



## Snort 2에서 Snort 3로 마이그레이션

다음 항목에서는 Snort 2에서 Snort 3로 마이그레이션하는 다양한 측면에 대해 설명합니다.

- [Snort 2와 Snort 3 비교, 1 페이지](#)
- [Snort 2에서 Snort 3로 마이그레이션, 2 페이지](#)
- [Snort 3 활성화 및 비활성화, 2 페이지](#)
- [Snort 2 및 Snort 3 기본 정책 매핑 보기, 4 페이지](#)
- [Snort 2 규칙과 Snort 3 동기화, 4 페이지](#)

## Snort 2와 Snort 3 비교

Snort 3는 Snort 2에 비해 동일한 리소스로 더 많은 트래픽을 검사하도록 아키텍처가 재설계되었습니다. Snort 3를 사용하면 트래픽 파서를 간단하고 유연하게 삽입할 수 있습니다. 또한 Snort 3의 새로운 규칙 syntax(명령문)를 통해 규칙을 더 쉽게 작성하고 해당하는 공유 개체 규칙을 볼 수 있습니다.

아래 표에는 검사 엔진 기능 측면에서 Snort 2와 Snort 3 버전 간의 차이점이 나와 있습니다.

기능	Snort 2	Snort 3
패킷 스레드	프로세스당 한 개	프로세스당 개수 제한 없음
구성 메모리 할당	프로세스 수 * xGB	총 xGB, 패킷에 더 많은 메모리 사용 가능
구성 다시 로드	더 느림	더 빠름, 한 스레드가 여러 코어에 분산되어 처리될 수 있음
규칙 syntax(명령문)	일관성이 없고 줄 이스케이프 필요	일관된 시스템이며 임의의 공백이 사용됨
규칙 코멘트	코멘트만 나열	#, #begin 및 #end 표시, C 언어 스타일

## Snort 2에서 Snort 3로 마이그레이션

Snort 2에서 Snort 3로 마이그레이션하려면 Firepower Threat Defense 디바이스의 검사 엔진을 Snort 2에서 Snort 3로 전환해야 합니다. 7.0 이상 버전의 디바이스만 Snort 3를 지원합니다.

Snort 3가 디바이스의 검사 엔진으로 활성화되면 액세스 제어 정책을 통해 디바이스에 적용된 Snort 3 버전이 활성화되어 디바이스를 통과하는 모든 트래픽에 적용됩니다. 지원되는 디바이스에서 Snort 3를 활성화하려면 [Snort 3 활성화 및 비활성화, 2 페이지](#) 항목을 참조하십시오.

## Snort 2 사용자 지정 규칙에 대한 변환 툴

사용자 지정 규칙을 사용하는 경우 Snort 2에서 Snort 3로 변환하기 전에 Snort 3용 규칙 세트를 관리할 준비가 되었는지 확인합니다. 서드파티 벤더의 규칙 세트를 사용하는 경우 해당 벤더에 연락하여 규칙이 Snort 3로 성공적으로 변환되는지 확인하거나 기본적으로 Snort 3용으로 작성된 대체 규칙 세트를 얻으십시오. 직접 작성한 사용자 지정 규칙이 있는 경우 변환 전에 Snort 3 규칙을 작성하는 방법을 숙지하여 변환 후 Snort 3 탐지를 최적화하도록 규칙을 업데이트할 수 있습니다. Snort 3의 규칙 작성에 대해 자세히 알아보려면 아래 링크를 참조하십시오.

- <https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html>
- <https://blog.snort.org/2020/10/talos-transition-to-snort-3.html>

Snort 3 규칙에 대해 자세히 알아보려는 경우 <https://blog.snort.org/>에서 다른 블로그를 참조할 수 있습니다.

시스템 제공 툴을 사용하여 Snort 2 규칙을 Snort 3 규칙으로 변환하려면 [Snort 2 사용자 지정 규칙을 Snort 3로 변환](#) 항목을 참조하십시오.



**중요** Snort 2 NAP(Network Analysis Policy, 네트워크 분석 정책) 설정은 Snort3에 자동으로 복사될 수 없습니다. NAP 설정은 Snort 3에서 수동으로 복제해야 합니다.

## Snort 3 활성화 및 비활성화

Snort 3은 버전 7.0 이상의 새로 등록된 FTD 디바이스에 대한 기본 검사 엔진입니다. 그러나 하위 버전의 FTD 디바이스의 경우 Snort 2가 기본 검사 엔진입니다. 매니지드 FTD 디바이스를 버전 7.0 이상으로 업그레이드할 경우 검사 엔진은 Snort 2에 남아 있습니다. 버전 7.0 이상의 업그레이드된 FTD에서 Snort 3을 사용하려면 명시적으로 활성화해야 합니다. 필요한 경우 언제든지 Snort 3에서 Snort 2로 다시 전환할 수 있습니다.

필요한 경우 Snort 버전을 전환할 수 있습니다. Snort 2와 Snort 3 침입 규칙은 매핑되며, 이 매핑은 시스템에서 제공됩니다. 그러나 Snort 2 및 Snort 3에서는 모든 침입 규칙의 일대일 매핑을 찾을 수 없습니다. Snort 2에서 규칙에 대한 규칙 작업을 변경한 경우 Snort 3로 전환하면 해당 변경 사항이 유지되

지 않습니다. 변경 사항을 유지하려면 Snort 2를 Snort 3와 동기화해야 합니다. 동기화에 대한 자세한 내용은 [Snort 2 규칙과 Snort 3 동기화](#), 4 페이지 항목을 참조하십시오.

## 개별 디바이스에서 Snort 3 활성화 및 비활성화

시작하기 전에

이러한 단계를 수행할 수 있는 지원되는 사용자 역할은 다음과 같습니다.

