FMC 6.6.1+ - 업그레이드 전/후 팁

목차

소개

이 문서에서는 Cisco FMC(Secure Firewall Management Center)를 버전 6.6.1+으로 업그레이드하기 전후에 완료하기 위한 검증 및 구성 모범 사례에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 하드웨어: Cisco FMC 1000
- 소프트웨어: 릴리스 7.0.0(빌드 94)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

FMC 업그레이드 전에 해야 할 일

FMC 대상 소프트웨어 버전 선택

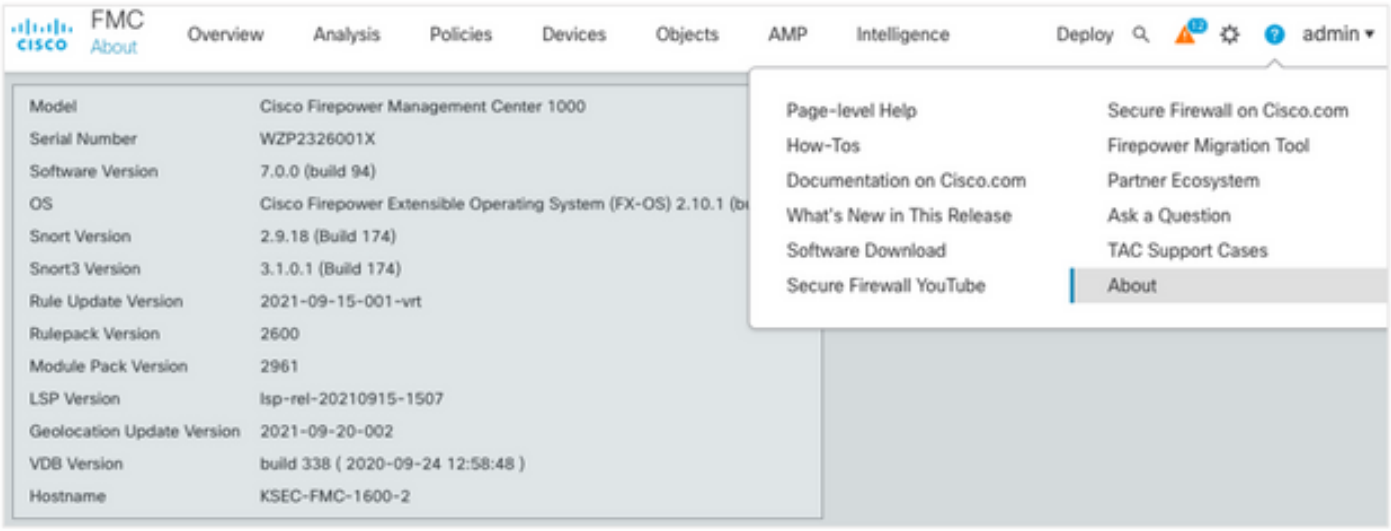
대상 버전에 대한 Firepower Release Notes를 검토하고 다음 사항을 숙지하십시오.

- 호환성
- 기능
- 해결된 문제
- 알려진 문제

현재 FMC 모델 및 소프트웨어 버전 확인

현재 FMC 모델 및 소프트웨어 버전을 확인합니다.

1. Help(**도움말**) > **About(정보)으로 이동합니다**.
2. **모델** 및 **소프트웨어 버전**을 **확인합니다**.



업그레이드 경로 계획

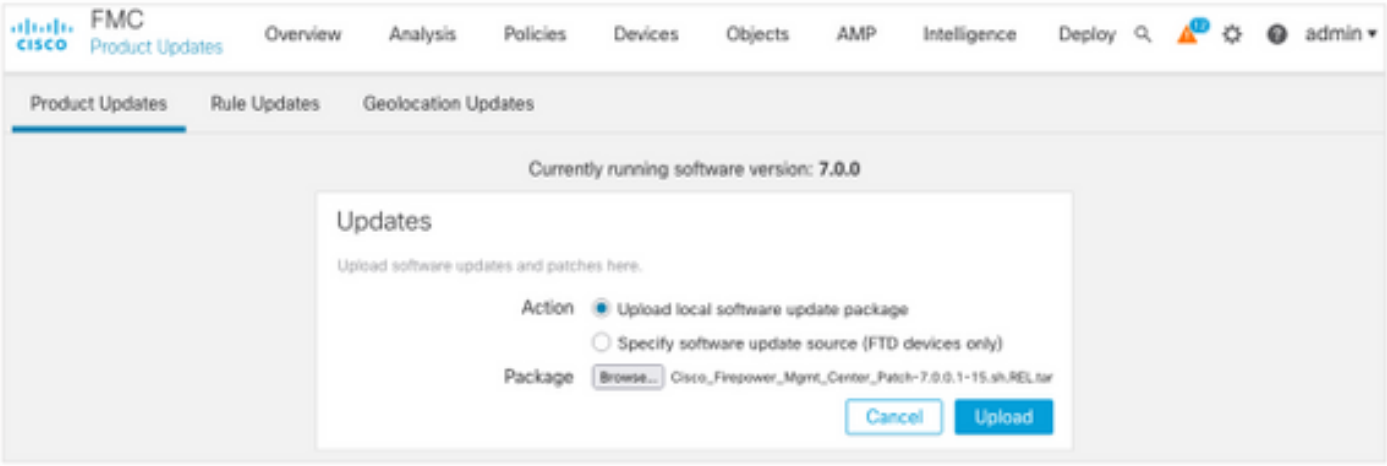
현재 및 대상 FMC 소프트웨어 버전에 따라 중간 업그레이드가 필요할 수 있습니다. Cisco

Firepower Management Center 업그레이드 가이드에서 **업그레이드 경로를 검토합니다. Firepower Management Centers** 섹션 및 업그레이드 경로를 계획합니다.

업그레이드 패키지 업로드

업그레이드 패키지를 디바이스에 업로드하려면 다음 단계를 완료하십시오.

1. 소프트웨어 다운로드 페이지에서 업그레이드 패키지를 다운로드합니다.
2. FMC에서 **System > Updates로 이동합니다**.
3. Upload **Update(업데이트 업로드)를 선택합니다**.
4. **Upload local software update package(로컬 소프트웨어 업데이트 패키지 업로드)** 라디오 버튼을 클릭합니다.
5. 찾아보기**를** 클릭하고 패키지를 선택합니다.
6. Upload(**업로드)를 클릭합니다**.

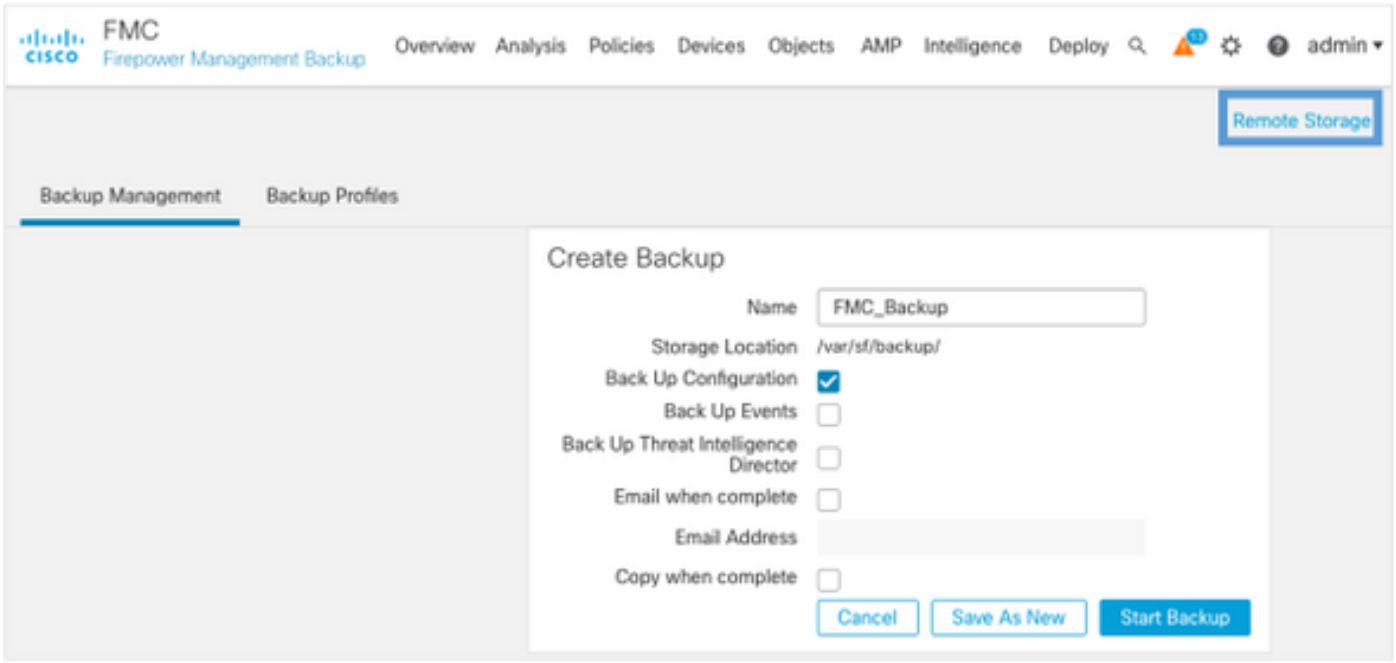


FMC 백업 생성

백업은 중요한 재해 복구 단계로서, 업그레이드에 중대한 장애가 발생할 경우 구성을 복원할 수 있습니다.

