정책 : 정책 생성

개요

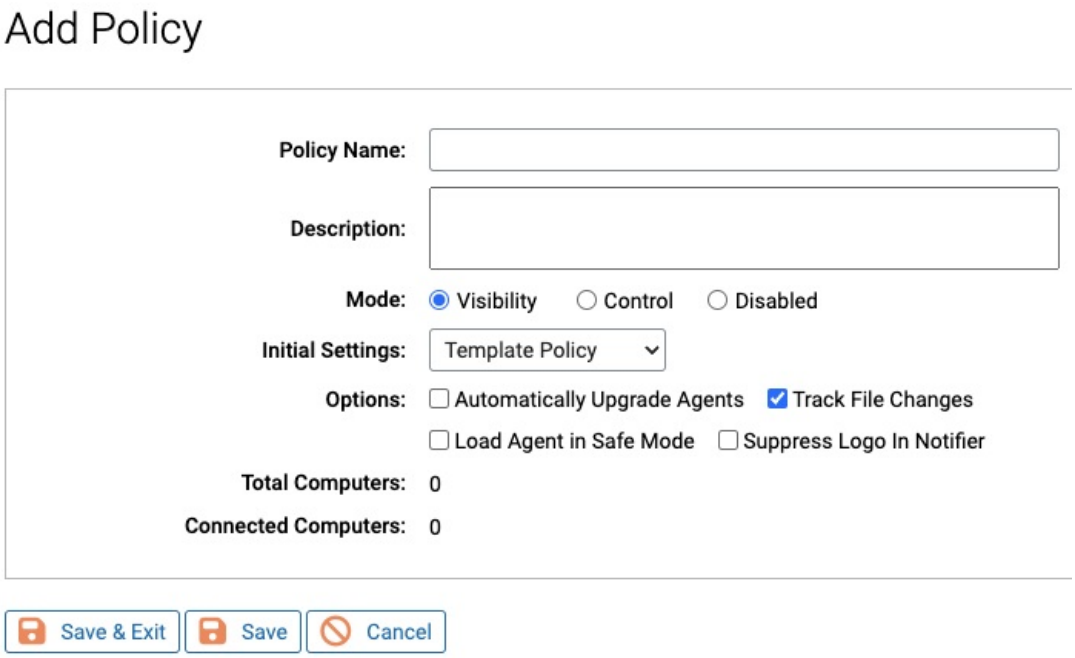
Carbon Black App Control 정책 생성에 대한 가이드 문서 입니다.

