



# **Cisco Security Cloud Control: Catalyst SD-WAN**

**Cisco Security Cloud Control**  
Updated NaN,



© 2025–2026 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](http://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)

|                                                                                        |           |
|----------------------------------------------------------------------------------------|-----------|
| <b>제 1 장 Security Cloud Control Firewall Management.....</b>                           | <b>5</b>  |
| Security Cloud Control Firewall Management의 개요.....                                    | 6         |
| Security Cloud Control Firewall Management 라이선스.....                                   | 6         |
| Security Cloud Control Firewall Management 플랫폼 유지 관리 일정.....                           | 7         |
| <b>제 2 장 Catalyst SD-WAN Manager를 Security Cloud Control와 통합합니다.....</b>               | <b>9</b>  |
| Catalyst SD-WAN와 Security Cloud Control Firewall Management 통합의 개요.....                | 10        |
| 시스템 토폴로지 다이어그램 .....                                                                   | 10        |
| Security Cloud Control를 사용하여 Catalyst SD-WAN Manager를 관리하는 엔드투엔드 워크플로우.....            | 12        |
| 최소 소프트웨어 요구 사항.....                                                                    | 13        |
| Security Cloud Control Firewall Management 및 Catalyst SD-WAN Manager의 RBAC 모델 정렬 ..... | 13        |
| Security Cloud Control에 Catalyst SD-WAN Manager 온보딩.....                               | 14        |
| Security Cloud Control에서 Catalyst SD-WAN Manager 디보딩.....                              | 16        |
| Security Cloud Control Firewall Management에서 Catalyst SD-WAN NGFW 기능을 관리하는 방법.....     | 17        |
| 침입 이벤트 보기.....                                                                         | 19        |
| 멀웨어 이벤트 보기.....                                                                        | 20        |
| 추가 리소스.....                                                                            | 20        |
| <b>제 3 장 Catalyst SD-WAN 디바이스 관리.....</b>                                              | <b>21</b> |
| Catalyst SD-WAN 디바이스 개요.....                                                           | 22        |
| Catalyst SD-WAN 디바이스에서 지원되는 작업.....                                                    | 22        |
| Catalyst SD-WAN 디바이스의 구성 보기.....                                                       | 22        |
| Security Cloud Control Firewall Management에서 정책 그룹 교차 실행.....                          | 23        |
| <b>제 4 장 Catalyst SD-WAN 보안 개체 및 보안 프로파일 관리.....</b>                                   | <b>25</b> |
| Catalyst SD-WAN 보안 개체 및 보안 프로파일의 개요.....                                               | 26        |
| 새 Catalyst SD-WAN 보안 개체 및 보안 프로파일을 생성합니다.....                                          | 26        |
| 애플리케이션 목록.....                                                                         | 27        |
| 데이터 접두사.....                                                                           | 28        |
| FQDN.....                                                                              | 28        |
| 지리위치.....                                                                              | 28        |
| Identity(ID).....                                                                      | 28        |
| 포트.....                                                                                | 29        |
| 프로토콜.....                                                                              | 29        |
| Security Group Tag(보안 그룹 태그).....                                                      | 29        |
| IPS 서명.....                                                                            | 30        |
| 허용 URL.....                                                                            | 30        |

|                                         |    |
|-----------------------------------------|----|
| URL 차단.....                             | 31 |
| 영역.....                                 | 31 |
| 고급 검사 프로파일.....                         | 31 |
| AMP(Advanced Malware Protection).....   | 32 |
| 침입 방지.....                              | 33 |
| TLS/SSL 해독.....                         | 33 |
| TLS/SSL 프로파일.....                       | 35 |
| URL 필터링.....                            | 35 |
| Catalyst SD-WAN 보안 개체 및 보안 프로파일 수정..... | 36 |
| Catalyst SD-WAN 보안 개체 삭제.....           | 37 |
| Catalyst SD-WAN 보안 개체 필터링 .....         | 38 |

## 제 5 장 Catalyst SD-WAN 보안 정책 관리.....41

|                                         |    |
|-----------------------------------------|----|
| Catalyst SD-WAN NGFW 보안 정책 소개.....      | 42 |
| 기존 Catalyst SD-WAN NGFW 보안 정책 관리.....   | 42 |
| Catalyst SD-WAN 보안 정책 생성.....           | 42 |
| Catalyst SD-WAN NGFW 정책에 정책 그룹 연결.....  | 47 |
| Catalyst SD-WAN Manager에서 정책 그룹 구축..... | 48 |

## 제 6 장 Cisco Security Analytics and Logging.....49

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| Security Cloud Control에서 Security Analytics and Logging(SaaS) 정보.....              | 50 |
| Security Cloud Control의 이벤트 유형.....                                                | 50 |
| Cisco Security Analytics and Logging(SaaS) 프로비저닝 해제.....                           | 50 |
| Security Analytics and Logging 라이선스.....                                           | 51 |
| Security Analytics and Logging 라이선스 구독.....                                        | 52 |
| Security Analytics and Logging 라이선스 정보 보기.....                                     | 53 |
| 보안 애널리틱스 및 로깅 데이터 계획 사용량 보기 및 이벤트 수집 속도.....                                       | 54 |
| Security Analytics and Logging 서비스 가용성 모니터링.....                                   | 55 |
| 이벤트 스토리지 기간 연장 및 이벤트 스토리지 용량 늘리기.....                                              | 56 |
| Security Analytics and Logging 알림 보기.....                                          | 57 |
| Security Analytics and Logging 라이선스에 대한 FAQ.....                                   | 57 |
| Catalyst SD-WAN에 대한 Security Analytics and Logging 개요.....                         | 58 |
| Catalyst SD-WAN 라우터가 Security Cloud Control Firewall Management와 이벤트를 공유하는 방법..... | 58 |
| 요건 및 지침.....                                                                       | 60 |
| Security Cloud Control Firewall Management에서 Catalyst SD-WAN 이벤트 보기.....           | 60 |

제

# 1 Security Cloud Control Firewall Management

---

장

- :
- Security Cloud Control Firewall Management □ □ □
  - Security Cloud Control Firewall Management □ □ □ □
  - Security Cloud Control Firewall Management □ □ □ □ □ □ □ □

이 문서에서는 사용자에게 방화벽 설정 및 관리, 보안 이벤트 모니터링을 위해 대시보드 맞춤 설정, Security Cloud Control의 새로운 기능 및 업데이트 소식을 안내합니다.

## 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 명칭: Cisco Defense Orchestrator 또는 CDO)는 클라우드 기반 보안 정책 관리 도구로, Cisco 방화벽은 물론 Cisco IOS 및 SSH와 같은 기타 디바이스 전반에 걸쳐 보안 정책을 간소화하고 통합하는 데 도움을 줍니다. 방화벽 및 디바이스는 Security Cloud Control 대시보드의 제품 아래에 나열된 방화벽에서 관리할 수 있습니다.

Security Cloud Control Firewall Management는 보안 정책 내의 불일치 사항을 파악하고 이를 수정할 수 있는 도구를 제공함으로써 보안 정책을 최적화할 수 있도록 도와줍니다. 개체 및 정책을 공유하고 설정 템플릿을 만드는 방법을 제공하여 디바이스 전반에 걸쳐 정책 일관성을 유지합니다.

Security Cloud Control Firewall Management은 ASDM(Adaptive Security Device Manager)과 함께 작동하므로, ASDM에서 수행된 구성 변경 사항을 추적하고 차이점을 조정합니다.

다양한 디바이스를 한 곳에서 관리할 수 있습니다. 기존 CLI 인터페이스에 몇 가지 개선 사항이 추가되어 고급 사용자가 관리 효율성을 더욱 높일 수도 있습니다.

Security Cloud Control Firewall Management은 또한 온프레미스 또는 클라우드 제공 Firewall Management Center에 위협 방어 디바이스를 신속하게 온보딩할 수 있도록 안내하는 "Day 0" 경험을 제공합니다. 또한 여러분이 활용할 수 있는 다른 주요 기능들을 제시하고, 이를 활성화하고 구성하는 데 도움을 줍니다.

### Cisco

Cisco Systems, Inc. 및 자회사("Cisco"로 통칭)에서는 개인 정보를 보호하고 사용자가 Cisco 웹사이트에서 그리고 Cisco 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 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.

- 기본: 1년, 3년 및 5년 동안의 구독을 제공하고 Security Cloud Control Firewall Management 조직에 액세스하고 적절하게 라이선스가 부여된 디바이스를 온보딩할 수 있는 권한을 제공합니다.
- 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 Management로 방화벽을 관리할 때 Security Analytics and Logging를 Security Cloud Control Firewall Management 구독과 결합하거나 Security Analytics and Logging 엔타이틀먼트를 별도의 구독으로 얻을 수 있습니다. Security Analytics and Logging 구독에 대한 자세한 내용은 [Security Analytics and Logging 라이선스](#) 페이지 51를 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.

#### 주

- 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 DNA(Cisco Digital Network Architecture) Essentials 또는 Advantage와 WAN Essentials 또는 Advantage 라이선스를 보유한 고객은 다른 라이선스 없이 이러한 기존 라이선스를 사용하여 통합에 사용할 수 있습니다. 그러나 Security Analytics and Logging에 액세스하려면 DNA Advantage(또는 WAN Advantage) 라이선스와 별도의 Security Analytics and Logging 라이선스가 필요합니다.

#### 주

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.

## 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.



주

- Security Cloud Control Firewall Management의 유지 관리 기간 동안에는 관리하는 디바이스에 구성을 생성하거나 구축하지 마십시오.
- Security Cloud Control Firewall Management과 통신이 중단되는 문제가 발생하면 Cisco는 해당 문제가 유지 보수 시간대 외의 시간대에 발생하더라도 영향을 받는 모든 테넌트에서 가능한 한 신속하게 해당 문제를 해결합니다.

# 제

## 2 Catalyst SD-WAN Manager Security Cloud Control .

---

### 장

:

- Catalyst SD-WAN Security Cloud Control Firewall Management □□□□□□
- □□□ □□□□ □□□□□□
- Security Cloud Control □ □□□□ Catalyst SD-WAN Manager □ □□□ □ □□□□ □□□□□
- □□ □□□□□ □□ □□
- Security Cloud Control Firewall Management □ Catalyst SD-WAN Manager □ RBAC □□ □□
- Security Cloud Control □ Catalyst SD-WAN Manager □□□
- Security Cloud Control □□ Catalyst SD-WAN Manager □□□
- Security Cloud Control Firewall Management □□ Catalyst SD-WAN NGFW □□□ □□□□ □□
- □□ □□□ □□
- □□□ □□□ □□
- □□ □□□

이 장에서는 Catalyst SD-WAN Manager와 Security Cloud Control를 통합하는 방법을 설명합니다.

## Catalyst SD-WAN Security Cloud Control Firewall Management

---

Security Cloud Control Firewall Management과 Catalyst SD-WAN Manager 통합을 통해 보안 정책을 효율적으로 구성, 모니터링 및 시행할 수 있으며, 지능형 위협 탐지, 로그 분석 및 AI 기반 문제 해결을 수행할 수 있습니다.

Catalyst 및 Secure Router 시리즈를 비롯한 Cisco SD-WAN 솔루션을 Cisco 보안 포트폴리오와 함께 사용하여 네트워크 보안 기능을 제어하고 관리할 수 있습니다.

Security Cloud Control Firewall Management과 Catalyst SD-WAN Manager의 통합을 통해 Cisco Catalyst SD-WAN 및 브랜치 WAN 환경에 대한 중앙 집중식 관리가 가능해집니다. 이를 통해 조직은 네트워크 전체에서 보안 정책을 설정, 모니터링 및 시행할 수 있습니다. 이 통합은 또한 Catalyst SD-WAN Manager에서의 고급 문제 해결, 규칙 최적화 및 변경 관리를 용이하게 합니다.

이점

이 통합을 통해 수행할 수 있는 작업은 다음과 같습니다.

- Security Cloud Control Firewall Management 대시보드를 사용하여 보안 정책 및 개체를 효율적으로 관리하고, 구성 및 편집하고, 변경 사항을 푸시합니다.
- 중앙 집중식 Security Cloud Control Firewall Management 대시보드에서 보안 위협을 효과적으로 모니터링하고 탐지합니다.
- Security Analytics and Logging에서 전송한 데이터로 Security Cloud Control Firewall Management 대시 보드의 로그 및 이벤트에서 발생하는 보안 위협을 분석합니다.

Security Cloud Control Firewall Management는 다음과 같은 기능을 제공합니다.

- 온보딩된 Catalyst SD-WAN Manager를 통해 기존 보안 구성 및 정책을 식별합니다.
- 플랫폼을 사용하여 새로운 보안 개체 및 정책을 생성할 수 있습니다.
- 여러 Cisco 솔루션에서 보안 개체, 정책 및 프로파일을 구현하기 위한 일관된 전략을 지원합니다.
- 로그 및 애널리틱스 데이터를 보는 기능을 제공합니다.
- 네트워크 내에서 탐지된 침입 및 멀웨어 이벤트를 보안 라우터에서 표시합니다.

---

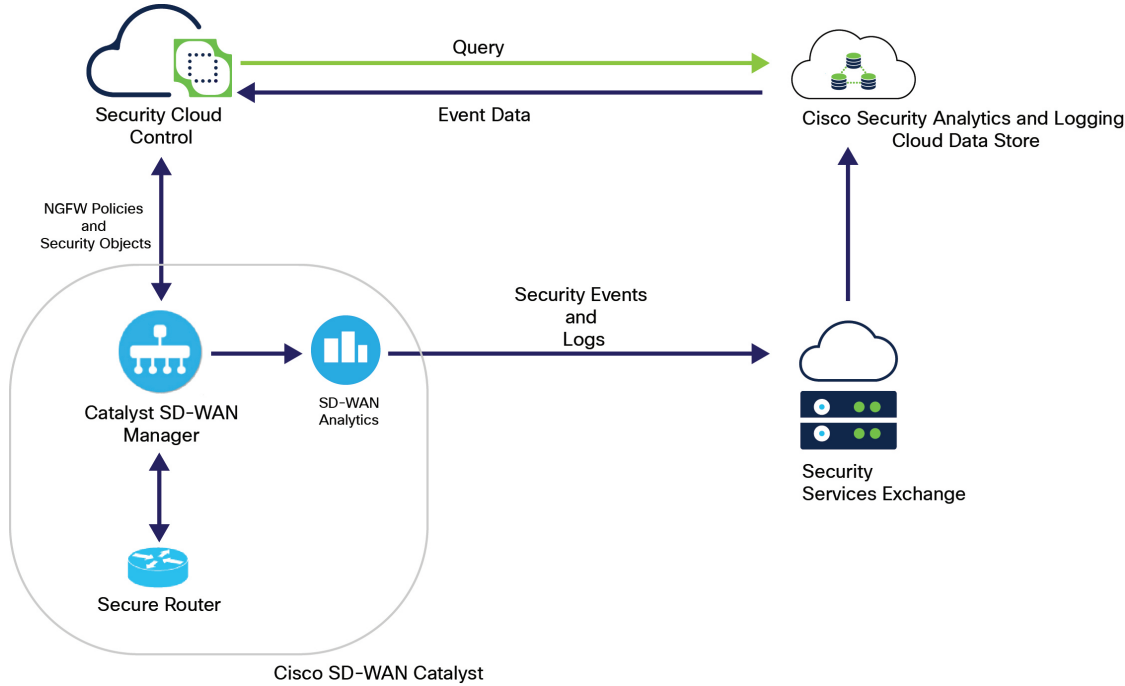
토폴로지 다이어그램은 Catalyst SD-WAN과 Security Cloud Control Firewall Management의 통합 및 기타 클라우드 서비스를 보여줍니다. 이는 정보의 흐름과 다양한 구성 요소 간의 상호 작용을 보여줍니다.

Security Cloud Control Firewall Management를 통해 Catalyst SD-WAN의 차세대 방화벽(NGFW) 기능을 관리하는 주된 용도는 Cisco의 보안 제품 전반에 걸쳐 보안 관리를 간소화하고 중앙 집중화하는 것입니다.

토폴로지 다이어그램은 Catalyst SD-WAN과 Security Cloud Control Firewall Management의 통합 및 기타 클라우드 서비스를 보여줍니다. 다이어그램은 정보의 흐름과 다양한 구성 요소 간의 상호 작용을 보여줍니다.



Cisco Catalyst 8000 및 Secure 8000 디바이스는 이하 '보안 라우터'로 총칭합니다.



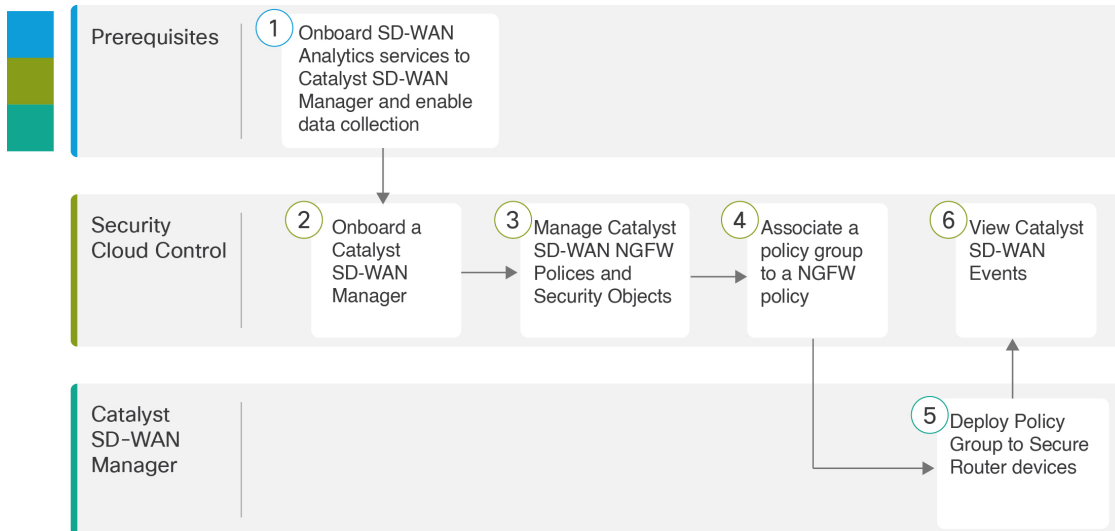
- **Security Cloud Control:** 보안 정책 시행 및 이벤트 상관관계 위한 중앙 지점 . 온보딩된 Catalyst SD-WAN Manager에서 NGFW(Next-Generation Firewall) 정책 및 보안 개체를 읽고, 고객이 이러한 NGFW 구성을 수정할 수 있도록 합니다. 또한 이벤트에 대해 Cisco Security Analytics and Logging 클라우드 데이터 저장소에 쿼리를 전송합니다.
- **Cisco Catalyst SD-WAN**는 다음과 같이 구성됩니다.
  - **Catalyst SD-WAN Manager:** SD-WAN 패브릭을 관리하고 온보딩될 경우 Security Cloud Control에 NGFW 정책 및 보안 개체를 표시합니다. Catalyst SD-WAN Manager는 보안 라우터에서 수신한 이벤트 데이터를 SD-WAN 애널리틱스로 전송합니다.
  - **SD-WAN 분석:** Security Services Exchange에 애널리틱스 데이터를 제공합니다.
  - **보안 라우터:** SD-WAN 에지 디바이스입니다.
- **Cisco Security Analytics and Logging Cloud** 데이터 저장소: 보안 애널리틱스 및 로깅 데이터를 위한 클라우드 기반 저장소입니다. 이는 SD-WAN 애널리틱스 엔진에서 분석 데이터를 가져오는 Security Services Exchange에서 보안 이벤트 및 로그를 수신합니다.
- **Security Services Exchange:** 다양한 Cisco 보안 서비스의 통합, 통신 및 관리를 용이하게 하도록 설계된 클라우드 기반 플랫폼입니다. SD-WAN 환경에서 수신한 보안 이벤트 및 로그를 전송하여 Cisco Security Analytics and Logging Cloud 데이터 저장소로 전달합니다.