1. System(**시스템) > Tools(툴) > Backup/Restore(백업/복원)로 이동합니다**.
2. Firepower **Management Backup을 선택합니다**.
3. Name(**이름**) 필드에 백업 이름을 입력합니다.
4. 백업에 포함할 스토리지 위치 및 정보를 선택합니다.
5. Start **Backup(백업 시작)을 클릭합니다**.
6. Notification(**알림) > Tasks(작업)**에서 백업 생성 진행 상황을 모니터링합니다.

팁: 안전한 원격 위치에 백업하고 전송 성공을 확인하는 것이 좋습니다. 원격 스토리지는 백업 관리 페이지에서 구성할 수 있습니다.



자세한 내용은 다음을 참조하십시오.

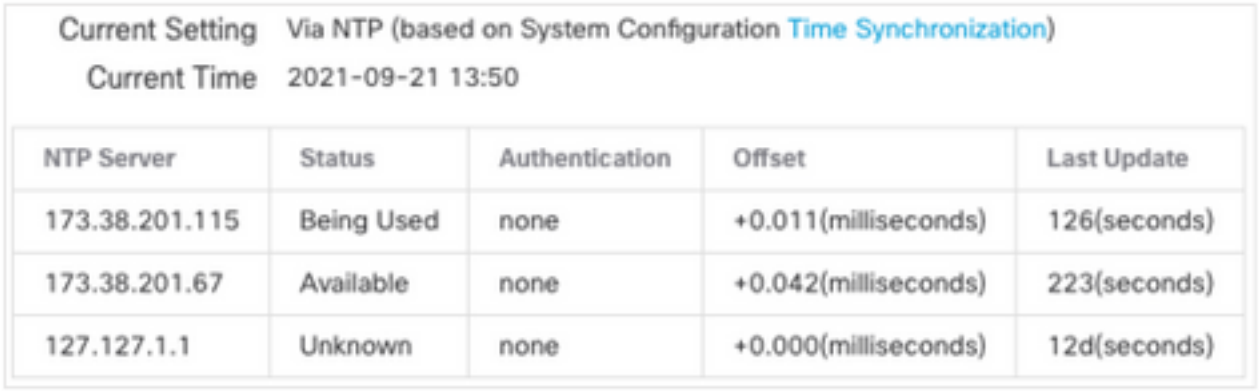
- Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 장: 백업 및 복원
- Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 원격 스토리지 관리

NTP 동기화 확인

성공적인 FMC 업그레이드를 위해서는 NTP 동기화가 필요합니다. NTP 동기화를 확인하려면 다음 단계를 완료하십시오.

1. System(**시스템) > Configuration(컨피그레이션) > Time(시간)으로 이동합니다**.
2. NTP **상태를 확인합니다**.

   참고: 상태: "사용 중"은 어플라이언스가 NTP 서버와 동기화되었음을 나타냅니다.

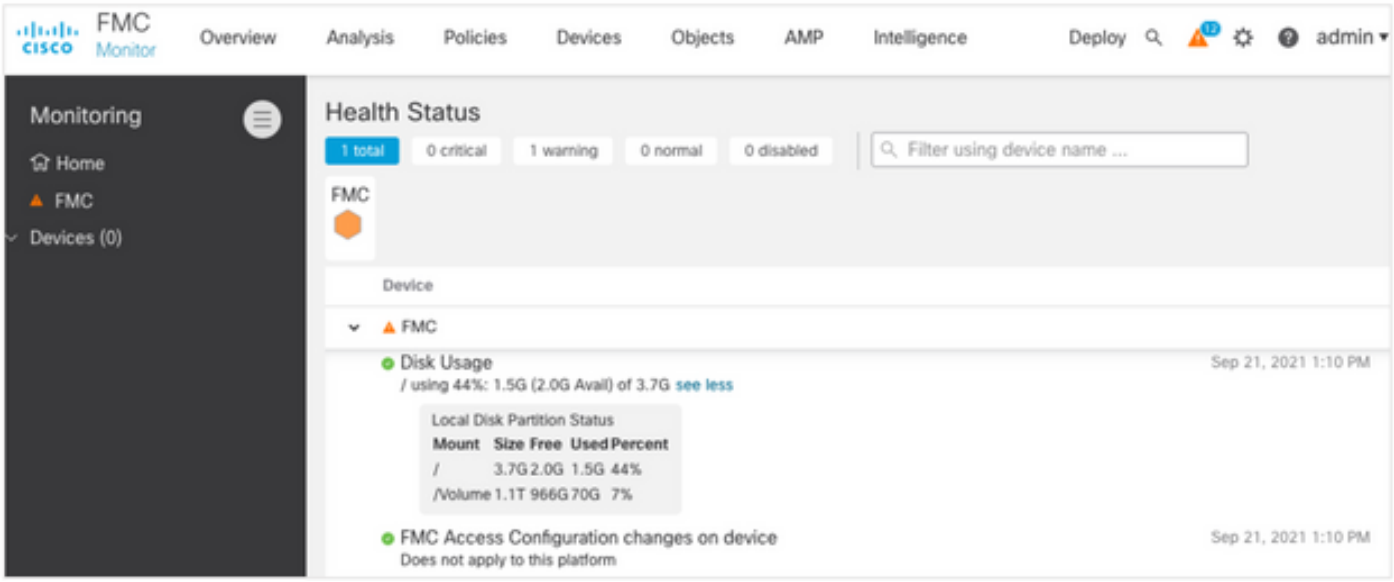


자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 시간 및 시간 동기화를 참조하십시오.

디스크 공간 확인

FMC 모델 및 대상 버전에 따라 사용 가능한 디스크 공간이 충분한지 확인하고, 그렇지 않으면 업그레이드가 실패합니다. 사용 가능한 FMC 디스크 공간을 확인하려면 다음 단계를 수행하십시오.

1. System(**시스템) > Health(상태) > Monitor(모니터)로 이동합니다**.
2. FMC를 선택합니다.
3. 메뉴를 확장하고 **디스크 사용량**을 **검색합니다**.
4. 디스크 공간 요구 사항은 시간 테스트 및 디스크 공간 요구 사항에서 확인할 수 있습니다.

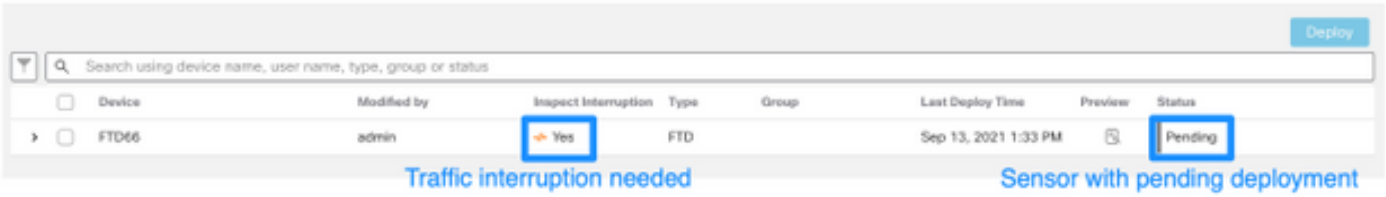


보류 중인 모든 정책 변경 사항 배포

업데이트 또는 패치 설치 전에 센서에 변경 사항을 구축해야 합니다. 보류 중인 모든 변경 사항이 배포되도록 하려면 다음 단계를 완료하십시오.

1. Deploy(구축) **> Deployment(구축)로 이동합니다**.
2. 목록에서 모든 디바이스를 선택하고 Deploy를 **선택합니다**.

   주의: Inspect Interference(검사 중단) 열은 트래픽 중단을 나타냅니다.

