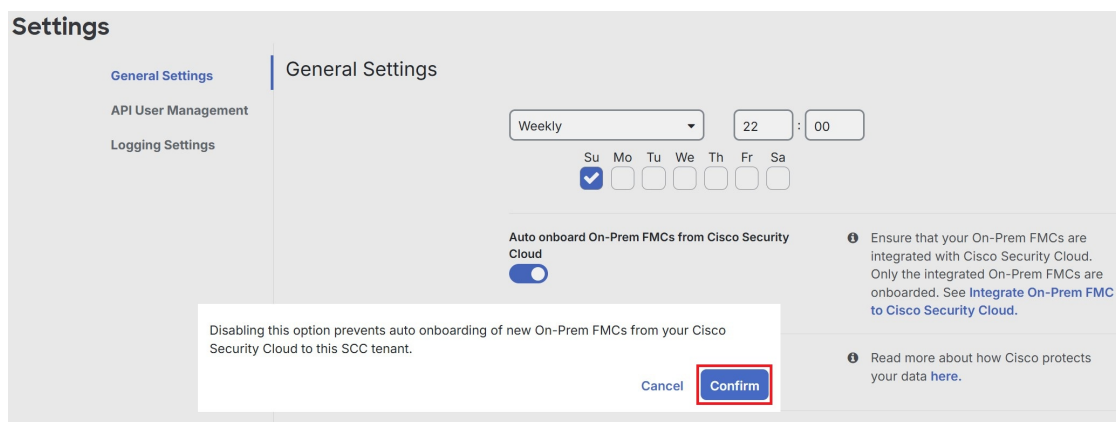
자동 온보딩 기능을 비활성화하면 새로운 온프레미스 Firewall Management Center가 Cisco Security Cloud 테넌트에서 자동으로 추가되는 것이 중지됩니다.



주

Security Cloud Control의 슈퍼 관리자 또는 관리자 사용자만 이 기능을 활성화하거나 비활성화할 수 있습니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
3. **Cisco Security Cloud**에서 온프레미스 **FMC** 자동 온보딩 토글 버튼을 해제하여 온프레미스 Firewall Management Center의 자동 온보딩을 비활성화합니다.
4. **OK(확인)**를 클릭합니다.



Talos

Talos 이벤트 데이터 공유를 관리하여 Cisco의 위협 인텔리전스에 기여하고 새로운 보안 위협에 대한 조직의 보호를 강화합니다. 조직의 정책에 따라 언제든지 익명 이벤트 데이터 공유를 옵트인 또는 옵트아웃할 수 있습니다.

시스코의 위협 인텔리전스 조직인 Talos와 디바이스의 악의적인 이벤트 데이터를 공유합니다. 이벤트 데이터를 공유하면 Talos 위협 탐지 및 대응 기능을 개선하는 데 도움이 되며, 이를 통해 네트워크에 더 맞춤형 보안 업데이트를 제공하고 새로운 위협에 대한 보호를 강화할 수 있습니다.

Talos에 대한 자세한 내용은 [Cisco Talos](#) 제품 페이지를 참조하십시오.



주

Security Cloud Control의 **Enable event data sharing with Talos**(Talos와 이벤트 데이터 공유 활성화) 설정과 클라우드 제공 Firewall Management Center의 **Talos Threat Hunting Telemetry**(Talos 위협 추적 텔레메트리) 옵션은 각각 별도의 설정입니다. Security Cloud Control의 설정은 디바이스의 악의적인 이벤트 데이터를 Talos와 공유합니다.

위협 추적 규칙을 전역 침입 정책에 추가하고 해당 규칙의 이벤트를 Talos로 전송하려면 **Administration(관리) → Configuration(구성) → Intrusion Policy Preferences(침입 정책 환경 설정)**의 클라우드 제공 Firewall Management Center에서 **Talos Threat Hunting Telemetry**(Talos 위협 추적 텔레메트리)를 활성화합니다.

Talos와 이벤트 데이터 공유 활성화 토글 버튼을 활성화해도 클라우드 제공 Firewall Management Center에서 Talos 위협 추적 텔레메트리 기능이 자동으로 활성화되지는 않습니다. 이 기능으로 최상의 결과를 얻으려면 클라우드 제공 Firewall Management Center에서 **Talos Threat Hunting Telemetry**도 활성화합니다. 자세한 내용은 [침입 정책 환경설정](#)을 참조하십시오.

Talos와 이벤트 데이터 공유는 기본적으로 활성화되어 있습니다. 옵트아웃하려면 다음 절차를 따르십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
3. 이 설정을 비활성화하려면 **Enable event data sharing with Talos**(Talos와 이벤트 데이터 공유 활성화) 토글 버튼을 끕니다.



이벤트 데이터를 공유하면 Talos 네트워크에 대한 관련 보안 인사이트를 제공할 수 있습니다. 이 설정을 비활성화하면 Talos의 기능을 완전히 활용하는 기능이 제한되어 진화하는 위협에 대한 네트워크 방어에 영향을 줄 수 있습니다.

테넌트 세부 정보는 Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다. 예를 들면 테넌트 ID, 엔터프라이즈 ID, Secure Services Exchange 테넌트 ID 및 테넌트 이름이 포함됩니다.

Firewall Management Instance Details(방화벽 관리 인스턴스 세부 정보)는 Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다. 복사 아이콘 클릭하여 이러한 테넌트 세부 정보를 복사할 수 있습니다.

- 방화벽 관리 인스턴스 이름: 방화벽 관리 인스턴스의 표시 이름입니다.
- 방화벽 관리 인스턴스 ID: Cisco Security Cloud Control에서 방화벽 관리 인스턴스에 대해 시스템에서 생성된 고유 식별자입니다.
- **Secure Services Exchange ID:** Secure Services Exchange 환경에 있는 방화벽 관리 인스턴스의 고유 식별자입니다. Cisco는 클라우드 서비스 전반의 서비스 통합 및 백엔드 상관관계에 이 값을 사용합니다.
- 보안 클라우드 제어 조직 ID: Security Cloud Control 방화벽 관리 인스턴스와 연결된, 조직의 고유 식별자입니다.

Security Cloud Control Firewall Management Platform Navigator

Platform Navigator는 사용자에게 다양한 Cisco 네트워킹 및 보안 애플리케이션에 대한 중앙 집중식 액세스를 제공하는 나인 블록 실행기입니다. 이 툴을 통해 사용자는 통합 Cisco 플랫폼 간에 원활하게 전환하여 인프라 및 보안 운영을 관리할 수 있습니다.

Platform Navigator는 9개의 블록으로 구성된 애플리케이션 크로스 런치(🗄️)로, Security Cloud Control의 오른쪽 상단에 표시됩니다. 다음 Cisco 네트워킹 및 보안 애플리케이션으로 쉽게 교차 실행할 수 있습니다:

- **Catalyst:** Cisco Catalyst 제품에는 다양한 네트워크 스위치, 무선 컨트롤러, 무선 액세스 포인트, 에지 플랫폼 및 라우터가 포함되어 있어 엔터프라이즈급 비즈니스 요구 사항부터 고강도 및 견고한 네트워킹 환경까지 지원합니다.
- **Intersight:** Cisco Intersight는 고급 인프라, 워크로드 최적화, Kubernetes 서비스의 선택적 모듈식 기능으로 구성된 클라우드 운영 플랫폼입니다. Cisco Intersight 인프라 서비스에는 물리적 및 가상 인프라의 구축, 모니터링, 관리 및 지원이 포함됩니다. Cisco UCS(Unified Computing System), Cisco HyperFlex HCI(hyperconverged infrastructure) 및 기타 타사 Intersight 연결 대상을 지원합니다.
- **IoT Operations Dashboard:** Cisco IoT Operations Dashboard는 운영 팀이 산업용 네트워킹 디바이스와 연결된 산업 자산을 대규모로 안전하게 연결, 유지 관리하고 인사이트를 얻을 수 있도록 지원하는 클라우드 기반 IoT 서비스 플랫폼입니다. 운영팀은 연결된 모든 산업 자산을 종합적으로 파악하여 운영을 간소화하고 비즈니스 연속성을 촉진하는 데 도움이 되는 귀중한 인사이트를 발견할 수 있습니다.
- **Meraki:** Cisco Meraki는 Cisco Meraki 디바이스를 위한 중앙 집중식 관리 플랫폼을 제공하는 IT 및 IoT 클라우드 관리 플랫폼입니다.

- **Spaces:** Cisco Spaces는 클라우드 기반 위치 서비스 플랫폼으로, 조직이 물리적 공간에서 사람과 사물이 어떻게 움직이는지에 대한 인사이트를 얻을 수 있도록 지원합니다. 이러한 인사이트를 통해 가치 있고 관련성 있는 컨텍스트 인게이지먼트를 제공할 수 있습니다. 조직은 사람들의 이동 경로를 파악하는 것 외에도 자산의 위치, 이동 및 활용도를 모니터링하여 운영 효율성을 높일 수 있습니다.
- **ThousandEyes:** Cisco ThousandEyes는 웹 애플리케이션, 서비스 및 네트워크의 가용성과 성능을 모니터링하고 측정하는 데 도움이 되는 클라우드 서비스 제품군입니다. 모든 네트워크에서 모든 사용자부터 모든 애플리케이션에 대한 엔드투엔드 가시성을 제공하여 기업이 문제의 원인을 신속하게 파악하고, 더 빠르게 문제를 해결하며, 성능을 효과적으로 관리할 수 있도록 지원합니다.
- **Workflows:** Cisco Workflows는 더 큰 Cisco Networking Cloud 비전의 일부인 클라우드 호스팅 자동화 애플리케이션입니다. Cisco 고객에게 도메인 간 자동화 기능에 대한 자격을 제공합니다. Cisco에서 제공하거나 독립적으로 구축하여 클라우드 또는 온프레미스의 대상에 도달할 수 있는 맞춤형 및 사전 제작 자동화 템플릿과 다양한 어댑터 옵션을 사용하여 Cisco 및 타사 애플리케이션 전반에서 반복적이고 오류가 발생하기 쉬운 작업을 간소화합니다.
- **Duo Security:** Cisco Duo는 모든 사용자, 디바이스, 애플리케이션의 민감한 데이터에 대한 액세스를 보호하는 2단계 인증 기능을 갖춘 사용자 중심의 제로 트러스트 보안 플랫폼입니다. 적응형 정책, SSO(Single Sign-On, 단일 인증), 고급 엔드포인트 가시성 등의 기능을 제공하여 원격 액세스를 보호하고 비즈니스 연속성을 유지하기 위한 종합적인 솔루션입니다.
- **Secure Access:** Cisco Secure Access는 단일 클라우드 관리 콘솔, 통합 클라이언트, 중앙 집중식 정책 생성 및 통합 보고를 통해 IT 운영을 간소화합니다. 하나의 솔루션에 통합된 광범위한 보안 기능(ZTNA, SWG, CASB, FWaaS, DNS 보안, RBI 등)은 제로 트러스트 원칙을 적용하고 세분화된 보안 정책을 시행하여 보안 위험을 완화합니다. 시장을 선도하는 Talos Threat Intelligence는 탁월한 위협 차단 기능을 통해 위험을 완화하고 조사 속도를 높입니다.
- **Secure Endpoint:** 이전에 Cisco AMP for Endpoints로 알려졌던 Cisco Secure Endpoint는 침해를 방지하고 위협을 신속하게 탐지, 억제 및 수정하도록 설계된 클라우드 관리형 엔드포인트 보안 솔루션입니다. 고급 추적 기능을 갖춘 클라우드 기반 스캐너와 비교하여 파일을 즉시 확인합니다. 보안 분석가는 이러한 기능을 통해 초기 아웃브레이크 소스를 식별하고 격리할 수 있습니다. 또한 이 솔루션은 악의적인 확인된 파일에 대한 회귀 격리도 제공합니다.
- **Cisco Security Provisioning and Administration:** Cisco Security Provisioning and Administration은 Cisco Security Cloud 전반에서 Cisco Secure 제품 인스턴스, 사용자 ID 및 사용자 액세스 관리를 중앙 집중식으로 관리하는 웹 애플리케이션입니다. Security Cloud Control 관리자는 새로운 Security Cloud 엔터프라이즈를 생성하고, 엔터프라이즈의 사용자를 관리하고, 도메인을 클레임하고, 조직의 SSO ID 제공자를 통합하는 등의 작업을 수행할 수 있습니다.
- **XDR:** Cisco XDR(Extended Detection and Response)은 보안 운영을 간소화하고 보안 팀이 정교한 위협을 탐지하고 우선 순위를 지정하여 대응할 수 있도록 설계된 클라우드 기반 솔루션입니다. Cisco XDR은 Cisco 및 타사 보안 솔루션을 통합 플랫폼에 통합함으로써 위협 관리에 대한 포괄적인 접근 방식을 제공합니다. Talos에서 제공하는 Threat Intelligence와 통합된 Cisco XDR은 추가적인 컨텍스트 및 자산 인사이트를 통해 사고 데이터를 보강하여 오탐을 줄이고 전반적인 위협 탐지, 대응 및 포렌식 기능을 강화합니다.

Security Cloud Control

Security Cloud Control에서 중앙 집중식 액세스 관리를 통해 조직 사용자 및 그룹을 관리하는 방법을 알아보십시오.

이 작업의 목적은 RBAC(역할 기반 액세스 제어)를 통해 Cisco 보안 제품 전체에서 사용자 액세스에 대한 중앙 집중식 및 자동화된 관리를 제공하는 것입니다.

Security Cloud Control는 RBAC(Role-Based Access Control)를 지원하여 조직 전체의 액세스 관리를 자동화합니다. 역할은 제품 내 기능에 대한 사용자의 액세스 수준 정의 Security Cloud Control을(를) 사용하면 조직 내 사용자

역할 관리를 중앙 집중화하여 조직 사용자가 반복적으로 로그인할 필요 없이 제품 간에 원활하게 전환할 수 있습니다.

그뿐만 아니라, Security Cloud Control Firewall Management에 대해 [API 전용 사용자를 생성](#)할 수도 있습니다. API 전용 사용자를 사용하면 시스템이 사용자 인터페이스 없이 API를 사용하여 Security Cloud Control와 상호 작용할 수 있습니다.

1. Security Cloud Control 홈 페이지에서 플랫폼 관리를 클릭합니다.
2. 선택 **Platform Management**(플랫폼 관리) > **Access Management**(액세스 관리) > **Administrator Access**(관리자 액세스)

자세한 내용은 Security Cloud Control 플랫폼 서비스 설명서에서 [사용자 관리](#)를 참조하십시오.

Security Cloud Control Firewall Management API

API 전용 사용자를 생성하고 Security Cloud Control 방화벽 관리에 프로그래밍 방식으로 액세스하기 위해 API 토큰을 생성하는 방법을 알아봅니다.

개발자는 Security Cloud Control Firewall Management REST API 호출을 할 때 Security Cloud Control Firewall Management API 토큰을 사용합니다. 호출이 성공하려면 REST API 인증 헤더에 API 토큰이 반드시 포함되어야 합니다. API 전용 사용자는 API 토큰을 생성할 수 있습니다. 일반 사용자는 자신 또는 다른 사용자의 API 토큰을 생성할 수 없습니다.

Security Cloud Control Firewall Management에서 API 전용 사용자를 생성하는 목적은 API 토큰을 사용하여 시스템에 프로그래밍 방식으로 안전하게 액세스할 수 있도록 하는 것입니다.

API 전용 사용자 역할을 사용하면 사용자는 사용자 인터페이스 없이도 API를 사용하여 Security Cloud Control Firewall Management와 상호 작용할 수 있습니다. API 전용 사용자는 Security Cloud Control 인터페이스에 직접 로그인할 수 없습니다. 이 역할은 조직에 이점을 제공합니다. 전용 사용자 역할은 자동화된 프로세스와 통합이 필요한 조직에서 유용합니다.

API 전용 사용자만 API 토큰을 생성할 수 있습니다. 일반 사용자는 자신이나 다른 사용자를 위해 API 토큰을 생성할 수 없습니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Administration**(관리) > **API User Management**(사용자 관리)를 선택합니다.
3. 테넌트에 새 사용자를 추가하려면 **Add a new user**(새 사용자 추가) () 아이콘을 클릭합니다.
4. **Username**(사용자 이름) 필드에 API 전용 사용자의 이름을 입력합니다.
5. **Role**(역할) 드롭다운 목록에서 API 전용 사용자의 **역할**을 선택하고 **Add**(추가)를 클릭합니다.
6. 새 API 전용 사용자의 토큰 열에서 **Generate API Token**(API 토큰 생성)을 클릭하여 API 토큰을 얻습니다. 민감한 데이터를 유지하기 위한 기업의 모범 사례에 따라 안전한 위치에 토큰을 저장하십시오.



편집을 클릭하여 기존 API 전용 사용자의 역할을 변경합니다.

Security Cloud Control

디바이스 이벤트, 알림 및 보고서에 대한 Security Cloud Control 알림을 보고, 검색하고, 해제하고 검토하는 방법을 알아봅니다.

알림 아이콘  을 클릭하여 테넌트에 온보딩한 디바이스에 발생했거나 영향을 미친 최신 알림을 확인합니다. 알림 설정 페이지에서 선택하는 설정에 따라, Security Cloud Control Firewall Management에 표시되는 알림 유형이 결정됩니다.

이 드롭다운 페이지는 Overview(개요), All(모두), Dismissed(해제됨)의 3개 탭으로 그룹화됩니다.

Overview()

Overview(개요) 탭은 가장 최근의 우선 순위가 높은 알림 및 구독한 이벤트를 조합하여 표시합니다. 우선 순위가 높은 이벤트는 다음과 같습니다.

- 구축 실패
- 백업 실패
- 업그레이드 실패
- FTD를 클라우드 제공 Firewall Management Center(으)로 마이그레이션 실패
- 디바이스가 오프라인 상태가 됨
- 디바이스 HA 상태가 변경됨
- 디바이스 인증서 만료

Notifications(알림 설정) 창에서 Notification Settings(알림 설정)를 클릭하거나 UserID(사용자 ID) > User Preferences(사용자 환경설정) 페이지에서 수신할 알림을 구성할 수 있습니다. 대시보드 오른쪽 상단 모서리에 있는 User ID(사용자 ID) 버튼.

All()

All(모두) 탭은 이메일 구독 알림 및 높은 우선 순위로 나열된 모든 항목을 포함하여 우선 순위와 상관없이 모든 알림을 표시합니다.

Dismissed()

해제된 알림을 표시합니다. 알림의 "x"를 클릭하면 개별 알림을 무시할 수 있습니다.

드롭다운 메뉴에서 알림 Dismiss(해제)를 선택하면 "개요" 및 "모두" 탭 모두에서 알림이 해제됩니다. Dismiss(해제) 탭에 30일 동안 유지되며, 그 이후에는 Security Cloud Control에서 제거됩니다.

알림 드롭다운 창을 보는 경우, 위에서 언급한 탭 중 하나를 사용하여 키워드나 알림을 쿼리할 수 있습니다.

Preferences(환경설정) 페이지에서 개인 환경설정을 확인합니다. 이 페이지에서 다음 **"Notify Me in Security Cloud Control When(다음 상황일 때 알림)"** 알림을 구성하고 이메일 알림을 활성화하여 원하는 알림을 수신할 수 있습니다. [알림 환경설정](#)을 참조하십시오.

Security Cloud Control Firewall Management 테넌트에 연결된 디바이스에 특정 이벤트가 발생할 때마다 알림을 생성합니다. 여기에는 디바이스에서 수행한 작업, 만료 또는 만료된 디바이스 인증서 또는 보고서 생성 작업의 시작, 완료 또는 실패가 포함됩니다. 기본적으로 이러한 알림은 활성화되어 있으며 역할에 관계없이 테넌트와 연결된 모든 사용자에게 표시됩니다. 관심 있는 알림만 표시하도록 개인 알림 환경설정을 사용자 지정할 수 있습니다. 이러한 환경설정은 사용자에게 고유하며 테넌트에 연결된 다른 사용자에게 영향을 주지 않습니다.



주

또한 아래에 나열된 알림에 대한 변경 사항은 실시간으로 자동 업데이트되며 구축이 필요하지 않습니다.

- 구축 - 이 작업은 하며, SSH 또는 IOS 디바이스에 대한 통합 인스턴스는 포함하지 않습니다.
- 백업 - 이 작업은 FDM 관리 디바이스에만 적용됩니다.
- 업그레이드 - 이 작업은 ASA 및 FDM 관리 디바이스에만 적용됩니다.
- **Firewall Threat Defense**를 클라우드로 마이그레이션 - 이 작업은 Firewall Threat Defense Device Manager를 Firewall Management Center에서 Security Cloud Control로 변경할 때 적용됩니다.
- 오프라인 상태 - 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 온라인 재전환 - 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 충돌 탐지됨 - 테넌트와 연결된 모든 디바이스에 적용됩니다.
- **HA** 상태 변경됨 - HA 또는 패일오버 쌍 내의 디바이스, 현재 상태 및 변경 이전 상태를 나타냅니다. 이 작업은 테넌트와 연결된 모든 HA 및 패일오버 구성에 적용됩니다.
- 사이트 간 세션 연결 끊김 - 테넌트에 구성된 모든 사이트 간 VPN 구성에 적용됩니다.
- 보고서 생성 시작됨: 보고서 생성 작업이 시작되면 알림을 받습니다. 이는 즉시 및 예약된 검색에 모두 적용됩니다.
- 보고서 생성 완료: 보고서 생성 작업이 종료되면 알림을 받습니다. 이는 즉시 및 예약된 검색에 모두 적용됩니다.
- 보고서 생성 실패: 보고서 생성 작업이 실패하면 알림을 받습니다. 이는 즉시 및 예약된 검색에 모두 적용됩니다. 매개변수 또는 쿼리를 확인하고 다시 시도하십시오.

- 애플리케이션 사용 가능: 모니터링되는 애플리케이션을 사용할 수 있게 되면 알림을 전송합니다.
- 애플리케이션 사용 불가: 모니터링되는 애플리케이션을 사용할 수 없게 되면 알림을 전송합니다.

기본적으로 모든 알림 유형이 활성화됩니다. 알림 유형 수신을 중지하려면, 해당 알림을 지우고 **Save(저장)**를 클릭합니다.

선택한 알림에 대한 이메일을 수신하려면 'Email notifications(이메일 알림)' 토글 버튼을 활성화합니다.

기본적으로 **Use Security Cloud Control notification settings above**(위의 Security Cloud Control 알림 설정 사용)가 선택됩니다. 이 옵션을 선택하면 이메일 알림은 **Notify Me in Security Cloud Control When**(다음의 경우 Security Cloud Control에서 내게 알림 전송) 섹션에서 선택한 것과 동일한 알림 및 이벤트와 일치합니다.

일부 알림에 대해서만 이메일 알림을 받으려면 **Use Security Cloud Control notification settings above**(Security Cloud Control 알림 설정 사용)의 선택을 취소하고 이메일로 수신할 알림 유형을 선택한 다음 **Save(저장)**를 클릭합니다.

테넌트 로깅 사용량, 월별 한도, 재설정 시간, 기록 사용량 및 스토리지 옵션을 검토하는 방법을 알아봅니다.

로깅 설정을 사용하여 테넌트에 대한 현재 로깅 사용량을 확인합니다.

페이지에 다음이 표시됩니다.

- 월별 이벤트 로깅 한도.
- 한도가 재설정될 때까지의 일 수입입니다.
- Cisco 클라우드가 수신한 압축된 이벤트 데이터를 나타내는 저장된 로깅 사용량.

지난 12개월 동안 테넌트가 받은 로그를 검토하려면 **View Historical Usage**(사용 기록 보기)를 클릭합니다.

페이지에는 추가 스토리지를 요청하는 데 사용할 수 있는 링크도 포함되어 있습니다.

Security Cloud Control Firewall Management

사용자 역할이 각 Security Cloud Control Firewall Management 조직의 권한을 어떻게 정의하는지 알아봅니다.

Security Cloud Control Firewall Management에서는 사용자 및 조직별로 역할을 할당합니다. 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우 해당 사용자는 동일한 사용자 ID를 갖지만 조직마다 다른 역할을 가질 수 있습니다. 예를 들어 사용자가 한 조직에서는 '읽기 전용' 역할을 갖고, 다른 조직에서는 '슈퍼 관리자' 역할을 가질 수 있습니다.

인터페이스 또는 설명서에서 **Read-Only** 사용자, **Admin** 사용자 또는 **Super Admin** 사용자를 언급하는 경우 특정 조직에 대한 해당 사용자의 권한 수준을 의미합니다.

읽기 전용 역할이 할당된 사용자는 모든 페이지에서 이 파란색 배너를 볼 수 있습니다.

Read Only User. You cannot make configuration changes.

Read-Only 역할이 있는 사용자는 다음을 수행할 수 있습니다:

- **Security Cloud Control**의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 **VPN** 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 **API** 토큰을 생성, 새로 고침 및 취소합니다. 읽기 전용 사용자가 자신의 토큰을 취소하면 다시 생성할 수 없습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

Read-Only 역할이 있는 사용자는 다음을 수행할 수 없습니다:

- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- **Security Cloud Control** 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

편집 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다:

- 개체, 정책, 규칙 세트, 인터페이스, **VPN** 등을 포함하되 이에 국한되지 않는 디바이스 구성을 편집하고 저장합니다.
- **Read Configuration(구성 읽기)** 작업을 통해 이루어진 구성 변경을 허용합니다.
- 변경 요청 관리 작업을 활용합니다.

편집 전용 역할이 있는 사용자는 다음을 수행할 수 없습니다:

- 디바이스 또는 여러 디바이스에 변경 사항을 구축합니다.
- 단계적 변경 또는 **OOB**를 통해 감지된 변경을 폐기합니다.
- **AnyConnect** 패키지를 업로드하거나 이러한 설정을 구성합니다.
- 디바이스에 대한 이미지 업그레이드를 예약하거나 수동으로 시작합니다.
- 보안 데이터베이스 업그레이드를 예약하거나 수동으로 시작합니다.
- **Snort 2**와 **Snort 3** 버전을 수동으로 전환합니다.
- 템플릿을 생성합니다.
- 기존 **OOB** 변경 설정을 변경합니다.
- 시스템 관리 설정을 수정합니다.
- 디바이스를 온보딩합니다.
- 디바이스를 삭제합니다.
- **VPN** 세션 또는 사용자 세션을 삭제합니다.
- **Security Cloud Control** 사용자 레코드를 생성합니다.

- 사용자 역할을 변경합니다.

구축 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다:

- 디바이스 또는 여러 디바이스에 단계적 변경 사항을 구축합니다.
- ASA 디바이스에 대한 구성 변경 사항을 되돌리거나 복원합니다.
- 디바이스에 대한 이미지 업그레이드를 예약하거나 수동으로 시작합니다.
- 보안 데이터베이스 업그레이드를 예약하거나 수동으로 시작합니다.
- 변경 요청 관리 작업을 활용합니다.

Deploy-Only 역할이 있는 사용자는 다음을 수행할 수 없습니다:

- Snort 2와 Snort 3 버전 사이를 수동으로 전환합니다.
- 템플릿을 생성합니다.
- 기존 OOB 변경 설정을 변경합니다.
- 시스템 관리 설정을 수정합니다.
- 디바이스를 온보딩합니다.
- 디바이스를 삭제합니다.
- VPN 세션 또는 사용자 세션을 삭제합니다.
- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- Security Cloud Control 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

VPN

VPN Sessions Manager 역할은 사이트 간 VPN 연결이 아닌 원격 액세스 VPN 연결을 모니터링하는 관리자를 위해 설계되었습니다.

VPN 세션 관리자 역할이 있는 사용자는 다음을 수행할 수 있습니다:

- Security Cloud Control의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 RA VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 참고로 VPN 세션 관리자 사용자가 자신의 토큰을 취소하면 토큰을 다시 만들 수 없습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보냅니다.
- 기존 RA VPN 세션을 종료합니다.

VPN 세션 관리자 역할이 있는 사용자는 다음을 수행할 수 없습니다:

- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- **Security Cloud Control** 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

'관리자' 역할의 사용자는 **Security Cloud Control Firewall Management**의 대부분의 영역에 대한 완전한 액세스 권한을 갖습니다.

- **Security Cloud Control Firewall Management**에서 개체 또는 정책을 생성, 읽기, 업데이트 및 삭제하고 설정을 구성합니다.
- 디바이스를 온보딩합니다.
- **Security Cloud Control**의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 토큰이 취소되면 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

관리 사용자는 다음을 수행할 수 없습니다.

- **Security Cloud Control** 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.

Super Admin(슈퍼 관리자) 역할이 있는 사용자는 **Security Cloud Control Firewall Management**의 모든 영역에 대한 완전한 액세스 권한을 갖습니다.

슈퍼 관리자 역할의 사용자는 다음을 수행할 수 있습니다.

- 사용자 역할 변경
- 사용자 레코드를 생성합니다.
- **Security Cloud Control Firewall Management**에서 개체 또는 정책을 생성, 읽기, 업데이트 및 삭제하고 설정을 구성합니다.
- 디바이스를 온보딩합니다.
- **Security Cloud Control Firewall Management**의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.

- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 토큰이 취소되면 다음을 수행할 수 있습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

,

디바이스 유형, 상태, 버전, 커넥터, 관리 애플리케이션, 레이블 등의 속성을 기준으로 디바이스, 정책 및 개체를 필터링하는 방법을 알아봅니다.

Security Devices(보안 디바이스), **Policies(정책)** 및 **Objects(개체)** 페이지에서 필터를 사용하여 디바이스 및 개체를 찾습니다. 필터링하려면 왼쪽 창에서 필터 아이콘을 선택합니다.

Security Devices(보안 디바이스) 페이지의 필터 패널에서는 디바이스 유형, 하드웨어 버전, 소프트웨어 버전, Snort 버전, 구성 상태, 연결 상태, 충돌 탐지, Secure Device Connector 및 레이블과 같은 기준으로 디바이스를 필터링할 수 있습니다. 선택한 디바이스 유형 탭 내에서 필터를 적용할 수 있습니다.

FTD 탭이 열려 있으면 필터 패널을 사용하여 Security Cloud Control가 액세스에 사용하는 관리 애플리케이션별로 **FTD** 디바이스를 필터링할 수도 있습니다.

필터링하려면 **Security Devices(보안 디바이스)**, **Policies(정책)** 및 **Objects(개체)** 탭의 왼쪽 창에서  을 클릭합니다.



주

FTD 탭이 열리면 필터 창이 Security Cloud Control에서 디바이스에 액세스하는 데 사용되는 관리 애플리케이션을 기반으로 **FDM** 관리 디바이스를 표시하는 필터를 제공합니다.

- **FDM: FTD API** 또는 **Firewall Device Manager**을(를) 사용하여 관리되는 디바이스.
- **FMC-FTD: Firepower Management Center**를 사용하여 관리되는 디바이스.
- **FTD: FTD 관리**를 사용하여 관리되는 디바이스.

제

4

장

:

- [Secure Connectors](#) □□

Secure Connectors

보안 커넥터가 네트워크 또는 클라우드 환경에서 **Security Cloud Control** 방화벽 관리와 관리 리소스 간의 통신을 지원하는 방법을 알아봅니다.

보안 커넥터는 네트워크 또는 지원되는 클라우드 환경에서 실행되는 커넥터 인스턴스이며, **Security Cloud Control Firewall Management**과(와) 매니지드 리소스 간의 보안 통신 경로를 제공합니다. 보안 커넥터는 **Security Cloud Control Firewall Management**가 인터넷에서 직접 연결할 수 없는 디바이스를 관리하는 데 도움이 되며, 로깅 및 애널리틱스 워크플로우를 위한 이벤트 전달을 지원합니다.

Secure Connector(보안 커넥터) 페이지를 사용하여 테넌트에 대한 커넥터 인스턴스를 보고, 구축하고, 관리합니다.

Secure Connector

Secure Connector 페이지에는 다음과 같은 커넥터 유형이 포함될 수 있습니다.

- **SDC(Secure Device Connector)**: **Security Cloud Control Firewall Management**과(와) 지원되는 매니지드 디바이스 간의 보안 통신 경로를 제공합니다.
- **SEC(Secure Event Connector)**: 지원되는 디바이스에서 이벤트를 수신하여 로깅 및 분석을 위해 **Cisco** 클라우드로 전달합니다.

Secure Device Connector

Secure Device Connector(SDC)는 인터넷에서 **Cisco** 디바이스에 직접 접속할 수 없을 때, 해당 디바이스가 **Security Cloud Control Firewall Management**와 통신할 수 있도록 해주는 지능형 프록시입니다. 디바이스 자격 증명을 사용하여 디바이스를 온보딩할 때, 네트워크 내에 **SDC**를 구축하여 디바이스와 **Security Cloud Control Firewall Management** 간의 통신을 프록시할 수 있습니다. 디바이스에 인터넷에서 직접 접속할 수 있는 경우, **SDC**를 사용하는 대신 디바이스의 외부 인터페이스를 통해 직접 통신을 허용할 수 있습니다. **SDC**은(는) 다음 기능을 수행합니다:

- 매니지드 디바이스에 대한 명령 및 메시지를 **Security Cloud Control Firewall Management**에서 모니터링합니다.
- **Security Cloud Control Firewall Management**를 대신하여 명령을 실행합니다.
- 매니지드 디바이스로 메시지를 릴레이합니다.
- 디바이스 응답을 반환합니다.

SDC과 **Security Cloud Control Firewall Management** 사이의 통신에 **TLS 1.3** 및 **AES-128-GCM**이 포함된 **HTTPS**가 사용됩니다. 온보딩된 디바이스 및 서비스에 대한 모든 자격 증명은 브라우저에서 **SDC**로 직접 암호화되며, **AES-128-GCM**을 사용하여 저장 상태에서도 암호화됩니다. **SDC**만 디바이스 자격 증명에 액세스할 수 있습니다.

Secure Device Connector 또는 **SEC(Secure Event Connector)**를 생성하려면 슈퍼 관리자 역할의 사용자가 필요합니다.

SDC를 통해 이러한 디바이스를 **Secure Device Connector**에 온보딩할 수 있습니다.

- 자격 증명 방법을 사용한 온프레미스 방화벽 **Management Center**
- **Meraki MX** 디바이스
- 일반 **SSH** 디바이스
- **Cisco IOS** 디바이스

클라우드 제공 **Firewall Management Center**에서 관리하는 **Secure Firewall Threat Defense** 디바이스는 **SDC**이(가) 필요하지 않으며 프록시를 통한 온보딩을 지원하지 않습니다. 이러한 디바이스가 클라우드 제공 **Firewall Management Center**에 연결할 수 있도록 적절한 **DNS** 설정과 아웃바운드 인터넷 연결이 있는지 확인합니다.

SDC와 **Security Cloud Control** 간의 통신을 허용하는 방법에 대한 자세한 내용은 [직접 클라우드 연결성 위한 인바운드 액세스 허용](#) 페이지 48의 내용을 참조하십시오.

자세한 내용은 [Secure Device Connector](#) 및 [Secure Event Connector](#)을 위한 **VM** 구축 페이지 49를 참조하십시오.

Security Cloud Control Firewall Management은 클라우드 커넥터 또는 **SDC**을(를) 통해 매니지드 디바이스에 연결합니다.

1:

연결 방법	다음 경우 사용	필요한 네트워크 액세스
직접 Cloud Connector	디바이스는 인터넷에서 직접 연결할 수 있습니다.	포트 443 또는 디바이스 관리에 사용하는 포트에서 클라우드 지역에 대한 Security Cloud Control Firewall Management IP 주소의 인바운드 액세스를 허용합니다.
SDC	인터넷에서 디바이스에 직접 연결할 수 없거나 소스에 온프레미스 SDC 가 명시적으로 필요합니다.	포트 443 또는 디바이스 관리에 사용하는 포트의 SDC 에서 전체 인바운드 액세스를 허용합니다. SDC VM 이 디바이스 관리 인터페이스에 연결할 수 있는지 확인합니다.

FDM 관리 디바이스는 인터넷에서 직접 액세스할 수 있는지 여부와 관계없이 디바이스 자격 증명, 등록 키 또는 일련 번호를 사용하여 **Security Cloud Control Firewall Management**에 온보딩할 수 있습니다. **FDM** 관리 디바이스가 인터넷에 직접 액세스할 수 없지만 인터넷에 액세스할 수 있는 네트워크에 있는 경우, 디바이스의 일부로 제공되는 **Security Services Exchange** 커넥터가 **Security Services Exchange** 클라우드에 연결하여 디바이스를 온보딩할 수 있습니다.

소스에서 다음을 온보딩하기 위해 온프레미스 **SDC**가 필요하다고 명시적으로 설명합니다.

- 클라우드에서 액세스할 수 없는 **ASA** 디바이스
- 자격 증명 온보딩 방법을 사용할 때 클라우드에서 액세스할 수 없는 **FDM** 관리 디바이스
- **Cisco IOS** 디바이스
- **SSH** 액세스가 가능한 디바이스

Security Cloud Control Firewall Management가 **Cloud Connector**를 사용하여 연결하므로 다른 모든 디바이스와 서비스에는 온프레미스 **SDC**이(가) 필요하지 않습니다.

SDC Docker

SDC는 **Docker** 컨테이너로 실행됩니다. **Docker**는 일반적으로 기본 브리지 네트워크 **docker0**에 172.17.0.0/16 서브넷을 사용합니다.

172.17.0.0/16 또는 **Docker**가 할당한 네트워크 공간의 일부가 기존 네트워크 **IP** 공간과 겹치는 경우, 구축하기 전에 **Docker** 네트워크 기본값을 변경한 다음 **SDC**을(를) 구축합니다. 대체 네트워크를 사용하려면 **/etc/docker/daemon.json** 구성을 편집합니다.

예를 들어 **Docker** 네트워킹 주소 풀에 슈퍼넷 10.198.0.1/24를 사용하고 IP 주소 10.198.128.0/17을 사용하여 서브넷 10.198.0.0/24의 기본 **docker** 브리지 인터페이스 **docker0**으로 사용합니다.

```
sudo vi /etc/docker/daemon.json

{
  "log-driver": "json-file",
  "log-opts": {
    "max-size": "100m",
    "max-file": "5"
  },
  "bip": "10.198.0.1/24",
  "default-address-pools": [
    {
      "base": "10.198.128.0/17",
      "size": 24
    }
  ]
}

(save and exit)

sudo reboot (required)
```

자세한 내용은 [네트워킹 개요](#)를 참조하십시오.

Security Cloud Control는 **Cloud Connector** 또는 (**SDC**)를 통해 관리하는 디바이스에 연결합니다.

Cloud Connector를 통해 디바이스에 직접 **Security Cloud Control Firewall Management**을 연결하는 경우 해당 지역의 IP 주소로부터 포트 443 또는 디바이스 관리용으로 구성된 포트에서의 인바운드 액세스를 허용합니다.

2:

지역	URL	다음으로부터의 인바운드 액세스 허용
아시아-태평양-일본(APJ)	https://security.cisco.com	54.199.195.111, 52.199.243.0
호주(AUS)	https://security.cisco.com	13.55.73.159, 13.238.226.118
유럽, 중동 및 아프리카(EMEA)	https://security.cisco.com	35.157.12.126, 35.157.12.15
인도(IN)	https://security.cisco.com	35.154.115.175 13.201.213.99
미국(US)	https://security.cisco.com	52.34.234.2 52.36.70.147

SDC

각 **Security Cloud Control Firewall Management** 조직에는 **SDC**(를) 무제한으로 포함할 수 있습니다. **SDC**은 한 조직에만 속하며 여러 조직 간에 공유되지 않습니다.구축을 계획할 경우 하나의 **SDC**이 약 500개의 디바이스를

지원할 것으로 예상됩니다. 실제 용량은 해당 디바이스에서 활성화된 기능 및 구성 파일의 크기에 따라 달라집니다.

둘 이상의 SDC을(를) 구축하면 다음을 수행할 수 있습니다.

- 성능 저하 없이 디바이스 관리를 확장합니다.
- 디바이스를 동일한 **Security Cloud Control Firewall Management** 조직 내에 유지하면서, SDC를 분리된 네트워크 세그먼트에 배치합니다.
- 각각의 추가 SDC에 대한 부트스트랩 절차에 따라 하나의 호스트에서 여러 개의 SDC를 실행합니다.

첫 번째 SDC 이름은 테넌트 이름과 숫자 1을 포함합니다. 각각의 추가 SDC은(는) 순서대로 번호가 매겨집니다.

Secure Device Connector Secure Event Connector VM

디바이스 자격 증명을 사용하여 **Security Cloud Control**를 디바이스에 연결하는 경우 네트워크에 SDC를 다운로드하고 구축하여 **Security Cloud Control**와 디바이스 간의 통신을 관리하는 것이 가장 좋습니다. 일반적으로 이러한 디바이스는 경계를 기반으로 하지 않으며 공용 IP 주소가 없거나 외부 인터페이스에 대한 개방형 포트가 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 **Security Cloud Control**를 모니터링합니다. SDC는 **Security Cloud Control**를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 **Security Cloud Control**에 메시지를 전송하고, 매니지드 디바이스에서 **Security Cloud Control**로 응답을 반환합니다.

