kaspersky

Kaspersky Industrial CyberSecurity for Nodes 5.0

© 2026 AO Kaspersky Lab

목차

Kaspersky Industrial CyberSecurity for Nodes
- 새로운 기능
- 수정된 문제
- 배포 패키지
- 하드웨어 및 소프트웨어 요구 사항
- 지원 Kaspersky Security Center 버전
- Kaspersky 바이러스 제거 도구
- 기능 요구 사항 및 제한 사항
  - 애플리케이션 설치 및 제거
  - 시스템 무결성 모니터링
  - 방화벽
  - 오래된 Windows 버전에 대한 제한 사항
  - Kaspersky Security Center와 통합
  - 기타 제한
- 일반 배포
- 다른 애플리케이션과의 호환성

애플리케이션 설치 및 제거
- 설치 계획
  - 관리 도구 선택
  - 설치 유형 선택
  - 사용되는 포트
- 마법사를 사용하여 애플리케이션 설치 및 제거
  - 설치 마법사를 사용한 설치
    - Kaspersky Industrial CyberSecurity for Nodes 설치
    - Kaspersky Industrial CyberSecurity for Nodes 콘솔 설치
    - 다른 장치에 애플리케이션 콘솔을 설치한 후의 고급 설정
    - Kaspersky Industrial CyberSecurity for Nodes 설치 후 수행할 동작
      - 데이터베이스 및 애플리케이션 모듈 업데이트 작업 시작 및 구성
      - 중요 영역 검사
  - 구성 요소 집합 수정 및 Kaspersky Industrial CyberSecurity for Nodes 복구
  - 설치 마법사를 사용한 제거
    - Kaspersky Industrial CyberSecurity for Nodes 제거
    - Kaspersky Industrial CyberSecurity for Nodes 콘솔 제거
- 명령줄에서 애플리케이션 설치 및 설치 제거
  - 명령줄을 통한 Kaspersky Industrial CyberSecurity for Nodes 설치 및 제거 정보
  - Windows Installer 서비스용 Kaspersky Industrial CyberSecurity for Nodes 소프트웨어 구성 요소 코드
  - 설치 및 복구 설정. Windows Installer 명령줄 옵션
  - Kaspersky Industrial CyberSecurity for Nodes 설치 명령의 예
  - Kaspersky Industrial CyberSecurity for Nodes 설치 후 수행할 동작
  - 구성 요소 추가/제거. 샘플 명령
  - Kaspersky Industrial CyberSecurity for Nodes 제거. 샘플 명령
  - 반환 코드

Kaspersky Security Center를 사용하여 애플리케이션 설치 및 설치 제거
Kaspersky Security Center를 통한 설치 일반 정보
Kaspersky Industrial CyberSecurity for Nodes 설치 또는 제거할 권한
Kaspersky Security Center를 통해 Kaspersky Industrial CyberSecurity for Nodes 설치
Kaspersky Industrial CyberSecurity for Nodes 설치 후 수행할 동작
Kaspersky Security Center를 통한 애플리케이션 콘솔 설치
Kaspersky Security Center를 통해 Kaspersky Industrial CyberSecurity for Nodes 제거
Kaspersky Security Center를 사용하여 애플리케이션 구성 요소 세트 변경
Active Directory 그룹 정책을 통해 애플리케이션 설치 및 제거
Active Directory 그룹 정책을 통해 Kaspersky Industrial CyberSecurity for Nodes 설치
Kaspersky Industrial CyberSecurity for Nodes 설치 후 수행할 동작
Active Directory 그룹 정책을 통해 Kaspersky Industrial CyberSecurity for Nodes 제거
Kaspersky Industrial CyberSecurity for Nodes 설치 및 제거 로그
Kaspersky Industrial CyberSecurity for Nodes 설치 후 시스템 변경 사항
Kaspersky Industrial CyberSecurity for Nodes 프로세스
Kaspersky Industrial CyberSecurity for Nodes 기능 확인. EICAR 테스트 바이러스 사용
EICAR 테스트 바이러스 정보
실시간 파일 보호 및 온디맨드 검사 기능 확인
이전 버전의 Kaspersky Industrial CyberSecurity for Nodes를 버전 5.0로 업그레이드
Kaspersky Industrial CyberSecurity for Nodes 업데이트
Kaspersky Industrial CyberSecurity for Nodes 관리 도구 업데이트
정책 및 작업 마이그레이션
업데이트하는 애플리케이션 버전의 설정 마이그레이션
Kaspersky Industrial CyberSecurity for Nodes 버전 4.0 및 5.0의 구성 요소 및 작업에 대한 대응
Kaspersky Security Gateway 설치 및 제거
Kaspersky Security Gateway 업데이트
설치 마법사를 사용하여 Kaspersky Security Gateway 설치
1단계. 설치 요구 사항 확인
2단계. 설치 절차의 시작 페이지
3단계. 최종 사용자 라이센스 계약서 및 개인정보취급방침 보기
4단계. 대상 폴더 선택
5단계. 구성 요소 선택
6단계. SCADA 시스템에 대한 연결 구성
7단계. Kaspersky Security Gateway 설치
명령줄에서 Kaspersky Security Gateway 설치
Kaspersky Security Gateway 제거
1단계. 나중에 사용하기 위해 Kaspersky Security Gateway 데이터 저장
2단계. Kaspersky Security Gateway 제거
OPC Core Components Redistributables 설치
애플리케이션 인터페이스
관리 플러그인 작업
Kaspersky Security Center에서 Kaspersky Industrial CyberSecurity for Nodes 관리
애플리케이션 설정 관리
Kaspersky Security Center에서 일반 애플리케이션 설정 구성
Kaspersky Security Center에서 인터페이스 및 검사 설정 구성
Kaspersky Security Center에서 보안 설정 구성

Kaspersky Security Center를 사용하여 연결 설정 구성
로컬 작업 실행 모드 구성
Kaspersky Security Center에서 격리 및 백업 설정 구성
정책 만들기 및 구성
정책 만들기
정책 구성
Kaspersky Security Center를 사용하여 작업 만들기 및 구성
Kaspersky Security Center에서 작업 만들기 정보
Kaspersky Security Center를 사용하여 작업 만들기
개별 컴퓨터에 대한 로컬 작업 설정 및 일반 애플리케이션 설정으로 이동
Kaspersky Security Center에서 그룹 작업 구성
애플리케이션 활성화 작업
업데이트 작업
애플리케이션 무결성 제어
작업 예약
Kaspersky Security Center 리포트
실시간 보호 상태
Kaspersky Industrial CyberSecurity for Nodes 콘솔 작업
애플리케이션 콘솔 시작
Kaspersky Industrial CyberSecurity for Nodes 콘솔 인터페이스
Kaspersky Industrial CyberSecurity for Nodes 콘솔 창
알림 영역의 시스템 트레이 아이콘
애플리케이션 콘솔을 통해 일반 설정 구성
Kaspersky Industrial CyberSecurity for Nodes 작업 관리
Kaspersky Industrial CyberSecurity for Nodes 작업 카테고리
수동으로 작업 시작, 일시 중지, 다시 시작, 중지
작업 예약
사용자 계정을 사용하여 작업 시작
계정을 사용한 작업 시작 정보
작업을 시작할 사용자 계정 지정
설정 가져오기 및 내보내기
설정 가져오기 및 내보내기 정보
설정 내보내기
설정 가져오기
보호 상태 및 Kaspersky Industrial CyberSecurity for Nodes 정보 보기
애플리케이션 콘솔에서 백업 설정을 구성하는 방법
웹 콘솔에서 웹 플러그인 작업
웹 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 관리
웹 플러그인 제한 사항
애플리케이션 설정 관리
웹 플러그인에서 일반 애플리케이션 설정 구성
웹 플러그인에서 인터페이스 및 검사 설정 구성
웹 플러그인에서 보안 및 신뢰성 설정 구성
웹 플러그인에서 연결 설정 구성
웹 플러그인에서 로컬 작업의 예약된 시작 구성
웹 플러그인에서 격리 및 백업 설정 구성
정책 만들기 및 구성

- Kaspersky Security Center를 사용하여 작업 만들기 및 구성
  - 웹 플러그인의 작업 생성 정보
  - 웹 플러그인에서 작업 생성
  - 웹 플러그인에서 그룹 작업 구성
    - 웹 플러그인에서 애플리케이션 활성화 작업 구성
    - 웹 플러그인에서 업데이트 작업 구성
  - 작업 예약
- Kaspersky Security Center 리포트

애플리케이션 라이센스

- 최종 사용자 라이센스 계약서 정보
- 라이센스 정보
- 라이센스 인증서 정보
- 키 정보
- 키 파일 정보
- 활성화 코드 정보
- 키 파일로 애플리케이션 활성화
- 활성화 코드로 애플리케이션 활성화
- 현재 라이센스 정보 보기
- 라이센스 갱신
- 키 삭제

Kaspersky Industrial CyberSecurity for Nodes 시작 및 중지

- 애플리케이션 시작 및 중지
- 컴퓨터 보호 및 제어 일시 중지 및 다시 시작

간편 진단 인터페이스

- 간편 진단 인터페이스 정보
- 간편 진단 인터페이스를 통해 Kaspersky Industrial CyberSecurity for Nodes 상태 검토
- 보안 이벤트 통계 검토
- 현재 애플리케이션 활동 검토
- 애플리케이션 추적 로그 및 메모리 덤프 기록 구성

Kaspersky Industrial CyberSecurity for Nodes 자기 보호

- 자기 보호 기능 작동 및 중지
- AM-PPL 기술 지원
- 운영 체제 서비스 보호하기
- Kaspersky Industrial CyberSecurity for Nodes를 관리하기 위한 사용자 권한 구성
- Kaspersky Industrial CyberSecurity for Nodes 서비스를 관리하기 위한 사용자 접근 권한 구성
- Kaspersky Industrial CyberSecurity for Nodes 기능 접근을 암호로 보호
- Secure Desktop 알림

신뢰 구역

- 검사 예외 생성
- 탐지 가능한 개체의 유형 선택
- 신뢰하는 애플리케이션 목록 편집
- 로컬 신뢰 구역 생성
- 신뢰 구역 내보내기 및 가져오기
- 신뢰하는 시스템 인증서 저장소 사용
- 사전 정의된 검사 예외 및 신뢰하는 애플리케이션
- 산업용 소프트웨어 예외 프로필

실시간 파일 보호
작업 보호 범위 및 보안 설정 정보
사전 정의된 보호 범위
사전 정의된 보안 레벨 정보
실시간 파일 보호 구성 요소에서 기본으로 검사하는 파일 확장자
실시간 파일 보호 구성 요소 구성
실시간 파일 보호 구성 요소의 보호 범위 구성
보안 설정 수동 구성
컨테이너 검사
KSN 사용
Kaspersky Security Network 사용 활성화
Kaspersky Security Network 사용 통계
Kaspersky Private Security Network의 제한 사항
KSN 프록시 설정
익스플로잇 방지
익스플로잇 방지 모드
익스플로잇 방지 사용 및 중지
메모리 보호 활성화 및 비활성화
보호 중인 프로세스 목록 생성
복원 엔진
Anti-Cryptor
로컬 폴더에 대한 암호화 보호 활성화 및 비활성화
외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호
외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 사용 및 중지
보호 범위 편집
외부 데이터 암호화를 위해 신뢰하는 컴퓨터 추가
신뢰하지 않는 컴퓨터의 차단 기간 구성
외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 시 예외 규칙 목록 내보내기 및 가져오기
네트워크 위협 보호
네트워크 위협 보호 사용 및 구성
차단 예외 생성
외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 시 예외 규칙 목록 내보내기 및 가져오기
AMSI 스캐너
AMSI 스캐너 사용 및 중지
AMSI 스캐너 설정
애플리케이션 실행 제어
애플리케이션 실행 제어 규칙 정보
소프트웨어 배포 제어 정보
애플리케이션 실행 제어를 위한 규칙 생성기 정보
애플리케이션 실행 제어 활성화 및 구성
소프트웨어 배포 제어 구성
애플리케이션 실행 제어 규칙 작업 방법
애플리케이션 실행 제어 규칙 추가
애플리케이션 실행 제어 규칙의 트리거 조건 추가
애플리케이션 실행 제어 규칙 범위에서 예외 추가
모든 애플리케이션 실행 허용

애플리케이션 실행 제어 규칙 내보내기
Kaspersky Security Center에서 차단된 애플리케이션 이벤트를 선택하여 텍스트 파일 생성
애플리케이션 실행 제어를 위한 규칙 생성기 그룹 작업 구성
애플리케이션 실행 제어를 위한 규칙 생성기 그룹 작업을 사용하여 규칙 생성.
장치 제어
장치 접근 규칙
유형별 장치 접근 관리
Wi-Fi 연결 제어
인쇄 제어
입력 장치 제어(HID)
모바일 장치에 대한 액세스 관리
이동식 드라이브 사용 감시
Bluetooth 장치에 대한 접근 관리
장치에 대한 사용자 접근 권한의 구분
장치 제어를 위한 규칙 생성기 정보
신뢰하는 장치 추가
신뢰하는 장치 목록 내보내기 및 가져오기
방화벽
방화벽 규칙 정보
방화벽 구성
일반 방화벽 설정 구성
방화벽 규칙 생성 및 구성
방화벽 규칙의 활성화와 비활성화
BadUSB 공격 방지
시스템 무결성 모니터링
시스템 무결성 모니터링 규칙 정보
실시간 시스템 무결성 모니터링
온디맨드 시스템 무결성 검사
시스템 무결성 모니터링 규칙 내보내기 및 가져오기
시스템 무결성 모니터링 리포트 보기
로그 검사
사용자 지정 규칙 추가
사전 정의된 규칙 구성
성능 분석기
온디맨드 검사
온디맨드 검사 작업 정보
작업 검사 범위 및 보안 설정 정보
사전 정의된 검사 범위
온라인 저장소 파일 검사
사전 정의된 보안 레벨 정보
이동식 드라이브 검사
온디맨드 검사 작업 설정 기본값
온디맨드 검사 작업 관리
온디맨드 검사 작업 만들기
백그라운드에서 온디맨드 검사 작업 실행
중요 영역 검사 실행 등록
온디맨드 검사 작업의 검사 범위 구성

온디맨드 검사 작업 설정 구성
이동식 드라이브 검사 구성
온디맨드 검사 작업에 대해 사전 정의된 보안 레벨 선택
보안 설정 수동 구성
온디맨드 검사 작업 통계
산업 네트워크 보호
PLC 프로젝트 무결성 검사 정보
PLC 프로젝트 무결성 검사 작업 구성
PLC 프로젝트 조사 구성
PLC 프로젝트 무결성 검사 구성
PLC 프로젝트 무결성 검사 활성화 및 비활성화
PLC 구성 레지스트리 정보
PLC 레지스트리 구성
보안 감사
보안 감사 작업 설정 제한 사항
지원하는 OVAL 검사 유형
보안 감사 작업 관리
기본 설정으로 보안 감사 작업 생성 및 구성
SCADA용 Kaspersky ICS CERT 취약점 데이터베이스를 사용하여 보안 감사 작업 설정 구성
보안 및 표준 준수 구성을 사용하여 보안 감사 작업 설정 구성
Kaspersky Security Center 저장소에서 사용자 지정 규칙 데이터베이스를 사용하여 보안 감사 작업 설정 구성
파일에서 사용자 지정 데이터베이스를 사용하여 보안 감사 작업 설정 구성
보안 감사 작업 실행 결과 보기
보안 감사 작업 실행 결과를 별도의 파일로 내보내기
OVAL 및 XCCDF 규칙을 사용하는 파일 서명용 인증서 지문 생성
사용자 지정 OVAL 및 XCCDF 규칙을 사용하여 Kaspersky Security Center 설치 패키지 생성
Kaspersky Security Gateway 사용
진단 정보
Kaspersky Security Gateway의 제한 사항 및 알려진 문제
Kaspersky Security Gateway Console 인터페이스
Kaspersky Security Center와의 연결 구성
Kaspersky Industrial CyberSecurity for Networks와의 연결 구성
DCOM 프로토콜 구성
통신 프로토콜을 사용하여 데이터 전송 설정 구성
IEC 60870-5-104 프로토콜을 사용하여 데이터 전송 구성
OPC DA 프로토콜을 사용하여 데이터 전송 구성
OPC UA 프로토콜을 사용하여 데이터 전송 구성
구성 파일을 사용하여 데이터 전송 구성
Kaspersky Security Gateway 추가 설정 구성
Kaspersky Security Gateway 이벤트 보기
BitLocker 전체 디스크 암호화 관리
BitLocker 드라이브 암호화 시작
BitLocker로 보호되는 하드 드라이브 복호화
BitLocker로 보호되는 드라이브에 대한 접근 복원
소프트웨어 업데이트를 위해 BitLocker 보호 일시 중지

타사 시스템과 통합
시스템 모니터용 성능 카운터
리소스 부족으로 처리되지 않은 요청 수
처리 제출 요청 수
초당 처리된 개체 수
감염된 개체 대기열의 요소 수
거부된 총 요청 수
건너뛴 총 요청 수
최대 파일 가로채기 디스패처 스트림 수
평균 파일 가로채기 디스패처 스트림 수
Kaspersky Industrial CyberSecurity for Nodes SNMP 카운터 및 트랩
Kaspersky Industrial CyberSecurity for Nodes SNMP 카운터
성능 카운터
백업 카운터
일반 카운터
업데이트 카운터
실시간 파일 보호 카운터
AMSI 스캐너 카운터
Kaspersky Industrial CyberSecurity for Nodes SNMP 트랩 및 해당 옵션
Kaspersky Industrial CyberSecurity for Nodes SNMP 트랩 옵션 설명 및 가능한 값
WMI 통합
Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 소프트웨어 모듈 업데이트
데이터베이스 및 애플리케이션 모듈 업데이트
업데이트 작업 정보
Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 모듈 업데이트 구성
업데이트 작업 구성
애플리케이션의 SMU 업데이트
애플리케이션 데이터베이스의 보안 복사
애플리케이션 데이터베이스의 보안 업데이트
Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 업데이트 롤백
업데이트 작업 통계
Detection and Response 솔루션
Kaspersky Industrial CyberSecurity Endpoint Detection and Response
솔루션 아키텍처
Kaspersky 애플리케이션과의 호환성
배포 및 초기 설정
솔루션 활성화
경고 세부 정보를 보기 위한 위협 리포트 구성
EDR 경고 위젯 추가
장치에서 솔루션 성능 모니터링
확장 기능이 포함된 Kaspersky Industrial CyberSecurity Endpoint Detection and Response로 업그레이드
대응 조치
장치의 네트워크 격리
IOC 검사
IOC 파일 요구 사항
IOC 검사를 위한 확장 원격 측정
레지스트리에서의 IOC 검사 범위(RegistryItem)

중요 영역 검사 실행
실행 방지
프로세스 시작
프로세스 종료
파일 가져오기
파일 삭제
격리 저장소로 파일 이동
격리된 파일 보기
격리에서 Kaspersky TIP으로 파일 전송
Cloud Sandbox
경고 세부 정보 작업
경고 세부 정보 정보
경고 세부 정보 보기
네트워크 격리 적용 및 제거
경고 세부 정보에서 파일을 격리로 이동
경고 세부 정보에서 IOC 검사 작업 생성
경고 세부 정보에서 개체 실행 방지
경고 세부 정보에서 Active Directory 사용자에 대한 대응 조치
사용자 암호 재설정
사용자 계정 차단
보안 그룹에 사용자 추가
보안 그룹에서 사용자 제거
경고 세부 정보에서 사용자에게 Kaspersky ASAP 교육 과정 할당
모니터링 및 리포트
경고 목록 보기
실행 방지 규칙 트리거 정보 보기
격리된 장치 목록 보기
Endpoint Agent 모드
Endpoint Agent 모드로 Kaspersky Industrial CyberSecurity for Nodes 설치
타사 EPP 애플리케이션과의 호환성
Managed Detection and Response
MDR 통합 구성
Kaspersky Anti Targeted Attack Platform
KATA 통합 구성
원격 측정 구성
Endpoint Detection and Response Expert(on-premises)
EDR Expert (on-premises) 통합 구성
EDR Expert(on-premises) 원격 측정 설정 구성
EDR Expert(on-premises) 원격 측정 예외
EDR Expert(on-premises) 이벤트 필터 내보내기 및 가져오기
YARA 검사
EDR 원격 측정 예외 규칙
Kaspersky Industrial CyberSecurity for Networks 통합
Kaspersky Industrial CyberSecurity for Networks 통합 관련 특별 고려 사항 및 제한 사항
Wi-Fi 네트워크 모니터링 구성
EDR 동작 모니터링

- Kaspersky Endpoint Agent
  - [KICS+KEA] 구성을 [KICS+내장 Endpoint Agent] 구성으로 마이그레이션
  - [KICS+KEA] 구성의 정책 및 작업을 [KICS+내장 에이전트] 구성으로 마이그레이션
- SIEM 통합
  - SIEM로 전송할 이벤트 필터링
  - 원격 측정 이벤트 필터링 규칙 내보내기 및 가져오기
- Sigma 규칙을 사용한 이상 행위 탐지
  - 시그마 규칙을 사용한 이상 행위 탐지의 특별 고려 사항 및 제한 사항
  - Sigma 규칙을 사용한 이상 행위 탐지 활성화
  - 사용자 지정 컬렉션에 Sigma 규칙 추가
  - 규칙 컬렉션 내에서 Sigma 규칙 필터링
  - 사용자 지정 컬렉션의 Sigma 규칙 내보내기 및 가져오기
  - Sigma 규칙 변경
  - Sigma 규칙의 예외
- 개체 격리 및 백업
  - 감염 의심 개체 격리. 격리 저장소
    - 격리 개체 보기
      - 격리된 개체 정렬
      - 격리된 개체 필터링
    - 격리된 개체 복원
    - 격리 저장소에서 개체 삭제
    - 분석을 위해 Kaspersky로 감염 의심 개체 보내기
    - 격리 설정 구성
  - 개체의 백업 복사본 만들기. 백업
    - 백업에서 개체 보기
      - 백업에서 파일 정렬
      - 백업에서 파일 필터링
    - 백업 저장소에서 파일 복원
    - 백업에서 파일 삭제
    - 백업 설정 구성
    - 백업 통계
  - 처리되지 않은 위협 제거
  - 네트워크 리소스에 대한 접근을 차단합니다. 차단된 네트워크 세션
    - 차단된 네트워크 세션 목록
    - 차단된 네트워크 세션 목록 관리
- 이벤트 등록. Kaspersky Industrial CyberSecurity for Nodes 로그
  - Kaspersky Industrial CyberSecurity for Nodes 이벤트를 등록하는 방법
  - 로그 설정 구성
    - 로그에서 이벤트 정렬
    - 로그에서 이벤트 필터링
    - 로그에서 이벤트 삭제
    - 로그에서 정보 내보내기
  - 시스템 감사 로그
  - 구성 요소 및 작업 로그
    - 작업 로그에서 Kaspersky Industrial CyberSecurity for Nodes 작업에 대한 통계 및 정보 보기
  - 이벤트 뷰어에서 Kaspersky Industrial CyberSecurity for Nodes의 이벤트 로그 보기

- 관리자 및 사용자 알림 방법
  - 관리자 및 사용자 알림 구성
  - 이메일 알림 구성
- 관리 서버와의 상호 작용 구성
- 인시던트 생성 구성

Portable Auditor
- 하드웨어 및 소프트웨어 요구 사항
- Portable Auditor 기능 제한
- Portable Auditor 생성
- Portable Auditor 업데이트
- Portable Auditor 콘솔 사용
- 장치 검사
  - 악성 코드 검사 작업 설정
  - 보안 감사 작업 설정
  - 네트워크 트래픽 기록 작업 설정
  - 작업 설정 가져오기 및 내보내기
- 라이센스 정보 보기
- 검사 결과 보기
  - 휴대용 감사기 결과 파일 및 스토리지
  - 일반 휴대용 감사기 리포트 보기
- Portable Auditor 데이터베이스 업데이트
- Portable Auditor 추적 로그 및 메모리 덤프 기록 구성
- 명령줄을 사용하여 Portable Auditor Console 사용
  - 보안 이동식 드라이브에서 Portable Auditor 결과 내보내기
- 보안 이동식 드라이브 접근 차단

명령줄에서 Kaspersky Industrial CyberSecurity for Nodes 관리
- APPCONTROL. 애플리케이션 실행 제어 규칙 가져오기
- APPCONTROL /CONFIG. 애플리케이션 실행 제어 구성 요소 구성
- APPCONTROL /GENERATE. 애플리케이션 실행 제어를 위한 규칙 생성기
- CONFIG. AM-PPL 기술 지원
- CREATEPORTABLE. Portable Auditor 생성
- DEVCONTROL. 장치 제어 규칙 가져오기
- DUMP. 메모리 덤프 기록
- EDR_EXPERT_ON_PREM. EDR Expert(on-premises) 통합
- EDRKATA. KATA 통합
- EXITPOLICY. 장치에서 정책 비활성화
- EXPORT. 애플리케이션 설정 내보내기
- FBRESET. iSwift 데이터베이스 지우기
- FIM /BASELINE. 베이스라인 시스템 무결성 모니터
- HELP. 명령 도움말 표시
- IMPORT. 애플리케이션 설정 가져오기
- KICS. Kaspersky Industrial CyberSecurity for Networks 통합
- ISOLATION. 네트워크 격리 관리
- KSN. KSN/KPSN 사용
- LICENSE. 애플리케이션 활성화
- MDR. Managed Detection and Response 통합 구성
- 네트워크 차단. 네트워크 차단 관리

OMSINFO. 애플리케이션 정보가 포함된 JSON 파일 생성
암호. Kaspersky Industrial CyberSecurity for Nodes 기능 접근을 암호로 보호
PATCHCOMPATIBILITYRESET. 호환되지 않는 패치 목록에서 패치 제거
성능 분석기. 성능 분석기 작업 결과 내보내기
PREVENTION. 실행 방지
REMOTEACCESS. 애플리케이션 콘솔 원격 연결 설정 관리
RESETMDRMACHINEID. 장치 ID 재설정
RESTORE. 파일 복원
ROLLBACK. 마지막 업데이트 롤백
RTP. 실시간 파일 보호
SCAN. 온디맨드 검사
SCAN-IOC. IOC 검사
SCAN-OVAL. 보안 감사
SCANCRITICAL. 중요 영역 검사
SERVERBINDINGDISABLE. 중앙 관리 서버 연결 보호 중지
SIEM. SIEM 시스템 통합
SIGMA. Sigma 규칙을 사용한 이상 행위 탐지
START. 애플리케이션 서비스 시작
STARTPOLICY. 정책 사용
STOP. 애플리케이션 서비스 중지
작업. 작업 관리
TELEMETRYFILTERS. 원격 측정 이벤트 필터링 규칙 내보내기 및 가져오기
토큰. 보안 이동식 드라이브에 대한 접근 차단 관리
TRACE. 애플리케이션 동작 추적
UPDATE. 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트
YARA. YARA 검사 실행
기술 지원 서비스에 문의
기술 지원을 요청하는 방법
Kaspersky CompanyAccount를 통한 기술 지원
기술 지원 전문가에게 확장 진단 정보 제공
애플리케이션 동작 추적
추적 파일의 내용 및 저장
메모리 덤프 기록
덤프 파일 및 추적 파일 보호
OS 데이터 가져오기(Kaspersky Get System Info)
Kaspersky Industrial CyberSecurity for Nodes에 관한 정보 출처
부록
빠른 검사를 위한 파일 확장자
애플리케이션 구성 요소 규칙의 사용자 계정
법률 정보
데이터 제공
최종 사용자 라이센스 계약서에 따른 데이터 프로비전
Detection and Response 솔루션 사용 시 데이터 제공
Kaspersky Industrial CyberSecurity Endpoint Detection and Response
Kaspersky Endpoint Detection and Response Expert(on-premises)
Kaspersky Industrial CyberSecurity for Networks 통합
SIEM 통합

Kaspersky Security Network 사용 시 데이터 제공
유럽 연합 법규(GDPR) 준수
타사 코드에 대한 정보
상표 고지

Kaspersky Industrial CyberSecurity for Nodes

*Kaspersky Industrial CyberSecurity for Nodes*는 산업 제어 시스템의 IT 위협을 처리하는 종합 서버 및 워크스테이션 보안 솔루션입니다.

이 애플리케이션은 산업용 기업 네트워크 컴퓨터의 동작을 제어하며 다음 구성 요소와 기능, 기술을 사용합니다:

- **애플리케이션 실행 제어**. 이 구성 요소는 사용자 애플리케이션 시작을 모니터링하고 애플리케이션 시작을 규제합니다.
- **장치 제어**. 이 구성 요소는 플래시 드라이브 또는 USB를 통해 연결된 기타 유형의 외부 장치를 사용하여 파일 교환을 진행하는 중에 발생할 수 있는 컴퓨터 보안 위협으로부터 컴퓨터를 보호하기 위해 외부 장치의 등록 및 사용을 제어합니다.
- **PLC 프로젝트 무결성 검사**. 이 기능은 산업 시스템에서 사용되는 프로그래밍 가능한 논리 컨트롤러(PLC) 프로젝트의 무결성을 검사하도록 설계되었습니다.

제어 구성 요소의 작동은 다음과 같은 규칙을 기반으로 합니다:

- 애플리케이션 실행 제어 구성 요소는 애플리케이션 실행 제어 규칙을 사용합니다.
- 장치 제어 구성 요소는 장치 접근 규칙 및 커넥터 버스 접근 규칙을 사용합니다.
- PLC Project Integrity Check 기능은 PLC 프로젝트 무결성 검사 규칙을 사용합니다.

각각의 위협은 별도의 구성 요소에서 처리합니다. 구성 요소는 개별적으로 작동 또는 중지하고 설정을 구성할 수 있습니다.

애플리케이션은 다음 구성 요소를 사용하여 산업 네트워크 구성 요소를 확인하고 보호합니다:

- **실시간 파일 보호**. 이 구성 요소는 컴퓨터의 파일 시스템이 감염되는 것을 방지합니다. 이 구성 요소는 Kaspersky Industrial CyberSecurity for Nodes와 함께 시작되고 컴퓨터의 RAM에서 계속 실행되며, 컴퓨터와 장착된 모든 드라이브에서 열리거나 저장되고 시작된 모든 파일을 검사합니다. 실시간 파일 보호 구성 요소는 각 파일 이벤트를 관찰하고 이 파일에 보안위협을 나타내는 바이러스 및 기타 프로그램이 있는지 확인합니다.
- **Wi-Fi 제어**. 이 구성 요소는 보호 중인 장치의 Wi-Fi 네트워크 연결 시도를 추적하고 탐지된 네트워크에 대한 연결을 차단하거나 허용합니다.
- **방화벽**. 모드에 따라 이 구성 요소는 다음 중 하나를 수행합니다: Windows 방화벽으로 트래픽 필터링 모니터링. 구성 요소의 로그에 보호 중인 컴퓨터의 네트워크 활동에 대한 이벤트만 기록. 방화벽 설정에 따라 네트워크 트래픽 필터링.
- **Anti-Cryptor**. 이 구성 요소를 사용하면 회사 네트워크의 원격 컴퓨터에서 보호 중인 장치의 네트워크 파일 리소스를 악의적으로 암호화하는 것을 탐지할 수 있습니다.
- **휴대용 감사 도구**. 이 구성 요소는 격리된 장치를 검사하고 보안 검사를 수행합니다.
- **BadUSB 공격 방지**. 구성 요소는 키보드를 에뮬레이션하는 감염된 USB 장치가 컴퓨터에 연결하지 못하도록 차단합니다.
- **파일 무결성 모니터**. Kaspersky Industrial CyberSecurity for Nodes는 작업 설정에 지정된 모니터링 범위 내에서 파일 변경을 탐지합니다. 이러한 변경은 보호 중인 장치의 보안 위반을 의미할 수 있습니다.

- **레지스트리 액세스 모니터링**. 이 구성 요소를 사용하면 작업 설정에 정의된 모니터링 범위 내 지정된 레지스트리 분기 및 키로 수행되는 동작을 모니터링할 수 있습니다.

- **로그 검사**. 이 구성 요소는 Windows 이벤트 로그 조사 결과를 기반으로 보호된 환경의 무결성을 모니터링합니다.

이 구성 요소가 제공하는 실시간 보호 외에도, 정기적으로 컴퓨터 검사를 실행하여 바이러스 및 위협을 유발할 수 있는 기타 애플리케이션을 확인할 것을 권장합니다. 이는 설정의 낮은 보호 수준이나 다른 이유로 인해 구성 요소가 탐지하지 못한 악성 코드의 확산을 방지하기 위한 것입니다.

Kaspersky Industrial CyberSecurity for Nodes를 계속 제대로 작동시키려면 프로그램의 작동 중에 활용된 데이터베이스 및 소프트웨어 모듈을 업데이트해야 합니다. 기본적으로 애플리케이션은 자동으로 업데이트되지만, 필요 시 애플리케이션 데이터베이스 및 모듈을 직접 업데이트할 수도 있습니다.

컴퓨터를 보호하기 위해 다음 작업이 진행됩니다:

- **전체 검사**. Kaspersky Industrial CyberSecurity for Nodes는 시스템 메모리, 운영 체제 시작 시 부팅되는 모든 개체, 운영 체제 백업을 포함한 운영 체제뿐만 아니라 모든 하드 및 이동식 드라이브를 철저히 확인합니다.

- **사용자 지정 검사**. Kaspersky Industrial CyberSecurity for Nodes는 사용자가 선택한 개체를 검사합니다.

- **중요 영역 검사**. Kaspersky Industrial CyberSecurity for Nodes는 운영 체제 시작 시 로드되거나 시스템 메모리에 있거나 루트킷을 포함할 수 있는 개체를 검사합니다.

- **업데이트**. Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 데이터베이스 및 모듈 업데이트를 다운로드합니다. 업데이트를 통해 바이러스 및 위협을 유발하는 기타 애플리케이션에 대한 컴퓨터 보호를 최신 상태로 유지할 수 있습니다.

Kaspersky Security Center를 통한 원격 접근

Kaspersky Security Center를 통해 Kaspersky Industrial CyberSecurity for Nodes를 시작 및 중지하고, 작업을 관리하며, 클라이언트 컴퓨터에서 프로그램 설정을 원격으로 조정할 수 있습니다.

애플리케이션 유틸리티

Kaspersky Industrial CyberSecurity for Nodes는 다양한 유틸리티를 포함합니다. 유틸리티는 애플리케이션을 최신 상태로 유지하고 애플리케이션의 지원 제공 기능을 확장하도록 설계되었습니다.