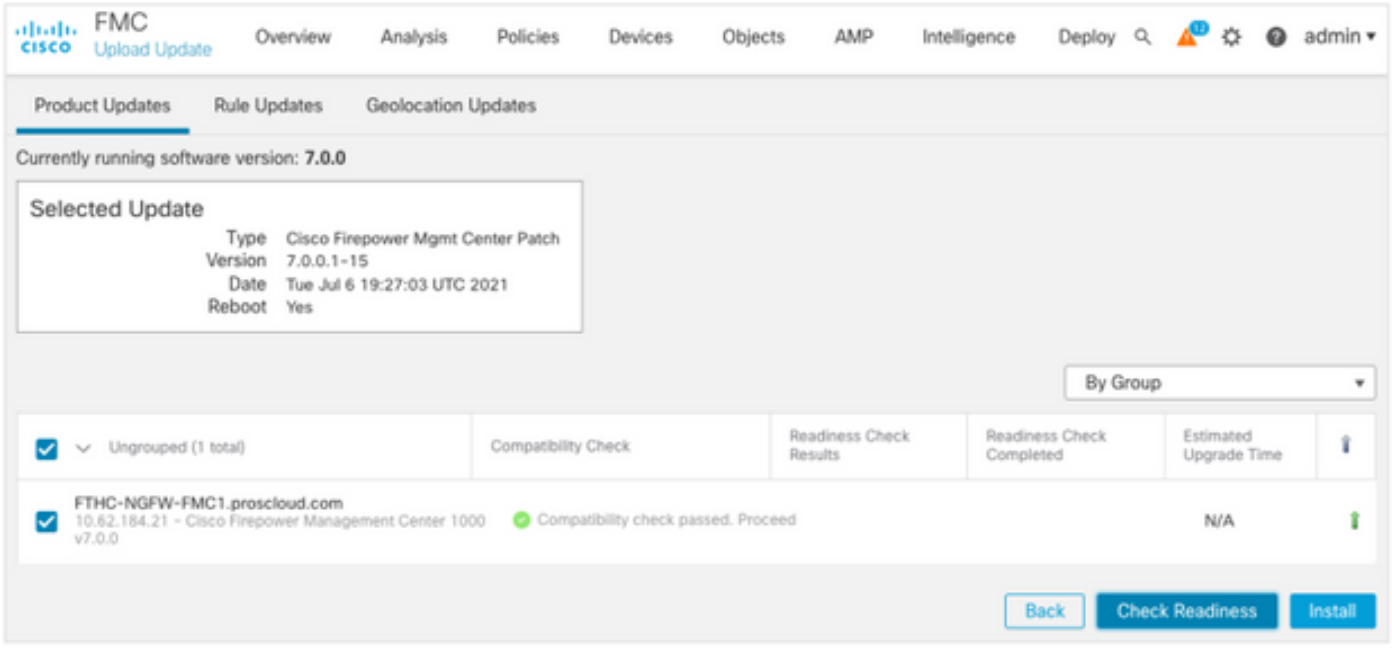


Firepower 소프트웨어 준비 검사 실행

준비도 검사는 소프트웨어 업그레이드를 위한 Firepower 어플라이언스의 준비 상태를 평가합니다.

소프트웨어 준비 검사를 수행하려면 다음 단계를 완료하십시오.

1. System(시스템) **> Updates(업데이트)로 이동합니다**.
2. 대상 버전 옆에 있는 **설치** 아이콘을 선택합니다.
3. FMC를 선택하고 Check Readiness를 **클릭합니다**.
4. 팝업 창에서 **확인**을 클릭합니다.
5. Notifications(알림) **> Tasks(작업)**에서 Readiness Check(준비 상태 확인) **프로세스를 모니터링합니다**.



자세한 내용은 Cisco Firepower Management Center 업그레이드 가이드 - Firepower Software 준비 상태 점검을 참조하십시오.

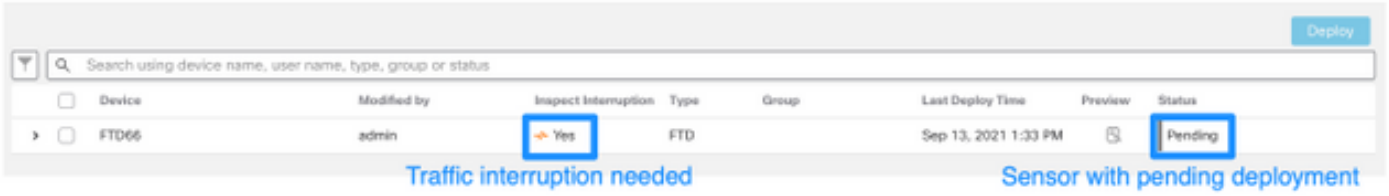
FMC 업그레이드 후 해야 할 최우선 사항

보류 중인 모든 정책 변경 사항 배포

모든 업데이트 또는 패치 설치 즉시 센서에 변경 사항을 구축해야 합니다. 보류 중인 모든 변경 사항이 배포되도록 하려면 다음 단계를 완료하십시오.

1. Deploy(구축) > **Deployment(구축)로 이동합니다**.
2. 목록에서 모든 디바이스를 선택하고 Deploy(구축)를 **클릭합니다**.

   주의: Inspect Interference(검사 중단) 열은 트래픽 중단을 나타냅니다.



최신 취약성 및 핑거프린트 데이터베이스가 설치되어 있는지 확인

현재 VDB(Fingerprint) 버전을 확인하려면 다음 단계를 수행하십시오.

1. Help(**도움말**) > **About(정보)으로 이동합니다**.
2. VDB 버전**을 확인합니다**.

cisco.com에서 직접 VDB 업데이트를 다운로드하려면 FMC에서 cisco.com으로 연결되어야 합니다.

1. System(**시스템**) > **Updates(업데이트)** > **Product Updates(제품 업데이트)로 이동합니다**.
2. Download **updates(업데이트 다운로드)를 선택합니다**.

3. 사용 가능한 최신 버전을 설치합니다.
4. 나중에 센서를 재구축해야 합니다.

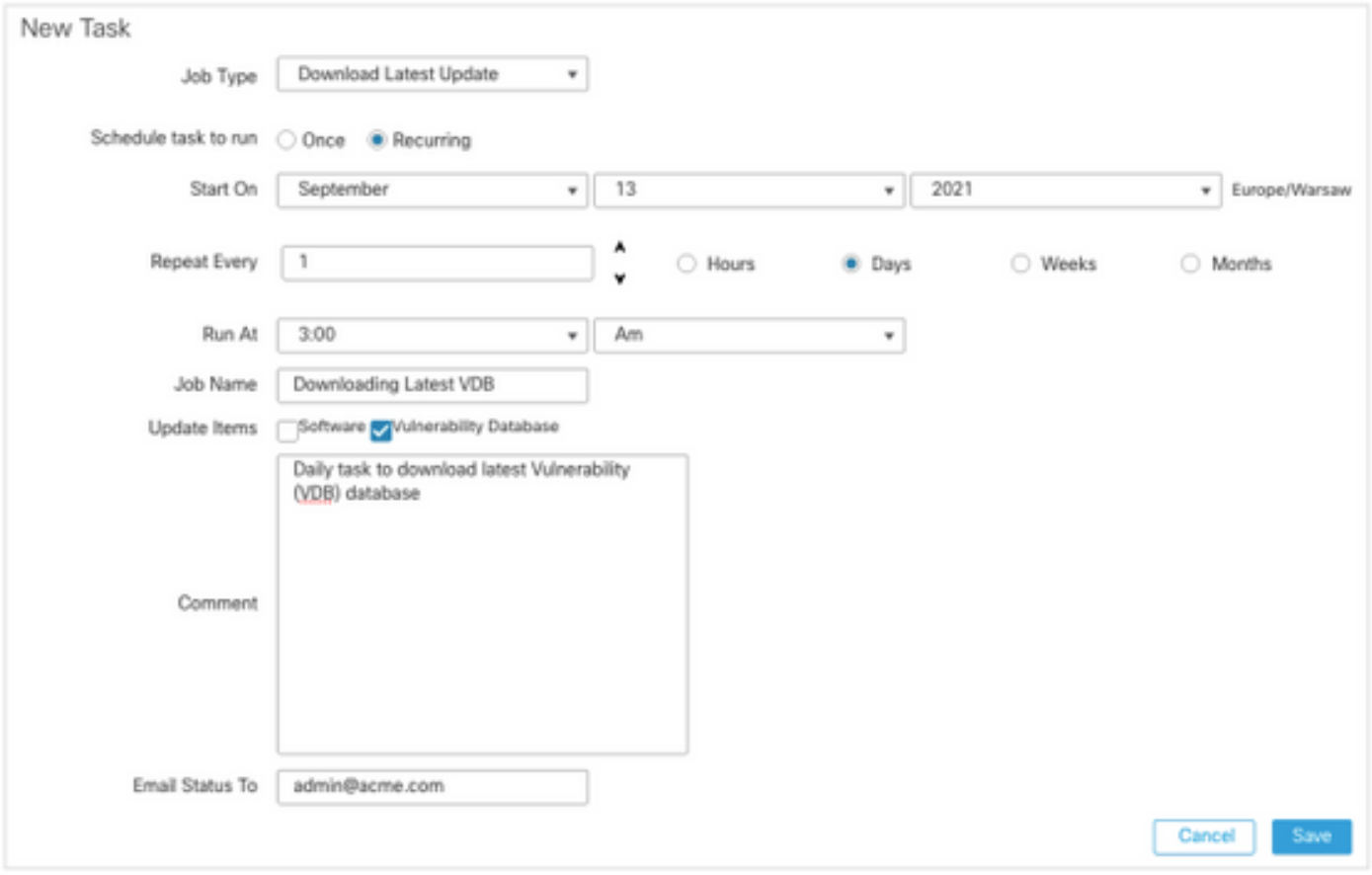
참고: FMC에 인터넷 액세스가 없으면 software.cisco.com에서 VDB 패키지를 직접 다운로드할 수 있습니다.

자동 VDB 패키지 다운로드 및 설치를 수행하도록 작업을 예약하는 것이 좋습니다.

모범 사례로서, VDB 업데이트를 매일 확인하고 주말에 FMC에 설치합니다.