단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다. 자세한 정보는 [단일 Security Cloud Control 테넌트에서 여러 SDC 사용](#)을 참조하십시오.

이 절차에서는 **Security Cloud Control**의 VM 이미지를 사용하여 네트워크에 SDC를 설치하는 방법을 설명합니다. 이는 SDC를 생성하는 권장 방법입니다.

시작하기 전에

- **Security Cloud Control**는 엄격한 인증서 확인이 필요하며 SDC(Secure Device Connector)와 인터넷 간의 웹 또는 콘텐츠 프로ksi 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 SDC와 **Security Cloud Control** 간의 트래픽 검사를 비활성화합니다.
- SDC는 TCP 포트 443 또는 디바이스 관리를 위해 구성된 포트에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.
- **Security Cloud Control**에서 관리하는 디바이스는 SDC VM의 IP 주소로부터의 인바운드 트래픽을 허용해야 합니다.
- [직접 클라우드 연결성 위한 인바운드 액세스 허용](#) 페이지 48를 **Secure Device Connector**에 연결을 검토하여 적절한 네트워크 액세스를 확인합니다.
- 네트워크에서 프록시를 사용하는 경우, 호스트 설정 명령을 실행하기 전에 필요한 모든 세부 정보를 준비합니다. 문제는 잘못된 프록시 설정과 관련이 있습니다. 중요한 세부 정보:
 - IP/호스트 이름.
 - 프록시가 트래픽을 가로채고 자체 인증서를 사용하여 다시 암호화하는지 여부. 이 세부 정보 때문에 SDC VM 설정과 관련된 대부분의 복잡성이 발생합니다.
 - 프록시가 트래픽을 가로채는 경우, VM 구성 시 루트 인증서를 준비하십시오. 메시지가 표시되면 붙여넣어 호스트 및 SDC가 프록시에서 생성한 인증서를 신뢰함을 알 수 있도록 할 수 있습니다.
 - 프록시가 트래픽을 가로채지 않는다면, 여기에 추가로 필요한 것은 없습니다.
- 다음 항목들은 프록시된 HTTP 및 HTTPS 연결에서 동일할 가능성이 가장 높습니다. 그러나 각 프로토콜마다 다른 프록시를 사용하는 경우, 각각에 대해 다음의 모든 것이 필요합니다.
 - 프록시 IP 주소

- 사용하는 프록시 포트
- 프록시 자체에 대한 연결이 HTTPS를 통해 이루어져야 하는지 여부(일반적으로 해당되지 않음). 예를 들어 프록시 주소가 <https://proxy.corp.com:80>로 나열되어 있으면 Yes로 응답합니다. 나열된 주소가 <http://proxy.corp.com:80>라면 No로 답해야 합니다. 두 URL 모두 포트 80을 사용하지만 프로토콜이 다르다는 점에 유의합니다.
- 프록시 인증 세부 정보:
 - 프록시가 인증을 요구하는지 여부(대부분은 요구하지 않음)
 - Yes라면 호스트를 구성할 때 사용할 수 있는 사용자 이름과 비밀번호가 필요합니다.
- Security Cloud Control은 vSphere 웹 클라이언트 또는 ESXi 웹 클라이언트를 사용하여 SDC VM OVF 이미지 설치를 지원합니다.
- Security Cloud Control는 vSphere 데스크톱 클라이언트를 사용한 SDC VM OVF 이미지 설치를 지원하지 않습니다.
- Security Cloud Control에서는 자체 Ubuntu 인스턴스에 SDC 설치를 지원합니다. 현재 버전 20LTS부터 24LTS까지 지원됩니다.
- ESXi 5.1 하이퍼바이저.
- 하나의 SDC를 가진 VM의 시스템 요구 사항:
 - vCPU 2개
 - 2GB 메모리
 - 64GB의 디스크 공간
- 호스트에 추가하는 각 SDC에는 vCPU 1개 및 1GB RAM이 필요합니다.
- Cisco Security Analytics 및 로깅에 사용되는 구성 요소인 SEC 하나를 탑재한 VM의 시스템 요구 사항:
 - vCPU 최소 4개
 - 8GB 메모리
- 호스트에 SEC를 추가할 때마다 해당 리소스를 두 배로 늘려야 합니다. 따라서 VMware ESXi 호스트에 SDC 1개와 SEC 1개를 구성할 경우 요구 사항은 다음과 같습니다.
 - vCPU 6개
 - 10GB 메모리
 - 64GB의 디스크 공간
- 호스트에서 네트워킹을 수동으로 구성하려면 다음 정보를 수집합니다.
 - SDC에 사용할 고정 IP 주소

- **cdouser**(또는 **sudo** 액세스 권한이 있는 사용자) 및 **sdcc** 사용자(**Docker**를 실행하는 사용자)에 사용할 비밀번호
 - 조직에서 사용하는 **DNS** 서버의 **IP** 주소
 - **SDC** 주소가 있는 네트워크의 게이트웨이 **IP** 주소
 - 시간/**NTP** 서버의 **FQDN** 또는 **IP** 주소.
- **SDC** 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 **80** 아웃바운드를 열어야 합니다.

네트워크에서 아웃바운드 연결에 허용/차단 목록을 사용하는 경우, 보안 업데이트를 적용할 수 있도록 **ubuntu.com**에 대한 연결을 허용해야 합니다.



주

우분투는 체크섬으로 업데이트를 보호하며 **HTTPS**가 아닌 **HTTP**만 사용합니다. 보안 업데이트를 받으려면 **ubuntu.com**에 대한 **HTTP** 연결을 허용해야 합니다.

VM

SDC 및 **SEC**를 실행하는 데 사용되는 **VM**을 구축하는 방법에는 두 가지 옵션이 있습니다.

1. 아래 단계에 따라 **Security Cloud Control**에서 제공하는 **VMware** 이미지를 다운로드합니다.
2. **Ubuntu 20, 22** 또는 **24**를 직접 구축. 자체 **Ubuntu** 인스턴스를 구축하는 경우, 다음 섹션을 건너뛰고 **VM** 구성 섹션으로 진행할 수 있습니다.

절차

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Administration(관리) > Integration(통합) > Secure Connectors(보안 커넥터)**를 클릭합니다.
3. **Services(서비스)** 페이지에서 **Secure Connectors(보안 커넥터)** 탭을 선택하고 파란색 플러스 버튼을 클릭한 후 **Secure Device Connector(보안 디바이스 커넥터)**를 선택합니다.
4. **Download the SDC VM image(SDC VM 이미지 다운로드)**를 클릭합니다. 새 탭에서 열립니다.
5. **.zip** 파일의 모든 파일을 추출합니다. 다음과 같이 표시됩니다.
 - CDO-SDC-VM-ddd50fa.ovf
 - CDO-SDC-VM-ddd50fa.mf
 - CDO-SDC-VM-ddd50fa-disk1.vmdk
6. **vSphere** 웹 클라이언트를 사용하여 **VMware** 서버에 관리자로 로그인합니다.



ESXi 웹 클라이언트를 사용하지 마십시오.

지시에 따라 OVF 템플릿에서 **Secure Device Connector** 가상 머신을 구축합니다.

7. 설정이 완료되면 **SDC VM**의 전원을 켭니다.
8. 새 **SDC VM**의 콘솔을 엽니다.
9. **cdo** 사용자 이름으로 로그인합니다. 기본 암호는 **adm123**입니다.

VM

이제 구축한 VM 이미지의 콘솔을 가져올 수 있으며, 직접 VM을 구축하고 SSH를 활성화한 경우에는 SSH를 통해 접속할 수도 있습니다. **SDC** 또는 **SEC Docker** 컨테이너를 실행할 수 있도록 호스트를 준비하려면 구성 스크립트를 실행해야 합니다.

1. **Security Cloud Control** 제공 VM을 다운로드한 경우, CLI가 이미 설치되어 있으며 2단계로 진행할 수 있습니다. 자체 VM을 구축한 경우 SSH로 연결하고 명령을 실행하여 CLI를 설치합니다.

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
&& tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh &&
./install.sh
```

2. 다음 명령어를 실행하여 호스트 구성을 시작합니다.

```
sudo sdc host configure
```

3. 비밀번호가 표시되면 **Security Cloud Control** 제공 VM의 경우 **adm123**을 입력하거나 자체 VM에 대해 선택한 관리자 비밀번호를 입력합니다.
4. 프롬프트에 따라 **sdc** 사용자를 구성합니다.
5. 네트워크 구성에 대한 프롬프트가 표시되면 다음 중 하나를 선택합니다.
 - 이 호스트에 정적 IP를 수동으로 구성: 이 호스트의 IP, 게이트웨이, DNS 서버 등을 지정하고 VM의 시스템 구성에 기록하려는 경우.
 - DHCP: VM에 고정 IP를 할당하는 DHCP 서버가 있는 경우.
 - 정적 IP는 이미 설정되어 있으며, 현재 네트워크 설정을 변경하고 싶지 않습니다.
6. 프록시 구성에 관한 질문이 표시되면 답변합니다. 이 주제의 상단에 있는 상세 목록을 검토하여 모든 필수 조건 및 잠재적인 프록시 구성 옵션을 확인합니다.
7. 프록시를 구성한 경우, 모든 프록시 설정을 적용하려면 VM을 재부팅하라는 메시지가 표시됩니다. 그렇지 않은 경우 재부팅을 요청받지 않으며 8단계로 진행할 수 있습니다.
8. 사용자 지정 인터넷 접속 테스트 URL 설정. 기본적으로 모든 아웃바운드 연결을 차단하는 경우에만 이 작업을 수행하면 됩니다. 해당 사항이 있다면, 허용 목록에 포함된 공개적으로 접근 가능한 웹 URL(예: <https://google.com>)을 지정합니다.
9. 최신 보안 패치를 설치합니다. 일부는 운영체제 도구와 **Docker** 서버가 필요합니다.
10. 프롬프트가 표시되면, 스크립트가 SSH 구성을 강화하도록 할 것인지 여부를 선택합니다.

VM을 사용하는 경우 계속 진행합니다. 자체 VM을 사용하고 SSH를 직접 구성하는 경우 현재 구성이 변경되지 않도록 이 단계를 건너뛸 수 있습니다.

11. SDC 또는 SEC 및 CLI 자체에 대한 자동 업데이트를 활성화하라는 메시지가 표시되면, 이 작업을 수행하여 버그 수정, 패치 및 새로운 기능을 최신 상태로 유지하는 것이 좋습니다. 정책으로 인해 자동 업데이트를 허용할 수 없는 경우에는 [Secure Device Connector 업데이트](#)를 참조하십시오.

VM

디바이스 자격 증명을 사용하여 Security Cloud Control를 디바이스에 연결하는 경우, 네트워크에서 SDC(Secure Device Connector)를 다운로드하고 구축하여 Security Cloud Control와 디바이스 간의 통신을 관리하는 것이 모범 사례입니다. 일반적으로 이러한 디바이스는 경계를 기반으로 하지 않으며 공용 IP 주소가 없거나 외부 인터페이스에 대한 개방형 포트가 있습니다. ASA(Adaptive Security Appliance), FDM 관리 디바이스, FMC(Firepower Management Center) 디바이스는 모두 디바이스 자격 증명을 사용하여 Security Cloud Control에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 Security Cloud Control를 모니터링합니다. SDC는 Security Cloud Control를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 Security Cloud Control에 메시지를 전송하고, 매니지드 디바이스에서 Security Cloud Control로 응답을 반환합니다.

단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다. 자세한 내용은 [하나의 조직에서 여러 개의 Secure Device Connector\(를\) 사용합니다](#) 페이지 67를 참조하십시오.

이 절차에서는 자체 가상 머신 이미지를 사용하여 네트워크에 SDC를 설치하는 방법을 설명합니다.

주

SDC를 설치하는 가장 쉽고 신뢰할 수 있는 방법은 Security Cloud Control의 SDC OVA 이미지를 다운로드하여 설치하는 것입니다.

- Security Cloud Control는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시를 지원하지 않습니다.
- SDC가 Security Cloud Control와 통신하려면 TCP 포트 443에서 인터넷에 대한 전체 아웃바운드 액세스 권한이 있어야 합니다.
- SDC를 통해 Security Cloud Control에 접속하는 디바이스는 포트 443에서 SDC로부터의 인바운드 액세스를 허용해야 합니다.
- 네트워킹 지침은 [Secure Device Connector를 사용하여 Security Cloud Control에 연결](#)을 검토하십시오.
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트

주

vSphere 데스크톱 클라이언트를 사용한 설치 지원되지 않습니다.

- ESXi 5.1 하이퍼바이저.
- Ubuntu 22.04 및 Ubuntu 24.04 운영 체제.

- SDC만 있는 VM의 시스템 요구 사항:
 - VMware ESXi 호스트에는 CPU 2개가 필요합니다.
 - VMware ESXi 호스트에는 최소 2GB의 메모리가 필요합니다.
 - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다. 이 값은 필요에 따라 필요한 디스크 공간을 확장할 수 있도록 파티션과 함께 LVM(논리적 볼륨 관리)을 사용한다고 가정합니다.
- VM의 CPU와 메모리를 업데이트한 후 VM의 전원을 켜고 Secure Connector(보안 커넥터) 페이지에 SDC가 "Active(활성)" 상태로 표시되는지 확인합니다.
- 이 절차를 수행하는 사용자는 Linux 환경에서 작업하고 파일 편집을 위해 vi 시각적 편집기를 사용하는 데 익숙해야 합니다.
- CentOS 가상 머신에 온프레미스 SDC를 설치하는 경우 정기적으로 Yum 보안 패치를 설치하는 것이 좋습니다. Yum 구성에 따라 Yum 업데이트를 가져오려면 포트 80 및 443에서 아웃바운드 액세스를 열어줘야 할 수 있습니다. 또한 업데이트를 예약하려면 yum-cron 또는 crontab을 구성해야 합니다. 보안 운영 팀과 함께 Yum 업데이트를 받기 위해 변경해야 하는 보안 정책이 있는지 확인합니다.



주

시작하기 전에: 절차의 명령을 복사하여 터미널 창에 붙여넣지 말고 대신 입력하십시오. 일부 명령에는 "n-대시"가 포함되며, 잘라내기 및 붙여넣기 프로세스에서 이러한 명령은 "m-대시"로 적용되어 명령이 실패할 수 있습니다.

1. SDC를 생성할 Security Cloud Control 테넌트에 로그인합니다.
2. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
3. 왼쪽 창에서 **Administration(관리) > Integration(통합) > Secure Connectors(보안 커넥터)**를 클릭합니다.
4. **Services(서비스)** 페이지에서 **Secure Connectors(보안 커넥터)** 탭을 선택하고 파란색 플러스 버튼을 클릭한 후 **Secure Device Connector(보안 디바이스 커넥터)**를 선택합니다.
5. 창의 2단계에서 부트스트랩 데이터를 메모장에 복사합니다.
6. 최소 SDC에 할당된 다음 RAM 및 디스크 공간을 사용하여 **CentOS 7** 가상 머신을 설치합니다.
 - 8GB RAM
 - 10GB 디스크 공간
7. 설치가 완료되면 SDC의 IP 주소, 서브넷 마스크 및 게이트웨이를 지정하는 등의 기본 네트워킹을 구성합니다.
8. DNS(Domain Name Server) 서버를 구성합니다.
9. NTP(Network Time Protocol) 서버를 구성합니다.
10. SDC의 CLI와의 손쉬운 상호 작용을 위해 CentOS에 SSH 서버를 설치합니다.

11. Yum 업데이트를 실행한 후 **open-vm-tools**, **nettools** 및 **bind-utils** 패키지를 설치합니다.

```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools
bind-utils
```

12. AWS CLI 패키지를 설치합니다. <https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html>의 내용을 참조하십시오.



주

--user 플래그를 사용하지 마십시오.

13. Docker CE 패키지를 설치합니다. <https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce>의 내용을 참조하십시오.



주

"저장소를 사용하여 설치" 방법을 사용합니다.

14. Docker 서비스를 시작하고 부팅 시 시작되도록 활성화합니다.

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service
to
/usr/lib/systemd/system/docker.service.
```

15. 두 사용자(cdo 및 sdc)를 생성합니다. 루트 사용자에게 직접 액세스하지 않고 관리 작업을 수행하려면 cdo 사용자를 사용합니다. sdc 사용자는 SDC 도커 컨테이너를 실행하도록 지정됩니다.

```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

16. sdc 사용자의 비밀번호를 생성합니다.

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

17. sdc 사용자를 wheel 그룹에 추가하여 관리(sudo) 권한을 부여합니다.

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

- 18** Docker가 설치되면 사용자 그룹이 생성됩니다. CentOS/Docker 버전에 따라 "docker" 또는 "dockerroot"라고 부를 수 있습니다. `/etc/group` 파일을 확인하여 어떤 그룹이 생성되었는지 확인한 다음 `sdc` 사용자를 이 그룹에 추가합니다.

```
[root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

- 19** `/etc/docker/daemon.json` 파일이 없는 경우 파일을 생성하고 아래 내용을 입력합니다. 생성되면 `docker` 데몬을 다시 시작합니다.



"group" 키에 입력한 그룹 이름이 이전 단계의 `/etc/group` 파일에서 찾은 그룹과 일치하는지 확인합니다.

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
{
  "live-restore": true,
  "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

- 20** 현재 vSphere 콘솔 세션을 사용 중인 경우 SSH로 전환하고 `cdo` 사용자로 로그인합니다. 로그인한 후에는 `sdc` 사용자로 변경합니다. 암호를 묻는 메시지가 표시되면 `cdo` 사용자의 암호를 입력합니다.

```
[CDO@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

- 21** 디렉터리를 `/usr/local/CDO`로 변경합니다.

- 22** `bootstrapdata`라는 새 파일을 생성하고 온프레미스 보안 디바이스 커넥터 구축 마법사의 2단계에서 가져온 부트스트랩 데이터를 이 파일에 붙여넣습니다. 파일을 **Save(저장)**합니다. `vi` 또는 `nano`를 사용하여 파일을 생성할 수 있습니다.

- 23** 부트스트랩 데이터는 `base64`로 인코딩됩니다. 이를 디코딩하고 `extractedbootstrapdata`라는 파일로 내보냅니다.

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/CDO/bootstrapdata >
/usr/local/CDO/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

`cat` 명령을 실행하여 디코딩된 데이터를 확인합니다. 명령 및 디코딩된 데이터는 다음과 같이 표시됩니다.

```
[sdc@sdc-vm ~]$ cat /usr/local/CDO/extractedbootstrapdata
CDO_TOKEN="<token string>"
CDO_DOMAIN="www.defenseorchestrator.com"
CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

24 다음 명령을 실행하여 디코딩된 부트스트랩 데이터의 섹션을 환경 변수로 내보냅니다.

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv &&
source sdcenv
[sdc@sdc-vm ~]$
```

25 Security Cloud Control에서 부트스트랩 번들을 다운로드합니다.

```
[sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN"
"$CDO_BOOTSTRAP_URL"
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:--
10654
[sdc@sdc-vm ~]$ ls -l /usr/local/ CDO/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48
/usr/local/CDO/tenant-name-SDC
```

26 SDC tarball의 압축을 풀고 bootstrap.sh 파일을 실행하여 SDC 패키지를 설치합니다.

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/CDO/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/ CDO/bootstrap/bootstrap.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to
 toolkit/toolkit.tar
 toolkit.sh
 common.sh
 [2018-07-23 13:54:04] startup new container
 Unable to find image 'ciscoDefenseOrchestrator/sdc_prod:latest'
 locally

sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458:
Pulling from
 ciscoDefenseOrchestrator/sdc_prod
 08d48e6f1cff: Pull complete
 ebbd10b629b1: Pull complete
 d14d580ef2ed: Pull complete
 45421d451ab8: Pull complete
<snipped - downloads>
no crontab for sdc
```

이제 SDC가 Security Cloud Control에서 "Active(활성)"로 표시됩니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Administration(관리) > Integration(통합) > Secure Connectors(보안 커넥터)**를 클릭합니다.
3. **Services(서비스)** 페이지에서 **Secure Connectors(보안 커넥터)** 탭을 선택하고, + 아이콘을 클릭한 후, **Secure Device Connector(보안 디바이스 커넥터)**를 선택합니다.
4. 창 의 2단계에서 부트스트랩 데이터를 메모장에 복사합니다.
5. 관리자 사용자(일반적으로 cdo)와 선택한 비밀번호를 사용하여 VM에 SSH로 연결합니다.

6. 다음 명령을 입력하여 `sdc` 사용자로 전환합니다.

```
sudo su - sdc
```

7. 다음 명령을 사용하여 새 SDC를 부트스트랩합니다.

```
sdc bootstrap <paste-your-bootstrap-data-here>
```

8. 사용하려는 SDC의 버전을 선택합니다.

SDC 버전에는 세 가지 옵션이 있습니다.

- SDC 2024 - 대부분의 사용자가 실행하고자 하는 버전입니다.
- FIPS가 활성화된 SDC 2024 - FedRamp 컴플라이언스가 적용되는 경우 이 버전을 선택합니다.
- SDC 레거시 - 이 버전은 더 이상 기능 업데이트를 수신하지 않으므로 대신 SDC 2024를 실행하는 것이 좋습니다.

9. CLI는 컨테이너 이미지를 가져와 SDC를 시작합니다. 사용자 인터페이스에서 SDC가 활성화되고 정상 작동하는지 확인할 수 있으며, 호스트에서도 다음 명령을 실행하여 확인할 수 있습니다.

```
sdc show running
```

테넌트에 대한 SDC가 표시됩니다.

Terraform vSphere Secure Device Connector

이 절차에서는 [vSphere용 Security Cloud Control SDC Terraform 모듈](#)을 [Security Cloud Control Terraform](#) 제공자와 함께 사용하여 SDC를 vSphere에 구축하는 방법을 자세히 설명합니다. 이 작업 절차를 수행하기 전에 다음 사전 요구 사항을 검토하십시오.

- vSphere 데이터센터 버전 7 이상을 보유하고 있습니다.
- 데이터센터에 관리자 어카운트가 있으며, 다음 작업을 수행할 수 있는 권한이 있습니다.
 - VM 생성
 - 폴더 생성
 - 콘텐츠 라이브러리 생성
 - 콘텐츠 라이브러리에 파일 업로드
- Terraform 정보

-
1. Security Cloud Control에서 API 전용 사용자를 생성하고 API 토큰을 복사합니다. API 전용 사용자를 생성하는 방법을 알아보려면 [API 전용 사용자 생성](#)을 참조하십시오.
 2. Security Cloud Control Terraform 제공자의 지침에 따라 Terraform 저장소에서 [Security Cloud Control Terraform](#) 제공자를 구성합니다.

Example

```

terraform {
  required_providers {
    cdo = {
      source = "CiscoDevNet/cdo"
      version = "0.7.0"
    }
  }
}

provider "cdo" {
  base_url = "<the CDO URL you use to access CDO>"
  api_token = "<the API Token generated in step 1>"
}

```

3. **Security Cloud Control Terraform** 제공자를 사용하여 `cdo_sdc` 리소스를 생성하는 **Terraform** 코드를 작성합니다. 자세한 내용은 [Security Cloud Control-sdc 리소스에 대한 Terraform 레지스트리](#)를 참조하십시오.

Example

```

Resource "cdo_sdc" "my-sdc" {
  name = "my-sdc-in-vm"
}

```

이 리소스의 `bootstrap_data` 속성은 **Security Cloud Control** 부트스트랩 데이터의 값으로 채워지며 다음 단계에서 `cdo_sdc` **Terraform** 모듈에 제공됩니다.

4. **Security Cloud Control_sdc Terraform 모듈**을 사용하여 **vSphere**에서 **SDC**를 생성하는 **Terraform** 코드를 작성합니다.

Example

```

data "cdo_tenant" "current" {}

module "vsphere-cdo-sdc" {
  source          = "CiscoDevNet/cdo-sdc/vsphere"
  version         = "1.0.0"
  vsphere_username = "<replace-with-username-with-admin-privileges>"
  vsphere_password = "<super-secure-password>"
  vsphere_server   = "<replace-with-address-of-vsphere-server>"
  datacenter       = "<replace-with-datacenter-name>"
  resource_pool    = "<replace-with-resource-pool-name>"
  cdo_tenant_name  = data.cdo_tenant.current.human_readable_name
  datastore        = "<replace-with-name-of-datastore-to-deploy-vm-in>"

  network         = "<replace-with-name-of-network-to-deploy-vm-in>"
  host             = "<replace-with-esxi-host-address>"
  allow_unverified_ssl = <boolean; set to true if your vsphere server does not have a valid SSL certificate>
  ip_address       = "<sdc-vm-ip-address; must be in the subnet of the assigned network for the VM>"
  gateway          = "<replace-with-network-gateway-address>"
  cdo_user_password = "<replace-with-password-for-cdo-user-in-sdc-vm>"
  root_user_password = "<replace-with-password-for-root-user-in-sdc-vm>"
  cdo_bootstrap_data = cdo_sdc.sdc-in-vm.bootstrap_data
}

```

생성된 VM에는 두 명의 사용자(root 사용자와 cdo라는 사용자)가 있으며 VM의 IP 주소는 정적으로 구성됩니다. cdo_bootstrap_data 속성에는 cdo_sdc 리소스가 생성될 때 생성된 bootstrap_data 속성의 값이 지정됩니다.

5. terraform 계획 및 terraform 적용을 사용하여 일반적으로 Terraform을 계획하고 적용합니다.

전체 예시는 CiscoDevNet의 [Security Cloud Control 자동화 저장소](#)를 참조하십시오.

SDC가 온보딩 상태를 유지한 경우 원격 콘솔을 사용하여 vSphere VM에 연결하고 cdo 사용자로 로그인한 후에 다음 명령을 실행합니다.

```
sdc host status
```

판독에 따라 수동으로 다음을 실행해야 할 수 있습니다.

```
sdc host configure
```



Security Cloud Control Terraform 모듈은 Apache 2.0 라이선스에 따라 오픈 소스 소프트웨어로 게시됩니다. 지원이 필요한 경우 GitHub에서 문제를 제출할 수 있습니다.

Terraform AWS VPC Secure Device Connector

이 절차에서는 Terraform 모듈을 사용하여 AWS VPC에서 보안 디바이스 커넥터를 구축하는 것과 관련된 단계를 자세히 설명합니다.

AWS VPC에서 SDC를 구축하기 전에 다음 사전 요건을 검토하십시오.

- Security Cloud Control는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 SDC(Secure Device Connector)와 Security Cloud Control 간의 트래픽 검사를 비활성화합니다.
- Secure Device Connector를 사용하여 Security Cloud Control에 연결을 확인하여 커넥터에 대한 적절한 네트워크 액세스를 확인합니다.
- 이 경우 AWS 어카운트, 하나 이상의 서브넷이 있는 AWS VPC 및 AWS Route53 호스팅 영역이 필요합니다.
- Security Cloud Control 부트스트랩 데이터, AWS VPC ID 및 해당 서브넷 ID가 있는지 확인합니다.
- SDC를 구축하는 프라이빗 서브넷에 NAT 게이트웨이가 연결되어 있는지 확인합니다.
- 방화벽 관리 HTTP 인터페이스가 실행 중인 포트에서 NAT 게이트웨이에 연결된 탄력적 IP로 이동하는 트래픽을 엽니다.

1. Terraform 파일에 다음 코드 줄을 추가합니다. 변수에 대한 입력을 수동으로 입력해야 합니다.

```
module "example-sdc" {
  source =
```

```
"git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"

env                = "example-env-ci"
instance_name      = "example-instance-name"
instance_size      = "r5a.xlarge"
cdo_bootstrap_data = "<replace-with-cdo-bootstrap-data>"
vpc_id             = <replace-with-vpc-id>
subnet_id          = <replace-with-private-subnet-id>
}
```

입력 변수 및 설명 목록은 [Secure Device Connector Terraform 모듈](#)을 참조하십시오.

2. Terraform 코드에서 instance_id를 출력으로 등록합니다.

```
output "example_sdc_instance_id" {
  value = module.example-sdc.instance_id
}
```

instance_id를 사용하여 **AWS Systems Manager** 세션 관리자(SSM)를 통한 문제 해결을 위해 **SDC** 인스턴스에 연결할 수 있습니다. 사용 가능한 출력 목록은 **Secure Device Connector Terraform 모듈**의 [출력](#)을 참조하십시오.

다음 작업:

모든 **SDC** 문제 해결의 경우, **AWS SSM**을 사용하여 **SDC** 인스턴스에 연결해야 합니다. 인스턴스에 연결하는 방법에 대한 자세한 내용은 [AWS Systems Manager 세션 관리자](#)를 참조하십시오. **SSH**를 사용하여 **SDC** 인스턴스에 연결하는 포트는 보안상의 이유로 노출되지 않습니다.



주

Security Cloud Control Terraform 모듈은 **Apache 2.0** 라이선스에 따라 오픈 소스 소프트웨어로 게시됩니다. 지원이 필요한 경우 **GitHub**에서 문제를 제출할 수 있습니다.

Secure Device Connector Secure Event Connector CentOS 7 Ubuntu

Security Cloud Control의 온프레미스 **Secure Device Connector(SDC)**는 지금까지 **CentOS 7** 가상 머신에 설치되었습니다. 이제 **CentOS 7**은 단종되었으며 **Security Cloud Control**에 의해 더 이상 사용되지 않으므로, 모든 **SDC**을 **CentOS 7**에서 **Ubuntu** 가상 머신으로 마이그레이션할 수 있도록 이 마이그레이션 프로세스를 생성했습니다.

- **SDC**는 **TCP 포트 443**에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.
- **SDC**를 실행 중인 **Ubuntu** 가상 머신은 **ASA** 및 **Cisco IOS** 디바이스와 같이 통신하는 디바이스의 관리 인터페이스에 대한 네트워크 액세스 권한이 있어야 합니다.
- 이전 **SDC VM**의 **IP 주소** 또는 **FQDN**이 디바이스에 도달하기 위해 생성된 모든 네트워킹 규칙은 새 **SDC VM**의 **IP 주소** 또는 **FQDN**으로 다시 생성해야 합니다.
- 마이그레이션에는 **10~15분**이 소요됩니다. 이 시간 동안 디바이스는 계속해서 보안 정책을 적용하고 네트워크 트래픽을 라우팅하지만 **SDC**를 통해 통신할 수 없습니다.

Secure Device Connector 및 Secure Event Connector를 실행하기 위한 VM 구축에 나와 있는 지침에 따라 새 호스트를 구축합니다.

SDC 및/또는 SEC를 마이그레이션하는 경우 이 절차를 따르십시오.

1. [여기](#)에서 새 VM 이미지를 다운로드합니다.
2. CDO-SDC_VM.zip 파일의 압축을 풉니다. 다음과 비슷하게 이름이 지정된 3개의 VM 파일이 표시됩니다.
 - CDO-SDC-VM-708cd33-2024-05-30-2031-disk1.vmdk
 - CDO-SDC-VM-708cd33-2024-05-30-2031.mf
 - CDO-SDC-VM-708cd33-2024-05-30-2031.ovf
3. 방금 다운로드한 VM을 구축합니다.
4. 새 VM에 할당된 고정 IP 주소 또는 FQDN을 기록해 둡니다.
5. SSH를 사용하여 새 VM에 cdo 사용자로 로그인합니다.
6. 프롬프트에 다음 명령을 입력합니다.

```
sudo sdc host configure
```



- 마이그레이션 스크립트의 지시를 잘 따릅니다. 스크립트는 잘 문서화되어 있으며 각 단계를 설명하면서 마이그레이션 프로세스를 안내합니다.
- 마이그레이션 스크립트가 끝나면 SDC가 새 VM으로 마이그레이션되었음을 알리는 메시지가 표시됩니다. SDC는 마이그레이션 후에도 해당 이름을 그대로 유지합니다.

SDC

절차:

1. SSH를 사용하여 이전(CentOS) SDC에 cdo 사용자로 로그인합니다.
2. 명령을 사용하여 CLI를 설치합니다.

```
curl -O https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh && ./install.sh
```

3. 다음 명령을 실행하고 프롬프트를 따릅니다.

```
sudo sdc migrate now
```

확인:

1. Security Cloud Control 테넌트에 로그인합니다.

2. 마이그레이션한 SDC를 선택하고 **Actions(작업)** 창에서 **Request Heartbeat(하트비트 요청)**을 클릭합니다.



SDC가 **Active(활성)** 상태인지 확인합니다.

SEC

절차:

1. SSH를 사용하여 이전(CentOS) SDC에 cdo 사용자로 로그인합니다.
2. 명령을 사용하여 CLI를 설치합니다.

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
&& tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh &&
./install.sh
```

3. 다음 명령을 실행하고 프롬프트를 따릅니다.

```
sudo sdc eventing migrate
```

4. SEC의 새 IP 주소를 가리키도록 디바이스를 구성하거나 이전 호스트를 종료하고 새 호스트에 이전 호스트와 동일한 IP 주소를 할당하여 디바이스를 업데이트할 필요가 없도록 할 수 있습니다.

확인:

SEC 상태에 대한 자세한 내용은 [상태 확인을 사용하여 Secure Event Connector의 상태 학습](#)을 참조하십시오.

이전 **SDC**를 다시 시작하지 않음

마이그레이션이 완료된 후에는 원래의 가상 머신에서 이전 **SDC**를 다시 시작하지 마십시오.

실패한 마이그레이션 되돌리기

어떤 이유로든 마이그레이션이 실패하거나 결과가 예상과 달라 이전 **SDC**으로 되돌리려면 아래 지침을 따릅니다.

1. 새 VM에 로그인하고 **SDC** 사용자로 전환합니다.
2. 다음 명령을 사용하여 새 VM에서 SDC가 현재 실행 중이 아닌지 확인합니다.

```
docker ps
```

3. SDC가 실행 중인 경우 명령을 실행합니다.

```
sdc stop
```

4. docker ps를 다시 실행하여 SDC 실행이 중지되었는지 확인합니다.

5. 이전 VM에 로그인하고 다음 명령을 실행합니다.

```
sdc migrate revert
```

6. 이전 SDC가 활성화 상태이고 UI에 표시되면 새 VM으로 돌아가 명령을 실행합니다.

```
sdc delete <your-tenant-name-here>
```

7. 브라우저를 완전히 새로 고치고 SDC를 클릭한 다음, 이전 호스트의 IP가 사이드바에 표시되는지 확인합니다.

이 단계를 수행했음에도 새 IP가 계속 표시된다면, 새 상태 확인을 요청하고 브라우저를 새로 고친 후 다시 확인합니다.

8. SEC 마이그레이션을 되돌리려면 다음 명령을 실행합니다.

```
sdc eventing revert
```

IP

자체 VM에 구축된 SDC(Secure Device Connector)를 사용하는 경우 VM을 다른 데이터 센터로 마이그레이션하는 등 여러 가지 이유로 SDC의 IP 주소를 변경해야 할 수 있습니다. 이 절차를 사용하여 SDC에 새 IP 주소를 할당합니다.

- 이 작업을 수행하려면 관리자여야 합니다.
- SDC는 TCP 포트 443 또는 디바이스 관리를 위해 구성된 포트에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.



주

SDC의 IP 주소를 변경한 후 디바이스를 Security Cloud Control에 다시 등록할 필요가 없습니다.

1. SDC에 대한 SSH 연결을 생성하거나 가상 머신의 콘솔을 열고 CDO 사용자로 로그인합니다.
2. IP 주소를 변경하기 전에 SDC VM의 네트워크 인터페이스 구성 정보를 보려면 다음 명령을 사용합니다.

```
[cdo@localhost ~]$ ip addr
```

3. 인터페이스의 IP 주소를 변경하려면 다음 명령을 사용하여 호스트 구성을 재시작합니다.

```
[cdo@localhost ~]$ sdc host configure network
```

4. 프롬프트에 비밀번호를 입력합니다.
5. 구성 스크립트는 이후 네트워크 설정에 대해 묻고, 새 IP를 포함한 새 구성 파일을 작성한 후 해당 구성을 적용합니다.



이 시점에서 SSH 연결이 끊어집니다.

6. SDC에 할당한 새 IP 주소를 사용하여 SSH 연결을 만들고 로그인합니다.
7. SDC는 자동으로 시작되어야 하지만, 그렇지 않은 경우 다음 명령어를 실행합니다.

