



## Cisco Defense Orchestrator를 사용한 FDM 디바이스 관리

초판: 2021년 3월 29일

### **Americas Headquarters**

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

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)

© 2021–2023 Cisco Systems, Inc. 모든 권리 보유.



## 목 차

---

서 문:

**Cisco Defense Orchestrator**를 사용한 FDM-관리 디바이스 관리 xxix

Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리 xxix

---

장 1

**Cisco Defense Orchestrator**의 기본 사항 1

네트워크 요구 사항 2

내부 인터페이스에서 FDM-관리 디바이스 관리 2

내부 인터페이스에서 FDM-관리 디바이스 관리 3

외부 인터페이스에서 FDM-관리 디바이스 관리 5

FDM-관리 디바이스의 외부 인터페이스 관리 6

CDO 테넌트 요청 8

라이선스 8

라이선스 정보 8

평가판 라이선스 9

클라우드 제공 Firewall Management Center 및 Threat Defense 라이선스 10

추가 지원 디바이스 및 라이선스 10

SDC(Secure Device Connector) 11

매니지드 디바이스에 Cisco Defense Orchestrator 연결 12

CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축 14

자체 VM에 보안 디바이스 커넥터 구축 18

Terraform 모듈을 사용하여 AWS VPC에 보안 디바이스 커넥터 구축 23

보안 디바이스 커넥터의 IP 주소 변경 24

보안 디바이스 커넥터 제거 26

SDC 간에 ASA 이동 27

Meraki MX 연결 자격 증명 업데이트 28

보안 디바이스 커넥터 이름 변경	28
보안 디바이스 커넥터 업데이트	29
단일 CDO 테넌트에서 여러 SDC 사용	29
동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기	30
보안 디바이스 커넥터 오픈 소스 및 서드파티 라이선스 특성	30
CDO에 로그인	39
새 CDO 테넌트에 대한 초기 로그인	40
로그인 실패 문제 해결	41
Cisco Secure Cloud Sign On ID 제공자로 마이그레이션	41
마이그레이션 후 로그인 실패 문제 해결	42
Cisco Secure Cloud Sign On 대시보드에서 CDO 실행	42
테넌트에서 슈퍼 관리자 관리	43
CDO에서 지원하는 소프트웨어 및 하드웨어	43
Secure Firewall Threat Defense 디바이스 지원 세부 사항	44
브라우저 지원	47
Cisco Defense Orchestrator 플랫폼 유지 관리 일정	47
테넌트 관리	48
일반 설정	48
사용자 설정	49
내 토큰	49
테넌트 설정	49
알림 설정	53
CDO 알림을 위한 서비스 통합 활성화	55
로깅 설정	57
SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 통합	58
SSO 인증서 갱신	58
API 토큰	58
API 토큰 형식 및 클레임	59
토큰 관리	59
ID 제공자 계정과 Cisco Defense Orchestrator 사용자 레코드 간의 관계	60
로그인 워크플로우	60

- 이 아키텍처의 의미 61
- 멀티 테넌트 포털 관리 62
  - 멀티 테넌트 포털에 테넌트 추가 63
  - 멀티 테넌트 포털에서 테넌트 삭제 64
  - 관리-테넌트 포털 설정 64
- Cisco Success Network 65
- 사용자 관리 66
  - 테넌트와 연결된 사용자 기록 보기 66
- 사용자 관리의 Active Directory 그룹 67
  - 시작하기 전에 68
  - 사용자 관리를 위한 Active Directory 그룹 추가 69
  - 사용자 관리를 위한 Active Directory 그룹 편집 70
  - 사용자 관리를 위한 Active Directory 그룹 삭제 71
- 새 CDO 사용자 생성 71
  - 새 사용자를 위해 Cisco Secure Cloud Sign On 계정 생성 71
    - CDO에 로그인 정보 71
    - 로그인하기 전에 72
  - 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성 72
- CDO 사용자 이름으로 CDO 사용자 레코드 생성 78
- 새 사용자가 Cisco Secure Sign-On 대시보드에서 CDO 열기 78
- Cisco Defense Orchestrator의 사용자 역할 79
  - 읽기 전용 역할 79
  - 편집 전용 역할 80
  - 배포 전용 역할 81
  - VPN 세션 관리자 역할 82
  - 관리자 역할 82
  - 슈퍼 관리자 83
  - 사용자 역할의 기록 변경 83
- 사용자 역할에 대한 사용자 레코드 생성 84
  - 사용자 레코드 생성 84
  - API 전용 사용자 생성 85

- 사용자 역할에 대한 사용자 레코드 편집 85
  - 사용자 역할 편집 86
- 사용자 역할에 대한 사용자 레코드 삭제 86
  - 사용자 레코드 삭제 86
- 서비스 페이지 정보 보기 87
- 디바이스 및 서비스 관리 90
  - CDO에서 디바이스의 IP 주소 변경 90
  - CDO에서 디바이스의 이름 변경 91
  - 디바이스 및 서비스 목록 내보내기 92
  - 디바이스 구성 내보내기 92
  - 디바이스의 외부 링크 93
    - 장치에서 외부 링크 생성 94
    - FDM에 대한 외부 링크 생성 94
    - 여러 디바이스에 대한 외부 링크 생성 95
    - 외부 링크 편집 또는 삭제 95
    - 여러 디바이스에 대한 외부 링크 편집 또는 삭제 96
  - CDO에 디바이스 대량 다시 연결 96
  - 테넌트 간 디바이스 이동 97
  - 디바이스 메모 작성 97
- 재고 목록 페이지 정보 보기 97
- 레이블 및 필터링 98
  - 디바이스 및 개체에 레이블 적용 98
  - 필터 99
- 동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기 100
- 검색 101
  - 글로벌 검색 101
    - 전체 인덱싱 시작 102
    - 전역 검색 수행 103
- CDO 명령줄 인터페이스 105
  - 명령줄 인터페이스 사용 105
  - 명령줄 인터페이스에 명령 입력 105

- 명령 기록 작업 106
- 대량 명령줄 인터페이스 107
  - 대량 CLI 인터페이스 107
  - 대량 명령 전송 108
  - 대량 명령 기록 작업 109
  - 대량 명령 필터 작업 109
    - 응답 기준 필터 109
    - 디바이스 기준 필터 110
- 디바이스 관리를 위한 CLI 매크로 111
  - 새 명령에서 CLI 매크로 생성 112
  - CLI 기록 또는 기존 CLI 매크로에서 CLI 매크로 생성 112
  - CLI 매크로 실행 113
  - CLI 매크로 편집 114
  - CLI 매크로 삭제 115
- 명령줄 인터페이스 설명서 115
- CLI 명령 결과 내보내기 115
  - CLI 명령 결과 내보내기 116
  - CLI 매크로의 결과 내보내기 116
  - CLI 명령 기록 내보내기 117
  - CLI 매크로 목록 내보내기 118
- 개체 118
  - 개체 유형 119
  - 공유 개체 121
  - 개체 재정의 122
  - 연결 해제된 개체 123
  - 개체 비교 124
  - 필터 125
    - 개체 필터 126
  - 개체 무시 128
  - 개체 삭제 129
    - 단일 개체 삭제 129

- 사용되지 않는 개체 그룹 삭제 129
  - 네트워크 개체 130
    - Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집 131
      - Firepower 네트워크 개체 생성 132
      - Firepower 네트워크 그룹 생성 133
      - Firepower 네트워크 개체 편집 134
      - Firepower 네트워크 그룹 편집 135
      - 개체 오버라이드 추가 136
      - 개체 오버라이드 편집 137
      - 공유 네트워크 그룹에 값 추가 137
      - 공유 네트워크 그룹의 추가 값 편집 139
      - 네트워크 개체 및 그룹 삭제 140
  - 애플리케이션 필터 개체 140
    - Firepower 애플리케이션 필터 개체 생성 및 편집 141
      - Firepower 애플리케이션 필터 개체 생성 141
      - Firepower 애플리케이션 필터 개체 편집 143
  - 지리위치 개체 143
    - Firepower 지리위치 필터 개체 생성 및 편집 144
      - 지리위치 개체 편집 144
  - DNS 그룹 개체 145
    - DNS 그룹 개체 생성 145
    - DNS 그룹 개체 편집 146
    - DNS 그룹 개체 삭제 146
    - DNS 그룹 개체를 FDM-관리 DNS 서버로 추가 147
  - 인증서 개체 147
    - 인증서 정보 147
    - 기능에 사용되는 인증서 유형 148
    - 인증서 구성 148
    - 내부 및 내부 CA 인증서 업로드 149
      - 절차 149
    - 신뢰할 수 있는 CA 인증서 업로드 150



절차	150
자체 서명 내부 및 내부 CA 인증서 생성	151
절차	152
IPsec 제안 구성	153
IKEv1 IPsec 제안 개체 관리	153
IKEv1 IPsec 제안 개체 생성 또는 편집	154
IKEv2 IPsec 제안 개체 관리	155
IKEv2 IPsec 제안 개체 생성 또는 편집	155
글로벌 IKE 정책 구성	156
IKEv1 정책 관리	156
IKEv1 정책 생성 또는 편집	157
IKEv2 정책 관리	158
IKEv2 정책 생성 또는 편집	158
RA VPN 개체	160
보안 영역 개체	160
Firepower 보안 영역 개체 생성 또는 편집	161
보안 영역 개체 생성	161
보안 영역 개체 편집	161
서비스 개체	162
Firepower 서비스 개체 생성 및 편집	163
Firepower 서비스 그룹 생성	164
Firepower 서비스 개체 또는 서비스 그룹 편집	165
보안 그룹 태그 그룹	165
보안 그룹 태그(Security Group Tags)	165
SGT 그룹 생성	167
SGT 그룹 편집	168
액세스 제어 규칙에 SGT 그룹 추가	168
시스템 로그 서버 개체	169
시스템 로그 서버 개체 생성 및 편집	169
Syslog 서버 개체 편집	170
SaaS(Secure Logging Analytics)를 위한 시스템 로그 서버 개체 생성	170

절차 171

URL 개체 171

    FDM-관리 URL 개체 생성 또는 편집 172

    Firepower URL 그룹 생성 173

    Firepower URL 개체 또는 URL 그룹 편집 173

장 2 디바이스 및 서비스 온보딩 175

    위협 방어 디바이스 온보딩 175

        내부 인터페이스에서 FDM-관리 디바이스 관리 178

        내부 인터페이스에서 FDM-관리 디바이스 관리 179

        외부 인터페이스에서 FDM-관리 디바이스 관리 181

        FDM-관리 디바이스의 외부 인터페이스 관리 182

    FDM-관리 디바이스를 CDO에 온보딩 183

        사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩 184

        등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩 186

        등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩 190

        디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩 195

        FDM-관리 고가용성 쌍 온보딩 204

        FTD 클러스터 온보딩 210

    스마트 라이선스 적용 또는 업데이트 211

        등록 키를 사용하여 온보딩 시 FDM-관리 디바이스에 스마트-라이선스 부여 212

        등록 키 또는 자격 증명을 사용하여 디바이스 온보딩 후 FDM-관리 디바이스에 스마트-라이선스 부여 214

        FTD 디바이스의 기존 스마트 라이선스 업데이트 214

        등록 키를 사용하여 온보딩된 FDM-관리 디바이스에 적용되는 스마트 라이선스 변경 214

        자격 증명을 사용하여 온보딩된 FDM-관리 디바이스에 적용되는 스마트 라이선스 변경 215

    FDM-관리 디바이스의 DHCP 주소 지정에 대한 CDO 지원 215

    FDM-관리 디바이스 라이선싱 유형 216

        가상 FDM-관리 디바이스 계층형 라이선스 218

        디바이스용 스마트-라이선스 보기 219

- 선택 가능한 라이선스 활성화 또는 비활성화 219
- 만료되거나 비활성화된 선택 가능한 라이선스의 영향 221
- Firewall Device Manager 모델 생성 및 가져오기 221
  - FDM-관리 디바이스 구성 내보내기 221
  - FDM-관리 디바이스 구성 가져오기 222
- CDO에서 디바이스 삭제 222
- 오프라인 관리를 위한 디바이스 컨피그레이션 가져오기 223
- FDM-관리 디바이스 백업 223
  - FDM-관리 온디맨드 디바이스 백업 224
    - 절차 225
  - 단일 FDM-관리 디바이스에 대한 반복 백업 일정 구성 225
    - 절차 225
- 디바이스 백업 다운로드 226
- 백업 편집 227
- 백업 삭제 227
- 디바이스 백업 관리 227
- FDM-관리 디바이스에 백업 복원 228
- FDM 소프트웨어 업그레이드 경로 229
  - 기타 업그레이드 제한 사항 231
  - 4100 및 9300 Series 디바이스 231
- FDM-관리 디바이스 업그레이드 사전 요건 232
- 단일 FTD 디바이스 업그레이드 233
  - Cisco Defense Orchestrator 저장소의 이미지로 단일 FDM-관리 디바이스 업그레이드 233
  - 자체 저장소의 이미지로 단일 FDM-관리 디바이스 업그레이드 234
  - 업그레이드 프로세스 모니터링 235
- 대량 FDM-관리 디바이스 업그레이드 235
  - Cisco Defense Orchestrator 저장소의 이미지로 대량 FDM-관리 디바이스 업그레이드 236
  - 자체 저장소의 이미지를 사용하여 대량 FDM-관리 디바이스 업그레이드 237
  - 대량 업그레이드 프로세스 모니터링 238
- FDM-관리 고가용성 쌍 업그레이드 238
  - Cisco Defense Orchestrator 저장소의 이미지로 FDM-관리 HA 쌍 업그레이드 238

자체 저장소의 이미지로 FDM-관리 HA 쌍 업그레이드 239  
 업그레이드 프로세스 모니터링 240  
 Snort 3.0으로 업그레이드 241  
 동시에 디바이스와 침입 방지 엔진 업그레이드 243  
 침입 방지 엔진 업그레이드 244  
 업그레이드 프로세스 모니터링 244  
 FDM-관리 디바이스용 Snort 3.0에서 되돌리기 245  
 Snort 3.0에서 되돌리기 245  
 보안 데이터베이스 업데이트 예약 246  
 예약된 보안 데이터베이스 업데이트 편집 247

---

**장 3**      **FTD 디바이스 구성 249**  
 인터페이스 250  
 Firepower 인터페이스 구성에 대한 지침 및 제한 사항 250  
     디바이스 모델별 VLAN 멤버의 최대 수 253  
 Firepower 데이터 인터페이스 254  
 관리/진단 인터페이스 255  
 인터페이스 설정 256  
     Firepower 인터페이스 설정에서 보안 영역 사용 256  
     보안 영역에 FDM-관리 디바이스 인터페이스 할당 257  
     Firepower 인터페이스 설정에서 자동 MDI/MDX 사용 258  
     Firepower 인터페이스 설정에서 MAC 주소 사용 258  
     Firepower 인터페이스 설정에서 MTU 설정 사용 258  
 Firepower 인터페이스용 IPv6 주소 지정 259  
 Firepower 인터페이스 구성 260  
     실제 Firepower 인터페이스 구성 261  
     Firepower VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성 265  
     고급 Firepower 인터페이스 옵션 구성 269  
     브리지 그룹 구성 271  
     FDM-관리 디바이스에 대한 EtherChannel 인터페이스 추가 277  
     FDM-관리 디바이스용 EtherChannel 인터페이스 편집 또는 제거 279

- EtherChannel 인터페이스에 하위 인터페이스 추가 281
- EtherChannel에서 하위 인터페이스 편집 또는 제거 282
- 가상 FDM-관리 디바이스에 인터페이스 추가 284
- FDM-관리 디바이스에 대한 스위치 포트 모드 인터페이스 285
- FDM-관리 디바이스 VLAN 구성 287
- 스위치 포트 모드에 대한 FDM-관리 디바이스 VLAN 구성 291
- Firepower 인터페이스 보기 및 모니터링 293
  - CLI에서 인터페이스 모니터링 293
- FXOS를 사용하여 Firepower 디바이스에 추가된 인터페이스 동기화 294
- 라우팅 295
  - 고정 라우팅 및 기본 경로 정보 295
    - 기본 라우터 295
    - 고정 경로 295
  - 라우팅 테이블과 경로 선택 296
    - 라우팅 테이블을 채우는 방법 296
    - 포워딩 결정 방법 297
  - FDM-관리 디바이스에 대한 고정 및 기본 경로 구성 298
    - 절차 298
    - 고정 경로 예시 299
  - 라우팅 모니터링 300
  - 고정 경로 네트워크 다이어그램 300
  - 가상 라우팅 및 포워딩 정보 301
- 개체 302
  - 개체 303
    - 개체 유형 304
    - 공유 개체 306
    - 개체 재정의 307
    - 연결 해제된 개체 308
    - 개체 비교 309
    - 필터 310
    - 개체 무시 313

- 개체 삭제 314
- 네트워크 개체 315
  - Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집 316
- 애플리케이션 필터 개체 325
  - Firepower 애플리케이션 필터 개체 생성 및 편집 325
- 지리위치 개체 328
  - Firepower 지리위치 필터 개체 생성 및 편집 329
- DNS 그룹 개체 330
  - DNS 그룹 개체 생성 330
  - DNS 그룹 개체 편집 331
  - DNS 그룹 개체 삭제 331
  - DNS 그룹 개체를 FDM-관리 DNS 서버로 추가 332
- 인증서 개체 332
  - 인증서 정보 332
  - 기능에 사용되는 인증서 유형 333
  - 인증서 구성 333
  - 내부 및 내부 CA 인증서 업로드 334
  - 신뢰할 수 있는 CA 인증서 업로드 335
  - 자체 서명 내부 및 내부 CA 인증서 생성 336
- IPsec 제안 구성 338
  - IKEv1 IPsec 제안 개체 관리 338
  - IKEv2 IPsec 제안 개체 관리 339
- 글로벌 IKE 정책 구성 341
  - IKEv1 정책 관리 341
  - IKEv2 정책 관리 343
- RA VPN 개체 345
- 보안 영역 개체 345
  - Firepower 보안 영역 개체 생성 또는 편집 345
- 서비스 개체 347
  - Firepower 서비스 개체 생성 및 편집 348
- 보안 그룹 태그 그룹 350



- 사용자 지정 Firepower 침입 방지 시스템 정책 388
- 보안 인텔리전스 정책 395
  - Firepower 보안 인텔리전스 정책 구성 395
  - Firepower 보안 인텔리전스 정책 차단 목록에 대한 예외 설정 397
  - Firepower 보안 인텔리전스 정책에 대한 보안 인텔리전스 피드 397
- FDM 매니지드 디바이스 ID 정책 398
  - Firepower ID 정책을 구현하는 방법 400
  - ID 정책 구성 401
  - ID 정책 설정 구성 403
  - Firepower ID 정책 기본 작업 구성 404
  - ID 규칙 구성 405
- SSL 암호 해독 정책 409
  - SSL 암호 해독 정책을 구현 및 유지 관리하는 방법 410
  - SSL 암호 해독 정보 411
  - SSL 암호 해독 정책 구성 416
  - 알려진 키 및 재서명 암호 해독을 위한 인증서 구성 428
  - 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드 429
- 규칙 집합 431
  - 디바이스에 대한 규칙 집합 구성 432
  - FDM-관리 템플릿이 포함된 규칙 집합 436
  - 기존 디바이스 규칙에서 규칙 집합 생성 436
  - OOB(Out of Band) 변경이 규칙 집합에 미치는 영향 437
  - 준비된 규칙 집합 변경 취소의 영향 438
  - 규칙 및 규칙 집합 보기 438
  - 규칙 집합 생성 후 로그 항목 변경 440
  - 선택한 규칙 집합에서 FTD 디바이스 분리 441
  - 규칙 및 규칙 집합 삭제 442
  - 선택한 FTD 디바이스에서 규칙 집합 제거 443
- 정책 및 규칙 집합의 규칙에 코멘트 추가 444
  - 규칙에 코멘트 추가 445
  - 정책 및 규칙 집합의 규칙에 대한 코멘트 편집 445



- 네트워크 주소 변환 447
- NAT 규칙 처리 순서 447
- 네트워크 주소 변환 마법사 449
  - NAT 마법사를 사용하여 NAT 규칙 생성 450
- NAT의 일반적인 사용 사례 450
  - 공용 IP 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화 451
  - 내부 네트워크의 사용자가 외부 인터페이스의 공용 IP 주소를 사용하여 인터넷에 액세스하도록 활성화 452
  - 공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정 453
  - 사설 IP 주소 범위를 공용 IP 주소 범위로 변환 456
  - 외부 인터페이스를 통과할 때 IP 주소 범위가 변환되지 않도록 방지 458
- 가상 프라이빗 네트워크 관리 459
  - 사이트 간 가상 프라이빗 네트워크 459
    - FDM-관리 디바이스에 대한 사이트 간 VPN 구성 460
    - 글로벌 IKE 정책 구성 478
    - IPsec 제안 구성 482
    - FDM-관리 디바이스 사이트 간 가상 사설망 모니터링 485
  - 원격 액세스 가상 프라이빗 네트워크 493
    - 원격 액세스 가상 프라이빗 네트워크 세션 494
    - FTD에 대한 원격 액세스 VPN 구성 499
- 템플릿 562
  - FDM-관리 디바이스 템플릿 563
  - FDM 템플릿 구성 564
    - FDM 템플릿 생성 564
    - FDM-관리 디바이스 템플릿 편집 566
    - FDM 템플릿 삭제 566
  - FDM 템플릿 적용 567
    - FDM-관리 디바이스에 템플릿 적용 569
    - 디바이스 및 네트워크 설정 검토 570
    - 디바이스에 변경 사항 구축 570
  - FDM-관리 디바이스 템플릿으로 ASA 구성 마이그레이션 571

- FDM-관리 고가용성 571
  - FDM-관리 관리 고가용성 쌍 요구 사항 573
  - FDM-관리 고가용성 쌍 생성 575
    - 절차 576
  - 고가용성의 FDM-관리 디바이스 페이지 577
    - 고가용성 관리 페이지 577
    - 고가용성 페일오버 기준 수정 577
  - FDM-관리 고가용성 페어링 끊기 578
  - FDM-관리 고가용성 쌍에서 강제 페일 오버 579
  - FDM-관리 고가용성 장애 조치 기록 580
  - FDM-관리 고가용성 상태 새로 고침 581
  - FDM-관리 고가용성용 페일오버 및 스테이트풀 링크 581
- FDM-관리 디바이스 설정 582
  - FTD 디바이스의 시스템 설정 구성 582
  - 관리 액세스 구성 583
    - 관리 인터페이스 규칙 생성 584
    - 데이터 인터페이스용 규칙 생성 584
  - 기록 설정 구성 585
    - 메시지 심각도 레벨 586
  - DHCP 서버 구성 587
  - DNS 서버 구성 589
  - 관리 인터페이스 589
    - 호스트 이름 590
  - NTP 서버 구성 590
  - URL 필터링 구성 591
  - 클라우드 서비스 592
    - Cisco Success Network에 연결 592
    - Cisco Cloud로 이벤트 전송 592
    - 웹 분석 활성화 또는 비활성화 593
- CDO 명령줄 인터페이스 594
  - 명령줄 인터페이스 사용 594

- 명령줄 인터페이스에 명령 입력 594
    - 명령 기록 작업 595
  - 대량 명령줄 인터페이스 596
    - 대량 CLI 인터페이스 596
    - 대량 명령 전송 597
    - 대량 명령 기록 작업 598
    - 대량 명령 필터 작업 598
      - 응답 기준 필터 598
      - 디바이스 기준 필터 599
  - 디바이스 관리를 위한 CLI 매크로 600
    - 새 명령에서 CLI 매크로 생성 601
    - CLI 기록 또는 기존 CLI 매크로에서 CLI 매크로 생성 601
    - CLI 매크로 실행 602
    - CLI 매크로 편집 603
    - CLI 매크로 삭제 604
  - 명령줄 인터페이스 설명서 604
  - CLI 명령 결과 내보내기 604
    - CLI 명령 결과 내보내기 605
    - CLI 매크로의 결과 내보내기 605
    - CLI 명령 기록 내보내기 606
    - CLI 매크로 목록 내보내기 607
  - CDO 공용 API 607
  - REST API 매크로 생성 608
    - API 툴 사용 608
    - Secure Firewall Threat Defense REST API 요청을 입력하는 방법 609
    - FTD REST API 매크로 정보 610
      - REST API 매크로 생성 611
      - REST API 매크로 실행 613
      - REST API 매크로 편집 614
      - REST API 매크로 삭제 615
  - 변경 사항 읽기, 삭제, 확인 및 구축 615

- 모든 디바이스 구성 읽기 616
- FDM-관리 디바이스에서 CDO로 구성 변경 사항 읽기 618
  - 변경 취소 절차 618
  - 보류 중인 변경 사항 되돌리기가 실패하는 경우 619
  - 충돌 검토 절차 619
  - 검토 없이 수락 절차 620
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축 620
- CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축 621
- 디바이스에 변경 사항 배포 622
  - 변경 취소 623
  - 변경 사항 취소 623
- 디바이스 구성 대량 구축 623
- 예약된 자동 배포 624
  - 자동 구축 예약 624
  - 예약된 배포 편집 625
  - 예약된 배포 삭제 625
- 구성 변경 사항 확인 626
- 변경 사항 취소 627
- 디바이스의 대역 외 변경 사항 628
- Defense Orchestrator와 디바이스 간 구성 동기화 628
  - 충돌 탐지 629
    - 충돌 탐지 활성화 629
- 디바이스에서 대역외 변경 사항 자동 수락 630
  - 변경 사항 자동 수락 구성 630
  - 테넌트의 모든 디바이스에 대한 변경 사항 자동 수락 비활성화 631
- 구성 충돌 해결 631
  - "동기화되지 않음" 상태 해결 631
  - "충돌 탐지됨" 상태 해결 632
- 디바이스 변경 사항에 대한 폴링 예약 632
- 보안 데이터베이스 업데이트 예약 633
  - 예약된 보안 데이터베이스 업데이트 생성 633

예약된 보안 데이터베이스 업데이트 편집 634  
 FDM-관리 디바이스 보안 데이터베이스 업데이트 635  
 워크플로우 636

장 4

모니터링 및 보고 639  
 변경 로그 639  
 FDM-관리 디바이스에 구축한 후 로그 항목 변경 641  
 FDM-관리 디바이스에서 변경 사항을 읽은 후 로그 항목 변경 641  
 변경 로그 차이 보기 642  
 변경 로그를 CSV 파일로 내보내기 643  
 CDO의 변경 로그 용량과 내보낸 변경 로그 크기의 차이 643  
 변경 요청 관리 644  
 변화 요청 관리 활성화 644  
 변경 요청 생성 644  
 변경 요청을 변경 로그 이벤트와 연결 645  
 변경 요청으로 변경 로그 이벤트 검색 645  
 변경 요청 검색 645  
 변경 요청 필터링 645  
 변경 요청 톨바 지우기 646  
 변경 로그 이벤트와 관련된 변경 요청 지우기 646  
 변경 요청 삭제 646  
 변화 요청 관리 비활성화 647  
 활용 사례 647  
 FDM-관리 디바이스 개요 보고서 648  
 FDM-관리 디바이스 요약 보고서 생성 649  
 작업 페이지 650  
 작업이 실패한 대량 작업 다시 시작 651  
 대량 작업 취소 652  
 워크플로우 페이지 652

장 5

Cisco Security Analytics and Logging 655

Security Analytics and Logging(SaaS) 정보	656
FDM-관리 디바이스에 대한 보안 로깅 분석	656
FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현	665
Cisco Defense Orchestrator 이벤트 로깅에 FDM 이벤트 전송	668
FDM-관리 이벤트를 Cisco Cloud에 직접 전송	668
FDM-관리 이벤트 유형	669
보안 이벤트 커넥터	670
보안 이벤트 커넥터 설치	671
SDC 가상 머신에 SEC(Secure Event Connector) 설치	671
CDO 이미지를 사용하여 SEC 설치	674
CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치	675
CDO 커넥터 VM에 보안 이벤트 커넥터 설치	679
VM 이미지를 사용하여 SEC 설치	680
VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치	681
생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성	686
CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치	686
Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치	689
Cisco Security Analytics and Logging(SaaS) 프로비저닝	690
보안 이벤트 커넥터 제거	690
CDO에서 SEC 제거	690
SDC에서 SEC 파일 제거	691
Cisco Secure Cloud Analytics 포털 프로비저닝	691
Secure Cloud Analytics에서 센서 상태 및 CDO 통합 상태 검토	693
전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축	693
CDO에서 Cisco Secure Cloud Analytics 알림 보기	694
Secure Cloud Analytics 포털에 사용자 초대	695
CDO에서 Secure Cloud Analytics로 교차 실행	695
Cisco Secure Cloud Analytics 및 동적 엔티티 모델링	695
방화벽 이벤트 기반 알림 작업	697
열린 알림 분류	698
나중에 분석하기 위해 알림 일시 중지	698

추가 조사를 위해 알람 업데이트	699
알람 검토 및 조사 시작	699
엔터티 및 사용자 검사	701
Secure Cloud Analytics를 사용하여 문제 해결	702
알람 업데이트 및 닫기	703
알람 우선순위 수정	703
라이브 이벤트 보기	704
라이브 이벤트 재생/일시 중지	704
과거 이벤트 보기	705
이벤트 보기 사용자 지정	706
이벤트 로깅 페이지의 열 표시 및 숨기기	707
사용자 지정 가능한 이벤트 필터	710
Security Analytics and Logging의 이벤트 속성	711
일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성	712
Syslog 이벤트에 대한 이벤트 이름 속성	714
시스템 로그 이벤트의 시간 속성	733
Cisco Secure Cloud Analytics 및 동적 엔터티 모델링	735
방화벽 이벤트 기반 알람 작업	736
열린 알람 분류	737
나중에 분석하기 위해 알람 일시 중지	738
추가 조사를 위해 알람 업데이트	738
알람 검토 및 조사 시작	739
엔터티 및 사용자 검사	741
알람 업데이트 및 닫기	741
알람 우선순위 수정	742
이벤트 로깅 페이지에서 이벤트 검색 및 필터링	742
라이브 또는 과거 이벤트 필터링	743
NetFlow 이벤트만 필터링	744
ASA 또는 FDM-관리 장치 syslog 이벤트에 대한 필터링(ASA NetFlow 이벤트 제외)	745
필터 요소 결합	745
백그라운드에서 기록 이벤트 검색	750

이벤트 로깅 페이지에서 이벤트 검색 750

이벤트 뷰어에서 백그라운드 검색 예약 751

백그라운드 검색 다운로드 752

데이터 스토리지 요금제 752

이벤트 스토리지 기간 연장 및 이벤트 스토리지 용량 늘리기 753

보안 애널리틱스 및 로깅 데이터 계획 사용량 보기 754

SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기 755

장 6 CDO와 Cisco Security Cloud Sign On 통합 757

SecureX 및 CDO 757

CDO 및 SecureX 계정 병합 758

CDO를 SecureX에 추가 758

CDO에서 SecureX 연결 759

CDO에서 SecureX 연결 끊김 760

CDO 타일을 SecureX에 추가 760

장 7 문제 해결 763

FDM-관리 디바이스 문제 해결 763

총괄 요약 보고서 문제 해결 763

FTD 온보딩 문제 해결 764

라이선스 부족으로 인해 실패 764

등록되지 않은 디바이스 문제 해결 765

등록 키로 온보딩 중 디바이스 등록 실패 문제 해결 766

침입 방지 시스템 문제 해결 767

SSL 암호 해독 문제 해결 767

일련 번호를 사용하여 FDM-관리 디바이스 온보딩 문제 해결 769

클레임 오류 769

프로비저닝 오류 772

FDM-관리 HA 생성 문제 해결 773

보안 디바이스 커넥터 문제 해결 774

SDC에 연결할 수 없음 774



- 배포 후 SDC 상태가 CDO에서 활성화되지 않음 774
- SDC의 변경된 IP 주소가 CDO에 반영되지 않음 775
- SDC와의 디바이스 연결 문제 해결 775
- 간헐적으로 또는 SDC에 연결되지 않음 776
- 보안 디바이스 커넥터에 영향을 미치는 컨테이너 권한 상승 취약점: cisco-sa-20190215-runc 777
  - CDO-표준 SDC 호스트 업데이트 777
  - 사용자 지정 SDC 호스트 업데이트 778
  - 버그 추적 778
- 보안 이벤트 커넥터 문제 해결 778
  - SEC 온보딩 실패 문제 해결 779
  - 보안 이벤트 커넥터 등록 실패 문제 해결 782
  - 보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결 782
  - NSEL 데이터 플로우 문제 해결 783
  - 문제 해결 로그 파일 이벤트 로깅 784
    - 문제 해결 스크립트 실행 784
    - sec\_troubleshoot.tar.gz 파일 압축 해제 785
  - SEC 부트스트랩 데이터를 생성하지 못했습니다. 786
  - 온보딩 후 CDO 보안 커넥터 페이지에서 SEC 상태가 "비활성"임 786
  - SEC가 "온라인"이지만 CDO 이벤트 로깅 페이지에 이벤트가 없습니다 787
  - SEC Cleanup 명령 788
    - SEC Cleanup 명령 실패 789
    - 상태 확인을 사용하여 보안 이벤트 커넥터의 상태 학습 789
- 문제 해결 Cisco Defense Orchestrator 790
  - 로그인 실패 문제 해결 790
    - 마이그레이션 후 로그인 실패 문제 해결 791
  - 액세스 및 인증서 문제 해결 791
    - 새 지문 탐지 상태 확인 791
    - 보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결 792
    - SSL 암호 해독 문제 해결 793
    - 침입 방지 시스템 문제 해결 794
    - 마이그레이션 후 로그인 실패 문제 해결 794

개체 문제 해결 795

- 중복 개체 문제 해결 795
- 일관성이 없거나 사용되지 않는 보안 영역 개체 해결 796
- 사용되지 않는 개체 문제 해결 796
- 불일치 개체 문제 해결 797
- 대량의 개체 문제 해결 799

디바이스 연결 상태 800

- 등록되지 않은 디바이스 문제 해결 802
- 라이선스 부족 문제 해결 802
- 유효하지 않은 자격 증명 문제 해결 803
- 새 인증서 문제 트러블슈팅 804
  - 새 인증서 탐지됨 812
- 온보딩 오류 문제 해결 813
- "충돌 탐지됨" 상태 해결 813
- "동기화되지 않음" 상태 해결 814
- 연결할 수 없는 연결 상태 문제 해결 814

SecureX 문제 해결 816

장 8

**FAQ 및 지원 819**

Cisco Defense Orchestrator 819

Cisco Defense Orchestrator에 디바이스 온보딩 관련 FAQ 820

- CDO에 Secure Firewall ASA 온보딩 관련 FAQ 820
- CDO에 FDM 매니지드 디바이스 온보딩 관련 FAQ 820
- 클라우드 사용 Firewall Management Center에 Secure Firewall Threat Defense 온보딩 관련 FAQ 820
- 온프레미스 Secure Firewall Management Center 관련 FAQ 821
- CDO에 Meraki 디바이스 온보딩 관련 FAQ 821
- CDO에 SSH 디바이스 온보딩 관련 FAQ 821
- CDO에 IOS 디바이스 온보딩 관련 FAQ 822

디바이스 유형 822

보안 823

문제 해결 825

로우 터치(Low-Touch) 프로비저닝에 사용되는 용어 및 정의 825

정책 최적화 826

연결성 826

CLI를 사용하여 Secure Firewall Threat Defense 디바이스의 초기 구성 완료 827

데이터 인터페이스 정보 831

CDO가 개인 정보를 처리하는 방법 831

Cisco Defense Orchestrator 지원팀에 문의 831

    워크플로우 내보내기 831

TAC를 사용하여 지원 티켓 열기 832

    CDO 고객이 TAC로 지원 티켓을 여는 방법 832

    CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법 834

CDO 서비스 상태 페이지 835





## Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리

• Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리, xxix 페이지

# Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리



중요 Secure Firewall device manager(FDM) 지원 및 기능은 요청 시에만 제공됩니다. 테넌트에서 Firewall Device Manager 지원을 아직 활성화하지 않은 경우 디바이스를 관리하거나 FDM 관리 디바이스에 구축할 수 없습니다. [TAC를 사용하여 지원 티켓 열기](#)에 요청을 보냅니다.

Cisco Defense Orchestrator는 간소화된 관리 인터페이스와 Secure Firewall device manager 디바이스에 대한 클라우드 액세스를 제공합니다. FDM 관리 관리자는 디바이스 인터페이스와 CDO 인터페이스 간에 많은 유사성을 확인할 수 있습니다. 관리자 간에 가능한 한 일관성을 유지하기 위해 CDO를 구축했습니다.

CDO를 사용하여 물리적 또는 가상 FDM 관리 디바이스의 다음 측면을 관리합니다.

- 위협 방어 디바이스 온보딩
- 디바이스 관리
- 디바이스 업그레이드
- ASA-위협 방어 마이그레이션
- 인터페이스 관리
- 라우팅
- 고가용성
- 보안 정책

- 정책 및 구성 일관성 승격
- 사이트 간 VPN
- 원격 액세스 VPN
- 네트워크 모니터링
- Cisco Security Analytics and Logging

소프트웨어 및 하드웨어 지원

CDO는 다양한 디바이스 또는 가상 머신에 설치할 수 있는 버전 6.4 이상을 지원합니다. 자세한 내용은 [Secure Firewall Threat Defense 디바이스 지원 세부 사항](#)을 참조하십시오.

스마트 라이선스 관리

Cisco Smart License를 사용하여 FDM 관리 디바이스를 CDO에 온보딩하는 동안 또는 디바이스를 온보딩한 후에 라이선싱할 수 있습니다. 스마트 라이선싱은 워크플로우에 편리하게 내장되어 있으며 CDO 인터페이스에서 쉽게 액세스할 수 있습니다. 자세한 내용은 [스마트 라이선스 적용 또는 업데이트](#)를 참조하십시오.



**참고** 온보딩하려는 디바이스가 소프트웨어 버전 6.4 또는 6.5를 실행 중이고, 이미 스마트 라이선스가 있는 경우, 해당 디바이스는 Cisco Smart Software Manager에 등록되어 있을 가능성이 높습니다. 등록 키를 사용하여 CDO에 온보딩하기 전에 **Cisco Smart Software Manager**에서 디바이스를 등록 취소해야 합니다. 등록을 취소하면 디바이스에 연결된 라이선스 및 선택 가능한 모든 라이선스가 가상 어카운트에서 해제됩니다.

온보딩하려는 디바이스가 소프트웨어 버전 6.6 이상을 실행 중이고, Cisco Cloud에 이미 등록되어 있는 경우, 등록 키를 사용하여 CDO에 온보딩하기 전에 **Cisco Cloud Services**에서 디바이스를 등록 취소해야 합니다.

**CDO 사용자 인터페이스**

**CDO GUI 및 CLI 인터페이스**

CDO는 그래픽 사용자 인터페이스(GUI)와 명령줄 인터페이스(CLI)를 모두 제공하는 웹 기반 관리 제품으로, 디바이스를 한 번에 하나씩 관리하거나 여러 디바이스를 동시에 관리할 수 있습니다.

CLI 인터페이스를 사용하면 CDO에서 직접 FDM 관리 디바이스로 명령을 전송할 수 있습니다. CLI 매크로를 사용하여 일반적으로 사용되는 명령을 저장하고 실행합니다. 자세한 내용은 [명령줄 인터페이스 설명서](#) 및 [CDO 명령줄 인터페이스, 105 페이지](#)의 내용을 참조하십시오.

**API 지원**

CDO는 기기의 REST API를 사용하여 FDM 관리 디바이스에서 고급 작업을 수행할 수 있는 API 도구 인터페이스를 제공합니다. 또한 이 인터페이스는 다음 기능을 제공합니다.

- 이미 실행된 API 명령의 기록을 기록합니다.
- 재사용할 수 있는 시스템 정의 API 매크로를 제공합니다.
- 이미 실행한 명령 또는 다른 사용자 정의 매크로에서 표준 API 매크로를 사용하여 사용자 정의 API 매크로를 생성할 수 있습니다.

API 틀에 대한 자세한 내용은 [API 틀 사용, 608 페이지](#)의 내용을 참조하십시오.

### FDM-관리 디바이스 온보딩

[위협 방어 디바이스 온보딩](#)하기 전에 일반 디바이스 요구 사항 및 온보딩 사전 요건을 검토합니다.

등록 토큰을 사용하여 FDM 관리 디바이스를 온보딩하는 것이 가장 좋습니다. 자세한 내용은 [등록 토큰을 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.

다음과 같은 추가 방법을 사용하여 FDM 관리 디바이스를 CDO에 온보딩할 수도 있습니다.

- 사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩, [184 페이지](#)
- 로우터치 프로비저닝을 사용하여 FDM-관리 디바이스를 온보딩하기 위한 워크플로우 및 전제 조건
- 로우터치 프로비저닝을 사용하여 FDM-관리 디바이스를 온보딩하기 위한 워크플로우 및 전제 조건, [196 페이지](#)

### 디바이스 관리

CDO를 사용하여 소프트웨어를 업그레이드하고, 고가용성을 구성하고, FDM 관리 디바이스에 대한 디바이스 설정 및 네트워크 리소스를 구성합니다.

- 시스템 설정. FDM 관리 디바이스에 라이선스를 부여하고 온보딩한 후에는 [FDM-관리 디바이스 설정](#)할 수 있습니다. 관리 액세스 프로토콜, 로깅 설정, DHCP 및 DNS 서버 상호 작용, 디바이스의 호스트 이름, 디바이스가 사용하는 시간 서버, URL 필터링 기본 설정을 구성할 수 있습니다.
- 보안 데이터베이스 업데이트. 필요한 경우 디바이스를 확인하고 업데이트하는 반복 작업을 통해 디바이스를 최신 상태로 유지하고 최신 [FDM-관리 디바이스 보안 데이터베이스 업데이트](#)를 준수합니다.
- 고가용성. [FDM-관리 고가용성 쌍 업그레이드](#)에서 HA 구성 및 작업을 관리합니다.

### 디바이스 업그레이드

다음 방법 중 하나를 사용하여 FDM 관리 디바이스에 대한 업그레이드를 즉시 수행하거나 예약합니다.

- 단일 FTD 디바이스 업그레이드.
- 대량 FDM-관리 디바이스 업그레이드.
- FDM-관리 고가용성 쌍 업그레이드.

## ASA-위협 방어 마이그레이션

CDO는 ASA(Adaptive Security Appliance)를 FDM 관리 디바이스로 마이그레이션하는 데 도움이 됩니다. CDO는 ASA에서 실행 중인 구성의 이러한 요소를 Firewall Device Manager 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

이 마이그레이션은 다음 요소에 대해 지원됩니다.

- 액세스 제어 규칙(ACL)
- 인터페이스
- NAT(네트워크 주소 변환) 규칙
- 네트워크 개체 및 네트워크 그룹 개체
- 경로
- 서비스 개체 및 서비스 그룹 개체
- 사이트 간 VPN

자세한 내용은 [FDM-관리 디바이스 템플릿으로 ASA 구성 마이그레이션](#)을 참조하십시오.

## 인터페이스 관리

CDO를 사용하여 FDM 관리 디바이스에서 [Firepower 인터페이스 구성](#)할 수 있습니다.

## 라우팅

라우팅은 소스에서 대상까지 네트워크에 걸친 정보의 이동입니다. 라우팅에는 2가지 기본적인 작업이 포함되는데, 최적의 라우팅 경로를 결정하는 것과 네트워크를 통한 패킷 전송입니다. CDO를 사용하여 라우팅의 다음 측면을 구성합니다.

- 정적 경로 및 기본 경로 구성. CDO를 사용하여 FDM 관리 디바이스에 대한 [기본 라우터](#)할 수 있습니다.
- 브리지 그룹 지원. 브리지 그룹은 하나 이상의 인터페이스를 그룹화하는 가상 인터페이스입니다. 인터페이스를 그룹화하는 주요 이유는 스위치 인터페이스 그룹을 생성하기 위해서입니다. CDO를 사용하여 디바이스에서 [브리지 그룹 구성](#)할 수 있습니다.
- **NAT(Network Address Translation)**. NAT 규칙은 내부(프라이빗) 네트워크에서 인터넷으로 트래픽을 라우팅하는 데 도움이 됩니다. 또한 NAT 규칙은 네트워크 외부에서 내부 IP 주소를 숨겨 보안 역할을 합니다. CDO를 사용하여 디바이스에 대한 NAT 규칙을 생성하고 편집할 수 있습니다. 자세한 내용은 [네트워크 주소 변환, 447 페이지](#)를 참조하십시오.

## 보안 정책

보안 정책은 네트워크 트래픽이 의도한 대상에 도달하도록 허용하거나 방지하는 최종 목표를 사용하여 네트워크 트래픽을 검사합니다. CDO를 사용하여 디바이스 보안 정책의 모든 구성 요소를 관리합니다.



- 규칙을 복사하여 붙여넣습니다. 정책 간에 규칙을 복사하여 붙여넣어 여러 정책에서 쉽게 공유할 수 있습니다. 자세한 내용은 [FDM-관리 액세스 제어 규칙 복사](#)를 참조하십시오.
- **SSL 암호 해독 정책.** HTTPS와 같은 일부 프로토콜은 SSL(Secure Sockets Layer) 또는 그 후속 버전인 TLS(Transport Layer Security)를 사용하여 안전한 전송을 위해 트래픽을 암호화합니다. 시스템에서는 암호화된 연결을 검사할 수 없으므로 상위 레이어의 트래픽 특성을 고려하여 액세스 의사 결정을 내리는 액세스 규칙을 적용하려면 SSL 암호 해독 정책을 적용하여 암호를 해독해야 합니다. 자세한 내용은 [SSL 암호 해독 정책](#)을 참조하십시오.
- **ID 정책.** 연결에서 사용자 ID 정보를 수집하기 위해 [절차](#)를 사용합니다. 그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고 사용자 또는 사용자 그룹을 기준으로 액세스 제어를 구성할 수 있습니다.
- **보안 인텔리전스 정책.** [보안 인텔리전스 정책](#)을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 시스템은 액세스 제어 정책을 사용하여 차단 목록에 추가된 트래픽을 평가 전에 삭제하며, 이에 따라 사용된 시스템 리소스의 양이 줄어듭니다.
- **액세스 제어 정책.** 액세스 제어 정책은 액세스 제어 규칙에 대해 네트워크 트래픽을 평가하여 네트워크 리소스에 대한 액세스를 제어합니다. Secure Firewall Device Manager는 액세스 제어 정책에 나타나는 순서대로 액세스 제어 규칙의 기준을 네트워크 트래픽과 비교합니다. 액세스 제어 규칙의 모든 트래픽 조건이 일치하면 Secure Firewall Device Manager는 규칙에 정의된 작업을 수행합니다. CDO를 사용하여 [FDM 액세스 제어 정책 구성](#)할 수 있습니다.
- **TLS 1.3 서버 ID 검색.** 버전 6.7에서 도입된 이 기능을 사용하면 TLS 1.3으로 암호화된 트래픽에서 URL 필터링 및 애플리케이션 제어를 수행할 수 있습니다. 자세한 내용은 [절차](#)를 참조하십시오.
- **침입 정책.** Cisco는 Firepower System에서 여러 침입 정책을 제공합니다. 이러한 정책은 Cisco Talos Security Intelligence and Research Group에서 설계했습니다. 여기서는 고급 설정과 침입 및 전처리 규칙 구문 상태를 설정합니다. 침입 정책은 액세스 제어 규칙의 측면입니다. 자세한 내용은 [FDM-관리 액세스 제어 규칙의 침입 정책 설정](#)을 참조하십시오.



**참고** Snort 3은 버전 6.7 이상을 실행하는 FDM 관리 디바이스에서 사용할 수 있습니다. Snort 2와 Snort 3 간에 전환할 수는 있지만 구성이 호환되지 않을 수 있습니다. Snort 3, 지원되는 디바이스 및 소프트웨어, 제한 사항에 대한 자세한 내용은 [Snort 3.0으로 업그레이드, 241 페이지](#)의 내용을 참조하십시오.

- **위협 이벤트.** [위협 이벤트](#)는 Cisco Talos의 침입 정책 중 하나와 일치한 후 삭제되거나 알림이 생성된 트래픽에 대한 보고서입니다. 대부분의 경우 IPS 규칙을 조정할 필요가 없습니다. 필요한 경우 CDO에서 일치 규칙 작업을 변경하여 이벤트 처리 방식을 오버라이드할 수 있습니다. CDO는 버전 6.4 및 6.6.1의 모든 버전에서 IPS 규칙 조정을 지원합니다. CDO는 버전 6.5, 6.6.1 이외의 6.6 버전 또는 6.7 버전에서 IPS 규칙 조정을 지원하지 않습니다.

- **NAT(Network Address Translation)**. **NAT 규칙 처리 순서**은 내부(프라이빗) 네트워크에서 인터넷으로 트래픽을 라우팅하는 데 도움이 됩니다. 또한 NAT 규칙은 네트워크 외부에서 내부 IP 주소를 숨겨 보안 역할을 합니다. CDO를 사용하여 Firepower Threat Defense에 대한 NAT 규칙을 생성하고 편집할 수 있습니다.

정책 및 구성 일관성 승격


개체 관리

개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 수정하면 해당 개체를 사용하는 다른 모든 정책에 영향을 미치므로 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 개체가 없으면 동일한 변경이 필요한 모든 정책을 개별적으로 수정해야 합니다.

CDO를 사용하여 다음 **개체 유형**을 생성하고 관리합니다.

- **Active Directory** 영역 개체 생성 또는 편집
- **RA VPN AnyConnect** 클라이언트 프로파일 업로드
- 애플리케이션 필터 개체
- 인증서 개체
- DNS 그룹 개체
- 지리위치 개체
- FDM-관리 장치에 대한 ID 소스 구성
- IKEv1 정책 관리
- IKEv1 IPsec 제안 개체 관리
- IKEv2 정책 관리
- IKEv2 IPsec 제안 개체 관리
- Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집
- 새 RA VPN 그룹 정책 생성
- 보안 영역 개체
- 서비스 개체
- 보안 그룹 태그(Security Group Tags)
- 시스템 로그 서버 개체 생성 및 편집
- FDM-관리 URL 개체 생성 또는 편집

## 개체 문제 해결

CDO에서는 여러 디바이스에서 사용되는 개체를 "공유 개체"라고 부르고 Objects(개체) 페이지에서 이 배지 로 식별합니다. 때때로 공유 객체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디바이스에서 완벽하게 공유되지 않습니다. CDO는 [중복 개체 문제 해결](#), [사용되지 않는 개체 문제 해결](#) 및 [불일치 개체 문제 해결](#)을 쉽게 하여 디바이스와 개체 저장소를 관리할 수 있습니다.

## 템플릿

Secure Firewall Device Manager 템플릿은 온보딩된 FDM 관리 디바이스 구성의 전체 복사본입니다. 그런 다음 해당 템플릿을 수정하고 관리하는 다른 FDM 관리 디바이스를 구성하는 데 사용할 수 있습니다. Secure Firewall Device Manager 템플릿은 디바이스 간의 정책 일관성을 촉진합니다. 자세한 내용은 [FDM-관리 디바이스 템플릿](#)을 참조하십시오.

## 고가용성

CDO를 사용하면 [FDM-관리 고가용성 쌍 생성](#)을 쉽게 구성하고 관리할 수 있습니다. 기존 HA 쌍을 온보딩하거나 CDO에서 HA 쌍을 생성할 수 있습니다. HA 구성을 사용하면 업그레이드 기간 또는 예기치 않은 디바이스 장애와 같이 디바이스를 사용할 수 없는 시나리오에서 보안 네트워크를 유지할 수 있습니다. 장애 조치 모드에서 스탠바이 디바이스는 이미 액티브 상태가 되도록 구성되어 있습니다. 즉, HA 디바이스 중 하나를 사용할 수 없는 경우에도 다른 디바이스가 트래픽을 계속 처리합니다.

CDO에서 FDM 관리 HA 쌍을 업그레이드할 수 있습니다. 자세한 내용은 [FDM-관리 고가용성 쌍 업그레이드](#)를 참조하십시오.

## 가상 프라이빗 네트워크 구성

### 사이트 간 VPN

VPN(가상 사설망)은 보안되지 않은 네트워크를 통해 개인 데이터를 서로 안전하게 전송하여 네트워크를 네트워크에 연결하는 여러 원격 피어로 구성됩니다. CDO는 터널을 사용하여 IP 기반 네트워크를 통한 전달을 위해 일반 IP 패킷 내에서 데이터 패킷을 캡슐화하고, 암호화를 사용하여 개인 정보를 보호하고 인증을 통해 데이터 무결성을 보장합니다. 자세한 내용은 [사이트 간 가상 프라이빗 네트워크](#)를 참조하십시오.

가상 사설 네트워크에 대한 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)를 참조하십시오.

### 원격 액세스 VPN

RA(Remote Access) VPN을 통해 개인은 지원되는 노트북, 데스크톱 및 모바일 디바이스를 사용하여 네트워크에 대한 보안 연결을 설정할 수 있습니다. CDO는 FDM 관리 디바이스에서 RA VPN을 설정할 수 있는 직관적인 사용자 인터페이스를 제공합니다. AnyConnect는 FDM 관리 디바이스에 대한 RA VPN 연결을 위해 엔드포인트 디바이스에서 지원되는 유일한 클라이언트입니다.

CDO는 FDM 관리 디바이스에서 RA VPN 기능의 다음 측면을 지원합니다.

- 프라이버시, 인증 및 데이터 무결성을 위한 TLS(Transport Layer Security) 또는 DTLS(Datagram Transport Layer Security)

- SSL 클라이언트 기반 원격 액세스
- IPv4 and IPv6 addressing
- 여러 FDM 관리 디바이스에서 공유 RA VPN 구성

자세한 내용은 [원격 액세스 가상 프라이빗 네트워크 세션](#)을 참조하십시오. 가상 사설 네트워크에 대한 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)를 참조하십시오.

### 네트워크 모니터링

CDO는 보안 정책의 영향과 해당 보안 정책에 의해 트리거된 주요 이벤트를 보는 방법을 요약한 보고서를 제공합니다. CDO는 또한 디바이스에 대한 변경 사항을 기록하고 이러한 변경 사항에 레이블을 지정하는 방법을 제공하므로 CDO에서 수행하는 작업을 지원 티켓 또는 기타 운영 요청과 연결할 수 있습니다.

### 총괄 요약 보고서

개요 보고서는 암호화된 트래픽, 차단된 위협, 탐지된 웹 카테고리 등의 운영 통계 모음을 표시합니다. 네트워크 트래픽이 FDM 관리 디바이스에서 액세스 규칙 또는 정책을 트리거할 때 보고서의 데이터가 생성됩니다. 디바이스가 보고서에 반영되는 이벤트를 생성할 수 있도록 악성코드 및 라이선스를 활성화하고 액세스 규칙에 대한 파일 로깅을 활성화하는 것이 좋습니다.

보고서에서 제공하는 내용과 이를 사용하여 네트워크 인프라를 개선하는 방법에 대한 자세한 내용은 [FDM-관리 디바이스 개요 보고서](#)를 참조하십시오. 보고서를 생성하고 관리하려면 [모니터링 및 보고](#)를 참조하십시오.

### Cisco Security Analytics and Logging

Cisco SaaS(Security Analytics and Logging)를 사용하면 모든 FDM 관리 디바이스에서 연결, 침입, 파일, 맬웨어 및 보안 인텔리전스 이벤트를 캡처하고, CDO의 한 곳에서 볼 수 있습니다.

이벤트는 Cisco Cloud에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 여기에서 이벤트를 필터링하고 검토하여 네트워크에서 어떤 보안 규칙이 트리거되고 있는지 명확하게 이해할 수 있습니다. **Logging and Troubleshooting**(기록 및 문제 해결) 패키지는 이러한 기능을 제공합니다.

방화벽 분석 및 모니터링 패키지를 통해 시스템은 FDM 관리 디바이스 이벤트에 Secure Cloud Analytics 동적 엔터티 모델링을 적용하고, 행동 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 알람을 생성할 수 있습니다. **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 패키지를 보유한 경우, 시스템은 FDM 관리 디바이스 이벤트와 네트워크 트래픽 모두에 동적 엔터티 모델링을 적용하고, 관찰 및 경고를 생성합니다. Cisco SSO(Single Sign-On, 단일 인증)를 사용하여 CDO에서 사용자에게 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다. 자세한 내용은 [Security Analytics and Logging\(SaaS\) 정보](#)를 참조하십시오.

## 변경 로그

[변경 로그, 639 페이지](#)는 CDO에서 수행되는 구성 변경 사항을 지속적으로 캡처합니다. 이 단일 보기에는 지원되는 모든 디바이스 및 서비스에 대한 변경 사항이 포함됩니다. 다음은 변경 로그의 몇 가지 기능입니다.

- 디바이스 구성에 대한 변경 사항을 나란히 비교합니다.
- 모든 변경 로그 항목에 대한 일반 영어 레이블입니다.
- 디바이스의 온보딩 및 제거를 기록합니다.
- CDO 외부에서 발생하는 정책 변경 충돌을 탐지합니다.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.
- 전체 변경 로그 또는 일부만 CSV 파일로 다운로드할 수 있습니다.

## 변경 요청 관리

[변경 요청 관리](#)를 사용하면 서드파티 티켓팅 시스템에서 연 변경 요청 및 해당 비즈니스 근거를 변경 로그의 이벤트와 연결할 수 있습니다. CDO에서 변경 요청을 생성하고, 이를 고유한 이름으로 식별하고, 변경에 대한 설명을 입력하고, 변경 요청을 변경 로그 이벤트와 연결하려면 변경 요청 관리를 사용합니다. 나중에 변경 로그에서 변경 요청 이름을 검색할 수 있습니다.





# 1 장

## Cisco Defense Orchestrator의 기본 사항

Cisco Defense Orchestrator (CDO)는 명확하고 간결한 인터페이스를 통해 정책 관리에 대한 고유한 보기를 제공합니다. 다음은 CDO를 처음 사용할 때 기본 사항을 다루는 항목입니다.

- 네트워크 요구 사항, 2 페이지
- CDO 테넌트 요청, on page 8
- 라이선스, 8 페이지
- SDC(Secure Device Connector), 11 페이지
- CDO에 로그인, 39 페이지
- **Cisco Secure Cloud Sign On** ID 제공자로 마이그레이션, 41 페이지
- Cisco Secure Cloud Sign On 대시보드에서 CDO 실행, on page 42
- 테넌트에서 슈퍼 관리자 관리, on page 43
- CDO에서 지원하는 소프트웨어 및 하드웨어, 43 페이지
- 브라우저 지원, on page 47
- **Cisco Defense Orchestrator** 플랫폼 유지 관리 일정, 47 페이지
- 테넌트 관리, 48 페이지
- 사용자 관리, 66 페이지
- 사용자 관리의 Active Directory 그룹, 67 페이지
- 새 CDO 사용자 생성, on page 71
- Cisco Defense Orchestrator의 사용자 역할, on page 79
- 사용자 역할에 대한 사용자 레코드 생성, on page 84
- 사용자 역할에 대한 사용자 레코드 편집, on page 85
- 사용자 역할에 대한 사용자 레코드 삭제, on page 86
- 서비스 페이지 정보 보기, 87 페이지
- 디바이스 및 서비스 관리, 90 페이지
- 재고 목록 페이지 정보 보기, 97 페이지
- 레이블 및 필터링, 98 페이지
- 동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기, on page 100
- 검색, on page 101
- 글로벌 검색, 101 페이지
- CDO 명령줄 인터페이스, on page 105

- 대량 명령줄 인터페이스, on page 107
- 디바이스 관리를 위한 CLI 매크로, on page 111
- 명령줄 인터페이스 설명서, on page 115
- CLI 명령 결과 내보내기, on page 115
- 개체, on page 118
- 네트워크 개체, on page 130
- 애플리케이션 필터 개체, on page 140
- 지리위치 개체, on page 143
- DNS 그룹 개체, 145 페이지
- 인증서 개체, on page 147
- IPsec 제안 구성, on page 153
- 글로벌 IKE 정책 구성, on page 156
- RA VPN 개체, 160 페이지
- 보안 영역 개체, on page 160
- 서비스 개체, on page 162
- 보안 그룹 태그 그룹, 165 페이지
- 시스템 로그 서버 개체, 169 페이지
- URL 개체, 171 페이지

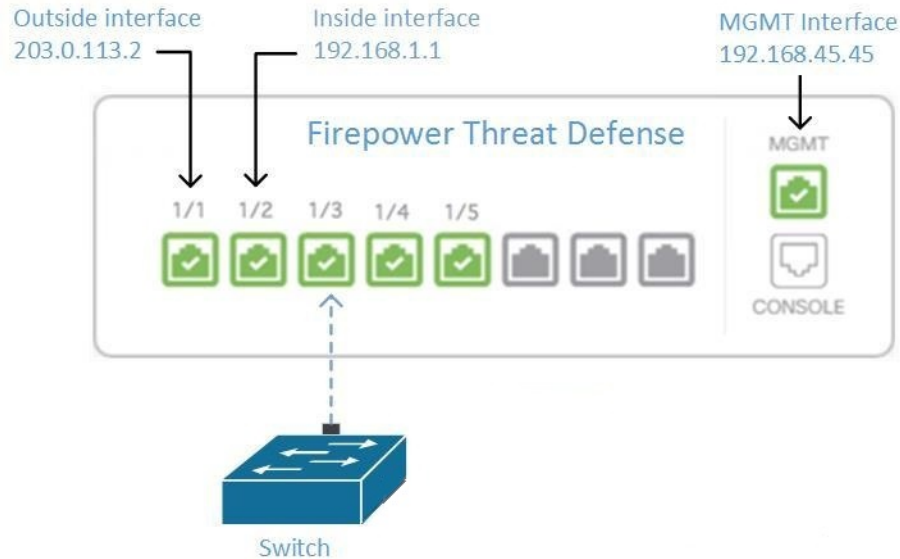
## 네트워크 요구 사항

### 내부 인터페이스에서 **FDM**-관리 디바이스 관리

전용 MGMT 인터페이스에 조직 내에서 라우팅할 수 없는 주소가 할당된 경우, 내부 인터페이스를 사용하여 FDM 관리 디바이스를 관리하는 것이 바람직할 수 있습니다. 예를 들어 데이터 센터나 연구실 내에서만 연결할 수 있습니다.



Figure 1: 인터페이스 주소



원격 액세스 VPN 요구 사항

CDO로 관리하는 FDM 관리 디바이스가 원격 액세스 VPN(RA VPN) 연결을 관리하는 경우 CDO는 내부 인터페이스를 사용하여 디바이스를 관리해야 합니다.

다음 작업:

FDM 관리 디바이스 구성 절차를 위해 내부 인터페이스에서 FDM-관리 디바이스 관리, on page 3로 계속하십시오.

## 내부 인터페이스에서 FDM-관리 디바이스 관리

이 구성 방법:

- FDM 관리 디바이스가 CDO에 온보딩되지 않았다고 가정합니다.
- 데이터 인터페이스를 내부 인터페이스로 구성합니다.
- MGMT 트래픽(HTTPS)을 수신하도록 내부 인터페이스를 구성합니다.
- 클라우드 커넥터의 주소가 디바이스의 내부 인터페이스에 도달하도록 허용합니다.

### Before you begin

다음 항목에서 이 구성의 사전 요구 사항을 검토합니다.

- 내부 인터페이스에서 FDM-관리 디바이스 관리, on page 2
- 매니지드 디바이스에 Cisco Defense Orchestrator 연결, on page 12

## Procedure

---

단계 1 Secure Firewall device manager에 로그인합니다.

단계 2 **System Settings**(시스템 설정) 메뉴에서 **Management Access**(관리 액세스)를 클릭합니다.

단계 3 **Data Interfaces**(데이터 인터페이스) 탭을 클릭하고 **Create Data Interface**(데이터 인터페이스 생성)를 클릭합니다.

- a. **Interface**(인터페이스) 필드의 인터페이스 목록에서 미리 명명된 "**inside**(내부)" 인터페이스를 선택합니다.
- b. **Protocols**(프로토콜) 필드에서 아직 HTTPS가 아닌 경우 **HTTPS**를 선택합니다.
- c. **Allowed Networks**(허용된 네트워크) 필드에서 FDM 관리 디바이스의 내부 주소에 액세스할 수 있는 조직 내부의 네트워크를 나타내는 네트워크 개체를 선택합니다. SDC 또는 클라우드 커넥터의 IP 주소는 디바이스의 내부 주소에 액세스할 수 있는 주소 중 하나여야 합니다.

**인터페이스 주소** 다이어그램에서 SDC의 IP 주소 192.168.1.10은 192.168.1.1에 도달할 수 있어야 합니다.

단계 4 변경 사항 배포. 이제 내부 인터페이스를 사용하여 디바이스를 관리할 수 있습니다.

---

## What to do next

클라우드 커넥터를 사용하는 경우 어떻게 됩니까?

위의 절차를 사용하고 다음 단계를 추가합니다.

- 내부 인터페이스(192.168.1.1)에 외부 인터페이스(203.0.113.2)를 "NAT"하는 단계를 추가합니다.
- 위 절차의 3c단계에서 "허용된 네트워크"는 클라우드 커넥터의 공용 IP 주소를 포함하는 네트워크 그룹 개체입니다.
- 클라우드 커넥터의 공용 IP 주소에서 외부 인터페이스(203.0.113.2)에 대한 액세스를 허용하는 액세스 제어 규칙을 생성하는 단계를 추가합니다.

유럽, 중동 또는 아프리카(EMEA) 고객이고, <https://defenseorchestrator.eu>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.

- 35.157.12.126
- 35.157.12.15

미국 고객이고, <https://defenseorchestrator.com>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.

- 52.34.234.2
- 52.36.70.147

**AJPC(Asia-Pacific-Japan-China)** 고객이고, <https://www.apj.cdo.cisco.com/>에서 CDO에 연결하는 경우 다음 IP 주소에서 인바운드 액세스를 허용합니다.

- 54.199.195.111
- 52.199.243.0

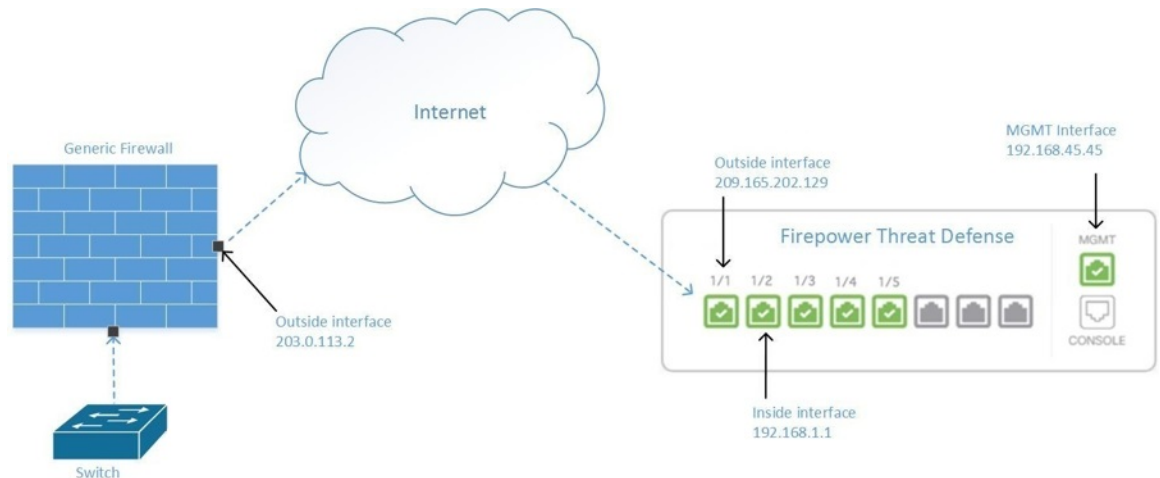
### FDM-관리 디바이스 온보딩

등록 토큰 온보딩 접근 방식은 FDM 관리 디바이스를 CDO에 온보딩하는 권장 방법입니다. Cloud Connector에서 FDM 관리 디바이스로의 관리 액세스를 허용하도록 내부 인터페이스를 구성한 후, 사용자 이름과 암호를 사용하여 FDM 관리디바이스를 온보딩합니다. 자세한 내용은 [위협 방어 디바이스 온보딩](#)을 참조하십시오. 내부 인터페이스의 IP 주소를 사용하여 연결합니다. 위의 시나리오에서 해당 주소는 192.168.1.1입니다.

## 외부 인터페이스에서 FDM-관리 디바이스 관리

지사에 할당된 하나의 공용 IP 주소가 있고 Cisco Defense Orchestrator가 다른 위치에서 클라우드 커넥터를 사용하여 관리되는 경우 외부 인터페이스에서 클라우드 사용 Firewall Management Center 디바이스를 관리하는 것이 바람직할 수 있습니다.

**Figure 2:** 외부 인터페이스에서 디바이스 관리



이 구성은 물리적 MGMT 인터페이스가 더 이상 디바이스의 관리 인터페이스가 아님을 의미하지 않습니다. 클라우드 사용 Firewall Management Center 디바이스가 있는 사무실에 있다면 MGMT 인터페이스의 주소에 연결하여 디바이스를 직접 관리할 수 있습니다.

### 원격 액세스 VPN 요구 사항

클라우드 사용 Firewall Management Center로 관리하는 디바이스가 원격 액세스 VPN(RA VPN) 연결을 관리하는 경우, 클라우드 사용 Firewall Management Center는 외부 인터페이스를 사용하여 클라우

드 사용 Firewall Management Center 디바이스를 관리해야 합니다. 대신 [내부 인터페이스에서 FDM-관리 디바이스 관리](#)를 참조하십시오.

다음 작업:

클라우드 사용 Firewall Management Center 디바이스 구성 절차를 위해 [FDM-관리 디바이스의 외부 인터페이스 관리](#), on page 6로 계속하십시오.

## FDM-관리 디바이스의 외부 인터페이스 관리

이 구성 방법:

1. FDM 관리 디바이스가 CDO에 온보딩되지 않았다고 가정합니다.
2. 데이터 인터페이스를 외부 인터페이스로 구성합니다.
3. 외부 인터페이스에서 관리 액세스를 구성합니다.
4. 클라우드 커넥터의 공용 IP 주소(방화벽을 통해 NAT된 후)가 외부 인터페이스에 도달하도록 허용합니다.

### Before you begin

다음 항목에서 이 구성의 사전 요구 사항을 검토합니다.

- [FDM-관리 디바이스의 외부 인터페이스 관리](#), on page 6
- [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#), on page 12

### Procedure

단계 1 Secure Firewall device manager에 로그인합니다.

단계 2 **System Settings**(시스템 설정) 메뉴에서 **Management Access**(관리 액세스)를 클릭합니다.

단계 3 **Data Interfaces**(데이터 인터페이스) 탭을 클릭하고 **Create Data Interface**(데이터 인터페이스 생성)를 클릭합니다.

- a. **Interface**(인터페이스) 필드의 인터페이스 목록에서 미리 명명된 "**outside**(외부)" 인터페이스를 선택합니다.
- b. **Protocols**(프로토콜) 필드에서 아직 HTTPS가 아닌 경우 **HTTPS**를 선택합니다. CDO은 HTTPS 액세스만 필요합니다.
- c. **Allowed Networks**(허용된 네트워크) 필드에서 방화벽을 통해 NAT된 후 클라우드 커넥터의 공용 IP 주소를 포함하는 호스트 네트워크 개체를 생성합니다.

[Device Management from Outside Interface\(외부 인터페이스의 장치 관리\)](#) 네트워크 다이어그램에서 클라우드 커넥터의 IP 주소인 10.10.10.55는 203.0.113.2로 NAT됩니다. 허용된 네트워크의 경우 값이 203.0.113.2인 호스트 네트워크 개체를 생성합니다.

**단계 4** Secure Firewall device manager에서 SDC 또는 클라우드 커넥터의 공용 IP 주소에서 FDM 관리 디바이스의 외부 인터페이스로의 관리 트래픽(HTTPS)을 허용하는 액세스 제어 정책을 생성합니다. 이 시나리오에서 소스 주소는 203.0.113.2이고 소스 프로토콜은 HTTPS입니다. 대상 주소는 209.165.202.129이고 프로토콜은 HTTPS입니다.

**단계 5** 변경 사항 배포. 이제 외부 인터페이스를 사용하여 디바이스를 관리할 수 있습니다.

### What to do next

클라우드 커넥터를 사용하는 경우 어떻게 됩니까?

프로세스는 다음 두 가지를 제외하고 매우 유사합니다.

- 위 절차의 3c단계에서 "허용된 네트워크"는 클라우드 커넥터의 공용 IP 주소를 포함하는 네트워크 그룹 개체입니다.
  - 유럽, 중동 또는 아프리카(EMEA) 고객이고, <https://defenseorchestrator.eu/>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.
    - 35.157.12.126
    - 35.157.12.15
  - 미국 고객이고, <https://defenseorchestrator.com/>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.
    - 52.34.234.2
    - 52.36.70.147
  - AJPC(Asia-Pacific-Japan-China) 고객이고, <https://www.apj.cdo.cisco.com/>에서 CDO에 연결하는 경우 다음 IP 주소에서 인바운드 액세스를 허용합니다.
    - 54.199.195.111
    - 52.199.243.0
- 위 절차의 4단계에서는 클라우드 커넥터의 공용 IP 주소에서 외부 인터페이스에 대한 액세스를 허용하는 액세스 제어 규칙을 생성합니다.

등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩 접근 방식은 FDM 관리 디바이스를 CDO에 온보딩하는 권장 방법입니다. 클라우드 커넥터에서 관리 액세스를 허용하도록 외부 인터페이스를 구성한 후 FDM 관리 디바이스를 온보딩합니다. 외부 인터페이스의 IP 주소를 사용하여 연결합니다. 이 시나리오에서 해당 주소는 209.165.202.129입니다.

## CDO 테넌트 요청

CDO 테넌트의 30일 무료 평가판을 요청하여 디바이스를 온보딩하고 관리할 수 있습니다. 그런 다음 Cisco 계정 팀에 연락하여 테넌트를 라이선스가 있는 테넌트로 업그레이드할 수 있습니다.

시작하기 전에

SecureX계정을 아직 생성하지 않았으면 생성하십시오. 새 [Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성](#)을 참조하십시오.

절차

1. <https://www.defenseorchestrator.com/new>로 진행합니다.
2. CDO 테넌트를 프로비저닝하려는 지역을 선택합니다.
3. **Sign Up with SecureX(SecureX로 가입)**를 클릭합니다.
4. SecureX 계정으로 로그인합니다.

성공적으로 로그인하면 등록된 이메일 ID로 테넌트 세부 정보가 포함된 이메일을 받게 됩니다. 선택한 지역에 새 CDO 테넌트가 생성됩니다. 이메일의 지침에 따라 새 CDO 테넌트에 액세스합니다.

CDO 테넌트에 처음으로 로그인하는 방법에 대한 자세한 내용은 [새 CDO 테넌트에 대한 초기 로그인](#)을 참조하십시오.

CDO 테넌트 및 다양한 테넌트 설정 관리에 대한 자세한 내용은 [새 CDO 테넌트에 대한 초기 로그인](#)을 참조하십시오.

추가 **CDO** 테넌트 요청

기존 테넌트를 추가로 생성하려면 어카운트 매니저에게 문의하십시오.

## 라이선스

Cisco Defense Orchestrator에서 디바이스를 온보딩하고 관리하려면, 관리하려는 디바이스에 따라 기본 구독 및 디바이스별 기간 기반 구독을 구매해야 합니다.

## 라이선스 정보

CDO는 테넌트 자격에 대한 기본 구독과 디바이스 관리를 위한 디바이스 라이선스가 필요합니다. 필요한 테넌트 수에 따라 하나 이상의 CDO 기본 구독을 구입하고 디바이스 모델 번호 및 수량에 따라 디바이스 라이선스를 구입할 수 있습니다. 즉, 기본 구독을 구매하면 CDO 테넌트가 제공되며 CDO를 사용하여 관리하기로 선택한 모든 디바이스에 대해 별도의 디바이스 라이선스가 필요합니다. 배포 계획을 위해 각 CDO 테넌트는 SDC(보안 디바이스 커넥터)를 통해 약 500개의 디바이스를 관리하

고 클라우드 커넥터를 사용하는 원하는 수의 디바이스를 관리할 수 있습니다. 자세한 내용은 [Secure Device Connector\(SDC\)](#)를 참조하십시오.

### 서브스크립션

Cisco Defense Orchestrator 구독은 기간 기반입니다.

- 기본- 1년, 3년 및 5년 동안의 구독을 제공하고 CDO 테넌트에 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 CDO에서 클라우드 사용 Firewall Management Center를 사용하여 Cisco Firepower 1010 디바이스를 관리하도록 선택할 수 있습니다.

CDO가 지원하는 Cisco 보안 디바이스에 대한 자세한 내용은 [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 참조하십시오.



**중요** CDO에서 고가용성 디바이스 쌍을 관리하기 위해 두 개의 별도 디바이스 라이선스가 필요하지 않습니다. ASA(Secure Firewall ASA) 또는 FTD(Secure Firewall Threat Defense) 고가용성 쌍이 있는 경우, CDO는 고가용성 디바이스 쌍을 하나의 단일 디바이스로 간주하므로 하나의 ASA 또는 FTD 디바이스 라이선스를 구입하는 것으로 충분합니다.



**참고** Cisco 스마트 라이선스 포털을 통해 CDO 라이선스를 관리할 수 없습니다.

### 소프트웨어 서브스크립션 지원

CDO 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 CDO 솔루션 지원을 활용할 수도 있습니다.

## 평가판 라이선스

### Cisco Defense Orchestrator 평가판 라이선스

SecureX 계정에서 30일 Cisco Defense Orchestrator 평가판을 요청할 수 있습니다. 자세한 내용은 [CDO 테넌트 요청](#)을 참조하십시오.

### 클라우드 사용 Firewall Management Center 평가 라이선스

클라우드 사용 Firewall Management Center에 90일 평가판 라이선스가 제공되며 그 이후에는 위협 방어 서비스가 차단됩니다.

CDO 테넌트에서 프로비저닝된 클라우드 사용 Firewall Management Center를 가져오는 방법을 알아보려면 [CDO 테넌트용 클라우드 사용 Firewall Management Center 요청](#)을 참조하십시오.

## 클라우드 제공 Firewall Management Center 및 Threat Defense 라이선스

CDO에서 클라우드 사용 Firewall Management Center를 사용하기 위해 별도의 라이선스를 구입할 필요가 없습니다. CDO 테넌트의 기본 구독에는 클라우드 사용 Firewall Management Center에 대한 비용이 포함됩니다.



참고 클라우드 사용 Firewall Management Center는 에어갭 네트워크의 디바이스에 대한 특정 라이선스 예약(SLR)을 지원하지 않습니다.

클라우드 제공 Firewall Management Center용 Threat Defense 라이선스

클라우드 사용 Firewall Management Center에서 관리하는 각 Secure Firewall Threat Defense 디바이스에 대해 개별 라이선스가 필요합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 사용 Firewall Management Center로 Firewall Threat Defense 관리에서 [라이선싱](#)을 참조하십시오.

CDO가 클라우드 사용 Firewall Management Center으로 마이그레이션된 디바이스에 대한 라이선스를 처리하는 방법을 알아보려면 [Management Center에서 Cloud로 Threat Defense 마이그레이션](#)을 참조하십시오.

## 추가 지원 디바이스 및 라이선스

클라우드 사용 Firewall Management Center, CDO를 통해 Secure Firewall Threat Defense 디바이스를 지원하는 것 외에도 다음 디바이스도 관리합니다.

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

CDO 기본 인타이틀먼트 라이선스와 관리하려는 디바이스에 특정한 라이선스가 필요합니다.



## SDC(Secure Device Connector)

디바이스 자격 증명을 사용하여 CDO에 디바이스를 온보딩할 때 CDO는 디바이스와 CDO 간의 프록시 통신을 위해 네트워크에서 SDC(Secure Device Connector)를 다운로드하고 구축하는 것이 모범 사례라고 간주합니다. 그러나 원하는 경우 CDO에서 외부 인터페이스를 통해 직접 통신을 수신하도록 디바이스를 활성화할 수 있습니다. ASA(Adaptive Security Appliance), FDM 관리 디바이스, FMC(Firepower Management Center), Secure Firewall Cloud Native 디바이스, SSH 및 IOS 디바이스는 모두 SDC를 사용하여 CDO에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.

SDC는 AES-128-GCM over HTTPS(TLS 1.2)를 사용하여 서명 및 암호화된 보안 통신 메시지를 사용하여 CDO와 통신합니다. 온보딩된 디바이스 및 서비스에 대한 모든 자격 증명은 브라우저에서 SDC로 직접 암호화되며, AES-128-GCM을 사용하여 저장 상태에서도 암호화됩니다. SDC만 디바이스 자격 증명에 액세스할 수 있습니다. 다른 CDO 서비스는 자격 증명에 액세스할 수 없습니다. SDC와 CDO 간의 통신을 허용하는 방법에 대한 자세한 내용은 [매니지드 디바이스에 Cisco Defense Orchestrator 연결, 12 페이지](#)의 내용을 참조하십시오.

SDC는 하이퍼바이저의 가상 머신으로 어플라이언스에 설치하거나 AWS 또는 Azure와 같은 클라우드 환경에 설치할 수 있습니다. CDO에서 제공하는 통합된 가상 머신 및 SDC 이미지를 사용하여 SDC를 설치하거나, 고유한 가상 머신을 생성하고 여기에 SDC를 설치할 수 있습니다. SDC 가상 어플라이언스는 CentOS 운영 체제를 포함하며 Docker 컨테이너 내에서 실행됩니다.

각 CDO 테넌트에는 무제한의 SDC가 있을 수 있습니다. 이러한 SDC는 테넌트 간에 공유되지 않으며 단일 테넌트 전용입니다. 단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다.

테넌트에 대해 둘 이상의 SDC를 구축하면 다음과 같은 이점도 제공됩니다.

- 성능 저하 없이 CDO 테넌트로 더 많은 디바이스를 관리할 수 있습니다.
- 네트워크 내의 격리된 네트워크 세그먼트에 SDC를 구축하고 동일한 CDO 테넌트로 해당 세그먼트의 디바이스를 계속 관리할 수 있습니다. 여러 SDC가 없으면 서로 다른 CDO 테넌트를 사용하여 격리된 네트워크 세그먼트에서 디바이스를 관리해야 합니다.

두 번째 또는 후속 SDC를 구축하는 절차는 첫 번째 SDC를 구축할 때와 동일합니다. 테넌트의 초기 SDC는 테넌트의 이름과 숫자 1을 통합하며 CDO의 페이지의 Secure Connectors(보안 커넥터) 탭에 표시됩니다. 각 추가 SDC는 순서대로 번호가 매겨집니다. [CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축, 14 페이지](#) 및 [자체 VM에 보안 디바이스 커넥터 구축, 18 페이지](#) 참조

관련 정보:

- [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#)
- [보안 디바이스 커넥터 문제 해결, 774 페이지](#)
- [보안 디바이스 커넥터 업데이트, 29 페이지](#)

- [보안 디바이스 커넥터 제거, 26 페이지](#)

## 매니지드 디바이스에 Cisco Defense Orchestrator 연결

CDO는 클라우드 커넥터 또는 SDC(Secure Device Connector)를 통해 관리하는 디바이스에 연결합니다.

인터넷에서 디바이스에 직접 액세스할 수 있는 경우 클라우드 커넥터를 사용하여 디바이스에 연결해야 합니다. 디바이스를 구성할 수 있는 경우 클라우드 지역의 CDO IP 주소에서 포트 443에 대한 인바운드 액세스를 허용합니다.

인터넷에서 디바이스에 액세스할 수 없는 경우 CDO가 디바이스와 통신할 수 있도록 네트워크에 온프레미스 SDC를 구축할 수 있습니다. 디바이스를 구성할 수 있는 경우 포트 443(또는 디바이스 관리를 위해 설정한 포트)에서 전체 인바운드 액세스를 허용해야 합니다.

FDM 관리 디바이스는 디바이스 자격 증명, 등록 키 또는 일련 번호를 사용하여 CDO에 온보딩할 수 있습니다(인터넷에서 직접 액세스할 수 있는지 여부). FDM 관리 디바이스가 인터넷에 직접 액세스할 수 없는 네트워크에 상주하는 경우, 디바이스의 일부로 제공되는 보안 서비스 익스체인지 커넥터는 보안 서비스 익스체인지 클라우드에 연결하여 FDM 관리 디바이스를 온보딩할 수 있습니다. 다양한 온보딩 방법에 대한 자세한 내용은 [위협 방어 디바이스 온보딩, on page 175](#)의 내용을 참조하십시오.

다음은 온보딩하려면 네트워크에 온프레미스 SDC가 필요합니다.

- 클라우드에서 액세스할 수 없는 ASA 디바이스.
- 클라우드에서 액세스할 수 없는 FDM 관리 디바이스 및 "자격 증명 온보딩" 방법이 사용됩니다.
- Cisco IOS 디바이스.
- SSH 액세스가 가능한 디바이스.

다른 모든 디바이스 및 서비스에는 온프레미스 SDC가 필요하지 않습니다. CDO는 "Cloud Connector"를 사용하여 연결합니다. 인바운드 액세스를 허용해야 하는 IP 주소를 확인하려면 다음 섹션을 참조하십시오.

클라우드 커넥터를 통해 디바이스를 **CDO**에 연결

클라우드 커넥터를 통해 CDO를 디바이스에 직접 연결할 때는 EMEA, 미국 또는 APJC 지역의 다양한 IP 주소에 대해 포트 443(또는 디바이스 관리를 위해 구성한 모든 포트)에서 인바운드 액세스를 허용해야 합니다.

유럽, 중동 또는 아프리카(EMEA) 지역의 고객이 <https://defenseorchestrator.eu/>에서 CDO에 연결하는 경우 다음 IP 주소에서의 인바운드 액세스를 허용합니다.

- 35.157.12.126
- 35.157.12.15

미국 지역의 고객이 <https://defenseorchestrator.com/>에서 CDO에 연결하는 경우 다음 IP 주소에서의 인바운드 액세스를 허용합니다.

- 52.34.234.2
- 52.36.70.147

**APJC**(아시아-태평양-일본-중국) 지역의 고객이 <https://www.apj.cdo.cisco.com/>에서 CDO에 연결하는 경우 다음 IP 주소에서의 인바운드 액세스를 허용합니다.

- 54.199.195.111
- 52.199.243.0

### SDC를 사용하여 CDO에 디바이스 연결

SDC를 통해 CDO를 디바이스에 연결할 때 CDO에서 관리하려는 디바이스는 포트 443(또는 디바이스 관리를 위해 구성된 모든 포트)에서 전체 인바운드 액세스를 허용해야 합니다. 이는 관리 액세스 제어 규칙을 사용하여 구성됩니다.

또한 SDC가 구축된 가상 머신이 매니지드 디바이스의 관리 인터페이스에 네트워크로 연결되어 있는지 확인해야 합니다.

### SDC에 ASA 또는 Secure Firewall Cloud Native를 연결하기 위한 특별 고려 사항

특히 ASA 또는 Secure Firewall Cloud Native의 경우 SDC는 ASDM에서 사용하는 것과 동일한 보안 통신 채널을 사용합니다.

관리 중인 ASA 또는 Secure Firewall Cloud Native도 AnyConnect VPN 클라이언트 연결을 허용하도록 구성된 경우 ASDM HTTP 서버 포트를 1024 이상의 값으로 변경해야 합니다. 이 포트 번호는 디바이스를 ASA 또는 Secure Firewall Cloud Native 디바이스에 온보딩할 때 사용되는 포트 번호와 동일합니다.

### ASA 또는 Secure Firewall Cloud Native 명령 예

다음 예에서는 ASA 또는 Secure Firewall Cloud Native 외부 인터페이스의 이름이 'outside'이고 AnyConnect 클라이언트가 ASA 또는 Secure Firewall Cloud Native에 구성되어 있으므로, ASDM HTTP 서버가 포트 8443에서 수신 대기 중이라고 가정합니다.

외부 인터페이스를 활성화하려면 다음 명령을 입력합니다.

EMEA:

**http 35.157.12.126 255.255.255.255 outside**

**http 35.157.12.15 255.255.255.255 outside**

미국:

**http 52.34.234.2 255.255.255.255 outside**

**http 52.36.70.147 255.255.255.255 outside**

아시아 태평양 일본 중국 지역:

**http 54.199.195.111 255.255.255.255 outside**

**http 52.199.243.0 255.255.255.255 outside**

AnyConnect VPN 클라이언트를 사용 중인 경우 ASDM HTTP 서버 포트를 활성화하려면 다음 명령을 입력합니다.

```
http server enable 8443
```

## CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축

디바이스 자격 증명을 사용하여 CDO를 디바이스에 연결하는 경우 네트워크에 SDC를 다운로드하고 배포하여 CDO와 디바이스 간의 통신을 관리하는 것이 가장 좋습니다. 일반적으로 이러한 디바이스는 경계를 기반으로 하지 않으며 공용 IP 주소가 없거나 외부 인터페이스에 대한 개방형 포트가 있습니다. ASA(Adaptive Security Appliance), FDM 관리 디바이스, FMC(Firepower Management Center), Secure Firewall Cloud Native 디바이스, SSH 및 IOS 디바이스는 모두 SDC를 사용하여 CDO에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.

단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다. 자세한 내용은 [단일 CDO 테넌트에서 여러 SDC 사용, 29 페이지](#)를 참조하십시오.

이 절차에서는 CDO의 VM 이미지를 사용하여 네트워크에 SDC를 설치하는 방법을 설명합니다. 이는 SDC를 생성하는 가장 쉽고 신뢰할 수 있는 방법입니다. 생성한 VM을 사용하여 SDC를 생성해야 하는 경우 [자체 VM에 보안 디바이스 커넥터 구축, 18 페이지](#)를 수행합니다.

시작하기 전에

SDC를 구축하기 전에 다음 사전 요건을 검토합니다.

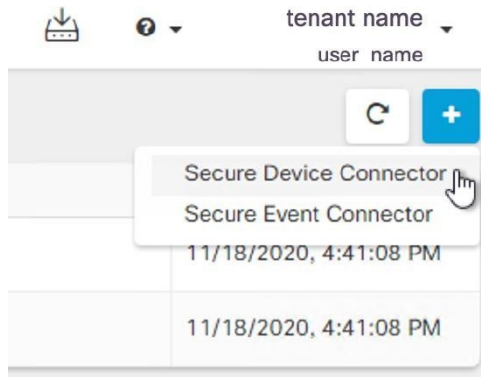
- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 SDC(보안 디바이스 커넥터)와 CDO 간의 트래픽 검사를 비활성화합니다.
- SDC는 TCP 포트 443 또는 디바이스 관리를 위해 구성된 포트에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다. CDO에서 관리하는 디바이스는 이 포트의 인바운드 트래픽도 허용해야 합니다.
- 매니지드 디바이스에 [Cisco Defense Orchestrator 연결](#)를 검토하여 적절한 네트워크 액세스를 확인합니다.
- CDO는 vSphere 웹 클라이언트 또는 ESXi 웹 클라이언트를 사용하여 SDC VM OVF 이미지를 설치를 지원합니다.
- CDO는 vSphere 데스크톱 클라이언트를 사용한 SDC VM OVF 이미지 설치를 지원하지 않습니다.
- ESXi 5.1 하이퍼바이저.
- Cent OS 7 게스트 운영체제.

- SDC가 하나만 있는 VMware ESXi 호스트의 시스템 요구 사항:
  - VMware ESXi 호스트에는 vCPU 2개가 필요합니다.
  - VMware ESXi 호스트에는 최소 2GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- 테넌트용 SDC 및 단일 SEC(Secure Event Connector)가 있는 VM의 시스템 요구 사항. (SEC는 [Security Analytics and Logging\(SaaS\) 정보](#)에서 사용되는 구성 요소입니다.)  
 VMware ESXi 호스트에 추가하는 각 SEC에는 4개의 CPU와 8GB의 추가 메모리가 필요합니다. 따라서 하나의 SDC와 하나의 SEC가 있는 VMware ESXi 호스트에 대한 요구 사항은 다음과 같습니다.
  - VMware ESXi 호스트에는 vCPU 6개가 필요합니다.
  - VMware ESXi 호스트에는 최소 10GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- docker IP는 SDC의 IP 범위 및 디바이스 IP 범위와 다른 서브넷에 있어야 합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - SDC에 사용할 고정 IP 주소
  - 설치 프로세스 중 생성하는 `root` 및 `cdo` 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - SDC 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- SDC 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.

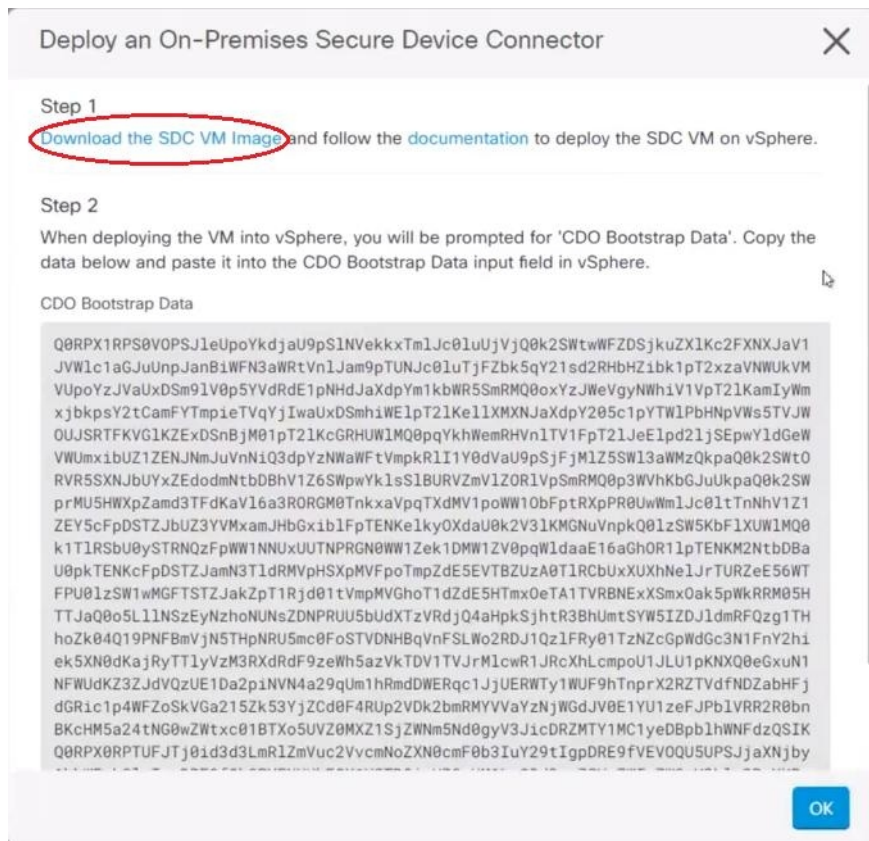
## 프로시저

- 
- 단계 1 SDC를 생성할 CDO 테넌트에 로그인합니다.
  - 단계 2 CDO 메뉴에서 **Tools & Services**(툴 및 서비스) > **Secure Connectors**(보안 커넥터)를 선택합니다.
  - 단계 3 Secure Connectors(보안 커넥터) 페이지에서 파란색 더하기 버튼을 클릭하고 **Secure Device Connector**(보안 디바이스 커넥터)를 클릭합니다.

CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축



단계 4 1단계에서 **Download the SDC VM image(SDC VM 이미지 다운로드)**를 클릭합니다. 별도의 탭에서 열립니다.



단계 5 .zip 파일의 모든 파일을 추출합니다. 다음과 같이 표시됩니다.

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

단계 6 vSphere 웹 클라이언트를 사용하여 VMware 서버에 관리자로 로그인합니다.

참고 ESXi 웹 클라이언트를 사용하지 마십시오.

단계 7 지시에 따라 OVF 템플릿에서 보안 디바이스 커넥터 가상 머신을 구축합니다.

단계 8 설정이 완료되면 SDC VM의 전원을 켭니다.

단계 9 새 SDC VM의 콘솔을 엽니다.

단계 10 사용자 이름 **cdo**로 로그인합니다. 기본 암호는 **adm123**입니다.

단계 11 프롬프트에 `sudo sdc-onboard setup`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

단계 12 비밀번호를 묻으면 `adm123`을 입력합니다.

단계 13 지시에 따라 `root` 사용자의 새 비밀번호를 생성합니다. 루트 사용자의 비밀번호를 입력합니다.

단계 14 지시에 따라 **cdo** 사용자의 새 암호를 생성합니다. **cdo** 사용자의 비밀번호를 입력합니다.

단계 15 **Please choose the CDO domain you connect to**(연결할 CDO 도메인을 선택하십시오) 메시지가 표시되면 Cisco Defense Orchestrator 도메인 정보를 입력합니다.

단계 16 메시지가 표시되면 SDC VM의 다음 도메인 정보를 입력합니다.

- a) IP 주소/CIDR
- b) 게이트웨이
- c) DNS 서버
- d) NTP 서버 또는 FQDN
- e) Docker 브리지

또는 docker 브리지가 적용되지 않는 경우 Enter 키를 누릅니다.

단계 17 **Are these values valid**(이 값이 올바릅니까?) (y/n) 메시지가 나타나면 **y**를 사용하여 입력을 확인합니다.

단계 18 입력을 확인합니다.

단계 19 **"Would you like to setup the SDC now?"**(지금 SDC를 설정하시겠습니까?) (y/n) 메시지가 나타나면 **n**을 입력합니다.

단계 20 VM 콘솔에서 자동으로 로그아웃됩니다.

단계 21 SDC에 대한 SSH 연결을 생성합니다. **cdo**로 로그인하고 비밀번호를 입력합니다.

단계 22 프롬프트에 `sudo sdc-onboard bootstrap`을 입력합니다.

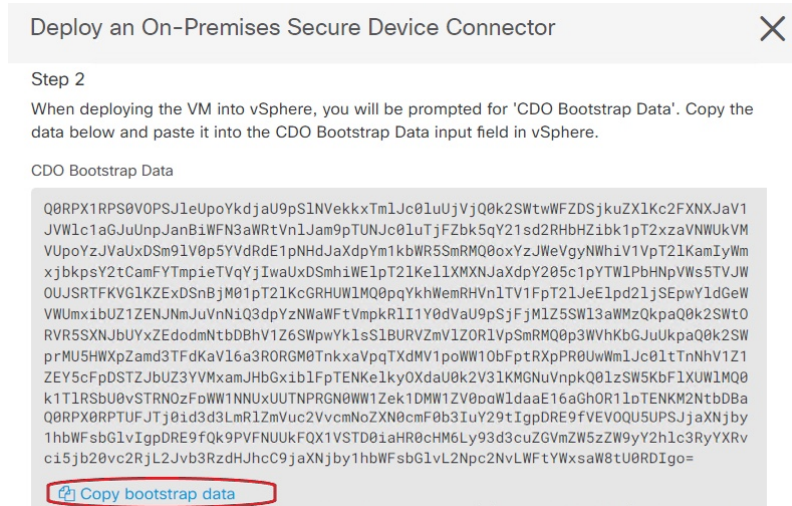
```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

단계 23 **[sudo]** 비밀번호를 묻는 메시지가 표시되면 단계 14에서 생성한 **cdo** 비밀번호를 입력합니다.

단계 24 **Please copy the bootstrap data form the Secure Connector Page of CDO**(CDO의 보안 커넥터 페이지에서 부트스트랩 데이터를 복사하십시오.) 메시지가 표시되면 다음 절차를 수행합니다.

1. CDO에 로그인합니다.
2. CDO 메뉴에서 **Admin**(관리) > **Secure Connector**(보안 커넥터)를 선택합니다.

3. Actions(작업) 창에서 **Deploy an On-Premises Secure Device Connector**(온프레미스 보안 디바이스 커넥터 구축)를 클릭합니다.
4. 대화 상자의 2단계에서 **Copy the bootstrap data**(부트스트랩 데이터 복사)를 클릭하고 SSH 창에 붙여넣습니다.



- 단계 25 **Do you want to update these setting**(이 설정을 업데이트하시겠습니까?) (y/n) 메시지가 나타나면 n을 입력합니다.
- 단계 26 **Secure Device Connector**(보안 디바이스 커넥터) 페이지로 돌아갑니다. 새 SDC의 상태가 **Active**(활성)로 변경될 때까지 화면을 새로 고칩니다.

#### 관련 정보:

- [보안 디바이스 커넥터 문제 해결, 774 페이지](#)
- [SDC와의 디바이스 연결 문제 해결, 775 페이지](#)

## 자체 VM에 보안 디바이스 커넥터 구축

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

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.



단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다. 자세한 내용은 [단일 CDO 테넌트에서 여러 SDC 사용, 29 페이지](#)를 참조하십시오.

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



참고 SDC를 설치하는 가장 쉽고 신뢰할 수 있는 방법은 CDO의 SDC OVA 이미지를 다운로드하여 설치하는 것입니다. 해당 지침은 [CDO의 VM 이미지를 사용하여 보안 디바이스 컨넥터 구축, 14 페이지](#)의 내용을 참조하십시오.

시작하기 전에

- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시를 지원하지 않습니다.
- SDC는 TCP 포트 443에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.
- 네트워킹 지침은 [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#)을 검토하십시오.
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트



참고 vSphere 데스크톱 클라이언트를 사용한 설치의 지원되지 않습니다.

- ESXi 5.1 하이퍼바이저.
- Cent OS 7 게스트 운영체제.
- SDC만 있는 VM의 시스템 요구 사항:
  - VMware ESXi 호스트에는 CPU 2개가 필요합니다.
  - VMware ESXi 호스트에는 최소 2GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다. 이 값은 필요에 따라 필요한 디스크 공간을 확장할 수 있도록 파티션과 함께 LVM(논리적 볼륨 관리)을 사용한다고 가정합니다.

- 테넌트용 SDC 및 단일 SEC(Secure Event Connector)가 있는 VM의 시스템 요구 사항. (SEC는 [Security Analytics and Logging\(SaaS\) 정보](#)에서 사용되는 구성 요소입니다.)

VMware ESXi 호스트에 추가하는 각 SEC에는 4개의 CPU와 8GB의 추가 메모리가 필요합니다.

따라서 하나의 SDC와 하나의 SEC가 있는 VMware ESXi 호스트에 대한 요구 사항은 다음과 같습니다.

- VMware ESXi 호스트에는 vCPU 6개가 필요합니다.
- VMware ESXi 호스트에는 최소 10GB의 메모리가 필요합니다.

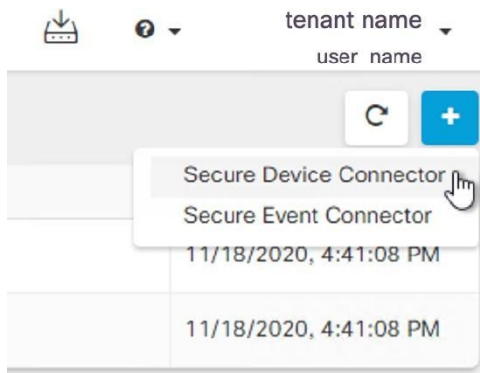
- VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- VM의 CPU와 메모리를 업데이트한 후 VM의 전원을 켜고 Secure Connector(보안 커넥터) 페이지에 SDC가 "Active(활성)" 상태로 표시되는지 확인합니다.
- 이 절차를 수행하는 사용자는 Linux 환경에서 작업하고 파일 편집을 위해 vi 시각적 편집기를 사용하는 데 익숙해야 합니다.
- CentOS 가상 머신에 온프레미스 SDC를 설치하는 경우 정기적으로 Yum 보안 패치를 설치하는 것이 좋습니다. Yum 구성에 따라 Yum 업데이트를 가져오려면 포트 80 및 443에서 아웃바운드 액세스를 열어야 할 수 있습니다. 또한 업데이트를 예약하려면 yum-cron 또는 crontab을 구성해야 합니다. 보안 운영 팀과 함께 Yum 업데이트를 받기 위해 변경해야 하는 보안 정책이 있는지 확인합니다.



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

## 프로시저

- 단계 1 SDC를 생성할 CDO 테넌트에 로그인합니다.
- 단계 2 CDO 메뉴에서 **Tools & Services(툴 및 서비스) > Secure Connectors(보안 커넥터)**를 선택합니다.
- 단계 3 Secure Connectors(보안 커넥터) 페이지에서 파란색 더하기 버튼을 클릭하고 **Secure Device Connector(보안 디바이스 커넥터)**를 클릭합니다.



- 단계 4 창의 2단계에서 부트스트랩 데이터를 메모장에 복사합니다.
- 단계 5 최소 SDC에 할당된 다음 RAM 및 디스크 공간을 사용하여 **CentOS 7** 가상 머신을 설치합니다.
  - 8GB RAM
  - 10GB 디스크 공간

- 단계 6 설치가 완료되면 SDC의 IP 주소, 서브넷 마스크 및 게이트웨이를 지정하는 등의 기본 네트워킹을 구성합니다.
- 단계 7 DNS(Domain Name Server) 서버를 구성합니다.
- 단계 8 NTP(Network Time Protocol) 서버를 구성합니다.
- 단계 9 SDC의 CLI와의 손쉬운 상호 작용을 위해 CentOS에 SSH 서버를 설치합니다.
- 단계 10 Yum 업데이트를 실행한 후 **open-vm-tools**, **nettools** 및 **bind-utils** 패키지를 설치합니다.

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

- 단계 11 AWS CLI 패키지를 설치합니다. <https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html>의 내용을 참조하십시오.

참고 **--user** 플래그를 사용하지 마십시오.

- 단계 12 Docker CE 패키지를 설치합니다. <https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce>의 내용을 참조하십시오.

참고 "저장소를 사용하여 설치" 방법을 사용합니다.

- 단계 13 Docker 서비스를 시작하고 부팅 시 시작되도록 활성화합니다.

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

- 단계 14 두 사용자("cdo" 및 "sdc")를 생성합니다. cdo 사용자는 관리 기능을 실행하기 위해 로그인하는 사용자이며(루트 사용자를 직접 사용할 필요가 없음), sdc 사용자는 SDC 도커 컨테이너를 실행하는 사용자입니다.

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

- 단계 15 cdo 사용자의 비밀번호를 생성합니다.

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

- 단계 16 cdo 사용자를 "Wheel" 그룹에 추가하여 관리(sudo) 권한을 부여합니다.

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

- 단계 17 Docker가 설치되면 사용자 그룹이 생성됩니다. CentOS/Docker 버전에 따라 "docker" 또는 "dockerroot"라고 부를 수 있습니다. /etc/group 파일을 확인하여 어떤 그룹이 생성되었는지 확인한 다음 sdc 사용자를 이 그룹에 추가합니다.

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

단계 18 /etc/docker/daemon.json 파일이 없는 경우 파일을 생성하고 아래 내용을 입력합니다. 생성되면 docker 데몬을 다시 시작합니다.

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

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

단계 19 현재 vSphere 콘솔 세션을 사용 중인 경우 SSH로 전환하고 "cdo" 사용자로 로그인합니다. 로그인한 후에는 "sdc" 사용자로 변경합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다.

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

단계 20 디렉토리를 /usr/local/cdo로 변경합니다.

단계 21 bootstrapdata라는 새 파일을 생성하고 온프레미스 보안 디바이스 컨넥터 구축 마법사의 2단계에서 가져온 부트스트랩 데이터를 이 파일에 붙여넣습니다. 파일을 Save(저장)합니다. vi 또는 nano를 사용하여 파일을 생성할 수 있습니다.

단계 22 부트스트랩 데이터는 base64로 인코딩됩니다. 이를 디코딩하고 extractedbootstrapdata라는 파일로 내보냅니다.

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

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

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

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

단계 23 다음 명령을 실행하여 디코딩된 부트스트랩 데이터의 섹션을 환경 변수로 내보냅니다.

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

단계 24 CDO에서 부트스트랩 번들을 다운로드합니다.

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

단계 25 SDC tarball의 압축을 풀고 bootstrap.sh 파일을 실행하여 SDC 패키지를 설치합니다.

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
 toolkit.sh
 common.sh
[2018-07-23 13:54:04] startup new container
Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458:
Pulling from
ciscodefenseorchestrator/sdc_prod
08d48e6f1cff: Pull complete
ebbd10b629b1: Pull complete
d14d580ef2ed: Pull complete
45421d451ab8: Pull complete
<snipped - downloads>
no crontab for sdc
```

이제 SDC가 CDO에서 "Active(활성)"로 표시됩니다.

다음에 수행할 작업

- [디바이스 및 서비스 온보딩](#)로 이동하여 CDO로 관리하려는 디바이스를 온보딩합니다.
- 보안 이벤트 커넥터를 설치하는 경우 [SDC 가상 머신에 SEC\(Secure Event Connector\) 설치](#), 671 페이지로 돌아갑니다.
- 테넌트에 두 번째 이상의 보안 이벤트 커넥터를 설치하는 경우, [CDO 이미지를 사용하여 SEC 설치](#)로 돌아갑니다.

## Terraform 모듈을 사용하여 AWS VPC에 보안 디바이스 커넥터 구축

시작하기 전에

AWS VPC에서 SDC를 구축하기 전에 다음 사전 요건을 검토하십시오.

- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 SDC(보안 디바이스 커넥터)와 CDO 간의 트래픽 검사를 비활성화합니다.
- [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#)를 검토하여 적절한 네트워크 액세스를 확인합니다.

- 이 경우 AWS 계정, 하나 이상의 서브넷이 있는 AWS VPC 및 AWS Route53 호스팅 영역이 필요합니다.
- CDO 부트스트랩 데이터, AWS VPC ID 및 해당 서브넷 ID가 있는지 확인합니다.
- SDC를 구축하는 프라이빗 서브넷에 NAT 게이트웨이가 연결되어 있는지 확인합니다.
- 방화벽 관리 HTTP 인터페이스가 실행 중인 포트에서 NAT 게이트웨이에 연결된 탄력적 IP로 이동하는 트래픽을 엽니다.

## 프로시저

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

```
module "example-sdc" {
  source =
  "git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"
  env = "example-env-ci"
  instance_name = "example-instance-name"
  instance_size = "r5a.xlarge"
  cdo_bootstrap_data = "<replace-with-cdo-bootstrap-data>"
  vpc_id = <replace-with-vpc-id>
  subnet_id = <replace-with-private-subnet-id>
}
```

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

**단계 2** Terraform 코드에서 `instance_id`를 출력으로 등록합니다.

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

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

다음에 수행할 작업

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

## 보안 디바이스 커넥터의 IP 주소 변경

시작하기 전에

- 이 작업을 수행하려면 관리자여야 합니다.

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



참고 SDC의 IP 주소를 변경한 후 디바이스를 CDO에 다시 등록할 필요가 없습니다.

### 프로시저

- 단계 1** SDC에 대한 SSH 연결을 생성하거나 가상 머신의 콘솔을 열고 CDO 사용자로 로그인합니다.
- 단계 2** IP 주소를 변경하기 전에 SDC VM의 네트워크 인터페이스 구성 정보를 보려면 `ifconfig` 명령을 사용합니다.
- ```
[cdo@localhost ~]$ ifconfig
```
- 단계 3** 인터페이스의 IP 주소를 변경하려면 `sudo sdc-onboard setup` 명령을 입력합니다.
- ```
[cdo@localhost ~]$ sudo sdc-onboard setup
```
- 단계 4** 프롬프트에 비밀번호를 입력합니다.
- ```
[sudo] password for cdo:
```
- 단계 5** 루트 및 CDO 비밀번호를 재설정하라는 프롬프트에 `n`을 입력합니다.
- ```
Would you like to reset the root and cdo passwords? (y/n):
```
- 단계 6** 네트워크 재구성 프롬프트에 `y`를 입력합니다.
- ```
Would you like to re-configure the network? (y/n):
```
- 단계 7** 메시지가 표시되면 SDC에 할당하려는 새 IP 주소와 SDC VM의 다른 도메인 정보를 입력합니다.
- IP Address(IP 주소)
  - 게이트웨이
  - DNS 서버
  - NTP 서버 또는 FQDN
- 또는 NTP 서버 또는 FQDN이 적용되지 않는 경우 Enter 키를 누릅니다.
- Docker 브리지
- 또는 docker 브리지가 적용되지 않는 경우 Enter 키를 누릅니다.
- 단계 8** 값의 정확성을 묻는 메시지가 표시되면 `y`로 항목을 확인합니다.
- ```
Are these values correct? (y/n):
```
- 참고 이 명령을 실행하면 이전 IP 주소에 대한 SSH 연결이 끊어지므로, `y`를 입력하기 전에 값이 정확한지 확인합니다.
- 단계 9** SDC에 할당한 새 IP 주소를 사용하여 SSH 연결을 만들고 로그인합니다.
- 단계 10** 연결 상태 테스트 명령을 실행하여 SDC가 실행 중인지 확인할 수 있습니다.

```
[cdo@localhost ~]$ sudo sdc-onboard status
```

모든 확인 항목은 녹색으로 [ OK(확인) ]이라고 표시되어야 합니다.

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

**단계 11** CDO 사용자 인터페이스를 통해 SDC의 연결을 확인할 수도 있습니다. 이렇게 하려면 CDO 애플리케이션을 열고 **Tools & Services(도구 및 서비스) > Secure Connectors** 페이지로 이동합니다.

**단계 12** 페이지를 한 번 새로 고치고 IP 주소를 변경한 보안 커넥터를 선택합니다.

**단계 13** **Actions(작업)** 창에서 **Request Heartbeat(하트비트 요청)**를 클릭합니다.

하트비트 요청 성공 메시지가 표시되고, 마지막 하트비트에 현재 날짜와 시간이 표시되어야 합니다.

중요 변경한 IP 주소는 GMT 오전 3시 이후에만 SDC의 세부 정보 창에 반영됩니다.

VM에 SDC를 배포하는 방법에 대한 자세한 내용은 [자체 VM에 보안 디바이스 커넥터 구축, 18 페이지](#)를 참조하세요.

## 보안 디바이스 커넥터 제거



### Warning

이 절차에서는 SDC(보안 디바이스 커넥터)를 삭제합니다. 이는 되돌릴 수 없습니다. 이 작업을 수행한 후에는 새 SDC를 설치하고 디바이스를 다시 연결할 때까지 해당 SDC에 연결된 디바이스를 관리할 수 없습니다. 디바이스를 다시 연결하려면 다시 연결해야 하는 각 디바이스에 대한 관리자 자격 증명을 다시 입력해야 할 수 있습니다.

테넌트에서 SDC를 제거하려면 다음 절차를 수행합니다.

### Procedure

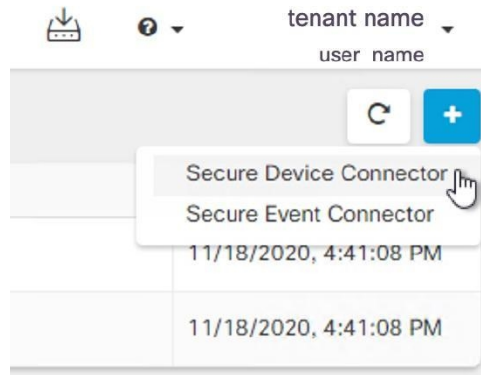
**단계 1** 삭제할 SDC에 연결된 모든 디바이스를 제거합니다.

- a. SDC에서 사용하는 모든 디바이스를 식별하려면 [동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기](#)를 참조하십시오.
- b. **Inventory(재고 목록)** 페이지에서 식별한 모든 디바이스를 선택합니다.
- c. **Device Actions(디바이스 작업)** 창에서 **Remove(제거)**를 클릭하고 **OK(확인)**를 클릭하여 작업을 확인합니다.

**단계 2** CDO 메뉴에서 **Tools & Services(도구 및 서비스) > Secure Connectors(보안 커넥터)**를 선택합니다.

**단계 3** **Secure Connectors(보안 커넥터)** 페이지에서 **파란색 더하기 버튼**을 클릭하고 **Secure Device Connector(보안 디바이스 커넥터)**를 선택합니다.





단계 4 Secure Connector(보안 커넥터) 테이블에서 제거할 SDC를 선택합니다. 이제 디바이스 수가 0이어야 합니다.

단계 5 작업 창에서 **Remove**(제거)를 클릭합니다. 다음 경고가 표시됩니다.

**Warning** <sdc\_name>을 삭제하려고 합니다. SDC 삭제는 되돌릴 수 없습니다. SDC를 삭제하면 디바이스를 온보딩하거나 다시 온보딩하기 전에 새 SDC를 생성하고 온보딩해야 합니다.

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

- 질문이나 우려 사항이 있는 경우 **Cancel**(취소)을 클릭하고 CDO 지원에 문의하십시오.
- 계속하려면 <sdc\_name>을 입력란에 입력하고 **OK**(확인)를 클릭합니다.

단계 6 확인 대화 상자에서 계속 진행하려면 경고 메시지에 나와 있는 SDC의 이름을 입력합니다.

단계 7 **OK**(확인)를 클릭하여 SDC 제거를 확인합니다.

## SDC 간에 ASA 이동

CDO는 단일 CDO 테넌트에서 여러 SDC 사용 다음 절차를 사용하여 한 SDC에서 다른 SDC로 관리형 ASA를 이동할 수 있습니다.

프로시저

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭한 다음 **ASA** 탭을 클릭합니다.

단계 3 다른 SDC로 이동하려는 ASA를 선택합니다.

단계 4 **Device Actions**(디바이스 작업) 창에서 **Update Credentials**(자격 증명 업데이트)를 클릭합니다.

단계 5 보안 디바이스 커넥터 버튼을 클릭하고 디바이스를 이동하려는 SDC를 선택합니다.

단계 6 CDO가 디바이스에 로그인하는 데 사용하는 관리자 사용자 이름과 암호를 입력하고 **Update**(업데이트)를 클릭합니다. 변경되지 않은 경우 관리자 사용자 이름과 암호는 ASA 온보딩에 사용한 것과 동일한 자격 증명입니다. 이러한 변경 사항을 디바이스에 배포할 필요는 없습니다.

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

## Meraki MX 연결 자격 증명 업데이트

Meraki 대시보드에서 새 API 키를 생성하는 경우 CDO에서 연결 자격 증명을 업데이트해야 합니다. 새 키를 생성하려면 **Meraki API 키 생성 및 검색**에서 자세한 내용을 확인하십시오. CDO에서는 디바이스 자체에 대한 연결 자격 증명을 업데이트할 수 없습니다. 필요한 경우 Meraki 대시보드에서 API 키를 수동으로 새로 고칠 수 있습니다. 자격 증명을 업데이트하고 통신을 다시 설정하려면 CDO UI에서 API 키를 수동으로 업데이트해야 합니다.



**Note** CDO가 디바이스를 동기화하지 못하면 CDO의 연결 상태에 "Invalid Credentials(유효하지 않은 자격 증명)"가 표시될 수 있습니다. 이 경우 API 키를 사용하려고 시도했을 수 있습니다. 선택한 Meraki MX의 API 키가 올바른지 확인합니다.

Meraki MX 디바이스에 대한 자격 증명을 업데이트하려면 다음 절차를 사용합니다.

### Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭한 다음 **Meraki** 탭을 클릭합니다.

단계 3 연결 자격 증명을 업데이트할 Meraki MX를 선택합니다.

단계 4 **Device Actions**(디바이스 작업) 창에서 **Update Credentials**(자격 증명 업데이트)를 클릭합니다.


단계 5 CDO가 디바이스에 로그인하는 데 사용하는 API 키를 입력하고 **Update**(업데이트)를 클릭합니다. 변경하지 않는 한 이 API 키는 Meraki MX를 온보딩하는 데 사용한 것과 동일한 자격 증명입니다. 이러한 변경 사항을 디바이스에 구축할 필요는 없습니다.

## 보안 디바이스 커넥터 이름 변경

### 프로시저

단계 1 CDO 메뉴에서 **Tools & Services**(툴 및 서비스) > **Secure Connectors**(보안 커넥터)를 선택합니다.

단계 2 이름을 바꾸려는 SDC를 선택합니다.

단계 3 세부 정보 창에서 SDC 이름 옆에 있는 편집 아이콘 를 클릭합니다.

단계 4 SDC의 이름을 바꿉니다.

---

**Inventory**(인벤토리) 창의 보안 디바이스 커넥터 필터를 포함하여 CDO 인터페이스에 SDC 이름이 나타날 때마다 이 새 이름이 나타납니다.

## 보안 디바이스 커넥터 업데이트

이 절차를 문제 해결 톨로 사용합니다. 일반적으로 SDC는 자동으로 업데이트되므로 이 절차를 사용할 필요가 없습니다. 그러나 VM의 시간 구성이 잘못된 경우 SDC는 업데이트를 수신하기 위해 AWS에 연결할 수 없습니다. 이 절차는 SDC의 업데이트를 시작하며 시간 동기화 문제로 인한 오류를 해결합니다.

### Procedure

단계 1 SDC에 연결합니다. SSH를 사용하여 연결하거나 VMware 하이퍼바이저에서 콘솔 보기를 사용할 수 있습니다.)

단계 2 **cdo** 사용자로 SDC에 로그인합니다.

단계 3 SDC 도커 컨테이너를 업데이트하려면 SDC 사용자로 전환합니다.

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

단계 4 SDC 툴킷을 업그레이드합니다.

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeToolkit
[sdc@sdc-vm ~]$
```

단계 5 SDC를 업그레이드합니다.

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeSDC
[sdc@sdc-vm ~]$
```

## 단일 CDO 테넌트에서 여러 SDC 사용

테넌트에 대해 둘 이상의 SDC를 구축하면 성능 저하 없이 더 많은 디바이스를 관리할 수 있습니다. 단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다.

테넌트에 SDC를 무제한으로 설치할 수 있습니다. 각 SDC는 하나의 네트워크 세그먼트를 관리할 수 있습니다. 이러한 SDC는 해당 네트워크 세그먼트의 디바이스를 동일한 CDO 테넌트에 연결합니다.


여러 SDC가 없으면 서로 다른 CDO 테넌트를 사용하여 격리된 네트워크 세그먼트에서 디바이스를 관리해야 합니다.

두 번째 또는 후속 SDC를 구축하는 절차는 첫 번째 SDC를 구축할 때와 동일합니다. CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축하거나 자체 VM에 보안 디바이스 커넥터 구축할 수 있습니다. 테넌트의 초기 SDC는 테넌트의 이름과 숫자 1을 포함합니다. 각 추가 SDC는 순서대로 번호가 매겨집니다.

## 동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기

동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스를 식별하려면 다음 절차를 수행합니다.

### Procedure

- 
- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
  - 단계 3 해당 디바이스 탭을 클릭합니다.
  - 단계 4 필터 기준이 이미 지정된 경우 **Inventory**(재고 목록) 테이블 상단에 있는 **clear**(지우기) 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.
  - 단계 5 필터 버튼  을 클릭하여 **필터** 메뉴를 확장합니다.
  - 단계 6 필터의 **Secure Device Connectors**(보안 디바이스 커넥터) 섹션에서 원하는 SDC의 이름을 확인합니다. **Inventory**(재고 목록) 테이블에는 필터에서 선택한 SDC를 통해 CDO에 연결하는 디바이스만 표시됩니다.
  - 단계 7 (선택 사항) 필터 메뉴에서 추가 필터를 선택하여 검색을 더욱 구체화합니다.
  - 단계 8 (선택 사항) 작업이 완료되면 **Inventory**(재고 목록) 테이블 상단에 있는 **clear**(지우기) 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.
- 

## 보안 디바이스 커넥터 오픈 소스 및 서드파티 라이선스 특성

=====

**\* amqplib \***

**amqplib copyright (c) 2013, 2014**

**Michael Bridgen <mikeb@squaremobius.net>**

이 패키지 "**amqplib**"는 MIT 라이선스에 따라 라이선스가 부여됩니다. 사본은 이 디렉토리의 **LICENSE-MIT** 파일에서 찾거나 다음에서 다운로드할 수 있습니다.

<http://opensource.org/licenses/MIT>

=====

**\* async \***

**Copyright (c) 2010-2016 Caolan McMahon**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

**\* bluebird \*****The MIT License (MIT)****Copyright (c) 2013-2015 Petka Antonov**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

**\* cheerio \*****Copyright (c) 2012 Matt Mueller <mattmuelle@gmail.com>**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

---



---

**\* command-line-args \***

**MIT 라이선스(MIT)**

**Copyright (c) 2015 Lloyd Brookes <75pound@gmail.com>**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

---



---

**\* ip \***

이 소프트웨어는 MIT 라이선스에 따라 라이선스가 부여됩니다.

**Copyright Fedor Indutny, 2012.**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

---



---

**\* json-buffer \***

**Copyright (c) 2013 Dominic Tarr**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 거래와 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 클레임, 손해, 또는 기타 책임에 대해서도 책임을 지지 않습니다.

**\* json-stable-stringify \***

이 소프트웨어는 **MIT** 라이선스에 따라 배포됩니다.

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

**\* json-stringify-safe \***

**ISC** 라이선스

**Copyright (c) Isaac Z. Schlueter and Contributors**

위의 저작권 고지와 이 허가 고지가 모든 사본에 포함되어 있는 한, 본 소프트웨어를 비용 여부에 상관없이 어떤 목적으로든 사용, 복사, 수정 및/또는 배포할 수 있는 권한이 여기에 부여됩니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 과실 또는 기타 불법 행위로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 징벌

적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

---



---

**\* lodash \***

**Copyright JS Foundation and other contributors** <<https://js.foundation/>>

**Underscore.js, copyright Jeremy Ashkenas** 기반

**DocumentCloud** 및 조사 리포터 및 편집자 <<http://underscorejs.org/>>

이 소프트웨어는 많은 개인의 자발적 기여로 구성됩니다. 정확한 기여 내역은 다음에서 제공되는 <https://github.com/lodash/lodash> 개정 내역을 참조하십시오.

다음 라이선스는 다음을 제외하고 이 소프트웨어의 모든 부분에 적용됩니다.

아래에 문서화:

====

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 우발적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

====

샘플 코드에 대한 저작권 및 관련 권리는 **CC0**을 통해 포기됩니다. 샘플 코드는 문서의 산문 내에 표시되는 모든 소스 코드로 정의됩니다.

CC0: <http://creativecommons.org/publicdomain/zero/1.0/>

====

**node\_modules** 및 공급업체 디렉토리에 있는 파일은 자체 라이선스가 있는 이 소프트웨어에서 사용하는 외부에서 유지 관리되는 라이브러리입니다. 용어가 위의 용어와 다를 수 있으므로 해당 용어를 읽어보는 것이 좋습니다.

---



---

**\* log4js \***

**Copyright 2015 Gareth Jones** (다른 많은 사람들의 기여 포함)



**Apache** 라이선스 버전 2.0("라이선스")에 따라 라이선스가 부여됩니다. 라이선스를 준수하지 않는 한 이 파일을 사용할 수 없습니다. 다음에서 라이선스 사본을 얻을 수 있습니다.

<http://www.apache.org/licenses/LICENSE-2.0>

해당 법률에서 요구하거나 서면으로 동의하지 않는 한 라이선스에 따라 배포된 소프트웨어는 명시적이든 묵시적이든 어떠한 종류의 보증이나 조건 없이 "있는 그대로" 배포됩니다. 라이선스에 따른 권한 및 제한 사항을 관리하는 특정 언어는 라이선스를 참조하십시오.

#### \* makedirs \*

Copyright 2010 James Halliday(mail@substack.net)

이 프로젝트는 MIT/X11 라이선스에 따라 배포되는 무료 소프트웨어입니다.

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

#### \* node-forge \*

새로운 BSD 라이선스(3개 조항)

Copyright (c) 2010, Digital Bazar, Inc.

All rights reserved.

다음 조건을 충족하는 경우 수정 여부에 관계없이 소스 및 바이너리 형식으로 재배포 및 사용이 허용됩니다.

\* 소스 코드의 재배포는 위의 저작권 표시, 이 조건 목록 및 다음 면책 조항을 유지해야 합니다.

\* 바이너리 형식의 재배포는 배포와 함께 제공된 설명서 및/또는 기타 자료에 위의 저작권 고지, 이 조건 목록 및 다음 면책 조항을 복제해야 합니다.

\* **Digital Bazar, Inc.**의 이름이나 기여자의 이름은 특정 사전 서면 허가 없이 이 소프트웨어에서 파생된 제품을 보증하거나 홍보하는 데 사용할 수 없습니다.

이 소프트웨어는 저작권자와 기여자에 의해 "있는 그대로" 제공되며, 명시적 또는 묵시적으로 상품성 및 특정 목적에의 적합성을 포함한 모든 보증이 거부됩니다. 어떠한 경우에도 **DIGITAL BAZAAR**는 어떠한 직접적, 간접적, 부수적, 특별, 징벌적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사

용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다. 이러한 손해가 계약, 엄격한 책임, 불법행위(과실 또는 기타 포함)에 대한 어떠한 책임 이론에 의거하여 발생하였는지 여부와 상관없이, 해당 손해의 가능성이 있음을 사전에 고지받았더라도, 이 소프트웨어의 사용으로 인해 발생하는 어떠한 방식의 책임도 지지 않습니다.

---

**\* request \***

**Apache License**

버전 2.0, January 2004

<http://www.apache.org/licenses/>

사용, 복제 및 배포에 대한 약관

**1. 정의.**

"라이선스"는 이 문서의 섹션 1에서 9까지 정의된 사용, 복제 및 배포에 대한 조건을 의미합니다.

"라이선스 제공자"는 라이선스를 부여하는 저작권 소유자 또는 저작권 소유자가 승인한 법인을 의미합니다.

"법적 실체"는 행위 실체와 해당 실체를 통제하거나 통제받거나 공동 통제하에 있는 다른 모든 실체의 조합을 의미합니다. 이 정의의 목적상 "통제"는 (i) 계약 또는 기타 방식으로 해당 법인의 지시 또는 관리를 유발하는 직간접적인 권한 또는 (ii) 50%(50%) 또는 더 많은 발행주식, 또는 (iii) 해당 법인의 수익적 소유권.

"귀하"(또는 "귀하의")는 계약 또는 기타 방식으로 본 라이선스에 의해 부여된 권한을 행사하는 개인 또는 법인을 의미하거나 (ii) 다음 중 50% 이상을 소유합니다. 발행주식, 또는 (iii) 그러한 법인의 수익적 소유권.

"소스" 형식은 소프트웨어 소스 코드, 문서 소스 및 구성 파일을 포함하되 이에 국한되지 않는 수정을 위한 기본 형식을 의미합니다.

"개체" 형식은 컴파일된 개체 코드, 생성된 문서 및 다른 미디어 유형으로의 변환을 포함하되 이에 국한되지 않는 소스 형식의 기계적 변환 또는 변환으로 인해 발생하는 모든 형식을 의미합니다.

"저작물"은 저작물에 포함되거나 첨부된 저작권 표시(예는 아래 부록에 제공됨)에 표시된 대로 라이선스에 따라 사용 가능한 소스 또는 개체 형식의 저작물을 의미합니다.

"파생 저작물"은 저작물을 기반으로 하는(또는 저작물에서 파생된) 원본 또는 개체 형식의 모든 저작물을 의미하며 편집 편집, 주석, 정교화 또는 기타 편집이 전체적으로 저자의 원본 저작물을 나타냅니다. 본 라이선스에서 파생물은 저작물 및 그 파생물과 분리된 상태를 유지하거나 인터페이스에 단순히 링크(또는 이름으로 연결)되는 저작물은 포함하지 않습니다.

"기여"는 원본 저작물과 저작물에 포함하기 위해 저작권 소유자 또는 저작권 소유자를 대신하여 제출할 권한이 있는 개인 또는 법인이 라이선스 허가자에게 의도적으로 제출된 저작물 또는 파생물에 대한 편집 또는 추가를 포함한 저작물을 의미합니다. 이 정의에서 "제출"은 저작물에 대해 논의하고 개선하기 위해 라이선스 허가자 또는 그 대리인에게 전송되는 모든 형태의 전자, 구두 또는 서면 제출을 의미합니다. 여기에는 저작물을 논의하고 개선할 목적으로 라이선스 허가자 또는 그 대리인이 관리하는 전자 메일 목록, 소스 코드 제어 시스템, 문제 추적 시스템을 통한 커뮤니케이션이 포함

되며 이에 국한되지 않습니다. 단, 저작권 소유자가 "기고문이 아님"을 명시적으로 표시하거나 서면으로 지정한 커뮤니케이션은 제외됩니다.

"기여자"는 라이선스 제공자 및 라이선스 제공자가 대신하여 기여물을 받아 작업물에 통합한 모든 개인 또는 법인을 의미합니다.

**2. 저작권 라이선스 부여.** 이 라이선스의 조건에 따라 각 기여자는 이로써 귀하에게 영구적이고 전 세계적이며 비독점적이고 무료이며 로열티가 없고 취소할 수 없는 저작권 라이선스를 부여합니다. 저작물 및 그러한 파생 저작물을 소스 또는 개체 형태로 재라이선스하고 배포합니다.

**3. 특허 라이선스 부여.** 본 라이선스의 약관에 따라 각 기여자는 귀하에게 저작물의 제작, 사용, 판매 제안, 판매, 가져오기, 기타 방식의 이전을 위한 영구적, 세계적, 비독점적, 요금 및 로열티 무료, 철회 불가능한(본 섹션에 명시된 경우 제외) 특허 라이선스를 부여합니다. 이러한 라이선스는 기여자가 부여할 수 있는 특허권에만 적용되며, 이는 기여물 단독으로 또는 기여물이 제출된 저작물과의 조합으로 인해 침해될 수 있습니다. 귀하가 저작물 또는 저작물에 통합된 기여가 직접적 또는 기여적 특허 침해를 구성한다고 주장하는 어떤 법인에 대해 특허 소송(소송에서 교차 청구 또는 반소 포함)을 제기하는 경우, 본 라이선스에 따라 귀하에게 부여된 모든 특허 라이선스는 작업은 그러한 소송이 제기된 날짜에 종료됩니다.

**4. 재배포.** 귀하는 다음 조건을 충족하는 경우 편집 여부에 관계없이 모든 매체와 소스 또는 개체 형식으로 저작물 또는 그 파생 저작물의 사본을 재생산 및 배포할 수 있습니다.

귀하는 저작물 또는 파생 저작물의 다른 수령인에게 본 라이선스의 사본을 제공해야 합니다. 그리고 귀하는 수정된 파일에 귀하가 파일을 변경했음을 알리는 눈에 띄는 통지를 전달해야 합니다. 그리고 파생 저작물의 일부와 관련되지 않은 통지를 제외하고 저작물의 소스 형식에서 가져온 모든 저작권, 특허, 상표 및 귀속 고지를 귀하가 배포하는 파생 저작물의 소스 형식으로 유지해야 합니다. 그리고 저작물이 배포의 일부로 **"NOTICE"** 텍스트 파일을 포함하는 경우 귀하가 배포하는 모든 파생 저작물에는 그러한 **NOTICE** 파일에 포함된 귀속 고지의 읽을 수 있는 사본이 포함되어야 합니다. 다음 위치 중 적어도 하나에 있는 **2차 저작물: 2차 저작물의 일부로 배포되는 NOTICE** 텍스트 파일 내에서 파생 저작물과 함께 제공되는 경우 소스 양식 또는 문서 내에서; 또는 파생 저작물에 의해 생성된 디스플레이 내에서 그러한 **제3자 고지**가 일반적으로 표시되는 경우. **NOTICE** 파일의 내용은 정보 제공의 목적으로만 사용되며 이에 따라 라이선스가 편집되지 않습니다. 저작물의 **NOTICE** 텍스트와 함께 또는 그 부록으로 배포하는 파생물 내 속성 고지로 인해 라이선스가 변경되지 않는 경우, 이러한 추가적인 속성 고지를 추가할 수 있습니다. 귀하는 귀하의 편집 사항에 자신의 저작권 진술을 추가할 수 있으며 편집 사항의 사용, 복제 또는 배포 또는 그러한 파생 저작물 전체에 대한 추가 또는 다른 라이선스 조건을 제공할 수 있습니다. 그렇지 않으면 저작물은 본 라이선스에 명시된 조건을 준수합니다.

**5. 기여물 제출.** 귀하가 달리 명시하지 않는 한, 귀하가 저작물에 포함하기 위해 라이선스 허가자에게 의도적으로 제출한 모든 기여물은 추가 약관 없이 본 라이선스의 약관에 따라야 합니다. 위의 내용에도 불구하고 여기의 어떠한 내용도 그러한 기여와 관련하여 귀하가 라이선스 제공자와 체결한 별도의 라이선스 계약 조건을 대체하거나 편집하지 않습니다.

**6. 상표.** 본 라이선스는 저작물의 출처를 설명하고 **NOTICE** 파일의 내용을 재생산하는 데 합당하고 관례적인 사용에 필요한 경우를 제외하고 라이선스 제공자의 상표명, 상표, 서비스 마크 또는 제품 이름을 사용할 수 있는 권한을 부여하지 않습니다.

7. 보증의 면책조항. 해당 법률에 의해 요구되는 경우나 서면으로 합의된 경우를 제외하고, 라이선서는 작업물(및 각 기여자는 자신의 기여물)을 "있는 그대로" 제공하며, 명시적이거나 묵시적으로 어떠한 종류의 보증이나 조건도 포함하지 않습니다. 이는 제목, 비침해성, 상품성 또는 특정 목적에 대한 적합성에 대한 어떠한 보증이나 조건을 포함합니다. 귀하는 저작물 사용 또는 재배포의 적합성을 판단할 전적인 책임이 있으며 본 라이선스에 따른 귀하의 권한 행사와 관련된 모든 위험을 감수합니다.

8. 책임의 제한. 어떠한 경우에도, 과실(비롯하여 과실포함 책임), 계약 또는 기타 이론에 의한, 해당 법에 의해 요구되는 경우(예: 고의적이고 중대한 과실 행위)나 서면으로 합의된 경우를 제외하고, 어떤 기여자도 본 라이선스로 인한 손해에 대해 법적으로 책임을 지지 않습니다. 이는 작업물의 사용 또는 사용 불능으로 인해 발생하는 어떠한 종류의 직접적, 간접적, 특수적, 우발적 또는 결과적 손해(예: 선의의 상실, 작업 중단, 컴퓨터 고장 또는 장애, 그 외 모든 상업적 손해나 손실을 포함)에 대해서도 책임을 지지 않습니다. 심지어 해당 기여자에게 그러한 손해의 가능성이 알려져 있더라도 마찬가지입니다.

9. 보증 또는 추가 책임 수락. 저작물 또는 그 파생물을 재배포하는 경우 귀하는 지원, 보증, 면책 또는 본 라이선스와 일치하는 기타 책임 의무 및/또는 권리의 수락을 제공하고 요금을 청구할 수 있습니다. 그러나 이러한 의무를 수락할 때에는 다른 기여자를 대신하여 행동하지 않고 오로지 자신의 명의로, 자신의 책임하에만 행동해야 하며, 해당 보증이나 추가적인 책임을 수락함으로써 발생하는 어떠한 책임에 대해서도 각 기여자를 면책시키고 방어하며 보호하기 위해 보증을 제공하는 경우에만 그렇게 행동할 수 있습니다.

이용 약관의 끝

---



---

**\* rimraf \***

**ISC 라이선스**

**Copyright (c) Isaac Z. Schlueter and Contributors**

위의 저작권 고지와 이 허가 고지가 모든 사본에 포함되어 있는 한, 본 소프트웨어를 비용 여부에 상관없이 어떤 목적으로든 사용, 복사, 수정 및/또는 배포할 수 있는 권한이 여기에 부여됩니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 과실 또는 기타 불법 행위로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 징벌적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 상실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

---



---

**\* uuid \***

**Copyright (c) 2010-2012 Robert Kieffer**

**MIT 라이선스-** <http://opensource.org/licenses/mit-license.php>

---



---

**\* validator \***

**Copyright (c) 2016 Chris O'Hara <cohara87@gmail.com>**

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 우발적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

---

#### \* when \*

오픈 소스 이니셔티브 **OSI - MIT** 라이선스

<http://www.opensource.org/licenses/mit-license.php>

#### Copyright (c) 2011 Brian Cavalier

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 우발적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

---

## CDO에 로그인

Cisco Defense Orchestrator(CDO)에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 **사용자 관리**가 있는 계정이 필요합니다.

IdP 어카운트에는 사용자의 자격 증명에 포함되며 IdP는 이러한 자격 증명을 기반으로 사용자를 인증합니다. 다단계 인증은 ID 보안의 추가 레이어를 제공합니다. CDO 사용자 레코드에는 주로 사용자

이름, 연결된 CDO 테넌트 및 사용자의 역할이 포함됩니다. 사용자가 로그인하면 CDO는 IdP의 사용자 ID를 CDO의 테넌트에 있는 기존 사용자 레코드에 매핑하려고 시도합니다. CDO가 일치 항목을 찾으면 사용자는 해당 테넌트에 로그인됩니다.

엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. Cisco Secure Cloud Sign-On은 다단계 인증에 Duo를 사용합니다. 고객은 원하는 경우 SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 통합할 수 있습니다.

CDO에 로그인하려면 먼저 Cisco Secure Cloud Sign-On에서 계정을 생성하고 Duo Security를 사용하여 MFA(Multi-Factor Authentication)를 구성하고 테넌트 최고 관리자가 CDO 레코드를 생성하도록 해야 합니다.

2019년 10월 14일에 CDO는 Cisco Secure Cloud Sign-On을 ID 제공자 및 MFA용 Duo로 사용하도록 기존의 모든 테넌트를 변환했습니다.



- 참고
- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 CDO에 로그인하는 경우 Cisco Secure Cloud Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
  - CDO 무료 평가판을 사용 중인 경우 이 전환이 영향을 미쳤습니다.

CDO 테넌트가 2019년 10월 14일 이후에 생성된 경우 [새 CDO 테넌트에 대한 초기 로그인, 40 페이지](#)를 참조하십시오.

2019년 10월 14일 이전에 CDO 테넌트가 존재했다면 [Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 41 페이지](#)를 참조하십시오.

## 새 CDO 테넌트에 대한 초기 로그인

Cisco Defense Orchestrator(CDO)는 Cisco Secure Cloud Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo를 사용합니다. CDO에 로그인하려면 먼저 **Cisco Secure Sign-On**에서 계정을 생성하고 **Duo**를 사용하여 **MFA**를 구성해야 합니다.

v에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.



- 중요
- 2019년 10월 14일 이전에 CDO 테넌트가 존재했다면 이 문서 대신 [Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 41 페이지](#)를 사용하여 로그인 지침을 사용합니다.**

시작하기 전에



**DUO Security** 설치. 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 [Duo 이중 인증 가이드: 등록 가이드](#)를 참고하십시오.

시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.

다음 작업?

새 [Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성](#), 72 페이지를 계속합니다. 이는 4 단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

## 로그인 실패 문제 해결

실수로 잘못된 CDO 지역에 로그인했기 때문에 로그인에 실패함

적절한 CDO 지역에 로그인했는지 확인합니다. <https://sign-on.security.cisco.com>에 로그인하면 액세스할 지역을 선택할 수 있습니다. CDO타일을 클릭하여 [defenceorchestrator.com](https://defenceorchestrator.com)에 액세스하거나 CDO(EU)를 클릭하여 [defenceorchestrator.eu](https://defenceorchestrator.eu)에 액세스합니다.

## Cisco Secure Cloud Sign On ID 제공자로 마이그레이션

2019년 10월 14일, Cisco Defense Orchestrator(CDO)는 모든 테넌트를 MFA(multi-factor authentication)를 위한 ID 제공자 및 Duo로 Cisco Secure Cloud Sign-On으로 변환했습니다. CDO에 로그인하려면 먼저 [Cisco Secure Sign-On](#)에서 계정을 활성화하고 Duo를 사용하여 MFA를 구성해야 합니다.

CDO에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.



참고

- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 CDO에 로그인하는 경우 Cisco Secure Cloud Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
- CDO 무료 평가판을 사용 중인 경우 이 전환이 적용됩니다.
- CDO 테넌트가 2019년 10월 14일 이후에 생성된 경우 이 문서 대신 [새 CDO 테넌트에 대한 초기 로그인](#), 40 페이지에서 로그인 지침을 참조하십시오.

시작하기 전에

마이그레이션하기 전에 다음 단계를 수행하는 것이 좋습니다.

-  **DUO Security** 설치. 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 [Duo 이중 인증 가이드: 등록 가이드](#)를 참고하십시오.

- 시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.
- 새 Cisco Secure Sign-On 어카운트 생성 및 Duo 다단계 인증 구성. 이는 4 단계 프로세스입니다. 4 단계를 모두 완료해야 합니다.

## 마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 CDO에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 72 페이지의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

**Cisco Secure Cloud Sign-On** 대시보드 로그인에 성공했지만 CDO를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 <https://cdo.onelogin.com>을 가리킬 수 있습니다.

해결 방법 <https://sign-on.security.cisco.com>에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성
- 해결 방법 새 계정을 생성한 경우 대시보드에서 Cisco Defense Orchestrator(US), Cisco Defense Orchestrator(EU) 또는 Cisco Defense Orchestrator(APJC)에 해당하는 CDO 타일을 클릭합니다.
- 해결 방법 <https://sign-on.security.cisco.com>을 가리키도록 북마크를 업데이트합니다.

## Cisco Secure Cloud Sign On 대시보드에서 CDO 실행

### Procedure

- 단계 1 Cisco Secure Cloud Sign-on 대시보드에서 해당 CDO 버튼을 클릭합니다. CDO 타일은 <https://defenseorchestrator.com>으로 안내하고 CDO(EU) 타일은 <https://defenseorchestrator.eu>로 안내합니다.
- 단계 2 두 인증자를 모두 설정한 경우 인증자 로고를 클릭하여 Duo Security 또는 Google Authenticator를 선택합니다.



- 기존 테넌트에 사용자 레코드가 이미 있는 경우 해당 테넌트에 로그인됩니다.
- 이미 여러 포털에 사용자 레코드가 있는 경우 연결할 포털을 선택할 수 있습니다.
- 여러 테넌트에 대한 사용자 레코드가 이미 있는 경우 연결할 CDO 테넌트를 선택할 수 있습니다.
- 기존 테넌트에 대한 사용자 레코드가 아직 없는 경우 CDO에 대해 자세히 알아보거나 평가판 테넌트를 요청할 수 있습니다.

포털 보기는 여러 테넌트에서 통합된 정보를 검색하고 표시합니다. 자세한 내용은 [멀티 테넌트 포털 관리](#), on page 62을 참조하십시오.

테넌트 보기에는 사용자 레코드가 있는 여러 테넌트가 표시됩니다.



## 테넌트에서 슈퍼 관리자 관리

테넌트의 슈퍼 관리자 수를 제한하는 것이 가장 좋습니다. 슈퍼 관리자 권한을 가져야 하는 사용자를 결정하고 [사용자 관리](#)를 검토한 다음 다른 사용자의 역할을 "Admin(관리자)"으로 변경합니다.

## CDO에서 지원하는 소프트웨어 및 하드웨어

CDO 설명서에서는 CDO가 지원하는 소프트웨어 및 디바이스에 대해 설명합니다. CDO가 지원하지 않는 소프트웨어 및 디바이스는 지적하지 않습니다. 소프트웨어 버전 또는 디바이스 유형에 대한 지원을 명시적으로 요청하지 않는 경우 지원되지 않습니다.

관련 정보:

- [Secure Firewall Threat Defense 디바이스 지원 세부 사항, 44 페이지](#)
- [브라우저 지원, 47 페이지](#)

## Secure Firewall Threat Defense 디바이스 지원 세부 사항



**Note** Secure Firewall device manager(FDM) 지원 및 기능은 요청 시에만 제공됩니다. 테넌트에서 Firewall Device Manager 지원을 아직 활성화하지 않은 경우 디바이스를 관리하거나 FDM 관리 디바이스에 구축할 수 없습니다. [TAC를 사용하여 지원 티켓 열기](#)에 요청을 보냅니다.

Secure Firewall Threat Defense 방화벽은 Cisco의 차세대 방화벽입니다. 이는 차세대 방화벽 서비스와 ASA 플랫폼의 장점을 결합하기 위해 노력합니다. 다양한 ASA 및 Firepower 하드웨어 디바이스 또는 가상 머신에 설치할 수 있습니다.

지원하는 기능을 검토하려면 [Cisco Defense Orchestrator를 사용한 FDM-관리 디바이스 관리](#)를 검토하십시오. 온보딩 사전 요건 및 요구 사항에 대한 자세한 내용은 [위협 방어 디바이스 온보딩](#)을 참조하십시오.



**Note** Snort 3은 버전 6.7 이상을 실행하는 FDM 관리 디바이스에서 사용할 수 있습니다. Snort 2와 Snort 3 간에 전환할 수는 있지만 구성이 호환되지 않을 수 있습니다. Snort 3, 지원되는 디바이스 및 소프트웨어, 제한 사항에 대한 자세한 내용은 [Snort 3.0으로 업그레이드, on page 241](#)의 내용을 참조하십시오.

**CDO**에서 지원하는 하드웨어 및 소프트웨어 이미지

다음 테이블의 CDO 열은 하드웨어 플랫폼인 CDO에서 지원하는 Secure Firewall Threat Defense 소프트웨어 버전을 나타냅니다.

**Table 1: Secure Firewall Threat Defense 관리자 및 버전별 하드웨어**

디바이스 플랫폼	디바이스 버전: <b>Management Center</b> 사용		디바이스 버전: <b>Device Manager</b> 사용	
	고객이 구축한 관리 센터	클라우드 사용 <b>Firewall Management Center *</b>	<b>Device Manager</b> 전용	<b>Device Manager + CDO</b>
Firepower 1010, 1120, 1140	6.4+	7.0.3+	6.4+	6.4+
Firepower 1010E	7.2.3+ 7.3에서 지원되지 않음	7.2.3+ 7.3에서 지원되지 않음	7.2.3+ 7.3에서 지원되지 않음	7.2.3+ 7.3에서 지원되지 않음

디바이스 플랫폼	디바이스 버전: <b>Management Center</b> 사용		디바이스 버전: <b>Device Manager</b> 사용	
	고객이 구축한 관리 센터	클라우드 사용 <b>Firewall Management Center *</b>	<b>Device Manager</b> 전용	<b>Device Manager + CDO</b>
Firepower 1150	6.5+	7.0.3+	6.5+	6.5+
Firepower 2110, 2120, 2130, 2140	6.2.1+	7.0.3+	6.2.1+	6.4+
Secure Firewall 3110, 3120, 3130, 3140	7.1+	7.0.3+	7.1+	7.1+
Firepower 4110, 4120, 4140	6.0.1~7.2	7.2+	6.5~7.2	6.5~7.2
Firepower 4150	6.1~7.2	7.2+	6.5~7.2	6.5~7.2
Firepower 4115, 4125, 4145	6.4+	7.0.3+	6.5+	6.5+
Firepower 4112	6.6+	7.0.3+	6.6+	6.6+
Firepower 9300: SM-24, SM-36, SM-44	6.0.1~7.2	7.0.3+	6.5~7.2	6.5~7.2
Firepower 9300: SM-40, SM-48, SM-56	6.4+	7.0.3+	6.5+	6.5+
ISA 3000	6.2.3 이상	7.0.3+	6.2.3 이상	6.4+
ASA 5506-X, 5506H-X, 5506W-X	6.0.1~6.2.3	—	6.1~6.2.3	—
ASA 5508-X, 5516-X	6.0.1~7.0	7.0.3~7.0.x	6.1~7.0	6.4~7.0
ASA 5512-X	6.0.1~6.2.3	—	6.1~6.2.3	—
ASA 5515-X	6.0.1~6.4	—	6.1~6.4	6.4
ASA 5525-X, 5545-X, 5555-X	6.0.1~6.6	—	6.1~6.6	6.4 ~ 6.6

\* 클라우드 사용 Firewall Management Center는 버전 7.1을 실행하는 threat defense 디바이스 또는 모든 버전을 실행하는 클래식 디바이스를 관리할 수 없습니다. 클라우드 관리 등록을 취소하고 비활성화하지 않는 한 클라우드 매니지드 디바이스를 버전 7.0.x에서 버전 7.1로 업그레이드할 수 없습니다. 디바이스를 버전 7.2 이상으로 직접 업그레이드하는 것이 좋습니다.

**CDO**에서 지원하는 가상 머신 플랫폼 및 소프트웨어 이미지

다음 표의 CDO 열린 가상 디바이스 플랫폼, CDO가 지원하는 Firepower Threat Defense 소프트웨어 버전을 나타냅니다.

**Table 2: Threat Defense Virtual** 관리자 및 버전별

디바이스 플랫폼	디바이스 버전: <b>Management Center</b> 사용		디바이스 버전: <b>Device Manager</b> 사용	
	고객이 구축한 관리 센터	클라우드 사용 <b>Firewall Management Center</b> *	<b>Device Manager</b> 전용	<b>Device Manager + CDO</b>
공용 클라우드				
Alibaba	7.2+	7.2%	—	—
AWS	6.0.1+	7.0.3+	6.6+	6.6+
Azure	6.2+	7.0.3+	6.5+	6.5+
GCP	6.7+	7.0.3+	7.2+	7.2%
OCI	6.7+	7.0.3+	—	—
온프레미스/프라이빗 클라우드				
HyperFlex	7.0+	7.0.3+	7.0+	7.0+
KVM	6.1+	7.0.3+	6.2.3 이상	6.4+
Nutanix	7.0+	7.0.3+	7.0+	7.0+
OpenStack	7.0+	7.0.3+	—	—
VMware 7.0	7.0+	7.0.3+	7.0+	7.0+
VMware 6.7	6.5+	7.0.3+	6.5+	6.5+
VMware 6.5	6.2.3 이상	7.0.3+	6.2.3 이상	6.4+
VMware 6.0	6.0~6.7	—	6.2.2~6.7	6.4~6.7
VMware 5.5	6.0.1~6.2.3	—	6.2.2~6.2.3	—
VMware 5.1	6.0.1만	—	—	—

\* 클라우드 사용 Firewall Management Center는 버전 7.1을 실행하는 threat defense 디바이스 또는 모든 버전을 실행하는 클래식 디바이스를 관리할 수 없습니다. 클라우드 관리 등록을 취소하고 비활성화하지 않는 한 클라우드 매니지드 디바이스를 버전 7.0.x에서 버전 7.1로 업그레이드할 수 없습니다. 디바이스를 버전 7.2 이상으로 직접 업그레이드하는 것이 좋습니다.

CDO를 사용하여 Firepower 디바이스 인터페이스를 관리하는 방법에 대한 자세한 내용은 [Firepower 인터페이스 구성에 대한 지침 및 제한 사항](#)을 참조하십시오.

#### ASA FirePOWER 서비스 모듈

CDO는 ASA FirePOWER 서비스 모듈을 지원하지 않습니다.

## 브라우저 지원

CDO는 다음 브라우저의 최신 버전을 지원합니다.

- Google Chrome
- Mozilla Firefox

## Cisco Defense Orchestrator 플랫폼 유지 관리 일정

#### Cisco Defense Orchestrator 유지 관리 일정

CDO은 새로운 기능과 품질 개선으로 매주 플랫폼을 업데이트합니다. 이 일정에 따라 업데이트가 3 시간 동안 이루어질 수 있습니다.

대부분의 경우 업데이트는 목요일에 완료되지만 필요한 경우 금요일 및 일요일의 유지 관리 시간이 사용됩니다.

표 3: CDO 유지 관리 일정

요일	시간 (24시간제)
목요일	09:00 UTC - 12:00 UTC
금요일	09:00 UTC - 12:00 UTC
일요일	09:00 UTC - 12:00 UTC

이 유지 관리 기간 동안 테넌트에 계속 액세스할 수 있으며 클라우드 사용 Firewall Management Center가 있는 경우, 해당 플랫폼에도 액세스할 수 있습니다. 또한 CDO에 온보딩한 디바이스가 보안 정책을 계속 적용합니다.



참고 유지 관리 기간 동안 관리하는 디바이스에 구성 변경 사항을 배포하는 데 CDO를 사용하지 않는 것이 좋습니다.

CDO를 중지하거나 클라우드 사용 Firewall Management Center과 통신을 중단되는 오류가 있는 경우, 해당 오류는 유지 관리 기간을 벗어나더라도 영향을 받는 모든 테넌트에서 가능한 한 빨리 해결됩니다.

#### 클라우드 제공 **Firewall Management Center** 유지 관리 일정

테넌트에 배포된 클라우드 사용 Firewall Management Center을 보유한 고객은 CDO가 클라우드 사용 Firewall Management Center 환경을 업데이트하기 약 1주일 전에 알림을 받습니다. 테넌트의 슈퍼 관리자 및 관리 사용자는 이메일로 알림을 받습니다. CDO는 또한 모든 사용자에게 예정된 업데이트를 알리는 배너를 홈페이지에 표시합니다.

테넌트에 대한 업데이트는 최대 1시간이 걸릴 수 있으며 테넌트 지역에 할당된 유지 관리 날짜의 3시간 유지 관리 시간 내에 이루어집니다. 테넌트가 업데이트되는 동안에는 클라우드 사용 Firewall Management Center 환경에 액세스할 수 없지만, CDO의 나머지 부분에 계속 액세스할 수 있습니다.

표 4: 클라우드 제공 **Firewall Management Center** 유지 관리 일정

요일	시간 (24시간제)	지역
수요일	04:00 UTC - 07:00 UTC	유럽, 중동 또는 아프리카 (EMEA)
수요일	17:00 UTC - 20:00 UTC	아시아-태평양-일본(APJ)
목요일	09:00 UTC - 12:00 UTC	아메리카

## 테넌트 관리

Cisco Defense Orchestrator(CDO)는 설정 페이지에서 테넌트 및 개별 사용자 계정의 특정 측면을 사용자 지정할 수 있는 기능을 제공합니다. CDO 메뉴의 왼쪽 탐색 패널에서 **Settings**(설정)를 클릭합니다.

관련 정보:

- [일반 설정, 48 페이지](#)
- [사용자 관리](#)
- [로깅 설정](#)
- [알림 설정, 53 페이지](#)

## 일반 설정

오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

일반 CDO 설정에 관한 다음 항목을 참조하십시오.

- 사용자 설정, on page 49
- 내 토큰은 [API 토큰, on page 58](#)를 참조하십시오.
- **Tenant Settings**(테넌트 설정)은 다음을 참조하십시오.
  - 변경 요청 추적 활성화, on page 49
  - Cisco 지원에서 테넌트를 볼 수 없도록 설정, on page 50
  - 자동 구축 예약 옵션 활성화, on page 51
  - 기본 충돌 탐지 간격, on page 50
  - 웹 분석, on page 51
  - 기본 반복 백업 일정 구성, on page 52
  - 테넌트 ID, on page 52
  - 테넌트 이름, on page 52

## 사용자 설정

CDO UI를 표시할 언어를 선택합니다. 이 선택은 이 변경을 수행하는 사용자에게만 영향을 미칩니다.

## 내 토큰

자세한 내용은 [API 토큰](#)을 참조하십시오.

## 테넌트 설정

### 변경 요청 추적 활성화

변경 요청 추적을 활성화하면 테넌트의 모든 사용자에게 영향을 미칩니다. 변경 요청 추적을 활성화하려면 다음 절차를 따르십시오.

#### Procedure

단계 1 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

단계 2 **General**(일반) 탭을 클릭합니다.

단계 3 변경 요청 추적 아래의 슬라이더를 클릭합니다.

확인되면 인터페이스의 왼쪽 하단 모서리에 변경 요청 도구 모음이 나타나고 변경 로그의 변경 요청 드롭다운 메뉴가 나타납니다.

## Cisco 지원에서 테넌트를 볼 수 없도록 설정

Cisco 지원에서는 지원 티켓을 해결하거나 두 개 이상의 고객에게 영향을 미치는 문제를 사전에 해결하기 위해 사용자를 테넌트와 연결합니다. 그러나 원하는 경우 계정 설정을 변경하여 Cisco 지원이 테넌트에 액세스하지 못하도록 할 수 있습니다. 이렇게 하려면 "Cisco 지원에서 이 테넌트를 볼 수 없도록 방지" 아래의 버튼을 밀어서 녹색 확인 표시를 표시합니다.

Cisco 지원에서 테넌트를 볼 수 없도록 하려면 다음 절차를 따르십시오.

### Procedure

단계 1 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.

단계 2 **General(일반)** 탭을 클릭합니다.

단계 3 **Cisco** 지원팀에서 이 테넌트를 볼 수 없도록 방지 아래의 슬라이더를 클릭합니다.

## 디바이스 변경 사항 자동 수락 옵션 활성화

디바이스 변경에 대한 자동 수락을 활성화하면 Defense Orchestrator가 디바이스에서 직접 수행된 모든 변경 사항을 자동으로 수락할 수 있습니다. 이 옵션을 비활성화된 상태로 두거나 나중에 비활성화하는 경우 수락하기 전에 각 디바이스 충돌을 검토해야 합니다.

디바이스 변경 사항에 대한 자동 수락을 활성화하려면 다음 절차를 따르십시오.

### Procedure

단계 1 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.

단계 2 **General(일반)** 탭을 클릭합니다.

단계 3 **Enable the option to auto-accept device changes(디바이스 변경 사항을 자동으로 수락하는 옵션 활성화)** 아래의 슬라이더를 클릭합니다.

## 기본 충돌 탐지 간격

이 간격은 CDO가 변경 사항을 위해 온보딩된 디바이스를 폴링하는 빈도를 결정합니다. 이 선택은 이 테넌트로 관리되는 모든 디바이스에 영향을 주며 언제든지 변경할 수 있습니다.



**Note** 하나 이상의 디바이스를 선택한 후 **Inventory(재고 목록)** 페이지에서 사용 가능한 **Conflict Detection(충돌 탐지)** 옵션을 통해 이 선택 항목을 오버라이드할 수 있습니다.

이 옵션을 구성하고 충돌 탐지를 위한 새 간격을 선택하려면 다음 절차를 수행합니다.




## Procedure

- 단계 1 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.
- 단계 2 **General Settings(일반 설정)** 탭을 클릭합니다.
- 단계 3 **Default Conflict Detection Interval(기본 충돌 탐지 간격)**의 드롭다운 메뉴를 클릭하고 시간 값을 선택합니다.

### 자동 구축 예약 옵션 활성화

자동 구축을 예약하는 옵션을 활성화하면 편리한 날짜와 시간에 향후 구축을 예약할 수 있습니다. 활성화되면 단일 또는 반복 자동 구축을 예약할 수 있습니다. 자동 구축을 예약하려면 [자동 구축 예약](#)을 참조하십시오.

전용 의 보류 중인 변경 사항이 있는 경우 디바이스에 대한 CDO의 변경 사항은 디바이스에 자동으로 구축되지 않습니다. 디바이스가 **Conflict Detected(충돌 탐지됨)** 또는 **Not Synced(동기화되지 않음)**와 같이 **Synced(동기화됨)** 상태가 아닌 경우 예약된 구축이 실행되지 않습니다. 예약된 구축이 실패한 모든 인스턴스가 작업 페이지에 나열됩니다.

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



**Important** CDO를 사용하여 디바이스에 대해 둘 이상의 예약된 구축을 생성하는 경우 새 구축이 기존 구축을 덮어씁니다. API를 사용하여 디바이스에서 둘 이상의 예약된 구축을 생성하는 경우, 새 구축을 예약하기 전에 기존 구축을 삭제해야 합니다.

자동 구축을 예약하는 옵션을 활성화하려면 다음 절차를 따르십시오.

## Procedure

- 단계 1 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.
- 단계 2 **General Settings(일반 설정)** 탭을 클릭합니다.
- 단계 3 **Enable the option to schedule automatic deployment(자동 구축을 예약하는 옵션 활성화)** 아래의 슬라이더를 클릭합니다.

### 웹 분석

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

웹 분석은 기본적으로 활성화됩니다. 웹 분석을 비활성화하거나 나중에 활성화하려면 다음 절차를 따르십시오.

### Procedure

- 
- 단계 1 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
  - 단계 2 **General Settings**(일반 설정) 탭을 클릭합니다.
  - 단계 3 웹 분석 아래의 슬라이더를 클릭합니다.
- 

## 기본 반복 백업 일정 구성

여러 디바이스에서 백업 일정을 일관되게 하려면 이 설정을 사용하여 기본 반복 백업 일정을 구성하십시오. 특정 디바이스에 대한 백업을 예약할 때 기본 설정을 사용하거나 변경할 수 있습니다. 기본 반복 백업 일정을 변경해도 기존의 예약된 백업이나 반복 백업 일정은 변경되지 않습니다.

### Procedure

- 
- 단계 1 **Frequency**(빈도) 필드에서 매일, 매주 또는 매월을 선택합니다.
  - 단계 2 백업을 수행할 시간을 24시간 단위로 선택합니다. UTC(Coordinated Universal Time)로 시간을 예약합니다.
    - 매주 백업하는 경우: 백업을 수행할 요일을 확인합니다.
    - 매월 백업하는 경우: **Days of Month**(날짜) 필드를 클릭하고 백업을 예약할 날짜를 추가합니다. 참고: 31일을 입력했지만 해당 월에 31일이 없는 경우 백업이 수행되지 않습니다. 예약된 백업 시간에 이름과 설명을 지정합니다.
  - 단계 3 **Save**(저장)를 클릭합니다.
- 자세한 내용은 [단일 FDM-관리 디바이스에 대한 반복 백업 일정 구성](#)을 참조하십시오.
- 

## 테넌트 ID

테넌트 ID는 테넌트를 식별합니다. 이 정보는Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다.

## 테넌트 이름

테넌트 이름도 테넌트를 식별합니다. 테넌트 이름은 조직 이름이 아닙니다. 이 정보는Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다.

## 알림 설정

테넌트와 연결된 디바이스가 특정 작업을 수행할 때마다 CDO에서 이메일 알림을 받도록 구독할 수 있습니다. 이러한 알림은 테넌트와 연결된 모든 디바이스에 적용되지만, 모든 디바이스 유형이 사용 가능한 모든 옵션을 지원하는 것은 아닙니다. 또한 아래에 나열된 CDO 알림에 대한 변경 사항은 실시간으로 자동 업데이트되며 구축이 필요하지 않습니다.

CDO의 이메일 알림은 작업 유형 및 영향을 받는 디바이스를 나타냅니다. 디바이스의 현재 상태 및 작업 내용에 대한 자세한 정보를 알아보려면 CDO에 로그인하여 영향을 받는 디바이스의 [변경 로그](#)를 검토하는 것이 좋습니다.

왼쪽 탐색 모음에서 **Settings(설정) > Notification Settings(알림 설정)**를 클릭합니다.

디바이스 워크플로우에 대한 알림 전송



**Note** 이러한 설정을 변경하거나 알림을 수동으로 구독하려면 최고 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 [Cisco Defense Orchestrator의 사용자 역할](#)을 참조하십시오.

알림을 받을 디바이스 워크플로우 시나리오를 모두 선택해야 합니다. 다음 작업을 수동으로 확인합니다.

- 구축 - 이 작업은 하며, SSH 또는 IOS 디바이스에 대한 통합 인스턴스는 포함하지 않습니다.
- 백업 - 이 작업은 FDM 관리 디바이스에만 적용됩니다.
- 업그레이드 - 이 작업은 ASA 및 FDM 관리 디바이스에만 적용됩니다.
- **threat defense**를 클라우드로 마이그레이션 - 이 작업은 threat defense Device Manager를 Management Center에서 CDO로 변경할 때 적용됩니다.

디바이스 이벤트에 대한 알림 전송



**Note** 이러한 설정을 변경하거나 알림을 수동으로 구독하려면 최고 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 [Cisco Defense Orchestrator의 사용자 역할](#)을 참조하십시오.

알림을 받을 디바이스 워크플로우 시나리오를 모두 선택해야 합니다. 다음 작업을 수동으로 확인합니다.

- 오프라인 상태 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 온라인 재전환 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 충돌 탐지됨 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- **HA** 상태 변경됨 - 이 작업은 HA 또는 페일오버 쌍 내의 디바이스, 현재 상태 및 변경된 상태를 나타냅니다. 이 작업은 테넌트와 연결된 모든 HA 및 페일오버 구성에 적용됩니다.

- 사이트 간 세션 연결 끊김 - 이 작업은 테넌트에 구성된 모든 사이트 간 VPN 구성에 적용됩니다.

#### 백그라운드 로그 검색을 위해 알림 전송

이러한 설정을 변경하거나 알림을 수동으로 구독하려면 최고 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 [Cisco Defense Orchestrator의 사용자 역할](#)을 참조하십시오.


테넌트에 로그인한 사용자가 백그라운드 검색을 생성하면 알림을 받습니다. 알림을 받을 디바이스 워크플로우 시나리오를 모두 선택해야 합니다. 다음 작업을 수동으로 확인합니다.

- 검색 시작 - 검색이 시작되면 알림을 받습니다. 이는 즉시 검색 및 예약된 검색에 모두 적용됩니다.
- 검색 완료 - 검색이 종료되면 알림을 받습니다. 이는 즉시 검색 및 예약된 검색에 모두 적용됩니다.
- 검색 실패 - 검색이 실패하면 알림을 받습니다. 이는 즉시 검색 및 예약된 검색에 모두 적용됩니다. 매개변수 또는 쿼리를 확인하고 다시 시도하십시오.

#### 가입자

**Subscribe to receive alerts**(알림 수신 구독) 토글을 활성화하여 테넌트 로그인과 연결된 이메일을 알림 목록에 추가합니다. 메일링 리스트에서 이메일을 제거하려면 토글을 선택 취소하여 회색으로 표시합니다.


특정 사용자 역할은 이 설정 페이지의 구독 작업에 제한적으로 액세스할 수 있습니다. 최고 관리자 사용자 역할의 사용자는 이메일 항목을 추가하거나 제거할 수 있습니다. 자신이 아닌 다른 사람 또는

대체 이메일 연락처를 구독 중인 사용자 목록에 추가하려면  을 클릭하고 이메일을 수동으로 입력합니다.



**Warning** 사용자를 수동으로 추가하는 경우 올바른 이메일을 입력해야 합니다. CDO는 테넌트와 연결된 알려진 사용자에 대한 이메일 주소를 확인하지 않습니다.

#### CDO 알림 보기

알림  아이콘을 클릭하여 테넌트에서 발생한 최신 알림을 확인합니다. CDO의 알림은 30일 후에 알림 목록에서 제거됩니다.



**Note** **Send Alerts When**(알림 전송 시기) 섹션에서 선택한 사항은 CDO에 표시되는 알림 유형에 영향을 미칩니다.

## 서비스 통합

메시징 앱에서 수신 Webhook를 활성화하고 앱 대시보드에서 직접 CDO 알림을 수신합니다. CDO에서 이 옵션을 활성화하려면 선택한 앱에서 수신 Webhook를 수동으로 허용하고 Webhook URL을 검색해야 합니다. 자세한 내용은 [CDO 알림을 위한 서비스 통합 활성화](#)를 참조하십시오.

## CDO 알림을 위한 서비스 통합 활성화

서비스 통합을 활성화하여 지정된 메시징 애플리케이션 또는 서비스를 통해 CDO 알림을 전달합니다. 알림을 받으려면 메시지 프로그램에서 웹훅 URL을 생성하고 CDO의 **Notification Settings**(알림 설정) 페이지에서 해당 웹훅을 CDO에 지정해야 합니다.

CDO는 기본적으로 Cisco Webex 및 Slack을 서비스 통합으로 지원합니다. 이러한 서비스로 전송되는 메시지는 채널 및 자동화된 봇용으로 특별히 형식이 지정됩니다.



**참고** 알림 설정 페이지에서 선택한 **Notification Settings**(알림 설정)은 메시지 프로그램으로 전달되는 이벤티입니다.

## Webex Teams에 대해 수신 Webhook

### 시작하기 전에

CDO 알림은 지정된 작업 공간에 표시되거나 비공개 메시지에 자동 봇으로 표시됩니다. Webex Teams이 웹훅을 처리하는 방법에 대한 자세한 정보는 [개발자용 Webex](#)를 참조하십시오.

Webex Teams에 대해 수신 웹훅을 허용하려면 다음 절차를 따르십시오.

### 프로시저

- 단계 1 Webex Teams 응용프로그램을 엽니다.
- 단계 2 창의 왼쪽 하단에서 **Apps**(앱) 아이콘을 클릭합니다. 이 작업은 기본 브라우저의 새 탭에서 Cisco Webex App Hub를 엽니다.
- 단계 3 수신 웹훅을 찾으려면 검색창을 사용하세요.
- 단계 4 **Connect**(연결)을 선택합니다. 이 작업은 새 탭에서 애플리케이션을 허용하는 OAuth 인증을 엽니다.
- 단계 5 **Accept**(수락)을 선택합니다. 탭은 자동으로 애플리케이션의 구성 페이지로 리디렉션됩니다.
- 단계 6 다음을 구성합니다.
  - **Webhook** 이름 - 이 애플리케이션에서 제공하는 메시지를 식별하기 위한 이름을 입력합니다.
  - 공간 선택 - 드롭다운 메뉴를 사용하여 **Space**(공간)를 선택합니다. 공간이 이미 Webex 팀에 존재해야 합니다. 공간이 존재하지 않는 경우 Webex Teams에서 새 공간을 만들고 애플리케이션의 구성 페이지를 새로 고쳐 새 공간을 표시할 수 있습니다.
- 단계 7 **Add**(추가)를 선택합니다. 선택한 Webex Space는 애플리케이션이 추가되었다는 알림을 받게 됩니다.

- 단계 8 웹후크 URL을 복사합니다.
- 단계 9 CDO에 로그인합니다.
- 단계 10 왼쪽 탐색 모음에서 **Settings**(설정) > **Notification Settings**(알림 설정)를 클릭합니다.
- 단계 11 **Service Integrations**(서비스 통합)으로 스크롤합니다.
- 단계 12 파란색 플러스 버튼을 클릭합니다.
- 단계 13 **Name**(이름)을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.
- 단계 14 드롭다운 메뉴를 확장하고 **Webex**를 서비스 유형으로 선택합니다.
- 단계 15 서비스에서 생성한 웹후크 URL을 붙여넣습니다.
- 단계 16 OK(확인)를 클릭합니다.

## Slack용 수신 Webhook

CDO 알림은 지정된 채널에 표시되거나 비공개 메시지에 자동 봇으로 표시됩니다. Slack이 수신 웹후크를 처리하는 방법에 대한 자세한 내용은 [Slack 앱](#)을 참조하십시오.

Slack에 대해 수신 웹후크를 허용하려면 다음 절차를 따르십시오.

### 프로시저

- 단계 1 Slack계정에 로그인합니다.
- 단계 2 왼쪽 패널에서 아래로 스크롤하여 **Add Apps**(앱 추가)를 선택합니다.
- 단계 3 **Incoming Webhooks**(수신 웹후크)에 대한 애플리케이션 디렉토리를 검색하고 앱을 찾습니다. **Add**(추가)를 선택합니다.
- 단계 4 Slack 워크스페이스의 관리자가 아닌 경우, 조직의 관리자에게 요청을 보내고 앱이 계정에 추가될 때까지 기다려야 합니다. **Request Configuration**(요청 구성)을 선택합니다. 선택적 메시지를 입력하고 **Submit Request**(요청 제출)을 선택합니다.
- 단계 5 워크스페이스에 수신 웹후크 앱이 활성화되면 Slack 설정 페이지를 새로고침하고 **Add New Webhook to Workspace**(워크스페이스에 새 웹후크 추가)를 선택합니다.
- 단계 6 드롭다운 메뉴를 사용하여 CDO 알림을 표시할 Slack 채널을 선택합니다. **Authorize**(승인)을 선택합니다. 요청이 활성화되기를 기다리는 동안 이 페이지에서 다른 곳으로 이동하려면 Slack에 로그인하고 왼쪽 상단 모서리에서 작업 공간 이름을 선택하기만 하면 됩니다. 드롭다운 메뉴에서 **Customize Workspace**(작업 공간 사용자 지정)을 선택하고 **Configure Apps**(앱 구성)을 선택합니다. **Custom Integrations**(사용자 지정 통합) > **Manage**(관리)로 이동합니다. **Incoming Webhooks**(수신 웹후크)를 선택하여 앱의 랜딩 페이지를 연 다음 탭에서 **Configuration**(구성)을 선택합니다. 그러면 이 앱이 활성화된 작업 공간 내의 모든 사용자가 나열됩니다. 계정 구성만 보고 편집할 수 있습니다. 작업 공간 이름을 선택하여 구성을 편집하고 계속 진행합니다.
- 단계 7 Slack 설정 페이지는 앱의 구성 페이지로 리디렉션됩니다. 웹후크 URL을 찾아 복사합니다.
- 단계 8 CDO에 로그인합니다.
- 단계 9 왼쪽 탐색 모음에서 **Settings**(설정) > **Notification Settings**(알림 설정)를 클릭합니다.

- 단계 10 **Service Integrations**(서비스 통합)으로 스크롤합니다.
- 단계 11 파란색 플러스 버튼을 클릭합니다.
- 단계 12 **Name**(이름)을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.
- 단계 13 드롭다운 메뉴를 확장하고 서비스 유형으로 **Slack**을 선택합니다.
- 단계 14 서비스에서 생성한 웹후크 URL을 붙여넣습니다.
- 단계 15 **OK**(확인)를 클릭합니다.

## 사용자 지정 통합을 위한 수신 웹후크

### 시작하기 전에

CDO는 사용자 지정 통합을 위한 메시지 형식을 지정하지 않습니다. 사용자 지정 서비스 또는 애플리케이션을 통합하기로 선택한 경우 CDO는 JSON 메시지를 보냅니다.

수신 웹후크를 활성화하고 웹후크 URL을 생성하는 방법에 대한 서비스 설명서를 참조하십시오. 웹후크 URL이 있으면 아래 절차를 사용하여 웹후크를 활성화합니다.

### 프로시저

- 단계 1 선택한 사용자 지정 서비스 또는 애플리케이션에서 웹후크 URL을 생성하고 복사합니다.
- 단계 2 CDO에 로그인합니다.
- 단계 3 왼쪽 탐색 모음에서 **Settings**(설정) > **Notification Settings**(알림 설정)를 클릭합니다.
- 단계 4 **Service Integrations**(서비스 통합)으로 스크롤합니다.
- 단계 5 파란색 플러스 버튼을 클릭합니다.
- 단계 6 **Name**(이름)을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.
- 단계 7 드롭다운 메뉴를 확장하고 서비스 유형으로 **Custom**(사용자 지정)을 선택합니다.
- 단계 8 서비스에서 생성한 웹후크 URL을 붙여넣습니다.
- 단계 9 **OK**(확인)를 클릭합니다.

## 로깅 설정

월별 이벤트 로깅 한도와 한도가 재설정될 때까지 남은 일수를 확인합니다. 저장된 로깅은 Cisco cloud가 수신한 압축된 이벤트 데이터를 나타냅니다.

지난 12개월 동안 테넌트가 받은 모든 로깅을 보려면 **View Historical Usage**(기록 히스토리 보기)를 클릭합니다.

추가 스토리지를 요청하는 데 사용할 수 있는 링크도 있습니다.

## SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 통합

Cisco Defense Orchestrator(CDO)는 Cisco Secure Sign-On을 SAML Single Sign-On Identity Provider(IdP) 및 MFA(다단계 인증)용 Duo Security로 사용합니다. 이는 CDO의 기본 인증 방법입니다.

그러나 고객이 자신의 SAML SSO(Single Sign-On) IdP 솔루션을 CDO와 통합하려는 경우 IdP가 SAML 2.0 및 IdP(Identity Provider) 시작 워크플로를 지원하는 경우라면 가능합니다.

자체 SAML 솔루션을 CDO와 통합하려면 지원 부서에 문의하여 [케이스를 생성](#)해야 합니다. 지침은 [Cisco Secure Cloud Sign-On ID 제공자 통합 가이드](#)를 참조하십시오.



**Attention** 케이스를 열 때 요청이 올바른 팀에 전달되도록 **Manually Select A Technology**(수동으로 A 기술 선택)를 선택하고 **SecureX - Sign-on and Administration**(SecureX - 로그인 및 관리)을 선택했는지 확인합니다.

## SSO 인증서 갱신

ID 공급자(IdP)는 일반적으로 SecureX SSO와 통합됩니다. [Cisco TAC](#) 사례를 열고 metadata.xml 파일을 제공하십시오. 자세한 내용은 [Cisco SecureX Sign-On 타사 ID 제공자 통합 가이드](#)를 참조하십시오.



주의 사례를 열 때 기술 수동 선택을 선택하고 요청이 올바른 팀에 전달되도록 **SecureX - 로그인 및 관리**를 선택했는지 확인합니다.

(레거시만 해당) IdP(Identity Provider) 통합이 CDO와 직접 통합된 경우 [CDO 고객이 TAC로 지원 티켓을 여는 방법](#)을 열고 metadata.xml 파일을 제공하십시오.



참고 IdP를 CDO와 직접 통합하는 대신 SecureX SSO와 통합하는 것이 매우 좋습니다.

## API 토큰

개발자는 CDO REST API 호출을 할 때 CDO API 토큰을 사용합니다. 호출이 성공하려면 REST API 인증 헤더에 API 토큰을 삽입해야 합니다. API 토큰은 만료되지 않는 "장기" 액세스 토큰입니다. 그러나 이를 갱신하고 취소할 수 있습니다.

CDO 내에서 API 토큰을 생성할 수 있습니다. 이러한 토큰은 생성 직후 일반 설정 페이지가 열려 있는 동안에만 표시됩니다. CDO에서 다른 페이지를 열고 일반 설정 페이지로 돌아가면, 토큰이 분명히 발급되었지만 토큰이 더 이상 표시되지 않습니다.

개별 사용자는 특정 테넌트에 대한 자체 토큰을 생성할 수 있습니다. 사용자는 다른 사용자를 대신하여 토큰을 생성할 수 없습니다. 토큰은 계정-테넌트 쌍에 고유하며 다른 사용자-테넌트 조합에 사용할 수 없습니다.



## API 토큰 형식 및 클레임

API 토큰은 JSON 웹 토큰(JWT)입니다. JWT 토큰 형식에 대해 자세히 알아보려면 [JSON 웹 토큰 소개](#)를 읽어보십시오.

CDO API 토큰은 다음과 같은 클레임 집합을 제공합니다.

- **id** - 사용자/디바이스 uid
- **parentId** - 데넌트 uid
- **ver** - 공개 키의 버전(초기 버전은 0, 예, `cdo_jwt_sig_pub_key.0`)
- **subscriptions** - 보안 서비스 익스체인지 구독 (선택 사항)
- **client\_id** - "api-client"
- **jti** - 토큰 ID

## 토큰 관리

### API 토큰 생성

#### Procedure

- 단계 1 왼쪽 내비게이션 바에서 **Settings(설정) > General Settings(일반 설정)**를 클릭합니다.
- 단계 2 내 토큰에서 **Generate API Token(API 토큰 생성)**를 클릭합니다.
- 단계 3 민감한 데이터를 유지하기 위한 기업의 모범 사례에 따라 안전한 위치에 토큰을 저장하십시오.

### API 토큰 갱신

API 토큰은 만료되지 않습니다. 그러나 사용자는 토큰이 분실되거나 손상된 경우 또는 기업의 보안 지침을 준수하기 위해 API 토큰을 갱신하도록 선택할 수 있습니다.

#### Procedure

- 단계 1 왼쪽 탐색 모음에서 **Settings(설정) > General Settings(일반 설정)**를 클릭합니다.
- 단계 2 내 토큰에서 **Renew(갱신)**을 클릭합니다. CDO에서 새 토큰을 생성합니다.
- 단계 3 민감한 데이터를 유지하기 위한 기업의 모범 사례에 따라 안전한 위치에 새 토큰을 저장하십시오.

## API 토큰 취소

## Procedure

단계 1 왼쪽 내비게이션 바에서 **Settings(설정) > General Settings(일반 설정)**를 클릭합니다.

단계 2 내 토큰에서 **Revoke(취소)**를 클릭합니다. CDO는 토큰을 취소합니다.

## ID 제공자 계정과 Cisco Defense Orchestrator 사용자 레코드 간의 관계

Cisco Defense Orchestrator(CDO)에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 CDO의 사용자 레코드가 있는 계정이 필요합니다. IdP 어카운트에는 사용자의 자격 증명도 포함되며 IdP는 이러한 자격 증명을 기반으로 사용자를 인증합니다. 다단계 인증은 ID 보안의 추가 레이어를 제공합니다. CDO 사용자 레코드에는 주로 사용자 이름, 연결된 CDO 테넌트 및 사용자의 역할이 포함됩니다. 사용자가 로그인하면 CDO는 IdP의 사용자 ID를 CDO의 테넌트에 있는 기존 사용자 레코드에 매핑하려고 시도합니다. CDO가 일치하는 항목을 찾으면 사용자는 해당 테넌트에 로그인됩니다.

엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. Cisco Secure Cloud Sign-On은 다단계 인증에 Duo를 사용합니다. 고객은 원하는 경우 [SAML SSO\(Single Sign-On\)](#)를 [Cisco Defense Orchestrator](#)와 통합할 수 있습니다.

### 로그인 워크플로우

다음은 IdP 계정이 CDO 사용자 레코드와 상호 작용하여 CDO 사용자에게 로그인하는 방법에 대한 간략한 설명입니다.

## Procedure

단계 1 사용자는 인증을 위해 Cisco Secure Cloud Sign-On(<https://sign-on.security.cisco.com>)과 같은 SAML 2.0 호환 ID 공급자(IdP)에 로그인하여 CDO에 대한 액세스를 요청합니다.

단계 2 IdP는 사용자가 인증되었다는 SAML 어설션을 발행하고 포털은 <https://defenseorchestrator.com> 또는 <https://defenseorchestrator.eu> 또는 <https://www.apj.cdo.cisco.com/>를 나타내는 타일과 같이 사용자가 액세스할 수 있는 애플리케이션을 표시합니다.

단계 3 CDO는 SAML 어설션의 유효성을 검사하고 사용자 이름을 추출한 다음 테넌트 중에서 해당 사용자 이름에 해당하는 사용자 레코드를 찾으려고 시도합니다.

- 사용자가 CDO의 단일 테넌트에 대한 사용자 레코드를 가지고 있는 경우 CDO는 사용자에게 테넌트에 대한 액세스 권한을 부여하고 사용자의 역할에 따라 수행할 수 있는 작업이 결정됩니다.
- 사용자가 두 개 이상의 테넌트에 대한 사용자 레코드를 가지고 있는 경우 CDO는 인증된 사용자에게 선택할 수 있는 테넌트 목록을 제공합니다. 사용자는 테넌트를 선택하고 해당 테넌트에 액세스할 수 있습니다. 특정 테넌트에 대한 사용자의 역할에 따라 수행할 수 있는 작업이 결정됩니다.

- CDO에 인증된 사용자와 테넌트의 사용자 레코드에 대한 매핑이 없는 경우 CDO는 사용자에게 CDO에 대해 자세히 알아보거나 무료 평가판을 요청할 수 있는 기회를 제공하는 랜딩 페이지를 표시합니다.

CDO에 사용자 레코드를 생성해도 IdP에 계정이 생성되지 않고 IdP에 계정을 생성해도 CDO에 사용자 레코드가 생성되지 않습니다.

마찬가지로 IdP에서 계정을 삭제한다고 해서 CDO에서 사용자 기록을 삭제한 것은 아닙니다. 그러나 IdP 계정이 없는 경우 사용자를 CDO에 인증할 방법이 없습니다. CDO 사용자 기록을 삭제한다고 해서 IdP 계정이 삭제된 것은 아닙니다. 그러나 CDO 사용자 레코드가 없는 경우 인증된 사용자가 CDO 테넌트에 액세스할 수 있는 방법이 없습니다.

## 이 아키텍처의 의미

### Cisco Security Cloud 로그인을 사용하는 고객

CDO의 Cisco Secure Cloud Sign-On ID 공급자를 사용하는 고객의 경우 슈퍼 관리자는 CDO에 사용자 레코드를 생성할 수 있으며 사용자는 CDO에 자체 등록할 수 있습니다. 두 사용자 이름이 일치하고 사용자가 올바르게 인증된 경우 사용자는 CDO에 로그인할 수 있습니다.

슈퍼 관리자가 사용자가 CDO에 액세스하지 못하도록 해야 하는 경우 CDO 사용자의 사용자 레코드를 간단히 삭제할 수 있습니다. Cisco Secure Cloud Sign-On 계정은 여전히 존재하며 슈퍼 관리자가 사용자를 복원하려는 경우 Cisco Secure Cloud Sign-On에 사용된 것과 동일한 사용자 이름으로 새 CDO 사용자 레코드를 생성하면 됩니다.

고객이 기술 지원 센터(TAC)에 전화해야 하는 CDO 문제에 직면한 경우 고객은 TAC 엔지니어를 위한 사용자 레코드를 생성하여 테넌트를 조사하고 정보와 제안을 고객에게 다시 보고할 수 있습니다.

### 자체 ID 공급자가 있는 고객

[SAML SSO\(Single Sign-On\)](#)를 [Cisco Defense Orchestrator와 통합](#)의 경우 ID 공급자 계정과 CDO 테넌트를 모두 제어합니다. 이러한 고객은 CDO에서 ID 공급자 계정 및 사용자 레코드를 만들고 관리할 수 있습니다.

사용자가 CDO에 액세스하지 못하도록 해야 하는 경우, IdP 계정, CDO 사용자 레코드 또는 둘 다를 삭제할 수 있습니다.

Cisco TAC의 도움이 필요한 경우, TAC 엔지니어를 위해 읽기 전용 역할이 있는 ID 공급자 계정과 CDO 사용자 레코드를 모두 생성할 수 있습니다. 그런 다음 TAC 엔지니어는 고객의 CDO 테넌트에 액세스하여 조사하고 고객에게 정보와 제안을 보고할 수 있습니다.<sup>3</sup>

### Cisco Managed Service 제공자

Cisco MSP(Managed Service Provider)가 CDO의 Cisco Secure Cloud Sign-On IdP를 사용하는 경우 Cisco Secure Cloud Sign-On에 자체 등록할 수 있으며 고객은 MSP가 고객의 테넌트를 관리할 수 있도록 CDO에 사용자 레코드를 생성할 수 있습니다. 물론 고객은 원할 때 MSP의 레코드를 삭제할 수 있는 모든 권한을 가집니다.

## 관련 주제

- [일반 설정](#)
- [사용자 관리](#)
- [Cisco Defense Orchestrator의 사용자 역할](#)

## 멀티 테넌트 포털 관리

CDO 다중 테넌트 포털 보기는 여러 테넌트의 모든 디바이스에서 정보를 검색하고 표시합니다. 이 다중 테넌트 포털은 디바이스 상태, 디바이스에서 실행 중인 소프트웨어 버전 등을 보여줍니다.



**Note** 다중 테넌트 포털에서 여러 지역에 걸쳐 테넌트를 추가하고 해당 테넌트가 관리하는 디바이스를 볼 수 있습니다. 다중 테넌트 포털에서 테넌트를 편집하거나 디바이스를 구성할 수 없습니다.

### 시작하기 전에

다중 테넌트 포털은 해당 기능이 테넌트에서 활성화된 경우에만 사용할 수 있습니다. 테넌트에 대해 다중 테넌트 포털을 활성화하려면 Cisco TAC에서 지원 티켓을 여십시오. 지원 티켓이 해결되고 포털이 생성되면 포털에서 최고 관리자 역할을 가진 사용자는 여기에 테넌트를 추가할 수 있습니다.

발생할 수 있는 특정 브라우저 관련 문제를 방지하려면 웹 브라우저에서 캐시와 쿠키를 지우는 것이 좋습니다.

### 멀티 테넌트 포털

포털은 다음 메뉴를 제공합니다.

- **디바이스:**
  - 포털에 추가된 테넌트에 있는 모든 디바이스를 표시합니다. 필터 및 검색 필드를 사용하여 보려는 디바이스를 검색합니다. 디바이스를 클릭하여 상태, 온보딩 방법, 방화벽 모드, 파일 오버 모드, 소프트웨어 버전 등을 볼 수 있습니다.
  - 인터페이스는 테이블에서 볼 디바이스 속성을 선택하거나 지울 수 있는 열 선택기 를 제공합니다. 'AnyConnect 원격 액세스 VPN'을 제외하고 다른 모든 디바이스 속성은 기본으로 선택됩니다. 테이블을 사용자 정의하면 CDO는 다음에 CDO에 로그인할 때 선택 사항을 기억합니다.
  - 디바이스를 클릭하면 오른쪽에서 세부 정보를 볼 수 있습니다.
  - 포털 정보를 쉼표로 구분된 값(csv) 파일로 내보낼 수 있습니다. 이 정보는 디바이스를 분석하거나 액세스 권한이 없는 사람에게 보내는 데 도움이 됩니다. 데이터를 내보낼 때마다 CDO는 새 .csv 파일을 생성합니다. 생성된 파일에는 이름에 날짜와 시간이 포함되어 있습니다.

- 디바이스를 관리하는 CDO 테넌트에서만 디바이스를 관리할 수 있습니다. 다중 테넌트 포털은 CDO 테넌트 페이지로 연결되는 장치 관리 링크를 제공합니다. 해당 테넌트에 대한 계정이 있고 테넌트가 포털과 동일한 지역에 있는 경우 디바이스에 이 링크가 표시됩니다. 테넌트에 액세스할 수 있는 권한이 없는 경우 디바이스 관리 링크가 표시되지 않습니다. 권한을 얻기 위해 조직의 슈퍼 관리자에게 문의할 수 있습니다.



#### Note

디바이스를 관리하는 테넌트가 다른 지역에 있는 경우 해당 지역의 CDO에 로그인할 수 있는 링크가 표시됩니다. 해당 지역의 CDO 또는 해당 지역의 테넌트에 액세스할 수 없는 경우 디바이스를 관리할 수 없습니다.

Name	Type	Region	Version	Hardware Version	Configuration	Connectivity State
52.53.207.153	ASA	Europe	9.8(3)18	ASAv (V01)	Synced	Online
Acton	Unknown	North America	16.03.07	CSR1000v	Synced	Online
Amsterdam	ASA	North America	9.13(1)7	ASAv (V01)	Synced	Online
Ayer	FTD	North America	6.4.0-44	Cisco Firepower Threat Defe	Synced	Online
Baltimore	ASA	North America	9.9(2)	ASAv (V01)	Synced	Online
Burak-crush-APJC	ASA Model	Asia-Pacific & Japan	9.1(5)		Synced	Online

- 테넌트:
  - 포털에 추가된 테넌트를 표시합니다.
  - 이를 통해 슈퍼 관리자는 포털에 테넌트를 추가할 수 있습니다.
  - 를 클릭하면 CDO 테넌트의 메인 페이지를 볼 수 있습니다.

## 멀티 테넌트 포털에 테넌트 추가

슈퍼 관리자 역할이 있는 사용자는 포털에 테넌트를 추가할 수 있습니다. 여러 지역에 걸쳐 테넌트를 추가할 수 있습니다. 예를 들어 유럽 지역의 테넌트를 미국 지역에 추가하거나 그 반대로 추가할 수 있습니다.



#### Important


테넌트에 대한 [API 전용 사용자 생성](#) 하고 CDO 인증을 위한 API 토큰을 생성하는 것이 좋습니다.



#### Note

포털에 여러 테넌트를 추가하려면 각 테넌트에서 API 토큰을 생성하고 텍스트 파일에 붙여넣습니다. 그런 다음 토큰을 생성하기 위해 매번 테넌트로 전환하지 않고도 포털에 테넌트를 차례로 쉽게 추가할 수 있습니다.

### Procedure

- 단계 1 왼쪽 내비게이션 바에서 **Settings(설정) > General Settings(일반 설정) > My Tokens(내 토큰)**를 클릭합니다.
- 단계 2 **Generate API Token(API 토큰 생성)**을 클릭한 다음 복사합니다.
- 단계 3 포털로 이동하여 **Tenants(테넌트)** 탭을 클릭합니다.
- 단계 4 오른쪽에  테넌트 추가 버튼을 클릭합니다.
- 단계 5 토큰을 붙여넣고 **Save(저장)**를 클릭합니다.

## 멀티 테넌트 포털에서 테넌트 삭제

### Procedure

- 단계 1 포털로 이동하여 **Tenants(테넌트)** 탭을 클릭합니다.
- 단계 2 오른쪽에 나타나는 해당 삭제 아이콘을 클릭하여 원하는 테넌트를 제거합니다.
- 단계 3 **Remove(제거)**를 클릭합니다. 연결된 디바이스도 포털에서 제거됩니다.

## 관리-테넌트 포털 설정

Cisco Defense Orchestrator(Defense Orchestrator)는 설정 페이지에서 다중 테넌트 포털 및 개별 사용자 계정의 특정 측면을 사용자 지정할 수 있는 기능을 제공합니다. 왼쪽 탐색 모음에서 **Settings(설정)**를 클릭하여 설정 페이지에 액세스합니다.

### 설정

#### General Settings(일반 설정)

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

웹 분석은 기본적으로 활성화됩니다. 웹 분석을 비활성화하거나 나중에 활성화하려면 다음 절차를 따르십시오.

1. CDO 대시보드 왼쪽의 내비게이션 바에서 **Settings(설정)**를 클릭합니다.
2. **General Settings(일반 설정)**를 클릭합니다.
3. 웹 분석 아래의 슬라이더를 클릭합니다.

사용자 관리

**User Management**(사용자 관리) 화면에서 다중 테넌트 포털과 연결된 모든 사용자 레코드를 볼 수 있습니다. 사용자 계정을 추가, 편집 또는 삭제할 수 있습니다. 자세한 내용은 User [사용자 관리](#)를 참조하십시오.

## 테넌트 전환

포털 테넌트가 둘 이상인 경우 CDO에서 로그아웃하지 않고 다른 포털 또는 테넌트 간에 전환할 수 있습니다.

### Procedure

단계 1 다중 테넌트 포털에서 오른쪽 상단 모서리에 나타나는 테넌트 메뉴를 클릭합니다.

단계 2 **Switch tenant**(테넌트 전환)를 클릭합니다.

단계 3 보려는 포털 또는 테넌트를 선택합니다.

## Cisco Success Network

Cisco Success Network는 사용자가 활성화하는 클라우드 서비스입니다. Cisco Success Network를 활성화하면 디바이스와 Cisco cloud간에 보안 연결이 설정되어 사용 정보 및 통계를 스트리밍합니다. 스트리밍 원격 측정은 디바이스에서 관심 있는 데이터를 선택하고 구조화된 형식으로 원격 관리 스테이션에 전송하는 메커니즘을 제공하여 다음과 같은 이점을 제공합니다.

- 네트워크에서 제품의 효율성을 향상시킬 수 있는 활용 가능한 미사용 기능을 알려줍니다.
- 제품에 사용할 수 있는 추가 기술 지원 서비스 및 모니터링에 대해 알려줍니다.
- Cisco가 제품을 개선할 수 있습니다.

디바이스는 항상 보안 연결을 설정하고 유지하며 Cisco Success Network에 등록할 수 있습니다. 디바이스를 등록하고 나면 Cisco Success Network 설정을 변경할 수 있습니다.



- 참고
- 위협 방어 고가용성 쌍의 경우 활성 디바이스 선택이 대기 디바이스의 Cisco Success Network 설정을 오버라이드합니다.
  - CDO는 Cisco Success Network 설정을 관리하지 않습니다. Firewall Device Manager 사용자 인터페이스를 통해 관리되는 설정 및 원격 분석 정보가 제공됩니다.

### Cisco Success Network 활성화 또는 비활성화

초기 시스템 설정 중에 Cisco Smart Software Manager에 디바이스를 등록하라는 메시지가 표시됩니다. 90일 평가 라이선스를 대신 선택한 경우에는 평가 기간이 종료되기 전에 디바이스를 등록해야 합니다. 디바이스를 등록하려면 Cisco Smart Software Manager(Smart Licensing 페이지)에 디바이스를 등록하거나 등록 키를 입력하여 CDO에 등록합니다.

디바이스를 등록할 때는 가상 어카운트가 디바이스에 라이선스를 할당합니다. 디바이스를 등록하면 활성화한 선택 가능한 라이선스도 등록됩니다.

Firewall Device Manager UI를 통해서만 이 옵션을 비활성화할 수 있지만 Cisco Success Network를 비활성화하여 언제든지 이 연결을 끌 수 있습니다. 비활성화하면 클라우드에서 디바이스의 연결이 끊어집니다. 연결 해제는 업데이트 수신 또는 스마트 라이선싱 기능 작동에 영향을 주지 않으므로 이러한 기능은 계속 정상적으로 작동됩니다. 자세한 내용은 [Firepower 디바이스 매니저 구성 가이드](#), 버전 6.4.0+에서 시스템 관리 창의 **Cisco Success Network**에 연결 섹션을 참조하십시오.

## 사용자 관리

CDO에서 사용자 레코드를 생성하거나 수정하기 전에 [ID 제공자 계정과 Cisco Defense Orchestrator 사용자 레코드 간의 관계](#)를 읽고 IdP(Identity Provider) 계정과 사용자 레코드의 상호 작용 방식을 확인하십시오. CDO사용자는 인증을 받고 CDO테넌트에 액세스할 수 있도록 CDO레코드 및 해당 IdP 계정이 필요합니다.

엔터프라이즈에 자체 IdP가 없는 경우 Cisco Secure Sign-On은 모든 CDO 테넌트에 대한 ID 제공자입니다. 이 문서의 나머지 부분에서는 Cisco Secure Sign-On을 ID 제공자로 사용한다고 가정합니다.

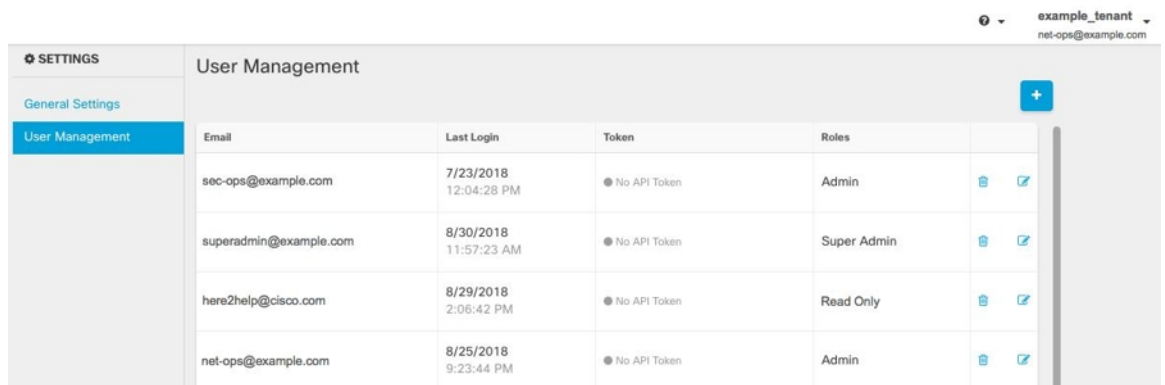
**User Management**(사용자 관리) 화면에서 테넌트와 연결된 모든 사용자 레코드를 볼 수 있습니다. 여기에는 지원 티켓을 해결하기 위해 사용자 어카운트와 일시적으로 연결된 모든 Cisco 지원 엔지니어가 포함됩니다.

## 테넌트와 연결된 사용자 기록 보기

프로시저

단계 1 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

단계 2 **User Management**(사용자 관리)를 클릭합니다.



Email	Last Login	Token	Roles
sec-ops@example.com	7/23/2018 12:04:28 PM	No API Token	Admin
superadmin@example.com	8/30/2018 11:57:23 AM	No API Token	Super Admin
here2help@cisco.com	8/29/2018 2:06:42 PM	No API Token	Read Only
net-ops@example.com	8/25/2018 9:23:44 PM	No API Token	Admin



참고 Cisco 지원이 테넌트에 액세스하지 못하도록 하려면, [일반 설정](#) 페이지에서 계정 설정을 구성합니다.

## 사용자 관리의 Active Directory 그룹

대량의 사용자에 대해 회전율이 높은 테넌트의 경우 개별 사용자를 CDO에 추가하는 대신 CDO를 AD(Active Directory) 그룹에 매핑하여 사용자 목록 및 사용자 역할을 더 쉽게 관리할 수 있습니다. 새 사용자 추가 또는 기존 사용자 제거와 같은 모든 사용자 변경은 이제 Active Directory에서 수행할 수 있으며 더 이상 CDO에서 수행할 필요가 없습니다.

사용자 관리 페이지에서 AD 그룹을 추가, 편집 또는 삭제하려면 **SuperAdmin** 사용자 역할이 있어야 합니다. 자세한 내용은 [Cisco Defense Orchestrator의 사용자 역할](#)을 참조하십시오.

### Active Directory 그룹 탭

**Settings(설정)** 페이지의 사용자 관리 섹션에는 현재 CDO에 매핑된 Active Directory 그룹에 대한 탭이 있습니다. 가장 중요한 것은 이 페이지에 AD 관리자에서 할당된 AD 그룹의 역할이 표시된다는 것입니다.

AD 그룹 내의 사용자는 Active Directory 그룹 탭이나 사용자 탭에 개별적으로 나열되지 않습니다.

### 감사 로그 탭

**Settings(설정)** 페이지의 User Management(사용자 관리) 섹션에는 Audit Logs(감사 로그) 탭이 있습니다. 이 새 섹션에는 CDO 테넌트에 액세스한 모든 사용자의 마지막 로그인 시간과 마지막 로그인 시간에 각 사용자가 보유한 역할이 표시됩니다. 여기에는 명시적 사용자 로그인과 AD 그룹 로그인이 모두 포함됩니다.

### 다중 역할 사용자

CDO의 IAM 기능에 따른 확장으로 이제 사용자가 여러 역할을 가질 수 있습니다.

사용자는 AD에서 여러 그룹의 일부가 될 수 있으며 각 그룹은 서로 다른 CDO 역할로 CDO에서 정의될 수 있습니다. 로그인 시 사용자가 얻는 최종 권한은 사용자가 속한 CDO에 정의된 모든 AD 그룹의 역할 조합입니다. 예를 들어 사용자가 두 개의 AD 그룹에 속해 있고 두 그룹이 편집 전용 및 배포 전용과 같은 두 가지 다른 역할로 CDO에 추가된 경우, 사용자는 편집 전용 및 배포 전용 권한을 모두 보유하게 됩니다. 이는 여러 그룹 및 역할에 적용됩니다.

AD 그룹 매핑은 CDO에서 한 번만 정의하면 되며, 이후에 다른 그룹 간에 사용자를 추가, 제거 또는 이동하여 사용자에 대한 액세스 및 권한 관리를 AD에서만 독점적으로 수행할 수 있습니다.



참고 사용자가 개별 사용자이자 동일한 테넌트에 있는 AD 그룹의 일부인 경우 개별 사용자의 사용자 역할이 AD 그룹의 사용자 역할을 오버라이드합니다.

## 시작하기 전에

사용자 관리의 형태로 CDO에 AD 그룹 매핑을 추가하기 전에 AD가 SecureX와 통합되어 있어야 합니다. AD ID 공급자(IdP)가 아직 통합되지 않은 경우 다음 작업을 수행해야 합니다.

1. Cisco TAC로 [지원 사례](#)를 열고 다음 정보와 함께 사용자 지정 AD IdP 통합을 요청하십시오.

- CDO 테넌트 이름 및 지역.
- 사용자 지정 라우팅을 정의할 도메인(예: @cisco.com, @myenterprise.com).
- XML 형식의 인증서 및 페더레이션 메타데이터.

2. AD에 다음 사용자 지정 SAML 클레임을 추가합니다. 이 값은 대소문자를 구분합니다.

- **SamlADUserGroupIds** - 이 속성은 사용자가 AD에 가지고 있는 모든 그룹 연결을 설명합니다. 예를 들어 Azure에서 아래 스크린샷과 같이 + **Add a group claim**(+ 그룹 클레임 추가)를 선택합니다.

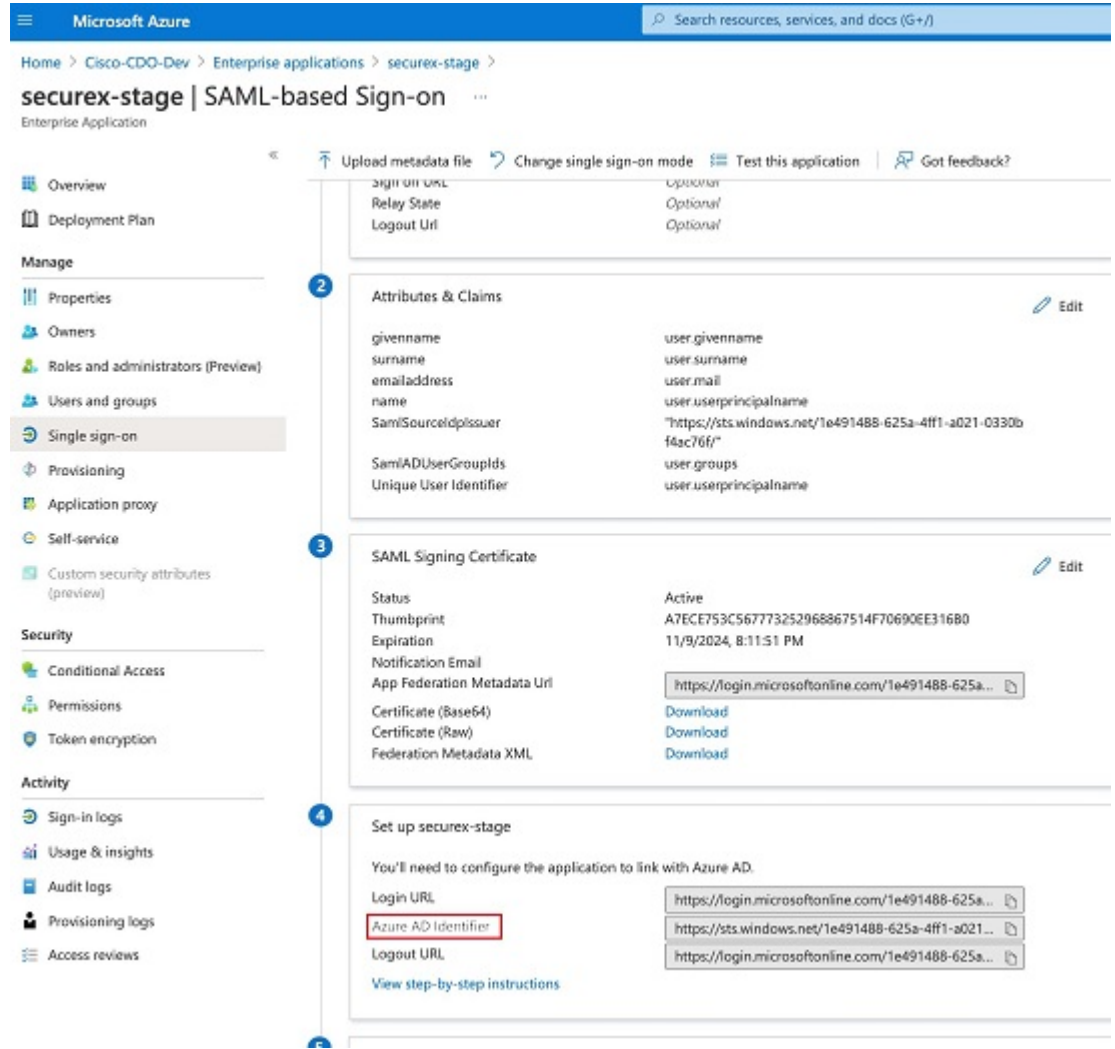
그룹 **3: Active Directory**에 정의된 사용자 지정 클레임

The screenshot shows the 'Attributes & Claims' configuration page in the Azure portal. It displays a table of claims under the 'Additional claims' section. Two claims are highlighted with red boxes:

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname
<b>SamlADUserGroupIds</b>	user.groups
<b>SamlSourceIdpIssuer</b>	"https://sts.windows.net/1e491488-..."

- **SamlSourceIdpIssuer** - 이 특성은 AD 인스턴스를 고유하게 식별합니다. 예를 들어 Azure에서 + **Add a group claim**(+ 그룹 클레임 추가)를 선택하고 스크롤하여 아래 스크린샷과 같이 Azure AD 식별자를 찾습니다.

그림 4: Azure Active Directory 식별자 찾기



## 사용자 관리를 위한 **Active Directory** 그룹 추가

프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
- 단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.
- 단계 4 테이블 상단에서 **Active Directory Groups**(활동 디렉토리 그룹) 탭을 선택합니다.
- 단계 5 현재 AD 그룹이 없는 경우 **Add AD group**(AD 그룹 추가)를 클릭합니다. 기존 항목이 있으면 Add(추가) 버튼을 클릭합니다.

단계 6 다음 정보를 입력합니다.

- 그룹 이름 - 고유한 이름을 입력합니다. 이 이름은 AD의 그룹 이름과 일치하지 않아도 됩니다. CDO에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- 그룹 ID - AD에서 그룹 ID를 수동으로 입력합니다. 그룹 ID의 값은 사용자 지정 클레임 정의의 그룹 ID와 동일해야 합니다. 그룹의 고유 ID에 해당하는 모든 값(예: my-favorite-group, 12345 등)이 될 수 있습니다.
- AD 발급자 - AD에서 AD 발급자 값을 수동으로 입력합니다.
- 역할 - 이 AD 그룹에 포함된 모든 사용자의 역할을 결정합니다. 자세한 내용은 사용자 역할을 참조하십시오.
- (선택 사항) 참고 - 이 AD 그룹에 적용 가능한 참고를 추가합니다.

단계 7 **OK**(확인)를 선택합니다.

## 사용자 관리를 위한 Active Directory 그룹 편집

시작하기 전에

CDO에서 AD 그룹의 사용자 관리를 편집하면 CDO가 AD 그룹을 제한하는 방식만 편집할 수 있습니다. CDO에서 AD 그룹 자체를 편집할 수 없습니다. AD 그룹 내의 사용자 목록을 편집하려면 AD를 사용하여 합니다.

프로시저

단계 1 CDO에 로그인합니다.

단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.

단계 4 테이블 상단에서 **Active Directory Groups**(활동 디렉토리 그룹) 탭을 선택합니다.

단계 5 편집할 AD 그룹을 식별하고 **Edit**(편집) 아이콘을 선택합니다.

단계 6 다음 값을 편집합니다.

- 그룹 이름 - 고유한 이름을 입력합니다. CDO에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- 그룹 ID - AD에서 그룹 ID를 수동으로 입력합니다. 그룹 ID의 값은 사용자 지정 클레임 정의의 그룹 ID와 동일해야 합니다. 그룹의 고유 ID에 해당하는 모든 값(예: my-favorite-group, 12345 등)이 될 수 있습니다.
- AD 발급자 - AD에서 AD 발급자 값을 수동으로 입력합니다.

- 역할 - 이 AD 그룹에 포함된 모든 사용자의 역할을 결정합니다. 자세한 내용은 사용자 역할을 참조하십시오.
- 참고 - 이 AD 그룹에 적용 가능한 참고를 추가합니다.

## 사용자 관리를 위한 **Active Directory** 그룹 삭제

프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
- 단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.
- 단계 4 테이블 상단에서 **Active Directory Groups**(활동 디렉토리 그룹) 탭을 선택합니다.
- 단계 5 삭제할 AD 그룹을 식별합니다.
- 단계 6 **Delete**(삭제) 아이콘을 선택합니다.
- 단계 7 **OK**(확인)를 클릭하여 AD 그룹 삭제를 확인합니다.

## 새 **CDO** 사용자 생성

새 CDO 사용자를 생성하려면 이 두 가지 작업이 필요합니다. 순차적으로 수행할 필요는 없습니다.

- 새 사용자를 위해 [Cisco Secure Cloud Sign On 계정 생성](#)
- [CDO 사용자 이름으로 CDO 사용자 레코드 생성](#)

이러한 작업이 완료되면 사용자는 [새 사용자가 Cisco Secure Sign-On 대시보드에서 CDO 열기](#)

## 새 사용자를 위해 **Cisco Secure Cloud Sign On** 계정 생성

Cisco Secure Cloud Sign-on 계정 생성은 새 사용자가 언제든지 수행할 수 있습니다. 사용자는 할당될 테넌트의 이름을 알 필요가 없습니다.

### CDO에 로그인 정보

Cisco Defense Orchestrator(CDO)는 Cisco Secure Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo를 사용합니다. CDO에 로그인하려면 먼저 **Cisco Security Cloud Sign On**에서 계정을 생성하고 **Duo**를 사용하여 **MFA**를 구성해야 합니다.

CDO에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.



**Important** 2019년 10월 14일 이전에 CDO 테넌트가 존재했다면 이 문서 대신 [Cisco Secure Cloud Sign On ID 제 공자로 마이그레이션](#), on page 41를 사용하여 로그인 지침을 사용합니다.

## 로그인하기 전에



**DUO Security** 설치. 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 [Duo 이중 인증 가이드: 등록 가이드](#)를 참고하십시오.

시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.

## 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성

초기 로그인 워크플로우는 4단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

### Procedure

#### 단계 1 새 Cisco Secure Cloud Sign-On 계정 등록

- a. <https://sign-on.security.cisco.com>으로 이동합니다.
- b. Sign In(로그인) 화면 하단에서 **Sign up**(등록)를 클릭합니다.

# Security Cloud Sign On

Formerly known as SecureX Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

- c. 계정 생성 상자의 필드를 채우십시오.

# Account Sign Up

Provide following information to create enterprise account.

[Back to login page](#)

Email \*

First name \*

Last name \*

Country \*

Password \*

Confirm Password \*

I agree to the [End User License Agreement and Privacy Statement](#).

Sign up

[Cancel](#)

다음은 몇 가지 팁입니다.

- **Email**(이메일) - CDO에 로그인하는 데 사용할 이메일 주소를 입력합니다.
- **암호** - 강력한 암호를 입력하십시오.

**d. Create Account**(계정 생성)를 클릭한 후.

Cisco는 등록된 주소로 확인 이메일을 보냅니다. 이메일을 열고 어카운트 활성화를 클릭합니다.

## 단계 2 Duo를 통한 다단계 인증 설정

다단계 인증을 설정할 때는 모바일 디바이스를 사용하는 것이 좋습니다.



- a. **Set up multi-factor authentication**(다단계 인증 설정) 화면에서 **Configure factor**(요인 구성)를 클릭합니다.
- b. **Start setup**(설정 시작)을 클릭하고 프롬프트에 따라 모바일 디바이스를 선택하고 해당 모바일 디바이스와 어카운트의 페어링을 확인합니다.

자세한 내용은 [Duo Guide to Two Factor Authentication: Enrollment Guide](#)를 참조하십시오. 디바이스에 이미 Duo 앱이 있는 경우 이 어카운트에 대한 활성화 코드를 받게 됩니다. Duo는 하나의 디바이스에서 여러 계정을 지원합니다.

- c. 마법사가 끝나면 **Continue to Login**(계속 로그인)를 클릭합니다.
- d. 2단계 인증을 사용하여 Cisco Secure Cloud Sign-On에 로그인합니다.

### 단계 3 (선택 사항) Google OTP를 추가 인증자로 설정

- a. Google Authenticator와 페어링할 모바일 디바이스를 선택하고 **Next**(다음)를 클릭합니다.
- b. 설정 마법사의 프롬프트에 따라 Google 인증기를 설정합니다.

### 단계 4 Cisco Secure Sign-On 어카운트에 대한 어카운트 복구 옵션 구성

- a. SMS를 사용하여 계정을 재설정하려면 복원 전화번호를 선택합니다.
- b. 보안 이미지를 선택합니다.
- c. **Create My Account**(내 계정 생성)를 클릭합니다. 이제 CDO 앱 타일이 있는 Cisco Security Sign-On 대시보드가 표시됩니다. 다른 앱 타일도 표시될 수 있습니다.

**Tip**

대시보드에서 타일을 끌어 원하는 대로 정렬하고, 탭을 생성하여 타일을 그룹화하고, 탭의 이

## CDO 사용자 이름으로 CDO 사용자 레코드 생성

"슈퍼 관리자" 권한이 있는 CDO 사용자만 CDO 사용자 레코드를 생성할 수 있습니다. 슈퍼 관리자는 위의 **Create Your CDO Username**(CDO 사용자 이름 생성) 작업에서 지정한 것과 동일한 이메일 주소로 사용자 레코드를 만들어야 합니다.


적절한 사용자 역할이 있는 사용자 레코드를 생성하려면 다음 절차를 수행합니다.

### Procedure

단계 1 CDO에 로그인합니다.

단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.

단계 4 파란색 더하기  버튼을 클릭하여 새 사용자를 테넌트에 추가합니다.

단계 5 사용자의 이메일 주소를 입력합니다.

**Note**      사용자의 이메일 주소는 Cisco Secure Log-On 계정의 이메일 주소와 일치해야 합니다.

단계 6 드롭다운 메뉴에서 사용자 **Cisco Defense Orchestrator**의 사용자 역할을 선택합니다.

단계 7 **OK**(확인)를 클릭합니다.

## 새 사용자가 Cisco Secure Sign-On 대시보드에서 CDO 열기

### Procedure

단계 1 Cisco Secure Sign-on 대시보드에서 적절한 **CDO** 타일을 클릭합니다. **CDO** 타일은 <https://defenseorchestrator.com>으로 안내하고 **CDO(EU)** 타일은 <https://defenseorchestrator.eu>로 안내합니다.

단계 2 두 인증자를 모두 설정한 경우 인증자 로고를 클릭하여 Duo Security 또는 Google Authenticator를 선택합니다.

- 기존 테넌트에 사용자 레코드가 이미 있는 경우 해당 테넌트에 로그인됩니다.
- 이미 여러 포털에 사용자 레코드가 있는 경우 연결할 포털을 선택할 수 있습니다.
- 여러 테넌트에 대한 사용자 레코드가 이미 있는 경우 연결할 CDO 테넌트를 선택할 수 있습니다.
- 기존 테넌트에 대한 사용자 레코드가 아직 없는 경우 CDO에 대해 자세히 알아보거나 평가판 테넌트를 요청할 수 있습니다.

포털 보기는 여러 테넌트에서 통합된 정보를 검색하고 표시합니다. 자세한 내용은 [멀티 테넌트 포털 관리](#)를 참조하십시오.

테넌트 보기에는 사용자 레코드가 있는 여러 테넌트가 표시됩니다.



## Cisco Defense Orchestrator의 사용자 역할

Cisco Defense Orchestrator(CDO)에는 읽기 전용, 편집 전용, 구축 전용, 관리자, 슈퍼 관리자 등 다양한 사용자 역할이 있습니다. 사용자 역할은 각 테넌트의 각 사용자에 대해 구성됩니다. CDO 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우, 사용자 ID는 동일하지만 테넌트마다 역할이 다를 수 있습니다. 사용자는 한 테넌트에 대해서는 읽기 전용 역할을, 다른 테넌트에서는 슈퍼 관리자 역할을 가질 수 있습니다. 인터페이스 또는 설명서에서 읽기 전용 사용자, Admin 사용자 또는 Super Admin 사용자를 언급하는 경우 특정 테넌트에 대한 사용자의 권한 수준을 의미합니다.

### 읽기 전용 역할

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

Read Only User. You cannot make configuration changes.

읽기 전용 역할의 사용자는 다음을 수행할 수 있습니다.

- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.

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

읽기 전용 사용자는 다음을 수행할 수 없습니다.

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

## 편집 전용 역할

편집 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다.

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

편집 전용 사용자는 다음을 수행할 수 없습니다.

- 디바이스 또는 여러 디바이스에 변경 사항을 배포합니다.
- 단계적 변경 또는 OOB를 통해 감지된 변경을 폐기합니다.
- AnyConnect 패키지를 업로드하거나 이러한 설정을 구성합니다.
- 디바이스에 대한 이미지 업그레이드를 예약하거나 수동으로 시작합니다.
- 보안 데이터베이스 업그레이드를 예약하거나 수동으로 시작합니다.
- Snort 2와 Snort 3 버전 사이를 수동으로 전환합니다.
- 템플릿을 생성합니다.
- 기존 OOB 변경 설정을 변경합니다.
- 시스템 관리 설정을 편집합니다.

- 디바이스를 온보딩합니다.
- 디바이스를 삭제합니다.
- VPN 세션 또는 사용자 세션을 삭제합니다.
- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.

## 배포 전용 역할

배포 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다.

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

배포 전용 사용자는 다음을 수행할 수 없습니다.

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

## VPN 세션 관리자 역할

VPN 세션 관리자 역할은 사이트 투 사이트 VPN 연결이 아닌 원격 액세스 VPN 연결을 모니터링하는 관리자를 위해 설계되었습니다.

VPN 세션 관리자 역할이 있는 사용자는 다음을 수행할 수 있습니다.

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

VPN 세션 관리자 사용자는 다음을 수행할 수 없습니다.

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

## 관리자 역할

관리 사용자는 대부분의 CDO 측면에 대한 완전한 액세스 권한을 가집니다. 관리 사용자는 다음을 수행할 수 있습니다.

- CDO에서 개체 또는 정책을 생성, 읽기, 업데이트 및 삭제하고 설정을 구성합니다.
- 디바이스를 온보딩합니다.
- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.



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

관리 사용자는 다음을 수행할 수 없습니다.

- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.

## 슈퍼 관리자

슈퍼 관리자는 CDO의 모든 측면에 대한 완전한 액세스 권한을 갖습니다. 슈퍼 관리자는 다음을 수행할 수 있습니다.

- 사용자 역할을 변경합니다.
- 사용자 레코드를 생성합니다.



**Note** 최고 관리자는 CDO 사용자 레코드를 생성할 수 있지만 사용자가 테넌트에 로그인하는 데 필요한 모든 사용자 레코드는 아닙니다. 사용자는 테넌트에서 사용하는 ID 제공자의 계정도 필요합니다. 엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. 사용자는 Cisco Secure Cloud Sign-On 계정에 자가 등록할 수 있습니다. 자세한 내용은 [새 CDO 테넌트에 대한 초기 로그인](#), on page 40를 참조하십시오.

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

## 사용자 역할의 기록 변경

사용자 레코드는 사용자의 현재 역할이 기록된 것입니다. 테넌트와 연결된 사용자를 보면 레코드별로 각 사용자의 역할을 확인할 수 있습니다. 사용자 역할을 변경하면 사용자 레코드가 변경됩니다. 사용자의 역할은 사용자 관리 테이블에서 해당 역할로 식별됩니다. 자세한 내용은 [사용자 관리](#)를 참조하십시오.

사용자 레코드를 변경하려면 슈퍼 관리자여야 합니다. 테넌트에 슈퍼 관리자가 없는 경우 [CDO 고객이 TAC로 지원 티켓을 여는 방법](#)에 문의하십시오.

## 사용자 역할에 대한 사용자 레코드 생성

CDO 사용자는 인증을 받고 CDO 테넌트에 액세스할 수 있도록 CDO 레코드 및 해당 IdP 계정이 필요합니다. 이 절차는 Cisco Secure Cloud Sign-On의 사용자 계정이 아니라 사용자의 CDO 사용자 레코드를 생성합니다. 사용자가 Cisco Security Cloud Sign On에 계정이 없는 경우, <https://sign-on.security.cisco.com>으로 이동하고 로그인 화면 하단에서 **Sign up**(등록)을 클릭하여 자가 등록할 수 있습니다. .



**Note** 이 작업을 수행하려면 CDO에서 [슈퍼 관리자](#) 역할이 있어야 합니다.

## 사용자 레코드 생성


적절한 사용자 역할이 있는 사용자 레코드를 생성하려면 다음 절차를 수행합니다.

### Procedure

단계 1 CDO에 로그인합니다.

단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.

단계 4 파란색 더하기  버튼을 클릭하여 새 사용자를 테넌트에 추가합니다.

단계 5 사용자의 이메일 주소를 입력합니다.

**Note** 사용자의 이메일 주소는 Cisco Secure Log-On 계정의 이메일 주소와 일치해야 합니다.


단계 6 드롭다운 메뉴에서 사용자 [Cisco Defense Orchestrator의 사용자 역할](#)을 선택합니다.

단계 7 **v**를 클릭합니다.

**Note** 최고 관리자는 CDO 사용자 레코드를 생성할 수 있지만 사용자가 테넌트에 로그인하는 데 필요한 모든 사용자 레코드는 아닙니다. 사용자는 테넌트에서 사용하는 ID 제공자의 계정도 필요합니다. 엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Sign-on입니다. 사용자는 Cisco Secure Sign-On 계정에 자가 등록할 수 있습니다. 자세한 내용은 [새 CDO 테넌트에 대한 초기 로그인](#), on page 40를 참조하십시오.

## API 전용 사용자 생성

프로시저

- 
- 단계 1 CDO에 로그인합니다.
  - 단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
  - 단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.
  - 단계 4 테넌트에 새 사용자를 추가하려면 파란색 플러스 버튼  를 클릭합니다.
  - 단계 5 **API Only User**(API 전용 사용자) 확인란을 선택합니다.
  - 단계 6 **Username**(사용자 이름) 필드에 사용자 이름을 입력하고 **OK**(확인)를 클릭합니다.
 

중요 사용자 이름은 이메일 주소이거나 '@yourtenant' 접미사가 사용자 이름에 자동으로 추가되므로 '@' 문자를 포함할 수 없습니다.
  - 단계 7 드롭다운 메뉴에서 사용자 **Cisco Defense Orchestrator의 사용자 역할**을 선택합니다.
  - 단계 8 **OK**(확인)를 클릭합니다.
  - 단계 9 **User Management**(사용자 관리) 탭을 클릭합니다.
  - 단계 10 새 API 전용 사용자의 토큰 열에서 **Generate API Token**(API 토큰 생성)을 클릭하여 API 토큰을 얻습니다.
- 

## 사용자 역할에 대한 사용자 레코드 편집

이 작업을 수행하려면 슈퍼 관리자 역할이 있어야 합니다. 슈퍼 관리자가 로그인한 CDO 사용자의 역할을 변경할 경우 역할이 변경되면 해당 사용자는 자동으로 세션에서 로그아웃됩니다. 사용자가 다시 로그인하면 새 역할을 받게 됩니다.




---

**Note** 이 작업을 수행하려면 CDO에서 **슈퍼 관리자** 역할이 있어야 합니다.

---




---

**Caution** 사용자 레코드의 역할을 변경하면 사용자 레코드와 연결된 **API 토큰**이 있는 경우 해당 토큰이 삭제됩니다. 사용자 역할이 변경되면 사용자는 새 API 토큰을 생성해야 합니다.

---

## 사용자 역할 편집



**Note** CDO 사용자가 로그인되어 있고 슈퍼 관리자가 역할을 변경하는 경우, 변경 사항을 적용하려면 사용자가 로그아웃했다가 다시 로그인해야 합니다.

사용자 레코드에 정의된 역할을 편집하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 CDO에 로그인합니다.
- 단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
- 단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.
- 단계 4 사용자 행에서 편집 아이콘을 클릭합니다.
- 단계 5 역할 드롭다운 메뉴에서 사용자의 새 **Cisco Defense Orchestrator의 사용자 역할**을 선택합니다.
- 단계 6 사용자 레코드에 사용자와 연결된 API 토큰이 있는 것으로 표시되면 사용자의 역할을 변경하고 결과적으로 API 토큰을 삭제할 것임을 확인해야 합니다.
- 단계 7 **v**를 클릭합니다.
- 단계 8 CDO가 API 토큰을 삭제한 경우 사용자에게 연락하여 새 API 토큰을 생성합니다.

## 사용자 역할에 대한 사용자 레코드 삭제

CDO에서 사용자 레코드를 삭제하면 Cisco Secure Cloud Sign-On 계정과 사용자 레코드의 매핑이 끊어져 연결된 사용자가 CDO에 로그인할 수 없습니다. 사용자 레코드를 삭제하면 해당 사용자 레코드와 연결된 API 토큰도 삭제됩니다. CDO에서 사용자 레코드를 삭제해도 Cisco Secure Cloud Sign-On에서 사용자의 IdP 계정은 삭제되지 않습니다.




**Note** 이 작업을 수행하려면 CDO에서 **슈퍼 관리자** 역할이 있어야 합니다.

## 사용자 레코드 삭제

사용자 레코드에 정의된 역할을 삭제하려면 다음 절차를 참조하십시오.


### Procedure


- 단계 1 CDO에 로그인합니다.

- 단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.
- 단계 3 **User Management(사용자 관리)** 탭을 클릭합니다.
- 단계 4 삭제할 사용자 행에서 휴지통 아이콘 를 클릭합니다.
- 단계 5 **OK(확인)**를 클릭합니다.
- 단계 6 확인을 클릭하여 테넌트에서 계정을 제거할 것임을 확인합니다.

## 서비스 페이지 정보 보기

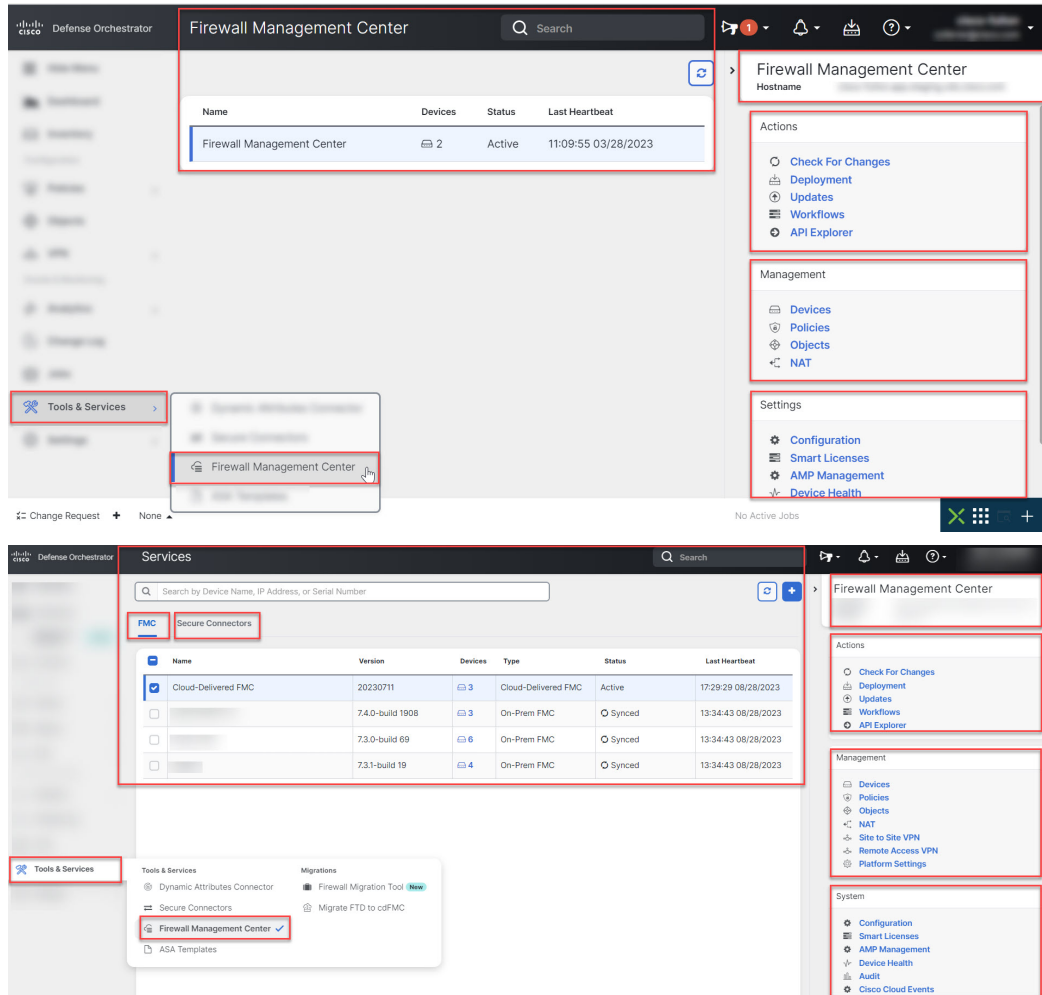
**Services(서비스)** 페이지에 CDO가 제공하는 서비스 목록이 표시됩니다. **FMC** 탭을 선택하면 CDO 계정에 연결된 클라우드 사용 Firewall Management Center 및 CDO에 온보딩된 모든 온프레미스 Management Center가 나열됩니다. 이러한 온프레미스 Management Center에서 관리하는 디바이스는 **Inventory(인벤토리)** 페이지에 나열됩니다. **Services(서비스)** 페이지의 **Secure Connector(보안 커넥터)** 탭 아래에도 보안 커넥터가 나열됩니다.

파란색 더하기 아이콘()을 클릭하여 **FMC** 탭을 선택하고 온프레미스 Management Center를 온보딩한 후 오른쪽 창의 옵션을 사용하여 디바이스 작업을 수행할 수 있습니다. 디바이스의 버전, Management Center에서 관리하는 디바이스의 수, 디바이스 유형, 디바이스 동기화 상태 등의 디바이스 정보도 확인할 수 있습니다. 매니지드 디바이스 아이콘을 클릭하면 **Inventory(인벤토리)** 페이지로 이동하며, 이 페이지에는 선택된 온프레미스 Management Center에서 관리하는 디바이스가 자동으로 필터링되어 표시됩니다. **Services(서비스)** 페이지에서는 하나 이상의 온프레미스 Management Center를 동시에 선택하여 Management Center 그룹에 대한 작업을 한 번에 수행할 수 있습니다. 클라우드 사용 Firewall Management Center가 선택된 상태에서는 어떤 온프레미스 Management Center도 선택할 수 없습니다. 새 보안 커넥터를 추가하거나 기존 보안 커넥터에 대해 작업을 수행하려면 **Secure**

**Connector(보안 커넥터)** 탭을 선택하고 를 클릭합니다.

CDO의 메인 메뉴에서 클라우드 사용 Firewall Management Center 애플리케이션 페이지를 엽니다.

**Tools & Services(툴 및 서비스)** > **Firewall Management Center**로 이동합니다.



클라우드 사용 Firewall Management Center의 경우 Services(서비스) 페이지에 다음 정보가 표시됩니다.

- 클라우드 사용 Firewall Management Center가 테넌트에 구축되지 않은 경우, **Request FMC(FMC 요청)**를 클릭합니다.
- 클라우드 사용 Firewall Management Center에 구축된 Secure Firewall Threat Defense 디바이스 수.
- CDO 및 클라우드 사용 Firewall Management Center 페이지 간의 연결 상태.
- 클라우드 사용 Firewall Management Center의 마지막 하트비트. 이는 클라우드 사용 Firewall Management Center 자체의 상태와 여기에서 관리하는 디바이스 수가 이 페이지의 테이블과 마지막으로 동기화된 것을 나타냅니다.
- 선택한 클라우드 사용 Firewall Management Center의 호스트 이름.

**Cloud-Delivered FMC(클라우드 제공 FMC)**를 선택하고 **Actions(작업)**, **Management(관리)** 또는 **Settings(설정)** 창의 링크를 사용하여 클릭한 링크와 연결된 구성 작업을 수행할 수 있는 클라우드 사용 Firewall Management Center 사용자 인터페이스를 엽니다.

클라우드 사용 Firewall Management Center 페이지가 열리면 파란색 물음표 버튼을 클릭하고 **Page-level Help**(페이지 수준 도움말)를 선택하여 현재 페이지와 수행 가능한 추가 작업에 대해 자세히 알아볼 수 있습니다.

클라우드 사용 **Firewall Management Center** 디바이스 수 및 상태 업데이트

**Cloud-Delivered FMC**(클라우드 제공 FMC)를 선택하고 **Actions**(작업) 창에서 **Check for Changes**(변경 사항 확인)를 클릭합니다. 테이블의 디바이스 수 및 상태 정보가 이 페이지와 클라우드 사용 Firewall Management Center가 마지막으로 동기화되었을 때 사용 가능한 정보로 업데이트됩니다. 동기화는 10분마다 이루어집니다.

다른 탭에서 **CDO** 및 클라우드 사용 **Firewall Management Center** 애플리케이션 열기 지원

클라우드 사용 Firewall Management Center에서 위협 방어 디바이스 또는 개체를 구성할 때 추가 브라우저 탭에서 해당 구성 페이지를 열면 로그아웃하지 않고도 CDO 및 클라우드 사용 Firewall Management Center 포털에서 동시에 작업할 수 있습니다. 예를 들어, 클라우드 사용 Firewall Management Center에서 개체를 생성하고 동시에 보안 정책에서 생성된 CDO의 이벤트 로그를 모니터링할 수 있습니다.

이 기능은 클라우드 사용 Firewall Management Center 포털로 이동하는 모든 CDO 링크에서 사용할 수 있습니다. 새 탭에서 클라우드 사용 Firewall Management Center 포털을 여는 방법:

CDO 포털에서 **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태로 해당 링크를 클릭합니다.



**참고** 한 번 클릭하면 동일한 탭에서 클라우드 사용 Firewall Management Center 페이지가 열립니다.

다음은 새 탭에서 클라우드 사용 Firewall Management Center 포털 페이지를 여는 몇 가지 예입니다.

- **Tools & Services**(툴 및 서비스) > **Firewall Management Center**를 선택하고 **Cloud-Delivered FMC**(클라우드 제공 FMC)를 선택합니다.  
오른쪽 창에서 **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태로 액세스하려는 페이지를 클릭합니다.
- **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체)를 선택합니다.
- CDO 페이지 오른쪽 상단 모서리에 있는 검색 아이콘을 클릭하고 표시되는 검색 필드에 검색 문자열을 입력합니다.  
검색 결과에서 **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태로 화살표 아이콘을 클릭합니다.
- **Dashboard**(대시보드) > **Quick Actions**(빠른 작업)를 선택합니다.  
**Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태에서 **Manage FTD Policies**(FTD 정책 관리) 또는 **Manage FTD Objects**(FTD 개체 관리)를 클릭합니다.