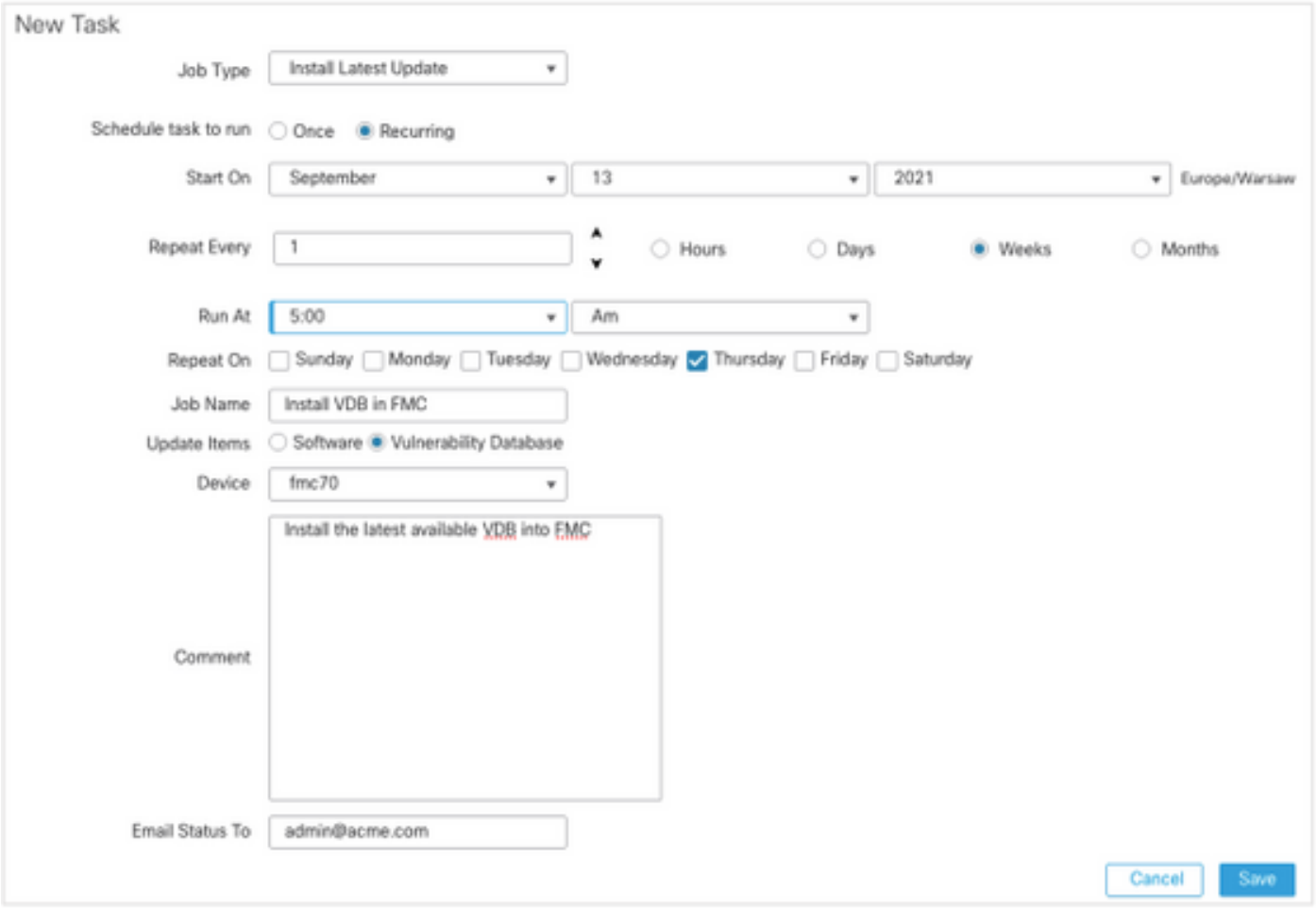
www.cisco.com에서 VDB를 매일 확인하려면 다음 단계를 완료하십시오.

1. System(시스템) **> Tools(툴) > Scheduling(예약)으로 이동합니다**.
2. 작업 **추가를 클릭합니다**.
3. Job **Type** 드롭다운 목록에서 Download Latest **Update(최신 업데이트 다운로드)를** 선택합니다**.**
4. Schedule **task to run(예약 작업**을 실행하려면 **Recurring(반복)** 라디오 버튼을 클릭합니다..
5. 매일 작업을 반복하고 오전 3시 또는 업무 시간 외 시간에 실행합니다.
6. Update **Items**의 경우 Vulnerability **Database** 확인란을 선택합니다..



FMC에 최신 VDB를 설치하려면 매주 정기 작업을 설정합니다.

1. System(시스템) **> Tools(툴) > Scheduling(예약)으로 이동합니다**.
2. 작업 **추가를 클릭합니다**.
3. Job **Type** 드롭다운 목록에서 Install Latest **Update(최신 업데이트 설치)를** 선택합니다.
4. Schedule **Task를 실행하려면 Recurring** 라디오 버튼을 클릭합니다.
5. 1주마다 작업을 반복하고 오전 5시 또는 업무 시간 외 시간에 실행합니다.
6. Update **Items**의 경우 Vulnerability **Database** 확인란을 선택합니다.



자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - VDB(Vulnerability Database) 업데이트를 참조하십시오.

Snort 규칙 및 경량 보안 패키지 현재 버전 확인

현재 SRU(Snort Rule), LSP(Lightweight Security Package) 및 지오로케이션 버전을 확인하려면 다음 단계를 완료하십시오.

1. Help(**도움말**) > **About(정보)으로 이동합니다**.
2. Rule **Update Version** 및 **LSP Version을 확인합니다**.

SRU 및 LSP를 www.cisco.com에서 직접 다운로드하려면 FMC에서 www.cisco.com로 연결할 수 있어야 합니다.

1. System(**시스템**) > **Updates(업데이트)** > **Rule Updates(규칙 업데이트)로 이동합니다**.
2. One-**Time Rule Update/Rules Import(일회성 규칙 업데이트/규칙 가져오기)** 탭에서 **Download new rule update from the Support Site(지원 사이트에서 새 규칙 업데이트 다운로드)**를 선택합니다.
3. 가져오기를 **선택합니다**.
4. 나중에 센서에 컨피그레이션을 구축합니다.

참고: FMC에 인터넷 액세스가 없으면 software.cisco.com에서 SRU 및 LSP 패키지를 직접 다운로드할 수 있습니다.

침입 규칙 업데이트는 누적되며 항상 최신 업데이트를 가져오는 것이 좋습니다.

SRU/LSP(Snort Rule Update)의 주간 다운로드 및 구축을 켜려면 다음 단계를 완료하십시오.

1. System(**시스템) > Updates(업데이트) > Rule Updates(규칙 업데이트)로 이동합니다**.
2. Recurring **Rule Update Imports** 탭에서 **Enable Recurring Rule Update Imports from the Support Site** 확인란을 선택합니다.
3. 가져오기 빈도를 주 단위로 선택하고 다운로드 및 정책 배포를 위해 요일 및 오후 늦게 선택합니다.
4. 저장을 **클릭합니다**.

자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 침입 규칙 업데이트를 참조하십시오.

지오로케이션 업데이트 현재 버전 확인

현재 지오로케이션 버전을 확인하려면 다음 단계를 완료하십시오.

1. Help(**도움말) > About(정보)으로 이동합니다**.
2. 지오로케이션 **업데이트 버전을 확인합니다**.

Geolocation Updates를 www.cisco.com에서 직접 다운로드하려면 FMC에서 www.cisco.com로 연결되어야 합니다.

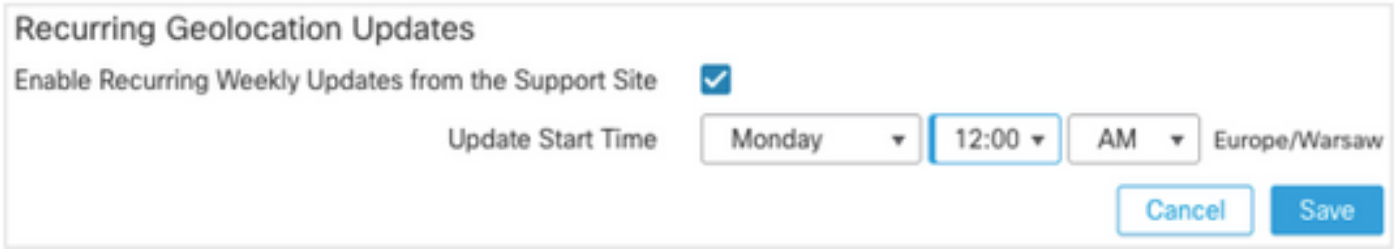
1. System(시스템) **> Updates(업데이트) > Geolocation Updates(지오로케이션 업데이트)로 이동합니다**.
2. One-**Time Geolocation Update(일회성 지오로케이션 업데이트**) 탭에서 **Download and install geolocation update from the Support Site(지원 사이트에서 지오로케이션 업데이트 다운로드 및 설치)를** 선택합니다.
3. 가져오기를 **클릭합니다**.

참고: FMC에 인터넷 액세스가 없는 경우 Geolocation Updates 패키지를 software.cisco.com에서 직접 다운로드할 수 있습니다.

자동 지오로케이션 업데이트를 켜려면 다음 단계를 완료하십시오.

1. System(시스템) **> Updates(업데이트) > Geolocation Updates(지오로케이션 업데이트)로 이동합니다**.
2. Recurring Geolocation Updates(반복 지오로케이션 업데이트) 섹션에서 **Enable Recurring Weekly Updates from the Support Site(지원 사이트에서 반복 주간 업데이트 활성화**) 확인란을 선택합니다.