기능 소개

1. Policies

1.1 정책 생성

- [App Control] 웹 콘솔 접속 > [Policies] 메뉴 선택 > [Add Policy] 버튼 클릭하여 정책 생성



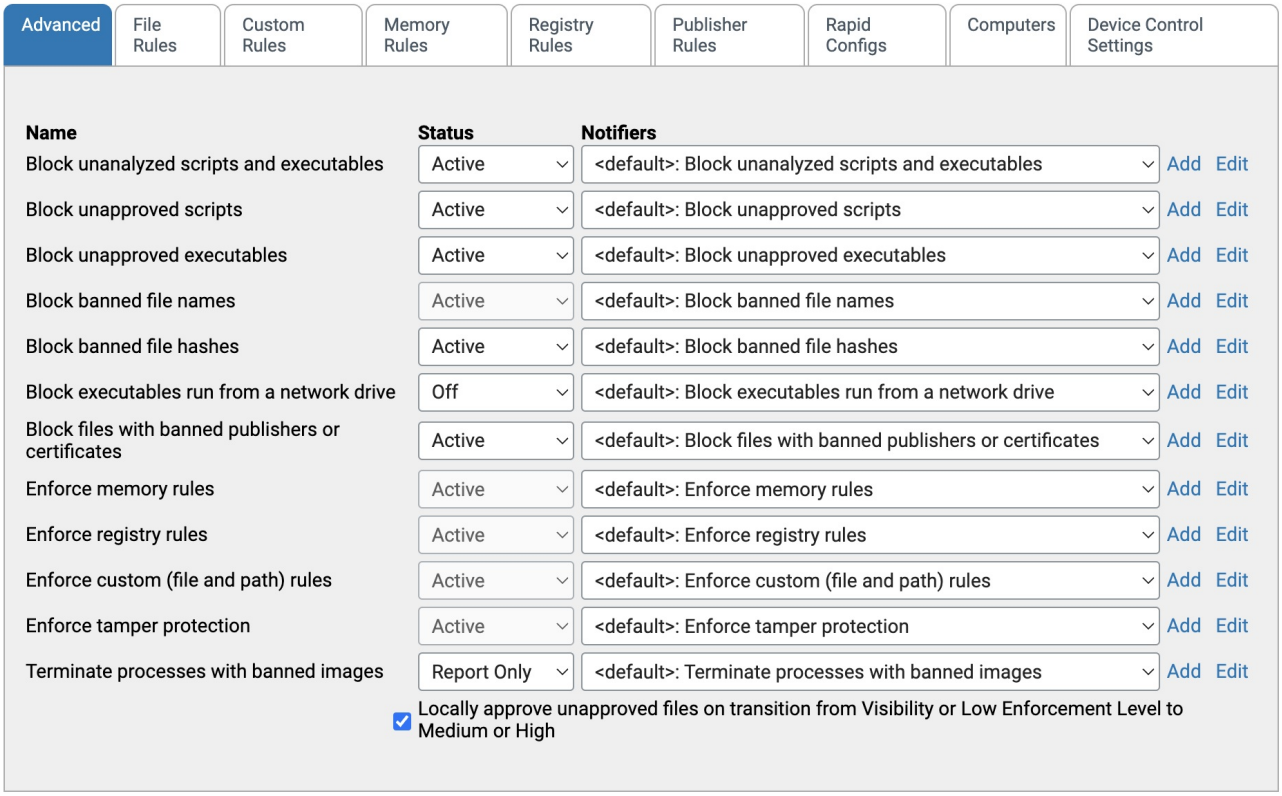
- 조직별 정책 및 목적별 정책을 생성하여 사용

- Policy Name : 정책 이름
- Description : 정책 설명
- Mode : 서버와 컴퓨터가 통신하는 상태 혹은 통신하지 않는 상태에 대해 동작할 모드 설정
  - Visibility : 파일 활동 및 이벤트 추적하기 위한 모드 (파일 실행/쓰기/금지 영향 없음) - 보안 기능을 인한 동작 방해 없음
  - Control : 파일 실행에 대한 제어 및 단계 설정
    - High (Block Unapproved) : 승인되지 않은 파일 실행 차단 및 이벤트 추적
    - Medium (Prompt Unapproved) : 승인되지 않은 파일 실행 차단 및 사용자가 파일 실행 여부 선택 가능
    - Low (Monitor Unapproved) : 승인되지 않은 파일 실행 허용 및 이벤트 추적
  - Disabled : 파일 활동에 대한 추적 중단 - 에이전트 제거 시 사용
- Initial Settings : 템플릿으로 사용할 정책 선택
- Options
  - Automatically Upgrade Agents : 에이전트에 대한 자동 업그레이드
  - Track File Changes : 파일 추가/삭제/변경 추적
  - Load Agent in Safe Mode (기본값) : 안전 모드에서 에이전트 로드
  - Suppress Logo in Notifier : 에이전트 알림이 발생할 경우 로고를 표시하지 않음
- Total Computer : 정책에 연결된 총 컴퓨터 갯수
- Connected Computer : 정책에 연결된 컴퓨터 중, 서버와 연결된 컴퓨터 개수