- **로그**. 애플리케이션이 작동하는 동안 각 구성 요소 및 작업의 활동은 로그에 기록됩니다. 로그는 Kaspersky Industrial CyberSecurity for Nodes의 작동과 애플리케이션이 수행한 모든 작동 중에 발생한 이벤트의 목록입니다. 문제 발생 시 Kaspersky로 로그가 전송되어 기술 지원 전문가가 분석할 수 있습니다.

- **저장소**. 바이러스 및 위협을 유발하는 기타 프로그램을 검사하는 동안 애플리케이션이 컴퓨터에서 감염 파일이나 감염 의심 파일을 탐지할 시 해당 파일을 차단합니다. Kaspersky Industrial CyberSecurity for Nodes는 감염 의심 파일을 전용 저장소인 격리 저장소로 전송합니다. Kaspersky Industrial CyberSecurity for Nodes는 치료 및 삭제된 파일의 복사본을 백업 저장소에 저장합니다. Kaspersky Industrial CyberSecurity for Nodes는 어떠한 이유로든 처리되지 않은 파일을 처리 안 된 파일 목록에 넣습니다. 파일을 검사하고, 파일을 원래 폴더로 복원하며, 파일을 수동으로 격리하고, 데이터 저장소를 비울 수 있습니다.

- **알림**. 알림 서비스는 사용자에게 이벤트와 컴퓨터의 현재 상태, Kaspersky Industrial CyberSecurity for Nodes의 작동에 관한 최신 정보를 제공합니다. 알림은 화면에 표시되거나 이메일로 전송될 수 있습니다.

- **Kaspersky Security Network**. 사용자가 Kaspersky Security Network(KSN) 참여 시 전 세계 사용자로부터 실시간으로 수집되는 파일 평판과 웹 리소스, 소프트웨어에 관한 정보를 시스템이 받아볼 수 있어 컴퓨터 보호가 향상됩니다.

- **익스플로잇 방지**. 프로세스에 주입된 보호 에이전트를 사용하여 프로세스 메모리가 악용되는 것을 보호할 수 있습니다.

- **차단된 네트워크 세션 목록**. 컴퓨터의 공유 네트워크 폴더에 접근하려는 네트워크 세션에서 악성 활동이 탐지될 경우 차단할 수 있습니다.

- **신뢰 구역**. Kaspersky Industrial CyberSecurity for Nodes에서 기본적으로 사용할 보호 또는 검사 범위 예외 목록을 생성할 수 있으며, 이는 온디맨드 검사와 실시간 파일 보호 작업, 예외 설정에서 지정한 경우 다른 작업에서 수행할 수 있습니다.

- **지원**. Kaspersky Industrial CyberSecurity for Nodes에 등록된 모든 사용자는 애플리케이션 데이터베이스 및 모듈 업데이트에 접근할 수 있으며, 이메일을 통해 애플리케이션의 설치와 구성, 사용과 관련된 질문을 Kaspersky 기술 지원 전문가에게 문의할 수 있습니다.

새로운 기능

5.0 업데이트

Kaspersky Industrial CyberSecurity for Nodes 5.0에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

- 애플리케이션은 Kaspersky Industrial CyberSecurity for Networks를 사용하는 보호 대상 장치의 사용자 계정 제어 수준을 강화하기 위해 사용자 세션 정보를 수집합니다. 사용자 세션 모니터링은 Kaspersky Industrial CyberSecurity for Networks 5.0 버전 이상에서 사용할 수 있습니다. 자세한 내용은 Kaspersky Industrial CyberSecurity for Networks 도움말을 참조하십시오.

- 이제 애플리케이션이 설치된 보호 대상 장치에서 탐지된 Wi-Fi 네트워크에 대한 데이터와 보호 대상 장치와 동일한 Wi-Fi 네트워크에 연결된 장치에 대한 데이터를 수집하여 Kaspersky Industrial CyberSecurity for Networks로 보낼 수 있습니다. Wi-Fi 네트워크 모니터링은 Kaspersky Industrial CyberSecurity for Networks 5.0 버전 이상에서 사용할 수 있습니다. 자세한 내용은 Kaspersky Industrial CyberSecurity for Networks 도움말을 참조하십시오.

- Kaspersky Industrial CyberSecurity for Networks 사용자를 위해 *파일 삭제*, *프로세스 실행*, *프로세스 종료*, *사용자 차단*, *사용자 차단 해제*, *사용자 세션 종료*, *사용자 암호 재설정*, *연결 차단*과 같은 새로운 대응 조치가 추가되었습니다. 지정된 대응 조치는 Kaspersky Industrial CyberSecurity for Networks 5.0 버전 이상에서 사용할 수 있습니다. 자세한 내용은 Kaspersky Industrial CyberSecurity for Networks 도움말을 참조하십시오.

- 휴대용 스캐너의 이름이 Portable Auditor로 변경되었습니다. 이 구성 요소에는 다음과 같은 변경 사항도 포함됩니다.

  - Portable Auditor를 관리하기 위한 전체 그래픽 사용자 인터페이스가 추가되었습니다.

  - Portable Auditor를 만들기 위한 Rutoken EDS 3.0 Flash 지원이 추가되었습니다.

  - 기본 설정을 사용하는 Portable Auditor 작업의 실행 속도가 향상되었습니다.

- 이제 지정된 주 간격으로 지정된 요일에만 예약된 작업이 실행되도록 구성할 수 있습니다. 이 스케줄은 Kaspersky Security Center 16.1 버전 이상에서 이용 가능합니다.
- 이제 정기 유지 관리 등을 수행하기 위해 선택한 시간 동안 온디맨드 검사 작업을 일시 중지할 수 있습니다.
- I/O 작업 수를 줄여 보호된 장치의 하드 드라이브 하위 시스템 성능을 최적화했습니다.
- 이제 Celeron III 및 VIA C3와 같은 구형 프로세서가 탑재된 장치에서도 애플리케이션을 실행할 수 있습니다.
- Sigma 규칙을 사용한 이상 행위 탐지 구성 요소에 이제 '네트워크 및 이동식 미디어를 통한 파일 공유 감사' 사전 정의 규칙 모음이 포함됩니다. 이 모음을 사용하면 네트워크 폴더의 파일 읽기, 쓰기 및 삭제와 로컬 노드의 이동식 미디어로 파일 복사와 관련된 이벤트를 기록할 수 있습니다.
- 이제 *PLC 프로젝트 무결성 검사* 작업에서 TREI-5B 컨트롤러가 지원됩니다.
- 이제 다음 운영 체제가 지원됩니다.
  - Windows 11 26H2
  - Windows 11 IoT 25H2
  - Windows Server 2025
- 이제 애플리케이션 콘솔에서 도메인 계정의 토큰 기반 인증이 지원됩니다. 이제 사용자 이름과 암호, 토큰 또는 스마트 카드를 사용하여 애플리케이션 기능에 접근할 수 있습니다.
- 이제 Kaspersky Endpoint Detection and Response 사용자는 새로운 원격 측정 이벤트를 사용할 수 있습니다. 이러한 새로운 이벤트는 Kaspersky EDR 솔루션을 사용한 위협 탐지 기능을 강화합니다.
- 지원되지 않는 유형의 OVAL 검사가 포함된 규칙 집합으로 *보안 감사* 작업을 시작할 때의 애플리케이션 동작을 수정했습니다. 이제 지원되지 않는 유형의 OVAL 검사가 탐지되어도 애플리케이션이 작업 실행을 중단하지 않으며, 지원되지 않는 검사에 대한 정보가 리포트에 오류로 표시됩니다.
- 확장 정책 감사는 Kaspersky Security Center 웹 콘솔 15.0 버전 이상에서 지원됩니다. 이제 정책 수정 사항을 확인하고 파일에 저장할 수 있습니다. 수정 처리에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.
- 이제 '*이 장치는 Kaspersky Industrial CyberSecurity for Nodes가 시작된 후에 사용해야 함*' 이벤트와 '*Kaspersky Industrial CyberSecurity for Nodes가 시작되기 전까지는 장치 연결이 차단됨*' 이벤트를 사용할 수 있습니다. 이제 애플리케이션이 실행되기 전에 장치가 차단되면 해당 이벤트가 생성되어 중앙 관리 서버로 전송됩니다.
- Kaspersky Industrial CyberSecurity for Networks 서버로 동기화 요청을 보내는 기본 간격이 5분에서 1분으로 변경되었습니다.
- Kaspersky Industrial CyberSecurity for Nodes 버전을 개발할 때 비공개 패치(PF23040, PF23051, PF23065, PF23087, PF23100, PF23106)에 포함된 변경 사항을 통합했습니다.

4.5 업데이트

Kaspersky Industrial CyberSecurity for Nodes 4.5에 구현된 새로운 기능 및 개선 사항은 다음과 같습니다.

- Kaspersky Security Center를 사용하여 애플리케이션을 관리하기 위한 애플리케이션 콘솔 및 플러그인의 사용자 인터페이스를 대대적으로 업데이트했습니다.
- Windows 11 24H2 지원
- 이제 애플리케이션 콘솔에서 애플리케이션이 설치된 컴퓨터에 연결하는 데 사용하는 포트를 변경할 수 있습니다.
- *신뢰 구역*에서 다음을 수행할 수 있습니다:
  - 애플리케이션을 설치하고 Kaspersky Security Center를 사용하여 애플리케이션 관리 정책을 생성할 때 산업용 애플리케이션에 대한 예외 프로필을 편집합니다.
  - 신뢰하는 프로세스를 더 세세하게 구성합니다.
  - 신뢰하는 인증서 저장소를 사용합니다.
- 애플리케이션을 관리할 수 있는 사용자 및 그룹 권한에 대한 새로운 설정.
- 새로운 *Anti-Rootkit* 구성 요소. 실시간 파일 보호를 활성화하면 이 구성 요소가 기본적으로 활성화됩니다. 이 구성 요소는 설치 중에, Kaspersky Industrial CyberSecurity for Nodes의 애플리케이션 구성 요소 변경 작업을 사용하여, 혹은 애플리케이션 설치 패키지 속성을 통해 비활성화할 수 있습니다.
- *익스플로잇 방지* 설정에서 이제 애플리케이션이 보호 프로세스를 자동 식별할 수 있습니다.
- 새로운 *복원 엔진* 구성 요소.
- *Anti-Cryptor* 구성 요소는 공유 폴더 및 로컬 폴더를 모니터링합니다.
- *애플리케이션 실행 제어* 구성 요소를 개편했습니다.
  - 구성 요소의 설정 구조를 대대적으로 변경했습니다.
  - 이제 드라이브 유형, KL 카테고리, KSN 그룹을 사용하여, 조건 및 예외를 트리거하는 애플리케이션 실행 제어 규칙을 지정할 수 있습니다.
- *장치 제어* 구성 요소를 개편했습니다.
  - 기본적으로 *장치 제어* 구성 요소가 모든 장치의 연결을 허용하도록 구성됩니다.
  - *Wi-Fi 제어*가 이제 별도의 구성 요소가 아니라 장치 제어의 일부입니다.
  - 연결 버스에 따라 연결된 장치를 제어하는 기능이 추가되었습니다.
  - 이전 버전의 애플리케이션에서 버전 4.3으로 업그레이드 시 이동식 드라이브에 대한 접근 설정 마이그레이션이 추가되었습니다.
- *방화벽 관리* 구성 요소가 *방화벽* 구성 요소로 개편되었으며, 이 구성 요소는 이제 Windows 방화벽에 접속하는 것 외에 방화벽의 기능도 수행합니다.

- *파일 무결성 모니터* 및 *레지스트리 접근 모니터링* 구성 요소의 기능이 새로운 *시스템 무결성 모니터링* 구성 요소로 통합되었습니다. 이러한 개선을 통해 파일 시스템 및 Windows 레지스트리의 변경 사항을 효율적으로 추적하여, 데이터의 무단 수정을 방지할 수 있습니다.

- 이제 Kaspersky Endpoint Agent 기능이 이제 내장 Endpoint Agent(Detection and Response)로 애플리케이션에 통합됩니다.

- SIEM으로의 전송을 위한 이벤트 구성이 확장되었습니다. 이제 Kaspersky Industrial CyberSecurity for Nodes는 Windows 이벤트 로그 이벤트 보내기를 지원합니다.

- 애플리케이션이 개별 구성 요소 스케줄을 지원하지 않습니다. 이 구성 요소를 활성화하면 애플리케이션이 실행되는 동안 계속 실행됩니다.

- 이제 Kaspersky Security Center Windows 15.1을 지원합니다.

- 추가된 그룹 작업:

  - Kaspersky Endpoint Agent 기능 구현: 보안 감사, 프로세스 실행, 프로세스 종료, IOC 검사, 파일 가져오기, 격리 저장소로 파일 이동, 파일 삭제.

  - 기타 작업:

    - 중앙 관리 서버 연결 보호

    - Kaspersky Industrial CyberSecurity for Nodes 구성 요소 변경

    - 베이스라인 파일 무결성 모니터 대신 베이스라인 시스템 무결성 모니터

    - 업데이트 복사 대신 업데이트, 애플리케이션 데이터베이스 업데이트, 소프트웨어 모듈 업데이트

    - 애플리케이션 데이터베이스 업데이트 롤백 대신 업데이트 롤백

    - 키 제거

- 이제 Kaspersky Industrial CyberSecurity for Networks로 전송되는 레벨 L2의 네트워크 통신 이벤트에 트래픽이 전달되는 네트워크 인터페이스의 IPv4 주소(adapter.address 필드)가 포함됩니다.

- Kaspersky Industrial CyberSecurity for Networks 솔루션과의 통합이 용이해졌습니다. Kaspersky Industrial CyberSecurity for Nodes 4.5 버전부터 다음 유형의 구성이 지원됩니다.

  - ARP 테이블

  - 라우팅 테이블

  - 암호 정책

  - 보안 감사 정책

  - 확장된 감사 정책

- 이제 Kaspersky Industrial CyberSecurity for Networks 통합 설정을 통해 애플리케이션 및 호스트의 네트워크 인터페이스에 대한 무차별 모드를 구성할 수 있으며, 이를 통해 확장 원격 측정을 Kaspersky Industrial CyberSecurity for Networks로 전송할 수 있습니다.

- 공유 폴더 및 로컬 호스트에 연결된 장치의 파일 작업(읽기, 쓰기, 삭제)에 대한 정보를 이제 Kaspersky Industrial CyberSecurity for Networks 서버로 전송할 수 있습니다. 파일 작업에 대한 정보를 가져오려면 해당 시그마 규칙의 모음이 필요합니다. Kaspersky Industrial CyberSecurity for Networks는 수신된 정보를 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 실행하는 컴퓨터의 네트워크 공유 간에 복사되는 파일이나 네트워크 공유에서 Kaspersky Industrial CyberSecurity for Nodes에 연결된 장치로 복사되는 파일의 인스턴스를 탐지합니다.

- Kaspersky Security Center 웹 콘솔에서 애플리케이션이 설치된 호스트 속성의 Detection and Response 섹션에서 이제 Kaspersky Industrial CyberSecurity for Nodes 위협 대응 기록을 호스트를 관리하는 다른 솔루션의 대응 기록과 함께 볼 수 있습니다.

- Kaspersky의 Endpoint Detection and Response(EDR) 솔루션 사용자는 다음과 같은 기능 및 개선 사항을 사용할 수 있습니다.

  - 새로운 데이터로 경고 세부 정보를 작성합니다. 이제 경고 세부 정보에는 EDR 위협에 대응할 때 애플리케이션이 작동하는 방식을 포함하여 위협에 대한 자세한 정보가 포함됩니다.

  - 이제 경고 세부 정보에서 네트워크 격리를 관리할 수 있습니다. 또한 경고 세부 정보에서 컴퓨터 네트워크 격리 기간을 지정하고 예외 규칙을 추가할 수 있습니다.

  - IOC 파일 처리를 개선했습니다. 이제 Kaspersky Security Center 웹 콘솔 인터페이스에서 IOC 파일의 내용을 보고 편집할 수 있습니다. IOC 파일을 로드하면 애플리케이션이 IOC 용어 애플리케이션에 대한 리포트를 표시합니다.

  - 탐지된 IOC에 대한 대응을 개선했습니다. 이제 작업 속성의 IOC 탐지 결과에서 *IOC 검사* 작업이 탐지한 파일을 격리할 수 있습니다. 작업 속성에서 네트워크에서 컴퓨터를 격리할 수도 있습니다.

  - 이제 TXT 파일에서 생성된 파일 해시, IP 주소 또는 DNS 이름 목록을 기반으로 *IOC 검사* 작업의 속성에서 직접 IOC 파일을 생성할 수 있습니다.

  - *IOC 검사* 작업을 위한 확장된 검사 범위. 이제 레지스트리의 IOC 검사 범위를 정의할 수 있습니다(**Windows 레지스트리 – RegistryItem**). 이전 버전의 애플리케이션에서는 레지스트리에서 사전 정의한 IOC 검사 범위만 사용할 수 있었습니다.

- *네트워크 위협 보호* 구성 요소는 네트워크 트래픽을 모니터링하여 포트 검사와 고강도 네트워크 요청을 탐지할 수 있습니다.

- 애플리케이션 콘솔의 **원격 측정 수집 서버** 섹션에서 이제 다음 통합을 구성할 수 있습니다.

  - Kaspersky Endpoint Detection and Response Expert(on-premise)와의 통합

  - KICS for Networks와 통합

  - SIEM 통합

- KICS for Networks와 통합의 일부로 소프트웨어 데이터 다이오드에 내장된 MQTT 브로커 서버로 원격 측정을 전송할 수 있습니다.

- *PLC 프로젝트 무결성 검사* 작업에 Allen-Bradley ControlLogix PLC에 대한 지원이 추가되었습니다.

- *성능 분석기* 도입. 성능 분석기는 장치의 파일 및 애플리케이션에 대한 액세스의 정보를 수집하고 분석하는 작업입니다. 이 정보는 애플리케이션이 산업용 소프트웨어 성능에 미치는 영향을 최소화하기 위해 신뢰 구역을 정의하는 데 도움이 될 수 있습니다.

- Sigma 규칙을 사용한 이상 행위 탐지 구성 요소에 대해 다음과 같은 새로운 모음을 사용할 수 있습니다.

  - *Windows 로그를 사용하는 사용자 활동 모니터링 규칙 모음*. 이 모음을 사용하면 새 사용자 추가, 사용자 권한 상승, 사용자 시스템 로그인 등의 이벤트를 등록할 수 있습니다.

  - *SIMATIC PCS7, Siemens STEP7, Siemens TIA Portal, Siemens WinCC 소프트웨어를 사용할 때 의심스러운 활동을 탐지하기 위한 규칙 모음*.

  - *Yokogawa CENTUM VP, ProSafe-RS 시스템을 사용할 때 의심스러운 활동을 탐지하기 위한 규칙 모음*.

- 애플리케이션은 설정을 저장하기 전에 제어 구성 요소의 구성을 확인합니다. 애플리케이션 실행 제어, 장치 제어, 시스템 무결성 모니터링 구성 요소에 대한 검사가 추가되었습니다. 이제 애플리케이션은 제어 구성 요소의 현재 설정이 컴퓨터의 부하를 증가시키거나 시스템 오류를 유발할 수 있는 경우 경고를 표시합니다. 예를 들어 애플리케이션 실행 제어의 경우, 허용한 애플리케이션을 제외한 모든 애플리케이션을 차단하는 모드를 선택하고 허용 규칙을 추가하지 않으면 이러한 구성이 시스템 오류를 유발할 수 있으므로 애플리케이션에서 경고를 표시합니다.

- 새로운 구성 요소를 추가했습니다.

  - *Managed Detection and Response for ICS*. 이 구성 요소는 Kaspersky Managed Detection and Response for Industrial Control Systems 솔루션과의 상호 작용을 원활하게 합니다. *Kaspersky Managed Detection and Response(MDR)* 솔루션은 산업용 인프라에서 보안 인시던트를 자동으로 감지하고 분석합니다. 이를 위해 MDR은 엔드포인트 및 기계 학습에서 수신한 원격 측정 데이터를 사용합니다. MDR은 인시던트 데이터를 Kaspersky 전문가에게 보냅니다. 그러면 전문가는 인시던트를 처리하고, 안티 바이러스 데이터베이스에 새 항목 추가 등의 행동을 할 수 있습니다.

  - *BadUSB 공격 방지* BadUSB 공격 방지 구성 요소는 키보드를 에뮬레이션하는 감염된 USB 장치가 컴퓨터에 연결하지 못하도록 차단합니다. 컴퓨터에 운영 체제가 키보드로 식별하는 USB 장치가 연결되면 애플리케이션은 사용자에게 키보드에 코드를 입력하여 키보드를 인증하라는 메시지를 표시합니다.

  - *BitLocker 전체 디스크 암호화*. BitLocker는 Windows 운영 체제에 내장된 암호화 기술입니다. Kaspersky Industrial CyberSecurity for Nodes를 사용하면 Kaspersky Security Center를 통해 Bitlocker를 제어하고 관리할 수 있습니다.

- Kaspersky Security Gateway를 통해 SCADA 시스템으로 데이터를 전송하기 위한 *OPC UA* 프로토콜 지원. IEC 60870-5-104 및 OPC DA 프로토콜 외에도 이제 애플리케이션에서 OPC UA 프로토콜을 지원하여 플랫폼 간 호환성을 제공합니다.

- Windows XP 및 Windows XP SP1에서 휴대용 스캐너 지원. 휴대용 스캐너는 격리된 장치에서 바이러스 및 기타 위협을 검사할 수 있습니다.

- *PLC 프로젝트 조사* 작업은 이제 Siemens SIMATIC S7-1200/1500 컨트롤러에 대한 인증을 지원합니다. 이제 작업 속성에서 이러한 PLC 모델의 연결에 대한 암호를 입력할 수 있습니다.

수정된 문제

아래 표에는 Kaspersky Industrial CyberSecurity for Nodes의 이전 버전에서 발견되어 현재 버전에서 수정된 모든 문제가 나열되어 있습니다.

버전 5.0에서 수정된 문제 목록

식별자	문제 설명
9527176	웹 콘솔에서는 이전에 애플리케이션 콘솔에서 내보낸 방화벽 규칙을 정책으로 가져올 수 없습니다.
9986614	웹 콘솔 및 Kaspersky Security Center 관리 콘솔에서는 웹 콘솔에서 내보낸, 차단된 장치 관련 Kaspersky Security Center 이벤트 선택 항목이 포함된 TXT 파일에서 신뢰하는 장치 목록을 가져올 수 없습니다.
10094028	Portable Auditor를 생성할 때 감사 구성 샘플 프로필이 운영 체제의 규정 준수 및 보안 구성 목록에 잘못 표시됩니다.
10700703	시스템 무결성 모니터링, 신뢰 구역, 애플리케이션 실행 제어 및 장치 제어 구성 요소의 인터페이스에서 **선택 항목 내보내기** 명령을 실행하기 위해 목록 항목을 선택하는 방법을 바로 알기 어렵습니다. 애플리케이션 도움말의 설명이 확장되었습니다.
10720231	Kaspersky Security Center 관리 콘솔의 정책에 있는 **장치 제어** 섹션에 신뢰하는 장치 카운터가 표시되지 않습니다.
10729552	이동식 드라이브의 파일 작업과 관련된 이벤트의 기록이 활성화되어 있어도 해당 이벤트가 생성되지 않습니다.
10752491	웹 콘솔에서는 관리 콘솔에서 내보낸, 차단된 장치 관련 Kaspersky Security Center 이벤트 선택 항목이 포함된 TXT 파일에서 신뢰하는 장치 목록을 가져올 수 없습니다.
10753980	*악성 코드 검사* 작업을 실행하면 Portable Auditor가 암호로 보호된 ZIP 압축 파일 대신 KLQ 파일을 잘못 생성합니다.

배포 패키지

배포 키트는 사용자가 다음 작업을 수행할 수 있는 시작 애플리케이션을 포함합니다:

- Kaspersky Industrial CyberSecurity for Nodes 애플리케이션 설치 마법사를 시작하십시오.
- Kaspersky Industrial CyberSecurity for Nodes 콘솔 설치 마법사를 시작합니다.
- Kaspersky 바이러스 제거 도구를 시작하십시오.
- Kaspersky Security Gateway 설정을 시작하십시오.
- 이 버전의 Kaspersky Industrial CyberSecurity for Nodes에 관해 자세히 알아보십시오.
- Kaspersky Industrial CyberSecurity for Nodes 5.0 도움말을 엽니다.
- Kaspersky Industrial CyberSecurity Endpoint Detection and Response 도움말을 엽니다.
- Kaspersky 웹사이트의 Kaspersky Industrial CyberSecurity for Nodes 페이지로 갑니다.
- Kaspersky 웹사이트를 방문하십시오.
- 기술 지원 웹사이트로 갑니다.

배포 키트 파일은 용도에 따라 다른 폴더에 저장됩니다(아래 표 참조).

Kaspersky Industrial CyberSecurity for Nodes 배포 키트 파일

파일	용도
autorun.inf	이동식 드라이브에서 애플리케이션 설치 시 Kaspersky Industrial CyberSecurity for Nodes 설치 마법사용 자동 실행 파일입니다.
setupui.exe	애플리케이션 시작 화면 실행 파일.
kics_win.kud	Kaspersky Security Center를 통해 애플리케이션을 원격 설치하기 위한 설치 패키지에 관한 설명을 포함한 Kaspersky 유니코드 정의 형식의 파일.

파일	용도
\client\kicstools.msi	Windows Installer 설치 패키지. 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes 콘솔을 설치하십시오.
\client\setup_kicstool.exe	Kaspersky Industrial CyberSecurity for Nodes 콘솔을 설치하기 위해 마법사를 시작하는 파일입니다. 마법사에서 지정된 설치 설정으로 설치 패키지 파일 kicstools.msi가 시작합니다.
\client\license.txt	Kaspersky Industrial CyberSecurity for Nodes 관리 콘솔 최종 사용자 라이센스 계약서 및 개인정보취급방침 텍스트 파일.
\exec\bases.cab	애플리케이션 배포 당시의 안티 바이러스 데이터베이스 보관 파일.
\exec\cleaner_v2.cab \exec\cleanerapi_v2.cab	호환되지 않는 소프트웨어를 제거하는 파일.
\exec\incompatible.txt	Kaspersky는 파일에 나열된 애플리케이션과 Kaspersky Industrial CyberSecurity for Nodes의 호환성을 보장하지 않습니다.
\exec\installer.ini	배포 패키지 내부 설정이 포함된 파일.
\exec\kics.cab	애플리케이션의 그래픽 인터페이스용 파일.
\exec\kics_win.kud	Kaspersky Security Center를 통해 애플리케이션을 원격 설치하기 위한 설치 패키지에 관한 설명을 포함한 Kaspersky 유니코드 정의 형식의 파일.
\exec\kics_win.msi	Windows Installer 설치 패키지: 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes 콘솔을 설치합니다.
\exec\klcfginst.msi	Kaspersky Security Center 통해 이용할 수 있는 Kaspersky Industrial CyberSecurity for Nodes 관리 플러그인용 설치 프로그램. Kaspersky Security Center 관리 콘솔을 Kaspersky Industrial CyberSecurity for Nodes 관리에 사용하려는 경우, Kaspersky Security Center 관리 콘솔이 설치된 각 보호 중인 장치에 관리 플러그인을 설치하십시오.
\exec\ksn_en.txt	KSN 진술문 텍스트가 포함된 파일.
\exec\license.txt	Kaspersky Industrial CyberSecurity for Nodes 최종 사용자 라이센스 계약서 및 개인정보취급방침 텍스트 파일.
\exec\package.kcat	배포 키트 파일의 서명이 있는 파일.
\exec\setup_kics.exe	보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes를 설치하기 위한 마법사를 시작하는 파일입니다. 마법사에 지정된 설치 설정으로 kics_win.msi 설치 프로그램 패키지 파일을 시작합니다.
\gateway\security_gateway.msi	Windows Installer 설치 패키지; Kaspersky Security Gateway를 설치하십시오.
\gateway\opc_redist.msi	Windows Installer 서비스 설치 패키지로, OPC Core Components 재배포 가능 패키지를 설치합니다.
\gateway\license.txt	Kaspersky Security Gateway 최종 사용자 라이센스 계약서 및 개인정보취급방침 텍스트 파일.
\kvrt\KVRT.exe	Kaspersky 바이러스 제거 도구 설치 프로그램.
\setup\images	애플리케이션 시작 화면 실행 파일이 포함된 폴더.
\setup\setup.hta	애플리케이션 시작 화면 실행 파일.
\setup\SETUP_STRINGS.JS	애플리케이션 문자열 리소스가 있는 파일.

배포 키트 파일은 설치 CD에서 실행할 수 있습니다. 배포 패키지 파일을 미리 로컬 드라이브에 복사한 경우, 배포 키트 파일의 구조를 유지하도록 해야 합니다.

하드웨어 및 소프트웨어 요구 사항

보호 중인 장치의 소프트웨어 요구 사항

이 문서에는 해당 애플리케이션이 테스트를 거쳤으며 정상적으로 작동하는 것이 보장되는 소프트웨어 버전이 나와 있습니다. 애플리케이션이 다른 소프트웨어 버전에서 작동할 수도 있지만, 이러한 구성은 전체 테스트를 거치지 않았으므로 지원 보장 버전 목록에 포함되지 않습니다.

Microsoft Windows XP를 실행하는 보호 중인 장치에서 애플리케이션을 제대로 설치하고 작동시키려면 Windows Installer 3.1이 필요합니다.

임베디드 운영 체제가 설치된 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치하고 사용하려면 필터 관리자 구성 요소(Filter Manager)가 필요합니다.

Kaspersky Industrial CyberSecurity for Nodes가 올바르게 작동하려면 Microsoft Windows에서 SHA-2 지원이 필요합니다. 자세한 내용은 기술 지원 웹사이트의 지식 베이스를 참조하십시오.

다음 32비트/64비트 Microsoft Windows 운영 체제 중 하나를 실행하는 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치할 수 있습니다.

데스크탑 운영 체제:

- Windows XP Professional SP2 32비트/64비트
- Windows XP Professional SP3 32비트
- Windows Vista SP2 32비트/64비트
- Windows 7 SP1 Home / Pro / Enterprise / Ultimate 32비트/64비트
- Windows 8 Pro / Enterprise 32비트/64비트
- Windows 8.1 Pro / Enterprise 32비트/64비트
- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트

- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 25H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 26H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트

서버 운영 체제:

- Windows Server 2003 SP1 Standard / Enterprise 32비트/64비트
- Windows Server 2008 R2 SP1 Foundation / Standard / Enterprise 64비트
- Windows Server 2008 R2 SP2 Foundation / Standard / Enterprise 64비트
- Windows Server 2008 SP2 Standard / Enterprise 64비트
- Windows Small Business Server 2011 Essentials / Standard 64비트
- Windows MultiPoint Server 2011 64비트
- Windows Server 2012 Foundation / Essentials / Standard 64비트
- Windows Server 2012 R2 Foundation / Essentials / Standard 64비트
- Windows Server 2016 Essentials / Standard 64비트
- Windows Server 2019 RS5 Essentials / Standard 64비트
- Windows Server 2022 21H2 64비트

- Windows Server 2022 버전 20348.350 64비트
- Windows Server 2025 버전 26100.1742 64비트

임베디드 시스템:

- Windows XP Embedded Service Pack 3 32비트
- Windows Embedded POSReady 7 32비트/64비트
- Windows Embedded Standard 7 Service Pack 1 32비트/64비트
- Windows Embedded 8 Standard 32비트/64비트
- Windows Embedded 8.1 Industry Pro 32비트/64비트
- Windows 10 IoT Enterprise 버전 1507 32비트/64비트
- Windows 10 IoT Enterprise 버전 1607 32비트/64비트
- Windows 10 IoT Enterprise 버전 1803 32비트/64비트
- Windows 10 IoT Enterprise 버전 1809 32비트/64비트
- Windows 10 IoT Enterprise 버전 1903 32비트/64비트
- Windows 10 IoT Enterprise 버전 2004 32비트/64비트
- Windows 10 IoT Enterprise 버전 20H2 32비트/64비트
- Windows 10 IoT Enterprise 버전 21H1 32비트/64비트
- Windows 10 IoT Enterprise 버전 21H2 32비트/64비트
- Windows 10 IoT Enterprise 버전 22H2 32비트/64비트
- Windows 11 IoT Enterprise 버전 21H2 64비트
- Windows 11 IoT Enterprise 버전 22H2 64비트
- Windows 11 IoT Enterprise 버전 23H2 64비트
- Windows 11 IoT Enterprise 버전 24H2 64비트
- Windows 11 IoT Enterprise 버전 25H2 64비트

보호 중인 장치의 하드웨어 요구 사항

보호 중인 장치의 하드웨어 요구 사항

OS 유형	OS 이름	최소 요구 사항	권장 요구 사항
워크스테이션	Windows XP x86	• 프로세서: 1GHz 싱글 코어 프로세서, Celeron III 이상 또는 VIA C3 • RAM: 256 MB • 디스크 여유 공간: 2GB	• 프로세서: 2.4GHz 쿼드 코어 • RAM: 2 GB • 디스크 여유 공간: 4GB
	Windows XP x64 Windows 7 / 8 x86	• 프로세서: 1.4 GHz 단일 코어 프로세서 Pentium IV(x64) 이상 • RAM: 256 MB • 디스크 여유 공간: 2GB	• 프로세서: 2.4GHz 쿼드 코어 • RAM: 2 GB • 디스크 여유 공간: 4GB
	Windows 7 / 8 / 10 / 11 x64	• 프로세서: 1.4 GHz 단일 코어 프로세서 Pentium IV(x64) 이상 • RAM: 256 MB • 디스크 여유 공간: 2GB	• 프로세서: 2.4GHz 쿼드 코어 • RAM: 2 GB • 디스크 여유 공간: 4GB
서버용	Windows Server 2003 x86/x64 Windows Server 2008 x86	• 프로세서: 1.4 GHz 단일 코어 프로세서 Pentium IV(x64) 이상 • RAM: 256 MB • 디스크 여유 공간: 4GB	• 프로세서: 2.4GHz 쿼드 코어 • RAM: 2 GB • 디스크 여유 공간: 4GB
	Windows Server 2016 x64 Windows Server 2012 x64 Windows Server 2008 x64 Windows Server 2019 x64 Windows Server 2022 x64	• 프로세서: 1.4GHz 싱글 코어 • RAM: 256 MB • 디스크 여유 공간: 4GB	• 프로세서: 2.4GHz 쿼드 코어 • RAM: 2 GB • 디스크 여유 공간: 4GB
임베디드	Windows Embedded XP	• 프로세서: 1.4 GHz 단일 코어 프로세서 Pentium IV(x64) 이상 • RAM: 256 MB • 디스크 여유 공간: 2GB	• 프로세서: 2.4GHz 쿼드 코어 • RAM: 2 GB • 디스크 여유 공간: 4GB
	Windows 7 / 8 / 10 Embedded	• 프로세서: 1.4 GHz 단일 코어 프로세서 Pentium IV(x64) 이상 • RAM: 256 MB • 디스크 여유 공간: 2GB	• 프로세서: 2.4GHz 쿼드 코어 • RAM: 2 GB • 디스크 여유 공간: 4GB

지원 산업 시스템

Kaspersky Industrial CyberSecurity for Nodes 5.0는 다음 프로그래밍 가능 논리 컨트롤러를 보호합니다:

- Siemens™ SIMATIC™ S7-300
- Siemens SIMATIC S7-400
- Siemens SIMATIC S7-400H
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- Siemens SIPROTEC 4
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580

- CODESYS V3를 기반으로 한 장치
- OWEN PLC210
- Fastwel CPM723-01
- Prosoft Systems Regul R500
- Emerson DeltaV
- Rockwell Automation Allen-Bradley ControlLogix
- TREI-5B

Kaspersky Security Gateway의 하드웨어 및 소프트웨어 요구 사항

하드웨어 및 소프트웨어 일반 요구 사항:

- 1GB의 디스크 여유 공간
- klakaut 서비스를 데이터 공급자로 선택하려면 Kaspersky Security Center 중앙 관리 서버를 설치해야 합니다

데스크탑 운영 체제:

- Windows 7 SP1 Pro / Enterprise / Ultimate 32비트/64비트
- Windows 8 Pro / Enterprise 32비트/64비트
- Windows 8.1 Pro / Enterprise 32비트/64비트
- Windows 10 LTSC 2015 버전 1507 32비트/64비트
- Windows 10 LTSC 2016 버전 1607 32비트/64비트
- Windows 10 RS4 버전 1803 Home / Pro / Education / Enterprise 32비트/64비트
- Windows 10 RS5 버전 1809 Home / Pro / Education / Enterprise 32비트/64비트
- Windows 10 LTSC 2019 버전 1809 32비트/64비트
- Windows 10 19H1 버전 1903 Home / Pro / Education / Enterprise 32비트/64비트
- Windows 10 20H1 버전 2004 Home / Pro / Education / Enterprise 32비트/64비트
- Windows 10 20H2 버전 2009 Home / Pro / Education / Enterprise 32비트/64비트
- Windows 10 21H1 Home / Pro / Education / Enterprise 32비트/64비트
- Windows 10 LTSC 2021 버전 21H2 32비트/64비트
- Windows 10 22H2 Home / Pro / Education / Enterprise 32비트/64비트

- Windows 11 23H2 Home / Pro / Education / Enterprise 64비트
- Windows 11 22H2 Home / Pro / Education / Enterprise 64비트
- Windows 11 21H2 Home / Pro / Education / Enterprise 64비트
- Windows 11 22H2 Home / Pro / Education / Enterprise 64비트
- Windows 11 23H2 Home / Pro / Education / Enterprise 64비트
- Windows 11 24H2 Home / Pro / Education / Enterprise 64비트
- Windows 11 25H2 Home / Pro / Education / Enterprise 64비트
- Windows 11 26H2 Home / Pro / Education / Enterprise 64비트

서버 운영 체제:

- Windows Server 2008 R2 Standard / Enterprise 32비트/64비트
- Windows Server 2008 SP1 R2 Standard / Enterprise 32비트/64비트
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter 64비트
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter 64비트
- Windows Server 2016 Essentials / Standard / Datacenter 64비트
- Windows Server 2019 Essentials / Standard / Datacenter 64비트
- Windows Server 2022 21H2 64비트
- Windows Server 2022 버전 20348.350 64비트
- Windows Server 2025 버전 26100.1742 64비트

지원 Kaspersky Security Center 버전

Kaspersky Industrial CyberSecurity for Nodes는 다음 버전의 Kaspersky Security Center와 호환됩니다:

- Kaspersky Security Center Linux 버전 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3, 17.0. Kaspersky Industrial CyberSecurity for Nodes의 관리는 Kaspersky Security Center 웹 콘솔로 지원합니다.
- Kaspersky Security Center Windows 버전 15.1. Kaspersky Industrial CyberSecurity for Nodes의 관리는 Kaspersky Security Center 관리 콘솔 및 Kaspersky Security Center 웹 콘솔로 지원합니다.
- Kaspersky Security Center Windows 14.0. Microsoft Windows XP SP3 운영 체제를 실행하는 장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes의 관리는 Kaspersky Security Center 관리 콘솔 및 Kaspersky Security Center 웹 콘솔을 통해 지원됩니다.
- Kaspersky Security Center Windows 10.5. Microsoft Windows XP SP2 운영 체제를 실행하는 장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes의 관리는 Kaspersky Security Center 관리 콘솔 및 Kaspersky Security Center 웹 콘솔을 통해 지원됩니다.