```
[cdo@localhost ~]$ sudo su - sdc
```

```
[cdo@localhost ~]$ sdc start
```



VM의 콘솔에서 이 절차를 수행하는 경우 값이 올바른지 확인하면 연결 상태 테스트가 자동으로 실행되고 상태가 표시됩니다.

8. Security Cloud Control 사용자 인터페이스를 통해 SDC의 연결을 확인할 수도 있습니다. 이렇게 하려면 Security Cloud Control 애플리케이션을 열고 **Administration(관리) > Integration(통합) > Secure Connectors(보안 커넥터)** 페이지로 이동합니다.
9. 페이지를 한 번 새로 고치고 IP 주소를 변경한 보안 커넥터를 선택합니다.
10. **Actions(작업)** 창에서 **Request Heartbeat(하트비트 요청)**를 클릭합니다. 하트비트 요청 성공 메시지가 표시되고, 마지막 하트비트에 현재 날짜와 시간이 표시되어야 합니다.

Secure Device Connector () ASA

Security Cloud Control Firewall Management는 테넌트당 둘 이상의 SDC 사용을 지원합니다. 다음 절차를 사용하여 한 SDC에서 다른 SDC로 관리형 ASA를 이동할 수 있습니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. **ASA** 탭을 클릭합니다.
3. 다른 SDC로 이동하려는 ASA를 선택합니다.
4. **Device Actions(디바이스 작업)** 창에서 **Update Credentials(자격 증명 업데이트)**를 클릭합니다.
5. Secure Device Connector 버튼을 클릭하고 디바이스를 이동할 SDC를 선택합니다.
6. Security Cloud Control가 디바이스에 로그인하는 데 사용하는 관리자 사용자 이름과 암호를 입력하고 **Update(업데이트)**를 클릭합니다. 변경되지 않은 경우 관리자 사용자 이름과 암호는 ASA 온보딩에 사용한 것과 동일한 자격 증명입니다. 이러한 변경 사항을 디바이스에 구축할 필요는 없습니다.



모든 ASA가 동일한 자격 증명을 사용하는 경우 한 SDC에서 다른 SDC로 ASA를 대량으로 이동할 수 있습니다. ASA에 다른 자격 증명에 있는 경우 한 번에 하나의 SDC에서 다른 하나로 이동해야 합니다.

1. 왼쪽 창에서 **Administration(관리) > Integration(통합) > Secure Connectors(보안 커넥터)**를 선택합니다.
2. 이름을 바꾸려는 SDC를 선택합니다.
3. 세부 정보 창에서 SDC 이름 옆에 있는 편집 아이콘 를 클릭합니다.
4. SDC의 이름을 바꿉니다.

Security Devices(보안 디바이스) 창의 **Secure Device Connector** 필터를 포함하여 **Security Cloud Control** 인터페이스에 SDC 이름이 나타날 때마다 이 새 이름이 나타납니다.

Secure Device Connector

이 작업을 문제 해결 도구로 사용합니다. 이 소스에 따르면, SDC는 보통 자동으로 업데이트되며, 오류가 발생하지 않는 한 수동으로 업데이트할 필요가 없다고 합니다.

1. SDC에 연결합니다. SSH를 사용하여 연결하거나 하이퍼바이저에서 콘솔 보기를 사용할 수 있습니다.)
2. 관리자 사용자(일반적으로 **cdo**)로 SDC에 로그인합니다.
3. SDC 도커 컨테이너를 업데이트하려면 SDC 사용자로 전환합니다:

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

4. SDC 업그레이드:

```
sdc upgrade
```



SDC 가상 머신의 권장 업데이트 및 유지 관리

조직의 내부 IT 보안 및 패치 관리 정책에 따라 Ubuntu 리눅스에서 실행되는 SDC VM을 모니터링하고 업데이트를 적용해야 합니다. SDC VM이 네트워크 환경 내에서 보안을 유지하고 최적으로 작동하도록 관련 보안 패치를 정기적으로 검토하고 적용할 것을 적극 권장합니다.

Secure Device Connector ()

테넌트에 SDC를 무제한으로 설치할 수 있습니다. 여러 개의 SDC를 사용하면 더 많은 디바이스를 관리하고 커넥터를 서로 다른 네트워크 세그먼트에 배치할 수 있지만 이러한 디바이스는 동일한 Security Cloud Control Firewall Management 테넌트에 유지합니다. 두 번째 이상 SDC를 구축하는 절차는 첫 번째 SDC의 절차와 동일합니다. 첫 번째 SDC 이름은 테넌트 이름과 숫자 '1'을 포함합니다. 각 추가 SDC는 순서대로 번호가 매겨집니다.

- 두 번째 또는 후속 SDC를 구축하는 절차는 첫 번째 SDC를 구축할 때와 동일합니다.
- 테넌트의 초기 SDC는 테넌트의 이름과 숫자 1을 통합합니다. 각 추가 SDC는 순서대로 번호가 매겨집니다.

Secure Device Connector ()

다음 절차에 따라 동일한 SDC을(를) 통해 연결되는 디바이스를 찾습니다.

1. 왼쪽 창에서 보안 디바이스.
2. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾습니다.
3. 해당 디바이스 탭을 클릭합니다.
4. 필터 기준이 이미 지정된 경우 **Security Devices(보안 디바이스)** 페이지 상단에 있는 **clear(지우기)** 버튼을 클릭하여 Security Cloud Control로 관리하는 모든 디바이스 및 서비스를 표시합니다.
5. 필터 버튼  을 클릭하여 **필터** 메뉴를 확장합니다.
6. 필터의 **Secure Device Connector** 섹션에서 원하는 SDC의 이름을 확인합니다. **Security Devices(보안 디바이스)** 페이지에는 필터에서 선택한 SDC를 통해 Security Cloud Control에 연결하는 디바이스만 표시됩니다.
7. (선택 사항) 필터 메뉴에서 추가 필터를 선택하여 검색을 더욱 구체화합니다.
8. (선택 사항) 작업이 완료되면 **Security Devices(보안 디바이스)** 페이지 상단에 있는 **clear(지우기)** 버튼을 클릭하여 Security Cloud Control로 관리하는 모든 디바이스 및 서비스를 표시합니다.

Secure Device Connector

SDC을(를) 삭제하면 되돌릴 수 없습니다. 이 디바이스를 제거한 후에는, 새 SDC을(를) 설치하고 디바이스를 다시 연결할 때까지 해당 SDC에 연결되었던 디바이스를 관리할 수 없습니다. 디바이스를 다시 연결하려면 관리자 자격 증명을 다시 입력해야 할 수 있습니다.

SDC을(를) 제거하기 전에 연결된 디바이스를 다른 SDC(으)로 이동하거나 Security Cloud Control Firewall Management에서 제거합니다.

1. 삭제하려는 SDC에 연결된 모든 디바이스를 제거합니다. 다음 두 가지 방법 중 하나로 하면 됩니다.

- 삭제할 SDC에 연결된 모든 디바이스를 Security Cloud Control에서 제거합니다.
 - a. SDC에서 사용하는 모든 디바이스를 식별하려면 동일한 SDC를 사용하여 Security Cloud Control에 연결하는 모든 디바이스 찾기를 참조하십시오.
 - b. Security Devices(보안 디바이스) 페이지에서 식별한 모든 디바이스를 선택합니다.
 - c. Device Actions(디바이스 작업) 창에서 Remove(제거)를 클릭하고 OK(확인)를 클릭하여 작업을 확인합니다.

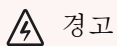
2. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.

3. 왼쪽 창에서 Administration(관리) > Integration(통합) > Secure Connectors(보안 커넥터)를 클릭합니다.

4. Secure Connectors(보안 커넥터) 탭이 선택된 Services(서비스) 페이지에서 파란색 플러스 버튼을 클릭한 후 Secure Device Connector(보안 디바이스 커넥터)를 선택합니다.

5. Secure Connector(보안 커넥터) 테이블에서 제거할 SDC를 선택합니다. 이제 디바이스 수가 0이어야 합니다.

6. 작업 창에서  Remove(제거)를 클릭합니다. 다음 경고가 표시됩니다.



경고

<sdc_name>을 삭제하려고 합니다. SDC 삭제는 되돌릴 수 없습니다. SDC를 삭제하면 디바이스를 온보딩하거나 다시 온보딩하기 전에 새 SDC를 생성하고 온보딩해야 합니다.

현재 온보딩된 디바이스가 있으므로 SDC를 제거하려면 새 SDC를 설정한 후 해당 디바이스를 다시 연결하고 자격 증명을 다시 제공해야 합니다.

- 질문이나 우려 사항이 있는 경우 Cancel(취소)을 클릭하고 Security Cloud Control 지원에 문의하십시오.
- 계속하려면 <sdc_name>을 입력란에 입력하고 OK(확인)를 클릭합니다.

7. 확인 대화 상자에서 계속 진행하려면 경고 메시지에 나와 있는 SDC의 이름을 입력합니다.

8. OK(확인)를 클릭하여 SDC 제거를 확인합니다.

제

5 Security Cloud Control Firewall Management

장

:

- [Cisco Meraki MX](#) □□□□ □□□

사전 요건, 커넥터 선택, 자격 증명, 레이블, 재고 목록 결과 등 여러 ASA를 Security Cloud Control Firewall Management의 디바이스에 온보딩하는 방법을 알아봅니다.

라이브 디바이스와 모델 디바이스를 모두 Security Cloud Control Firewall Management에 온보딩할 수 있습니다. 모델 디바이스는 Security Cloud Control Firewall Management을 사용하여 보고 편집할 수 있는 업로드된 구성 파일입니다.

대부분의 라이브 디바이스 및 서비스는 Secure Device Connector가 Security Cloud Control Firewall Management를 디바이스 또는 서비스에 연결할 수 있도록 개방형 HTTPS 연결을 필요로 합니다.

SDC 및 해당 상태에 대한 자세한 내용은 [Secure Device Connector 정보](#) 페이지 46의 내용을 참조하십시오.

Cisco Meraki MX

Cisco Meraki 환경에서 Cisco Meraki MX 디바이스를 온보딩하여 해당 디바이스 또는 서비스를 관리할 수 있도록 하는 방법을 알아봅니다.

이 장에서는 Cisco Meraki MX 디바이스를 온보딩하는 단계를 제공합니다.

Meraki MX Security Cloud Control

디바이스 또는 서비스를 관리에 사용할 수 있도록 Meraki MX를 Security Cloud Control에 온보딩하는 방법을 알아봅니다.

MX 디바이스는 Security Cloud Control와 Meraki 대시보드 모두에서 관리할 수 있습니다. Security Cloud Control는 구성 변경 사항을 Meraki 대시보드에 구축합니다. 그러면 구성이 디바이스에 안전하게 구축됩니다.

- Security Cloud Control을 매지니드 디바이스를 연결하는 방법에 대한 자세한 내용은, [직접 클라우드 연결성 위한 인바운드 액세스 허용](#) 페이지 48을(를) 참조하십시오.
- 먼저 Meraki 대시보드에서 Meraki MX를 등록해야 합니다. Meraki 대시보드에 액세스하지 않으면 Meraki 클라우드에서 조직을 인식할 수 없습니다. 따라서 디바이스를 온보딩하기 위한 API 토큰을 생성할 수 없습니다.
- Security Cloud Control는 호스트와 연결된 모든 비트를 0으로 설정하여 잘못된 CIDR 접두사 표기법 IP 주소 및 IP 주소 범위를 유효한 형식으로 자동 변환합니다.
- Meraki MX 디바이스 또는 템플릿을 온보딩하는 데 더 이상 SDC(Secure Device Connector)를 통한 연결이 필요하지 않습니다. 이전에 온보딩된 Meraki MX 디바이스가 있고 SDC를 사용하여 Security Cloud Control에 연결하는 경우 연결은 계속 작동합니다. 디바이스를 제거했다가 다시 온보딩하거나 [연결 자격 증명을 업데이트](#)하면 연결이 작동하지 않습니다.
- Security Cloud Control에서 관리하기 위해 MX 디바이스를 Meraki 클라우드에 연결할 필요는 없습니다. MX 디바이스가 클라우드에 연결된 적이 없는 경우 디바이스 연결은 연결할 수 없음으로 나열됩니다. 이는 정상적인 현상이며, 이 디바이스에 대한 정책을 관리하거나 구축하는 기능에는 영향을 미치지 않습니다.

1. Meraki MX 디바이스를 온보딩할 때 Meraki API 키를 생성해야 합니다. 디바이스를 안전하게 온보딩할 수 있도록 이 키를 통해 대시보드가 요청을 인증할 수 있습니다. Meraki API 키 생성 및 검색에 대한 자세한 내용은 [Meraki API 키 생성 및 검색](#)을 참조하십시오.
2. API 키를 사용하여 Meraki 디바이스를 Security Cloud Control에 온보딩합니다.

Meraki API

다음 절차를 사용하여 API 액세스를 사용하여 Meraki 대시보드에 대한 Security Cloud Control 액세스를 활성화합니다.

[Meraki MX를 Security Cloud Control에 온보딩](#) 페이지 70의 참고 사항 및 사전 요건을 검토합니다.

1. Meraki 대시보드에 로그인합니다.
2. **Organization(조직) > Settings(설정)**를 선택합니다.

3. **Dashboard API Access**(대시보드 API 액세스) 섹션에서 **Enable access to the Cisco Meraki Dashboard API**(Cisco Meraki 대시보드 API에 대한 액세스 활성화)를 선택합니다. 이 옵션을 활성화하지 않으면 MX 디바이스를 Security Cloud Control에 온보딩하기 위한 API 키를 생성할 수 없습니다.
4. **Save Changes**(변경 내용 저장)를 클릭합니다.
5. Meraki 대시보드에서 **username**을 클릭한 다음 **My Profile**(내 프로필)을 클릭합니다.
6. API 액세스 헤더를 찾아 **Generate new API key**(새 API 키 생성)를 클릭합니다. API 키를 복사하고 사용할 준비가 될 때까지 메모에 붙여 넣습니다. API 키가 포함된 윈도우나 탭을 닫고 붙여넣을 경우 복사한 API 키에 액세스할 수 없게 됩니다.



디바이스당 하나의 API 키만 있으면 됩니다. 새 키를 생성하지 않고 Meraki 디바이스를 다시 온보딩할 수 있습니다.

계속해서 [Meraki 디바이스](#)를 [Security Cloud Control](#)에 온보딩합니다.

Security Cloud Control MX

다음 절차를 사용하여 Cisco Meraki 디바이스를 온보딩합니다.

[Meraki API 키 생성 및 검색](#) 페이지 70.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
 2. 보안 디바이스를 선택합니다.
 3. 파란색 추가 버튼  을 클릭합니다.
 4. **Meraki** 타일을 클릭합니다.
 5. 이 디바이스가 통신할 [Secure Device Connector](#) 정보 페이지 46를 선택합니다. 기본 SDC가 표시되지만 파란색 **Change**(변경) 링크를 클릭하여 변경할 수 있습니다.
 6. **Connect to Cisco Meraki**(Cisco Meraki 에 연결) 페이지에서 다음 단계를 수행합니다.
 - a) 복사한 API 액세스 키를 붙여넣고 **Connect**(연결)를 클릭합니다.
키가 불완전하거나 올바르지 않으면 디바이스를 온보딩할 수 없습니다.
 - b) 드롭다운 목록을 사용하여 올바른 조직을 선택합니다. 생성된 조직 목록은 Meraki 대시보드에서 검색되며 디바이스 및 템플릿을 포함합니다. **Select**(선택)를 클릭합니다.
 - c) 드롭다운 목록을 사용하여 올바른 네트워크를 선택합니다. 생성된 네트워크 목록은 Meraki 네트워크에서 검색됩니다. **Select**(선택)를 클릭합니다.
 - d) (선택 사항) 디바이스의 고유한 레이블을 추가합니다. 이 레이블을 기준으로 디바이스 목록을 필터링할 수 있습니다. **Continue**(계속)를 클릭합니다.
- 디바이스가 온보딩 프로세스를 시작합니다. 프로세스가 완료되면 **Security Devices**(보안 디바이스) 페이지로 리디렉션됩니다.

Meraki Security Cloud Control

디바이스 또는 서비스를 관리에 사용할 수 있도록 Meraki 템플릿을 Security Cloud Control에 온보딩하는 방법을 알아봅니다.

Meraki 템플릿을 사용하면 단일 정책으로 여러 위치 또는 네트워크를 관리할 수 있습니다. 이러한 템플릿은 Security Cloud Control과 Meraki 대시보드 모두에서 관리할 수 있습니다. Security Cloud Control은 구성 변경 사항을 Meraki 대시보드에 구축하며, 그러면 대시보드가 구성을 템플릿에 안전하게 구축합니다. Security Cloud Control가 Meraki와 통신하는 방법에 대한 자세한 내용.



주

Security Cloud Control에 템플릿을 온보딩하려면 먼저 Meraki 대시보드에서 템플릿을 생성해야 합니다. Meraki 대시보드에 대한 액세스 권한이 없으면 Meraki 클라우드에서 조직을 인식할 수 없으며 디바이스의 API 토큰을 생성할 수 없습니다. Meraki 대시보드에서 **Organization(조직) > Configuration Templates(템플릿)**를 클릭합니다. 자세한 내용은 [구성 템플릿으로 여러 네트워크 관리](#)를 참조하십시오.

Meraki 템플릿을 온보딩하려면 다음 세 단계를 완료해야 합니다.

1. Meraki 대시보드에서 템플릿 네트워크를 생성합니다. Meraki 템플릿 모범 사례에 대한 자세한 내용은 [Meraki 템플릿 모범 사례](#)를 참조하십시오.
2. [Meraki API 키를 생성하고 검색합니다](#). Meraki 템플릿을 온보딩할 때 Meraki API 키를 생성해야 합니다. 키를 사용하여 대시보드를 인증하고 디바이스를 안전하게 온보딩합니다.
3. 키를 사용하여 [Meraki 템플릿을 Security Cloud Control에 온보딩합니다](#).

Meraki API

다음 절차를 사용하여 API 액세스를 사용하여 Meraki 대시보드에 대한 Security Cloud Control 액세스를 활성화합니다.

1. Meraki 대시보드에 로그인합니다.
2. **Organization(조직) > Settings(설정)**를 선택합니다.
3. **Dashboard API Access(대시보드 API 액세스)** 섹션에서 **Enable access to the Cisco Meraki Dashboard API(Cisco Meraki 대시보드 API에 대한 액세스 활성화)**를 선택합니다. 이 옵션을 활성화하지 않으면 MX 디바이스를 Security Cloud Control에 온보딩하기 위한 API 키를 생성할 수 없습니다.
4. **Save Changes(변경 내용 저장)**를 클릭합니다.
5. Meraki 대시보드에서 **username**을 클릭한 다음 **My Profile(내 프로필)**을 클릭합니다.
6. API 액세스 헤더를 찾아 **Generate new API key(새 API 키 생성)**를 클릭합니다. API 키를 복사하고 사용할 준비가 될 때까지 메모에 붙여 넣습니다. API 키가 포함된 윈도우나 탭을 닫고 붙여넣을 경우 복사한 API 키에 액세스할 수 없게 됩니다.



템플릿당 하나의 API 키만 있으면 됩니다. 새 키를 생성하지 않고 템플릿을 다시 온보딩할 수 있습니다.

Meraki Security Cloud Control

Meraki 템플릿을 온보딩하려면 다음 절차를 수행합니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.
3. 파란색 추가 버튼  을 클릭합니다.
4. **Connect to Cisco Meraki**(Cisco Meraki에 연결)클릭합니다.
5. 복사한 API 액세스 키를 붙여넣습니다. 키가 불완전하거나 올바르지 않으면 디바이스를 온보딩할 수 없습니다. **Connect**(연결)를 클릭합니다.
6. 드롭다운 목록을 사용하여 템플릿 이름을 **Organization**(조직)으로 선택합니다. 생성된 조직 목록은 Meraki 대시보드에서 검색되며 디바이스 및 템플릿을 포함합니다. 원하는 템플릿을 선택하고 **Select**(선택)를 클릭합니다.
7. (선택 사항) 디바이스에 고유한 레이블을 추가할 수 있습니다. 이 레이블을 기준으로 디바이스 목록을 필터링할 수 있습니다.
8. **Continue**(계속)를 클릭합니다.

디바이스가 온보딩 프로세스를 시작합니다. 완료되면 Security Cloud Control에서 **Security Devices**(보안 디바이스)로 리디렉션합니다. 템플릿이 Security Cloud Control에 동기화되면 **Security Devices**(보안 디바이스) 페이지에 템플릿과 연결된 디바이스의 이름이 표시되고 의 디바이스 세부 정보 창에 템플릿에 바인딩된 네트워크 수가 표시됩니다.

Meraki MX

Meraki MX 연결 자격 증명을 업데이트하는 방법을 알아보십시오.

Meraki 대시보드에서 새 API 키를 생성하는 경우 Security Cloud Control Firewall Management에서 연결 자격 증명을 업데이트해야 합니다.

Security Cloud Control Firewall Management에서는 디바이스 자체의 연결 자격 증명을 업데이트할 수 없습니다. 필요한 경우 Meraki 대시보드에서 API 키를 수동으로 새로 고칩니다. 자격 증명을 업데이트하고 통신을 다시 설정하려면 Security Cloud Control Firewall Management UI에서 API 키를 수동으로 업데이트해야 합니다.



Security Cloud Control가 디바이스를 동기화하지 못하면 Security Cloud Control의 연결 상태에 "Invalid Credentials(유효하지 않은 자격 증명)"가 표시될 수 있습니다. 이 상황에서는 API 키를 사용하려고 시도했을 수 있습니다. 선택한 Meraki MX의 API 키가 올바른지 확인합니다.

Meraki MX 디바이스에 대한 자격 증명을 업데이트하려면 다음 절차를 사용합니다:

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.
3. **Devices(디바이스)** 탭을 클릭한 다음 **Meraki** 탭을 클릭합니다.
4. 연결 자격 증명을 업데이트할 Meraki MX를 선택합니다.
5. **Device Actions(디바이스 작업)** 창에서 **Update Credentials(자격 증명 업데이트)**를 클릭합니다.
6. Security Cloud Control Firewall Management가 디바이스에 로그인하는 데 사용하는 API 키를 입력하고 **Update(업데이트)**를 클릭합니다. 변경하지 않는 한 이 API 키는 Meraki MX를 온보딩하는 데 사용한 것과 동일한 자격 증명입니다. 이러한 변경 사항은 디바이스에 구축할 필요가 없습니다.

Security Cloud Control Firewall Management

Security Cloud Control Firewall Management에서 디바이스를 삭제하는 방법을 알아봅니다.

Security Cloud Control Firewall Management에서 디바이스를 삭제하려면 다음 단계를 따르십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.
3. 삭제할 디바이스를 선택합니다.
4. **Device Actions(디바이스 작업)** 창에서 **Remove(제거)**를 클릭합니다.
5. 디바이스 제거를 확인하려면 **OK(확인)**를 클릭합니다.
디바이스를 온보드 상태로 유지하려면 **Cancel(취소)**를 클릭합니다.

제

6 Meraki

장

- :
- Security Cloud Control Firewall Management
 - Meraki
 -
 -
 - Meraki
 - Meraki

Security Cloud Control Firewall Management

규칙 순서, 인터페이스 할당, 로깅, 검색, 구축 고려 사항을 포함하여 Security Cloud Control Firewall Management에서 방화벽에 대한 보안 정책을 관리하는 방법을 알아봅니다.

보안 정책에서 네트워크 트래픽을 검사하는 궁극적인 목표는 트래픽을 의도한 대상으로 허용하거나 보안 위협이 식별된 경우 트래픽을 삭제하는 것입니다. Security Cloud Control을 사용하여 다양한 유형의 디바이스에서 보안 정책을 구성할 수 있습니다.

Meraki

Meraki MX 디바이스 템플릿에 대한 액세스 제어 규칙의 생성, 편집, 삭제, 재정렬 및 구축을 포함하여 Security Cloud Control에서 Meraki 액세스 제어 정책을 관리하는 방법을 알아봅니다.

Meraki MX 디바이스는 Security Cloud Control에 온보딩하기 전에 Meraki 대시보드에서 관리되었을 수 있으며 디바이스에 이미 일부 아웃바운드 규칙이 있을 수 있습니다. 이러한 규칙은 Security Cloud Control에서 액세스 제어 규칙으로 표시됩니다.

이러한 규칙을 수정하고 액세스 제어 정책 내에서 추가 규칙을 생성할 수 있습니다. 액세스 제어 정책을 맞춤화하려면 개체를 생성하고 연결합니다. 자세한 내용은 관련 문서 섹션을 참조하십시오.



주

Meraki 액세스 제어 정책의 작업은 기본적으로 **Allow(허용)**입니다. 작업을 변경할 수 없습니다.

Security Cloud Control을 사용하여 Meraki 액세스 제어 정책을 편집하려면 다음 절차를 수행합니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.
3. **Templates(템플릿)** 탭을 클릭합니다.
4. **Meraki** 탭을 클릭하고 액세스 제어 정책을 수정할 Meraki MX 디바이스 템플릿을 선택합니다.
5. **Management(관리)** 창에서 **Policy(정책)**를 선택합니다.
6. 다음 중 하나를 수행합니다.
 - 새 규칙을 생성하려면 버튼  을 클릭합니다.
 - 기존 규칙을 편집하려면 규칙을 선택하고 **Actions(작업)** 창에서 **Edit(편집)** 버튼  을 클릭합니다. 편집 모드로 들어가지 않고 간단한 인라인 편집을 할 수 있습니다.
 - 더 이상 필요하지 않은 규칙을 삭제하려면 규칙을 선택하고 **Actions(작업)** 창에서 **Remove(제거)** 버튼  을 클릭합니다.
 - 정책 내에서 규칙을 이동하려면 액세스 제어 테이블에서 규칙을 선택하고 규칙 행의 끝에 있는 위쪽 또는 아래쪽 화살표를 클릭하여 규칙을 이동합니다.
7. **Order(순서)** 필드에서 정책 내 규칙의 위치를 선택합니다. 네트워크 트래픽은 1부터 "마지막"까지 숫자 순서대로 규칙 목록을 기준으로 평가됩니다.

규칙은 처음 일치하는 항목을 기준으로 적용됩니다. 매우 구체적인 트래픽 일치 기준이 있는 규칙은 해당 트래픽에 적용될 수 있는 일반적인 기준의 정책보다 앞에 위치해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 수정합니다.

8. 규칙 이름을 입력합니다. 영숫자, 공백 및 다음 특수 문자를 사용할 수 있습니다: + . _ , -)는 사용할 수 있습니다.

 주

액세스 제어 규칙의 이름은 **Security Cloud Control**에서 규칙의 이름으로 사용되는 반면, **Remark(비고)** 필드는 **Meraki** 대시보드에서 규칙의 이름으로 처리됩니다. 두 필드는 서로 중속되지 않습니다.

9. 네트워크 트래픽이 규칙과 일치하는 경우 적용할 작업을 선택합니다.

- **Block(차단):** 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.
- **Allow(허용):** 정책에서 침입 및 기타 검사 설정이 적용되는 트래픽을 허용합니다.

 주

규칙 작업만 설정하거나 수정할 수 있습니다. **Security Cloud Control**에서 기본 정책 작업을 변경할 수 없습니다.

10. 다음 탭의 속성을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source(소스): Source(소스)** 탭을 클릭하고 네트워크 트래픽이 시작된 네트워크(네트워크 및 대륙 포함) 또는 포트를 추가하거나 제거합니다. 기본값은 "Any(모두)"입니다.
- **Destination(대상): Destination(대상)** 탭을 클릭하고 트래픽이 도착하는 네트워크(네트워크 및 대륙 포함) 또는 포트를 추가하거나 제거합니다. 기본값은 "Any(모두)"입니다.

 주

소스 및 대상 네트워크는 구성된 **VLAN** 서브넷 중 하나 또는 **VLAN** 서브넷이 수동으로 구성되지 않은 경우 기본 **VPN** 서브넷 내에 있어야 합니다. 유효하지 않은 소스 또는 대상 네트워크를 포함하는 규칙을 구축하면 실패합니다.

11. **Save(저장)**를 클릭합니다.

12. 지금 변경한 내용을 **검토 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Meraki

Meraki 템플릿에 대한 개요, 정의, 사용 시기, 관리자를 위한 주요 고려 사항이 포함된 개요입니다.

Meraki 템플릿은 여러 사이트나 네트워크와 공유할 수 있는 네트워크 구성입니다. 개별 사이트 네트워크를 템플릿 네트워크에 바인딩할 수 있습니다. 단일 템플릿을 변경하면 바인딩된 모든 네트워크가 자동으로 업데이트됩니다. 바인딩된 네트워크를 Security Cloud Control에서 바인딩된 디바이스로 볼 수 있습니다. 이 구성은 서로 다른 위치에 있는 여러 네트워크에 단일 정책을 적용하는 데 이상적입니다.

단일 템플릿에 두 개 이상의 네트워크를 구성하는 방법에 대한 자세한 내용은 [구성 템플릿을 사용하여 여러 네트워크 관리](#)를 참조하십시오. Meraki 템플릿, 템플릿 계획 및 설정에 대한 자세한 내용은 [Meraki 템플릿 모범 사례](#)를 참조하십시오.

Meraki 디바이스를 관리하는 것과 동일한 방식으로 Meraki 템플릿을 관리합니다. 먼저 Meraki 대시보드를 사용하여 템플릿 구성한 다음 Security Cloud Control에 온보딩합니다. Security Cloud Control에 템플릿을 온보딩하면 기존 규칙 또는 IP 그룹이 Security Cloud Control로 [읽어들이고](#) 개체로 변환됩니다. 동기화한 후에는 Security Devices(보안 디바이) 페이지의 Device Details(디바이스 세부 정보) 창에서 템플릿 이름 및 연결된 네트워크의 수(바인딩된 디바이스로)를 확인합니다. 또한 Security Cloud Control에서 템플릿 및 바인딩된 네트워크와 관련된 정책을 관리, 수정 및 배포할 수 있습니다. Security Cloud Control에 Meraki 템플릿을 온보딩하는 방법에 대한 자세한 내용은 [Security Cloud Control에 Meraki 템플릿 온보딩](#)을 참조하십시오.

Security Cloud Control의 공유 개체가 하나의 개체 정의가 여러 디바이스 및 정책에 적용되도록 하여 정책 일관성을 유지하는 데 어떻게 도움이 되는지 알아보십시오.

공유 개체는 여러 디바이스에서 이름과 내용이 동일한 개체입니다. 개체 변경은 해당 공유 개체를 사용하는 모든 정책에 영향을 미치므로 공유 개체는 정책을 유지 관리하는 데 도움이 됩니다.

공유 개체는 이 아이콘으로 식별됩니다.



Objects(개체) 페이지에서 공유 개체를 사용하면 한 곳에서 개체를 수정할 수 있으며 변경 사항은 해당 개체를 사용하는 다른 모든 정책에 영향을 미치므로 정책을 쉽게 유지 관리할 수 있습니다. 공유 개체가 없으면 동일한 변경이 필요한 모든 정책을 개별적으로 수정해야 합니다.

공유 개체를 볼 때 Security Cloud Control는 개체 테이블에 있는 개체의 내용을 표시합니다. 공유 개체는 정확히 동일한 내용을 갖습니다. Security Cloud Control는 세부 정보 창에서 개체 요소의 결합된 보기 또는 "평평한" 보기를 보여줍니다. 세부 정보 창에서 네트워크 요소는 간단한 목록으로 병합되며 명명된 개체와 직접 연결되지 않습니다.

Name	Devices	Type	Issues
ARW-DNS1	3	Network Object	
ARW-DNS2	3	Network Object	
ARW-DNS3	3	Network Object	
ARW-JIRA	3	Network Object	
ARW-RUMBAPCGX280	3	Network Object	

Network Address
139.232.120.146

Details
139.232.120.146

Relationships
large-asa ASA
Cloud-delivered FMC Cloud-delivered FMC

디바이스, 문제, 공유 상태, 연결 상태, 개체 유형, 시스템 정의 상태 및 검색 값별로 Security Cloud Control의 개체를 필터링하여 대상 개체 결과를 찾는 방법을 알아보십시오.

Objects(개체) 페이지의 필터를 사용하여 디바이스, 문제, 공유 상태, 연결 상태, 개체 유형 또는 검색 값별로 개체를 찾습니다. 또한 시스템 정의 개체를 포함하거나 제외할 수 있습니다.

개체 유형 필터를 사용하면 네트워크 개체, 네트워크 그룹, URL 개체, URL 그룹, 서비스 개체, 서비스 그룹 등의 유형별로 개체를 필터링할 수 있습니다. 공유 개체 필터를 사용하면 기본값, 재정의 값 또는 추가 값이 있는 개체를 필터링할 수 있습니다.

디바이스 필터와 개체 필터를 결합하여 집중 검색 전략을 생성할 수 있습니다. 예를 들어, **Issues(문제)**가 **Unused(미사용) OR Inconsistent(일관성 없음) AND Shared Objects(공유 개체)**에 **Default Values(기본값) OR Additional Values(추가 값)**이 있고 **AND Unassociated Objects(연결되지 않은 개체)**가 선택된 논리와 일치하는 개체를 검색할 수 있습니다.

The screenshot shows a filter configuration interface. At the top is a 'Filter' input field. Below it is a 'Filter by Device' button with a dropdown arrow. A checkbox labeled 'Show System-Defined Objects' is present. The main section contains several expandable categories, each with a dropdown arrow and a count in a red pill: 'Issues' (18661), 'Ignored Issues' (0), 'Shared Objects' (0), 'Unassociated Objects' (0), and 'Object Type' (0). Under 'Issues', there are three sub-items: 'Unused' (checked, 4754), 'Duplicate' (unchecked, 13846), and 'Inconsistent' (checked, 61). Under 'Ignored Issues', there is 'Ignored' (unchecked). Under 'Shared Objects', there are 'Default Values' (checked), 'Override Values' (unchecked), and 'Additional Values' (checked). Under 'Unassociated Objects', there is 'Unassociated' (checked). Under 'Object Type', there are 'Network' (unchecked), 'Protocol' (unchecked), and 'Service' (unchecked).

필터링하려면 **Objects(개체)** 탭의 왼쪽 창에서  을(를) 클릭합니다.

- **Filter by Device(디바이스별 필터링):** 선택한 디바이스에 있는 개체를 표시합니다.
- **Show System-Defined Objects(시스템 정의 개체 표시):** 검색 및 필터 결과에 사전 정의된 시스템 개체를 포함합니다. 시스템 개체는 편집하거나 삭제할 수 없습니다. 일부 디바이스는 공통 서비스에 대해 사전 정의된 개체가 함께 제공됩니다. 이러한 시스템 개체는 이미 생성되어 규칙 및 정책에서 사용할 수 있으므로 편리합니다. 개체 테이블에는 여러 시스템 개체가 있을 수 있습니다. 시스템 개체는 편집하거나 삭제할 수 없습니다.
- **Issues(문제):** 사용되지 않거나, 중복되거나 일치하지 않는 개체를 표시합니다. 문제를 하나 이상 선택하면 선택한 문제 범주의 개체가 포함됩니다.
- **Ignored Issues(무시된 문제):** 관리자가 문제를 무시한 개체를 표시합니다.
- **Shared Objects(공유 개체):** 공유 개체를 표시합니다. 기본값, 재정의 값, 추가 값 또는 조합을 기준으로 필터링할 수 있습니다.

- **Unassociated Objects**(연결되지 않은 개체): 규칙이나 정책과 연결되지 않은 개체를 표시합니다.
- **Object Type**(개체 유형): 네트워크 개체, 네트워크 그룹, URL 개체, URL 그룹, 서비스 개체, 서비스 그룹 등 선택한 개체 유형을 표시합니다.

기본 필터 내에서 하위 필터를 사용하면 네트워크, 서비스 또는 프로토콜 등의 개체 유형별로 결과를 더욱 좁힐 수 있습니다. 여러 범주의 필터는 **AND** 관계로 결합됩니다. 범주 내에서 여러 항목을 선택하면 **OR** 관계로 결합될 수 있습니다.

예를 들어 필터 집합은 선택한 디바이스 의 개체 **AND** 일치하지 않는 개체 **AND** 네트워크 개체 또는 서비스 개체 및 그룹을 포함하는 개체 이름과 이 논리와 일치하는 개체를 검색할 수 있습니다.

Meraki

Meraki 대시보드에서 로컬 Meraki 네트워크 개체를 생성하고 읽기 전용 FTD 네트워크 개체 또는 개체 그룹으로 Security Cloud Control에 동기화하는 방법을 알아봅니다.

Meraki 대시보드에서 로컬 Meraki 네트워크 개체를 만들어야 합니다. 아직 Security Cloud Control에 온보딩되지 않은 Meraki 디바이스가 있는 경우 기존 로컬 개체가 디바이스에 온보딩됩니다. 온보딩된 Meraki 디바이스가 있는 경우 Security Cloud Control에서 디바이스를 동기화하여 새 구성 및 로컬 개체를 읽습니다.



주

Meraki 네트워크 개체 또는 네트워크 개체 그룹을 참조하는 디바이스 구성이 Security Cloud Control UI에 온보딩되거나 동기화되면 이러한 개체는 **FTD** 네트워크 개체 또는 개체 그룹으로 표시됩니다.

이러한 개체 및 개체 그룹은 Security Cloud Control에서 읽기 전용입니다.

Meraki의 오픈 베타 네트워크 개체를 활성화하지 않은 경우, Meraki 대시보드에 로그인하고 조직 > 정책 개체로 이동하여 등록하고 로컬 개체 및 개체 그룹에 대한 액세스 권한을 얻으십시오.

1. Meraki 대시보드에 로그인하고 로컬 개체 또는 로컬 개체 그룹을 생성합니다. 자세한 내용은 [Meraki 네트워크 개체 구성 가이드](#)를 참조하십시오.
2. Security Cloud Control에 로그인합니다.
참고: 아직 Meraki 디바이스를 Security Cloud Control에 온보딩하지 않은 경우 자세한 내용은 [Security Cloud Control에 MX 디바이스 온보딩](#) 페이지 71를 참조하십시오. 디바이스를 온보딩하면 기존 개체도 모두 온보딩됩니다.
3. 왼쪽 창에서 보안 디바이스를 클릭합니다.
4. Meraki 디바이스를 찾아 디바이스 행이 강조 표시되도록 선택합니다. 디바이스 상태는 충돌 감지됨입니다. 오른쪽에 있는 창에서 **Review Conflict**(충돌 검토)를 선택하여 디바이스 구성에 대한 변경 사항을 검토하거나 **Accept without Review**(검토 없이 수락)을 선택하여 모든 구성 변경 사항을 수락합니다.

Meraki

MX 디바이스는 Firepower 및 ASA 네트워크 개체와 동일한 형식을 사용하며 CIDR 표기법으로 표현된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 네트워크 개체 및 그룹에 추가하는 기타

개별 주소 또는 서브넷의 모음입니다. 네트워크 개체 및 네트워크 그룹은 액세스 규칙에 사용됩니다. **Security Cloud Control**을 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

네트워크 개체에 추가할 수 있는 **IP** 주소

디바이스 유형	IPv4 / IPv6	단일 주소	주소 범위	전체(Fully Qualified) 도메인 이름	CIDR 표기법의 서브넷
MX	IPv4	예	예	아니요	예



주

클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

Objects(개체) 페이지에서 FTD, FDM 또는 ASA 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 클라우드 제공 Firewall Management Center에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects**(네트워크 개체 검색 및 관리)가 활성화된 각 온프레미스 Firewall Management Center에 대한 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 Firewall Management Center에 구축할 수 있습니다.



주

클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects**(네트워크 개체 검색 및 관리)가 활성화된 각 온프레미스 Firewall Management Center에 대한 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 Firewall Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Meraki



주

클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

Objects(개체) 페이지에서 FTD, FDM 또는 ASA 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 클라우드 제공 Firewall Management Center에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects**(네트워크 개체 검색 및 관리)가 활성화된 각 온프레미스 Firewall Management Center에 대한 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 Firewall Management Center에 구축할 수 있습니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 개체를 클릭합니다.
3. 를 클릭하고, **FTD** > 네트워크 또는 **ASA** > 네트워크를 클릭합니다.
4. 개체 이름을 입력합니다.
5. **Create a network object**(네트워크 개체 생성)를 선택합니다.
6. 값 섹션에서 단일 IP 주소 또는 CIDR 표기법으로 표현된 서브넷 주소를 입력합니다.

7. **Add(추가)**를 클릭합니다.

8. 지금 변경 사항을 **검토하고 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Meraki

네트워크 그룹은 여러 네트워크 개체 또는 IP 주소로 구성됩니다.

네트워크 그룹을 네트워크 개체로 구성하려면 위의 "네트워크 개체 생성" 절차를 사용하여 IP 주소에 대한 개별 네트워크 개체를 생성합니다.



클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

Objects(개체) 페이지에서 FTD, FDM 또는 ASA 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 클라우드 제공 Firewall Management Center에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects(네트워크 개체 검색 및 관리)**가 활성화된 각 온프레미스 Firewall Management Center에 대한 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 Firewall Management Center에 구축할 수 있습니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 Security Cloud Control 탐색 모음에서 개체를 클릭합니다.
3.  를 클릭하고, **FTD > 네트워크** 또는 **ASA > 네트워크**를 클릭합니다.
4. 개체 이름을 입력합니다.
5. **Create a network group(네트워크 그룹 생성)**을 선택합니다.
6. **Add Object(개체 추가)**를 클릭하고 목록에서 네트워크 개체를 선택한 다음 **Select(선택)**를 클릭합니다.
원하는 모든 네트워크 개체를 추가할 때까지 이 작업을 계속합니다.
7. **Add(추가)**를 클릭합니다.
8. 지금 변경 사항을 **검토하고 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Firepower



주

클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects**(네트워크 개체 검색 및 관리)가 활성화된 각 온프레미스 Firewall Management Center에 대한 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 Firewall Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 개체를 클릭합니다.
3. 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.
4. 편집할 개체를 선택합니다.
5. 세부 정보 창에서 편집 버튼  을 클릭합니다.
6. 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.
7. **Save(저장)**를 클릭합니다.
8. Security Cloud Control에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.
9. 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Security Cloud Control

클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

개체 페이지에서 네트워크 개체 또는 그룹을 삭제하면 클라우드 제공 Firewall Management Center의 개체 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며, 그 반대의 경우도 마찬가지입니다.

Meraki

Security Cloud Control이 Meraki 대시보드 규칙 값을 MX 디바이스 정책 관리를 위한 네트워크, 서비스 또는 프로토콜 개체로 나타내는 방법을 알아봅니다.

Meraki

Meraki 대시보드는 아웃바운드 액세스 제어 규칙의 소스 및 대상 필드에서 IP 주소, 프로토콜 또는 포트 범위의 그룹을 활용합니다. 온보딩되면 Security Cloud Control은 IP 주소를 네트워크 개체로, 애플리케이션 레이어 프로토콜 값을 서비스 개체 또는 프로토콜 개체로 변환합니다.

Security Cloud Control의 단일 규칙이 대시보드에서 여러 규칙으로 변환될 수 있습니다. 예를 들어 TCP 및 UDP 프로토콜을 모두 포함하는 ASA 프로토콜 그룹을 Security Cloud Control의 단일 액세스 제어 규칙에 추가하는 경우, Security Cloud Control은 하나의 Security Cloud Control 규칙을 대시보드에서 여러 규칙으로 변환합니다. 하나의 규칙은 TCP 프로토콜을 포함하고 하나의 규칙은 UDP 프로토콜을 포함합니다.

Meraki 대시보드와 Security Cloud Control은 모두 CIDR 서브넷 표기법을 지원합니다. 레이어 3 스위치 인터페이스 및 MX 디바이스 레이아웃에 대한 자세한 내용은 [Meraki 기술 자료](#)를 참조하십시오.

Security Cloud Control Meraki ?

Security Cloud Control에는 MX 디바이스 전용인 개체가 없습니다. 대신 FTD, FDM 및 ASA 개체를 생성하거나 공유하고 디바이스에 구축된 규칙에서 이러한 개체를 연결할 수 있습니다. Meraki는 FTD 및 ASA 개체와 완전히 호환되지 않으므로 MX 디바이스에서 개체를 사용하는 방법에 영향을 미치는 몇 가지 제한 사항이 있을 수 있습니다.

참고로 FTD, FDM 및 ASA 개체를 MX 디바이스와 연결하면 해당 개체가 공유됩니다. 해당 개체를 변경하면 해당 개체가 공유되는 모든 디바이스에 영향을 미치며 디바이스의 구성 상태가 **Not Synced**(동기화되지 않음)로 표시됩니다. 자세한 내용은 [공유 개체](#)를 참조하십시오. 개체에 영향을 미칠 수 있는 추가 개체 상태는 이 페이지의 하단에 있는 관련 문서 섹션을 참조하십시오.

Meraki는 IPv6 주소 또는 FQDN을 포함하는 개체를 지원하지 않습니다.

Security Cloud Control의 개체	Meraki와 호환
프로토콜 개체	TCP, UDP, ICMP
네트워크 개체	예
네트워크 그룹	예
서비스 개체	예
ASA 서비스 그룹	아니요
FTD 서비스 그룹	아니요

Meraki

네트워크 개체 및 개체 그룹을 사용하면 Meraki 디바이스에 대한 방화벽 규칙을 더 쉽게 관리할 수 있습니다. 이는 방화벽 규칙과 같은 액세스 정책에 사용할 수 있는 IP 서브넷 및 FQDN에 대한 레이블 역할을 합니다. 동일한 IP 서브넷 또는 FQDN을 사용하는 여러 액세스 정책을 수정해야 하는 경우, 네트워크 개체만 수정하면 모든 정책에 반영됩니다. 현재 이 개체를 생성하거나 수정하려면 Meraki 대시보드를 사용해야 합니다. 이러한 개체가 사용자 환경에서 수행할 수 있는 작업에 대한 자세한 내용은 Meraki의 네트워크 개체 하이라이트를 참조하십시오.



주

Meraki 네트워크 개체 또는 네트워크 개체 그룹을 참조하는 디바이스 구성이 Security Cloud ControlUI에 온보딩되거나 동기화되면 이러한 개체는 FTD 네트워크 개체로 표시됩니다.

이러한 개체 및 개체 그룹은 Security Cloud Control에서 읽기 전용입니다.

Security Cloud Control Meraki

디바이스의 정책 페이지에서 개체를 보거나 디바이스를 기준으로 개체 페이지를 필터링할 수 있습니다. 정책 페이지에서 액세스 제어 규칙을 보고, 편집하고, 순서를 바꿀 수 있습니다. Security Cloud Control은 Meraki 대시보드의 아웃바운드 규칙을 개체가 포함된 액세스 제어 규칙으로 변환하므로 Meraki 대시보드의 규칙 및 프로토콜은 다르게 보일 수 있습니다. 다음 표에서는 디바이스가 Security Cloud Control에 온보딩된 경우의 새 프로토콜 이름을 다룹니다.

Meraki 대시보드의 규칙 또는 프로토콜 헤더

정책

Source IP

목적지 IP

소스 포트

대상 포트

레이어 3 애플리케이션 프로토콜

Security Cloud Control의 규칙 또는 개체 헤더

작업

네트워크 개체 또는 네트워크 그룹

네트워크 개체 또는 네트워크 그룹

네트워크 개체 또는 네트워크 그룹

네트워크 개체 또는 네트워크 그룹

포트(프로토콜 그룹, 포트 그룹 또는 서비스 개체)

다음은 Meraki 대시보드의 아웃바운드 규칙이 Security Cloud Control에 표시되는 내용의 예입니다.

Access Control				
#	Name	Action	Source	Destination
1	L3_Rule_1	Allow	[NETS] 192.168.128...	[PORTS] TCP:any
2	L3_Rule_2	Block	[NETS] 192.168.128... [PORTS] UDP:80-100	[NETS] 10.10.0.2/16

Meraki

서비스 개체는 TCP/IP 프로토콜 및 포트를 지정하는 재사용 가능한 구성 요소입니다. Security Cloud Control은 이러한 개체를 서비스 개체로 분류합니다. MX 디바이스에 구축할 때 Security Cloud Control은 개체를 프로토콜 또는 포트 범위로 변환합니다. Security Cloud Control가 Meraki 프로토콜을 개체로 처리하는 방법에 대한 자세한 내용은 [Meraki 디바이스와 연결된 개체](#) 페이지 84을 참조하십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 개체를 클릭합니다.
3. 를 클릭한 다음 FTD Service(FTD 서비스) 또는 ASA Service(ASA 서비스)를 클릭합니다.  > >
4. 개체 이름과 설명을 입력합니다.
5. **Create a service object**(서비스 개체 생성)를 선택합니다.
6. **Service Type**(서비스 유형) 버튼을 클릭하고 개체를 생성할 프로토콜을 선택합니다.
7. 다음 작업 중 하나를 수행하여 프로토콜을 식별하기 위한 정보를 입력합니다.
 - TCP 또는 UDP 포트의 특정 포트 번호를 입력합니다.
 - ICMP 또는 ICMPv6 메시지 유형을 선택합니다.
 - "기타" 서비스 유형을 선택한 경우 목록에서 TCP/IP 프로토콜 중 하나를 선택합니다.
8. **Add**(추가)를 클릭합니다.
9. 지금 변경 사항을 [검토하고 구축](#)하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 개체를 클릭합니다.
3.  를 클릭한 다음 **FTD > Service(서비스)**를 클릭합니다.



주

Meraki는 ASA 서비스 그룹을 지원하지 않습니다.

4. 개체 이름과 설명을 입력합니다.
5. **Create a service group(서비스 그룹 생성)**를 선택합니다.
6. **Add Object(개체 추가)**를 클릭하고, 개체를 선택하고, **Select(선택)**을 클릭하여 기존 개체를 추가합니다. 개체를 더 추가하려면 이 단계를 반복합니다.
7. 서비스 그룹에 서비스 개체 및 서비스 값 추가를 완료하면 **Add(추가)**를 클릭합니다.
8. 지금 변경 사항을 **검토하고 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 개체를 클릭합니다.
3. 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.
4. 세부 정보 창에서 **Edit(편집)**  를 클릭합니다.
5. 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.
6. **Save(저장)**를 클릭합니다.
7. Security Cloud Control에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다. 이제 개체를 Meraki 정책에서 사용할 준비가 되었습니다.
8. 지금 변경 사항을 **검토하고 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Firepower



클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects**(네트워크 개체 검색 및 관리)가 활성화된 각 온프레미스 Firewall Management Center에 대한 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 Firewall Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 개체를 클릭합니다.
3. 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.
4. 편집할 개체를 선택합니다.
5. 세부 정보 창에서 편집 버튼  을 클릭합니다.
6. 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.
7. **Save(저장)**를 클릭합니다.
8. Security Cloud Control에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.
9. 지금 변경 사항을 **검토하고 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

:

- Security Cloud Control Firewall Management ☐ ☐ ☐ ☐ ☐ IP ☐ ☐ ☐ ☐
- Security Cloud Control Firewall Management ☐ ☐ ☐ ☐ ☐ ☐ ☐
- ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
- ☐ ☐ ☐ ☐ ☐ ☐
- ☐ ☐ ☐ ☐ ☐
- Security Cloud Control Firewall Management ☐ ☐ ☐ ☐ ☐ ☐
- ☐ ☐ ☐ ☐ ☐ ☐
- ☐ ☐ ☐ ☐ ☐ ☐
- ☐ ☐ ☐ ☐
- Security Cloud Control Firewall Management ☐ ☐ ☐ ☐ ☐
- ☐ ☐ ☐ ☐ ☐
- Firewall Threat Defense ☐ ☐ ☐ ☐ ☐
- Security Cloud Control Firewall Management ☐ ☐ ☐ Firewall Threat Defense ☐ ☐ ☐ ☐
- ☐ ☐ ☐ ☐ ☐
- Security Cloud Control Firewall Management ☐ ☐ ☐ ☐ ☐
- Security Cloud Control Firewall Management ☐ ☐ ☐ ☐ ☐

이 장에서는 온보딩된 디바이스의 디바이스 설정 관리에 대한 지침을 제공합니다.

Security Cloud Control Firewall Management IP

Security Cloud Control Firewall Management에서 디바이스의 IP 주소를 변경하는 방법을 알아보십시오.

IP 주소를 사용하여 Security Cloud Control Firewall Management에 디바이스를 온보딩하면 Security Cloud Control Firewall Management는 해당 IP 주소를 데이터베이스에 저장하고 해당 IP 주소를 사용하여 디바이스와 통신합니다. 디바이스의 IP 주소가 변경되면 새 주소와 일치하도록 Security Cloud Control Firewall Management에 저장된 IP 주소를 업데이트할 수 있습니다. Security Cloud Control Firewall Management에서 디바이스의 IP 주소를 변경해도 디바이스의 구성은 변경되지 않습니다.

Security Cloud Control가 디바이스와 통신하는 데 사용하는 IP 주소를 변경하려면 다음 절차를 수행합니다.

1. 선택 보안 디바이스
2. **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
3. 해당 디바이스 탭을 클릭합니다.
필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.
4. IP 주소를 변경할 디바이스를 선택합니다.
5. **Device Details**(디바이스 세부 정보) 창 위에서 디바이스의 IP 주소 옆에 있는 편집 버튼을 클릭합니다.

Nashua Building 1 
ASA 10.86.118.4:443 

6. 필드에 새 IP 주소를 입력하고 파란색 확인 버튼을 클릭합니다.
디바이스 자체는 변경되지 않으므로 디바이스의 **Configuration Status**(구성 상태)는 계속해서 **Synced**(동기화됨)로 표시됩니다.

Security Cloud Control Firewall Management

Security Cloud Control Firewall Management에서 디바이스의 IP 주소를 변경하는 방법을 알아보십시오.

모든 디바이스, 모델, 템플릿 및 서비스는 온보딩되거나 Security Cloud Control Firewall Management에서 생성될 때 이름이 지정됩니다. 디바이스 자체의 구성을 변경하지 않고 해당 이름을 변경할 수 있습니다.

1. 보안 디바이스를 선택합니다.
2. **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
3. 이름을 변경하려는 디바이스를 선택합니다.
4. **Device Details**(디바이스 세부 정보) 창 위에서 디바이스의 이름 옆에 있는 편집 버튼을 클릭합니다.

Nashua Building 1 

5. 필드에 새 이름을 입력하고 파란색 확인 버튼을 클릭합니다.

디바이스 자체는 변경되지 않으므로 디바이스의 **Configuration Status**(구성 상태)는 계속해서 **Synced**(동기화됨)로 표시됩니다.

Security Cloud Control Firewall Management에서 디바이스 및 서비스 목록을 내보내는 방법을 알아보십시오.

이 문서에서는 디바이스 및 서비스 목록을 쉼표로 구분된 값(.csv) 파일로 내보내는 방법을 설명합니다. 이 형식이 되면 **Microsoft Excel**과 같은 스프레드시트 애플리케이션에서 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다.

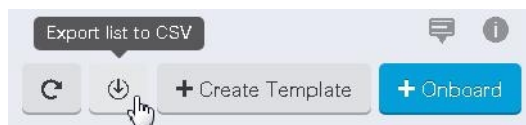
내보내기 버튼은 디바이스 및 템플릿 탭에서 사용할 수 있습니다. 또한 선택한 디바이스 유형 탭의 디바이스에서 세부 정보를 내보낼 수 있습니다.

디바이스 및 서비스 목록을 내보내기 전에 필터 창을 살펴보고 **Security Devices**(보안 디바이스) 테이블에 내보내려는 정보가 표시되는지 확인합니다. 모든 필터를 지워 모든 매니지드 디바이스 및 서비스를 확인하거나 정보를 필터링하여 모든 디바이스 및 서비스의 하위 집합을 표시합니다. 내보내기 기능에는 현재 **Security Devices**(보안 디바이스) 페이지에 표시된 정보만 포함됩니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.
3. **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
4. 해당 디바이스 유형 탭을 클릭하여 해당 탭 아래의 디바이스에서 세부 정보를 내보내거나 **All**(모두)를 클릭하여 모든 디바이스에서 세부 정보를 내보냅니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

5. **Export list to CSV**(CSV로 목록 내보내기)를 클릭합니다.



6. 메시지가 표시되면 .csv 파일을 저장합니다.
7. 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

Security Cloud Control Firewall Management에서 디바이스 구성을 내보내는 방법을 알아보십시오.

한 번에 하나의 디바이스 구성만 내보낼 수 있습니다. 다음 절차를 사용하여 디바이스의 구성을 **JSON** 파일로 내보냅니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.

2. 보안 디바이스를 선택합니다.
3. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
4. 해당 디바이스 탭을 클릭합니다.
필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.
5. 원하는 디바이스를 선택하여 강조 표시하십시오.
6. **Actions(작업)** 창에서 **Export Configuration(구성 내보내기)**를 선택합니다.
7. **Confirm(확인)**을 선택하여 구성을 JSON 파일로 저장합니다.

Security Cloud Control Firewall Management에서 디바이스의 외부 링크에 대해 알아봅니다.

외부 리소스에 대한 하이퍼링크를 생성하여 Security Cloud Control로 관리하는 디바이스와 연결할 수 있습니다. 이 기능을 사용하여 디바이스 중 하나의 로컬 관리자에 대한 편리한 링크를 생성할 수 있습니다(ASA의 경우, FTD의 경우). 또한 이를 사용하여 검색 엔진, 설명서 리소스, 회사 Wiki 또는 선택한 다른 URL에 연결할 수 있습니다. 외부 링크를 원하는 만큼 디바이스에 연결할 수 있습니다. 동일한 링크를 여러 디바이스와 동시에 연결할 수도 있습니다.

생성한 링크는 어디에나 연결할 수 있지만 회사의 보안 요구 사항은 변경되지 않습니다. 예를 들어 특정 URL에 도달하기 위해 온프레미스 또는 VPN 연결을 통해 일반적으로 기업 네트워크에 연결해야 하는 경우 이러한 요구 사항은 그대로 유지됩니다. 회사에서 특정 URL을 차단하는 경우 해당 URL은 계속 차단됩니다. 제한되지 않은 URL은 계속해서 제한되지 않습니다.

URL에 통합할 수 있는 {location} 변수를 생성했습니다. 이 변수는 디바이스의 IP 주소로 채워집니다. 예를 들면 다음과 같습니다.