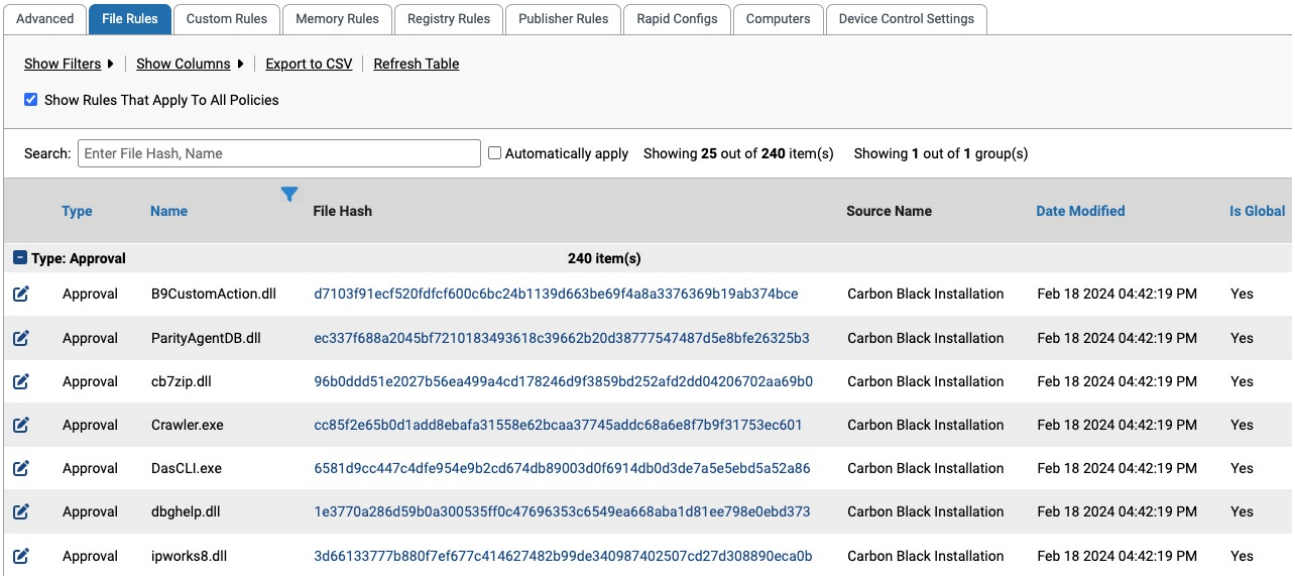
1.2 정책 구성

> 정책 별 상세 가이드 : https://bs.etevers.tech/books/carbon-black-app-control-handbook/page/3def1

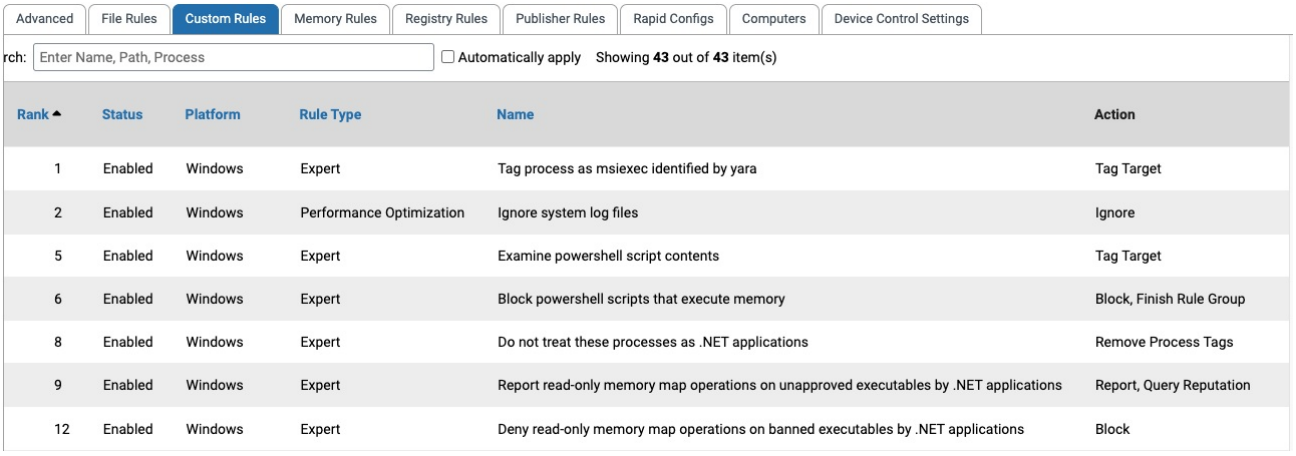
- [App Control] 웹 콘솔 접속 > [Policies] 메뉴 선택 > '정책' 의 (View Details) 버튼 클릭