## Security Cloud Control      Catalyst SD-WAN Manager

이 개념은 Security Cloud Control를 사용하여 Catalyst SD-WAN Manager의 방화벽 기능을 관리하기 위한 개략적인 엔드투엔드 워크플로우에 대해 설명합니다.

Catalyst SD-WAN Manager를 Security Cloud Control Firewall Management와 통합하면 Security Cloud Control 플랫폼을 통해 사용자가 NGFW(Next-Generation Firewall) 기능을 관리할 수 있습니다.

이 순서도는 Security Cloud Control를 사용하여 Catalyst SD-WAN Manager의 방화벽 기능을 관리하는 개괄적인 워크플로우를 보여줍니다.



| 단계 | 애플리케이션                  | 설명                                                                                                                                                                                      |
|----|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 사전 요건                   | SD-WAN 애널리틱스 서비스를 Catalyst SD-WAN Manager에 온보딩하고 데이터 수집을 활성화합니다. 자세한 내용은 <a href="#">Cisco SD-WAN 애널리틱스 온보딩</a> 을 참조하십시오.                                                               |
| 2  | Security Cloud Control  | Catalyst SD-WAN Manager를 온보딩합니다. 온보딩 프로세스에서는 연결된 보안 라우터 라우터도 가져옵니다. 자세한 내용은 <a href="#">Catalyst SD-WAN Manager를 Security Cloud Control와 통합합니다</a> . 페이지 9를 참조하십시오.                     |
| 3  | Security Cloud Control  | Catalyst SD-WAN 보안 개체, 보안 프로파일 및 NGFW(Next-Generation Firewall) 정책을 생성, 수정 또는 삭제합니다. 자세한 내용은 <a href="#">개체 및 프로파일 관리</a> 및 <a href="#">NGFW 정책 관리</a> 를 참조하십시오.                        |
| 4  | Security Cloud Control  | 정책 그룹을 Catalyst SD-WAN NGFW 정책에 연결합니다. 자세한 내용은 <a href="#">그룹 정책 연결</a> 을 참조하십시오.                                                                                                       |
| 5  | Catalyst SD-WAN Manager | 정책 그룹을 보안 라우터 라우터에 구축합니다. 자세한 내용은 <a href="#">정책 그룹 구성</a> 을 참조하십시오.                                                                                                                    |
| 6  | Security Cloud Control  | 모니터링 및 위협 탐지를 위해 Security Analytics and Logging을 사용하여 Catalyst SD-WAN에서 수신한 보안 이벤트를 확인합니다. 자세한 내용은 <a href="#">Catalyst SD-WAN 디바이스용 Security Analytics and Logging(SaaS)</a> 을 참조하십시오. |

이 개념은 Catalyst SD-WAN가 Security Cloud Control Firewall Management와 통합하는 데 Catalyst SD-WAN Manager 버전 20.18 이상이 필요함을 설명합니다. 보안 라우터 호환성은 이전 두 버전의 디바이스(예: 20.18의 경우 20.15 및 20.12)에 대한 Catalyst SD-WAN Manager 이전 버전과의 호환성 지원을 따릅니다.

Catalyst SD-WAN과 Security Cloud Control Firewall Management 통합을 위한 최소 소프트웨어 요구 사항:

- Catalyst SD-WAN Manager 지원되는 버전: 20.18 이상
- 보안 라우터 지원 버전: Catalyst SD-WAN Manager의 마지막 두 버전에서 지원되는 디바이스는 버전 20.18 이상과 호환됩니다. 예를 들어, Catalyst SD-WAN Manager 버전 20.18을 사용하는 경우, 버전 20.15 및 20.12의 디바이스는 호환됩니다.

Cisco TAC에 문의하여 호환되지 않는 인덱스를 확인하고 호환되지 않는 인덱스를 제거하십시오. 자세한 내용은 [Cisco SD-WAN 제어 구성 요소 호환성 매트릭스](#)를 참조하십시오.

## Security Cloud Control Firewall Management Catalyst SD-WAN Manager RBAC

이 개념은 Catalyst SD-WAN Manager 및 Security Cloud Control Firewall Management의 사용자 역할이 개별적으로 작동하며, 각 역할은 특정 책임에 의해 정의됩니다. 그러나 두 플랫폼의 RBAC(역할 기반 액세스 제어) 모델은 일관성과 원활한 사용자 작업을 제공하도록 정렬됩니다.

Catalyst SD-WAN Manager 및 Security Cloud Control Firewall Management의 사용자 역할은 독립적으로 작동하며, 각각 특정 책임에 따라 정의됩니다. 그러나 이러한 플랫폼 전반의 RBAC(역할 기반 액세스 제어) 모델은 일관되고 원활한 사용자 작업을 보장하도록 정렬됩니다.

Security Cloud Control Firewall Management에서 높은 권한을 가진 사용자라도, Catalyst SD-WAN Manager에서 맡은 역할의 권한이 더 낮다면 여전히 제한을 받을 수 있으며, 그 반대의 경우도 마찬가지입니다.

Catalyst SD-WAN Manager에서 적절한 권한 없이 Security Cloud Control Firewall Management의 변경 사항을 저장하려고 하면 오류가 발생합니다. 예를 들어, Security Cloud Control Firewall Management에서 특정 플랫폼에서 ‘슈퍼 관리자’ 역할을 할당받은 사용자는 해당 플랫폼에서 ‘운영자’ 역할을 가지고 있는 경우, NGFW 보안 정책 변경 사항을 Catalyst SD-WAN Manager에 저장할 수 없습니다.

이 표에서는 Catalyst SD-WAN Manager 및 Security Cloud Control Firewall Management에서 사용자 역할의 다양한 조합에 대한 액세스 권한을 간략하게 설명합니다.

### 1: Catalyst SD-WAN Manager Security Cloud Control Firewall Management RBAC

| Security Cloud Control Firewall Management 역할 이름 | Catalyst SD-WAN Manager 역할 이름 | 허용된 작업                                                                                                    |
|--------------------------------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------|
| 읽기 전용                                            | 운영자                           | Security Cloud Control Firewall Management에서 읽기 전용 액세스 허용됨<br><br>Catalyst SD-WAN Manager에서 읽기 전용 액세스 허용됨 |
| VPN 세션 관리자                                       | 운영자                           | Catalyst SD-WAN Manager에서 읽기 전용 액세스 허용됨                                                                   |

| Security Cloud Control Firewall Management 역할 이름 | Catalyst SD-WAN Manager 역할 이름 | 허용된 작업                                                                                                                                                           |
|--------------------------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 관리자                                              | security_operations           | Security Cloud Control Firewall Management에서 보안 정책을 생성/편집하도록 허용됨<br><br>Catalyst SD-WAN Manager에서 할당된 SecOps 사용자 역할                                              |
| 슈퍼 관리자                                           | security_operations           | Security Cloud Control Firewall Management의 모든 기능에 무제한 액세스<br><br>Catalyst SD-WAN Manager에서 할당된 SecOps 사용자 역할                                                    |
| 구축 전용                                            | 운영자                           | Security Cloud Control Firewall Management에서 보안 정책 생성/편집이 허용되지 않음<br><br>Catalyst SD-WAN Manager에서 읽기 전용 액세스 허용됨                                                 |
| 편집 전용                                            | security_operations           | Catalyst SD-WAN Manager 온보딩 또는 디보딩이 허용되지 않음<br><br>Security Cloud Control Firewall Management의 모든 기능에 무제한 액세스<br><br>Catalyst SD-WAN Manager에서 할당된 SecOps 사용자 역할 |

## Security Cloud Control Catalyst SD-WAN Manager

Security Cloud Control에 Catalyst SD-WAN Manager를 온보딩하는 방법, 스마트 계정 또는 가상 계정의 관리자 권한을 확인하는 방법, SD-WAN 조직 이름을 확인하는 방법, 그리고 클라우드 서비스, 분석 및 서비스 액세스 권한을 활성화하는 방법을 알아봅니다.

이 절차를 사용하여 Catalyst SD-WAN Manager를 Security Cloud Control 플랫폼에 온보딩합니다.

### 주

Catalyst SD-WAN Manager가 Security Cloud Control에 온보딩되면 Security Cloud Control에서만 보안 작업(정책, 개체 및 프로파일 관리)을 수행할 수 있습니다.

Security Cloud Control에서는 버전 제어 기능이 지원되지 않습니다.

- 온보딩하려는 조직 정보가 포함된 컨트롤러 프로파일에 연결된 가상 어카운트에 대해 스마트 어카운트 관리자 또는 가상 어카운트 관리자 권한을 보유하고 있어야 합니다.

어카운트 및 가상 어카운트에 대한 자세한 내용은 [Cisco Catalyst SD-WAN 포털 액세스](#)를 참고하십시오.

- 온보딩 중에 필요하므로, Catalyst SD-WAN Manager의 조직 이름을 알고 있어야 합니다.

1. Catalyst SD-WAN Manager에 로그인합니다.

2. **Administration(관리) > Settings(설정) > System(시스템) > Organization Name(조직 이름)**을 선택합니다.

조직 이름 필드에는 SD-WAN 환경 내에서 보안 제어 연결을 설정하는 고유 식별자가 포함되어 있습니다.

- 서비스 액세스 권한 부여를 활성화하여 온보딩 프로세스가 성공적으로 완료되도록 합니다.

1. Catalyst SD-WAN Manager에 로그인합니다.

2. **Administration(관리) > Settings(설정) > Cloud Services(클라우드 서비스)**를 선택합니다.

3. **Cloud Services(Cloud Services), Analytics(애널리틱스) 및 Service Access Authorization(서비스 액세스 권한 부여)**을 활성화합니다.



주

Catalyst SD-WAN Manager서 관리하는 모든 보안 라우터 디바이스는 **Device Status(디바이스 상태)**에 관계없이 Security Cloud Control에 온보딩됩니다.

- Security Cloud Control에 관리자 또는 슈퍼 관리자 역할이 있어야 합니다.

---

1. 왼쪽 창에서 **Administration(관리) > Integration(통합) > Catalyst SD-WAN**를 선택합니다.

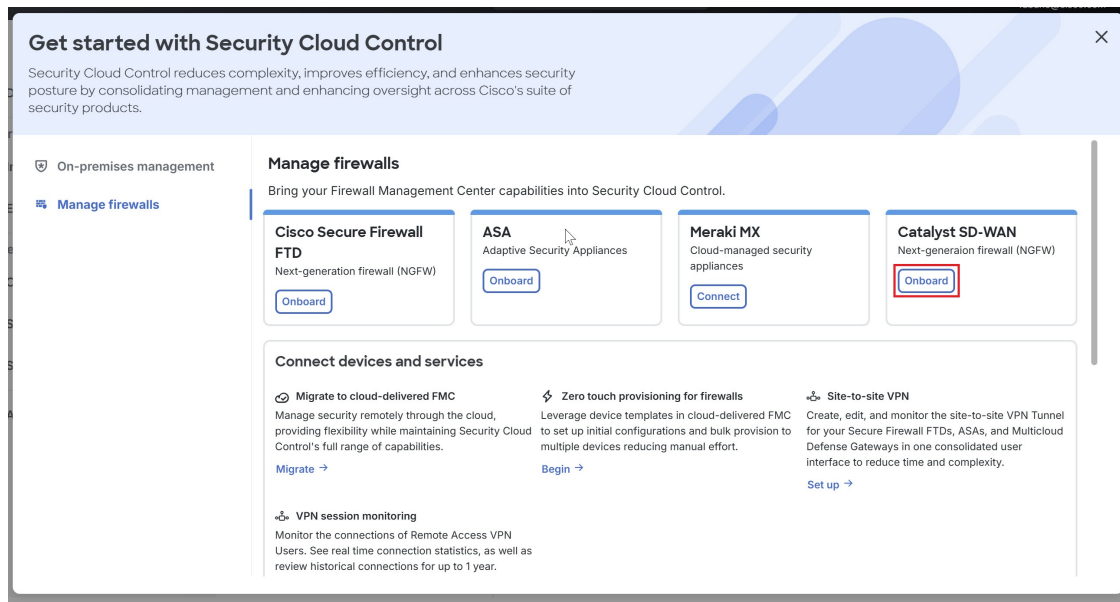
2. Catalyst SD-WAN 탭의 오른쪽 상단 모서리에 있는  아이콘을 클릭합니다.

3. **Security Cloud Control** 시작하기 인터페이스를 사용하여 Catalyst SD-WAN Manager를 온보딩할 수 있습니다.

- a. 상단 메뉴에서 를 클릭합니다.

- b. **Manage firewalls(방화벽 관리)** 탭을 클릭합니다.

- c. Catalyst SD-WAN 타일에서 **Onboard(온보드)**를 클릭합니다.



#### 4. Select Organization(조직 선택) 드롭다운 목록에서 조직을 선택합니다.

드롭다운에 표시되는 조직 목록은 Security Cloud Control이 구축된 지역을 기반으로 합니다.

#### 5. Create label(레이블 생성) 필드에 원하는 레이블을 입력하고 Connect(연결)을 클릭합니다.

디바이스를 Security Cloud Control에 온보딩하면 시스템에서 레이블을 적용합니다. 이 레이블을 사용하여 디바이스를 그룹화하고 Security Devices(보안 디바이스) 페이지에서 해당 디바이스를 필터링할 수 있습니다.

#### 6. 온보딩 중인 Catalyst SD-WAN Manager의 세부 정보를 확인한 다음 Close(닫기)를 클릭합니다.

Services(서비스) 페이지에 Catalyst SD-WAN에 온보딩된 관리자가 표시됩니다.

온보딩이 성공하면 다음과 같은 세부 정보가 Security Cloud Control에 표시됩니다.

- 모든 보안 개체, 보안 프로파일 및 NGFW 정책. 시스템은 Policies(정책) > WAN Branch Edge(브랜치 엣지)에 이러한 가져오기한 정책을 표시합니다.
- 보안 라우터 디바이스 및 해당 실행 중인 설정에 대한 세부 정보.

다음 작업: Management(관리) 창에서 Devices(디바이스)를 클릭하여 온보딩된 보안 라우터 디바이스를 확인합니다.

## Security Cloud Control Catalyst SD-WAN Manager

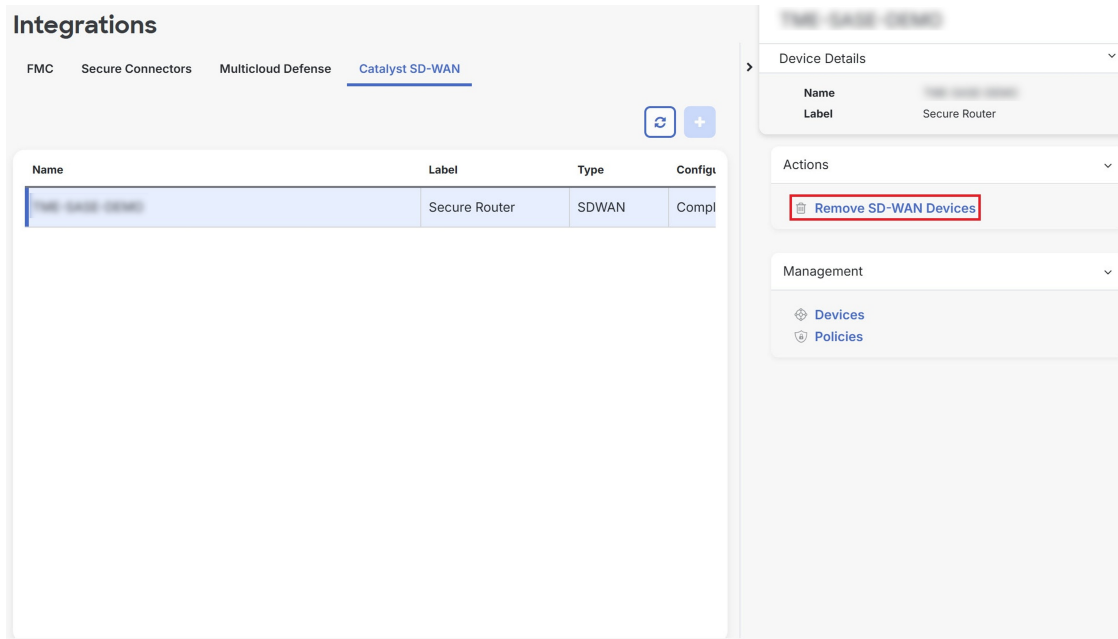
Security Cloud Control에서 Catalyst SD-WAN Manager을 디보딩하면 어떻게 관련 디바이스, NGFW 정책 및 보안 개체를 Security Cloud Control에서 자동으로 제거하는지 알아보십시오.