참고 새 CDO 테넌트로 전환하면 새 탭에서 이미 열린 해당 클라우드 사용 Firewall Management Center 포털이 로그아웃됩니다.

## 디바이스 및 서비스 관리

Cisco CDO(Defense Orchestrator)는 지원되는 디바이스 및 서비스를 보고, 관리하고, 필터링하고, 평가하는 기능을 제공합니다. **Inventory**(인벤토리) 페이지에서 다음을 수행할 수 있습니다.

- CDO 관리를 위한 디바이스 및 서비스를 온보딩합니다.
- 관리 디바이스 및 서비스의 구성 상태 및 연결 상태를 봅니다.
- 별도의 탭으로 분류된 온보딩된 디바이스 및 템플릿을 봅니다. [재고 목록 페이지 정보 보기, 97 페이지](#)을 참조하십시오.
- 개별 디바이스 및 서비스를 평가하고 조치를 취합니다.
- 디바이스 및 서비스별 정보를 보고 문제를 해결합니다.
- 다음에서 관리하는 위협 방어 디바이스의 디바이스 상태를 확인합니다.
  - [클라우드 사용 Firewall Management Center](#)
  - [온프레미스 Management Center](#)

클라우드 사용 Firewall Management Center에서 관리하는 위협 방어 디바이스의 경우, 클러스터에 있는 디바이스의 노드 상태도 볼 수 있습니다.

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

## CDO에서 디바이스의 IP 주소 변경

IP 주소를 사용하여 CDO(Cisco Defense Orchestrator)에 디바이스를 온보딩하면 CDO는 해당 IP 주소를 데이터베이스에 저장하고 해당 IP 주소를 사용하여 디바이스와 통신합니다. 디바이스의 IP 주소가 변경되면 새 주소와 일치하도록 CDO에 저장된 IP 주소를 업데이트할 수 있습니다. CDO에서 디바이스의 IP 주소를 변경해도 디바이스의 구성은 변경되지 않습니다.

CDO가 디바이스와 통신하는 데 사용하는 IP 주소를 변경하려면 다음 절차를 수행합니다.



## Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 IP 주소를 변경할 디바이스를 선택합니다.

단계 5 **Device Details**(디바이스 세부 정보) 창 위에서 디바이스의 IP 주소 옆에 있는 편집 버튼을 클릭합니다.

Nashua Building 1   
ASA 10.86.118.4:443 

단계 6 필드에 새 IP 주소를 입력하고 파란색 확인 버튼을 클릭합니다.

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

### 관련 정보:

- [테넌트 간 디바이스 이동, on page 97](#)
- [CDO에 디바이스 대량 다시 연결, on page 96](#)

## CDO에서 디바이스의 이름 변경

모든 디바이스, 모델, 템플릿 및 서비스는 온보딩되거나 CDO에서 생성될 때 이름이 지정됩니다. 디바이스 자체의 구성을 변경하지 않고 해당 이름을 변경할 수 있습니다.

## Procedure

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 이름을 변경하려는 디바이스를 선택합니다.

단계 4 **Device Details**(디바이스 세부 정보) 창 위에서 디바이스의 이름 옆에 있는 편집 버튼을 클릭합니다.

Nashua Building 1 

단계 5 필드에 새 이름을 입력하고 파란색 확인 버튼을 클릭합니다.

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

## 디바이스 및 서비스 목록 내보내기

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

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

디바이스 및 서비스 목록을 내보내기 전에 필터 창을 살펴보고 재고 목록 테이블에 내보내려는 정보가 표시되는지 확인합니다. 모든 필터를 지워 모든 매니지드 디바이스 및 서비스를 확인하거나 정보를 필터링하여 모든 디바이스 및 서비스의 하위 집합을 표시합니다. 내보내기 기능은 Inventory(재고 목록) 테이블에서 확인할 수 있는 내용을 내보냅니다.

### Procedure

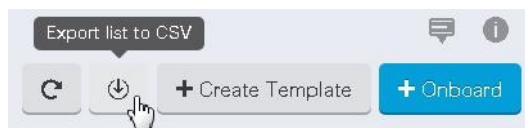
단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 유형 탭을 클릭하여 해당 탭 아래의 디바이스에서 세부 정보를 내보내거나 **All**(모두)를 클릭하여 모든 디바이스에서 세부 정보를 내보냅니다.

**필터 및 검색** 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 **Export list to CSV**(CSV로 목록 내보내기)를 클릭합니다.



단계 5 메시지가 표시되면 .csv 파일을 저장합니다.

단계 6 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

## 디바이스 구성 내보내기

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

## 프로시저

- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.  
필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.
- 단계 4 원하는 디바이스를 선택하여 강조 표시하십시오.
- 단계 5 **Actions**(작업) 창에서 **Export Configuration**(구성 내보내기)를 선택합니다.
- 단계 6 **Confirm**(확인)을 선택하여 구성을 JSON 파일로 저장합니다.

## 디바이스의 외부 링크

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

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

### 위치 변수

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

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

또는 FDM 매니지드 디바이스의 FDM에 도달해야 합니다.

### 관련 정보:

- [디바이스 메모 작성, on page 97](#)

- [디바이스 및 서비스 목록 내보내기](#), on page 92

## 장치에서 외부 링크 생성

### Procedure

- 
- 단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
  - 단계 3 해당 디바이스 탭을 클릭합니다.
  - 단계 4 장치 또는 모델을 선택합니다.  
필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.
  - 단계 5 세부 정보 창의 오른쪽에서, **External Links**(외부 링크) 섹션으로 이동합니다.
  - 단계 6 링크 이름을 입력합니다.
  - 단계 7 URL 필드에 링크의 URL을 입력합니다. 예를 들어 Cisco의 경우 <http://www.cisco.com>을 입력하는 것과 같이 전체 URL을 지정해야 합니다.
  - 단계 8 +를 클릭하여 링크를 디바이스와 연결합니다.
- 

## FDM에 대한 외부 링크 생성

다음은 CDO에서 직접 과 FTD의 FDM(Firepower Device Manager)을 여는 편리한 방법입니다.

### Procedure

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

## 여러 디바이스에 대한 외부 링크 생성

### Procedure

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

**필터** 및 **검색** 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 여러 디바이스 또는 모델을 선택합니다.

단계 5 세부 정보 창의 오른쪽에서, **External Links**(외부 링크) 섹션으로 이동합니다.

단계 6 링크 이름을 입력합니다.

단계 7 다음 방법 중 하나를 사용하여 도달하려는 URL을 입력하십시오.

- 입력

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

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

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

단계 8 +를 클릭하여 링크를 디바이스와 연결합니다.

## 외부 링크 편집 또는 삭제

### Procedure

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

**필터** 및 **검색** 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 디바이스 또는 모델을 선택합니다.

단계 5 세부 정보 창의 오른쪽에서, **External Links**(외부 링크) 섹션으로 이동합니다.

단계 6 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.

단계 7 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.

## 여러 디바이스에 대한 외부 링크 편집 또는 삭제

### Procedure

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

**필터** 및 **검색** 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 여러 디바이스 또는 모델을 선택합니다.

단계 5 세부 정보 창의 오른쪽에서, **External Links**(외부 링크) 섹션으로 이동합니다.

단계 6 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.

단계 7 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.

## CDO에 디바이스 대량 다시 연결

관리자는 CDO를 통해 둘 이상의 매니지드 디바이스를 CDO에 동시에 다시 연결할 수 있습니다. CDO가 관리하는 디바이스가 "unreachable(연결할 수 없음)"로 표시되면 CDO는 더 이상 대역 외 구성 변경 사항을 탐지하거나 디바이스를 관리할 수 없습니다. 연결이 끊어지는 데에는 여러 가지 이유가 있을 수 있습니다. 디바이스에 대한 CDO 관리를 복원하는 첫 번째 단계는 디바이스를 다시 연결하는 것입니다.



**Note** 새 인증서가 있는 디바이스를 다시 연결하는 경우 CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다. 그러나 하나의 디바이스에만 다시 연결하는 경우 CDO는 계속해서 다시 연결하려면 인증서를 수동으로 검토하고 수락하라는 메시지를 표시합니다.

### Procedure


단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 디바이스를 찾으려면 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

**필터**를 사용하여 연결 상태가 "unreachable(연결할 수 없음)"인 디바이스를 찾습니다.

단계 4 필터링된 결과에서 다시 연결을 시도할 디바이스를 선택합니다.

단계 5 **Reconnect**(다시 연결)  을 클릭합니다. CDO는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.

단계 6 알림 탭에서 대량 디바이스 다시 연결 작업의 진행 상황을 확인합니다. 대량 디바이스 다시 연결 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 [작업 페이지](#), on page 650로 이동합니다.

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

## 테넌트 간 디바이스 이동

디바이스를 CDO 테넌트에 온보딩하면 한 CDO 테넌트 간에 디바이스를 마이그레이션할 수 없습니다. 디바이스를 새 테넌트로 이동하려면 이전 테넌트에서 디바이스를 제거하고 새 테넌트에 다시 온보딩해야 합니다.

## 디바이스 메모 작성

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


### Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 메모를 작성할 디바이스 또는 모델을 선택합니다.

단계 5 오른쪽의 **Management**(관리) 창에서 **Notes**(메모)를 클릭합니다.  [Notes](#).

단계 6 오른쪽의 편집기 버튼을 클릭하고 기본 텍스트 편집기, Vim 또는 Emacs 텍스트 편집기를 선택합니다.

단계 7 메모 페이지를 편집합니다.

단계 8 **Save**(저장)를 클릭합니다.  
메모가 탭에 저장됩니다.

## 재고 목록 페이지 정보 보기

**Inventory**(재고 관리) 페이지에는 모든 물리적 및 가상 온보딩된 디바이스와 온보딩된 디바이스에서 생성된 템플릿이 표시됩니다. 이 페이지는 유형에 따라 디바이스 및 템플릿을 분류하고 각 디바이스

유형 전용 해당 탭에 표시합니다. **검색** 기능을 사용하거나 **필터**를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

이 페이지에서 다음 세부 정보를 볼 수 있습니다.

- **Device**(디바이스) 탭에는 CDO에 온보딩된 모든 라이브 디바이스가 표시됩니다.
- **Templates**(템플릿)에는 CDO로 가져온 라이브 디바이스 또는 구성 파일에서 생성된 모든 템플릿 디바이스가 표시됩니다.

## 레이블 및 필터링

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



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

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

## 디바이스 및 개체에 레이블 적용

디바이스에 레이블을 적용하려면 다음 단계를 수행하십시오.


프로시저

- 단계 1** 디바이스에 레이블을 추가하려면 왼쪽 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다. 개체에 레이블을 추가하려면 왼쪽 탐색 창에서 **Objects**(개체)를 클릭합니다.
- 단계 2** **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3** 해당 디바이스 탭을 클릭합니다.
- 단계 4** 생성된 테이블에서 하나 이상의 디바이스 또는 모델을 선택합니다.
- 단계 5** 오른쪽의 **Add Groups and Labels**(그룹 및 레이블 추가) 필드에서 디바이스의 레이블을 지정합니다.
- 단계 6** 파란색 + 아이콘을 클릭합니다.



## 필터

**Inventory**(재고 목록) 및 **Objects**(개체) 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

필터링하려면 **Devices and Services**(디바이스 및 서비스), **Policies**(정책) 및 **Objects**(개체) 탭의 왼쪽 창에서  을 클릭합니다.

**Inventory**(재고 목록) 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.



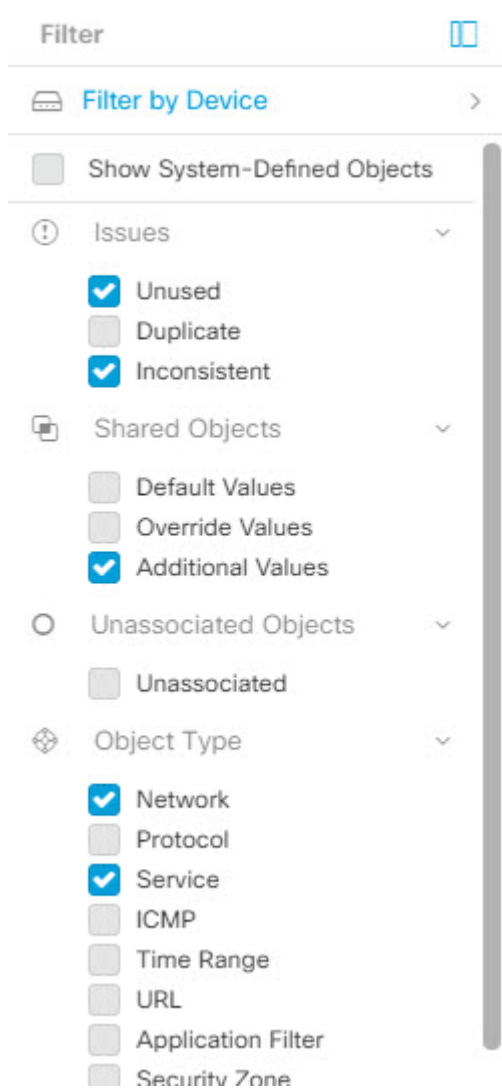
**참고** **FTD** 탭이 열리면 필터 창이 CDO에서 디바이스에 액세스하는 데 사용되는 관리 애플리케이션을 기반으로 FDM 관리 디바이스를 표시하는 필터를 제공합니다.

- FDM: FTD API 또는 FDM을 사용하여 관리되는 디바이스.
- FMC-FTD: Firepower Management Center를 사용하여 관리되는 디바이스.
- FTD: FTD 관리를 사용하여 관리되는 디바이스.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(사용되었거나 일관성 없음)" 및 추가 값이 있는 공유 개체 및 네트워크 또는 서비스 유형의 개체 검색에 필터를 적용합니다.




## 동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기

동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스를 식별하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 필터 기준이 이미 지정된 경우 Inventory(재고 목록) 테이블 상단에 있는 **clear**(지우기) 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.

단계 5 필터 버튼  을 클릭하여 **필터** 메뉴를 확장합니다.

단계 6 필터의 Secure Device Connectors(보안 디바이스 커넥터) 섹션에서 원하는 SDC의 이름을 확인합니다. Inventory(재고 목록) 테이블에는 필터에서 선택한 SDC를 통해 CDO에 연결하는 디바이스만 표시됩니다.

단계 7 (선택 사항) 필터 메뉴에서 추가 필터를 선택하여 검색을 더욱 구체화합니다.

단계 8 (선택 사항) 작업이 완료되면 Inventory(재고 목록) 테이블 상단에 있는 **clear**(지우기) 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.

## 검색

CDO는 디바이스, 개체 및 액세스 그룹을 쉽게 찾을 수 있는 강력한 검색 기능을 제공합니다. **Devices & Service**(디바이스 및 서비스) 공간에서 검색 창에 입력을 시작하면 검색 기준에 맞는 디바이스가 표시됩니다. 디바이스의 일부 부분 이름, IP 주소 또는 물리적 디바이스의 일련 번호를 입력하여 디바이스를 찾을 수 있습니다.

마찬가지로 **Objects**(개체) 공간의 검색 창을 사용하여 개체 이름의 일부를 입력하거나 IP 주소, 포트, 명명된 주소, 프로토콜의 일부를 입력하여 개체를 찾을 수 있습니다.

### Procedure

단계 1 인터페이스 상단 근처의 검색 창으로 이동합니다.

단계 2 검색 표시줄에 검색 기준을 입력하면 해당 결과가 표시됩니다.

## 글로벌 검색

전체 검색 기능을 사용하면 CDO에서 관리하는 장치를 빠르게 찾고 탐색할 수 있습니다.

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

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

자세한 내용은 [전체 인덱싱 시작, 102 페이지](#)를 참고하십시오.

- 증분 인덱싱 - 장치 또는 개체가 추가, 수정 또는 삭제될 때마다 검색 인덱스가 자동으로 업데이트되는 이벤트 기반 인덱싱 프로세스입니다.

검색 필드에 입력하는 정보는 대소문자를 구분하지 않습니다. 다음 엔터티를 사용하여 전역 검색을 수행할 수 있습니다.

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

CDO에서 관리되는 클라우드 제공 방화벽 관리 센터 및 온프레미스 FMC는 다음 정책 유형을 지원합니다.

- 액세스 제어 정책
- 사전 필터 정책
- 위협 방어 NAT 정책

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

검색 결과에는 검색 문자열과 일치하는 모든 장치 및 개체가 표시됩니다. 검색 문자열이 디바이스 또는 개체보다 더 많이 일치하면 결과가 범주(디바이스, 개체 및 `connected_fmc`) 아래에 나타납니다.

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



#### 참고

- 전역 검색은 중복 검색 결과를 표시하지 않습니다. 개체의 경우 공유 개체의 UID는 개체 보기로 이동하는 데 사용됩니다.
- CDO에서 장치를 삭제하면, 연결된 모든 개체가 전역 검색 인덱스에서 제거됩니다.
- 정책에서 개체를 삭제하고 전체 인덱싱을 시작하기 전에 장치를 유지하면, 개체가 장치와 연결되어 있기 때문에 전역 검색 인덱스에 남아 있습니다.

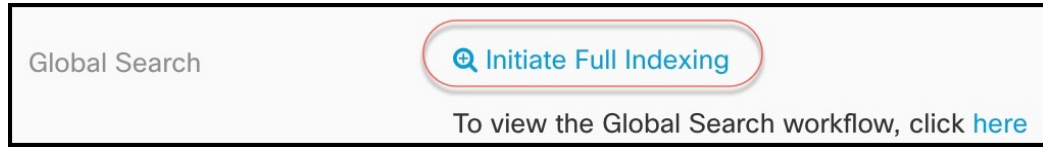
## 전체 인덱싱 시작

### 프로시저

단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 **2** CDO 메뉴 표시줄에서 **Settings(설정) > General Settings(일반 설정)**를 탐색합니다.

단계 **3** 전역 검색에서 **Initiate Full Indexing(전체 인덱싱 시작)**을 클릭하여 인덱싱을 트리거합니다.



참고 전체 인덱싱을 시작하면 CDO 테넌트의 기존 인덱싱이 지워집니다.

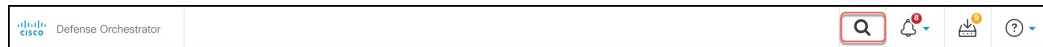
단계 4 글로벌 검색 워크플로우를 보려면 **here**(여기)를 클릭합니다.

## 전역 검색 수행

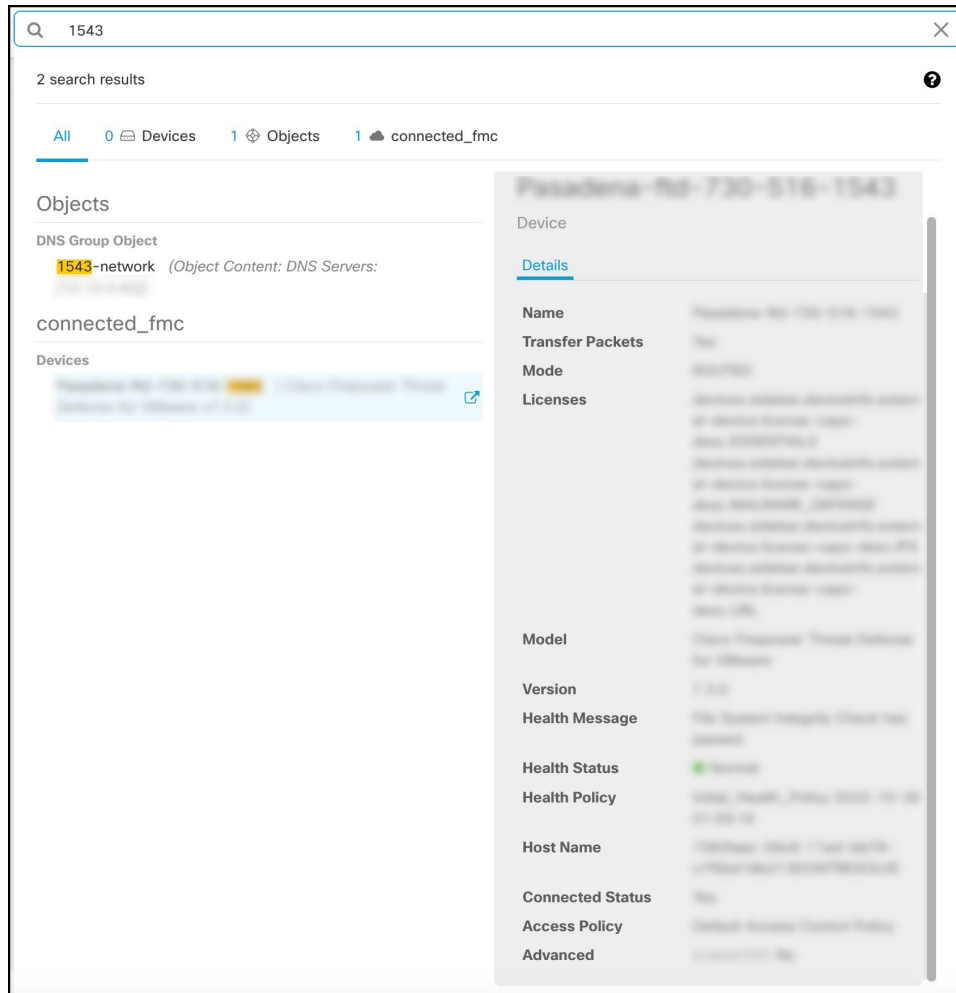
프로시저

단계 1 CDO에 로그인합니다.

단계 2 CDO 페이지 오른쪽 상단 모서리에 있는 검색 아이콘을 클릭하고 표시되는 검색 필드에 검색 문자열을 입력합니다.



검색 문자열을 입력하기 시작하면 검색 결과에 가능한 항목 목록이 표시됩니다. 검색 결과는 All, Devices, Objects 및 connected\_fmc의 네 가지 범주 아래에 나타납니다. 오른쪽 창에는 선택한 검색 결과에 대한 정보가 표시됩니다.



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

**참고** 클라우드 사용 Firewall Management Center에서 디바이스 검색 결과를 선택하면, CDO에서 클라우드 사용 Firewall Management Center 사용자 인터페이스로 이동할 수 있습니다.

클라우드 사용 Firewall Management Center에 대한 자세한 내용은 [Cisco Defense Orchestrator에서 Cloud-Delivered Firewall Management Center로 Firewall Threat Defense 관리](#)를 참조하십시오.

**단계 4** **X**를 클릭하여 검색 표시줄을 닫습니다.

## CDO 명령줄 인터페이스

CDO는 사용자에게, FDM 관리 위협 방어 디바이스를 관리하기 위한 CLI(명령줄 인터페이스)를 제공합니다. 사용자는 단일 디바이스 또는 여러 디바이스에 동시에 명령을 전송할 수 있습니다.

관련 정보:

- FTD CLI 설명서는 [Cisco Firepower Threat Defense 명령 참조](#)를 참조하십시오. 참고로 FDM 관리 디바이스는 CLI 기능이 제한되어 있습니다. 이러한 디바이스에는 show, ping, traceroute, packet-tracer, failover 및 shutdown 명령만 있습니다.

## 명령줄 인터페이스 사용

### Procedure

- 단계 1 **Inventory**(재고 목록) 페이지를 엽니다.
- 단계 2 재고 목록 테이블 위에 있는 디바이스 버튼을 클릭합니다.
- 단계 3 명령줄 인터페이스(CLI)를 사용하여 관리하려는 디바이스를 찾으려면 디바이스 탭과 필터 버튼을 사용합니다.
- 단계 4 디바이스를 선택합니다.
- 단계 5 **Device Actions**(장치 작업) 창에서 >**\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 **Command Line Interface**(명령줄 인터페이스) 탭을 클릭합니다.
- 단계 7 명령 창에 명령을 입력하고 **Send**(보내기)를 클릭합니다. 명령에 대한 디바이스의 응답은 "응답 창" 아래에 표시됩니다.

**Note** 실행할 수 있는 명령에 제한 사항이 있는 경우 해당 제한 사항은 명령 창 위에 나열됩니다.

### Related Topics

[명령줄 인터페이스에 명령 입력](#), 105 페이지

## 명령줄 인터페이스에 명령 입력

한 줄에 하나의 명령을 입력하거나 여러 줄에 여러 명령을 순차적으로 입력할 수 있으며 CDO는 명령을 순서대로 실행합니다. 다음 ASA 예에서는 세 개의 네트워크 개체와 해당 네트워크 개체를 포함하는 네트워크 개체 그룹을 생성하는 명령 배치를 전송합니다.

```

> object network email_server_north
  host 192.168.10.2
  object network email_server_south
  host 192.168.20.2
  object network email_server_headquarters
  host 192.168.30.2
  object-group network email_servers_all
  network-object object email_server_north
  network-object object email_server_south
  network-object object email_server_headquarters

```

Press Cmd+Enter to send command

**FDM 관리 디바이스 명령 입력:** CLI 콘솔은 기본 위협 방어 CLI를 사용합니다. CLI 콘솔을 사용하여 진단 CLI, 전문가 모드 또는 FXOS CLI(FXOS를 사용하는 모델)를 시작할 수는 없습니다. 기타 CLI 모드를 시작해야 하는 경우에는 SSH를 사용합니다.

## 명령 기록 작업

CLI 명령을 보낸 후 CDO는 **Command Line Interface(명령줄 인터페이스)** 페이지의 기록 창에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다.


### Procedure

단계 **1 Inventory(인벤토리)** 페이지에서 구성할 디바이스를 선택합니다.

단계 **2 Devices(디바이스)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** **> Command Line Interface(명령줄 인터페이스)**를 클릭합니다.

단계 **5** 아직 확장되지 않은 경우 시계 아이콘  을 클릭하여 기록 창을 확장합니다.

단계 **6** 편집하거나 다시 보내려는 히스토리 창에서 명령을 Select(선택)합니다.

단계 **7** 명령 창에서 명령을 그대로 재사용하거나 편집하고 **Send(보내기)**를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

**Note** CDO는 다음 두 가지 상황에서 응답창에 Done! (완료!) 메시지를 표시합니다.

- 명령이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료! 를 반환합니다.



## 대량 명령줄 인터페이스

CDO는 CLI(command line interface)를 사용하여 Secure Firewall ASA, FDM 관리, 위협 방어, SSH 및 Cisco IOS Secure Firewall Cloud Native 디바이스를 관리할 수 있는 기능을 사용자에게 제공합니다. 사용자는 단일 디바이스 또는 같은 종류의 여러 디바이스에 동시에 명령을 보낼 수 있습니다. 이 섹션에서는 한 번에 여러 디바이스에 CLI 명령을 보내는 방법을 설명합니다.

관련 정보:

- FDM 관리 디바이스 설명서의 경우 CDO는 기본 FTD CLI만 지원합니다. 이러한 디바이스에는 show, ping, traceroute, packet-tracer, failover 및 shutdown 명령만 있습니다.

위협 방어 CLI 설명서는 [Cisco Firepower Threat Defense 명령 참조](#)를 참조하십시오.

## 대량 CLI 인터페이스

The screenshot displays the Bulk CLI interface. On the left, a history list (1) shows previous commands like 'show version', 'show ssh sessions', 'show reload', and 'show ip'. The main area (2) has a command input field with 'show run | grep user' and a 'Send' button (3). Below the input is a 'My List' table (4) with columns for 'My List' and 'Execution', containing IP addresses 10.82.109.160, 10.82.109.181, and 10.82.109.187. On the right, the 'Response' section (5) shows the output for 1 device (10.82.109.181):

```

user-identity default-domain LOCAL
username bart password 53kEphYd3EDVgfrh encrypted privilege 10
username admin password ORJrHGMoergg.1Cq encrypted privilege 15
username chris password EBj1ypjrtLoG.Wfn encrypted privilege 10
username alice password QsDL/.kvhFAPwPbv encrypted privilege 10
user-statistics accounting
user-statistics accounting
  
```



**Note** CDO는 다음 두 가지 상황에서 **Done!(완료!)** 메시지를 표시합니다.

- 명령이 오류 없이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료!를 반환합니다.

숫자	설명
1	시계를 클릭하여 명령 기록 창을 확장하거나 축소합니다.

숫자	설명
2	명령 기록. 명령을 보낸 후 CDO는 이 히스토리 창에 명령을 기록하므로 돌아가서 선택하고 다시 실행할 수 있습니다.
3	명령 창. 이 창의 프롬프트에 명령을 입력합니다.
4	<p>응답 창. CDO는 명령에 대한 디바이스의 응답과 CDO 메시지를 표시합니다. 두 개 이상의 디바이스에 대한 응답이 동일한 경우 응답 창에 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.</p> <p><b>Note</b> CDO는 다음 두 가지 상황에서 <b>Done!(완료!)</b> 메시지를 표시합니다.</p> <ul style="list-style-type: none"> <li>• 명령이 오류 없이 성공적으로 실행된 후.</li> <li>• 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 <b>show</b> 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료!를 반환합니다.</li> </ul>
5	<b>My List</b> (내 목록) 탭에는 <b>Inventory</b> (인벤토리) 테이블에서 선택한 디바이스가 표시되며 명령을 보낸 디바이스를 포함하거나 제외할 수 있습니다.
6	위 그림에서 강조 표시된 <b>Execution</b> (실행) 탭은 히스토리 창에서 선택한 명령의 디바이스를 표시합니다. 이 예에서 <b>show run   grep user</b> 명령이 기록 창에서 선택되고 실행 탭에 10.82.109.160, 10.82.109.181 및 10.82.10.9.187로 전송된 것으로 표시됩니다.
7	<b>By Response</b> (응답별) 탭을 클릭하면 명령에 의해 생성된 응답 목록이 표시됩니다. 동일한 응답은 한 행에 함께 그룹화됩니다. <b>By Response</b> (응답별) 탭에서 행을 선택하면 CDO는 응답 창에 해당 명령에 대한 응답을 표시합니다.
8	<b>By Device</b> (디바이스별) 탭을 클릭하면 각 디바이스의 개별 응답이 표시됩니다. 목록에서 디바이스 중 하나를 클릭하면 특정 디바이스에서 명령에 대한 응답을 볼 수 있습니다.

## 대량 명령 전송

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 디바이스를 찾으려면 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 탭을 선택하고 필터 버튼을 사용하여 명령줄 인터페이스를 사용하여 구성할 디바이스를 찾습니다.

단계 4 디바이스를 선택합니다.

단계 5 **Device Actions**(장치 작업) 창에서 >**Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 내 목록 필드에서 명령을 보낼 디바이스를 선택하거나 선택 취소할 수 있습니다.

단계 7 명령 창에 명령을 입력하고 **Send**(보내기)를 클릭합니다. 명령 출력은 응답 창에 표시되고 명령은 변경 로그에 기록되며 CDO 명령은 대량 CLI 창의 기록 창에 명령을 기록합니다.

## 대량 명령 기록 작업

대량 CLI 명령을 보낸 후, CDO는 **대량 CLI 인터페이스** 기록에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다. 기록 창의 명령은 명령이 실행된 원래 디바이스와 연결됩니다.

### Procedure

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 디바이스를 찾으려면 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 필터 아이콘을 클릭하여 구성하려는 디바이스를 찾습니다.

단계 4 디바이스를 선택합니다.

단계 5 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 편집하거나 다시 보내려는 히스토리 창에서 명령을 **Select**(선택)합니다. 선택하는 명령은 특정 디바이스와 연결되며 반드시 첫 번째 단계에서 선택한 디바이스와 연결되지는 않습니다.

단계 7 내 목록 탭을 보고 전송하려는 명령이 예상하는 디바이스로 전송되는지 확인합니다.

단계 8 명령 창에서 명령을 편집하고 **Send**(보내기)를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

## 대량 명령 필터 작업

대량 CLI 명령을 실행한 후 **By Resonse**(응답별) 필터 및 **By Device**(디바이스별) 필터를 사용하여 계속해서 디바이스를 구성할 수 있습니다.

### 응답 기준 필터

대량 명령을 실행한 후 CDO는 명령을 보낸 디바이스에서 반환된 응답 목록으로 **By Response**(응답별) 탭을 채웁니다. 응답이 동일한 디바이스는 단일 행에 통합됩니다. **By Response**(응답별) 탭에서 행을 클릭하면 응답 창에 디바이스의 응답이 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. **X devices**(X 디바이스)를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.



명령 응답과 관련된 디바이스 목록에 명령을 보내려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 **By Response**(응답별) 탭에서 행의 명령 기호를 클릭합니다.
- 단계 2 명령 창에서 명령을 검토하고 **Send**(보내기)를 클릭하여 명령을 다시 보내거나 **Clear**(지우기)를 클릭하여 명령 창을 지우고 디바이스로 보낼 새 명령을 입력한 다음 **Send**(보내기)를 클릭합니다.
- 단계 3 명령에서 받은 응답을 검토하십시오.
- 단계 4 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확인하는 경우 명령 창에 *write memory*를 입력하고 **Send**(보내기)를 클릭합니다. 이렇게 하면 실행 중인 구성이 시작 구성에 저장됩니다.

## 디바이스 기준 필터

대량 명령을 실행한 후 CDO는 실행 탭과 디바이스별 탭을 명령을 보낸 디바이스 목록으로 채웁니다. 디바이스별 탭에서 행을 클릭하면 각 디바이스에 대한 응답이 표시됩니다.

동일한 디바이스 목록에서 명령을 실행하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 **By Device**(디바이스 별) 탭을 클릭합니다.
- 단계 2 **>\_Execute a command on these devices**(이 디바이스에서 명령 실행)를 클릭합니다.
- 단계 3 **Clear**(지우기)를 클릭하여 명령 창을 지우고 새 명령을 입력합니다.
- 단계 4 내 목록 창에서 목록의 개별 디바이스를 선택하거나 선택 취소하여 명령을 보낼 디바이스 목록을 지정합니다.
- 단계 5 **Send**(보내기)를 클릭합니다. 명령에 대한 응답이 응답 창에 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.

단계 6 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send**(보내기)를 클릭합니다.

## 디바이스 관리를 위한 CLI 매크로

CLI 매크로는 즉시 사용할 수 있는 완전한 형식의 CLI 명령이거나 실행 전에 수정할 수 있는 CLI 명령의 템플릿입니다. 모든 매크로는 하나 이상의 FTD 디바이스에서 동시에 실행할 수 있습니다.

여러 디바이스에서 동일한 명령을 동시에 실행하려면 템플릿과 유사한 CLI 매크로를 사용합니다. CLI 매크로는 디바이스 구성 및 관리의 일관성을 유지합니다. 완전한 형식의 CLI 매크로를 사용하여 디바이스에 대한 정보를 가져옵니다. FTD 디바이스에서 즉시 사용할 수 있는 다양한 CLI 매크로가 있습니다.

자주 수행하는 작업을 모니터링하기 위해 CLI 매크로를 생성할 수 있습니다. 자세한 내용은 [새 명령에서 CLI 매크로 생성](#)을 참조하십시오.

CLI 매크로는 시스템 정의 또는 사용자 정의입니다. 시스템 정의 매크로는 CDO에서 제공하며 편집하거나 삭제할 수 없습니다. 사용자 정의 매크로는 사용자가 생성하며 편집하거나 삭제할 수 있습니다.



**Note** 디바이스가 CDO에 온보딩된 후에만 디바이스에 대한 매크로를 생성할 수 있습니다.

ASA를 예로 들어 ASA 중 하나에서 특정 사용자를 찾으려면 다음 명령을 실행할 수 있습니다.

```
show running-config | grep username
```

명령을 실행할 때 사용자 이름을 검색할 사용자의 사용자 이름으로 대체합니다. 이 명령으로 매크로를 만들려면 동일한 명령을 사용하고 사용자 이름을 중괄호로 묶습니다.

```
> show running-config | grep {{username}}
```

매개변수의 이름은 원하는 대로 지정할 수 있습니다. 이 매개변수 이름을 사용하여 동일한 매크로를 생성할 수도 있습니다.

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

매개변수 이름은 설명적일 수 있으며 영숫자 문자와 밑줄을 사용해야 합니다. 이 경우 명령 구문은 `show running-config | grep`

명령의 일부이며 명령을 전송하는 디바이스에 대해 적절한 CLI 구문을 사용해야 합니다.

## 새 명령에서 CLI 매크로 생성

### Procedure

단계 1 CLI 매크로를 생성하기 전에 CDO의 명령줄 인터페이스에서 명령을 테스트하여 명령 구문이 올바른지, 그리고 신뢰할 수 있는 결과를 반환하는지 확인합니다.

**Note**

- FTD 디바이스의 경우 CDO는 FDM의 CLI 콘솔에서 실행할 수 있는 명령(show, ping, traceroute, packet-tracer, failover, reboot 및 shutdown)만 지원합니다. 이러한 명령의 구문에 대한 전체 설명은 [Cisco Firepower Threat Defense 명령 참조](#)를 참조하십시오.

단계 2 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 3 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 4 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.

단계 5 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다.

단계 7 더하기 버튼  을 클릭합니다.

단계 8 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.

단계 9 **Command**(명령) 필드에 전체 명령을 입력합니다.

단계 10 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 11 **Create**(생성)를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 [CLI 매크로 실행](#)을 참조하십시오.


## CLI 기록 또는 기존 CLI 매크로에서 CLI 매크로 생성

이 절차에서는 이미 실행한 명령, 다른 사용자 정의 매크로 또는 시스템 정의 매크로에서 사용자 정의 매크로를 생성합니다.

### 프로시저

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

참고 CLI 기록에서 사용자 정의 매크로를 생성하려면 명령을 실행한 디바이스를 선택합니다. CLI 매크로는 동일한 계정의 디바이스 간에 공유되지만 CLI 기록은 공유되지 않습니다.

- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.
- 단계 4 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 5 CLI 매크로를 만들려는 명령을 찾아 선택합니다. 다음 방법 중 하나를 사용합니다.
- 해당 디바이스에서 실행한 명령을 보려면 시계 ⌚를 클릭합니다. 매크로로 전환할 항목을 선택하면 명령 창에 명령이 나타납니다.
  - CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다. 변경할 사용자 정의 또는 시스템 정의 CLI 매크로를 선택합니다. 명령 창에 명령이 나타납니다.
- 단계 6 명령 창의 명령을 사용하여 CLI 매크로 검색 별 를 클릭합니다. 이 명령은 이제 새 CLI 매크로의 기본이 됩니다.
- 단계 7 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.
- 단계 8 명령 필드에서 명령을 검토하고 원하는 대로 변경합니다.
- 단계 9 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶은 매개변수 이름으로 교체합니다.
- 단계 10 **Create**(생성)를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.
- 명령을 실행하려면 [CLI 매크로 실행](#)을 참조하십시오.

## CLI 매크로 실행

### Procedure

- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 유형 탭을 클릭하고 하나 이상의 디바이스를 선택합니다.
- 단계 4 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 5 명령 패널에서 별표 ★를 클릭합니다.
- 단계 6 명령 패널에서 CLI 매크로를 선택합니다.
- 단계 7 다음 두 가지 방법 중 하나로 매크로를 실행합니다.
- 매크로에 정의할 매개변수가 없는 경우 **Send**(전송)를 클릭합니다. 명령에 대한 응답이 응답 창에 나타납니다. 다했습니다.
  - 아래의 Configure DNS 매크로와 같은 매개변수가 매크로에 포함된 경우 **>\_View Parameters**(매개변수 보기)를 클릭합니다.

```

★ Using Macro: Configure DNS
> dns domain-lookup {{IF_NAME}}
  dns server-group DefaultDNS
  name-server {{IP_ADDR}}

```

단계 8 Parameters(매개변수) 창의 Parameters(매개변수) 필드에 매개변수 값을 입력합니다.

단계 9 **Send**(보내기)를 클릭합니다. CDO가 성공적으로 명령을 전송하고 디바이스의 구성을 업데이트하면 완료됩니다!

- FTD의 경우 디바이스의 활성 구성이 업데이트됩니다.

단계 10 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.

⚠ Some commands may have made changes to the running config [Write to Disk](#) [Dismiss](#)

- **Write to Disk**(디스크에 쓰기)를 클릭하면 이 명령의 변경 사항과 실행 중인 구성의 다른 모든 변경 사항이 디바이스의 시작 구성에 저장됩니다.
- **Dismiss**(해제)를 클릭하면 메시지가 사라집니다.

## CLI 매크로 편집

사용자 정의 CLI 매크로는 편집할 수 있지만 시스템 정의 매크로는 편집할 수 없습니다. CLI 매크로를 수정하면 모든 FTD 디바이스에 대해 변경됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

### Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택합니다.




- 단계 5 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 편집할 사용자 정의 매크로를 선택합니다.
- 단계 7 매크로 레이블에서 편집 아이콘을 클릭합니다.
- 단계 8 Edit Macro(매크로 편집) 대화 상자에서 CLI 매크로를 편집합니다.
- 단계 9 **Save**(저장)를 클릭합니다.

CLI 매크로를 실행하는 방법에 대한 지침은 [CLI 매크로 실행](#)를 참조하십시오.

## CLI 매크로 삭제

사용자 정의 CLI 매크로는 삭제할 수 있지만 시스템 정의 매크로는 삭제할 수 없습니다. CLI 매크로를 삭제하면 모든 디바이스에서 삭제됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

### Procedure

- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 디바이스를 선택합니다.
- 단계 5 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 삭제할 사용자 정의 CLI 매크로를 선택합니다.
- 단계 7 CLI 매크로 레이블에서 휴지통 아이콘 를 클릭합니다.
- 단계 8 CLI 매크로를 제거할지 확인합니다.

## 명령줄 인터페이스 설명서

CDO는 FDM 관리 디바이스의 명령줄 인터페이스를 부분적으로 지원합니다. 사용자가 단일 디바이스 및 여러 디바이스에 명령 및 응답 형식으로 동시에 명령을 전송할 수 있도록 CDO 내에서 터미널과 유사한 인터페이스를 제공합니다. CDO에서 지원되지 않는 명령의 경우 PuTTY 또는 SSH 클라이언트와 같은 디바이스 GUI 터미널을 사용하여 디바이스에 액세스하고, 추가 명령은 [CLI 설명서](#)를 참조하십시오.

## CLI 명령 결과 내보내기


독립형 디바이스 또는 여러 디바이스에 실행된 CLI 명령의 결과를 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다. 단일 디바이스 또는 여러 디바이스의 CLI 결과를 한 번에 내보낼 수 있습니다. 내보낸 정보에는 다음이 포함됩니다.

- 디바이스
- 날짜
- 사용자
- 명령
- 출력

## CLI 명령 결과 내보내기

명령 창에서 방금 실행한 명령의 결과를 .csv 파일로 내보낼 수 있습니다.

### Procedure


- 단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 디바이스를 선택하여 강조 표시하십시오.
- 단계 5 디바이스에 대한 **Device Actions**(디바이스 작업) 창에서 **> Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 명령줄 인터페이스 창에서 명령을 입력하고 **Send**(보내기)를 클릭하여 디바이스에 명령을 실행합니다.
- 단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.
- 단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

## CLI 매크로의 결과 내보내기

명령 창에서 실행된 매크로의 결과를 내보낼 수 있습니다. 하나 이상의 디바이스에서 실행된 CLI 매크로의 결과를 .csv 파일로 내보내려면 다음 절차를 따르십시오.

### Procedure



- 단계 1 **Devices & Services**(디바이스 및 서비스) 페이지를 엽니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 디바이스를 선택하여 강조 표시하십시오.

- 단계 5 디바이스에 대한 **Device Actions**(디바이스 작업) 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 ★를 선택합니다.
- 단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send**(보내기)를 클릭합니다.
- 단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.
- 단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

## CLI 명령 기록 내보내기

다음 절차를 사용하여 하나 또는 여러 디바이스의 CLI 기록을 .csv 파일로 내보냅니다.

### Procedure

- 단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 디바이스를 선택하여 강조 표시하십시오.
- 단계 5 디바이스에 대한 디바이스 작업 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 아직 확장되지 않은 경우 시계 아이콘 을 클릭하여 기록 창을 확장합니다.
- 단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.
- 단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.


### 관련 정보:

- [CDO 명령줄 인터페이스, on page 105](#)
- [새 명령에서 CLI 매크로 생성](#)
- [CLI 매크로 삭제](#)
- [CLI 매크로 편집](#)
- [CLI 매크로 실행](#)
- [명령줄 인터페이스 설명서](#)
- [대량 명령줄 인터페이스](#)

## CLI 매크로 목록 내보내기

명령 창에서 실행된 매크로만 내보낼 수 있습니다. 다음 절차를 사용하여 하나 이상의 디바이스의 CLI 매크로를 .csv 파일로 내보냅니다.


프로시저

- 
- 단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
  - 단계 3 해당 디바이스 탭을 클릭합니다.
  - 단계 4 디바이스를 선택하여 강조 표시하십시오.
  - 단계 5 디바이스에 대한 디바이스 작업 창에서 **> Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
  - 단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 ★를 선택합니다.
  - 단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send**(보내기)를 클릭합니다.
  - 단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.
  - 단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다.
- 


## 개체


개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 단일 개체를 만들고 다른 정책을 사용하고 개체를 편집할 수 있으며 해당 변경 사항은 개체를 사용하는 모든 정책에 전파됩니다. 개체가 없는 경우 동일한 변경이 필요한 모든 정책을 개별적으로 편집해야 합니다.


디바이스를 온보딩하면, CDO는 해당 디바이스에서 사용하는 모든 개체를 인식하고, 저장한 다음, **Objects**(개체) 페이지에 나열합니다. **Objects**(개체) 페이지에서 기존 개체를 편집하고 보안 정책에 사용할 새 개체를 생성할 수 있습니다.

CDO은 여러 디바이스에서 사용되는 개체를 **shared object**(공유 개체)라고 부르고 **Objects**(개체) 페이지에서 이 배지 로 식별합니다.

때때로 공유 개체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디바이스에서 완벽하게 공유되지 않습니다.

- **Duplicate objects**(중복 개체)는 이름은 다르지만 값은 같은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 일반적으로 비슷한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체는 다음 문제 아이콘 로 식별됩니다.
- **Inconsistent objects**(일관성 없는 개체)는 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체입니다. 때로는 사용자가 동일한 이름과 콘텐츠로 다른 구성으로 개체를 생성하지만 시

간이 지남에 따라 이러한 개체의 값이 달라져 불일치가 발생합니다. 일관성 없는 개체는 다음 문제 아이콘 로 식별됩니다.

- 사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다. 사용되지 않는 개체는 다음 문제 아이콘 로 식별됩니다.

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수도 있습니다. 규칙 또는 정책과 연결되지 않은 개체를 생성할 수 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용하는 경우, CDO는 해당 개체의 복사본을 생성하고 해당 복사본을 사용합니다.

**Objects(개체)** 메뉴로 이동하거나 네트워크 정책의 세부 정보에서 확인하여 CDO에 의해 관리되는 개체를 볼 수 있습니다.

CDO은 한 위치에서 지원되는 디바이스 전체에 걸쳐 네트워크 및 서비스 개체를 관리할 수 있습니다. CDO에서는 다음과 같은 방법으로 개체를 관리할 수 있습니다.

- 다양한 기준에 따라 모든 개체를 검색하고 **개체 필터**합니다.
- 디바이스에서 중복되거나, 사용되지 않거나, 일관성이 없는 개체를 찾고 이러한 개체 문제를 통합, 삭제 또는 해결하십시오.
- 연결되지 않은 개체를 찾아 사용하지 않는 경우 삭제합니다.
- 여러 디바이스에서 공통적인 공유 개체를 검색합니다.
- 변경 사항을 커밋하기 전에 일련의 정책 및 디바이스에 대한 개체 변경 사항의 영향을 평가합니다.
- 다양한 정책 및 디바이스와 개체 및 개체의 관계 집합을 비교합니다.
- CDO에 온보딩된 후 디바이스에서 사용 중인 개체를 캡처합니다.

온보딩된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 [문제 해결 Cisco Defense Orchestrator, on page 790](#)를 참조하십시오.

## 개체 유형

다음 표에서는 CDO를 사용하여 디바이스에 대해 생성하고 관리할 수 있는 개체에 대해 설명합니다.

**Table 5: FDM** 관리 디바이스 개체 유형

개체	설명
<a href="#">애플리케이션 필터 개체</a>	애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.

개체	설명
RA VPN AnyConnect 클라이언트 프로파일 업로드	AnyConnect 클라이언트 프로파일 개체는 파일 개체이며 구성(일반적으로 원격 액세스 VPN 정책)에서 사용되는 파일을 나타냅니다. AnyConnect 클라이언트 프로파일 및 AnyConnect 클라이언트 이미지 파일을 포함할 수 있습니다.
인증서 개체	디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.
DNS 그룹 개체	www.example.com과 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인하려면 DNS 서버가 필요합니다. 관리 및 데이터 인터페이스에 대해서도 다른 DNS 그룹 개체를 구성할 수 있습니다.
Firepower 지리위치 필터 개체 생성 및 편집	지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소를 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.
IKEv1 정책 생성 또는 편집	IKEv1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 매개변수가 포함되어 있습니다.
IKEv2 정책	IKEv2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 매개변수가 포함되어 있습니다.
IKEv1 IPSEC 제안	IPsec 제안 개체는 IKE 1단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.
IKEv2 IPSEC 제안	IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.
네트워크 개체	네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다.

개체	설명
보안 영역 개체	보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다.
서비스 개체	서비스 개체, 서비스 그룹 및 포트 그룹은 TCP/IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다.
SGT 그룹 생성	SGT 동적 개체는 ISE에서 할당된 SGT를 기반으로 소스 또는 대상 주소를 식별하며, 그런 다음 수신 트래픽과 일치시킬 수 있습니다.
시스템 로그 서버 개체	Syslog 서버 개체는 연결 지향형 또는 진단 Syslog(Syslog) 메시지를 수신할 수 있는 서버를 식별합니다.
URL 개체	URL 개체 및 그룹(URL 개체로 총칭함)을 사용하여 웹 요청의 URL 또는 IP 주소를 정의합니다. 이러한 개체를 사용하여 액세스 제어 정책에서 수동 URL 필터링 또는 보안 인텔리전스 정책에서 차단 기능을 구현할 수 있습니다.

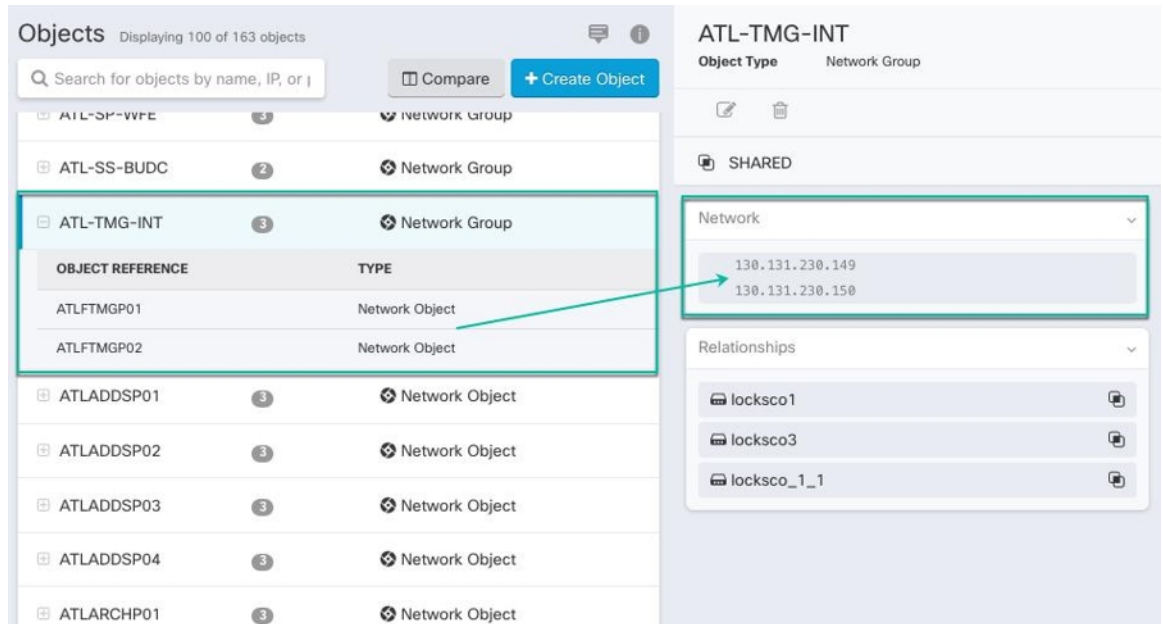
## 공유 개체

CDO(Cisco Defense Orchestrator)는 이름과 콘텐츠가 동일한 여러 디바이스의 개체인 공유 개체를 호출합니다. 공유 개체는 이 아이콘으로 식별됩니다.



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

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



## 개체 재정의

개체 오버라이드를 사용하면 특정 디바이스에서 공유 네트워크 개체의 값을 오버라이드할 수 있습니다. CDO는 오버라이드를 구성할 때 지정한 디바이스에 해당하는 값을 사용합니다. 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체에 대하여 CDO는 이러한 값이 오버라이드 되기 때문에 **Inconsistent objects**(일관성 없는 개체)로 식별하지 않습니다.

대부분의 디바이스에 대한 정의가 해당하는 개체를 생성하고 다른 정의가 필요한 일부 디바이스의 개체에 대한 특정 변경 사항을 지정하는 오버라이드를 사용할 수 있습니다. 모든 디바이스에 오버라이드가 필요한 개체를 생성할 수도 있습니다. 하지만 이 경우 모든 디바이스에 단일 정책을 생성할 수 있습니다. 개체 오버라이드는 필요한 경우 개별 디바이스의 정책을 바꾸지 않고도 디바이스 전반에 걸쳐 사용이 가능한 작은 공유 정책 집합을 생성하도록 합니다.

예를 들어 각 사무실에 프린터 서버가 있고, 프린터 서버 개체인 `print-server`를 만든 시나리오를 생각해 보십시오. ACL에는 프린터 서버가 인터넷에 액세스하는 것을 거부하는 규칙이 있습니다. 프린터 서버 개체에는 한 사무실에서 다른 사무실로 변경하려는 기본값이 있습니다. 값이 다를 수 있지만 개체 오버라이드를 사용하고 규칙과 "프린터-서버" 개체를 모든 위치에서 일관되게 유지함으로써 이 작업을 수행할 수 있습니다.



Editing Shared Network Object
✕

Object Name \*

Devices

2 Devices ...

Usage

0 Rule Sets ...

Description

Default Value ▾

ASAv-99-18 ...

Override Values ▾

Value	Devices	
126.0.2.4	Pasadena-ftd-730-516-...	✎ ⬆ 🗑
126.0.1.6	BGL_FTD_7.3	✎ ⬆ 🗑
126.0.1.9	connected_fmc	✎ ⬆ 🗑

Cancel
Save



**Note** CDO를 사용하면 규칙 세트의 규칙과 연관된 개체를 오버라이드할 수 있습니다. 규칙에 새 개체를 추가할 때 디바이스를 규칙 세트에 연결하고 변경 사항을 저장한 후에만 오버라이드할 수 있습니다. 자세한 내용은 [디바이스에 대한 규칙 집합 구성](#)을 참조하십시오.



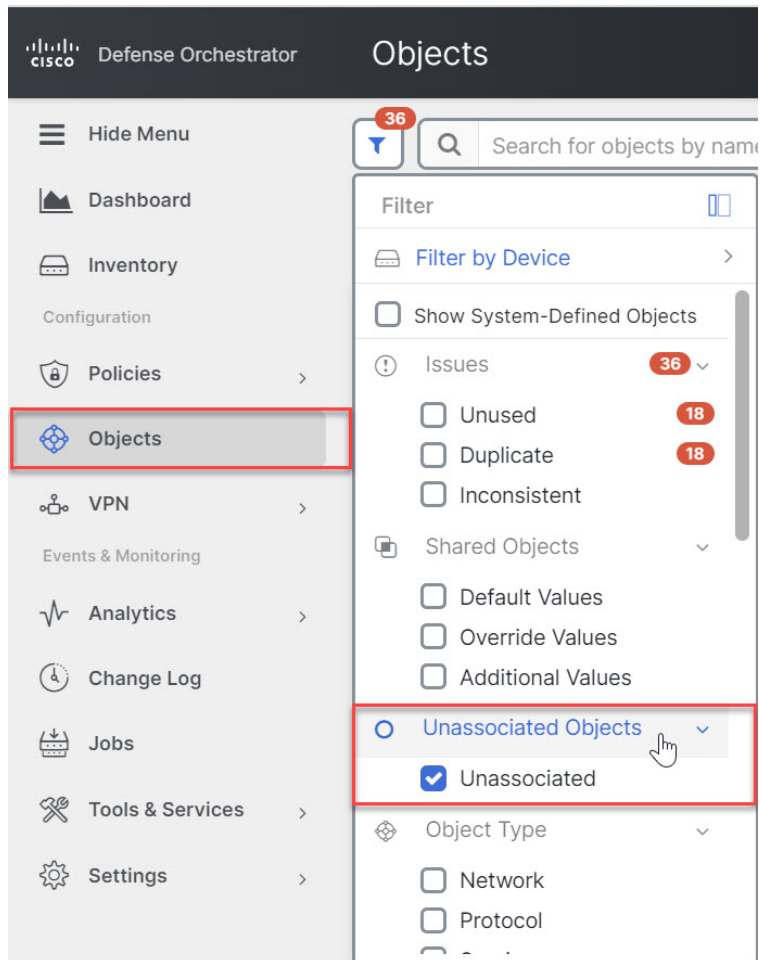
**Note** 일관되지 않은 개체가 있는 경우 오버라이드를 통해 개체를 단일 공유 개체로 결합할 수 있습니다. 자세한 내용은 [불일치 개체 문제 해결](#), on page 797를 참조하십시오.

## 연결 해제된 개체

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수 있습니다. 규칙이나 정책과 연결되지 않은 개체를 생성할 수도 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용할 때, CDO는 해당 개체의 사본을 생성하고 해당 사본을 사용합니다. 연결되지 않은 원래 개체는 야간 유지 관리 작업에 의해 삭제되거나 사용자가 삭제할 때까지 사용 가능한 개체 목록에 남아 있습니다.

개체와 연결된 규칙 또는 정책이 실수로 삭제된 경우 모든 구성이 손실되지 않도록 연결되지 않은 개체는 사본으로 CDO에 남아 있습니다.

연결되지 않은 개체를 보려면 개체 탭의 왼쪽 창에서 ▼를 클릭하고 **Unassociated** (연결되지 않음) 확인란을 선택합니다.



## 개체 비교

### Procedure

단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.

단계 2 페이지에서 개체를 필터링하여 비교하려는 개체를 찾습니다.

단계 3 **Compare**(비교) 버튼  를 클릭합니다.

단계 4 비교할 개체를 최대 3개까지 선택합니다.


단계 5 화면 하단에서 개체를 나란히 봅니다.

- 개체 세부 정보 제목 표시줄에서 위쪽 및 아래쪽 화살표를 클릭하면 개체 세부 정보를 더 많이 또는 더 적게 볼 수 있습니다.
- 세부 정보 및 관계 상자를 확장하거나 축소하여 더 많거나 적은 정보를 확인합니다.

단계 6 (선택 사항) 관계 상자는 개체가 사용되는 방식을 보여줍니다. 디바이스 또는 정책과 연결될 수 있습니다. 개체가 디바이스와 연결된 경우 디바이스 이름을 클릭한 다음 **View Configuration**(구성 보기)을 클릭하여 디바이스 구성을 볼 수 있습니다. CDO는 디바이스의 구성 파일을 표시하고 해당 개체에 대한 항목을 강조 표시합니다.

## 필터

**Inventory**(재고 목록) 및 **Objects**(개체) 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

필터링하려면 **Devices and Services**(디바이스 및 서비스), **Policies**(정책) 및 **Objects**(개체) 탭의 왼쪽 창에서 을 클릭합니다.

**Inventory**(재고 목록) 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.



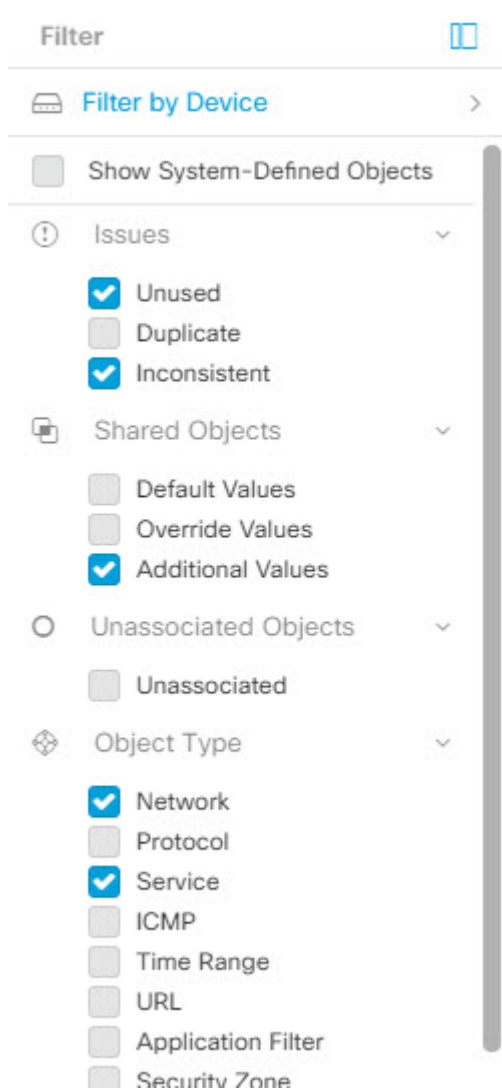
참고 **FTD** 탭이 열리면 필터 창이 CDO에서 디바이스에 액세스하는 데 사용되는 관리 애플리케이션을 기반으로 FDM 관리 디바이스를 표시하는 필터를 제공합니다.

- FDM: FTD API 또는 FDM을 사용하여 관리되는 디바이스.
- FMC-FTD: Firepower Management Center를 사용하여 관리되는 디바이스.
- FTD: FTD 관리를 사용하여 관리되는 디바이스.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(사용되었거나 일관성 없음)" 및 추가 값이 있는 공유 개체 및 네트워크 또는 서비스 유형의 개체 검색에 필터를 적용합니다.



## 개체 필터

필터링하려면 Objects(개체) 탭의 왼쪽 창에서 ▼(를) 클릭합니다.

- **All Objects**(모든 개체) - 이 필터는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 개체를 제공합니다. 이 필터는 모든 개체를 찾아보거나 하위 필터를 검색하거나 추가로 적용하기 위한 시작점으로 유용합니다.
- **Shared Objects**(공유 개체) - 이 빠른 필터는 CDO가 두 개 이상의 디바이스에서 공유하는 것으로 확인한 모든 개체를 표시합니다.
- **Objects By Device**(디바이스별 개체) - 선택한 디바이스에 있는 개체를 볼 수 있도록 특정 디바이스를 선택할 수 있습니다.

하위 필터 - 각 기본 필터에는 선택 범위를 좁히기 위해 적용할 수 있는 하위 필터가 있습니다. 이러한 하위 필터는 네트워크, 서비스, 프로토콜 등의 개체 유형을 기반으로 합니다.

이 필터 표시줄에서 선택한 필터는 다음 기준과 일치하는 개체를 반환합니다.

- \* 두 디바이스 중 하나에 있는 개체. (디바이스를 지정하려면 **Filter by Device**(디바이스별 필터링)를 클릭합니다.) AND는
- \* 일치하지 않는 개체 AND는
- \* 네트워크 개체 또는 서비스 개체 AND
- \* 개체 명명 규칙에 "group"이라는 단어가 있습니다.

**Show System Objects**(시스템 개체 표시)를 선택했으므로 결과에 시스템 개체와 사용자 정의 개체가 모두 포함됩니다.

#### 시스템 개체 필터 표시

일부 디바이스는 공통 서비스에 대해 사전 정의된 개체가 함께 제공됩니다. 이러한 시스템 개체는 이미 생성되어 규칙 및 정책에서 사용할 수 있으므로 편리합니다. 개체 테이블에는 여러 시스템 개체가 있을 수 있습니다. 시스템 개체는 편집하거나 삭제할 수 없습니다.


**Show System Objects**(시스템 개체 표시)는 기본적으로 꺼져 있습니다. 개체 테이블에 시스템 개체를 표시하려면 필터 표시줄에서 **Show System Objects**(시스템 개체 표시)를 선택합니다. 개체 테이블에서 시스템 개체를 숨기려면 필터 표시줄에서 Show System Objects(시스템 개체 표시)를 선택하지 않은 상태로 둡니다.

시스템 개체를 숨기면 검색 및 필터링 결과에 포함되지 않습니다. 시스템 개체를 표시하면 개체 검색 및 필터링 결과에 포함됩니다.

#### 개체 필터 구성

원하는 만큼 기준을 필터링할 수 있습니다. 더 많은 범주를 필터링할수록 예상되는 결과는 줄어듭니다.

#### Procedure

- 단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.
- 단계 2 페이지 상단의 필터 아이콘  을 클릭하여 필터 패널을 엽니다. 선택한 필터를 선택 취소하여 실수로 필터링된 개체가 없는지 확인합니다. 또한 검색 필드를 살펴보고 검색 필드에 입력되었을 수 있는 텍스트를 삭제합니다.
- 단계 3 특정 디바이스에 있는 것으로 결과를 제한하려면 다음을 수행합니다.
  - a. **Filter By Device**(디바이스별 필터링)를 클릭합니다.
  - b. 모든 디바이스를 검색하거나 디바이스 탭을 클릭하여 특정 종류의 디바이스만 검색합니다.
  - c. 필터 기준에 포함할 디바이스를 선택합니다.
  - d. **OK**(확인)를 클릭합니다.
- 단계 4 검색 결과에 시스템 개체를 포함하려면 **Show System Objects**(시스템 개체 표시)를 선택합니다. 검색 결과에서 시스템 개체를 제외하려면 **Show System Objects**(시스템 개체 표시)의 선택을 취소합니다.

필터 기준에서 디바이스를 제외해야 하는 경우

- 단계 5 필터링할 개체 **Issues**(문제)를 선택합니다. 두 개 이상의 문제를 선택하면 선택한 범주의 개체가 필터 결과에 포함됩니다.
- 단계 6 문제가 있었지만 관리자가 무시한 개체를 확인하려면 **Ignored**(무시됨) 문제를 선택합니다.
- 단계 7 두 개 이상의 디바이스 간에 공유되는 개체를 필터링하는 경우 **Shared Objects**(공유 개체)에서 필수 필터를 선택합니다.
- **Default Values**(기본값): 기본값만 있는 개체를 필터링합니다.
  - **Override Values**(값 재정의): 오버라이드된 값이 있는 개체를 필터링합니다.
  - **Additional Values**(추가 값): 추가 값이 있는 개체를 필터링합니다.
- 단계 8 규칙 또는 정책의 일부가 아닌 개체를 필터링하는 경우 **Unassociated**(연결되지 않음)를 선택합니다.
- 단계 9 필터링할 개체 유형을 선택합니다.
- 단계 10 **Objects**(개체) 검색 필드에 개체 이름, IP 주소 또는 포트 번호를 추가하여 필터링된 결과 중에서 검색 기준으로 개체를 찾을 수도 있습니다.

필터 기준에서 디바이스를 제외해야 하는 경우

필터링 기준에 디바이스를 추가하면 결과에 디바이스의 개체가 표시되지만 해당 개체와 다른 디바이스의 관계는 표시되지 않습니다. 예를 들어 **ObjectA**가 ASA1과 ASA2 간에 공유된다고 가정합니다. ASA1에서 공유 개체를 찾기 위해 개체를 필터링하는 경우 **ObjectA**를 찾을 수 있지만 **Relationships**(관계) 창에는 해당 개체가 ASA1에 있다는 것만 표시됩니다.

개체와 관련된 모든 디바이스를 보려면 검색 기준에 디바이스를 지정하지 마십시오. 다른 기준으로 필터링하고 원하는 경우 검색 기준을 추가하십시오. CDO가 식별하는 개체를 선택한 다음 관계 창을 살펴봅니다. 개체와 관련된 모든 디바이스 및 정책이 표시됩니다.

## 개체 무시

사용되지 않거나 중복되거나 일관성이 없는 개체를 해결하는 한 가지 방법은 해당 개체를 무시하는 것입니다. **사용되지 않은 개체 문제 해결 중복 개체 문제 해결 불일치 개체 문제 해결** 해당 상태에 대한 타당한 이유가 있다고 판단하고 개체 문제를 해결되지 않은 상태로 두도록 선택할 수 있습니다. 나중에 무시된 개체를 해결해야 할 수도 있습니다. CDO는 개체 문제를 검색할 때 무시된 개체를 표시하지 않으므로 무시된 개체에 대한 개체 목록을 필터링한 다음 결과에 따라 조치를 취해야 합니다.

### Procedure

- 단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.
- 단계 2 **개체 필터**
- 단계 3 **Object**(개체) 테이블에서 무시를 취소할 개체를 선택합니다. 한 번에 하나의 개체를 무시 취소할 수 있습니다.
- 단계 4 세부 정보 창에서 **Unignore**(무시)를 클릭합니다.

단계 5 요청을 확인합니다. 이제 문제별로 개체를 필터링하면 이전에 무시되었던 개체를 찾아야 합니다.

## 개체 삭제

단일 개체 또는 여러 개체를 삭제할 수 있습니다.

### 단일 개체 삭제



#### Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.


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

#### Procedure

단계 1 왼쪽의 CDO 탐색 모음에서 **Objects(개체)**를 선택하고 옵션을 선택합니다.

단계 2 개체 필터와 검색 필드를 사용하여 삭제하려는 개체를 찾아 선택합니다.

단계 3 **Relationships(관계)** 창을 검토합니다. 개체가 정책 또는 개체 그룹에서 사용되는 경우 해당 정책 또는 그룹에서 개체를 제거할 때까지 개체를 삭제할 수 없습니다.

단계 4 작업 창에서 **Remove(제거)** 아이콘 를 클릭합니다.

단계 5 **OK(확인)**을 클릭하여 개체 삭제를 확인합니다.

단계 6 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나**, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.


### 사용되지 않는 개체 그룹 삭제

디바이스를 온보딩하고 개체 문제를 해결하기 시작하면 사용하지 않는 개체를 많이 찾습니다. 한 번에 최대 50개의 사용하지 않는 개체를 삭제할 수 있습니다.

#### 프로시저

단계 1 **Issues(문제)** 필터를 사용하여 미사용 개체를 찾습니다. 디바이스 필터를 사용하여 디바이스 없음 선택하여 디바이스와 연결되지 않은 개체를 찾을 수도 있습니다. 개체 목록을 필터링하면 개체 확인란이 나타납니다.

단계 2 개체 테이블 머리글에서 **Select all**(모두 선택) 확인란을 선택하여 개체 테이블에 나타나는 필터에 의해 발견된 모든 개체를 선택합니다. 또는 삭제할 개별 개체에 대한 개별 확인란을 선택합니다.

단계 3 작업 창에서 **Remove**(제거) 아이콘 를 클릭합니다.

단계 4 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 네트워크 개체

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 그룹은 그룹에 추가하는 네트워크 개체 및 기타 개별 주소 또는 서브 네트워크의 모음입니다. 네트워크 개체 및 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.

**Table 6:** 네트워크 개체의 허용되는 값

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

**Table 7:** 네트워크 그룹의 허용되는 콘텐츠

디바이스 유형	IP 값	네트워크 개체	네트워크 그룹
FTD	아니요	예	예

제품 간 네트워크 개체 재사용

클라우드 사용 Firewall Management Center가 포함된 Cisco Defense Orchestrator 테넌트가 있는 경우:

Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체 또는 그룹을 생성하면 클라우드 사용 Firewall Management Center를 구성할 때 사용되는 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 개체 목록에도 개체의 복사본이 추가되며, 그 반대의 경우도 마찬가지입니다.

한 페이지에서 네트워크 개체 또는 그룹에 대한 변경 사항은 두 페이지의 개체 또는 그룹 인스턴스에 적용됩니다. 한 페이지에서 개체를 삭제하면 다른 페이지에서도 개체의 해당 복사본이 삭제됩니다.

예외:

- 클라우드 사용 Firewall Management Center에 대해 동일한 이름의 네트워크 개체가 이미 있는 경우 Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체는 Cisco Defense Orchestrator의 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에서 복제되지 않습니다.



- 온프레미스 Secure Firewall Management Center에서 관리하는 온보딩된 위협 방어 디바이스의 네트워크 개체 및 그룹은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 복제되지 않으며, 클라우드 사용 Firewall Management Center에서 사용할 수 없습니다.

클라우드 사용 Firewall Management Center로 마이그레이션된 온프레미스 Secure Firewall Management Center 인스턴스의 경우, 네트워크 개체 및 그룹이 FTD 디바이스에 구축된 정책에서 사용되었다면 네트워크 개체 및 그룹이 CDO 개체 페이지에 복제됩니다.

- CDO와 클라우드 사용 Firewall Management Center 간에 네트워크 개체 공유는 새로운 테넌트에서 자동으로 활성화되지만 기존 테넌트에 대해서는 요청해야 합니다. 네트워크 개체를 클라우드 사용 Firewall Management Center와 공유하지 않는 경우 **CDO 고객이 TAC로 지원 티켓을 여는 방법**하여 테넌트에서 기능을 활성화하십시오.

### 네트워크 개체 보기

CDO를 사용하여 생성한 네트워크 개체와 온보딩된 디바이스 구성에서 인식되는 CDO가 **Objects(개체)** 페이지에 표시됩니다. 개체 유형으로 레이블이 지정됩니다. 이렇게 하면 개체 유형으로 필터링하여 원하는 개체를 빠르게 찾을 수 있습니다.

**Objects(개체)** 페이지에서 네트워크 개체를 선택하면 **Details(세부 정보)** 창에 개체의 값이 표시됩니다. **Relationships(관계)** 창에는 개체가 정책에서 사용되는지 여부와 개체가 저장된 디바이스가 표시됩니다.

네트워크 그룹을 클릭하면 해당 그룹의 콘텐츠가 표시됩니다. 네트워크 그룹은 네트워크 개체에 의해 제공되는 모든 값의 복합물입니다.

관련 정보:

- [Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집](#)

## Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집

**Firepower** 네트워크 개체는 CIDR 표기법으로 표시된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에 사용되는 네트워크 개체 및 네트워크 그룹의 복합 그룹입니다. Cisco Defense Orchestrator(CDO)를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

Firepower 네트워크 개체 및 그룹은 ASA, 위협 방어, FDM 관리 및 Meraki 디바이스에서 사용할 수 있습니다. [제품 간 네트워크 개체 재사용, on page 130](#)을 참조하십시오.



**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

**Caution**

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

**Table 8:** 네트워크 개체에 추가할 수 있는 IP 주소

디바이스 유형	IPv4 / IPv6	단일 주소	주소 범위	PQDN(Partially Qualified Domain Name)	CIDR 표기법의 서브넷
Firepower	IPv4 / IPv6	예	예	예	예

관련 정보:

- [Firepower 네트워크 개체 생성, on page 132](#)
- [Firepower 네트워크 개체 편집, on page 134](#)
- [공유 네트워크 그룹에 값 추가, on page 137](#)
- [공유 네트워크 그룹의 추가 값 편집, on page 139](#)

## Firepower 네트워크 개체 생성

**Note**

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **FTD > Network(네트워크)**를 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 **Create a network object(네트워크 개체 생성)**를 선택합니다.

단계 6 **Value(값)** 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소, CIDR 표기법으로 표시된 서브넷 주소 또는 PQDN(Partially Qualified Domain Name)을 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다.

**Note** 호스트 비트 값을 설정하지 마십시오. 0이 아닌 호스트 비트 값을 입력하면 클라우드 사용 Firewall Management Center에서 호스트 비트가 설정되지 않은 IPv6 개체만 허용하므로 CDO가 개체를 생성하는 동안 이 값을 설정 해제합니다.

단계 7 **Add**(추가)를 클릭합니다.

주의: 새로 생성된 네트워크 개체는 규칙 또는 정책의 일부가 아니므로 FDM 관리 디바이스와 연결되지 않습니다. 이러한 개체를 보려면 개체 필터에서 **Unassociated**(연결되지 않음) 개체 범주를 선택합니다. 자세한 내용은 **개체 필터 구성**를 참고하십시오. 디바이스의 규칙 또는 정책에서 연결되지 않은 개체를 사용하면 이러한 개체는 해당 디바이스와 연결됩니다.

## Firepower 네트워크 그룹 생성


네트워크 그룹은 네트워크 개체와 네트워크 그룹을 포함할 수 있습니다. 새 네트워크 그룹을 만들 때 이름, IP 주소, IP 주소 범위 또는 FQDN으로 기존 개체를 검색하고 네트워크 그룹에 추가할 수 있습니다. 개체가 없는 경우 동일한 인터페이스에서 해당 개체를 즉시 생성하고 네트워크 그룹에 추가할 수 있습니다.



**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.
- 단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.
- 단계 3 **FTD** > **Network**(네트워크)를 클릭합니다.
- 단계 4 개체 이름을 입력합니다.
- 단계 5 **Create a network group**(네트워크 그룹 생성)을 선택합니다.
- 단계 6 값 필드에 값이나 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.
- 단계 7 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 8 CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add**(추가)를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 9 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name**(이 이름의 새 개체로 추가)을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object**(새 개체로 추가)를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

참고: 편집 아이콘을 클릭하여 세부 정보를 편집할 수 있습니다. 삭제 버튼을 클릭해도 개체 자체는 삭제되지 않습니다. 대신 네트워크 그룹에서 제거됩니다.

단계 10 필요한 개체를 추가한 후 **Save**(저장)을 클릭하여 새 네트워크 그룹을 생성합니다.

단계 11 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).

## Firepower 네트워크 개체 편집



### Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 네트워크 개체를 선택하고 **Actions**(작업) 창에서 편집 아이콘  을 클릭합니다.

단계 4 "Firepower 네트워크 그룹 생성"에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 편집합니다.

**Note** 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

## Firepower 네트워크 그룹 편집



### Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

### Procedure


단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 네트워크 그룹을 찾습니다.

단계 3 SGT 그룹을 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 필요한 경우 개체 이름과 설명을 변경합니다.

단계 5 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

- a. 개체 이름 또는 네트워크 그룹 옆에 나타나는 편집 아이콘  을 클릭하여 편집합니다.
- b. 확인 표시를 클릭하여 변경 사항을 저장합니다. 참고: 네트워크 그룹에서 값을 제거하려면 삭제 아이콘을 클릭합니다.

단계 6 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

- a. **Values(값)** 필드에 새 값이나 기존 네트워크 개체의 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다. 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.
- b. CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(추가)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.
- c. 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.
  - 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(이 이름의 새 개체로 추가)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
  - 새 개체를 생성하려면 **Add as New Object(새 개체로 추가)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 7 **Save(저장)**를 클릭합니다. CDO에 변경의 영향을 받을 정책이 표시됩니다.

단계 8 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 9 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

## 개체 오버라이드 추가



주의 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

### 프로시저

단계 1 왼쪽 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 오버라이드를 추가할 개체를 찾습니다.

단계 3 네트워크 개체를 선택하고 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.

단계 4 **Override Values**(오버라이드 값) 대화 상자에 값을 입력하고 + **Add Value**(+ 값 추가)를 클릭합니다.

중요 추가하려는 오버라이드에는 개체에 포함된 것과 동일한 유형의 값이 있어야 합니다. 예를 들어 네트워크 개체에 대해 호스트 값이 아닌 네트워크 값으로만 오버라이드를 구성할 수 있습니다.

단계 5 값이 추가된 것을 확인하면, 오버라이드 값에서 **Devices**(디바이스) 열의 셀을 클릭합니다.

단계 6 **Add Devices**(디바이스 추가)를 클릭하고 오버라이드를 추가할 디바이스를 선택합니다. 선택한 디바이스에는 오버라이드를 추가할 개체가 포함되어 있어야 합니다.

단계 7 **Save**(저장)를 클릭합니다. CDO는 변경의 영향을 받는 디바이스를 표시합니다.

단계 8 **Confirm**(확인)을 클릭하여 개체 및 개체의 영향을 받는 모든 디바이스에 대한 오버라이드 추가를 완료합니다.

참고 개체에 두 개 이상의 오버라이드를 추가할 수 있습니다. 그러나 오버라이드를 추가할 때마다 개체가 포함된 다른 디바이스를 선택해야 합니다.

단계 9 개체 오버라이드에 대해 자세히 알아보고 [개체 오버라이드 편집](#), 137 페이지가 기존 오버라이드를 편집하려면 [개체 재정의](#), 122 페이지를 참조하십시오.


## 개체 오버라이드 편집

개체가 디바이스에 있는 한 기존 오버라이드 값을 편집할 수 있습니다.


### Procedure

단계 1 왼쪽 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 오버라이드가 있는 개체를 찾습니다.

단계 3 오버라이드가 있는 개체를 선택하고 작업 창에서 편집 아이콘  를 클릭합니다.

단계 4 오버라이드 값을 편집합니다.

- 값을 편집하려면 편집 아이콘을 클릭합니다.
- **Override Values(오버라이드 값)의 Devices(디바이스) 열에 있는 셀을 클릭하여 새 디바이스를 할당합니다.** 이미 할당된 디바이스를 선택하고 **Remove Overrides(오버라이드 제거)**를 클릭하여 해당 디바이스에서 오버라이드를 제거할 수 있습니다.
- **Override Values(오버라이드 값)에서**  화살표를 클릭하여 무시하고 공유 개체의 기본값으로 생성합니다.
- 제거하려는 오버라이드 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save(저장)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 7 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.**

## 공유 네트워크 그룹에 값 추가

연결된 모든 디바이스에 있는 공유 네트워크 그룹의 값을 "기본값"이라고 합니다. CDO를 사용하면 공유 네트워크 그룹에 "추가 값"을 추가하고 해당 공유 네트워크 그룹과 연결된 일부 디바이스에 해당 값을 할당할 수 있습니다. CDO는 변경 사항을 디바이스에 구축할 때 콘텐츠를 확인하고 공유 네트워크 그룹과 연결된 모든 디바이스에 "기본값"을 무시하고 지정된 디바이스에만 "추가 값"을 무시합니다.

모든 사이트에서 액세스할 수 있어야 하는 본사에 4개의 AD 기본 서버가 있는 시나리오를 예로 들어 보겠습니다. 따라서 모든 사이트에서 사용할 "Active-Directory"라는 개체 그룹을 생성했습니다. 이제 지사 중 하나에 두 개의 AD 서버를 추가하려고 합니다. 개체 그룹 "Active-Directory"에서 해당 지사에 특정한 추가 값으로 세부 정보를 추가하여 이 작업을 수행할 수 있습니다. 이 두 서버는 "Active-Directory" 개체가 일관성이 있는지 또는 공유되는지를 확인하는 데 참여하지 않습니다. 따라서 모든 사이트에서 4개의 AD 기본 서버에 액세스할 수 있지만 지사(2개의 추가 서버 포함)는 2개의 AD 서버와 4개의 AD 기본 서버에 액세스할 수 있습니다.




**Note** 일치하지 않는 공유 네트워크 그룹이 있는 경우 추가 값을 사용하여 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 자세한 내용은 [불일치 개체 문제 해결, on page 797](#)를 참조하십시오.



**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:  
또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.  
한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 개체 필터 및 검색 필드를 사용하여 편집할 공유 네트워크 그룹을 찾습니다.
- 단계 3 **Actions(작업)** 창에서 편집 아이콘  을 클릭합니다.
  - **Devices(디바이스)** 필드에는 공유 네트워크 그룹이 있는 디바이스가 표시됩니다.
  - **Usage(사용)** 필드에는 공유 네트워크 그룹과 연결된 규칙 집합이 표시됩니다.
  - **Default Values(기본값)** 필드는 생성 중에 제공된 공유 네트워크 그룹과 연결된 기본 네트워크 개체 및 해당 값을 지정합니다. 이 필드 옆에서 이 기본값이 포함된 디바이스의 수를 볼 수 있으며, 클릭하여 해당 이름 및 디바이스 유형을 볼 수 있습니다. 이 값과 연결된 규칙 집합도 확인할 수 있습니다.
- 단계 4 **Additional Values(추가 값)** 필드에 값 또는 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.
- 단계 5 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.
- 단계 6 CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(추가)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.
- 단계 7 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.
  - 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(이 이름의 새 개체로 추가)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
  - 새 개체를 생성하려면 **Add as New Object(새 개체로 추가)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.



값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

- 단계 8 **Devices**(디바이스) 열에서 새로 추가된 개체와 연결된 셀을 클릭하고 **Add Devices**(디바이스 추가)를 클릭합니다.
- 단계 9 원하는 디바이스를 선택하고 **OK**(확인)를 클릭합니다.
- 단계 10 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.
- 단계 11 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.
- 단계 12 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

## 공유 네트워크 그룹의 추가 값 편집




### Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

### Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.
- 단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 오버라이드가 있는 개체를 찾습니다.
- 단계 3 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.
- 단계 4 오버라이드 값을 편집합니다.
  - 값을 편집하려면 편집 아이콘을 클릭합니다.
  - **Devices**(디바이스) 열의 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides**(오버라이드 제거)를 클릭하여 해당 디바이스에서 오버라이드를 제거할 수 있습니다.
  - **Default Values**(기본값)의 ▼ 화살표를 클릭하여 푸시하고 공유 네트워크 그룹의 추가 값으로 설정합니다. 공유 네트워크 그룹과 연결된 모든 디바이스가 자동으로 할당됩니다.
  - **Override Values**(값 재정의)에서 ▲ 화살표를 클릭하여 공유 네트워크 그룹의 기본 개체로 푸시하고 설정합니다.
  - 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 7 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).

## 네트워크 개체 및 그룹 삭제

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지에서 네트워크 개체나 그룹을 삭제하면

**Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며, 그 반대의 경우도 마찬가지입니다.

## 애플리케이션 필터 개체

애플리케이션 필터 개체는 Firepower 디바이스에서 사용됩니다. 애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.

개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

애플리케이션 필터 개체를 사용하지 않고 정책에서 애플리케이션과 애플리케이션 필터를 직접 선택할 수 있습니다. 그러나 애플리케이션 또는 필터의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다. 시스템에는 수정하거나 삭제할 수 없는 사전 정의된 여러 애플리케이션 필터가 포함되어 있습니다.



**Note** Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.



**Note** FDM 관리 FTD 디바이스가 CDO에 온보딩되면 액세스 규칙 또는 SSL 암호 해독에 정의된 규칙을 변경하지 않고 애플리케이션 필터를 애플리케이션 필터 개체로 변환합니다. 구성 변경으로 인해 디바이스의 구성 상태가 '동기화되지 않음'으로 변경되며 CDO에서 구성 구축이 필요합니다. 일반적으로 FDM은 필터를 수동으로 저장할 때까지 애플리케이션 필터를 애플리케이션 필터 개체로 변환하지 않습니다.

관련 정보:

- Firepower 애플리케이션 필터 개체 생성 및 편집
- 개체 삭제

## Firepower 애플리케이션 필터 개체 생성 및 편집

애플리케이션 필터 개체를 사용하면 직접 선택한 애플리케이션 또는 필터로 식별된 애플리케이션 그룹을 대상으로 지정할 수 있습니다. 이 애플리케이션 필터 개체는 정책에서 사용할 수 있습니다.

### Firepower 애플리케이션 필터 개체 생성

애플리케이션 필터 개체를 만들려면 다음 절차를 따르십시오.

#### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 **Create Object(개체 생성) > FTD > Application Service(애플리케이션 서비스)**를 클릭합니다.

단계 3 개체의 개체 이름 및 설명(선택 사항)을 입력합니다.

단계 4 **Add Filter(필터 추가)**를 클릭하고 개체에 추가할 애플리케이션 및 필터를 선택합니다.

초기 목록(계속 스크롤 가능)에는 애플리케이션이 표시됩니다. 고급 필터를 클릭하면 필터 옵션을 확인하고 애플리케이션을 더 쉽게 선택할 수 있는 보기를 표시할 수 있습니다. 원하는 항목을 선택한 후 **Add(추가)**를 클릭합니다. 이 프로세스를 반복하여 애플리케이션이나 필터를 더 추가할 수 있습니다.

**Note** 단일 필터 기준으로 여러 선택 항목이 OR 관계를 갖습니다. 예를 들어 위험은 높음 OR 매우 높음입니다. 반면 필터 간의 관계는 AND입니다. 즉, 위험은 높음 OR 매우 높음 AND 사업 타당성은 낮음 OR 매우 낮음과 같습니다. 필터를 선택하면 디스플레이의 애플리케이션 목록이 업데이트되어 기준을 충족하는 애플리케이션만 표시됩니다. 이러한 필터를 사용하여 개별적으로 추가하려는 애플리케이션을 찾거나, 규칙에 추가할 적절한 필터를 선택하고 있는지를 확인할 수 있습니다.

**Filter Applications**

Risks: High, Very High

Categories: ad portal

Business Relevance: Very Low, Low

Tags: displays ads

Types: Web Application

Filter the list of applications

4 matches

Application Name	Description
MyWay	Adware and spyware, categorized as an internet browser hijacker.
Olx.pl	Platform to connect local people to buy, sell or exchange used goods and services through their mobile phone or on the web.
PopAds	Advertising network specialized in popunders on the Internet.
PopCash	Advertising platform.

Cancel OK

**위험:** 애플리케이션이 조직의 보안 정책에 위배되는 목적으로 사용될 가능성은 매우 낮음에서 매우 높음까지입니다.

**비즈니스 관련성:** 애플리케이션이 오락용이 아니라 조직의 비즈니스 운영 컨텍스트 내에서 사용될 가능성은 매우 낮음에서 매우 높음까지입니다.

**유형:** 애플리케이션 유형

- **애플리케이션 프로토콜:** 호스트 간의 통신을 나타내는 HTTP 및 SSH와 같은 애플리케이션 프로토콜.
- **클라이언트 프로토콜:** 호스트에서 실행 중인 소프트웨어를 나타내는 웹 브라우저 및 이메일 클라이언트와 같은 클라이언트.
- **웹 애플리케이션:** HTTP 트래픽에 대한 콘텐츠 또는 요청된 URL을 나타내는 MPEG 비디오 및 Facebook과 같은 웹 애플리케이션.

**범주:** 가장 필수적인 기능을 설명하는 애플리케이션의 일반적인 분류.

**태그:** 카테고리과 유사한 애플리케이션에 대한 추가 정보.

암호화된 트래픽의 경우, 시스템은 SSL Protocol(SSL 프로토콜) 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 또한 암호화된 트래픽 또는 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에는 암호 해독된 트래픽 태그가 할당됩니다.

애플리케이션 목록(디스플레이 하단): 목록 위의 옵션에서 필터를 선택하면 이 목록이 업데이트되므로 현재 필터와 일치하는 애플리케이션을 볼 수 있습니다. 이 목록을 사용하여 규칙에 필터 기준을 추가하려는 경우 필터가 적절한 애플리케이션을 대상으로 하는지를 확인할 수 있습니다. 개체에 특정 애플리케이션을 추가하려면 필터링된 목록에서 선택합니다. 애플리케이션을 선택하면 필터가 더 이상 적용되지 않습니다. 필터 자체가 개체가 되도록 하려면 목록에서 애플리케이션을 선택하지 마십시오. 그런 다음 개체는 필터로 식별된 모든 애플리케이션을 나타냅니다.

단계 5 **OK**(확인)를 클릭하여 변경 사항을 저장합니다.


## Firepower 애플리케이션 필터 개체 편집

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 편집할 개체를 선택합니다.

단계 4 세부정보 패널의 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.

단계 5 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 6 **Save**(저장)를 클릭합니다.

단계 7 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

### 관련 정보:

- [개체](#)
- [개체 필터](#)
- [개체 삭제](#)

## 지리위치 개체

지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소만을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다. 지리적 위치를

사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

일반적으로는 지리위치 개체를 사용하지 않고 정책에서 직접 지리적 위치를 선택합니다. 그러나 국가와 대륙의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다.

#### 지리위치 데이터베이스 업데이트

최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다. 현재는 Cisco Defense Orchestrator를 사용하여 수행할 수 있는 작업이 아닙니다. GeoDB 및 업데이트 방법에 대한 자세한 내용은 [디바이스가 실행 중인 버전의 Firepower Device Manager용 Cisco Firepower Threat Defense 설정 가이드](#)의 다음 섹션을 참조하십시오.

- 시스템 데이터베이스 및 피드 업데이트
- 시스템 데이터베이스 업데이트

## Firepower 지리위치 필터 개체 생성 및 편집

개체 페이지에서 또는 보안 정책을 생성할 때 지리위치 개체를 생성할 수 있습니다. 이 절차에서는 개체 페이지에서 지리위치 개체를 생성합니다.

지리위치 개체를 생성하려면 다음 단계를 수행합니다.

#### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 **Create Object(개체 생성) > FTD > Geolocation(지리위치)**을 클릭합니다.
- 단계 3 개체의 개체 이름 및 설명(선택 사항)을 입력합니다.
- 단계 4 필터 표시줄에서 국가 또는 지역의 이름을 입력하기 시작하면 가능한 일치 목록이 표시됩니다.
- 단계 5 개체에 추가할 국가 또는 지역을 선택합니다.
- 단계 6 **Add(추가)**를 클릭합니다.

## 지리위치 개체 편집

#### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 필터 창과 검색 필드를 사용하여 개체를 찾습니다.
- 단계 3 작업 창에서 **Edit(편집)**를 클릭합니다.
- 단계 4 개체의 이름을 변경하고 개체에 국가 및 지역을 추가하거나 제거할 수 있습니다.
- 단계 5 **Save(저장)**를 클릭합니다.

단계 6 장치가 영향을 받는 경우 알림을 받게 됩니다. **OK(확인)**를 클릭합니다.

단계 7 장치 또는 정책이 영향을 받은 경우 **Inventory(인벤토리)** 페이지를 열고 장치에 대한 변경 사항을 미리 보고 배포합니다.

## DNS 그룹 개체

DNS(Domain Name System) 그룹은 DNS 서버 및 일부 관련 특성의 목록을 정의합니다. `www.example.com` 과 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인하려면 DNS 서버가 필요합니다. 관리 및 데이터 인터페이스에 대해 서로 다른 DNS 그룹 개체를 구성할 수 있습니다.

새 DNS 그룹 개체를 생성하기 전에 FDM 관리 디바이스에 DNS 서버가 구성되어 있어야 합니다. Cisco Defense Orchestrator(CDO)의 **DNS 서버 구성**에 DNS 서버를 추가하거나 firewall device manager에서 DNS 서버를 생성한 다음 FDM 관리 구성을 CDO에 동기화할 수 있습니다. firewall device manager에서 DNS 서버 설정을 생성하거나 수정하려면 **Cisco Firepower Device Manager 구성 가이드**, 버전 6.4 이상의 데이터 및 관리 인터페이스에 대한 **DNS 구성**을 참조하십시오.

## DNS 그룹 개체 생성

CDO에서 새 DNS 그룹 개체를 생성하려면 다음 절차를 따르십시오.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **FTD > DNS Group(DNS 그룹)**을 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 (선택 사항) 설명을 추가합니다.

단계 6 **DNS 서버의 IP 주소**를 입력합니다. 최대 6개의 DNS 서버를 추가할 수 있습니다. **Add DNS Server(DNS 서버 추가)**를 클릭합니다. 서버 주소를 제거하려면 삭제 아이콘을 클릭합니다.

**Note** 목록은 우선순위에 따라 나열됩니다. 목록의 첫 번째 서버가 항상 사용되며, 그다음 서버는 위에 있는 서버에서 응답이 수신되지 않는 경우에만 사용됩니다. 최대 6개의 서버를 추가할 수 있지만 나열된 처음 3개의 서버만 관리 인터페이스에 사용됩니다.

단계 7 도메인 검색 이름을 입력합니다. 이 도메인은 정규화되지 않은 호스트 이름(예: `serverA.example.com` 이 아닌 `serverA`)에 추가됩니다.

단계 8 재시도 횟수를 입력합니다. 시스템이 응답을 받지 못한 경우 DNS 서버 목록을 재시도하는 횟수(0~10)입니다. 기본값은 2입니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.

단계 9 시간 초과 값을 입력합니다. 다음 DNS 서버를 시도하기 전에 기다리는 시간(1~30초)입니다. 기본값은 2초입니다. 시스템이 서버 목록을 재시도할 때마다 이 시간 초과 값이 두 배로 늘어납니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.

단계 10 Add(추가)를 클릭합니다.


## DNS 그룹 개체 편집

Cisco Defense Orchestrator 또는 firewall device manager에서 생성된 DNS 그룹 개체를 편집할 수 있습니다. 기존 DNS 그룹 개체를 편집하려면 다음 절차를 따르십시오.

### Procedure

단계 1 왼쪽 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 **DNS Group Object(DNS 그룹 개체)**를 찾습니다.

단계 3 개체를 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 다음 항목을 편집합니다.

- 개체 이름
- 설명
- DNS 서버 이 목록에서 DNS 서버를 편집, 추가 또는 제거할 수 있습니다.
- 도메인 검색 이름
- 재시도.
- 시간이 초과되었습니다.

단계 5 **Save(저장)**를 클릭합니다.

단계 6 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).


## DNS 그룹 개체 삭제

CDO에서 DNS 그룹 개체를 삭제하려면 다음 절차를 따르십시오.

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 **DNS Group Object(DNS 그룹 개체)**를 찾습니다.

단계 3 개체를 선택하고 **Remove(제거)** 아이콘  를 클릭합니다.



단계 4 DNS 그룹 개체를 삭제할 것인지 확인하고 **Ok(확인)**를 클릭합니다.

단계 5 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

## DNS 그룹 개체를 FDM-관리 DNS 서버로 추가

데이터 인터페이스 또는 관리 인터페이스에 대한 기본 설정 DNS 그룹으로 DNS 그룹 개체를 추가할 수 있습니다. 자세한 내용은 [FDM-관리 디바이스 설정](#)을 참조하십시오.

## 인증서 개체

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.

디바이스에서 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 [재사용 가능한 개체](#) 장의 인증서 정보 및 인증서 구성 섹션을 참조하십시오.

## 인증서 정보

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. 디지털 인증서는 사용자 또는 디바이스의 공개 키 사본 하나도 포함합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.

다음과 같은 인증서 유형을 생성할 수 있습니다.

- 내부 인증서 - 내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.

시스템은 그대로 사용하거나 대체할 수 있는 사전 정의된 내부 인증서 **DefaultInternalCertificate** 및 **DefaultWebServerCertificate**와 함께 제공됩니다.

- 내부 CA(Certificate Authority) - 내부 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.

시스템은 **NGFW-Default-InternalCA**와 같은 미리 정의된 내부 CA 인증서와 함께 제공되며, 이를 그대로 사용하거나 교체할 수 있습니다.

- 신뢰할 수 있는 CA(Certificate Authority) 인증서 - 신뢰할 수 있는 CA 인증서는 다른 인증서에 서명하는 데 사용됩니다. 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.

CA(인증 증명)는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 컨텍스트에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다. CA는 VeriSign과 같이 신뢰받는 서드파티이거나, 조직 내에서 설정한 전용 (내부) CA일 수 있습니다. CA는 인증서 요청을 관리하고 디지털 인증서를 발급하는 기능을 담당합니다.

시스템에는 서드파티 인증 증명에서 제공되는 수많은 신뢰할 수 있는 CA 인증서도 포함됩니다. 이러한 인증서는 Decrypt Re-Sign(암호 해독 재서명) 작업을 위한 SSL 암호 해독 정책에서 사용됩니다.

자세한 내용은 디바이스가 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 재사용 가능한 개체 장의 기능에서 사용하는 인증서 유형 섹션을 참조하십시오.

## 기능에 사용되는 인증서 유형

각 기능에 대해 적절한 유형의 인증서를 생성해야 합니다. 인증서가 필요한 기능은 다음과 같습니다.

### ID 정책(캡티브 포털) - 내부 인증서

(선택 사항). 캡티브 포털은 ID 정책에 사용됩니다. 사용자는 신원을 증명하고 IP 주소를 사용자 이름과 연결하기 위해 디바이스에 인증할 때 이 인증서를 수락해야 합니다. 인증서를 제공하지 않으면 디바이스는 자동으로 생성된 인증서를 사용합니다.

### SSL 암호 해독 정책 — 내부, 내부 CA 및 신뢰할 수 있는 CA 인증서

(필수) SSL 암호 해독 정책은 다음 목적을 위해 인증서를 사용합니다.

- 내부 인증서는 알려진 키 암호 해독 규칙에 사용됩니다.
- 내부 CA 인증서는 클라이언트와 디바이스 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 사용됩니다.
- 신뢰할 수 있는 CA 인증서
  - 신뢰할 수 있는 CA 인증서는 디바이스와 서버 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 간접적으로 사용됩니다. 다른 인증서와 달리 이러한 인증서는 SSL 암호 해독 정책에서 직접 구성하지 않고 시스템에 업로드하기만 하면 됩니다. 시스템에는 신뢰할 수 있는 CA 인증서가 많이 포함되어 있으므로 추가 인증서를 업로드할 필요가 없을 수도 있습니다.
  - Active Directory 영역 개체를 생성하고 암호화를 사용하도록 디렉터리 서버를 구성할 때.

## 인증서 구성

ID 정책 또는 SSL 암호 해독 정책에 사용되는 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다. 필요한 경우 OpenSSL을 사용하여 인증서를 생성하거나 신뢰할 수 있는 인증 기관에서 가져오거나 자체 서명된 인증서를 생성할 수 있습니다.

다음 절차를 사용하여 인증서 개체를 구성합니다.

- 내부 및 내부 CA 인증서 업로드
- 신뢰할 수 있는 CA 인증서 업로드
- 자체 서명 내부 및 내부 CA 인증서 생성
- 인증서를 보거나 편집하려면 인증서의 편집 아이콘 또는 보기 아이콘을 클릭합니다.
- 참조되지 않는 인증서를 삭제하려면 해당 인증서의 삭제 아이콘을 클릭합니다. **개체 삭제**를 참조하십시오.

## 내부 및 내부 CA 인증서 업로드

내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.

내부 CA(Certificate Authority) 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 [기능에 사용되는 인증서 유형](#)을 참조하십시오.


### 절차

이 절차에서는 인증서 파일을 업로드하거나 기존 인증서 텍스트를 텍스트 상자에 붙여넣어 내부 또는 내부 CA 인증서를 생성합니다. 자체 서명된 인증서를 생성하려면 [자체 서명 내부 및 내부 CA 인증서 생성](#)을 참조하십시오.

내부 또는 내부 CA 인증서 개체를 만들거나 새 인증서 개체를 정책에 추가하려면 다음 절차를 따르십시오.

#### Procedure

단계 1 다음 중 하나를 수행합니다.

- 개체 페이지에서 인증서 개체를 생성합니다.
  - a. 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
  - b. 플러스 버튼 를 클릭하고 **FTD > Certificate(인증서)**를 선택합니다.
- 정책에 새 인증서 개체를 추가할 때 **Create New Object(새 개체 생성)**를 클릭합니다.

단계 2 인증서의 **Name(이름)**을 입력합니다. 이름은 구성에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 3 1단계에서 내부 인증서 또는 내부 CA를 선택합니다.

단계 4 2단계에서 **Upload**(업로드)를 선택하여 인증서 파일을 업로드합니다.

단계 5 3단계에서 서버 인증서 영역의 텍스트 상자에 인증서 내용을 붙여넣거나 마법사의 설명에 따라 인증서 파일을 업로드합니다. 텍스트 상자에 인증서를 붙여넣는 경우 인증서에 BEGIN CERTIFICATE 및 END CERTIFICATE 줄이 포함되어야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIICMTCCAzoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFAADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQv21kZ210
(...5 lines removed...)
shGJDReryJQqilHHzrYTWZAYTrD7NQPhtK+ZiJng67cPgnNDuXEn55UwMOQoHbP
HMUwmhiGZLzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02Ceba6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfwxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
v1k3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

단계 6 3단계의 인증서 키 영역에서 키 내용을 인증서 키 텍스트 상자에 붙여넣거나 마법사의 설명에 따라 키 파일을 업로드합니다. 텍스트 상자에 키를 붙여넣는 경우 키에는 BEGIN PRIVATE KEY 또는 BEGIN RSA PRIVATE KEY 및 END PRIVATE KEY 또는 END PRIVATE KEY 행이 포함되어야 합니다.

**Note** 키는 암호화할 수 없습니다.

단계 7 **Add**(추가)를 클릭합니다.

## 신뢰할 수 있는 CA 인증서 업로드

신뢰할 수 있는 CA(Certificate Authority) 인증서는 다른 인증서에 서명하는 데 사용되며, 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.


이러한 인증서를 사용하는 기능에 대한 자세한 내용은 [기능에 사용되는 인증서 유형](#)을 참조하십시오.

외부 인증 기관으로부터 신뢰할 수 있는 CA 인증을 획득하거나, OpenSSL 도구 등 자체 내부 CA를 사용하여 CA 인증을 생성합니다. 그런 다음, 아래 절차를 사용하여 인증서를 업로드합니다.

### 절차

#### Procedure

단계 1 다음 중 하나를 수행합니다.

- 개체 페이지에서 인증서 개체를 생성합니다.
  - a. 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.
  - b. 플러스 버튼 를 클릭하고 **FTD > Certificate**(인증서)를 선택합니다.

- 정책에 새 인증서 개체를 추가할 때 **Create New Object**(새 개체 생성)를 클릭합니다.

**단계 2** 인증서의 **Name**(이름)을 입력합니다. 이름은 구성에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

**단계 3** 1단계에서 **External CA Certificate**(외부 CA 인증서)를 선택하고 **Continue**(계속)를 클릭합니다. 마법사가 3단계로 진행합니다.

**단계 4** 3단계의 **Certificate Contents**(인증서 내용) 영역에서 텍스트 상자에 인증서 내용을 붙여넣거나 마법사의 설명에 따라 인증서 파일을 업로드합니다.

인증서는 다음 지침을 따라야 합니다.

- 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.
- 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.
- 붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTA1VTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjE2LjEuMTEUMBIGA1UEAwLMTKyLjE2OC4xLjEwHhcNMjYxMjMjIzNDE3
WhcNMjYxMjMjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBACMBmF1c3RpbjEUMBIGA1UECgwLTKyLjE2OC4xLjEwExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GpkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6H0gKlOwXbRvOdkstzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

**단계 5 Add**(추가)를 클릭합니다.

## 자체 서명 내부 및 내부 CA 인증서 생성

내부 **ID** 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 **OpenSSL** 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.

내부 **CA(Certificate Authority)** 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 **OpenSSL** 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.

**OpenSSL**을 사용하여 이러한 인증서를 생성하거나, 신뢰할 수 있는 CA에서 인증서를 가져오고 업로드할 수 있습니다. 자세한 내용은 **내부 및 내부 CA 인증서 업로드**를 참조하십시오.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 **기능에 사용되는 인증서 유형**을 참조하십시오.



**Note** 새로운 자체 서명 인증서는 유효 기간이 5년으로 생성됩니다. 만료되기 전에 인증서를 교체하십시오.



**Warning** 자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 [새 인증서 탐지됨](#)을 참조하십시오.


## 절차

이 절차는 마법사에서 적절한 인증서 필드 값을 입력하여 자체 서명된 인증서를 생성합니다. 인증서 파일을 업로드하여 내부 또는 내부 CA 인증서를 생성하려면 [내부 및 내부 CA 인증서 업로드](#)를 참조하십시오.

자체 서명된 인증서를 생성하려면 다음 절차를 따르십시오.

### Procedure

단계 1 다음 중 하나를 수행합니다.

- 개체 페이지에서 인증서 개체를 생성합니다.
  - a. 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
  - b. 플러스 버튼 를 클릭하고 **FTD > Certificate(인증서)**를 선택합니다.
- 정책에 새 인증서 개체를 추가할 때 **Create New Object(새 개체 생성)**를 클릭합니다.

단계 2 인증서의 **Name(이름)**을 입력합니다. 이름은 구성에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 3 1단계에서 내부 인증서 또는 내부 CA를 선택합니다.

단계 4 2단계에서 **Self-Signed(자체 서명됨)**을 선택하여 이 단계에서 자체 서명된 인증서를 생성합니다.

단계 5 인증서 주체와 발급자 정보에 다음 중 한 가지 이상의 정보를 구성합니다.

- 국가(C)- 드롭다운 목록에서 국가 코드를 선택합니다.
- State or Province(주/도)(ST) - 인증서에 포함할 주/도.
- Locality or City(구/군/시)(L) - 인증서에 포함할 구/군/시(예: 도시 이름).
- Organization(조직)(O) - 인증서에 포함할 조직 또는 회사 이름.
- Organizational Unit(Department)(조직 단위(부서))(OU) - 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.

- Common Name(공용 이름)(CN) - 인증서에 포함할 X.509 일반 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.

단계 6 Add(추가)를 클릭합니다.

## IPsec 제안 구성

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성하여 선택합니다.
- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.



**Note** IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

- [IKEv1 IPsec 제안 개체 관리](#)
- [IKEv2 IPsec 제안 개체 관리](#)

## IKEv1 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 CDO(Cisco Defense Orchestrator)는 IKEv1 IPsec 제안 개체를 지원합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.



**Note** IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

### Related Topics

[IKEv1 IPsec 제안 개체 생성 또는 편집](#), 483 페이지

## IKEv1 IPsec 제안 개체 생성 또는 편집


여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv1 Proposal**(새 IKEv1 제안 생성) 링크를 클릭하여 사이트 투 사이트 VPN 연결에서 IKEv1 IPsec 설정을 편집하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv1 IPsec Proposal**(제안)을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit**(편집)를 클릭합니다.

단계 3 새 개체의 개체 이름을 입력합니다.

단계 4 IKEv1 IPsec 제안 개체가 작동하는 모드를 선택합니다.

- 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPsec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec이 구현되는 통상적인 방식입니다.
- 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPsec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.

단계 5 이 제안에 대한 **ESP Encryption**(ESP 암호화)(Encapsulating Security Protocol) 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#), on page 471를 참조하십시오.



단계 6 인증에 사용할 **ESP Hash(ESP 해시)** 또는 무결성 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정, on page 472](#)를 참조하십시오.

단계 7 **Add(추가)**를 클릭합니다.

## IKEv2 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

### Related Topics

[IKEv2 IPsec 제안 개체 생성 또는 편집, 484 페이지](#)

## IKEv2 IPsec 제안 개체 생성 또는 편집


여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IPsec Proposal(새 IPsec 제안 생성)** 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 편집하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv2 IPsec Proposal(제안)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(편집)**를 클릭합니다.

단계 3 새 개체의 개체 이름을 입력합니다.

단계 4 IKE2 IPsec 제안 개체 구성:

- Encryption(암호화)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정, on page 471](#)를 참조하십시오.

- **Integrity Hash**(무결성 해시) - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정, on page 472](#)를 참조하십시오.

단계 5 **Add**(추가)를 클릭합니다.

## 글로벌 IKE 정책 구성

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 **Edit**(수정)을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

다음 항목에서는 각 버전에 대해 IKE 정책을 구성하는 방법에 대해 설명합니다.

- [IKEv1 정책 관리](#)
- [IKEv2 정책 관리](#)

## IKEv1 정책 관리

IKEv1 정책을 생성하고 편집하는 방법을 설명합니다.

### IKEv1 정책 정보

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이

며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 **State(상태)** 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

### Related Topics

[IKEv1 정책 생성 또는 편집](#), 479 페이지


## IKEv1 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy(새 IKE 정책 생성)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv1 정책을 생성할 수도 있습니다.

### Procedure

**단계 1** 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

**단계 2** 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv1 Policy(IKEv1 정책)**를 선택하여 새 IKEv1 정책을 생성합니다.
- 개체 페이지에서 편집할 IKEv1 정책을 선택하고 오른쪽의 **Actions(작업)** 창에서 **Edit(편집)**를 클릭합니다.

**단계 3** 개체 이름을 최대 128자로 입력합니다.

**단계 4** IKEv1 속성을 구성합니다.

- **Priority(우선순위)**-IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에서 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Encryption(암호화)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 과생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Lifetime(라이프타임)**-SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다.

다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

- **Authentication(인증)** - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 [사용할 인증 방법 결정, on page 473](#)를 참조하십시오.
  - **Preshared Key(사전 공유 키)** - 각 디바이스에 정의된 사전 공유 키를 사용합니다. 이 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.
  - **Certificate(인증서)** - 서로 식별할 피어에 대해 디바이스 ID 인증서를 사용합니다. Certificate Authority에서 각 피어를 등록하여 이 인증서를 가져와야 합니다. 또한 각 피어에서 ID 인증서 서명에 사용되는 신뢰할 수 있는 CA 루트 및 중간 CA 인증서를 업로드해야 합니다. 피어는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.
- **Hash(해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 [VPN에서 사용되는 암호화 및 해시 알고리즘, on page 470](#)를 참조하십시오.

단계 5 **Add(추가)**를 클릭합니다.

## IKEv2 정책 관리

IKEv2 정책을 생성하고 편집하는 방법을 설명합니다.

### IKEv2 정책 정보

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 **State(상태)** 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

### Related Topics

[IKEv2 정책 생성 또는 편집, 481 페이지](#)


## IKEv2 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv2 Policy(새 IKEv2 정책 생성)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv2 정책을 생성할 수도 있습니다.

## Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv2 Policy(FTD IKEv2 정책)**를 선택하여 새 IKEv2 정책을 생성합니다.
- 개체 페이지에서 수정할 IKEv2 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit(편집)**를 클릭합니다.

단계 3 개체 이름을 최대 128자로 입력합니다.

단계 4 IKEv2 속성을 구성합니다.

- **Priority(우선순위)**-IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에서 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **State(상태)** - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Encryption(암호화)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을 둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는 반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정, on page 471](#)를 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 Diffie-Hellman 모듈러스 그룹 결정, on page 472](#)를 참조하십시오.
- **Integrity Hash(무결성 해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 [VPN에서 사용되는 암호화 및 해시 알고리즘, on page 470](#)를 참조하십시오.
- **PRF(Pseudo-Random Function) 해시** - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해서도 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피

어와 협상을 합니다. 옵션에 대한 설명은 [VPN에서 사용되는 암호화 및 해시 알고리즘](#), on page 470를 참조하십시오.

- **Lifetime**(라이프타임)-SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 5 **Add**(추가)를 클릭합니다.

## RA VPN 개체

### 보안 영역 개체

보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 여러 영역을 정의할 수 있지만, 지정된 인터페이스는 하나의 영역에만 속할 수 있습니다.

Firepower System은 초기 구성 중에 다음 영역을 생성하며 Defense Orchestrator의 개체 페이지에 표시됩니다. 영역을 편집하여 인터페이스를 추가하거나 제거할 수도 있고, 더 이상 사용하지 않는 영역을 삭제할 수도 있습니다.

- **inside\_zone** - 내부 인터페이스를 포함합니다. 이 영역은 내부 네트워크를 나타내는 데 사용됩니다.
- **outside\_zone** - 외부 인터페이스를 포함합니다. 이 영역은 인터넷 등 제어 범위 외부에 있는 네트워크를 나타내는 데 사용됩니다.

일반적으로는 인터페이스가 네트워크에서 수행하는 역할별로 인터페이스를 그룹화합니다. 예를 들어 인터넷에 연결하는 인터페이스는 **outside\_zone** 보안 영역에 배치하고 내부 네트워크용의 모든 인터페이스는 **inside\_zone** 보안 영역에 배치합니다. 그러면 외부 영역에서 들어오는 트래픽과 내부 영역으로 이동하는 트래픽에 액세스 제어 규칙을 적용할 수 있습니다.

영역을 생성하기 전에 네트워크에 적용할 액세스 규칙 및 기타 정책을 고려하십시오. 예를 들어 모든 내부 인터페이스를 같은 영역에 배치할 필요는 없습니다. 내부 네트워크가 4개인데 그중 하나를 나머지 3개와 다른 방식으로 취급하려는 경우에는 영역을 하나가 아닌 두 개 생성할 수 있습니다. 공개 웹 서버에 대한 외부 액세스를 허용해야 하는 인터페이스가 있는 경우에는 해당 인터페이스용으로 별도의 영역을 사용할 수 있습니다.

관련 정보:

- [Firepower 보안 영역 개체 생성 또는 편집](#)

- 보안 영역에 Firepower 인터페이스 할당
- 개체 삭제

## Firepower 보안 영역 개체 생성 또는 편집


보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 여러 영역을 정의할 수 있지만, 지정된 인터페이스는 하나의 영역에만 속할 수 있습니다. 자세한 내용은 [보안 영역 개체](#)를 참조하십시오.

보안 영역 개체는 해당 디바이스에 대한 규칙에서 사용되지 않는 한 디바이스와 연결되지 않습니다.

### 보안 영역 개체 생성

보안 영역 개체를 생성하려면 다음 지침을 따르십시오.

#### Procedure



- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 파란색 플러스 버튼  을 클릭하고 **FTD > Security Zone(보안 영역)**을 선택하여 새 개체를 생성합니다.
- 단계 3 개체의 이름과 설명(선택 사항)을 입력합니다.
- 단계 4 보안 영역에 넣을 인터페이스를 선택합니다.
- 단계 5 **Add(추가)**를 클릭합니다.

### 보안 영역 개체 편집

FDM 관리 디바이스를 온보딩한 후 이미 두 개 이상의 보안 영역이 있음을 알 수 있습니다. 하나는 `inside_zone`이고 다른 하나는 `outside_zone`입니다. 이러한 영역은 편집하거나 삭제할 수 있습니다. 보안 영역 개체를 편집하려면 다음 지침을 따르십시오.


#### Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 편집할 개체를 찾습니다.
  - 개체의 이름을 알고 있는 경우 개체 페이지에서 검색할 수 있습니다.
  - 보안 영역별로 목록을 필터링합니다.
  - 검색 필드에 개체 이름을 입력합니다.
  - 개체를 선택합니다.

- 개체가 디바이스와 연결되어 있는 경우 **Inventory**(인벤토리) 페이지에서 시작하여 개체를 검색할 수 있습니다.
  - 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
  - **Devices**(디바이스) 탭을 클릭합니다.
  - 해당 탭을 클릭합니다.
  - 디바이스 **필터** 및 **검색** 표시줄을 사용하여 디바이스를 찾습니다.
  - 디바이스를 선택합니다.
- 오른쪽의 관리 창에서  **Objects**(개체)를 클릭합니다.
- 개체 **필터**  과 **검색** 표시줄을 사용하여 찾고 있는 개체를 찾습니다.

**Note**      생성한 보안 영역 개체가 디바이스에 대한 정책의 규칙과 연결되지 않은 경우 "연결되지 않은" 것으로 간주되어 디바이스 검색 결과에 표시되지 않습니다.

단계 3 개체를 선택합니다.

단계 4 우측의 작업 창에서 **Edit**(편집) 아이콘  를 클릭합니다.

단계 5 개체의 속성을 편집한 후, **Save**(저장)를 클릭합니다.

단계 6 저장을 클릭하면 이러한 변경 사항이 다른 디바이스에 어떤 영향을 미치는지 설명하는 메시지가 표시됩니다. **Confirm**(확인)을 클릭하여 변경 사항을 저장하거나 취소합니다.

## 서비스 개체

### Firepower 서비스 개체

FTD 서비스 개체, 서비스 그룹 및 포트 그룹은 IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다.

FTD 서비스 그룹은 서비스 개체의 모음입니다. 서비스 그룹은 하나 이상의 프로토콜에 대한 개체를 포함할 수 있습니다. 이러한 개체 및 그룹을 보안 정책에서 사용하여 네트워크 트래픽 일치 기준(예: 특정 TCP 포트에 대한 트래픽을 허용하는 액세스 규칙을 사용하기 위한 기준)을 정의할 수 있습니다. 시스템에는 일반 서비스를 위해 사전 정의된 개체가 여러 개 포함되어 있으며, 정책에서 이러한 개체를 사용할 수 있지만 시스템 정의 개체를 편집하거나 삭제할 수는 없습니다.

Firepower Device Manager 및 Firepower Management Center는 서비스 개체를 포트 개체 및 서비스 그룹 및 포트 그룹으로 참조하십시오.

자세한 내용은 [Firepower 서비스 개체 생성 및 편집](#)을 참조하십시오.



### 프로토콜 개체

프로토콜 개체는 덜 일반적으로 사용되는 또는 레거시 프로토콜을 포함하는 서비스 개체 유형입니다. 프로토콜 개체는 이름 및 **프로토콜 번호**로 식별됩니다. CDO는 ASA 및 Firepower(FDM 관리) 구성에서 이러한 개체를 인식하고 사용자가 쉽게 찾을 수 있도록 자체 필터인 "프로토콜"을 제공합니다.

자세한 내용은 [Firepower 서비스 개체 생성 및 편집](#)을 참조하십시오.

### ICMP 개체

ICMP(Internet Control Message Protocol) 개체는 ICMP 및 IPv6-ICMP 메시지를 위한 서비스 개체입니다. CDO는 ASA 및 Firepower 구성에서 해당 디바이스가 온보딩되고 사용자가 개체를 쉽게 찾을 수 있도록 해당 디바이스에 "ICMP" 필터를 제공할 때 이러한 개체를 인식합니다.

CDO를 사용하면 ASA 구성에서 ICMP 개체를 제거하거나 이름을 바꿀 수 있습니다. CDO를 사용하여 Firepower 구성에서 ICMP 및 ICMPv6 개체를 생성, 업데이트 및 삭제할 수 있습니다.



**Note** ICMPv6 프로토콜의 경우 AWS는 특정 인수 선택을 지원하지 않습니다. 모든 ICMPv6 메시지를 허용하는 규칙만 지원됩니다.

자세한 내용은 [Firepower 서비스 개체 생성 및 편집](#)을 참조하십시오.

관련 정보:


- [개체 삭제](#), on page 129

## Firepower 서비스 개체 생성 및 편집

Firepower 서비스 개체를 생성하려면 다음 단계를 수행합니다.

firewall device manager(FDM 관리) 서비스 개체는 TCP/IP 프로토콜 및 포트를 지정하는 재사용 가능한 구성 요소입니다. firewall device manager, 온프레미스 Firewall Management Center 및 클라우드 사용 Firewall Management Center는 이러한 개체를 "포트 개체"라고 합니다.

### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 오른쪽에 있는 파란색 버튼  을 클릭하여 개체를 생성하고 **FTD > Service(FTD 서비스)**를 선택합니다.
- 단계 3 개체 이름과 설명을 입력합니다.
- 단계 4 **Create a service object(서비스 개체 생성)**를 선택합니다.
- 단계 5 **Service Type(서비스 유형)** 버튼을 클릭하고 개체를 생성할 프로토콜을 선택합니다.
- 단계 6 다음과 같이 프로토콜을 구성합니다.

- **TCP, UDP**

- **eq**를 선택하고 포트 번호 또는 프로토콜 이름을 입력합니다. 예를 들어 포트 번호로 80을 입력하거나 프로토콜 이름으로 HTTP를 입력할 수 있습니다.
- 범위를 선택한 다음 포트 번호의 범위를 입력할 수도 있습니다(예: **1 65535**(모든 포트 포함)).

- **ICMP, IPv6-ICMP-ICMP** 유형을 선택합니다. 해당 유형을 모든 ICMP 메시지에 적용하려면 모두를 선택합니다. 유형과 코드에 대한 자세한 내용은 다음 페이지를 참조하십시오.

- ICMP-<http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml>
- ICMPv6-<http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml>

- 기타 - 원하는 프로토콜을 선택합니다.

단계 7 **Add**(추가)를 클릭합니다.


단계 8 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## Firepower 서비스 그룹 생성

서비스 그룹은 하나 이상의 프로토콜을 나타내는 하나 이상의 서비스 개체로 구성될 수 있습니다. 서비스 개체를 그룹에 추가하려면 먼저 서비스 개체를 생성해야 합니다. Firepower Device Manager 및 Firepower Management Center에서는 이러한 개체를 "포트 개체"라고 합니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 오른쪽에 있는 파란색 버튼  을 클릭하여 개체를 생성하고 **FTD > Service**(서비스)를 선택합니다.

단계 3 개체 이름과 설명을 입력합니다.

단계 4 **Create a service group**(서비스 그룹 생성)를 선택합니다.

단계 5 **Add Object**(개체 추가)를 클릭하여 그룹에 개체를 추가합니다.


- 위의 **Firepower 서비스 개체 생성 및 편집**에서 수행한 것처럼 **Create**(생성)를 클릭하여 새 개체를 생성합니다.
- 기존 서비스 개체를 그룹에 추가하려면 **Choose**(선택)를 클릭합니다. 개체를 더 추가하려면 이 단계를 반복합니다.

단계 6 서비스 그룹에 서비스 개체 추가를 완료하면 **Add**(추가)를 클릭합니다.

단계 7 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## Firepower 서비스 개체 또는 서비스 그룹 편집

### Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.
- 단계 3 작업 창에서 **Edit(편집)**  를 클릭합니다.
- 단계 4 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.
- 단계 5 **Save(저장)**를 클릭합니다.
- 단계 6 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.
- 단계 7 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 보안 그룹 태그 그룹

### 보안 그룹 태그(Security Group Tags)

#### 보안 그룹 태그 정보

Cisco ISE(Identity Services Engine)를 사용하여 Cisco TrustSec 네트워크에서 트래픽을 분류하기 위해 SGT(Security Group Tag)를 정의하고 사용하는 경우, SGT를 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다. 따라서 IP 주소가 아니라 보안 그룹 멤버십을 기준으로 액세스를 차단하거나 허용할 수 있습니다.

ISE에서는 SGT를 생성하고 호스트 또는 네트워크 IP 주소를 각 태그에 할당할 수 있습니다. SGT를 사용자의 계정에 할당하면 SGT가 사용자의 트래픽에 할당됩니다. ISE 서버에 연결하도록 FDM 관리 디바이스를 구성하고 SGT를 생성한 후 Cisco Defense Orchestrator에서 SGT 그룹을 생성하고 이를 중심으로 액세스 제어 규칙을 작성할 수 있습니다. SGT를 FDM 관리 디바이스에 연결하려면 먼저 ISE의 SXP(SGT Exchange Protocol) 매핑을 구성해야 합니다. 자세한 내용은 현재 실행 중인 버전의 [Cisco ISE\(Identity Services Engine\) 관리자 설명서](#)에서 보안 그룹 태그 교환 프로토콜을 참조하십시오.

FDM 관리 디바이스가 SGT를 액세스 제어 규칙에 대한 트래픽 일치 기준으로 평가하는 경우, 다음 우선순위를 사용합니다.

1. 패킷에 정의된 소스 SGT(있는 경우). 대상 일치하는 이 기술을 사용하여 수행되지 않습니다. SGT를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메시지를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.
2. ISE 세션 디렉토리에서 다운로드된 대로 사용자 세션에 할당된 SGT. 이러한 유형의 SGT 일치에 대한 세션 디렉토리 정보를 수신 대기하려면 해당 옵션을 활성화해야 합니다. 그러나 이 옵션은

처음에 ISE ID 소스를 생성할 때 기본적으로 켜집니다. SGT는 소스 또는 대상과 일치할 수 있습니다. 필수 사항은 아니지만 일반적으로 사용자 ID 정보를 수집하기 위해 AD 영역과 함께 ISE ID 소스를 사용하여 패시브 인증 ID 규칙도 설정합니다.

3. SXP를 사용하여 다운로드한 SGT-IP 주소 매핑. IP 주소가 SGT 범위 내에 있는 경우 트래픽은 SGT를 사용하는 액세스 제어 규칙과 일치합니다. SGT는 소스 또는 대상과 일치할 수 있습니다.



**Note** ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다. SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

### 버전 지원

CDO는 현재 버전 6.5 이상을 FDM 관리실행하는 FDM 매니지드 디바이스에서 SGT 및 SGT 그룹을 지원합니다. FDM 관리 디바이스를 사용하면 버전 6.5 이상에서 ISE 서버를 구성하고 연결할 수 있지만 버전 6.7까지는 UI에서 SGT 구성이 지원되지 않습니다.

FDM 관리 UI에서 이는 버전 6.5 이상을 실행하는 FDM 관리 디바이스가 SGT의 SXP 매핑을 다운로드할 수 있지만, 개체 또는 액세스 제어 규칙에 수동으로 추가할 수 없음을 의미합니다. 버전 6.5 또는 버전 6.6을 실행하는 디바이스의 SGT를 변경하려면 ISE UI를 사용해야 합니다. 그러나 버전 6.5를 실행하는 디바이스가 Cisco Defense Orchestrator에 온보딩된 경우 디바이스와 연결된 현재 SGT를 확인하고 SGT 그룹을 생성할 수 있습니다.

### CDO의 SGT

#### 보안 그룹 태그(Security Group Tags)

SGT는 CDO에서 읽기 전용입니다. CDO에서 SGT를 생성하거나 편집할 수 없습니다. SGT를 생성하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 관리자 설명서](#)를 참조하십시오.

#### SGT 그룹



**Note** FDM 관리 디바이스는 SGT 그룹을 SGT 동적 개체로 지칭합니다. CDO에서는 이러한 태그 목록을 현재 SGT 그룹이라고 합니다. FDM 관리 디바이스 또는 ISE UI를 참조하지 않고 CDO에서 SGT 그룹을 생성할 수 있습니다.

SGT 그룹을 사용하여 ISE가 할당한 SGT를 기준으로 소스 또는 대상 주소를 식별합니다. 그 다음 트래픽 일치 기준을 정의하는 목적으로 액세스 제어 규칙의 개체를 사용할 수 있습니다. ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다.

SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

CDO에서 SGT 그룹을 생성하려면 하나 이상의 SGT가 이미 구성되어 있어야 하며, 사용하려는 디바이스의 FDM 관리 콘솔에 대해 ISE 서버에서 SGT 매핑이 구성되어 있어야 합니다. 둘 이상의 FDM 관리 디바이스가 동일한 ISE 서버와 연결된 경우 SGT 또는 SGT 그룹을 둘 이상의 디바이스에 적용할 수 있습니다. 디바이스가 ISE 서버와 연결되지 않은 경우, SGT 개체를 액세스 제어 규칙에 포함하거나 SGT 그룹을 해당 디바이스 설정에 적용할 수 없습니다.

#### 규칙의 SGT 그룹

SGT 그룹을 액세스 제어 규칙에 추가할 수 있습니다. 이는 소스 또는 대상 네트워크 개체로 나타납니다. 네트워크가 규칙에서 작동하는 방식에 대한 자세한 내용은 [FDM-관리 액세스 제어 규칙의 소스 및 대상 기준](#)을 참조하십시오.

Objects(개체) 페이지에서 SGT 그룹을 생성할 수 있습니다. 자세한 내용은 [SGT 그룹 생성, on page 167](#)를 참조하십시오.

## SGT 그룹 생성

액세스 제어 규칙에 사용할 수 있는 SGT 그룹을 생성하려면 다음 절차를 사용합니다.

### Before you begin

SGT(보안 그룹 태그) 그룹을 생성하기 전에 다음 구성 또는 환경을 구성해야 합니다.

- FDM 관리 디바이스는 버전 6.5 이상을 실행해야 합니다.
- SXP 매핑을 구독하고 변경 사항을 구축하도록 ISE ID 소스를 구성해야 합니다. SXP 매핑을 관리하려면 사용 중인 버전 6.7 이상에 대한 [Firepower Device Manager 구성 가이드](#)의 **ISE**에서 보안 그룹 및 **SXP** 게시 구성을 참조하십시오.
- 모든 SGT는 ISE에서 생성해야 합니다. SGT를 생성하려면 현재 실행 중인 버전의 [Cisco ISE\(Identity Services Engine\) 구성 설명서](#)를 참조하십시오.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **FTD > Network(네트워크)**를 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 (선택 사항) 설명을 추가합니다.

단계 6 **SGT**를 클릭하고 드롭다운 메뉴를 사용하여 그룹에 포함할 모든 해당 SGT를 선택합니다. SGT 이름을 기준으로 목록을 정렬할 수 있습니다.

단계 7 **Save(저장)**를 클릭합니다.

**Note** CDO에서 SGT를 생성하거나 편집할 수 없으며 SGT 그룹에서 추가하거나 제거할 수만 있습니다. SGT를 생성하거나 편집하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 구성 설명서](#)를 참조하십시오.


## SGT 그룹 편집

SGT 그룹을 편집하려면 다음 절차를 따르십시오.

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 SGT 그룹을 찾습니다.

단계 3 SGT 그룹을 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 SGT 그룹을 편집합니다. 그룹과 관련된 이름, 설명 또는 SGT를 편집합니다.

단계 5 **Save(저장)**를 클릭합니다.

**Note** CDO에서 SGT를 생성하거나 편집할 수 없으며 SGT 그룹에서 추가하거나 제거할 수만 있습니다. SGT를 생성하거나 편집하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 구성 설명서](#)를 참조하십시오.

## 액세스 제어 규칙에 SGT 그룹 추가

액세스 제어 규칙에 SGT 그룹을 추가하려면 다음 절차를 따르십시오.


### Procedure

단계 1 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.

단계 2 **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 **FTD** 탭을 클릭하고 SGT 그룹을 추가할 디바이스를 선택합니다.

단계 4 **Management(관리)** 창에서 **Policy(정책)**를 선택합니다.

단계 5 소스 또는 대상 개체에 대한 파란색 플러스 버튼  을 클릭하고 **SGT** 그룹을 선택합니다.

단계 6 개체 필터 및 검색 필드를 사용하여 편집하려는 SGT 그룹을 찾습니다.

단계 7 **Save(저장)**를 클릭합니다.

단계 8 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).

**Note** 추가 SGT 그룹을 생성해야 하는 경우 **Create New Object**(새 개체 생성)를 클릭합니다. **SGT 그룹 생성** 및 규칙에 SGT 그룹 추가에 언급된 필수 정보를 입력하고 SGT 그룹을 규칙에 추가합니다.

## 시스템 로그 서버 개체


FDM 관리 디바이스는 이벤트를 저장할 수 있는 용량이 제한되어 있습니다. 이벤트에 대한 스토리지를 최대화하기 위해 외부 서버를 구성할 수 있습니다. 시스템 로그(syslog) 서버 개체는 연결 지향형 또는 진단 시스템 로그 메시지를 수신할 수 있는 서버를 식별합니다. 로그 수집 및 분석을 위해 syslog 서버를 설정한 경우, Cisco Defense Orchestrator를 사용하여 개체를 생성하여 정의한 후 관련 정책에 이 개체를 사용할 수 있습니다.

## 시스템 로그 서버 개체 생성 및 편집

새 시스템 로그 서버 개체를 생성하려면 다음 단계를 수행합니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 **Create Object**(개체 생성) 버튼  을 클릭합니다.

단계 3 FDM 관리 디바이스 개체 유형에서 **Syslog Server**(시스템 로그 서버)를 선택합니다.

단계 4 시스템 로그 서버 개체 속성을 구성합니다.

- **IP 주소** - syslog 서버의 IP 주소를 입력합니다.
- **Protocol Type**(프로토콜 유형) — 시스템 로그 서버가 메시지를 수신하는 데 사용하는 프로토콜을 선택합니다. TCP를 선택하는 경우 시스템은 syslog 서버를 사용할 수 없는 경우를 인식할 수 있으며, 서버를 다시 사용할 수 있을 때까지 이벤트 전송을 중지합니다.
- **Port Number**(포트 번호) — 시스템 로그에 사용할 유효한 포트 번호를 입력합니다. 시스템 로그 서버가 기본 포트를 사용하는 경우 기본 UDP 포트 514를 입력하거나 기본 TCP 포트 1470을 입력합니다. 서버에서 기본 포트를 사용하지 않는 경우 올바른 포트 번호를 입력합니다. 포트가 1025~65535 범위에 포함되어야 합니다.
- **Select an interface**(인터페이스 선택) - 진단 시스템 로그 메시지를 보내는 데 사용해야 하는 인터페이스를 선택합니다. 연결 및 침입 이벤트는 항상 관리 인터페이스를 사용합니다. 선택하는 인터페이스에 따라 syslog 메시지와 연결되는 IP 주소가 결정됩니다. 아래에 나열된 옵션 중 하나만 선택할 수 있습니다. 둘 다 선택할 수는 없습니다. 다음 옵션 중 하나를 선택합니다.
  - **Data Interface**(데이터 인터페이스) - 진단 syslog 메시지에 대해 선택하는 데이터 인터페이스를 사용합니다. 생성된 목록에서 인터페이스를 선택합니다. 브리지 그룹 멤버 인터페이스를 통해 서버에 액세스할 수 있는 경우에는 BVI(브리지 그룹 인터페이스)를 선택합니다.

진단 인터페이스(물리적 관리 인터페이스)를 통해 서버에 액세스할 수 있는 경우에는 이 옵션 대신 **Management Interface**(관리 인터페이스)를 선택하는 것이 좋습니다. 패시브 인터페이스는 선택할 수 없습니다. 연결 및 침입 시스템 로그 메시지의 경우 소스 IP 주소는 관리 인터페이스용이거나, 데이터 인터페이스를 통해 라우팅하는 경우 게이트웨이 인터페이스용입니다.

- **Management Interface**(관리 인터페이스) - 모든 유형의 syslog 메시지에 대해 가상 관리 인터페이스를 사용합니다. 소스 IP 주소는 관리 인터페이스용이거나, 데이터 인터페이스를 통해 라우팅하는 경우 게이트웨이 인터페이스용입니다.

단계 5 **Add**(추가)를 클릭합니다.


단계 6 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## Syslog 서버 개체 편집

기존 Syslog 서버 개체를 편집하려면 다음 단계를 따르십시오.

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.

단계 2 원하는 Syslog 서버 개체를 찾아 선택합니다. Syslog 서버 개체 유형별로 개체 목록을 필터링  할 수 있습니다.

단계 3 작업 창에서 **Edit**(편집)를 클릭합니다.

단계 4 원하는 대로 편집하고 **Save**(저장)를 클릭합니다.

단계 5 변경 사항을 확인합니다.

단계 6 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

관련 정보:

- [개체 삭제](#)

## SaaS(Secure Logging Analytics)를 위한 시스템 로그 서버 개체 생성

이벤트를 전송할 SEC(Secure Event Connector)의 IP 주소, TCP 포트 또는 UDP 포트를 사용하여 시스템 로그 서버 개체를 생성합니다. 테넌트에 온보딩한 모든 SEC에 대해 하나의 시스템 로그 개체를 생성하지만, 하나의 규칙에서 하나의 SEC를 나타내는 하나의 시스템 로그 개체로만 이벤트를 전송합니다.




### 사전 요구 사항

이 작업은 더 큰 워크플로우의 일부입니다. 시작하기 전에 [FDM-관리 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현, on page 665](#)을 참조하십시오.

## 절차

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 **Create Object(개체 생성)** 버튼  을 클릭합니다.

단계 3 FDM 관리 장치 개체 유형에서 **Syslog Server(Syslog 서버)**를 선택합니다.

단계 4 시스템 로그 서버 개체 속성을 구성합니다. SEC의 이러한 속성을 찾으려면 **Admin(관리) > Secure Connector(보안 커넥터)**를 선택합니다. 그런 다음 syslog 개체를 구성할 보안 이벤트 커넥터를 선택하고 오른쪽의 세부 정보 창을 살펴봅니다.

- IP 주소 - SEC의 IP 주소를 입력합니다.
- 프로토콜 유형 - TCP 또는 UDP를 선택합니다.
- 포트 번호 - TCP를 선택한 경우 포트 10125를 입력하고 UDP를 선택한 경우 10025를 입력합니다.
- 인터페이스 선택 - SEC에 도달하도록 구성된 인터페이스를 선택합니다.

**Note** FDM 관리 장치는 IP 주소당 하나의 syslog 개체를 지원하므로 TCP와 UDP 사용 중에서 선택해야 합니다.

단계 5 **Add(추가)**를 클릭합니다.

### What to do next

SaaS(Secure Logging Analytics)를 구현하고 보안 이벤트 커넥터를 통해 Cisco Cloud로 이벤트를 전송하는 기존 CDO 고객 워크플로우.

## URL 개체

URL 개체 및 URL 그룹은 Firepower 디바이스에서 사용됩니다. URL 개체 및 그룹(URL 개체로 총칭함)을 사용하여 웹 요청의 URL 또는 IP 주소를 정의합니다. 이러한 개체를 사용하여 액세스 제어 정책에서 수동 URL 필터링 또는 보안 인텔리전스 정책에서 차단 기능을 구현할 수 있습니다. URL 개체는 단일 URL 또는 IP 주소를 정의하는 반면 URL 그룹은 여러 URL 또는 IP 주소를 정의할 수 있습니다.

시작하기 전에

URL 개체를 생성할 때는 다음 사항에 유의하십시오.

- 경로를 포함하지 않는 경우(즉, URL에 / 문자가 없음), 이 일치하는 서버의 호스트 이름만을 기준으로 합니다. 호스트 이름은 // 구분자 뒷부분 또는 호스트 이름의 의 뒷부분이 같아야 일치하는 것으로 간주됩니다. 예를 들어 ign.com은 ign.com 및 www.ign.com과 일치하지만 verisign.com과는 일치하지 않습니다.
- 하나 이상의 / 문자를 포함하는 경우, 전체 URL 문자열이 서버 이름, 경로 및 쿼리 파라미터를 비롯한 부분 문자열 일치에 사용됩니다. 그러나 서버가 재구성되고 페이지가 새 경로로 이동될 수 있으므로 개별 웹 페이지 또는 사이트 일부를 차단하거나 허용하기 위해 수동 URL 필터링은 사용하지 않는 것이 좋습니다. 부분 문자열 일치는 예기치 않은 일치로 이어질 수도 있으며, 이 경우에는 URL 개체에 포함하는 문자열도 쿼리 파라미터 내부에 있는 의도하지 않은 서버 또는 문자열의 경로와 일치됩니다.
- 시스템에서는 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 다시 말해, 특정 웹 사이트를 차단하는 경우 애플리케이션 조건을 사용하여 특정 프로토콜을 대상으로 하지 않는 한 해당 웹 사이트에 대한 HTTP 및 HTTPS 트래픽이 모두 차단됩니다. URL 개체를 생성할 때에는 개체 생성 시 프로토콜을 지정할 필요가 없습니다. 예를 들어 <http://example.com> 대신 [example.com](https://example.com)을 사용합니다.
- URL 개체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 개체를 생성합니다. 또한 주체 CN에 포함된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 [www.example.com](https://www.example.com) 대신 [example.com](https://example.com)을 사용하십시오.

그러나 인증서의 주체 일반 이름은 웹 사이트의 도메인 이름과 아무런 관련도 없을 수 있습니다. 예를 들어, [youtube.com](https://youtube.com) 인증서의 주체 일반 이름은 \*.google.com입니다(언제든 변경 가능). URL 필터링 규칙이 암호 해독된 트래픽에서 작동하도록 SSL 암호 해독 정책을 사용하여 HTTPS 트래픽을 암호 해독하면 더 일관성 있는 결과를 얻게 됩니다.



**참고** 인증서 정보를 더 이상 사용할 수 없어 브라우저에서 TLS 세션을 다시 시작하는 경우에는 URL 개체가 HTTPS 트래픽과 일치되지 않습니다. 따라서 URL 개체를 주의하여 구성하더라도 HTTPS 연결에 대해 일관성 없는 결과를 얻을 수 있습니다.

## FDM-관리 URL 개체 생성 또는 편집

URL 개체는 URL 또는 IP 주소를 지정하는 재사용 가능한 구성 요소입니다.

URL 개체를 만들려면 다음 단계를 수행합니다.

### Procedure

- 단계 1 왼쪽 Cisco Defense Orchestrator 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 **Create Object(개체 생성) > FTD > URL**을 클릭합니다.
- 단계 3 개체 이름과 설명을 입력합니다.
- 단계 4 **Create URL object(URL 개체 생성)**를 선택합니다.
- 단계 5 개체의 특정 URL 또는 IP 주소를 입력합니다.
- 단계 6 **Add(추가)**를 클릭합니다.

## Firepower URL 그룹 생성


URL 그룹은 하나 이상의 URL 또는 IP 주소를 나타내는 하나 이상의 URL 개체로 구성될 수 있습니다. Firepower Device Manager 및 Firepower Management Center는 이러한 개체를 "URL 개체"라고도 합니다.

### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 **Create Object(개체 생성) > FTD > URL**을 클릭합니다.
- 단계 3 개체 이름과 설명을 입력합니다.
- 단계 4 **Create a URL group(URL 그룹 생성)**을 선택합니다.
- 단계 5 **Add Object(개체 추가)**를 클릭하고, 개체를 선택하고, **Select(선택)**을 클릭하여 기존 개체를 추가합니다. 개체를 더 추가하려면 이 단계를 반복합니다.
- 단계 6 URL 그룹에 URL 개체 추가를 완료하면 **Add(추가)**를 클릭합니다.

## Firepower URL 개체 또는 URL 그룹 편집

### Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.
- 단계 3 세부 정보 창에서  를 클릭하여 편집합니다.
- 단계 4 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.
- 단계 5 **Save(저장)**를 클릭합니다.

단계 6 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

---



## 2 장

# 디바이스 및 서비스 온보딩

라이브 디바이스와 모델 디바이스를 모두 CDO에 온보딩할 수 있습니다. 모델 디바이스는 CDO를 사용하여 보고 편집할 수 있는 업로드된 구성 파일입니다.

대부분의 라이브 디바이스 및 서비스는 보안 디바이스 커넥터가 CDO를 디바이스 또는 서비스에 연결할 수 있도록 개방형 HTTPS 연결을 필요로 합니다.

SDC 및 해당 상태에 대한 자세한 내용은 [SDC\(Secure Device Connector\)](#), 11 페이지의 내용을 참조하십시오.

이 장에는 다음 섹션이 포함되어 있습니다.

- 위협 방어 디바이스 온보딩, on page 175
- CDO에서 디바이스 삭제, 222 페이지
- 오프라인 관리를 위한 디바이스 컨피그레이션 가져오기, 223 페이지
- FDM-관리 디바이스 백업, on page 223
- FDM 소프트웨어 업그레이드 경로, on page 229
- FDM-관리 디바이스 업그레이드 사전 요건, on page 232
- 단일 FTD 디바이스 업그레이드, on page 233
- 대량 FDM-관리 디바이스 업그레이드, on page 235
- FDM-관리 고가용성 쌍 업그레이드, on page 238
- Snort 3.0으로 업그레이드, on page 241
- FDM-관리 디바이스용 Snort 3.0에서 되돌리기, on page 245
- 보안 데이터베이스 업데이트 예약, on page 246

## 위협 방어 디바이스 온보딩



### Attention

Secure Firewall device manager(FDM) 지원 및 기능은 요청 시에만 제공됩니다. 테넌트에서 Firewall Device Manager 지원을 아직 활성화하지 않은 경우 디바이스를 관리하거나 FDM 관리 디바이스에 구축할 수 없습니다. [TAC를 사용하여 지원 티켓 열기](#)에 요청을 보냅니다.

위협 방어 디바이스를 온보딩하는 다양한 방법이 있습니다. 등록 키 방법을 사용하는 것이 좋습니다.

디바이스를 온보딩하는 동안 문제가 발생하는 경우 [일련 번호를 사용하여 FDM-관리 디바이스 온보딩 문제 해결, on page 769](#) 또는 [라이선스 부족으로 인해 실패, on page 764](#)에서 자세한 내용을 참조하십시오.

위협 방어 디바이스를 클라우드 사용 **Firewall Management Center**에 온보딩

버전 7.2 이상을 실행하는 위협 방어 디바이스를 클라우드 사용 Firewall Management Center에 온보딩할 수 있습니다. 자세한 내용은 [클라우드 사용 Firewall Management Center에 FTD 온보딩](#)을 참조하십시오.

일련 번호로 위협 방어 디바이스 온보딩

이 절차는 지원되는 버전의 소프트웨어를 실행하는 , Firepower 1000, Firepower 2100, 또는 Secure Firewall 3100 시리즈 물리적 디바이스를 온보딩하는 간소화된 방법입니다. 디바이스를 온보딩하려면 디바이스의 새시 일련 번호 또는 PCA 일련 번호가 필요하며 디바이스가 인터넷에 연결할 수 있는 네트워크에 추가되었는지 확인합니다.

공장에서 배송된 새 디바이스 또는 이미 CDO에 구성된 디바이스를 온보딩할 수 있습니다.

자세한 내용은 [디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩, on page 195](#)을 참조하십시오.

등록 키를 사용하여 위협 방어 디바이스 온보딩

등록 키를 사용하여 위협 방어 디바이스를 온보딩하는 것이 좋습니다. 이는 DHCP를 사용하여 디바이스에 IP 주소가 할당된 경우 유용합니다. 등록 키로 온보딩했다면 어떤 이유로든 해당 IP 주소가 변경되더라도 위협 방어 디바이스는 CDO에 연결된 상태로 유지됩니다.

- [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩, on page 186](#)
- [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩, on page 190](#)

자격 증명을 사용하여 위협 방어 디바이스 온보딩

네트워크에서 디바이스가 구성된 방식에 따라 디바이스 자격 증명 및 디바이스 외부, 내부 또는 관리 인터페이스의 IP 주소를 사용하여 위협 방어 디바이스를 온보딩할 수 있습니다. 자격 증명을 사용하여 디바이스를 온보딩하려면 [사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩, on page 184](#)의 내용을 참조하십시오. 인터페이스 주소를 사용하여 온보딩하려면 이 문서의 뒷부분에 나오는 [위협 방어 디바이스 온보딩](#)을 참조하십시오.

디바이스를 관리하려면 CDO에 디바이스에 대한 HTTPS 액세스가 필요합니다. 디바이스에 대한 HTTPS 액세스를 허용하는 방법은 네트워크에서 디바이스가 구성된 방식 및 디바이스를 온보딩하는 디바이스가 [SDC\(Secure Device Connector\)](#)인지 클라우드 커넥터인지에 따라 달라집니다.



**Note** <https://www.defenseorchestrator.eu>에 연결하고 소프트웨어 버전 6.4를 사용하는 경우 이 방법으로 위협 방어 디바이스를 온보딩해야 합니다. 등록 키 방법을 사용할 수 없습니다.

디바이스 자격 증명을 사용하여 CDO를 디바이스에 연결하는 경우, 네트워크에서 SDC(Secure Device Connector)를 다운로드하고 구축하여 CDO과 디바이스 간의 통신을 관리하는 것이 모범 사례입니다. 일반적으로 이러한 디바이스는 경계를 기반으로 하지 않으며 공용 IP 주소가 없거나 외부 인터페이스에 대한 개방형 포트가 있습니다. 자격 증명으로 온보딩된 위협 방어 디바이스는 SDC를 사용하여 CDO에 온보딩할 수 있습니다.

VPN 연결을 위한 헤드엔드로도 위협 방어 디바이스를 사용하는 고객은 외부 인터페이스를 사용하여 디바이스를 관리할 수 없습니다.

위협 방어 클러스터 온보딩

CDO에 온보딩 전에 클러스터링된 위협 방어 디바이스를 온보딩할 수 있습니다. 클러스터링을 사용하면 여러 방화벽 위협 방어 유닛을 하나의 논리적 디바이스로 그룹화하여 단일 디바이스의 편의성(관리, 네트워크 통합)을 제공하는 동시에 여러 디바이스의 처리량 증가 및 이중화를 달성할 수 있습니다.

[클러스터된 Secure Firewall Threat Defense 디바이스 온보딩, on page 210](#)의 내용을 참조하십시오.

온보딩을 위한 **FDM**-관리 디바이스 구성 사전 요건

**FDM**-관리 디바이스 관리

Secure Firewall device manager (FDM)에서 관리 중인 위협 방어 디바이스만 온보딩할 수 있습니다. Secure Firewall Management Center에서 관리 중인 위협 방어 디바이스는 클라우드 사용 Firewall Management Center에서 관리할 수 없습니다.

디바이스가 로컬 관리용으로 구성되지 않은 경우 디바이스를 온보딩하기 전에 로컬 관리로 전환해야 합니다. [Firepower Device Manager용 Secure Firewall Threat Defense 구성 가이드](#)의 로컬 및 원격 관리 간 전환 장을 참조하십시오.

라이선싱

일부 상황에서는 스마트 라이선스를 적용할 수 있지만 디바이스를 CDO에 온보딩하려면 최소한 라이선스가 설치되어 있어야 합니다.

온보딩 방법	Secure Firewall device manager 소프트웨어 버전	90일 평가판 라이선스가 허용됩니까?	온보딩 전에 디바이스에 이미 스마트 라이선스가 부여될 수 있습니까?	온보딩 전에 디바이스를 Cisco Cloud Services에 이미 등록할 수 있습니까?
자격 증명(사용자 이름 및 비밀번호)	계	예	예	예
등록 키	6.4 또는 6.5	예	아니요. 스마트 라이선스를 등록 취소한 다음 디바이스를 온보딩합니다.	해당 없음

온보딩 방법	<b>Secure Firewall device manager</b> 소프트웨어 버전	90일 평가판 라이선스가 허용됩니까?	온보딩 전에 디바이스에 이미 스마트 라이선스가 부여될 수 있습니까?	온보딩 전에 디바이스를 <b>Cisco Cloud Services</b> 에 이미 등록할 수 있습니까?
등록 키	6.6 이상	예	예	아니요. Cisco Cloud Services에서 디바이스를 등록 취소한 다음 디바이스를 온보딩합니다.
로우 터치 프로비저닝	6.7 이상	예	예	예
일련 번호로 디바이스 온보딩	6.7 이상	예	예	예

자세한 내용은 [Cisco Firepower System 기능 라이선스](#)를 참조하십시오.

#### 디바이스 주소 지정

FDM 관리 디바이스를 온보딩하는 데 사용하는 주소는 고정 주소인 것이 가장 좋습니다. 디바이스의 IP 주소가 DHCP에 의해 할당된 경우 DDNS(동적 도메인 이름 시스템)를 사용하여 디바이스의 도메인 이름 항목이 변경되는 경우 디바이스의 새 IP 주소로 자동으로 업데이트하는 것이 가장 좋습니다.



**Note** FDM 관리 디바이스는 기본적으로 DDNS를 지원하지 않습니다. 사용자 고유의 DDNS를 구성해야 합니다.



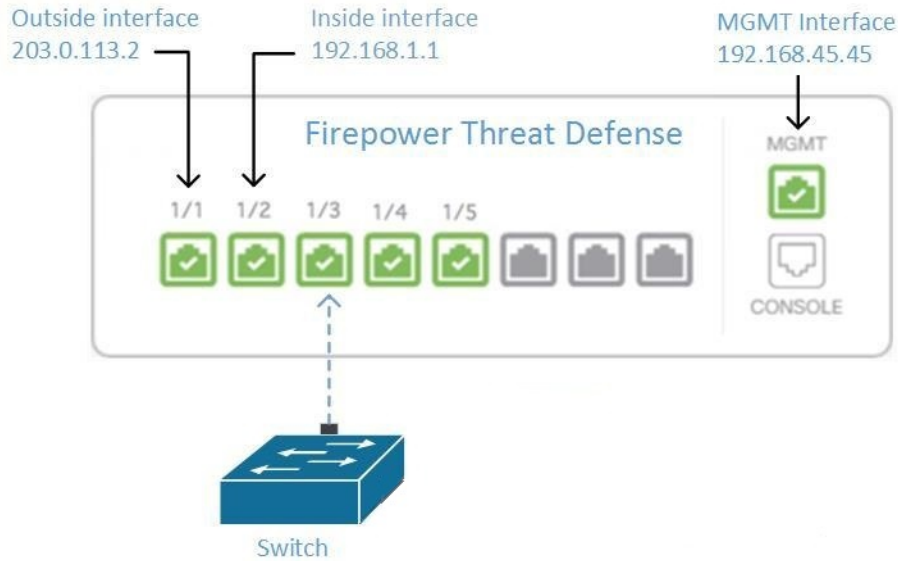
**Important** 디바이스가 DHCP 서버에서 IP 주소를 가져오는데 FDM 관리 디바이스의 도메인 이름 항목을 새 IP 주소로 업데이트하는 DDNS 서버가 없거나 디바이스가 새 주소를 수신하는 경우, [CDO에서 디바이스의 IP 주소 변경](#)한 다음 [CDO에 디바이스 대량 다시 연결](#)할 수 있습니다. 등록 키를 사용하여 디바이스를 온보딩하는 것이 더 좋습니다.

## 내부 인터페이스에서 **FDM**-관리 디바이스 관리

전용 MGMT 인터페이스에 조직 내에서 라우팅할 수 없는 주소가 할당된 경우, 내부 인터페이스를 사용하여 FDM 관리 디바이스를 관리하는 것이 바람직할 수 있습니다. 예를 들어 데이터 센터나 연구실 내에서만 연결할 수 있습니다.



**Figure 5:** 인터페이스 주소



원격 액세스 **VPN** 요구 사항

CDO로 관리하는 FDM 관리 디바이스가 원격 액세스 VPN(RA VPN) 연결을 관리하는 경우 CDO는 내부 인터페이스를 사용하여 디바이스를 관리해야 합니다.

다음 작업:

FDM 관리 디바이스 구성 절차를 위해 [내부 인터페이스에서 FDM-관리 디바이스 관리](#), on page 3로 계속하십시오.

## 내부 인터페이스에서 **FDM**-관리 디바이스 관리

이 구성 방법:

- FDM 관리 디바이스가 CDO에 온보딩되지 않았다고 가정합니다.
- 데이터 인터페이스를 내부 인터페이스로 구성합니다.
- MGMT 트래픽(HTTPS)을 수신하도록 내부 인터페이스를 구성합니다.
- 클라우드 커넥터의 주소가 디바이스의 내부 인터페이스에 도달하도록 허용합니다.

### Before you begin

다음 항목에서 이 구성의 사전 요구 사항을 검토합니다.

- [내부 인터페이스에서 FDM-관리 디바이스 관리](#), on page 2
- [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#), on page 12

## Procedure

---

단계 1 Secure Firewall device manager에 로그인합니다.

단계 2 **System Settings**(시스템 설정) 메뉴에서 **Management Access**(관리 액세스)를 클릭합니다.

단계 3 **Data Interfaces**(데이터 인터페이스) 탭을 클릭하고 **Create Data Interface**(데이터 인터페이스 생성)를 클릭합니다.

- a. **Interface**(인터페이스) 필드의 인터페이스 목록에서 미리 명명된 "**inside**(내부)" 인터페이스를 선택합니다.
- b. **Protocols**(프로토콜) 필드에서 아직 HTTPS가 아닌 경우 **HTTPS**를 선택합니다.
- c. **Allowed Networks**(허용된 네트워크) 필드에서 FDM 관리 디바이스의 내부 주소에 액세스할 수 있는 조직 내부의 네트워크를 나타내는 네트워크 개체를 선택합니다. SDC 또는 클라우드 커넥터의 IP 주소는 디바이스의 내부 주소에 액세스할 수 있는 주소 중 하나여야 합니다.

**인터페이스 주소** 다이어그램에서 SDC의 IP 주소 192.168.1.10은 192.168.1.1에 도달할 수 있어야 합니다.

단계 4 변경 사항 배포. 이제 내부 인터페이스를 사용하여 디바이스를 관리할 수 있습니다.

---

## What to do next

클라우드 커넥터를 사용하는 경우 어떻게 됩니까?

위의 절차를 사용하고 다음 단계를 추가합니다.

- 내부 인터페이스(192.168.1.1)에 외부 인터페이스(203.0.113.2)를 "NAT"하는 단계를 추가합니다.
- 위 절차의 3c단계에서 "허용된 네트워크"는 클라우드 커넥터의 공용 IP 주소를 포함하는 네트워크 그룹 개체입니다.
- 클라우드 커넥터의 공용 IP 주소에서 외부 인터페이스(203.0.113.2)에 대한 액세스를 허용하는 액세스 제어 규칙을 생성하는 단계를 추가합니다.

유럽, 중동 또는 아프리카(EMEA) 고객이고, <https://defenseorchestrator.eu/>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.

- 35.157.12.126
- 35.157.12.15

미국 고객이고, <https://defenseorchestrator.com/>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.

- 52.34.234.2
- 52.36.70.147

**AJPC(Asia-Pacific-Japan-China)** 고객이고, <https://www.apj.cdo.cisco.com/>에서 CDO에 연결하는 경우 다음 IP 주소에서 인바운드 액세스를 허용합니다.

- 54.199.195.111
- 52.199.243.0

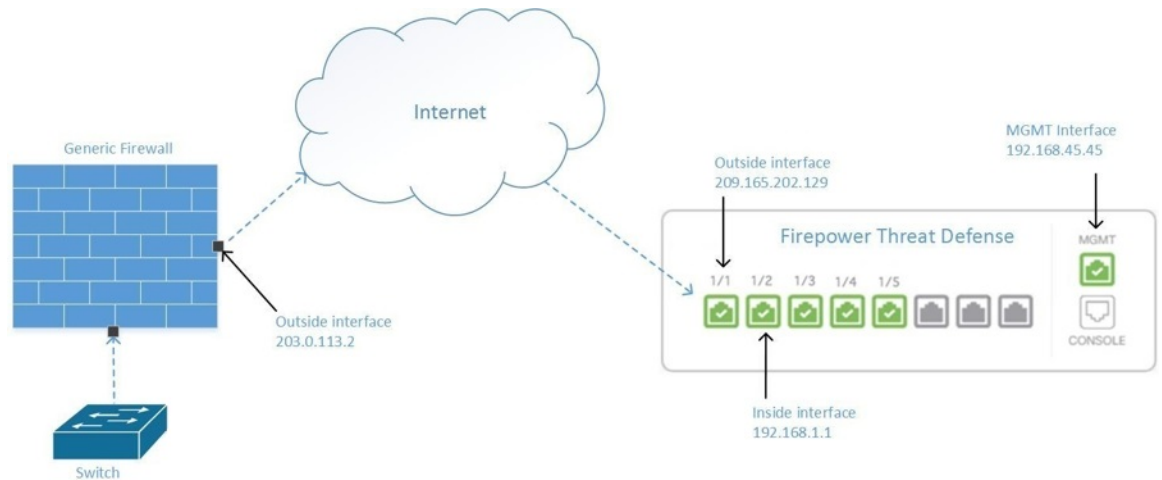
**FDM**-관리 디바이스 온보딩

등록 토큰 온보딩 접근 방식은 FDM 관리 디바이스를 CDO에 온보딩하는 권장 방법입니다. Cloud Connector에서 FDM 관리 디바이스로의 관리 액세스를 허용하도록 내부 인터페이스를 구성한 후, 사용자 이름과 암호를 사용하여 FDM 관리디바이스를 온보딩합니다. 자세한 내용은 [위협 방어 디바이스 온보딩](#)을 참조하십시오. 내부 인터페이스의 IP 주소를 사용하여 연결합니다. 위의 시나리오에서 해당 주소는 192.168.1.1입니다.

## 외부 인터페이스에서 **FDM**-관리 디바이스 관리

지사에 할당된 하나의 공용 IP 주소가 있고 Cisco Defense Orchestrator가 다른 위치에서 클라우드 커넥터를 사용하여 관리되는 경우 외부 인터페이스에서 클라우드 사용 Firewall Management Center 디바이스를 관리하는 것이 바람직할 수 있습니다.

**Figure 6:** 외부 인터페이스에서 디바이스 관리



이 구성은 물리적 MGMT 인터페이스가 더 이상 디바이스의 관리 인터페이스가 아님을 의미하지 않습니다. 클라우드 사용 Firewall Management Center 디바이스가 있는 사무실에 있다면 MGMT 인터페이스의 주소에 연결하여 디바이스를 직접 관리할 수 있습니다.

원격 액세스 **VPN** 요구 사항

클라우드 사용 Firewall Management Center로 관리하는 디바이스가 원격 액세스 VPN(RA VPN) 연결을 관리하는 경우, 클라우드 사용 Firewall Management Center는 외부 인터페이스를 사용하여 클라우

드 사용 Firewall Management Center 디바이스를 관리해야 합니다. 대신 [내부 인터페이스에서 FDM-관리 디바이스 관리](#)를 참조하십시오.

다음 작업:

클라우드 사용 Firewall Management Center 디바이스 구성 절차를 위해 [FDM-관리 디바이스의 외부 인터페이스 관리](#), on page 6로 계속하십시오.

## FDM-관리 디바이스의 외부 인터페이스 관리

이 구성 방법:

1. FDM 관리 디바이스가 CDO에 온보딩되지 않았다고 가정합니다.
2. 데이터 인터페이스를 외부 인터페이스로 구성합니다.
3. 외부 인터페이스에서 관리 액세스를 구성합니다.
4. 클라우드 커넥터의 공용 IP 주소(방화벽을 통해 NAT된 후)가 외부 인터페이스에 도달하도록 허용합니다.

### Before you begin

다음 항목에서 이 구성의 사전 요구 사항을 검토합니다.

- [FDM-관리 디바이스의 외부 인터페이스 관리](#), on page 6
- [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#), on page 12

### Procedure

단계 1 Secure Firewall device manager에 로그인합니다.

단계 2 **System Settings**(시스템 설정) 메뉴에서 **Management Access**(관리 액세스)를 클릭합니다.

단계 3 **Data Interfaces**(데이터 인터페이스) 탭을 클릭하고 **Create Data Interface**(데이터 인터페이스 생성)를 클릭합니다.

- a. **Interface**(인터페이스) 필드의 인터페이스 목록에서 미리 명명된 "**outside**(외부)" 인터페이스를 선택합니다.
- b. **Protocols**(프로토콜) 필드에서 아직 HTTPS가 아닌 경우 **HTTPS**를 선택합니다. CDO은 HTTPS 액세스만 필요합니다.
- c. **Allowed Networks**(허용된 네트워크) 필드에서 방화벽을 통해 NAT된 후 클라우드 커넥터의 공용 IP 주소를 포함하는 호스트 네트워크 개체를 생성합니다.

[Device Management from Outside Interface\(외부 인터페이스의 장치 관리\)](#) 네트워크 다이어그램에서 클라우드 커넥터의 IP 주소인 10.10.10.55는 203.0.113.2로 NAT됩니다. 허용된 네트워크의 경우 값이 203.0.113.2인 호스트 네트워크 개체를 생성합니다.

**단계 4** Secure Firewall device manager에서 SDC 또는 클라우드 커넥터의 공용 IP 주소에서 FDM 관리 디바이스의 외부 인터페이스로의 관리 트래픽(HTTPS)을 허용하는 액세스 제어 정책을 생성합니다. 이 시나리오에서 소스 주소는 203.0.113.2이고 소스 프로토콜은 HTTPS입니다. 대상 주소는 209.165.202.129이고 프로토콜은 HTTPS입니다.

**단계 5** 변경 사항 배포. 이제 외부 인터페이스를 사용하여 디바이스를 관리할 수 있습니다.

### What to do next

클라우드 커넥터를 사용하는 경우 어떻게 됩니까?

프로세스는 다음 두 가지를 제외하고 매우 유사합니다.

- 위 절차의 3c단계에서 "허용된 네트워크"는 클라우드 커넥터의 공용 IP 주소를 포함하는 네트워크 그룹 개체입니다.
  - 유럽, 중동 또는 아프리카(EMEA) 고객이고, <https://defenseorchestrator.eu/>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.
    - 35.157.12.126
    - 35.157.12.15
  - 미국 고객이고, <https://defenseorchestrator.com/>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.
    - 52.34.234.2
    - 52.36.70.147
  - AJPC(Asia-Pacific-Japan-China) 고객이고, <https://www.apj.cdo.cisco.com/>에서 CDO에 연결하는 경우 다음 IP 주소에서 인바운드 액세스를 허용합니다.
    - 54.199.195.111
    - 52.199.243.0
- 위 절차의 4단계에서는 클라우드 커넥터의 공용 IP 주소에서 외부 인터페이스에 대한 액세스를 허용하는 액세스 제어 규칙을 생성합니다.

등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩 접근 방식은 FDM 관리 디바이스를 CDO에 온보딩하는 권장 방법입니다. 클라우드 커넥터에서 관리 액세스를 허용하도록 외부 인터페이스를 구성한 후 FDM 관리 디바이스를 온보딩합니다. 외부 인터페이스의 IP 주소를 사용하여 연결합니다. 이 시나리오에서 해당 주소는 209.165.202.129입니다.

## FDM-관리 디바이스를 CDO에 온보딩

다음 절차에 따라 아래의 방법으로 FDM 관리를 CDO로 온보딩합니다.

## 사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩

디바이스 자격 증명 및 디바이스의 관리 IP 주소만 사용하여 FDM 관리 디바이스를 온보딩하려면 이 절차를 사용합니다. 이는 FDM 관리 디바이스를 온보딩하는 가장 간단한 방법입니다. 그러나 FDM 관리 디바이스를 CDO에 온보딩하는 데 권장하는 방법은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#)를 사용하는 것입니다.

### Before you begin



#### Important

Cisco Defense Orchestrator에 FDM 관리 디바이스를 온보딩하기 전에 [위협 방어 디바이스 온보딩 및 매니지드 디바이스에 Cisco Defense Orchestrator 연결, on page 12](#)을 읽어 보십시오. 디바이스를 온보딩하는 데 필요한 일반 디바이스 요구 사항 및 온보딩 사전 요건을 제공합니다.

- 자격 증명 방법을 사용하여 FDM 관리 디바이스를 온보딩하려면 다음 정보가 필요합니다.
  - 디바이스 자격 증명 CDO은 디바이스에 연결하는 데 사용됩니다.
  - 디바이스 관리에 사용 중인 인터페이스의 디바이스 IP 주소입니다. 이는 네트워크를 구성한 방법에 따라 관리 인터페이스, 내부 인터페이스 또는 외부 인터페이스일 수 있습니다.
  - 디바이스를 CDO에 온보딩하려면 로컬 관리를 위해 Secure Firewall device manager이 디바이스를 관리하고 구성해야 합니다. Secure Firewall Management Center에서 관리할 수 없습니다.




#### Note

<https://www.defenseorchestrator.eu>에 연결하고 FDM 관리 디바이스에서 소프트웨어 버전 6.4를 실행 중인 경우 이 방법을 사용해야 합니다. 소프트웨어 버전 6.5 이상을 실행하는 FDM 관리 디바이스만 온보딩할 수 있습니다.

### Procedure

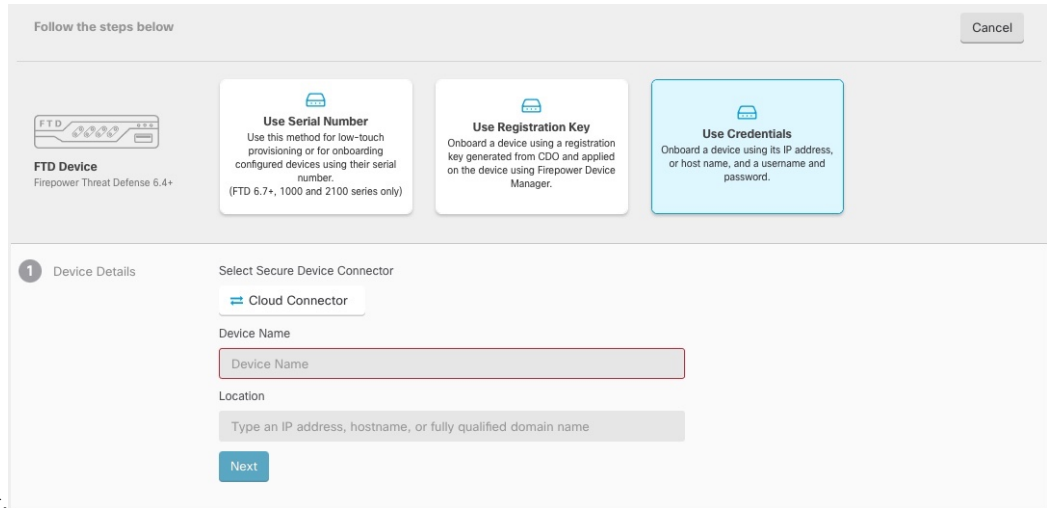
단계 1 CDO에 로그인합니다.

단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼 을 클릭하여 디바이스를 온보딩합니다.

단계 3 **FTD**를 클릭합니다.

**Important** FDM 관리 디바이스 온보딩을 시도하면 CDO는 테넌트에 대한 일회성 활동인 Secure Firewall Threat Defense EULA(엔드 유저 라이선스 동의서)를 읽고 동의하라는 메시지를 표시합니다. EULA에 동의하면 CDO은 EULA가 변경되지 않는 한 동의하라는 메시지를 다시 표시하지 않습니다.

#### 단계 4 온보딩 마법사에서 Use Credentials(자격 증명 사용)를 클릭합니



다.

#### 단계 5 디바이스 세부 정보 단계에서 다음을 수행합니다.

- **Secure Device Connector**(보안 디바이스 커넥터) 버튼을 클릭하고 네트워크에 설치된 SDC(보안 디바이스 커넥터)를 선택합니다. SDC를 사용하지 않으려면 CDO는 Cloud Connector를 사용하여 FDM 관리 디바이스에 연결할 수 있습니다. 선택은 매니지드 디바이스에 [Cisco Defense Orchestrator 연결](#)하는 방법에 따라 달라집니다.
- **Device Name**(디바이스 이름) 필드에 디바이스 이름을 입력합니다. 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.
- **Location**(위치) 필드에 디바이스 관리에 사용 중인 인터페이스의 IP 주소, 호스트 이름 또는 디바이스의 정규화된 도메인 이름을 입력합니다. 기본 포트는 443입니다.

**Important** SecureX 또는 Cisco Threat Response(CTR) 계정이 이미 있는 경우, 디바이스를 SecureX에 등록하려면 CDO 테넌트와 SecureX/CTR 계정을 병합해야 합니다. SecureX 포털을 통해 어카운트를 병합할 수 있습니다. 자세한 내용은 [CDO 및 SecureX 계정 병합](#)을 참조하십시오. 어카운트가 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 활용할 수 없습니다.

#### 단계 6 Database Updates(데이터베이스 업데이트) 영역에서 **Immediately perform security updates, and enable recurring updates**(즉시 보안 업데이트를 수행하고 반복 업데이트 활성화)가 기본적으로 활성화됩니다. 이 옵션은 보안 업데이트를 즉시 트리거할 뿐 아니라 매주 월요일 오전 2시에 추가 업데이트를 확인하도록 디바이스를 자동으로 예약합니다. 자세한 내용은 [FDM-관리 디바이스 보안 데이터베이스 업데이트](#) 및 [보안 데이터베이스 업데이트 예약](#)을 참조하십시오.

이 옵션을 비활성화해도 FDM을 통해 구성했을 수 있는 이전에 예약된 업데이트에는 영향을 주지 않습니다.

**Next**(다음)를 클릭합니다.

#### 단계 7 디바이스 관리자의 사용자 이름과 비밀번호를 입력하고 **Next**(다음)를 클릭합니다.

단계 8 디바이스의 Secure Firewall device manager에 보류 중인 변경 사항이 있는 경우 알림이 표시되며, 변경 사항을 되돌리거나 관리자에 로그인하여 보류 중인 변경 사항을 구축할 수 있습니다. Secure Firewall device manager에 보류 중인 변경 사항이 없으면 프롬프트가 표시되지 않습니다.

단계 9 (선택 사항) 디바이스의 레이블을 추가합니다. 자세한 내용은 [레이블 및 필터링](#)을 참조하십시오.

## 등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩

이 절차에서는 등록 키를 사용하여 FDM 관리 디바이스를 온보딩하는 방법을 설명합니다. 이 방법은 Cisco Defense Orchestrator에 FDM 관리 디바이스를 온보딩하는 데 권장되는 방법이고 DHCP를 사용하여 FDM 관리에 IP 주소를 할당한 경우 유용합니다. 어떤 이유로 해당 IP 주소가 변경되더라도 FDM 관리 디바이스는 CDO에 연결된 상태로 유지됩니다. 또한 FDM 관리 디바이스는 로컬 영역 네트워크에 주소를 가질 수 있으며 외부 네트워크에 액세스할 수 있는 한 이 방법을 사용하여 CDO에 온보딩할 수 있습니다.



### Warning

이미 SecureX 또는 CTR(Cisco Threat Response) 계정이 있는 경우 디바이스를 SecureX에 등록하려면 CDO 테넌트와 SecureX/CTR 계정을 병합해야 합니다. 계정이 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 이용할 수 없습니다. SecureX에서 CDO 모듈을 생성하기 전에 계정을 병합하는 것을 강력히 권장합니다. SecureX 포털을 통해 계정을 병합할 수 있습니다. 자세한 내용은 [어카운트 병합](#)을 참조하십시오.

### 온보딩 전

- 버전 6.4를 실행하는 고객의 경우 이 온보딩 방법은 미국 지역(defenseorchestrator.com)에서만 지원됩니다.
- 버전 6.4를 실행하고 EU 지역(defense Orchestrator.eu)에 연결하는 고객의 경우 [사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩](#)를 사용하여 디바이스를 온보딩해야 합니다.
- 버전 6.5 이상을 실행하고 US, EU 또는 APJC 지역(apj.cdo.cisco.com) 지역에 연결하는 고객은 이 온보딩 방법을 사용할 수 있습니다.
- CDO를 FDM 관리 디바이스에 연결하는 데 필요한 네트워크 요구 사항에 대해서는 [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#), on page 12를 검토하십시오.
- Secure Firewall Management Center가 아닌 Secure Firewall device manager에서 디바이스를 관리하는지 확인합니다.
- 버전 6.4 및 6.5를 실행하는 디바이스는 등록 키로 온보딩하기 전에 Cisco Smart Software Manager에 등록하지 않아야 합니다. CDO에 온보딩하기 전에 해당 FDM 관리의 스마트 라이선스를 등록 취소해야 합니다. 아래의 "스마트 라이선스 Firewall Device Manager 등록 취소"를 참조하십시오.
- 디바이스에서 90일 평가판 라이선스를 사용 중일 수 있습니다.
- FDM 관리 디바이스에 로그인하고 디바이스에서 대기 중인 변경 사항이 없는지 확인합니다.



- DNS가 FDM 관리 디바이스에 올바르게 구성되어 있는지 확인합니다.
- FDM 관리 디바이스에서 시간 서비스가 올바르게 구성되었는지 확인합니다.
- FDM 관리 디바이스에 올바른 날짜 및 시간이 표시되는지 확인합니다. 그렇지 않으면 온보딩이 실패합니다.

다음 작업

다음 두 가지 중 하나를 수행합니다.

- 이미 스마트 라이선스가 있는 경우 Cisco Smart Software Manager에서 FDM 관리 디바이스 등록을 취소합니다. 등록 키를 사용하여 CDO에 온보딩하기 전에 Cisco Smart Software Manager에서 디바이스를 등록 취소해야 합니다. [스마트 라이선스 FDM-관리 디바이스 등록 취소, on page 187](#)를 계속합니다.
- 디바이스에 스마트 라이선스가 없는 경우 등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스를 온보딩하는 절차, [on page 188](#)을 계속 진행합니다.

### 스마트 라이선스 FDM-관리 디바이스 등록 취소

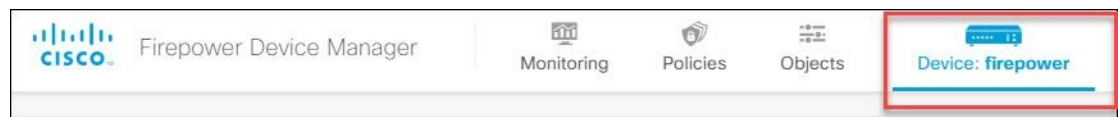
온보딩하려는 디바이스가 버전 6.4 또는 6.5를 실행 중이고, 이미 스마트 라이선스가 있는 경우, 해당 디바이스는 Cisco Smart Software Manager에 등록되어 있을 가능성이 높습니다. 등록 키를 사용하여 CDO에 온보딩하기 전에 Cisco Smart Software Manager에서 디바이스를 등록 취소해야 합니다. 등록을 취소하면 디바이스에 연결된 기본 라이선스 및 선택 가능한 모든 라이선스가 가상 어카운트에서 해제됩니다.

디바이스를 등록 취소한 후에도 디바이스의 현재 컨피그레이션 및 정책은 계속 원래대로 작동하지만 변경을 수행하거나 변경 사항을 구축할 수는 없습니다.

### Procedure

단계 1 Secure Firewall device manager를 사용하여 디바이스에 로그인합니다.

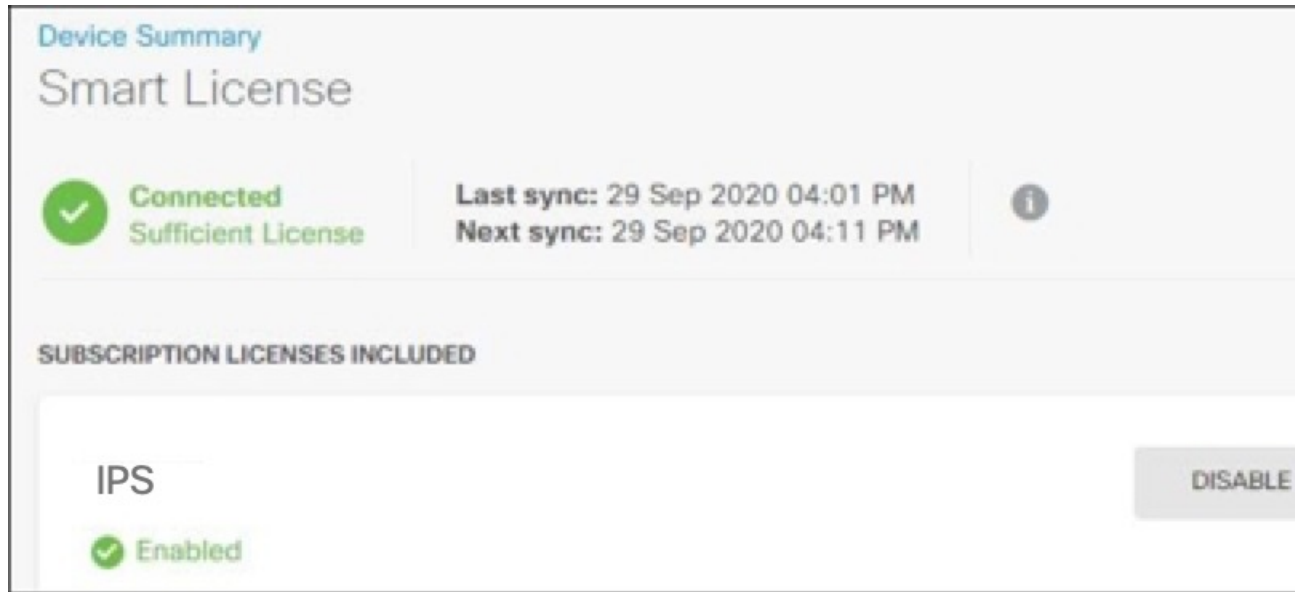
단계 2 상단 탭에서 디바이스 아이콘을 클릭합니다.



단계 3 Smart License(스마트 라이선스) 영역에서 View Configuration(구성 보기)을 클릭합니다.

단계 4 Go to Cloud Services(클라우드 서비스로 이동) 기어 메뉴를 클릭하고 Unregister Device(디바이스 등록 취소)를 선택합니다.

등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스를 온보딩하는 절차



단계 5 경고를 확인한 후에 디바이스를 등록 취소하려면 **Unregister**(등록 취소)를 클릭합니다.

#### What to do next


CDO에 온보딩하기 위해 등록을 취소한 경우 [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스를 온보딩하는 절차, on page 188](#)로 계속합니다.

등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스를 온보딩하는 절차  
등록 키를 사용하여 FDM 관리를 온보딩하려면 다음 절차를 수행합니다.

#### Before you begin

[등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩, on page 186](#)에서 설명하는 사전 요건을 검토하십시오.

#### Procedure

- 단계 1 CDO에 로그인합니다.
- 단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.
- 단계 3 **FTD**를 클릭합니다.

**Important** FDM 관리 디바이스를 온보딩하려고 하면 Cisco Defense Orchestrator에서 Firepower Threat Defense EULA(최종 사용자 라이선스 계약)를 읽고 동의하라는 메시지가 표시됩니다. 이는 테넌트의 일회성 활동입니다. 이 동의서에 동의하면 CDO는 후속 FDM 관리 온보딩에서 이를 다시 확인하지 않습니다. 나중에 EULA 계약이 변경되는 경우 메시지가 표시되면 다시 동의해야 합니다.

**단계 4 Onboard FTD Device(온보드 FTD 디바이스) 화면에서 Use Registration Key(등록 키 사용)를 클릭합니다.**


**단계 5 Device Name(디바이스 이름) 필드에 디바이스 이름을 입력합니다. 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.**

**단계 6 Database Updates(데이터베이스 업데이트) 영역에서 Immediately perform security updates, and enable recurring updates(즉시 보안 업데이트를 수행하고 반복 업데이트 활성화) 옵션이 기본적으로 활성화됩니다. 이 옵션은 보안 업데이트를 즉시 트리거할 뿐 아니라 매주 월요일 오전 2시에 추가 업데이트를 확인하도록 디바이스를 자동으로 예약합니다. 자세한 내용은 FDM-관리 디바이스 보안 데이터베이스 업데이트 및 보안 데이터베이스 업데이트 예약을 참조하십시오.**

**Note** 이 옵션을 비활성화해도 Secure Firewall device manager을 통해 구성했을 수 있는 이전에 예약된 업데이트에는 영향을 주지 않습니다.

**단계 7 Create Registration Key(등록 키 생성) 영역에서 CDO가 등록 키를 생성합니다.**

**Note** 키가 생성된 후 디바이스가 완전히 온보딩되기 전에 온보딩 화면에서 나갈 경우, 온보딩 화면으로 돌아갈 수 없습니다. 그러나 CDO는 Inventory(재고 목록) 페이지에서 해당 디바이스에 대한 자리 표시자를 생성합니다. 디바이스의 자리 표시자를 선택하면 오른쪽에 있는 작업 창에서 해당 디바이스의 키를 볼 수 있습니다.

**단계 8 Copy(복사) 아이콘 을 클릭하여 등록 키를 복사합니다.**

**Note** 등록 키 복사를 건너뛰고 Next(다음)를 클릭하여 디바이스에 대한 자리 표시자 항목을 완료한 다음 나중에 디바이스를 등록할 수 있습니다. 이 옵션은 디바이스를 먼저 생성하고 나중에 디바이스를 등록하려는 경우 또는 고객 네트워크에 POV(Proof of Value) 디바이스를 설치하는 Cisco 파트너인 경우 유용합니다.

**Inventory(재고 목록) 페이지에서 디바이스가 현재 연결 상태인 "Unprovisioned(프로비저닝되지 않음)"에 있음을 확인할 수 있습니다. Unprovisioned(프로비저닝되지 않음) 아래에 표시되는 등록 키를 Firewall Device Manager에 복사하여 온보딩 프로세스를 완료합니다.**

**단계 9 CDO에 온보딩하려는 디바이스의 Secure Firewall device manager에 로그인합니다.**

**단계 10 System Settings(시스템 설정)에서 Cloud Services(클라우드 서비스)를 클릭합니다.**

**단계 11 CDO 타일에서 Get Started(시작하기)를 클릭합니다.**

**단계 12 Region(지역) 필드에서 테넌트가 할당된 Cisco Cloud 지역을 선택합니다.**

- defenseorchestrator.com에 로그인하는 경우 US를 선택합니다.
- defenseorchestrator.eu에 로그인하는 경우 EU를 선택합니다.
- apj.cdo.cisco.com에 로그인하는 경우 APJ를 선택합니다.

**Note** 이 단계는 버전 6.4를 실행하는 FDM 관리 디바이스에는 적용되지 않습니다.

**단계 13 Registration Key(등록 키) 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.**

**단계 14 Register(등록)**를 클릭한 다음, **Accept Cisco Disclosure(Cisco 공개 동의)**를 클릭합니다.

**단계 15** CDO으로 돌아옵니다. 디바이스에 적용할 모든 라이선스를 선택합니다.

자세한 내용은 [스마트 라이선스 적용 또는 업데이트](#)를 참조하십시오. **Skip(건너뛰기)**을 클릭하여 90일 평가 라이선스로 온보딩을 계속할 수도 있습니다.

**단계 16** CDO로 돌아가 **Inventory(재고 목록)** 페이지를 열고 디바이스 상태가 "Unprovisioned(프로비저닝되지 않음)"에서 "Locating(찾기 중)", "Syncing(동기화 중)"에서 "Synced(동기화됨)"로 진행되는지 확인합니다.

## 등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩

이 절차에서는 등록 키를 사용하여 버전 6.6 이상을 실행하는 FDM 관리 디바이스를 온보딩하는 방법을 설명합니다. 이 방법은 FDM 관리 디바이스를 Cisco Defense Orchestrator에 온보딩하는 데 권장되는 방법이며 DHCP를 사용하여 FDM 매니지드 디바이스에 IP 주소가 할당된 경우에 유용합니다. 어떤 이유로 해당 IP 주소가 변경되더라도 FDM 관리 디바이스는 CDO에 연결된 상태로 유지됩니다. 또한 FDM 관리 디바이스는 로컬 영역 네트워크에 주소를 가질 수 있으며 외부 네트워크에 액세스할 수 있는 한 이 방법을 사용하여 CDO에 온보딩할 수 있습니다.

**Warning**

이미 SecureX 또는 CTR(Cisco Threat Response) 계정이 있는 경우 디바이스를 SecureX에 등록하려면 CDO 테넌트와 SecureX/CTR 계정을 병합해야 합니다. 계정이 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 이용할 수 없습니다. SecureX에서 CDO 모듈을 생성하기 전에 계정을 병합하는 것을 강력히 권장합니다. SecureX 포털을 통해 계정을 병합할 수 있습니다. 자세한 내용은 [어카운트 병합](#)을 참조하십시오.

버전 6.4 또는 6.5를 실행하는 FDM 관리 디바이스를 온보딩하려면 [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.

## 온보딩 전

- 이 온보딩 방법은 현재 버전 6.6 이상과 [defenceorchestrator.com](#), [defenceorchestrator.eu](#) 및 [apj.cdo.cisco.com](#)에 연결하는 고객이 사용할 수 있습니다.
- CDO를 FDM 관리 디바이스에 연결하는 데 필요한 네트워크 요구 사항에 대해서는 [매니지드 디바이스에 Cisco Defense Orchestrator 연결, on page 12](#)를 검토하십시오.
- Secure Firewall Management Center가 아닌 Secure Firewall device manager에서 디바이스를 관리하는지 확인합니다.
- 디바이스는 90일 평가 라이선스를 사용하거나 스마트 라이선스를 사용할 수 있습니다. 버전 6.6 이상을 실행하는 디바이스는 설치된 스마트 라이선스의 등록을 취소하지 않고 등록 키를 사용하여 CDO에 온보딩할 수 있습니다.
- 디바이스를 Cisco Cloud 서비스에 이미 등록할 수 없습니다. 온보딩하기 전에 아래의 "Cisco Cloud Services에서 FDM-관리 디바이스 등록 취소"를 참조하십시오.
- 디바이스의 Secure Firewall device manager UI에 로그인하고 디바이스에서 대기 중인 변경 사항이 없는지 확인합니다.
- DNS가 FDM 관리 디바이스에 올바르게 구성되어 있는지 확인합니다.
- FDM 관리 디바이스에서 시간 서비스가 구성되었는지 확인합니다.
- FDM 관리 디바이스에 올바른 날짜 및 시간이 표시되는지 확인합니다. 그렇지 않으면 온보딩이 실패합니다.

## 다음 작업:

다음 중 하나를 수행합니다.

- 버전 6.6 이상을 실행하는 FDM 관리 디바이스가 이미 Cisco Cloud Services에 등록된 경우 온보딩하기 전에 디바이스 등록을 취소해야 합니다. [Cisco Cloud Services에서 FDM-관리 디바이스 등록 취소, on page 192](#)를 진행합니다.
- 디바이스가 Cisco Cloud Services에 등록되지 않은 경우 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차, on page 193](#)를 계속 진행합니다.

## Cisco Cloud Services에서 FDM-관리 디바이스 등록 취소

다음 절차는 Cisco Cloud Services에서 디바이스를 등록 취소하기 위한 것입니다. 등록 키를 사용하여 FDM 관리 디바이스를 CDO에 온보딩하기 전에 이 방법을 사용합니다.



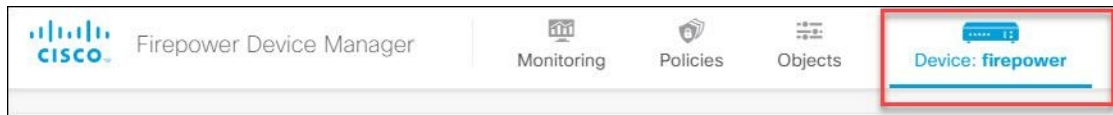
**Note** 버전 7.0 이상을 실행하는 가상 FDM 관리 디바이스를 온보딩하는 경우 가상 FDM 관리 디바이스를 CDO에 등록하면 성능 계층화된 스마트 라이선싱 선택 항목이 기본 계층인 **Variable(변수)**로 자동 재설정됩니다. 온보딩 후 Secure Firewall device manager UI를 통해 디바이스에 연결된 라이선스와 일치하는 계층을 수동으로 다시 선택해야 합니다.

이 절차를 사용하여 Cisco Cloud Services에 등록되지 않았는지 확인합니다.

### Procedure

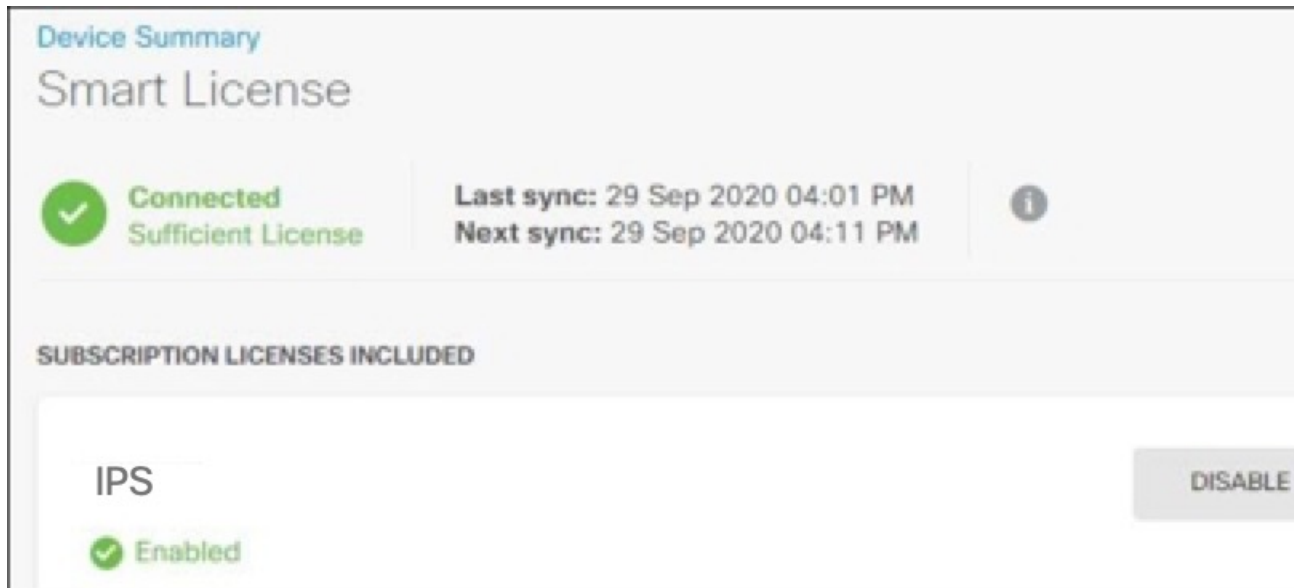
단계 1 Secure Firewall device manager를 사용하여 디바이스에 로그인합니다.

단계 2 상단 탭에서 디바이스 아이콘을 클릭합니다.



단계 3 **System Settings**(시스템 설정) 메뉴를 확장한 다음 **Cloud Services**(클라우드 서비스)를 클릭합니다.

단계 4 **Cloud Services**(클라우드 서비스) 페이지에서 기어 메뉴를 클릭하고 **Unregister Cloud Services**(클라우드 서비스 등록 취소)를 선택합니다.



단계 5 경고를 확인한 후에 디바이스를 등록 취소하려면 **Unregister**(등록 취소)를 클릭합니다.

**What to do next**


버전 6.6 이상을 실행하는 FDM 관리 디바이스를 온보딩하려는 경우 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차](#), on page 193을 계속 진행하십시오.

등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차

등록 키를 사용하여 FDM 관리 디바이스를 온보딩하려면 다음 절차를 수행합니다.

**Procedure**

단계 1 CDO에 로그인합니다.

단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.

단계 3 **FTD**를 클릭합니다.

**Important** FDM 관리 디바이스 온보딩을 시도하면 Cisco Defense Orchestrator에서는 테넌트에 대한 일회성 활동인 EULA(엔드 유저 라이선스 동의서)를 읽고 동의하라는 메시지를 표시합니다. 이 동의서에 동의하면 CDO는 후속 온보딩에서 이를 다시 확인하지 않습니다. 나중에 EULA 계약이 변경되는 경우 메시지가 표시되면 다시 동의해야 합니다.

단계 4 **Onboard FTD Device**(온보드 FTD 디바이스) 화면에서 **Use Registration Key**(등록 키 사용)를 클릭합니다.


단계 5 **Device Name**(디바이스 이름) 필드에 디바이스 이름을 입력합니다. 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.

단계 6 **Database Updates**(데이터베이스 업데이트) 영역에서 **Immediately perform security updates, and enable recurring updates**(즉시 보안 업데이트를 수행하고 반복 업데이트 활성화)가 기본적으로 활성화됩니다. 이 옵션은 보안 업데이트를 즉시 트리거할 뿐 아니라 매주 월요일 오전 2시에 추가 업데이트를 확인하도록 디바이스를 자동으로 예약합니다. 자세한 내용은 [FDM-관리 디바이스 보안 데이터베이스 업데이트](#) 및 [보안 데이터베이스 업데이트 예약](#)을 참조하십시오.

**Note** 이 옵션을 비활성화해도 Secure Firewall device manager을 통해 구성했을 수 있는 이전에 예약된 업데이트에는 영향을 주지 않습니다.

단계 7 **Create Registration Key**(등록 키 생성) 단계에서 CDO가 등록 키를 생성합니다.

**Note** 키가 생성된 후 디바이스가 완전히 온보딩되기 전에 온보딩 화면에서 나갈 경우, 온보딩 화면으로 돌아갈 수 없습니다. 그러나 CDO는 **Inventory**(재고 목록) 페이지에서 해당 디바이스에 대한 자리 표시자를 생성합니다. 디바이스의 자리 표시자를 선택하면 해당 페이지에서 해당 디바이스의 키를 볼 수 있습니다.

단계 8 Copy(복사) 아이콘  을 클릭하여 등록 키를 복사합니다.

등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차

**Note** 등록 키 복사를 건너뛰고 **Next(다음)**를 클릭하여 디바이스에 대한 자리 표시자 항목을 완료한 다음 나중에 디바이스를 등록할 수 있습니다. 이 옵션은 디바이스를 먼저 생성하고 나중에 디바이스를 등록하려는 경우 또는 고객 네트워크에 POV(Proof of Value) 디바이스를 설치하는 Cisco 파트너인 경우 유용합니다.

**Inventory(재고 목록)** 페이지에서 디바이스가 현재 연결 상태인 "Unprovisioned(프로비저닝되지 않음)"에 있음을 확인할 수 있습니다. **Unprovisioned(프로비저닝되지 않음)** 아래에 표시되는 등록 키를 Firewall Device Manager에 복사하여 온보딩 프로세스를 완료합니다.

단계 9 온보딩 중인 디바이스의 Secure Firewall device manager에 로그인합니다.

단계 10 **System Settings(시스템 설정)**에서 **Cloud Services(클라우드 서비스)**를 클릭합니다.

단계 11 **Region(지역)** 필드에서 테넌트가 할당된 Cisco Cloud 지역을 선택합니다.

- defenseorchestrator.com에 로그인하는 경우 US를 선택합니다.
- defenseorchestrator.eu에 로그인하는 경우 EU를 선택합니다.
- apj.cdo.cisco.com에 로그인하는 경우 APJ를 선택합니다.

단계 12 **Enrollment Type(등록 유형)** 영역에서 **Security Account(보안 어카운트)**를 클릭합니다.

**Note** 버전 6.6을 실행하는 디바이스의 경우 CDO의 Tenancy(테넌시) 탭 제목이 **Security Account(보안 계정)**이며 Secure Firewall device manager에서 CDO를 수동으로 활성화해야 합니다.

The screenshot shows the 'Enrollment Type' configuration page. At the top, there are two tabs: 'Security/CDO Account' (which is active) and 'Smart Licensing'. Below the tabs is a 'Region' dropdown menu currently showing 'US Region'. Underneath is a 'Registration Key' input field with the placeholder text 'Enter Registration Key'. The 'Service Enrollment' section is expanded, showing two options: 'Cisco Defense Orchestrator' and 'Cisco Success Network'. Both have checkboxes that are checked. The 'Cisco Defense Orchestrator' section includes a description and a link to 'See more'. The 'Cisco Success Network' section also includes a description and a link to 'See more'. At the bottom of the page, there is a blue 'REGISTER' button and a 'Need help?' link.

단계 13 **Registration Key(등록 키)** 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.



- 단계 14 버전 6.7 이상을 실행하는 디바이스의 경우, Service Enrollment(서비스 등록) 영역에서 **Enable Cisco Defense Orchestrator(Cisco Defense Orchestrator 활성화)**를 선택합니다.
- 단계 15 Cisco Success Network 등록에 대한 정보를 검토합니다. 참여하지 않으려면 **Enroll Cisco Success Network(Cisco Success Network 등록)** 확인란의 선택을 취소합니다.
- 단계 16 **Register(등록)**를 클릭한 다음 Cisco 고지 사항을 수락합니다. Secure Firewall device manager는 CDO에 등록 요청을 보냅니다.
- 단계 17 CDO로 돌아가 **Create Registration Key(등록 키 생성)** 영역에서 **Next(다음)**를 클릭합니다.
- 단계 18 디바이스에 적용할 모든 라이선스를 선택합니다. **Next(다음)**를 클릭합니다.
- 단계 19 CDO로 돌아가 **Inventory(재고 목록)** 페이지를 열고 디바이스 상태가 "Unprovisioned(프로비저닝되지 않음)"에서 "Locating(찾기 중)", "Syncing(동기화 중)"에서 "Synced(동기화됨)"로 진행되는지 확인합니다.

## 디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩

이 절차는 FDM 관리 디바이스를 Cisco Defense Orchestrator에 온보딩하고 설정하는 간소화된 방법입니다. 디바이스의 새시 일련 번호 또는 PCA 일련 번호만 있으면 됩니다. 디바이스를 온보딩할 때 스마트 라이선스를 적용하거나 90일 평가 라이선스를 사용할 수 있습니다.

[로우터치 프로비저닝을 사용하여 FDM-관리 디바이스를 온보딩하기 위한 워크플로우 및 전제 조건](#)을 수행하기 전에 활용 사례를 읽고 개념을 이해해야 합니다.



**Important** 이러한 FDM 관리 디바이스를 온보딩하는 방법은 버전 6.7 이상을 실행하는 디바이스에서만 사용할 수 있습니다.

### 활용 사례

- [디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩, on page 195](#): 네트워크에 추가되고 인터넷에서 연결되는 새로운 공장 출하 FDM 관리 디바이스를 온보딩합니다. 디바이스에서 초기 디바이스 설정 마법사가 완료되지 않았습니다.
- [디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩, on page 202](#): 이미 구성된 FDM 관리 디바이스 또는 네트워크에 이미 추가되고 인터넷에서 연결되는 업그레이드된 디바이스를 온보딩합니다. 디바이스에서 초기 디바이스 설정 마법사가 완료되었습니다.



**Important** 이 방법을 사용하여 디바이스에 대해 지원되는 이전 소프트웨어 버전에서 실행 중인 디바이스를 온보딩하려면 업그레이드 대신 해당 디바이스에서 소프트웨어를 새로 설치(리이미징)해야 합니다.

### 관련 정보:

- [로우 터치\(Low-Touch\) 프로비저닝에 사용되는 용어 및 정의](#)
- [일련 번호를 사용하여 FDM-관리 디바이스 온보딩 문제 해결](#)

## 로우터치 프로비저닝을 사용하여 FDM-관리 디바이스를 온보딩하기 위한 워크플로우 및 전제 조건

로우터치 프로비저닝은 새로운 Firepower 1000, Firepower 2100 또는 Secure Firewall 3100 시리즈 디바이스를 자동으로 프로비저닝 및 구성하여, CDO에 디바이스를 온보딩하는 것과 관련된 대부분의 수동 작업을 제거하는 기능입니다. 로우터치 프로비저닝은 직원이 네트워크 디바이스 사용 경험이 적은 원격 사무실 또는 기타 위치를 위한 것입니다.

로우터치 프로비저닝 프로세스를 사용하려면, 디바이스를 CDO에 온보딩하고 인터넷에 연결할 수 있는 네트워크에 연결한 다음 디바이스의 전원을 켭니다. 자세한 내용은 [디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩](#), on page 202을 참조하십시오.



**Note** CDO에 온보딩하기 전이나 후에 디바이스의 전원을 켤 수 있습니다. 먼저 디바이스를 CDO에 온보딩하고 디바이스의 전원을 켜 다음 브랜치 네트워크에 연결하는 것이 좋습니다. CDO에서 디바이스를 온보딩하면 디바이스가 Cisco Cloud의 CDO 테넌트 및 CDO와 연결되고 자동으로 디바이스 구성이 동기화됩니다.

이 절차를 사용하여 외부 공급업체에서 구매한 디바이스를 온보딩하거나 다른 지역의 다른 클라우드 테넌트에서 이미 관리하는 디바이스를 온보딩할 수도 있습니다. 그러나 디바이스가 이미 외부 벤더의 클라우드 테넌트 또는 다른 지역의 클라우드 테넌트에 등록된 경우 CDO는 디바이스를 온보딩하지 않지만 "Device serial number already claimed(디바이스 일련 번호가 이미 클레임됨)" 오류 메시지를 표시합니다. 이러한 경우 CDO 관리자는 이전 클라우드 테넌트에서 디바이스의 일련 번호를 등록 취소한 다음 자신의 테넌트에서 CDO 디바이스를 클레임해야 합니다. 문제 해결 장에서 [디바이스 일련 번호가 이미 요청됨](#)을 참조하십시오.

디바이스 연결 상태가 "Online(온라인)"으로 변경되고 구성 상태가 "Synced(동기화됨)"로 변경됩니다. FDM 관리 디바이스가 CDO에 온보딩됩니다.

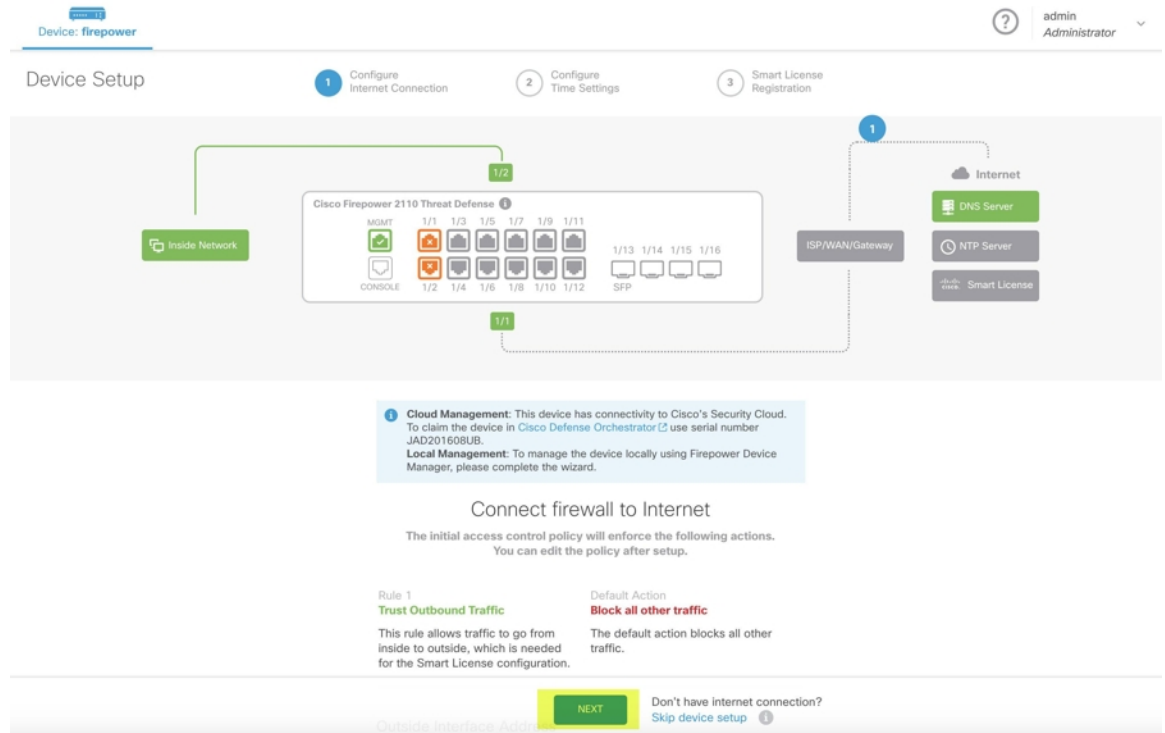
하드웨어 후면 패널에서 상태 LED(Firepower 1010), SYS LED(Firepower 2100) 또는 S LED(Secure Firewall 3100)가 녹색으로 깜박이는 것을 볼 수 있습니다. 클라우드에 연결되면 디바이스 LED가 녹색으로 계속 깜박입니다. 디바이스가 Cisco cloud에 연결할 수 없거나 연결 후 연결이 끊어지면 상태 LED(Firepower 1010), SYS LED(Firepower 2100) 또는 M LED(Secure Firewall 3100)가 녹색과 황색으로 번갈아 깜박이는 것을 볼 수 있습니다.

LED 표시등을 이해하려면 [로우터치 프로비저닝을 사용하여 Cisco Firepower 방화벽 설치](#) 비디오를 참조하십시오.



**Important** FDM 관리 디바이스 콘솔, SSH 또는 Secure Firewall Threat Defense에 로그인한 경우, 첫 번째 로그인 시 디바이스의 비밀번호를 변경했을 것입니다. CDO를 사용하여 디바이스를 온보딩하는 데도 로우터치 프로비저닝 프로세스를 사용할 수 있습니다. Secure Firewall Threat Defense에 로그인한 후에는 외부 인터페이스를 구성하는 디바이스 설정 마법사 단계를 완료하지 마십시오. 이 단계를 완료하면 디바이스가 클라우드에서 등록 취소되고 로우터치 프로비저닝 프로세스를 사용할 수 없습니다.

Secure Firewall Threat Defense에 로그인하면 대시보드에 다음 화면이 표시됩니다.



Secure Firewall Threat Defense UI에서 더 이상 진행하지 않고 일련 번호 온보딩 마법사로 이동하여 디바이스를 온보딩합니다. 디바이스 비밀번호가 이미 변경되었으므로, 여기서 **Default Password Changed**(기본 비밀번호 변경됨)를 선택해야 합니다.

사전 요건

소프트웨어 및 하드웨어 요구 사항

FDM 관리 디바이스는 일련 번호 온보딩을 지원하는 소프트웨어를 실행해야 합니다. 다음 표를 가이드로 사용합니다.

**Table 9:** 하드웨어 및 소프트웨어 지원

로우 터치( <b>Low-Touch</b> ) 프로비저닝을 지원하는 방화벽 모델 번호	지원되는 방화벽 소프트웨어 버전	소프트웨어 패키지
Firepower 1000 시리즈 디바이스 모델: 1010, 1120, 1140, 1150	6.7 이상	SF-F1K-TDx.x-K9
Firepower 2100 시리즈 디바이스 모델: 2110, 2120, 2130, 2140	6.7 이상	SF-F2K-TDx.x-K9
Secure Firewall 3100 시리즈 디바이스 모델: 3110, 3120, 3130, 3140	7.1 이상	SF-F3K-TDx.x-K9

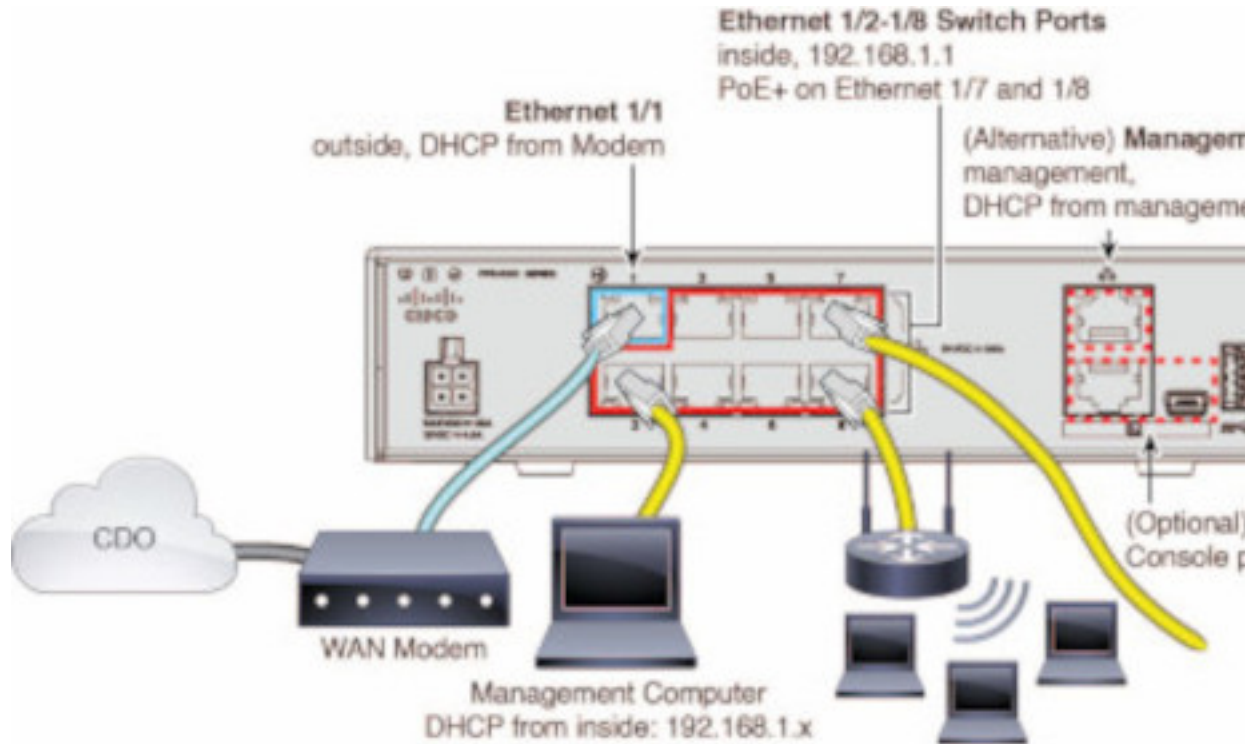
관리 플랫폼이 올바른 버전을 실행 중인지 확인합니다.

Table 10: FTD Manager 버전 지원

매니저	지원되는 버전
Secure Firewall Device Manager	7.0 이상
온프레미스 Firewall Management Center	7.2 이상
클라우드 사용 Firewall Management Center	해당 없음

하드웨어 설치를 위한 구성 사전 요건

- 브랜치 오피스에 있는 네트워크는 **192.168.1.0/24** 어드레스 스페이스를 사용할 수 없습니다. 이더넷 1/1 (외부)의 네트워크는 192.168.1.0/24 어드레스 스페이스를 사용할 수 없습니다. FTD 6.7을 실행하는 1000 및 2100 Series 디바이스에서 이더넷 1/2 "내부" 인터페이스의 기본 IP 주소는 192.168.1.1이며, 해당 서브넷에 있는 경우 WAN 모뎀이 할당한 DHCP 주소와 충돌할 수 있습니다.
  - 내부—이더넷 1/2, IP 주소 192.168.1.1
  - 외부—이더넷 1/1, DHCP의 IP 주소 또는 설정 중 지정하는 주소



외부 인터페이스 설정을 변경할 수 없는 경우, 충돌을 방지하기 위해 Secure Firewall device manager를 사용하여 이더넷 1/2 "내부" 인터페이스 설정의 서브넷을 변경합니다. 예를 들어 다음 서브넷 설정으로 변경할 수 있습니다.

- IP 주소: 192.168.95.1
- DHCP 서버 범위: 192.168.95.5-192.168.95.254

물리적 인터페이스를 구성하는 단계에 대해 알아보려면 "[Secure Firewall Device Manager 구성 가이드](#)"를 참조하십시오. "인터페이스" 장에서 "물리적 인터페이스 구성" 섹션을 참조하십시오.

- 위협 방어 디바이스를 Cisco Cloud에 설치하고 연결해야 합니다.
- 디바이스의 외부 또는 관리 인터페이스는 DHCP 주소 지정을 제공하는 네트워크에 연결해야 합니다. 일반적으로 디바이스는 외부 또는 관리 인터페이스에 기본 DHCP 클라이언트가 있습니다.



**Note** 관리 인터페이스가 DHCP 서버가 있는 네트워크에 연결된 경우 Linux 스택 시작 트래픽에 대해 외부 인터페이스보다 우선적으로 적용됩니다.

- 외부 또는 관리 인터페이스에서 액세스해야 직렬 온보딩 방법을 위해 다음 보안 서비스 익스체인지 도메인에 액세스할 수 있습니다.
  - 미국 지역
    - api-sse.cisco.com
    - est.sco.cisco.com(전 지역 공통)
    - mx\*.sse.itd.cisco.com(현재 mx01.sse.itd.cisco.com만)
    - dex.sse.itd.cisco.com(고객 성공용)
    - eventing-ingest.sse.itd.cisco.com(CTR 및 CDO용)
    - registration.us.sse.itd.cisco.com(지역 Cisco Cloud에 디바이스 등록 허용)
  - EU 지역
    - api.eu.sse.itd.cisco.com
    - est.sco.cisco.com(전 지역 공통)
    - mx\*.eu.sse.itd.cisco.com(현재 mx01.eu.sse.itd.cisco.com만)
    - dex.eu.sse.itd.cisco.com(고객 성공용)
    - eventing-ingest.eu.sse.itd.cisco.com(CTR 및 CDO용)
    - registration.eu.sse.itd.cisco.com(지역 Cisco Cloud에 디바이스 등록 허용)
  - APJ 지역
    - api.apj.sse.itd.cisco.com
    - est.sco.cisco.com(전 지역 공통)
    - mx\*.apj.sse.itd.cisco.com(현재 mx01.apj.sse.itd.cisco.com만)

- dex.apj.sse.itd.cisco.com(고객 성공용)
- eventing-ingest.apj.sse.itd.cisco.com(CTR 및 CDO용)
- <http://registration.apj.sse.itd.cisco.com>(지역 Cisco Cloud에 대한 디바이스 등록 허용)

• 디바이스의 외부 인터페이스에 Cisco Umbrella DNS에 대한 DNS 액세스 권한이 있어야 합니다.

**CDO**에서 디바이스를 클레임하기 전에

CDO에서 디바이스를 클레임하기 전에 다음 정보가 있는지 확인합니다.

- 위협 방어 디바이스의 새시 일련 번호 또는 PCA 번호입니다. 이 정보는 하드웨어 새시 하단 또는 디바이스가 배송된 상자에 있습니다. 다음 예시 그림에서 Firepower 1010 새시 하단의 일련 번호 "\*\*\*\*\*XOR9"를 볼 수 있습니다.



- 디바이스의 기본 비밀번호입니다.
- 추가 기능을 사용하기 위해 [Cisco Smart Software Manager](#)에서 생성된 스마트 라이선스입니다. 그러나 90일 평가 라이선스를 사용하여 디바이스 온보딩을 완료하고 나중에 스마트 라이선스를 적용할 수 있습니다.



**Caution** 디바이스가 Cisco Defense Orchestrator에서 온보딩되는 경우 Secure Firewall device manager를 사용하여 디바이스 간편 설정을 수행하지 않는 것이 좋습니다. 이로 인해 CDO에서 임시 오류가 발생합니다.

## Before you begin

온프레미스 Management Center로 관리하려는 의도로 디바이스를 온보딩하는 경우 온프레미스 Management Center는 버전 7.4 이상을 실행해야 합니다. 이전 버전은 로우터치 프로비저닝을 지원하지 않습니다.

## Procedure

- 
- 단계 1 외부 벤더에서 구매한 디바이스를 온보딩하는 경우 먼저 디바이스를 이미지 재설치해야 합니다. 자세한 내용은 [Cisco FXOS 문제 해결 가이드](#)의 "이미지 재설치 절차" 장을 참조하십시오.
- 단계 2 CDO에 로그인합니다.
- 단계 3 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.
- 단계 4 **FTD tile**(타일)을 클릭합니다.
- Important** 디바이스 온보딩을 시도하면 CDO는 테넌트에 대한 일회성 활동인 EULA(엔드 유저 라이선스 동의서)를 읽고 동의하라는 메시지를 표시합니다. 이 동의서에 동의하면 CDO는 후속 온보딩에서 이를 다시 확인하지 않습니다. 나중에 EULA 계약이 변경되는 경우 메시지가 표시되면 다시 동의해야 합니다.
- 단계 5 **Onboard FTD Device**(온보드 FTD 디바이스) 화면에서 **Use Serial Number**(일련 번호 사용)를 클릭합니다.
- 단계 6 **FMC** 선택단계에서 드롭다운 메뉴를 사용하여 CDO에 이미 온보딩된 온프레미스 Management Center를 선택합니다. **Next**(다음)를 클릭합니다.
- 온프레미스 Management Center에서 버전 7.4 이상을 실행해야 합니다. 온프레미스 Management Center가 온보딩되지 않은 경우 온보딩 마법사에 대해 **+Onboard**(+온프레미스 FMC)를 클릭합니다.
- 단계 7 **Connection**(연결) 단계에서 디바이스의 일련 번호와 디바이스 이름을 입력합니다. **Next**(다음)를 클릭합니다.
- 단계 8 로우터치 프로비저닝의 경우 디바이스가 새 제품이어야 하거나 이미지를 다시 설치해야 합니다. **Password Reset**(비밀번호 재설정)의 경우 **Yes, this new device has never been logged into or configured for a manager**(예, 이 새 디바이스가 관리자에 로그인하거나 구성한 적이 없습니다.)를 선택해야 합니다. 새 비밀번호를 입력하고 디바이스의 새 비밀번호를 확인한 후 **Next**(다음)를 클릭합니다.
- 단계 9 **Policy Assignment**(정책 할당) 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다. 사용자 지정 정책이 없는 경우 CDO는 기본 액세스 제어 정책을 자동으로 선택합니다. **Next**(다음)를 클릭합니다.
- 단계 10 디바이스에 적용할 모든 라이선스를 선택합니다. **Next**(다음)를 클릭합니다.
- 단계 11 (선택사항) 기기에 라벨을 추가합니다. CDO는 디바이스가 성공적으로 온보딩되면 이러한 레이블을 적용합니다.
-

### What to do next

CDO에서는 디바이스 클레임을 시작하고, 오른쪽에 **Claiming**(클레임 중) 메시지가 표시됩니다. CDO에서는 디바이스가 온라인 상태이고 클라우드에 등록되어 있는지 확인하기 위해 1시간 동안 지속적으로 폴링합니다. 클라우드에 등록되면 CDO에서 초기 프로비저닝을 시작하고 디바이스를 성공적으로 온보딩합니다. 디바이스에서 LED 상태가 녹색으로 깜박이면 디바이스 등록을 확인할 수 있습니다. 디바이스가 Cisco 클라우드에 연결할 수 없거나 연결 후 연결이 끊어지면 상태 LED (Firepower 1000) 또는 SYS LED (Firepower 2100)가 녹색과 황색으로 번갈아 깜박이는 것을 확인할 수 있습니다.

디바이스가 처음 1시간 이내에 클라우드에 등록되지 않으면 시간 초과가 발생하며, 이제 CDO에서 10분마다 주기적으로 폴링하여 디바이스 상태를 확인하고 **Claiming**(클레임 중) 상태를 유지합니다. 디바이스가 켜져 있고 클라우드에 연결되어 있으면 온보딩 상태를 확인하기 위해 10분 동안 기다릴 필요가 없습니다. 언제든지 **Check Status**(상태 확인) 링크를 클릭하여 상태를 확인할 수 있습니다. CDO에서는 초기 프로비저닝을 시작하고 디바이스를 온보딩합니다.



#### Important

디바이스 설정 마법사(디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩 참조)를 이미 완료한 경우 디바이스가 클라우드에서 등록 취소되며, 이 경우 CDO에서는 **Claiming**(클레임 중) 상태를 유지합니다. Secure Firewall device manager에서 수동 등록을 완료하여 CDO에 추가해야 합니다. (Secure Firewall device manager에서 **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)로 이동하여 **Auto-enroll with Tenancy from Cisco Defense Orchestrator**(Cisco Defense Orchestrator에서 테넌시에 자동 등록) 옵션을 선택하고 **Register**(등록)를 클릭합니다). 그런 다음 **Check Status**(상태 확인)를 클릭합니다.

### 디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩

이 절차는 이미 관리용으로 구성된 디바이스에 적용됩니다. 디바이스 설정 마법사가 이미 구성된 FDM 관리 디바이스에서 완료되었으므로 디바이스가 클라우드에서 등록 취소되며, 로우터치 프로비저닝 프로세스를 사용하여 이러한 디바이스를 CDO에 온보딩할 수 없습니다.

디바이스가 관리되거나 구성된 적이 없는 새로운 디바이스인 경우, 로우터치 프로비저닝을 사용하여 디바이스를 온보딩할 수 있습니다. 자세한 내용은 [로우터치 프로비저닝을 사용하여 FDM-관리 디바이스 온보딩](#), on page 200을 참조하십시오.



#### Note

디바이스가 Cisco 클라우드에 연결되어 있지 않으면 상태 LED(Firepower 1000), SYS LED(Firepower 2100) 또는 M LED(Secure Firewall 3100)가 녹색과 황색으로 번갈아 깜박이는 것을 볼 수 있습니다.

다음 작업을 수행하기 위해 디바이스 설정 마법사를 완료했을 수 있습니다.

- 디바이스는 버전 6.7 이상을 실행해야 합니다.
- 디바이스의 관리 인터페이스에서 고정 IP 주소를 구성합니다. 인터페이스가 필요한 동적 IP 주소를 가져올 수 없거나 DHCP 서버가 게이트웨이 경로를 제공하지 않는 경우 고정 IP 주소를 구성해야 합니다.
- PPPoE를 사용하여 주소를 가져오고 외부 인터페이스를 구성합니다.



- Secure Firewall device manager 또는 Secure Firewall Management Center를 사용하여 버전 6.7 이상 디바이스를 실행하는 디바이스를 관리합니다.




### Important

Secure Firewall device manager에서 Secure Firewall Management Center으로 또는 그 반대로 Secure Firewall Threat Defense 디바이스 관리자를 전환할 수 있습니다. 디바이스가 실행하는 버전에 맞는 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 관리" 장의 로컬 및 원격 관리 간 전환 섹션에 설명된 단계를 수행합니다.

디바이스를 온보딩하려면 다음을 수행합니다.

### Procedure

- 단계 1 [라우터치 프로비저닝을 사용하여 FDM-관리 디바이스를 온보딩하기 위한 워크플로우 및 전제 조건](#)에서 온보딩을 위한 전제 조건을 검토합니다.
- 단계 2 Secure Firewall device manager UI에서 **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)로 이동하여 **Auto-enroll with Tenancy from Cisco Defense Orchestrator**(Cisco Defense Orchestrator에서 테넌시에 자동 등록) 옵션을 선택하고 **Register**(등록)를 클릭합니다.
- 단계 3 CDO에 로그인합니다.
- 단계 4 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.
- 단계 5 **FTD tile**(타일)을 클릭합니다.
- 단계 6 **Onboard FTD Device**(온보드 FTD 디바이스) 화면에서 **Use Serial Number**(일련 번호 사용)를 클릭합니다.
- 단계 7 **FMC** 선택단계에서 드롭다운 메뉴를 사용하여 CDO에 이미 온보딩된 온프레미스 Management Center를 선택합니다. **Next**(다음)를 클릭합니다.  
온프레미스 Management Center에서 버전 7.4 이상을 실행해야 합니다. 온프레미스 Management Center이 온보딩되지 않은 경우 온보딩 마법사에 대해 +Onboard(+온프레미스 FMC)를 클릭합니다.
- 단계 8 **Connection**(연결) 단계에서 디바이스의 일련 번호와 디바이스 이름을 입력합니다. **Next**(다음)를 클릭합니다.
- 단계 9 새 기기가 아니고 관리용으로 이미 구성된 경우, **Password Reset**(암호 재설정)을 위해 예, 이 새 기기는 비밀번호 재설정을 위해 로그인하거나 관리자용으로 구성된 적이 없음을 선택합니다. **Next**(다음)를 클릭합니다.
- 단계 10 **Policy Assignment**(정책 할당) 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다. 사용자 지정 정책이 없는 경우 CDO는 기본 액세스 제어 정책을 자동으로 선택합니다. **Next**(다음)를 클릭합니다.
- 단계 11 디바이스에 적용할 모든 라이선스를 선택합니다. **Next**(다음)를 클릭합니다.

CDO가 디바이스 연결 상태를 "Online(온라인)"으로 변경하고 구성 상태를 "Synced(동기화됨)" 상태로 변경합니다. FDM 관리 디바이스가 CDO에 온보딩됩니다. 하드웨어 후면 패널에서 상태 LED(Firepower 1000), SYS LED(Firepower 2100) 또는 M LED가 녹색으로 깜박이는 것을 볼 수 있습니다. Cisco Cloud에 연결되면 디바이스 LED가 녹색으로 계속 깜박입니다. 디바이스가 Cisco Cloud에 연결할 수 없거나 연결 후 연결이 끊어지면 동일한 상태 LED가 녹색과 황색으로 번갈아 깜박이는 것을 볼 수 있습니다.

관련 정보:

- [로우 터치\(Low-Touch\) 프로비저닝에 사용되는 용어 및 정의](#)

## FDM-관리 고가용성 쌍 온보딩

Secure Firewall Threat Defense HA 쌍을 CDO에 온보딩하려면 쌍의 각 디바이스를 개별적으로 온보딩해야 합니다. 쌍의 두 피어가 모두 온보딩되면 CDO는 **Inventory**(재고 목록) 페이지에서 단일 항목으로 자동으로 결합됩니다. 디바이스 로그인 자격 증명 또는 등록 키를 사용하여 디바이스를 온보딩합니다. 동일한 방법으로 두 디바이스를 모두 온보딩하는 것이 좋습니다. 또한 대기 모드에 있는 디바이스를 먼저 온보딩하는 경우 CDO는 해당 디바이스를 배포하거나 읽을 수 있는 기능을 비활성화합니다. HA 쌍 내의 액티브 디바이스만 읽거나 배포할 수 있습니다.



**참고** CDO는 등록 키가 있는 디바이스 온보딩을 강력히 권장합니다. 등록 키를 사용한 온보딩은 특정 버전을 실행하는 Threat Defense 디바이스에서 약간 다릅니다. 자세한 내용은 [버전 6.4 또는 버전 6.5를 실행하는 FDM-관리 HA 쌍 온보딩, 205 페이지](#) 및 [버전 6.6 또는 버전 6.7 이상을 실행하는 FDM-관리 HA 쌍 온보딩, 206 페이지](#)를 참조하십시오.

CDO에 Threat Defense HA 쌍을 온보딩하기 전에 다음을 검토합니다.

- CDO에 대한 온보딩 전에 HA 쌍이 이미 형성되어 있습니다.
- 두 디바이스 모두 정상 상태입니다. 쌍은 기본/활성 및 보조/대기 또는 기본/대기 및 보조/활성 모드일 수 있습니다. 비정상 디바이스는 CDO에 동기화되지 않습니다.
- HA 쌍은 Secure Firewall Management Center가 아니라 Secure Firewall device manager이 관리합니다.
- 클라우드 커넥터는 <https://www.defenseorchestrator.com>에서 CDO에 연결됩니다.

등록 키를 사용하여 **FDM-관리 고가용성 쌍 온보딩**

등록 키를 사용하여 FDM 관리 HA(고가용성) 쌍을 온보딩하기 전에 다음 사전 요건을 확인합니다.

- 등록 키로 버전 6.4를 실행하는 디바이스 온보딩은 미국 지역(defenseorchestrator.com)에 대해서만 지원됩니다. EU 지역(defenseorchestrator.eu)에 연결하려면 사용자 이름, 비밀번호 및 IP 주소를 사용하여 HA 쌍을 온보딩해야 합니다.
- 버전 6.5 이상을 실행하고 미국, EU 또는 APJC 지역에 연결하는 고객은 이 온보딩 방법을 사용할 수 있습니다.

- 버전 6.4 및 6.5를 실행하는 디바이스는 등록 키로 온보딩하기 전에 Cisco Smart Software Manager에 등록하지 않아야 합니다. CDO에 온보딩하기 전에 해당 FDM 관리의 스마트 라이선스를 등록 취소해야 합니다. 자세한 내용은 [스마트 라이선스 FDM-관리 디바이스 등록 취소, on page 187](#)를 참조하십시오.

버전 6.4 또는 버전 6.5를 실행하는 FDM-관리 HA 쌍 온보딩

소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM 관리 HA 쌍을 온보딩하려면 디바이스를 한 번에 하나씩 온보딩해야 합니다. 액티브 또는 보조, 기본 또는 보조 디바이스를 온보딩하는지 여부는 중요하지 않습니다.




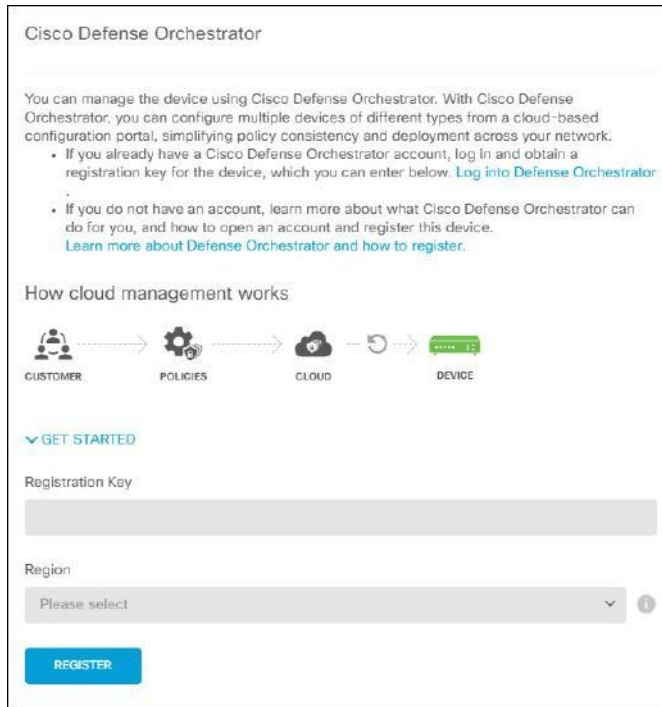
**Note** 등록 키를 사용하여 HA 쌍의 디바이스 중 하나를 온보딩하는 경우 동일한 방법으로 다른 피어 디바이스를 온보딩해야 합니다.

버전 6.4 또는 6.5를 실행하는 HA 쌍을 온보딩하려면 다음 단계를 사용합니다.

**Procedure**

- 단계 1** 피어 디바이스를 온보딩합니다. [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하여 쌍 내의 첫 번째 디바이스를 온보딩합니다.
- 단계 2** 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 3** **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 4** **FTD** 탭을 클릭합니다. 디바이스가 동기화되면 디바이스를 선택하여 강조 표시합니다. **Device Details**(디바이스 세부 정보) 바로 아래에 있는 작업 창에서 **Onboard Device**(디바이스 온보드)를 클릭합니다.
- 단계 5** 이미 온보딩된 피어 디바이스의 **HA Peer Device Name**(HA 피어 디바이스 이름) 을 입력합니다. **Next**(다음)를 클릭합니다.
- 단계 6** 첫 번째 디바이스에 대한 스마트 라이선스를 제공한 경우, CDO은 현재 디바이스를 온보딩하는 데 사용할 수 있도록 해당 라이선스를 다시 채웁니다. **Next**(다음)를 클릭합니다.
 

**Note** 디바이스 온보딩을 위해 FDM 관리 디바이스의 스마트 라이선스 등록을 취소한 경우, 여기에서 스마트 라이선스를 다시 적용합니다.
- 단계 7** CDO은 온보딩을 준비하는 디바이스에 대한 등록 키를 자동으로 생성합니다. **Copy**(복사) 아이콘  을 클릭하여 등록 키를 복사합니다.
- 단계 8** 온보딩 중인 디바이스의 Secure Firewall device manager UI에 로그인합니다.
- 단계 9** **System Settings**(시스템 설정)에서 **Cloud Services**(클라우드 서비스)를 클릭합니다.
- 단계 10** CDO 파일에서 **Get Started**(시작하기)를 클릭합니다.
- 단계 11** **Registration Key**(등록 키) 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.



단계 12 **Region**(지역) 필드에서 테넌트가 할당된 Cisco Cloud 지역을 선택합니다.

- defenseorchestrator.com에 로그인하는 경우 US를 선택합니다.
- defenseorchestrator.eu에 로그인하는 경우 EU를 선택합니다.
- apj.cdo.cisco.com에 로그인하는 경우 APJ를 선택합니다.

**Note** 이 단계는 버전 6.4에서 실행되는 FDM 관리 디바이스에는 적용되지 않습니다.

단계 13 **Register**(등록)를 클릭한 다음, **Accept Cisco Disclosure**(Cisco 공개 동의)를 클릭합니다.

단계 14 CDO으로 돌아가서, **Create Registration Key**(등록 키 생성) 영역에서 **Next**(다음)을 클릭합니다.

단계 15 **Go to Inventory**(재고 목록로 이동)을 클릭합니다. CDO는 자동으로 디바이스를 온보딩하고 단일 항목으로 결합합니다. 온보딩하는 첫 번째 피어 디바이스와 마찬가지로 디바이스 상태가 "Unprovisioned(프로비저닝되지 않음)"에서 "Locating(찾는 중)", "Syncing(동기화 중)"에서 "Synced(동기화됨)"로 변경됩니다.


버전 6.6 또는 6.7을 실행하는 FDM 관리 HA 쌍을 온보딩하려면 한 번에 하나씩 디바이스를 온보딩해야 합니다. 액티브 또는 보조, 기본 또는 보조 디바이스를 온보딩하는지 여부는 중요하지 않습니다.



**Note** 등록 키를 사용하여 HA 쌍의 디바이스 중 하나를 온보딩하는 경우 동일한 방법으로 다른 피어 디바이스를 온보딩해야 합니다.

버전 6.6 또는 6.7을 실행하는 HA 쌍을 온보딩하려면 다음 단계를 사용합니다.

### Procedure

- 단계 1 피어 디바이스를 온보딩합니다. 자세한 내용은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.
- 단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 3 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 4 **FTD** 탭을 클릭합니다. 디바이스가 동기화되면 디바이스를 선택하여 강조 표시합니다. **Device Details**(디바이스 세부 정보) 바로 아래에 있는 작업 창에서 **Onboard Device**(디바이스 온보드)를 클릭합니다.
- 단계 5 이미 온보딩된 피어 디바이스의 HA 피어 디바이스 이름을 입력합니다. **Next**(다음)를 클릭합니다.
- 단계 6 첫 번째 디바이스에 대한 스마트 라이선스를 제공한 경우, CDO은 현재 디바이스를 온보딩하는 데 사용할 수 있도록 해당 라이선스를 다시 채웁니다. **Next**(다음)를 클릭합니다.
- 단계 7 CDO은 온보딩을 준비하는 디바이스에 대한 등록 키를 자동으로 생성합니다. **Copy**(복사) 아이콘 을 클릭하여 등록 키를 복사합니다.
- 단계 8 CDO에 온보딩하려는 디바이스의 Secure Firewall device manager UI에 로그인합니다.
- 단계 9 **System Settings**(시스템 설정)에서 **Cloud Services**(클라우드 서비스)를 클릭합니다.
- 단계 10 **Enrollment Type**(등록 유형) 영역에서 **Security/CDO Account**(보안/CDO 계정)를 클릭합니다.

**Note** 버전 6.6을 실행하는 디바이스의 경우, CDO의 Tenancy(테넌시) 탭의 제목이 **Security Account**(보안 어카운트)이며 Secure Firewall device managerUI에서 CDO를 수동으로 활성화해야 합니다.

The screenshot shows a web form for enrolling a device into Cisco Defense Orchestrator. The 'Enrollment Type' section has two options: 'Security/CDO Account' (selected) and 'Smart Licensing'. The 'Region' dropdown menu is set to 'US Region'. Below that is a text input field for 'Registration Key' with the placeholder 'Enter Registration Key'. The 'Service Enrollment' section contains two main sections: 'Cisco Defense Orchestrator' and 'Cisco Success Network'. Under 'Cisco Defense Orchestrator', there is a checked checkbox for 'Enable Cisco Defense Orchestrator'. Under 'Cisco Success Network', there is a checked checkbox for 'Enroll Cisco Success Network'. At the bottom of the form is a blue 'REGISTER' button and a link for 'Need help?'. The 'Service Enrollment' section has a progress indicator on the left with a blue dot at the current step.

단계 11 **Region**(지역) 필드에서 테넌트가 할당된 Cisco Cloud 지역을 선택합니다.

- defenseorchestrator.com에 로그인하는 경우 US를 선택합니다.
- defenseorchestrator.eu에 로그인하는 경우 EU를 선택합니다.
- apj.cdo.cisco.com에 로그인하는 경우 APJ를 선택합니다.