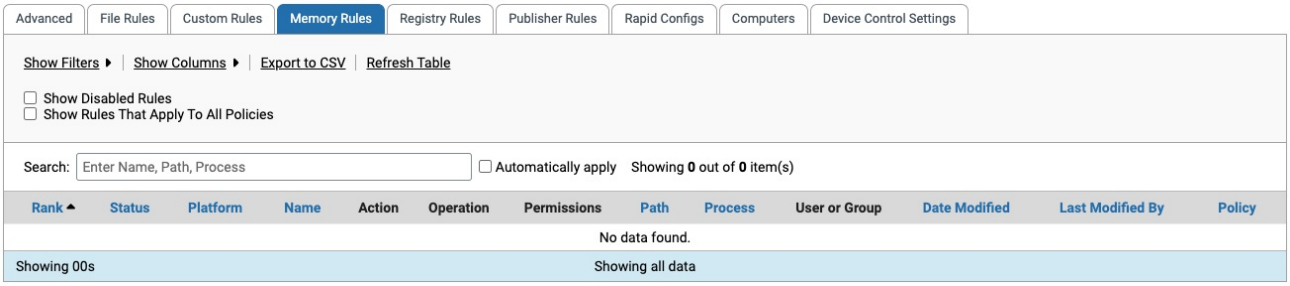
- Advanced : 개별적으로 등록되는 타 정책과 달리 전체 범위에서의 특정 동작에 대한 파일/스크립트 허용 및 차단
  - Active : 활성화
  - Off : 비활성화
  - Report Only : 정책 테스트 - 파일 차단에 대한 로그 기록



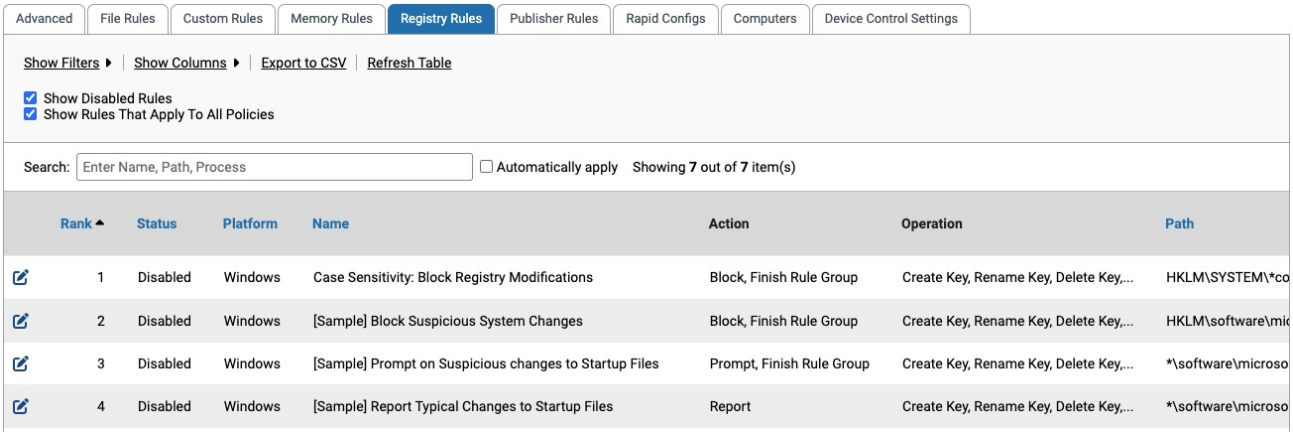
- File Rules : 엔드포인트 설치 시 검출된 파일 또는 사용자가 등록한 개별 파일 해시 값을 통한 파일 승인 및 차단
  - Approval : 파일 실행 허용
  - Ban : 파일 실행 차단
  - Ban (Monitor) : 파일 실행에 대한 이벤트 발생