Deboarding Catalyst SD-WAN Manager from Security Cloud Control automatically removes its associated devices, policies, and objects from Security Cloud Control.



When you deboard Catalyst SD-WAN Manager from Security Cloud Control, all the policies and objects created through Security Cloud Control are deleted from Security Cloud Control but remain in Catalyst SD-WAN Manager. You can then edit security objects and policies from Catalyst SD-WAN Manager.

1. Choose **Administration(관리) > Integration(통합) > Catalyst SD-WAN**.
2. Select the manager that you want to delete and click **Remove SD-WAN Devices**.



3. Click **OK** to confirm the action.

## Security Cloud Control Firewall Management Catalyst SD-WAN NGFW

Security Cloud Control Firewall Management를 사용하면 Catalyst SD-WAN NGFW 정책에 대한 전역 검색 및 정책 그룹 연결을 사용하여 차세대 방화벽(NGFW) 정책, 보안 개체 및 프로파일을 생성, 수정 및 삭제할 수 있습니다. 변경 사항은 자동으로 Catalyst SD-WAN Manager에 저장되지만, Catalyst SD-WAN Manager를 통해 보안 라우터 디바이스에 수동으로 구축해야 합니다. Security Cloud Control Firewall Management에서 직접 디바이스를 구축하는 것은 지원되지 않습니다.

Catalyst SD-WAN Manager가 Security Cloud Control Firewall Management와 통합되면, 기존의 NGFW(Next-Generation Firewall) 정책, 보안 개체 및 보안 프로파일 을 Catalyst SD-WAN Manager에서 Security Cloud Control Firewall Management로 자동으로 가져옵니다. 이러한 NGFW 매개변수를 수정하거나 Security Cloud Control Firewall Management에서 새 매개변수를 생성할 수 있습니다. Security Cloud Control Firewall Management에서 변경한 모든 내용은 동기화되고 Catalyst SD-WAN Manager에 저장됩니다.

Catalyst SD-WAN Manager을 Security Cloud Control Firewall Management에 온보딩한 후에는 더 이상 Catalyst SD-WAN Manager을 통해 정책, 개체 또는 프로파일을 관리할 수 없습니다. 이러한 규칙은 Security Cloud Control Firewall Management에서만 관리해야 합니다.

통합을 나타내는 "SCC(Security Cloud Control)에 의해 관리됨" 배너가 Security Cloud Control Firewall Management에 온보딩된 Catalyst SD-WAN Manager에 표시됩니다. 이 메시지는 Catalyst SD-WAN Manager에서 관련 구성 섹션으로 이동하면 볼 수 있습니다.

- 보안 개체 및 프로파일의 경우: **Configuration(구성) > Policy Groups(정책 그룹) > Objects(개체) 및 Profiles(프로파일) > Security Objects(보안 개체)**를 선택합니다.
- NGFW 정책의 경우: **Configuration(그상) > Policy Groups(정책 그룹) > NGFW**를 선택합니다.

Catalyst SD-WAN Manager와 Security Cloud Control Firewall Management 통합의 제한 사항

- 클라우드 연결은 필수입니다.  
Catalyst SD-WAN Manager는 온프레미스 또는 Cisco Cloud에서 호스팅될 수 있습니다. 제대로 작동하려면 클라우드 연결이 있어야 합니다. Catalyst SD-WAN Manager가 NAT 디바이스 뒤에 있는 경우, 지원되지만 제한이 있습니다. 특히 클라우드 연결을 활성화하려면 포트 443(Https)만 열어야 합니다.
- Catalyst SD-WAN Manager를 디보딩하여 NGFW 정책, 보안 개체 및 보안 프로파일을 편집합니다.  
Catalyst SD-WAN Manager에서 NGFW 정책, 보안 개체 및 보안 프로파일을 변경하려면, Security Cloud Control Firewall Management에서 이를 디보딩해야 합니다.
- 사용자 지정 IPS 프로파일은 지원되지 않음  
보안 프로파일 내의 IPS 정책(서명 세트 개체)을 편집하거나 사용자 지정할 수 없습니다.
- Cisco Security Analytics and Logging(SAL)에서는 라이브 로그를 사용할 수 없음  
Security Cloud Control Firewall Management에서 SAL 을 사용하여 라이브 로그를 볼 수 없습니다. 과거 이벤트만 볼 수 있습니다.
- Security Cloud Control Firewall Management사용자의 사용자 역할 권한을 신중하게 수정하십시오.  
Security Cloud Control Firewall Management에 속한 사용자의 경우 Catalyst SD-WAN Manager에서 사용자 역할 권한을 변경할 때는 주의하십시오. Security Cloud Control Firewall Management 연결된 사용자에 대한 권한을 수정하면 구성이 실패할 수 있습니다.
- 온프레미스 멀티테넌트 Catalyst SD-WAN Manager은 지원되지 않음  
Catalyst SD-WAN Manager의 온프레미스 멀티테넌트 구축은 버전 20.18.1의 경우 Security Cloud Control Firewall Management에서 지원되지 않습니다. 이 릴리스에서는 단일 테넌트 Catalyst SD-WAN Manager 구축만 Security Cloud Control Firewall Management와 호환됩니다.
- 다크 모드는 지원되지 않음  
Catalyst SD-WAN Manager가 통합되면 Security Cloud Control Firewall Management에서 다크 모드가 비활성화됩니다.



주

NGFW 정책, 개체 및 프로파일 변경은 Security Cloud Control Firewall Management에서 디보딩된 후 Catalyst SD-WAN Manager에서만 수행할 수 있습니다.

Security Cloud Control Firewall Management에서 다음 작업을 수행할 수 있습니다.

- NGFW 정책, 보안 개체 및 보안 프로파일을 생성하거나, 수정하거나, 삭제합니다.

- 전역 검색 기능 사용하여 디바이스 전반에서 보안 개체를 검색합니다.
- 정책 그룹을 Catalyst SD-WAN NGFW 정책과 연결합니다.

Security Cloud Control Firewall Management에서 NGFW 정책, 보안 개체 및 보안 프로파일에 대한 변경 사항이 Catalyst SD-WAN Manager에 자동으로 저장됩니다. 단, 업데이트된 구성을 Catalyst SD-WAN Manager를 사용하여 수동으로 보안 라우터 디바이스에 구축해야 합니다. 이러한 변경 사항을 Security Cloud Control Firewall Management에서 디바이스로 직접 푸시할 수 없습니다.

IPS(Intrusion Prevention System) dashlet은 Cisco Talos 위협 인텔리전스를 사용하여 차단된 네트워크 공격과 허용된 네트워크 공격을 강조 표시합니다. 이 대시보드 보기는 Catalyst SD-WAN Manager 보안 모니터 IPS/AMP dashlet에 매핑됩니다.

IPS(Intrusion Prevention System)를 사용하면 Cisco Talos 위협 인텔리전스를 기반으로 네트워크 침입 및 악의적인 활동을 탐지하고 차단할 수 있습니다.

Security Cloud Control Firewall Management 대시 보드의 상위 침입 및 멀웨어 이벤트 dashlet은 Catalyst SD-WAN Manager **Security(보안)** 탭에 있는 **Monitor(모니터)** 페이지의 **Intrusion Prevention(침입 방지)** 및 **Advanced Malware Protection(고급 멀웨어 보호)** dashlets에 매핑됩니다.

1. **Dashboard(대시보드)**를 클릭합니다.
2. 상위 침입 및 멀웨어 이벤트 dashlet으로 이동합니다.
3. **Data Sources(데이터 소스)** 아래에서 **SDWAN**을 클릭합니다.
4. **Intrusion Events(침입 이벤트)** 탭을 클릭합니다.
5. dashlet 근처의 드롭다운에서 **Blocked(차단됨)**를 선택합니다.  
기본적으로 **Allowed(허용됨)**가 선택되어 있습니다.

Top Intrusion & Malware Events Last 90 days ▾ ⋮

Data Sources: All FTD **SDWAN**

Intrusion Events Malware Events

| Name                             | Priority | Count |
|----------------------------------|----------|-------|
| PROTOCOL - DNS Hosts and DNS ... | Medium   | 12    |
| MALWARE - DNS DNS Port Four ...  | High     | 4     |

Blocked ^  
 Allowed  
**Blocked**

6. Catalyst SD-WAN Manager에서 표시할 이벤트를 클릭합니다.  
Catalyst SD-WAN Manager **Monitor(모니터링)** 페이지의 교차 실행 창이 나타납니다.
7. 이벤트를 보려면 **Intrusion Prevention(침입 방지)** dashlet으로 이동합니다.

Advanced Malware Protection(AMP) 이벤트 dashlet을 확인하여 악의적인, 알 수 없는, 정상인 파일 수를 시간 경과에 따라 보여줍니다. 이 대시보드 보기는 Catalyst SD-WAN Manager 보안 모니터 IPS/AMP dashlet에 매핑됩니다.

**Advanced Malware Protection(AMP) 이벤트 dashlet**은 선택한 기간 동안 AMP에서 식별한 악의적인, 알 수 없는 파일 및 정상 파일의 개수를 표시합니다. AMP는 파일 평판을 기반으로 멀웨어를 차단하고 추가 분석을 위해 알 수 없는 파일을 Cisco AMP Threat Grid에 업로드합니다.

Security Cloud Control Firewall Management 대시 보드의 상위 침입 및 멀웨어 이벤트 dashlet은 Catalyst SD-WAN Manager **Security(보안)** 탭에 있는 **Monitor(모니터)** 페이지의 **Intrusion Prevention(침입 방지)** 및 **Advanced Malware Protection(고급 멀웨어 보호)** dashlets에 매핑됩니다.

1. **Dashboard(대시보드)**를 클릭합니다.
2. 상위 침입 및 멀웨어 이벤트 **dashlet**으로 이동합니다.
3. **Data Sources(데이터 소스)** 아래에서 **SDWAN**을 클릭합니다.
4. **Malware Events(멀웨어 이벤트)** 탭을 클릭합니다.
5. dashlet 근처의 드롭다운에서 **Blocked(차단됨)**를 선택합니다. 기본적으로 **Allowed(허용됨)**가 선택되어 있습니다.

## Top Intrusion & Malware Events

Data Sources: All FTD SDWAN

Intrusion Events Malware Events

Blocked

| Detection Name | File SHA256                                                                     | Count |
|----------------|---------------------------------------------------------------------------------|-------|
| Malicious      | 07192322e254ad3271509f5a2c2158336320150a9028715032a6715034712170415037a0b671503 | 10000 |

Last 90 days

6. Catalyst SD-WAN Manager에서 표시할 이벤트를 클릭합니다.
- Catalyst SD-WAN Manager **Monitor**(모니터링) 페이지의 교차 실행 창이 나타납니다.
7. 이벤트를 확인하려면 **Advanced Malware Protection** dashlet으로 이동합니다.

이 개념은 Catalyst SD-WAN 구성 가이드 및 정책 그룹 구성 가이드와 같은 추가 리소스를 제공합니다.

- Cisco Catalyst SD-WAN 보안 구성 가이드
- 정책 그룹 구성 가이드, Cisco IOS XE Catalyst SD-WAN
- Security Cloud Control과 Cisco Catalyst SD-WAN Manager 통합

제

## 3 Catalyst SD-WAN

---

장

:

- Catalyst SD-WAN □□□□ □□
- Catalyst SD-WAN □□□□□□ □□□□  
□ □□
- Catalyst SD-WAN □□□□□ □□ □□
- Security Cloud Control Firewall  
Management□□ □□ □□ □□ □□

Security Cloud Control을 사용하면 Security Devices (Security 디바이스) 페이지에서 온보딩된 디바이스의 디바이스 구성을 보고 Catalyst SD-WAN Manager의 정책 그룹 페이지를 교차 실행할 수 있습니다.

## Catalyst SD-WAN

온보딩된 디바이스 및 템플릿 보기, 디바이스 구성 검토, 정책 그룹 실행, 디바이스 제거 등을 포함하여, 에서 Security Cloud Control Firewall Management을 Catalyst SD-WAN를 관리하는 방법을 알아봅니다.

Catalyst SD-WAN 디바이스는 안전한 고성능 연결성 제공하도록 설계된 고급 네트워킹 솔루션입니다. 이러한 디바이스는 SD-WAN 기능과 강력한 보안 기능을 통합하여 조직이 멀티 클라우드 환경, 브랜치 오피스 및 데이터 센터 전반에 걸쳐 사용자를 애플리케이션에 원활하게 연결할 수 있도록 합니다. Security Cloud Control Firewall Management는 Catalyst SD-WAN 디바이스에 대한 중앙 집중식 가시성과 보안 정책 관리 기능을 제공합니다.

## Catalyst SD-WAN

Security Cloud Control 방화벽 관리에서 온보딩된 디바이스 및 템플릿 보기, 디바이스 설정 검토, 정책 그룹 실행, 디바이스 제거 등 Catalyst SD-WAN 디바이스를 관리하는 방법을 알아봅니다.

Catalyst SD-WAN 디바이스는 관련 Catalyst SD-WAN Manager가 온보딩된 후 Security Cloud Control Firewall Management를 통해 관리할 수 있는 온보딩된 WAN 브랜치 에지 또는 보안 라우터 디바이스입니다. Security Cloud Control Firewall Management에서는 **Security Devices(보안 디바이스)** 페이지에서 온보딩된 디바이스를 확인, 관리 및 제거할 수 있습니다. **Security Devices(보안 디바이스)** 페이지에서 다음을 수행할 수 있습니다.

- 별도의 탭에서 온보딩된 디바이스 및 템플릿을 봅니다.  
자세한 내용은 [보안 디바이스 정보 페이지](#)를 참조하십시오.
- 온보딩된 디바이스의 구성 파일을 확인합니다.
- Catalyst SD-WAN 플랫폼에서 정책 그룹을 실행합니다.



주

하나의 Security Cloud Control Firewall Management 조직만 단일 Catalyst SD-WAN Manager에 온보딩할 수 있습니다.

## Catalyst SD-WAN

Security Cloud Control 방화벽 관리에서 온보딩된 디바이스 및 템플릿 보기, 디바이스 설정 검토, 정책 그룹 실행, 디바이스 제거 등 Catalyst SD-WAN 디바이스를 관리하는 방법을 알아봅니다.

Security Cloud Control Firewall Management에서는 **Security Devices(보안 디바이스)** 페이지에서 온보딩된 디바이스의 구성 정보를 확인할 수 있습니다.



1. **Manage(관리) > Security Devices(보안 디바이스)**를 선택합니다.
2. **WAN Branch Edge(WAN 브랜치 에지)** 탭을 클릭합니다.
3. 디바이스를 선택하고 **Management(관리)** 아래에서 **Configuration(구성)**을 클릭합니다.

The screenshot shows the 'Security Devices' management interface. At the top, there are tabs for 'Devices' and 'Templates'. A search bar is present. Below the tabs, there are filters for 'All', 'ASA', 'AWS VPC', 'WAN Branch Edge' (selected), and 'FTD'. A table displays a list of devices. The table has columns for 'Name', 'Connectivity', 'Site Name', and 'Device Model'. One device is highlighted in blue. To the right of the table, there is a 'Device Details' panel with fields for 'Hostname', 'Device Model', 'Site Name', 'Device Health', and 'Policy Group'. Below this, there is a 'Management' section with a red box around the 'Configuration' link.

4. 디바이스 목록을 CSV 파일로 내보내려면 내보내기 아이콘(📄)을 클릭합니다.

## Security Cloud Control Firewall Management

Security Cloud Control 방화벽 관리에서 온보딩된 디바이스 및 템플릿 보기, 디바이스 설정 검토, 정책 그룹 실행, 디바이스 제거 등 Catalyst SD-WAN 디바이스를 관리하는 방법을 알아봅니다.

Security Cloud Control Firewall Management를 사용하면 온보딩된 Catalyst SD-WAN Manager에 대해 Catalyst SD-WAN Manager의 **Policy Groups**(정책 그룹) 페이지로 교차 실행할 수 있습니다.

1. **Manage(관리) > Security Devices(보안 디바이스)**를 선택합니다.
2. **WAN Branch Edge(WAN 브랜치 에지)** 탭을 클릭합니다.
3. 디바이스를 선택하고 **Management(관리)** 아래에서 **Policy Groups(정책 그룹)**를 클릭합니다.

Security Devices

Y

Devices

Templates

Q

Search by Device Name, IP Address, or

Displaying 30 of 12 results

?

C

⏮

+

AllASAAWS VPCWAN Branch EdgeFTD

| <div><input type="checkbox"/></div> | Name                        | Connectivity | Site Name     | Device Model |  |
|-------------------------------------|-----------------------------|--------------|---------------|--------------|--|
| <input type="checkbox"/>            | San Francisco Branch        | Unreachable  | San Francisco | Cisco        |  |
| <input type="checkbox"/>            | London Office Edge 2        | Online       | London        | Cisco        |  |
| <input type="checkbox"/>            | London Office Branch        | Unreachable  | London        | Cisco        |  |
| <input type="checkbox"/>            | New York Branch             | Unreachable  | New York      | Cisco        |  |
| <input checked="" type="checkbox"/> | New York Branch             | Online       | New York      | Cisco        |  |
| <input type="checkbox"/>            | London Branch (uplink only) | Online       | London        | Cisco        |  |

Rows per page501 - 12 of 121

New York Branch

Clear selection

Device Details

Hostname

Device Model

Site Name

Device Health

Policy Group

Management

Configuration

Policy Groups

# 제

## 4 Catalyst SD-WAN

---

### 장

:

- Catalyst SD-WAN □□ □□ □ □□ □□□□ □□
- □ Catalyst SD-WAN □□ □□ □ □□ □□□□□ □□□□□.
- Catalyst SD-WAN □□ □□ □ □□ □□□ □□
- Catalyst SD-WAN □□ □□ □□
- Catalyst SD-WAN □□ □□ □□□

이 문서에서는 사용자에게 Catalyst SD-WAN 보안 개체 및 프로파일을 생성, 수정, 삭제 및 관리하는 방법을 안내하여 SD-WAN 환경 내에서 네트워크 보안 정책을 정확하게 시행하고 애플리케이션, 트래픽 및 액세스 설정을 효율적으로 제어할 수 있도록 지원합니다.