3. 가져오기 빈도를 주 단위로 선택하고 월요일 자정을 선택합니다.
4. 저장을 **클릭합니다**.

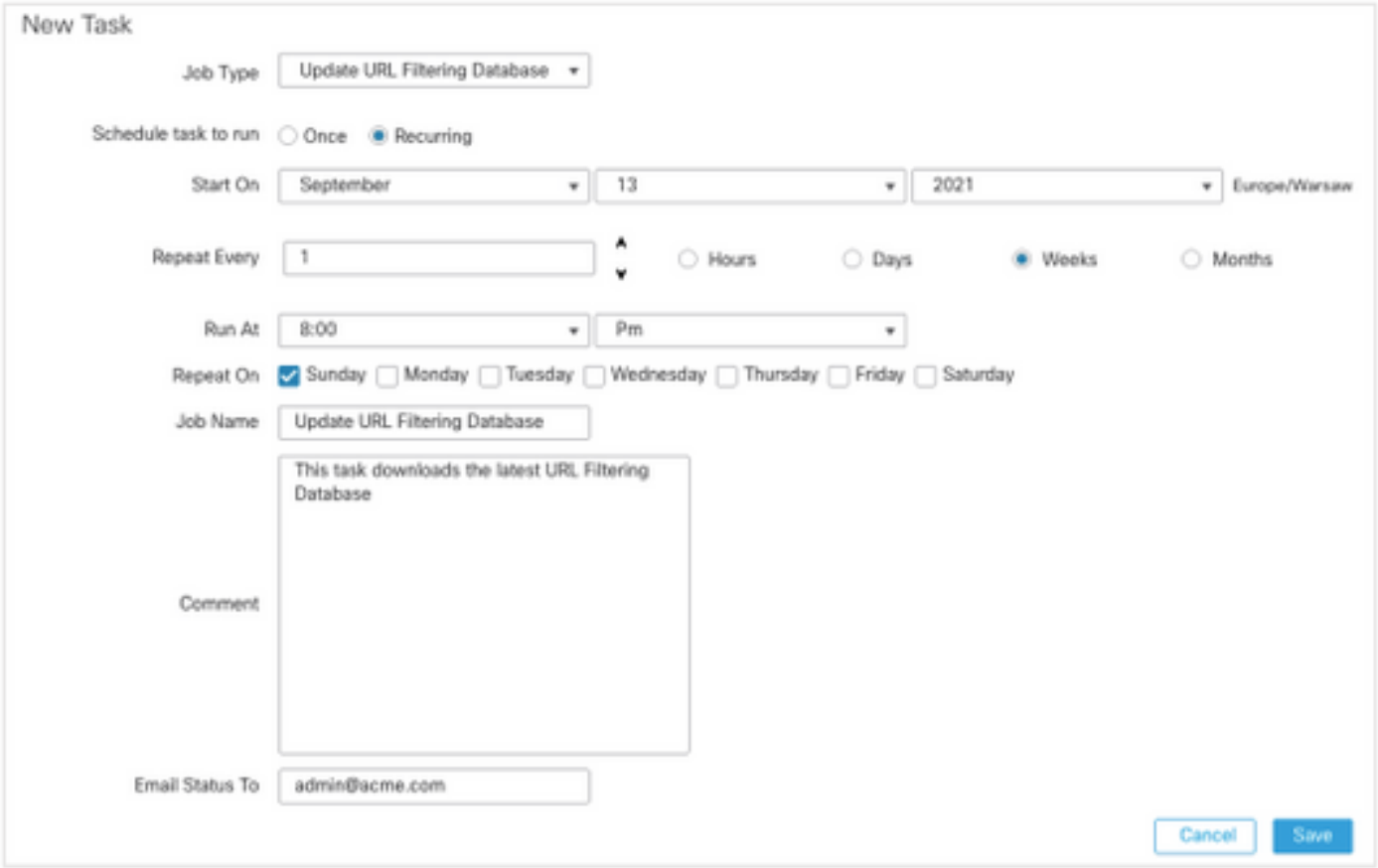


자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - GeoDB(Geolocation Database) 업데이트를 참조하십시오.

예약된 작업으로 URL 필터링 데이터베이스 업데이트 자동화

URL 필터링의 위협 데이터가 최신 상태인지 확인하기 위해 시스템은 Cisco CSI(Collective Security Intelligence) 클라우드에서 데이터 업데이트를 받아야 합니다. 이 프로세스를 자동화하려면 다음 단계를 수행하십시오.

1. System(시스템) **> Tools(툴) > Scheduling(예약)으로 이동합니다**.
2. 작업 **추가를 클릭합니다**.
3. **Job Type** 드롭다운 목록에서 **Update URL Filtering Database**를 선택합니다.
4. Schedule **task to run**(**예약 작업**을 실행하려면 **Recurring** 라디오 버튼을 클릭합니다.
5. 매주 작업을 반복한 다음 일요일 오후 8시 또는 업무 시간 외 시간에 실행합니다.
6. 저장을 **클릭합니다**.

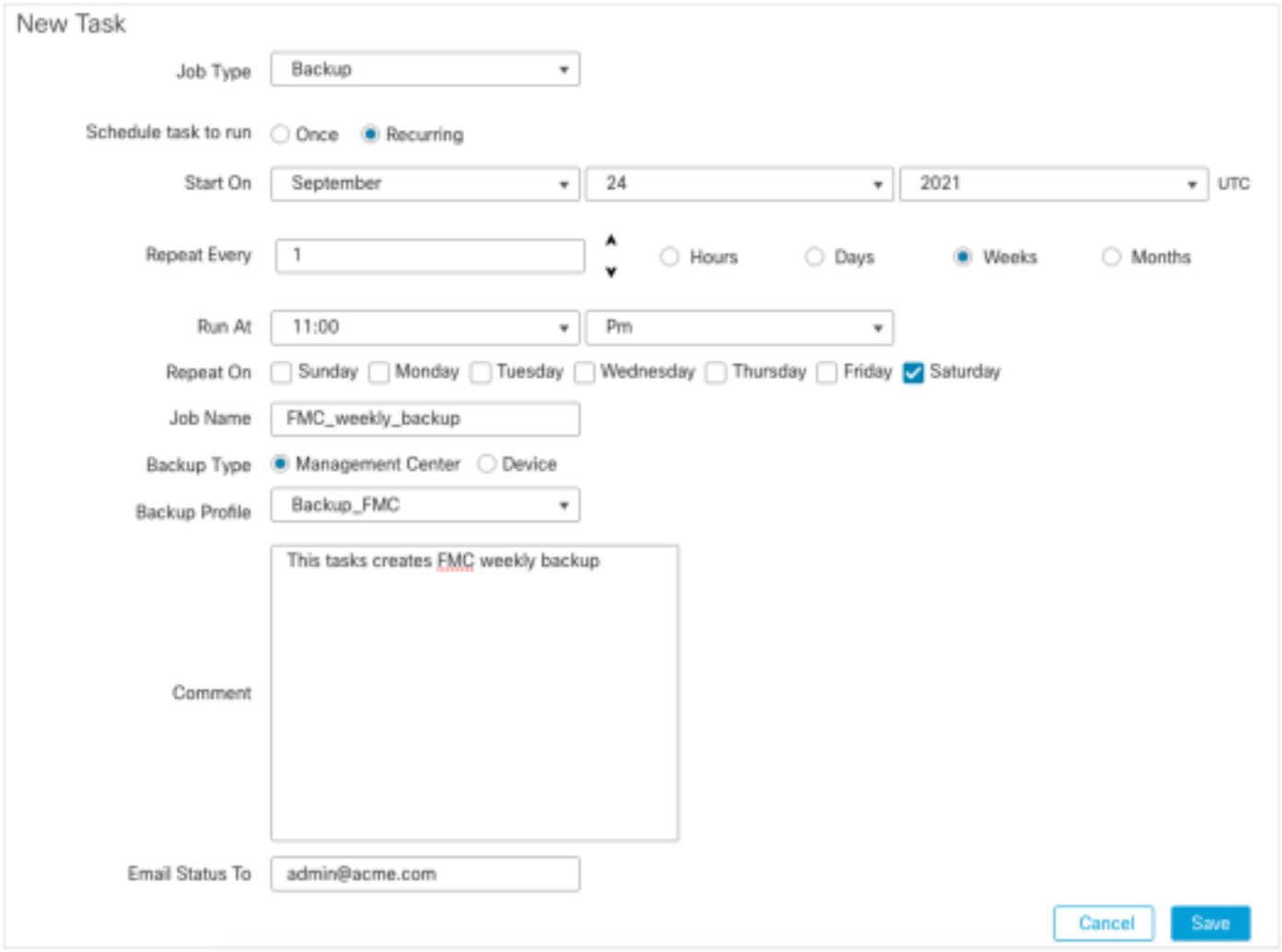


자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 예약된 작업을 사용하여 URL 필터링 업데이트 자동화를 참조하십시오.

정기 백업 구성

재해 복구 계획의 일환으로 정기적인 백업을 수행하는 것이 좋습니다.