```
https://{location}
```

또는

관련 설정, 요구 사항 및 사용자 워크플로우를 위해 디바이스에서 외부 링크를 생성하는 방법을 알아봅니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.

3. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
 4. 해당 디바이스 탭을 클릭합니다.
 5. 디바이스 또는 모델을 선택합니다.
필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.
 6. 외부 링크 섹션의 세부 정보 창에 링크의 이름을 입력합니다.
 7. URL 필드에 링크의 URL을 입력합니다. 전체 URL을 지정해야 합니다. 예를 들어 Cisco의 경우 <http://www.cisco.com>을 입력합니다.
 8. +를 클릭하여 링크를 디바이스와 연결합니다.
-

ASDM FDM에 대한 외부 링크를 생성하는 방법을 알아보십시오. ASA의 ASDM(Adaptive Security Device Manager), FDM 매니지드 디바이스의 FDM(Firepower Device Manager)을 여는 편리한 방법은 다음과 같습니다.

다음은 Security Cloud Control에서 직접 과 을 여는 편리한 방법입니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
 2. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
 3. 해당 디바이스 탭을 클릭합니다.
필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.
 4. 디바이스 또는 모델을 선택합니다.
 5. 세부 정보 창의 오른쪽에서, **External Links(외부 링크)** 섹션으로 이동합니다.
 6. 과 같은 링크 이름을 입력합니다.
 7. URL 필드에 <https://{location}>을 입력합니다. {location} 변수는 디바이스의 IP 주소로 채워집니다.
 8. + 상자를 클릭합니다.
-

1. 보안 디바이스를 선택합니다.
2. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
3. 해당 디바이스 탭을 클릭합니다.
필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.
4. 여러 디바이스 또는 모델을 선택합니다.
5. 세부 정보 창의 오른쪽에서, **External Links(외부 링크)** 섹션으로 이동합니다.
6. 링크 이름을 입력합니다.
7. 다음 방법 중 하나를 사용하여 도달하려는 URL을 입력하십시오.

- 입력