## Catalyst SD-WAN

Catalyst SD-WAN Manager의 보안 개체 및 보안 프로파일은 차세대 방화벽(NGFW) 보안 정책을 생성하고 시행하는 데 필수적입니다. 끊임 없는 연결과 최적화된 애플리케이션 성능을 보장하면서 사이버 위협으로부터 네트워크를 보호하므로 강력한 네트워크 보안 관리와 효과적인 NGFW 정책 구현에 필수적입니다.

Catalyst SD-WAN 보안 개체 및 보안 프로파일은 차세대 방화벽(NGFW) 보안 정책을 생성 및 시행하고 사이버 위협으로부터 네트워크를 보호하고, 끊임 없는 연결을 보장하며, 애플리케이션 성능을 최적화하는 데 필수적입니다. 이러한 구성 요소는 Catalyst SD-WAN 보안 정책 제어를 위해 Security Cloud Control Firewall Management가 가져오기, 관리, 동기화하는 재사용 가능한 정책 구성 요소입니다. 이는 강력한 네트워크 보안 관리와 효과적인 NGFW 정책 구현에 필수적입니다.

## Catalyst SD-WAN

Security Cloud Control Firewall Management를 사용하여 새 Catalyst SD-WAN 보안 개체 및 보안 프로파일을 생성합니다.

Security Cloud Control Firewall Management를 사용하여 새 Catalyst SD-WAN 보안 개체 및 보안 프로파일을 생성합니다.

1. 개체를 선택합니다.
2. WAN Branch Edge(WAN 브랜치 에지) 탭을 클릭합니다.
3. Create Object(개체 생성) (+) 아이콘을 클릭합니다.

**Objects**

Firewall **WAN Branch Edge**

74 Search for objects by name, IP, or port number Displaying 50 of 55 objects

|                          | Name                     | References | Type                        |
|--------------------------|--------------------------|------------|-----------------------------|
| <input type="checkbox"/> | WAN-Edge                 | 0          | Data Prefix                 |
| <input type="checkbox"/> | WAN-Edge                 | 0          | Data Prefix                 |
| <input type="checkbox"/> | WAN-Edge                 | 0          | Data Prefix                 |
| <input type="checkbox"/> | WAN-Edge                 | 0          | Data Prefix                 |
| <input type="checkbox"/> | Cloud-Malware-protection | 0          | Advanced Malware Protection |
| <input type="checkbox"/> | Cloud-Malware-protection | 1          | Intrusion Prevention        |
| <input type="checkbox"/> | Cloud-Net                | 2          | Data Prefix                 |
| <input type="checkbox"/> | Cloud-Net                | 2          | Zone                        |

4. 생성하려는 개체 또는 프로파일을 클릭합니다.

개체:

- 애플리케이션 목록
- 데이터 접두사
- FQDN

- [지리위치](#)
- [ID](#)
- [포트](#)
- [프로토콜](#)
- [보안 그룹 태그](#)
- [서명](#)
- [URL 허용](#)
- [URL 차단](#)
- [Zone](#)

프로파일:

- [고급 검사 프로파일](#)
- [AMP\(Advanced Malware Protection\)](#)
- [침입 방지](#)
- [TLS/SSL 해독](#)
- [TLS/SSL 프로파일](#)
- [URL 필터링](#)

5. **Save(저장)**를 클릭합니다.

개체는 Security Cloud Control Firewall Management에서 생성됩니다. Catalyst SD-WAN Manager의 로그를 보려면 **Monitor(모니터) > Logs(로그) > Audit Logs(감사 로그)**로 이동합니다..

애플리케이션 목록 개체는 애플리케이션을 NGFW 정책에서 사용할 애플리케이션을 목록으로 그룹화합니다.

애플리케이션 목록 개체는 NGFW 정책에서 사용할 애플리케이션을 목록으로 그룹화합니다.

2:

| 필드                   | 설명                                                                                                                                                                                                                                 |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 개체 이름                | 애플리케이션 목록의 이름입니다.                                                                                                                                                                                                                  |
| 애플리케이션 또는 애플리케이션 제품군 | <p>애플리케이션은 정책 설정을 위해 함께 그룹화된 특정 애플리케이션의 모음입니다. 이를 통해 관리자는 여러 애플리케이션에 대한 트래픽 규칙을 단일 엔터티로 정의하고 관리할 수 있습니다. 예: "Webex", "Microsoft Teams", "Zoom."</p> <p>애플리케이션 제품군은 기능 범주를 기준으로 애플리케이션을 그룹화합니다. 예: "웹", "인스턴트 메시징", "네트워크 서비스".</p> |

**Selected Items(선택한 항목)** 필드에 선택한 항목이 표시됩니다.

데이터 접두사 개체는 **SD-WAN** 패브릭 내에서 트래픽 라우팅 정책을 정의하고 관리하는 데 사용되는 특정 IP 주소 범위 또는 접두사입니다.

데이터 접두사 개체는 **SD-WAN** 패브릭 내에서 트래픽 라우팅 정책을 정의하고 관리하는 데 사용되는 특정 IP 주소 범위 또는 접두사입니다.

### 3:

| 필드      | 설명                 |
|---------|--------------------|
| 개체 이름   | 데이터 접두사 개체의 이름입니다. |
| 데이터 접두사 | 데이터 접두사 값입니다.      |

## FQDN

**FQDN(Fully Qualified Domain Name)** 개체는 데이터 센터 또는 프라이빗 클라우드의 독립형 서버를 일치시키는 데 사용됩니다. 공용 URL을 매칭할 때 권장되는 일치 작업은 삭제입니다.

**FQDN(Fully Qualified Domain Name)** 개체는 데이터 센터 또는 프라이빗 클라우드의 독립형 서버를 일치시키는 데 사용됩니다. 공용 URL을 일치시킬 때 권장되는 일치 작업은 삭제입니다. 공개 URL에 대해 검사 기능을 사용하는 경우, 관련된 모든 하위 URL과 리디렉션 URL을 정의해야 합니다.

### 4: FQDN

| 필드    | 설명                                             |
|-------|------------------------------------------------|
| 개체 이름 | FQDN 개체의 이름입니다.                                |
| FQDN  | 검표로 구분된 URL 이름입니다. 예를 들어 <b>cisco.com</b> 입니다. |

지리위치 개체를 사용하면 IP 주소가 아닌 지리적 위치를 기반으로 방화벽 규칙을 구성할 수 있습니다.

지리위치 개체를 사용하면 IP 주소가 아닌 지리적 위치를 기반으로 방화벽 규칙을 구성할 수 있습니다.

### 5:

| 필드    | 설명                                                                       |
|-------|--------------------------------------------------------------------------|
| 개체 이름 | 지리위치 개체의 이름입니다.                                                          |
| 지리위치  | 드롭다운 목록에서 하나 이상의 지리위치를 선택합니다. 예를 들어, 아프리카, 남극 대륙, 아시아 또는 유럽을 입력할 수 있습니다. |

## Identity(ID)

ID 개체는 **SD-WAN** 패브릭 내에서 사용자 ID 및 사용자 그룹을 나타내는 데 사용되는 보안 개체입니다. 이 ID 정보는 **SD-WAN** 패브릭에 통합되어 ID 기반 방화벽 정책 및 마이크로 세그멘테이션을 활성화합니다.

ID 개체는 **SD-WAN** 패브릭 내에서 사용자 ID 및 사용자 그룹을 나타내는 데 사용되는 보안 개체입니다. 이 ID 정보는 **SD-WAN** 패브릭에 통합되어 ID 기반 방화벽 정책 및 마이크로 세그멘테이션을 활성화합니다.

**6: ID**

| 필드     | 설명                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------|
| 개체 이름  | ID 개체의 이름입니다.                                                                                                                      |
| 사용자    | 사용자 및 사용자 그룹의 소스는 <b>Catalyst SD-WAN Manager</b> 에서 구성된 <b>Cisco ISE(Cisco Identity Services Engine) AD(Active Directory)</b> 입니다. |
| 사용자 그룹 |                                                                                                                                    |

포트 개체는 **SD-WAN** 패브릭 내 디바이스에 대한 포트 관련 설정을 정의하고 관리하는 데 사용되는 구성 요소입니다.

포트 개체는 **SD-WAN** 패브릭 내에서 디바이스의 포트 관련 설정을 정의하고 관리하는 데 사용되는 구성 요소입니다.

**7:**

| 필드    | 설명                                          |
|-------|---------------------------------------------|
| 개체 이름 | 포트 개체의 이름입니다.                               |
| 포트    | 범위로 구분된 포트 값입니다.<br>범위는 <b>0~65535</b> 입니다. |

보안 정책 내에서, 사전 정의된 목록(예: **TCP, UDP, ICMP**)에서 프로토콜을 선택하여 트래픽 관리 및 보안 시행을 위한 특정 규칙을 정의할 수 있습니다.

보안 정책의 사전 정의된 목록(예: **TCP, UDP, ICMP**)에서 프로토콜 개체를 선택하여 트래픽 관리 및 보안 시행을 위한 특정 규칙을 정의할 수 있습니다.

**8:**

| 필드    | 설명                                                                                        |
|-------|-------------------------------------------------------------------------------------------|
| 개체 이름 | 프로토콜 개체의 이름입니다.                                                                           |
| 프로토콜  | 드롭다운 목록에서 하나 이상의 프로토콜 이름을 선택합니다. 예를 들어, <b>SNMP, TCP, UDP, ICMP, Echo, Telnet</b> 이 있습니다. |

**Selected Items**(선택한 항목) 필드에 선택한 항목이 표시됩니다.

**Security Group Tag(     )**

**Cisco ISE(Identity Services Engine)**를 사용하여 **Cisco TrustSec** 네트워크에서 트래픽을 분류하기 위해 **SGT(Security Group Tag)**를 정의하고 사용하여, **SGT**를 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다.

**Cisco ISE(Identity Services Engine)**를 사용하여 **Cisco TrustSec** 네트워크에서 트래픽을 분류하기 위해 **SGT(Security Group Tag)**를 정의하고 사용하는 경우, **SGT**를 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다.

SGT는 Security Cloud Control Firewall Management에서 생성하거나 편집할 수 없습니다. 모든 SGT는 ISE에서 생성해야 합니다.

#### 9: Security Group Tag( )

| 필드       | 설명                            |
|----------|-------------------------------|
| 개체 이름    | 보안 그룹 태그의 이름입니다.              |
| 보안 그룹 태그 | 해당 확인란을 선택하여 보안 그룹 태그를 선택합니다. |

**Selected Items**(선택한 항목) 필드에 선택한 항목이 표시됩니다.

## IPS

Catalyst SD-WAN Manager의 IPS 서명 개체는 네트워크 공격을 탐지하고 방지하기 위해 IPS(Intrusion Prevention System)에서 사용하는 규칙 세트를 의미합니다.

IPS 서명 개체는 네트워크 공격을 탐지하고 방지하기 위해 IPS(Intrusion Prevention System)에서 사용하는 규칙 집합을 나타냅니다. CVSS(Common Vulnerability Scoring System) 점수가 9 이상인 취약성을 차단합니다. 또한 멀웨어 CPU, 익스플로잇 키트, SQL 인젝션 또는 차단 목록의 규칙 범주에 속하는 경우 지난 2년 내에 게시된 CVE(Common Vulnerabilities and Exposures)를 차단합니다.

#### 10: IPS

| 필드     | 설명                                                                          |
|--------|-----------------------------------------------------------------------------|
| 개체 이름  | 개체의 이름입니다.                                                                  |
| IPS 서명 | 생성자 ID:서명 ID 형식의 IPS 서명이며, 쉼표로 구분됩니다. 예: 1234:5678.<br>범위는 0~4294967295입니다. |

## URL

Catalyst SD-WAN Manager의 허용 URL 개체는 SD-WAN URL 필터링 기능을 통해 명시적으로 허용해야 할 URL을 정의하는 데 사용됩니다.

허용 URL 개체는 SD-WAN URL 필터링 기능을 통해 명시적으로 허용되어야 하는 URL을 정의하는 데 사용됩니다.

이러한 목록에서 다음과 같은 몇 가지 중요 유의 사항이 있습니다.

- 허용된 URL에는 범주 기반 필터링이 적용되지 않습니다.
- 허용된 목록과 차단된 목록 모두에 동일한 항목이 설정된 경우 트래픽이 허용됩니다.
- 트래픽이 허용 목록 또는 차단 목록과 일치하지 않는 경우 범주 기반 및 평판 기반 필터링을 거칩니다.

#### 11: URL

| 필드     | 설명                |
|--------|-------------------|
| 개체 이름  | 허용 URL 개체의 이름입니다. |
| 허용 URL | 허용할 URL입니다.       |

## URL

Catalyst SD-WAN Manager의 URL 차단 개체는 SD-WAN URL 필터링 기능을 통해 거부되어야 하는 URL을 정의하는 데 사용됩니다.

**URL** 차단 개체는 SD-WAN URL 필터링 기능을 통해 거부되어야 하는 URL을 정의하는 데 사용됩니다.

### 12: URL

| 필드     | 설명                |
|--------|-------------------|
| 개체 이름  | URL 차단 개체의 이름입니다. |
| URL 차단 | 차단할 URL입니다.       |

Catalyst SD-WAN Manager의 영역 개체는 트래픽 제어를 위한 보안 경계를 정의하는 데 사용됩니다.

영역 개체는 트래픽 제어를 위한 보안 경계를 정의하는 데 사용됩니다. 영역은 **VPN** 또는 인터페이스를 기반으로 구성할 수 있습니다.

- 영역은 결제 처리 네트워크, 기업 사용자 또는 게스트의 로컬 인터넷 등 특정 **VPN**에 대해 생성할 수 있습니다. 이러한 영역을 사용하면 **VPN** 내부 또는 **VPN** 간의 트래픽에 보안 정책을 적용할 수 있습니다.
- 영역에 인터페이스를 할당할 수도 있습니다. 예를 들어 **Ethernet**, **GigabitEthernet** 또는 기타 인터페이스 유형은 영역으로 그룹화할 수 있습니다. 이를 통해 인터페이스 간의 트래픽을 세부적으로 제어할 수 있습니다.

### 13:

| 필드                       | 설명                                                                                                                                                                                                                           |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 개체 이름                    | 영역의 이름입니다.                                                                                                                                                                                                                   |
| <b>VPN</b>               | 영역 유형이 <b>VPN</b> 인 영역을 구성하려면 선택합니다. 드롭다운 목록에서 영역에 <b>VPN</b> 을 추가합니다. 다음과 같은 옵션을 사용할 수 있습니다. <ul style="list-style-type: none"> <li>● 지불 처리 네트워크</li> <li>● 기업 사용자</li> <li>● 게스트용 로컬 인터넷</li> <li>● 물리적 보안 디바이스</li> </ul> |
| <b>Interface</b> (인터페이스) | 영역 유형을 인터페이스로 사용하여 영역을 구성하려면 선택합니다. <b>Add Interface</b> (인터페이스 추가) 드롭다운 목록에서 영역에 인터페이스를 추가합니다.                                                                                                                              |

**Selected Items**(선택한 항목) 필드에 선택한 항목이 표시됩니다.

디바이스 레벨에서 전역 고급 검사 프로파일(**AIP**)을 적용합니다. 이렇게 하면 디바이스의 사전 정의된 규칙과 일치하는 모든 트래픽은 고급 검사 프로파일을 사용하여 철저하게 검사됩니다.

디바이스 레벨에서 전역 고급 검사 프로파일(**AIP**)을 적용합니다. 이렇게 하면 디바이스의 사전 정의된 규칙과 일치하는 모든 트래픽은 **AIP**를 사용하여 철저하게 검사됩니다.

## 14:

| 필드                                      | 설명                                                                                                                                                 |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 개체 이름                                   | 고급 검사 프로파일의 이름입니다.                                                                                                                                 |
| 침입 방지                                   | 드롭다운 목록에서 침입 방지 옵션을 선택합니다.                                                                                                                         |
| URL 필터링                                 | 드롭다운 목록에서 URL 필터를 선택합니다.                                                                                                                           |
| <b>AMP(Advanced Malware Protection)</b> | Advanced Malware Protection 옵션을 선택합니다.                                                                                                             |
| <b>TLS 작업</b>                           | TLS 작업을 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다. <ul style="list-style-type: none"> <li>● 암호 해독</li> <li>● 통과</li> <li>● Do not decrypt(암호 해독 안 함)</li> </ul> |

**AMP(Advanced Malware Protection)**

지능형 멀웨어 보호 정책은 지능형 멀웨어 보호 기능을 통합 보안 정책 프레임워크에 통합하도록 특별히 설계된 보안 정책입니다.

**AMP(Advanced Malware Protection)** 정책은 **AMP(고급 멀웨어 방지)** 기능을 통합 보안 정책 프레임워크에 통합하기 위해 특별히 설계된 보안 정책입니다.



주

일부 고급 설정의 경우, Catalyst SD-WAN에서 Threat Grid Server(위협 그리드 서버) 구성이 필요합니다.

**15: AMP(Advanced Malware Protection)**

| 필드                 | 설명                                                                                                               |
|--------------------|------------------------------------------------------------------------------------------------------------------|
| 개체 이름              | Advanced Malware Protection 정책의 이름입니다.                                                                           |
| <b>AMP 클라우드 지역</b> | <b>AMT</b> 클라우드 지역은 Cisco SD-WAN 클라우드 아키텍처와 연결된 <b>AMT(Analytics, Management, and Telemetry)</b> 클라우드 지역을 의미합니다. |
| 알림 로그 레벨           | 모든 시스템 로그 메시지는 저장할 시스템 로그 메시지의 심각도를 나타내는 우선순위 레벨과 연결되어 있습니다.                                                     |
| 파일 분석              | 업로드된 파일에 대한 파일 분석을 활성화합니다.                                                                                       |
| <b>TG</b> 클라우드 지역  | 지역을 선택합니다. Threat Grid(TG) 클라우드 서비스가 호스팅되는 지리적 지역을 의미합니다.                                                        |
| 파일 형식              | 분석할 파일 유형을 선택합니다.                                                                                                |

침입 방지 정책 프로파일은 사전 정의된 규칙과 서명을 활용하여 알려진 네트워크 공격을 탐지하고 차단하도록 설계된 보안 기능입니다.