1. **전역 도메인**에 있는지 **확인합니다**.
2. FMC 백업 프로필을 생성합니다. 자세한 내용은 **FMC 백업 생성** 섹션**을** 참조하십시오.
3. System(시스템) **> Tools(툴) > Scheduling(예약)으로 이동합니다**.
4. 작업 **추가를 클릭합니다**.
5. Job **Type** 드롭다운 목록에서 Backup을 **선택합니다.**
6. Schedule **task to run**(**예약 작업**을 실행하려면 **Recurring** 라디오 버튼을 클릭합니다.
   백업 빈도는 조직의 요구 사항에 맞게 조정되어야 합니다. 유지 보수 기간 또는 기타 사용량이 적은 시간에 백업을 생성하는 것이 좋습니다.
7. **Backup Type(백업 유형)**에서 **Management Center** 라디오 버튼**을** 클릭합니다.
8. Backup **Profile** 드롭다운 목록에서 Backup Profile을 선택합니다.
9. 저장을 **클릭합니다**.



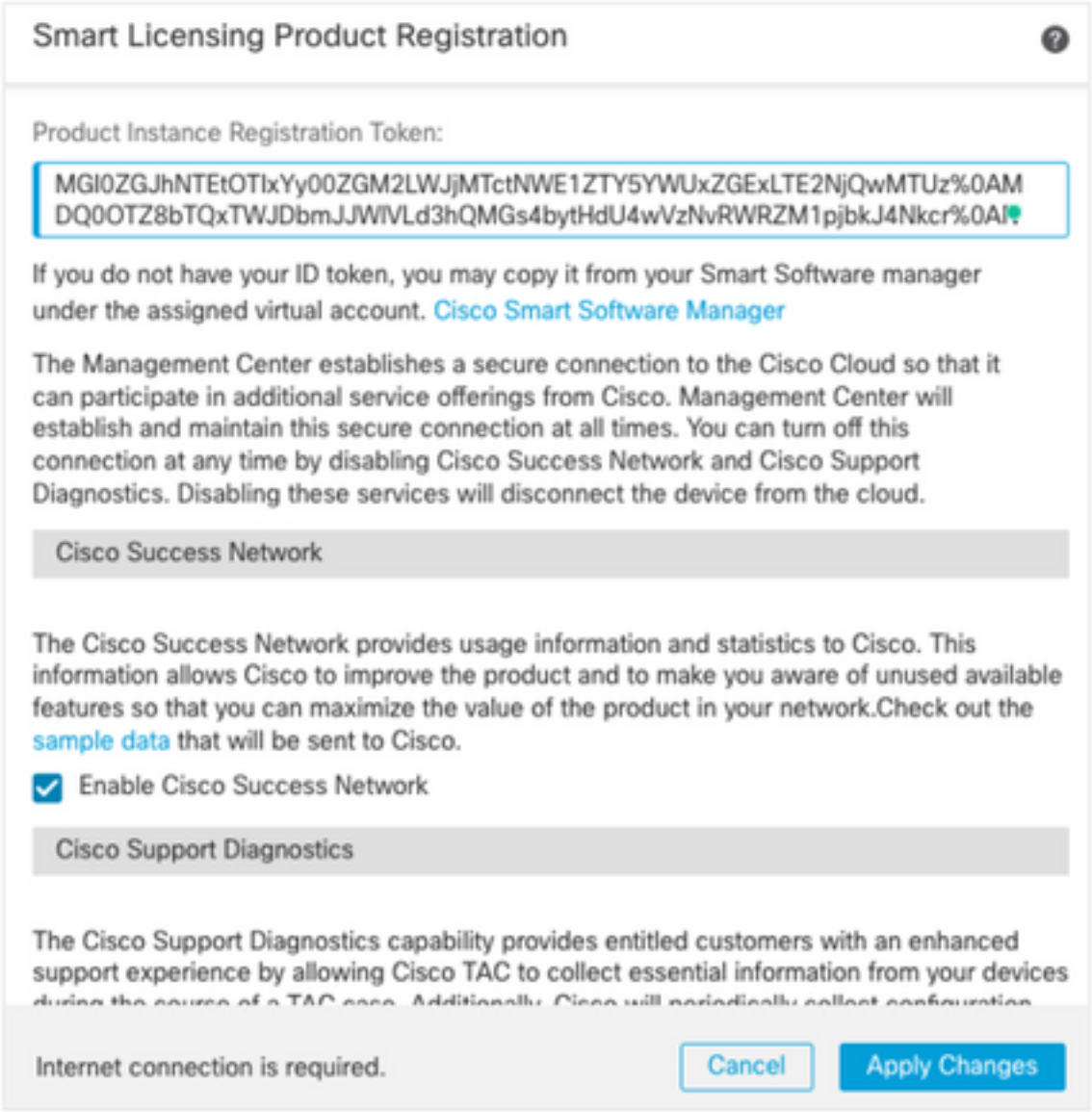
자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 장: 백업 및 복원.

Smart License가 등록되었는지 확인합니다.

Cisco Firewall Management Center를 Cisco Smart Software Manager에 등록하려면 다음 단계를 완료하십시오.

1. https://software.cisco.com에서 **Smart Software Manager > Manage licenses**로 **이동합니다**.

2. Inventory(**인벤토리) > General(일반)** 탭으로 이동하고 **New Token(새 토큰)**을 **생성합니다**.
3. FMC UI에서 **System > Licenses > Smart Licenses로 이동합니다**.
4. Register(**등록)를 클릭합니다**.
5. Cisco Smart Software Licensing 포털에 생성된 토큰을 삽입합니다.
6. **Cisco Success Network가 활성화되었는지 확인합니다**.
7. Apply Changes(**변경 사항 적용)를 클릭합니다**.
8. Smart License 상태를 확인합니다.



자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - Smart 라이센스 등록을 참조하십시오.

변수 집합의 구성 검토

HOME_NET 변수에 조직의 내부 네트워크/서브넷만 포함되어 있는지 확인합니다. 잘못된 변수 집합 정의가 방화벽의 성능에 부정적인 영향을 미칩니다.

1. Objects **> Variable Set로 이동합니다**.
2. 침입 정책에서 사용하는 변수 집합을 수정합니다. 서로 다른 설정을 사용하여 침입 정책당 하나의 변수 집합을 가질 수 있습니다.
3. 환경에 따라 변수를 조정하고 Save(저장)를 **클릭합니다**.

DNS_SERVERS 또는 HTTP_SERVERS에 관심이 있는 다른 변수도 있습니다.

자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 변수 집합을 참조하십시오.

클라우드 서비스 지원 확인

다양한 클라우드 서비스를 활용하려면System(**시스템) > Integration(통합) > Cloud Services(클라우드 서비스)로 이동합니다**.

URL 필터링

1. URL 필터링을 활성화하고 자동 업데이트를 허용하고 Query Cisco Cloud for Unknown URLs(알 수 없는 URL에 대해 Cisco 클라우드 쿼리)를 설정합니다.
   더 자주 캐시 URL 만료를 수행하려면 클라우드에 대한 더 많은 쿼리가 필요하므로 웹 로드가 느려집니다.
2. 변경 사항을 저장합니다.

팁: 캐시 URL 만료의 경우 기본 Never를 **유지합니다**. 더 엄격한 웹 재분류가 필요한 경우 이 설정을 적절히 수정할 수 있습니다.

AMP for Networks

1. 두 설정이 모두 설정되어 있는지 확인합니다. **자동 로컬 악성코드 탐지 업데이트**를 활성화하고 **Cisco와 악성코드 이벤트의 URI를 공유합니다**.
2. FMC 6.6.X에서 대신 사용된 TCP 포트가 443이 되도록 AMP for Networks용 레거시 포트 32137의 사용을 비활성화합니다.
3. 변경 사항을 저장합니다.

참고: 이 설정은 FMC 7.0+에서 더 이상 사용할 수 없으며 포트는 항상 443입니다.

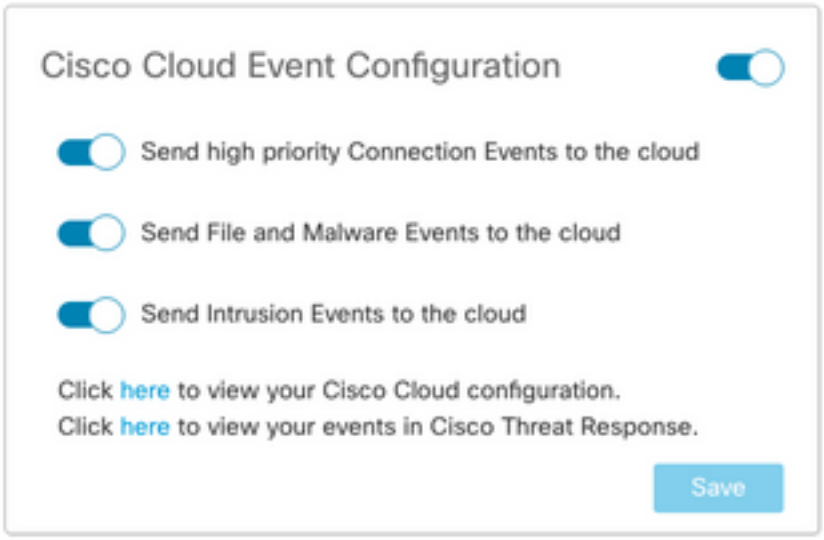
Cisco 클라우드 지역

1. 클라우드 영역은 SecureX 조직 영역과 일치해야 합니다. SecureX 조직이 생성되지 않은 경우 FMC 설치에 가까운 지역을 선택합니다. APJ 지역, EU 지역 또는 미국 지역.
2. 변경 사항을 저장합니다.