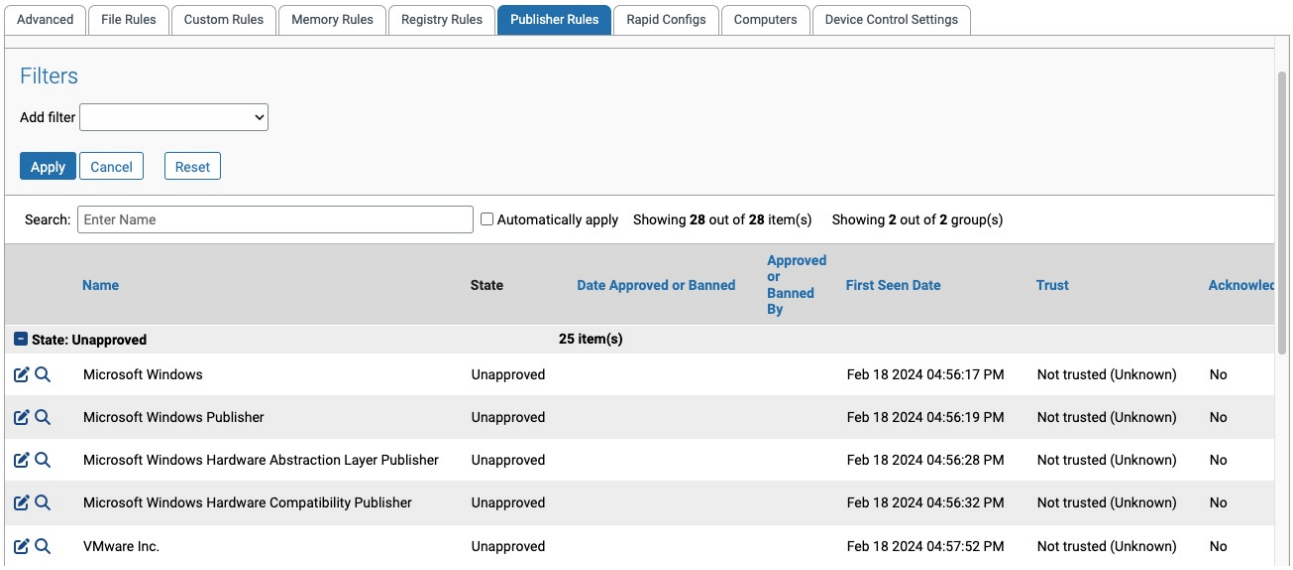
- Custom Rules : 사용자가 소프트웨어 프로세스 행위에 대한 작업 규칙



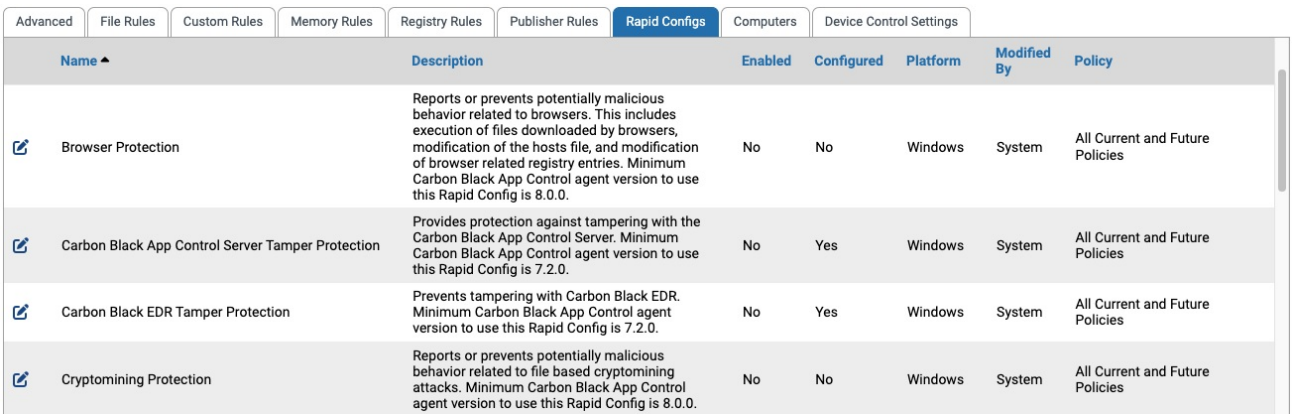
- Memory Rules : 사용자나 프로세스가 특정 프로세스의 메모리에 접근하거나 변경하는 등의 행위 허용 및 차단