단계 12 **Registration Key**(등록 키) 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.

단계 13 버전 6.7 이상을 실행하는 디바이스의 경우, **Service Enrollment**(서비스 등록) 영역에서 **Enable Cisco Defense Orchestrator**(Cisco Defense Orchestrator 활성화)를 선택합니다.

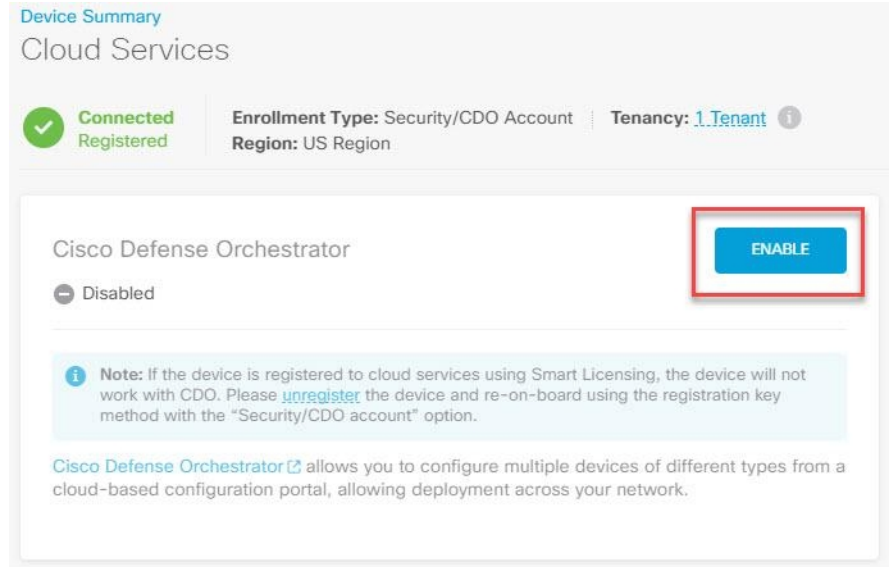
단계 14 Cisco Success Network 등록에 대한 정보를 검토합니다. 참여하지 않으려면 **Enroll Cisco Success Network**(Cisco Success Network 등록) 확인란의 선택을 취소합니다.

단계 15 **Register**(등록)를 클릭한 다음, **Accept Cisco Disclosure**(Cisco 공개 동의)를 클릭합니다. FDM에서 CDO에 등록 요청을 전송합니다.

단계 16 CDO로 돌아가 **Create Registration Key**(등록 키 생성) 영역에서 **Next**(다음)를 클릭합니다.

단계 17 **Smart License**(스마트 라이선스) 영역에서 FDM 관리 디바이스에 스마트 라이선스를 적용하고 **Next**(다음)를 클릭하거나 **Skip**(건너뛰기)을 클릭하여 90일 평가 라이선스로 온보딩을 계속할 수 있습니다.(또는 디바이스에 이미 스마트 라이선스가 있는 경우). 자세한 내용은 [FTD 디바이스의 기존 스마트 라이선스 업데이트](#)를 참조하십시오.

**Note** 디바이스에서 버전 6.6을 실행 중인 경우 CDO와의 통신을 수동으로 활성화해야 합니다. 디바이스의 FDM 관리 UI에서 **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)로 이동하여 **Cisco Defense Orchestrator** 타일에서 **Enable**(활성화)를 클릭합니다.



**단계 18** CDO으로 돌아가 **Go to Inventory**(인벤토리로 이동)를 클릭합니다. CDO는 자동으로 디바이스를 온보딩하고 단일 항목으로 결합합니다. 온보딩하는 첫 번째 피어 디바이스와 마찬가지로 디바이스 상태가 "Unprovisioned(프로비저닝되지 않음)"에서 "Locating(찾는 중)", "Syncing(동기화 중)"에서 "Synced(동기화됨)"로 변경됩니다.

**FDM-관리 고가용성 쌍 온보딩**



**참고** HA 쌍의 첫 번째 디바이스를 어떤 방법으로 온보딩하든 다른 피어 디바이스도 동일한 방법으로 온보딩해야 합니다.

CDO 외부에서 생성된 FDM 관리 HA 쌍을 온보딩하려면 다음 절차를 수행합니다.

**프로시저**

**단계 1** HA 쌍 내의 피어 디바이스 중 하나를 온보딩합니다. 사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩, 등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차 또는 디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩를 사용하여 디바이스를 온보딩합니다.

**단계 2** 디바이스가 동기화되면 **Inventory**(재고 목록) 페이지에서 **Devices**(디바이스) 탭을 클릭합니다.

**단계 3** **FTD** 탭을 클릭합니다.

- 단계 4 디바이스를 선택합니다. **Device Details**(디바이스 세부 정보) 바로 아래에 있는 작업 창에서 **Onboard Device**(디바이스 온보드)를 클릭합니다.
- 단계 5 팝업 창에서 HA 피어의 디바이스 이름 및 위치를 입력합니다.
- 단계 6 **Onboard Device**(디바이스 온보드)를 클릭합니다. 두 디바이스가 CDO에 성공적으로 동기화되면 HA 쌍이 **Inventory**(재고 목록) 페이지에 단일 엔터티로 표시됩니다.

## FTD 클러스터 온보딩

•

### 클러스터된 **Secure Firewall Threat Defense** 디바이스 온보딩

다음 절차를 사용하여 이미 클러스터링된 위협 방어 디바이스를 온보딩합니다.

시작하기 전에


다음 디바이스는 클러스터링을 지원합니다.

- Secure Firewall 3100 디바이스
- Firepower 4100 디바이스
- Firepower 9300 디바이스
- Threat Defense Virtual 디바이스(AWS, Azure, VMware, KVM, GCP)

클러스터된 디바이스의 경우 다음과 같은 제한 사항을 참고하십시오.

- 디바이스는 버전 6.4 이상을 실행해야 합니다.
- 디바이스는 물리적 또는 가상 Secure Firewall Management Center으로 관리해야 합니다.
- Firepower 4100 및 Firepower 9300 디바이스는 디바이스의 새시 관리자를 통해 클러스터링되어야 합니다.
- Secure Firewall 3100 디바이스, KVM 및 VMware 환경은 Secure Firewall Management Center UI를 통해 클러스터링되어야 합니다.
- Azure, AWS 및 GCP 환경 클러스터는 자체 환경을 통해 생성하고 Secure Firewall Management Center에 온보딩해야 합니다.

프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.
- 단계 3 **FTD**를 클릭합니다.



**단계 4 Management Mode(관리 모드)에서 FTD가 선택되어 있는지 확인합니다.**

FTD를 선택하면 Secure Firewall Management Center를 관리 플랫폼으로 유지하게 됩니다. FDM을 선택하면 관리자가 Secure Firewall Management Center에서 Firewall Device Manager 또는 클라우드 사용 Firewall Management Center와 같은 로컬 관리자로 전환됩니다. 관리자를 전환하면 인터페이스 구성을 제외한 모든 기존 정책 구성이 재설정되며 디바이스를 온보딩한 후 정책을 다시 구성해야 합니다.

**단계 5 Onboard FTD Device(온보드 FTD 디바이스) 화면에서 Use CLI Registration Key(CLI 등록 키 사용)를 클릭합니다.**

**단계 6 Device Name(디바이스 이름) 필드에 디바이스 이름을 입력합니다.** 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.

**단계 7 Policy Assignment(정책 할당) 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다.** 구성된 정책이 없는 경우 **Default Access Control Policy(기본 액세스 제어 정책)**를 선택합니다.

**단계 8** 온보딩 중인 디바이스가 물리적 디바이스인지 가상 디바이스인지 지정합니다. 가상 디바이스를 온보딩하는 경우 드롭다운 메뉴에서 디바이스의 성능 계층을 선택해야 합니다.

**단계 9** 디바이스에 적용할 기본 라이선스를 선택합니다. **Next(다음)**를 클릭합니다.

**단계 10** CDO는 등록 키를 사용하여 명령을 생성합니다. 디바이스의 CLI에 전체 등록 키를 그대로 붙여넣습니다.

**단계 11** 디바이스의 온보딩이 시작됩니다. 선택적 단계로 Inventory(재고 목록) 페이지를 정렬하고 필터링하는 데 도움이 되도록 디바이스에 레이블을 추가할 수 있습니다. 레이블을 입력하고 파란색 더하기 버튼을 선택합니다. .

다음에 수행할 작업

디바이스가 동기화되면 CDO에서 디바이스가 클러스터링되었음을 자동으로 탐지합니다. 여기에서 Inventory(재고 목록) 페이지에서 방금 온보딩한 디바이스를 선택하고 오른쪽에 있는 Management(관리) 창 아래에 나열된 옵션 중 하나를 선택합니다. 다음 작업을 수행하는 것이 좋습니다.

- 아직 생성하지 않은 경우 사용자 환경에 맞게 보안을 사용자 지정하려면 사용자 지정 액세스 제어 정책을 생성합니다. 자세한 내용은 [FDM-관리 액세스 제어 정책, 358 페이지](#)를 참조하십시오.
- Cisco SAL(Security Analytics and Logging)을 활성화하여 CDO 대시보드에서 이벤트를 보거나 보안 분석을 위해 디바이스를 Secure Firewall Management Center에 등록합니다.

## 스마트 라이선스 적용 또는 업데이트

**FDM-관리 디바이스에 새 스마트 라이선스 적용**

FTD(Firepower Threat Defense) 디바이스를 스마트 라이선싱하려면 다음 절차 중 하나를 수행합니다.

- 등록 키를 사용하여 온보딩하는 FDM 관리 디바이스의 스마트 라이선스입니다.
- 등록 키 또는 관리자 자격 증명을 사용하여 디바이스를 온보딩한 후 FDM 관리 디바이스에 스마트 라이선스를 부여합니다.



**Note** FDM 관리 디바이스에서 90일 평가 라이선스를 사용 중이거나 라이선스가 등록 취소되었을 수 있습니다.

## 등록 키를 사용하여 온보딩 시 FDM-관리 디바이스에 스마트-라이선스 부여

### Procedure

단계 1 [Cisco Smart Software Manager](#)에 로그인하고 새 스마트 라이선스 키를 생성합니다. 새로 생성된 키를 복사합니다. 자세한 내용은 [스마트 라이선싱 생성](#) 비디오를 참조하십시오.

The screenshot shows the Cisco Smart Software Licensing interface. At the top, it displays 'Cisco Software Central > Smart Software Licensing' and the user 'Example Co admin@example.com'. The main heading is 'Smart Software Licensing'. Below this, there are navigation tabs: Alerts, Inventory, Convert to Smart Licensing, Reports, Preferences, On-Prem Accounts, and Activity. A 'Virtual Account' section shows 'Example Co' with a description 'Licenses for US Region' and 'Default Virtual Account: No'. Underneath, there is a 'Product Instance Registration Tokens' section with a 'New Token...' button and a table of existing tokens.

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
MTU2MmRiY2MTYjJhY.	2021-Jul-30 19:43:22 (in 305...)	12 of 30	Allowed	CDO	admin1	Actions
NDFhZGRJNmMOTJk.	Expired		Allowed		admin2	Actions

단계 2 등록 키를 사용하여 FDM 관리 디바이스 온보딩을 시작합니다. 자세한 내용은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#) 또는 [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.

단계 3 온보딩 마법사 4단계의 **Smart License here**(여기에 스마트 라이선스)에서 **Activate**(활성화) 필드에 스마트 라이선스를 붙여넣고 **Next**(다음)를 클릭합니다.

**3** Subscription License

Please indicate if this FTD is physical or virtual:

Physical FTD Device

Virtual FTD Device

**1** Enable subscription licenses. CDO will attempt to enable the selected licenses when the device is connected to CDO and registered with the supplied Smart License. Learn more about [Cisco Smart Accounts](#).

Note: All virtual FTDs require performance tier license. Make sure your subscription licensing account contains the available licenses you need. Its important to choose the tier that matches the license you have in your account. Until you choose a tier, your FTDv defaults to FTDv50 selection.

License Type	Includes
<input checked="" type="checkbox"/> Essentials	Base Firewall Capabilities
<input type="checkbox"/> Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
<input type="checkbox"/> IPS	Intrusion Policy
<input type="checkbox"/> Malware Defense	File Policy
<input type="checkbox"/> URL	URL Reputation
<input type="checkbox"/> RA VPN <span style="border: 1px solid #ccc; padding: 2px;">VPN Only</span>	RA VPN

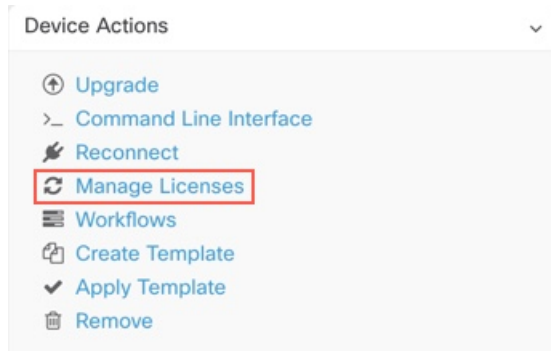
[Next](#)

단계 4 **Go to Inventory page**(재고 목록 페이지로 이동)를 클릭합니다.

단계 5 **FTD** 탭을 클릭하고 온보딩 프로세스의 진행 상황을 확인합니다. 디바이스에서 동기화를 시작하고 스마트 라이선스를 적용합니다.

이제 디바이스가 **Online**(온라인) 연결 상태임을 확인할 수 있습니다. 디바이스가 온라인 연결 상태가 아닌 경우 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리) > **Refresh Licenses**(라이선스 새로 고침)를 클릭하여 연결 상태를 업데이트합니다.

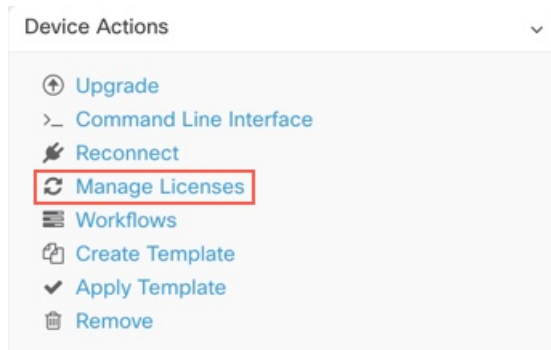
단계 6 스마트 라이선스를 FDM 관리 디바이스에 성공적으로 적용한 후 **Manage Licenses**(라이선스 관리)를 클릭합니다. 디바이스 상태에 "**Connected, Sufficient License**(연결됨, 라이선스가 충분함)"가 표시됩니다. 필요에 따라 라이선스를 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 [FDM-관리 디바이스 라이선싱 유형](#)을 참조하십시오.



## 등록 키 또는 자격 증명을 사용하여 디바이스 온보딩 후 FDM-관리 디바이스에 스마트-라이선스 부여

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 라이선스를 부여할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)를 클릭합니다.



- 단계 5 화면의 지침에 따라 Cisco Smart Software Manager에서 생성된 스마트 라이선스를 입력합니다.
- 단계 6 상자에 새 라이선스 키를 붙여넣고 **Register Device**(디바이스 등록)를 클릭합니다. 디바이스와 동기화되면 연결 상태가 'Online(온라인)'으로 변경됩니다. 스마트 라이선스를 FDM 관리 디바이스에 성공적으로 적용하면 디바이스 상태에 "**Connected, Sufficient License**(연결됨, 라이선스가 충분함)"가 표시됩니다. 필요에 따라 라이선스를 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 [FDM-관리 디바이스 라이선싱 유형](#)을 참조하십시오.

## FTD 디바이스의 기존 스마트 라이선스 업데이트

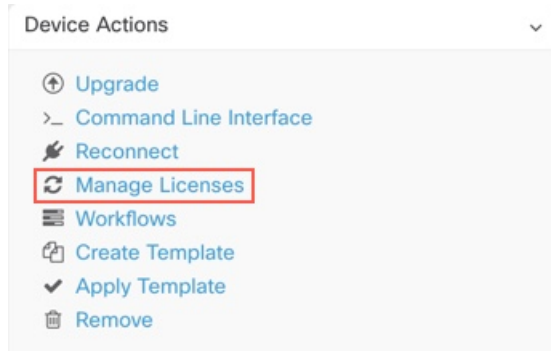
스마트 라이선스가 있는 FTD 디바이스에 새 스마트 라이선스를 적용할 수 있습니다. 디바이스 온보딩을 위해 선택한 방법에 따라 적절한 절차를 선택합니다.

## 등록 키를 사용하여 온보딩된 FDM-관리 디바이스에 적용되는 스마트 라이선스 변경

### Procedure

- 단계 1 Cisco Defense Orchestrator에서 해당 FDM 관리 디바이스를 제거합니다.
- 단계 2 해당 디바이스의 Secure Firewall device manager에 로그인하고 스마트 라이선스를 등록 취소합니다. 자세한 내용은 [스마트 라이선스 FDM-관리 디바이스 등록 취소](#)를 참조하십시오.

- 단계 3 CDO에서 등록 키를 사용하여 FDM 관리 디바이스를 다시 온보딩합니다. 자세한 내용은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.
- 단계 4 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 5 탭을 클릭합니다.
- 단계 6 온보딩 프로세스 중에 또는 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)를 클릭하여 새 스마트 라이선스를 적용합니다.



## 자격 증명을 사용하여 온보딩된 FDM-관리 디바이스에 적용되는 스마트 라이선스 변경

### Procedure

- 단계 1 해당 디바이스의 Secure Firewall device manager에 로그인하고 스마트 라이선스를 등록 취소합니다. 자세한 내용은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.
- 단계 2 Secure Firewall device manager의 FDM 관리 디바이스에 새 스마트 라이선스를 적용합니다.
  - a. **Smart License**(스마트 라이선스) 영역에서 **View Configuration**(구성 보기)을 클릭합니다.
  - b. **Register Now**(지금 등록)를 클릭하고 화면의 지침을 따릅니다.
- 단계 3 CDO의 **Inventory**(재고 목록) 페이지에서 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 4 **FTD** 디바이스를 클릭합니다. CDO에서 FDM 관리 디바이스의 구축된 구성 복사본을 만들고 CDO 데이터베이스에 저장할 수 있도록 FDM 관리 디바이스 구성 변경 사항이 있는지 확인합니다. 자세한 내용은 [변경 사항 읽기, 삭제, 확인 및 구축](#)을 참조하십시오.

## FDM-관리 디바이스의 DHCP 주소 지정에 대한 CDO 지원

내 FDM 관리 디바이스에서 사용하는 IP 주소가 변경되면 어떻게 됩니까?

CDO(Cisco Defense Orchestrator)에는 DHCP를 사용하여 통신 사업자가 제공한 IP 주소로 디바이스를 온보딩한 많은 ASA(Adaptive Security Appliance) 및 FDM 관리 디바이스 고객이 있습니다.

고정 IP 주소가 변경되었거나 DHCP로 인해 IP 주소가 변경되는 등 어떤 이유로든 디바이스의 IP 주소가 변경되면 CDO에서 디바이스의 IP 주소 변경 디바이스를 다시 연결할 수 있습니다.

이 필드는 CDO에서 관리하는 브랜치 구축 FDM 관리 디바이스의 경우와 관련하여 우려 사항을 나타냅니다. FDM 관리 디바이스의 외부 인터페이스에는 고정 IP가 필요합니다. 일부 SE의 보기에서는 FDM 관리 디바이스가 외부 인터페이스에 대해 구성된 DHCP 주소를 보유한 경우 관리 솔루션으로 CDO를 사용할 수 없습니다.

그러나 이 상황은 원격 브랜치 방화벽에 대한 VPN 터널이 있는 고객에게는 영향을 미치지 않습니다. 대다수의 고객이 브랜치에서 데이터 센터로 다시 연결되는 사이트 간 터널을 보유하고 있습니다. 사이트 간 VPN을 사용하여 디바이스에서 중앙 사이트에 연결하는 경우 외부 인터페이스의 DHCP는 CDO 및 모든 관리 플랫폼이 내부 정적 주소 지정 인터페이스(구성된 경우)를 통해 FW에 연결할 수 있기 때문에 문제가 되지 않습니다. 이는 권장되는 방법이며, 이 구축 모드를 사용하는 디바이스(+1000)를 많이 보유한 CDO 고객이 있습니다.

또한 인터페이스 IP 주소가 DHCP를 통해 발급된다고 해서 고객이 해당 IP를 사용하여 디바이스를 관리할 수 있는 것도 아닙니다. 이는 최적의 방법은 아니지만, 잠재적으로 CDO에서 IP 주소를 정기적으로 변경해야 하는 경험은 고객에게 장애로 여겨지지 않습니다. 이러한 상황은 CDO에만 해당되는 것은 아니며 ASDM, FDM 또는 SSH를 비롯한 외부 인터페이스를 사용하는 모든 관리자에서 발생합니다.

## FDM-관리 디바이스 라이선싱 유형

스마트 라이선싱 유형

다음 표에서는 FDM 관리 디바이스에 사용할 수 있는 라이선싱에 대해 설명합니다.

FDM 관리 디바이스 구매 시 기본 라이선싱이 자동으로 포함됩니다. 모든 추가 라이선싱은 선택 사항입니다.

라이선싱	기간	부여된 기능
라이선싱(자동 포함)	영구	구독 기간 라이선싱이 적용되지 않는 모든 기능.  이 토큰을 사용하여 등록된 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.

라이선스	기간	부여된 기능
	기간 기준	<p>침입 탐지 및 방지 - 침입 정책은 침입 및 익스플로잇의 트래픽을 분석하고, 선택적으로 문제가 되는 패킷을 삭제할 수 있습니다.</p> <p>파일 제어 - 파일 정책은 사용자가 특정 유형의 파일을 업로드(전송)하거나 다운로드(수신)하는 것을 탐지하고, 선택적으로 차단할 수 있습니다. 악성코드 라이선스가 필요한 AMP for Firepower를 사용하면 악성코드가 포함된 파일을 검사하고 차단할 수 있습니다. 모든 유형의 파일 정책을 사용하려면 라이선스가 있어야 합니다.</p> <p>보안 인텔리전스 필터링 - 트래픽이 액세스 제어 규칙을 기준으로 분석 대상이 되기 전에 선택한 트래픽을 삭제합니다. 동적 피드를 사용하면 최신 인텔리전스를 기반으로 연결을 즉시 삭제할 수 있습니다.</p>
악성코드	기간 기준	<p>악성코드를 확인하는 파일 정책으로서 Cisco AMP(Advanced Malware Protection)를 AMP for Firepower(네트워크 기반 Advanced Malware Protection) 및 Cisco Threat Grid와 함께 사용합니다.</p> <p>파일 정책은 네트워크를 통해 전송된 파일에서 악성코드를 탐지하고 차단할 수 있습니다.</p>
URL 라이선스	기간 기준	<p>범주 및 평판 기반 URL 필터링</p> <p>이 라이선스가 없어도 개별 URL에 대해 URL 필터링을 수행할 수 있습니다.</p>

라이선스	기간	부여된 기능
	라이선스 유형에 따라 기간 기준 또는 영구	<p>원격 액세스 VPN 컨피그레이션 Essentials 라이선스는 RA VPN을 구성하기 위해 내보내기 제어 기능을 허용해야 합니다. 디바이스를 등록할 때 내보내기 요구사항을 충족하는지를 선택합니다.</p> <p>Firepower Device Manager는 유효한 모든 AnyConnect 라이선스를 사용할 수 있습니다. 제공되는 기능은 라이선스 유형에 따라 달라지지 않습니다. 아직 구매하지 않은 경우 원격 액세스 VPN에 대한 라이선싱 요구 사항을 참조하십시오.</p> <p>또한 Cisco AnyConnect 주문 가이드, <a href="http://www.cisco.com/zh/na/products/anyconnect/">http://www.cisco.com/zh/na/products/anyconnect/</a>를 참조하십시오.</p>

## 가상 FDM-관리 디바이스 계층형 라이선스

버전 7.0에는 처리량 요구 사항 및 RA VPN 세션 제한을 기반으로 하는 가상 FDM-관리 디바이스에 대한 성능 계층형 스마트 라이선싱 지원이 추가되었습니다. 사용 가능한 성능 라이선스 중 하나로 가상 FDM-관리 디바이스에 라이선스가 부여되면 RA VPN에 대한 세션 제한이 설치된 가상 FDM-관리 디바이스 플랫폼 엔타이틀먼트 계층에 의해 결정되고 속도 제한기를 통해 적용됩니다.

CDO에서는 현재 계층형 스마트 라이선싱을 완전히 지원하지 않습니다. 다음 제한 사항을 참조하십시오.

- CDO를 통해 계층화된 라이선스를 수정할 수 없습니다. Secure Firewall device manager UI에서 변경해야 합니다.
- 클라우드 사용 Firewall Management Center에서 관리할 가상 FDM-관리 디바이스를 등록하면 계층화된 라이선스 선택이 기본 계층인 **Variable**(변수)로 자동 재설정됩니다.
- 버전 7.0 이상을 실행하는 가상 FDM-관리 디바이스를 온보딩하고 온보딩 프로세스 중에 기본 라이선스가 아닌 라이선스를 선택하면 계층화된 라이선스 선택이 자동으로 기본 계층인 **Variable**(변수)로 재설정됩니다.

위에 나열된 문제를 방지하려면 디바이스를 온보딩한 후 가상 FDM-관리 디바이스 라이선스의 계층을 선택하는 것이 좋습니다. 자세한 내용은 [스마트 라이선스 관리](#)를 참조하십시오.



## 디바이스용 스마트-라이선스 보기

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 FDM 관리 디바이스를 선택하여 현재 라이선스 상태를 확인합니다.
- 단계 5 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)를 클릭합니다.

**Manage Licenses**(라이선스 관리) 화면에는 다음 정보가 제공됩니다.

- **Smart License Agent**(스마트 라이선스 대리인) 상태: 90일 평가판 라이선스를 사용하는지 또는 Cisco Smart Software Manager에 등록했는지 여부를 표시합니다. 스마트 라이선스 대리인 상태는 다음과 같을 수 있습니다.
  - **"Connected," "Sufficient Licenses"**("연결됨", "충분한 라이선스") - 디바이스가 라이선스 기관에 연결하여 정상적으로 등록되었으며, 어플라이언스에 대한 라이선스 자격이 부여되었습니다. 디바이스는 현재 컴플라이언스 상태입니다.
  - **Out-of-Compliance**(규정 미준수) - 디바이스에 대해 사용 가능한 라이선스 자격이 없습니다. 라이선스 기능은 계속 작동합니다. 그러나 추가 자격을 구매하거나 확보하여 디바이스의 규정을 준수하는 상태가 될 수 있습니다.
  - **Authorization Expired**(권한 부여 만료됨) - 디바이스가 90일 이상 라이선싱 기관과 통신하지 않았습니다. 라이선스 기능은 계속 작동합니다. 이 상태에서 스마트 라이선스 에이전트는 권한 부여 요청을 다시 시도합니다. 다시 시도가 성공하면 대리인은 **Out-of-Compliance**(규정 미준수) 또는 **Authorized**(권한 있음) 상태로 설정되며 새 권한 부여 기간이 시작됩니다. 이 경우 디바이스를 수동으로 동기화해 보십시오.
- **License Registration**(라이선스 등록): 이미 온보딩된 FDM 관리 디바이스에 스마트 라이선스를 적용할 수 있습니다. 등록된 경우 Cisco Smart Software Manager에 대한 연결 상태와 각 라이선스 유형의 상태를 확인할 수 있습니다.
- **License Status**(라이선스 상태): FDM 관리 디바이스에서 사용 가능한 라이선스(선택 사항)의 상태를 표시합니다. 라이선스를 통해 제어하는 기능을 사용하도록 라이선스를 설정할 수 있습니다.

## 선택 가능한 라이선스 활성화 또는 비활성화

90일 평가 라이선스 또는 전체 라이선스를 사용하는 FDM 관리 디바이스에서 필요에 따라 라이선스를 활성화(등록)할 수 있습니다. 라이선스를 통해 제어되는 기능을 사용하려면 라이선스를 활성화해야 합니다.

필요에 따라 기간별 라이선스가 적용되는 기능을 더 이상 사용하지 않으려는 경우 라이선스를 비활성화(해제)할 수 있습니다. 비활성화하는 라이선스는 Cisco Smart Software Manager 계정에서 해제되므로 다른 디바이스에 적용할 수 있습니다.

평가 모드에서는 필요에 따라 라이선스의 평가 버전을 활성화하고 모든 작업을 수행할 수도 있습니다. 이 모드에서 라이선스는 디바이스를 등록할 때까지 Cisco Smart Software Manager에 등록되지 않습니다.



**Note** 평가 모드에서는 라이선스를 활성화할 수 없습니다.

### Before you begin

라이선스를 비활성화하기 전에 해당 라이선스를 사용하고 있지 않은지 확인합니다. 라이선스가 필요한 정책은 재작성하거나 삭제합니다.

고가용성 컨피그레이션에서 작동 중인 유닛의 경우 액티브 유닛에서만 라이선스를 활성화하거나 비활성화합니다. 다음번 구성 구축 시에 스탠바이 유닛이 필요한 라이선스를 요청하거나 해제할 때 변경사항이 스탠바이 유닛에 반영됩니다. 라이선스를 활성화하는 경우에는 Cisco Smart Software Manager 어카운트에 사용 가능한 라이선스가 충분한지 확인해야 합니다. 그렇지 않으면 각 유닛의 컴플라이언스 상태가 서로 다를 수 있습니다.

필요에 따라 라이선스를 활성화하거나 비활성화하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 **Inventory**(재고 목록) 페이지에서 원하는 FDM 관리 디바이스를 선택하고 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)를 클릭합니다. 그러면 **Manage Licenses**(라이선스 관리) 화면이 나타납니다.
- 단계 2 필요에 따라 각 라이선스의 슬라이더 컨트롤을 클릭하여 라이선스를 활성화하거나 비활성화하도록 설정합니다. 활성화되면 라이선스 상태가 OK(정상)로 표시됩니다.
  - **Enabled**(활성화됨): Cisco Smart Software Manager 계정에 라이선스를 등록하고 제어되는 기능을 활성화합니다. 이제 라이선스를 통해 제어되는 정책을 구성하고 구축할 수 있습니다.
  - **Disabled**(비활성화됨): Cisco Smart Software Manager 계정에서 라이선스를 등록 취소하고 제어되는 기능을 비활성화합니다. 이렇게 하면 새 정책에서 기능을 구성할 수 없으며 해당 기능을 사용하는 정책을 구축할 수도 없습니다.
- 단계 3 **Save**(저장)를 클릭하여 변경사항을 저장합니다.

## 만료되거나 비활성화된 선택 가능한 라이선스의 영향

선택 가능한 라이선스가 만료되어도 해당 라이선스를 필요로 하는 기능은 계속 사용할 수 있습니다. 그러나 라이선스는 컴플라이언스 상태가 아닌 것으로 표시되며, 라이선스를 컴플라이언스 상태로 다시 설정하려면 라이선스를 구매하여 계정에 추가해야 합니다.

선택 가능한 라이선스를 비활성화하면 시스템은 다음과 같이 대응합니다.

- **악성코드 라이선스:** 시스템이 AMP 클라우드 쿼리를 중지하며 AMP 클라우드에서 전송하는 회귀적 이벤트 확인도 중지합니다. 악성코드 탐지를 적용하는 파일 정책을 포함하는 기존 액세스 제어 정책은 재구축할 수 없습니다. 악성코드 라이선스가 비활성화된 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 이 기간이 만료되고 나면 시스템은 해당 파일에 사용할 수 없음 상태를 할당합니다.
- : 시스템이 더 이상 침입 또는 파일 제어 정책을 적용하지 않습니다. 보안 인텔리전스 정책의 경우 시스템은 더 이상 정책을 적용하지 않고 피드 업데이트 다운로드를 중지합니다. 라이선스가 필요한 기존 정책은 재구축할 수 없습니다.
- **URL:** URL 범주 조건이 포함된 액세스 제어 규칙의 URL 필터링이 즉시 중지되며 시스템이 URL 데이터에 대한 업데이트를 더 이상 다운로드하지 않습니다. 범주 및 평판 기반 URL 조건이 들어 있는 규칙을 포함하는 기존 액세스 제어 정책은 재적용할 수 없습니다.
- : 원격 액세스 VPN 구성을 편집할 수는 없지만, 제거할 수는 있습니다. 사용자는 RA VPN 컨피그레이션을 사용하여 계속 연결할 수 있습니다. 그러나 디바이스 등록을 변경하여 시스템이 더 이상 내보내기 방식을 준수하지 않는 경우에는 원격 액세스 VPN 구성이 즉시 중지되며, 원격 사용자가 VPN을 통해 연결할 수 없습니다.

## Firewall Device Manager 모델 생성 및 가져오기

Cisco Defense Orchestrator는 CDO 테넌트에 있는 FDM 관리 디바이스의 전체 구성을 JSON 파일 형식으로 내보낼 수 있는 기능을 제공합니다. 그런 다음 이 파일을 다른 테넌트에 Firewall Device Manager 모델로 가져와서 해당 테넌트의 새 디바이스에 적용할 수 있습니다. 이 기능은 관리하는 여러 테넌트에서 FDM 관리 디바이스의 구성을 사용하려는 경우에 유용합니다.



**Note** FDM 관리 디바이스에 규칙 집합이 포함되어 있으면 구성을 내보낼 때 규칙 집합과 연결된 공유 규칙이 로컬 규칙으로 수정됩니다. 나중에 모델을 다른 테넌트로 가져와 FDM 관리 디바이스에 적용하면 디바이스에 로컬 규칙이 표시됩니다.

### FDM-관리 디바이스 구성 내보내기

FDM 관리 디바이스에 다음 구성이 있는 경우 구성 내보내기 기능을 사용할 수 없습니다.


- 고가용성
- Snort 3 활성화됨

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 FDM 관리 디바이스를 선택하고 오른쪽 창의 **Device Actions**(디바이스 작업)에서 **Export Configuration**(구성 내보내기)을 클릭합니다.

## FDM-관리 디바이스 구성 가져오기

### Procedure

- 단계 1 **Inventory**(재고 목록) 페이지에서 과란색 더하기() 버튼을 클릭하여 구성을 가져옵니다.
- 단계 2 오프라인 관리를 위해 구성을 가져오려면 **Import**(가져오기)를 클릭합니다.
- 단계 3 **Device Type**(디바이스 유형)을 **FTD**로 선택합니다.
- 단계 4 **Browse**(찾아보기)를 클릭하고 업로드할 구성 파일(JSON 형식)을 선택합니다.
- 단계 5 구성이 확인되면 디바이스 또는 서비스에 레이블을 지정하라는 메시지가 표시됩니다. 자세한 내용은 [레이블 및 필터링](#)을 참조하십시오.
- 단계 6 모델 디바이스에 레이블을 지정한 후에는 **Inventory**(재고 목록) 목록에서 볼 수 있습니다.

**Note**      구성의 크기 및 다른 디바이스 또는 서비스의 수에 따라 구성을 분석하는 데 시간이 걸릴 수 있습니다.

## CDO에서 디바이스 삭제

CDO에서 디바이스를 삭제하려면 다음 절차를 따르십시오.

### 프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 **Inventory**(인벤토리) 페이지로 이동합니다.
- 단계 3 삭제할 디바이스를 찾아 디바이스 행에서 디바이스를 확인하고 선택합니다.
- 단계 4 오른쪽에 있는 디바이스 작업 패널에서 **Remove**(제거)를 선택합니다.

단계 5 메시지가 표시되면 **OK(확인)**를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보딩 상태로 유지하려면 **Cancel(취소)**를 선택합니다.

FDM 관리 HA 쌍의 두 디바이스를 동시에 삭제해야 합니다. 개별 피어가 아닌 FDM 관리 HA 쌍 이름을 클릭합니다.

## 오프라인 관리를 위한 디바이스 컨피그레이션 가져오기

오프라인 관리를 위해 디바이스의 구성을 가져오면 네트워크의 라이브 디바이스에서 작업하지 않고도 디바이스의 구성을 검토하고 최적화할 수 있습니다. CDO는 이러한 업로드된 구성 파일을 "모델"이라고도 합니다.

이러한 디바이스의 구성을 CDO로 가져올 수 있습니다.

- ASA(Adaptive Security Appliance)
- FTD(Firepower Threat Defense) FTD 모델 생성 및 가져오기를 참고하십시오.
- ASR(Aggregation Services Router) 및 ISR(Integrated Services Router)과 같은 Cisco IOS 디바이스

## FDM-관리 디바이스 백업

FDM 관리 디바이스를 이전 상태로 복원할 수 있도록 디바이스의 시스템 구성을 백업하는 데 Cisco Defense Orchestrator를 사용할 수 있습니다. 백업은 구성만 포함하며 시스템 소프트웨어는 포함하지 않습니다. 디바이스를 완전히 재이미징해야 하는 경우 소프트웨어를 다시 설치해야 합니다. 그런 다음 백업을 업로드하고 구성을 복원할 수 있습니다. CDO는 디바이스에 대해 만들어진 마지막 5개의 백업을 저장합니다. 새 백업이 발생하면 최신 백업을 저장하기 위해 가장 오래된 백업이 삭제됩니다.



**Note** 백업에는 관리 IP 주소 구성이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 구성을 복원할 수도 있습니다.

구성 데이터베이스는 백업하는 동안 잠겨 있습니다. 백업 중에는 정책, 대시보드 등을 볼 수는 있지만 구성을 변경할 수는 없습니다. 복원 중에는 시스템을 완전히 사용할 수 없게 됩니다.

여러 디바이스에서 백업 일정을 일관되게 만들기 위해 고유한 기본 백업 일정을 구성할 수 있습니다. 특정 디바이스에 대한 백업을 예약할 때 자신의 기본 설정을 사용하거나 변경할 수 있습니다. 매일에서 월 1회 반복 백업을 예약하고 주문형 백업을 수행할 수 있습니다. 백업을 다운로드한 다음 위협 방어 디바이스 관리자를 사용하여 복원할 수도 있습니다.

**CDO**를 사용하여 **FDM** 관리 디바이스를 백업 및 복원하기 위한 요구 사항 및 모범 사례

- CDO는 소프트웨어 버전 6.5 이상을 실행하는 FDM 관리 디바이스를 백업할 수 있습니다.

- FDM 관리 디바이스를 등록 키를 사용하여 CDO에 온보딩해야 합니다.
- 두 디바이스가 동일한 모델이며 동일한 버전의 소프트웨어(같은 시기에 릴리스되었을 뿐만 아니라 빌드 번호도 동일해야 함)를 실행하는 경우에만 교체 디바이스에 백업을 복원할 수 있습니다. 예를 들어 소프트웨어 버전 6.6.0-90을 실행하는 FDM 관리 디바이스의 백업은 6.6.0-90을 실행하는 FDM 관리 디바이스로만 복원할 수 있습니다. 백업 및 복원 프로세스를 사용하여 어플라이언스 간에 구성을 복사하지 마십시오. 백업 파일은 어플라이언스를 고유하게 식별하는 정보를 포함하므로 이러한 방식을 통해 공유할 수 없습니다.
- CDO에서 Secure Firewall Threat Defense 백업 기능이 작동하려면, 위협 방어가 테넌트 지역을 기반으로 이러한 CDO URL 중 하나에 액세스해야 합니다.
  - [edge.us.cdo.cisco.com](https://edge.us.cdo.cisco.com)
  - [edge.eu.cdo.cisco.com](https://edge.eu.cdo.cisco.com)
  - [edge.apj.cdo.cisco.com](https://edge.apj.cdo.cisco.com)
- 포트 443에 HTTPS 프로토콜에 대한 외부 및 아웃바운드 액세스 권한이 있는지 확인합니다. 포트가 방화벽 뒤에서 차단된 경우 백업 및 복원 프로세스가 실패할 수 있습니다.

#### 모범 사례

백업하려는 디바이스는 CDO에서 동기화됨 상태여야 합니다. CDO는 CDO가 아닌 디바이스에서 디바이스 구성을 백업합니다. 따라서 디바이스가 동기화되지 않은 상태이면 CDO의 변경 사항이 백업되지 않습니다. 디바이스가 충돌 감지 상태이면 해당 변경 사항이 백업됩니다.

#### 관련 정보:

- [기본 반복 백업 일정 구성](#)
- [단일 FDM-관리 디바이스에 대한 반복 백업 일정 구성](#)
- [FDM-관리 온디맨드 디바이스 백업](#)
- [디바이스 백업 다운로드](#)
- [백업 편집](#)
- [FDM-관리 디바이스에 백업 복원, on page 228](#)

## FDM-관리 온디맨드 디바이스 백업

이 절차는 필요한 경우 복원할 수 있도록 FDM 관리 디바이스를 백업하는 방법을 설명합니다.

#### 시작하기 전에

FDM 관리 디바이스를 백업하기 전에 이러한 [FDM-관리 디바이스 백업](#)를 검토하십시오.

## 절차

## Procedure

- 
- 단계 1 (선택 사항) 백업에 대한 [변경 요청 관리](#)를 생성합니다.
  - 단계 2 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
  - 단계 3 **Devices**(디바이스) 탭을 클릭합니다.
  - 단계 4 **FTD** 탭을 클릭하고 백업할 디바이스를 선택합니다.
  - 단계 5 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Backups**(백업 관리)를 클릭합니다.
  - 단계 6 **Backup Now**(지금 백업)를 클릭합니다. 디바이스가 **Backing Up**(백업 중) 구성 상태로 전환됩니다.

백업이 완료되면 Cisco Defense Orchestrator는 백업이 시작되기 전의 디바이스 구성 상태를 표시합니다. 변경 로그 페이지를 열어 "Backup completed successfully(백업이 성공적으로 완료되었습니다)."라는 설명이 포함된 최근 변경 로그 레코드를 찾을 수도 있습니다.

1단계에서 변경 요청을 생성한 경우 해당 값으로 필터링하여 변경 로그 항목을 찾을 수도 있습니다.

- 단계 7 1단계에서 변경 요청을 생성한 경우 더 이상 예기치 않게 변경 사항을 변경 요청과 연결하지 않도록 변경 요청 값을 지우십시오.
- 

## 단일 FDM-관리 디바이스에 대한 반복 백업 일정 구성

시작하기 전에

FDM 관리 디바이스를 백업하기 전에 이러한 [FDM-관리 디바이스 백업](#)를 검토하십시오.

## 절차

## Procedure

- 
- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
  - 단계 3 **FTD** 탭을 클릭하고 백업할 디바이스를 선택합니다.
  - 단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Backups**(백업 관리)를 클릭합니다.
  - 단계 5 **Device Backups**(디바이스 백업) 페이지에서 **Set Recurring Backup**(반복 백업 설정)을 클릭하거나 **Recurring Backup**(반복 백업) 필드에서 일정을 클릭합니다. CDO는 테넌트의 모든 FDM 관리 디바이스에 대한 기본 백업 일정을 제공합니다. 자세한 내용은 [기본 반복 백업 일정 구성](#)을 참조하십시오.
  - 단계 6 백업을 수행할 시간을 24시간 단위로 선택합니다. UTC(Coordinated Universal Time) 시간대로 시간을 예약합니다.
  - 단계 7 **Frequency**(빈도) 필드에서 매일, 매주 또는 매월을 선택합니다.

- **Daily backups(매일 백업):** 예약된 백업에 이름과 설명을 지정합니다.
- **Weekly backups(매주 백업):** 백업을 수행할 요일을 선택합니다. 예약된 백업 시간에 이름과 설명을 지정합니다.
- **Monthly backups(매월 백업):** Days of Month(날짜) 필드를 클릭하고 백업을 예약할 날짜를 추가합니다. 참고: 31일을 입력했지만 해당 월에 31일이 없는 경우 백업이 수행되지 않습니다. 예약된 백업 시간에 이름과 설명을 지정합니다.

단계 8 **Save(저장)**를 클릭합니다. Device Backup(디바이스 백업) 페이지에서 Recurring Backup(반복 백업) 필드가 사용자가 설정한 백업 일정으로 교체되고 로컬 시간이 반영됩니다.

## 디바이스 백업 다운로드

이 절차는 FDM 관리 디바이스의 백업이 포함된 .tar 파일을 다운로드하는 방법을 설명합니다.


### Procedure

단계 1 탐색 모음에서 **Inventory(재고 목록)**를 클릭합니다.

단계 2 **Devices(디바이스)** 탭을 클릭합니다.

단계 3 **FTD** 탭과 다운로드할 백업이 있는 디바이스를 클릭합니다.

단계 4 오른쪽의 작업 창에서 **Manage Backups(백업 관리)**를 클릭합니다.

단계 5 다운로드할 백업을 선택하고 해당 행에서 다운로드 링크 생성 버튼 를 클릭합니다. 버튼이 "백업 이미지 다운로드"로 변경됩니다.

단계 6 이제 버튼에 백업 이미지 다운로드가 표시됩니다. 다음 중 하나를 수행합니다.


- 복원하려는 디바이스의 Firewall Device Manager에도 연결할 수 있는 디바이스에 있는 경우 백업 이미지 다운로드 버튼을 클릭하고 다운로드한 파일을 저장합니다. 기억할 수 있는 이름으로 저장하십시오.
- 복원하려는 디바이스의 FDM에도 연결할 수 있는 디바이스에 있지 않은 경우:
  - a. 백업 이미지 다운로드 버튼을 마우스 오른쪽 버튼으로 클릭하고 링크 주소를 복사합니다.  
**Important** 링크 주소는 다운로드 링크 생성 버튼을 클릭한 후 15분이 지나면 만료됩니다.
  - b. 이미지를 복원하려는 Secure Firewall Threat Defense의 Firewall Device Manager에 도달하는 디바이스에서도 브라우저를 엽니다.
  - c. 브라우저 주소 표시줄에 다운로드 링크를 입력하고 해당 디바이스에 백업 파일을 다운로드합니다. 기억할 수 있는 이름으로 저장하십시오.



## 백업 편집

이 절차를 통해 성공적인 FDM 관리 디바이스 다운로드의 이름 또는 설명을 편집할 수 있습니다.


### Procedure

- 
- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
  - 단계 3 **FTD** 탭을 클릭하고 편집할 디바이스를 선택합니다.
  - 단계 4 오른쪽의 작업 창에서 **Manage Backups**(백업 관리)를 클릭합니다.
  - 단계 5 편집할 백업과 해당 행을 선택하고 편집 아이콘  를 클릭합니다.
  - 단계 6 백업의 이름이나 설명을 변경합니다. 디바이스 백업 페이지에서 새 정보를 볼 수 있습니다.
- 

## 백업 삭제

CDO는 디바이스에 대해 생성된 마지막 5개의 백업을 저장합니다. 새 백업이 발생하면 최신 백업을 저장하기 위해 가장 오래된 백업이 삭제됩니다. 기존 백업을 삭제하면 보관할 백업과 삭제할 백업을 관리하는 데 도움이 될 수 있습니다.

### Procedure

- 
- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
  - 단계 3 **FTD** 탭을 클릭하고 삭제할 디바이스를 선택합니다.
  - 단계 4 오른쪽의 Actions(작업) 창에서 **Manage Backups**(백업 관리)를 클릭합니다.
  - 단계 5 삭제할 백업과 해당 행을 선택하고 휴지통  아이콘을 클릭합니다.
  - 단계 6 **OK**(확인)를 클릭하여 확인합니다.
- 

## 디바이스 백업 관리

Cisco Defense Orchestrator를 사용하여 생성하는 FDM 관리 디바이스의 백업은 Device Backups(디바이스 백업) 페이지에서 확인할 수 있습니다.

### Procedure

- 
- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭합니다.

단계 4 디바이스 테이블에 FDM 관리 디바이스만 표시하려면 필터 아이콘을 클릭하고 **Devices/Services**(디바이스/서비스) 아래에서 **FDM**을 선택합니다.

단계 5 원하는 디바이스를 선택합니다.

단계 6 **Device Actions**(디바이스 작업) 창에서 **Manage Backups**(백업 관리)를 클릭합니다. 해당 디바이스의 최신 백업을 5개까지 볼 수 있습니다.

### What to do next

백업을 복구하려면 [FDM-관리 디바이스에 백업 복원, on page 228](#)의 내용을 참조하십시오.

## FDM-관리 디바이스에 백업 복원

FDM 관리 관리 위협 방어 디바이스의 백업을 복원하기 전에 이 정보를 검토하십시오.

- FDM 관리 위협 방어 디바이스를 복원하기 전에 이러한 [FDM-관리 디바이스 백업](#)를 검토하십시오.
- 복원하려는 백업 복사본이 디바이스에 아직 없는 경우 복원 전에 백업을 먼저 업로드해야 합니다.
- 복원 중에는 시스템을 완전히 사용할 수 없게 됩니다. 백업이 복원되면 디바이스가 재부팅됩니다.
- 이 절차에서는 디바이스에 복원할 준비가 된 디바이스의 기존 백업이 있다고 가정합니다.
- 디바이스가 고가용성 쌍의 일부인 경우 백업을 복원할 수 없습니다. 먼저 **Device**(디바이스) > **High Availability**(고가용성) 페이지에서 **HA**를 해제해야 백업을 복원할 수 있습니다. 백업이 **HA** 구성을 포함하는 경우 디바이스가 **HA** 그룹에 다시 조인합니다. 두 유닛에서 동일한 백업을 복원하지 마십시오. 이렇게 하면 두 유닛이 모두 액티브로 설정됩니다. 대신 액티브로 설정할 유닛에서 백업을 먼저 복원한 후에 다른 유닛에서 해당하는 백업을 복원합니다.



**Note** 백업에는 관리 IP 주소 구성이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 구성을 복원할 수도 있습니다.


### Procedure

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭하고 복원할 디바이스를 선택합니다.

단계 4 오른쪽의 **Device Actions**(장치 작업)에서 **Manage Backups**(백업 관리)를 클릭합니다.

단계 5 복원하려는 백업을 선택합니다. 해당 행에서 다운로드 링크 생성 버튼 를 클릭합니다.

**Note** 링크 주소는 다운로드 링크 생성 버튼을 클릭한 후 15분이 지나면 만료됩니다.

단계 6 이제 버튼에 백업 이미지 다운로드가 표시됩니다. 다음 중 하나를 수행합니다.

- 복원하려는 디바이스의 Firewall Device Manager에도 연결할 수 있는 디바이스에 있는 경우 백업 이미지 다운로드 버튼을 클릭하고 다운로드한 파일을 저장합니다. 기억할 수 있는 이름으로 저장하십시오.
- 복원하려는 디바이스의 firewall device manager에도 연결할 수 있는 디바이스에 있지 않은 경우:
  - a. 백업 이미지 다운로드 버튼을 마우스 오른쪽 버튼으로 클릭하고 링크 주소를 복사합니다.
  - b. 이미지를 복원하려는 firewall device manager에 도달하는 디바이스에서도 브라우저를 엽니다.
  - c. 브라우저 주소 표시줄에 다운로드 링크를 입력하고 해당 디바이스에 백업 파일을 다운로드합니다. 기억할 수 있는 이름으로 저장하십시오.

단계 7 복원하려는 디바이스의 Firewall Device Manager에 로그인합니다.

단계 8 [Firepower Device Manager용 Cisco Firepower Threat Defense 컨피그레이션 가이드](#) 버전 6.5 이상을 엽니다. 시스템 관리 창으로 이동하여 백업 복원을 검색합니다. 해당 지침에 따라 방금 FDM 관리 디바이스에 다운로드한 이미지를 복원하십시오.

**Tip** 이미지를 복원하려면 firewall device manager에 이미지를 업로드해야 합니다.

단계 9 firewall device manager의 프롬프트를 따르십시오. 복원이 시작되면 브라우저와 firewall device manager의 연결이 끊어집니다. 복원이 완료되면 디바이스가 재부팅됩니다.

관련 정보:

- [FDM-관리 디바이스 백업](#)
- [FDM-관리 온디맨드 디바이스 백업](#)
- [단일 FDM-관리 디바이스에 대한 반복 백업 일정 구성](#)
- [디바이스 백업 다운로드](#)
- [백업 편집](#)

## FDM 소프트웨어 업그레이드 경로

**FDM** 버전 업그레이드

CDO를 사용하여 FDM 관리 방화벽을 업그레이드하는 경우, CDO가 업그레이드할 수 있는 버전을 결정하며 이 항목은 필요하지 않습니다. FDM 이미지의 자체 저장소를 유지 관리하고 자체 이미지를 사

용하여 FDM 관리 디바이스를 업그레이드하는 경우, 이 주제에서는 사용할 수 있는 업그레이드 경로에 대해 설명합니다.

FDM 관리 디바이스를 하나의 주요 또는 유지 보수 버전에서 다른 버전으로 직접 업그레이드할 수 있습니다. 예를 들어 버전 6.4.0을 6.5.0으로, 또는 버전 6.4.0을 7.0.1으로 업그레이드 할 수 있습니다. 특정 패치 레벨을 실행할 필요는 없습니다.

직접 업그레이드가 불가능한 경우 업그레이드 경로에 중간 버전(예: 버전 6.4.0 > 7.0.0 > 7.1.0)이 포함되어야 합니다.

**Table 11:** 주요 릴리스의 업그레이드 경로

대상 버전	대상 버전으로 업그레이드할 수 있는 가장 오래된 릴리스
7.3.x	7.0.0
7.2.x	6.6.0
7.1.x	6.5.0
7.0.x	6.4.0
6.7.x	6.4.0
6.6.x	6.4.0
6.5.0	6.4.0

### FDM 관리 디바이스 구성

한 버전의 패치를 다른 버전의 패치로 직접 업그레이드할 수 없습니다(예: 버전 6.4.0.1 > 6.5.0.1). 먼저 주요 릴리스로 업그레이드한 다음 해당 릴리스를 패치해야 합니다. 예를 들어 버전 6.4.0.1 > 6.5.0 > 6.5.0.1로 업그레이드해야 합니다.

### Firepower 핫픽스

CDO는 핫픽스 업데이트 또는 설치를 지원하지 않습니다. 디바이스 모델 또는 소프트웨어 버전에 사용 가능한 핫픽스가 있는 경우 구성된 관리자의 대시보드 또는 UI를 사용하는 것이 좋습니다. 디바이스에 핫픽스가 설치되면 CDO가 대역 외 구성 변경 사항을 탐지합니다.

### FDM 업그레이드 제거

CDO를 사용하여 주요 릴리스, 유지 보수 또는 패치 릴리스 유형을 제거하거나 다운그레이드할 수 없습니다.

Secure Firewall Threat Defense defense 버전 6.7.0부터는 Firepower Device Manager 또는 FTD CLI를 사용하여 성공적으로 업그레이드된 디바이스를 마지막 주요 또는 유지 보수 업그레이드 직전의 상태로 되돌릴 수 있습니다(스냅샷이라고도 함). 패치를 적용한 후 되돌리면 패치도 제거됩니다. 되돌린 후에는 업그레이드와 되돌리기 사이에 변경한 모든 구성을 다시 적용해야 합니다. **FDM 버전 6.5.0~6.6.x**로의 주요 또는 유지 보수 업그레이드를 되돌리려면 이미지를 재설치해야 합니다. 자세한 내용은

[Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 관리" 섹션을 참조하십시오.

### FDM 패치 제거

CDO 또는 FDM을 사용하여 FDM 패치를 제거할 수 없습니다. 패치를 제거하려면 주 또는 유지 보수 릴리스로 이미지 재설치해야 합니다.

### Snort 업그레이드

Snort는 제품의 기본 검사 엔진이며 사용자의 편의를 위해 Secure Firewall Threat Defense 소프트웨어에 패키징됩니다. 버전 6.7에는 언제든지 업그레이드하거나 되돌릴 수 있는 패키지 업데이트가 도입되었습니다. Snort 버전을 자유롭게 전환할 수는 있지만, Snort 2.0의 일부 침입 규칙은 Snort 3.0에는 없을 수 있으며 그 반대의 경우도 마찬가지입니다. 자세한 내용은 버전 6.7.0용 Firepower Device Manager 구성 가이드에서 차이점을 참조하십시오.

CDO UI에서 Snort 3을 사용하도록 FDM 관리 디바이스를 업그레이드하거나 Snort 3에서 Snort 2로 다시 되돌리려면 FTD의 경우 각각 [Snort 3.0으로 업그레이드](#) 및 [FDM-관리 디바이스용 Snort 3.0에서 되돌리기](#)를 참조하십시오.

## 기타 업그레이드 제한 사항

### 2100 시리즈

CDO는 어플라이언스 모드를 실행 중인 경우에만 Firepower 2100 Series 디바이스를 업그레이드할 수 있습니다.

- Firepower Threat Defense 디바이스는 항상 어플라이언스 모드입니다.

다음에 수행할 작업

이러한 명령에 대한 자세한 내용은 "[Cisco Firepower 2100 시작 가이드](#)"를 참조하십시오.

## 4100 및 9300 Series 디바이스

CDO는 4100 또는 9300 Series 디바이스에 대한 업그레이드를 지원하지 않습니다. 이러한 디바이스는 CDO 외부에서 업그레이드해야 합니다.

관련 정보:

- [FDM-관리 디바이스 업그레이드 사전 요건](#)
- [단일 FTD 디바이스 업그레이드](#).
- [대량 FDM-관리 디바이스 업그레이드](#)
- [FDM-관리 고가용성 쌍 업그레이드](#)

## FDM-관리 디바이스 업그레이드 사전 요건

Cisco Defense Orchestrator(CDO)는 개별 디바이스 또는 HA 쌍에 설치된 Firewall Device Manager(FDM) 이미지를 업그레이드하는 데 도움이 되는 마법사를 제공합니다.

마법사는 호환 가능한 이미지를 선택하고 설치하고 디바이스를 재부팅하여 업그레이드를 완료하는 프로세스를 안내합니다. Cisco에서는 CDO에서 선택한 이미지가 FDM 관리 디바이스에 복사되고 설치된 이미지인지 확인하여 업그레이드 프로세스를 보호합니다. 업그레이드하는 FDM 관리 디바이스는 인터넷에 대한 아웃바운드 액세스 권한이 있어야 합니다.

FDM 관리 디바이스에 인터넷에 대한 아웃바운드 액세스 권한이 없는 경우 Cisco.com에서 원하는 이미지를 다운로드하여 자체 저장소에 저장하고 업그레이드 마법사에 해당 이미지에 대한 맞춤형 URL을 제공하면 CDO가 해당 이미지를 사용하여 업그레이드를 수행할 수 있습니다. 그러나 이 경우에는 어떤 이미지로 업그레이드할지 결정합니다. CDO는 이미지 무결성 확인 또는 디스크 공간 확인을 수행하지 않습니다.

### 컨피그레이션 사전 요구 사항

- FDM 관리 디바이스에서 DNS를 활성화해야 합니다. 자세한 내용은 디바이스에서 실행 중인 버전의 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 시스템 관리 장의 "DNS 구성" 섹션을 참조하십시오.
- CDO의 이미지 저장소에서 업그레이드 이미지를 사용하는 경우 FDM 관리 디바이스에서 인터넷에 연결할 수 있어야 합니다.
- FDM 관리 디바이스가 CDO에 성공적으로 온보딩되었습니다.
- FDM 관리 디바이스에 연결할 수 없습니다.
- FDM 관리 디바이스가 동기화됩니다.
  - CDO에서 보류 중인 변경 사항이 있는 디바이스를 업데이트하고 변경 사항을 수락하지 않으면 업그레이드가 완료된 후 보류 중인 변경 사항이 손실됩니다. 업그레이드하기 전에 보류 중인 변경 사항을 구축하는 것이 가장 좋습니다.
  - firewall device manager에서 변경 사항을 준비했으며 디바이스가 동기화되지 않은 경우 자격 확인 시 CDO에서 업그레이드가 실패합니다.

### FTD를 실행하는 4100 및 9300 Series

CDO는 4100 또는 9300 Series 디바이스에 대한 업그레이드를 지원하지 않습니다. 이러한 디바이스는 CDO 외부에서 업그레이드해야 합니다.

### 소프트웨어 및 하드웨어 요구 사항

CDO는 클라우드 관리 플랫폼입니다. 소프트웨어 업데이트는 시간이 지남에 따라 릴리스되며 일반적으로 하드웨어에 의존하지 않습니다. 지원되는 하드웨어 유형에 대한 자세한 내용은 [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 참조하십시오.

firewall device manager 소프트웨어를 실행하는 디바이스에는 최적의 성능을 위한 권장 업그레이드 경로가 있습니다. 자세한 내용은 [FDM 소프트웨어 업그레이드 경로](#)를 참조하십시오.

업그레이드 참고 사항

업그레이드 중에는 디바이스에 변경 사항을 구축할 수 없습니다.

관련 정보:

- [FDM 소프트웨어 업그레이드 경로](#)
- [단일 FTD 디바이스 업그레이드](#)
- [대량 FDM-관리 디바이스 업그레이드](#)
- [FDM-관리 고가용성 쌍 업그레이드](#)

## 단일 FTD 디바이스 업그레이드

시작하기 전에

업그레이드하기 전에 [FDM-관리 디바이스 업그레이드 사전 요건](#), [FDM 소프트웨어 업그레이드 경로](#), [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 자세히 읽어보십시오. 이 문서에서는 원하는 Firepower 소프트웨어 버전으로 업그레이드하기 전에 알아야 할 모든 요구 사항 및 경고에 대해 설명합니다.

## Cisco Defense Orchestrator 저장소의 이미지로 단일 FDM-관리 디바이스 업그레이드

CDO의 저장소에 저장된 소프트웨어 이미지를 사용하여 독립형 FDM 관리 디바이스를 업그레이드하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 업그레이드할 디바이스를 선택합니다.
- 단계 5 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 6 1단계에서 **Use CDO Image Repository**(CDO 이미지 저장소 사용)를 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
- 단계 7 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.

- 단계 8 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.
- Warning** 진행 중인 업그레이드를 취소하려면 **Upgrade**(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 확인하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 9 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 10 **알림 탭**에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **작업 페이지**로 이동합니다.
- 단계 11 시스템 데이터베이스를 업그레이드합니다. **Firewall Device Manager**에서 이 단계를 수행해야 합니다. 자세한 내용은 **Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드**의 "시스템 데이터베이스 업데이트"를 참조하십시오.

## 자체 저장소의 이미지로 단일 FDM-관리 디바이스 업그레이드

소프트웨어 이미지를 찾기 위해 URL 프로토콜을 사용하여 독립형 FDM 관리 디바이스를 업그레이드하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 업그레이드할 디바이스를 선택합니다.
- 단계 5 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 6 1단계에서 **Specify Image URL**(이미지 URL 지정)을 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
- 단계 7 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 8 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.



**Warning** 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 Cisco Defense Orchestrator는 디바이스에서 변경 사항을 구축하거나 확인하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.

**단계 9** 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 Schedule Upgrade(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 Schedule Upgrade(업그레이드 예약) 버튼을 클릭합니다.

**단계 10** 알림 탭에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 작업 페이지로 이동합니다.

**단계 11** 시스템 데이터베이스를 업그레이드합니다. Firewall Device Manager에서 이 단계를 수행해야 합니다. 자세한 내용은 [Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 데이터베이스 업데이트"를 참조하십시오.

## 업그레이드 프로세스 모니터링

**Inventory**(재고 목록) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 단일 디바이스의 진행 상황을 볼 수 있습니다. CDO에서 해당 디바이스의 Device Upgrade(디바이스 업그레이드) 페이지로 이동합니다.

업그레이드가 실패하면 CDO는 메시지를 표시합니다. CDO는 업그레이드 프로세스를 자동으로 다시 시작하지 않습니다.



**Warning** 자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 [새 인증서 탐지됨](#)를 참조하십시오.

## 대량 FDM-관리 디바이스 업그레이드

시작하기 전에

업그레이드하기 전에 [FDM-관리 디바이스 업그레이드 사전 요건](#), [FDM 소프트웨어 업그레이드 경로](#), [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 자세히 읽어보십시오. 이 문서에서는 원하는 Firepower 소프트웨어 버전으로 업그레이드하기 전에 알아야 할 모든 요구 사항 및 경고에 대해 설명합니다.



**Note** 모두 동일한 소프트웨어 버전으로 업그레이드하는 경우에만 FDM 관리 디바이스를 대량 업그레이드할 수 있습니다.

## Cisco Defense Orchestrator 저장소의 이미지로 대량 FDM-관리 디바이스 업그레이드

CDO의 저장소에 저장된 소프트웨어 이미지를 사용하여 여러 FDM 관리 디바이스를 업그레이드하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 **필터**를 사용하여 대량 업그레이드에 포함할 디바이스 목록을 좁힐 수 있습니다.
- 단계 5 필터링된 디바이스 목록에서 업그레이드할 디바이스를 선택합니다.
- 단계 6 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 7 **Bulk Device Upgrade**(대량 디바이스 업그레이드) 페이지에 업그레이드할 수 있는 디바이스가 표시됩니다. 선택한 디바이스 중 업그레이드할 수 없는 디바이스가 있으면 CDO에서 업그레이드할 수 없는 디바이스를 볼 수 있는 링크를 제공합니다.
- 단계 8 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 9 1단계에서 **Use CDO Image Repository**(CDO 이미지 저장소 사용)를 클릭하여 업그레이드할 소프트웨어 이미지를 선택합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다. **Continue**(계속)를 클릭합니다.
- 단계 10 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 11 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.
 

**Warning** 진행 중인 업그레이드를 취소하려면 **Upgrade**(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드를 시작한 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 롤링하지 않습니다. 업그레이드를 취소한 후에도 디바이스가 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 12 **알림** 탭에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **작업 페이지**로 이동합니다.
- 단계 13 시스템 데이터베이스를 업그레이드합니다. Firewall Device Manager에서 이 단계를 수행해야 합니다. 디바이스가 실행 중인 버전에 대한 **Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드**의 시스템 데이터베이스 업데이트를 참조하십시오.

## 자체 저장소의 이미지를 사용하여 대량 FDM-관리 디바이스 업그레이드

소프트웨어 이미지를 찾기 위해 URL 프로토콜을 사용하여 여러 FDM 관리 디바이스를 업그레이드 하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 **필터**를 사용하여 대량 업그레이드에 포함할 디바이스 목록을 좁힐 수 있습니다.
- 단계 5 필터링된 디바이스 목록에서 업그레이드할 디바이스를 선택합니다.
- 단계 6 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 7 **Bulk Device Upgrade**(대량 디바이스 업그레이드) 페이지에 업그레이드할 수 있는 디바이스가 표시됩니다. 선택한 디바이스 중 업그레이드할 수 없는 디바이스가 있으면 Cisco Defense Orchestrator에서 업그레이드할 수 없는 디바이스를 볼 수 있는 링크를 제공합니다.
- 단계 8 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 9 1단계에서 **Specify Image URL**(이미지 URL 지정)을 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다.
- 단계 10 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 11 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.
 

**Warning** 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 폴링하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 12 **알림 탭**에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **작업 페이지**로 이동합니다.
- 단계 13 시스템 데이터베이스를 업그레이드합니다. Firewall Device Manager에서 이 단계를 수행해야 합니다. 자세한 내용은 [Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 데이터베이스 업데이트"를 참조하십시오.

## 대량 업그레이드 프로세스 모니터링

**Inventory**(인벤토리) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 벌크 업그레이드에 포함된 단일 디바이스의 진행 상황을 볼 수 있습니다. 탐색 창에서 **Jobs**(작업)을 클릭하고 대량 작업을 확장하여 진행 세부 정보를 볼 수도 있습니다.

업그레이드가 실패하면 CDO는 메시지를 표시합니다. CDO는 업그레이드 프로세스를 자동으로 다시 시작하지 않습니다.

## FDM-관리 고가용성 쌍 업그레이드

트래픽 중단 없이 HA 쌍을 업그레이드합니다. 스탠바이 디바이스는 보조 디바이스가 업그레이드되는 동안 트래픽 탐지를 계속 처리합니다.

HA 쌍을 업그레이드할 때 CDO는 업그레이드를 시작하기 전에 자격 확인을 실행하고 이미지 위치를 복사하거나 식별합니다. 고가용성 쌍의 보조 디바이스는 현재 액티브 디바이스인 경우에도 먼저 업그레이드됩니다. 보조 디바이스가 액티브 디바이스인 경우 페어링된 디바이스는 업그레이드 프로세스의 역할을 자동으로 전환합니다. 보조 디바이스가 성공적으로 업그레이드되면 디바이스가 역할을 전환한 다음 새 스탠바이 디바이스가 업그레이드됩니다. 업그레이드가 완료되면 기본 디바이스가 액티브 상태가 되고 보조 디바이스가 스탠바이 상태가 되도록 디바이스가 자동으로 구성됩니다.

업그레이드 프로세스 중에는 HA 쌍에 구축하지 않는 것이 좋습니다.

시작하기 전에

- 업그레이드하기 전에 보류 중인 모든 변경 사항을 액티브 디바이스에 구축합니다.
- 업그레이드 중에 실행 중인 작업이 없는지 확인합니다.
- HA 쌍의 두 디바이스가 모두 정상입니다.
- 업그레이드할 준비가 되었는지 확인합니다. CDO에서는 이전 버전으로 롤백할 수 없습니다.
- [FDM-관리 디바이스 업그레이드 사전 요건](#), [FDM 소프트웨어 업그레이드 경로](#), [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 읽고 업그레이드 프로세스 중에 발생할 수 있는 요구 사항 및 경고를 검토합니다.

## Cisco Defense Orchestrator 저장소의 이미지로 FDM-관리 HA 쌍 업그레이드

CDO의 저장소에 저장된 소프트웨어 이미지를 사용하여 FDM 관리 HA 쌍을 업그레이드하려면 다음 절차를 수행합니다.

### Procedure

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 업그레이드할 HA 쌍을 선택합니다.
- 단계 5 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 6 1단계에서 **Use CDO Image Repository**(CDO 이미지 저장소 사용)를 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
- 단계 7 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 8 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.
- Warning** 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 폴링하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 9 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 10 **알림 탭**에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **작업 페이지**로 이동합니다.
- 단계 11 시스템 데이터베이스를 업그레이드합니다. 이 단계는 FDM에서 수행해야 합니다. 자세한 내용은 [Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 데이터베이스 업데이트"를 참조하십시오.

## 자체 저장소의 이미지로 FDM-관리 HA 쌍 업그레이드

소프트웨어 이미지를 찾기 위해 URL 프로토콜을 사용하여 FDM 관리 HA 쌍을 업그레이드하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 업그레이드할 HA 쌍을 선택합니다.
- 단계 5 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.

- 단계 6** 1단계에서 **Specify Image URL**(이미지 URL 지정)을 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
- 단계 7** 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 8** 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.
- Warning** 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 Cisco Defense Orchestrator는 디바이스에서 변경 사항을 구축하거나 폴링하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 9** 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 10** **알림 탭**에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **작업 페이지**로 이동합니다.
- 단계 11** 시스템 데이터베이스를 업그레이드합니다. Firewall Device Manager에서 이 단계를 수행해야 합니다. 자세한 내용은 **Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드**의 "시스템 데이터베이스 업데이트"를 참조하십시오.

## 업그레이드 프로세스 모니터링

**Inventory**(재고 목록) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 단일 디바이스의 진행 상황을 볼 수 있습니다. Cisco Defense Orchestrator에서 해당 디바이스의 **Device Upgrade**(디바이스 업그레이드) 페이지로 이동합니다.

업그레이드 중에 시스템은 시스템 라이브러리를 업데이트하는 동안 HA를 일시 중단합니다. 여기에는 자동 구축이 포함되며 전체 업그레이드 프로세스 동안 정상 상태가 아닐 수 있습니다. 이것은 예상되는 동작입니다. 이 프로세스의 마지막 부분을 수행하는 동안에는 SSH 연결에 디바이스를 사용할 수 있으므로 업그레이드를 적용한 후 바로 로그인하는 경우 HA가 일시 중단된 상태로 표시될 수 있습니다. 업그레이드 프로세스 중에 시스템에 문제가 발생하고 HA 썬이 일시 중단된 것으로 보이는 경우, 액티브 디바이스의 Firewall Device Manager 콘솔에서 HA를 수동으로 재개합니다.



**Note** 업그레이드가 실패할 경우 CDO에서 메시지를 표시합니다. CDO는 업그레이드 프로세스를 자동으로 재시작하지 않습니다.

**Warning**

자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 [새 인증서 탐지됨](#)를 참조하십시오.

## Snort 3.0으로 업그레이드

Snort 3은 최신 snort 엔진 또는 Firepower 버전 6.7 이상에서 사용 가능한 오픈 소스 IPS(Intrusion Prevention System)를 사용하는 강력한 전처리기입니다. Snort 엔진은 악의적인 네트워크 활동을 정의하는 데 도움이 되는 일련의 규칙을 사용하며, 이러한 규칙을 사용하여 일치하는 패킷을 찾고 사용자에게 알림을 생성하며 이상적으로는 패킷 스니퍼, 패킷 로거 또는 더 전통적으로는 독립형 네트워크 IPS로 사용됩니다.

Snort 3에서는 이제 사용자 지정 침입 정책을 생성할 수 있습니다. Snort 3를 실행하는 모든 FDM 관리 디바이스에는 Cisco의 Talos Intelligence Group(Talos)에서 사전 정의된 침입 정책 집합이 있습니다. Snort 3에서는 이러한 기본 정책을 변경할 수 있지만, 보다 강력한 정책을 위해 기반 위에 구축하는 것이 좋습니다.

Snort 2에서는 맞춤형 정책을 생성할 수 없습니다.

### Snort 2에서 Snort 3으로 전환

Snort 버전을 자유롭게 전환할 수는 있지만, Snort 2.0의 일부 침입 규칙은 Snort 3.0에는 없을 수 있으며 그 반대의 경우도 마찬가지입니다. 기존 규칙에 대한 규칙 동작을 변경한 경우에는 해당 변경 사항이 유지되지 않습니다. 해당 변경 사항은 Snort 3으로 전환했다가 다시 Snort 2로 전환하거나 Snort 3으로 다시 전환하는 경우에는 유지되지 않습니다. 두 버전에 모두 있는 규칙의 규칙 동작에 대한 변경 사항은 유지됩니다. Snort 3과 Snort 2의 규칙 간 매핑은 일대일 또는 일대 다수가 될 수 있으므로 변경 사항을 가장 효과적으로 유지할 수 있습니다.

Snort 2에서 Snort 3으로 업그레이드하도록 선택하는 경우 Snort 엔진 업그레이드는 시스템 업그레이드와 유사합니다. 네트워크에 대한 트래픽 모니터링 중단을 최소화하려면 유지 보수 기간에 업그레이드하는 것이 좋습니다. Snort 버전 전환이 규칙이 트래픽을 처리하는 방식에 미치는 영향에 대해서는 *Firepower Device Manager* 구성 가이드의 [침입 정책 관리\(Snort3\)](#)를 참조하십시오.

**Tip**

**Inventory**(재고 목록) 페이지에서 Snort 버전으로 필터링할 수 있으며, 선택한 디바이스의 **Details**(세부 정보) 창에 디바이스에서 실행 중인 현재 버전이 표시됩니다.

### Snort 3 제한 사항

#### 라이선스 요건

Snort 엔진이 침입 및 악성코드 애널리틱스를 위해 트래픽을 처리하도록 허용하려면 FDM 관리 디바이스에 대해 활성화된 라이선스가 있어야 합니다. Firewall Device Manager를 통해 이 라이선스를 활성화하려면 Firewall Device Manager UI에 로그인하고 **Device**(디바이스) > **View Configuration**(구성 보기) > **Enable/Disable**(활성화/비활성화)로 이동하여 라이선스를 활성화합니다.

### 하드웨어 지원

다음 디바이스는 Snort 3을 지원합니다.

- FTD 1000 Series
- FTD 2100 Series
- FTD 4100 Series
- AWS를 사용하는 FTD 가상
- Azure를 사용하는 FTD 가상
- FTD를 사용하는 ASA 5500-X 시리즈

### 소프트웨어 지원

디바이스는 Firewall Device Manager 버전 6.7 이상을 실행하고 있어야 합니다. Cisco Defense Orchestrator에서는 버전 6.7 이상을 실행하는 디바이스에 대해 Snort 3 기능을 지원합니다.

FTD 1000 및 2000 Series의 경우 FXOS 패치 지원에 대한 자세한 내용은 [FXOS 번들 지원](#)을 참조하십시오.

### 구성 제한 사항

디바이스에 다음 구성이 있는 경우 CDO는 Snort 3으로의 업그레이드를 지원하지 않습니다.

- 디바이스가 버전 6.7 이상에서 실행되고 있지 않습니다.
- 디바이스에 보류 중인 변경 사항이 있는 경우 업그레이드하기 전에 변경 사항을 구축합니다.
- 디바이스가 현재 업그레이드 중인 경우 디바이스가 동기화될 때까지 디바이스를 업그레이드하거나 구축하지 마십시오.
- 디바이스가 가상 라우터로 구성된 경우



**Note** Snort 버전을 업그레이드하거나 되돌리는 경우, 시스템은 Snort 2 침입 정책과 Snort 3 침입 정책 간의 변경 사항을 구현하기 위해 자동으로 구축됩니다.

### 규칙 집합 및 Snort 3

현재 Snort 3은 전체 기능을 지원하지 않습니다. CDO 규칙 집합은 Snort 3 디바이스에서 지원되지 않습니다. 디바이스를 Firewall Device Manager 6.7 이상으로 동시에 업그레이드하고 Snort 2에서 Snort 3로 업그레이드하는 경우, 업그레이드 전에 구성된 모든 규칙 집합이 분리되고 그 안의 규칙이 개별 규칙으로 저장됩니다.

Snort 3에 대해 구성된 디바이스와 관련된 규칙 집합 지원의 전체 목록은 [규칙 집합, on page 431](#)의 내용을 참조하십시오.



## 동시에 디바이스와 침입 방지 엔진 업그레이드

CDO를 사용하면 디바이스를 버전 6.7 및 Snort 3로 업그레이드할 수 있습니다. 다음 절차를 사용하여 FTD 시스템을 업그레이드합니다.

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
  - 단계 3 **FTD** 탭을 클릭하고 업그레이드할 디바이스를 하나 이상 선택합니다.
  - 단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
  - 단계 5 업그레이드 토크를 **FTD System Upgrade**(FTD 시스템 업그레이드)로 설정합니다.
- FTD System Upgrade
  Intrusion Prevention Engine
- 단계 6 (선택 사항) CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다.
  - 단계 7 1단계에서 업그레이드 방법을 선택합니다. CDO 이미지 저장소 및 자체 저장소의 이미지를 사용합니다.
    - **Use CDO Image Repository**(CDO 이미지 저장소 사용) - 이 옵션을 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
    - **Specify Image URL**(이미지 URL 지정) - 이 옵션을 클릭하여 현재 저장소에 저장되어 있는 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
  - 단계 8 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
  - 단계 9 **Upgrade to Snort 3 Engine**(Snort 3 엔진으로 업그레이드)을 선택합니다.
  - 단계 10 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.

**Warning** 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 확인하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.

## 침입 방지 엔진 업그레이드

Snort 2가 설치된 버전 6.7을 이미 실행 중인 디바이스의 경우 다음 절차를 사용하여 Snort 엔진만 버전 3으로 업데이트합니다.

### Procedure

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

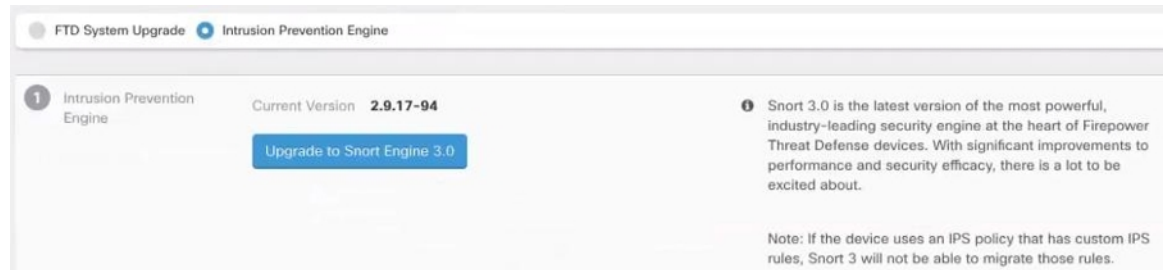
단계 3 **FTD** 탭을 클릭하고 업그레이드할 디바이스를 하나 이상 선택합니다.

단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.

단계 5 업그레이드 토글을 **Intrusion Prevention Engine**(침입 방지 엔진)으로 설정합니다.



단계 6 **Upgrade to Snort Engine 3.0**(Snort 엔진 3.0으로 업그레이드)을 클릭합니다.



단계 7 **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.

## 업그레이드 프로세스 모니터링



**경고!** 진행 중인 업그레이드를 취소하려면 **Upgrade**(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 확인하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.

**Inventory**(재고 목록) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 단일 디바이스의 진행 상황을 볼 수 있습니다. CDO에서 해당 디바이스의 **Device Upgrade**(디바이스 업그레이드) 페이지로 이동합니다.

업그레이드가 실패하면 CDO는 메시지를 표시합니다. CDO는 업그레이드 프로세스를 자동으로 다시 시작하지 않습니다.



**경고!** 자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 [새 인증서 탐지됨](#)를 참조하십시오.

## FDM-관리 디바이스용 Snort 3.0에서 되돌리기

Snort 2.0의 일부 침입 규칙은 Snort 3.0에 없을 수 있습니다. 2.0으로 다운그레이드하는 경우, 생성한 사용자 지정 침입 정책이 사용자 지정 정책에 사용된 기본 정책으로 변환됩니다. 가능한 한 규칙 작업 오버라이드가 유지됩니다. 두 개 이상의 사용자 지정 정책이 동일한 기본 정책을 사용하는 경우, 대부분의 액세스 제어 정책에 사용되는 사용자 지정 정책의 오버라이드는 유지되며 다른 사용자 지정 정책의 오버라이드는 손실됩니다. 이러한 "중복" 정책을 사용하는 액세스 제어 규칙은 이제 가장 많이 사용되는 사용자 지정 정책에서 생성된 기본 정책을 사용합니다. 모든 사용자 지정 정책이 삭제됩니다.

Snort 3.0에서 복귀하도록 선택하기 전에 *Firepower Device Manager* 구성 가이드의 [침입 정책 관리 \(Snort2\)](#)를 읽고 Snort 엔진 버전 전환이 현재 규칙 및 정책에 어떤 영향을 미치는지 확인합니다.



**Note** 버전 2로 되돌려도 Firepower 소프트웨어 버전은 제거되지 않습니다.

## Snort 3.0에서 되돌리기

Snort 버전을 변경하는 경우 시스템에서는 자동 구축을 수행하여 변경을 구현합니다. 개별 디바이스는 Snort 3.0에서 버전 2로만 되돌릴 수 있습니다.

침입 방지 엔진을 되돌리려면 다음 절차를 수행합니다.

### Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

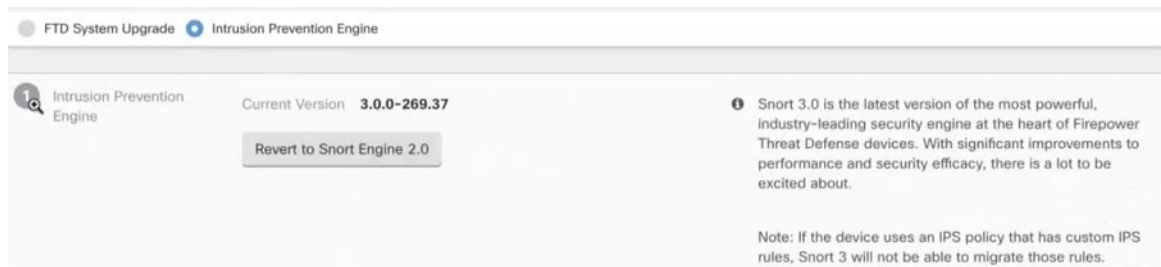
단계 3 **FTD** 탭을 클릭하고 되돌릴 디바이스를 클릭합니다.

단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.

단계 5 업그레이드 토글을 **Intrusion Prevention Engine**(침입 방지 엔진)으로 설정합니다.

FTD System Upgrade  Intrusion Prevention Engine

단계 6 1단계에서는 Snort 버전 3에서 되돌릴 것임을 확인하고 **Revert to Snort Engine 2**(Snort 엔진 2로 복귀)를 클릭합니다.



단계 7 **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.

## 보안 데이터베이스 업데이트 예약

FTD 디바이스에 대한 보안 데이터베이스를 확인하고 업데이트하는 예약된 작업을 생성하려면 다음 절차를 수행합니다.

### Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭하고 원하는 FTD 디바이스를 선택합니다.

단계 4 **Actions**(작업) 창에서 **Security Database Updates**(보안 데이터베이스 업데이트) 섹션을 찾아 추가 + 버튼을 클릭합니다.

**Note**      선택한 디바이스에 대해 기존에 예약된 작업이 있는 경우 편집 아이콘을 클릭하여 새 작업을 생성합니다. 새 작업을 생성하면 기존 작업을 덮어씁니다.

단계 5 다음을 사용하여 예약된 작업을 구성합니다.

- **Frequency**(빈도) - 업데이트를 매일, 매주 또는 매월 수행하도록 선택합니다.
- **Time**(시간) - 시간을 선택합니다. 표시되는 시간은 UTC입니다.
- **Select Days**(요일 선택) - 업데이트를 수행할 요일을 선택합니다.

단계 6 **Save**(저장)를 클릭합니다.

단계 7 디바이스의 구성 상태가 "데이터베이스 업데이트 중"으로 변경됩니다.

## 예약된 보안 데이터베이스 업데이트 편집

FTD 디바이스에 대한 보안 데이터베이스를 확인하고 업데이트하기 위해 기존의 예약된 작업을 편집하려면 다음 절차를 따르십시오.

### Procedure

---

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
  - 단계 3 **FTD** 탭을 클릭하고 원하는 FTD 디바이스를 선택합니다.
  - 단계 4 **Actions**(작업) 창에서 데이터베이스 업데이트 섹션을 찾고 편집 아이콘을 클릭합니다.
  - 단계 5 다음을 사용하여 예약된 작업을 편집합니다.
    - **Frequency**(빈도) - 업데이트를 매일, 매주 또는 매월 수행하도록 선택합니다.
    - **Time**(시간) - 시간을 선택합니다. 표시되는 시간은 UTC입니다.
    - **Select Days**(요일 선택) - 업데이트를 수행할 요일을 선택합니다.
  - 단계 6 **Save**(저장)를 클릭합니다.
  - 단계 7 디바이스의 구성 상태가 "데이터베이스 업데이트 중"으로 변경됩니다.
-





# 3 장

## FTD 디바이스 구성

- 인터페이스, on page 250
- FXOS를 사용하여 Firepower 디바이스에 추가된 인터페이스 동기화, 294 페이지
- 라우팅, on page 295
- 개체, on page 302
- 보안 정책 관리, 358 페이지
- FDM 정책 구성, on page 358
- 가상 프라이빗 네트워크 관리, 459 페이지
- 템플릿, on page 562
- FDM-관리 고가용성, on page 571
- FDM-관리 디바이스 설정, 582 페이지
- CDO 명령줄 인터페이스, on page 594
- 대량 명령줄 인터페이스, on page 596
- 디바이스 관리를 위한 CLI 매크로, on page 600
- 명령줄 인터페이스 설명서, on page 604
- CLI 명령 결과 내보내기, on page 604
- CDO 공용 API, 607 페이지
- REST API 매크로 생성, on page 608
- 변경 사항 읽기, 삭제, 확인 및 구축, 615 페이지
- 모든 디바이스 구성 읽기, on page 616
- FDM-관리 디바이스에서 CDO로 구성 변경 사항 읽기, on page 618
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 620 페이지
- CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축, on page 621
- 디바이스에 변경 사항 배포, on page 622
- 디바이스 구성 대량 구축, on page 623
- 예약된 자동 배포, on page 624
- 구성 변경 사항 확인, on page 626
- 변경 사항 취소, on page 627
- 디바이스의 대역 외 변경 사항, on page 628
- Defense Orchestrator와 디바이스 간 구성 동기화, 628 페이지

- 충돌 탐지, on page 629
- 디바이스에서 대역외 변경 사항 자동 수락, on page 630
- 구성 충돌 해결, on page 631
- 디바이스 변경 사항에 대한 폴링 예약, on page 632
- 보안 데이터베이스 업데이트 예약, 633 페이지
- FDM-관리 디바이스 보안 데이터베이스 업데이트, on page 635

## 인터페이스

CDO(Cisco Defense Orchestrator)를 사용하여 FTD(Firepower Threat Defense) 디바이스에서 데이터 인터페이스 또는 관리/진단 인터페이스를 구성하고 편집할 수 있습니다.

현재 CDO는 라우팅 인터페이스 및 브리지 그룹만 구성할 수 있습니다. 구성 패시브 인터페이스는 지원하지 않습니다.

## Firepower 인터페이스 구성에 대한 지침 및 제한 사항

Cisco Defense Orchestrator(CDO)를 사용하여 디바이스를 구성할 때는 인터페이스 구성에 여러 가지 제한이 적용됩니다. 다음 기능이 필요한 경우 Firepower Management Center를 사용하여 디바이스를 구성해야 합니다.

### 방화벽

- 라우팅 방화벽 모드만 지원됩니다. 투명 방화벽 모드 인터페이스는 구성할 수 없습니다.
- 물리적 Firepower 1010 디바이스만 스위치 포트 모드에 대해 구성된 인터페이스를 지원합니다. 자세한 내용은 [FDM-관리 디바이스에 대한 스위치 포트 모드 인터페이스](#)를 참조하십시오.

### 수동

- 현재 Cisco Defense Orchestrator(CDO)는 패시브 또는 ERSPAN 인터페이스를 구성할 수 없는 인터페이스 테이블 광고에서 패시브 인터페이스 모드를 식별하지 않습니다. 패시브 인터페이스를 구성하고 식별하려면 FDM 관리 UI를 사용해야 합니다.

### IPS 전용 모드

- 인터페이스를 IPS 전용 처리를 위해 인라인(인라인 집합 내) 또는 인라인 탭으로 구성할 수는 없습니다. IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 그에 비해 방화벽 모드 인터페이스는 흐름 유지, IP 및 TCP 레이어 둘 다에서 흐름 상태 추적, IP 조각 모음 및 TCP 표준화와 같은 방화벽 기능에 트래픽을 적용합니다.
- 보안 정책에 따라 이 방화벽 모드 트래픽에 대해 IPS 기능을 선택 사항으로 구성할 수도 있습니다.



## EtherChannel

CDO는 버전 6.5 이상을 실행하는 디바이스에 대한 읽기, 생성 및 기능을 지원합니다. Etherchannel 인터페이스를 생성하는 방법에 대한 자세한 내용은 [FDM-관리 디바이스에 대한 EtherChannel 인터페이스 추가](#)를 참조하십시오. 생성하려면

- 물리적 Firepower 디바이스에서 최대 48개의 EtherChannel을 구성할 수 있지만, 한 번에 활성화할 수 있는 인터페이스의 수는 디바이스 모델에 따라 다릅니다. 디바이스별 제한 사항은 [디바이스별 제한 사항](#)을 참조하십시오.
- 채널 그룹의 모든 인터페이스는 미디어 유형 및 용량이 동일해야 하며 속도 및 듀플렉스를 동일하게 설정해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 없습니다.
- EtherChannel을 연결하는 디바이스는 802.3ad EtherChannel도 지원해야 합니다.
- FDM 매니지드 디바이스는 VLAN 태그가 지정된 LACPDU를 지원하지 않습니다. Cisco IOS `vlan dot1q tag native` 명령을 사용하여 인접한 스위치에서 네이티브 VLAN 태그를 활성화할 경우, FDM 관리 디바이스에서는 태그 처리된 LACPDU를 제거합니다. 인접한 스위치에서 네이티브 VLAN 태그를 비활성화해야 합니다.
- 모든 FDM 관리 디바이스 컨피그레이션에서는 멤버 물리적 인터페이스 대신 논리적 EtherChannel 인터페이스를 참조합니다.



**Note** PortChannel로 설정된 인터페이스는 물리적 인터페이스, 이중 인터페이스만 사용할 수 있으며 하위 인터페이스는 브리지 그룹 멤버 인터페이스로 지원됩니다.

## 브리지 그룹

현재 CDO는 하나의 브리지 그룹 구성을 지원합니다. 디바이스가 브리지 그룹을 지원하는지 확인하려면 자세한 내용은 [FDM-관리 구성의 브리지 그룹 호환성](#)을 참조하십시오.

브리지 그룹에 인터페이스를 추가할 때는 다음 사항에 유의하십시오.

- 인터페이스에 이름이 있어야 합니다.
- 인터페이스에 대해 IPv4 또는 IPv6 주소(고정 주소 또는 DHCP를 통해 제공된 주소)가 정의되어 있으면 안 됩니다.
- BVI는 멤버 인터페이스로 VLAN 인터페이스 또는 기타 라우팅된 인터페이스를 가질 수 있지만, 단일 BVI에서 둘 다 멤버 인터페이스로 가질 수는 없습니다.
- BVI는 멤버 인터페이스로 VLAN 인터페이스 또는 기타 라우팅된 인터페이스를 가질 수 있지만, 단일 BVI에서 둘 다 멤버 인터페이스로 가질 수는 없습니다.
- 인터페이스는 PPPoE(Point-to-Point Protocol over Ethernet)일 수 없습니다.

- 인터페이스는 보안 영역(영역에 있는 경우)과 연결할 수 없습니다. 브리지 그룹에 인터페이스를 추가하려면 먼저 인터페이스에 대한 NAT 규칙을 삭제해야 합니다.
- 멤버 인터페이스는 개별적으로 활성화 및 비활성화합니다. 그러므로 사용하지 않는 인터페이스는 브리지 그룹에서 제거할 필요 없이 비활성화할 수 있습니다. 브리지 그룹 자체는 항상 활성화됩니다.
- 브리지 그룹의 멤버로 추가할 인터페이스를 구성할 수 있습니다. 인터페이스 요구 사항 및 생성에 대한 내용은 [브리지 그룹 구성](#)을 참조하십시오.

### Point-to-Point Protocol over Ethernet

- IPv4에 대해서는 PPPoE(Point-to-Point Protocol over Ethernet)를 구성할 수 없습니다. 인터넷 인터페이스가 DSL/케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하며 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우에는 FDM을 사용하여 이러한 설정을 구성해야 합니다.

### VLAN

VLAN 인터페이스 및 VLAN 멤버 구성에 대한 자세한 내용은 [FDM-관리 디바이스 VLAN 구성](#)을 참조하십시오. 스위치 포트 모드에 대한 VLAN 구성에 대한 자세한 내용은 [스위치 포트 모드에 대한 FDM-관리 디바이스 VLAN 구성](#)을 참조하십시오.

- 인터페이스는 물리적 인터페이스여야 합니다.
- 인터페이스는 관리 전용일 수 없습니다.
- 인터페이스는 BVI, 하위 인터페이스, 다른 VLAN 인터페이스, EtherChannel 등 다른 유형의 인터페이스로 연결할 수 없습니다.
- 인터페이스는 BVI 멤버 또는 etherchannel 멤버일 수 없습니다.
- 디바이스 모델은 다양한 수의 VLAN 멤버를 지원합니다. 자세한 내용은 [디바이스 모델별 VLAN 멤버의 최대 수](#)를 참조하십시오.




---

**Note** 사용자 환경에 VLAN을 구성하려면 자세한 내용은 [Firepower VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성](#)을 참조하십시오.

---

### 네트워크 모듈 카드

선택적 네트워크 모듈 설치: ASA 5515-X, 5525-X, 5545-X, 5555-X 및 Firepower 2100 Series 디바이스로 제한됩니다.

- 카드는 부트스트랩 중(즉, 초기 설치/리이미징 시 또는 로컬/제거 관리 간 전환 시)에만 검색됩니다. CDO는 이러한 인터페이스의 속도 및 듀플렉스를 올바른 기본값으로 설정합니다. 사용 가능한 인터페이스의 총 개수는 변경하지 않고 선택 사항인 카드를 인터페이스의 속도/듀플렉스 옵션을 변경하는 카드로 교체하는 경우, 시스템이 교체된 인터페이스에 대한 올바른 속도/듀플렉스 값을 인식하도록 디바이스를 재부팅합니다. 디바이스를 사용하는 SSH 또는 콘솔 세션에서

reboot 명령을 입력합니다. 그런 다음 시스템에서는 원래 설정을 자동으로 수정하지 않으므로 CDO를 사용하여 기능 변경 사항이 있는 각 물리적 인터페이스를 편집하고 유효한 속도 및 듀플렉스 옵션을 선택합니다. 시스템 행동을 수정하려면 변경 사항을 바로 구축합니다.

- FDM 관리 Secure Firewall 3100 시리즈 디바이스에서 네트워크 모듈을 활성화 또는 비활성화하거나 인터페이스의 브레이크아웃 온라인 삽입 및 제거(OIR)를 수행할 수 없습니다.



**Note** 카드를 인터페이스의 총 개수를 변경하는 카드로 교체하거나 다른 개체에서 참조하는 인터페이스를 제거하면 예기치 않은 문제가 발생할 수 있습니다. 이러한 유형의 변경을 수행해야 하는 경우, 먼저 제거할 인터페이스에 대한 모든 참조(예: 보안 영역 멤버십, VPN 연결 등)를 제거합니다. 또한, 변경을 수행하기 전에 백업을 수행하는 것이 좋습니다.

#### 가상 FDM-관리 디바이스의 인터페이스

- 가상 FDM 관리 디바이스를 다시 초기화하지 않고는 인터페이스를 추가하거나 제거할 수 없습니다. FDM 관리 디바이스에서 이러한 작업을 실행해야 합니다.



**Note** 인터페이스를 다른 속도/듀플렉스 기능이 있는 인터페이스로 교체하는 경우, 다음 절차에 따라 시스템이 새로운 속도/듀플렉스 값을 인식하도록 디바이스를 재부팅합니다. 장치의 CLI 콘솔에서 reboot 명령을 입력합니다. 그런 다음 시스템에서는 원래 설정을 자동으로 수정하지 않으므로 CDO에서는 기능 변경 사항이 있는 각 인터페이스를 편집하고 유효한 속도 및 듀플렉스 옵션을 선택합니다. 시스템 행동을 수정하려면 변경 사항을 바로 구축합니다.

## 디바이스 모델별 VLAN 멤버의 최대 수

디바이스 모델은 구성할 수 있는 VLAN 하위 인터페이스의 최대 수를 제한합니다. 하위 인터페이스는 데이터 인터페이스에서만 구성할 수 있으며 관리 인터페이스에서는 구성할 수 없습니다. 다음 표에서는 각 디바이스 모델의 제한 사항에 대해 설명합니다.

모델	VLAN 하위 인터페이스의 최대 수
Firepower 1010	60
Firepower 1120	512
Firepower 1140, Firepower 1150	1024
Firepower 2100	1024
Secure Firewall 3100	1024
Firepower 4100	1024

모델	VLAN 하위 인터페이스의 최대 수
Firepower 9300	1024
ASA 5508-X	50
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	100

## Firepower 데이터 인터페이스

CDO(Cisco Defense Orchestrator)는 FDM 관리 디바이스에서 라우팅 인터페이스 및 브리지 가상 인터페이스 구성을 지원합니다.

### 라우팅 인터페이스

각 레이어 3 라우팅 인터페이스(또는 하위 인터페이스)에는 고유한 서브넷의 IP 주소가 필요합니다. 이러한 인터페이스는 보통 스위치, 다른 라우터의 포트 또는 ISP/WAN 게이트웨이에 연결합니다.

고정 주소를 할당할 수도 있고, DHCP 서버에서 주소를 가져올 수도 있습니다. 그러나 DHCP 서버가 디바이스에서 고정으로 정의된 인터페이스와 같은 서브넷의 주소를 제공하는 경우 시스템은 DHCP 인터페이스를 비활성화합니다. DHCP를 사용하여 주소를 가져오는 인터페이스가 트래픽 전달을 중지하는 경우에는 주소가 디바이스의 다른 인터페이스에 대한 서브넷과 중복되는지 확인하십시오.

라우팅 인터페이스에서 IPv6 주소와 IPv4 주소를 모두 구성할 수 있습니다. IPv4 및 IPv6 모두에 대한 기본 경로를 구성해야 합니다. 이 작업은 Firepower Device Manager를 사용하여 FDM 관리 디바이스에서 수행해야 합니다. 기본 경로 구성에 대한 자세한 내용은 "[Firepower Device Manager 버전 x.x.x용 Cisco Firepower Threat Defense 구성 가이드](#)"의 기본 사항 > 라우팅을 참조하십시오.

### 브리지 그룹 및 브리지 가상 인터페이스

브리지 그룹은 FDM 관리 디바이스에서 경로 대신 브리징하는 인터페이스 그룹입니다. 브리지 인터페이스는 브리지 그룹에 속하며 모든 인터페이스는 동일한 네트워크에 있습니다. 브리지 그룹은 브리지 네트워크에 IP 주소가 있는 BVI(브리지 가상 인터페이스)로 표시됩니다. 브리지 그룹에 포함된 인터페이스를 "멤버"라고 합니다.

BVI의 이름을 지정하면 라우팅 인터페이스와 BVI를 라우팅할 수 있습니다. 이 경우 BVI는 멤버 인터페이스와 라우팅 인터페이스 간의 게이트웨이 역할을 합니다. BVI의 이름을 지정하지 않으면 브리지 그룹 멤버 인터페이스의 트래픽은 브리지 그룹을 벗어날 수 없습니다. 일반적으로는 인터넷에 멤버 인터페이스를 라우팅할 수 있도록 인터페이스 이름을 지정합니다.

FDM 관리 디바이스는 브리지 그룹을 하나만 지원합니다. 따라서 CDO는 하나의 브리지 그룹만 관리할 수 있으며, 디바이스에서 추가 브리지 그룹을 생성할 수 없습니다. CDO는 가상 FDM 관리 디바이스 인스턴스가 아닌 하드웨어에 직접 설치된 FDM 관리 디바이스의 BVI만 관리할 수 있습니다.

라우팅 모드에서 브리지 그룹을 사용하는 방식 중 하나는 외부 스위치 대신 FDM 관리 디바이스에서 추가 인터페이스를 사용하는 것입니다. 브리지 그룹 멤버 인터페이스에 엔드포인트를 직접 연결할 수 있습니다. 또한 스위치를 연결하여 BVI와 같은 네트워크에 엔드포인트를 더 추가할 수도 있습니다.

### 수동 인터페이스

패시브 인터페이스는 스위치 SPAN(Switched Port Analyzer) 또는 미러 포트를 사용하여 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다.

현재 CDO는 FDM 관리 디바이스에서 패시브 인터페이스 관리를 제한적으로 지원합니다.

- FDM 관리 디바이스에서 패시브 인터페이스를 구성해야 합니다.
- 라우팅된 인터페이스는 패시브 인터페이스로 변경할 수 없으며, 패시브 인터페이스는 CDO를 사용하여 라우팅된 인터페이스로 변경할 수 없습니다.
- CDO는 인터페이스 테이블에서 패시브 인터페이스를 식별하지 않습니다.

### 관련 정보:

- [Firepower 인터페이스용 IPv6 주소 지정](#)
- [Firepower 인터페이스 구성에 대한 지침 및 제한 사항](#)
- [실제 Firepower 인터페이스 구성](#)

## 관리/진단 인터페이스

Management(관리)라는 레이블이 지정된 물리적 포트 또는 FDM 관리 Device Virtual의 경우 Management 0/0 가상 인터페이스에는 실제로 두 개의 개별 인터페이스가 연결되어 있습니다.

- 관리 가상 인터페이스 - 시스템 통신에 사용되는 IP 주소입니다. 이 주소는 시스템이 데이터베이스 업데이트를 검색할 때와 스마트 라이선싱에 사용하는 주소입니다. 이 주소에 대해 관리 세션(Firepower Device Manager 및 CLI)을 열 수 있습니다. **System Settings(시스템 설정)>Management Interface(관리 인터페이스)**에서 정의되는 관리 주소를 설정해야 합니다.
- 진단 실제 인터페이스 - 물리적 관리 포트의 실제 이름은 진단입니다. 이 인터페이스를 사용하여 외부 syslog 서버로 syslog 메시지를 전송할 수 있습니다. 진단 실제 인터페이스에 대한 IP 주소는 필요한 경우에만 구성하면 됩니다. 즉, syslog에 사용하려는 경우에만 인터페이스를 구성합니다. 이 인터페이스는 **Inventory(재고 목록)>Interfaces(인터페이스)** 페이지에 표시되며 해당 페이지

에서 구성할 수 있습니다. 진단 실제 인터페이스는 관리 트래픽만 허용하며 통과 트래픽은 허용하지 않습니다.

(하드웨어 디바이스.) 관리/진단을 구성할 때는 물리적 포트를 네트워크에 유선으로 연결하지 않는 것이 좋습니다. 대신 관리 IP 주소만 구성하고 인터넷에서 업데이트를 가져오는 게이트웨이로 데이터 인터페이스를 사용하도록 해당 주소를 구성합니다. 그런 다음 HTTPS/SSH 트래픽으로 연결되는 내부 인터페이스를 열고(기본값으로 HTTPS는 활성화되어 있음) 내부 IP 주소를 사용하여 Firepower Device Manager를 엽니다. 이 작업은 Firepower Device Manager에서 직접 수행해야 합니다. 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 "관리 액세스 목록 구성"을 참조하십시오.

FDM 관리 Device Virtual의 경우 권장되는 구성은 Management0/0을 내부 인터페이스와 같은 네트워크에 연결하고 내부 인터페이스를 게이트웨이로 사용하는 것입니다. 진단에 대해 별도의 주소를 구성하지는 마십시오.



**Note** 관리 인터페이스를 편집하는 방법에 대한 특별 지침은 **Firepower** 버전 **6.4** 이상용 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)를 참조하십시오. 가이드를 열고 **The Basic > Interfaces > Management/Diagnostic Interface**(기본 인터페이스 관리/진단 인터페이스)로 이동합니다. 관리 인터페이스 구성은 Firepower Device Manager에서 수행해야 합니다.

## 인터페이스 설정

다음 항목을 사용하여 인터페이스 설정을 구성합니다.

### Firepower 인터페이스 설정에서 보안 영역 사용

각 인터페이스는 단일 보안 영역에 할당할 수 있습니다. 그런 후에 영역을 기준으로 하여 보안 정책을 적용합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. 예를 들어, 트래픽이 내부에서 외부로 이동하되 외부에서 내부로 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다.

각 영역은 라우팅 또는 패시브 모드가 됩니다. 이 모드는 인터페이스 모드와 직접 관련이 있습니다. 라우팅 및 패시브 인터페이스는 같은 모드의 보안 영역에만 추가할 수 있습니다.

BVI(Bridge Virtual Interface)는 보안 영역에 추가되지 않습니다. 멤버 인터페이스만 보안 영역에 추가됩니다.

영역에 진단 또는 관리 인터페이스를 포함하지 않습니다. 영역은 데이터 인터페이스에만 적용됩니다.

CDO는 현재 ASA 또는 FTD 디바이스에서 VTI(Virtual Tunnel Interface) 터널의 관리, 모니터링 또는 사용을 지원하지 않습니다. VTI 터널이 구성된 디바이스는 CDO에 온보딩될 수 있지만 VTI 인터페이스는 무시됩니다. 보안 영역 또는 고정 경로가 VTI를 참조하는 경우 CDO는 VTI 참조 없이 보안 영역 및 고정 경로를 읽습니다. VTI 터널에 대한 CDO 지원이 곧 제공될 예정입니다.

보안 영역에 대한 자세한 내용은 [보안 영역 개체](#)를 참조하십시오.

## 보안 영역에 FDM-관리 디바이스 인터페이스 할당

시작하기 전에

보안 영역을 추가할 때 인터페이스에는 다음과 같은 제한 사항이 있습니다.

- 인터페이스에 이름이 있어야 합니다.
- 인터페이스는 관리 전용일 수 없습니다. 이 옵션은 인터페이스의 **Advanced**(고급) 탭에서 활성화 및 비활성화됩니다.
- 브릿지 그룹 인터페이스에는 보안 영역을 할당할 수 없습니다.
- 스위치 포트 모드에 대해 구성된 인터페이스에는 보안 영역을 할당할 수 없습니다.
- CDO는 현재 ASA 또는 FDM 관리 디바이스에서 VTI(Virtual Tunnel Interface) 터널의 관리, 모니터링 또는 사용을 지원하지 않습니다. VTI 터널이 구성된 디바이스는 CDO에 온보딩될 수 있지만 VTI 인터페이스는 무시됩니다. 보안 영역 또는 고정 경로가 VTI를 참조하는 경우 CDO는 VTI 참조 없이 보안 영역 및 고정 경로를 읽습니다. VTI 터널에 대한 CDO 지원이 곧 제공될 예정입니다.

### 보안 영역에 Firepower 인터페이스 할당

보안 영역을 기존 인터페이스에 연결하려면 다음 절차를 수행합니다.

#### Procedure


단계 1 CDO에 로그인합니다.

단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 3 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 4 **FTD** 디바이스를 클릭하고 수정할 FDM 관리 디바이스를 선택합니다.

단계 5 오른쪽에 있는 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.

단계 6 보안 영역을 추가할 인터페이스를 선택하고  **Edit**(편집)를 클릭합니다.

단계 7 **Security Zone**(보안 영역) 드롭다운 메뉴를 사용하여 이 인터페이스와 연결할 보안 영역을 선택합니다.

**Note** 필요한 경우 이 드롭다운 메뉴에서 **Create New**(새로 만들기)를 클릭하여 새 보안 영역을 생성합니다.

단계 8 **Save**(저장)를 클릭합니다.

단계 9 CDO에서 [FDM-관리 디바이스로 구성 변경 사항 구축](#)

관련 정보:

- [보안 영역 개체](#)

- Firepower 보안 영역 개체 생성 또는 편집
- Firepower 인터페이스 구성에 대한 지침 및 제한 사항

## Firepower 인터페이스 설정에서 자동 MDI/MDX 사용

RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 Auto-MDI/MDIX 기능도 포함됩니다. Auto-MDI/MDIX는 자동 협상 단계에서 직선 케이블이 감지된 경우 내부 크로스오버를 수행하므로 크로스오버 케이블이 필요 없습니다. 인터페이스에서 Auto-MDI/MDIX를 활성화하려면 속도 또는 양방향을 자동 협상하도록 설정해야 합니다. 속도와 양방향 둘 다 명시적으로 고정 값으로 설정한 경우 두 설정 모두에 대해 자동 협상을 사용 해제하면 Auto-MDI/MDIX도 사용 해제됩니다. 기가비트 인터넷의 경우 속도와 양방향을 1000 및 최대로 설정하면 인터페이스에서 항상 자동 협상이 실행되므로 Auto-MDI/MDIX 기능도 항상 사용 설정된 상태이고 이를 사용 해제할 수 없습니다.

이러한 설정은 인터페이스를 편집할 때 Advanced(고급) 탭에서 구성됩니다.

## Firepower 인터페이스 설정에서 MAC 주소 사용

MAC(Media Access Control) 주소를 수동으로 구성하여 기본값을 재정의할 수 있습니다.

고가용성 컨피그레이션의 경우, 인터페이스에 대해 액티브 및 스탠바이 MAC 주소를 모두 구성할 수 있습니다. 액티브 유닛이 페일오버하고 스탠바이 유닛이 활성화되면 새 액티브 유닛은 액티브 MAC 주소를 사용하기 시작하므로 네트워크 중단이 최소화됩니다.

액티브 및 스탠바이 MAC 주소는 인터페이스를 구성할 때 Advanced(고급) 탭에서 구성됩니다.

### 기본 MAC 주소

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용합니다.
- 하위 인터페이스 - 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된(burned-in) MAC 주소를 사용합니다. 하위 인터페이스에 고유한 MAC 주소를 할당할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크-로컬 주소는 MAC 주소를 기준으로 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크-로컬 주소를 사용할 수 있습니다.

## Firepower 인터페이스 설정에서 MTU 설정 사용

### MTU 정보

MTU는 FDM 관리 디바이스가 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, VLAN 태깅 또는 기타 오버헤드가 없는 프레임 크기입니다. 예를 들어, MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더 포함 시 1518바이트이고 VLAN 사용 시에는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오.



### 경로 MTU 검색

FDM 관리 디바이스에서는 경로 MTU 검색을 지원하며(RFC 1191에 규정), 이 기능을 사용하면 두 호스트 간의 네트워크 경로에 있는 모든 디바이스에서 MTU를 조율할 수 있으므로, 경로의 최저 MTU에 대한 표준을 설정할 수 있습니다.

### MTU 및 단편화

IPv4의 경우 지정된 MTU보다 큰 발신 IP 패킷은 2개 이상의 프레임으로 단편화됩니다. 분할된 패킷은 목적지(또는 일부 경우 중간 홉에서)에서 다시 합쳐지며, 분할이 일어날 경우 성능이 저하될 수 있습니다. IPv6의 경우에는 일반적으로 패킷의 단편화가 전혀 허용되지 않습니다. 따라서 분할을 방지하려면 IP 패킷이 MTU 크기 내에 맞아야 합니다.

UDP 또는 ICMP의 경우 애플리케이션은 단편화 방지를 위해 MTU를 고려해야 합니다.



**Note** FDM 관리 디바이스는 메모리에 여유 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다.

### MTU와 점보 프레임

큰 MTU를 사용하는 경우 더 큰 패킷을 전송할 수 있습니다. 큰 패킷은 네트워크에서 더욱 효율적으로 사용할 수 있습니다. 다음 지침을 참조하십시오.

- 트래픽 경로에서 일치하는 MTU: 트래픽 경로를 따라 모든 FDM 관리 디바이스 인터페이스 및 기타 디바이스 인터페이스에서 MTU를 동일하게 설정하는 것이 좋습니다. MTU를 일치시키면 패킷 분할 시 디바이스가 중간에 끼어드는 현상을 방지할 수 있습니다.
- 점보 프레임 수용: 점보 프레임은 표준 최대값인 1522바이트(계층 2 헤더 및 VLAN 헤더 포함)보다 큰 이더넷 패킷으로 최대 9216바이트입니다. 점보 프레임을 수용하기 위해 MTU를 최대 9198바이트로 설정할 수 있습니다. 최대값은 가상 FDM 관리의 경우 9000입니다.



**Note** MTU를 늘리면 점보 프레임에 더 많은 메모리가 할당되므로 액세스 규칙 등 다른 기능의 최대 사용량이 제한될 수 있습니다. ASA 5500-X Series 디바이스 또는 가상 FDM 관리에서 기본 1500 이상으로 MTU를 늘리면 시스템을 재부팅해야 합니다. 점보 프레임 지원이 항상 활성화되는 Firepower 2100 Series 디바이스는 재부팅하지 않아도 됩니다.

점보 프레임 지원은 Firepower 3100 디바이스에서 기본적으로 활성화됩니다.

## Firepower 인터페이스용 IPv6 주소 지정

Firepower 물리적 인터페이스에 대해 두 가지 유형의 유니캐스트 IPv6 주소를 구성할 수 있습니다.

- **Global(전역)**—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다. 브리지 그룹의 경우 각 멤버 인터페이스가 아닌 BVI(브리지 가상 인터페이스)에 대해 글로벌 주소를 구성합니다. 다음 항목은 글로벌 주소로 지정할 수 없습니다.

- 내부에서 예약된 IPv6 주소: fd00::<56(from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
- ::/128 등의 지정되지 않은 주소
- 루프백 주소(::1/128)
- 멀티캐스트 주소, ff00::/8
- 링크-로컬 주소(fe80::/10)

- **Link-local(링크-로컬)**—링크-로컬 주소는 직접 연결된 네트워크에서만 사용할 수 있는 사설 주소입니다. 라우터에서 링크-로컬 주소를 사용하여 패킷을 전달하지 않습니다. 이는 특정 물리적 네트워크 세그먼트에서의 통신에만 사용됩니다. 이러한 주소는 주소 확인 및 네이버 검색과 같은 네트워크 검색 기능이나 주소 컨피그레이션에만 사용할 수 있습니다. 각 인터페이스에는 자체 주소가 있어야 합니다. 링크-로컬 주소는 세그먼트에서만 사용 가능하며 인터페이스 MAC 주소와 연결되기 때문입니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 설정하면 링크-로컬 주소가 인터페이스에서 자동으로 구성되므로 링크-로컬 주소를 특별히 구성하지 않아도 됩니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

## Firepower 인터페이스 구성

물리적 또는 가상 인터페이스 연결에 케이블을 연결하려면 인터페이스를 구성해야 합니다. 최소한 인터페이스 이름을 지정하고 트래픽을 전달하도록 인터페이스를 활성화해야 합니다. 인터페이스가 브리지 그룹의 멤버인 경우에는 인터페이스의 이름을 지정하는 작업만 수행하면 됩니다. 인터페이스가 BVI(브리지 가상 인터페이스)인 경우 BVI에 IP 주소를 할당해야 합니다. 지정된 포트의 단일 실제 인터페이스가 아닌 VLAN 하위 인터페이스를 생성하려는 경우에는 일반적으로 실제 인터페이스가 아닌 하위 인터페이스에 IP 주소를 구성합니다. VLAN 하위 인터페이스를 사용하면 실제 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다.

인터페이스 목록에는 사용 가능한 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다. 인터페이스 행을 선택하고 Actions(작업) 창에서 **Edit(편집)**를 클릭하여 인터페이스의 상태를 on 또는 off로 변경하거나 인터페이스를 편집할 수 있습니다. 목록에는 컨피그레이션을 기준으로 인터페이스 특성이 표시됩니다. 인터페이스 행을 확장하여 하위 인터페이스 또는 브리지 그룹 멤버를 확인합니다.

관련 정보:

- [인터페이스](#)
- [실제 Firepower 인터페이스 구성](#)
- [고급 Firepower 인터페이스 옵션 구성, on page 269](#)
- [Firepower VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성](#)
- [스위치 포트 모드에 대한 FDM-관리 디바이스 VLAN 구성](#)

## 실제 Firepower 인터페이스 구성

실제 인터페이스를 사용하려면 최소한 인터페이스를 활성화해야 합니다. 일반적으로 이름을 지정하고 IP 주소 지정을 구성할 수도 있지만 VLAN 하위 인터페이스를 생성하려는 경우, 패시브 모드 인터페이스를 구성하는 경우 또는 인터페이스를 브리지 그룹에 추가하려는 경우에는 IP 주소를 구성하지 않습니다.



**Note** 브리지 그룹 멤버 인터페이스 또는 패시브 인터페이스에서는 IP 주소를 구성할 수 없습니다. 그러나 IPv6 주소 지정과 관련이 없는 고급 설정을 수정할 수는 있습니다.

인터페이스를 비활성화하여 연결된 네트워크에서 전송을 일시적으로 차단할 수 있습니다. 인터페이스 컨피그레이션을 제거할 필요는 없습니다. 현재 Cisco Defense Orchestrator(CDO)는 라우팅 인터페이스 및 브리지 그룹만 구성할 수 있습니다. CDO는 패시브 인터페이스를 나열하지만 CDO의 액티브 인터페이스로 재설정할 수는 없습니다.



**Note** 참고: CDO는 IPv4에 대해 PPPoE(Point-to-Point Protocol over Ethernet) 구성을 지원하지 않습니다. FDM 관리에서 이 옵션을 구성하면 CDO UI에 문제가 발생할 수 있습니다. 디바이스에 대해 PPPoE를 구성해야 하는 경우 FDM 관리 디바이스에서 적절하게 변경해야 합니다.

절차

### Procedure

- 단계 1 **Devices & Services**(디바이스 및 서비스) 페이지에서 인터페이스를 구성하려는 디바이스를 클릭하고 오른쪽의 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.
- 단계 2 **Interfaces**(인터페이스) 페이지에서 구성할 물리적 인터페이스를 선택합니다.
- 단계 3 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.
- 단계 4 물리적 인터페이스에 논리적 이름을 지정하고 필요한 경우 설명을 입력합니다. 하위 인터페이스를 구성하는 경우가 아니면 인터페이스에는 이름이 있어야 합니다.

**Note** 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

- 단계 5 다음 옵션 중 하나를 선택합니다.

- 하위 인터페이스를 추가하려면 다음을 수행합니다.

이 실제 인터페이스에 대해 하위 인터페이스를 구성하려는 경우에는 이러한 작업만 수행하면 될 가능성이 높습니다. **Save**(저장)를 클릭하고 **Firepower VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성**을 계속합니다. 아니면 계속 진행합니다.

**Note** 하위 인터페이스를 구성할 때도 인터페이스 이름을 지정하고 IP 주소를 제공할 수 있습니다. 이러한 방식은 일반적인 설정은 아니지만, 필요한 경우에는 해당 설정을 구성할 수 있습니다.

- 하위 인터페이스를 추가하지 않으려면 [물리적 인터페이스에 대한 IPv4 주소 지정 구성](#) 및 [물리적 인터페이스에 대한 IPv6 주소 지정 구성](#) 중 하나 또는 둘 다를 계속 진행합니다.

## 물리적 인터페이스에 대한 IPv4 주소 지정 구성



### Warning

DHCP 주소 풀을 구성하고 저장하면 DHCP 주소 풀이 인터페이스의 구성된 IP 주소에 바인딩됩니다. DHCP 주소 풀을 구성한 후 인터페이스의 서브넷 마스크를 편집하면 FDM 관리 디바이스에 대한 구축이 실패합니다. 또한 FDM 관리 콘솔에서 DHCP 주소 풀을 편집하고 FDM 관리 디바이스에서 Cisco Defense Orchestrator로 구성을 읽는 경우에도 읽기가 실패합니다.

### Procedure

**단계 1** "Editing Physical Interface(물리적 인터페이스 편집)" 대화 상자에서 **IPv4 Address(IPv4 주소)** 탭을 클릭합니다.

**단계 2** Type(유형) 필드에서 다음 옵션 중 하나를 선택합니다.

- **Static(고정)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 입력하는 주소가 네트워크 ID 또는 네트워크의 브로드캐스트 주소가 아니며 해당 주소가 네트워크에서 이미 사용되지 않았는지 확인합니다.
- **Standby IP Address and Subnet Mask(스탠바이 IP 주소 및 서브넷 마스크)** - 고가용성을 구성하고 이 인터페이스에서 HA를 모니터링하는 경우 동일한 서브넷에서도 스탠바이 IP 주소를 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- (선택 사항) **DHCP Address Pool(DHCP 주소 풀)** - 단일 DHCP 서버 IP 주소 또는 IP 어드레스 레인지를 입력합니다. 이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소, 브로드캐스트 주소 또는 서브넷 네트워크 주소는 포함할 수 없습니다. 풀의 시작 주소와 끝 주소를 하이픈으로 구분하여 지정합니다. 이 DHCP 서버를 일시적으로 비활성화하려면 [DHCP 서버 구성](#) 페이지의 **DHCP Servers(DHCP 서버)** 섹션에서 서버를 편집합니다.
- **Dynamic(동적)(DHCP)** - 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 필요에 따라 다음 옵션을 변경합니다.

- **Obtain Default Route**(기본 경로 얻기) - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로 이 옵션을 선택합니다.
- **DHCP Route Metric**(DHCP 경로 메트릭) - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 AD(Administrative Distance)(1~255)를 입력합니다.

**Note** 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다.

단계 3 완료한 경우 **Save**(저장)를 클릭하거나 다음 절차 중 하나를 계속합니다.

- 이 인터페이스 및 IPv4 주소에 IPv6 주소를 할당하려면 **물리적 인터페이스에 대한 IPv6 주소 지정 구성**합니다.
- **고급 Firepower 인터페이스 옵션 구성**, on page 269에 전달하는 고성능 고속 어플라이언스입니다. 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 인터페이스를 저장한 경우 고급 인터페이스 옵션을 계속 진행하지 않으려면 **물리적 인터페이스 활성화**를 계속 진행합니다.

## 물리적 인터페이스에 대한 IPv6 주소 지정 구성

### Procedure

단계 1 "Editing Physical Interface(물리적 인터페이스 편집)" 대화 상자에서 IPv6 Address(IPv6 주소) 탭을 클릭합니다.

단계 2 **State**(상태)-IPv6 처리를 활성화하고 전역 주소를 구성하지 않을 때 링크 로컬 주소를 자동으로 구성하려면 **State**(상태) 슬라이더를 클릭하여 사용하도록 설정합니다. 링크-로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

**Note** IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 구성용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

단계 3 **Address Auto Configuration**(주소 자동 구성)-주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성된 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 FDM 관리 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

**단계 4 Suppress RA(RA 표시 안 함)**-라우터 알림을 표시하지 않으려면 이 상자를 선택합니다. Firepower Threat Defense 디바이스는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

Firepower Threat Defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

**단계 5 Link-Local Address(링크-로컬 주소)**-주소를 링크 로컬로만 사용하려면 Link-Local Address(링크-로컬 주소) 필드에 주소를 입력합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

**Note** 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:fee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

**단계 6 Standby Link-Local Address(스탠바이 링크-로컬 주소)**-인터페이스가 고가용성 디바이스 쌍을 연결하는 경우 이 주소를 구성합니다. 이 인터페이스가 연결된 다른 FDM 관리 디바이스에 있는 인터페이스의 링크-로컬 주소를 입력합니다.

**단계 7 Static Address/Prefix(고정 주소/접두사)**-스테이트리스 자동 설정을 사용하지 않는 경우 전체 고정 전역 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 [Firepower 인터페이스용 IPv6 주소 지정](#)을 참조하십시오.

**단계 8 Standby IP Address(스탠바이 IP 주소)**-고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

**단계 9** 완료한 경우 **Save(저장)**를 클릭하거나 다음 절차 중 하나를 계속합니다.

- **고급 Firepower 인터페이스 옵션 구성**, on page 269에 전달하는 고성능 고속 어플라이언스입니다. 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 인터페이스를 저장한 경우 고급 인터페이스 옵션을 계속 진행하지 않으려면 **물리적 인터페이스 활성화**를 계속 진행합니다.

## 물리적 인터페이스 활성화

## Procedure

- 
- 단계 1 활성화할 인터페이스를 선택합니다.
  - 단계 2 인터페이스의 논리적 이름과 연결된 창의 오른쪽 상단에 있는 **State(상태)** 슬라이더를 파란색으로 합니다.
  - 단계 3 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 번 변경 사항을 한 번에 구축합니다.
- 

## Firepower VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성

VLAN 하위 인터페이스를 사용하면 실제 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 정해진 실제 인터페이스에서 트래픽을 따로 유지할 수 있으므로, 실제 인터페이스 또는 디바이스를 더 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다.

스위치의 트렁크 포트에 물리적 인터페이스를 연결하는 경우 하위 인터페이스를 생성합니다. 스위치 트렁크 포트에 표시될 수 있는 각 VLAN에 대해 하위 인터페이스를 생성합니다. 스위치의 액세스 포트에 물리적 인터페이스를 연결하는 경우 하위 인터페이스를 생성할 필요가 없습니다.




---

**Note** 브리지 그룹 멤버 인터페이스에서는 IP 주소를 구성할 수 없습니다. 그러나 필요에 따라 고급 설정을 수정할 수는 있습니다.

---

## 시작하기 전에

물리적 인터페이스에서 태그가 지정되지 않은 패킷을 방지합니다. 하위 인터페이스를 사용하는 경우 물리적 인터페이스에서도 트래픽을 전달하도록 하지 않는 것이 일반적입니다. 물리적 인터페이스는 태그가 지정되지 않은 패킷을 전달하기 때문입니다. 하위 인터페이스에서 트래픽을 전달하려면 실제 인터페이스를 활성화해야 하므로, 인터페이스의 이름을 지정하지 않는 방법을 통해 실제 인터페이스가 트래픽을 전달하지 않도록 해야 합니다. 실제 인터페이스에서 태그가 지정되지 않은 패킷을 전달할 수 있도록 하려면 일반적인 방식으로 인터페이스 이름을 지정하면 됩니다.

## 절차

## Procedure

- 
- 단계 1 탐색 창에서 **Devices & Services(디바이스 및 서비스)**를 클릭합니다.
  - 단계 2 **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 FTD 탭을 클릭하고 인터페이스를 구성할 디바이스를 클릭합니다.

단계 4 오른쪽의 **Management(관리)** 창에서 **Interfaces(인터페이스)**를 클릭합니다.

단계 5 Interfaces(인터페이스) 페이지에서 구성할 물리적 인터페이스를 선택하고 오른쪽의 **Actions(작업)** 창에서 **+ New Subinterface(새로운 하위 인터페이스)**를 클릭합니다.

**Parent Interface(상위 인터페이스)** 필드에 이 하위 인터페이스를 생성하는 물리적 인터페이스의 이름이 표시됩니다. 하위 인터페이스를 생성한 후에는 상위 인터페이스를 변경할 수 없습니다.

단계 6 하위 인터페이스에 논리적 이름을 지정하고 필요한 경우 설명을 입력합니다. 논리적 이름을 입력하지 않으면 나머지 인터페이스 구성이 무시됩니다.

**Note** 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

단계 7 VLAN ID 및 하위 인터페이스 ID를 구성합니다.

- **VLAN ID** - 이 하위 인터페이스에서 패킷에 태그를 지정하는 데 사용할 1~4094 사이의 VLAN ID를 입력합니다.
- **하위 인터페이스 ID** - 하위 인터페이스 ID를 1~4294967295 사이의 정수로 입력합니다. 허용되는 하위 인터페이스의 개수는 **디바이스 모델별 VLAN 멤버의 최대 수**. 하위 인터페이스를 생성한 후에는 하위 인터페이스 ID를 변경할 수 없습니다.

하위 인터페이스에 대한 IPv4 주소 지정 구성 및 하위 인터페이스에 대한 IPv6 주소 지정 구성을 계속 진행합니다.

## 하위 인터페이스에 대한 IPv4 주소 지정 구성

### Procedure

단계 1 "Adding Subinterface(하위 인터페이스 추가)" 대화 상자에서 **IPv4 Address(IPv4 주소)** 탭을 클릭합니다.

단계 2 Type(유형) 필드에서 다음 옵션 중 하나를 선택합니다.

- **Static(고정)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다.

인터페이스에 연결된 네트워크에 대해 인터페이스의 **IP** 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 입력하는 주소가 네트워크 ID 또는 네트워크의 브로드캐스트 주소가 아니며 해당 주소가 네트워크에서 이미 사용되지 않았는지 확인합니다.

- 이 인터페이스가 디바이스의 고가용성 쌍에서 사용되고 있는 경우에만 스탠바이 **IP** 주소 및 서브넷 마스크를 입력합니다.



- **Dynamic(동적)(DHCP)** - 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Obtain Default Route(기본 경로 얻기)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로 이 옵션을 선택합니다.
  - **DHCP Route Metric(DHCP 경로 메트릭)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 AD(Administrative Distance)(1~255)를 입력합니다.

DHCP 서버 구성을 참조하십시오.

**Note** 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다.

단계 3 완료한 경우 **Create(생성)**를 클릭하거나 다음 절차 중 하나를 계속합니다.

- 이 인터페이스 및 IPv4 주소에 IPv6 주소를 할당하려면 "**물리적 인터페이스에 대한 IPv6 주소 지정 구성**"을 진행합니다.
- **고급 Firepower 인터페이스 옵션 구성**, on page 269에 전달하는 고성능 고속 어플라이언스입니다. 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 하위 인터페이스를 생성한 경우 **물리적 인터페이스 활성화**로 이동합니다.

## 하위 인터페이스에 대한 IPv6 주소 지정 구성

### Procedure

단계 1 IPv6 Address(IPv6 주소) 탭을 클릭합니다.

단계 2 **Enable IPv6 Processing(IPv6 처리 활성화)** - 전역 주소를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **State(상태)** 슬라이더를 파란색으로 이동합니다. 링크-로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

**Note** IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 구성용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

단계 3 **Address Auto Configuration(주소 자동 구성)**-주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 설정에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 전역 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 전역 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

**단계 4 Suppress RA(RA 표시 안 함)**-라우터 알림을 표시하지 않으려면 이 상자를 선택합니다. Firepower Threat Defense 디바이스는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

Firepower Threat Defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

**단계 5 Link-Local Address(링크-로컬 주소)**-주소를 링크 로컬로만 사용하려면 Link-Local Address(링크-로컬 주소) 필드에 주소를 입력합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다.

**Note** 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feec:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

**단계 6 Standby Link-Local Address(스탠바이 링크-로컬 주소)**- 인터페이스가 고가용성 디바이스 쌍을 연결하는 경우 이 주소를 구성합니다.

**단계 7 Static Address/Prefix(고정 주소/접두사)**- 스테이트리스 자동 설정을 사용하지 않는 경우 전체 고정 전역 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정(136페이지)을 참조하십시오.

**단계 8 Standby IP Address(스탠바이 IP 주소)**- 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

**단계 9** 완료한 경우 **Create(생성)**를 클릭하거나 다음 절차 중 하나를 계속합니다.

- **Advanced(고급)** 탭을 클릭하여 **고급 Firepower 인터페이스 옵션 구성, on page 269**합니다. 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.
- 하위 인터페이스를 생성한 경우 **물리적 인터페이스 활성화**로 이동합니다.

## 물리적 인터페이스 활성화

### Procedure

**단계 1** 하위 인터페이스를 활성화하려면 하위 인터페이스의 논리적 이름과 연결된 State(상태) 슬라이더를 파란색으로 만듭니다.

단계 2 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 고급 Firepower 인터페이스 옵션 구성

고급 인터페이스 옵션에는 대부분의 네트워크에 적합한 기본 설정이 있습니다. 네트워킹 문제를 해결하는 경우에만 이러한 설정을 구성하십시오.

다음 절차에서는 인터페이스가 이미 정의되어 있다고 가정합니다. 인터페이스를 처음 수정하거나 생성할 때 이러한 설정을 수정할 수도 있습니다.

이 절차 및 모든 단계는 선택 사항입니다.

제한 사항:

- Firepower 2100 디바이스에서는 관리 인터페이스의 MTU, 듀플렉스 또는 속도를 설정할 수 없습니다.
- 이름 없는 인터페이스의 MTU는 반드시 1500바이트로 설정해야 합니다.

### Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 **FTD** 탭을 클릭하고 인터페이스를 구성할 디바이스를 클릭합니다.

단계 4 오른쪽의 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.

단계 5 **Interfaces**(인터페이스) 페이지에서 구성할 물리적 인터페이스를 선택하고 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

단계 6 **Advanced**(고급) 탭을 클릭합니다.

단계 7 **Enable for HA Monitoring**(HA 모니터링 활성화)이 자동으로 활성화됩니다. 이 옵션을 활성화하면 디바이스는 HA 쌍이 고가용성 구성에서 피어 디바이스로 페일오버할지 여부를 결정할 때 인터페이스의 상태를 요소로 포함합니다. 이 옵션은 고가용성을 구성하지 않는 경우 무시되며 인터페이스의 이름을 구성하지 않는 경우에도 무시됩니다.

단계 8 데이터 인터페이스 관리만 수행하려면 **Management Only**(관리만)를 선택합니다.

관리 전용 인터페이스에서는 통과 트래픽을 허용하지 않으므로 데이터 인터페이스를 관리 전용 인터페이스로 설정할 때 사용할 수 있는 값은 거의 없습니다. 관리/진단 인터페이스(항상 관리 전용)의 경우에는 이 설정을 변경할 수 없습니다.

단계 9 IPv6 DHCP 구성 설정을 수정합니다.

- **IPv6** 주소 구성에 **DHCP** 활성화 - IPv6 라우터 알림 패킷에서 관리 주소 구성 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 구성 클라이언트에게 DHCPv6를 사용하여 파생된 스테이트리스 자동 구성 주소 이외의 주소도 얻도록 안내합니다.

- **IPv6** 비주소 구성에 **DHCP** 활성화 - IPv6 라우터 알림 패킷에서 기타 주소 구성 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 구성 클라이언트에게 DHCPv6를 사용하여 DHCPv6로부터 추가 정보(예: DNS 서버 주소)를 얻도록 안내합니다.

**단계 10 DAD** 시도 구성 - 인터페이스가 DAD(Duplicate Address Detection)를 수행하는 빈도를 0~600 사이의 값으로 설정합니다. 기본값은 1입니다. 스테이트리스 자동 구성 프로세스에서 DAD는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다. 인터페이스에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.

**단계 11 MTU**(Maximum Transmission Unit)를 원하는 값으로 변경합니다.

기본 MTU는 1500바이트입니다. 64~9198(Firepower Threat Defense Virtual의 경우 9000) 사이의 값을 지정할 수 있습니다. 네트워크에서 대개 점보 프레임이 표시되면 높은 값을 설정합니다. 자세한 내용은 [Firepower 인터페이스 설정에서 MTU 설정 사용](#)을 참조하십시오.

**Note** ASA 5500-X Series 디바이스, ISA 3000 Series 디바이스 또는 Firepower Threat Defense Virtual에서 MTU를 1500보다 큰 값으로 늘리는 경우에는 디바이스를 재부팅해야 합니다. 이렇게 하려면 CLI에 로그인하여 reboot 명령을 사용합니다. 점보 프레임 지원이 항상 활성화되는 Firepower 2100 또는 Secure Firewall 3100 시리즈 디바이스는 재부팅하지 않아도 됩니다.

**단계 12** (실제 인터페이스만 해당됨) 속도 및 이중 설정을 수정합니다.

기본적으로 인터페이스는 연결 반대쪽의 인터페이스와 최적의 이중 및 속도를 협상하지만, 필요한 경우 특정 이중이나 속도를 강제 적용할 수 있습니다. 나열된 옵션은 인터페이스에서 지원하는 유일한 옵션입니다. 네트워크 모듈의 인터페이스에 이러한 옵션을 설정하기 전에 [Firepower 인터페이스 구성에 대한 지침 및 제한 사항](#)을 읽어보십시오.

- **Duplex**(듀플렉스) — Auto(자동), Half(하프), Full(풀) 또는 Default(기본값)를 선택합니다. 인터페이스가 지원하는 경우 자동으로 기본값입니다. 예를 들어 Firepower 2100 또는 Secure Firewall 3100 시리즈 디바이스의 SFP 인터페이스에 대해서는 Auto(자동)를 선택할 수 없습니다. Firepower Device Manager에서 설정을 구성할 필요가 없음을 나타내려면 Default(기본값)를 선택합니다.

모든 기존 컨피그레이션이 변경되지 않은 상태로 유지됩니다.

- **Speed**(속도) — Auto(자동)를 선택하여 인터페이스가 속도를 협상하도록 하거나(이 옵션이 기본값임), 10, 100, 1000, 10000Mbps 중에서 특정 속도를 선택합니다. 다음과 같은 특수 옵션을 선택할 수도 있습니다.

모든 기존 컨피그레이션이 변경되지 않은 상태로 유지됩니다.

인터페이스 유형에 따라 선택할 수 있는 옵션이 제한됩니다. 예를 들어 Firepower 2100 Series 디바이스의 SFP+ 인터페이스에서는 1000(1Gbps) 및 10000(10Gbps)만 지원하며, SFP 인터페이스에서는 1000(1Gbps)만 지원합니다. 반면 GigabitEthernet 포트에서는 10000(10Gbps)을 지원하지 않습니다. 다른 디바이스의 SPF 인터페이스에는 No Negotiate(협상 안 함) 옵션이 필요할 수 있습니다. 인터페이스에서 지원하는 옵션에 대한 정보는 하드웨어 설명서를 참조하십시오.

**단계 13** (선택 사항, 하위 인터페이스 및 고가용성 유닛의 경우 권장함.) MAC 주소를 구성합니다.

**MAC Address(MAC 주소)** - H.H.H. 형식의 MAC(Media Access Control) 주소입니다. 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다(즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없음).

**Standby MAC Address(스탠바이 MAC 주소)** - 고가용성에 사용할 주소입니다. 액티브 유닛이 페일 오버되고 스탠바이 유닛이 액티브 상태가 되면, 네트워크 중단을 최소화하기 위해 새 액티브 유닛에서 액티브 MAC 주소를 사용하기 시작하고 기존 액티브 유닛은 스탠바이 주소를 사용합니다.

단계 14 **Create(생성)**를 클릭합니다.

## 브리지 그룹 구성

브리지 그룹은 하나 이상의 인터페이스를 그룹화하는 가상 인터페이스입니다. 인터페이스를 그룹화하는 주요 이유는 스위치 인터페이스 그룹을 생성하기 위해서입니다. 따라서 브리지 그룹에 포함된 인터페이스에 워크스테이션 또는 기타 엔드포인트 디바이스를 직접 연결할 수 있습니다. 이러한 워크스테이션이나 디바이스는 별도의 물리적 스위치를 통해 연결할 필요는 없지만, 브리지 그룹 멤버에 스위치를 연결할 수도 있습니다.

그룹 멤버에는 IP 주소가 없습니다. 대신 모든 멤버 인터페이스는 BVI(브리지 가상 인터페이스)의 IP 주소를 공유합니다. BVI에서 IPv6를 활성화하는 경우 멤버 인터페이스에는 고유한 링크-로컬 주소가 자동으로 할당됩니다.

일반적으로는 BVI(브리지 그룹 인터페이스)에서 DHCP 서버를 구성합니다. 이 서버는 멤버 인터페이스를 통해 연결된 모든 엔드포인트에 대해 IP 주소를 제공합니다. 그러나 원하는 경우에는 멤버 인터페이스에 연결된 엔드포인트에서 고정 주소를 구성할 수 있습니다. 브리지 그룹 내의 모든 엔드포인트에는 브리지 그룹 IP 주소와 같은 서브넷의 IP 주소가 있어야 합니다.



**Note** ISA 3000의 경우 디바이스는 브리지 그룹 BVI(이름: 내부)이 미리 구성된 상태로 제공됩니다. 이 그룹에는 외부 인터페이스를 제외한 모든 데이터 인터페이스가 포함됩니다. 따라서 디바이스에는 인터넷 또는 기타 업스트림 네트워크에 연결하는 데 사용되는 포트 하나가 미리 구성되어 있습니다. 그리고 기타 모든 포트는 엔드포인트에 대한 직접 연결용으로 활성화되어 있으며 사용 가능합니다. 새 서브넷에 대해 내부 인터페이스를 사용하려는 경우에는 먼저 BVI에서 필요한 인터페이스를 제거해야 합니다.

FDM 관리 디바이스는 브리지 그룹을 하나만 지원합니다. 따라서 Cisco Defense Orchestrator는 하나의 브리지 그룹만 관리할 수 있으며, 디바이스에서 추가 브리지 그룹을 생성할 수 없습니다.

CDO에서 브리지 그룹을 만든 후에는 구성이 FDM 관리 디바이스에 구축될 때까지 브리지 그룹 ID를 알 수 없습니다. FDM 관리 디바이스는 브리지 그룹 ID(예: BVI1)를 할당합니다. 인터페이스가 삭제되고 새 브리지 그룹이 생성되면 새 브리지 그룹은 증가된 숫자(예: BVI2)를 수신합니다.

시작하기 전에

브리지 그룹의 멤버로 추가할 인터페이스를 구성합니다. 구체적으로 각 멤버 인터페이스는 다음 요건을 충족해야 합니다.

- 인터페이스에 이름이 있어야 합니다.
- 인터페이스는 관리 전용으로 구성할 수 없습니다.
- 인터페이스는 패시브 모드에 대해 구성할 수 없습니다.
- 인터페이스는 EtherChannel 인터페이스 또는 EtherChannel 하위 인터페이스일 수 없습니다.
- 인터페이스에 대해 IPv4 또는 IPv6 주소(고정 주소 또는 DHCP를 통해 제공된 주소)가 정의되어 있으면 안 됩니다. 현재 사용 중인 인터페이스에서 주소를 제거해야 하는 경우에는 주소가 있는 인터페이스를 사용하는 인터페이스의 다른 컨피그레이션(예: 정적 경로, DHCP 서버 또는 NAT 규칙)도 제거해야 할 수 있습니다. IP 주소가 있는 인터페이스를 브리지 그룹에 추가하려고 하면 CDO에서 경고를 표시합니다. 브리지 그룹에 인터페이스를 계속 추가하면 CDO가 인터페이스 구성에서 IP 주소를 제거합니다.
- BVI는 멤버 인터페이스로 VLAN 인터페이스 또는 기타 라우팅된 인터페이스를 가질 수 있지만, 단일 BVI에서 둘 다 멤버 인터페이스로 가질 수는 없습니다.
- 인터페이스는 PPPoE(Point-to-Point Protocol over Ethernet)일 수 없습니다.
- 인터페이스는 보안 영역(영역에 있는 경우)과 연결할 수 없습니다. 브리지 그룹에 인터페이스를 추가하려면 먼저 인터페이스에 대한 NAT 규칙을 삭제해야 합니다.
- 멤버 인터페이스는 개별적으로 활성화 및 비활성화합니다. 그러므로 사용하지 않는 인터페이스는 브리지 그룹에서 제거할 필요 없이 비활성화할 수 있습니다. 브리지 그룹 자체는 항상 활성화됩니다.
- 브리지 그룹은 클러스터링을 지원하지 않습니다.



**Note** 브리지 그룹은 라우팅 모드의 Firepower 2100 디바이스 또는 브리지된 ixgbevf 인터페이스가 있는 VMware에서 지원되지 않습니다.

## 브릿지 그룹 인터페이스의 이름 구성 및 브릿지 그룹 멤버 선택

이 절차에서는 BVI(브릿지 그룹 인터페이스)에 이름을 지정하고 브리지 그룹에 추가할 인터페이스를 선택합니다.

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 브리지 그룹을 생성할 디바이스를 선택합니다.
- 단계 4 다음 중 하나를 수행합니다.
  - BVI 브리지 그룹을 선택하고 Actions(작업) 창에서 **Edit**(편집)를 클릭합니다.

- 더하기  버튼을 클릭하고 Bridge Group Interface(브릿지 그룹 인터페이스)를 선택합니다.

**Note** 단일 브리지 그룹을 생성하고 구성할 수 있습니다. 브리지 그룹을 이미 정의한 경우에는 새 그룹을 생성하는 대신 해당 그룹을 수정해야 합니다. 새 브리지 그룹을 생성해야 하는 경우 먼저 기존 브리지 그룹을 삭제해야 합니다.

단계 5 다음을 구성합니다.

- **Logical Name(논리적 이름)** - 브리지 그룹에 이름을 지정해야 합니다. 최대 48자까지 입력할 수 있습니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이름을 입력하지 않으면 나머지 인터페이스 컨피그레이션이 무시됩니다.

**Note** 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

- (선택 사항) **Description(설명)** - 설명은 줄바꿈 없이 1줄, 최대 200자로 작성합니다.

단계 6 **Bridge Group Member(브리지 그룹 멤버)** 탭을 클릭합니다. 브리지 그룹은 단일 브리지 그룹에 인터페이스 또는 하위 인터페이스를 64개까지 추가할 수 있습니다.

- 인터페이스를 선택하여 브리지 그룹에 추가합니다.
- 브리지 그룹에서 제거할 인터페이스의 선택을 취소합니다.

단계 7 **Save(저장)**를 클릭합니다.

이제 BVI에 이름 및 멤버 인터페이스가 있습니다. 다음 작업을 계속 진행하여 브릿지 그룹 인터페이스를 구성합니다. 멤버 인터페이스 자체에 대해서는 다음 작업을 수행하지 않습니다.

- BVI에 IPv4 주소를 할당하는 경우 [BVI용 IPv4 주소 구성](#).
- BVI에 IPv6 주소를 할당하는 경우 [BVI용 IPv6 주소 구성](#).
- 브릿지 그룹 인터페이스에 대한 [고급 인터페이스 옵션 구성](#)합니다.

## BVI용 IPv4 주소 구성

### Procedure

단계 1 브리지 그룹을 생성할 디바이스를 선택합니다.

단계 2 인터페이스 목록에서 BVI를 선택하고 Actions(작업) 창에서 **Edit(편집)**를 클릭합니다.

단계 3 IPv4 Address(IPv4 주소) 탭을 클릭하여 IPv4 주소를 구성합니다.

단계 4 Type(유형) 필드에서 다음 옵션 중 하나를 선택합니다.

- **Static(고정)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 브리지 그룹의 IP 주소와 서브넷 마스크를 입력합니다. 연결되는 모든 엔드포인트는 이 네트워크에 포함됩니다. 사전 구성된 브리지 그룹이 있는 모델의 경우 BVI "inside" 네트워크의 기본값은 192.168.1.1/24(255.255.255.0)입니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

**Note** 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 구성을 참조하십시오.

- **Dynamic(동적)(DHCP)** - 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 이 옵션은 브리지 그룹에 대해 일반적으로 구성하는 항목은 아니지만 필요한 경우 구성할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(경로 메트릭)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 AD(Administrative Distance)(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(기본 경로 얻기)** - DHCP 서버에서 기본 경로를 가져오려면 이 옵션을 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).

단계 5 다음 절차 중 하나를 계속합니다.

- BVI에 IPv4 주소를 할당하는 경우 [BVI용 IPv6 주소 구성](#)합니다.
- 고급 인터페이스 옵션을 구성합니다.
- **Save(저장)**를 클릭하고 Firepower 디바이스에 변경 사항을 구축합니다. 자세한 정보는 [CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축](#)을 참조하십시오.

## BVI용 IPv6 주소 구성

### Procedure

단계 1 IPv6 Address(IPv6 주소) 탭을 클릭하여 BVI용 IPv6 주소 지정을 구성합니다.

단계 2 IPv6 주소 지정의 다음 측면을 구성합니다.



**단계 3 Enable IPv6 Processing(IPv6 처리 활성화)** - 전역 주소를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **State(상태)** 슬라이더를 파란색으로 끕니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

**Note** IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

**단계 4 Suppress RA(RA 표시 안 함)** - 라우터 알람을 표시하지 않을지를 선택합니다. Firepower Threat Defense 디바이스는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알람에 참여할 수 있습니다. 기본적으로 라우터 알람 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

FTD 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

**단계 5 Static Address/Prefix(고정 주소/접두사)** - 스테이트리스 자동 구성을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정을 참조하십시오.

**단계 6 Standby IP Address(스탠바이 IP 주소)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

**단계 7** 다음 절차 중 하나를 계속합니다.

- 고급 인터페이스 옵션을 구성합니다.
- **Save(저장)**를 클릭하고 Firepower 디바이스에 변경 사항을 구축합니다. 자세한 정보는 [CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축](#)을 참조하십시오.

## 고급 인터페이스 옵션 구성

브리지 그룹 멤버 인터페이스에서 대부분의 고급 옵션을 구성하지만, 일부 옵션은 브릿지 그룹 인터페이스 자체에 사용할 수 있습니다.

### Procedure

**단계 1** 고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

**단계 2 OK(확인)**를 클릭합니다.

단계 3 **Save**(저장)를 클릭하고 Firepower 디바이스에 변경 사항을 구축합니다. 자세한 정보는 [CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축](#)을 참조하십시오.

#### What to do next

- 사용하려는 모든 멤버 인터페이스가 활성화되어 있는지 확인합니다.
- 브리지 그룹에 대해 DHCP 서버를 구성합니다. [DHCP 서버 구성](#)을 참조하십시오.
- 적절한 보안 영역에 멤버 인터페이스를 추가합니다.
- ID, NAT, 액세스 등의 정책이 브리지 그룹 및 멤버 인터페이스에 필요한 서비스를 제공하는지 확인합니다.

#### FDM-관리 구성의 브리지 그룹 호환성

인터페이스를 지정할 수 있는 다양한 구성에서는 경우에 따라 브리지 BVI(가상 인터페이스)를 지정할 수 있으며, 경우에 따라 브리지 그룹의 멤버를 지정할 수 있습니다. 이 테이블에서는 BVI를 사용할 수 있는 경우와 멤버 인터페이스를 사용할 수 있는 경우에 대해 설명합니다.

Firepower Threat Defense 구성 유형	BVI를 사용할 수 있음	BVI 멤버를 사용할 수 있음
DHCP 서버	예	아니요
DNS 서버	예	예
관리 액세스	예	아니요
NAT(Network Address Translation)	아니요	예
보안 영역	아니요	예
사이트 투 사이트 VPN 액세스 포인트	아니요	예
Syslog 서버	예	아니요

#### 브리지 그룹 삭제

브리지 그룹을 삭제하면 해당 멤버는 표준 라우팅 인터페이스가 되며 모든 NAT 규칙 또는 보안 영역 멤버십은 유지됩니다. 인터페이스를 수정하여 IP 주소를 지정할 수 있습니다. 새 브리지 그룹을 생성해야 하는 경우 먼저 기존 브리지 그룹을 삭제해야 합니다.

#### Procedure

단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 FTD 탭을 클릭하고 브리지 그룹을 삭제할 디바이스를 선택합니다.

단계 4 BVI 브리지 그룹을 선택하고 Actions(작업) 창에서 **Remove(제거)**를 클릭합니다.

단계 5 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## FDM-관리 디바이스에 대한 EtherChannel 인터페이스 추가

### EtherChannel 인터페이스 제한 사항

디바이스 모델에 따라 EtherChannel은 동일한 미디어 유형 및 용량의 여러 멤버 인터페이스를 포함할 수 있으며 동일한 속도 및 듀플렉스로 설정해야 합니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 없습니다. LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel 인터페이스에는 물리적 구성 및 소프트웨어 버전에 따라 여러 가지 제한 사항이 있습니다. 자세한 내용은 아래 섹션을 참조하십시오.

### 일반 인터페이스 제한 사항

- EtherChannel은 FDM 관리 버전 6.5 이상을 실행하는 디바이스에서만 사용할 수 있습니다.
- Cisco Defense Orchestrator는 Firepower 디바이스 1010, 1120, 1140, 1150, 2110, 2120, 2130, 2140, 3110, 3120, 3130, 3140에서 EtherChannel 인터페이스 구성을 지원합니다. 디바이스 모델별 인터페이스 제한 사항은 [디바이스별 제한 사항](#)을 참조하십시오.
- 채널 그룹의 모든 인터페이스는 미디어 유형 및 용량이 동일해야 하며 속도 및 듀플렉스를 동일하게 설정해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 없습니다.
- EtherChannel을 연결하는 디바이스는 802.3ad EtherChannel도 지원해야 합니다.
- FDM 관리 디바이스에서는 VLAN 태그 처리된 LACPDU를 지원하지 않습니다. Cisco IOS vlan dot1Q tag native 명령을 사용하여 인접한 스위치에서 네이티브 VLAN 태깅을 활성화할 경우, FDM 관리 디바이스에서는 태그 처리된 LACPDU를 제거합니다. 인접한 스위치에서 네이티브 VLAN 태깅을 비활성화해야 합니다.
- 모든 FDM 관리 디바이스 컨피그레이션에서는 멤버 물리적 인터페이스 대신 논리적 EtherChannel 인터페이스를 참조합니다.
- Portchannel 인터페이스는 물리적 인터페이스로 표시됩니다.

### 디바이스별 제한 사항

다음 디바이스에는 특정 인터페이스 제한이 있습니다.

#### 1000 Series

- Firepower 1010은 최대 8개의 EtherChannel 인터페이스를 지원합니다.
- Firepower 1120,1140,1150은 최대 12개의 EtherChannel 인터페이스를 지원합니다.
- 1000 시리즈는 LACP 빠른 속도를 지원하지 않습니다. LACP는 항상 일반 속도를 사용합니다. 이 설정은 구성 가능하지 않습니다.

### 2100 Series

- Firepower 2110 및 2120 모델은 최대 12개의 EtherChannel 인터페이스를 지원합니다.
- Firepower 2130 및 2140 모델은 최대 16개의 EtherChannel 인터페이스를 지원합니다.
- 2100 시리즈는 LACP 빠른 속도를 지원하지 않습니다. LACP는 항상 일반 속도를 사용합니다. 이 설정은 구성 가능하지 않습니다.

### Secure Firewall 3100 시리즈

- 모든 Secure Firewall 3100 모델은 최대 16개의 EtherChannel 인터페이스를 지원합니다.
- Secure Firewall 3100 모델은 LACP 빠른 속도를 지원합니다.
- Secure Firewall 3100 Series 모델은 네트워크 모듈 및 인터페이스의 OIR(Breakout Online Insertion and Removal) 활성화 또는 비활성화를 지원하지 않습니다.

### 4100 Series 및 9300 Series

- 4100 및 9300 Series에서는 EtherChannel을 생성하거나 구성할 수 없습니다. 이러한 디바이스에 대한 Etherchannel은 FXOS 새시에서 구성해야 합니다.
- 4100 및 9300 Series의 Etherchannel은 Cisco Defense Orchestrator에서 물리적 인터페이스로 표시 됩니다.

## EtherChannel 인터페이스 추가


다음 절차를 사용하여 FDM 매니지드 디바이스에 EtherChannel을 추가합니다.



**Note** 다른 EtherChannel을 즉시 생성하려면 **Create Another**(다른 **EtherChannel** 생성) 체크 박스를 선택하고 **Create**(생성)를 클릭합니다.

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 **FTD** 탭을 클릭하고 EtherChannel을 추가할 디바이스를 선택합니다.
- 단계 4 오른쪽에 있는 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 선택합니다.

단계 5 파란색 더하기  버튼을 클릭하고 **EtherChannel**을 선택합니다.

단계 6 (선택 사항) **Logical Name**(논리적 이름)을 입력합니다.

단계 7 (선택 사항) 설명을 입력합니다.

단계 8 **EtherChannel ID**를 입력합니다.

Firepower 1010 Series의 경우 1~8 사이의 값을 입력합니다.

Firepower 2100, 3100, 4100, 9300 Series의 경우 1~48 사이의 값을 입력합니다.

단계 9 **Link Aggregation Control Protocol**(링크 어그리게이션 제어 프로토콜)의 드롭다운 버튼을 클릭하고 두 가지 옵션 중 하나를 선택합니다.

- **Active**(액티브) - LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- **On**(켜짐) - EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. **On**(켜짐)인 EtherChannel은 **On**(켜짐)으로 구성된 다른 EtherChannel과만 연결할 수 있습니다.

단계 10 EtherChannel에 멤버로 포함할 인터페이스를 검색하여 선택합니다. 하나 이상의 인터페이스를 포함해야 합니다.

경고: EtherChannel 인터페이스를 멤버로 추가하고 이미 IP 주소가 구성된 경우 CDO는 멤버의 IP 주소를 제거합니다.

단계 11 **Create**(생성)를 클릭합니다.

#### 관련 정보:

- [FDM-관리 디바이스용 EtherChannel 인터페이스 편집 또는 제거](#)
- [EtherChannel 인터페이스에 하위 인터페이스 추가](#)
- [EtherChannel에서 하위 인터페이스 편집 또는 제거](#)
- [Firepower 인터페이스 구성에 대한 지침 및 제한 사항](#)
- [보안 영역에 FDM-관리 디바이스 인터페이스 할당](#)
- [FDM-관리 디바이스에 대한 EtherChannel 인터페이스 추가, on page 277](#)

## FDM-관리 디바이스용 EtherChannel 인터페이스 편집 또는 제거

다음 절차를 사용하여 기존 EtherChannel 인터페이스를 수정하거나 FDM 관리 디바이스에서 EtherChannel 인터페이스를 제거합니다.

### EtherChannel 편집

EtherChannel에는 수정할 때 알고 있어야 하는 몇 가지 제한 사항이 있습니다. 자세한 내용은 [EtherChannel](#)을 참조하십시오.



**Note** EtherChannel에는 하나 이상의 멤버가 있어야 합니다.

기존 EtherChannel을 편집하려면 다음 절차를 수행합니다.


### Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭하고 수정할 EtherChannel과 연결된 위협 방어를 선택합니다.

단계 4 오른쪽에 있는 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.

단계 5 **Interfaces**(인터페이스) 페이지에서 편집할 EtherChannel 인터페이스를 선택합니다. 오른쪽의 **Actions**(작업) 창에서 편집  아이콘을 클릭합니다.

단계 6 다음 항목을 수정합니다.

- 논리적 이름.
- 도.
- 설명
- 보안 영역 할당.
- Link Aggregation Control Protocol 상태.
- **IPv4, IPv6** 또는 **Advanced**(고급) 탭의 IP 주소 구성.
- EtherChannel 멤버.

**Warning** 경고: EtherChannel 인터페이스를 멤버로 추가하고 이미 IP 주소가 구성된 경우 CDO는 멤버의 IP 주소를 제거합니다.

단계 7 **Save**(저장)를 클릭합니다.

## EtherChannel 인터페이스 제거



**Note** HA(고가용성) 또는 기타 구성과 연결된 EtherChannel 인터페이스입니다. CDO에서 삭제하기 전에 모든 구성에서 EtherChannel 인터페이스를 수동으로 제거해야 합니다.

FDM 관리 디바이스에서 EtherChannel 인터페이스를 제거하려면 다음 절차를 수행합니다.

## Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 **FTD** 탭을 클릭하고 삭제할 EtherChannel과 연결된 위협 방어를 클릭합니다.
- 단계 4 오른쪽에 있는 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 선택합니다.
- 단계 5 **Interfaces**(인터페이스) 페이지에서 편집할 EtherChannel 인터페이스를 선택합니다. 오른쪽의 Actions(작업) 창에서 **Remove**(제거)를 클릭합니다.
- 단계 6 EtherChannel 인터페이스 삭제를 확인하고 **OK**(확인)를 클릭합니다.

## EtherChannel 인터페이스에 하위 인터페이스 추가

### EtherChannel 하위 인터페이스

**Interfaces**(인터페이스) 페이지에서는 각 인터페이스를 확장하여 하위 인터페이스가 있는 디바이스의 인터페이스를 볼 수 있습니다. 이 확장된 보기에는 하위 인터페이스의 고유한 논리적 이름, 활성화/비활성화 상태, 연결된 보안 영역 및 모드도 표시됩니다. 하위 인터페이스의 인터페이스 유형 및 모드는 상위 인터페이스에 의해 결정됩니다.

### 일반 제한 사항

CDO는 다음 인터페이스 유형에 대한 하위 인터페이스를 지원하지 않습니다.

- 관리 전용으로 구성된 인터페이스.
- 스위치 포트 모드로 구성된 인터페이스.
- 수동 인터페이스.
- VLAN 인터페이스.
- BVI(Bridge Virtual Interface).
- 이미 다른 EtherChannel 인터페이스의 멤버인 인터페이스.

다음에 대한 하위 인터페이스를 생성할 수 있습니다.

- 브리지 그룹 멤버.
- EtherChannel 인터페이스.
- 물리적 인터페이스.

## EtherChannel 인터페이스에 하위 인터페이스 추가

기존 인터페이스에 하위 인터페이스를 추가하려면 다음 절차를 수행합니다.



**Note** 다른 하위 인터페이스를 즉시 생성하려면 **Create Another**(다른 하위 인터페이스 생성) 체크 박스를 선택하고 **Create**(생성)를 클릭합니다.

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 **FTD** 탭을 클릭하고 EtherChannel을 추가할 위협 방어를 선택합니다. 오른쪽에 있는 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 선택합니다.
- 단계 4 하위 인터페이스를 그룹화할 인터페이스를 선택합니다. 오른쪽의 **Action**(작업) 창에서 **+ New Subinterface** 버튼을 클릭합니다.
- 단계 5 (선택 사항) **Logical Name**(논리적 이름)을 입력합니다.
- 단계 6 (선택 사항) 설명을 입력합니다.
- 단계 7 (선택 사항) 하위 인터페이스에 보안 영역을 할당합니다. 하위 인터페이스에 논리적 이름이 없으면 보안 영역을 할당할 수 없습니다.
- 단계 8 VLAN ID를 입력합니다.
- 단계 9 **EtherChannel ID**를 입력합니다. 1~48 사이의 값을 사용합니다. Firepower 1010 Series의 경우 1~8 사이의 값을 입력합니다.
- 단계 10 **IPv4**, **IPv6**, **Advanced**(고급) 탭 중에서 선택하여 하위 인터페이스의 IP 주소를 구성합니다.
- 단계 11 **Create**(생성)를 클릭합니다.

## EtherChannel에서 하위 인터페이스 편집 또는 제거

다음 절차를 사용하여 기존 하위 인터페이스를 수정하거나 Etherchannel 인터페이스에서 하위 인터페이스를 제거합니다.



**Note** 하위 인터페이스 및 EtherChannel 인터페이스에는 구성에 영향을 줄 수 있는 일련의 지침 및 제한 사항이 있습니다. 자세한 내용은 [일반 제한 사항](#)을 참조하십시오.

### 하위 인터페이스 편집

EtherChannel 인터페이스와 연결된 기존 하위 인터페이스를 편집하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 CDO에 로그인합니다.




단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 3 **Devices**(디바이스) 탭을 클릭합니다.

단계 4 **FTD** 탭을 클릭하고 편집할 EtherChannel 및 하위 인터페이스와 연결된 위협 방어를 선택합니다.

단계 5 오른쪽에 있는 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 선택합니다.

단계 6 하위 인터페이스가 속해 있는 EtherChannel 인터페이스를 찾아 확장합니다.

단계 7 편집할 하위 인터페이스를 선택합니다. 오른쪽의 Action(작업) 창에서 편집  아이콘을 클릭합니다.

단계 8 다음 항목을 수정합니다.

- 논리적 이름.
- 도.
- 설명
- 보안 영역 할당.
- VLAN ID
- IPv4, IPv6 또는 Advanced(고급) 탭의 IP 주소 구성.

단계 9 **Save**(저장)를 클릭합니다.

## EtherChannel에서 하위 인터페이스 제거

다음 절차를 사용하여 EtherChannel 인터페이스에서 기존 하위 인터페이스를 제거합니다.

### Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭하고 편집할 EtherChannel 및 하위 인터페이스와 연결된 위협 방어를 선택합니다. 오른쪽에 있는 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 선택합니다.

단계 4 하위 인터페이스가 속해 있는 EtherChannel 인터페이스를 찾아 확장합니다.

단계 5 삭제할 하위 인터페이스를 선택합니다.

단계 6 오른쪽의 Actions(작업) 창에서 **Remove**(제거)를 클릭합니다.

단계 7 하위 인터페이스 인터페이스 삭제를 확인하고 **OK**(확인)를 클릭합니다.

## 가상 FDM-관리 디바이스에 인터페이스 추가

가상 FDM 관리 디바이스를 구축할 때는 가상 머신에 인터페이스를 할당합니다. 그런 다음, FDM 관리 디바이스 내에서 하드웨어 디바이스에 사용하려는 것과 같은 메시드로 해당 인터페이스를 구성합니다.

그러나 가상 머신에 가상 인터페이스를 더 추가한 다음, FDM에서 이를 자동으로 인식하도록 할 수는 없습니다. 가상 FDM 관리 디바이스에 대한 실제 인터페이스와 동일한 인터페이스가 더 필요한 경우에는 기본적으로 인터페이스 구성을 다시 시작해야 합니다. 새 가상 머신을 구축할 수도 있고 다음 절차를 사용할 수도 있습니다.



**Caution** 가상 머신에 인터페이스를 추가하려면 가상 FDM 관리 구성을 완전히 지워야 합니다. 컨피그레이션에서 그대로 유지되는 부분은 관리 주소와 게이트웨이 설정뿐입니다.

시작하기 전에

FDM 관리 디바이스에서 다음을 수행합니다.

- 가상 FDM 관리 디바이스 구성을 검사하여 새 가상 머신에서 복제할 설정을 적어 둡니다.
- **Devices(디바이스) > Smart License(스마트 라이선스) > View Configuration(구성 보기)**을 선택하고 모든 기능 라이선스를 비활성화합니다.

### Procedure

단계 1 가상 FDM 관리 디바이스 전원 끄기

단계 2 가상 머신 소프트웨어를 사용하여 가상 FDM 관리 디바이스에 인터페이스를 추가합니다. VMware의 경우 가상 어플라이언스는 기본적으로 e1000(1Gbit/s) 인터페이스를 사용합니다. vmxnet3 또는 ixgbe(10Gbit/s) 인터페이스를 사용할 수도 있습니다.

단계 3 가상 FDM 관리 디바이스 전원 켜기

단계 4 가상 FDM 관리 디바이스 콘솔을 열고 로컬 관리자를 삭제한 후 활성화합니다. 로컬 관리자를 삭제했다가 활성화하면 디바이스 컨피그레이션이 재설정되며 시스템이 새 인터페이스를 인식하게 됩니다. 관리 인터페이스 컨피그레이션은 재설정되지 않습니다. 다음 SSH 세션은 해당 명령을 보여줍니다.

```
> show managers
Managed locally.
> configure manager delete
If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager. Otherwise, those licenses remain assigned to the device
in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled
> show managers
No managers configured.
> configure manager local
>
```

단계 5 FDM 관리 디바이스에 대한 브라우저 세션을 열고 디바이스 설정 마법사를 완료한 다음 디바이스를 구성합니다. 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#), 버전 xxx 가이드 시작하기 장의 "초기 구성 완료" 섹션을 참조하십시오.

## FDM-관리 디바이스에 대한 스위치 포트 모드 인터페이스

각 물리적 Firepower 1010 인터페이스의 경우, 해당 작업을 방화벽 인터페이스 또는 스위치 포트에 설정할 수 있습니다. 스위치 포트에서는 하드웨어에서 스위칭 기능을 사용하여 레이어 2에서 트래픽을 전달합니다. 동일한 VLAN의 스위치 포트는 하드웨어 스위칭을 사용하여 서로 통신할 수 있으며 트래픽에는 FDM 관리 디바이스 보안 정책이 적용되지 않습니다. 액세스 포트의 경우 태그 없는 트래픽만 허용되며 이러한 포트는 단일 VLAN에 할당할 수 있습니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용되며 둘 이상의 VLAN에 속할 수 있습니다. 버전 6.4로 이미 재설치된 디바이스의 경우, 이더넷 1/2~1/8이 VLAN 1의 액세스 스위치 포트에 구성됩니다. 버전 6.4 이상으로 수동으로 업그레이드한 디바이스의 경우 이더넷 구성은 업그레이드 이전의 구성을 유지합니다. 동일한 VLAN의 스위치 포트는 하드웨어 스위칭을 사용하여 서로 통신할 수 있으며 트래픽에는 FDM 관리 디바이스 보안 정책이 적용되지 않습니다.

### 액세스 또는 트렁크

스위치 포트에 구성된 물리적 인터페이스는 액세스 포트 또는 트렁크 포트에 할당할 수 있습니다.

액세스 포트는 하나의 VLAN에만 트래픽을 전달하고 태그가 지정되지 않은 트래픽만 수락합니다. 단일 호스트 또는 디바이스로 트래픽을 전달하려는 경우 이 옵션을 사용하는 것이 좋습니다. 또한 인터페이스와 연결할 VLAN을 지정해야 합니다. 그렇지 않으면 VLAN 1이 기본값이 됩니다.

트렁크 포트는 여러 VLAN에 트래픽을 전달합니다. 하나의 VLAN 인터페이스를 기본 트렁크 포트에 할당하고 하나 이상의 VLAN을 연결된 트렁크 포트에 할당해야 합니다. 스위치 포트 인터페이스와 연결할 최대 20개의 인터페이스를 선택할 수 있습니다. 그러면 서로 다른 VLAN ID의 트래픽이 스위치 포트 인터페이스를 통과할 수 있습니다. 태그가 지정되지 않은 트래픽이 스위치 포트를 통과하는 경우 트래픽은 기본 VLAN 인터페이스의 VLAN ID로 태그가 지정됩니다. 1002와 1005 사이의 기본 FDDI(Fibre Distributed Data Interface) 및 토큰 링 ID는 VLAN ID에 사용할 수 없습니다.

### 포트 모드 변경

라우팅 모드에 대해 VLAN 멤버로 구성된 인터페이스를 선택하면 CDO는 자동으로 인터페이스를 스위치 포트 모드로 변환하고 기본적으로 인터페이스를 액세스 포트에 구성합니다. 따라서 논리적 이름 및 연결된 고정 IP 주소가 인터페이스에서 제거됩니다.

### 구성 제한 사항

다음 제한 사항에 유의하십시오.

- 물리적 Firepower 1010 디바이스만 스위치 포트 모드 구성을 지원합니다. 가상 FDM 관리 디바이스는 스위치 포트 모드를 지원하지 않습니다.
- Firepower 1010 디바이스는 최대 60개의 VLAN을 허용합니다.

- 스위치 포트 모드에 대해 구성된 VLAN 인터페이스는 이름이 지정되지 않아야 합니다. 즉, MTU를 반드시 1500바이트로 구성해야 합니다.
- 스위치 포트 모드로 구성된 인터페이스는 삭제할 수 없습니다. 인터페이스 모드를 스위치 포트 모드에서 라우팅 모드로 수동으로 변경해야 합니다.
- 스위치 포트 모드에 대해 구성된 인터페이스는 IP 주소를 지원하지 않습니다. 인터페이스가 현재 VPN, DHCP에 대해 참조되거나 구성된 경우 또는 고정 경로와 연결된 경우 IP 주소를 반드시 수동으로 제거해야 합니다.
- 브리지 그룹 인터페이스의 어떤 멤버도 스위치 포트로 사용할 수 없습니다.
- VLAN 인터페이스의 MTU는 반드시 1500바이트여야 합니다. 명명되지 않은 VLAN 인터페이스는 다른 구성을 지원하지 않습니다.
- 스위치 포트 모드는 다음을 지원하지 않습니다.
  - 진단 인터페이스.
  - 동적, 멀티캐스트 또는 ECMP(Equal-Cost Multi-Path) 라우팅.
  - 수동 인터페이스.
  - etherchannel을 포트하거나 etherchannel의 멤버인 인터페이스를 사용합니다.
  - 하위 인터페이스.
  - 페일오버 및 상대 링크.

#### 고가용성 및 스위치 포트 모드 인터페이스

고가용성 사용 시 스위치 포트 기능을 사용해서는 안 됩니다. 스위치 포트는 하드웨어에서 작동하므로 액티브 유닛과 스탠바이 유닛 모두에서 트래픽을 계속 전달합니다. 고가용성은 트래픽이 스탠바이 유닛을 통과하는 것을 방지하도록 설계되었지만, 이 기능은 스위치 포트로 확장되지 않습니다. 일반 고가용성 네트워크 설정에서 두 유닛의 액티브 스위치 포트는 네트워크 루프로 이어집니다. 모든 스위칭 기능에는 외부 스위치를 사용하는 것이 좋습니다. VLAN 인터페이스는 장애 조치를 통해 모니터링될 수 있지만 스위치 포트는 그럴 수 없습니다.



**Note** 방화벽 인터페이스만 페일 오버 링크로 사용할 수 있습니다.

#### 템플릿의 스위치 포트 모드 구성

스위치 포트 모드에 대해 구성된 인터페이스를 사용하여 디바이스의 템플릿을 생성할 수 있습니다. 템플릿에서 디바이스로 인터페이스를 매핑할 때는 다음 시나리오에 유의하십시오.

- 템플릿을 적용하기 전에 템플릿 인터페이스에 VLAN 멤버가 포함되어 있지 않으면 CDO는 동일한 속성을 가진 사용 가능한 디바이스 인터페이스에 자동으로 매핑합니다.

- VLAN 멤버를 포함하지 않는 템플릿 인터페이스가 **N/A**로 구성된 디바이스 인터페이스에 매핑된 경우 CDO는 템플릿을 적용할 디바이스에 인터페이스를 자동으로 생성합니다.
- VLAN 멤버를 포함하는 템플릿 인터페이스가 존재하지 않는 디바이스 인터페이스에 매핑된 경우 템플릿 적용이 실패합니다.
- 템플릿은 동일한 디바이스 인터페이스에 두 개 이상의 템플릿 인터페이스를 매핑하는 것을 지원하지 않습니다.
- 템플릿의 관리 인터페이스는 디바이스의 관리 인터페이스에 매핑되어야 합니다.


## FDM-관리 디바이스 VLAN 구성

하위 인터페이스 또는 스위치 포트를 구성하려면 먼저 VLAN 인터페이스를 구성해야 합니다.



**Note** FDM 관리 디바이스는 최대 60개의 VLAN 인터페이스를 지원합니다.

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 VLAN을 생성할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.
- 단계 5 **Interfaces**(인터페이스) 페이지에서  버튼을 클릭합니다.
- 단계 6 다음을 구성합니다.
  - **Parent Interface**(상위 인터페이스) - 상위 인터페이스는 하위 인터페이스를 추가할 물리적 인터페이스입니다. 하위 인터페이스를 생성한 후에는 상위 인터페이스를 변경할 수 없습니다.
  - (선택 사항) **Logical Name**(논리적 이름) - VLAN의 이름을 최대 48자로 설정합니다. 영문자는 소문자로 입력해야 합니다. VLAN과 기타 VLAN 또는 방화벽 인터페이스 간에 라우팅하지 않으려는 경우에는 VLAN 인터페이스 이름을 비워 둡니다.
 

**Note** 이름을 입력하지 않으면 **Advanced Options**(고급 옵션)의 MTU를 1500으로 설정해야 합니다. MTU를 1500 이외의 다른 값으로 변경하는 경우 VLAN의 이름을 지정해야 합니다.
  - (선택 사항) **Description**(설명) - 설명은 줄바꿈 없이 1줄, 최대 200자로 작성합니다.
  - (선택 사항) **Security Zone**(보안 영역) - 보안 영역에 하위 인터페이스를 할당합니다. 논리적 이름이 없는 하위 인터페이스는 할당할 수 없습니다. 하위 인터페이스를 생성한 후 보안 영역을 할당할 수도 있습니다. 자세한 내용은 [Firepower 인터페이스 설정에서 보안 영역 사용](#)을 참조하십시오.

- (선택 사항) **VLAN ID** - 이 하위 인터페이스에서 패킷에 태그를 지정하는 데 사용할 1~4070 사이의 VLAN ID를 입력합니다.

**Note** VLAN 인터페이스는 기본적으로 라우팅됩니다. 나중에 이 VLAN 인터페이스를 브리지 그룹에 추가하면 Cisco Defense Orchestrator(CDO)가 자동으로 모드를 **BridgeGroupMember**로 변경합니다. 마찬가지로, 이 VLAN 인터페이스를 스위치 포트 모드로 변경하면 CDO는 자동으로 모드를 스위치 포트로 변경합니다.

- (선택 사항) 하위 인터페이스 **ID** - 하위 인터페이스 ID를 1~4294967295 사이의 정수로 입력합니다. 이 ID는 인터페이스 ID에 추가됩니다(예: Ethernet1/1.100). 편의를 위해 VLAN ID를 일치시킬 수 있으나 꼭 그렇게 해야 하는 것은 아닙니다. 하위 인터페이스를 생성한 후에는 ID를 변경할 수 없습니다.

**단계 7 IPv4 Address(IPv4 주소)** 탭을 클릭하고 Type(유형) 필드에서 다음 옵션 중 하나를 선택합니다.

- **Static(고정)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

**Note** 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. 자세한 내용은 [DHCP 서버 구성](#)을 참조하십시오.

- **Dynamic(동적)(DHCP)** - 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.

- **Route Metric(경로 메트릭)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
- **Obtain Default Route(기본 경로 얻기)** - DHCP 서버에서 기본 경로를 가져오려면 이 옵션을 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).

- **DHCP Address Pool(DHCP 주소 풀)** - 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 구성이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다.

**단계 8 (선택 사항) IPv6 Address(IPv6 주소)** 탭을 클릭하고 다음을 구성합니다.

- **Sate(상태)** - 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 State(상태) 슬라이더를 파란색으로 끕니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

**Note** IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(주소 자동 구성)** - 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

- **Suppress RA(RA 표시 안 함)**-라우터 알림을 표시하지 않을지를 선택합니다. 위협 방어는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

FDM 관리 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 것을 제안합니다.

- **Static Address/Prefix(고정 주소/접두사)** - 스테이트리스 자동 구성을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48 와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 [Firepower 인터페이스용 IPv6 주소 지정](#)을 참조하십시오.
- **Standby IP Address(스탠바이 IP 주소)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

## 단계 9 (선택 사항) **Advanced**(고급) 탭을 클릭합니다.

- 시스템에서 고가용성 구성의 피어 유닛으로 페일오버를 수행할지 여부를 결정할 때 인터페이스 상태를 고려하려면 **HA Monitoring(HA 모니터링)**에 대해 **Enable(활성화)**을 선택합니다.

이 옵션은 고가용성을 구성하지 않는 경우 무시되며 인터페이스의 이름을 구성하지 않는 경우에도 무시됩니다.

- 데이터 인터페이스 관리만 수행하려면 **Management Only(관리만)**를 선택합니다.

관리 전용 인터페이스에서는 통과 트래픽을 허용하지 않으므로 데이터 인터페이스를 관리 전용으로 설정할 때 사용할 수 있는 값은 거의 없습니다. 관리/진단 인터페이스(항상 관리 전용)의 경우에는 이 설정을 변경할 수 없습니다.

- IPv6 컨피그레이션 설정을 수정합니다.
  - **IPv6 주소 구성에 DHCP 활성화** - IPv6 라우터 알림 패킷에서 관리 주소 구성 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 구성 클라이언트에게 DHCPv6를 사용하여 파생된 스테이트리스 자동 구성 주소 이외의 주소도 얻도록 안내합니다.
  - **IPv6 비주소 구성에 DHCP 활성화** - IPv6 라우터 알림 패킷에서 기타 주소 구성 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6로부터 추가 정보(예: DNS 서버 주소)를 얻도록 안내합니다.
  - **DAD 시도** - 인터페이스가 DAD(Duplicate Address Detection)를 수행하는 빈도를 0~600 사이의 값으로 설정합니다. 기본값은 1입니다. 스테이트리스 자동 컨피그레이션 프로세스에서 DAD는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다. 인터페이스에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.
- **MTU(Maximum Transmission Unit)**를 원하는 값으로 변경합니다.

기본 MTU는 1500바이트입니다. 64~9198(가상 FDM 관리 디바이스의 경우 9000, Firepower 4100/9300의 경우 9184)의 값을 지정할 수 있습니다. 네트워크에서 대개 점보 프레임이 표시되면 높은 값을 설정합니다.

**Note** ASA 5500-X Series 디바이스, ISA 3000 Series 디바이스 또는 가상 FDM 관리 디바이스에서 MTU를 1500보다 큰 값으로 늘리는 경우에는 VLAN 이름 지정을 취소하고 디바이스를 재부팅해야 합니다. 이렇게 하려면 CLI에 로그인하여 reboot 명령을 사용합니다. HA를 위해 디바이스를 구성한 경우, 스탠바이 디바이스도 재부팅해야 합니다. 점보 프레임 지원이 항상 활성화되어 있는 Firepower 모델은 리부팅하지 않아도 됩니다.

- (하위 인터페이스 및 HA 쌍의 경우 선택 사항) **MAC** 주소를 구성합니다.

시스템은 기본적으로 인터페이스에 대해 NIC(Network Interface Card)에 버닝된 MAC 주소를 사용합니다. 따라서 인터페이스의 모든 하위 인터페이스는 같은 MAC 주소를 사용하므로 하위 인터페이스별로 고유한 주소를 생성할 수 있습니다. 고가용성을 구성하는 경우에는 액티브/스탠바이 MAC 주소도 수동으로 구성하는 것이 좋습니다. MAC 주소를 정의하면 페일오버 시 네트워크에서 일관성을 유지할 수 있습니다.

- **MAC Address(MAC 주소)** - H.H.H. 형식의 MAC(Media Access Control) 주소입니다. 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다(즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없음).



- 스탠바이 MAC 주소 - HA 쌍과 함께 사용합니다. 액티브 유닛이 페일오버되고 스탠바이 유닛이 액티브 상태가 되면, 네트워크 중단을 최소화하기 위해 새 액티브 유닛에서 액티브 MAC 주소를 사용하기 시작하고 기존 액티브 유닛은 스탠바이 주소를 사용합니다.

- 단계 10 이 디바이스에 대해 다른 하위 인터페이스를 생성하려면 하위 인터페이스 구성을 완료하기 전에 **Create another**(다른 하위 인터페이스 생성)를 선택합니다.
- 단계 11 (선택 사항) 팝업 창의 오른쪽 상단 모서리에 있는 **State**(상태) 슬라이더를 회색에서 파란색으로 전환하여 하위 인터페이스를 생성할 때 활성화합니다.
- 단계 12 확인을 클릭합니다.
- 단계 13 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 스위치 포트 모드에 대한 FDM-관리 디바이스 VLAN 구성


구성하기 전에 스위치 포트 모드에 대한 제한 사항을 읽어보십시오. 자세한 내용은 [FDM-관리 디바이스에 대한 스위치 포트 모드 인터페이스](#)를 참조하십시오.



**Note** 언제든지 물리적 인터페이스에 VLAN 멤버를 할당하거나 편집할 수 있습니다. 새 구성을 확인한 후 디바이스에 변경 사항을 구축해야 합니다.

### 스위치 포트 모드에 대한 VLAN 인터페이스 생성

#### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 인터페이스를 구성할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.
- 단계 5 **Interfaces**(인터페이스) 페이지에서  버튼을 클릭하여 **VLAN Interface**(VLAN 인터페이스)를 선택합니다.
- 단계 6 **VLAN Members**(VLAN 멤버) 탭을 보고 원하는 물리적 인터페이스를 선택합니다.


**Note** 액세스 또는 기본 트렁크에 대해 구성된 VLAN 인터페이스를 참조하는 멤버를 추가하도록 선택한 경우 하나의 VLAN만 멤버로 선택할 수 있습니다. 연결된 트렁크에 대해 구성된 VLAN 인터페이스를 참조하는 물리적 인터페이스는 최대 20개의 인터페이스를 멤버로 지원합니다.

- 단계 7 [FDM-관리 디바이스 VLAN 구성](#)에 설명된 대로 VLAN 인터페이스의 나머지 부분을 구성합니다.

- 단계 8 **Save**(저장)를 클릭합니다. VLAN 구성을 재설정하고 인터페이스에 IP 주소를 재할당할 것임을 확인합니다.
- 단계 9 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 스위치 포트 모드에 대한 기존 물리적 인터페이스 구성

### Procedure


- 단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 인터페이스를 구성할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Interfaces**(인터페이스)를 클릭합니다.
- 단계 5 **Interfaces**(인터페이스) 페이지에서 수정할 물리적 인터페이스를 선택합니다. 오른쪽의 **Action**(작업) 창에서 편집  아이콘을 클릭합니다.
- 단계 6 스위치 포트 모드에 대해 구성된 인터페이스는 논리적 이름을 지원하지 않습니다. 인터페이스에 논리적 이름이 있는 경우 삭제합니다.
- 단계 7 **Mode**(모드)를 찾은 다음 드롭다운 메뉴를 사용하여 **Switch Port**(스위치 포트)를 선택합니다.
- 단계 8 스위치 포트 모드에 대한 물리적 인터페이스를 구성합니다.
- (선택 사항) **Protected Port**(보호된 포트) 체크 박스를 선택하여 이 스위치 포트를 보호된 상태로 설정합니다. 그러면 스위치 포트가 동일한 VLAN에서 보호되는 다른 스위치 포트와 통신하는 것을 방지할 수 있습니다. 스위치 포트의 디바이스가 주로 다른 VLAN에서 액세스되어 VLAN 간 액세스를 허용할 필요가 없으며 감염 또는 기타 보안 침입 시 디바이스를 서로 분리하려는 경우 스위치 포트가 서로 통신하지 못하도록 할 수 있습니다. 예를 들어 세 개의 웹 서버를 호스팅하는 DMZ가 있는 경우, 이 옵션을 각 스위치 포트에 적용하면 웹 서버를 서로 분리할 수 있습니다. 내부 및 외부 네트워크 둘 다 세 개의 웹 서버와 통신할 수 있지만 웹 서버 간에 서로 통신할 수는 없습니다.
  - Usage Type(사용 유형)으로 **Access**(액세스) 또는 **Trunk**(트렁크)를 선택합니다. 필요한 포트 유형을 확인하려면 **FDM-관리 디바이스에 대한 스위치 포트 모드 인터페이스**를 참조하십시오.
    - **Trunk**(트렁크)를 선택하는 경우, 하나의 VLAN 인터페이스를 기본 트렁크 VLAN으로 선택하여 태그가 지정되지 않은 트래픽을 전달하고 하나 이상의 연결된 VLAN을 선택하여 태그가 지정된 트래픽을 전달해야 합니다.  아이콘을 클릭하여 기존 물리적 인터페이스를 확인합니다. 최대 20개의 VLAN 인터페이스를 연결된 VLAN으로 선택할 수 있습니다.
    - **Create New VLAN**(새 VLAN 생성)을 클릭하여 액세스 모드로 설정된 새 VLAN 인터페이스를 생성할 수 있습니다.

- 단계 9 **Save(저장)**를 클릭합니다. VLAN 구성을 재설정하고 인터페이스에 IP 주소를 재할당할 것임을 확인합니다.
- 단계 10 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 번 변경 사항을 한 번에 구축합니다.

## Firepower 인터페이스 보기 및 모니터링

Firepower 인터페이스를 보려면 다음 단계를 수행합니다.

### Procedure

- 단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 인터페이스를 확인할 디바이스를 클릭합니다.
- 단계 4 오른쪽의 **Management(관리)** 창에서 **Interfaces(인터페이스)**()를 선택합니다.
- 단계 5 인터페이스 테이블에서 인터페이스를 선택합니다.
- 인터페이스 행을 확장하면 하위 인터페이스 정보가 표시됩니다.
  - 오른쪽에 자세한 인터페이스 정보가 표시됩니다.

## CLI에서 인터페이스 모니터링

SSH를 사용하여 디바이스에 연결하고 아래 명령을 실행하여 인터페이스에 대한 몇 가지 기본 정보, 동작 및 통계를 볼 수 있습니다.

SSH를 사용하여 디바이스에 쉽게 연결하려면 모니터링할 FDM 관리 디바이스를 SSH 디바이스로 온보딩한 다음, CDO에서 >\_ 명령줄 인터페이스를 사용합니다.

- **show interface** 는 인터페이스 통계 및 구성 정보를 표시합니다. 이 명령에는 필요한 정보를 가져오는 데 사용할 수 있는 여러 키워드가 있습니다. 사용 가능한 옵션을 확인하려면 키워드로 ? 를 사용합니다.
- **show ipv6 interface** 는 인터페이스에 대한 IPv6 구성 정보를 표시합니다.
- **show bridge-group** 은 멤버 정보와 IP 주소를 비롯하여 BVI(Bridge Virtual Interfaces)에 대한 정보를 표시합니다.
- **show conn** 은 인터페이스를 통해 현재 설정되어 있는 연결에 대한 정보를 표시합니다.
- **show traffic** 은 각 인터페이스를 통과하는 트래픽에 대한 통계를 표시합니다.
- **show ipv6 traffic** 은 디바이스를 통과하는 IPv6 트래픽에 대한 통계를 표시합니다.

- `show dhcpd` 는 인터페이스의 DHCP 사용량에 대한 통계와 기타 정보(특히 인터페이스에 구성된 DHCP 서버 관련 정보)를 표시합니다.

## FXOS를 사용하여 Firepower 디바이스에 추가된 인터페이스 동기화

Firepower 4100 Series 또는 9300 Series 디바이스에서 FXOS(Firepower eXtensible Operating System) Chassis Manager를 사용하여 인터페이스를 Firepower 디바이스에 추가하는 경우, Cisco Defense Orchestrator는 해당 구성 변경을 인식하지 못하고 구성 충돌을 보고합니다.

CDO에서 새로 추가된 인터페이스를 확인하려면 다음 절차를 수행합니다.

프로시저

- 단계 1 FDM 관리 디바이스에 로그인합니다.
- 단계 2 FDM 관리 기본 페이지의 Interfaces(인터페이스) 패널에서 **View All Interfaces**(모든 인터페이스 보기)를 클릭합니다.
- 단계 3 **Scan Interfaces**(인터페이스 스캔) 버튼을 클릭합니다.



- 단계 4 인터페이스가 스캔될 때까지 기다린 다음, **OK**(확인)를 클릭합니다.
- 단계 5 FDM 관리 디바이스에서 변경 사항을 구축합니다.
- 단계 6 관리자 또는 최고 관리자로 CDO에 로그인합니다.
- 단계 7 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 8 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 9 **FTD** 탭을 클릭하고 예상되는 새 인터페이스 구성이 포함된 디바이스를 선택합니다.
- 단계 10 **Check for Changes**(변경 사항 확인)를 클릭하면 디바이스의 구성 복사본과 CDO에 저장된 구성의 복사본을 즉시 비교합니다. CDO는 인터페이스 변경을 탐지하고 디바이스의 **Inventory**(재고 목록) 페이지에 있는 "Conflict Detected(충돌 탐지됨)" 상태를 보고합니다.
- 단계 11 **Review Conflict**(충돌 검토)를 클릭한 다음 OOB(Out of Band) 변경 사항을 수락하여 Conflict Detected(충돌 탐지됨) 상태를 해결합니다.

## 라우팅

라우팅은 소스에서 대상까지 네트워크에 걸친 정보의 이동입니다. 그 과정에서 적어도 하나의 중간 노드를 일반적으로 만나게 됩니다. 라우팅에는 2가지 기본적인 작업이 포함되는데, 최적의 라우팅 경로를 결정하는 것과 네트워크를 통한 패킷 전송입니다.

CDO(Cisco Defense Orchestrator)를 사용하여 FTD(Firepower Threat Defense) 디바이스에 대한 기본 경로 및 기타 고정 경로를 정의할 수 있습니다. 다음 항목에서는 라우팅 기본 사항과 CDO를 사용하여 FDM 관리 디바이스에 정적 라우팅을 구성하는 방법에 대해 설명합니다.

- 고정 라우팅 및 기본 경로 정보
- 라우팅 테이블과 경로 선택
- FDM-관리 디바이스에 대한 고정 및 기본 경로 구성
- 라우팅 모니터링

## 고정 라우팅 및 기본 경로 정보

연결되지 않은 호스트 또는 네트워크로 트래픽을 라우팅하려면 해당 호스트 또는 네트워크에 대한 경로를 정의해야 합니다. 정의된 경로는 고정 경로입니다. 기본 경로를 구성하는 것도 고려해 보십시오. 기본 경로는 다른 방법으로는 기본 네트워크 게이트웨이(대개 다음 홉 라우터)에 라우팅되지 않는 모든 트래픽에 적용됩니다.

관련 정보:

- 기본 라우터
- 고정 경로

## 기본 라우터

특정 네트워크로 가는 경로를 모르는 경우 가장 간단한 옵션은 트래픽을 라우팅하는 라우터에 의존하여 모든 트래픽을 업스트림 라우터로 보내는 기본 경로를 구성하는 것입니다. 기본 경로는 FTD 디바이스가 고정 경로를 정의하지 않은 모든 IP 패킷을 보내는 게이트웨이 IP 주소를 식별합니다. 기본 경로는 대상 IP 주소가 0.0.0.0/0(IPv4) 또는 ::0(IPv6)인 고정 경로일 뿐입니다.

## 고정 경로

고정 경로는 라우팅 테이블에 수동으로 정의하고 입력하는 한 네트워크에서 다른 네트워크로의 경로입니다. 다음과 같은 경우, 고정 경로를 사용할 수 있습니다.

- 사용 중인 네트워크 규모가 작고 안정적이며, 디바이스 간에 경로를 수동으로 추가하고 변경하는 것을 쉽게 관리할 수 있습니다.
- 네트워크에서 지원하지 않는 라우터 검색 프로토콜을 사용합니다.
- 트래픽이나 CPU 오버헤드를 라우팅 프로토콜과 연결하지 않는 것이 좋습니다.

- 기본 경로만으로 충분하지 않을 때도 있습니다. 기본 게이트웨이가 목적지 네트워크에 도달할 수 없는 경우가 있기 때문에 보다 구체적인 고정 경로도 구성해야 합니다. 예를 들어, 기본 게이트웨이가 밖에 있는 경우 기본 경로는 FDM 관리 디바이스에 직접 연결되지 않은 내부 네트워크로 트래픽을 연결할 수 없습니다.
- 동적 라우팅 프로토콜을 지원하지 않는 기능을 사용 중입니다.

#### 제한 사항:

- CDO는 현재 ASA 또는 FDM 관리 디바이스에서 VTI(Virtual Tunnel Interface) 터널의 관리, 모니터링 또는 사용을 지원하지 않습니다. VTI 터널이 구성된 디바이스는 CDO에 온보딩될 수 있지만 VTI 인터페이스는 무시됩니다. 보안 영역 또는 고정 경로가 VTI를 참조하는 경우 CDO는 VTI 참조 없이 보안 영역 및 고정 경로를 읽습니다. VTI 터널에 대한 CDO 지원이 곧 제공될 예정입니다.
- 소프트웨어 버전 7.0 이상에서 실행되는 FDM 관리 디바이스는 ECMP(Equal-Cost Multi-Path) 트래픽 영역을 구성할 수 있습니다. FDM 관리 디바이스가 CDO에 온보딩된 경우 동일한 메트릭 값을 사용하는 같은 대상 네트워크에 대한 경로를 허용하지 않으므로, 전역 VRF 경로에서 사용할 수 있는 ECMP 구성을 읽을 수는 있어도 수정할 수는 없습니다. FDM을 통해 ECMP 트래픽 영역을 생성하고 변경한 후 CDO로 읽을 수 있습니다. ECMP에 대한 자세한 내용은 [Firepower Device Manager 버전 7.0 이상용 Cisco Firepower Threat Defense 구성 가이드](#)의 "라우팅 기본 사항 및 고정 경로" 장의 "ECMP(Equal-Cost Multi-Path) 라우팅" 섹션을 참조하십시오.

## 라우팅 테이블과 경로 선택

NAT 변환(xlates) 및 규칙에서 이그레스 인터페이스를 결정하지 않는 경우, 시스템에서는 라우팅 테이블을 사용하여 패킷의 경로를 결정합니다.

라우팅 테이블의 경로에는 지정된 경로에 대한 상대적 우선순위를 제공하는 "AD(Administrative Distance)"라는 메트릭이 있습니다. 패킷이 둘 이상의 경로 항목과 일치하는 경우에는 거리가 가장 짧은 항목이 사용됩니다. 직접 연결된 네트워크(인터페이스에서 정의된 네트워크)는 거리가 0이므로 항상 기본적으로 사용됩니다. 고정 경로의 기본 거리는 1이지만 1~254 범위의 원하는 거리를 사용하여 고정 경로를 생성할 수 있습니다.

특정 대상을 식별하는 경로는 기본 경로(대상이 0.0.0.0/0 또는 ::/0인 경로)보다 먼저 적용됩니다.

## 라우팅 테이블을 채우는 방법

FDM 관리 디바이스 라우팅 테이블은 정적으로 정의된 경로 및 직접 연결된 경로로 채워질 수 있습니다. 동일한 경로가 둘 이상의 방식으로 입력될 수 있습니다. 같은 목적지로의 두 경로를 라우팅 테이블에 넣으면 라우팅 테이블에 유지되는 항목은 다음과 같이 결정됩니다.

- 두 경로의 네트워크 접두사 길이(네트워크 마스크)가 다르면 두 경로 모두 고유한 것으로 간주되어 라우팅 테이블에 입력됩니다. 그런 다음 패킷 전달 로직에서 둘 중 어느 것을 사용할지 결정합니다.

예를 들어, 다음 경로가 라우팅 테이블에 입력되어 있다고 가정합니다.

- 192.168.32.0/24
- 192.168.32.0/19

192.168.32.0/24 경로의 네트워크 접두사가 더 길어도 두 경로는 각각의 프리픽스 길이(서브넷 마스크)가 다르기 때문에 라우팅 테이블에 설치됩니다. 이들은 다른 목적지로 간주되며 패킷 전달 로직에서 사용할 경로를 결정합니다.

- 동일한 대상에 대한 여러 경로가 라우팅 테이블에 입력된 경우 고정 경로로 입력된 더 나은 메트릭이 있는 경로가 라우팅 테이블에 입력됩니다.

메트릭은 특정 경로와 연결되는 값이며, 선호도가 가장 높은 것부터 순위를 지정합니다. 메트릭을 결정하는 데 사용되는 매개변수는 라우팅 프로토콜에 따라 다릅니다. 가장 낮은 메트릭을 갖는 경로가 최적의 경로로 선택되고 라우팅 테이블에 설치됩니다. 동일한 목적지의 다중 경로가 메트릭 값이 같을 경우 이 동일 비용 경로에 대한 로드 밸런싱이 수행됩니다.

관련 정보:

- [포워딩 결정 방법](#)

## 포워딩 결정 방법

포워딩 결정은 다음 순서로 이루어집니다.

- NAT 변환(xlates) 및 규칙을 사용하여 이그레스 인터페이스를 결정합니다. NAT 규칙이 이그레스 인터페이스를 결정하지 않는 경우 시스템은 라우팅 테이블을 사용하여 패킷의 경로를 결정합니다.
- 목적지가 라우팅 테이블 내의 항목과 일치하지 않으면 패킷이 기본 경로에 지정된 인터페이스를 통해 포워딩됩니다. 기본 경로가 구성되지 않은 경우 패킷이 폐기됩니다.
- 목적지가 라우팅 테이블의 단일 항목과 일치하는 경우 패킷이 해당 경로와 연결된 인터페이스를 통해 포워딩됩니다.
- 목적지가 라우팅 테이블에 있는 두 개 이상의 항목과 일치하면 패킷은 네트워크 접두사가 더 긴 경로와 연결된 인터페이스를 통해 전달됩니다. 예를 들어 목적지가 192.168.32.1인 패킷은 라우팅 테이블의 다음 경로를 통해 인터페이스에 도착합니다.
  - 192.168.32.0/24 게이트웨이 10.1.1.2
  - 192.168.32.0/19 게이트웨이 10.1.1.3

이 경우 192.168.32.1이 192.168.32.0/24 네트워크 범위에 해당되기 때문에 목적지가 192.168.32.1인 패킷은 10.1.1.2로 전달됩니다. 이 주소는 라우팅 테이블 내 다른 경로에도 포함되지만, 라우팅 테이블의 다른 경로 접두사는 19비트인 데 비해 192.168.32.0/24의 접두사는 24비트이므로 이 경로의 접두사가 상대적으로 길입니다. 패킷을 전달할 때는 항상 더 긴 접두사가 우선합니다.



**Note** 새로운 유사한 연결이 경로 변경으로 인해 다른 동작을 유발하는 경우에도 기존의 연결은 계속해서 설정된 인터페이스를 사용합니다.

## FDM-관리 디바이스에 대한 고정 및 기본 경로 구성

시스템의 인터페이스에 직접 연결되지 않은 네트워크에 바인딩된 패킷을 보낼 위치를 알 수 있도록 FTD(Firepower Threat Defense) 디바이스에 정적 경로를 정의합니다.

기본 경로 생성을 고려하십시오. 이는 네트워크 0.0.0.0/0에 대한 경로입니다. 이 경로는 기존 NAT 변환이나 고정 NAT 규칙 또는 기타 정적 경로를 통해 이그레스 인터페이스를 확인할 수 없는 패킷을 전송할 위치를 정의합니다.


기본 게이트웨이를 사용하여 모든 네트워크에 액세스할 수 없는 경우 다른 고정 경로가 필요할 수 있습니다. 예를 들어 기본 경로는 대개 외부 인터페이스의 업스트림 라우터입니다. 디바이스에 직접 연결되지 않는 추가 내부 네트워크가 있으며 기본 게이트웨이를 통해 해당 네트워크에 액세스할 수 없는 경우에는 이러한 각 내부 네트워크에 대해 고정 경로가 필요합니다.

시스템 인터페이스에 직접 연결된 네트워크에 대해서는 고정 경로를 정의할 수 없습니다. 시스템에서 이러한 경로를 자동으로 생성합니다.

### 절차

#### Procedure

- 단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 디바이스를 클릭하고 고정 경로를 정의할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Routing**(라우팅)을 클릭합니다.
- 단계 5 Static Routing(정적 라우팅) 페이지에서 다음 중 하나를 수행합니다.

- 새로운 고정 경로를 추가하려면 더하기  버튼을 클릭합니다.
- 편집할 경로의 편집 아이콘을 클릭합니다.

경로가 더 이상 필요하지 않은 경우 해당 경로의 휴지통 아이콘을 클릭하여 경로를 삭제합니다.

- 단계 6 경로 속성을 구성합니다.
  - **Protocol**(프로토콜) - 경로가 IPv4 또는 IPv6 주소에 대한 경로인지 선택합니다.
  - **Interface**(인터페이스) — 트래픽을 전송하는 데 사용할 인터페이스를 선택합니다. 이 인터페이스를 통해 게이트웨이 주소에 액세스할 수 있어야 합니다.
  - **Gateway**(게이트웨이) — 대상 네트워크에 대해 게이트웨이의 IP 주소를 식별하는 네트워크 개체를 선택합니다. 트래픽은 이 주소로 전송됩니다.
  - **Metric**(메트릭) - 경로의 AD(Administrative Distance)(1~254)입니다. 기본값은 고정 경로의 경우 1입니다. 인터페이스와 게이트웨이 간에 추가 라우터가 있으면 홉 수를 관리 거리로 입력합니다.



관리 거리는 경로를 비교하는 데 사용되는 파라미터입니다. 값이 작을수록 경로에는 더 높은 우선 순위가 지정됩니다. 연결된 경로(디바이스의 인터페이스에 직접 연결되는 네트워크)가 항상 고정 경로보다 우선적으로 사용됩니다.

- **Destination Network(대상 네트워크)** - 대상 네트워크를 식별하고 이 경로에서 게이트웨이를 사용하는 호스트를 포함하는 네트워크 개체를 선택합니다.

기본 경로를 정의하려면 사전 정의된 **any-ipv4** 또는 **any-ipv6** 네트워크 개체를 사용하거나 **0.0.0.0/0(IPv4)** 또는 **::/0(IPv6)** 네트워크에 대한 개체를 생성합니다.

단계 7 **OK(확인)**를 클릭합니다.

단계 8 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 고정 경로 예시

이 예에서 사용된 주소는 **고정 경로 네트워크 다이어그램**을 참조하십시오.

목표는 대상 네트워크 20.30.1.0/24에서 20.30.1.2의 호스트에 대한 반환 트래픽을 허용하는 고정 경로를 생성하는 것입니다.

패킷은 목적지에 도달하기 위해 모든 경로를 사용할 수 있습니다. 네트워크는 인터페이스에서 패킷을 수신하면 목적지에 가장 적합한 경로에 대한 패킷을 전달할 위치를 결정합니다.



**Note** DMZ는 인터페이스에 직접 연결되어 있으므로 고정 경로가 없습니다.

예를 들어 목적지에 도달하기 위해 다음 두 가지 경로를 고려합니다.

경로 1:

### Procedure

단계 1 패킷은 **20.30.1.2**를 찾는 외부 인터페이스 **209.165.201.0/27**로 다시 돌아옵니다.

단계 2 패킷이 내부 인터페이스를 사용하여 대상과 동일한 네트워크에 있는 게이트웨이 192.168.1.2로 이동하도록 지시합니다.

단계 3 여기에서 해당 네트워크의 게이트웨이 주소 20.30.1.1로 대상 네트워크를 식별합니다.

단계 4 IP 주소 20.30.1.2는 20.30.1.1과 동일한 서브넷에 있습니다. 라우터는 패킷을 스위치로 전달하고, 스위치는 패킷을 20.30.1.2로 전달합니다.

Interface:Inside Destination\_N/W:20.30.1.0/24 Gateway: 192.168.1.2 Metric: 1

## 경로 2:

## Procedure

단계 1 패킷은 **20.30.1.2**를 찾는 외부 인터페이스 **209.165.201.0/27**로 다시 돌아옵니다.

단계 2 패킷이 내부 인터페이스를 사용하여 대상 네트워크에서 여러 홉이 있는 게이트웨이 **192.168.50.20**로 이동하도록 지시합니다.

단계 3 여기에서 해당 네트워크의 게이트웨이 주소 **20.30.1.1**로 대상 네트워크를 식별합니다.

단계 4 IP 주소 **20.30.1.2**는 **20.30.1.0**과 동일한 서브넷에 있습니다. 라우터는 패킷을 스위치로 전달하고, 스위치는 패킷을 **20.30.1.2**로 전달합니다.

Interface:Inside Destination\_N/W:20.30.1.0/24 Gateway: 192.168.50.20 Metric: 100

완료된 Add Static Route(고정 경로 추가) 테이블은 이러한 경로에 대해 다음과 같이 표시합니다.

Interface	IP Type	Destination Networks	Gateway IP	Metric
inside	IPv4	20.30.1.1   20.30.1.1/24	192.168.50.20	1
internal	IPv4	192.168.50.20   192.168.50.20	192.168.50.20	100

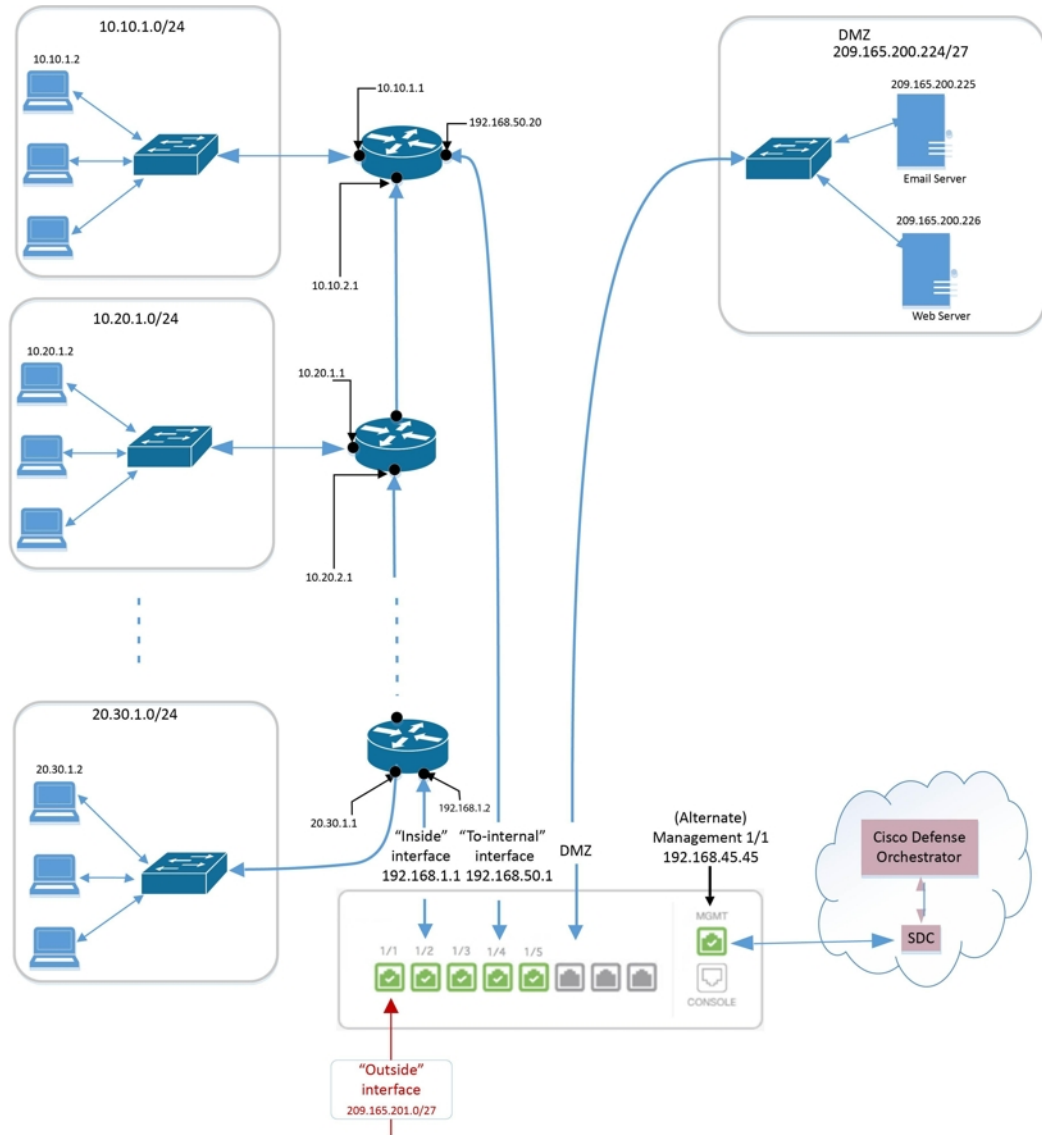
## 라우팅 모니터링

라우팅을 모니터링하고 문제를 해결하려면 디바이스의 **Firewall Device Manager**를 열어 **CLI 콘솔**을 열거나 **SSH**를 사용하여 디바이스 **CLI**에 로그인하고 다음 명령을 사용합니다.

- `show route`는 직접 연결된 네트워크의 경로를 포함하여 데이터 인터페이스에 대한 라우팅 테이블을 표시합니다.
- `show ipv6 route`는 직접 연결된 네트워크의 경로를 포함하여 데이터 인터페이스에 대한 **IPv6** 라우팅 테이블을 표시합니다.
- `show network`는 관리 게이트웨이를 포함하여 가상 관리 인터페이스의 컨피그레이션을 표시합니다. 관리 게이트웨이로 데이터 인터페이스를 지정하는 경우가 아니면 가상 인터페이스를 통한 라우팅은 데이터 인터페이스 라우팅 테이블에 의해 처리되지 않습니다.
- `show network-static-routes`는 `configure network static-routes` 명령을 사용하여 가상 관리 인터페이스에 대해 구성된 정적 경로를 표시합니다. 대부분의 경우에는 관리 라우팅에 관리 게이트웨이만 사용하면 되므로, 일반적으로는 정적 경로가 없습니다. 데이터 인터페이스의 트래픽에는 이러한 경로를 사용할 수 없습니다. 이 명령은 **CLI 콘솔**에서 사용할 수 없습니다.

## 고정 경로 네트워크 다이어그램

**FDM-관리 디바이스**에 대한 고정 및 기본 경로 구성에 대해 논의할 때 다음 네트워크 다이어그램을 참조하십시오.



## 가상 라우팅 및 포워딩 정보

### VRF 정보

VRF(가상 라우팅 및 포워딩)를 사용하면 라우터에 라우팅 테이블의 여러 인스턴스가 존재할 수 있습니다. Firepower 버전 6.6에는 기본 VRF 테이블 및 사용자 생성 VRF 테이블을 포함하는 기능이 도입되었습니다. 단일 VRF 테이블은 EX, OSPF, BGP, IGRP 등 여러 유형의 다양한 라우팅 프로토콜을 처리할 수 있습니다. VRF 테이블 내의 각 라우팅 프로토콜은 항목으로 나열됩니다. 여러 유형의 공통 라우팅 프로토콜을 처리하는 것 외에도 다른 VRF의 인터페이스를 참조하도록 라우팅 프로토콜을 구성할 수 있습니다. 이를 통해 여러 디바이스를 사용하지 않고도 네트워크 경로를 분할할 수 있습니다.

자세한 내용은 [가상 라우터 및 VRF\(가상 라우팅 및 포워딩\) 정보](#)를 참조하십시오.

### Cisco Defense Orchestrator의 VRF

이 기능은 Firepower 버전 6.6의 새로운 기능입니다. FDM 관리 디바이스가 CDO에 온보딩된 경우 디바이스 라우팅 페이지는 FDM 관리 디바이스의 전역 라우터에 정의된 VRF만 읽고 지원합니다. CDO에서 전역 VRF를 보려면 **Inventory**(재고 목록) 페이지에서 디바이스를 선택하고 창 오른쪽에 있는 **Management**(관리) 창에서 **Routing**(라우팅)을 선택합니다. 여기에서 전역 VRF를 보고, 수정하고, 삭제할 수 있습니다. CDO는 FDM에서 구성을 읽을 때 VRF의 이름을 유지합니다.


CDO firewall device manager는 사용자 정의 가상 라우터에 구성된 VRF를 읽지 않습니다. firewall device manager를 통해 VRF 테이블을 생성하고 관리해야 합니다.

전역 및 사용자 정의 경로에 대한 자세한 내용은 [Firepower Device Manager 버전 7.0 이상용 Cisco Firepower Threat Defense 구성 가이드](#)에 나와 있는 "가상 라우터" 장의 "가상 라우터 관리" 섹션을 참조하십시오.




## 개체

개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 단일 개체를 만들고 다른 정책을 사용하고 개체를 편집할 수 있으며 해당 변경 사항은 개체를 사용하는 모든 정책에 전파됩니다. 개체가 없는 경우 동일한 변경이 필요한 모든 정책을 개별적으로 편집해야 합니다.

디바이스를 온보딩하면, CDO는 해당 디바이스에서 사용하는 모든 개체를 인식하고, 저장한 다음, **Objects**(개체) 페이지에 나열합니다. **Objects**(개체) 페이지에서 기존 개체를 편집하고 보안 정책에 사용할 새 개체를 생성할 수 있습니다.

CDO는 여러 디바이스에서 사용되는 개체를 **shared object**(공유 개체)라고 부르고 **Objects**(개체) 페이지에서 이 배지 로 식별합니다.

때때로 공유 개체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디바이스에서 완벽하게 공유되지 않습니다.

- **Duplicate objects**(중복 개체)는 이름은 다르지만 값은 같은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 일반적으로 비슷한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체는 다음 문제 아이콘 로 식별됩니다.
- **Inconsistent objects**(일관성 없는 개체)는 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체입니다. 때로는 사용자가 동일한 이름과 콘텐츠로 다른 구성으로 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라져 불일치가 발생합니다. 일관성 없는 개체는 다음 문제 아이콘 로 식별됩니다.
- 사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다. 사용되지 않는 개체는 다음 문제 아이콘 로 식별됩니다.

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수도 있습니다. 규칙 또는 정책과 연결되지 않은 개체를 생성할 수 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용하는 경우, CDO는 해당 개체의 복사본을 생성하고 해당 복사본을 사용합니다.

**Objects(개체)** 메뉴로 이동하거나 네트워크 정책의 세부 정보에서 확인하여 CDO에 의해 관리되는 개체를 볼 수 있습니다.

CDO은 한 위치에서 지원되는 디바이스 전체에 걸쳐 네트워크 및 서비스 개체를 관리할 수 있습니다. CDO에서는 다음과 같은 방법으로 개체를 관리할 수 있습니다.


- 다양한 기준에 따라 모든 개체를 검색하고 **개체 필터**합니다.
- 디바이스에서 중복되거나, 사용되지 않거나, 일관성이 없는 개체를 찾고 이러한 개체 문제를 통합, 삭제 또는 해결하십시오.
- 연결되지 않은 개체를 찾아 사용하지 않는 경우 삭제합니다.
- 여러 디바이스에서 공통적인 공유 개체를 검색합니다.
- 변경 사항을 커밋하기 전에 일련의 정책 및 디바이스에 대한 개체 변경 사항의 영향을 평가합니다.
- 다양한 정책 및 디바이스와 개체 및 개체의 관계 집합을 비교합니다.
- CDO에 온보딩된 후 디바이스에서 사용 중인 개체를 캡처합니다.

온보딩된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 [문제 해결 Cisco Defense Orchestrator, on page 790](#)를 참조하십시오.



## 개체


개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 단일 개체를 만들고 다른 정책을 사용하고 개체를 편집할 수 있으며 해당 변경 사항은 개체를 사용하는 모든 정책에 전파됩니다. 개체가 없는 경우 동일한 변경이 필요한 모든 정책을 개별적으로 편집해야 합니다.

디바이스를 온보딩하면, CDO는 해당 디바이스에서 사용하는 모든 개체를 인식하고, 저장한 다음, **Objects(개체)** 페이지에 나열합니다. **Objects(개체)** 페이지에서 기존 개체를 편집하고 보안 정책에 사용할 새 개체를 생성할 수 있습니다.

CDO은 여러 디바이스에서 사용되는 개체를 **shared object(공유 개체)**라고 부르고 **Objects(개체)** 페이지에서 이 배지 로 식별합니다.

때때로 공유 개체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디바이스에서 완벽하게 공유되지 않습니다.

- **Duplicate objects(중복 개체)**는 이름은 다르지만 값은 같은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 일반적으로 비슷한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체는 다음 문제 아이콘 로 식별됩니다.
- **Inconsistent objects(일관성 없는 개체)**는 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체입니다. 때로는 사용자가 동일한 이름과 콘텐츠로 다른 구성으로 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라져 불일치가 발생합니다. 일관성 없는 개체는 다음 문제 아이콘 로 식별됩니다.

- 사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다. 사용되지 않는 개체는 다음 문제 아이콘 로 식별됩니다.

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수도 있습니다. 규칙 또는 정책과 연결되지 않은 개체를 생성할 수 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용하는 경우, CDO는 해당 개체의 복사본을 생성하고 해당 복사본을 사용합니다.

**Objects(개체)** 메뉴로 이동하거나 네트워크 정책의 세부 정보에서 확인하여 CDO에 의해 관리되는 개체를 볼 수 있습니다.

CDO은 한 위치에서 지원되는 디바이스 전체에 걸쳐 네트워크 및 서비스 개체를 관리할 수 있습니다. CDO에서는 다음과 같은 방법으로 개체를 관리할 수 있습니다.

- 다양한 기준에 따라 모든 개체를 검색하고 **개체 필터**합니다.
- 디바이스에서 중복되거나, 사용되지 않거나, 일관성이 없는 개체를 찾고 이러한 개체 문제를 통합, 삭제 또는 해결하십시오.
- 연결되지 않은 개체를 찾아 사용하지 않는 경우 삭제합니다.
- 여러 디바이스에서 공통적인 공유 개체를 검색합니다.
- 변경 사항을 커밋하기 전에 일련의 정책 및 디바이스에 대한 개체 변경 사항의 영향을 평가합니다.
- 다양한 정책 및 디바이스와 개체 및 개체의 관계 집합을 비교합니다.
- CDO에 온보딩된 후 디바이스에서 사용 중인 개체를 캡처합니다.

온보딩된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 [문제 해결 Cisco Defense Orchestrator, on page 790](#)를 참조하십시오.

## 개체 유형

다음 표에서는 CDO를 사용하여 디바이스에 대해 생성하고 관리할 수 있는 개체에 대해 설명합니다.

**Table 12: FDM** 관리 디바이스 개체 유형

개체	설명
애플리케이션 필터 개체	애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.

개체	설명
RA VPN AnyConnect 클라이언트 프로파일 업로드	AnyConnect 클라이언트 프로파일 개체는 파일 개체이며 구성(일반적으로 원격 액세스 VPN 정책)에서 사용되는 파일을 나타냅니다. AnyConnect 클라이언트 프로파일 및 AnyConnect 클라이언트 이미지 파일을 포함할 수 있습니다.
인증서 개체	디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.
DNS 그룹 개체	www.example.com과 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인하려면 DNS 서버가 필요합니다. 관리 및 데이터 인터페이스에 대해 서로 다른 DNS 그룹 개체를 구성할 수 있습니다.
Firepower 지리위치 필터 개체 생성 및 편집	지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소를 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.
IKEv1 정책 생성 또는 편집	IKEv1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 매개변수가 포함되어 있습니다.
IKEv2 정책	IKEv2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 매개변수가 포함되어 있습니다.
IKEv1 IPSEC 제안	IPsec 제안 개체는 IKE 1단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.
IKEv2 IPSEC 제안	IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.
네트워크 개체	네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다.

개체	설명
보안 영역 개체	보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다.
서비스 개체	서비스 개체, 서비스 그룹 및 포트 그룹은 TCP/IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다.
SGT 그룹 생성	SGT 동적 개체는 ISE에서 할당된 SGT를 기반으로 소스 또는 대상 주소를 식별하며, 그런 다음 수신 트래픽과 일치시킬 수 있습니다.
시스템 로그 서버 개체	Syslog 서버 개체는 연결 지향형 또는 진단 Syslog(Syslog) 메시지를 수신할 수 있는 서버를 식별합니다.
URL 개체	URL 개체 및 그룹(URL 개체로 총칭함)을 사용하여 웹 요청의 URL 또는 IP 주소를 정의합니다. 이러한 개체를 사용하여 액세스 제어 정책에서 수동 URL 필터링 또는 보안 인텔리전스 정책에서 차단 기능을 구현할 수 있습니다.

## 공유 개체

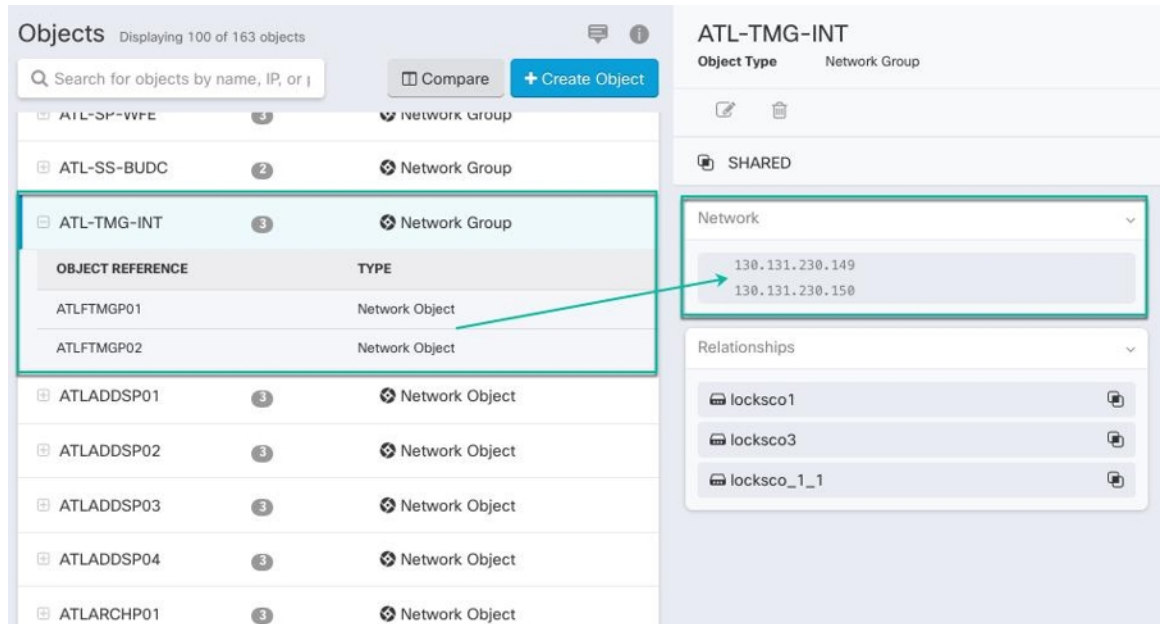
CDO(Cisco Defense Orchestrator)는 이름과 콘텐츠가 동일한 여러 디바이스의 개체인 공유 개체를 호출합니다. 공유 개체는 이 아이콘으로 식별됩니다.



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

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





## 개체 재정의

개체 오버라이드를 사용하면 특정 디바이스에서 공유 네트워크 개체의 값을 오버라이드할 수 있습니다. CDO는 오버라이드를 구성할 때 지정한 디바이스에 해당하는 값을 사용합니다. 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체에 대하여 CDO는 이러한 값이 오버라이드 되기 때문에 **Inconsistent objects**(일관성 없는 개체)로 식별하지 않습니다.

대부분의 디바이스에 대한 정의가 해당하는 개체를 생성하고 다른 정의가 필요한 일부 디바이스의 개체에 대한 특정 변경 사항을 지정하는 오버라이드를 사용할 수 있습니다. 모든 디바이스에 오버라이드가 필요한 개체를 생성할 수도 있습니다. 하지만 이 경우 모든 디바이스에 단일 정책을 생성할 수 있습니다. 개체 오버라이드는 필요한 경우 개별 디바이스의 정책을 바꾸지 않고도 디바이스 전반에 걸쳐 사용이 가능한 작은 공유 정책 집합을 생성하도록 합니다.

예를 들어 각 사무실에 .프린터 서버가 있고, 프린터 서버 개체인 `print-server`를 만든 시나리오를 생각해 보십시오. ACL에는 프린터 서버가 인터넷에 액세스하는 것을 거부하는 규칙이 있습니다. 프린터 서버 개체에는 한 사무실에서 다른 사무실로 변경하려는 기본값이 있습니다. 값이 다를 수 있지만 개체 오버라이드를 사용하고 규칙과 "프린터-서버" 개체를 모든 위치에서 일관되게 유지함으로써 이 작업을 수행할 수 있습니다.

Editing Shared Network Object
✕

Object Name \* Devices 2 Devices Usage 0 Rule Sets

print-server

Description

printer server object

Default Value ▾

eq ▲ 126.0.1.0 ASAv-99-18

Override Values ▾

Enter a value to add it

Value	Devices	
126.0.2.4	Pasadena-ftd-730-516-...	<span style="font-size: small;">✎ ⬆ 🗑</span>
126.0.1.6	BGL_FTD_7.3	<span style="font-size: small;">✎ ⬆ 🗑</span>
126.0.1.9	connected_fmc	<span style="font-size: small;">✎ ⬆ 🗑</span>

Cancel Save



**Note** CDO를 사용하면 규칙 세트의 규칙과 연관된 개체를 오버라이드할 수 있습니다. 규칙에 새 개체를 추가할 때 디바이스를 규칙 세트에 연결하고 변경 사항을 저장한 후에만 오버라이드할 수 있습니다. 자세한 내용은 [디바이스에 대한 규칙 집합 구성](#)을 참조하십시오.



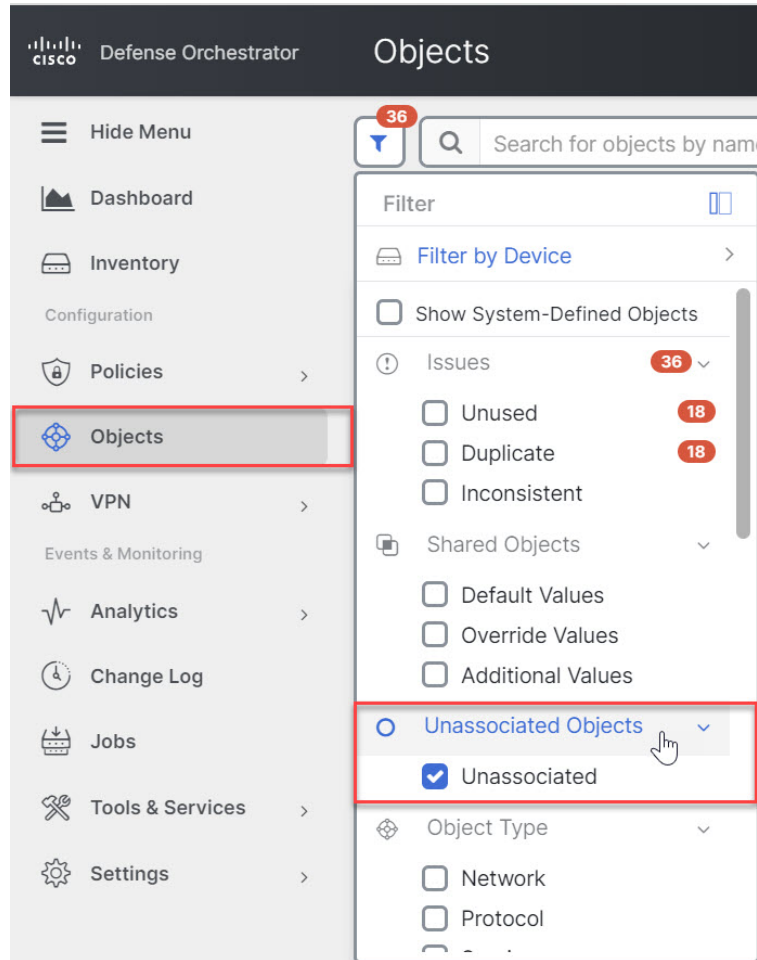
**Note** 일관되지 않은 개체가 있는 경우 오버라이드를 통해 개체를 단일 공유 개체로 결합할 수 있습니다. 자세한 내용은 [불일치 개체 문제 해결, on page 797](#)를 참조하십시오.

## 연결 해제된 개체

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수 있습니다. 규칙이나 정책과 연결되지 않은 개체를 생성할 수도 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용할 때, CDO는 해당 개체의 사본을 생성하고 해당 사본을 사용합니다. 연결되지 않은 원래 개체는 야간 유지 관리 작업에 의해 삭제되거나 사용자가 삭제할 때까지 사용 가능한 개체 목록에 남아 있습니다.

개체와 연결된 규칙 또는 정책이 실수로 삭제된 경우 모든 구성이 손실되지 않도록 연결되지 않은 개체는 사본으로 CDO에 남아 있습니다.

연결되지 않은 개체를 보려면 개체 탭의 왼쪽 창에서 를 클릭하고 **Unassociated** (연결되지 않음) 확인란을 선택합니다.

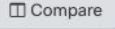


## 개체 비교

### Procedure

단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.

단계 2 페이지에서 개체를 필터링하여 비교하려는 개체를 찾습니다.

단계 3 **Compare**(비교) 버튼  를 클릭합니다.

단계 4 비교할 개체를 최대 3개까지 선택합니다.


단계 5 화면 하단에서 개체를 나란히 봅니다.

- 개체 세부 정보 제목 표시줄에서 위쪽 및 아래쪽 화살표를 클릭하면 개체 세부 정보를 더 많이 또는 더 적게 볼 수 있습니다.
- 세부 정보 및 관계 상자를 확장하거나 축소하여 더 많거나 적은 정보를 확인합니다.

단계 6 (선택 사항) 관계 상자는 개체가 사용되는 방식을 보여줍니다. 디바이스 또는 정책과 연결될 수 있습니다. 개체가 디바이스와 연결된 경우 디바이스 이름을 클릭한 다음 **View Configuration**(구성 보기)을 클릭하여 디바이스 구성을 볼 수 있습니다. CDO는 디바이스의 구성 파일을 표시하고 해당 개체에 대한 항목을 강조 표시합니다.

## 필터

**Inventory**(재고 목록) 및 **Objects**(개체) 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

필터링하려면 **Devices and Services**(디바이스 및 서비스), **Policies**(정책) 및 **Objects**(개체) 탭의 왼쪽 창에서 을 클릭합니다.

**Inventory**(재고 목록) 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.



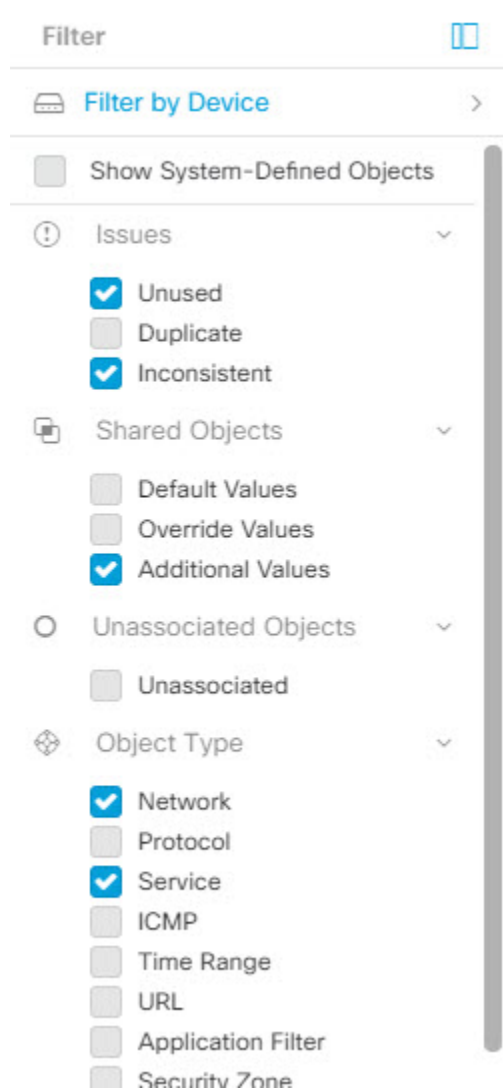
참고 **FTD** 탭이 열리면 필터 창이 CDO에서 디바이스에 액세스하는 데 사용되는 관리 애플리케이션을 기반으로 FDM 관리 디바이스를 표시하는 필터를 제공합니다.

- FDM: FTD API 또는 FDM을 사용하여 관리되는 디바이스.
- FMC-FTD: Firepower Management Center를 사용하여 관리되는 디바이스.
- FTD: FTD 관리를 사용하여 관리되는 디바이스.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(사용되었거나 일관성 없음)" 및 추가 값이 있는 공유 개체 및 네트워크 또는 서비스 유형의 개체 검색에 필터를 적용합니다.



## 개체 필터

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

- **All Objects(모든 개체)** - 이 필터는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 개체를 제공합니다. 이 필터는 모든 개체를 찾아보거나 하위 필터를 검색하거나 추가로 적용하기 위한 시작점으로 유용합니다.
- **Shared Objects(공유 개체)** - 이 빠른 필터는 CDO가 두 개 이상의 디바이스에서 공유하는 것으로 확인한 모든 개체를 표시합니다.
- **Objects By Device(디바이스별 개체)** - 선택한 디바이스에 있는 개체를 볼 수 있도록 특정 디바이스를 선택할 수 있습니다.

하위 필터 - 각 기본 필터에는 선택 범위를 좁히기 위해 적용할 수 있는 하위 필터가 있습니다. 이러한 하위 필터는 네트워크, 서비스, 프로토콜 등의 개체 유형을 기반으로 합니다.

이 필터 표시줄에서 선택한 필터는 다음 기준과 일치하는 개체를 반환합니다.

\* 두 디바이스 중 하나에 있는 개체. (디바이스를 지정하려면 **Filter by Device**(디바이스별 필터링)를 클릭합니다.) AND는

\* 일치하지 않는 개체 AND는

\* 네트워크 개체 또는 서비스 개체 AND

\* 개체 명명 규칙에 "group"이라는 단어가 있습니다.

**Show System Objects**(시스템 개체 표시)를 선택했으므로 결과에 시스템 개체와 사용자 정의 개체가 모두 포함됩니다.

시스템 개체 필터 표시

일부 디바이스는 공통 서비스에 대해 사전 정의된 개체가 함께 제공됩니다. 이러한 시스템 개체는 이미 생성되어 규칙 및 정책에서 사용할 수 있으므로 편리합니다. 개체 테이블에는 여러 시스템 개체가 있을 수 있습니다. 시스템 개체는 편집하거나 삭제할 수 없습니다.


**Show System Objects**(시스템 개체 표시)는 기본적으로 꺼져 있습니다. 개체 테이블에 시스템 개체를 표시하려면 필터 표시줄에서 **Show System Objects**(시스템 개체 표시)를 선택합니다. 개체 테이블에서 시스템 개체를 숨기려면 필터 표시줄에서 **Show System Objects**(시스템 개체 표시)를 선택하지 않은 상태로 둡니다.

시스템 개체를 숨기면 검색 및 필터링 결과에 포함되지 않습니다. 시스템 개체를 표시하면 개체 검색 및 필터링 결과에 포함됩니다.

## 개체 필터 구성

원하는 만큼 기준을 필터링할 수 있습니다. 더 많은 범주를 필터링할수록 예상되는 결과는 줄어듭니다.

### Procedure

- 단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.
- 단계 2 페이지 상단의 필터 아이콘 을 클릭하여 필터 패널을 엽니다. 선택한 필터를 선택 취소하여 실수로 필터링된 개체가 없는지 확인합니다. 또한 검색 필드를 살펴보고 검색 필드에 입력되었을 수 있는 텍스트를 삭제합니다.
- 단계 3 특정 디바이스에 있는 것으로 결과를 제한하려면 다음을 수행합니다.
  - a. **Filter By Device**(디바이스별 필터링)를 클릭합니다.
  - b. 모든 디바이스를 검색하거나 디바이스 탭을 클릭하여 특정 종류의 디바이스만 검색합니다.
  - c. 필터 기준에 포함할 디바이스를 선택합니다.
  - d. **OK**(확인)를 클릭합니다.
- 단계 4 검색 결과에 시스템 개체를 포함하려면 **Show System Objects**(시스템 개체 표시)를 선택합니다. 검색 결과에서 시스템 개체를 제외하려면 **Show System Objects**(시스템 개체 표시)의 선택을 취소합니다.

- 단계 5 필터링할 개체 **Issues**(문제)를 선택합니다. 두 개 이상의 문제를 선택하면 선택한 범주의 개체가 필터 결과에 포함됩니다.
- 단계 6 문제가 있었지만 관리자가 무시한 개체를 확인하려면 **Ignored**(무시됨) 문제를 선택합니다.
- 단계 7 두 개 이상의 디바이스 간에 공유되는 개체를 필터링하는 경우 **Shared Objects**(공유 개체)에서 필수 필터를 선택합니다.
- **Default Values**(기본값): 기본값만 있는 개체를 필터링합니다.
  - **Override Values**(값 재정의): 오버라이드된 값이 있는 개체를 필터링합니다.
  - **Additional Values**(추가 값): 추가 값이 있는 개체를 필터링합니다.
- 단계 8 규칙 또는 정책의 일부가 아닌 개체를 필터링하는 경우 **Unassociated**(연결되지 않음)를 선택합니다.
- 단계 9 필터링할 개체 유형을 선택합니다.
- 단계 10 **Objects**(개체) 검색 필드에 개체 이름, IP 주소 또는 포트 번호를 추가하여 필터링된 결과 중에서 검색 기준으로 개체를 찾을 수도 있습니다.

#### 필터 기준에서 디바이스를 제외해야 하는 경우

필터링 기준에 디바이스를 추가하면 결과에 디바이스의 개체가 표시되지만 해당 개체와 다른 디바이스의 관계는 표시되지 않습니다. 예를 들어 **ObjectA**가 ASA1과 ASA2 간에 공유된다고 가정합니다. ASA1에서 공유 개체를 찾기 위해 개체를 필터링하는 경우 **ObjectA**를 찾을 수 있지만 **Relationships**(관계) 창에는 해당 개체가 ASA1에 있다는 것만 표시됩니다.

개체와 관련된 모든 디바이스를 보려면 검색 기준에 디바이스를 지정하지 마십시오. 다른 기준으로 필터링하고 원하는 경우 검색 기준을 추가하십시오. CDO가 식별하는 개체를 선택한 다음 관계 창을 살펴봅니다. 개체와 관련된 모든 디바이스 및 정책이 표시됩니다.