Kaspersky Security Center를 통해 Kaspersky Industrial CyberSecurity for Nodes를 관리하려면 Kaspersky Security Center 네트워크 에이전트가 필요합니다.

Kaspersky Security Center 네트워크 에이전트는 Kaspersky Industrial CyberSecurity for Nodes 배포 키트에 포함되어 있지 않습니다. **Kaspersky Security Center** 섹션의 애플리케이션 다운로드 페이지 에서 다운로드할 수 있습니다.

Kaspersky 바이러스 제거 도구

Kaspersky 바이러스 제거 도구는 Microsoft Windows 운영 체제를 실행하는 감염 컴퓨터를 확인하고 치료하도록 설계된 유틸리티입니다. Kaspersky 바이러스 제거 도구는 바이러스, 트로이목마 등 보호 중인 장치를 위협하는 기타 프로그램을 탐지하며, 사용자가 탐지된 감염 개체의 처리 방법을 선택할 수 있도록 합니다.

Kaspersky 바이러스 제거 도구는 설치할 필요가 없습니다. 애플리케이션은 다음과 같은 방법으로 시작할 수 있습니다:

- kvrt\ 폴더에서 Kaspersky Industrial CyberSecurity for Nodes 5.0 배포 키트에 포함된 kvrt.exe 실행 파일을 시작하십시오.
- 시작 창에서 **Kaspersky Virus Removal Tool 실행** 링크를 클릭합니다.

유틸리티는 Kaspersky Industrial CyberSecurity for Nodes 5.0의 로컬 콘솔 또는 관리 플러그인을 통해서는 시작할 수 없습니다.

탐지된 감염을 치료한 후에는 컴퓨터를 다시 시작해야 합니다. Kaspersky 바이러스 제거 도구는 산업 네트워크 작업의 기술 창에서만 실행할 것을 권장합니다.

Kaspersky 바이러스 제거 도구는 Kaspersky Industrial CyberSecurity for Nodes 솔루션에 포함되지 않으며 애플리케이션 구성 요소에 의존하지 않습니다.

안티 바이러스 데이터베이스 업데이트는 Kaspersky Industrial CyberSecurity for Nodes 5.0 업데이트와 별도로 수행됩니다. Kaspersky 바이러스 제거 도구를 시작할 때 애플리케이션에서 업데이트가 필요한지 알립니다. 유틸리티를 업데이트하려면 인터넷에 연결되어 있어야 합니다.

Kaspersky 바이러스 제거 도구의 작동에는 별도의 최종 사용자 라이센스 계약서가 적용되며, 이는 기술 지원 웹사이트 에서 확인할 수 있습니다.

기술 지원 웹사이트에서는 유틸리티가 시작되는 컴퓨터의 시스템 요구 사항에 관한 정보와 Kaspersky 바이러스 제거 도구 사용에 대한 상세 지침도 제공합니다.

기능 요구 사항 및 제한 사항

이 섹션에서는 Kaspersky Industrial CyberSecurity for Nodes 구성 요소의 추가 기능 요구 사항과 기존 제한 사항에 관해 설명합니다.

애플리케이션 설치 및 제거

- Kaspersky Industrial CyberSecurity for Nodes가 올바르게 작동하려면 Microsoft Windows에서 SHA-2 지원이 필요합니다.
- 애플리케이션 설치 시 Kaspersky Industrial CyberSecurity for Nodes 설치 폴더의 지정된 경로가 150자를 초과하는 경우 화면에 경고가 표시될 수 있습니다. 이 경고는 설치 프로세스에 영향을 주지 않으며, Kaspersky Industrial CyberSecurity for Nodes를 설치하고 실행할 수 있습니다.
- SNMP 프로토콜 지원 구성 요소를 설치하려면 SNMP 서비스가 실행 중일 시 SNMP 서비스를 다시 시작해야 합니다.
- 임베디드 운영 체제를 실행하는 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치하고 실행하려면 필터 관리자 구성 요소를 설치해야 합니다.
- Microsoft Active Directory® 그룹 정책을 통해 관리 도구를 설치할 수 없습니다.
- 설치된 애플리케이션 구성 요소 목록에서 안티 바이러스 보호 노드 제외 시, 설치가 완료되면 이용 가능한 구성 요소 목록에서 이 노드가 사라집니다. 안티 바이러스 보호 노드의 구성 요소를 설치하려면 설치 패키지에서 설치 마법사를 시작하십시오. 설치 패키지에는 구성 요소의 전체 목록이 포함되어 있습니다.
- Kaspersky Industrial CyberSecurity for Nodes 관리 콘솔이 설치된 경우 설치 마법사가 컴퓨터를 다시 시작하라는 메시지를 표시할 수 있습니다. 이 경우 재부팅은 필수가 아닙니다. 관리 콘솔을 설치한 사용자의 세션을 종료하고 시스템에 다시 로그인하는 것으로 충분합니다.
- Windows XP 또는 Windows Vista 장치에 애플리케이션을 설치할 때 드라이버 서명 확인을 활성화하기 위해 DigiCert Assured ID Root CA 인증서를 설치해야 할 수 있습니다. 필요한 경우 이 인증서는 애플리케이션 설치 패키지에서 운영 체제의 신뢰할 수 있는 루트 인증서 저장소에 자동으로 설치됩니다.
- Windows XP 또는 Windows Vista 장치에 애플리케이션을 설치할 때 DigiCert High Assurance EV Root CA.가 있는지 확인해야 합니다.

  해당 루트 인증서를 설치하지 않은 경우 애플리케이션이 제대로 작동하지 않을 수 있습니다. 가능한 빨리 인증서를 설치하는 것이 좋습니다.
- 설치 폴더의 경로가 애플리케이션 데이터베이스 폴더, 백업 폴더, 격리 저장소의 개체 복구용 폴더, 임시 파일 폴더 중 하나 이상의 경로와 같다면 오류와 함께 애플리케이션 설치가 종료됩니다.
- Kaspersky Security Center 클라우드 콘솔을 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 관리하는 경우 애플리케이션을 로컬에서 업데이트할 수 없습니다. 로컬에서 애플리케이션을 업데이트할 때 Kaspersky Security Center Cloud Console에 대한 데이터 처리 계약을 수락할 수 없습니다.

시스템 무결성 모니터링

기본적으로 시스템 무결성 모니터링 구성 요소는 시스템 폴더나 파일 시스템의 관리 파일에서 발생하는 변경 사항을 모니터링하지 않습니다. 이는 운영 체제에서 계속 수행되는 일반적인 파일 변경 정보를 포함하여 작업 리포트를 불필요하게 복잡하게 만드는 것을 방지하기 위함입니다. 이러한 폴더는 모니터링 범위에 포함할 수 없습니다.

다음 폴더 및 파일은 모니터링 범위에서 제외됩니다:

- 파일 ID가 0부터 33까지인 NTFS 관리 파일
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\Windows\TaskScheduler\

애플리케이션은 최상위 폴더를 제외합니다.

이 구성 요소는 ReFS/NTFS 파일 시스템을 우회하는 파일 변경 사항(BIOS, LiveCD 등을 통한 파일 변경 사항)을 모니터링하지 않습니다.

방화벽

- 주소를 하나 이상 지정해야 합니다. 아니면 IPv6으로 작업할 수 없습니다.
- 사전 설정된 방화벽 규칙은 보호 중인 장치와 중앙 관리 서버 간의 상호 작용에 대한 기본 시나리오를 지원합니다. Kaspersky Security Center 기능을 최대한 활용하려면 포트 규칙을 구성해야 합니다. Kaspersky Security Center 기술 자료에서 포트 번호와 프로토콜, 그 기능에 관한 정보를 찾을 수 있습니다.
- 애플리케이션을 설치하고 방화벽 규칙을 구성하면 애플리케이션은 방화벽 구성 요소가 실행 중일 시 Windows 방화벽 규칙 및 규칙 그룹의 변경 사항을 모니터링합니다. 상태를 업데이트하고 필요한 Windows 방화벽 규칙을 추가하려면 방화벽 구성 요소를 다시 시작하십시오.
- 방화벽 구성 요소 시작 시 거부 규칙 및 아웃바운드 트래픽을 제어하는 규칙이 Windows 방화벽 설정에서 자동으로 제거됩니다.
- 문자 `*` 및 `?`는 애플리케이션 경로와 애플리케이션용 방화벽 규칙의 이름에 사용할 수 없습니다.
- *Windows 방화벽 상태 관찰* 모드를 선택하면 Windows 방화벽 설정(**설정 → 업데이트 및 보안 → Windows 보안 → 방화벽 및 네트워크 보호**)에 Kaspersky Industrial CyberSecurity for Nodes 방화벽이 비활성화된 것으로 표시됩니다. 방화벽을 활성화하는 버튼을 클릭하면 운영 모드가 *차단* 모드로 변경됩니다.
- Windows 7 및 Windows Server 2008 R2를 실행하는 컴퓨터에서 서비스 이름에 기반한 TermService 서비스에 대해 구성된 방화벽 규칙은 RDP를 통한 접근을 제한하지 않습니다.
- 방화벽이 **차단** 모드에서 실행 중인 경우 애플리케이션은 DHCP 서버에서 IP 주소를 가져오는 것을 방지합니다. IP 주소를 가져오려면 svchost.exe 시스템 프로세스를 허용하도록 방화벽을 구성하십시오.

오래된 Windows 버전에 대한 제한 사항

- Windows XP SP2 버전은 원격 장치를 차단하고 차단된 네트워크 세션 목록 설정을 구성할 수 없습니다. 이 Windows 버전에서는 **악성 활동을 보이는 세션의 네트워크 공유 리소스 접근 차단** 옵션이 비활성되어 있습니다.
- Kaspersky Industrial CyberSecurity for Nodes 설치:
  - Windows XP SP2 Professional(32비트/64비트), Windows Server 2003 또는 Windows Server 2003 R2를 실행하는 컴퓨터에서 Kaspersky Security Center를 사용하여 애플리케이션을 설치하는 경우, 네트워크 에이전트 10.5.1781 설치 패키지의 setup.exe 파일을 애플리케이션 설치 패키지 폴더에 넣고 Kaspersky Security Center용 개인 패치를 설치해야 합니다.
  - Windows XP SP3 Professional(32비트) 또는 Windows XP Embedded SP3(32비트)를 실행하는 컴퓨터에서 Kaspersky Security Center를 사용하여 애플리케이션을 설치하는 경우, 네트워크 에이전트 14.0.0.20023 설치 패키지의 setup.exe 파일을 애플리케이션 설치 패키지 폴더에 넣고 Kaspersky Security Center용 개인 패치를 설치해야 합니다.

    필요 파일과 지침의 경우 기술 지원을 문의하십시오.

- Kaspersky Security Center를 통해 Kaspersky Industrial CyberSecurity for Nodes를 관리하려면:
  - Windows XP SP2 Professional(32비트/64비트)이나 Windows Server 2003, Windows Server 2003 R2를 실행하는 컴퓨터에서는 Kaspersky Security Center 네트워크 에이전트 버전 10.5.1781을 사용해야 합니다.
  - Windows XP SP3 Professional(32비트)이나 Windows XP Embedded SP3(32비트)를 실행하는 컴퓨터에서는 Kaspersky Security Center 네트워크 에이전트 버전 14.0.0.20023를 사용해야 합니다.
- Windows XP 컴퓨터에서는 MQTT 프로토콜을 사용하여 원격 측정을 데이터 다이오드로 전송할 수 없습니다.
- *성능 분석기* 작업이 올바르게 작동하려면 작업이 시작된 컴퓨터가 Windows Vista 이상을 실행해야 합니다.

Kaspersky Security Center와 통합

- 업데이트 패키지를 수신하면 중앙 관리 서버는 네트워크의 보호 중인 장치에 업데이트를 전송하기 전에 데이터베이스 업데이트를 확인합니다. Kaspersky Security Center 중앙 관리 서버는 애플리케이션 모듈 업데이트를 확인하지 않습니다.
- 네트워크 목록을 통해 Kaspersky Security Center로 동적 데이터를 전송하는 구성 요소(격리 저장소, 백업 저장소)를 사용할 경우, Kaspersky Security Center 중앙 관리 서버와의 상호 작용 설정에서 필요한 확인란이 선택되어 있는지 확인하십시오.
- Network Agent 10.5는 설치된 구성 요소에 관한 정보를 Kaspersky Security Center 중앙 관리 서버로 전송하지 않습니다. 이러한 이유로 Kaspersky Security Center 관리 콘솔 및 Kaspersky Security Center 웹 콘솔에서는 Network Agent 10.5가 설치된 장치의 설정이 설치된 Kaspersky Industrial CyberSecurity for Nodes 구성 요소 및 그 설정을 표시하지 않습니다.
- Kaspersky Security Center 네트워크 에이전트 10.5가 장치에 설치되어 있는 경우, Kaspersky Security Center 웹 콘솔 사용하여 백업 저장소에서 파일을 다운로드할 수 없습니다.
- Kaspersky Security Center 네트워크 에이전트의 리소스 소비 절약 모드가 활성화된 상태(기본값, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`)로 Kaspersky Industrial CyberSecurity for Nodes를 설치한 후 네트워크 에이전트를 설치할 경우, Kaspersky Industrial CyberSecurity for Nodes Windows 방화벽에서 네트워크 에이전트에 대한 예외를 생성하지 않으므로 Windows 방화벽이 네트워크 에이전트를 차단합니다.
- Kaspersky Security Center 네트워크 에이전트의 리소스 소비 절약 모드가 활성화된 상태(기본값, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`)로 Kaspersky Industrial CyberSecurity for Nodes를 설치한 경우, 네트워크 목록의 수정 사항이 Kaspersky Security Center 관리 콘솔에 약 10분 정도의 지연 후 반영됩니다.
- Kaspersky Security Center 관리 콘솔에서 관리 중인 장치를 검색할 때 **애플리케이션 구성 요소** 탭에는 이전 버전의 Kaspersky Industrial CyberSecurity for Nodes에 해당하는 이름을 포함하여 동일한 애플리케이션 구성 요소의 이름이 여러가지 변형으로 동시에 표시될 수 있습니다. 일부 구성 요소의 이름이 중복될 수도 있습니다.

  구성 요소로 검색하려면 표시된 변형 중 하나를 선택하기만 하면 됩니다. 장치 검색에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

기타 제한

온디맨드 검사 및 실시간 파일 보호

- 연결된 MTP 장치는 검사할 수 없습니다.
- 압축 파일 검사는 SFX 압축 파일 검사 없이 진행할 수 없습니다. Kaspersky Industrial CyberSecurity for Nodes의 보호 설정에서 압축 파일 검사 활성화 시 애플리케이션이 압축 파일과 SFX 압축 파일 모두에서 자동으로 개체를 검사합니다. SFX 압축 파일 검사는 압축 파일 검사 없이 진행할 수 있습니다.
- **실행 프로세스 심층 분석(분석 기간 중 프로세스 실행이 차단됩니다)** 확인란과 **KSN 사용**이 동시에 활성화될 경우, "알림" 모드를 선택했더라도 URL 웹 주소를 인수로 받는 모든 시작된 프로세스가 차단됩니다. 프로세스가 차단되지 않으려면 다음 옵션 중 하나를 선택합니다:
  - **KSN 사용** 비활성화.
  - **실행 프로세스 심층 분석(분석 기간 중 프로세스 실행이 차단됩니다)** 확인란 비활성화

  권장 옵션: **실행 프로세스 심층 분석(분석 기간 중 프로세스 실행이 차단됩니다)** 확인란을 선택 해제합니다.

라이센스

- SUBST 명령을 사용하여 키를 생성했거나 키 파일의 경로가 네트워크 경로인 경우에는 설치 마법사의 키로 애플리케이션을 활성화할 수 없습니다.
- Kaspersky Security Center 프록시 서버를 사용하여 클라이언트 장치에서 제품을 활성화하려면 Kaspersky Security Center 네트워크 에이전트 설치 시 해당 장치에서 VDI 최적화를 비활성화하십시오.

업데이트

- Windows XP 장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes 패치를 설치하거나 제거할 때 이 운영 체제의 특성으로 인해 장치를 다시 시작해야 할 수 있습니다.
- 기본적으로 Kaspersky Industrial CyberSecurity for Nodes 중요 모듈 업데이트를 설치한 후에는 애플리케이션 아이콘이 숨겨집니다.
- KLRAMDISK는 Windows XP 또는 Windows Server® 2003 운영 체제를 실행하는 보호 중인 장치를 지원하지 않습니다.
- Kaspersky Industrial CyberSecurity for Nodes 패치 설치에 실패할 시 패치가 롤백되고 운영 체제를 다시 시작하라는 메시지가 표시됩니다.

인터페이스

- 애플리케이션 콘솔에서 격리 저장소나 백업 저장소, 시스템 감사 로그, 작업 로그의 필터링은 대소문자를 구분합니다.
- 애플리케이션 콘솔에서 보호 또는 검사 범위를 구성 시, 경로 끝에서 하나의 마스크만 사용할 수 있습니다. 올바른 마스크의 예는 `C:\Temp\Temp*`, `C:\Temp\Temp???.doc`, `C:\Temp\Temp*.doc`입니다. 이 제한 사항은 신뢰 구역의 구성에 영향을 주지 않습니다.
- 애플리케이션 콘솔의 **원격 측정 수집 서버** 섹션에는 작업 실행이 예정된 시간이 표시되지 않습니다. **시작 시간** 열은 비어 있습니다.
- 256자를 초과하는 인터페이스 텍스트 요소에 대한 팝업 알림은 Kaspersky Security Center 관리 콘솔 또는 애플리케이션 콘솔에 표시되지 않습니다.
- Kaspersky Security Center 관리 콘솔의 **사용자 또는 사용자 그룹 선택** 창에는 Kaspersky Security Center 사용자 목록의 처음 50,000명의 사용자만 표시됩니다. 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

보안

- 운영 체제의 사용자 계정 제어 기능이 활성화된 경우, 트레이 알림 영역의 애플리케이션 아이콘을 더블클릭하여 애플리케이션 콘솔을 열 수 있으려면 사용자 계정이 KICS 관리자 그룹에 속해 있어야 합니다. 아니면 간편 진단 인터페이스 또는 Microsoft 관리 콘솔 스냅인을 열 수 있는 사용자로 로그인해야 합니다.
- 사용자 계정 제어가 활성화된 경우, Microsoft Windows 프로그램 및 기능 창을 통해 애플리케이션을 제거할 수 없습니다.

익스플로잇 방지

- apphelp.dll 라이브러리가 현재 환경 구성에서 로드되지 않은 경우 익스플로잇 방지 구성 요소를 사용할 수 없습니다.
- 익스플로잇 방지 구성 요소는 Microsoft Windows 10 운영 체제를 실행하는 보호 중인 장치에서 Microsoft의 EMET 유틸리티와 호환되지 않습니다. EMET 유틸리티가 설치된 보호 중인 장치에 익스플로잇 방지 구성 요소가 설치되어 있는 경우 Kaspersky Industrial CyberSecurity for Nodes는 EMET를 차단합니다.
- 익스플로잇 방지 구성 요소는 SQL Server® 2012 데이터베이스 엔진과 호환되지 않습니다. MS SQL Server 2012가 설치된 컴퓨터에 Kaspersky Industrial CyberSecurity for Nodes 설치하는 경우 데이터베이스 서버의 sqlos.dll 라이브러리를 익스플로잇 방지 작업의 예외 목록에 추가해야 합니다.

Detection and Response

- 보안위협 대응 프로세스 중 공유 폴더 접근 오류가 발생하면 해당 오류가 보안위협 대응 기록에 반영되지 않습니다(Kaspersky Security Center 웹 콘솔 → 애플리케이션이 설치된 호스트의 속성 → **Detection and Response** – **응답 이력** 섹션).

- 네트워크 에이전트 버전 10.5.1781이 설치된 Windows XP 실행 보호 장치에서는 보안 위협 대응 기록 보기를 사용할 수 없습니다.

- Kaspersky Industrial CyberSecurity for Nodes 버전 4.5에서는 다음 EDR Expert(on-premises) 원격 측정 이벤트를 지원하지 않습니다.

  - LDAP Attribute Change
  - GPO Change
  - SCCM Local Config Mismatch
  - SCCM Config Change
  - SCCM Deployment Task
  - Smb Connection Open

  버전 5.0부터 Kaspersky Industrial CyberSecurity for Nodes는 이러한 EDR Expert(on-premises) 원격 측정 이벤트를 모두 지원하지만 LDAP Attribute Change은 지원하지 않습니다.

- [KICS+KEA] 구성을 [KICS+내장 에이전트] 구성으로 마이그레이션 시, Kaspersky Endpoint Agent 애플리케이션 제거 오류가 발생할 수 있습니다. 이 애플리케이션 제거 오류는 Kaspersky Endpoint Agent의 최신 버전에서 수정되었습니다. Kaspersky Endpoint Agent를 제거하려면, 컴퓨터를 다시 시작하고 애플리케이션 제거 작업을 생성하십시오.

- [KICS+KEA+내장 에이전트] 구성은 지원되지 않습니다. 이러한 구성은 조직에서 배포되는 애플리케이션과 Detection and Response 솔루션 간에 상호 작용을 방해합니다. 또한 동일한 컴퓨터에서 Kaspersky Endpoint Agent와 내장 에이전트를 사용하면 원격 측정이 중복될 수 있고 컴퓨터 및 네트워크에 로드가 증가할 수 있습니다. [KICS + 내장 에이전트] 구성으로 마이그레이션한 후엔 Kaspersky Endpoint Agent가 해당 컴퓨터에서 제거될 수 있도록 합니다. 마이그레이션 후에 Kaspersky Endpoint Agent가 계속해서 작동한다면 애플리케이션을 수동으로 제거합니다(예를 들어 *애플리케이션을 원격으로 제거* 작업 사용).

  설치된 Kaspersky Industrial CyberSecurity for Nodes과 내장 에이전트로 설치 프로그램을 통해 컴퓨터에 Kaspersky Endpoint Agent를 배포할 수 있습니다. Kaspersky Endpoint Agent와 내장 에이전트는 또한 *애플리케이션 구성 요소 변경* 작업의 결과로 하나의 컴퓨터에 설치 가능합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes과 Kaspersky Endpoint Agent 버전에 근거하여 동작합니다.

이벤트 구성

Kaspersky Security Center 정책의 **이벤트 구성** 섹션에서 구성할 수 있는 *제어 영역에서 미관리 파일 동작* 이벤트의 설정은 다음 이벤트에도 적용됩니다.

- *신뢰할 수 있는 사용자가 제어 영역에서 파일 동작을 수행하도록 허용됨.*
- *제어 영역에서 금지된 파일 동작.*

- *통계 전용: 제어 영역에서 금지된 파일 동작.*
- *제어 영역에서 미관리 파일 동작.*

간편 진단 인터페이스

Windows XP 컴퓨터에서 간편 진단 인터페이스가 작동하려면 터미널 서비스가 필요합니다.

장치 제어

재시작하지 않고 애플리케이션을 제거 및 재설치할 경우, 장치 제어 구성 요소가 활성화 상태로 유지될 수 잇습니다. 장치 제어 구성 요소가 제대로 작동하도록 복원하려면 컴퓨터를 재시작합니다.

Windows 안전 모드 사용 시

애플리케이션은 Windows Safe Mode에서 작동하지 않습니다.

일반 배포

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Industrial CyberSecurity 솔루션의 일부입니다.

Kaspersky Industrial CyberSecurity 솔루션은 다음 유틸리티 및 애플리케이션을 포함합니다:

- Kaspersky Security Gateway.
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks.
- Kaspersky Security Center

Kaspersky Industrial CyberSecurity for Networks 및 Kaspersky Industrial CyberSecurity for Nodes는 서로 다른 수준의 *전용 네트워크*에서 작동합니다. Kaspersky Industrial CyberSecurity 전용 네트워크는 산업 시스템과 보조 하드웨어(예: 스위치)를 보호하기 위해 Kaspersky Industrial CyberSecurity 애플리케이션을 실행하도록 설계된 컴퓨터를 포함한 산업 네트워크의 일부입니다.

Kaspersky Industrial CyberSecurity for Networks는 산업 네트워크 트래픽을 모니터링하고 분석합니다. 산업 네트워크 노드에 설치되는 Kaspersky Industrial CyberSecurity for Nodes는 알려진 컴퓨터 보안 위협으로부터 컴퓨터를 보호하고 검사 범위에 포함된 PLC 프로젝트의 무결성을 모니터링합니다.

단일 Kaspersky Security Center 관리 콘솔을 사용하여 동일한 전용 네트워크에 배포된 Kaspersky Industrial CyberSecurity for Networks 및 Kaspersky Industrial CyberSecurity for Nodes를 제어할 수 있습니다. 또한, Kaspersky Security Gateway를 사용하여 Kaspersky Industrial CyberSecurity for Networks 및 Kaspersky Industrial CyberSecurity for Nodes에서 받은 진단 정보가 Kaspersky Security Center에서 SCADA 시스템으로 전송되도록 구성할 수 있습니다.

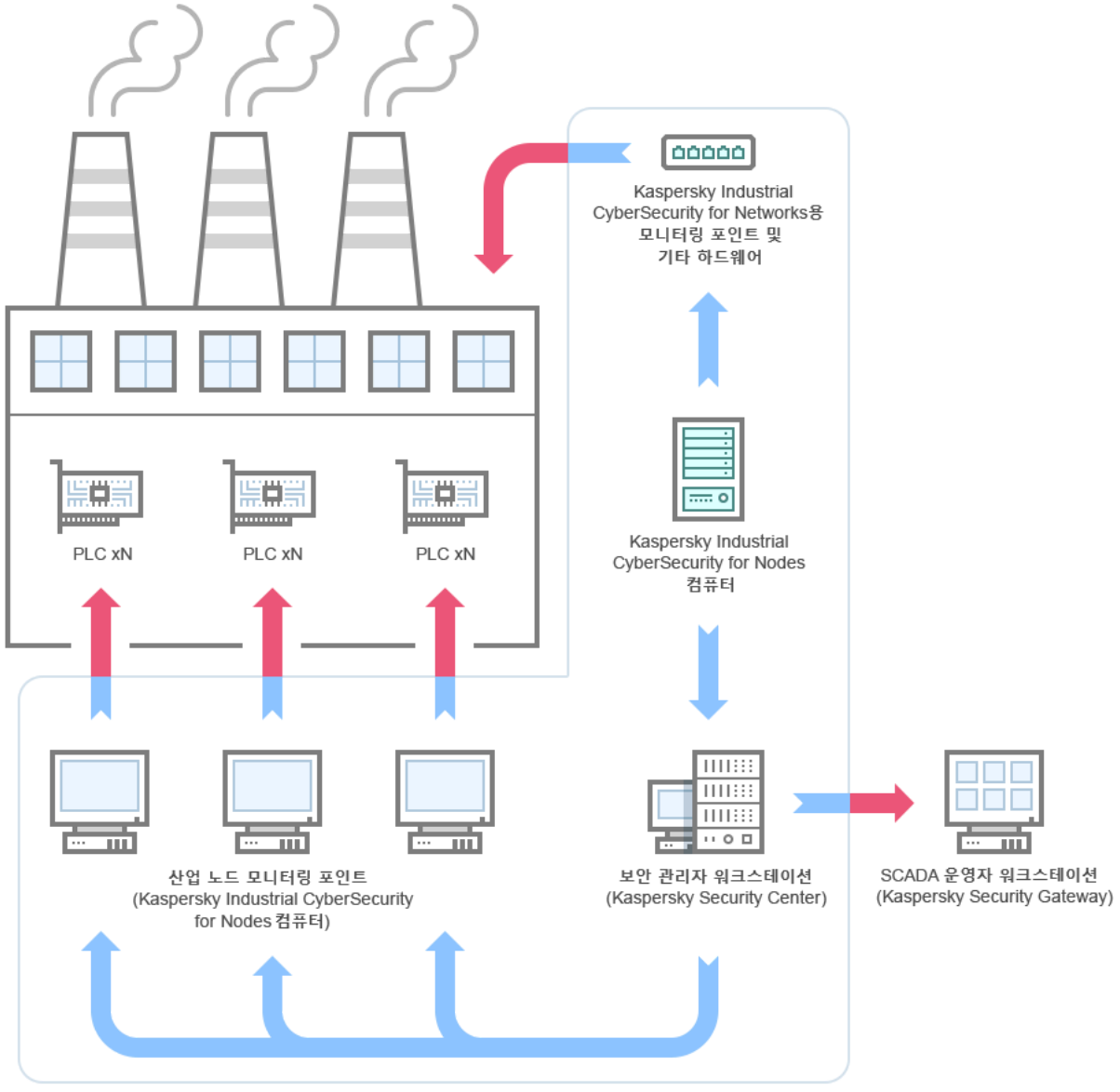
Kaspersky Industrial CyberSecurity for Nodes는 다음을 포함합니다:

- *기능 모듈* – 산업 네트워크 노드의 상태에 관한 정보를 기록하고 데이터 위협으로부터 노드를 보호합니다.

- *콘솔* – 로컬 그래픽 사용자 인터페이스입니다. Kaspersky Industrial CyberSecurity for Nodes 콘솔을 사용하여 산업 네트워크 노드의 애플리케이션을 제어할 수 있습니다. 콘솔은 Kaspersky Industrial CyberSecurity for Nodes가 설치된 컴퓨터 또는 보호 네트워크에 있는 다른 컴퓨터에 설치할 수 있습니다. 이 경우 콘솔을 사용하여 애플리케이션을 원격으로 제어합니다. 또한, 하나의 콘솔로 Kaspersky Industrial CyberSecurity for Nodes로 보호되는 여러 컴퓨터를 제어할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 보호 노드의 보안 이벤트를 기록하고 이벤트를 애플리케이션 콘솔 및 Kaspersky Security Center 관리 콘솔로 전송합니다. 기업의 산업 프로세스를 모니터링하는 전문가의 워크스테이션과 정보 보안 전문가의 워크스테이션에서 로컬 애플리케이션 콘솔 및 Kaspersky Security Center 관리 콘솔에 접근합니다.