**Intrusion Prevention(침입 방지)** 정책 프로파일은 사전 정의된 규칙 및 서명을 활용하여 알려진 네트워크 공격을 탐지하고 차단하도록 설계된 보안 기능입니다.

#### 16:

| 필드            | 설명                                                                                                                                                                                                                       |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 개체 이름         | 침입 방지 정책의 이름입니다.                                                                                                                                                                                                         |
| 서명 세트         | 트래픽 평가를 위한 규칙을 정의하는 서명 세트를 <b>Signature Set(서명 세트)</b> 드롭다운 목록에서 선택합니다.                                                                                                                                                  |
| 검사 모드         | <b>Inspection Mode(검사 모드)</b> 를 선택합니다.                                                                                                                                                                                   |
| 사용자 지정 서명 세트: | 드롭다운 목록에서 하나 이상의 웹 범주를 선택합니다.<br>사용자 지정 서명은 <b>Administration(관리) &gt; Settings(설정) &gt; External Services(외부 서비스) &gt; UTD Snort Subscribe Signature(UTD Snort 구독 서명) &gt; 아래의 Catalyst SD-WAN Manager에서 활성화해야 합니다.</b> |
| 서명 허용 목록      | 서명 허용 목록을 선택합니다.                                                                                                                                                                                                         |
| 알림 로그 레벨      | 알림 로그 레벨을 선택합니다.<br>이는 시스템에서 생성된 로그의 심각도 레벨을 의미하며, 기록되는 정보의 세분성을 제어하도록 구성할 수 있습니다.                                                                                                                                       |

## TLS/SSL

Catalyst SD-WAN Manager의 TLS/SSL 해독 프로파일은 관리자가 네트워크를 통과하는 암호화된 트래픽을 검사하고 관리할 수 있게 해주는 기능 또는 구성을 의미합니다.

관리자는 **TLS/SSL** 암호 해독 프로파일을 사용하여 네트워크 내에서 암호화된 트래픽을 검사하고 관리할 수 있습니다.

### 주

Security Cloud Control Firewall Management에서 **TLS/SSL** 암호 해독 프로파일을 생성하기 전에, **Configuration(구성) > Certificates(인증서) > Certificate Authority(인증 기관)** 아래의 Catalyst SD-WAN Manager에서 인증 기관(CA)을 구성해야 합니다.

#### 17: TLS/SSL

| 필드        | 설명                                             |
|-----------|------------------------------------------------|
| 개체 이름     | TLS/SSL 해독 정책의 이름입니다. 이름은 최대 32자까지 사용할 수 있습니다. |
| 서버 인증서 확인 |                                                |

| 필드              | 설명                                                                                                                                                                                |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 만료된 인증서         | <p>서버 인증서가 만료된 경우 정책이 수행할 작업을 정의합니다. 다음과 같은 옵션을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> <li>● 삭제: 트래픽 삭제</li> <li>● 암호 해독: 트래픽 암호 해독</li> </ul>                        |
| 신뢰할 수 없는 인증서    | <p>서버 인증서를 신뢰할 수 없는 경우 정책이 수행할 작업을 정의합니다. 다음과 같은 옵션을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> <li>● 삭제: 트래픽 삭제</li> <li>● 암호 해독: 트래픽 암호 해독</li> </ul>                   |
| 인증서 해지 상태       | <p>서버 인증서의 해지 상태를 확인하기 위해 OCSP(Online Certificate Status Protocol)를 사용해야 하는지 여부를 정의합니다. 사용 가능한 옵션은 <b>Enabled(활성화)</b> 또는 <b>Disabled(비활성화)</b>입니다.</p>                           |
| 알 수 없는 해지 상태    | <p>OCSP 해지 상태가 알 수 없음인 경우 정책 작업을 정의합니다.</p> <ul style="list-style-type: none"> <li>● 삭제: 트래픽 삭제</li> <li>● 암호 해독: 트래픽 암호 해독</li> </ul>                                            |
| 지원되지 않는 모드 확인   |                                                                                                                                                                                   |
| 지원되지 않는 프로토콜 버전 | <p>지원되지 않는 프로토콜 버전을 정의합니다.</p> <ul style="list-style-type: none"> <li>● Drop(삭제): 지원되지 않는 프로토콜 버전을 삭제합니다.</li> <li>● No Decrypt(암호 해독 안 함): 지원되지 않는 프로토콜 버전을 암호 해독합니다.</li> </ul> |
| 지원되지 않는 암호 그룹   | <p>지원되지 않는 암호 그룹을 정의합니다.</p> <ul style="list-style-type: none"> <li>● Drop(삭제): 지원되지 않는 암호 그룹을 삭제합니다.</li> <li>● No Decrypt(암호 해독 안 함): 지원되지 않는 암호 그룹을 암호 해독합니다.</li> </ul>       |
| 실패 모드           | <p>실패 모드를 정의합니다. 옵션은 <b>Close(닫기)</b> 및 <b>Open(열기)</b>입니다.</p>                                                                                                                   |
| 인증서 번들          | <p>기본 CA를 사용하려면 <b>Use Default CA Certificate(기본 CA 인증서 사용)</b> 확인란을 선택합니다.</p>                                                                                                   |
| 최소 TLS 버전       | <p>프록시가 지원해야 하는 TLS의 최소 버전을 설정합니다. 사용 가능한 옵션: TLS 1.0, TLS 1.1 또는 TLS 1.2</p>                                                                                                     |
| 프록시 인증서 속성      |                                                                                                                                                                                   |
| RSA 키 쌍 모듈      | <p>프록시 인증서 RSA 키 모듈을 정의합니다. 사용 가능한 옵션: 1024-bit RSA, 2048-bit RSA 또는 4096-bit RSA</p>                                                                                             |
| EC 키 유형         | <p>키 유형을 정의합니다. 사용 가능한 옵션: P256, P384 또는 P521</p>                                                                                                                                 |
| 인증서 수명(일)       | <p>프록시 인증서의 수명(일)을 설정합니다.</p>                                                                                                                                                     |

## TLS/SSL

Catalyst SD-WAN Manager의 TLS/SSL 프로파일 정책은 통합 보안 정책 내에서 암호화된 트래픽을 관리하는 데 사용됩니다.

**TLS/SSL** 프로파일 정책은 통합 보안 정책 내에서 암호화된 트래픽을 관리하는 데 사용됩니다. Security Cloud Control Firewall Management에서 TLS/SSL 프로파일 정책을 생성하려면 먼저 Catalyst SD-WAN에서 인증 기관(CA) 인증서를 구성해야 합니다. 이는 TLS 프록시 기능을 활성화하기 위한 사전 조건입니다.

### 18: TLS/SSL

| 필드              | 설명                                                                                  |
|-----------------|-------------------------------------------------------------------------------------|
| 개체 이름           | TLS/SSL 프로파일의 이름입니다.                                                                |
| 작업을 할당할 범주      | 범주를 설정하고 암호 해독, 암호 해독 안 함 및 통과 URL 범주 등의 작업을 할당합니다.<br>또는 여러 범주를 선택하고 작업을 설정합니다.    |
| 평판              | 평판을 활성화하여 <b>Decrypt Threshold</b> (임계값 암호 해독)를 선택합니다.<br>URL 평판 레벨에 기반한 작업을 지원합니다. |
| 도메인 암호 해독 목록    | 도메인 암호 해독 목록을 선택합니다.                                                                |
| 도메인 암호 해독 목록 없음 | 도메인 암호 해독 목록 없음을 선택합니다.                                                             |
| 암호 해독 실패        | 암호 해독에 실패한 경우 암호 해독 실패 옵션을 활성화합니다.                                                  |

## URL

Catalyst SD-WAN Manager의 URL 필터링 프로파일 정책은 관리자가 범주, 평판 및 맞춤형 목록을 기준으로 웹사이트에 대한 액세스를 제어할 수 있는 보안 기능입니다.

**URL** 필터링 프로파일 정책은 관리자가 범주, 평판, 맞춤형 목록을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있는 보안 기능입니다.

### 19: URL

| 필드    | 설명                                                      |
|-------|---------------------------------------------------------|
| 개체 이름 | URL 필터링 정책의 이름입니다.                                      |
| 웹 범주  | 웹 범주를 선택합니다. 사용 가능한 옵션은 차단 및 허용입니다. 웹 사이트는 범주로 분류됩니다.   |
| 웹 평판  | 드롭다운 목록에서 웹 평판을 선택합니다.<br>URL에는 위험 수준에 따라 평판 점수가 할당됩니다. |
| 허용 목록 | 허용 URL 목록을 선택합니다.                                       |
| 차단 목록 | 차단 URL 목록을 선택합니다.                                       |

| 필드        | 설명                                                                                                                                                                                                                                                           |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 페이지 서버 차단 | <p>다음 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> <li>● <b>Block Page Content</b>(페이지 콘텐츠 차단): 기본 콘텐츠 헤더 및 콘텐츠 본문을 입력합니다.</li> <li>● <b>Redirect URL</b>(리디렉션 URL): 리디렉션 URL을 입력합니다.</li> </ul> <p>차단된 사용자는 맞춤형 페이지로 리디렉션하거나 메시지를 표시할 수 있습니다.</p> |
| 알림 및 로그   | <p>알림 및 로그 유형을 선택합니다.</p> <ul style="list-style-type: none"> <li>● 차단 목록</li> <li>● 허용 목록</li> <li>● 평판/범주</li> </ul>                                                                                                                                        |

## Catalyst SD-WAN

Security Cloud Control Firewall Management의 Catalyst SD-WAN 보안 개체 및 보안 프로파일과 연결된 값을 편집합니다.

이 절차를 사용하여 Security Cloud Control Firewall Management의 Catalyst SD-WAN 보안 개체 및 보안 프로파일과 연결된 값을 편집할 수 있습니다.

1. **Administration(관리) > Integration(통합) > Catalyst SD-WAN**을(를) 선택합니다.
2. 개체을(를) 선택합니다.
3. **WAN Branch Edge(WAN 브랜치 에지)** 탭을 클릭합니다.
4. 수정할 보안 개체 또는 프로파일을 선택합니다. 개체를 찾으려면 **필터**를 사용합니다.
5. **Actions(작업)** 창에서 **Edit(편집)**를 클릭합니다.  
변경하려는 구성을 수정합니다.
6. **Save(저장)**를 클릭하여 확인합니다.

## Editing SDWAN Zone



Object Name \*

Employees\_zone

☒ VPN ☐ Interface

Zone

Select one or more VPN(s)

☐ Corporate\_Users☐ CorporateUsers☒ Employees☐ home-guests☐ IOT\_OT☐ Local\_Internet\_for\_Guests☐ OOB☐ Payment\_Processing\_Network

Selected items:

Employees x

Cancel

Save

## Catalyst SD-WAN

정책, 개체 또는 구성에서 참조하지 않는 경우 **Security Cloud Control Firewall Management**에서 **Catalyst SD-WAN** 보안 개체를 삭제할 수 있습니다. 개체를 삭제하기 전에 보안 정책에서 해당 개체에 대한 모든 참조를 수동으로 제거해야 합니다. 시스템은 추적 가능성 및 컴플라이언스를 위해 삭제된 개체를 로깅합니다.

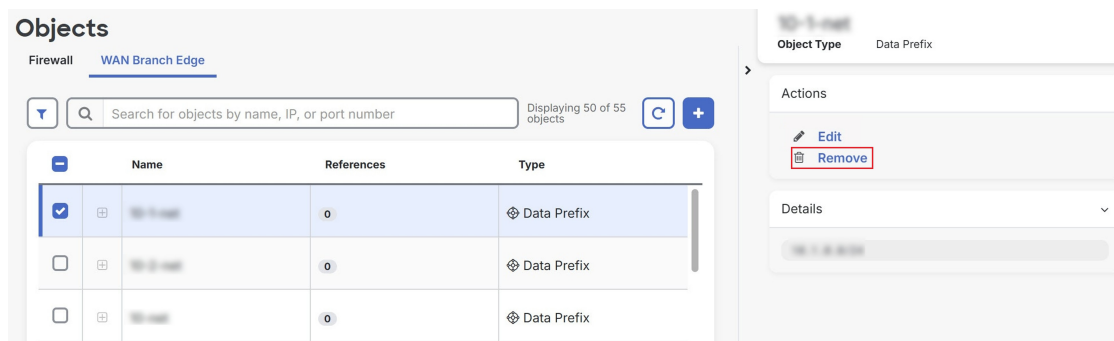
Catalyst SD-WAN 보안 개체 하나 또는 여러 개를 삭제할 수 있습니다.

- 보안 개체가 **Catalyst SD-WAN Manager**와 동기화된 경우 이를 삭제하면 일관성을 위해 **Security Cloud Control Firewall Management**와 **Catalyst SD-WAN Manager** 모두 업데이트됩니다.
- 삭제된 개체를 참조하는 보안 정책 또는 구성은 자동으로 삭제되지 않습니다. 개체를 삭제하기 전에 보안 정책에서 참조를 수동으로 제거해야 합니다.
- 감사 및 추적 가능성을 위해 삭제 작업이 로깅됩니다.

삭제할 **Catalyst SD-WAN** 보안 개체가 다른 개체, 정책 또는 구성에서 사용되거나 참조되고 있지 않은지 확인하십시오.

1. **Administration(관리) > Integration(통합) > Catalyst SD-WAN**을(를) 선택합니다.
2. 개체을(를) 선택합니다.
3. **WAN Branch Edge(WAN 브랜치 에지)** 탭을 클릭합니다.
4. 삭제할 보안 개체를 하나 이상 선택합니다.

5. **Actions(작업)** 창에서 **Remove(제거)**를 클릭합니다.



6. **OK(확인)**를 클릭하여 확인합니다.

선택한 Catalyst SD-WAN 보안 개체가 삭제됩니다. 삭제 작업이 감사 목적으로 로깅되므로 변경 사항을 추적할 수 있습니다.

로그를 보려면 다음을 수행합니다.

- Security Cloud Control 애플리케이션에서 **Events & Logs(이벤트 및 로그) > Logs(로그) > Change Log(변경 로그)**를 선택합니다.
- Catalyst SD-WAN Manager 애플리케이션에서 **Monitor(모니터) > Logs(로그) > Audit Logs(감사 로그)**를 선택합니다.

## Catalyst SD-WAN

Catalyst SD-WAN Manager를 사용하면 사용자가 개체 유형 및 프로파일 유형별로 보안 개체를 효율적으로 필터링하고 검색하여 네트워크 보안 관리를 간소화할 수 있습니다. 이 기능은 WAN 브랜치 에지 환경에서 보안 개체를 찾고, 검토하고, 수정 또는 삭제하는 기능을 개선하여 시스템 성능을 최적화하고, 효과적인 SD-WAN 보안 개체 관리를 보장합니다.

개체 유형 및 프로파일 유형을 기준으로 Catalyst SD-WAN 보안 개체를 필터링하고 검색하는 기능을 통해 사용자는 이러한 개체를 효율적으로 찾고, 검토하고, 수정하고, 필요 시 삭제할 수 있습니다. 이 접근 방식은 최적의 시스템 성능을 유지하는 데 도움이 됩니다.

**Object Type(개체 유형)** 및 **Profile Type(프로파일 유형)**이라는 두 매개변수를 사용하여 개체를 필터링할 수 있습니다.

- 1.
2. **Administration(관리) > Integration(통합) > Catalyst SD-WAN을(를)** 선택합니다.
3. 개체을(를) 선택합니다.
4. **WAN Branch Edge(WAN 브랜치 에지)** 탭을 클릭합니다.
5. 필터 아이콘 (  )을 클릭하고 **Object Type(개체 유형)** 또는 **Profile Type(프로파일 유형)**별로 개체를 선택합니다.

**Objects**

Firewall **WAN Branch Edge**

Search for objects by name, IP, or port number Displaying 8 of 8 objects

**Filter**

- Object Type
  - ☒ Application List
  - ☐ Data Prefix
  - ☐ FQDN
  - ☐ Geolocation
  - ☐ Identity
  - ☐ Port
  - ☐ Protocol
  - ☐ Security Group Tag
  - ☐ IPS Signature
  - ☐ Allow URL
  - ☐ Block URL
  - ☐ Zone
- Profile Type
  - ☐ Advanced Inspection ...
  - ☐ Advanced Malware Pr...
  - ☐ Intrusion Prevention
  - ☐ TLS/SSL Decryption
  - ☐ TLS/SSL Profile
  - ☐ URL Filtering

| References | Type             |
|------------|------------------|
| 1          | Application List |
| 0          | Application List |
| 2          | Application List |
| 1          | Application List |
| 1          | Application List |
| 0          | Application List |
| 3          | Application List |
| 0          | Application List |

필터를 사용하여 개체를 검색할 수 있습니다. 개체 이름, IP 주소 또는 포트 번호를 입력하여 검색 범위를 좁히는 방식으로 결과를 구체화합니다.



# 제

## 5 Catalyst SD-WAN

---

### 장

:

- Catalyst SD-WAN NGFW □□ □□ □□
- □□ Catalyst SD-WAN NGFW □□ □□ □□
- Catalyst SD-WAN □□ □□ □□
- Catalyst SD-WAN NGFW □□□ □□ □□
- Catalyst SD-WAN Manager□□ □□ □□

이 문서에서는 Security Cloud Control 및 Catalyst SD-WAN Manager의 통합을 통해 Catalyst SD-WAN NGFW 보안 정책을 관리(생성, 조회, 편집 및 구축)하는 방법, 즉 하위 정책, 소스/대상 영역 및 정책 그룹을 구성하고, 정책 그룹을 보안 라우터 디바이스에 구축하는 방법을 설명합니다.

## Catalyst SD-WAN NGFW

Catalyst SD-WAN Manager NGFW 보안 정책은 무단 액세스 및 위협으로부터 네트워크, 시스템 및 데이터에 대해 강력한 보호 기능을 제공합니다. 포괄적인 관리 프레임워크 통해 사용자는 NGFW(Next-Generation Firewall) 보안 정책을 효율적으로 구현 및 관리하여 고급 사이버 보안, 간소화된 정책 제어 및 엔터프라이즈 환경에 대한 향상된 위협 방지 보장할 수 있습니다.

Catalyst SD-WAN Manager의 NGFW 보안 정책은 시스템, 네트워크 및 데이터를 무단 액세스, 오용 또는 위협으로부터 보호하기 위해 설계된 규칙 및 구성입니다. Catalyst SD-WAN Manager는 NGFW 보안 정책을 구현 및 관리하기 위한 포괄적인 프레임워크를 제공합니다.

