



데이터 비우기 및 저장

- FMC에 저장된 데이터, 1 페이지
- 외부 데이터 스토리지, 3 페이지
- 데이터 스토리지 기록, 6 페이지

FMC에 저장된 데이터

대상	확인
FMC의 데이터 스토리지에 대한 일반 정보	디스크 사용량 위젯
오래된 데이터 제거	Management Center 데이터베이스에서 데이터 제거, 2 페이지
FMC의 데이터에 대한 외부 액세스 허용(고급 기능)	외부 데이터베이스 액세스
백업	백업 및 원격 스토리지 관리 및 하위 항목
보고서	로컬 스토리지 설정
이벤트	연결 로깅 데이터베이스 및 하위 항목
네트워크 검색 데이터	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 검색 데이터 스토리지 설정 및 후속 항목

대상	확인
파일	<p>Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 악성코드 보호 및 파일 정책 장에서 모범 사례를 포함한 파일 저장에 관한 정보를 참고하십시오.</p> <p>파일 및 악성코드 검사 성능 및 스토리지 조정 Cisco Secure Firewall Management Center 디바이스 구성 가이드</p>
패킷 데이터	<p>Cisco Secure Firewall Management Center 디바이스 구성 가이드의 일반 설정 편집</p>
사용자 및 사용자 활동	<p>Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사용자 데이터베이스</p> <p>Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사용자 활동 데이터베이스</p>

Management Center 데이터베이스에서 데이터 제거

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



주의 데이터베이스를 삭제하면 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 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 Host(호스트)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 뿐만 아니라 User Indications of Compromise flags(보안 침해 플래그 사용자 표시)를 데이터베이스에서 제거합니다.

참고 Microsoft Azure AD 영역에 대한 사용자 활동 이벤트, 사용자 로그인 및 사용자 기록 데이터는 제거되지 않습니다.

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 원격 스토리지 디바이스 및 하위 항목
보고서	원격 스토리지 디바이스 및 하위 항목 원격 스토리지로 보고서 이동

대상	확인
Events(이벤트)	<p>시스템 로그 및 기타 리소스에 대한 정보 외부 톨을 사용하여 이벤트 분석</p> <p>Cisco Secure Cloud Analytics의 원격 데이터 스토리지, 5 페이지</p> <p>Secure Network Analytics 어플라이언스의 원격 데이터 스토리지, 5 페이지</p> <p>연결 이벤트를 원격으로 저장하는 경우, FMC에서 연결 이벤트 스토리지를 비활성화하는 것이 좋습니다. 자세한 정보는 데이터베이스 및 하위 주제를 참조하십시오.</p>



중요 Syslog를 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.

Security Analytics and Logging 원격 이벤트 스토리지 옵션 비교

다음은 이벤트 데이터를 외부적으로 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.
<p>지원되는 이벤트 유형:</p> <ul style="list-style-type: none"> • 연결 • 보안 인텔리전스 • 침입 • 파일 및 악성코드 • LINA 	<p>지원되는 이벤트 유형:</p> <ul style="list-style-type: none"> • 연결 • 보안 인텔리전스 • 침입 • 파일 및 악성코드
시스템 로그 및 직접 통합을 모두 지원합니다.	시스템 로그 및 직접 통합을 모두 지원합니다.
<ul style="list-style-type: none"> • Secure Network Analytics Manager에서 모든 이벤트 확인합니다. • FMC 이벤트 뷰어에서 교차 실행하여 Secure Network Analytics Manager의 이벤트를 확인합니다. • FMC에서 원격으로 저장된 연결 및 보안 인텔리전스 이벤트 보기 	<p>라이선스에 따라 CDO 또는 Secure Network Analytics의 이벤트를 확인합니다. FMC 이벤트 뷰어에서 교차 실행합니다.</p>

온프레미스	SaaS
자세한 내용은 Secure Network Analytics 어플라이언스의 원격 데이터 스토리지, 5 페이지 의 링크를 참조하십시오.	자세한 내용은 Cisco Secure Cloud Analytics의 원격 데이터 스토리지, 5 페이지 의 링크를 참조하십시오.

Cisco Secure Cloud Analytics의 원격 데이터 스토리지

Security Analytics and Logging(SaaS)를 사용하여 선택한 Firepower 이벤트 데이터를 Secure Cloud Analytics로 전송합니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다.

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

직접 또는 시스템 로그를 통해 이벤트를 전송할 수 있습니다.



중요 Syslog를 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.