```
https://{location}
```

URL 필드에, {location} 변수는 디바이스의 IP 주소로 채워집니다. 이렇게 하면 디바이스의 ASDM에 대한 자동 링크가 생성됩니다.

- URL 필드에 링크의 URL을 입력합니다. 예를 들어 Cisco의 경우 <http://www.cisco.com>을 입력하는 것과 같이 전체 URL을 지정해야 합니다.

8. +를 클릭하여 링크를 디바이스와 연결합니다.

1. 보안 디바이스를 선택합니다.
 2. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
 3. 해당 디바이스 탭을 클릭합니다.
필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.
 4. 디바이스 또는 모델을 선택합니다.
 5. 세부 정보 창에서 **External Links(외부 링크)** 섹션으로 이동합니다.
 6. 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.
 7. 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.
-

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
 2. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
 3. 해당 디바이스 탭을 클릭합니다.
필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.
 4. 여러 디바이스 또는 모델을 선택합니다.
 5. 세부 정보 창의 오른쪽에서, **External Links(외부 링크)** 섹션으로 이동합니다.
 6. 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.
 7. 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.
-

Security Cloud Control Firewall Management

디바이스를 Security Cloud Control Firewall Management에 대량으로 재연결하는 방법을 알아보십시오.

관리자는 **Security Cloud Control Firewall Management**를 통해 둘 이상의 매니지드 디바이스를 **Security Cloud Control Firewall Management**에 동시에 다시 연결할 수 있습니다. **Security Cloud Control Firewall Management**가 관리하는 디바이스가 "unreachable(연결할 수 없음)"로 표시되면 **Security Cloud Control Firewall Management**는 더 이상 대역 외 구성 변경 사항을 탐지하거나 디바이스를 관리할 수 없습니다. 연결이 끊어지는 데에는 여러 가지 이유가 있을 수 있습니다. 디바이스에 대한 **Security Cloud Control Firewall Management** 관리를 복원하는 첫 번째 단계는 디바이스를 다시 연결하는 것입니다.

주

새 인증서가 있는 디바이스를 다시 연결하는 경우 **Security Cloud Control Firewall Management**는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다. 그러나 하나의 디바이스에만 다시 연결하는 경우 **Security Cloud Control Firewall Management**는 계속해서 다시 연결하려면 인증서를 수동으로 검토하고 수락하라는 메시지를 표시합니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. 디바이스를 찾으려면 **Devices(디바이스)** 탭을 클릭합니다.
3. 해당 디바이스 탭을 클릭합니다.
필터를 사용하여 연결 상태가 "unreachable(연결할 수 없음)"인 디바이스를 찾습니다.
4. 필터링된 결과에서 다시 연결을 시도할 디바이스를 선택합니다.
5. **Reconnect(다시 연결)**  를 클릭합니다. **Security Cloud Control**는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.
6. 알림 탭에서 대량 디바이스 다시 연결 작업의 진행 상황을 확인합니다. 대량 디바이스 다시 연결 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review(검토)** 링크를 클릭합니다. 그러면 **Security Cloud Control**에서 **작업 모니터링** 페이지 132로 이동합니다.

팁

디바이스의 인증서 또는 자격 증명이 변경되어 재연결 실패가 발생한 경우, 해당 디바이스에 개별적으로 다시 연결하여 새 자격 증명을 추가하고 새 인증서를 수락해야 합니다.

Security Cloud Control Firewall Management에서 조직 간에 디바이스를 이동하는 방법을 알아보십시오.

Security Cloud Control Firewall Management 조직에 디바이스를 온보딩한 후에는 한 **Security Cloud Control Firewall Management** 조직에서 다른 조직으로 디바이스를 마이그레이션할 수 없습니다. 디바이스를 새 조직으로 이동하려면 이전 테넌트에서 디바이스를 제거하고 새 조직에 다시 온보딩해야 합니다.

Security Cloud Control Firewall Management의 디바이스 인증서 만료 감지에 대해 알아보십시오.

관리 인증서는 Security Cloud Control Firewall Management에서 FDM 관리 및 ASA 디바이스에 액세스하는 데 사용되지만, Cisco Secure Client(이전 AnyConnect)는 Security Cloud Control Firewall Management의 ASA, FDM 관리 및 FTD 디바이스에서 가상 프라이빗 네트워크 기능을 사용하는데 필요합니다.

Security Cloud Control Firewall Management는 이러한 인증서의 만료 상태를 적극적으로 모니터링하고 이러한 인증서가 만료 날짜에 가까워지거나 만료되면 사용자에게 알립니다. 이렇게 하면 인증서 만료로 인해 디바이스 작동이 중단되는 것을 방지할 수 있습니다. 이 문제를 해결하려면 해당 인증서를 갱신해야 합니다.

관리 인증서 만료 확인은 ASA 및 FDM 매니지드 디바이스에 적용되며, Secure Client 인증서 만료 확인은 ASA, FDM 관리 및 FTD 디바이스에 적용됩니다.

오른쪽 상단에서 알림() 아이콘을 클릭하여 테넌트에 온보딩된 디바이스에 발생했거나 영향을 미친 가장 최신 알림을 확인합니다. 우선순위가 높은 섹션에는 인증서 만료 알림이 표시됩니다.

이러한 알림은 인증서 만료일 30, 14 및 7일 전에 전송되며, 그 이후에는 인증서가 만료되거나 유효한 인증서로 갱신할 때까지 매일 전송됩니다. 사용자 환경설정 페이지의 알림 설정 섹션에서 이러한 알림을 이메일로 수신하도록 구독할 수도 있습니다. 자세한 내용은 [사용자 알림 환경설정](#)을 참조하십시오.

Security Cloud Control Firewall Management에서 디바이스 메모를 작성하는 방법에 대해 알아봅니다.

이 절차를 사용하여 디바이스에 대한 단일 일반 텍스트 메모 파일을 생성합니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
3. 해당 디바이스 탭을 클릭합니다.
4. 메모를 작성할 디바이스 또는 모델을 선택합니다.
5. 오른쪽의 **Management(관리)** 창에서 **Notes(메모)**를 클릭합니다.  [Notes](#).
6. 오른쪽의 편집기 버튼을 클릭하고 기본 텍스트 편집기, Vim 또는 Emacs 텍스트 편집기를 선택합니다.
7. 메모 페이지를 수정합니다.
8. **Save(저장)**를 클릭합니다.
메모가 탭에 저장됩니다.

Security Cloud Control Firewall Management

Security Cloud Control Firewall Management에서 디바이스를 삭제하는 방법을 알아봅니다.

Security Cloud Control Firewall Management에서 디바이스를 삭제하려면 다음 단계를 따르십시오.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.
3. 삭제할 디바이스를 선택합니다.
4. **Device Actions**(디바이스 작업) 창에서 **Remove**(제거)를 클릭합니다.
5. 디바이스 제거를 확인하려면 **OK**(확인)를 클릭합니다.
디바이스를 온보드 상태로 유지하려면 **Cancel**(취소)을 클릭합니다.

Security Cloud Control Firewall Management에서 보안 디바이스를 관리하는 방법을 알아봅니다.

Security Cloud Control Firewall Management **Security Devices**(보안 디바이스) 페이지에서 온보딩된 디바이스를 보고, 관리하고, 필터링하고, 평가할 수 있는 기능을 제공합니다. **Security Devices**(보안 디바이스) 페이지에서 다음을 수행할 수 있습니다.

- [Security Cloud Control](#) 관리를 위한 디바이스 및 서비스를 온보딩합니다.
- 매니지드 디바이스 및 서비스의 구성 상태 및 연결 상태를 봅니다.
- 별도의 탭으로 분류된 온보딩된 디바이스 및 템플릿을 봅니다. [보안 디바이스 개요](#) 페이지 99를 참조하십시오.
- 개별 디바이스 및 서비스를 평가하고 조치를 취합니다.
- 디바이스 및 서비스별 정보를 보고 문제를 해결합니다.
- 다음에서 관리하는 위협 방어 디바이스의 디바이스 상태를 확인합니다.
 - [클라우드 제공 Firewall Management Center](#)
 - [온프레미스 Firewall Management Center](#)

클라우드 제공 **Firewall Management Center**에서 관리하는 위협 방어 디바이스의 경우, 클러스터에 있는 디바이스의 노드 상태도 볼 수 있습니다.

- 이름, 유형, IP 주소, 모델 이름, 일련 번호 또는 레이블로 디바이스 또는 템플릿을 검색합니다. 검색은 대/소문자를 구분하지 않습니다. 여러 검색어를 제공하면 검색어 중 하나 이상과 일치하는 디바이스 및 서비스가 나타납니다. [페이지 레벨 검색](#) 페이지 101를 참조하십시오.
- 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 감지, 보안 디바이스 커넥터 및 레이블을 기준으로 디바이스 또는 템플릿 필터를 필터링합니다. [필터](#)를 참조하십시오.
- 디바이스 삭제

Firewall Threat Defense

Security Cloud Control Firewall Management에서 관리하는 **Firewall Threat Defense** 디바이스를 백업하는 방법에 대해 알아봅니다.

Security Cloud Control 매니지드 **Firewall Threat Defense** 디바이스 유형을 백업하는 방법을 알아보려면 다음을 참조하십시오.

Firewall Management Center Firewall Threat Defense

- Security Cloud Control 왼쪽 창에서 **Administration(관리) > Firewall Management Center**를 선택합니다.
- **FMC** 탭에서 **Cloud-delivered FMC(클라우드 제공 FMC)**를 선택합니다.
- 오른쪽 창에서 **Devices(디바이스)**를 클릭하여 클라우드 제공 Firewall Management Center로 이동합니다.
- 클라우드 제공 Firewall Management Center에서 위협 방어 Threat Defense Device 백업 단계를 계속 진행합니다.

Security Cloud Control Firewall Management Management Center Firewall Threat Defense

- Security Cloud Control 왼쪽 창에서 **Administration(관리) > Firewall Management Center**를 선택합니다.
- Firewall Threat Defense 디바이스가 백업하려는 온프레미스 방화벽 Management Center를 선택합니다.
- 오른쪽 창에서 **FMC Cross Launch URL**을 클릭하여 온프레미스 Firewall Management Center로 이동하거나 온프레미스 Firewall Management Center에 수동으로 로그인합니다.
- Cisco Secure Firewall Management Center 관리 가이드에서 Management Center에서 디바이스 백업 단계를 계속합니다.

Security Cloud Control Firewall Management Firewall Device Manager Firewall Threat Defense

FDM 매니지드 디바이스 백업 단계를 수행합니다.

Security Cloud Control Firewall Management Firewall Threat Defense

Security Cloud Control Firewall Management를 통해 Firewall Threat Defense 디바이스를 관리하는 방법을 알아봅니다.

Security Cloud Control Firewall Management는 하드웨어 및 가상 형식 모두로 Firewall Threat Defense 디바이스를 관리할 수 있는 통합 인터페이스를 제공합니다.

이 세 가지 관리 애플리케이션과 연결된 Firewall Threat Defense 디바이스는 Security Cloud Control 플랫폼에서 관리할 수 있습니다.

- 보안 Firewall Device Manager
- Secure Firewall Management Center
- 보안 클라우드 제공 Firewall Management Center

1. Security Cloud Control 플랫폼에 로그인합니다.
2. 왼쪽 창에서 **Security Devices(보안 디바이스)**를 클릭합니다.
3. **FTD** 탭을 클릭합니다.

4. 왼쪽 위 모서리에 있는  를 클릭합니다.

디바이스/서비스 아래에서, 필터창은 해당 Security Cloud Control 디바이스가 액세스되는 관리 애플리케이션에 따라 Firewall Threat Defense 디바이스를 표시하는 필터를 제공합니다.

- **FDM:** Firewall Device Manager에서 관리하는 Firewall Threat Defense 디바이스

- **FMC-FTD: Firepower Management Center**를 사용하여 관리되는 **Firewall Threat Defense** 디바이스
- **FTD: 클라우드 제공 Firewall Management Center**에서 관리하는 **Firewall Threat Defense** 디바이스

5. 관리 애플리케이션에서 **Firewall Threat Defense** 디바이스를 보려면 해당 체크 박스를 선택합니다.

Security Cloud Control의 보안 디바이스 페이지에서 온보딩된 디바이스 및 템플릿을 보고, 필터를 적용하고, 지원 계획 및 보고를 위해 하드웨어 단종이 임박한 디바이스를 식별하는 방법을 알아봅니다.

Security Devices(보안 디바이스) 페이지에는 모든 물리적 및 가상 온보딩된 디바이스와 온보딩된 디바이스에서 생성된 템플릿이 표시됩니다. 이 페이지는 유형에 따라 디바이스 및 템플릿을 분류하고 각 디바이스 유형 전용 해당 탭에 표시합니다.

Security Devices(보안 디바이스) 페이지에서 다음 세부 정보를 볼 수 있습니다.

- **Device(디바이스)** 탭에는 **Security Cloud Control**에 온보딩된 모든 라이브 디바이스가 표시됩니다.
- **Templates(템플릿)**에는 **Security Cloud Control**로 가져온 라이브 디바이스 또는 구성 파일에서 생성된 모든 템플릿 디바이스가 표시됩니다.

Security Devices(보안 디바이스) 페이지의 **Filter(필터)** 패널에서는 결과 범위를 좁히고 특정 속성을 기준으로 디바이스를 찾을 수 있는 여러 옵션이 제공됩니다. 여기에는 디바이스/서비스, 하드웨어 버전, 디바이스 단종, 소프트웨어 버전, **Snort** 버전, 구성 상태, 연결 상태, 탐지, 상태, **Secure Device Connector** 및 레이블이 포함됩니다.

하드웨어 단종(**EoL**) 필터

하드웨어 단종(**EoL**) 필터를 사용 하면 하드웨어 지원 만료일이 임박했거나 사용한 디바이스를 식별할 수 있습니다. 지원 종료일 이후에는 **Cisco**가 더 이상 소프트웨어 업데이트, 보안 패치 또는 기술 지원을 제공하지 않으므로 지원되지 않는 하드웨어를 사용하면 운영 및 보안 위험이 발생할 수 있습니다.



주

하드웨어 **EoL** 필터는 현재 온프레미스 **Firewall Management Center** 및 클라우드 제공 **Firewall Management Center**에서 관리하는 **Firewall Threat Defense** 디바이스와 **ASA** 디바이스를 지원합니다.

절차

1. **Devices(디바이스)** 탭에서 필터 아이콘을 클릭합니다.
2. 사용 가능한 필터 목록의 **Device End-of-Life(디바이스 단종)** 아래에서 **Hardware End-of-Life(하드웨어 단종)**를 선택합니다.
목록에는 이제 하드웨어 수명이 다해가는 중이거나 이미 다한 모든 디바이스가 표시됩니다.
3. 디바이스를 선택하여 오른쪽 창에서 자세한 정보를 봅니다.
4. **Device End of Life(디바이스 단종)** 섹션까지 아래로 스크롤하여 다음 세부 정보를 확인합니다.
 - 정확한 단종 날짜입니다.
 - 지원 종료일까지 남은 시간입니다.

5. Know more(자세히 알아보기)를 클릭합니다.

다음 정보를 제공하는 세부 정보 페이지를 볼 수 있습니다.

- 시스코가 권장하는 교체용 디바이스와 제품 사양, 그리고 공식 데이터 시트를 확인할 수 있는 링크입니다.
- [Cisco에 문의 페이지](#)를 통해 요청을 제출하는 방법 및 Cisco 전문가에게 직접 문의할 수 있는 옵션에 대한 지침.
- [제품 재활용 프로그램](#)에 대한 정보입니다.

6. Export(내보내기)를 클릭하여 오프라인 분석을 위해 디바이스 보고서를 CSV 형식으로 다운로드합니다.

Security Cloud Control Firewall Management

Security Cloud Control Firewall Management 레이블 을 사용하여 디바이스 및 개체를 그룹화하고, 레이블 그룹을 생성하고, 할당된 레이블을 기준으로 디바이스 또는 개체 테이블을 필터링하는 방법을 알아봅니다.

레이블은 디바이스 또는 개체를 그룹화하는 데 사용됩니다. 온보딩 중에 또는 온보딩 후에 언제든지 하나 이상의 디바이스에 레이블을 적용할 수 있습니다. 개체를 생성한 후 개체에 레이블을 적용할 수 있습니다. 디바이스 및 개체에 레이블을 적용한 후에는 해당 레이블을 사용하여 디바이스 테이블 또는 개체 테이블의 내용을 필터링할 수 있습니다.



주

디바이스에 적용된 레이블은 연결된 개체로 확장되지 않으며, 공유 개체에 적용된 레이블은 연결된 개체로 확장되지 않습니다.

group name:label 구문을 사용하여 레이블 그룹을 생성할 수 있습니다(예: Region:East 또는 Region:West). 이 두 레이블을 생성하는 경우 그룹 레이블은 Region(지역)이 되며 해당 그룹의 East(동부) 또는 West(서부) 중에서 선택할 수 있습니다.

디바이스에 레이블을 적용하려면 다음 단계를 수행합니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. 왼쪽 창에서 **Objects**(개체)를 클릭합니다.
3. **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
4. 해당 디바이스 탭을 클릭합니다.
5. 하나 이상의 디바이스를 선택합니다.
6. 오른쪽의 **Add Groups and Labels**(그룹 및 레이블 추가) 필드에서 디바이스의 레이블을 지정합니다.
7.  아이콘을 클릭합니다.

,
디바이스 유형, 상태, 버전, 커넥터, 관리 애플리케이션, 레이블 등의 속성을 기준으로 디바이스, 정책 및 개체를 필터링하는 방법을 알아봅니다.

Security Devices(보안 디바이스), Policies(정책) 및 Objects(개체) 페이지에서 필터를 사용하여 디바이스 및 개체를 찾습니다. 필터링하려면 왼쪽 창에서 필터 아이콘을 선택합니다.

Security Devices(보안 디바이스) 페이지의 필터 패널에서는 디바이스 유형, 하드웨어 버전, 소프트웨어 버전, Snort 버전, 구성 상태, 연결 상태, 충돌 탐지, **Secure Device Connector** 및 레이블과 같은 기준으로 디바이스를 필터링할 수 있습니다. 선택한 디바이스 유형 탭 내에서 필터를 적용할 수 있습니다.

FTD 탭이 열려 있으면 필터 패널을 사용하여 **Security Cloud Control**가 액세스에 사용하는 관리 애플리케이션별로 **FTD** 디바이스를 필터링할 수도 있습니다.

필터링하려면 **Security Devices(보안 디바이스), Policies(정책) 및 Objects(개체)** 탭의 왼쪽 창에서  을 클릭합니다.



FTD 탭이 열리면 필터 창이 **Security Cloud Control**에서 디바이스에 액세스하는 데 사용되는 관리 애플리케이션을 기반으로 **FDM** 관리 디바이스를 표시하는 필터를 제공합니다.

- **FDM:** FTD API 또는 **Firewall Device Manager**을(를) 사용하여 관리되는 디바이스.
- **FMC-FTD:** **Firepower Management Center**를 사용하여 관리되는 디바이스.
- **FTD:** FTD 관리를 사용하여 관리되는 디바이스.

Security Cloud Control Firewall Management

테넌트 전체에서 디바이스, 정책, 개체, VPN 항목, 변경 로그, 작업을 찾기 위해 페이지 수준 검색과 전역 검색을 사용하여 **Security Cloud Control Firewall Management**을(를) 검색하는 방법을 알아봅니다.

Security Cloud Control Firewall Management 플랫폼에는 필요한 모든 항목을 쉽게 찾을 수 있는 매우 효율적인 검색 기능이 있습니다. 각 페이지의 검색 창은 해당 페이지의 콘텐츠에 따라 맞춤화되지만, 전역 검색을 사용하면 전체 테넌트에 대한 포괄적인 검색이 가능합니다. 이렇게 하면 필요한 정보를 신속하게 찾을 수 있으므로 시간과 노력을 절약할 수 있습니다.

페이지 레벨 검색을 사용하면 보안 디바이스, 정책, 개체, VPN, 변경 로그 및 작업 페이지에서 특정 항목을 검색할 수 있습니다.

- **Security Devices(보안 디바이스)** 공간에서 검색 창에 입력을 시작하면 검색 기준에 맞는 디바이스가 표시됩니다. 디바이스의 일부 부분 이름, IP 주소 또는 물리적 디바이스의 일련 번호를 입력하여 디바이스를 찾을 수 있습니다.
- **Policies(정책)** 영역에서는 이름, 구성 요소 또는 사용된 개체를 기준으로 정책을 검색할 수 있습니다.
- **Objects(개체)** 영역에서는 개체 이름 또는 IP 주소 일부, 포트나 프로토콜을 입력하여 개체를 검색할 수 있습니다.
- **VPN** 영역에서는 터널 이름, 디바이스 이름 및 VPN 정책에 사용된 IP 주소를 기준으로 검색할 수 있습니다.

- **Change log(변경 로그)** 영역에서는 이벤트, 디바이스 이름 또는 작업을 기준으로 로그를 검색할 수 있습니다.

1. 인터페이스 상단 근처의 검색 창으로 이동합니다.
2. 검색 표시줄에 검색 기준을 입력하면 해당 결과가 표시됩니다.

Security Cloud Control의 전역 검색은 중앙 집중식 방법을 제공하여 온보딩된 디바이스, 개체 및 정책을 신속하게 찾고 탐색할 수 있습니다.

전체 검색 기능을 사용하면 Security Cloud Control에서 관리하는 디바이스를 빠르게 찾고 탐색할 수 있습니다.



주

현재 Security Cloud Control는 ASA, 클라우드 제공 Firewall Management Center, Security Cloud Control에서 관리하는 온프레미스 Firewall Management Center, Firewall Threat Defense 및 Meraki에 대한 글로벌 검색을 지원합니다.

전역 검색은 Security Cloud Control Firewall Management을(를) Security Cloud Control에 온보딩한 경우에만 사용할 수 있습니다.

모든 검색 결과는 선택한 인덱싱 옵션을 기반으로 합니다. 인덱싱 옵션은 다음과 같습니다:

- **전체 인덱싱** - 전체 인덱싱 프로세스를 호출해야 합니다. 이 프로세스는 시스템의 모든 디바이스와 개체를 검색하고 인덱싱을 호출한 후에만 검색 인덱스에 표시합니다. 전체 인덱싱을 호출하려면 관리 권한이 있어야 합니다.

자세한 내용은 [전체 인덱싱 시작](#)을 참조하십시오.

- **중분 인덱싱** - 디바이스 또는 개체가 추가, 수정 또는 삭제될 때마다 검색 인덱스가 자동으로 업데이트되는 이벤트 기반 인덱싱 프로세스입니다.

검색 필드에 입력하는 정보는 대소문자를 구분하지 않습니다. 다음 엔티티를 사용하여 글로벌 검색을 수행할 수 있습니다:

- **디바이스 이름**—부분 디바이스 이름, URL, IP 주소 또는 범위를 지원합니다.
- **개체 유형** - 개체 이름, 개체 설명 및 구성된 값을 지원합니다.
- **정책 유형** - 정책 이름, 정책 설명, 규칙 이름 및 규칙 설명을 지원합니다.

클라우드 제공 Firewall Management Center 및 Security Cloud Control에서 관리되는 온프레미스 Firewall Management Center는 다음 정책 유형을 지원합니다:

- 액세스 제어 정책
- 사전 필터 정책
- 위협 방어 NAT 정책

검색식을 입력하면 인터페이스에 검색 결과가 표시되기 시작하므로 검색을 실행하기 위해 **Enter** 키를 누를 필요가 없습니다.

검색 결과에는 검색 문자열과 일치하는 모든 디바이스 및 개체가 표시됩니다. 검색어가 둘 이상의 디바이스 또는 개체와 일치하면 결과가 **devices, objects, connected_fmc** 등의 범주로 표시됩니다.

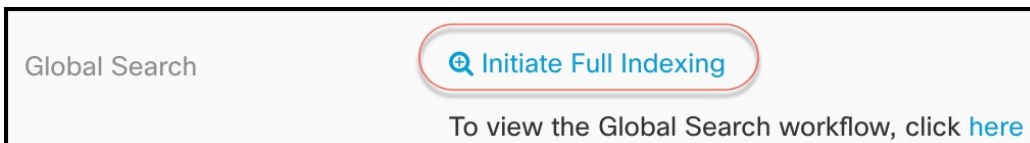
기본적으로 검색 결과의 첫 번째 항목이 강조 표시되고 해당 항목에 대한 관련 정보가 오른쪽 창에 나타납니다. 검색 결과를 스크롤하고 항목을 클릭하면 해당 정보를 볼 수 있습니다. 항목 옆의 화살표 아이콘을 클릭하여 해당 페이지로 이동할 수 있습니다.

주

- 전역 검색은 중복 검색 결과를 표시하지 않습니다. 개체의 경우 공유 개체의 **UID**는 개체 보기로 이동하는 데 사용됩니다.
- **Security Cloud Control**에서 디바이스를 삭제하면, 연결된 모든 개체가 전역 검색 인덱스에서 제거됩니다.
- 정책에서 개체를 삭제하고 전체 인덱싱을 시작하기 전에 디바이스를 유지하면, 개체가 디바이스와 연결되어 있기 때문에 전역 검색 인덱스에 남아 있습니다.

전역 검색을 위한 전체 인덱싱을 시작하는 절차.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Administration(관리) > General Settings(일반 설정)**를 클릭합니다.
3. 전역 검색에서 **Initiate Full Indexing(전체 인덱싱 시작)**을 클릭하여 인덱싱을 트리거합니다.



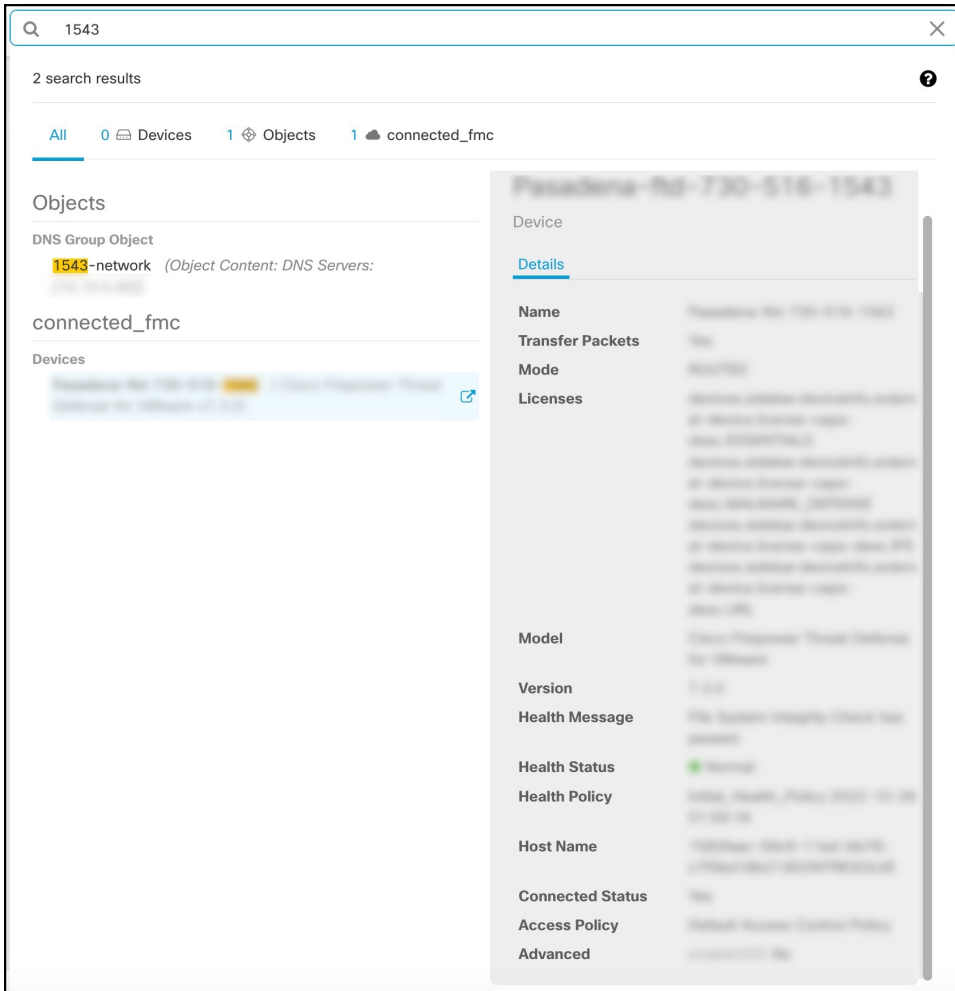
주

전체 인덱싱을 시작하면 **Security Cloud Control** 테넌트의 기존 인덱싱이 지워집니다.

4. 글로벌 검색 워크플로우를 보려면 **here(여기)**를 클릭합니다.

1. **Security Cloud Control**에 로그인합니다.
2. **Security Cloud Control** 페이지에서 검색 아이콘을 클릭하고 표시되는 검색 필드에 검색 문자열을 입력합니다.
또는 **Windows**에서는 **Ctrl** 키와 **/** 키를 동시에 누르고, **Mac**에서는 **Command** 키와 **/** 키를 동시에 눌러 검색 창을 열 수 있습니다.

검색 문자열을 입력하기 시작하면 검색 결과에 가능한 항목 목록이 표시됩니다. 검색 결과는 모두, 디바이스, 개체 및 클라우드 제공 **Firewall Management Center**의 네 가지 범주 아래에 나타납니다. 오른쪽 창에는 선택한 검색 결과에 대한 정보가 표시됩니다.



3. 검색 결과에서 디바이스 또는 개체를 선택하고 화살표 아이콘을 클릭하여 검색 결과에서 해당 디바이스 및 개체 페이지로 이동합니다. 검색 결과에서 항목을 선택하고 화살표 아이콘을 클릭하여 검색 결과에서 해당 페이지로 이동합니다.

📄 주

클라우드 제공 **Firewall Management Center**에서 디바이스 검색 결과를 선택하면, **Security Cloud Control**에서 클라우드 제공 **Firewall Management Center** 사용자 인터페이스로 이동할 수 있습니다.

4. **X**를 클릭하여 검색 표시줄을 닫습니다.

:

- □□ □□ □□ □□, □□ □□ □□
- Security Cloud Control□(□) □□□□ □□ □□□□

Security Cloud Control가 매니지드 디바이스 구성의 동기화를 유지하고 보류 중이거나 충돌하는 변경 사항을 해결하기 위해 디바이스 구성 변경 사항을 읽고, 비교하고, 삭제하고, 수락하고, 구축하는 방법을 알아봅니다.

디바이스를 관리하기 위해 Security Cloud Control는 디바이스 구성의 복사본을 로컬 데이터베이스에 저장합니다. Security Cloud Control가 매니지드 디바이스에서 구성을 읽을 때 해당 구성을 복사 및 저장합니다.

Security Cloud Control는 디바이스가 온보딩될 때도 디바이스 구성의 복사본을 읽고 저장합니다. 이러한 각 작업은 특정 용도로 사용됩니다.

- **Discard Changes(변경 사항 취소):** 이 작업은 디바이스의 구성 상태가 "Not Synced(동기화되지 않음)"인 경우에 사용할 수 있습니다. **Not Synced(동기화되지 않음)** 상태에서는 Security Cloud Control에서 보류 중인 디바이스의 구성에 대한 변경 사항이 있습니다. 이 옵션을 사용하면 보류 중인 모든 변경 사항을 취소할 수 있습니다. 보류 중인 변경 사항이 삭제되고 Security Cloud Control가 디바이스에 저장된 구성의 복사본으로 구성의 복사본을 덮어씁니다.
- **Check for Changes(변경 사항 확인):** 이 작업은 디바이스의 구성 상태가 "Synced(동기화됨)"인 경우에 사용할 수 있습니다. **Check for Changes(변경 사항 확인)**를 클릭하면 Security Cloud Control가 디바이스 구성의 복사본을 디바이스에 저장된 복사본과 비교하게 됩니다. 차이가 있는 경우 Security Cloud Control는 디바이스에 저장된 복사본으로 디바이스 구성의 복사본을 즉시 덮어씁니다.
- **Review Conflict(충돌 검토) 및 Accept Without Review(검토 없이 수용):** 디바이스에서 **Conflict Detection(충돌 탐지)**을 활성화한 경우 Security Cloud Control는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 디바이스에 저장된 구성의 복사본이 변경된 경우 Security Cloud Control는 "Conflict Detected(충돌 탐지됨)" 구성 상태를 표시하여 사용자에게 알립니다.
 - **Review Conflict(충돌 검토):** Review Conflict(충돌 검토)를 클릭하여 디바이스에서 직접 변경된 사항을 검토하고 수락하거나 거부합니다.
 - **Accept Without Review(검토 없이 수락):** 이 작업은 Security Cloud Control의 디바이스 구성 복사본을 디바이스에 저장된 구성의 최신 복사본으로 덮어씁니다. Security Cloud Control에서는 덮어쓰기 작업을 수행하기 전에 구성의 두 복사본에서 차이점을 확인하라는 메시지를 표시하지 않습니다.

Read All(모두 읽기): 대량 작업입니다. 상태에 상관없이 원하는 수의 디바이스를 선택하고 **Read All(모두 읽기)**을 클릭하여 Security Cloud Control에 저장된 모든 디바이스 구성을 디바이스에 저장된 구성으로 덮어쓸 수 있습니다.

- **Deploy Changes(변경 사항 구축):** 디바이스의 구성을 변경하면 Security Cloud Control는 변경 사항을 구성의 자체 복사본에 저장합니다.

다. 이러한 변경 사항은 디바이스에 구축할 때까지 **Security Cloud Control**에서 보류 중으로 유지됩니다. 구축되지 않은 보류 중인 변경 사항이 있는 경우 디바이스는 **Not Synced**(동기화되지 않음) 구성 상태가 됩니다.

보류 중인 구성 변경 사항은 네트워크 트래픽에 영향을 주지 않습니다. **Security Cloud Control**가 디바이스에 변경 사항을 구축한 후에만 적용됩니다.

Security Cloud Control는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 전체 디바이스 구성 파일을 덮어쓰지 않습니다. 변경 사항을 하나의 디바이스 또는 여러 디바이스에 동시에 구축할 수 있습니다.

- **Discard All**(모두 취소): 이 옵션은 **Preview and Deploy...(미리보기 및 구축...)**를 클릭한 후에 나타납니다.. **Preview and Deploy...(미리보기 및 구축...)**를 클릭하면 **Security Cloud Control**는 **Security Cloud Control**에 보류 중인 변경 사항의 미리보기를 표시합니다. **Discard All**(모두 취소)을 클릭하여 선택한 디바이스에 변경 사항을 구축하지 않고 **Security Cloud Control**에서 보류 중인 모든 변경 사항을 삭제할 수 있습니다. "**Discard Changes**(변경 사항 취소)"와 달리 보류 중인 변경 사항을 삭제하면 작업이 완료됩니다.

Security Cloud Control Firewall Management에서 구성 변경 사항을 읽고, 취소하고, 구축하는 방법을 알아보십시오.

Security Cloud Control 외부의 디바이스에 대한 구성이 변경되면 Security Cloud Control에 저장된 디바이스의 구성과 디바이스의 로컬 구성의 사본은 더 이상 동일하지 않습니다. 구성을 다시 동일하게 만들기 위해 디바이스에 저장된 구성으로 Security Cloud Control의 디바이스 구성 복사본을 덮어쓰려는 경우가 많습니다. **Read All(모두 읽기)** 링크를 사용하여 여러 디바이스에서 동시에 이 작업을 수행할 수 있습니다.

Security Cloud Control에서 디바이스 구성의 두 복사본을 관리하는 방법에 대한 자세한 내용은 [Reading, Discarding, Checking for, and Deploying Configuration Changes\(구성 변경 사항 읽기, 취소, 확인 및 구축\)](#)을 참조하십시오.

다음은 **Read All(모두 읽기)**을 클릭하면 Security Cloud Control의 디바이스 구성 복사본을 디바이스의 구성 복사본으로 덮어쓰는 세 가지 구성 상태입니다.

- **Conflict Detected(충돌 탐지됨):** 충돌 탐지가 활성화된 경우 Security Cloud Control는 관리하는 디바이스를 10분마다 폴링하여 구성 변경 사항을 확인합니다. Security Cloud Control는 디바이스의 구성이 변경된 것을 발견하면 Security Cloud Control는 디바이스에 대한 구성 상태를 "충돌 탐지됨"으로 표시합니다.
- **Synced(동기화됨):** 디바이스가 동기화된 상태에서 **Read All(모두 읽기)**을 클릭하면 Security Cloud Control는 즉시 디바이스를 확인하여 구성이 직접 변경되었는지 확인합니다. **Read All(모두 읽기)**을 클릭하면 Security Cloud Control는 디바이스 구성의 복사본을 덮어쓸 것임을 확인한 다음 Security Cloud Control는 덮어쓰기를 수행합니다.
- **Not Synced(동기화되지 않음):** 디바이스가 **Not Synced(동기화되지 않음)** 상태에서 **Read All(모두 읽기)**을 클릭하면 Security Cloud Control는 Security Cloud Control를 사용하여 변경한 디바이스 구성에 오류 중인 변경 사항이 있으며, **Read All(모두 읽기)** 작업을 진행하면 해당 변경 사항이 삭제된 다음 Security Cloud Control의 구성 복사본을 디바이스의 구성으로 덮어쓴다고 경고합니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.
3. **Devices(디바이스)** 탭을 클릭합니다.
4. 해당 디바이스 탭을 클릭합니다.
5. (선택 사항) 변경 로그에서 이 대량 작업의 결과를 쉽게 식별할 수 있도록 **변경 요청 레이블**을 생성합니다.
6. Security Cloud Control에 구성을 저장할 디바이스를 선택합니다.
Security Cloud Control는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.
Security Cloud Control는 선택한 디바이스 중 Security Cloud Control에 스테이징된 구성 변경 사항이 있는 경우 경고하고, 대량 구성 읽기 작업을 계속할지 묻습니다.
7. 계속하려면 **Read All(모두 읽기)**을 클릭합니다.
8. **Read All(모두 읽기)** 구성 작업의 진행 상황은 **알림** 탭에서 확인합니다. 대량 작업의 개별 작업이 성공하거나 실패한 방식에 대한 자세한 내용을 보려면 파란색 **Review(검토)** 링크를 클릭합니다. 그러면 **Jobs(작업) 페이지**로 이동합니다.
9. 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

Security Cloud Control에서 보류 중인 구성 변경 사항을 검토하고 매니지드 디바이스에 구축하고, 구축 진행 상황을 추적하고, 작업 또는 이벤트 로그에서 결과를 확인하는 방법을 알아봅니다.

Security Cloud Control는 조직의 디바이스에 대한 구성을 변경했지만 해당 변경 사항을 구축하지 않은 경우 구축 아이콘 에 주황색 점을 표시하여 알려줍니다. 이러한 변경의 영향을 받는 각 디바이스는 **Security Devices**(보안 디바이스) 페이지에서 **"Not Synced(동기화되지 않음)"** 상태로 표시됩니다. **Deploy(구축)**를 클릭하면 보류 중인 변경 사항이 있는 디바이스를 검토하고 해당 디바이스에 변경 사항을 구축할 수 있습니다.

이 구축 방법은 지원되는 모든 디바이스에서 사용할 수 있습니다.

단일 구성 변경 사항에 이 구축 방법을 사용할 수 있습니다. 또는 기다렸다가 여러 변경 사항을 한 번에 구축할 수 있습니다.

이 구축 방법은 Security Cloud Control Firewall Management가 Security Cloud Control에 온보딩된 경우에만 사용할 수 있습니다.

-
1. Security Cloud Control의 메뉴 모음에서 **Deploy(구축)** 버튼 을 클릭합니다.
 2. 구축하려는 변경 사항이 있는 디바이스를 선택합니다. 디바이스에 노란색 주의 삼각형이 있는 경우 해당 디바이스에 변경 사항을 구축할 수 없습니다. 노란색 주의 삼각형 위에 포인터를 올려놓으면 이유를 확인할 수 있습니다.
 3. (선택 사항) 보류 중인 변경 사항에 대한 자세한 정보를 보려면 **View Detailed Change log(자세한 변경 로그 보기)** 링크를 클릭하여 해당 변경과 관련된 변경 로그를 엽니다. **Deploy(구축)** 아이콘을 클릭하여 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 페이지로 돌아갑니다.
 4. 선택한 디바이스에 변경 사항을 즉시 구축하려면 **Deploy Now(지금 구축)**를 클릭합니다. 작업 트레이의 활성 작업 표시기에 진행 상황이 표시됩니다.
 5. (선택 사항) 구축이 완료된 후 **Platform(플랫폼)** 메뉴에서 **Firewall(방화벽)**을 클릭한 다음 **Events & Logs(이벤트 및 로그) > Events(이벤트) > Jobs(작업)**을 선택합니다. 구축 결과를 보여주는 최근 "Deploy Changes(변경 사항 구축)" 작업이 표시됩니다.
-

-
1. Security Cloud Control을 사용하여 디바이스에 대한 구성을 변경하고 저장하면 해당 변경 사항이 디바이스 구성의 Security Cloud Control 인스턴스에 저장됩니다.
 2. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
 3. 보안 디바이스를 선택합니다.
 4. **Devices(디바이스)** 탭을 클릭합니다.
 5. 해당 디바이스 탭을 클릭합니다. 변경 작업을 수행한 후에는 디바이스의 구성 상태가 **"Not synced(동기화되지 않음)"**로 표시됩니다.
 6. 변경 사항을 구축하려면 다음 방법 중 하나를 선택합니다:
 - 디바이스를 선택하고 **"Not Synced(동기화되지 않음)"** 창에서 **Preview and Deploy(미리보기 및 구축)**를 클릭합니다. **Pending Changes** 화면에서 변경 사항을 검토합니다. 보류 중인 버전에 만족하면 **Deploy Now(지금 구축)**를 클릭합니다.

변경 사항이 성공적으로 구축되면 **변경 로그**를 보고 확인할 수 있습니다.

- **Deploy(구축)** 아이콘  을 클릭합니다. 자세한 내용은 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#) 페이지 108를 참조하십시오.

Security Cloud Control에서 디바이스로 변경 사항을 구축할 때 **Cancel(취소)**를 클릭하면 변경 사항이 디바이스에 구축되지 않습니다. 프로세스가 취소됩니다. 변경 사항은 여전히 Security Cloud Control에서 보류 중이며 최종적으로 FDM 관리 디바이스에 구축하기 전에 추가로 편집할 수 있습니다.

변경 내용을 미리 볼 때 **Discard all(모두 삭제)**를 클릭하면 변경한 내용 및 다른 사용자가 변경했지만 디바이스에 구축하지 않은 기타 모든 변경 내용이 삭제됩니다. Security Cloud Control는 보류 중인 구성이 변경되기 전에 마지막으로 읽거나 구축한 구성으로 되돌아갑니다.

예를 들어 공유 개체를 수정하여 여러 디바이스를 변경한 경우 해당 변경 사항을 영향을 받는 모든 디바이스에 한 번에 적용할 수 있습니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. **Devices(디바이스)** 탭을 클릭합니다.
3. 해당 디바이스 탭을 클릭합니다.
4. Security Cloud Control에서 구성을 변경한 모든 디바이스를 선택합니다. 이러한 디바이스는 "동기화되지 않음" 상태로 표시되어야 합니다.
5. 다음 방법 중 하나를 사용하여 변경 사항을 구축합니다.

- 화면 오른쪽 상단의  버튼을 클릭하여 **Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스)** 창을 엽니다. 이렇게 하면 구축하기 전에 선택한 디바이스에서 보류 중인 변경 사항을 검토할 수 있습니다. **Deploy Now(지금 구축)**를 클릭하여 변경 사항을 구축합니다.



Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스) 화면에서 디바이스 옆에 노란색 경고 삼각형이 표시되면 해당 디바이스에 변경 사항을 구축할 수 없습니다. 변경 사항을 해당 디바이스에 구축할 수 없는 이유에 대한 정보를 보려면 경고 삼각형 위에 마우스를 올려놓습니다.

- 세부 정보 창에서 **Deploy All(모두 구축)**  을 클릭합니다. 경고를 검토하고 **OK(확인)**를 클릭합니다. 대량 구축은 변경 사항을 검토하지 않고 즉시 시작됩니다.

6. (선택 사항) 탐색 모음에서 **Jobs(작업)** 아이콘  을 클릭하여 대량 구축의 결과를 확인합니다.

Security Cloud Control를 사용하면 CDO에서 관리하는 하나 이상의 디바이스에 대한 구성을 변경한 다음 편리한 시간에 해당 디바이스에 변경 사항을 구축하도록 예약할 수 있습니다.

Settings(설정) 페이지의 **Tenant Settings**(테넌트 설정) 탭에 **예약된 자동 구축 활성화** 페이지 31 있는 경우에만 구축을 예약할 수 있습니다. 이 옵션이 활성화되면 예약된 구축을 생성, 편집 또는 삭제할 수 있습니다. 예약된 구축은 Security Cloud Control에 저장된 모든 단계적 변경 사항을 설정된 날짜 및 시간에 구축합니다. Jobs(작업) 페이지에서 예약된 구축을 보고 삭제할 수도 있습니다.

Security Cloud Control에서 **읽히지** 않은 디바이스 변경 사항이 있는 경우 충돌이 해결될 때까지 예약된 구축을 건너뛵니다. 예약된 구축이 실패한 인스턴스가 Jobs(작업) 페이지에 나열됩니다. **Enable the Option to Schedule Automatic Deployments**(자동 구축 예약 옵션 활성화)가 해제된 경우 예약된 모든 구축이 삭제됩니다.



경고

여러 디바이스에 대해 새 배포를 예약하는 경우 해당 디바이스 중 일부가 이미 배포를 예약한 경우, 새로 예약된 배포가 기존의 예약된 배포를 덮어씁니다.



주

예약된 배포를 생성하면 디바이스의 표준 시간대가 아닌 현지 시간으로 일정이 생성됩니다. 예약된 구축은 일광 절약 시간에 맞게 자동으로 조정되지 않습니다.

구축 일정은 단일 이벤트 또는 반복 이벤트일 수 있습니다. 반복 자동 구축을 사용하면 유지 보수 기간에 맞춰 반복 구축을 편리하게 이용할 수 있습니다. 단일 디바이스에 대해 일회성 또는 반복 구축을 예약하려면 다음 절차를 따릅니다.

중요사항

이 절차는 ASA 및 FDM 매니지드 디바이스에만 적용됩니다.

온프레미스 Firewall Management Center 또는 클라우드 제공 Firewall Management Center에서 관리되는 Secure Firewall Threat Defense 디바이스의 구축을 예약하려면 [Scheduling\(예약\)](#)을 참조하십시오.



주

기존 구축이 예약된 디바이스에 대한 구축을 예약하는 경우 새로 예약된 구축이 기존 구축을 덮어씁니다.

1. Security Cloud Control 홈 페이지에서 보안 디바이스를 클릭합니다.

2. **Devices**(디바이스) 탭을 클릭합니다.
3. 해당 디바이스 탭을 클릭합니다.
4. 하나 이상의 디바이스를 선택합니다.
5. **Device Details**(디바이스 세부 정보) 창에서 **Scheduled Deployments**(예약된 구축) 탭을 찾아 **Schedule**(예약)을 클릭합니다.
6. 구축을 수행해야 하는 시기를 선택합니다.
 - 일회성 구축의 경우 **Once on**(한 번) 옵션을 클릭하여 달력에서 날짜와 시간을 선택합니다.
 - 반복 구축의 경우 **Every**(마다) 옵션을 클릭합니다. 매일 또는 일주일에 한 번 구축을 선택할 수 있습니다. 구축을 수행해야 하는 날짜와 시간을 선택합니다.
7. **Save**(저장)를 클릭합니다.

예약된 구축을 편집하려면 다음 절차를 따르십시오.

1. **Security Cloud Control** 홈 페이지에서 보안 디바이스를 클릭합니다.
 2. **Devices**(디바이스) 탭을 클릭합니다.
 3. 해당 디바이스 탭을 클릭합니다.
 4. 하나 이상의 디바이스를 선택합니다.
 5. **Device Details**(디바이스 세부 정보) 창에서 예약된 구축 탭을 찾아 **Edit**(편집)를 클릭합니다.
- 
6. 예약된 구축의 반복, 날짜 또는 시간을 수정합니다.
 7. **Save**(저장)를 클릭합니다.

예약된 구축을 삭제하려면 다음 절차를 따르십시오.



주

여러 디바이스에 대한 구축을 예약한 다음 일부 디바이스에 대한 일정을 변경하거나 삭제하면 나머지 디바이스에 대한 원래 예약된 구축이 유지됩니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. **Devices**(디바이스) 탭을 클릭합니다.
3. 해당 디바이스 탭을 클릭합니다.
4. 하나 이상의 디바이스를 선택합니다.

5. **Device Details**(디바이스 세부 정보) 창에서 **Scheduled Deployments**(예약된 구축) 탭을 찾아  **Delete**(삭제)를 클릭합니다.

- 구성 변경 사항 읽기, 삭제, 확인 및 구축
- 모든 디바이스 구성 읽기 페이지 107
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축 페이지 108

디바이스의 구성이 디바이스에서 직접 변경되었으며 **Security Cloud Control**에 저장된 구성의 복사본과 더 이상 동일하지 않은지 확인하려면 변경 사항을 확인합니다. 디바이스가 "Synced(동기화됨)" 상태일 때 이 옵션이 표시됩니다.

변경 사항을 확인하려면 다음을 수행합니다.

1. **Security Cloud Control** 홈 페이지에서 보안 디바이스를 클릭합니다.
2. **Devices**(디바이스) 탭을 클릭합니다.
3. 해당 디바이스 탭을 클릭합니다.
4. 구성이 디바이스에서 직접 변경되었을 가능성이 있는 디바이스를 선택합니다.
5. 오른쪽의 **Synced**(동기화) 창에서 **Check for Changes**(변경 사항 확인)를 클릭합니다.
6. 다음 동작은 디바이스에 따라 약간 다릅니다.

- **Meraki** 디바이스의 경우 디바이스의 구성이 변경된 경우 다음 메시지가 표시됩니다.

디바이스에서 정책을 읽는 중입니다. 디바이스에 활성 구축이 있는 경우 완료 후 읽기가 시작됩니다.

- 계속하려면 **OK**(확인)를 클릭하십시오. 디바이스의 구성이 **Security Cloud Control**에 저장된 구성을 덮어씁니다.
- 작업을 취소하려면 **Cancel**(취소)을 클릭합니다.

- 디바이스의 경우:

- a. 표시되는 두 가지 구성을 비교합니다. **Continue**(계속)를 클릭합니다. **Last Known Device Configuration**(마지막으로 알려진 디바이스 구성) 레이블이 지정된 구성은 **Security Cloud Control**에 저장된 구성입니다. **Found on Device**(디바이스에서 발견) 레이블이 지정된 구성은 **ASA**에 저장된 구성입니다.
- b. 다음 중 하나를 선택합니다.
 1. "마지막으로 알려진 디바이스 구성"을 유지하려면 대역 외 변경 사항을 거부합니다.
 2. 대역 외 변경 사항을 수락하여 **Security Cloud Control**에 저장된 디바이스의 구성을 디바이스에 있는 구성으로 덮어씁니다.
- c. **Continue**(계속)를 클릭합니다.

Security Cloud Control를 사용하여 디바이스의 구성에 적용한 구축 해제된 구성 변경 사항을 모두 "실행 취소"하려면 **Discard Changes**(변경 사항 취소)를 클릭합니다. **Discard Changes**(변경 사항 취소)를 클릭하면 Security Cloud Control는 디바이스 구성의 로컬 복사본을 디바이스에 저장된 구성으로 완전히 덮어씁니다.

Discard Changes(변경 사항 취소)를 클릭하면 디바이스의 구성 상태가 **Not Synced**(동기화되지 않음) 상태가 됩니다. 변경 사항을 취소하면 Security Cloud Control의 구성 복사본이 디바이스의 구성 복사본과 동일하게 되며 Security Cloud Control의 구성 상태는 **Synced**(동기화)로 돌아갑니다.

디바이스에 대해 구축되지 않은 모든 구성 변경 사항을 취소하거나 "실행 취소"하려면 다음을 수행합니다.

1. Security Cloud Control 홈 페이지에서 보안 디바이스를 클릭합니다.
2. **Devices**(디바이스) 탭을 클릭합니다.
3. 해당 디바이스 탭을 클릭합니다.
4. 구성을 변경한 디바이스를 선택합니다.
5. 오른쪽의 **Not Synced**(동기화되지 않음) 창에서 **Discard Changes**(변경 사항 취소)를 클릭합니다.
 - FDM 관리 디바이스의 경우 Security Cloud Control는 "Security Cloud Control에서 보류 중인 변경 사항이 취소되고 이 디바이스에 대한 Security Cloud Control 구성이 디바이스에서 현재 실행 중인 구성으로 교체됩니다."라고 경고합니다. 변경 사항을 취소하려면 **Continue**(계속)를 클릭합니다.
 - Meraki 디바이스의 경우 Security Cloud Control가 변경 사항을 즉시 삭제합니다.
 - AWS 디바이스의 경우 Security Cloud Control는 삭제하려는 항목을 표시합니다. **Accept**(수락) 또는 **Cancel**(취소)을 클릭합니다.

대역 외 변경 사항은 Security Cloud Control를 사용하지 않고 디바이스에서 직접 변경한 사항을 의미합니다. 이러한 변경은 SSH 연결을 통해 디바이스의 명령줄 인터페이스를 사용하거나 ASA용 ASDM(Adaptive Security Device Manager), FDM 관리 디바이스용 또는 온프레미스 방화벽 Management Center 사용자 인터페이스의 온프레미스 방화벽 Management Center용 FDM과 같은 로컬 관리자를 사용하여 수행할 수 있습니다. 대역 외 변경 사항은 Security Cloud Control에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

ASA 또는 FDM 관리 디바이스, Cisco IOS 디바이스 또는 온프레미스 방화벽 Management Center에 대해 **Conflict Detection**(충돌 탐지)이 활성화된 경우 Security Cloud Control는 10분마다 디바이스를 확인하여 Security Cloud Control 외부에서 디바이스의 구성에 직접 적용된 새로운 변경 사항을 검색합니다.

Security Cloud Control에 저장되지 않은 디바이스 구성 변경 사항이 있음을 발견하면 Security Cloud Control는 해당 디바이스의 구성 상태를 "충돌 탐지됨" 상태로 변경합니다.

Security Cloud Control에서 충돌을 탐지하는 경우 다음 두 가지 조건 중 하나가 발생할 수 있습니다.

- Security Cloud Control의 데이터베이스에 저장되지 않은 디바이스에 직접 적용된 구성 변경 사항이 있습니다.
- FDM 관리 디바이스의 경우 구축되지 않은 FDM 관리 디바이스에 "보류 중인" 구성 변경 사항이 있을 수 있습니다.
- 온프레미스 방화벽 Management Center의 경우, 예를 들어 Security Cloud Control 외부의 개체에 변경 사항이 있어 Security Cloud Control와의 동기화를 위해 보류 중이거나 Security Cloud Control에서 변경 사항이 있어 온프레미스 방화벽 Management Center에 구축하기 위해 보류 중일 수 있습니다.

Security Cloud Control ()

Security Cloud Control과(와) 디바이스 간에 구성을 동기화하는 방법을 알아보십시오.

Security Devices(보안 디바이스) 페이지에서 디바이스 또는 서비스의 상태가 "Synced(동기화됨)", "Not Synced(동기화되지 않음)" 또는 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. Security Cloud Control을 사용하여 관리하는 온프레미스 방화벽 Management Center의 상태를 확인하려면 **Administration(관리) > Integration(통합) > Firewall Management Center**으로 이동합니다.

- 디바이스가 동기화되면 Security Cloud Control의 구성과 디바이스에 로컬로 저장된 구성이 동일합니다.