## Catalyst SD-WAN NGFW

Security Cloud Control Firewall Management에서 Catalyst SD-WAN NGFW 보안 정책을 확인, 편집, 정책 그룹에 연결, 삭제 또는 복사합니다.

NGFW(Next-Generation Firewall) 정책이 이미 Catalyst SD-WAN의 정책 그룹과 연결되어 있는 경우, Security Cloud Control Firewall Management에서 해당 정책을 삭제할 수 없습니다.

1. **Policies(정책) > WAN Branch Edge(브랜치 엣지)**를 선택합니다.
2. 정책으로 이동하고 **Action(작업)** 열 아래의 줄임표(...)를 클릭합니다.
3. **View(보기), Edit(편집), Associate Policy Group(정책 그룹 연결), Delete(삭제)** 또는 **Copy(복사)**를 클릭합니다.

| NGFW Policy <span>6</span>                        |             |                 |                             |                                                                                                                       |            |                           |                        |
|---------------------------------------------------|-------------|-----------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------|------------|---------------------------|------------------------|
| <div> <div>Q</div> <div>Search Table</div> </div> |             |                 |                             |                                                                                                                       |            |                           |                        |
| Add NGFW Policy                                   |             |                 |                             | As of: Jan 08, 2025 12:31:47 PM  |            |                           |                        |
| Name                                              | Description | Device Solution | Policy Group                | References                                                                                                            | Updated By | Last Updated              | Action                 |
| 01111111-NGFW-Policy                              |             | sdwan           | 01111111-NGFW-Policy        | 1                                                                                                                     | Initial    | Aug 20, 2025, 3:50:11 AM  | ...                    |
| 01111111-NGFW-Policy                              |             | sdwan           | 01111111-NGFW-Policy        | 1                                                                                                                     | Initial    | Oct 14, 2025, 12:31:47 PM | View                   |
| Business Branch-NGFW-policy                       |             | sdwan           |                             | 0                                                                                                                     | Initial    | Aug 14, 2025, 12:31:47 PM | Edit                   |
| Business Branch-NGFW-policy                       |             | sdwan           | Business Branch-NGFW-policy | 1                                                                                                                     | Initial    | Aug 14, 2025, 12:31:47 PM | Associate Policy Group |
| 01111111-NGFW-Policy                              |             | sdwan           |                             | 0                                                                                                                     | Initial    | Aug 14, 2025, 12:31:47 PM | Delete                 |
| 01111111-NGFW-Policy                              |             | sdwan           |                             | 0                                                                                                                     | Initial    | Aug 14, 2025, 12:31:47 PM | Copy                   |

## Catalyst SD-WAN

NGFW 정책 생성 워크플로우를 사용하여 Security Cloud Control Firewall Management에 Catalyst SD-WAN NGFW 보안 정책을 생성합니다.

구성 그룹을 사용하여 이러한 디바이스를 구축하고 관리했는지 확인합니다. 구성 그룹 생성에 대한 자세한 내용은 [구성 그룹 및 기능 프로파일](#)을 참조하십시오.

NGFW 정책 생성 워크플로우를 사용하여 Security Cloud Control Firewall Management에서 Catalyst SD-WAN NGFW 보안 정책을 생성하려면 다음 단계를 따르십시오.

1. **Policies(정책) > WAN Branch Edge(브랜치 엣지)**를 선택합니다.
2. **Catalyst SD-WAN NGFW Policies(Catalyst SD-WAN NGFW 정책)** 페이지에서 **Add NGFW Policy(NGFW 정책 추가)**를 클릭합니다.  
그러면 **NGFW** 정책 생성 워크플로우가 시작됩니다.
3. **Security Policy Name(보안 정책 이름)** 탭에서 **Policy Name(정책 이름)** 및 **Description(설명)**을 입력하고 **Device Solution(디바이스 솔루션)**에서 **SDWAN** 라디오 버튼을 클릭합니다.
4. **Next(다음)**를 클릭합니다.
5. **Select the optional Configuration Group to connect the NGFW policy(NGFW 정책과 연결할 선택적 구성 그룹 선택)** 페이지에서 NGFW 정책과 연결할 구성 그룹을 선택하고 **Next(다음)**를 클릭합니다.
6. **Create Sub-Policies(하위 정책 생성)** 탭에서 **+Add Sub-Policy(+하위 정책 추가)**를 클릭하여 보안 정책에 대한 하위 정책을 추가합니다.

**Catalyst SD-WAN NGFW Policies**

**Create NGFW Policy**

Let's keep your network secure by creating policies

Based on your configuration group we found the following and recommending these settings, feel free to edit or add more rules

ngfw-policy (Total Zone Pairs: 2)

Search Security Sub Policy

**+ Add Sub-Policy** **Additional Settings**

Source Zone: CorporateUsers\_zone → Destination Zone: Untrusted 1

Search Action Default action: Drop **+ Add Rule**

| # | Rule Name | Action | Log                      | Advanced Inspection Profile | Source | Des |
|---|-----------|--------|--------------------------|-----------------------------|--------|-----|
| 1 | Rule1     | Drop   | <input type="checkbox"/> |                             | Any    | Any |

Cancel Back Next

필드

VPN/인터페이스

설명

VPN 또는 인터페이스를 지정합니다.

| 필드    | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 소스 영역 | <p>데이터 패킷의 소스인 영역을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>● Corporate_Users_zone</li> <li>● Local_Internet_for_Guests_zone</li> <li>● No_zone</li> <li>● Payment_Processing_Network_zone</li> <li>● Physical_Security_Devices_zone</li> <li>● 본인</li> <li>● 신뢰 안 함</li> </ul> <p>+ <b>Create New(새로 만들기)</b>를 클릭하여 새 소스 영역을 생성합니다. <b>Name(이름)</b>을 입력하고 드롭다운에서 <b>VPN</b>을 선택합니다.</p> <div>  주         <p>하나의 소스 영역 내에서 여러 VPN을 선택할 수 있습니다.</p> </div>    |
| 대상 영역 | <p>데이터 트래픽을 전송할 영역을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>● Corporate_Users_zone</li> <li>● Local_Internet_for_Guests_zone</li> <li>● No_zone</li> <li>● Payment_Processing_Network_zone</li> <li>● Physical_Security_Devices_zone</li> <li>● 본인</li> <li>● 신뢰 안 함</li> </ul> <p>새 대상 영역을 만들려면 + <b>Create New(새로 만들기)</b>를 클릭합니다. <b>Name(이름)</b>을 입력하고 드롭다운에서 <b>VPN</b>을 선택합니다.</p> <div>  주         <p>하나의 대상 영역 내에서 여러 VPN을 선택할 수 있습니다.</p> </div> |

7. 보안 정책에 대한 추가 설정을 구성하려면 **Additional Settings(추가 설정)**를 클릭합니다. 절차에 사용되는 단계에 대한 자세한 내용은 [NGFW 추가 설정 구성](#)을 참조하십시오.
8. **Save(저장)**를 클릭합니다.

**Catalyst SD-WAN NGFW Policies**

**Create NGFW Policy**

✓ Security Policy Name

✓ Select Configuration Groups (Optio...

✓ Create Sub-Policies

4 Summary

Let's keep your network secure by creating policies

Based on your configuration group we found the following and recommending these settings, feel free to edit or add more rules

ngfw-policy (Total Zone Pairs: 2)

Search Security Sub Policy

+ Add Sub-Policy

**Additional Settings**

Source Zone: CorporateUsers\_zone → Destination Zone: Untrusted 1

Search Action Default action: Drop + Add Rule

| # | Rule Name | Action | Log                      | Advanced Inspection Profile | Source | Des |
|---|-----------|--------|--------------------------|-----------------------------|--------|-----|
| 1 | Rule1     | Drop   | <input type="checkbox"/> |                             | Any    | Any |

Cancel Back Next

9. 기존 하위 정책의 왼쪽 상단 모서리에 있는 줄임표(...)를 클릭하여 편집, 삭제 또는 복사를 수행합니다.
10. NGFW 정책 규칙을 하위 정책에 추가하려면 하위 정책으로 이동하여 **+ Add Rule(+ 규칙 추가)**을 클릭합니다.

| 필드    | 설명          |
|-------|-------------|
| 규칙 이름 | 규칙의 이름입니다.  |
| 시퀀스   | 시퀀스를 지정합니다. |

| 필드 | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 일치 | <p><b>Add Conditions(조건 추가)</b> 드롭다운 목록에서 원하는 일치 조건을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>● Source <ul style="list-style-type: none"> <li>● 지리위치</li> <li>● IPv4 프리픽스</li> <li>● 포트</li> </ul> </li> <li>● 대상 <ul style="list-style-type: none"> <li>● FQDN</li> <li>● 지리위치</li> <li>● IPv4 프리픽스</li> <li>● 포트</li> </ul> </li> <li>● 프로토콜</li> <li>● 애플리케이션</li> </ul> <p>ISE(Identity Services Engine)가 활성화된 경우, <b>Source(소스)</b> 및 <b>Destination(대상)</b> 필드에서 SGT 옵션을 사용할 수 있습니다. ID 사용자 또는 사용자 그룹은 <b>Source(소스)</b>에 대해서만 지원됩니다.</p> |
| 조치 | <p>원하는 조치 조건을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>● 통과</li> <li>● 차단</li> <li>● 검사</li> <li>● 로그 이벤트: 검사 작업에 대한 통합 로깅.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                          |

11. 기존 규칙을 수정하려면 연필 아이콘 클릭하여 **Edit(편집)**, **Disable(비활성화)**, **Delete(삭제)**, **Clone rule(규칙 복제)**, **Add rule on top(맨 위에 규칙 추가)** 또는 **Add rule below(아래에 규칙 추가)**를 클릭합니다.

**Catalyst SD-WAN NGFW Policies**

**Create NGFW Policy**

Let's keep your network secure by creating policies

Based on your configuration group we found the following and recommending these settings, feel free to edit or add more rules

ngfw-policy (Total Zone Pairs: 2)

Search Security Sub Policy

+ Add Sub-Policy Additional Settings

Source Zone: CorporateUsers\_zone → Destination Zone: Untrusted 1

Search Action Default action: Drop + Add Rule

| # | Rule Name | Action | Log                      | Advanced Inspection Profile | Source | Des |
|---|-----------|--------|--------------------------|-----------------------------|--------|-----|
| 1 | Rule1     | Drop   | <input type="checkbox"/> |                             | Any    | Any |

Edit Disable Delete Clone rule Add rule on top Add rule below

Cancel Back Next

12 Next(다음)를 클릭합니다.

13 Summary(요약)페이지에서 **NGFW Policy(NGFW 정책)**, **Sub-Policies(하위 정책)** 및 **Settings(설정)**를 검토하고 **Create NGFW Policy(NGFW 정책 생성)**를 클릭합니다.

**Catalyst SD-WAN NGFW Policies**

**Create NGFW Policy**

Security Policy Name

Select Configuration Groups (Optio...

Create Sub-Policies

4 Summary

**Summary**

Here is a summary of your NGFW policy

NGFW Policy Edit

Sub-Policies Edit

Settings Edit

Cancel Back Create NGFW Policy

## Catalyst SD-WAN NGFW

매니지드 디바이스 전체에서 일관된 보안 시행을 보장하려면 정책 그룹을 Catalyst SD-WAN NGFW 정책과 연결합니다. Security Cloud Control Firewall Management를 사용하여 관리자는 정책 그룹을 NGFW 정책에 쉽게 연결하고 구축하여 네트워크 보안 관리를 간소화하고 WAN 브랜치 에지 환경을 위한 중앙 집중식 정책 구축을 개선할 수 있습니다.

이 섹션에서는 정책 그룹을 **Catalyst SD-WAN NGFW** 정책과 연결하여 해당 그룹에서 관리하는 디바이스에 정책을 구축할 수 있도록 하는 단계를 간략하게 설명합니다. 이렇게 하면 해당 디바이스 전반에 일관된 보안 시행이 보장됩니다. 연결되면 정책 그룹을 구축하여 디바이스에서 정책을 활성화할 수 있습니다.

1. **Policies(정책) > WAN Branch Edge(브랜치 엣지)**를 선택합니다.
2. 정책 그룹과 연계할 정책으로 이동합니다. **Action(작업)** 열 아래의 생략부호(...)를 클릭하고 **Associate Policy Group(정책 그룹 연결)**을 선택합니다.

**Catalyst SD-WAN NGFW Policies**

NGFW Policy 6

Search Table

Add NGFW Policy

| Name                   | Description | Device Solution | Policy Group           | References | Updated By | Last Updated             | Action                 |
|------------------------|-------------|-----------------|------------------------|------------|------------|--------------------------|------------------------|
| SD-WAN NGFW Policy     |             | sdwan           | SD-WAN NGFW Policy     | 1          | admin      | Aug 20, 2025, 3:50:11 AM | ...                    |
| SD-WAN NGFW Policy     |             | sdwan           | SD-WAN NGFW Policy     | 1          | admin      | Oct 14, 2025             | View                   |
| WAN Branch Edge Policy |             | sdwan           |                        | 0          | admin      | Aug 14, 2025             | Edit                   |
| WAN Branch Edge Policy |             | sdwan           | WAN Branch Edge Policy | 1          | admin      | Aug 14, 2025             | Associate Policy Group |
| SD-WAN NGFW Policy     |             | sdwan           |                        | 0          | admin      | Aug 14, 2025             | Delete                 |
|                        |             |                 |                        |            |            |                          | Copy                   |

3. 정책을 선택하고 **Save(저장)**를 클릭합니다.

## Catalyst SD-WAN Manager

Catalyst SD-WAN의 정책 그룹은 NGFW 보안 정책을 논리적으로 묶은 것으로, 여러 디바이스나 사이트에 걸친 구축을 간소화합니다. Catalyst SD-WAN Manager를 사용하여 관리자는 보안 개체 및 프로파일을 포함한 정책 그룹 업데이트를 보안 라우터 디바이스에 구축하여 네트워크 보안 관리를 최적화하고 SD-WAN 정책 시행을 간소화할 수 있습니다.

Catalyst SD-WAN의 정책 그룹은 차세대 방화벽(NGFW) 보안 정책에서 사용되는 관련 항목 또는 구성의 논리적 그룹입니다. 이러한 그룹은 여러 디바이스 또는 사이트에서 정책을 적용하는 프로세스를 간소화합니다.

Catalyst SD-WAN Manager를 사용하여 Security Cloud Control Firewall Management에서 보안 라우터 디바이스로 보안 개체 및 보안 프로파일을 포함한 NGFW 정책 수정을 구축할 수 있습니다.

Catalyst SD-WAN Manager의 **Workflows(워크플로우) > Deploy Policy Group(정책 그룹 구축)** 메뉴에서 워크플로우에 액세스할 수 있습니다. 이 워크플로우를 사용하면 보안 라우터 디바이스를 연결하고 선택한 디바이스에 정책 그룹을 구축할 수 있습니다.

자세한 내용은 [정책 그룹 구성 가이드](#), [Cisco IOS XE Catalyst SD-WAN](#)의 정책 그룹 워크플로우 구축 섹션을 참조하십시오.

제

## 6 Cisco Security Analytics and Logging

---

장

:

- Security Cloud Control □ □ Security Analytics and Logging(SaaS) □ □
- Security Cloud Control □ □ □ □ □ □
- Cisco Security Analytics and Logging(SaaS) □ □ □ □ □ □
- Security Analytics and Logging □ □ □ □
- Catalyst SD-WAN □ □ □ Security Analytics and Logging □ □
- Catalyst SD-WAN □ □ □ □ Security Cloud Control Firewall Management □ □ □ □ □ □ □ □
- □ □ □ □ □ □
- Security Cloud Control Firewall Management □ □ Catalyst SD-WAN □ □ □ □ □ □

## Security Cloud Control Security Analytics and Logging(SaaS)

Cisco SAL( Cisco Security Analytics and Logging) 클라우드에서 방화벽 보안 이벤트를 수집하고 중앙 집중화하여 어떻게 Security Cloud Control을 통해 통합 가시성 및 필터링을 지원하는지 알아봅니다.

용어 참고: 이 설명서에서는 보안 이벤트 모니터링 및 분석을 위해 Cisco Security Analytics and Logging(SaaS 제품)을 Security Cloud Control과 함께 사용할 때, Cisco Security Analytics and Logging(SaaS) 또는 SAL(SaaS)이라고 하는 이 통합 기능이 표시됩니다.

Cisco SAL(Security Analytics and Logging)을 사용하면 모든 방화벽 디바이스에서 지원되는 유형의 보안 이벤트를 캡처하고 Security Cloud Control에서 확인할 수 있습니다. 이벤트는 Security Analytics and Logging 클라우드에 저장되며 **Event Logging**(이벤트 로깅) 페이지에서 볼 수 있습니다. **Event Logging**(이벤트 로깅) 페이지에서는 보안 이벤트 데이터를 검색, 필터링 및 분석하여 네트워크에서 어떤 보안 규칙이 트리거되는지 파악할 수 있습니다.

## Security Cloud Control

SaaS(Secure Logging Analytics)를 사용하면 ASA, FTD 및 Catalyst SD-WAN, 디바이스의 보안 이벤트를 AAA, BotNet, 방화벽 트래픽, 침입, AI 방어 등의 이벤트 유형별로 필터링하고 분석할 수 있습니다. 이러한 필터는 포괄적인 보안 가시성을 위해 네트워크 활동을 모니터링하고, 위협을 탐지하고, 보안 정책을 시행하는 데 도움이 됩니다.

Secure Logging Analytics(SaaS)에 기록된 보안 이벤트를 필터링할 때, Security Cloud Control가 지원하는 Catalyst SD-WAN 이벤트 유형 목록에서 선택할 수 있습니다. Security Cloud Control 메뉴에서 **Analytics**(분석) > **Event Logging**(이벤트 로깅)으로 이동하고 필터 아이콘을 클릭하여 이벤트를 선택합니다.

Catalyst SD-WAN 디바이스는 현재 SD-WAN 이벤트 유형 하에서 연결 이벤트만 기록합니다. SD-WAN Catalyst 디바이스는 시스템 로그 이벤트를 Security Cloud Control로 전송하는 기능을 지원하지 않습니다. Catalyst SD-WAN 이벤트에 대한 시스템 로그 ID에 대한 자세한 내용은 [Cisco Catalyst SD-WAN 모니터링 및 유지 관리 구성 가이드](#)를 참조하십시오.