Kaspersky Industrial CyberSecurity 솔루션의 일환으로 Kaspersky Industrial CyberSecurity for Nodes를 배포하는 예(아래 그림 참조)에서 전용 네트워크는 파란색으로 표시되고 산업 네트워크 구성 요소는 빨간색으로 표시됩니다. 배포 구성은 Kaspersky Industrial CyberSecurity 솔루션의 애플리케이션을 설치할 산업 네트워크의 특성에 따라 다릅니다.



Kaspersky Industrial CyberSecurity for Nodes 배포 구성

다른 애플리케이션과의 호환성

전체 기능 구성의 Kaspersky Industrial CyberSecurity for Nodes는 타사 엔드포인트 보호 시스템(Endpoint Protection Platform, EPP)의 일부인 애플리케이션과 호환되지 않습니다. Kaspersky Industrial CyberSecurity for Nodes는 다른 애플리케이션 및 일부 Kaspersky 애플리케이션과 호환되지 않을 수 있습니다. 호환성을 확인하기 위해 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky에서 준비한 소프트웨어 목록을 참조합니다. 이 목록은 incompatible.txt 파일에 포함되어 있습니다. 이 파일은 배포 키트에 포함되어 있습니다.

Incompatible.txt 목록에 있는 애플리케이션이 탐지되면 설치 프로그램이 Kaspersky Industrial CyberSecurity for Nodes 설치를 중지합니다. 타사 안티바이러스 애플리케이션을 제거해야 합니다. 설치 프로그램은 목록에서 일부 애플리케이션을 자동으로 삭제할 수 있습니다.

컴퓨터에 Windows 방화벽이 설치되어 있다면 설치 프로그램이 방화벽을 끄고 Kaspersky Industrial CyberSecurity for Nodes 설치를 진행합니다.

위험을 감수하고 incompatible.txt 목록에 있는 애플리케이션과 함께 Kaspersky Industrial CyberSecurity for Nodes를 동일한 장치에 설치해야 하는 경우, 설치된 타사 안티바이러스 애플리케이션 검사를 건너뛸 수 있습니다. 그러려면 설치 프로그램을 실행할 때 `SKIPPRODUCTCHECK=1` 및 `SKIPPRODUCTUNINSTALL=1` 파라미터를 지정합니다.

예:

```
setup_kics.exe /s EULA=1 PRIVACYPOLICY=1 SKIPPRODUCTCHECK=1 SKIPPRODUCTUNINSTALL=1
```

Endpoint Agent 구성의 Kaspersky Industrial CyberSecurity for Nodes는 타사 EPP 애플리케이션과 같은 컴퓨터에 설치할 수 있습니다 .

애플리케이션 설치 및 제거

이 섹션에서는 Kaspersky Industrial CyberSecurity for Nodes의 설치 및 제거에 대한 단계별 지침을 제공합니다.

설치 계획

이 섹션에서는 Kaspersky Industrial CyberSecurity for Nodes 관리 도구 세트와, 마법사 사용, 명령줄, Kaspersky Security Center 사용, Active Directory 그룹 정책을 통한 Kaspersky Industrial CyberSecurity for Nodes 설치 및 제거의 특수한 측면에 대해 설명합니다.

Kaspersky Embedded Systems Security for Windows 또는 Kaspersky Endpoint Security for Windows 제거 후 Kaspersky Industrial CyberSecurity for Nodes 설치하려면 컴퓨터를 다시 시작해야 합니다.

Kaspersky Industrial CyberSecurity for Nodes의 설치를 시작하기 전에 설치의 주요 단계를 계획합니다.

1. Kaspersky Industrial CyberSecurity for Nodes를 관리하고 구성할 때 사용할 관리 도구를 결정합니다.
2. 설치에 필요한 애플리케이션 구성 요소를 선택합니다.
3. 설치 방법을 선택합니다.

관리 도구 선택

Kaspersky Industrial CyberSecurity for Nodes 설정을 구성하고 애플리케이션을 관리할 때 사용할 관리 도구를 결정합니다. Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 콘솔, 명령줄 유틸리티, Kaspersky Security Center 관리 콘솔로 관리할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔

Kaspersky Industrial CyberSecurity for Nodes 콘솔은 Microsoft 관리 콘솔에 추가된 독립실행형 스냅인입니다. Kaspersky Industrial CyberSecurity for Nodes는 보호 중인 장치나 회사 네트워크의 다른 장치에 설치된 애플리케이션 콘솔로 관리할 수 있습니다.

작성자 모드로 열린 하나의 Microsoft 관리 콘솔에 Kaspersky Industrial CyberSecurity for Nodes 스냅인을 여러 개 추가하여, Kaspersky Industrial CyberSecurity for Nodes가 설치된 여러 장치의 보호를 관리할 수 있습니다.

명령줄 유틸리티

보호 중인 장치의 명령줄에서 Kaspersky Industrial CyberSecurity for Nodes를 관리할 수 있습니다.

명령줄 유틸리티는 Kaspersky Industrial CyberSecurity for Nodes 소프트웨어 구성 요소 그룹에 포함됩니다.

Kaspersky Security Center

Kaspersky Security Center를 사용해 회사 장치의 안티 바이러스 보호를 중앙 집중식으로 관리한다면, Kaspersky Security Center 관리 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes를 관리할 수 있습니다.

이를 위해서는 다음 구성 요소를 설치해야 합니다.

- **Kaspersky Security Center 네트워크 에이전트와의 통합을 위한 모듈**. 이 구성 요소는 Kaspersky Industrial CyberSecurity for Nodes 소프트웨어 구성 요소 그룹에 포함됩니다. 이를 통해 Kaspersky Industrial CyberSecurity for Nodes가 네트워크 에이전트와 통신할 수 있습니다. 보호 중인 장치에 Kaspersky Security Center 네트워크 에이전트와의 통합을 위한 모듈을 설치합니다.

- **Kaspersky Security Center 네트워크 에이전트**. 각 보호 중인 장치에 이 구성 요소를 설치합니다. 이 구성 요소는 보호 중인 장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Security Center 관리 콘솔 간의 상호작용을 지원합니다. 네트워크 에이전트 설치 파일은 Kaspersky Security Center 배포 키트 폴더에 포함됩니다.

- **Kaspersky Industrial CyberSecurity for Nodes 관리 플러그인**. 또한 Kaspersky Security Center 중앙 관리 서버가 설치된 보호 중인 장치의 관리 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 관리용 플러그인을 설치합니다. 이는 Kaspersky Security Center를 통한 애플리케이션 관리 인터페이스를 제공합니다. 관리 플러그인 설치 파일 \exec\klcfginst.exe는 Kaspersky Industrial CyberSecurity for Nodes 배포 키트에 포함되어 있습니다.

설치 유형 선택

Kaspersky Industrial CyberSecurity for Nodes 설치를 위한 소프트웨어 구성 요소를 지정한 후, 애플리케이션 설치 방법을 선택해야 합니다.

네트워크 아키텍처와 다음 조건에 따라 설치 방법을 선택합니다.

- 특별한 Kaspersky Industrial CyberSecurity for Nodes 설치 설정이나 권장 설치 설정의 필요 여부.

- 설치 설정이 모든 보호 중인 장치에서 같은지, 또는 보호 중인 장치에 따라 다른지.

Kaspersky Industrial CyberSecurity for Nodes는 설치 마법사를 사용하여 대화식으로 설치하거나 사용자가 개입 없이 숨김 모드로 설치할 수 있으며, 명령줄에서 설치 설정으로 설치 패키지 파일을 실행하여 호출할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes의 중앙 집중식 원격 설치는 Active Directory 그룹 정책을 사용하거나 Kaspersky Security Center 원격 설치 작업을 사용하여 수행할 수 있습니다.

구성 파일에 저장된 설정으로 Kaspersky Industrial CyberSecurity for Nodes를 단일 보호 중인 장치에 설치하고 구성할 수 있습니다. 그러면 이 파일을 사용하여 다른 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치할 수 있습니다. Active Directory 그룹 정책을 사용하여 애플리케이션을 설치한 경우에는 이 기능이 작동하지 않습니다.

설치 마법사 시작

설치 마법사는 다음을 설치할 수 있습니다.

- 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes 구성 요소(setupui.exe를 열거나 배포 키트에 있는 \exec\setup_kics.exe 파일로 바로 시작할 수 있는 시작 애플리케이션의 링크를 클릭).
- 보호 중인 장치나 LAN의 다른 장치에 Kaspersky Industrial CyberSecurity for Nodes 콘솔(setupui.exe를 열거나 배포 키트에 있는 \client\setup_kicstools.exe 파일로 바로 시작할 수 있는 시작 애플리케이션의 링크를 클릭).

필요한 설치 설정을 사용하여 명령줄에서 설치 패키지 파일 실행

명령줄 옵션 없이 설치 패키지 파일을 시작하면, Kaspersky Industrial CyberSecurity for Nodes가 기본 설정으로 설치됩니다. Kaspersky Industrial CyberSecurity for Nodes 옵션을 사용하여 설치 설정을 수정할 수 있습니다.

애플리케이션 콘솔은 보호 중인 장치 또는 관리자 워크스테이션에 설치할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 및 애플리케이션 콘솔 설치를 위한 샘플 명령을 사용할 수도 있습니다.

Kaspersky Security Center에서 중앙 집중식 설치

네트워크로 연결된 장치의 안티 바이러스 보호 관리를 위해 네트워크에서 Kaspersky Security Center를 사용한다면, 원격 설치 작업으로 Kaspersky Industrial CyberSecurity for Nodes를 여러 장치에 설치할 수 있습니다.

Kaspersky Security Center로 Kaspersky Industrial CyberSecurity for Nodes를 설치할 보호 중인 장치는 Kaspersky Security Center와 같거나 다른 도메인에 있을 수도 있고, 아무 도메인에도 없을 수 있습니다.

Active Directory 그룹 정책을 사용한 중앙 집중식 설치

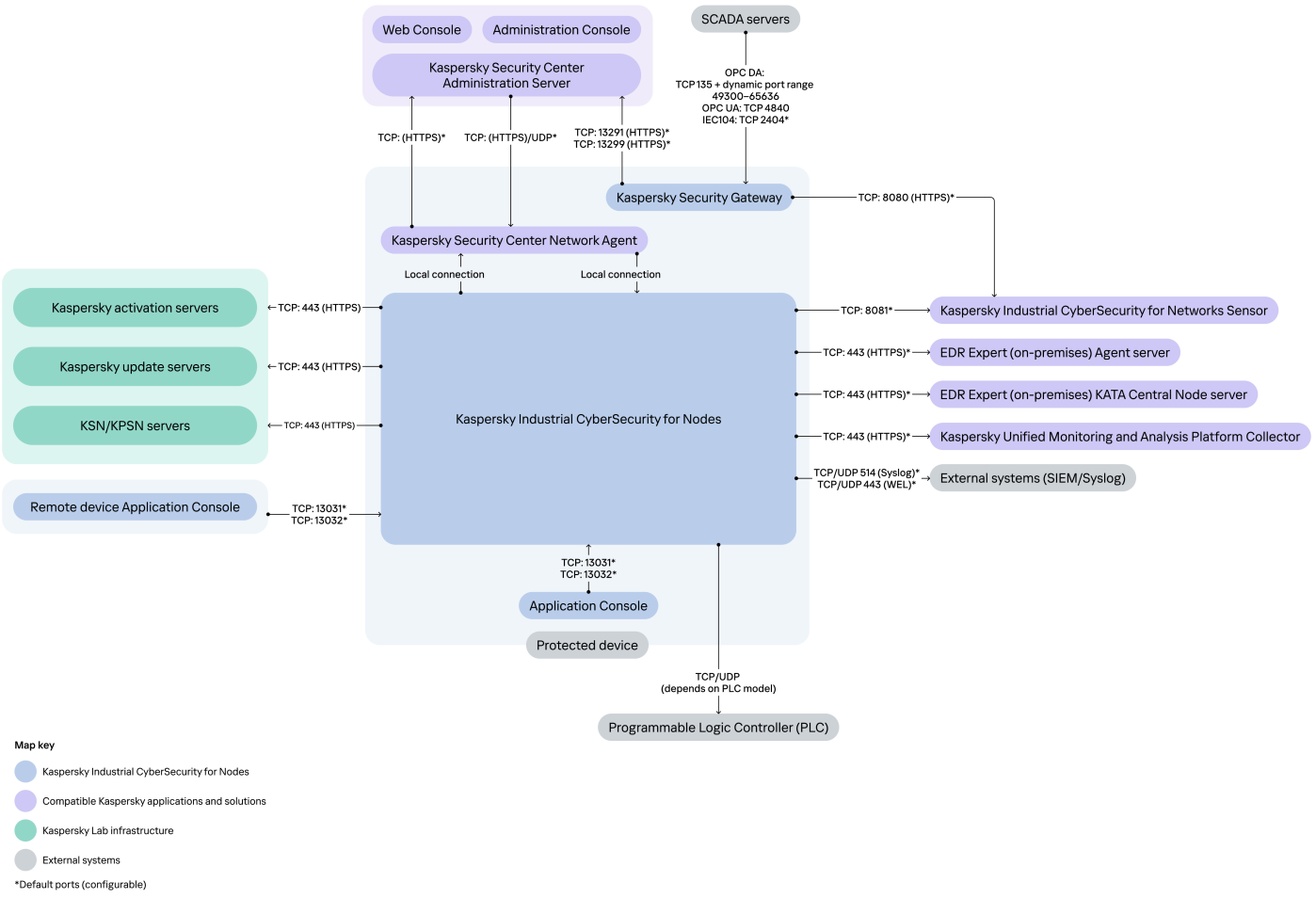
Active Directory 그룹 정책을 사용하여 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치할 수 있습니다. 애플리케이션 콘솔은 보호 중인 장치나 관리자 워크스테이션에 설치할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 권장 설치 설정만을 사용하여 설치할 수 있습니다.

Active Directory 그룹 정책을 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 설치한 보호 중인 장치는 같은 도메인 및 조직 단위에 있어야 합니다. 보호 중인 장치 시작 시, Microsoft Windows에 로그인하기 전에 설치가 수행됩니다.

사용되는 포트

Kaspersky Industrial CyberSecurity for Nodes 구성 요소를 설치하고 실행하려면 아래 다이어그램에 표시된 포트가 네트워크 장비 또는 네트워크 트래픽 제어 소프트웨어의 설정에서 열려 있어야 합니다.



Kaspersky Industrial CyberSecurity for Nodes에서 사용하는 포트

포트의 용도는 아래 표에 설명되어 있습니다.

사용되는 포트의 용도

용도	통신 주체		기본 포트	사용자 지정 포트 사용 가능	프로토콜
	소스	목적지			
Kaspersky Security Center에서 Kaspersky Industrial CyberSecurity for Nodes 관리	Kaspersky Security Center 중앙 관리 서버	Kaspersky Security Center 네트워크 에이전트	Kaspersky Security Center 도움말 을 참조하십시오	예	TCP(HTTPS), UDP(Kaspersky Security Center 도움말 참조)
	Kaspersky Security Center 네트워크 에이전트	Kaspersky Security Center 중앙 관리 서버			
Kaspersky Industrial CyberSecurity for Nodes Console을 사용하여 애플리케이션 관리	애플리케이션 콘솔	Kaspersky Industrial CyberSecurity for Nodes	13031, 13032	예	TCP
	원격 장치의 애플리케이션 콘솔	Kaspersky Industrial CyberSecurity for Nodes	13031, 13032	예	TCP

용도	통신 주체		기본 포트	사용자 지정 포트 사용 가능	프로토콜
	소스	목적지			
Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 소프트웨어 모듈 업데이트	Kaspersky Industrial CyberSecurity for Nodes	Kaspersky 업데이트 서버	443	아니오	TCP(HTTPS)
Kaspersky Industrial CyberSecurity for Nodes 활성화	Kaspersky Industrial CyberSecurity for Nodes	Kaspersky 활성화 서버	443	아니오	TCP(HTTPS)
KSN 사용	Kaspersky Industrial CyberSecurity for Nodes	KSN/KPSN 서버	443	아니오	TCP(HTTPS)
Kaspersky Industrial CyberSecurity for Networks 통합	Kaspersky Industrial CyberSecurity for Nodes	Kaspersky Industrial CyberSecurity for Networks 센서	8081	예	TCP
Kaspersky Security Gateway 사용	Kaspersky Security Gateway	Kaspersky Security Center 중앙 관리 서버	13291, 13299	예	TCP(HTTPS)
	Kaspersky Security Gateway	Kaspersky Industrial CyberSecurity for Networks 센서	8080	예	TCP(HTTPS)
	SCADA 서버	Kaspersky Security Gateway	OPC DA: 135 + 동적 포트 범위 49300–65635 OPC UA: 4840 IEC104: 2404	예	TCP
Endpoint Detection and Response Expert(on-premises) 통합	Kaspersky Industrial CyberSecurity for Nodes	EDR Expert(on-premises) 에이전트 서버	443	예	TCP(HTTPS)
	Kaspersky Industrial CyberSecurity for Nodes	EDR Expert(on-premises) KATA Central Node 서버	443	예	TCP(HTTPS)
	Kaspersky Industrial CyberSecurity for Nodes	KUMA 컬렉터	443	예	TCP(HTTPS)

용도	통신 주체		기본 포트	사용자 지정 포트 사용 가능	프로토콜
	소스	목적지			
산업 네트워크 보호	Kaspersky Industrial CyberSecurity for Nodes	Siemens SIMATIC S7-300	102	예	TCP
		Siemens SIMATIC S7-400			
		Siemens SIMATIC S7-400H			
		Siemens SIMATIC S7-1200			
		Siemens SIMATIC S7-1500			
		Siemens SIPROTEC 4	50000	예	UDP
		Schneider Electric Modicon M340	502	예	TCP
		Schneider Electric Modicon M580			
		CODESYS V3를 기반으로 한 장치	11740	예	TCP
		OWEN PLC210			
		Fastwel CPM723-01			
		Prosoft Systems Regul R500			
		Emerson DeltaV	23(Telnet), 18550	예	TCP
		Rockwell Automation Allen-Bradley ControlLogix	44818	예	TCP
		TREI-5B	6000	예	TCP
SIEM 통합	Kaspersky Industrial CyberSecurity for Nodes	SIEM / Syslog 서버	Syslog: 514 WEL: 443	예	TCP/UDP(사용자 지정 가능)

마법사를 사용하여 애플리케이션 설치 및 제거

이 섹션에서는 설치 마법사를 사용하여 Kaspersky Industrial CyberSecurity for Nodes와 애플리케이션 콘솔을 설치 및 제거하는 방법, Kaspersky Industrial CyberSecurity for Nodes의 추가 구성과 설치 시 수행해야 하는 동작에 관해 설명합니다.

설치 마법사를 사용한 설치

다음 섹션에는 Kaspersky Industrial CyberSecurity for Nodes 및 애플리케이션 콘솔의 설치에 관한 정보가 포함되어 있습니다.

Kaspersky Industrial CyberSecurity for Nodes를 설치하고 사용하려면:

1. 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치하십시오.
2. Kaspersky Industrial CyberSecurity for Nodes를 관리할 장치에 애플리케이션 콘솔을 설치하십시오.
3. 네트워크에서 보호 중인 장치 이외의 장치에 애플리케이션 콘솔이 설치된 경우, 애플리케이션 콘솔 사용자가 Kaspersky Industrial CyberSecurity for Nodes를 원격으로 관리할 수 있도록 추가 구성을 수행합니다.
4. Kaspersky Industrial CyberSecurity for Nodes 설치 후 작업을 수행합니다.

Kaspersky Industrial CyberSecurity for Nodes 설치

Kaspersky Industrial CyberSecurity for Nodes를 설치하기 전에 다음을 수행합니다:

1. 보호 중인 장치에 다른 안티 바이러스 애플리케이션이 설치되지 않도록 확인합니다.
2. 설치 마법사를 실행할 때 사용하는 계정이 보호 중인 장치의 관리자 그룹에 속하는지 확인합니다.

위에서 설명한 동작을 수행한 후 설치 절차를 진행합니다. 설치 마법사의 지침에 따라 Kaspersky Industrial CyberSecurity for Nodes 설치를 위한 설정을 지정합니다.

설치(설치 제거) 설정에 대해 추가 정보를 얻을 수 있습니다.

설치 마법사를 통해 Kaspersky Industrial CyberSecurity for Nodes를 설치하려면:

1. 보호 중인 장치에서 setupui.exe 파일을 실행합니다.
2. 창이 열리면 **설치**에서 **Kaspersky Industrial CyberSecurity for Nodes 5.0 설치** 링크를 따라갑니다.
3. Kaspersky Industrial CyberSecurity for Nodes 설치 마법사의 시작 화면에서 **다음 >** 버튼을 클릭합니다.
   최종 사용자 라이센스 계약서 창이 열립니다.
4. 라이센스 계약서 및 개인정보취급방침을 검토합니다.
5. 최종 사용자 라이센스 계약서와 개인정보취급방침의 약관에 동의하면 **최종 사용자 라이센스 계약서의 이용 약관을 완전히 읽고 이해했으며, 수락함을 확인합니다** 및 **본인은 개인정보 취급방침에 설명된 대로 본인의 개인정보가 취급 및 전송(제3국 전송 포함)된다는 것을 알고 이에 동의합니다. 본인은 개인정보 취급방침을 모두 읽고 이해했음을 확인합니다** 확인란을 선택합니다.

   최종 사용자 라이센스 계약서 또는 개인정보취급방침에 동의하지 않으면 설치가 중단됩니다.

6. **다음 >** 버튼을 클릭합니다.

   사용자 지정 설치 창이 열립니다. 설치할 구성 요소를 선택합니다.

   - **전체 기능**

     기본적으로 성능 계수기 및 Endpoint Agent를 제외한 모든 Kaspersky Industrial CyberSecurity for Nodes 구성 요소를 설치할 것을 권장합니다.

Kaspersky Industrial CyberSecurity for Nodes의 SNMP 프로토콜 지원 구성 요소는 보호 중인 장치에 Microsoft Windows SNMP 서비스가 설치되었을 때만 설치 제안 구성 요소 목록에만 표시됩니다.

- **Endpoint Agent**

  이 옵션을 선택하면 Endpoint Agent 구성에 Kaspersky Industrial CyberSecurity for Nodes가 설치됩니다. 이 구성에 대한 자세한 내용은 이 섹션을 참조하십시오.

7. **다음 >** 버튼을 클릭합니다.
8. **대상 폴더 선택** 창에서 다음을 수행합니다:
   - 필요한 경우 Kaspersky Industrial CyberSecurity for Nodes 파일을 복사할 폴더를 지정합니다.
   - 필요한 경우 **찾아보기** 버튼을 클릭하여 로컬 드라이브에서 사용 가능한 공간에 대한 정보를 검토합니다.
9. **다음 >** 버튼을 클릭합니다.
10. **기본 폴더 변경** 창에서 애플리케이션이 사용하는 폴더의 경로를 편집할 수 있습니다.

    설치 폴더의 경로가 애플리케이션 데이터베이스 폴더, 백업 폴더, 격리 저장소의 개체 복구용 폴더, 임시 파일 폴더 중 하나 이상의 경로와 같다면 오류와 함께 애플리케이션 설치가 종료됩니다.

11. **고급 설정** 창에서 개체 및 폴더를 보호 범위에서 제외하고 실시간 파일 보호를 구성할 수 있습니다.

    필요하다면 산업 애플리케이션 예외 프로필을 선택합니다. 이는 신뢰하는 프로세스 및 예외 목록에 산업 애플리케이션 프로세스 및 파일을 추가하고 애플리케이션 실행 제어 규칙 및 설정을 구성하기 위한 구성 규칙의 XML 집합입니다.

    실시간 파일 보호 실행 모드를 선택하지 않으면 설치 마법사의 다음 단계로 진행할 수 없습니다.

12. **다음 >** 버튼을 클릭합니다.
13. 이전 버전의 애플리케이션에서 생성된 기존 구성 파일에서 Kaspersky Industrial CyberSecurity for Nodes 설정을 가져오려면, **구성 파일에서 설정 가져오기** 창에서 구성 파일의 경로를 지정합니다.
14. **다음 >** 버튼을 클릭합니다.
15. **원격 액세스 설정** 섹션에서 필요하다면 애플리케이션 콘솔에서 애플리케이션이 설치된 컴퓨터에 원격으로 연결하는 데 사용되는 TCP 포트 번호를 변경합니다.

    Windows 자격 증명을 사용하여 연결하기 위한 기본 포트 번호는 13032이며, 수동 생성 사용자의 자격 증명을 사용하여 연결하기 위한 기본 포트 번호는 13031입니다. 가능한 포트 번호 범위: 1~65535.

    수동으로 생성한 사용자 계정의 자격 증명으로 연결하는 것을 방지하기 위해 **수동으로 생성된 사용자의 자격 증명을 사용** 확인란을 선택 해제합니다.

16. **다음 >** 버튼을 클릭합니다.

17. **애플리케이션 활성화** 창에서 다음 중 하나를 수행합니다:

    - 애플리케이션을 활성화하려면 애플리케이션 활성화를 위해 Kaspersky Industrial CyberSecurity for Nodes 키 파일을 지정합니다.
    - 나중에 애플리케이션을 활성화하려면 **다음 >** 버튼을 클릭합니다.
    - 이전에 배포 키트의 \exec 폴더에 키 파일을 저장했다면, 이 파일의 이름이 **키** 필드에 표시됩니다.

    키 파일이 추가되면 라이센스 정보가 창에 표시됩니다. Kaspersky Industrial CyberSecurity for Nodes가 라이센스의 계산된 만료 날짜를 표시합니다. 라이센스 기간은 키를 추가한 시간부터 시작되어 키 파일 만료 날짜에 만료됩니다.

18. **다음 >** 버튼을 클릭해 애플리케이션에 키 파일을 추가합니다.

19. 필요하다면 **설치 준비** 창에서 **설치 프로세스 보호** 옵션을 비활성화할 수 있습니다. 설치 보호는 악성 애플리케이션에 의한 배포 패키지 변조 차단, Kaspersky Industrial CyberSecurity for Nodes 설치 폴더 접근 차단, 애플리케이션 키가 포함된 시스템 레지스트리 섹션 접근 차단 등이 포함됩니다. 하지만, 애플리케이션을 설치할 수 없는 경우(예, Windows Remote Desktop으로 원격 설치를 수행할 때), 설치 프로세스의 보호를 해제하십시오.

20. 필요하다면 명령줄 인터페이스를 편리하게 사용할 수 있도록 %PATH% 시스템 변수에 kavshell.exe 파일 경로를 추가할 수 있습니다.

21. **설치** 버튼을 클릭합니다.

    마법사가 Kaspersky Industrial CyberSecurity for Nodes 설치를 시작합니다. 설치가 완료되면 **애플리케이션 설치 마법사 종료** 창이 열립니다.

22. **마침** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔 설치

설치 마법사의 지시에 따라 애플리케이션 콘솔의 설치 설정을 조정합니다. 설치 프로세스는 마법사의 어느 단계에서나 중지할 수 있습니다. 중지하려면 설치 마법사 창에서 **취소** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔을 설치하려면, 다음을 실행합니다.

1. 설치 마법사를 실행하는 데 사용하는 계정이 장치의 관리자 그룹에 속하는지 확인하십시오.

2. 보호 중인 장치에서 setupui.exe 파일을 실행합니다.

   시작 창이 열립니다.

3. **Kaspersky Industrial CyberSecurity for Nodes 콘솔 설치** 링크를 클릭합니다.

   설치 마법사 시작 창이 열립니다.

4. **다음 >** 버튼을 클릭합니다.

5. 최종 사용자 라이센스 계약서와 개인정보취급방침의 약관에 동의하면 **최종 사용자 라이센스 계약서의 이용 약관을 완전히 읽고 이해했으며, 수락함을 확인합니다** 및 **본인은 개인정보 취급방침에 설명된 대로 본인의 개인정보가 취급 및 전송(제3국 전송 포함)된다는 것을 알고 이에 동의합니다. 본인은 개인정보 취급방침을 모두 읽고 이해했음을 확인합니다** 확인란을 선택합니다.

6. 필요한 경우 **대상 폴더 선택** 창에서 설치 파일을 저장할 다른 폴더를 지정합니다.

7. **다음 >** 버튼을 클릭합니다.

8. **설치 준비** 창의 **설치** 버튼을 클릭합니다.

   마법사가 Kaspersky Industrial CyberSecurity for Nodes 콘솔 설치를 시작합니다.

9. **마침** 버튼을 클릭합니다.

애플리케이션 콘솔이 설치됩니다.

네트워크에서 보호 중인 장치가 아닌 다른 장치에 애플리케이션 콘솔이 설치된 경우, 고급 설정을 구성합니다.

다른 장치에 애플리케이션 콘솔을 설치한 후의 고급 설정

네트워크에서 보호 중인 장치 외의 장치에 애플리케이션 콘솔이 설치되었다면, 다음 동작을 수행하여 사용자가 Kaspersky Industrial CyberSecurity for Nodes를 원격 관리할 수 있도록 합니다.

- 애플리케이션 설정에서 원격 연결 권한이 있는 사용자 계정을 사용합니다. 기본적으로 관리자 그룹과 KICS 관리자 그룹의 모든 사용자는 이 권한을 보유합니다.
- 원격 장치의 Windows 방화벽 설정에서 Windows 시스템 사용자 계정의 연결을 위한 TCP 13032 포트를 열고 애플리케이션 설정에서 수동으로 생성한 사용자 계정의 연결을 위한 TCP 13031 포트를 엽니다. Kaspersky Industrial CyberSecurity for Nodes 원격 관리 프로세스의 실행 파일인 avp.exe의 네트워크 연결도 허용합니다. 명령줄에서 애플리케이션을 설치할 때 `ADDWFEXCLUSION=1` 옵션을 사용하여 이 설정을 관리할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes를 원격으로 실행해야 하는 경우 추가로 다음을 수행하십시오.

애플리케이션을 원격으로 시작할 사용자 계정이 관리자 그룹에 속해 있어야 합니다. 이 계정에 Kaspersky Industrial CyberSecurity for Nodes를 관리하고 Kaspersky Industrial CyberSecurity for Nodes 서비스을 관리하는 데 필요한 권한이 있는지 확인합니다.

- 원격 장치의 Windows 방화벽 설정에서 **파일 및 프린터 공유(SMB-In)** 규칙(포트 TCP 445)을 활성화하십시오. 또한 장치와의 원활한 연결을 위해 TCP 135 포트를 여는 것이 좋습니다.
- Windows Vista 이상을 실행하고 도메인에 포함되지 않거나 로컬 사용자 계정이 관리하는 원격 장치의 경우, **사용자 계정 원격 제어(UAC)를 비활성화합니다.**

  1. 컴퓨터에서 레지스트리 편집기를 엽니다.
  2. 레지스트리 편집기에서 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System 키를 엽니다.
  3. LocalAccountTokenFilterPolicy 값을 엽니다.

     이 키 아래 LocalAccountTokenFilterPolicy 값이 누락된 경우 이 이름으로 DWORD(32비트) 값을 생성합니다(자세한 내용은 Microsoft 기술 지원 웹사이트를 참조하십시오).

  4. 1로 설정하고 **확인**을 클릭합니다.

     원격 UAC를 비활성화해도 로컬 UAC에는 영향이 없습니다.

- 애플리케이션 콘솔이 설치된 장치 또는 보호 중인 장치에서 Windows 8.1 또는 이전 버전의 Windows를 실행하는 경우, **Windows 10 이상을 실행하는 장치에서 SMB 1.0/CIFS 파일에 대한 공유 접근 지원을 활성화합니다.**

  - "Windows 기능" 애플리케이션에서

    1. **시작 → 제어판 → 프로그램 및 기능 → Windows 기능 켜기/끄기** 옵션을 선택합니다.
    2. **Windows 기능** 창에서 **SMB 1.0/CIFS 파일 공유 지원** 확인란을 선택합니다.
    3. **확인**을 누릅니다.

  - Windows PowerShell에서:

    1. Windows PowerShell을 관리자 권한으로 실행합니다.
    2. 다음 명령을 실행합니다:

    ```
    Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
    ```

다른 소프트웨어나 하드웨어 방화벽을 구성할 때도 같은 단계를 적용해야 합니다.

보호 중인 장치와 애플리케이션 콘솔이 설치된 장치 간의 연결을 구성할 때 애플리케이션 콘솔이 열려 있다면:

1. 애플리케이션 콘솔을 닫습니다.
2. Kaspersky Industrial CyberSecurity for Nodes 원격 관리 프로세스 avp.exe가 완료될 때까지 기다립니다.
3. 애플리케이션 콘솔을 다시 시작합니다.
   새 연결 설정이 적용됩니다.

Kaspersky Industrial CyberSecurity for Nodes 설치 후 수행할 동작

Kaspersky Industrial CyberSecurity for Nodes를 활성화했다면, 애플리케이션 설치 직후 보호 및 검사 작업이 시작됩니다. Kaspersky Industrial CyberSecurity for Nodes 설치 시 **애플리케이션 설치 후 실시간 파일 보호 활성화(권장 사항)**(기본 옵션) 옵션을 선택했다면, 장치의 파일 시스템 개체에 접근할 때 애플리케이션이 이 개체를 검사합니다. 사용자 지정 설치 과정에서 스크립트 모니터링 구성 요소를 설치했다면, 스크립트를 시작할 때 Kaspersky Industrial CyberSecurity for Nodes가 모든 스크립트의 소스 코드를 검사합니다. Kaspersky Industrial CyberSecurity for Nodes는 매주 금요일 오후 8시에 *중요 영역 검사* 작업을 실행합니다.

Kaspersky Industrial CyberSecurity for Nodes 설치 후에는 다음 단계 수행을 권장합니다.

- 애플리케이션 데이터베이스 업데이트 작업을 시작합니다. 설치 후 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 배포 키트에 포함된 데이터베이스를 사용하여 개체를 검사합니다.

  Kaspersky Industrial CyberSecurity for Nodes 데이터베이스가 만료되었을 수 있으므로 즉시 업데이트하는 것이 좋습니다.

  그러면 애플리케이션이 작업에서 구성된 기본 일정에 따라 매시간 데이터베이스를 업데이트합니다.

- Kaspersky Industrial CyberSecurity for Nodes 설치 전에 장치에 실시간 파일 보호 기능이 있는 안티 바이러스 소프트웨어가 설치되어 있지 않았다면, 장치에서 중요 영역 검사를 실행합니다.
- Kaspersky Industrial CyberSecurity for Nodes 이벤트에 대한 관리자 알림을 구성합니다.

데이터베이스 및 애플리케이션 모듈 업데이트 작업 시작 및 구성

설치 후 애플리케이션 데이터베이스를 업데이트하려면:

1. *업데이트*에서 업데이트 경로에 대한 연결을 구성합니다.
2. *업데이트* 작업을 실행합니다.