Cisco 클라우드 이벤트 컨피그레이션

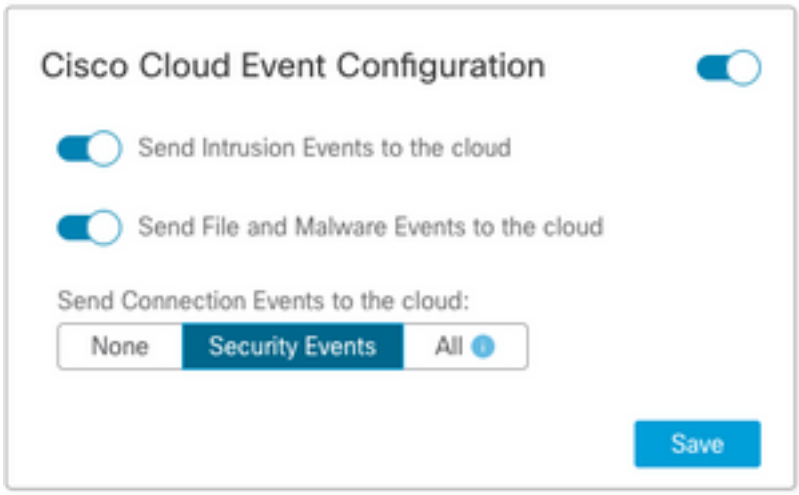
FMC 6.6.x의 경우

1. 세 가지 옵션 모두 확인: **우선 순위가 높은 Connection Events를 클라우드로 전송**, **Send File and Malware Events to the cloud(클라우드에 파일 및 악성코드 이벤트 전송)**, **Send Intrusion Events to the Cloud(클라우드에 침입 이벤트 보내기)가** 선택됩니다.
2. 변경 사항을 저장합니다.



FMC 7.0 이상의 경우

1. 두 옵션이 모두 선택되었는지 확인합니다. **Send Intrusion Events to the cloud(클라우드에 침입 이벤트 전송)** 및 **Send File and Malware Events to the cloud(파일 및 악성코드 이벤트 전송)**.
2. 연결 이벤트 유형에 대해 Security Analytics and Logging 솔루션을 사용 중인 경우 **All**(모두)을 선택합니다. SecureX의 경우 Security Events만 **선택합니다**.
3. 변경 사항을 저장합니다.



SecureX 통합 사용

SecureX 통합은 Cisco 보안 제품 전반의 위협 환경에 대한 즉각적인 가시성을 제공합니다. SecureX를 연결하고 리본을 활성화하려면 다음 단계를 수행하십시오.

SecureX 리본 통합

참고: 이 옵션은 FMC 버전 7.0 이상에서 사용할 수 있습니다.

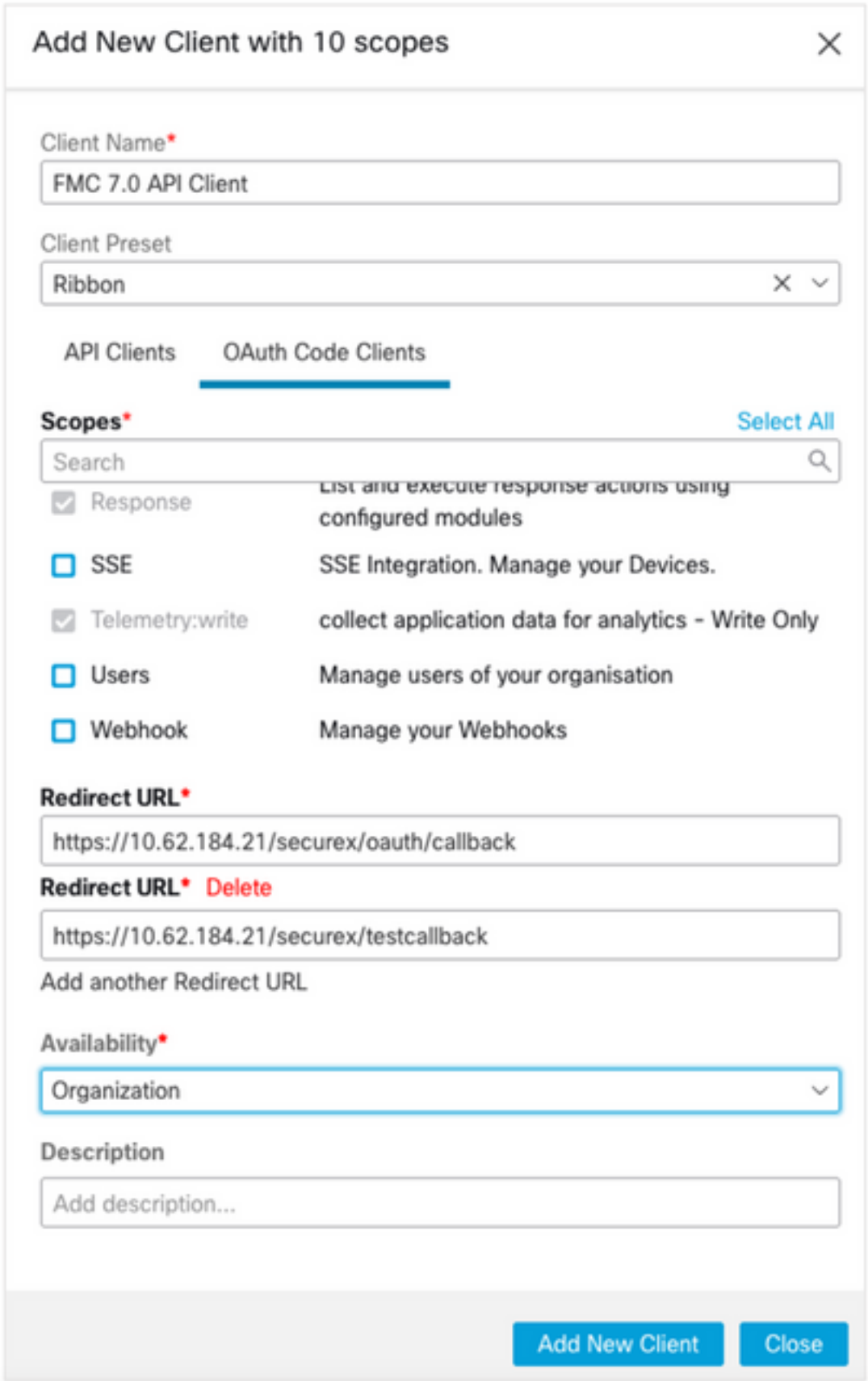
1. SecureX에 로그인하여 API 클라이언트를 생성합니다. Client Name(**클라이언트 이름**) 필드에 FMC를 설명하는 이름을 입력합니다. 예를 들어, FMC 7.0 API Client입니다.Oauth **Code Clients 탭을** 클릭합니다.Client **Preset** 드롭다운 목록에서 **리본**을 선택합니다. 범위를 선택합니다. Casebook, Eness:read, Global Intel:read, Inspect:read, Notification, Orbeability, Private

Intel, Profile, Response, Telemetry:write.FMC에 표시되는 두 개의 리디렉션 URL을 추가합니다.

리디렉션 URL: <FMC_URL>/securex/oauth/callback

두 번째 리디렉션 URL: <FMC_URL>/securex/testcallback

1. Availability(가용성) 드롭다운 목록에서 Organization(조직)을 **선택합니다**.Add **New Client를 클릭합니다**.



2. FMC에서 **시스템 > SecureX로 이동합니다**.

3. 오른쪽 상단 모서리에서 토글을 켜고 표시된 영역이 SecureX 조직과 일치하는지 확인합니다.

4. **클라이언트 ID** 및 **클라이언트 비밀번호**를 복사하여 FMC에 붙여넣습니다.

