# 데이터 스토리지



# FMC에 저장된 데이터

| 대상 | 확인 |
|---|---|
| FMC의 데이터 스토리지에 대한 일반 정보 | 디스크 사용량 위젯 |
| 오래된 데이터 제거 | FMC 데이터베이스에서 데이터 제거, 2 페이지 |
| FMC의 데이터에 대한 외부 액세스 허용(고급 기능) | 외부 데이터베이스 액세스 설정 |
| 백업 | 백업 및 원격 스토리지 관리 및 하위 항목 |
| 보고서 | 로컬 스토리지 설정 |
| 이벤트 | 연결 로깅<br>데이터베이스 이벤트 제한 수 및 하위 항목 |
| 네트워크 검색 데이터 | 네트워크 검색 데이터 스토리지 설정 및 후속 주제 |
| 파일 | 모범 사례를 포함하여 파일 정책 및 악성코드 보호에 파일을 저장하는 방법을 설명합니다.<br>파일 및 악성코드 탐지 성능 및 저장 조정 |
| 패킷 데이터 | 일반 설정 편집 |
| 사용자 및 사용자 활동 | 사용자 데이터베이스<br>사용자 활동 데이터베이스 |

# FMC 데이터베이스에서 데이터 제거

데이터베이스 제거 페이지를 사용하여 검색, ID, 연결 및 보안 인텔리전스 데이터 파일을 FMC 데이터베이스에서 제거할 수 있습니다. 데이터베이스를 삭제하면 해당 프로세스가 다시 시작됩니다.

⚠

주의 데이터베이스를 삭제하면 Firepower Management Center에서 지정한 데이터가 제거됩니다. 데이터를 삭제한 후에는 복구할 수 없습니다 .

시작하기 전에

데이터를 제거하려면 관리자 또는 보안 분석가 권한이 있어야 합니다. 글로벌 도메인에만 속할 수 있습니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Data Purge(**데이터 제거**)**을(를) 선택합니다.

단계 **2** **Discovery and Identity(**검색 및 **ID)**에서 다음 중 하나 또는 모두를 실행합니다.

- 데이터베이스에서 모든 네트워크 검색 이벤트를 제거하려면 **Network Discovery Events(**네트워크 검색 이벤트**)** 확인란을 선택합니다.
- **Hosts(**호스트**)** 확인란을 선택하여 모든 호스트 및 Indications of Compromise flags(보안 침해 플래그 표시)를 데이터베이스에서 제거합니다.
- **User Activity(**사용자 활동**)** 확인란을 선택하고 모든 사용자 활동 이벤트를 데이터베이스에서 제거합니다.
- **User Identities(**사용자 **ID)** 확인란을 선택하고 모든 사용자 로그인 및 사용자 기록 데이터 를 데이터베이스에서 제거합니다.

단계 **3** **Connections(**연결**)** 아래에서 다음 중 하나 또는 모두를 실행합니다.

- **Connection Events(**연결 이벤트**)** 확인란을 선택하고 모든 연결 데이터를 데이터베이스에서 제거합니다.
- **Connection Summary Events(**연결 요약 이벤트**)** 확인란을 선택하고 모든 연결 요약 데이터를 데이터베이스에서 제거합니다.
- **Security Intelligence Events(**보안 인텔리전스 이벤트**)** 확인란을 선택하고 모든 보안 인텔리전스 데이터를 데이터베이스에서 제거합니다.

참고 **Connection Events(**연결 이벤트**)** 확인란을 선택해도 보안 인텔리전스 이벤트는 제거되지 않습니다. 보안 인텔리전스 데이터와의 연결은 계속 보안 인텔리전스(Security Intelligence) 이벤트 페이지에 나타납니다(Analysis(분석)> Connections(연결) 메뉴 하단) 따라서 **Security Intelligence Events(**보안 인텔리전스 이벤트**)** 확인란을 선택해도 보안 인텔리전스 데이터 관련 연결 이벤트는 제거되지 않습니다.

단계 **4** **Purge Selected Events(**선택된 이벤트 제거**)**를 클릭합니다.
항목이 삭제되고 해당 프로세스가 다시 시작됩니다.