네트워크에서 웹 프록시 자동 검색 프로토콜(Web Proxy Auto-Discovery Protocol, WPAD)이 LAN에서 프록시 서버 설정을 자동 감지하도록 구성되지 않을 수 있습니다. 이를 위해 네트워크에서 프록시 서버에 접근할 때 인증을 요구할 수 있습니다.

선택적인 프록시 서버 설정과 프록시 서버 접근을 위한 인증 설정을 지정하려면:

1. 애플리케이션 콘솔에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 마우스 오른쪽 메뉴를 엽니다.
2. **애플리케이션 속성** 옵션을 선택합니다.
3. 열린 창에서 **네트워크 설정** 탭을 선택합니다.
4. **프록시 서버 설정** 섹션에서 **설정** 버튼을 클릭하고, 열린 창에서 **지정한 프록시 서버 설정 사용** 확인란을 선택합니다.
5. **주소** 필드에 프록시 서버 주소를 입력하고 **포트** 필드에 프록시 서버의 포트 번호를 입력합니다.
6. 필요하다면 **로컬 주소에 대해 프록시 서버 우회** 확인란을 선택 해제합니다. 이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 설치된 보호 중인 장치를 호스팅하는 네트워크에서 직접 장치에 접근합니다. 이 옵션은 기본적으로 활성화되어 있습니다.
7. **프록시 서버 인증 설정** 섹션에서 드롭다운 목록으로 필요한 인증 방법을 선택합니다.
   - **인증 사용하지 않음**.
   - **NTLM 인증**. 현재 사용자 계정을 사용한 NTLM 인증(기본값).
   - **사용자 이름 및 암호를 사용한 NTLM 인증**. 직접 지정한 자격 증명을 사용한 NTLM 인증.
   - **Kerberos 인증**. 현재 사용자 계정을 사용한 Kerberos 인증.

     프록시 서버 주소로 CNAME 레코드를 사용할 때 Kerberos 인증이 올바르게 작동하도록 하려면 각 CNAME 레코드에 대해 SPN(서비스 사용자 이름)을 등록해야 합니다.

   - **사용자 이름 및 암호를 사용한 Kerberos 인증**. 직접 지정한 자격 증명을 사용한 Kerberos 인증.
   - **사용자 이름 및 암호**. 직접 지정한 자격 증명을 사용한 인증.

   필요한 경우 사용자 이름 및 암호를 입력합니다.

Kerberos 인증을 선택한 경우, 프록시 서버 설정에 따라 Kaspersky Industrial CyberSecurity for Nodes는 Kerberos 또는 NTLM 프로토콜을 사용하여 인증을 수행합니다.

8. **확인**을 누릅니다.

업데이트 작업을 실행하려면:

1. 애플리케이션 콘솔 트리에서 **업데이트** 노드를 확장합니다.
2. **데이터베이스 업데이트** 하위 노드의 마우스 오른쪽 메뉴에서, **시작** 항목을 선택합니다.

   업데이트 작업이 시작됩니다.

작업을 완료한 후 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 결과 창에서 설치된 최신 데이터베이스 업데이트의 릴리스 날짜를 확인할 수 있습니다.

중요 영역 검사

Kaspersky Industrial CyberSecurity for Nodes 데이터베이스를 업데이트한 후 *중요 영역 검사* 작업을 사용하여 보호 중인 장치에서 악성 코드를 검사하십시오.

중요 영역 검사 작업을 실행하려면:

1. 애플리케이션 콘솔 트리에서 **온디맨드 검사** 노드를 확장합니다.
2. **중요 영역 검사** 하위 노드의 마우스 오른쪽 메뉴에서 **시작** 명령을 선택합니다.

작업이 시작되고 작업 영역에 **실행 중** 작업 상태가 표시됩니다.

작업 로그를 보려면,

중요 영역 검사 노드의 결과 창에서 **작업 로그 열기** 링크를 클릭합니다.

구성 요소 집합 수정 및 Kaspersky Industrial CyberSecurity for Nodes 복구

Kaspersky Industrial CyberSecurity for Nodes 구성 요소를 추가하거나 제거할 수 있습니다. 실시간 파일 보호 구성 요소를 제거하려면 실시간 파일 보호 작업을 중지해야 합니다. 그 밖의 상황에서는 실시간 파일 보호 작업이나 Kaspersky Industrial CyberSecurity for Nodes 서비스를 중지할 필요가 없습니다.

애플리케이션 관리가 암호로 보호되어 있으면, 설치 마법사에서 구성 요소를 제거하거나 구성 요소 집합을 수정하려고 할 때 Kaspersky Industrial CyberSecurity for Nodes가 암호를 요청합니다.

Kaspersky Industrial CyberSecurity for Nodes 구성 요소 세트를 수정하려면:

1. Windows **제어판**에서 **앱 및 기능**을 선택합니다. **수정 또는 제거** 창이 열립니다.
2. **Kaspersky Industrial CyberSecurity for Nodes**를 우클릭하고 **편집**을 선택합니다.

   설치 마법사 **애플리케이션 수정, 복구 또는 제거** 창이 열립니다.

3. **수정** 옵션을 선택합니다.

   사용자 지정 설치 창이 열립니다. **전체 기능** 옵션을 선택하고 **다음(N) >** 버튼을 클릭합니다.

4. **사용자 지정 설치** 창의 사용 가능한 구성 요소 목록에서, Kaspersky Industrial CyberSecurity for Nodes에서 추가하거나 제거할 구성 요소를 선택합니다. 이를 위해서는 다음 동작을 수행합니다.

   - 구성 요소 세트를 변경하려면 선택한 구성 요소 이름 옆에 있는 버튼을 클릭합니다. 마우스 오른쪽 메뉴에서 다음을 선택합니다.

     - 구성 요소 하나를 설치하려면 **로컬 하드 드라이브에 기능을 설치합니다**.

     - 구성 요소 그룹을 설치하려면 **로컬 하드 드라이브에 전체 기능 및 그 하위 기능을 설치합니다**.

   - 이전에 설치한 구성 요소를 제거하려면 선택한 구성 요소 이름 옆의 버튼을 클릭합니다. 마우스 오른쪽 메뉴에서 **기능을 이용할 수 없게 됩니다**를 선택합니다.

   다음(N) > 버튼을 클릭합니다.

5. **설치 준비** 창에서 **설치** 버튼을 클릭하여 애플리케이션 구성 요소의 조회를 확인합니다.

6. 설치가 완료되면 열린 창에서 **마침** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes 구성 요소 세트가 지정된 설정에 따라 수정됩니다.

Kaspersky Industrial CyberSecurity for Nodes 작동 중에 문제가 발생한다면(Kaspersky Industrial CyberSecurity for Nodes가 크래시, 작업이 크래시되거나 시작되지 않음), Kaspersky Industrial CyberSecurity for Nodes의 복구를 수행할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes의 현재 설정을 저장하면서 복원하거나 Kaspersky Industrial CyberSecurity for Nodes 설정 모두를 기본값으로 재설정하는 옵션을 선택할 수도 있습니다.

애플리케이션이나 작업이 크래시된 후 Kaspersky Industrial CyberSecurity for Nodes를 복구하려면:

1. Windows **제어판**에서 **앱 및 기능**을 선택합니다. **수정 또는 제거** 창이 열립니다.

2. **Kaspersky Industrial CyberSecurity for Nodes**를 우클릭하고 **편집**을 선택합니다.

3. 설치 마법사 **애플리케이션 수정, 복구 또는 제거** 창이 열립니다.

4. **복구** 옵션을 선택합니다.

   Kaspersky Industrial CyberSecurity for Nodes 복구 창이 열립니다. **다음(N) >** 버튼을 클릭합니다.

5. 복원 작업이 완료될 때까지 기다렸다가 창이 열리면 **마침** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes가 지정된 설정을 사용하여 복구됩니다.

설치 마법사를 사용한 제거

이 섹션에는 설정/제거 마법사를 사용하여 보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes 및 애플리케이션 콘솔을 제거하는 방법에 관한 지침이 포함되어 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 제거

Kaspersky Industrial CyberSecurity for Nodes 제거 시 덤프 및 추적 파일은 삭제되지 않습니다. 덤프 및 추적 파일 쓰기 구성 중에 지정한 폴더에서 덤프 및 추적 파일을 직접 삭제할 수 있습니다.

설정 이름은 설치된 Windows 운영 체제마다 다를 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 설치/제거 마법사를 사용하여 보호 중인 장치에서 제거할 수 있습니다.

보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes를 제거한 후 다시 시작해야 할 수 있습니다. 나중에 다시 시작할 수도 있습니다.

Windows 제어판에서는 해당 애플리케이션의 설치, 제거 및 복구 기능을 사용할 수 없습니다.

Kaspersky Industrial CyberSecurity for Nodes는 사용자가 설치 마법사에서 구성 요소 집합을 제거하거나 수정하려고 시도할 때 사용자 계정의 자격 증명을 요청합니다. 충분한 권한이 있는 사용자 자격 증명을 입력해야 합니다. 제거를 수행하는 사용자 계정에 Windows 암호가 공란으로 설정되어 있는 경우, 제거를 시작하기 전 **중요 작업을 확인하기 위한 암호 요청** 기능을 비활성화합니다.

Kaspersky Industrial CyberSecurity for Nodes를 제거하려면:

1. Windows **제어판**에서 **앱 및 기능**을 선택합니다. **수정 또는 제거** 창이 열립니다.
2. **Kaspersky Industrial CyberSecurity for Nodes**를 우클릭하고 **편집**을 선택합니다.
3. 설치 마법사 **애플리케이션 수정, 복구 또는 제거** 창이 열립니다.
4. **제거** 옵션을 선택합니다.
   개체 저장 창이 열립니다.
5. 필요하다면 **개체 저장** 창에서 다음을 수행합니다.
   개체 저장에서 유지할 개체 또는 설정을 지정합니다. 확인란은 기본적으로 선택이 취소됩니다.
   - **활성화 데이터** 확인란을 선택합니다.
   - **백업 파일** 확인란을 선택합니다.
   - **애플리케이션 운영 설정** 확인란을 선택합니다.

개체 내보내기에서 내보낼 개체를 지정합니다. 확인란은 기본적으로 선택이 취소됩니다.

- Kaspersky Industrial CyberSecurity for Nodes가 격리된 개체를 내보내게 하려면 **격리된 개체 내보내기** 확인란을 선택합니다. 기본적으로 확인란의 선택이 취소됩니다.
- Kaspersky Industrial CyberSecurity for Nodes 백업 저장소에서 개체를 내보내려면 **백업 개체 내보내기** 확인란을 선택합니다. 기본적으로 확인란의 선택이 취소됩니다.
- **저장** 버튼을 클릭하고 개체를 내보낼 폴더를 선택합니다. 개체를 내보내는 기본 위치는 %ProgramData%\Kaspersky Lab\KICS.5.0\QB입니다.

  다음 버튼을 클릭합니다.

6. **제거 준비** 창에서 **제거** 버튼을 클릭하여 제거를 확인합니다.
7. 제거가 완료되면 열린 창에서 **마침** 버튼을 클릭합니다.

보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes가 제거됩니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔 제거

설정 이름은 설치된 Windows 운영 체제마다 다를 수 있습니다.

설치/제거 마법사를 사용하여 보호 중인 장치에서 애플리케이션 콘솔을 제거할 수 있습니다.

애플리케이션 콘솔을 제거한 후에는 보호 중인 장치를 다시 시작할 필요가 없습니다.

애플리케이션 콘솔을 제거하려면:

1. Windows **제어판**에서 **앱 및 기능**을 선택합니다. **수정 또는 제거** 창이 열립니다.
2. **Kaspersky Industrial CyberSecurity for Nodes 콘솔**을 우클릭하고 **편집**을 선택합니다.

   애플리케이션 수정, 복구 또는 제거 마법사 창이 열립니다.
3. **제거** 옵션을 선택합니다.

   제거 준비 창이 열립니다. **제거** 버튼을 클릭합니다.
4. 제거가 완료되면 열린 창에서 **정상** 버튼을 클릭합니다.

제거가 완료되면 설치 마법사가 닫힙니다.

명령줄에서 애플리케이션 설치 및 설치 제거

이 섹션에서는 명령줄을 통한 Kaspersky Industrial CyberSecurity for Nodes 설치 및 설치 제거 방법을 자세히 설명하고, 명령줄에서 Kaspersky Industrial CyberSecurity for Nodes를 설치 및 설치 제거하는 명령 예제와 명령줄에서 Kaspersky Industrial CyberSecurity for Nodes 구성 요소를 추가 및 제거하는 명령 예제를 보여줍니다.

명령줄을 통한 Kaspersky Industrial CyberSecurity for Nodes 설치 및 제거 정보

Kaspersky Industrial CyberSecurity for Nodes 제거 시 덤프 및 추적 파일은 삭제되지 않습니다. 덤프 및 추적 파일 쓰기 구성 중에 지정한 폴더에서 덤프 및 추적 파일을 직접 삭제할 수 있습니다.

명령줄 옵션으로 설치 설정을 지정한 후 명령줄에서 \exec\kics_win.msi 설치 패키지 파일을 실행하여 Kaspersky Industrial CyberSecurity for Nodes를 설치/제거하고 그 구성 요소를 추가/제거할 수 있습니다.

보호 중인 장치나 네트워크의 다른 장치에 Kaspersky Industrial CyberSecurity for Nodes 콘솔을 설치해 애플리케이션을 사용해 로컬 또는 원격 작업할 수 있습니다. 이를 위해서는 \client\kicstools.msi 설치 패키지를 사용하십시오.

애플리케이션이 설치된 보호 중인 장치의 관리자 그룹에 포함된 계정으로 설치하십시오.

보호 중인 장치에서 추가 명령줄 옵션 없이 \exec\kics_win.msi 파일을 실행하면 Kaspersky Industrial CyberSecurity for Nodes가 기본 설치 설정으로 설치됩니다.

ADDLOCAL 명령줄 옵션을 사용하고 선택한 구성 요소나 구성 요소 세트의 코드를 나열하여 설치할 구성 요소 세트를 할당할 수 있습니다.

Windows Installer 서비스용 Kaspersky Industrial CyberSecurity for Nodes 소프트웨어 구성 요소 코드

\exec\kics_win.msi 파일은 Kaspersky Industrial CyberSecurity for Nodes를 설치하도록 설계되었습니다.

\client\kicstools.msi 파일은 Kaspersky Industrial CyberSecurity for Nodes 콘솔을 설치하도록 설계되었습니다.

다음 표에는 Kaspersky Industrial CyberSecurity for Nodes 소프트웨어 구성 요소의 코드와 설명이 포함되어 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 소프트웨어 구성 요소의 설명

구성 요소	코드	구성 요소 기능
실시간 파일 보호	`FileThreatProtection`	이 구성 요소는 이러한 파일에 접근할 때 보호 중인 장치에서 파일의 바이러스 검사를 수행합니다.
AMSI 스캐너	`AMSI`	이 구성 요소는 Microsoft의 Antimalware Scan Interface를 지원합니다. AMSI(Antimalware Scan Interface)를 사용하는 경우 AMSI를 지원하는 타사 애플리케이션이 추가 검사를 위해 Kaspersky Industrial CyberSecurity for Nodes에 PowerShell 스크립트 등의 개체를 전송하고 해당 개체에 대한 검사 결과를 받을 수 있습니다.
Anti-Cryptor	`BehaviorDetection`	이 구성 요소는 차단된 호스트 목록에 악성 활동을 보이는 원격 장치의 이름을 기록합니다.
익스플로잇 방지	`ExploitPrevention`	이 구성 요소를 사용하면 장치의 메모리에서 프로세스가 사용하는 메모리를 보호하기 위한 설정을 관리할 수 있습니다.
복원 엔진	`RemediationEngine`	이 구성 요소를 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 운영 체제에서 악성 코드가 수행한 활동을 롤백합니다.

구성 요소	코드	구성 요소 기능
방화벽	`Firewall`	이 구성 요소를 이용하면 Kaspersky Industrial CyberSecurity for Nodes 그래픽 사용자 인터페이스를 통해 Windows 방화벽을 관리할 수 있습니다.
네트워크 위협 보호	`NetworkThreatProtection`	이 구성 요소는 인바운드 네트워크 트래픽에 네트워크 공격을 위한 일반적인 활동이 있는지 검사합니다. 사용자 컴퓨터를 표적으로 하는 네트워크 공격 시도가 탐지되면 Kaspersky Industrial CyberSecurity for Nodes가 공격 컴퓨터의 네트워크 활동을 차단합니다.
애플리케이션 실행 제어	`ApplicationControl`	이 구성 요소는 애플리케이션을 시작하려는 사용자 시도를 모니터링하고 특정 애플리케이션 실행 제어 규칙에 따라 애플리케이션의 시작을 허용하거나 거부합니다.
장치 제어	`DeviceControl`	이 구성 요소는 보호 중인 장치에 외부 장치를 연결하려는 시도를 추적하고 지정된 장치 제어 규칙에 따라 해당 장치의 사용을 허용하거나 거부합니다.
Kaspersky Security Center 네트워크 에이전트와의 통합을 위한 모듈	`AdminKitConnector`	Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Security Center 네트워크 에이전트를 연결합니다. Kaspersky Security Center에서 애플리케이션을 관리하려는 경우 보호 중인 장치에 이 구성 요소를 설치할 수 있습니다.
로그 검사	`LogInspector`	이 구성 요소는 Windows 이벤트 로그 조사 결과를 기반으로 보호된 환경의 무결성을 모니터링합니다.
시스템 무결성 모니터링	`SystemIntegrityMonitor`	이 구성 요소에는 파일 무결성 모니터의 모든 기능이 포함되어 있으며 추가로 레지스트리 변경 사항 및 외부 장치의 연결을 모니터링할 수 있습니다.
Endpoint Detection and Response(Industrial CyberSecurity)	`EDR`	이 구성 요소는 Kaspersky Industrial CyberSecurity Endpoint Detection 솔루션과의 통합을 원활하게 합니다.
Endpoint Detection and Response Expert(on-premises)	`AntiAPT`	이 구성 요소는 Kaspersky Anti Targeted Attack Platform에 포함된 Endpoint Detection and Response 솔루션과의 통합을 원활하게 합니다.
BadUSB 공격 방지	`BadUSBAttackPrevention`	구성 요소는 키보드를 에뮬레이션하는 감염된 USB 장치가 컴퓨터에 연결하지 못하도록 차단합니다.
Managed Detection and Response	`MDR`	이 구성 요소는 Kaspersky Managed Detection and Response 솔루션과의 상호작용을 원활하게 합니다.
KICS for Networks와 통합	`KicsForNetworks`	이 구성 요소는 Kaspersky Industrial CyberSecurity for Networks 솔루션과의 통합을 원활하게 합니다.
Portable Auditor	`PortableScanner`	이 구성 요소를 사용하면 격리된 장치에서 바이러스 및 기타 악성 코드를 검사하고, 지정된 시간 동안 검사 대상 장치의 송수신 트래픽을 기록하고, 장치에 대한 보안 감사를 실행할 수 있습니다.
PLC 프로젝트 조사	`KicsPlcFeature`	이 구성 요소로 현재 산업 네트워크에서 사용되는 PLC 프로젝트 정보를 받을 수 있습니다.
PLC 프로젝트 무결성 검사	`KicsPlcFeature`	이 구성 요소로 산업 시스템에서 사용되는 PLC 프로젝트의 무결성을 검사할 수 있습니다
온디맨드 검사	`Ods`	이 구성 요소는 Kaspersky Industrial CyberSecurity for Nodes 시스템 파일과 온디맨드 검사 작업(요청에 따라 보호 중인 장치에서 개체를 검사함)을 설치합니다.
KSN 사용	`Ksn`	이 구성 요소는 Kaspersky 클라우드 기술 기반의 보호를 제공합니다. 이 구성 요소는 Kaspersky Security Network 서비스로의 요청 전송과 해당 서비스로부터의 결론 수신을 구현합니다.
Sigma 규칙을 사용한 이상 행위 탐지	`SigmaMonitoring`	이 구성 요소는 Sigma 규칙을 사용하여 내부 이벤트 데이터와 이벤트 로그에 이상이 있는지 분석합니다.
SIEM 통합	`SiemTelemetry`	이 구성 요소를 사용하면 SIEM 서버와의 통합을 구성할 수 있습니다.

설치 및 복구 설정, Windows Installer 명령줄 옵션

이 섹션에서는 Kaspersky Industrial CyberSecurity for Nodes 설치 및 복원 설정을 설명합니다. 이 섹션에는 설치 설정 변경을 위한 키와 가능한 키 값도 포함되어 있습니다. 이 키는 명령줄로 Kaspersky Industrial CyberSecurity for Nodes를 설치할 때 Windows Installer 서비스의 `msiexec` 명령을 위한 표준 키와 함께 사용할 수 있습니다.

설치 설정 및 Windows Installer 명령줄 옵션

- 최종 사용자 라이센스 계약서 조건 동의.

  `EULA=<value>`는 다음 값을 사용할 수 있습니다.

  - `0` – 최종 사용자 라이센스 계약서 조항 거부(기본값).
  - `1` – 최종 사용자 라이센스 계약 조항 수락.

- 개인정보취급방침 약관 수락.

  `PRIVACYPOLICY=<value>`는 다음 값을 사용할 수 있습니다.

  - `0` – 개인정보취급방침 조항 거부(기본 값).
  - `1` – 개인정보취급방침 조항 수락(기본값).

- 애플리케이션 모드 선택.

  `STANDALONEMODE=<value>`는 다음 값을 사용할 수 있습니다.

  - `0` – 전체 기능(기본 값).
  - `1`: Endpoint Agent.

- 설치 시 Kaspersky Industrial CyberSecurity for Nodes 파일이 저장될 대상 폴더입니다. 다른 폴더를 지정할 수 있습니다.

  `INSTALLDIR=<full path to the folder>` 명령줄 옵션의 기본값은 다음과 같습니다.

  - Microsoft Windows 32비트 버전:
    - Kaspersky Industrial CyberSecurity for Nodes: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0
    - Kaspersky Industrial CyberSecurity for Nodes 콘솔: %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Console 5.0.0
  - Microsoft Windows 64비트 버전: %ProgramFiles(x86)% 및 나머지는 Microsoft Windows 32비트 버전 경로와 비슷합니다.

- Kaspersky Industrial CyberSecurity for Nodes 시작 직후 *실시간 파일 보호* 작업 시작.

  `RUNRTP=<value>`는 다음 값을 사용할 수 있습니다.

  - `1` – 시작(기본값).
  - `0` – 시작하지 않음.

- *실시간 파일 보호* 작업 운영 모드.

  `RTP_BLOCKING=<value>`는 다음 값을 사용할 수 있습니다.

  - `1` – 권장(기본값).
  - `0` – 알림.

- 신뢰하는 프로세스 및 예외 규칙 목록에 산업용 소프트웨어의 프로세스 및 파일 추가 및 애플리케이션 시작 제어 규칙 구성. 다음 명령줄 옵션을 사용하여 프로세스 및 파일을 예외 규칙에 추가합니다: `ADDEXCLUSION=<exclusion profile name 1>;<exclusion profile name 2>;...;<exclusion profile name n>`. 지원되는 예외 프로필의 이름은 여기 나열됩니다.

- 키 파일의 경로(`LICENSEKEYPATH`). 기본적으로 Windows Installer는 배포 키트의 \exec 폴더에서 .key 확장자를 가진 파일을 찾으려 합니다. \exec 폴더에 파일이 여러 개라면 Windows Installer가 만료 날짜가 가장 많은 남은 키 파일을 선택합니다. 키 파일은 \exec 폴더나 `LICENSEKEYPATH` 파라미터에서 지정할 수 있는 다른 경로에 미리 저장할 수 있습니다.

  `LICENSEKEYPATH`는 다음 값을 사용할 수 있습니다.

  - 이름을 포함한 키 파일의 전체 경로입니다.
  - 키 파일이 저장된 폴더의 경로입니다.

  Kaspersky Industrial CyberSecurity for Nodes를 설치한 후 원하는 관리 도구를 사용하여(예: 애플리케이션 콘솔) 키를 추가할 수 있습니다. 애플리케이션 설치 중에 키를 추가하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 동작하지 않습니다.

- 구성 파일 경로. Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션에서 생성한 지정된 구성 파일에서 설정을 가져옵니다. Kaspersky Industrial CyberSecurity for Nodes는 구성 파일에서 작업 시작을 위한 계정 암호나 프록시 서버 연결을 위한 암호 등을 가져오지 않습니다. 일단 설정을 가져오면 직접 모든 암호를 입력해야 합니다. 구성 파일이 지정되지 않으면 애플리케이션은 설치 후 기본 설정으로 작업을 시작합니다.

  `CONFIGPATH=<configuration file name>`의 기본값은 지정되지 않습니다.

- *운영 체제 시작 시 검사* 모드(`SCANSTARTUP_BLOCKING`). Kaspersky Industrial CyberSecurity for Nodes를 `SCANSTARTUP_BLOCKING` 키 없이 설치했다면 *운영 체제 시작 시 검사*의 **검사 범위** 파라미터가 다음과 같이 설정됩니다.

  - 감염된 개체 및 기타 개체에 대해 수행할 동작: **알림**.
  - 감염 가능성이 있는 개체에 대해 수행할 동작: **알림**.

  Kaspersky Industrial CyberSecurity for Nodes를 `SCANSTARTUP_BLOCKING` 키로 설치했다면 *운영 체제 시작 시 검사*의 **검사 범위** 파라미터가 다음과 같이 설정됩니다.

  - 감염된 개체 및 기타 개체에 대해 수행할 동작: **권장 작업 수행**.
  - 감염 가능성이 있는 개체에 대해 수행할 동작: **권장 작업 수행**.

  운영 체제 시작 시 검사 작업이 자동 생성됩니다. **알림** 모드는 기본적으로 적용됩니다. 이 경우, 장치에 Kaspersky Industrial CyberSecurity for Nodes를 배포한 후에, 검사에서 시스템 서비스 문제가 발견되지 않으면 *운영 체제 시작 시 검사* 작업을 활성화할 수 있습니다. 애플리케이션이 중요 시스템 서비스를 감염되었거나 감염 의심 개체로 탐지하면 **알림** 모드가 원인을 파악하고 문제를 해결할 시간을 제공합니다. 애플리케이션이 **권장 작업 수행** 모드를 적용하면, **치료 - 불가능한 경우 삭제** 동작이 수행됩니다. 시스템 파일을 치료하거나 제거하면 운영 체제 시작에 심각한 문제가 발생할 수 있습니다.

- 운영 체제 서비스 보호 기능 구성입니다.

  본 기능을 활성화하면 타사 애플리케이션이 운영 체제의 프로세스를 작동할 수 없습니다.
  `PROTECTOSSERVICES=<value>`는 다음 값을 사용할 수 있습니다.

  - `1`은 운영 체제 서비스 보호가 활성화되었음을 의미합니다(기본 설정).
  - `0`은 운영 체제 서비스 보호가 비활성화되었음을 의미합니다.

- 애플리케이션 콘솔과 애플리케이션이 설치된 컴퓨터의 원격 연결에 사용되는 포트를 구성하는 방법은 다음과 같습니다.

  Windows 자격 증명으로 연결용 포트를 구성하려면 `UIPORT=<port number>` 파라미터를 사용하면 됩니다. 가능한 포트 번호 범위: 1~65535. 번호가 지정된 간격을 벗어나면 기본 포트 번호가 사용됩니다. 기본값은 13032입니다.

  필요하다면 `ENABLEUIKLPORT=<value>` 파라미터를 사용하여 수동 생성된 사용자의 자격 증명으로 연결용 포트를 닫을 수 있습니다.

  - `1` 포트를 엽니다(기본 설정).
  - `0` 포트를 닫습니다.

  이 포트의 기본값은 13031입니다. `UIKLPORT=<port>` 매개변수를 지정하여 포트 번호를 변경할 수 있습니다. 가능한 포트 번호 범위: 1~65535.

- 다른 컴퓨터에 설치된 애플리케이션 콘솔을 사용하여 Kaspersky Industrial CyberSecurity for Nodes의 원격 관리를 위한 네트워크 연결을 활성화하는 설정입니다.

  `ADDWFEXCLUSION=<value>`는 다음 값을 사용할 수 있습니다.

  - `1`: 이 값이 지정되면 애플리케이션이 설치된 컴퓨터에 대한 애플리케이션 콘솔 원격 연결을 위해 구성된 TCP 포트(`UIPORT=<port>` 및 `UIKLPORT=<port>` 파라미터)가 Windows 방화벽에서 열리고, Kaspersky Industrial CyberSecurity for Nodes 원격 관리 프로세스의 실행 파일, avp.exe에 대한 네트워크 연결이 허용됩니다.

    다른 장치에 애플리케이션 설치 시 추가 구성도 읽어 보십시오.

  - `0`: 이 값을 지정하면 아무 일도 발생하지 않습니다.

- 호환되지 않는 소프트웨어 확인 비활성화. 이 설정을 사용하면 보호 중인 장치에 애플리케이션을 백그라운드로 설치하는 동안 호환되지 않는 소프트웨어의 검사를 사용하거나 사용하지 않을 수 있습니다. 이 설정의 값과 상관없이 Kaspersky Industrial CyberSecurity for Nodes를 설치하는 동안 애플리케이션은 보호 중인 장치에 설치된 애플리케이션의 다른 버전에 대해 항상 경고합니다.

  `SKIPPRODUCTCHECK=<value>` 명령줄 옵션에 사용할 수 있는 값은 다음과 같습니다(`SKIPINCOMPATIBLESW=<value>`도 사용할 수 있습니다).

  - `0` - 호환되지 않는 소프트웨어에 대한 검사가 수행됩니다(기본값).
  - `1` - 호환되지 않는 소프트웨어에 대한 검사가 수행되지 않습니다.

- 호환되지 않는 소프트웨어 자동 제거 사용 안 함.

  `SKIPPRODUCTUNINSTALL=1` 옵션을 지정하면 Kaspersky Industrial CyberSecurity for Nodes는 호환되지 않는 소프트웨어를 제거하지 않습니다. 이 옵션을 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes는 호환되지 않는 소프트웨어 제거를 자동으로 시도합니다.

  > msiexec 설치 프로그램을 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 설치하면 호환되지 않는 소프트웨어 제거가 수행되지 않습니다. 호환성 문제를 유발할 수 있는 소프트웨어를 자동으로 제거하려면 setup_kics.exe 파일을 사용합니다.

- 애플리케이션 설치 또는 업데이트 중에 고유한 컴퓨터 식별자(Sensor ID)를 생성합니다.

Sensor ID는 Kaspersky Anti Targeted Attack Platform 솔루션에서 서버로 원격 측정 데이터를 전송하는 컴퓨터를 식별하는 데 사용됩니다. Sensor ID를 생성할 때, 애플리케이션은 마더보드 일련 번호와 같은 컴퓨터의 구성을 고려하는 알고리즘을 사용합니다. 예를 들어, 가상 환경에서 애플리케이션을 사용하는 경우와 같이, Sensor ID가 중복될 수 있습니다. 그러면 Kaspersky Anti Targeted Attack Platform이 원격 측정 데이터를 전송하는 컴퓨터를 식별할 수 없습니다. 고유한 Sensor ID를 생성하려면 `ENABLEUNIQUESENSORID=1` 매개변수를 설정해야 합니다. 결과적으로 애플리케이션은 컴퓨터에 관한 다른 데이터를 고려하는 다른 알고리즘을 사용하여 Sensor ID를 생성합니다. 이렇게 하면 Sensor ID의 고유성이 보장됩니다.

기본적으로 이 매개변수는 설정되어 있지 않습니다. 애플리케이션은 다음과 같은 경우에 Sensor ID를 상속합니다:

- 애플리케이션 버전 업데이트
- [KICS+KEA] 구성을 [KICS+내장 에이전트] 구성으로 마이그레이션

애플리케이션 복구의 일부로 설치 프로그램은 Sensor ID 상속을 시도합니다. Sensor ID를 복원할 수 없는 경우, 애플리케이션이 새로운 Sensor ID를 생성합니다.

- KB5007186 운영 체제 업데이트 확인을 비활성화합니다.

  KB5007186 업데이트를 설치한 후에도 애플리케이션이 계속해서 정상 작동하고 시스템 보안은 손상되지 않지만, 애플리케이션의 마이너 버전 업데이트가 불가능해집니다. 애플리케이션을 설치하기 전에 설치 프로그램이 설치된 운영 체제 업데이트를 확인합니다. KB5007186 업데이트가 발견되면, 설치 프로그램은 설치를 중단합니다. 명령줄에서 `SKIPKB5007186CHECK` 키를 입력하여 KB5007186 운영 체제 업데이트 확인을 활성화 또는 비활성화합니다.

  `SKIPKB5007186CHECK=<value>`는 다음 값을 사용할 수 있습니다.

  - `0`: 설치 프로그램이 KB5007186 운영 체제 업데이트가 설치되었는지 확인합니다.
  - `1`: 설치 프로그램은 KB5007186 운영 체제 업데이트가 설치되었는지 확인하지 않습니다.

  키가 설정되지 않는 `0`이 기본값입니다.

- 운영 체제의 신뢰할 수 있는 인증서 저장소에 DigiCert Assured ID Root CA 루트 인증서를 설치하는 과정을 건너뜁니다.

  애플리케이션을 설치할 때 `SKIPINSTALLROOTCACERTIFICATES` 옵션을 지정하면 DigiCert Assured ID Root CA 루트 인증서가 설치되지 않습니다. 기본적으로 인증서는 애플리케이션 설치 패키지에서 자동으로 설치됩니다.

- Rutoken 이동식 드라이브 접근 차단 사용자 지정. 차단을 활성화하면 애플리케이션이 설치된 장치에서 사용자는 휴대용 감사 도구를 생성하고 해당 장치에서 *애플리케이션 데이터베이스의 안전한 복사* 및 *애플리케이션 데이터베이스의 안전한 업데이트* 작업만 실행할 수 있으며, 운영 체제의 표준 수단을 사용한 보호된 이동식 드라이브 접근은 차단됩니다.

  `TOKENPROTECTION=<value>`는 다음 값을 사용할 수 있습니다.

  - `0` – 차단 비활성화됨(기본값)
  - `1` – 차단 활성화됨

복구 설정 및 Windows Installer 명령줄 옵션

- 격리된 개체 복원.

RESTOREQTN=<value>는 다음 값을 사용할 수 있습니다.

- 0 – 격리된 콘텐츠를 제거합니다(기본값).
- 1– 격리된 콘텐츠를 RESTOREPATH 파라미터에서 지정한 폴더의 \QB 하위 폴더에 복원합니다.

- 백업 콘텐츠 복원.

  RESTOREBCK=<value>는 다음 값을 사용할 수 있습니다.