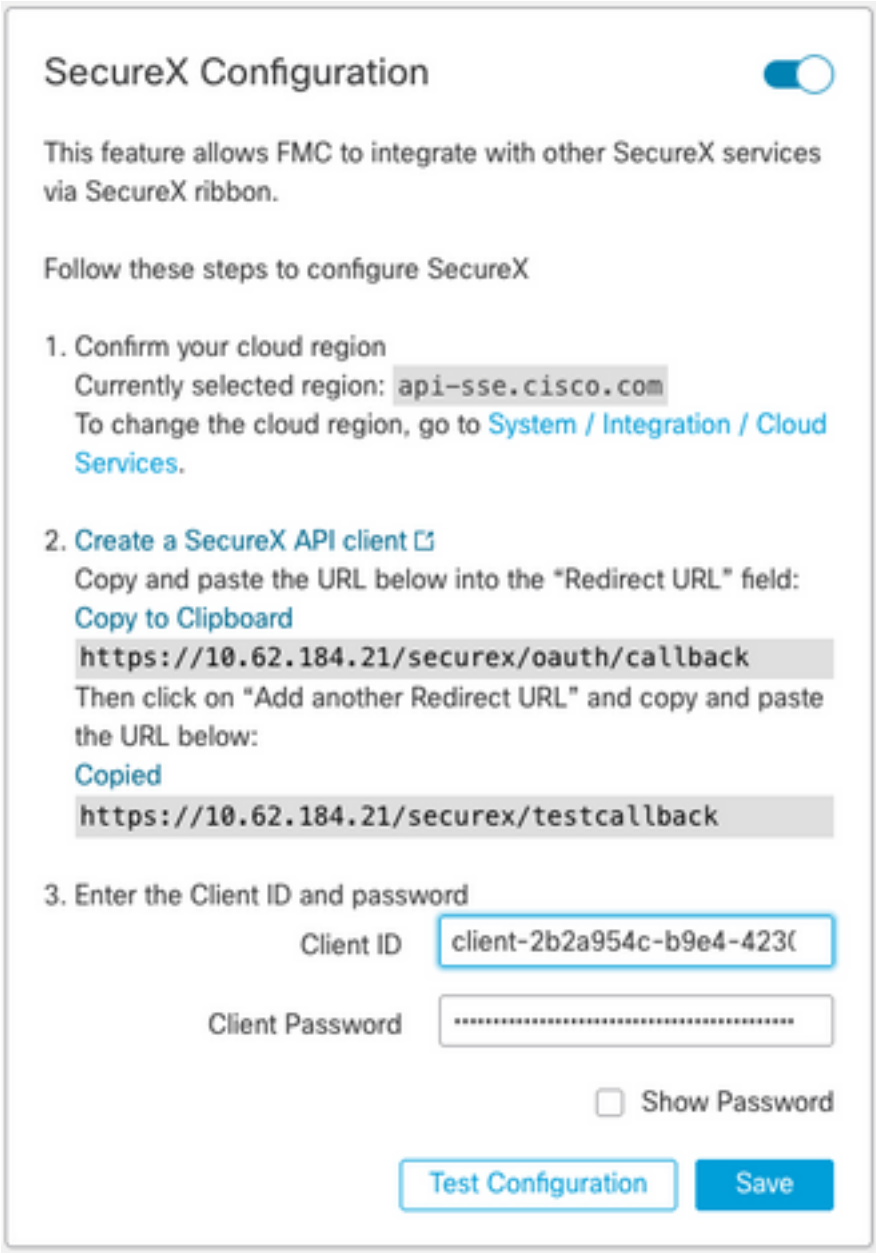
5. **구성 테스트를 선택합니다**.

6. SecureX에 로그인하여 API 클라이언트를 인증합니다.

7. 변경 사항을 저장하고 브라우저를 새로 고쳐 맨 아래에 표시된 리본을 확인합니다.

8. 리본을 확장하고 SecureX **가져오기를 선택합니다**. 프롬프트가 표시되면 SecureX 자격 증명을 입력합니다.

9. 이제 SecureX 리본이 FMC 사용자에 대해 완벽하게 작동합니다.



5YVPsGdzrkX8q8q0yYl-tDitezO6p_17MtH6NATx68fUZ5u9T3qOEQ

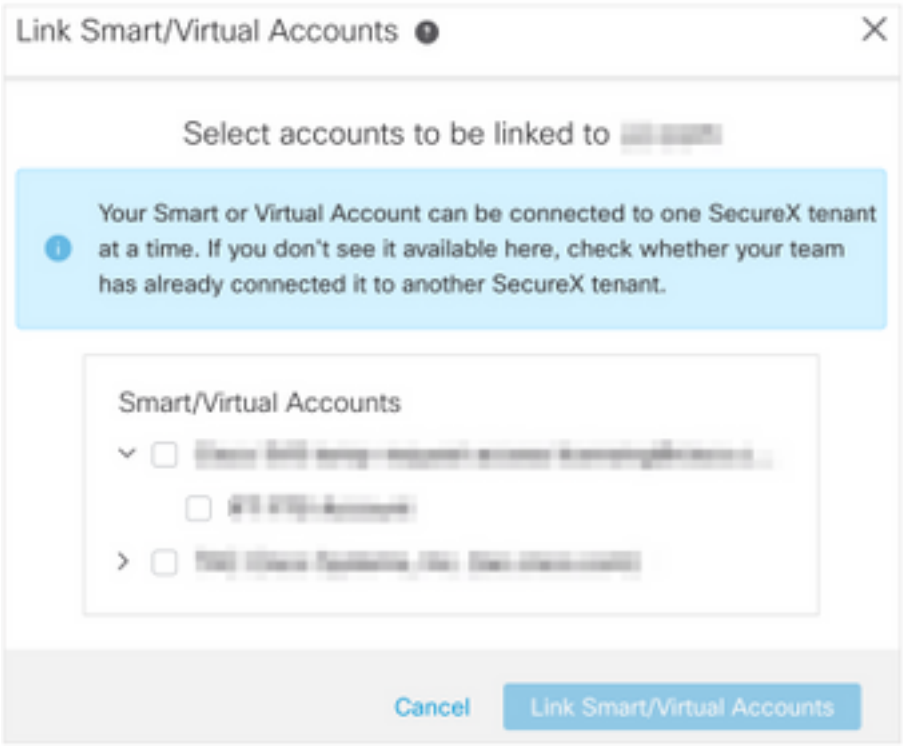
> **참고:** 다른 FMC 사용자가 리본에 액세스해야 하는 경우 해당 사용자는 SecureX 자격 증명을 사용하여 리본에 로그인해야 합니다.

SecureX에 연결 이벤트 보내기

1. FMC에서 **System(시스템) > Integration(통합) > Cloud Services(클라우드 서비스)로** 이동하고 **Turn on Cloud Services(클라우드 서비스 켜기)** 섹션에 설명된 대로 **Cisco Cloud Event**

Configuration(Cisco 클라우드 이벤트 컨피그레이션)이 Intrusion, File, and Malware(침입, 파일 및 악성코드) 이벤트를 전송하는지확인합니다.

2. Register the Smart Licenses(**스마트 라이센스 등록**) 섹션에 설명된 대로 FMC가 Smart License**에 등록되었는지** 확인합니다.
3. FMC에 표시된 Assigned **Virtual Account** 이름을 System(시스템) **> Licenses(라이센스) > Smart Licenses(스마트 라이센스)**에서 **메모합니다**.
4. FMC를 SecureX에 등록합니다. SecureX에서 Administration(관리) **> Devices(디바이스)로 이동합니다**.Manage **Devices를 선택합니다**.브라우저에서 팝업 창이 허용되는지 확인합니다 .SSE(Security Services Exchange)에 로그인합니다.Tools **메뉴 > Link Smart/Virtual Accounts로 이동합니다**.Link more **accounts(추가 계정 연결)를 선택합니다**.FMC에 할당된 가상 어카운트를 선택합니다(3단계).Link **Smart/Virtual Accounts를 선택합니다.**



- FMC 디바이스가 디바이스에 나열되는지 확인합니다.
- **Cloud Services(클라우드 서비스) 탭으로 이동하여 Cisco SecureX 위협 응답 및 이벤트 처리 기능을 설정합니다.**
- 이벤트 처리 기능 옆에 있는 **추가 서비스 설정**(기어 모양 아이콘)을 선택합니다.
- General(일반) 탭에서 Share **event data with Talos를** 선택합니다.
- Auto-Promote Events(이벤트 자동 승격) 탭의 By Event Type(이벤트 유형별) 섹션에서 사용 가능한 모든 이벤트 유형을 선택하고 Save(**저장)를 선택합니다**.

5. 기본 SecureX 포털에서 **Integration Modules(통합 모듈) > Firepower(Firepower)로 이동하고** Firepower 통합 모듈을 추가합니다.

6. 새 대시보드를 생성합니다.

7. Firepower 관련 타일을 추가합니다.

보안 엔드포인트 통합(AMP for Endpoints)

Firepower 구축에서 AMP(Secure Endpoint) 통합을 활성화하려면 다음 단계를 수행하십시오.

1. AMP **> AMP Management로 이동합니다**.

2. Add **AMP Cloud Connection을 선택합니다**.
3. 클라우드를 선택하고 **등록**.

참고: Enabled 상태**는** 클라우드에 대한 연결이 설정되었음을 의미합니다.

통합 보안 악성코드 분석(Threat Grid)

기본적으로 Firepower Management Center는 파일 제출 및 보고서 검색을 위해 공용 Cisco Threat Grid 클라우드에 연결할 수 있습니다. 이 연결을 삭제할 수 없습니다. 그러나 구축 클라우드에 가장 가까운 곳을 선택하는 것이 좋습니다.

1. AMP **> Dynamic Analysis Connections로 이동합니다**.
2. 작업 섹션에서 편집(연필 아이콘)을 클릭합니다.
3. 올바른 클라우드 이름을 선택합니다.
4. 자세한 보고 및 고급 샌드박스 기능을 위해 Threat Grid 어카운트를 연결하려면 **Associate** 아이콘을 클릭합니다.

자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 퍼블릭 클라우드에서 동적 분석 결과에 대한 액세스 활성화를 참조하십시오.

온프레미스 Thread Grid 어플라이언스 통합에 대한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - Dynamic Analysis On-Premises Appliance(Cisco Threat Grid)를 참조하십시오.