#### 개체 무시

사용되지 않거나 중복되거나 일관성이 없는 개체를 해결하는 한 가지 방법은 해당 개체를 무시하는 것입니다. **사용되지 않은 개체 문제 해결 중복 개체 문제 해결 불일치 개체 문제 해결** 해당 상태에 대한 타당한 이유가 있다고 판단하고 개체 문제를 해결되지 않은 상태로 두도록 선택할 수 있습니다. 나중에 무시된 개체를 해결해야 할 수도 있습니다. CDO는 개체 문제를 검색할 때 무시된 개체를 표시하지 않으므로 무시된 개체에 대한 개체 목록을 필터링한 다음 결과에 따라 조치를 취해야 합니다.

#### Procedure

- 단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.
- 단계 2 **개체 필터**
- 단계 3 **Object**(개체) 테이블에서 무시를 취소할 개체를 선택합니다. 한 번에 하나의 개체를 무시 취소할 수 있습니다.
- 단계 4 세부 정보 창에서 **Unignore**(무시)를 클릭합니다.

단계 5 요청을 확인합니다. 이제 문제별로 개체를 필터링하면 이전에 무시되었던 개체를 찾아야 합니다.

## 개체 삭제

단일 개체 또는 여러 개체를 삭제할 수 있습니다.

### 단일 개체 삭제



#### Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

#### Procedure

단계 1 왼쪽의 CDO 탐색 모음에서 **Objects(개체)**를 선택하고 옵션을 선택합니다.

단계 2 개체 필터와 검색 필드를 사용하여 삭제하려는 개체를 찾아 선택합니다.

단계 3 **Relationships(관계)** 창을 검토합니다. 개체가 정책 또는 개체 그룹에서 사용되는 경우 해당 정책 또는 그룹에서 개체를 제거할 때까지 개체를 삭제할 수 없습니다.

단계 4 작업 창에서 **Remove(제거)** 아이콘 를 클릭합니다.

단계 5 **OK(확인)**을 클릭하여 개체 삭제를 확인합니다.

단계 6 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

### 사용되지 않는 개체 그룹 삭제


디바이스를 온보딩하고 개체 문제를 해결하기 시작하면 사용하지 않는 개체를 많이 찾습니다. 한 번에 최대 50개의 사용하지 않는 개체를 삭제할 수 있습니다.

#### 프로시저

단계 1 **Issues(문제)** 필터를 사용하여 미사용 개체를 찾습니다. 디바이스 필터를 사용하여 디바이스 없음을 선택하여 디바이스와 연결되지 않은 개체를 찾을 수도 있습니다. 개체 목록을 필터링하면 개체 확인란이 나타납니다.

단계 2 개체 테이블 머리글에서 **Select all(모두 선택)** 확인란을 선택하여 개체 테이블에 나타나는 필터에 의해 발견된 모든 개체를 선택합니다. 또는 삭제할 개별 개체에 대한 개별 확인란을 선택합니다.



단계 3 작업 창에서 **Remove**(제거) 아이콘 를 클릭합니다.

단계 4 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 네트워크 개체

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 그룹은 그룹에 추가하는 네트워크 개체 및 기타 개별 주소 또는 서브 네트워크의 모음입니다. 네트워크 개체 및 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.

**Table 13:** 네트워크 개체의 허용되는 값

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

**Table 14:** 네트워크 그룹의 허용되는 콘텐츠

디바이스 유형	IP 값	네트워크 개체	네트워크 그룹
FTD	아니요	예	예

### 제품 간 네트워크 개체 재사용

클라우드 사용 Firewall Management Center가 포함된 Cisco Defense Orchestrator 테넌트가 있는 경우:

Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체 또는 그룹을 생성하면 클라우드 사용 Firewall Management Center를 구성할 때 사용되는 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 개체 목록에도 개체의 복사본이 추가되며, 그 반대의 경우도 마찬가지입니다.

한 페이지에서 네트워크 개체 또는 그룹에 대한 변경 사항은 두 페이지의 개체 또는 그룹 인스턴스에 적용됩니다. 한 페이지에서 개체를 삭제하면 다른 페이지에서도 개체의 해당 복사본이 삭제됩니다.

예외:

- 클라우드 사용 Firewall Management Center에 대해 동일한 이름의 네트워크 개체가 이미 있는 경우 Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체는 Cisco Defense Orchestrator의 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에서 복제되지 않습니다.

- 온프레미스 Secure Firewall Management Center에서 관리하는 온보딩된 위협 방어 디바이스의 네트워크 개체 및 그룹은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 복제되지 않으며, 클라우드 사용 Firewall Management Center에서 사용할 수 없습니다.

클라우드 사용 Firewall Management Center로 마이그레이션된 온프레미스 Secure Firewall Management Center 인스턴스의 경우, 네트워크 개체 및 그룹이 FTD 디바이스에 구축된 정책에서 사용되었다면 네트워크 개체 및 그룹이 CDO 개체 페이지에 복제됩니다.

- CDO와 클라우드 사용 Firewall Management Center 간에 네트워크 개체 공유는 새로운 테넌트에서 자동으로 활성화되지만 기존 테넌트에 대해서는 요청해야 합니다. 네트워크 개체를 클라우드 사용 Firewall Management Center와 공유하지 않는 경우 [CDO 고객이 TAC로 지원 티켓을 여는 방법](#)하여 테넌트에서 기능을 활성화하십시오.

### 네트워크 개체 보기

CDO를 사용하여 생성한 네트워크 개체와 온보딩된 디바이스 구성에서 인식되는 CDO가 Objects(개체) 페이지에 표시됩니다. 개체 유형으로 레이블이 지정됩니다. 이렇게 하면 개체 유형으로 필터링하여 원하는 개체를 빠르게 찾을 수 있습니다.

Objects(개체) 페이지에서 네트워크 개체를 선택하면 Details(세부 정보) 창에 개체의 값이 표시됩니다. Relationships(관계) 창에는 개체가 정책에서 사용되는지 여부와 개체가 저장된 디바이스가 표시됩니다.

네트워크 그룹을 클릭하면 해당 그룹의 콘텐츠가 표시됩니다. 네트워크 그룹은 네트워크 개체에 의해 제공되는 모든 값의 복합물입니다.

관련 정보:

- [Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집](#)

## Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집

**Firepower** 네트워크 개체는 CIDR 표기법으로 표시된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에 사용되는 네트워크 개체 및 네트워크 그룹의 복합 그룹입니다. Cisco Defense Orchestrator(CDO)를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

Firepower 네트워크 개체 및 그룹은 ASA, 위협 방어, FDM 관리 및 Meraki 디바이스에서 사용할 수 있습니다. [제품 간 네트워크 개체 재사용, on page 130](#)을 참조하십시오.



**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.



**Caution**

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

**Table 15:** 네트워크 개체에 추가할 수 있는 IP 주소

디바이스 유형	IPv4 / IPv6	단일 주소	주소 범위	PQDN(Partially Qualified Domain Name)	CIDR 표기법의 서브넷
Firepower	IPv4 / IPv6	예	예	예	예

관련 정보:

- [Firepower 네트워크 개체 생성, on page 132](#)
- [Firepower 네트워크 개체 편집, on page 134](#)
- [공유 네트워크 그룹에 값 추가, on page 137](#)
- [공유 네트워크 그룹의 추가 값 편집, on page 139](#)

**Firepower** 네트워크 개체 생성




**Note**

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

**Procedure**

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.
- 단계 3 **FTD > Network(네트워크)**를 클릭합니다.
- 단계 4 개체 이름을 입력합니다.
- 단계 5 **Create a network object(네트워크 개체 생성)**를 선택합니다.
- 단계 6 **Value(값)** 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소, CIDR 표기법으로 표시된 서브넷 주소 또는 PQDN(Partially Qualified Domain Name)을 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다.

**Note** 호스트 비트 값을 설정하지 마십시오. 0이 아닌 호스트 비트 값을 입력하면 클라우드 사용 Firewall Management Center에서 호스트 비트가 설정되지 않은 IPv6 개체만 허용하므로 CDO가 개체를 생성하는 동안 이 값을 설정 해제합니다.

단계 7 **Add**(추가)를 클릭합니다.

주의: 새로 생성된 네트워크 개체는 규칙 또는 정책의 일부가 아니므로 FDM 관리 디바이스와 연결되지 않습니다. 이러한 개체를 보려면 개체 필터에서 **Unassociated**(연결되지 않음) 개체 범주를 선택합니다. 자세한 내용은 **개체 필터 구성**를 참고하십시오. 디바이스의 규칙 또는 정책에서 연결되지 않은 개체를 사용하면 이러한 개체는 해당 디바이스와 연결됩니다.

## Firepower 네트워크 그룹 생성


네트워크 그룹은 네트워크 개체와 네트워크 그룹을 포함할 수 있습니다. 새 네트워크 그룹을 만들 때 이름, IP 주소, IP 주소 범위 또는 FQDN으로 기존 개체를 검색하고 네트워크 그룹에 추가할 수 있습니다. 개체가 없는 경우 동일한 인터페이스에서 해당 개체를 즉시 생성하고 네트워크 그룹에 추가할 수 있습니다.



**Note** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

## Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.
- 단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.
- 단계 3 **FTD** > **Network**(네트워크)를 클릭합니다.
- 단계 4 개체 이름을 입력합니다.
- 단계 5 **Create a network group**(네트워크 그룹 생성)을 선택합니다.
- 단계 6 값 필드에 값이나 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.
- 단계 7 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 8 CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(추가)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 9 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(이 이름의 새 개체로 추가)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(새 개체로 추가)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

참고: 편집 아이콘을 클릭하여 세부 정보를 편집할 수 있습니다. 삭제 버튼을 클릭해도 개체 자체는 삭제되지 않습니다. 대신 네트워크 그룹에서 제거됩니다.

단계 10 필요한 개체를 추가한 후 **Save(저장)**을 클릭하여 새 네트워크 그룹을 생성합니다.

단계 11 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.**

## Firepower 네트워크 개체 편집



### Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 네트워크 개체를 선택하고 **Actions(작업)** 창에서 편집 아이콘  을 클릭합니다.

단계 4 "Firepower 네트워크 그룹 생성"에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 편집합니다.

**Note** 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save(저장)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.



단계 6 **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

## Firepower 네트워크 그룹 편집



**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:  
또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.  
한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

**Procedure**

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 네트워크 그룹을 찾습니다.
- 단계 3 SGT 그룹을 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.
- 단계 4 필요한 경우 개체 이름과 설명을 변경합니다.
- 단계 5 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.
- a. 개체 이름 또는 네트워크 그룹 옆에 나타나는 편집 아이콘  을 클릭하여 편집합니다.
  - b. 확인 표시를 클릭하여 변경 사항을 저장합니다. 참고: 네트워크 그룹에서 값을 제거하려면 삭제 아이콘을 클릭합니다.
- 단계 6 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.
- a. **Values(값)** 필드에 새 값이나 기존 네트워크 개체의 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다. 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.
  - b. CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(추가)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.
  - c. 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.
    - 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(이 이름의 새 개체로 추가)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
    - 새 개체를 생성하려면 **Add as New Object(새 개체로 추가)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.
- 단계 7 **Save(저장)**를 클릭합니다. CDO에 변경의 영향을 받을 정책이 표시됩니다.

단계 8 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 9 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

## 개체 오버라이드 추가



주의 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

## 프로시저

단계 1 왼쪽 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 오버라이드를 추가할 개체를 찾습니다.

단계 3 네트워크 개체를 선택하고 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.

단계 4 **Override Values**(오버라이드 값) 대화 상자에 값을 입력하고 + **Add Value**(+ 값 추가)를 클릭합니다.

중요 추가하려는 오버라이드에는 개체에 포함된 것과 동일한 유형의 값이 있어야 합니다. 예를 들어 네트워크 개체에 대해 호스트 값이 아닌 네트워크 값으로만 오버라이드를 구성할 수 있습니다.

단계 5 값이 추가된 것을 확인하면, 오버라이드 값에서 **Devices**(디바이스) 열의 셀을 클릭합니다.

단계 6 **Add Devices**(디바이스 추가)를 클릭하고 오버라이드를 추가할 디바이스를 선택합니다. 선택한 디바이스에는 오버라이드를 추가할 개체가 포함되어 있어야 합니다.

단계 7 **Save**(저장)를 클릭합니다. CDO는 변경의 영향을 받는 디바이스를 표시합니다.

단계 8 **Confirm**(확인)을 클릭하여 개체 및 개체의 영향을 받는 모든 디바이스에 대한 오버라이드 추가를 완료합니다.



참고 개체에 두 개 이상의 오버라이드를 추가할 수 있습니다. 그러나 오버라이드를 추가할 때마다 개체가 포함된 다른 디바이스를 선택해야 합니다.

단계 9 개체 오버라이드에 대해 자세히 알아보고 **개체 오버라이드 편집**, 137 페이지가 기존 오버라이드를 편집하려면 **개체 재정의**, 122 페이지를 참조하십시오.

## 개체 오버라이드 편집

개체가 디바이스에 있는 한 기존 오버라이드 값을 편집할 수 있습니다.

## Procedure

- 단계 1 왼쪽 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 오버라이드가 있는 개체를 찾습니다.
- 단계 3 오버라이드가 있는 개체를 선택하고 작업 창에서 편집 아이콘  를 클릭합니다.
- 단계 4 오버라이드 값을 편집합니다.
- 값을 편집하려면 편집 아이콘을 클릭합니다.
  - **Override Values(오버라이드 값)**의 **Devices(디바이스)** 열에 있는 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides(오버라이드 제거)**를 클릭하여 해당 디바이스에서 오버라이드를 제거할 수 있습니다.
  - **Override Values(오버라이드 값)**에서  화살표를 클릭하여 푸시하고 공유 개체의 기본값으로 생성합니다.
  - 제거하려는 오버라이드 옆에 있는 삭제 아이콘을 클릭합니다.
- 단계 5 **Save(저장)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.
- 단계 6 **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.
- 단계 7 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).

## 공유 네트워크 그룹에 값 추가

연결된 모든 디바이스에 있는 공유 네트워크 그룹의 값을 "기본값"이라고 합니다. CDO를 사용하면 공유 네트워크 그룹에 "추가 값"을 추가하고 해당 공유 네트워크 그룹과 연결된 일부 디바이스에 해당 값을 할당할 수 있습니다. CDO는 변경 사항을 디바이스에 구축할 때 콘텐츠를 확인하고 공유 네트워크 그룹과 연결된 모든 디바이스에 "기본값"을 푸시하고 지정된 디바이스에만 "추가 값"을 푸시합니다.

모든 사이트에서 액세스할 수 있어야 하는 본사에 4개의 AD 기본 서버가 있는 시나리오를 예로 들어 보겠습니다. 따라서 모든 사이트에서 사용할 "Active-Directory"라는 개체 그룹을 생성했습니다. 이제 지사 중 하나에 두 개의 AD 서버를 추가하려고 합니다. 개체 그룹 "Active-Directory"에서 해당 지사에 특정한 추가 값으로 세부 정보를 추가하여 이 작업을 수행할 수 있습니다. 이 두 서버는 "Active-Directory" 개체가 일관성이 있는지 또는 공유되는지를 확인하는 데 참여하지 않습니다. 따라서 모든 사이트에서 4개의 AD 기본 서버에 액세스할 수 있지만 지사(2개의 추가 서버 포함)는 2개의 AD 서버와 4개의 AD 기본 서버에 액세스할 수 있습니다.



**Note** 일치하지 않는 공유 네트워크 그룹이 있는 경우 추가 값을 사용하여 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 자세한 내용은 [불일치 개체 문제 해결, on page 797](#)를 참조하십시오.



**Caution**

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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

**Procedure**

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 공유 네트워크 그룹을 찾습니다.

단계 3 **Actions(작업)** 창에서 편집 아이콘  을 클릭합니다.

- **Devices(디바이스)** 필드에는 공유 네트워크 그룹이 있는 디바이스가 표시됩니다.
- **Usage(사용)** 필드에는 공유 네트워크 그룹과 연결된 규칙 집합이 표시됩니다.
- **Default Values(기본값)** 필드는 생성 중에 제공된 공유 네트워크 그룹과 연결된 기본 네트워크 개체 및 해당 값을 지정합니다. 이 필드 옆에서 이 기본값이 포함된 디바이스의 수를 볼 수 있으며, 클릭하여 해당 이름 및 디바이스 유형을 볼 수 있습니다. 이 값과 연결된 규칙 집합도 확인할 수 있습니다.

단계 4 **Additional Values(추가 값)** 필드에 값 또는 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.

단계 5 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 6 CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(추가)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 7 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(이 이름의 새 개체로 추가)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(새 개체로 추가)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 8 **Devices(디바이스)** 열에서 새로 추가된 개체와 연결된 셀을 클릭하고 **Add Devices(디바이스 추가)**를 클릭합니다.

단계 9 원하는 디바이스를 선택하고 **OK(확인)**를 클릭합니다.

단계 10 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 11 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 12 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

## 공유 네트워크 그룹의 추가 값 편집



**Caution** 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

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



## Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 오버라이드가 있는 개체를 찾습니다.

단계 3 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.

단계 4 오버라이드 값을 편집합니다.

- 값을 편집하려면 편집 아이콘을 클릭합니다.
- **Devices**(디바이스) 열의 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides**(오버라이드 제거)를 클릭하여 해당 디바이스에서 오버라이드를 제거할 수 있습니다.
- **Default Values**(기본값)의  화살표를 클릭하여 푸시하고 공유 네트워크 그룹의 추가 값으로 설정합니다. 공유 네트워크 그룹과 연결된 모든 디바이스가 자동으로 할당됩니다.
- **Override Values**(값 재정의)에서  화살표를 클릭하여 공유 네트워크 그룹의 기본 개체로 푸시하고 설정합니다.
- 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 7 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

## 네트워크 개체 및 그룹 삭제

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지에서 네트워크 개체나 그룹을 삭제하면 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며, 그 반대의 경우도 마찬가지입니다.

## 애플리케이션 필터 개체

애플리케이션 필터 개체는 Firepower 디바이스에서 사용됩니다. 애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.

개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

애플리케이션 필터 개체를 사용하지 않고 정책에서 애플리케이션과 애플리케이션 필터를 직접 선택할 수 있습니다. 그러나 애플리케이션 또는 필터의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다. 시스템에는 수정하거나 삭제할 수 없는 사전 정의된 여러 애플리케이션 필터가 포함되어 있습니다.



**Note** Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.



**Note** FDM 관리 FTD 디바이스가 CDO에 온보딩되면 액세스 규칙 또는 SSL 암호 해독에 정의된 규칙을 변경하지 않고 애플리케이션 필터를 애플리케이션 필터 개체로 변환합니다. 구성 변경으로 인해 디바이스의 구성 상태가 '동기화되지 않음'으로 변경되며 CDO에서 구성 구축이 필요합니다. 일반적으로 FDM은 필터를 수동으로 저장할 때까지 애플리케이션 필터를 애플리케이션 필터 개체로 변환하지 않습니다.

관련 정보:

- [Firepower 애플리케이션 필터 개체 생성 및 편집](#)
- [개체 삭제](#)

## Firepower 애플리케이션 필터 개체 생성 및 편집

애플리케이션 필터 개체를 사용하면 직접 선택한 애플리케이션 또는 필터로 식별된 애플리케이션 그룹을 대상으로 지정할 수 있습니다. 이 애플리케이션 필터 개체는 정책에서 사용할 수 있습니다.

## Firepower 애플리케이션 필터 개체 생성

애플리케이션 필터 개체를 만들려면 다음 절차를 따르십시오.

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 **Create Object(개체 생성) > FTD > Application Service(애플리케이션 서비스)**를 클릭합니다.

단계 3 개체의 개체 이름 및 설명(선택 사항)을 입력합니다.

단계 4 **Add Filter(필터 추가)**를 클릭하고 개체에 추가할 애플리케이션 및 필터를 선택합니다.

초기 목록(계속 스크롤 가능)에는 애플리케이션이 표시됩니다. 고급 필터를 클릭하면 필터 옵션을 확인하고 애플리케이션을 더 쉽게 선택할 수 있는 보기를 표시할 수 있습니다. 원하는 항목을 선택한 후 **Add(추가)**를 클릭합니다. 이 프로세스를 반복하여 애플리케이션이나 필터를 더 추가할 수 있습니다.

**Note** 단일 필터 기준으로 여러 선택 항목이 OR 관계를 갖습니다. 예를 들어 위험은 높음 OR 매우 높음입니다. 반면 필터 간의 관계는 AND입니다. 즉, 위험은 높음 OR 매우 높음 AND 사업 타당성은 낮음 OR 매우 낮음과 같습니다. 필터를 선택하면 디스플레이의 애플리케이션 목록이 업데이트되어 기준을 충족하는 애플리케이션만 표시됩니다. 이러한 필터를 사용하여 개별적으로 추가하려는 애플리케이션을 찾거나, 규칙에 추가할 적절한 필터를 선택하고 있는지를 확인할 수 있습니다.

Filter Applications

Risks: High \* Very High \*

Categories: ad portal \*

Business Relevance: Very Low \* Low \*

Tags: displays ads \* |

Types: Web Application \*

Filter the list of applications

4 matches

Application Name	Description
MyWay	Adware and spyware, categorized as an internet browser hijacker.
Olx.pl	Platform to connect local people to buy, sell or exchange used goods and services through their mobile phone or on the web.
PopAds	Advertising network specialized in popunders on the Internet.
PopCash	Advertising platform.

Cancel OK

**위험:** 애플리케이션이 조직의 보안 정책에 위배되는 목적으로 사용될 가능성은 매우 낮음에서 매우 높음까지입니다.

**비즈니스 관련성:** 애플리케이션이 오락용이 아니라 조직의 비즈니스 운영 컨텍스트 내에서 사용될 가능성은 매우 낮음에서 매우 높음까지입니다.

**유형:** 애플리케이션 유형

- **애플리케이션 프로토콜:** 호스트 간의 통신을 나타내는 HTTP 및 SSH와 같은 애플리케이션 프로토콜.
- **클라이언트 프로토콜:** 호스트에서 실행 중인 소프트웨어를 나타내는 웹 브라우저 및 이메일 클라이언트와 같은 클라이언트.
- **웹 애플리케이션:** HTTP 트래픽에 대한 콘텐츠 또는 요청된 URL을 나타내는 MPEG 비디오 및 Facebook과 같은 웹 애플리케이션.

**범주:** 가장 필수적인 기능을 설명하는 애플리케이션의 일반적인 분류.

**태그:** 카테고리화 유사한 애플리케이션에 대한 추가 정보.

암호화된 트래픽의 경우, 시스템은 SSL Protocol(SSL 프로토콜) 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 또한 암호화된 트래픽 또는 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에는 암호 해독된 트래픽 태그가 할당됩니다.

애플리케이션 목록(디스플레이 하단): 목록 위의 옵션에서 필터를 선택하면 이 목록이 업데이트되며 현재 필터와 일치하는 애플리케이션을 볼 수 있습니다. 이 목록을 사용하여 규칙에 필터 기준을 추가하려는 경우 필터가 적절한 애플리케이션을 대상으로 하는지를 확인할 수 있습니다. 개체에 특정 애플리케이션을 추가하려면 필터링된 목록에서 선택합니다. 애플리케이션을 선택하면 필터가 더 이상 적용되지 않습니다. 필터 자체가 개체가 되도록 하려면 목록에서 애플리케이션을 선택하지 마십시오. 그런 다음 개체는 필터로 식별된 모든 애플리케이션을 나타냅니다.

단계 5 **OK(확인)**를 클릭하여 변경 사항을 저장합니다.


## Firepower 애플리케이션 필터 개체 편집

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 편집할 개체를 선택합니다.

단계 4 세부정보 패널의 Actions(작업) 창에서 편집 아이콘  를 클릭합니다.

단계 5 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 6 **Save(저장)**를 클릭합니다.

단계 7 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

#### 관련 정보:

- [개체](#)
- [개체 필터](#)
- [개체 삭제](#)

## 지리위치 개체

지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소를 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

일반적으로는 지리위치 개체를 사용하지 않고 정책에서 직접 지리적 위치를 선택합니다. 그러나 국가와 대륙의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다.

지리위치 데이터베이스 업데이트

최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다. 현재는 Cisco Defense Orchestrator를 사용하여 수행할 수 있는 작업이 아닙니다. GeoDB 및 업데이트 방법에 대한 자세한 내용은 [디바이스가 실행 중인 버전의 Firepower Device Manager용 Cisco Firepower Threat Defense 설정 가이드](#)의 다음 섹션을 참조하십시오.

- 시스템 데이터베이스 및 피드 업데이트
- 시스템 데이터베이스 업데이트

## Firepower 지리위치 필터 개체 생성 및 편집

개체 페이지에서 또는 보안 정책을 생성할 때 지리위치 개체를 생성할 수 있습니다. 이 절차에서는 개체 페이지에서 지리위치 개체를 생성합니다.

지리위치 개체를 생성하려면 다음 단계를 수행합니다.

### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 **Create Object(개체 생성) > FTD > Geolocation(지리위치)**을 클릭합니다.
- 단계 3 개체의 개체 이름 및 설명(선택 사항)을 입력합니다.
- 단계 4 필터 표시줄에서 국가 또는 지역의 이름을 입력하기 시작하면 가능한 일치 목록이 표시됩니다.
- 단계 5 개체에 추가할 국가 또는 지역을 선택합니다.
- 단계 6 **Add(추가)**를 클릭합니다.

### 지리위치 개체 편집

### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 필터 창과 검색 필드를 사용하여 개체를 찾습니다.
- 단계 3 작업 창에서 **Edit(편집)**를 클릭합니다.
- 단계 4 개체의 이름을 변경하고 개체에 국가 및 지역을 추가하거나 제거할 수 있습니다.
- 단계 5 **Save(저장)**를 클릭합니다.
- 단계 6 장치가 영향을 받는 경우 알림을 받게 됩니다. **OK(확인)**를 클릭합니다.

단계 7 장치 또는 정책이 영향을 받은 경우 **Inventory**(인벤토리) 페이지를 열고 장치에 대한 변경 사항을 미리 보고 배포합니다.

## DNS 그룹 개체


DNS(Domain Name System) 그룹은 DNS 서버 및 일부 관련 특성의 목록을 정의합니다. `www.example.com` 과 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인하려면 DNS 서버가 필요합니다. 관리 및 데이터 인터페이스에 대해 서로 다른 DNS 그룹 개체를 구성할 수 있습니다.

새 DNS 그룹 개체를 생성하기 전에 FDM 관리 디바이스에 DNS 서버가 구성되어 있어야 합니다. Cisco Defense Orchestrator(CDO)의 [DNS 서버 구성](#)에 DNS 서버를 추가하거나 firewall device manager에서 DNS 서버를 생성한 다음 FDM 관리 구성을 CDO에 동기화할 수 있습니다. firewall device manager에서 DNS 서버 설정을 생성하거나 수정하려면 [Cisco Firepower Device Manager 구성 가이드](#), 버전 6.4 이상의 데이터 및 관리 인터페이스에 대한 **DNS** 구성을 참조하십시오.

## DNS 그룹 개체 생성

CDO에서 새 DNS 그룹 개체를 생성하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.
  - 단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.
  - 단계 3 **FTD** > **DNS Group**(DNS 그룹)를 클릭합니다.
  - 단계 4 개체 이름을 입력합니다.
  - 단계 5 (선택 사항) 설명을 추가합니다.
  - 단계 6 **DNS** 서버의 IP 주소를 입력합니다. 최대 6개의 DNS 서버를 추가할 수 있습니다. **Add DNS Server**(DNS 서버 추가)를 클릭합니다. 서버 주소를 제거하려면 삭제 아이콘을 클릭합니다.
- Note** 목록은 우선순위에 따라 나열됩니다. 목록의 첫 번째 서버가 항상 사용되며, 그다음 서버는 위에 있는 서버에서 응답이 수신되지 않는 경우에만 사용됩니다. 최대 6개의 서버를 추가할 수 있지만 나열된 처음 3개의 서버만 관리 인터페이스에 사용됩니다.
- 단계 7 도메인 검색 이름을 입력합니다. 이 도메인은 정규화되지 않은 호스트 이름(예: `serverA.example.com` 이 아닌 `serverA`)에 추가됩니다.
  - 단계 8 재시도 횟수를 입력합니다. 시스템이 응답을 받지 못한 경우 DNS 서버 목록을 재시도하는 횟수(0~10)입니다. 기본값은 2입니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.
  - 단계 9 시간 초과 값을 입력합니다. 다음 DNS 서버를 시도하기 전에 기다리는 시간(1~30초)입니다. 기본값은 2초입니다. 시스템이 서버 목록을 재시도할 때마다 이 시간 초과 값이 두 배로 늘어납니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.



단계 10 **Add(추가)**를 클릭합니다.


## DNS 그룹 개체 편집

Cisco Defense Orchestrator 또는 firewall device manager에서 생성된 DNS 그룹 개체를 편집할 수 있습니다. 기존 DNS 그룹 개체를 편집하려면 다음 절차를 따르십시오.

### Procedure

단계 1 왼쪽 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 **DNS Group Object(DNS 그룹 개체)**를 찾습니다.

단계 3 개체를 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 다음 항목을 편집합니다.

- 개체 이름
- 설명
- DNS 서버 이 목록에서 DNS 서버를 편집, 추가 또는 제거할 수 있습니다.
- 도메인 검색 이름
- 재시도.
- 시간이 초과되었습니다.

단계 5 **Save(저장)**를 클릭합니다.

단계 6 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).


## DNS 그룹 개체 삭제

CDO에서 DNS 그룹 개체를 삭제하려면 다음 절차를 따르십시오.

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 **DNS Group Object(DNS 그룹 개체)**를 찾습니다.

단계 3 개체를 선택하고 **Remove(제거)** 아이콘  를 클릭합니다.

단계 4 DNS 그룹 개체를 삭제할 것인지 확인하고 **Ok(확인)**를 클릭합니다.

단계 5 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).

## DNS 그룹 개체를 FDM-관리 DNS 서버로 추가

데이터 인터페이스 또는 관리 인터페이스에 대한 기본 설정 DNS 그룹으로 DNS 그룹 개체를 추가할 수 있습니다. 자세한 내용은 [FDM-관리 디바이스 설정](#)을 참조하십시오.

## 인증서 개체

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.

디바이스에서 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 [재사용 가능한 개체](#) 장의 인증서 정보 및 인증서 구성 섹션을 참조하십시오.

## 인증서 정보

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. 디지털 인증서는 사용자 또는 디바이스의 공개 키 사본 하나도 포함합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.

다음과 같은 인증서 유형을 생성할 수 있습니다.

- 내부 인증서 - 내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.

시스템은 그대로 사용하거나 대체할 수 있는 사전 정의된 내부 인증서 **DefaultInternalCertificate** 및 **DefaultWebServerCertificate**와 함께 제공됩니다.

- 내부 CA(Certificate Authority) - 내부 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.

시스템은 **NGFW-Default-InternalCA**와 같은 미리 정의된 내부 CA 인증서와 함께 제공되며, 이를 그대로 사용하거나 교체할 수 있습니다.

- 신뢰할 수 있는 CA(Certificate Authority) 인증서 - 신뢰할 수 있는 CA 인증서는 다른 인증서에 서명하는 데 사용됩니다. 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.

CA(인증 증명)는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 컨텍스트에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다. CA는 VeriSign과 같이 신뢰받는 서드파티이거나, 조직 내에서 설정한 전용 (내부) CA일 수 있습니다. CA는 인증서 요청을 관리하고 디지털 인증서를 발급하는 기능을 담당합니다.

시스템에는 서드파티 인증 증명에서 제공되는 수많은 신뢰할 수 있는 CA 인증서도 포함됩니다. 이러한 인증서는 Decrypt Re-Sign(암호 해독 재서명) 작업을 위한 SSL 암호 해독 정책에서 사용됩니다.

자세한 내용은 디바이스가 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 재사용 가능한 개체 장의 기능에서 사용하는 인증서 유형 섹션을 참조하십시오.

## 기능에 사용되는 인증서 유형

각 기능에 대해 적절한 유형의 인증서를 생성해야 합니다. 인증서가 필요한 기능은 다음과 같습니다.

### ID 정책(캡티브 포털) - 내부 인증서

(선택 사항). 캡티브 포털은 ID 정책에 사용됩니다. 사용자는 신원을 증명하고 IP 주소를 사용자 이름과 연결하기 위해 디바이스에 인증할 때 이 인증서를 수락해야 합니다. 인증서를 제공하지 않으면 디바이스는 자동으로 생성된 인증서를 사용합니다.

### SSL 암호 해독 정책 — 내부, 내부 CA 및 신뢰할 수 있는 CA 인증서

(필수) SSL 암호 해독 정책은 다음 목적을 위해 인증서를 사용합니다.

- 내부 인증서는 알려진 키 암호 해독 규칙에 사용됩니다.
- 내부 CA 인증서는 클라이언트와 디바이스 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 사용됩니다.
- 신뢰할 수 있는 CA 인증서
  - 신뢰할 수 있는 CA 인증서는 디바이스와 서버 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 간접적으로 사용됩니다. 다른 인증서와 달리 이러한 인증서는 SSL 암호 해독 정책에서 직접 구성하지 않고 시스템에 업로드하기만 하면 됩니다. 시스템에는 신뢰할 수 있는 CA 인증서가 많이 포함되어 있으므로 추가 인증서를 업로드할 필요가 없을 수도 있습니다.
  - Active Directory 영역 개체를 생성하고 암호화를 사용하도록 디렉터리 서버를 구성할 때.

## 인증서 구성

ID 정책 또는 SSL 암호 해독 정책에 사용되는 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다. 필요한 경우 OpenSSL을 사용하여 인증서를 생성하거나 신뢰할 수 있는 인증 기관에서 가져오거나 자체 서명된 인증서를 생성할 수 있습니다.

다음 절차를 사용하여 인증서 개체를 구성합니다.

- [내부 및 내부 CA 인증서 업로드](#)
- [신뢰할 수 있는 CA 인증서 업로드](#)
- [자체 서명 내부 및 내부 CA 인증서 생성](#)
- 인증서를 보거나 편집하려면 인증서의 편집 아이콘 또는 보기 아이콘을 클릭합니다.

- 참조되지 않는 인증서를 삭제하려면 해당 인증서의 삭제 아이콘을 클릭합니다. [개체 삭제](#)를 참조하십시오.

## 내부 및 내부 CA 인증서 업로드

내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.

내부 CA(Certificate Authority) 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 [기능에 사용되는 인증서 유형](#)을 참조하십시오.


### 절차

이 절차에서는 인증서 파일을 업로드하거나 기존 인증서 텍스트를 텍스트 상자에 붙여넣어 내부 또는 내부 CA 인증서를 생성합니다. 자체 서명된 인증서를 생성하려면 [자체 서명 내부 및 내부 CA 인증서 생성](#)을 참조하십시오.

내부 또는 내부 CA 인증서 개체를 만들거나 새 인증서 개체를 정책에 추가하려면 다음 절차를 따르십시오.

#### Procedure

단계 1 다음 중 하나를 수행합니다.

- 개체 페이지에서 인증서 개체를 생성합니다.
  - a. 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
  - b. 플러스 버튼 를 클릭하고 **FTD > Certificate(인증서)**를 선택합니다.
- 정책에 새 인증서 개체를 추가할 때 **Create New Object(새 개체 생성)**를 클릭합니다.

단계 2 인증서의 **Name(이름)**을 입력합니다. 이름은 구성에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 3 1단계에서 내부 인증서 또는 내부 CA를 선택합니다.

단계 4 2단계에서 **Upload(업로드)**를 선택하여 인증서 파일을 업로드합니다.

단계 5 3단계에서 서버 인증서 영역의 텍스트 상자에 인증서 내용을 붙여넣거나 마법사의 설명에 따라 인증서 파일을 업로드합니다. 텍스트 상자에 인증서를 붙여넣는 경우 인증서에 BEGIN CERTIFICATE 및 END CERTIFICATE 줄이 포함되어야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
```

```

UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ210
(...5 lines removed...)
shGJDReRYJQqilhHZrYTZWZAYTrD7NQPhtK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZ1zJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfwxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
v1k3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----

```

단계 6 3단계의 인증서 키 영역에서 키 내용을 인증서 키 텍스트 상자에 붙여넣거나 마법사의 설명에 따라 키 파일을 업로드합니다. 텍스트 상자에 키를 붙여넣는 경우 키에는 BEGIN PRIVATE KEY 또는 BEGIN RSA PRIVATE KEY 및 END PRIVATE KEY 또는 END PRIVATE KEY 행이 포함되어야 합니다.

**Note** 키는 암호화할 수 없습니다.

단계 7 Add(추가)를 클릭합니다.

## 신뢰할 수 있는 CA 인증서 업로드

신뢰할 수 있는 CA(Certificate Authority) 인증서는 다른 인증서에 서명하는 데 사용되며, 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.


이러한 인증서를 사용하는 기능에 대한 자세한 내용은 [기능에 사용되는 인증서 유형](#)을 참조하십시오.

외부 인증 기관으로부터 신뢰할 수 있는 CA 인증을 획득하거나, OpenSSL 도구 등 자체 내부 CA를 사용하여 CA 인증을 생성합니다. 그런 다음, 아래 절차를 사용하여 인증서를 업로드합니다.

### 절차

#### Procedure

단계 1 다음 중 하나를 수행합니다.

- 개체 페이지에서 인증서 개체를 생성합니다.
  - a. 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
  - b. 플러스 버튼  를 클릭하고 **FTD > Certificate(인증서)**를 선택합니다.
- 정책에 새 인증서 개체를 추가할 때 **Create New Object(새 개체 생성)**를 클릭합니다.

단계 2 인증서의 **Name(이름)**을 입력합니다. 이름은 구성에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 3 1단계에서 **External CA Certificate(외부 CA 인증서)**를 선택하고 **Continue(계속)**를 클릭합니다. 마법사가 3단계로 진행합니다.

단계 4 3단계의 **Certificate Contents**(인증서 내용) 영역에서 텍스트 상자에 인증서 내용을 붙여넣거나 마법사의 설명에 따라 인증서 파일을 업로드합니다.

인증서는 다음 지침을 따라야 합니다.

- 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.
- 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.
- 붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxZAJBgNV
BAYTA1VTMQswCQYDVQQLIDAJUWDEPMA0GA1UEBwwGZXVzdGluMRQwEgYDVQKDAx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTEyMDI3MjIzNDE3
WhcNMTEyMDI3MjIzNDE3WjBXMQswCQYDVQQLGEwJVUzELMAkGA1UECAwCVFgxZDZAN
BgNVBACMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjEwFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwTP
ES6Ve+S9z7WLGX5JlF58AvH82GpkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgK1OwXbRvOdkstzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN200jv
2b1sf0ydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

단계 5 **Add**(추가)를 클릭합니다.

## 자체 서명 내부 및 내부 CA 인증서 생성

내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.

내부 CA(Certificate Authority) 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.

OpenSSL을 사용하여 이러한 인증서를 생성하거나, 신뢰할 수 있는 CA에서 인증서를 가져오고 업로드할 수 있습니다. 자세한 내용은 [내부 및 내부 CA 인증서 업로드](#)를 참조하십시오.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 [기능에 사용되는 인증서 유형](#)을 참조하십시오.



**Note** 새로운 자체 서명 인증서는 유효 기간이 5년으로 생성됩니다. 만료되기 전에 인증서를 교체하십시오.

**Warning**

자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 [새 인증서 탐지됨](#)를 참조하십시오.


## 절차

이 절차는 마법사에서 적절한 인증서 필드 값을 입력하여 자체 서명된 인증서를 생성합니다. 인증서 파일을 업로드하여 내부 또는 내부 CA 인증서를 생성하려면 [내부 및 내부 CA 인증서 업로드](#)를 참조하십시오.

자체 서명된 인증서를 생성하려면 다음 절차를 따르십시오.

**Procedure**

단계 1 다음 중 하나를 수행합니다.

- 개체 페이지에서 인증서 개체를 생성합니다.
  - a. 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
  - b. 플러스 버튼 를 클릭하고 **FTD > Certificate(인증서)**를 선택합니다.
- 정책에 새 인증서 개체를 추가할 때 **Create New Object(새 개체 생성)**를 클릭합니다.

단계 2 인증서의 **Name(이름)**을 입력합니다. 이름은 구성에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 3 1단계에서 내부 인증서 또는 내부 **CA**를 선택합니다.

단계 4 2단계에서 **Self-Signed(자체 서명됨)**을 선택하여 이 단계에서 자체 서명된 인증서를 생성합니다.

단계 5 인증서 주체와 발급자 정보에 다음 중 한 가지 이상의 정보를 구성합니다.

- 국가(C)- 드롭다운 목록에서 국가 코드를 선택합니다.
- State or Province(주/도)(ST) - 인증서에 포함할 주/도.
- Locality or City(구/군/시)(L) - 인증서에 포함할 구/군/시(예: 도시 이름).
- Organization(조직)(O) - 인증서에 포함할 조직 또는 회사 이름.
- Organizational Unit(Department)(조직 단위(부서))(OU) - 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- Common Name(공용 이름)(CN) - 인증서에 포함할 X.500 일반 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.

단계 6 **Add(추가)**를 클릭합니다.

## IPsec 제안 구성

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성하여 선택합니다.
- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.



**Note** IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

- [IKEv1 IPsec 제안 개체 관리](#)
- [IKEv2 IPsec 제안 개체 관리](#)

### IKEv1 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 CDO(Cisco Defense Orchestrator)는 IKEv1 IPsec 제안 개체를 지원합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.



**Note** IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

#### Related Topics

[IKEv1 IPsec 제안 개체 생성 또는 편집, 483 페이지](#)



## IKEv1 IPsec 제안 개체 생성 또는 편집


여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv1 Proposal**(새 IKEv1 제안 생성) 링크를 클릭하여 사이트 투 사이트 VPN 연결에서 IKEv1 IPsec 설정을 편집하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

### Procedure

**단계 1** 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

**단계 2** 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv1 IPsec Proposal(제안)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(편집)**를 클릭합니다.

**단계 3** 새 개체의 개체 이름을 입력합니다.

**단계 4** IKEv1 IPsec 제안 개체가 작동하는 모드를 선택합니다.

- 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPsec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec이 구현되는 통상적인 방식입니다.
- 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPsec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.

**단계 5** 이 제안에 대한 **ESP Encryption(ESP 암호화)(Encapsulating Security Protocol)** 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정, on page 471](#)를 참조하십시오.

**단계 6** 인증에 사용할 **ESP Hash(ESP 해시)** 또는 무결성 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정, on page 472](#)를 참조하십시오.

**단계 7** **Add(추가)**를 클릭합니다.

## IKEv2 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

### Related Topics

[IKEv2 IPsec 제안 개체 생성 또는 편집](#), 484 페이지

## IKEv2 IPsec 제안 개체 생성 또는 편집


여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IPsec Proposal**(새 IPsec 제안 생성) 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 편집하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv2 IPsec Proposal**(제안)을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit**(편집)를 클릭합니다.

단계 3 새 개체의 개체 이름을 입력합니다.

단계 4 IKE2 IPsec 제안 개체 구성:

- Encryption**(암호화) - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#), on page 471를 참조하십시오.
- Integrity Hash**(무결성 해시) - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정](#), on page 472를 참조하십시오.

단계 5 **Add**(추가)를 클릭합니다.

## 글로벌 IKE 정책 구성

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 Edit(수정)을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

다음 항목에서는 각 버전에 대해 IKE 정책을 구성하는 방법에 대해 설명합니다.

- [IKEv1 정책 관리](#)
- [IKEv2 정책 관리](#)

### IKEv1 정책 관리

IKEv1 정책을 생성하고 편집하는 방법을 설명합니다.

#### IKEv1 정책 정보

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

#### Related Topics

[IKEv1 정책 생성 또는 편집](#), 479 페이지


## IKEv1 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy**(새 IKE 정책 생성) 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv1 정책을 생성할 수도 있습니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv1 Policy**(IKEv1 정책)를 선택하여 새 IKEv1 정책을 생성합니다.
- 개체 페이지에서 편집할 IKEv1 정책을 선택하고 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

단계 3 개체 이름을 최대 128자로 입력합니다.

단계 4 IKEv1 속성을 구성합니다.

- **Priority**(우선순위)-IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Encryption**(암호화) - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Diffie-Hellman Group**(Diffie-Hellman 그룹) - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Lifetime**(라이프타임)-SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.
- **Authentication**(인증) - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 [사용할 인증 방법 결정, on page 473](#)를 참조하십시오.
  - **Preshared Key**(사전 공유 키) - 각 디바이스에 정의된 사전 공유 키를 사용합니다. 이 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.

- **Certificate(인증서)** - 서로 식별할 피어에 대해 디바이스 ID 인증서를 사용합니다. Certificate Authority에서 각 피어를 등록하여 이 인증서를 가져와야 합니다. 또한 각 피어에서 ID 인증서 서명에 사용되는 신뢰할 수 있는 CA 루트 및 중간 CA 인증서를 업로드해야 합니다. 피어는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.
- **Hash(해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 [VPN에서 사용되는 암호화 및 해시 알고리즘, on page 470](#)를 참조하십시오.

단계 5 **Add(추가)**를 클릭합니다.

## IKEv2 정책 관리

IKEv2 정책을 생성하고 편집하는 방법을 설명합니다.

### IKEv2 정책 정보

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 **State(상태)** 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

### Related Topics

[IKEv2 정책 생성 또는 편집, 481 페이지](#)


### IKEv2 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv2 Policy(새 IKEv2 정책 생성)** 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv2 정책을 생성할 수도 있습니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv2 Policy(FTD IKEv2 정책)**를 선택하여 새 IKEv2 정책을 생성합니다.
- 개체 페이지에서 수정할 IKEv2 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit(편집)**를 클릭합니다.

단계 3 개체 이름을 최대 128자로 입력합니다.

단계 4 IKEv2 속성을 구성합니다.

- **Priority(우선순위)**-IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에서 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **State(상태)** - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Encryption(암호화)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을 둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는 반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정, on page 471](#)를 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 Diffie-Hellman 모듈러스 그룹 결정, on page 472](#)를 참조하십시오.
- **Integrity Hash(무결성 해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 [VPN에서 사용되는 암호화 및 해시 알고리즘, on page 470](#)를 참조하십시오.
- **PRF(Pseudo-Random Function) 해시** - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해서도 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [VPN에서 사용되는 암호화 및 해시 알고리즘, on page 470](#)를 참조하십시오.
- **Lifetime(라이프타임)**-SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 5 Add(추가)를 클릭합니다.

## RA VPN 개체

### 보안 영역 개체

보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 여러 영역을 정의할 수 있지만, 지정된 인터페이스는 하나의 영역에만 속할 수 있습니다.

Firepower System은 초기 구성 중에 다음 영역을 생성하며 Defense Orchestrator의 개체 페이지에 표시됩니다. 영역을 편집하여 인터페이스를 추가하거나 제거할 수도 있고, 더 이상 사용하지 않는 영역을 삭제할 수도 있습니다.

- **inside\_zone** - 내부 인터페이스를 포함합니다. 이 영역은 내부 네트워크를 나타내는 데 사용됩니다.
- **outside\_zone** - 외부 인터페이스를 포함합니다. 이 영역은 인터넷 등 제어 범위 외부에 있는 네트워크를 나타내는 데 사용됩니다.

일반적으로는 인터페이스가 네트워크에서 수행하는 역할별로 인터페이스를 그룹화합니다. 예를 들어 인터넷에 연결하는 인터페이스는 **outside\_zone** 보안 영역에 배치하고 내부 네트워크용의 모든 인터페이스는 **inside\_zone** 보안 영역에 배치합니다. 그러면 외부 영역에서 들어오는 트래픽과 내부 영역으로 이동하는 트래픽에 액세스 제어 규칙을 적용할 수 있습니다.

영역을 생성하기 전에 네트워크에 적용할 액세스 규칙 및 기타 정책을 고려하십시오. 예를 들어 모든 내부 인터페이스를 같은 영역에 배치할 필요는 없습니다. 내부 네트워크가 4개인데 그중 하나를 나머지 3개와 다른 방식으로 취급하려는 경우에는 영역을 하나가 아닌 두 개 생성할 수 있습니다. 공개 웹 서버에 대한 외부 액세스를 허용해야 하는 인터페이스가 있는 경우에는 해당 인터페이스용으로 별도의 영역을 사용할 수 있습니다.

관련 정보:

- [Firepower 보안 영역 개체 생성 또는 편집](#)
- [보안 영역에 Firepower 인터페이스 할당](#)
- [개체 삭제](#)

### Firepower 보안 영역 개체 생성 또는 편집


보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 여러 영역을 정의할 수 있지만, 지정된 인터페이스는 하나의 영역에만 속할 수 있습니다. 자세한 내용은 [보안 영역 개체](#)를 참조하십시오.

보안 영역 개체는 해당 디바이스에 대한 규칙에서 사용되지 않는 한 디바이스와 연결되지 않습니다.

#### 보안 영역 개체 생성

보안 영역 개체를 생성하려면 다음 지침을 따르십시오.



## Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 파란색 플러스 버튼  을 클릭하고 **FTD > Security Zone(보안 영역)**을 선택하여 새 개체를 생성합니다.
- 단계 3 개체의 이름과 설명(선택 사항)을 입력합니다.
- 단계 4 보안 영역에 넣을 인터페이스를 선택합니다.
- 단계 5 **Add(추가)**를 클릭합니다.

## 보안 영역 개체 편집

FDM 관리 디바이스를 온보딩한 후 이미 두 개 이상의 보안 영역이 있음을 알 수 있습니다. 하나는 `inside_zone`이고 다른 하나는 `outside_zone`입니다. 이러한 영역은 편집하거나 삭제할 수 있습니다. 보안 영역 개체를 편집하려면 다음 지침을 따르십시오.


## Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 편집할 개체를 찾습니다.
- 개체의 이름을 알고 있는 경우 개체 페이지에서 검색할 수 있습니다.
    - 보안 영역별로 목록을 필터링합니다.
    - 검색 필드에 개체 이름을 입력합니다.
    - 개체를 선택합니다.
  - 개체가 디바이스와 연결되어 있는 경우 **Inventory(인벤토리)** 페이지에서 시작하여 개체를 검색할 수 있습니다.
    - 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.
    - **Devices(디바이스)** 탭을 클릭합니다.
    - 해당 탭을 클릭합니다.
    - 디바이스 **필터** 및 **검색** 표시줄을 사용하여 디바이스를 찾습니다.
    - 디바이스를 선택합니다.
  - 오른쪽의 관리 창에서  **Objects(개체)**를 클릭합니다.
  - 개체 필터  과 검색 표시줄을 사용하여 찾고 있는 개체를 찾습니다.



**Note** 생성한 보안 영역 개체가 디바이스에 대한 정책의 규칙과 연결되지 않은 경우 "연결되지 않은" 것으로 간주되어 디바이스 검색 결과에 표시되지 않습니다.

단계 3 개체를 선택합니다.

단계 4 우측의 작업 창에서 **Edit**(편집) 아이콘  를 클릭합니다.

단계 5 개체의 속성을 편집한 후, **Save**(저장)를 클릭합니다.

단계 6 저장을 클릭하면 이러한 변경 사항이 다른 디바이스에 어떤 영향을 미치는지 설명하는 메시지가 표시됩니다. **Confirm**(확인)을 클릭하여 변경 사항을 저장하거나 취소합니다.

## 서비스 개체

### Firepower 서비스 개체

FTD 서비스 개체, 서비스 그룹 및 포트 그룹은 IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다.

FTD 서비스 그룹은 서비스 개체의 모음입니다. 서비스 그룹은 하나 이상의 프로토콜에 대한 개체를 포함할 수 있습니다. 이러한 개체 및 그룹을 보안 정책에서 사용하여 네트워크 트래픽 일치 기준(예: 특정 TCP 포트에 대한 트래픽을 허용하는 액세스 규칙을 사용하기 위한 기준)을 정의할 수 있습니다. 시스템에는 일반 서비스를 위해 사전 정의된 개체가 여러 개 포함되어 있으며, 정책에서 이러한 개체를 사용할 수 있지만 시스템 정의 개체를 편집하거나 삭제할 수는 없습니다.

Firepower Device Manager 및 Firepower Management Center는 서비스 개체를 포트 개체 및 서비스 그룹 및 포트 그룹으로 참조하십시오.

자세한 내용은 [Firepower 서비스 개체 생성 및 편집](#)을 참조하십시오.

### 프로토콜 개체

프로토콜 개체는 덜 일반적으로 사용되는 또는 레거시 프로토콜을 포함하는 서비스 개체 유형입니다. 프로토콜 개체는 이름 및 [프로토콜 번호](#)로 식별됩니다. CDO는 ASA 및 Firepower(FDM 관리) 구성에서 이러한 개체를 인식하고 사용자가 쉽게 찾을 수 있도록 자체 필터인 "프로토콜"을 제공합니다.

자세한 내용은 [Firepower 서비스 개체 생성 및 편집](#)을 참조하십시오.

### ICMP 개체

ICMP(Internet Control Message Protocol) 개체는 ICMP 및 IPv6-ICMP 메시지를 위한 서비스 개체입니다. CDO는 ASA 및 Firepower 구성에서 해당 디바이스가 온보딩되고 사용자가 개체를 쉽게 찾을 수 있도록 해당 디바이스에 "ICMP" 필터를 제공할 때 이러한 개체를 인식합니다.

CDO를 사용하면 ASA 구성에서 ICMP 개체를 제거하거나 이름을 바꿀 수 있습니다. CDO를 사용하여 Firepower 구성에서 ICMP 및 ICMPv6 개체를 생성, 업데이트 및 삭제할 수 있습니다.



**Note** ICMPv6 프로토콜의 경우 AWS는 특정 인수 선택을 지원하지 않습니다. 모든 ICMPv6 메시지를 허용하는 규칙만 지원됩니다.

자세한 내용은 [Firepower 서비스 개체 생성 및 편집](#)을 참조하십시오.

관련 정보:

- [개체 삭제, on page 129](#)


## Firepower 서비스 개체 생성 및 편집

Firepower 서비스 개체를 생성하려면 다음 단계를 수행합니다.

firewall device manager(FDM 관리) 서비스 개체는 TCP/IP 프로토콜 및 포트를 지정하는 재사용 가능한 구성 요소입니다. firewall device manager, 온프레미스 Firewall Management Center 및 클라우드 사용 Firewall Management Center는 이러한 개체를 "포트 개체"라고 합니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 오른쪽에 있는 파란색 버튼  을 클릭하여 개체를 생성하고 **FTD > Service(FTD 서비스)**를 선택합니다.

단계 3 개체 이름과 설명을 입력합니다.

단계 4 **Create a service object(서비스 개체 생성)**를 선택합니다.

단계 5 **Service Type(서비스 유형)** 버튼을 클릭하고 개체를 생성할 프로토콜을 선택합니다.

단계 6 다음과 같이 프로토콜을 구성합니다.

- **TCP, UDP**

- **eq**를 선택하고 포트 번호 또는 프로토콜 이름을 입력합니다. 예를 들어 포트 번호로 80을 입력하거나 프로토콜 이름으로 HTTP를 입력할 수 있습니다.

- 범위를 선택한 다음 포트 번호의 범위를 입력할 수도 있습니다(예: **1 65535**(모든 포트 포함)).

- **ICMP, IPv6-ICMP-ICMP** 유형을 선택합니다. 해당 유형을 모든 ICMP 메시지에 적용하려면 모두를 선택합니다. 유형과 코드에 대한 자세한 내용은 다음 페이지를 참조하십시오.

- ICMP-<http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml>

- ICMPv6-<http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml>

- 기타 - 원하는 프로토콜을 선택합니다.

단계 7 **Add(추가)**를 클릭합니다.


단계 8 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## Firepower 서비스 그룹 생성

서비스 그룹은 하나 이상의 프로토콜을 나타내는 하나 이상의 서비스 개체로 구성될 수 있습니다. 서비스 개체를 그룹에 추가하려면 먼저 서비스 개체를 생성해야 합니다. Firepower Device Manager 및 Firepower Management Center에서는 이러한 개체를 "포트 개체"라고 합니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 오른쪽에 있는 파란색 버튼  을 클릭하여 개체를 생성하고 **FTD > Service(서비스)**를 선택합니다.

단계 3 개체 이름과 설명을 입력합니다.

단계 4 **Create a service group(서비스 그룹 생성)**를 선택합니다.

단계 5 **Add Object(개체 추가)**를 클릭하여 그룹에 개체를 추가합니다.

- 위의 **Firepower 서비스 개체 생성 및 편집**에서 수행한 것처럼 **Create(생성)**를 클릭하여 새 개체를 생성합니다.
- 기존 서비스 개체를 그룹에 추가하려면 **Choose(선택)**를 클릭합니다. 개체를 더 추가하려면 이 단계를 반복합니다.

단계 6 서비스 그룹에 서비스 개체 추가를 완료하면 **Add(추가)**를 클릭합니다.


단계 7 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## Firepower 서비스 개체 또는 서비스 그룹 편집

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 3 작업 창에서 **Edit(편집)**  를 클릭합니다.

단계 4 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 5 **Save(저장)**를 클릭합니다.

단계 6 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 7 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 보안 그룹 태그 그룹

### 보안 그룹 태그(Security Group Tags)

#### 보안 그룹 태그 정보

Cisco ISE(Identity Services Engine)를 사용하여 Cisco TrustSec 네트워크에서 트래픽을 분류하기 위해 SGT(Security Group Tag)를 정의하고 사용하는 경우, SGT를 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다. 따라서 IP 주소가 아니라 보안 그룹 멤버십을 기준으로 액세스를 차단하거나 허용할 수 있습니다.

ISE에서는 SGT를 생성하고 호스트 또는 네트워크 IP 주소를 각 태그에 할당할 수 있습니다. SGT를 사용자의 계정에 할당하면 SGT가 사용자의 트래픽에 할당됩니다. ISE 서버에 연결하도록 FDM 관리 디바이스를 구성하고 SGT를 생성한 후 Cisco Defense Orchestrator에서 SGT 그룹을 생성하고 이를 중심으로 액세스 제어 규칙을 작성할 수 있습니다. SGT를 FDM 관리 디바이스에 연결하려면 먼저 ISE의 SXP(SGT Exchange Protocol) 매핑을 구성해야 합니다. 자세한 내용은 현재 실행 중인 버전의 [Cisco ISE\(Identity Services Engine\) 관리자 설명서](#)에서 보안 그룹 태그 교환 프로토콜을 참조하십시오.

FDM 관리 디바이스가 SGT를 액세스 제어 규칙에 대한 트래픽 일치 기준으로 평가하는 경우, 다음 우선순위를 사용합니다.

1. 패킷에 정의된 소스 SGT(있는 경우). 대상 일치는 이 기술을 사용하여 수행되지 않습니다. SGT를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메서드를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.
2. ISE 세션 디렉토리에서 다운로드된 대로 사용자 세션에 할당된 SGT. 이러한 유형의 SGT 일치에 대한 세션 디렉토리 정보를 수신 대기하려면 해당 옵션을 활성화해야 합니다. 그러나 이 옵션은 처음에 ISE ID 소스를 생성할 때 기본적으로 켜집니다. SGT는 소스 또는 대상과 일치할 수 있습니다. 필수 사항은 아니지만 일반적으로 사용자 ID 정보를 수집하기 위해 AD 영역과 함께 ISE ID 소스를 사용하여 패시브 인증 ID 규칙도 설정합니다.
3. SXP를 사용하여 다운로드한 SGT-IP 주소 매핑. IP 주소가 SGT 범위 내에 있는 경우 트래픽은 SGT를 사용하는 액세스 제어 규칙과 일치합니다. SGT는 소스 또는 대상과 일치할 수 있습니다.



**Note** ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다. SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

## 버전 지원

CDO는 현재 버전 6.5 이상을 FDM 관리 실행하는 FDM 매니저 디바이스에서 SGT 및 SGT 그룹을 지원합니다. FDM 관리 디바이스를 사용하면 버전 6.5 이상에서 ISE 서버를 구성하고 연결할 수 있지만 버전 6.7까지는 UI에서 SGT 구성이 지원되지 않습니다.

FDM 관리 UI에서 이는 버전 6.5 이상을 실행하는 FDM 관리 디바이스가 SGT의 SXP 매핑을 다운로드할 수 있지만, 개체 또는 액세스 제어 규칙에 수동으로 추가할 수 없음을 의미합니다. 버전 6.5 또는 버전 6.6을 실행하는 디바이스의 SGT를 변경하려면 ISE UI를 사용해야 합니다. 그러나 버전 6.5를 실행하는 디바이스가 Cisco Defense Orchestrator에 온보딩된 경우 디바이스와 연결된 현재 SGT를 확인하고 SGT 그룹을 생성할 수 있습니다.

## CDO의 SGT

### 보안 그룹 태그(Security Group Tags)

SGT는 CDO에서 읽기 전용입니다. CDO에서 SGT를 생성하거나 편집할 수 없습니다. SGT를 생성하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 관리자 설명서](#)를 참조하십시오.

### SGT 그룹



**Note** FDM 관리 디바이스는 SGT 그룹을 SGT 동적 개체로 지칭합니다. CDO에서는 이러한 태그 목록을 현재 SGT 그룹이라고 합니다. FDM 관리 디바이스 또는 ISE UI를 참조하지 않고 CDO에서 SGT 그룹을 생성할 수 있습니다.

SGT 그룹을 사용하여 ISE가 할당한 SGT를 기준으로 소스 또는 대상 주소를 식별합니다. 그 다음 트래픽 일치 기준을 정의하는 목적으로 액세스 제어 규칙의 개체를 사용할 수 있습니다. ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다.

SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

CDO에서 SGT 그룹을 생성하려면 하나 이상의 SGT가 이미 구성되어 있어야 하며, 사용하려는 디바이스의 FDM 관리 콘솔에 대해 ISE 서버에서 SGT 매핑이 구성되어 있어야 합니다. 둘 이상의 FDM 관리 디바이스가 동일한 ISE 서버와 연결된 경우 SGT 또는 SGT 그룹을 둘 이상의 디바이스에 적용할 수 있습니다. 디바이스가 ISE 서버와 연결되지 않은 경우, SGT 개체를 액세스 제어 규칙에 포함하거나 SGT 그룹을 해당 디바이스 설정에 적용할 수 없습니다.

### 규칙의 SGT 그룹

SGT 그룹을 액세스 제어 규칙에 추가할 수 있습니다. 이는 소스 또는 대상 네트워크 개체로 나타납니다. 네트워크가 규칙에서 작동하는 방식에 대한 자세한 내용은 [FDM-관리 액세스 제어 규칙의 소스 및 대상 기준](#)을 참조하십시오.

Objects(개체) 페이지에서 SGT 그룹을 생성할 수 있습니다. 자세한 내용은 [SGT 그룹 생성, on page 167](#)를 참조하십시오.

## SGT 그룹 생성

액세스 제어 규칙에 사용할 수 있는 SGT 그룹을 생성하려면 다음 절차를 사용합니다.

### Before you begin

SGT(보안 그룹 태그) 그룹을 생성하기 전에 다음 구성 또는 환경을 구성해야 합니다.

- FDM 관리 디바이스는 버전 6.5 이상을 실행해야 합니다.
- SXP 매핑을 구독하고 변경 사항을 구축하도록 ISE ID 소스를 구성해야 합니다. SXP 매핑을 관리하려면 사용 중인 버전 6.7 이상에 대한 [Firepower Device Manager 구성 가이드](#)의 **ISE**에서 보안 그룹 및 **SXP** 게시 구성을 참조하십시오.
- 모든 SGT는 ISE에서 생성해야 합니다. SGT를 생성하려면 현재 실행 중인 버전의 [Cisco ISE\(Identity Services Engine\) 구성 설명서](#)를 참조하십시오.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **FTD > Network(네트워크)**를 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 (선택 사항) 설명을 추가합니다.

단계 6 **SGT**를 클릭하고 드롭다운 메뉴를 사용하여 그룹에 포함할 모든 해당 SGT를 선택합니다. SGT 이름을 기준으로 목록을 정렬할 수 있습니다.

단계 7 **Save(저장)**를 클릭합니다.

**Note** CDO에서 SGT를 생성하거나 편집할 수 없으며 SGT 그룹에서 추가하거나 제거할 수만 있습니다. SGT를 생성하거나 편집하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 구성 설명서](#)를 참조하십시오.


## SGT 그룹 편집

SGT 그룹을 편집하려면 다음 절차를 따르십시오.

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 SGT 그룹을 찾습니다.

단계 3 SGT 그룹을 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 SGT 그룹을 편집합니다. 그룹과 관련된 이름, 설명 또는 SGT를 편집합니다.

단계 5 **Save**(저장)를 클릭합니다.

**Note** CDO에서 SGT를 생성하거나 편집할 수 없으며 SGT 그룹에서 추가하거나 제거할 수만 있습니다. SGT를 생성하거나 편집하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 구성 설명서](#)를 참조하십시오.

## 액세스 제어 규칙에 SGT 그룹 추가

액세스 제어 규칙에 SGT 그룹을 추가하려면 다음 절차를 따르십시오.


### Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 **FTD** 탭을 클릭하고 SGT 그룹을 추가할 디바이스를 선택합니다.

단계 4 **Management**(관리) 창에서 **Policy**(정책)를 선택합니다.

단계 5 소스 또는 대상 개체에 대한 파란색 플러스 버튼  을 클릭하고 **SGT** 그룹을 선택합니다.

단계 6 개체 필터 및 검색 필드를 사용하여 편집하려는 SGT 그룹을 찾습니다.

단계 7 **Save**(저장)를 클릭합니다.

단계 8 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).

**Note** 추가 SGT 그룹을 생성해야 하는 경우 **Create New Object**(새 개체 생성)를 클릭합니다. [SGT 그룹 생성](#) 및 규칙에 SGT 그룹 추가에 언급된 필수 정보를 입력하고 SGT 그룹을 규칙에 추가합니다.

## 시스템 로그 서버 개체


FDM 관리 디바이스는 이벤트를 저장할 수 있는 용량이 제한되어 있습니다. 이벤트에 대한 스토리지를 최대화하기 위해 외부 서버를 구성할 수 있습니다. 시스템 로그(syslog) 서버 개체는 연결 지향형 또는 진단 시스템 로그 메시지를 수신할 수 있는 서버를 식별합니다. 로그 수집 및 분석을 위해 syslog 서버를 설정한 경우, Cisco Defense Orchestrator를 사용하여 개체를 생성하여 정의한 후 관련 정책에 이 개체를 사용할 수 있습니다.

## 시스템 로그 서버 개체 생성 및 편집

새 시스템 로그 서버 개체를 생성하려면 다음 단계를 수행합니다.

## Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 **Create Object(개체 생성)** 버튼  을 클릭합니다.

단계 3 FDM 관리 디바이스 개체 유형에서 **Syslog Server(시스템 로그 서버)**를 선택합니다.

단계 4 시스템 로그 서버 개체 속성을 구성합니다.

- **IP 주소** - syslog 서버의 IP 주소를 입력합니다.
- **Protocol Type(프로토콜 유형)** — 시스템 로그 서버가 메시지를 수신하는 데 사용하는 프로토콜을 선택합니다. TCP를 선택하는 경우 시스템은 syslog 서버를 사용할 수 없는 경우를 인식할 수 있으며, 서버를 다시 사용할 수 있을 때까지 이벤트 전송을 중지합니다.
- **Port Number(포트 번호)** — 시스템 로그에 사용할 유효한 포트 번호를 입력합니다. 시스템 로그 서버가 기본 포트를 사용하는 경우 기본 UDP 포트 514를 입력하거나 기본 TCP 포트 1470을 입력합니다. 서버에서 기본 포트를 사용하지 않는 경우 올바른 포트 번호를 입력합니다. 포트가 1025~65535 범위에 포함되어야 합니다.
- **Select an interface(인터페이스 선택)** - 진단 시스템 로그 메시지를 보내는 데 사용해야 하는 인터페이스를 선택합니다. 연결 및 침입 이벤트는 항상 관리 인터페이스를 사용합니다. 선택하는 인터페이스에 따라 syslog 메시지와 연결되는 IP 주소가 결정됩니다. 아래에 나열된 옵션 중 하나만 선택할 수 있습니다. 둘 다 선택할 수는 없습니다. 다음 옵션 중 하나를 선택합니다.
  - **Data Interface(데이터 인터페이스)** - 진단 syslog 메시지에 대해 선택하는 데이터 인터페이스를 사용합니다. 생성된 목록에서 인터페이스를 선택합니다. 브리지 그룹 멤버 인터페이스를 통해 서버에 액세스할 수 있는 경우에는 BVI(브리지 그룹 인터페이스)를 선택합니다. 진단 인터페이스(물리적 관리 인터페이스)를 통해 서버에 액세스할 수 있는 경우에는 이 옵션 대신 Management Interface(관리 인터페이스)를 선택하는 것이 좋습니다. 패시브 인터페이스는 선택할 수 없습니다. 연결 및 침입 시스템 로그 메시지의 경우 소스 IP 주소는 관리 인터페이스용이거나, 데이터 인터페이스를 통해 라우팅하는 경우 게이트웨이 인터페이스용입니다.
  - **Management Interface(관리 인터페이스)** - 모든 유형의 syslog 메시지에 대해 가상 관리 인터페이스를 사용합니다. 소스 IP 주소는 관리 인터페이스용이거나, 데이터 인터페이스를 통해 라우팅하는 경우 게이트웨이 인터페이스용입니다.

단계 5 **Add(추가)**를 클릭합니다.

단계 6 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## Syslog 서버 개체 편집

기존 Syslog 서버 개체를 편집하려면 다음 단계를 따르십시오.



## Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 원하는 Syslog 서버 개체를 찾아 선택합니다. Syslog 서버 개체 유형별로 개체 목록을 필터링 할 수 있습니다.
- 단계 3 작업 창에서 **Edit(편집)**를 클릭합니다.
- 단계 4 원하는 대로 편집하고 **Save(저장)**를 클릭합니다.
- 단계 5 변경 사항을 확인합니다.
- 단계 6 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

관련 정보:

- [개체 삭제](#)

## SaaS(Secure Logging Analytics)를 위한 시스템 로그 서버 개체 생성


이벤트를 전송할 SEC(Secure Event Connector)의 IP 주소, TCP 포트 또는 UDP 포트를 사용하여 시스템 로그 서버 개체를 생성합니다. 테넌트에 온보딩한 모든 SEC에 대해 하나의 시스템 로그 개체를 생성하지만, 하나의 규칙에서 하나의 SEC를 나타내는 하나의 시스템 로그 개체로만 이벤트를 전송합니다.

사전 요구 사항

이 작업은 더 큰 워크플로우의 일부입니다. 시작하기 전에 [FDM-관리 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현, on page 665](#)을 참조하십시오.

절차

## Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 **Create Object(개체 생성)** 버튼  을 클릭합니다.
- 단계 3 FDM 관리 장치 개체 유형에서 **Syslog Server(Syslog 서버)**를 선택합니다.
- 단계 4 시스템 로그 서버 개체 속성을 구성합니다. SEC의 이러한 속성을 찾으려면 **Admin(관리) > Secure Connector(보안 커넥터)**를 선택합니다. 그런 다음 syslog 개체를 구성할 보안 이벤트 커넥터를 선택하고 오른쪽의 세부 정보 창을 살펴봅니다.
  - IP 주소 - SEC의 IP 주소를 입력합니다.
  - 프로토콜 유형 - TCP 또는 UDP를 선택합니다.
  - 포트 번호 - TCP를 선택한 경우 포트 10125를 입력하고 UDP를 선택한 경우 10025를 입력합니다.

- 인터페이스 선택 - SEC에 도달하도록 구성된 인터페이스를 선택합니다.

**Note** FDM 관리 장치는 IP 주소당 하나의 syslog 개체를 지원하므로 TCP와 UDP 사용 중에서 선택해야 합니다.

단계 5 **Add(추가)**를 클릭합니다.

### What to do next

SaaS(Secure Logging Analytics)를 구현하고 보안 이벤트 커넥터를 통해 Cisco Cloud로 이벤트를 전송하는 기존 CDO 고객 워크플로우.

## URL 개체

URL 개체 및 URL 그룹은 Firepower 디바이스에서 사용됩니다. URL 개체 및 그룹(URL 개체로 총칭)을 사용하여 웹 요청의 URL 또는 IP 주소를 정의합니다. 이러한 개체를 사용하여 액세스 제어 정책에서 수동 URL 필터링 또는 보안 인텔리전스 정책에서 차단 기능을 구현할 수 있습니다. URL 개체는 단일 URL 또는 IP 주소를 정의하는 반면 URL 그룹은 여러 URL 또는 IP 주소를 정의할 수 있습니다.

시작하기 전에

URL 개체를 생성할 때는 다음 사항에 유의하십시오.

- 경로를 포함하지 않는 경우(즉, URL에 / 문자가 없음), 이 일치하는 서버의 호스트 이름만을 기준으로 합니다. 호스트 이름은 // 구분자 뒷부분 또는 호스트 이름의 의 뒷부분이 같아야 일치하는 것으로 간주됩니다. 예를 들어 ign.com은 ign.com 및 www.ign.com과 일치하지만 verisign.com과는 일치하지 않습니다.
- 하나 이상의 / 문자를 포함하는 경우, 전체 URL 문자열이 서버 이름, 경로 및 쿼리 파라미터를 비롯한 부분 문자열 일치에 사용됩니다. 그러나 서버가 재구성되고 페이지가 새 경로로 이동될 수 있으므로 개별 웹 페이지 또는 사이트 일부를 차단하거나 허용하기 위해 수동 URL 필터링은 사용하지 않는 것이 좋습니다. 부분 문자열 일치하는 예기치 않은 일치로 이어질 수도 있으며, 이 경우에는 URL 개체에 포함하는 문자열도 쿼리 파라미터 내부에 있는 의도하지 않은 서버 또는 문자열의 경로와 일치됩니다.
- 시스템에서는 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 다시 말해, 특정 웹 사이트를 차단하는 경우 애플리케이션 조건을 사용하여 특정 프로토콜을 대상으로 하지 않는 한 해당 웹사이트에 대한 HTTP 및 HTTPS 트래픽이 모두 차단됩니다. URL 개체를 생성할 때에는 개체 생성 시 프로토콜을 지정할 필요가 없습니다. 예를 들어 <http://example.com> 대신 [example.com](https://example.com)을 사용합니다.
- URL 개체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 개체를 생성합니다. 또한 주체 CN에 포함된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 [www.example.com](http://www.example.com) 대신 [example.com](https://example.com)을 사용하십시오.

그러나 인증서의 주체 일반 이름은 웹 사이트의 도메인 이름과 아무런 관련도 없을 수 있습니다. 예를 들어, youtube.com 인증서의 주체 일반 이름은 \*.google.com입니다(언제든 변경 가능). URL 필터링 규칙이 암호 해독된 트래픽에서 작동하도록 SSL 암호 해독 정책을 사용하여 HTTPS 트래픽을 암호 해독하면 더 일관성 있는 결과를 얻게 됩니다.



**참고** 인증서 정보를 더 이상 사용할 수 없어 브라우저에서 TLS 세션을 다시 시작하는 경우에는 URL 개체가 HTTPS 트래픽과 일치되지 않습니다. 따라서 URL 개체를 주의하여 구성하더라도 HTTPS 연결에 대해 일관성 없는 결과를 얻을 수 있습니다.

## FDM-관리 URL 개체 생성 또는 편집

URL 개체는 URL 또는 IP 주소를 지정하는 재사용 가능한 구성 요소입니다.

URL 개체를 만들려면 다음 단계를 수행합니다.

### Procedure

- 단계 1 왼쪽 Cisco Defense Orchestrator 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 **Create Object(개체 생성) > FTD > URL**을 클릭합니다.
- 단계 3 개체 이름과 설명을 입력합니다.
- 단계 4 **Create URL object(URL 개체 생성)**를 선택합니다.
- 단계 5 개체의 특정 URL 또는 IP 주소를 입력합니다.
- 단계 6 **Add(추가)**를 클릭합니다.

## Firepower URL 그룹 생성

URL 그룹은 하나 이상의 URL 또는 IP 주소를 나타내는 하나 이상의 URL 개체로 구성될 수 있습니다. Firepower Device Manager 및 Firepower Management Center는 이러한 개체를 "URL 개체"라고도 합니다.

### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 **Create Object(개체 생성) > FTD > URL**을 클릭합니다.
- 단계 3 개체 이름과 설명을 입력합니다.
- 단계 4 **Create a URL group(URL 그룹 생성)**을 선택합니다.

단계 5 **Add Object**(개체 추가)를 클릭하고, 개체를 선택하고, **Select**(선택)을 클릭하여 기존 개체를 추가합니다. 개체를 더 추가하려면 이 단계를 반복합니다.

단계 6 URL 그룹에 URL 개체 추가를 완료하면 **Add**(추가)를 클릭합니다.

## Firepower URL 개체 또는 URL 그룹 편집

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.

단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 3 세부 정보 창에서  를 클릭하여 편집합니다.

단계 4 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 5 **Save**(저장)를 클릭합니다.

단계 6 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

## 보안 정책 관리

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

- [FDM 정책 구성, 358 페이지](#)
- [네트워크 주소 변환, 447 페이지](#)

## FDM 정책 구성

보안 정책에서 네트워크 트래픽을 검사하는 궁극적인 목표는 트래픽을 의도한 대상으로 허용하거나 보안 위협이 식별된 경우 트래픽을 삭제하는 것입니다. CDO를 사용하여 FDM 관리 디바이스 보안 정책의 모든 구성 요소를 관리합니다.

## FDM-관리 액세스 제어 정책

Cisco Defense Orchestrator을 사용하여 FDM 관리 디바이스의 액세스 제어 정책을 관리할 수 있습니다. 액세스 제어 정책은 액세스 제어 규칙을 기준으로 네트워크 트래픽을 평가하여 네트워크 리소스에 대한 액세스를 제어합니다. FDM 관리 디바이스는 액세스 제어 정책에 나타나는 순서대로 액세스 제어 규칙의 기준을 네트워크 트래픽과 비교합니다. 액세스 제어 규칙의 모든 트래픽 조건이

- **Trust(신뢰)** - 어떤 종류든 추가 검사 없이 트래픽을 허용합니다.
- **Allow(허용)** - 정책에서 침입 및 기타 검사 설정이 적용되는 트래픽을 허용합니다.
- **Block(차단)** - 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.

액세스 제어 정책의 규칙이 네트워크 트래픽과 일치하지 않으면 FDM 관리 디바이스는 액세스 제어 규칙 아래에 나열된 기본 작업을 수행합니다.

## FDM-관리 액세스 제어 정책 읽기

### Procedure

- 단계 1 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.
- 단계 2 **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 정책을 읽을 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management(관리)** 창에서 **Policy(정책)**를 선택합니다.
- 단계 5 전체 정책을 보려면 **Filter(필터)** 패널에서 **Show All(모두 표시)**을 클릭합니다.
- 단계 6 규칙 열 표시를 전환하여 열이 더 많거나 적은 규칙을 확인합니다. FDM 관리 디바이스에서 액세스 제어 규칙을 보는 데 익숙한 경우 규칙 열 표시를 전환하여 더 많은 열을 표시합니다.



다음은 정책에서 규칙을 읽는 방법의 예입니다. 모든 트래픽은 일치 항목을 기준으로 먼저 규칙 1에 대해 평가됩니다. 트래픽이 규칙 1과 일치하면 해당 규칙에 대한 작업이 트래픽에 적용됩니다. 내부 영역에서, 아프리카 또는 호주에서, HTTP 또는 HTTPS 포트에서 시작되어 외부 영역으로, 올란드 제도 또는 알바니아로, 임의의 포트로, ABC 또는 About.com으로 도착하는 트래픽은 소스에서 대상으로 이동할 수 있습니다. 또한 침입 정책과 파일 정책이 규칙에 적용되고 규칙의 이벤트가 로깅되고 있음을 확인할 수 있습니다.

#	Name	Action	Source		Destination		Layer 7			Users
			Zones	Networks	Ports	Zones	Networks	Ports	Applications	
1	Allow in...	Allow	inside	Africa Australia	HTTP HTTPS	outside	Aland Islands Albania	Any	ABC About.com	Any
2	Block o...	Block	outside	Any	Any	inside	Any	Any	Social Net... (Sites with Security ... Gambling (Any Reputation)	Any

### 관련 정보:

- [FDM 액세스 제어 정책 구성](#)

## FDM 액세스 제어 정책 구성

FDM 관리 디바이스에는 단일 정책이 있습니다. 해당 정책의 섹션에는 액세스 제어 규칙이 있습니다. 설명의 편의를 위해 액세스 제어 규칙이 있는 정책의 섹션을 액세스 제어 정책이라고 합니다. FDM 관리 디바이스를 온보딩한 후 액세스 제어 정책에 규칙을 추가하거나 편집합니다.

새 FDM 관리 디바이스를 온보딩하는 경우 가져온 정책에 규칙이 없을 수 있습니다. 이 경우 FDM Policy(FDM 정책) 페이지를 열면 "No results found(결과를 찾을 수 없음)" 메시지가 표시됩니다. 이 메시지가 표시되면 FDM 매니지드 디바이스 정책에 규칙 추가를 시작한 다음 CDO에서 디바이스에 구축할 수 있습니다.

시작하기 전에 팁

조건을 액세스 제어 규칙에 추가할 경우 다음 팁을 고려하십시오.




- 규칙에 추가할 때 일부 조건에 대한 맞춤형 개체를 생성할 수 있습니다. 대화 상자에서 맞춤형 개체를 생성할 수 있는 링크를 확인합니다.
- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용하려면 트래픽이 규칙의 모든 조건과 일치해야 합니다. 예를 들어, 특정 호스트 또는 네트워크에 대해 URL 필터링을 수행하는 단일 규칙을 사용할 수 있습니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 어느 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어, 최대 50개의 애플리케이션 또는 애플리케이션 필터에 대해 애플리케이션 제어를 적용하는 단일 규칙을 사용할 수 있습니다. 따라서 단일 조건의 항목 간 관계는 OR이고 조건 유형 간의 관계(예: 소스/대상과 애플리케이션 간의 관계)는 AND가 됩니다.
- 일부 기능을 사용하려면 적절한 Firepower 라이선스를 활성화해야 합니다.
- 일부 편집 작업에서는 편집 모드로 들어가지 않아도 됩니다. 정책 페이지에서 해당 조건 열 내의 + 버튼을 클릭하여 규칙의 조건을 수정하고 팝업 대화 상자에서 원하는 개체 또는 요소를 선택할 수 있습니다. 개체 또는 요소의 **x**를 클릭하면 규칙에서 제거할 수도 있습니다.

### FDM-관리 액세스 제어 정책 생성 또는 편집

Cisco Defense Orchestrator를 사용하여 FDM 관리 액세스 제어 정책을 편집하려면 다음 절차를 수행합니다.

#### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭과 정책을 편집할 액세스 제어 사용자를 클릭합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 선택합니다.
- 단계 5 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 파란색 더하기 버튼  을 클릭합니다.
- 기존 규칙을 편집하려면 규칙을 선택하고 **Actions**(작업) 창에서 **Edit**(편집)  아이콘을 클릭합니다. (간단한 편집은 편집 모드를 시작하지 않고 인라인으로 수행할 수도 있습니다.)
- 더 이상 필요하지 않은 규칙을 삭제하려면 규칙을 선택하고 **Actions**(작업) 창에서 **Remove**(제거)  아이콘을 클릭합니다.
- 정책 내에서 규칙을 이동하려면 액세스 제어 테이블에서 규칙을 선택하고 규칙 행의 끝에 있는 위쪽 또는 아래쪽 화살표를 클릭하여 규칙을 이동합니다.

규칙을 편집하거나 추가하려는 경우 이 절차의 나머지 단계를 계속 진행합니다.

**단계 6 Order(순서) 필드**에서 정책 내 규칙의 위치를 선택합니다. 네트워크 트래픽은 1부터 "마지막"까지 숫자 순서대로 규칙 목록을 기준으로 평가됩니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

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

**단계 7** 규칙 이름을 입력합니다. 영숫자, 공백 및 특수 문자(+, ., \_, -)는 사용할 수 있습니다.

**단계 8** 네트워크 트래픽이 규칙과 일치하는 경우 적용할 작업을 선택합니다.

- **Trust(신뢰)** - 어떤 종류든 추가 검사 없이 트래픽을 허용합니다.
- **Allow(허용)** - 정책에서 침입 및 기타 검사 설정이 적용되는 트래픽을 허용합니다.
- **Block(차단)** - 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.

**단계 9** 다음 탭의 속성을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source(소스) - Source(소스)** 탭을 클릭하고 보안 영역(인터페이스), 네트워크(네트워크, 대륙 및 사용자 지정 지리위치 포함) 또는 네트워크 트래픽이 발생한 포트를 추가하거나 제거합니다. 기본값은 "Any(모두)"입니다.
- **Destination(대상) - Destination(대상)** 탭을 클릭하고 보안 영역(인터페이스), 네트워크(네트워크, 대륙 및 사용자 지정 지리위치 포함) 또는 트래픽이 도착하는 포트를 추가하거나 제거합니다. 기본값은 "Any(모두)"입니다. [FDM-관리 액세스 제어 규칙의 소스 및 대상 기준](#)을 참조하십시오.
- **Applications(애플리케이션) - Application(애플리케이션)** 탭을 클릭하고 웹 애플리케이션 또는 유형, 범주, 태그, 위험이나 비즈니스 관련성에 따라 애플리케이션을 정의하는 필터를 추가하거나 제거합니다. 기본값은 모든 애플리케이션입니다. [FDM-관리 액세스 제어 규칙의 애플리케이션 기준](#)을 참조하십시오.
- **URL - URL** 탭을 클릭하고 웹 요청의 URL 또는 URL 범주를 추가하거나 제거합니다. 기본값은 모든 URL입니다. URL 범주 및 평판 필터를 사용하여 이 조건을 미세 조정하는 방법을 알아보려면 [FDM-관리 액세스 제어 규칙 내 URL 조건](#)을 참조하십시오.

- **Users(사용자)** - Active Directory 영역 개체, 특수 ID(인증 실패, 게스트, 인증 없음, 알 수 없음) 및 firewall device manager에서 규칙에 추가된 사용자 그룹이 규칙 행에 표시되지만, CDO에서는 아직 편집할 수 없습니다.

**Caution** 개별 사용자 개체는 CDO의 액세스 제어 정책 규칙에 아직 표시되지 않습니다. FDM 관리 디바이스에 로그인하여 개별 사용자 개체가 액세스 제어 정책 규칙에 어떤 영향을 미칠 수 있는지 확인합니다.

**단계 10** (선택 사항, Allow(허용) 작업이 있는 규칙의 경우) **Intrusion Policy(침입 정책)** 탭을 클릭하여 트래픽에서 침입 및 익스플로잇을 검사할 침입 검사 정책을 할당합니다. [FDM-관리 액세스 제어 규칙의 침입 정책 설정](#)을 참조하십시오.

- 침입 정책 규칙에 의해 생성된 침입 이벤트를 로깅하려면 디바이스에 대한 ["FDM-관리 디바이스 설정"](#)을 참조하십시오.

**단계 11** (선택 사항, Allow(허용) 작업이 포함된 규칙의 경우) **File Policy(파일 정책)** 탭을 클릭하여 악성코드가 포함된 파일 및 차단해야 하는 파일에 대한 트래픽을 검사하는 파일 정책을 할당합니다. [FDM-관리 액세스 제어 규칙의 파일 정책 설정](#)을 참조하십시오.

- 파일 정책 규칙에 의해 생성된 파일 이벤트를 로깅하려면 디바이스에 대한 ["FDM-관리 디바이스 설정"](#)을 참조하십시오.

**단계 12** (선택 사항) 로깅을 활성화하고 액세스 제어 규칙에 의해 보고된 연결 이벤트를 수집하려면 **Logging(로깅)** 탭을 클릭합니다.

로깅 설정에 대한 자세한 내용은 [FDM-관리 액세스 제어 규칙의 로깅 설정](#)을 참조하십시오.

Cisco Security Analytics and Logging을 구독하는 경우 CDO에서 연결 이벤트를 구성하고 [SaaS\(Secure Logging Analytics\)](#)를 위한 시스템 로그 서버 개체 생성 SEC로 전송할 수 있습니다. 이 기능에 대한 자세한 내용은 [FDM-관리 디바이스에 대한 보안 로깅 분석](#)을 참조하십시오. 테넌트에 온보딩된 모든 SEC에 대해 하나의 시스템 로그 개체를 생성할 수 있지만, 하나의 규칙에 의해 생성된 이벤트만 하나의 SEC를 나타내는 하나의 시스템 로그 개체로 보낼 수 있습니다.

**단계 13** **Save(저장)**를 클릭합니다. 이제 보안 정책에서 특정 규칙을 구성했습니다.

**단계 14** 이제 보안 정책 전체에 대해 **Default Action(기본 작업)**을 구성할 수 있습니다. Default Action(기본 작업)은 네트워크 트래픽이 액세스 제어 정책, 침입 정책 또는 파일/악성코드 정책의 규칙과 일치하지 않는 경우 수행할 작업을 정의합니다.

**단계 15** 정책의 Default Action(기본 작업)을 클릭합니다.

**단계 16** 위의 9단계에서와 같이 침입 정책을 구성합니다.

**단계 17** Default Action(기본 작업)에 의해 생성된 로깅 연결 이벤트를 구성합니다.

Cisco Security Analytics and Logging을 구독하는 경우 [SaaS\(Secure Logging Analytics\)](#)를 위한 시스템 로그 서버 개체 생성 기본 작업으로 생성된 이벤트를 SEC로 보낼 수 있습니다. 이 기능에 대한 자세한 내용은 [FDM-관리 디바이스에 대한 보안 로깅 분석](#)을 참조하십시오. 테넌트에 온보딩된 모든 SEC에 대해 하나의 시스템 로그 개체를 생성할 수 있지만, 규칙에 의해 생성된 이벤트만 하나의 SEC를 나타내는 하나의 시스템 로그 개체로 보낼 수 있습니다.



- 단계 18 (선택 사항) 생성한 규칙에 대해 해당 규칙을 선택하고 Add Comments(코멘트 추가) 필드에 코멘트를 추가할 수 있습니다. 규칙 코멘트에 대한 자세한 내용은 [정책 및 규칙 집합의 규칙에 코멘트 추가](#)를 참조하십시오.
- 단계 19 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 번 변경 사항을 한 번에 구축합니다.


## 액세스 정책 설정 구성

정책 내 특정 규칙이 아닌 액세스 정책에 적용되는 설정을 구성할 수 있습니다.

### 절차

이러한 설정은 정책 내의 특정 규칙이 아닌 액세스 정책 전체에 적용됩니다.

#### 프로시저

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭과 정책을 편집할 액세스 제어 사용자를 클릭합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서  **Policy**(정책)를 선택합니다.
- 단계 5 **Settings**(설정) 아이콘을 클릭하고 다음 설정을 구성합니다.
- **TLS Server Identity Discovery**(TLS 서버 ID 검색) - TLS 1.3 인증서가 암호화됩니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 제어 규칙과 일치하는지 확인하려면 이 옵션을 활성화하는 것이 좋습니다. 설정은 인증서만 암호 해독합니다. 연결은 암호화된 상태로 유지됩니다. 이 옵션을 활성화하면 TLS 1.3 인증서를 해독할 수 있습니다. 해당 SSL 암호 해독 규칙을 생성할 필요가 없습니다. 소프트웨어 버전 6.7 이상을 실행하는 FDM 관리 디바이스에서 사용할 수 있습니다.
  - **Reputation Enforcement on DNS Traffic**(DNS 트래픽에 대한 평판 시행) - URL 필터링 범주 및 평판 규칙을 DNS 조회 요청에 적용하려면 이 옵션을 활성화합니다. 조회 요청의 FQDN(Fully Qualified Domain Name)에 차단 중인 범주 및 평판이 있는 경우 시스템은 DNS 응답을 차단합니다. 사용자는 DNS 확인을 받지 않으므로 연결을 완료할 수 없습니다. 웹 이외의 트래픽에 URL 범주 및 평판 필터링을 적용하려면 이 옵션을 사용합니다. 자세한 내용은 DNS 요청 필터링을 참조하십시오. 소프트웨어 버전 7.0 이상을 실행하는 FDM 관리 디바이스에서 사용할 수 있습니다.
- 단계 6 **Save**(저장)를 클릭합니다.

## TLS 서버 ID 검색 정보


보통 TLS 1.3 인증서가 암호화됩니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호

호화된 연결이 올바른 액세스 제어 규칙과 일치하도록 하려면 초기 애플리케이션 탐지 및 URL 분류를 사용하는 것이 좋습니다. 이 설정은 인증서만 암호 해독합니다. 연결은 암호화된 상태로 유지됩니다.



**Note** 이 기능은 현재 소프트웨어 버전 6.7 이상에서 실행되는 FDM 관리 디바이스에서 사용할 수 있습니다.

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭과 정책을 편집할 액세스 제어 사용자를 클릭합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 선택합니다.
- 단계 5 설정  버튼을 클릭합니다.
- 단계 6 **TLS Server Identity Discovery**(TLS 서버 ID 검색) 옆에 있는 슬라이더를 클릭하여 암호화된 연결에 대한 초기 애플리케이션 탐지 및 URL 분류를 활성화합니다.
- 단계 7 **Save**(저장)를 클릭합니다.

## FDM-관리 액세스 제어 규칙 복사

이 절차를 사용하여 현재 위치에서 액세스 제어 규칙을 복사하여 동일한 정책의 새 위치에 붙여넣거나 다른 FDM 관리 디바이스의 정책에 붙여넣어 액세스 제어 규칙을 복사합니다. 정책의 다른 규칙 앞이나 뒤에 규칙을 붙여넣을 수 있습니다. 그러면 규칙이 정책 내에서 적절한 순서로 네트워크 트래픽을 평가합니다.

디바이스 내에서 규칙 복사

FDM 관리 디바이스의 규칙을 복사하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 정책을 편집할 FDM 관리 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다.
- 단계 5 복사할 액세스 제어 규칙을 하나 이상 선택하고 오른쪽의 **Actions**(작업) 창에서 **Copy**(복사)를 클릭합니다.

단계 6 규칙을 붙여넣을 정책에서 복사한 규칙이 앞이나 뒤에 있어야 하는 규칙을 선택하고 **Actions**(작업) 창에서 다음 옵션 중 하나를 클릭합니다.

- **Paste Before**(앞에 붙여넣기)는 하나 이상의 복사된 규칙을 선택한 규칙 위에 자동으로 붙여넣습니다. 이에 따라 복사한 규칙은 그 위에 정렬됩니다.
- **Paste After**(다음에 붙여넣기)는 하나 이상의 복사한 규칙을 선택한 규칙 아래에 자동으로 붙여넣습니다. 이에 따라 복사한 규칙은 그 아래에 정렬됩니다.

필요한 위치에서 붙여넣기 작업을 여러 번 수행할 수 있습니다.

**Note** FDM 관리 디바이스 내에 규칙을 붙여넣을 때 동일한 이름의 규칙이 있는 경우 원래 이름에 '-Copy'가 추가됩니다. 이름을 바꾼 이름도 있는 경우 원래 이름에 '- Copy n'이 추가됩니다. 예를 들어 'rule name - Copy 2'와 같습니다.

단계 7 변경 사항을 검토하고 지금 **CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축하십시오.

한 FDM-관리 디바이스 정책에서 다른 FDM-관리 디바이스 정책으로 규칙 복사

한 FDM 관리 디바이스 정책에서 다른 FDM 관리 디바이스 정책으로 규칙을 복사하면 해당 규칙과 연결된 개체도 새 FDM 관리 디바이스에 복사됩니다.

CDO는 규칙을 붙여넣을 때 일부 조건을 검증합니다. 자세한 내용은 [다른 디바이스에 규칙을 붙여넣을 때의 개체 동작](#)을 참조하십시오.



#### Important

중요: CDO를 사용하면 두 디바이스의 동일한 소프트웨어 버전이 같은 경우에만 한 FDM 관리 디바이스에서 다른 FDM 관리 디바이스로 규칙을 복사할 수 있습니다. 소프트웨어 버전이 다른 경우, 규칙을 붙여넣으려고 할 때 "Rules could not be pasted because they are not compatible with the version of this device(규칙이 이 디바이스의 버전과 호환되지 않기 때문에 규칙을 붙여넣을 수 없음)" 오류가 나타납니다. **Details**(세부 정보) 링크를 클릭하여 세부 정보를 확인할 수 있습니다.

규칙을 다른 FDM 관리 디바이스로 복사하려면 다음 절차를 따르십시오.

#### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 규칙을 복사할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다.
- 단계 5 복사할 액세스 제어 규칙을 하나 이상 선택하고 오른쪽의 **Actions**(작업) 창에서 **Copy**(복사)를 클릭합니다.

- 단계 6 **Inventory**(재고 목록)를 클릭하고 규칙을 붙여넣을 FDM 관리 디바이스로 이동합니다.
- 단계 7 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다.
- 단계 8 방금 복사한 규칙을 붙여넣을 정책에서 복사한 규칙이 앞이나 뒤에 와야 하는 규칙을 선택하고 **Actions**(작업) 창에서 **Paste Before**(앞에 붙여넣기) 또는 **Paste After**(뒤에 붙여넣기)를 클릭합니다.
- 단계 9 복사한 규칙을 붙여넣을 액세스 제어 규칙을 선택하고 **Actions**(작업) 창에서 다음 옵션 중 하나를 클릭합니다.

- **Paste Before**(앞에 붙여넣기)는 자동으로 선택한 규칙 위에 하나 이상의 규칙을 추가하므로, 복사한 규칙은 선택한 규칙보다 먼저 네트워크 트래픽을 평가합니다.
- **Paste After**(뒤에 붙여넣기)는 자동으로 선택한 규칙 아래에 하나 이상의 규칙을 추가하므로, 복사한 규칙은 선택한 규칙 이후에 네트워크 트래픽을 평가합니다.

필요한 위치에서 붙여넣기 작업을 여러 번 수행할 수 있습니다.

**Note** 규칙을 다른 FDM 관리 디바이스에 붙여넣을 때 동일한 이름의 규칙이 있는 경우 원래 이름에 '-Copy'가 추가됩니다. 이름을 바꾼 이름도 있는 경우 원래 이름에 '- Copy n'이 추가됩니다. 예를 들어 'rule name-Copy 2'와 같습니다.

- 단계 10 한 FDM 관리 디바이스에서 다른 디바이스로 규칙을 복사할 때 대상 디바이스의 구성 상태는 'Not Synced(동기화되지 않음)' 상태가 됩니다. 변경 사항을 검토하고 지금 **CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축하십시오.

관련 정보:

- [FDM-관리 액세스 제어 규칙 이동](#)
- [다른 디바이스에 규칙을 붙여넣을 때의 개체 동작](#)

## FDM-관리 액세스 제어 규칙 이동

이 기능을 사용하여 액세스 제어 규칙을 정책의 현재 위치에서 잘라내어 동일한 정책의 새 위치 또는 다른 FDM 관리 디바이스의 정책에 붙여넣는 방식으로 이동할 수 있습니다. 정책의 다른 규칙 앞이나 뒤에 규칙을 붙여넣을 수 있습니다. 그러면 규칙이 정책 내에서 적절한 순서로 네트워크 트래픽을 평가합니다.

디바이스 내에서 규칙 이동

FDM 관리 디바이스의 규칙을 이동하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 정책을 편집할 FDM 관리 디바이스를 선택합니다.

- 단계 4 오른쪽의 **Management(관리)** 창에서 **Policy(정책)**를 클릭합니다.
- 단계 5 이동할 액세스 제어 규칙을 하나 이상 선택하고 오른쪽의 **Actions(작업)** 창에서 **Cut(잘라내기)**을 클릭합니다. 선택한 규칙은 노란색으로 강조 표시됩니다. 참고: 선택을 취소하려면 규칙을 선택하고 **Copy(복사)**를 클릭합니다.
- 단계 6 방금 잘라낸 규칙을 붙여넣을 정책에서 잘라낸 규칙이 앞이나 뒤에 있어야 하는 규칙을 선택하고 **Actions(작업)** 창에서 다음 옵션 중 하나를 클릭합니다.

- **Paste Before(앞에 붙여넣기)**는 자동으로 선택한 규칙 위에 하나 이상의 규칙을 붙여넣으므로, 잘라낸 규칙은 선택한 규칙보다 먼저 네트워크 트래픽을 평가합니다.
- **Paste After(뒤에 붙여넣기)**는 자동으로 선택한 규칙 아래에 하나 이상의 규칙을 붙여넣으므로, 잘라낸 규칙은 선택한 규칙 이후에 네트워크 트래픽을 평가합니다.

필요한 위치에서 붙여넣기 작업을 여러 번 수행할 수 있습니다.

**Note** FDM 관리 디바이스 내에 규칙을 붙여넣을 때 동일한 이름의 규칙이 있는 경우 원래 이름에 '-Copy'가 추가됩니다. 이름을 바꾼 이름도 있는 경우 원래 이름에 '- Copy n'이 추가됩니다. 예를 들어 'rule name - Copy 2'와 같습니다.

- 단계 7 변경 사항을 검토하고 지금 **CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축하십시오.

## 한 FDM-관리 디바이스 정책에서 다른 FDM-관리 디바이스 정책으로 규칙 이동

한 FDM 관리 디바이스 정책에서 다른 FDM 관리 디바이스 정책으로 규칙을 이동하면 해당 규칙과 연결된 개체도 새 FDM 관리 디바이스에 복사됩니다.

CDO는 규칙을 붙여넣을 때 일부 조건을 검증합니다. 이러한 조건에 대한 자세한 내용은 [다른 디바이스에 규칙을 붙여넣을 때의 개체 동작](#)을 참조하십시오.

규칙을 다른 FDM 관리 디바이스로 이동하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.
- 단계 2 **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 규칙을 복사할 FDM 관리 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management(관리)** 창에서 **Policy(정책)**를 클릭합니다.
- 단계 5 이동할 액세스 제어 규칙을 하나 이상 선택하고 오른쪽의 **Actions(작업)** 창에서 **Cut(잘라내기)**을 클릭합니다.
- 단계 6 **Inventory(재고 목록)**를 클릭하고 하나 이상의 선택한 규칙을 옮길 FDM 관리 디바이스로 이동합니다.
- 단계 7 오른쪽의 **Management(관리)** 창에서 **Policy(정책)**를 클릭합니다.

**단계 8** 방금 잘라낸 규칙을 붙여넣을 정책에서 잘라낸 규칙이 앞이나 뒤에 와야 하는 규칙을 선택하고 **Actions**(작업) 창에서 **Paste Before**(앞에 붙여넣기) 또는 **Paste After**(뒤에 붙여넣기)를 클릭합니다.

- **Paste Before**(앞에 붙여넣기)는 자동으로 선택한 규칙 위에 하나 이상의 규칙을 추가하므로, 잘라낸 규칙은 선택한 규칙보다 먼저 네트워크 트래픽을 평가합니다.
- **Paste After**(뒤에 붙여넣기)는 자동으로 선택한 규칙 아래에 하나 이상의 규칙을 추가하므로, 잘라낸 규칙은 선택한 규칙 이후에 네트워크 트래픽을 평가합니다.

필요한 위치에서 붙여넣기 작업을 여러 번 수행할 수 있습니다.

**Note** FDM 관리 디바이스 내에 규칙을 붙여넣을 때 동일한 이름의 규칙이 있는 경우 원래 이름에 '-Copy'가 추가됩니다. 이름을 바꾼 이름도 있는 경우 원래 이름에 '- Copy n'이 추가됩니다. 예를 들어 'rule name - Copy 2'와 같습니다.

**단계 9** 한 FDM 관리 디바이스에서 다른 디바이스로 규칙을 복사할 때 소스 및 대상 디바이스의 구성 상태는 'Not Synced(동기화되지 않음)' 상태가 됩니다. 변경 사항을 검토하고 지금 **CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축하십시오.

관련 정보:

- [FDM-관리 액세스 제어 규칙 복사](#)
- [다른 디바이스에 규칙을 붙여넣을 때의 개체 동작](#)

## 다른 디바이스에 규칙을 붙여넣을 때의 개체 동작

잘라내거나 복사한 규칙에 개체가 포함되어 있고 이러한 규칙을 다른 FDM 관리 디바이스 정책에 붙여넣으면, CDO는 다음 조건 중 하나가 충족될 때 해당 규칙의 개체를 대상 FDM 관리 디바이스에 복사합니다.

모든 개체 유형의 경우(보안 영역 제외)

- 대상 디바이스에 개체가 포함되어 있지 않습니다. 이 경우 CDO는 먼저 대상 디바이스에서 개체를 생성한 다음 규칙을 붙여넣습니다.
- 대상 디바이스에 소스 디바이스와 이름 및 값이 동일한 개체가 포함되어 있습니다.

보안 영역 개체의 경우

- 대상 디바이스에 소스와 이름 및 인터페이스가 동일한 보안 영역 개체가 포함되어 있습니다.
- 대상 디바이스에 동일한 보안 영역 개체가 포함되어 있지 않으며 대상에서 사용할 인터페이스가 있습니다.
- 대상 디바이스에 비어 있는 상태로 대상에서 사용할 인터페이스가 있는 보안 영역 개체가 포함되어 있습니다.

**AD(Active Directory)** 영역이 있는 개체의 경우

- CDO는 동일한 이름의 영역이 대상 디바이스에 이미 있는 경우에만 AD(Active Directory) 영역 개체와 함께 규칙을 붙여넣습니다.



**Important** 다음과 같은 경우 붙여넣기 작업이 실패합니다.

- 두 디바이스 버전 간에 취약성, 지리위치, 침입 또는 URL 데이터베이스에 차이가 있는 경우 CDO는 대상 디바이스에 규칙을 붙여넣을 수 없습니다. 새 디바이스에서 수동으로 규칙을 다시 생성해야 합니다.
- 추가하려는 규칙에 'management-only' 유형의 인터페이스를 포함하는 보안 영역이 있는 경우.

관련 정보:

- [FDM-관리 액세스 제어 규칙 복사](#)
- [FDM-관리 액세스 제어 규칙 이동](#)

## FDM-관리 액세스 제어 규칙의 소스 및 대상 기준

액세스 규칙의 소스 및 대상 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소나 IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 프로토콜과 포트를 정의합니다. 기본값은 모든 영역, 주소, 지리적 위치, 프로토콜 및 포트입니다.

액세스 제어 규칙에서 소스 또는 대상 조건을 수정하려면 **FDM 액세스 제어 정책 구성**의 절차를 사용하여 규칙을 편집할 수 있습니다. 단순 편집은 편집 모드로 들어가지 않고 수행할 수 있습니다. 정책 페이지에서 규칙을 선택하고 소스 또는 대상 조건 열 내에서 + 버튼을 클릭하고 팝업 대화 상자에서 새 개체 또는 요소를 선택하여 규칙의 조건을 수정할 수 있습니다. 개체 또는 요소의 **x**를 클릭하면 규칙에서 제거할 수도 있습니다.

다음 기준을 사용하여 규칙과 일치하는 소스 및 대상을 식별할 수 있습니다.

소스 영역, 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우가 이 기준을 사용해야 합니다. 예를 들어 내부 호스트로 이동하는 모든 트래픽에서 침입을 검사하려는

경우에는 내부 영역을 Destination Zones(대상 영역)로 선택하고 소스 영역은 비워 둡니다. 규칙에서 침입 필터링을 구현하려면 규칙 작업이 Allow(허용)여야 하며 규칙에서 침입 정책을 선택해야 합니다.



**Note** 단일 규칙에서 패시브 보안 영역과 라우팅 보안 영역을 함께 사용할 수는 없습니다. 또한 패시브 보안 영역은 소스 영역으로만 지정할 수 있으며 대상 영역으로 지정할 수는 없습니다.

#### 소스 네트워크, 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다. FQDN(Fully Qualified Domain Name)을 사용하여 주소를 정의하는 개체를 사용할 수 있습니다. 주소는 DNS 조회를 통해 확인됩니다.
- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.



**Note** 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다.

#### 소스 포트, 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP/UDP의 경우 여기에는 포트가 포함될 수 있습니다. ICMP의 경우에는 코드와 유형이 포함될 수 있습니다.

- 특정 프로토콜이나 포트에서 나오는 트래픽을 일치시키려면 소스 포트를 구성합니다. 소스 포트는 TCP/UDP 전용일 수 있습니다.
- 특정 프로토콜이나 포트로 향하는 트래픽을 일치시키려면 대상 포트/프로토콜을 구성합니다. 조건에 대상 포트만 추가할 경우, 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다.



ICMP 및 기타 비TCP/UDP 사양은 대상 포트에서만 허용되며 소스 포트에서는 허용되지 않습니다.

- 특정 TCP/UDP 포트에서 발생하는 트래픽과 특정 TCP/UDP 포트에 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 조건에 소스 및 대상 포트를 모두 추가한 경우, 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.


## FDM-관리 액세스 제어 규칙 내 URL 조건

액세스 제어 규칙의 URL 조건은 웹 요청에 사용되는 URL 또는 요청된 URL이 속하는 범주를 정의합니다. 범주가 일치하는 경우 허용하거나 차단할 사이트의 상대적 평판을 지정할 수도 있습니다. 기본적으로는 모든 URL이 허용됩니다.

URL 카테고리 및 평판을 통해 액세스 제어 규칙의 URL 조건을 신속하게 만들 수 있습니다. 예를 들어 모든 게임 사이트를 차단하거나 모든 높은 위험의 소셜 네트워킹 사이트를 차단할 수 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL 검색을 시도하는 모든 경우, 세션이 차단됩니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 예상대로 제어할 수 있습니다. 마지막으로, Cisco의 위협 인텔리전스는 새로운 URL, 새로운 범주 및 기존 URL의 새로운 범주와 위험이 적용되어 지속적으로 업데이트되므로 시스템은 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 사이트는 새로운 정책을 업데이트하고 구축하는 것보다 빠르게 나타났다가 사라질 수 있습니다.

액세스 제어 규칙에서 URL 및 URL 범주 조건을 수정하려면 **FDM 액세스 제어 정책 구성**의 절차를 사용하여 규칙을 편집할 수 있습니다. 단순 편집은 편집 모드로 들어가지 않고 수행할 수 있습니다. 정책 페이지에서 규칙을 선택하고 URL 조건 열에서 + 버튼을 클릭한 다음 팝업 대화 상자에서 새 개체, 요소, URL 평판 또는 URL 범주를 선택하여 규칙의 URL 조건을 수정할 수 있습니다. 개체 또는 요소의 **x**를 클릭하면 규칙에서 제거할 수도 있습니다.

과관색 더하기  아이콘을 클릭하고 URL 개체, 그룹 또는 URL 범주를 선택한 후 **Save(저장)**를 클릭합니다. 필요한 URL 개체가 없는 경우 **Create New Object(새 개체 생성)**를 클릭할 수 있습니다. URL 개체에 대한 자세한 내용은 **FDM-관리 URL 개체 생성 또는 편집**을 참조하십시오.

### URL 필터링의 라이선스 요건


URL 필터링을 사용하려면 FDM 관리 디바이스에서 **URL** 라이선스를 활성화해야 합니다.

### 규칙에서 사용되는 URL 범주에 대한 평판 지정

기본적으로 URL 범주의 모든 URL은 규칙에 의해 동일한 방식으로 처리됩니다. 예를 들어, 소셜 네트워크 URL을 차단하는 규칙이 있는 경우 평판에 관계없이 모든 URL을 차단합니다. 고위험 소셜 네트워크 사이트만 차단하도록 이 설정을 조정할 수 있습니다. 마찬가지로, 고위험 사이트를 제외한 URL 범주의 모든 URL을 허용할 수 있습니다.

액세스 제어 규칙의 URL 범주에 평판 필터를 사용하려면 다음 절차를 수행합니다.

## Procedure

- 단계 1 FTD Policy(FTD 정책) 페이지에서 편집할 규칙을 선택합니다.
- 단계 2 **Edit**(편집)을 클릭합니다.
- 단계 3 **URLs(URL)** 탭을 클릭합니다.
- 단계 4 파란색 더하기  버튼을 클릭하고 URL 범주를 선택합니다.
- 단계 5 **Apply Reputation to Selected Categories**(선택한 범주에 평판 적용) 또는 방금 선택한 URL 범주에서 **Any Reputation**(모든 평판) 링크를 클릭합니다.
- 단계 6 **Any Reputation**(모든 평판) 체크 박스의 선택을 취소합니다.
- 단계 7 평판을 기준으로 URL 필터링:
  - 규칙에 차단 작업이 있는 경우 평판 슬라이더를 오른쪽으로 밀어 평판이 빨간색으로 표시된 사이트만 차단합니다. 예를 들어 슬라이더를 "Sites with Security Risks(보안 위험이 있는 사이트)"로 이동하면 차단 규칙이 "Sites with Security Risks(보안 위험이 있는 사이트)", "Suspicious Sites(의심스러운 사이트)", "High-Risk Sites(고위험 사이트)"를 차단하지만, "Well-known Sites(잘 알려진 사이트)" 및 "Benign Sites(무해한 사이트)"의 트래픽은 허용합니다.
  - 규칙에 허용 작업이 있는 경우 평판 슬라이더를 오른쪽으로 밀어 평판이 녹색으로 표시된 사이트만 허용합니다. 예를 들어 슬라이더를 "Benign Sites(무해한 사이트)"로 이동하면 규칙이 "Well-known Sites(잘 알려진 사이트)" 및 "Benign Sites(무해한 사이트)"의 트래픽을 허용하지만, "Sites with Security Risks(보안 위험이 있는 사이트)", "Suspicious Sites(의심스러운 사이트)", "High-Risk Sites(고위험 사이트)"의 트래픽은 차단합니다.
- 단계 8 **Save**(저장)를 클릭합니다.
- 단계 9 **Select**(선택)를 클릭합니다.
- 단계 10 **Save**(저장)를 클릭합니다.
- 단계 11 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## FDM-관리 액세스 제어 규칙의 침입 정책 설정

Cisco는 Firepower System에서 여러 침입 정책을 제공합니다. 이러한 정책은 Cisco Talos Security Intelligence and Research Group에서 설계했습니다. 여기서는 고급 설정과 침입 및 전처리기 규칙 구분 상태를 설정합니다.

침입 정책을 위한 라이선스 및 작업 요건

- 라이선스 - 규칙에 침입 정책을 추가하려면 FDM 관리 디바이스에서 라이선스를 활성화해야 합니다.
- 규칙 작업 - 트래픽을 허용하는 규칙에 대해서만 침입 및 파일 정책을 구성할 수 있습니다. 트래픽을 **trust**(신뢰) 또는 **block**(차단)하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또

한, 액세스 제어 정책의 기본 작업이 허용이면 침입 정책은 구성할 수 있지만 파일 정책은 구성할 수 없습니다.

액세스 제어 규칙에 사용 가능한 침입 정책

트래픽을 허용하는 액세스 제어 규칙의 경우 다음 침입 정책 중 하나를 선택하여 트래픽에서 침입 및 익스플로잇을 검사할 수 있습니다. 침입 정책은 패킷을 기반으로 디코딩된 패킷에서 공격을 검사하며 악의적인 트래픽을 차단하거나 변경할 수 있습니다.

정책은 안전성이 가장 낮은 항목부터 가장 높은 항목 순서로 나열됩니다.

- **Connectivity over Security**(연결이 보안에 우선함) - 모든 리소스에 접근할 수 있는 연결이 네트워크 인프라 보안에 우선하는 조직을 위해 작성된 정책입니다. 침입 정책은 Security Over Connectivity(보안이 연결에 우선함)에서 활성화된 것보다 훨씬 더 적은 규칙을 활성화합니다. 트래픽을 차단하는 가장 중요한 규칙만 사용 설정됩니다. 네트워크의 보안을 크게 신뢰하는 경우 어느 정도 침입 차단을 적용하려면 이 정책을 선택합니다.
- **Balanced Security and Connectivity**(보안과 연결의 균형 유지) - 전반적인 네트워크 성능과 네트워크 인프라 보안의 균형을 유지할 수 있도록 설계된 정책입니다. 이 정책은 대부분의 네트워크에 적합합니다. 침입 방지를 적용하려는 대부분의 상황에 대해 이 정책을 선택합니다.
- **Security over Connectivity**(보안이 연결에 우선함) - 네트워크 인프라 보안이 사용자 편의에 우선하는 조직을 위해 작성된 정책입니다. 침입 정책은 적합한 트래픽에 대해 경계하거나 중단할 수 있는 다양한 네트워크 이상 침입 규칙을 활성화합니다. 보안이 가장 중요할 때나 트래픽의 위험성이 높을 때는 이 정책을 선택합니다.
- **Maximum Detection**(최대 탐지) - 보안이 연결에 우선함 정책을 통해 지정할 수 있는 것보다 네트워크 인프라 보안이 더욱 강조되는 조직을 위해 작성된 정책이며, 사용하는 경우 운영에 더 큰 영향을 미칠 수 있습니다. 예를 들어 이 침입 정책에서는 악성코드, 익스플로잇 킷, 오래된 일반적인 취약점, 통제되지 않은 알려진 익스플로잇 등 다수의 위협 범주에서 규칙을 활성화합니다. 이 정책을 선택할 경우 정상적인 트래픽이 너무 많이 삭제되지 않는지 신중하게 평가해야 합니다.

관련 정보

- [FDM-관리 액세스 제어 정책의 침입, 파일 및 악성코드 검사](#)

## FDM-관리 액세스 제어 규칙의 파일 정책 설정

AMP for Firepower(Advanced Malware Protection for Firepower)를 사용하여 악성 소프트웨어, 즉 악성 코드를 탐지할 때 파일 정책을 사용합니다. 파일 제어를 수행하는 데에도 파일 정책을 사용할 수 있습니다. 그러면 파일에 악성코드가 있는지와 관계없이 특정 유형의 모든 파일에 대한 제어가 가능합니다.

AMP for Firepower는 AMP 클라우드를 사용하여 네트워크 트래픽에서 탐지될 가능성이 있는 악성코드의 상태를 검색하고 로컬 악성코드 분석 및 파일 사전 분류 업데이트를 가져옵니다. 관리 인터페이스에는 AMP 클라우드에 연결하고 악성코드 조회를 수행하기 위한 인터넷으로 연결되는 경로가 있어야 합니다. 디바이스는 적합한 파일을 탐지하면 파일의 SHA-256 해시 값을 사용하여 AMP 클라우드에서 파일의 상태를 쿼리합니다. 가능한 상태는 다음과 같습니다.

- **Malware(악성코드)** - AMP 클라우드가 파일을 악성코드로 분류했습니다. 아카이브 파일(예: zip 파일)은 해당 파일 내에 악성코드인 파일이 있으면 악성코드로 표시됩니다.
- **Clean(정상)** - AMP 클라우드가 파일을 악성코드가 포함되어 있지 않은 정상 파일로 분류했습니다. 아카이브 파일은 해당 파일 내의 모든 파일이 정상이면 정상으로 표시됩니다.
- **Unknown(알 수 없음)** - AMP 클라우드가 파일에 상태를 아직 할당하지 않았습니다. 아카이브 파일은 해당 파일 내에 알 수 없는 상태의 파일이 있으면 알 수 없음으로 표시됩니다.
- **Unavailable(사용할 수 없음)** - 시스템이 AMP 클라우드를 쿼리하여 파일의 상태를 확인하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다. "사용할 수 없음" 이벤트가 연속하여 여러 개 표시되는 경우에는 관리 주소에 대한 인터넷 연결이 정상적으로 작동하는지 확인하십시오.

#### 파일 정책을 위한 라이선스 및 작업 요구 사항

라이선스 - 규칙에 파일 정책을 추가하려면 Firepower Device Manager에서 2개의 라이선스를 활성화해야 합니다.

- 라이선스
- 악성코드 라이선스

규칙 작업 - 트래픽을 허용하는 규칙에 대해서만 파일 정책을 구성할 수 있습니다. 트래픽을 trust(신뢰) 또는 block(차단)하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또한, 액세스 제어 정책의 기본 작업이 허용이면 침입 정책은 구성할 수 있지만 파일 정책은 구성할 수 없습니다.

#### 액세스 제어 규칙에 사용 가능한 파일 정책

- **None(없음)** - 전송된 파일에서 악성코드를 평가하지 않으며 파일별 차단을 수행하지 않습니다. 파일 전송을 신뢰할 수 있거나 거의 또는 전혀 수행될 가능성이 없는 규칙 또는 애플리케이션이나 URL 필터링이 네트워크를 적절하게 보호한다고 확신할 수 있는 규칙의 경우 이 옵션을 선택합니다.
- **Block Malware All(악성코드 모두 차단)** - 네트워크를 지나는 파일이 악성코드를 포함하는지 확인한 다음 위협이 되는 파일을 차단하기 위해 AMP 클라우드에 쿼리합니다.
- **Cloud Lookup All(모두 클라우드 조회)** - 네트워크를 지나는 파일의 전송을 허용하되 그 파일의 속성을 확인하고 로깅하기 위해 AMP 클라우드에 쿼리합니다.
- **Office 문서 및 PDF 업로드 차단, 악성코드 기타 차단** - 사용자가 Microsoft Office 문서 및 PDF 업로드를 업로드하지 못하도록 차단합니다. 또한 네트워크를 지나는 파일이 악성코드를 포함하는지 확인한 다음 위협이 되는 파일을 차단하기 위해 AMP 클라우드에 쿼리합니다.
- **Office 문서 업로드 차단, 악성코드 기타 차단** - 사용자가 Microsoft Office 문서를 업로드하지 못하도록 차단합니다. 또한 네트워크를 지나는 파일이 악성코드를 포함하는지 확인한 다음 위협이 되는 파일을 차단하기 위해 AMP 클라우드에 쿼리합니다.

#### 관련 정보:

- [FDM-관리 액세스 제어 규칙의 침입 정책 설정](#)

## FDM-관리 액세스 제어 규칙의 로깅 설정

### 액세스 제어 규칙의 로깅 설정

액세스 규칙의 로깅 설정에 따라 규칙과 일치하는 트래픽에 대해 연결 이벤트가 생성되는지가 결정됩니다.

조직의 보안 및 규정 준수 필요에 따라 연결을 로깅해야 합니다. 사용자가 생성하고 기능을 향상시키는 이벤트의 수를 제한하는 것이 사용자의 목표라면 사용자의 분석에 중요한 연결에 대한 로깅만 사용 설정합니다. 그러나, 자료 수집을 목적으로 사용자의 네트워크 트래픽에 대한 광범위한 견해를 원할 경우, 추가 연결에 대한 로깅을 사용 설정할 수 있습니다.



#### Caution

DoS(서비스 거부) 공격 중에 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며, 데이터베이스가 유사한 다수의 이벤트로 가득 찰 수 있습니다. 차단 규칙에 대한 로깅을 활성화하기 전에 이 규칙이 인터넷 연결 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스용인지를 고려하십시오.

절차

### Procedure

단계 1 **FDM 액세스 제어 정책 구성 Logging**(로깅) 탭을 클릭합니다.

단계 2 로그 작업을 지정합니다.

- 연결 시작 및 종료 시 로깅 - 연결 시작 및 종료 시에 이벤트를 생성합니다. 연결 종료 이벤트는 연결 시작 이벤트에 포함된 모든 항목과 연결 중에 수집되었을 수 있는 모든 정보를 포함하므로 허용하는 트래픽에 대해서는 이 옵션을 선택하지 않는 것이 좋습니다. 두 이벤트를 모두 로깅하면 시스템 성능에 영향을 줄 수 있습니다. 하지만 차단된 트래픽의 경우에는 이 옵션만 사용할 수 있습니다.
- 연결 종료 시 로깅 - 연결 종료 시에 연결 로깅을 활성화하려면 이 옵션을 선택합니다. 허용되는 트래픽이나 신뢰하는 트래픽의 경우 이 옵션을 선택하는 것이 좋습니다.
- 로그 없음 - 규칙에 대해 로깅을 비활성화하려면 이 옵션을 선택합니다. 이는 기본값입니다.

#### Note

액세스 제어 규칙에서 호출한 침입 정책이 침입을 탐지하고 침입 이벤트를 생성하면, 시스템은 규칙의 로깅 구성에 상관없이 침입이 발생한 연결의 종료를 자동으로 로깅합니다. 침입이 차단된 연결을 위한 연결 로그 내 연결 작업은 **Block**(차단)입니다. 그 이유는 **Intrusion**(침입) **Block**(차단)이며, 침입 탐지를 수행하려면 **Allow**(허용) 규칙을 사용해야 합니다.

단계 3 연결 이벤트를 전송할 위치를 지정합니다.

외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우 syslog 서버를 정의하는 서비스 개체를 선택합니다. 필요한 개체가 아직 없는 경우 새로 만들어야 합니다. 자세한 내용은 [시스템 로그 서버 개체 생성 및 편집](#)을 참조하십시오.

디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 시스템 로그 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 애널리틱스 성능이 개선됩니다.

**FDM-관리 디바이스에 대한 보안 로깅 분석** 구독자의 경우:

- SEC(Secure Event Connector)를 통해 Cisco Cloud에 이벤트를 전송하는 경우 [SaaS\(Secure Logging Analytics\)](#)를 위한 [시스템 로그 서버 개체 생성](#) 그러면 파일 정책 및 악성코드 정책 연결 이벤트와 함께 이러한 이벤트를 볼 수 있습니다.
- SEC 없이 Cisco Cloud에 직접 이벤트를 전송하는 경우 이벤트를 로깅할 시점(연결 시작 또는 종료 시)을 지정하되, SEC를 시스템 로그 서버로 지정하지 마십시오.

#### 단계 4 파일 이벤트

금지된 파일 또는 악성코드 이벤트 로깅을 활성화하려면 **Log Files**(로그 파일)를 선택합니다. 이 옵션을 구성하려면 규칙에서 파일 정책을 선택해야 합니다. 규칙에 대해 파일 정책을 선택하는 경우 기본값으로 이 옵션을 활성화합니다. 이 옵션은 활성화된 상태로 유지하는 것이 좋습니다.

금지된 파일을 탐지하면 다음 유형의 이벤트 중 하나가 자동으로 FDM 관리 내부 버퍼에 로깅됩니다.

- 파일 이벤트 - 악성코드 파일을 포함하여 탐지되거나 차단된 파일을 나타냅니다.
- 악성코드 이벤트 - 탐지되거나 차단된 악성코드 파일만 나타냅니다.
- 소급 적용되는 악성코드 이벤트 - 이전에 탐지된 파일에 대한 악성코드 상태가 변경되는 경우 생성됩니다.

파일이 차단된 경우의 연결을 위한 연결 로그 내 연결 작업은 **Block**(차단)입니다. 파일 또는 악성코드 탐지를 수행하려는 경우에도 **Allow**(허용) 규칙을 사용해야 합니다. 연결하는 이유는 파일 모니터링(파일 유형 또는 악성코드가 탐지된 경우), 악성코드 차단 또는 파일 차단(파일이 차단된 경우)입니다.

단계 5 **Save**(저장)를 클릭합니다.

단계 6 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#)하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 보안 그룹 태그(Security Group Tags)

보안 그룹 태그 정보

Cisco ISE(Identity Services Engine)를 사용하여 Cisco TrustSec 네트워크에서 트래픽을 분류하기 위해 **SGT(Security Group Tag)**를 정의하고 사용하는 경우, SGT를 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다. 따라서 IP 주소가 아니라 보안 그룹 멤버십을 기준으로 액세스를 차단하거나 허용할 수 있습니다.

ISE에서는 SGT를 생성하고 호스트 또는 네트워크 IP 주소를 각 태그에 할당할 수 있습니다. SGT를 사용자의 계정에 할당하면 SGT가 사용자의 트래픽에 할당됩니다. ISE 서버에 연결하도록 FDM 관리 디바이스를 구성하고 SGT를 생성한 후 Cisco Defense Orchestrator에서 SGT 그룹을 생성하고 이를 중심으로 액세스 제어 규칙을 작성할 수 있습니다. SGT를 FDM 관리 디바이스에 연결하려면 먼저 ISE의 SXP(SGT Exchange Protocol) 매핑을 구성해야 합니다. 자세한 내용은 현재 실행 중인 버전의 [Cisco ISE\(Identity Services Engine\) 관리자 설명서](#)에서 보안 그룹 태그 교환 프로토콜을 참조하십시오.

FDM 관리 디바이스가 SGT를 액세스 제어 규칙에 대한 트래픽 일치 기준으로 평가하는 경우, 다음 우선순위를 사용합니다.

1. 패킷에 정의된 소스 SGT(있는 경우). 대상 일치는 이 기술을 사용하여 수행되지 않습니다. SGT를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메시지를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.
2. ISE 세션 디렉토리에서 다운로드된 대로 사용자 세션에 할당된 SGT. 이러한 유형의 SGT 일치에 대한 세션 디렉토리 정보를 수신 대기하려면 해당 옵션을 활성화해야 합니다. 그러나 이 옵션은 처음에 ISE ID 소스를 생성할 때 기본적으로 켜집니다. SGT는 소스 또는 대상과 일치할 수 있습니다. 필수 사항은 아니지만 일반적으로 사용자 ID 정보를 수집하기 위해 AD 영역과 함께 ISE ID 소스를 사용하여 패시브 인증 ID 규칙도 설정합니다.
3. SXP를 사용하여 다운로드한 SGT-IP 주소 매핑. IP 주소가 SGT 범위 내에 있는 경우 트래픽은 SGT를 사용하는 액세스 제어 규칙과 일치합니다. SGT는 소스 또는 대상과 일치할 수 있습니다.



#### Note

ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다. SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

#### 버전 지원

CDO는 현재 버전 6.5 이상을 FDM 관리 실행하는 FDM 매니지드 디바이스에서 SGT 및 SGT 그룹을 지원합니다. FDM 관리 디바이스를 사용하면 버전 6.5 이상에서 ISE 서버를 구성하고 연결할 수 있지만 버전 6.7까지는 UI에서 SGT 구성이 지원되지 않습니다.

FDM 관리 UI에서 이는 버전 6.5 이상을 실행하는 FDM 관리 디바이스가 SGT의 SXP 매핑을 다운로드할 수 있지만, 개체 또는 액세스 제어 규칙에 수동으로 추가할 수 없음을 의미합니다. 버전 6.5 또는 버전 6.6을 실행하는 디바이스의 SGT를 변경하려면 ISE UI를 사용해야 합니다. 그러나 버전 6.5를 실행하는 디바이스가 Cisco Defense Orchestrator에 온보딩된 경우 디바이스와 연결된 현재 SGT를 확인하고 SGT 그룹을 생성할 수 있습니다.

#### CDO의 SGT

##### 보안 그룹 태그(Security Group Tags)

SGT는 CDO에서 읽기 전용입니다. CDO에서 SGT를 생성하거나 편집할 수 없습니다. SGT를 생성하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 관리자 설명서](#)를 참조하십시오.

## SGT 그룹



**Note** FDM 관리 디바이스는 SGT 그룹을 SGT 동적 개체로 지칭합니다. CDO에서는 이러한 태그 목록을 현재 SGT 그룹이라고 합니다. FDM 관리 디바이스 또는 ISE UI를 참조하지 않고 CDO에서 SGT 그룹을 생성할 수 있습니다.

SGT 그룹을 사용하여 ISE가 할당한 SGT를 기준으로 소스 또는 대상 주소를 식별합니다. 그 다음 트래픽 일치 기준을 정의하는 목적으로 액세스 제어 규칙의 개체를 사용할 수 있습니다. ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다.

SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

CDO에서 SGT 그룹을 생성하려면 하나 이상의 SGT가 이미 구성되어 있어야 하며, 사용하려는 디바이스의 FDM 관리 콘솔에 대해 ISE 서버에서 SGT 매핑이 구성되어 있어야 합니다. 둘 이상의 FDM 관리 디바이스가 동일한 ISE 서버와 연결된 경우 SGT 또는 SGT 그룹을 둘 이상의 디바이스에 적용할 수 있습니다. 디바이스가 ISE 서버와 연결되지 않은 경우, SGT 개체를 액세스 제어 규칙에 포함하거나 SGT 그룹을 해당 디바이스 설정에 적용할 수 없습니다.

## 규칙의 SGT 그룹

SGT 그룹을 액세스 제어 규칙에 추가할 수 있습니다. 이는 소스 또는 대상 네트워크 개체로 나타납니다. 네트워크가 규칙에서 작동하는 방식에 대한 자세한 내용은 [FDM-관리 액세스 제어 규칙의 소스 및 대상 기준](#)을 참조하십시오.

Objects(개체) 페이지에서 SGT 그룹을 생성할 수 있습니다. 자세한 내용은 [SGT 그룹 생성, on page 167](#)를 참조하십시오.

## SGT 그룹 생성

액세스 제어 규칙에 사용할 수 있는 SGT 그룹을 생성하려면 다음 절차를 사용합니다.

**Before you begin**

SGT(보안 그룹 태그) 그룹을 생성하기 전에 다음 구성 또는 환경을 구성해야 합니다.

- FDM 관리 디바이스는 버전 6.5 이상을 실행해야 합니다.
- SXP 매핑을 구독하고 변경 사항을 구축하도록 ISE ID 소스를 구성해야 합니다. SXP 매핑을 관리하려면 사용 중인 버전 6.7 이상에 대한 [Firepower Device Manager 구성 가이드](#)의 ISE에서 보안 그룹 및 SXP 게시 구성을 참조하십시오.
- 모든 SGT는 ISE에서 생성해야 합니다. SGT를 생성하려면 현재 실행 중인 버전의 [Cisco ISE\(Identity Services Engine\) 구성 설명서](#)를 참조하십시오.



## Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **FTD > Network(네트워크)**를 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 (선택 사항) 설명을 추가합니다.

단계 6 **SGT**를 클릭하고 드롭다운 메뉴를 사용하여 그룹에 포함할 모든 해당 SGT를 선택합니다. SGT 이름을 기준으로 목록을 정렬할 수 있습니다.

단계 7 **Save(저장)**를 클릭합니다.

**Note** CDO에서 SGT를 생성하거나 편집할 수 없으며 SGT 그룹에서 추가하거나 제거할 수만 있습니다. SGT를 생성하거나 편집하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 구성 설명서](#)를 참조하십시오.


## SGT 그룹 편집

SGT 그룹을 편집하려면 다음 절차를 따르십시오.

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 SGT 그룹을 찾습니다.

단계 3 SGT 그룹을 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 SGT 그룹을 편집합니다. 그룹과 관련된 이름, 설명 또는 SGT를 편집합니다.

단계 5 **Save(저장)**를 클릭합니다.

**Note** CDO에서 SGT를 생성하거나 편집할 수 없으며 SGT 그룹에서 추가하거나 제거할 수만 있습니다. SGT를 생성하거나 편집하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 구성 설명서](#)를 참조하십시오.

## 액세스 제어 규칙에 SGT 그룹 추가

액세스 제어 규칙에 SGT 그룹을 추가하려면 다음 절차를 따르십시오.


### Procedure

단계 1 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 **FTD** 탭을 클릭하고 SGT 그룹을 추가할 디바이스를 선택합니다.

단계 4 **Management**(관리) 창에서 **Policy**(정책)를 선택합니다.

단계 5 소스 또는 대상 개체에 대한 파란색 플러스 버튼  을 클릭하고 **SGT** 그룹을 선택합니다.

단계 6 개체 필터 및 검색 필드를 사용하여 편집하려는 SGT 그룹을 찾습니다.

단계 7 **Save**(저장)를 클릭합니다.

단계 8 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

**Note** 추가 SGT 그룹을 생성해야 하는 경우 **Create New Object**(새 개체 생성)를 클릭합니다. **SGT 그룹 생성** 및 규칙에 SGT 그룹 추가에 언급된 필수 정보를 입력하고 SGT 그룹을 규칙에 추가합니다.

## FDM-관리 액세스 제어 규칙의 애플리케이션 기준

액세스 규칙의 애플리케이션 기준은 IP 연결 또는 필터에 사용되는 애플리케이션을 정의하며 유형, 범주, 태그, 위험 또는 사업 타당성에 따라 애플리케이션을 정의합니다. 기본값은 모든 애플리케이션입니다.

규칙에서 개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하고 할 경우, 세션은 차단됩니다.

이와 더불어 Cisco에서는 시스템 및 VDB(Vulnerability Database)를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

규칙에서 애플리케이션 및 필터를 직접 지정하거나 이러한 특성을 정의하는 애플리케이션 필터 개체를 생성할 수 있습니다. 이 두 가지 경우의 사양은 동일하지만, 개체를 사용하면 복잡한 규칙을 생성할 때에도 시스템 제한(기준당 항목 50개)을 유지하기가 더욱 쉽습니다. 애플리케이션 필터 개체 생성에 대한 자세한 내용은 [Firepower 애플리케이션 필터 개체 생성 및 편집](#)을 참조하십시오.

규칙에서 사용되는 애플리케이션 및 애플리케이션 필터를 수정하려면 **FDM-관리 액세스 제어 정책**의 절차를 사용하여 규칙을 편집할 수 있습니다. 단순 편집은 편집 모드로 들어가지 않고 수행할 수 있습니다. 정책 페이지에서 규칙을 선택하고 애플리케이션 조건 열에서 + 버튼을 클릭한 다음, 팝업 대화 상자에서 새 개체 또는 요소를 선택하여 규칙의 애플리케이션 조건을 수정할 수 있습니다. 개체 또는 요소의 **x**를 클릭하면 규칙에서 제거할 수도 있습니다.

## FDM-관리 액세스 제어 정책의 침입, 파일 및 악성코드 검사

침입 정책 및 파일 정책은 트래픽이 원하는 대상에 도달하도록 허용하기 전에 최종 방어선으로 함께 사용됩니다.

- 침입 정책은 시스템의 침입 방지 기능을 제어합니다.

- 파일 정책은 시스템의 파일 제어 및 AMP for Firepower 기능을 제어합니다.

기타 모든 트래픽 처리는 네트워크 트래픽에서 침입, 금지된 파일 및 악성코드를 검사하기 전에 수행됩니다. 침입 또는 파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 트래픽을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 허용하는 규칙에 대해서만 침입 및 파일 정책을 구성할 수 있습니다. 트래픽을 trust(신뢰) 또는 block(차단)하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또한, 액세스 제어 정책의 기본 작업이 허용이면 침입 정책은 구성할 수 있지만 파일 정책은 구성할 수 없습니다.

액세스 제어 규칙으로 처리되는 단일한 연결의 경우, 침입 검사 전에 파일 검사가 이루어집니다. 즉, 시스템에서는 파일 정책 또는 침입에 의해 차단된 파일은 검사하지 않습니다. 파일 검사 내에서 유형을 기준으로 한 간단한 차단은 악성코드 검사 및 차단보다 우선합니다. 세션에서 파일이 탐지되고 차단될 때까지, 세션의 패킷은 침입 검사 대상이 될 수 있습니다.



**Note** 기본적으로, 시스템에서는 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다. 검사는 암호화되지 않은 트래픽에 대해서만 작동합니다.

관련 정보:

- [FDM-관리 액세스 제어 규칙의 침입 정책 설정](#)
- [FDM-관리 액세스 제어 규칙의 파일 정책 설정](#)

## FDM-관리 액세스 제어 규칙의 사용자 지정 IPS 정책

단일 디바이스에 연결된 동일한 사용자 지정 IPS 정책의 인스턴스를 두 개 이상 가질 수 없습니다.




**Note** IPS 정책을 액세스 제어 규칙과 연결하면 통과하는 트래픽이 심층 패킷 검사에 제출됩니다. IPS 정책이 포함된 액세스 제어 규칙에 대해 지원되는 유일한 규칙 작업은 **Allow**(허용)입니다.

사용자 지정 IPS 정책을 FDM 관리 디바이스에 연결하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1** 사용자 지정 IPS 정책을 생성합니다. 자세한 내용은 [Firepower 사용자 지정 IPS 정책 구성](#)을 참조하십시오.
- 단계 2** Cisco Defense Orchestrator 탐색창에서 **Policies**(정책)를 선택합니다. **FTD / Meraki / AWS Policies**(FTD/Meraki/AWS 정책)를 클릭합니다.
- 단계 3** FDM 관리 디바이스 정책 목록을 스크롤하거나 필터링하고 사용자 지정 IPS 정책과 연결할 정책을 선택합니다.

- 단계 4 파란색 더하기  버튼을 클릭합니다.
- 단계 5 **Order**(순서) 필드에서 정책 내 규칙의 위치를 선택합니다. 네트워크 트래픽은 1부터 "마지막"까지 숫자 순서대로 규칙 목록을 기준으로 평가됩니다.
- 단계 6 규칙 이름을 입력합니다. 영숫자, 공백 및 특수 문자(+, ,, \_ , -)는 사용할 수 있습니다.
- 단계 7 **Intrusion Policy**(침입 정책) 탭을 선택합니다. 드롭다운 메뉴를 확장하여 사용 가능한 모든 침입 정책을 확인하고 원하는 사용자 지정 IPS 정책을 선택합니다.
- 단계 8 **Source/Destination**(소스/대상), **URLs, Applications**(애플리케이션), **File Policy**(파일 정책) 탭에서 속성의 조합을 사용하여 트래픽 일치 기준을 정의합니다.
- 단계 9 (선택 사항) 로깅을 활성화하고 액세스 제어 규칙에 의해 보고된 연결 이벤트를 수집하려면 **Logging**(로깅) 탭을 클릭합니다.
- 단계 10 **Save**(저장)를 클릭합니다.
- 단계 11 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## Firepower Threat Defense의 TLS 서버 ID 검색

이제 사용자 환경과 관련하여 제어 및 정확성을 허용하는 위협 방어의 고유한 TLS 서버 ID 검색을 통해 트래픽에서 향상된 URL 필터링 및 애플리케이션 제어를 수행할 수 있습니다. 이 기능이 작동하기 위해 트래픽 암호를 해독할 필요는 없습니다.




**Note** 서버 ID 검색 기능에 대한 지원은 버전 6.7 이상으로 제한됩니다.

### TLS 서버 ID 검색 활성화

FDM 관리 액세스 제어 정책에 대해 TLS 서버 ID 검색 기능을 활성화하거나 비활성화하려면 다음 절차를 수행합니다.

#### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 선택합니다.
- 단계 5 테이블의 오른쪽 상단 모서리에 있는 **Access Policy Settings**(액세스 정책 설정) 기어  아이콘을 클릭합니다.
- 단계 6 토글을 밀어 TLS 서버 ID 검색을 활성화합니다.

단계 7 **Save**(저장)를 클릭합니다.

## Intrusion Prevention System(침입 방지 시스템)

Cisco Talos Intelligence Group(Talos)은 실시간으로 위협을 탐지하고 상관관계를 애널리틱스하며 수십억 개의 파일에 대한 평판 속성을 유지합니다. Cisco IOS IPS(침입 방지 시스템)는 악성 트래픽을 실시간으로 정확하게 식별, 분류 및 삭제하기 위해 Talos의 위협 정보 데이터를 사용하여 네트워크에 대한 공격을 완화하는 인라인 심층 패킷 검사 기능입니다.

Cisco Defense Orchestrator(CDO)에서는 소프트웨어 버전 6.4.x.x~6.6.0.x 및 6.6.1.x를 실행하는 FDM 관리 디바이스에서 IPS 기능을 활성화하고 조정하는 기능을 제공합니다.



**Note** CDO에서는 현재 버전 6.7에서 IPS 규칙 조정을 지원하지 않습니다.

CDO 메뉴 모음에서 **Policies**(정책) > **Signature Overrides**(서명 재정의)로 이동하여 다음 작업을 수행합니다.

- 여러 디바이스에서 재정의의 불일치를 해결합니다.
- 위협 이벤트를 보고 숨깁니다.
- 규칙 작업을 변경하여 위협 이벤트를 처리하는 방법을 재정의합니다.

관련 정보:

- [Firepower 침입 정책 서명 오버라이드](#)
- [위협 이벤트](#)
- [침입 방지 시스템 문제 해결](#)

## 위협 이벤트

위협 이벤트 보고서는 Cisco Talos의 침입 정책 중 하나와 일치한 후 삭제되거나 알림이 생성된 트래픽에 대한 보고서입니다. 대부분의 경우 IPS 규칙을 조정할 필요가 없습니다. 필요한 경우 Cisco Defense Orchestrator에서 일치하는 규칙 작업을 변경하여 이벤트가 처리되는 방식을 오버라이드할 수 있습니다.

Threats(위협) 페이지의 다음 동작에 유의하십시오.

- 표시되는 위협 이벤트는 라이브가 아닙니다. 디바이스는 추가 위협 이벤트에 대해 매시간 폴링됩니다.
- [라이브 이벤트 보기](#) 보기에 포함되지 않은 위협 이벤트는 Cisco Security Analytics and Logging의 일부가 아닙니다.
- 보기에서 숨긴 위협 이벤트를 보려면 필터 아이콘을 클릭하고 숨김 보기 옵션을 선택합니다.

- FDM-관리 디바이스에 대한 보안 로깅 분석 가입자인 경우, Threat Events(위협 이벤트) 테이블에 표시되는 이벤트에는 보안 이벤트 커넥터로 전송된 이벤트가 포함되지 않습니다.

## Procedure

단계 1 탐색창에서 **Monitoring**(모니터링) > **Threats**(위협)를 선택합니다. 표시되는 이벤트를 **개체 필터**하고 소스 IP 주소로 검색할 수 있습니다.

단계 2 위협 이벤트를 클릭하여 오른쪽의 상세정보 패널을 펼칩니다.

- 규칙에 대한 자세한 내용을 보려면 **Rule Details**(규칙 세부 정보) 섹션에서 **Rule Document**(규칙 문서) URL를 클릭합니다.
- 이 이벤트를 숨기려면 **Hide Events**(이벤트 숨기기) 토글 스위치를 선택합니다. 이벤트 처리는 계속 진행되지만 **View Hidden**(숨김 보기)을 클릭하거나 이 이벤트의 숨김을 해제하지 않으면 여기에 표시되지 않습니다.
- 규칙 오버라이드를 편집하려면 **Tune Rule**(규칙 조정)를 클릭합니다. CDO에서 규칙 작업을 변경하면 사전 정의된 모든 정책에 오버라이드가 적용됩니다. 이는 각 규칙이 정책마다 다를 수 있는 FDM 관리 디바이스와는 다릅니다.

**Note** CDO는 소프트웨어 버전 6.4.xx~6.6.0.x 및 6.6.1.x를 실행하는 FDM 관리 디바이스에서 규칙을 조정하는 기능을 제공합니다. CDO는 현재 FDM 관리 버전 6.7에서 규칙 조정을 지원하지 않습니다.

- **Override All**(모두 재정의) 디바이스 풀다운에서 작업을 선택하고 **Save**(저장)를 클릭합니다.

- **Drop**(삭제) - 이 옵션을 선택하면 이 규칙이 트래픽과 일치할 경우 이벤트를 생성한 다음 연결을 삭제합니다. 이 작업을 사용하여 특정 규칙의 보안을 강화합니다. 예를 들어 **Drop**(삭제)을 지정하면 액세스 제어 규칙에 대해 "Connectivity over Security(보안보다 연결 우선)" 정책이 지정된 경우에도 Talos 규칙이 일치할 때 보안이 더 엄격해집니다.
- **Alert**(알림) - 이 옵션을 선택하면 이 규칙이 트래픽과 일치할 경우, 이벤트를 생성하지만 연결을 삭제하지는 않습니다. "알림"의 사용 사례는 트래픽이 차단되었지만 고객이 허용하기를 원하는 경우이며, 규칙을 비활성화하기 전에 알림을 확인합니다.
- **Disabled**(비활성) - 이 옵션을 선택하면 트래픽이 규칙과 일치하지 않습니다. 아무런 이벤트도 생성되지 않습니다. "Disabled(비활성화됨)"의 사용 사례는 보고서에서 오탐을 중지하거나 사용자 환경에 적용되지 않는 규칙을 제거하는 것입니다(예: httpd를 사용하지 않는 경우 Apache httpd 규칙 비활성화).
- **Default**(기본값) - 이 옵션을 선택하면 규칙이 나열된 침입 정책에 대해 Talos에서 할당된 기본 작업으로 규칙을 반환합니다. 예를 들어 침입 규칙을 "Default(기본값)"로 반환하면 해당 작업은 "균형 잡힌 보안 및 연결성" 정책의 "Connectivity over Security(보안에 대한 연결성)" 정책 및 "Block(차단)"에서 "Alert(알림)"에 반환됩니다.

- 디바이스별 규칙 오버라이드를 편집하려면 **Advanced Options**(고급 옵션) 슬라이더를 선택합니다. 이 섹션에는 영향을 받는 디바이스를 확인하고 오버라이드 작업을 선택한 다음 **Save**(저장)를 클릭하여 변경할 수 있는 각 디바이스에 대해 구성된 규칙 작업이 표시됩니다.

- 영향을 받는 디바이스는 소스 디바이스를 나타내지 않습니다. 대신 이벤트를 보고하는 FDM 관리 디바이스가 표시됩니다.

**Note**

- 새로 고침(↻) 버튼을 클릭하여 현재 검색 필터를 기반으로 위협을 표시하는 테이블을 새로 고칩니다.
- 위협의 현재 요약을 쉼표로 구분된 값(.csv) 파일로 다운로드하려면 내보내기(↓) 버튼을 클릭합니다. Microsoft Excel과 같은 스프레드시트 애플리케이션에서 .csv 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다. CDO는 시간, 소스 및 디바이스와 같은 추가 정보를 제외하고 기본 위협 세부 정보를 파일로 내보냅니다.

**단계 3** 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 번 변경 사항을 한 번에 구축합니다.

## Firepower 침입 정책 서명 오버라이드


대부분의 경우 IPS 규칙을 조정할 필요가 없습니다. 필요한 경우 CDO에서 일치하는 규칙 작업을 변경하여 이벤트가 처리되는 방식을 오버라이드할 수 있습니다. CDO는 오버라이드 문제를 해결할 수 있는 옵션을 제공합니다.



### 서명 재정의 관리

#### Procedure

**단계 1** 기본 내비게이션 바에서 **Policies(정책) > Signature Overrides(서명 재정의)**를 클릭합니다. 표시되는 디바이스 및 정책 재정의 정책을 **개체 필터**할 수 있습니다. 이름 또는 침입 규칙 SID로 침입 정책을 검색할 수도 있습니다.

**단계 2** 정책 재정의 정책의 이름을 클릭하여 오른쪽의 세부 정보 패널을 펼칩니다.

**단계 3** **Issues(문제)** 창에서  배지는 재정의가 디바이스 전체에서 일정하지 않음을 나타냅니다. 영향을 받는 디바이스의 수가 포함된 **INCONSISTENT** 필드를 확인할 수 있습니다.

 INCONSISTENT  [Resolve](#) | [Ignore](#)

a) 문제를 무시하려면 **Ignore(무시)**를 클릭합니다. 이렇게 해도 문제가 변경되지는 않지만, **Issues(문제)** 열에서 지표 배지는 제거됩니다.

b) 문제를 해결하려면 **Resolve(해결)**를 클릭합니다. 왼쪽 패널에서 비교할 정책을 선택하고 일관성 있는 재정의와 일관성 없는 재정을 표시합니다.

- 정책을 병합하려면 다음을 수행합니다.

- 모든 디바이스에서 동일한 재정의가 있는 단일 정책으로 통합하려면 **Resolve by Merging(병합하여 해결)**을 클릭합니다.
- OK(확인)**를 클릭합니다.

- 정책 이름을 바꾸려면 다음을 수행합니다.
  1. 정책 섹션에서 **Rename**(이름 변경)을 클릭하고 다른 이름을 지정합니다.
  2. **OK**(확인)를 클릭합니다.
- 정책을 무시하려면 다음을 수행합니다.
  1. 정책 섹션에서 **Ignore**(무시)를 클릭합니다.
  2. **OK**(확인)를 클릭합니다.
- 모든 불일치를 무시하려면 **Ignore All**(모두 무시)을 클릭합니다.

**단계 4** FDM 관리 디바이스를 사용하여 디바이스에서 변경된 개별 Talos 침입 규칙이 있는 경우 **Overrides**(재정의) 창에 해당 규칙이 표시됩니다. **Tune**(조정) 링크를 클릭하고 재정의 작업을 선택하여 침입 규칙에 대한 재정의 작업을 변경할 수 있습니다. 이 작업은 해당 규칙이 사용되는 모든 Talos 침입 정책에 해당 규칙에 적용됩니다. 기본 작업 규칙(기본값)을 복구하도록 선택하는 경우, 환경에 의해 트리거될 때까지 침입 규칙을 다시 조정할 수 없습니다.

- **Connectivity over Security**(연결이 보안에 우선함)
- **Balanced Security and Connectivity**(균형 잡힌 보안 및 연결성)
- **Security over Connectivity**(보안이 연결에 우선함)
- **Maximum Detection**(최대 탐지)

디바이스 간의 일관성을 위해 재정의 작업은 침입 재정의 정책과 연결된 모든 디바이스에 저장됩니다.

재정의 작업의 영향은 다음과 같습니다.

- **Drop**(삭제) - 이 옵션을 선택하면 이 규칙이 트래픽과 일치할 경우 이벤트를 생성한 다음 연결을 삭제합니다. 이 작업을 사용하여 특정 규칙의 보안을 강화합니다. 예를 들어 **Drop**(삭제)을 지정하면 액세스 제어 규칙에 대해 "**Connectivity over Security**(보안보다 연결 우선)" 정책이 지정된 경우에도 Talos 규칙이 일치할 때 보안이 더 엄격해집니다.
- **Alert**(알림) - 이 옵션을 선택하면 이 규칙이 트래픽과 일치할 경우, 이벤트를 생성하지만 연결을 삭제하지는 않습니다. "알림"의 사용 사례는 트래픽이 차단되었지만 고객이 허용하기를 원하는 경우이며, 규칙을 비활성화하기 전에 알림을 확인합니다.
- **Disabled**(비활성) - 이 옵션을 선택하면 트래픽이 규칙과 일치하지 않습니다. 아무런 이벤트도 생성되지 않습니다. "**Disabled**(비활성화됨)"의 사용 사례는 보고서에서 오탐을 중지하거나 사용자 환경에 적용되지 않는 규칙을 제거하는 것입니다(예: httpd를 사용하지 않는 경우 Apache httpd 규칙 비활성화).
- **Default**(기본값) - 이 선택 사항은 규칙의 기본 작업이 Talos 침입 정책 레벨과 다른 경우에만 적용됩니다. 예를 들어, 침입 규칙을 "**Default**(기본값)"로 반환하면 해당 작업은 "**Balanced Security and Connectivity**(균형 잡힌 보안 및 연결성)" 정책의 "**Connectivity over Security**(보안에 대한 연결성)" 정책 및 "**Block**(차단)"에서 "**Alert**(알림)"에 반환됩니다.



- 다음 옵션을 사용하여 규칙 재정의를 편집합니다.
  - **Override for all devices**(모든 디바이스에 대해 재정의) - 이 옵션은 CDO에서 관리하는 모든 디바이스에 필요한 작업을 설정합니다. 드롭다운 메뉴에서 옵션을 선택합니다. 규칙이 다른 침입 재정의 정책에 대해 상이한 재정의 값을 가지는 경우 드롭다운 옵션은 기본적으로 "Multiple(다중)"입니다.
  - **Edit rule overrides by device**(디바이스별 규칙 재정의 편집) - **Advanced Options**(고급 옵션) 슬라이더를 선택하고 **Overrides by Devices**(디바이스별 재정의) 탭을 선택합니다. 이 옵션에서는 각 디바이스에 대해 구성된 규칙 작업을 표시합니다. 이 작업은 영향을 받는 디바이스를 확인하고 재정의 작업을 선택한 다음 **Save**(저장)를 클릭하여 변경할 수 있습니다.
  - **Edit rule overrides by policy**(정책별 규칙 재정의 편집) - **Advanced Options**(고급 옵션) 슬라이더를 선택하고 **All Overrides**(모두 재정의) 탭을 선택합니다. 이 섹션은 테넌트에 둘 이상의 IPS 정책이 구성된 경우에만 적용됩니다. 둘 이상의 디바이스가 연결된 정책을 포함하여 이 페이지에서 모든 IP 정책을 관리할 수 있습니다.

단계 5 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 서명 재정의 생성

FTD 디바이스에서 이미 트리거된 IPS 규칙에 대해서만 서명 재정의 생성할 수 있습니다. CDO에서 서명 재정의 생성하면 재정의는 구성된 작업(**Drop**(삭제), **Alert**(알림), **Disabled**(비활성화됨), **Default**(기본값))을 모든 정책 레벨에 자동으로 적용합니다.

### Procedure

- 단계 1 기본 내비게이션 바에서 **Monitoring**(모니터링) > **Threats**(위협)를 클릭합니다.
- 단계 2 테이블에서 위협을 선택하고 확장합니다. Tune Actions(튜닝 작업) 창에서 **Tune**(튜닝)을 클릭합니다.
- 단계 3 **Firepower 침입 정책 서명 오버라이드** 절차의 4단계에 설명된 대로 규칙을 조정합니다.
- 단계 4 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 서명 재정의 제거

### Procedure

- 단계 1 기본 내비게이션 바에서 **Policies**(정책) > **Signature Overrides**(서명 재정의)를 클릭합니다.
- 단계 2 재정의의 이름을 클릭하여 오른쪽의 세부 정보 패널을 펼칩니다.
- 단계 3 **Overrides**(재정의) 창을 확장하고 제거할 재정의 선택한 다음 **Tune**(조정)을 클릭합니다.

단계 4 기본 작업을 **Default**(기본)로 설정합니다.

단계 5 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 사용자 지정 Firepower 침입 방지 시스템 정책

### 사용자 지정 IPS 정책 정보

버전 6.7이 도입되면서 향상된 Snort 3 처리 엔진을 사용하면 Cisco Talos Intelligence Group(Talos)에서 제공하는 규칙을 사용하여 IPS(침입 방지 시스템) 정책을 생성하고 사용자 지정할 수 있습니다. 모범 사례는 제공된 Talos 정책 템플릿을 기반으로 고유한 정책을 생성하고 규칙 작업을 조정해야 하는 경우 변경하는 것입니다.



**Note** 현재 CDO는 사용자 지정 IPS 규칙을 지원하지 않습니다. Talos에서 제공하는 규칙을 사용하여 사용자 지정 IPS 정책을 생성하고 수정할 수 있지만, 고유한 IPS 규칙을 생성하여 사용자 지정 IPS 정책에 적용할 수는 없습니다.

기본 템플릿에는 동일한 침입 규칙 목록(서명이라고도 함)이 포함되지만, 각 규칙에 대해 수행되는 작업은 다릅니다. 예를 들어 규칙이 한 정책에서는 사용되지만, 다른 정책에서는 사용되지 않을 수 있습니다. 또 다른 예로, 가령 특정 규칙이 차단하지 말아야 할 트래픽을 차단하여 오탐(False Positive)이 지나치게 많이 발생하고 있다는 사실을 알게 될 경우, 보안이 더 낮은 침입 정책으로 전환하지 않고도 규칙을 비활성화할 수 있습니다. 또는 트래픽을 삭제하지 않고 일치 항목에 대해 알리도록 규칙을 변경할 수 있습니다.

### IPS 정책 기본 템플릿

기본 템플릿에는 동일한 침입 규칙 목록(서명이라고도 함)이 포함되지만, 각 규칙에 대해 수행되는 작업은 다릅니다. 예를 들어 어떤 규칙은 어떤 정책에서는 활성화되지만, 다른 정책에서는 비활성화될 수 있습니다. 가령 특정 규칙이 차단하지 말아야 할 트래픽을 차단하여 오탐(False Positive)이 지나치게 많이 발생하고 있다는 사실을 알게 될 경우, 보안이 더 낮은 침입 정책으로 전환하지 않고도 규칙을 비활성화할 수 있습니다. 또는 트래픽을 삭제하지 않고 일치 항목에 대해 알리도록 규칙을 변경할 수 있습니다.

제공되는 기본 템플릿은 네트워크에 필요할 수 있는 보호 유형을 기반으로 제안된 구성입니다. 새 정책을 생성할 때 다음 템플릿 중 하나를 기본으로 사용할 수 있습니다.



**Caution** Snort 3가 활성화된 FDM 관리 디바이스와 함께 제공되는 기본 IPS 정책을 수정하지 마십시오. 아래에 나열된 기본 IPS 정책의 이름과 다른 고유한 이름을 새 정책에 사용하려면 아래의 템플릿을 기반으로 새 사용자 지정 IPS 정책을 생성하는 것이 좋습니다. 정책 문제를 해결해야 하는 경우 Cisco TAC는 쉽게 사용자 지정 정책을 찾아 기본 정책으로 되돌릴 수 있습니다. 이렇게 하면 사용자 지정된 변경 사항이 손실되지 않고 네트워크를 보호할 수 있습니다.

제공되는 기본 템플릿은 네트워크에 필요할 수 있는 보호 유형을 기반으로 제안된 구성입니다. 새 정책을 생성할 때 다음 템플릿 중 하나를 기본으로 사용할 수 있습니다.

- **Maximum Detection(최대 탐지)** - 이러한 정책은 Security over Connectivity(연결보다 보안 우선) 정책에서보다 네트워크 인프라 보안이 강조되는 네트워크에 구축되며, 운영에 더 큰 영향을 미칠 수 있습니다.
- **Security Over Connectivity(연결보다 보안 우선)** - 이러한 정책은 네트워크 인프라 보안이 사용자 편의보다 우선하는 네트워크에 구축됩니다. 침입 정책은 적합한 트래픽에 대해 경계하거나 중단할 수 있는 다양한 네트워크 이상 침입 규칙을 활성화합니다.
- **Balanced Security and Connectivity(균형 잡힌 보안 및 연결성)** - 이 정책은 속도 및 탐지 모두에 구축됩니다. 두 정책을 함께 사용하는 것은 대부분의 네트워크 및 구축 유형에 대해 좋은 시작점이 됩니다.
- **Connectivity Over Security(보안보다 연결 우선)** - 이러한 정책은 연결(모든 리소스에 접근할 수 있는 기능)이 네트워크 인프라 보안보다 우선하는 네트워크에 구축됩니다. 트래픽을 차단하는 가장 중요한 규칙만 사용 설정됩니다.
- **No Rules Active(활성 규칙 없음)** - 정책에 포함된 규칙은 기본적으로 비활성화되어 있습니다.



**Tip** **Maximum Detection(최대 탐지)** 기본 템플릿이 효과적으로 작동하려면 상당한 양의 메모리와 CPU가 필요합니다. CDO에서는 이 템플릿을 사용하여 2100, 4100 또는 가상 디바이스와 같은 모델에 IPS 정책을 구축할 것을 권장합니다.

새로운 취약성이 알려지면 Talos에서 침입 규칙 업데이트를 릴리스합니다. 이러한 규칙 업데이트는 Cisco에서 제공하는 네트워크 애널리틱스 또는 침입 정책을 수정할 수 있으며, 기존 규칙 및 정책 설정에 자동으로 적용되는 새 침입 규칙 및 전처리기 규칙을 제공할 수 있습니다. 또한 규칙 업데이트는 기존 템플릿 기반에서 규칙을 삭제하고 새 규칙 범주를 제공하며 기본 변수 집합을 수정할 수 있습니다.

### IPS 정책 모드

기본적으로 모든 침입 정책은 **Prevention(차단)** 모드에서 작동하여 IPS를 구현합니다. Prevention(차단) 검사 모드에서 연결이 트래픽을 삭제하는 작업을 수행하는 침입 규칙과 일치하는 경우 연결이 능동적으로 차단됩니다.

대신 네트워크에서 침입 정책의 영향을 테스트하려는 경우, 모드를 IDS(Intrusion Detection System)를 구현하는 **Detection(탐지)**으로 변경할 수 있습니다. 이 검사 모드에서 삭제 규칙은 일치하는 연결에 대한 알림을 받는 알림 규칙처럼 처리되지만, 작업 결과는 **Would Have Blocked(차단되었을 수 있음)**가 되고 연결은 실제로 차단되지 않습니다.

### IPS 규칙 그룹 보안 레벨

CDO 정책에 포함된 규칙 그룹의 보안 레벨을 수정할 수 있습니다. 이 보안 레벨은 개별 규칙이 아니라 규칙 그룹의 모든 규칙에 적용됩니다.



**Note** 규칙 그룹의 보안 레벨에 대한 변경 사항은 자동으로 제출되며 되돌릴 수 없습니다. 보안 레벨 수정 사항을 제출하기 위해 **Save(저장)**를 클릭하지 않아도 됩니다. 보안 레벨을 수동으로 다시 변경해야 합니다.

### IPS 규칙 작업

언제든지 규칙 그룹 내의 개별 규칙 또는 여러 규칙의 작업을 수정할 수 있습니다. IPS 규칙은 다음 옵션으로 설정할 수 있습니다.

- **Disabled(비활성화됨)** — 트래픽을 이 규칙과 일치시키지 않습니다. 아무런 이벤트도 생성되지 않습니다.
- **Alert(알림)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하지만 연결을 삭제하지는 않습니다.
- **Drop(삭제)** — 이 규칙이 트래픽과 일치할 경우 이벤트를 생성하고 연결도 삭제합니다.

### FDM 템플릿 및 사용자 지정 IPS 정책

Snort 3가 활성화된 디바이스에서 파생된 템플릿은 Snort 3도 활성화된 디바이스에만 적용할 수 있습니다. Snort 2 및 Snort 3에서 지원되고 처리되는 규칙의 가변성으로 인해 Snort 3로 구성된 템플릿은 Snort 2로 구성된 디바이스를 완전히 지원하고 보호할 수 없습니다. 자세한 내용은 [Snort 3.0으로 업그레이드](#)를 참조하십시오.

ASA 마이그레이션 툴을 사용하여 ASA 구성에서 FDM 템플릿을 생성하는 경우 IPS 정책을 구성하거나 구성 해제하지 않는 것이 좋습니다. ASA 디바이스는 Snort 엔진을 지원하지 않으며 ASA 구성에서 FDM 관리 디바이스 구성으로 IPS 정책을 마이그레이션하면 문제가 발생할 수 있습니다. ASA 마이그레이션 툴을 사용하는 경우 템플릿을 생성 및 구축한 후 디바이스에 대한 사용자 지정 IPS 정책을 생성하는 것이 좋습니다.

템플릿에 대한 자세한 내용은 [FDM-관리 디바이스 템플릿](#)을 참조하십시오.

### 규칙 집합 및 사용자 지정 IPS 정책

규칙 집합은 Snort 3에 대해 구성된 디바이스에서 아직 지원되지 않습니다. 다음과 같은 제한 사항이 적용됩니다.

- Snort 3 지원 디바이스에는 규칙 집합을 연결할 수 없습니다.
- Snort 3이 설치된 기존 디바이스에서는 규칙 집합을 생성할 수 없습니다.
- 사용자 지정 IPS 정책을 규칙 집합에 연결할 수 없습니다.

### 사전 요건

**Intrusion Policies(침입 정책)** 페이지에서 사용 가능한 IPS 정책을 볼 수 있지만, 다음 사전 요건이 없으면 사용자 지정 IPS 정책을 만들거나 수정할 수 없습니다.

## 장치 지원

- Firepower 1000 Series
- Firepower 2100 Series
- Firepower 4100 Series
- AWS를 사용하는 위협 방어 가상
- Azure를 사용하는 위협 방어 가상

## 소프트웨어 지원

s

디바이스는 FDM 버전 6.7 이상 및 Snort 3를 실행해야 합니다.

디바이스에서 6.7 이전 버전을 실행 중인 경우 디바이스를 업그레이드합니다. 자세한 내용은 [단일 FTD 디바이스 업그레이드](#)를 참조하십시오.

디바이스에서 Snort 2와 버전 6.7을 실행 중인 경우 Snort 2.0의 일부 침입 규칙이 Snort 3.0에 없을 수 있습니다. 자세한 내용은 [Snort 3.0으로 업그레이드](#)를 참조하십시오.



**Note** 디바이스에서 실행 중인 소프트웨어 버전 및 Snort 엔진의 버전을 확인하려면 **Inventory**(재고 목록) 페이지에서 디바이스를 찾아 선택하고 **Device Details**(디바이스 세부 정보)를 확인합니다.

## 관련 정보:

- [Firepower 사용자 지정 IPS 정책 구성](#)
- [FDM-관리 액세스 제어 규칙의 사용자 지정 IPS 정책](#)

## Firepower 사용자 지정 IPS 정책 구성

CDO에서 FTD 디바이스에 대한 사용자 지정 IPS 정책을 생성하거나 수정하기 전에 [사용자 지정 Firepower 침입 방지 시스템 정책](#)을 읽어보십시오.

현재 CDO는 사용자 지정 IPS 규칙을 지원하지 않습니다. Talos에서 제공하는 규칙을 사용하여 사용자 지정 IPS 정책을 생성하고 수정할 수 있지만, 고유한 IPS 규칙을 생성하여 사용자 지정 IPS 정책에 적용할 수는 없습니다.

CDO에서 IPS 정책을 생성하거나 수정하는 데 문제가 있는 경우 [침입 방지 시스템 문제 해결](#), on page 767에서 자세한 내용을 참조하십시오.



**Note** 사용자 지정 IPS 정책의 규칙 그룹 내에서 규칙을 삭제하거나 순서를 바꿀 수 없습니다.

## 사용자 지정 IPS 정책 생성

Talos에서 제공하는 IPS 규칙을 사용하여 새 사용자 지정 IPS 정책을 생성하려면 다음 절차를 수행합니다.

### Procedure

단계 1 CDO Navigation(탐색) 창에서 **Policies**(정책)를 클릭합니다.

단계 2 **Intrusion Policies**(침입 정책)를 선택합니다.

단계 3 파란색 더하기  버튼을 클릭합니다.

단계 4 **Base Template**(기본 템플릿)의 드롭다운 메뉴를 확장합니다. 디바이스에서 Snort 3와 함께 버전 7.2를 실행 중인 경우 드롭다운을 확장한 다음 **Choose**(선택)를 클릭하여 템플릿을 선택해야 합니다. 디바이스가 버전 7.1.x 이하를 실행 중인 경우 드롭다운 메뉴를 확장하고 다음 템플릿 중 하나를 선택합니다.

- **Maximum Detection**(최대 탐지) - 이러한 정책은 Security over Connectivity(연결보다 보안 우선) 정책에서보다 네트워크 인프라 보안이 강조되는 네트워크에 구축되며, 운영에 더 큰 영향을 미칠 수 있습니다.

**Tip** **Maximum Detection**(최대 탐지) 기본 템플릿이 효과적으로 작동하려면 상당한 양의 메모리와 CPU가 필요합니다. CDO는 2100, 3100, 4100 또는 위협 방어 가상 등의 모델에 이 템플릿을 사용하여 IPS 정책을 구축할 것을 권장합니다.

- **Security Over Connectivity**(연결보다 보안 우선) - 이러한 정책은 네트워크 인프라 보안이 사용자 편의보다 우선하는 네트워크에 구축됩니다. 침입 정책은 적합한 트래픽에 대해 경계하거나 중단할 수 있는 다양한 네트워크 이상 침입 규칙을 활성화합니다.
- **Balanced Security and Connectivity**(균형 잡힌 보안 및 연결성) - 이 정책은 속도 및 탐지 모두에 구축됩니다. 두 정책을 함께 사용하는 것은 대부분의 네트워크 및 구축 유형에 대해 좋은 시작점이 됩니다.
- **Connectivity Over Security**(보안보다 연결 우선) - 이러한 정책은 연결(모든 리소스에 접근할 수 있는 기능)이 네트워크 인프라 보안보다 우선하는 네트워크에 구축됩니다. 트래픽을 차단하는 가장 중요한 규칙만 사용 설정됩니다.
- **No Rules Active**(활성 규칙 없음) - 정책에 포함된 규칙은 기본적으로 비활성화되어 있습니다.

단계 5 정책의 이름을 입력합니다.

기본 템플릿과 다른 고유한 이름을 사용하는 것이 좋습니다. IPS 정책 문제를 해결해야 하는 경우 Cisco TAC는 쉽게 사용자 지정 정책을 찾기 기본 정책으로 되돌릴 수 있습니다. 이렇게 하면 사용자 지정된 변경 사항이 손실되지 않고 네트워크를 보호할 수 있습니다.

단계 6 (선택 사항) 정책의 설명을 추가합니다.

단계 7 **IPS Mode**(IPS 모드)를 선택합니다.

- **Prevention**(차단) - 작업이 트래픽 삭제인 침입 규칙과 연결이 일치하는 경우 연결이 능동적으로 차단됩니다.

- **Detection(탐지)** - 작업이 트래픽 삭제인 침입 규칙과 연결이 일치하는 경우, 작업 결과는 차단되었을 수 있으며 아무 작업도 수행되지 않습니다.

단계 8 **Save(저장)**를 클릭합니다.

다음 단계는 무엇입니까?

FDM 관리 디바이스 액세스 제어 규칙에 IPS 정책을 추가합니다. 자세한 내용은 [FDM-관리 액세스 제어 규칙의 사용자 지정 IPS 정책](#)을 참조하십시오.

## 사용자 지정 IPS 정책 편집

이미 IPS 정책이 있는 FDM 관리 디바이스를 온보딩한 경우, FDM에서 IPS 정책을 생성하고 CDO에서 구축된 구성의 정책을 읽는 경우, 또는 방금 새 IPS 정책을 생성한 경우 기존 IPS 정책을 편집할 수 있습니다.


기존 사용자 지정 IPS 정책을 수정하려면 다음 절차를 수행합니다.

### Procedure

단계 1 CDO Navigation(탐색) 창에서 **Policies(정책)**를 클릭합니다.

단계 2 **Intrusion Policies(침입 정책)**를 선택합니다.

단계 3 편집할 IPS 정책을 식별합니다. **Edit(편집)**를 클릭합니다.

단계 4 페이지 상단에서 편집  아이콘을 클릭합니다.

단계 5 다음 중 원하는 필드를 편집합니다.

- 기본 템플릿.
- Name(이름)입니다.
- 설명
- IPS 모드.

단계 6 **Save(저장)**를 클릭합니다.

단계 7 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#)하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 사용자 지정 IPS 정책에서 규칙 그룹 편집

규칙 그룹 내에서 규칙의 기본 작업을 재정의할 수 있습니다. 규칙 그룹 내에 포함된 규칙을 편집하려면 다음 절차를 수행합니다.

## Procedure

---

단계 1 CDO 탐색창에서 **Policies**(정책)를 클릭합니다.

단계 2 **Intrusion Policies**(침입 정책)를 선택합니다.

단계 3 편집할 IPS 정책을 식별합니다. **Edit**(편집)를 클릭합니다.

단계 4 왼쪽에 있는 Rule Group(규칙 그룹) 탭에서 원하는 규칙 그룹을 확장합니다. 확장된 목록에서 그룹을 선택합니다.

단계 5 규칙 그룹을 편집합니다.

- a) 보안 레벨 표시줄을 선택하여 전체 규칙 그룹의 **Security Level**(보안 레벨)을 편집합니다. 보안 레벨을 전체 규칙 그룹에 적용할 보안 유형으로 직접 드래그합니다. 제출을 클릭합니다.
- b) 오른쪽에 있는 규칙의 드롭다운 메뉴를 확장하여 개별 규칙의 **Rule Action**(규칙 작업)을 편집합니다.
- c) 원하는 규칙의 체크 박스를 선택하고 규칙 테이블 위에 있는 드롭다운 메뉴를 확장하여 여러 규칙의 **Rule Action**(규칙 작업)을 편집합니다. 이 선택은 선택한 모든 규칙에 영향을 미칩니다.
- d) 테이블의 제목 행에서 체크 박스를 선택하고 규칙 테이블 위에 있는 드롭다운 메뉴를 확장하여 모든 규칙의 **Rule Action**(규칙 작업)을 편집합니다. 이 선택은 규칙 그룹의 모든 규칙에 영향을 미칩니다.

단계 6 정책 페이지 맨 위에서 **Save**(저장)를 클릭합니다.

단계 7 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

---

## 사용자 지정 IPS 정책 삭제

CDO에서 사용자 지정 IPS 정책을 삭제하려면 다음 절차를 수행합니다.

## Procedure

---

단계 1 CDO 탐색창에서 **Policies**(정책)를 클릭합니다.

단계 2 **Intrusion Policies**(침입 정책)를 선택합니다.

단계 3 편집할 IPS 정책을 식별합니다. **Delete**(삭제)를 클릭합니다.

단계 4 **OK**(확인)를 클릭하여 정책을 삭제합니다.

단계 5 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

---



## 보안 인텔리전스 정책

### 보안 인텔리전스 정보

보안 인텔리전스 정책을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 시스템은 액세스 제어 정책을 사용하여 차단 목록에 추가된 트래픽을 평가 전에 삭제하며, 이에 따라 사용된 시스템 리소스의 양이 줄어듭니다.

다음은 기반으로 트래픽을 차단할 수 있습니다.

- **Cisco Talos 피드** — Cisco Talos에서는 정기적으로 업데이트된 보안 인텔리전스 피드에 액세스할 수 있도록 지원합니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 사이트는 맞춤형 컨피그레이션을 업데이트하고 구축하는 속도보다 빠르게 나타났다가 사라질 수 있습니다. 시스템에서는 피드 업데이트를 정기적으로 다운로드하므로 컨피그레이션을 재구축하지 않아도 새로운 위협 인텔리전스를 사용할 수 있습니다.



**Note** Cisco Talos 피드는 기본적으로 1시간마다 업데이트됩니다. Firepower Device Manager에 로그인하고 홈 페이지(Device(디바이스) > Updates(업데이트) > View Configuration(구성 보기))로 이동하여 업데이트 빈도를 변경하고 온디맨드 방식으로 피드를 업데이트할 수도 있습니다.

- **네트워크 및 URL 개체** — 차단하고 싶은 특정 IP 주소 또는 URL을 알고 있는 경우, 이에 대한 개체를 생성하여 차단 목록 또는 허용 목록에 추가할 수 있습니다.

IP 주소(네트워크) 및 URL에 대한 별도의 차단 및 허용 목록을 생성합니다.

### 보안 인텔리전스를 위한 라이선스 요건

보안 인텔리전스를 사용하려면 FDM 관리 디바이스에서 라이선스를 활성화해야 합니다.

자세한 내용은 해당 [Firepower Device Manager용 Cisco FTD 구성 가이드](#)의 보안 정책 장의 보안 인텔리전스 피드 범주 섹션을 참조하십시오.


## Firepower 보안 인텔리전스 정책 구성

보안 인텔리전스 정책을 사용하면 소스/대상 IP 주소 또는 대상 URL을 기준으로 원치 않는 트래픽을 미리 삭제할 수 있습니다. 모든 허용된 연결은 계속해서 액세스 제어 정책을 통해 평가되고 결과적으로 삭제될 수도 있습니다. 보안 인텔리전스를 사용하려면 라이선스를 활성화해야 합니다.


### Firepower 보안 인텔리전스 정책 구성

#### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 보안 인텔리전스 정책을 생성하거나 편집할 FDM 관리 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서  **Policy**(정책)를 클릭합니다.
- 단계 5 FDM 관리 Device Policies(FDM 매니지드 디바이스 정책) 페이지의 정책 표시줄에서 **Security Intelligence**(보안 인텔리전스)를 클릭합니다.
- 단계 6 정책이 활성화되지 않은 경우 **Security Intelligence**(보안 인텔리전스) 슬라이더를 클릭하여 활성화하거나 About Security Intelligence information(보안 인텔리전스 정보) 상자에서 **Enable**(활성화)을 클릭합니다.

**Note** 보안 인텔리전스 토글을 클릭하여 켜기로 전환하면 언제든지 보안 인텔리전스를 비활성화할 수 있습니다. 컨피그레이션은 보존되므로 정책을 다시 활성화할 때 다시 구성할 필요가 없습니다.

- 단계 7 **Blocked List**(차단 목록)의 행을 선택합니다. 테이블 보기에 따라 네트워크, 네트워크 개체, 네트워크 피드, URL, URL 개체 및 URL 피드 열에 더하기 기호  가 있다는 점에 유의하십시오.

- **Add Networks to Blocked List**(차단 목록에 네트워크 추가) 대화 상자 및 **Add URL Object to Blocked List**(차단 목록에 URL 개체 추가) 대화 상자에서 기존 개체를 검색하거나 필요에 따라 생성할 수 있습니다. 차단할 개체를 선택하고 **Select**(선택)를 클릭합니다.


**Note** 보안 인텔리전스는 /0 넷마스크를 사용하는 IP 주소 블록을 무시합니다. 여기에는 any-ipv4 및 any-ipv6 네트워크 개체가 포함됩니다. 네트워크 차단 목록 추가용으로 이러한 개체를 선택하지 마십시오.

- **Add URL Objects to Blocked List**(차단 목록에 URL 개체 추가) 및 **Add Network Feeds to Blocked List**(차단 목록에 네트워크 피드 추가) 대화 상자에서 차단할 피드를 선택하고 **Select**(선택)를 클릭합니다. 피드 행의 끝에 있는 아래쪽 화살표를 클릭하여 피드의 설명을 읽을 수 있습니다. [Firepower 보안 인텔리전스 정책에 대한 보안 인텔리전스 피드](#)에도 설명되어 있습니다.

- 단계 8 이전 단계에서 지정한 네트워크 그룹, 네트워크 피드, URL 개체 또는 URL 피드에 포함된 네트워크, IP 주소 또는 URL이 있음을 알고 있는 경우 예외를 적용하려면 **Allowed List**(허용 목록)의 행을 선택합니다.

- 단계 9 예외를 만들 네트워크, IP 주소 및 URL에 대한 개체를 선택하거나 생성합니다. **Select**(선택) 또는 **Add**(추가)를 클릭하면 Allowed List(허용 목록) 행에 추가됩니다.

- 단계 10 (선택 사항) 보안 인텔리전스 정책에 의해 생성된 이벤트를 로깅하려면 다음을 수행합니다.

- 로깅을 구성하려면 로깅 설정  아이콘을 클릭합니다. 로깅을 활성화하면 차단 목록 항목과 일치하는 항목이 로깅됩니다. 로깅이 활성화된 상태에서 제외된 연결이 액세스 제어 규칙과 일치하는 경우에는 로그 메시지를 받더라도 예외 항목과 일치하는 항목은 로깅되지 않습니다.
- Connection Events Logging**(연결 이벤트 로깅) 토글을 클릭하여 이벤트 로깅을 활성화합니다.
- 이벤트를 전송할 위치를 선택합니다.

- **None**(없음)을 클릭하면 FDM 관리 디바이스에 이벤트가 저장됩니다. 이는 FDM 이벤트 뷰어에 표시됩니다. FDM 관리 디바이스의 저장 공간은 매우 제한적입니다. **None**(없음)을 선택하

는 대신 시스템 로그 서버 개체를 정의하여 시스템 로그 서버에 연결 이벤트를 저장하는 것이 가장 좋습니다.

- **Create**(생성) 또는 **Choose**(선택)를 클릭하면 시스템 로그 서버 개체로 표시되는 로깅 이벤트를 전송할 시스템 로그 서버를 생성하거나 선택할 수 있습니다. 디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 시스템 로그 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 애널리틱스 성능이 개선됩니다.

Cisco Security Analytics and Logging에 대한 서브스크립션이 있는 경우 [SaaS\(Secure Logging Analytics\)를 위한 시스템 로그 서버 개체 생성](#)하여 보안 이벤트 커넥터에 이벤트를 전송합니다. 이 기능에 대한 자세한 내용은 [FDM-관리 디바이스에 대한 보안 로깅 분석](#)을 참조하십시오.

**단계 11** (선택 사항) 생성한 규칙에 대해 해당 규칙을 선택하고 **Add Comments**(코멘트 추가) 필드에 코멘트를 추가할 수 있습니다. 규칙 코멘트에 대한 자세한 내용은 [정책 및 규칙 집합의 규칙에 코멘트 추가](#)를 참조하십시오.

**단계 12** 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#)하거나 기다렸다가 여러 번 변경 사항을 한 번에 구축합니다.

## Firepower 보안 인텔리전스 정책 차단 목록에 대한 예외 설정

[Firepower 보안 인텔리전스 정책 구성](#)에서 생성하는 각 차단 목록에 대해 연결된 허용 목록을 생성할 수 있습니다. 허용 목록을 사용하는 유일한 목적은 차단 목록에 표시되는 IP 주소 또는 URL에 대해 예외를 만드는 것입니다. 즉, 사용해야 하는 주소 또는 URL이 안전한데도 차단 목록에 구성된 피드에 있는 경우 허용 목록에 입력하여 해당 주소 또는 URL을 제외할 수 있습니다. 이렇게 하면 하나의 주소 또는 URL을 위해 차단 목록에서 전체 피드를 제거할 필요가 없습니다.

보안 인텔리전스 정책을 통과한 후 허용되는 트래픽은 액세스 제어 정책에 의해 평가됩니다. 연결의 최종 허용/삭제 여부는 연결과 일치하는 액세스 제어 규칙에 따라 결정됩니다. 또한, 액세스 규칙에 따라 연결에 침입 또는 악성코드 검사를 적용할지도 결정됩니다.

## Firepower 보안 인텔리전스 정책에 대한 보안 인텔리전스 피드

다음 표에서는 Cisco Talos 피드에서 사용할 수 있는 카테고리에 대해 설명합니다. 이러한 범주는 네트워크 및 URL 차단 목록에 모두 입력할 수 있습니다.

카테고리	설명
attackers(공격자)	아웃바운드 악성 활동으로 알려져 있는, 활성화된 스캐너 및 차단 목록에 추가된 호스트
bogon	bogon 네트워크 및 할당되지 않은 IP 주소
bots(봇)	바이너리 악성코드 드로퍼를 호스팅하는 사이트
CnC	봇넷용 C&C(Command-and-Control) 서버를 호스팅하는 사이트

카테고리	설명
dga	C&C 서버에서 RP(Rendezvous Point) 역할을 하는 많은 수의 도메인 이름을 생성하는 데 사용되는 악성코드 알고리즘
exploitkit(익스플로잇 킷)	클라이언트에서 소프트웨어 취약점을 식별하도록 설계된 소프트웨어 킷
malware(악성코드)	악성코드 바이너리 또는 익스플로잇 킷을 호스팅하는 사이트
open_proxy(오픈 프록시)	익명의 웹 브라우저를 허용하는 오픈 프록시
open_relay(오픈 릴레이)	스팸에 사용되는 것으로 알려진 오픈 메일 릴레이
phishing(피싱)	피싱 페이지를 호스팅하는 사이트
response(대응)	악성 활동 또는 의심스러운 활동에 적극적으로 참여하고 있는 IP 주소 및 URL
spam(스팸)	스팸을 전송하는 것으로 알려진 메일 호스트
suspicious(의심스러움)	알려진 악성코드와 유사한 특성을 지니고 있으며 의심스러워 보이는 파일
tor_exit_node(Tor 종료 노드)	Tor 종료 노드

## FDM 매니저드 디바이스 ID 정책

### ID 정책 개요

연결에서 사용자 ID 정보를 수집하기 위해 ID 정책을 사용합니다. 그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고 사용자 또는 사용자 그룹을 기준으로 액세스 제어를 구성할 수 있습니다. 시스템에서 네트워크 행동, 트래픽 및 이벤트를 개별 사용자 및 그룹과 직접 연결하므로 정책 위반, 공격 또는 네트워크 취약성의 소스를 손쉽게 식별할 수 있습니다.

예를 들어 침입 이벤트의 대상인 호스트를 소유한 사용자와 내부 공격 또는 포트 스캔을 시작한 사용자를 식별할 수 있습니다. 부적절한 웹 사이트 또는 애플리케이션에 액세스하는 사용자 및 대역폭을 많이 사용하는 사용자도 식별할 수 있습니다.

그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고, AD(Active Directory) 영역 개체(해당 AD의 모든 사용자와 일치), 특수 ID(예: 실패한 인증, 게스트, 인증 필요 없음 또는 알 수 없는 ID) 또는 사용자 그룹을 기반으로 액세스 제어를 구성할 수 있습니다.

다음 방법을 통해 사용자 ID를 획득할 수 있습니다.

- 패시브 인증 - 모든 유형의 연결에 대해, 사용자 이름과 비밀번호를 입력하라는 메시지를 표시하지 않고 다른 인증 서비스를 통해 사용자 ID를 획득합니다.
- 액티브 인증 - HTTP 연결에만 사용자 이름과 비밀번호를 입력하라는 메시지를 표시하고, 소스 IP 주소의 사용자 ID를 획득하기 위해 지정된 ID 소스를 통해 인증을 수행합니다.

#### 패시브 인증을 통한 사용자 ID 설정

패시브 인증은 사용자에게 사용자 이름 및 비밀번호를 요구하지 않고 사용자 ID를 수집합니다. 시스템은 지정된 ID 소스에서 매핑을 가져옵니다.

다음 소스에서 패시브 방식으로 사용자-IP 주소 매핑을 획득할 수 있습니다.

- 원격 액세스 VPN 로그인. 패시브 ID에 대해 지원되는 사용자 유형은 다음과 같습니다.
  - 외부 인증 서버에 정의된 사용자 어카운트.
  - FDM 관리 디바이스에 정의된 로컬 사용자 계정.
- Cisco ISE(Identity Services Engine), Cisco ISE PIC(Identity Services Engine Passive Identity Connector)

지정된 사용자가 둘 이상의 소스를 통해 식별되는 경우에는 원격 액세스 VPN 로그인 ID가 우선적으로 사용됩니다.

#### 활성 인증을 통한 사용자 ID 설정

인증은 사용자의 ID를 확인하는 작업입니다.

활성 인증을 사용하는 경우, 시스템에 사용자-ID 매핑이 없는 IP 주소에서 HTTP 트래픽 흐름이 유입되는 경우 시스템에 구성된 디렉터리에 대해 트래픽 흐름을 시작한 사용자를 인증할지를 결정할 수 있습니다. 사용자가 정상적으로 인증하면 해당 IP 주소는 인증된 사용자의 ID를 포함하는 것으로 간주됩니다.

인증이 실패해도 사용자의 네트워크 액세스는 차단되지 않습니다. 최종적으로는 액세스 규칙에 따라 이러한 사용자에게 제공할 액세스 권한이 결정됩니다.

#### 알 수 없는 사용자 처리

FDM 관리 디바이스를 사용하여 ID 정책에 대해 디렉터리 서버를 구성할 때 FDM 관리 디렉터리 서버에서 사용자 및 그룹 멤버십 정보를 다운로드합니다. Active Directory 정보는 24시간마다 자정에 또는 디렉터리 구성을 편집하고 저장할 때 새로 고침됩니다. 정보를 변경하지 않는 경우에도 마찬가지입니다.

사용자가 활성 인증 ID 규칙에 따라 인증에 성공했으나, 사용자 이름이 다운로드된 사용자 ID 정보에 없으면 해당 사용자는 Unknown(알 수 없음)으로 표시됩니다. 사용자 ID와 사용자 일치 그룹 규칙은 ID 관련 대시보드에 표시되지 않습니다.

그러나 알 수 없음 사용자에 대한 모든 액세스 제어 규칙은 적용됩니다. 예를 들어 알 수 없음 사용자에 대한 연결을 차단하는 경우, 해당 사용자는 인증에 성공하더라도(즉, 디렉터리 서버에서 사용자와 비밀번호를 유효한 것으로 인식하더라도) 차단됩니다.

그러므로 사용자를 추가 또는 삭제하거나 그룹 멤버십을 변경하는 등 디렉터리 서버를 변경하면 시스템이 디렉터리에서 업데이트를 다운로드할 때까지는 해당 변경 사항이 정책 시행에 반영되지 않습니다.

매일 자정 업데이트가 수행될 때까지 기다리지 않으려면 디렉터리 영역 정보를 편집하여 강제로 업데이트할 수 있습니다(FDM 관리 디바이스에 로그인하여 **Objects(개체) > Identity Sources(ID 소스)**로 이동 후 영역 편집). **OK(확인)**를 클릭한 다음 변경 사항을 구축합니다. 그러면 시스템이 업데이트를 즉시 다운로드합니다.



**Note** FDM 관리 디바이스에 로그인하고 **Policies(정책) > Access Control(액세스 제어)**로 이동한 다음 **Add Rule(규칙 추가)(+)** 버튼을 클릭하고 **Users(사용자)** 탭에서 사용자 목록을 확인하여 새 사용자 정보 또는 삭제된 사용자 정보가 FDM 관리 시스템에 있는지 확인할 수 있습니다. 새 사용자를 찾을 수 없거나 삭제된 사용자를 찾을 수 있으면 시스템의 정보는 오래된 것입니다.

## Firepower ID 정책을 구현하는 방법

CDO(Cisco Defense Orchestrator)를 사용하여 FDM 관리 디바이스에 대한 ID 정책을 관리하려면 먼저 ID 소스를 생성해야 합니다. Defense Orchestrator를 사용하여 나머지 설정을 구성할 수 있습니다.

이러한 항목을 정확하게 구성하면 FDM에서 모니터링 대시보드 및 이벤트에서 사용자 이름을 확인할 수 있습니다. 또한 액세스 제어 및 SSL 암호 해독 규칙에서 사용자 ID를 트래픽 일치 기준으로 사용할 수도 있습니다.



**Note** 현재 CDO는 원격 액세스 VPN 및 Cisco Identity Services Engine과 같은 ID 정책을 구현하는 데 필요한 일부 구성 요소를 구성할 수 없습니다. 이러한 구성 요소는 디바이스의 로컬 관리자인 FDM에서 구성해야 합니다. 아래 절차의 일부 단계에서는 ID 정책을 구현하기 위해 FDM을 사용하여 일부 ID 구성 요소를 구성해야 함을 나타냅니다.

### 절차

다음 절차에서는 ID 정책이 작동하도록 하려면 구성해야 하는 항목의 개요를 제공합니다.

#### Procedure

**단계 1** AD ID 영역을 생성합니다. 사용자 ID를 액티브 방식으로 수집하든 아니면 패시브 방식으로 수집하든 관계없이 사용자 ID 정보가 포함된 AD(Active Directory) 서버를 구성해야 합니다. 자세한 내용은 [FTD Active Directory 영역 개체 생성](#)을 참조하십시오.

**단계 2** 패시브 인증 ID 규칙을 사용하려는 경우 FDM을 사용하여 패시브 ID 소스를 구성합니다.

디바이스에서 구현하는 서비스와 네트워크에서 사용 가능한 서비스를 기준으로 하여 다음 중 원하는 소스를 구성할 수 있습니다.

- 원격 액세스 VPN - 디바이스에 대한 원격 액세스 VPN 연결을 지원하려는 경우 사용자 로그인은 FDM 관리 디바이스 내에 정의된 로컬 사용자 또는 AD 서버를 기준으로 하여 ID를 제공할 수 있습니다. 원격 액세스 VPN 구성에 대한 자세한 내용은 디바이스에서 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드의 원격 액세스 VPN 구성 장](#)을 참조하십시오.
- Cisco ISE(Identity Services Engine) 또는 Cisco ISE PIC(Identity Services Engine Passive Identity Connector) - 이러한 제품을 사용하는 경우에는 디바이스를 pxGrid 서브스크라이버로 구성하고 ISE에서 사용자 ID를 획득할 수 있습니다. 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드의 ID 서비스 엔진 구성 장](#)을 참조하십시오.

- 단계 3 **Defense Orchestrator**를 사용하여 ID 정책을 활성화하고 패시브 또는 활성 인증을 구성합니다. 자세한 내용은 [ID 정책 설정 구성](#)을 참조하십시오.
- 단계 4 **Defense Orchestrator**, [Firepower ID 정책 기본 작업 구성](#)을 참조하십시오. 패시브 인증만 사용하려는 경우에는 기본 작업을 패시브 인증으로 설정할 수 있으며, 구체적인 규칙을 생성할 필요가 없습니다.
- 단계 5 **Defense Orchestrator**, [ID 규칙 구성](#)을 참조하십시오. 관련 네트워크에서 패시브 또는 액티브 사용자 ID를 수집할 규칙을 생성합니다.
- 단계 6 (선택 사항) 생성한 규칙에 대해 해당 규칙을 선택하고 Add Comments(코멘트 추가) 필드에 코멘트를 추가할 수 있습니다. 규칙 코멘트에 대한 자세한 내용은 [정책 및 규칙 집합의 규칙에 코멘트 추가](#)를 참조하십시오.
- 단계 7 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#)하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.


## ID 정책 구성

연결에서 사용자 ID 정보를 수집하기 위해 ID 정책을 사용할 수 있습니다. 그런 다음 FDM 대시보드에서 사용자 ID를 기반으로 사용량을 보고 사용자 또는 사용자 그룹을 기반으로 액세스 제어를 구성할 수 있습니다.

다음은 ID 정책을 통해 사용자 ID를 얻는 데 필요한 요소를 구성하는 방법에 대한 개요입니다.

### 절차


#### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 ID 정책을 구성할 디바이스를 선택한 다음 오른쪽의 **Management**(관리) 창에서  **Policy**(정책)를 클릭합니다.
- 단계 4 Policy(정책) 표시줄에서 **Identity**(ID)를 클릭합니다.

단계 5 ID 정책을 아직 활성화하지 않은 경우 패시브 및 액티브 인증에 대해 읽고 **Enable(활성화)**을 클릭합니다. 패시브 인증 정책 또는 액티브 인증 정책이 아닌 ID 정책을 활성화하고 있습니다. 정책의 규칙은 액티브 또는 패시브 인증을 지정합니다.

단계 6 ID 정책을 관리합니다.

ID 설정을 구성하고 나면 이 페이지에 모든 규칙이 순서대로 나열됩니다. 목록의 맨 위에서부터 규칙과 트래픽의 일치 여부를 확인하며, 첫 번째로 일치하는 규칙에 따라 적용할 작업이 결정됩니다. 이 페이지에서는 다음을 수행할 수 있습니다.

- ID 정책을 활성화하거나 비활성화하려면 ID 토글을 클릭합니다. 자세한 내용은 [ID 정책 설정 구성](#)을 참조하십시오.
- 패시브 인증 설정을 읽으려면 ID 표시줄에서 **Passive Auth**(패시브 인증) 레이블 옆에 있는 버튼을 클릭합니다. 자세한 내용은 [ID 정책 설정 구성](#)을 참조하십시오.
- 액티브 인증을 활성화하려면 ID 표시줄의 **Active Auth**(액티브 인증) 레이블 옆에 있는 버튼을 클릭합니다. 자세한 내용은 [ID 정책 설정 구성](#)을 참조하십시오.
- 기본 작업을 변경하려면 기본 작업 버튼을 클릭하고 원하는 작업을 선택합니다. [Firepower ID 정책 기본 작업 구성](#)을 참조하십시오.
- 테이블에서 규칙을 이동하려면 규칙을 선택하고 규칙 테이블에서 규칙 행의 끝에 있는 위쪽 또는 아래쪽 화살표를 클릭합니다.
- 테이블에서 규칙을 이동하려면 규칙을 선택하고 규칙 테이블에서 규칙 행의 끝에 있는 위쪽 또는 아래쪽 화살표를 클릭합니다.
- 규칙을 구성하려면 다음을 수행합니다.
  - 새 규칙을 생성하려면 더하기  버튼을 클릭합니다.
  - 기존 규칙을 편집하려면 규칙을 선택하고 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다. 테이블에서 속성을 클릭하여 규칙 속성을 선택적으로 수정할 수도 있습니다.
  - 더 이상 필요하지 않은 규칙을 삭제하려면 규칙을 선택하고 **Actions**(작업) 창에서 **Remove**(제거)를 클릭합니다.

ID 규칙 생성 및 수정에 대한 자세한 내용은 [ID 규칙 구성](#)을 참조하십시오.

단계 7 (선택 사항) 생성한 규칙에 대해 해당 규칙을 선택하고 **Add Comments**(코멘트 추가) 필드에 코멘트를 추가할 수 있습니다. 규칙 코멘트에 대한 자세한 내용은 [정책 및 규칙 집합의 규칙에 코멘트 추가](#)를 참조하십시오.

단계 8 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#)하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.



## ID 정책 설정 구성

ID 정책이 작동하려면 사용자 ID 정보를 제공하는 소스를 구성해야 합니다. 구성해야 하는 설정은 구성할 규칙의 유형(패시브, 액티브 또는 모두)에 따라 다릅니다.



**Note** 현재 CDO는 Active Directory ID 영역, 원격 액세스 VPN 및 Cisco Identity Services Engine과 같은 ID 정책을 구현하는 데 필요한 일부 구성 요소를 구성할 수 없습니다. 이러한 구성 요소는 FTD 디바이스의 로컬 관리자인 FDM에서 구성해야 합니다. 아래 절차의 일부 단계에서는 ID 정책을 구현하기 위해 FDM을 사용하여 일부 ID 구성 요소를 구성해야 함을 나타냅니다.

### 절차

#### Before you begin


디렉터리 서버, FDM 관리 디바이스 및 클라이언트에서 시간 설정이 서로 일치하는지 확인합니다. 이러한 디바이스 간에 시간이 바뀌면 사용자가 정상적으로 인증하지 못할 수 있습니다. 여기서 "일치"란 여러 표준 시간대를 사용할 수는 있지만 이러한 표준 시간대를 기준으로 할 때 시간이 동일해야 한다는 의미입니다. 예를 들어 PST로 오전 10시는 EST로 오후 1시에 해당합니다.

#### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 ID 정책을 구성할 디바이스를 선택한 다음 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다.
- 단계 4 ID 토글을 클릭하여 ID 정책을 활성화합니다. 또는 ⓘ 버튼을 클릭하고 패시브 및 액티브 인증에 대한 설명을 검토한 후 대화 상자에서 **Enable**(활성화)를 클릭할 수 있습니다.
- 단계 5 **Passive Authentication**(패시브 인증) 설정을 읽습니다. ID 표시줄에서 **Passive Auth**(패시브 인증) 버튼을 클릭합니다.  
  
Firepower Device Manager를 사용하여 원격 액세스 VPN 또는 Cisco Identity Services 엔진을 구성한 경우 Passive Authentication(패시브 인증) 버튼이 **Enabled**(활성화됨)로 표시됩니다.  
  
패시브 인증 규칙을 생성하려면 하나 이상의 패시브 ID 소스를 구성한 상태여야 합니다.
- 단계 6 액티브 인증을 구성합니다. ID 규칙에서 사용자에게 대한 액티브 인증을 요구하는 경우 사용자는 연결 시에 사용한 인터페이스의 캡티브 포털 포트로 리디렉션되며, 그리고 나면 인증하라는 메시지가 표시됩니다.
  - a) Identity(ID) 표시줄에서 **Active Auth**(활성 인증) 버튼을 클릭합니다.
  - b) 아직 활성화하지 않은 경우 **Enable**(활성화) 링크를 클릭하여 SSL Description(SSL 설명)을 활성화합니다. Enable(활성화) 링크가 표시되지 않으면 "c" 단계로 건너뛩니다.

1. **Select Decrypt Re-Sign Certificate**(재서명 암호 해독 인증서 선택) 메뉴에서 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다.

사전 정의된 **NGFW-Default-InternalCA** 인증서를 사용하거나, 메뉴를 클릭하고 **Create**(생성) 또는 **Choose**(선택)를 선택하여 새 인증서를 생성하거나, FDM 관리 디바이스에 이미 업로드한 인증서를 선택할 수 있습니다.

클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼  을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. **재서명 암호 해독 규칙을 위한 CA 인증서 다운로드**를 참조하십시오.

**Note** SSL 암호 해독 정책을 아직 구성하지 않은 경우에만 SSL 암호 해독 설정에 대한 프롬프트가 표시됩니다. ID 정책을 활성화한 후에 이러한 설정을 변경하려면 SSL 암호 해독 정책 설정을 편집합니다.

2. **Save**(저장)를 클릭합니다.

- c) **Server Certificate**(서버 인증서) 메뉴를 클릭하여 활성 인증 중에 사용자에게 제공할 내부 인증서를 선택합니다. 필요한 인증서를 아직 생성하지 않은 경우 **Create**(생성)를 클릭합니다. 사용자의 브라우저에서 이미 신뢰하는 인증서를 업로드하지 않으면 사용자가 인증서를 허용해야 합니다.
- d) **Port**(포트) 필드에서 캡티브 포털의 포트 번호를 입력합니다. 기본값은 885(TCP)입니다. 다른 포트를 구성하는 경우에는 포트가 1025-65535 범위에 포함되어야 합니다.

**Note** HTTP 기본, HTTP 대응 페이지 및 NTLM 인증 방법의 경우 사용자는 인터페이스의 IP 주소를 사용하여 캡티브 포털로 리디렉션됩니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 `firewall-hostname.AD-domain-name`을 사용하여 리디렉션됩니다. HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다.

- e) **Save**(저장)를 클릭합니다.

단계 7 **Firepower ID 정책 기본 작업 구성**을 계속 진행합니다.

## Firepower ID 정책 기본 작업 구성


ID 정책은 개별 ID 규칙과 일치하지 않는 모든 연결에 대해 구현되는 기본 작업입니다.

실제로 규칙이 없는 것도 정책에 대해 유효한 컨피그레이션입니다. 모든 트래픽 소스에서 패시브 인증을 사용하려는 경우에는 기본 작업으로 패시브 인증을 구성하면 됩니다.

절차

### Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 ID 정책을 구성할 디바이스를 선택한 다음 오른쪽의 **Management**(관리) 창에서  **Policy**(정책)를 클릭합니다.
- 단계 4 Policy(정책) 표시줄에서 **Identity**(ID)를 클릭합니다.
- 단계 5 아직 구성하지 않은 경우 [ID 정책 설정](#) 구성합니다.
- 단계 6 화면 하단에서 **Default Action**(기본 작업) 버튼을 클릭하고 다음 중 하나를 선택합니다.
- **Passive Auth**(패시브 인증) - ID 규칙과 일치하지 않는 연결에 대해 구성된 모든 패시브 ID 소스를 통해 사용자 ID가 결정됩니다. 패시브 ID 소스를 구성하지 않는 경우 **Passive Auth**(패시브 인증)를 기본값으로 사용하는 것은 **No Auth**(인증 없음)를 사용하는 것과 같습니다.
  - **No Auth**(인증 없음) - ID 규칙과 일치하지 않는 연결에 대해서는 사용자 ID가 결정되지 않습니다.
- 단계 7 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#)하거나 기다렸다가 여러 번 변경 사항을 한 번에 구축합니다.

## ID 규칙 구성

ID 규칙은 일치하는 트래픽에 대해 사용자 ID 정보를 수집할지 여부를 결정합니다. 일치하는 트래픽에 대해 사용자 ID 정보를 수집하지 않으려는 경우에는 인증 없음을 구성할 수 있습니다.


규칙 컨피그레이션에 관계없이 액티브 인증은 HTTP 트래픽에 대해서만 수행됩니다. 따라서 액티브 인증에서 비 HTTP 트래픽을 제외하는 규칙을 생성할 필요가 없습니다. 모든 HTTP 트래픽에 대해 사용자 ID 정보를 가져오려면 모든 소스와 대상에 대해 활성 인증 규칙만 적용하면 됩니다.




**Note** 인증에서 장애가 발생해도 네트워크 액세스에는 아무 영향이 없습니다. ID 정책은 사용자 ID 정보만 수집합니다. 인증 시에 장애가 발생한 사용자의 네트워크 액세스를 차단하려는 경우에는 액세스 규칙을 사용해야 합니다.

## 절차

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 ID 정책을 구성할 디바이스를 선택한 다음 오른쪽의 **Management**(관리) 창에서  **Policy**(정책)를 클릭합니다.
- 단계 4 Policy(정책) 표시줄에서 **Identity**를 클릭합니다.

단계 5 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 더하기  버튼을 클릭합니다. ID 소스 개체 및 이러한 개체가 규칙에 미치는 영향을 이해하려면 [FDM-관리 장치에 대한 ID 소스 구성](#)를 참조하십시오.
- 기존 규칙을 편집하려면 편집할 규칙을 클릭하고 오른쪽의 Actions(작업) 창에서 **Edit**(편집)를 클릭합니다.
- 더 이상 필요 없는 규칙을 삭제하려면 삭제할 규칙을 클릭하고 오른쪽의 Actions(작업) 창에서 **Remove**(제거)를 클릭합니다.

단계 6 **Order**(순서)에서 순서가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

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

단계 7 **Name**(이름)에 규칙의 이름을 입력합니다.

단계 8 FDM 관리 디바이스가 일치 항목에 적용해야 하는 작업을 선택하고 필요한 경우 AD(Active Directory) ID 소스를 선택합니다.

패시브 및 활성 인증 규칙용 사용자 계정을 포함하는 AD ID 영역을 선택해야 합니다. 다음 중 하나를 선택합니다.

- **Passive Auth**(패시브 인증) - 패시브 인증을 통해 사용자 ID를 확인합니다. 구성된 모든 ID 소스가 표시됩니다. 규칙은 구성된 모든 소스를 자동으로 사용합니다.
- **Active Auth**(활성 인증) - 활성 인증을 통해 사용자 ID를 확인합니다. 활성 인증은 HTTP 트래픽에만 적용됩니다. 다른 트래픽 유형이 활성 인증을 요구하거나 허용하는 ID 정책과 일치하는 경우에는 활성 인증을 시도하지 않습니다.
- **No Auth**(인증 없음) - 사용자 ID를 가져오지 않습니다. 이 트래픽에는 ID 기반 액세스 규칙이 적용되지 않습니다. 이러한 사용자는 인증 필요 없음으로 표시됩니다.

**Note** 패시브 인증과 활성 인증 모두에서 AD 영역 ID 소스를 선택할 수 있습니다. 즉시 준비된 ID 소스 개체가 없는 경우 **Create New Object**(새 개체 생성)를 클릭하여 ID 소스 개체 마법사를 시작합니다. 자세한 내용은 [Active Directory 영역 개체 생성 또는 편집](#)을 참조하십시오.

단계 9 (액티브 인증에만 해당됨) **Active Authentication**(활성 인증) 탭을 클릭하고 디렉터리 서버에서 지원하는 인증 방법(유형)을 선택합니다.

- **HTTP 기본** - 암호화되지 않은 HTTP 기본 인증 연결을 통해 사용자를 인증합니다. 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다. 이는 기본값입니다.
- **NTLM** - NTLM(NT LAN Manager) 연결을 통해 사용자를 인증합니다. 이 선택 사항은 AD 영역을 선택할 때만 사용 가능합니다. 사용자가 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인

인합니다. 그러나 사용자가 Windows 도메인 로그인을 통해 투명하게 인증을 하도록 Internet Explorer 및 Firefox 브라우저를 구성할 수 있습니다. 이 작업은 FDM에서 수행됩니다. 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#) > 보안 정책 > ID 정책 > 투명 사용자 인증 활성화를 참조하십시오.

- **HTTP 협상** - 디바이스가 사용자 에이전트(사용자가 트래픽 흐름을 시작하는 데 사용 중인 애플리케이션)와 Active Directory 서버 간에 방법을 협상할 수 있도록 합니다. 협상 시에는 일반적으로 지원되는 가장 강력한 방법이 순서대로 사용됩니다(NTLM -> 기본). 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.
- **HTTP 대응 페이지** - 시스템 제공 웹 페이지를 통해 인증하라는 메시지를 사용자에게 표시합니다. 이 방법은 일종의 HTTP 기본 인증입니다.

**Note** HTTP 기본, HTTP 대응 페이지 및 NTLM 인증 방법의 경우 사용자는 인터페이스의 IP 주소를 사용하여 캡티브 포털로 리디렉션됩니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 `firewall-hostname.AD-domain-name`을 사용하여 리디렉션됩니다. HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다.

**단계 10** (활성 인증에만 해당됨) 활성 인증에서 장애가 발생하는 사용자에게 게스트 사용자 레이블을 지정할지를 결정하려면 **Fall Back as Guest(게스트로 폴백) > On/Off(켜기/끄기)**를 선택합니다.


사용자에게는 3번의 인증 기회가 제공됩니다. 인증에서 장애가 발생하면 이 옵션의 선택 여부에 따라 사용자 표시 방법이 결정됩니다. 이러한 값을 기준으로 액세스 규칙을 구축할 수 있습니다.

- **Fall Back as Guest(게스트로 폴백) > On(켜기)** - 사용자가 게스트로 표시됩니다.
- **Fall Back as Guest(게스트로 폴백) > Off(끄기)** - 사용자가 실패한 인증으로 표시됩니다.

**단계 11** **Source(소스)** 및 **Destination(대상)** 탭에서 **Passive Authentication(패시브 인증)**, **Active Authentication(활성 인증)** 또는 **No Authentication(인증 없음)** 규칙 작업에 대한 트래픽 일치 기준을 정의합니다.

HTTP 트래픽에 대해서만 액티브 인증을 시도합니다. 그러므로 비 HTTP 트래픽에 대해서는 인증 없음 규칙을 구성할 필요가 없으며 액티브 인증 규칙을 생성할 필요도 없습니다. 그러나 패시브 인증은 모든 유형의 트래픽에 유효합니다.

ID 규칙의 소스/대상 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소나 IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 프로토콜과 포트를 정의합니다. 기본값은 모든 영역, 주소, 지리적 위치, 프로토콜 및 포트입니다.

조건을 수정하려면 해당 조건 내의  버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화 상자에서 OK(확인)를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 **Create New Object(새 개체 생성)**를 클릭하면 됩니다.

조건에서 개체를 제거하려면 개체 위에 마우스를 놓고 X를 클릭합니다.

다음과 같은 트래픽 일치 기준을 구성할 수 있습니다.

소스 영역, 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 내부 네트워크에서 생성되는 모든 트래픽에서 사용자 ID를 수집하려는 경우 내부 영역을 소스 영역으로 선택하고 대상 영역은 비워 둡니다.

**Note** 단일 규칙에서 패시브 보안 영역과 라우팅 보안 영역을 함께 사용할 수는 없습니다. 또한 패시브 보안 영역은 소스 영역으로만 지정할 수 있으며 대상 영역으로 지정할 수는 없습니다.

#### 소스 네트워크, 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다.
- 국가/대륙 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.
- 사용자 지정 지리위치 - 지정한 국가 및 대륙과 정확히 일치하는 지리위치 개체를 선택하거나 생성합니다.

**Note** 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다. 자세한 내용은 [Firepower 지리위치 필터 개체 생성 및 편집](#)를 참조하십시오.

### 소스 포트, 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP/UDP의 경우 여기에는 포트가 포함될 수 있습니다.

- 특정 프로토콜이나 포트에서 나오는 트래픽을 일치시키려면 소스 포트를 구성합니다. 소스 포트는 TCP/UDP 전용일 수 있습니다.
- 특정 프로토콜이나 포트에 향하는 트래픽을 일치시키려면 대상 포트/프로토콜을 구성합니다.
- 특정 TCP/UDP 포트에서 발생하는 트래픽과 특정 TCP/UDP 포트에 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 조건에 소스 및 대상 포트를 모두 추가한 경우, 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

단계 12 **Save**(저장)를 클릭합니다.

단계 13 **Inventory**(재고 목록) 페이지로 돌아갑니다.

단계 14 ID 정책에 이러한 규칙을 추가한 디바이스를 선택합니다.

단계 15 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## SSL 암호 해독 정책

HTTPS와 같은 일부 프로토콜은 SSL(Secure Sockets Layer) 또는 그 후속 버전인 TLS(Transport Layer Security)를 사용하여 안전한 전송을 위해 트래픽을 암호화합니다. 시스템에서는 암호화된 연결을 검사할 수 없으므로 상위 레이어의 트래픽 특성을 고려하여 액세스 의사 결정을 내리는 액세스 규칙을 적용하려면 SSL 암호 해독 정책을 적용하여 암호를 해독해야 합니다.



**Caution** 트래픽을 암호 해독한 다음 재암호화하면 디바이스의 처리 부하가 증가하므로 전체 시스템 성능이 감소된다는 점에 유의하십시오.

다음 항목을 계속 진행합니다.

- [SSL 암호 해독 정보](#)
- [SSL 암호 해독 정책을 구현 및 유지 관리하는 방법](#)
- [SSL 암호 해독 정책 구성](#)
- [알려진 키 및 재서명 암호 해독을 위한 인증서 구성](#)
- [재서명 암호 해독 규칙을 위한 CA 인증서 다운로드](#)
- [SSL 암호 해독 문제 해결](#)

## SSL 암호 해독 정책을 구현 및 유지 관리하는 방법

SSL 암호 해독 정책을 사용하여 암호화된 트래픽을 일반 텍스트 트래픽으로 전환할 수 있으므로 URL 필터링, 침입 및 악성코드 제어 그리고 기타 서비스(DPI(Deep Packet Inspection)를 필요로 함)를 적용할 수 있습니다. 정책에서 트래픽을 허용하는 경우, 트래픽은 디바이스를 떠나기 전에 다시 암호화됩니다.

SSL 암호 해독 정책은 암호화된 트래픽에만 적용됩니다. 암호화되지 않은 연결은 SSL 암호 해독 규칙을 기준으로 평가되지 않습니다.

일부 다른 보안 정책과 달리 SSL 암호 해독 정책은 인증서가 만료되거나 목적지 서버에서 변경될 수 있기 때문에 적극적으로 모니터링하고 유지 관리해야 합니다. 또한, MITM(Man-In-The-Middle) 공격과 재서명 암호 해독 작업은 구분할 수 없기 때문에 클라이언트 소프트웨어의 변경 사항에 따라 특정 연결을 암호 해독하는 능력이 변경될 수 있습니다.

다음 절차에서는 SSL 암호 해독 정책을 구현하고 유지 관리하는 엔드 투 엔드 프로세스에 대해 설명합니다.

### 절차

#### Procedure

**단계 1** 재서명 암호 해독 규칙을 구현할 경우 필요한 내부 CA 인증서를 생성합니다.

내부 CA(인증 기관) 인증서를 사용해야 합니다. 다음과 같은 옵션이 있습니다. 사용자가 인증서를 신뢰해야 하므로 클라이언트 브라우저가 이미 신뢰하도록 구성되어 있는 인증서를 업로드하거나 업로드하는 인증서가 브라우저의 신뢰 저장소에 추가되어 있는지 확인합니다.

- 디바이스 자체에서 서명한 자체 서명 내부 CA 인증서를 생성합니다. [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#) > 재사용 가능한 개체 > 인증서 > 자체 서명 내부 및 내부 CA 인증서 생성을 참조하십시오.
- 외부 신뢰 CA 또는 조직 내부의 CA에서 서명한 키와 내부 CA 인증서를 업로드합니다. [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#) > 재사용 가능한 개체 > 인증서 > 내부 및 내부 CA 인증서 업로드를 참조하십시오.

**단계 2** 알려진 키 암호 해독 규칙을 구현할 경우, 각 내부 서버에서 인증서와 키를 수집합니다.

서버에서 인증서와 키를 얻어야 하므로 알려진 키 암호 해독은 제어하고 있는 서버에만 사용할 수 있습니다. 이러한 인증서와 키를 내부 인증서(내부 CA 인증서 아님)로 업로드합니다. [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#) > 재사용 가능한 개체 > 인증서 > 내부 및 내부 CA 인증서 업로드를 참조하십시오.

**단계 3** SSL 암호 해독 정책 구성을 참조하십시오.

정책을 활성화하는 경우 몇 가지 기본 설정도 구성합니다.

**단계 4** 기본 SSL 암호 해독 작업 구성



의심스러운 경우에는 Do Not Decrypt(암호 해독 안 함)를 기본 동작으로 선택합니다. 액세스 제어 정책은 여전히 필요한 경우 기본 SSL 암호 해독 규칙과 일치하는 트래픽을 삭제할 수 있습니다.

#### 단계 5 SSL 암호 해독 규칙 구성.

암호 해독할 트래픽과 적용할 암호 해독 유형을 확인합니다.

단계 6 알려진 키 암호 해독을 구성하는 경우 SSL 암호 해독 정책 설정을 편집하여 해당 인증서를 포함합니다. [알려진 키 및 재서명 암호 해독을 위한 인증서 구성](#)을 참조하십시오.

단계 7 필요시 재서명 암호 해독 규칙에 사용된 CA 인증서를 다운로드하고 클라이언트 워크스테이션에서 브라우저에 업로드합니다.

인증서를 다운로드하고 클라이언트에게 배포하는 데 대한 자세한 내용은 [재서명 암호 해독 규칙을 위한 CA 인증서 다운로드](#)를 참조하십시오.

단계 8 주기적으로 재서명 및 알려진 키 인증서를 업데이트합니다.

- 재서명 인증서 - 만료되기 전에 이 인증서를 업데이트합니다. Firepower Device Manager를 통해 인증서를 생성하는 경우, 유효 기간은 5년입니다. 인증서 만료 시기를 확인하려면 Objects(개체) 페이지에서 인증서의 보기 아이콘을 클릭합니다.
- 알려진 키 인증서 - 모든 알려진 키 암호 해독 규칙의 경우 대상 서버의 현재 인증서와 키를 업로드했는지 확인해야 합니다. 또한, 지원되는 서버에서 인증서와 키가 변경될 때마다 새 인증서와 키를 내부 인증서로 업로드하고 새 인증서를 사용하도록 SSL 암호 해독 설정을 업데이트해야 합니다.

단계 9 외부 서버에 대해 누락된, 신뢰할 수 있는 CA 인증서를 업로드합니다.

시스템에는 신뢰할 수 있는 CA 루트 및 중간 인증서(서드파티에서 발급)가 다양하게 포함되어 있습니다. 이러한 항목은 암호 해독 재서명 규칙에 대해 FDM 관리 디바이스와 대상 서버 간의 연결을 협상할 때 필요합니다.

루트 CA의 트러스트 체인 내의 모든 인증서를 신뢰할 수 있는 CA 인증서 목록에 업로드하며, 여기에는 루트 CA 인증서 및 모든 중간 CA 인증서가 포함됩니다. 이렇게 하지 않으면 중간 CA가 발급한 신뢰할 수 있는 인증서를 탐지하는 것이 더 어려워집니다. Objects(개체) > Certificates(인증서) 페이지에서 인증서를 업로드합니다. [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#) > 재사용 가능한 개체 > 인증서 > 신뢰할 수 있는 CA 인증서 업로드를 참조하십시오.

## SSL 암호 해독 정보

일반적으로 액세스 제어 정책은 네트워크 연결을 허용할지 차단할지 결정합니다. 그러나 SSL 암호 해독 정책을 활성화하는 경우에는 암호화된 연결이 가장 먼저 SSL 암호 해독 정책을 통해 암호가 해독되어야 하는지 아니면 차단되어야 하는지가 결정됩니다. 암호 해독 여부와 관계없이 차단되지 않은 모든 연결은 액세스 제어 정책을 통해 최종 허용/차단 여부가 결정됩니다.



**Note** ID 정책에서 활성 인증 규칙을 구현하려면 SSL 암호 해독 정책을 활성화해야 합니다. SSL 암호 해독을 활성화하여 ID 정책을 활성화하되 다른 방법으로는 SSL 암호 해독을 구현하지 않으려는 경우에는 SSL Decryption(SSL 암호 해독) 페이지에서 Do Not Decrypt(암호 해독 안 함)를 기본 작업으로 선택하고 추가 SSL 암호 해독 규칙을 생성하지 마십시오. ID 정책은 필요한 규칙이라면 무엇이든 자동으로 생성합니다.

다음 주제에서는 암호화된 트래픽 플로우 관리 및 암호 해독에 대해 자세히 설명합니다.

- [SSL 암호 해독을 구현하는 이유](#)
- [자동 생성된 SSL 암호 해독 규칙](#)
- [암호 해독이 불가능한 트래픽 처리](#)

## SSL 암호 해독을 구현하는 이유

HTTPS 연결과 같이 암호화된 트래픽은 검사할 수 없습니다. 은행 및 기타 금융 기관에 대한 연결 등 많은 연결이 합법적으로 암호화되어 있으며, 많은 웹 사이트에서 암호화를 사용하여 개인 정보 또는 민감한 데이터를 보호합니다. 예를 들어, Firepower Device Manager에 대한 연결은 암호화됩니다. 그러나 사용자는 암호화된 연결 내에서 부적절한 트래픽을 숨길 수도 있습니다.

SSL 암호 해독을 구현함으로써 연결을 암호 해독하고, 연결에 위협 또는 다른 부적절한 트래픽이 포함되어 있지 않은지 검사한 다음, 연결을 계속하도록 허용하기 전에 재암호화할 수 있습니다. 암호 해독된 트래픽은 액세스 제어 정책을 통과하고 암호 해독된 연결의 검사받은 특성(암호화된 특성 아님)을 기반으로 하는 규칙과 일치합니다. 따라서 액세스 제어 정책을 적용해야 하는 필요와 민감한 정보를 보호해야 하는 사용자의 필요 간의 균형을 유지할 수 있습니다.

또한, 네트워크에 원하지 않는 유형의 암호화된 트래픽을 차단하기 위해 SSL 암호 해독 규칙을 구성할 수 있습니다.



**Caution** 트래픽을 암호 해독한 다음 재암호화하면 디바이스의 처리 부하가 증가하므로 전체 시스템 성능이 감소된다는 점에 유의하십시오.

## 암호화된 트래픽에 적용할 수 있는 작업

SSL 암호 해독 규칙을 구성할 때 다음 주제에 설명된 작업을 적용할 수 있습니다. 이러한 작업은 명시적인 규칙과 일치하지 않는 모든 트래픽에 적용되는 기본 작업에도 사용할 수 있습니다.

- [재서명 암호 해독](#)
- [알려진 키 암호 해독](#)
- [암호 해독 안 함](#)
- [차단](#)



**Note** SSL 암호 해독 정책을 통과하는 모든 트래픽은 이후에 액세스 제어 정책을 통과해야 합니다. SSL 암호 해독 정책에서 삭제하는 트래픽을 제외하고는 액세스 제어 정책에 따라 최종 허용/삭제 여부가 결정됩니다.

#### 재서명 암호 해독

트래픽 암호 해독 및 재서명을 선택하는 경우, 시스템이 MITM(Man-In-The-Middle) 역할을 합니다.

브라우저에서 <https://www.cisco.com>의 사용자 유형을 예로 들 수 있습니다. 트래픽이 FTD 디바이스에 도달하면 디바이스에서는 규칙에 지정된 CA 인증서를 사용하는 사용자와 협상하며 사용자와 FTD 디바이스 간에 SSL 터널을 구축합니다. 동시에 이 디바이스는 <https://www.cisco.com>에 접속하여 서버와 FTD 디바이스 간에 SSL 터널을 생성합니다.

따라서 사용자는 [www.cisco.com](https://www.cisco.com)에서 인증서 대신 SSL 암호 해독 규칙에 대해 구성된 CA 인증서를 보게 됩니다. 연결을 완료하려면 사용자가 인증서를 신뢰해야 합니다. 그러면 FTD 디바이스에서는 사용자와 대상 서버 간의 양방향 트래픽에서 암호 해독/재암호화를 수행합니다.



**Note** 클라이언트가 서버 인증서 재서명에 쓰이는 CA를 신뢰하지 않을 경우 신뢰할 수 없는 인증서임을 사용자에게 경고합니다. 이를 방지하려면 클라이언트가 신뢰하는 CA 저장소에 CA 인증서를 가져오십시오. 또는 조직에 개인 PKI가 있을 경우, 조직의 모든 클라이언트가 자동으로 신뢰하는 루트 CA에 의해 서명된 중간 CA 인증서를 발급한 다음 그 CA 인증서를 디바이스에 업로드할 수 있습니다.

Decrypt - Re-Sign(암호 해독 - 다시 서명) 작업으로 규칙을 구성할 경우 이 규칙은 구성된 규칙 조건과 더불어 참조된 내부 CA 인증서의 서명 알고리즘 유형을 기반으로 트래픽을 매칭합니다. SSL 암호 해독 정책용 단일 재서명 인증서를 선택할 수 있으므로 이 경우 재서명 규칙에 대한 트래픽 일치 제한할 수 있습니다.

예를 들어, 재서명 인증서가 EC(Elliptic Curve) 기반 CA 인증서인 경우에만 EC 알고리즘을 사용하여 암호화된 발신 트래픽이 재서명 암호 해독 규칙과 일치합니다. 이와 유사하게 글로벌 재서명 인증서가 RSA인 경우에만 RSA 알고리즘을 사용하여 암호화된 트래픽이 재서명 암호 해독 규칙과 일치합니다. 즉, 구성된 다른 모든 규칙 조건이 일치하더라도 EC 알고리즘을 사용하여 암호화된 발신 트래픽은 이 규칙과 일치하지 않습니다.

### 알려진 키 암호 해독

목적지 서버를 소유하고 있는 경우 알려진 키를 사용하여 암호 해독을 구현할 수 있습니다. 이 경우 사용자가 <https://www.cisco.com>에 대한 연결을 열면 인증서를 제시하는 FTD 디바이스인 경우에도 [www.cisco.com](https://www.cisco.com)에 대한 실제 인증서가 사용자에게 표시됩니다.



소속된 조직은 도메인 및 인증서의 소유자여야 합니다. [cisco.com](https://www.cisco.com)을 예로 들면, 엔드 유저가 Cisco 인증서를 확인할 수 있으려면 실제로 [cisco.com](https://www.cisco.com) 도메인을 소유(즉, 엔드 유저가 Cisco Systems)하고 공용 CA에서 서명한 [cisco.com](https://www.cisco.com) 인증서의 소유권을 갖고 있어야만 합니다. 조직이 소유한 사이트에 대해 알려진 키를 사용해야만 암호를 해독할 수 있습니다.

알려진 키로 암호 해독을 수행하는 주요 목적은 HTTPS 서버로 향하는 트래픽을 암호 해독하여 외부 공격으로부터 서버를 보호하는 것입니다. 외부 HTTPS 사이트에 대한 클라이언트 측 트래픽을 검사하기 위해서는 서버를 소유하고 있지 않으므로 재서명 암호 해독을 사용해야 합니다.



**Note** 알려진 키 암호 해독을 사용하려면 서버 인증서 및 키를 내부 ID 인증서로 업로드한 다음 SSL 암호 해독 정책 설정에서 알려진 키 인증서 목록에 추가해야 합니다. 그러면 서버 주소를 수신 주소로 사용하여 알려진 키 암호 해독에 대한 규칙을 구축할 수 있습니다. SSL 암호 해독 정책에 인증서를 추가하는 방법에 대한 자세한 내용은 [SSL 암호 해독 정책 구성](#)을 참조하십시오.

### 암호 해독 안 함

특정 유형의 트래픽은 암호 해독을 우회하도록 선택하는 경우, 해당 트래픽에는 처리 작업이 수행되지 않습니다. 암호화된 트래픽은 일치하는 액세스 제어 규칙을 기반으로 허용 또는 차단되는 액세스 제어 정책으로 계속 진행됩니다.

### 차단

SSL 암호 해독 규칙과 일치하는 암호화된 트래픽을 간단하게 차단할 수 있습니다. SSL 암호 해독 정책에서 차단 기능을 사용하면 액세스 제어 정책에 연결할 수 없게 됩니다.

HTTPS 연결을 차단하는 경우 사용자에게 시스템 기본 차단 응답 페이지가 표시되지 않습니다. 대신 보안 연결 실패를 나타내는 브라우저의 기본 페이지가 표시됩니다. 오류 메시지는 사이트가 정책으로 인해 차단되었음을 나타내지 않습니다. 대신 일반적인 암호화 알고리즘이 없다는 오류가 표시될 수 있습니다. 이 메시지만으로는 연결이 의도적으로 차단되었는지를 명확하게 파악할 수 없습니다.

### 자동 생성된 SSL 암호 해독 규칙

SSL 암호 해독 정책을 활성화하는지 여부에 관계없이 FDM 관리 장치는 활성 인증을 구현하는 각 ID 정책 규칙에 대해 Decrypt Re-sign 규칙을 자동으로 생성합니다. 이 작업은 HTTPS 연결에 대한 활성 인증을 활성화하는 데 필요합니다.

SSL 암호 해독 정책을 활성화하면 Identity Policy Active Authentication Rules(ID 정책 활성화 인증 규칙) 머리글 아래에서 이 규칙을 확인할 수 있습니다. 이러한 규칙은 SSL 암호 해독 정책 상단에 읽기 전용으로 그룹화되어 있습니다. ID 정책을 변경해야만 규칙을 변경할 수 있습니다.

### 암호 해독이 불가능한 트래픽 처리

연결의 암호 해독이 불가능하게 만드는 몇 가지 특성이 있습니다. 연결에 다음 특성이 있는 경우, 연결이 다른 방법으로 일치할 수 있는 어떤 규칙과도 관계없이 기본 작업이 연결에 적용됩니다. 암호 해독 안 함 대신 차단을 기본 작업으로 선택하는 경우, 합법적인 트래픽의 과도한 삭제를 포함한 문제가 발생할 수 있습니다.

- 압축된 세션 — 데이터 압축이 연결에 적용되었습니다.
- SSLv2 세션 — 지원되는 최소 SSL 버전은 SSLv3입니다.
- 알려지지 않은 암호 그룹 — 시스템에서 연결에 대한 암호 그룹을 인식하지 않습니다.
- 지원되지 않는 암호 그룹 — 시스템에서 탐지된 암호 그룹을 기반으로 암호 해독을 지원하지 않습니다.
- 세션이 캐시되지 않음 — SSL 세션에서 세션 재사용이 활성화되었고 클라이언트 및 서버가 세션 식별자로 세션을 재설정했으며 시스템에서 해당 세션 식별자를 캐시하지 않았습니다.
- 핸드셰이크 오류 — SSL 핸드셰이크 협상 중에 오류가 발생했습니다.
- 암호 해독 오류 — 암호 해독 작업 중에 오류가 발생했습니다.
- 패시브 인터페이스 트래픽 — 패시브 인터페이스(패시브 보안 영역)의 모든 트래픽은 암호 해독할 수 없습니다.

### SSL 암호 해독 정책을 위한 라이선스 요건

SSL 암호 해독 정책을 사용하는 데에는 특수 라이선스가 필요하지 않습니다.

그러나 URL 카테고리 및 평판을 일치 기준으로 사용하는 규칙을 생성하려면 URL 라이선스가 필요합니다. 라이선스 구성에 대한 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#) > 시스템 라이선싱 > 선택적 라이선스 활성화 또는 비활성화를 참조하십시오.

### SSL 암호 해독에 대한 지침

SSL 암호 해독 정책을 구성하고 모니터링할 때는 다음 사항에 유의하십시오.

- 액세스 제어 규칙이 다음에 해당할 때 신뢰 또는 차단으로 설정된 규칙과 일치하는 연결의 경우 SSL 암호 해독 정책이 우회됩니다.
  - 보안 영역, 네트워크, 지리위치 및 포트를 트래픽 일치 기준으로만 사용하는 경우.
  - 검사가 필요한 다른 규칙(예: 애플리케이션이나 URL을 기준으로 하는 연결과 일치하는 규칙) 앞에 오거나 침입 또는 파일 검사를 적용하는 규칙을 허용하는 경우.
- URL 카테고리 일치를 사용할 때는 사이트의 로그인 페이지가 사이트 자체의 카테고리나 다른 카테고리에 포함되는 경우가 있음을 고려해야 합니다. 예를 들어 Gmail은 "웹 기반 이메일" 범주

에 포함되지만, 로그인 페이지는 "인터넷 포털" 범주에 포함됩니다. 이러한 사이트에 대한 연결을 암호 해독하려면 두 카테고리를 모두 규칙에 포함해야 합니다.

- 활성 인증 규칙이 있는 경우에는 SSL 암호 해독 정책을 비활성화할 수 없습니다. SSL 암호 해독 정책을 비활성화하려면 ID 정책을 비활성화하거나 활성 인증을 사용하는 ID 규칙을 삭제해야 합니다.

## SSL 암호 해독 정책 구성

SSL 암호 해독 정책을 사용하여 암호화된 트래픽을 일반 텍스트 트래픽으로 전환할 수 있으므로 URL 필터링, 침입 및 악성코드 제어 그리고 기타 서비스(DPI(Deep Packet Inspection)를 필요로 함)를 적용할 수 있습니다. 정책에서 트래픽을 허용하는 경우, 트래픽은 디바이스를 떠나기 전에 다시 암호화됩니다.

SSL 암호 해독 정책은 암호화된 트래픽에만 적용됩니다. 암호화되지 않은 연결은 SSL 암호 해독 규칙을 기준으로 평가되지 않습니다.



### Caution

트래픽을 암호 해독한 다음 재암호화하면 디바이스의 처리 부하가 증가하므로 전체 시스템 성능이 감소된다는 점에 유의하십시오.



### Note

VPN 터널은 SSL 암호 해독 정책이 평가되기 전에 암호 해독되므로 정책은 터널에 적용되지 않습니다. 그러나 터널 내의 암호화된 연결은 모두 SSL 암호 해독 정책을 기준으로 평가받습니다.

다음 절차에서는 SSL 암호 해독 정책을 구성하는 방법에 대해 설명합니다. SSL 암호 해독 생성 및 관리의 엔드 투 엔드 프로세스에 대한 설명은 [SSL 암호 해독 정책을 구현 및 유지 관리하는 방법](#)을 참조하십시오.

## 절차

### Before you begin


SSL 암호 해독 규칙 테이블에는 다음과 같이 두 가지 섹션이 있습니다.

- **Identity Policy Active Authentication Rules(ID 정책 활성 인증 규칙)** - ID 정책을 활성화하고 활성 인증을 사용하는 규칙을 생성하는 경우, 시스템에서는 정책이 작동하도록 설정하는 데 필요한 SSL 암호 해독 규칙을 자동으로 생성합니다. 이러한 규칙은 항상 직접 생성하는 SSL 암호 해독 규칙보다 먼저 평가됩니다. 또한, 이러한 규칙은 ID 정책을 변경하는 방식으로 간접적으로만 변경할 수 있습니다.
- **SSL Native Rules(SSL 기본 규칙)** - 이미 구성된 규칙입니다. 규칙은 이 섹션에만 추가할 수 있습니다.

## Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 SSL 정책을 생성할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다.
- 단계 5 정책 표시줄에서 **SSL Decryption**(SSL 암호 해독)을 클릭합니다.
- 단계 6 정책을 아직 활성화하지 않은 경우 **Enable SSL Decryption**(SSL 암호 해독 활성화)을 클릭하여 **SSL 암호 해독 정책 활성화**에 설명된 대로 정책 설정을 구성합니다.
- 단계 7 정책의 기본 작업을 구성합니다. 가장 안전한 방법은 Do Not Decrypt(암호 해독 안 함)를 선택하는 것입니다. 자세한 내용은 디바이스에서 실행 중인 버전의 **Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드**에 나와 있는 보안 정책 장의 기본 **SSL** 암호 해독 작업 구성 섹션을 참조하십시오.
- 단계 8 SSL 암호 해독 정책을 관리합니다.

SSL 암호 해독 설정을 구성하고 나면 이 페이지에 모든 규칙이 순서대로 나열됩니다. 목록의 맨 위에서부터 규칙과 트래픽의 일치 여부를 확인하며, 첫 번째로 일치하는 규칙에 따라 적용할 작업이 결정됩니다. 이 페이지에서는 다음을 수행할 수 있습니다.

- 정책을 비활성화하려면 **SSL Decryption Policy**(SSL 암호 해독 정책) 토글을 클릭합니다. **Enable SSL Decryption**(SSL 암호 해독 활성화)을 클릭하여 다시 활성화할 수 있습니다.
- 정책에 사용된 인증서 목록을 포함하여 정책 설정을 편집하려면 SSL 툴바에서 구성 버튼 (**Configuration** **NGFW-Default-InternalCA**)을 클릭합니다. 또한, 클라이언트에게 배포할 수 있도록 재서명 암호 해독 규칙에 사용되는 인증서를 다운로드할 수 있습니다. 자세한 내용은 디바이스에서 실행 중인 버전의 **Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드**에 나와 있는 보안 정책 장에서 다음 섹션을 참조하십시오.
  - 알려진 키 및 재서명 암호 해독을 위한 인증서 구성
  - 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드
- 규칙을 구성하려면 다음을 수행합니다.
  - 새 규칙을 만들고 규칙이 생성하는 이벤트를 로깅하려면 파란색 더하기  버튼을 클릭합니다. **SSL 암호 해독 규칙 구성**을 참조하십시오.
  - 기존 규칙을 편집하려면 규칙 테이블에서 규칙을 클릭하고 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다. 테이블에서 속성을 클릭하여 규칙 속성을 선택적으로 수정할 수도 있습니다.
  - 더 이상 필요하지 않은 규칙을 삭제하려면 규칙 테이블에서 규칙을 클릭하고 **Actions**(작업) 창에서 **Remove**(제거)를 클릭합니다.

- 규칙을 이동하려면 규칙 테이블에서 규칙 위에 마우스를 올려놓습니다. 행의 끝에서 위쪽 및 아래쪽 화살표를 사용하여 규칙 테이블과 함께 해당 위치를 이동합니다.
- (선택 사항) 생성한 규칙에 대해 해당 규칙을 선택하고 Add Comments(코멘트 추가) 필드에 코멘트를 추가할 수 있습니다. 규칙 코멘트에 대한 자세한 내용은 [정책 및 규칙 집합의 규칙에 코멘트 추가](#)를 참조하십시오.

단계 9 [SSL 암호 해독 정책 활성화](#)를 참조하십시오.

## SSL 암호 해독 정책 활성화

SSL 암호 해독 규칙을 구성하기 전에 정책을 활성화하고 몇 가지 기본 설정을 구성해야 합니다. 다음 절차에서는 정책을 직접 활성화하는 방법에 대해 설명합니다. ID 정책을 활성화하는 경우에도 정책을 활성화할 수 있습니다. ID 정책의 경우 SSL 암호 해독 정책을 활성화해야 합니다.

### 절차

#### Before you begin

SSL 암호 해독 정책이 없는 릴리스에서 업그레이드했지만 활성 인증 규칙이 있는 ID 정책을 구성한 경우에는 SSL 암호 해독 정책이 이미 활성화되어 있습니다. 사용할 재서명 암호 해독 인증서를 선택하고 선택적으로 사전 정의된 규칙을 활성화합니다.

[SSL 암호 해독 정책 구성](#)을 검토하지 않았으면 살펴봅니다.

#### Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 **FTD** 탭을 클릭하고 SSL 암호 해독 정책을 활성화할 디바이스를 선택합니다.

단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다.

단계 5 정책 표시줄에서 **SSL Decryption**(SSL 암호 해독)을 클릭합니다.


단계 6 SSL 표시줄에서 **SSL Decryption**(SSL 암호 해독) 토글을 클릭하여 SSL 암호 해독 정책을 활성화합니다.

- 정책을 처음 활성화하는 경우 **Decrypt Known-Key**(알려진 키 암호 해독) 및 **Decrypt Re-Sign SSL**(재서명 SSL 암호 해독) 암호 해독의 설명을 읽고 **Enable**(활성화)을 클릭합니다.
- 이미 한 번 정책을 구성했다가 비활성화한 경우, 간단히 이전 설정 및 규칙을 사용하여 정책을 다시 활성화할 수 있습니다. SSL 암호 해독 구성 버튼 **Configuration** **NGFW-Default-InternalCA** **알려진 키 및 재서명 암호 해독을 위한 인증서 구성**을 클릭하고 설명된 대로 설정을 구성할 수 있습니다.



단계 7 **Select Decrypt Re-Sign Certificate**(암호 해독 재서명 인증서 선택)의 경우 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다.

사전 정의된 NGFW-Default-InternalCA 인증서를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다. 인증서가 아직 없으면 **Create**(생성)를 클릭하여 FDM 관리 디바이스 내부 CA 인증서를 추가합니다.

클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼  을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. **재서명 암호 해독 규칙을 위한 CA 인증서 다운로드**를 참조하십시오.

단계 8 **Save**(저장)를 클릭합니다.

단계 9 **기본 SSL 암호 해독 작업 구성**을 계속 진행하여 정책에 대한 기본 작업을 설정합니다.

## 기본 SSL 암호 해독 작업 구성

특정 SSL 암호 해독 규칙과 일치하지 않는 암호화된 연결은 SSL 암호 해독 정책의 기본 작업에 의해 처리됩니다.

## 절차

### Before you begin

아직 수행하지 않은 경우 다음 절차를 검토하고 해당 절차를 따르십시오.

1. [SSL 암호 해독 정책 구성](#)
2. [SSL 암호 해독 정책 활성화](#)

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 기본 SSL 암호 해독 작업을 구성할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다.
- 단계 5 정책 표시줄에서 **SSL Decryption**(SSL 암호 해독)을 클릭합니다.
- 단계 6 **Default Action**(기본 작업) 버튼을 클릭합니다.
- 단계 7 일치하는 트래픽에 적용할 작업을 선택합니다.

- **Do Not Decrypt**(암호 해독 안 함) - 암호화된 연결을 허용합니다. 그러면 액세스 제어 정책이 암호화된 연결을 평가하고 액세스 제어 규칙을 기반으로 삭제 또는 허용합니다.
- **Block**(차단) - 연결을 즉시 삭제합니다. 연결은 액세스 제어 정책으로 전달되지 않습니다.

**단계 8** (선택 사항). 기본 작업에 대한 로깅을 구성합니다. SSL 암호 해독 정책에서 이벤트를 캡처하려면 로깅을 활성화해야 합니다. 다음 옵션 중에서 선택합니다.

- **At End of Connection**(연결 종료 시) — 연결 종료 시 이벤트를 생성합니다.
  - **Send Connection Events To**(다음으로 연결 이벤트 보내기) — 외부 시스템 로그 서버로 이벤트의 복사본을 전송하려는 경우 시스템 로그 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server**(새 Syslog 서버 생성)를 클릭하여 개체를 생성합니다. syslog 서버에 대한 로깅을 비활성화하려면 서버 목록에서 **Any**(모두)를 선택합니다.

디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.

Cisco Security Analytics and Logging을 구독한 경우 [Cisco Defense Orchestrator 이벤트 로깅에 FDM 이벤트 전송](#). 이 기능에 대한 자세한 내용은 [FDM-관리 디바이스에 대한 보안 로깅 분석](#)을 참조하십시오.
- **No Logging**(로깅 없음) — 이벤트를 생성하지 않습니다.

**단계 9** **Save**(저장)를 클릭합니다.

**단계 10** 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## SSL 암호 해독 규칙 구성

SSL 암호 해독 규칙을 사용하여 암호화된 연결 처리 방법을 결정합니다. SSL 암호 해독 정책의 규칙은 위에서부터 아래로 평가됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다.

SSL 기본 규칙 섹션에서만 규칙을 생성하고 편집할 수 있습니다.



**Caution** 트래픽을 암호 해독한 다음 재암호화하면 디바이스의 처리 부하가 증가하므로 전체 시스템 성능이 감소된다는 점에 유의하십시오.



**Note** VPN 연결(사이트 대 사이트 및 원격 액세스 모두)에 대한 트래픽은 SSL 암호 해독 정책이 연결을 평가하기 전에 암호 해독됩니다. 따라서 SSL 암호 해독 규칙은 VPN 연결에 적용되지 않으며 이러한 규칙을 생성할 때 VPN 연결을 고려할 필요가 없습니다. 그러나 VPN 터널 내에서 사용된 암호화된 연결은 모두 평가됩니다. 예를 들어, RA VPN 연결을 통과하는 내부 서버에 대한 HTTPS 연결은 SSL 암호 해독 규칙을 기준으로 평가됩니다. 단, RA VPN 터널 자체는 이미 암호 해독되어 있으므로 이를 통과하는 경우에는 평가되지 않습니다.

## 절차




**Before you begin**

SSL 암호 해독 정책 구성, SSL 암호 해독 정책 활성화, 기본 SSL 암호 해독 작업 구성을 살펴보지 않은 경우 검토하여 규칙이 추가될 SSL 암호 해독 정책을 구성합니다.

알려진 키 암호 해독 규칙을 생성하는 경우, 목적지 서버(내부 인증서 역할)의 인증서 및 키를 업로드하고, SSL 암호 해독 정책 설정을 편집하여 이 인증서를 사용합니다. 알려진 키 규칙은 일반적으로 규칙의 대상 네트워크 기준에서 목적지 서버를 지정합니다. 자세한 내용은 [알려진 키 및 재서명 암호 해독을 위한 인증서 구성](#)을 참조하십시오.

**Procedure**

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 SSL 암호 해독 정책을 활성화할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다.
- 단계 5 정책 표시줄에서 **SSL Decryption**(SSL 암호 해독)을 클릭합니다.
- 단계 6 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 파란색 더하기  버튼을 클릭합니다.
- 기존 규칙을 편집하려면 해당 규칙의 편집  아이콘을 클릭합니다.
- 더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 제거  아이콘을 클릭합니다.

- 단계 7 **Order**(순서)에서 번호가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.

SSL Native Rules(SSL 기본 규칙) 섹션에만 규칙을 삽입할 수 있습니다. Identity Policy Active Authentication Rules(ID 정책 활성화 인증 규칙)가 ID 정책에서 자동으로 생성되며, 이 규칙은 읽기 전용입니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

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

- 단계 8 **Name**(이름)에 규칙의 이름을 입력합니다.

이름에는 공백을 포함할 수 없지만, 영숫자 및 특수 문자(+, ,, \_ , -)는 사용할 수 있습니다.


- 단계 9 일치하는 트래픽에 적용할 작업을 선택합니다. 각 옵션에 대한 자세한 내용은 다음을 참조하십시오.

- [재서명 암호 해독](#)

- 알려진 키 암호 해독
- 암호 해독 안 함
- 차단

단계 10 다음 탭을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source/Destination(소스/대상)** - 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 TCP 포트입니다. 기본값은 영역, 주소, 지리적 위치 및 TCP 포트입니다. [SSL 암호 해독 규칙에 대한 소스/대상 기준](#)을 참조하십시오.
- **URL** - 웹 요청의 URL 카테고리입니다. 기본값은 일치를 위해 고려되지 않은 URL 카테고리 및 평판입니다. [SSL 암호 해독 규칙에 대한 URL 기준](#)을 참조하십시오.
- **Application(애플리케이션)** - 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터 또는 애플리케이션입니다. 기본값은 암호화된 애플리케이션입니다. [SSL 암호 해독 규칙에 대한 애플리케이션 기준](#)을 참조하십시오.
- **사용자** - 사용자 또는 사용자 그룹입니다. ID 정책에 따라 트래픽 일치에 사용자 및 그룹 정보를 사용할 수 있는지가 결정됩니다. 이 기준을 사용하려면 ID 정책을 구성해야 합니다. [SSL 암호 해독 규칙에 대한 사용자 기준](#)을 참조하십시오.
- **Advanced(고급)** - SSL/TLS 버전 및 인증서 상태와 같이 연결에서 사용하는 인증서에서 파생된 특성입니다. [SSL 암호 해독 규칙에 대한 고급 기준](#)을 참조하십시오.

조건을 수정하려면 해당 조건 내의 파란색 더하기  버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화 상자에서 **Select(선택)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 **Create New Object(새 개체 생성)**를 클릭하면 됩니다. 개체 또는 요소의 x를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

SSL 암호 해독 규칙에 조건을 추가하는 경우 다음 팁을 고려하십시오.

- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용하려면 트래픽이 규칙의 모든 조건과 일치해야 합니다. 예를 들어, URL 카테고리를 기반으로 트래픽을 암호 해독하는 단일 규칙을 사용할 수 있습니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 어느 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어, 최대 50개의 애플리케이션 또는 애플리케이션 필터에 대해 애플리케이션 제어를 적용하는 단일 규칙을 사용할 수 있습니다. 따라서 단일 조건의 항목 간 관계는 OR이고 조건 유형 간의 관계(예: 소스/대상과 애플리케이션 간의 관계)는 AND가 됩니다.
- 일치하는 URL 범주에는 URL 라이선스가 필요합니다.

단계 11 (선택 사항). 규칙에 대해 로깅을 구성합니다.

대시보드 데이터 또는 이벤트 뷰어에 포함될 규칙과 일치하는 트래픽에 대한 로깅을 활성화해야 합니다. 다음 옵션 중에서 선택합니다.

- **No Logging(로깅 없음)** — 이벤트를 생성하지 않습니다.

- **Send Connection Events To**(다음으로 연결 이벤트 보내기) — 외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우, syslog 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create**(생성)를 클릭하여 개체를 생성합니다. syslog 서버에 대한 로깅을 비활성화하려면 서버 목록에서 Any(모두)를 선택합니다.
- **At End of Connection**(연결 종료 시) — 연결 종료 시 이벤트를 생성합니다. 디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.

Cisco Security Analytics and Logging을 구독한 경우 보안 이벤트 커넥터의 IP 주소와 포트를 사용하여 [SaaS\(Secure Logging Analytics\)](#)를 위한 시스템 로그 서버 개체 생성하거나 지정합니다. 자세한 내용은 [Cisco Security Analytics and Logging\(Cisco 보안 분석 및 기록\)](#)을 참조하십시오.


단계 12 **Save**(저장)를 클릭합니다.

단계 13 (선택 사항) 생성한 규칙에 대해 해당 규칙을 선택하고 **Add Comments**(코멘트 추가) 필드에 코멘트를 추가할 수 있습니다. 규칙 코멘트에 대한 자세한 내용은 [정책 및 규칙 집합의 규칙에 코멘트 추가](#)를 참조하십시오.

단계 14 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#)하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## SSL 암호 해독 규칙에 대한 소스/대상 기준

SSL 암호 해독 규칙의 소스/대상 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 TCP 포트를 정의합니다. 기본값은 영역, 주소, 지리적 위치 또는 TCP 포트입니다. TCP는 SSL 암호 해독 규칙과 일치되는 유일한 프로토콜입니다.

조건을 수정하려면 해당 조건 내의 파란색  버튼을 클릭하고 원하는 개체 또는 요소를 선택한 다음 **Select**(선택)를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 **Create New Object**(새 개체 생성)를 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

소스 영역, 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 외부 호스트에서 내부 호스트로 이동하는 모든 트래픽을 암호 해독하려는 경우에는 외부 영역을 Source Zones(소스 영역)로, 내부 영역을 Destination Zones(대상 영역)로 선택합니다.

소스 네트워크, 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.

규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 메뉴 옵션에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다.



**Note** 알려진 키 암호 해독 규칙의 경우 업로드한 인증서와 키를 사용하는 목적지 서버의 IP 주소를 사용하는 개체를 선택합니다.

- 국가/대륙 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다.
- 사용자 지정 지리위치 - 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

소스 포트, 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP 프로토콜 및 포트는 SSL 암호 해독 규칙에 대해서만 지정할 수 있습니다.

- TCP 포트에서 발생하는 트래픽을 일치시키려면 Source Ports(소스 포트)를 구성합니다.
- TCP 포트에 향하는 트래픽을 일치시키려면 Destination Ports/Protocols(대상 포트/프로토콜)를 구성합니다.

특정 TCP 포트에서 발생하는 트래픽과 특정 TCP 포트에 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

단계 10


## SSL 암호 해독 규칙에 대한 애플리케이션 기준

SSL 암호 해독 규칙의 애플리케이션 기준은 유형, 카테고리, 태그, 위험 또는 사업 타당성에 따라 애플리케이션을 정의하는 필터 또는 IP 연결에 사용되는 애플리케이션을 정의합니다. 기본값은 SSL 프로토콜 태그가 있는 모든 애플리케이션입니다. SSL 암호 해독 규칙은 어떤 암호화되지 않은 애플리케이션과도 일치시킬 수 없습니다.

규칙에서 개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 암호 해독하거나 차단하는 SSL 암호 해독 규칙을 생성할 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 암호 해독되거나 차단됩니다.

이와 더불어 Cisco에서는 시스템 및 VDB(Vulnerability Database)를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션에 대한 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

규칙에서 애플리케이션 및 필터를 직접 지정하거나 이러한 특성을 정의하는 애플리케이션 필터 개체를 생성할 수 있습니다. 이 두 가지 경우의 사양은 동일하지만, 개체를 사용하면 복잡한 규칙을 생성할 때에도 시스템 제한(기준당 항목 50개)을 유지하기가 더욱 쉽습니다.

애플리케이션 및 필터 목록을 수정하려면 조건 내의  버튼을 클릭하고 원하는 애플리케이션 또는 애플리케이션 필터 개체를 선택한 다음 팝업 대화 상자에서 Select(선택)와 Save(저장)를 차례로 클릭합니다. 애플리케이션, 필터 또는 개체에 대해 x를 클릭하면 정책에서 해당 항목을 제거할 수 있습니다. Save As Filter(필터로 저장) 링크를 클릭하면 아직 개체가 아닌 결합된 기준을 새 애플리케이션 필터 개체로 저장할 수 있습니다.

애플리케이션 기준과 고급 필터를 구성하고 애플리케이션을 선택하는 방법에 대한 자세한 내용은 [Firepower 애플리케이션 필터 개체 생성 및 편집](#)을 참조하십시오.

SSL 암호 해독 규칙에서 애플리케이션 기준을 사용할 때 다음 팁을 고려합니다.

- 시스템은 StartTLS를 사용하여 암호화되는 해독된 애플리케이션을 식별할 수 있습니다. 여기에는 SMTPS, POPS, FTPS, TelnetS, IMAPS 같은 애플리케이션이 포함됩니다. 또한, 시스템은 TLS ClientHello 메시지 내 서버 이름 지표 또는 서버 인증서 주체 고유 이름 값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다.
- 시스템은 서버 인증서 교환 이후에만 애플리케이션을 식별할 수 있습니다. SSL 핸드셰이크 중에 교환된 트래픽이 애플리케이션 조건을 포함하는 SSL 규칙의 다른 모든 조건과 일치하지만 식별이 완료되지 않은 경우, SSL 정책을 사용하여 패킷을 통과하도록 할 수 있습니다. 이러한 동작을 통해 핸드셰이크가 완료되므로 애플리케이션을 식별할 수 있습니다. 시스템에서 식별을 완료하면, 애플리케이션 조건과 매칭되는 나머지 세션 트래픽에 SSL 규칙 작업을 적용합니다.

## 단계 10

### SSL 암호 해독 규칙에 대한 URL 기준

SSL 암호 해독 규칙의 URL 기준은 웹 요청의 URL이 속하는 카테고리를 정의합니다. 또한, 암호 해독, 차단 또는 암호 해독 없이 허용할 사이트의 상대적인 평판을 지정할 수 있습니다. 기본값은 URL 카테고리를 기반으로 하는 연결과 일치하지 않습니다.

예를 들어, 암호화된 모든 게임 사이트를 차단하거나 위험이 높은 모든 소셜 네트워킹 사이트를 암호 해독할 수 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL을 찾아보려고 시도하는 경우, 세션이 차단 또는 암호 해독됩니다.

SSL 암호 해독 규칙에 URL 기준을 추가하려면 다음을 수행합니다.

## Procedure

단계 1 URL 탭을 클릭하여 SSL 암호 해독 규칙에 URL 범주를 추가합니다.

단계 2 차단할 URL 범주를 검색하여 선택합니다.

단계 3 기본적으로 선택한 범주의 URL에서 오는 트래픽은 보안 평판과 상관없이 SSL 암호 해독 규칙에 의해 암호 해독됩니다. 그러나 평판에 따라 일부 사이트를 암호 해독에서 제외하도록 규칙의 URL 범주 또는 모든 URL 범주를 미세 조정할 수 있습니다.

- URL에서 단일 범주의 평판을 세부 조정하려면 다음을 수행합니다.

- a. 선택한 URL 범주를 클릭합니다.
- b. **Any Reputation**(모든 평판)의 선택을 취소합니다.
- c. 녹색 슬라이더를 오른쪽으로 밀어 규칙에서 제외할 URL 평판 설정을 선택하고 **Save**(저장)를 클릭합니다.

슬라이더의 범위에 포함된 평판은 규칙의 영향에서 제외됩니다. 예를 들어, 녹색 슬라이더를 **Benign Sites**(무해한 사이트)로 이동하면 **Well Known Sites**(잘 알려진 사이트) 및 무해한 사이트는 선택한 범주에 대한 SSL 암호 해독 규칙의 영향에서 제외됩니다. 보안 위험이 있는 사이트, 의심스러운 사이트 및 고위험 사이트로 간주되는 URL은 여전히 해당 URL 범주에 대한 규칙의 영향을 받습니다.

- 규칙에 추가한 모든 URL 범주의 평판을 세부적으로 조정하려면 다음을 수행합니다.

- a. SSL 암호 해독 규칙에 포함할 모든 범주를 선택한 후 **Apply Reputation to Selected Categories**(선택한 범주에 평판 적용)를 클릭합니다.
- b. **Any Reputation**(모든 평판)의 선택을 취소합니다.
- c. 녹색 슬라이더를 오른쪽으로 밀어 규칙에서 제외할 URL 평판 설정을 선택하고 **Save**(저장)를 클릭합니다.

슬라이더의 범위에 포함된 평판은 규칙의 영향에서 제외됩니다. 예를 들어, 녹색 슬라이더를 **Benign Sites**(무해한 사이트)로 이동하면 **Well Known Sites**(잘 알려진 사이트) 및 무해한 사이트는 선택한 모든 범주에 대한 SSL 암호 해독 규칙의 영향에서 제외됩니다. 보안 위험이 있는 사이트, 의심스러운 사이트 및 고위험 사이트로 간주되는 URL은 여전히 모든 URL 범주에 대한 규칙의 영향을 받습니다.

단계 4 **Select**(선택)를 클릭합니다.

단계 5 **Save**(저장)를 클릭합니다.



## 단계 10

### SSL 암호 해독 규칙에 대한 사용자 기준

SSL 암호 해독 규칙의 사용자 기준은 IP 연결의 사용자 또는 사용자 그룹을 정의합니다. 규칙에 사용자 또는 사용자 그룹 기준을 포함하려면 ID 정책 및 관련 디렉터리 서버를 구성해야 합니다.

ID 정책에 따라 특정 연결에 대해 사용자 ID가 수집되는지가 결정됩니다. ID가 설정된 경우에는 호스트의 IP 주소가 식별된 사용자와 연결됩니다. 그러므로 해당 소스 IP 주소가 사용자에게 매핑된 트래픽은 해당 사용자가 보내는 것으로 간주됩니다. IP 패킷 자체는 사용자 ID 정보를 포함하지 않으므로 이 IP 주소에서 사용자로의 매핑은 가능한 최적의 근사치입니다.

규칙에는 최대 50개의 사용자나 그룹을 추가할 수 있으므로 일반적으로는 개별 사용자를 선택하는 것보다 그룹을 선택하는 것이 더 효율적입니다. 예를 들어 외부 네트워크에서 오는 엔지니어링 그룹에 대한 트래픽을 해독하는 규칙을 생성하고 이 그룹에서 나오는 발신 트래픽의 암호를 해독하지 않는 별도의 규칙을 만들 수 있습니다. 그러면 신규 엔지니어에 대해 규칙을 적용하려는 경우 디렉터리 서버의 엔지니어링 그룹에 해당 엔지니어를 추가하기만 하면 됩니다.

사용자 목록을 수정하려면 조건 내에서 + 버튼을 클릭하고 원하는 사용자 그룹을 선택한 후 Select(선택)를 클릭합니다.

## 단계 10

### SSL 암호 해독 규칙에 대한 고급 기준

고급 트래픽 일치 기준은 연결에 사용되는 인증서에서 파생된 특성과 관련이 있습니다. 다음 옵션 중 하나 또는 모두를 구성할 수 있습니다.

#### 인증서 속성

선택한 속성 중 하나와 일치하는 트래픽은 규칙의 인증서 속성 옵션과 일치합니다. 다음을 구성할 수 있습니다.

- **Certificate Status**(인증서 상태): 인증서 상태가 Valid(유효함) 또는 Invalid(유효하지 않음)인지 여부입니다. 인증서 상태가 중요하지 않은 경우, Any(모두)(기본값)를 선택합니다. 인증서는 다음 조건을 모두 충족하는 경우 유효한 것으로 간주되며, 그렇지 않은 경우에는 유효하지 않습니다.
  - 정책이 인증서를 발급한 CA를 신뢰합니다.
  - 인증서의 내용에 대해 인증서의 서명을 제대로 검증할 수 있습니다.
  - 발급자 CA 인증서가 정책의 신뢰할 수 있는 CA 인증서 목록에 저장됩니다.
  - 정책의 신뢰할 수 있는 CA 중 인증서를 취소한 CA가 없습니다.
  - 현재 날짜가 인증서의 유효 시작일과 유효 만료일 사이에 해당합니다.
- **Self-Signed**(자체 서명됨): 서버 인증서에 동일한 주체 및 발급자 고유 이름이 포함되어 있는지 여부입니다. 다음 중 하나를 선택합니다.

- Self-Signing(자체 서명) — 서버 인증서가 자체 서명되었습니다.
- CA-Signing(CA 서명) — 서버 인증서가 CA(인증 기관)에 의해 서명되었습니다. 즉, 발급자와 주체가 동일하지 않습니다.
- Any(모두) — 인증서가 일치 기준으로 자체 서명되었는지를 신경 쓰지 않습니다.

#### 지원되는 버전

일치하는 SSL/TLS 버전입니다. 규칙은 선택한 버전 중 하나를 사용하는 트래픽에 적용됩니다. 기본값은 모든 버전입니다. 다음에서 선택: SSLv3.0, TLSv1.0, TLSv1.1, TLSv1.2.


예를 들어 TLSv1.2 연결만 허용하려는 경우 TLSv1.2 이외의 버전에 대한 차단 규칙을 생성할 수 있습니다. 나열되지 않은 버전(예: SSL v2.0)을 사용하는 트래픽은 SSL 암호 해독 정책에 대한 기본 작업에 의해 처리됩니다.

#### 단계 10

## 알려진 키 및 재서명 암호 해독을 위한 인증서 구성


재서명하거나 알려진 키를 사용하여 암호 해독을 구현하는 경우, SSL 암호 해독 규칙에서 사용할 수 있는 인증서를 식별해야 합니다. 모든 인증서가 유효하고 만료되지 않았는지 확인합니다.


특히 알려진 키 암호 해독의 경우, 암호 해독 중인 연결을 지닌 각 목적지 서버의 현재 인증서 및 키가 시스템에 있는지 확인해야 합니다. 알려진 키 암호 해독 규칙과 함께 암호 해독을 위해 목적지 서버의 실제 인증서와 키를 사용합니다. 따라서 FDM 관리 디바이스에는 항상 현재 인증서 및 키가 있어야 합니다. 그렇지 않으면 암호 해독에 실패합니다.


알려진 키 규칙으로 목적지 서버에서 인증서 또는 키를 변경할 때마다 새로운 내부 인증서와 키를 업로드합니다. 단, 내부 CA 인증서가 아니라 내부 인증서로 업로드합니다. 다음 절차 중에 인증서를 업로드하거나,  버튼을 클릭하고 **FTD > Certificate(인증서)**를 선택하여 인증서를 **Objects(개체)** 페이지에 업로드할 수 있습니다.

로드하거나,  버튼을 클릭하고 **FTD > Certificate(인증서)**를 선택하여 인증서를 **Objects(개체)** 페이지에 업로드할 수 있습니다.

#### Procedure

- 단계 1 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.
- 단계 2 **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 SSL 정책을 생성할 디바이스를 선택한 다음 오른쪽의 **Management(관리)** 창에서 **Policy(정책)**를 클릭합니다.
- 단계 4 정책 표시줄에서 **SSL Decryption(SSL 암호 해독)**을 클릭합니다.
- 단계 5 SSL 암호 해독 정책 표시줄에서 인증서 버튼  을 클릭합니다.
- 단계 6 SSL Decryption Configuration(SSL 암호 해독 구성) 대화 상자에서 **Select Decrypt Re-Sign Certificate(암호 해독 재서명 인증서 선택)** 메뉴를 클릭하고 다시 서명된 인증서로 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택하거나 생성합니다. 사전 정의된 **NGFW-Default-InternalCA** 인증서를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다.

클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼  을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. 또한 디바이스에서 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 보안 정책 장의 암호 해독 규칙을 위한 CA 인증서 다운로드 섹션을 참조하십시오.

- 단계 7 알려진 키를 사용하여 암호를 해독하는 각 규칙의 경우 목적지 서버의 내부 인증서 및 키를 업로드합니다.
- 단계 8 **Decrypt Known-Key Certificates**(알려진 키 암호 해독 인증서) 아래에서  를 클릭합니다.
- 단계 9 내부 ID 인증서를 선택하거나 **Create New Internal Certificate**(새 내부 인증서 생성)를 클릭하여 바로 업로드합니다.
- 단계 10 **Save**(저장)를 클릭합니다.
- 단계 11 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#)하거나 기다렸다가 여러 번 변경 사항을 한 번에 구축합니다.

## 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드

트래픽을 암호 해독하려는 경우, 사용자는 TLS/SSL을 사용하는 애플리케이션에서 신뢰할 수 있는 루트 인증 기관으로 정의된 암호화 프로세스에 사용되는 내부 CA 인증서를 보유하고 있어야 합니다. 일반적으로 인증서를 생성하거나 인증서를 하나 가져오게 되는 경우, 해당 인증서는 아직 이러한 애플리케이션에서 신뢰할 수 있는 인증서로 정의되어 있지 않습니다. 기본적으로 대부분의 웹 브라우저에서는 사용자가 HTTPS 요청을 전송할 때 클라이언트 애플리케이션에서 웹 사이트의 보안 인증서에 문제가 있음을 알려주는 경고 메시지를 표시합니다. 일반적으로 오류 메시지는 신뢰할 수 있는 인증 기관에서 웹 사이트의 보안 인증서를 발행한 것이 아니거나 알 수 없는 기관에서 웹 사이트를 인증했음을 나타냅니다. 하지만 경고는 MITM(Man-In-The-Middle) 공격이 진행 중일 수 있다는 점을 나타낼 수도 있습니다. 일부 다른 클라이언트 애플리케이션은 사용자에게 이 경고 메시지를 표시하지 않으며 사용자가 인식할 수 없는 인증서를 수락하도록 허용하지도 않습니다.

사용자에게 필수 인증서를 제공하는 데에는 다음과 같은 옵션이 있습니다.

루트 인증서를 수락하도록 사용자에게 알림

조직의 사용자에게 회사의 새로운 정책에 대해 알리고 조직에서 제공하는 루트 인증서를 신뢰할 수 있는 소스로 수락하도록 통지할 수 있습니다. 사용자는 다음에 사이트에 액세스할 때 다시 프롬프트가 나타나지 않도록 인증서를 수락하고 신뢰할 수 있는 루트 인증 기관 보관 영역에 저장해야 합니다.



**Note** 사용자는 대체 인증서를 생성한 CA 인증서를 수락하고 신뢰해야 합니다. 대신 사용자가 대체 서버 인증서를 신뢰하는 경우, 사용자는 방문하는 서로 다른 각 HTTPS 사이트에 대해 계속 경고를 보게 됩니다.

클라이언트 디바이스에 루트 인증서 추가

신뢰할 수 있는 루트 인증 기관으로 네트워크에 있는 모든 클라이언트 디바이스에 루트 인증서를 추가할 수 있습니다. 이렇게 하면 클라이언트 애플리케이션이 루트 인증서를 포함하는 트랜잭션을 자동으로 수락합니다.

인증서를 이메일 발송하거나 공유 사이트에 배치하는 방식을 통해 사용자가 인증서를 사용할 수 있게 하거나 인증서를 기업 워크스테이션 이미지에 통합하고 애플리케이션 업데이트 시설을 사용하여 사용자에게 자동으로 배포되게 할 수 있습니다.

다음 절차에서는 내부 CA 인증서를 다운로드하고 Windows 클라이언트에 설치하는 방법에 대해 설명합니다.

## 절차


프로세스는 운영 체제 및 브라우저의 유형에 따라 달라집니다. 예를 들어, Windows에서 실행 중인 Internet Explorer 및 Chrome에는 다음과 같은 프로세스를 사용할 수 있습니다. Firefox의 경우 **Tools(툴) > Options(옵션) > Advanced(고급)** 페이지를 통해 설치합니다.

성공적으로 가져왔음을 알리는 메시지가 표시됩니다. 잘 알려진 서드파티 인증 기관에서 인증서를 얻는 대신 자체 서명 인증서를 생성한 경우 Windows에서 인증서를 검증할 수 없다는 중간 대화 상자 경고가 표시될 수 있습니다.

이제 인증서 및 인터넷 옵션 대화 상자를 닫으면 됩니다.

## Procedure

**단계 1** Firepower Device Manager에서 인증서를 다운로드합니다.

- a) 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.
- b) **Devices(디바이스)** 탭을 클릭하여 디바이스를 찾거나 **Templates(템플릿)** 탭을 클릭하여 모델 디바이스를 찾습니다.
- c) **FTD** 탭을 클릭하고 인증서가 저장된 디바이스를 선택합니다.
- d) 오른쪽의 **Management(관리)** 창에서 **Policy(정책)**를 클릭합니다.
- e) 정책 표시줄에서 **SSL Decryption(SSL 암호 해독)**을 클릭합니다.
- f) SSL 암호 해독 정책 표시줄에서 SSL 암호 해독 구성 **Configuration NGFW-Default-InternalCA** 버튼을 클릭합니다.
- g) 다운로드  버튼을 클릭합니다.
- h) 다운로드 위치를 선택하고 선택적으로 파일 이름(확장자 제외)을 변경한 다음 **Save(저장)**를 클릭합니다.
- i) 이제 **SSL Decryption Settings(SSL 암호 해독 설정)** 대화 상자에서 취소 작업을 할 수 있습니다.

**단계 2** 클라이언트 시스템의 웹 브라우저에서 신뢰할 수 있는 루트 인증 기관 보관 영역에 인증서를 설치하거나 클라이언트가 직접 인증서를 설치할 수 있도록 합니다. 이 절차는 브라우저 및 운영 체제에 따라 다릅니다.

## Warning(경고)

## FDM-관리 디바이스를 통해 구성된 CA 인증서

Cisco Defense Orchestrator는 여러 디바이스를 관리할 수 있지만, 디바이스 구성 저장 시 저장되는 추가 정보가 제한되므로 내부 CA 인증서를 처리할 때 몇 가지 문제가 발생할 수 있습니다. CDO는 FDM 관리 콘솔을 통해 구성된 CA 인증서의 인증서 또는 키 정보를 저장하지 않습니다. FDM 관리에서 구성된 CA 인증서를 사용하여 보조 디바이스에 구축된 SSL 정책에 적용하려고 하면 CDO는 CA 인증서의 로컬 복사본을 생성하지만 키 정보는 복사하지 않으며, 복사할 수도 없습니다. 따라서 CDO 또는 보조 디바이스에 키 정보가 없으므로 CA 인증서를 성공적으로 구축할 수 없습니다. 이는 CA 인증서의 로컬 복사본에 대한 다운로드 링크를 사용할 수 없다는 의미이기도 합니다.

FDM 관리 디바이스를 통해 추가 디바이스에 대해 별도의 CA 인증서를 구성하거나 CDO UI를 통해 CA 인증서를 생성하는 것이 좋습니다.

## 규칙 집합

## 규칙 집합 정보

규칙 세트는 여러 FDM 관리 디바이스와 공유할 수 있는 액세스 제어 규칙 모음입니다. 규칙 집합의 규칙에 대한 모든 변경 사항은 이 규칙 집합을 사용하는 다른 매니지드 디바이스에 영향을 미칩니다. FDM 관리 디바이스에는 디바이스별(로컬) 및 공유(규칙 집합) 규칙이 있을 수 있습니다. FDM 관리 디바이스의 기존 규칙에서 규칙 집합을 생성할 수도 있습니다.



**Important** "규칙 세트" 기능은 현재 FDM 관리 디바이스 **단일 FTD 디바이스 업그레이드**에서 사용할 수 있습니다. 또한 규칙 집합은 Snort 3에 대해 활성화된 디바이스를 지원하지 않습니다.

다음과 같은 제한 사항이 적용됩니다.

- Snort 3 지원 디바이스에는 규칙 집합을 연결할 수 없습니다.
- Snort 3이 설치된 기존 디바이스에서는 규칙 집합을 생성할 수 없습니다.
- 사용자 지정 IPS 정책을 규칙 집합과 연결할 수 없습니다.

## 규칙 집합과 연결된 규칙 복사 또는 이동

규칙 집합 내에서 또는 다른 규칙 집합 간에 액세스 제어 규칙을 복사하거나 이동할 수 있습니다. 또한 로컬 및 규칙 집합 간에 규칙을 복사하거나 이동할 수 있습니다. 자세한 내용은 [FDM-관리 액세스 제어 규칙 복사](#) 및 [FDM-관리 액세스 제어 규칙 이동](#)을 참조하십시오.

## 기존 규칙 집합 자동 탐지

디바이스를 온보딩할 때 Cisco Defense Orchestrator는 디바이스의 기존 규칙 집합을 자동으로 탐지하여 디바이스의 규칙과 일치시키려고 시도합니다. 일치에 성공하면 CDO는 새로 온보딩된 디바이스

에 규칙 집합을 자동으로 연결합니다. 그러나 디바이스의 동일한 규칙 집합에 대해 여러 규칙 집합이 일치하는 경우, 그 중 어떤 것도 연결되지 않으며 수동으로 할당해야 합니다.

## 디바이스에 대한 규칙 집합 구성

아래 섹션을 사용하여 규칙 집합을 생성하고 구축합니다.

### Procedure

#### 단계 1 디바이스에 대한 규칙 집합 구성.

- 새 규칙 집합을 생성하고 규칙을 할당합니다.
- 규칙에 개체를 할당합니다.
- 규칙 집합의 우선순위를 설정합니다.
- 필요한 경우 규칙의 순서를 변경합니다.

#### 단계 2 디바이스에 대한 규칙 집합 구성.

- 규칙 집합에 여러 디바이스를 연결합니다.
- 규칙 집합을 검토하고 디바이스에 구축합니다.


## 규칙 집합 생성 또는 편집


규칙 집합을 생성하고 여기에 새 액세스 제어 규칙을 추가할 수 있습니다.

여러 FDM 관리 디바이스에 대한 규칙 집합을 생성하려면 다음 절차를 수행합니다.

### Procedure

단계 1 탐색창에서 **Policies(정책) > FTD Rulesets(FTD 규칙 집합)**를 클릭합니다.


단계 2 더하기  버튼을 클릭하여 새 규칙 집합을 생성합니다.

**Note** 기존 규칙 집합을 편집하려면 규칙 집합을 선택하고 편집  아이콘을 클릭합니다.

단계 3 규칙 집합의 이름을 입력하고 **Create(생성)**를 클릭합니다.

단계 4 액세스 제어 규칙을 생성하여 규칙 집합에 추가합니다. 지침은 [FDM 액세스 제어 정책 구성](#)을 참조하십시오.

**Note** 규칙 집합의 액세스 제어 규칙은 사용자 기준에 대한 기준을 지원하지 않습니다.

단계 5 창의 오른쪽 상단 모서리에서 규칙 집합의 우선순위()를 선택합니다. 디바이스가 규칙 집합에 연결되지 않은 경우 우선순위를 설정할 수 있습니다. 이 선택은 해당 규칙 집합에 포함된 모든 규칙과 디바이스에서 규칙이 처리되는 방식에 영향을 미칩니다.

- **Top(상위)** - 디바이스의 다른 모든 규칙보다 먼저 규칙 집합이 처리됩니다. 규칙은 규칙 목록의 맨 위에 정렬되며 먼저 처리됩니다. 다른 규칙 집합은 이 정책의 규칙보다 우선되지 않습니다. 디바이스당 상위 규칙 집합을 하나만 가질 수 있습니다.
- **Bottom(하위)** - 디바이스의 다른 모든 규칙 이후에 규칙 집합이 처리됩니다. 정책의 기본 작업 외에는 이 정책의 규칙을 이어받을 수 있는 규칙 집합이 없습니다. 디바이스당 하위 규칙 집합을 하나만 가질 수 있습니다. 기본적으로 우선순위는 **Bottom(하위)**으로 설정됩니다.

**Local Rules(로컬 규칙)**에는 디바이스의 모든 디바이스별 규칙이 표시됩니다.

**Note** 규칙 집합이 디바이스에 연결된 경우 우선순위를 변경할 수 없습니다. 디바이스를 분리하고 우선순위를 변경해야 합니다.

단계 6 **Save(저장)**를 클릭합니다. 규칙은 원하는 만큼 생성할 수 있습니다.

단계 7 (선택 사항) 생성한 규칙에 대해 해당 규칙을 선택하고 **Add Comments(코멘트 추가)** 필드에 코멘트를 추가할 수 있습니다. 규칙 코멘트에 대한 자세한 내용은 [정책 및 규칙 집합의 규칙에 코멘트 추가](#)를 참조하십시오.

- Note**
- 규칙 집합에 디바이스가 연결된 경우에도 규칙 집합에서 규칙의 순서를 변경할 수 있습니다. 규칙 집합의 우선순위를 변경하려면 다음 절차를 수행합니다.
    - a. 탐색창에서 **Policies(정책) > Rulesets(규칙 집합)**를 클릭하고 수정할 규칙 집합을 선택합니다.
    - b. 이동할 규칙을 선택합니다.
    - c. 규칙 행 내부에 커서를 놓고 **Move Up(위로 이동)(↑)** 또는 **Move Down(아래로 이동)(↓)** 화살표를 사용하여 규칙을 원하는 순서로 옮깁니다.
  - CDO를 사용하면 규칙 집합의 규칙과 연결된 **개체 재정의**할 수 있습니다. 규칙에 새 개체를 추가하는 경우, 규칙 집합에 디바이스를 연결하고 변경 사항을 저장한 후에 재정의할 수 있습니다.


## 여러 FDM-관리 디바이스 또는 템플릿에 규칙 집합 구축

규칙을 적용하려면 디바이스 또는 템플릿에 규칙 집합을 연결해야 합니다. 변경 사항을 검토한 후 디바이스에 구성을 구축할 수 있습니다. 새 FDM 관리 디바이스에 템플릿을 적용하면 템플릿에 포함된 규칙 집합이 디바이스에 푸시됩니다.

자세한 내용은 [FDM-관리 템플릿이 포함된 규칙 집합](#)을 참조하십시오.

시작하기 전에 다음 정보를 고려하십시오.

- 이미 Cisco Defense Orchestrator에 온보딩된 FDM 관리 디바이스에만 규칙 집합을 연결할 수 있습니다.
- 디바이스에는 하위 또는 상위 규칙 집합이 하나만 있을 수 있습니다.

- 규칙 집합에서 디바이스를 연결하거나 제거하면 변경 사항이 CDO에 준비되지만 구축되지 않으며, 디바이스가 CDO와 **Not Synced**(동기화되지 않음) 상태가 됩니다. 화면의 오른쪽 상단 모서리에 있는  아이콘을 클릭하여 디바이스에 변경 사항을 구축합니다.
- 디바이스를 연결한 후에 규칙 집합과 연결된 새 규칙이 디바이스와 연결된 기존 규칙을 덮어쓰지 않습니다.

다음 두 가지 방법으로 규칙 집합을 디바이스와 연결할 수 있습니다.

- Ruleset(규칙 집합) 페이지에서 규칙 집합에 디바이스를 추가합니다.
- Device Policy(디바이스 정책) 페이지에서 디바이스에 규칙 집합을 추가합니다.

## 규칙 집합 페이지에서 규칙 집합에 디바이스 추가

### Procedure

단계 1 탐색창에서 **Policies**(정책) > **FTD Rulesets**(FTD 규칙 집합)를 클릭합니다.

단계 2 FTD 디바이스에 할당할 규칙 집합을 선택하고 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

단계 3 오른쪽 상단 모서리에서 **Ruleset for**(다음에 대한 규칙 집합) 옆에 표시되는 **Device**(디바이스)

Ruleset for  버튼을 클릭합니다.

단계 4 적격 FTD 디바이스 목록에서 선택합니다.

단계 5 기어 아이콘에서 시스템이 규칙 집합의 규칙과 디바이스별 규칙 간에 중복된 이름을 확인하는 경우 수행할 작업을 다음 중 하나 선택합니다.

- **Fail on conflicting rules**(충돌 규칙 실패)(기본 옵션): CDO가 디바이스에 규칙 집합을 추가하지 않습니다. 수동으로 중복 규칙의 이름을 변경한 다음 규칙 집합을 추가해야 합니다.
- **Rename conflicting rules**(충돌하는 규칙 이름 변경): CDO는 디바이스에 있는 충돌하는 규칙의 이름을 바꿉니다(로컬 규칙).

단계 6 **Save**(저장)를 클릭합니다. **Attached Ruleset to Devices**(디바이스에 연결된 규칙 집합) 마법사가 닫힙니다.

단계 7 오른쪽 상단 모서리에 있는 **Save**(저장)를 클릭하여 규칙 집합의 변경 사항을 저장합니다. 규칙 집합을 저장하면 CDO에 대한 변경 사항이 준비됩니다.

**Note** 규칙 집합을 수정할 때마다 **Save**(저장)를 클릭해야 합니다. 이 작업을 수행하면 모든 변경 사항이 CDO에 준비됩니다. 변경 사항을 수동으로 구축해야 합니다.


단계 8 **OK**(확인)를 클릭합니다. 규칙 집합을 저장하면 CDO에 대한 변경 사항이 준비됩니다.

단계 9 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다. 디바이스에서 준비된 규칙 집합 변경 사항을 **변경 사항 취소**하는 경우 자세한 내용은 **준비된 규칙 집합 변경 취소의 영향**을 참조하십시오.



## 디바이스 정책 페이지에서 디바이스에 규칙 집합 추가

**Procedure**

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 목록에서 원하는 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다.
- 단계 5 창의 오른쪽 상단 모서리에 있는  버튼을 클릭합니다.
- 단계 6 원하는 규칙 집합을 선택합니다.
- 단계 7 기어 아이콘에서 시스템이 규칙 집합의 규칙과 디바이스별 규칙 간에 중복된 이름을 확인하는 경우 수행할 작업을 다음 중 하나 선택합니다.

- **Fail on conflicting rules**(충돌 규칙 실패)(기본 옵션): CDO가 디바이스에 규칙 집합을 추가하지 않습니다. 수동으로 중복 규칙의 이름을 변경한 다음 규칙 집합을 추가해야 합니다.
- **Rename conflicting rules**(충돌하는 규칙 이름 변경): CDO는 디바이스에 있는 충돌하는 규칙의 이름을 바꿉니다(로컬 규칙).

**Note**       선택한 디바이스에 충돌하는 규칙이 없는 경우 CDO는 변경 없이 규칙 집합을 디바이스에 연결합니다.

- 단계 8 **Attach Ruleset**(규칙 집합 연결)를 클릭합니다. 규칙 집합은 규칙 집합의 우선순위에 따라 디바이스에 추가됩니다.
- 단계 9 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다. 디바이스에서 준비된 규칙 집합 변경 사항을 **변경 사항 취소**하는 경우 자세한 내용은 **준비된 규칙 집합 변경 취소의 영향**을 참조하십시오.

**관련 정보:**

- [규칙 집합](#)
- [FDM-관리 템플릿이 포함된 규칙 집합](#)
- [선택한 규칙 집합에서 FTD 디바이스 분리](#)
- [규칙 및 규칙 집합 삭제](#)
- [OOB\(Out of Band\) 변경이 규칙 집합에 미치는 영향](#)
- [규칙 및 규칙 집합 보기](#)
- [규칙 집합 생성 후 로그 항목 변경](#)
- [기존 디바이스 규칙에서 규칙 집합 생성](#)

## FDM-관리 템플릿이 포함된 규칙 집합

Cisco Defense Orchestrator를 사용하면 FDM 관리 템플릿에 규칙 집합을 할당할 수 있습니다.

- 규칙 집합이 있는 FDM 관리 디바이스에서 템플릿을 생성하면 CDO는 소스 디바이스에 있던 규칙 집합에 템플릿을 자동으로 추가합니다. 규칙 집합에서 템플릿을 관리할 수 있습니다.
- 대상 FDM 관리 디바이스에 규칙 집합이 포함된 템플릿을 적용하면 CDO는 대상 디바이스를 규칙 집합에 자동으로 추가하므로 규칙 집합에서 대상 디바이스를 관리하게 됩니다.
- 이미 다른 규칙 집합이 있는 대상 FDM 관리 디바이스에 규칙 집합이 포함된 템플릿이 적용되면 CDO는 대상 디바이스에서 기존 규칙 집합을 제거하고 템플릿과 연결된 새 규칙 집합을 추가합니다.

자세한 내용은 [여러 FDM-관리 디바이스 또는 템플릿에 규칙 집합 구축](#)을 참조하십시오.

관련 정보:

- [규칙 집합](#)
- [디바이스에 대한 규칙 집합 구성](#)
- [기존 디바이스 규칙에서 규칙 집합 생성](#)
- [OOB\(Out of Band\) 변경이 규칙 집합에 미치는 영향](#)
- [규칙 및 규칙 집합 보기](#)
- [규칙 집합 생성 후 로그 항목 변경](#)
- [선택한 규칙 집합에서 FTD 디바이스 분리](#)
- [규칙 및 규칙 집합 삭제](#)

## 기존 디바이스 규칙에서 규칙 집합 생성

FDM 관리 디바이스에서 기존 규칙을 선택하여 규칙 집합을 생성할 수 있습니다.

기존 디바이스 규칙에서 규칙 집합을 생성하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 목록에서 원하는 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다. 디바이스의 기존 규칙이 나타납니다.
- 단계 5 요구 사항에 따라 다음을 수행합니다.
  - a) **Top**(상위) 규칙을 생성하려면 맨 위에 있는 첫 번째 규칙부터 연속된 규칙을 선택합니다.

b) **Bottom**(하위) 규칙을 생성하려면 맨 아래에 마지막 규칙을 포함하는 연속된 규칙을 선택합니다.

단계 6 오른쪽의 **Actions**(작업) 창에서 **Create Ruleset**(규칙 집합 생성)를 클릭합니다.

**Note**        선택 항목에 첫 번째 또는 마지막 규칙이 포함되어야 **Create Ruleset**(규칙 집합 생성) 링크를 클릭할 수 있습니다.

단계 7 **Ruleset Name**(규칙 집합 이름) 필드에 이름을 지정하고 **Create**(생성)를 클릭합니다. 해당 규칙 집합이 디바이스에서 생성됩니다.

디바이스의 나머지 규칙을 사용하여 규칙 집합을 계속 생성할 수 있습니다.

## OOB(Out of Band) 변경이 규칙 집합에 미치는 영향

FDM 관리 디바이스 사용하여 새 규칙을 추가하거나 기존 규칙을 변경하고 FDM 관리에 대해 Cisco Defense Orchestrator에서 Conflict Detection(충돌 탐지)을 활성화한 경우, CDO는 OOB(Out of Band) 변경 사항을 탐지하고 디바이스의 구성 상태가 **Conflict Detected**(충돌 탐지됨)로 표시됩니다. [구성 충돌 해결](#).

디바이스 변경 사항을 수락하면 CDO는 마지막으로 알려진 구성을 디바이스에 적용된 새 변경 사항으로 덮어씁니다. 다음 변경 사항이 적용됩니다.

- 변경 사항의 영향을 받는 규칙 집합은 디바이스와의 관계를 잃게 됩니다.
- 이러한 규칙 집합과 연결된 규칙은 로컬 규칙으로 변환됩니다.

디바이스 변경 사항을 거부하면 CDO는 새 변경 사항을 거부하고 디바이스의 구성을 CDO에서 마지막으로 동기화된 구성으로 교체합니다.

관련 정보:

- [규칙 집합](#)
- [디바이스에 대한 규칙 집합 구성](#)
- [기존 디바이스 규칙에서 규칙 집합 생성](#)
- [준비된 규칙 집합 변경 취소의 영향](#)
- [규칙 및 규칙 집합 보기](#)
- [규칙 집합 생성 후 로그 항목 변경](#)
- [선택한 규칙 집합에서 FTD 디바이스 분리](#)
- [규칙 및 규칙 집합 삭제](#)

## 준비된 규칙 집합 변경 취소의 영향

CDO를 사용하여 규칙 집합에 새 규칙을 추가하거나 규칙 집합과 연결된 기존 규칙을 변경하는 경우, CDO는 변경 사항을 구성 파일의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 "구축"될 때까지 CDO에서 "보류 중"인 것으로 간주됩니다.

디바이스에서 보류 중인 규칙 집합 변경 사항을 **변경 사항 취소**하면 CDO는 디바이스 구성의 로컬 복사본을 디바이스에 저장된 구성으로 완전히 덮어씁니다.

규칙 집합 및 관련 디바이스에서 다음 변경 사항이 발생합니다.

- 변경 사항의 영향을 받는 규칙 집합은 디바이스와의 관계를 잃게 됩니다.
- 이러한 규칙 집합과 연결된 규칙은 로컬 규칙으로 변환됩니다.
- CDO는 새로 준비된 변경 사항을 무시하고 디바이스에 있는 구성을 유지합니다.

관련 정보:

- [규칙 집합](#)
- [디바이스에 대한 규칙 집합 구성](#)
- [기존 디바이스 규칙에서 규칙 집합 생성](#)
- [OOB\(Out of Band\) 변경이 규칙 집합에 미치는 영향](#)
- [규칙 및 규칙 집합 보기](#)
- [규칙 집합 생성 후 로그 항목 변경](#)
- [선택한 규칙 집합에서 FTD 디바이스 분리](#)
- [규칙 및 규칙 집합 삭제](#)

## 규칙 및 규칙 집합 보기

디바이스 정책 페이지에서 규칙 보기

FDM 관리 디바이스 정책 페이지에 개별(로컬) 및 공유 규칙(규칙 집합과 연결됨)이 표시됩니다.

정책 페이지에서 FDM 관리 디바이스 규칙 집합을 보려면 다음 절차를 수행합니다.

### Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.


단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 **FTD** 탭을 클릭하고 원하는 디바이스를 선택합니다.

단계 4 오른쪽의 **Management**(관리) 창에서 **Policy**(정책)를 클릭합니다. 지정한 구성에 따라 다음 규칙이 표시됩니다.

- **Top Rules**(상위 규칙): 디바이스에서 다른 모든 규칙보다 먼저 처리되는 필수 공유 규칙을 표시합니다.
- **Local Rules**(로컬 규칙): 디바이스에서 필수 규칙 이후에 처리될 디바이스별 규칙을 표시합니다.
- **Bottom**(하위): 디바이스에서 다른 모든 규칙 다음에 처리될 기본 공유 규칙을 표시합니다.

**Note** 해당 규칙 집합 페이지로 이동하여 규칙 집합을 편집할 수 있습니다.

- 규칙 집합 헤더의 오른쪽 상단 모서리에서 **Go to Ruleset**(규칙 집합으로 이동) 를 클릭합니다.
- 규칙 내용을 필요한 만큼 변경하고 **Save**(저장)를 클릭합니다. 새 변경 사항은 규칙 집합과 연결된 모든 디바이스에서 업데이트됩니다.

## 규칙 집합 보기

**Rulesets**(규칙 집합) 페이지에는 테넌트에서 사용 가능한 모든 규칙 집합이 표시됩니다. 또한 규칙 집합과 연결된 디바이스에 대한 정보도 제공합니다.

Rulesets(규칙 집합) 페이지에서 모든 규칙 집합을 보려면 다음 절차를 수행합니다.

### Procedure

- 단계 1** Navigation(탐색) 창에서 **Policies**(정책) > **Rulesets**(규칙 집합)를 클릭합니다. 테넌트에서 사용 가능한 규칙이 표시됩니다.
- 단계 2** 규칙 집합을 클릭하면 해당 세부 정보가 표시됩니다. **Devices**(디바이스) 열에는 각 규칙 집합에 연결된 FTD 디바이스의 수가 표시됩니다.
- 단계 3** **Management**(관리) 창에서 **Workflows**(워크플로우)를 클릭합니다. 이 페이지에는 디바이스에서 수행한 모든 작업이 표시됩니다. **Diagram**(다이어그램)을 클릭하여 그림으로 표현한 워크플로우를 볼 수 있습니다.

## 규칙 집합 검색

**Filter by Device**(디바이스별 필터링) 필터를 사용하여 할당된 규칙 집합을 볼 디바이스를 선택할 수 있습니다.

### Procedure

- 단계 1** 탐색창에서 **Policies**(정책) > **Rulesets**(규칙 집합)를 클릭합니다.
- 단계 2** 필터 아이콘을 클릭하고 **Filter by Device**(디바이스별 필터링)를 클릭합니다.
- 단계 3** 목록에서 하나 이상의 디바이스를 선택하고 **OK**(확인)를 클릭합니다.

선택한 디바이스를 기반으로 규칙 집합을 볼 수 있습니다.

### 규칙 집합과 연결된 작업 보기

**Jobs**(작업) 페이지는 FTD 디바이스에 규칙 집합을 적용하거나 FTD 디바이스에서 제거할 때의 작업을 기록합니다. 또한 작업의 성공 또는 실패 여부도 확인합니다.

#### Procedure

단계 1 Navigation(탐색) 창에서 **Policies**(정책) > **Rulesets**(규칙 집합)를 클릭합니다.

단계 2 규칙 집합을 클릭하면 해당 세부 정보가 표시됩니다.

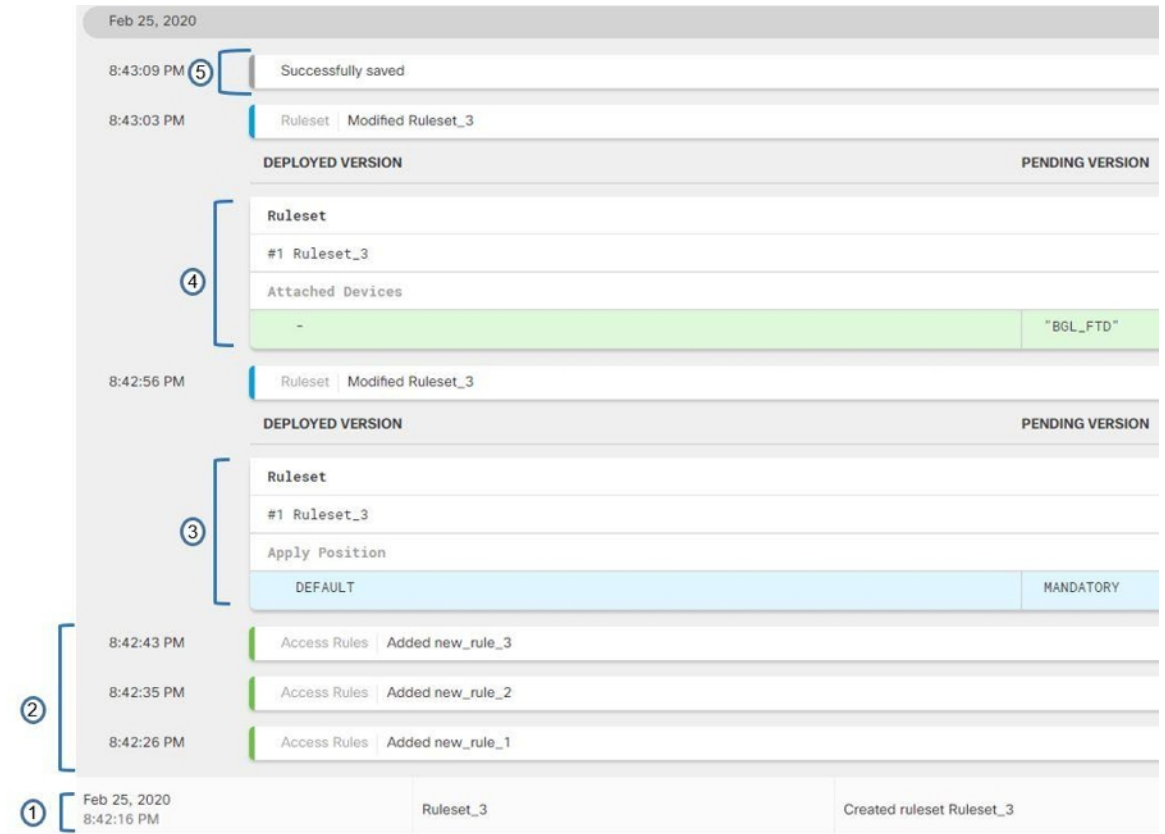
단계 3 **Management**(관리) 창에서 **Jobs**(작업)를 클릭합니다. 이 페이지에는 규칙 집합에서 수행한 작업이 표시됩니다.

### 규칙 집합 생성 후 로그 항목 변경

CDO는 규칙 집합에서 변경 사항을 탐지하면 규칙 집합에서 수행되는 모든 작업에 대한 변경 로그 항목을 생성합니다.

변경 로그 항목 행에서 파란색 [변경 로그 차이 보기](#) 링크를 클릭하면 실행 중인 구성 파일의 컨텍스트에서 변경 내용을 나란히 비교하여 표시합니다.

다음 예에서 변경 로그는 규칙 집합에 세 개의 규칙이 추가된 새 규칙 집합에 대한 항목을 보여줍니다. 또한 규칙 집합의 우선순위 및 규칙 집합에 연결된 FTD 디바이스 설정에 대한 정보도 표시합니다.



그림의 번호	설명
1	새 규칙 집합 "Ruleset_3"은 2020년 2월 25일 오전 11:03:18에 생성됩니다.
2	새 액세스 규칙 "new_rule_1", "new_rule_3" 및 "new_rule_3"이 규칙 집합에서 생성됩니다.
3	규칙 집합의 우선순위는 "Mandatory(필수)"로 설정됩니다.
4	규칙 집합이 "BGL_FTD" 디바이스에 연결됩니다.
5	규칙 집합 변경 사항이 저장됩니다.

## 선택한 규칙 집합에서 FTD 디바이스 분리

규칙 집합에서 디바이스를 분리하려면 다음 절차를 수행합니다.

### Procedure

단계 1 탐색창에서 **Policies(정책)** > **Rulesets(규칙 집합)**를 클릭합니다.

- 단계 2 편집할 규칙 집합을 선택하고 **Actions**(작업) 창에서 **Edit**(편집) 링크를 클릭합니다.
- 단계 3 오른쪽 상단 모서리에서 **Ruleset for**(다음에 대한 규칙 집합) 옆에 표시되는 **Device**(디바이스) 버튼을 클릭합니다.
- 단계 4 현재 규칙 집합에 연결된 디바이스의 선택을 취소하거나 **Clear**(지우기)를 클릭하여 모든 디바이스를 한 번에 제거합니다.
- 단계 5 **Save**(저장)를 클릭합니다.
- 단계 6 오른쪽 상단 창에서 **Save**(저장)를 클릭하여 규칙 집합을 저장합니다. 정책을 저장하면 CDO에 대한 변경 사항이 준비됩니다.
- 단계 7 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

---

관련 정보:

- [규칙 집합](#)
- [디바이스에 대한 규칙 집합 구성](#)
- [기존 디바이스 규칙에서 규칙 집합 생성](#)
- [OOB\(Out of Band\) 변경이 규칙 집합에 미치는 영향](#)
- [규칙 및 규칙 집합 보기](#)
- [규칙 집합 생성 후 로그 항목 변경](#)
- [규칙 및 규칙 집합 삭제](#)

## 규칙 및 규칙 집합 삭제

### 규칙 집합에서 규칙 삭제

규칙 집합에서 더 이상 필요하지 않은 규칙을 삭제할 수 있습니다.  
규칙을 삭제하려면 다음 절차를 수행합니다.

#### Procedure

---

- 단계 1 탐색창에서 **Policies**(정책) > **Rulesets**(규칙 집합)를 클릭하고 규칙 집합을 선택합니다.
- 단계 2 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.
- 단계 3 삭제할 규칙을 선택하고 **Actions**(작업) 아래에서 **Remove**(제거)를 클릭합니다.
- 단계 4 **OK**(확인)를 클릭하여 삭제를 확인합니다.
- 단계 5 오른쪽 상단 모서리에 있는 **Save**(저장)를 클릭하여 규칙 집합의 변경 사항을 저장합니다. 규칙 집합을 저장하면 CDO에 대한 변경 사항이 준비됩니다.



단계 6 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 여러 번 변경한 후 한 번에 구축할 수 있습니다.

## 규칙 집합 삭제

연결된 모든 디바이스를 분리한 후에만 규칙 집합을 삭제할 수 있습니다. [규칙 및 규칙 집합 삭제](#)  
규칙 집합을 삭제하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 탐색창에서 **Policies**(정책) > **Rulesets**(규칙 집합)를 클릭하고 삭제할 규칙 집합을 선택합니다.
- 단계 2 규칙 집합 행 내부에서 **Remove**(제거)를 클릭합니다.
- 단계 3 규칙 집합을 영구적으로 삭제하려면 **Confirm**(확인)을 클릭합니다.
- 단계 4 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 여러 번 변경한 후 한 번에 구축할 수 있습니다.

- [규칙 집합](#)
- [디바이스에 대한 규칙 집합 구성](#)
- [선택한 규칙 집합에서 FTD 디바이스 분리](#)

## 선택한 FTD 디바이스에서 규칙 집합 제거

선택한 FTD 디바이스에서 규칙 집합을 제거하는 두 가지 방법이 있습니다. 각 방법의 동작은 약간 다릅니다.

- **선택한 FDM-관리 디바이스에서 규칙 집합 삭제:** 이 기능은 선택한 FTD 디바이스에서 규칙 집합 및 관련 공유 규칙을 삭제합니다.
- **선택한 FDM-관리 디바이스에서 규칙 집합 연결 해제:** 이 기능은 공유 규칙을 제거하지 않습니다. 대신 공유 규칙을 로컬 규칙으로 변환합니다.

## 선택한 FDM-관리 디바이스에서 규칙 집합 삭제

선택한 FDM 관리 디바이스에서 규칙 집합 및 관련 공유 규칙을 삭제할 수 있습니다. 해당 규칙 집합 페이지의 [선택한 규칙 집합에서 FTD 디바이스 분리](#)할 수도 있습니다.

### Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 FTD 탭을 클릭하고 목록에서 원하는 디바이스를 선택합니다.

단계 4 규칙 집합의 오른쪽 상단 모서리에 나타나는 삭제 아이콘을 클릭합니다.

단계 5 OK(확인)를 클릭합니다.

단계 6 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

## 선택한 FDM-관리 디바이스에서 규칙 집합 연결 해제

FDM 관리 디바이스의 규칙 집합에 새 디바이스별 규칙을 추가하려면 해당 규칙 집합을 FDM 관리 디바이스에서 분리해야 합니다. 그러면 연결된 공유 규칙이 로컬 규칙으로 변환됩니다. 그런 다음 원하는 규칙을 로컬 규칙에 추가할 수 있습니다.


### Procedure

단계 1 탐색창에서 Inventory(재고 목록)를 클릭합니다.

단계 2 Devices(디바이스) 탭을 클릭하여 디바이스를 찾거나 Templates(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 FTD 탭을 클릭하고 목록에서 원하는 디바이스를 선택합니다.

단계 4 오른쪽의 Management(관리) 창에서 Policy(정책)를 클릭합니다.

단계 5 규칙 집합의 오른쪽 상단 모서리에 나타나는  아이콘을 클릭합니다.

단계 6 OK(확인)를 클릭합니다.

단계 7 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

## 정책 및 규칙 집합의 규칙에 코멘트 추가

FDM 관리 디바이스 정책의 규칙 및 규칙 집합의 규칙에 설명을 추가하여 규칙의 일부 특성을 문서화할 수 있습니다. 규칙 설명은 Cisco Defense Orchestrator에서만 볼 수 있습니다. FDM 관리 디바이스에 기록되지 않으며 FDM에서도 볼 수 없습니다.

코멘트는 규칙이 생성되어 CDO에 저장된 후 규칙에 추가됩니다. 규칙 코멘트는 CDO의 기능일 뿐이므로, 규칙 코멘트를 생성, 변경 또는 삭제해도 CDO에서 디바이스의 구성 상태는 "Not Synced(동기화되지 않음)"로 변경되지 않습니다. 규칙 설명을 저장하기 위해 CDO에서 FDM 관리 디바이스로 변경 사항을 쓸 필요가 없습니다.

디바이스 정책의 규칙과 관련된 설명은 디바이스의 FDM 관리 정책 페이지에서 보고 편집할 수 있습니다. FDM 관리 디바이스 규칙 세트의 규칙과 연결된 설명은 규칙 세트 페이지에서 보고 편집할 수 있습니다. 정책에서 규칙 집합을 사용하는 경우, 규칙 집합의 규칙과 관련된 코멘트가 정책의 코멘트 영역에 표시됩니다. 코멘트는 읽기 전용입니다.

정책, 규칙 집합 또는 변경 로그에서 문자열을 검색하면 CDO는 규칙의 다른 속성 및 값과 함께 해당 문자열에 대한 규칙과 관련된 코멘트를 검색합니다.

규칙에 대한 코멘트를 추가하거나 편집하면 해당 작업이 변경 로그에 기록됩니다. 규칙 코멘트는 CDO에서만 기록되고 유지 관리되므로 변경 로그에서 (CDO 전용 변경) 레이블이 지정됩니다.

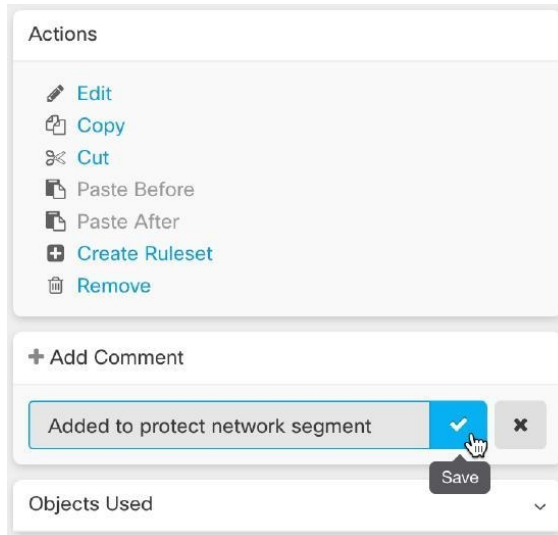


**Caution** FDM 관리 디바이스의 구성에 대역 외 변경 사항이 있고 CDO가 해당 구성을 데이터베이스로 읽어들이는 경우, 규칙과 관련된 코멘트는 지워집니다.

## 규칙에 코멘트 추가

### Procedure

- 단계 1 코멘트를 달고자 하는 규칙이 포함된 정책 또는 규칙 집합을 엽니다.
- 단계 2 규칙을 선택합니다.
- 단계 3 규칙에 대한 Add Comment(코멘트 추가) 영역에서 **Add Comment(코멘트 추가)**를 클릭합니다.
- 단계 4 텍스트 상자에 코멘트를 추가합니다.
- 단계 5 **Save(저장)**를 클릭합니다.




## 정책 및 규칙 집합의 규칙에 대한 코멘트 편집

### 정책의 규칙에 대한 코멘트 편집

이 절차를 사용하여 FDM 관리 디바이스 정책의 규칙에 대한 코멘트를 편집합니다.


## Procedure

- 단계 1 CDO 메뉴 모음에서 **Policies(정책) > FTD/Meraki/AWS Policies(FTD/Meraki/AWS 정책)**를 선택합니다.
- 단계 2 코멘트를 추가할 로컬 규칙이 있는 FDM 관리 디바이스 정책을 선택합니다. 정책 내 규칙 집합의 규칙에 코멘트를 추가할 수 없습니다.
- 단계 3 Comment(코멘트) 창에서 편집 아이콘()을 클릭합니다.
- 단계 4 코멘트를 편집하고 Save(저장)를 클릭합니다. 코멘트 변경 사항이 Comment(코멘트) 영역에 즉시 반영된 것을 확인할 수 있습니다.

## 규칙 집합의 규칙에 대한 코멘트 편집

정책 페이지에 반영된 규칙 집합의 규칙에 대한 코멘트 변경 사항을 보려면 코멘트 및 규칙을 특정 순서로 변경해야 합니다.

## Procedure

- 단계 1 CDO 탐색 패널에서 **Policies(정책) > FTD Rulesets(FTD 규칙 집합)**를 선택합니다.
- 단계 2 코멘트를 추가할 규칙이 있는 규칙 집합을 선택합니다.
- 단계 3 Actions(작업) 창에서 **Edit(편집)**를 클릭합니다.
- 단계 4 규칙을 선택합니다.
- 단계 5 Comment(코멘트) 창에서 편집 아이콘()을 클릭합니다.
- 단계 6 코멘트를 편집하고 Save(저장)를 클릭합니다. 코멘트 변경 사항이 규칙 집합 페이지의 Comment(코멘트) 영역에 즉시 반영된 것을 확인할 수 있습니다.
- 단계 7 변경할 규칙을 선택하고 Actions(작업) 창에서 **Edit(편집)**를 클릭합니다.
- 단계 8 규칙을 편집하고 파란색 확인 버튼을 클릭하여 변경 사항을 저장합니다.
- 단계 9 규칙 집합 페이지 상단에서 **Save(저장)**를 클릭하여 규칙 집합을 저장합니다. 이제 규칙 집합의 규칙에 대한 새 코멘트가 정책 페이지에 반영됩니다.
- 단계 10 정책 페이지에서 코멘트 변경 사항을 확인하려면 다음을 수행합니다.
  - a) CDO 메뉴 모음에서 **Policies(정책) > FTD/Meraki/AWS Policies(FTD/Meraki/AWS 정책)**를 선택합니다.
  - b) 방금 편집한 규칙 집합을 포함하는 FDM 관리 디바이스 정책을 선택합니다.
  - c) 방금 편집한 코멘트가 있는 규칙을 선택합니다. Comment(코멘트) 창에 새 코멘트가 표시되어야 합니다.

## 네트워크 주소 변환

IP 네트워크 내의 각 컴퓨터와 디바이스에는 호스트를 식별하는 고유한 IP 주소가 할당됩니다. 공용 IPv4 주소의 부족 때문에 이러한 IP 주소는 대부분 사설이며, 사설 회사 네트워크 외부로 라우팅되지 않습니다. RFC 1918의 정의에 따르면 사설 IP 주소는 내부적으로 사용할 수 있지만 외부에 알려서는 안 되는 주소입니다.

- 10.0.0.0~10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0~192.168.255.255

NAT의 주요 기능 중 하나는 사설 IP 네트워크가 인터넷에 연결되도록 하는 것입니다. NAT는 사설 IP 주소를 공용 IP 주소로 교체하여, 내부 사설 네트워크의 사설 주소를 공용 인터넷에서 사용할 수 있는 합법적이고 라우팅 가능한 주소로 전환합니다. 이렇게 하여 NAT는 공용 주소를 절약합니다. 전체 네트워크에 대해 최소 하나의 공용 주소만 외부에 알리도록 구성할 수 있기 때문입니다.

NAT의 기타 기능은 다음과 같습니다.

- 보안 - 직접 공격을 피할 수 있도록 내부 IP 주소를 숨깁니다.
- IP 라우팅 솔루션 - NAT를 사용하는 경우 중첩 IP 주소 문제가 발생하지 않습니다.
- 유연성 - 외부적으로 사용 가능한 공용 주소에 영향을 주지 않고 내부 IP 주소 지정 방식을 변경할 수 있습니다. 예를 들어 인터넷에 액세스할 수 있는 서버의 경우, 인터넷용으로는 고정 IP 주소를 유지하고 내부적으로는 서버 주소를 변경할 수 있습니다.
- IPv4와 IPv6 간 변환(라우팅된 방식 전용) - IPv6 네트워크를 IPv4 네트워크에 연결하려는 경우 NAT를 이용하면 두 가지 주소 유형 간에 변환할 수 있습니다.

Cisco Defense Orchestrator를 사용하여 다양한 활용 사례에 대한 NAT 규칙을 생성할 수 있습니다. NAT 규칙 마법사 또는 다음 항목을 사용하여 다른 NAT 규칙을 생성합니다.

## NAT 규칙 처리 순서

네트워크 개체 NAT 규칙과 2회 NAT 규칙은 세 개의 섹션으로 구분되는 단일 테이블에 저장됩니다. 섹션 1 규칙이 먼저 적용된 다음, 일치가 발견될 때까지 섹션 2, 마지막으로 섹션 3이 적용됩니다. 예를 들어 섹션 1에서 일치 발견되면 섹션 2와 3은 평가되지 않습니다. 다음 표는 각 섹션 내의 규칙 순서를 보여줍니다.

Table 16: NAT 규칙 테이블

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 1	2회 NAT(ASA) 수동 NAT(FTD)	첫 번째 일치부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 첫 번째 일치가 적용되므로, 일반 규칙 앞에 특수 규칙이 오도록 해야 합니다. 그렇지 않으면 특수 규칙이 원하는 대로 적용되지 않을 수 있습니다. 기본적으로 2회 NAT 규칙은 섹션 1에 추가됩니다.
섹션 2	네트워크 개체 NAT(ASA) 자동 NAT(FTD)	<p>섹션 1에서 일치하는 항목을 찾을 수 없으면 섹션 2 규칙이 다음 순서로 적용됩니다.</p> <ol style="list-style-type: none"> <li>고정 규칙</li> <li>동적 규칙</li> </ol> <p>각 규칙 유형 내에서는 다음의 순서 지침이 사용됩니다.</p> <ol style="list-style-type: none"> <li>실제 IP 주소의 수량 - 가장 적은 것에서 가장 많은 것. 예를 들면 주소가 1개인 개체가 주소가 10개인 개체보다 먼저 평가됩니다.</li> <li>수량이 동일한 경우 IP 주소 번호가 낮은 것에서 높은 것 순으로 사용됩니다. 예를 들면, 10.1.1.0이 11.1.1.0보다 먼저 평가됩니다.</li> <li>IP 주소가 동일한 경우 네트워크 개체의 이름이 알파벳순으로 사용됩니다. 예를 들어 "Arlington" 개체는 "Detroit" 개체보다 먼저 평가됩니다.</li> </ol>
섹션 3	2회 NAT(ASA) 수동 NAT(FTD)	아직도 일치가 발견되지 않으면 섹션 3 규칙이 첫 번째부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 이 섹션에는 가장 일반적인 규칙을 포함해야 합니다. 또한 이 섹션에서는 특정 규칙이 일반 규칙보다 먼저 적용되도록 해야 합니다.

예를 들어 섹션 2 규칙의 경우 네트워크 개체 내에서 다음 IP 주소를 정의합니다.

- 192.168.1.0/24(고정)
- 192.168.1.0/24(동적)
- 10.1.1.0/24(고정)
- 192.168.1.1/32(고정)

- 172.16.1.0/24(동적)(개체 Detroit)
- 172.16.1.0/24(동적)(개체 Arlington)

결과 순서는 다음과 같습니다.

- 192.168.1.1/32(고정)
- 10.1.1.0/24(고정)
- 192.168.1.0/24(고정)
- 172.16.1.0/24(동적)(개체 Arlington)
- 172.16.1.0/24(동적)(개체 Detroit)
- 192.168.1.0/24(동적)

## 네트워크 주소 변환 마법사

NAT(Network Address Translation) 마법사는 다음 유형의 액세스에 대해 디바이스에서 NAT 규칙을 만드는 데 도움이 됩니다.

- 내부 사용자의 인터넷 액세스를 활성화합니다. 이 NAT 규칙을 사용하여 내부 네트워크의 사용자가 인터넷에 연결할 수 있습니다.
- 내부 서버를 인터넷에 노출합니다. 이 NAT 규칙을 사용하여 네트워크 외부의 사람들이 내부 웹 또는 이메일 서버에 도달하도록 허용할 수 있습니다.

"내부 사용자를 위한 인터넷 액세스 활성화"의 전제 조건

NAT 규칙을 생성하기 전에 다음 정보를 수집하십시오.

- 사용자에게 가장 가까운 인터페이스 이것은 일반적으로 "내부" 인터페이스라고 합니다.
- 인터넷 연결에 가장 가까운 인터페이스 이것은 일반적으로 "외부" 인터페이스라고 합니다.
- 특정 사용자만 인터넷에 연결할 수 있도록 하려면 해당 사용자의 서브넷 주소가 필요합니다.

"내부 서버를 인터넷에 노출"하기 위한 전제 조건

NAT 규칙을 생성하기 전에 다음 정보를 수집하십시오.

- 사용자에게 가장 가까운 인터페이스 이것은 일반적으로 "내부" 인터페이스라고 합니다.
- 인터넷 연결에 가장 가까운 인터페이스 이것은 일반적으로 "외부" 인터페이스라고 합니다.
- 인터넷 연결 IP 주소로 변환하려는 네트워크 내부 서버의 IP 주소입니다.
- 서버에서 사용할 공용 IP 주소입니다.

다음 작업

NAT 마법사를 사용하여 NAT 규칙 생성, on page 450의 내용을 참조하십시오.

## NAT 마법사를 사용하여 NAT 규칙 생성

### Before you begin

NAT 마법사를 사용하여 NAT 규칙을 만드는 데 필요한 사전 요구 사항은 [네트워크 주소 변환 마법사, on page 449](#)를 참조하십시오.

### Procedure

단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 **필터** 및 **검색** 필드를 사용하여 NAT 규칙을 생성하려는 디바이스를 찾으십시오.

단계 5 상세정보 패널의 **Management**(관리) 영역에서 **NAT** > **NAT**를 클릭합니다.

단계 6  > **NAT Wizard**(NAT 마법사)를 클릭합니다.

단계 7 NAT 마법사 질문에 응답하고 화면의 지시를 따르십시오.

- NAT 마법사는 [네트워크 개체, on page 130](#)를 사용하여 규칙을 생성합니다. 드롭다운 메뉴에서 기존 개체를 선택하거나 만들기 버튼 **+ Create...** 를 사용하여 새 개체를 생성합니다.
- NAT 규칙을 저장하려면 먼저 모든 IP 주소를 네트워크 개체로 정의해야 합니다.

단계 8 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#)하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## NAT의 일반적인 사용 사례

### 2회 NAT 및 수동 NAT

다음은 "자동 NAT"라고도 하는 "네트워크 개체 NAT"를 사용하여 수행할 수 있는 몇 가지 일반적인 작업입니다.

- [공용 IP 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화, 451 페이지](#)
- [내부 네트워크의 사용자가 외부 인터페이스의 공용 IP 주소를 사용하여 인터넷에 액세스하도록 활성화, 452 페이지](#)
- [공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정, 453 페이지](#)



- [사설 IP 주소 범위를 공용 IP 주소 범위로 변환, 456 페이지](#)

### 네트워크 개체 및 NAT 자동 NAT

다음은 "수동 NAT"라고도 하는 "Twice NAT"를 사용하여 수행할 수 있는 일반적인 작업입니다.

- [외부 인터페이스를 통과할 때 IP 주소 범위가 변환되지 않도록 방지, 458 페이지](#)

## 공용 IP 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화

### 활용 사례

인터넷에서 액세스해야 하는 사설 IP 주소가 있는 서버가 있고 사설 IP 주소에 대해 하나의 공용 IP 주소를 NAT하기에 충분한 공용 IP 주소가 있는 경우 이 NAT 전략을 사용합니다. 공용 IP 주소가 제한된 경우 [공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정](#)을 참조하세요 (해당 솔루션이 더 적합할 수 있음).


### 전략

서버에는 정적 사설 IP 주소가 있으며 네트워크 외부의 사용자는 서버에 연결할 수 있어야 합니다. 고정 사설 IP 주소를 고정 공용 IP 주소로 변환하는 네트워크 개체 NAT 규칙을 생성합니다. 그런 다음 해당 공용 IP 주소에서 사설 IP 주소에 도달하는 트래픽을 허용하는 액세스 정책을 생성합니다. 마지막으로 이러한 변경 사항을 디바이스에 배포합니다.

### Before you begin

시작하기 전에 두 개의 네트워크 개체를 생성합니다. 하나의 개체는 *servername\_inside*로 이름을 지정하고 다른 개체는 *servername\_outside*로 이름을 지정합니다. *servername\_inside* 네트워크 개체는 서버의 사설 IP 주소를 포함해야 합니다. *servername\_outside* 네트워크 개체에는 서버의 공용 IP 주소가 포함되어야 합니다. 지침은 [네트워크 개체](#)을 참조하십시오.

### Procedure

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.

- a. 원본 주소 메뉴를 확장하고 **Choose**(선택)을 클릭한 다음 **servername\_inside** 개체를 선택합니다.
- b. 변환된 주소 메뉴를 확장하고 **Choose**(선택)을 클릭한 다음 **servername\_outside** 개체를 선택합니다.

단계 10 섹션 4, **Advanced**(고급)을 건너뛴니다.

단계 11 FDM 관리 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.

단계 12 **Save**(저장)를 클릭합니다.

단계 13 ASA의 경우 네트워크 정책 규칙을 배포하거나 기다렸다가, FDM 관리 디바이스의 경우 액세스 제어 정책 규칙을 배포하여 트래픽이 *servername\_inside*에서 *servername\_outside*로 흐를 수 있도록 합니다.

단계 14 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

## 내부 네트워크의 사용자가 외부 인터페이스의 공용 IP 주소를 사용하여 인터넷에 액세스하도록 활성화

### 활용 사례

외부 인터페이스의 공용 주소를 공유하여 개인 네트워크의 사용자와 컴퓨터가 인터넷에 연결할 수 있도록 합니다.

### 전략

사설 네트워크의 모든 사용자가 디바이스의 외부 인터페이스 공용 IP 주소를 공유할 수 있도록 허용하는 포트 주소 변환(PAT) 규칙을 생성합니다.

사설 주소가 공용 주소 및 포트 번호에 매핑된 후 디바이스는 해당 매핑을 기록합니다. 해당 공용 IP 주소 및 포트에 향하는 들어오는 트래픽이 수신되면 디바이스는 이를 요청한 사설 IP 주소로 다시 보냅니다.

### Procedure

단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.

단계 6  > **Network Object NAT**를 클릭합니다.

단계 7 섹션 1, 유형 에서 **Dynamic**(동적)을 선택합니다. **Continue**(계속)를 클릭합니다.

단계 8 섹션 2, 인터페이스에서, 소스 인터페이스로 **any**(아무거나)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.

단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.

- a. 원래 주소 메뉴를 확장하고, **Choose**(선택)을 클릭한 다음 네트워크 구성에 따라 **any-ipv4** 또는 **any-ipv6** 개체를 선택합니다.
- b. 변환된 주소 메뉴를 확장하고 사용 가능한 목록에서 인터페이스를 선택합니다. 인터페이스는 외부 인터페이스의 공용 주소를 사용하도록 나타냅니다.

단계 10 FTD(Firepower Threat Defense)의 경우 섹션 5, **Name**(이름)에서 NAT 규칙에 이름을 지정합니다.

단계 11 **Save**(저장)를 클릭합니다.

단계 12 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.



**Note** 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

이 절차에 의해 생성된 **NAT** 규칙