- Admin(관리자)
- 침입 관리자

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 디바이스를 클릭하여 디바이스 홈 페이지로 이동합니다.

참고 디바이스가 Snort 2 또는 Snort 3로 나타나 디바이스의 현재 버전을 표시합니다.

단계 3 디바이스 탭을 클릭합니다.

단계 4 **Inspection Engine**(검사 엔진) 섹션에서 **Upgrade**(업그레이드)를 클릭합니다.

참고 Snort 3을 비활성화하려면 **Inspection Engine**(검사 엔진) 섹션에서 **Revert to Snort 2**(Snort 2로 되돌리기)를 클릭합니다.

단계 5 **Yes**(예)를 클릭합니다.

다음에 수행할 작업

디바이스에서 변경 사항을 구축합니다. 참고, [컨피그레이션 변경 사항 구축](#).

시스템은 구축 프로세스 중에 선택한 Snort 버전과 호환되도록 정책 설정을 변환합니다.



중요 구축 프로세스 중에는 현재 검사 엔진을 종료해야 하므로 일시적인 트래픽 손실이 발생합니다.

## 여러 디바이스에서 Snort 3 활성화 및 비활성화

여러 디바이스에서 Snort 3를 활성화하려면 모든 필수 FTD(Firepower Threat Defense) 디바이스가 버전 7.0 이상인지 확인하십시오.

시작하기 전에

이러한 단계를 수행할 수 있는 지원되는 사용자 역할은 다음과 같습니다.

- Admin(관리자)

- 침입 관리자

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 Snort 3를 활성화하거나 비활성화할 모든 디바이스를 선택합니다.

참고 디바이스가 Snort 2 또는 Snort 3로 나타나 디바이스의 현재 버전을 표시합니다.

단계 3 **Select Bulk Action**(대량 작업 선택) 드롭다운 목록을 클릭합니다.

단계 4 **Upgrade to Snort 3**(Snort 3로 업그레이드)를 클릭합니다.

참고 Snort 3를 비활성화하려면 **Downgrade to Snort 2**(Snort 2로 다운그레이드)를 클릭합니다.

단계 5 **Yes**(예)를 클릭합니다.

다음에 수행할 작업

디바이스에서 변경 사항을 구축합니다. 참고, [권피그레이션 변경 사항 구축](#).

시스템은 구축 프로세스 중에 선택한 Snort 버전과 호환되도록 정책 설정을 변환합니다.



중요 구축 프로세스 중에는 현재 검사 엔진을 종료해야 하므로 일시적인 트래픽 손실이 발생합니다.

## Snort 2 및 Snort 3 기본 정책 매핑 보기

단계 1 **Policies**(정책) > **Intrusion**(침입)을 선택합니다.

단계 2 **Intrusion Policies**(침입 정책) 탭이 선택되었는지 확인합니다.

단계 3 **IPS Mapping**(IPS 매핑)을 클릭합니다.

## Snort 2 규칙과 Snort 3 동기화

침입 정책의 Snort 2 및 Snort 3 버전은 요구 사항에 맞게 독립적으로 변경할 수 있습니다. 그러나 Snort 2에서 Snort 3으로 전환하려는 경우 이로 인해 차이가 발생할 수 있습니다. Snort 2 버전 설정과 사용자 지정 규칙이 유지되고 Snort 3에 전달되도록 하기 위해 FMC는 동기화 기능을 제공합니다. 동기화는 Snort 2 규칙 제정의 설정 및 사용자 지정 규칙에 도움이 됩니다. 이는 지난 몇 개월 또는 몇 년간 Snort 3 버전에서 복제하도록 변경되거나 추가되었을 수 있습니다.



중요


- Snort 2 규칙 재정의와 사용자 지정 규칙이 Snort 3에 복사되기만 하며 그 반대로는 복사되지 않습니다. Snort 2 및 Snort 3에서는 모든 침입 규칙의 일대일 매핑을 찾을 수 없습니다. 다음 절차를 수행할 때 두 버전에 있는 규칙에 대한 규칙 작업의 변경 사항이 동기화됩니다.
- 동기화 시 사용자 지정 규칙 또는 시스템 제공 규칙의 임계값 및 억제 설정이 Snort 2에서 Snort 3로 마이그레이션되지 않습니다.


단계 1 **Policies**(정책) > **Intrusion**(침입)을 선택합니다.

단계 2 **Intrusion Policies**(침입 정책) 탭이 선택되었는지 확인합니다.

단계 3 **Snort 3** 동기화 상태 표시를 클릭합니다.

단계 4 동기화되지 않은 침입 정책을 식별합니다.

단계 5 **Sync**(동기화) 아이콘()을 클릭합니다.

참고 Snort 2 버전과 Snort 3 버전의 침입 정책이 동기화된 경우 **Sync**(동기화) 아이콘이 녹색()으로 표시됩니다.

단계 6 요약을 읽고 필요한 경우 요약 사본을 다운로드합니다.

단계 7 **Re-Sync**(재동기화)를 클릭합니다.

- 참고
- 동기화된 설정은 Snort 3 침입 엔진이 디바이스에 적용되고 구축이 성공한 경우에만 적용됩니다.
  - Snort 2 사용자 지정 규칙은 시스템 제공 툴을 사용하여 Snort 3로 변환할 수 있습니다. Snort 2 사용자 지정 규칙이 있는 경우 **Custom Rules**(사용자 지정 규칙) 탭을 클릭하고 화면의 지침에 따라 규칙을 변환합니다. 자세한 내용은 [단일 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환](#)를 참고하십시오.

다음에 수행할 작업

컨피그레이션 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)를 참고하십시오.