  - 0 – 백업 내용을 제거합니다(기본값).
  - 1 – 백업 콘텐츠를 RESTOREPATH 파라미터에서 지정한 폴더의 \QB 하위 폴더에 복원합니다.

- 현재 암호를 입력하여 복원을 확인합니다(암호 보호 사용 시).

  UNLOCK_PASSWORD=<specified password>의 기본값은 지정되지 않습니다.

- 개체 복구용 폴더. 복원된 개체가 지정된 폴더에 저장됩니다.

  RESTOREPATH=<full path to the folder> 명령줄 옵션의 기본값은 %ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KICS.5.0.0\QB\Restored 입니다.

Kaspersky Industrial CyberSecurity for Nodes 설치 명령의 예

이 섹션에서는 Kaspersky Industrial CyberSecurity for Nodes를 설치할 때 사용되는 명령의 예제를 제공합니다.

보호 중인 장치에서 배포 키트에 있는 kics_win.msi 파일을 실행합니다.

Windows Installer의 표준 명령 및 명령줄 옵션 사용에 대한 자세한 내용은 Microsoft에서 제공한 설명서에 제공됩니다.

setup_kics.exe 파일에서 Kaspersky Industrial CyberSecurity for Nodes를 설치하는 예

사용자의 개입 없이 권장 설치 설정으로 Kaspersky Industrial CyberSecurity for Nodes를 설치하려면:

```
\exec\setup_kics.exe EULA=1 PRIVACYPOLICY=1
```

장치 제어와 같은 구성 요소를 설치하려면:

```
\exec\setup_kics.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0
```

설치 후 시스템 충돌의 원인이 되는 네트워크 장치 및 SCSI 장치가 있는 컴퓨터에 Kaspersky Industrial CyberSecurity for Nodes를 설치할 때 이 명령에 다음 추가 옵션을 사용할 수 있습니다.

```
/p SKIP_NETWORK_UPPERFILTERS=<1|0>
```

네트워크 어댑터 연결 가로채기를 활성화(1)하거나 비활성화(0)합니다.

```
/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>
```

SCSI 어댑터 연결 가로채기를 활성화(1)하거나 비활성화(0)합니다.

키 파일을 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 설치하고 활성화하려면:

```
setup_kics.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

Windows 사용자 자격 증명으로 애플리케이션 콘솔과 애플리케이션이 설치된 컴퓨터의 원격 연결에 사용되는 포트를 변경하려면:

```
setup_kics.exe /pUIPORT=<port number>
```

가능한 포트 번호 범위: 1~65535. 기본값은 13032입니다.

설치에 사용된 명령 목록: .msi 파일 실행

사용자의 개입 없이 권장 설치 설정으로 Kaspersky Industrial CyberSecurity for Nodes를 설치하려면:

```
msiexec /i kics_win.msi /qn EULA=1 PRIVACYPOLICY=1
```

권장 설치 설정으로 Kaspersky Industrial CyberSecurity for Nodes를 설치하고 설치 인터페이스를 표시하려면:

```
msiexec /i kics_win.msi /qf EULA=1 PRIVACYPOLICY=1
```

권장 설치 설정으로 Kaspersky Industrial CyberSecurity for Nodes를 설치하고 추적 파일 수가 지정된 최대 수에 도달할 때 추적 파일 순환을 활성화하려면:

```
msiexec /i kics_win.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1 PRIVACYPOLICY=1
```

TRACE_FOLDER 파라미터는 필수 항목입니다.

TRACE_MAX_ROLL_COUNT 파라미터에 다음 규칙이 적용됩니다:

- 이 파라미터를 지정하면 추적 파일 수가 파라미터에 지정된 최대 수에 도달하면 추적 파일 교체가 사용됩니다. 사용 가능한 파라미터값 범위: 1부터 999까지.
- 추적 파일의 최대 수를 0으로 지정하면 추적 파일 회전을 사용할 수 없습니다.
- 파라미터값을 지정했지만 잘못되었거나 사용 가능한 값 범위(1~999)를 벗어나면 추적 파일 회전이 활성화되고 최대 추적 파일 수의 기본값이 5로 설정됩니다.

- 파라미터를 지정하지 않은 경우:
  - 장치에 추적 파일 순환이 이미 구성된 경우 해당 설정은 변경되지 않습니다. 애플리케이션은 입력한 파라미터를 무시합니다.
  - 장치에 추적 파일 순환이 구성되어 있지 않으면 순환 옵션이 사용되며 최대 추적 파일 수의 기본값은 5로 설정됩니다.

키 파일 C:\0000000A.key를 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 설치하고 활성화하려면:

```
msiexec /i kics_win.msi     LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

활성 프로세스와 로컬 디스크의 부트 섹터를 사전 검사하여 Kaspersky Industrial CyberSecurity for Nodes를 설치하려면:

```
msiexec /i kics_win.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

C:\KICS 설치 폴더에 Kaspersky Industrial CyberSecurity for Nodes를 설치하려면:

```
msiexec /i kics_win.msi INSTALLDIR=C:\KICS /qn EULA=1 PRIVACYPOLICY=1
```

Kaspersky Industrial CyberSecurity for Nodes를 설치하고 Kaspersky Industrial CyberSecurity for Nodes msi 파일이 저장된 폴더에 kics.log 설치 로그 파일을 저장하려면:

```
msiexec /i kics_win.msi/l*v kics.log /qn EULA=1 PRIVACYPOLICY=1
```

Kaspersky Industrial CyberSecurity for Nodes 콘솔을 설치하려면:

```
msiexec /i kicstools.msi /qn EULA=1
```

키 파일 C:\0000000A.key를 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 설치 및 활성화하고, 구성 파일 C:\settings.xml의 설정에 따라 Kaspersky Industrial CyberSecurity for Nodes를 구성하려면:

```
msiexec /i kics_win.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

Kaspersky Industrial CyberSecurity for Nodes가 암호로 보호되어 있을 때 애플리케이션 패치를 설치하려면:

```
msiexec /p "<MSP file path>" UNLOCK_PASSWORD=<password>
```

Kaspersky Industrial CyberSecurity for Nodes 설치 후 수행할 동작

Kaspersky Industrial CyberSecurity for Nodes를 활성화했다면, 애플리케이션 설치 직후 보호 및 검사 작업이 시작됩니다. Kaspersky Industrial CyberSecurity for Nodes 설치 중 **애플리케이션 설치 후 실시간 파일 보호 활성화(권장 사항)** 확인란을 선택하면, 장치의 파일 시스템 개체에 접근할 때 애플리케이션이 이 개체를 검사합니다. 사용자 지정 설치 과정에서 스크립트 모니터링 구성 요소를 설치했다면, 스크립트를 시작할 때 Kaspersky Industrial CyberSecurity for Nodes가 모든 스크립트의 소스 코드를 검사합니다. Kaspersky Industrial CyberSecurity for Nodes는 매주 금요일 오후 8시에 *중요 영역 검사* 작업을 실행합니다.

Kaspersky Industrial CyberSecurity for Nodes 설치 후에는 다음 단계 수행을 권장합니다.

- Kaspersky Industrial CyberSecurity for Nodes 업데이트 작업을 시작합니다. 설치 후에는 Kaspersky Industrial CyberSecurity for Nodes가 배포 키트에 포함된 데이터베이스를 사용하여 개체를 검사합니다. Kaspersky Industrial CyberSecurity for Nodes 데이터베이스를 즉시 업데이트하는 것이 좋습니다. 이를 위해서는 *업데이트* 작업을 실행합니다. 그러면 업데이트가 기본 일정에 따라 매시간 실행됩니다.

  예를 들어 다음 명령을 실행하여 *업데이트* 작업을 시작할 수 있습니다.

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
  ```

  이 경우 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 업데이트가 Kaspersky 업데이트 서버에서 다운로드됩니다.

- Kaspersky Industrial CyberSecurity for Nodes 설치 전에 장치에 실시간 파일 보호 기능이 있는 안티 바이러스 소프트웨어가 설치되어 있지 않다면 *중요 영역 검사* 작업을 시작합니다.

  명령줄에서 다음 명령을 실행하여 *중요 영역 검사* 작업을 시작할 수 있습니다.

  ```
  KAVSHELL SCANCRITICAL /W:scancritical.log
  ```

  이 명령은 현재 폴더에 있는 scancritical.log 파일에 작업 로그를 저장합니다.

- Kaspersky Industrial CyberSecurity for Nodes 이벤트에 대한 관리자 알림을 구성합니다.

구성 요소 추가/제거. 샘플 명령

온디맨드 검사 구성 요소는 자동으로 설치됩니다. Kaspersky Industrial CyberSecurity for Nodes 구성 요소를 추가 또는 삭제하면 ADDLOCAL 키 값 목록에 수동 검사 구성 요소를 지정할 필요가 없습니다.

이미 설치된 구성 요소에 애플리케이션 실행 제어 구성 요소를 추가하려면 다음 명령을 실행합니다.

```
msiexec /i kics_win.msi ADDLOCAL=Oas,AppCtrl /qn
```

또는

```
\exec\setup_kics.exe /s /p ADDLOCAL=Oas,AppCtrl
```

이미 설치한 구성 요소와 함께 설치하려는 구성 요소를 열거하면, Kaspersky Industrial CyberSecurity for Nodes가 기존 구성 요소를 다시 설치합니다.

설치된 구성 요소를 제거하려면 다음 명령을 실행합니다.

```
msiexec /i kics_win.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,Bases,Core,CoreBLFiles,CoreFolders,CoreWPFiles,DevCtrl,Driver
ADD_ADV=IDS,RegMonitor REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

Kaspersky Industrial CyberSecurity for Nodes 제거. 샘플 명령

보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes를 제거하려면 다음 명령을 실행합니다.

```
msiexec /x kics_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

또는

```
msiexec /x {DF1C0C50-2E34-4B22-A07D-133E3DC961C7} KLLOGIN=<user name> KLPASSWD=<password> /qn
```

또는

```
setup_kics.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

여기서 `<user name>`은 제거를 위한 충분한 권한을 보유한 사용자의 이름과 로그인 계정입니다.

제거를 수행하는 사용자 계정에 Windows 암호가 공란으로 설정되어 있는 경우, 제거를 시작하기 전 **중요 작업을 확인하기 위한 암호 요청** 기능을 비활성화합니다.

숨김 모드에서 Kaspersky Industrial CyberSecurity for Nodes 콘솔을 제거하려면 다음 명령을 실행합니다.

```
msiexec /x kicstools.msi /qn
```

또는

```
msiexec /x {5209F134-35AD-4A12-85B9-257FA5B52917} /qn
```

반환 코드

애플리케이션 설치 프로그램이 이 글에 설명된 반환 코드를 반환할 수 있습니다.

아래의 표에는 명령줄 반환 코드 목록이 나와 있습니다.

반환 코드

코드	설명
27100	컴퓨터에서 테스트 모드로 인증 에이전트가 설치된 드라이브가 탐지됩니다.
27101	컴퓨터에서 테스트 모드로 인증 에이전트가 설치된 드라이브가 탐지됩니다.
27102	암호화된 디스크를 찾지 못했습니다.
27200	RAM에서 애플리케이션을 언로드하지 못했습니다.
27201	AVP.exe 프로세스 시작 중 오류가 발생했습니다. 컴퓨터가 감염되었을 수 있습니다.
27204	배포 패키지 캐싱에 실패했습니다.
27205	라이센스 정보 마이그레이션에 실패했습니다.
27206	라이센스 정보 제거에 실패했습니다.
27207	호환되지 않는 소프트웨어 제거에 실패했습니다.
27208	호환되지 않는 소프트웨어 확인에 실패했습니다.
27209	캐비닛에서 파일 추출에 실패했습니다.
27210	자기 보호 구성에 실패했습니다.
27211	자기 보호 활성화에 실패했습니다.
27212	운영 체제 버전 정보를 가져오는 데 실패했습니다.
27213	시작 디렉터리를 가져오는 데 실패했습니다.
27214	설치 디렉터리를 확인하는 데 실패했습니다.
27215	서비스 구성에 실패했습니다.
27216	klcp 업그레이드 구성에 실패했습니다.
27217	klcp 업그레이드에 실패했습니다.
27218	kl1 드라이버 파라미터 구성에 실패했습니다.
27219	klelam 드라이버 파라미터 구성에 실패했습니다.
27220	klwfp 드라이버 파라미터 구성에 실패했습니다.
27221	드라이버 호환성 모드 구성에 실패했습니다.
27222	레지스트리 키 제거에 실패했습니다.
27223	운영 체제 다시 시작에 실패했습니다.
27224	드라이버 설치에 실패했습니다.
27225	드라이버 설정 마이그레이션에 실패했습니다.
27226	드라이버 중지에 실패했습니다.
27227	드라이버 시작 차단에 실패했습니다.
27228	파일의 서명 확인에 실패했습니다.
27230	kldl 드라이버 설정 준비에 실패했습니다.
27231	kldl 드라이버 설정 구성에 실패했습니다.
27300	드라이버 설치 오류.
27301	드라이버 제거 오류.
27302	네트워크 구성 요소 설치 오류.
27303	드라이버의 등록 정보가 일치하지 않거나 완전하지 않습니다. 운영 체제를 다시 시작한 후 다시 시도하십시오.
27305	드라이버 비활성화 오류.
27310	디지털 서명된 카탈로그 파일 설치에 실패했습니다.
27311	디지털 서명된 카탈로그 파일 제거에 실패했습니다.
27312	인증서 설치에 실패했습니다.

코드	설명
27313	인증서 제거에 실패했습니다.
27320	서비스 구성에 실패했습니다.
27321	서비스 보호 해제에 실패했습니다.
27350	<patch name> 패치는 <application name> 애플리케이션 현지화를 위한 것이 아닙니다.
27352	전체 디스크 암호화 패치는 제거할 수 없습니다.
27353	<patch 1 name> 패치는 <patch 2 name> 패치와 함께 설치할 수만 있습니다.
27354	애플리케이션을 수정/복원하기 전에 패치를 적용하려면 컴퓨터를 다시 시작해야 합니다.
27355	전체 디스크 암호화 관리 잠금에 실패했습니다. 전체 디스크 암호화 관리 잠금에 실패했습니다. 전체 디스크 암호화용 업데이트를 설치하려면 암호화를 완료해야 합니다.
27356	패치를 설치할 수 없습니다.
27357	설치 패키지에 리콜된 패치가 포함된 것으로 확인되었습니다. 설치가 중단됩니다.
27360	패치를 등록할 수 없습니다.
27361	패치 설치 매개변수 설정에 실패했습니다.
27363	패치에 설치된 암호화 라이브러리와 호환되지 않는 암호화 라이브러리가 포함되어 있습니다.
27370	.NET 8.0 압축 해제 초기화 중 오류.
27371	.NET 8.0을 압축 해제 중 오류.
27372	이전 애플리케이션 버전에 대한 등록 정보가 삭제되었습니다. 설치를 다시 시작하십시오.
27373	이전 애플리케이션 버전에 대한 등록 정보 삭제에 실패했습니다.
27374	애플리케이션을 업그레이드하는 중입니다. 잠시 후 다시 시도하십시오.
27375	제거 암호 또는 사용자 이름이 지정되지 않았거나 잘못되었습니다.
27376	Kaspersky Endpoint Agent 제거에 실패했습니다. 직접 제거하거나 설정에서 암호 보호를 비활성화하십시오. 그런 다음 애플리케이션 설치를 다시 시작합니다.
27377	Kaspersky Security for Windows Server 제거에 실패했습니다. 직접 제거하거나 설정에서 암호 보호를 비활성화하십시오. 그런 다음 애플리케이션 설치를 다시 시작합니다.
27378	디스크 여유 공간 부족.
27379	호환되지 않는 구성 요소가 선택되어 애플리케이션 설치에 실패했습니다. 구성 요소 집합을 변경하고 설치를 다시 시작하십시오.
27380	유효하지 않은 구성 파일이 선택되었습니다.
27381	유효하지 않은 라이센스 키가 선택되었습니다.
27382	애플리케이션 관리 그룹 생성 실패.
27383	잘못된 폴더를 선택했습니다. 대상 폴더의 이름은 최대 160자입니다.
27384	잘못된 폴더나 드라이브를 선택했습니다. 애플리케이션은 로컬 하드 드라이브에 설치해야 합니다.
27385	잘못된 폴더를 선택했습니다. 루트 폴더에는 애플리케이션을 설치할 수 없습니다.
27386	잘못된 폴더를 선택했습니다. Windows 폴더나 그 하위 폴더에는 애플리케이션을 설치할 수 없습니다.
27387	잘못된 폴더를 선택했습니다. 임시 하위 폴더가 포함된 폴더에는 애플리케이션을 설치할 수 없습니다.
27388	잘못된 폴더를 선택했습니다. 애플리케이션을 프로그램 파일 폴더에 직접 설치할 수는 없습니다.
27389	잘못된 폴더를 선택했습니다. 가상 디스크에는 애플리케이션을 설치할 수 없습니다.
27390	잘못된 폴더나 드라이브를 선택했습니다. 애플리케이션의 이전 버전이 설치된 폴더에는 애플리케이션을 설치할 수 없습니다.
27391	선택한 폴더 또는 드라이브에는 이미 파일이 포함되어 있습니다. 다른 데이터가 포함된 폴더에는 애플리케이션을 설치할 수 없습니다. 자기 보호를 활성화하면 이 데이터를 사용하지 못하게 될 수 있습니다.
27392	리파싱 지점이 포함된 폴더에는 애플리케이션을 설치할 수 없습니다. 다른 설치 폴더를 선택하십시오.
27393	이름에 세미콜론(;)이 포함된 폴더에는 애플리케이션을 설치할 수 없습니다. 다른 설치 폴더를 선택하십시오.
27394	잘못된 폴더를 선택했습니다. 루트 폴더는 지정할 수 없습니다.
27395	잘못된 폴더를 선택했습니다. Windows 폴더나 그 하위 폴더는 지정할 수 없습니다.

코드	설명
27396	잘못된 폴더를 선택했습니다. 프로그램 파일 폴더는 직접 지정할 수 없습니다.
27397	잘못된 폴더를 선택했습니다. 임시 하위 폴더가 포함된 폴더는 지정할 수 없습니다.
27400	파일 업데이트 초기화 오류가 발생했습니다.
27450	CAB 파일을 설치할 수 없습니다.
27451	제거 중 오류.
27452	파일 제거 중 오류.
27453	파일 이동 중 오류.
27454	레지스트리 파일 생성에 실패했습니다.
27455	운영 체제 버전 정보를 가져오는 데 실패했습니다.
27456	레지스트리 값 롤백 스케줄에 실패했습니다.
27457	잘 알려진 보안 식별자(SID) 가져오기에 실패했습니다.
27460	보안 설명자 생성 중 오류.
27461	보안 설명자 복원 중 오류.
27462	Microsoft Windows 방화벽 규칙 생성에 실패했습니다.
27463	Microsoft Windows 방화벽 규칙 삭제에 실패했습니다.

Kaspersky Security Center를 사용하여 애플리케이션 설치 및 설치 제거

이 섹션에는 Kaspersky Security Center를 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 설치하는 방법에 관한 정보, Kaspersky Security Center를 통해 Kaspersky Industrial CyberSecurity for Nodes를 설치 및 제거하는 절차에 관한 설명, Kaspersky Industrial CyberSecurity for Nodes 실행 후 취해야 하는 조치에 관한 설명이 포함되어 있습니다.

Kaspersky Security Center를 통한 설치 일반 정보

원격 설치 작업을 사용하여 Kaspersky Security Center를 통해 Kaspersky Industrial CyberSecurity for Nodes를 설치할 수 있습니다.

원격 설치 작업이 완료되면, Kaspersky Industrial CyberSecurity for Nodes가 보호 중인 장치 여러 대에 같은 설정으로 설치됩니다.

모든 보호 중인 장치는 단일 관리 그룹으로 통합할 수 있으며, 이 그룹의 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치하는 그룹 작업을 생성할 수 있습니다.

관리 그룹이 다른 보호 중인 장치 세트에 Kaspersky Industrial CyberSecurity for Nodes 원격 설치 작업을 생성할 수 있습니다. 이 작업을 생성할 때는 Kaspersky Industrial CyberSecurity for Nodes를 설치할 각 보호 중인 장치의 목록을 생성해야 합니다.

원격 설치 작업에 대한 자세한 내용은 Kaspersky Security Center 도움말에 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 설치 또는 제거할 권한

원격 설치(제거) 작업에서 지정된 계정은 아래 설명한 경우를 제외한 모든 경우에 각 보호 중인 장치의 관리자 그룹에 포함되어야 합니다.

- Kaspersky Industrial CyberSecurity for Nodes를 설치할 보호 중인 장치에 Kaspersky Security Center 네트워크 에이전트가 이미 설치된 경우(보호 중인 장치가 있는 도메인 또는 도메인 소속 여부와 관계없이).

  보호 중인 장치에 아직 네트워크 에이전트를 설치하지 않았으면 원격 설치 작업으로 Kaspersky Industrial CyberSecurity for Nodes와 함께 설치할 수 있습니다. 네트워크 에이전트를 설치하기 전에 작업에서 지정하려는 계정이 각 보호 중인 장치의 관리자 그룹에 포함되어 있는지 확인하십시오.

- Kaspersky Industrial CyberSecurity for Nodes를 설치하려는 모든 보호 중인 장치가 중앙 관리 서버와 같은 도메인에 속해 있고 중앙 관리 서버가 **도메인 관리자** 계정으로 등록된 경우(이 계정이 도메인 내에서 보호 중인 장치에 대한 로컬 관리자 권한을 가지고 있다면).

기본적으로, **강제 설치** 방법 사용 시 중앙 관리 서버가 실행되는 계정에서 원격 설치 작업이 실행됩니다.

강제 설치(제거) 모드에서 그룹 작업이나 보호 중인 장치 세트에 대한 작업 수행 시, 계정에 보호 중인 장치에 대한 다음 권한이 있어야 합니다.

- 애플리케이션을 원격 실행할 수 있는 권한.
- **Admin$** 공유에 관한 권한.
- **서비스로 로그온**할 수 있는 권한.

Kaspersky Security Center를 통해 Kaspersky Industrial CyberSecurity for Nodes 설치

Kaspersky Security Center를 통한 Kaspersky Industrial CyberSecurity for Nodes 설치에는 다음 단계가 포함됩니다.

1. **설치 패키지 만들기**

   *설치 패키지*는 Kaspersky Security Center를 통한 Kaspersky 애플리케이션 원격 설치용으로 생성된 파일 집합입니다. 설치 패키지에는 애플리케이션을 설치하고 설치 후 즉시 이를 실행하는데 필요한 설정 범위가 있습니다. 설치 패키지는 애플리케이션 배포 키트에 포함된 확장자가 .kpd 및 .kud인 파일을 사용해 생성됩니다.

   Kaspersky Security Center Administration Console에서 설치 패키지를 만드는 방법

   1. Kaspersky Security Center 관리 콘솔 트리에서 **고급** → **원격 설치** → **설치 패키지** 폴더를 선택합니다.
   2. 결과 창에서 **설치 패키지 생성** 버튼을 클릭합니다.

      새 패키지 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 설치 패키지 유형 선택

Kaspersky 애플리케이션에 대한 설치 패키지 생성 옵션을 선택합니다.

2단계. 설치 패키지 이름 정의

설치 패키지의 이름을 입력합니다(*Kaspersky Industrial CyberSecurity for Nodes* 등).

3단계. 설치할 배포 패키지 선택

Kaspersky Industrial CyberSecurity for Nodes 배포 키트의 kics_win.kud 파일을 설치 패키지 파일로 지정합니다.

필요하다면 **저장소에서 설치 패키지로 업데이트 파일 복사** 확인란을 선택하여 설치 패키지에서 안티 바이러스 데이터베이스를 업데이트합니다.

4단계. 최종 사용자 라이센스 계약서 및 개인정보취급방침

최종 사용자 라이센스 계약서와 개인정보취급방침의 약관에 동의하면 **이 최종 사용자 라이센스 계약서의 이용 약관을 모두 읽고 이해했으며 수락함을 확인합니다** 및 **개인정보취급방침에 설명된 대로 제 데이터가 처리되고 전송(제3국으로의 전송 포함)되는 것을 알고 있으며 이에 동의합니다. 개인정보취급방침을 모두 읽고 이해했음을 확인합니다** 확인란을 선택합니다.

계속하려면 라이센스 계약서 및 개인정보취급방침에 동의해야 합니다.

설치 패키지가 생성되어 Kaspersky Security Center에 추가됩니다. 설치 패키지를 사용하여 기업 네트워크 컴퓨터에 Kaspersky Industrial CyberSecurity for Nodes를 설치하거나 애플리케이션 버전을 업데이트할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes의 설치할 구성 요소 세트와 만든 설치 패키지의 기본 설치 설정 을 변경하려면:

1. Kaspersky Security Center 관리 콘솔에서 **원격 설치** 노드를 확장합니다.
2. **설치 패키지** 하위 노드의 결과 창에서 생성된 Kaspersky Industrial CyberSecurity for Nodes 설치 패키지의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
3. **속성:<설치 패키지 이름>** 창에서 **설정** 섹션을 엽니다.
4. 애플리케이션 설치 유형 선택:

   안티바이러스 베이스로 컴퓨터 보호 구성을 선택하면 방화벽 및 성능 카운터 구성 요소를 제외한 모든 Kaspersky Industrial CyberSecurity for Nodes 구성 요소가 기본적으로 포함됩니다.

컴퓨터 보호에 시그니처 분석 및 안티 바이러스 데이터베이스를 사용하지 않는 애플리케이션 버전에 **안티바이러스 베이스로 컴퓨터 보호** 구성의 애플리케이션을 덮어 설치하면 다음 구성 요소가 추가되어 애플리케이션 구성 요소 집합이 자동으로 확장됩니다.

- 실시간 파일 보호
- 온디맨드 검사
- 네트워크 위협 보호

업데이트 기능을 제공하는 구성 요소는 **기본 거부 기술을 통해 컴퓨터를 보호** 구성에 포함되지 않습니다.

기본 거부 기술을 통해 컴퓨터를 보호 구성을 선택하면 다음 구성 요소가 기본적으로 포함됩니다.

- 익스플로잇 방지
- 애플리케이션 실행 제어
- 시스템 트레이 아이콘

컴퓨터 보호에 시그니처 분석 및 안티 바이러스 데이터베이스를 사용하는 애플리케이션 버전에 **기본 거부 기술을 통해 컴퓨터를 보호** 구성의 애플리케이션을 덮어 설치하면 다음 구성 요소가 제거되어 애플리케이션 구성 요소 집합이 자동으로 축소됩니다.

- 실시간 파일 보호
- 온디맨드 검사
- 업데이트 기능을 제공하는 구성 요소

이 구성은 리소스가 제한된 장치를 보호하는 데 권장됩니다. 이 경우 애플리케이션을 장기간 활성화할 수 있으며 애플리케이션 실행 제어 구성 요소가 컴퓨터 보호 기능을 제공합니다.

- **전체 기능**

  기본적으로 성능 계수기 및 Endpoint Agent를 제외한 모든 Kaspersky Industrial CyberSecurity for Nodes 구성 요소를 설치할 것을 권장합니다.

  Kaspersky Industrial CyberSecurity for Nodes의 SNMP 프로토콜 지원 구성 요소는 보호 중인 장치에 Microsoft Windows SNMP 서비스가 설치되었을 때만 설치 제안 구성 요소 목록에만 표시됩니다.

- **Endpoint Agent**

  이 옵션을 선택하면 Endpoint Agent 구성에 Kaspersky Industrial CyberSecurity for Nodes가 설치됩니다. 이 구성에 대한 자세한 내용은 이 섹션을 참조하십시오.

5. **구성** 버튼을 클릭하여 산업 시스템의 예외 목록을 지정합니다.
6. **구성 요소 선택** 블록에서 설치할 Kaspersky Industrial CyberSecurity for Nodes 구성 요소 이름 옆의 확인란을 선택합니다.
7. **실시간 파일 보호 모드** 블록에서 **애플리케이션 설치 후 실시간 파일 보호 활성화(권장 사항)** 확인란을 선택하고 구성 요소 운영 모드를 선택합니다.

8. 필요하다면 애플리케이션 콘솔에서 애플리케이션이 설치된 컴퓨터에 원격으로 연결하는 데 사용되는 TCP 포트 번호를 변경합니다.

   Windows 자격 증명을 사용하여 연결하기 위한 기본 포트 번호는 13032이며, 수동 생성 사용자의 자격 증명을 사용하여 연결하기 위한 기본 포트 번호는 13031입니다. 가능한 포트 번호 범위: 1~65535.

   수동으로 생성한 사용자 계정의 자격 증명으로 연결하는 것을 방지하기 위해 **수동으로 생성된 사용자의 자격 증명을 사용** 확인란을 선택 해제합니다.

9. 기본 설치 폴더가 아닌 다른 폴더를 설치하려면 **애플리케이션 설치 경로 구성** 블록에서 **설정** 버튼을 클릭하여 폴더 이름과 경로를 지정합니다.

10. 사전 정의된 설정으로 애플리케이션을 설치하려면 구성 파일을 업로드합니다.

11. 변경 사항을 저장합니다.

웹 콘솔에서 설치 패키지를 만드는 방법

1. 다음 중 하나를 수행합니다:

   - 웹 콘솔의 메인 창에서 **발견 및 배포 → 배포 및 할당 → 설치 패키지** 옵션을 선택합니다.
   - 웹 콘솔의 메인 창에서 **동작 → 저장소 → 설치 패키지** 옵션을 선택합니다.

   Kaspersky Security Center로 다운로드한 설치 패키지 목록이 열립니다.

2. **추가** 버튼을 클릭합니다.

새 패키지 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 설치 패키지 유형 선택

Kaspersky 애플리케이션에 대한 설치 패키지 생성 옵션을 선택합니다.

마법사가 Kaspersky 서버에 있는 배포 패키지에서 설치 패키지를 생성합니다. 새 버전의 애플리케이션이 릴리즈되면 이 목록은 자동으로 업데이트됩니다.

파일로 설치 패키지를 생성할 수도 있습니다.

2단계. 설치 패키지

Kaspersky Industrial CyberSecurity for Nodes 설치 패키지 선택. 설치 패키지 생성 프로세스가 시작됩니다. 설치 패키지를 생성하는 동안 최종 사용자 라이센스 계약서 및 개인정보 취급방침을 반드시 수락해야 합니다.

> 계속하려면 라이센스 계약서 및 개인정보취급방침에 동의해야 합니다.

설치 패키지가 생성되어 Kaspersky Security Center에 추가됩니다. 설치 패키지를 사용하여 기업 네트워크 컴퓨터에 Kaspersky Industrial CyberSecurity for Nodes를 설치하거나 애플리케이션 버전을 업데이트할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes의 설치할 구성 요소 세트와 만든 설치 패키지의 기본 설치 설정 을 변경하려면:

1. **설치 패키지** 창으로 이동하여 앞서 생성한 Kaspersky Industrial CyberSecurity for Nodes 설치 패키지의 이름을 클릭합니다.

2. 창이 열리면 **설정** 탭을 선택합니다.

3. **보호 구성 요소** 섹션을 선택합니다.

4. 애플리케이션 설치 유형 선택:

   안티바이러스 베이스로 컴퓨터 보호 구성을 선택하면 방화벽 및 성능 카운터 구성 요소를 제외한 모든 Kaspersky Industrial CyberSecurity for Nodes 구성 요소가 기본적으로 포함됩니다.

   컴퓨터 보호에 시그니처 분석 및 안티 바이러스 데이터베이스를 사용하지 않는 애플리케이션 버전에 **안티바이러스 베이스로 컴퓨터 보호** 구성의 애플리케이션을 덮어 설치하면 다음 구성 요소가 추가되어 애플리케이션 구성 요소 집합이 자동으로 확장됩니다.

   - 실시간 파일 보호
   - 온디맨드 검사
   - 네트워크 위협 보호

   > 업데이트 기능을 제공하는 구성 요소는 **기본 거부 기술을 통해 컴퓨터를 보호** 구성에 포함되지 않습니다.

   기본 거부 기술을 통해 컴퓨터를 보호 구성을 선택하면 다음 구성 요소가 기본적으로 포함됩니다.

   - 익스플로잇 방지
   - 애플리케이션 실행 제어
   - 시스템 트레이 아이콘

   컴퓨터 보호에 시그니처 분석 및 안티 바이러스 데이터베이스를 사용하는 애플리케이션 버전에 **기본 거부 기술을 통해 컴퓨터를 보호** 구성의 애플리케이션을 덮어 설치하면 다음 구성 요소가 제거되어 애플리케이션 구성 요소 집합이 자동으로 축소됩니다.

   - 실시간 파일 보호
   - 온디맨드 검사
   - 업데이트 기능을 제공하는 구성 요소

   이 구성은 리소스가 제한된 장치를 보호하는 데 권장됩니다. 이 경우 애플리케이션을 장기간 활성화할 수 있으며 애플리케이션 실행 제어 구성 요소가 컴퓨터 보호 기능을 제공합니다.

   - **전체 기능**

     기본적으로 성능 계수기 및 Endpoint Agent를 제외한 모든 Kaspersky Industrial CyberSecurity for Nodes 구성 요소를 설치할 것을 권장합니다.

     Kaspersky Industrial CyberSecurity for Nodes의 SNMP 프로토콜 지원 구성 요소는 보호 중인 장치에 Microsoft Windows SNMP 서비스가 설치되었을 때만 설치 제안 구성 요소 목록에만 표시됩니다.

- **Endpoint Agent**

  이 옵션을 선택하면 Endpoint Agent 구성에 Kaspersky Industrial CyberSecurity for Nodes가 설치됩니다. 이 구성에 대한 자세한 내용은 이 섹션을 참조하십시오.

5. **구성** 버튼을 클릭하여 산업 시스템의 예외 목록을 지정합니다.

6. **설치할 구성 요소 선택** 섹션에서 설치할 Kaspersky Industrial CyberSecurity for Nodes 구성 요소 이름 옆의 확인란을 선택합니다.

7. **실시간 파일 보호 모드** 블록에서 **애플리케이션 설치 후 실시간 파일 보호 활성화(권장 사항)** 확인란을 선택하고 구성 요소 운영 모드를 선택합니다.

8. 필요하다면 애플리케이션 콘솔에서 애플리케이션이 설치된 컴퓨터에 원격으로 연결하는 데 사용되는 TCP 포트 번호를 변경합니다.

   Windows 자격 증명을 사용하여 연결하기 위한 기본 포트 번호는 13032이며, 수동 생성 사용자의 자격 증명을 사용하여 연결하기 위한 기본 포트 번호는 13031입니다. 가능한 포트 번호 범위: 1~65535.