```
object network any_network
nat (any,outside) dynamic interface
```

## 공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정

활용 사례


공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

사전 요구 사항

시작하기 전에 FTP, HTTP 및 SMTP 서버에 각각 하나씩 세 개의 개별 네트워크 개체를 생성합니다. 다음 절차를 위해 이러한 개체를 **ftp-server-object**, **http-server-object** 및 **smtp-server-object**라고 합니다. 지침은 **Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집**을 참조하십시오.

## FTP 서버에 대한 NAT 수신 FTP 트래픽

## Procedure

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.
  - 원본 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 **ftp-server-object**를 선택합니다.
  - 변환된 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 **Interface**(인터페이스)를 선택합니다.
  - **Use Port Translation**(포트 변환 사용)을 선택합니다.
  - **tcp, ftp, ftp**를 선택합니다.



- 단계 10 섹션 4, **Advanced**(고급)을 건너뛴니다.
- 단계 11 FTD(Firepower Threat Defense)의 경우 섹션 5, **Name**(이름)에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save**(저장)를 클릭합니다. NAT 테이블의 **NAT 규칙 처리 순서**에 새 규칙이 생성됩니다.
- 단계 13 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.


## HTTP 서버에 대한 NAT 수신 HTTP 트래픽

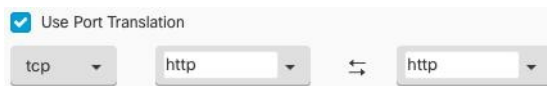
공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

## Before you begin

시작하기 전에 http 서버에 대한 네트워크 개체를 생성합니다. 이 절차에서는 개체를 **http-object**라고 합니다. 지침은 [Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집](#)을 참조하십시오.

## Procedure

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.
  - 원본 주소 메뉴를 확장하고 **Choose**(선택)을 클릭한 다음 **http-object**를 선택합니다.
  - 변환된 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 **Interface**(인터페이스)를 선택합니다.
  - **Use Port Translation**(포트 변환 사용)을 선택합니다.
  - **tcp, http, http**를 선택합니다.



- 단계 10 섹션 4, **Advanced**(고급)을 건너뛴니다.
- 단계 11 FTD(Firepower Threat Defense)의 경우 섹션 5, **Name**(이름)에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save**(저장)를 클릭합니다. NAT 테이블의 **NAT 규칙 처리 순서**에 새 규칙이 생성됩니다.
- 단계 13 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.


## SMTP 서버에 대한 NAT 수신 SMTP 트래픽

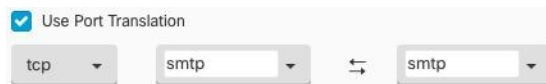
공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

### Before you begin

시작하기 전에 smtp 서버에 대한 네트워크 개체를 생성합니다. 이 절차에서는 개체를 **smtp-개체**라고 합니다. 지침은 [Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집](#)을 참조하십시오.

## Procedure

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.
- 원본 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 smtp-server-object를 선택합니다.
  - 변환된 주소 메뉴를 확장하고, **Choose**(선택)를 클릭한 다음 **Interface**(인터페이스)를 선택합니다.
  - **Use Port Translation**(포트 변환 사용)을 선택합니다.
  - **tcp, smtp, smtp**를 선택합니다.



- 단계 10 섹션 4, **Advanced**(고급)을 건너뛴니다.
- 단계 11 FTD(Firepower Threat Defense)의 경우 섹션 5, **Name**(이름)에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save**(저장)를 클릭합니다. NAT 테이블의 **NAT 규칙 처리 순서**에 새 규칙이 생성됩니다.
- 단계 13 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

## 사설 IP 주소 범위를 공용 IP 주소 범위로 변환

### 활용 사례

수신 디바이스(트랜잭션의 다른 끝에 있는 디바이스)가 트래픽을 허용하도록 IP 주소를 특정 범위로 변환해야 하는 특정 디바이스 유형 또는 사용자 유형 그룹이 있는 경우 이 접근 방식을 사용합니다.

## 내부 주소 풀을 외부 주소 풀로 변환

**Before you begin**

변환하려는 사설 IP 주소 풀에 대한 네트워크 개체를 생성하고 해당 사설 IP 주소를 변환하려는 공용 주소 풀에 대한 네트워크 개체를 생성합니다.




**Note** ASA FTD의 경우 "변환된 주소" 풀을 정의하는 네트워크 그룹은 서브넷을 정의하는 네트워크 개체일 수 없습니다.

이러한 주소 풀을 생성할 때 지침을 보려면 [하고 Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집을 사용하십시오.](#)

다음 절차를 위해 개인 주소 풀의 이름을 **inside\_pool**로 지정하고 공용 주소 풀의 이름을 **outside\_pool**로 지정했습니다.

**Procedure**

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Network Object NAT**를 클릭합니다.
- 단계 7 섹션 1 **Type**(유형)에서 **Dynamic**(동적)을 선택하고 **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, 인터페이스에서 소스 인터페이스를 내부로, 대상 인터페이스를 외부로 설정합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, **Packets**(패킷)에서, 다음 작업을 수행합니다.
  - 원본 주소의 경우 **Choose**(선택)을 클릭한 다음 위의 전제 조건 섹션에서 만든 **inside\_pool** 네트워크 개체(또는 네트워크 그룹)를 선택합니다.
  - 변환된 주소의 경우 **Choose**(선택)을 클릭한 다음 위의 전제 조건 섹션에서 만든 **outside\_pool** 네트워크 개체(또는 네트워크 그룹)를 선택합니다.
- 단계 10 섹션 4, **Advanced**(고급)을 건너뛵니다.
- 단계 11 FTD(Firepower Threat Defense)의 경우 섹션 5, **Name**(이름)에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save**(저장)를 클릭합니다.
- 단계 13 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 외부 인터페이스를 통과할 때 IP 주소 범위가 변환되지 않도록 방지

### 활용 사례

이 Twice NAT 사용 사례를 사용하여 사이트 투 사이트 VPN을 활성화합니다.

### 전략

네트워크의 한 위치에 있는 IP 주소가 다른 위치에 변경되지 않고 도착하도록 IP 주소 풀을 자체적으로 변환하고 있습니다.

## 2회 NAT 규칙 생성


### Before you begin

변환할 IP 주소 풀을 정의하는 네트워크 개체 또는 네트워크 그룹을 생성합니다. FTD의 경우 주소 범위는 서브넷을 정의하는 네트워크 개체 또는 범위의 모든 주소를 포함하는 네트워크 그룹 개체로 정의할 수 있습니다.

네트워크 개체 또는 네트워크 그룹을 생성할 때 지침을 보려면 [Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집](#)을 사용합니다.

다음 절차를 위해 네트워크 개체 또는 네트워크 그룹인 Site-to-Site-PC-Pool을 호출합니다.

### Procedure

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Management**(관리) 창에서 **NAT**를 클릭합니다.
- 단계 6  > **Twice NAT(2회 NAT)**를 클릭합니다..
- 단계 7 섹션 1, **Type**(유형)에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 8 섹션 2, **Interfaces**(인터페이스)에서 소스 인터페이스로 **inside**(내부)를 선택하고 대상 인터페이스로 **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
- 단계 9 섹션 3, 패킷에서 다음과 같이 변경합니다.
  - 원래 주소 메뉴를 확장하고 **Choose**(선택)를 클릭한 다음 전제 조건 섹션에서 생성한 사이트 투 사이트 PC 풀 개체를 선택합니다.
  - 변환된 주소 메뉴를 펼치고 **Choose**(선택)를 클릭한 후 전제 조건 섹션에서 생성한 Site-to-Site-PC-Pool 개체를 선택합니다.
- 단계 10 섹션 4, **Advanced**(고급)을 건너뛴니다.



- 단계 11 FTD(Firepower Threat Defense)의 경우 섹션 5, **Name(이름)**에서 NAT 규칙에 이름을 지정합니다.
- 단계 12 **Save(저장)**를 클릭합니다.
- 단계 13 ASA의 경우 암호화 맵을 생성합니다. 암호화 맵 생성에 대한 자세한 내용은 [CLI 책 3: Cisco ASA Series VPN CLI 구성 가이드](#)를 참조하고 LAN-to-LAN IPsec VPN에 대한 장을 검토하십시오.
- 단계 14 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

## 가상 프라이빗 네트워크 관리

VPN(Virtual Private Network)은 인터넷과 같은 공용 네트워크를 통해 엔드포인트 간에 보안 터널을 설정합니다.

이 섹션은 FDM 매니저드 디바이스의 원격 액세스 및 사이트 투 사이트 VPN에 적용됩니다. FTD에서 사이트 간 VPN 연결을 구축하기 위한 IPsec(Internet Protocol Security) 표준에 대해 설명합니다. 또한 FTD에서 VPN 연결을 배포하고 원격 액세스하는 데 사용되는 SSL 표준에 대해서도 설명합니다.

CDO에서는 다음과 같은 유형의 VPN 연결을 지원합니다.

- [사이트 간 가상 프라이빗 네트워크, 459 페이지](#)
- [원격 액세스 가상 프라이빗 네트워크](#)

가상 사설 네트워크에 대한 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)를 참조하십시오.

## 사이트 간 가상 프라이빗 네트워크

사이트간 VPN 터널은 다양한 위치에 있는 네트워크를 연결합니다. 관리형 디바이스 및 관리형 디바이스와 모든 관련 표준을 준수하는 다른 Cisco 또는 타사 피어 간에 Site-to-Site IPsec 연결을 만들 수 있습니다. 이러한 피어는 IPv4와 IPv6 주소를 사용하여 내부 주소와 외부 주소를 함께 포함할 수 있습니다. Site-to-Site 터널은 IPsec(Internet Protocol Security) 프로토콜 제품군 및 인터넷 키 교환 버전 2(IKEv2)를 사용하여 구축됩니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다.

### VPN 토폴로지

새로운 Site-to-Site VPN 토폴로지를 생성하려면 고유한 이름을 부여하거나 토폴로지 유형을 지정하거나 IPsec IKEv1 또는 IKEv2에 사용되는 IKE 버전 또는 둘 다 및 인증 방법을 선택해야 합니다. 구성된 후 토폴로지를 FTD에 구축합니다.

### IPsec 및 IKE

CDO에서 Site-to-Site VPN은 IKE 정책과 VPN 토폴로지에 할당된 IPsec 제안을 기반으로 구성됩니다. 정책 및 제안은 IPsec 터널에서 트래픽을 보호하는 데 사용되는 보안 프로토콜 및 알고리즘과 같은

Site-to-Site VPN의 특성을 정의하는 파라미터 집합입니다. VPN 토폴로지에 할당할 수 있는 전체 구성 이미지를 정의하려면 몇 가지 정책 유형이 필요할 수 있습니다.

### 인증

VPN 연결을 인증하려면 각 디바이스의 토폴로지에서 사전 공유 키를 구성합니다. 사전 공유 키를 사용하면 IKE 인증 단계에서 사용되는 보안 키를 두 피어 간에 공유할 수 있습니다.

### Virtual Tunnel Interface(VTI)

CDO는 현재 FTD에서 VTI(Virtual Tunnel Interface) 터널의 관리, 모니터링 또는 사용을 지원하지 않습니다. VTI 터널이 구성된 디바이스는 CDO에 온보딩될 수 있지만 VTI 인터페이스는 무시됩니다. 보안 영역 또는 고정 경로가 VTI를 참조하는 경우 CDO는 VTI 참조 없이 보안 영역 및 고정 경로를 읽습니다. VTI 터널에 대한 CDO 지원이 곧 제공될 예정입니다.

관련 정보:

- [FDM-관리 디바이스에 대한 사이트 간 VPN 구성, on page 460](#)
- [FDM-관리 디바이스 사이트 간 가상 사설망 모니터링](#)

## FDM-관리 디바이스에 대한 사이트 간 VPN 구성

Cisco Defense Orchestrator(CDO)는 FDM 관리 디바이스에서 사이트 간 VPN 기능의 다음 측면을 지원합니다.

- IPsec IKEv1 및 IKEv2 프로토콜이 모두 지원됩니다.
- 인증을 위한 자동 또는 수동 사전 공유 키.
- IPv4 및 IPv6. 내부와 외부의 모든 조합이 지원됩니다.
- IPsec IKEv2 사이트 간 VPN 토폴로지는 보안 인증을 준수하기 위한 구성 설정을 제공합니다.
- 정적 및 동적 인터페이스.
- 엔드포인트로 작동하는 엑스트라넷 디바이스의 동적 IP 주소 지원.

### 엑스트라넷 디바이스

각 토폴로지 유형에는 CDO에서 관리되지 않는 엑스트라넷 디바이스가 포함될 수 있습니다. 예를 들면 다음과 같습니다.

- CDO에서 지원하지만 조직에는 책임이 부여되지 않는 Cisco 디바이스. 회사 내의 다른 조직에서 관리하는 네트워크의 스포크 또는 서비스 제공자나 파트너의 네트워크에 대한 연결 등이 포함됩니다.
- 관리되지 않는 디바이스. CDO를 사용하여 관리되지 않는 디바이스에 구성을 생성하거나 구축할 수 없습니다. 관리되지 않는 디바이스를 VPN 토폴로지에 "엑스트라넷" 디바이스로 추가합니다. 또한 각 원격 디바이스의 IP 주소를 지정합니다.

### 동적 주소 지정 피어로 사이트 간 VPN 연결 구성

CDO를 사용하면 피어의 VPN 인터페이스 IP 주소 중 하나를 알 수 없거나 인터페이스가 DHCP 서버에서 주소를 가져올 때 피어 간에 사이트 간 VPN 연결을 생성할 수 있습니다. 사전 공유 키, IKE 설정 및 IPsec 구성이 다른 피어와 일치하는 모든 동적 피어는 사이트 간 VPN 연결을 설정할 수 있습니다.

피어 A와 B를 고려하십시오. 고정 피어는 VPN 인터페이스의 IP 주소가 고정되어 있는 디바이스이고 동적 피어는 VPN 인터페이스의 IP 주소를 알 수 없거나 임시 IP 주소가 있는 디바이스입니다.

다음 사용 사례에서는 동적으로 주소가 지정된 피어를 사용하여 안전한 사이트 간 VPN 연결을 설정하는 다양한 시나리오를 설명합니다.

- A는 정적 피어이고 B는 동적 피어이거나 그 반대입니다.
- A는 고정 피어이고 B는 DHCP 서버에서 확인된 IP 주소를 사용하거나 그 반대로 하는 동적 피어입니다. **Bind VPN to the assigned IP(할당된 IP에 VPN 바인딩)**를 선택하여 고정 피어의 IP 주소와 동적 피어의 DHCP 할당 IP 주소 간에 VPN 연결을 설정할 수 있습니다.
- A 및 B는 DHCP 서버에서 확인된 IP 주소를 사용하는 동적 주소입니다. 이 경우 고정 피어의 IP 주소와 동적 피어의 DHCP 할당 IP 주소 간에 VPN 연결을 설정하려면 하나 이상의 피어에 대해 **Bind VPN to the assigned IP(할당된 IP에 VPN 바인딩)**을 선택해야 합니다.
- A는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다.
- A는 DHCP 서버에서 확인된 IP 주소를 사용하는 동적 피어이고, B는 고정 또는 동적 IP 주소를 사용하는 엑스트라넷 디바이스입니다. **Bind VPN to the assigned IP(할당된 IP에 VPN 바인딩)**를 선택하여 고정 피어의 IP 주소와 동적 피어의 DHCP 할당 IP 주소 간에 VPN 연결을 설정할 수 있습니다.



#### Important

**Bind VPN to the assigned IP(할당된 IP에 VPN 바인딩)**를 선택하면 VPN이 DHCP 할당 IP 주소에 고정으로 바인딩합니다. 그러나 이 동적 인터페이스는 피어가 재시작된 후 여러 개의 새 IP 주소를 수신할 수 있습니다. VPN 터널이 새 IP 주소를 업데이트하더라도 다른 피어는 새 구성으로 업데이트되지 않습니다. 다른 피어에서 대역 외 변경 사항을 적용하려면 사이트 간 구성을 다시 구축해야 합니다.



#### Note

firewall device manager와 같은 로컬 관리자를 사용하여 인터페이스의 IP 주소를 변경하면 CDO에서 해당 피어의 **Configuration Status(구성 상태)**가 "Conflict Detected(충돌 탐지됨)"로 표시됩니다. **구성 충돌 해결**하면 다른 피어의 **Configuration Status(구성 상태)**가 "Not Synced(동기화되지 않음)" 상태로 변경됩니다. "Not Synced(동기화되지 않음)" 상태인 디바이스에 CDO 구성을 구축해야 합니다.

일반적으로 동적 피어는 연결을 시작하는 피어야 합니다. 다른 피어는 동적 피어의 IP 주소를 알지 못하기 때문입니다. 원격 피어가 연결을 설정하려고 시도하면 다른 피어가 사전 공유 키, IKE 설정 및 IPsec 구성을 사용하여 연결을 검증합니다.

원격 피어에서 연결을 시작한 후에만 VPN 연결이 설정되므로 VPN 터널에서 트래픽을 허용하는 액세스 제어 규칙과 일치하는 모든 아웃바운드 트래픽은 연결이 설정될 때까지 중단됩니다. 이를 통해 데이터가 적절한 암호화 및 VPN 보호 없이 네트워크를 벗어나지 않게 합니다.



**Note** 다음 시나리오에서는 사이트 간 VPN 연결을 구성할 수 없습니다.

- 두 피어 모두에 DHCP 할당 IP 주소가 있는 경우
  - 해결 방법: 피어 중 하나에 DHCP 서버에서 확인된 IP 주소가 있는 경우 사이트 간 VPN을 구성할 수 있습니다. 이 경우 **Bind VPN to the assigned IP**(할당된 IP에 VPN 바인딩)을 선택하여 사이트 간 VPN을 구성해야 합니다.
- 디바이스에 둘 이상의 동적 피어 연결이 있는 경우
  - 해결 방법: 다음 단계를 수행하여 사이트 간 VPN을 구성할 수 있습니다.
    - 3개의 디바이스 A, B 및 C를 고려하십시오.
    - A(고정 피어)와 B(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다.
    - 엑스트라넷 디바이스를 생성하여 A와 C(동적 피어) 간에 사이트 간 VPN 연결을 구성합니다. A의 고정 VPN 인터페이스 IP 주소를 엑스트라넷 디바이스에 할당하고 C와의 연결을 설정합니다.

#### FDM-관리 디바이스 사이트 간 VPN 가이드 및 제한 사항

- CDO는 S2S VPN에 대한 흥미로운 트래픽을 설계하기 위해 `crypto-acl`을 지원하지 않습니다. 이는 보호된 네트워크만 지원됩니다.
- CDO는 현재 ASA 또는 FDM 관리 디바이스에서 VTI(Virtual Tunnel Interface) 터널의 관리, 모니터링 또는 사용을 지원하지 않습니다. VTI 터널이 구성된 디바이스는 CDO에 온보딩될 수 있지만 VTI 인터페이스는 무시됩니다. 보안 영역 또는 고정 경로가 VTI를 참조하는 경우 CDO는 VTI 참조 없이 보안 영역 및 고정 경로를 읽습니다. VTI 터널에 대한 CDO 지원이 곧 제공될 예정입니다.
- IKE 포트 500/4500이 사용 중이거나 활성화된 일부 PAT 변환이 있을 때마다 사이트 간 VPN을 동일한 포트에서 구성할 수 없으므로 해당 포트에서 서비스를 시작하는 데 실패합니다.
- 전송 모드는 지원되지 않으며 터널 모드만 지원됩니다. IPsec 터널 모드는 새 IP 패킷에서 페이로드가 되는 원래 IP 데이터그램 전체를 암호화합니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec이 구현되는 통상적인 방식입니다.
- 이 릴리스에서는 하나 이상의 VPN 터널을 포함하는 PTP 토폴로지만 지원됩니다. Point-to-Point 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.

#### 관련 정보:

- [사이트 간 VPN 생성](#)
- [기존 CDO 사이트 간 VPN 편집](#)

- VPN에서 사용되는 암호화 및 해시 알고리즘
- NAT에서 사이트 간 VPN 트래픽 제외

## 사이트 간 VPN 생성

단순 구성 및 고급 구성의 두 가지 방법 중 하나를 사용하여 사이트 간 VPN을 생성할 수 있습니다. 단순 구성에서는 사이트 간 VPN 연결을 설정하는 데 기본 구성이 사용됩니다. **Advanced(고급)** 모드에서 구성을 수정할 수 있습니다.

각 사이트 간 VPN 토폴로지에는 CDO에서 관리하지 않는 엑스트라넷 디바이스가 포함될 수 있습니다. 엑스트라넷 디바이스는 CDO에 의해 관리되지 않는 모든 디바이스(Cisco 또는 타사)일 수 있습니다.


이 릴리스에서는 사이트 간 연결당 하나의 터널을 포함하는 PTP 토폴로지만 지원됩니다. Point-to-Point 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.

관련 정보:

- [단순 구성을 사용하여 사이트 투 사이트 VPN 생성, on page 463](#)
- [고급 구성을 사용하여 사이트 간 VPN 생성, on page 464](#)
- [사이트 대 사이트 피어 간 보호된 트래픽에 대한 네트워킹 구성, on page 466](#)

## 단순 구성을 사용하여 사이트 투 사이트 VPN 생성


### Procedure

- 
- 단계 1** 탐색 창에서 **VPN > Site-to-Site VPN**을 선택합니다.
- 단계 2** 파란색 더하기  버튼을 클릭하여 VPN 터널을 생성합니다.
- Note** 또는 **Inventory(재고 목록)** 페이지에서 Site-to-Site VPN 연결을 생성할 수 있습니다.
- 탐색 모음에서 **Inventory(재고 목록)**를 클릭합니다.
  - 구성하려는 두 개의 FDM 관리 디바이스를 선택합니다. 엑스트라넷 디바이스를 선택하는 경우 엑스트라넷 디바이스의 IP 주소를 지정합니다.
  - 오른쪽 페이지의 **Device Actions(디바이스 작업)** 아래에서 **Create Site-to-Site VPN(사이트 간 VPN 생성)**를 클릭합니다.
- 단계 3** 고유한 토폴로지 **Configuration Name(설정 이름)**을 입력합니다. FDM 관리 디바이스 VPN 및 해당 토폴로지 유형임을 나타내도록 토폴로지의 이름을 지정하는 것이 좋습니다.
- 단계 4** **Devices(디바이스)**에서 이 VPN 배포에 대한 엔드포인트 디바이스를 선택합니다.
- 단계 5** **Peer 2(피어 2)**에서 엑스트라넷 디바이스를 선택하는 경우 **Static(고정)**을 선택하고 IP 주소를 지정하거나, DHCP가 할당된 IP를 사용하는 엑스트라넷 디바이스의 경우 **Dynamic(동적)**을 선택합니다. **IP**

**Address(IP 주소)**에는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP 할당)**가 표시됩니다.

단계 6 엔드포인트 디바이스에 대한 **VPN Access Interface(VPN 액세스 인터페이스)**를 선택합니다.

**Note** 엔드포인트 디바이스 중 하나 또는 둘 다에 동적 IP 주소가 있는 경우 추가 지침은 [동적 주소 지정 피어로 사이트 간 VPN 연결 구성](#)을 참조하십시오.

단계 7 파란색 더하기  버튼을 클릭하여 참여하는 디바이스에 대해 **Protected Networks(보호된 네트워크)**를 추가합니다.

단계 8 (선택 사항) **NAT 제외**를 선택하여 로컬 VPN 액세스 인터페이스의 NAT 정책에서 VPN 트래픽을 제외합니다. 개별 피어에 대해 수동으로 구성해야 합니다. NAT 규칙을 로컬 네트워크에 적용하지 않으려는 경우 로컬 네트워크를 호스팅하는 인터페이스를 선택합니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 멤버 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 [NAT에서 사이트 간 VPN 트래픽 제외](#)를 참조하십시오.

단계 9 **Create VPN(VPN 생성)**을 클릭한 다음 **Finish(마침)**를 클릭합니다.


단계 10 추가 필수 구성을 수행합니다. [사이트 대 사이트 피어 간 보호된 트래픽에 대한 네트워킹 구성](#)을 참조하십시오.

사이트 투 사이트 VPN이 구성되었습니다.

## 고급 구성을 사용하여 사이트 간 VPN 생성

### Procedure


단계 1 내비게이션 바에서 **VPN**을 선택합니다.

단계 2 파란색 더하기  버튼을 클릭하여 VPN 터널을 생성합니다.

단계 3 **Peer Devices(피어 디바이스)** 섹션에서 다음 디바이스 구성을 지정합니다.

- a. 고유한 토폴로지 **Configuration Name(설정 이름)**을 입력합니다. FDM 관리 디바이스 VPN 및 해당 토폴로지 유형임을 나타내도록 토폴로지의 이름을 지정하는 것이 좋습니다.
- b. **Devices(디바이스)**에서 이 VPN 구축에 대한 엔드포인트 디바이스를 선택합니다.
- c. 엑스트라넷 디바이스를 선택하는 경우 **Static(고정)**을 선택하고 IP 주소를 지정하거나, DHCP가 할당된 IP를 사용하는 엑스트라넷 디바이스의 경우 **Dynamic(동적)**을 선택합니다. **IP Address(IP 주소)**에는 정적 인터페이스의 IP 주소 또는 동적 인터페이스의 **DHCP Assigned(DHCP 할당)**가 표시됩니다.
- d. 엔드포인트 디바이스에 대한 **VPN 액세스 인터페이스**를 선택합니다.

**Note**      엔드포인트 디바이스 중 하나 또는 둘 다에 동적 IP 주소가 있는 경우 추가 지침은 [동적 주소 지정 피어로 사이트 간 VPN 연결 구성](#)을 참조하십시오.

단계 4 파란색 더하기  버튼을 클릭하여 참여하는 디바이스에 대해 **Protected Networks**(보호된 네트워크)를 추가합니다.


단계 5 **Advanced**(고급)를 클릭합니다.


단계 6 **IKE Settings**(IKE 설정) 섹션에서 IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택하고 프라이버시 구성을 지정합니다. IKE 정책에 대한 자세한 내용은 [글로벌 IKE 정책 구성, on page 156](#)의 내용을 참조하십시오.

**Note**      IKE 정책은 디바이스에 전역적이며 연결된 모든 VPN 터널에 적용됩니다. 따라서 정책을 추가하거나 삭제하면 이 디바이스가 참여하는 모든 VPN 터널에 영향을 미칩니다.



a. 필요에 따라 두 옵션 중 하나를 선택하거나 두 옵션을 모두 선택합니다.

**Note**      기본적으로 **IKEV** 버전 2가 활성화되고 **IKEV2** 정책이 활성화됩니다.

b. 파란색 더하기  버튼을 클릭하고 IKEv2 정책을 선택합니다.

**Create New IKEv2 Policy**(새 IKEv2 정책 생성)를 클릭하여 새 IKEv2 정책을 생성합니다. 또는 CDO 내비게이션 바로 이동하여 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭한 다음,  > **IKEv2 Policy**(IKEv2 정책)를 클릭해도 됩니다. 새 IKEv2 정책 생성에 대한 자세한 내용은 [IKEv2 정책 관리](#)을 참고하십시오. 기존 IKEv2 정책을 삭제하려면 선택한 정책 위에 마우스를 놓고 **x** 아이콘을 클릭합니다.

c. **IKE Version 1**(IKE 버전 1)을 클릭하여 활성화합니다.

d. 파란색  더하기 버튼을 클릭하고 IKEv1 정책을 선택합니다. **Create New IKEv1 Policy**(새 IKEv1 정책 생성)를 클릭하여 새 IKEv1 정책을 생성합니다. 또는 CDO 내비게이션 바로 이동하여 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭한 다음,  > **IKEv1 Policy**(IKEv1 정책)를 클릭해도 됩니다. 새 IKEv1 정책 생성에 대한 자세한 내용은 [IKEv1 정책 관리](#)을 참고하십시오. 기존 IKEv1 정책을 삭제하려면 선택한 정책 위에 마우스 커서를 올리고 **x** 아이콘을 클릭합니다.

e. 참여 디바이스에 대한 사전 공유 키를 입력합니다. 사전 공유 키는 연결에서 각 피어에 컨피그레이션된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용됩니다.

- (IKEv2) 피어 1 사전 공유 키, 피어 2 사전 공유 키: IKEv2의 경우 각 피어에서 고유한 키를 구성할 수 있습니다. 사전 공유 키를 입력합니다. **Show Override**(재정의 표시) 버튼을 클릭하고 피어에 대해 적절한 사전 공유를 입력할 수 있습니다. 키는 영숫자 1~127자가 될 수 있습니다. 다음 표에서는 두 피어에 대한 사전 공유 키의 용도에 대해 설명합니다.


	로컬 사전 공유 키	원격 피어 사전 공유 키
피어 1	피어 1 사전 공유 키	피어 2 사전 공유 키
피어 2	피어 2 사전 공유 키	피어 1 사전 공유 키


- (IKEv1) 사전 공유 키: IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 컨피그레이션해야 합니다. 키는 영숫자 1~127자가 될 수 있습니다. 이 시나리오에서 피어 1과 피어 2는 동일한 사전 공유 키를 사용하여 데이터를 암호화하고 해독합니다.

f. **Next**(다음)를 클릭합니다.

**단계 7 IPSec Settings(IPSec 설정)** 섹션에서 IPSec 구성을 지정합니다. **IKE Settings(IKE 설정)** 단계에서 선택한 항목에 따라 해당 IKEV 제안을 사용할 수 있습니다.

IPSec 설정에 대한 자세한 내용은 [IPsec 제안 구성, on page 153](#)의 내용을 참조하십시오.

- a. 파란색  더하기 버튼을 클릭하고 IKEv2 제안을 선택합니다. 기존 IKEv2 제안을 삭제하려면 선택한 제안 위에 마우스를 올려 놓고 **x** 아이콘을 클릭합니다.

**Note** Create New IKEv2 Proposal(새 IKEv2 제안 생성)을 클릭하여 새 IKEv2 제안을 생성합니다. 또는 CDO 내비게이션 바로 이동하여 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭한 다음,  **> IKEv2 IPsec Proposal(IKEv2 IPsec 제안)**을 클릭해도 됩니다.

새 IKEv2 정책 생성에 대한 자세한 내용은 [IKEv2 IPsec 제안 개체 관리](#)를 참고하십시오.

- b. **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다. 자세한 내용은 [사용할 Diffie-Hellman 모듈러스 그룹 결정](#)을 참조하십시오.
- c. **Create VPN(VPN 생성)**을 클릭합니다.
- d. 구성을 읽고 만족하면 **Finish**(마침)를 클릭합니다.
- e. 추가 필수 구성을 수행합니다. [사이트 대 사이트 피어 간 보호된 트래픽에 대한 네트워킹 구성](#)을 참조하십시오.

## 사이트 대 사이트 피어 간 보호된 트래픽에 대한 네트워킹 구성

사이트 간 연결 구성을 완료한 후에는 VPN이 모든 대상 디바이스에서 작동하도록 다음 구성을 수행해야 합니다.

### Procedure

**단계 1 AC 정책을 구성합니다.**

두 피어 뒤에 있는 보호된 네트워크 간의 양방향 트래픽을 허용하기 위해 AC 정책을 구성합니다. 이러한 정책은 패킷이 손실되지 않고 의도된 대상으로 이동하도록 도와줍니다.

**Note** 두 피어 모두에서 수신 및 발신 트래픽에 대한 AC 정책을 생성해야 합니다.

- a. 왼쪽의 Cisco Defense Orchestrator 탐색 모음에서 **Policies(정책)**를 클릭하고 원하는 옵션을 선택합니다.



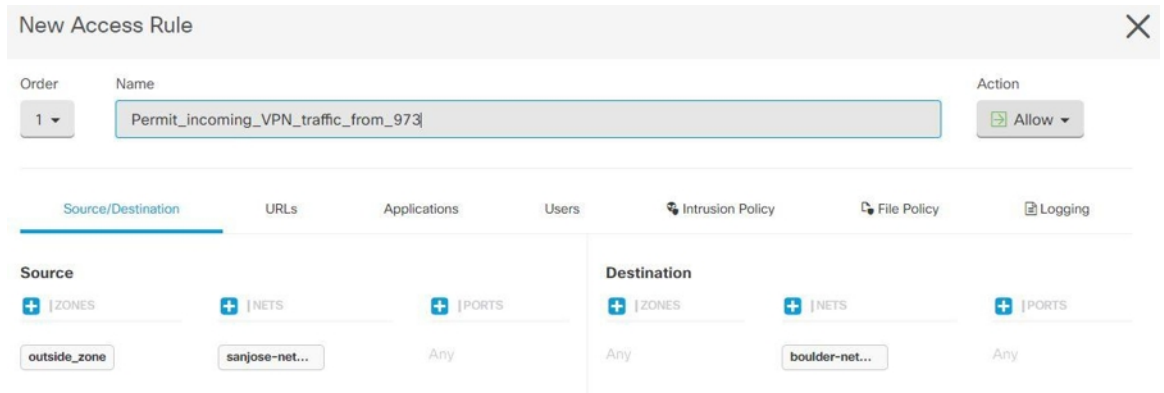
- b. 두 피어 모두에서 수신 및 발신 트래픽에 대한 정책을 생성합니다. AC 정책 생성에 대한 자세한 내용은 [FDM 액세스 제어 정책 구성](#)을 참조하십시오.

다음 예는 두 피어 모두에서 AC 정책을 생성하는 단계를 보여줍니다.

각각 2개의 보호된 네트워크 'boulder-network' 및 'sanjose-network' 간에 Site-to-Site VPN 연결을 사용하는 2개의 FDM 관리 디바이스 'FTD\_BGL\_972' 및 'FTD\_BGL\_973'을 고려하십시오.

수신 트래픽을 허용하기 위한 AC 정책 생성:

'FTD\_BGL\_972' 디바이스에서 피어(FTD\_BGL\_973)의 수신 트래픽을 허용하기 위해 'Permit\_incoming\_VPN\_traffic\_from\_973' 정책이 생성됩니다.



- **Source Zone**(소스 영역): 네트워크 트래픽이 시작되는 피어 디바이스의 영역을 설정합니다. 이 예에서 트래픽은 FTD\_BGL\_973에서 시작되어 FTD\_BGL\_972에 도달합니다.
- **Source Network**(소스 네트워크): 네트워크 트래픽이 시작되는 피어 디바이스의 보호된 네트워크를 설정합니다. 이 예에서 트래픽은 피어 디바이스(FTD\_BGL\_973) 뒤에 있는 보호되는 네트워크인 'sanjose-network'에서 시작됩니다.
- **Destination Network**(대상 네트워크): 네트워크 트래픽이 도착하는 디바이스의 보호된 네트워크를 설정합니다. 이 예에서 트래픽은 피어 디바이스(FTD\_BGL\_972) 뒤에 있는 보호되는 네트워크인 'boulder-network'에 도착합니다. 참고: 나머지 필드는 기본값("Any(모두)")을 사용할 수 있습니다.
- 정책에서 침입 및 기타 검사 설정의 영향을 받는 트래픽을 허용하려면 **Action**(작업)을 **Allow**(허용)으로 설정합니다.

발신 트래픽을 허용하기 위한 AC 정책 생성:

피어(FTD\_BGL\_973)로의 발신 트래픽을 허용하기 위해 'FTD\_BGL\_972' 디바이스에서 'Permit\_outgoing\_VPN\_traffic\_to\_973' 정책이 생성됩니다.

The screenshot shows the 'New Access Rule' configuration page. At the top, the rule name is 'Permit\_outgoing\_VPN\_traffic\_to\_973' and the action is 'Allow'. Below this, there are tabs for 'Source/Destination', 'URLs', 'Applications', 'Users', 'Intrusion Policy', 'File Policy', and 'Logging'. The 'Source/Destination' tab is selected, showing a grid for configuring source and destination. The source is set to 'Any' and 'boulder-net...'. The destination is set to 'outside\_zone' and 'sanjose-net...'.

- **Source Network(소스 네트워크):** 네트워크 트래픽이 시작되는 피어 디바이스의 보호된 네트워크를 설정합니다. 이 예에서 트래픽은 피어 디바이스(FTD\_BGL\_972) 뒤에 있는 보호되는 네트워크인 'boulder-network'에서 시작됩니다.
- **Destination Zone(대상 영역):** 네트워크 트래픽이 도착하는 피어 디바이스의 영역을 설정합니다. 이 예에서는 트래픽이 FTD\_BGL\_972에서 도착하여 FTD\_BGL\_973에 도달하고 있습니다.
- **Destination Network(대상 네트워크):** 네트워크 트래픽이 도착하는 피어의 보호된 네트워크를 설정합니다. 이 예에서 트래픽은 피어 디바이스(FTD\_BGL\_972) 뒤에 있는 보호되는 네트워크인 'sanjose-network'에 도착합니다. 참고: 나머지 필드는 기본값("Any(모두)")을 사용할 수 있습니다.
- 정책에서 침입 및 기타 검사 설정의 영향을 받는 트래픽을 허용하려면 **Action(작업)**을 **Allow(허용)**으로 설정합니다.

한 디바이스에서 AC 정책을 생성한 후에는 해당 피어에서 유사한 정책을 생성해야 합니다.

**단계 2** NAT가 피어 디바이스 중 하나에 구성된 경우 NAT 제외 규칙을 수동으로 구성해야 합니다. [NAT에서 사이트 간 VPN 트래픽 제외](#) 를 참조하십시오.

**단계 3** 각 피어에서 반환 VPN 트래픽을 수신하기 위한 라우팅을 구성합니다. 자세한 내용은 [FDM-관리 디바이스에 대한 고정 및 기본 경로 구성](#)을 참조하십시오.

- Gateway(게이트웨이)** — 대상 네트워크에 대해 게이트웨이의 IP 주소를 식별하는 네트워크 개체를 선택합니다. 트래픽은 이 주소로 전송됩니다.
- Interface(인터페이스)** — 트래픽을 전송하는 데 사용할 인터페이스를 선택합니다. 이 예에서 트래픽은 '외부' 인터페이스를 통해 전송됩니다.
- Destination Networks(대상 네트워크)** -대상 네트워크를 식별하는 하나 이상의 네트워크 개체를 선택합니다. 이 예에서 대상은 피어(FTD\_BGL\_973) 뒤에 있는 'sanjose-network'입니다.

한 디바이스에서 라우팅 설정을 구성한 후에는 해당 피어에서 유사한 설정을 구성해야 합니다.

## 기존 CDO 사이트 간 VPN 편집

고급 구성 마법사는 기본적으로 기존 사이트 간 VPN 구성을 수정하는 데 사용됩니다.

### Procedure

단계 1 내비게이션 바에서 **VPN > Site-to-Site VPN**(사이트 간 VPN)을 선택합니다.

단계 2 편집할 원하는 사이트 간 VPN 터널을 선택합니다.

단계 3 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

**Note** 또는 다음을 수행하여 구성을 편집할 수 있습니다.

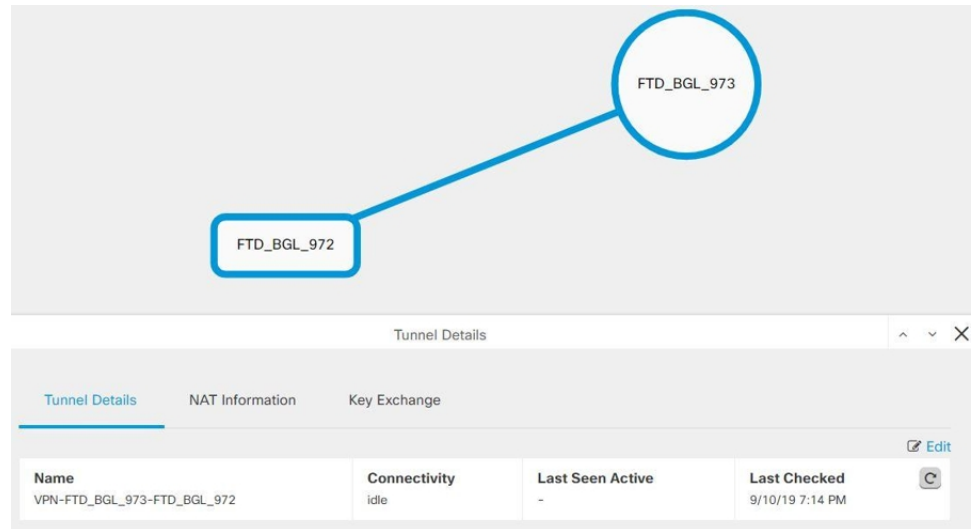
- VPN 페이지를 열고 필터 패널에서 **Global View**(전역 보기) 버튼을 클릭합니다(자세한 내용은 [사이트 간 VPN 터널 검색 및 필터링](#) 참조).

모든 디바이스에서 사용 가능한 모든 사이트 간 VPN 터널의 그림이 나타납니다.

구성을 편집하려면 피어 중 하나가 FDM 관리 디바이스여야 합니다.

- 상자를 클릭하여 디바이스를 선택합니다.
- View details**(세부 정보 보기)를 클릭하여 피어를 확인합니다.
- 터널 세부 정보를 보려면 피어 디바이스를 클릭합니다.

디바이스와 관련된 터널 세부 정보, NAT 정보 및 키 교환 정보를 볼 수 있습니다.





- Tunnel Details**(터널 세부 정보)에서 **Edit**(편집)을 클릭합니다.


단계 4 **Peer Devices**(피어 디바이스) 섹션에서 **Configuration Name**(구성 이름), **VPN Access Interface**(VPN 액세스 인터페이스) 및 **Protected Networks**(보호된 네트워크) 디바이스 구성을 수정할 수 있습니다.

**Note** 참여 디바이스는 변경할 수 없습니다.

단계 5 **IKE Settings(IKE 설정)** 섹션에서 다음 IKEv2 정책 구성을 수정할 수 있습니다.

- a. 각 디바이스에 대한 파란색 더하기  버튼을 클릭하고 새 IKEv2 정책을 선택합니다. 기존 IKEv2 정책을 삭제하려면 선택한 정책 위에 마우스를 놓고 **x** 아이콘을 클릭합니다.
- b. 참여 디바이스에 대한 사전 공유 키를 수정합니다. 엔드포인트 디바이스의 사전 공유 키가 다른 경우 파란색 설정  버튼을 클릭하고 디바이스에 대한 적절한 사전 공유 키를 입력합니다.
- c. **Next(다음)**를 클릭합니다.

단계 6 **IPSec Settings(IPSec 설정)** 섹션에서 다음 IPSec 구성을 수정할 수 있습니다.

- a. 파란색 더하기  버튼을 클릭하여 새 IKEv2 제안을 선택합니다. 기존 IKEv2 제안을 삭제하려면 선택한 제안 위에 마우스를 올려 놓고 **x** 아이콘을 클릭합니다.
- b. **Perfect Forward Secrecy**용 **Diffie-Hellman** 그룹을 선택합니다.
- c. **Edit VPN(VPN 편집)**을 클릭한 다음 **Finish(마침)**를 클릭합니다.

---

포인트 투 포인트 VPN이 수정되고 모든 변경 사항으로 업데이트됩니다.

기존 CDO 사이트 투 사이트 VPN 삭제

### Procedure

---

단계 1 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 선택합니다.

단계 2 삭제할 원하는 사이트 투 사이트 VPN 터널을 선택합니다.

단계 3 **Actions(작업)** 창에서 **Delete(삭제)**를 클릭합니다.

---

선택한 사이트 투 사이트 VPN 터널이 삭제됩니다.

**VPN**에서 사용되는 암호화 및 해시 알고리즘

VPN 터널은 일반적으로 공용 네트워크(대개 인터넷)를 통과하므로 연결을 암호화하여 트래픽을 보호해야 합니다. IKE 정책 및 IPSec 제안을 사용하여 적용할 암호화 및 기타 보안 기술을 정의합니다.

디바이스 라이선스에서 강력한 암호화 적용이 허용되는 경우에는 광범위한 암호화 및 해시 알고리즘과 Diffie-Hellman 그룹 중에서 선택할 수 있습니다. 그러나 일반적으로는 터널에 적용하는 암호화가 강력할수록 시스템 성능은 더 나빠집니다. 따라서 효율성을 저하하지 않으면서 충분한 보호 기능을 제공하는 보안과 성능 간의 적절한 균형 지점을 찾아야 합니다.

Cisco는 선택할 수 있는 옵션에 대한 구체적인 지침을 제공하지는 않습니다. 대규모 기업이나 기타 조직 내에서 보안을 담당하는 경우 충족해야 하는 표준이 이미 정의되어 있을 수 있습니다. 그렇지 않은 경우, 선택할 수 있는 옵션에 대해 조사해야 합니다.

다음 주제에서는 사용 가능한 옵션에 대해 설명합니다.

#### 사용할 암호화 알고리즘 결정

IKE 정책 또는 IPsec 제안에 사용할 암호화 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다.

IKEv2의 경우 여러 암호화 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

IPsec 제안의 경우 알고리즘은 인증, 암호화 및 재생 방지 서비스를 제공하는 ESP(Encapsulating Security Protocol)에서 사용됩니다. ESP는 IP 프로토콜 유형 50입니다. IKEv1 IPsec 제안에서 알고리즘 이름에는 ESP- 접두사가 붙습니다.

디바이스 라이선스에 따라 강력한 암호화를 사용할 수 있는 경우 다음 암호화 알고리즘 중에서 선택할 수 있습니다. 강력한 암호화를 사용할 수 없으면 DES만 선택할 수 있습니다.

- AES-GCM - (IKEv2만 해당) 기밀 유지 및 데이터 원본 인증 기능을 제공하는 블록 암호화 작동 모드인 AES-GCM(Advanced Encryption Standard in Galois/Counter Mode)은 AES보다 보안성이 뛰어납니다. AES-GCM은 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다. GCM은 NSA Suite B를 지원하는 데 필요한 AES의 모드입니다. NSA Suite B는 암호화 강도에 대한 연방 기준을 충족시키기 위해 디바이스가 지원해야 하는 암호화 알고리즘 세트입니다.
- AES-GMAC - (IKEv2 IPsec 제안만 해당) AES-GMAC(Advanced Encryption Standard Galois Message Authentication Code)는 데이터 원본 인증 기능만 제공하는 블록 암호화 작동 모드입니다. 이 모드는 데이터를 암호화하지 않고 데이터 인증을 허용하는 AES-GCM의 변형입니다. AES-GMAC는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다.
- AES - AES(Advanced Encryption Standard)는 DES보다 보안성이 뛰어나며 3DES보다 계산 효율성이 높은 대칭 암호화 알고리즘입니다. AES는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다.
- DES - 56비트 키를 사용하여 암호화를 수행하는 DES(Data Encryption Standard)는 대칭 보안 키 블록 알고리즘입니다. 라이선스 어카운트가 내보내기 제어에 대한 요건을 충족하지 않는 경우에는 이 옵션이 유일한 옵션입니다. 3DES보다 속도가 빠르며 시스템 리소스를 더 적게 사용하지만 보안성은 더 낮습니다. 강력한 데이터 기밀 유지 기능이 필요하지 않으며 시스템 리소스나 속도가 중요한 경우에는 DES를 선택하십시오.
- 3DES - 56비트 키를 사용하여 암호화를 3회 수행하는 3DES(Triple DES)는 서로 다른 키를 사용하여 각 데이터 블록을 3회 처리하므로 DES보다 안전합니다. 그러나 시스템 리소스를 더 많이 사용하며 DES보다 속도가 느립니다.
- NULL - null 암호화 알고리즘은 암호화를 수행하지 않는 인증 기능을 제공합니다. 이 알고리즘은 대개 테스트용으로만 사용됩니다.

### 사용할 해시 알고리즘 결정

IKE 정책에서 해시 알고리즘은 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성합니다. IKEv2에서 해시 알고리즘은 두 가지 옵션으로 구분됩니다. 그중 하나는 무결성 알고리즘 옵션이고 다른 하나는 PRF(Pseudo-Random Function: 의사 난수 함수) 옵션입니다.

IPsec 제안에서 해시 알고리즘은 인증을 위한 ESP(Encapsulating Security Protocol)에서 사용됩니다. IKEv2 IPsec 제안에서는 이러한 알고리즘을 무결성 해시라고 합니다. IKEv1 IPsec 제안에서는 알고리즘 이름에 ESP- 접두사가 붙으며 -HMAC(Hash Method Authentication Code) 접미사도 붙습니다.

IKEv2의 경우 여러 해시 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

다음 해시 알고리즘 중에서 선택할 수 있습니다.

- SHA(Secure Hash Algorithm) - 표준 SHA(SHA-1)에서는 160비트 다이제스트를 생성합니다. SHA는 MD5보다 무차별 암호 대입 공격에 대한 방어력이 뛰어납니다. 그러나 MD5보다 리소스를 더 많이 사용합니다. 최고 보안 레벨이 필요한 구현의 경우 SHA 해시 알고리즘을 사용합니다.
- IKEv2 컨피그레이션에는 다음과 같은 더욱 안전한 SHA-2 옵션을 사용할 수 있습니다. NSA Suite B 암호화 사양을 구현하려는 경우 이러한 옵션 중 하나를 선택합니다.
  - SHA-256 - 256비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
  - SHA-384 - 384비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
  - SHA-512 - 512비트 다이제스트를 생성하는 Secure Hash Algorithm SHA-2를 지정합니다.
- MD5(Message Digest 5) - 128비트 다이제스트를 생성합니다. MD5는 SHA보다 전반적으로 성능이 우수하여 처리 시간이 짧지만 SHA보다 취약한 것으로 간주됩니다.
- null 또는 None(NULL, ESP-NONE) - (IPsec 제안에만 해당됨) null 해시 알고리즘으로, 대개 테스트용으로만 사용됩니다. 그러나 암호화 알고리즘으로 AES-GCM/GMAC 옵션 중 하나를 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null 이외의 옵션을 선택하더라도 이러한 암호화 표준에 대해서는 무결성 해시가 무시됩니다.

### 사용할 Diffie-Hellman 모듈러스 그룹 결정

다음 Diffie-Hellman 키 파생 알고리즘을 사용하여 IPsec 보안 연계(SA) 키를 생성할 수 있습니다. 각 그룹의 크기 모듈러스는 서로 다릅니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어에 일치하는 모듈러스 그룹이 있어야 합니다.

AES 암호화를 선택하는 경우 AES에 필요한 큰 키를 지원하려면 DH(Diffie-Hellman) 그룹 5 이상을 사용해야 합니다. IKEv1 정책에서는 아래에 나열된 그룹을 모두 지원하지는 않습니다.

NSA Suite B 암호화 사양을 구현하려면 IKEv2를 사용하고 ECDH(Elliptic Curve Diffie-Hellman) 옵션 19, 20, 21 중 하나를 선택합니다. 2048비트 모듈러스를 사용하는 엘립틱 커브 옵션과 그룹은 Logjam과 같은 공격에 노출될 가능성이 작습니다.

IKEv2의 경우에는 여러 그룹을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

- 2 - Diffie-Hellman 그룹 2: 1024비트 MODP(모듈식 지수) 그룹. 이 옵션은 더 이상 좋은 보호 방법으로 간주되지 않습니다.
- 5 - Diffie-Hellman 그룹 5: 1536비트 MODP 그룹. 전에는 이 옵션이 128비트 키에 대해 좋은 보호 방법으로 간주되었지만 이제는 더 이상 좋은 보호 방법으로 간주되지 않습니다.
- 14 - Diffie-Hellman 그룹 14: 2048비트 MODP(모듈식 지수) 그룹. 192비트 키에 적합한 보호를 제공합니다.
- 19 - Diffie-Hellman 그룹 19: NIST(국내 표준 및 기술) 256비트 ECP(elliptic curve modulo a prime) 그룹
- 20 - Diffie-Hellman 그룹 20: NIST 384비트 ECP 그룹
- 21 - Diffie-Hellman 그룹 21: NIST 521비트 ECP 그룹
- 24 - Diffie-Hellman 그룹 24: 2048비트 MODP 그룹 및 256비트 소수 위수 하위 그룹. 이 옵션은 더 이상 권장되지 않습니다.

#### 사용할 인증 방법 결정

다음과 같은 방법을 사용하여 사이트 간 VPN 연결에서 피어를 인증할 수 있습니다.

#### 사전 공유 키

사전 공유 키는 연결에서 각 피어에 컨피그레이션된 암호 키 문자열입니다. 이 키는 인증 단계 중에 IKE에서 사용됩니다. IKEv1의 경우, 각 피어에서 동일한 사전 공유 키를 컨피그레이션해야 합니다. IKEv2의 경우, 각 피어에 고유 키를 컨피그레이션할 수 있습니다.

사전 공유 키는 인증서에 비해 확장성이 떨어집니다. 다수의 Site-to-Site VPN 연결을 컨피그레이션해야 하는 경우, 사전 공유 키 방법 대신 인증서 방법을 사용하십시오.

#### NAT에서 사이트 간 VPN 트래픽 제외

인터페이스에 사이트 대 사이트 VPN 연결이 정의되어 있고 해당 인터페이스에 대한 NAT 규칙도 있는 경우 NAT 규칙에서 VPN의 트래픽을 선택적으로 제외할 수 있습니다. VPN 연결의 원격 쪽에서 내부 주소를 처리할 수 있는 경우 이러한 VPN 트래픽을 제외할 수 있습니다.

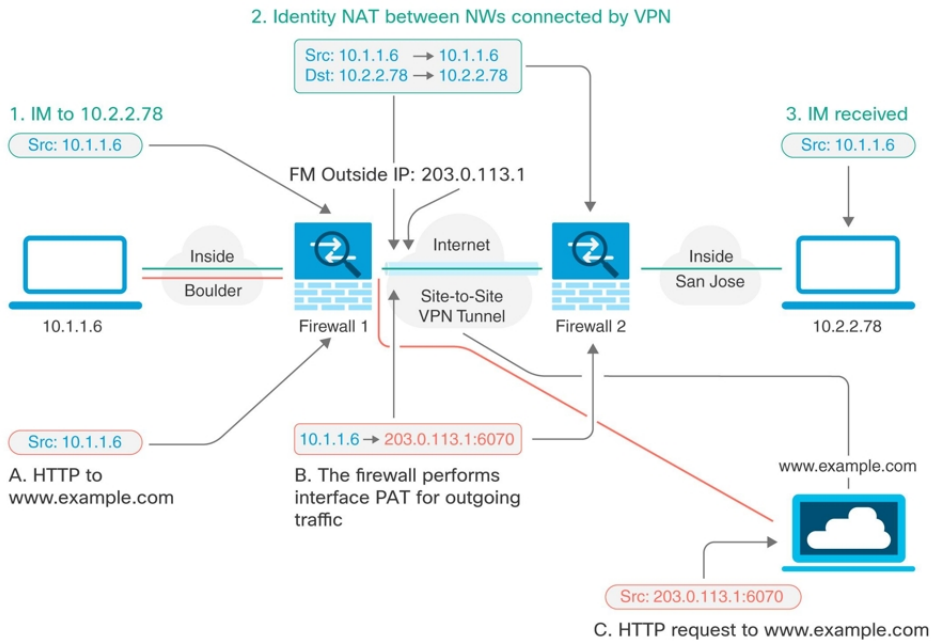
VPN 연결을 생성할 때 **NAT Exempt(NAT 제외)** 옵션을 선택하여 규칙을 자동으로 생성할 수 있습니다. 그러나 브리지 그룹 멤버가 아닌 단일 라우팅 인터페이스를 통해 보호된 로컬 네트워크에 연결하는 경우에만 이 방법을 사용할 수 있습니다. 그렇지 않고 연결의 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 멤버에 있는 경우에는 NAT 제외 규칙을 수동으로 구성해야 합니다.

NAT 규칙에서 VPN 트래픽을 제외하려면 대상이 원격 네트워크일 때 로컬 트래픽에 대한 ID 수동 NAT 규칙을 생성합니다. 그런 다음 대상이 인터넷 등의 다른 항목일 때 트래픽에 NAT를 적용합니

다. 로컬 네트워크의 인터페이스가 여러 개인 경우 각 인터페이스에 대해 규칙을 생성합니다. 또한 다음과 같은 제안 사항을 고려합니다.

- 연결에 로컬 네트워크가 여러 개 있으면 네트워크를 정의하는 개체를 포함할 네트워크 개체 그룹을 생성합니다.
- VPN에 IPv4 및 IPv6 네트워크를 둘 다 포함하는 경우 각 네트워크에 대해 별도의 ID NAT 규칙을 생성합니다.

볼더 사무실과 산호세 사무실을 연결하는 사이트 대 사이트 터널을 보여주는 다음 예를 살펴보십시오. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래 예에서는 인터페이스 PAT(Port Address Translation) 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: 볼더의 10.1.1.6에서 산호세의 10.2.2.78로)에 대해서는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 ID NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. ID NAT는 주소를 동일한 주소로 변환합니다.



다음 예에서는 방화벽1(볼더)의 컨피그레이션에 대해 설명합니다. 이 예에서는 내부 인터페이스가 브리지 그룹이라고 가정하므로 각 멤버 인터페이스에 대해 규칙을 작성해야 합니다. 라우팅 내부 인터페이스가 하나이든 여러 개이든 프로세스는 동일합니다.




**Note** 이 예에서는 IPv4만 사용한다고 가정합니다. VPN에 IPv6 네트워크도 포함되어 있으면 IPv6용 병렬 규칙을 생성합니다. IPv6 인터페이스 PAT를 구현할 수는 없으므로 PAT에 사용할 고유 IPv6 주소가 포함된 호스트 개체를 생성해야 합니다.




## Procedure

단계 1 여러 네트워크를 정의하기 위한 개체를 생성합니다.

- a. 좌측의 CDO 내비게이션 바에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- b. 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.
- c. **FTD > Network(네트워크)**를 클릭합니다.
- d. 볼더 내부 네트워크를 확인합니다.
- e. 개체 이름을 입력합니다(예: boulder-network).
- f. **Create a network object(네트워크 개체 생성)**를 선택합니다.
- g. Value(값) 섹션에서 다음을 수행합니다.
  - eq를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
  - 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력

합니다.

- h. **Add(추가)**를 클릭합니다.
- i. 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.
- j. 내부 산호세 네트워크를 정의합니다.
- k. 개체 이름(예: san-jose)을 입력합니다.
- l. **Create a network object(네트워크 개체 생성)**를 선택합니다.
- m. Value(값) 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소 또는 CIDR 표기법으로 표시된 서브넷 주소를 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다. 예를 들어 네트워크 주소를 10.1.1.0/24로 입력

The screenshot shows a web interface for adding a network object. The title is "Adding FTD Network Object". There are three main sections: "Object Name" with the value "sanjose-network", "Description" with the value "Object description", and "Value" with a dropdown menu set to "eq" and a text input field containing "10.2.2.0/24". Below these fields are two radio buttons: "Create a network group" (unselected) and "Create a network object" (selected).

합니다.


- n. **Add**(추가)를 클릭합니다.

단계 2 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

- a. CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- b. 필터를 사용하여 NAT 규칙을 생성할 디바이스를 찾습니다.
- c. 상세정보 패널의 Management(관리) 영역에서 **NAT** > **NAT**를 클릭합니다.
- d. **+ > 2회 NAT**를 클릭합니다.
  - 섹션 1에서 **Static**(정적)을 선택합니다. **Continue**(계속)를 클릭합니다.
  - 섹션 2에서 **Source Interface**(소스 인터페이스) = **inside**(내부) 및 **Destination Interface**(대상 인터페이스) = **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.
  - 섹션 3에서 **Source Original Address**(소스 원본 주소) = 'boulder-network' 및 **Source Translated Address**(소스 변환 주소) = 'boulder-network'를 선택합니다.
  - **Use Destination**(대상 사용)을 선택합니다.
  - **Destination Original Address**(대상 원본 주소) = 'sanjose-network' 및 **Source Translated Address**(소스 변환 주소) = 'sanjose-network'를 선택합니다. 참고: 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에

대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다. 이 규칙은 소스 및 대상 둘다에 대해 ID NAT를 구성합니다.

FTD: FTD\_BGL\_972 / NAT Rules



Type: **Static**


Interfaces: Source Interface: **inside**, Destination Interface: **outside**

Packets: **Source** Original Address: **boulder-network**, Translated Address: **boulder-network**  
 Use Destination  
**Destination** Original Address: **sanjose-network**, Translated Address: **sanjose-network**  
 Use Service Objects

Advanced:  Disable proxy ARP for incoming packets  
 Use route lookup to determine the egress interface

- **Disable proxy ARP for Incoming packet**(수신 패킷에 대해 프록시 ARP 비활성화)을 선택합니다.
- **Save**(저장)를 클릭합니다.
- 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

**단계 3** 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다. 참고: 모든 IPv4 트래픽에 적용되는 내부 인터페이스용 동적 인터페이스 PAT 규칙은 이미 있을 수 있습니다. 이러한 규칙은 초기 구성 중에 기본적으로 생성되기 때문입니다. 그러나 여기서는 완전한 설명을 위해 컨피그레이션을 제공합니다. 이러한 단계를 완료하기 전에 내부 인터페이스와 네트워크에 적용되는 규칙이 이미 있는지 확인하고 해당 규칙이 있으면 이 단계를 건너뛸니다.

-  > 2회 NAT를 클릭합니다.
- 섹션 1에서 **Dynamic**(동적)을 선택합니다. **Continue**(계속)를 클릭합니다.
- 섹션 2에서 **Source Interface**(소스 인터페이스) = **inside**(내부) 및 **Destination Interface**(대상 인터페이스) = **outside**(외부)를 선택합니다. **Continue**(계속)를 클릭합니다.

- d. 섹션 3에서 **Source Original Address**(소스 원본 주소) = 'boulder-network' 및 **Source Translated Address**(소스 변환 주소) = 'interface'를 선택합니다.

FTD: FTD\_BGL\_972 / NAT Rules

Cancel Save

Type: **Dynamic**

Interfaces: Source Interface: **inside**, Destination Interface: **outside**

Packets: Source Original Address: **boulder-network**, Translated Address: **interface**

Use Destination  
 Use Service Objects

- e. **Save**(저장)를 클릭합니다.
- f. 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 4 CDO에 구성 변경 사항을 구축합니다. 자세한 내용은 [CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축](#)을 참조하십시오.

단계 5 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 boulder-network일 때는 sanjose-network용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 sanjose-network용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

## 글로벌 IKE 정책 구성

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선 순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높

습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 Edit(수정)을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

다음 항목에서는 각 버전에 대해 IKE 정책을 구성하는 방법에 대해 설명합니다.

- [IKEv1 정책 관리](#)

- [IKEv2 정책 관리](#)

## IKEv1 정책 관리

IKEv1 정책을 생성하고 편집하는 방법을 설명합니다.

### IKEv1 정책 정보

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

### Related Topics

[IKEv1 정책 생성 또는 편집](#), 479 페이지


### IKEv1 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy**(새 IKE 정책 생성) 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv1 정책을 생성할 수도 있습니다.

### Procedure

**단계 1** 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

**단계 2** 다음 중 하나를 수행합니다.

- **파란색 더하기  버튼을 클릭하고 FDM > IKEv1 Policy(IKEv1 정책)를 선택하여 새 IKEv1 정책을 생성합니다.**
- **개체 페이지에서 편집할 IKEv1 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit(편집)**를 클릭합니다.**

단계 3 개체 이름을 최대 128자로 입력합니다.

단계 4 IKEv1 속성을 구성합니다.

- **Priority(우선순위)**—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에서 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Encryption(암호화)** - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.
- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Lifetime(라이프타임)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.
- **Authentication(인증)** - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 [사용할 인증 방법 결정](#)을 참조하십시오.
  - **Preshared Key(사전 공유 키)** - 각 디바이스에 정의된 사전 공유 키를 사용합니다. 이 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.
  - **Certificate(인증서)** - 서로 식별할 피어에 대해 디바이스 ID 인증서를 사용합니다. Certificate Authority에서 각 피어를 등록하여 이 인증서를 가져와야 합니다. 또한 각 피어에서 ID 인증서 서명에 사용되는 신뢰할 수 있는 CA 루트 및 중간 CA 인증서를 업로드해야 합니다. 피어는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.
- **Hash(해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 [사용할 Diffie-Hellman 모듈러스 그룹 결정](#)을 참조하십시오.

단계 5 Add(추가)를 클릭합니다.

## IKEv2 정책 관리

IKEv2 정책을 생성하고 편집하는 방법을 설명합니다.

## IKEv2 정책 정보

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

## Related Topics

[IKEv2 정책 생성 또는 편집](#), 481 페이지


## IKEv2 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv2 Policy**(새 IKEv2 정책 생성) 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv2 정책을 생성할 수도 있습니다.

## Procedure

**단계 1** 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

**단계 2** 다음 중 하나를 수행합니다.

- 파란색 더하기  버튼을 클릭하고 **FTD > IKEv2 Policy**(IKEv2 정책)를 선택하여 새 IKEv2 정책을 생성합니다.
- 개체 페이지에서 수정할 IKEv2 정책을 선택하고 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

**단계 3** 개체 이름을 최대 128자로 입력합니다.

**단계 4** IKEv2 속성을 구성합니다.

- **Priority**(우선순위)—IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위로 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **State**(상태) - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Encryption**(암호화) - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을 둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는 반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#)을 참조하십시오.

- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 [사용할 Diffie-Hellman 모듈러스 그룹 결정을](#) 참조하십시오.
- **Integrity Hash(무결성 해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정을](#) 참조하십시오.
- **PRF(Pseudo-Random Function) 해시** - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해서도 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정을](#) 참조하십시오.
- **Lifetime(라이프타임)**—SA(보안 연결)의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 5 Add(추가)를 클릭합니다.

## IPsec 제안 구성

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성하여 선택합니다.
- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각



조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.



**Note** IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

- [IKEv1 IPsec 제안 개체 관리](#)
- [IKEv2 IPsec 제안 개체 관리](#)

## IKEv1 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 CDO(Cisco Defense Orchestrator)는 IKEv1 IPsec 제안 개체를 지원합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.



**Note** IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

### Related Topics

[IKEv1 IPsec 제안 개체 생성 또는 편집](#), 483 페이지

### IKEv1 IPsec 제안 개체 생성 또는 편집


여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv1 Proposal**(새 IKEv1 제안 생성) 링크를 클릭하여 사이트 투 사이트 VPN 연결에서 IKEv1 IPsec 설정을 편집하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM > IKEv1 IPsec Proposal**(IKEv1 IPsec 제안)을 선택하여 새 개체를 생성합니다.

- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(편집)**를 클릭합니다.

단계 3 새 개체의 개체 이름을 입력합니다.

단계 4 IKEv1 IPsec 제안 개체가 작동하는 모드를 선택합니다.

- 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPsec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec이 구현되는 통상적인 방식입니다.
- 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPsec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.

단계 5 이 제안에 대한 **ESP Encryption(ESP 암호화)(Encapsulating Security Protocol)** 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#)을 참조하십시오.

단계 6 인증에 사용할 **ESP Hash(ESP 해시)** 또는 무결성 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정](#)을 참조하십시오.

단계 7 **Add(추가)**를 클릭합니다.

## IKEv2 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

### Related Topics

[IKEv2 IPsec 제안 개체 생성 또는 편집](#), 484 페이지

## IKEv2 IPsec 제안 개체 생성 또는 편집


여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IPsec Proposal(새 IPsec 제안 생성)** 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 편집하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

## Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FDM > IKEv2 IPsec Proposal(IKEv2 IPsec 제안)**을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(편집)**를 클릭합니다.

단계 3 새 개체의 개체 이름을 입력합니다.

단계 4 IKE2 IPsec 제안 개체 구성:

- **Encryption(암호화)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#)을 참조하십시오.
- **Integrity Hash(무결성 해시)** - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정](#)을 참조하십시오.

단계 5 **Add(추가)**를 클릭합니다.

## FDM-관리디바이스 사이트 간 가상 사설망 모니터링

CDO를 사용하면 온보딩된 FDM 관리 디바이스에서 기존 또는 새로 생성된 사이트 간 VPN 구성을 모니터링, 수정 및 삭제할 수 있습니다.

사이트 투 사이트 **VPN** 터널 연결 확인

**Check Connectivity(연결 확인)** 버튼을 사용하여 터널에 대한 실시간 연결 확인을 트리거하여 터널이 현재 **사이트 간 VPN 터널 검색 및 필터링**인지를 식별합니다. 온디맨드 연결 확인 버튼을 클릭하지 않으면 온보딩된 모든 디바이스에서 사용 가능한 모든 터널의 확인이 1시간에 한 번 수행됩니다.



### Note

- CDO는 FTD에서 이 연결성 검사 명령을 실행하여 터널이 활성 상태인지 유효 상태인지를 확인합니다.  

```
show vpn-sessiondb 121 sort ipaddress
```
- 모델 ASA 디바이스 터널은 항상 유효로 표시됩니다.

VPN 페이지에서 터널 연결을 확인하려면 다음을 수행합니다.

## Procedure

- 
- 단계 1 기본 탐색 모음에서 VPN > ASA/FDM Site-to-Site VPN를 클릭합니다.
- 단계 2 사이트 투 사이트 VPN 터널에 대한 터널 목록을 [사이트 간 VPN 터널 검색 및 필터링](#)하고 선택합니다.
- 단계 3 오른쪽의 작업 창에서 **Check Connectivity**(연결 확인)를 클릭합니다.
- 

## VPN 문제 식별



CDO는 FTD에서 VPN 문제를 식별할 수 있습니다. (이 기능은 아직 AWS VPC 사이트 투 사이트 VPN 터널에 사용할 수 없습니다.) 이 문서에서는 다음을 설명합니다.

- 누락된 피어가 있는 VPN 터널 찾기
  - 암호화 키 문제가 있는 VPN 피어 찾기
  - 터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기
  - 터널 구성에서 문제 찾기
- 터널 구성 문제 해결, [on page 488](#)

### 누락된 피어가 있는 VPN 터널 찾기

"Missing IP Peer" 상태는 FDM 관리 디바이스보다 ASA 디바이스에서 발생할 가능성이 높습니다.

## Procedure



- 
- 단계 1 CDO 탐색 창에서 VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)을 클릭하여 VPN 페이지를 엽니다.
- 단계 2 **Table View**(테이블 보기)를 선택합니다.
- 단계 3 필터 아이콘 을 클릭하여 필터 패널을 엽니다.
- 단계 4 감지된 문제를 확인합니다.
- 단계 5 문제 를 보고하는 각 디바이스를 선택하고 오른쪽의 Peers(피어) 창을 확인합니다. 하나의 피어 이름이 나열됩니다. CDO는 다른 피어 이름을 "[Missing peer IP.]"로 보고합니다.
- 

### 암호화 키 문제가 있는 VPN 피어 찾기

이 접근 방식을 사용하여 다음과 같은 암호화 키 문제가 있는 VPN 피어를 찾습니다.

- IKEv1 또는 IKEv2 키가 잘못되었거나 누락되었거나 일치하지 않습니다.
- 사용되지 않거나 낮은 암호화 터널



## Procedure

- 단계 1 CDO 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 클릭하여 VPN 페이지를 엽니다.
- 단계 2 **Table View**(테이블 보기)를 선택합니다.
- 단계 3 필터 아이콘 을 클릭하여 필터 패널을 엽니다.
- 단계 4 문제 를 보고하는 각 디바이스를 선택하고 오른쪽의 **Peers(피어)** 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.
- 단계 5 디바이스 중 하나에 대해 **View Peers(피어 보기)**를 클릭합니다.
- 단계 6 **Diagram View**(다이어그램 보기)에서 문제를 보고하는 디바이스를 두 번 클릭합니다.
- 단계 7 하단의 **Tunnel Details(터널 세부 정보)** 창에서 **Key Exchange(키 교환)**를 클릭합니다. 두 디바이스를 모두 보고 해당 지점에서 주요 문제를 진단할 수 있습니다.

### 터널에 대해 정의된 불완전하거나 잘못 구성된 액세스 목록 찾기

"불완전하거나 잘못 구성된 액세스 목록" 상태는 ASA 디바이스에서만 발생할 수 있습니다.

## Procedure





- 단계 1 CDO 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 클릭하여 VPN 페이지를 엽니다.
- 단계 2 **Table View**(테이블 보기)를 선택합니다.
- 단계 3 필터 아이콘 을 클릭하여 필터 패널을 엽니다.
- 단계 4 문제 를 보고하는 각 디바이스를 선택하고 오른쪽의 **Peers(피어)** 창을 확인합니다. 피어 정보에는 두 피어가 모두 표시됩니다.
- 단계 5 디바이스 중 하나에 대해 **View Peers(피어 보기)**를 클릭합니다.
- 단계 6 **Diagram View**(다이어그램 보기)에서 문제를 보고하는 디바이스를 두 번 클릭합니다.
- 단계 7 하단의 **Tunnel Details(터널 세부 정보)** 패널에서 **Tunnel Details(터널 세부 정보)**를 클릭합니다. "Network Policy: Incomplete(네트워크 정책: 완료되지 않음)" 메시지가 표시됩니다.

### 터널 구성에서 문제 찾기

터널 구성 오류는 다음 시나리오에서 발생할 수 있습니다.

- 사이트 투 사이트 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.

## Procedure

- 단계 1 CDO 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 클릭하여 VPN 페이지를 엽니다.
- 단계 2 **Table View**(테이블 보기)를 선택합니다.
- 단계 3 필터 아이콘 을 클릭하여 필터 패널을 엽니다.
- 단계 4 터널 문제에서 탐지된 문제를 클릭하여 오류를 보고하는 VPN 구성을 봅니다. 구성 보고 문제 를 볼 수 있습니다.
- 단계 5 VPN 구성 보고 문제를 선택합니다.
- 단계 6 오른쪽의 피어 창에 문제가 있는 피어에 대한  아이콘이 나타납니다.  아이콘 위로 마우스를 가져 가면 문제와 해결 방법을 볼 수 있습니다.

다음 단계: [터널 구성 문제 해결](#).

## 터널 구성 문제 해결

이 절차는 다음과 같은 터널 구성 문제를 해결하려고 시도합니다.

- 사이트 투 사이트 VPN 인터페이스의 IP 주소가 변경되면 "피어 IP 주소 값이 변경되었습니다."
- VPN 터널의 IKE 값이 다른 VPN 터널과 일치하지 않으면 "IKE 값 불일치" 메시지가 나타납니다.

자세한 내용은 [터널 구성에서 문제 찾기](#)를 참조하십시오.


## 프로시저

- 단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 유형 탭을 클릭하고 문제를 보고하는 VPN 구성과 연결된 디바이스를 선택합니다.
- 단계 4 **"충돌 탐지됨" 상태 해결**
- 단계 5 CDO 탐색 창에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 클릭하여 VPN 페이지를 엽니다.
- 단계 6 이 문제를 보고하는 VPN 구성을 선택합니다.
- 단계 7 **Actions**(작업)창에서 **Edit**(편집) 아이콘을 클릭합니다.
- 단계 8 4단계에서 **Finish**(마침) 버튼을 클릭할 때까지 각 단계에서 **Next**(다음)를 클릭합니다.
- 단계 9 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 620 페이지.

## 사이트 간 VPN 터널 검색 및 필터링

필터 사이드바 를 검색 필드와 함께 사용하여 VPN 터널 다이어그램에 표시된 VPN 터널 검색에 집중할 수 있습니다.


### Procedure

- 단계 1 기본 내비게이션 바에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**으로 이동합니다.
- 단계 2 필터 아이콘 을 클릭하여 필터 창을 엽니다.
- 단계 3 다음 필터를 사용하여 검색을 구체화합니다.
  - **Filter by Device**(디바이스별 필터링) - **Filter by Device**(디바이스별 필터링)를 클릭하고 디바이스 유형 탭을 선택한 후 필터링을 통해 찾으려는 디바이스를 선택합니다.
  - **Tunnel Issues**(터널 문제) - 터널의 양쪽에 문제가 있음을 탐지했는지 여부입니다. 디바이스에 문제가 있는 몇 가지 예로는 연결된 인터페이스 또는 피어 IP 주소 또는 액세스 목록 누락, IKEv1 제안 불일치 등이 있습니다(AWS VPC VPN 터널에서는 터널 문제 탐지를 아직 사용할 수 없음).
  - **Devices/Services**(디바이스/서비스) - 디바이스 유형을 기준으로 필터링합니다.
  - **Status**(상태) - 터널 상태는 활성 또는 유휴 상태일 수 있습니다.
    - **Active**(활성) - 네트워크 패킷이 VPN 터널을 통과하는 열린 세션이 있거나 성공적인 세션이 설정되었고 아직 시간 초과되지 않았습니다. **Active**(활성)는 터널이 활성 상태이고 관련성이 있음을 나타내는 데 도움이 될 수 있습니다.
    - **Idle**(유휴) - CDO가 이 터널에 대한 열린 세션을 검색할 수 없습니다. 터널이 사용 중이 아니거나 이 터널에 문제가 있을 수 있습니다.
  - **Onboarded**(온보딩됨) - CDO에서 디바이스를 관리하거나 CDO에서 관리하지 않을 수 있습니다 (관리되지 않음).
    - 관리됨 - CDO가 관리하는 디바이스별로 필터링합니다.
    - 관리되지 않음 - CDO가 관리하지 않는 디바이스로 필터링합니다.
  - **Device Types**(디바이스 유형) - 터널의 한쪽이 라이브(연결된 디바이스) 디바이스인지 아니면 모델 디바이스인지 여부입니다.
- 단계 4 검색 창에 디바이스 이름 또는 IP 주소를 입력하여 필터링된 결과를 검색할 수도 있습니다. 검색은 대/소문자를 구분하지 않습니다.

## 관리되지 않는 디바이스 온보딩

CDO는 피어 중 하나가 온보딩될 때 사이트 간 VPN 터널을 검색 합니다. 두 번째 피어가 CDO에서 관리되지 않는 경우 VPN 터널 목록을 필터링하여 관리되지 않는 디바이스를 찾아 온보딩할 수 있습니다.

### Procedure

- 단계 1 기본 내비게이션 바에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**을 선택하여 VPN 페이지를 엽니다.
- 단계 2 **Table View**(테이블 보기)를 선택합니다.
- 단계 3 를 클릭하여 필터 패널을 엽니다.
- 단계 4 **Unmanaged**(관리되지 않음)를 선택합니다.
- 단계 5 결과의 테이블에서 터널을 선택합니다.
- 단계 6 오른쪽의 **Peers**(피어) 창에서 **Onboard Device**(온보드 디바이스)를 클릭하고 화면의 지침을 따릅니다.

### 관련 정보:

- [디바이스 및 서비스 온보딩, on page 175](#)
- [위협 방어 디바이스 온보딩, on page 175](#)

## 사이트 투 사이트 VPN 터널의 IKE 개체 세부 정보 보기

선택한 터널의 피어/디바이스에 구성된 IKE 개체의 세부 정보를 볼 수 있습니다. 이러한 세부 정보는 IKE 정책 개체의 우선 순위에 따라 계층 구조의 트리 구조로 나타납니다.



**Note** 엑스트라넷 디바이스는 IKE 개체 세부 정보를 표시하지 않습니다.

### Procedure

- 단계 1 왼쪽의 CDO 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN(ASA/FDM 사이트 간 VPN)**를 클릭합니다.
- 단계 2 **VPN Tunnels**(VPN 터널) 페이지에서 피어를 연결하는 VPN 터널의 이름을 클릭합니다.
- 단계 3 오른쪽의 **Relationships**(관계) 아래에 세부 정보를 보려는 개체를 확장합니다.



마지막으로 성공한 사이트 투 사이트 VPN 터널 설정 날짜 보기

### Procedure

- 단계 1 [사이트 간 VPN 터널 정보 보기](#).
- 단계 2 **Tunnel Details**(터널 세부 정보) 창을 클릭합니다.
- 단계 3 **Last Seen Active**(마지막 확인한 활성) 필드를 확인합니다.

사이트 간 VPN 터널 정보 보기

사이트 간 VPN 테이블 보기는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 사이트 간 VPN 터널의 전체 목록입니다. 터널은 이 목록에 한 번만 존재합니다. 테이블에 나열된 터널을 클릭하면 추가 조사를 위해 터널의 피어로 직접 이동할 수 있는 옵션이 오른쪽 사이드바에 제공됩니다.

CDO가 터널의 양쪽을 모두 관리하지 않는 경우 [관리되지 않는 디바이스 온보딩](#)을 클릭하여 언매니지드 피어의 온보드 기본 온보딩 페이지를 열 수 있습니다. CDO가 터널의 양쪽을 모두 관리하는 경우 Peer 2(피어 2) 옆에 매니지드 디바이스의 이름이 포함됩니다. 그러나 AWS VPC의 경우 Peer 2 옆에 VPN 게이트웨이의 IP 주소가 포함됩니다.

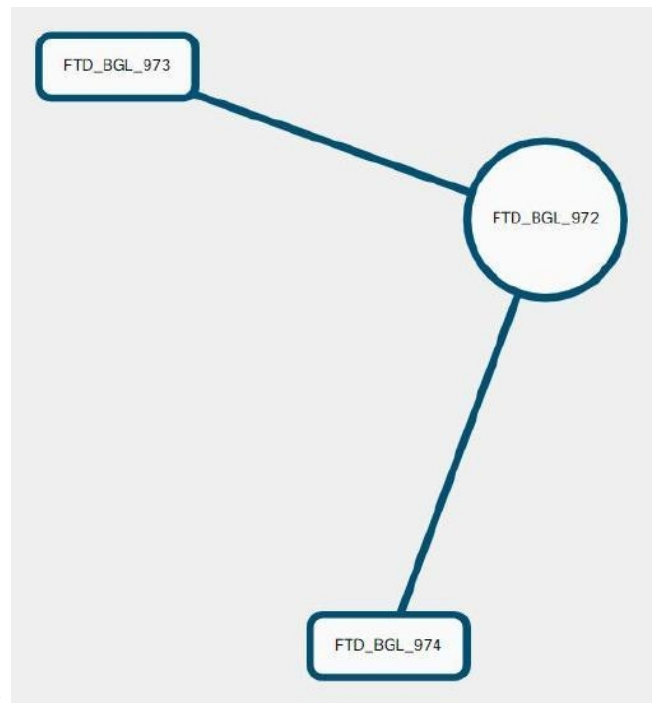
테이블 보기에서 사이트 간 VPN 연결을 보려면 다음을 수행합니다.

### Procedure

- 단계 1 기본 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN**를 클릭합니다.
- 단계 2 **Table view**(테이블 보기) 버튼을 클릭합니다.
- 단계 3 [사이트 간 VPN 터널 검색 및 필터링](#)를 사용하여 특정 터널을 찾거나 전역 보기 그래픽을 확대하여 원하는 VPN 게이트웨이 및 해당 피어를 찾습니다.

## 사이트 투 사이트 VPN 전역 보기

다음은 전역 보기의 예입니다. 그림에서 'FTD\_BGL\_972'에는 FTD\_BGL\_973 및 FTD\_BGL\_974 디바



이스와의 사이트 투 사이트 연결이 있습니다.

### Procedure

- 단계 1 기본 탐색 모음에서 **VPN > ASA/FDM Site-to-Site VPN**를 클릭합니다.
- 단계 2 **Global view**(전역 보기) 버튼을 클릭합니다.
- 단계 3 **사이트 간 VPN 터널 검색 및 필터링**를 사용하여 특정 터널을 찾거나 전역 보기 그래픽을 확대하여 원하는 VPN 게이트웨이 및 해당 피어를 찾습니다.
- 단계 4 전역 보기에 표시된 피어 중 하나를 선택합니다.
- 단계 5 **View Details**(세부사항 보기)를 클릭합니다.
- 단계 6 VPN 터널의 다른 쪽 끝을 클릭하면 CDO에 해당 연결에 대한 **Tunnel Details**(터널 세부 정보), **NAT Information**(NAT 정보) 및 **Key Exchange**(키 교환) 정보가 표시됩니다.
  - **Tunnel Details**(터널 세부 정보) - 터널에 대한 이름 및 연결 정보를 표시합니다. **Refresh**(새로 고침) 아이콘을 클릭하면 터널에 대한 연결 정보가 업데이트됩니다.
  - **Tunnel Details specific to AWS connections**(AWS 연결 관련 터널 세부 정보) - AWS 사이트 투 사이트 연결에 대한 터널 세부 정보는 다른 연결과 약간 다릅니다. AWS VPC에서 VPN 게이트웨이의 각 연결에 대해 AWS는 2개의 VPN 터널을 생성합니다. 이는고가용성을 위한 것입니다.
    - 터널의 이름은 VPN 게이트웨이가 연결된 VPC의 이름을 나타냅니다. 터널에 이름이 지정된 IP 주소는 VPN 게이트웨이가 VPC로 인식하는 IP 주소입니다.

- CDO 연결 상태가 "active(활성)"로 표시되면 AWS 터널 상태가 "Up(가동 중)"입니다. CDO 연결 상태가 "inactive(비활성)"인 경우 AWS 터널 상태는 "Down(중단)"입니다.
- **NAT Information(NAT 정보)** - 사용 중인 NAT 규칙의 유형, 원래 및 변환된 패킷 정보를 표시하고, 해당 터널에 대한 NAT 규칙을 볼 수 있는 NAT 테이블에 대한 링크를 제공합니다. (AWS VPC 사이트 투 사이트 VPN에는 아직 사용할 수 없습니다.)
- **Key Exchange(키 교환)** - 터널 및 키 교환 문제에서 사용 중인 암호화 키를 표시합니다. (AWS VPC 사이트 투 사이트 VPN에는 아직 사용할 수 없습니다.)

## 터널 창

Tunnels(터널) 창에는 특정 VPN 게이트웨이와 연결된 모든 터널의 목록이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 사이트 간 VPN 연결의 경우, tunnels(터널) 창에는 VPN 게이트웨이에서 VPC로의 모든 터널이 표시됩니다. VPN 게이트웨이와 AWS VPC 간의 각 사이트 간 VPN 연결에는 2개의 터널이 있으므로 다른 디바이스에 대해 일반적으로 표시되는 터널 수가 두 배입니다.

### VPN 게이트웨이 세부 정보

VPN 게이트웨이에 연결된 피어의 수 및 VPN 게이트웨이의 IP 주소를 표시합니다. 이는 VPN Tunnels(VPN 터널) 페이지에만 표시됩니다.

### 피어 창

사이트 간 VPN 피어 쌍을 선택하면 Peers(피어) 창에 쌍의 두 디바이스가 나열되며 디바이스 중 하나에 대해 **View Peers(피어 보기)**를 클릭할 수 있습니다. **View Peers(피어 보기)**를 클릭하면 디바이스가 연결된 다른 사이트 간 피어가 표시됩니다. 이는 Table(테이블) 보기 및 Global(전역) 보기에 표시됩니다.

## 원격 액세스 가상 프라이빗 네트워크

RA VPN(원격 액세스 VPN)을 사용하면 개별 사용자가 인터넷에 연결된 컴퓨터 또는 기타 지원되는 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 따라서 모바일 근무자가 홈 네트워크 또는 공개 Wi-Fi 네트워크 등에서 연결할 수 있습니다.

RA VPN 구성은 다음 구성 요소로 구성됩니다.

- **연결 프로파일:** 홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있도록 원격 액세스 VPN 연결 프로파일을 생성할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다. 연결 프로파일은 ID 소스와 그룹 정책으로 구성됩니다.

### 관련 정보:

- [FTD에 대한 원격 액세스 VPN 구성](#)

## 원격 액세스 가상 프라이빗 네트워크 세션

RA VPN(Remote Access Virtual Private Network)은 모바일 사용자 또는 재택 근무자와 같은 원격 사용자에게 보안 연결을 제공합니다. 이러한 연결을 모니터링하면 연결 및 사용자 세션 성능에 대한 중요한 지표를 얻을 수 있습니다. Cisco Defense Orchestrator (CDO) RA VPN 모니터링 기능을 통해 원격 액세스 VPN 문제가 있는지 여부와 존재 여부를 신속하게 확인할 수 있습니다. 그런 다음 이 정보를 적용하고 네트워크 관리 도구를 사용하여 네트워크 및 사용자의 문제를 줄이거나 없앨 수 있습니다. 필요에 따라 원격 액세스 VPN 세션의 연결을 끊을 수도 있습니다.


Remote Access Virtual Private Monitoring(원격 액세스 가상 프라이빗 모니터링) 페이지는 다음 정보를 제공합니다.

- 지난 90일 동안의 활성 세션 및 기록 세션 목록입니다.
- CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 직관적인 그래픽 시각적 개체를 표시합니다.
- 라이브 세션 화면에는 CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 VPN 연결 프로파일이 표시됩니다. 또한 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- 디바이스 유형, 디바이스 이름, 세션 길이, 전송 및 수신된 데이터의 양과 같은 기준을 기반으로 검색 범위를 좁힐 수 있는 필터링 기능입니다.

관련 정보:

- [라이브 AnyConnect 원격 액세스 VPN 세션 모니터링, on page 494](#)
- [기록 AnyConnect RA VPN 세션 모니터링, on page 496](#)
- [RA VPN 세션 검색 및 필터링](#)
- [RA VPN 모니터링 보기 사용자 지정](#)
- [RA VPN 세션을 CSV 파일로 내보내기](#)
- [FDM-관리 디바이스에서 활성 RA VPN 세션 연결 끊기](#)

### 라이브 AnyConnect 원격 액세스 VPN 세션 모니터링


디바이스의 활성 AnyConnect RA VPN 세션에서 실시간 데이터를 모니터링할 수 있습니다. 이 데이터는 10분마다 자동으로 새로 고쳐집니다. 언제든지 최신 세션 목록을 검색하려면 화면 오른쪽 모서리에 나타나는 다시 로드 아이콘  을 클릭하십시오.

시작하기 전에

- RA VPN 헤드 엔드를 CDO에 온보딩합니다.
- 라이브 데이터를 모니터링하려는 디바이스의 연결 상태는 **Inventory**(인벤토리) 페이지에서 "Online(온라인)"인지 확인합니다.

## 프로시저

단계 1 CDO 탐색 창에서 **VPN > Remote Access VPN Monitoring(VPN 원격 액세스 VPN 모니터링)**을 클릭합니다.

또는 CDO 홈 페이지에서 **View Active Remote Access VPN Sessions(활성 원격 액세스 VPN 세션 보기)**를 클릭하거나 **VPN > Remote Access VPN(원격 액세스 VPN)**으로 이동하여 화면 오른쪽 상단 모서리에 있는  아이콘을 클릭할 수 있습니다.

단계 2 **RA VPN**을 클릭합니다.

단계 3 **Live(라이브)**를 클릭합니다.

**RA VPN 세션 검색 및 필터링**하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.

참고 데이터 **TX** 및 데이터 **RX** 정보는 FTD에서 사용할 수 없습니다.

## 라이브 데이터 보기

라이브 데이터는 대시보드 및 테이블 형식으로 표시됩니다.

### Dashboard(대시보드) 보기

대시보드를 보려면 화면의 오른쪽 상단 모서리에 나타나는 **Show Charts View(차트 보기 표시)** 아이콘을 클릭해야 합니다.

대시보드는 CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 확인할 수 있도록 제공합니다.

- **Breakdown (All Devices)(애널리틱스 데이터(모든 디바이스))**: 총 라이브 세션 수를 표시합니다. 4개의 호 길이로 구분된 원도표도 표시됩니다. 세션 수가 가장 많은 상위 3개 디바이스의 VPN 세션 비율을 보여줍니다. 나머지 호 길이는 다른 디바이스의 어그리게이션을 나타냅니다.
- CDO 테넌트에서 가장 많이 사용되는 운영 체제 및 연결 프로파일이 표시됩니다.
- 평균 세션 기간과 업로드 및 다운로드한 데이터도 표시됩니다.
- **Active Sessions by Country(국가별 활성 세션)**: RA VPN 헤드엔드에 연결된 사용자 위치의 인터랙티브 히트맵을 표시합니다.
  - 사용자가 연결한 국가는 해당 국가에서 설정된 세션의 상대적 비율에 따라 점점 더 짙은 파란색 음영으로 표시됩니다. 파란색이 어두울수록 해당 국가에서 더 많은 세션이 설정되었음을 의미합니다.
  - 맵의 맨 아래에 있는 범례는 국가의 세션 수와 국가를 표시하는 데 사용되는 파란색 음영 간의 상관관계를 나타내는 척도를 제공합니다.
  - 맵에 마우스 포인터를 올려놓으면 해당 국가의 이름 및 해당 국가에서 설정된 총 활성 사용자 세션 수를 확인할 수 있습니다.

- 테이블 위에 마우스 포인터를 올려놓으면 해당 국가의 위치와 맵의 총 활성 사용자 세션 수를 확인할 수 있습니다.

#### 테이블 형식 보기

데이터를 테이블 형식으로 보려면 화면의 오른쪽 상단 모서리에 있는 **Show Tabular View**(테이블 형식 보기 표시) 아이콘을 클릭합니다.

테이블 형식은 현재 연결된 VPN 사용자의 전체 목록을 제공합니다.

- **Location**(위치) 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.



**중요** CDO는 라이브 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 사용자 지정 필터는 시각적 대시보드 보기에서 지원되지 않으므로, 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 적용한 모든 필터를 제거하려면 **Clear**(지우기)를 클릭합니다. 표준 필터는 제거할 수 없습니다.

**RA VPN 세션 검색 및 필터링** 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

**Status**(상태) 열에 **Active**(활성) 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.

### 기록 AnyConnect RA VPN 세션 모니터링


지난 3개월 동안 기록된 AnyConnect RA VPN 세션의 기록 데이터를 모니터링할 수 있습니다.

#### 시작하기 전에

- RA VPN 헤드 엔드를 CDO에 온보딩합니다.

#### 프로시저

**단계 1** CDO 탐색 창에서 **VPN > Remote Access VPN Monitoring**(VPN 원격 액세스 VPN 모니터링)을 클릭합니다.

또는 CDO 홈 페이지에서 **View Active Remote Access VPN Sessions**(활성 원격 액세스 VPN 세션 보기)를 클릭하거나 **VPN > Remote Access VPN**(VPN 원격 액세스 VPN)으로 이동하여 오른쪽 상단 모서리에 있는 아이콘  을 클릭할 수 있습니다.

**단계 2** **RA VPN**을 클릭합니다.

**단계 3** **Historical**(기록)을 클릭합니다.

CDO는 지난 3개월 동안 기록된 RA VPN 세션의 기록 데이터를 표시합니다.

**RA VPN 세션 검색 및 필터링** 기능을 사용하여 디바이스 유형, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다.

데이터 **TX** 및 데이터 **RX** 정보는 FTD에서 사용할 수 없습니다.

## 이력 데이터 보기

이력 데이터는 대시보드 및 표 형식으로 표시됩니다.

### Dashboard(대시보드) 보기

대시보드를 보려면 화면의 오른쪽 상단에 나타나는 **Show Charts View**(차트 보기 표시) 아이콘을 클릭해야 합니다. 테이블 보기와 함께 대시보드 보기가 표시됩니다.

대시보드는 CDO에서 관리하는 모든 활성 VPN 헤드엔드의 보기를 한눈에 볼 수 있도록 제공합니다. 지난 24시간, 7일 및 30일 동안 모든 디바이스에 대해 기록된 VPN 세션을 보여주는 막대 그래프를 제공합니다. 드롭다운에서 기간을 선택할 수 있습니다. 개별 막대에 마우스 커서를 대면 해당 날짜의 총 세션 수와 날짜를 확인할 수 있습니다.

### 테이블 형식 보기

대시보드를 보려면 화면의 오른쪽 상단에 나타나는 **Show Tabular View**(테이블 형식 보기 표시) 아이콘을 클릭하여 테이블 형식 보기만 표시해야 합니다. 테이블 형식은 지난 3개월 동안 연결된 VPN 사용자의 전체 목록을 제공합니다.

**Location**(위치) 열에는 공용 IP 주소를 지리위치 지정하여 VPN 헤드엔드에 연결된 모든 사용자의 위치가 표시됩니다. 사용자 상세정보를 보려면 행을 클릭합니다. 왼쪽 창의 위치 링크를 클릭하면 사용자의 위치가 Google 맵에 표시됩니다.



**중요** CDO는 기록 데이터에 표준 필터를 적용하고 대시보드에 표시합니다. 대시보드는 맞춤형 필터를 지원하지 않으므로 테이블 형식 데이터가 표시되는 경우에만 새 필터를 적용할 수 있습니다. 새로 적용된 필터를 지우면 대시보드가 다시 실행됩니다. 화면에서 **Clear**(지우기)를 클릭하여 수동으로 적용된 필터를 제거합니다. 표준 필터는 제거할 수 없습니다.

**RA VPN 세션 검색 및 필터링** 기능을 사용하여 세션 날짜와 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위와 같은 기준에 따라 검색 범위를 좁힐 수 있습니다. 한 번에 최대 10,000개의 결과를 표시할 수 있습니다.

**Status**(상태) 열에 **Active**(활성) 레이블이 있는 녹색 점은 활성 VPN 사용자의 세션을 나타냅니다.

## RA VPN 세션 검색 및 필터링

### 검색


검색 창 기능을 사용하여 RA VPN 세션을 찾습니다. 검색 창에 디바이스 이름, IP 주소 또는 일련 번호를 입력하기 시작합니다. 그러면 검색 기준에 맞는 RA VPN 세션이 표시됩니다. 검색은 대/소문자를 구분하지 않습니다.

### 필터

필터 사이드바를 사용하여 세션 시간 범위, 세션 길이, 업로드 및 다운로드 데이터 범위 등의 기준에 따라 RA VPN 세션을 찾습니다. 필터 기능은 라이브 보기와 기록 보기 모두에서 사용할 수 있습니다.

- **Filter by Devices**(디바이스별 필터링): **All Types**(모든 유형) 탭에서 하나 또는 모든 디바이스를 선택하여 선택한 디바이스의 세션을 봅니다. 창은 또한 유형에 따라 디바이스를 분류하고 해당 탭 아래에 표시합니다.
- **Sessions Time Range**(세션 시간 범위)(기록 데이터에만 적용 가능): 지정된 날짜 및 시간 범위의 기록 세션을 표시합니다. 지난 3개월 동안 기록된 데이터를 볼 수 있습니다.
- **Sessions Length**(세션 길이): 지정된 세션의 기간 길이를 기준으로 세션을 표시합니다. 시간 단위(시간, 분 또는 초)를 설정하고 슬라이더를 이동하여 최소 및 최대 기간 길이를 지정합니다. 제공된 필드에 길이를 지정할 수도 있습니다.
- **Upload (TX)**(업로드(TX)): 보안 네트워크에 업로드되거나 전송된 데이터의 지정된 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.
- **Download (RX)**(다운로드(RX)): 보안 네트워크에서 다운로드하거나 수신한 지정된 데이터 양을 기준으로 세션을 표시합니다. 단위(GB, MB 또는 KB)를 설정하고 그에 따라 슬라이더를 이동하여 범위를 선택합니다. 사용 가능한 필드에 값을 지정할 수도 있습니다.

## RA VPN 모니터링 보기 사용자 지정

원하는 보기에 적용되는 열 헤더만 포함하도록 라이브 및 기록 모드에서 RA VPN 모니터링 보기를 편집할 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘  을 클릭하고 원하는 열을 선택하거나 선택 취소합니다.

CDO는 다음에 CDO에 로그인할 때 선택 항목을 기억합니다.


## RA VPN 세션을 CSV 파일로 내보내기

하나 이상의 디바이스의 RA VPN 세션을 쉽표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. Microsoft Excel과 같은 스프레드시트 애플리케이션에서 .csv 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다. 이 정보는 RA VPN 세션을 분석하는 데 도움이 됩니다. 세션을 내보낼 때마다 CDO는 새 .csv 파일을 생성합니다. 생성된 파일에는 이름에 날짜와 시간이 포함되어 있습니다.

CDO는 최대 100,000개의 활성 세션을 CSV 파일로 내보낼 수 있습니다. 모든 디바이스의 총 세션 수가 최대 제한을 초과하는 경우 **View By Device**(디바이스별 보기) 필터를 사용하여 개별 디바이스에 대한 보고서를 생성할 수 있습니다.



## Procedure

- 단계 1 CDO 탐색 창에서 **VPN > Remote Access VPN Monitoring(VPN 원격 액세스 VPN 모니터링)**을 클릭합니다.
- 단계 2 **View By Devices(디바이스별 보기)** 영역에서 다음 중 하나를 선택합니다.
  - **All Devices(모든 디바이스)** - 그 아래에 나열된 모든 디바이스에서 활성 세션을 내보냅니다.
  - 해당 디바이스의 세션을 내보낼 디바이스를 클릭합니다.
- 단계 3 오른쪽 상단 모서리에 있는  아이콘을 클릭합니다. CDO는 화면에 표시되는 규칙을 .csv 파일로 내보냅니다.
- 단계 4 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

## FDM-관리 디바이스에서 활성 RA VPN 세션 연결 끊기

현재 Cisco Defense Orchestrator 인터페이스를 사용하는 FDM 관리 디바이스에서 RA VPN 세션을 종료하는 것은 불가능합니다. 대신 SSH를 사용하여 위협 방어 CLI에 연결하고 원하는 사용자의 연결을 끊을 수 있습니다. CDO에 온보딩된 온라인 FDM 관리 디바이스에서 이 작업을 수행할 수 있습니다.

## Procedure

- 단계 1 Firewall Device Manager에 로그인하고 디바이스에서 실행 중인 버전에 맞는 **Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드**의 "시작하기" 장의 명령줄 인터페이스(CLI)에 로그인 섹션에 설명된 대로 디바이스 CLI를 사용합니다.
- 단계 2 `vpn-sessionsdb logoff {name}` 명령을 실행하고 **name**을 사용자 이름으로 대체합니다. 이 명령은 지정한 사용자 이름에 대한 모든 세션을 종료합니다.

## FTD에 대한 원격 액세스 VPN 구성

CDO는 새로운 RA VPN(Remote Access Virtual Private Network)을 구성하기 위한 직관적인 사용자 인터페이스를 제공합니다. 또한 CDO에서 보드에 있는 여러 FDM 관리 디바이스에 대해 RA VPN 연결을 빠르고 쉽게 구성할 수 있습니다. AnyConnect는 FDM 관리 디바이스에 대한 RA VPN 연결을 위해 엔드포인트 디바이스에서 지원되는 유일한 클라이언트입니다.

AnyConnect 클라이언트는 FDM 관리 디바이스와 SSL VPN 연결을 협상할 때 TLS(Transport Layer Security: 전송 계층 보안) 또는 DTLS(Datagram Transport Layer Security: 데이터그램 전송 계층 보안)를 사용하여 연결합니다. DTLS는 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다. 클라이언트 및 FDM 관리 디바이스에서는 사용할 TLS/DTLS 버전을 협상합니다. 클라이언트가 지원하는 경우 DTLS가 사용됩니다.

CDO는 FDM 관리 디바이스에서 RA VPN 기능의 다음 측면을 지원합니다.

- SSL 클라이언트 기반 원격 액세스

- IPv4 and IPv6 addressing
- 여러 FDM 관리 디바이스에서 공유 RA VPN 구성



### Important

온보딩 FDM 관리 디바이스(소프트웨어 버전 6.7 이상에서 실행)에 SAML 서버가 인증 소스인 RA VPN 구성이 포함된 경우, CDO는 현재 릴리스에서 SAML 서버 개체를 관리하지 않으므로 연결 프로파일의 AAA 세부 정보를 채우지 않습니다. 따라서 CDO에서 이러한 RA VPN 구성을 관리할 수 없습니다. 그러나 CDO는 RA VPN 연결 프로파일 및 연결된 신뢰할 수 있는 CA 인증서 및 SAML 서버 개체를 읽습니다.

### 관련 정보:

- RADIUS 및 그룹 정책을 이용한 사용자 권한 및 속성 제어
- FDM-관리 디바이스에 대한 말단 간 원격 액세스 VPN 구성 프로세스
  - AnyConnect 클라이언트 소프트웨어 패키지 다운로드
  - 버전 6.4.0을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드
  - 버전 6.5 이상을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드
  - RA VPN AnyConnect 클라이언트 프로파일 업로드, on page 552
  - FDM-관리 장치에 대한 ID 소스 구성
    - Active Directory 영역 개체 생성 또는 편집
    - RADIUS 서버 개체 또는 그룹 생성 또는 편집
  - 새 RA VPN 그룹 정책 생성
  - RA VPN 구성 생성
  - RA VPN 연결 프로파일 컨피그레이션
  - 원격 액세스 VPN을 통한 트래픽 허용
  - 버전 6.4.0을 실행하는 FDM-관리 디바이스에서 AnyConnect 패키지 업그레이드
- FDM-관리 디바이스용 원격 액세스 VPN의 지침 및 제한 사항
- FDM-관리 디바이스에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법
- 원격 액세스 VPN에 대한 라이선싱 요구 사항
- 디바이스 모델별 최대 동시 VPN 세션
- RADIUS COA(Change of Authorization)
  - FTD 디바이스에서 COA(Change of Authorization) 구성

- RA VPN 사용자를 위한 스플릿 터널링(헤어 피닝)
- FDM-관리 디바이스의 원격 액세스 VPN 구성 확인
- FDM-관리 디바이스의 원격 액세스 VPN 구성 세부 정보 보기

## RA VPN 사용자를 위한 스플릿 터널링(헤어 피닝)

이 문서에서는 RA VPN에 대한 스플릿 터널링에 대해 설명합니다.

일반적으로 원격 액세스 VPN에서는 VPN 사용자가 디바이스를 통해 인터넷에 액세스하도록 할 수 있습니다. 그러나 VPN 사용자가 RA VPN에 연결되어 있는 동안 외부 네트워크에 액세스하도록 허용할 수 있습니다. 이 기술을 스플릿 터널링 또는 헤어피닝이라고도 합니다. 스플릿 터널을 이용하면 보안 터널을 통한 원격 네트워크 VPN 연결이 가능하며, VPN 터널 외부의 네트워크에도 연결할 수 있습니다. 스플릿 터널링은 FTD 디바이스의 네트워크 부하를 줄이고 외부 인터페이스의 대역폭을 늘립니다.

스플릿 터널 목록을 구성하려면 표준 액세스 목록 또는 확장 액세스 목록을 생성해야 합니다. 디바이스가 실행 중인 버전에 대해 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드 VPN\(Virtual Private Network\) 장의 외부 인터페이스에서 원격 액세스 VPN 사용자를 위한 외부 인터페이스에서 인터넷 액세스를 제공하는 방법\(헤어 피닝\) 섹션에 설명된 지침을 따르십시오.](#) 실행 중입니다.

## RADIUS 및 그룹 정책을 이용한 사용자 권한 및 속성 제어

이 문서에서는 외부 RADIUS 서버 또는 그룹 정책에서 RA VPN 연결에 특성을 적용하는 방법에 대한 정보를 제공합니다.

외부 RADIUS 서버 또는 FTD 디바이스에 정의된 그룹 정책에서 RA VPN 연결에 사용자 인증 속성(사용자 자격 또는 권한이라고도 함)을 적용할 수 있습니다. FTD 디바이스에서 그룹 정책에 구성된 속성과 충돌하는 속성을 AAA 서버로부터 수신하는 경우, AAA 서버에서 오는 속성이 항상 우선 적용됩니다.

FTD 디바이스에서는 다음 순서로 속성을 적용합니다.

### Procedure

- 단계 1** 외부 AAA 서버에 정의된 사용자 속성 - 인증 및/또는 권한 부여가 성공적으로 수행되면 서버에서 이 속성을 반환합니다.
- 단계 2** FTD 디바이스에 구성된 그룹 정책 - RADIUS 서버에서 사용자에게 대해 RADIUS CLASS 속성 IETF-Class-25(OU=group-policy) 값을 반환하면, FTD 디바이스에서는 해당 사용자를 이름이 같은 그룹 정책에 배치하고 서버에서 반환하지 않은 그룹 정책의 모든 속성을 적용합니다.
- 단계 3** 연결 프로파일에서 할당된 그룹 정책 - 연결 프로파일에는 연결을 위한 예비 설정이 있으며 인증 전에 사용자에게 적용되는 기본 그룹 정책을 포함합니다. FTD 디바이스에 처음 접속하는 모든 사용자는 이 그룹에 속하며, 이를 통해 AAA 서버에서 반환한 사용자 속성 또는 사용자에게 할당된 그룹 정책에 없는 모든 속성을 제공합니다.

FTD 디바이스에서는 벤더 ID가 3076인 RADIUS 속성을 지원합니다. 사용하는 RADIUS 서버에 이러한 속성이 정의되지 않은 경우, 수동으로 정의해야 합니다. 특성을 정의하려면 특성 이름 또는 번호, 유형, 값 및 공급업체 코드(3076)를 사용합니다.

다음 주제에서는 값이 RADIUS 서버에 정의되어 있는지 또는 값이 시스템에서 RADIUS 서버로 전송하는 값인지 여부에 따라 지원되는 속성을 설명합니다.

### RADIUS 서버로 전송되는 속성

RADIUS 속성 146 및 150은 인증 및 권한 부여 요청을 위해 FDM 관리 디바이스에서 RADIUS 서버로 전송됩니다. 다음 속성 모두 계정 관리 시작, 중간 업데이트, 중단 요청을 위해 FDM 관리 디바이스에서 RADIUS 서버로 전송됩니다.

**Table 17: Secure Firewall Threat Defense**에서 RADIUS로 전송하는 속성

특성	특성	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
클라이언트 유형	150	정수	단일	VPN에 접속 중인 클라이언트의 유형: 2= AnyConnect 클라이언트 SSL VPN
세션 유형	151	정수	단일	연결 유형: 1 = AnyConnect Client SSL VPN
터널 그룹 이름	146	문자열	단일	FDM 관리 디바이스에 정의된 대로 세션을 설정하는 데 사용된 연결 프로파일의 이름입니다. 이름은 1~253자일 수 있습니다.

### RADIUS 서버에서 수신한 속성

다음 사용자 권한 부여 속성은 RADIUS 서버에서 FDM 관리 디바이스로 전송됩니다.

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Access-List-Inbound	86	문자열	단일	두 Access-List(액세스 목록) 속성 모두 FDM 관리 디바이스에 구성된 ACL의 이름을 따릅니다. 스마트 CLI 확장 액세스 목록 개체 유형을 사용해 firewall device manager에서 이 ACL을 생성합니다 (firewall device manager에 로그인하고 <b>Device</b> (디바이스)> <b>Advanced Configuration</b> (고급 구성)> <b>Smart CLI</b> (스마트 CLI)> <b>Objects</b> (개체) 선택). 이 ACL에서는 인바운드(FDM 관리 디바이스로 들어가는 트래픽) 또는 아웃바운드(FDM 관리 디바이스에서 나가는 트래픽) 방향으로 트래픽 흐름을 제어합니다.
Access-List-Outbound	87	문자열	단일	
Address-Pools	217	문자열	단일	RA VPN에 접속하는 클라이언트에 대한 주소 풀로 사용될 서브넷을 식별하는 FDM 관리 디바이스에 정의된 네트워크 개체의 이름입니다. <b>Objects</b> (개체) 페이지에서 네트워크 개체를 정의합니다.

특성	속성 번호	구문, 유형	단일 또는 다중 값 지정	설명 또는 값
Banner1	15	문자열	단일	사용자가 로그인하면 표시할 배너입니다.
Banner2	36	문자열	단일	사용자가 로그인하면 표시할 배너의 두 번째 부분입니다. 배너2는 배너1에 추가됩니다.
Group-Policy	25	문자열	단일	연결에 사용할 그룹 정책입니다. <b>RA VPN Group Policy</b> (그룹 정책) 페이지에서 그룹 정책을 생성해야 합니다. 다음 형식 중 하나를 사용할 수 있습니다. <ul style="list-style-type: none"> <li>• <i>group policy name</i></li> <li>• <i>OU=group policy name</i></li> <li>• <i>OU=group policy name;</i></li> </ul>
Simultaneous-Logins	2	정수	단일	사용자가 설정할 수 있는 별도의 동시 연결 개수입니다(0~2147483647).
VLAN	140	정수	단일	사용자의 연결을 제한할 VLAN입니다(0~4094). 또한 FDM 관리 디바이스의 하위 인터페이스에 이 VLAN을 컨피그레이션해야 합니다.

## 이중 인증

RA VPN에 대한 이중 인증을 컨피그레이션할 수 있습니다. 이중 인증의 경우, 사용자는 사용자 이름 및 정적 암호뿐 아니라 Duo 암호와 같은 추가 항목도 제공해야 합니다. 이중 인증이 두 번째 인증 소스를 사용하는 것과 다른 점은 두 가지 인증 요소가 기본 인증 소스와 연결된 Duo 서버와의 관계에 따라 단일 인증 소스에서 컨피그레이션된다는 것입니다. 보조 인증 소스로 Duo LDAP 서버를 구성하는 Duo LDAP은 예외입니다.

- RADIUS를 사용하는 Duo 이중 인증, 505 페이지
- LDAP를 사용하는 Duo 이중 인증, 509 페이지

### RADIUS를 사용하는 Duo 이중 인증

듀오 RADIUS 서버를 기본 인증 소스로 컨피그레이션할 수 있습니다. 이 접근 방식에서는 듀오 RADIUS 인증 프록시를 사용합니다.

듀오를 컨피그레이션하는 세부 절차는 <https://duo.com/docs/cisco-firepower>의 내용을 참조하십시오.

그런 다음, 프록시 서버로 가는 인증 요청을 전달하여 다른 RADIUS 서버 또는 Microsoft AD(Active Directory) 서버를 첫 번째 인증 요소로 사용하고 Duo 클라우드 서비스는 두 번째 요소로 사용하도록 Duo를 구성합니다.

이 접근 방식을 사용하는 경우, 사용자는 듀오 인증 프록시 및 연결된 RADIUS/AD 서버 둘 다에 컨피그레이션된 사용자 이름과 RADIUS/AD 서버에 컨피그레이션된 사용자 이름의 암호(다음 듀오 코드 중 하나가 바로 뒤에 나옴)를 사용해 인증해야 합니다.

**Duo-passcode.** 예: *my-password,12345*.

**push.** 예: *my-password,push*. **push**(푸시)를 사용하여 듀오에게 듀오 모바일 앱으로 푸시 인증을 전송하도록 지시합니다. 사용자는 이미 이 앱을 설치하여 등록했어야 합니다.

**SMS.** 예: *my-password,SMS*. SMS를 사용하여 듀오에게 사용자의 모바일 디바이스로 새로운 암호 배치가 포함된 SMS 메시지를 전송하도록 지시합니다. SMS를 사용하는 경우, 사용자의 인증 시도가 실패합니다. 그러면 사용자는 다시 인증하고 두 번째 요인으로 새 암호를 입력해야 합니다.

**phone(전화).** 예: *my-password,phone*. 전화를 사용해 듀오에게 전화 콜백 인증을 수행하도록 지시합니다.

사용자 이름과 비밀번호가 인증된 경우 Duo Authentication Proxy는 Duo 클라우드 서비스에 연결하여 요청이 구성된 유효한 프록시 디바이스에서 왔는지 확인한 다음, 지시에 따라 사용자의 모바일 디바이스로 임시 패스코드를 푸시합니다. 사용자가 이 암호를 수락하면 듀오에서 세션을 인증된 것으로 표시하고 RA VPN이 설정됩니다.

자세한 설명은 [Duo RADIUS를 사용하여 이중 인증을 구성하는 방법, 505 페이지](#)의 내용을 참조하십시오.

### Duo RADIUS를 사용하여 이중 인증을 구성하는 방법

듀오 RADIUS 서버를 기본 인증 소스로 컨피그레이션할 수 있습니다. 이 접근 방식에서는 듀오 RADIUS 인증 프록시를 사용합니다.

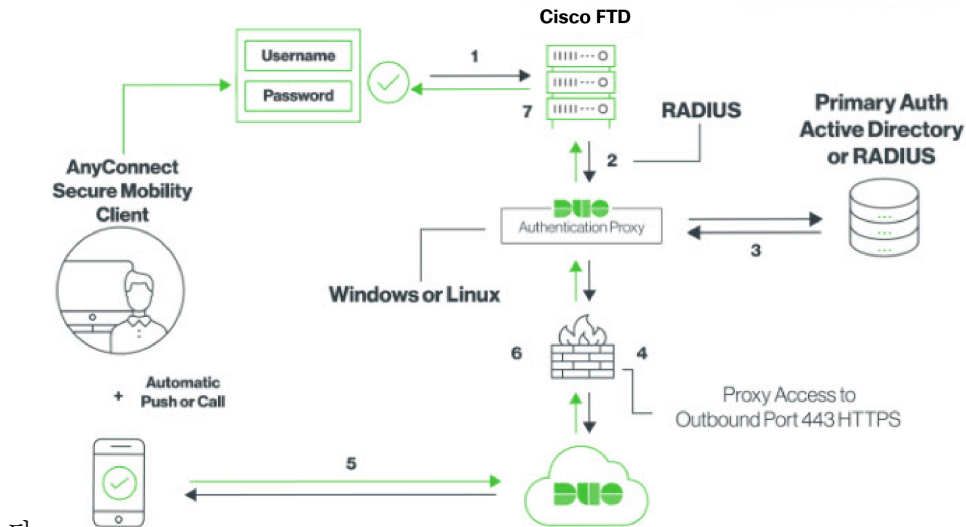
그런 다음, 프록시 서버로 가는 인증 요청을 전달하여 다른 RADIUS 서버 또는 AD 서버를 첫 번째 인증 요소로 사용하고 듀오 클라우드 서비스는 두 번째 요소로 사용하도록 컨피그레이션합니다.

다음 주제에서는 구성에 대해 자세히 설명합니다.

- [Duo RADIUS 보조 인증을 위한 시스템 플로우, 506 페이지](#)
- [CDO를 사용하여 Duo RADIUS용 디바이스 구성, 507 페이지](#)

Duo RADIUS 보조 인증을 위한 시스템 플로우

다음은 시스템 플로우에 대한 설명입니다.



다.

1. 사용자는 FDM 관리 디바이스에 원격 액세스 VPN을 연결하고 RADIUS/AD 서버와 연결된 사용자 이름, RADIUS/AD 서버에 구성된 사용자 이름의 비밀번호, DUO 코드, Duo 비밀번호, 푸시, SMS 또는 전화 중 하나를 제공합니다. 자세한 정보는 [RADIUS를 사용하는 Duo 이중 인증, 505 페이지](#)의 내용을 참조하십시오.
2. FDM 관리 디바이스에서 Duo Authentication Proxy에 인증 요청을 전송합니다.
3. Duo Authentication Proxy에서는 기본 인증 서버(Active Directory 또는 RADIUS일 수 있음)를 사용하여 이 기본 인증 시도를 인증합니다.
4. 자격 증명이 인증되면 Duo Authentication Proxy가 TCP 포트 443을 통해 Duo Security에 연결됩니다.
5. 그런 다음 Duo에서 푸시 알림, 패스코드를 사용한 문자 메시지 또는 전화 통화를 통해 사용자를 개별적으로 인증합니다. 사용자는 이 인증을 성공적으로 완료해야 합니다.
6. Duo Authentication Proxy가 인증 응답을 수신합니다.
7. 보조 인증에 성공하면 FDM 관리 디바이스에서 사용자의 AnyConnect 클라이언트와 원격 액세스 VPN 연결을 설정합니다.



## Duo RADIUS 보조 인증 구성

Duo Authentication Proxy에서는 기본 인증 서버(Active Directory 또는 RADIUS일 수 있음)를 사용하여 이 기본 인증 시도를 인증합니다.

### Duo 계정 생성

Duo 어카운트를 생성하고 통합 키, 비밀 키 및 API 호스트 이름을 가져옵니다.

프로세스는 간단히 다음과 같습니다. 자세한 내용은 Duo 웹 사이트를 참고하십시오.

#### 프로시저

단계 1 Duo 어카운트에 등록합니다.

단계 2 Duo Admin Panel에 로그인하여 **Applications**(애플리케이션)로 이동합니다.

단계 3 애플리케이션 목록에서 **Protect an Application**(애플리케이션 보호)을 클릭하고 **Cisco Firepower Threat Defense VPN**을 찾습니다.

단계 4 **Protect this Application**(이 애플리케이션 보호)을 클릭하여 통합 키, 암호 키 및 API 호스트 이름을 가져옵니다. 프록시를 구성할 때 이 정보가 필요합니다. 도움이 필요한 경우 *Duo Getting Started* 가이드 (<https://duo.com/docs/getting-started>)를 참조하십시오.

단계 5 Duo 인증 프록시를 설치하고 구성합니다. 자세한 내용은 <https://duo.com/docs/cisco-firepower>의 "Duo Authentication Proxy 설치" 섹션을 참조하십시오.

단계 6 인증 프록시를 시작합니다. 자세한 내용은 <https://duo.com/docs/cisco-firepower>의 "프록시 시작" 섹션을 참조하십시오.

Duo에 새 사용자를 등록하는 방법은 <https://duo.com/docs/enrolling-users>를 참조하십시오.

## CDO를 사용하여 Duo RADIUS용 디바이스 구성

#### 프로시저

단계 1 FTD Radius 서버 개체를 구성합니다.

a) 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

b)  > **RA VPN Objects (ASA & FTD)**(RA VPN 개체(ASA 및 FTD)) > **Identity Source**(ID 소스)를 클릭합니다.

c) 이름을 입력하고 **Device Type**(디바이스 유형)을 **FTD**로 설정합니다.

d) **Radius Server Group**(Radius 서버 그룹)을 선택하고 **Continue**(계속)를 클릭합니다. 자세한 내용은 **RADIUS 서버 그룹 생성, 531 페이지**의 6단계를 참조하십시오.

e) **Radius Server**(Radius 서버) 섹션에서 **Add**(추가) 버튼을 클릭하고 **Create New Radius Server**(새 Radius 서버 생성)를 클릭합니다. **RADIUS 서버 개체 생성, 530 페이지**의 내용을 참조하십시오.

**Server Name**(서버 이름) 또는 **IP Address**(IP 주소) 필드에 Duo Authentication Proxy 서버의 정규화된 호스트 이름 또는 IP 주소를 입력합니다.

Adding FTD RADIUS Server
✕

Object Name

Device Type

FTD ▾

Description

---

**1** Identity Source Type     **RADIUS Server**

---

**2** Edit Identity Source

Server Name or IP Address

Authentication Port

Timeout (seconds) ⓘ

1 - 300

Server Secret Key

RA VPN Only (if this object is used in RA VPN Configuration)

Cancel
Add

- f) Duo RADIUS 서버를 그룹에 추가했으면 **Add**(추가)를 클릭하여 새 Duo RADIUS 서버 그룹을 생성합니다

Adding FTD RADIUS Server Group
✕

Object Name

Device Type

FTD ▾

Description

---

**1** Identity Source Type     **RADIUS Server Group**

---

**2** Edit Identity Source

Dead Time ⓘ

0-1440 minutes

Dynamic Authorization (for RA VPN only)

Port

1024-65535

Realm that Supports the RADIUS Server

Relam\_Active\_Directory ▾

Maximum Failed Attempts

1-5

RADIUS Server ⓘ

+
RADIUS SERVERS

DuoRadiusServerObject
✕

- 단계 2 Remote Access VPN Authentication Method(원격 액세스 VPN 인증 방법)를 Duo RADIUS로 변경합니다.
- CDO 내비게이션 메뉴에서 **VPN > Remote Access VPN Configuration**(원격 액세스 VPN 구성)을 클릭합니다.
  - VPN 구성을 확장하고 Duo를 추가할 연결 프로파일을 클릭합니다.
  - 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.
  - Authentication Type**(인증 유형)은 **AAA** 또는 **AAA and Client Certificate**(AAA 및 클라이언트 인증서)가 될 수 있습니다.
  - Primary Identity Source for User Authentication**(사용자 인증을 위한 기본 ID 소스) 목록에서 이전에 생성한 서버 그룹을 선택합니다.

- 일반적으로 "Authorization Server(권한 부여 서버)" 또는 "Accounting Server(과금 서버)"를 선택할 필요가 없습니다.
  - Continue**(계속)를 클릭합니다.
  - Summary and Instructions**(요약 및 지침) 단계에서 **Done**(완료)을 클릭하여 구성을 저장합니다.
- 단계 3 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

### LDAP를 사용하는 Duo 이중 인증

기본 소스로 Microsoft AD(Active Directory) 또는 RADIUS 서버를 함께 사용하여 Duo LDAP 서버를 보조 인증 소스로 사용할 수 있습니다. Duo LDAP를 사용하는 경우 보조 인증에서는 Duo 패스코드, 푸시 알림 또는 전화 통화를 사용하여 기본 인증을 검증합니다.



참고 Duo 이중 인증 기능은 Firepower Threat [단일 FTD 디바이스 업그레이드](#)을 실행하는 디바이스의 CDO에서 사용할 수 있습니다.

FTD 디바이스에서는 TCP/636 포트를 통해 LDAPS를 사용하여 Duo LDAP과 통신합니다.

이 접근 방식을 사용하는 경우 사용자는 AD/RADIUS 서버 및 Duo LDAP 서버에 구성된 사용자 이름을 사용하여 인증해야 합니다. AnyConnect에서 로그인하라는 프롬프트가 표시되면 사용자는 기본 Password(비밀번호) 필드에 AD/RADIUS 비밀번호를 입력하고 Secondary Password(보조 비밀번호)에

## Duo LDAP를 사용하여 이중 인증을 구성하는 방법

는 Duo를 사용하여 인증하기 위해 다음 중 하나를 입력합니다. 자세한 내용은 <https://guide.duo.com/anyconnect>의 "요소 선택을 위한 두 번째 비밀번호" 섹션을 참조하십시오.

- **Duo passcode(Duo 암호)** - Duo Mobile을 통해 생성되었거나 SMS를 통해 전송되었거나 하드웨어 토큰에 의해 생성되었거나 관리자가 제공한 암호를 사용하여 인증합니다. 1234567을 예로 들 수 있습니다.
- **push(푸시)** - Duo Mobile 앱을 설치하고 활성화한 경우 전화기에 로그인 요청을 푸시합니다. 요청을 검토하고 **Approve(승인)**를 눌러 로그인합니다.
- **phone(전화기)** - 전화기 콜백을 사용하여 인증합니다.
- **sms** - 텍스트 메시지로 Duo 암호를 요청합니다. 로그인 시도가 실패합니다. 새 암호를 사용하여 다시 로그인합니다.

자세한 설명은 [Duo LDAP를 사용하여 이중 인증을 구성하는 방법, 510 페이지](#)의 내용을 참조하십시오.

## Duo LDAP를 사용하여 이중 인증을 구성하는 방법

기본 소스로 Microsoft AD(Microsoft Active Directory) 또는 RADIUS 서버를 함께 사용하여 Duo LDAP 서버를 보조 인증 소스로 사용할 수 있습니다. Duo LDAP를 사용하는 경우 보조 인증에서는 Duo 패스코드, 푸시 알림 또는 전화 통화를 사용하여 기본 인증을 검증합니다.

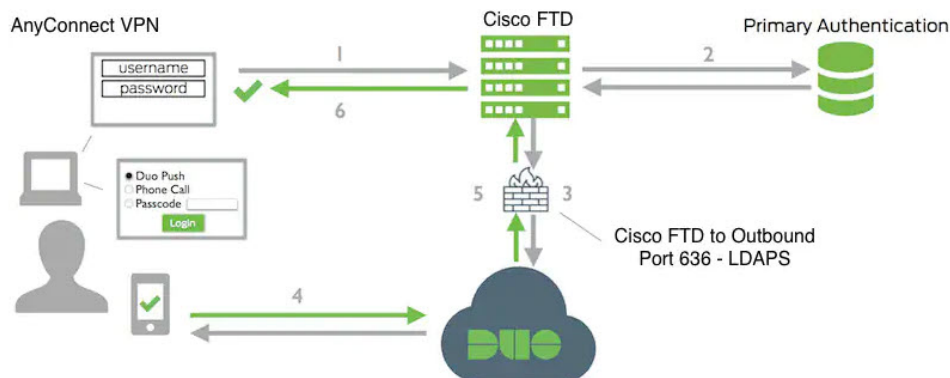
다음 주제에서는 구성에 대해 자세히 설명합니다.

- [Duo LDAP 보조 인증을 위한 시스템 플로우, 510 페이지](#)
- [Duo LDAP 보조 인증 구성, 511 페이지](#)

## Duo LDAP 보조 인증을 위한 시스템 플로우

다음 그래픽에는 LDAP를 사용하여 이중 인증을 제공하기 위해 위협 방어 및 Duo가 함께 작동하는 방법이 나와 있습니다.

다음은 시스템 플로우에 대한 설명입니다.



1. 사용자는 FDM 관리 디바이스에 대한 원격 액세스 VPN 연결을 설정하고 사용자 이름과 비밀번호를 입력합니다.

2. FDM 관리 디바이스에서는 기본 인증 서버(Active Directory 또는 RADIUS일 수 있음)를 사용하여 이 기본 인증 시도를 인증합니다.
3. 기본 인증이 작동하는 경우 FDM 관리 디바이스에서는 보조 인증에 대한 요청을 Duo LDAP 서버로 전송합니다.
4. 그런 다음 Duo에서 푸시 알림, 패스코드를 사용한 문자 메시지 또는 전화 통화를 통해 사용자를 개별적으로 인증합니다. 사용자는 이 인증을 성공적으로 완료해야 합니다.
5. Duo에서는 사용자가 성공적으로 인증되었는지 여부를 나타내기 위해 FDM 관리 디바이스에 응답합니다.
6. 보조 인증에 성공하면 FDM 관리 디바이스에서 사용자의 AnyConnect 클라이언트와 원격 액세스 VPN 연결을 설정합니다.

### Duo LDAP 보조 인증 구성

다음 절차에서는 Duo LDAP를 보조 인증 소스로 사용하여 원격 액세스 VPN에 이중 인증을 구성하는 엔드 투 엔드 프로세스에 대해 설명합니다. 이 구성을 완료하려면 Duo를 사용하는 어카운트가 있어야 하며 Duo에서 일부 정보를 얻어야 합니다.

### Duo 계정 생성

Duo 어카운트를 생성하고 통합 키, 비밀 키 및 API 호스트 이름을 가져옵니다.

프로세스는 간단히 다음과 같습니다. 자세한 내용은 Duo 웹 사이트를 참고하십시오.

프로시저

---

단계 1 Duo 어카운트에 등록합니다.

단계 2 Duo Admin Panel에 로그인하여 **Applications**(애플리케이션)로 이동합니다.

단계 3 애플리케이션 목록에서 **Protect an Application**(애플리케이션 보호)을 클릭하고 **Cisco Firepower Threat Defense VPN**을 찾습니다.

단계 4 **Protect this Application**(이 애플리케이션 보호)을 클릭하여 통합 키, 암호 키, API 호스트 이름을 가져옵니다. 도움이 필요한 경우 Duo 시작하기 가이드(<https://duo.com/docs/getting-started>)를 참조하십시오.

Duo에 새 사용자를 등록하는 방법은 <https://duo.com/docs/enrolling-users>를 참조하십시오.

---

### FDM-관리 디바이스에 신뢰할 수 있는 CA 인증서 업로드

FDM 관리 디바이스에는 Duo LDAP 서버에 대한 연결을 검증하는 데 필요한 신뢰할 수 있는 CA 인증서가 있어야 합니다. <https://www.digicert.com/digicert-root-certificates.htm>으로 직접 이동하여 **DigiCertSHA2HighAssuranceServerCA** 또는 **DigiCert High Assurance EV** 루트 CA를 다운로드하고 Firewall Device Manager(FDM)을 사용하여 업로드할 수 있습니다.

---

 프로시저
 

---


- 단계 1 FDM 관리 디바이스의 firewall device manager 페이지에 액세스하여 **Objects(개체)** > **Certificates(인증서)**를 선택합니다.
- 단계 2 + > **Add Trusted CA Certificate(신뢰받는 CA 인증서 추가)**를 클릭합니다.
- 단계 3 인증서의 이름(예: DigiCert\_High\_Assurance\_EV\_Root\_CA)을 입력합니다. 공백은 허용되지 않습니다.
- 단계 4 **Upload Certificate(인증서 업로드)**를 클릭하고 다운로드한 파일을 선택합니다.
- 단계 5 **OK(확인)**를 클릭합니다.
- 단계 6 아직 온보딩하지 않은 경우 Cisco Defense Orchestrator에 디바이스를 온보딩합니다.
- 단계 7 [모든 디바이스 구성 읽기](#).
- 

## CDO에서 Duo LDAP용 FTD 구성

---

 프로시저
 

---

- 단계 1 Duo LDAP 서버의 Duo LDAP ID 소스 개체를 생성합니다.
- 좌측의 CDO 내비게이션 바에서, **Objects(개체)** > **FDM Objects(FDM 개체)**을 클릭합니다.
  -  을 클릭하여 개체를 열고 **RA VPN Objects (ASA & FTD)(RA VPN 개체(ASA 및 FTD))** > **Identity Source(ID 소스)**를 클릭합니다.
  - 개체의 이름을 입력합니다(예: Duo-LDAP-server).
  - Device Type(장치 유형)**을 **FTD**로 선택합니다.

e) **Duo LDAP Identity Source(Duo LDAP ID 소스)**를 클릭하고 **Continue(계속)**를 클릭합니

다.

f) **Edit Identity Source(ID 소스 편집)** 영역에서 다음 세부 정보를 입력합니다.

- **API Hostname(API 호스트 이름):** Duo 계정에서 가져온 API 호스트 이름을 입력합니다. 호스트 이름은 X가 고유한 값으로 교체되면 API-XXXXXXXXX.DUOSEcurity.COM과 유사하게 표시되어야 합니다. 대문자는 필요하지 않습니다.
- **Port(포트):** LDAPS에 사용할 TCP 포트를 입력합니다. 포트는 다른 포트를 사용하도록 Duo 에서 지시한 경우를 제외하고는 636이어야 합니다. 액세스 제어 목록에서 이 포트를 통해 Duo LDAP 서버에 대한 트래픽을 허용하는지 확인해야 합니다.
- **Timeout(시간 초과):** Duo 서버에 연결할 시간 제한(초)을 입력합니다. 이 값은 1~300초일 수 있습니다. 기본값은 120입니다. 기본값을 사용하려면 120을 입력하거나 특성 줄을 삭제합니다.
- **Integration Key(통합 키):** Duo 계정에서 가져온 통합 키를 입력합니다.
- **Secret Key(암호 키):** Duo 계정에서 가져온 암호 키를 입력합니다. 이 키는 이후에 마스킹됩니다.
- **Interface used to connect to Duo Server(Duo 서버에 연결하는 데 사용되는 인터페이스):** Duo 서버에 연결하는 데 사용할 인터페이스를 선택합니다.
  - **Resolve via route lookup(경로 조회를 통해 확인):** 라우팅 테이블을 사용하여 올바른 경로를 찾으려면 이 옵션을 선택합니다. 라우팅 테이블을 생성하는 방법은 라우팅을 참조하십시오.
  - **Manually choose interface(수동으로 인터페이스 선택):** 이 옵션을 선택하고 목록에서 인터페이스 중 하나를 선택합니다. 기본 인터페이스는 진단 인터페이스지만, 이는 인터페

이스의 IP 주소를 구성하는 경우에만 작동합니다. 참고: 선택한 인터페이스가 Duo 서버에 연결하려는 동일한 디바이스에 있는지 확인합니다.

- **Add(추가)**를 클릭합니다.

**단계 2** (선택 사항) 인증 시간 초과에 60초 이상을 지정하는 프로필을 생성하려면 AnyConnect 프로필 편집기를 사용합니다.

사용자에게 Duo 암호를 얻고 보조 인증을 완료할 추가 시간을 제공해야 합니다. 60초 이상 제공하는 것이 좋습니다. 다음 절차에서는 인증 시간 초과만 구성된 후 프로필을 FDM 관리 디바이스에 업로드하는 방법에 대해 설명합니다. 다른 설정을 변경하려는 경우 지금 하면 됩니다.

- 아직 작업을 수행하지 않은 경우, AnyConnect 프로필 편집기 패키지를 다운로드하여 설치합니다. 이는 Cisco Software Center(software.cisco.com)(AnyConnect 버전용 폴더)에서 찾을 수 있습니다. 이 문서를 작성할 시점의 기본 경로는 **Downloads Home**(다운로드 홈) > **Security**(보안) > **VPN and Endpoint Security Clients**(VPN 및 엔드포인트 보안 클라이언트) > **Cisco VPN Clients**(Cisco VPN 클라이언트) > **AnyConnect Secure Mobility Client**(AnyConnect Secure Mobility 클라이언트)입니다.
- AnyConnect **VPN Profile Editor**(VPN 프로필 편집기)를 엽니다.
- 목차에서 **Preferences(Part 2)**(기본 설정(파트 2))를 선택하고 페이지 끝으로 스크롤한 다음, **Authentication Timeout**(인증 시간 제한)을 60 이상으로 변경합니다. 다음 이미지는 AnyConnect 4.7 VPN 프로필 편집기의 이미지입니다(이전 버전 또는 후속 버전의 경우 다를 수 있음).
- File**(파일) > **Save**(저장)를 선택하고 프로필 XML 파일을 적절한 이름(예: duo-ldap-profile.xml)의 워크스테이션에 저장합니다.
- 이제 **VPN** 프로필 편집기 애플리케이션을 닫으면 됩니다.
- CDO에서 [RA VPN AnyConnect 클라이언트 프로파일 업로드](#).

**단계 3** 그룹 정책을 생성하고 정책에서 AnyConnect 프로필을 선택합니다.

사용자에게 할당하는 그룹 정책으로 인해 연결의 여러 측면이 제어됩니다. 다음 절차에서는 프로필 XML 파일을 그룹에 할당하는 방법에 대해 설명합니다. 자세한 내용은 [새 RA VPN 그룹 정책 생성](#)을 참조하십시오.

- 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.
- 기존 그룹 정책을 편집하려면 **RA VPN** 그룹 정책 필터를 사용하여 기존 그룹 정책만 확인한 후 원하는 정책을 수정하고 저장합니다.
- 새 그룹 정책을 생성하려면 **RA VPN Objects (ASA & FTD)**(RA VPN 개체(ASA 및 FTD)) > **RA VPN Group Policy**(RA VPN 그룹 정책)를 클릭합니다.
- General**(일반) 페이지에서 다음 속성을 구성합니다.
  - **Name**(이름) - 새 프로필의 경우 이름을 입력합니다. 예를 들어, Duo-LDAP-group과 같이 입력합니다.
  - **AnyConnect Client Profiles**(AnyConnect 클라이언트 프로파일) - 생성한 AnyConnect 클라이언트 프로파일 개체를 선택합니다.
- Add**(추가)를 클릭하여 개체를 저장합니다.
- VPN** > **Remote Access VPN Configuration**(원격 액세스 VPN 구성)을 클릭합니다.

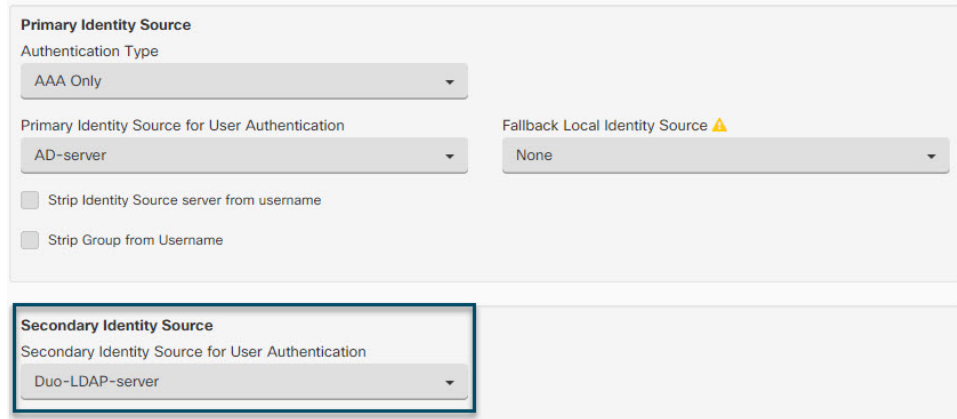


- g) 업데이트할 원격 액세스 VPN 구성을 클릭합니다.
- h) 오른쪽의 **Actions**(작업) 창에서 **Group Policies**(그룹 정책)를 클릭합니다.
- i) +를 클릭하여 VPN 구성과 연결할 그룹 정책을 선택합니다.
- j) **Save**(저장)를 클릭하여 그룹 정책을 저장합니다.

**단계 4 Duo-LDAP 보조 인증에 사용할 원격 액세스 VPN 연결 프로필을 생성하거나 수정합니다.**

다음 절차에서는 Duo-LDAP를 보조 인증 소스로 활성화하고 AnyConnect 클라이언트 프로필을 적용하기 위한 주요 변경 사항에 대해서만 설명합니다. 새 연결 프로필의 경우 나머지 필수 필드를 구성해야 합니다. 이 절차에서는 기존 연결 프로필을 편집하는 중이며 이러한 두 가지 설정만 변경하면 된다고 가정합니다.

- a) CDO 내비게이션 페이지에서 **VPN > Remote Access VPN Configuration**(원격 액세스 VPN 구성)을 클릭합니다.
- b) 원격 액세스 VPN 구성을 확장하고 업데이트할 연결 프로필을 클릭합니다.
- c) 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.
- d) **Primary Identity Source**(기본 ID 소스) 아래에서 다음을 구성합니다.
  - **Authentication Type**(인증 유형) - AAA Only(AAA 전용) 또는 AAA and Client Certificate(AAA 및 클라이언트 인증서) 중 하나를 선택합니다. AAA를 사용하지 않는 한, 이중 인증을 구성할 수 없습니다.
  - **Primary Identity Source for User Authentication**(사용자 인증을 위한 기본 ID 소스) - 기본 Active Directory 또는 RADIUS 서버를 선택합니다. Duo-LDAP ID 소스를 기본 소스로 선택할 수 있습니다. 그러나 Duo-LDAP에서는 인증 서비스만 제공하며 ID 서비스는 제공하지 않습니다. 따라서 이를 기본 인증 소스로 사용하는 경우, 어떠한 대시보드에도 RA VPN 연결과 관련된 사용자 이름이 표시되지 않으며, 이러한 사용자에 대한 액세스 제어 규칙을 작성할 수 없게 됩니다. 원하는 경우 로컬 ID 소스로의 대체 기능을 구성할 수 있습니다.
  - **Secondary Identity Source**(보조 ID 소스) - Duo-LDAP ID 소스를 선택합니다.



**참고** **Primary Identity Source**(기본 ID 소스) 및 **Secondary Identity Source**(보조 ID 소스)의 사용자 이름이 동일한 경우, Connection Profile(연결 프로필)의 **Advanced**(고급) 옵션에서 **Use Primary username for Secondary login**(보조 로그인에 기본 사용자 이름 사용)을 활성화하는 것이 좋습니다. 이 방법으로 구성하면 엔드 유저는 기본 및 보조 ID 소스 모두에 단일 사용자 이름을 사용할 수 있습니다.

- e) **Continue**(계속)를 클릭합니다.
- f) **Group Policy**(그룹 정책) 페이지에서 사용자가 생성했거나 편집한 그룹 정책을 선택합니



- g) **Continue**(계속)를 클릭합니다.
- h) **Done**(완료)을 클릭하여 연결 프로필에 변경 사항을 저장합니다.

단계 5 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 620 페이지.

## FDM-관리 디바이스에 대한 말단 간 원격 액세스 VPN 구성 프로세스

이 섹션에서는 CDO에 온보딩된 FDM 관리 디바이스에서 원격 액세스 가상 프라이빗망(RA VPN)을 구성하기 위한 엔드 투 엔드 절차를 제공합니다.

클라이언트에 대한 원격 액세스 VPN을 활성화하려면 여러 개의 개별 항목을 구성해야 합니다. 다음 절차에서는 이러한 엔드 투 엔드 프로세스를 제공합니다.

### Procedure

단계 1 두 개의 라이선스를 활성화합니다.

- 디바이스를 등록할 때는 내보내기 제어 기능에 대해 활성화된 Smart Software Manager 어카운트를 사용하여 등록을 수행해야 합니다. 라이선스는 원격 액세스 VPN을 구성하기 전에 수출 통제 요구 사항을 충족해야 합니다. 또한, 평가 라이선스로는 기능을 구성할 수 없습니다. FDM 관리 디바이스 구매에 라이선스가 자동으로 포함됩니다. 라이선스는 선택적 라이선스가 적용되지 않는 모든 기능을 포함합니다. 영구 라이선스입니다. 디바이스를 Secure Firewall device manager에 등록해야 합니다. 디바이스가 실행 중인 버전에 대해서는 [Secure Firewall Threat Defense Cisco 구성 가이드](#)의 시스템 라이선싱 장에서 디바이스 등록 섹션을 참조하십시오.
- 라이선스. 자세한 내용은 [원격 액세스 VPN에 대한 라이선싱 요구 사항](#)을 참조하십시오.
  - 라이선스를 활성화하려면 디바이스가 실행 중인 버전에 대한 Secure Firewall Threat Defense 구성 가이드의 [시스템 라이선스 섹션](#)에서 선택적 라이선스 활성화 또는 비활성화 섹션을 참조하십시오.

단계 2 인증서를 구성합니다.

클라이언트와 디바이스 간의 SSL 연결을 인증하려면 인증서가 필요합니다. VPN에 대해 미리 정의된 DefaultInternalCertificate를 사용하거나 직접 만들 수 있습니다.

인증에 사용되는 디렉터리 영역에 대해 암호화된 연결을 사용하는 경우에는 신뢰할 수 있는 CA 인증서를 업로드해야 합니다. 인증서 및 업로드 방법에 대한 자세한 내용은 [인증서 구성](#)을 참조하십시오.

단계 3 원격 사용자 인증에 사용되는 ID 소스를 구성합니다.

다음 소스를 사용하여 RA VPN을 사용하여 네트워크에 연결을 시도하는 사용자를 인증할 수 있습니다. 또한 인증을 위해 클라이언트 인증서를 단독으로 또는 ID 소스와 함께 사용할 수 있습니다.

- AD(Active Directory) ID 영역: 기본 인증 소스로 사용됩니다. AD(Active Directory) 서버에서 사용자 어카운트가 정의됩니다. AD ID 영역 구성을 참조하십시오. [Active Directory 영역 개체 생성 또는 편집](#)을 참조하십시오.
- RADIUS 서버 그룹: 기본 또는 보조 인증 소스로서, 권한 부여 및 계정 관리를 위한 것입니다. [RADIUS 서버 개체 또는 그룹 생성 또는 편집](#)을 참조하십시오.
- Local Identity Source(로컬 사용자 데이터베이스): 기본 또는 대체 소스로 사용됩니다. 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 설명한 것과 같은 사용자 이름/비밀번호를 정의해야 합니다.

**Note** Secure Firewall device manager에서만 FDM 관리 디바이스에서 직접 사용자 계정을 만들 수 있습니다. [로컬 사용자 구성](#)을 참조하십시오.

#### 단계 4 (선택 사항). 새 RA VPN 그룹 정책 생성

그룹 정책에서는 사용자와 관련된 속성을 정의합니다. 그룹 멤버십에 근거하여 리소스에 차등 액세스를 제공하도록 그룹 정책을 구성할 수 있습니다. 또는 모든 연결에 기본 정책을 사용합니다.

#### 단계 5 RA VPN 구성 생성

#### 단계 6 RA VPN 연결 프로파일 컨피그레이션

#### 단계 7 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

#### 단계 8 원격 액세스 VPN을 통한 트래픽 허용

단계 9 (선택 사항). ID 정책을 활성화하고 패시브 인증에 사용할 규칙을 생성합니다. 패시브 사용자 인증을 활성화하는 경우 원격 액세스 VPN을 통해 로그인한 사용자는 대시보드에 표시되며 정책에서 트래픽 일치 기준으로 사용할 수 있게 됩니다. 패시브 인증을 활성화하지 않는 경우 RA VPN 사용자는 활성 인증 정책과 일치하는 경우에만 사용 가능합니다. 대시보드에서 또는 트래픽 일치용으로 사용자 이름 정보를 가져오려면 ID 정책을 활성화해야 합니다. [ID 정책 구성](#)



**Important** Secure Firewall device manager와 같은 로컬 관리자를 사용하여 원격 액세스 VPN 구성을 변경하면, CDO에서 해당 디바이스의 구성 상태가 "충돌 감지됨"으로 표시됩니다. [디바이스의 대역 외 변경 사항](#)을 참조하십시오. 이 FDM 관리 디바이스에서 [구성 충돌 해결](#)할 수 있습니다.

#### What to do next

RA VPN 구성이 FDM 관리 디바이스에 다운로드되면 사용자는 인터넷에 연결된 컴퓨터나 지원되는 다른 iOS 또는 Android 디바이스를 사용하여 원격 위치에서 네트워크에 연결할 수 있습니다. 테넌트의 모든 온보딩 RA VPN 헤드엔드에서 실시간 AnyConnect 원격 액세스 RA VPN(가상 프라이빗망) 세션을 모니터링할 수 있습니다. [원격 액세스 가상 프라이빗 네트워크 세션](#)을 참조하십시오.

## AnyConnect 클라이언트 소프트웨어 패키지 다운로드

원격 액세스 VPN를 구성하려면 먼저 AnyConnect 소프트웨어 패키지를 <https://software.cisco.com/download/home/283000185>에서 워크스테이션에 다운로드해야 합니다. 원하는 운영 체제에 대한 "AnyConnect 헤드엔드 배포 패키지"를 다운로드했는지 확인합니다. 나중에 VPN을 정의할 때 이러한 패키지를 FTD(Firepower Threat Defense) 디바이스에 업로드할 수 있습니다.

항상 최신 AnyConnect 버전을 다운로드하여 최신 기능, 버그 편집 및 보안 패치가 있는지 확인합니다. 디바이스에서 패키지를 정기적으로 업데이트합니다.



**Note** 운영 체제(Windows, Mac, Linux)별로 AnyConnect 패키지를 하나씩 업로드할 수 있습니다. 지정된 OS 유형의 여러 버전을 업로드할 수는 없습니다.

## 버전 6.4.0을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드

firewall device manager API 탐색기를 사용하여 FDM 관리 디바이스 버전 6.4.0에 AnyConnect 소프트웨어 패키지를 업로드할 수 있습니다. RA VPN 연결을 생성하려면 디바이스에 최소 하나의 AnyConnect 소프트웨어 패키지가 있어야 합니다.

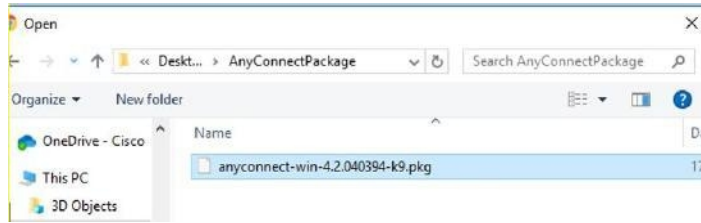


**Important** 해당 절차는 firewall device manager 버전 6.4에만 적용됩니다. firewall device manager 버전 6.5 이상을 사용하는 경우 Cisco Defense Orchestrator 인터페이스를 사용하여 버전 6.5 이상을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드합니다.

firewall device manager 버전 6.4.0에 AnyConnect 패키지를 업로드하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 <https://software.cisco.com/download/home/283000185>에서 AnyConnect 패키지를 다운로드합니다.
  - EULA에 동의하고 K9(암호화된 이미지) 권한이 있는지 확인합니다.
  - 운영 체제에 맞는 "AnyConnect Headend Deployment Package" 패키지를 선택합니다. 패키지 이름은 "anyconnect-win-4.7.04056-webdeploy-k9.pkg"와 유사합니다. Windows, macOS 및 Linux용 별도의 헤드엔드 Webs Deploy 패키지가 있습니다.
- 단계 2 브라우저를 사용하여 시스템의 홈페이지를 엽니다. 예를 들어 <https://ftd.example.com>입니다.
- 단계 3 Firewall Device Manager에 로그인합니다.
- 단계 4 `##/api-explorer`를 가리키도록 URL을 편집합니다(예: <https://ftd.example.com/##/api-explorer>).
- 단계 5 아래로 스크롤하여 **Upload(업로드)** > `/action/uploaddiskfile`를 클릭합니다.
- 단계 6 **fileToUpload** 필드에서 파일 선택(**Choose File**)을 클릭하고 필요한 AnyConnect 패키지를 선택합니다. 패키지를 한 번에 하나씩 업로드할 수 있습니다.



단계 7 **Open**(열기)를 클릭합니다.

단계 8 아래로 스크롤하여 **TRY IT OUT!**(사용해보세요!)를 클릭합니다. 패키지가 완전히 업로드될 때까지 기다리십시오. **Response Body**(응답 본문)에서 API 응답은 다음 형식으로 나타납니다.

```
{ "version": null, "name": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
  "fileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
  "id": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
  "type": "fileuploadstatus",
  "links": {
  "self":
  "https://ftd.example.com:972/api/fdm/...90d111e9-a361-%20cf32937ce0df.pkg"
  } }
```

POST 작업을 수행할 때 동일한 문자열을 입력해야 하므로 응답에서 패키지의 **fileName**을 기록합니다. 이 예에서 파일 이름은 **691f47e1-90c7-11e9-a361-79e2452f0c57.pkg**입니다.

단계 9 위협 방어 REST API 페이지 상단 근처에서 위로 스크롤하고 **AnyConnectPackageFile > POST /object/anyconnectpackagefiles**를 클릭합니다. 페이로드에 있는 패키지 파일의 임시 준비 **diskFileName** 및 OS 유형을 제공하는 API에 대해 POST 작업을 수행합니다. 이 작업은 AnyConnect 패키지 파일을 생성합니다.

단계 10 본문 필드에 패키지 세부 정보를 다음 형식으로만 입력합니다.

```
{ "platformType": "WINDOWS",
  "diskFileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
  "type": "anyconnectpackagefile",
  "name": "AnyConnectWindowsBGL" }
```

- platformType** 필드에 OS 플랫폼을 WINDOWS, MACOS 또는 LINUX로 입력합니다.
- diskFileName** 필드에는 디스크 파일을 업로드한 후 기록한 **fileName**을 입력합니다.
- name** 필드에 원하는 패키지 이름을 입력합니다.
- TRY IT OUT!**(사용해 보세요!)를 클릭합니다.

**Response Body**(응답 본문) 필드에서 API 응답은 성공적인 POST 작업 후 다음 형식으로 나타납니다.

```
{ "version": "ni7xeneslft3p",
  "name": "AnyConnectWindowsBGL",
  "description": null,
  "diskFileName": "41d592e3-90ca-11e9-a361-6d05320a165d.pkg",
```

```

"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": { "self":
" https://>/ftd.example.com:972...1-cf32937ce0df"https://bglgrp1224-pod.cisco.com:972/api/fdm/v3/object/
anyconnectpackagefiles/7f8248c7-90d1-11e9-a361-cf32937ce0df
}
}

```

AnyConnect 패키지는 firewall device manager에서 생성됩니다.

단계 11 **AnyConnectPackageFile > GET /object/anyconnectpackagefiles > TRY IT OUT!**(사용해 보세요!)를 클릭합니다.

**Response Body**(응답 본문)에는 모든 AnyConnect 패키지 파일이 표시됩니다.

샘플 응답은 다음과 같습니다.