- 디바이스가 동기화되지 않으면 Security Cloud Control에 저장된 구성이 변경되어 이제 디바이스에 로컬로 저장된 구성과 다릅니다. Security Cloud Control에서 디바이스로 변경 사항을 구축하면 Security Cloud Control의 버전과 일치하도록 디바이스의 구성이 변경됩니다.
- Security Cloud Control 외부에서 디바이스에 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경이 수행되면 디바이스에 대해 충돌 탐지가 활성화된 경우 디바이스 상태가 "Conflict Detected(충돌 탐지됨)"로 변경됩니다. 대역 외 변경 사항을 수락하면 Security Cloud Control의 구성을 디바이스의 구성과 일치하도록 변경합니다.

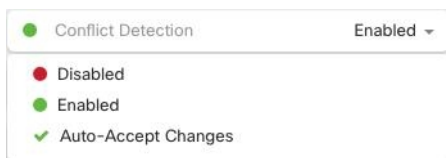
충돌 탐지가 활성화된 경우 Security Cloud Control는 기본 간격 동안 디바이스를 폴링하여 Security Cloud Control 외부에서 디바이스의 구성이 변경되었는지 확인합니다. Security Cloud Control는 변경 사항을 탐지하면 디바이스의 구성 상태를 **Conflict Detected(충돌 탐지됨)**로 변경합니다. Security Cloud Control 외부에서 디바이스에 적용된 변경 사항을 "대역 외" 변경 사항이라고 합니다.

Security Cloud Control에서 관리하는 온프레미스 방화벽 Management Center의 경우, 준비되는 변경 사항이 있고 디바이스가 **Not Synced(동기화되지 않음)** 상태이면 Security Cloud Control는 디바이스 폴링을 중지하여 변경 사항을 확인합니다. Security Cloud Control 외부에서 이루어진 변경 사항 중 Security Cloud Control와의 동기화를 위해 보류 중인 변경 사항과 Security Cloud Control에서 수행된 변경 사항 중 온프레미스 Firewall Management Center에 구축되기 위해 보류 중인 사항이 있는 경우, Security Cloud Control는 온프레미스 Firewall Management Center이 **Conflict Detected(충돌 탐지됨)** 상태임을 선언합니다.

이 옵션이 활성화되면 디바이스별로 충돌 또는 OOB 변경 사항이 탐지되는 빈도를 구성할 수 있습니다. 자세한 내용은 [디바이스 변경 사항에 대한 폴링 예약](#) 페이지 118를 참조하십시오.

충돌 탐지를 활성화하면 Security Cloud Control 외부에서 디바이스가 변경된 경우 인스턴스에 알림이 표시됩니다.

1. 보안 디바이스를 선택합니다.
2. **Devices(디바이스)** 탭을 클릭합니다.
3. 해당 디바이스 탭을 선택합니다.
4. 충돌 탐지를 활성화할 디바이스를 선택합니다.
5. 디바이스 테이블 오른쪽에 있는 충돌 감지 상자의 목록에서 **Enabled(활성화됨)**을 선택합니다.



변경 사항 자동 수락을 활성화하여 매니지드 디바이스에 대한 직접 변경 사항을 자동으로 수락하도록 **Security Cloud Control**를 구성할 수 있습니다. **Security Cloud Control**를 사용하지 않고 디바이스에 직접 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경은 **Security Cloud Control**에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

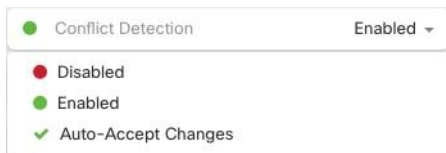
자동 수락 변경 기능은 충돌 탐지를 개선한 것입니다. 디바이스에서 변경 사항 자동 수락이 활성화된 경우 **Security Cloud Control**는 10분마다 변경 사항을 확인하여 디바이스의 구성에 대한 대역 외 변경 사항이 있는지 확인합니다. 구성이 변경된 경우 **Security Cloud Control**는 사용자에게 확인 상자를 표시하지 않고 디바이스 구성의 로컬 버전을 자동으로 업데이트합니다.

Security Cloud Control에서 아직 디바이스에 구축되지 않은 구성 변경 사항이 있는 경우 **Security Cloud Control**는 구성 변경을 자동으로 수락하지 않습니다. 화면의 프롬프트에 따라 다음 작업을 결정합니다.

자동 수락 변경 사항을 사용하려면 먼저 테넌트가 **Security Devices(보안 디바이스)** 페이지의 **Conflict Detection(충돌 탐지)** 메뉴에서 자동 수락 옵션을 표시하도록 활성화합니다. 그런 다음 개별 디바이스에 대한 변경 사항 자동 수락을 활성화합니다.

Security Cloud Control가 대역 외 변경 사항을 탐지하지만 수동으로 수락하거나 거부할 수 있는 옵션을 제공하도록 하려면 대신 [충돌 탐지](#) 페이지 114를 활성화합니다.

1. 관리자 또는 슈퍼 관리자 권한이 있는 어카운트를 사용하여 **Security Cloud Control**에 로그인합니다.
2. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
3. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
4. **Tenant Settings(테넌트 설정)** 영역에서, 토글을 클릭하여 디바이스 변경 사항을 자동으로 수락하는 옵션 활성화로 전환합니다. 이렇게 하면 변경 사항 자동 수락 메뉴 옵션이 **Security Devices(보안 디바이스)** 페이지의 충돌 감지 메뉴에 표시됩니다.
5. 왼쪽 창에서 보안 디바이스를 클릭하고 대역 외 변경 사항을 자동으로 수락할 디바이스를 선택합니다.
6. **Conflict Detection(충돌 감지)** 메뉴의 드롭다운 메뉴에서 **Auto-Accept Changes(변경 사항 자동 수락)**을 선택합니다.



1. 관리자 또는 슈퍼 관리자 권한이 있는 어카운트를 사용하여 **Security Cloud Control**에 로그인합니다.
2. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
3. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
4. **Tenant Settings(테넌트 설정)** 영역에서 회색 X가 표시되도록 토글을 왼쪽으로 밀어 "디바이스 변경 사항을 자동으로 수락하는 옵션 활성화"를 비활성화합니다. 이렇게 하면 충돌 감지 메뉴에서 변경 사항 자동 수락 옵션이 비활성화되고 테넌트의 모든 디바이스에 대한 기능이 비활성화 됩니다.



"자동 수락"을 비활성화하면 **Security Cloud Control**에 수락하기 전에 각 디바이스 충돌을 검토해야 합니다. 여기에는 이전에 변경 사항을 자동으로 수락하도록 구성된 디바이스가 포함됩니다.

이 섹션에서는 디바이스에서 발생하는 구성 충돌을 해결하는 방법에 대한 정보를 제공합니다.

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

1. 보안 디바이스를 선택합니다.



온프레미스 방화벽 **Management Center**의 경우, **Administration(관리) > Integration(통합) > Firewall Management Center**를 클릭하고 **Not Synced(동기화되지 않음)** 상태인 **FMC**를 선택한 후 5단계부터 계속 진행합니다.

2. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
3. 해당 디바이스 탭을 클릭합니다.
4. 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.
5. 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.
 - **미리보기 및 구축...** - **Security Cloud Control**에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 **미리 보고 구축**하거나 한 번에 여러 변경 사항을 기다렸다가 구축하십시오.

- 변경 사항 취소 - Security Cloud Control에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 Security Cloud Control에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 Security Cloud Control에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

Security Cloud Control를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. [충돌 탐지](#) 페이지 114이 활성화되어 있고 Security Cloud Control를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected(충돌 탐지됨)**로 표시됩니다.

Conflict Detected(충돌 탐지됨) 상태를 해결하려면 다음 절차를 수행합니다:

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.



주

온프레미스 방화벽 Management Center의 경우, **Administration(관리) > Integration(통합) > Firewall Management Center**를 클릭하고 **Not Synced(동기화되지 않음)** 상태인 FMC를 선택한 후 5단계부터 계속 진행합니다.

3. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾습니다.
4. 해당 디바이스 탭을 클릭합니다.
5. 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict(충돌 검토)**를 클릭합니다.
6. **Device Sync(디바이스 동기화)** 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.
 - "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 Security Cloud Control에 저장된 디바이스 구성입니다.
 - "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.
7. 다음 중 하나를 선택하여 충돌을 해결합니다.
 - **Accept Device changes(디바이스 변경 사항 수락)**: 구성 및 Security Cloud Control에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.



주

Security Cloud Control는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 구축하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review(검토 없이 수락)**를 선택하는 것입니다.

- **Reject Device Changes(디바이스 변경 거부)**: 디바이스에 저장된 구성을 Security Cloud Control에 저장된 구성으로 덮어씁니다.



거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

디바이스 변경 사항에 대한 폴링 예약을 맞춤화하여 **Security Cloud Control**을(를) 최적화합니다. 충돌 탐지 또는 자동 수락이 활성화된 경우 디바이스별로 특정 폴링 간격을 정의합니다. 이는 테넌트 기본값을 재정의하여 효율적이고 자동화된 디바이스 관리 및 동기화를 위해 네트워크 전체에서 디바이스 구성 변경 사항을 정확하게 모니터링하도록 합니다.

충돌 탐지 페이지 114을(를) 활성화하거나 **Settings(설정)** 페이지에서 **Enable the option to auto-accept device changes(디바이스 변경 사항 자동 수락 옵션 활성화)**를 활성화하면 **Security Cloud Control**은 기본 간격으로 디바이스를 폴링하여 **Security Cloud Control** 외부에서 구성이 변경되었는지 확인합니다. **Security Cloud Control**가 디바이스별로 변경 사항을 폴링하는 빈도를 맞춤화할 수 있습니다. 이 사용자 지정은 여러 디바이스에 적용할 수 있습니다.

디바이스에 대한 선택을 구성하지 않으면 간격이 자동으로 "테넌트 기본값"으로 구성됩니다.



Security Devices(보안 디바이스) 페이지에서 디바이스별 간격을 맞춤 설정하면 **General Settings(일반 설정)** 페이지에서 **Default Conflict Detection Interval(기본 충돌 탐지 간격)**로 선택한 폴링 간격이 재정의됩니다.

Security Devices(보안 디바이스) 페이지에서 **Conflict Detection(충돌 탐지)**을 활성화하거나 **Settings(설정)** 페이지에서 디바이스 변경 사항을 자동 수락하는 옵션을 활성화한 후 다음 절차를 사용하여 **Security Cloud Control**가 디바이스를 폴링할 빈도를 예약합니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.
3. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾습니다.
4. 해당 디바이스 탭을 클릭합니다.
5. 충돌 탐지를 활성화할 디바이스를 선택합니다.
6. **Conflict Detection(충돌 탐지)** 옆에서 **Check every(확인 간격)**의 드롭다운 메뉴를 클릭하고 원하는 폴링 간격을 선택합니다.

 **Conflict Detection**

● Enabled

▼

Check every:

Tenant default (24 hours)

▼

Tenant default (24 hours)

10 minutes

1 hour

6 hours

24 hours

제

9 ,

장

:

- Security Cloud Control□ □□ □□
- □□ □□ □□□ □□
- □□ □□ □□
- □□ □□ □□□□
- Security Cloud Control□□ □□ □□□□
□
- Security Cloud Control□□ □□□□□□
□□□□

네트워크 보안 태세를 이해하기 위해 구성 변경, 대량 디바이스 작업 및 디바이스 통신 프로세스를 추적하기 위해 변경 로그, 워크플로우, 작업을 모니터링하고 보고하는 방법을 설명합니다.

Security Cloud Control는 구성 변경 로그, 대량 디바이스 작업, 디바이스와 통신할 때 실행되는 프로세스를 효과적으로 모니터링합니다. 이를 통해 네트워크의 기존 정책이 보안 상태에 어떤 영향을 미치는지 파악할 수 있습니다.

Security Cloud Control

Security Cloud Control의 변경 로그를 사용하여 구성 변경을 검토하고, 누가 언제 변경했는지 추적하고, 충돌 항목을 식별하고, 차이점을 비교하고, 문제 해결 또는 보고를 위해 로그 데이터를 내보내는 방법을 설명합니다.

변경 로그는

- Security Cloud Control에서 수행한 구성 변경 사항을 캡처하여 지원되는 모든 디바이스 및 서비스의 변경 사항을 포함하는 단일 보기를 제공하고,
- 디바이스 구성 변경 사항을 나란히 비교하여 제공하며,
- 디바이스의 온보딩 및 제거를 기록하고,
- Security Cloud Control 외부에서 발생하는 정책 변경 충돌을 탐지합니다.

변경 로그는 설정 관리 및 문제 해결을 위해 다음과 같은 기능을 제공합니다.

- 모든 변경 로그 항목에 대한 레이블을 제공합니다.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.
- 전체 변경 로그 또는 일부만 CSV 파일로 다운로드할 수 있습니다.



주

클라우드 제공 Firewall Management Center에서 변경한 사항은 변경 로그에 반영되지 않습니다.

Change log capacity(변경 로그 용량): Security Cloud Control는 변경 로그 정보를 1년 동안 보관하고 1년이 지난 데이터는 삭제합니다.

Security Cloud Control의 데이터베이스에 저장된 변경 로그 정보와 내보낸 변경 로그에 표시되는 변경 로그 정보에는 차이가 있습니다. 자세한 내용은 [변경 로그 내보내기](#) 페이지 130를 참조하십시오.

Change log entries(변경 로그 항목): 변경 로그 항목은 단일 디바이스 구성의 변경 사항, 디바이스에서 수행된 작업 또는 Security Cloud Control 외부에서 디바이스에 이루어진 변경 사항을 반영합니다:

- 구성 변경 내용이 포함된 변경 로그 항목의 경우 해당 행의 아무 곳이나 클릭하여 변경 내용에 대한 세부 정보를 볼 수 있습니다.
- Security Cloud Control 외부에서 이루어진 대역 외 변경이 충돌로 감지되는 경우 시스템 사용자가 마지막 사용자로 보고됩니다.
- Security Cloud Control의 디바이스 구성이 디바이스의 구성과 동기화된 후 또는 디바이스가 Security Cloud Control에서 제거되면 Security Cloud Control는 변경 로그 항목을 닫습니다. 구성은 디바이스에서 Security Cloud Control로 구성을 읽거나 Security Cloud Control에서 디바이스로 구성을 구축한 후에 동기화된 것으로 간주됩니다.
- Security Cloud Control는 변경의 성공 여부와 관계없이 기존 항목을 완료한 후 즉시 새 변경 로그 항목을 만듭니다. 새 변경 로그 항목이 열리면 추가 구성 변경 사항이 추가됩니다.
- 디바이스에 대한 읽기, 구축 및 삭제 작업에 대한 이벤트가 표시됩니다. 이러한 작업은 디바이스의 변경 로그를 닫습니다.

- (읽기 또는 구축을 통해) **Security Cloud Control**가 디바이스의 구성과 동기화된 후에 또는 **Security Cloud Control**가 더 이상 디바이스를 관리하지 않는 경우 변경 로그가 닫힙니다.
- **Security Cloud Control** 외부에서 디바이스를 변경하면 변경 로그에 "충돌 감지됨" 항목이 포함됩니다.

Pending and completed change log entries(보류 중 및 완료된 변경 로그 항목): 변경 로그의 상태는 **Pending**(보류 중) 또는 **Completed**(완료됨)입니다. **Security Cloud Control**를 사용하여 디바이스의 구성을 변경하면 이러한 변경 사항은 보류 중인 변경 로그 항목에 기록됩니다. 보류 중인 변경 로그를 완료한 활동:

- 디바이스에서 **Security Cloud Control**로 구성을 읽기
- **Security Cloud Control**에서 디바이스로 변경 사항 구축
- **Security Cloud Control**에서 디바이스 삭제
- 실행 중인 구성 파일을 업데이트하는 CLI 명령 실행

Search and filter change log entries(변경 로그 항목 검색 및 필터링): 변경 로그 항목을 검색하고 필터링할 수 있습니다. 검색 필드를 사용하여 이벤트를 찾습니다. 필터()를 사용하여 지정한 기준에 맞는 항목을 찾습니다. 변경 로그를 필터링하고 검색 필드에 키워드를 추가하여 필터링된 결과 내에서 항목을 찾는 방식으로 두 작업을 결합할 수도 있습니다.

변경 로그에서 디바이스 구성 변경 사항에 대한 추가, 수정, 삭제 및 메시지 항목을 검토하려면 나란히 비교 보기를 구성합니다.

변경 로그 차이를 보고 실행 중인 구성 파일의 이전 및 이후 상태를 검사하여 디바이스에 대한 구성 변경 사항을 분석합니다.

변경 로그 차이는 원본 설정 파일과 수정된 구성 파일을 자세히 비교하여 디바이스 구성에 어떤 변경 사항이 있는지 이해하는 데 도움이 됩니다. 나란히 보기에는 실행 중인 구성에서 추가, 수정 및 삭제된 항목이 강조 표시됩니다.

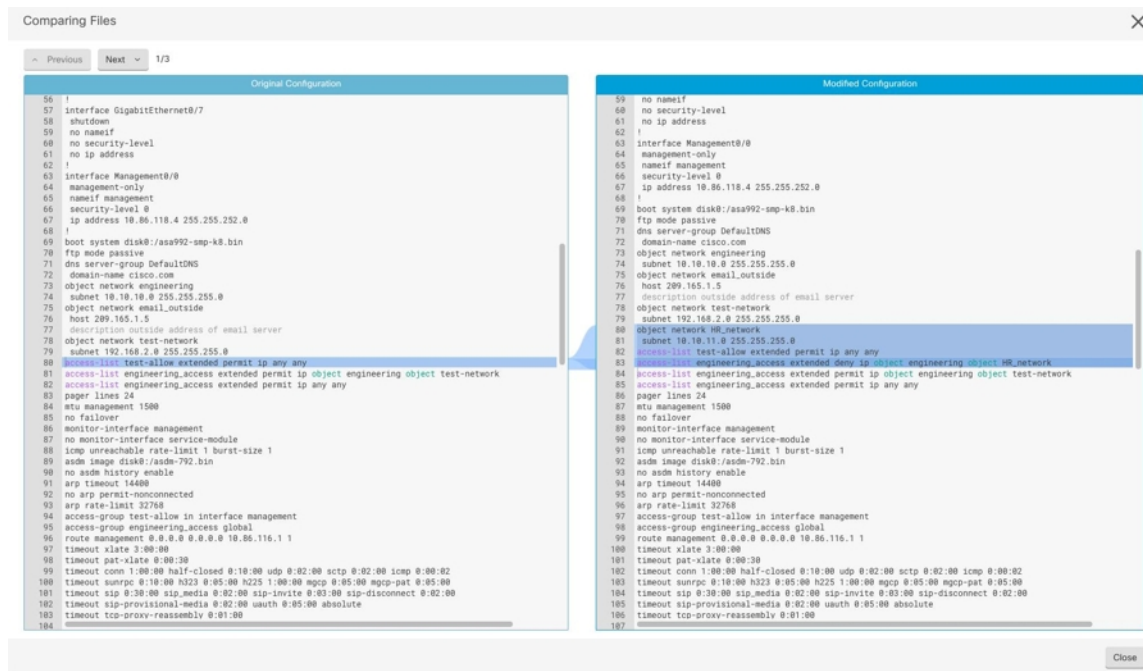
1. 변경 로그에서 **Diff**를 클릭합니다.

디바이스의 실행 구성 파일 변경 사항을 나란히 비교하는 화면이 열립니다.

Original Configuration(원래 구성) 열에는 ASA 디바이스에 변경 사항을 기록하기 전의 실행 구성 파일이 표시됩니다. **Modified Configuration**(수정된 구성) 열에는 변경 사항이 작성된 후 실행 중인 구성 파일이 표시됩니다.

2. 변경 사항을 확인하려면 왼쪽에서 오른쪽 열까지의 선을 따라 이동합니다.

비교 보기에서 **HR_network** 개체, 그리고 엔지니어링 네트워크의 주소가 **HR_network** 네트워크의 주소에 도달하지 못하도록 하는 액세스 규칙 등의 추가 사항을 확인할 수 있습니다. **Original Configuration**(원본 구성) 열은 **Modified Configuration**(수정된 구성) 열의 변경 사항을 이해하기 위한 참조 포인트를 제공하는 행을 강조 표시합니다.



3. **Previous**(이전) 및 **Next**(다음)를 클릭하여 파일의 변경 사항으로 이동합니다.

원래 디바이스 구성과 수정된 디바이스 구성의 구성 차이점을 보고 분석하여 구성 업데이트 프로세스 중에 변경된 사항을 정확하게 파악할 수 있습니다.

변경 요청 관리로 인해 어떻게 비즈니스 근거를 서드파티 티켓팅 시스템을 통해 변경 로그 이벤트에 연결할 수 있는지 설명합니다.

변경 요청 관리

- **Change Request**(변경 요청) 및 해당 비즈니스 근거를 **Change Log**(변경 로그) 이벤트에 연결할 수 있도록 하고,
- 서드파티 티켓팅 시스템에서 **Change Request**(변경 요청)을 열며,
- **Security Cloud Control**에서 변경 요청을 생성하여 이를 변경 로그 이벤트와 연계할 수 있게 해주는 기능입니다.

Change Request Management(변경 요청 관리)를 사용하여 **Security Cloud Control**에서 **Change Request**(변경 요청)을 생성하고 변경 로그 이벤트와 연결합니다. 변경 로그 내에서 이름으로 이 변경 요청을 검색할 수 있습니다.



Security Cloud Control에서 변경 요청 추적과 변경 요청 관리는 동일한 기능을 의미합니다.

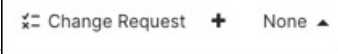
변경 요청 추적을 구성하여 조직 전체의 구성 변경 사항을 모니터링하고 관리합니다.

변경 요청 추적을 활성화하여 조직의 모든 사용자가 수행한 구성 변경 사항에 대한 가시성과 제어를 제공합니다.

변경 요청 추적을 활성화하면 조직의 모든 사용자에게 영향을 미칩니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.

3. **Change Request Tracking(변경 요청 추적)** 토글 버튼 활성화



이 기능을 활성화하면 변경 요청 메뉴가 왼쪽 하단에 나타나고 변경 로그 페이지에서 변경 요청 드롭다운 목록을 사용할 수 있습니다.

이제 조직에 대해 변경 요청 추적이 활성화되었습니다. **Change Request(변경 요청)** 메뉴는 왼쪽 하단에 있으며, **Change Request(변경 요청)** 드롭다운 목록은 **Change Log(변경 로그)** 페이지에 나타납니다.

조직 내 디바이스 구성 변경 사항을 추적하고 관리하기 위해 변경 요청을 구성합니다.

변경 요청을 생성하여 네트워크의 디바이스에 적용될 구성 변경 사항을 구성하고 추적하여 적절한 문서화를 수행하고 수정 사항을 감독할 수 있습니다.

변경 요청은 관련 구성 변경 사항을 그룹화하고 수정 사항에 대한 감사 추적을 유지 관리하는 구조화된 방법을 제공합니다. 생성된 이후의 모든 변경 사항은 지워지거나 비활성화될 때까지 활성 변경 요청에 연결됩니다.

1. Security Cloud Control에서 왼쪽 하단의 **Change Request (변경 요청)** 메뉴에서 변경 요청 생성(+) 아이콘을 클릭합니다.
2. **Name(이름)** 및 **Description(설명)**을 입력합니다.

Name(이름)이 조직에서 사용하려는 **Change Request(변경 요청)** 이름과 일치하는지, **Description(설명)**에 변경의 목적이 설명되어 있는지 확인합니다.



Change Request(변경 요청)을 생성한 후에는 이름을 변경할 수 없습니다.

3. **Save(저장)**를 클릭합니다.



Change Request(변경 요청)이 저장되면 **Security Cloud Control**은 모든 새 변경 사항을 해당 **Change Request(변경 요청)** 이름에 연결합니다. 이 연결은 **변경 요청을 비활성화**하거나 메뉴에서 **변경 요청 세부 정보를 지울** 때까지 계속됩니다.

변경 요청이 생성되어 활성 변경 요청이 됩니다. 변경 요청 관리를 비활성화하거나 변경 요청 세부 정보를 지울 때까지 모든 후속 구성 변경 사항은 이 변경 요청과 연결됩니다.

변경 요청과 변경 로그 이벤트 간의 연결을 구성하여 구성 변경을 추적합니다.

변경 요청을 변경 로그 이벤트와 연결하여 감사 추적을 유지하고 구성 변경 이유를 추적합니다.

구성 변경에 대한 권한 부여 및 이론적 근거를 문서화하기 위해 변경 요청을 특정 변경 로그 이벤트에 연결해야 하는 경우 이 절차를 사용합니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 를 클릭합니다 **Events & Logs(이벤트 및 로그) > Logs(로그) > Change Log(변경 로그)**.
3. 변경 로그를 확장하여 변경 요청과 연결하려는 이벤트를 확인합니다.
4. 해당 변경 로그 항목 옆에 있는 드롭다운 목록을 클릭합니다.



최신 변경 요청은 변경 요청 목록 상단에 표시됩니다.

5. 변경 요청을 선택하고 **Select(선택)**을 클릭합니다.

이제 변경 요청이 변경 로그 이벤트와 연결되어 권한 부여와 구성 변경 간에 추적 가능한 링크를 생성합니다.

시스템에서 특정 변경 요청과 관련된 변경 로그 이벤트를 찾으려면 검색 매개변수를 구성합니다.

이 작업은 관련 변경 요청 이름을 검색하여 특정 변경 로그 이벤트를 찾는 데 도움이 되며, 변경 사항 및 해당 설명서를 추적할 수 있습니다.

감사, 추적 또는 분석 목적으로 특정 변경 요청과 연결된 변경 로그 이벤트를 찾아야 할 경우 이 절차를 사용합니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Events & Logs(이벤트 및 로그) > Logs(로그) > Change Log(변경 로그)**.
3. 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 이름을 입력합니다.

Security Cloud Control는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

시스템은 검색 기준과 일치하는 변경 로그 이벤트를 표시하며, 쉽게 식별 수 있도록 정확한 일치가 강조 표시됩니다.

변경 요청 시스템에서 이름 또는 키워드로 변경 요청을 찾으도록 검색을 구성합니다.

사용자가 부분 일치 항목을 사용해 이름과 설명을 통해 검색하여 기존 변경 요청을 신속하게 찾을 수 있습니다. 시스템의 여러 항목 중에서 특정 변경 요청을 찾아야 할 경우 이 검색 기능을 사용합니다.

1. **Security Cloud Control**에서 왼쪽 하단의 **Change Request(변경 요청)** 메뉴에서 변경 요청 생성(+) 아이콘을 클릭합니다.
2. 검색 필드에 **Change Request(변경 요청)**의 이름 또는 관련 키워드를 입력합니다. 값을 입력하면 입력한 내용과 부분적으로 일치하는 결과가 이름 및 설명 필드에 모두 표시됩니다.

시스템은 이름 및 설명 필드 모두에서 검색 기준과 일치하는 변경 요청을 표시하므로, 원하는 변경 요청을 신속하게 찾을 수 있습니다.

변경 로그 테이블에서 특정 변경 요청을 검색하고 확인하도록 필터를 구성합니다.

변경 요청을 필터링하여 보안 환경에서 특정 구성 변경 사항 또는 이벤트를 신속하게 찾고 검토합니다.

변경 로그의 필터 기능을 사용하여 특정 기준에 따라 변경 요청 목록을 좁힐 수 있습니다. 이렇게 하면 디바이스 전체의 구성 변경 사항을 효율적으로 검토하고 관리하는 데 도움이 됩니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Events & Logs(이벤트 및 로그) > Logs(로그) > Change Log(변경 로그)**.
3. 모든 옵션을 보려면 필터 아이콘을 클릭합니다.
4. 검색 필드에 **Change Request(변경 요청)**의 이름을 입력합니다.

값을 입력하면 입력한 값과 부분적으로 일치하는 결과가 표시됩니다.

5. 해당 체크 박스 을 선택 하여 변경 요청 을 선택합니다.

일치하는 항목은 **Change Log(변경 로그)** 테이블에 표시됩니다. **Security Cloud Control**는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

변경 로그 테이블에는 검색 기준과 일치하는 필터링된 변경 요청만 표시되며, 쉽게 식별할 수 있도록 정확한 일치가 강조 표시됩니다.

변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 변경 요청 도구 모음을 구성합니다.

변경 요청 도구 모음을 지우면 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않습니다.

변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 하려면 변경 요청 도구 모음에서 정보를 지우십시오.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 하단의 변경 요청 메뉴에서 변경 요청 생성(+) 아이콘을 클릭합니다.
3. **Clear(지우기)**를 클릭합니다.

이제 변경 요청 메뉴에 **None(없음)**이 표시됩니다.

변경 요청 도구 모음이 지워지고 **None(없음)**이 표시되어 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않습니다.

이러한 항목 간의 원치 않는 연결을 제거하기 위해 변경 로그 이벤트에서 변경 요청 연결 해제를 구성합니다.

이 작업을 사용하면 연결이 더 이상 필요하지 않거나 오류로 인해 생성된 경우 변경 요청과 변경 로그 이벤트 간의 연결을 제거할 수 있습니다.

변경 로그 인터페이스의 변경 로그 이벤트에서 변경 요청의 연결을 해제해야 하는 경우 이 절차를 사용합니다. 이렇게 하면 변경 사항을 정확한 추적 및 구성을 유지하는 데 도움이 됩니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Events & Logs(이벤트 및 로그) > Logs(로그) > Change Log(변경 로그)**를 클릭합니다.
3. 변경 로그를 확장하여 변경 요청에서 연결 해제하려는 이벤트를 표시합니다.
4. 해당 변경 로그 항목 옆에 있는 드롭다운 목록을 클릭합니다.
5. **Clear(지우기)**를 클릭합니다.

변경 요청과 선택한 변경 로그 이벤트의 연결이 성공적으로 해제되고, 둘 간의 연결이 제거됩니다.

변경 로그에는 유지하면서 변경 요청 목록에서 해당 항목을 제거하려면 변경 요청 삭제를 구성합니다.

더 이상 필요하지 않은 변경 요청을 삭제하여 활성 변경 요청 목록에서 제거합니다.

변경 요청을 삭제하면 변경 요청 목록에서는 삭제되지만 변경 로그에서는 삭제되지 않습니다.

1. 왼쪽 하단의 변경 요청 메뉴에서 변경 요청 생성(+) 아이콘을 클릭합니다.
2. 변경 요청 을 선택하고 저장소 아이콘을 클릭하여 삭제합니다.
3. 확인 표시를 클릭하여 확인합니다.

변경 요청은 변경 요청 목록에서 제거되지만 기록 참조를 위해 변경 로그에서 계속 사용할 수 있습니다.

Change Request Management(변경 요청 관리) 또는 **Change Request Tracking(변경 요청 추적)** 기능을 비활성화하도록 계정을 구성합니다.

이 작업은 더 이상 필요하지 않거나 바람직하지 않은 경우 계정에 대한 변경 요청 관리 기능을 비활성화합니다.

Change Request Management(변경 요청 관리)를 비활성화하거나 **Change Request Tracking(변경 요청 추적)**을 비활성화하면 어카운트의 모든 사용자에게 영향을 미칩니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > General Settings(일반 설정)**를 선택합니다.
3. **Change Request Tracking(변경 요청 추적)** 토글 버튼 비활성화

어카운트의 모든 사용자에게 **Change Request Management(변경 요청 관리)** 및 **Change Request Tracking(변경 요청 추적)** 기능이 비활성화됩니다.

방화벽 디바이스에 대한 변경 사항을 추적하고 외부 티켓 또는 변경 요청과 연결하도록 변경 요청 관리를 구성합니다.

이 작업은 방화벽 디바이스에 대한 변경 사항을 추적하고 외부 시스템에서 유지 관리되는 티켓을 해결하기 위한 변경 요청과 연결하는 데 도움이 됩니다. 변경 요청을 생성하고, 변경 로그 이벤트를 요청에 연결하고, 특정 변경 요청과 관련된 이벤트를 검색할 수 있습니다.

이 사용 사례에서는 변경 요청 관리를 활성화했다고 가정합니다. 다양한 시나리오에서 변경 요청 관리를 사용하여 감사 추적을 유지하고 방화벽 변경 사항을 외부 티켓팅 시스템과 연결할 수 있습니다.

1. 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽 디바이스에 적용된 변경 사항을 추적

이 활용 사례에서는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽 디바이스를 변경하고 이러한 방화벽 변경에서 발생하는 변경 로그 이벤트를 변경 요청에 연결하려는 시나리오에 대해 설명합니다.

 - a. **변경 요청 생성** 페이지 125.
 - b. 외부 시스템의 티켓 이름이나 번호를 변경 요청의 이름으로 사용하고 설명 필드에 변경의 정당성 및 기타 관련 정보를 추가합니다.

- c. 변경 요청 도구 모음에 새 변경 요청이 표시되는지 확인합니다.
- d. 방화벽 디바이스를 변경합니다.
- e. 탐색창에서 변경 로그를 클릭하고 새 변경 요청과 연결된 변경 로그 이벤트를 찾습니다.
- f. 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 하기 위한 [변경 요청 도구 모음 지우기](#) 페이지 128.

2. 방화벽 디바이스 변경 후 개별 변경 로그 이벤트 수동 업데이트

이 사용 사례에서는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽 디바이스를 변경했지만 변경 요청 관리 기능을 사용하여 변경 요청을 변경 로그 이벤트와 연결하는 것을 잊어버린 시나리오를 설명합니다. 티켓 번호로 변경 로그 이벤트를 업데이트하려고 합니다.

- a. [변경 요청 생성](#) 페이지 125. 외부 시스템의 티켓 이름 또는 번호를 변경 요청 이름으로 사용합니다. 설명 필드를 사용하여 변경 및 기타 관련 정보에 대한 근거를 추가합니다.
- b. 탐색창에서 **Change Log(로그 변경)**를 클릭하고 변경 사항과 관련된 변경 로그 이벤트를 검색합니다.
- c. [변경 요청을 변경 로그 이벤트와 연결](#) 페이지 126.
- d. 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 하기 위한 [변경 요청 도구 모음 지우기](#) 페이지 128.

3. 변경 요청과 관련된 변경 로그 이벤트 검색

이 사용 사례에서는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 수행한 작업으로 인해 변경 로그에 어떤 변경 로그 이벤트가 기록되었는지 확인하려는 시나리오를 설명합니다.

- a. 탐색창에서 **Change Log(변경 로그)**를 클릭합니다.
- b. 다음 방법 중 하나를 사용하여 변경 요청과 관련된 변경 로그 이벤트를 검색합니다:
 - 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 정확한 이름을 입력합니다. **Security Cloud Control**는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.
 - 변경 로그 이벤트를 찾기 위한 [변경 요청 필터링](#) 페이지 127
- c. 관련된 변경 요청을 보여주는 강조 표시된 변경 로그 이벤트를 찾으려면 각 변경 로그를 봅니다.

변경 요청을 성공적으로 관리하고 변경 로그 이벤트를 외부 티켓과 연결했습니다. 이제 변경 로그에는 변경 요청과 연결된 추적 가능한 이벤트가 포함되므로 방화벽 수정에 대한 감사 추적을 제공합니다.

보고 또는 분석을 위해 변경 레코드를 필터링, 정렬 및 유지할 수 있도록 모든 또는 선택한 변경 로그 데이터의 CSV 파일 내보내기를 구성합니다.

변경 로그 데이터를 쉼표로 구분된 값(.CSV) 파일로 내보내 시스템 외부의 변경 기록 필터링, 정렬 및 분석을 활성화합니다.

Security Cloud Control 변경 로그 전체 또는 하위 집합을 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다.

변경 로그를 .csv 파일로 내보내려면 다음 절차를 수행합니다:

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Events & Logs**(이벤트 및 로그) > **Logs**(로그) > **Change Log**(변경 로그)를 클릭합니다.
3. 다음 작업 중 하나를 수행하여 내보낼 변경 사항을 찾습니다.

- 필터() 및 검색 필드를 사용하여 내보낼 항목을 찾습니다. 예를 들어 디바이스를 기준으로 필터링하면 선택한 디바이스에 대한 변경 사항만 표시됩니다.
- 변경 로그에서 모든 필터 및 검색 기준을 지웁니다. 이렇게 하면 전체 변경 로그를 내보낼 수 있습니다.



Security Cloud Control은 1년간의 변경 로그 데이터를 보관합니다. 1년 동안의 전체 변경 로그 기록을 다운로드하는 것보다 변경 로그 내용을 필터링하여 그 결과를 .csv 파일로 다운로드하는 것이 좋습니다.

4. 페이지 오른쪽 상단에 있는 내보내기  아이콘을 클릭합니다.
5. .csv 파일을 설명이 포함된 이름과 함께 로컬 파일 시스템에 저장합니다.

변경 로그 데이터는 로컬 시스템에서 CSV 파일로 내보내지며, 필요에 따라 추가 필터링, 정렬 및 분석을 수행할 수 있습니다.

Security Cloud Control

Security Cloud Control가 데이터베이스에 저장하는 변경 로그 정보와 내보낸 변경 로그에 포함된 정보 간의 차이점에 대해 설명합니다.

변경 로그 용량 차이

- Security Cloud Control 데이터베이스에 저장된 전체 변경 로그 정보와 내보낸 파일에 포함된 정보의 일부를 구분하는 데이터 저장 방식의 차이입니다.
- 이는 데이터베이스 운영과 내보내기 기능에 대한 서로 다른 저장 요구 사항에서 비롯되며,
- 사용자가 변경 로그 데이터를 내보낼 때 파일 크기에 영향을 미칩니다.

모든 변경 로그에 대해 Security Cloud Control은 두 개의 디바이스 구성 사본을 저장합니다. 하나는 시작 구성이고, 다른 하나는 닫힌 변경 로그의 경우 종료 구성 또는 열린 변경 로그의 경우 현재 구성입니다. 이를 통해 Security Cloud Control은 구성 차이를 나란히 표시할 수 있습니다. 또한 Security Cloud Control은 변경한 사용자 이름, 변경한 시간 및 기타 세부 정보와 함께 모든 단계(변경 이벤트)를 추적하고 저장합니다.

그러나 변경 로그를 내보낼 때 구성의 전체 사본 두 개가 내보내기에 포함되지 않습니다. 두 여기에는 내보내기 파일이 변경 로그 Security Cloud Control가 저장하는 것보다 훨씬 작은 변경 이벤트만 포함됩니다.

Security Cloud Control은 변경 로그 정보를 1년 동안 저장합니다. 여기에는 두 개의 구성 사본이 포함됩니다.

Security Cloud Control

Security Cloud Control에서 대량 작업을 모니터링하고, 작업 진행 상황 및 디바이스 수준 결과를 검토하고, 작업, 사용자 또는 상태별로 작업을 검색하거나 필터링하고, 대량 작업을 다시 시작하거나 취소하는 방법을 설명합니다.

Security Cloud Control의 작업 모니터링은

- 여러 디바이스 다시 연결, 여러 디바이스에서 구성 읽기, 여러 디바이스 동시 업그레이드 등 대량 작업의 진행 상황에 대한 개요를 제공하고,
- 개별 작업의 상태와 함께 색상으로 구분된 행을 사용하여 성공 또는 실패 여부를 나타내며,
- 행을 확장하면 대량 작업의 영향을 받는 각 디바이스의 결과를 표시합니다.

Jobs(작업) 페이지는 다음과 같은 두 가지 방법으로 액세스할 수 있습니다.

- 새 작업 알림이 있을 때 **Notifications(알림)** 탭에서 **Review(검토)** 링크를 클릭합니다. **Jobs(작업)** 페이지로 리디렉션되고 해당 알림이 나타내는 특정 작업이 표시됩니다.
- 왼쪽 창에서 을 클릭합니다 **Monitor(모니터링)** > **Events heading(이벤트 제목)** > **Jobs(작업)**. 이 표에는 Security Cloud Control에서 수행되는 대량 작업의 전체 목록이 나와 있습니다.

테이블의 한 행은 단일 대량 작업을 나타냅니다. 예를 들어 1개의 대량 작업이 20개의 디바이스를 다시 연결하려는 시도일 수 있습니다. **Jobs(작업)** 페이지에서 행을 확장하면 대량 작업의 영향을 받는 각 디바이스에 대한 결과가 표시됩니다.

The screenshot displays the 'Jobs' page in Security Cloud Control. At the top, there is a search bar labeled 'Search for jobs by action'. Below it is a table with columns: Action, Status, User, Start, End, and Scheduled. The table lists several jobs, including 'Execute CLI Command', 'Deploy Changes', and 'Toggle Conflict Detection'. The 'Toggle Conflict Detection' job is highlighted in blue. Below the table, there is a section titled 'View Jobs' showing details for a job named 'Reconnecting...'. This section includes a status bar with icons for success, failure, and warnings, and a 'Review' link. A callout box explains that the notifications tab displays status information about the job, including the number of actions in the job (20), actions being processed (13), number of actions failed (1), number of warnings (0), and number of actions succeeded (6).

Jobs(작업) 페이지에서 다양한 작업, 작업을 수행한 사용자 및 작업 상태를 기준으로 필터링하고 검색할 수 있습니다.

이전에 실행한 대량 작업에서 실패한 작업을 해결하기 위해 대량 작업 재시도를 구성합니다.

이 작업을 통해 전체 작업을 다시 실행하지 않고도 대량 작업 내에서 실패한 작업을 다시 시도할 수 있습니다.

Jobs(작업) 페이지를 검토한 후 대량 작업에서 하나 이상의 작업이 실패한 것을 발견하면 필요한 수정을 한 후 대량 작업을 다시 시도할 수 있습니다. **Security Cloud Control**는 실패한 작업에 대해서만 작업을 다시 실행합니다.

1. **Jobs(작업)** 페이지에서 실패한 작업을 나타내는 행을 선택합니다.
2. **Retry(재시도)**() 아이콘을 클릭합니다.

시스템은 원래 대량 작업에서 실패한 작업만 재시도하며, 그에 따라 작업 상태가 업데이트됩니다.

여러 디바이스에서 현재 진행 중인 대량 작업의 취소를 구성합니다.

예상보다 오래 걸리거나 더 이상 필요하지 않은 여러 디바이스에서 진행 중인 작업을 중지해야 하는 경우 현재 진행 중인 대량 작업을 취소합니다.

여러 디바이스에서 현재 진행 중인 대량 작업을 취소할 수 있습니다. 예를 들어 매니지드 디바이스 4개를 재연결하려고 시도했는데 그 중 3개가 성공적으로 재연결되었지만 네 번째 디바이스가 여전히 연결되지 않거나 연결이 끊어진 경우 대량 작업을 취소할 수 있습니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 을 클릭합니다 **Monitor(모니터링) > Events heading(이벤트 제목) > Jobs(작업)**.
3. 실행 중인 대량 작업을 식별하고 오른쪽의 **Cancel(취소)** 링크를 클릭합니다.



대량 작업의 일부가 성공하면 취소할 수 없습니다. 진행 중인 모든 작업이 취소됩니다.

대량 작업이 취소되어, 진행 중인 작업이 중지되며 성공적으로 완료된 작업 부분은 유지됩니다.

Security Cloud Control

Security Cloud Control 워크플로우를 모니터링하고, 실패한 디바이스 또는 커넥터 작업의 문제 해결, **TAC** 분석을 위해 워크플로우 세부 정보를 내보내고, 해결되지 않은 오류에 대해 스택 추적을 복사하는 방법을 설명합니다.

워크플로우 모니터링은 **Security Cloud Control** 기능으로,

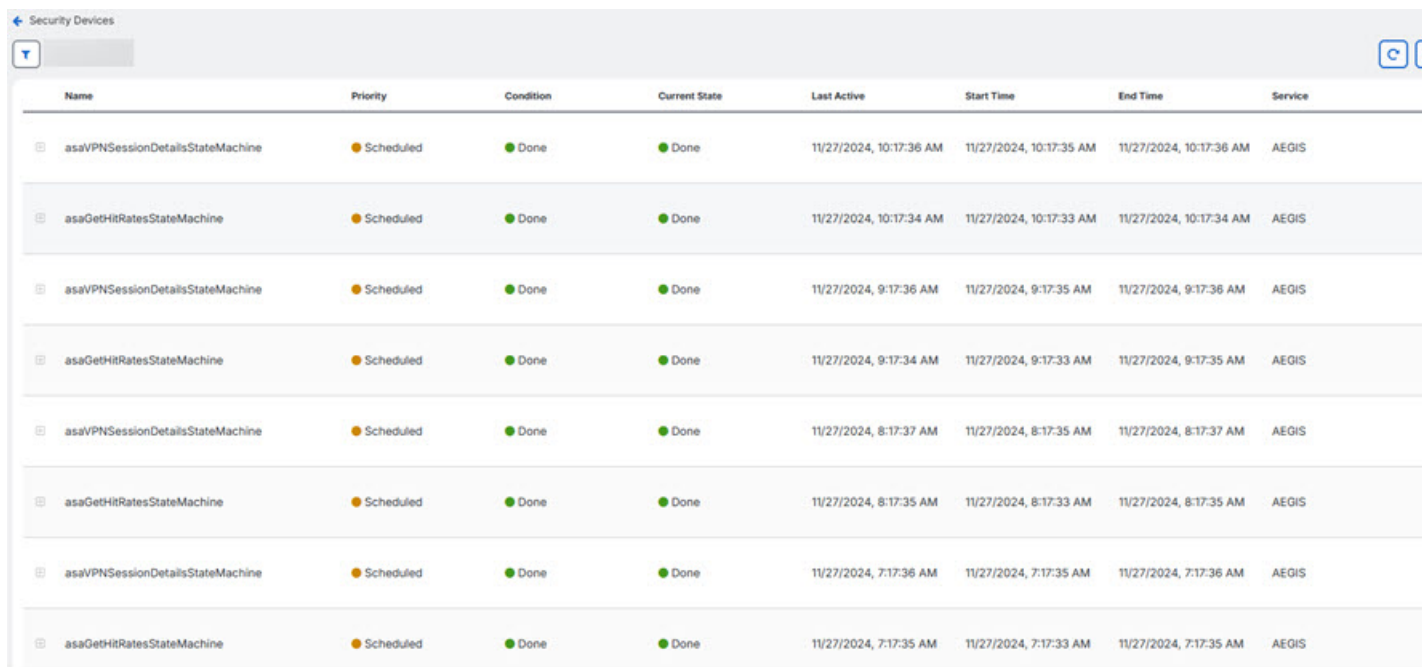
- 디바이스, **SDC(Secure Device Connector)** 또는 **SEC(Secure Event Connector)**와 통신할 때와 디바이스에 규칙 세트 변경 사항을 적용할 때 **Security Cloud Control**이 실행하는 모든 프로세스를 추적하고,
- 모든 단계에 대해 워크플로우 테이블에 항목을 생성하고 그 결과를 표시하며,
- 상호 작용하는 디바이스가 아니라 **Security Cloud Control**가 수행한 작업과 관련된 정보만 포함합니다.

Security Cloud Control는 디바이스에서 작업을 수행하지 못할 때 오류를 보고합니다. 워크플로우 페이지로 이동하여 오류가 발생한 단계를 확인하여 자세한 내용을 확인하십시오.

또한 이 페이지에서는 오류를 확인 및 해결하거나 필요한 경우 TAC와 정보를 공유할 수 있습니다.

Workflows(워크플로우) 페이지로 이동하려면, 왼쪽 창의 **Security Devices(보안 디바이스)**를 클릭하고, **Devices(디바이스)** 탭을 클릭합니다. 적절한 디바이스 유형 탭을 클릭하여 디바이스를 찾고 원하는 디바이스를 선택합니다. 오른쪽 창의 **Devices and Actions(디바이스 및 작업)**에서 **Workflows(워크플로우)**를 클릭합니다.

1: Workflows()



Name	Priority	Condition	Current State	Last Active	Start Time	End Time	Service
asaVPNSessionDetailsStateMachine	Scheduled	Done	Done	11/27/2024, 10:17:36 AM	11/27/2024, 10:17:35 AM	11/27/2024, 10:17:36 AM	AEGIS
asaGetHitRatesStateMachine	Scheduled	Done	Done	11/27/2024, 10:17:34 AM	11/27/2024, 10:17:33 AM	11/27/2024, 10:17:34 AM	AEGIS
asaVPNSessionDetailsStateMachine	Scheduled	Done	Done	11/27/2024, 9:17:36 AM	11/27/2024, 9:17:35 AM	11/27/2024, 9:17:36 AM	AEGIS
asaGetHitRatesStateMachine	Scheduled	Done	Done	11/27/2024, 9:17:34 AM	11/27/2024, 9:17:33 AM	11/27/2024, 9:17:35 AM	AEGIS
asaVPNSessionDetailsStateMachine	Scheduled	Done	Done	11/27/2024, 8:17:37 AM	11/27/2024, 8:17:35 AM	11/27/2024, 8:17:37 AM	AEGIS
asaGetHitRatesStateMachine	Scheduled	Done	Done	11/27/2024, 8:17:35 AM	11/27/2024, 8:17:33 AM	11/27/2024, 8:17:35 AM	AEGIS
asaVPNSessionDetailsStateMachine	Scheduled	Done	Done	11/27/2024, 7:17:36 AM	11/27/2024, 7:17:35 AM	11/27/2024, 7:17:36 AM	AEGIS
asaGetHitRatesStateMachine	Scheduled	Done	Done	11/27/2024, 7:17:35 AM	11/27/2024, 7:17:33 AM	11/27/2024, 7:17:35 AM	AEGIS

디바이스 워크플로우 내보내기:

- 전체 워크플로우 정보를 JSON 파일로 다운로드하고 TAC 팀에서 추가 분석을 요청할 때 제공할 수 있습니다. 워크플로우 정보를 내보내려면 해당 디바이스를 선택하고 해당 워크플로우 페이지로 이동하여 오른쪽 상단에 나타나는 내보내기(📄) 아이콘을 클릭합니다.

스택 추적 복사:

- 해결할 수 없는 오류가 발생하여 TAC에 문의하면 스택 추적 사본을 요청할 수 있습니다. 오류에 대한 스택 추적을 수집하려면 **Stack Trace(스택 추적)** 링크를 클릭하고 **Copy Stacktrace(스택 추적 복사)**를 클릭하여 화면에 나타나는 스택을 클립보드로 복사합니다.

제

10 Terraform

장

:

- [Terraform](#) □□

이 장에서는 Security Cloud Control 설정 및 관리 방법에 대해 설명합니다.

Terraform

Security Cloud Control Terraform 제공자 및 모듈을 사용하여 사용자를 관리하고, 방화벽 디바이스를 온보딩하고, 보안 디바이스 및 이벤트 커넥터를 구축하고, 반복 가능한 버전 제어 인프라 구성을 유지 관리하는 방법을 알아봅니다.

Security Cloud Control 고객은 [Security Cloud Control Terraform 제공자](#) 및 Security Cloud Control Terraform 모듈을 통해 반복 가능하고 버전 제어되는 코드로 테넌트를 신속하게 설정할 수 있습니다. Security Cloud Control Terraform 제공자를 통해 사용자는 다음을 수행할 수 있습니다.

- 사용자 관리
- 클라우드 제공 Firewall Management Center의 Secure Firewall Threat Defense 디바이스, Cisco Secure ASA 디바이스 및 iOS 디바이스 온보딩
- vSphere 및 AWS에 보안 디바이스 커넥터 온보딩
- AWS의 보안 이벤트 커넥터 온보딩

자세한 정보는 다음 페이지를 참조하십시오.

- [Security Cloud Control Terraform 제공자 페이지](#)
- [vSphere 모듈 페이지의 Security Cloud Control SDC](#)
- [AWS 모듈 페이지의 Security Cloud Control SDC](#)
- [AWS 모듈 페이지의 Security Cloud Control SEC](#)
- [Devnet 학습 랩을 통한 작업](#)
- [Security Cloud Control Terraform 제공자를 사용하여 보안 인프라 관리 자동화 - 학습 랩](#)
- [GitHub의 Security Cloud Control 자동화 예시](#)

Security Cloud Control Terraform 제공자 및 모듈은 Apache 2.0 라이선스에 따라 오픈 소스 소프트웨어로 게시됩니다. 지원이 필요한 경우 아래 저장소의 [GitHub](#)에서 문제를 제출하십시오.

모듈	리포지토리
Security Cloud Control Terraform 제공자	https://github.com/cisco/devnet/terraform-provider-Security-Cloud-Control
Security Cloud Control SDC 모듈(vSphere)	https://github.com/CiscoDevNet/terraform-vsphere-Security-Cloud-Control-sdc
Security Cloud Control SDC 모듈 (AWS)	https://github.com/CiscoDevNet/terraform-aws-Security-Cloud-Control-sdc
Security Cloud Control SEC 모듈(AWS)	https://github.com/CiscoDevNet/terraform-aws-Security-Cloud-Control-sec

Security Cloud Control 팀은 위의 저장소에 대한 기여를 환영합니다. 제공자 및 모듈 개선에 참여하려면 이 [GitHub 리포지토리](#)에서 풀 요청을 생성합니다.

- Terraform을 사용하여 vSphere에 SDC 구축
- Terraform을 사용하여 AWS VPC에 SDC 구축
- Terraform을 사용하여 AWS VPC에 SEC 구축

제

11

장

:

- [Secure Device Connector](#) □□ □□
- □□ □□ [Security Cloud Control](#)
- □□□□ □□ □□

이 장에서는 **Security Cloud Control Firewall Management**에서 다양한 구성 요소로 작업할 때 발생할 수 있는 오류 문제를 문제 해결 방법을 자세히 설명합니다.

Secure Device Connector

연결할 수 없는 SDC, 비활성 상태, IP 주소 변경, 디바이스 연결성 문제, 시스템 시간 오류, 버전 문제, AWS 인증서 또는 연결 오류 등의 보안 디바이스 커넥터 문제를 문제 해결 방법을 알아봅니다.

다음 주제를 사용하여 온프레미스 SDC(Secure Device Connector) 문제를 해결합니다.

이러한 시나리오와 일치하지 않는 경우 [Cisco 기술 지원 센터에서 케이스를 엽니다](#).

SDC

Security Cloud Control에서 연속으로 두 개의 하트비트 요청에 응답하지 못한 경우 SDC는 "도달할 수 없음" 상태입니다. SDC에 연결할 수 없는 경우 테넌트는 온보딩한 디바이스와 통신할 수 없습니다.

Security Cloud Control는 다음과 같은 방식으로 SDC에 연결할 수 없음을 나타냅니다.

- "일부 SDC(Secure Device Connector)에 연결할 수 없습니다."라는 메시지가 표시됩니다. Security Cloud Control 홈페이지에서 이러한 SDC와 연결된 디바이스와 통신할 수 없습니다.
- Services(서비스) 페이지에서 SDC의 상태는 "연결할 수 없음"입니다.

먼저 이 문제를 해결하려면 SDC를 테넌트에 다시 연결해 봅니다.

1. SDC 가상 머신이 실행 중이고 해당 지역의 Security Cloud Control IP 주소에 도달할 수 있는지 확인합니다.

[직접 클라우드 연결성 위한 인바운드 액세스 허용](#) 페이지 48을 참조하십시오.

2. 하트비트를 수동으로 요청하여 Security Cloud Control와 SDC를 다시 연결해 봅니다. SDC가 하트비트 요청에 응답하면 "활성" 상태로 돌아갑니다. 하트비트를 수동으로 요청하려면 다음과 같이 작업합니다.

- a. 왼쪽 창에서 **Administration(관리) > Integration(통합) > Secure Connectors(보안 커넥터)**를 선택합니다.
- b. 연결할 수 없는 SDC를 클릭합니다.
- c. 작업 창에서 **Request Heartbeat(하트비트 요청)**를 클릭합니다.
- d. **Reconnect(다시 연결)**를 클릭합니다.

3. 테넌트에 수동으로 다시 연결하려고 시도한 후에도 SDC가 활성 상태로 돌아가지 않으면, [구축 후 SDC 상태가 Security Cloud Control에서 활성화되지 않음](#) 페이지 140의 지침을 따르십시오.

SDC Security Cloud Control

Security Cloud Control가 구축 후 약 10분 동안 SDC가 활성 상태임을 나타내지 않으면 SDC를 구축할 때 생성한 Security Cloud Control 사용자 및 암호를 사용하여 SSH로 SDC VM에 연결합니다.

1. Security Cloud Control에서 활성 상태로 표시되지 않는 SDC를 클릭하고 **Request Heartbeat(하트비트 요청)**을 클릭합니다.

2. 다음 명령을 사용하여 컨테이너가 실행 중인지 확인합니다.