# 외부 데이터 스토리지

선택적으로 원격 데이터 스토리지를 사용하여 특정 유형의 데이터를 저장할 수 있습니다.

| 대상 | 확인 |
|---|---|
| 백업 | 백업 및 원격 스토리지 관리 및 하위 항목<br>원격 스토리지 관리 및 하위 항목 |
| 보고서 | 원격 스토리지 관리 및 하위 항목<br>원격 스토리지로 보고서 이동 |
| Events(이벤트) | 시스템 로그 및 기타 리소스에 대한 정보 외부 툴을 사용하여 이벤트 분석<br>Stealthwatch 클라우드의 원격 데이터 스토리지, 4 페이지<br>Stealthwatch 어플라이언스의 원격 데이터 스토리지, 4 페이지<br>연결 이벤트를 원격으로 저장하는 경우, FMC에서 연결 이벤트 스토리지를 비활성화하는 것이 좋습니다. 자세한 정보는 데이터베이스 이벤트 제한 수 및 하위 주제를 참조하십시오. |

중요 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

## Cisco Security Analytics and Logging 원격 이벤트 스토리지 옵션 비교

다음은 이벤트 데이터를 외부적으로 Firepower Management Center에 저장하는 비슷하지만, 다른 옵션입니다.

| 온프레미스 | **SaaS** |
|---|---|
| 방화벽 뒤에서 스토리지 시스템을 구매, 라이선싱, 설정합니다. | 라이선스 및 데이터 스토리지 요금제를 구매하고 Cisco 클라우드로 데이터를 전송합니다. |

| 온프레미스 | SaaS |
| --- | --- |
| 지원되는 이벤트 유형:<br>• 연결<br>• 보안 인텔리전스<br>• 침입<br>• 파일 및 악성코드 | 지원되는 이벤트 유형:<br>• 연결<br>• 보안 인텔리전스<br>• 침입<br>• 파일 및 악성코드 |
| 시스템 로그를 통해 이벤트를 스토리지로 전송합니다. | 시스템 로그를 통해 이벤트를 스토리지로 전송합니다. |
| Stealthwatch Management Console 어플라이언스를 사용하여 이벤트를 확인합니다. FMC 이벤트 뷰어에서 크로스 실행합니다. | 라이선스에 따라 CDO 또는 Stealthwatch의 이벤트를 확인합니다. FMC 이벤트 뷰어에서 교차 실행합니다. |
| 자세한 내용은 Stealthwatch 어플라이언스의 원격 데이터 스토리지, 4 페이지의 링크를 참조하십시오. | 자세한 내용은 Stealthwatch 클라우드의 원격 데이터 스토리지, 4 페이지의 링크를 참조하십시오. |

# Stealthwatch 클라우드의 원격 데이터 스토리지

Cisco Security Analytics and Logging(SaaS) 을(를) 사용하여 선택한 Firepower 이벤트 데이터를 시스템 로그를 통해 Stealthwatch 클라우드로 전송합니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다.

자세한 내용은 https://cisco.com/go/firepower-sal-saas-integration-docs에 있는 *Firepower Management Center* 및 *Cisco SaaS(Security Analytics and Logging)* 통합 가이드를 참조하십시오

중요 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

# Stealthwatch 어플라이언스의 원격 데이터 스토리지

Firepower 어플라이언스가 제공할 수 있는 것보다 더 많은 데이터 스토리지가 필요한 경우, Cisco Security Analytics 및 로깅(온프레미스) 을 사용하여 Firepower 데이터를 Stealthwatch 어플라이언스에 저장할 수 있습니다. 자세한 내용은 https://cisco.com/go/sal-on-prem-docs에서 확인 가능한 설명서를 참조하십시오.

또는 FMC의 이벤트에서 Stealthwatch의 관련 이벤트로 빠르게 피벗하려면 다음에 대한 교차 실행 링크 설정 Stealthwatch 및 상황별 크로스 실행을 이용한 이벤트 조사의 내용을 참조하십시오.

중요 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

# 데이터 스토리지 기록

| 기능 | 버전 | 세부 사항 |
|---|---|---|
| Stealthwatch 어플라이언스의 원격 데이터 스토리지 | 6.7 | 이제 Cisco Security Analytics 및 로깅(온프레미스)을 사용하여 대량의 Firepower 이벤트 데이터를 원격으로 저장할 수 있습니다. FMC에서 이벤트를 볼 때 신속하게 교차 실행을 수행하여 원격 데이터 스토리지 위치에서 이벤트를 확인할 수 있습니다.<br><br>지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다. 이벤트는 시스템 로그를 사용하여 전송됩니다.<br><br>이 솔루션은 SWE(Stealthwatch Enterprise) 버전 7.3을 실행하는 SMC(Stealthwatch Management Console) 가상 버전의 사용 가용성에 따라 달라집니다.<br><br>Stealthwatch 어플라이언스의 원격 데이터 스토리지, 4 페이지의 내용을 참조하십시오. |
| Stealthwatch 클라우드의 원격 데이터 스토리지 | 6.4 | 시스템 로그를 사용하여 Cisco Security Analytics and Logging(SaaS) 을 통해 선택한 Firepower 데이터를 전송합니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다.<br><br>자세한 내용은 다음에 있는 *Firepower Management Center* 및 *Cisco SaaS(Security Analytics and Logging)* 통합 가이드를 참조하십시오. https://cisco.com/go/firepower-sal-saas-integration-docs |