```

{
"items": [
{
"version": "la4nwceqk2sg4",
"name": "AnyConnectWindowsBGL",
"description": null,
"diskFileName": "82f1e362-9cd8-11e9-a361-9758ba07962d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": {
"self":
"https://ftd.example.com:972...1-23534f081c43"
}
}
],

```

단계 12 OS 유형별로 기타 AnyConnect 패키지를 업로드합니다. 4~10단계를 반복합니다.

단계 13 웹 페이지를 가리키도록 URL(예: <https://ftd.example.com>)을 편집합니다.

단계 14 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes**(변경 사항 구축) 아이콘을 클릭합니다. 배포되지 않은 변경 사항이 있으면 아이콘이 점으로 강조 표시됩니다.

단계 15 변경 사항에 만족하는 경우 **Deploy Now**(지금 구축)를 클릭하여 작업을 즉시 시작할 수 있습니다. 창에는 배포가 진행 중임이 표시됩니다. 창을 닫을 수도 있고 배포가 완료될 때까지 기다릴 수도 있습니다.



**Note** FDM 관리디바이스에서 패키지를 삭제하려면, **AnyConnectPackageFile > Delete(삭제)** 를 클릭합니다. **objID** 필드에 패키지 ID를 입력하고 **TRY IT OUT!**를 클릭합니다.

VPN 연결을 완료하려면 사용자가 해당 워크스테이션에 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 자세한 내용은 [FDM-관리 디바이스에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법](#), on page 554를 참고하십시오.

버전 6.5 이상을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드

**단일 FTD 디바이스 업그레이드**을 실행하는 FDM 관리 디바이스를 사용하여 RA VPN을 구성하는 경우, Cisco Defense Orchestrator의 RA VPN 마법사를 사용하여 AnyConnect 소프트웨어 패키지를 디바이스에 업로드할 수 있습니다. RA VPN 마법사에서 AnyConnect 패키지가 미리 로드된 원격 HTTP 또는 HTTPS 서버의 URL을 제공해야 합니다.



**Note** 버전 6.4.0을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드를 사용하여 AnyConnect 패키지를 업로드할 수도 있습니다.

CDO 저장소에서 AnyConnect 패키지 업로드


원격 액세스 VPN 구성 마법사는 CDO 저장소에서 운영 체제별로 AnyConnect 패키지를 제공하며, 이러한 패키지를 선택하여 디바이스에 업로드할 수 있습니다. 디바이스가 인터넷 및 적절한 DNS 구성에 액세스할 수 있는지 확인합니다.



**참고** 표시된 목록에서 원하는 패키지를 사용할 수 없거나 디바이스에서 인터넷에 액세스할 수 없는 경우 AnyConnect 패키지가 미리 로드된 서버를 사용하여 패키지를 업로드할 수 있습니다.

프로시저

**단계 1** 운영 체제에 해당하는 필드를 클릭하고 AnyConnect 패키지를 선택합니다.

**단계 2**  를 클릭하여 패키지를 업로드합니다. 체크섬이 일치하지 않으면 AnyConnect 패키지 업로드가 실패합니다. 장애에 대한 자세한 내용은 디바이스의 워크플로우 탭을 참조하십시오.

시작하기 전에

원하는 운영 체제에 대한 "AnyConnect 헤드엔드 배포 패키지"를 다운로드했는지 확인하십시오. 항상 최신 AnyConnect 버전을 다운로드하여 최신 기능, 버그 편집 및 보안 패치가 있는지 확인합니다. 디바이스에서 패키지를 정기적으로 업데이트합니다.



**Note** 운영 체제(Windows, Mac, Linux)별로 AnyConnect 패키지를 하나씩 업로드할 수 있습니다. 지정된 OS 유형의 여러 버전을 업로드할 수는 없습니다.

### Procedure

단계 1 <https://software.cisco.com/download/home/283000185>에서 AnyConnect 패키지를 다운로드합니다.

- EULA에 동의하고 K9(암호화된 이미지) 권한이 있는지 확인합니다.
- 운영 체제에 맞는 "AnyConnect Headend Deployment Package" 패키지를 선택합니다. 패키지 이름은 "anyconnect-win-4.7.04056-webdeploy-k9.pkg"와 유사합니다. Windows, macOS 및 Linux용 별도의 헤드엔드 패키지가 있습니다.

단계 2 AnyConnect 패키지를 원격 HTTP 또는 HTTPS 서버에 업로드합니다. FDM 관리 디바이스에서 HTTP 또는 HTTPS 서버로의 네트워크 경로가 있는지 확인합니다.

**Note** AnyConnect 패키지를 HTTPS 서버에 업로드하는 경우 다음 단계를 수행해야 합니다.

- firewall device manager에서 FDM 관리 디바이스에 있는 해당 서버의 신뢰할 수 있는 CA 인증서를 업로드합니다. 인증서를 업로드하려면 [Firepower Device Manager, 버전 XY용 Cisco Firepower Threat Defense 구성 가이드](#)의 "인증서" 장의 "신뢰할 수 있는 CA 인증서 업로드" 섹션을 참조하십시오.
- HTTPS 서버에 신뢰할 수 있는 CA 인증서를 설치합니다.

단계 3 원격 서버의 URL은 인증 프롬프트가 표시되지 않는 직접 링크여야 합니다. URL이 사전 인증된 경우 RA VPN 마법사의 URL을 지정하여 파일을 다운로드할 수 있습니다.

단계 4 원격 서버 IP 주소가 NAT된 경우 원격 서버 위치의 NAT된 공용 IP 주소를 제공해야 합니다.

### 새 AnyConnect 패키지 업로드

다음 절차를 사용하여 버전 6.5.0을 실행하는 FDM 관리 디바이스에 새 AnyConnect 패키지를 업로드합니다.

### Procedure


단계 1 [RA VPN 구성 생성](#).

단계 2 **AnyConnect Package Detected**(AnyConnect 패키지 감지됨)에서 Windows, Mac 및 Linux 엔드포인트용 개별 패키지를 업로드할 수 있습니다.

단계 3 해당하는 Platform(플랫폼) 필드에서 Windows, Mac 및 Linux와 호환되는 AnyConnect 패키지가 사전 업로드되는 서버의 경로를 지정합니다. 서버 경로의 예:



```
'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg',
'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'
```

- 단계 4  를 클릭하여 패키지를 업로드합니다. CDO는 경로에 연결할 수 있고 지정된 파일 이름이 유효한 패키지인지 확인합니다. 검증에 성공하면 AnyConnect 패키지의 이름이 나타납니다. RA VPN 구성에 FDM 관리 디바이스를 추가하면 AnyConnect 패키지를 해당 디바이스에 업로드할 수 있습니다.
- 단계 5 **OK**(확인)를 클릭합니다. AnyConnect 패키지가 RA VPN 구성에 추가됩니다.
- 단계 6 6단계부터 **RA VPN 구성 생성**을 계속 진행합니다.

### What to do next

VPN 연결을 완료하려면 사용자가 해당 워크스테이션에 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 자세한 내용은 [FDM-관리 디바이스에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법을 참조하십시오.](#)



### 기존 AnyConnect 패키지 교체

AnyConnect 패키지가 디바이스에 이미 있는 경우 RA VPN 마법사에서 확인할 수 있습니다. 드롭다운 목록에서 운영 체제에 대해 사용 가능한 모든 AnyConnect 패키지를 볼 수 있습니다. 목록에서 기존 패키지를 선택하고 새 패키지로 교체할 수 있지만 새 패키지를 목록에 추가할 수는 없습니다.



**Note** 기존 패키지를 새 패키지로 교체하려면 FDM 관리 디바이스가 연결할 수 있는 네트워크의 서버에 새 AnyConnect 패키지가 이미 업로드되어 있는지 확인합니다.

### Procedure


- 단계 1 왼쪽의 CDO 내비게이션 바에서 **VPN > Remote Access VPN**(원격 액세스 VPN)을 클릭합니다.
- 단계 2 수정할 RA VPN 구성을 선택하고 **Actions**(작업) 아래에서 **Edit**(편집)를 클릭합니다.
- 단계 3 **AnyConnect Packages Detected**(AnyConnect 패키지 탐지됨)에서 기존 AnyConnect 패키지 옆에 나타나는  아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 교체할 패키지를 선택하고 **Edit**(편집)를 클릭합니다. 해당 필드에서 기존 패키지가 사라집니다.
- 단계 4 새 AnyConnect 패키지가 사전 로드되는 서버의 경로를 지정하고  을 클릭하여 패키지를 업로드합니다.
- 단계 5 **OK**(확인)를 클릭합니다. 새 AnyConnect 패키지가 RA VPN 구성에 추가됩니다.
- 단계 6 6단계부터 **RA VPN 구성 생성**을 계속 진행합니다.

### AnyConnect 패키지 삭제

## Procedure

단계 1 왼쪽의 CDO 내비게이션 바에서 **VPN > Remote Access VPN**(원격 액세스 VPN)을 클릭합니다.

단계 2 수정할 RA VPN 구성을 선택하고 **Actions**(작업) 아래에서 **Edit**(편집)를 클릭합니다.

단계 3 **AnyConnect Packages Detected**(탐지된 AnyConnect 패키지)에서 삭제할 AnyConnect 패키지 옆에 표시되는  아이콘을 클릭합니다. 운영 체제에 여러 버전의 AnyConnect 패키지가 있는 경우 목록에서 삭제할 패키지를 선택합니다. 해당 필드에서 기존 패키지가 사라집니다.

**Note** 삭제 작업을 중지하고 기존 패키지를 유지하려면 **Cancel**(취소)을 클릭합니다.


단계 4 **OK**(확인)를 클릭합니다. 디바이스의 구성 상태가 '동기화되지 않음' 상태입니다.

**Note** 이 단계에서 삭제 작업을 실행 취소하려면 **Device & Services**(디바이스 및 서비스) 페이지로 이동하여 **Discard Changes**(변경 사항 취소)를 클릭하여 기존 AnyConnect 패키지를 유지합니다.

단계 5 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

## FDM-관리 장치에 대한 ID 소스 구성

Microsoft AD 영역 및 RADIUS 서버와 같은 ID 소스는 조직의 사용자에게 대한 사용자 계정을 정의하는 AAA 서버 및 데이터베이스입니다. 이 정보는 IP 주소와 연결된 사용자 ID를 제공하거나, 원격 액세스 VPN 연결 또는 Cisco Defense Orchestrator 액세스를 인증하는 등 다양한 방식으로 사용할 수 있습니다.

**Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭한 다음  를 클릭하고 > **RA VPN Objects (ASA & FTD)**(RA VPN 개체(ASA 및 FTD)) > **Identity Source**(ID 소스)를 선택하여 소스를 생성합니다. 그런 다음, ID 소스가 필요한 서비스를 구성할 때 이러한 개체를 사용할 수 있습니다. 적절한 필터를 적용하여 기존 소스를 검색하고 관리할 수 있습니다.

### Active Directory 영역

Active Directory에서 사용자 어카운트 및 인증 정보를 제공합니다. AD 영역을 포함하는 구성을 FDM 관리 디바이스에 구축하면 CDO는 AD 서버에서 사용자 및 그룹을 가져옵니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 원격 액세스 VPN(기본 ID 소스로 사용) AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(활성 인증용으로 사용/패시브 인증에 사용되는 사용자 ID 소스로 사용)
- 사용자의 활성 인증을 위한 ID 규칙.

사용자 ID를 사용하여 액세스 제어 규칙을 생성할 수 있습니다. 자세한 내용은 [Firepower ID 정책을 구현하는 방법](#)을 참조하십시오.

CDO는 24시간마다 한 번씩 업데이트된 사용자 그룹 목록을 요청합니다. 규칙에는 최대 50개의 사용자나 그룹을 추가할 수 있으므로 일반적으로는 개별 사용자를 선택하는 것보다 그룹을 선택하는 것이 더 효율적입니다. 예를 들어 엔지니어링 그룹의 개발 네트워크 액세스를 허용하는 규칙을 생성한 다음 네트워크에 대한 기타 모든 액세스를 거부하는 후속 규칙을 생성할 수 있습니다. 그러면 신규 엔지니어에 대해 규칙을 적용하려는 경우 디렉터리 서버의 엔지니어링 그룹에 해당 엔지니어를 추가하기만 하면 됩니다.

**CDO의 Active Directory 영역**

AD ID 개체를 생성할 때 AD 영역을 구성합니다. ID 소스 개체 마법사는 AD 서버에 연결하는 방법 및 네트워크에서 AD 서버의 위치를 결정하는 데 도움이 됩니다.



**Note** CDO에서 AD 영역을 생성하는 경우, CDO는 가맹 ID 소스 개체를 생성할 때와 ID 규칙에 해당 개체를 추가할 때 AD 비밀번호를 기억합니다.

**FDM의 Active Directory 영역**

CDO 개체 마법사에서 FDM에서 생성된 AD 영역 개체를 가리킬 수 있습니다. CDO는 FDM에서 생성된 AD 영역 개체의 AD 비밀번호를 읽지 않습니다. CDO에 올바른 AD 비밀번호를 수동으로 입력해야 합니다.

firewall device manager에서 AD 영역을 구성하려면 디바이스에서 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 재사용 가능한 개체 장의 인증서 정보 및 인증서 구성 섹션을 참조하십시오.

지원되는 디렉터리 서버

Windows Server 2008 및 2012에서 Microsoft AD(Active Directory)를 사용할 수 있습니다.

서버 컨피그레이션과 관련하여 다음 사항에 유의하십시오.

- 사용자 그룹 또는 그룹 내의 사용자에 대해 사용자 제어를 수행하려면 디렉터리 서버에서 사용자 그룹을 구성해야 합니다. 서버가 기본 개체 계층으로 사용자를 구성하는 경우 시스템은 사용자 그룹 제어를 수행할 수 없습니다.
- 디렉터리 서버는 시스템에 대해 다음 표에 나와 있는 필드 이름을 순서대로 사용하여 해당 필드에 대한 사용자 메타데이터를 서버에서 검색해야 합니다.

메타데이터	Active Directory Field(Active Directory 필드)
LDAP user name(LDAP 사용자 이름)	samaccountname
이름	이름
Last Name(성)	sn
email address(이메일 주소)	mail userprincipalname(메일에 값이 없는 경우)

메타데이터	Active Directory Field(Active Directory 필드)
부서	department distinguishedname(부서에 값이 없는 경우)
전화 번호	telephonenumber

## 디렉터리 기본 DN 결정

디렉터리 속성을 구성할 때는 사용자와 그룹에 대한 공통 기본 DN(고유 이름)을 지정해야 합니다. 이 기준은 디렉터리 서버에서 정의되며 네트워크마다 다릅니다. 올바른 기준을 입력해야 ID 정책이 실행됩니다. 기준이 잘못된 경우 시스템이 사용자 또는 그룹 이름을 확인할 수 없으므로 ID 기반 정책이 실행될 수 없습니다.



**Note** 올바른 기준을 가져오려면 디렉터리 서버 담당 관리자에게 문의하십시오.

Active Directory의 경우 도메인 관리자로 AD 서버에 로그인하여 다음과 같이 명령 프롬프트에 **dsquery** 명령을 사용해 기준을 확인하여 올바른 기준을 확인할 수 있습니다.

### 사용자 검색 기준

알려진 사용자 이름(부분 또는 전체)을 포함한 **dsquery user** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 부분 이름 "John\*"를 사용하여 "John"으로 시작되는 모든 사용자에 대한 정보를 반환합니다.

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

### 그룹 검색 기준

알려진 그룹 이름을 포함한 **dsquery group** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어 다음 명령은 그룹 이름 Employees를 사용하여 고유 이름을 반환합니다.

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 그룹 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

ADSI 편집 프로그램을 사용하여 AD 구조를 찾을 수도 있습니다(**Start(시작) > Run(실행) > adsiedit.msc**). ADSI 편집에서 조직 단위(OU), 그룹, 사용자 등의 개체를 마우스 오른쪽 단추로 클릭하고 **Properties(속성)**를 선택하여 고유 이름을 확인합니다. 그러면 DC 값 문자열을 기준으로 복사할 수 있습니다.

기준이 올바른지를 확인하려면 다음 단계를 수행합니다.

## Procedure

- 단계 1 디렉터리 속성의 **Test Connection**(연결 테스트) 버튼을 클릭하여 연결을 확인합니다. 모든 문제를 해결하고 디렉터리 속성을 저장합니다.
- 단계 2 디바이스에 변경 사항을 커밋합니다.
- 단계 3 액세스 규칙을 생성하고 **Users**(사용자) 탭을 선택한 다음 디렉터리에서 알려진 사용자 및 그룹 이름을 추가해 봅니다. 디렉터리가 포함된 영역에서 일치하는 사용자 및 그룹을 입력하면 자동 완성 제안 사항이 표시됩니다. 이러한 제안 사항이 드롭다운 목록에 표시되는 경우 시스템이 디렉터리를 정상적으로 쿼리한 것입니다. 입력한 문자열이 사용자 또는 그룹 이름에 포함되어 있는데 제안 사항이 표시되지 않으면 해당하는 검색 기준을 편집해야 합니다.

## What to do next

자세한 내용은 [Active Directory 영역 개체 생성 또는 편집](#)을 참조하십시오.

## RADIUS 서버 및 그룹

RADIUS 서버를 사용하여 관리 사용자를 인증하고 권한을 부여할 수 있습니다.

RADIUS 서버를 사용하도록 기능을 구성할 때는 개별 서버 대신 RADIUS 그룹을 선택합니다. RADIUS 그룹은 서로의 복사본인 RADIUS 서버가 모인 컬렉션입니다. 그룹에 서버가 여러 개 포함된 경우 이러한 서버는 백업 서버 체인을 형성하여 한 서버를 사용할 수 없는 경우 이중화를 제공합니다. 하지만 서버가 하나뿐이더라도 멤버가 하나인 그룹을 생성하여 기능에 대한 RADIUS 지원을 구성해야 합니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 인증용 ID 소스이자 권한 부여 및 과금 용도의 원격 액세스 VPN. AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)

자세한 내용은 [RADIUS 서버 개체 또는 그룹 생성 또는 편집](#)을 참조하십시오.

관련 정보:

- [Active Directory 영역 개체 생성 또는 편집](#)
- [RADIUS 서버 개체 또는 그룹 생성 또는 편집](#)
- [ID 정책 구성](#)

## Active Directory 영역 개체 생성 또는 편집

### Active Directory 영역 개체 정보


AD 영역 개체와 같은 ID 소스 개체를 생성하거나 편집할 때 Cisco Defense Orchestrator는 SDC를 통해 FDM 관리 디바이스에 구성 요청을 보냅니다. 그런 다음 FDM 관리 장치는 구성된 AD 영역과 통신합니다.

CDO는 firewall device manager 콘솔을 통해 구성된 AD 영역의 디렉터리 비밀번호를 읽지 않습니다. 원래 firewall device manager에서 생성된 AD 영역 개체를 사용하는 경우 디렉터리 비밀번호를 수동으로 입력해야 합니다.

## FTD Active Directory 영역 개체 생성

개체를 생성하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2  를 클릭한 다음, **RA VPN Objects(개체) (ASA & FTD) > Identity Source(ID 소스)**를 클릭합니다.
- 단계 3 개체의 **Object name(개체 이름)**을 입력합니다.
- 단계 4 **Device Type(장치 유형)**을 **FTD**로 선택합니다.
- 단계 5 마법사의 첫 번째 부분에서 **ID 소스 유형**으로 **Active Directory** 영역을 선택합니다. **Continue(계속)**를 클릭합니다.
- 단계 6 기본 영역 속성을 구성합니다.
  - 디렉터리 사용자 이름, 디렉터리 암호- 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유한 사용자 이름과 암호입니다. AD의 경우 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 정규화되어야 합니다. 예를 들어 [Administrator@example.com](#)(단순히 Administrator가 아님)입니다.
  - Note** 시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 [Administrator@example.com](#)은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환의 일부이므로 여기에서 일반 이름 "users" 폴더 아래에 지정하는 사용자를 구성해야 합니다.
  - **Base Distinguished Name(기본 고유 이름)**- 사용자 및 그룹 정보를 검색하거나 조회하기 위한 디렉터리 트리, 즉 사용자 및 그룹의 공통 상위. cn=users,dc=example,dc=com을 예로 들 수 있습니다.
  - **AD 기본 도메인**- 디바이스가 가입해야 하는 정규화된 AD 도메인 이름입니다. 예를 들어 example.com입니다.
- 단계 7 디렉터리 서버 속성을 구성합니다.
  - **Hostname/IP Address(호스트 이름/IP 주소)**- 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.
  - **Port(포트)**- 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.

- **Encryption(암호화)** - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려는 경우에는 **STARTTLS** 또는 **LDAPS** 중에서 원하는 방법을 선택합니다. 기본값은 **None(없음)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.
  - **STARTTLS**는 암호화 방법을 협상하여 디렉토리 서버가 지원하는 가장 강력한 방법을 사용하며 포트 389를 사용합니다. 원격 액세스 VPN에 영역을 사용하는 경우에는 이 옵션이 지원되지 않습니다.
  - **LDAPS**를 선택하는 경우 LDAP over SSL이 필요합니다. 이 옵션은 포트 636을 사용합니다.
- **Trusted CA Certificate(신뢰할 수 있는 CA 인증서)** - 암호화 방법을 선택하는 경우 CA(인증 증명) 인증서를 업로드하여 시스템과 디렉토리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

단계 8 (선택 사항) **Test(테스트)** 버튼을 사용하여 구성을 확인합니다.

단계 9 (선택 사항) AD 영역에 여러 AD 서버를 추가하려면 **Add another configuration(다른 구성 추가)**를 클릭합니다. 이 AD 서버들은 서로의 중복이어야 하고 동일한 AD 도메인을 지원해야 합니다. 따라서 디렉터리 이름, 디렉터리 암호 및 기본 고유 이름과 같은 기본 영역 속성은 해당 AD 영역과 연결된 모든 AD 서버에서 동일해야 합니다.

단계 10 **Add(추가)**를 클릭합니다.

단계 11 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## FTD Active Directory 영역 개체 편집


ID 소스 개체를 편집할 때는 ID 소스 유형을 변경할 수 없습니다. 올바른 유형으로 새 개체를 생성해야 합니다.

### Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 편집할 개체를 선택합니다.

단계 4 세부정보 패널의 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 5 위의 절차에서 만든 것과 같은 방식으로 대화 상자에서 값을 편집합니다. 아래 나열된 구성 표시줄을 확장하여 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트합니다.

단계 6 **Save(저장)**를 클릭합니다.

단계 7 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 8 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

관련 정보:

- RADIUS 서버 개체 또는 그룹 생성 또는 편집
- ID 정책 구성
- ID 규칙 구성
- ID 정책 설정 구성

RADIUS 서버 개체 또는 그룹 생성 또는 편집

**RADIUS** 서버 개체 또는 그룹 정보

RADIUS 서버 개체 또는 RADIUS 서버 개체 그룹과 같은 ID 소스 개체를 생성하거나 편집할 때 CDO는 SDC를 통해 FDM 관리 디바이스에 구성 요청을 보냅니다. 그런 다음 FDM 관리 디바이스는 구성된 AD 영역과 통신합니다.

RADIUS 서버 개체 생성

RADIUS 서버는 AAA(인증, 권한 부여 및 계정 관리) 서비스를 제공합니다.

개체를 생성하려면 다음 절차를 따르십시오.

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2  를 클릭한 다음, **RA VPN Objects(개체) (ASA & FTD) > Identity Source(ID 소스)**를 클릭합니다.

단계 3 개체의 **Object name(개체 이름)**을 입력합니다.

단계 4 장치 유형 으로 **FTD**를 선택합니다.

단계 5 ID 소스 유형으로 **RADIUS** 서버를 선택합니다. **Continue(계속)**를 클릭합니다.

단계 6 다음 속성을 사용하여 ID 소스 구성을 편집합니다.

- **Server Name or IP Address(서버 이름 또는 IP 주소)** - 서버의 정규화된 호스트 이름(FQDN) 또는 IP 주소입니다.
- **Authentication Port(인증 포트)(선택 사항)** - RADIUS 인증 및 권한 부여가 수행되는 포트입니다. 기본값은 1,812입니다.
- **Timeout(시간 제한)** - 시스템이 다음 서버로 요청을 보내기 전까지 서버의 응답을 기다리는 시간 (1~300초)입니다. 기본값은 10초입니다.
- **서버 비밀 키입력(선택 사항)** - Firepower Threat Defense 디바이스와 RADIUS 서버 간에 데이터를 암호화하는 데 사용되는 공유 비밀입니다. 이 키는 대/소문자를 구분하며 공백은 포함하지 않는 영숫자 문자열(최대 64자)입니다. 또한 영숫자 문자 또는 밑줄로 시작해야 하며 특수 문자 \$ & -



\_, + @는 포함할 수 없습니다. 문자열은 RADIUS 서버에 구성된 것과 일치해야 합니다. 비밀번호를 구성하지 않으면 연결이 암호화되지 않습니다.

단계 7 네트워크에 대해 Cisco ISE(Identity Services Engine)가 이미 구성되어 있고 원격 액세스를 위해 서버를 사용하는 경우 VPN 인증 변경 구성, **RA VPN** 전용 링크를 클릭하고 다음을 구성합니다.

- **ACL** 리디렉션 - RA VPN 리디렉션 ACL에 사용할 확장 ACL(액세스 제어 목록)을 선택합니다. 확장 ACL이 없는 경우 FDM 관리 디바이스 콘솔의 Smart CLI 템플릿에서 필요한 확장 ACL 개체를 생성해야 합니다. 디바이스가 실행 중인 버전은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 고급 구성 장에서 스마트 CLI 개체 구성 섹션을 참조하십시오. 리디렉션 ACL의 목적은 초기 트래픽을 USE로 보내 클라이언트 상태를 평가하는 것입니다. ACL에서는 ISE에 HTTPS 트래픽을 전송해야 하지만, 이미 ISE가 대상으로 지정된 트래픽 또는 이름 확인을 위해 DNS 서버로 전송되는 트래픽은 전송해서는 안 됩니다. 디바이스가 실행 중인 버전은 [Firepower Device Manager용 Cisco Firepower Threat Defense 컨피그레이션 가이드](#)의 VPN(가상 프라이빗망) 장에서 권한 변경 구성 섹션을 참조하십시오.
- 진단 인터페이스- 이 옵션을 활성화하면 시스템이 항상 "진단" 인터페이스를 사용하여 서버와 통신할 수 있습니다. 이 기능을 비활성화된 상태로 두면 CDO는 기본적으로 라우팅 테이블을 사용하여 사용할 인터페이스를 결정합니다.

단계 8 **Add**(추가)를 클릭합니다.

단계 9 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## RADIUS 서버 그룹 생성

RADIUS 서버 그룹은 하나 이상의 RADIUS 서버 개체를 포함합니다. 그룹 내의 서버는 서로의 복사본이어야 합니다. 이러한 서버는 백업 서버 체인을 형성하므로 첫 번째 서버를 사용할 수 없는 경우 시스템이 목록의 다음 서버 사용을 시도할 수 있습니다.

개체 그룹을 생성하려면 다음 절차를 따르십시오.

### Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.

단계 2  를 클릭한 다음 **FTD > Identity Source**(ID 소스)를 클릭합니다.

단계 3 개체의 **Object name**(개체 이름)을 입력합니다.


단계 4 **Device Type**(장치 유형)을 **FTD**로 선택합니다.

단계 5 ID 소스 유형으로 **RADIUS Server Group**(RADIUS 서버 그룹)을 선택합니다. **Continue**(계속)를 클릭합니다.

단계 6 다음 속성을 사용하여 ID 소스 구성을 편집합니다.

- 데드 타임 - 실패한 서버는 모든 서버가 실패한 후에만 재활성화됩니다. 데드 시간은 모든 서버를 다시 활성화하기 전에 마지막 서버가 실패한 후 대기하는 시간입니다.


- **Maximum Failed Attempts(최대 실패 시도 횟수)**- 다음 서버 사용을 시도하기 전에 그룹의 RADIUS 서버로 전송되었으나 실패한 요청(즉, 응답을 받지 못한 요청)의 수입니다. 최대 실패 시도 횟수가 초과되면 시스템에서 해당 서버를 **Failed(장애 발생)**로 표시합니다. 특정 기능에 대해 로컬 데이터베이스를 사용하여 대체 방법을 구성했는데 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 대체 방법을 시도합니다. 서버 그룹은 데드 타임 동안 응답하지 않는 것으로 표시된 상태를 유지하므로 해당 기간 내의 추가 AAA 요청은 서버 그룹에 연결을 시도하지 않으며 폴백 방법이 즉시 사용됩니다.
- **Dynamic Authorization/Port(동적 인증/포트) (선택사항)** - RADIUS 동적 인증 또는 이 RADIUS 서버 그룹에 대한 CoA(Change of Authorization) 서비스를 활성화할 경우, 해당 그룹은 CoA 알림이 등록되며 Cisco ISE(Identity Services Engine)의 CoA 정책 업데이트를 위해 지정된 포트를 수신합니다. ISE와 함께 원격 액세스 VPN에서 이 서버 그룹을 사용하는 경우에만 동적 인증을 활성화합니다.

- 단계 7 드롭다운 메뉴에서 RADIUS 서버를 지원하는 AD 영역을 선택합니다. AD 영역을 아직 생성하지 않은 경우 드롭다운 메뉴에서 **Create(생성)**를 클릭합니다.
- 단계 8 기존 RADIUS 서버 개체를 추가하려면 **Add(추가)** 버튼  를 클릭합니다. 선택사항으로 이 창에서 새 RADIUS 서버 개체를 만들 수 있습니다.
- Note** 목록의 첫 번째 서버가 응답하지 않을 때까지 사용되므로 이러한 개체를 우선 순위에 추가하십시오. FDM 관리 디바이스는 목록의 다음 서버로 기본 설정됩니다.
- 단계 9 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## RADIUS 서버 개체 또는 그룹 편집

Radius 서버 개체 또는 Radius 서버 그룹을 편집하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.
- 단계 3 편집할 개체를 선택합니다.
- 단계 4 세부정보 패널의 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.
- 단계 5 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 편집합니다. 호스트 이름/IP 주소 또는 암호화 정보를 편집하거나 테스트하려면 구성 표시줄을 확장합니다.
- 단계 6 **Save(저장)**를 클릭합니다.
- 단계 7 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 8 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 여러 변경 사항을 여러 변경 사항을 한 번에 배포합니다.

### 새 RA VPN 그룹 정책 생성

그룹 정책은 원격 액세스 VPN 연결을 위한 사용자 중심 속성/값 쌍의 집합입니다. 연결 프로파일은 터널이 설정된 이후에 사용자 연결을 위한 조건을 설정하는 그룹 정책을 사용합니다. 그룹 정책을 사용하면 각 사용자에게 대해 개별적으로 각 특성을 지정할 필요 없이 사용자 또는 사용자 그룹에 전체 특성 집합을 적용할 수 있습니다.

시스템에는 "DfltGrpPolicy"라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.



**Note** 일치하지 않는 그룹 정책 개체를 RA VPN 구성에 추가할 수 없습니다. RA VPN 구성 그룹 정책을 추가하기 전에 모든 불일치를 해결하십시오.

### Procedure

단계 1 왼쪽 Cisco Defense Orchestrator 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 파란색 더하기  버튼을 클릭합니다.

단계 3 **RA VPN Objects(개체) (ASA & FTD) > RA VPN Group Policy(그룹 정책)**을 클릭합니다.

단계 4 그룹 정책의 이름을 입력합니다. 이름은 최대 64자까지 입력할 수 있고 공백이 허용됩니다.

단계 5 **Device Type(디바이스 유형)** 드롭다운에서 **FTD**를 선택합니다.

단계 6 다음 중 하나를 수행합니다.

- 필요한 탭을 클릭하고 페이지에서 속성을 구성합니다.
  - [RA VPN 그룹 정책 속성](#)
  - [AnyConnect 클라이언트 프로파일, on page 534](#)
  - [세션 설정 속성, on page 535](#)
  - [주소 할당 속성, on page 536](#)
  - [스플릿 터널링 속성, on page 536](#)
  - [AnyConnect 속성, on page 537](#)
  - [트래픽 필터 속성, on page 539](#)
  - [Windows 브라우저 프록시 속성, on page 539](#)

단계 7 **Save**(저장)를 클릭하여 그룹 정책을 생성합니다.

## RA VPN 그룹 정책 속성

그룹 정책의 일반 속성에서는 그룹의 이름 및 기타 기본 설정을 정의합니다. Name(이름) 속성만 필수 속성입니다.

- **DNS Server(DNS 서버)**: VPN에 연결할 때 클라이언트가 도메인 이름 확인에 사용해야 하는 DNS 서버를 정의하는 DNS 서버 그룹을 선택합니다. 필요한 그룹이 아직 정의되지 않은 경우, **Create DNS Group(DNS 그룹 생성)**을 클릭하여 바로 생성합니다.
- **Banner(배너)**: 로그인 시 사용자에게 표시할 배너 텍스트 또는 환영 메시지입니다. 기본값은 배너 없음입니다. 길이는 최대 496자까지 가능합니다. AnyConnect 클라이언트에서는 부분 HTML을 지원합니다. 원격 사용자에게 배너가 적절히 표시되게 하려면 <BR> 태그를 사용하여 줄 바꿈을 나타냅니다.
- **Default Domain(기본 도메인)**: RA VPN의 사용자에게 대한 기본 도메인 이름입니다. example.com 등을 예로 들 수 있습니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com)이 아닌 serverA)에 추가됩니다.
- **AnyConnect Client Profiles(AnyConnect 클라이언트 프로파일)**: +를 클릭하고 이 그룹에 사용할 AnyConnect 클라이언트 프로파일을 선택합니다. [RA VPN AnyConnect 클라이언트 프로파일 업로드](#)를 참조하십시오. 연결 프로파일에서 외부 인터페이스에 대해 FQDN(fully-qualified domain name)을 컨피그레이션하는 경우, 기본 프로파일이 생성됩니다. 원하는 클라이언트 프로파일을 직접 업로드할 수도 있습니다. software.cisco.com에서 다운로드하여 설치할 수 있는 독립형 AnyConnect 프로파일 편집기를 사용하여 이러한 프로파일을 생성합니다. 클라이언트 프로파일을 선택하지 않으면 AnyConnect 클라이언트는 모든 옵션에 대해 기본값을 사용합니다. 이 목록의 항목은 프로파일 자체가 아니라 AnyConnect 클라이언트 프로파일 개체입니다. 드롭다운 목록에서 **Create New AnyConnect Client Profile(새 AnyConnect 클라이언트 프로파일 생성)**을 클릭하면 새 프로파일을 생성하고 업로드할 수 있습니다.

### AnyConnect 클라이언트 프로파일

이 기능은 소프트웨어 버전 6.7 이상을 실행하는 firewall device manager에서 지원됩니다.

Cisco AnyConnect VPN 클라이언트는 다양한 내장 모듈을 통해 향상된 보안을 제공합니다. 이러한 모듈은 웹 보안, 엔드 포인트 플로우에 대한 네트워크 가시성, 네트워크 외부 로밍 보호와 같은 서비스를 제공합니다. 각 클라이언트 모듈에는 요구 사항에 따라 사용자 지정 구성 그룹이 포함된 클라이언트 프로파일이 포함되어 있습니다.

VPN 사용자가 VPN AnyConnect 클라이언트 소프트웨어를 다운로드할 때 클라이언트에 다운로드할 AnyConnect VPN 프로파일 개체 및 AnyConnect 모듈을 선택할 수 있습니다.

1. AnyConnect VPN 프로파일 개체를 선택하거나 생성합니다. [RA VPN AnyConnect 클라이언트 프로파일 업로드](#), on page 552의 내용을 참조하십시오. DART 및 Start Before Login(로그인 전 시작) 모듈을 제외하고 AnyConnect VPN 프로파일 개체를 선택해야 합니다.
2. **Add Any Connect Client Module(모든 연결 클라이언트 모듈 추가)**을 클릭합니다.

다음 AnyConnect 모듈은 선택 사항이며 이러한 모듈을 VPN AnyConnect 클라이언트 소프트웨어와 함께 다운로드하도록 구성할 수 있습니다.

- **AMP Enabler** — 엔드포인트용 AMP(Advanced Malware Protection)를 구축합니다.
- **DART** — 시스템 로그 및 기타 진단 정보를 캡처하여 데스크톱에 .zip 파일을 만듭니다. 따라서 편리하게 Cisco TAC로 문제 해결 정보를 보낼 수 있습니다.
- **Feedback(피드백)** - 고객이 활성화하고 사용한 기능 및 모듈에 대한 정보를 제공합니다.
- **ISE Posture: OPSWAT v3** 라이브러리를 사용하여 엔드포인트의 컴플라이언스를 평가하기 위한 상태 확인을 수행합니다.
- **Network Access Manager - 802.1X(계층 2)**와 유선 및 무선 네트워크에 액세스하기 위한 디바이스 인증을 제공합니다.
- **Network Visibility(네트워크 가시성)** — 용량 및 서비스 계획, 감사, 컴플라이언스 및 보안 분석을 수행하기 위한 엔터프라이즈 관리자의 역량을 개선합니다.
- **Start Before Login(로그인 전 시작)** - Windows 로그인 대화 상자가 나타나기 전에 AnyConnect를 시작하여 Windows에 로그인하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다.
- **Umbrella** 로밍 보안 — 활성화 VPN이 없을 때 DNS 레이어 보안을 제공합니다.
- 웹 보안 - 정의된 보안 정책에 따라 웹 페이지의 요소를 분석하고 허용되는 콘텐츠를 허용하며 악성 또는 허용되지 않는 콘텐츠를 차단합니다.

3. 클라이언트 모듈 목록에서 **AnyConnect** 모듈을 선택합니다.

4. **Profile(프로파일)** 목록에서 AnyConnect 클라이언트 프로파일을 포함하는 프로파일 개체를 선택하거나 생성합니다.

5. 프로파일과 함께 클라이언트 모듈을 다운로드하려면 **Enable Module Download(모듈 다운로드 활성화)**를 선택하여 엔드포인트를 활성화합니다. 선택하지 않으면 엔드포인트는 클라이언트 프로파일만 다운로드할 수 있습니다.

### 세션 설정 속성

그룹 정책의 세션 설정에서는 사용자가 VPN을 통해 연결할 수 있는 시간과 설정할 수 있는 별도 연결의 개수를 제어합니다.

- **Maximum Connection Time(최대 연결 시간)**: 사용자가 로그아웃했다가 다시 연결하지 않고 VPN에 연결된 상태를 유지할 수 있는 최대 시간을 1~4473924(분)로 입력하거나 비워 둡니다. 기본값은 무제한(비워 둠)이지만 유희 시간 제한은 계속 적용됩니다.
- **Connection Time Alert Interval(연결 시간 알림 간격)**: 최대 연결 시간을 지정하는 경우, 알림 간격에서는 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 최대 시간을 정의합니다. 사용자는 연결 종료를 선택하고 다시 접속해 타이머를 다시 시작할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.

- **Idle Time**(유휴 시간): VPN 연결이 자동으로 종료될 때까지 유휴 상태일 수 있는 시간을 1~35791394(분) 범위 내로 입력합니다. 이 연속되는 분 단위 시간 동안 연결에서 통신 활동이 없는 경우, 시스템에서는 연결을 중지합니다. 기본값은 30분입니다.
- **Idle Time Alert Interval**(유휴 시간 알림 간격): 유휴 세션으로 인해 사용자에게 앞으로 다가올 자동 연결 해제에 관해 경고를 표시하기까지 지나야 할 유휴 시간입니다. 어떤 활동에서도 타이머를 재설정할 수 있습니다. 기본값은 1분입니다. 1분에서 30분까지 지정할 수 있습니다.
- **Simultaneous Login Per User**(사용자당 동시 로그인 수): 한 사용자에게 허용되는 동시 연결의 최대 개수입니다. 기본값은 3입니다. 1~2147483647개의 연결을 지정할 수 있습니다. 다수의 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.

### 주소 할당 속성

그룹 정책의 주소 할당 속성에서는 그룹에 대해 IP 주소 풀을 정의합니다. 여기에 정의된 풀은 이 그룹을 사용하는 모든 연결 프로파일에 정의된 풀을 재정의합니다. 연결 프로파일에 정의된 풀을 사용하려면 이러한 설정을 비워둡니다.

- **IPv4 Address Pool(IPv4 주소 풀), IPv6 Address Pool(IPv6 주소 풀)**: 이 옵션에서는 원격 엔드포인트의 주소 풀을 정의합니다. 클라이언트가 VPN 연결을 설정하는 데 사용하는 IP 버전에 따라 이러한 풀의 주소가 클라이언트에 할당됩니다. 지원하려는 각 IP 유형에 대한 서브넷을 정의하는 네트워크 개체를 선택합니다. 해당 IP 버전을 지원하고 싶지 않은 경우, 목록을 비워두십시오. 예를 들어 IPv4 풀을 10.100.10.0/24로 정의할 수 있습니다. 주소 풀은 외부 인터페이스의 IP 주소와 동일한 서브넷에 있을 수 없습니다. 로컬 주소 할당에 사용할 최대 6개의 주소 풀로 구성된 목록을 지정할 수 있습니다. 풀을 지정하는 순서는 중요합니다. 시스템에서는 풀이 표시되는 순서에 따라 이 풀에서 주소를 할당합니다.
- **DHCP Scope(DHCP 범위)**: 연결 프로파일에 주소 풀에 대한 DHCP 서버를 컨피그레이션하는 경우, DHCP 범위에서는 이 그룹에 대한 풀에 사용할 서브넷을 식별합니다. 또한 DHCP 서버 주소에는 해당 범위에서 식별하는 동일한 풀에 주소가 있어야 합니다. 이 범위를 통해 사용자는 DHCP 서버에 정의된 주소 풀의 하위 집합을 선택하여 이 특정 그룹에 사용할 수 있습니다. 네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순으로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다. 범위를 지정하려면 네트워크 번호 호스트 주소를 포함하는 네트워크 개체를 선택합니다. 개체가 아직 없는 경우, **Create New Network**(새 네트워크 생성)를 클릭합니다. 예를 들어 192.168.5.0/24 서브넷 풀에서 주소를 사용하도록 DHCP 서버에 지시하려면 192.168.5.0을 호스트 주소로 지정하는 네트워크 개체를 선택하십시오. IPv4 주소 지정에만 DHCP를 사용할 수 있습니다.

### 스플릿 터널링 속성

그룹 정책의 스플릿 터널링 속성에서는 내부 네트워크로 가는 트래픽과 외부로 가는 트래픽을 시스템에서 각각 분별하여 처리하는 방식을 정의합니다. 스플릿 터널링은 일부 네트워크 트래픽이 VPN 터널(암호화됨)을 통과하도록 유도하고 나머지 네트워크 트래픽은 VPN 터널 외부(암호화되지 않음 또는 일반 텍스트 형식)로 보냅니다.

- **IPv4 Split Tunneling(IPv4 스플릿 터널링), IPv6 Split Tunneling(IPv6 스플릿 터널링)**: 트래픽에서 IPv4와 IPv6 중 어떤 주소 지정을 사용하는지에 따라 다른 옵션을 지정할 수 있지만, 각각의

경우 옵션은 동일합니다. 스플릿 터널링을 활성화하려는 경우, 네트워크 개체를 선택해야 하는 옵션 중 하나를 지정합니다.

- **Allow all traffic over tunnel**(터널을 지나는 모든 트래픽 허용): 스플릿 터널링은 실행하지 마십시오. 사용자가 RA VPN 연결을 하면 사용자의 모든 트래픽은 보호된 터널을 통과합니다. 이는 기본값입니다. 또한 이 기본값은 가장 안전한 옵션으로 간주됩니다.
- **Allow specified traffic over tunnel**(터널을 지나는 지정된 트래픽 허용): 대상 네트워크 및 호스트 주소를 정의하는 네트워크 개체를 선택합니다. 이러한 대상으로 가는 모든 트래픽은 보호된 터널을 통과합니다. 클라이언트는 다른 대상으로 가는 트래픽을 터널 외부의 연결(예: 로컬 Wi-Fi 또는 네트워크 연결)로 라우팅합니다.
- **Exclude networks specified below**(아래에 지정된 네트워크 제외): 대상 네트워크 또는 호스트 주소를 정의하는 네트워크 개체를 선택합니다. 클라이언트는 이러한 대상으로 가는 모든 트래픽을 터널 외부 연결로 라우팅합니다. 기타 대상으로 가는 트래픽은 터널을 통과합니다.
- **Split DNS**(스플릿 DNS): 보안 연결을 통해 일부 DNS 요청을 전송하도록 시스템을 구성함과 동시에 클라이언트가 클라이언트에 구성된 DNS 서버로 다른 DNS 요청을 전송하도록 허용할 수 있습니다. 다음 DNS 동작을 컨피그레이션할 수 있습니다.
  - **Send DNS Request as per split tunnel policy**(스플릿 터널 정책에 따라 DNS 요청 전송): 이 옵션을 사용하면 스플릿 터널 옵션을 정의하는 것과 동일한 방식으로 DNS 요청이 처리됩니다. 스플릿 터널링을 활성화하는 경우, DNS 요청은 대상 주소에 근거하여 전송됩니다. 스플릿 터널링을 활성화하지 않는 경우, 모든 DNS 요청은 보호된 연결을 경유해 전송됩니다.
  - **Always send DNS requests over tunnel**(항상 터널을 통해 DNS 요청 전송): 스플릿 터널링을 활성화하되 모든 DNS 요청을 보호된 연결을 경유해 그룹에 정의된 DNS 서버로 전송하려는 경우, 이 옵션을 선택합니다.
  - **Send only specified domains over tunnel**(지정된 도메인만 터널을 통해 전송): 보호된 DNS 서버에서 특정 도메인에 대해서만 주소를 확인하게 하고 싶은 경우, 이 옵션을 선택합니다. 그런 다음, 도메인 이름을 쉼표로 구분하여 해당 도메인을 지정합니다. example.com, example1.com을 예로 들 수 있습니다. 내부 DNS 서버에서는 내부 도메인의 이름을 확인하고 외부 DNS 서버에서는 다른 모든 인터넷 트래픽을 처리하게 하려는 경우, 이 옵션을 사용합니다.

### AnyConnect 속성

그룹 정책의 AnyConnect 속성에서는 원격 액세스 VPN 연결에 대해 AnyConnect 클라이언트에서 사용하는 일부 SSL 및 연결 설정을 정의합니다.

- **SSL 설정**
  - **Enable Datagram Transport Layer Security (DTLS)**(DTLS(Datagram Transport Layer Security) 활성화): AnyConnect 클라이언트에서 2개의 터널(SSL 터널 및 DTLS 터널)을 동시에 사용하도록 허용할지 여부를 선택합니다. DTLS를 사용하면 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능

을 개선할 수 있습니다. DTLS를 활성화하지 않은 경우에는 SSL VPN 연결을 설정하는 AnyConnect 클라이언트 사용자가 SSL 터널만 사용하여 연결합니다.

- **DTLS Compression(DTLS 압축)**: LZS를 사용하여 이 그룹에 대한 DTLS(Datagram Transport Layer Security) 연결을 압축할지 여부를 선택합니다. DTLS 압축은 기본적으로 비활성화되어 있습니다.
- **SSL 압축**: 데이터 압축 활성화 여부를 선택하고, 활성화하는 경우 압축 해제 또는 **LZS** 중 사용할 데이터 압축 방법을 선택합니다. SSL 압축은 기본적으로 **Disabled**(비활성화) 상태입니다. 데이터를 압축하면 전송 속도가 빨라지지만 각 사용자 세션에 대한 메모리 요건 및 CPU 사용량이 증가합니다. 따라서 SSL 압축으로 인해 디바이스의 전체 처리량은 줄어듭니다.
- **SSL Rekey Method(SSL 키 재입력 방법)**, **SSL Rekey Interval(SSL 키 재입력 간격)**: 클라이언트는 VPN 연결에 키를 재입력하여 암호화 키 및 초기화 벡터를 재협상할 수 있어 연결 보안이 강화됩니다. **None**(없음)을 선택하여 키 재입력을 비활성화합니다. 키 재입력을 활성화하려면 **New Tunnel**(새 터널)을 선택하여 매번 새 터널을 생성합니다. (**Existing Tunnel**(기존 터널) 옵션을 선택하면 **New Tunnel**(새 터널)과 동일한 조치가 수행됩니다.) 키 재입력을 활성화하는 경우, 키 재입력 간격도 설정하십시오. 기본값은 4분입니다. 4~10080분(일주일) 범위 내에서 간격을 설정할 수 있습니다.

#### • Connection Settings(연결 설정)

- **Ignore the DF (Don't Fragment) bit(DF(Don't Fragment) 비트 무시)**: 단편화해야 하는 패킷에서 DF(Don't Fragment) 비트를 무시할지 여부를 선택합니다. 이 옵션을 선택하면 DF 비트가 설정된 패킷의 강제 단편화가 허용되므로 이 패킷이 터널을 통과할 수 있습니다.
- **Client Bypass Protocol**(클라이언트 우회 프로토콜): 이 옵션을 선택하면 보안 게이트웨이에서 IPv6 트래픽만 예상할 때 IPv4 트래픽을 관리하는 방법 또는 IPv4 트래픽만 예상할 때 IPv6 트래픽을 관리하는 방법을 구성할 수 있습니다.

AnyConnect 클라이언트에서 헤드엔드와의 VPN 연결을 수행할 때 헤드엔드에서는 IPv4 주소나 IPv6 주소 또는 IPv4 및 IPv6 주소 모두를 지정합니다. 헤드엔드에서 AnyConnect 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, 헤드엔드에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 헤드엔드를 우회하여 암호화되지 않은 또는 “일반 텍스트” 형태(활성화 및 확인된 상태)로 클라이언트에서 전송되는 것을 허용하도록 Client Bypass Protocol(클라이언트 우회 프로토콜)을 컨피그레이션할 수 있습니다.

예를 들어 보안 게이트웨이에서 AnyConnect 연결에 IPv4 주소만 지정하고 엔드포인트는 이중 스택이라고 가정합니다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회 프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.

- **MTU**: Cisco AnyConnect VPN 클라이언트에서 설정한 SSL VPN 연결의 MTU(Maximum Transmission Unit)입니다. 기본값은 1406바이트입니다. 범위는 576~1462바이트입니다.
  - **Keepalive Messages Between AnyConnect and VPN Gateway(AnyConnect와 VPN 게이트웨이 간의 연결 유지 메시지)**: 피어 간에 연결 유지 메시지를 교환하여 터널에서 데이터를 송수신하는 데 사용할 수 있다는 것을 시연할지 여부를 선택합니다. 연결 유지 메시지는 설정된 간격에 따라 전송됩니다. 기본 간격은 20초, 유효 범위는 15~600초입니다.



- **DPD on Gateway Side Interval**(게이트웨이 측 간격의 DPD), **DPD on Client Side Interval**(클라이언트 측 간격의 DPD): DPD(Dead Peer Detection)를 활성화하면 피어가 더 이상 응답하지 않을 경우 VPN 게이트웨이 또는 VPN 클라이언트를 신속하게 탐지할 수 있습니다. 게이트웨이 또는 클라이언트 DPD를 별도로 활성화할 수 있습니다. DPD 메시지 전송의 기본 간격은 30초입니다. 간격은 5-3600초 사이일 수 있습니다.

### 트래픽 필터 속성

그룹 정책의 트래픽 필터 속성에서는 그룹에 할당된 사용자에게 부과하고 싶은 제한 사항을 정의합니다. 액세스 제어 정책 규칙을 생성하는 대신 이 속성을 사용해 RA VPN 사용자를 호스트 또는 서브넷 주소 및 프로토콜, VLAN에 따라 특정 리소스로 제한할 수 있습니다. 기본적으로 그룹 정책에 따라 RA VPN 사용자는 보호된 네트워크의 어떤 대상에 액세스하는 것도 제한되지 않습니다.

- **Access List Filter**(액세스 목록 필터): 확장된 ACL(액세스 제어 목록)을 사용하여 액세스를 제한합니다. Smart CLI 확장 ACL 개체를 선택합니다. 확장 ACL을 통해 소스 주소, 대상 주소 및 프로토콜(예: IP 또는 TCP)을 기준으로 필터링할 수 있습니다. ACL은 하향식, 최초 일치 방식에 따라 평가되므로 특정 규칙이 다수의 일반 규칙보다 먼저 배치되도록 보장합니다. ACL의 끝에는 암묵적 "deny any(모두 거부)"가 있으므로 서브넷 몇 개에 대한 액세스만 거부하고 다른 모든 액세스는 허용하려면 ACL의 끝에 "permit any(모두 허용)" 규칙을 포함하십시오. 확장 ACL 스마트 CLI 개체를 수정하는 중에는 네트워크 개체를 생성할 수 없으므로 그룹 정책을 수정하기 전에 ACL을 생성해야 합니다. 그러지 않는 경우, 개체만 생성할 수 있습니다. 그런 다음 다시 돌아가 네트워크 개체를 생성한 후 필요한 모든 액세스 제어 항목을 생성하면 됩니다. ACL을 생성하려면 firewall device manager에 로그인하고 **Device**(디바이스) > **Advanced Configuration**(고급 구성) > **Smart CLI**(스마트 CLI) > **Objects**(개체)로 이동하여 개체를 생성하고 **Extended Access List**(확장 액세스 목록)를 개체 유형으로 선택합니다.
- **Restrict VPN to VLAN**(VPN을 VLAN으로 제한): "VLAN 매핑"이라고도 하는 이 속성에서는 이 그룹 정책이 적용되는 세션에 이그레스(egress) VLAN 인터페이스를 지정합니다. 시스템에서는 이 그룹에서 나오는 모든 트래픽을 선택한 VLAN으로 전달합니다. 이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 속성에 값을 할당하는 방법도 가능합니다. 디바이스에서 하위 인터페이스에 정의된 VLAN 번호를 반드시 지정하십시오. 값의 범위는 1에서 4094까지입니다.

### Windows 브라우저 프록시 속성

그룹 정책의 Windows 브라우저 프록시 속성에서는 사용자의 브라우저에 정의된 프록시의 작동 방식과 작동 여부를 결정합니다.

**Browser Proxy During VPN Session**(VPN 세션 중 브라우저 프록시)에 대해 다음 값 중 하나를 선택할 수 있습니다.

- **No change in endpoint settings**(엔드포인트 설정에 변경 사항 없음): 이 옵션을 통해 사용자는 HTTP에 대해 브라우저 프록시를 컨피그레이션하거나 컨피그레이션하지 않을 수 있으며 컨피그레이션되어 있는 경우 프록시를 사용할 수 있습니다.
- **Disable browser proxy**(브라우저 프록시 비활성화): 브라우저에 대해 정의된 프록시(있는 경우)를 사용하지 않습니다. 이 경우 프록시를 통해 브라우저 연결이 설정되지 않습니다.

- **Auto detect settings**(설정 자동 탐지): 클라이언트 디바이스에 대해 브라우저에서 자동 프록시 서버 감지를 사용하도록 활성화합니다.
- **Use custom settings**(사용자 정의 설정 사용): HTTP 트래픽에 대해 모든 클라이언트 디바이스에서 사용해야 하는 프록시를 정의합니다. 다음 설정을 구성합니다.
  - **Proxy Server IP or Hostname**(프록시 서버 IP 또는 호스트네임), **Port**(포트): 프록시 서버의 IP 주소 또는 호스트네임, 프록시 서버에서 프록시 연결에 사용하는 포트입니다. 호스트와 포트를 합해 100자를 초과할 수 없습니다.
  - **Browser Exemption List**(브라우저 면제 목록): 면제 목록의 호스트/포트에 대한 연결은 프록시를 통과하지 않습니다. 프록시를 사용해서는 안 되는 대상에 대해 모든 호스트/포트 값을 추가합니다. [www.example.com](http://www.example.com) port 80을 예로 들 수 있습니다. 목록에 항목을 추가하려면 **Add Proxy Exemption**(프록시 예외 추가)을 클릭합니다. 항목을 삭제하려면 휴지통 아이콘을 클릭합니다. 모든 주소와 포트를 합한 전체 프록시 예외 목록은 255자를 초과할 수 없습니다.

## RA VPN 구성 생성

CDO를 사용하면 RA VPN 구성 마법사에 하나 이상의 FDM 관리 디바이스를 추가하고 디바이스와 연결된 VPN 인터페이스, 액세스 제어 및 NAT 면제 설정을 구성할 수 있습니다. 따라서 각 RA VPN 구성에는 RA VPN 구성과 연결된 여러 FDM 관리 디바이스에서 공유되는 연결 프로파일 및 그룹 정책이 있을 수 있습니다. 또한 연결 프로파일 및 그룹 정책을 생성하여 구성을 개선할 수 있습니다.

RA VPN 설정으로 이미 구성된 FDM 관리 디바이스 또는 RA VPN 설정이 없는 새 디바이스를 온보딩할 수 있습니다. 이미 RA VPN 설정이 있는 FDM 관리 디바이스를 온보딩하는 경우 CDO는 자동으로 "기본 RA VPN 구성"을 생성하고 FDM 관리 디바이스를 이 구성과 연결합니다. 또한 이 기본 구성은 디바이스에 정의된 모든 연결 프로파일 개체를 포함할 수 있습니다.



### Important

- 동일한 원격 액세스 VPN 구성에서 ASA 및 FDM 관리 디바이스를 추가할 수 없습니다.
- FDM 관리 디바이스는 두 개 이상의 RA VPN 구성을 가질 수 없습니다.

### 사전 요구 사항



RA VPN 구성에 FDM 관리 디바이스를 추가하기 전에 다음 사전 요구 사항을 충족해야 합니다.

- FDM 관리 디바이스에 다음이 있는지 확인합니다.
  - 유효한 라이선스. 자세한 내용은 [원격 액세스 VPN에 대한 라이선싱 요구 사항](#)을 참조하십시오.
  - FDM 버전 6.4.0의 경우, 최소 하나의 AnyConnect 소프트웨어 패키지가 디바이스에 사전 업로드되었는지 확인합니다. 자세한 내용은 [버전 6.4.0을 실행하는 FDM-관리 디바이스에서 AnyConnect 패키지 업그레이드](#)를 참조하십시오.

- FDM 버전 6.5.0+의 경우 CDO를 사용하여 AnyConnect 패키지를 업로드할 수 있습니다. 자세한 내용은 [버전 6.5 이상을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드](#)를 참조하십시오.
- 보류 중인 구성 배포가 없습니다.
- FDM 변경 사항은 CDO에 동기화됩니다.
  1. 왼쪽의 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭하고 동기화할 하나 이상의 FDM 관리 디바이스를 검색합니다.
  2. 하나 이상의 디바이스를 선택한 다음 **Check for changes**(변경 사항 확인)를 클릭합니다. CDO는 하나 이상의 FDM 관리 디바이스와 통신하여 변경 사항을 동기화합니다.
- RA VPN 구성 그룹 정책 개체가 일치합니다.
  - 일치하지 않는 모든 그룹 정책 개체는 RA VPN 구성에 추가할 수 없으므로 확인해야 합니다. 문제를 해결하거나 **Objects**(개체) 페이지에서 일치하지 않는 그룹 정책 개체를 제거합니다. 자세한 내용은 [중복 개체 문제 해결 및 불일치 개체 문제 해결](#)을 참조하십시오.
- FDM 관리 디바이스의 RA VPN 그룹 정책이 RA VPN 구성 그룹 정책과 일치합니다.

## 절차

## Procedure

- 단계 1 왼쪽의 Cisco Defense Orchestrator 탐색 모음에서 **VPN** > 원격 액세스 **VPN** 구성을 클릭합니다.
- 단계 2 파란색 더하기  버튼을 클릭하여 새 RA VPN 구성을 생성합니다.
- 단계 3 원격 액세스 VPN 구성의 이름을 입력합니다.
- 단계 4 파란색 더하기  버튼을 클릭하여 FDM 관리 디바이스를 구성에 추가합니다. 디바이스 세부 정보를 추가하고 디바이스와 연결된 네트워크 트래픽 관련 권한을 구성할 수 있습니다.
  - a. 다음 디바이스 세부 사항을 입력합니다.
    - 디바이스: 추가할 FDM 관리 디바이스를 선택하고 **Select**(선택)를 클릭합니다.
    - Important** 동일한 원격 액세스 VPN 구성에서 ASA 및 FDM 관리 디바이스를 추가할 수 없습니다.
    - **Certificate of Device Identity**(디바이스 ID의 인증서): 디바이스의 ID를 설정하는 데 사용되는 내부 인증서를 선택합니다. 그러면 AnyConnect 클라이언트가 디바이스에 연결할 때 디바이스 ID를 설정합니다. 보안 VPN 연결을 완료하려면 클라이언트가 이 인증서를 허용해야 합니다. 인증서가 아직 없는 경우 드롭다운 목록에서 **Create New Internal Certificate**(새 내부 인증서 생성)를 클릭합니다. [자체 서명 내부 및 내부 CA 인증서 생성](#)을 참조하십시오.

- **Outside Interface(외부 인터페이스)**: 사용자가 원격 액세스 VPN 연결을 설정할 때 연결하는 인터페이스입니다. 이 인터페이스는 대개 외부(인터넷 연결) 인터페이스이지만, 이 연결 프로파일을 사용하여 지원하려는 디바이스와 엔드 유저 간의 인터페이스를 선택하면 됩니다. 새 하위 인터페이스를 생성하려면 **Firepower VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성**을 참조하십시오.
- 외부 인터페이스의 **FQDN(Fully-Qualified Domain Name)** 또는 **IP: ravpn.example.com**과 같은 인터페이스의 이름 또는 IP 주소를 제공해야 합니다. 이름을 지정하는 경우 시스템이 클라이언트 프로파일을 자동으로 생성할 수 있습니다. 참고:VPN과 클라이언트에 사용되는 DNS 서버가 외부 인터페이스 IP 주소에 대해 이 이름을 확인할 수 있도록 해야 합니다. 관련 DNS 서버에 FQDN을 추가합니다.

**b. Continue(계속)**를 클릭하여 트래픽 권한을 구성합니다.

- **Bypass Access Control policy for decrypted traffic(암호 해독된 트래픽에 대해 액세스 제어 정책 우회)(sysopt permit-vpn)**: 암호 해독된 트래픽은 기본적으로 액세스 제어 정책 검사를 받습니다. 이 옵션을 활성화하면 암호 해독된 트래픽 옵션이 액세스 제어 정책 검사를 무시하지만, VPN 필터 ACL과 AAA 서버에서 다운로드한 인증 ACL이 VPN 트래픽에 계속 적용됩니다. 이 옵션을 선택하는 경우, 시스템에서는 전역 설정인 `sysopt connection permit-vpn` 명령을 구성한다는 점에 유의하십시오. 이로 인해 Site-to-Site VPN 연결의 동작도 영향을 받습니다. 이 옵션을 선택하지 않는 경우, 외부 사용자가 원격 액세스 VPN 주소 풀의 IP 주소를 스푸핑할 수 있고, 따라서 네트워크에 액세스할 수 있습니다. 이것이 가능한 이유는 주소 풀에서 내부 리소스에 액세스할 수 있게 허용하는 액세스 제어 규칙을 생성해야 하기 때문입니다. 액세스 제어 규칙을 사용하는 경우, 소스 IP 주소만 사용하기보다 사용자 사양을 이용해 액세스를 제어하는 것이 좋습니다. 이 옵션을 선택할 경우의 단점은 VPN 트래픽이 검사되지 않는다는 것입니다. 즉 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다.
- **NAT Exempt(NAT 제외)**: NAT 변환에서 원격 액세스 VPN 엔드포인트와 주고받는 트래픽을 제외하려면 NAT 제외를 활성화합니다. NAT에서 VPN 트래픽을 제외하지 않는 경우 내부 인터페이스와 외부 인터페이스에 대한 기존 NAT 규칙이 주소의 RA VPN 풀에 적용되지 않는지 확인합니다. NAT 제외 규칙은 지정된 소스/대상 인터페이스 및 네트워크 조합에 대한 수동 고정 ID NAT 규칙이며 NAT 정책에서는 반영되지 않고 숨겨집니다. NAT 제외를 활성화하는 경우에는 다음 항목도 구성해야 합니다.
  - 내부 인터페이스: 원격 사용자가 액세스할 내부 네트워크의 인터페이스를 선택합니다. NAT 규칙은 이러한 인터페이스에 대해 생성됩니다.
  - 내부 네트워크: 원격 사용자가 액세스할 내부 네트워크를 나타내는 네트워크 개체를 선택합니다. 네트워크 목록에는 지원할 주소 풀과 동일한 IP 유형이 포함되어 있어야 합니다.

단계 5 확인을 클릭합니다.

- firewall device manager 버전 6.4.0 디바이스를 온보딩한 경우, 탐지된 **AnyConnect** 패키지에 디바이스에서 사용 가능한 AnyConnect 패키지가 표시됩니다.

- firewall device manager 버전 6.5.0 이상 디바이스를 온보딩한 경우 AnyConnect 패키지가 사전 업로드된 서버에서 AnyConnect 패키지를 추가해야 합니다. 지침은 [버전 6.5 이상을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드](#)를 참조하십시오.

단계 6 **OK**(확인)를 클릭합니다. 디바이스가 구성에 추가됩니다.

### What to do next



**Note** 구성을 선택하고 **Actions**(작업) 아래에서 적절한 작업을 클릭합니다.



- **Group Policies**(그룹 정책) - 그룹 정책을 추가하거나 제거합니다.
  - +를 클릭하여 필요한 그룹 정책을 선택합니다. 새 RA VPN 그룹 정책을 만들려면 [새 RA VPN 그룹 정책 생성](#)을 참조하십시오.
- **Remove**(제거) - 선택한 RA VPN 구성을 삭제합니다.

### RA VPN 구성 수정

기존 RA VPN 구성의 이름 및 디바이스 세부 정보를 수정할 수 있습니다.

### Procedure

수정할 구성을 선택하고 **Actions**(작업) 아래에서 **Edit**(편집)를 클릭합니다.

- 필요한 경우 이름을 수정합니다.
- 디바이스를 추가하려면 파란색 더하기 버튼  을 클릭합니다.
-  를 클릭하여 FDM 관리 디바이스에서 다음을 수행합니다.
  - **Edit**(편집)를 클릭하여 기존 RA VPN 구성을 수정합니다.
  - **Remove**(제거)를 클릭하여 RA VPN 구성에서 FDM 관리 디바이스를 제거합니다. 그룹 정책을 제외하고 해당 디바이스와 연결된 모든 연결 프로파일 및 RA VPN 설정이 삭제됩니다. 개체 페이지에서 그룹 정책을 명시적으로 제거할 수 있습니다. 참고: 구성을 사용하는 유일한 디바이스인 경우 FDM 관리 디바이스를 제거할 수 없습니다. 이 경우 대신 RA VPN 구성을 제거할 수 있습니다.

구성 또는 디바이스의 이름을 입력하여 Remote Access VPN 구성을 검색할 수도 있습니다.

## 관련 정보:

- [RA VPN 연결 프로파일 컨피그레이션](#)
- [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.](#)
- [원격 액세스 VPN을 통한 트래픽 허용](#)

## RA VPN 연결 프로파일 컨피그레이션

RA VPN 연결 프로파일은 외부 사용자가 AnyConnect 클라이언트를 사용하여 시스템에 대한 VPN 연결을 생성할 수 있도록 허용하는 특성을 정의합니다. 각 프로파일은 사용자 인증에 사용되는 AAA 서버 및 인증서, 사용자 IP 주소 할당을 위한 주소 풀, 다양한 사용자 지향 속성을 정의하는 그룹 정책을 정의합니다.

여러 사용자 그룹에 가변적인 서비스를 제공해야 하는 경우 또는 다양한 인증 소스가 있는 경우, RA VPN 구성 내에 프로파일을 여러 개 생성합니다. 예를 들어 조직이 다른 인증 서버를 사용하는 다른 조직과 병합하는 경우, 해당 인증 서버를 사용하는 새 그룹에 대해 프로파일을 만들 수 있습니다.

RA VPN 연결 프로파일을 사용하면 홈 네트워크 등의 외부 네트워크에 있는 사용자가 내부 네트워크에 연결할 수 있습니다. 다른 인증 방법을 수용하기 위해 별도 프로파일을 생성합니다.

## 시작하기 전에

RA(원격 액세스) VPN 연결을 구성하기 전에 다음 작업을 수행합니다.

- 원격 액세스 VPN 연결을 종료하는 외부 인터페이스가 HTTPS 연결을 허용하는 관리 액세스 목록도 포함할 수는 없습니다. RA VPN을 구성하기 전에 외부 인터페이스에서 HTTPS 규칙을 삭제하십시오. [Firepower Device Manager 버전 X.Y용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 설정" 장에서 "관리 액세스 목록 구성" 섹션을 참조하십시오.
- RA VPN 구성을 생성합니다. [RA VPN 구성 생성](#)을 참조하십시오.

## 절차

## Procedure

- 단계 1 CDO 내비게이션 페이지에서 **VPN > Remote Access VPN Configuration**(원격 액세스 VPN 구성)을 클릭합니다. VPN 구성을 클릭하여 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지에 대한 요약 정보를 볼 수 있습니다.
- 단계 2 연결 프로파일을 클릭하고 오른쪽 사이드바의 **Actions**(작업) 아래에서 **Add Connection Profile**(연결 프로파일 추가)를 클릭합니다.
- 단계 3 기본 연결 속성을 구성합니다.

- **Connection Profile Name**(연결 프로파일 이름): 이 연결의 이름을 공백 없이 50자까지 입력합니다. 예를 들면 MainOffice를 입력합니다.

**Note** 여기서 입력하는 이름이 AnyConnect 클라이언트에서 사용자에게 표시되는 연결 목록에 나타납니다. 따라서 사용자가 쉽게 이해할 수 있는 이름을 선택해야 합니다.

- **Group Alias(그룹 별칭), Group URL(그룹 URL):** 별칭에는 특정 연결 프로파일에 대한 대체 이름 또는 URL이 포함되어 있습니다. FDM 관리 디바이스에 연결하는 경우, VPN 사용자는 연결 목록의 AnyConnect 클라이언트에서 별칭 이름을 선택할 수 있습니다. 연결 프로파일 이름이 그룹 별칭으로 자동 추가됩니다. 또한 원격 액세스 VPN 연결을 시작하는 동안 엔드포인트에서 선택할 수 있는 그룹 URL의 목록을 구성할 수 있습니다. 사용자가 그룹 URL을 사용하여 연결하는 경우, 시스템에서는 URL과 일치하는 연결 프로파일을 자동으로 사용합니다. 이 URL은 설치된 AnyConnect 클라이언트가 아직 없는 클라이언트에서 사용됩니다. 그룹 별칭 및 URL을 필요한 만큼 추가하십시오. 이러한 별칭 및 URL은 디바이스에 정의된 모든 연결 프로파일 전반에 걸쳐 고유한 것이어야 합니다. 그룹 URL은 **https://**로 시작해야 합니다.
- 예를 들어 별칭 계약자 및 그룹 URL <https://ravpn.example.com/contractor>가 있을 수 있습니다. AnyConnect 클라이언트가 설치된 후 사용자는 연결의 AnyConnect VPN 드롭다운 목록에서 그룹 별칭을 선택하기만 하면 됩니다.

**단계 4** 기본 ID 소스를 구성하고, 선택적으로 보조 ID 소스를 구성합니다. 이 옵션을 통해 원격 사용자가 원격 액세스 VPN 연결을 활성화하기 위해 디바이스에 인증하는 방식을 결정합니다. 가장 간단한 방식은 AAA만 사용하여 AD 영역을 선택하거나 LocalIdentitySource를 사용하는 것입니다. **Authentication Type(인증 유형)**에는 다음과 같은 방식을 사용할 수 있습니다.

- **AAA Only(AAA만):** 사용자 이름 및 암호에 근거하여 사용자를 인증하고 사용자에게 권한을 부여합니다. 자세한 내용은 [연결 프로파일에 대해 AAA 구성](#)을 참조하십시오.
- **Client Certificate Only(클라이언트 인증서만):** 클라이언트 디바이스 ID 인증서에 근거하여 사용자를 인증합니다. 자세한 내용은 [연결 프로파일에 대한 인증서 인증 구성](#)을 참조하십시오.
- **AAA and ClientCertificate(AAA 및 ClientCertificate):** 사용자 이름/암호와 클라이언트 디바이스 ID 인증서를 모두 사용합니다.

**단계 5** 클라이언트에 대해 주소 풀을 구성합니다. 주소 풀에서는 원격 클라이언트가 VPN 연결을 설정할 때 시스템에서 원격 클라이언트에 할당할 수 있는 IP 주소를 정의합니다. 자세한 내용은 [클라이언트 주소 풀 할당 구성](#)을 참조하십시오.

**단계 6** **Continue(계속)**를 클릭합니다.


**단계 7** 목록에서 이 프로파일에 사용할 **Group Policy(그룹 정책)**를 선택하고 **Select(선택)**를 클릭합니다. 그룹 정책에서는 터널이 설정된 후에 사용자 연결에 대한 조건을 설정합니다. 시스템에는 DfltGrpPolicy 라는 이름의 기본 그룹 정책이 포함되어 있습니다. 필요한 서비스를 제공하는 추가 그룹 정책을 만들 수 있습니다.

**Note** 필요한 그룹 정책이 아직 없는 경우 **Objects(개체)** 페이지에서 그룹 정책을 생성한 다음 해당 정책을 RA VPN 구성에 연결합니다. 그룹 정책에 대한 세부 정보는 [새 RA VPN 그룹 정책 생성](#)을 참조하십시오.

**단계 8** **Continue(계속)**를 클릭합니다.

**단계 9** 요약 검토합니다. 먼저 요약이 정확한지 확인합니다. AnyConnect 소프트웨어를 처음으로 설치하고 VPN 연결을 완료할 수 있는지를 테스트하기 위해 엔드 사용자가 수행해야 하는 작업을 파악할 수



있습니다.  를 클릭하여 지침을 클립보드에 복사한 다음 사용자에게 배포합니다.

**단계 10** Done(완료)를 클릭합니다.

### What to do next

원격 액세스 VPN을 통한 트래픽 허용에 설명된 대로 VPN 터널에서 트래픽이 허용되는지 확인합니다.

### 연결 프로파일에 대해 AAA 구성

인증, 권한 부여, 계정 관리 (AAA) 서버에서는 사용자 이름과 암호를 사용하여 사용자에게 원격 액세스 VPN에 대한 액세스가 허용되어 있는지 확인합니다. RADIUS 서버를 사용하는 경우, 인증된 사용자들 사이에서 권한 부여 수준을 구별하여 보호받는 리소스에 대한 차등 액세스를 제공할 수 있습니다. 또한 RADIUS 계정 관리 서비스를 사용하여 사용량을 추적할 수 있습니다.

AAA를 구성하는 경우, 기본 ID 소스를 구성해야 합니다. 보조 및 대체 소스는 선택 사항입니다. 2단계 인증을 구현하려면 RSA 토큰 또는 듀오와 같은 보조 소스를 사용합니다.

### 기본 ID 소스 옵션

- **Primary Identity Source for User Authentication**(사용자 인증을 위한 기본 ID 소스): 원격 사용자 인증에 사용되는 기본 ID 소스입니다. VPN 연결을 완료하려면 이 소스 또는 대체 소스(선택 사항)에서 최종 사용자를 정의해야 합니다. 다음 중 하나를 선택합니다.
  - AD(Active Directory) ID 영역. 필요한 영역이 아직 없는 경우, **Create New Identity Realm**(새 ID 영역 생성)을 클릭합니다.
  - Radius 서버 그룹.
  - LocalIdentitySource(로컬 사용자 데이터베이스): 외부 서버를 사용하지 않고 디바이스에서 직접 사용자를 정의할 수 있습니다.
- **Fallback Local Identity Source**(대체 로컬 ID 소스): 기본 소스가 외부 서버인데 기본 서버를 사용할 수 없는 경우, 대체 소스로 LocalIdentitySource를 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우 외부 서버에 정의한 것과 같은 로컬 사용자 이름/비밀번호를 정의해야 합니다.
- **Strip options**(제거 옵션): 영역은 관리 도메인입니다. 다음 옵션을 활성화하면 사용자 이름에만 근거하여 인증할 수 있습니다. 이러한 옵션의 조합을 활성화할 수 있습니다. 그러나 서버에서 구분 기호를 구문 분석할 수 없는 경우, 두 확인란을 모두 선택해야 합니다.
  - **Strip Identity Source Server from Username**(사용자 이름에서 ID 소스 서버 제거): AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 ID 소스 이름을 제거할지 여부. 예를 들어 이 옵션을 선택하고 사용자가 도메인\사용자 이름을 사용자 이름으로 입력하는 경우, 도



메인은 사용자 이름에서 제거되고 인증을 위해 AAA 서버로 전송됩니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

- **Strip Group from Username**(사용자 이름에서 그룹 제거): AAA 서버로 사용자 이름을 전달하기 전에 사용자 이름에서 그룹 이름을 제거할지 여부. 이 옵션은 `username@domain` 형식에서 지정된 이름에 적용되며, 도메인 및 `@` 기호를 제거합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

#### 보조 ID 소스

- **Secondary Identity Source for User Authorization**(사용자 권한 부여를 위한 보조 ID 소스): 두 번째 ID 소스로서 선택 사항입니다. 사용자가 기본 소스로 인증에 성공하는 경우, 사용자에게 보조 소스를 사용해 인증하라는 메시지가 표시됩니다. AD 영역, RADIUS 서버 그룹 또는 로컬 ID 소스를 선택할 수 있습니다.
- **Advanced options**(고급 옵션): **Advanced**(고급) 링크를 클릭하고 다음 옵션을 구성합니다.
  - **Fallback Local Identity Source for Secondary**(보조용 대체 시스템 로컬 ID 소스): 보조 소스가 외부 서버인데 보조 서버를 사용할 수 없는 경우, `LocalIdentitySource`를 대체 소스로 선택할 수 있습니다. 로컬 데이터베이스를 대체 소스로 사용하는 경우, 보조 외부 서버에 정의한 것과 같은 로컬 사용자 이름/암호를 정의해야 합니다.
  - **Use Primary Username for Secondary Login**(보조 로그인에 기본 사용자 이름 사용): 보조 ID 소스를 사용하는 경우, 시스템에서는 기본적으로 보조 소스에 대한 사용자 이름 및 암호를 모두 입력하라는 메시지를 표시합니다. 이 옵션을 선택하는 경우, 시스템에서는 보조 암호만 입력하라는 메시지를 표시하고 기본 ID 소스에 대해 인증된 보조 소스에 동일한 사용자 이름을 사용합니다. 기본 및 보조 ID 소스 모두에서 동일한 사용자 이름을 구성하는 경우, 이 옵션을 선택합니다.
    - **Username for Session Server**(세션 서버의 사용자 이름): 인증에 성공하면 사용자 이름이 이벤트 및 통계 대시보드에 표시되고, 이 이름은 사용자 또는 그룹 기반 SSL 암호 해독 및 액세스 제어 규칙에 대한 일치 여부를 확인하고 계정을 관리하는 데 사용됩니다. 두 가지 인증 소스를 사용하고 있기 때문에 기본 또는 보조 사용자 이름을 사용자 ID로 사용할지 여부를 시스템에 알려주어야 합니다. 기본적으로 기본 이름을 사용합니다.
    - **Password Type**(암호 유형): 보조 서버의 암호를 가져오는 방법. 기본값은 **Prompt**(프롬프트)입니다. 이는 사용자에게 암호를 입력하라는 메시지가 표시됨을 뜻합니다. 사용자가 기본 서버에 인증할 때 입력한 암호를 자동으로 사용하려면 **Primary Identity Source Password**(기본 ID 소스 암호)를 선택합니다. 모든 사용자에 대해 동일한 암호를 사용하려면 **Common Password**(공통 암호)를 선택한 다음, **Common Password**(공통 암호) 필드에 해당 암호를 입력합니다.
  - **Authorization Server**(권한 부여 서버): 원격 액세스 VPN 사용자를 인증하도록 구성된 RADIUS 서버 그룹. 인증이 완료되면 권한 부여 기능에서 인증된 각 사용자에게 사용할 수 있는 서비스 및 명령을 제어합니다. 권한 부여 기능은 사용자가 수행할 수 있도록 인가를 받은 것이 무엇인지, 즉 사용자의 실제 능력 및 제한 사항을 설명하는 일련의 속성을 결합함으로써 작동합니다. 권한 부여 기능을 사용하지 않는 경우, 인증 기능에서만 인증된 모든 사용자에게 동일한 액세스 권한을 제공합니다. 권한 부여를 위해 RADIUS를 구성하는 방법에 대한 자세한

한 내용은 [RADIUS 및 그룹 정책을 이용한 사용자 권한 및 속성 제어](#)를 참조하십시오. 시스템이 그룹 정책에 정의된 것과 중복되는 권한 부여 속성을 RADIUS 서버에서 가져오는 경우, RADIUS 속성은 그룹 정책 속성을 재정의한다는 점에 유의하십시오.

- **Accounting Server(과금 서버):** (선택 사항) 원격 액세스 VPN 세션에 대한 계정 관리에 사용할 RADIUS 서버 그룹입니다. 계정 관리 기능에서는 사용자가 액세스 중인 서비스뿐 아니라 사용 중인 네트워크 리소스의 수까지도 추적합니다. FTD 디바이스에서는 RADIUS 서버에 사용자 활동을 보고합니다. 계정 관리 정보에는 세션 시작 및 중지 시각, 사용자 이름, 각 세션의 디바이스를 통과한 바이트 수, 사용한 서비스, 각 세션의 지속시간이 포함됩니다. 네트워크 관리, 클라이언트 요금 청구 또는 감사에 대한 데이터를 분석할 수 있습니다. 관리 계정 기능을 단독으로 사용하거나 인증 및 권한 부여 기능과 함께 사용할 수 있습니다.

연결 프로파일에 대한 인증서 인증 구성



**Note** 이 섹션은 **Authentication Type(인증 유형)**이 **AAA Only(AAA만)**인 경우에는 적용되지 않습니다.

클라이언트 디바이스에 설치된 인증서를 사용해 원격 액세스 VPN 연결을 인증할 수 있습니다.

클라이언트 인증서를 사용하는 경우에도 보조 ID 소스, 대체 소스, 권한 부여 및 과금 서버를 구성할 수 있습니다. 이는 AAA 옵션입니다. 자세한 내용은 [RA VPN 연결 프로파일 컨피그레이션](#)을 참조하십시오.

다음은 인증서별 속성입니다. 기본 및 보조 ID 소스에 대해 개별적으로 이러한 속성을 구성할 수 있습니다. 보조 소스 구성은 선택 사항입니다.

- **Username from Certificate(인증서의 사용자 이름):** 다음 중 하나를 선택합니다.
  - **Map Specific Field(특정 필드 매핑): Primary Field(기본 필드) 및 Secondary Field(보조 필드)의 순서대로 인증서 요소를 사용합니다.** 기본값은 CN(Common Name) 및 OU(Organizational Unit)입니다. 조직에 대해 작동하는 옵션을 선택합니다. 필드는 서로 결합하여 사용자 이름을 제공하고, 이 이름은 이벤트, 대시보드에서 사용되며 SSL 암호 해독 및 액세스 제어 규칙에서 일치 목적으로 사용됩니다.
  - **Use entire DN (distinguished name) as username(전체 DN(고유 이름)을 사용자 이름으로 사용):** 시스템은 DN 필드에서 사용자 이름을 자동으로 파생합니다.
- **고급 옵션(Authentication Type(인증 유형)이 Client Certificate Only(클라이언트 인증서 전용))인 경우에는 해당되지 않음): Advanced(고급) 링크를 클릭하고 다음 옵션을 구성합니다.**
  - **Prefill username from certificate on user login window(인증서의 사용자 이름을 사용자 로그인 창에 미리 채우기):** 사용자에게 인증하라는 메시지를 표시할 때 사용자 이름 필드에 검색된 사용자 이름을 입력할지 여부.
  - **Hide username in login window(로그인 창에서 사용자 이름 숨기기): Prefill(미리 채우기) 옵션을 선택하면 사용자 이름을 숨길 수 있습니다.** 따라서 사용자는 암호 프롬프트에서 사용자 이름을 편집할 수 없습니다.

### 클라이언트 주소 풀 할당 구성

원격 액세스 VPN에 연결하는 엔드포인트에 대한 IP 주소를 시스템에서 제공할 방법이 있어야 합니다. AAA 서버는 이러한 주소, DHCP 서버, 그룹 정책에 구성된 IP 주소 풀 또는 연결 프로파일에 구성된 IP 주소 풀을 제공할 수 있습니다. 시스템은 순서대로 이 리소스를 시도하고 사용 가능한 주소를 가져올 때 중지했다가 이 주소를 클라이언트에 할당합니다. 따라서 동시 연결 수가 비정상적인 경우에 페일세이프를 생성할 수 있는 여러 가지 옵션을 구성할 수 있습니다.

연결 프로파일에 대한 주소 풀을 구성하려면 다음 방법 중 한 가지 이상을 사용합니다.

- **IPv4 Address Pool(IPv4 주소 풀) 및 IPv6 Address Pool(IPv6 주소 풀)**: 먼저 서브넷을 지정하는 최대 6개의 네트워크 개체를 생성합니다. IPv4 및 IPv6에 대해 별도 풀을 구성할 수 있습니다. 그런 다음, 그룹 정책 또는 연결 프로파일의 **IPv4 Address Pool(IPv4 주소 풀) 및 IPv6 Address Pool(IPv6 주소 풀)** 옵션에서 이러한 개체를 선택합니다. IPv4 및 IPv6 모두 구성할 필요는 없고 지원하려는 주소 체계를 구성하면 됩니다. 또한 그룹 정책 및 연결 프로파일 모두에서 풀을 구성할 필요는 없습니다. 그룹 정책에서는 연결 프로파일 설정을 오버라이드하므로 그룹 정책에서 풀을 구성하는 경우, 연결 프로파일에서 옵션을 비워두십시오. 풀은 나열한 순서대로 사용된다는 점에 유의하십시오.
- **DHCP Servers(DHCP 서버)**: 먼저 RA VPN에 대한 IPv4 주소 범위를 하나 이상 사용하여 DHCP 서버를 구성합니다(DHCP를 사용하여 IPv6 풀을 구성할 수는 없음). 그런 다음, DHCP 서버의 IP 주소로 호스트 네트워크 개체를 생성합니다. 그러면 연결 프로파일의 **DHCP Servers(DHCP 서버)** 속성에서 이 개체를 선택할 수 있습니다. 두 개 이상의 DHCP 서버를 구성할 수 있습니다. DHCP 서버에 주소 풀이 여러 개인 경우, 연결 프로파일에 연결하는 그룹 정책에서 **DHCP Scope(DHCP 범위)** 속성을 통해 어떤 풀을 사용할지 선택할 수 있습니다. 풀의 네트워크 주소로 호스트 네트워크 개체를 생성합니다. 예를 들어 DHCP 풀에 192.168.15.0/24 및 192.168.16.0/24가 포함된 경우, DHCP 범위를 192.168.16.0으로 설정하면 192.168.16.0/24 서브넷에서 주소가 선택됩니다.

### 원격 액세스 VPN을 통한 트래픽 허용

다음 기법 중 하나를 사용해 원격 액세스 VPN 터널에서 트래픽 플로우를 활성화할 수 있습니다.

- **sysopt connection permit-vpn** 명령을 구성합니다. 이 명령에서는 VPN 연결과 일치하는 트래픽을 액세스 제어 정책에서 제외합니다. 이 명령의 기본값은 **no sysopt connection permit-vpn**입니다. 이는 액세스 제어 정책에서도 VPN 트래픽을 허용해야 한다는 의미입니다. 이 방법은 외부 사용자가 원격 액세스 VPN 주소 풀에서 IP 주소를 스누핑할 수 없기 때문에 VPN에서 트래픽을 더 안전하게 허용할 수 있습니다. 하지만 VPN 트래픽이 검사되지 않는다는 단점이 있습니다. 즉, 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다. 즉 트래픽에 대해 연결 이벤트가 생성되지 않고, 따라서 통계 대시보드에 VPN 연결이 반영되지 않는다는 의미이기도 합니다. 이 명령을 구성하려면 RA VPN 구성에서 **Bypass Access Control policy for decrypted traffic**(암호 해독된 트래픽에 대해 액세스 제어 정책 우회) 옵션을 선택합니다. [RA VPN 구성 생성](#)을 참조하십시오.
- 원격 액세스 VPN 주소 풀에서 연결을 허용하는 액세스 제어 규칙을 생성합니다. 이 방법을 사용하는 경우 VPN 트래픽이 검사되며, 연결에 고급 서비스를 적용할 수 있습니다. 하지만 외부 사용자가 IP 주소를 스누핑하여 내부 네트워크에 액세스할 가능성이 있다는 단점이 있습니다. [FDM 액세스 제어 정책 구성](#)을 참조하십시오.

버전 6.4.0을 실행하는 FDM-관리 디바이스에서 AnyConnect 패키지 업그레이드

Cisco Defense Orchestrator를 사용하여 FDM 관리 디바이스에서 사용 가능한 AnyConnect 패키지를 업그레이드하여 RA VPN 사용자에게 배포할 수 있습니다.

다음은 AnyConnect 패키지 업그레이드와 관련된 주요 단계입니다.

### Procedure

단계 1 firewall device manager를 사용하여 AnyConnect 패키지를 제거하고 최신 버전의 패키지를 업로드합니다. 이 작업을 수행하려면 다음 방법 중 하나를 사용합니다.

- 이전 패키지를 제거하고 firewall device manager UI에서 새 패키지를 업로드합니다.
- 이전 패키지를 제거하고 firewall device manager API 탐색기에서 새 패키지를 업로드합니다.

단계 2 디바이스에 firewall device manager 변경 사항을 구축합니다.

단계 3 새 구성 정보를 CDO로 읽습니다.

단계 4 RA VPN 연결 프로파일에서 새 패키지를 확인합니다.

### 사전 요구 사항

- 연결 프로파일이 있는 하나 이상의 RA VPN 구성이 이미 FDM 관리 디바이스에 구축되어 있습니다.
- <https://software.cisco.com/download/home/283000185>에서 원하는 AnyConnect 패키지를 다운로드합니다. Cisco에서는 사용 가능한 최신 패키지로 업그레이드할 것을 권장합니다.


Firewall Device Manager를 사용하여 Secure Firewall Threat Defense에 원하는 AnyConnect 패키지 업로드

### Procedure

단계 1 브라우저를 사용하여 시스템의 홈페이지를 엽니다. 예를 들면 <https://ftd.example.com>입니다.

단계 2 Firewall Device Manager에 로그인합니다.

단계 3 **Device**(디바이스) > **Remote Access VPN**(원격 액세스 VPN) 그룹에서 **View Configuration**(구성 보기)을 클릭합니다. 현재 얼마나 많은 연결 프로파일 및 그룹 정책이 컨피그레이션되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

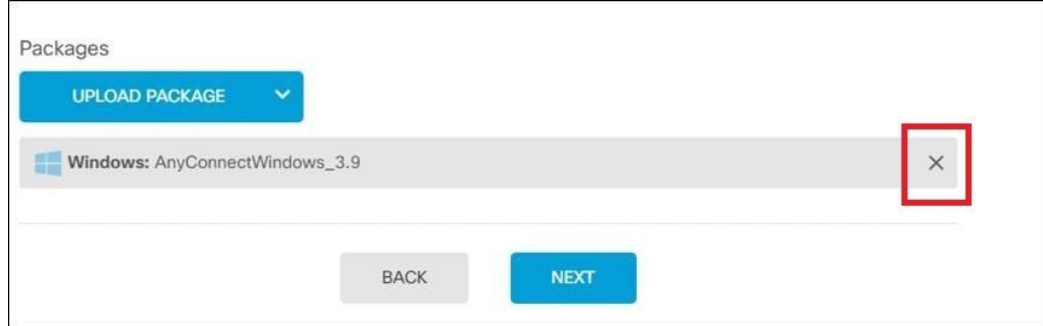
단계 4 보기( 버튼)(구성 **View**(보기) 버튼)을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다.

**Note** 연결 프로파일 중 하나를 수정하여 AnyConnect 패키지를 FDM 관리 디바이스에 업로드할 수 있습니다.

단계 5 **Edit**(편집) 버튼을 클릭하여 변경합니다.

단계 6 **Global Settings**(전역 설정) 화면이 나타날 때까지 **Next**(다음)를 클릭합니다. **AnyConnect Package**(AnyConnect 패키지)에는 FDM 관리 디바이스에서 사용 가능한 AnyConnect 패키지가 표시됩니다.

단계 7 'X' 버튼을 클릭하여 교체할 AnyConnect 패키지를 제거합니다.



단계 8 **Upload Package**(패키지 업로드)를 클릭한 다음 호환되는 패키지를 업로드할 OS를 클릭합니다.

단계 9 패키지를 선택하고 **Open**(열기)을 클릭합니다. Firewall Device Manager UI에서 업로드 중인 패키지를 확인할 수 있습니다.

단계 10 마침을 클릭합니다. 구성이 저장됩니다.

**Note** 또는 Firewall Device Manager API 탐색기를 사용하여 새 AnyConnect 패키지를 제거하고 업로드할 수 있습니다.

- a. `##/api-explorer`를 가리키도록 URL을 편집합니다(예: <https://ftd.example.com/##/api-explorer>).
- b. FDM 관리디바이스에서 패키지를 삭제하려면, **AnyConnectPackageFile > Delete**(삭제)를 클릭합니다. **objID** 필드에 패키지 ID를 입력하고 **TRY IT OUT!**을 클릭합니다.
- c. **버전 6.4.0을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드** 섹션에 설명된 단계를 수행하여 새 패키지를 업로드합니다.

단계 11 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes**(변경 사항 구축) 아이콘을 클릭합니다. 배포되지 않은 변경 사항이 있으면 아이콘이 점으로 강조 표시됩니다.

단계 12 변경 사항에 만족하는 경우 **Deploy Now**(지금 구축)를 클릭하여 작업을 즉시 시작할 수 있습니다. 창에는 구축이 진행 중임이 표시됩니다. 창을 닫을 수도 있고 구축이 완료될 때까지 기다릴 수도 있습니다.

RA VPN 연결 프로파일에서 새 패키지가 참조되는지 확인

### Procedure

단계 1 왼쪽의 CDO 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭하고 업그레이드된 AnyConnect 패키지가 있는 FTD 디바이스를 선택합니다. 이 디바이스에서 충돌을 보고합니다.

단계 4 디바이스의 실행 중인 구성으로 CDO에 저장된 구성 및 보류 중인 변경 사항을 덮어쓰려면 OOB(Out of Band) 변경 사항을 수락합니다. 자세한 내용은 "충돌 탐지됨" 상태 해결을 참조하십시오.

단계 5 다음을 수행하여 새 AnyConnect 패키지를 확인합니다.

- VPN > Remote Access VPN(원격 액세스 VPN)을 클릭합니다.
- 이 FTD 디바이스와 연결된 RA VPN 구성을 클릭합니다.
- Actions(작업) 아래에서 Edit(편집)를 클릭합니다. 새 패키지가 Devices(디바이스) 아래에 표시됩니다.

### RA VPN AnyConnect 클라이언트 프로파일 업로드

원격 액세스 VPN AnyConnect 클라이언트 프로파일은 파일에 저장된 구성 매개변수의 그룹입니다. 핵심 클라이언트 VPN 기능과 선택적 클라이언트 모듈인 Network Access Manager, AMP Enabler, ISE Posture, 네트워크 가시성, 고객 피드백 경험 프로파일, Umbrella 로밍 보안 및 웹 보안에 대한 구성 설정을 포함하는 다양한 AnyConnect 클라이언트 프로파일이 있습니다.

CDO는 이러한 프로파일을 나중에 그룹 정책에서 사용할 수 있는 개체로 업로드할 수 있습니다.

- **AnyConnect VPN** 프로파일 - AnyConnect 클라이언트 프로파일은 AnyConnect 클라이언트 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 AnyConnect 클라이언트 환경 설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다. CDO는 XML 파일 형식을 지원합니다.
- **AMP Enabler** 서비스 프로파일 - 이 프로파일은 AnyConnect AMP Enabler에 사용됩니다. 원격 액세스 VPN 사용자가 VPN에 연결하면 AMP Enabler 및 이 프로파일이 FDM 관리 디바이스에서 엔드 포인트로 푸시됩니다. CDO는 XML 및 ASP 파일 형식을 지원합니다.
- **피드백 프로파일** - 고객 경험 피드백 프로파일을 추가하고 이 유형을 선택하여 고객이 활성화하고 사용하는 기능 및 모듈에 대한 정보를 수신할 수 있습니다. CDO는 FSP 파일 형식을 지원합니다.
- **ISE Posture** 프로파일 - AnyConnect ISE Posture 모듈용 프로파일 파일을 추가하는 경우 이 옵션을 선택합니다. CDO는 XML 및 ISP 파일 형식을 지원합니다.
- **Network Access Manager** 서비스 프로파일 - Network Access Manager 프로파일 편집기를 사용하여 NAM 프로파일 파일을 설정하고 추가합니다. CDO는 XML 및 NSP 파일 형식을 지원합니다.
- **네트워크 가시성** 서비스 프로파일 - AnyConnect 네트워크 가시성 모듈의 프로파일 파일입니다. NVM 프로파일 편집기를 사용하여 프로파일을 생성할 수 있습니다. CDO는 XML 및 NVMSPP 파일 형식을 지원합니다.
- **Umbrella** 로밍 보안 프로파일 - Umbrella 로밍 보안 모듈을 구축하는 경우 이 파일 유형을 선택해야 합니다. CDO는 XML 및 JSON 파일 형식을 지원합니다.
- **웹 보안** 서비스 프로파일 - 웹 보안 모듈용 프로파일 파일을 추가할 때 이 파일 유형을 선택합니다. CDO는 XML, WSO 및 WSP 파일 형식을 지원합니다.

## Before you begin

적합한 GUI 기반 AnyConnect 프로파일 편집기를 사용하여 필요한 프로파일을 생성합니다. AnyConnect Secure Mobility Client 범주의 [Cisco 소프트웨어 다운로드 센터](#)에서 프로파일 편집기를 다운로드하고 AnyConnect "프로파일 편집기 - Windows/독립형 설치 프로그램(MSI)"을 설치할 수 있습니다. 프로파일 편집기 설치 프로그램에는 독립형 버전의 프로파일 편집기가 포함되어 있습니다. 설치 파일은 Windows 전용이며 파일 이름은 anyconnect-profileeditor-win-<version>-k9.msi입니다. 여기서 <version>은 AnyConnect 버전입니다. 예를 들면 anyconnect-profileeditor-win-4.3.04027-k9.msi와 같습니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다.

Umbrella 로밍 보안 프로파일 편집기를 제외하고 이 패키지에는 모듈을 생성하는 데 필요한 모든 프로파일 편집기가 포함되어 있습니다. 자세한 내용은 [Cisco AnyConnect Secure Mobility Client 관리자 가이드](#)에서 해당 릴리스의 AnyConnect 프로파일 편집기 장을 참조하십시오. Umbrella 대시보드와 별도로 Umbrella 로밍 보안 프로파일을 다운로드합니다. 자세한 내용은 [Cisco Umbrella 사용 설명서](#)의 "Umbrella 로밍 보안" 장에서 "Umbrella 대시보드에서 AnyConnect 로밍 보안 프로필 다운로드" 섹션을 참조하십시오.

## Procedure

단계 1 좌측의 CDO 내비게이션 바에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 파란색 더하기  버튼을 클릭합니다.

단계 3 **RA VPN Objects (ASA & FDM)(RA VPN 개체(ASA 및 FDM)) > AnyConnect Client Profile(AnyConnect 클라이언트 프로파일)**를 클릭합니다.

단계 4 **Object Name(개체 이름)** 필드에 AnyConnect 클라이언트 프로파일의 이름을 입력합니다.

단계 5 **Browse(찾아보기)**를 클릭하고 프로파일 편집기를 사용하여 생성한 파일을 선택합니다.

단계 6 **Open(열기)**을 클릭하여 프로파일을 업로드합니다.

단계 7 **Add(추가)**를 클릭하여 개체를 추가합니다.

### 관련 정보:

- RA VPN 그룹 정책 창에서 클라이언트 모듈을 AnyConnect VPN 프로파일과 연결합니다. [새 RA VPN 그룹 정책 생성](#)을 참조하십시오.



**Note** 클라이언트 모듈 연결은 소프트웨어 버전 6.7 이상을 실행하는 모든 ASA 버전 및 FDM에서 지원됩니다.

## FDM-관리 디바이스용 원격 액세스 VPN의 지침 및 제한 사항

RA VPN을 구성할 때 다음 지침 및 제한 사항을 염두에 두십시오.

- firewall device manager을 사용하여 버전 6.4.0을 실행하는 FDM-관리 디바이스에 AnyConnect 패키지를 사전 로드해야 합니다.



**Note** Cisco Defense Orchestrator의 원격 액세스 VPN 구성 마법사를 사용하여 버전 6.5.0을 실행하는 FDM-관리 디바이스에 AnyConnect 패키지를 별도로 업로드합니다.

- CDO에서 RA VPN을 구성하기 전에,
  - firewall device manager에서 FDM 관리 디바이스에 대한 라이선스를 등록합니다.
  - 내보내기 제어 기능이 있는 firewall device manager에서 라이선스를 활성화합니다.
- CDO는 확장 액세스 목록 개체를 지원하지 않습니다. firewall device manager에서 Smart CLI를 사용하여 개체를 구성한 다음 VPN 필터 및 CoA(Change of Authorization) 리디렉션 ACL에서 사용합니다.
- FDM 관리 디바이스에서 생성한 템플릿에는 RA VPN 구성이 포함되지 않습니다.
- IP 풀 개체 및 RADIUS ID 소스에는 디바이스별 오버라이드가 필요합니다.
- 동일한 TCP 포트에 대해 동일한 인터페이스에서 firewall device manager 액세스(관리 액세스 목록의 HTTPS 액세스)와 AnyConnect 원격 액세스 SSL VPN을 모두 구성할 수 없습니다. 예를 들어, 외부 인터페이스에서 원격 액세스 SSL VPN을 구성하는 경우, 포트 443에서 HTTPS 연결에 대한 외부 인터페이스도 열 수 없습니다. firewall device manager의 이러한 기능에서 사용되는 포트를 구성할 수 없으므로 동일한 인터페이스에서 두 가지 기능을 모두 구성할 수는 없습니다.
- RADIUS 및 RSA 토큰을 사용하여 2단계 인증을 구성하는 경우, 기본 인증 시간 제한 값인 12초는 너무 짧아 대부분의 경우 성공적인 인증을 허용하기 어렵습니다. [RA VPN AnyConnect 클라이언트 프로파일 업로드, on page 552](#)에 설명된 대로 사용자 지정 AnyConnect 클라이언트 프로파일을 생성하고 RA VPN 연결 프로파일에 적용하여 인증 제한 시간 값을 늘리십시오. 사용자가 RSA 토큰을 인증한 다음 붙여넣고 토큰의 왕복 확인에 충분한 시간을 가질 수 있도록 최소 60초의 인증 제한 시간을 권장합니다.

#### FDM-관리 디바이스에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법

firewall device manager API를 사용하여 AnyConnect 클라이언트 소프트웨어 패키지를 FDM 관리 디바이스에 업로드하여 사용자에게 배포합니다. [버전 6.4.0을 실행하는 FDM-관리 디바이스에 AnyConnect 소프트웨어 패키지 업로드](#)를 참조하십시오.

VPN 연결을 완료하려면 사용자가 AnyConnect 클라이언트 소프트웨어를 설치해야 합니다. 기존 소프트웨어 배포 방법을 사용하여 소프트웨어를 직접 설치할 수 있습니다. 또는 사용자가 FDM 관리 디바이스에서 AnyConnect 클라이언트를 직접 설치하게 할 수도 있습니다.



**Note** 소프트웨어를 설치하려면 사용자에게 워크스테이션에 대한 관리자 권한이 있어야 합니다.

사용자가 FDM 관리 디바이스에서 소프트웨어를 처음 설치하도록 하려면 사용자에게 다음 단계를 수행하도록 하십시오.





**Note** Android 및 iOS 사용자는 해당 앱 스토어에서 AnyConnect를 다운로드해야 합니다.

### Procedure

- 단계 1 웹 브라우저를 사용하여 **https://ravpn-address**를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 원격 액세스 VPN을 구성할 때 이 인터페이스를 식별합니다. 시스템에서 사용자에게 로그인하라는 메시지를 표시합니다.
- 단계 2 사이트에 로그인합니다. 사용자는 원격 액세스 VPN용으로 구성된 디렉터리 서버를 사용하여 인증을 합니다. 로그인이 성공해야 설치를 계속할 수 있습니다. 로그인이 성공하면 시스템은 사용자에게 필요한 AnyConnect 클라이언트 버전이 이미 있는지를 확인합니다. 사용자 컴퓨터에 AnyConnect 클라이언트가 없거나 클라이언트가 하위 레벨인 경우에는 시스템에서 AnyConnect 소프트웨어 설치를 자동으로 시작합니다. 설치가 완료되면, AnyConnect에서 원격 액세스 VPN 연결을 완료합니다.

### 새 AnyConnect 클라이언트 소프트웨어 버전 배포

이전 버전을 제거하지 않고 새 버전의 AnyConnect 클라이언트 소프트웨어를 FDM 관리 디바이스에 업로드하여 사용자에게 배포할 수 있습니다. AnyConnect 클라이언트가 성공적으로 업로드되면 이전 버전을 제거할 수 있습니다.

AnyConnect 클라이언트는 사용자가 다음 VPN 연결에서 새 버전을 탐지합니다. 그러면 시스템에서 업데이트된 클라이언트 소프트웨어를 다운로드하여 설치하라는 메시지를 사용자에게 자동으로 표시합니다. 이러한 자동화로 인해 개발자와 고객을 위한 소프트웨어 배포를 간소화할 수 있습니다.

다음 그림에는 Windows OS용 AnyConnect 클라이언트 소프트웨어의 두 가지 버전 (**AnyConnectWindows\_3.2\_BGL** 및 **AnyConnectWindows\_4.2\_BGL**)이 포함된 FDM 관리 디바이스의 예가 나와 있습니다.

```

Response Body
{
  "items": [
    {
      "version": "nh14yz7tgfgva",
      "name": "AnyConnectWindows_3.2_BGL",
      "description": null,
      "diskFileName": "f3b4daa9-a3b3-11e9-a361-f958979569ccd.pkg",
      "md5Checksum": "bf3013d9e8ce52e905ba4bd4495678c0",
      "platformType": "WINDOWS",
      "id": "3f3a329a-a3b4-11e9-a361-338c2bfc8d92",
      "type": "anyconnectpackagefile",
      "links": {
        "self": "https://bglgrp1224-pod.cisco.com:972/api/fdm/v3/object/anyconnectpackagefiles/3f3a329a-a3b4-11e9-a361-338c2bfc8d92"
      }
    },
    {
      "version": "d51dzvydhbn26",
      "name": "AnyConnectWindows_4.2_BGL",
      "description": null,
      "diskFileName": "ae43a4ad-a3b4-11e9-a361-5f4e70129b91.pkg",
      "md5Checksum": "ac1269fd5d172709954f093d56735d76",
    }
  ]
}

```

## RA VPN AnyConnect 클라이언트 프로파일 업로드

원격 액세스 VPN AnyConnect 클라이언트 프로파일은 파일에 저장된 구성 매개변수의 그룹입니다. 핵심 클라이언트 VPN 기능과 선택적 클라이언트 모듈인 Network Access Manager, AMP Enabler, ISE Posture, 네트워크 가시성, 고객 피드백 경험 프로파일, Umbrella 로밍 보안 및 웹 보안에 대한 구성 설정을 포함하는 다양한 AnyConnect 클라이언트 프로파일이 있습니다.

CDO는 이러한 프로파일을 나중에 그룹 정책에서 사용할 수 있는 개체로 업로드할 수 있습니다.

- **AnyConnect VPN** 프로파일 — AnyConnect 클라이언트 프로파일은 AnyConnect 클라이언트 소프트웨어와 함께 클라이언트에 다운로드됩니다. 이러한 프로파일은 시작 시의 자동 연결 및 자동 다시 연결, 그리고 엔드 유저가 AnyConnect 클라이언트 환경 설정 및 고급 설정에서 옵션을 변경할 수 있는지 여부와 같은 여러 클라이언트 관련 옵션을 정의합니다. CDO는 XML 파일 형식을 지원합니다.
- **AMP Enabler** 서비스 프로파일 - 이 프로파일은 AnyConnect AMP Enabler에 사용됩니다. 원격 액세스 VPN 사용자가 VPN에 연결하면 AMP Enabler 및 이 프로파일이 FDM 관리 디바이스에서 엔드 포인트로 푸시됩니다. CDO는 XML 및 ASP 파일 형식을 지원합니다.
- **피드백 프로파일** - 고객 경험 피드백 프로파일을 추가하고 이 유형을 선택하여 고객이 활성화하고 사용하는 기능 및 모듈에 대한 정보를 수신할 수 있습니다. CDO는 FSP 파일 형식을 지원합니다.
- **ISE Posture** 프로파일 - AnyConnect ISE Posture 모듈용 프로파일 파일을 추가하는 경우 이 옵션을 선택합니다. CDO는 XML 및 ISP 파일 형식을 지원합니다.
- **Network Access Manager** 서비스 프로파일 - Network Access Manager 프로파일 편집기를 사용하여 NAM 프로파일 파일을 설정하고 추가합니다. CDO는 XML 및 NSP 파일 형식을 지원합니다.
- **네트워크 가시성** 서비스 프로파일 - AnyConnect 네트워크 가시성 모듈의 프로파일 파일입니다. NVM 프로파일 편집기를 사용하여 프로파일을 생성할 수 있습니다. CDO는 XML 및 NVMSPP 파일 형식을 지원합니다.
- **Umbrella** 로밍 보안 프로파일 - Umbrella 로밍 보안 모듈을 구축하는 경우 이 파일 유형을 선택해야 합니다. CDO는 XML 및 JSON 파일 형식을 지원합니다.
- **웹 보안** 서비스 프로파일 - 웹 보안 모듈용 프로파일 파일을 추가할 때 이 파일 유형을 선택합니다. CDO는 XML, WSO 및 WSP 파일 형식을 지원합니다.


### Before you begin

적합한 GUI 기반 AnyConnect 프로파일 편집기를 사용하여 필요한 프로파일을 생성합니다. AnyConnect Secure Mobility Client 범주의 [Cisco 소프트웨어 다운로드 센터](#)에서 프로파일 편집기를 다운로드하고 AnyConnect "프로파일 편집기 - Windows/독립형 설치 프로그램(MSI)"을 설치할 수 있습니다. 프로파일 편집기 설치 프로그램에는 독립형 버전의 프로파일 편집기가 포함되어 있습니다. 설치 파일은 Windows 전용이며 파일 이름은 anyconnect-profileeditor-win-<version>-k9.msi입니다. 여기서 <version>은 AnyConnect 버전입니다. 예를 들면 anyconnect-profileeditor-win-4.3.04027-k9.msi와 같습니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다.

Umbrella 로밍 보안 프로파일 편집기를 제외하고 이 패키지에는 모듈을 생성하는 데 필요한 모든 프로파일 편집기가 포함되어 있습니다. 자세한 내용은 [Cisco AnyConnect Secure Mobility Client 관리자](#)

가이드에서 해당 릴리스의 *AnyConnect* 프로파일 편집기 장을 참조하십시오. Umbrella 대시보드와 별도로 Umbrella 로밍 보안 프로파일을 다운로드합니다. 자세한 내용은 [Cisco Umbrella 사용 설명서](#)의 "Umbrella 로밍 보안" 장에서 "Umbrella 대시보드에서 AnyConnect 로밍 보안 프로파일 다운로드" 섹션을 참조하십시오.

## Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 파란색 더하기  버튼을 클릭합니다.
- 단계 3 **RA VPN Objects (ASA & FDM)(RA VPN 개체(ASA 및 FDM)) > AnyConnect Client Profile(AnyConnect 클라이언트 프로파일)**를 클릭합니다.
- 단계 4 **Object Name(개체 이름)** 필드에 AnyConnect 클라이언트 프로파일의 이름을 입력합니다.
- 단계 5 **Browse(찾아보기)**를 클릭하고 프로파일 편집기를 사용하여 생성한 파일을 선택합니다.
- 단계 6 **Open(열기)**를 클릭하여 프로파일을 업로드합니다.
- 단계 7 **Add(추가)**를 클릭하여 개체를 추가합니다.

### 관련 정보:

- RA VPN 그룹 정책 창에서 클라이언트 모듈을 AnyConnect VPN 프로파일과 연결합니다. [새 RA VPN 그룹 정책 생성](#)을 참조하십시오.



**Note** 클라이언트 모듈 연결은 소프트웨어 버전 6.7 이상을 실행하는 모든 ASA 버전 및 FDM에서 지원됩니다.

## 원격 액세스 VPN에 대한 라이선싱 요구 사항

firewall device manager에서 FDM 관리 디바이스에 대한 라이선스를 활성화(등록)하여 RA VPN 연결을 구성합니다. 디바이스를 등록할 때는 내보내기 제어 기능에 대해 활성화된 Smart Software Manager(SSM) 어카운트를 사용하여 등록을 수행해야 합니다. 또한, 평가 라이선스로는 기능을 구성할 수 없습니다.

또한 라이선스를 구매하여 활성화해야 합니다. 중 하나일 수 있습니다. 이러한 라이선스는 FDM 관리 디바이스에 대해 동일하게 처리되지만, ASA 소프트웨어 기반 헤드엔드와 함께 사용할 때는 각기 다른 기능 집합을 허용하도록 설계되었습니다.

firewall device manager에서 라이선스 활성화에 대한 자세한 내용은 디바이스가 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 원격 액세스 VPN 장의 원격 액세스 VPN 라이선싱 요구 사항 섹션을 참조하십시오.

자세한 내용은 [Cisco AnyConnect 주문 가이드](#)를 참조하십시오. 다른 데이터 시트도 <http://www.cisco.com/c/en/us/product...t-listing.html>에서 확인할 수 있습니다.

라이선스 상태를 보려면 다음을 수행합니다.

## Procedure

- 단계 1 왼쪽의 Cisco Defense Orchestrator 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 디바이스를 클릭합니다.
- 단계 3 **FTD** 탭을 클릭하고 원하는 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)를 클릭합니다. 라이선스가 유효한 경우 **Status**(상태)에 **Enabled**(활성화됨)가 표시됩니다.

## 디바이스 모델별 최대 동시 VPN 세션

디바이스 모델에 따라 디바이스에서 허용되는 동시 원격 액세스 VPN 세션 수에는 최대 제한이 적용됩니다. 이 제한은 시스템 성능이 허용할 수 없는 수준으로 저하되지 않도록 설계되었습니다. 용량 계획 시에 이러한 제한을 사용하십시오.

디바이스 모델	최대 동시 원격 액세스 VPN 세션
Firepower 2110	1,500
Firepower 2120	3,500
Firepower 2130	7,500
Firepower 2140	10,000
Firepower Threat Defense Virtual	250

## RADIUS COA(Change of Authorization)

RADIUS CoA(Change of Authorization: 권한 부여 변경) 기능은 인증 후 AAA(인증, 권한 부여 및 계정 관리) 세션의 특성을 변경하는 메커니즘을 제공합니다. RA VPN의 주요 당면 과제는 감염된 엔드포인트로부터 내부 네트워크를 보호하는 것입니다. 또한 엔드포인트에 대한 공격을 해결하여 바이러스 또는 악성코드의 침해를 받을 때 엔드포인트 자체를 보호하는 것입니다. RA VPN 세션 전, 중, 후 모든 단계에서 엔드포인트와 내부 네트워크를 보호해야 합니다. RADIUS CoA 기능을 통해 이 목표를 달성할 수 있습니다.

Cisco Identity Services Engine(ISE) RADIUS 서버를 사용하는 경우, CoA(Change of Authorization) 정책 시행을 구성할 수 있습니다. 정책에서 AAA의 사용자 또는 사용자 그룹을 변경하는 경우, ISE에서는 FTD 디바이스로 CoA 메시지를 전송하여 인증을 다시 시작하고 새 정책을 적용합니다. IPEP(Inline Posture Enforcement Point: 인라인 보안 상태 시행 지점)에는 FTD 디바이스로 설정된 각 VPN 세션에 대한 ACL(Access Control List: 액세스 제어 목록)이 필요하지 않습니다.

관련 정보:

- [FTD 디바이스에서 COA\(Change of Authorization\) 구성](#)

## FTD 디바이스에서 COA(Change of Authorization) 구성

CoA(Change of Authorization) 정책의 대부분은 ISE 서버에서 구성됩니다. 그러나 ISE에 올바르게 연결하려면 FTD 디바이스를 구성해야 합니다.

시작하기 전에

개체에서 호스트 이름을 사용하는 경우 디바이스가 실행 중인 버전에 대한 [Firepower Device Manager 용 Cisco Firepower Threat Defense 설정 가이드](#), 시스템 설정 장의 데이터 및 관리 인터페이스용 **DNS** 구성에 설명된 대로 데이터 인터페이스에 사용할 DNS 서버를 구성해야 합니다. 일반적으로 시스템이 완전히 작동하려면 DNS를 구성해야 합니다.

절차

## Procedure

**단계 1** FDM 관리 디바이스에 대해 firewall device manager에 로그인합니다.

**단계 2** 초기 연결을 ISE로 리디렉션하기 위한 확장 ACL(Access Control List)을 컨피그레이션합니다. 리디렉션 ACL의 목적은 초기 트래픽을 ISE로 전송하여 ISE에서 클라이언트 보안 상태를 평가할 수 있게 하는 것입니다. ACL에서는 ISE에 HTTPS 트래픽을 전송해야 하지만, 이미 ISE가 대상으로 지정된 트래픽 또는 이름 확인을 위해 DNS 서버로 전송되는 트래픽은 전송해서는 안 됩니다. 샘플 리디렉션 ACL은 다음과 같이 표시될 수 있습니다.

```
access-list redirect extended deny ip any host<ISE server IP>
access-list redirect extended deny ip any host<DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

하지만 ACL에는 마지막 ACE(액세스 제어 항목)인 암시적 “deny any any”가 있다는 점에 유의하십시오. 이 예에서는 TCP 포트 www(즉 포트 80)와 일치하는 마지막 ACE가 첫 ACE 3개와 일치하는 모든 트래픽과 일치하지 않습니다. 따라서 이 ACE 3개는 이중화됩니다. 마지막 ACE로 ACL을 생성하기만 해도 동일한 결과를 얻을 수 있습니다. 리디렉션 ACL의 허용 및 거부 작업에서는 일치하는 것은 허용하고 일치하지 않는 것은 거부하여 ACL과 일치하는 트래픽을 확인할 뿐이라는 점에 유의하십시오. 트래픽이 실제로 차단되는 경우는 없으며, 거부된 트래픽은 ISE로 리디렉션되지 않을 뿐입니다. 리디렉션 ACL을 생성하려면 스마트 CLI 개체를 컨피그레이션해야 합니다.

- a. **Device**(디바이스) > **Advanced Configuration**(고급 구성) > **Smart CLI**(스마트 CLI) > **Objects**(개체)를 선택합니다.
- b. +를 클릭하여 새 개체를 생성합니다.
- c. ACL의 이름을 입력합니다. 예: **redirect**(리디렉션).
- d. **CLI Template**(CLI 템플릿)에서 **Extended Access List**(확장 액세스 목록)를 선택합니다.
- e. **Template**(템플릿) 본문에서 다음과 같이 컨피그레이션합니다.
  - configure access-list-entry action = permit
  - source-network = any-ipv4
  - destination-network = any-ipv4
  - configure permit port = any-source
  - destination-port = HTTP

- configure logging = disabled

ACE는 다음과 같이 표시되어야 합니다.

Name	Description
redirect	

CLI Template  
Extended Access List

Template Show disabled Reset

```

1 access-list redirect extended
2 configure access-list-entry permit
3 permit network source [any-ipv4] destination [any-ipv4]
4 configure permit port any-source
5 permit port source ANY destination [HTTP]
6 configure logging disabled
7 disabled log set log-level INFORMATIONAL log-interval 300

```

CANCEL OK

- f. **OK**(확인)를 클릭합니다.

이 ACL은 다음번에 변경 사항을 구축할 때 컨피그레이션됩니다. 다른 정책에서 개체를 사용하여 구축을 강제 적용할 필요가 없습니다.

**Note** 이 ACL은 IPv4에만 적용됩니다. IPv6도 지원하려면 속성이 모두 동일한 두 번째 ACE를 추가하기만 하면 됩니다. 단, 소스 및 대상 네트워크용으로 선택된 any-ipv6은 제외합니다. 트래픽이 ISE 또는 DNS 서버로 리디렉션되지 않도록 다른 ACE를 추가할 수도 있습니다. 먼저 해당 서버의 IP 주소를 보유할 호스트 네트워크 개체를 생성해야 합니다.

단계 3 동적 권한 부여를 위해 RADIUS 서버 그룹을 컨피그레이션합니다.

[RADIUS 서버 개체 또는 그룹 생성 또는 편집](#) 섹션에 제공된 지침에 따라 아래 단계를 수행합니다.

- RADIUS 서버 개체 생성
- RADIUS 서버 그룹 생성

단계 4 이 RADIUS 서버 그룹을 사용하는 연결 프로파일을 생성합니다. [RA VPN 연결 프로파일 컨피그레이션](#)을 참조하십시오. **AAA Authentication**(AAA 인증)을 사용하고(이것만 사용하거나 인증서와 함께 사용), **Primary Identity Source for User Authentication**(사용자 인증을 위한 기본 ID 소스), **Authorization**(권한 부여) 및 **Accounting**(계정 관리) 옵션에서 서버 그룹을 선택합니다.

## FDM-관리 디바이스의 원격 액세스 VPN 구성 확인

원격 액세스 VPN을 구성하고 디바이스에 구성을 배포한 후에는 원격 연결을 수행할 수 있는지 확인합니다.

## Procedure

- 단계 1 외부 네트워크에서 AnyConnect 클라이언트를 사용하여 VPN 연결을 설정합니다. 웹 브라우저를 사용하여 **https://ravpn-address**를 엽니다. 여기서 *ravpn-address*는 VPN 연결을 허용할 외부 인터페이스의 IP 주소 또는 호스트 이름입니다. 필요한 경우, 클라이언트 소프트웨어를 설치하여 연결을 완료합니다. 사용자가 **FDM-관리 디바이스에서 사용자가 AnyConnect 클라이언트 소프트웨어를 설치할 수 있는 방법**을 참조하십시오. 그룹 URL을 구성한 경우, 그룹 URL도 시도해 보십시오.
- 단계 2 **Inventory**(재고 목록) 페이지에서 확인하려는 디바이스를 선택하고 **Device Actions**(디바이스 작업)에서 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 3 **show vpn-sessiondb** 명령을 사용하여 현재 VPN 세션에 대한 요약 정보를 봅니다.
- 단계 4 통계에는 활성 AnyConnect 클라이언트 세션, 누적 세션에 대한 정보, 최대 동시 세션 수, 비활성 세션이 표시되어야 합니다. 다음은 명령의 샘플 출력입니다.

```
> show vpn-sessiondb
-----
VPN Session Summary
-----
Active : Cumulative : Peak Concur : Inactive
-----
AnyConnect Client      :    1 :    49 :    3 :    0
  SSL/TLS/DTLS         :    1 :    49 :    3 :    0
Clientless VPN         :    0 :    1 :    1 :    0
  Browser               :    0 :    1 :    1 :    0
-----

Total Active and Inactive :    1          Total Cumulative :    50
Device Total VPN Capacity : 10000
Device Load                :    0%
-----

Tunnels Summary
-----
Active : Cumulative : Peak Concurrent
-----
Clientless              :    0 :    1 :    1
AnyConnect-Parent      :    1 :    49 :    3
SSL-Tunnel              :    1 :    46 :    3
DTLS-Tunnel             :    1 :    46 :    3
-----
Totals                  :    3 :   142
-----

IPv6 Usage Summary
-----
Active : Cumulative : Peak Concurrent
-----
AnyConnect SSL/TLS/DTLS :    :    :
  Tunneled IPv6         :    1 :   20 :    2
-----
```

- 단계 5 **show vpn-sessiondb anyconnect** 명령을 사용하여 현재 AnyConnect VPN 세션에 대한 세부 정보를 봅니다. 세부 정보에는 사용된 암호화, 전송 및 수신한 바이트 수, 기타 통계 정보가 포함됩니다. VPN 연결을 사용하면 이 명령을 다시 호출할 경우 전송/수신한 바이트 수 변경 사항이 표시되어야 합니다.

```

> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username      : User1|                               Index      : 4820
Assigned IP   : 172.18.0.1                       Public IP   : 192.168.2.20
Assigned IPv6 : 2009::1
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 27731                             Bytes Rx   : 14427
Group Policy  : MyRaVpn|Policy                   Tunnel Group : MyRaVpn
Login Time    : 21:58:10 UTC Mon Apr 10 2017
Duration      : 0h:51m:13s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                               VLAN       : none
Audt Sess ID  : c0a800fd012d400058ebfff2
Security Grp  : none                               Tunnel Zone : 0

```


## FDM-관리 디바이스의 원격 액세스 VPN 구성 세부 정보 보기

### Procedure

단계 1 왼쪽의 CDO 탐색 모음에서 **VPN** > 원격 액세스 **VPN** 구성를 클릭합니다.

단계 2 존재하는 VPN 구성 개체를 클릭합니다.

현재 얼마나 많은 연결 프로파일 및 그룹 정책이 구성되어 있는지 나타내는 요약 정보를 그룹에서 표시합니다.

- RA VPN 구성을 확장하여 연결된 모든 연결 프로파일을 확인합니다.
  - 추가 + 버튼을 클릭하여 새 연결 프로파일을 추가합니다.
  - 보기 버튼()을 클릭하여 연결 프로파일 및 연결 지침에 관한 요약 정보를 엽니다. **Actions**(작업) 아래에서 **Edit**(편집)를 클릭하여 변경 사항을 편집할 수 있습니다.
- **Actions**(작업) 아래의 다음 옵션 중 하나를 클릭하여 추가 작업을 수행할 수 있습니다.
  - 그룹 정책을 할당/추가하려면 **Group Policies**(그룹 정책)를 클릭합니다.
  - 더 이상 필요하지 않은 구성 개체 또는 연결 프로파일을 클릭하고 **Remove**(제거)를 클릭하여 삭제합니다.

## 템플릿

템플릿은 디바이스 구성 파일의 기본 사용 버전 및 일반 사용 버전을 개발할 수 있는 수단을 제공합니다.



- 템플릿은 기존 기본 구성 파일에서 생성됩니다.
- IP 주소 및 포트 번호를 포함하여 예상 값을 쉽게 사용자 지정할 수 있도록 값 매개변수를 지원합니다.
- 여러 디바이스에서 사용하기 위해 매개변수 대체와 함께 내보낼 수 있습니다.

#### 관련 정보

- [FDM-관리 디바이스 템플릿, on page 563](#)
  - [FDM 템플릿 구성, on page 564](#)
  - [FDM-관리 디바이스에 템플릿 적용, on page 569](#)

## FDM-관리 디바이스 템플릿

### FDM-관리 디바이스 템플릿 정보

Cisco Defense Orchestrator를 사용하면 온보딩된 FDM 관리 디바이스 구성의 FDM 관리 디바이스 템플릿을 생성할 수 있습니다. 템플릿을 생성할 때 FDM 관리 디바이스 템플릿에 포함할 부분(개체, 정책, 설정, 인터페이스 및 NAT)을 선택합니다. 그런 다음 해당 템플릿을 수정하고 관리하는 다른 FDM 관리 디바이스를 구성하는 데 사용할 수 있습니다. FDM 관리 디바이스 템플릿은 FDM 관리 디바이스 간의 정책 일관성을 촉진하는 하나의 방법입니다.

FDM 관리 디바이스 템플릿을 생성할 때 전체 템플릿 또는 사용자 지정 템플릿을 생성하도록 선택할 수 있습니다.

- 전체 템플릿은 FDM 관리 구성의 모든 부분을 포함하며 다른 FDM 관리 디바이스에 모든 것을 적용합니다.
- 사용자 지정 템플릿에는 사용자가 선택하는 FDM 관리 구성의 하나 이상의 부분만 포함되며, 다른 FDM 관리 디바이스에서는 해당 부분 및 관련 엔터티만 적용됩니다.



**Important** FDM 관리 디바이스 템플릿은 인증서, Radius, AD 및 RA VPN 개체를 포함하지 않습니다.

### FDM-관리 디바이스 템플릿을 사용하는 방법

다음은 FDM 관리 디바이스 템플릿을 사용할 수 있는 몇 가지 방법입니다.

- 다른 FDM 관리 디바이스의 구성 템플릿을 적용하여 하나의 FDM 관리 디바이스를 구성합니다. 적용하는 템플릿은 모든 FDM 관리 디바이스에서 사용하려는 "모범 사례" 구성을 나타낼 수 있습니다.
- 템플릿을 사용하여 디바이스 구성을 변경하고 랩 환경에서 시뮬레이션한 다음 변경 사항을 라이브 FDM 관리 디바이스에 적용하기 전에 기능을 테스트합니다.

- 템플릿을 생성할 때 인터페이스 및 하위 인터페이스의 특성을 매개변수화합니다. 템플릿을 적용할 때 인터페이스 및 하위 인터페이스의 매개변수화된 값을 변경할 수 있습니다.

변경 로그에 표시되는 내용

디바이스에 템플릿을 적용하면 해당 디바이스의 전체 구성을 덮어씁니다. CDO 변경 로그는 결과적으로 수행되는 모든 변경 사항을 기록합니다. 따라서 변경 로그 항목은 디바이스에 템플릿을 적용한 후 매우 길어집니다.

관련 정보:

- [FDM 템플릿 구성](#)
- [FDM 템플릿 적용](#)

## FDM 템플릿 구성

사전 요구 사항

FDM 관리 디바이스 템플릿을 생성하기 전에 템플릿을 생성할 FDM 관리 디바이스를 Cisco Defense Orchestrator에 온보딩합니다. 온보딩된 FDM 관리 디바이스에서만 FDM 관리 디바이스 템플릿을 생성할 수 있습니다.

템플릿을 사용하여 환경에 추가할 새로운 FDM 관리 디바이스를 구성하는 것이 좋습니다.



**Note** FDM 관리 디바이스에서 템플릿을 생성하는 경우 RA VPN 개체는 템플릿에 포함되지 않습니다.

## FDM 템플릿 생성

템플릿을 생성할 때 모든 부분을 선택하면 관리 IP 주소, 인터페이스 구성, 정책 정보 등 해당 디바이스 구성의 모든 측면이 템플릿에 포함됩니다.

일부분만 선택하면 사용자 지정 템플릿에 다음 엔터티가 포함됩니다.

템플릿 부분	사용자 지정 템플릿에 포함된 부분
액세스 규칙	액세스 제어 규칙 및 해당 규칙에 대한 모든 관련 엔터티를 포함합니다. 개체 및 인터페이스(하위 인터페이스 포함)를 예로 들 수 있습니다.
NAT 규칙	NAT 규칙 및 이러한 NAT 규칙에 필요한 모든 관련 엔터티를 포함합니다. 개체 및 인터페이스(하위 인터페이스 포함)를 예로 들 수 있습니다.
설정	시스템 설정 및 해당 설정에 필요한 모든 관련 엔터티를 포함합니다. 개체 및 인터페이스(하위 인터페이스 포함)를 예로 들 수 있습니다.

템플릿 부분	사용자 지정 템플릿에 포함된 부분
인터페이스	인터페이스 및 하위 인터페이스를 포함합니다.
개체	개체 및 해당 개체에 필요한 모든 관련 엔터티를 포함합니다. 인터페이스 및 하위 인터페이스를 예로 들 수 있습니다.

다음 절차를 사용하여 FDM 관리 디바이스 템플릿을 생성합니다.

**Procedure**

- 단계 1 Cisco Defense Orchestrator 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
  - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
  - 단계 3 **FTD** 탭을 클릭하고 목록에서 원하는 디바이스를 선택합니다.
  - 단계 4 **필터** 또는 **검색** 필드를 사용하여 템플릿을 생성할 FDM 관리 디바이스를 찾습니다.
  - 단계 5 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Create Template**(템플릿 생성)을 클릭합니다. **Name Template**(이름 템플릿)은 디바이스에 있는 각 부분의 개수를 제공합니다. 하위 인터페이스(있는 경우)의 수도 표시됩니다.
  - 단계 6 템플릿에 포함할 부분을 선택합니다.
  - 단계 7 템플릿의 이름을 입력합니다.
  - 단계 8 **Create Template**(보고서 생성)을 클릭합니다.
  - 단계 9 **Parameterize Template**(템플릿 매개변수화) 영역에서 다음을 수행할 수 있습니다.
    - 인터페이스를 매개변수화하려면 중괄호가 표시될 때까지 마우스를 이동하고 해당 인터페이스에 해당하는 셀을 클릭합니다.
    - 하위 인터페이스를 매개변수화하려면 하위 인터페이스가 있는 인터페이스를 확장하고 마우스를 중괄호가 표시될 때까지 옮겨 해당 하위 인터페이스에 해당하는 셀을 클릭합니다.
- 다음 속성을 매개변수화하여 디바이스별로 사용자 지정할 수 있습니다.
- 논리적 이름
  - 주/도
  - IP 주소/넷마스크
- Note** 이러한 속성은 매개변수당 하나의 값만 지원됩니다.
- 단계 10 **Continue**(계속)를 클릭합니다.
  - 단계 11 템플릿 및 모든 매개변수화를 검토합니다. **Done**(완료)을 클릭하여 템플릿을 생성합니다. 이제 방금 생성한 FDM 관리 디바이스 템플릿이 **Inventory**(재고 목록) 페이지에 표시됩니다.

**Note**      템플릿 생성 후 CDO는 **Inventory**(재고 목록) 창에서 해당 템플릿에 포함된 부분을 보여주는 해당 템플릿 부분 아이콘을 표시합니다. 이 정보는 디바이스를 클릭하거나 아이콘 위에 마우스 포인터를 올려놓아도 **Device Details**(디바이스 세부사항) 창에 나타납니다.

다음 그림은 템플릿에 "액세스 규칙", "NAT 규칙" 및 "개체"가 포함되어 있음을 보여주는 부분 아이콘의 예입니다.



## FDM-관리 디바이스 템플릿 편집

다음 절차에 따라 템플릿 매개변수를 편집합니다.

### Procedure

- 단계 1 Cisco Defense Orchestrator 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Templates**(템플릿) 탭을 클릭합니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 **Model/Template**(모델/템플릿) 필터를 사용하여 수정할 템플릿을 찾습니다.
- 단계 5 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Edit Parameters**(매개변수 편집)를 클릭합니다.
- 단계 6 (선택 사항) 텍스트 상자를 직접 편집하여 매개변수를 변경합니다.
- 단계 7 **Save**(저장)를 클릭합니다.

라이브 FDM 관리 디바이스의 구성과 마찬가지로 나머지 FDM 관리 디바이스 템플릿을 편집할 수 있습니다. 다음 구성을 사용하여 FDM 관리 디바이스 템플릿을 편집할 수 있습니다.

- [FDM-관리 디바이스 설정](#)
- [가상 프라이빗 네트워크 관리](#)
- [RA VPN 구성 생성](#)
- [FDM 정책 구성](#)
- [정책 및 구성 일관성 승격](#)

## FDM 템플릿 삭제

Cisco Defense Orchestrator에서 FDM 관리 디바이스를 제거하는 것처럼 FDM 관리 디바이스 템플릿을 삭제합니다.

## Procedure

- 단계 1 CDO 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Templates**(템플릿) 탭을 클릭합니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 필터 및 검색 필드를 사용하여 삭제할 FDM 관리 디바이스 템플릿을 찾습니다.
- 단계 5 **Device Actions**(디바이스 작업) 창에서 **Remove**(제거)(🗑️)를 클릭합니다.
- 단계 6 경고 메시지를 읽고 **OK**(확인)를 클릭하여 템플릿을 삭제합니다.

### 관련 정보:

- [FDM-관리 디바이스 템플릿](#)
- [FDM 템플릿 적용](#)

## FDM 템플릿 적용

템플릿을 적용하기 전에 **Inventory**(재고 목록) 페이지 및 **Model/Template**(모델/템플릿) 필터로 이동하여 템플릿의 내용을 식별할 수 있습니다. Cisco Defense Orchestrator는 해당 템플릿에 포함된 부분을 보여주는 해당 템플릿 부분 아이콘을 표시합니다. 이 정보는 디바이스를 클릭하거나 아이콘 위에 마우스 포인터를 올려놓아도 **Device Details**(디바이스 세부사항) 창에 나타납니다.

다음 속성을 매개변수화하여 디바이스별 맞춤화를 활성화할 수 있습니다. 즉, 템플릿을 적용할 때 디바이스별 값을 적용할 수 있습니다.

FDM 관리 디바이스 템플릿을 적용할 때 템플릿을 생성할 때 구성된 인터페이스 및 하위 인터페이스의 매개변수화된 값을 변경할 수 있습니다.

### 전체 템플릿 적용

전체 FDM 관리 디바이스 템플릿을 적용하여 새 FDM 관리 디바이스를 생성하면 CDO에서 디바이스로 아직 배포되지 않은 모든 단계적 변경 사항을 포함하여 FDM 관리 디바이스의 기존 구성을 완전히 덮어씁니다. 템플릿에 포함되지 않은 디바이스의 모든 항목은 손실됩니다.

### 사용자 지정 템플릿 적용

사용자 지정 FDM 관리 디바이스 템플릿을 다른 FDM 관리 디바이스에 적용하면 템플릿 부분을 기반으로 하는 기존 구성이 유지되거나 제거됩니다. 다음 표에는 다른 FDM 관리 디바이스에서 사용자 지정 템플릿을 적용한 후 발생하는 변경 사항이 나와 있습니다.

템플릿 부분	맞춤형 템플릿 적용 후
액세스 규칙	<ul style="list-style-type: none"> <li>• 사용자 지정 템플릿에 있는 새 액세스 제어 규칙은 디바이스의 기존 액세스 제어 규칙을 덮어씁니다.</li> <li>• 사용자 지정 템플릿의 새 개체 및 인터페이스(하위 인터페이스 포함)는 기존 개체 및 인터페이스를 삭제하지 않고 디바이스에 적용됩니다.</li> </ul>
NAT 규칙	<ul style="list-style-type: none"> <li>• 사용자 지정 템플릿에 있는 새 NAT 규칙은 디바이스의 기존 NAT 규칙을 덮어씁니다.</li> <li>• 사용자 지정 템플릿의 새 개체 및 인터페이스(하위 인터페이스 포함)는 기존 개체 및 인터페이스를 삭제하지 않고 디바이스에 적용됩니다.</li> </ul>
설정	<ul style="list-style-type: none"> <li>• 기존 시스템 설정을 삭제하지 않고 사용자 지정 템플릿의 새 시스템 설정이 디바이스에 적용됩니다.</li> <li>• 사용자 지정 템플릿의 새 개체 및 인터페이스(하위 인터페이스 포함)는 기존 개체 및 인터페이스를 삭제하지 않고 디바이스에 적용됩니다.</li> </ul>
인터페이스	<ul style="list-style-type: none"> <li>• 기존 인터페이스 및 하위 인터페이스를 삭제하지 않고 사용자 지정 템플릿의 새 인터페이스 및 하위 인터페이스가 디바이스에 적용됩니다.</li> <li>• CDO는 디바이스에 있는 인터페이스보다 더 많은 인터페이스가 템플릿에 정의된 디바이스에 템플릿을 적용하는 것을 허용하지 않습니다.</li> </ul>
개체	<ul style="list-style-type: none"> <li>• 기존 개체를 삭제하지 않고 사용자 지정 템플릿의 새 개체가 디바이스에 적용됩니다.</li> <li>• 기존 인터페이스 및 하위 인터페이스를 삭제하지 않고 사용자 지정 템플릿의 새 인터페이스 및 하위 인터페이스가 디바이스에 적용됩니다.</li> </ul>

사전 요구 사항

템플릿을 적용하기 전에 다음 조건을 충족해야 합니다.

- 템플릿을 사용하는 경우, 템플릿에 대한 변경 사항이 커밋되었고 템플릿이 **Inventory**(재고 목록) 페이지에서 "Synced(동기화됨)" 상태인지 확인합니다.
- FDM 관리 디바이스를 템플릿으로 사용하는 경우, 디바이스에 배포하려는 CDO의 변경 사항이 배포되었는지, 그리고 배포되지 않은 **firewall device manager** 콘솔의 변경 사항이 없는지 확인합니다. 디바이스는 **Inventory**(재고 목록) 페이지에서 Synced(동기화됨) 상태로 표시되어야 합니다.

디바이스에 템플릿을 적용하는 것은 3단계 프로세스입니다.

1. 전체 템플릿 적용
2. 디바이스 및 네트워크 설정 검토

### 3. 디바이스에 변경 사항 구축

## FDM-관리 디바이스에 템플릿 적용



**Important** 디바이스에 변경 사항을 구축하기 전에 다음 절차를 계속 진행합니다.

#### 디바이스 및 네트워킹 설정 검토

템플릿을 적용하기 전에 **변경 요청 관리**를 사용하여 변경 사항에 추적 레이블을 적용할 수 있습니다. 다음 절차에 따라 FDM 관리 디바이스 템플릿을 적용합니다.

#### Procedure

단계 1 (선택 사항) 시작하기에 앞서 FDM 관리 디바이스에 다른 템플릿을 적용하기 전에 디바이스의 템플릿을 만듭니다. 이렇게 하면 디바이스 및 네트워킹 설정을 다시 적용해야 할 때 참조할 수 있는 구성 백업이 제공됩니다.

단계 2 CDO 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.

단계 3 **Templates**(템플릿) 탭을 클릭합니다.

단계 4 **FTD** 탭을 클릭합니다.

단계 5 필터 및 검색 필드를 사용하여 템플릿을 적용할 FDM 관리 디바이스 또는 템플릿을 찾습니다.

**Note** 이 시점에서 템플릿의 이름을 변경하면 전체 디바이스 구성 또는 템플릿이 *DeviceName*에 적용됩니다. *DeviceName*에 이 변경 사항을 구축하면 해당 디바이스에서 실행 중인 전체 구성을 덮어씁니다.

단계 6 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Apply Template**(템플릿 적용)을 클릭합니다.

단계 7 **Select Template**(템플릿 선택)을 클릭하고 원하는 템플릿을 선택한 후 **Continue**(계속)를 클릭합니다.

단계 8 다음을 구성하고 각 화면에 나타나는 **Continue**(계속)를 클릭합니다.

a. **Map Interfaces**(인터페이스 매핑): 템플릿과 디바이스 간의 인터페이스 매핑을 확인하거나 변경합니다. 단일 디바이스 인터페이스에 두 개 이상의 템플릿 인터페이스를 매핑할 수는 없습니다. 인터페이스 구성이 지원되지 않는 경우 계속해서 템플릿을 적용할 수 없습니다.

**Note** CDO는 디바이스에 있는 인터페이스보다 더 많은 인터페이스가 템플릿에 정의된 디바이스에 템플릿을 적용하는 것을 허용하지 않습니다.

b. **Fill Parameters**(매개변수 작성): 템플릿을 적용할 디바이스의 인터페이스 또는 하위 인터페이스 매개변수 값을 사용자 지정합니다.

c. **Review**(검토): 템플릿 구성을 검토하고 기존 디바이스 구성을 템플릿의 구성으로 덮어쓸 준비가 되면 **Apply Template**(템플릿 적용)을 클릭합니다.

단계 9 **Review and deploy**(검토 및 구축)를 클릭해서 지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 디바이스 및 네트워킹 설정 검토

FDM 관리 디바이스 템플릿을 생성할 때 Cisco Defense Orchestrator는 전체 디바이스 구성을 템플릿에 복사합니다. 따라서 원래 디바이스의 관리 IP 주소 같은 것이 템플릿에 포함됩니다. 디바이스에 템플릿을 적용하기 전에 다음 디바이스 및 네트워크 설정을 검토합니다.

### Procedure

단계 1 이러한 FDM 관리 디바이스 설정을 검토하여 새 FDM 관리 디바이스에 대한 올바른 정보를 반영하는지 확인합니다.

- [FDM-관리 디바이스 설정](#)
- [관리 인터페이스](#)
- [호스트 이름](#)

단계 2 **FDM 액세스 제어 정책 구성**을 검토하여 해당하는 경우 규칙이 새 FDM 관리 디바이스의 IP 주소를 참조하는지 확인합니다.

단계 3 **inside\_zone** 및 **outside\_zone** 보안 개체를 검토하여 새 FDM 관리 디바이스에 대한 올바른 IP 주소를 참조하는지 확인합니다.

단계 4 NAT 정책을 검토하여 새 FDM 관리 디바이스에 대한 올바른 IP 주소를 참조하는지 확인합니다.

단계 5 인터페이스 구성을 검토하여 새 FDM 관리 디바이스에 대한 올바른 구성을 반영하는지 확인합니다.

## 디바이스에 변경 사항 구축

지금 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

관련 정보:

- [FDM-관리 디바이스 템플릿](#)
- [FDM 템플릿 구성](#)



## FDM-관리 디바이스 템플릿으로 ASA 구성 마이그레이션



**Attention** Secure Firewall device manager(FDM) 지원 및 기능은 요청 시에만 제공됩니다. 테넌트에서 Firewall Device Manager 지원을 아직 활성화하지 않은 경우 디바이스를 관리하거나 FDM 관리 디바이스에 구축할 수 없습니다. [TAC를 사용하여 지원 티켓 열기](#)에 요청을 보냅니다.

Cisco Defense Orchestrator는 ASA를 FDM 관리 디바이스로 마이그레이션하는 데 도움이 됩니다. CDO는 ASA에서 실행 중인 구성의 이러한 요소를 FDM 관리 디바이스 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

- 액세스 제어 규칙(ACL)
- 인터페이스
- NAT(네트워크 주소 변환) 규칙
- 네트워크 개체 및 네트워크 그룹 개체
- 경로
- 서비스 개체 및 서비스 그룹 개체
- 사이트 간 VPN

ASA 실행 구성의 이러한 요소가 FDM 관리 디바이스 템플릿으로 마이그레이션되면 FDM 템플릿을 CDO에서 관리하는 새 FDM 관리 디바이스에 적용할 수 있습니다. FDM 관리 디바이스는 템플릿에 정의된 구성을 채택하므로, 이제 FDM 관리 디바이스는 ASA 실행 구성의 일부 측면으로 구성됩니다.

구성을 실행하는 ASA의 다른 요소는 이 프로세스를 사용하여 마이그레이션되지 않습니다. 이러한 다른 요소는 FDM 관리 디바이스 템플릿에서 빈 값으로 표시됩니다. 템플릿이 FDM 관리 디바이스에 적용되면 마이그레이션한 값을 새 FDM 관리 디바이스에 적용하고 빈 값은 무시합니다. 새 FDM 관리 디바이스의 다른 기본값은 그대로 유지됩니다. 마이그레이션하지 않은 구성을 실행하는 ASA의 다른 요소는 마이그레이션 프로세스 외부의 FDM 관리 디바이스에서 다시 생성해야 합니다.

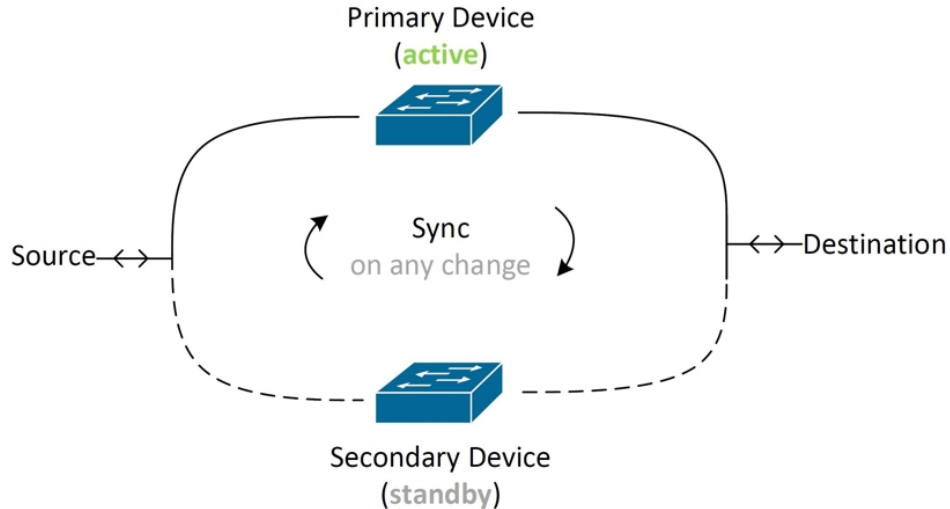
CDO를 사용하여 ASA를 FDM 관리 디바이스로 마이그레이션하는 프로세스에 대한 전체 설명은 [Cisco Defense Orchestrator를 사용하여 ASA를 FDM 매니지드 디바이스로 마이그레이션](#)을 참조하십시오.

## FDM-관리 고가용성

### 고가용성 정보

HA(고가용성) 또는 페일오버 구성은 기본/보조 설정에 두 디바이스를 결합하여 기본 디바이스에 장애가 발생할 경우 보조 디바이스가 자동으로 대신 작동하도록 합니다. 페일오버라고도 하는 고가용성을 구성하려면 2개의 동일한 FDM 관리 디바이스가 전용 페일오버 링크와 선택 사항인 상태 링크를 통해 서로 연결되어 있어야 합니다. 액티브 유닛의 상태(하드웨어, 인터페이스, 소프트웨어 및 환경 상태)를 모니터링하여 특정 페일오버 조건이 충족되는지 확인합니다. 이러한 조건이 충족되면 장애 조치가 이루어집니다. 이렇게 하면 디바이스 오류가 발생하는 경우 또는 디바이스가 업그레이드

되는 유지 보수 기간에 네트워크 운영을 유지할 수 있습니다. 자세한 내용은 아래의 관련 문서를 참조하십시오.



두 유닛은 액티브/스탠바이 쌍을 이루는데, 여기서 기본 유닛은 액티브 유닛이며 트래픽을 전달합니다. 보조(스탠바이) 유닛은 능동적으로 트래픽을 전달하지 않지만, 액티브 유닛에서 컨피그레이션 및 기타 상태 정보를 동기화합니다. 유닛 두 개에서는 페일오버 링크를 통해 통신을 수행하여 각 유닛의 작동 상태를 확인합니다.



**Note** HA 쌍의 변경 사항을 수락하거나 FDM 관리 HA 쌍에 구축하도록 선택하면 HA 쌍의 액티브 디바이스와 통신하게 됩니다. 즉, 구성 및 백업은 액티브 디바이스에서만 가져옵니다.

인증서 및 고가용성 쌍

FDM 관리 HA 쌍에 인증서를 적용하면 CDO는 액티브 디바이스에만 인증서를 적용합니다. 액티브 디바이스를 구축하는 경우에만 구성 및 인증서가 스탠바이 디바이스와 동기화됩니다. FDM 관리를 통해 액티브 디바이스에 새 인증서를 적용하는 경우 액티브 디바이스와 스탠바이 디바이스에 서로 다른 두 개의 인증서가 있을 수 있습니다. 이로 인해 다양한 문제가 발생할 수 있으며, 특히 페일오버 또는 페일오버 기록에 문제가 생길 수 있습니다. 두 디바이스가 성공적으로 작동하려면 동일한 인증서가 있어야 합니다. FDM 관리를 통해 인증서를 변경해야 하는 경우 변경 사항을 구축하고 HA 쌍 내에서 인증서를 동기화해야 합니다.

관련 정보:

- [FDM-관리 고가용성용 페일오버 및 스테이트풀 링크](#)
- [FDM-관리 관리 고가용성 쌍 요구 사항](#)
- [FDM-관리 고가용성 쌍 생성](#)
- [고가용성의 FDM-관리 디바이스 페이지](#)

- FDM-관리 고가용성 페어링 끊기
- FDM-관리고가용성 장애 조치 기록
- FDM-관리 고가용성 상태 새로 고침
- FDM-관리 고가용성 쌍에서 강제 페일 오버
- FDM-관리 고가용성 쌍 업그레이드
- 변경 사항 읽기, 삭제, 확인 및 구축
- FDM-관리 디바이스에서 CDO로 구성 변경 사항 읽기
- CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축

## FDM-관리 관리 고가용성 쌍 요구 사항

고가용성 요구 사항

고가용성(HA) 쌍을 생성하기 전에 설정해야 하는 몇 가지 요구 사항이 있습니다.

**HA**에 대한 물리적 및 가상 디바이스 요구 사항

다음 하드웨어 요구 사항을 충족해야 합니다.

- 디바이스의 하드웨어 모델이 동일해야 합니다.
- 디바이스에 동일한 모듈이 설치되어 있어야 합니다. 예를 들어, 한 디바이스에 네트워크 모듈(선택 사항)이 있는 경우 다른 디바이스에도 동일한 네트워크 모듈을 설치해야 합니다.
- 디바이스의 인터페이스 유형과 수가 동일해야 합니다.
- Cisco Defense Orchestrator에서 HA 쌍을 생성하려면 두 디바이스에 모두 관리 인터페이스가 구성되어 있어야 합니다. 디바이스에 데이터 인터페이스가 구성된 경우 FDM 관리 UI를 통해 HA 쌍을 생성한 다음 CDO에 쌍을 온보딩해야 합니다.



**Note** HA 쌍에서는 FDM 관리 템플릿을 사용할 수 없습니다.

**HA**의 소프트웨어 요구 사항

물리적 및 가상 FDM 관리 디바이스 모두에 대해 다음 소프트웨어 요구 사항을 충족해야 합니다.

- Defense Orchestrator에 온보딩된 두 개의 독립형 FDM 관리 디바이스가 있습니다.
- 두 디바이스가 정확히 동일한 소프트웨어 버전을 실행해야 합니다. 즉, 주 버전 번호(첫 번째), 부 버전 번호(두 번째) 및 유지 보수 버전 번호(세 번째)가 같아야 합니다. **Inventory**(재고 목록) 페이지의 **Device Details**(장치 세부 정보) 창에서 버전을 찾거나 CLI에서 `show version` 명령을 사용할 수 있습니다.



**Note** 각기 다른 버전이 설치된 디바이스도 조인할 수는 있지만, 유닛을 같은 소프트웨어 버전으로 업그레이드할 때까지는 컨피그레이션을 스탠바이 유닛으로 가져올 수 없으며 페일오버가 작동하지 않습니다.

- 두 디바이스가 모두 로컬 관리자 모드여야 합니다(FDM을 사용하여 구성되어 있어야 함). 두 디바이스에서 모두 FDM에 로그인할 수 있다면 로컬 관리자 모드인 것입니다. CLI에서 `show managers` 명령을 사용하여 확인할 수도 있습니다.
- CDO를 온보딩하기 전에 각 디바이스에 대해 초기 설정 마법사를 완료해야 합니다.
- 각 디바이스에 자체 관리 IP 주소가 있어야 합니다. 관리 인터페이스의 컨피그레이션은 디바이스 간에 동기화되지 않습니다.
- 디바이스의 NTP 컨피그레이션이 같아야 합니다.
- DHCP를 사용하여 주소를 획득하도록 인터페이스를 구성할 수는 없습니다. 즉, 모든 인터페이스에 고정 IP 주소가 있어야 합니다.

참고: 인터페이스 구성을 변경하는 경우 HA를 설정하기 전에 디바이스에 변경 사항을 구축해야 합니다.

- 두 디바이스를 모두 동기화해야 합니다. 보류 중인 변경 사항 또는 충돌이 탐지된 경우 자세한 내용은 [구성 충돌 해결](#) 및 [구성 충돌 해결](#)을 참조하십시오.



**Note** HA 쌍의 변경 사항을 수락하거나 FDM 관리 HA 쌍에 구축하도록 선택하면 HA 쌍의 액티브 디바이스와 통신하게 됩니다. 즉, 구성 및 백업은 액티브 디바이스에서만 가져옵니다.

## HA의 스마트 라이선스 요구 사항

물리적 및 가상 FDM 관리 디바이스 모두에 대해 다음 라이선스 요구 사항을 충족해야 합니다.

- HA 쌍의 두 디바이스에는 모두 등록된 라이선스 또는 평가판 라이선스가 있어야 합니다. 등록된 디바이스는 다른 Cisco Smart Software Manager 어카운트에 등록할 수 있습니다. 단, 이러한 어카운트의 내보내기 제어 기능 설정 상태가 같아야 합니다(둘 다 활성화되어 있거나 비활성화되어 있어야 함). 그러나 각 디바이스에 각기 다른 선택적 라이선스를 활성화했는지는 중요하지 않습니다.
- 작동 중에는 HA 쌍 내의 두 디바이스에 동일한 라이선스가 있어야 합니다. 라이선스가 부족하면 디바이스별로 컴플라이언스 상태가 달라질 수 있습니다. Smart License에 포함되어 있는 구매한 엔타이틀먼트가 충분하지 않으면 정확한 수의 라이선스를 구매할 때까지 어카운트는 컴플라이언스 위반 상태(디바이스 중 하나가 규정을 준수하더라도)가 됩니다.

디바이스가 평가 모드인 경우에는 해당 디바이스에서 CDO에 대한 등록 상태도 동일한지 확인해야 합니다. 또한 Cisco Success Network 참여에 대한 동의 여부도 동일한지 확인해야 합니다. 등록된 디바

이스의 경우 유닛별로 설정은 다를 수 있지만, 기본(액티브) 디바이스에 구성된 설정에 따라 보조 디바이스가 등록되거나 등록 취소됩니다. 기본 디바이스에서 Cisco Success Network 참여에 동의하는 것은 보조 디바이스에서도 Cisco Success Network 참여에 동의한다는 의미입니다.

내보내기 제어 기능에 대한 설정이 서로 다른 계정에 디바이스를 등록하거나 한 유닛은 등록하고 다른 유닛은 평가 모드에 있는 HA 쌍을 생성하려는 경우, HA 가입에 실패할 수 있습니다. 내보내기 제어 기능에 대한 일관성 없는 설정으로 IPsec 암호화 키를 구성하면 HA를 활성화한 후에 두 디바이스가 모두 활성화됩니다. 이로 인해 지원되는 네트워크 세그먼트에서의 라우팅이 영향을 받게 되고, 이를 복구하기 위해서는 보조 유닛에서 HA를 수동으로 해제해야 합니다.

### HA의 클라우드 서비스 구성

HA 쌍 내의 두 디바이스 모두 Cisco Cloud에 이벤트 전송이 활성화되어 있어야 합니다. 이 기능은 FDM UI에서 사용할 수 있습니다. 이 기능을 활성화하려면 **System Settings**(시스템 설정)로 이동하여 **Cloud Services**(클라우드 서비스)를 클릭합니다. 이 옵션을 활성화하지 않으면 CDO에서 HA 쌍을 구성할 수 없으며 이벤트 설명 오류가 발생합니다. 자세한 내용은 실행 중인 버전의 [Firepower Device Manager 구성 가이드](#)에서 클라우드 서비스 구성 장을 참조하십시오.

## FDM-관리 고가용성 쌍 생성

Defense Orchestrator에서 FDM 관리HA 쌍을 생성하기 전에 먼저 [FDM-관리 관리 고가용성 쌍 요구 사항](#)에 설명된 요구 사항을 충족하는 두 개의 독립형 FDM 관리디바이스를 온보딩해야 합니다.



**Note** CDO에서 HA 쌍을 생성하려면 두 디바이스에 모두 관리 인터페이스가 구성되어 있어야 합니다. 디바이스에 데이터 인터페이스 구성이 있는 경우 FDM 콘솔을 통해 HA 쌍을 생성한 다음 CDO에 온보딩해야 합니다.

FDM 관리 HA 쌍을 생성하면 기본 디바이스가 액티브 디바이스가 되고 보조 디바이스는 기본적으로 스탠바이 디바이스가 됩니다. 모든 구성 변경 또는 구축은 기본 디바이스를 통해 이루어지며, 보조 디바이스는 기본 유닛을 사용할 수 없게 될 때까지 스탠바이 모드를 유지합니다.

HA 쌍에서 구성 변경 사항을 수락하거나 FDM 관리 HA 쌍에 구축하도록 선택하면 HA 쌍의 액티브 디바이스와 통신하게 됩니다. 기본 디바이스에 대한 모든 변경 사항은 기본 디바이스와 보조 디바이스 간의 링크를 통해 전송됩니다. CDO는 기본 디바이스에 변경 사항을 구축하고 기본 디바이스에서 변경 사항을 수락합니다. 따라서 **Inventory**(재고 목록) 페이지에 쌍에 대한 단일 항목이 표시됩니다. 구축이 완료되면 기본 디바이스가 모든 구성 변경 사항을 보조 디바이스에 동기화했습니다.

CDO가 액티브 디바이스와만 통신하는 방식과 마찬가지로, FDM 관리 HA 쌍을 예약하거나 백업하도록 선택하면 액티브 디바이스만 백업할 수 있습니다.



**Note** 생성 프로세스 중에 HA 디바이스에 문제가 발생하거나 HA 쌍이 정상 상태가 아닌 경우, 쌍 생성을 다시 시도하기 전에 HA 구성을 수동으로 해제해야 합니다.

## 절차

다음 절차에 따라 두 개의 독립형 FTD 디바이스에서 HA 쌍을 생성합니다.

### Procedure

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 **FTD** 탭을 클릭하고 기본 디바이스로 설정할 디바이스를 선택합니다.

**Note** CDO는 DHCP로 구성된 디바이스와의 HA 쌍 생성을 지원하지 않습니다.

단계 4 Management(관리) 창에서 **High Availability**(고가용성)를 클릭합니다.

단계 5 보조 디바이스에 대한 영역을 찾고 **Select Device**(디바이스 선택)를 클릭한 다음 대상 디바이스 목록에서 디바이스를 선택합니다.

단계 6 Failover Link(페일오버 링크)를 구성합니다.

- a. **Physical Interface**(물리적 인터페이스)를 클릭하고 드롭다운 메뉴에서 인터페이스를 선택합니다.
- b. 적절한 **IP Type**(IP 유형)을 선택합니다.
- c. 기본 **IP** 주소를 입력합니다.
- d. 보조 **IP** 주소를 입력합니다.
- e. 넷마스크를 입력합니다. 기본적으로 이 값은 24입니다.
- f. 해당하는 경우 유효한 **IPSec** 암호화 키를 입력합니다.

단계 7 스테이트풀 링크를 구성합니다. 페일오버 링크와 동일한 구성을 사용하려면 **The same as Failover Link**(페일오버 링크와 동일) 체크 박스를 선택합니다. 다른 구성을 사용하려면 다음 절차를 수행합니다.

- a. **Physical Interface**(물리적 인터페이스)를 클릭하고 드롭다운 메뉴에서 인터페이스를 선택합니다. 기본 디바이스와 보조 디바이스의 물리적 인터페이스 수가 동일해야 합니다.
- b. 적절한 **IP Type**(IP 유형)을 선택합니다.
- c. 기본 **IP** 주소를 입력합니다.
- d. 보조 **IP** 주소를 입력합니다.
- e. 넷마스크를 입력합니다. 기본적으로 이 값은 24입니다.

단계 8 화면 오른쪽 상단에 있는 **Create**(생성)를 클릭하여 마법사를 종료합니다. CDO는 즉시 **High Availability Status**(고가용성 상태) 페이지로 리디렉션합니다. 이 페이지에서 HA 생성 상태를 모니터링할 수 있습니다. HA 쌍이 생성되면 **Inventory**(재고 목록) 페이지에 해당 쌍이 단일 행으로 표시됩니다.

단계 9 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 고가용성의 FDM-관리 디바이스 페이지

HA(고가용성)의 FDM 관리 디바이스 관리 페이지는 FDM 관리 디바이스에 대한 다목적 페이지입니다. 이 페이지는 이미 HA 쌍으로 구성된 디바이스에만 사용할 수 있습니다. FDM 관리 HA 쌍을 온보딩하거나 두 개의 독립형 FDM 관리 디바이스에서 FDM 관리 HA 쌍을 생성할 수 있습니다.

**Inventory**(재고 목록) 페이지에서 독립형 FDM 관리 디바이스를 선택하는 경우 이 페이지는 HA 쌍을 생성하는 마법사 역할을 합니다. 현재 두 개의 Cisco Defense Orchestrator 디바이스가 FDM 관리에 온보딩되어 있어야 쌍을 생성할 수 있습니다. CDO에서 FDM 관리 HA 쌍을 생성하려면 [FDM-관리 고가용성 쌍 생성](#)을 참조하십시오.

**Inventory**(재고 목록) 페이지에서 FDM 관리 HA 쌍을 선택하는 경우 이 페이지는 **Overview**(개요) 페이지 역할을 합니다. 여기에서 HA 구성 및 페일오버 기록은 물론 페일오버 강제 실행, 페일오버 기준 편집, HA 링크 제거 등의 실행 가능한 작업 항목을 볼 수 있습니다.

### 고가용성 관리 페이지

High Availability(고가용성) 페이지를 보려면 다음 절차를 사용합니다.

#### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 독립형 FDM 관리 디바이스 또는 FDM 관리 HA 쌍의 액티브 FDM 관리 디바이스를 선택합니다.
- 단계 4 **Management**(관리) 창에서 **High Availability**(고가용성)를 클릭합니다.

#### 관련 정보:

- [FDM-관리고가용성 장애 조치 기록](#)
- [고가용성 페일오버 기준 수정](#)
- [FDM-관리 고가용성 쌍에서 강제 페일 오버](#)
- [FDM-관리 고가용성 페어링 끊기](#)
- [FDM-관리 고가용성 상태 새로 고침](#)

### 고가용성 페일오버 기준 수정

FTD HA 쌍이 생성된 후 페일오버 기준을 편집할 수 있습니다.

## Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 FTD HA 쌍의 액티브 디바이스를 선택합니다.
- 단계 4 Management(관리) 창에서 **High Availability**(고가용성)를 클릭합니다.
- 단계 5 Failover Criteria(페일오버 기준) 창에서 **Edit**(편집)를 클릭합니다.
- 단계 6 필요에 따라 변경하고 **Save**(저장)를 클릭합니다.
- 단계 7 액티브 디바이스에 대한 변경 사항을 바로 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## FDM-관리 고가용성 페어링 끊기

HA를 중단하면 대기 디바이스에 구성된 인터페이스가 자동으로 비활성화됩니다. 이 프로세스 중에 디바이스에서 트래픽 중단이 발생할 수 있습니다. HA 쌍이 성공적으로 제거되면 상태 페이지에서 **High Availability**(고가용성) 페이지로 리디렉션됩니다. 이 페이지에서 동일한 기본 디바이스를 사용하여 다른 HA 쌍을 생성할 수 있습니다.



**Note** HA 쌍이 성공적으로 제거될 때까지 두 디바이스 중 어디에도 배포할 수 없습니다.

관리 인터페이스를 사용하여 **HA** 중단

관리 인터페이스를 사용하여 구성된 쌍에 대해 HA를 중단하면 중단을 완료하는 데 10분 이상 걸릴 수 있으며, 이 프로세스 중에 두 디바이스가 모두 오프라인 상태가 됩니다. HA 구성이 성공적으로 제거되면 CDO는 **Services & Devices**(서비스 및 디바이스) 페이지에서 두 디바이스를 독립형 디바이스로 표시합니다.

데이터 인터페이스를 사용하여 **HA** 중단

데이터 인터페이스로 구성된 쌍에 대해 HA를 중단하면 중단을 완료하는 데 20분 이상 걸릴 수 있으며 두 디바이스 모두 오프라인이 됩니다. HA 구성이 제거된 후 활성 디바이스를 수동으로 다시 연결해야 합니다.

대기 디바이스는 HA 구성을 유지하지만 활성 디바이스와 동일한 구성을 가지므로 연결할 수 없게 됩니다. CDO 외부에서 IP 인터페이스를 수동으로 재구성한 다음 디바이스를 독립형으로 다시 온보딩해야 합니다.

### 고가용성 분리

다음 절차를 사용하여 두 FDM 관리 디바이스의 HA 페어링을 제거합니다.



## Procedure

- 단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭하고 FDM 관리 HA 쌍의 액티브 디바이스를 선택합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 **Management**(관리) 창에서 **High Availability**(고가용성)를 클릭합니다.
- 단계 5 **Break High Availability**(고가용성 중단)를 클릭합니다.
- 단계 6 CDO가 HA 구성을 제거하고 두 디바이스가 **Inventory**(재고 목록) 페이지에 독립형 디바이스로 표시됩니다.
- 단계 7 두 디바이스에 새 구성을 구축하려면 **CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축**.
- 단계 8 액티브 디바이스에 대한 변경 사항을 바로 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## OOB(Out of Band) 고가용성 분리

FDM 인터페이스를 사용하여 FDM 관리 HA 쌍을 해제하면 Cisco Defense Orchestrator에서 HA 쌍의 구성 상태가 **Conflict Detected**(충돌 탐지됨)로 변경됩니다. HA를 해제한 후에는 FDM 관리를 통해 기본 디바이스에 변경 사항을 구축한 다음 CDO에서 **구성 충돌 해결**해야 합니다.

디바이스가 Synced(동기화됨) 상태가 되면 CDO에서 수행한 구성 변경 사항을 디바이스에 구축할 수 있습니다.

FDM 관리 인터페이스를 사용하여 HA를 해제한 후에는 CDO에서 변경 사항을 되돌리지 않는 것이 좋습니다.

관련 정보:


- [FDM-관리고가용성 장애 조치 기록](#)
- [FDM-관리 고가용성 상태 새로 고침](#)
- [FDM-관리 고가용성 쌍에서 강제 페일 오버](#)
- [변경 사항 읽기, 삭제, 확인 및 구축](#)

## FDM-관리 고가용성 쌍에서 강제 페일 오버

페일 오버를 강제 실행하여 FDM 관리 HA 쌍 내에서 활성 및 대기 디바이스를 전환합니다. 최근에 새 인증서를 활성 디바이스에 적용했고 변경 사항을 배포하지 않은 경우 대기 디바이스는 원래 인증서를 유지하고 페일 오버가 실패합니다. 활성 및 대기 디바이스에는 동일한 인증서가 적용되어야 합니다. 페일 오버를 수동으로 강제 적용하려면 다음 절차를 따르십시오.

## Procedure

---

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 FDM 관리 HA 쌍의 활성 디바이스를 선택합니다.
- 단계 5 관리 창에서 **High Availability**(고가용성)를 클릭합니다.
- 단계 6 옵션 아이콘  를 클릭합니다.
- 단계 7 **Switch Mode**(모드 전환)를 클릭합니다. 활성 디바이스는 이제 대기 상태이며 대기 디바이스는 이제 활성 상태입니다.

### 관련 정보:

- [FDM-관리 고가용성 페어링 끊기](#)
- [FDM-관리고가용성 장애 조치 기록](#)
- [FDM-관리 고가용성 상태 새로 고침](#)
- [FDM-관리 고가용성 쌍에서 강제 페일 오버](#)

## FDM-관리고가용성 장애 조치 기록

### Procedure

---

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 FDM 관리 HA 쌍의 활성 디바이스를 선택합니다.
- 단계 5 관리 창에서 **High Availability**(고가용성)를 클릭합니다.
- 단계 6 장애 조치 기록을 클릭합니다. CDO는 HA 쌍이 형성된 이후 기본 및 보조 장치 모두에 대한 장애 조치 기록을 자세히 설명하는 창을 생성합니다.

**Note** 장애 조치 기록은 **Inventory**(인벤토리) 페이지에서 사용할 수 있는 쌍의 변경 로그에도 표시됩니다.


### 관련 정보:

- [FDM-관리 고가용성 페어링 끊기](#)
- [FDM-관리고가용성 장애 조치 기록](#)
- [FDM-관리 고가용성 상태 새로 고침](#)

- FDM-관리 고가용성 쌍에서 강제 페일 오버

## FDM-관리 고가용성 상태 새로 고침

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 FDM 관리 디바이스 또는 FDM 관리 HA 쌍을 선택합니다.
- 단계 4 **Management**(관리) 창에서 **High Availability**(고가용성)를 클릭합니다.
- 단계 5 옵션 아이콘  를 클릭합니다.
- 단계 6 **Get Latest Status**(최신 상태 가져오기)를 클릭합니다. CDO는 기본 디바이스에서 상태를 요청합니다.

### 관련 정보:

- FDM-관리 고가용성 페어링 끊기
- FDM-관리고가용성 장애 조치 기록
- FDM-관리 고가용성 상태 새로 고침
- FDM-관리 고가용성 쌍에서 강제 페일 오버

## FDM-관리 고가용성용 페일오버 및 스테이트풀 링크

### 페일오버 링크 및 (선택 사항) 스테이트풀 링크

페일오버 링크는 두 유닛 사이의 전용 연결입니다. 스테이트풀 페일오버 링크 역시 전용 연결이지만, 페일오버 링크 하나를 페일오버/상태가 결합된 링크로 사용할 수도 있고 별도의 전용 상태 링크를 생성할 수도 있습니다. 페일오버 링크만 사용하는 경우에는 스테이트풀 정보가 해당 링크를 통해 전송되며 스테이트풀 페일오버 기능도 유지됩니다. 기본적으로 페일오버 및 스테이트풀 페일오버 링크의 통신은 암호화되지 않은 일반 텍스트로 이루어집니다. IPsec 암호화 키를 구성하면 통신을 암호화하여 보안을 강화할 수 있습니다.

사용되지 않는 모든 데이터 물리적 인터페이스를 페일오버 링크 및 전용 상태 링크(선택 사항)로 사용할 수 있습니다. 그러나 현재 특정 이름으로 구성되어 있거나 하위 인터페이스가 있는 인터페이스는 선택할 수 없습니다. 페일오버 및 스테이트풀 페일오버 링크 인터페이스는 일반 네트워킹 인터페이스로 구성되지 않습니다. 이러한 인터페이스는 페일오버 통신에만 사용되며 통과 트래픽 또는 관리 액세스에는 사용할 수 없습니다. 컨피그레이션이 디바이스 간에 동기화되므로 링크의 양쪽 끝에 같은 포트 번호를 선택해야 합니다. 예를 들어 페일오버 링크를 위해 두 디바이스에서 모두 GigabitEthernet1/3을 선택합니다.



**Note** FDM 관리 디바이스에서는 사용자 데이터와 장애 조치 링크 간에 인터페이스 공유를 지원하지 않습니다.

### 페일오버 링크

페일오버 쌍의 두 유닛은 페일오버 링크를 통해 지속적으로 통신하여 각 유닛의 작동 상태를 확인하고 컨피그레이션 변경 사항을 동기화합니다. 다음 정보는 링크를 통해 공유됩니다.

- 유닛 상태(액티브 또는 스탠바이)
- Hello 메시지(keep-alives)
- 네트워크 링크 상태
- MAC 주소 교환
- 컨피그레이션 복제 및 동기화

사용되지 않는 데이터 인터페이스(물리적, 이중화 또는 EtherChannel)는 모두 페일오버 링크로 사용할 수 있습니다. 그러나 현재 이름이 구성된 인터페이스는 지정할 수 없습니다. 하위 인터페이스를 페일오버 링크로 사용하지 마십시오.

장애 조치 링크 인터페이스는 일반적인 네트워킹 인터페이스로 구성되지 않으며, 장애 조치 통신용으로만 존재합니다. 이 인터페이스는 장애 조치 링크용으로만 사용할 수 있습니다(또한 상태 링크용으로도 사용 가능).

### 스테이트풀 링크

액티브 유닛은 상태 링크를 사용하여 연결 상태 정보를 스탠바이 디바이스에 전달합니다. 즉, 스탠바이 유닛은 사용자에게 영향을 주지 않고 특정 유형의 연결을 유지할 수 있습니다. 페일오버 수행 시에 스탠바이 유닛은 이 정보를 사용하여 기존 연결을 유지할 수 있습니다.

상태 링크에 전용 데이터 인터페이스(물리적, 이중화 또는 EtherChannel)를 사용할 수 있습니다. 상태 링크로 사용된 EtherChannel의 경우, EtherChannel의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다.

인터페이스를 유지하는 가장 좋은 방법은 페일오버 및 스테이트풀 페일오버 링크 모두에 단일 링크를 사용하는 것입니다. 그러나 컨피그레이션 규모가 크고 네트워크의 트래픽이 많은 경우에는 상태 링크와 페일오버 링크에 대해 전용 인터페이스를 사용하는 것을 고려해야 합니다. 스테이트풀 페일오버 링크의 대역폭은 디바이스 데이터 인터페이스의 최대 대역폭과 일치하는 것이 좋습니다.

## FDM-관리 디바이스 설정

### FTD 디바이스의 시스템 설정 구성

단일 FTD 디바이스에서 설정을 구성하려면 다음 절차를 수행합니다.

## Procedure

- 단계 1 **Inventory**(재고 목록) 페이지를 엽니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 설정을 구성할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Management**(관리) 창에서 **Settings**(설정)를 클릭합니다.
- 단계 5 **System Settings**(시스템 설정) 탭을 클릭합니다.
- 단계 6 다음 디바이스 설정을 편집합니다.
- [관리 액세스 구성](#)
  - [기록 설정 구성](#)
  - [DHCP 서버 구성](#)
  - [DNS 서버 구성](#)
  - [호스트 이름](#)
  - [NTP 서버 구성](#)
  - [URL 필터링 구성](#)
  - [클라우드 서비스](#)
  - [웹 분석 활성화 또는 비활성화](#)

## 관리 액세스 구성

기본적으로는 모든 IP 주소에서 디바이스의 관리 주소에 연결할 수 있습니다. 시스템 액세스는 사용자 이름과 비밀번호로만 보호됩니다. 그러나 특정 IP 주소 또는 서브넷으로부터의 연결만 허용하도록 액세스 목록을 구성하여 보호 레벨을 추가로 제공할 수 있습니다.

데이터 인터페이스를 열어 FDM 관리 디바이스 또는 SSH의 CLI 연결을 허용할 수도 있습니다. 그러면 관리 주소를 사용하지 않고도 디바이스를 관리할 수 있습니다. 예를 들어 디바이스를 원격으로 구성하기 위해 외부 인터페이스에 대한 관리 액세스를 허용할 수 있습니다. 사용자 이름 및 비밀번호를 통해 원치 않는 연결로부터 디바이스를 보호할 수 있습니다. 기본적으로 데이터 인터페이스에 대한 HTTPS 관리 액세스는 내부 인터페이스에서는 활성화되지만 외부 인터페이스에서는 비활성화됩니다. 즉, 기본 "내부" 브리지 그룹이 있는 디바이스 모델의 경우 브리지 그룹 내에 있는 모든 데이터 인터페이스를 통해 브리지 그룹 IP 주소(기본값: 192.168.1.1)에 대한 FDM 관리 디바이스 연결을 설정할 수 있습니다. 디바이스에 진입하는 데 사용하는 인터페이스에서만 관리 연결을 열 수 있습니다.



주의 특정 주소에 대한 액세스를 제한하면 시스템이 잠겨 사용이 차단되기 쉽습니다. 현재 사용 중인 IP 주소에 대한 액세스 권한을 삭제하여 "모든" 주소에 대한 항목이 없으면 정책 배포 시 시스템에 액세스할 수 없게 됩니다. 액세스 목록을 구성할 때 이 점에 유의하십시오.

## 관리 인터페이스 규칙 생성

관리 인터페이스에 대한 규칙을 생성하려면 다음 절차를 수행합니다.

### 프로시저

단계 1 Management Interface(관리 인터페이스) 섹션에서 **New Access**(새 액세스)를 클릭합니다.

- **Protocol**(프로토콜). 규칙이 HTTPS(포트 443)용인지 아니면 SSH(포트 22)용인지를 선택합니다.
- **Allowed Networks**(허용된 네트워크). 시스템에 액세스할 수 있어야 하는 IPv4 또는 IPv6 네트워크나 호스트를 정의하는 네트워크 개체를 선택합니다. "임의" 주소를 지정하려면 **any-ipv4**(0.0.0.0/0) 및 **any-ipv6**(::/0)를 선택합니다.

단계 2 **Save**(저장)를 클릭합니다.

## 데이터 인터페이스용 규칙 생성

데이터 인터페이스에 대한 규칙을 생성하려면 다음 절차를 수행합니다.

### 프로시저

단계 1 Data Interface(데이터 인터페이스) 섹션에서 **New Access**(새 액세스)를 클릭합니다.

- 인터페이스. 관리 액세스를 허용할 인터페이스를 선택합니다.
- **Protocol**(프로토콜). 규칙이 HTTPS(포트 443)용인지, SSH(포트 22)용인지 아니면 둘 다에 사용할 수 있는지를 선택합니다. 원격 액세스 VPN 연결 프로파일에 사용되는 외부 인터페이스에 대해서는 HTTPS 규칙을 구성할 수 없습니다.
- **Allowed Networks**(허용된 네트워크). 시스템에 액세스할 수 있어야 하는 IPv4 또는 IPv6 네트워크나 호스트를 정의하는 네트워크 개체를 선택합니다. "임의" 주소를 지정하려면 **any-ipv4**(0.0.0.0/0) 및 **any-ipv6**(::/0)를 선택합니다.

단계 2 **Save**(저장)를 클릭합니다.

단계 3 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.


## 기록 설정 구성

이 절차에서는 **데이터(진단) 이벤트**, **파일 이벤트** 및 **악성코드 이벤트** 이벤트, **침입 이벤트** 이벤트, **콘솔 이벤트**의 로깅을 활성화하는 방법을 설명합니다. **연결 이벤트**는 이러한 설정의 결과로 로깅되지 않습니다. 연결 로깅이 액세스 규칙, 보안 인텔리전스 정책 또는 SSL 암호 해독 규칙에 구성된 경우 연결 이벤트가 로깅됩니다.

### Procedure

단계 1 **FTD 디바이스의 시스템 설정 구성.**

단계 2 System Settings(시스템 설정) 페이지의 settings(설정) 메뉴에서 **Logging**(로깅)을 클릭합니다.

단계 3 데이터 로깅. **Data Logging**(데이터 로깅) 슬라이더를 **On**(켜기)으로 밀어 진단 로깅 시스템 로그 메시지를 캡처합니다. 더하기 버튼  을 클릭하여 이벤트를 전송할 시스템 로그 서버를 나타내는 **시스템 로그 서버 개체**를 지정합니다. (이 시점에서 시스템 로그 서버 개체를 생성할 수도 있습니다.) 또한 로깅할 **메시지 심각도 레벨**의 최소 레벨을 선택합니다.

이렇게 하면 선택한 최소 심각도 레벨과 함께 모든 유형의 시스템 로그 메시지에 대한 데이터 로깅 이벤트가 시스템 로그 서버로 전송됩니다.

**Note** Cisco Defense Orchestrator는 현재 데이터 로깅을 위한 맞춤형 로깅 필터 생성을 지원하지 않습니다. 시스템 로그 서버에 전송할 메시지를 더 세부적으로 제어하려면 FDM 관리 디바이스에서 이 설정을 정의하는 것이 좋습니다. 이렇게 하려면 FDM 관리 디바이스에 로그인하고 **System Settings**(시스템 설정) > **Logging Settings**(로깅 설정)로 이동합니다.

**Tip** Cisco Security Analytics and Logging 고객은 데이터 로깅 이벤트를 **보안 이벤트 커넥터** 이외의 시스템 로그 서버로 전달하지 않는 한 데이터 로깅을 활성화하지 마십시오. 데이터 이벤트(진단 이벤트)는 트래픽 이벤트가 아닙니다. 데이터 이벤트를 다른 시스템 로그 서버로 전송하면 SEC가 이벤트를 분석하고 필터링하는 부담이 사라집니다.

단계 4 파일/악성코드 로그 설정. 슬라이더를 **On**(켜기)으로 밀어 **파일 이벤트** 및 **악성코드 이벤트**를 캡처합니다. 이벤트를 전송할 시스템 로그 서버를 나타내는 **시스템 로그 서버 개체**를 지정합니다. 아직 생성하지 않은 경우 이 시점에서 시스템 로그 서버 개체를 생성할 수도 있습니다.

파일 및 악성코드 이벤트는 동일한 심각도 레벨에서 생성됩니다. 선택한 **메시지 심각도 레벨**의 최소 레벨이 모든 파일 및 악성코드 이벤트에 할당됩니다.

액세스 제어 규칙의 파일 또는 악성코드 정책이 트리거되면 파일 및 악성코드 이벤트가 보고됩니다. 이는 연결 이벤트와는 다릅니다. 파일 및 맬웨어 이벤트에 대한 **syslog** 설정은 및 **Malware** 라이선스가 필요한 파일 또는 맬웨어 정책을 적용하는 경우에만 관련됩니다.

Cisco Security Analytics and Logging 구독자의 경우:

- SEC(Secure Event Connector)를 통해 Cisco Cloud에 이벤트를 전송하는 경우 SEC를 시스템 로그 서버로 지정합니다. 그러면 파일 정책 및 악성코드 정책 연결 이벤트와 함께 이러한 이벤트를 볼 수 있습니다.

- SEC 없이 Cisco Cloud에 직접 이벤트를 전송하는 경우 이 설정을 활성화할 필요가 없습니다. 액세스 제어 규칙이 연결 이벤트를 전송하도록 구성된 경우 파일 및 악성코드 이벤트가 전송됩니다.

단계 5 침입 기록. 이벤트를 전송할 시스템 로그 서버를 나타내는 **시스템 로그 서버 개체**를 지정하여 시스템 로그 서버에 **침입 이벤트**를 보냅니다. 아직 생성하지 않은 경우 이 시점에서 시스템 로그 서버 개체를 생성할 수도 있습니다.

액세스 제어 규칙의 침입 정책이 트리거되면 침입 이벤트가 보고됩니다. 이는 연결 이벤트와는 다릅니다. 침입 이벤트에 대한 syslog 설정은 라이선스가 필요한 침입 정책을 적용하는 경우에만 관련됩니다.

Cisco Security Analytics and Logging 구독자의 경우:

- SEC(Secure Event Connector)를 통해 Cisco Cloud에 이벤트를 전송하는 경우 SEC를 시스템 로그 서버로 지정합니다. 그러면 파일 정책 및 악성코드 정책 연결 이벤트와 함께 이러한 이벤트를 볼 수 있습니다.
- SEC 없이 Cisco Cloud에 직접 이벤트를 전송하는 경우 이 설정을 활성화할 필요가 없습니다. 액세스 제어 규칙이 연결 이벤트를 전송하도록 구성된 경우 침입 이벤트가 Cisco Cloud로 전송됩니다.

단계 6 콘솔 필터. 데이터 로깅(진단 로깅) 이벤트를 시스템 로그 서버가 아닌 콘솔로 전송하려면 슬라이더를 **On(켜기)**으로 밀니다. 또한 로깅할 이벤트 심각도의 최소 레벨을 선택합니다. 그러면 선택한 심각도 레벨과 함께 모든 유형의 시스템 로그 메시지에 대한 데이터 로깅 이벤트가 전송됩니다.

FDM 관리 디바이스의 콘솔 포트에서 CLI에 로그인하면 이러한 메시지가 표시됩니다. **show console-output** 명령을 사용하면 다른 FDM 관리 디바이스 인터페이스에 대한 SSH 세션에서도 이러한 로그를 확인할 수 있습니다(관리 인터페이스 포함). 또한, 기본 CLI에서 **system support diagnostic-cli**를 입력하여 진단 CLI에서 실시간으로 이러한 메시지를 확인할 수 있습니다.

단계 7 **Save(저장)**를 클릭합니다.

단계 8 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 메시지 심각도 레벨

다음 표는 syslog 메시지 심각도 수준을 나열합니다.

레벨 번호	심각도 레벨	설명
0	<b>emergencies(비상)</b>	시스템을 사용할 수 없습니다.
1	<b>Alert(긴급 경고)</b>	즉각적인 행동이 필요합니다.
2	<b>critical(심각)</b>	심각한 상태입니다.
3	<b>error(오류)</b>	오류 상태입니다.



레벨 번호	심각도 레벨	설명
4	<b>warning</b> (경고)	경고 상태입니다.
5	<b>notification</b> (알림)	일반적이지만 중요한 상태입니다.
6	<b>informational</b> (정보)	정보 메시지만 해당됩니다.
7	<b>debugging</b> (디버깅)	디버깅 메시지만 해당됩니다.
<b>Note</b>	FDM 관리 디바이스는 심각도 수준이 0(비상)인 syslog 메시지를 생성하지 않습니다.	

## DHCP 서버 구성

DHCP(Dynamic Host Configuration Protocol) 서버는 IP 주소와 같은 네트워크 구성 매개 변수를 DHCP 클라이언트에 제공합니다. 연결된 네트워크의 DHCP 클라이언트에 컨피그레이션 파라미터를 제공하기 위해 인터페이스에서 DHCP 서버를 구성할 수 있습니다.

IPv4 DHCP 클라이언트는 서버와 연결하는 데 멀티캐스트 주소가 아닌 브로드캐스트를 사용합니다. DHCP 클라이언트는 UDP 포트 68에서 메시지를 수신 대기합니다. DHCP 서버는 UDP 포트 67에서 메시지를 수신합니다. DHCP 서버는 BOOTP 요청을 지원하지 않습니다.

DHCP 클라이언트는 서버가 활성화된 인터페이스와 같은 네트워크에 있어야 합니다. 서버와 클라이언트 사이에 스위치는 있을 수 있지만 개입하는 라우터가 있어서는 안 됩니다.



**Caution** 이미 DHCP 서버가 작동 중인 네트워크에서는 DHCP 서버를 구성하지 마십시오. 이렇게 하면 두 서버가 서로 충돌하여 예측할 수 없는 결과가 발생합니다.

### Procedure

**단계 1** 섹션에는 두 개의 영역이 있습니다. 먼저 **Configuration**(구성) 섹션에는 글로벌 매개변수가 표시됩니다. DHCP Servers(DHCP 서버) 영역에는 서버를 구성한 인터페이스, 서버 활성화 여부 및 서버의 주소 풀이 표시됩니다.

**단계 2 Configuration**(구성) 섹션에서 자동 설정과 글로벌 설정을 구성합니다.

DHCP 자동 설정은 DHCP 서버가 지정된 인터페이스에서 실행 중인 어떤 DHCP 클라이언트로부터 얻은 DNS 서버, 도메인 이름, WINS 서버 정보를 DHCP 클라이언트에 제공할 수 있게 합니다. 일반적으로는 외부 인터페이스의 DHCP를 사용하여 주소를 가져오는 경우 자동 설정을 사용하지만, DHCP를 통해 주소를 가져오는 모든 인터페이스를 선택할 수 있습니다. 자동 설정을 사용할 수 없는 경우에는 필요한 옵션을 수동으로 정의할 수 있습니다.

- a. 자동 구성을 사용하려면 **Enable Auto Configuration**(자동 구성 활성화) 슬라이더를 켜기로 클릭하고 **From Interface**(인터페이스에서) 폴다운에서 DHCP를 통해 주소를 가져오는 인터페이스를 선택합니다.

- b. 자동 구성을 활성화하지 않거나 자동으로 구성된 설정을 재정의하려는 경우 다음의 글로벌 옵션을 구성합니다. 이러한 설정은 DHCP 서버를 호스팅하는 모든 인터페이스의 DHCP 클라이언트에 전송됩니다.
  1. **Primary WINS IP Address**(기본 WINS IP 주소), **Secondary WINS IP Address**(보조 WINS IP 주소). 클라이언트가 NetBIOS 이름 확인에 사용해야 하는 WINS(Windows 인터넷 이름 서비스) 서버의 주소입니다.
  2. **Primary DNS IP Address**(기본 DNS IP 주소), **Secondary DNS IP Address**(보조 DNS IP 주소). 클라이언트가 도메인 이름 확인에 사용해야 하는 DNS(Domain Name System) 서버의 주소입니다. DNS IP 주소 필드를 Cisco Umbrella DNS 서버로 채우려면 **Apply Umbrella Settings(Umbrella 설정 적용)**를 클릭합니다. 버튼을 클릭하면 필드에 적절한 IP 주소가 로드됩니다.
- c. **Save(저장)**를 클릭합니다.

단계 3 DHCP Servers(DHCP 서버) 섹션에서 기존 서버를 편집하거나 **New DHCP Server**(새 DHCP 서버)를 클릭하여 새 서버를 추가 및 구성합니다.

- a. 서버 속성을 구성합니다.
  1. **DHCP** 서버 활성화. 서버를 활성화할지를 선택합니다. 서버를 구성하되 사용할 준비가 될 때까지 비활성화해 둘 수 있습니다.
  2. 인터페이스. 클라이언트에 DHCP 주소를 제공할 인터페이스를 선택합니다. 이 인터페이스에는 고정 IP 주소가 있어야 합니다. 인터페이스에서 DHCP 서버를 실행하려는 경우 DHCP를 사용하여 인터페이스 주소를 가져올 수는 없습니다. 브리지 그룹의 경우 멤버 인터페이스가 아닌 BVI(브리지 가상 인터페이스)에서 DHCP 서버를 구성합니다. 그러면 서버가 모든 멤버 인터페이스에서 작동합니다. 진단 인터페이스에서는 DHCP 서버를 구성할 수 없습니다. 대신 **Device**(디바이스) > **System Settings**(시스템 설정) > **Management Interface**(관리 인터페이스) 페이지를 통해 관리 인터페이스에서 DHCP 서버를 구성합니다.
  3. 주소 풀. DHCP 서버의 단일 IP 주소 또는 IP 주소 범위를 추가합니다. 서버가 주소를 요청하는 클라이언트에 제공할 수 있는 IP 주소의 범위(최저 범위에서 최고 범위 순서)입니다. 이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소, 브로드캐스트 주소 또는 서브넷 네트워크 주소는 포함할 수 없습니다. 풀의 시작 주소와 끝 주소를 하이픈으로 구분하여 지정합니다. 예를 들면 10.100.10.12-10.100.10.250과 같이 지정합니다.
- b. **OK(확인)**를 클릭합니다.

단계 4 **Save(저장)**를 클릭합니다.

단계 5 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## DNS 서버 구성

DNS(Domain Name System) 서버는 호스트 이름을 IP 주소로 확인하는 데 사용됩니다. DNS 서버는 관리 인터페이스에서 사용됩니다.

### Procedure

- 단계 1 1차, 2차, 3차 DNS IP 주소에 최대 3개 DNS 서버의 IP 주소를 선호하는 순서대로 입력합니다. 연결할 수 없는 경우를 제외하면 1차 DNS 서버가 사용됩니다. 이 서버에 연결할 수 없으면 2차 서버에 연결을 시도하며, 마지막으로 3차 서버에 연결을 시도합니다. DNS IP 주소 필드를 Cisco Umbrella DNS 서버로 채우려면 **Apply Umbrella Settings(Umbrella 설정 적용)**를 클릭합니다. 버튼을 클릭하면 필드에 적절한 IP 주소가 로드됩니다.
- 단계 2 **Domain Search Name(도메인 검색 이름)**에서 example.com과 같은 네트워크의 도메인 이름을 입력합니다. 이 도메인은 정규화되지 않은 호스트 이름(예: serverA가 serverA.example.com이 됨)에 추가됩니다.
- 단계 3 **Save(저장)**를 클릭합니다.
- 단계 4 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 관리 인터페이스

관리 인터페이스는 물리적 관리 포트에 연결된 가상 인터페이스입니다. 물리적 포트는 이름이 진단 인터페이스이며, 다른 물리적 포트와 함께 인터페이스 페이지에서 구성할 수 있습니다. 가상 FDM 관리 디바이스에서는 두 인터페이스가 모두 가상 인터페이스라도 이처럼 두 인터페이스를 모두 사용할 수 있습니다.

관리 인터페이스는 다음과 같은 두 가지 용도로 사용됩니다.

- IP 주소에 대한 웹 및 SSH 연결을 열고 인터페이스를 통해 디바이스를 구성할 수 있습니다.
- 시스템은 이 IP 주소를 통해 스마트 라이선싱 및 데이터베이스 업데이트를 가져옵니다.

CLI 설정 마법사를 사용하는 경우 초기 시스템 구성 중에 디바이스의 관리 주소 및 게이트웨이를 구성합니다. FDM 관리 설정 마법사를 사용하는 경우에는 관리 주소와 게이트웨이가 기본값으로 유지됩니다.

필요한 경우 FDM 관리 디바이스를 통해 이러한 주소를 변경할 수 있습니다. **configure network ipv4 manual** 및 **configure network ipv6 manual** 명령을 사용하여 CLI에서 관리 주소 및 게이트웨이를 변경할 수도 있습니다.

고정 주소를 정의할 수도 있고, 관리 네트워크의 다른 디바이스가 DHCP 서버로 작동하는 경우에는 DHCP를 통해 주소를 가져올 수 있습니다. 기본적으로, 관리 주소는 고정 주소이며 DHCP 서버는 포트(DHCP 서버가 없는 가상 FDM-관리 제외)에서 실행됩니다. 따라서 관리 포트에 디바이스를 직접 연결하여 워크스테이션의 DHCP 주소를 가져올 수 있습니다. 이렇게 하면 디바이스를 쉽게 연결하고 구성할 수 있습니다.



**Caution** 현재 연결된 주소를 변경할 경우 변경 사항을 저장하면 즉시 적용되므로 FDM 관리 디바이스 또는 CLI에 액세스할 수 없게 됩니다. 디바이스와 다시 연결해야 합니다. 관리 네트워크에서 새 주소가 유효하며 사용 가능한지 확인합니다.

### Procedure

- 단계 1 IPv4, IPv6 중 하나 또는 둘 다의 관리 IP 주소, 네트워크 마스크 또는 IPv6 접두사 및 게이트웨이(필요한 경우)를 구성합니다. 속성 집합을 하나 이상 구성해야 합니다. 특정 집합의 주소 지정 방법을 비활성화하려면 해당 집합을 비워 둡니다.
- 단계 2 **Type(유형)** > **DHCP**를 선택하여 DHCP 또는 IPv6 자동 구성을 통해 주소와 게이트웨이를 가져옵니다. 그러나 데이터 인터페이스를 게이트웨이로 사용하는 경우에는 DHCP를 사용할 수 없습니다. 이 경우에는 고정 주소를 사용해야 합니다.
- 단계 3 **Save(저장)**를 클릭합니다.
- 단계 4 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 호스트 이름

디바이스 호스트 이름을 변경할 수 있습니다.

### Procedure

- 단계 1 **Firewall Hostname(방화벽 호스트 이름)** 필드에 디바이스의 새 호스트 이름을 입력합니다.
- 단계 2 **Save(저장)**를 클릭합니다.
- 단계 3 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## NTP 서버 구성

시스템에서 시간을 정의하려면 NTP(Network Time Protocol) 서버를 구성합니다.

### Procedure

- 단계 1 자체(수동) 또는 Cisco의 시간 서버를 사용할지 선택합니다.
  - **New NTP Server(새 NTP 서버)**. 사용하려는 NTP 서버의 IP 주소 또는 FQDN(Fully-Qualified Domain Name)을 입력합니다. 예를 들어 ntp1.example.com 또는 10.100.10.10을 입력합니다.

- **Use Default**(기본값 사용).

단계 2 **Save**(저장)를 클릭합니다.

단계 3 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## URL 필터링 구성

시스템은 Cisco CSI(Collective Security Intelligence)에서 URL 카테고리 및 평판 데이터베이스를 가져옵니다. 이러한 환경 설정은 데이터베이스 업데이트 및 시스템이 카테고리나 평판을 알 수 없는 URL을 처리하는 방법을 제어합니다. 이러한 환경 설정을 지정하려면 URL 필터링 라이선스를 활성화해야 합니다.



**Caution** URL 스마트 라이선스가 없지만 구축하는 데 스마트 라이선스가 필요한 경우 URL 필터링 기본 설정을 구성할 수 있습니다. URL 스마트 라이선스를 추가할 때까지 구축이 차단됩니다.

### Procedure

단계 1 해당 옵션을 활성화합니다.

- **Enable Automatic Updates**(자동 업데이트 활성화) 슬라이드 켜기를 클릭하여 업데이트된 URL 데이터를 시스템에서 자동으로 확인하고 다운로드할 수 있도록 합니다. 이 데이터에는 범주 및 평판 정보가 포함됩니다. 구축 후 FDM 관리 디바이스는 30분마다 업데이트를 확인합니다.
- **Query Cisco CSI for Unknown URLs**(Cisco CSI에서 알 수 없는 URL 쿼리) 슬라이더 켜기를 클릭하여 로컬 URL 필터링 데이터베이스에 범주 및 평판 데이터가 없는 URL에 대해 Cisco CSI에 업데이트된 정보를 확인할 수 있도록 합니다.
- **URL TTL(Time to Live)**은 **Query Cisco CSI for Unknown URLs**(알 수 없는 URL에 대해 Cisco CSI 쿼리) 옵션을 활성화한 경우에만 적용됩니다. 지정된 URL에 대한 범주 및 평판 조회 값을 캐시할 기간을 결정합니다. TTL(Time to Live)이 만료되면 다음 번에 URL 액세스를 시도할 때 카테고리/평판을 새로 조회합니다. 이 시간이 짧을수록 URL 필터링 정확도가 높아지고, 시간이 길수록 알 수 없는 URL에 대한 필터링 성능이 향상됩니다. 기본 선택은 **Never**(없음)입니다.

단계 2 **Save**(저장)를 클릭합니다.

단계 3 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 클라우드 서비스

Cloud Services(클라우드 서비스) 페이지를 사용하여 클라우드 기반 서비스를 관리합니다.



**Note** Cisco Success Network에 연결하고 Cisco 클라우드로 전송되는 이벤트를 구성하는 것은 소프트웨어 버전 6.6 이상을 실행하는 FTD 디바이스에서 구성할 수 있는 기능입니다.

### Cisco Success Network에 연결

Cisco Success Network를 활성화하면 Cisco가 기술 지원을 제공하는 데 필수적인 사용자 정보 및 통계를 Cisco에 제공하게 됩니다. 또한, 이 정보를 통해 Cisco는 제품을 개선할 수 있으며 사용 가능하지만 사용되지 않은 기능을 알려 네트워크의 제품 가치를 최대화하도록 할 수 있습니다.

연결을 활성화하는 경우, 디바이스에서는 기술 지원 서비스, 클라우드 관리 및 모니터링 서비스와 같은 Cisco의 추가 제공 서비스에 참여할 수 있도록 Cisco Cloud에 대한 보안 연결을 설정합니다. 디바이스는 이 안전한 연결을 설정하고 항상 유지합니다.

시작하기 전에

Cisco Success Network를 활성화하려면 FDM 관리 디바이스를 사용하여 디바이스를 클라우드에 등록해야 합니다. 디바이스를 등록하려면 Cisco Smart Software Manager(Smart Licensing 페이지)에 디바이스를 등록하거나 등록 키를 입력하여 Cisco Defense Orchestrator에 등록합니다.



**Attention** 고가용성 그룹의 액티브 유닛에서 Cisco Success Network를 활성화하면 스탠바이 유닛에서도 연결이 활성화됩니다.

#### Procedure

단계 1 **Cloud Services**(클라우드 서비스) 탭을 클릭합니다.

단계 2 설정을 적절하게 변경하려면 Cisco Success Network 기능의 **Enabled**(활성화됨) 슬라이더를 클릭합니다.

단계 3 **Save**(저장)를 클릭합니다.

단계 4 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

### Cisco Cloud로 이벤트 전송

Cisco Cloud 서버에 이벤트를 전송할 수 있습니다. 여기서는 다양한 Cisco Cloud 서비스에서 이벤트에 액세스할 수 있습니다. 그러면 이러한 클라우드 애플리케이션(예: Cisco Threat Response)을 사용하여 이벤트를 분석하고 디바이스에 발생했을 가능성이 있는 위협을 평가할 수 있습니다.

시작하기 전에

디바이스를 Cisco Smart Software Manager에 등록해야 이 서비스를 활성화할 수 있습니다.

미국 지역의 경우 <https://visibility.amp.cisco.com/>에서, EU 지역의 경우에는 <https://visibility.amp.cisco.com/>에서 Cisco Threat Response에 연결할 수 있습니다. <http://cs.co/CTRvideos>에서 YouTube를 통해 애플리케이션의 용도와 이점에 대한 비디오를 볼 수 있습니다. FTD와 함께 Cisco Threat Response를 사용하는 방법에 대한 자세한 내용은 *Firepower* 및 *CTR* 통합 가이드(<https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html>에서 확인 가능)를 참조하십시오.

## Procedure

단계 1 **Cloud Services**(클라우드 서비스) 탭을 클릭합니다.

단계 2 설정을 적절하게 변경하려면 **Send Events to the Cisco Cloud**(Cisco Cloud에 이벤트 전송) 옵션의 **Enabled**(활성화됨) 슬라이더를 클릭합니다.

단계 3 서비스를 활성화하는 경우 클라우드에 전송할 이벤트를 선택하라는 메시지가 표시됩니다.

- **File/Malware**(파일/악성코드) - 액세스 제어 규칙에 적용한 모든 파일 정책에 해당합니다.
- **Intrusion Events**(침입 이벤트) - 액세스 제어 규칙에 적용한 모든 침입 정책에 해당합니다.
- **Connection Events**(연결 이벤트) - 기록을 활성화한 액세스 제어 규칙에 해당합니다. 이 옵션을 선택하는 경우 모든 연결 이벤트를 전송하거나 높은 우선순위 연결 이벤트만 전송하도록 선택할 수도 있습니다. 높은 우선순위 연결 이벤트는 침입, 파일 또는 악성코드 이벤트를 트리거하는 연결이나 보안 인텔리전스 차단 정책과 일치하는 연결과 관련된 이벤트입니다.

단계 4 **Save**(저장)를 클릭합니다.

단계 5 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 웹 분석 활성화 또는 비활성화

웹 분석을 활성화하면 페이지 조회 수를 기반으로 하는 익명 제품 사용 정보가 Cisco에 제공됩니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다. CDO를 사용하여 모든 버전의 FDM 관리 디바이스에서 이 기능을 구성할 수 있습니다.

웹 분석은 기본적으로 활성화됩니다.

## Procedure

단계 1 **Web Analytics**(웹 분석) 탭을 클릭합니다.

단계 2 설정을 적절하게 변경하려면 **Web Analytics**(웹 분석) 기능의 **Enable**(활성화) 슬라이더를 클릭합니다.

단계 3 **Save**(저장)를 클릭합니다.

단계 4 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## CDO 명령줄 인터페이스

CDO는 사용자에게, FDM 관리 위협 방어 디바이스를 관리하기 위한 CLI(명령줄 인터페이스)를 제공합니다. 사용자는 단일 디바이스 또는 여러 디바이스에 동시에 명령을 전송할 수 있습니다.

관련 정보:

- FTD CLI 설명서는 [Cisco Firepower Threat Defense 명령 참조](#)를 참조하십시오. 참고로 FDM 관리 디바이스는 CLI 기능이 제한되어 있습니다. 이러한 디바이스에는 `show`, `ping`, `traceroute`, `packet-tracer`, `failover` 및 `shutdown` 명령만 있습니다.

## 명령줄 인터페이스 사용

### Procedure

단계 1 **Inventory**(재고 목록) 페이지를 엽니다.

단계 2 재고 목록 테이블 위에 있는 디바이스 버튼을 클릭합니다.

단계 3 명령줄 인터페이스(CLI)를 사용하여 관리하려는 디바이스를 찾으려면 디바이스 탭과 필터 버튼을 사용합니다.

단계 4 디바이스를 선택합니다.

단계 5 **Device Actions**(장치 작업) 창에서 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 **Command Line Interface**(명령줄 인터페이스) 탭을 클릭합니다.

단계 7 명령 창에 명령을 입력하고 **Send**(보내기)를 클릭합니다. 명령에 대한 디바이스의 응답은 "응답 창" 아래에 표시됩니다.

**Note** 실행할 수 있는 명령에 제한 사항이 있는 경우 해당 제한 사항은 명령 창 위에 나열됩니다.

### Related Topics

[명령줄 인터페이스에 명령 입력](#), 105 페이지

## 명령줄 인터페이스에 명령 입력

한 줄에 하나의 명령을 입력하거나 여러 줄에 여러 명령을 순차적으로 입력할 수 있으며 CDO는 명령을 순서대로 실행합니다. 다음 ASA 예에서는 세 개의 네트워크 개체와 해당 네트워크 개체를 포함하는 네트워크 개체 그룹을 생성하는 명령 배치를 전송합니다.



```

> object network email_server_north
host 192.168.10.2
object network email_server_south
host 192.168.20.2
object network email_server_headquarters
host 192.168.30.2
object-group network email_servers_all
network-object object email_server_north
network-object object email_server_south
network-object object email_server_headquarters

```


Press Cmd+Enter to send command

**FDM 관리 디바이스 명령 입력:** CLI 콘솔은 기본 위협 방어 CLI를 사용합니다. CLI 콘솔을 사용하여 진단 CLI, 전문가 모드 또는 FXOS CLI(FXOS를 사용하는 모델)를 시작할 수는 없습니다. 기타 CLI 모드를 시작해야 하는 경우에는 SSH를 사용합니다.

## 명령 기록 작업

CLI 명령을 보낸 후 CDO는 **Command Line Interface**(명령줄 인터페이스) 페이지의 기록 창에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다.

### Procedure

- 단계 1 **Inventory**(인벤토리) 페이지에서 구성할 디바이스를 선택합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 5 아직 확장되지 않은 경우 시계 아이콘  을 클릭하여 기록 창을 확장합니다.
- 단계 6 편집하거나 다시 보내려는 히스토리 창에서 명령을 **Select**(선택)합니다.
- 단계 7 명령 창에서 명령을 그대로 재사용하거나 편집하고 **Send**(보내기)를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

**Note** CDO는 다음 두 가지 상황에서 응답창에 Done! (완료!) 메시지를 표시합니다.

- 명령이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료!를 반환합니다.

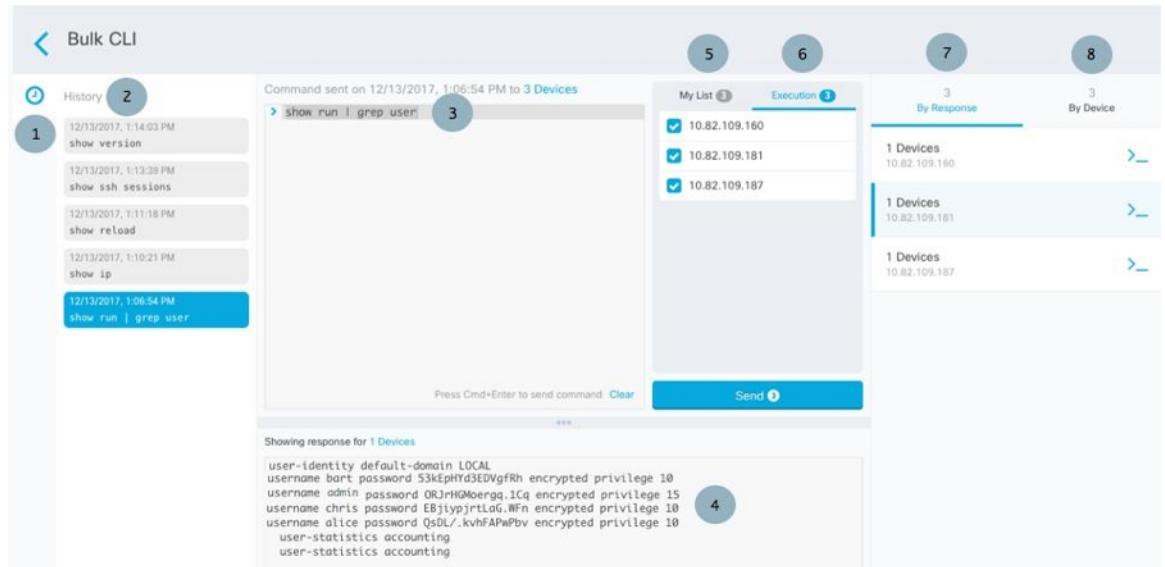
# 대량 명령줄 인터페이스

CDO는 CLI(command line interface)를 사용하여 Secure Firewall ASA, FDM 관리, 위협 방어, SSH 및 Cisco IOS Secure Firewall Cloud Native 디바이스를 관리할 수 있는 기능을 사용자에게 제공합니다. 사용자는 단일 디바이스 또는 같은 종류의 여러 디바이스에 동시에 명령을 보낼 수 있습니다. 이 섹션에서는 한 번에 여러 디바이스에 CLI 명령을 보내는 방법을 설명합니다.

관련 정보:

- FDM 관리 디바이스 설명서의 경우 CDO는 기본 FTD CLI만 지원합니다. 이러한 디바이스에는 show, ping, traceroute, packet-tracer, failover 및 shutdown 명령만 있습니다.
- 위협 방어 CLI 설명서는 [Cisco Firepower Threat Defense 명령 참조](#)를 참조하십시오.

## 대량 CLI 인터페이스



**Note** CDO는 다음 두 가지 상황에서 **Done!(완료!)** 메시지를 표시합니다.

- 명령이 오류 없이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료!를 반환합니다.

숫자	설명
1	시계를 클릭하여 명령 기록 창을 확장하거나 축소합니다.

숫자	설명
2	명령 기록. 명령을 보낸 후 CDO는 이 히스토리 창에 명령을 기록하므로 돌아가서 선택하고 다시 실행할 수 있습니다.
3	명령 창. 이 창의 프롬프트에 명령을 입력합니다.
4	<p>응답 창. CDO는 명령에 대한 디바이스의 응답과 CDO 메시지를 표시합니다. 두 개 이상의 디바이스에 대한 응답이 동일한 경우 응답 창에 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.</p> <p><b>Note</b> CDO는 다음 두 가지 상황에서 <b>Done!(완료!)</b> 메시지를 표시합니다.</p> <ul style="list-style-type: none"> <li>명령이 오류 없이 성공적으로 실행된 후.</li> <li>명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 <b>show</b> 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 <b>완료!</b>를 반환합니다.</li> </ul>
5	<b>My List</b> (내 목록) 탭에는 <b>Inventory</b> (인벤토리) 테이블에서 선택한 디바이스가 표시되며 명령을 보낼 디바이스를 포함하거나 제외할 수 있습니다.
6	위 그림에서 강조 표시된 <b>Execution</b> (실행) 탭은 히스토리 창에서 선택한 명령의 디바이스를 표시합니다. 이 예에서 <b>show run   grep user</b> 명령이 기록 창에서 선택되고 실행 탭에 10.82.109.160, 10.82.109.181 및 10.82.10.9.187로 전송된 것으로 표시됩니다.
7	<b>By Response</b> (응답별) 탭을 클릭하면 명령에 의해 생성된 응답 목록이 표시됩니다. 동일한 응답은 한 행에 함께 그룹화됩니다. <b>By Response</b> (응답별) 탭에서 행을 선택하면 CDO는 응답 창에 해당 명령에 대한 응답을 표시합니다.
8	<b>By Device</b> (디바이스별) 탭을 클릭하면 각 디바이스의 개별 응답이 표시됩니다. 목록에서 디바이스 중 하나를 클릭하면 특정 디바이스에서 명령에 대한 응답을 볼 수 있습니다.

## 대량 명령 전송

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 디바이스를 찾으려면 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 탭을 선택하고 필터 버튼을 사용하여 명령줄 인터페이스를 사용하여 구성할 디바이스를 찾습니다.

단계 4 디바이스를 선택합니다.

단계 5 **Device Actions**(장치 작업) 창에서 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 내 목록 필드에서 명령을 보낼 디바이스를 선택하거나 선택 취소할 수 있습니다.

단계 7 명령 창에 명령을 입력하고 **Send**(보내기)를 클릭합니다. 명령 출력은 응답 창에 표시되고 명령은 변경 로그에 기록되며 CDO 명령은 대량 CLI 창의 기록 창에 명령을 기록합니다.

## 대량 명령 기록 작업

대량 CLI 명령을 보낸 후, CDO는 **대량 CLI 인터페이스** 기록에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다. 기록 창의 명령은 명령이 실행된 원래 디바이스와 연결됩니다.

### Procedure

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 디바이스를 찾으려면 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 필터 아이콘을 클릭하여 구성하려는 디바이스를 찾습니다.

단계 4 디바이스를 선택합니다.

단계 5 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 편집하거나 다시 보내려는 히스토리 창에서 명령을 **Select**(선택)합니다. 선택하는 명령은 특정 디바이스와 연결되며 반드시 첫 번째 단계에서 선택한 디바이스와 연결되지 않습니다.

단계 7 내 목록 탭을 보고 전송하려는 명령이 예상하는 디바이스로 전송되는지 확인합니다.

단계 8 명령 창에서 명령을 편집하고 **Send**(보내기)를 클릭합니다. CDO는 응답 창에 명령 결과를 표시합니다.

## 대량 명령 필터 작업

대량 CLI 명령을 실행한 후 **By Resonse**(응답별) 필터 및 **By Device**(디바이스별) 필터를 사용하여 계속해서 디바이스를 구성할 수 있습니다.

### 응답 기준 필터

대량 명령을 실행한 후 CDO는 명령을 보낸 디바이스에서 반환된 응답 목록으로 **By Response**(응답별) 탭을 채웁니다. 응답이 동일한 디바이스는 단일 행에 통합됩니다. **By Response**(응답별) 탭에서 행을 클릭하면 응답 창에 디바이스의 응답이 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. **X devices**(X 디바이스)를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.



명령 응답과 관련된 디바이스 목록에 명령을 보내려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 **By Response**(응답별) 탭에서 행의 명령 기호를 클릭합니다.
- 단계 2 명령 창에서 명령을 검토하고 **Send**(보내기)를 클릭하여 명령을 다시 보내거나 **Clear**(지우기)를 클릭하여 명령 창을 지우고 디바이스로 보낼 새 명령을 입력한 다음 **Send**(보내기)를 클릭합니다.
- 단계 3 명령에서 받은 응답을 검토하십시오.
- 단계 4 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확인하는 경우 명령 창에 `write memory`를 입력하고 **Send**(보내기)를 클릭합니다. 이렇게 하면 실행 중인 구성이 시작 구성에 저장됩니다.

## 디바이스 기준 필터

대량 명령을 실행한 후 CDO는 실행 탭과 디바이스별 탭을 명령을 보낸 디바이스 목록으로 채웁니다. 디바이스별 탭에서 행을 클릭하면 각 디바이스에 대한 응답이 표시됩니다.

동일한 디바이스 목록에서 명령을 실행하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 **By Device**(디바이스 별) 탭을 클릭합니다.
- 단계 2 **>\_Execute a command on these devices**(이 디바이스에서 명령 실행)를 클릭합니다.
- 단계 3 **Clear**(지우기)를 클릭하여 명령 창을 지우고 새 명령을 입력합니다.
- 단계 4 내 목록 창에서 목록의 개별 디바이스를 선택하거나 선택 취소하여 명령을 보낼 디바이스 목록을 지정합니다.
- 단계 5 **Send**(보내기)를 클릭합니다. 명령에 대한 응답이 응답 창에 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.

단계 6 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send**(보내기)를 클릭합니다.

## 디바이스 관리를 위한 CLI 매크로

CLI 매크로는 즉시 사용할 수 있는 완전한 형식의 CLI 명령이거나 실행 전에 수정할 수 있는 CLI 명령의 템플릿입니다. 모든 매크로는 하나 이상의 FTD 디바이스에서 동시에 실행할 수 있습니다.

여러 디바이스에서 동일한 명령을 동시에 실행하려면 템플릿과 유사한 CLI 매크로를 사용합니다. CLI 매크로는 디바이스 구성 및 관리의 일관성을 유지합니다. 완전한 형식의 CLI 매크로를 사용하여 디바이스에 대한 정보를 가져옵니다. FTD 디바이스에서 즉시 사용할 수 있는 다양한 CLI 매크로가 있습니다.

자주 수행하는 작업을 모니터링하기 위해 CLI 매크로를 생성할 수 있습니다. 자세한 내용은 [새 명령에서 CLI 매크로 생성](#)을 참조하십시오.

CLI 매크로는 시스템 정의 또는 사용자 정의입니다. 시스템 정의 매크로는 CDO에서 제공하며 편집하거나 삭제할 수 없습니다. 사용자 정의 매크로는 사용자가 생성하며 편집하거나 삭제할 수 있습니다.



**Note** 디바이스가 CDO에 온보딩된 후에만 디바이스에 대한 매크로를 생성할 수 있습니다.

ASA를 예로 들어 ASA 중 하나에서 특정 사용자를 찾으려면 다음 명령을 실행할 수 있습니다.

```
show running-config | grep username
```

명령을 실행할 때 사용자 이름을 검색할 사용자의 사용자 이름으로 대체합니다. 이 명령으로 매크로를 만들려면 동일한 명령을 사용하고 사용자 이름을 중괄호로 묶습니다.

```
> show running-config | grep {{username}}
```

매개변수의 이름은 원하는 대로 지정할 수 있습니다. 이 매개변수 이름을 사용하여 동일한 매크로를 생성할 수도 있습니다.

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

매개변수 이름은 설명적일 수 있으며 영숫자 문자와 밑줄을 사용해야 합니다. 이 경우 명령 구문은

```
show running-config | grep
```

명령의 일부이며 명령을 전송하는 디바이스에 대해 적절한 CLI 구문을 사용해야 합니다.

## 새 명령에서 CLI 매크로 생성

### Procedure

단계 1 CLI 매크로를 생성하기 전에 CDO의 명령줄 인터페이스에서 명령을 테스트하여 명령 구문이 올바른지, 그리고 신뢰할 수 있는 결과를 반환하는지 확인합니다.

#### Note

- FTD 디바이스의 경우 CDO는 FDM의 CLI 콘솔에서 실행할 수 있는 명령(show, ping, traceroute, packet-tracer, failover, reboot 및 shutdown)만 지원합니다. 이러한 명령의 구문에 대한 전체 설명은 [Cisco Firepower Threat Defense 명령 참조](#)를 참조하십시오.

단계 2 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 3 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 4 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.

단계 5 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다.

단계 7 더하기 버튼  을 클릭합니다.

단계 8 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.

단계 9 **Command**(명령) 필드에 전체 명령을 입력합니다.

단계 10 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 11 **Create**(생성)를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 [CLI 매크로 실행](#)을 참조하십시오.




## CLI 기록 또는 기존 CLI 매크로에서 CLI 매크로 생성

이 절차에서는 이미 실행한 명령, 다른 사용자 정의 매크로 또는 시스템 정의 매크로에서 사용자 정의 매크로를 생성합니다.

### 프로시저


단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

참고 CLI 기록에서 사용자 정의 매크로를 생성하려면 명령을 실행한 디바이스를 선택합니다. CLI 매크로는 동일한 계정의 디바이스 간에 공유되지만 CLI 기록은 공유되지 않습니다.

- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.
- 단계 4 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 5 CLI 매크로를 만들려는 명령을 찾아 선택합니다. 다음 방법 중 하나를 사용합니다.
- 해당 디바이스에서 실행한 명령을 보려면 시계 를 클릭합니다. 매크로로 전환할 항목을 선택하면 명령 창에 명령이 나타납니다.
  - CLI 매크로 즐겨찾기 스타 를 클릭하여 이미 존재하는 매크로를 확인합니다. 변경할 사용자 정의 또는 시스템 정의 CLI 매크로를 선택합니다. 명령 창에 명령이 나타납니다.
- 단계 6 명령 창의 명령을 사용하여 CLI 매크로 금색 별 를 클릭합니다. 이 명령은 이제 새 CLI 매크로의 기본이 됩니다.
- 단계 7 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.
- 단계 8 명령 필드에서 명령을 검토하고 원하는 대로 변경합니다.
- 단계 9 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.
- 단계 10 **Create**(생성)를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.
- 명령을 실행하려면 [CLI 매크로 실행](#)을 참조하십시오.

## CLI 매크로 실행

### Procedure

- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 유형 탭을 클릭하고 하나 이상의 디바이스를 선택합니다.
- 단계 4 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 5 명령 패널에서 별표 를 클릭합니다.
- 단계 6 명령 패널에서 CLI 매크로를 선택합니다.
- 단계 7 다음 두 가지 방법 중 하나로 매크로를 실행합니다.
- 매크로에 정의할 매개변수가 없는 경우 **Send**(전송)를 클릭합니다. 명령에 대한 응답이 응답 창에 나타납니다. 다 됐습니다.
  - 아래의 Configure DNS 매크로와 같은 매개변수가 매크로에 포함된 경우 **>\_View Parameters**(매개변수 보기)를 클릭합니다.



```

★ Using Macro: Configure DNS
> dns domain-lookup {{IF_NAME}}
  dns server-group DefaultDNS
  name-server {{IP_ADDR}}

```

단계 8 Parameters(매개변수) 창의 Parameters(매개변수) 필드에 매개변수 값을 입력합니다.

단계 9 **Send**(보내기)를 클릭합니다. CDO가 성공적으로 명령을 전송하고 디바이스의 구성을 업데이트하면 완료됩니다!

- FTD의 경우 디바이스의 활성 구성이 업데이트됩니다.

단계 10 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.

⚠ Some commands may have made changes to the running config [Write to Disk](#) [Dismiss](#)

- **Write to Disk**(디스크에 쓰기)를 클릭하면 이 명령의 변경 사항과 실행 중인 구성의 다른 모든 변경 사항이 디바이스의 시작 구성에 저장됩니다.
- **Dismiss**(해제)를 클릭하면 메시지가 사라집니다.

## CLI 매크로 편집

사용자 정의 CLI 매크로는 편집할 수 있지만 시스템 정의 매크로는 편집할 수 없습니다. CLI 매크로를 수정하면 모든 FTD 디바이스에 대해 변경됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

### Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택합니다.

단계 5 **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 편집할 사용자 정의 매크로를 선택합니다.

단계 7 매크로 레이블에서 편집 아이콘을 클릭합니다.

단계 8 **Edit Macro**(매크로 편집) 대화 상자에서 CLI 매크로를 편집합니다.

단계 9 **Save**(저장)를 클릭합니다.

CLI 매크로를 실행하는 방법에 대한 지침은 [CLI 매크로 실행](#)를 참조하십시오.

## CLI 매크로 삭제

사용자 정의 CLI 매크로는 삭제할 수 있지만 시스템 정의 매크로는 삭제할 수 없습니다. CLI 매크로를 삭제하면 모든 디바이스에서 삭제됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

### Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.


단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택합니다.

단계 5 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.

단계 6 삭제할 사용자 정의 CLI 매크로를 선택합니다.

단계 7 CLI 매크로 레이블에서 휴지통 아이콘 를 클릭합니다.

단계 8 CLI 매크로를 제거할지 확인합니다.

## 명령줄 인터페이스 설명서

CDO는 FDM 관리 디바이스의 명령줄 인터페이스를 부분적으로 지원합니다. 사용자가 단일 디바이스 및 여러 디바이스에 명령 및 응답 형식으로 동시에 명령을 전송할 수 있도록 CDO 내에서 터미널과 유사한 인터페이스를 제공합니다. CDO에서 지원되지 않는 명령의 경우 PuTTY 또는 SSH 클라이언트와 같은 디바이스 GUI 터미널을 사용하여 디바이스에 액세스하고, 추가 명령은 [CLI 설명서](#)를 참조하십시오.

## CLI 명령 결과 내보내기


독립형 디바이스 또는 여러 디바이스에 실행된 CLI 명령의 결과를 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다. 단일 디바이스 또는 여러 디바이스의 CLI 결과를 한 번에 내보낼 수 있습니다. 내보낸 정보에는 다음이 포함됩니다.

- 디바이스
- 날짜
- 사용자
- 명령
- 출력

## CLI 명령 결과 내보내기

명령 창에서 방금 실행한 명령의 결과를 .csv 파일로 내보낼 수 있습니다.

### Procedure


- 단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 디바이스를 선택하여 강조 표시하십시오.
- 단계 5 디바이스에 대한 **Device Actions**(디바이스 작업) 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 명령줄 인터페이스 창에서 명령을 입력하고 **Send**(보내기)를 클릭하여 디바이스에 명령을 실행합니다.
- 단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.
- 단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

## CLI 매크로의 결과 내보내기

명령 창에서 실행된 매크로의 결과를 내보낼 수 있습니다. 하나 이상의 디바이스에서 실행된 CLI 매크로의 결과를 .csv 파일로 내보내려면 다음 절차를 따르십시오.

### Procedure



- 단계 1 **Devices & Services**(디바이스 및 서비스) 페이지를 엽니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 디바이스를 선택하여 강조 표시하십시오.

- 단계 5 디바이스에 대한 **Device Actions**(디바이스 작업) 창에서 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 ★를 선택합니다.
- 단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send**(보내기)를 클릭합니다.
- 단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.
- 단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

## CLI 명령 기록 내보내기

다음 절차를 사용하여 하나 또는 여러 디바이스의 CLI 기록을 .csv 파일로 내보냅니다.

### Procedure

- 단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 디바이스를 선택하여 강조 표시하십시오.
- 단계 5 디바이스에 대한 디바이스 작업 창에서 **>\_Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 아직 확장되지 않은 경우 시계 아이콘  을 클릭하여 기록 창을 확장합니다.
- 단계 7 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.
- 단계 8 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.


### 관련 정보:

- [CDO 명령줄 인터페이스, on page 105](#)
- [새 명령에서 CLI 매크로 생성](#)
- [CLI 매크로 삭제](#)
- [CLI 매크로 편집](#)
- [CLI 매크로 실행](#)
- [명령줄 인터페이스 설명서](#)
- [대량 명령줄 인터페이스](#)

## CLI 매크로 목록 내보내기

명령 창에서 실행된 매크로만 내보낼 수 있습니다. 다음 절차를 사용하여 하나 이상의 디바이스의 CLI 매크로를 .csv 파일로 내보냅니다.

프로시저

- 단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 디바이스를 선택하여 강조 표시하십시오.
- 단계 5 디바이스에 대한 디바이스 작업 창에서 > **Command Line Interface**(명령줄 인터페이스)를 클릭합니다.
- 단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 ★를 선택합니다.
- 단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send**(보내기)를 클릭합니다.
- 단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.
- 단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다.

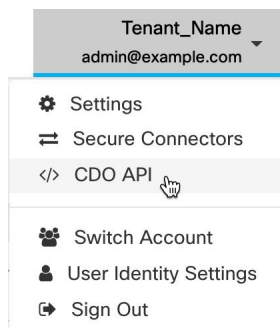
## CDO 공용 API

CDO는 공용 API를 게시하고 문서, 예시 및 테스트를 위한 플레이그라운드를 제공했습니다. 공용 API의 목표는 CDO UI에서 일반적으로 수행할 수 있는 많은 작업을 코드에서 간단하고 효과적으로 수행할 수 있는 방법을 제공하는 것입니다.

이 API를 사용하려면 GraphQL을 알아야 합니다. 공식 가이드(<https://graphql.org/learn/>)를 통해 쉽고 간단하게 읽을 수 있습니다.

전체 스키마 설명서를 찾으려면 [GraphQL 플레이그라운드](#)로 이동하여 페이지 오른쪽에 있는 Docs(문서) 탭을 클릭합니다.

사용자 메뉴에서 CDO 공용 API를 선택하여 시작할 수 있습니다.



# REST API 매크로 생성

## API 툴 사용

CDO은 FDM 관리 디바이스에서 고급 작업을 수행하기 위해 FDM 관리 디바이스 REST(REpresentational State Transfer) API(애플리케이션 프로그래밍) 요청을 실행할 수 있는 API 툴 인터페이스를 제공합니다. REST API는 JSON(JavaScript Object Notation) 형식을 사용하여 개체를 표시합니다.

인터페이스는 시스템 정의 또는 사용자 정의 API 매크로를 제공합니다. 시스템 정의 매크로는 CDO에서 제공하며 편집하거나 삭제할 수 없습니다. 사용자 정의 매크로는 사용자가 생성하며 편집하거나 삭제할 수 있습니다. Secure Firewall device manager API 탐색기에서 지원되는 모든 리소스 그룹을 사용할 수 있습니다.



**Note** CDO은 JSON을 반환하는 API 엔드포인트만 지원합니다.

### 가정

사용자에게 프로그래밍에 대한 일반적인 지식과 REST API 및 JSON에 대한 구체적인 이해가 있다고 가정합니다. 이러한 기술을 처음 접하는 경우, REST API에 대한 일반적인 가이드를 먼저 읽어보십시오.

### 지원되는 문서

- 자세한 내용은 [Cisco Firepower Threat Defense REST API 가이드](#)를 참조하십시오.
- [Cisco DevNet 사이트](#)에서 참조 정보 및 예시 온라인을 확인할 수도 있습니다.

### 지원되는 HTTP 방법

다음과 같은 HTTP 방법만 사용할 수 있으며,



**Important** Cisco Defense Orchestrator의 사용자 역할 역할의 사용자는 GET 작업만 수행할 수 있습니다.

속성	설명
GET	디바이스에서 데이터를 읽습니다.
POST	리소스 유형에 대한 새 개체를 만듭니다. 예를 들어, POST를 사용하여 새 네트워크 개체를 생성합니다.

속성	설명
PUT	기존 리소스의 속성을 변경합니다. PUT을 사용할 때는 전체 JSON 개체를 포함해야 합니다. 개체 내에서 개별 특성을 선택적으로 업데이트할 수는 없습니다. 예를 들어, PUT을 사용하여 기존 네트워크 개체 내에 포함된 주소를 수정합니다.
DELETE	자신 또는 다른 사용자가 생성한 리소스를 제거합니다. 예를 들어, DELETE를 사용하여 더 이상 사용하지 않는 네트워크 개체를 제거합니다.

관련 정보:

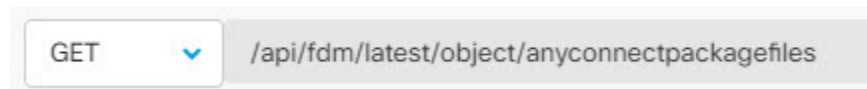
- [Secure Firewall Threat Defense REST API 요청을 입력하는 방법](#)
- [FTD REST API 매크로 정보](#)
  - [REST API 매크로 생성](#)
  - [REST API 매크로 실행](#)
  - [REST API 매크로 편집](#)
  - [REST API 매크로 삭제](#)

## Secure Firewall Threat Defense REST API 요청을 입력하는 방법

FDM 관리 디바이스를 선택하고 단일 명령을 지정하거나 추가 매개변수가 필요한 명령을 실행할 수 있습니다.

REST API 요청의 구문을 확인하려면 <https://ftd.example.com/#/api-explorer> 같은 디바이스의 API Explorer(예: API 탐색기) 페이지에 로그인하고 필요한 리소스 그룹을 클릭하여 실행할 명령의 구문을 확인합니다. 예를 들어 <https://10.10.5.84/#/api-explorer>입니다.

다음 그림은 Cisco Defense Orchestrator에서 단일 REST API 요청의 예를 보여줍니다.



다음 그림에는 추가 매개변수가 필요한 REST API 요청의 예가 나와 있습니다. 요청 본문에서 데이터를 수동으로 지정해야 합니다. 명령의 구문을 확인하려면 디바이스의 API Explorer(API 탐색기) 페이지에 로그인합니다.



**Note** POST 요청을 실행하려면 디바이스가 동기화된 상태여야 합니다.



## Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 REST API를 사용하여 관리할 FDM 관리 디바이스를 선택하고, 오른쪽의 **Device Actions**(디바이스 작업)에서 **API Tool**(API 툴)을 클릭합니다.
- 단계 5 드롭다운에서 요청 방법을 선택하고 **/api/fdm/latest/**를 입력한 다음 실행할 명령을 입력합니다. POST 또는 PUT 명령을 실행하는 경우 요청 본문을 입력합니다.
- 단계 6 **Send**(보내기)를 클릭합니다. **Response Body**(응답 본문)에는 실행된 명령의 응답이 표시됩니다.

**Important** POST 요청은 일반적으로 디바이스에서 준비된 구성을 변경합니다. **Commit Changes in FDM**(FDM에서 변경 사항 커밋)을 클릭하여 FDM 관리 디바이스에 변경 사항을 전송합니다.

### 관련 정보:

- [API 툴 사용, on page 608](#)
- [FTD REST API 매크로 정보](#)
  - [REST API 매크로 생성](#)
  - [REST API 매크로 실행](#)
  - [REST API 매크로 편집](#)
  - [REST API 매크로 삭제](#)

## FTD REST API 매크로 정보

REST API 매크로는 즉시 사용할 수 있는 완전한 형식의 REST API 명령이거나 실행 전에 수정할 수 있는 REST API 명령의 템플릿입니다. 모든 REST API 매크로는 하나 이상의 FTD 디바이스에서 동시에 실행할 수 있습니다.



여러 디바이스에서 동일한 명령을 동시에 실행하려면 템플릿과 유사한 REST API 매크로를 사용합니다. REST API 매크로는 디바이스 구성 및 관리의 일관성을 유지합니다. 완전한 형식의 REST API 매크로를 사용하여 디바이스에 대한 정보를 가져옵니다. FTD 디바이스에서 즉시 사용할 수 있는 다양한 REST API 매크로가 있습니다.

자주 수행하는 작업에 대해 REST API 매크로를 생성할 수 있습니다. 자세한 내용은 [REST API 매크로 생성](#)을 참조하십시오.

REST API 매크로는 시스템 정의 또는 사용자 정의입니다. 시스템 정의 매크로는 CDO에서 제공하며 편집하거나 삭제할 수 없습니다. 사용자 정의 매크로는 사용자가 생성하며 편집하거나 삭제할 수 있습니다.



**Note** 디바이스가 CDO에 온보딩된 후에만 디바이스에 대한 매크로를 생성할 수 있습니다.

관련 정보:

- [REST API 매크로 생성](#)
- [REST API 매크로 실행](#)
- [REST API 매크로 편집](#)
- [REST API 매크로 삭제](#)

## REST API 매크로 생성

새 명령에서 REST API 매크로 생성

### Procedure

**단계 1** REST API 매크로를 생성하기 전에 CDO의 REST API 인터페이스에서 명령을 테스트하여 명령 syntax(명령문)가 올바른지, 그리고 신뢰할 수 있는 결과를 반환하는지 확인합니다.

**Note** 디바이스가 CDO에 온보딩된 후에만 디바이스에 대한 매크로를 생성할 수 있습니다.

**단계 2** REST API를 사용하여 관리할 FTD 디바이스를 선택하고 오른쪽의 **Device Actions**(디바이스 작업)에서 **API Tool**(API 툴)을 클릭합니다.

**단계 3** REST API 매크로 즐겨찾기 스타(★)를 클릭하여 이미 존재하는 매크로를 확인합니다.

**단계 4** 더하기  버튼을 클릭합니다.

**단계 5** 매크로에 고유한 이름을 지정합니다. 원하는 경우 REST API 매크로에 대한 설명 및 참고 사항을 제공합니다.

**단계 6** **Request Method**(요청 방법)를 선택하고 **Request Endpoint**(요청 엔드포인트) 필드에 엔드포인트 URL을 입력합니다. 자세한 내용은 [Cisco Firepower Threat Defense REST API 가이드](#)를 참조하십시오.

**단계 7** 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

Request Method	Request Endpoint
POST	/api/fdm/latest/object/networks
Request Body*	
The request body can be parameterized by adding tags around the parameter names. e.g. { "name": "{{object_name}}". } When using this macro you will be able to fill in the parameters.	
Note: Only alphanumeric characters and underscores are allowed for parameter names	
<pre>{   "name": "{{object_name}}",   "subType": "NETWORK",   "value": "{{ip}}/{{subnet_mask}}",   "type": "networkobject" }</pre>	<b>Parameters</b> <ul style="list-style-type: none"> <li>object_name 1</li> <li>ip 1</li> <li>subnet_mask 1</li> </ul>

단계 8 **OK**(확인)를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 [REST API 매크로 실행](#)을 참조하십시오.

## 기록 또는 기존 REST API 매크로에서 REST API 매크로 생성

이 절차에서는 이미 실행한 명령, 다른 사용자 정의 매크로 또는 시스템 정의 매크로에서 사용자 정의 REST API 매크로를 생성합니다.

### Procedure

단계 1 REST API를 사용하여 관리할 FDM 관리 디바이스를 선택하고, 오른쪽의 **Device Actions**(디바이스 작업)에서 **API Tool**(API 툴)을 클릭합니다.

**Note** REST API 기록에서 사용자 정의 매크로를 생성하려면 명령을 실행한 디바이스를 선택합니다. REST API 매크로는 동일한 계정의 여러 디바이스에서 공유되지만, REST API 기록은 공유되지 않습니다.

단계 2 API 매크로를 만들 명령을 찾아 선택합니다. 다음 방법 중 하나를 사용합니다.

- 해당 디바이스에서 실행한 명령을 보려면 시계 ⌚를 클릭합니다. 매크로로 변환할 항목을 더블 클릭하여 선택하면 **Command**(명령) 창에 명령이 나타납니다.
- API 매크로 즐겨찾기 스타(★)를 클릭하여 이미 존재하는 매크로를 확인합니다. 변경할 사용자 정의 또는 시스템 정의 API 매크로를 선택합니다. **Command**(명령) 창에 명령이 나타납니다.

단계 3 명령 창의 명령을 사용하여 API 매크로 금색 스타(★)를 클릭합니다. 이 명령은 이제 새 API 매크로의 기본이 됩니다.

단계 4 매크로에 고유한 이름을 지정합니다. 원하는 경우 API 매크로에 대한 설명 및 참고 사항을 제공합니다.

단계 5 명령 필드에서 명령을 검토하고 원하는 대로 변경합니다.

단계 6 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 7 **Create**(생성)를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 [REST API 매크로 실행](#)을 참조하십시오.

관련 정보:

[FTD REST API 매크로 정보](#)

## REST API 매크로 실행

### Procedure

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 **FTD** 탭을 클릭합니다.

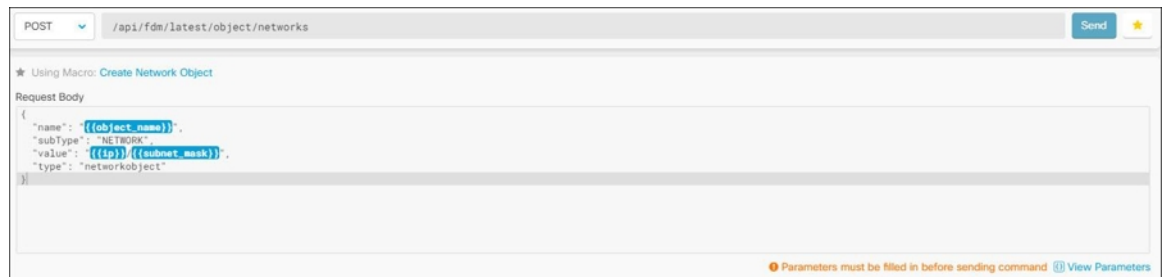
단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **API Tool**(API 툴)를 클릭합니다.

단계 5 명령 패널에서 별표 ★를 클릭하여 REST API 매크로를 확인합니다.

단계 6 명령 패널에서 REST API 매크로를 선택합니다.

단계 7 다음 두 가지 방법 중 하나로 매크로를 실행합니다.

- 매크로에 정의할 매개변수가 없는 경우 **Send**(전송)를 클릭합니다. 명령에 대한 응답이 응답 창에 나타납니다. 다 됐습니다.
- 아래의 Create Network Object(네트워크 개체 생성) 매크로와 같은 매개변수가 매크로에 포함되어 있으면 **View Parameters**(매개변수 보기)를 클릭합니다.



단계 8 **Parameters**(매개변수) 창의 **Parameters**(매개변수) 필드에 매개변수 값을 입력합니다.

단계 9 **Send**(보내기)를 클릭합니다.