Secure Network Analytics 어플라이언스의 원격 데이터 스토리지

Firepower 어플라이언스가 제공할 수 있는 것보다 더 많은 데이터 스토리지가 필요한 경우, Security Analytics and Logging(보안 애널리틱스)을 사용하여 Firepower 데이터를 Secure Network Analytics 어플라이언스에 저장할 수 있습니다. 자세한 내용은 <https://cisco.com/go/sal-on-prem-docs>에서 확인 가능한 설명서를 참조하십시오.

Secure Network Analytics 어플라이언스에 저장된 경우에도 management center에서 연결 이벤트를 볼 수 있습니다. [Secure Network Analytics 어플라이언스에 저장된 연결 이벤트](#)로 [Secure Firewall Management Center](#)에서 작업의 내용을 참조하십시오.



중요 Syslog를 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	배치 사항	<p>최소</p> <p>t a e r h T e s n e f e D</p>
낮은 우선순위 연결 이벤트를 이벤트 속도 제한에서 제외	7.0 버전	<p>이벤트를 저장하므로 management center에 연결 이벤트를 저장하지 않기로 선택하는 경우, 해당 이벤트는 management center 하드웨어 디바이스의 플로우 속도 제한에 포함되지 않습니다.</p> <p>새 7.0 설정을 사용하여 Security Analytics and Logging(보안 애널리틱스)에 이벤트를 전송하는 경우, 이 설정을 해당 통합의 일부로 구성합니다.</p> <p>그렇지 않으면 데이터베이스 이벤트 제한 수의 연결 데이터베이스에 대한 정보를 참조하십시오.</p> <p>신규/수정된 페이지: 없음 동작 변경만 해당됩니다.</p>
Secure Network Analytics 어플라이언스로 이벤트를 전송하기 위한 향상된 프로세스	7.0 버전	<p>마법사를 사용하면 Security Analytics and Logging(보안 애널리틱스)을(를) 통해 Secure Network Analytics 어플라이언스로 직접 이벤트를 전송할 수 있습니다.</p> <p>또한 이 마법사로 management center에서 이벤트 페이지를 보는 동안 원격으로 저장된 연결 이벤트를 볼 수 있으며, Secure Network Analytics 어플라이언스에서 이벤트를 확인할 수 있도록 management center에서 교차 실행할 수 있습니다.</p> <p>시스템 로그를 사용하여 이벤트를 전송하도록 시스템을 이미 설정한 경우, 해당 설정을 비활성화하지 않는 한 이벤트는 시스템 로그를 통해 계속 전송됩니다.</p> <p>자세한 내용은 Secure Network Analytics 어플라이언스의 원격 데이터 스토리지, 5 페이지의 참조 설명서를 확인하십시오.</p> <p>신규/수정된 페이지: 이제 System(시스템) > Logging(로깅) > Security Analytics & Logging(보안 분석 및 로깅) 페이지에 교차 실행 옵션을 생성하는 데 설정 대신 마법사가 표시됩니다.</p>
Secure Network Analytics 어플라이언스의 원격 데이터 스토리지	6.7 버전	<p>Security Analytics and Logging(보안 애널리틱스)을 사용하여 대량의 Firepower 이벤트 데이터를 원격으로 저장할 수 있습니다. management center에서 이벤트를 볼 때 신속하게 교차 실행을 수행하여 원격 데이터 스토리지 위치에서 이벤트를 확인할 수 있습니다.</p> <p>지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다. 이벤트는 시스템 로그를 사용하여 전송됩니다.</p> <p>이 솔루션은 SWE(Stealthwatch Enterprise) 버전 7.3을 실행하는 SMC(Stealthwatch Management Console) 가상 버전의 사용 가용성에 따라 달라집니다.</p> <p>Secure Network Analytics 어플라이언스의 원격 데이터 스토리지, 5 페이지의 내용을 참조하십시오.</p>

기능	배관 사항 t a e r h T e s n e f e D	최소
Cisco Secure Cloud Analytics의 원격 데이터 스토리지	64 소스 데이터를 전송합니다. 자세한 내용은	A를 사용하여 Security Analytics and Logging(SaaS)을 통해 선택한 Firepower 데이터를 전송합니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다. 용은 https://cisco.com/go/firepower-sal-saas-integration-docs 에 있는 <i>Firepower Management Center</i> 및 <i>Cisco SaaS(Security Analytics and Logging)</i> 통합 가이드를 참조하십시오.

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.