```
docker ps
```

3. SDC 로그를 보고 명령을 사용하여 오류를 확인합니다.

```
sdctl show logs
```

4. 다음 명령을 사용하여 컨테이너를 다시 시작합니다.

```
sdc restart
```

SDC IP Security Cloud Control

SDC의 업데이트된 IP 주소를 보려면, 이전에 제공된 단계를 사용하여 하트비트를 요청한 다음 브라우저를 새로 고칩니다.

Security Cloud Control에서 활성 상태로 표시되지 않는 SDC를 클릭하고, 사이드바에서 **Request Heartbeat**(하트비트 요청)를 클릭합니다.

1. `docker ps` 명령을 사용하여 컨테이너가 실행 중인지 확인합니다.
2. `sdc show logs` 명령을 사용하여 SDC 로그를 보고 오류를 확인합니다.
3. `sdc restart` 명령을 사용하여 컨테이너를 다시 시작합니다.

SDC

이 도구를 사용하여 Security Cloud Control에서 SDC(Secure Device Connector)를 통해 디바이스로의 연결을 테스트합니다. 디바이스가 온보딩에 실패하거나 온보딩 전에 Security Cloud Control가 디바이스에 연결할 수 있는지 확인하려는 경우 이 연결을 테스트할 수 있습니다.

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 왼쪽 창에서 **Administration(관리) > Integration(통합) > Firewall Management Center**를 클릭하고 **Secure Connector(보안 커넥터)** 탭을 클릭합니다.
3. SDC를 선택합니다.
4. 오른쪽의 **Troubleshooting(문제 해결)** 창에서 **Device Connectivity(디바이스 연결)**를 클릭합니다.
5. 문제 해결을 시도하거나 연결을 시도하는 디바이스의 유효한 IP 주소 또는 FQDN 및 포트 번호를 입력하고 **Go(이동)**를 클릭합니다. Security Cloud Control는 다음 검증을 수행합니다.
 - a) **DNS 확인** - IP 주소 대신 FQDN을 제공하는 경우 SDC가 도메인 이름을 확인하고 IP 주소를 가져올 수 있는지 확인합니다.
 - b) **연결 테스트** - 디바이스에 연결할 수 있는지 확인합니다.
 - c) **TLS 지원** - 디바이스와 SDC가 모두 지원하는 TLS 버전 및 암호를 탐지합니다.
 - 지원되지 않는 암호 - 디바이스와 SDC에서 모두 지원하는 TLS 버전이 없는 경우 Security Cloud Control는 디바이스에서 지원하는 TLS 버전 및 암호도 테스트하지만 SDC는 테스트하지 않습니다.
 - d) **SSL 인증서** - 문제 해결에서 인증서 정보를 제공합니다.
6. 디바이스에 대한 온보딩 또는 연결 문제가 계속 발생하는 경우 [Security Cloud Control 지원에 문의](#)하십시오.

SDC

SDC(Secure Device Connector)는 지금까지 CentOS 7 가상 머신에 설치되었습니다. 그러나 CentOS는 단종되어 Security Cloud 제어의 방화벽에서 더 이상 지원되지 않으므로 CentOS 7의 모든 SDC를 Ubuntu 가상 머신으로 마이그레이션하는 것이 좋습니다.

자세한 내용은 온프레미스 [Secure Device Connector](#) 및 [Secure Event Connector](#)를 CentOS 7 가상 머신에서 Ubuntu 가상 머신으로 마이그레이션을 참조하십시오.

이 절차는 여전히 CentOS를 사용하는 경우에 온프레미스 SDC에만 적용됩니다.

증상: 간헐적으로 또는 SDC에 연결되지 않음

진단: 이 문제는 디스크 공간이 거의 찼을 때(80% 이상) 발생할 수 있습니다.

디스크 공간 사용량을 확인하려면 다음 단계를 수행합니다.

1. SDC(Secure Device Connector) VM용 콘솔을 엽니다.
2. 사용자 이름 **cdo**로 로그인합니다.
3. 최초 로그인 시 생성한 비밀번호를 입력합니다.
4. 먼저 **df -h**를 입력하여 사용 가능한 디스크 공간이 없는지 확인하여 디스크 여유 공간을 확인합니다.

Docker에서 디스크 공간을 소비한 것을 확인할 수 있습니다. 정상적인 디스크 사용량은 2GB 미만일 것으로 예상됩니다.

5. Docker 폴더의 디스크 사용량을 보려면,

sudo du -h /var/lib/docker | sort -h를 실행합니다.

Docker 폴더의 디스크 공간 사용량을 볼 수 있습니다.

Docker 폴더의 디스크 공간 사용량이 거의 가득 찬 경우 docker 구성 파일에서 다음을 정의합니다.

- 최대 크기: 현재 파일이 최대 크기에 도달하면 로그 회전을 강제합니다.
- 최대 파일: 최대 한도에 도달했을 때 초과 회전된 로그 파일을 삭제합니다.

다음을 수행하십시오.

1. **sudo vi /etc/docker/daemon.json**를 실행합니다.
2. 파일에 다음 줄을 삽입합니다.

```
{
  "log-driver": "json-file",
  "log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. **ESC** 키를 누른 다음 **:wq!**를 입력합니다. 변경 사항을 쓰고 파일을 닫습니다.



sudo cat /etc/docker/daemon.json을 실행하여 파일의 변경 사항을 확인할 수 있습니다.

4. **sudo systemctl restart docker**를 실행하여 docker 파일을 다시 시작합니다.

변경 사항이 적용되려면 몇 분 정도 걸립니다. **sudo du -h /var/lib/docker | sort -h**를 실행하여 docker 폴더의 업데이트된 디스크 사용량을 봅니다.

5. **df -h**를 실행하여 사용 가능한 디스크 크기가 증가했는지 확인합니다.

6. SDC 상태를 Unreachable(연결 불가)에서 Active(활성)로 변경하려면 먼저 **Administration(관리) > Integration(통합) > Firewall Management Center**에서 **Secure Connector(보안 커넥터)** 탭으로 이동하여 **Actions(작업)** 메뉴에서 **Request Reconnect(재연결 요청)**를 클릭해야 합니다.

Secure Device Connector : cisco-sa-20190215-runc

Cisco PSIRT(제품 보안 사고 대응 팀)는 Docker의 심각도가 높은 취약성에 대해 설명하는 보안 자문 **cisco-sa-20190215-runc**를 게시했습니다. 취약성에 대한 전체 설명은 [전체 PSIRT 팀 자문을 참조하십시오](#).

이 취약성은 모든 Security Cloud Control 고객에게 영향을 미칩니다.

- Security Cloud Control의 클라우드 구축 SDC(Secure Device Connector)를 사용하는 고객은 Security Cloud Control 운영팀에서 교정 단계를 이미 수행했으므로 아무 작업도 수행할 필요가 없습니다.
- 온프레미스에 구축된 SDC를 사용하는 고객은 최신 Docker 버전을 사용하도록 SDC 호스트를 업그레이드해야 합니다. 다음 지침에 따라 이 작업을 수행할 수 있습니다.
 - [Security Cloud Control-표준 SDC 호스트 업데이트 페이지 143](#)
 - [사용자 지정 SDC 호스트 업데이트 페이지 144](#)
 - [버그 추적 페이지 144](#)

Security Cloud Control- SDC

- SDC(Secure Device Connector)는 지금까지 CentOS 7 가상 머신에 설치되었습니다. 그러나 CentOS는 단종되어 Security Cloud 제어의 방화벽에서 더 이상 지원되지 않으므로 CentOS 7의 모든 SDC를 Ubuntu 가상 머신으로 마이그레이션하는 것이 좋습니다.

자세한 내용은 온프레미스 [Secure Device Connector](#) 및 [Secure Event Connector](#)를 [CentOS 7 가상 머신에서 Ubuntu 가상 머신으로 마이그레이션](#)을 참조하십시오.

이 절차는 여전히 CentOS를 사용하는 경우에 적용됩니다.

- [Security Cloud Control 이미지를 사용하여 SDC를 구축](#)한 경우 이 지침을 사용합니다.

1. SSH 또는 하이퍼바이저 콘솔을 사용하여 SDC 호스트에 연결합니다.
2. 다음 명령을 실행하여 Docker 서비스 버전을 확인합니다.

```
docker version
```

3. 최신 VM(가상 머신) 중 하나를 실행 중인 경우 다음과 같은 출력이 표시됩니다.

```
> docker version
Client:
 Version: 18.06.1-ce
 API version: 1.38
 Go version: go1.10.3
 Git commit: e68fc7a
 Built: Tue Aug 21 17:23:03 2018
 OS/Arch: linux/amd64
 Experimental: false
```

여기에서 이전 버전을 볼 수 있습니다.

4. 다음 명령을 실행하여 **Docker**를 업데이트하고 서비스를 다시 시작하십시오.

```
> sudo yum update docker-ce
> sudo service docker restart
```



Docker 서비스가 다시 시작되는 동안 **Security Cloud Control**와 디바이스 간에 짧은 연결 중단이 발생합니다.

5. `docker version` 명령을 다시 실행하십시오. 다음 출력이 표시되어야 합니다.

```
> docker version
Client:
  Version: 18.09.2
  API version: 1.39
  Go version: go1.10.6
  Git commit: 6247962
  Built: Sun Feb XX 04:13:27 2019
  OS/Arch: linux/amd64
  Experimental: false
```

6. 마쳤습니다. 이제 패치가 적용된 최신 버전의 **Docker**로 업그레이드되었습니다.

SDC

SDC(Secure Device Connector)는 지금까지 **CentOS 7** 가상 머신에 설치되었습니다. 그러나 **CentOS**는 단종되어 **Security Cloud** 제어의 방화벽에서 더 이상 지원되지 않으므로 **CentOS 7**의 모든 **SDC**를 **Ubuntu** 가상 머신으로 마이그레이션하는 것이 좋습니다.

자세한 내용은 [온프레미스 Secure Device Connector](#) 및 [Secure Event Connector](#)를 **CentOS 7** 가상 머신에서 **Ubuntu** 가상 머신으로 마이그레이션을 참조하십시오.

이 절차는 여전히 **CentOS**를 사용하는 경우에 적용됩니다.

- 자체 **SDC** 호스트를 생성한 경우 **Docker** 설치 방법에 따라 업데이트 지침을 따라야 합니다. **CentOS**, **yum** 및 **Docker-ce**(커뮤니티 에디션)를 사용한 경우 이전 절차가 작동합니다.
- **Docker-ee**(엔터프라이즈 버전)를 설치했거나 다른 방법을 사용하여 **Docker**를 설치한 경우 **Docker**의 고정 버전이 다를 수 있습니다. **Docker** 페이지를 확인하여 설치할 올바른 버전([Docker 보안 업데이트 및 컨테이너 보안 모범 사례](#))을 결정할 수 있습니다.

Cisco는 이 취약성을 계속 평가하고 있으며 추가 정보가 제공되는 대로 권고를 업데이트할 것입니다. 권고가 최종으로 표시되면 관련 **Cisco** 버그에서 자세한 내용을 참조할 수 있습니다.

[CSCvo33929-CVE-2019-5736: runc container breakout](#)

SDC(Secure Device Connector)는 지금까지 **CentOS 7** 가상 머신에 설치되었습니다. 그러나 **CentOS**는 단종되어 **Security Cloud** 제어의 방화벽에서 더 이상 지원되지 않으므로 **CentOS 7**의 모든 **SDC**를 **Ubuntu** 가상 머신으로 마이그레이션하는 것이 좋습니다.

자세한 내용은 [온프레미스 Secure Device Connector](#) 및 [Secure Event Connector](#)를 CentOS 7 가상 머신에서 Ubuntu 가상 머신으로 마이그레이션을 참조하십시오.

이 절차는 여전히 CentOS를 사용하는 경우에 적용됩니다.

- Security Cloud Control에서는 SDC(Secure Device Connector)와의 새로운 통신 방식을 채택하고 있습니다. 이를 위해 Security Cloud Control는 2024년 2월 1일까지 기존 SDC를 새 통신 방법으로 마이그레이션해야 합니다.



주

SDC가 2024년 2월 1일까지 마이그레이션되지 않으면 Security Cloud Control는 더 이상 SDC를 통해 디바이스와 통신할 수 없습니다.

- Security Cloud Control의 운영팀이 SDC 마이그레이션을 시도했지만 SDC 시스템 시간이 AWS 시스템 시간보다 15분 빠르거나 늦어 마이그레이션에 성공하지 못했습니다.

아래 단계에 따라 시스템 시간 문제를 해결합니다. 이 문제가 해결되면 마이그레이션을 진행할 수 있습니다.

1. VM 터미널을 통해 또는 SSH 연결을 통해 SDC VM에 로그인합니다.
2. 프롬프트에서 `sudo sdc-onboard setup`을 입력하고 인증합니다.
3. 이제 SDC를 처음 설정하는 것처럼 SDC 설정 질문에 응답해야 합니다. NTP 서버 주소를 제외하고는 이전과 동일한 비밀번호와 네트워크 정보를 모두 다시 입력합니다.
 - a) SDC를 설정하는 데 사용한 것과 동일한 비밀번호로 루트 및 Security Cloud Control 사용자 비밀번호를 재설정합니다.
 - b) 프롬프트가 표시되면 **y**를 입력하여 네트워크를 재설정합니다.
 - c) 이전과 같이 IP 주소/CIDR의 값을 입력합니다.
 - d) 이전과 같이 네트워크 게이트웨이의 값을 입력합니다.
 - e) 이전과 같이 DNS 서버 값을 입력합니다.
 - f) NTP 서버에 대한 프롬프트가 표시되면 유효한 NTP 서버 주소(예: `time.aws.com`)를 제공해야 합니다.
 - g) 제공한 값을 검토하고 값이 올바른 경우 **y**를 입력합니다.
4. 프롬프트에서 날짜를 입력하여 시간 서버에 연결할 수 있고 SDC와 동기화되는지 확인합니다. UTC 날짜 및 시간이 표시되며 SDC 시간과 비교할 수 있습니다.

이러한 단계를 완료했거나 오류가 발생하는 경우에는 [Cisco Technical Assistance Center\(TAC\)](#)에 문의하십시오. 이 단계를 성공적으로 완료하면 Security Cloud Control 운영팀에서 새로운 통신 방법의 SDC 마이그레이션을 완료할 수 있습니다.

SDC 202311****

SDC(Secure Device Connector)는 지금까지 CentOS 7 가상 머신에 설치되었습니다. 그러나 CentOS는 단종되어 Security Cloud 제어의 방화벽에서 더 이상 지원되지 않으므로 CentOS 7의 모든 SDC를 Ubuntu 가상 머신으로 마이그레이션하는 것이 좋습니다.

자세한 내용은 [온프레미스 Secure Device Connector](#) 및 [Secure Event Connector](#)를 CentOS 7 가상 머신에서 Ubuntu 가상 머신으로 마이그레이션을 참조하십시오.

이 절차는 여전히 CentOS를 사용하는 경우에 적용됩니다.

- Security Cloud Control에서는 SDC(Secure Device Connector)와의 새로운 통신 방식을 채택하고 있습니다. 이를 위해 Security Cloud Control는 2024년 2월 1일까지 기존 SDC를 새 통신 방법으로 마이그레이션해야 합니다.



주

SDC가 2024년 2월 1일까지 마이그레이션되지 않으면 Security Cloud Control는 더 이상 SDC를 통해 디바이스와 통신할 수 없습니다.

- Security Cloud Control의 운영팀이 SDC 마이그레이션을 시도했지만 테넌트가 202311****보다 낮은 버전을 실행하고 있어 실패했습니다.
- SDC의 현재 버전은 Security Cloud Control 탐색 메뉴, **Administration(관리) > Integration(통합) > Secure Connectors(보안 커넥터)**에서 보안 커넥터로 이동하면 보안 커넥터 페이지에 나열됩니다. SDC를 선택하면 화면 오른쪽의 **Details(세부 사항)** 창에서 버전 번호를 확인할 수 있습니다.

SDC 버전을 업그레이드하려면 아래 단계를 따르십시오. 이 문제가 해결되면 Security Cloud Control 작업에서 마이그레이션 프로세스를 다시 실행할 수 있습니다.

1. SDC VM에 로그인하고 인증합니다.
2. 프롬프트에 `sudo su - sdc`를 입력하고 인증합니다.
3. 프롬프트에 `crontab -r`를 입력합니다.

`no crontab for sdc`(sdc에 대한 crontab 없음) 메시지가 표시되는 경우 이 메시지를 무시하고 다음 단계로 이동할 수 있습니다.

4. 메시지가 표시되면 `./toolkit/toolkit.sh upgrade`를 입력합니다. Security Cloud Control는 업그레이드가 필요한지 확인하고 툴킷을 업그레이드합니다. 콘솔에서 보고된 오류가 없는지 확인합니다.
5. SDC의 새 버전을 확인합니다.
 - a) Security Cloud Control에 로그인합니다.
 - b) Security Cloud Control 메뉴 모음에서 **Tools & Services(툴 및 서비스) > Secure Connectors(보안 커넥터)**를 탐색하여 보안 커넥터 페이지로 이동합니다.
 - c) SDC를 선택하고 **Actions(작업)** 창에서 **Request Heartbeat(하트비트 요청)**를 클릭합니다.
 - d) SDC 버전이 202311**** 이상인지 확인합니다.

이러한 단계를 완료했거나 오류가 발생하는 경우에는 [Cisco Technical Assistance Center\(TAC\)](#)에 문의하십시오. 이러한 단계를 성공적으로 완료하면 Security Cloud Control 운영팀이 마이그레이션 프로세스를 다시 실행할 수 있습니다.

AWS

Security Cloud Control에서는 SDC(Secure Device Connector)와의 새로운 통신 방식을 채택하고 있습니다. 이를 위해 Security Cloud Control는 2024년 2월 1일까지 기존 SDC를 새 통신 방법으로 마이그레이션해야 합니다.



SDC가 2024년 2월 1일까지 마이그레이션되지 않으면 Security Cloud Control는 더 이상 SDC를 통해 디바이스와 통신할 수 없습니다.

Security Cloud Control의 운영팀이 SDC 마이그레이션을 시도했지만 연결 문제가 발생하여 실패했습니다. 아래 단계에 따라 연결 문제를 해결하십시오. 이 문제가 해결되면 마이그레이션을 진행할 수 있습니다.

1. 포트 443에서 해당 지역의 도메인에 대한 아웃바운드 프록시 연결을 허용하는 방화벽 규칙을 생성합니다.

- 호주 지역의 프로덕션 테넌트:
 - cognito-identity.ap-southeast-2.amazonaws.com
 - cognito-idp.ap-southeast-2.amazonaws.com
 - sns.ap-southeast-2.amazonaws.com
 - sqs.ap-southeast-2.amazonaws.com
- 인도 지역의 프로덕션 테넌트:
 - cognito-identity.ap-south-1.amazonaws.com
 - cognito-idp.ap-south-1.amazonaws.com
 - sns.ap-south-1.amazonaws.com
 - sqs.ap-south-1.amazonaws.com
- 미국 지역의 프로덕션 테넌트:
 - cognito-identity.us-west-2.amazonaws.com
 - cognito-idp.us-west-2.amazonaws.com
 - sns.us-west-2.amazonaws.com
 - sqs.us-west-2.amazonaws.com
- EU 지역의 프로덕션 테넌트:
 - cognito-identity.eu-central-1.amazonaws.com
 - cognito-idp.eu-central-1.amazonaws.com
 - sns.eu-central-1.amazonaws.com
 - sqs.eu-central-1.amazonaws.com
- APJ 지역의 프로덕션 테넌트:
 - cognito-identity.ap-northeast-1.amazonaws.com
 - cognito-idp.ap-northeast-1.amazonaws.com
 - sqs.ap-northeast-1.amazonaws.com

- sns.ap-northeast-1.amazonaws.com

2. 아래 명령 중 하나를 사용하여 방화벽의 "허용 목록"에 추가해야 하는 전체 IP 주소 목록을 확인할 수 있습니다.

주

아래 명령은 **jq**가 설치되어 있는 사용자를 위한 명령입니다. IP 주소가 단일 목록에 표시됩니다.

- 미국 지역의 프로덕션 테넌트:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[]
| select( (.service == "AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- EU 지역의 프로덕션 테넌트:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[]
| select( (.service == "AMAZON" ) and .region == "eu-central-1") |
.ip_prefix'
```

- APJ 지역의 프로덕션 테넌트:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[]
| select( (.service == "AMAZON" ) and .region == "ap-northeast-1") |
.ip_prefix'
```

주

jq가 설치되어 있지 않은 경우, 명령의 다음 단축 버전을 사용할 수 있습니다.

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

이러한 단계를 완료했거나 오류가 발생하는 경우에는 [Cisco Technical Assistance Center\(TAC\)](#)에 문의하십시오. 이 단계를 성공적으로 완료하면 Security Cloud Control 운영팀에서 새로운 통신 방법으로서의 SDC 마이그레이션을 완료할 수 있습니다.

Security Cloud Control

로그인 실패, 액세스 및 인증서 문제, 개체 관련 오류 등의 Security Cloud Control 문제를 해결하는 방법을 알아 봅니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. **Devices(디바이스)** 탭을 클릭합니다.
3. 해당 디바이스 탭을 클릭합니다.
4. 새 핑거프린트 감지됨 상태에서 디바이스를 선택합니다.
5. 새 핑거프린트 감지됨 창에서 핑거프린트 검토를 클릭합니다.
6. 핑거프린트를 검토하고 수락하라는 메시지가 표시되면
 - a. **Download Fingerprint(핑거프린트 다운로드)**를 클릭하고 검토합니다.
 - b. 핑거프린트에 만족하면 **Accept(수락)**를 클릭합니다. 그렇지 않은 경우 **Cancel(취소)**를 클릭합니다.
7. 새 핑거프린트 문제를 해결한 후 디바이스의 연결 상태가 온라인으로 표시되고 구성 상태가 "동기화되지 않음" 또는 "충돌 감지됨"으로 표시될 수 있습니다. **구성 충돌 해결**을 검토하여 **Security Cloud Control**와 디바이스 간의 구성 차이를 검토하고 해결합니다.

SSL

(SSL)

스마트폰 및 기타 디바이스용 일부 앱은 **SSL**(또는 인증 기관) 피닝이라는 기술을 사용합니다. **SSL** 피닝 기술은 원래 서버 인증서의 해시를 앱 자체에 포함합니다. 따라서 앱이 **Firepower Threat Defense** 디바이스에서 재서명된 인증서를 받으면 해시 검증에 실패하고 연결이 중단됩니다.

이때 기본적인 증상은 사용자가 사이트 앱을 사용해서는 웹 사이트에 연결할 수 없지만 웹 브라우저를 사용하면 연결할 수 있다는 것입니다(앱으로 연결에 실패한 디바이스에서 브라우저를 사용할 때도 연결 가능). 예를 들어 사용자는 **Facebook iOS** 또는 **Android** 앱을 사용할 수 없지만 **Safari** 또는 **Chrome**을 <https://www.facebook.com>으로 지정하고 성공적으로 연결할 수 있습니다.

SSL 피닝은 특별히 메시지 가로채기(**man-in-the-middle**) 공격을 차단하는 데 사용되므로 이러한 현상을 해결하는 방법은 없습니다. 다음 옵션 중에서 선택해야 합니다.

기타 세부정보

특정 사이트가 브라우저에서는 작동하는데 동일 디바이스의 앱에서는 작동하지 않는 경우 **SSL** 피닝 인스턴스를 살펴봐야 합니다. 하지만 심층적으로 확인하려면 연결 이벤트를 사용해 브라우저 테스트와 더불어 **SSL** 피닝을 확인할 수 있습니다.

앱은 두 가지 방식으로 해시 검증 장애를 처리할 수 있습니다.

- **Facebook** 등의 그룹 1 앱은 서버에서 **SH, CERT, SHD** 메시지를 받는 즉시 **SSL ALERT** 메시지를 보냅니다. **Alert**는 보통 **SSL** 피닝을 나타내는 "**Unknown CA (48)**(알 수 없는 **CA(48)**)" 알림입니다. 알림 메시지 후에는 **TCP Reset(TCP 재설정)**이 전송됩니다. 이벤트 세부사항에는 다음 증상이 표시됩니다.
 - **SSL Flow Flag(SSL 플로우 플래그)**에는 **ALERT_SEEN**이 포함되어 있습니다.
 - **SSL Flow Flag(SSL 플로우 플래그)**에는 **APP_DATA_C2S** 또는 **APP_DATA_S2C**가 포함되어 있지 않습니다.
 - **SSL Flow Message(SSL 플로우 메시지)**는 보통 **CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE**입니다.

- Dropbox 등의 그룹 2 앱은 알림을 보내지 않습니다. 대신 핸드셰이크가 완료될 때까지 기다렸다가 TCP Reset(TCP 재설정)을 전송합니다. 이벤트에는 다음 증상이 표시됩니다.
 - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN, APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.
 - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED입니다.

잘못된 사용자 이름 또는 암호로 인해 **Security Cloud Control**에 로그인하지 못함

Security Cloud Control에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 **Cisco Secure Cloud Sign-On** 어카운트를 사용하려면 의 지침에 따라 새 **Cisco Secure Cloud Sign-On** 어카운트에 등록해야 합니다. 새 **Cisco Security Cloud Sign On** 어카운트를 등록해야 합니다.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 **Security Cloud Control**를 실행할 수 없음

Security Cloud Control 테넌트와 다른 사용자 이름으로 **Cisco Secure Cloud Sign-On** 어카운트를 만들었을 수 있습니다. **Security Cloud Control**와 **Cisco Secure Sign-On** 간의 사용자 정보를 표준화하려면 [Cisco TAC\(Technical Assistance Center\)](#)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 <https://cdo.onelogin.com>을 가리킬 수 있습니다.

<https://security.cisco.com>에 로그인합니다.

- 새 **Secure Sign-On** 어카운트를 만든 경우 대시보드에서 테넌트가 만들어진 지역에 해당하는 **Security Cloud Control** 타일을 클릭합니다.
 - Security Cloud Control APJ
 - Security Cloud Control 호주
 - Security Cloud Control EU
 - Security Cloud Control 인도
 - Security Cloud Control US
- <https://security.cisco.com>를 가리키도록 즐겨찾기를 업데이트합니다.

Security Cloud Control에서 디바이스 연결 상태를 해석하고 오프라인 디바이스, 라이선스 부족, 유효하지 않은 자격 증명, 온보딩 오류, 새 인증서 및 등록되지 않은 디바이스와 같은 문제를 해결하는 방법을 알아봅니다.

Security Cloud Control 테넌트에 온보딩된 디바이스의 연결 상태를 볼 수 있습니다. 이 항목은 다양한 연결 상태를 이해하는 데 도움이 됩니다. **Security Devices**(보안 디바이스) 페이지에서 **Connectivity**(연결성) 열은 디바이스 연결 상태를 표시합니다.

디바이스 연결 상태가 '온라인'이면 디바이스의 전원이 켜져 있고 **Security Cloud Control**에 연결되어 있음을 의미합니다. 아래 표에 설명된 다른 상태는 일반적으로 여러 가지 이유로 디바이스에 문제가 발생할 때 발생합니다. 이 표는 이러한 문제에서 복원하는 방법을 제공합니다. 연결 실패를 일으키는 문제가 두 개 이상 있을 수 있

습니다. 다시 연결을 시도하면, **Security Cloud Control**는 다시 연결을 수행하기 전에 먼저 이러한 모든 문제를 편집하라는 메시지를 표시합니다.

디바이스 연결 상태	가능한 이유	해결 방법
온라인	디바이스의 전원이 켜져 있고 Security Cloud Control 에 연결되어 있습니다.	해당 없음
오프라인	디바이스의 전원이 꺼졌거나 네트워크 연결이 끊겼습니다.	디바이스가 오프라인 상태인지 확인합니다.
불충분한 라이선스	디바이스에 충분한 라이선스가 없습니다.	라이선스 부족 문제 해결 페이지 151
유효하지 않은 자격 증명	디바이스에 연결하기 위해 Security Cloud Control 에서 사용하는 사용자 이름과 암호 조합이 올바르지 않습니다.	유효하지 않은 자격 증명 문제 해결 페이지 152
온보딩	디바이스 온보딩이 시작되었지만 완료되지 않았습니다.	디바이스의 연결을 확인하고 디바이스 등록을 완료해야 합니다.
Unknown	디바이스 온보딩에 실패했으며 Security Cloud Control 에서 디바이스의 연결성 상태를 가져올 수 없습니다.	보안 디바이스 페이지에서 디바이스를 선택하고 오른쪽 창에서 Check for Changes (변경 사항 확인)를 선택하여 디바이스에서 최신 구성 가져오기를 시도합니다.
새 인증서 탐지됨	디바이스의 인증서가 변경되었습니다. 디바이스가 자체 서명된 인증서를 사용하는 경우 디바이스의 전원을 껐다 켜서 이 문제가 발생했을 수 있습니다.	새 인증서 문제 해결 페이지 152
온보딩 오류	Security Cloud Control 는 디바이스를 온보딩할 때 디바이스와의 연결이 끊어졌을 수 있습니다.	온보딩 오류 문제 해결 페이지 160

디바이스 연결 상태가 "**Insufficient License**(라이선스 부족)"로 표시되면 다음을 수행합니다.

- 디바이스가 라이선스를 획득할 때까지 잠시 기다립니다. 일반적으로 **Cisco Smart Software Manager**가 디바이스에 새 라이선스를 적용하는 데 시간이 걸립니다.
- 디바이스 상태가 변경되지 않으면 **Security Cloud Control**에서 로그아웃하고 다시 로그인하여 **Security Cloud Control** 포털을 새로 고침한 후 라이선스 서버와 디바이스 간의 네트워크 통신 문제를 해결합니다.
- 포털을 새로 고침해도 디바이스 상태가 변경되지 않으면 다음을 수행합니다.

1. **Cisco Smart Software Manager**에서 새 토큰을 생성하고 복사합니다. 자세한 내용은 [스마트 라이선싱 생성 동영상](#)을 참조하십시오.
2. 왼쪽 창에서 보안 디바이스를 클릭합니다.

3. **Devices**(디바이스) 탭을 클릭합니다.
4. 적절한 디바이스 유형 탭을 클릭하고 **Insufficient License**(라이선스 부족) 상태의 디바이스를 선택합니다.
5. **Device Details**(디바이스 세부 정보) 창에서 **Insufficient Licenses**(불충분한 라이선스)에 표시되는 **Manage Licenses**(라이선스 관리)를 클릭합니다. **Manage Licenses**(라이선스 관리) 창이 나타납니다.
6. 활성화 필드에 새 토큰을 붙여넣고 디바이스 등록을 클릭합니다.
토큰이 디바이스에 성공적으로 적용되면 연결 상태가 온라인으로 바뀝니다.

유효하지 않은 자격 증명으로 인한 디바이스 연결 끊김을 해결하려면 다음을 수행합니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. **Devices**(디바이스) 탭을 클릭합니다.
3. 적절한 디바이스 유형 탭을 클릭하고 **Invalid Credentials**(유효하지 않은 자격 증명) 상태의 디바이스를 선택합니다.
4. **Device Details**(디바이스 세부 정보) 창에서 **Invalid Credentials**(잘못된 자격 증명)에 나타나는 **Reconnect**(재연결)을 클릭합니다. Security Cloud Control가 디바이스에 재연결을 시도합니다.
5. 프롬프트가 나타나면 Linux 사용자 이름 및 비밀번호를 입력합니다.
6. **Continue**(계속)를 클릭합니다.
7. 디바이스가 온라인 상태가 되고 사용할 준비가 되면 **Close**(닫기)를 클릭합니다.
8. Security Cloud Control가 잘못된 자격 증명을 사용하여 디바이스에 연결하려고 시도했기 때문에 Security Cloud Control가 디바이스에 연결하는 데 사용해야 하는 사용자 이름 및 비밀번호 조합이 디바이스에서 직접 변경되었을 수 있습니다. 이제 디바이스가 "Online(온라인)"이지만 구성 상태가 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. [Resolve Configuration Conflicts\(구성 충돌 해결\)](#)를 사용하여 Security Cloud Control와 디바이스 간의 구성 차이를 검토하고 해결합니다.

Security Cloud Control

Security Cloud Control는 디바이스에 연결할 때 인증서의 유효성을 확인합니다. 특히 Security Cloud Control는 다음을 요구합니다.

1. 디바이스에서 1.0 이상의 TLS 버전을 사용합니다.
2. 디바이스에서 제시한 인증서가 만료되지 않았으며 발급 날짜가 과거입니다(즉, 이미 유효하며 나중에 유효해질 예정이 아님).
3. 인증서는 SHA-256 인증서여야 합니다. SHA-1 인증서는 허용되지 않습니다.
4. 다음 조건 중 하나가 참입니다.
 - 디바이스가 자체 서명 인증서를 사용하며, 인증된 사용자가 신뢰하는 최신 인증서와 동일합니다.
 - 디바이스는 신뢰할 수 있는 CA(Certificate Authority)에서 서명한 인증서를 사용하며, 제공된 리프 인증서를 관련 CA에 연결하는 인증서 체인을 제공합니다.

다음은 Security Cloud Control가 브라우저와 다른 방식으로 인증서를 사용하는 방법입니다.

- 자체 서명 인증서의 경우 **Security Cloud Control**는 도메인 이름 확인을 재정의하며, 그 대신 디바이스 온보딩 또는 재연결 중에 인증된 사용자가 신뢰하는 인증서와 인증서가 정확히 일치하는지 확인합니다.
- **Security Cloud Control**는 아직 내부 **CA**를 지원하지 않습니다. 현재는 내부 **CA**가 서명한 인증서를 확인할 수 있는 방법이 없습니다.

디바이스별로 **ASA** 디바이스에 대한 인증서 확인을 비활성화할 수 있습니다. **Security Cloud Control**에서 **ASA**의 인증서를 신뢰할 수 없는 경우 해당 디바이스에 대한 인증서 검사를 비활성화할 수 있습니다. 디바이스에 대한 인증서 확인을 비활성화하려고 시도했지만 여전히 디바이스를 온보딩할 수 없는 경우, 디바이스에 대해 지정한 **IP** 주소 및 포트가 잘못되었거나 연결할 수 없는 것일 수 있습니다. 인증서 검사를 전역적으로 비활성화하거나 지원되는 인증서가 있는 디바이스에 대한 인증서 검사를 비활성화할 수 있는 방법은 없습니다. 비 **ASA** 디바이스에 대한 인증서 확인을 비활성화할 수 있는 방법은 없습니다.

디바이스에 대한 인증서 확인을 비활성화하면 **Security Cloud Control**은 **TLS**를 사용하여 디바이스에 연결하지만 연결을 설정하는 데 사용된 인증서를 검증하지 않습니다. 즉, 수동적인 중간자 공격자는 연결을 도청할 수 없지만, 활성 상태의 중간자 공격자는 **Security Cloud Control**에 유효하지 않은 인증서를 제공하여 연결을 가로챌 수 있습니다.

Security Cloud Control가 디바이스를 온보딩하지 못할 수 있는 몇 가지 이유가 있습니다. UI에 "**Security Cloud Control cannot connect to the device using the certificate presented**(제공된 인증서를 사용하여 디바이스에 연결할 수 없음)"라는 메시지가 표시되면 인증서에 문제가 있는 것입니다. UI에 이 메시지가 표시되지 않으면 연결 문제(디바이스에 연결할 수 없음) 또는 기타 네트워크 오류와 관련이 있을 가능성이 높습니다.

Security Cloud Control가 지정된 인증서를 거부하는 이유를 확인하려면 **SDC** 호스트 또는 관련 디바이스에 연결할 수 있는 다른 호스트에서 **openssl** 명령줄 툴을 사용할 수 있습니다. 다음 명령을 사용하여 디바이스에서 제공하는 인증서를 보여주는 파일을 생성합니다.

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

이 명령은 인터랙티브 세션을 시작하므로 몇 초 후에 종료하려면 **Ctrl-c**를 사용해야 합니다.

이제 다음과 같은 출력이 포함된 파일이 생성됩니다.