**Note** FTD 디바이스의 활성 구성이 업데이트됩니다.

관련 정보:

[FTD REST API 매크로 정보](#)

## REST API 매크로 편집

사용자 정의 REST API 매크로는 편집할 수 있지만 시스템 정의 매크로는 편집할 수 없습니다. REST API 매크로를 편집하면 모든 FDM 관리 디바이스에 대해 변경됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

### Procedure

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 **FTD** 탭을 클릭합니다.

단계 4 REST API를 사용하여 관리할 FDM 관리 디바이스를 선택하고, 오른쪽의 **Device Actions**(디바이스 작업)에서 **API Tool**(API 툴)을 클릭합니다.

단계 5 편집할 사용자 정의 매크로를 선택합니다.

단계 6 매크로 레이블에서 편집 아이콘을 클릭합니다.

단계 7 Edit Macro(매크로 편집) 대화 상자에서 REST API 매크로를 편집합니다.

단계 8 **Save**(저장)를 클릭합니다.

REST API 매크로를 실행하는 방법에 대한 지침은 [REST API 매크로 실행](#)을 참조하십시오.


관련 정보:

[FTD REST API 매크로 정보](#)

## REST API 매크로 삭제

사용자 정의 REST API 매크로는 삭제할 수 있지만 시스템 정의 매크로는 삭제할 수 없습니다. REST API 매크로를 삭제하면 모든 디바이스에서 삭제됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 디바이스를 선택하고 오른쪽의 **Device Actions**(디바이스 작업)에서 **API Tool**(API 툴)을 클릭합니다.
- 단계 5 삭제할 사용자 정의 REST API 매크로를 선택합니다.
- 단계 6 REST API 매크로 레이블에서 휴지통 아이콘 을 클릭합니다.
- 단계 7 REST API 매크로를 제거할지 확인합니다.

관련 정보:

[FTD REST API 매크로 정보](#)

## 변경 사항 읽기, 삭제, 확인 및 구축

디바이스를 관리하려면 CDO의 로컬 데이터베이스에 저장된 디바이스 구성의 자체 복사본이 있어야 합니다. CDO는 관리하는 디바이스에서 구성을 "읽을 때" 디바이스 구성의 복사본을 가져와 저장합니다. CDO가 디바이스 구성의 복사본을 처음 읽고 저장하는 경우는 디바이스가 온보딩될 때입니다. 이러한 선택 항목은 다양한 목적으로 구성을 읽는 것을 설명합니다.

- **Discard Changes**(변경 사항 취소)는 디바이스의 구성 상태가 "Not Synced(동기화되지 않음)"인 경우에 사용할 수 있습니다. **Not Synced(동기화되지 않음)** 상태에서는 CDO에서 보류 중인 디바이스의 구성에 대한 변경 사항이 있습니다. 이 옵션을 사용하면 보류 중인 모든 변경 사항을 취소할 수 있습니다. 보류 중인 변경 사항이 삭제되고 CDO가 디바이스에 저장된 구성의 복사본으로 구성의 복사본을 덮어씁니다.
- 변경 사항을 확인합니다. 이 작업은 디바이스의 구성 상태가 동기화된 경우에 사용할 수 있습니다. **Checking for Changes**(변경 사항 확인)를 클릭하면 CDO가 디바이스의 구성 복사본을 디바이스에 저장된 구성의 복사본과 비교하게 됩니다. 차이가 있는 경우 CDO는 디바이스에 저장된 복사본으로 디바이스 구성의 복사본을 즉시 덮어씁니다.
- 충돌을 검토하고 검토 없이 수락합니다. 디바이스에서 **Conflict Detection**(충돌 탐지)을 활성화한 경우 CDO는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 디바이스에 저장된 구성의 복사본이 변경된 경우 CDO는 "Conflict Detected(충돌 탐지됨)" 구성 상태를 표시하여 사용자에게 알립니다.

- 충돌을 검토합니다. **Review Conflict**(충돌 검토)를 클릭하면 디바이스에서 직접 변경 사항을 검토하고 이를 수락하거나 거부할 수 있습니다.
- 검토 없이 수락합니다. 이 작업은 CDO의 디바이스 구성 복사본을 디바이스에 저장된 구성의 최신 복사본으로 덮어씁니다. CDO에서는 덮어쓰기 작업을 수행하기 전에 구성의 두 복사본에서 차이점을 확인하라는 메시지를 표시하지 않습니다.

모두 읽기는 대량 작업입니다. 상태에 상관없이 둘 이상의 디바이스를 선택하고 **Read All**(모두 읽기)을 클릭하여 CDO에 저장된 모든 디바이스의 구성을 디바이스에 저장된 구성으로 덮어쓸 수 있습니다.

#### 변경 사항 구축

디바이스의 구성을 변경하면 CDO는 변경 사항을 구성의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 구축될 때까지 CDO에서 "보류 중"입니다. 디바이스에 구축되지 않은 설정 변경 사항이 있는 경우 디바이스는 동기화되지 않은 설정 상태가 됩니다.

보류 중인 구성 변경 사항은 디바이스를 통해 실행되는 네트워크 트래픽에 영향을 주지 않습니다. CDO가 디바이스에 변경 사항을 구축한 후에야 적용됩니다. CDO는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다. 구축은 단일 디바이스 또는 둘 이상의 디바이스에서 동시에 시작할 수 있습니다.



참고 구축 또는 반복 구축을 예약할 수 있습니다. 자세한 내용은 [자동 구축 예약, 624 페이지](#)를 참조하십시오.

**Discard All**(모두 취소)은 **Preview and Deploy**(미리보기 및 구축)...를 클릭한 후에만 사용할 수 있는 옵션입니다.. **Preview and Deploy**(미리보기 및 구축)를 클릭하면 CDO는 CDO에 보류 중인 변경 사항의 미리보기를 표시합니다. **Discard All**(모두 취소)을 클릭하면 CDO에서 보류 중인 모든 변경 사항이 삭제되며 선택한 디바이스에 어떤 것도 구축되지 않습니다. 위의 "변경 사항 취소"와 달리 보류 중인 변경 사항을 삭제하면 작업이 종료됩니다.

## 모든 디바이스 구성 읽기

CDO(Cisco Defense Orchestrator) 외부의 디바이스에 대한 구성이 변경되면 CDO에 저장된 디바이스의 구성과 디바이스 구성의 로컬 복사본은 더 이상 동일하지 않습니다. 구성을 다시 동일하게 만들기 위해 디바이스에 저장된 구성으로 CDO의 디바이스 구성 복사본을 덮어쓰려는 경우가 많습니다.

**Read All**(모두 읽기) 링크를 사용하여 여러 디바이스에서 동시에 이 작업을 수행할 수 있습니다.

CDO에서 디바이스 구성의 두 복사본을 관리하는 방법에 대한 자세한 내용은 [변경 사항 읽기, 삭제, 확인 및 구축](#)을 참조하십시오.

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

- 충돌 탐지 - 충돌 탐지가 활성화된 경우 CDO는 구성 변경 사항에 대해 10분마다 관리하는 디바이스를 폴링합니다. CDO는 디바이스의 구성이 변경된 것을 발견하면 디바이스에 대한 구성 상태를 "충돌 탐지됨"으로 표시합니다.
- 동기화됨 - 디바이스가 동기화된 상태인 경우 **Read All**(모두 읽기)을 클릭하면 CDO는 즉시 디바이스를 확인하여 구성이 직접 변경되었는지 확인합니다. **Read All**(모두 읽기)을 클릭하면 CDO가 디바이스 구성의 복사본을 덮어쓸 것임을 확인한 다음 덮어쓰기를 수행합니다.
- 동기화되지 않음 - 디바이스가 Not Synced(동기화되지 않음) 상태인 경우 **Read All**(모두 읽기)을 클릭하면 CDO는 CDO를 사용하는 디바이스의 구성에 대해 보류 중인 변경 사항이 있으며 **Read All**(모두 읽기) 작업을 진행하면 해당 변경 사항이 삭제되고 디바이스의 구성이 포함된 CDO의 구성 복사본입니다. 이 **Read All**(모두 읽기)은 **변경 사항 취소**와 같은 기능을 합니다.

## Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 (선택 사항) 변경 로그에서 이 대량 작업의 결과를 쉽게 식별할 수 있도록 **변경 요청 관리**를 생성합니다.
- 단계 5 CDO를 저장할 디바이스를 선택합니다. CDO는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.
- 단계 6 **Read All**(모두 읽기)을 클릭합니다.
- 단계 7 CDO는 CDO에 준비된 구성 변경 사항이 있는 경우 선택한 디바이스에 대해 경고하고, 구성 대량 읽기 작업을 계속할 것인지 묻습니다. 계속하려면 **Read All**(모두 읽기)을 클릭합니다.
- 단계 8 **Read All**(모두 읽기) 구성 작업의 진행 상황은 **작업 페이지**에서 확인합니다. 대량 작업의 개별 작업이 성공하거나 실패한 방식에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **작업 페이지** 페이지로 이동합니다.
- 단계 9 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

## 관련 정보

- [변경 사항 읽기, 삭제, 확인 및 구축](#)
- [변경 사항 취소](#)
- [구성 변경 사항 확인](#)

# FDM-관리 디바이스에서 CDO로 구성 변경 사항 읽기

## Cisco Defense Orchestrator가 FDM 관리 디바이스 구성을 읽는 이유는 무엇입니까?

FDM 관리 디바이스를 관리하려면 CDO에 FDM 관리 디바이스 구성의 자체 저장된 복사본이 있어야 합니다. CDO는 FDM 관리 디바이스에서 구성을 읽을 때, FDM 관리 디바이스의 배포된 구성 복사본을 가져와 자체 데이터베이스에 저장합니다. CDO가 디바이스 구성 파일의 복사본을 처음 읽고 저장하는 경우는 디바이스가 온보딩될 때입니다. 자세한 내용은 [변경 사항 읽기](#), [삭제](#), [확인 및 구축](#)를 참조하십시오.

### 보류 중 및 배포된 변경 사항

FDM(Firepower Device Manager) 또는 해당 CLI를 통해 직접 FDM 관리 디바이스에 수행된 구성 변경은 배포될 때까지 FDM 관리 디바이스에 준비된 변경이라고 합니다. 준비되거나 보류 중인 변경 사항은 FDM 관리 디바이스를 통해 실행되는 트래픽에 영향을 주지 않고 편집하거나 삭제할 수 있습니다. 그러나 보류 중인 변경 사항이 배포되면 FDM 관리 디바이스에 의해 적용되며 디바이스를 통해 실행되는 트래픽에 영향을 미칩니다.

### 충돌 탐지

디바이스에서 [충돌 탐지](#)를 활성화한 경우 CDO는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 디바이스에 저장된 구성의 복사본이 변경된 경우 CDO는 "충돌 탐지됨" 구성 상태를 표시하여 사용자에게 알립니다. 충돌 감지를 활성화하지 않았거나 자동 폴링 사이의 10분 간격 내에 디바이스의 구성이 변경된 경우, 변경 사항 확인을 클릭하면 CDO가 디바이스의 구성을 CDO에 저장된 구성 복사본과 즉시 비교하라는 메시지를 표시합니다. 충돌 검토를 선택하여 디바이스 구성과 CDO에 저장된 구성 간의 차이점을 검토한 다음, **Discard Changes**(변경 사항 취소)를 선택하여 준비된 변경 사항을 제거하고 저장된 구성으로 되돌리거나 변경 사항을 확인할 수 있습니다. **Accept without Review**(검토 없이 수락)을 선택할 수도 있습니다. 이 옵션은 구성을 가져와서 현재 CDO에 저장된 내용을 덮어 씩습니다.

## 변경 취소 절차

FDM 관리 디바이스에서 구성 변경 사항을 삭제하려면 다음 절차를 따르십시오.


### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 유형 탭을 클릭합니다.
- 단계 4 구성이 충돌 감지됨으로 설정된 디바이스를 선택하고 보류 중인 변경 사항 되돌리기 링크를 제공합니다. 이 메시지는 링크를 클릭하여 보류 중인 변경 사항을 되돌리거나 로컬 관리자 FDM을 사용하여 디바이스에 로그인하고 변경 사항을 먼저 배포할 수 있다고 설명합니다. [필터](#)를 사용하여 충돌 상태의 디바이스를 찾을 수 있습니다.




**Caution** 보류 중인 변경 사항 되돌리기 링크를 클릭하면 FDM 관리 디바이스에서 보류 중인 변경 사항이 즉시 삭제됩니다. 먼저 변경 사항을 검토할 기회가 없습니다.

단계 5 보류 중인 변경 사항 되돌리기를 클릭하기 전에 FDM에서 변경 사항을 검토합니다.

- a. 브라우저 창을 열고 [https://<IP\\_address\\_of\\_the\\_FTD>](https://<IP_address_of_the_FTD>)를 입력합니다.
- b. FDM에서 배포 아이콘을 찾습니다. 배포할 준비가 된 변경 사항이 있음을 나타내는 주황색 원이 표시됩니다. 
- c. 아이콘을 클릭하고 보류 중인 변경 사항을 검토합니다.
  - 변경 사항을 삭제할 수 있는 경우 CDO로 돌아가서 "보류 중인 변경 사항 되돌리기"를 클릭합니다. 이 시점에서 FDM 관리 디바이스의 구성과 CDO의 구성 사본이 동일해야 합니다. 마쳤습니다.
  - 변경 사항을 디바이스에 배포하려면 **Deploy Now**(지금 배포)를 클릭합니다. 이제 FDM 관리 디바이스에 배포된 구성과 CDO에 저장된 구성이 다릅니다. 그런 다음 CDO로 돌아가서 디바이스에서 변경 사항 [구성 변경 사항 확인](#). CDO는 FDM 관리 디바이스에 변경 사항이 있음을 식별하고 충돌을 검토할 기회를 제공합니다. 해당 상태를 해결하려면 [충돌 탐지](#)를 참조하십시오.

## 보류 중인 변경 사항 되돌리기가 실패하는 경우

시스템 데이터베이스 및 보안 피드에 대한 변경 사항은 CDO로 되돌릴 수 없습니다. CDO는 보류 중인 변경 사항이 있음을 인식하고 되돌리려고 시도한 다음 실패합니다. 되돌리기 실패가 보류 중인 데이터베이스 업데이트 또는 보안 피드 업데이트로 인한 것인지 확인하려면 디바이스의 FDM 콘솔에 로그인합니다. 배포할 준비가 된 변경 사항이 있음을 나타내는 주황색 원이 표시됩니다.  보류 중인 변경 사항을 검토하고 필요에 따라 배포하거나 기다렸다가 삭제하려면 배포 버튼을 클릭합니다.

## 충돌 검토 절차

FDM 관리 디바이스의 구성 변경 사항을 검토하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 구성이 충돌 감지됨으로 표시된 디바이스를 선택하면 오른쪽의 충돌 감지됨 창에서 충돌 검토에 대한 링크를 제공합니다.
- 단계 5 충돌 검토를 클릭합니다.

단계 6 표시되는 두 가지 구성을 비교합니다.

단계 7 다음 작업 중 하나를 수행합니다.

- **Accept**(수락) 을 클릭하여 CDO에서 마지막으로 알려진 구성을 디바이스에서 찾은 구성으로 덮어씁니다. 참고: CDO에 저장된 전체 구성은 디바이스에서 찾은 구성으로 완전히 덮어씁니다.
- **Reject**(거부)를 클릭하여 디바이스에 대한 변경 사항을 거부하고 CDO에서 마지막으로 알려진 구성으로 바꿉니다.
- **Cancel**(취소)를 클릭하여 작업을 중지합니다.

**Note** 디바이스가 동기화됨 상태에 있는 동안 **구성 변경 사항 확인**을 클릭하여 대역 외 변경 사항에 대해 디바이스를 즉시 확인하도록 CDO에 메시지를 표시할 수 있습니다.

## 검토 없이 수락 절차

검토 없이 FDM 관리 디바이스의 구성 변경 사항을 수락하려면 다음 절차를 따르십시오.

### Procedure

단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭합니다.

단계 4 구성이 충돌 감지됨으로 표시된 디바이스를 선택하면 오른쪽의 충돌 감지됨 창에서 **Accept Without Review**(검토 없이 수락)에 대한 링크를 제공합니다.

단계 5 **Accept Without Review**(검토 없이 수락)를 클릭합니다. CDO는 현재 구성을 수락하고 덮어씁니다.

관련 정보:

- [변경 사항 읽기, 삭제, 확인 및 구축](#)
- [충돌 탐지](#)
- [변경 사항 취소](#)

## 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축

테넌트의 디바이스에 대한 구성을 변경했지만 해당 변경 사항을 구축하지 않은 경우 Deploy(구축) 아이콘




. 이러한 변경의 영향을 받는 디바이스는 **Devices and Services**(디바이스 및 서비스) 페이지에서 "Not Synced(동기화되지 않음)" 상태로 표시됩니다. **Deploy**(구축)를 클릭하면 보류 중인 변경 사항이 있는 디바이스를 검토하고 해당 디바이스에 변경 사항을 구축할 수 있습니다.

이 구축 방법은 지원되는 모든 디바이스에서 사용할 수 있습니다.

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

프로시저

- 단계 1 화면의 오른쪽 상단에서 **Deploy**(구축) 아이콘  을 클릭합니다.
- 단계 2 구축하려는 변경 사항이 있는 디바이스를 선택합니다. 디바이스에 노란색 주의 삼각형이 있는 경우 해당 디바이스에 변경 사항을 구축할 수 없습니다. 노란색 주의 삼각형 위에 마우스를 올려놓으면 해당 디바이스에 변경 사항을 구축할 수 없는 이유를 확인할 수 있습니다.
- 단계 3 디바이스를 선택한 후 오른쪽 패널에서 디바이스를 확장하고 특정 변경 사항을 미리 볼 수 있습니다.
- 단계 4 (선택 사항) 보류 중인 변경 사항에 대한 자세한 정보를 보려면 **View Detailed Changelog**(자세한 변경 로그 보기) 링크를 클릭하여 해당 변경과 관련된 변경 로그를 엽니다. **Deploy**(구축) 아이콘을 클릭하여 **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지로 돌아갑니다.
- 단계 5 (선택 사항) **Devices with Pending Changes**(보류 중인 변경 사항이 있는 디바이스) 페이지에서 나가지 않고 변경 사항을 추적하려면 [변경 요청 관리](#)합니다.
- 단계 6 선택한 디바이스에 변경 사항을 즉시 구축하려면 **Deploy Now**(지금 구축)를 클릭합니다. 작업 트레이의 활성 작업 표시기에 진행 상황이 표시됩니다.
- 단계 7 (선택 사항) 구축이 완료되면 CDO 탐색 모음에서 **Jobs**(작업)를 클릭합니다. 구축 결과를 보여주는 최근 "Deploy Changes(변경 사항 구축)" 작업이 표시됩니다.
- 단계 8 변경 요청 레이블을 생성했으며 더 이상 연결할 구성 변경 사항이 없는 경우 해당 레이블을 지웁니다.

다음에 수행할 작업

- [예약된 자동 배포](#)
- [CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축, 621 페이지](#)
- [FDM-관리 디바이스에 구축한 후 로그 항목 변경, 641 페이지](#)

## CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축

**CDO가 FDM-관리 디바이스에 변경 사항을 구축하는 이유**

CDO를 사용하여 디바이스의 구성을 관리하고 변경하면 CDO는 변경 사항을 구성 파일의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 구축될 때까지 CDO에서 준비된 것으로 간주됩니다. 준비된 구성 변경은 디바이스를 통해 실행되는 네트워크 트래픽에 영향을 주지 않습니다. CDO가

디바이스에 변경 사항을 구축한 후에야 디바이스를 통해 실행되는 트래픽에 영향을 미칩니다. CDO는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다.

CDO와 마찬가지로 FDM 관리 디바이스에는 보류 중인 변경 사항 및 구축된 변경 사항의 개념이 있습니다. FDM 관리 디바이스에서 보류 중인 변경 사항은 CDO의 준비된 변경 사항과 같습니다. 보류 중인 변경 사항은 FDM 관리 디바이스를 통해 실행되는 트래픽에 영향을 주지 않고 편집하거나 삭제할 수 있습니다. 그러나 보류 중인 변경 사항이 구축되면 FDM 관리 디바이스에 의해 적용되며 디바이스를 통해 실행되는 트래픽에 영향을 미칩니다.

FTD 매니지드 디바이스는 2단계 프로세스로 구성 파일을 편집하므로, CDO는 자신이 관리하는 다른 디바이스와는 약간 다르게 FDM 관리 디바이스에 변경 사항을 구축합니다. CDO는 먼저 변경 사항을 FDM 관리 디바이스에 구축하며 변경 사항은 보류 상태입니다. 그런 다음 CDO가 디바이스에 변경 사항을 구축하고 라이브 상태가 됩니다. 변경 사항이 구축되었으므로 이제 FDM 관리 디바이스를 통해 실행되는 트래픽에 영향을 미칩니다. 이는 독립형 및 고가용성(HA) 디바이스 모두에 적용됩니다.

구축은 단일 디바이스 또는 둘 이상의 디바이스에서 동시에 시작할 수 있습니다. 단일 디바이스에 대해 개별 구축 또는 반복 구축을 예약할 수 있습니다.

두 가지 이유로 CDO가 FDM 관리 디바이스에 변경 사항을 구축할 수 없습니다.

- FDM 관리 디바이스에 준비된 변경이 있는 경우, 이 상태를 해결하는 방법에 대한 자세한 내용은 [충돌 탐지](#)를 참조하십시오.
- CDO는 FDM 관리 디바이스에 구축되는 프로세스에 변경 사항이 있는 경우 변경 사항을 구축하지 않습니다.

#### 자동 구축 예약

또한 [예약된 자동 배포](#)하는 보류 중인 변경 사항이 있는 단일 디바이스에 대한 구축을 예약하도록 테넌트를 구성할 수도 있습니다.

## 디바이스에 변경 사항 배포

### Procedure

**단계 1** CDO를 사용하여 디바이스에 대한 구성을 변경하고 저장하면 해당 변경 사항이 디바이스 구성의 CDO 인스턴스에 저장됩니다.

**단계 2** 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.


**단계 3** **Devices**(디바이스) 탭을 클릭합니다.

**단계 4** 해당 디바이스 탭을 클릭합니다. 변경한 디바이스의 구성 상태가 이제 "동기화되지 않음"으로 표시되어야 합니다.

**단계 5** 다음 방법 중 하나를 사용하여 변경 사항을 배포합니다.

- 디바이스를 선택하고 오른쪽의 동기화되지 않음 창에서 **Preview and Deploy**(미리 보기 및 배포)를 클릭합니다. Pending Changes 화면에서 변경 사항을 검토합니다. 보류 중인 버전에 만족하면

**Deploy Now**(지금 배포)를 클릭합니다. 변경 사항이 성공적으로 배포되면 [변경 로그](#)를 보고 방금 일어난 일을 확인할 수 있습니다.

- 화면의 오른쪽 상단에 있는 **Deploy**(구축) 아이콘 를 클릭합니다. 자세한 내용은 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#), on page 620를 참조하십시오.

## 변경 취소

CDO에서 디바이스로 변경 사항을 배포할 때 **Cancel**(취소)를 클릭하면 변경 사항이 디바이스에 배포되지 않습니다. 프로세스가 취소됩니다. 변경 사항은 여전히 CDO에서 보류 중이며 최종적으로 FDM 관리 디바이스에 배포하기 전에 추가로 편집할 수 있습니다.

## 변경 사항 취소


변경 사항을 미리 볼 때 **Discard all**(모두 취소)을 클릭하면 변경 사항 및 다른 사용자가 수행했지만 디바이스에 구축하지 않은 기타 변경 사항이 삭제됩니다. CDO는 보류 중인 구성을 변경하기 전에 마지막으로 읽거나 구축한 구성으로 되돌립니다.

## 디바이스 구성 대량 구축


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

### Procedure

- 단계 1 탐색 창에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 CDO에서 구성을 변경한 모든 디바이스를 선택합니다. 이러한 디바이스는 "동기화되지 않음" 상태로 표시되어야 합니다.
- 단계 5 다음 방법 중 하나를 사용하여 변경 사항을 구축합니다.

- 화면의 오른쪽 상단에 있는 **Deploy**(구축) 버튼 을 클릭합니다. 이렇게 하면 구축하기 전에 선택한 디바이스에서 보류 중인 변경 사항을 검토할 수 있습니다. **Deploy Now**(지금 구축)를 클릭하여 변경 사항을 구축합니다.

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

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

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

관련 정보:

- [자동 구축 예약, on page 624](#)

## 예약된 자동 배포

CDO를 사용하면 CDO에서 관리하는 하나 이상의 디바이스에 대한 구성을 변경한 다음 편리한 시간에 해당 디바이스에 변경 사항을 배포하도록 예약할 수 있습니다.

Settings(설정) 페이지의 **Tenant Settings**(테넌트 설정) 탭에 [자동 구축 예약 옵션 활성화, on page 51](#) 있는 경우에만 배포를 예약할 수 있습니다. 이 옵션이 활성화되면 예약된 배포를 생성, 편집 또는 삭제할 수 있습니다. 예약된 배포는 CDO에 저장된 모든 단계적 변경 사항을 설정된 날짜 및 시간에 배포합니다. Jobs(작업) 페이지에서 예약된 배포를 보고 삭제할 수도 있습니다.

CDO에서 [변경 사항 읽기, 삭제, 확인 및 구축](#) 않은 디바이스 변경 사항이 있는 경우 충돌이 해결될 때까지 예약된 배포를 건너뛵니다. 예약된 배포가 실패한 인스턴스가 Jobs(작업) 페이지에 나열됩니다.

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



### Caution

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



### Note

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

## 자동 구축 예약

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



### Note

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

## Procedure

- 
- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 하나 이상의 디바이스를 선택합니다.
- 단계 5 **Device Details**(디바이스 세부 정보) 창에서 **Scheduled Deployments**(예약된 구축) 탭을 찾아 **Schedule**(예약)을 클릭합니다.
- 단계 6 구축을 수행해야 하는 시기를 선택합니다.
- 일회성 구축의 경우 **Once on**(한 번) 옵션을 클릭하여 달력에서 날짜와 시간을 선택합니다.
  - 반복 구축의 경우 **Every**(마다) 옵션을 클릭합니다. 매일 또는 일주일에 한 번 구축을 선택할 수 있습니다. 구축을 수행해야 하는 날짜와 시간을 선택합니다.
- 단계 7 **Save**(저장)를 클릭합니다.
- 

## 예약된 배포 편집

예약된 배포를 편집하려면 다음 절차를 따르십시오.

### Procedure

- 
- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 하나 이상의 디바이스를 선택합니다.
- 단계 5 **Device Details**(디바이스 세부 정보) 창에서 예약된 배포 탭을 찾아 **Edit**(편집)를 클릭합니다.



- 단계 6 예약된 배포의 반복, 날짜 또는 시간을 편집합니다.
- 단계 7 **Save**(저장)를 클릭합니다.
- 


## 예약된 배포 삭제

예약된 배포를 삭제하려면 다음 절차를 따르십시오.



**Note** 여러 디바이스에 대한 배포를 예약한 다음 일부 디바이스에 대한 일정을 변경하거나 삭제하면 나머지 디바이스에 대한 원래 예약된 배포가 유지됩니다.

### Procedure

- 단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 하나 이상의 디바이스를 선택합니다.
- 단계 5 **Device Details**(장치 세부 정보)창에서 예약된 배포 탭을 찾아 **Delete**(삭제) 를 클릭합니다.

### What to do next

- 변경 사항 읽기, 삭제, 확인 및 구축
- 모든 디바이스 구성 읽기, [on page 616](#)
- CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축, [on page 621](#)
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, [on page 620](#)

## 구성 변경 사항 확인

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

변경 사항을 확인하려면 다음을 수행합니다.

### Procedure

- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 구성이 디바이스에서 직접 변경되었을 가능성이 있는 디바이스를 선택합니다.
- 단계 5 오른쪽의 Synced(동기화) 창에서 **Check for Changes**(변경 사항 확인)를 클릭합니다.
- 단계 6 다음 동작은 디바이스에 따라 약간 다릅니다.
  - FTD 디바이스의 경우 디바이스의 구성이 변경된 경우 다음 메시지가 표시됩니다.



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

- 계속하려면 **OK(확인)**를 클릭하십시오. 디바이스의 구성이 CDO에 저장된 구성을 덮어씁니다.
- 작업을 취소하려면 **Cancel(취소)**를 클릭합니다.

• 디바이스의 경우:

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

## 변경 사항 취소

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

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

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

### Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 구성을 변경한 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Not Synced**(동기화되지 않음) 창에서 **Discard Changes**(변경 사항 취소)를 클릭합니다.

- FDM 관리 디바이스의 경우 CDO는 "CDO에서 보류 중인 변경 사항이 취소되고 이 디바이스에 대한 CDO 구성이 디바이스에서 현재 실행 중인 구성으로 교체됩니다."라고 경고합니다. 변경 사항을 취소하려면 **Continue**(계속)를 클릭합니다.
- Meraki 디바이스의 경우 CDO가 변경 사항을 즉시 삭제합니다.
- AWS 디바이스의 경우 CDO는 삭제하려는 항목을 표시합니다. **Accept**(수락) 또는 **Cancel**(취소)을 클릭합니다.

## 디바이스의 대역 외 변경 사항

대역 외 변경 사항은 CDO를 사용하지 않고 디바이스에서 직접 변경한 사항을 의미합니다. 이러한 변경은 SSH 연결을 통해 디바이스의 명령줄 인터페이스를 사용하거나 ASA용 ASDM(Adaptive Security Device Manager) 또는 FDM 관리 디바이스용 FDM과 같은 로컬 관리자를 사용하여 수행할 수 있습니다. 대역 외 변경은 CDO에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

디바이스에서 대역 외 변경 탐지

ASA, FDM 관리 디바이스 또는 Cisco IOS 디바이스에 대해 Conflict Detection(충돌 탐지)이 활성화된 경우 CDO는 10분마다 디바이스를 확인하여 CDO 외부에서 디바이스의 구성에 직접 적용된 새로운 변경 사항을 검색합니다.

CDO에 저장되지 않은 디바이스 구성 변경 사항이 있음을 발견하면 CDO는 해당 디바이스의 구성 상태를 "충돌 탐지됨" 상태로 변경합니다.

Defense Orchestrator에서 충돌을 탐지하는 경우 다음 두 가지 조건 중 하나가 발생할 수 있습니다.

- CDO의 데이터베이스에 저장되지 않은 디바이스에 직접 적용된 구성 변경 사항이 있습니다.
- FDM 관리 디바이스의 경우 구축되지 않은 FDM 관리 디바이스에 "보류 중인" 구성 변경 사항이 있을 수 있습니다.

## Defense Orchestrator와 디바이스 간 구성 동기화

구성 충돌 정보

디바이스 및 서비스 페이지에서 디바이스 또는 서비스의 상태가 "Synced(동기화됨)", "Not Synced(동기화되지 않음)" 또는 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다.

- 디바이스가 동기화되면 CDO(Cisco Defense Orchestrator)의 구성과 디바이스에 로컬로 저장된 구성이 동일합니다.

- 디바이스가 동기화되지 않은 경우 CDO에 저장된 구성이 변경되었으며 이제 디바이스에 로컬로 저장된 구성이 다릅니다. CDO에서 디바이스로 변경 사항을 구축하면 CDO의 버전과 일치하도록 디바이스의 구성이 변경됩니다.
- CDO 외부에서 디바이스에 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경이 수행되면 디바이스에 대해 충돌 탐지가 활성화된 경우 디바이스 상태가 "Conflict Detected(충돌 탐지됨)"로 변경됩니다. 대역 외 변경 사항을 수락하면 는 CDO의 구성을 디바이스의 구성과 일치하도록 변경합니다.

## 충돌 탐지

충돌 탐지가 활성화된 경우 CDO(Cisco Defense Orchestrator)는 기본 간격 동안 디바이스를 폴링하여 CDO 외부에서 디바이스의 구성이 변경되었는지 확인합니다. CDO는 변경 사항을 탐지하면 디바이스의 구성 상태를 **Conflict Detected(충돌 탐지됨)**로 변경합니다. CDO 외부에서 디바이스에 적용된 변경 사항을 "대역 외" 변경 사항이라고 합니다.

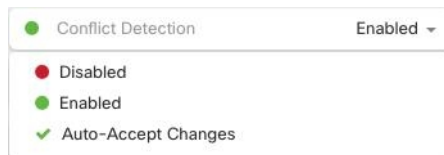
이 옵션이 활성화되면 디바이스별로 충돌 또는 OOB 변경 사항이 탐지되는 빈도를 구성할 수 있습니다. 자세한 내용은 [디바이스 변경 사항에 대한 폴링 예약](#), on page 632를 참조하십시오.

## 충돌 탐지 활성화

충돌 감지를 활성화하면 Defense Orchestrator 외부의 디바이스가 변경된 인스턴스에 대해 경고합니다.

### Procedure

- 단계 1 탐색 모음에서 **Inventory(재고 목록)**를 클릭합니다.
- 단계 2 **Devices(디바이스)** 탭을 클릭합니다.
- 단계 3 해당 디바이스 탭을 선택합니다.
- 단계 4 충돌 탐지를 활성화할 디바이스를 선택합니다.
- 단계 5 디바이스 테이블 오른쪽에 있는 충돌 감지 상자의 목록에서 **Enabled(활성화됨)**을 선택합니다.



## 디바이스에서 대역외 변경 사항 자동 수락

변경 사항 자동 수락을 활성화하여 매니지드 디바이스에 대한 직접 변경 사항을 자동으로 수락하도록 CDO(Cisco Defense Orchestrator)를 구성할 수 있습니다. CDO를 사용하지 않고 디바이스에 직접 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경은 CDO에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

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

CDO에서 아직 디바이스에 구축되지 않은 구성 변경 사항이 있는 경우 CDO는 구성 변경을 자동으로 수락하지 않습니다. 화면의 프롬프트에 따라 다음 작업을 결정합니다.

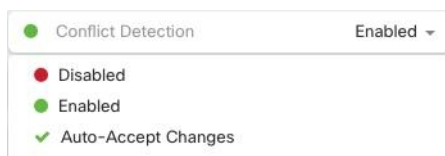
자동 수락 변경 사항을 사용하려면 먼저 테넌트가 **Inventory**(재고 목록) 페이지의 **Conflict Detection**(충돌 탐지) 메뉴에서 **auto-accept**(자동 수락) 옵션을 표시하도록 활성화합니다. 그런 다음 개별 디바이스에 대한 변경 사항 자동 수락을 활성화합니다.

CDO가 대역 외 변경 사항을 탐지하지만 수동으로 수락하거나 거부할 수 있는 옵션을 제공하도록 하려면 대신 **충돌 탐지**, [on page 629](#)를 활성화합니다.

## 변경 사항 자동 수락 구성

### Procedure

- 단계 1 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.
- 단계 2 CDO 메뉴에서 **Settings**(설정) > **General Settings**(일반 설정)를 탐색합니다.
- 단계 3 **Tenant Settings**(테넌트 설정) 영역에서, 토글을 클릭하여 "디바이스 변경 사항을 자동으로 수락하는 옵션 활성화"로 전환합니다. 이렇게 하면 변경 사항 자동 수락 메뉴 옵션이 **Inventory**(인벤토리) 페이지의 충돌 감지 메뉴에 표시됩니다.
- 단계 4 **Inventory**(인벤토리) 페이지를 열고 대역 외 변경을 자동으로 수락할 디바이스를 선택합니다.
- 단계 5 **Conflict Detection**(충돌 감지) 메뉴의 드롭다운 메뉴에서 **Auto-Accept Changes**(변경 사항 자동 수락)을 선택합니다.



## 테넌트의 모든 디바이스에 대한 변경 사항 자동 수락 비활성화

### Procedure

단계 1 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 2 CDO 메뉴에서 **Settings**(설정) > **General Settings**(일반 설정)를 탐색합니다.

단계 3 **Tenant Settings**(테넌트 설정) 영역에서 회색 X가 표시되도록 토글을 왼쪽으로 밀어 "디바이스 변경 사항을 자동으로 수락하는 옵션 활성화"를 비활성화합니다. 이렇게 하면 충돌 감지 메뉴에서 변경 사항 자동 수락 옵션이 비활성화되고 테넌트의 모든 디바이스에 대한 기능이 비활성화 됩니다.

**Note** "자동 수락"을 비활성화하면 CDO에 수락하기 전에 각 디바이스 충돌을 검토해야 합니다. 여기에는 이전에 변경 사항을 자동으로 수락하도록 구성된 디바이스가 포함됩니다.

## 구성 충돌 해결

이 섹션에서는 디바이스에서 발생하는 구성 충돌을 해결하는 방법에 대한 정보를 제공합니다.

### "동기화되지 않음" 상태 해결

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

### Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.

단계 5 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- **미리보기 및 배포...** - CDO에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 한 번에 여러 변경 사항을 기다렸다가 배포하십시오.
- **변경 사항 취소** - CDO에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 CDO에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 CDO에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

## "충돌 탐지됨" 상태 해결

CDO를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. [충돌 탐지, on page 629](#)이 활성화되어 있고 CDO를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected**(충돌 탐지됨)로 표시됩니다.

"충돌 탐지됨" 상태를 해결하려면 다음 절차를 수행합니다.

### Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict**(충돌 검토)를 클릭합니다.

단계 5 **Device Sync**(디바이스 동기화) 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.

- "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 CDO에 저장된 디바이스 구성입니다.
- "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.

단계 6 다음 중 하나를 선택하여 충돌을 해결합니다.

- **Accept Device changes**(디바이스 변경 사항 수락): 구성 및 CDO에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.

**Note** CDO는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 배포하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review**(검토 없이 수락)를 선택하는 것입니다.

- **Reject Device Changes**(디바이스 변경 거부): 디바이스에 저장된 구성을 CDO에 저장된 구성으로 덮어씁니다.

**Note** 거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

## 디바이스 변경 사항에 대한 폴링 예약

[충돌 탐지, on page 629](#)를 활성화했거나 **Settings**(설정) 페이지에서 **Enable device changes to auto-accept device changes**(디바이스 변경 자동 수락 옵션 활성화)를 선택한 경우 CDO는 기본 간격 동안 디바이스를 폴링하여 CDO 외부에서 디바이스의 구성이 변경되었는지 확인합니다. CDO가 디바이스별로 변경 사항을 폴링하는 빈도를 맞춤화할 수 있습니다. 이러한 변경 사항은 둘 이상의 디바이스에 적용할 수 있습니다.

디바이스에 대해 구성된 선택 항목이 없으면 "테넌트 기본값"에 대한 간격이 자동으로 구성됩니다.

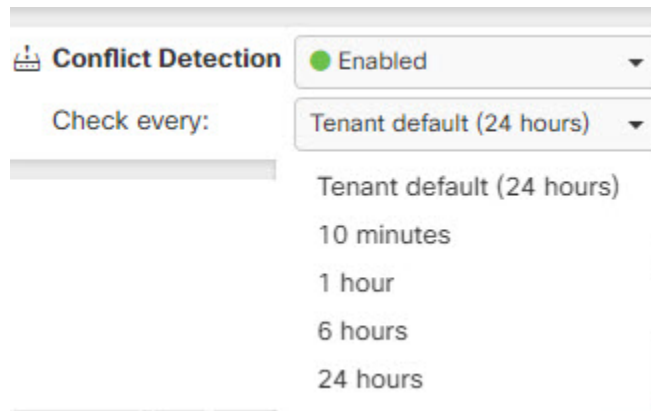


**Note** **Devices & Services**(디바이스 및 서비스) 페이지에서 디바이스별 간격을 맞춤 설정하면 **General Settings**(일반 설정) 페이지에서 **기본 충돌 탐지 간격**로 선택한 폴링 간격이 재정의됩니다.

**Devices & Services**(디바이스 및 서비스) 페이지에서 **Conflict Detection**(충돌 탐지)을 활성화하거나 **Settings**(설정) 페이지에서 디바이스 변경 사항을 자동 수락하는 옵션을 활성화한 후 다음 절차를 사용하여 CDO가 디바이스를 폴링할 빈도를 예약합니다.

### Procedure

- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 충돌 탐지를 활성화할 디바이스를 선택합니다.
- 단계 5 **Conflict Detection**(충돌 탐지)과 동일한 영역에서 **Check every**(확인 간격)의 드롭다운 메뉴를 클릭하고 원하는 폴링 간격을 선택합니다.



## 보안 데이터베이스 업데이트 예약

이 섹션에서는 디바이스에서 보안 데이터베이스 업데이트를 예약하는 방법에 대한 정보를 제공합니다.


### 예약된 보안 데이터베이스 업데이트 생성

FTD 디바이스에 대한 보안 데이터베이스를 확인하고 업데이트하는 예약된 작업을 생성하려면 다음 절차를 수행합니다.

## Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 디바이스 선택
- 단계 5 **Actions**(작업) 창에서 **Security Database Updates**(보안 데이터베이스 업데이트) 섹션을 찾아 추가 + 버튼을 클릭합니다.

### Note

선택한 디바이스에 대해 기존에 예약된 작업이 있는 경우 편집 아이콘  을 클릭하여 새 작업을 생성합니다. 새 작업을 생성하면 기존 작업을 덮어씁니다.

- 단계 6 다음을 사용하여 예약된 작업을 구성합니다.
- 빈도. 업데이트를 매일, 매주 또는 매월 수행하도록 선택합니다.
  - 시간. 시간을 선택합니다. 표시되는 시간은 UTC입니다.
  - 요일 선택. 업데이트를 수행할 요일을 선택합니다.


- 단계 7 **Save**(저장)를 클릭합니다.

디바이스의 구성 상태가 "데이터베이스 업데이트 중"으로 변경됩니다.

## 예약된 보안 데이터베이스 업데이트 편집

FTD 디바이스에 대한 보안 데이터베이스를 확인하고 업데이트하기 위해 기존의 예약된 작업을 편집하려면 다음 절차를 따르십시오.

## Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 디바이스 선택
- 단계 5 **Actions**(작업) 창에서 보안 데이터베이스 업데이트 섹션을 찾고 편집 아이콘  를 클릭합니다.
- 단계 6 다음을 사용하여 예약된 작업을 편집합니다.
- 빈도. 업데이트를 매일, 매주 또는 매월 수행하도록 선택합니다.
  - 시간. 시간을 선택합니다. 표시되는 시간은 UTC입니다.
  - 요일 선택. 업데이트를 수행할 요일을 선택합니다.



단계 7 **Save**(저장)를 클릭합니다.

단계 8 디바이스의 구성 상태가 "데이터베이스 업데이트 중"으로 변경됩니다.

## FDM-관리 디바이스 보안 데이터베이스 업데이트

FDM 관리 디바이스에서 보안 데이터베이스를 업데이트하면 SRU(침입 규칙), SI(보안 인텔리전스), VDB(취약성 데이터베이스) 및 지리위치 데이터베이스가 업데이트됩니다. Cisco Defense Orchestrator UI를 통해 보안 데이터베이스를 업데이트하도록 선택하는 경우 언급된 모든 데이터베이스가 업데이트됩니다. 업데이트할 데이터베이스는 선택할 수 없습니다.

보안 데이터베이스 업데이트는 되돌릴 수 없습니다.



**Note** 보안 데이터베이스를 업데이트할 때 일부 패킷이 삭제되거나 검사되지 않은 상태로 통과될 수 있습니다. 유지 보수 기간에 보안 데이터베이스 업데이트를 예약하는 것이 좋습니다.

### 온보딩 중 FDM-관리 디바이스 보안 데이터베이스 업데이트

FDM 관리 디바이스를 CDO에 온보딩할 때 온보딩 프로세스의 일부를 통해 데이터베이스에 대해 예약된 반복 업데이트를 활성화할 수 있습니다. 이 옵션은 기본적으로 선택되어 있습니다. 활성화되면 CDO는 보안 업데이트를 즉시 확인하고 적용할 뿐 아니라 디바이스에서 추가 업데이트를 확인하도록 자동으로 예약합니다. 디바이스가 온보딩된 후 예약된 작업의 날짜 및 시간을 수정할 수 있습니다.

보안 데이터베이스 업데이트를 정기적으로 확인하고 적용하려면 온보딩 프로세스 중에 자동 스케줄러를 활성화하는 것이 좋습니다. 이렇게 하면 디바이스가 항상 최신 상태로 유지됩니다. FDM 관리 디바이스를 온보딩하는 동안 보안 데이터베이스를 업데이트하려면, [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.



**Note** 등록 키 방법을 사용하여 디바이스를 온보딩하는 경우 디바이스를 스마트 라이선스로 등록해서는 안 됩니다. 라이선스를 등록하는 것이 좋습니다. 다른 방법으로, 디바이스의 [사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩](#)를 사용하여 디바이스를 온보딩할 수 있습니다.

### 온보딩 후 FDM-관리 디바이스 보안 데이터베이스 업데이트

FDM 관리 디바이스가 CDO에 온보딩된 후 업데이트를 예약하여 보안 데이터베이스 업데이트를 확인하도록 디바이스를 구성할 수 있습니다. 업데이트가 예약된 디바이스를 선택하여 언제든지 이 예약된 작업을 수정할 수 있습니다. 자세한 내용은 [보안 데이터베이스 업데이트 예약](#)을 참조하십시오.

## 워크플로우

### 디바이스 라이선스

라이선스가 없는 경우 Cisco Defense Orchestrator는 보안 데이터베이스를 업데이트할 수 없습니다. FDM 관리 디바이스에 최소 라이선스가 있는 것이 좋습니다.

라이선스가 없는 디바이스를 온보딩하는 경우 CDO가 디바이스를 온보딩하는 것을 금지하지 않습니다. 대신 디바이스에 "라이선스 부족"이라는 연결 상태가 표시됩니다. 이 문제를 해결하려면 FDM 관리 디바이스 UI를 통해 올바른 라이선스를 적용해야 합니다.



**Note** FDM 관리 디바이스를 온보딩하고 향후 보안 데이터베이스 업데이트를 예약하도록 옵트인하고 디바이스에 등록된 라이선스가 없는 경우 CDO는 여전히 예약된 작업을 생성하지만 적절한 라이선스가 적용되고 디바이스가 성공적으로 동기화될 때까지 작업을 트리거하지 않습니다.

보안 데이터베이스 업데이트가 **FDM**에서 보류 중입니다

FDM 관리 디바이스 UI를 통해 보안 데이터베이스를 업데이트하고 디바이스에서 **conflict detection**(충돌 감지)를 활성화한 경우 CDO는 보류 중인 업데이트를 충돌로 감지합니다.



**Note** FDM 관리 디바이스를 온보딩하고 업데이트 일정을 선택하면, CDO는 보안 데이터베이스와 다음 배포 중에 저장된 구성에 대한 기타 보류 중인 변경 사항을 자동으로 업데이트합니다. 구성 배포 일 필요는 없습니다.

디바이스에 보안 데이터베이스 업데이트 중에 **OOB** 변경 또는 단계적 변경이 있습니다

OOB(대역 외) 변경 또는 배포되지 않은 단계적 변경이 있는 FDM 관리 디바이스에 대한 보안 데이터베이스 업데이트를 예약하는 경우 CDO는 보안 데이터베이스만 확인하고 업데이트합니다. CDO는 OOB 또는 단계적 변경 사항을 배포하지 않습니다.

디바이스에 이미 보안 데이터베이스를 업데이트하도록 예약된 작업이 있습니다.

각 디바이스에는 예약된 작업이 하나만 있을 수 있습니다. 디바이스에 보안 데이터베이스를 업데이트하는 예약된 작업이 이미 있는 경우 새 데이터베이스를 생성하면 이를 덮어씁니다. 이는 CDO 또는 FDM 관리 디바이스에서 생성된 작업에 적용됩니다.

사용 가능한 보안 데이터베이스 업데이트가 없습니다.

사용 가능한 업데이트가 없는 경우 CDO는 디바이스에 아무 것도 배포하지 않습니다.

**FDM** 관리 고가용성(HA) 쌍에 대한 보안 데이터베이스 업데이트

보안 데이터베이스 업데이트는 HA 쌍의 기본 디바이스에만 적용됩니다.

**관련 정보:**

- 등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩
- 사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩, on page 184
- 보안 데이터베이스 업데이트 예약





## CHAPTER 4

# 모니터링 및 보고

CDO의 모니터링 및 보고 기능은 기존 정책 및 그로 인한 보안 태세의 영향에 대한 유용한 정보를 제공합니다.

- 변경 로그, on page 639
- FDM-관리 디바이스에 구축한 후 로그 항목 변경, on page 641
- FDM-관리 디바이스에서 변경 사항을 읽은 후 로그 항목 변경, on page 641
- 변경 로그 차이 보기, on page 642
- 변경 로그를 CSV 파일로 내보내기, on page 643
- 변경 요청 관리, on page 644
- FDM-관리 디바이스 개요 보고서, on page 648
- 작업 페이지, on page 650
- 워크플로우 페이지, 652 페이지

## 변경 로그

### 변경 로그 정보

변경 로그는 CDO에서 수행되는 구성 변경 사항을 지속적으로 캡처합니다. 이 단일 보기에는 지원되는 모든 디바이스 및 서비스에 대한 변경 사항이 포함됩니다. 다음은 변경 로그의 몇 가지 기능입니다.

- 디바이스 구성에 대한 변경 사항을 나란히 비교합니다.
- 모든 변경 로그 항목에 대한 일반 영어 레이블입니다.
- 디바이스의 온보딩 및 제거를 기록합니다.
- CDO 외부에서 발생하는 정책 변경 충돌 탐지.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.
- 전체 변경 로그 또는 일부만 CSV 파일로 다운로드할 수 있습니다.

### 로그 용량 변경

CDO는 1년 동안 변경 로그에 정보를 보관합니다. 1년이 지난 정보는 삭제됩니다.

CDO가 데이터베이스에 저장하는 변경 로그 정보와 변경 로그를 내보낼 때 표시되는 정보는 다릅니다. 자세한 내용은 [변경 로그를 CSV 파일로 내보내기](#), on page 643를 참조하십시오.

### 변경 로그 페이지의 변경 로그 항목

변경 로그 항목은 단일 디바이스 구성의 변경 사항, 디바이스에서 수행된 작업 또는 CDO 외부에서 디바이스가 변경된 경우를 반영합니다.

- 구성에 대한 변경 사항이 포함된 변경 로그 항목의 경우, 행의 아무 곳이나 클릭하여 변경 사항을 확장할 수 있습니다.
- 충돌로 탐지된 CDO 외부의 대역 외 변경 사항의 경우, 시스템 사용자는 마지막 사용자로 보고됩니다.
- CDO의 디바이스 구성이 디바이스의 구성과 동기화된 후 또는 디바이스가 CDO에서 제거되면 CDO는 변경 로그 항목을 닫습니다. 디바이스에서 CDO로 구성을 "읽은" 후 또는 CDO에서 디바이스로 구성을 배포하면 구성이 동기화됩니다.
- CDO는 기존 항목을 닫은 직후 새 변경 로그 항목을 생성합니다. 추가 구성 변경 사항이 열린 변경 로그 항목에 추가됩니다.
- 디바이스에 대한 읽기, 배포 및 삭제 작업에 대한 이벤트가 표시됩니다. 이러한 작업은 디바이스의 변경 로그를 닫습니다.
- CDO가 디바이스의 구성과 동기화되거나(읽기 또는 배포를 통해) CDO가 더 이상 디바이스를 관리하지 않는 경우 변경 로그가 닫힙니다.
- CDO 외부에서 디바이스가 변경되면 변경 로그에 "충돌 탐지됨" 항목이 기록됩니다.

### 활성 및 완료된 변경 로그 항목

변경 로그는 활성 또는 완료 상태입니다. CDO를 사용하여 디바이스의 구성을 변경하면 해당 변경 사항이 활성 변경 로그 항목에 기록됩니다. 디바이스에서 CDO로 구성을 읽고, CDO에서 디바이스로 변경 사항을 배포하거나, CDO에서 디바이스를 삭제하거나, 실행 중인 구성 파일을 업데이트하는 CLI 명령을 실행하면 활성 변경 로그가 완성되고 향후 변경을 위해 새 로그가 생성됩니다.

### 변경 로그에서 항목 찾기

변경 로그 이벤트는 검색 및 필터링이 가능합니다. 검색 창을 사용하여 키워드와 일치하는 이벤트를 찾습니다. 필터 ▼를 사용하여 지정한 모든 기준을 충족하는 항목을 찾습니다. 변경 로그를 필터링하고 검색 필드에 키워드를 추가하여 필터링된 결과 내에서 항목을 찾는 방식으로 작업을 결합할 수도 있습니다.

## FDM-관리 디바이스에 구축한 후 로그 항목 변경

FDM 관리 디바이스에 대한 변경 로그 항목의 변경 사항은 일반 영어로 요약됩니다. 변경 로그 항목에서 변경 사항을 클릭하면 변경된 내용을 정확하게 확인할 수 있습니다. CDO에서 FDM 관리 디바이스로 변경 사항을 기록한 후, 변경 로그 항목이 완료되고 Defense Orchestrator가 향후 변경 사항에 대한 새 항목을 생성합니다. 변경 로그 항목 행에서 파란색 [변경 로그 차이 보기](#) 링크를 클릭하면 실행 중인 구성 파일의 컨텍스트에서 변경 사항을 나란히 비교하여 표시합니다.

빨간색 변경 사항은 삭제, 파란색 변경 사항은 수정 사항, 녹색 변경 사항은 디바이스 구성에 대한 추가 사항, 회색 변경 사항은 메시지입니다.

아래 그림에서 추가된 **HR\_network**에 대한 확장된 변경 사항을 확인합니다. 이는 네트워크 개체 HR\_network의 추가입니다. 변경 전에 디바이스에 HR\_network 개체가 없었기 때문에 배포된 버전 열이 비어 있습니다. Pending Version(보류 중인 버전) 열은 HR\_network 개체가 10.10.11.0/24 값으로 생성되었음을 보여줍니다.

Last Updated	Device Name	Last Description	Last User	
Sep 11, 2018 4:01:17 PM	ftd		-	Diff
Sep 11, 2018 4:01:16 PM	ftd	Changes written successfully	admin@example.com	Diff

Sep 11, 2018	
4:01:16 PM	Changes written successfully
3:51:22 PM	Access Rules: Removed Block-rule
3:49:40 PM	Access Rules: Modified Deny engineering to reach HR_Network
3:48:53 PM	Objects: Added HR_network

DEPLOYED VERSION	PENDING VERSION
Objects	
#1 HR_network	name: HR_network contents: - sourceElement: 10.10.11.0/24 description: HR_network enabled: true

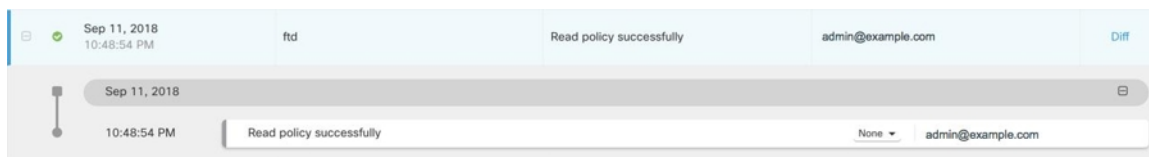
3:48:52 PM	Access Rules: Added Deny engineering to reach HR_Network
3:47:07 PM	Access Rules: Added Allow engineering to reach test-network

## FDM-관리 디바이스에서 변경 사항을 읽은 후 로그 항목 변경

CDO는 FDM 관리 디바이스에서 변경 사항을 감지하면, 디바이스에 대한 구성 상태 열의 **Inventory**(인벤토리) 페이지에 "충돌 감지됨" 상태를 등록합니다. 변경 로그에 해당 구성 상태를 기록하지 않습니다.

CDO 외부에서 이루어진 구성 변경 사항을 수락하면 CDO는 작업을 만들고 인터페이스의 오른쪽 하단 모서리에 작업 처리 상태를 표시합니다. 작업이 완료될 때까지 추가 작업을 수행하지 않는 것이 좋습니다. 그렇게 하면 변경 사항이 손실될 수 있습니다.

작업이 성공적으로 완료되면 변경 로그 항목에 대한 ["변경 로그 차이 보기"](#) 링크를 클릭합니다.



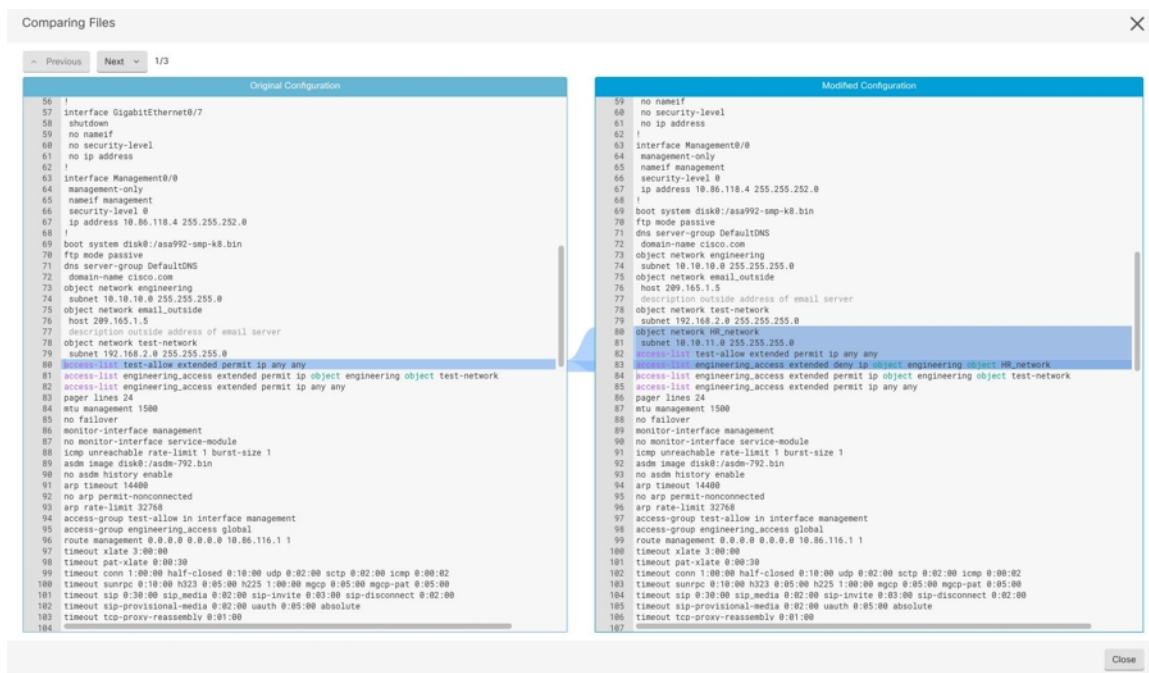
관련 정보:

- 변경 사항 읽기, 삭제, 확인 및 구축, on page 615

## 변경 로그 차이 보기

변경 로그에서 파란색 "Diff" 링크를 클릭하면 디바이스의 실행 중인 구성 파일에서 변경 사항을 나란히 비교할 수 있습니다. 두 버전의 차이점을 확인할 수 있습니다.

아래 그림에서 "Original Configuration(원본 구성)"은 변경 사항이 ASA에 기록되기 전에 실행 중인 구성 파일이며, "Modified Configuration(수정된 구성)" 열은 변경 사항이 기록된 후 실행 중인 구성 파일을 보여줍니다. 이 경우 Original Configuration(원본 구성) 열은 실행 중인 구성 파일에서 실제로 변경되지 않은 행을 강조 표시하지만 Modified Configuration(수정된 구성) 열에서 참조 지점을 제공합니다. 왼쪽에서 오른쪽 열로 이어지는 선을 따라가면 "engineering" 네트워크의 주소가 "HR\_network" 네트워크의 주소에 도달하지 못하도록 하는 HR\_network 개체 및 액세스 규칙이 추가된 것을 확인할 수 있습니다. **Previous(이전)** 및 **Next(다음)** 버튼을 사용하여 파일의 변경 사항을 클릭합니다.



관련 주제

- 변경 로그, on page 639



## 변경 로그를 CSV 파일로 내보내기


CDO 변경 로그 전체 또는 하위 집합을 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다.

변경 로그를 .csv 파일로 내보내려면 다음 절차를 수행합니다.


### Procedure

단계 1 탐색창에서 **Change Log**(변경 로그)를 클릭합니다.

단계 2 다음 작업 중 하나를 수행하여 내보낼 변경 사항을 찾습니다.

- 필터  필드 및 검색 필드를 사용하여 내보낼 항목을 정확하게 찾습니다. 예를 들어 디바이스를 기준으로 필터링하면 선택한 디바이스에 대한 변경 사항만 표시됩니다.
- 변경 로그에서 모든 필터 및 검색 기준을 지웁니다. 이렇게 하면 전체 변경 로그를 내보낼 수 있습니다.

**Note** CDO는 1년간의 변경 로그 데이터를 저장합니다. 최대 1년의 변경 로그 기록을 다운로드 하는 것보다 변경 로그 내용을 필터링하고 .csv 파일로 결과를 다운로드하는 것이 더 나을 수 있습니다.

단계 3 변경 로그  의 오른쪽 상단에 있는 파란색 내보내기 버튼을 클릭합니다.

단계 4 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다.

## CDO의 변경 로그 용량과 내보낸 변경 로그 크기의 차이

CDO의 변경 로그 페이지에서 내보내는 정보는 CDO가 데이터베이스에 저장하는 변경 로그 정보와 다릅니다.

모든 변경 로그에 대해 CDO는 디바이스 구성의 두 사본을 저장합니다. 하나는 "시작" 구성이고, 다른 하나는 닫힌 변경 로그의 경우 "종료" 구성 또는 열린 변경 로그의 경우 "현재" 구성입니다. 이를 통해 CDO는 구성 차이를 나란히 표시할 수 있습니다. 또한 CDO는 변경한 사용자 이름, 변경한 시간 및 기타 세부 정보와 함께 모든 단계 "변경 이벤트"를 추적하고 저장합니다.

그러나 변경 로그를 내보낼 때 구성의 전체 사본 2개가 내보내기에 포함되지 않습니다. 여기에는 내보내기 파일이 변경 로그 CDO가 저장하는 것보다 훨씬 작은 "변경 이벤트"만 포함됩니다.

CDO는 최대 1년의 변경 로그 정보를 저장하며 여기에는 두 개의 구성 사본이 포함됩니다.

## 변경 요청 관리

변경 요청 관리를 사용하면 서드파티 티켓팅 시스템에서 연 변경 요청 및 해당 비즈니스 근거를 변경 로그의 이벤트와 연결할 수 있습니다. CDO에서 변경 요청을 생성하고, 이를 고유한 이름으로 식별하고, 변경에 대한 설명을 입력하고, 변경 요청을 변경 로그 이벤트와 연결하려면 변경 요청 관리를 사용합니다. 나중에 변경 로그에서 변경 요청 이름을 검색할 수 있습니다.



**Note** CDO에서 변경 요청 추적에 대한 참조를 확인할 수도 있습니다. 변경 요청 추적 및 변경 요청 관리는 동일한 기능을 나타냅니다.

## 변화 요청 관리 활성화

변경 요청 추적을 활성화하면 테넌트의 모든 사용자에게 영향을 미칩니다. 변경 요청 추적을 활성화하려면 다음 절차를 따르십시오.

### Procedure

단계 1 사용자 메뉴에서 **Settings**(설정)를 선택합니다.

단계 2 사용자 메뉴에서 **General Settings**(일반 설정)를 클릭합니다.

단계 3 "변경 요청 추적" 아래의 슬라이더를 클릭합니다.

확인되면 Defense Orchestrator 인터페이스의 왼쪽 하단 모서리에 변경 요청 도구 모음이 나타나고 변경 로그의 변경 요청 드롭다운 메뉴가 나타납니다.

## 변경 요청 생성

### Procedure

단계 1 CDO 페이지에서 페이지 왼쪽 하단 모서리에 있는 변경 요청 도구 모음의 파란색 + 버튼을 클릭합니다.

단계 2 변경 요청에 이름과 설명을 지정합니다. 조직에서 구현하려는 변경 요청 식별자를 변경 요청 이름에 반영하십시오. 설명 필드를 사용하여 변경 목적을 설명하십시오.

**Note** 변경 요청을 생성한 후에는 변경 요청의 이름을 변경할 수 없습니다.

단계 3 변경 요청을 저장합니다.

**Note** CDO는 변경 요청을 비활성화하거나 변경 요청 도구 모음에서 변경 요청 정보를 지울 때 까지 모든 새 변경을 해당 변경 요청 이름과 연결하여 변경 요청을 저장합니다.

## 변경 요청을 변경 로그 이벤트와 연결

### Procedure

- 단계 1 탐색 창에서 **Change Log**(로그 변경)를 클릭합니다.
- 단계 2 변경 로그를 확장하여 변경 요청과 연결하려는 이벤트를 표시합니다.
- 단계 3 변경 요청 열에서 이벤트의 드롭다운 메뉴를 클릭합니다. 최신 변경 요청이 변경 요청 목록의 맨 위에 나열됩니다.
- 단계 4 변경 요청의 이름을 클릭하고 **Select**(선택)를 클릭합니다.

## 변경 요청으로 변경 로그 이벤트 검색

### Procedure

- 단계 1 탐색 창에서 **Change Log**(로그 변경)를 클릭합니다.
- 단계 2 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 정확한 이름을 입력합니다. CDO는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

## 변경 요청 검색

### Procedure

- 단계 1 변경 요청 도구 모음에서 변경 요청 메뉴를 클릭합니다.
- 단계 2 변경 요청 이름 또는 검색 중인 키워드 입력을 시작합니다. 변경 요청 목록의 이름 필드와 설명 필드 모두에서 부분 일치에 대한 결과가 표시되기 시작합니다.

## 변경 요청 필터링

필터 트레이에는 로그 변경 이벤트를 찾는 데 사용할 수 있는 변경 요청 필터가 있습니다.

### Procedure

- 단계 1 **Change Log**(로그 변경) 페이지 왼쪽의 필터 트레이에서 변경 요청 영역을 찾습니다.
- 단계 2 필터를 확장하고 검색 필드에 변경 요청 이름을 입력하기 시작합니다. 부분 일치 항목이 검색 필드 아래에 나타나기 시작합니다.
- 단계 3 변경 요청 이름을 선택하고 해당 확인란을 선택하면 변경 로그 테이블에 일치 항목이 나타납니다. CDO는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

## 변경 요청 툴바 지우기

변경 요청 도구 모음을 지우면 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않습니다.

### Procedure

- 단계 1 변경 요청 도구 모음에서 변경 요청 메뉴를 선택합니다.
- 단계 2 **Clear**(지우기)를 클릭합니다. 변경 요청 메뉴가 **None**(없음)으로 변경됩니다.

## 변경 로그 이벤트와 관련된 변경 요청 지우기

### Procedure

- 단계 1 탐색창에서 **Change Log**(변경 로그)를 클릭합니다.
- 단계 2 변경 로그를 확장하여 변경 요청에서 연결 해제하려는 이벤트를 표시합니다.
- 단계 3 변경 요청 열에서 이벤트의 드롭다운 메뉴를 클릭합니다.
- 단계 4 **Clear**(지우기)를 클릭합니다.

## 변경 요청 삭제

변경 요청을 삭제하면 변경 로그가 아닌 변경 요청 목록에서 삭제됩니다.

### Procedure

- 단계 1 변경 요청 도구 모음에서 변경 요청 메뉴를 클릭합니다.
- 단계 2 변경 요청 이름을 클릭합니다.
- 단계 3 해당 행에서 삭제 아이콘을 클릭합니다.

단계 4 녹색 확인 표시를 클릭하여 변경 요청 삭제를 확인합니다.

## 변화 요청 관리 비활성화

변경 요청 관리를 비활성화하면 계정의 모든 사용자에게 영향을 미칩니다. 변경 요청 관리를 비활성화하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 사용자 이름 메뉴에서 **Settings**(설정)를 선택합니다.
- 단계 2 변경 요청 추적 아래의 버튼을 밀어 회색 X를 표시합니다.

## 활용 사례

이러한 사용 사례는 이전에 위의 지침에 따라 변경 요청 관리를 활성화했다고 가정합니다.

외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 수행된 방화벽 변경 사항 추적

이 사용 사례에서 사용자는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽을 변경하고 있습니다. 사용자는 이러한 방화벽 변경으로 인한 변경 로그 이벤트를 변경 요청과 연결하려고 합니다. 이 절차에 따라 변경 요청을 생성하고 변경 로그 이벤트를 연결합니다.

1. **변경 요청 생성, on page 644.** 외부 시스템의 티켓 이름 또는 번호를 변경 요청 이름으로 사용합니다. 설명 필드를 사용하여 변경 또는 기타 관련 정보에 대한 근거를 추가합니다.
2. 변경 요청 도구 모음에 새 변경 요청이 표시되는지 확인합니다.
3. 방화벽을 변경하십시오.
4. 탐색 창에서 변경 로그를 클릭하고 새 변경 요청과 연결된 변경 로그 이벤트를 찾습니다.
5. 완료되면 **변경 요청 톨바 지우기, on page 646.**

방화벽을 변경한 후 개별 변경 로그 이벤트를 수동으로 업데이트합니다.

이 사용 사례에서 사용자는 외부 시스템에 유지 관리되는 티켓을 해결하기 위해 방화벽을 변경했지만 변경 요청 관리 기능을 사용하여 변경 요청을 변경 로그 이벤트와 연결하는 것을 잊었습니다. 사용자는 티켓 번호로 변경 로그 이벤트를 업데이트하기 위해 변경 로그로 돌아가려고 합니다. 변경 요청을 변경 로그 이벤트와 연결하려면 이 절차를 따르십시오.

1. **변경 요청 생성, on page 644.** 외부 시스템의 티켓 이름 또는 번호를 변경 요청 이름으로 사용합니다. 설명 필드를 사용하여 변경 또는 기타 관련 정보에 대한 근거를 추가합니다.
2. 탐색 창에서 **Change Log**(로그 변경)를 클릭하고 방화벽 변경 사항과 관련된 변경 로그 이벤트를 검색합니다.

3. [변경 요청을 변경 로그 이벤트와 연결, on page 645.](#)
4. 완료되면 변경 요청 도구 모음을 지웁니다.

#### 변경 요청과 관련된 변경 로그 이벤트 검색

이 사용 사례에서 사용자는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 수행한 작업의 결과로 변경 로그에 기록된 변경 로그 이벤트를 확인하려고 합니다. 변경 요청과 관련된 변경 로그 이벤트를 검색하려면 다음 절차를 따르십시오.

1. 탐색 창에서 **Change Log**(로그 변경)를 클릭합니다.
2. 다음 방법 중 하나를 사용하여 변경 요청과 관련된 변경 로그 이벤트를 검색합니다.
  - 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 정확한 이름을 입력합니다. CDO는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.
  - 변경 로그 이벤트를 찾기 위한 [변경 요청 필터링, on page 645](#)
3. 관련된 변경 요청을 보여주는 강조 표시된 변경 로그 이벤트를 찾으려면 각 변경 로그를 봅니다.

## FDM-관리 디바이스 개요 보고서

개요 보고서는 모든 FDM 관리 디바이스에 대한 운영 통계 모음을 제공합니다. 디바이스가 온보딩되면 Cisco Defense Orchestrator가 Firewall Device Manager에서 이 정보를 수집하는 데 최대 2시간이 걸릴 수 있습니다. 초기 보고서 생성 후 데이터는 1시간마다 컴파일됩니다. 보고서 정보는 이벤트 요청의 일부가 아니므로 이벤트와 보고서는 동일한 케이던스에서 사용할 수 없습니다.

네트워크 트래픽이 FDM 관리 디바이스에서 액세스 규칙 또는 정책을 트리거할 때 보고서의 데이터가 생성됩니다. 디바이스가 보고서에 반영되는 이벤트를 생성할 수 있도록 악성코드 방어 및 IPS 라이선스를 활성화하고 액세스 규칙에 대한 파일 로깅을 활성화하는 것이 좋습니다.

보고서에 표시되는 모든 정보는 페이지 상단에 있는 **Time Range**(시간 범위) 토글에 따라 달라집니다. 선택한 시간 범위 동안 정책에서 다양한 트래픽 또는 트리거가 발생할 수 있습니다.

개요 보고서에 문제가 발생하거나 예기치 않은 트래픽 양이 표시되는 경우 [총괄 요약 보고서 문제 해결, on page 763](#)에서 자세한 내용을 참조하십시오.

#### 네트워크 운영 데이터 생성

디바이스가 CDO에 온보딩되면 이벤트 데이터가 자동으로 수집됩니다. 수집되는 데이터는 디바이스 구성에 따라 달라집니다. 모든 FDM 관리 디바이스와 함께 제공되는 라이선스는 네트워크 운영 보고서 내의 모든 옵션을 지원하지 않습니다. 데이터를 수집하려는 디바이스에 대해 다음 구성을 권장합니다.

- **Logging**(로깅) - 해당 액세스 제어 규칙에서 파일 로깅을 활성화합니다. 자세한 내용은 [FDM-관리 액세스 제어 규칙의 로깅 설정](#)을 참조하십시오.
- **Malware Events**(악성코드 이벤트) - 악성코드 스마트 라이선스를 활성화합니다.

- **Security Intelligence**(보안 인텔리전스) - 스마트 라이선스를 활성화합니다.
- **IPS Threats**(IPS 위협) - 스마트 라이선스를 활성화합니다.
- **Web Categories**(웹 범주) - URL 스마트 라이선스를 활성화합니다.
- **Files Detected**(탐지된 파일) - 스마트 라이선스를 활성화합니다.

스마트 라이선스 및 이러한 라이선스가 제공하는 기능에 대한 자세한 내용은 [FDM-관리 디바이스 라이선싱 유형](#)을 참조하십시오.



**Note** 개요에는 VPN을 통해 발생하는 트래픽이 기본적으로 포함되지 않습니다.

### 개요

Overview(개요) 탭에는 트리거된 규칙, 위협 및 파일 유형의 시각적 개체가 표시됩니다. 이러한 항목은 숫자로 표시되며, 가장 큰 또는 가장 자주 적중되는 규칙, 이벤트 또는 파일이 먼저 나열됩니다.

악성코드 이벤트는 탐지되거나 차단된 악성코드 파일만 나타냅니다. 파일 상태는 변경될 수 있습니다(예: 정상에서 악성코드로 또는 악성코드에서 정상으로). 최신 침입 규칙(SRU)으로 디바이스를 최신 상태로 유지하려면 [보안 데이터베이스 업데이트 예약](#)하는 것이 좋습니다.

Top Ten Access Rule Hits(상위 10개 액세스 규칙 적중 횟수)에서는 세 가지 탭 간에 전환하여 패킷을 차단한 상위 10개 규칙 전송, 연결 또는 규칙을 볼 수 있습니다.

### 네트워크 평가

Network Assessment(네트워크 평가) 탭에서는 웹 사이트 범주 및 탐지된 파일 유형을 다룹니다. 이 표시는 가장 자주 발견되는 상위 10개 범주 및 파일 유형만 캡처합니다. 선택한 시간 범위 외에는 이 탭을 사용하여 특정 웹 범주 또는 파일 유형이 탐지된 시기를 확인할 수 없습니다.

### 위협

Threats(위협) 탭은 침입 이벤트에 의해 생성된 통계를 표시합니다. **Top Attacker**(상위 공격자)는 이벤트의 시작 IP 주소를 캡처하고, **Top Targets**(상위 대상)는 이벤트의 대상 IP 주소를 캡처하며, **Top Threats**(상위 위협)는 위협으로 분류된 이벤트 유형을 캡처합니다.

이 탭에는 탐지된 위협 및 악성코드 유형도 자세히 설명되어 있습니다.

### 보고서 생성

보고서를 원하는 대로 구성한 후에는 언제든지 보고서의 PDF를 생성할 수 있습니다. 자세한 내용은 [FDM-관리 디바이스 요약 보고서 생성](#)을 참조하십시오.

## FDM-관리 디바이스 요약 보고서 생성

CDO는 FDM 관리 디바이스를 통과하는 트래픽에 대한 보안 정책의 영향을 분석하는 데 사용할 수 있는 여러 보고서를 제공합니다. 개요 보고서에는 가장 영향력 있는 악성코드, 위협 및 영향을 받는

보안 인텔리전스가 요약되어 있습니다. CDO는 1시간마다 디바이스를 폴링하여 이벤트를 수집합니다. 전체 요약에서 제공하는 내용에 대해 자세히 알아보려면, [FDM-관리 디바이스 개요 보고서](#)에서 자세한 내용을 참조하십시오.



**Important** FDM 관리 디바이스 보고서는 현재 테넌트에 온보딩된 FDM 관리 디바이스에서만 사용할 수 있습니다. 이러한 보고서는 매시간 생성되며 이벤트 요청의 일부가 아니므로 이벤트와 보고서를 동일한 케이던스에서 사용할 수 없습니다. FDM 관리 디바이스를 처음 온보딩한 후 CDO에서 보고서를 생성하는 데 최대 2시간이 걸릴 수 있습니다. 표시할 보고서가 있을 때까지 **Monitoring**(모니터링) 옵션 아래의 **Reports**(보고서) 탭이 표시되지 않을 수 있습니다.


[Security Analytics and Logging\(SaaS\) 정보](#) 가입자인 경우 네트워크 보고서는 SEC(보안 이벤트 커넥터)로 전달된 이벤트를 반영하지 않습니다.



**Note** 트래픽 관련 보고서에 사용되는 데이터는 액세스 제어 규칙 및 기타 보안 정책에 의해 트리거된 이벤트에서 수집됩니다. 생성된 보고서는 로깅이 활성화되지 않은 규칙 또는 트리거되지 않은 규칙에 대한 트래픽을 반영하지 않습니다. 따라서 중요한 정보를 사용하여 규칙을 구성해야 합니다.

다음 절차를 사용하여 개요 보고서를 생성합니다.

### Procedure

- 단계 1 탐색창에서 **Monitoring**(모니터링) > **Executive Summary Report**(개요 보고서)를 클릭합니다.
- 단계 2 보고서의 시간 범위를 **Last 24 Hours**(지난 24시간), **Last 7 Days**(지난 7일), **Last 30 Days**(지난 30일) 또는 **Last 90 Days**(지난 90일) 중에서 선택합니다.
- 단계 3 (선택 사항) 필터 아이콘  을 클릭하여 사용자 지정 디바이스 목록에 대한 보고서를 생성합니다.
- 단계 4 **Generate Report (PDF)**(보고서 생성(PDF))를 클릭합니다.
- 단계 5 보고서를 PDF로 저장하려면 **Save**(저장)를 클릭합니다. 저장 위치를 찾아 **Save**(저장)를 클릭합니다. 보고서를 저장하지 않으려면 언제든지 **Cancel**(취소)를 클릭합니다.

관련 정보:

- [FDM-관리 디바이스 개요 보고서](#)
- [총괄 요약 보고서 문제 해결, on page 763](#)

## 작업 페이지

Jobs(작업) 페이지에는 벌크 작업의 상태에 대한 정보가 표시됩니다. 대량 작업은 여러 디바이스를 다시 연결하거나, 여러 디바이스에서 구성을 읽거나, 여러 디바이스를 동시에 업그레이드하는 것일 수 있습니다. 작업 테이블에서 색상으로 구분된 행은 성공하거나 실패한 개별 작업을 나타냅니다.

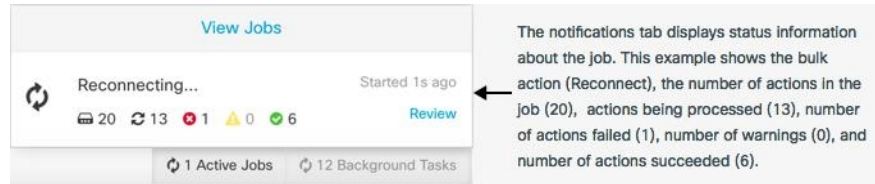


테이블의 한 행은 단일 대량 작업을 나타냅니다. 예를 들어 1개의 대량 작업이 20개의 디바이스를 다시 연결하려는 시도일 수 있습니다. Jobs(작업) 페이지에서 행을 확장하면 대량 작업의 영향을 받는 각 디바이스에 대한 결과가 표시됩니다.

ACTION	STATUS	USER	START	END
Reconnect Devices	0 1 0 19	user1@example.com	11/9/2017, 8:12:04 AM	11/9/2017, 8:12:10 AM
DEVICE	STATUS	START	END	
<b>Issues</b>				
ctx-70	Error	11/9/2017, 8:12:04 AM	11/9/2017, 8:12:05 AM	
<b>Active / Done</b>				
ctx-77	Done	11/9/2017, 8:12:04 AM	11/9/2017, 8:12:09 AM	
ctx-72	Done	11/9/2017, 8:12:04 AM	11/9/2017, 8:12:09 AM	

Jobs(작업) 페이지는 다음과 같은 세 가지 방법으로 액세스할 수 있습니다.

- 알림 탭에서 알림 행의 **Review**(검토) 링크를 클릭합니다. Jobs(작업) 페이지로 리디렉션되고 해당 알림이 나타내는 특정 작업이 표시됩니다.



- Notifications(알림) 탭 상단에서 "Viewjobs(작업 보기)" 링크를 클릭하면 Jobs(작업) 페이지로 이동합니다.
- CDO의 메뉴에서 **Monitoring**(모니터링) > **Jobs**(작업)를 선택합니다. 이 표에는 CDO에서 수행되는 대량 작업의 전체 목록이 나와 있습니다.

필터링 및 검색

Jobs(작업) 페이지에서 작업 유형, 해당 작업을 수행한 사용자 및 작업 상태별로 필터링하고 검색할 수 있습니다.

## 작업이 실패한 대량 작업 다시 시작

작업 페이지를 검토할 때 대량 작업에서 하나 이상의 작업이 실패한 경우 필요한 편집을 수행한 후 대량 작업을 다시 실행할 수 있습니다. CDO는 실패한 작업에 대해서만 작업을 다시 실행합니다. 대량 작업을 다시 실행하려면 다음을 실행합니다.

**Procedure**

- 단계 1 작업 페이지에서 실패한 작업을 나타내는 행을 선택합니다.
- 단계 2 다시 시작 아이콘을 클릭합니다.

## 대량 작업 취소

이제 여러 디바이스에서 수행한 활성화 대량 작업을 취소할 수 있습니다. 예를 들어 4개의 관리 디바이스를 다시 연결하려고 시도했는데 그 중 3개의 디바이스가 성공적으로 다시 연결되었지만 네 번째 디바이스는 다시 연결에 성공하거나 실패하지 않았습니다.

대량 작업을 취소하려면 다음을 수행합니다.

### Procedure

단계 1 CDO 탐색 메뉴에서 **Jobs**(작업)를 클릭합니다.

단계 2 아직 실행 중인 대량 작업을 찾아 작업 행 오른쪽에 있는 **Cancel**(취소) 링크를 클릭합니다.

대량 작업의 일부가 성공한 경우 해당 작업은 취소되지 않습니다. 아직 실행 중이던 모든 작업이 취소됩니다.

## 워크플로우 페이지

워크플로우 페이지에서는 디바이스, SDC(보안 디바이스 커넥터) 또는 SEC(보안 이벤트 커넥터)와 통신할 때와 디바이스에 규칙 세트 변경 사항을 적용할 때 CDO가 실행하는 모든 프로세스를 모니터링할 수 있습니다. CDO는 모든 단계에 대해 워크플로우 테이블에 항목을 만들고 이 페이지에 그 결과를 표시합니다. 이 항목에는 상호 작용하는 디바이스가 아니라 CDO가 수행하는 작업에만 관련된 정보가 포함되어 있습니다.

CDO는 디바이스에서 작업을 수행하지 못할 때 오류를 보고하며 자세한 내용은 오류가 발생한 단계를 보기 위해 워크플로우 페이지로 이동할 수 있습니다.

이 페이지를 방문하여 오류를 확인 및 해결하거나 TAC가 요구할 때 정보를 공유할 수 있습니다.

워크플로우 페이지로 이동하려면 **Inventory**(인벤토리) 페이지에서 디바이스 탭을 클릭합니다. 적절한 디바이스 유형 탭을 클릭하여 디바이스를 찾고 원하는 디바이스를 선택합니다. 오른쪽 창의 장치 및 작업에서 워크플로를 클릭합니다. 다음 그림은 워크플로우 테이블의 항목이 있는 워크플로우 페이지를 보여줍니다.

Name	Priority	Condition	Current State	Last Active	Time
ftdObjDetectionStateMachine	Scheduled	Done	Done	12/4/2020, 2:17:16 PM	14:17:00.381 / 14:17:16.640
ftdVpnSessionDetailsStateMachine	Scheduled	Done	Done	12/4/2020, 2:04:02 PM	14:04:00.278 / 14:04:02.481
ftdVpnSessionDetailsStateMachine	Scheduled	Done	Done	12/4/2020, 1:04:02 PM	13:04:00.433 / 13:04:02.747
ftdVpnSessionDetailsStateMachine	Scheduled	Done	Done	12/4/2020, 12:04:02 PM	12:04:00.307 / 12:04:02.507
ftdVpnSessionDetailsStateMachine	Scheduled	Done	Done	12/4/2020, 11:04:02 AM	11:04:00.205 / 11:04:02.290
ftdVpnSessionDetailsStateMachine	Scheduled	Done	Done	12/4/2020, 10:04:02 AM	10:04:00.312 / 10:04:02.541
ftdVpnSessionDetailsStateMachine	Scheduled	Error	Error	12/2/2020, 1:10:25 PM	13:04:00.291 / 13:10:25.140


  

ACTION	TIME	START STATE	END STATE	RESULT
FtdInitiateVpnSessionCheckAction	13:04:00.310 / 13:04:00.317	PENDING_GET_VPN_SESSION_DETAILS	INITIATE_GET_VPN_SESSION_DETAILS	SUCCESS
FtdInitiateGetBaseObjectsAction	13:04:00.335 / 13:04:00.372	INITIATE_GET_VPN_SESSION_DETAILS	WAIT_FOR_GET_VPN_SESSION_DETAILS	SUCCESS
FtdInitiateGetVpnSessionDetailsResponseHandler	13:10:25.116 / 13:10:25.132	AWAIT_RESPONSE_FROM_executedRequests	ERROR	FAILURE Error Message / Stack Trace

HOOK	TYPE	TIME	RESULT
DeviceStateMachineClearErrorBeforehook	Before	13:04:00.292 / 13:04:00.302	clearedErrors
AddDeviceNameToStateMachineDebugAfterhook	After	13:10:25.142 / 13:10:25.143	No debug record
DeviceStateMachineSetErrorAfterhook	After	13:10:25.143 / 13:10:25.157	setErrorOnDevice

### 워크플로우 정보 다운로드

전체 워크플로우 정보를 JSON 파일로 다운로드하고 TAC 팀에서 추가 분석을 요청할 때 제공할 수 있습니다. 이 정보를 다운로드하려면 디바이스를 선택하고 해당 워크플로우 페이지로 이동한 다음 오른쪽 상단 모서리에 나타나는 내보내기 버튼  를 클릭합니다.

### 스택 추적 생성

해결할 수 없는 오류가 있는 경우 TAC에서 스택 추적 사본을 요청할 수 있습니다. 오류에 대한 스택 추적을 수집하려면 **Stack Trace**(스택 추적) 링크를 클릭하고 **Copy Stacktrace**(스택 추적 복사)를 클릭하여 화면에 나타나는 스택을 클립보드로 복사합니다.





# 5 장

## Cisco Security Analytics and Logging

- Security Analytics and Logging(SaaS) 정보, 656 페이지
- FDM-관리 디바이스에 대한 보안 로깅 분석, 656 페이지
- FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현, on page 665
- Cisco Defense Orchestrator 이벤트 로깅에 FDM 이벤트 전송, on page 668
- FDM-관리 이벤트를 Cisco Cloud에 직접 전송, on page 668
- FDM-관리 이벤트 유형, on page 669
- 보안 이벤트 커넥터, 670 페이지
- 보안 이벤트 커넥터 설치, 671 페이지
- Cisco Security Analytics and Logging(SaaS) 프로비저닝, 690 페이지
- 보안 이벤트 커넥터 제거, 690 페이지
- Cisco Secure Cloud Analytics 포털 프로비저닝, on page 691
- Secure Cloud Analytics에서 센서 상태 및 CDO 통합 상태 검토, 693 페이지
- 전체 네트워크 분석 및 보고를 위한 **Cisco Secure Cloud Analytics** 센서 구축, on page 693
- CDO에서 Cisco Secure Cloud Analytics 알림 보기, on page 694
- Cisco Secure Cloud Analytics 및 동적 엔티티 모델링, on page 695
- 방화벽 이벤트 기반 알림 작업, on page 697
- 알림 우선순위 수정, 703 페이지
- 라이브 이벤트 보기, on page 704
- 이벤트 로깅 페이지의 열 표시 및 숨기기, on page 707
- 사용자 지정 가능한 이벤트 필터, on page 710
- Security Analytics and Logging의 이벤트 속성, on page 711
- 이벤트 로깅 페이지에서 이벤트 검색 및 필터링, 742 페이지
- 백그라운드 검색 다운로드, 752 페이지
- 데이터 스토리지 요금제, on page 752
- SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기, on page 755

## Security Analytics and Logging(SaaS) 정보

Cisco SAL(Security Analytics and Logging)을 사용하면 모든 FDM 관리 디바이스에서 연결, 침입, 파일, 맬웨어 및 보안 인텔리전스 이벤트와 ASA에서 모든 syslog 이벤트 및 NSEL(Netflow Secure Event Logging) 이벤트를 캡처하고 CDO(Cisco Defense Orchestrator)의 한 곳에서 볼 수 있습니다. 이벤트는 Cisco 클라우드에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 이 페이지에서 이벤트를 필터링하고 검토하여 네트워크에서 트리거되는 보안 규칙을 명확하게 파악할 수 있습니다.

추가 라이선싱을 사용하면 이러한 이벤트를 캡처한 후 CDO에서 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다. Secure Cloud Analytics는 이벤트 및 네트워크 플로우 데이터에 대한 행동 분석을 수행하여 네트워크의 상태를 추적하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

용어 참고: 이 설명서에서는 Cisco Security Analytics and Logging을 Secure Cloud Analytics 포털(Software as a Service 제품)과 함께 사용하는 경우 이러한 통합을 Cisco Security Analytics and Logging(SaaS) 또는 SAL(SaaS)이라고 합니다.

## FDM-관리 디바이스에 대한 보안 로깅 분석

Cisco SaaS(Security Analytics and Logging)를 사용하면 모든 FDM 관리 디바이스에서 연결, 침입, 파일, 맬웨어 및 보안 인텔리전스 이벤트를 캡처하고, Cisco Defense Orchestrator의 한 곳에서 볼 수 있습니다.

이벤트는 Cisco Cloud에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 여기에서 이벤트를 필터링하고 검토하여 네트워크에서 어떤 보안 규칙이 트리거되고 있는지 명확하게 이해할 수 있습니다. **Logging and Troubleshooting**(기록 및 문제 해결) 패키지는 이러한 기능을 제공합니다.

**Logging Analytics and Detection**(로그 분석 및 탐지) 패키지(이전의 **Firewall Analytics and Logging**(방화벽 분석 및 로그) 패키지)를 통해 시스템은 Secure Cloud Analytics 동적 엔티티 모델링을 FDM 관리 디바이스 이벤트에 적용하고 동작 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 경고를 생성할 수 있습니다. **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 패키지를 보유한 경우, 시스템은 FDM 관리 디바이스 이벤트와 네트워크 트래픽 모두에 동적 엔티티 모델링을 적용하고, 관찰 및 경고를 생성합니다. Cisco Single Sign-On을 사용하여 CDO에서 사용자를 위해 프로비저닝된 Cisco Secure Cloud Analytics 포털로 교차 실행할 수 있습니다.

### FDM 이벤트가 CDO 이벤트 뷰어에 표시되는 방법

개별 규칙이 이벤트를 로깅하도록 구성되고 네트워크 트래픽이 규칙 기준과 일치하면 연결, 침입, 파일, 악성코드 및 보안 인텔리전스 이벤트가 생성됩니다. 이벤트가 Cisco cloud에 저장되면 CDO에서 볼 수 있습니다. 이벤트를 Cisco cloud로 보내도록 FDM 관리 디바이스를 구성하는 방법에는 두 가지가 있습니다.

- 모든 디바이스에서 여러 SEC(Secure Event Connector)를 설치하고 규칙에 의해 생성된 이벤트를 마치 시스템 로그 서버인 것처럼 SEC로 전송할 수 있습니다. 그런 다음 SEC는 Cisco Cloud에 이벤트를 전달합니다.
- FDM 관리 디바이스가 등록 키를 사용하도록 CDO에 온보딩된 경우, Secure Firewall device manager의 컨트롤을 사용하여 이벤트를 Cisco cloud로 직접 보낼 수 있습니다.

### 보안 이벤트 커넥터를 사용하여 Cisco Cloud로 이벤트를 전송하는 방법

**Logging and Troubleshooting**(기본 로그 및 문제 해결) 라이선스를 사용하여, Secure Firewall device manager 이벤트가 Cisco cloud에 도달하는 방법은 다음과 같습니다.

1. 사용자 이름과 암호를 사용하거나 등록 키를 사용하여 FDM 관리 디바이스를 CDO에 온보딩합니다.
2. 액세스 제어 규칙, 보안 인텔리전스 규칙 및 SSL 암호 해독 규칙과 같은 개별 규칙을 구성하여 마치 Syslog 서버인 것처럼 SEC 중 하나로 이벤트를 전달합니다. 액세스 제어 규칙에서 파일 및 악성코드 정책과 침입 정책을 활성화하고 해당 정책에 의해 생성된 이벤트를 SEC에 전달할 수도 있습니다.
3. 파일 이벤트에 대한 **System Settings**(시스템 설정) > **Logging**(기록)에서 파일/악성코드 로깅을 구성합니다.
4. 침입 이벤트에 대한 **System Settings**(시스템 설정) > **Logging**(기록)에서 침입 기록을 구성합니다.
5. SEC는 이벤트가 저장된 Cisco Cloud로 이벤트를 전달합니다.
6. CDO은 설정한 필터에 따라 이벤트 로그 페이지에 Cisco cloud의 이벤트가 표시됩니다.

**Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 사용하면 다음 작업도 수행됩니다.

1. Cisco Secure Cloud Analytics는 Cisco cloud에 저장된 Secure Firewall device manager 연결 이벤트에 분석을 적용합니다.
2. 생성된 관찰 및 경고는 CDO 포털과 연결된 Secure Cloud Analytics 포털에서 액세스할 수 있습니다.
3. CDO 포털에서 Secure Cloud Analytics 포털을 교차 실행하여 이러한 관찰 및 경고를 검토할 수 있습니다.

**Secure Firewall device manager**에서 **Cisco Cloud**로 이벤트가 직접 전송되는 방식

기본 로그 및 문제 해결 라이선스를 사용하면 다음과 같이 Secure Firewall device manager 이벤트가 Cisco cloud에 도달합니다.

1. 등록 토큰을 사용하여 FDM 관리 디바이스를 CDO에 온보딩합니다.
2. 액세스 제어 규칙, 보안 인텔리전스 규칙, SSL 암호 해독 규칙 등의 개별 규칙을 구성하여 이벤트를 로깅하지만 이벤트를 전송할 Syslog 서버는 지정하지 않습니다. 액세스 제어 규칙에서 파일 및 악성코드 정책과 침입 정책을 활성화하고 해당 정책에 의해 생성된 이벤트를 Cisco Cloud로 전달할 수도 있습니다.
3. 파일 및 악성코드 정책과 침입 정책이 연결 이벤트를 로깅하도록 액세스 제어 규칙에 구성된 경우 파일 이벤트 및 침입 이벤트가 Cisco Cloud로 전송됩니다.
4. Secure Firewall device manager에서 Cloud Logging을 활성화하면 다양한 규칙에 기록된 이벤트가 Cisco cloud로 전송됩니다.
5. CDO은 설정한 필터를 기반으로 Cisco cloud에서 이벤트를 가져와 이벤트 뷰어에 표시합니다.

**Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 사용하면 다음 작업도 수행됩니다.

1. Cisco Secure Cloud Analytics는 Cisco cloud에 저장된 Secure Firewall device manager 연결 이벤트에 분석을 적용합니다.
2. 생성된 관찰 및 경고는 CDO 포털과 연결된 Secure Cloud Analytics 포털에서 액세스할 수 있습니다.
3. CDO 포털에서 Secure Cloud Analytics 포털을 교차 실행하여 이러한 관찰 및 경고를 검토할 수 있습니다.

## 구성 비교

다음은 SEC를 통해 Cisco cloud로 이벤트를 보내는 것과 Cisco cloud로 직접 이벤트를 보내는 것 사이의 CDO 구성 차이점에 대한 요약입니다.

FDM-관리 디바이스 구성	SEC(보안 이벤트 커넥터)를 통해 이벤트를 전송하는 경우	이벤트를 <b>Cisco Cloud</b> 에 직접 전송하는 경우
FDM-관리 디바이스에 대한 CDO 온보딩 방법	자격 증명(사용자 이름 및 비밀번호) 등록 토큰	등록 토큰 일련 번호
버전 지원	버전 6.4+	등록 토큰 - 버전 6.5+ 일련 번호 - 버전 6.7+



FDM-관리 디바이스 구성	<b>SEC</b> (보안 이벤트 커넥터)를 통해 이벤트를 전송하는 경우	이벤트를 <b>Cisco Cloud</b> 에 직접 전송하는 경우
Cisco Security Analytics and Logging (SaaS) 라이선스	로깅 및 문제 해결 로깅 분석 및 탐지(선택 사항) 총 네트워크 분석 및 모니터링(선택 사항)	로깅 및 문제 해결 로깅 분석 및 탐지(선택 사항) 총 네트워크 분석 및 모니터링(선택 사항)
라이선스	라이선스  -침입 규칙, 파일 제어 규칙 또는 보안 인텔리전스 필터링에서 연결 이벤트를 수집하려는 경우.  맬웨어 -파일 제어 규칙에서 연결 이벤트를 수집하려는 경우.	라이선스  -침입 규칙, 파일 제어 규칙 또는 보안 인텔리전스 필터링에서 연결 이벤트를 수집하려는 경우.  맬웨어 -파일 제어 규칙에서 연결 이벤트를 수집하려는 경우.
보안 이벤트 커넥터	필수	해당 없음
데이터 압축*	이벤트가 압축됨*	이벤트가 압축되지 않음*
데이터 요금제	필수	필수



참고 데이터 서브스크립션 및 과거 월간 사용량은 사용하는 압축되지 않은 데이터의 양을 기준으로 합니다.

#### 솔루션의 구성 요소

Cisco SaaS(Security Analytics and Logging)는 이러한 구성 요소를 사용하여 CDO에 다음 이벤트를 전달합니다.

보안 디바이스 커넥터(**SDC**)- SDC는 CDO를 FDM 관리 디바이스에 연결합니다. FDM 관리 디바이스의 로그인 자격 증명은 SDC에 저장됩니다. 자세한 내용은 [SDC\(Secure Device Connector\)](#), 11 페이지를 참조하십시오.

보안 이벤트 커넥터(**SEC**)-SEC는 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco cloud로 전달하는 애플리케이션입니다. Cisco cloud에 있으면 CDO의 Event Logging 페이지에서 이벤트를 보거나 Cisco Secure Cloud Analytics로 분석할 수 있습니다. 테넌트와 연결된 SEC가 하나 이상 있을 수 있습니다. 환경에 따라 보안 디바이스 커넥터 또는 CDO 커넥터 VM에 보안 이벤트 커넥터를 설치합니다.

**Secure Firewall device manager**- FDM 관리 디바이스는 Cisco의 차세대 방화벽입니다. 네트워크 트래픽 및 액세스 제어에 대한 상태 저장 검사 외에도, FDM 관리 디바이스는 맬웨어 및 애플리케이션 계층 공격으로부터 보호, 통합 침입 방지 및 클라우드 제공 위협 인텔리전스와 같은 기능을 제공합니다.

**Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 Cisco SaaS(Security Analytics and Logging)는 Cisco Secure Cloud Analytics를 사용하여 CDO에 전달된 이벤트를 추가로 분석합니다.

**Cisco Secure Cloud Analytics-Secure Cloud Analytics**는 이벤트에 동적 엔터티 모델링을 적용하여 이 정보를 기반으로 탐지를 생성합니다. 이렇게 하면 네트워크에서 수집한 텔레메트리를 심층적으로 분석하여 추세를 식별하고 네트워크 트래픽의 이상 동작을 검사할 수 있습니다.

#### 라이선싱

이 솔루션을 구성하려면 다음 계정 및 라이선스가 필요합니다.

**Cisco Defense Orchestrator.** CDO 테넌트가 있어야 합니다.

**Secure Device Connector.** SDC에 대한 별도의 라이선스는 없습니다.

**Secure Event Connector.** SEC에 대한 별도의 라이선스는 없습니다.

**Secure Logging Analytics(SaaS). Logging and Troubleshooting** 라이선스를 구매해야 합니다. 이 패키지의 목표는 온보딩 FDM 관리 디바이스에서 파생된 실시간 및 기록 이벤트를 네트워크 운영 팀에 제공하여 네트워크의 트래픽 문제를 해결하고 분석하는 것입니다.

또한 **Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 구매하여 Cisco Secure Cloud Analytics를 적용할 수 있습니다. 이 패키지의 목표는 네트워크 운영 팀에 이벤트(및 Total Network Analytics 및 Monitoring 라이선스가 있는 네트워크 트래픽)에 대한 추가 통찰력을 제공하여 가능한 비정상적인 동작을 더 잘 식별하고 이에 대응하는 것입니다.

라이선스 이름	제공된 기능	사용 가능한 라이선스 기간	기능 사전 요건
로깅 및 문제 해결	CDO에서 라이브 피드 및 기록 보기로 이벤트 및 이벤트 세부 정보 보기	<ul style="list-style-type: none"> <li>• 1년</li> <li>• 3년</li> <li>• 5년</li> </ul>	<ul style="list-style-type: none"> <li>• CDO</li> <li>• 버전 6.4 이상을 실행하는 온프레미스 배포</li> <li>• 이벤트를 클라우드로 전달하기 위해 하나 이상의 SEC 배포</li> </ul>

라이선스 이름	제공된 기능	사용 가능한 라이선스 기간	기능 사전 요건
로깅 분석 및 탐지(이전 이름 방화벽 분석 및 모니터링)	<p>로깅 및 문제 해결 기능 추가:</p> <ul style="list-style-type: none"> <li>• FDM 관리 디바이스 이벤트에 동적 엔터티 모델링 및 동작 분석을 적용합니다</li> <li>• CDO 이벤트 뷰어에서 교차 실행하여 이벤트 데이터를 기반으로 Secure Cloud Analytics에서 알림을 엮습니다.</li> </ul>	<ul style="list-style-type: none"> <li>• 1년</li> <li>• 3년</li> <li>• 5년</li> </ul>	<ul style="list-style-type: none"> <li>• CDO</li> <li>• 버전 6.4 이상을 실행하는 온프레미스 배포.</li> <li>• 이벤트를 클라우드로 전달하기 위해 하나 이상의 SEC 배포.</li> <li>• 새로 프로비저닝된 또는 기존의 Secure Cloud Analytics 포털.</li> </ul>

라이선스 이름	제공된 기능	사용가능한라이선스기간	기능 사전 요건
총 네트워크 분석 및 모니터링	<p>로깅 분석 및 탐지, 추가:</p> <ul style="list-style-type: none"> <li>이벤트, 온프레미스 네트워크 트래픽 및 클라우드 기반 네트워크 트래픽에 동적 엔터티 모델링 및 동작 분석을 적용합니다.</li> <li>이벤트 데이터, Secure Cloud Analytics 센서에서 수집한 온프레미스 네트워크 트래픽 플로우 데이터, Secure Cloud Analytics로 전달된 클라우드 기반 네트워크 트래픽의 조합을 기반으로 Secure Cloud Analytics에서 경고를 열고, CDO 이벤트 뷰어에서 교차 실행합니다.</li> </ul>	<ul style="list-style-type: none"> <li>1년</li> <li>3년</li> <li>5년</li> </ul>	<ul style="list-style-type: none"> <li>CDO</li> <li>버전 6.4 이상을 실행하는 온프레미스 배포</li> <li>이벤트를 클라우드로 전달하기 위해 하나 이상의 SEC 배포</li> <li>네트워크 트래픽 플로우 데이터를 클라우드로 전달하기 위해 하나 이상의 Secure Cloud Analytics 센서 버전 4.1 이상을 배포하거나, 네트워크 트래픽 플로우 데이터를 Secure Cloud Analytics로 전달하기 위해 Secure Cloud Analytics를 클라우드 기반 배포와 통합합니다.</li> <li>새로 프로비저닝된 또는 기존의 Secure Cloud Analytics 포털.</li> </ul>

**FDM-관리 장치.** FDM 관리 디바이스를 실행하고 보안 이벤트를 생성하는 규칙을 생성하려면 다음 라이선스가 있어야 합니다.

라이선스	기간	부여된 기능
Essentials(이센셜)(자동 포함)	영구	<p>선택적 기간 라이선스가 적용되지 않는 모든 기능.</p> <p>이 토큰을 사용하여 등록된 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.</p>
	기간 기준	<p>침입 탐지 및 방지 - 침입 정책은 침입 및 익스플로잇의 트래픽을 분석하고, 선택적으로 문제가 되는 패킷을 삭제할 수 있습니다.</p> <p>파일 제어 - 파일 정책은 사용자가 특정 유형의 파일을 업로드(전송)하거나 다운로드(수신)하는 것을 탐지하고, 선택적으로 차단할 수 있습니다. 맬웨어 라이선스가 필요한 AMP for Firepower를 사용하면, 맬웨어가 포함된 파일을 검사하고 차단할 수 있습니다. 모든 유형의 파일 정책을 사용하려면 Threat(위협) 라이선스가 있어야 합니다.</p> <p>보안 인텔리전스 필터링 - 트래픽이 액세스 제어 규칙을 기준으로 분석 대상이 되기 전에 선택한 트래픽을 삭제합니다. 동적 피드를 사용하면 최신 인텔리전스를 기반으로 연결을 즉시 삭제할 수 있습니다.</p>

라이선스	기간	부여된 기능
맬웨어	기간 기준	악성코드를 확인하는 파일 정책으로서 Cisco AMP(Advanced Malware Protection)를 AMP for Firepower(네트워크 기반 Advanced Malware Protection) 및 Cisco Threat Grid와 함께 사용합니다.  파일 정책은 네트워크를 통해 전송된 파일에서 악성코드를 탐지하고 차단할 수 있습니다.

### 데이터 요금제

Cisco cloud가 온보딩 FDM 관리 디바이스에서 매일 수신하는 이벤트 수를 반영하는 데이터 스토리지 플랜을 구매해야 합니다. 수집 속도를 결정하는 가장 좋은 방법은 SaaS(Secure Logging Analytics)를 구매하기 전에 무료 평가관에 참여하는 것입니다. 이를 통해 이벤트 볼륨을 적절하게 예측할 수 있습니다. 또한 [Logging Volume Estimator Tool](#)을 사용할 수 있습니다.



**주의** 이벤트를 Cisco cloud로 직접 전송하거나 SEC를 통해 동시에 전송하도록 FDM 관리 디바이스를 구성할 수 있습니다. 이렇게 하면 동일한 이벤트가 두 번 "수집"되고 데이터 요금제에 대해 두 번 계산되지만 Cisco Cloud에는 한 번만 저장됩니다. 불필요한 요금이 발생하지 않도록 한 가지 방법 또는 다른 방법을 사용하여 Cisco Cloud에 이벤트를 전송해야 합니다.

데이터 요금제는 일별 볼륨 1GB 단위로 제공되며 1년, 3년 또는 5년 단위로 제공됩니다. 데이터 요금제에 대한 자세한 내용은 [Secure Logging Analytics\(SaaS\) 주문 가이드](#)를 참조하십시오.



**참고** Security Analytics and Logging 라이선스 및 데이터 요금제를 보유하고 있는 경우 나중에 다른 라이선스를 취득할 수 있으며, 이것만 있으면 다른 데이터 요금제를 구매할 필요가 없습니다. 네트워크 트래픽 처리량이 변경되어 다른 데이터 플랜을 취득하는 경우에는 다른 Security Analytics and Logging 라이선스를 구입하지 않아도 됩니다.

### 30일 무료 평가관

CDO에 로그인하고 분석 > 이벤트 로깅로 이동하여 30일 위험 부담 없는 평가관을 요청할 수 있습니다. 30일 평가관이 끝나면 [SaaS\(Secure Logging Analytics\) 주문 가이드](#)의 지침에 따라 CCW(Cisco Commerce Workspace)에서 서비스를 계속하기 위해 원하는 이벤트 데이터 볼륨을 주문할 수 있습니다.

### 다음 작업?

[FDM-관리 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현, 665 페이지](#)를 계속 진행합니다.

# FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현

## 시작하기 전에

- 다음에 대한 자세한 사항은 [FDM-관리 디바이스에 대한 보안 로깅 분석, on page 656](#)의 내용을 검토합니다.
  - Cisco Cloud로 이벤트를 전송하는 방법
  - 솔루션의 애플리케이션
  - 필요한 라이선스
  - 필요한 데이터 요금제
- 매니지드 서비스 제공자 또는 Cisco Defense Orchestrator 영업 담당자에게 문의했으며 CDO 테넌트가 있습니다.
- 테넌트는 CDO가 FDM 관리 디바이스와 연결하는 데 SDC(Secure Device Connector)를 사용하거나 사용하지 않을 수 있습니다. 디바이스 자격 증명을 사용하여 온보딩하는 FDM 관리 디바이스에 대해 테넌트에 SDC가 설치되어 있어야 하며, [SDC\(Secure Device Connector\)](#), 등록 키 또는 일련 번호를 사용하여 FDM 관리 디바이스를 온보딩하는 경우 SDC가 필요하지 않습니다.
- 테넌트에 대한 SDC를 설치한 경우 SDC 상태가 **Active(활성)**이고 최근 하트비트를 기록했는지 확인합니다.
- SDC를 설치하는 경우 다음 방법 중 하나를 사용하여 설치합니다.
  - CDO의 준비된 VM 이미지를 사용하여 SDC를 설치하려면 [CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축](#)을 사용합니다. 이는 SDC를 구축하는 가장 쉬운 방법입니다.
  - 자체 VM에 보안 디바이스 커넥터 구축을 사용합니다.
- 테넌트에 대해 [CDO 이미지를 사용하여 SEC 설치](#)할 수 있으며, 임의의 Firewall Device Manager에서 테넌트에 온보딩된 하나의 SEC로 이벤트를 전송할 수 있습니다.
- firewall device manager에서 Cisco 클라우드로 이벤트를 직접 전송하는 경우 관리 인터페이스의 포트 443에서 아웃바운드 액세스를 연 것입니다.
- 어카운트 사용자에 대한 [CDO에 로그인](#)했습니다.

**SaaS(Secure Logging Analytics)**를 구현하고 보안 이벤트 커넥터를 통해 **Cisco Cloud**로 이벤트를 전송하는 새로운 **CDO** 고객 워크플로우

1. **위협 방어 디바이스 온보딩** 관리자 사용자 이름 및 비밀번호 또는 등록 토큰을 사용하여 디바이스를 온보딩할 수 있습니다.

2. 시스템 로그 서버 개체.
3. 연결 이벤트를 기록하도록 **FDM-관리 액세스 제어 정책**을 구성합니다.
4. **Cisco Defense Orchestrator** 이벤트 로깅에 **FDM 이벤트 전송**하도록 FDM 관리 디바이스를 구성합니다.
5. 이벤트가 CDO에 표시되는지 확인합니다. 내비게이션 바에서 분석 > 이벤트 로깅을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
6. **Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 **Cisco Secure Cloud Analytics**에서 **이벤트 분석**을 계속 진행합니다.

**SaaS(Secure Logging Analytics)**를 구현하고 **Cisco Cloud**에 직접 이벤트를 전송하는 새로운 **CDO** 고객 워크플로우

1. **위협 방어 디바이스 온보딩** 등록 키만 사용할 수 있습니다.
2. 연결 이벤트를 기록하도록 **FDM-관리 액세스 제어 정책**을 구성합니다.
3. **FDM-관리 이벤트를 Cisco Cloud에 직접 전송**하도록 FDM 관리 디바이스를 구성합니다.
4. 이벤트가 CDO에 표시되는지 확인합니다. 내비게이션 바에서 분석 > 이벤트 로깅을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
5. **Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 **Cisco Secure Cloud Analytics**에서 **이벤트 분석**을 계속 진행합니다.

**SaaS(Secure Logging Analytics)**를 구현하고 보안 이벤트 커넥터를 통해 **Cisco Cloud**로 이벤트를 전송하는 기존 **CDO** 고객 워크플로우

1. **위협 방어 디바이스 온보딩** 관리자 사용자 이름 및 비밀번호 또는 등록 토큰을 사용하여 디바이스를 온보딩할 수 있습니다.
2. 시스템 로그 서버 개체.
3. 연결 이벤트를 기록하도록 **FDM-관리 액세스 제어 정책**을 구성합니다.
4. **Cisco Defense Orchestrator** 이벤트 로깅에 **FDM 이벤트 전송**.
5. 이벤트가 CDO에 표시되는지 확인합니다. 내비게이션 바에서 분석 > 이벤트 로깅을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
6. **Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 **Cisco Secure Cloud Analytics**에서 **이벤트 분석**을 계속 진행합니다.



**SaaS(Secure Logging Analytics)**를 구현하고 **Cisco Cloud**에 직접 이벤트를 전송하는 기존 **CDO** 고객 워크 플로우

1. 위협 방어 디바이스 온보딩 등록 키만 사용할 수 있습니다.
2. 연결 이벤트를 기록하도록 **FDM-관리 액세스 제어 정책**을 구성합니다.
3. **FDM-관리 이벤트를 Cisco Cloud에 직접 전송**하도록 FDM 관리 디바이스를 구성합니다.
4. 이벤트가 CDO에 표시되는지 확인합니다. 내비게이션 바에서 분석 > 이벤트 로깅을 선택합니다. 라이브 이벤트를 보려면 Live(라이브) 탭을 클릭합니다.
5. **Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 **Cisco Secure Cloud Analytics**에서 이벤트 분석을 계속 진행합니다.

**Cisco Secure Cloud Analytics**에서 이벤트 분석

**Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 이전 단계와 함께 다음을 수행합니다.

1. **Cisco Secure Cloud Analytics 포털 프로비저닝**, on page 691.
2. **Total Network and Monitoring** 라이선스를 구매한 경우 하나 이상의 Secure Cloud Analytics 센서를 내부 네트워크에 구축합니다. 전체 네트워크 분석 및 보고를 위한 **Cisco Secure Cloud Analytics 센서 구축**, on page 693의 내용을 참조하십시오.
3. Cisco SSO(Single Sign-On) 자격 증명에 연결된 Secure Cloud Analytics 사용자 어카운트를 생성하도록 사용자를 초대합니다. CDO에서 **Cisco Secure Cloud Analytics 알림 보기**, on page 694의 내용을 참조하십시오.
4. firewall device manager 이벤트에서 생성된 Secure Cloud Analytics 알림을 모니터링하려면 CDO에서 Secure Cloud Analytics를 교차 실행합니다. CDO에서 **Cisco Secure Cloud Analytics 알림 보기**, on page 694의 내용을 참조하십시오.

**CDO**에서 교차 실행하여 **Secure Cloud Analytics** 알림 검토

**Logging Analytics and Detection**(로깅 애널리틱스 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 애널리틱스 및 모니터링) 라이선스를 사용하면 CDO에서 Secure Cloud Analytics로 교차 실행하여 firewall device manager 이벤트를 기반으로 Secure Cloud Analytics에서 생성된 알림을 검토할 수 있습니다.

자세한 내용은 다음 문서를 참조하십시오.

- **CDO에 로그인**
- **CDO에서 Cisco Secure Cloud Analytics 알림 보기**, on page 694
- **Cisco Secure Cloud Analytics 및 동적 엔티티 모델링**, on page 695
- **방화벽 이벤트 기반 알림 작업**

**SaaS(Secure Analytics and Logging) 워크플로우**

보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결에서는 SaaS(Secure Logging Analytics)에서 생성된 이벤트를 사용하여 사용자가 네트워크 리소스에 액세스할 수 없는 이유를 확인하는 방법을 설명합니다.

방화벽 이벤트 기반 알림 작업도 참고합니다.

## Cisco Defense Orchestrator 이벤트 로깅에 FDM 이벤트 전송

이벤트 로깅 뷰어에서 액세스 제어 규칙, 보안 인텔리전스 규칙 및 SSL 암호 해독 규칙의 FDM 관리 이벤트를 보려면 먼저 해당 이벤트를 Cisco 클라우드로 전송해야 합니다.

- 액세스 제어 규칙. 네트워크 연결의 시작 또는 종료 시 **FDM-관리 이벤트 유형**을 로깅할 수 있습니다. 이 규칙 유형에 대한 로깅 구성에 대한 자세한 내용은 **FDM 액세스 제어 정책 구성 및 FDM-관리 액세스 제어 규칙의 로깅 설정**을 참조하십시오.
- 보안 인텔리전스 규칙. 보안 인텔리전스 규칙에 의해 생성된 **FDM-관리 이벤트 유형**을 로깅할 수 있습니다. 로깅을 활성화하면 차단 목록 항목과 일치하는 항목이 로깅됩니다. 로깅이 활성화된 상태에서 제외된 연결이 액세스 제어 규칙과 일치하는 경우에는 로그 메시지를 받더라도 예외 항목과 일치하는 항목은 로깅되지 않습니다. 로깅 구성에 대한 자세한 내용은 **Firepower 보안 인텔리전스 정책 구성**을 참조하십시오.
- SSL 암호 해독 규칙. SSL 암호 해독 규칙에 의해 생성된 **FDM-관리 이벤트 유형**을 로깅할 수 있습니다.

파일 및 악성코드 이벤트 또는 침입 이벤트를 Cisco Cloud로 전송하고 보안 이벤트 커넥터를 사용하는 경우 **기록 설정 구성**해야 합니다.

관련 정보:

- **SaaS(Secure Logging Analytics)를 위한 시스템 로그 서버 개체 생성**

## FDM-관리 이벤트를 Cisco Cloud에 직접 전송

Firewall Device Manager 버전 6.5부터는 연결 이벤트, 침입, 파일 및 악성코드 이벤트를 FDM 관리 디바이스에서 Cisco Cloud로 직접 전송할 수 있습니다. Cisco Cloud에 있으면 Cisco Defense Orchestrator(CDO)로 모니터링하고 Cisco Secure Cloud Analytis로 분석할 수 있습니다. 이 방법에서는 SDC(보안 디바이스 커넥터) 가상 머신에 SEC(보안 이벤트 커넥터) 컨테이너를 설치할 필요가 없습니다.

**Before you begin**

다음 항목을 검토합니다.

- **FDM-관리 디바이스에 대한 보안 로깅 분석, on page 656**
- **FDM-관리 디바이스에 대한 SaaS(Secure Logging Analytics) 구현**

## Procedure

- 단계 1 Cisco Cloud로 이벤트를 전송하려는 디바이스의 Firewall Device Manager에 로그인합니다.
- 단계 2 이렇게 하려면 **Device**(디바이스) > **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)를 선택합니다.
- 단계 3 Send Events to the Cisco Cloud(Cisco cloud로 이벤트 전송) 창에서 **Enable**(활성화)를 클릭합니다.

# FDM-관리 이벤트 유형

## 이벤트 유형

시스템은 다음 이벤트 유형을 생성할 수 있습니다. 모니터링 대시보드에서 관련된 통계를 확인하려면 이러한 이벤트를 생성해야 합니다.

### 데이터(진단) 이벤트

데이터 기록에서는 디바이스 및 시스템 상태, 네트워크 구성 관련 이벤트에 대한 **syslog** 메시지를 제공합니다. 이러한 이벤트는 연결과 관련이 없습니다. 개별 액세스 제어 규칙 내에서 연결 로깅을 구성합니다.

데이터 기록에서는 데이터 플레인에서 실행되는 기능, 즉 **show running-config** 명령으로 볼 수 있는 CLI 구성에 정의된 기능에 대해 메시지를 생성합니다. 여기에는 라우팅, VPN, 데이터 인터페이스, DHCP 서버, NAT 등과 같은 기능이 포함됩니다.

### 연결 이벤트

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 결정되지만, 일반적으로는 다음과 같습니다.

- 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 또는 연결과 관련된 사용자 등
- 연결이 로깅된 사유에 대한 메타데이터: 어떤 설정이 트래픽을 처리했는지, 연결이 허용 또는 차단되었는지, 암호화 및 해독된 연결에 대한 상세정보 등

### 침입 이벤트

시스템은 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성에 영향을 미칠 수 있는 악성 활동 탐지를 위해 네트워크를 통과하는 패킷을 검토합니다. 시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트를 생성합니다. 침입 이벤트는 호출하는 액세스 제어 규칙의 로깅 컨피그레이션과 관계없이 차단하거나 알리도록 설정된 모든 침입 규칙에 대해 생성됩니다.

### 파일 이벤트

파일 이벤트는 파일 정책을 기준으로 하여 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 파일을 나타냅니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다.

시스템이 파일 이벤트를 생성하는 경우 호출하는 액세스 제어 규칙의 로깅 컨피그레이션과 관계없이 시스템은 관련 연결의 종료도 로깅합니다.

### 악성코드 이벤트

시스템은 전체적인 액세스 제어 컨피그레이션의 일부로 네트워크 트래픽에서 악성코드를 탐지할 수 있습니다. AMP for Firepower는 결과 이벤트의 상태와 악성코드가 탐지된 방법, 위치, 시간에 대한 상황 데이터를 포함하는 악성코드 이벤트를 생성할 수 있습니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 활성화해야 합니다.

파일 상태는 변경될 수 있습니다(예: 정상에서 악성코드로 또는 악성코드에서 정상으로). AMP for Firepower가 AMP 클라우드에 파일에 대해 쿼리하고, 쿼리한지 일주일 이내에 상태가 변경되었음을 클라우드에서 확인하는 경우, 시스템에서는 회귀적 악성코드 이벤트를 생성합니다.

### 보안 인텔리전스 이벤트

보안 인텔리전스 이벤트는 정책에 따라 차단되거나 또는 모니터링된 각 연결의 보안 인텔리전스 정책에 의해 생성된 연결 이벤트 유형입니다. 모든 보안 인텔리전스 이벤트에는 내용이 채워진 Security Intelligence Category(보안 인텔리전스 카테고리) 필드가 있습니다.

이러한 각 이벤트에는 해당하는 "일반" 연결 이벤트가 있습니다. 보안 인텔리전스 정책은 액세스 제어를 비롯한 다른 많은 보안 정책보다 먼저 평가되기 때문에 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

## 보안 이벤트 커넥터

SEC(Secure Event Connector)는 보안 분석 및 로깅 SaaS 솔루션의 구성 요소입니다. ASA 및 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco Cloud에 전달합니다. CDO는 관리자가 해당 페이지에서 또는 Cisco Secure Cloud Analytics를 사용하여 이벤트를 분석할 수 있도록 Event Logging(이벤트 로깅) 페이지에 이벤트를 표시합니다.

SEC는 네트워크 또는 AWS Virtual Private Cloud(VPC)에 구축된 보안 디바이스 커넥터 또는 네트워크에 구축된 자체 CDO 커넥터 가상 머신에 설치됩니다.

### 보안 이벤트 커넥터 ID

Cisco TAC(Technical Assistance Center) 또는 기타 CDO 지원과 협력할 때는 SEC의 ID가 필요할 수 있습니다. 이 ID는 CDO의 Secure Connector(보안 커넥터) 페이지에 있습니다. SEC ID를 찾으려면 다음을 수행합니다.

1. 왼쪽의 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
2. 식별할 SEC를 클릭합니다.
3. SEC ID는 Details(세부 정보) 창의 Tenant ID(테넌트 ID) 위에 나열되는 ID입니다.

#### 관련 정보:

- [FDM-관리 디바이스에 대한 보안 로깅 분석](#)
- [SDC 가상 머신에 SEC\(Secure Event Connector\) 설치, 671 페이지](#)
- [VM 이미지를 사용하여 SEC 설치](#)
- [VM 이미지를 사용하여 SEC 설치](#)
- [Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치, 689 페이지](#)
- [보안 이벤트 커넥터 제거](#)
- [Cisco Security Analytics and Logging\(SaaS\) 프로비저닝](#)

## 보안 이벤트 커넥터 설치

SEC(보안 이벤트 커넥터)는 SDC가 있거나 없는 테넌트에 설치할 수 있습니다.

보안 디바이스 커넥터(있는 경우)와 동일한 가상 머신에 하나의 SEC를 설치할 수 있습니다. 또는 네트워크에서 유지 관리하는 자체 CDO 커넥터 가상 머신에 SEC를 설치할 수 있습니다.

다양한 설치 사례를 설명하는 다음 항목을 참조하십시오.

- [VM 이미지를 사용하여 SEC 설치, 680 페이지](#)
- [CDO 이미지를 사용하여 SEC 설치, 674 페이지](#)
- [Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치, 689 페이지](#)

## SDC 가상 머신에 SEC(Secure Event Connector) 설치

SEC(Secure Event Connector)는 ASA 및 FDM 관리 디바이스에서 이벤트를 수신하여 Cisco Cloud에 전달합니다. CDO는 관리자가 해당 페이지에서 또는 Cisco Secure Cloud Analytics를 사용하여 이벤트를 분석할 수 있도록 Event Logging(이벤트 로깅) 페이지에 이벤트를 표시합니다.

보안 디바이스 커넥터(있는 경우)와 동일한 가상 머신에 하나의 SEC를 설치할 수 있습니다. 또는 네트워크에서 유지 관리하는 자체 CDO 커넥터 가상 머신에 SEC를 설치할 수 있습니다.

이 문서에서는 SDC와 동일한 가상 머신에 SEC를 설치하는 방법을 설명합니다. 더 많은 SEC를 설치하려면 [CDO 이미지를 사용하여 SEC 설치, 674 페이지](#) 또는 [VM 이미지를 사용하여 SEC 설치, 680 페이지](#)의 내용을 참조하십시오.

시작하기 전에

- Cisco Security and Analytics 로깅, 로깅 및 트러블슈팅 라이선스를 구매합니다. 또는 Cisco Security and Analytics 로그아웃을 먼저 시도하려면 CDO에 로그인하고 기본 탐색 모음에서 분석 > 이벤트 로깅을 선택하고 **Request Trial**(평가판 요청)을 클릭합니다. 또한 **Logging Analytics and Detection**(로깅 분석 및 탐지) 및 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수 있습니다.
- SDC가 설치되었는지 확인합니다. SDC를 설치해야 하는 경우 다음 절차 중 하나를 수행합니다.
  - [CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축](#)
  - [자체 VM에 보안 디바이스 커넥터 구축](#)



참고 자체 VM에 온프레미스 SDC를 설치한 경우 이벤트가 SDC에 도달하도록 허용하려면 [생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성](#)이 필요합니다.

- SDC가 CDO와 통신하는지 확인합니다.
  1. CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
  2. SDC의 마지막 하트비트가 SEC 설치 전 10분 미만이었으며 SDC의 상태가 활성화인지 확인합니다.
- 시스템 요구 사항 - SDC를 실행하는 가상 머신에 추가 CPU 및 메모리를 할당합니다.
  - CPU: 총 6개의 CPU를 만들기 위해 SEC를 수용할 수 있도록 추가로 4개의 CPU를 할당합니다.
  - 메모리: 총 10GB의 메모리를 만들려면 SEC에 8GB의 메모리를 추가로 할당합니다.  
SEC를 수용하도록 VM의 CPU와 메모리를 업데이트한 후 VM의 전원을 켜고 Secure Connector(보안 커넥터) 페이지에 SDC가 "Active(활성)" 상태로 표시되는지 확인합니다.

프로시저

단계 1 CDO에 로그인합니다.

단계 2 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 3 파란색 더하기 버튼을 클릭하고 **Secure Event Connector**(보안 이벤트 커넥터)를 클릭합니다.

단계 4 마법사의 1단계를 건너뛰고 2단계로 이동합니다. 마법사 2단계에서 링크를 클릭하여 SEC 부트스트랩 데이터를 복사합니다

### Deploy an On-Premises Secure Event Connector

```
dRaU9pSmhNM1UxWTJVMFppMDNnakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0pq
YkdsbGJuUmZhV1FpT2lKaGNHa3RZMnhwW1c1ME1uMC5tZzh0bTZMZ1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYTZQYzVsRjRITT1teVVEVzh2Qk5FWW44c3V0Z3NTQUo0TH15N0xzVGsYdEx4N05nbs00STB6SmZ6
aWdQTkRiV1RsRW1tcjI5SkFVZ2NBWEhySkdzcktMREszUnJUM0hZU3JkZ21Hd1dGb3FwWUdZnkJHRU
VacmI0YVFLSjFTdnJ5RjVfZ2FqajZFZkNvaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBxVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTfsYmE3VksNOUp4bk9RS1pqaW
1rdDNsYnRRbDNrTHMxeWduaXdVU1RuWkQxM0c5T2FJWEcxQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEVOQU5UPSJDRE9fY2lzy28tYW1hbGxpbYIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ21uZy5kZXlYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lzy28tYW1hbGxpbY
IKT05MwV9FVkv0VE10Rz0idHJ1ZSIK
```

[Copy CDO Bootstrap Data](#)

#### Step 2

Read the [instructions](#) about deploying the Secure Event Connector on vSphere. Copy the bootstrap data below and paste it when prompted for "SEC bootstrap Data".

**⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM**

```
U1NFX0RFVklDRV9JRD0iZTBhZTJkNmMtMDdhYy00Y2JkLWEzNWQtOGYzZDJKMjI1ZmU3IqTU0VfRE
U0VfT1RQPSI5Y2IzNTI4ZWZlMzg0TQ2NjViMDFkZmEyYjUyMGUxNSIKVEVOQU5UX05BTUU9IKNET1
9jaXNjby1hbWFSbG1vIg==
```

[Copy SEC Bootstrap Data](#)

#### Step 3

Verify the connection status of the new SEC by exiting this dialog and checking the "Last Heartbeat" information.

Cancel

OK

다.

단계 5 터미널 창을 열고 SDC에 "cdo" 사용자로 로그인합니다.

단계 6 로그인한 후에는 "sdc" 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

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

단계 7 프롬프트에서 **sec.sh** 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 8 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9Uo0iUY8VHGHFXREWRTygfVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.

```

=====
Running SEC health check for tenant ██████████
-----
SEC cloud URL ██████████ is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the
=====

```

등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 [SEC 온보딩 실패 문제 해결](#)로 이동하십시오.

**단계 9** SDC 및 SEC가 실행 중인 VM에 추가 구성이 필요한지 확인합니다.

- 자체 가상 머신에 SDC를 설치한 경우 [생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 686 페이지](#)를 계속 진행합니다.
- CDO 이미지를 사용하여 SDC를 설치한 경우 "다음 작업"을 진행합니다.

다음에 수행할 작업

[FDM-관리 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현, 665 페이지](#)으로 돌아갑니다.

관련 정보:

- [보안 디바이스 커넥터 문제 해결, 774 페이지](#)
- [보안 이벤트 커넥터 문제 해결](#)
- [SEC 온보딩 실패 문제 해결](#)
- [보안 이벤트 커넥터 등록 실패 문제 해결, 782 페이지](#)

## CDO 이미지를 사용하여 SEC 설치

SEC(보안 이벤트 커넥터)는 ASA 및 FTD에서 Cisco cloud로 이벤트를 전달하므로 라이선스에 따라 Event Logging 페이지에서 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(보안 이벤트 커넥터)를 설치하고 ASAs 및 FDM 관리 디바이스의 이벤트를 설치한 SEC로 보낼 수 있습니다. 여러 SEC를 사용하면 서로 다른 위치에 SEC를 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 배포할 수 있습니다.



SEC 설치는 2단계로 진행됩니다.

1. [CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 675 페이지](#) 설치하는 모든 SEC에 대해 하나의 CDO 커넥터가 필요합니다. CDO 커넥터는 SDC(보안 디바이스 커넥터)와 다릅니다.
2. [CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 686 페이지](#).



참고 고유한 VM을 생성하여 CDO 커넥터를 생성하려면 [생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성](#)을 참조하십시오.

다음 작업:

[CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 675 페이지](#)를 계속 진행합니다.

## CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치

시작하기 전에

- Cisco Security and Analytics Logging, **Logging and Troubleshooting**(로깅 및 문제 해결) 라이선스를 구매하고, **Logging Analytics and Detection**(로깅 분석 및 탐지), **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수도 있습니다.
- 원하는 경우 CDO에 로그인하여 Security Analytics and Logging(보안 분석 및 로깅) 평가판을 요청하고 기본 내비게이션 바에서 분석 > 이벤트 로깅을 선택하고 **Request Trial**(평가판 요청)을 클릭합니다.
- CDO는 엄격한 인증서 확인이 필요하며 CDO 커넥터와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 CDO 커넥터와 CDO 간의 트래픽 검사를 비활성화합니다.
- 이 프로세스에서 설치된 **CDO** 커넥터는 **TCP 포트 443**에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.
- **매니지드 디바이스**에 [Cisco Defense Orchestrator 연결](#)를 검토하여 **CDO** 커넥터에 대한 적절한 네트워크 액세스를 확인합니다.
- CDO는 vSphere 웹 클라이언트 또는 ESXi 웹 클라이언트를 사용한 CDO 커넥터 VM OVF 이미지를 설치를 지원합니다.
- CDO는 VM vSphere 데스크톱 클라이언트를 사용한 CDO 커넥터 VM OVF 이미지 설치를 지원하지 않습니다.
- ESXi 5.1 하이퍼바이저.
- CDO 커넥터 및 SEC만 호스팅하는 VM의 시스템 요구 사항:

- VMware ESXi 호스트에는 vCPU 4개가 필요합니다.
- VMware ESXi 호스트에는 최소 8GB의 메모리가 필요합니다.
- VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - CDO 커넥터 VM에 사용할 고정 IP 주소.
  - 설치 프로세스 중 생성하는 **root** 및 **cdo** 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - SDC 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- CDO 커넥터 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.

## 프로시저

- 단계 1 CDO 커넥터를 생성할 CDO 테넌트에 로그인합니다.
- 단계 2 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
- 단계 3 파란색 더하기 버튼을 클릭하고 **Secure Event Connector**(보안 이벤트 커넥터)를 클릭합니다.



- 단계 4 1단계에서 **Download the CDO Connector VM image**(CDO 커넥터 VM 이미지 다운로드)를 클릭합니다. 이는 SEC를 설치하는 특수 이미지입니다. 최신 이미지를 사용하려면 항상 CDO 커넥터 VM을 다운로드하십시오.



- 단계 5 .zip 파일의 모든 파일을 추출합니다. 다음과 같이 표시됩니다.

- CDO-SDC-VM-ddd50fa.ovf

- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

단계 6 vSphere 웹 클라이언트를 사용하여 VMware 서버에 관리자로 로그인합니다.

참고 VM vSphere 데스크톱 클라이언트를 사용하지 마십시오.

단계 7 지시에 따라 OVF 템플릿에서 온프레미스 CDO 커넥터 가상 머신을 구축합니다. (템플릿을 구축하려면 .ovf, .mf 및 .vdk 파일이 필요합니다.)

단계 8 설정이 완료되면 VM의 전원을 켭니다.

단계 9 새 CDO 커넥터 VM의 콘솔을 엽니다.

단계 10 **cdo** 사용자로 로그인합니다. 기본 암호는 adm123입니다.

단계 11 프롬프트에 `sudo sdc-onboard setup`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

단계 12 프롬프트가 표시되면 **cdo** 사용자의 기본 비밀번호 adm123을 입력합니다.

단계 13 지시에 따라 **root** 사용자의 새 암호를 생성합니다.

단계 14 지시에 따라 **cdo** 사용자의 새 암호를 생성합니다.

단계 15 지시에 따라 Cisco Defense Orchestrator 도메인 정보를 입력합니다.

단계 16 CDO 커넥터 VM에 사용할 고정 IP 주소를 입력합니다.

단계 17 CDO 커넥터 VM이 설치된 네트워크의 게이트웨이 IP 주소를 입력합니다.

단계 18 CDO 커넥터의 NTP 서버 주소 또는 FQDN을 입력합니다.

단계 19 Docker 브리지 정보를 묻는 프롬프트가 표시되면 정보를 입력하거나 해당되지 않는 경우 비워두고 <Enter> 키를 누릅니다.

단계 20 입력을 확인합니다.

단계 21 "지금 SDC를 설정하시겠습니까?"라는 프롬프트가 나타나면 **n**을 입력합니다.

단계 22 **cdo** 사용자로 로그인하여 CDO 커넥터에 대한 SSH 연결을 생성합니다.

단계 23 프롬프트에 `sudo sdc-onboard bootstrap`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

단계 24 프롬프트가 표시되면 **cdo** 사용자의 비밀번호를 입력합니다.

단계 25 프롬프트가 표시되면 CDO로 돌아가 CDO 부트스트랩 데이터를 복사한 다음 SSH 세션에 붙여넣습니다. CDO 부트스트랩 데이터를 복사하려면 다음을 수행합니다.

1. CDO에 로그인합니다.
2. CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
3. 온보딩을 시작한 보안 이벤트 커넥터를 선택합니다. 상태가 "Onboarding(온보딩)"으로 표시되어야 합니다.
4. Actions(작업) 창에서 **Deploy an On-Premises Secure Event Connector**(온프레미스 보안 디바이스 커넥터 구축)를 클릭합니다.

## 5. 대화 상자의 1 단계에서 CDO 부트스트랩 데이터를 복사합니

Deploy an On-Premises Secure Event Connector
✕

i SEC will be deployed on a new VM

**Step 1**

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

CDO Bootstrap Data

```

Q0RPX1RPS0V0PSJ1eUp0YkdjaU9pS1NVekkxTm1Jc01uUjVjQ0k2SWtwWFZDSjkuZX1KM1pYSW1PaU
l3SW13aWMyTnZjr1VpT2xzaWRISjFjM1FpTENKeVpXRmtJaXdpZDNKcGRHVWlMQ0poTTJVMVkyVTBa
aTAzTWpGa0xUUmhaVfV0T1dNd05DMH10VGRpT1R0aE1qZzFPR1VpWFN3aV1XMX1Jam9pYzJGdGJDSX
NjBkp2YkdWek1qcGJJbEpQVEVWZ1UxVlFSVkpUUVVST1NVNG1YU3dpYVh0ek1qb2lhwWFJrSW13aVky
eDFjM1JsY2tsa01qb2lNU01zSW1sa01qb2labVF3T0dReVpHVXRNM1ZpT1MwMFpEYzRMV0kwW1dNdf
pUWXh0V0UyWmpjNFkyUm1JaXdpYzNWaWftVmpkR1I1Y0dVaU9pSjFjM1Z5SW13aWfuUnBJam9pTURB
VacmI0YVFLSjFTdnJ5RjVfZ2FqajZfZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZXlMT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VkkxN0Up4bk9RS1pqaW
1rdDNsYnRRbDNRTHMxeWduaXdVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZJVNUdGT2RS
NFN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEVOQU5UPSJDRE9fy2lZy28tYW1hbGxpbyIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ2lUy5kZXYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fy2lZy28tYW1hbGxpby
IKT05MWV9FVkvOVE1ORz0idHJ1ZSIK
          
```

📄 Copy CDO Bootstrap Data
←

Cancel
OK

다.

단계 26 이 설정을 업데이트하시겠습니까?라는 메시지가 표시되면 **n**을 입력합니다.

단계 27 CDO의 Deploy an On-Premises Secure Event Connector(온프레미스 보안 이벤트 커넥터 구축) 대화 상자로 돌아가 **OK**(확인)를 클릭합니다. Secure Connector(보안 커넥터) 페이지에서 Secure Event Connector(보안 이벤트 커넥터)가 노란색 Onboarding(온보딩) 상태로 표시됩니다.

다음에 수행할 작업

[CDO 커넥터 VM에 보안 이벤트 커넥터 설치, 679 페이지](#)를 진행합니다.

## CDO 커넥터 VM에 보안 이벤트 커넥터 설치

시작하기 전에

CDO VM 이미지를 사용하여 보안 이벤트 커넥터를 지원하기 위한 CDO 커넥터 설치, 675 페이지에 설명된 대로 CDO 커넥터 VM을 설치해야 합니다.

프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
- 단계 3 위에서 온보딩한 CDO 커넥터를 선택합니다. Secure Connector(보안 커넥터) 테이블에서는 이를 보안 이벤트 커넥터(보안 이벤트 커넥터)라고 하며 여전히 "Onboarding(온보딩)" 상태여야 합니다.
- 단계 4 오른쪽의 작업 창에서 **Deploy an On-Premises Secure Event Connector**(온프레미스 보안 디바이스 커넥터 구축)를 클릭합니다.
- 단계 5 마법사 2단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니다.

Deploy an On-Premises Secure Event Connector

VGxfrWYk8ekLSMhNJDWXTSWPvavpTLUXOPH1f5WK0Y0e0yVmlLPUZAWKKJNeXKS18v010W1KZet:5XK1  
JaanM0WTJSaUJpd21hb1JwSWpvaU1ESXpNVFEwTkdVdFqQWnhNqzAwT1RZMkcxSTFZek10TURNMVpe  
VXdNe1kwwpaaE1uMG5Yb1hrRnVKOVE4NGZfcG1seFFmN0ppSDNZYTh4NKEwcWNTF3hVekFM0U9Dzn  
Z2VWZPeC14anfSZChveHdPRGtzoUNQX2ZGYVpLLVfPbmFjWV1UTTRtaVR6bUI5dGJ2Y110dnA3T1NT  
VmFWW6ZJbaxQUH1LUUJHTGJJNw9FTGVJdDhxU2o0M0RGmVUWXDHZ2S1VWxJdjVTZFRkSDda0nY4S1  
JGNWZvV3N9WTIySDhXRzZRQWLSz2prZEhPa2pfaGNS9pFbmNaNjYebFU0S9B5RC11bkNMY1h2YjUz  
bm5KVU5F0TNDWwJCSHJ6b3pMekg2bHvATWRDT05uVXAYOXcWmfU4R3BMUWZ1d1Z1cXhuLXcWsuFueF  
BwcfRpe0Vadmphe1B2ZWhVdk5kUTVEWHZIEUyZbntHbG56QkZVUNQUdkwV1FMUGdQcWZHUkVhYTLX  
S2xPeYE1CKNET19ET01BSU49InN8YwDpbncuZGV2LmXvY2toYXJ0LmlvTgpDRE9fVE0QU5UPSJhbm  
R5BWFab61vLWpcc2NvIgpDRE9fQk9PVFNuUkFQX1VSTDB1aHR0cHN6Ly9zdGFnaW5tLnR1di55b2Nr  
aGfYdC5pbY9ZzGMvYm9vdHN0cmFwL2FuZ3H1tYXxsaW8tY21zY28vYW5keW1hbGxpbY1jaXNjby1TRE  
M1ck90TF1FRVZFT1RJTkc9InRydWUiCg==

Copy CDO Bootstrap Data

Step 2  
Follow the [documentation](#) to install the Secure Event Connector.  
Copy the data below and paste it when prompted for "SEC bootstrap Data".

SEC Bootstrap Data ⚠ valid until 11/24/2020, 3:34:51 PM

U1NFx0RFVklDRV9JF00i0GZhmj1mMzctNmR1Y80YnQ5LWJhZTctMDNmYmVvYzJjOTY1IgpTU0VfRE  
VMSUNfX085TLU9I1NDSU0gREVNSUNfIgpTU0VfR1FE1j9ic3RhZ21uZyY1czUuY21zY28vY29tIgpT  
U0VfFT1RQPSJhMjg2YzIwZmZAA4MjgkMDM2YmRjOTUzMzExOWQ2YWIzYiIKVEV0QU5LU085BTU09ImFuZ3H  
1tYXxsaW8tY21zY281

Copy SEC Bootstrap Data

- 단계 6 CDO 커넥터에 대한 SSH 연결을 생성하고 **cdo** 사용자로 로그인합니다.
- 단계 7 로그인한 후에는 **sdc** 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

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

- 단계 8 프롬프트에서 **sec.sh** 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

- 단계 9 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

Please copy the bootstrap data from Setup Secure Event Connector page of CDO:

**KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE**

**RtyfUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjkhOuihIuyftyXtfcghvjbkB=**

SEC가 온보딩되면 sec.sh는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.

```
=====
Running SEC health check for tenant
-----
SEC cloud URL [redacted] is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====
```

등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 [SEC 온보딩 실패 문제 해결, 779 페이지](#)로 이동하십시오.

성공 메시지가 표시되면 CDO로 돌아가고 **Deploy on-Premise Secure Event Connector**(온프레미스 보안 이벤트 커넥터 구축) 대화 상자에서 Done(완료)를 클릭합니다.

단계 10 "What to do next(다음 작업)로 계속합니다."

다음에 수행할 작업

[FDM-관리 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현, 665 페이지](#)으로 돌아갑니다.

관련 정보:

- [보안 디바이스 커넥터 문제 해결, 774 페이지](#)
- [보안 이벤트 커넥터 문제 해결, 778 페이지](#)
- [SEC 온보딩 실패 문제 해결, 779 페이지](#)

## VM 이미지를 사용하여 SEC 설치

SEC(보안 이벤트 커넥터)는 ASA 및 FTD에서 Cisco cloud로 이벤트를 전달하므로 라이선스에 따라 Event Logging 페이지에서 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

테넌트에 두 개 이상의 SEC(보안 이벤트 커넥터)를 설치하고 ASA 및 FDM 매니지드 디바이스의 이벤트를 설치한 SEC로 보낼 수 있습니다. 여러 SEC를 사용하면 서로 다른 위치에 SEC를 설치하고 Cisco Cloud에 이벤트를 전송하는 작업을 배포할 수 있습니다.

자체 VM 이미지를 사용하여 여러 SEC를 설치하는 작업은 3단계로 진행됩니다. 다음 각 단계를 수행해야 합니다.

1. [VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 681 페이지](#)

2. 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 686 페이지를 사용하여 VM에 대한 몇 가지 추가 구성 단계를 수행합니다.
3. CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치



참고 CDO 커넥터용 CDO VM 이미지를 사용하는 것이 가장 쉽고 정확하며 선호되는 CDO 커넥터 설치 방법입니다. 이 방법을 사용하려면 [CDO 이미지를 사용하여 SEC 설치, 674 페이지](#)의 내용을 참조하십시오.

다음 작업:

[VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 681 페이지](#)를 계속합니다.

## VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치

CDO 커넥터 VM은 SEC를 설치하는 가상 머신입니다. CDO 커넥터의 목적은 Cisco SaaS(Security Analytics and Logging) 고객을 위한 SEC를 지원하는 것입니다.

시작하기 전에

- Cisco Security and Analytics Logging, **Logging and Troubleshooting**(로깅 및 문제 해결) 라이선스를 구매하고, **Logging Analytics and Detection**(로깅 분석 및 탐지), **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 구매하여 Secure Cloud Analytics를 이벤트에 적용할 수도 있습니다.

원하는 경우 CDO에 로그인하여 Security Analytics and Logging(보안 분석 및 로깅) 평가판을 요청하고 기본 탐색 모음에서 분석 > 이벤트 로깅을 선택하고 **Request Trial**(평가판 요청)를 클릭합니다.

- CDO는 엄격한 인증서 확인이 필요하며 CDO 커넥터와 인터넷 간의 웹/콘텐츠 프록시를 지원하지 않습니다.
- CDO 커넥터는 **TCP 포트 443**에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.
- **매니지드 디바이스에 Cisco Defense Orchestrator 연결**을 검토하여 CDO 커넥터에 대한 적절한 네트워크 액세스를 확인합니다.
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트




참고 vSphere 데스크톱 클라이언트를 사용한 설치 는 지원되지 않습니다.

- ESXi 5.1 하이퍼바이저.
- Cent OS 7 게스트 운영체제.

- CDO 커넥터 및 SEC만 호스팅하는 VM의 시스템 요구 사항:
  - CPU: SEC를 수용할 수 있도록 4개의 CPU를 할당합니다.
  - 메모리: SEC에 대해 8GB의 메모리를 할당합니다.
  - 디스크 공간: 64GB
- 이 절차를 수행하는 사용자는 Linux 환경에서 작업하고 파일 편집을 위해 vi 시각적 편집기를 사용하는 데 익숙해야 합니다.
- CentOS 가상 머신에 CDO Connector를 설치하는 경우 정기적으로 Yum 보안 패치를 설치하는 것이 좋습니다. Yum 구성에 따라 Yum 업데이트를 가져오려면 포트 80 및 443에서 아웃바운드 액세스를 열어야 할 수 있습니다. 또한 업데이트를 예약하려면 yum-cron 또는 crontab을 구성해야 합니다. 보안 운영 팀과 함께 Yum 업데이트를 받기 위해 변경해야 하는 보안 정책이 있는지 확인합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - CDO 커넥터에 사용할 고정 IP 주소.
  - 설치 프로세스 중 생성하는 root 및 cdo 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - CDO 커넥터 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- CDO 커넥터 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.
- 시작하기 전에: 이 절차의 명령을 복사하여 터미널 창에 붙여넣지 말고 대신 입력하십시오. 일부 명령에는 "n-대시"가 포함되며, 잘라내기 및 붙여넣기 프로세스에서 이러한 명령은 "m-대시"로 적용되어 명령이 실패할 수 있습니다.

## 프로시저

- 단계 1 보안 디바이스 커넥터 페이지에서 파란색 플러스 버튼  을 클릭하고 보안 이벤트 커넥터(보안 이벤트 커넥터)를 클릭합니다.
- 단계 2 제공된 링크를 사용하여 "Deploy an On-Premises 보안 이벤트 커넥터(온프레미스 보안 이벤트 커넥터 배포)" 창의 2단계에서 SEC 부트스트랩 데이터를 복사합니다.
- 단계 3 이 절차의 사전 요구 사항에 나와 있는 메모리, CPU 및 디스크 공간 이상으로 CentOS 7 가상 머신 ([http://isoredirect.centos.org/centos/7/isos/x86\\_64/CentOS-7-x86\\_64-Minimal-1804.iso](http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso))을 설치합니다.
- 단계 4 설치가 완료되면 CDO 커넥터의 IP 주소, 서브넷 마스크 및 게이트웨이를 지정하는 등의 기본 네트워킹을 구성합니다.
- 단계 5 DNS(Domain Name Server) 서버를 구성합니다.



단계 6 NTP(Network Time Protocol) 서버를 구성합니다.

단계 7 CDO 커넥터의 CLI와의 손쉬운 상호 작용을 위해 CentOS에 SSH 서버를 설치합니다.

단계 8 Yum 업데이트를 실행한 후 **open-vm-tools**, **nettools** 및 **bind-utils** 패키지를 설치합니다.

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

단계 9 **AWS CLI package(AWS CLI 패키지)** (<https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html>)를 설치합니다.

참고 `--user` 플래그를 사용하지 마십시오.

단계 10 **Docker CE packages(Docker CE 패키지)** (<https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce>)를 설치합니다.

참고 "저장소를 사용하여 설치" 방법을 사용합니다.

단계 11 Docker 서비스를 시작하고 부팅 시 시작되도록 활성화합니다.

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

단계 12 두 사용자(**cdo** 및 **sdc**)를 생성합니다. **cdo** 사용자는 관리 기능을 실행하기 위해 로그인하는 사용자이며(루트 사용자를 직접 사용할 필요가 없음), **sdc** 사용자는 CDO 커넥터 도커 컨테이너를 실행하는 사용자입니다.

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

단계 13 **cdo** 사용자의 비밀번호를 생성합니다.

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

단계 14 **cdo** 사용자를 "Wheel" 그룹에 추가하여 관리(sudo) 권한을 부여합니다.

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

단계 15 Docker가 설치되면 사용자 그룹이 생성됩니다. CentOS/Docker 버전에 따라 "docker" 또는 "dockerroot"라고 부를 수 있습니다. `/etc/group` 파일을 확인하여 어떤 그룹이 생성되었는지 확인한 다음 **sdc** 사용자를 이 그룹에 추가합니다.

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

단계 16 `/etc/docker/daemon.json` 파일이 없는 경우 파일을 생성하고 아래 내용을 입력합니다. 생성되면 **docker** 데몬을 다시 시작합니다.

참고 "group" 키에 입력한 그룹 이름이 [단계 15](#)과 일치하는지 확인합니다.

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

**단계 17** 현재 vSphere 콘솔 세션을 사용하는 경우 SSH로 전환하고 **cdo** 사용자로 로그인합니다. 로그인 후에는 **sdc** 사용자로 변경합니다. 암호를 묻는 메시지가 표시되면 **cdo** 사용자의 암호를 입력합니다.

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

**단계 18** 디렉토리를 **/usr/local/cdo**로 변경합니다.

**단계 19** **bootstrapdata**라는 새 파일을 생성하고 배포 마법사 1단계의 부트스트랩 데이터를 이 파일에 붙여넣습니다. 파일을 **Save(저장)**합니다. **vi** 또는 **nano**를 사용하여 파일을 생성할 수 있습니다

### Deploy an On-Premises Secure Event Connector


 SEC will be deployed on a new VM

#### Step 1

Download the [CDO Connector VM](#) and follow the [documentation](#) to deploy the CDO VM on vSphere. You will be prompted for "CDO Bootstrap Data". Copy the data below and paste it into the CDO Bootstrap Data input field in vSphere.

CDO Bootstrap Data

```
Q0RPX1RPS0V0PSJ1eUpoykdjaU9pS1NVekxTm1Jc0luUjVjQ0k2SWtwWFZDSjkuZX1KM1pYSW1PaU
13SW13aWMyTnZjR1VpT2xzaWRISjFjM1FpTENKeVpXRmtJaXdpZDNkcGRHVW1MQ0poTTJVMVkyVTBa
aTAzTWpGa0xUUmhaVFV0T1dNd05DMH10VGRpT1R0aE1qZzFPR1VpWFN3aV1XMX1Jam9pYzJGdGJDSX
NjBkp2YkdWek1qcGJJbEpQVEVWZ1UxV1FSVkpUUVVST1NVNG1YU3dpYVh0ek1qb2lhWFJrSW13aVky
eDFjM1JsY2tsa01qb2lNU01zSW1sa01qb2labVF3T0dReVpHVXRNM1ZpT1MwMFpEYzRMV0kwW1dNdF
pUWXh0V0UyWmpjNFkyUm1JaXdpYzNWaWFtVmpkRII1Y0dVaU9pSjFjM1Z5SW13aWfuUnBJam9pTURB
VacmI0YVFLSjFtdnJ5RjVfZ2FqajZfZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VksNOU4bk9RS1pqaW
1rdDNsYnRRbDNRTHMxeWduaXdVU1RuWkQxM0c5T2FJWEExCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NFN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxyY2toYXJ0Lm
1vIgpDRE9fVEVOQU5UPSJDRE9fY21zY28tYW1hbGxpbYIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
Oi8vc3RhZ21uZy5kZXZubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY21zY28tYW1hbGxpbY
IKT05MMWV9FVkvOVE10Rz0idHJ1ZSIK
```

 Copy CDO Bootstrap Data

Cancel

OK

다.

단계 20 부트스트랩 데이터는 base64로 인코딩됩니다. 이를 디코딩하고 **extractedbootstrapdata**라는 파일로 내보냅니다.

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

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

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

ONLY_EVENTING="true"
```

단계 21 다음 명령을 실행하여 디코딩된 부트스트랩 데이터의 섹션을 환경 변수로 내보냅니다.

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

단계 22 CDO에서 부트스트랩 번들을 다운로드합니다.

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

단계 23 CDO 커넥터 tarball을 추출하고 bootstrap\_sec\_only.sh 파일을 실행하여 CDO 커넥터 패키지를 설치합니다.

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/cdo/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/cdo/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

다음에 수행할 작업

생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 686 페이지를 계속합니다.

## 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성

자체 CentOS 7 가상 머신에 CDO 커넥터를 설치한 경우, 이벤트가 SEC에 도달하도록 허용하려면 다음 추가 구성 절차 중 하나를 수행해야 합니다.

- CentOS 7 VM에서 **firewalld** 서비스를 비활성화합니다.. 이는 Cisco 제공 SDC VM의 구성과 일치합니다.
- **firewalld** 서비스가 실행되도록 허용하고 방화벽 규칙을 추가하여 이벤트 트래픽이 SEC에 도달하도록 허용합니다., 686 페이지. 이는 인바운드 이벤트 트래픽을 허용하는 보다 세부적인 접근 방식입니다.

**CentOS 7 VM에서 firewalld 서비스를 비활성화합니다.**

1. SDC VM의 CLI에 "cdo" 사용자로 로그인합니다.
2. firewalld 서비스를 중지한 다음, 이후에 VM을 재부팅할 때 비활성화된 상태로 유지되는지 확인합니다. 메시지가 표시되면 **cdo** 사용자의 비밀번호를 입력합니다.

```
[cdo@SDC-VM ~]$ sudo systemctl stop firewalld
cdo@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Docker 서비스를 다시 시작하여 Docker 관련 항목을 로컬 방화벽에 다시 삽입합니다.

```
[cdo@SDC-VM ~]$ sudo systemctl restart docker
```

4. **CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 686 페이지**를 진행합니다.

**firewalld** 서비스가 실행되도록 허용하고 방화벽 규칙을 추가하여 이벤트 트래픽이 **SEC**에 도달하도록 허용합니다.

1. SDC VM의 CLI에 "cdo" 사용자로 로그인합니다.
2. 구성된 TCP, UDP 또는 NSEL 포트에서 SEC로 수신되는 트래픽을 허용하도록 로컬 방화벽 규칙을 추가합니다. SEC에서 사용하는 포트에 대해서는 **SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기**를 참조하십시오. 메시지가 표시되면 **cdo** 사용자의 비밀번호를 입력합니다. 다음은 이러한 명령의 예입니다. 다른 포트 값을 지정해야 할 수 있습니다.

```
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10425/udp
```

3. firewalld 서비스를 다시 시작하여 새 로컬 방화벽 규칙을 활성화 및 영구 규칙으로 설정합니다.

```
[cdo@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. **CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치, 686 페이지**를 진행합니다.

## CDO 커넥터 가상 머신에 보안 이벤트 커넥터 설치

시작하기 전에

다음 두 가지 작업을 수행합니다.

- VM 이미지를 사용하여 SEC를 지원하도록 CDO 커넥터 설치, 681 페이지
- 생성한 VM에 설치된 SDC 및 CDO 커넥터에 대한 추가 구성, 686 페이지

## 프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.
- 단계 3 위의 사전 요구 사항에 있는 절차를 사용하여 설치한 CDO 커넥터를 선택합니다. Secure Connector(보안 커넥터) 테이블에서는 이를 보안 이벤트 커넥터(보안 이벤트 커넥터)라고 합니다.
- 단계 4 오른쪽의 작업 창에서 **Deploy an On-Premises Secure Event Connector**(온프레미스 보안 디바이스 커넥터 구축)를 클릭합니다.
- 단계 5 마법사 2단계에서 링크를 클릭하여 **SEC** 부트스트랩 데이터를 복사합니

## Deploy an On-Premises Secure Event Connector



```
dRaU9pSmhNM1UxWTJVMFppMDNnakZrTFRSaFpUVXRPV013TkMweU5UZG10VE5oTWpnMU9HVW1MQ0pq
YkdsbGJuUmZhV1FpT21KaGNHa3RZMnhwW1c1ME1uMC5tTzh0bTZMZ1N6cjI4b1ZGZERqYjJNRzVqUE
ZmYTZQYzVsRjRITt1teVVEVzh2Qk5FWW44c3V0Z3NTQuo0TH15N0xzVGsydEx4N05nbS00STB6SmZ6
aWdQTKrRiV1RsRW1tcjI5SkFVZ2NBWEhySkdzcktMREszUnJUM0hZU3JkZ21Hd1dGb3FwWUdZnkJHRU
VacmI0YVFLSjFTdnJ5RjVfZ2FqajZfZkNVaERNMUE3Q3c1Q0p1Sn1JMnFZbGpNUzBXeVg3Nm9KeTQ2
ZX1MT09qcjRicEN0UnhYaEVNMUFzV19qQW1PNXM3Tm02Sn1rMXR1QTFsYmE3VvxN0Up4bk9RS1pqaW
1rdDNsYnRRbDNRTHMxeWduaXduVU1RuWkQxM0c5T2FJWExCQ093T3NESGdNeH16UU13ZWJVNUdGT2RS
NfN6c2ZBb1VXRDNwZ2V2V0gzUzBNT2ciCkNET19ET01BSU49InN0YWdpbmcuZGV2LmxvY2toYXJ0Lm
1vIgpDRE9fVEV0QU5UPSJDRE9fY2lZy28tYW1hbGxpbyIKQ0RPX0JPT1RTVFJBUf9VUkw9Imh0dHBz
0i8vc3RhZ21uZy5kZXlYubG9ja2hhcnQuaW8vc2RjL2Jvb3RzdHJhcC9DRE9fY2lZy28tYW1hbGxpby
IKT05MwV9FVkv0VE10Rz0idHJ1ZSIK
```

[Copy CDO Bootstrap Data](#)

## Step 2

Read the [instructions](#) about deploying the Secure Event Connector on vSphere.  
Copy the bootstrap data below and paste it when prompted for "SEC bootstrap Data".

**⚠ The SEC bootstrap data is valid until 10/13/2021, 10:44:14 AM**

```
U1NFX0RFVklDRV9JRD0iZTBhZTJkNmMtMDdhYy00Y2JkLWEzNWQ0OGYzZDJKMjQ1ZmU3IgpTU0VfRE
U0VfT1RQPSI5Y2IzNTI4ZWZ1Mzg0TQ2NjViMDFkZmEyYjUyMGUxNSIKVEV0QU5UX05BTUU9IKNET1
9jaXNjby1hbWFSbG1vIg==
```

[Copy SEC Bootstrap Data](#)

## Step 3

Verify the connection status of the new SEC by exiting this dialog and checking the "Last Heartbeat" information.

Cancel

OK

다.

단계 6 SSH를 사용하여 Secure Connector에 연결하고 **cdo** 사용자로 로그인합니다.

단계 7 로그인한 후에는 **sdc** 사용자로 전환합니다. 암호를 묻는 메시지가 표시되면 "cdo" 사용자의 암호를 입력합니다. 다음은 이러한 명령의 예입니다.

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

단계 8 프롬프트에서 **sec.sh** 설정 스크립트를 실행합니다.

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

단계 9 프롬프트 끝에 4단계에서 복사한 부트스트랩 데이터를 붙여넣고 **Enter** 키를 누릅니다.

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyfUIyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjkhOuihIuyftyXtfcghvjbkhB=
```

SEC가 온보딩되면 **sec.sh**는 SEC의 상태를 확인하는 스크립트를 실행합니다. 모든 상태 확인이 "녹색"인 경우 상태 확인은 이벤트 로그에 샘플 이벤트를 전송합니다. 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.

```
=====
Running SEC health check for tenant
=====
SEC cloud URL          is: Reachable
=====
SEC Connector status: Active
=====
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
=====
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====
```

등록에 실패했거나 SEC 온 보딩에 실패했다는 메시지가 표시되면 [보안 이벤트 커넥터 문제 해결](#)로 이동하십시오.

성공 메시지가 표시되면 **Deploy an ON-Premise Secure Event Connector**(온프레미스 보안 이벤트 커넥터 구축) 대화 상자에서 **Done**(완료)를 클릭합니다. VM 이미지에 SEC 설치를 완료했습니다.

단계 10 "다음 작업"을 계속합니다.

다음에 수행할 작업

SAL SaaS의 구현을 계속하려면 이 절차로 돌아가십시오. [FDM-관리 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현, 665 페이지](#).

관련 정보:

- [보안 디바이스 커넥터 문제 해결, 774 페이지](#)
- [보안 이벤트 커넥터 문제 해결](#)
- [SEC 온보딩 실패 문제 해결](#)
- [보안 이벤트 커넥터 등록 실패 문제 해결](#)

## Terraform 모듈을 사용하여 AWS VPC에 보안 이벤트 커넥터 설치

시작하기 전에

- 이 작업을 수행하려면 CDO 테넌트에서 SAL을 활성화해야 합니다. 이 섹션에서는 SAL 라이선스가 있다고 가정합니다. 라이선스가 없는 경우 Cisco 보안 및 분석 로깅, 로깅 및 문제 해결 라이선스를 구매합니다.
- 새 SEC가 설치되어 있는지 확인합니다. 새 SEC를 생성하려면 [SDC 가상 머신에 SEC\(Secure Event Connector\) 설치, 671 페이지](#)의 내용을 참조하십시오.
- SEC를 설치할 때 CDO 부트스트랩 데이터 및 SEC 부트스트랩 데이터를 적어 두십시오.

프로시저

**단계 1** Terraform 레지스트리의 [Secure Event Connector Terraform 모듈](#)로 이동하고 지침에 따라 SEC Terraform 모듈을 Terraform 코드에 추가합니다.

**단계 2** Terraform 코드를 적용합니다.

**단계 3** `instance_id` 및 `sec_fqdn` 출력은 나중에 절차에서 필요하므로 인쇄해야 합니다.

**참고** SEC 문제를 해결하려면 AWS Systems Manager Session Manager(SSM)를 사용하여 SEC 인스턴스에 연결해야 합니다. SSM을 사용하여 인스턴스에 연결하는 방법에 대한 자세한 내용은 [AWS Systems Manager Session Manager](#) 설명서를 참조하십시오.

SSH를 사용하여 SDC 인스턴스에 연결하는 포트는 보안상의 이유로 노출되지 않습니다.

**단계 4** ASA에서 SEC로 로그를 전송하려면 생성한 SEC의 인증서 체인을 가져와 **단계 3**의 출력과 함께 다음 명령을 실행하여 리프 인증서를 제거합니다.

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 </dev/null | awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++}; out="/tmp/cert_chain.pem"; if(a > 1) print >>out}'
```

**단계 5** `/tmp/cert_chain.pem`의 내용을 클립보드에 복사합니다.

**단계 6** 다음 명령을 사용하여 SEC의 IP 주소를 기록해 둡니다.

```
nslookup <FQDN>
```

**단계 7** CDO에 로그인하고 새 트러스트 포인트 개체 추가를 시작합니다. 자세한 내용은 [신뢰할 수 있는 CA 인증서 개체 추가](#)를 참조하십시오. **Add(추가)**를 클릭하기 전에 **Other Options(기타 옵션)**에서 **Enable CA flag in basic constraints extension(기본 제약 조건 확장에서 CA 플래그 활성화)** 확인란의 선택을 취소해야 합니다.

**단계 8** **Add(추가)**를 클릭하고 **Install Certificate(인증서 설치)** 페이지의 CDO에서 생성한 CLI 명령을 복사한 다음 **Cancel(취소)**를 클릭합니다.

**단계 9** `enrollment terminal`(등록 터미널) 아래 텍스트 클립보드에 `no ca-check`를 추가합니다.

**단계 10** SSH로 ASA 디바이스에 연결하거나 CDO에서 ASA CLI 옵션을 사용하고 다음 명령을 실행합니다.

```
DataCenterFW-1> en
Password: *****
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

다음에 수행할 작업

SEC가 AWS SSM을 사용하여 패킷을 수신하고 있는지 확인할 수 있습니다.

다음과 유사한 로그가 표시됩니다.

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

## Cisco Security Analytics and Logging(SaaS) 프로비저닝

Cisco SaaS(Security Analytics and Logging) 유료 라이선스가 만료되도록 허용하는 경우 90일의 유예 기간이 제공됩니다. 이 유예 기간 동안 유료 라이선스를 갱신하는 경우 서비스가 중단되지 않습니다.

그렇지 않고 90일의 유예 기간이 경과하도록 허용하면 시스템은 모든 고객 데이터를 비웁니다. 더 이상 이벤트 로깅 페이지에서 ASA 또는 FTD 이벤트를 보거나 ASA 또는 FTD 이벤트 및 네트워크 플로우 데이터에 동적 엔터티 모델링 동작 분석을 적용할 수 없습니다.

## 보안 이벤트 커넥터 제거

경고: 이 절차는 보안 디바이스 커넥터에서 보안 이벤트 커넥터를 삭제합니다. 이렇게 하면 SaaS(Secure Logging Analytics)를 사용할 수 없습니다. 이는 되돌릴 수 없습니다. 질문이나 우려 사항이 있는 경우 이 작업을 수행하기 전에 [Cisco Defense Orchestrator 지원팀에 문의](#)하십시오.

보안 디바이스 커넥터에서 보안 이벤트 커넥터를 제거하는 작업은 다음의 2단계 프로세스입니다.

1. CDO에서 SEC 제거
2. SDC에서 SEC 파일 제거.

후속 작업:[CDO에서 SEC 제거](#) 계속

## CDO에서 SEC 제거

시작하기 전에

[보안 이벤트 커넥터 제거](#), 690 페이지의 내용을 참조하십시오.



## 프로시저

단계 1 CDO에 로그인합니다.

단계 2 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 3 디바이스 유형인 보안 이벤트 커넥터가 있는 행을 선택합니다.

경고: 주의하십시오. 보안 디바이스 커넥터를 선택하지 마십시오.

단계 4 Actions(작업) 창에서 **Remove(제거)**를 클릭합니다.

단계 5 **OK(확인)**를 클릭하여 보안 이벤트 커넥터 삭제를 확인합니다.

다음에 수행할 작업

[SDC에서 SEC 파일 제거, 691 페이지](#)를 진행합니다.

## SDC에서 SEC 파일 제거

이는 SDC에서 보안 이벤트 커넥터를 제거하는 2단계 절차의 두 번째 부분입니다. 시작하기 전에 [보안 이벤트 커넥터 제거, 690 페이지](#)을 참조하십시오.

## 프로시저

단계 1 가상 머신 하이퍼바이저를 열고 SDC에 대한 콘솔 세션을 시작합니다.

단계 2 SDC 사용자로 전환합니다.

```
[cdo@tenant toolkit]$sudo su sdc
```

단계 3 프롬프트에서 다음 명령 중 하나를 입력합니다.

- 자체 테넌트만 관리하는 경우:

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
```

- 둘 이상의 테넌트를 관리하는 경우 테넌트 이름의 시작 부분에 CDO\_를 추가합니다. 예를 들면 다음과 같습니다.

```
[sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
```

단계 4 SEC 파일을 제거할 것인지 확인합니다.

## Cisco Secure Cloud Analytics 포털 프로비저닝

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

**Logging Analytics and Detection**(로깅 분석 및 탐지) 또는 **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 구매한 경우, SEC(Secure Event Connector)를 구축하고 구성한 후 Secure Cloud Analytics 포털을 CDO 포털에 연결해야 Secure Cloud Analytics 알림을 볼 수 있습니다. 기존 Secure Cloud Analytics 포털이 있는 경우 라이선스를 구매할 때 Secure Cloud Analytics 포털 이름을 제공하고 CDO 포털에 즉시 연결할 수 있습니다.

그렇지 않은 경우 CDO UI에서 새 Secure Cloud Analytics 포털을 요청할 수 있습니다. Secure Cloud Analytics 알림에 처음 액세스하면 시스템은 Secure Cloud Analytics 포털을 요청할 수 있는 페이지로 이동합니다. 이 포털을 요청하는 사용자에게는 포털에서 관리자 권한이 부여됩니다.

## Procedure

- 단계 1 CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택하여 새 창에서 Secure Cloud Analytics UI를 엽니다.
- 단계 2 **Start Free Trial**(무료 평가판 시작)을 클릭하여 Secure Cloud Analytics 포털을 프로비저닝하고 CDO 포털과 연결합니다.

**Note** 포털을 요청한 후 프로비저닝에 몇 시간이 걸릴 수 있습니다.

다음 단계로 이동하기 전에 포털이 프로비저닝되었는지 확인합니다.

1. CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택하여 새 창에서 Secure Cloud Analytis UI를 엽니다.
2. 다음 옵션을 이용할 수 있습니다.
  - Secure Cloud Analytics 포털을 요청했는데 시스템에서 포털을 프로비저닝하는 중이라고 표시되면 기다렸다가 나중에 알림에 액세스해 보십시오.
  - Secure Cloud Analytics 포털이 프로비저닝된 경우 **Username**(사용자 이름) 및 **Password**(비밀 번호)를 입력하고 **Sign in**(로그인)을 클릭합니다.



**Note** 관리자 사용자는 다른 사용자를 초대하여 Secure Cloud Analytis 포털 내에서 계정을 생성할 수 있습니다. 자세한 내용은 [CDO에서 Cisco Secure Cloud Analytics 알림 보기](#), on page 694를 참조하십시오.

## What to do next

- **Logging Analytics and Detection**(로깅 분석 및 탐지) 라이선스를 구매한 경우 구성이 완료된 것입니다. Secure Cloud Analytics 포털 UI에서 CDO 통합 또는 센서 상태를 보려면 [Secure Cloud Analytics에서 센서 상태 및 CDO 통합 상태 검토](#), on page 693에서 자세한 내용을 확인하십시오. Secure Cloud Analytics 포털에서 알림으로 작업하려는 경우 자세한 내용은 [CDO에서 Cisco Secure Cloud Analytics 알림 보기](#), on page 694 및 [방화벽 이벤트 기반 알림 작업](#)을 참조하십시오.

- **Total Network Analytics and Monitoring** 라이선스를 구매한 경우 내부 네트워크에 하나 이상의 Secure Cloud Analytics 센서를 구축하여 네트워크 플로우 데이터를 클라우드에 전달합니다. 클라우드 기반 네트워크 플로우 데이터를 모니터링하려면 플로우 데이터를 Secure Cloud Analytics로 전달하도록 클라우드 기반 구축을 구성합니다. 자세한 내용은 [전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축](#), on page 693를 참조하십시오.

## Secure Cloud Analytics에서 센서 상태 및 CDO 통합 상태 검토

### 센서 상태

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytis 웹 UI의 Sensor List(센서 목록) 페이지에서 CDO 통합 상태 및 구성된 센서를 볼 수 있습니다. CDO 통합은 읽기 전용 연결 이벤트 센서입니다. Stelathwatch Cloud는 기본 메뉴에서 센서의 전반적인 상태를 제공합니다.

- 녹색 클라우드 아이콘(☑) - 모든 센서와 연결 설정됨, 구성된 경우 CDO
- 노란색 클라우드 아이콘(⚠) - 일부 센서 또는 CDO(구성된 경우)와의 연결이 설정되었으며 하나 이상의 센서가 제대로 구성되지 않음
- 빨간색 클라우드 아이콘(❌) - 구성된 모든 센서 및 CDO(구성된 경우)와의 연결 끊김

센서 또는 CDO 통합에서 녹색 아이콘은 설정된 연결을 나타내고, 빨간색 아이콘은 연결 끊김을 나타냅니다.

### 프로시저

단계 1 1. Secure Cloud Analytis 포털 UI에서 **Settings(설정)**(⚙) > **Sensors(센서)**를 선택합니다.

단계 2 **Sensor List(센서 목록)**를 선택합니다.

## 전체 네트워크 분석 및 보고를 위한 Cisco Secure Cloud Analytics 센서 구축

### Secure Cloud Analytics 센서 개요 및 배포

필수 라이선스: 전체 네트워크 분석 및 모니터링

**Total Network Analytics and Monitoring(전체 네트워크 분석 및 모니터링)** 라이선스를 취득한 경우 Secure Cloud Analytics 포털을 프로비저닝한 후 다음을 수행할 수 있습니다.

- 분석을 위해 네트워크 플로우 데이터를 클라우드로 전달하기 위해 온프레미스 네트워크 내에 Secure Cloud Analytics 센서를 배포하고 구성합니다.
- 분석을 위해 네트워크 플로우 로그 데이터를 Secure Cloud Analytics에 전달하도록 클라우드 기반 배포를 구성합니다.

네트워크 경계의 방화벽은 내부 네트워크와 외부 네트워크 간의 트래픽에 대한 정보를 수집하는 반면, Secure Cloud Analytics 센서는 내부 네트워크 내의 트래픽에 대한 정보를 수집합니다.



**Note** FDM 관리 Secure Firewall Threat Defense 디바이스가 NetFlow 데이터를 전달하도록 구성할 수 있습니다. 센서를 배포할 때, 이벤트 정보를 CDO로 전달하도록 구성된 FDM 관리 Secure Firewall Threat Defense 디바이스에서 NetFlow 데이터를 전달하도록 센서를 구성하지 마십시오.

센서 배포 지침 및 권장 사항은 [Secure Cloud Analytics 센서 설치 설명서](#)를 참조하십시오.

클라우드 기반 배포 구성 지침 및 권장 사항은 [Secure Cloud Analytics 퍼블릭 클라우드 모니터링 가이드](#)를 참조하십시오.



**Note** Secure Cloud Analytics 포털 UI의 지침을 검토하여 센서 및 클라우드 기반 배포를 구성할 수도 있습니다.

Secure Cloud Analytics에 대한 자세한 내용은 [Secure Cloud Analytics 무료 평가판 가이드](#)를 참조하십시오.

다음 단계

- CDO에서 [Cisco Secure Cloud Analytics 알림 보기](#), on page 694를 계속 진행합니다.

## CDO에서 Cisco Secure Cloud Analytics 알림 보기

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Events logging(이벤트 로깅) 페이지에서 방화벽 이벤트를 검토할 수 있지만 CDO 포털 UI에서 Cisco Secure Cloud Analytics 알림을 검토할 수는 없습니다. Security Analytics(보안 분석) 메뉴 옵션을 사용하여 CDO에서 Secure Cloud Analytics 포털로 교차 실행하고, 방화벽 이벤트 데이터(전체 네트워크 분석 및 모니터링을 활성화한 경우 네트워크 플로우 데이터)에서 생성된 알림을 볼 수 있습니다. Security Analytics(보안 분석) 메뉴 옵션은 하나 이상의 열려 있는 워크플로우 상태의 Secure Cloud Analytics 알림 수와 함께 배지를 표시합니다.

Security Analytics and Logging(보안 분석 및 로깅) 라이선스를 사용하여 Secure Cloud Analytics 알림을 생성하고 새 Secure Cloud Analytics 포털을 프로비저닝한 경우, CDO에 로그인한 다음 Cisco Secure Cloud Sign-On을 사용하여 Secure Cloud Analytics를 교차 실행합니다. URL을 통해 Secure Cloud Analytics 포털에 직접 액세스할 수도 있습니다.

자세한 내용은 [Cisco Security Cloud Sign On](#)을 참조하십시오.

## Secure Cloud Analytics 포털에 사용자 초대

Secure Cloud Analytics 포털 프로비저닝을 요청하는 초기 사용자는 Secure Cloud Analytics 포털에서 관리자 권한을 갖습니다. 해당 사용자는 이메일로 다른 사용자를 초대하여 포털에 참여할 수 있습니다. 이러한 사용자에게 Cisco Secure Cloud Sign-On 자격증명이 없는 경우 초대 이메일의 링크를 사용하여 생성할 수 있습니다. 그러면 사용자는 Cisco Secure Cloud Sign-On 자격증명을 사용하여 CDO에서 Secure Cloud Analytics로 교차 실행하는 동안 로그인할 수 있습니다.

이메일로 다른 사용자를 Secure Cloud Analytics 포털에 초대하려면 다음을 수행합니다.

### Procedure

- 
- 단계 1 Secure Cloud Analytics 포털에 관리자로 로그인합니다.
  - 단계 2 **Settings(설정) > Account Management(계정 관리) > User Management(사용자 관리)**를 선택합니다.
  - 단계 3 이메일 주소를 입력합니다.
  - 단계 4 **Invite(초대)**를 클릭합니다.
- 

## CDO에서 Secure Cloud Analytics로 교차 실행

CDO에서 보안 알림을 보려면 다음을 수행합니다.

### Procedure

- 
- 단계 1 CDO 포털에 로그인합니다.
  - 단계 2 CDO 메뉴에서 분석 > **Secure Cloud Analytics**를 선택합니다.
  - 단계 3 Secure Cloud Analytics 인터페이스에서 **Monitor(모니터링) > Alerts(알림)**를 선택합니다.
- 

## Cisco Secure Cloud Analytics 및 동적 엔티티 모델링

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytics는 온프레미스 및 클라우드 기반 네트워크 구축을 모니터링하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성함

니다. 알림과 함께 Secure Cloud Analytics는 알림을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

### 동적 엔터티 모델링

동적 엔터티 모델링은 방화벽 이벤트 및 네트워크 플로우 데이터에 대한 동작 분석을 수행하여 네트워크의 상태를 추적합니다. Secure Cloud Analytics의 컨텍스트에서 엔터티는 네트워크의 호스트 또는 엔드포인트와 같이 시간이 지남에 따라 추적할 수 있는 항목입니다. 동적 엔터티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔터티에 대한 정보를 수집합니다. **Logging Analytics and Detection**(로깅 분석 및 탐지) 라이선스와 통합된 Secure Cloud Analytics는 엔터티가 일반적으로 전송하는 트래픽 유형을 확인하기 위해 방화벽 이벤트 및 기타 트래픽 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 구매한 경우 Secure Cloud Analytics는 엔터티 트래픽 모델링에 NetFlow 및 기타 트래픽 정보도 포함할 수 있습니다. Secure Cloud Analytics는 각 엔터티의 최신 모델을 유지하기 위해 엔터티가 계속해서 트래픽을 전송하고 잠재적으로 다른 트래픽을 전송하므로 시간이 지남에 따라 이러한 모델을 업데이트합니다. 이 정보에서 Secure Cloud Analytics는 다음을 식별합니다.

- 엔터티의 역할 - 엔터티가 일반적으로 수행하는 작업을 설명합니다. 예를 들어 엔터티가 일반적으로 이메일 서버와 연결된 트래픽을 전송하는 경우, Secure Cloud Analytics는 엔터티를 이메일 서버 역할로 할당합니다. 엔터티는 여러 역할을 수행할 수 있으므로 역할/엔터티 관계는 다대일일 수 있습니다.
- 엔터티에 대한 관찰 - 외부 IP 주소와의 하트비트 연결 또는 다른 엔터티와 설정된 원격 액세스 세션과 같이 네트워크에서의 엔터티 동작에 대한 팩트입니다. CDO와 통합하는 경우 방화벽 이벤트에서 이러한 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스도 구매한 경우, 시스템은 NetFlow에서 팩트를 가져오고 방화벽 이벤트와 NetFlow 모두에서 관찰을 생성할 수 있습니다. 관찰 자체는 관찰이 나타내는 것 이상의 의미를 전달하지 않습니다. 일반적인 고객은 수천 개의 관찰 및 몇 가지 알림을 가질 수 있습니다.

### 알림 및 분석

역할, 관찰 및 기타 위협 인텔리전스의 조합을 기반으로 Secure Cloud Analytics는 시스템에서 식별한 가능한 악의적인 행동을 나타내는 실행 가능한 항목인 알림을 생성합니다. 하나의 알림이 여러 관찰을 나타낼 수 있습니다. 방화벽이 동일한 연결 및 엔터티와 관련된 여러 연결 이벤트를 로깅하는 경우 하나의 알림만 생성될 수 있습니다.

예를 들어, 새 내부 디바이스 관찰 자체는 악의적인 행동을 구성하지 않습니다. 그러나 시간이 지남에 따라 엔터티가 도메인 컨트롤러와 일치하는 트래픽을 전송하면 시스템은 해당 엔터티에 도메인 컨트롤러 역할을 할당합니다. 이후에 엔터티가 비정상적인 포트를 사용하여 이전에 연결을 설정하지 않은 외부 서버에 연결하고 대량의 데이터를 전송하는 경우, 시스템은 새로운 대규모 연결(외부) 관찰 및 예외적인 도메인 컨트롤러 관찰을 로깅합니다. 해당 외부 서버가 Talos 감시 목록에 있는 것으로 식별된 경우, 이 모든 정보의 조합으로 인해 Secure Cloud Analytics가 이 엔터티의 동작에 대한 알림을 생성하고, 악성 동작을 조사하고 교정하기 위한 추가 작업을 수행하라는 메시지가 표시됩니다.

Secure Cloud Analytics 웹 포털 UI에서 알림을 열면 시스템이 알림을 생성하도록 유도한 지원 관찰을 볼 수 있습니다. 이러한 관찰을 통해 관련 엔터티에 대한 추가 컨텍스트(전송한 트래픽 포함) 및 외부

위협 인텔리전스(사용 가능한 경우)도 볼 수 있습니다. 또한 엔티티가 관련된 다른 관찰 및 알림을 보고 이 동작이 다른 잠재적인 악의적인 동작과 관련이 있는지 확인할 수 있습니다.

Secure Cloud Analytics에서 알림을 보고 닫을 때는 Secure Cloud Analytics UI의 트래픽을 허용하거나 차단할 수 없습니다. 디바이스를 액티브 모드로 구축한 경우에는 트래픽을 허용하거나 차단하도록 방화벽 액세스 제어 규칙을 업데이트하고, 패시브 모드에서 디바이스를 구축한 경우에는 방화벽 액세스 제어 규칙을 업데이트해야 합니다.

## 방화벽 이벤트 기반 알림 작업

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 워크플로우

알림의 워크플로우는 상태를 기반으로 합니다. 시스템에서 알림을 생성할 때 기본 상태는 Open(열림)이며 사용자가 할당되지 않습니다. Alerts(알림) 요약을 볼 때 즉시 문제가 되는 모든 열린 알림이 기본적으로 표시됩니다.

참고: **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 알림은 NetFlow에서 생성된 관찰, 방화벽 이벤트에서 생성된 관찰 또는 두 데이터 소스의 관찰을 기반으로 할 수 있습니다.

알림 요약을 검토할 때 알림에 대한 상태를 초기 분류로 할당, 태그 지정 및 업데이트할 수 있습니다. 필터 및 검색 기능을 사용하여 특정 알림을 찾거나, 다른 상태의 알림을 표시하거나, 다른 태그 또는 담당자와 연결할 수 있습니다. 알림의 상태를 스누즈로 설정할 수 있습니다. 이 경우 스누즈 기간이 경과할 때까지 미해결 알림 목록에 다시 나타나지 않습니다. 알림에서 스누즈 상태를 제거하여 미해결 알림으로 다시 표시할 수도 있습니다. 알림을 검토할 때 자신 또는 시스템의 다른 사용자에게 할당할 수 있습니다. 사용자는 사용자 이름에 할당된 모든 알림을 검색할 수 있습니다.

Alerts(알림) 요약에서 알림 상세정보 페이지를 볼 수 있습니다. 이 페이지에서는 이 알림을 생성한 지원 관찰에 대한 추가 컨텍스트 및 이 알림과 관련된 엔티티에 대한 추가 컨텍스트를 검토할 수 있습니다. 이 정보는 네트워크에서 문제를 추가로 조사하고 잠재적으로 악의적인 동작을 해결하기 위해 실제 문제를 정확히 찾아내는 데 도움이 될 수 있습니다.

Stealthwatch Cloud 웹 포털 UI, CDO 및 네트워크에서 조사할 때 결과를 설명하는 알림과 함께 코멘트를 남길 수 있습니다. 이렇게 하면 나중에 참조할 수 있는 연구 기록을 만드는 데 도움이 됩니다.

분석을 완료한 경우 상태를 Closed(닫힘)로 업데이트하고 더 이상 기본적으로 미결 알림으로 표시되지 않도록 할 수 있습니다. 상황이 바뀌면 나중에 닫힌 알림을 다시 열 수도 있습니다.

다음은 지정된 알림을 조사하는 방법에 대한 일반적인 지침 및 제안 사항입니다. Stealthwatch Cloud는 알림을 로깅할 때 추가 컨텍스트를 제공하므로 이 컨텍스트를 조사에 활용할 수 있습니다.

이러한 단계는 포괄적이거나 모든 것을 포함하지 않습니다. 이는 알림 조사를 시작하는 데 사용할 수 있는 일반적인 프레임워크를 제공할 뿐입니다.

일반적으로 알림을 검토할 때 다음 단계를 수행할 수 있습니다.

### 1. 열린 알림 분류, on page 698

2. 나중에 분석하기 위해 알림 일시 중지, on page 698
3. 추가 조사를 위해 알림 업데이트, on page 699
4. 알림 검토 및 조사 시작, on page 699
5. 엔터티 및 사용자 검사, on page 701
6. Secure Cloud Analytics를 사용하여 문제 해결, on page 702
7. 알림 업데이트 및 닫기, on page 703

## 열린 알림 분류

특히 둘 이상의 알림이 아직 조사되지 않은 경우, 미해결 알림을 분류합니다.

- CDO에서 SWC로 교차 실행하고 알림을 보는 방법에 대한 자세한 내용은 [CDO에서 Cisco Secure Cloud Analytics 알림 보기](#)을 참조하십시오.

다음 질문을 합니다.

- 이 알림 유형을 높은 우선순위로 구성했습니까?
- 영향을 받는 서브넷에 대해 높은 감도를 설정했습니까?
- 네트워크의 새 엔터티에서 발생하는 비정상적인 동작입니까?
- 엔터티의 일반적인 역할은 무엇이며 이 알림의 동작이 해당 역할과 어떻게 일치합니까?
- 이 엔터티의 정상적인 동작에서 예외적으로 벗어났습니까?
- 사용자가 관련된 경우, 이는 사용자의 예상된 동작입니까, 아니면 예외적인 것입니까?
- 보호되거나 민감한 데이터가 손상될 위험이 있습니까?
- 이 동작이 계속 허용되는 경우 네트워크에 미치는 영향은 어느 정도입니까?
- 외부 엔터티와 통신하는 경우, 이러한 엔터티가 과거에 네트워크의 다른 엔터티와 연결을 설정했습니까?

우선순위가 높은 알림인 경우 조사를 계속하기 전에 인터넷에서 엔터티를 격리하거나 연결을 닫는 것을 고려하십시오.

## 나중에 분석하기 위해 알림 일시 중지

다른 알림에 비해 우선 순위가 낮은 알림을 스누즈합니다. 예를 들어 조직에서 이메일 서버를 FTP 서버로 용도를 변경하고 시스템에서 긴급 프로파일 알림(엔터티의 현재 트래픽이 이전에 일치하지 않았던 행동 프로파일과 일치함을 나타냄)을 생성하는 경우 이 알림을 나중에 다시 확인할 수 있습니다. 스누즈된 알림은 열린 알림과 함께 표시되지 않습니다. 이러한 스누즈된 알림을 검토하려면 특별히 필터링해야 합니다.

알림 스누즈:



## Procedure

- 단계 1 **Close Alert**(알림 닫기)를 클릭합니다.
- 단계 2 **Snooze this alert**(이 알림 스누즈) 창의 드롭다운에서 스누즈 기간을 선택합니다.
- 단계 3 **Save**(저장)를 클릭합니다.

## What to do next

이러한 알림을 검토할 준비가 되면 다시 알림을 해제할 수 있습니다. 이렇게 하면 상태가 Open(열림)으로 설정되고 다른 Open(열림) 알림과 함께 알림이 표시됩니다.

스누즈된 알림의 스누즈를 해제합니다.

- 스누즈된 알림에서 **Unsnaze Alert**(알림 스누즈 해제)를 클릭합니다.

## 추가 조사를 위해 알림 업데이트

알림 세부 정보를 엽니다.

## Procedure

- 단계 1 **Monitor**(모니터링) > **Alerts**(알림)를 선택합니다.
- 단계 2 알림 유형 이름을 클릭합니다.

## What to do next

초기 분류 및 우선순위에 따라 알림을 할당하고 태그를 지정합니다.

- Assignee**(담당자) 드롭다운에서 사용자를 선택하여 알림을 할당하면 사용자가 조사를 시작할 수 있습니다.
- 드롭다운에서 하나 이상의 **Tags**(태그)를 선택하여 알림에 태그를 추가하여 향후 식별을 위해 알림을 더 잘 분류하고 알림에서 장기적 패턴을 설정합니다.
- 이 알림에 대한 코멘트를 입력한 다음 **Comment**(코멘트)를 클릭하여 초기 결과를 추적하고 알림에 할당된 사람을 지원하는 데 필요한 코멘트를 남깁니다. 알림은 시스템 코멘트와 사용자 코멘트를 모두 추적합니다.

## 알림 검토 및 조사 시작

할당된 알림을 검토하는 경우 알림 세부 정보를 검토하여 **Stealthwatch Cloud**에서 알림을 생성한 이유를 파악합니다. 지원 관찰을 검토하여 이러한 관찰이 소스 엔터티에 미치는 영향을 파악합니다.

경고가 방화벽 이벤트를 기반으로 생성된 경우, 시스템은 방화벽 구축이 이 경고의 소스임을 인식하지 않습니다.

이 소스 엔터티에 대한 모든 지원 관찰을 확인하여 일반 동작 및 패턴을 파악하고 이 활동이 더 긴 추세의 일부일 수 있는지 확인합니다.

프로시저

**단계 1** 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(↕)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.

**단계 2** **All Observations for Network**(네트워크에 대한 모든 관찰) 옆에 있는 화살표 아이콘(↕)을 클릭하여 이 알림의 소스 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

이러한 관찰에 대한 추가 분석을 수행하려면 쉽표로 구분된 값 파일로 지원 관찰을 다운로드합니다.

- 알림 세부 정보의 **Supporting Observations**(지원 관찰) 창에서 **CSV**를 클릭합니다.

관찰 결과에서 소스 엔터티 동작이 악의적인 동작을 나타내는지 확인합니다. 소스 엔터티가 여러 외부 엔터티와의 연결을 설정한 경우, 외부 엔터티가 어떤 식으로든 관련이 있는지 확인합니다(예: 모든 엔터티가 유사한 지리위치 정보를 가지고 있거나 해당 IP 주소가 동일한 서브넷에 있는지 여부).

소스 엔터티 IP 주소 또는 호스트 이름에서 소스 엔터티와 관련된 추가 컨텍스트를 확인합니다. 여기에는 관련될 수 있는 기타 알림 및 관찰, 디바이스 자체에 대한 정보, 전송 중인 세션 트래픽 유형이 포함됩니다.

- 엔터티와 관련된 모든 알림을 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Alerts**(알림)를 선택합니다.
- **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Observations**(관찰)를 선택하여 엔터티와 관련된 모든 관찰을 확인합니다.
- 디바이스에 대한 정보를 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Device**(디바이스)를 선택합니다.
- 이 엔터티와 관련된 세션 트래픽을 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic**(세션 트래픽)을 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy**(복사)를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 소스 엔터티는 항상 네트워크 내부에 있습니다. 이를 방화벽 이벤트의 Initiator IP(이니시어터 IP)와 비교해 보십시오. 이 IP는 연결을 시작한 엔터티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

관찰에서 다른 외부 엔터티에 대한 정보를 검토합니다. 지리위치 정보를 검토하고 지리위치 데이터 또는 Umbrella 데이터가 악성 엔터티를 식별하는지 확인합니다. 이러한 엔터티에 의해 생성된 트래픽을 확인합니다. Talos, AbuseIPDB 또는 Google에 이러한 엔터티에 대한 정보가 있는지 확인합니다. 여러 날짜의 IP 주소를 찾고 외부 엔터티가 네트워크의 엔터티와 설정한 다른 유형의 연결을 확인합

니다. 필요한 경우 이러한 내부 엔터티를 찾아 보안 침해 또는 의도하지 않은 행동의 증거가 있는지 확인합니다.

소스 엔터티가 연결을 설정한 외부 엔터티 IP 주소 또는 호스트 이름에 대한 컨텍스트를 검토합니다.

- 이 엔터티에 대한 최근 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **IP Traffic(IP 트래픽)**을 선택합니다.
- 이 엔터티에 대한 최근 세션 트래픽 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic(세션 트래픽)**을 선택합니다.
- **AbuseIPDB** 웹사이트에서 이 엔터티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 AbuseIPDB를 선택합니다.
- Cisco Umbrella 웹사이트에서 이 엔터티에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Cisco Umbrella**를 선택합니다.
- Google에서 이 IP 주소를 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Google Search(Google 검색)**를 선택합니다.
- Talos 웹사이트에서 이 정보에 대한 정보를 보려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Talos Intelligence**를 선택합니다.
- IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Add IP to watchlist(감시 목록에 IP 추가)**를 선택하여 이 엔터티를 감시 목록에 추가합니다.
- 이 엔터티의 지난 달 트래픽을 검색하려면 IP address or hostname(IP 주소 또는 호스트 이름) 드롭다운에서 **Find IP on multiple days(여러 날짜의 IP 찾기)**를 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy(복사)**를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 연결된 엔터티는 항상 네트워크 외부에 있습니다. 이를 방화벽 이벤트의 Responder IP(응답자 IP)와 비교해 보십시오. 이는 연결 요청에 응답한 엔터티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(코멘트)**를 클릭합니다.

## 엔터티 및 사용자 검사

Stealthwatch Cloud 포털 UI에서 알림을 검토한 후 소스 엔터티, 이 알림과 관련되었을 수 있는 사용자 및 기타 관련 엔터티에 대해 직접 추가 검사를 수행할 수 있습니다.

- 소스 엔터티가 물리적으로 또는 클라우드에서 네트워크의 어느 위치에 있는지 확인하고 직접 액세스합니다. 이 엔터티에 대한 로그 파일을 찾습니다. 네트워크의 물리적 엔터티인 경우 디바이스에 액세스하여 로그 정보를 검토하고 이 동작의 원인에 대한 정보가 있는지 확인합니다. 가상 엔터티이거나 클라우드에 저장된 경우 로그에 액세스하여 이 엔터티와 관련된 항목을 검색합니다. 무단 로그인, 승인되지 않은 구성 변경 등에 대한 자세한 내용은 로그를 검사합니다.

- 엔티티를 검사합니다. 엔티티 자체에서 악성코드 또는 취약성을 식별할 수 있는지 확인합니다. 조직에서 승인하지 않은 USB 스틱과 같이 디바이스에 대한 물리적 변경이 있는지를 포함하여 악의적인 변경이 있는지 확인합니다.
- 네트워크의 사용자 또는 네트워크 외부의 사용자가 관련되었는지 확인합니다. 가능한 경우 사용자에게 무엇을 하고 있었는지 물어봅니다. 사용자가 사용할 수 없는 경우, 액세스 권한이 있어야 했는지, 그리고 퇴사한 직원이 퇴사 전에 외부 서버에 파일을 업로드하는 등의 상황이 발생했는지 확인합니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(코멘트)**를 클릭합니다.

## Secure Cloud Analytics를 사용하여 문제 해결

악의적인 행동으로 인해 알림이 발생한 경우 악의적인 행동을 교정합니다. 예를 들면 다음과 같습니다.

- 악의적인 엔티티 또는 사용자가 네트워크 외부에서 로그인을 시도한 경우 엔티티 또는 사용자가 네트워크에 액세스하지 못하도록 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 엔티티가 무단 도메인 또는 악의적인 도메인에 액세스하려고 시도한 경우 영향을 받는 엔티티를 검사하여 악성코드가 원인인지 확인합니다. 악의적인 DNS 리디렉션이 있는 경우 네트워크의 다른 엔티티 또는 봇넷의 일부가 영향을 받는지 확인합니다. 사용자가 이러한 작업을 수행하려는 경우 방화벽 설정을 테스트하는 등 합법적인 이유가 있는지 확인합니다. 도메인에 대한 추가 액세스를 방지하려면 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 엔티티가 기록 엔티티 모델 동작과 다른 동작을 보이는 경우 동작 변경이 의도된 것인지 확인합니다. 의도하지 않은 작업인 경우 네트워크의 다른 권한이 있는 사용자가 변경을 담당하는지 확인합니다. 의도하지 않은 동작이 네트워크 외부의 엔티티와의 연결과 관련된 경우 이를 해결하기 위해 방화벽 규칙 및 방화벽 구성을 업데이트합니다.
- 취약성 또는 익스플로잇을 식별한 경우, 영향을 받는 엔티티를 업데이트 또는 패치하여 취약성을 제거하거나 무단 액세스를 방지하도록 방화벽 구성을 업데이트합니다. 네트워크의 다른 엔티티가 유사하게 영향을 받을 수 있는지 확인하고 해당 엔티티에 동일한 업데이트 또는 패치를 적용합니다. 현재 취약성 또는 익스플로잇에 수정 사항이 없는 경우 해당 벤더에 문의하십시오.
- 악성코드가 확인되면 엔티티를 격리하고 악성코드를 제거합니다. 방화벽 파일 및 악성코드 이벤트를 검토하여 네트워크의 다른 엔티티가 위험에 노출되어 있는지 확인하고, 이 악성코드가 확산되지 않도록 엔티티를 격리 및 업데이트합니다. 이 악성코드 또는 이 악성코드를 유발한 엔티티에 대한 정보로 보안 인텔리전스를 업데이트합니다. 향후 이 악성코드가 네트워크를 감염시키는 것을 방지하려면 방화벽 액세스 제어와 파일 및 악성코드 규칙을 업데이트하십시오. 필요에 따라 벤더에 알립니다.
- 악의적인 행동으로 인해 데이터가 유출된 경우 무단 소스로 전송되는 데이터의 특성을 확인합니다. 무단 데이터 유출에 대한 조직의 프로토콜을 따르십시오. 이 소스에 의한 향후 데이터 유출 시도를 방지하려면 방화벽 구성을 업데이트하십시오.

## 알림 업데이트 및 닫기

결과에 따라 태그를 추가합니다.

### Procedure

단계 1 Secure Cloud Analytics 포털 UI에서 **Monitor**(모니터링) > **Alerts**(알림)를 선택합니다.

단계 2 드롭다운에서 하나 이상의 **Tags**(태그)를 선택합니다.

조사 결과 및 수행한 교정 단계를 설명하는 최종 코멘트를 추가합니다.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment**(코멘트)를 클릭합니다.

알림을 닫고 유용하거나 도움이 되지 않음으로 표시합니다.

1. 알림 세부 정보에서 **Close Alert**(알림 닫기)를 클릭합니다.
2. 알림이 도움이 되었으면 **Yes**(예)를 선택하고, 알림이 도움이 되지 않았다면 **No**(아니요)를 선택합니다. 이는 알림이 악의적인 행동으로 인해 발생했음을 의미하는 것이 아니라 해당 알림이 조직에 도움이 되었음을 의미합니다.
3. **Save**(저장)를 클릭합니다.

### What to do next

#### 종료된 알림 다시 열기

종료된 알림과 관련된 추가 정보를 발견하거나 알림과 관련된 코멘트를 더 추가하려는 경우 알림을 다시 열어 상태를 **Open**(열림)으로 변경할 수 있습니다. 그런 다음 필요에 따라 알림을 변경한 다음 추가 조사가 완료되면 알림을 닫을 수 있습니다.

종료된 알림을 다시 엽니다.

- 닫힌 알림의 세부 사항에서 **Reopen Alert**(알림 다시 열기)를 클릭합니다.

## 알림 우선순위 수정

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 유형은 기본 우선순위와 함께 제공되며, 이는 시스템이 이 유형의 알림 생성에 대한 민감도에 영향을 미칩니다. 알림은 기본적으로 Cisco 인텔리전스 및 기타 요인에 따라 낮음 또는 보통으로 설정됩니다. 네트워크 환경에 따라 알림 유형의 우선순위를 다시 지정하여 우려되는 특정 알림을 강조할 수 있습니다. 모든 알림 유형을 낮음, 보통 또는 높음 우선순위로 구성할 수 있습니다.

- **Monitor**(모니터링) > **Alerts**(알림)를 선택합니다.

- Settings(설정) 드롭다운 아이콘(☰)을 클릭한 다음 **Alert Types and Priorities**(알림 유형 및 우선 순위)를 선택합니다.
- 알림 유형 옆에 있는 편집 아이콘(✎)을 클릭하고 낮음, 중간 또는 높음을 선택하여 우선순위를 변경합니다.

## 라이브 이벤트 보기

Live events(라이브 이벤트) 페이지에는 입력한 **이벤트 로깅 페이지에서 이벤트 검색 및 필터링**과 일치하는 최신 500개의 이벤트가 표시됩니다. 라이브 이벤트 페이지에 최대 500개의 이벤트가 표시되고 더 많은 이벤트가 스트리밍되는 경우, CDO는 최신 라이브 이벤트를 표시하고 가장 오래된 라이브 이벤트를 기록 이벤트 페이지로 전송하여 총 라이브 이벤트 수를 500개로 유지합니다. 이 전송을 수행하는 데 약 1분이 걸립니다. 필터링 기준이 추가되지 않은 경우, 이벤트를 로깅하도록 구성된 규칙에 의해 생성된 모든 최신 라이브 500 이벤트가 표시됩니다.

이벤트의 타임스탬프는 이벤트를 보는 CDO 관리자의 현지 시간으로 표시됩니다.

라이브 이벤트가 재생 중인지 일시 중지되었는지에 상관없이 필터링 기준을 변경하면 이벤트 화면이 지워지고 수집 프로세스가 다시 시작됩니다.

CDO 이벤트 뷰어에서 라이브 이벤트를 보려면 다음을 수행합니다.

### Procedure

단계 1 탐색창에서 분석 > 이벤트 로깅을 선택합니다.

단계 2 **Live**(라이브) 탭을 클릭합니다.



### What to do next

이벤트를 재생하고 일시 중지하는 방법을 참조하십시오.

관련 정보:

- [라이브 이벤트 재생/일시 중지, on page 704](#)
- [과거 이벤트 보기, on page 705](#)
- [이벤트 보기 사용자 지정, on page 706](#)

## 라이브 이벤트 재생/일시 중지

라이브 이벤트가 스트리밍될 때 라이브 이벤트를 "재생"  또는 "일시 중지"  할 수 있습니다. 라이브 이벤트가 "재생" 중인 경우 CDO는 이벤트 뷰어에 지정된 필터링 기준과 일치하는 이벤트를 수신된 순서대로 표시합니다. 이벤트가 일시 중지된 경우 CDO는 라이브 이벤트 재생을 다시 시작할 때까지 라이브 이벤트 페이지를 업데이트하지 않습니다. 이벤트 재생을 다시 시작하면 CDO는 이벤

트 재생을 다시 시작한 시점부터 Live(라이브) 페이지에 이벤트를 채우기 시작합니다. 누락된 항목은 다시 채우지 않습니다.

라이브 이벤트 스트리밍을 재생하거나 일시 중지했는지 여부에 관계없이 CDO가 수신한 모든 이벤트를 보려면 Historical(기록) 탭을 클릭합니다.

#### 라이브 이벤트 자동 일시 중지

약 5분 동안 이벤트를 표시한 후 CDO는 라이브 이벤트의 스트림을 일시 중지한다고 경고합니다. 이때 링크를 클릭하여 다른 5분 동안 라이브 이벤트 스트리밍을 계속하거나 스트림을 중지할 수 있습니다. 준비가 되면 라이브 이벤트 스트림을 다시 시작할 수 있습니다.

#### 이벤트 수신 및 보고

라이브 이벤트 뷰어에서 SEC(Secure Event Connector) 수신 이벤트와 CDO 계시 이벤트 사이에 약간의 지연이 발생할 수 있습니다. Live(라이브) 페이지에서 간격을 볼 수 있습니다. 이벤트의 타임스탬프는 SEC에서 이벤트를 수신한 시간입니다.

Events

Y Q Search by event fields and values

Historical
Live

	Date/Time	Event Type
⚙️ Waiting for matching events after 1:38:40 PM.		
+	May 31, 2019 1:33:35 PM	Connection
+	May 31, 2019 1:33:36 PM	Connection
+	May 31, 2019 1:33:44 PM	Connection

## 과거 이벤트 보기

Live events(라이브 이벤트) 페이지에는 입력한 이벤트 로깅 페이지에서 이벤트 검색 및 필터링과 일치하는 최신 500개의 이벤트가 표시됩니다. 가장 최근의 500개 이벤트보다 오래된 이벤트는 기록 이벤트 테이블로 전송됩니다. 이 전송을 수행하는 데 약 1분이 걸립니다. 그런 다음 저장한 모든 이벤트를 필터링하여 원하는 이벤트를 찾을 수 있습니다.

과거 이벤트를 보려면:

#### Procedure

- 단계 1 탐색창에서 분석 > 이벤트 로깅을 선택합니다.
- 단계 2 기록 탭을 클릭합니다. 기본적으로 기록 이벤트 테이블을 열면 지난 1시간 내에 수집된 이벤트가 표시되도록 필터가 설정됩니다.

이벤트 속성은 FDM(Firepower Device Manager) 또는 ASDM(Adaptive Security Device Manager)에서 보고하는 것과 거의 동일합니다.

- Firepower Threat Defense 이벤트 속성에 대한 전체 설명은 [Cisco FTD 시스템 로그 메시지를 참조 하십시오.](#)
- ASA 이벤트 속성에 대한 전체 설명은 [Cisco ASA Series 시스템 로그 메시지를 참조 하십시오.](#)


## 이벤트 보기 사용자 지정

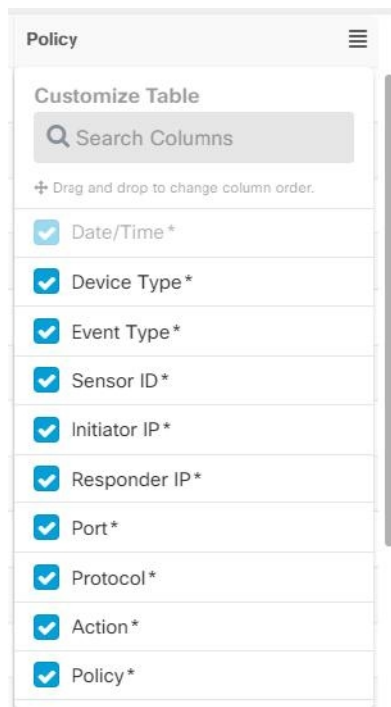
Event Logging(이벤트 로깅) 페이지에 대한 모든 변경 사항은 이 페이지에서 빠져나왔다가 나중에 다시 돌아올 때를 위해 자동으로 저장됩니다.



**Note** 라이브 및 기록 이벤트 보기의 구성은 동일합니다. 이벤트 보기를 사용자 정의하면 이러한 변경 사항이 Live(라이브) 및 Historical(기록) 보기에 모두 적용됩니다.

### 열


원하는 보기에 적용되는 열 헤더만 포함하도록 라이브 및 기록 이벤트에 대한 이벤트 보기를 수정할 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘  을 클릭하고 원하는 열을 선택하거나 선택 취소합니다.





별표가 있는 열은 언제든지 제거할 수 있지만 기본적으로 이벤트 테이블 내에 제공됩니다. 검색 창을 사용하여 포함할 추가 열에 대한 키워드를 수동으로 검색합니다.

순서

Events(이벤트) 보기의 열 순서를 바꿀 수 있습니다. 열 오른쪽에 있는 열 필터 아이콘  을 클릭하여 선택한 열 목록을 확장하고 원하는 순서로 열을 수동으로 끌어서 놓습니다. 여기서 드롭다운 메뉴의 목록 맨 위에 있는 열은 이벤트 보기에서 맨 왼쪽에 있는 열입니다.

관련 정보:


- [이벤트 로깅 페이지에서 이벤트 검색 및 필터링](#)
- [Security Analytics and Logging의 이벤트 속성](#)

## 이벤트 로깅 페이지의 열 표시 및 숨기기

Event Logging(이벤트 로깅) 페이지에는 구성된 ASA 및 FDM 관리 디바이스에서 Cisco Cloud로 전송된 ASA 및 FTD Syslog 이벤트 및 ASA NSEL(NetFlow Secure Event Logging) 이벤트가 표시됩니다.

테이블과 함께 Show/Hide(표시/숨기기) 위젯을 사용하여 Event Logging(이벤트 로깅) 페이지에서 열을 표시하거나 숨길 수 있습니다.

### Procedure

- 단계 1 CDO 탐색 모음에서 분석 > 이벤트 로깅을 선택합니다.
- 단계 2 테이블의 맨 오른쪽으로 스크롤하여 **Show/Hide Columns**(열 표시/숨기기) 버튼  를 클릭합니다.
- 단계 3 표시하려는 열을 선택하고, 숨기려는 열을 선택 취소합니다.
- 단계 4 Show/Hide Columns(열 표시/숨기기) 드롭다운 메뉴의 열 이름 위에 마우스를 올려 놓고 회색 십자 표시를 눌러 열 순서를 다시 정렬합니다.

테넌트에 로그인하는 다른 사용자는 열이 다시 표시되거나 숨겨질 때까지 표시하도록 선택한 것과 동일한 열을 볼 수 있습니다.

이 표에서는 열 헤더에 대해 설명합니다.

열 헤더	설명
날짜/시간	디바이스가 이벤트를 생성한 시간 시간은 컴퓨터의 로컬 시간으로 표시됩니다.
디바이스 유형	또는 FTD(Firepower Threat Defense)

열 헤더	설명
이벤트 유형	<p>이 복합 열에는 다음 중 하나가 포함될 수 있습니다.</p> <ul style="list-style-type: none"> <li>• <b>FTD 이벤트 유형</b> <ul style="list-style-type: none"> <li>• <b>Connection(연결)</b> - 액세스 제어 규칙의 연결 이벤트를 표시합니다.</li> <li>• <b>File(파일)</b> - 액세스 제어 규칙의 파일 정책에 의해 보고된 이벤트를 표시합니다.</li> <li>• <b>Intrusion(침입)</b> - 액세스 제어 규칙의 침입 정책에 의해 보고된 이벤트를 표시합니다.</li> <li>• <b>Malware(악성코드)</b> - 액세스 제어 규칙의 악성코드 정책에 의해 보고된 이벤트를 표시합니다.</li> </ul> </li> <li>• <b>ASAEvent Types(이벤트 유형)</b> - 이러한 이벤트 유형은 Syslog 또는 NetFlow 이벤트의 그룹을 나타냅니다. 어떤 Syslog ID 또는 어떤 NetFlow ID가 어떤 그룹에 포함되어 있는지에 대한 자세한 내용은 <a href="#">ASA 이벤트 유형</a>을 참조하십시오. <ul style="list-style-type: none"> <li>• <b>구문 분석된 이벤트</b> - 구문 분석된 Syslog 이벤트는 다른 Syslog 이벤트보다 더 많은 이벤트 속성을 포함하며, CDO는 이러한 속성을 기반으로 더 빠르게 검색 결과를 반환할 수 있습니다. 구문 분석된 이벤트는 필터링 카테고리가 아닙니다. 그러나 구문 분석된 이벤트 ID는 Event Types(이벤트 유형) 열에 기울임꼴로 표시됩니다. 기울임꼴로 표시되지 않은 이벤트 ID는 구문 분석되지 않습니다.</li> <li>• <b>ASA NetFlow Event IDs(NetFlow 이벤트 ID)</b>: ASA의 모든 <a href="#">Netflow(NSEL) 이벤트</a>가 여기에 표시됩니다.</li> </ul> </li> </ul>
센서 ID	<p>센서 ID는 이벤트가 보안 이벤트 커넥터로 전송되는 IP 주소입니다. 이는 일반적으로 Firepower Threat Defense 또는 ASA의 관리 인터페이스입니다.</p>

열 헤더	설명
초기자 IP	이는 네트워크 트래픽 소스의 IP 주소입니다. Initiator address(이니시에이터 주소) 필드의 값은 이벤트 세부사항의 InitiatorIP(이니시에이터 IP) 필드 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
응답기 IP	이것은 패킷의 대상 IP 주소입니다. Destination address(대상 주소) 필드의 값은 이벤트 세부사항의 ResponderIP 필드에 있는 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
포트	세션 responder가 사용하는 포트 또는 ICMP 코드 대상 포트의 값은 이벤트 세부사항의 ResponderPort 값에 해당합니다.
프로토콜	이벤트의 프로토콜을 나타냅니다.

열 헤더	설명
작업	<p>규칙에 의해 정의된 보안 작업을 지정합니다. 입력하는 값은 찾으려는 값과 정확히 일치해야 합니다. 그러나 대/소문자는 중요하지 않습니다. 연결, 파일, 침입, 악성코드, Syslog 및 NetFlow 이벤트 유형에 대해 서로 다른 값을 입력합니다.</p> <ul style="list-style-type: none"> <li>• 연결 이벤트 유형의 경우 필터는 AC_RuleAction 특성에서 일치 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.</li> <li>• 파일 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.</li> <li>• 침입 이벤트 유형의 경우 필터는 InLineResult 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allowed(허용됨), Blocked(차단됨), Trusted(신뢰할 수 있음)일 수 있습니다.</li> <li>• 악성코드 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Cloud Lookup Timeout(클라우드 조회 시간 초과)일 수 있습니다.</li> <li>• Syslog 및 NetFlow 이벤트 유형의 경우 필터는 Action(작업) 속성에서 일치하는 항목을 검색합니다.</li> </ul>
정책	이벤트를 트리거한 정책의 이름입니다. ASA 및 FDM 관리디바이스의 이름은 다릅니다.

관련 정보:

[이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 742](#)

## 사용자 지정 가능한 이벤트 필터

SaaS(Secure Logging Analytics) 고객은 자주 사용하는 맞춤형 필터를 생성하고 저장할 수 있습니다.

필터의 요소는 구성할 때 필터 탭에 저장됩니다. Event Logging(이벤트 로깅) 페이지로 돌아갈 때마다 이러한 검색을 사용할 수 있습니다. 테넌트의 다른 CDO 사용자는 사용할 수 없습니다. 둘 이상의 테넌트를 관리하는 경우 다른 테넌트에서는 사용할 수 없습니다.



**Note** 필터 탭에서 작업할 때 필터 기준을 수정하면 해당 변경 사항이 사용자 지정 필터 탭에 자동으로 저장됩니다.

### Procedure

단계 1 주 메뉴에서 분석 > 이벤트 로깅을(를) 선택합니다.

단계 2 모든 값의 Search(검색) 필드를 지웁니다.

단계 3 이벤트 테이블 위에서 파란색 더하기 버튼을 클릭하여 View(보기) 탭을 추가합니다. 필터 보기에는 이름을 지정할 때까지 "View 1", "View 2", "View 3" 등의 레이블이 지정됩니다.



단계 4 View(보기) 탭을 선택합니다.

단계 5 필터 표시줄을 열고 맞춤형 필터에서 원하는 필터 속성을 선택합니다. [이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 742](#)의 내용을 참조하십시오. 필터 특성만 맞춤형 필터에 저장됩니다.

단계 6 이벤트 로깅 테이블에 표시할 열을 사용자 정의합니다. 열 표시 및 숨기기에 대한 설명은 [이벤트 로깅 페이지의 열 표시 및 숨기기, on page 707](#)의 내용을 참조하십시오.

단계 7 "View X" 레이블이 있는 필터 탭을 두 번 클릭하고 이름을 바꿉니다.

단계 8 (선택 사항) 맞춤형 필터를 생성했으므로 이제 Search(검색) 필드에 검색 기준을 추가하여 맞춤형 필터를 변경하지 않고도 Event Logging(이벤트 로깅) 페이지에 표시되는 결과를 미세 조정할 수 있습니다. [이벤트 로깅 페이지에서 이벤트 검색 및 필터링, on page 742](#)의 내용을 참조하십시오.

## Security Analytics and Logging의 이벤트 속성

### 이벤트 속성 설명

CDO에서 사용하는 이벤트 속성은 FDM(Firepower Device Manager) 또는 ASDM(Adaptive Security Device Manager)에서 보고하는 것과 거의 동일합니다.

- FDM 매니지드 디바이스 이벤트 속성에 대한 전체 설명은 [Cisco Firepower Threat Defense 시스템 그 메시지](#)를 참조하십시오.

일부 ASA 시스템 로그 이벤트는 "구문 분석"되며, 다른 이벤트에는 속성:값 쌍을 사용하여 이벤트 로깅 테이블의 내용을 필터링할 때 사용할 수 있는 추가 속성이 있습니다. 시스템 로그 이벤트의 다른 중요한 속성은 다음 추가 항목을 참조하십시오.

- 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성
- Syslog 이벤트에 대한 이벤트 이름 속성

- 시스템 로그 이벤트의 시간 속성

## 일부 시스템 로그 메시지에 대한 EventGroup 및 EventGroupDefinition 속성

일부 시스템 로그 이벤트에는 추가 속성 "EventGroup" 및 "EventGroupDefinition"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 이러한 추가 속성을 사용하여 이벤트 테이블을 필터링할 수 있습니다. 예를 들어 Event Logging(이벤트 로깅) 테이블의 검색 필드에 apfw:415\*를 입력하여 애플리케이션 방화벽 이벤트를 필터링할 수 있습니다.

Syslog 메시지 클래스와 연결된 메시지 ID 번호

EventGroup	EventGroupDefinition	시스템 로그 메시지 ID 번호(처음 3자리)
aaa/auth	사용자 인증	109, 113
acl/session	액세스 목록/사용자 세션	106
apfw	애플리케이션 방화벽	415
bridge	투명한 방화벽	110, 220
ca	PKI 인증 기관	717
citrix	Citrix 클라이언트	723
clst	클러스터링	747
cmgr	카드 관리	323
config	CLI(Command Line Interface)	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	Dynamic Access Policy	734
eap, eapoudp	Network Admission Control용 EAPoUDP 또는 EAP	333, 334
eigrp	EIGRP 라우팅	336
email	이메일 프록시	719
ipaa/envmon	환경 모니터링	735
HA	페일오버	101, 102, 103, 104, 105, 210, 311, 709
idfw	ID 기반 방화벽	746
ids	Intrusion Detection System(침입 탐지 시스템)	733

EventGroup	EventGroupDefinition	시스템 로그 메시지 ID 번호(처음 3자리)
ids/ips	침입 탐지 시스템/침입 방지 시스템	400
ikev2	IKEv2 툴킷	750, 751, 752
ip	IP 스택	209, 215, 313, 317, 408
ipaa	IP 주소 할당	735
ips	Intrusion Protection System(침입 방지 시스템)	401, 420
ipv6	IPv6	325
l4tm	차단 목록, 허용 목록, 그레이리스트	338
lic	라이선싱	444
mdm-proxy	MDM 프록시	802
nac	NAC(Network Admission Control)	731, 732
vpn/nap	IKE 및 IPsec/네트워크 액세스 포인트	713
np	네트워크 프로세서	319
ospf	OSPF 라우팅	318, 409, 503, 613
passwd	비밀번호 암호화	742
PP	전화 프록시	337
rip	RIP 라우팅	107, 312
rm	리소스 관리자	321
sch	Smart Call Home	120
session	사용자 세션	108, 201, 202, 204, 302, 303, 304, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
session/natpat	사용자 세션/NAT 및 PAT	305
snmp	SNMP	212
ssafe	ScanSafe	775
ssl/np ssl	SSL 스택/NP SSL	725
svc	SSL VPN 클라이언트	722

EventGroup	EventGroupDefinition	시스템 로그 메시지 ID 번호(처음 3자리)
sys	시스템	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711, 741
tre	트랜잭션 규칙 엔진	780
ucime	UC-IME	339
tag-switching	서비스 태그 스위칭	779
td	위협 탐지	733
VM	VLAN 매핑	730
vpdn	PPTP 및 L2TP 세션	213, 403, 603
vpn	IKE 및 IPSEC	316, 320, 404, 501, 602, 402
vpnc	VPN 클라이언트	611
vpnfo	VPN 페일오버	720
vpnlb	VPN 로드 밸런싱	718
vxlan	VXLAN	778
webfo	WebVPN 페일오버	721
webvpn	WebVPN 및 AnyConnect Client	716
session/natpat	사용자 세션/NAT 및 PAT	305

## Syslog 이벤트에 대한 이벤트 이름 속성

일부 시스템 로그 이벤트에는 추가 속성 "EventName"이 있습니다. attribute:value 쌍을 기준으로 필터링하여 EventName 특성을 사용하여 이벤트 테이블을 필터링하여 찾을 수 있습니다. 예를 들어 Event Logging(이벤트 로깅) 테이블의 검색 필드에 **EventName:"Denied IP Packet"**을 입력하여 "Denied IP packet(거부된 IP 패킷)"에 대한 이벤트를 필터링할 수 있습니다.

시스템 로그 이벤트 ID 및 이벤트 이름 테이블

- AAA 시스템 로그 이벤트 ID 및 이벤트 이름
- 봇넷 시스템 로그 이벤트 ID 및 이벤트 이름
- 페일오버 시스템 로그 이벤트 ID 및 이벤트 이름
- 방화벽 거부 시스템 로그 이벤트 ID 및 이벤트 이름
- 방화벽 트래픽 시스템 로그 이벤트 ID 및 이벤트 이름
- ID 기반 방화벽 시스템 로그 이벤트 ID 및 이벤트 이름



- IPSec 시스템 로그 이벤트 ID 및 이벤트 이름
- NAT 시스템 로그 이벤트 ID 및 이벤트 이름
- SSL VPN 시스템 로그 이벤트 ID 및 이벤트 이름

#### AAA 시스템 로그 이벤트 ID 및 이벤트 이름

이벤트 ID	이벤트 이름
109001	AAA Begin
109002	AAA Failed
109003	AAA Server Failed
109005	Authentication Success
109006	Authentication Failed
109007	Authorization Success
109008	Authorization Failed
109010	AAA Pending
109011	AAA Session Started
109012	AAA Session Ended
109013	AAA
109014	AAA Failed
109016	AAA ACL not found
109017	AAA Limit Reach
109018	AAA ACL Empty
109019	AAA ACL error
109020	AAA ACL error
109021	AAA error
109022	AAA HTTP limit reached
109023	AAA auth required
109024	Authorization Failed
109025	Authorization Failed
109026	AAA error
109027	AAA Server error

이벤트 ID	이벤트 이름
109028	AAA Bypassed
109029	AAA ACL error
109030	AAA ACL error
109031	Authentication Failed
109032	AAA ACL error
109033	Authentication Failed
109034	Authentication Failed
109035	AAA Limit Reach
113001	AAA Session limit reach
113003	AAA overridden
113004	AAA Successful
113005	Authorization Rejected
113006	AAA user locked
113007	AAA User unlocked
113008	AAA successful
113009	AAA retrieved
113010	AAA Challenge received
113011	AAA retrieved
113012	Authentication Successful
113013	AAA error
113014	AAA error
113015	Authentication Rejected
113016	AAA Rejected
113017	AAA Rejected
113018	AAA ACL error
113019	AAA Disconnected
113020	AAA error
113021	AAA Logging Fail

이벤트 ID	이벤트 이름
113022	AAA Failed
113023	AAA reactivated
113024	AAA Client certification
113025	AAA Authentication fail
113026	AAA error
113027	AAA error

봇넷 시스템 로그 이벤트 ID 및 이벤트 이름

이벤트 ID	이벤트 이름
338001	Botnet Source Block List
338002	Botnet Destination Block List
338003	Botnet Source Block List
338004	Botnet Destination Block List
338101	Botnet Source Allow List
338102	Botnet destination Allow List
338202	Botnet destination Grey
338203	Botnet Source Grey
338204	Botnet Destination Grey
338301	Botnet DNS Intercepted
338302	Botnet DNS
338303	Botnet DNS
338304	Botnet Download successful
338305	Botnet Download failed
338306	Botnet Authentication failed
338307	Botnet Decrypt failed
338308	Botnet Client
338309	Botnet Client
338310	Botnet dyn filter failed

## 페일오버 시스템 로그 이벤트 ID 및 이벤트 이름

이벤트 ID	이벤트 이름
101001	Failover Cable OK
101002	Failover Cable BAD
101003	Failover Cable not connected
101004	Failover Cable not connected
101005	Failover Cable reading error
102001	Failover Power failure
103001	No response from failover mate
103002	Failover mate interface OK
103003	Failover mate interface BAD
103004	Failover mate reports failure
103005	Failover mate reports self failure
103006	Failover version incompatible
103007	Failover version difference
104001	Failover role switch
104002	Failover role switch
104003	Failover unit failed
104004	Failover unit OK
106100	Permit/Denied by ACL
210001	Stateful Failover error
210002	Stateful Failover error
210003	Stateful Failover error
210005	Stateful Failover error
210006	Stateful Failover error
210007	Stateful Failover error
210008	Stateful Failover error
210010	Stateful Failover error
210020	Stateful Failover error

이벤트 ID	이벤트 이름
210021	Stateful Failover error
210022	Stateful Failover error
311001	Stateful Failover update
311002	Stateful Failover update
311003	Stateful Failover update
311004	Stateful Failover update
418001	Denied Packet to Management
709001	Failover replication error
709002	Failover replication error
709003	Failover replication start
709004	Failover replication complete
709005	Failover receive replication start
709006	Failover receive replication complete
709007	Failover replication failure
710003	Denied access to Device

방화벽 거부 시스템 로그 이벤트 ID 및 이벤트 이름

이벤트 ID	이벤트 이름
106001	Denied by Security Policy
106002	Outbound Deny
106006	Denied by Security Policy
106007	Denied Inbound UDP
106008	Denied by Security Policy
106010	Denied by Security Policy
106011	Denied Inbound
106012	Denied due to Bad IP option
106013	Dropped Ping to PAT IP
106014	Denied Inbound ICMP

이벤트 ID	이벤트 이름
106015	Denied by Security Policy
106016	Denied IP Spoof
106017	Denied due to Land Attack
106018	Denied outbound ICMP
106020	Denied IP Packet
106021	Denied TCP
106022	Denied Spoof packet
106023	Denied IP Packet
106025	Dropped Packet failed to Detect context
106026	Dropped Packet failed to Detect context
106027	Dropped Packet failed to Detect context
106100	Permit/Denied by ACL
418001	Denied Packet to Management
710003	Denied access to Device

방화벽 트래픽 시스템 로그 이벤트 ID 및 이벤트 이름

이벤트 ID	이벤트 이름
108001	Inspect SMTP
108002	Inspect SMTP
108003	Inspect ESMTP Dropped
108004	Inspect ESMTP
108005	Inspect ESMTP
108006	Inspect ESMTP Violation
108007	Inspect ESMTP
110002	No Router found
110003	Failed to Find Next hop
209003	Fragment Limit Reach
209004	Fragment invalid Length

이벤트 ID	이벤트 이름
209005	Fragment IP discard
302003	H245 Connection Start
302004	H323 Connection start
302009	Restart TCP
302010	Connection USAGE
302012	H225 CALL SIGNAL CONN
302013	Built TCP
302014	Teardown TCP
302015	Built UDP
302016	Teardown UDP
302017	Built GRE
302018	Teardown GRE
302019	H323 Failed
302020	Built ICMP
302021	Teardown ICMP
302022	Built TCP Stub
302023	Teardown TCP Stub
302024	Built UDP Stub
302025	Teardown UDP Stub
302026	Built ICMP Stub
302027	Teardown ICMP Stub
302033	Connection H323
302034	H323 Connection Failed
302035	Built SCTP
302036	Teardown SCTP
303002	FTP file download/upload
303003	Inspect FTP Dropped
303004	Inspect FTP Dropped

이벤트 ID	이벤트 이름
303005	Inspect FTP reset
313001	ICMP Denied
313004	ICMP Drop
313005	ICMP Error Msg Drop
313008	ICMP ipv6 Denied
324000	GTP Pkt Drop
324001	GTP Pkt Error
324002	Memory Error
324003	GTP Pkt Drop
324004	GTP Version 지원하지 않음
324005	GTP Tunnel Failed
324006	GTP Tunnel Failed
324007	GTP Tunnel Failed
337001	Phone Proxy SRTP Failed
337002	Phone Proxy SRTP Failed
337003	Phone Proxy SRTP Auth Fail
337004	Phone Proxy SRTP Auth Fail
337005	Phone Proxy SRTP no Media Session
337006	Phone Proxy TFTP Unable to Create File
337007	Phone Proxy TFTP Unable to Find File
337008	Phone Proxy Call Failed
337009	Phone Proxy Unable to Create Phone Entry
400000	IPS IP options-Bad Option List
400001	IPS IP options-Record Packet Route
400002	IPS IP options-Timestamp
400003	IPS IP options-Security
400004	IPS IP options-Loose Source Route
400005	IPS IP options-SATNET ID



이벤트 ID	이벤트 이름
400006	IPS IP options-Strict Source Route
400007	IPS IP Fragment Attack
400008	IPS IP Impossible Packet
400009	IPS IP Fragments Overlap
400010	IPS ICMP Echo Reply
400011	IPS ICMP Host Unreachable
400012	IPS ICMP Source Quench
400013	IPS ICMP Redirect
400014	IPS ICMP Echo Request
400015	IPS ICMP Time Exceeded for a Datagram
400017	IPS ICMP Timestamp Request
400018	IPS ICMP Timestamp Reply
400019	ICMP Information Request
400020	IPS ICMP Information Reply
400021	ICMP Address Mask Request
400022	ICMP Address Mask Request
400023	IPS Fragmented ICMP Traffic
400024	IPS Large ICMP Traffic
400025	IPS Ping of Death Attack
400026	IPS TCP NULL flags
400027	IPS TCP SYN+FIN flags
400028	IPS TCP FIN only flags
400029	IPS FTP Improper Address Specified
400030	IPS FTP Improper Port Specified
400031	IPS UDP Bomb attack
400032	IPS UDP Snork attack
400033	IPS UDP Chargen DoS attack
400034	IPS DNS HINFO Request

이벤트 ID	이벤트 이름
400035	IPS DNS Zone Transfer
400036	IPS DNS Zone Transfer from High Port
400037	IPS DNS Request for All Records
400038	IPS RPC Port Registration
400039	IPS RPC Port Unregistration
400040	IPS RPC Dump
400041	IPS Proxied RPC Request
400042	IPS YP server Portmap Request
400043	IPS YP bind Portmap Request
400044	IPS YP password Portmap Request
400045	IPS YP update Portmap Request
400046	IPS YP transfer Portmap Request
400047	IPS Mount Portmap Request
400048	IPS Remote execution Portmap Request
400049	IPS Remote execution Attempt
400050	IPS Statd Buffer Overflow
406001	Inspect FTP Dropped
406002	Inspect FTP Dropped
407001	Host Limit Reach
407002	Embryonic limit Reached
407003	Established limit Reached
415001	Inspect Http Header Field Count
415002	Inspect Http Header Field Length
415003	Inspect Http body Length
415004	Inspect Http content-type
415005	Inspect Http URL length
415006	Inspect Http URL Match
415007	Inspect Http Body Match

이벤트 ID	이벤트 이름
415008	Inspect Http Header match
415009	Inspect Http Method match
415010	Inspect transfer encode match
415011	Inspect Http Protocol Violation
415012	Inspect Http Content-type
415013	Inspect Http Malformed
415014	Inspect Http Mime-Type
415015	Inspect Http Transfer-encoding
415016	Inspect Http Unanswered
415017	Inspect Http Argument match
415018	Inspect Http Header length
415019	Inspect Http status Matched
415020	Inspect Http non-ASCII
416001	Inspect SNMP dropped
419001	Dropped packet
419002	Duplicate TCP SYN
419003	Packet modified
424001	Denied IP Packet
424002	Dropped Packet
431001	Dropped RTP
431002	Dropped RTCP
500001	Inspect ActiveX
500002	Inspect Java
500003	Inspect TCP Header
500004	Inspect TCP Header
500005	Inspect Connection Terminated
508001	Inspect DCERPC Dropped
508002	Inspect DCERPC Dropped

이벤트 ID	이벤트 이름
509001	Prevented No Forward Cmd
607001	Inspect SIP
607002	Inspect SIP
607003	Inspect SIP
608001	Inspect Skinny
608002	Inspect Skinny dropped
608003	Inspect Skinny dropped
608004	Inspect Skinny dropped
608005	Inspect Skinny dropped
609001	Built Local-Host
609002	Teardown Local Host
703001	H225 Unsupported Version
703002	H225 Connection
726001	Inspect Instant Message

**ID** 기반 방화벽 시스템 로그 이벤트 **ID** 및 이벤트 이름

이벤트 ID	이벤트 이름
746001	Import started
746002	Import complete
746003	Import failed
746004	Exceed user group limit
746005	AD Agent down
746006	AD Agent out of sync
746007	Netbios response failed
746008	Netbios started
746009	Netbios stopped
746010	Import user failed
746011	Exceed user limit

이벤트 ID	이벤트 이름
746012	User IP add
746013	User IP delete
746014	FQDN Obsolete
746015	FQDN resolved
746016	DNS lookup failed
746017	Import user issued
746018	Import user done
746019	Update AD Agent failed

**IPSec** 시스템 로그 이벤트 ID 및 이벤트 이름

이벤트 ID	이벤트 이름
402114	Invalid SPI received
402115	Unexpected protocol received
402116	Packet doesn't match identity
402117	Non-IPSEC packet received
402118	Invalid fragment offset
402119	Anti-Replay check failure
402120	Authentication failure
402121	Packet dropped
426101	cLACP Port Bundle
426102	cLACP Port Standby
426103	cLACP Port Moved To Bundle From Standby
426104	cLACP Port Unbundled
602103	Path MTU updated
602104	Path MTU exceeded
602303	New SA created
602304	SA deleted
702305	SA expiration - Sequence rollover
702307	SA expiration - Data rollover

**NAT** 시스템 로그 이벤트 ID 및 이벤트 이름

이벤트 ID	이벤트 이름
201002	Max connection Exceeded for host
201003	Embryonic limit exceed
201004	UDP connection limit exceed
201005	FTP connection failed
201006	RCMD connection failed
201008	New connection Disallowed
201009	Connection Limit exceed
201010	Embryonic Connection limit exceeded
201011	Connection Limit exceeded
201012	Per-client embryonic connection limit exceeded
201013	Per-client connection limit exceeded
202001	Global NAT exhausted
202005	Embryonic connection error
202011	Connection Limit exceeded
305005	No NAT group found
305006	Translation failed
305007	Connection dropped
305008	NAT allocation issue
305009	NAT Created
305010	NAT teardown
305011	PAT created
305012	PAT teardown
305013	Connection denied

#### SSL VPN 시스템 로그 이벤트 ID 및 이벤트 이름

이벤트 ID	이벤트 이름
716001	WebVPN Session Started
716002	WebVPN Session Terminated
716003	WebVPN User URL access
716004	WebVPN User URL access denied
716005	WebVPN ACL error
716006	WebVPN User Disabled

이벤트 ID	이벤트 이름
716007	WebVPN Unable to Create
716008	WebVPN Debug
716009	WebVPN ACL error
716010	WebVPN User access network
716011	WebVPN User access
716012	WebVPN User Directory access
716013	WebVPN User file access
716014	WebVPN User file access
716015	WebVPN User file access
716016	WebVPN User file access
716017	WebVPN User file access
716018	WebVPN User file access
716019	WebVPN User file access
716020	WebVPN User file access
716021	WebVPN user access file denied
716022	WebVPN Unable to connect proxy
716023	WebVPN session limit reached
716024	WebVPN User access error
716025	WebVPN User access error
716026	WebVPN User access error
716027	WebVPN User access error
716028	WebVPN User access error
716029	WebVPN User access error
716030	WebVPN User access error
716031	WebVPN User access error
716032	WebVPN User access error
716033	WebVPN User access error
716034	WebVPN User access error
716035	WebVPN User access error
716036	WebVPN User login successful
716037	WebVPN User login failed
716038	WebVPN User Authentication Successful

이벤트 ID	이벤트 이름
716039	WebVPN User Authentication Rejected
716040	WebVPN User logging denied
716041	WebVPN ACL hit count
716042	WebVPN ACL hit
716043	WebVPN Port forwarding
716044	WebVPN Bad Parameter
716045	WebVPN Invalid Parameter
716046	WebVPN connection terminated
716047	WebVPN ACL usage
716048	WebVPN memory issue
716049	WebVPN Empty SVC ACL
716050	WebVPN ACL error
716051	WebVPN ACL error
716052	WebVPN Session Terminated
716053	WebVPN SSO Server added
716054	WebVPN SSO Server deleted
716055	WebVPN Authentication Successful
716056	WebVPN Authentication Failed
716057	WebVPN Session terminated
716058	WebVPN Session lost
716059	WebVPN Session resumed
716060	WebVPN Session Terminated
722001	WebVPN SVC Connect request error
722002	WebVPN SVC Connect request error
722003	WebVPN SVC Connect request error
722004	WebVPN SVC Connect request error
722005	WebVPN SVC Connect update issue
722006	WebVPN SVC Invalid address
722007	WebVPN SVC Message
722008	WebVPN SVC Message
722009	WebVPN SVC Message
722010	WebVPN SVC Message



이벤트 ID	이벤트 이름
722011	WebVPN SVC Message
722012	WebVPN SVC Message
722013	WebVPN SVC Message
722014	WebVPN SVC Message
722015	WebVPN SVC invalid frame
722016	WebVPN SVC invalid frame
722017	WebVPN SVC invalid frame
722018	WebVPN SVC invalid frame
722019	WebVPN SVC Not Enough Data
722020	WebVPN SVC no address
722021	WebVPN Memory issue
722022	WebVPN SVC connection established
722023	WebVPN SVC connection terminated
722024	WebVPN Compression Enabled
722025	WebVPN Compression Disabled
722026	WebVPN Compression reset
722027	WebVPN Decompression reset
722028	WebVPN Connection Closed
722029	WebVPN SVC Session terminated
722030	WebVPN SVC Session terminated
722031	WebVPN SVC Session terminated
722032	WebVPN SVC connection Replacement
722033	WebVPN SVC Connection established
722034	WebVPN SVC New connection
722035	WebVPN Received Large packet
722036	WebVPN transmitting Large packet
722037	WebVPN SVC connection closed
722038	WebVPN SVC session terminated
722039	WebVPN SVC invalid ACL
722040	WebVPN SVC invalid ACL
722041	WebVPN SVC IPv6 not available
722042	WebVPN invalid protocol

이벤트 ID	이벤트 이름
722043	WebVPN DTLS disabled
722044	WebVPN unable to request address
722045	WebVPN Connection terminated
722046	WebVPN Session terminated
722047	WebVPN Tunnel terminated
722048	WebVPN Tunnel terminated
722049	WebVPN Session terminated
722050	WebVPN Session terminated
722051	WebVPN address assigned
722053	WebVPN Unknown client
723001	WebVPN Citrix connection Up
723002	WebVPN Citrix connection Down
723003	WebVPN Citrix no memory issue
723004	WebVPN Citrix bad flow control
723005	WebVPN Citrix no channel
723006	WebVPN Citrix SOCKS error
723007	WebVPN Citrix connection list broken
723008	WebVPN Citrix invalid SOCKS
723009	WebVPN Citrix invalid connection
723010	WebVPN Citrix invalid connection
723011	WebVPN citrix Bad SOCKS
723012	WebVPN Citrix Bad SOCKS
723013	WebVPN Citrix invalid connection
723014	WebVPN Citrix connected to Server
724001	WebVPN Session not allowed
724002	WebVPN Session terminated
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL handshake Started
725002	SSL Handshake completed
725003	SSL Client session resume
725004	SSL Client request Authentication

이벤트 ID	이벤트 이름
725005	SSL Server request authentication
725006	SSL Handshake failed
725007	SSL Session terminated
725008	SSL Client Cipher
725009	SSL Server Cipher
725010	SSL Cipher
725011	SSL Device choose Cipher
725012	SSL Device choose Cipher
725013	SSL Server choose cipher
725014.	SSL LIB error
725015	SSL client certificate failed

## 시스템 로그 이벤트의 시간 속성

Event Logging(이벤트 로깅) 페이지에서 다양한 타임스탬프의 목적을 이해하면 원하는 이벤트를 필터링하고 찾을 수 있습니다.

Historical		Live							
Date/Time	Event Type	Sensor ID	Initiator	Responder	Port	Protocol	Action	Policy	
Aug 20, 2019 10:44:14 AM	Malware	192.168.20.53			80	tcp	Cloud Lookup Timeout	BlockOfficeDocumentsPDFUpload_BlockMalwareOthers	
<b>1</b> Date/Time <b>2</b> Application: HTTP ClientApplication: Web browser EventSecond: 1566312254 EventType: MalwareEvent FileAction: Cloud Lookup Timeout FileDirection: Download FileName: eicar.com FilePolicy: BlockOfficeDocumentsPDFUpload_BlockMalwareOthers FileSHA256: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f		<b>3</b> FileSize: 68 FileType: EICAR <b>4</b> FirstPacketSecond: Aug 20, 2019 10:44:08 AM InitiatorIP: [redacted] <b>4</b> InitiatorPort: 65386 LastPacketSecond: Aug 20, 2019 10:44:14 AM ResponderIP: [redacted] ResponderPort: 80		<b>5</b> SensorID: 192.168.20.53 SHA_Disposition: Unavailable SperoDisposition: Spero detection not performed on file ThreatName: Unknown timestamp: Aug 20, 2019 10:44:14 AM URI: /eicar.com Username: No Authentication Required					
Date/Time	Device Type	Event Type	Sensor ID	Initiator IP	Responder IP	Port	Protocol	Action	Policy
Jun 12, 2020, 7:27:02 AM	ASA	302013	admin	192.168.25.4	192.168.0.68	443	TCP	Built	
Action: Built ConnectionID: 1169028 DeviceType: ASA Direction: inbound EgressInterface: identity EventGroup: session EventGroupDefinition: User Session EventName: Built TCP		EventType: 302013 IngressInterface: management InitiatorIP: 192.168.25.4 InitiatorPort: 36540 MappedInitiatorIP: 192.168.25.4 MappedInitiatorPort: 36540 MappedResponderIP: 192.168.0.68 MappedResponderPort: 443		Protocol: TCP ResponderIP: 192.168.0.68 ResponderPort: 443 SensorID: admin Severity: Informational <b>6</b> SyslogTimestamp: 2020-06-12 11:15:26 +0000 UTC timestamp: Jun 12, 2020, 7:27:02 AM					
<b>Message</b> ASA-6-302013: Built inbound TCP connection 1169028 for management:192.168.25.4/36540 (192.168.25.4/36540) to identity:192.168.0.68/443 (192.168.0.68/443)									

Date/Time	Device Type	Event Type	Sensor ID	Initiator IP	Responder IP	Port	Protocol	Action	Policy
Jun 12, 2020, 7:27:13 AM	ASA	5	192.168.0.169	192.168.25.4	192.168.0.169	443	TCP	Update	
<b>Action</b>	Update		<b>InitiatorBytes</b>	0		<b>Protocol</b>	TCP		
<b>ConnectionID</b>	482168		<b>InitiatorIP</b>	192.168.25.4		<b>ResponderBytes</b>	3581		
<b>DeviceType</b>	ASA		<b>InitiatorPackets</b>	0		<b>ResponderIP</b>	192.168.0.169		
<b>EgressInterface</b>	65535		<b>InitiatorPort</b>	38068		<b>ResponderPackets</b>	33		
<b>EventType</b>	5		<b>LastPacketSecond</b>	Jun 12, 2020, 7:27:07 A		<b>ResponderPort</b>	443		
<b>FirewallExtendedEvent</b>	2034			M		<b>SensorID</b>	192.168.0.169		
<b>FirstPacketSecond</b>	Jun 12, 2020, 7:27:07 A		<b>MappedInitiatorIP</b>	192.168.25.4		<b>Severity</b>	Informational		
	M		<b>MappedInitiatorPort</b>	38068		<b>timestamp</b>	Jun 12, 2020, 7:27:13 A		
<b>ICMPCode</b>	0		<b>MappedResponderIP</b>	192.168.0.169			M		
<b>ICMPType</b>	0		<b>MappedResponderPort</b>	443					
<b>IngressInterface</b>	9		<b>NetFlowTimestamp</b>	1591961232					

번호	라벨	설명
1	날짜/시간	SEC(Secure Event Connector)가 이벤트를 처리한 시간. 방화벽이 해당 트래픽을 검사한 시간과 다를 수 있습니다. 타임스탬프와 동일한 값입니다.
2	EventSecond	LastPacketSecond와 같음.
3	FirstPacketSecond	연결이 열린 시간입니다. 이때 방화벽은 패킷을 검사합니다.  FirstPacketSecond의 값은 LastPacketSecond에서 ConnectionDuration을 빼서 계산됩니다.  연결 시작 시 로깅된 연결 이벤트의 경우 FirstPacketSecond, LastPacketSecond 및 EventSecond 값은 모두 동일합니다.
4	LastPacketSecond	연결이 닫힌 시간입니다. 연결 종료 시 로깅된 연결 이벤트의 경우, LastPacketSecond 및 EventSecond는 동일합니다.
5	timestamp	SEC(Secure Event Connector)가 이벤트를 처리한 시간. 방화벽이 해당 트래픽을 검사한 시간과 다를 수 있습니다. 날짜/시간과 동일한 값입니다.
6	시스템 로그 타임스탬프	'logging timestamp'가 사용되는 경우 시스템 로그가 시작된 시간을 나타냅니다. 시스템 로그에 이 정보가 없으면 SEC가 이벤트를 수신한 시간이 반영됩니다.

번호	라벨	설명
7	NetflowTimeStamp	ASA에서 NetFlow 패킷을 채운 다음 플로우 컬렉터로 전송할 충분한 플로우 레코드/이벤트 수집을 완료한 시간입니다.

## Cisco Secure Cloud Analytics 및 동적 엔티티 모델링

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

Secure Cloud Analytics는 온프레미스 및 클라우드 기반 네트워크 구축을 모니터링하는 SaaS(Software as a Service) 솔루션입니다. 방화벽 이벤트 및 네트워크 플로우 데이터를 비롯한 소스에서 네트워크 트래픽에 대한 정보를 수집하여 트래픽에 대한 관찰을 생성하고 트래픽 패턴을 기반으로 네트워크 엔티티의 역할을 자동으로 식별합니다. Secure Cloud Analytics는 Talos와 같은 위협 인텔리전스의 다른 소스와 결합된 이 정보를 사용하여 본질적으로 악의적인 행동이 있음을 나타내는 경고를 생성합니다. 알람과 함께 Secure Cloud Analytics는 알람을 조사하고 악의적인 동작의 소스를 찾기 위한 더 나은 기반을 제공하기 위해 수집한 네트워크 및 호스트 가시성 및 상황 정보를 제공합니다.

### 동적 엔티티 모델링

동적 엔티티 모델링은 방화벽 이벤트 및 네트워크 플로우 데이터에 대한 동작 분석을 수행하여 네트워크의 상태를 추적합니다. Secure Cloud Analytics의 컨텍스트에서 엔티티는 네트워크의 호스트 또는 엔드포인트와 같이 시간이 지남에 따라 추적할 수 있는 항목입니다. 동적 엔티티 모델링은 전송하는 트래픽 및 네트워크에서 수행하는 활동을 기반으로 엔티티에 대한 정보를 수집합니다. **Logging Analytics and Detection**(로깅 분석 및 탐지) 라이선스와 통합된 Secure Cloud Analytics는 엔티티가 일반적으로 전송하는 트래픽 유형을 확인하기 위해 방화벽 이벤트 및 기타 트래픽 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스를 구매한 경우 Secure Cloud Analytics는 엔티티 트래픽 모델링에 NetFlow 및 기타 트래픽 정보도 포함할 수 있습니다. Secure Cloud Analytics는 각 엔티티의 최신 모델을 유지하기 위해 엔티티가 계속해서 트래픽을 전송하고 잠재적으로 다른 트래픽을 전송하므로 시간이 지남에 따라 이러한 모델을 업데이트합니다. 이 정보에서 Secure Cloud Analytics는 다음을 식별합니다.

- 엔티티의 역할 - 엔티티가 일반적으로 수행하는 작업을 설명합니다. 예를 들어 엔티티가 일반적으로 이메일 서버와 연결된 트래픽을 전송하는 경우, Secure Cloud Analytics는 엔티티를 이메일 서버 역할로 할당합니다. 엔티티는 여러 역할을 수행할 수 있으므로 역할/엔티티 관계는 다대일일 수 있습니다.
- 엔티티에 대한 관찰 - 외부 IP 주소와의 하트비트 연결 또는 다른 엔티티와 설정된 원격 액세스 세션과 같이 네트워크에서의 엔티티 동작에 대한 팩트입니다. CDO와 통합하는 경우 방화벽 이벤트에서 이러한 정보를 가져올 수 있습니다. **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스도 구매한 경우, 시스템은 NetFlow에서 팩트를 가져오고 방화벽 이벤트와 NetFlow 모두에서 관찰을 생성할 수 있습니다. 관찰 자체는 관찰이 나타내는 것 이상의 의미를 전달하지 않습니다. 일반적인 고객은 수천 개의 관찰 및 몇 가지 알람을 가질 수 있습니다.

## 알림 및 분석

역할, 관찰 및 기타 위협 인텔리전스의 조합을 기반으로 Secure Cloud Analytics는 시스템에서 식별한 가능한 악의적인 행동을 나타내는 실행 가능한 항목인 알림을 생성합니다. 하나의 알림이 여러 관찰을 나타낼 수 있습니다. 방화벽이 동일한 연결 및 엔터티와 관련된 여러 연결 이벤트를 로깅하는 경우 하나의 알림만 생성될 수 있습니다.

예를 들어, 새 내부 디바이스 관찰 자체는 악의적인 행동을 구성하지 않습니다. 그러나 시간이 지남에 따라 엔터티가 도메인 컨트롤러와 일치하는 트래픽을 전송하면 시스템은 해당 엔터티에 도메인 컨트롤러 역할을 할당합니다. 이후에 엔터티가 비정상적인 포트를 사용하여 이전에 연결을 설정하지 않은 외부 서버에 연결하고 대량의 데이터를 전송하는 경우, 시스템은 새로운 대규모 연결(외부) 관찰 및 예외적인 도메인 컨트롤러 관찰을 로깅합니다. 해당 외부 서버가 Talos 감시 목록에 있는 것으로 식별된 경우, 이 모든 정보의 조합으로 인해 Secure Cloud Analytics가 이 엔터티의 동작에 대한 알림을 생성하고, 악성 동작을 조사하고 교정하기 위한 추가 작업을 수행하라는 메시지가 표시됩니다.

Secure Cloud Analytics 웹 포털 UI에서 알림을 열면 시스템이 알림을 생성하도록 유도한 지원 관찰을 볼 수 있습니다. 이러한 관찰을 통해 관련 엔터티에 대한 추가 컨텍스트(전송한 트래픽 포함) 및 외부 위협 인텔리전스(사용 가능한 경우)도 볼 수 있습니다. 또한 엔터티가 관련된 다른 관찰 및 알림을 보고 이 동작이 다른 잠재적인 악의적인 동작과 관련이 있는지 확인할 수 있습니다.

Secure Cloud Analytics에서 알림을 보고 닫을 때는 Secure Cloud Analytics UI의 트래픽을 허용하거나 차단할 수 없습니다. 디바이스를 액티브 모드로 구축한 경우에는 트래픽을 허용하거나 차단하도록 방화벽 액세스 제어 규칙을 업데이트하고, 패시브 모드에서 디바이스를 구축한 경우에는 방화벽 액세스 제어 규칙을 업데이트해야 합니다.

## 방화벽 이벤트 기반 알림 작업

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

### 알림 워크플로우

알림의 워크플로우는 상태를 기반으로 합니다. 시스템에서 알림을 생성할 때 기본 상태는 Open(열림)이며 사용자가 할당되지 않습니다. Alerts(알림) 요약을 볼 때 즉시 문제가 되는 모든 열린 알림이 기본적으로 표시됩니다.

참고: **Total Network Analytics and Monitoring**(전체 네트워크 분석 및 모니터링) 라이선스가 있는 경우 알림은 NetFlow에서 생성된 관찰, 방화벽 이벤트에서 생성된 관찰 또는 두 데이터 소스의 관찰을 기반으로 할 수 있습니다.

알림 요약을 검토할 때 알림에 대한 상태를 초기 분류로 할당, 태그 지정 및 업데이트할 수 있습니다. 필터 및 검색 기능을 사용하여 특정 알림을 찾거나, 다른 상태의 알림을 표시하거나, 다른 태그 또는 담당자와 연결할 수 있습니다. 알림의 상태를 스누즈로 설정할 수 있습니다. 이 경우 스누즈 기간이 경과할 때까지 미해결 알림 목록에 다시 나타나지 않습니다. 알림에서 스누즈 상태를 제거하여 미해결 알림으로 다시 표시할 수도 있습니다. 알림을 검토할 때 자신 또는 시스템의 다른 사용자에게 할당할 수 있습니다. 사용자는 사용자 이름에 할당된 모든 알림을 검색할 수 있습니다.

Alerts(알림) 요약에서 알림 상세정보 페이지를 볼 수 있습니다. 이 페이지에서는 이 알림을 생성한 지원 관찰에 대한 추가 컨텍스트 및 이 알림과 관련된 엔터티에 대한 추가 컨텍스트를 검토할 수 있습니다.

니다. 이 정보는 네트워크에서 문제를 추가로 조사하고 잠재적으로 악의적인 동작을 해결하기 위해 실제 문제를 정확히 찾아내는 데 도움이 될 수 있습니다.

Stealthwatch Cloud 웹 포털 UI, CDO 및 네트워크에서 조사할 때 결과를 설명하는 알림과 함께 코멘트를 남길 수 있습니다. 이렇게 하면 나중에 참조할 수 있는 연구 기록을 만드는 데 도움이 됩니다.

분석을 완료한 경우 상태를 Closed(닫힘)로 업데이트하고 더 이상 기본적으로 미결 알림으로 표시되지 않도록 할 수 있습니다. 상황이 바뀌면 나중에 닫힌 알림을 다시 열 수도 있습니다.

다음은 지정된 알림을 조사하는 방법에 대한 일반적인 지침 및 제안 사항입니다. Stealthwatch Cloud 는 알림을 로깅할 때 추가 컨텍스트를 제공하므로 이 컨텍스트를 조사에 활용할 수 있습니다.

이러한 단계는 포괄적이거나 모든 것을 포함하지 않습니다. 이는 알림 조사를 시작하는 데 사용할 수 있는 일반적인 프레임워크를 제공할 뿐입니다.

일반적으로 알림을 검토할 때 다음 단계를 수행할 수 있습니다.

1. [열린 알림 분류, on page 698](#)
2. [나중에 분석하기 위해 알림 일시 중지, on page 698](#)
3. [추가 조사를 위해 알림 업데이트, on page 699](#)
4. [알림 검토 및 조사 시작, on page 699](#)
5. [엔터티 및 사용자 검사, on page 701](#)
6. [Secure Cloud Analytics를 사용하여 문제 해결, on page 702](#)
7. [알림 업데이트 및 닫기, on page 703](#)

## 열린 알림 분류

특히 둘 이상의 알림이 아직 조사되지 않은 경우, 미해결 알림을 분류합니다.

- CDO에서 SWC로 교차 실행하고 알림을 보는 방법에 대한 자세한 내용은 [CDO에서 Cisco Secure Cloud Analytics 알림 보기](#)을 참조하십시오.

다음 질문을 합니다.

- 이 알림 유형을 높은 우선순위로 구성했습니까?
- 영향을 받는 서브넷에 대해 높은 감도를 설정했습니까?
- 네트워크의 새 엔터티에서 발생하는 비정상적인 동작입니까?
- 엔터티의 일반적인 역할은 무엇이며 이 알림의 동작이 해당 역할과 어떻게 일치합니까?
- 이 엔터티의 정상적인 동작에서 예외적으로 벗어났습니까?
- 사용자가 관련된 경우, 이는 사용자의 예상된 동작입니까, 아니면 예외적인 것입니까?
- 보호되거나 민감한 데이터가 손상될 위험이 있습니까?
- 이 동작이 계속 허용되는 경우 네트워크에 미치는 영향은 어느 정도입니까?

- 외부 엔터티와 통신하는 경우, 이러한 엔터티가 과거에 네트워크의 다른 엔터티와 연결을 설정했습니까?

우선순위가 높은 알림인 경우 조사를 계속하기 전에 인터넷에서 엔터티를 격리하거나 연결을 닫는 것을 고려하십시오.

## 나중에 분석하기 위해 알림 일시 중지

다른 알림에 비해 우선 순위가 낮은 알림을 스누즈합니다. 예를 들어 조직에서 이메일 서버를 FTP 서버로 용도를 변경하고 시스템에서 긴급 프로파일 알림(엔터티의 현재 트래픽이 이전에 일치하지 않았던 행동 프로파일과 일치함을 나타냄)을 생성하는 경우 이 알림을 나중에 다시 확인할 수 있습니다. 스누즈된 알림은 열린 알림과 함께 표시되지 않습니다. 이러한 스누즈된 알림을 검토하려면 특별히 필터링해야 합니다.

알림 스누즈:

### Procedure

단계 1 **Close Alert**(알림 닫기)를 클릭합니다.

단계 2 **Snooze this alert**(이 알림 스누즈) 창의 드롭다운에서 스누즈 기간을 선택합니다.

단계 3 **Save**(저장)를 클릭합니다.

### What to do next

이러한 알림을 검토할 준비가 되면 다시 알림을 해제할 수 있습니다. 이렇게 하면 상태가 Open(열림)으로 설정되고 다른 Open(열림) 알림과 함께 알림이 표시됩니다.

스누즈된 알림의 스누즈를 해제합니다.

- 스누즈된 알림에서 **Unsnaze Alert**(알림 스누즈 해제)를 클릭합니다.

## 추가 조사를 위해 알림 업데이트

알림 세부 정보를 엽니다.

### Procedure

단계 1 **Monitor**(모니터링) > **Alerts**(알림)를 선택합니다.

단계 2 알림 유형 이름을 클릭합니다.

### What to do next

초기 분류 및 우선순위에 따라 알림을 할당하고 태그를 지정합니다.



1. **Assignee**(담당자) 드롭다운에서 사용자를 선택하여 알림을 할당하면 사용자가 조사를 시작할 수 있습니다.
2. 드롭다운에서 하나 이상의 **Tags**(태그)를 선택하여 알림에 태그를 추가하여 향후 식별을 위해 알림을 더 잘 분류하고 알림에서 장기적 패턴을 설정합니다.
3. 이 알림에 대한 코멘트를 입력한 다음 **Comment**(코멘트)를 클릭하여 초기 결과를 추적하고 알림에 할당된 사람을 지원하는 데 필요한 코멘트를 남깁니다. 알림은 시스템 코멘트와 사용자 코멘트를 모두 추적합니다.

## 알림 검토 및 조사 시작

할당된 알림을 검토하는 경우 알림 세부 정보를 검토하여 **Stealthwatch Cloud**에서 알림을 생성한 이유를 파악합니다. 지원 관찰을 검토하여 이러한 관찰이 소스 엔터티에 미치는 영향을 파악합니다.

경고가 방화벽 이벤트를 기반으로 생성된 경우, 시스템은 방화벽 구축이 이 경고의 소스임을 인식하지 않습니다.

이 소스 엔터티에 대한 모든 지원 관찰을 확인하여 일반 동작 및 패턴을 파악하고 이 활동이 더 긴 추세의 일부일 수 있는지 확인합니다.

### 프로시저

- 단계 1 알림 세부사항에서 관찰 유형 옆에 있는 화살표 아이콘(☺)을 클릭하여 해당 유형의 모든 로깅된 관찰을 확인합니다.
- 단계 2 **All Observations for Network**(네트워크에 대한 모든 관찰) 옆에 있는 화살표 아이콘(☺)을 클릭하여 이 알림의 소스 엔터티에 대해 로깅된 모든 관찰을 확인합니다.

이러한 관찰에 대한 추가 분석을 수행하려면 쉽표로 구분된 값 파일로 지원 관찰을 다운로드합니다.

- 알림 세부 정보의 **Supporting Observations**(지원 관찰) 창에서 **CSV**를 클릭합니다.

관찰 결과에서 소스 엔터티 동작이 악의적인 동작을 나타내는지 확인합니다. 소스 엔터티가 여러 외부 엔터티와의 연결을 설정한 경우, 외부 엔터티가 어떤 식으로든 관련이 있는지 확인합니다(예: 모든 엔터티가 유사한 지리위치 정보를 가지고 있거나 해당 IP 주소가 동일한 서버넷에 있는지 여부).

소스 엔터티 IP 주소 또는 호스트 이름에서 소스 엔터티와 관련된 추가 컨텍스트를 확인합니다. 여기에는 관련될 수 있는 기타 알림 및 관찰, 디바이스 자체에 대한 정보, 전송 중인 세션 트래픽 유형이 포함됩니다.

- 엔터티와 관련된 모든 알림을 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Alerts**(알림)를 선택합니다.
- **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Observations**(관찰)를 선택하여 엔터티와 관련된 모든 관찰을 확인합니다.
- 디바이스에 대한 정보를 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Device**(디바이스)를 선택합니다.

- 이 엔티티와 관련된 세션 트래픽을 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic**(세션 트래픽)을 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy**(복사)를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 소스 엔티티는 항상 네트워크 내부에 있습니다. 이를 방화벽 이벤트의 Initiator IP(이니시에이터 IP)와 비교해 보십시오. 이 IP는 연결을 시작한 엔티티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

관찰에서 다른 외부 엔티티에 대한 정보를 검토합니다. 지리위치 정보를 검토하고 지리위치 데이터 또는 Umbrella 데이터가 악성 엔티티를 식별하는지 확인합니다. 이러한 엔티티에 의해 생성된 트래픽을 확인합니다. Talos, AbuseIPDB 또는 Google에 이러한 엔티티에 대한 정보가 있는지 확인합니다. 여러 날짜의 IP 주소를 찾고 외부 엔티티가 네트워크의 엔티티와 설정한 다른 유형의 연결을 확인합니다. 필요한 경우 이러한 내부 엔티티를 찾아 보안 침해 또는 의도하지 않은 행동의 증거가 있는지 확인합니다.

소스 엔티티가 연결을 설정한 외부 엔티티 IP 주소 또는 호스트 이름에 대한 컨텍스트를 검토합니다.

- 이 엔티티에 대한 최근 트래픽 정보를 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **IP Traffic**(IP 트래픽)을 선택합니다.
- 이 엔티티에 대한 최근 세션 트래픽 정보를 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Session Traffic**(세션 트래픽)을 선택합니다.
- AbuseIPDB 웹사이트에서 이 엔티티에 대한 정보를 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 AbuseIPDB를 선택합니다.
- Cisco Umbrella 웹사이트에서 이 엔티티에 대한 정보를 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Cisco Umbrella**를 선택합니다.
- Google에서 이 IP 주소를 검색하려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Google Search**(Google 검색)를 선택합니다.
- Talos 웹사이트에서 이 정보에 대한 정보를 보려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Talos Intelligence**를 선택합니다.
- **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Add IP to watchlist**(감시 목록에 IP 추가)를 선택하여 이 엔티티를 감시 목록에 추가합니다.
- 이 엔티티의 지난 달 트래픽을 검색하려면 **IP address or hostname**(IP 주소 또는 호스트 이름) 드롭다운에서 **Find IP on multiple days**(여러 날짜의 IP 찾기)를 선택합니다.
- IP 주소 또는 호스트 이름 드롭다운에서 **Copy**(복사)를 선택하여 IP 주소 또는 호스트 이름을 복사합니다.

Stealthwatch Cloud의 연결된 엔티티는 항상 네트워크 외부에 있습니다. 이를 방화벽 이벤트의 Responder IP(응답자 IP)와 비교해 보십시오. 이는 연결 요청에 응답한 엔티티를 나타내며, 네트워크의 내부 또는 외부에 있을 수 있습니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(코멘트)**를 클릭합니다.

## 엔터티 및 사용자 검사

Stealthwatch Cloud 포털 UI에서 알림을 검토한 후 소스 엔터티, 이 알림과 관련되었을 수 있는 사용자 및 기타 관련 엔터티에 대해 직접 추가 검사를 수행할 수 있습니다.

- 소스 엔터티가 물리적으로 또는 클라우드에서 네트워크의 어느 위치에 있는지 확인하고 직접 액세스합니다. 이 엔터티에 대한 로그 파일을 찾습니다. 네트워크의 물리적 엔터티인 경우 디바이스에 액세스하여 로그 정보를 검토하고 이 동작의 원인에 대한 정보가 있는지 확인합니다. 가상 엔터티이거나 클라우드에 저장된 경우 로그에 액세스하여 이 엔터티와 관련된 항목을 검색합니다. 무단 로그인, 승인되지 않은 구성 변경 등에 대한 자세한 내용은 로그를 검사합니다.
- 엔터티를 검사합니다. 엔터티 자체에서 악성코드 또는 취약성을 식별할 수 있는지 확인합니다. 조직에서 승인하지 않은 USB 스틱과 같이 디바이스에 대한 물리적 변경이 있는지를 포함하여 악의적인 변경이 있는지 확인합니다.
- 네트워크의 사용자 또는 네트워크 외부의 사용자가 관련되었는지 확인합니다. 가능한 경우 사용자에게 무엇을 하고 있었는지 물어봅니다. 사용자가 사용할 수 없는 경우, 액세스 권한이 있어야 했는지, 그리고 퇴사한 직원이 퇴사 전에 외부 서버에 파일을 업로드하는 등의 상황이 발생했는지 확인합니다.

결과에 대한 코멘트를 남겨 주십시오.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(코멘트)**를 클릭합니다.

## 알림 업데이트 및 닫기

결과에 따라 태그를 추가합니다.

### Procedure

**단계 1** Secure Cloud Analytics 포털 UI에서 **Monitor(모니터링)** > **Alerts(알림)**를 선택합니다.

**단계 2** 드롭다운에서 하나 이상의 **Tags(태그)**를 선택합니다.

조사 결과 및 수행한 교정 단계를 설명하는 최종 코멘트를 추가합니다.

- 알림 세부 정보에서 이 알림에 대한 코멘트를 입력하고 **Comment(코멘트)**를 클릭합니다.

알림을 닫고 유용하거나 도움이 되지 않음으로 표시합니다.

1. 알림 세부 정보에서 **Close Alert(알림 닫기)**를 클릭합니다.
2. 알림이 도움이 되었으면 **Yes(예)**를 선택하고, 알림이 도움이 되지 않았다면 **No(아니요)**를 선택합니다. 이는 알림이 악의적인 행동으로 인해 발생했음을 의미하는 것이 아니라 해당 알림이 조직에 도움이 되었음을 의미합니다.

### 3. Save(저장)를 클릭합니다.

#### What to do next

##### 종료된 알림 다시 열기

종료된 알림과 관련된 추가 정보를 발견하거나 알림과 관련된 코멘트를 더 추가하려는 경우 알림을 다시 열어 상태를 Open(열림)으로 변경할 수 있습니다. 그런 다음 필요에 따라 알림을 변경한 다음 추가 조사가 완료되면 알림을 닫을 수 있습니다.

종료된 알림을 다시 엽니다.

- 닫힌 알림의 세부 사항에서 **Reopen Alert**(알림 다시 열기)를 클릭합니다.

## 알림 우선순위 수정

필수 라이선스: 로깅 분석 및 탐지 또는 전체 네트워크 분석 및 모니터링

알림 유형은 기본 우선순위와 함께 제공되며, 이는 시스템이 이 유형의 알림 생성에 대한 민감도에 영향을 미칩니다. 알림은 기본적으로 Cisco 인텔리전스 및 기타 요인에 따라 낮음 또는 보통으로 설정됩니다. 네트워크 환경에 따라 알림 유형의 우선순위를 다시 지정하여 우려되는 특정 알림을 강조할 수 있습니다. 모든 알림 유형을 낮음, 보통 또는 높음 우선순위로 구성할 수 있습니다.

- **Monitor**(모니터링) > **Alerts**(알림)를 선택합니다.
- **Settings**(설정) 드롭다운 아이콘(⚙)을 클릭한 다음 **Alert Types and Priorities**(알림 유형 및 우선순위)를 선택합니다.
- 알림 유형 옆에 있는 편집 아이콘(✎)을 클릭하고 낮음, 중간 또는 높음을 선택하여 우선순위를 변경합니다.

## 이벤트 로깅 페이지에서 이벤트 검색 및 필터링

특정 이벤트에 대한 기록 및 라이브 이벤트 테이블을 검색하고 필터링하는 것은 CDO에서 다른 정보를 검색하고 필터링할 때와 동일한 방식으로 작동합니다. 필터 기준을 추가하면 CDO가 Events(이벤트) 페이지에 표시되는 내용을 제한하기 시작합니다. 검색 필드에 검색 기준을 입력하여 특정 값의 이벤트를 찾을 수도 있습니다. 필터링 및 검색 메커니즘을 결합하는 경우, 검색은 이벤트를 필터링한 후 표시된 결과 중에서 입력한 값을 찾으려고 시도합니다.

다음은 이벤트 로그 검색을 수행하는 옵션입니다.

- [이벤트 로깅 페이지에서 이벤트 검색, 750 페이지](#)
- [백그라운드에서 기록 이벤트 검색, 750 페이지](#)

필터링은 라이브 이벤트를 시간 기준으로 필터링할 수 없다는 점을 제외하고 기록 이벤트와 동일한 방식으로 라이브 이벤트에 대해 작동합니다.



이러한 필터링 방법에 대해 알아보십시오.

- [라이브 또는 과거 이벤트 필터링, 743 페이지](#)
- [NetFlow 이벤트만 필터링, 744 페이지](#)
- [ASA 또는 FDM-관리 장치 syslog 이벤트에 대한 필터링\(ASA NetFlow 이벤트 제외\), 745 페이지](#)
- [필터 요소 결합, 745 페이지](#)

## 라이브 또는 과거 이벤트 필터링

이 절차에서는 이벤트 필터링을 사용하여 Event Logging(이벤트 로깅) 페이지에서 이벤트의 하위 집합을 확인하는 방법을 설명합니다. 특정 필터 기준을 반복적으로 사용하는 경우 사용자 지정 필터를 생성하여 저장할 수 있습니다. 자세한 내용은 [사용자 지정 가능한 이벤트 필터](#)를 참조하십시오.

### Procedure

- 단계 1 탐색 모음에서 분석 > 이벤트 로깅을 선택합니다.
- 단계 2 Historical(기록) 또는 Live(라이브) 탭을 클릭합니다.
- 단계 3 필터 버튼 를 클릭합니다. 필터링 열은 고정 아이콘 을 클릭하여 열 수 있습니다.
- 단계 4 저장된 필터 요소가 없는 View(보기) 탭을 클릭합니다.



- 단계 5 필터링할 이벤트 세부 정보를 선택합니다.

- **FTD 이벤트 유형**
  - Connection(연결) - 액세스 제어 규칙의 연결 이벤트를 표시합니다.
  - File(파일) - 액세스 제어 규칙의 파일 정책에 의해 보고된 이벤트를 표시합니다.
  - Intrusion(침입) - 액세스 제어 규칙의 침입 정책에 의해 보고된 이벤트를 표시합니다.
  - Malware(악성코드) - 액세스 제어 규칙의 악성코드 정책에 의해 보고된 이벤트를 표시합니다.

이러한 이벤트 유형에 대한 자세한 내용은 [FDM-관리 이벤트 유형](#)을 참조하십시오.

- **ASAEvent Types(이벤트 유형)** - 이러한 이벤트 유형은 Syslog 또는 NetFlow 이벤트의 그룹을 나타냅니다.
- **Time Range(시간 범위)** - 표시할 기간의 시작과 끝을 선택하려면 Start(시작) 또는 End(종료) 시간 필드를 클릭합니다. 타임스탬프는 컴퓨터의 로컬 시간으로 표시됩니다.
- **Action(작업)** - 규칙에 의해 정의된 보안 작업을 지정합니다. 입력하는 값은 찾으려는 값과 정확히 일치해야 합니다. 그러나 대/소문자는 중요하지 않습니다. 연결, 파일, 침입, 악성코드, Syslog 및 NetFlow 이벤트 유형에 대해 서로 다른 값을 입력합니다.


- 연결 이벤트 유형의 경우 필터는 AC\_RuleAction 특성에서 일치 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.
  - 파일 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allow(허용), Block(차단), Trust(신뢰)일 수 있습니다.
  - 침입 이벤트 유형의 경우 필터는 InLineResult 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Allowed(허용됨), Blocked(차단됨), Trusted(신뢰할 수 있음)일 수 있습니다.
  - 악성코드 이벤트 유형의 경우 필터는 FileAction 속성에서 일치하는 항목을 검색합니다. 이러한 값은 Cloud Lookup Timeout(클라우드 조회 시간 초과)일 수 있습니다.
  - Syslog 및 NetFlow 이벤트 유형의 경우 필터는 Action(작업) 속성에서 일치하는 항목을 검색합니다.
- **센서 ID** - 센서 ID는 이벤트가 보안 이벤트 커넥터로 전송되는 관리 IP 주소입니다.  
FDM 관리 디바이스의 경우 센서 ID는 일반적으로 디바이스 관리 인터페이스의 IP 주소입니다.
  - **IP 주소**
    - 이니시에이터 - 네트워크 트래픽 소스의 IP 주소입니다. Initiator address(이니시에이터 주소) 필드의 값은 이벤트 세부사항의 InitiatorIP(이니시에이터 IP) 필드 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
    - 응답자 - 패킷의 대상 IP 주소입니다. Destination address(대상 주소) 필드의 값은 이벤트 세부사항의 ResponderIP 필드에 있는 값에 해당합니다. 단일 주소(예: 10.10.10.100) 또는 CIDR 표기법으로 정의된 네트워크(예: 10.10.10.0/24)를 입력할 수 있습니다.
  - **포트**
    - 이니시에이터-세션 이니시에이터가 사용하는 포트 또는 ICMP 유형입니다. 소스 포트의 값은 이벤트 세부정보의 InitiatorPort 값에 해당합니다. (범위 추가 - 시작 포트 종료 포트 및 이니시에이터와 응답자 사이 또는 둘 다 사이에 공백)
    - **Responder(응답기)**-세션 responder가 사용하는 포트 또는 ICMP 코드입니다. 대상 포트의 값은 이벤트 세부사항의 ResponderPort 값에 해당합니다.

단계 6 (선택 사항) View(보기) 탭에서 클릭하여 필터를 사용자 지정 필터로 저장합니다.

## NetFlow 이벤트만 필터링

이 절차에서는 ASA NetFlow 이벤트만 찾습니다.


## Procedure

- 단계 1 CDO 메뉴 모음에서 분석 > 이벤트 로깅을 선택합니다.
  - 단계 2 Filter(필터) 아이콘  을 클릭하고 필터를 열린 상태로 고정합니다.
  - 단계 3 Netflow ASA 이벤트 필터를 확인합니다.
  - 단계 4 다른 모든 ASA 이벤트 필터를 지웁니다.
- ASA NetFlow 이벤트만 Event Logging(이벤트 로깅) 테이블에 표시됩니다.

## ASA 또는 FDM-관리 장치 syslog 이벤트에 대한 필터링(ASA NetFlow 이벤트 제외)

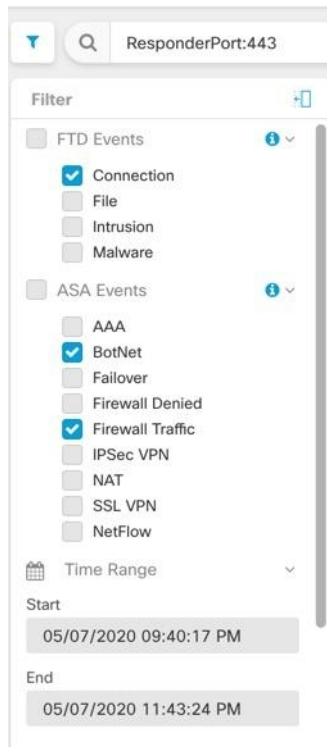
이 절차에서는 Syslog 이벤트만 찾습니다.

## Procedure

- 단계 1 CDO 메뉴 모음에서 분석 > 이벤트 로깅을 선택합니다.
- 단계 2 Filter(필터) 아이콘  을 클릭하고 필터를 열린 상태로 고정합니다.
- 단계 3 필터 표시줄의 맨 아래로 스크롤하여 **Include NetFlow Events(NetFlow 이벤트 포함)** 필터가 선택 취소되었는지 확인합니다.
- 단계 4 ASA Events(이벤트) 필터 트리로 다시 스크롤하여 **NetFlow** 상자가 선택 취소되었는지 확인합니다.
- 단계 5 ASA 또는 FDM 필터 기준의 나머지를 선택합니다.

## 필터 요소 결합

필터링 이벤트는 일반적으로 CDO의 표준 필터링 규칙을 따릅니다. 필터링 범주는 "AND"되고 범주 내의 값은 "OR"됩니다. 필터를 사용자 고유의 검색 기준과 결합할 수도 있습니다. 이벤트 필터의 경우 그러나 디바이스 이벤트 필터도 "OR"됩니다. 예를 들어 필터에서 다음 값을 선택한 경우,



이 필터를 사용하면 CDO는 위협 방어 디바이스 연결 이벤트 또는 ASA BotNet 또는 방화벽 트래픽 이벤트 및 시간 범위의 두 번 사이에 발생한 이벤트 및 ResponderPort 443도 포함하는 이벤트를 표시합니다. 시간 범위 내의 기록 이벤트를 기준으로 필터링할 수 있습니다. 라이브 이벤트 페이지에는 항상 최신 이벤트가 표시됩니다.

#### 특정 속성: 값 쌍 검색

검색 필드에 이벤트 속성 및 값을 입력하여 라이브 또는 기록 이벤트를 검색할 수 있습니다. 이 작업을 수행하는 가장 쉬운 방법은 검색하려는 Event Logging(이벤트 로깅) 테이블의 속성을 클릭하는 것입니다. 그러면 CDO가 Search(검색) 필드에 해당 속성을 입력합니다. 롤오버하면 클릭할 수 있는 이벤트가 과란색으로 표시됩니다. 예를 들면 다음과 같습니다.



## Event Logging

Historical
Live

InitiatorIP: "10.10.11.11" AND EventType: "3" ?

Clear
Time Range
After 05/03/2023 07:23:40 PM

+ Views
View 1

Date/Time	Device Type	Event Type	Sensor ID / Hostname	Initiator IP
May 3, 2023, 7:23:40 PM	ASA	3		

Action	Deny	IngressACLID
ConnectorID	08c0a888-b619-4f1a-a655-d4bd005dd8c8	IngressInterface
DeviceType	ASA	InitiatorIP
EgressInterface	4	InitiatorPort
EventType	3	LastPacketSecond
FirewallExtendedEvent	1001	MappedInitiatorIP
ICMPCode	0	MappedInitiatorPort
ICMPType	0	MappedResponderIP

이 예에서는 InitiatorIP 값 10.10.11.11을 롤오버하고 이를 클릭하여 검색을 시작했습니다. 이니시에이터 IP 및 해당 값이 검색 문자열에 추가되었습니다. 다음으로, Event Type(이벤트 유형) 3를 클릭하여 검색 문자열에 추가하고 CDO에서 AND를 추가했습니다. 따라서 이 검색의 결과는 10.10.11.11에서 시작된 이벤트 및 3 이벤트 유형의 목록이 됩니다.

위의 예에서 값 3 옆에 돋보기가 있습니다. 돋보기를 롤오버하는 경우 AND, OR, AND NOT, OR NOT 연산자를 선택하여 검색에 추가할 값을 입력할 수도 있습니다.

아래 예에서는 "OR"가 선택되었습니다. 이 검색의 결과는 10.10.11.11에서 시작된 이벤트 또는 106023 이벤트 유형의 목록이 됩니다. 검색 필드가 비어 있고 테이블에서 값을 마우스 오른쪽 버튼으로 클릭하면 다른 값이 없으므로 NOT만 사용할 수 있습니다.

The screenshot shows the Event Logging interface with a search filter for InitiatorIP: "10.10.11.11" AND EventType: "3". A dropdown menu is open, highlighting logical operators: AND, OR, NOT, AND NOT, and OR NOT. The main table displays event details for May 3, 2023, 7:23:40 PM on an ASA device. The event type is 3, and the action is Deny. The connector ID is 08c0a888-b619-41bd005dd8c8. The device type is ASA, egress interface is 4, and firewall extended event is 1001. The ICMP code and type are 0. The table also lists sensor ID/hostnames and initiator IPs.

값을 롤오버하고 파란색으로 강조 표시되면 해당 값을 검색 문자열에 추가할 수 있습니다.

### AND, OR, NOT, AND NOT, OR NOT 필터 연산자

검색 문자열에서 사용되는 "AND", "OR", "NOT", "AND NOT" 및 "OR NOT"의 동작은 다음과 같습니다.

#### AND

필터 문자열에서 AND 연산자를 사용하여 모든 특성을 포함하는 이벤트를 찾습니다. AND 연산자는 검색 문자열을 시작할 수 없습니다.

예를 들어 아래의 검색 문자열은 이니시에이터IP 주소 10.10.10.43에서 시작되고 이니시에이터 포트 59614에서 전송된 TCP 프로토콜 AND를 포함하는 이벤트를 검색합니다. 각 추가 AND 문을 사용하여 기준을 충족하는 이벤트의 수가 점점 더 적을 것으로 예상됩니다.

Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"

또는

필터 문자열에서 **OR** 연산자를 사용하여 특성을 포함하는 이벤트를 찾습니다. **OR** 연산자는 검색 문자열을 시작할 수 없습니다.

예를 들어 아래의 검색 문자열은 TCP 프로토콜을 포함하는 이벤트를 포함하는 이벤트, 또는 이니시에이터 IP 주소 10.10.10.43에서 시작된 또는 이니시에이터 포트 59614에서 전송된 이벤트를 표시합니다. 각 추가 **OR** 문에서 기준을 충족하는 이벤트의 수가 점점 더 커질 것으로 예상됩니다.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

### NOT

특정 속성이 있는 이벤트를 제외하려면 검색 문자열의 시작 부분에만 이를 사용하십시오. 예를 들어 이 검색 문자열은 InitiatorIP 192.168.25.3인 이벤트를 결과에서 제외합니다.