사용자가 시스템을 통과하는 트래픽을 생성할 때 연결에 대한 이벤트를 생성할 수 있습니다. 액세스 규칙에서 연결 로깅을 활성화하여 이러한 이벤트를 생성합니다. 보안 인텔리전스 정책과 SSL 암호 해독 규칙에서 로깅을 활성화하여 연결 이벤트를 생성할 수도 있습니다.

연결 이벤트에는 탐지된 세션에 관한 데이터가 포함되어 있습니다. 모든 개별 연결 이벤트에 대한 정보는 몇 가지 요소에 따라 가용성이 결정됩니다. 일반적으로 이 정보에는 다음이 포함됩니다.

- 기본 연결 속성: 타임 스탬프, 소스 및 대상 IP 주소, 인그레스 및 이그레스 영역, 연결을 처리한 디바이스 등
- 시스템에서 검색하거나 유추한 추가 연결 속성: 애플리케이션, 요청된 URL, 연결과 관련된 사용자 등
- 연결이 로깅된 사유를 설명하는 메타데이터: 어떤 설정이 트래픽을 처리했는지, 연결이 허용 또는 차단되었는지, 암호화 및 해독된 연결에 대한 상세정보.

## Cisco Security Analytics and Logging(SaaS)

Cisco Security Analytics and Logging(SaaS) 구독 관리를 사용하면 보안 이벤트 데이터 및 애널리틱스에 대한 지속적인 액세스를 보장합니다. 활성 구독을 유지하면 데이터 손실을 방지하고 저장된 방화벽 이벤트 및 행동 애널리틱스를 사용하여 보안 위협을 모니터링하고 분석하고 대응하는 기능을 유지할 수 있습니다.

Cisco Security Analytics and Logging(SaaS) 유료 구독이 만료되면 새로운 이벤트 수집이 즉시 중단됩니다. 만료일로부터 90일이 지나면 더 이상 기존 이벤트 데이터를 보거나 쿼리할 수 없습니다. 구독을 리뉴얼할 수 있는 기간은 180일입니다.

180일의 유예 기간이 경과하도록 허용하면 시스템에서 모든 이벤트 데이터를 비웁니다. 이제 **Event Logging**(이벤트 로깅) 페이지에서 보안 이벤트를 확인할 수 없으며, 보안 이벤트 및 네트워크 플로우 데이터에 동적 엔터티 모델링(DEM) 행동 분석이 적용되지 않습니다.

## Security Analytics and Logging

**Security Analytics and Logging** 구독은 디바이스별 라이선스, 사용자 지정 가능한 로그 저장 및 보존을 포함하여, **Security Cloud Control**에서 방화벽 로그를 관리하기 위한 유연한 옵션을 제공합니다. **Essentials**, **Advantage** 및 **Premier** 계층 중에서 선택하여 최대 5년의 보존 기간, 최대 10TB의 스토리지 용량을 통해 운영 및 컴플라이언스 요구 사항을 충족할 수 있습니다.

### Security Analytics and Logging

SAL를 **Security Cloud Control** 구독에 결합할 수 있습니다. **Security Cloud Control**로 방화벽을 관리할 경우, 다음과 같은 방법으로 **Security Analytics and Logging** 엔타이틀먼트를 얻을 수 있습니다.

- 무제한 로깅 기능이 포함된 디바이스 관리: 이 옵션은 디바이스별 라이선스를 제공합니다. 방화벽 디바이스에 대한 디바이스 관리 기능과 90일간의 롤링 기간 동안 무제한 로그 저장을 포함합니다.
- 선택적 클라우드 로깅 기능이 포함된 디바이스 관리 전용: 이 옵션은 관리 기능만을 위한 디바이스별 라이선스 구매를 포함합니다. 그런 다음 **Security Analytics and Logging**를 별도의 클라우드 로깅 구독으로 추가할 수 있습니다. 이를 통해 특정 운영 및 규정 준수 요구 사항에 따라 로깅 데이터 저장 및 로그 보존 기간을 맞춤 설정할 수 있습니다.

### 90

일일 데이터 수집 속도를 정확하게 예측하려면 **Security Cloud Control**에 로그인한 후 **Events & Logs**(이벤트 및 로그) > **Events**(이벤트) > **Event Logging**(이벤트 로깅) 탭으로 이동하여 90일 무료 체험을 신청하십시오. 원하는 구독 계획을 구매하여 **Security Cloud Control Firewall Management** 주문 가이드의 지침을 검토하여 서비스를 계속할 수 있습니다.

### Security Analytics and Logging

무제한 로깅 옵션이 포함된 디바이스 관리를 사용하지 않으려면 로깅 용량을 별도로 구매할 수 있습니다. 이 독립형 **Security Analytics and Logging** 구독은 더 큰 유연성, 더 긴 기본 보존 기간 및 증가된 저장 용량 권한을 제공합니다. 이러한 구독 등급의 기본 최소 보존 기간은 1년입니다.

다음과 같은 경우 유연한 **Security Analytics and Logging** 구독 계층을 선택합니다.

- 방화벽 디바이스는 이미 다른 주문으로 구매했습니다.
- 특정 로깅 용량 추정치에 따라 고정된 인제스트, 저장, 로깅 보존 용량을 기준으로 계층을 구매하고자 합니다.
- 로그 보존 기간을 90일 이상으로 설정해야 합니다.

**Security Analytics and Logging** 구독은 **Essentials**, **Advantage** 및 **Premier**의 세 가지 계층으로 분류됩니다. 이 표에서는 각 계층에서 사용할 수 있는 스토리지 용량 및 로그 보존 기간을 나열합니다.

| 설명                      | 보존 기간        | 스토리지 제한 | 구독 기간 |
|-------------------------|--------------|---------|-------|
| Cisco SAL Essentials 구독 | 1년, 2년 또는 3년 | 2TB     | 0~5년  |
| Cisco SAL Advantage 구독  | 1년, 2년 또는 3년 | 4TB     | 0~5년  |
| Cisco SAL Premier 구독    | 1년, 2년 또는 3년 | 10 TB   | 0~5년  |

구독 요금제에 대한 자세한 내용은 **Security Cloud Control Firewall Management** 주문 가이드를 참조하십시오.



유료 구독의 경우, **Security Analytics and Logging**은 이벤트 데이터를 자동으로 관리하여 라이선스 보존 기간과 일치하도록 합니다. **Security Analytics and Logging**는 지정된 보존 기간보다 오래된 이벤트 데이터를 매일 삭제하며, 전체 보존 기간 내의 모든 이벤트 데이터에 대한 접근 권한을 항상 유지할 수 있도록 보장합니다.

**Cisco Cloud**가 귀사의 연동된 방화벽 디바이스로부터 매일 수신하는 이벤트 수에 맞는 구독 요금제를 구매합니다. 이를 일일 수집 속도라고 합니다. **Logging Volume Estimator** 툴을 사용하여 일일 수집 속도를 예측할 수 있으며, 속도가 변경되면 데이터 요금제를 업데이트할 수 있습니다.

## Security Analytics and Logging

**Security Analytics and Logging** 평가판은 90일 동안 전체 기능에 액세스할 수 있으므로 이벤트 로깅 성능을 평가하고 일일 수집 속도를 추정하고 스토리지 요구 사항을 결정할 수 있습니다. 귀중한 인사이트를 얻어 최적의 구독을 선택하고 **Cisco Cloud**의 방화벽 보안 데이터에 대한 지속적인 액세스를 보장합니다.

### Security Analytics and Logging

온보딩된 보안 디바이스가 **Cisco** 클라우드로 전송하는 일일 이벤트 볼륨과 일치하는 데이터 스토리지 요금제를 구매합니다. 이 양을 일일 수집 속도라고 합니다. 구매 전에 **Security Analytics and Logging** 무료 평가판에 참여하여 수집 속도를 정확히 추정합니다.

- 이 평가판 요금제를 사용하면 90일 동안 모든 **Security Analytics and Logging** 기능에 액세스할 수 있습니다.
- 90일 평가판 기간 동안 온보딩된 방화벽은 **Security Analytics and Logging**에 이벤트를 전송합니다. 이벤트 수집 속도를 모니터링하고, 스토리지 요구 사항을 파악하며, 성능을 평가하십시오. 이 데이터는 가장 적합한 유료 구독을 계획하고 선택하는 데 도움이 됩니다.
- 평가판이 활성화된 상태에서 유료 **Security Analytics and Logging** 구독을 활성화하면, **Security Cloud Control**는 해당 제품 인스턴스의 평가판 라이선스가 유료 라이선스로 대체되고 평가판이 종료됩니다.
- 유료 구독을 체험판에 적용하지 않기로 선택하면, 90일 후 이벤트 수집이 자동으로 중단됩니다. 이후에는 **Security Analytics and Logging** 기능에 액세스할 수 없습니다. 그러나 기존 로그 데이터는 체험판 만료일로부터 추가로 90일간 **Security Analytics and Logging** 클라우드에 보관됩니다.



이 90일 유예 기간 내에 유료 **Security Analytics and Logging** 라이선스를 구독하지 않으면, 모든 체험판 데이터가 영구적으로 삭제됩니다.

### Security Analytics and Logging

**Security Analytics and Logging** 사용 후 계속 사용하거나 기존 로깅 기능을 업그레이드하려면 다음을 수행합니다.

1. 시험 사용 기간 동안 얻은 인사이트(일일 수집 속도, 필요한 보존 기간, 스토리지 용량)를 활용하여 가장 적합한 **Security Analytics and Logging** 구독 플랜을 결정합니다.
2. 적절한 **Security Analytics and Logging** 구독을 구매하려면 **Cisco** 담당자 또는 공인 파트너와 협력하십시오.

## Security Analytics and Logging

새로운 Security Analytics and Logging 구독을 구매한 후, Security Cloud Control내에 활성화할 수 있는 클레임 코드를 받게 됩니다. 구독 클레임 코드가 포함된 환영 이메일이 구매 과정에서 지정한 프로비저닝 담당자에게 자동으로 발송됩니다. 최종 고객 연락처를 포함시킨 경우, 해당 고객도 사본을 받게 됩니다. 구독 시작 요청일에 이 이메일을 수신하게 됩니다.

Security Cloud Control 관리자는 클레임 코드를 사용하여 조직의 구독을 활성화합니다. 구독을 신청하고 활성화하는 방법에 대한 자세한 내용은 [구독 클레임](#)을 참조하십시오.

## Security Analytics and Logging

활성 Security Analytics and Logging 구독을 유지하면 지속적인 기록과 과거 데이터 접근이 보장됩니다.

- Security Analytics and Logging 구독이 리뉴얼되지 않고 만료되면 방화벽에서 이벤트 수집이 즉시 중단됩니다.
- 구독이 만료된 후에도 기존 이벤트 데이터를 90일 동안 계속해서 조회하고 검색할 수 있습니다. 90일이 지나면 이벤트 데이터에 더 이상 액세스할 수 없습니다.
- 기존 데이터는 구독 만료일로부터 180일간의 유예 기간 동안 Security Analytics and Logging 클라우드에 보관됩니다.
- 이 180일 유예 기간 내에 Security Analytics and Logging 구독을 리뉴얼하지 않으면, 모든 이벤트 데이터가 Security Analytics and Logging 클라우드에서 영구적으로 삭제됩니다.

## Security Analytics and Logging

스토리지 한도 및 보존 기간을 추적하려면 Security Analytics and Logging 라이선스를 모니터링합니다. 대시보드는 Security Cloud Control 구독 내에서 이벤트 데이터 관리를 최적화하고, 초과 사용을 방지하고, 컴플라이언스 유지하는 데 도움이 됩니다.

부여받은 월간 스토리지 한도 및 이벤트 스토리지 보존 기간과 같은 Security Analytics and Logging 라이선스 정보를 확인합니다. 별도의 Security Analytics and Logging 라이선스 및 데이터 플랜이 없는 경우, 90일 롤링 데이터 스토리지 세부 정보가 라이선스 정보에 표시됩니다.

- 
1. **Administration(관리) > Logging Settings(로깅 설정)**을 선택합니다.
  2. 로깅 스토리지 사용량 보기를 클릭합니다.



또는 **Events & Logs(이벤트 및 로그) > Events(이벤트) > Event Logging(이벤트 로깅)**로 이동한 다음 **View Dashboard(대시보드 보기)** 버튼을 클릭하여 **Security Analytics and Logging** 라이선스 정보를 확인합니다.

**Event Logging Overview(이벤트 로깅 개요)** 대시보드는 **Security Analytics and Logging** 라이선스 구독에 대한 포괄적인 개요를 제공합니다:

- **Retention policy(보존 정책):** 구독에 따른 이벤트 로그 보존 기간을 표시합니다. 보존 기간보다 오래된 이벤트 데이터는 매일 제거되며, 항상 전체 보존 기간 내의 모든 이벤트 데이터에 액세스할 수 있습니다.
- **Storage capacity(스토리지 용량):** **Security Analytics and Logging** 라이선스에 따라 부여된 총 데이터, 현재 사용된 스토리지의 양 및 남은 사용 가능한 스토리지를 표시합니다.

인터랙티브 대시보드를 사용하여 **Security Cloud Control**에서 스토리지 사용량 및 이벤트 추세에 대한 인사이트를 확보합니다. 정기적인 분석을 통해 보안 환경 전반에서 이벤트 로깅을 최적화하고, 스토리지 설정을 조정하고, 초과사용을 방지하고, 효율적인 컴플라이언스 및 성능을 유지할 수 있습니다.

현재 보안 애널리틱스 및 로깅 스토리지 사용량을 확인하고 이벤트 로깅 추세를 분석합니다. 이벤트 유형, 디바이스 유형 및 개별 디바이스별로 스토리지 사용량 추세를 분석하여 스토리지 사용 패턴에 대한 심층적인 인사이트를 얻을 수 있습니다. 빠르고 쉬운 분석을 위해 데이터 시각화를 사용합니다. 현재 스토리지 용량을 평가하고 스토리지 사용량이 보안 분석 및 로깅 라이선스에 지정된 한도에 근접할 경우 로깅 속도를 줄이기 위한 조치를 취할 수 있습니다.

1. **Administration(관리) > Logging Settings(로깅 설정)**를 선택합니다.

2. 로깅 스토리지 사용량 보기를 클릭합니다.



또는 왼쪽 탐색 모음에서 **Events & Logs(이벤트 및 로그) > Events(이벤트) > Event Logging(이벤트 로깅)**로 이동한 다음 **View Dashboard(대시보드 보기)** 버튼을 클릭하여 **Security Analytics and Logging** 스토리지 사용량 및 이벤트 수집 추세를 확인합니다.

3. 다음 대시보드를 사용하여 스토리지 사용량을 맞춤 설정하고 분석하며, 방화벽 구축 환경의 이벤트 로깅 동향에 대한 인사이트를 얻습니다.

- **Usage Trends(사용 추세)** 대시보드에는 지난 12개월 동안의 스토리지 사용량이 표시됩니다. 막대 위에 마우스를 올려 놓으면 해당 월의 데이터 사용량을 확인할 수 있습니다.
- **EPS(초당 이벤트 수)** 추세 대시보드에는 온보딩된 디바이스의 이벤트 수집 속도가 표시됩니다. 특정 시간대 또는 디바이스에 대해 초당 이벤트 추세 보기를 맞춤 설정하여 더 세분화된 데이터를 확인합니다. 지난 1주, 2주, 3주 또는 1개월 동안의 데이터를 필터링할 수 있습니다.



디바이스 드롭다운 목록에는 이벤트를 Cisco Security Cloud에 전송하는 매니지드 방화벽 디바이스가 표시됩니다.

- **Utilization by event type(이벤트 유형별 사용량) 추세:** 다양한 이벤트 유형별로 사용된 이벤트 데이터 저장 용량을 일일 바이트 단위로 표시합니다. 이 위젯을 사용하여 이벤트 유형별 스토리지 사용량을 모니터링하고, 특정 이벤트 유형에 대한 스토리지 사용량의 급증 또는 비정상적인 변화를 식별합니다. 이 인사이트를 통해 특정 이벤트 유형에 대한 로깅 설정을 조정하고 스토리지 사용량을 관리할 수 있습니다.
- **Utilization by Device type Trends(디바이스 유형별 사용량 추세):** 매니지드 디바이스 유형별로 일일 사용 이벤트 데이터 저장 용량을 바이트 단위로 표시합니다. 이 위젯을 사용하여 디바이스 유형별 저장소 사용량을 모니터링하고, 특정 디바이스 유형의 저장소 사용량에서 급증 현상이나 비정상적인 변화를 식별합니다.
- **Utilization by device Trend(디바이스별 사용량):** Security Cloud 제어에 이벤트를 전송하는 각 보안 디바이스에서 사용된 이벤트 데이터 스토리지를 일일 바이트 단위로 표시합니다. 이 위젯은 저장소 사용량이 초당 평균 바이트 수를 초과하는 디바이스에 집중하여 사용성 향상을 위해 상위 5개 디바이스만 표시합니다. 이 위젯을 사용하여 각 디바이스의 저장소 사용량을 모니터링하고 급증 또는 비정상적인 변화를 식별합니다. 이 인사이트를 통해 특정 디바이스에 대한 로깅 설정을 조정하고 저장소 사용을 효과적으로 관리할 수 있습니다.

## Security Analytics and Logging

Security Analytics and Logging 서비스 가용성을 확인하고, FTD 디바이스 이벤트 로깅 상태를 검토하고, Security Analytics and Logging가 매니지드 Firewall Threat Defense 디바이스에서 이벤트를 마지막으로 수신한 시간을 확인합니다.

Security Analytics and Logging(SaaS) 서비스의 가용성과 상태를 모니터링하고, Firewall Threat Defense 디바이스 이벤트 로깅 상태를 검토하고, Security Analytics and Logging가 매니지드 디바이스에서 이벤트를 마지막으로 수신한 시간을 확인합니다.



**Service Status(서비스 상태)** 탭은 현재 Firewall Threat Defense 디바이스를 지원합니다.

의미 있는 디바이스 로깅 상태 및 마지막 이벤트 세부 정보를 볼 수 있도록 매니지드 Firewall Threat Defense 디바이스가 이벤트를 Security Analytics and Logging 클라우드 클라우드 전송하도록 합니다.