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN =
*.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzW9TylihJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjQsMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzW9TylihJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
```

```

MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTA1VT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB

    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z..T..H~v0s....@[.
0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5....o}.
0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o.....1[...eo..
0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.....3(
0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "...:Y...\\!...R(E.
0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r...#...|....+.B.
0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
00a0 - 72 a4 ad
00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---

```

이 출력에서 가장 먼저 확인할 사항은 반환 코드 확인이 표시되는 마지막 줄입니다. 인증서 문제가 있는 경우 반환 코드는 0이 아니며 오류에 대한 설명이 표시됩니다.

일반적인 오류 및 해결 방법을 보려면 이 인증서 오류 코드 목록을 확장합니다.

0 X509_V_OK 작업에 성공했습니다.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT 신뢰할 수 없는 인증서의 발급자 인증서를 찾을 수 없습니다.

3 X509_V_ERR_UNABLE_TO_GET_CRL 인증서의 CRL을 찾을 수 없습니다.

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE 인증서 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 이는 RSA 키에만 의미가 있습니다.

- 5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE CRL 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 사용되지 않음.
- 6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY 인증서 SubjectPublicKeyInfo의 공개 키를 읽을 수 없습니다.
- 7 X509_V_ERR_CERT_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.
- 8 X509_V_ERR_CRL_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.
- 9 X509_V_ERR_CERT_NOT_YET_VALID 인증서가 아직 유효하지 않습니다. notBefore 날짜가 현재 시간 이후입니다. 자세한 내용은 아래의 **반환 코드 확인: 9(인증서가 아직 유효하지 않음)**를 참조하십시오.
- 10 X509_V_ERR_CERT_HAS_EXPIRED 인증서가 만료되었습니다. 즉, notAfter 날짜는 현재 시간 이전입니다. 자세한 내용은 아래의 **반환 코드 확인: 10(인증서가 만료되었습니다)**을 참조하십시오.
- 11 X509_V_ERR_CRL_NOT_YET_VALID CRL이 아직 유효하지 않습니다.
- 12 X509_V_ERR_CRL_HAS_EXPIRED CRL이 만료되었습니다.
- 13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD 인증서 notBefore 필드에 잘못된 시간이 포함되어 있습니다.
- 14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD 인증서 notAfter 필드에 유효하지 않은 시간이 포함되어 있습니다.
- 15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD CRL lastUpdate 필드에 잘못된 시간이 포함되어 있습니다.
- 16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD CRL nextUpdate 필드에 유효하지 않은 시간이 포함되어 있습니다.
- 17 X509_V_ERR_OUT_OF_MEM 메모리를 할당하는 동안 오류가 발생했습니다. 이러한 현상은 발생해서는 안 됩니다.
- 18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT 전달된 인증서가 자체 서명되었으며 신뢰할 수 있는 인증서 목록에서 동일한 인증서를 찾을 수 없습니다.
- 19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN 신뢰할 수 없는 인증서를 사용하여 인증서 체인을 구축할 수 있지만 루트를 로컬에서 찾을 수 없습니다.
- 20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 로컬로 조회된 인증서의 발급자 인증서를 찾을 수 없습니다. 이는 일반적으로 신뢰할 수 있는 인증서 목록이 완전하지 않음을 의미합니다.
- 21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE 체인에 하나의 인증서만 포함되어 있으며 자체 서명되지 않았으므로 서명을 확인할 수 없습니다. 자세한 내용은 아래의 "반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)"를 참조하십시오. 자세한 내용은 아래의 **반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)**을 참조하십시오.
- 22 X509_V_ERR_CERT_CHAIN_TOO_LONG 인증서 체인 길이가 제공된 최대 깊이보다 큼니다. 사용되지 않음.
- 23 X509_V_ERR_CERT_REVOKED 인증서가 해지되었습니다.
- 24 X509_V_ERR_INVALID_CA CA 인증서가 유효하지 않습니다. CA가 아니거나 확장명이 제공된 목적과 일치하지 않습니다.
- 25 X509_V_ERR_PATH_LENGTH_EXCEEDED basicConstraints pathlength 매개변수가 초과되었습니다.
- 26 X509_V_ERR_INVALID_PURPOSE 제공된 인증서를 지정된 용도로 사용할 수 없습니다.
- 27 X509_V_ERR_CERT_UNTRUSTED 루트 CA가 지정된 용도로 신뢰할 수 있는 것으로 표시되지 않았습니다.
- 28 X509_V_ERR_CERT_REJECTED 루트 CA가 지정된 용도를 거부하도록 표시되었습니다.
- 29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH 해당 주체 이름이 현재 인증서의 발급자 이름과 일치하지 않아 현재 후보 발급자 인증서가 거부되었습니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.
- 30 X509_V_ERR_AKID_SKID_MISMATCH 현재 후보 발급자 인증서가 거부되었습니다. 해당 주체 키 식별자가 있고 인증 기관 키 식별자가 현재 인증서와 일치하지 않기 때문입니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH 발급자 이름 및 일련 번호가 존재하고 현재 인증서의 기관 키 식별자와 일치하지 않으므로 현재 발급자 인증서가 거부되었습니다. **-issuer_checks** 옵션이 설정된 경우에만 표시됩니다.

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN keyUsage 확장이 인증서 서명을 허용하지 않으므로 현재 발급자 인증서가 거부되었습니다.

50 X509_V_ERR_APPLICATION_VERIFICATION 애플리케이션 관련 오류입니다. 사용되지 않음.

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 **Security Cloud Control**는 **Configuration Status**(구성 상태) 및 **Connectivity**(연결성) 상태로 **"New Certificate Detected"**(새 인증서 탐지됨) 메시지를 생성할 수 있습니다. **Security Cloud Control**에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.



주

두 개 이상의 매니지드 디바이스를 **Security Cloud Control**에 동시에 **대량으로 재연결**하는 경우, **Security Cloud Control**는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. 필터를 사용하여 **New Certificate Detected**(새 인증서 탐지됨) 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.
3. 작업창에서 **Review Certificate**(인증서 검토)를 클릭합니다. **Security Cloud Control**에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.
4. **Device Sync**(디바이스 동기화) 창에서 **Accept**(수락)를 클릭하거나 **Reconnecting to Device**(디바이스에 다시 연결 중) 창에서 **Continue**(계속)를 클릭합니다.

Security Cloud Control는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화된 후 디바이스를 확인하려면 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

반환 코드 확인: **0 (ok)** 하지만 **Security Cloud Control**에서 인증서 오류를 반환합니다.

Security Cloud Control에 인증서가 있으면 "https://<device_ip>:<port>"에 GET 호출을 하여 URL에 연결을 시도합니다. 그래도 문제가 해결되지 않으면 **Security Cloud Control**에 인증서 오류가 표시됩니다. 인증서가 유효한 경우(**openssl**에서 **0 ok** 반환) 연결하려는 포트에서 다른 서비스가 수신 대기하는 문제일 수 있습니다. 다음 명령을 사용할 수 있습니다.

```
curl -k -u <username>:<password>
https://<device_id>:<device_port>/admin/exec/show%20version
```

ASA와 통신하고 있는지 확인하고 HTTPS 서버가 ASA의 올바른 포트에서 실행 중인지 확인합니다.

#	show asp table socket
Protocol Address	Socket State Local Address Foreign
SSL	00019b98 LISTEN 192.168.1.5:443
0.0.0.0:*	

SSL	00029e18	LISTEN	192.168.2.5:443
0.0.0.0:*			
TCP	00032208	LISTEN	192.168.1.5:22
0.0.0.0:*			

반환 코드 확인: 9(인증서가 아직 유효하지 않음)

이 오류는 제공된 인증서의 발급 날짜가 미래이므로 클라이언트가 이를 유효한 것으로 처리하지 않음을 의미합니다. 이는 잘못 구성된 인증서로 인해 발생할 수 있으며, 자체 서명 인증서의 경우 인증서를 생성할 때 잘못된 디바이스 시간이 원인일 수 있습니다.

인증서의 **notBefore** 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

이 오류를 통해 인증서가 유효한 시점을 확인할 수 있습니다.

치료

인증서의 **notBefore** 날짜는 과거여야 합니다. 이전 날짜의 인증서를 재발급할 수 있습니다. 이 문제는 클라이언트 또는 발급 디바이스에서 시간이 올바르게 설정되지 않은 경우에도 발생할 수 있습니다.

반환 코드 확인: 10(인증서가 만료되었습니다)

이 오류는 제공된 인증서 중 하나 이상이 만료되었음을 의미합니다. 인증서의 **notBefore** 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
error 10 at 0 depth lookup:certificate has expired
```

만료 날짜는 인증서 본문에 있습니다.

치료

인증서가 실제로 만료된 경우 유일한 교정 방법은 다른 인증서를 가져오는 것입니다. 인증서의 만료 날짜가 아직 미래이지만 **openssl**이 만료되었다고 주장하는 경우, 컴퓨터의 시간과 날짜를 확인합니다. 예를 들어 인증서가 2020년에 만료되도록 설정되어 있지만 컴퓨터의 날짜가 2021년이면 컴퓨터는 해당 인증서를 만료된 것으로 처리합니다.

반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)

이 오류는 인증서 체인에 문제가 있음을 나타내며, **openssl**은 디바이스에서 제공하는 인증서를 신뢰할 수 있는지 확인할 수 없습니다. 인증서 체인이 작동하는 방식을 확인하려면 위의 예에서 인증서 체인을 살펴보겠습니다.

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzW9TylihnhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
```

```

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjQSMAGCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTA1VT
....lots of base64...
tzW9TylihMjZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuaGAwIBAgIDervmMA0GCSqGSIb3DQEBCwUAME4xCzAJBgNVBAYTA1VT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----

```

인증서 체인은 서버에서 제공하는 인증서 목록으로, 서버의 자체 인증서부터 시작하여 점점 더 높은 수준의 중간 인증서를 포함하여 서버의 인증서를 인증 기관의 최상위 인증서와 연결합니다. 각 인증서에는 해당 주체('로 시작하는 줄) 및 발급자('로 시작하는 줄)가 나열됩니다.

주체는 인증서로 식별되는 엔티티입니다. 여기에는 조직 이름이 포함되며 경우에 따라 인증서가 발급된 엔티티의 공용 이름이 포함됩니다.

발급자는 인증서를 발급한 엔티티입니다. 여기에는 **Organization**(조직) 필드도 포함되며, 경우에 따라 **Common Name**(일반 이름)도 포함됩니다.

서버에 신뢰할 수 있는 인증 기관에서 직접 발급한 인증서가 있는 경우 인증서 체인에 다른 인증서를 포함할 필요가 없습니다. 다음과 같은 인증서를 제공합니다.

```

--- Certificate chain 0
s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com i:/C=US/O=Trusted
Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAuSTELMAkGA1UE
....lots of base64...
tzW9TylihMjZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

```

이 인증서가 제공되면 **openssl**은 ***.example.com**에 대한 **ExampleCo** 인증서가 신뢰할 수 있는 기관 인증서에 의해 올바르게 서명되었는지 확인합니다. 이 인증서는 **openssl**의 기본 제공 신뢰 저장소에 있습니다. 확인 후 **openssl**이 디바이스에 성공적으로 연결됩니다.

그러나 대부분의 서버에는 신뢰할 수 있는 **CA**에서 직접 서명한 인증서가 없습니다. 대신 첫 번째 예에서와 같이 서버의 인증서가 하나 이상의 중간 인증서에 의해 서명되고, 최상위 중간 인증서에는 신뢰할 수 있는 **CA**가 서명한 인증서가 있습니다. **OpenSSL**은 기본적으로 이러한 중간 **CA**를 신뢰하지 않으며, 신뢰할 수 있는 **CA**로 끝나는 완전한 인증서 체인이 제공되는 경우에만 이를 확인할 수 있습니다.

중간 기관이 인증서에 서명한 서버는 모든 중간 인증서를 포함하여 이를 신뢰할 수 있는 **CA**에 연결하는 모든 인증서를 제공해야 합니다. 이 전체 체인을 제공하지 않는 경우 **openssl**의 출력은 다음과 같습니다.

```

depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate

```

```

verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
  Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
  Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---

```

이 출력은 서버가 하나의 인증서만 제공했으며 제공된 인증서가 신뢰할 수 있는 루트가 아닌 중간 기관에 의해 서명되었음을 보여줍니다. 출력에는 특성 확인 오류도 표시됩니다.

치료

이 문제는 디바이스에서 제공하는 인증서가 잘못 구성되어 발생합니다. **Security Cloud Control** 또는 다른 프로그램이 디바이스에 안전하게 연결할 수 있도록 이 문제를 해결하는 유일한 방법은 올바른 인증서 체인을 디바이스에 로드하여 연결하는 클라이언트에 완전한 인증서 체인을 제공하도록 하는 것입니다.

트러스트 포인트에 중간 **CA**를 포함하려면 아래 링크 중 하나를 따르십시오(**CSR**이 **ASA**에서 생성되었는지 여부에 따라).

- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13>
- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15>

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 Security Cloud Control는 **Configuration Status**(구성 상태) 및 **Connectivity**(연결성) 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. Security Cloud Control에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.

주

두 개 이상의 매니지드 디바이스를 Security Cloud Control에 동시에 CDO에 대량으로 다시 연결하는 경우, Security Cloud Control는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. **Devices**(디바이스) 탭을 클릭합니다.
3. 해당 디바이스 탭을 클릭합니다.
4. 필터를 사용하여 **New Certificate Detected**(새 인증서 탐지됨) 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.
5. 작업창에서 **Review Certificate**(인증서 검토)를 클릭합니다. Security Cloud Control에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.
6. **Device Sync**(디바이스 동기화) 창에서 **Accept**(수락)를 클릭하거나 **Reconnecting to Device**(디바이스에 다시 연결 중) 창에서 **Continue**(계속)를 클릭합니다.

Security Cloud Control는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화된 후 디바이스를 확인하려면 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

디바이스 온보딩 오류는 여러 가지 이유로 발생할 수 있습니다.

다음과 같은 작업을 수행할 수 있습니다.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. 적절한 디바이스 유형 탭을 클릭하고 이 오류가 발생하는 디바이스를 선택합니다. 경우에 따라 오른쪽에 오류 설명이 표시됩니다. 설명에 언급된 필요한 조치를 취하십시오.
또는
3. Security Cloud Control에서 디바이스 인스턴스를 제거하고 디바이스 온보딩을 다시 시도하십시오.

Security Cloud Control를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. [충돌 탐지](#) 페이지 114이 활성화되어 있고 Security Cloud Control를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected(충돌 탐지됨)**로 표시됩니다.

Conflict Detected(충돌 탐지됨) 상태를 해결하려면 다음 절차를 수행합니다:

1. Security Cloud Control 홈 페이지에서 방화벽을 클릭합니다.
2. 보안 디바이스를 선택합니다.



온프레미스 방화벽 Management Center의 경우, **Administration(관리) > Integration(통합) > Firewall Management Center**를 클릭하고 **Not Synced(동기화되지 않음)** 상태인 FMC를 선택한 후 5단계부터 계속 진행합니다.

3. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾습니다.
4. 해당 디바이스 탭을 클릭합니다.
5. 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict(충돌 검토)**를 클릭합니다.
6. **Device Sync(디바이스 동기화)** 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.
 - "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 Security Cloud Control에 저장된 디바이스 구성입니다.
 - "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.
7. 다음 중 하나를 선택하여 충돌을 해결합니다.
 - **Accept Device changes(디바이스 변경 사항 수락):** 구성 및 Security Cloud Control에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.



Security Cloud Control는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 구축하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review(검토 없이 수락)**를 선택하는 것입니다.

- **Reject Device Changes(디바이스 변경 거부):** 디바이스에 저장된 구성을 Security Cloud Control에 저장된 구성으로 덮어씁니다.



거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

1. 보안 디바이스를 선택합니다.



온프레미스 방화벽 Management Center의 경우, **Administration(관리) > Integration(통합) > Firewall Management Center**를 클릭하고 **Not Synced(동기화되지 않음)** 상태인 FMC를 선택한 후 5단계부터 계속 진행합니다.

2. **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.

3. 해당 디바이스 탭을 클릭합니다.

4. 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.

5. 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- **미리보기 및 구축...** - Security Cloud Control에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 **미리 보고 구축**하거나 한 번에 여러 변경 사항을 기다렸다가 구축하십시오.
- **변경 사항 취소** - Security Cloud Control에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 Security Cloud Control에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 Security Cloud Control에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

제

12 FAQ

장

- :
- Security Cloud Control
 - Security Cloud Control □ □ □ □ □ □
□ □ □ FAQ
 - □ □ □ □ □ □
 - □ □
 - □ □ □ □
 - □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
□ □
 - □ □ □ □ □
 - □ □ □
 - □ □ □ □ □ □ □ □ □
 - Security Cloud Control □ □ □ □ □ □
□ □ □ □ □ □
 - Security Cloud Control □ □ □ □

이 장에는 다음 섹션이 포함되어 있습니다.

Security Cloud Control

Security Cloud Control에서 관리자가 단일 클라우드 기반 인터페이스에서 지원되는 디바이스 전반에 걸쳐 일관된 보안 정책을 생성, 모니터링, 유지 관리하도록 지원하는 방법을 알아봅니다.

Security Cloud Control는 무엇입니까?

Security Cloud Control(이전 Cisco Defense Orchestrator)는 네트워크 관리자가 다양한 보안 디바이스에서 일관된 보안 정책을 만들고 유지할 수 있도록 하는 클라우드 기반 다중 디바이스 관리자입니다.

Security Cloud Control를 디바이스를 관리하는 데 사용할 수 있습니다.

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Threat Defense
- Cisco Umbrella
- Meraki
- Cisco IOS 디바이스
- 아마존 웹 서비스(AWS) 인스턴스
- SSH 연결을 사용하여 관리되는 디바이스

Security Cloud Control 관리자는 단일 인터페이스를 통해 이러한 모든 디바이스 유형을 모니터링하고 유지할 수 있습니다.

Security Cloud Control FAQ

Secure Firewall ASA, Firewall Threat Defense, 온프레미스 Firewall Management Center, Meraki, SSH 및 IOS 디바이스를 포함하여 Security Cloud Control에서 지원되는 디바이스 유형에 대한 온보딩 관련 FAQ에 대해 알아봅니다.

Security Cloud Control Secure Firewall ASA FAQ

ASA ?

ASA를 한 번에 하나씩 온보딩하거나 대량 작업으로 온보딩할 수 있습니다. 고가용성 쌍의 일부인 ASA를 온보딩하는 경우 쌍의 기본 디바이스만 온보딩하는 데 [ASA 디바이스 온보딩](#)을 사용합니다. 보안 상황 또는 관리 상황을 온보딩하는 방법은 다른 ASA를 온보딩하는 방법과 동일합니다.

ASA ?

CSV 파일을 사용하여 ASA 목록을 생성할 수 있으며, Security Cloud Control은 목록의 모든 ASA를 온보딩합니다. 대량 ASA 온보딩에 대한 지침은 [대량 ASA 온보드](#)를 참조하십시오.

ASA ?

시작하려면 [Security Cloud Control로 ASA 관리](#)를 참조하십시오.

Firewall Management Center Secure Firewall Threat Defense FAQ

Secure Firewall Threat Defense ?

CLI 등록 키, 제로 터치 프로비저닝 또는 일련 번호를 사용하여 FTD 디바이스를 온보딩할 수 있습니다.

Secure Firewall Threat Defense ?

디바이스가 동기화되면 **Administration(관리) > Integration(통합) > Firewall Management Center**로 이동하여 **Actions(작업)**, **Management(관리)** 또는 **Settings(설정)** 창에서 작업을 선택하여 클라우드 제공 **Firewall Management Center**에서 **Threat Defense** 디바이스의 구성을 시작합니다. 시작하려면 [클라우드 제공 Firewall Management Center 애플리케이션 페이지](#)를 참조하십시오.

Secure Firewall Threat Defense ?

[Secure Firewall Threat Defense 온보딩 문제 해결](#)을 참조하십시오.

Firewall Management Center FAQ

이 개념은 온프레미스 **Firewall Management Center**을 **Security Cloud Control**에 온보딩하는 방법을 설명하지만, 디바이스 관리 변경 사항은 여전히 온프레미스 **Firewall Management Center UI**에서 직접 수행해야 합니다.

Firewall Management Center ?

온프레미스 **Firewall Management Center**를 **Security Cloud Control**에 온보딩할 수 있습니다. 온프레미스 **Firewall Management Center**을(를) 온보딩하면 온프레미스 **Firewall Management Center**에 등록된 모든 디바이스도 온보딩됩니다. **Security Cloud Control**는 온프레미스 **Firewall Management Center**와 연결된 개체 또는 정책 또는 온프레미스 **Firewall Management Center**에 등록된 디바이스의 생성이나 수정을 지원하지 않습니다. 온프레미스 **Firewall Management Center UI**에서 이러한 변경을 수행해야 합니다. 자세한 내용은 [온프레미스 Management Center 온보딩](#)을 참조하십시오.

Security Cloud Control Meraki FAQ

Meraki ?

MX 디바이스는 **Security Cloud Control**와 **Meraki** 대시보드에서 모두 관리할 수 있습니다. **Security Cloud Control**는 구성 변경 사항을 **Meraki** 대시보드에 구축하며, 그러면 구성이 디바이스에 안전하게 구축됩니다. 시작하려면 [Meraki MX 디바이스 온보딩](#)을 참조하십시오.

Security Cloud Control SSH FAQ

SSH ?

SSH 디바이스에 저장된 높은 권한을 가진 사용자의 사용자 이름과 암호를 사용하여 **SDC(Secure Device Connector)**로 디바이스를 온보딩할 수 있습니다. 시작하려면 [SSH 디바이스 온보딩](#)을 참조하십시오.

?

Security Devices(보안 디바이스) 페이지에서 디바이스를 삭제할 수 있습니다.

Security Cloud Control IOS FAQ

Cisco IOS ?

SDC(Secure Device Connector)를 사용하여 **Cisco IOS(Internetwork Operating System)**를 실행하는 라이브 **Cisco** 디바이스를 온보딩할 수 있습니다. 시작하려면 [Cisco IOS 디바이스 온보딩](#)을 참조하십시오.

?

Security Devices(보안 디바이스) 페이지에서 디바이스를 삭제할 수 있습니다.

동기화 및 충돌 상태, 구축 동작, 규모 제한, ISR, ASR 및 SMA 디바이스에 대한 지원을 포함하여 Security Cloud Control의 디바이스 유형에 대한 FAQ(자주 묻는 질문)에 대해 알아봅니다.

ASA(Adaptive Security Appliance) ?

Cisco ASA에서는 고급 스테이트풀 방화벽 및 VPN 집선 디바이스 기능을 하나의 디바이스에서 제공하며 애드온 모듈과 통합된 서비스를 제공합니다. ASA에는 다중 보안 상황(가상 방화벽과 유사), 클러스터링(다중 방화벽을 단일 방화벽으로 통합), 투명(Layer 2) 방화벽 또는 라우팅(Layer 3) 방화벽 가동, 고급 검사 엔진, IPsec VPN, SSL VPN 및 클라이언트리스 SSL VPN 지원 등의 다양한 기능이 포함되어 있습니다. ASA는 가상 머신 또는 지원되는 하드웨어에 설치할 수 있습니다.

ASA ?

ASA 모델은 Security Cloud Control에 온보딩한 ASA 디바이스의 실행 중인 구성 파일의 사본입니다. ASA 모델을 사용하여 디바이스 자체를 온보딩하지 않고도 ASA 디바이스의 구성을 분석할 수 있습니다.

?

Security Cloud Control의 구성과 디바이스에 로컬로 저장된 구성이 동일한 경우.

?

Security Cloud Control에 저장된 구성이 변경되어 이제 디바이스에 로컬로 저장된 구성과 다른 경우.

?

디바이스의 구성이 Security Cloud Control(대역 외) 외부에서 변경되어 이제 Security Cloud Control에 저장된 구성과 다른 경우.

OOB(out-of-band) ?

Security Cloud Control 외부에서 디바이스가 변경된 경우. CLI 명령을 사용하거나 ASDM 또는 FDM과 같은 온디바이스 관리자를 사용하여 디바이스에서 직접 변경합니다. 대역 외 변경으로 인해 Security Cloud Control는 디바이스에 대해 "충돌 감지" 상태를 보고합니다.

?

디바이스를 Security Cloud Control에 등록한 후 Security Cloud Control는 해당 구성의 복사본을 유지 관리합니다. Security Cloud Control를 변경하면 Security Cloud Control는 디바이스 구성의 사본을 변경합니다. 변경 사항을 디바이스에 다시 "구축"하면 Security Cloud Control는 디바이스의 구성 복사본에 대한 변경 사항을 복사합니다. 다음 항목을 참조하십시오.

- [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#) 페이지 108

ASA ?

모든 명령 디바이스 활동 아래에 **Command Line Interface(명령줄 인터페이스)**를 클릭하여 ASA CLI를 사용합니다.

?

Security Cloud Control의 클라우드 아키텍처를 통해 수천 개의 디바이스로 확장할 수 있습니다.

Security Cloud Control Cisco Integrated Services Routers Aggregation Services Routers ?

Security Cloud Control를 사용하면 ISR 및 ASR에 대한 모델 디바이스를 생성하고 해당 구성을 가져올 수 있습니다. 그런 다음 가져온 구성을 기반으로 템플릿을 생성하고 일관된 보안을 위해 신규 또는 기존 ISR 및 ASR 디바이스에 배포할 수 있는 표준화된 구성으로 구성을 내보낼 수 있습니다.

Security Cloud Control SMA ?

아니요, Security Cloud Control는 현재 SMA를 관리하지 않습니다.

데이터 보호, 다단계 인증, OTP 로그인 오류, 보안 디바이스 커넥터 사용, 프라이빗 디바이스 연결성 및 VPN 터널 상태 확인을 포함한 보안 FAQ에 대해 알아봅니다.

Security Cloud Control "OTP" .

데스크톱 또는 모바일 디바이스 시계가 세계 시간 서버와 동기화되어 있는지 확인합니다. 시계가 1분 미만 또는 그 이상 동기화되지 않으면 잘못된 OTP가 생성될 수 있습니다.

Security Cloud Control ?

예. 보안 연결은 디바이스와 Security Cloud Control 플랫폼 간의 프로토콜로 사용되는 Security Cloud Control SDC를 사용하여 수행됩니다. 보안을 최우선으로 고려하여 설계된 Security Cloud Control 아키텍처를 사용하면 디바이스를 오가는 데이터를 완전히 분리할 수 있습니다.

IP ?

네트워크 내에 구축할 수 있고 외부 포트를 열 필요가 없는 Security Cloud Control SDC(Secure Device Connector)를 활용할 수 있습니다. SDC가 구축되면 내부(인터넷 라우팅 불가) IP 주소로 디바이스를 온보딩할 수 있습니다.

자세한 내용은 [SDC\(Secure Device Connector\)](#)를 참조하십시오.

SDC ?

아니요.

?

Security Cloud Control는 매시간 터널 연결 확인을 자동으로 수행하지만, 터널을 선택하고 연결 확인을 요청하여 임시 VPN 터널 연결 확인을 수행할 수 있습니다. 결과를 처리하는 데 몇 초가 걸릴 수 있습니다.

IP ?

예. 이름과 피어 IP 주소 모두에서 사용 가능한 필터 및 검색 기능을 사용하여 특정 VPN 터널 세부 정보를 검색하고 피벗합니다.

구축 경고, 대역 외 설정 차이, 충돌 해결 및 인증서 거부 문제를 포함하여, Security Cloud Control의 문제 해결 FAQ에 대해 알아봅니다.

Security Cloud Control " " . ?

전체 구성(Security Cloud Control 지원 명령 이상으로 수행된 변경 사항)을 디바이스에 구축할 때 오류가 발생하면 "변경 사항 확인"을 클릭하여 디바이스에서 사용 가능한 최신 구성을 가져옵니다. 이렇게 하면 문제가 해결

될 수 있으며 계속해서 **Security Cloud Control**를 변경하고 구축할 수 있습니다. 문제가 지속되면 **Contact Support**(지원 문의) 페이지에서 **Cisco TAC**에 문의하십시오.

(Security Cloud Control ,) Security Cloud Control Security Cloud Control . ?

Security Cloud Control가 기능을 확장함에 따라 더 나은 정책 및 디바이스 관리 분석을 위해 필요한 모든 데이터를 강화하고 유지하기 위해 디바이스 구성에서 추가 정보가 수집됩니다. 이는 관리되는 디바이스에서 발생한 변경 사항이 아니라 이미 존재하는 정보입니다. 충돌 감지 상태를 해결하는 것은 디바이스에서 변경 사항을 확인하고 발생한 변경 사항을 검토하여 쉽게 해결할 수 있습니다.

클레임 및 파킹된 디바이스, 초기 프로비저닝, FTD 디바이스가 **Cisco Cloud** 통해 온보딩되는 방법을 포함하여 **Security Cloud Control**의 제로 터치 프로비저닝 용어에 대한 **FAQ**에 대해 알아봅니다.

- 클레임됨 - **Security Cloud Control**에서 일련 번호 온보딩의 컨텍스트에서 사용됩니다. 일련 번호가 **Security Cloud Control** 테넌트에 온보딩된 경우 디바이스가 "클레임"됩니다.
- 파킹됨 - **Security Cloud Control**에서 일련 번호 온보딩의 컨텍스트에서 사용됩니다. **Cisco Cloud**에 연결되어 있고 **Security Cloud Control** 테넌트가 일련 번호를 요청하지 않은 경우 디바이스는 "파킹"됩니다.
- 초기 프로비저닝 - 초기 FTD 설정의 컨텍스트에서 사용됩니다. 이 단계에서 디바이스는 EULA를 수락하고, 새 비밀번호를 생성하고, 관리 IP 주소를 구성하고, FQDN을 설정하고, DNS 서버를 설정하고, FDM을 사용하여 디바이스를 로컬로 관리하도록 선택합니다.
- 제로 터치 프로비저닝 - 공장에서 고객 사이트(일반적으로 브랜치 오피스)로 FTD를 배송하고, 사이트의 직원이 FTD를 네트워크에 연결하고, 디바이스가 **Cisco Cloud**에 연결하는 프로세스입니다. 이 시점에서 일련 번호가 이미 "클레임"되었거나 **Security Cloud Control** 테넌트가 클레임할 때까지 FTD가 **Cisco Cloud**에 "파킹"된 경우 디바이스는 **Security Cloud Control** 테넌트에 온보딩됩니다.

네트워크 정책 관리를 사용하여 동일한 액세스 그룹 내에서 완전히 새도우 액세스 규칙을 식별하는 방법을 포함하여, **Security Cloud Control**에서 정책 최적화에 대한 **FAQ**를 알아봅니다.

() ?

Security Cloud Control NPM(네트워크 정책 관리)은 규칙 세트 내에서 상위 규칙이 다른 규칙을 가리고 있는지 식별하고 사용자에게 경고할 수 있습니다. 사용자는 모든 네트워크 정책 사이를 탐색하거나 필터링하여 모든 새도우 문제를 식별할 수 있습니다.



주

Security Cloud Control는 완전히 새도우 규칙만 지원합니다.

SDC IP 주소 변경 처리, 디바이스 IP 주소 업데이트, 매니지드 디바이스를 다시 연결하고 ASA 네트워킹 요구 사항을 충족하는 방법 등을 포함하여, **Security Cloud Control**의 연결성 **FAQ**에 대해 알아봅니다.

Secure Device Connector IP Security Cloud Control . ?

Security Cloud Control 내에서 새로운 SDC(Secure Device Connector)를 얻고 업데이트하려면 다음 명령을 사용하여 컨테이너를 다시 시작해야 합니다.

```
Stop Docker daemon>#service docker stop
Change IP address
Start Docker daemon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$
./cdo/toolkit/toolkit.sh restartSDC <tenant-name>
```

(FTD ASA) Security Cloud Control IP ?

정적 IP 주소의 변경이든 DHCP로 인한 IP 주소의 변경이든 어떤 이유로든 디바이스의 IP 주소가 변경되면, Security Cloud Control가 디바이스에 연결하는 데 사용하는 IP 주소를 변경할 수 있습니다(참조 [Security Cloud Control Firewall Management](#)에서 [디바이스의 IP 주소 변경](#) 페이지 90). 그런 다음 디바이스를 다시 연결합니다(참조 [Security Cloud Control Firewall Management](#)에 [디바이스 대량 재연결](#) 페이지 94). 디바이스를 다시 연결할 때 디바이스의 새 IP 주소를 입력하고 인증 자격 증명을 다시 입력하라는 메시지가 표시됩니다.

ASA Security Cloud Control ?

- ASDM 이미지가 있고 ASA에 대해 활성화되어 있습니다.
- 52.25.109.29, 52.34.234.2, 52.36.70.147에 대한 공용 인터페이스 액세스
- ASA의 HTTPS 포트는 443 또는 1024 이상의 값으로 설정해야 합니다. 예를 들어 포트 636으로 설정할 수 없습니다.
- 관리 중인 ASA도 AnyConnect VPN 클라이언트 연결을 허용하도록 구성된 경우 ASA HTTPS 포트를 1024 이상의 값으로 변경해야 합니다.

FTD 통신을 위한 관리 또는 데이터 인터페이스 사용, 외부 인터페이스에서의 원격 관리, 고가용성 지원, 주요 데이터 인터페이스 제한 사항을 비롯하여 데이터 인터페이스에 대해 배웁니다.

디바이스와 통신에 전용 관리 인터페이스 또는 일반 데이터 인터페이스를 사용할 수 있습니다. 외부 인터페이스에서 FTD를 원격으로 관리하거나 별도의 관리 네트워크가 없는 경우 데이터 인터페이스의 Security Cloud Control 액세스가 유용합니다. Security Cloud Control에서는 데이터 인터페이스에서 원격으로 관리되는 FTD의 고가용성을 지원합니다.

데이터 인터페이스에서의 FTD 관리 액세스에는 다음과 같은 제한이 있습니다.

- 하나의 물리적 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 Security Cloud Control를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.

Security Cloud Control

Security Cloud Control가 개인정보를 어떻게 처리하는지에 대한 FAQ를 확인하고, 개인 식별 정보 처리 세부 사항에 대한 Cisco의 개인정보 처리방침을 어디에서 찾을 수 있는지 알아봅니다.

Security Cloud Control가 개인 식별 정보를 처리하는 방법을 알아보려면 [Security Cloud Control 프라이버시 데이터 시트](#)를 참조하십시오.

Security Cloud Control

Security Cloud Control의 지원에 문의하고, 워크플로우 세부 정보를 내보내고, Cisco TAC 지원 티켓을 여는 방법, 그리고 Security Cloud Control의 서비스 상태 페이지를 확인하는 방법을 알아봅니다.

이 장에는 다음 섹션이 포함되어 있습니다.

지원 티켓을 열기 전에 경험 문제가 있는 디바이스의 워크플로우를 내보내는 것이 좋습니다. 이 추가 정보는 지원 팀이 문제 해결 노력을 신속하게 식별하고 편집하는 데 도움이 될 수 있습니다.

워크플로우를 내보내려면 다음 절차를 따르십시오.

1. 왼쪽 창에서 보안 디바이스를 클릭합니다.
2. **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
3. 적절한 디바이스 유형 탭을 클릭하고 문제 해결이 필요한 디바이스를 선택합니다.
필터 또는 검색 표시줄을 사용하여 문제를 해결해야 하는 디바이스를 찾으십시오. 디바이스를 선택하여 강조 표시합니다.
4. **Device Actions**(디바이스 작업) 창에서 **Workflows**(워크플로우)를 선택합니다.
5. 이벤트 표 위의 페이지 오른쪽 상단에 있는 **Export**(내보내기) 버튼을 클릭합니다. 파일은 자동으로 로컬에 .json 파일로 저장됩니다. TAC로 여는 이메일이나 티켓에 이것을 첨부하십시오.

TAC

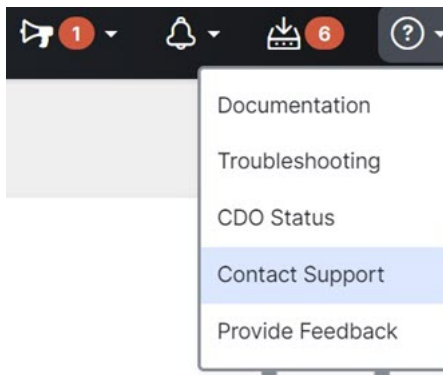
30일 평가판 또는 라이선스가 부여된 Security Cloud Control 어카운트를 사용하는 고객은 Cisco TAC(Technical Assistance Center)에서 지원 티켓을 열 수 있습니다.

- Security Cloud Control 고객이 TAC로 지원 티켓을 여는 방법.
- Security Cloud Control 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법.

Security Cloud Control TAC

이 섹션에서는 라이선스가 부여된 Security Cloud Control 테넌트를 사용하는 고객이 Cisco의 TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법을 설명합니다.

1. Security Cloud Control에 로그인합니다.
2. 테넌트 이름 옆에 있는 **help**(도움말) 버튼을 클릭하고 **Contact Support**(지원 문의)를 선택합니다.



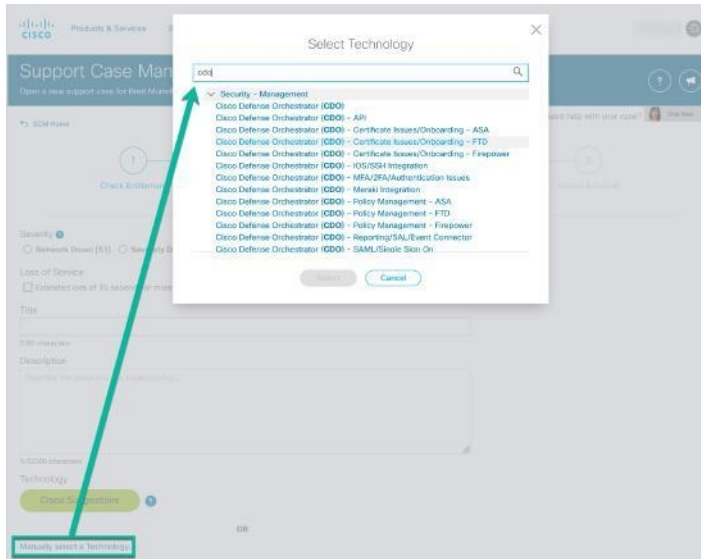
3. 지원 케이스 관리자를 클릭합니다.
4. 파란색 **Open New Case**(새 케이스 열기) 버튼을 클릭합니다.
5. **Open a Case**(케이스 열기)를 클릭합니다.
6. **Products and Services**(제품 및 서비스)를 선택한 다음 **Open Case**(케이스 열기)를 클릭합니다.
7. **Request Type**(요청 유형)을 선택합니다.
8. **Find Product by Service Agreement**(서비스 계약별 제품 찾기)행을 확장합니다.
9. 모든 필드를 입력합니다. 많은 필드가 명확합니다. 다음은 몇 가지 추가 정보입니다.
 - **Product Name(제품 이름) (PID)** - 이 번호가 더 이상 없는 경우 [Security Cloud Control 데이터 시트](#)를 참조하십시오.
 - **Product Description**(제품 설명) - PID에 대한 설명입니다.
 - **Site Name**(사이트 이름) - 사이트 이름을 입력합니다. 고객 중 한 명의 케이스를 여는 Cisco 파트너인 경우 고객의 이름을 입력합니다.
 - **Service Contract**(서비스 계약) - 서비스 계약 번호를 입력합니다.
 - 중요: 케이스를 Cisco.com 어카운트와 연결하려면 계약 번호를 Cisco.com 프로필에 연결해야 합니다. 이 절차를 사용하여 계약 번호를 Cisco.com 프로필에 연결합니다.
 - a. [Cisco Profile Manager](#)를 엽니다.
 - b. **Access Management**(액세스 관리) 탭을 클릭합니다.
 - c. **Add Access**(액세스 추가)를 클릭합니다.
 - d. **TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com**(TAC 및 RMA 케이스 생성, 소프트웨어 다운로드, 지원 툴, Cisco.com의 자격 콘텐츠)를 선택하고 **Go**(이동)를 클릭합니다.
 - e. 제공된 공간에 서비스 계약 번호를 입력하고 **Submit**(제출)를 클릭합니다. 서비스 계약 연결이 완료되었다는 알림이 이메일로 전송됩니다. 서비스 계약 연결을 완료하는 데 최대 6시간이 걸릴 수 있습니다.

중요사항

중요: 아래 링크에 액세스할 수 없는 경우 공인 Cisco 파트너 또는 리셀러, Cisco 어카운트 담당자 또는 Cisco 서비스 계약 정보를 관리하는 회사 내 담당자에게 문의하십시오.

10. **Next**(다음)를 클릭합니다.
11. **Describe Problem**(문제 설명) 화면에서 아래로 스크롤하여 **Manually select a Technology**(수동으로 기술 선택)를 클릭하고 검색 필드에 **Security Cloud Control**를 입력합니다.

12 요청과 가장 일치하는 범주를 선택하고 **Select(선택)**를 클릭합니다.



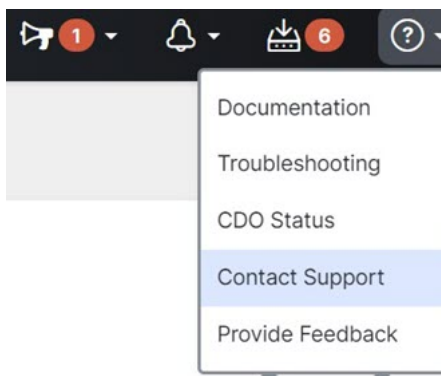
13 서비스 요청의 나머지 부분을 완료하고 **Submit(제출)**를 클릭합니다.

Security Cloud Control TAC

이 섹션에서는 Security Cloud Control 테넌트의 무료 평가판을 사용하는 고객이 Cisco TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법에 대해 설명합니다.

1. Security Cloud Control에 로그인합니다.

2. 테넌트 및 어카운트 이름 옆에 있는 **help(도움말)** 버튼을 클릭하고 **Contact Support(지원 문의)**를 선택합니다.



3. 아래에 문제 또는 요청 입력 필드에서 직면한 문제 또는 요청을 지정하고 **Submit(제출)**를 클릭합니다.

기술 정보와 함께 귀하의 요청이 지원 팀으로 전송되고 기술 지원 엔지니어가 귀하의 질문에 응답합니다.

Security Cloud Control

Security Cloud Control는 Security Cloud Control 서비스가 작동 중이고 서비스 중단이 있었는지 여부를 보여주는 고객 대면 서비스 상태 페이지를 유지 관리합니다. 일별, 주별 또는 월별 그래프로 가동 시간 정보를 볼 수 있습니다.

Security Cloud Control의 모든 페이지에 있는 도움말 메뉴에서 [Security Cloud Control Status](#)를 클릭하면 Security Cloud Control 상태 페이지에 도달할 수 있습니다.

상태 페이지에서 **Subscribe to Updates**(업데이트 구독)를 클릭하면 Security Cloud Control 서비스가 다운될 경우 알림을 받을 수 있습니다.

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.