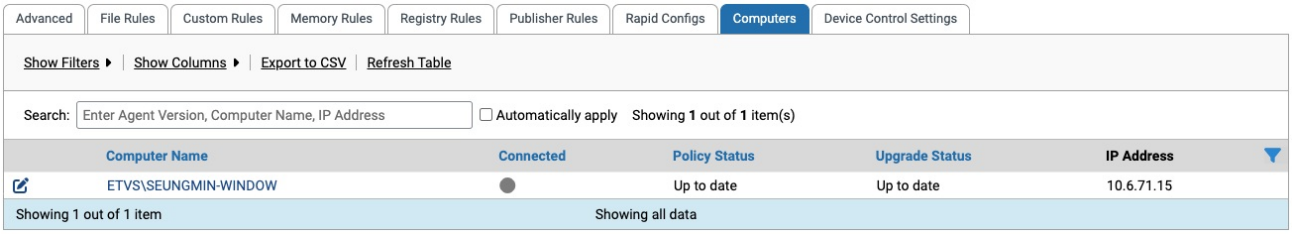
- Registry Rules : Windows OS에서 특정 레지스트리를 변경하는 행위 허용 및 차단



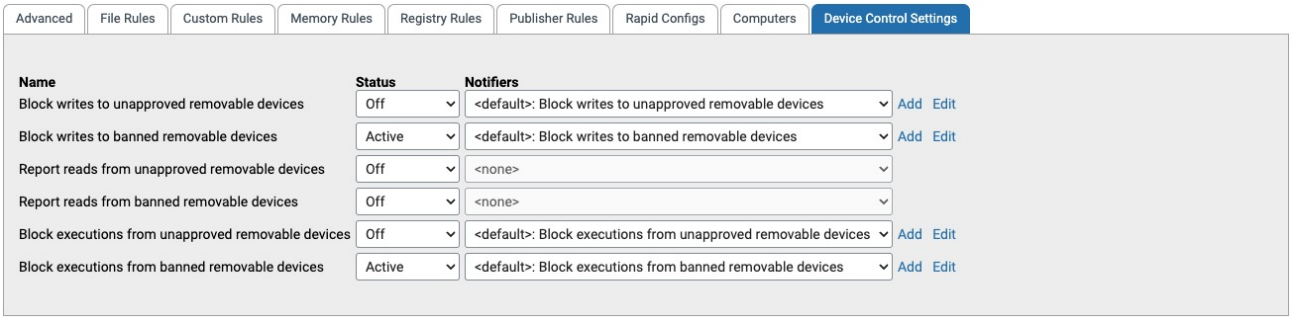
- Publisher Rules : Windows 및 MAC 에서 사용되는 소프트웨어 인증서에 대한 승인 및 미승인 규칙 정의하여 파일 허용 및 차단



- Rapid Configs : 세부적인 정책을 적용하기 전, 신속하게 엔드포인트 보호 환경을 정의하기 위한 정책 적용



- Computers : 정책이 적용된 엔드포인트 목록 확인



- Device Control Settings : 금지 및 미승인된 이동식 장치에 대한 실행 및 쓰기 행위에 대한 허용 및 차단

버전 #8
★생성 16 2월 2024 09:55:07
수정 18 4월 2025 17:06:16