1. **Administration(관리) > Logging Settings(로깅 설정)**을 선택합니다.
2. 로깅 스토리지 사용량 보기를 클릭합니다.



또는 **Events & Logs(이벤트 및 로그) > Events(이벤트) > Event Logging(이벤트 로깅)**로 이동한 다음 **View Dashboard(대시보드 보기)** 버튼을 클릭하여 Security Analytics and Logging 서비스 상태를 확인합니다.

3. **Service Status(서비스 상태)** 탭을 클릭합니다.
4. **SAL 서비스 가용성(SAL Service Availability)** 위젯을 검토하여 Security Analytics and Logging 서비스 상태를 확인합니다.  
Security Analytics and Logging 서비스 상태가 **Degraded(저하됨)**로 표시되는 경우, Security Analytics and Logging 서비스에 문제가 발생하여 이벤트 수집이 지연되거나 중단될 수 있습니다.
5. **Last Event Received(마지막으로 수신된 이벤트)** 위젯을 선택하여 Security Analytics and Logging가 디바이스에서 이벤트를 마지막으로 수신한 시간을 확인합니다.
6. **Firewall Logging Status(방화벽 로깅 상태)** 위젯을 검토하여 Firewall Threat Defense 디바이스 이벤트 로깅 상태를 확인합니다.
  - **Connected(연결됨)**: Security Analytics and Logging에 이벤트를 전송하도록 활성화된 Firewall Threat Defense 디바이스의 수를 나타냅니다.
  - **Disabled(비활성화됨)**: Security Analytics and Logging로 이벤트를 전송하지 못하도록 비활성화된 Firewall Threat Defense 디바이스의 수를 나타냅니다.
7. **Firewall Details(방화벽 세부 정보 목록에서 Firewall Threat Defense 디바이스가 마지막으로 Security Analytics and Logging로 이벤트를 보낸 시간을 확인합니다.**  
이벤트가 지연될 수 있는지 또는 수집되지 않을 수 있는지 식별하려면 **SAL Service Availability(SAL 서비스 가용성)** 및 마지막 이벤트 수신(**Last Event Received**) 위젯과 함께 이 정보를 사용합니다.

Security Analytics and Logging 라이선스를 업그레이드하면 이벤트 스토리지를 기본 90일에서 최대 3년으로 연장할 수 있습니다. 스토리지 용량을 개선하면 네트워크 모니터링을 위한 장기 데이터 보존, 컴플라이언스 및 향상된 보안 가시성이 보장됩니다. 조직에서 이벤트 저장 또는 보존을 늘려야 하는 경우 이 작업을 수행합니다.

롤링 이벤트 스토리지 용량을 확장하거나 이벤트 클라우드 저장 용량을 늘리려면 다음 단계를 따르십시오.

1. [Cisco Commerce](#)에 사용자 어카운트로 로그인합니다.
2. Security Cloud Control PID를 선택합니다.
3. 프롬프트에 따라 스토리지 용량의 기간 또는 용량을 업그레이드합니다.

증가된 비용은 기존 라이선스의 남은 기간에 따라 비례 배분됩니다. 자세한 지침은 [Cisco Defense Orchestrator 제품 견적에 대한 지침](#)을 참조하십시오.

## Security Analytics and Logging

방화벽 디바이스의 **Security Analytics and Logging** 구성 및 이벤트 문제에 대한 실시간 알림을 수신합니다. 알림을 신속하게 처리하면 데이터 손실을 방지하고, 컴플라이언스를 유지하는 데 도움이 되며, 네트워크에서 신뢰할 수 있는 보안 모니터링을 보장할 수 있습니다.

매니지드 방화벽 디바이스에 대해 **Security Analytics and Logging** 구성과 이벤트 설정에 대한 알림을 확인합니다.

1. **Administration(관리) > Logging Settings(로깅 설정)**을 선택합니다.
2. **View Logging Storage Usage(로깅 스토리지 사용량 보기)** 버튼을 클릭합니다.



또는 왼쪽 내비게이션 바에서 **Events & Logs(이벤트 및 로그) > Events(이벤트) > Event Logging(이벤트 로깅)**로 이동한 다음 **View Dashboard(대시보드 보기)**를 클릭하여 **Security Analytics and Logging** 라이선스 정보를 확인합니다.

**Alerts and Notifications(알림 및 알림)** 섹션에는 이벤트 기록에 영향을 미치는 설정에 대한 알림이 표시됩니다. 이러한 알림을 통해 문제 해결을 위한 작업을 수행할 수 있습니다. 이러한 설정 중 일부는 다음과 같습니다.

- 클라우드 설정으로 이벤트 전송이 비활성화됩니다.
- 클라우드 설정으로 이벤트 전송이 디바이스 레벨에서 비활성화됩니다.
- 보안 이벤트 커넥터를 사용할 수 없게 됩니다.
- 이벤트 수집 속도가 증가합니다.
- 보안 분석 및 로깅 라이선스가 만료되었거나 할당된 데이터 스토리지가 초과됩니다.

## Security Analytics and Logging FAQ

어떤 이벤트가 **Security Analytics and Logging** 데이터 할당량에 포함되는지, 스토리지 한도를 관리하는 방법, 라이선스가 만료되면 어떻게 되는지, 보존 기간이 장기 데이터 스토리지에 미치는 영향에 대해 알아봅니다. 스토리지를 최적화하고 보안 이벤트 데이터에 대한 지속적인 액세스를 유지하기 위한 실질적인 팁을 얻으십시오.

### Security Analytics and Logging ?

Cisco 클라우드 또는 **Secure Event Connector**로 직접 전송된 모든 이벤트는 **Security Analytics and Logging**에 누적되며 데이터 할당량에 포함됩니다.

이벤트 뷰어를 필터링해도 **Security Analytics and Logging**에 저장된 이벤트 수는 줄어들지 않습니다. 이는 이벤트 뷰어에 표시되는 이벤트의 수만 줄여줄 뿐입니다.

?

이 문제를 해결하는 두 가지 방법은 다음과 같습니다.

- [추가 스토리지를 요청합니다.](#)

- 이벤트를 로깅하는 규칙의 수를 줄이는 것을 고려합니다. SSL 정책 규칙, 보안 인텔리전스 규칙, 액세스 제어 규칙, 침입 정책, 파일 및 멀웨어 정책에서도 이벤트를 로깅할 수 있습니다. 현재 로깅 설정을 검토하여, 구성된 모든 규칙 및 정책에 대한 이벤트를 로깅해야 하는지 확인합니다.

## Security Analytics and Logging ?

유료 Security Analytics and Logging 라이선스가 만료되면 방화벽에서 이벤트 수집이 즉시 중지됩니다. 그러나 180일의 유예 기간 동안 기존 데이터에 Security Analytics and Logging 클라우드에서 계속 액세스할 수 있습니다. 이 유예 기간 동안 유료 라이선스를 리뉴얼하는 경우 서비스가 중단 없이 계속 제공됩니다. 180일 이내에 라이선스를 리뉴얼하지 않으면 모든 데이터가 영구적으로 삭제됩니다.

### 1 5 Security Analytics and Logging , 5 ?

보존 기간은 각 로그가 저장되는 기간을 정의합니다. 1년의 보존 기간으로 인해, 특정 시점에서는 가장 최근 1년간의 로그 데이터만 이용 가능합니다. 1년 이상 된 로그 데이터는 새로운 데이터가 수집됨에 따라 덮어쓰기되거나 삭제됩니다. 5년 기간이란 해당 기간 동안 데이터가 계속 수집되지만, 보존 기간 제한은 로그 데이터 자체에 적용됨을 의미합니다.

## Catalyst SD-WAN Security Analytics and Logging

Catalyst SD-WAN는 고급 방화벽 및 보안 기능을 통합하여, 중앙 집중식 정책 적용과 안전한 클라우드 액세스를 가능하게 합니다. 디바이스를 Security Cloud Control에 온보딩하면 한 위치에서 연결 이벤트를 모니터링, 검색 및 분석할 수 있으므로 분산된 네트워크 전반에서 위협 추적 및 포괄적인 보안 관리를 지원할 수 있습니다.

보안 라우터는 방화벽 기능을 아키텍처에 통합하여 분산 네트워크 전반에 걸쳐 강력한 보안을 보장합니다.

- Catalyst SD-WAN은 SD-WAN 패브릭에 직접 보안 기능을 통합하여 보안 DIA(Direct Cloud Access) 및 DCA(Direct Cloud Access)를 활성화합니다.
- 차세대 방화벽, 통합 침입 방지 기능 및 URL 필터링을 포함합니다.
- Catalyst SD-WAN 플랫폼을 통해 모든 사용자에게 중앙 집중식 정책을 적용할 수 있으며, 기업 VPN 아키텍처를 프라이빗 클라우드로 확장할 수 있습니다.

매니지드 디바이스의 보안 기능을 관리하기 위해 Catalyst SD-WAN Manager을 Security Cloud Control에 온보딩합니다.

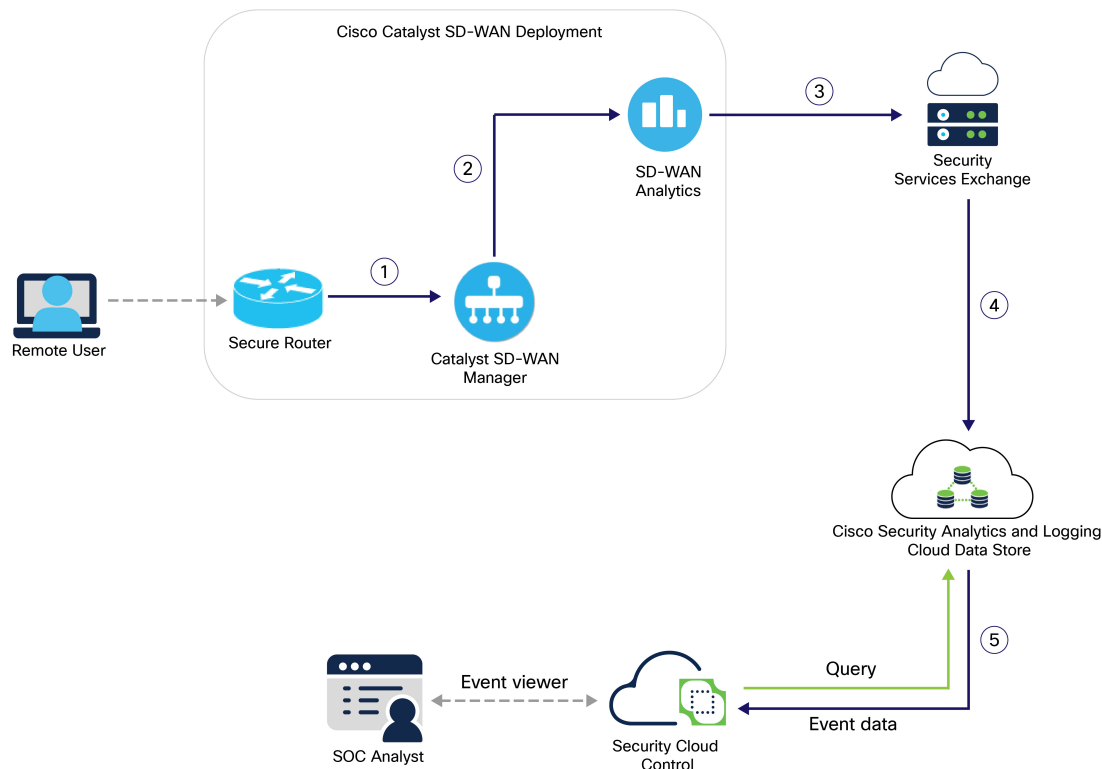
- 온보딩된 Catalyst SD-WAN 디바이스는 클라우드 데이터 저장소에 저장하기 위해 연결 이벤트를 Security Analytics and Logging로 전송합니다.
- Security Analytics and Logging를 통해 모든 Catalyst SD-WAN 디바이스의 연결 이벤트를 Security Cloud Control의 하나의 중앙 집중식 위치인 이벤트 로깅 페이지에서 확인할 수 있습니다.
- Event Logging(이벤트 로깅) 페이지에서 이벤트를 보고, 필터링하고, 검색하여 위협 추적을 수행하고 네트워크에서 트리거된 보안 규칙을 분석할 수 있습니다.

## Catalyst SD-WAN Security Cloud Control Firewall Management

Catalyst SD-WAN 이벤트 흐름을 통해 Security Cloud Control와 보안 이벤트를 자동으로 공유할 수 있어, 원활한 데이터 내보내기, 클라우드 저장 및 데이터 보강이 가능합니다. 이 통합을 통해 이벤트 가시성과 분석이 간소화되어, SOC 분석가들이 Catalyst SD-WAN 보안 데이터를 사용하여 네트워크 활동을 모니터링하고 위협 탐지 능력을 실시간으로 강화할 수 있게 됩니다.

이 다이어그램은 Catalyst SD-WAN가 Security Cloud Control에서 Security Cloud Control Firewall Management와 보안 이벤트를 공유하는 방법을 설명합니다.

### 1: Catalyst SD-WAN Security Cloud Control



| 단계 | 설명                                                                                                                                                                                                                                                                                |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 원격 사용자가 네트워크에 액세스하고 <b>Catalyst SD-WAN</b> 디바이스는 해당 트래픽에 대한 이벤트 로그를 생성합니다. 그런 다음 디바이스는 이벤트 데이터를 <b>PSV</b> 파일로 내보내고 <b>Catalyst SD-WAN Manager</b> 로 전송합니다.                                                                                                                       |
| 2  | <b>Catalyst SD-WAN Manager</b> 는 이벤트 데이터를 <b>SD-WAN 애널리틱스 클라우드</b> 로 전송합니다.                                                                                                                                                                                                       |
| 3  | <b>SD-WAN 애널리틱스 Security Services Exchange</b> 에서 액세스할 수 있도록 이벤트 데이터를 클라우드에 저장하고 <b>Security Services Exchange</b> 에 알립니다.<br><br><b>SD-WAN 애널리틱스 클라우드</b> 에서 알림을 수신한 후 <b>Security Services Exchange</b> 는 <b>SD-WAN AWS 클라우드</b> 에서 이벤트 데이터를 다운로드합니다.                           |
| 4  | <b>Security Services Exchange</b> 는 이벤트 데이터를 <b>PSV</b> 에서 <b>JSON</b> 형식으로 변환하여 <b>Cisco Security Analytics and Logging</b> 로 전송합니다.                                                                                                                                             |
| 5  | <b>SaaS(Security Analytics and Logging)</b> 는 다양한 서비스를 사용하여 이벤트 데이터를 처리하여 <b>Security Cloud Control</b> 에서 사용할 수 있도록 분류 및 보강합니다.<br><br><b>Security Analytics and Logging(SAL)</b> 은 이벤트 데이터를 클라우드 데이터 저장소에 저장합니다. 이벤트 뷰어는 이 데이터 저장소를 쿼리하여 보안 운영 센터(SOC) 분석가에게 관련 이벤트 데이터를 제공합니다. |

---

Catalyst SD-WAN Manager을 Security Cloud Control에 온보딩하면 연결 이벤트를 중앙에서 확인할 수 있습니다. Cisco Cloud에서 SD-WAN 보안 이벤트에 대한 컴플라이언스 및 효과적인 모니터링을 보장하기 위해, 일일 데이터 수집량을 추정하여 적합한 Security Analytics and Logging 구독 플랜을 선택합니다.

- Catalyst SD-WAN Manager를 보안 이벤트를 보려는 Security Cloud Control 조직에 온보딩. 자세한 내용은 [Security Cloud Control에 Catalyst SD-WAN Manager 온보딩](#) 페이지 14을 참조하십시오.
- SD-WAN 애널리틱스 서비스를 Catalyst SD-WAN Manager에 온보딩하고 데이터 수집을 활성화. 자세한 내용은 [Cisco SD-WAN Analytics 온보딩](#)을 참조하십시오.
- 유효한 Security Analytics and Logging 구독 플랜이 있는 Security Cloud Control Firewall Management 조직. 구독 플랜에 대한 자세한 내용은 [Security Analytics and Logging 라이선스](#) 페이지 51를 참조하십시오.
- 이 통합은 Security Cloud Control에서 Catalyst SD-WAN 디바이스에 발생하는 연결 이벤트를 확인하는 기능만 지원합니다.
- Cisco cloud에 온보딩된 Catalyst SD-WAN 디바이스에서 매일 수신되는 이벤트 수를 반영하는 Security Analytics and Logging 구독 플랜을 보유하고 있는지 확인하십시오. 이를 일일 수집 속도라고 합니다. [Logging Volume Estimator](#) 툴을 사용하여 일일 수집 속도를 예측할 수 있으며, 속도가 변경되면 데이터 요금제를 업데이트할 수 있습니다.
- Security Analytics and Logging 구독 플랜이 없는 경우 Security Cloud Control에 로그인하고 **Events & Logs**(이벤트 및 로그) > **Events**(이벤트) > **Event Logging**(이벤트 로깅) 탭으로 이동하여 90일 평가판을 요청할 수 있습니다. [Security Cloud Control Firewall Management 주문 가이드](#)의 지침을 따라 일일 사용량을 정확히 추정하고 원하는 구독 플랜을 구매할 수 있습니다.

## Security Cloud Control Firewall Management Catalyst SD-WAN

---

이벤트 로깅 페이지에서 Catalyst SD-WAN 연결 이벤트를 필터링하여 네트워크 활동 및 보안 이벤트를 신속하게 식별합니다. 이벤트 분석을 간소화하고, 위협 탐지를 강화하며, 컴플라이언스를 유지 관리하려면 이 기능을 사용합니다. 네트워크 관리자는 효과적인 보안 모니터링을 위해 이 작업을 정기적으로 수행해야 합니다.

[요건 및 지침](#) 페이지 60에서 모든 요건을 충족했는지 확인합니다.

- 
1. 탐색창에서 **Events & Logs**(이벤트 및 로그) > **Events**(이벤트) > **Event Logging**(이벤트 로깅)를 선택합니다.
  2. 필터 아이콘(▼)을 클릭합니다.
  3. **Catalyst SD-WAN Events(Catalyst SD-WAN Events)** 섹션으로 스크롤하여 **Connection**(연결) 체크박스를 선택합니다.
-

#### 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.