   수동으로 생성한 사용자 계정의 자격 증명으로 연결하는 것을 방지하기 위해 **수동으로 생성된 사용자의 자격 증명을 사용한 원격 연결용 포트** 확인란을 선택 해제합니다.

9. **설치 설정** 섹션을 선택합니다.

10. **고급 설정** 섹션에서 다음 설정을 구성할 수 있습니다.

    - **환경 변수 %PATH%에 애플리케이션 위치 추가**. 애플리케이션을 명령줄에서 편리하게 관리할 수 있도록 %PATH% 변수에 설치 경로를 추가할 수 있습니다.

    - **OS 시작 시 검사 중 권장 작업 실행**. 이 확인란을 선택하면 *운영 체제 시작 시 검사* 작업이 **권장 작업 수행** 모드로 실행됩니다.

    - **Kaspersky Security Center 네트워크 에이전트에 대한 저자원 소모 모드 사용**. 절전 모드를 사용하면 보호 중인 장치에서 네트워크 에이전트가 사용하는 RAM의 양을 제한할 수 있습니다. 기본적으로 절전 모드는 비활성화되어 있습니다.

    - **작업 표시줄에 시스템 상자 아이콘 표시**. 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 설치된 후 애플리케이션 아이콘이 Microsoft Windows 작업 표시줄 알림 영역에 나타납니다.

11. 필요하다면 **설치 프로세스 보호** 기능을 비활성화하십시오.

12. 필요하다면 애플리케이션 설치 중에 보호 중인 장치에 생성되는 기본 폴더를 변경합니다.

13. 사전 정의된 설정으로 애플리케이션을 설치하려면 **구성 파일 추가** 링크를 클릭하고 구성 파일을 업로드합니다.

    Kaspersky Security Center 웹 콘솔에서 애플리케이션 제어 규칙을 사용하는 경우 업로드된 파일의 최대 지원 크기는 4MB입니다. Kaspersky Security Center 관리 콘솔에서 설치 패키지로 작업하는 경우 이 제한이 적용되지 않습니다.

14. 변경 사항을 저장합니다.

2 원격 설치 작업 만들기

원격으로 애플리케이션 설치 작업을 통해 Kaspersky Industrial CyberSecurity for Nodes를 원격으로 설치할 수 있습니다. *원격으로 애플리케이션 설치* 작업을 통해 애플리케이션의 설치 패키지를 조직의 모든 컴퓨터에 배포할 수 있습니다.

Kaspersky Security Center Administration Console에서 원격 설치 작업을 생성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업** 옵션을 선택합니다.
   작업 목록이 열립니다.
3. **새 작업** 버튼을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Security Center 중앙 관리 서버 → 원격으로 애플리케이션 설치를 선택합니다.

2단계. 설치 패키지 선택

목록에서 Kaspersky Industrial CyberSecurity for Nodes 설치 패키지를 선택합니다. 목록에 Kaspersky Industrial CyberSecurity for Nodes용 설치 패키지가 포함되어 있지 않으면 마법사에서 패키지를 생성할 수 있습니다.

Kaspersky Security Center에서 설치 패키지 설정을 구성할 수 있습니다. 예를 들어 컴퓨터에 설치할 애플리케이션 구성 요소를 선택할 수 있습니다.

네트워크 에이전트가 Kaspersky Industrial CyberSecurity for Nodes와 함께 설치됩니다. *네트워크 에이전트*를 설치하면 중앙 관리 서버와 클라이언트 컴퓨터가 원활하게 상호 작용할 수 있습니다. 네트워크 에이전트가 컴퓨터에 이미 설치되어 있으면 다시 설치되지 않습니다.

3단계. 추가 작업

네트워크 에이전트 설치 패키지를 선택합니다. 선택한 네트워크 에이전트 버전이 Kaspersky Industrial CyberSecurity for Nodes와 함께 설치됩니다.

4단계. 설정

다음과 같은 추가 애플리케이션 설정을 구성하십시오.

- **강제 설치 패키지 다운로드**. 애플리케이션 설치 방법 선택:

  - **네트워크 에이전트 이용**. 네트워크 에이전트는 Kaspersky Industrial CyberSecurity for Nodes 설치 패키지를 클라이언트 컴퓨터로 전달하는 작업을 담당합니다. 네트워크 에이전트가 설치되어 있지 않으면 작업이 종료되고 오류가 발생합니다. 이 경우 네트워크 에이전트 설치 패키지를 *원격으로 애플리케이션 설치* 작업에 추가하고 운영 체제 리소스를 통한 파일 전달을 활성화합니다. 그런 다음 운영 체제 리소스를 사용하여 네트워크 에이전트가 설치됩니다. Kaspersky Industrial CyberSecurity for Nodes는 그 다음에 네트워크 에이전트를 사용하여 설치됩니다.

  - **배포 지점에서 대상 운영 체제의 관리 공유 폴더로 다운로드**. 설치 패키지가 배포 지점을 통해 운영 체제 리소스를 사용하여 클라이언트 컴퓨터로 배달됩니다. 네트워크에 배포 지점이 하나 이상 있으면 이 옵션을 선택할 수 있습니다. 배포 지점에 대한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.

  - **중앙 관리 서버에서 대상 운영 체제의 관리 공유 폴더로 다운로드**. 중앙 관리 서버를 통해 운영 체제 리소스를 사용하여 클라이언트 컴퓨터로 파일이 배달됩니다. 이 옵션은 클라이언트 컴퓨터에 네트워크 에이전트가 설치되어 있지 않아도 선택할 수 있지만, 이 경우 클라이언트 컴퓨터는 중앙 관리 서버와 같은 네트워크에 있어야 합니다.

- **다른 중앙 관리 서버를 통해 관리되는 기기를 위한 동작**. Kaspersky Industrial CyberSecurity for Nodes 설치 방법 선택. 네트워크에 중앙 관리 서버가 두 대 이상 설치되어 있으면 해당 서버가 같은 클라이언트 컴퓨터를 확인할 수 있습니다. 이 경우 서로 다른 중앙 관리 서버를 통해 같은 클라이언트 컴퓨터에 애플리케이션이 여러 번 원격으로 설치되는 등의 문제나 기타 충돌이 발생할 수 있습니다.

- **이미 설치한 애플리케이션은 설치하지 않음**. 이전 버전의 애플리케이션을 설치하려는 등의 경우 이 확인란의 선택을 취소합니다.

5단계. 운영 체제 재시작 설정 선택

컴퓨터를 다시 시작해야 하는 경우 수행할 처리 방법을 선택합니다. Kaspersky Industrial CyberSecurity for Nodes를 설치할 때 다시 시작할 필요가 없습니다. 설치 전에 호환되지 않는 애플리케이션을 제거해야 하는 경우에만 재시작이 필요합니다. 애플리케이션 버전을 업데이트할 때도 컴퓨터를 다시 시작해야 할 수 있습니다.

6단계. 작업을 할당할 장치 선택

Kaspersky Industrial CyberSecurity for Nodes를 설치할 컴퓨터를 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.

- 관리 그룹에 작업 할당. 이 경우 이전에 만든 관리 그룹에 포함된 컴퓨터에 작업이 할당됩니다.
- 네트워크에서 중앙 관리 서버가 탐지한 컴퓨터 선택: *미할당 장치*. 미할당 장치에는 네트워크 에이전트가 설치되지 않습니다. 이 경우 특정 장치에 작업이 할당됩니다. 이 특정 장치에는 관리 그룹에 속하는 장치와 미할당 장치가 포함될 수 있습니다.
- 장치 주소를 직접 지정하거나 주소 목록에서 가져옵니다. 작업을 할당할 장치의 NetBIOS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

7단계. 작업을 실행할 계정 선택

운영 체제의 도구를 사용하여 네트워크 에이전트를 설치하기 위한 계정을 선택합니다. 이 경우 컴퓨터 접근을 위한 관리자 권한이 필요합니다. 계정은 여러 개 추가할 수 있습니다. 계정에 충분한 권한이 없으면 설치 마법사는 다음 계정을 사용합니다. 네트워크 에이전트 도구를 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 설치하는 경우에는 계정을 선택할 필요가 없습니다.

8 단계. 작업 시작 스케줄 구성

작업 시작 스케줄(예: 직접 또는 컴퓨터가 유휴 상태일 때)을 구성하십시오.

9단계. 작업 이름 정의

작업 이름을 입력합니다(*Kaspersky Industrial CyberSecurity for Nodes for Windows 5.0 설치* 등).

10 단계. 작업 생성 완료

마법사를 완료합니다. 필요하다면 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다. 애플리케이션이 숨김 모드로 설치됩니다. 설치가 완료되면 사용자 컴퓨터의 알림 영역에 아이콘이 추가됩니다. 아이콘이 표시되는 경우 애플리케이션을 활성화했는지 확인하십시오.

웹 콘솔에서 원격 설치 작업을 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
   작업 목록이 열립니다.
2. **추가** 버튼을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 일반 작업 설정 구성

일반 작업 설정을 구성하려면 다음을 수행하십시오.

1. **애플리케이션** 드롭다운 목록에서 **Kaspersky Security Center**를 선택합니다.
2. **작업 유형** 드롭다운 목록에서 **원격으로 애플리케이션 설치** 옵션을 선택합니다.
3. **작업 이름** 필드에 *Kaspersky Industrial CyberSecurity for Nodes for Managers 설치*와 같은 간단한 설명을 입력합니다.
4. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.

2단계. 설치할 컴퓨터 선택

이 단계에서는 선택한 작업 범위 옵션에 따라 Kaspersky Industrial CyberSecurity for Nodes를 설치할 컴퓨터를 선택합니다.

3단계. 설치 패키지 구성

이 단계에서는 설치 패키지를 구성합니다:

1. Kaspersky Industrial CyberSecurity for Nodes for Windows (5.0) 설치 패키지를 선택합니다.
2. 네트워크 에이전트 설치 패키지를 선택합니다.

   선택한 네트워크 에이전트 버전이 Kaspersky Industrial CyberSecurity for Nodes와 함께 설치됩니다. *네트워크 에이전트*를 설치하면 중앙 관리 서버와 클라이언트 컴퓨터가 원활하게 상호 작용할 수 있습니다. 네트워크 에이전트가 컴퓨터에 이미 설치되어 있으면 다시 설치되지 않습니다.

3. **강제 설치 패키지 다운로드** 블록에서 애플리케이션 설치 방법을 선택합니다:

   - **네트워크 에이전트 이용**. 네트워크 에이전트는 Kaspersky Industrial CyberSecurity for Nodes 설치 패키지를 클라이언트 컴퓨터로 전달하는 작업을 담당합니다. 네트워크 에이전트가 설치되어 있지 않으면 작업이 종료되고 오류가 발생합니다. 이 경우 네트워크 에이전트 설치 패키지를 *원격으로 애플리케이션 설치* 작업에 추가하고 운영 체제 리소스를 통한 파일 전달을 활성화합니다. 그런 다음 운영 체제 리소스를 사용하여 네트워크 에이전트가 설치됩니다. Kaspersky Industrial CyberSecurity for Nodes는 그 다음에 네트워크 에이전트를 사용하여 설치됩니다.

   - **배포 지점에서 대상 운영 체제의 관리 공유 폴더로 다운로드**. 설치 패키지가 배포 지점을 통해 운영 체제 리소스를 사용하여 클라이언트 컴퓨터로 배달됩니다. 네트워크에 배포 지점이 하나 이상 있으면 이 옵션을 선택할 수 있습니다. 배포 지점에 대한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.

   - **중앙 관리 서버에서 대상 운영 체제의 관리 공유 폴더로 다운로드**. 중앙 관리 서버를 통해 운영 체제 리소스를 사용하여 클라이언트 컴퓨터로 파일이 배달됩니다. 이 옵션은 클라이언트 컴퓨터에 네트워크 에이전트가 설치되어 있지 않아도 선택할 수 있지만, 이 경우 클라이언트 컴퓨터는 중앙 관리 서버와 같은 네트워크에 있어야 합니다.

4. **최대 동시 다운로드 수** 필드에서 중앙 관리 서버로 전송되는 설치 패키지 다운로드 요청 수의 제한을 설정합니다. 요청 수를 제한하면 네트워크 오버로드를 방지할 수 있습니다.

5. **최대 설치 시도 횟수** 필드에서 애플리케이션 설치 시도 횟수의 제한을 설정합니다. Kaspersky Industrial CyberSecurity for Nodes 설치 종료 시 오류가 발생하면 설치 작업에서 설치가 자동으로 다시 시작됩니다.

6. 필요하다면 **이미 설치한 애플리케이션은 설치하지 않음** 확인란을 선택 해제합니다. 그러면 애플리케이션의 이전 버전 중 하나를 설치하는 등의 작업을 수행할 수 있습니다.

7. 필요하다면 **다운로드하기 전에 운영 체제 유형 확인** 확인란을 선택 해제합니다. 이렇게 하면 컴퓨터의 운영 체제가 소프트웨어 요구 사항을 충족하지 않는 경우 애플리케이션 배포 패키지가 다운로드되지 않습니다. 컴퓨터 운영 체제가 소프트웨어 요구 사항을 확실히 충족한다면 이 확인을 건너뛸 수 있습니다.

8. 필요하다면 **Active Directory 그룹 정책에 패키지 설치 지정** 확인란을 선택합니다. Kaspersky Industrial CyberSecurity for Nodes는 네트워크 에이전트를 통해 설치되거나 Active Directory를 통해 직접 설치됩니다. 네트워크 에이전트를 설치하려면 도메인 관리자 권한으로 원격 설치 작업을 실행해야 합니다.

9. 필요하다면 **실행 중인 애플리케이션의 종료 여부를 사용자에게 물어 보기** 확인란을 선택합니다. Kaspersky Industrial CyberSecurity for Nodes를 설치할 때는 컴퓨터 리소스가 사용됩니다. 사용자의 편의를 위해 애플리케이션 설치 마법사에서는 설치를 시작하기 전에 실행 중인 애플리케이션을 닫으라는 메시지가 표시됩니다. 이렇게 하면 다른 애플리케이션의 동작 중단과 컴퓨터의 오작동 가능성을 방지할 수 있습니다.

10. **다른 중앙 관리 서버를 통해 관리되는 기기를 위한 동작** 블록에서 Kaspersky Industrial CyberSecurity for Nodes 설치 방법을 선택합니다. 네트워크에 중앙 관리 서버가 두 대 이상 설치되어 있으면 해당 서버가 같은 클라이언트 컴퓨터를 확인할 수 있습니다. 이 경우 서로 다른 중앙 관리 서버를 통해 같은 클라이언트 컴퓨터에 애플리케이션이 여러 번 원격으로 설치되는 등의 문제나 기타 충돌이 발생할 수 있습니다.

4단계. 작업을 실행할 계정 선택

운영 체제의 도구를 사용하여 네트워크 에이전트를 설치하기 위한 계정을 선택합니다. 이 경우 컴퓨터 접근을 위한 관리자 권한이 필요합니다. 계정은 여러 개 추가할 수 있습니다. 계정에 충분한 권한이 없으면 설치 마법사는 다음 계정을 사용합니다. 네트워크 에이전트 도구를 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 설치하는 경우에는 계정을 선택할 필요가 없습니다.

5단계. 작업 생성 완료

마침 버튼을 클릭해 마법사를 마칩니다. 작업 목록에 새 작업이 표시됩니다. 작업을 실행하려면 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다. 애플리케이션이 숨김 모드로 설치됩니다. 설치가 완료되면 사용자 컴퓨터의 알림 영역에 아이콘이 추가됩니다. 아이콘이 표시되는 경우 애플리케이션을 활성화했는지 확인하십시오.

설치 패키지 생성과 원격 설치 작업 생성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Industrial CyberSecurity for Nodes 설치 후 수행할 동작

Kaspersky Industrial CyberSecurity for Nodes를 설치한 후 장치의 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스를 업데이트하고, Kaspersky Industrial CyberSecurity for Nodes 설치 전에 장치에 실시간 보호가 활성화된 안티 바이러스 애플리케이션이 없었을 시 장치에서 중요 영역 검사를 수행하는 것이 좋습니다.

Kaspersky Industrial CyberSecurity for Nodes가 설치된 보호 중인 장치가 Kaspersky Security Center의 같은 관리 그룹에 있다면, 다음 방법으로 이 작업을 수행할 수 있습니다.

1. Kaspersky Industrial CyberSecurity for Nodes가 설치된 보호 중인 장치 그룹에 대한 *업데이트* 작업 생성. Kaspersky Security Center 중앙 관리 서버를 업데이트 경로로 설정합니다.
2. *중요 영역 검사* 상태로 그룹 온디맨드 검사 작업을 생성합니다. Kaspersky Security Center는 *중요 영역 검사* 작업이 아닌 이 작업의 결과를 바탕으로 그룹에 속한 각 보호 중인 장치의 보안 상태를 평가합니다.
3. 보호 중인 장치의 그룹에 대해 새 정책을 생성합니다. 정책 속성의 **애플리케이션 설정** 섹션에 있는 **로컬 시스템 작업 실행** 하위 섹션의 설정에서 중앙 관리 그룹의 보호 중인 장치에 대한 로컬 시스템 온디맨드 검사 작업 및 *업데이트* 작업의 예약된 시작을 비활성화합니다.

Kaspersky Industrial CyberSecurity for Nodes 이벤트에 대한 관리자 알림을 구성할 수도 있습니다.

Kaspersky Security Center를 통한 애플리케이션 콘솔 설치

설치 패키지와 원격 설치 작업의 생성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

원격 설치 작업을 사용하여 애플리케이션 콘솔을 설치하려면:

1. Kaspersky Security Center 관리 콘솔에서 **고급** 노드를 확장하고 다음을 수행합니다.
2. **원격 설치** 하위 노드를 확장합니다.

3. 설치 패키지를 만듭니다:

   a. **설치 패키지** 하위 노드의 결과 창에서 **설치 패키지 생성** 버튼을 클릭합니다.

   b. **새 패키지 마법사** 창에서 선택 **지정한 실행 파일에 대한 설치 패키지 생성**을 패키지 유형으로 선택합니다.

   c. 새 설치 패키지 이름을 입력합니다.

   d. Kaspersky Industrial CyberSecurity for Nodes 배포 키트 폴더에서 \client\setup_kicstool.exe 파일을 선택하고 **전체 폴더를 설치 패키지로 복사** 확인란을 선택합니다.

   e. **실행 파일 실행 설정(옵션)** 필드에서 파라미터 값 EULA=1 및 PRIVACYPOLICY=1을 지정합니다.

   ```
   /s /p "EULA=1 PRIVACYPOLICY=1"
   ```

   아니면 구성 요소를 설치할 수 없습니다.

   f. 필요하다면 **실행 파일 시작 설정(옵션)** 필드에서 ADDLOCAL 명령줄 파라미터를 지정하여 설치할 구성 요소 세트를 변경할 수 있으며, INSTALLDIR 명령줄 파라미터를 지정하여 기본 폴더가 아닌 다른 대상 폴더를 지정할 수 있습니다. 예를 들어 C:\KasperskyConsole 폴더에 애플리케이션 콘솔을 독립 실행형으로 설치하려면 다음 명령줄 옵션을 사용하십시오:

   ```
   /s /p "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
   ```

4. **설치 패키지** 하위 노드에서 선택한 보호 중인 장치(관리 그룹)에 애플리케이션 콘솔을 원격으로 설치하는 작업을 만듭니다.

5. 작업 설정을 구성합니다.

6. 원격 설치 작업을 실행합니다.

애플리케이션 콘솔은 작업에 지정된 보호 중인 장치에 설치됩니다.

Kaspersky Security Center를 통해 Kaspersky Industrial CyberSecurity for Nodes 제거

Kaspersky Industrial CyberSecurity for Nodes 제거 시 덤프 및 추적 파일은 삭제되지 않습니다. 덤프 및 추적 파일 쓰기 구성 중에 지정한 폴더에서 덤프 및 추적 파일을 직접 삭제할 수 있습니다.

네트워크 장치에서 Kaspersky Industrial CyberSecurity for Nodes의 관리가 암호로 보호되어 있다면 여러 애플리케이션 제거 작업을 생성할 때 암호를 입력해야 합니다. Kaspersky Security Center 정책에서 암호 보호를 중앙 관리하지 않는다면, 입력된 암호가 설정 값과 일치할 때 Kaspersky Industrial CyberSecurity for Nodes가 장치에서 제거됩니다. 다른 보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes가 제거되지는 않습니다.

Kaspersky Industrial CyberSecurity for Nodes를 제거하려면:

1. Kaspersky Security Center 관리 콘솔에서 애플리케이션 제거 작업을 생성하고 시작합니다.

2. 이 작업에서 제거 방법을 선택하고(설치 방법 선택과 유사, 이전 섹션 참조) 중앙 관리 서버가 보호 중인 장치에 접근할 때 사용할 계정을 지정합니다. Kaspersky Industrial CyberSecurity for Nodes는 기본 제거 설정으로만 제거할 수 있습니다.

Kaspersky Security Center를 사용하여 애플리케이션 구성 요소 세트 변경

애플리케이션 구성 요소 변경 작업을 사용하면 애플리케이션을 설치한 이후에도 Kaspersky Industrial CyberSecurity for Nodes의 구성 요소 집합을 변경할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 애플리케이션 구성 요소 집합을 변경하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **작업**을 선택합니다.
   작업 목록이 열립니다.

2. **새 작업** 버튼을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Industrial CyberSecurity for Nodes (5.0) → 애플리케이션 구성 요소 변경 옵션을 선택합니다.

2단계. 애플리케이션 구성 요소 변경을 위한 작업 설정

사용자 컴퓨터에서 사용 가능한 애플리케이션 구성 요소를 선택합니다. 작업에 대한 고급 설정을 구성합니다(아래 표 참조).

MDR용 Endpoint Agent를 사용하도록 애플리케이션 구성을 수정할 때, 원격 측정 수신을 담당하는 모든 구성 요소가 활성화되어 있는지 확인하십시오.

3단계. 작업을 할당할 장치 선택

작업을 수행할 컴퓨터를 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.

- 관리 그룹에 작업 할당. 이 경우 이전에 만든 관리 그룹에 포함된 컴퓨터에 작업이 할당됩니다.
- 네트워크에서 중앙 관리 서버가 탐지한 컴퓨터 선택: *미할당 장치*. 이 특정 장치에는 관리 그룹에 속하는 장치와 미할당 장치가 포함될 수 있습니다.
- 장치 주소를 직접 지정하거나 주소 목록에서 가져옵니다. 작업을 할당할 장치의 NetBIOS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

4 단계. 작업 시작 스케줄 구성

작업 시작 스케줄(예: 직접 또는 컴퓨터가 유휴 상태일 때)을 구성하십시오.

5단계. 작업 이름 정의

작업 이름을 입력하십시오(예: *애플리케이션 제어 구성 요소 추가*).

6단계. 작업 생성 완료

마법사를 완료합니다. 필요하다면 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서 애플리케이션 구성 요소 집합을 변경하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
   작업 목록이 열립니다.
2. **추가** 버튼을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 일반 작업 설정 구성

일반 작업 설정을 구성하려면 다음을 수행하십시오.

1. **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes 5.0.0** 옵션을 선택합니다.
2. **작업 유형** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes 구성 요소 변경** 옵션을 선택합니다.

3. **작업 이름** 필드에 *애플리케이션 제어 구성 요소 추가* 등의 간단한 설명을 입력합니다.

4. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.

2단계. 작업을 할당할 장치 선택

작업을 수행할 컴퓨터를 선택합니다. 예를 들어 별도의 관리 그룹을 선택하거나 선택 항목을 작성합니다.

3단계. 작업 생성 완료

1. **생성이 완료되면 작업 세부 정보 열기** 확인란을 선택하고 마법사를 종료합니다.

2. 작업 속성에서 **애플리케이션 설정** 탭을 선택합니다.

3. 사용자 컴퓨터에서 사용 가능한 애플리케이션 구성 요소를 선택합니다. 작업에 대한 고급 설정을 구성합니다(아래 표 참조).

> MDR용 Endpoint Agent를 사용하도록 애플리케이션 모드를 수정할 때, 원격 측정 수신을 담당하는 모든 구성 요소가 활성화되어 있는지 확인하십시오.

그 결과 사용자 컴퓨터의 Kaspersky Industrial CyberSecurity for Nodes 구성 요소 세트가 숨김 모드로 변경됩니다.

고급 작업 설정

파라미터	설명
산업용 소프트웨어 예외 프로필	*애플리케이션 구성 요소 변경* 작업의 경우 검사 예외와 신뢰하는 애플리케이션만 신뢰 구역에 추가할 수 있습니다.
애플리케이션 구성 요소 변경 시 암호 사용	관리자는 일반적으로 암호 보호를 사용하여 Kaspersky Industrial CyberSecurity for Nodes에 대한 액세스를 제한합니다. 즉, 애플리케이션 구성 요소를 수정하기 위해서는 **애플리케이션 제거 / 수정 / 복원** 권한을 가진 사용자의 자격 증명을 입력해야 합니다. 예를 들어, KLAdmin 계정을 사용할 수 있습니다.
호환되지 않는 타사 애플리케이션 확인	기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 설치된 애플리케이션의 호환성을 확인합니다. 호환되지 않는 소프트웨어 목록은 배포 키트에 포함된 incompatible.txt 파일에서 확인할 수 있습니다. 호환되지 않는 소프트웨어 검사를 사용하는 경우 Kaspersky Industrial CyberSecurity for Nodes는 목록에서 애플리케이션이 탐지되면 작업을 중지합니다. 타사 소프트웨어 공급업체 설명서에 Endpoint Protection Platform(EPP)과의 호환성이 나와 있는 경우 설치된 소프트웨어 검사를 비활성화할 수 있습니다.
호환되지 않는 타사 애플리케이션 제거	구성 요소 세트를 변경하기 전에 incompatible.txt 목록에서 애플리케이션 자동 제거. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 작업을 계속하기 위해 호환성 문제를 유발할 수 있는 애플리케이션을 제거하려고 시도합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

Active Directory 그룹 정책을 통해 애플리케이션 설치 및 제거

이 섹션에서는 Active Directory 그룹 정책을 통해 Kaspersky Industrial CyberSecurity for Nodes를 설치 및 제거하는 방법과 그룹 정책을 통해 Kaspersky Industrial CyberSecurity for Nodes를 설치한 후 수행해야 하는 동작에 대한 정보를 설명합니다.

Active Directory 그룹 정책을 통해 Kaspersky Industrial CyberSecurity for Nodes 설치

Active Directory 그룹 정책을 통해 여러 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치할 수 있습니다. 같은 방법으로 애플리케이션 콘솔을 설치할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 또는 애플리케이션 콘솔을 설치할 보호 중인 장치는 같은 도메인 및 단일 조직 단위에 있어야 합니다.

정책을 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 설치할 보호 중인 장치의 운영 체제는 버전이 서로 같아야 합니다(32비트 또는 64비트).

도메인 관리자 권한이 필요합니다.

Kaspersky Industrial CyberSecurity for Nodes를 설치하려면 kics_win.msi 설치 패키지를 사용하십시오. 애플리케이션 콘솔을 설치하려면 kicstools.msi 설치 패키지를 사용하십시오.

Active Directory 그룹 정책 사용에 대한 자세한 내용은 Microsoft에서 제공하는 문서를 참조하십시오.

Kaspersky Industrial CyberSecurity for Nodes 또는 애플리케이션 콘솔을 설치하려면:

1. kics_win.msi를 도메인 컨트롤러의 공유 폴더에 저장합니다.
2. 키 파일을 도메인 컨트롤러의 동일한 공용 폴더에 저장합니다.
3. 도메인 컨트롤러의 동일한 공유 폴더에서 아래 행을 포함하는 install_props.json 파일을 생성하십시오. 이는 최종 사용자 라이센스 계약서 및 개인정보취급방침에 동의함을 의미합니다.

   ```
   {
   "EULA": "1",
   "PRIVACYPOLICY": "1"
   }
   ```

4. 도메인 컨트롤러에서 보호 중인 장치가 속한 그룹에 대한 새 정책을 만듭니다.
5. **그룹 정책 개체 편집기**를 사용하여 **컴퓨터 구성** 노드에서 새 설치 패키지를 만듭니다. UNC(Universal Naming Convention) 형식으로 Kaspersky Industrial CyberSecurity for Nodes(또는 애플리케이션 콘솔)용 msi 파일의 경로를 지정합니다.
6. 선택한 그룹의 **컴퓨터 구성** 노드와 **사용자 구성** 노드에서 Windows Installer의 **항상 상승된 권한으로 설치** 확인란을 선택합니다.
7. `gpupdate / force` 명령으로 변경사항을 적용합니다.

그룹의 보호 중인 장치를 다시 시작하면 Kaspersky Industrial CyberSecurity for Nodes가 설치됩니다.

Kaspersky Industrial CyberSecurity for Nodes 설치 후 수행할 동작

보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치한 후, 애플리케이션 데이터베이스를 즉시 업데이트하고 중요 영역 검사를 실행하는 것이 좋습니다. 애플리케이션 콘솔에서 이 동작을 수행할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 이벤트에 대한 관리자 알림을 구성할 수도 있습니다.

Active Directory 그룹 정책을 통해 Kaspersky Industrial CyberSecurity for Nodes 제거

Kaspersky Industrial CyberSecurity for Nodes 제거 시 덤프 및 추적 파일은 삭제되지 않습니다. 덤프 및 추적 파일 쓰기 구성 중에 지정한 폴더에서 덤프 및 추적 파일을 직접 삭제할 수 있습니다.

Active Directory 그룹 정책을 사용하여 보호 중인 장치 그룹에 Kaspersky Industrial CyberSecurity for Nodes(또는 애플리케이션 콘솔)를 설치했다면, 이 정책을 사용하여 Kaspersky Industrial CyberSecurity for Nodes(또는 애플리케이션 콘솔)를 제거할 수 있습니다.

기본 제거 파라미터만으로 이 애플리케이션을 제거할 수 있습니다.

Active Directory 그룹 정책 사용에 대한 자세한 내용은 Microsoft에서 제공하는 문서를 참조하십시오.

애플리케이션 관리가 암호로 보호 중이라면 Active Directory 그룹 정책을 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 제거할 수 없습니다.

Kaspersky Industrial CyberSecurity for Nodes(또는 애플리케이션 콘솔)를 제거하려면:

1. 도메인 컨트롤러에서 Kaspersky Industrial CyberSecurity for Nodes 또는 애플리케이션 콘솔을 제거할 보호 중인 장치가 있는 조직 단위를 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 설치를 위해 생성된 정책을 선택하고 **그룹 정책 개체 편집기**의 **소프트웨어 설치** 노드(**컴퓨터 구성** > **소프트웨어 설정** > **소프트웨어 설치**)에서 Kaspersky Industrial CyberSecurity for Nodes(또는 애플리케이션 콘솔) 설치 패키지의 마우스 오른쪽 메뉴를 연 다음 **모든 작업** > **제거** 명령을 선택합니다.
3. **사용자 및 컴퓨터에서 소프트웨어를 즉시 제거** 제거 방법을 선택합니다.
4. `gpupdate /force` 명령으로 변경사항을 적용합니다.

   다시 시작된 후 Microsoft Windows에 로그인하기 전에 보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes가 제거됩니다.

Kaspersky Industrial CyberSecurity for Nodes 설치 및 제거 로그

설치/제거 마법사를 사용하여 Kaspersky Industrial CyberSecurity for Nodes나 애플리케이션 콘솔을 설치/제거하면 Windows Installer 서비스가 설치/제거 로그를 생성합니다. kl-install-<uid>.log(여기서<uid> 는 고유한 8자 로그 식별자)라는 로그 파일이 setup_kics.exe 또는 setup_kicstool.exe 파일 시작에 사용한 계정의 사용자 %temp% 폴더에 저장됩니다.