```
NOT InitiatorIP: "192.168.25.3"
```

### AND NOT

특정 특성을 포함하는 이벤트를 제외하려면 필터 문자열에서 **AND NOT** 연산자를 사용합니다. **AND NOT**은 검색 문자열의 시작 부분에 사용할 수 없습니다.

예를 들어 이 필터 문자열은 InitiatorIP 192.168.25.3인 이벤트를 표시하지만 ResponderIP 주소가 10.10.10.1인 이벤트는 표시하지 않습니다.

```
InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

**NOT**과 **AND NOT**을 조합하여 여러 속성을 제외할 수도 있습니다. 예를 들어 이 필터 문자열은 InitiatorIP 192.168.25.3의 이벤트 및 ResponderIP 10.10.10.1의 이벤트를 제외합니다.

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

### OR NOT

특정 요소를 제외하는 검색 결과를 포함하려면 **OR NOT** 연산자를 사용합니다. **OR NOT** 연산자는 검색 문자열의 시작 부분에 사용할 수 없습니다.

예를 들어 이 검색 문자열은 프로토콜이 TCP인 이벤트 또는 InitiatorIP가 10.10.10.43인 이벤트 또는 InitiatorPort 59614가 아닌 이벤트를 찾습니다.

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

(프로토콜: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614")를 검색할 수도 있습니다.

### 와일드카드 검색

이벤트 내에서 결과를 찾으려면 **attribute:value** 검색의 value 필드에서 와일드카드를 나타내려면 별표(\*)를 사용합니다. 예를 들어, 이 필터 문자열

```
URL:*feedback*
```

은 문자열 **feedback**을 포함하는 이벤트의 URL 특성 필드에서 문자열을 찾습니다.

관련 정보:

- [이벤트 로깅 페이지의 열 표시 및 숨기기](#)
- [Security Analytics and Logging의 이벤트 속성](#)

## 백그라운드에서 기록 이벤트 검색

CDO는 검색 기준을 정의하고 정의된 검색 기준에 따라 이벤트 로그를 검색하는 기능을 제공합니다. 백그라운드 검색 기능을 사용하여 백그라운드에서 이벤트 로그 검색을 수행하고 백그라운드 검색이 완료되면 검색 결과를 볼 수도 있습니다.

구성한 구독 알림 및 서비스 통합을 기반으로 백그라운드 검색이 완료되면 알림을 받습니다.

백그라운드 검색 페이지에서 직접 검색 결과를 보거나 다운로드하거나 삭제할 수 있습니다. 또한 백그라운드 검색이 일회성 이벤트에 대해 실행되도록 예약하거나 반복 일정을 예약할 수도 있습니다. 알림 설정 페이지로 이동하여 구독 옵션을 보거나 수정합니다.

## 이벤트 로깅 페이지에서 이벤트 검색

검색 및 백그라운드 검색 기능을 사용하여 Event Logging(이벤트 로깅) 페이지에서 로깅된 모든 이벤트를 볼 수 있습니다. 백그라운드 검색은 기록 이벤트에 대해서만 수행할 수 있습니다.

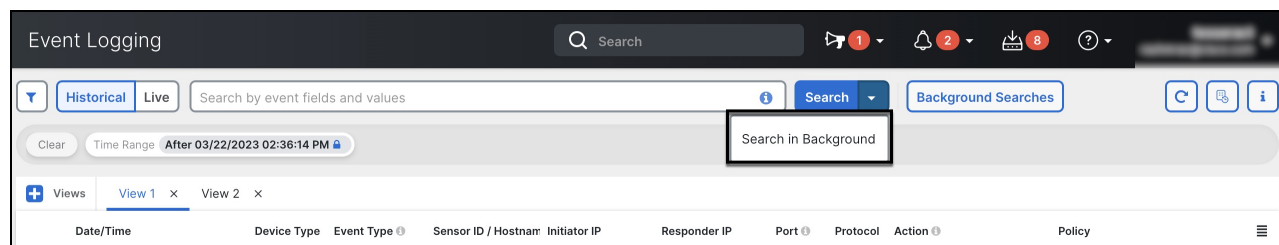
프로시저

단계 1 탐색 모음에서 분석 > 이벤트 로깅을 선택합니다.

단계 2 **Historical**(기록) 또는 **Live**(라이브) 탭을 클릭합니다.

단계 3 내비게이션 창으로 이동하여 검색식을 입력하고 **Search**(검색) 버튼을 입력하여 검색을 실행합니다. 절대 시간 범위 또는 상대 시간 범위를 사용하여 검색을 좁히거나 확장할 수 있습니다.

또는 **Search**(검색) 드롭다운 목록에서 **Search in Background**(백그라운드에서 검색)를 선택하여 검색 페이지에서 벗어나 있는 동안 백그라운드에서 검색을 실행합니다. 검색 결과가 준비되면 알림이 표시됩니다.



**Search**(검색) 버튼을 클릭하면 결과가 Event Logging(이벤트 로깅) 보기에 직접 나타납니다. 특정 검색 결과를 선택하면 쉽게 참조할 수 있도록 검색 기준이 검색 창에 나타납니다.

백그라운드에서 검색을 실행하도록 선택하면 검색 작업이 대기열에 추가되고 검색이 완료되면 알림이 표시됩니다. 백그라운드에서 여러 검색 쿼리를 실행할 수 있습니다.

단계 4 **Background Searches**(백그라운드 검색) 버튼을 클릭하여 Background Searches(백그라운드 검색) 페이지를 봅니다.

Background Searches ✕

[Start a Background Search](#)
[View Notification Settings](#)

Search Name	File Size	User	Status	Run Time	Actions
<input type="checkbox"/> Search_1679428080471	3.74 KB	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 3:48:03 PM Completed in 2 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>
<input type="checkbox"/> Search_1679428045727	3.74 KB	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 3:47:27 PM Completed in 2 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>
<input type="checkbox"/> Search_1679427993327	2.25 KB	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 3:46:35 PM Completed in 2 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>
<input type="checkbox"/> Search_167942230313	662 Bytes	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 1:58:39 PM Completed in 3 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>
<input type="checkbox"/> Search_1679408015574	662 Bytes	admin@example.com	✔ Completed (Expires in 5 days)	Started Mar 21, 2023, 10:13:44 AM Completed in 3 seconds	<a href="#">View</a> <a href="#">Download</a> <a href="#">...</a>

[Close](#)

Background Searches(백그라운드 검색) 페이지에 검색 결과 목록이 표시됩니다. 검색 결과를 보거나, 다운로드하거나, 삭제할 수 있습니다. 알림 설정 페이지로 이동하여 구독 옵션을 보거나 편집할 수도 있습니다. 이 페이지에서 검색을 시작하려면 **Start a Background Search**(백그라운드 검색 시작) 버튼을 선택합니다.

구독 옵션을 보거나 수정하는 방법에 대한 정보는 [알림 설정, 53 페이지](#)을 참조하십시오.

다음에 수행할 작업

반복 쿼리가 필요한 경우, 모든 백그라운드 검색을 예약된 백그라운드 검색으로 전환할 수 있습니다. 자세한 내용은 [이벤트 뷰어에서 백그라운드 검색 예약, 751 페이지](#)를 참조하십시오.

## 이벤트 뷰어에서 백그라운드 검색 예약

이벤트 뷰어 페이지에서 백그라운드에서 반복 쿼리를 예약합니다. 검색은 기록 이벤트에 대해서만 예약할 수 있습니다. 예약된 검색은 언제든지 수정하거나 취소할 수 있습니다. 기존 쿼리를 반복 검색으로 수정할 수도 있습니다.



**참고** 시작, 완료 또는 실패한 검색에 대한 알림을 수신하도록 선택할 수 있습니다. 자세한 내용은 [알림 설정, 53 페이지](#)를 참조하십시오.

기록 이벤트에 대해서만 백그라운드 검색을 예약할 수 있습니다. 예약 백그라운드 검색을 생성하려면 다음 단계를 수행하십시오.

프로시저

단계 1 탐색 모음에서 **Analytics**(애널리틱스) > **Event Logging**(이벤트 로깅)를 선택합니다.

- 단계 2 **Historical**(기록) 토글을 클릭하여 선택합니다. 기록 이벤트에 대한 백그라운드 검색만 예약할 수 있습니다.
- 단계 3 검색창에 검색하려는 검색 표현식을 입력합니다. **Search**(검색) 드롭다운 버튼을 클릭하고 **Search in background**(백그라운드에서 검색)를 선택합니다.
- 단계 4 (선택 사항) 검색 이름을 변경합니다.
- 단계 5 기본적으로 **Search Now**(지금 검색) 확인란이 선택되어 있습니다. 선택된 경우, 저장 시 검색이 시작됩니다. 이 확인란을 선택하지 않으면 백그라운드 쿼리가 향후 검색으로에서만 실행됩니다.
- 단계 6 **Setup recurring schedule**(설정 반복 예약)을 확인하고 다음 설정을 구성합니다.
- **Search Logs for the Last**(마지막 검색 로그) - 얼마나 이전까지 검색하고자 하는지입니다.
  - **Frequency**(빈도) - 예약 검색을 얼마나 자주 수행할지 선택합니다.
- 단계 7 창 하단에서 예약된 검색 기준을 확인합니다. **Schedule and Search Now**(지금 예약 및 검색)를 선택합니다. 또는 즉시 검색을 시작하도록 선택하지 않은 경우 버튼이 **Schedule Search**(검색 예약)로 표시됩니다.

---

다음에 수행할 작업

예약된 백그라운드 검색의 결과는 CDO에서 자동으로 삭제하기 전 최대 7일 동안 검토할 수 있습니다.

## 백그라운드 검색 다운로드

검색 결과 및 일정 쿼리는 CDO가 자동으로 제거하기 전까지 7일 동안 저장됩니다. 과거 이벤트에 대해 수행된 백그라운드 검색의 CSV 복사본을 다운로드합니다.

프로시저

- 단계 1 내비게이션 바에서 **Analytics**(분석) > **Event Logging**(이벤트 로깅)으로 이동합니다.
- 단계 2 **Background Searches**(백그라운드 검색) > **Actions**(작업) > **Download**(다운로드)를 클릭합니다.
- 단계 3 검색을 찾습니다. 예약된 검색은 **Queries**(쿼리) 탭에 저장됩니다.
- 단계 4 **Download**(다운로드)를 클릭합니다. .CSV 파일은 로컬 드라이브의 기본 스토리지 위치에 자동으로 다운로드됩니다.

## 데이터 스토리지 요금제

Cisco Cloud가 온보딩된 ASA 및 FDM 매니지드 디바이스에서 매일 수신하는 이벤트 수를 반영하는 데이터 스토리지 요금제를 구매해야 합니다. 이를 "일일 수집 속도"라고 합니다. 데이터 요금제는 1

년, 3년 또는 5년 단위의 GB/일 단위로 제공됩니다. 수집 속도를 결정하는 가장 좋은 방법은 Secure Logging Analytics(SaaS)를 구매하기 전에 무료 평가판에 참여하는 것입니다. 이를 통해 이벤트 볼륨을 적절하게 예측할 수 있습니다.

고객은 90일의 롤링 데이터 스토리지를 자동으로 수신합니다. 즉, 최근 90일간의 이벤트가 Cisco Cloud에 저장되고 91일이 되면 삭제됩니다.

고객은 기본 90일 이상의 추가 이벤트 보존으로 업그레이드하거나 기존 구독에 변경 주문을 통해 일일 볼륨(GB/일)을 추가할 수 있으며, 남은 구독 기간에 대해서만 일할 계산하여 청구됩니다.

데이터 요금제에 대한 자세한 내용은 [Secure Logging Analytics\(SaaS\) 주문 가이드](#)를 참조하십시오.



**Note** Security Analytics and Logging 라이선스 및 데이터 요금제를 보유하고 있는 경우 나중에 다른 Security Analytics and Logging 라이선스를 취득할 수 있으며, 다른 데이터 요금제를 구매할 필요가 없습니다. 네트워크 트래픽 처리량이 변경되어 다른 데이터 플랜을 취득하는 경우에는 다른 Security Analytics and Logging 라이선스를 구입하지 않아도 됩니다.

내 할당량에 대해 어떤 데이터가 계산됩니까?

보안 이벤트 커넥터로 전송된 모든 이벤트는 Secure Logging Analytics(SaaS) 클라우드에 누적되며 데이터 할당량에 포함됩니다.

이벤트 뷰어에 표시되는 내용을 필터링해도 Secure Logging Analytics(SaaS) 클라우드에 저장된 이벤트 수는 줄어들지 않으며, 이벤트 뷰어에서 볼 수 있는 이벤트 수는 줄어듭니다.

이벤트는 90일 동안 Secure Logging Analytics(SaaS) 클라우드에 저장됩니다. 그 후에는 제거됩니다.

스토리지 할당량을 빠르게 사용하고 있습니다. 어떻게 해야 합니까?

이 문제를 해결하는 두 가지 방법은 다음과 같습니다.

- **추가 스토리지를 요청합니다.** 필요한 것을 과소 평가했을 수 있습니다.
- 이벤트를 로깅하는 규칙의 수를 줄입니다. SSL 정책 규칙, 보안 인텔리전스 규칙, 액세스 제어 규칙은 물론 침입 정책, 파일 및 악성코드 정책에서도 이벤트를 로깅할 수 있습니다. 로깅 대상을 확인합니다. 생각보다 많은 규칙 및 정책에서 이벤트를 로깅해야 합니까?

## 이벤트 스토리지 기간 연장 및 이벤트 스토리지 용량 늘리기

Security Analytics and Logging(보안 분석 및 로깅) 고객은 이러한 [라이선싱](#)을 구매할 때 90일의 이벤트 스토리지를 받게 됩니다.

- 로깅 및 문제 해결
- 로깅 분석 및 탐지
- 총 네트워크 분석 및 모니터링

라이선스를 처음 구매할 때 또는 라이선스 기간 중 언제든지 1년, 2년 또는 3년치 롤링 이벤트 스토리지로 업그레이드하도록 선택할 수 있습니다.

Security Analytics and Logging 라이선스를 처음 구매할 때 스토리지 용량을 업그레이드할지 묻는 메시지가 표시됩니다. "예"라고 답하면 구매 중인 PID 목록에 추가 PID(Product Identifier)가 추가됩니다.

라이선스 기간 중간에 롤링 이벤트 스토리지를 연장하거나 이벤트 클라우드 스토리지의 양을 늘리기로 결정한 경우 다음을 수행할 수 있습니다.

프로시저

단계 1 [Cisco Commerce](#)에 사용자 계정으로 로그인합니다.

단계 2 Cisco Defense Orchestrator PID를 선택합니다.

단계 3 프롬프트에 따라 스토리지 용량의 길이 또는 용량을 업그레이드합니다.

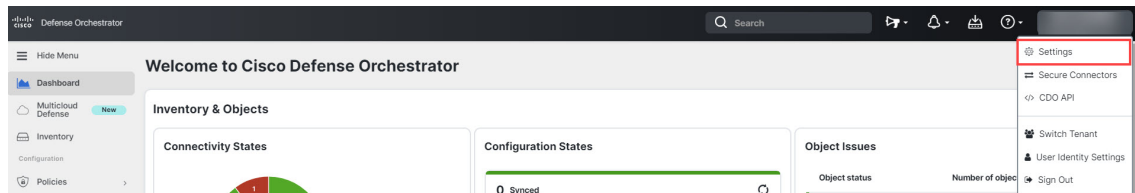
증가된 비용은 기존 라이선스의 남은 기간에 따라 비례 배분됩니다. 자세한 지침은 [Secure Logging Analytics\(SaaS\) 주문 가이드](#)를 참조하십시오.

## 보안 애널리틱스 및 로깅 데이터 계획 사용량 보기

월별 로깅 제한, 사용한 스토리지의 양, 사용 기간이 0으로 재설정된 경우를 확인하려면 다음을 수행합니다.

### Procedure

단계 1 테넌트를 클릭하고 **Settings(설정)**를 선택합니다.



단계 2 **Logging Settings(로깅 설정)**를 클릭합니다.

단계 3 **View Historical Usage(기록 사용량 보기)**를 클릭하여 최근 12개월까지의 스토리지 사용량을 확인할 수도 있습니다.



# SaaS(Secure Logging Analytics)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기

SaaS(Secure Logging Analytics)를 사용하면 ASA 또는 FDM 관리 디바이스에서 SEC(Secure Event Connector)의 특정 UDP, TCP 또는 NSEL 포트에 이벤트를 보낼 수 있습니다. 그런 다음 SEC는 해당 이벤트를 Cisco 클라우드로 전달합니다.

이러한 포트가 아직 사용 중이 아닌 경우, SEC는 이벤트를 수신하는 데 포트를 제공하며, SaaS(Secure Logging Analytics) 설명서에서는 기능을 구성할 때 포트 사용을 권장합니다.

- TCP: 10125
- UDP: 10025
- NSEL: 10425

이러한 포트가 이미 사용 중인 경우 SaaS(Secure Logging Analytics)를 구성하기 전에 SEC 디바이스 세부 정보를 확인하여 실제로 이벤트를 수신하는 데 사용 중인 포트를 확인합니다.

SEC에서 사용하는 포트 번호를 찾으려면 다음을 수행합니다.

## Procedure

단계 1 CDO 메뉴에서 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 2 Secure Connector(보안 커넥터) 페이지에서 이벤트를 전송할 SEC를 선택합니다.

단계 3 Details(세부 정보) 창에 이벤트를 전송해야 하는 TCP, UDP 및 NetFlow(NSEL) 포트가 표시됩니다.

Boston-SEC	
Details	
ID	54b039f6-8944-46a4-ac07
Tenant ID	0a2cdcb4-5e63-4491-9fda
Version	202004270848
IP Address	192.168.25.4
TCP Port	10125
UDP Port	10025
NetFlow Port	10425





# 6 장

## CDO와 Cisco Security Cloud Sign On 통합

• [SecureX 및 CDO, on page 757](#)

### SecureX 및 CDO

Cisco SecureX 플랫폼은 가시성을 통합하고 자동화를 가능하게 하며 네트워크, 엔드포인트, 클라우드 및 애플리케이션 전반에서 보안을 강화하는 일관된 경험을 위해 Cisco의 광범위한 통합 보안 포트폴리오와 고객의 인프라를 연결합니다. 통합 플랫폼에서 기술을 연결함으로써 SecureX는 측정 가능한 통찰력, 바람직한 결과 및 더할 나위 없는 팀 간 협업을 제공합니다. SecureX가 무엇이고 이 플랫폼이 제공하는 기능에 대한 자세한 내용은 [SecureX 정보](#)를 참조하십시오.

SecureX가 CDO 테넌트에 액세스하도록 허용하면 총 디바이스 수는 물론 오류가 있는 디바이스, 충돌이 있는 디바이스 및 현재 동기화되지 않을 수 있는 디바이스를 포함하여 디바이스 이벤트가 요약됩니다. 이벤트 요약은 또한 현재 적용된 정책 및 해당 정책과 관련된 개체를 집계하는 두 번째 창을 제공합니다. 정책은 디바이스 유형으로 정의되며 개체는 개체 유형을 통해 식별됩니다.

SecureX 대시보드에 CDO 모듈을 추가하려면 여러 단계가 필요합니다. 자세한 내용은 [CDO를 SecureX에 추가](#)를 참조하십시오.



**Warning** CDO 및 SecureX 계정을 아직 병합하지 않은 경우, 온보딩된 모든 디바이스에 대한 이벤트가 표시되지 않을 수 있습니다. SecureX에서 CDO 모듈을 생성하기 전에 계정을 병합하는 것을 강력히 권장합니다. 자세한 내용은 [CDO 및 SecureX 계정 병합](#)을 참조하십시오.

#### SecureX 리본

SecureX 리본은 SecureX 계정 생성 여부와 상관없이 CDO에서 사용할 수 있습니다. 페이지 하단에 있

는 SecureX 탭  을 클릭하여 리본을 확장합니다.

리본을 사용하려면 SecureX 계정을 확인해야 합니다. SecureX에 액세스하는 데 사용하는 것과 동일한 인증 로그인을 사용하는 것이 좋습니다. 리본이 인증되면 CDO에서 직접 SecureX 기능을 활용할 수 있습니다.

자세한 내용은 [SecureX 리본 설명서](#)를 참조하십시오.

### SecureX 문제 해결

이 경험에는 두 가지 제품이 포함됩니다. 발생할 수 있는 문제를 식별, 해결 또는 문의하는 데 도움이 되도록 [SecureX 문제 해결](#), on page 816을 참조하십시오.

관련 정보:

- [SecureX 정보](#)
- [CDO 및 SecureX 계정 병합](#)
- [CDO에서 SecureX 연결](#), on page 759
- [CDO에서 SecureX 연결 끊김](#), on page 760
- [CDO를 SecureX에 추가](#)
- [SecureX 문제 해결](#), on page 816

## CDO 및 SecureX 계정 병합

이미 SecureX 또는 CTR(Cisco Threat Response) 계정이 있는 경우 디바이스를 SecureX에 등록하려면 CDO 테넌트와 SecureX/CTR 계정을 병합해야 합니다. 계정을 SecureX 포털에 병합할 수 있습니다. CDO 모듈을 만들기 전에 계정을 병합하는 것이 매우 좋습니다. 계정이 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 이용할 수 없습니다.



**Note** 이 프로세스를 시작할 때 유의하십시오. CDO를 SecureX에 병합하는 데에는 시간이 오래 걸릴 수 있습니다.

자세한 내용은 [계정 병합](#)을 참조하십시오.



**Note** 둘 이상의 지역 클라우드에 계정이 있는 경우 각 지역 클라우드에 대해 별도로 계정을 병합해야 합니다.

관련 정보:

- [SecureX 및 CDO](#)
- [CDO를 SecureX에 추가](#)
- [SecureX 문제 해결](#)

## CDO를 SecureX에 추가

SecureX가 등록된 디바이스에 액세스하도록 허용하고 SecureX 대시보드에 CDO 모듈을 추가하여 보안 포트폴리오의 다른 Cisco 플랫폼과 함께 디바이스 정책 및 개체 요약을 확인합니다.



**Note** 이 프로세스를 시작할 때 유의하십시오. CDO를 SecureX에 병합하는 데에는 시간이 오래 걸릴 수 있습니다.

시작하기 전에

CDO에서 SecureX를 연결하기 전에 다음 항목을 작업하는 것이 매우 좋습니다.

- 최소한 SecureX 계정에 대한 관리자여야 합니다.
- CDO 테넌트에 대한 슈퍼 관리자 사용자 역할이 있어야 합니다.
- 테넌트 통신을 용이하게 하기 위해 보안 서비스 익스체인지에 테넌트 계정을 병합합니다. 자세한 내용은 [CDO 및 SecureX 계정 병합](#)을 참조하십시오.
- CDO 테넌트를 보안 서비스 익스체인지와 병합한 후, CDO 테넌트에서 로그아웃하고 다시 로그인해야 합니다.
- 아직 구성하지 않은 경우 Cisco Secure Sign-On을 MFA(Multi-Factor Authentication)용 SAML SSO(Single Sign-On IdP) 및 Duo Security로 구성합니다. CDO 및 SecureX는 이를 인증 방법으로 사용합니다. 자세한 내용은 [SAML SSO\(Single Sign-On\)를 Cisco Defense Orchestrator와 통합](#)을 참조하십시오.



**Note** 참고: 테넌트가 여러 개인 경우 SecureX에서 테넌트당 하나의 모듈을 생성해야 합니다. 각 테넌트는 인증을 위해 고유한 API 토큰이 필요합니다.

## CDO에서 SecureX 연결

SecureX 및 CDO 계정을 병합한 후 두 플랫폼 간의 통신을 승인하고 수동으로 CDO 모듈을 SecureX 대시보드에 추가하도록 활성화해야 합니다. CDO UI를 통해 SecureX를 연결하고 보안 포트폴리오의 다른 Cisco 플랫폼과 함께 디바이스의 정책, 이벤트 유형, 개체 등에 대한 요약을 확인합니다.



**Note** SecureX 대시보드에 구성된 CDO 모듈이 이미 있는 경우 **Connect Tenant to SecureX** 옵션은 중복 CDO 모듈을 생성합니다. 이 문제가 발생하면 자세한 내용은 [SecureX 문제 해결](#)을 참조하십시오.

다음 절차를 사용하여 CDO에서 API 토큰을 조달하고 CDO 모듈을 SecureX에 추가합니다.

### Procedure

단계 1 CDO에 로그인합니다.

단계 2 오른쪽 상단 모서리에 있는 사용자 메뉴에서 **Settings(설정)**을 선택합니다.

단계 3 창 왼쪽에서 **General Settings(일반 설정)** 탭을 선택합니다.

- 단계 4 **Tenant Settings**(테넌트 설정) 섹션을 찾아 **Connect SecureX**(SecureX 연결)를 클릭합니다. 브라우저 창이 SecureX 로그인 페이지로 리디렉션됩니다. CDO 테넌트와 연결하려는 조직 자격 증명으로 SecureX에 로그인합니다.
- 단계 5 SecureX에 성공적으로 로그인하면 브라우저가 자동으로 다시 CDO로 리디렉션됩니다. **General Settings**(일반 설정) 페이지의 **User Management**(사용자 관리) 탭에서 SecureX에 로그인한 조직의 이름을 포함하는 새 사용자를 볼 수 있습니다. 이 사용자는 읽기 전용이며 SecureX로 데이터를 보내는 데만 사용됩니다.

## CDO에서 SecureX 연결 끊김

CDO와 SecureX 조직 간의 통신 요청 연결을 끊을 수 있습니다. 이 옵션은 SecureX에서 조직을 제거하지 않지만, CDO에서 읽기 전용 API 사용자를 제거하고 이전에 SecureX 조직과 연결된 테넌트는 이벤트 보고서 전송을 중지합니다.

이것은 CDO의 SecureX 리본에서 테넌트를 로그아웃하거나, 어떠한 방식으로든 리본을 비활성화하지 않습니다. 리본에서 로그아웃하려면 **Support Case Manager**(지원 사례 매니저)에서 사례를 열어 리본 로그인을 수동으로 재설정해야 합니다. 이 요청은 테넌트를 리본에서 로그아웃합니다.

프로시저


- 단계 1 CDO에 로그인합니다.
- 단계 2 오른쪽 상단 모서리에 있는 사용자 메뉴에서 **Settings**(설정)을 선택합니다.
- 단계 3 창 왼쪽에서 **General Settings**(일반 설정) 탭을 선택합니다.
- 단계 4 **Tenant Settings**(테넌트 설정) 섹션을 찾아 **SecureX Disconnect**(연결 끊기)를 클릭합니다. **General Settings**(일반 설정) 페이지의 **User Management**(사용자 관리) 탭에서, SecureX로 데이터를 보내기 위해 생성된 읽기 전용 사용자가 삭제됩니다.

## CDO 타일을 SecureX에 추가

CDO 모듈을 활성화한 후 이제 CDO 타일을 SecureX 대시보드에 추가할 수 있습니다. 제품의 모듈은 CDO의 상태 정보에 액세스하고 두 가지 가능한 타일 선택을 통해 대시보드에 데이터를 보고합니다.

SecureX 대시보드에 CDO 타일을 추가하려면 다음 절차를 따르십시오.

### Procedure

- 단계 1 SecureX 대시보드 탭에서  **New Dashboard**(새 대시보드)를 클릭합니다. SecureX 대시보드에 처음 액세스하는 경우 **Add Tiles**(타일 추가)를 클릭할 수도 있습니다.
- 단계 2 (선택 사항) 대시보드 이름을 변경합니다.

**Tip**           테넌트가 여러 개인 경우 이 이름 변경 옵션을 사용하여 CDO 타일이 연결된 테넌트를 식별합니다.

**단계 3 Available Tiles(사용 가능한 타일)** 목록에서 CDO를 선택하고 옵션을 확장하여 사용 가능한 타일을 확인합니다. 대시보드에 포함하려는 모든 타일을 선택합니다.

- **CDO Device Summary(CDO 디바이스 요약)** - 이 타일에는 현재 CDO 테넌트에 온보딩된 모든 디바이스와 해당 상태가 나열됩니다.
- **CDO Objects and Policies(CDO 개체 및 선택)** - 이 타일에는 디바이스에 현재 적용된 모든 정책 및 해당 정책과 관련된 개체가 나열됩니다.

**Note**           CDO가 나열되지 않으면, SecureX에 저장된 CDO의 유효한 API 토큰이 없는 것입니다. 자세한 내용은 [CDO 타일을 SecureX에 추가](#)를 참조하십시오.

**단계 4 Save(저장)**를 클릭합니다.

---

관련 정보:

- [CDO 및 SecureX 계정 병합](#)
- [SecureX 문제 해결](#)







# 7 장

## 문제 해결

이 장에는 다음 섹션이 포함되어 있습니다.

- [FDM-관리 디바이스 문제 해결, on page 763](#)
- [보안 디바이스 커넥터 문제 해결, 774 페이지](#)
- [보안 이벤트 커넥터 문제 해결, on page 778](#)
- [문제 해결 Cisco Defense Orchestrator, on page 790](#)
- [디바이스 연결 상태, on page 800](#)
- [SecureX 문제 해결, on page 816](#)

## FDM-관리 디바이스 문제 해결

다음 문서를 사용하여 FDM 관리 디바이스 문제를 해결하십시오.

- [등록 키로 온보딩 중 디바이스 등록 실패 문제 해결](#)
- [FDM-관리 HA 생성 문제 해결, on page 773](#)

## 총괄 요약 보고서 문제 해결

이동하여 네트워크 운영 보고서를 생성했는데 예상한 결과 또는 데이터가 전혀 표시되지 않을 수 있습니다. 경우에 따라 요약에 **No data available**(사용 가능한 데이터 없음)이 표시될 수 있습니다. 몇 가지 시나리오를 살펴보겠습니다.

- CDO는 디바이스가 온보딩된 시간부터 **1시간**마다 이벤트를 폴링합니다. 일부 예약된 이벤트는 10분, 60분, 6시간 또는 24시간마다 다양한 시간 간격으로 폴링되는 여러 작업을 트리거할 수 있습니다. 선택한 디바이스가 방금 온보딩된 경우 데이터를 수집하고 컴파일하는 데 시간이 충분하지 않을 수 있습니다.
- 스마트 라이선스가 부족할 수 있습니다. 충분한 라이선스가 있는 디바이스만 데이터를 생성합니다. 원하는 데이터를 생성하는 데 필요한 스마트 라이선스를 확인하려면 [FDM-관리 디바이스 라이선싱 유형, on page 216](#)의 내용을 참조하십시오.

- 액세스 제어 규칙에 대한 로깅이 활성화되지 않았습니다. 자세한 내용은 [FDM-관리 액세스 제어 규칙의 로깅 설정, on page 375](#)를 참조하십시오.
- 선택한 시간 범위에 표시할 데이터가 부족하거나, 액세스 제어 규칙이 선택한 시간 범위 내에 트리거되지 않았을 수 있습니다. **Time Range**(시간 범위) 옵션 간에 전환하여 다른 기간이 보고서에 영향을 미치는지 확인합니다.

## FTD 온보딩 문제 해결

### 연결성

- ping으로 디바이스 연결을 확인합니다. ASA에서 직접 FP 관리 IP 주소를 ping해 보십시오. ICMP가 외부로부터의 통신을 차단하면 인터넷에서 FP 관리 인터페이스를 ping 할 수 없습니다. cUrl/wget은 구성된 IP/포트에서 FP 관리 인터페이스에 액세스할 수 있는지 확인하는 데 도움이 됩니다.
- 호환성을 위해 ASA 및/또는 ASDM 소프트웨어 버전을 확인합니다. 자세한 내용은 [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 참조하십시오.
- ASA 로그를 사용하여 CDO 트래픽이 ASA에 의해 차단되는지 확인합니다. SSH를 통해 FP HTTP 관리 인터페이스에 연결하려는 시도는 `/var/log/httpd/httpsd_access_log`에 기록됩니다.

### 모듈의 잘못된 구성

- 지원되지 않는 구성 모듈이 특정 요구 사항을 충족하지 않는 경우 CDO는 디바이스의 구성을 지원하지 못할 수 있습니다.

### HTTP 인증

- CDO는 온보딩 프로세스 중에 ASA 디바이스를 인증하기 위해 토큰 기반 SSO를 발급합니다. 멀티 컨텍스트 모드인 ASA의 경우 비관리 컨텍스트에서 FP 모듈을 온보딩하려고 하면 토큰 문제가 발생할 수 있습니다. 잘못된 토큰은 `/var/log/mojo/mojo.log`에서 **ASDM SSO** 로그인으로 식별됩니다.

## 라이선스 부족으로 인해 실패

디바이스 연결 상태가 "Insufficient License(라이선스 부족)"로 표시되면 다음을 수행합니다.

- 디바이스가 라이선스를 획득할 때까지 잠시 기다립니다. 일반적으로 Cisco Smart Software Manager가 디바이스에 새 라이선스를 적용하는 데 시간이 걸립니다.
- 디바이스 상태가 변경되지 않으면 CDO에서 로그아웃하고 다시 로그인하여 CDO 포털을 새로 고침한 후 라이선스 서버와 디바이스 간의 네트워크 통신 문제를 해결합니다.
- 포털을 새로 고침해도 디바이스 상태가 변경되지 않으면 다음을 수행합니다.

## Procedure

- 단계 1 **Cisco Smart Software Manager**에서 새 등록 키를 생성하고 복사합니다. 자세한 내용은 [스마트 라이선싱 생성](#) 비디오를 참조하십시오.
- 단계 2 CDO 탐색 모음에서 **Inventory**(재고 목록) 페이지를 클릭합니다.
- 단계 3 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 4 적절한 디바이스 유형 탭을 클릭하고 **Insufficient License**(라이선스 부족) 상태의 디바이스를 선택합니다.
- 단계 5 **Device Details**(디바이스 세부 정보) 창에서 **Insufficient Licenses**(불충분한 라이선스)에 표시되는 **Manage Licenses**(라이선스 관리)를 클릭합니다. **Manage Licenses**(라이선스 관리) 창이 나타납니다.
- 단계 6 **Activate**(활성화) 필드에 새 등록 키를 붙여넣고 **Register Device**(디바이스 등록)를 클릭합니다.

새 등록 키가 디바이스에 성공적으로 적용되면 연결 상태가 **Online**(온라인)으로 바뀝니다.


관련 정보:

- [위협 방어 디바이스 온보딩](#)
- [사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩, on page 184](#)
- [스마트 라이선스 적용 또는 업데이트](#)

## 등록되지 않은 디바이스 문제 해결

FDM 관리 디바이스가 Firewall Device Manager를 통해 클라우드에서 등록 취소되었을 수 있습니다. 클라우드에 디바이스를 다시 등록하려면 다음을 수행하십시오.

프로시저

- 단계 1 **Inventory**(인벤토리) 페이지에서 **Devices**(장치) 탭을 클릭합니다.
- 단계 2 **FTD** 탭을 클릭하고 "미등록된 디바이스" 상태의 디바이스를 선택하면 오른쪽의 오류 메시지가 표시됩니다.
- 단계 3 등록되지 않은 디바이스가 등록 키를 사용하여 온보딩된 경우, Cisco Defense Orchestrator는 이전에 적용된 키가 만료되었으므로 새 등록 키를 생성하라는 메시지를 표시합니다.
  - a) 새로 고침 버튼을 클릭하여 새 등록 키를 생성한 다음 Copy(복사) 아이콘 를 클릭합니다.
  - b) CDO에 등록하려는 디바이스의 Firewall Device Manager에 로그인합니다.
  - c) **System Settings**(시스템 설정)에서 **Cloud Services**(클라우드 서비스)를 클릭합니다.
  - d) Cisco Defense Orchestrator 영역에서 **Get Started**(시작하기)를 클릭합니다.
  - e) **Registration Key**(등록 키) 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.
  - f) **Register**(등록)를 클릭한 다음 Cisco 고지 사항을 수락합니다. Firewall Device Manager는 CDO에 등록 요청을 보냅니다.

- g) 디바이스의 연결 상태가 "읽기 오류"로 변경될 때까지 CDO에서 **Inventory**(인벤토리) 페이지를 새로 고칩니다.
  - h) 디바이스에서 구성을 읽으려면 CDO에 대한 **Read Configuration**(구성 읽기)를 클릭합니다.
- 단계 4** 등록되지 않은 디바이스가 일련 번호를 사용하여 온보딩된 경우, CDO는 Firewall Device Manager에서 디바이스를 자동 등록하라는 메시지를 표시합니다.
- a) CDO에 등록하려는 디바이스의 Firewall Device Manager에 로그인합니다.
  - b) **System Settings**(시스템 설정)에서 **Cloud Services**(클라우드 서비스)를 클릭합니다.
  - c) **Auto-enroll with Tenancy from Cisco Defense Orchestrator**(Cisco Defense Orchestrator에서 테넌시로 자동 등록) 옵션을 선택하고 **Register**(등록)를 클릭합니다.
  - d) 디바이스의 연결 상태가 "읽기 오류"로 변경될 때까지 CDO에서 **Inventory**(인벤토리) 페이지를 새로 고칩니다.
  - e) 디바이스에서 구성을 읽으려면 CDO에 대한 **Read Configuration**(구성 읽기)를 클릭합니다.

## 등록 키로 온보딩 중 디바이스 등록 실패 문제 해결

클라우드 서비스 **FQDN**을 확인하지 못함

클라우드 서비스 FQDN 확인 실패로 인해 디바이스 등록에 실패하면, 네트워크 연결 또는 DNS 구성을 확인하고 디바이스 온보딩을 다시 시도하십시오.

잘못된 등록 키로 인해 실패

잘못된 등록 키로 인해 디바이스 등록이 실패하는 경우로, 올바르게 않은 등록 키를 Firewall Device Manager에 붙여넣으면 발생할 수 있습니다.

Cisco Defense Orchestrator에서 동일한 등록 키를 다시 복사하고 디바이스 등록을 시도합니다. 디바이스에 이미 스마트 라이선스가 있는 경우 등록 키를 firewall device manager에 붙여넣기 전에 스마트 라이선스를 제거해야 합니다.

라이선스 부족으로 인해 실패

디바이스 연결 상태가 "Insufficient License(라이선스 부족)"로 표시되면 다음을 수행합니다.

- 디바이스가 라이선스를 획득할 때까지 잠시 기다립니다. 일반적으로 Cisco Smart Software Manager가 디바이스에 새 라이선스를 적용하는 데 시간이 걸립니다.
- 디바이스 상태가 변경되지 않으면 CDO에서 로그아웃하고 다시 로그인하여 CDO 포털을 새로 고침한 후 라이선스 서버와 디바이스 간의 네트워크 통신 문제를 해결합니다.
- 포털을 새로 고침해도 디바이스 상태가 변경되지 않으면 다음을 수행합니다.
  1. **Cisco Smart Software Manager**에서 새 등록 키를 생성하고 복사합니다. 자세한 내용은 **스마트 라이선싱 생성** 비디오를 참조하십시오.
  2. CDO 탐색 모음에서 **Inventory**(재고 목록) 페이지를 클릭합니다.

3. **Insufficient License**(불충분한 라이선스) 상태의 디바이스를 선택합니다.
  4. **Device Details**(디바이스 세부 정보)창에서 **Insufficient Licenses**(불충분한 라이선스)에 표시되는 **Manage Licenses**(라이선스 관리)를 클릭합니다. 라이선스 관리 창이 열립니다.
  5. **Activate**(활성화) 필드에 새 등록 키를 붙여넣고 **Register Device**(디바이스 등록)를 클릭합니다.
- 새 등록 키가 디바이스에 성공적으로 적용되면 연결 상태가 **Online**(온라인)으로 바뀝니다.

## 침입 방지 시스템 문제 해결

### 내 IPS 정책 옵션은 무엇입니까?

온보딩된 모든 디바이스는 "기본 재정의"라는 Cisco Defense Orchestrator 제공 IPS 정책에 자동으로 연결됩니다. CDO에서는 모든 FDM 관리 디바이스에 대해 새 IPS 정책을 생성하므로 이 이름을 가진 여러 정책이 있을 수 있습니다. 기본 IP 정책을 사용하지만 서명 오버라이드 옵션을 편집하려는 경우 자세한 내용은 [Firepower 침입 정책 서명 오버라이드](#)를 참조하십시오. 디바이스마다 다른 서명 오버라이드를 구성하면 기본 오버라이드 정책이 일관되지 않을 수 있습니다.

### 모든 디바이스에 대해 서로 다른 IPS 정책을 사용하려면 어떻게 해야 합니까?

CDO는 모든 FDM 관리 디바이스에 대해 새 IPS 정책을 생성하므로 이 이름을 가진 정책이 여러 개 있을 수 있습니다. 각 디바이스가 온보딩된 후 CDO 제공 IPS 정책의 이름을 바꿀 필요가 없습니다. 정책을 확장하면 연결된 디바이스가 표시되며 디바이스 또는 정책별로 위협 이벤트 페이지 및 서명 오버라이드 페이지를 필터링할 수도 있습니다. 기본 오버라이드 정책을 사용자 지정하려면 디바이스별로 서명 오버라이드를 구성합니다. 이로 인해 기본 오버라이드 침입 정책이 일관되지 않게 되지만 기능이 금지되지는 않습니다.

**FDM** 관리 디바이스에서 오버라이드가 구성된 디바이스를 온보딩했습니다.

CDO 외부에서 구성된 오버라이드는 디바이스 구성이나 기능에 문제를 일으키지 않습니다.

오버라이드가 이미 구성되어 있는 디바이스를 온보딩하고 이 새 디바이스가 오버라이드가 없는 디바이스와 IP 정책을 공유하는 경우 IPS 정책이 일관성 없음으로 표시됩니다. 일관성 없음을 해결하려면 [Firepower 침입 정책 서명 오버라이드](#)를 참조하십시오.

## SSL 암호 해독 문제 해결

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리(**SSL** 또는 인증 기관 피닝)

스마트폰 및 기타 디바이스용 일부 앱은 SSL(또는 인증 기관) 피닝이라는 기술을 사용합니다. SSL 피닝 기술은 원래 서버 인증서의 해시를 앱 자체에 포함합니다. 따라서 앱이 FDM 관리 디바이스에서 재서명된 인증서를 받으면 해시 검증에 실패하고 연결이 중단됩니다.

이때 기본적인 증상은 사용자가 사이트 앱을 사용해서는 웹 사이트에 연결할 수 없지만 웹 브라우저를 사용하면 연결할 수 있다는 것입니다(앱으로 연결에 실패한 디바이스에서 브라우저를 사용할 때도 연결 가능). 사용자가 Facebook iOS 또는 Android 앱은 사용할 수 없지만 Safari나 Chrome에서 <https://www.facebook.com/>을 입력하면 연결할 수 있는 경우를 예로 들 수 있습니다.

SSL 피닝은 특별히 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이러한 현상을 해결하는 방법은 없습니다. 다음 옵션 중에서 선택해야 합니다.

- 앱 사용자를 지원합니다. 이 경우 사이트로의 트래픽을 암호 해독할 수 없습니다. SSL Decryption(SSL 암호 해독) 규칙의 Application(애플리케이션) 탭에서 사이트 애플리케이션용 Do Not Decrypt(암호 해독 안 함) 규칙을 생성하고, 이 규칙을 연결에 적용할 Decrypt Re-sign(재서명 암호 해독) 규칙 앞에 배치합니다.
- 사용자들이 브라우저만 사용하도록 강제합니다. 사이트로의 트래픽을 암호 해독해야 하는 경우에는 사용자에게 네트워크를 통해 연결할 때 사이트 앱을 사용할 수 없으며 브라우저만 사용해야 함을 알려야 합니다.

#### 기타 세부정보

특정 사이트가 브라우저에서는 작동하는데 동일 디바이스의 앱에서는 작동하지 않는 경우 SSL 피닝 인스턴스를 살펴봐야 합니다. 하지만 심층적으로 확인하려면 연결 이벤트를 사용해 브라우저 테스트와 더불어 SSL 피닝을 확인할 수 있습니다.

앱은 두 가지 방식으로 해시 검증 장애를 처리할 수 있습니다.

- Facebook 등의 그룹 1 앱은 서버에서 SH, CERT, SHD 메시지를 받는 즉시 SSL ALERT 메시지를 보냅니다. Alert는 보통 SSL 피닝을 나타내는 "Unknown CA (48)(알 수 없는 CA(48))" 알림입니다. 알림 메시지 후에는 TCP Reset(TCP 재설정)이 전송됩니다. 이벤트 세부사항에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT\_SEEN이 포함되어 있습니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 APP\_DATA\_C2S 또는 APP\_DATA\_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT\_HELLO, SERVER\_HELLO, SERVER\_CERTIFICATE, SERVER\_KEY\_EXCHANGE, SERVER\_HELLO\_DONE입니다.
- Dropbox 등의 그룹 2 앱은 알림을 보내지 않습니다. 대신 핸드셰이크가 완료될 때까지 기다렸다가 TCP Reset(TCP 재설정)을 전송합니다. 이벤트에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT\_SEEN, APP\_DATA\_C2S 또는 APP\_DATA\_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT\_HELLO, SERVER\_HELLO, SERVER\_CERTIFICATE, SERVER\_KEY\_EXCHANGE, SERVER\_HELLO\_DONE, CLIENT\_KEY\_EXCHANGE, CLIENT\_CHANGE\_CIPHER\_SPEC, CLIENT\_FINISHED, SERVER\_CHANGE\_CIPHER\_SPEC, SERVER\_FINISHED입니다.

**CA** 인증서에 대한 다운로드 버튼이 비활성화됨

CDO에 준비되었지만 아직 디바이스에 다시 구축되지 않은 인증서(셀프 서명되고 업로드됨)에 대해서는 다운로드 버튼이 비활성화됩니다. 인증서는 디바이스에 구축한 후에만 다운로드할 수 있습니다.

## 일련 번호를 사용하여 FDM-관리 디바이스 온보딩 문제 해결

- 프로비저닝 오류
  - 디바이스 비밀번호가 변경되지 않았음
  - 디바이스 비밀번호가 이미 변경됨
- 클레임 오류
  - 유효하지 않은 일련 번호
  - 디바이스 일련 번호가 이미 요청됨
  - 디바이스가 오프라인임
  - 디바이스를 클레임하지 못했음

### 클레임 오류

유효하지 않은 일련 번호



Cisco Defense Orchestrator에서 디바이스를 클레임하는 동안 잘못된 일련 번호가 입력되었습니다.

해결 방법

1. CDO에서 FDM 관리 디바이스 인스턴스를 삭제합니다.
2. 올바른 일련 번호를 입력하여 새 FDM 관리 디바이스 인스턴스를 생성하고 디바이스를 클레임합니다.

디바이스 일련 번호가 이미 요청됨

일련 번호를 사용하여 FDM 관리 디바이스를 온보딩할 때 다음 오류가 발생합니다.



원인

이 오류는 다음 이유 중 하나로 인해 발생할 수 있습니다.

- 디바이스가 외부 벤더로부터 구매되었을 수 있으며 디바이스가 벤더의 테넌시에 있습니다.
- 디바이스가 이전에 다른 지역의 다른 CDO 인스턴스에서 관리되었을 수 있으며 해당 클라우드 테넌시에 등록되어 있습니다.

#### 해결 방법

다른 클라우드 테넌시에서 디바이스의 일련 번호를 등록 취소한 다음 테넌트에서 회수해야 합니다.

#### 사전 요구 사항

디바이스는 클라우드 테넌시에 연결할 수 있는 인터넷에 연결되어 있어야 합니다.

#### 외부 벤더에서 구매한 디바이스

외부 벤더에서 구매한 디바이스가 벤더의 클라우드 테넌시에 등록되었을 수 있습니다.

1. CDO에서 디바이스 인스턴스를 삭제합니다.
2. 디바이스에 FXOS 이미지를 설치합니다. 자세한 내용은 [FTD를 사용하는 Firepower 1000/21000용 Cisco FXOS 문제 해결 가이드](#)의 "리이미징 절차" 장을 참조하십시오.
3. 콘솔 포트에서 FXOS CLI에 연결합니다.
4. 현재 관리자 비밀번호를 사용하여 FXOS에 로그인합니다.
5. FXOS CLI에서 local-mgmt: firepower # **connect local-mgmt**에 연결합니다.
6. 명령을 실행하여 클라우드 테넌시에서 디바이스를 등록 취소합니다. firepower(local-mgmt)#**cloud deregister**.
7. 등록 취소에 성공하면 CLI 인터페이스에서 성공 메시지를 반환합니다.

예: **firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9**

디바이스가 이미 클라우드 테넌시에서 등록 취소된 경우 CLI 인터페이스에 디바이스 일련 번호가 클라우드 테넌시에 등록되지 않았음을 나타냅니다. **RESULT=success MESSAGE=DEVICE\_NOT\_FOUND: Device with serial number JAD213082x9 is not registered with 보안 서비스 익스체인지, X-Flow-Id: 63e48b4c-8426-48fb-9bd0-25fcd7777b99**

8. 일련 번호를 제공하여 CDO에서 디바이스를 다시 클레임합니다. 자세한 내용은 디바이스 [디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩](#)을 참조하십시오.
9. 디바이스에 FDM 관리 디바이스 애플리케이션(버전 6.7 이상)을 설치합니다. 로우 터치(low-touch) 프로비저닝이 디바이스에서 시작되고 Cisco Cloud에 자체적으로 등록됩니다. CDO은 디바이스를 온보딩합니다.

#### 다른 지역의 다른 클라우드 테넌시에서 이미 관리하는 FDM-관리 디바이스 온보딩

디바이스가 이전에 다른 지역의 다른 CDO 인스턴스에서 관리되었을 수 있으며 해당 클라우드 테넌시에 등록되어 있습니다.

사례 1: 디바이스를 소유하는 테넌트에 액세스할 수 있습니다.



1. 영역 1의 CDO에서 디바이스 인스턴스를 삭제합니다.
2. Firewall Device Manager에서 **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스) 페이지로 이동합니다. 디바이스가 CDO에서 제거되었음을 나타내는 경고 메시지가 나타납니다.
3. 링크를 클릭하고 드롭다운 목록에서 **Unregister Cloud Services**(클라우드 서비스 등록 취소)를 선택합니다.
4. 경고를 읽고 **Unregister**(등록 취소)를 클릭합니다.
5. 영역 2의 CDO에서 디바이스를 클레임합니다.
6. Firewall Device Manager에서 **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)로 이동하여 **Auto-enroll with Tenancy from Cisco Defense Orchestrator**(Cisco Defense Orchestrator에서 테넌시에 자동 등록) 옵션을 선택하고 **Register**(등록)를 클릭합니다. 디바이스는 새 지역에 속하는 새 테넌트에 매핑되고 CDO는 디바이스를 온보딩합니다.

사례 2: 디바이스를 소유하는 테넌트에 액세스할 수 없습니다.

1. 콘솔 포트에서 FXOS CLI에 연결합니다.
  2. 현재 관리자 비밀번호를 사용하여 FXOS에 로그인합니다.
  3. FXOS CLI에서 `local-mgmt: firepower # connect local-mgmt`에 연결합니다.
  4. 명령을 실행하여 클라우드 테넌시에서 디바이스를 등록 취소합니다. `firepower(local-mgmt)#cloud deregister`.
  5. 등록 취소에 성공하면 CLI 인터페이스에서 성공 메시지를 반환합니다.  
예: `firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9`
- 디바이스가 클라우드에서 등록 취소됩니다.
6. 영역 2의 CDO에서 디바이스를 클레임합니다.
  7. Firewall Device Manager에서 **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)로 이동하여 **Auto-enroll with Tenancy from Cisco Defense Orchestrator**(Cisco Defense Orchestrator에서 테넌시에 자동 등록) 옵션을 선택하고 **Register**(등록)를 클릭합니다. 디바이스는 새 지역에 속하는 새 테넌트에 매핑되고 CDO는 디바이스를 온보딩합니다.

디바이스가 오프라인임



원인

다음 이유 중 하나로 인해 디바이스에서 Cisco Cloud에 연결할 수 없습니다.

- 디바이스가 잘못 연결되었습니다.
- 네트워크에 디바이스의 고정 IP 주소가 필요할 수 있습니다.

- 네트워크에서 맞춤형 DNS를 사용하거나 고객 네트워크에서 외부 DNS 차단이 있습니다.
- PPPoE 인증이 필요합니다. (유럽 지역에서 일반적입니다.)
- FDM 관리 디바이스가 프록시 뒤에 있습니다.

#### 해결 방법

1. 디바이스에 로그인하고 부트스트랩 CLI 프로세스 또는 CDO Easy 설정 프로세스를 통해 디바이스가 인터넷에 연결할 수 있도록 먼저 구성합니다.
2. 케이블링 및 네트워크 연결을 확인합니다.
3. 방화벽이 트래픽을 차단하고 있지 않은지 확인합니다.
4. 보안 서비스 익스체인지 도메인에 연결할 수 있는지 확인합니다. 자세한 내용은 [로우터치 프로비저닝을 사용하여 FDM-관리 디바이스 온보딩](#)을 참조하십시오.

#### 디바이스를 클레임하지 못했음

##### 원인

이 오류는 다음 이유 중 하나로 인해 발생할 수 있습니다.

- 보안 서비스 익스체인지에 일시적인 문제가 있을 수 있습니다.
- 서버가 다운되었을 수 있습니다.

#### 해결 방법

1. CDO에서 FDM 관리 디바이스 인스턴스를 삭제합니다.
2. 새 FDM 관리 디바이스 인스턴스를 생성하고 잠시 후 디바이스를 다시 클레임합니다.



참고 디바이스를 클레임할 수 없는 경우 워크플로로 이동하여 오류 메시지를 확인하고 CDO 지원 팀에 세부 정보를 전송합니다.

## 프로비저닝 오류

#### 디바이스 비밀번호가 변경되지 않았음

Cisco Defense Orchestrator에서 디바이스를 클레임할 때 디바이스의 초기 프로비저닝이 실패하고 **Inventory**(재고 목록) 페이지에 "Unprovisioned(프로비저닝되지 않음)" 메시지가 표시될 수 있습니다.

##### 원인

기본 비밀번호가 변경되지 않은 새 FDM 관리 디바이스에 대해 CDO FDM 관리 디바이스 시리얼 온보딩 마법사에서 "Default Password Changed(기본 비밀번호 변경)" 옵션을 선택했을 수 있습니다.

#### 해결 방법

디바이스의 비밀번호를 변경하려면 **Inventory**(재고 목록) 페이지에서 **Enter Password**(비밀번호 입력)를 클릭해야 합니다. CDO가 새 비밀번호를 사용하여 계속 진행하고 디바이스를 온보딩합니다.

디바이스 비밀번호가 이미 변경됨

CDO에서 디바이스를 클레임할 때 디바이스의 초기 프로비저닝이 실패하고 **Inventory**(재고 목록) 페이지에 "Unprovisioned(프로비저닝되지 않음)" 메시지가 표시될 수 있습니다.

원인

기본 비밀번호가 이미 변경된 FDM 관리 디바이스에 대해 CDO FDM 관리 디바이스 시리얼 온보딩 마법사에서 "Default Password Not Changed(기본 비밀번호가 변경되지 않음)" 옵션을 선택했을 수 있습니다.

해결 방법

시리얼 온보딩 마법사에서 제공된 새 비밀번호를 무시하려면 **Inventory**(재고 목록) 페이지에서 **Confirm and Proceed**(확인 및 진행)를 클릭해야 합니다. CDO가 새 비밀번호를 사용하여 계속 진행하고 디바이스를 온보딩합니다.

기타 오류

다른 모든 프로비저닝 오류의 경우 **Retry**(재시도)를 클릭하여 프로비저닝을 다시 시작할 수 있습니다. 여러 번 재시도한 후에도 실패하면 다음 단계를 수행합니다.

1. CDO에서 FDM 관리 디바이스 인스턴스를 삭제하고 새 인스턴스를 생성합니다. 온보딩 단계는 [디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩](#)을 참조하십시오.
2. Firewall Device Manager에서 **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)로 이동하여 **Auto-enroll with Tenancy from Cisco Defense Orchestrator**(Cisco Defense Orchestrator에서 테넌시에 자동 등록) 옵션을 선택하고 **Register**(등록)를 클릭합니다.

## FDM-관리 HA 생성 문제 해결

이벤트 설명 오류

Cisco Defense Orchestrator에서 FDM 관리 HA 쌍을 온보딩하거나 생성하려고 하면 HA 쌍이 형성되지 않고 다음 메시지와 함께 오류가 표시될 수 있습니다.

**Event description**(이벤트 설명): CD App Sync 오류는 Cisco Threat Response가 Active에서는 활성화되지만 Standb에서는 활성화되지 않는다는 것입니다.

이 오류가 표시되면 HA 쌍 내의 디바이스 중 하나 또는 둘 모두의 디바이스가 CDO, Firepower Threat Response 또는 Cisco Success Network와 같은 Cisco cloud 서버에 이벤트를 보낼 수 있도록 구성되지 않은 것입니다.

Firewall Device Manager UI에서 **Send Events to the Cisco Cloud**(Cisco Cloud로 이벤트 보내기) 기능을 활성화해야 합니다. 자세한 내용은 실행 중인 버전의 [Firepower Device Manager 구성 가이드](#)에서 클라우드 서비스 구성 장을 참조하십시오.

HA를 생성한 후 디바이스 중 하나가 잘못된 상태입니다.

HA를 만드는 동안 디바이스 중 하나가 비정상 상태이거나 오류 상태가 되면 HA 쌍을 끊고 디바이스 상태를 확인한 다음 HA를 다시 생성합니다. [FDM-관리고가용성 장애 조치 기록](#)이 문제를 진단하는데 도움이 될 수 있습니다.

## 보안 디바이스 커넥터 문제 해결

다음 주제를 사용하여 온프레미스 SDC(Secure Device Connector) 문제를 해결합니다.

이러한 시나리오와 일치하지 않는 경우 [CDO 고객이 TAC로 지원 티켓을 여는 방법](#).

### SDC에 연결할 수 없음

CDO에서 연속으로 두 개의 하트비트 요청에 응답하지 못한 경우 SDC는 "도달할 수 없음" 상태입니다. SDC에 연결할 수 없는 경우 테넌트는 온보딩된 디바이스와 통신할 수 없습니다.

CDO는 다음과 같은 방식으로 SDC에 연결할 수 없음을 나타냅니다.

- "일부 보안 디바이스 커넥터(SDC)에 연결할 수 없습니다."라는 메시지가 표시됩니다. CDO 홈페이지에서 이러한 SDC와 연결된 디바이스와 통신할 수 없습니다.
- Secure Connectors(보안 커넥터) 페이지에서 SDC의 상태는 "연결할 수 없음"입니다.

먼저 이 문제를 해결하려면 SDC를 테넌트에 다시 연결해 봅니다.

1. SDC 가상 머신이 실행 중이고 해당 지역의 CDO IP 주소에 도달할 수 있는지 확인합니다. [매니지드 디바이스에 Cisco Defense Orchestrator 연결, 12 페이지](#)를 참조하십시오.
2. 하트비트를 수동으로 요청하여 CDO와 SDC를 다시 연결해 봅니다. SDC가 하트비트 요청에 응답하면 "활성" 상태로 돌아갑니다. 하트비트를 수동으로 요청하려면 다음과 같이 작업합니다.
  1. CDO 메뉴에서 **Admin(관리) > Secure Connector(보안 커넥터)**를 선택합니다.
  2. 연결할 수 없는 SDC를 클릭합니다.
  3. 작업 창에서 **Request Heartbeat(하트비트 요청)**를 클릭합니다.
  4. **Reconnect(다시 연결)**를 클릭합니다.
3. 테넌트에 수동으로 다시 연결하려고 시도한 후에도 SDC가 활성 상태로 돌아가지 않으면, [배포 후 SDC 상태가 CDO에서 활성화되지 않음, 774 페이지](#)의 지침을 따르십시오.

### 배포 후 SDC 상태가 CDO에서 활성화되지 않음

CDO가 배포 후 약 10분 동안 SDC가 활성 상태임을 나타내지 않으면 SDC를 배포할 때 생성한 cdo 사용자 및 암호를 사용하여 SSH를 사용하여 SDC VM에 연결합니다.

## Procedure

- 단계 1** /opt/cdo/configure.log를 검토합니다. SDC에 대해 입력한 구성 설정과 성공적으로 적용되었는지 여부를 보여줍니다. 설정 프로세스에 오류가 있거나 값이 올바르게 입력되지 않은 경우 sdc-onboard 설정을 다시 실행합니다.
- [cdo@localhost cdo]\$ 프롬프트에서 `sudo sdc-onboard setup`을 입력합니다.
  - cdouser의 암호를 입력합니다.
  - 프롬프트에 따라 수행합니다. 설정 스크립트는 설정 마법사에서 수행한 모든 구성 단계를 안내하고 입력한 값을 변경할 수 있는 기회를 제공합니다.
- 단계 2** 로그를 검토하고 `sudo sdc-onboard setup`을 실행한 후에도 CDO가 여전히 SDC가 **Active(활성)** 상태를 나타내지 않으면, [Cisco Defense Orchestrator 지원팀에 문의](#).

## SDC의 변경된 IP 주소가 CDO에 반영되지 않음

SDC의 IP 주소를 변경한 경우 GMT 오전 3시 이후까지는 CDO에 반영되지 않습니다.

## SDC와의 디바이스 연결 문제 해결

이 도구를 사용하여 CDO에서 SDC(보안 디바이스 커넥터)를 통해 디바이스로의 연결을 테스트합니다. 디바이스가 온보딩에 실패하거나 온보딩 전에 CDO가 디바이스에 연결할 수 있는지 확인하려는 경우 이 연결을 테스트할 수 있습니다.

### Procedure

- 단계 1** CDO 메뉴에서 **Admin(관리) > Secure Connector(보안 커넥터)**를 선택합니다.
- 단계 2** SDC를 선택합니다.
- 단계 3** 오른쪽의 **Troubleshooting(문제 해결)** 창에서 **Device Connectivity(디바이스 연결)**를 클릭합니다.
- 단계 4** 문제 해결을 시도하거나 연결을 시도하는 디바이스의 유효한 IP 주소 또는 FQDN 및 포트 번호를 입력하고 **Go(이동)**를 클릭합니다. CDO는 다음 확인을 수행합니다.
- DNS 확인** - IP 주소 대신 FQDN을 제공하는 경우 SDC가 도메인 이름을 확인하고 IP 주소를 가져올 수 있는지 확인합니다.
  - 연결 테스트** - 디바이스에 연결할 수 있는지 확인합니다.
  - TLS 지원** - 디바이스와 SDC가 모두 지원하는 TLS 버전 및 암호를 탐지합니다.
    - 지원되지 않는 암호 - 디바이스와 SDC에서 모두 지원하는 TLS 버전이 없는 경우 CDO는 디바이스에서 지원하는 TLS 버전 및 암호도 테스트하지만 SDC는 테스트하지 않습니다.
  - SSL 인증서** - 문제 해결에서 인증서 정보를 제공합니다.

단계 5 디바이스에 대한 온보딩 또는 연결 문제가 계속 발생하는 경우 [Cisco Defense Orchestrator 지원팀에 문의](#)하십시오.

## 간헐적으로 또는 SDC에 연결되지 않음

이 섹션에서 설명하는 솔루션은 온프레미스 SDC(보안 디바이스 커넥터)에만 적용됩니다.

증상: 간헐적으로 또는 SDC에 연결되지 않음

진단: 이 문제는 디스크 공간이 거의 찼을 때(80% 이상) 발생할 수 있습니다.

디스크 공간 사용량을 확인하려면 다음 단계를 수행합니다.

1. SDC(보안 디바이스 커넥터) VM용 콘솔을 엽니다.
2. 사용자 이름 **cdo**로 로그인합니다.
3. 최초 로그인 시 생성한 비밀번호를 입력합니다.
4. 먼저 **df -h**를 입력하여 사용 가능한 디스크 공간이 없는지 확인하여 디스크 여유 공간을 확인합니다.

Docker에서 디스크 공간을 소비한 것을 확인할 수 있습니다. 정상적인 디스크 사용량은 2GB 미만일 것으로 예상됩니다.

5. Docker 폴더의 디스크 사용량을 보려면,

**sudo du -h /var/lib/docker | sort -h**를 실행합니다.

Docker 폴더의 디스크 공간 사용량을 볼 수 있습니다.

절차

Docker 폴더의 디스크 공간 사용량이 거의 가득 찬 경우 docker 구성 파일에서 다음을 정의합니다.

- 최대 크기: 현재 파일이 최대 크기에 도달하면 로그 회전을 강제합니다.
- 최대 파일: 최대 한도에 도달했을 때 초과 회전된 로그 파일을 삭제합니다.

다음을 수행하십시오.

1. **sudo vi /etc/docker/daemon.json**를 실행합니다.
2. 파일에 다음 줄을 삽입합니다.

```
{
  "log-driver": "json-file",
  "log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. ESC 키를 누른 다음 **:wq!**를 입력합니다. 변경 사항을 쓰고 파일을 닫습니다.



참고 `sudo cat /etc/docker/daemon.json`을 실행하여 파일의 변경 사항을 확인할 수 있습니다.

4. `sudo systemctl restart docker`를 실행하여 docker 파일을 다시 시작합니다.  
변경 사항이 적용되려면 몇 분 정도 걸립니다. `sudo du -h /var/lib/docker | sort -h`를 실행하여 docker 폴더의 업데이트된 디스크 사용량을 봅니다.
5. `df -h`를 실행하여 사용 가능한 디스크 크기가 증가했는지 확인합니다.
6. SDC 상태를 Unreachable(연결 불가)에서 Active(활성)로 변경하려면 먼저 CDO에서 Secure Connector(보안 커넥터) 페이지로 이동하여 Actions(작업) 메뉴에서 **Request Reconnect**(재연결 요청)를 클릭해야 합니다.

## 보안 디바이스 커넥터에 영향을 미치는 컨테이너 권한 상승 취약점: **cisco-sa-20190215-runc**

Cisco PSIRT(제품 보안 사고 대응 팀)는 Docker의 심각도가 높은 취약성에 대해 설명하는 보안 자문 **cisco-sa-20190215-runc**를 게시했습니다. 취약성에 대한 전체 설명은 [전체 PSIRT 팀 자문을 참조하십시오](#).

이 취약성은 모든 CDO 고객에게 영향을 미칩니다.

- CDO의 클라우드 배포 SDC(보안 디바이스 커넥터)를 사용하는 고객은 CDO 운영 팀에서 교정 단계를 이미 수행했으므로 아무 작업도 수행할 필요가 없습니다.
- 온프레미스에 배포된 SDC를 사용하는 고객은 최신 Docker 버전을 사용하도록 SDC 호스트를 업그레이드해야 합니다. 다음 지침에 따라 이 작업을 수행할 수 있습니다.
  - [CDO-표준 SDC 호스트 업데이트, 777 페이지](#)
  - [사용자 지정 SDC 호스트 업데이트, 778 페이지](#)
  - [버그 추적, 778 페이지](#)

### CDO-표준 SDC 호스트 업데이트

CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축한 경우 이 지침을 사용합니다.

프로시저

단계 1 SSH 또는 하이퍼바이저 콘솔을 사용하여 SDC 호스트에 연결합니다.

단계 2 다음 명령을 실행하여 Docker 서비스 버전을 확인합니다.

```
docker version
```

단계 3 최신 VM(가상 머신) 중 하나를 실행 중인 경우 다음과 같은 출력이 표시됩니다.

```
> docker version
Client:
  Version: 18.06.1-ce
  API version: 1.38
  Go version: go1.10.3
  Git commit: e68fc7a
  Built: Tue Aug 21 17:23:03 2018
  OS/Arch: linux/amd64
  Experimental: false
```

여기에서 이전 버전을 볼 수 있습니다.

**단계 4** 다음 명령을 실행하여 Docker를 업데이트하고 서비스를 다시 시작하십시오.

```
> sudo yum update docker-ce
> sudo service docker restart
```

참고 Docker 서비스가 다시 시작되는 동안 CDO와 디바이스 간에 짧은 연결 중단이 발생합니다.

**단계 5** `docker version` 명령을 다시 실행하십시오. 다음 출력이 표시되어야 합니다.

```
> docker version
Client:
  Version: 18.09.2
  API version: 1.39
  Go version: go1.10.6
  Git commit: 6247962
  Built: Sun Feb XX 04:13:27 2019
  OS/Arch: linux/amd64
  Experimental: false
```

**단계 6** 마쳤습니다. 이제 패치가 적용된 최신 버전의 Docker로 업그레이드되었습니다.

## 사용자 지정 SDC 호스트 업데이트

자체 SDC 호스트를 생성한 경우 Docker 설치 방법에 따라 업데이트 지침을 따라야 합니다. CentOS, yum 및 Docker-ce(커뮤니티 에디션)를 사용한 경우 이전 절차가 작동합니다.

Docker-ee(엔터프라이즈 버전)를 설치했거나 다른 방법을 사용하여 Docker를 설치한 경우 Docker의 고정 버전이 다를 수 있습니다. Docker 페이지를 확인하여 설치할 올바른 버전([Docker 보안 업데이트 및 컨테이너 보안 모범 사례](#))을 결정할 수 있습니다.

## 버그 추적

Cisco는 이 취약성을 계속 평가하고 있으며 추가 정보가 제공되는 대로 권고를 업데이트할 것입니다. 권고가 최종으로 표시되면 관련 Cisco 버그에서 자세한 내용을 참조할 수 있습니다.

[CSCvo33929-CVE-2019-5736: runc container breakout](#)

## 보안 이벤트 커넥터 문제 해결

이러한 시나리오와 일치하지 않는 경우 [CDO 고객](#)이 TAC로 지원 티켓을 여는 방법.



## SEC 온보딩 실패 문제 해결

이러한 문제 해결 항목에서는 SEC(보안 이벤트 커넥터) 온보딩 실패와 관련된 여러 가지 증상에 대해 설명합니다.

### SEC 온보딩 실패

증상: SEC 온보딩에 실패했습니다.

복구: SEC를 제거하고 다시 온보딩합니다.

이 오류가 표시되는 경우:

1. 가상 머신 컨테이너에서 [보안 이벤트 커넥터 제거](#) 및 해당 파일을 제거합니다.
2. [보안 디바이스 커넥터 업데이트, 29 페이지](#). 일반적으로 SDC는 자동으로 업데이트되므로 이 절차를 사용할 필요가 없지만 이 절차는 문제 해결 시 유용합니다.
3. [SDC 가상 머신에 SEC\(Secure Event Connector\) 설치, 671 페이지](#).



팁 SEC를 온보딩할 때는 항상 복사 링크를 사용하여 부트스트랩 데이터를 복사합니다.



참고 이 절차로 문제가 해결되지 않으면 [문제 해결 로그 파일 이벤트 로깅](#)하고 관리 서비스 제공자 또는 [Cisco 기술 지원 센터](#)에 문의하십시오.

### SEC 부트스트랩 데이터가 제공되지 않음

메시지: 오류가 발생하여 보안 이벤트 커넥터를 부트스트랩할 수 없습니다. 부트스트랩 데이터가 제공되지 않아 종료하는 중입니다.

```
[sdc@localhost ~]# /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not provided, exiting.
```

진단: 프롬프트가 표시될 때 부트스트랩 데이터가 설정 스크립트에 입력되지 않았습니다.

복구: 온보딩 시 부트스트랩 데이터 입력에 대한 프롬프트가 표시되면 CDO UI에서 생성된 SEC 부트스트랩 데이터를 제공합니다.

부트스트랩 구성 파일이 없습니다.

메시지: 오류가 발생하여 테넌트 <tenant\_name>에 대한 보안 이벤트 커넥터를 부트스트랩할 수 없습니다. 부트스트랩 구성 파일("/usr/local/cdo/es\_bootstrapdata")이 없어 종료하는 중입니다.

진단: SEC 부트스트랩 데이터 파일("/usr/local/cdo/es\_bootstrapdata")이 없습니다.

복구: CDO UI에서 생성된 SEC 부트스트랩 데이터를 **/usr/local/cdo/es\_bootstrapdata** 파일에 배치하고 다시 온보딩을 시도합니다.

1. 온보딩 절차를 반복합니다.
2. 부트스트랩 날짜를 복사합니다.
3. 'sdc' 사용자로 SEC VM에 로그인합니다.
4. CDO UI에서 생성된 SEC 부트스트랩 데이터를 `/usr/local/cdo/es_bootstrapdata` 파일에 배치하고 다시 온보딩을 시도합니다.

#### 부트스트랩 데이터 디코딩 실패

메시지: 오류가 발생하여 테넌트 <tenant\_name>에 대한 보안 이벤트 커넥터를 부트스트랩할 수 없습니다. SEC 부트스트랩 데이터를 디코딩하지 못하여 종료하는 중입니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
failed to decode SEC bootstrap data, exiting.
```

#### 진단: 부트스트랩 데이터 디코딩 실패

복구: SEC 부트스트랩 데이터를 재생성하고 온보딩을 다시 시도합니다.

부트스트랩 데이터에 **SEC**를 온보딩하는 데 필요한 정보가 없습니다.

메시지:

- **ERROR**는 테넌트에 대한 보안 이벤트 커넥터 컨테이너를 부트스트랩할 수 없습니다. 보안 서비스 익스체인지 FQDN이 설정되지 않았습니다. 종료됩니다.
- **ERROR**는 테넌트에 대한 보안 이벤트 커넥터 컨테이너를 부트스트랩할 수 없습니다. 보안 서비스 익스체인지 OTP가 설정되지 않았습니다. 종료됩니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 보안 서비스
익스체인지 FQDN not set, exiting.
```

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 보안 서비스
익스체인지 FQDN not set, exiting.
```

진단: 부트스트랩 데이터에 **SEC**를 온보딩하는 데 필요한 정보가 없습니다.

복구: 부트스트랩 데이터를 재생성하고 다시 온보딩을 시도합니다.

#### 툴킷 **cron** 현재 실행 중

메시지: 오류 SEC 툴킷이 이미 실행 중이어서 종료하는 중입니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

진단: 툴킷 **cron**이 현재 실행 중입니다.

복구: 온보딩 명령을 다시 시도합니다.

적절한 CPU 및 메모리를 사용할 수 없음

메시지: 오류가 발생하여 보안 이벤트 커넥터를 설정할 수 없습니다. 최소 4개의 CPU와 8GB의 RAM이 필요하여 종료하는 중입니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8 GB ram required, exiting.
```

진단: 적절한 CPU 및 메모리를 사용할 수 없습니다.

복구: 최소 4개의 CPU 및 8GB RAM이 VM에서 SEC 전용으로 프로비저닝되었는지 확인하고 다시 온보딩을 시도합니다.

**SEC가 이미 실행 중**

메시지: 오류. 보안 이벤트 커넥터가 이미 실행 중입니다. 새 보안 이벤트 커넥터를 온보딩하기 전에 'cleanup'을 실행하십시오. 종료하는 중입니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup' before onboarding a new Secure Event Connector, exiting.
```

진단: SEC가 이미 실행 중입니다.

복구: 새 SEC를 온보딩하기 전에 **SEC Cleanup 명령**을 실행합니다.

**SEC 도메인 연결 불가**

메시지:

- api-sse.cisco.com:443에 연결 실패; 연결 거부됨
- 오류가 발생하여 보안 이벤트 커넥터를 설정할 수 없습니다. 도메인 api-sse.cisco.com에 연결할 수 없어 종료하는 중입니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com unreachable, exiting.
```

진단: SEC 도메인에 연결할 수 없음

복구: 온프레미스 SDC가 인터넷에 연결되어 있는지 확인하고 다시 온보딩을 시도합니다.

온보딩 **SEC** 명령이 오류 없이 성공했지만 **SEC** 도커 컨테이너가 작동하지 않음

증상: 온보딩 SEC 명령이 오류 없이 성공했지만 SEC 도커 컨테이너가 작동하지 않습니다.

진단: 온보딩 SEC 명령이 오류 없이 성공했지만 SEC 도커 컨테이너가 작동하지 않습니다.

복구:

1. 'sdc' 사용자로 SEC에 로그인합니다.
2. SEC 도커 컨테이너 시작 로그(/usr/local/cdo/data/<tenantDir> /event\_streamer/logs/startup.log)에 오류가 있는지 확인합니다.

3. 있는 경우 **SEC Cleanup 명령**을 실행하고 온보딩을 다시 시도합니다.

#### CDO 지원 문의

이러한 시나리오와 일치하지 않는 경우 **CDO 고객**이 **TAC로 지원 티켓을 여는 방법**.

## 보안 이벤트 커넥터 등록 실패 문제 해결

증상: 클라우드 이벤트 서비스에 대한 Cisco Secure Event Connector 등록이 실패합니다.

진단: SEC가 이벤트 클라우드 서비스에 등록하지 못하는 가장 일반적인 이유입니다.

- SEC가 SEC에서 **Eventing** 클라우드 서비스에 연결할 수 없습니다.

복구: 포트 443에서 인터넷에 액세스할 수 있고 DNS가 올바르게 구성되어 있는지 확인합니다.

- SEC 부트스트랩 데이터의 유효하지 않거나 만료된 일회용 비밀번호로 인한 등록 실패

복구:

#### Procedure

단계 1 'sdc' 사용자로 SDC에 로그인합니다.

단계 2 커넥터 로그 보기: (`/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log`)에서 등록 상태를 확인합니다.

유효하지 않은 토큰으로 인해 등록에 실패한 경우 로그 파일에 아래와 유사한 오류 메시지가 표시됩니다.

컨텍스트: `(*contextImpl).handleFailed`] 등록 - **CE2001**: 등록 실패 - 잘못된 토큰으로 인해 디바이스를 등록하지 못했습니다. 유효한 새 토큰을 사용하여 다시 시도하십시오. - 실패"

단계 3 SDC VM에서 **SEC Cleanup 명령** 단계를 실행하여 보안 커넥터 페이지에서 SEC를 제거합니다.

단계 4 새 SEC 부트스트랩 데이터를 생성하고 SEC 온보딩 단계를 다시 시도합니다.

## 보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결

다음은 이벤트 뷰어를 사용하여 네트워크 문제를 트러블슈팅하는 데 사용할 수 있는 기본 프레임워크입니다.

이 시나리오에서는 네트워크 운영 팀에서 사용자가 네트워크의 리소스에 액세스할 수 없다는 보고를 받은 것으로 가정합니다. 문제를 보고하는 사용자와 해당 위치를 기반으로, 네트워크 운영 팀은 어떤 방화벽이 리소스에 대한 액세스를 제어하는지를 합리적으로 파악합니다.



**Note** 또한 이 시나리오에서는 FDM 관리 디바이스가 네트워크 트래픽을 관리하는 방화벽이라고 가정합니다. Security Analytics and Logging(보안 분석 및 로깅)은 다른 디바이스 유형에서 로깅 정보를 수집하지 않습니다.

### Procedure

단계 1 탐색창에서 분석 > 이벤트 로깅을 선택합니다.

단계 2 기록 탭을 클릭합니다.

단계 3 시간 범위를 기준으로 이벤트 필터링을 시작합니다. 기본적으로 Historical(기록) 탭에는 이벤트의 마지막 시간이 표시됩니다. 올바른 시간 범위인 경우 현재 날짜와 시간을 **End**(종료) 시간으로 입력합니다. 올바른 시간 범위가 아닌 경우 보고된 문제의 시간을 포함하는 시작 및 종료 시간을 입력합니다.

단계 4 **Sensor ID**(센서 ID) 필드에 사용자의 액세스를 제어하는 것으로 의심되는 방화벽의 IP 주소를 입력합니다. 방화벽이 두 개 이상인 경우 검색 창에서 속성:값 쌍을 사용하여 이벤트를 필터링합니다. 두 항목을 만들고 OR 문으로 결합합니다. 예: SensorID:192.168.10.2 OR SensorID:192.168.20.2.

단계 5 Events(이벤트) 필터 표시줄의 **Source IP**(소스 IP) 필드에 사용자의 IP 주소를 입력합니다.

단계 6 사용자가 리소스에 액세스할 수 없는 경우 **Destination IP**(대상 IP) 필드에 해당 리소스의 IP 주소를 입력해 보십시오.

단계 7 결과에서 이벤트를 확장하고 세부 정보를 확인합니다. 다음은 몇 가지 세부 사항입니다.

- **AC\_RuleAction** - 규칙이 트리거될 때 수행된 작업(허용, 신뢰, 차단).
- **FirewallPolicy** - 이벤트를 트리거한 규칙이 상주하는 정책입니다.
- **FirewallRule** - 이벤트를 트리거한 규칙의 이름입니다. 값이 Default Action(기본 작업)인 경우 정책의 규칙 중 하나가 아니라 이벤트를 트리거한 것은 정책의 기본 작업입니다.
- **UserName** - 이니시에이터 IP 주소와 연결된 사용자입니다. 이니시에이터 IP 주소는 소스 IP 주소와 동일합니다.

단계 8 규칙 작업이 액세스를 차단하는 경우 FirewallRule 및 FirewallPolicy 필드를 확인하여 액세스를 차단하는 정책의 규칙을 식별합니다.

## NSEL 데이터 플로우 문제 해결

및 을 했으면 다음 절차를 사용하여 NSEL 이벤트가 사용자 ASA에서 Cisco Cloud로 전송되고 Cisco Cloud가 이를 수신하는지 확인합니다.

ASA가 NSEL 이벤트를 SEC(보안 이벤트 커넥터)로 보낸 다음 Cisco Cloud로 보내도록 구성된 후에는 데이터가 즉시 흐르지 않습니다. NET에서 생성되는 NSEL 관련 트래픽이 있다고 가정하면 첫 번째 NSEL 패킷이 ASA에 도착하는 데 몇 분 정도 걸릴 수 있습니다.



**Note** 이 워크플로우는 "flow-export counters" 명령 및 "capture" 명령을 사용하여 NSEL 데이터 플로우 문제를 해결하는 방법을 보여줍니다. 이러한 명령 사용에 대한 자세한 내용은 [CLI Book 1: Cisco ASA 시리즈 일반 운영 CLI 구성 가이드](#)의 "패킷 캡처" 및 [Cisco ASA NetFlow 구현 가이드](#)의 "NSEL 모니터링"을 참조하십시오.

다음 세 가지 작업을 수행합니다.

- NetFlow 패킷이 SEC로 전송되고 있는지 확인
- Cisco Cloud에서 NetFlow 패킷을 수신하고 있는지 확인

## 문제 해결 로그 파일 이벤트 로깅

SEC(Secure Event Connector) Troubleshooting.sh는 모든 이벤트 스트리머 로그를 수집하여 single.tar.gz 파일로 압축합니다.

다음 절차를 사용하여 Compared.tar.gz 파일을 생성하고 파일의 압축을 풉니다.

1. [문제 해결 스크립트 실행, 784 페이지](#).
2. [sec\\_troubleshoot.tar.gz 파일 압축 해제, 785 페이지](#).

## 문제 해결 스크립트 실행

SEC(보안 이벤트 커넥터) Troubleshooting.sh는 모든 이벤트 스트리머 로그를 수집하여 single.tar.gz 파일로 압축합니다. Troubleshooting.sh 스크립트를 실행하려면 다음 절차를 따르십시오.

### Procedure

단계 1 VM 하이퍼바이저를 열고 SDC(Secure Device Connector)에 대한 콘솔 세션을 시작합니다.

단계 2 로그인한 다음 **root** 사용자로 전환합니다.

```
[cdo@localhost ~]$sudo su root
```

**Note** sdc 사용자로 전환할 수도 있지만 루트 역할을 하면 IP 테이블 정보도 수신 됩니다. IP 테이블 정보는 방화벽이 디바이스 및 모든 방화벽 경로에서 실행 중임을 보여줍니다. 방화벽이 보안 이벤트 커넥터 TCP 또는 UDP 포트를 차단하는 경우 이벤트는 이벤트 로깅 테이블에 표시되지 않습니다. IP 테이블은 이러한 경우를 확인하는 데 도움이 됩니다.

단계 3 프롬프트에서 문제 해결 스크립트를 실행하고 테넌트 이름을 지정합니다. 다음은 명령 구문입니다.

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

예를 들면 다음과 같습니다.

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

명령 출력에서 sec\_troubleshoot 파일이 SDC의 /tmp/troubleshoot 디렉터리에 저장되어 있음을 확인할 수 있습니다. 파일 이름은 sec\_troubleshoot-*timestamp*.tar.gz 규칙을 따르십시오.

단계 4 파일을 검색하려면 CDO 사용자로 로그인하고 SCP 또는 SFTP를 사용하여 파일을 다운로드합니다.

예를 들면 다음과 같습니다.

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

### What to do next

[sec\\_troubleshoot.tar.gz 파일 압축 해제, on page 785](#)를 진행합니다.

## sec\_troubleshoot.tar.gz 파일 압축 해제

SEC(Secure Event Connector) [문제 해결 스크립트 실행](#) 스크립트는 모든 이벤트 스트리머 로그를 수집하여 단일 sec\_troubleshoot.tar.gz 파일로 압축합니다. 다음 절차에 따라 sec\_troubleshoot.tar.gz 파일의 압축을 풉니다.

1. VM 하이퍼바이저를 열고 SDC(Secure Device Connector)에 대한 콘솔 세션을 시작합니다.
2. 로그인한 다음 **root** 사용자로 전환합니다.

```
[cdo@localhost ~]$sudo su root
```



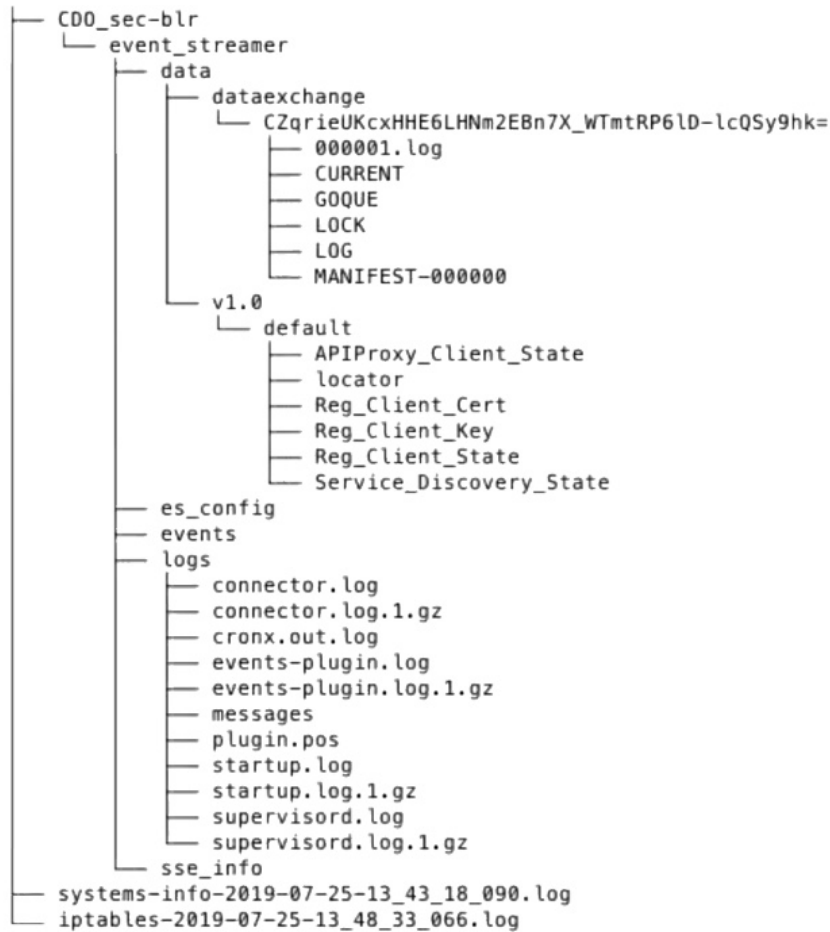
**Note** sdc 사용자로 전환할 수도 있지만 루트 역할을 하면 IP 테이블 정보도 수신 됩니다. IP 테이블 정보는 방화벽이 디바이스 및 모든 방화벽 경로에서 실행 중임을 보여줍니다. 방화벽이 보안 이벤트 커넥터 TCP 또는 UDP 포트를 차단하는 경우 이벤트는 이벤트 로깅 테이블에 표시되지 않습니다. IP 테이블은 이러한 경우를 확인하는 데 도움이 됩니다.

3. 프롬프트에서 다음 명령을 입력합니다.

```
[root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
```

로그 파일은 테넌트의 이름을 따서 명명된 디렉터리에 저장됩니다. 이러한 로그는 sec\_troubleshoot-timestamp.tar.gz 파일에 저장됩니다. 루트 사용자로 모든 로그 파일을 수집한 경우 iptables 파일이 포함됩니다.

SEC 부트스트랩 데이터를 생성하지 못했습니다.



## SEC 부트스트랩 데이터를 생성하지 못했습니다.

증상: CDO에서 SEC 부트스트랩 데이터를 생성하는 동안, "부트스트랩 생성" 단계가 "부트스트랩 데이터를 가져오는 중에 오류가 발생했습니다." 오류와 함께 실패합니다. 다시 시도하십시오.

수리: 부트스트랩 데이터 생성을 다시 시도하십시오. 여전히 실패하면 [CDO 고객이 TAC로 지원 티켓을 여는 방법](#) 하십시오.

## 온보딩 후 CDO 보안 커넥터 페이지에서 SEC 상태가 "비활성"임

**Symptom(증상):** 보안 이벤트 커넥터 상태가 다음 이유 중 하나로 CDO 보안 커넥터 페이지에서 "비활성"으로 표시됩니다.

- 하트비트 실패
- 커넥터 등록 실패

복구:



- **Heartbeat failed**(하트비트 실패): SEC 하트비트를 요청하고 보안 커넥터 페이지를 새로 고쳐 상태가 "활성"으로 변경되는지 확인하고 그렇지 않으면 보안 디바이스 커넥터 등록이 실패했는지 확인합니다.
- **Connector registration failed**(커넥터 등록 실패): [보안 이벤트 커넥터 등록 실패 문제 해결](#)을 참조하십시오.

## SEC가 "온라인"이지만 CDO 이벤트 로깅 페이지에 이벤트가 없습니다

**Symptom**(증상): CDO 보안 커넥터 페이지에 보안 이벤트 커넥터가 "활성"으로 표시되지만 CDO 이벤트 뷰어에는 이벤트가 표시되지 않습니다.

**Solution or workaround**(해결 방법):

### Procedure

**단계 1** 온프레미스 SDC의 VM에 'sdc' 사용자로 로그인합니다. 프롬프트에서 **sudo su - sdc**를 입력합니다.

**단계 2** 다음 확인을 수행합니다.

- SEC 커넥터 로그( /usr/local/cdo/data/<tenantDir>/event\_streamer/logs/connector.log )를 확인하고 SEC 등록이 성공했는지 확인합니다. 그렇지 않은 경우 ["보안 이벤트 커넥터 등록 실패 문제 해결"](#) 문제를 참조하십시오.
- SEC 이벤트 로그( /usr/local/cdo/data/<tenantDir>/event\_streamer/logs/events-plugin.log )를 확인하고 이벤트가 처리되고 있는지 확인합니다. 그렇지 않은 경우 [CDO 고객이 TAC로 지원 티켓을 여는 방법](#).
- SEC 도커 컨테이너에 로그인하고 "supervisorctl -c /opt/cssp/data/conf/supervisord.conf" 명령을 실행하고 출력이 아래와 같고 모든 프로세스가 RUNNING 상태인지 확인합니다. 그렇지 않은 경우 [CDO 고객이 TAC로 지원 티켓을 여는 방법](#).

**estreamer-connector RUNNING pid 36, 업타임 5:25:17**

**estreamer-cron RUNNING pid 39, 업타임 5:25:17**

**estreamer-plugin RUNNING pid 37, 업타임 5:25:17**

**estreamer-rsyslog RUNNING pid 38, 업타임 5:25:17**

- 온프레미스 SDC의 방화벽 규칙이 보안 커넥터 페이지에서 SEC에 대해 표시된 UDP 및 TCP 포트를 차단하지 않는지 확인합니다. 어떤 포트를 열어야 하는지 확인하려면 [SaaS\(Secure Logging Analytics\)에 사용되는 디바이스의 TCP, UDP 및 NSEL 포트 찾기](#)를 참조하십시오.

ID	Type	Deployment	Status	Last Heartbeat
CDO_solution_es1-SDC	Secure Device Connector	On-Prem	Active	5/31/2019, 3:00:21 PM
6c24d6bb-e307-4a05-9dd7-4f6f6c084d6b	Secure Event Connector	On-Prem	Active	5/31/2019, 3:00:23 PM

**6c24d6bb-e307-4a05-9dd7-4f6f6c084d6b**

Details

Version	83a49e199bdd85b7cdfb8dd05972e50c5929abf4
IP Address	192.168.0.191
TCP Port	10125
UDP Port	10025

- 자체 CentOS 7 VM을 사용하여 SDC를 수동으로 설정하고 들어오는 요청을 차단하도록 방화벽을 구성한 경우, 다음 명령을 실행하여 UDP 및 TCP 포트의 차단을 해제할 수 있습니다.

```
firewall-cmd --zone=public --add-port=<udp_port>/udp --permanent
```

```
firewall-cmd --zone=public --add-port=<tcp_port>/tcp --permanent
```

```
firewall-cmd --reload
```

- 선택한 Linux 네트워크 도구를 사용하여 이 포트에서 패킷이 수신되고 있는지 확인합니다. 수신되지 않는 경우 FTD 로그 구성을 다시 확인합니다.

위의 수리 중 어느 것도 작동하지 않으면, [CDO 고객이 TAC로 지원 티켓을 여는 방법](#).

## SEC Cleanup 명령

SEC(보안 이벤트 커넥터) cleanup 명령은 SDC(보안 디바이스 커넥터) VM에서 SEC 컨테이너 및 관련 파일을 제거합니다. [보안 이벤트 커넥터 등록 실패 문제 해결, on page 782](#) 또는 온보딩에 실패할 경우 이 명령을 실행할 수 있습니다.

명령을 실행하려면 다음을 수행합니다.

### Before you begin

이 작업을 수행하려면 테넌트의 이름을 알아야 합니다. 테넌트 이름을 찾으려면 CDO에서 사용자 메뉴를 열고 **Settings**(설정)를 클릭합니다. 페이지를 아래로 스크롤하여 테넌트 이름을 찾습니다.

### Procedure

단계 1 'sdc' 사용자로 SDC에 로그인합니다. 프롬프트에서 `sudo su - sdc`를 입력합니다.

단계 2 `/usr/local/cdo/toolkit` 디렉터리에 연결합니다.

단계 3 `sec.sh removetenant_name`을 실행하고 SEC를 제거할 의도를 확인합니다.

예:

```
[sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

**What to do next**

이 명령이 SEC를 제거하지 못한 경우 [SEC Cleanup 명령 실패, on page 789](#)를 계속하십시오.

**SEC Cleanup 명령 실패**

[SEC Cleanup 명령, on page 788](#)가 실패한 경우 이 절차를 사용합니다.

메시지: SEC를 찾을 수 없습니다. 종료합니다.

증상: Cleanup SEC 명령이 기존 SEC를 정리하지 못합니다.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42] SEC
not found, exiting.
```

복구: 정리 명령이 실패할 때 보안 이벤트 커넥터를 수동으로 정리합니다.

이미 실행 중인 SEC 도커 컨테이너를 제거합니다.

**Procedure**

단계 1 'sdc' 사용자로 SDC에 로그인합니다. 프롬프트에서 `sudo su - sdc`를 입력합니다.

단계 2 `docker ps` 명령을 실행하여 SEC 컨테이너의 이름을 찾습니다. SEC 이름은 "es\_name" 형식입니다.

단계 3 `docker stop` 명령을 실행하여 SEC 컨테이너를 중지합니다.

단계 4 `rm` 명령을 실행하여 SEC 컨테이너를 제거합니다.

예를 들면 다음과 같습니다.

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

**상태 확인을 사용하여 보안 이벤트 커넥터의 상태 학습**

SEC(보안 이벤트 커넥터) 상태 확인 스크립트는 SEC의 상태에 대한 정보를 제공합니다.

상태 확인을 실행하려면 다음 절차를 따르십시오.

**Procedure**

단계 1 VM 하이퍼바이저를 열고 SDC(보안 디바이스 커넥터)에 대한 콘솔 세션을 시작합니다.

단계 2 "cdo" 사용자로 SDC에 로그인합니다.

단계 3 "sdc" 사용자로 전환합니다.

```
[cdo@tenant]$sudo su sdc
```

단계 4 프롬프트에서 `healthcheck.sh` 스크립트를 실행하고 테넌트 이름을 지정합니다.

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

예를 들면 다음과 같습니다.

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

스크립트의 출력은 다음과 같은 종류의 정보를 제공합니다.

```
=====
Running SEC health check for tenant [redacted]
-----
SEC cloud URL [redacted] is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====
```

상태 확인 출력의 값:

- **SEC Cloud URL(SEC 클라우드 URL):** CDO 클라우드 URL 및 SEC가 CDO에 연결할 수 있는지 여부를 표시합니다.
- **SEC 커넥터:** SEC 커넥터가 올바르게 온보딩되고 시작된 경우 "Running(실행 중)"으로 표시됩니다.
- **SEC UDP 시스템 로그 서버:** UDP Syslog 서버가 UDP 이벤트를 전송할 준비가 된 경우 "Running(실행 중)"으로 표시됩니다.
- **SEC TCP 시스템 로그 서버:** TCP Syslog 서버가 TCP 이벤트를 전송할 준비가 된 경우 "Running(실행 중)"으로 표시됩니다.
- **SEC 커넥터 상태:** SEC가 실행 중이고 CDO에 온보딩된 경우 Active(활성)로 표시됩니다.
- **SEC Send sample event(SEC 샘플 이벤트 전송):** 상태 확인이 종료될 때 모든 상태 확인이 "녹색"인 경우 틀이 샘플 이벤트를 전송합니다. (프로세스 중 하나라도 "Down" 상태이면 테스트 이벤트 전송을 건너뛸 것입니다.) 샘플 이벤트는 이벤트 로그에 "sec-health-check"라는 정책으로 표시됩니다.

## 문제 해결 Cisco Defense Orchestrator

### 로그인 실패 문제 해결

실수로 잘못된 **CDO** 지역에 로그인했기 때문에 로그인에 실패함

적절한 CDO 지역에 로그인했는지 확인합니다. <https://sign-on.security.cisco.com>에 로그인하면 액세스할 지역을 선택할 수 있습니다. **CDO**타일을 클릭하여 [defenceorchestrator.com](https://defenceorchestrator.com)에 액세스하거나 **CDO(EU)**를 클릭하여 [defenceorchestrator.eu](https://defenceorchestrator.eu)에 액세스합니다.

## 마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 72 페이지의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

**Cisco Secure Cloud Sign-On** 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 <https://cdo.onelogin.com>을 가리킬 수 있습니다.

해결 방법 <https://sign-on.security.cisco.com>에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성
- 해결 방법 새 계정을 생성한 경우 대시보드에서 Cisco Defense Orchestrator(US), Cisco Defense Orchestrator(EU) 또는 Cisco Defense Orchestrator(APJC)에 해당하는 CDO 타일을 클릭합니다.
- 해결 방법 <https://sign-on.security.cisco.com>을 가리키도록 북마크를 업데이트합니다.

## 액세스 및 인증서 문제 해결

### 새 지문 탐지 상태 확인

#### Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 새 지문 감지됨 상태에서 디바이스를 선택합니다.

단계 5 새 지문 감지됨 창에서 지문 검토를 클릭합니다.

단계 6 지문을 검토하고 수락하라는 메시지가 표시되면

- Download Fingerprint**(지문 다운로드)를 클릭하고 검토합니다.
- 지문에 만족하면 **Accept**(수락)를 클릭합니다. 그렇지 않은 경우 **Cancel**(취소)를 클릭합니다.

단계 7 새 지문 문제를 해결한 후 디바이스의 연결 상태가 온라인으로 표시되고 구성 상태가 "동기화되지 않음" 또는 "충돌 감지됨"으로 표시될 수 있습니다. 구성 충돌 해결을 검토하여 CDO와 디바이스 간의 구성 차이를 검토하고 해결합니다.

## 보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결

다음은 이벤트 뷰어를 사용하여 네트워크 문제를 트러블슈팅하는 데 사용할 수 있는 기본 프레임워크입니다.

이 시나리오에서는 네트워크 운영 팀에서 사용자가 네트워크의 리소스에 액세스할 수 없다는 보고를 받은 것으로 가정합니다. 문제를 보고하는 사용자와 해당 위치를 기반으로, 네트워크 운영 팀은 어떤 방화벽이 리소스에 대한 액세스를 제어하는지를 합리적으로 파악합니다.



**Note** 또한 이 시나리오에서는 FDM 관리 디바이스가 네트워크 트래픽을 관리하는 방화벽이라고 가정합니다. Security Analytics and Logging(보안 분석 및 로깅)은 다른 디바이스 유형에서 로깅 정보를 수집하지 않습니다.

### Procedure

단계 1 탐색창에서 분석 > 이벤트 로깅을 선택합니다.

단계 2 기록 탭을 클릭합니다.

단계 3 시간 범위를 기준으로 이벤트 필터링을 시작합니다. 기본적으로 Historical(기록) 탭에는 이벤트의 마지막 시간이 표시됩니다. 올바른 시간 범위인 경우 현재 날짜와 시간을 **End**(종료) 시간으로 입력합니다. 올바른 시간 범위가 아닌 경우 보고된 문제의 시간을 포함하는 시작 및 종료 시간을 입력합니다.

단계 4 **Sensor ID**(센서 ID) 필드에 사용자의 액세스를 제어하는 것으로 의심되는 방화벽의 IP 주소를 입력합니다. 방화벽이 두 개 이상인 경우 검색 창에서 속성:값 쌍을 사용하여 이벤트를 필터링합니다. 두 항목을 만들고 OR 문으로 결합합니다. 예: SensorID:192.168.10.2 OR SensorID:192.168.20.2.

단계 5 Events(이벤트) 필터 표시줄의 **Source IP**(소스 IP) 필드에 사용자의 IP 주소를 입력합니다.

단계 6 사용자가 리소스에 액세스할 수 없는 경우 **Destination IP**(대상 IP) 필드에 해당 리소스의 IP 주소를 입력해 보십시오.

단계 7 결과에서 이벤트를 확장하고 세부 정보를 확인합니다. 다음은 몇 가지 세부 사항입니다.

- **AC\_RuleAction** - 규칙이 트리거될 때 수행된 작업(허용, 신뢰, 차단).
- **FirewallPolicy** - 이벤트를 트리거한 규칙이 상주하는 정책입니다.
- **FirewallRule** - 이벤트를 트리거한 규칙의 이름입니다. 값이 Default Action(기본 작업)인 경우 정책의 규칙 중 하나가 아니라 이벤트를 트리거한 것은 정책의 기본 작업입니다.
- **UserName** - 이니시에이터 IP 주소와 연결된 사용자입니다. 이니시에이터 IP 주소는 소스 IP 주소와 동일합니다.

단계 8 규칙 작업이 액세스를 차단하는 경우 FirewallRule 및 FirewallPolicy 필드를 확인하여 액세스를 차단하는 정책의 규칙을 식별합니다.

## SSL 암호 해독 문제 해결

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리(SSL 또는 인증 기관 피닝)

스마트폰 및 기타 디바이스용 일부 앱은 SSL(또는 인증 기관) 피닝이라는 기술을 사용합니다. SSL 피닝 기술은 원래 서버 인증서의 해시를 앱 자체에 포함합니다. 따라서 앱이 Firepower Threat Defense 디바이스에서 재서명된 인증서를 받으면 해시 검증에 실패하고 연결이 중단됩니다.

이때 기본적인 증상은 사용자가 사이트 앱을 사용해서는 웹 사이트에 연결할 수 없지만 웹 브라우저를 사용하면 연결할 수 있다는 것입니다(앱으로 연결에 실패한 디바이스에서 브라우저를 사용할 때도 연결 가능). 예를 들어 사용자는 Facebook iOS 또는 Android 앱을 사용할 수 없지만 Safari 또는 Chrome을 <https://www.facebook.com>으로 지정하고 성공적으로 연결할 수 있습니다.

SSL 피닝은 특별히 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이러한 현상을 해결하는 방법은 없습니다. 다음 옵션 중에서 선택해야 합니다.

기타 세부정보

특정 사이트가 브라우저에서는 작동하는데 동일 디바이스의 앱에서는 작동하지 않는 경우 SSL 피닝 인스턴스를 살펴봐야 합니다. 하지만 심층적으로 확인하려면 연결 이벤트를 사용해 브라우저 테스트와 더불어 SSL 피닝을 확인할 수 있습니다.

앱은 두 가지 방식으로 해시 검증 장애를 처리할 수 있습니다.

- Facebook 등의 그룹 1 앱은 서버에서 SH, CERT, SHD 메시지를 받는 즉시 SSL ALERT 메시지를 보냅니다. Alert는 보통 SSL 피닝을 나타내는 "Unknown CA (48)(알 수 없는 CA(48))" 알림입니다. 알림 메시지 후에는 TCP Reset(TCP 재설정)이 전송됩니다. 이벤트 세부사항에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT\_SEEN이 포함되어 있습니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 APP\_DATA\_C2S 또는 APP\_DATA\_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT\_HELLO, SERVER\_HELLO, SERVER\_CERTIFICATE, SERVER\_KEY\_EXCHANGE, SERVER\_HELLO\_DONE입니다.
- Dropbox 등의 그룹 2 앱은 알림을 보내지 않습니다. 대신 핸드셰이크가 완료될 때까지 기다렸다가 TCP Reset(TCP 재설정)을 전송합니다. 이벤트에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT\_SEEN, APP\_DATA\_C2S 또는 APP\_DATA\_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT\_HELLO, SERVER\_HELLO, SERVER\_CERTIFICATE, SERVER\_KEY\_EXCHANGE, SERVER\_HELLO\_DONE, CLIENT\_KEY\_EXCHANGE, CLIENT\_CHANGE\_CIPHER\_SPEC, CLIENT\_FINISHED, SERVER\_CHANGE\_CIPHER\_SPEC, SERVER\_FINISHED입니다.

## 침입 방지 시스템 문제 해결

### 내 IPS 정책 옵션은 무엇입니까?

온보딩된 모든 디바이스는 "기본 오버라이드"라는 CDO 제공 IPS 정책과 자동으로 연결됩니다. CDO는 모든 FTD 디바이스에 대해 새 IPS 정책을 생성하므로 이 이름을 가진 정책이 여러 개 있을 수 있습니다. 기본 IP 정책을 사용하지만 서명 오버라이드 옵션을 편집하려는 경우 자세한 내용은 [Firepower 침입 정책 서명 오버라이드](#)를 참조하십시오. 디바이스마다 다른 서명 오버라이드를 구성하면 기본 오버라이드 정책이 일관되지 않을 수 있습니다.

### 모든 디바이스에 대해 서로 다른 IPS 정책을 사용하려면 어떻게 해야 합니까?

CDO는 모든 FTD 디바이스에 대해 새 IPS 정책을 생성하므로 이 이름을 가진 정책이 여러 개 있을 수 있습니다. 각 디바이스가 온보딩된 후 CDO 제공 IPS 정책의 이름을 바꿀 필요가 없습니다. 정책을 확장하면 연결된 디바이스가 표시되며 디바이스 또는 정책별로 위협 이벤트 페이지 및 서명 오버라이드 페이지를 필터링할 수도 있습니다. 기본 오버라이드 정책을 사용자 지정하려면 디바이스별로 서명 오버라이드를 구성합니다. 이로 인해 기본 오버라이드 침입 정책이 일관되지 않게 되지만 기능이 금지되지는 않습니다.

**FDM**에서 오버라이드가 구성된 디바이스를 온보딩했습니다.

CDO 외부에서 구성된 오버라이드는 디바이스 구성이나 기능에 문제를 일으키지 않습니다.

오버라이드가 이미 구성되어 있는 디바이스를 온보딩하고 이 새 디바이스가 오버라이드가 없는 디바이스와 IP 정책을 공유하는 경우 IPS 정책이 일관성 없음으로 표시됩니다. 일관성 없음을 해결하려면 [Firepower 침입 정책 서명 오버라이드](#)를 참조하십시오.

## 마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 [Cisco Secure Cloud Sign-On](#) 계정을 사용하려면 새 [Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 72 페이지](#)의 지침에 따라 새 [Cisco Secure Cloud Sign-On](#) 계정에 등록해야 합니다.

**Cisco Secure Cloud Sign-On** 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 [Cisco Secure Cloud Sign-On](#) 계정을 만들었을 수 있습니다. CDO와 [Cisco Secure Sign-On](#) 간의 사용자 정보를 표준화하려면 [Cisco TAC\(Technical Assistance Center\)](#)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 <https://cdo.onelogin.com>을 가리킬 수 있습니다.

해결 방법 <https://sign-on.security.cisco.com>에 로그인합니다.



- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 새 [Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성](#)
- 해결 방법 새 계정을 생성한 경우 대시보드에서 Cisco Defense Orchestrator(US), Cisco Defense Orchestrator(EU) 또는 Cisco Defense Orchestrator(APJC)에 해당하는 CDO 타일을 클릭합니다.
- 해결 방법 <https://sign-on.security.cisco.com>을 가리키도록 북마크를 업데이트합니다.

## 개체 문제 해결

### 중복 개체 문제 해결

중복 개체란 이름은 다르지만 값은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 대개 실수로 생성되고 유사한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체 문제를 해결한 후 CDO는 유지된 개체 이름으로 영향을 받는 모든 개체 참조를 업데이트합니다.

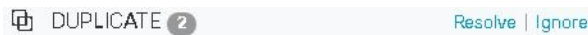
중복 개체 문제를 해결하려면 다음을 수행합니다.

#### Procedure

단계 1 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.

단계 2 그런 다음 개체를 **개체 필터**하여 중복 개체 문제를 찾습니다.

단계 3 결과 중 하나를 선택합니다. 개체 세부 정보 패널에 영향을 받는 중복 수가 포함된 **DUPLICATE** 필드가 표시됩니다.



단계 4 **Resolve**(해결)를 클릭합니다. CDO는 비교할 중복 개체를 표시합니다.

단계 5 비교할 두 개체를 선택합니다.

단계 6 이제 다음과 같은 옵션이 제공됩니다.

- 개체 중 하나를 다른 개체로 교체하려면 유지할 개체에 대해 **Pick**(선택)을 클릭하고 **Resolve**(확인)를 클릭하여 영향을 받을 디바이스 및 네트워크 정책을 확인한 다음, 변경 사항이 마음에 들면 **Confirm**(확인)를 클릭합니다. CDO는 선택한 개체를 교체로 유지하고 중복 항목을 삭제합니다.
- 목록에 무시할 개체가 있는 경우 **Ignore**(무시)를 클릭합니다. 개체를 무시하면 CDO에 표시되는 중복 개체 목록에서 제거됩니다.
- 개체는 유지하지만 CDO가 중복 개체를 검색할 때 찾지 않도록 하려면 **Ignore All**(모두 무시)를 클릭합니다.

단계 7 중복 개체 문제가 해결되면 지금 변경 사항을 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 추적](#), 기다렸다가 여러 변경 사항을 한 번에 배포합니다.


## 일관성이 없거나 사용되지 않는 보안 영역 개체 해결

보안 영역 개체는 다른 개체처럼 일관성이 없거나 사용되지 않는 것으로 표시될 수 있습니다. 이러한 문제를 해결하는 방법에 대한 지침은 [사용되지 않는 개체 문제 해결](#) 및 [불일치 개체 문제 해결](#)을 참조하십시오.

관련 정보:

- [보안 영역 개체](#)
- [보안 영역에 Firepower 인터페이스 할당](#)
- [개체 삭제](#)

## 사용되지 않는 개체 문제 해결

사용되지 않는 개체 는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다.

관련 정보:

- [디바이스 및 서비스 목록 내보내기, 92 페이지](#)
- [CDO에 디바이스 대량 다시 연결, 96 페이지](#)

## 사용되지 않는 개체 문제 해결


### Procedure

단계 1 왼쪽의 CDO 내비게이션 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.

단계 2 그런 다음 개체를 **개체 필터**하여 사용하지 않는 개체 문제를 찾습니다.

단계 3 하나 이상의 사용되지 않는 개체를 선택합니다.

단계 4 이제 다음과 같은 옵션이 제공됩니다.



- **Actions**(작업) 창에서 **Remove**(제거) 를 클릭하여 CDO에서 사용되지 않는 개체를 제거합니다.
- **Issues**(문제) 창에서 **Ignore**(무시)를 클릭합니다. 개체를 무시하면 CDO는 사용되지 않는 개체의 결과에 해당 개체를 표시하지 않습니다.

단계 5 사용되지 않는 개체를 제거한 경우, [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 620](#) 지금 변경한 사항을 수행하거나 대기하고 여러 변경 사항을 한 번에 구축합니다.



**Note**      사용되지 않는 개체 문제를 벌크로 해결하려면 [대량의 개체 문제 해결](#)을 참조하십시오.

## 사용되지 않는 개체 대량 제거

## Procedure

- 단계 1 왼쪽의 CDO 내비게이션 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.
- 단계 2 그런 다음 개체를 **개체 필터**하여 사용하지 않는 개체 문제를 찾습니다.
- 단계 3 삭제하려는 사용되지 않는 개체를 선택합니다.
- 개체 테이블 헤더 행의 확인란을 클릭하여 페이지의 모든 개체를 선택합니다.
  - 개체 테이블에서 사용하지 않는 개별 개체를 선택합니다.
- 단계 4 오른쪽의 작업 창에서 **Remove**(제거) 를 클릭하여 CDO에서 선택한 사용되지 않는 개체를 모두 제거합니다. 한 번에 99개의 개체를 제거할 수 있습니다.
- 단계 5 **OK**(확인)을 클릭하여 사용하지 않는 개체를 삭제할 것인지 확인합니다.
- 단계 6 이러한 변경 사항을 배포하기 위한 두 가지 선택 사항이 있습니다.
- 지금 변경한 내용을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.
  - **Inventory**(인벤토리) 페이지를 열고 변경의 영향을 받은 디바이스를 찾습니다. 변경의 영향을 받은 모든 디바이스를 선택하고 관리 창에서 **Deploy All**(모두 배포) 를 클릭합니다. 경고를 읽고 적절한 조치를 취합니다.

## 불일치 개체 문제 해결

불일치 개체  INCONSISTENT  [Resolve](#) | [Ignore](#) 는 두 개 이상의 디바이스에서 이름은 같지만 값이 다른 개체입니다. 사용자가 동일한 이름 및 콘텐츠를 사용하여 서로 다른 구성에서 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라지므로 불일치가 발생하는 경우가 있습니다.

참고: 일관되지 않은 개체 문제를 벌크로 해결하려면 [대량의 개체 문제 해결](#)을 참고하십시오.

일치하지 않는 개체에 대해 다음을 수행할 수 있습니다.

- **Ignore**(무시): CDO가 개체 간의 불일치를 무시하고 해당 값을 유지합니다. 개체가 더 이상 불일치 범주에 나열되지 않습니다.
- **Merge**(병합): CDO가 선택한 모든 개체와 해당 값을 단일 개체 그룹으로 결합합니다.
- **Rename**(이름 바꾸기): CDO를 사용하면 일치하지 않는 개체 중 하나의 이름을 바꾸고 새 이름을 지정할 수 있습니다.
- **Convert Shared Network Objects to Overrides**(공유 네트워크 개체를 오버라이드로 변환): CDO를 사용하면 일관성이 없는 공유 개체(오버라이드가 있거나 없는)를 오버라이드가 있는 단일 공

유 개체로 결합할 수 있습니다. 일치하지 않는 개체의 가장 일반적인 기본값은 새로 형성된 개체의 기본값으로 설정됩니다.



**Note** 공통 기본값이 여러 개인 경우 그 중 하나가 기본값으로 선택됩니다. 나머지 기본값 및 재정의 값은 해당 개체의 재정의로 설정됩니다.

- **Convert Shared Network Group to Additional Values**(공유 네트워크 그룹을 추가 값으로 변환):  
- CDO를 사용하면 일치하지 않는 공유 네트워크 그룹을 추가 값이 있는 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 이 기능의 기준은 변환할 일관되지 않은 네트워크 그룹에 동일한 값을 가진 공통 개체가 하나 이상 있어야 한다는 것입니다. 이 기준과 일치하는 모든 기본값은 기본값이 되며, 나머지 개체는 새로 형성된 네트워크 그룹의 추가 값으로 할당됩니다.

예를 들어, 일치하지 않는 두 개의 공유 네트워크 그룹을 고려하십시오. 첫 번째 네트워크 그룹 'shared\_network\_group'은 'object\_1'(192.0.2.x) 및 'object\_2'(192.0.2.y)로 구성됩니다. 여기에는 추가 값 'object\_3'(192.0.2.a)도 포함됩니다. 두 번째 네트워크 그룹 'shared\_network\_group'은 'object\_1'(192.0.2.x) 및 추가 값 'object\_4'(192.0.2.b)로 구성됩니다. 공유 네트워크 그룹을 추가 값으로 변환할 때 새로 형성된 그룹 'shared\_network\_group'에는 'object\_1'(192.0.2.x) 및 'object\_2'(192.0.2.y)가 포함되며, 'object\_3'(192.0.2.a) 및 'object\_4'(192.0.2.b)를 추가 값으로 사용합니다.



**Note** 새 네트워크 개체를 생성하면 CDO는 자동으로 해당 값을 동일한 이름의 기존 공유 네트워크 개체에 오버라이드로 할당합니다. 이는 새 디바이스가 CDO에 온보딩된 경우에도 적용됩니다.

자동 할당은 다음 기준을 충족하는 경우에만 발생합니다.

1. 새 네트워크 개체를 디바이스에 할당해야 합니다.
2. 이름과 유형이 같은 공유 개체는 테넌트에 하나만 있어야 합니다.
3. 공유 개체에 이미 오버라이드가 포함되어 있어야 합니다.

일관성 없는 개체 문제를 해결하려면 다음을 수행합니다.

### Procedure

- 단계 1 왼쪽의 CDO 내비게이션 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.
- 단계 2 그런 다음 개체를 **개체 필터**하여 일관성 없는 개체 문제를 찾습니다.
- 단계 3 일치하지 않는 개체를 선택합니다. 개체 세부 정보 패널에 영향을 받는 개체의 수가 포함된 INCONSISTENT 필드가 표시됩니다.



- 단계 4 **Resolve**(해결)를 클릭합니다. CDO는 비교할 일치하지 않는 개체를 표시합니다.

단계 5 이제 다음과 같은 옵션이 제공됩니다.

- 모두 무시:
  - a. 표시된 개체를 비교하고 개체 중 하나에서 **Ignore**(무시)를 클릭합니다. 또는 모든 개체를 무시하려면 **Ignore All**(모두 무시)을 클릭합니다.
  - b. **OK**(확인)를 클릭하여 확인합니다.
- 개체를 병합하여 해결합니다.
  - a. **Resolve by Merging X Objects**(X개 개체를 병합하여 해결)를 클릭합니다.
  - b. **OK**(확인)를 클릭합니다.
- **Rename**(이름 바꾸기):
  - a. **Rename**(이름 변경)을 클릭합니다.
  - b. 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm**(확인)을 클릭합니다.
- **Convert to Overrides**(오버라이드로 변환)(일치하지 않는 공유 개체의 경우): 공유 개체를 오버라이드와 비교할 때, 비교 패널의 **Inconsistent Values**(일관되지 않는 값) 필드에 기본값만 표시됩니다.
  - a. **Convert to Overrides**(재정의로 변환)를 클릭합니다. 일치하지 않는 모든 개체는 오버라이드가 포함된 단일 공유 개체로 변환됩니다.
  - b. **OK**(확인)를 클릭합니다. **Edit Shared Object**(공유 개체 편집)를 클릭하여 새로 형성된 개체의 세부 정보를 볼 수 있습니다. 위쪽 및 아래쪽 화살표를 사용하여 기본값과 재정의의 간에 값을 이동할 수 있습니다.
- **Convert to Additional Values**(추가 값으로 변환)(일치하지 않는 네트워크 그룹의 경우):
  - a. **Convert to Additional Values**(추가 값으로 변환)를 클릭합니다. 일치하지 않는 모든 개체는 추가 값이 있는 단일 공유 개체로 변환됩니다.
  - b. 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm**(확인)을 클릭합니다.

단계 6 불일치를 해결한 후 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

## 대량의 개체 문제 해결

사용되지 않는 개체 문제 해결 중복 개체 문제 해결 불일치 개체 문제 해결, on page 797 문제가 있는 개체를 해결하는 한 가지 방법은 이러한 개체를 무시하는 것입니다. 개체에 둘 이상의 문제가 있더라

도 여러 개체를 선택하고 무시할 수 있습니다. 예를 들어 개체가 일치하지 않고 사용되지 않는 경우 한 번에 하나의 문제 유형만 무시할 수 있습니다.



### Important

나중에 개체가 다른 문제 유형과 연결될 경우 커밋한 무시 작업은 해당 시점에 선택한 문제에만 영향을 미칩니다. 예를 들어, 개체가 중복되었기 때문에 개체를 무시했고 개체가 나중에 일치하지 않는 것으로 표시되는 경우, 중복 개체로 무시한다고 해서 일치하지 않는 개체로 무시되는 것은 아닙니다.

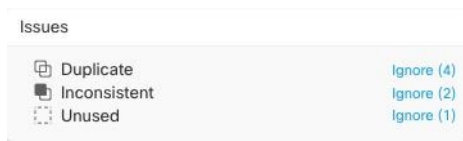
대량으로 문제를 무시하려면 다음 절차를 수행합니다.

### Procedure

단계 1 왼쪽의 CDO 내비게이션 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.

단계 2 검색 범위를 좁히기 위해 개체 문제를 **개체 필터**할 수 있습니다.

단계 3 Object(개체) 테이블에서 무시할 적용 가능한 모든 개체를 선택합니다. Issues(문제) 창은 문제 유형별로 개체를 그룹화합니다.



단계 4 유형별로 문제를 무시하려면 **Ignore**(무시)를 클릭합니다. 각 문제 유형을 개별적으로 무시해야 합니다.

단계 5 **OK**(확인)를 클릭하여 해당 개체를 무시할 것임을 확인합니다.

## 디바이스 연결 상태

CDO 테넌트에 온보딩된 디바이스의 연결 상태를 볼 수 있습니다. 이 항목은 다양한 연결 상태를 이해하는 데 도움이 됩니다. **Inventory**(인벤토리) 페이지에서 **Connectivity**(연결) 열은 디바이스 연결 상태를 표시합니다.

디바이스 연결 상태가 '온라인'이면 디바이스의 전원이 켜져 있고 CDO에 연결되어 있음을 의미합니다. 아래 표에 설명된 다른 상태는 일반적으로 여러 가지 이유로 디바이스에 문제가 발생할 때 발생합니다. 이 표는 이러한 문제에서 복원하는 방법을 제공합니다. 연결 실패를 일으키는 문제가 두 개 이상 있을 수 있습니다. 다시 연결을 시도하면, CDO는 다시 연결을 수행하기 전에 먼저 이러한 모든 문제를 편집하라는 메시지를 표시합니다.


디바이스 연결 상태	가능한 이유	해결 방법
온라인	디바이스의 전원이 켜져 있고 CDO에 연결되어 있습니다.	해당 없음

디바이스 연결 상태	가능한 이유	해결 방법
오프라인	디바이스의 전원이 꺼졌거나 네트워크 연결이 끊겼습니다.	디바이스가 오프라인 상태인지 확인합니다.
불충분한 라이선스	디바이스에 충분한 라이선스가 없습니다.	<a href="#">라이선스 부족 문제 해결, on page 802</a>
유효하지 않은 자격 증명	디바이스에 연결하기 위해 CDO에서 사용하는 사용자 이름과 암호 조합이 올바르지 않습니다.	<a href="#">유효하지 않은 자격 증명 문제 해결, on page 803</a>
새 인증서 탐지됨	디바이스의 인증서가 변경되었습니다. 디바이스가 자체 서명된 인증서를 사용하는 경우 디바이스의 전원을 껐다 켜서 이 문제가 발생했을 수 있습니다.	<a href="#">새 인증서 문제 트러블슈팅, on page 804</a>
미등록 디바이스	FTD 디바이스가 FDM을 통해 클라우드에서 등록 취소되었습니다.	<a href="#">등록되지 않은 디바이스 문제 해결, on page 765</a>
클레임 오류	CDO가 FTD 디바이스를 요청하지 못했습니다. 가능한 이유 중 일부는 유효하지 않은 일련 번호를 입력했거나 디바이스 일련 번호가 이미 요청되었기 때문일 수 있습니다.	클레임 오류
온보딩 오류	CDO는 디바이스를 온보딩할 때 디바이스와의 연결이 끊어졌을 수 있습니다.	<a href="#">온보딩 오류 문제 해결, on page 813</a>
프로비저닝 오류	FTD 디바이스 초기 프로비저닝에 실패했습니다.	프로비저닝 오류
연결 불가	<ul style="list-style-type: none"> <li>디바이스의 전원이 꺼져 있습니다.</li> <li>디바이스에서 IP 주소가 변경되었습니다.</li> <li>디바이스가 Cisco Cloud에서 삭제되었습니다.</li> </ul>	<a href="#">연결할 수 없는 연결 상태 문제 해결, on page 814</a>

## 등록되지 않은 디바이스 문제 해결

FDM 관리 디바이스가 Firewall Device Manager을 통해 클라우드에서 등록 취소되었을 수 있습니다. 클라우드에 디바이스를 다시 등록하려면 다음을 수행하십시오.

프로시저

- 
- 단계 1 **Inventory**(인벤토리) 페이지에서 **Devices**(장치) 탭을 클릭합니다.
- 단계 2 **FTD** 탭을 클릭하고 "미등록된 디바이스" 상태의 디바이스를 선택하면 오른쪽의 오류 메시지가 표시 됩니다.
- 단계 3 등록되지 않은 디바이스가 등록 키를 사용하여 온보딩된 경우, Cisco Defense Orchestrator는 이전에 적용된 키가 만료되었으므로 새 등록 키를 생성하라는 메시지를 표시합니다.
- 새로 고침 버튼을 클릭하여 새 등록 키를 생성한 다음 Copy(복사) 아이콘 를 클릭합니다.
  - CDO에 등록하려는 디바이스의 Firewall Device Manager에 로그인합니다.
  - System Settings**(시스템 설정)에서 **Cloud Services**(클라우드 서비스)를 클릭합니다.
  - Cisco Defense Orchestrator 영역에서 **Get Started**(시작하기)를 클릭합니다.
  - Registration Key**(등록 키) 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.
  - Register**(등록)를 클릭한 다음 Cisco 고지 사항을 수락합니다. Firewall Device Manager는 CDO에 등록 요청을 보냅니다.
  - 디바이스의 연결 상태가 "읽기 오류"로 변경될 때까지 CDO에서 **Inventory**(인벤토리) 페이지를 새로 고칩니다.
  - 디바이스에서 구성을 읽으려면 CDO에 대한 **Read Configuration**(구성 읽기)를 클릭합니다.
- 단계 4 등록되지 않은 디바이스가 일련 번호를 사용하여 온보딩된 경우, CDO는 Firewall Device Manager에서 디바이스를 자동 등록하라는 메시지를 표시합니다.
- CDO에 등록하려는 디바이스의 Firewall Device Manager에 로그인합니다.
  - System Settings**(시스템 설정)에서 **Cloud Services**(클라우드 서비스)를 클릭합니다.
  - Auto-enroll with Tenancy from Cisco Defense Orchestrator**(Cisco Defense Orchestrator에서 테넌 시로 자동 등록) 옵션을 선택하고 **Register**(등록)를 클릭합니다.
  - 디바이스의 연결 상태가 "읽기 오류"로 변경될 때까지 CDO에서 **Inventory**(인벤토리) 페이지를 새로 고칩니다.
  - 디바이스에서 구성을 읽으려면 CDO에 대한 **Read Configuration**(구성 읽기)를 클릭합니다.
- 

## 라이선스 부족 문제 해결

디바이스 연결 상태가 "Insufficient License(라이선스 부족)"로 표시되면 다음을 수행합니다.

- 디바이스가 라이선스를 획득할 때까지 잠시 기다립니다. 일반적으로 Cisco Smart Software Manager가 디바이스에 새 라이선스를 적용하는 데 시간이 걸립니다.



- 디바이스 상태가 변경되지 않으면 CDO에서 로그아웃하고 다시 로그인하여 CDO 포털을 새로 고침한 후 라이선스 서버와 디바이스 간의 네트워크 통신 문제를 해결합니다.
- 포털을 새로 고침해도 디바이스 상태가 변경되지 않으면 다음을 수행합니다.

### Procedure

- 단계 1 Cisco Smart Software Manager에서 새 토큰을 생성하고 복사합니다. 자세한 내용은 [스마트 라이선싱 생성](#) 비디오를 참조하십시오.
- 단계 2 CDO 탐색 모음에서 **Devices & Services**(디바이스 및 서비스) 페이지를 클릭합니다.
- 단계 3 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 4 적절한 디바이스 유형 탭을 클릭하고 **Insufficient License**(라이선스 부족) 상태의 디바이스를 선택합니다.
- 단계 5 **Device Details**(디바이스 세부 정보) 창에서 **Insufficient Licenses**(불충분한 라이선스)에 표시되는 **Manage Licenses**(라이선스 관리)를 클릭합니다. **Manage Licenses**(라이선스 관리) 창이 나타납니다.
- 단계 6 활성화 필드에 새 토큰을 붙여넣고 디바이스 등록을 클릭합니다.  
토큰이 디바이스에 성공적으로 적용되면 연결 상태가 온라인으로 바뀝니다.

## 유효하지 않은 자격 증명 문제 해결

유효하지 않은 자격 증명으로 인한 디바이스 연결 끊김을 해결하려면 다음을 수행합니다.

### Procedure

- 단계 1 **Inventory**(재고 목록) 페이지를 엽니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 적절한 디바이스 유형 탭을 클릭하고 **Invalid Credentials**(유효하지 않은 자격 증명) 상태의 디바이스를 선택합니다.
- 단계 4 **Device Details**(디바이스 세부 정보) 창에서 **Invalid Credentials**(잘못된 자격 증명)에 나타나는 **Reconnect**(재연결)을 클릭합니다. CDO가 디바이스와의 재연결을 시도합니다.
- 단계 5 프롬프트가 나타나면 Linux 사용자 이름 및 비밀번호를 입력합니다.
- 단계 6 **Continue**(계속)를 클릭합니다.
- 단계 7 디바이스가 온라인 상태가 되고 사용할 준비가 되면 **Close**(닫기)를 클릭합니다.
- 단계 8 CDO가 잘못된 자격 증명을 사용하여 디바이스에 연결하려고 시도했기 때문에 CDO가 디바이스에 연결하는 데 사용해야 하는 사용자 이름 및 비밀번호 조합이 디바이스에서 직접 변경되었을 수 있습니다. 이제 디바이스가 "Online(온라인)"이지만 구성 상태가 "Conflict Detected(충돌 탐지됨)"인 것을

확인할 수 있습니다. **구성 충돌 해결**를 사용하여 CDO와 디바이스 간의 구성 차이를 검토하고 해결합니다.

## 새 인증서 문제 트러블슈팅

### CDO의 인증서 사용

CDO는 디바이스에 연결할 때 인증서의 유효성을 확인합니다. 특히 CDO는 다음을 요구합니다.

1. 디바이스에서 1.0 이상의 TLS 버전을 사용합니다.
2. 디바이스에서 제시한 인증서가 만료되지 않았으며 발급 날짜가 과거입니다(즉, 이미 유효하며 나중에 유효해질 예정이 아님).
3. 인증서는 SHA-256 인증서여야 합니다. SHA-1 인증서는 허용되지 않습니다.
4. 다음 조건 중 하나가 참입니다.
  - 디바이스가 자체 서명 인증서를 사용하며, 인증된 사용자가 신뢰하는 최신 인증서와 동일합니다.
  - 디바이스는 신뢰할 수 있는 CA(Certificate Authority)에서 서명한 인증서를 사용하며, 제공된 리프 인증서를 관련 CA에 연결하는 인증서 체인을 제공합니다.

다음은 CDO가 브라우저와 다른 방식으로 인증서를 사용하는 방법입니다.

- 자체 서명 인증서의 경우 CDO는 도메인 이름 확인을 오버라이드하며, 그 대신 디바이스 온보딩 또는 재연결 중에 인증된 사용자가 신뢰하는 인증서와 인증서가 정확히 일치하는지 확인합니다.
- CDO는 아직 내부 CA를 지원하지 않습니다. 현재는 내부 CA가 서명한 인증서를 확인할 수 있는 방법이 없습니다.

디바이스별로 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있습니다. CDO에서 ASA의 인증서를 신뢰할 수 없는 경우 해당 디바이스에 대한 인증서 검사를 비활성화할 수 있습니다. 디바이스에 대한 인증서 확인을 비활성화하려고 시도했지만 여전히 디바이스를 온보딩할 수 없는 경우, 디바이스에 대해 지정한 IP 주소 및 포트가 잘못되었거나 연결할 수 없는 것일 수 있습니다. 인증서 검사를 전역적으로 비활성화하거나 지원되는 인증서가 있는 디바이스에 대한 인증서 검사를 비활성화할 수 있는 방법은 없습니다. 비 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있는 방법은 없습니다.

디바이스에 대한 인증서 확인을 비활성화하면 CDO는 TLS를 사용하여 디바이스에 연결하지만 연결을 설정하는 데 사용된 인증서를 검증하지 않습니다. 즉, 수동적인 중간자 공격자는 연결을 도청할 수 없지만, 활성 상태의 중간자 공격자는 CDO에 유효하지 않은 인증서를 제공하여 연결을 가로챌 수 있습니다.

## 인증서 문제 식별

CDO가 디바이스를 온보딩하지 못할 수 있는 몇 가지 이유가 있습니다. UI에 "CDO cannot connect to the device using the certificate presented(CDO가 제공된 인증서를 사용하여 디바이스에 연결할 수 없음)"라는 메시지가 표시되면 인증서에 문제가 있는 것입니다. UI에 이 메시지가 표시되지 않으면 연결 문제(디바이스에 연결할 수 없음) 또는 기타 네트워크 오류와 관련이 있을 가능성이 높습니다.

CDO가 지정된 인증서를 거부하는 이유를 확인하려면 SDC 호스트 또는 관련 디바이스에 연결할 수 있는 다른 호스트에서 `openssl` 명령줄 툴을 사용할 수 있습니다. 다음 명령을 사용하여 디바이스에서 제공하는 인증서를 보여주는 파일을 생성합니다.

```
openssl s_client -showcerts -connect <host>:<port> && <filename>.txt
```

이 명령은 인터랙티브 세션을 시작하므로 몇 초 후에 종료하려면 `Ctrl-c`를 사용해야 합니다.

이제 다음과 같은 출력이 포함된 파일이 생성됩니다.

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
...lots of base64...
tzw9TylihnhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIx CzAJBgNVBAYTA1VT
...lots of base64...
tzw9TylihnhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDftCCAuaqAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTA1VT
...lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhd8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
```

```

No ALPN negotiated
SSL-Session:
  Protocol : TLSv1.2
  Cipher : ECDHE-RSA-AES128-GCM-SHA256
  Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
  Session-ID-ctx:
  Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

  Key-Arg : None
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 100800 (seconds)
  TLS session ticket:
0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[...eo..
0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.....3(
0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c....c.d.6
0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d ".:Y...!\..R(E.
0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I....
0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
00a0 - 72 a4 ad
00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

이 출력에서 가장 먼저 확인할 사항은 반환 코드 확인이 표시되는 마지막 줄입니다. 인증서 문제가 있는 경우 반환 코드는 0이 아니며 오류에 대한 설명이 표시됩니다.

일반적인 오류 및 해결 방법을 보려면 이 인증서 오류 코드 목록을 확장합니다.

0 X509\_V\_OK 작업에 성공했습니다.

2 X509\_V\_ERR\_UNABLE\_TO\_GET\_ISSUER\_CERT 신뢰할 수 없는 인증서의 발급자 인증서를 찾을 수 없습니다.

3 X509\_V\_ERR\_UNABLE\_TO\_GET\_CRL 인증서의 CRL을 찾을 수 없습니다.

4 X509\_V\_ERR\_UNABLE\_TO\_DECRYPT\_CERT\_SIGNATURE 인증서 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 이는 RSA 키에만 의미가 있습니다.

5 X509\_V\_ERR\_UNABLE\_TO\_DECRYPT\_CRL\_SIGNATURE CRL 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 사용되지 않음.

6 X509\_V\_ERR\_UNABLE\_TO\_DECODE\_ISSUER\_PUBLIC\_KEY 인증서 SubjectPublicKeyInfo의 공개 키를 읽을 수 없습니다.

7 X509\_V\_ERR\_CERT\_SIGNATURE\_FAILURE 인증서의 서명이 유효하지 않습니다.

8 X509\_V\_ERR\_CRL\_SIGNATURE\_FAILURE 인증서의 서명이 유효하지 않습니다.

9 X509\_V\_ERR\_CERT\_NOT\_YET\_VALID 인증서가 아직 유효하지 않습니다. notBefore 날짜가 현재 시간 이후입니다. 자세한 내용은 아래의 **반환 코드 확인: 9(인증서가 아직 유효하지 않음)**를 참조하십시오.

- 10 X509\_V\_ERR\_CERT\_HAS\_EXPIRED 인증서가 만료되었습니다. 즉, notAfter 날짜는 현재 시간이 전입니다. 자세한 내용은 아래의 **반환 코드 확인: 10(인증서가 만료되었습니다)**을 참조하십시오.
- 11 X509\_V\_ERR\_CRL\_NOT\_YET\_VALID CRL이 아직 유효하지 않습니다.
- 12 X509\_V\_ERR\_CRL\_HAS\_EXPIRED CRL이 만료되었습니다.
- 13 X509\_V\_ERR\_ERROR\_IN\_CERT\_NOT\_BEFORE\_FIELD 인증서 notBefore 필드에 잘못된 시간이 포함되어 있습니다.
- 14 X509\_V\_ERR\_ERROR\_IN\_CERT\_NOT\_AFTER\_FIELD 인증서 notAfter 필드에 유효하지 않은 시간이 포함되어 있습니다.
- 15 X509\_V\_ERR\_ERROR\_IN\_CRL\_LAST\_UPDATE\_FIELD CRL lastUpdate 필드에 잘못된 시간이 포함되어 있습니다.
- 16 X509\_V\_ERR\_ERROR\_IN\_CRL\_NEXT\_UPDATE\_FIELD CRL nextUpdate 필드에 유효하지 않은 시간이 포함되어 있습니다.
- 17 X509\_V\_ERR\_OUT\_OF\_MEM 메모리를 할당하는 동안 오류가 발생했습니다. 이러한 현상은 발생해서는 안 됩니다.
- 18 X509\_V\_ERR\_DEPTH\_ZERO\_SELF\_SIGNED\_CERT 전달된 인증서가 자체 서명되었으며 신뢰할 수 있는 인증서 목록에서 동일한 인증서를 찾을 수 없습니다.
- 19 X509\_V\_ERR\_SELF\_SIGNED\_CERT\_IN\_CHAIN 신뢰할 수 없는 인증서를 사용하여 인증서 체인을 배포할 수 있지만 루트를 로컬에서 찾을 수 없습니다.
- 20 X509\_V\_ERR\_UNABLE\_TO\_GET\_ISSUER\_CERT\_LOCALLY 로컬로 조회된 인증서의 발급자 인증서를 찾을 수 없습니다. 이는 일반적으로 신뢰할 수 있는 인증서 목록이 완전하지 않음을 의미합니다.
- 21 X509\_V\_ERR\_UNABLE\_TO\_VERIFY\_LEAF\_SIGNATURE 체인에 하나의 인증서만 포함되어 있으며 자체 서명되지 않았으므로 서명을 확인할 수 없습니다. 자세한 내용은 아래의 "반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)"를 참조하십시오. 자세한 내용은 아래의 **반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)**을 참조하십시오.
- 22 X509\_V\_ERR\_CERT\_CHAIN\_TOO\_LONG 인증서 체인 길이가 제공된 최대 깊이보다 큼니다. 사용되지 않음.
- 23 X509\_V\_ERR\_CERT\_REVOKED 인증서가 해지되었습니다.
- 24 X509\_V\_ERR\_INVALID\_CA CA 인증서가 유효하지 않습니다. CA가 아니거나 확장명이 제공된 목적과 일치하지 않습니다.
- 25 X509\_V\_ERR\_PATH\_LENGTH\_EXCEEDED basicConstraints pathlength 매개변수가 초과되었습니다.
- 26 X509\_V\_ERR\_INVALID\_PURPOSE 제공된 인증서를 지정된 용도로 사용할 수 없습니다.
- 27 X509\_V\_ERR\_CERT\_UNTRUSTED 루트 CA가 지정된 용도로 신뢰할 수 있는 것으로 표시되지 않았습니다.
- 28 X509\_V\_ERR\_CERT\_REJECTED 루트 CA가 지정된 용도를 거부하도록 표시되었습니다.

29 X509\_V\_ERR\_SUBJECT\_ISSUER\_MISMATCH 해당 주체 이름이 현재 인증서의 발급자 이름과 일치하지 않아 현재 후보 발급자 인증서가 거부되었습니다. -issuer\_checks 옵션이 설정된 경우에만 표시됩니다.

30 X509\_V\_ERR\_AKID\_SKID\_MISMATCH 현재 후보 발급자 인증서가 거부되었습니다. 해당 주체 키 식별자가 있고 인증 기관 키 식별자가 현재 인증서와 일치하지 않기 때문입니다. -issuer\_checks 옵션이 설정된 경우에만 표시됩니다.

31 X509\_V\_ERR\_AKID\_ISSUER\_SERIAL\_MISMATCH 발급자 이름 및 일련 번호가 존재하고 현재 인증서의 기관 키 식별자와 일치하지 않으므로 현재 발급자 인증서가 거부되었습니다. -issuer\_checks 옵션이 설정된 경우에만 표시됩니다.

32 X509\_V\_ERR\_KEYUSAGE\_NO\_CERTSIGN keyUsage 확장이 인증서 서명을 허용하지 않으므로 현재 발급자 인증서가 거부되었습니다.

50 X509\_V\_ERR\_APPLICATION\_VERIFICATION 애플리케이션 관련 오류입니다. 사용되지 않음.

#### 새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 CDO는 **Configuration Status**(구성 상태) 및 **Connectivity**(연결성) 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. CDO에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.



**Note** 두 개 이상의 관리 디바이스를 동시에 CDO에 다시 **CDO에 디바이스 대량 다시 연결**하는 경우 CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

1. **Device & Services**(디바이스 및 서비스) 페이지로 이동합니다.
2. 필터를 사용하여 **New Certificate Detected**(새 인증서 탐지됨) 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.
3. Action(작업) 창에서 **Review Certificate**(인증서 검토)를 클릭합니다. CDO에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.
4. Device Sync(디바이스 동기화) 창에서 **Accept**(수락)를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue**(계속)를 클릭합니다.

CDO는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화되면 디바이스를 확인하려면 **Devices & Services**(디바이스 및 서비스) 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

#### 인증서 오류 코드

반환 코드 확인: **0 (ok)** 하지만 CDO에서 인증서 오류를 반환합니다.

CDO에 인증서가 있으면 "https://<device\_ip>:<port>"에 GET 호출을 하여 URL에 연결을 시도합니다. 그래도 문제가 해결되지 않으면 CDO에 인증서 오류가 표시됩니다. 인증서가 유효한 경우(openssl에서 0 ok 반환) 연결하려는 포트에서 다른 서비스가 수신 대기하는 문제일 수 있습니다. 다음 명령을 사용할 수 있습니다.

```
curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

ASA와 통신하고 있는지 확인하고 HTTPS 서버가 ASA의 올바른 포트에서 실행 중인지 확인합니다.

```
# show asp table socket
Protocol      Socket      State      Local Address      Foreign Address
SSL           00019b98    LISTEN     192.168.1.5:443    0.0.0.0:*
SSL           00029e18    LISTEN     192.168.2.5:443    0.0.0.0:*
TCP           00032208    LISTEN     192.168.1.5:22     0.0.0.0:*
```

**반환 코드 확인: 9(인증서가 아직 유효하지 않음)**

이 오류는 제공된 인증서의 발급 날짜가 미래이므로 클라이언트가 이를 유효한 것으로 처리하지 않음을 의미합니다. 이는 잘못 구성된 인증서로 인해 발생할 수 있으며, 자체 서명 인증서의 경우 인증서를 생성할 때 잘못된 디바이스 시간이 원인일 수 있습니다.

인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

이 오류를 통해 인증서가 유효한 시점을 확인할 수 있습니다.

치료

인증서의 notBefore 날짜는 과거여야 합니다. 이전 날짜의 인증서를 재발급할 수 있습니다. 이 문제는 클라이언트 또는 발급 디바이스에서 시간이 올바르게 설정되지 않은 경우에도 발생할 수 있습니다.

**반환 코드 확인: 10(인증서가 만료되었습니다)**

이 오류는 제공된 인증서 중 하나 이상이 만료되었음을 의미합니다. 인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
error 10 at 0 depth lookup:certificate has expired
```

만료 날짜는 인증서 본문에 있습니다.

치료

인증서가 실제로 만료된 경우 유일한 교정 방법은 다른 인증서를 가져오는 것입니다. 인증서의 만료 날짜가 아직 미래이지만 openssl이 만료되었다고 주장하는 경우, 컴퓨터의 시간과 날짜를 확인합니다. 예를 들어 인증서가 2020년에 만료되도록 설정되어 있지만 컴퓨터의 날짜가 2021년이면 컴퓨터는 해당 인증서를 만료된 것으로 처리합니다.

**반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)**

이 오류는 인증서 체인에 문제가 있음을 나타내며, `openssl`은 디바이스에서 제공하는 인증서를 신뢰할 수 있는지 확인할 수 없습니다. 인증서 체인이 작동하는 방식을 확인하려면 위의 예에서 인증서 체인을 살펴보겠습니다.

```

---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TyIimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqsMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTA1VT
....lots of base64...
tzw9TyIimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTA1VT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----

```

인증서 체인은 서버에서 제공하는 인증서 목록으로, 서버의 자체 인증서부터 시작하여 점점 더 높은 수준의 중간 인증서를 포함하여 서버의 인증서를 인증 기관의 최상위 인증서와 연결합니다. 각 인증서에는 해당 주체('로 시작하는 줄) 및 발급자('i'로 시작하는 줄)가 나열됩니다.

주체는 인증서로 식별되는 엔티티입니다. 여기에는 조직 이름이 포함되며 경우에 따라 인증서가 발급된 엔티티의 공용 이름이 포함됩니다.

발급자는 인증서를 발급한 엔티티입니다. 여기에는 **Organization**(조직) 필드도 포함되며, 경우에 따라 **Common Name**(일반 이름)도 포함됩니다.

서버에 신뢰할 수 있는 인증 기관에서 직접 발급한 인증서가 있는 경우 인증서 체인에 다른 인증서를 포함할 필요가 없습니다. 다음과 같은 인증서를 제공합니다.

```

--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TyIimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

```

이 인증서가 제공되면 `openssl`은 **\*.example.com**에 대한 **ExampleCo** 인증서가 신뢰할 수 있는 기관 인증서에 의해 올바르게 서명되었는지 확인합니다. 이 인증서는 `openssl`의 기본 제공 신뢰 저장소에 있습니다. 확인 후 `openssl`이 디바이스에 성공적으로 연결됩니다.

그러나 대부분의 서버에는 신뢰할 수 있는 **CA**에서 직접 서명한 인증서가 없습니다. 대신 첫 번째 예에서와 같이 서버의 인증서가 하나 이상의 중간 인증서에 의해 서명되고, 최상위 중간 인증서에는 신



되할 수 있는 CA가 서명한 인증서가 있습니다. OpenSSL은 기본적으로 이러한 중간 CA를 신뢰하지 않으며, 신뢰할 수 있는 CA로 끝나는 완전한 인증서 체인이 제공되는 경우에만 이를 확인할 수 있습니다.

중간 기관이 인증서에 서명한 서버는 모든 중간 인증서를 포함하여 이를 신뢰할 수 있는 CA에 연결하는 모든 인증서를 제공해야 합니다. 이 전체 체인을 제공하지 않는 경우 openssl의 출력은 다음과 같습니다.

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

이 출력은 서버가 하나의 인증서만 제공했으며 제공된 인증서가 신뢰할 수 있는 루트가 아닌 중간 기관에 의해 서명되었음을 보여줍니다. 출력에는 특성 확인 오류도 표시됩니다.

#### 치료

이 문제는 디바이스에서 제공하는 인증서가 잘못 구성되어 발생합니다. CDO 또는 다른 프로그램이 디바이스에 안전하게 연결할 수 있도록 이 문제를 해결하는 유일한 방법은 올바른 인증서 체인을 디바이스에 로드하여 연결하는 클라이언트에 완전한 인증서 체인을 제공하도록 하는 것입니다.

트러스트 포인트에 중간 CA를 포함하려면 아래 링크 중 하나를 따르십시오(CSR이 ASA에서 생성되었는지 여부에 따라).

- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13>
- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15>

## 새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 CDO는 **Configuration Status**(구성 상태) 및 **Connectivity**(연결성) 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. CDO에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.



**참고** 두 개 이상의 관리 디바이스를 CDO에 동시에 **CDO에 디바이스 대량 다시 연결**하는 경우, CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

#### 프로시저

- 단계 1** 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2** **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3** 해당 디바이스 탭을 클릭합니다.
- 단계 4** 필터를 사용하여 **New Certificate Detected**(새 인증서 탐지됨) 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.
- 단계 5** Action(작업) 창에서 **Review Certificate**(인증서 검토)를 클릭합니다. CDO에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.
- 단계 6** Device Sync(디바이스 동기화) 창에서 **Accept**(수락)를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue**(계속)를 클릭합니다.

CDO는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화되면 디바이스를 확인하려면 **Devices & Services**(디바이스 및 서비스) 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

## 온보딩 오류 문제 해결

디바이스 온보딩 오류는 여러 가지 이유로 발생할 수 있습니다.

다음과 같은 작업을 수행할 수 있습니다.

### Procedure

- 단계 1 **Inventory**(인벤토리) 페이지에서 **Devices**(장치) 탭을 클릭합니다.
- 단계 2 적절한 디바이스 유형 탭을 클릭하고 이 오류가 발생하는 디바이스를 선택합니다. 경우에 따라 오른쪽 쪽에 오류 설명이 표시됩니다. 설명에 언급된 필요한 조치를 취하십시오.  
또는
- 단계 3 CDO에서 디바이스 인스턴스를 제거하고 디바이스 온보딩을 다시 시도하십시오.

## "충돌 탐지됨" 상태 해결

CDO를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. [충돌 탐지, on page 629](#)이 활성화되어 있고 CDO를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected**(충돌 탐지됨)로 표시됩니다.

"충돌 탐지됨" 상태를 해결하려면 다음 절차를 수행합니다.

### Procedure

- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 해당 디바이스 탭을 클릭합니다.
- 단계 4 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict**(충돌 검토)를 클릭합니다.
- 단계 5 **Device Sync**(디바이스 동기화) 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.
  - "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 CDO에 저장된 디바이스 구성입니다.
  - "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.
- 단계 6 다음 중 하나를 선택하여 충돌을 해결합니다.

- **Accept Device changes**(디바이스 변경 사항 수락): 구성 및 **CDO**에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.

**Note** CDO는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 배포하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review**(검토 없이 수락)를 선택하는 것입니다.

- **Reject Device Changes**(디바이스 변경 거부): 디바이스에 저장된 구성을 CDO에 저장된 구성으로 덮어씁니다.

**Note** 거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

## "동기화되지 않음" 상태 해결

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

### Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.


단계 5 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- **미리보기 및 배포...** - CDO에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축**하거나 한 번에 여러 변경 사항을 기다렸다가 배포하십시오.
- **변경 사항 취소** - CDO에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 CDO에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 CDO에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

## 연결할 수 없는 연결 상태 문제 해결

다음과 같은 여러 가지 이유로 디바이스가 "접근 불가" 상태일 수 있습니다.

## Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 적절한 디바이스 유형 탭을 클릭하고 접근 불가 상태의 디바이스를 선택합니다.
- 단계 4  **Reconnect**(다시 연결)를 클릭합니다.
- 단계 5 오른쪽에 나타나는 메시지에 따라 다음 작업 중 하나를 수행합니다.
- a. IP 주소 및 디바이스 자격 증명을 사용하여 FDM 관리 디바이스를 온보딩한 경우 다음 메시지가 나타납니다.
 

"이 디바이스에 연결할 수 없습니다. IP 주소와 포트를 검토하십시오," 메시지 상자에 디바이스의 새 IP 주소 및/또는 새 포트 정보를 입력하십시오. CDO가 잘못된 IP 주소에 연결을 시도했기 때문에 디바이스의 IP 주소가 디바이스에서 직접 변경되었을 수 있습니다.

**Note** 디바이스가 재부팅되고 보류 중인 다른 변경 사항이 없는 경우 디바이스는 온라인 연결 상태로 돌아가야 하며 추가 작업이 필요하지 않습니다.

이제 디바이스가 "Online(온라인)"이지만 구성 상태가 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. **구성 충돌 해결**를 사용하여 CDO와 디바이스 간의 구성 차이를 검토합니다.
  - b. 등록 토큰 또는 일련 번호를 사용하여 FDM 관리 디바이스를 온보딩하는 경우 다음 메시지가 나타납니다.
 

"디바이스가 Cisco Cloud에서 삭제되었습니다. RMA(Return Material Authorization) 프로세스의 일부로 삭제될 수 있습니다." RMA 팀에 반환한 결함 있는 디바이스가 RMA 프로세스의 일부로 Cisco Cloud에서 삭제되었음을 의미합니다.

결과적으로 디바이스 연결 상태가 CDO에서 "연결할 수 없음"임을 알 수 있습니다.

    - RMA 케이스의 경우 CDO에서 다음 단계를 수행해야 합니다.
      1. 디바이스가 성공적으로 온보딩된 경우 디바이스 구성을 템플릿으로 저장해야 합니다. **FDM 템플릿 구성**을 참조하십시오.  
CDO에서 디바이스 인스턴스를 삭제합니다.
      2. RMA 팀에서 받은 새 교체 디바이스의 전원을 켜고 CDO에 온보딩합니다. **디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩**을 참조하십시오.  
**Important** 교체 디바이스의 일련 번호가 다를 수 있으며 새 디바이스로 온보딩해야 합니다.  
이제 디바이스가 "온라인"이지만 구성 상태는 "충돌 감지됨"임을 알 수 있습니다.
      3. **구성 충돌 해결**를 사용하여 CDO와 디바이스 간의 구성 차이를 검토합니다.  
이전에 저장한 템플릿을 새 디바이스에 적용합니다. **FDM 템플릿 적용**을 참조하십시오.
    - 디바이스 구성을 지우지 않고 디바이스를 판매하거나 소유권을 테넌트 외부의 다른 사용자에게 양도한 경우 더 이상 디바이스를 소유하지 않습니다. 이 오류는 구매자가 디바이스의

이미지를 다시 만들 때 발생합니다. 디바이스가 올바르게 구성되고 이전에 동기화된 경우 디바이스 구성을 템플릿으로 저장한 다음 CDO에서 디바이스 인스턴스를 제거할 수 있습니다.

## SecureX 문제 해결

SecureX와 함께 CDO를 사용하려고 시도하는 동안 오류, 경고 및 문제가 발생할 수 있습니다. SecureX UI에 표시되는 문제의 경우 SecureX 설명서를 사용해야 합니다. 자세한 내용은 [SecureX 지원](#)을 참조하십시오.

CDO 내의 SecureX 리본 기능 또는 SecureX 리본에 대한 테넌트 액세스 가능성에 대한 사례를 열려면 [Cisco Defense Orchestrator 지원팀에 문의](#)에서 자세한 내용을 참조하십시오. 테넌트 ID를 제공하라는 요청을 받을 수 있습니다.

### SecureX UI 문제 해결

**SecureX** 대시보드에 중복된 **CDO** 모듈이 표시됩니다.

SecureX에서 단일 제품의 여러 모듈을 수동으로 구성할 수 있습니다. 예를 들어 여러 CDO 테넌트가 있는 경우 테넌트당 하나의 CDO 모듈을 생성할 수 있습니다. 중복 모듈은 동일한 CDO 테넌트에서 두 개의 개별 API 토큰이 있음을 의미합니다. 이러한 중복은 혼란을 야기하고 대시보드를 복잡하게 만들 수 있습니다.

SecureX에서 CDO 모듈을 수동으로 구성한 다음 CDO의 일반 설정 페이지에서 **SecureX** 연결을 선택한 경우 이로 인해 하나의 테넌트가 SecureX에 여러 모듈을 가질 수 있습니다.

이 문제를 해결하려면 SecureX에서 원래 CDO 모듈을 제거하고 중복 모듈로 CDO 성능을 계속 모니터링하는 것이 좋습니다. 이 모듈은 더 안전하고 SecureX 리본과 호환되는 더 강력한 API 토큰으로 생성됩니다.

### CDO UI 문제 해결

SecureX 내의 CDO 모듈에 대한 사례를 열려면 [SecureX 약관](#), [개인 정보 보호](#), [지원](#)의 지원 섹션에서 자세한 내용을 참조하십시오.

### OAuth 오류

다음 메시지와 함께 OAuth 오류가 발생할 수 있습니다. "사용자가 필요한 모든 범위 또는 충분한 권한을 가지고 있지 않은 것 같습니다." 이 문제가 발생하면 다음 가능성을 고려하십시오.

- 계정이 활성화되지 않았을 수 있습니다. <https://visibility.test.iroh.site/>에서 등록된 이메일 주소를 사용하여 계정이 활성화되었는지 확인합니다. 계정이 활성화되지 않은 경우 CDO 테넌트가 SecureX와 병합되지 않을 수 있습니다. 이 문제를 해결하려면 Cisco TAC에 문의해야 합니다. 자세한 내용은 [Cisco Defense Orchestrator 지원팀에 문의](#)를 참조하십시오.

잘못된 조직 자격 증명으로 **SecureX**에 로그인했습니다.

일반 설정 페이지의 테넌트 설정 섹션에 있는 **Connect SecureX** 옵션을 사용하여 CDO 이벤트를 SecureX로 보내기로 선택했지만 잘못된 자격 증명을 사용하여 SecureX에 로그인한 경우, 잘못된 테넌트의 이벤트가 SecureX 대시보드에 표시될 수 있습니다.

이 문제를 해결하려면 CDO의 일반 설정 페이지에서 **SecureX** 연결 끊기를 클릭합니다. 이렇게 하면 SecureX 조직과 정보를 주고 받는 데 사용되는 읽기 전용 API 사용자가 종료되고 결과적으로 SecureX 대시보드가 종료됩니다.

그런 다음 **Connect Tenant to SecureX**를 다시 활성화하고 SecureX에 로그인하라는 메시지가 표시되면 올바른 조직 로그인 자격 증명을 사용해야 합니다.

잘못된 계정으로 리본에 로그인했습니다.

이때 잘못된 계정 정보로 리본에 로그인하면 리본에서 로그아웃할 수 없습니다. 리본 로그인을 수동으로 재설정하려면 [Support Case Manager](#)에서 사례를 열어야 합니다.

**SecureX** 리본을 실행할 수 없습니다.

적절한 범위에 대한 액세스 권한이 없을 수 있습니다. 이 문제를 해결하려면 Cisco TAC에 문의해야 합니다. 자세한 내용은 [Cisco Defense Orchestrator 지원팀에 문의](#)를 참조하십시오.

SecureX 리본 작동 방식에 대한 자세한 내용은 [SecureX 리본 설명서](#)를 참조하십시오.







## 8 장

# FAQ 및 지원

이 장에는 다음 섹션이 포함되어 있습니다.

- [Cisco Defense Orchestrator, on page 819](#)
- [Cisco Defense Orchestrator에 디바이스 온보딩 관련 FAQ, 820 페이지](#)
- [디바이스 유형, on page 822](#)
- [보안, on page 823](#)
- [문제 해결, on page 825](#)
- [로우 터치\(Low-Touch\) 프로비저닝에 사용되는 용어 및 정의, on page 825](#)
- [정책 최적화, on page 826](#)
- [연결성, on page 826](#)
- [CLI를 사용하여 Secure Firewall Threat Defense 디바이스의 초기 구성 완료, on page 827](#)
- [데이터 인터페이스 정보, 831 페이지](#)
- [CDO가 개인 정보를 처리하는 방법, 831 페이지](#)
- [Cisco Defense Orchestrator 지원팀에 문의, on page 831](#)

## Cisco Defense Orchestrator

**Cisco Defense Orchestrator**란 무엇입니까?

Cisco CDO(Defense Orchestrator)는 네트워크 관리자가 다양한 보안 디바이스에서 일관된 보안 정책을 만들고 유지할 수 있도록 하는 클라우드 기반 다중 디바이스 관리자입니다.

CDO를 사용하여 다음 디바이스를 관리할 수 있습니다.

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Cloud Native
- Cisco Umbrella
- Meraki
- Cisco IOS 디바이스

- 아마존 웹 서비스(AWS) 인스턴스
- SSH 연결을 사용하여 관리되는 디바이스

CDO 관리자는 단일 인터페이스를 통해 이러한 모든 디바이스 유형을 모니터링하고 유지할 수 있습니다.

## Cisco Defense Orchestrator에 디바이스 온보딩 관련 FAQ

### CDO에 Secure Firewall ASA 온보딩 관련 FAQ

자격 증명을 사용하여 어떻게 ASA를 온보딩합니까?

ASA를 한 번에 하나씩 온보딩하거나 대량 작업으로 온보딩할 수 있습니다. 고가용성 쌍의 일부인 ASA를 온보딩하는 경우 쌍의 기본 디바이스만 온보딩하는 데 [ASA 디바이스 온보딩](#)을 사용합니다. 보안 상황 또는 관리 상황을 온보딩하는 방법은 다른 ASA를 온보딩하는 방법과 동일합니다.

한 번에 하나 이상의 ASA를 온보딩하려면 어떻게 해야 합니까?

CSV 파일을 사용하여 ASA 목록을 생성할 수 있으며, CDO는 목록의 모든 ASA를 온보딩합니다. 대량 ASA 온보딩에 대한 지침은 [대량 ASA 온보드](#)를 참조하십시오.

ASA를 온보딩한 후 무엇을 해야 합니까?

시작하려면 [Cisco Defense Orchestrator](#)로 [ASA 관리](#)를 참조하십시오.

### CDO에 FDM 매니지드 디바이스 온보딩 관련 FAQ

FDM 매니지드 디바이스를 온보딩하려면 어떻게 해야 합니까?

FDM 매니지드 디바이스를 온보딩하는 다양한 방법이 있습니다. 등록 키 방법을 사용하는 것이 좋습니다. 시작하려면 [FDM 매니지드 디바이스 온보딩](#)을 참조하십시오.

## 클라우드사용 FirewallManagementCenter에 SecureFirewallThreatDefense 온보딩 관련 FAQ

Secure Firewall Threat Defense를 온보딩하려면 어떻게 합니까?

CLI 등록 키, 로우 터치 프로비저닝 또는 일련 번호를 사용하여 FTD 디바이스를 온보딩할 수 있습니다.

**Secure Firewall Threat Defense**를 온보딩한 후에는 어떻게 해야 하나요?

디바이스가 동기화되면 Tools & Services(툴 및 서비스) - Firewall Management Center로 이동하여 Actions(작업), Management(관리) 또는 Settings(설정) 창에서 작업을 선택하여 클라우드 제공 Firewall Management Center에서 위협 방어 디바이스의 구성을 시작합니다. 시작하려면 [클라우드 사용 Firewall Management Center 애플리케이션 페이지](#)를 참조하십시오.

**Secure Firewall Threat Defense** 문제를 어떻게 해결하나요?

[Secure Firewall Threat Defense 온보딩 문제 해결](#)을 참조하십시오.

## 온프레미스 Secure Firewall Management Center 관련 FAQ

**온프레미스 Management Center**를 온보딩하려면 어떻게 하나요?

온프레미스 Management Center를 CDO에 온보딩할 수 있습니다. 온프레미스 Management Center를 온보딩하면 온프레미스 Management Center에 등록된 모든 디바이스도 온보딩됩니다. CDO는 온프레미스 Management Center 또는 온프레미스 Management Center에 등록된 디바이스와 연결된 개체 또는 정책의 생성이나 수정을 지원하지 않습니다. 온프레미스 Management Center UI에서 이러한 변경을 수행해야 합니다. 시작하려면 [온프레미스 Management Center 온보딩](#)을 참조하십시오.

## CDO에 Meraki 디바이스 온보딩 관련 FAQ

**Meraki** 디바이스를 온보딩하려면 어떻게 해야 하나요?

MX 디바이스는 CDO와 Meraki 대시보드에서 모두 관리할 수 있습니다. CDO는 구성 변경 사항을 Meraki 대시보드에 구축하며, 그러면 구성이 디바이스에 안전하게 구축됩니다. 시작하려면 [Meraki MX 디바이스 온보딩](#)을 참조하십시오.

## CDO에 SSH 디바이스 온보딩 관련 FAQ

**SSH** 디바이스를 어떻게 온보딩하나요?

SSH 디바이스에 저장된 높은 권한을 가진 사용자의 사용자 이름과 암호를 사용하여 SDC(보안 디바이스 커넥터)로 디바이스를 온보딩할 수 있습니다. 시작하려면 [SSH 디바이스 온보딩](#)을 참조하십시오.

## 디바이스를 삭제하려면 어떻게 하나요?

재고 목록 페이지에서 디바이스를 삭제할 수 있습니다.

## CDO에 IOS 디바이스 온보딩 관련 FAQ

### Cisco IOS 디바이스를 어떻게 온보딩합니까?

SDC(보안 디바이스 커넥터)를 사용하여 Cisco IOS(Internetwork Operating System)를 실행하는 라이브 Cisco 디바이스를 온보딩할 수 있습니다. 시작하려면 [Cisco IOS 디바이스 온보딩](#)을 참조하십시오.

### 디바이스를 삭제하려면 어떻게 합니까?

Inventory(재고 목록) 페이지에서 디바이스를 삭제할 수 있습니다.

## 디바이스 유형

### ASA(Adaptive Security Appliance)란 무엇입니까?

Cisco ASA에서는 고급 스테이트풀 방화벽 및 VPN 집선 디바이스 기능을 하나의 디바이스에서 제공하며 애드온 모듈과 통합된 서비스를 제공합니다. ASA에는 다중 보안 상황(가상 방화벽과 유사), 클러스터링(다중 방화벽을 단일 방화벽으로 통합), 투명(Layer 2) 방화벽 또는 라우팅(Layer 3) 방화벽 가동, 고급 검사 엔진, IPsec VPN, SSL VPN 및 클라이언트리스 SSL VPN 지원 등의 다양한 기능이 포함되어 있습니다. ASA는 가상 머신 또는 지원되는 하드웨어에 설치할 수 있습니다.

### ASA 모델이란 무엇입니까?

ASA 모델은 CDO에 온보딩한 ASA 디바이스의 실행 중인 구성 파일의 사본입니다. ASA 모델을 사용하여 디바이스 자체를 온보딩하지 않고도 ASA 디바이스의 구성을 분석할 수 있습니다.

### FTD(Firepower Threat Defense)란 무엇입니까?

Cisco의 차세대 방화벽 소프트웨어 이미지. 최고의 Sourcefire 차세대 방화벽 서비스와 ASA 플랫폼을 결합하기 위해 노력합니다. 다양한 Firepower 하드웨어 디바이스 또는 가상 머신에 설치할 수 있습니다. 이것은 ASA FirePOWER 모듈과 동일하지 않습니다. 자세한 내용은 [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 참조하십시오.

### FDM(Firepower Device Manager)이란 무엇입니까?

Firepower Device Manager는 FTD 이미지와 함께 제공되는 Firepower Threat Defense 관리 소프트웨어입니다. FDM은 함께 제공되는 하나의 FTD를 관리하도록 설계되었습니다. FDM을 "로컬 디바이스 관리자"라고 부르기도 합니다.

### Firepower란 무엇입니까?

Firepower는 차세대 방화벽 하드웨어 및 소프트웨어 그룹을 나타내는 일반적인 용어입니다.

### 디바이스는 언제 동기화됩니까?

CDO의 구성과 디바이스에 로컬로 저장된 구성이 동일한 경우.

디바이스가 언제 동기화되지 않습니까?

CDO에 저장된 구성이 변경되어 이제 디바이스에 로컬로 저장된 구성과 다른 경우.

디바이스가 충돌 감지 상태인 경우는 언제입니까?

디바이스의 구성이 CDO(대역 외) 외부에서 변경되어 이제 CDO에 저장된 구성과 다른 경우.

**OOB(out-of-band) 변경이란 무엇입니까?**

CDO 외부에서 디바이스가 변경된 경우, CLI 명령을 사용하거나 ASDM 또는 FDM과 같은 온디바이스 관리자를 사용하여 디바이스에서 직접 변경합니다. 대역 외 변경으로 인해 CDO는 디바이스에 대해 "충돌 감지" 상태를 보고합니다.

디바이스에 변경 사항을 배포한다는 것은 무엇을 의미합니까?

디바이스를 CDO에 등록한 후 CDO는 해당 구성의 복사본을 유지 관리합니다. CDO를 변경하면 CDO는 디바이스 구성의 사본을 변경합니다. 변경 사항을 디바이스에 다시 "배포"하면 CDO는 디바이스의 구성 복사본에 대한 변경 사항을 복사합니다. 다음 항목을 참조하십시오.

- [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 620](#)
- [CDO에서 FDM-관리 디바이스로 구성 변경 사항 구축](#)

현재 지원되는 **ASA** 명령은 무엇입니까?

모든 명령 디바이스 활동 아래에 **Command Line Interface**(명령줄 인터페이스)를 클릭하여 ASA CLI를 사용합니다.

디바이스 관리에 대한 규모 제한이 있습니까?

CDO의 클라우드 아키텍처를 통해 수천 개의 디바이스로 확장할 수 있습니다.

**CDO는 Cisco Integrated Services Routers 및 Aggregation Services Routers를 관리합니까?**

CDO를 사용하면 ISR 및 ASR에 대한 모델 디바이스를 생성하고 해당 구성을 가져올 수 있습니다. 그런 다음 가져온 구성을 기반으로 템플릿을 생성하고 일관된 보안을 위해 신규 또는 기존 ISR 및 ASR 디바이스에 배포할 수 있는 표준화된 구성으로 구성을 내보낼 수 있습니다.

**CDO가 SMA를 관리할 수 있습니까?**

아니오, CDO는 현재 SMA를 관리하지 않습니다.

## 보안

**CDO는 안전한가요?**

CDO는 다음 기능을 통해 고객 데이터에 대한 엔드 투 엔드 보안을 제공합니다.

- 새 CDO 테넌트에 대한 초기 로그인, on page 40
- API 및 데이터베이스 작업에 대한 인증 호출
- 이동 중 및 유휴 상태의 데이터 격리
- 역할 분리

CDO는 사용자가 클라우드 포털에 연결할 때 다단계 인증을 요구합니다. 다단계 인증은 고객의 신원을 보호하는 데 필요한 필수 기능입니다.

이동 중이거나 유휴 상태의 모든 데이터는 암호화됩니다. 고객 프리미엄 및 CDO의 디바이스와의 통신은 SSL로 암호화되며 모든 고객 테넌트 데이터 볼륨은 암호화됩니다.

CDO의 다중 테넌트 아키텍처는 테넌트 데이터를 격리하고 데이터베이스와 애플리케이션 서버 간의 트래픽을 암호화합니다. 사용자가 CDO에 액세스하기 위해 인증하면 토큰을 받습니다. 이 토큰은 키 관리 서비스에서 키를 가져오는 데 사용되며 키는 데이터베이스에 대한 트래픽을 암호화하는 데 사용됩니다.

CDO는 고객 자격 증명을 보호하면서 신속하게 고객에게 가치를 제공합니다. 이는 자격 증명 데이터가 고객 프리미엄을 떠나지 않도록 모든 인바운드 및 아웃바운드 트래픽을 제어하는 클라우드 또는 고객 자체 네트워크(로드맵)에 "보안 데이터 커넥터"를 배포하여 달성됩니다.

**CDO에 처음 로그인할 때 "OTP를 확인할 수 없음" 오류가 발생했습니다.**

데스크톱 또는 모바일 디바이스 시계가 세계 시간 서버와 동기화되어 있는지 확인합니다. 시계가 1분 미만 또는 그 이상 동기화되지 않으면 잘못된 OTP가 생성될 수 있습니다.

디바이스가 **Cisco Defense Orchestrator** 클라우드 플랫폼에 직접 연결되어 있습니까?

예. 보안 연결은 디바이스와 CDO 플랫폼 간의 프록시로 사용되는 CDO SDC를 사용하여 수행됩니다. 보안을 최우선으로 고려하여 설계된 CDO 아키텍처를 사용하면, 디바이스를 오가는 데이터를 완전히 분리할 수 있습니다.

공용 IP 주소가 없는 디바이스를 어떻게 연결할 수 있습니까?

네트워크 내에 배포할 수 있고 외부 포트를 열 필요가 없는 SDC(Secure Device Connector)를 활용할 수 있습니다. SDC가 배포되면 내부(인터넷 라우팅 불가) IP 주소로 디바이스를 온보딩할 수 있습니다.

**SDC에 추가 비용이나 라이선스가 필요합니까?**

아니요.

현재 CDO에서 어떤 유형의 VPN(가상 프라이빗망)이 지원됩니까?

ASA 고객의 경우, CDO는 IPsec 사이트 투 사이트 VPN 터널 관리만 지원합니다. What's New 페이지의 업데이트를 계속 지켜봐 주십시오.

터널 상태를 어떻게 확인할 수 있습니까? 상태 옵션

CDO는 매시간 터널 연결 확인을 자동으로 수행하지만, 터널을 선택하고 연결 확인을 요청하여 임시 VPN 터널 연결 확인을 수행할 수 있습니다. 결과를 처리하는 데 몇 초가 걸릴 수 있습니다.

디바이스 이름과 피어 중 하나의 IP 주소를 기반으로 터널을 검색할 수 있습니까?

예. 이름과 피어 IP 주소 모두에서 사용 가능한 필터 및 검색 기능을 사용하여 특정 VPN 터널 세부 정보를 검색하고 피벗합니다.

## 문제 해결

**CDO**에서 관리 디바이스로 디바이스 구성을 완전히 배포하는 동안 "변경 사항을 디바이스에 배포할 수 없습니다"라는 경고가 표시됩니다. 해결하려면 어떻게 해야 하나요?

전체 구성(CDO 지원 명령 이상으로 수행된 변경 사항)을 디바이스에 배포할 때 오류가 발생하면 "변경 사항 확인"을 클릭하여 디바이스에서 사용 가능한 최신 구성을 가져옵니다. 이렇게 하면 문제가 해결될 수 있으며 계속해서 CDO를 변경하고 배포할 수 있습니다. 문제가 지속되면 **Contact Support**(지원 문의) 페이지에서 Cisco TAC에 문의하십시오.

대역 외 문제(CDO 외부에서 수행된 변경, 디바이스에 직접 변경)를 해결하는 동안 CDO에 있는 구성과 디바이스의 구성을 비교하는 동안 CDO는 내가 추가하거나 편집하지 않은 추가 메타데이터를 제공합니다. 왜 그럴까요?

CDO가 기능을 확장함에 따라 더 나은 정책 및 디바이스 관리 분석을 위해 필요한 모든 데이터를 강화하고 유지하기 위해 디바이스 구성에서 추가 정보가 수집됩니다. 이는 관리되는 디바이스에서 발생한 변경 사항이 아니라 이미 존재하는 정보입니다. 충돌 감지 상태를 해결하는 것은 디바이스에서 변경 사항을 확인하고 발생한 변경 사항을 검토하여 쉽게 해결할 수 있습니다.

**CDO**가 내 인증서를 거부하는 이유는 무엇입니까?

[새 인증서 문제 트러블슈팅](#)을 참조하십시오.

## 로우 터치(Low-Touch) 프로비저닝에 사용되는 용어 및 정의

- 클레임됨 - CDO에서 일련 번호 온보딩의 컨텍스트에서 사용됩니다. 일련 번호가 CDO 테넌트에 온보딩된 경우 디바이스가 "클레임"됩니다.
- 파킹됨 - CDO에서 일련 번호 온보딩의 컨텍스트에서 사용됩니다. Cisco Cloud에 연결되어 있고 CDO 테넌트가 일련 번호를 요청하지 않은 경우 디바이스는 "파킹"됩니다.
- 초기 프로비저닝 - 초기 FTD 설정의 컨텍스트에서 사용됩니다. 이 단계에서 디바이스는 EULA를 수락하고, 새 비밀번호를 생성하고, 관리 IP 주소를 구성하고, FQDN을 설정하고, DNS 서버를 설정하고, FDM을 사용하여 디바이스를 로컬로 관리하도록 선택합니다.

- 로우 터치(**Low-touch**) 프로비저닝 - 공장에서 고객 사이트(일반적으로 브랜치 오피스)로 FTD를 배송하고, 사이트의 직원이 FTD를 네트워크에 연결하고, 디바이스가 Cisco Cloud에 연결하는 프로세스입니다. 이 시점에서 일련 번호가 이미 "클레임"되었거나 CDO 테넌트가 클레임할 때까지 FTD가 Cisco Cloud에 "파킹"된 경우 디바이스는 CDO 테넌트에 온보딩됩니다.
- 일련 번호 온보딩 - 이미 구성(설치 및 설정)된 일련 번호를 사용하여 FTD를 온보딩하는 프로세스입니다.

## 정책 최적화

두 개 이상의 액세스 목록(동일한 액세스 그룹 내)이 서로 새도잉되는 경우를 어떻게 식별할 수 있습니까?

Cisco Defense Orchestrator NPM(네트워크 정책 관리)은 규칙 세트 내에서 상위 규칙이 다른 규칙을 가리고 있는지 식별하고 사용자에게 경고할 수 있습니다. 사용자는 모든 네트워크 정책 사이를 탐색하거나 필터링하여 모든 새도우 문제를 식별할 수 있습니다.



**Note** CDO는 완전히 새도우 규칙만 지원합니다.

## 연결성

보안 장치 커넥터가 IP 주소를 변경했지만 **CDO**에 반영되지 않았습니다. 변경 사항을 반영하려면 어떻게 해야 합니까?

CDO 내에서 새로운 SDC(Secure Device Connector)를 얻고 업데이트하려면 다음 명령을 사용하여 컨테이너를 다시 시작해야 합니다.

```
Stop Docker daemon>#service docker stop
Change IP address
Start Docker daemon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$ ./cdo/toolkit/toolkit.sh restartSDC
<tenant-name>
```

내 장치(**FTD** 또는 **ASA**)를 관리하기 위해 **CDO**에서 사용하는 IP 주소가 변경되면 어떻게 됩니까?

정적 IP 주소의 변경이든 DHCP로 인한 IP 주소의 변경이든 어떤 이유로든 장치의 IP 주소가 변경되면, CDO가 장치에 연결하는 데 사용하는 IP 주소를 변경할 수 있습니다(참조 [CDO에서 디바이스의 IP 주소 변경](#), on page 90). 그런 다음 장치를 다시 연결합니다(참조 [CDO에 디바이스 대량 다시 연결](#), on page 96). 장치를 다시 연결할 때 장치의 새 IP 주소를 입력하고 인증 자격 증명을 다시 입력하라는 메시지가 표시됩니다.

내 **ASA**를 **CDO**에 연결하려면 어떤 네트워킹이 필요합니까?

- ASDM 이미지가 있고 ASA에 대해 활성화되어 있습니다.



- 52.25.109.29, 52.34.234.2, 52.36.70.147에 대한 공용 인터페이스 액세스
- ASA의 HTTPS 포트는 443 또는 1024 이상의 값으로 설정해야 합니다. 예를 들어 포트 636으로 설정할 수 없습니다.
- 관리 중인 ASA도 AnyConnect VPN 클라이언트 연결을 허용하도록 구성된 경우 ASA HTTPS 포트를 1024 이상의 값으로 변경해야 합니다.

## CLI를 사용하여 Secure Firewall Threat Defense 디바이스의 초기 구성 완료

디바이스의 CLI에 연결하여 설정 마법사를 사용하여 관리 IP 주소, 게이트웨이 및 기타 기본 네트워크 설정을 포함한 초기 설정을 수행합니다. 통신을 위해 모든 DNS 및 방화벽 포트에 액세스할 수 있는지 확인합니다.

전용 관리 인터페이스는 자체 네트워크 설정이 있는 특수 인터페이스입니다. 관리 인터페이스를 사용하지 않으려는 경우, 대신 CLI를 사용하여 데이터 인터페이스를 구성할 수 있습니다.

### Before you begin

이 절차는 다음 시나리오에 적용됩니다.

- Firepower 1000, Firepower 2100, Secure Firewall 3100 및 ISA 3000 모델이 해당됩니다.
- 이 구성은 CLI 등록 키로 온보딩될 디바이스에 이상적입니다.



**Note** 로우터치 프로비저닝으로 온보딩 중인 디바이스에는 이 구성 절차를 사용하지 마십시오.

### Procedure

**단계 1** 콘솔 포트에서 또는 관리 인터페이스에 대한 SSH를 사용하여 디바이스의 CLI에 연결합니다. 네트워크 설정을 변경하려는 경우 연결이 끊어지지 않도록 콘솔 포트를 사용하는 것이 좋습니다.

Firepower 1000, Firepower 2100, Secure Firewall 3100 모델: 콘솔 포트는 FXOS CLI에 연결됩니다. SSH 세션은 threat defense CLI에 직접 연결됩니다.

**단계 2** 사용자 이름 **admin** 및 비밀번호 **Admin123**로 로그인합니다.

(Firepower 및 Secure Firewall 하드웨어 모델) 콘솔 포트에서 FXOS CLI에 연결합니다. FXOS에 처음 로그인하면 암호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 threat defense 로그인에도 사용됩니다.

**Note** 비밀번호가 이미 변경된 경우 모르는 경우, 비밀번호를 기본값으로 재설정하려면 디바이스를 재 이미지화해야 합니다. Firepower 및 Secure Firewall 하드웨어 모델의 경우: [이미지 재설치 절차에 대한 FXOS 문제 해결 가이드](#)를 참고하십시오.

**Example:**

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

**단계 3** (Firepower 및 Secure Firewall 하드웨어 모델) 콘솔 포트에서 FXOS에 연결한 경우 threat defense CLI에 연결합니다.

**connect ftd****Example:**

```
firepower# connect ftd
>
```

**단계 4** 디바이스에 처음 로그인할 경우, 엔드 유저 라이선스 계약(EULA)에 동의하고 SSH 연결을 사용 중인 경우 관리자 비밀번호를 변경하라는 메시지가 표시됩니다. 그 다음에는 CLI 설정 스크립트가 표시됩니다.

**Note** 이미지 재설치 등을 통해 컨피그레이션을 지우지 않으면 CLI 설정 마법사를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network**(네트워크 구성) 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. [threat defense 명령 참조](#)를 참조하십시오.

기본값 또는 이전에 입력한 값이 괄호 안에 표시됩니다. 이전에 입력한 값을 승인하려면 **Enter**를 누릅니다.

**Note** 관리 인터페이스 설정은 데이터 인터페이스에서 threat defense 액세스를 활성화한 경우에도 사용됩니다. 예를 들어 데이터 인터페이스를 통해 백플레인으로 라우팅되는 관리 트래픽은 데이터 인터페이스 DNS 서버가 아닌 관리 인터페이스 DNS 서버를 사용하여 FQDN을 확인합니다.

다음 지침을 참조하십시오.

- **Configure IPv4 via DHCP or manually?(DHCP를 통해 또는 수동으로 IPv4를 구성하시겠습니까?)** - 관리 인터페이스 대신 threat defense 액세스용 데이터 인터페이스를 사용하려면 **manual**(수동)을 선택합니다. 관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다. 관리 인터페이스가 DHCP로 설정된 경우 관리를 위해 데이터 인터페이스를 설정할 수 없습니다. 데이터 인터페이스(데이터 인터페이스)여야 하는 기본 경로(다음 글머리 기호 참조)가 DHCP 서버에서 수신한 기본 경로를 덮어 쓸 수 있기 때문입니다.

- **Enter the IPv4 default gateway for the management interface**(관리 인터페이스에 대한 IPv4 기본 게이트웨이 입력) - 관리 인터페이스 대신 threat defense 액세스에 데이터 인터페이스를 사용하려면 게이트웨이를 **data-interfaces** 데이터 인터페이스(데이터 인터페이스)로 설정합니다. 이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 FMC 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다.
- **If your networking information has changed, you will need to reconnect**(네트워킹 정보가 변경된 경우 다시 연결해야 합니다) — SSH를 통해 연결되어 있지만 최초 설정에서 IP 주소를 변경한 경우 연결이 끊깁니다. 새 IP 주소 및 비밀번호를 사용하여 다시 연결합니다. 콘솔 연결에는 영향을 미치지 않습니다.
- 디바이스를 로컬로 관리하시겠습니까? - 클라우드 사용 Firewall Management Center 또는 Secure Firewall device manager에서 관리할 디바이스에 대해 디바이스를 구성하려면 예를 입력합니다.  
디바이스를 로컬로 관리하시겠습니까? - 온프레미스 Management Center에서 원격 관리를 위해 디바이스를 구성하려면 아니오를 입력합니다.
- **Configure firewall mode?**(방화벽 모드를 설정하시겠습니까?)—초기 설정에서 방화벽 모드를 설정하는 것이 좋습니다. 초기 설정 후에 방화벽 모드를 변경하면 실행 중인 구성이 지워집니다. 데이터 인터페이스 threat defense 액세스는 라우팅 방화벽 모드에서만 지원됩니다.

단계 5 (Optional) management center 액세스 인터페이스의 이름을 구성합니다.

#### configure network management-data-interface

그러면 데이터 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

**Note** 이 명령을 사용할 때는 콘솔 포트를 사용해야 합니다. 관리 인터페이스에 SSH를 사용하는 경우 연결이 끊기고 콘솔 포트에 다시 연결해야 할 수 있습니다. SSH 사용량에 대한 자세한 내용은 아래를 참조하십시오.

이 명령 사용에 대한 자세한 내용은 다음을 참조하십시오. 자세한 내용은 [데이터 인터페이스 정보, on page 831](#)의 내용을 참조하십시오.

- 관리에 데이터 인터페이스를 사용하려는 경우 원래 관리 인터페이스에서 DHCP를 사용할 수 없습니다. 초기 설정 중에 IP 주소를 수동으로 설정하지 않은 경우 지금 **configure network {ipv4 | ipv6} manual** 명령을 사용하여 설정할 수 있습니다. 관리 인터페이스 게이트웨이를 아직 **data-interfaces**로 설정하지 않은 경우, 이 명령이 이제 설정합니다.
- Cisco Defense Orchestrator를 통해 위협 방어 관리를 위해 디바이스에 온보딩하면 Cisco Defense Orchestrator는 인터페이스 이름과 IP 주소, 게이트웨이에 대한 정적 경로, DNS 서버 및 DDNS 서버 설정을 포함하여 인터페이스 구성을 검색하고 유지 관리합니다. DNS 서버 설정에 관한 자세한 내용은 아래를 참조하십시오. 나중에 액세스 인터페이스 구성을 변경할 수 있지만, 디바이스 또는 Cisco Defense Orchestrator가 관리 연결을 재설정하지 못하게 할 수 있는 변경은 수행하지 않아야 합니다. 관리 연결이 중단되면 디바이스에 이전 구축을 복구하는 **configure policy rollback** 명령이 포함됩니다.
- 이 명령은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 스크립트로 설정하거나 **configure network dns servers** 명령을 사용하여 설정한 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다.

또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 유지됩니다. 예를 들어 관리 인터페이스를 사용하여 디바이스를 등록한 다음 나중에 **configure network management-data-interface** 명령을 사용하여 데이터 인터페이스를 구성하는 경우 디바이스 구성과 일치하도록 DNS 서버를 포함하여 CDO에서 이러한 모든 설정을 수동으로 구성해야 합니다.

- Threat Defense를 통해 위협 방어 관리용 **threat defense**를 온보딩한 후 관리 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.
- 설정 마법사에서 설정한 FQDN이 이 인터페이스에 사용됩니다.
- 명령의 일부로 전체 디바이스 구성을 지울 수 있습니다. 복구 시나리오에서는 이 옵션을 사용할 수 있지만 초기 설정 또는 정상 작동에는 이 옵션을 사용하지 않는 것이 좋습니다.
- 데이터 관리를 비활성화하려면 **configure network management-data-interface disable** 명령을 입력합니다.

### Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

>

### Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

>

단계 6 (Optional) 특정 네트워크에서 Cisco Defense Orchestrator에 대한 데이터 인터페이스 액세스를 제한합니다.

**configure network management-data-interface client ip\_address netmask**

기본적으로 모든 네트워크가 허용됩니다.

## 데이터 인터페이스 정보

디바이스와의 통신에 전용 관리 인터페이스 또는 일반 데이터 인터페이스를 사용할 수 있습니다. 외부 인터페이스에서 원격으로 FTD를 관리하려는 경우 또는 별도의 관리 네트워크가 없는 경우 데이터 인터페이스의 액세스가 유용합니다.

데이터 인터페이스에서의 FTD 관리 액세스에는 다음과 같은 제한이 있습니다.

- 하나의 물리적 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.

## CDO가 개인 정보를 처리하는 방법

Cisco Defense Orchestrator가 개인 식별 정보를 처리하는 방법을 알아보려면 [Cisco Defense Orchestrator 프라이버시 데이터 시트](#)를 참조하십시오.

## Cisco Defense Orchestrator 지원팀에 문의

이 장에는 다음 섹션이 포함되어 있습니다.

### 워크플로우 내보내기

지원 티켓을 열기 전에 경험 문제가 있는 디바이스의 워크플로우를 내보내는 것이 좋습니다. 이 추가 정보는 지원 팀이 문제 해결 노력을 신속하게 식별하고 편집하는 데 도움이 될 수 있습니다.

워크플로우를 내보내려면 다음 절차를 따르십시오.

프로시저

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 문제 해결이 필요한 디바이스를 선택합니다.

필터 또는 검색 표시줄을 사용하여 문제를 해결해야 하는 디바이스를 찾으십시오. 디바이스를 선택하여 강조 표시합니다.

단계 4 **Device Actions**(장치 작업) 창에서 **Workflows**(워크플로우)를 선택합니다.

단계 5 이벤트 표 위의 페이지 오른쪽 상단에 있는 **Export**(내보내기) 버튼을 클릭합니다. 파일은 자동으로 로컬에 **.json** 파일로 저장됩니다. TAC로 여는 이메일이나 티켓에 이것을 첨부하십시오.

## TAC를 사용하여 지원 티켓 열기

30일 평가판 또는 라이선스가 부여된 CDO 계정을 사용하는 고객은 Cisco TAC(Technical Assistance Center)에서 지원 티켓을 열 수 있습니다.

- CDO 고객이 TAC로 지원 티켓을 여는 방법
- CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법

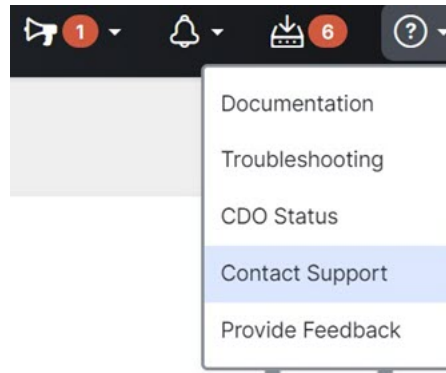
## CDO 고객이 TAC로 지원 티켓을 여는 방법

이 섹션에서는 라이선스가 부여된 CDO 테넌트를 사용하는 고객이 Cisco의 TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법을 설명합니다.

### Procedure

단계 1 CDO에 로그인합니다.

단계 2 테넌트 이름 옆에 있는 help(도움말) 버튼을 클릭하고 **Contact Support**(지원 문의)를 선택합니다.



단계 3 지원 케이스 관리자를 클릭합니다.

단계 4 파란색 **Open New Case**(새 케이스 열기) 버튼을 클릭합니다.

단계 5 **Open a Case**(케이스 열기)를 클릭합니다.

단계 6 **Products and Services**(제품 및 서비스)를 선택한 다음 **Open Case**(케이스 열기)를 클릭합니다.

단계 7 **Request Type**(요청 유형)을 선택합니다.

단계 8 **Find Product by Service Agreement**(서비스 계약별 제품 찾기) 행을 확장합니다.

단계 9 모든 필드를 입력합니다. 많은 필드가 명확합니다. 다음은 몇 가지 추가 정보입니다.

- **Product Name**(제품 이름) (**PID**) - 이 번호가 더 이상 없는 경우 [Cisco Defense Orchestrator 데이터 시트](#)를 참조하십시오.
- **Product Description**(제품 설명) - PID에 대한 설명입니다.
- **Site Name**(사이트 이름) - 사이트 이름을 입력합니다. 고객 중 한 명의 케이스를 여는 Cisco 파트너인 경우 고객의 이름을 입력합니다.
- **Service Contract**(서비스 계약) - 서비스 계약 번호를 입력합니다.
  - 중요: 케이스를 Cisco.com 어카운트와 연결하려면 계약 번호를 Cisco.com 프로파일에 연결해야 합니다. 이 절차를 사용하여 계약 번호를 Cisco.com 프로파일에 연결합니다.
    - a. [Cisco Profile Manager](#)를 엽니다.
    - b. **Access Management**(액세스 관리) 탭을 클릭합니다.
    - c. **Add Access**(액세스 추가)를 클릭합니다.
    - d. **TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com**(TAC 및 RMA 케이스 생성, 소프트웨어 다운로드, 지원 툴, Cisco.com의 엔터프라이즈 콘텐츠)를 선택하고 **Go**(이동)를 클릭합니다.
    - e. 제공된 공간에 서비스 계약 번호를 입력하고 **Submit**(제출)을 클릭합니다. 서비스 계약 연결이 완료되었다는 알림이 이메일로 전송됩니다. 서비스 계약 연결을 완료하는 데 최대 6시간이 걸릴 수 있습니다.

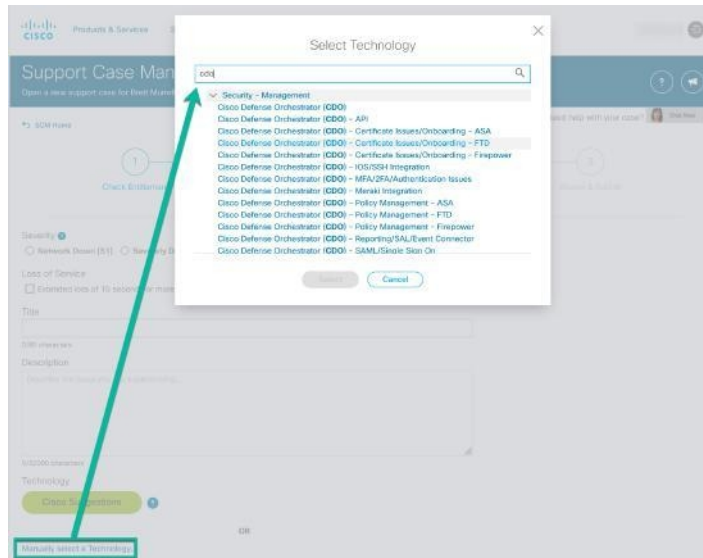
**Important** 중요: 아래 링크에 액세스할 수 없는 경우 공인 Cisco 파트너 또는 리셀러, Cisco 어카운트 담당자 또는 Cisco 서비스 계약 정보를 관리하는 회사 내 담당자에게 문의하십시오.

## CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법

단계 10 **Next**(다음)를 클릭합니다.

단계 11 **Describe Problem**(문제 설명) 화면에서 아래로 스크롤하여 **Manually select a Technology**(수동으로 기술 선택)를 클릭하고 검색 필드에 **CDO**를 입력합니다.

단계 12 요청과 가장 일치하는 범주를 선택하고 **Select**(선택)를 클릭합니다.



단계 13 서비스 요청의 나머지 부분을 완료하고 **Submit**(제출)을 클릭합니다.

## CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법

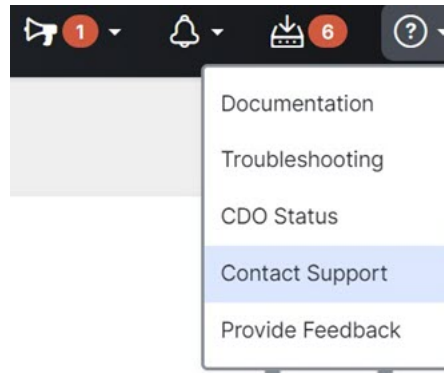
이 섹션에서는 CDO 테넌트의 무료 평가판을 사용하는 고객이 Cisco TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법에 대해 설명합니다.

### 프로시저

단계 1 CDO에 로그인합니다.

단계 2 테넌트 및 계정 이름 옆에 있는 **help**(도움말) 버튼을 클릭하고 **Contact Support**(지원 문의)를 선택합니다.





단계 3 아래에 문제 또는 요청 입력 필드에서 직면한 문제 또는 요청을 지정하고 **Submit(제출)**를 클릭합니다.

기술 정보와 함께 귀하의 요청이 지원 팀으로 전송되고 기술 지원 엔지니어가 귀하의 질문에 응답합니다.

## CDO 서비스 상태 페이지

CDO는 CDO 서비스가 작동 중이고 서비스 중단이 있었는지 여부를 보여주는 고객 대면 서비스 상태 페이지를 유지 관리합니다. 일별, 주별 또는 월별 그래프로 가동 시간 정보를 볼 수 있습니다.

CDO의 모든 페이지에 있는 도움말 메뉴에서 **CDO Status(CDO 상태)**를 클릭하면 CDO 상태 페이지에 도달할 수 있습니다.

상태 페이지에서 **Subscribe to Updates(업데이트 구독)**을 클릭하면 CDO 서비스가 다운될 경우 알림을 받을 수 있습니다.



## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.