명령줄에서 Kaspersky Industrial CyberSecurity for Nodes를 설치 또는 설치 제거하는 경우에는 기본적으로 설치 로그 파일이 만들어지지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes를 설치하고 디스크 C:\에 로그 파일을 생성하려면 다음 명령을 실행합니다.

```
msiexec /i kics_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

Kaspersky Industrial CyberSecurity for Nodes 설치 후 시스템 변경 사항

Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Nodes 콘솔을 함께 설치하면, Windows Installer 서비스가 보호 중인 장치를 다음과 같이 수정합니다.

- 보호 중인 장치와 애플리케이션 콘솔이 설치된 장치에 Kaspersky Industrial CyberSecurity for Nodes 폴더가 생성됩니다.
- Kaspersky Industrial CyberSecurity for Nodes service가 등록됩니다.
- Kaspersky Industrial CyberSecurity for Nodes 사용자 그룹이 생성됩니다.
- Kaspersky Industrial CyberSecurity for Nodes 키가 시스템 레지스트리에 등록됩니다.
- Windows 작업 스케줄러에 표시되는 Kaspersky Industrial CyberSecurity for Nodes OS Upgrade Detect 시스템 작업이 생성됩니다.
- Windows 방화벽 규칙이 생성됩니다.

이러한 변경 사항에 관한 설명은 아래에 있습니다.

보호 중인 장치의 Kaspersky Industrial CyberSecurity for Nodes 폴더

Kaspersky Industrial CyberSecurity for Nodes를 설치하면, 보호 중인 장치에 다음 폴더가 생성됩니다:

- Kaspersky Industrial CyberSecurity for Nodes 실행 파일을 포함하는 Kaspersky Industrial CyberSecurity for Nodes 기본 설치 폴더. 기본적으로 다음 설치 폴더가 사용됩니다:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0

- SNMP 프로토콜을 사용하여 Kaspersky Industrial CyberSecurity for Nodes에서 게시한 카운터와 후크에 대한 설명이 포함된 Management Information Base (MIB) 파일.

  %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0\mibs

- Kaspersky Industrial CyberSecurity for Nodes service 파일:

  - %ProgramData%\Kaspersky Lab\KICS.5.0\Data
  - %ProgramData%\Kaspersky Lab\KICS.5.0\Settings
  - %ProgramData%\Kaspersky Lab\KICS.5.0\Dskm

- 업데이트 경로 설정이 있는 파일:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Data

- *업데이트* 작업을 사용하여 다운로드한 데이터베이스와 소프트웨어 모듈의 업데이트(폴더는 *업데이트* 작업을 사용하여 처음 업데이트를 다운로드할 때 생성됨).

  %ProgramData%\Kaspersky Lab\KICS.5.0\Update distribution

- 작업 로그 및 시스템 감사 로그:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Reports

- 현재 사용 중인 데이터베이스 집합:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Bases

- 데이터베이스의 백업 복사본, 데이터베이스를 업데이트할 때마다 대체됩니다:

  %ProgramData%\Kaspersky Lab\KICS.5.0\QB

- 업데이트 작업을 실행하는 중에 만들어진 임시 파일:

  %ProgramData%\Kaspersky Lab\KICS.5.0\Data\temp\temporaryFolder

- 격리된 개체(기본 폴더):

  %ProgramData%\Kaspersky Lab\KICS.5.0\QB

- 백업 중인 개체(기본 폴더):

  %ProgramData%\Kaspersky Lab\KICS.5.0\QB

- 백업과 격리에서 복원된 개체(복원된 개체의 기본 폴더):

  %ProgramData%\Kaspersky Lab\KICS.5.0\QB\Restored

애플리케이션 콘솔 설치 시 생성된 폴더

애플리케이션 콘솔의 기본 설치 폴더는 운영 체제 비트 설정에 따라 다릅니다. 기본적으로 다음 설치 폴더가 사용됩니다:

%ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Console 5.0.0

Kaspersky Industrial CyberSecurity for Nodes service

다음 Kaspersky Industrial CyberSecurity for Nodes 서비스는 SYSTEM 계정으로 실행됩니다.

- Kaspersky Industrial CyberSecurity for Nodes 서비스 (AVP.KICS.5.0). Kaspersky Industrial CyberSecurity for Nodes의 주요 시스템 서비스로, 바이러스 및 기타 위협으로부터 장치를 보호합니다
- Kaspersky Industrial CyberSecurity for Nodes Side-by-Side 서비스 (AVP.KICS.5.0.SbS). Kaspersky Industrial CyberSecurity for Nodes가 업데이트 또는 복원되거나 구성 요소가 변경되는 동안 장치를 보호하는 시스템 서비스입니다
- Kaspersky Seamless Update Service (avpsus.KICS.5.0). 긴급 또는 승인된 애플리케이션 모듈 업데이트를 설치하거나 롤백하는 시스템 서비스입니다
- Kaspersky Industrial CyberSecurity for Nodes 원격 제어 서비스 서비스 (avpcos.KICS.5.0). 애플리케이션 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes Service를 원격으로 다시 시작하거나 중지하기 위한 시스템 서비스입니다

Kaspersky Industrial CyberSecurity for Nodes 그룹

KICS 관리자는 보호 중인 장치의 그룹이며, 이 그룹의 구성원은 모든 Kaspersky Industrial CyberSecurity for Nodes 기능에 대한 전체 접근 권한을 가집니다.

시스템 레지스트리 키

Kaspersky Industrial CyberSecurity for Nodes를 설치하면 다음 시스템 레지스트리 키가 생성됩니다:

- Kaspersky Industrial CyberSecurity for Nodes 설정:

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.KICS.5.0]
- Kaspersky Industrial CyberSecurity for Nodes 이벤트 로그(Kaspersky Event Log) 파라미터:

  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Industrial CyberSecurity for Nodes]
- 추적 파일 설정:

  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.5.0\Trace]

- 애플리케이션 작업 및 기능에 대한 설정:
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.5.0\environment]

Kaspersky Industrial CyberSecurity for Nodes OS 업그레이드 탐지 시스템 작업

Windows Installer 서비스는 애플리케이션 설치 중에 Kaspersky Industrial CyberSecurity for Nodes OS 업그레이드 탐지(OS Upgrade Detect) 작업을 생성합니다. 작업은 생성 즉시 시작되며 나중에는 OS를 시작할 때마다 시작됩니다. 작업이 애플리케이션에서 사용하는 드라이버의 버전을 확인합니다. 운영 체제 버전이 업데이트되면 애플리케이션은 운영 체제의 해당 버전에 대한 드라이버를 업데이트합니다.

이 작업은 애플리케이션에 영향을 주지 않으며 삭제할 수 있습니다. 운영 체제 업그레이드 시나리오를 염두에 두는 것이 좋습니다.

Windows 방화벽 규칙

지정한 설치 설정에 따라 아래 표에 설명된 수신 연결용 Windows 방화벽 허용 규칙이 보호 대상 장치에 생성될 수 있습니다.

Windows 방화벽 규칙

규칙 이름	규칙 설명	규칙 생성 조건
AVP.KICS.5.0	실행 파일 avp.exe에 대한 허용 규칙입니다.	항상 생성됩니다.
AVP.KICS.5.0 Remote UI Connection	TCP 포트 13032에 대한 허용 규칙입니다.	`ADDWFEXCLUSION=1` 매개변수를 사용하여 애플리케이션 설치.
AVP.KICS.5.0 Remote UI Connection	TCP 포트 13031에 대한 허용 규칙입니다. 기본적으로 이 포트 번호가 사용됩니다. `UIKLPORT=<port>` 매개변수를 지정하여 포트 번호를 변경할 수 있습니다. 이 경우 애플리케이션은 지정한 포트 번호에 대한 규칙을 생성합니다.	`ADDWFEXCLUSION=1` 및 `UIKLPORT=13031` 매개변수를 사용하여 애플리케이션 설치. `ENABLEUIKLPORT=0` 매개변수가 전달되면 규칙이 생성되지 않음
DHCP Discover In	UDP 포트 67에 대한 허용 규칙입니다.	KICS for Networks와 통합 구성 요소를 포함하여 애플리케이션 설치.
SSDP Discover In	UDP 포트 1900에 대한 허용 규칙입니다.	

Kaspersky Industrial CyberSecurity for Nodes 프로세스

Kaspersky Industrial CyberSecurity for Nodes는 아래 표에서 설명하는 프로세스를 시작합니다.

Kaspersky Industrial CyberSecurity for Nodes 프로세스

파일 이름	용도
avp.exe	Kaspersky Industrial CyberSecurity for Nodes 작업 흐름
avpsus.exe	이 프로세스를 통해 중요하고 승인된 애플리케이션 모듈 업데이트를 설치하고 롤백할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 기능 확인. EICAR 테스트 바이러스 사용

이 섹션에서는 EICAR 테스트 바이러스와 EICAR 테스트 바이러스를 사용하여 Kaspersky Industrial CyberSecurity for Nodes의 실시간 파일 보호와 온디맨드 검사 기능을 확인하는 방법에 대해 설명합니다.

EICAR 테스트 바이러스 정보

이 테스트 바이러스는 안티 바이러스 애플리케이션의 동작을 확인하기 위해 설계되었습니다. 이 바이러스는 EICAR(European Institute for Computer Antivirus Research)에 의해 개발되었습니다.

테스트 바이러스는 악성 개체가 아니며 사용자 장치의 실행 코드도 들어있지 않지만, 안티 바이러스 애플리케이션 대부분에서 위협으로 식별합니다.

이 테스트 바이러스가 포함된 파일은 eicar.com이라고 합니다. EICAR 웹사이트에서 다운로드할 수 있습니다.

장치의 하드 드라이브 폴더에 파일을 저장하기 전에 해당 드라이브에서 실시간 파일 보호 구성 요소를 비활성화했는지 확인하십시오.

eicar.com 파일에는 한 줄의 텍스트가 포함되어 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 파일 검사 시 이 텍스트 줄에서 테스트 위협을 탐지하면 **감염** 상태를 파일에 할당하고 삭제합니다. 파일에서 탐지한 위협에 대한 정보는 애플리케이션 콘솔과 작업 로그에 표시됩니다.

eicar.com 파일을 사용하여 Kaspersky Industrial CyberSecurity for Nodes의 감염 개체 치료 방법과 감염 의심 개체 탐지 방법을 확인할 수 있습니다. 이렇게 하려면 텍스트 편집기를 사용하여 파일을 열고 아래 표에 나열된 접두어 중 하나를 파일의 텍스트 줄 시작 부분에 추가한 후, 파일을 새 이름(예: eicar_cure.com)으로 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes에서 접두사가 포함된 eicar.com 파일을 처리하도록 하려면 **개체 보호** 보안 설정 섹션에서 Kaspersky Industrial CyberSecurity for Nodes의 실시간 컴퓨터 보호 작업 및 기본 온디맨드 검사 작업에 **모든 개체** 값을 설정합니다.

EICAR 파일의 접두사

접두사	검사 후 파일 상태 및 Kaspersky Industrial CyberSecurity for Nodes 동작
접두사 없음	**Kaspersky Industrial CyberSecurity for Nodes는 개체에 감염 상태를 지정한 후 개체를 삭제합니다.**
SUSP–	Kaspersky Industrial CyberSecurity for Nodes는 휴리스틱 분석기에서 탐지한 개체에 **감염 의심** 상태를 지정한 후 개체를 삭제합니다(감염된 개체가 치료되지 않음).
WARN–	Kaspersky Industrial CyberSecurity for Nodes는 개체 코드가 알려진 위협 코드와 부분적으로 일치하는 개체에 **감염 의심** 상태를 지정한 후 개체를 삭제합니다(감염 가능성 있는 개체가 치료되지 않음).
CURE–	Kaspersky Industrial CyberSecurity for Nodes는 개체에 **감염** 상태를 지정한 후 바이러스를 치료합니다. 바이러스 치료가 완료되면 파일에 있는 전체 텍스트가 "CURE" 단어로 바뀝니다.

실시간 파일 보호 및 온디맨드 검사 기능 확인

Kaspersky Industrial CyberSecurity for Nodes를 설치한 후 Kaspersky Industrial CyberSecurity for Nodes가 악성 코드가 포함된 개체를 탐지하는지 확인할 수 있습니다. 이렇게 하려면 EICAR 테스트 바이러스를 사용합니다.

실시간 파일 보호 기능을 확인하려면:

1. EICAR 웹사이트에서 eicar.com 파일을 다운로드합니다. 이 파일을 네트워크에 있는 아무 장치의 로컬 드라이브 내 공유 폴더에 저장합니다.

   폴더에 파일을 저장하기 전에 이 폴더에서 실시간 파일 보호가 비활성화되었는지 확인하십시오.

2. 네트워크 사용자 알림이 작동하는지 확인하려면, 보호 중인 장치와 eicar.com 파일을 저장한 장치에서 Microsoft Windows Messenger 서비스를 사용할 수 있는지 확인합니다.

3. 보호 중인 장치에서 애플리케이션 콘솔을 엽니다.

4. 다음 방법 중 하나를 사용하여 저장된 eicar.com 파일을 보호 중인 장치의 로컬 드라이브에 복사합니다.

   - 터미널 서비스 창에서 알림을 테스트하려면 Remote Desktop Connection 유틸리티를 사용하여 보호 중인 장치에 연결한 후 eicar.com 파일을 보호 중인 장치로 복사합니다.

   - Microsoft Windows Messenger 서비스를 통해 알림을 테스트하려면, 장치의 네트워크 환경을 사용하여 eicar.com 파일을 저장한 장치에서 해당 파일을 복사합니다.

다음 조건을 충족하는 경우 실시간 파일 보호 구성 요소가 올바르게 작동합니다.

- 보호 중인 장치에서 eicar.com 파일이 삭제됩니다.

- 애플리케이션 콘솔에서 작업 로그에 *심각* 상태가 표시됩니다. 로그에 eicar.com 파일의 보안위협에 대한 정보가 들어 있는 새 줄이 추가됩니다.

- 파일을 복사한 장치에 다음 Microsoft Windows 메신저 서비스 메시지가 표시됩니다: Kaspersky Industrial CyberSecurity for Nodes가 <이벤트 발생 시간>에 <네트워크 장치 이름> 컴퓨터에서 <장치의 파일 경로>\eicar.com에 대한 접근을 차단했습니다. 이유: 위협이 탐지됨. 바이러스: EICAR-Test-File. 사용자 이름: <사용자 이름>. 컴퓨터 이름: <파일을 복사한 네트워크 장치 이름>.

  eicar.com 파일을 복사한 장치에서 Microsoft Windows 메신저 서비스가 실행 중인지 확인하십시오.

작업 로그를 보려면 다음과 같이 하십시오.

1. 애플리케이션 콘솔 트리에서 **온디맨드 검사** 노드를 확장합니다.

2. 생성된 온디맨드 검사 작업을 선택합니다.

3. 노드 결과 창에서 **작업 로그 열기** 링크를 클릭합니다.

온디맨드 검사 기능을 확인하려면:

1. EICAR 웹사이트에서 eicar.com 파일을 다운로드합니다. 이 파일을 네트워크에 있는 아무 장치의 로컬 드라이브 내 공유 폴더에 저장합니다.

   > 폴더에 파일을 저장하기 전에 이 폴더에서 실시간 파일 보호가 비활성화되었는지 확인하십시오.

2. 애플리케이션 콘솔을 열고 **온디맨드 검사** 노드를 확장합니다.
3. **중요 영역 검사** 하위 노드를 선택합니다.
4. 검사 범위의 **설정** 탭에서 **네트워크** 노드의 컨텍스트 메뉴를 엽니다.
5. **네트워크 파일 추가**를 선택합니다.
6. UNC(Universal Naming Convention) 형식으로 원격 컴퓨터에 있는 eicar.com 파일의 네트워크 경로를 입력합니다.
7. 추가된 네트워크 경로가 검사 범위에 포함되도록 체크박스를 선택합니다.
8. 중요 영역 검사 작업을 실행합니다.

다음 조건을 충족하는 경우 온디맨드 검사가 올바르게 작동합니다.

- eicar.com 파일이 장치의 하드 드라이브에서 삭제됩니다.
- 애플리케이션 콘솔에서 작업 로그에 *심각* 상태가 표시됩니다. 온디맨드 검사 작업 로그에 eicar.com 파일의 보안위협에 대한 정보가 담긴 줄이 새로 추가됩니다.

이전 버전의 Kaspersky Industrial CyberSecurity for Nodes를 버전 5.0로 업그레이드

이전 버전의 Kaspersky Industrial CyberSecurity for Nodes를 5.0 버전으로 업그레이드할 때는 다음 권장 사항을 따릅니다.

- 미리 계획하고 업그레이드 일정을 잡습니다. 서버가 가장 적은 부하로 작동하는 시간(주말 등)을 선택합니다.
- 업그레이드가 끝나면 애플리케이션 구성 요소를 하나씩 켭니다. 예를 들어 먼저 실시간 파일 보호 구성 요소만 활성화한 다음, 다른 보호 구성 요소를 활성화하고 제어 구성 요소를 활성화하는 식입니다. 각 단계에서 애플리케이션을 테스트하는 것이 좋습니다.
- 업그레이드를 단계별로 수행합니다. 먼저 컴퓨터 한 대를 업그레이드한 후 컴퓨터 여러 대를 업그레이드한 다음 조직의 모든 컴퓨터를 업그레이드합니다.

업그레이드 절차의 단계

다음 순서에 따라 Kaspersky Industrial CyberSecurity for Nodes 버전 5.0로 업그레이드합니다.

1. **Kaspersky Security Center 업그레이드**

   사용자 컴퓨터 및 Kaspersky Security Center 웹 콘솔의 네트워크 에이전트를 포함하여 Kaspersky Security Center 구성 요소 전체를 버전 14.2 이상으로 업그레이드합니다.

2. **Kaspersky Industrial CyberSecurity for Nodes 웹 플러그인 업그레이드**

   Kaspersky Security Center 웹 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 웹 플러그인을 5.0로 업그레이드합니다.

3. **Kaspersky Industrial CyberSecurity for Nodes 작업 및 정책 마이그레이션**

   정책 및 작업을 마이그레이션한 후에는, 애플리케이션의 이전 버전에 없어서 마이그레이션 마법사가 마이그레이션하지 못한 설정을 구성해야 합니다. 마이그레이션 마법사가 모든 설정을 올바르게 마이그레이션했는지도 확인하는 것이 좋습니다.

4. **Kaspersky Industrial CyberSecurity for Nodes 5.0 설치**

   Kaspersky Industrial CyberSecurity for Nodes 버전 5.0는 DCOM 프로토콜 대신 HTTPS 프로토콜을 사용합니다. 따라서 Kaspersky Industrial CyberSecurity for Nodes의 새 버전을 설치하기 전에, KICS 서비스를 원격으로 시작할 수 있도록 애플리케이션이 업데이트될 장치를 구성해야 합니다. 이러한 구성을 수행하지 않으면 원격 서비스를 시작할 수 없습니다.

   Kaspersky Industrial CyberSecurity for Nodes 5.0는 이전 버전의 애플리케이션을 제거한 후 설치하거나, 그 위에 설치할 수 있습니다.

   이전 버전의 애플리케이션 위에 설치한다면 같은 애플리케이션 구성 요소 집합이 설치되며, 이 때 일부 구성 요소의 새로운 이름과 내용도 고려합니다.

   원격 설치 시 설치 프로그램은 사용자가 설치 패키지 속성에서 선택한 구성 요소를 설치합니다.

5. **필요하다면 Kaspersky Industrial CyberSecurity for Nodes 5.0를 활성화**

   Kaspersky Industrial CyberSecurity for Nodes 5.0를 이전 버전의 애플리케이션 위에 설치하면, 현재 라이센스가 애플리케이션에 자동 적용되며 새 애플리케이션 구성 요소 및 작업을 완전히 사용할 수 있습니다. 라이센스 기간은 변경되지 않습니다.

6. **애플리케이션이 작동하는지 확인**

   Kaspersky Industrial CyberSecurity for Nodes를 업그레이드한 후 애플리케이션이 의도한 대로 작동하는지 확인합니다. 애플리케이션에 대해 보고된 오류가 없는지 확인하고, 중앙 관리 서버에 대한 마지막 연결 시간과 마지막 데이터베이스 업데이트 시간 및 컴퓨터 보호 상태를 확인합니다.

   예외 목록, 신뢰하는 애플리케이션, 장치 제어 규칙, 애플리케이션 실행 제어 규칙의 마이그레이션에 주의합니다.

Kaspersky Industrial CyberSecurity for Nodes 업데이트

Kaspersky Industrial CyberSecurity for Nodes 5.0로의 업그레이드는 3.2 이상의 버전에서 지원됩니다. 이전 버전의 애플리케이션에서 업데이트하려면 설치된 버전을 제거하고 버전 5.0를 설치해야 합니다.

업데이트는 설치된 애플리케이션 버전 위에 새 버전의 애플리케이션을 설치하여 수행되며 컴퓨터를 다시 시작할 필요가 없습니다.

기본적으로 애플리케이션은 기존 애플리케이션 설치 폴더의 경로를 기반으로 새 애플리케이션 버전의 이름을 사용하여 새 설치 폴더를 생성합니다. 애플리케이션 설치 폴더의 새 경로를 직접 지정할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 버전 5.0로 업그레이드하면, 이전에 설치한 애플리케이션 버전이 자동 삭제됩니다.

암호로 보호된 Kaspersky Industrial CyberSecurity for Nodes 설치 업데이트 시 다음 방법 중 하나로 설치 프로그램에 암호를 전달합니다:

- 설치 마법사 인터페이스를 통해 로컬로 설치하거나 대화식 CLI 모드로 설치할 때는 요청 시 암호를 입력합니다.
- 비대화식 CLI 모드로 로컬로 설치할 때는 `UNLOCK_PASSWORD` 키에 암호를 입력합니다.
- Active Directory 그룹 정책을 사용하여 설치할 때는 install_props.json 구성 파일에 `UNLOCK_PASSWORD` 키의 값을 사용합니다.

Kaspersky Security Center를 통해 원격으로 업그레이드하는 애플리케이션이 암호로 보호되어 있다면 먼저 Kaspersky Security Center 정책을 사용하여 암호 보호를 비활성화해야 합니다.

애플리케이션을 업데이트할 때 현재 라이센스가 Kaspersky Industrial CyberSecurity for Nodes 버전 5.0에 자동 적용되며, 새 애플리케이션 구성 요소 및 작업 전체를 사용할 수 있습니다. 라이센스 기간은 변경되지 않습니다.

만료된 라이센스로 애플리케이션을 업데이트하면 설치 후 새 버전의 애플리케이션이 기능 제한 모드로 실행됩니다(예: 애플리케이션 데이터베이스 업데이트 사용 불가).

Kaspersky Industrial CyberSecurity for Nodes 관리 도구 업데이트

Kaspersky Security Center로 애플리케이션을 관리하기 위한 관리 플러그인은 버전 3.2, 4.0 이상에서 버전 5.0로만 업데이트할 수 있습니다. 이전 버전의 관리 플러그인 및 애플리케이션 콘솔을 업데이트하려면 설치된 버전을 제거한 후 버전 5.0를 설치해야 합니다.

새 버전의 관리 플러그인이 이전에 설치한 버전 옆에 설치되며, 업데이트하는 동안 컴퓨터를 다시 시작할 필요는 없습니다.

관리 플러그인 설정 마이그레이션 방법에 관한 자세한 내용은 이 글을 참조하십시오.

정책 및 작업 마이그레이션

다음과 같은 방법으로 이전 버전의 애플리케이션에서 정책 및 작업 설정을 버전 5.0로 마이그레이션할 수 있습니다.

- 정책 및 작업 변환 마법사 사용(Kaspersky Security Center 관리 콘솔에서만 사용 가능).
- Kaspersky Industrial CyberSecurity for Nodes 5.0 정책 및 작업 마이그레이션 마법사 사용(Kaspersky Security Center 웹 콘솔에서만 이용 가능).

우선 단일 컴퓨터에서 Kaspersky Industrial CyberSecurity for Nodes의 정책 및 작업 마이그레이션을 시작한 다음, 컴퓨터 그룹을 거쳐 조직의 모든 컴퓨터를 대상으로 마이그레이션을 완료할 것을 권장합니다.

정책 및 작업 변환 마법사를 사용하여 정책 및 작업 설정을 마이그레이션하는 방법

1. Kaspersky Security Center 관리 콘솔에서 중앙 관리 서버를 선택하고 마우스 오른쪽 메뉴를 엽니다.
2. **모든 작업 → 정책 및 작업 변환 마법사**를 선택합니다.

   정책 및 작업 변환 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 정책 및 작업을 변환할 애플리케이션 선택

Kaspersky Industrial CyberSecurity for Nodes 5.0를 선택합니다. 다음 단계로 넘어갑니다.

2단계. 정책 전환

Kaspersky Industrial CyberSecurity for Nodes 5.0를 위해 생성할, 업그레이드되는 애플리케이션 버전의 정책을 선택합니다.

3단계. Kaspersky Endpoint Agent와 마이그레이션

필요하다면 마법사의 이전 단계에서 선택한 Kaspersky Industrial CyberSecurity for Nodes 정책에 대해, 새로운 Kaspersky Industrial CyberSecurity for Nodes 5.0 정책에 설정을 추가할 Kaspersky Endpoint Agent 정책을 하나씩 선택합니다. 다음 단계로 넘어갑니다.

4단계. 작업 전환

Kaspersky Industrial CyberSecurity for Nodes 5.0를 위해 전환할, 업그레이드되는 애플리케이션 버전의 그룹 작업을 선택합니다.

그룹이 아닌 작업(개별 장치에 할당된 작업)은 현재 단계에서는 표시되지 않습니다.

사용 중인 애플리케이션 버전의 그룹이 아닌 작업을 Kaspersky Industrial CyberSecurity for Nodes 5.0로 변환하려면:

1. **다음** 버튼을 클릭합니다.
   스케줄 및 비그룹 작업 추가 마이그레이션 창이 열립니다.
2. **비그룹 작업 마이그레이션** 확인란을 선택합니다.
3. Kaspersky Security Center 중앙 관리 서버에 대한 연결 설정을 지정합니다.
4. **확인** 버튼을 클릭합니다.

5단계. 마법사 완료

마법사를 완료합니다. 결과적으로 마법사는 다음을 수행합니다.

- Kaspersky Industrial CyberSecurity for Nodes 5.0에 대한 새 정책이 생성됩니다.
  새 정책에는 선택된 Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Endpoint Agent 정책의 설정과 Kaspersky Industrial CyberSecurity for Nodes 5.0에 도입된 새 설정이 포함됩니다. 새 정책의 이름은 변환 전의 Kaspersky Industrial CyberSecurity for Nodes 정책 이름에 “(converted)”가 추가된 것입니다. 새 정책은 *비활성 정책* 상태입니다.
- Kaspersky Industrial CyberSecurity for Nodes 5.0에 대한 새 작업이 생성됩니다.
  새 작업에는 선택된 Kaspersky Industrial CyberSecurity for Nodes 작업의 설정과 Kaspersky Industrial CyberSecurity for Nodes 5.0에 도입된 새 설정이 포함되어 있습니다. 새 작업의 이름은 변환 전의 Kaspersky Industrial CyberSecurity for Nodes 작업 이름에 "(conversion)"가 추가된 것입니다.
- 변환을 위해 선택한 정책 및 작업은 변경되지 않습니다.

마이그레이션 마법사를 사용하여 정책 및 작업 설정을 마이그레이션하는 방법

웹 콘솔 또는 Cloud Console의 메인 창에서 **동작** → **Kaspersky Industrial CyberSecurity for Nodes 5.0.0으로 마이그레이션** 옵션을 선택합니다.

정책 및 작업 마이그레이션 마법사가 열립니다. 마법사의 지침을 따릅니다.

1단계. 정책 마이그레이션

Kaspersky Industrial CyberSecurity for Nodes를 선택하고, 필요하다면 설정을 병합하려는 Kaspersky Endpoint Agent 정책을 선택합니다.

알맞은 정책을 선택했는지 확인하고 다음 단계로 넘어갑니다.

2단계. 정책 마이그레이션

Kaspersky Industrial CyberSecurity for Nodes 5.0를 위해 생성할 Kaspersky Industrial CyberSecurity for Nodes 작업을 선택합니다.

다음 단계로 넘어갑니다.

3단계. 마법사 완료

마법사를 완료합니다. 결과적으로 마법사는 다음을 수행합니다.

- Kaspersky Industrial CyberSecurity for Nodes 5.0에 대한 새 정책이 생성됩니다.

  새 정책은 마이그레이션된 Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Endpoint Agent 정책의 설정과 Kaspersky Industrial CyberSecurity for Nodes 5.0에 도입된 새 설정을 포함합니다. 새 정책 이름은 병합 전의 Kaspersky Industrial CyberSecurity for Nodes 정책 이름에 "KICS에서 복사됨" 문구가 추가된 것입니다. 새 정책은 *비활성 정책* 상태입니다.

- Kaspersky Industrial CyberSecurity for Nodes 5.0에 대한 새 작업이 생성됩니다.

  새 작업에는 마이그레이션된 Kaspersky Industrial CyberSecurity for Nodes 작업의 설정과 Kaspersky Industrial CyberSecurity for Nodes 5.0에 도입된 새 설정이 포함됩니다. 새 작업 이름은 병합 전의 Kaspersky Industrial CyberSecurity for Nodes 작업 이름에 "KICS에서 복사됨" 문구가 추가된 것입니다.

업데이트하는 애플리케이션 버전의 설정 마이그레이션

애플리케이션 및 해당 관리 플러그인을 버전 5.0로 업그레이드 시, 다음은 변경 없이 마이그레이션됩니다.

- 기본값으로 다시 설정되거나 "설정 및 구성 요소 마이그레이션의 제한"에 나열된 설정을 제외한 구성 요소 및 작업 설정
- 작업 로그 및 시스템 감사 로그와 Windows 이벤트 로그의 기록
- 작업 알림 설정
- 작업이 시작되는 사용자 계정

- 애플리케이션 관리를 위한 사용자 접근 권한
- 프록시 서버 연결 암호
- Kaspersky Security Center 정책에서 속성의 상태.

애플리케이션 및 해당 플러그인을 버전 5.0로 업그레이드 시, 새 버전의 애플리케이션에 대해 다음 설정이 초기화되거나 기본값으로 설정됩니다.

- 안티 바이러스 데이터베이스 상태를 포함한 모든 카운터
- 애플리케이션 모듈 및 안티 바이러스 데이터베이스의 설치된 업데이트 관련 데이터
- 작업 상태
- Kaspersky Industrial CyberSecurity for Nodes 서비스 관리에 필요한 사용자 접근 권한
- 레지스트리를 통해 구성되는 애플리케이션 및 작업 설정
- 중요 픽스 설치 중에 변경된 애플리케이션 및 작업 설정
- 이벤트 구성
- Kaspersky Security Center 중앙 관리 서버로의 데이터 전송 설정: 기본적으로 모든 데이터 전송이 활성화됩니다
- 추적 및 덤프 설정
- **알림** 탭의 애플리케이션 로컬 작업 설정.

업데이트하는 애플리케이션 버전에 없는 설정은 기본값이 설정됩니다.

설정 및 구성 요소 마이그레이션의 제한 사항

- 업그레이드 중인 버전의 격리 저장소 콘텐츠는 백업 버전 5.0로 이동됩니다. 업그레이드 후 백업 저장소의 최대 크기는 업그레이드되는 애플리케이션의 백업 및 격리 저장소의 최대 크기를 합한 값으로 설정됩니다. 사용 가능한 공간 한도 역시 이에 맞게 업데이트됩니다. 동시에, 백업 저장소의 최대 기본 크기가 400MB로 증가하고 사용 가능한 공간 한도가 100MB로 증가합니다.
- Kaspersky Industrial CyberSecurity for Nodes 4.0 설정 **격리 저장소 폴더**, **백업 폴더**, **개체 복구용 폴더**는 Kaspersky Industrial CyberSecurity for Nodes 4.5 이상에는 존재하지 않으므로 마이그레이션되지 않습니다. 이전 버전에는 있지만 새 버전에는 없는 다른 설정도 마이그레이션되지 않습니다.
- [KICS+KEA] 구성을 [KICS+내장 에이전트]로 마이그레이션할 시, Kaspersky Endpoint Agent 격리 저장소의 콘텐츠는 Kaspersky Industrial CyberSecurity for Nodes 5.0 격리 저장소로 마이그레이션됩니다.
- 클라이언트 컴퓨터의 차단된 네트워크 세션 목록은 마이그레이션되지 않습니다. 동시에, 차단된 네트워크 파일 리소스에 대한 접근 자동 차단 해제 설정은 애플리케이션 업그레이드 후에도 변경되지 않습니다.
- 암호 보호 설정은 마이그레이션되지 않습니다. Kaspersky Industrial CyberSecurity for Nodes 4.5에서는 암호 보호가 대대적으로 바뀌었습니다. 필요한 경우 암호 보호를 켜고 암호를 설정합니다.

- 신뢰 구역
  - Kaspersky Industrial CyberSecurity for Nodes 5.0에서 신뢰 구역 개체를 선택하는 방법이 변경되었습니다. 개별 파일이나 파일 또는 폴더 경로로 정의된 예외를 마이그레이션할 수 있습니다. 사전 정의된 범위(예: 하드 드라이브)나 스크립트 URL로 정의된 예외는 마이그레이션되지 않습니다. 마이그레이션 후에는 이러한 예외를 수동으로 추가해야 합니다.
  - 신뢰 구역에 서버의 애플리케이션 설정과 해당 애플리케이션 및 산업용 소프트웨어의 상호 작용을 돕는 사전 정의된 검사 예외 및 신뢰하는 애플리케이션이 추가되었습니다.
- 애플리케이션 실행 제어 및 장치 제어 구성 요소가 대폭 개편되었습니다. 업그레이드 중인 버전의 구성 요소 설정은 Kaspersky Industrial CyberSecurity for Nodes 5.0의 새 설정 구조를 고려하여 마이그레이션됩니다. 따라서 애플리케이션 설정을 저장하려면 중앙 관리 서버에 더 많은 공간이 필요할 수 있습니다.
- 업그레이드되는 애플리케이션 버전의 파일 무결성 모니터와 레지스트리 접근 모니터링 구성 요소의 설정은 시스템 무결성 모니터링 구성 요소의 설정으로 마이그레이션됩니다.
- 방화벽 관리 구성 요소가 방화벽 구성 요소로 개편되었으며, 이 구성 요소는 이제 Windows 방화벽에 접속하는 것 외에 방화벽의 기능도 수행합니다. 마이그레이션을 완료한 후 처음부터 구성 요소 모드를 구성해야 합니다.
- KSN을 사용하려면 KSN 진술문을 다시 읽고 수락해야 합니다.
- 4.5 버전 이상의 애플리케이션은 개별 구성 요소의 스케줄을 지원하지 않습니다. 이 구성 요소를 활성화하면 애플리케이션이 실행되는 동안 계속 실행됩니다.
- 작업을 마이그레이션할 때, 작업의 스케줄된 시작 시각은 마이그레이션이 수행되는 컴퓨터의 OS 설정에서 구성한 시간대와 일치하는 시간만큼 상쇄됩니다. 예를 들어 이전 버전의 애플리케이션에서 작업의 시작 시각이 7:00이고 운영 체제에 구성된 시간대가 UTC +3:00이라고 가정합니다. 그러면 작업 마이그레이션 후 시작 시각이 10:00으로 변경됩니다.
- 실시간 파일 보호 구성 요소와 온디맨드 검사 작업의 설정에서 감염 의심 개체에 수행할 처리 방법 설정 섹션이 제거되었습니다. 이러한 설정은 최신 애플리케이션 버전으로 마이그레이션되지 않습니다.
- 4.5 버전 이상의 애플리케이션을 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 솔루션의 일부로 사용할 시, 경고 세부 정보를 관리하려면 Endpoint Detection and Response의 웹 플러그인을 버전 15.1 이상으로 업그레이드해야 합니다. 또는 Kaspersky Endpoint Agent 웹 플러그인을 설치했다면 이 웹 플러그인으로 열리는 보안위협 개발 체인의 인시던트 카드에 제한된 데이터 또는 오류가 포함될 수 있습니다.
- 애플리케이션을 버전 4.0 이하에서 4.5 이상으로 업그레이드한 후에 격리 저장소 및 백업 저장소의 개체를 마이그레이션했거나, Kaspersky Anti Targeted Attack Platform 또는 Kaspersky Industrial CyberSecurity for Networks 시나리오에 따라 해당 개체를 저장소에 넣었다면, 분석을 위해 이 개체를 Kaspersky로 보낼 때 Kaspersky Security Center 웹 콘솔이나 관리 콘솔을 사용할 수 없습니다.
- 주문형 검사 작업을 마이그레이션할 때 사전 정의된 검사 범위에 대한 기본 보안 수준이 *알림*에서 *사용자 지정*으로 변경됩니다.
- SIEM에 전송된 이벤트는 이제 새로운 날짜 및 시간 형식을 사용합니다. Kaspersky Industrial CyberSecurity for Nodes의 이전 버전에서는 이벤트가 타임스탬프와 함께 생성되었습니다. 이제 애플리케이션은 `<DATE-TIME>` 형식의 날짜와 시간으로 이벤트를 생성합니다. 필요한 경우 날짜와 시간이 타임스탬프 형식으로 변환되도록 SIEM 상호 작용을 재구성합니다.
- Kaspersky Industrial CyberSecurity for Nodes를 로컬 업그레이드할 때 이전에 설치에 포함된 구성 요소를 설치하지 않으면 해당 구성 요소의 설정이 유지되지 않습니다. 이후에 이 구성 요소를 설치하면 기본 설정이 적용됩니다.

Kaspersky Industrial CyberSecurity for Nodes 버전 4.0 및 5.0의 구성 요소 및 작업에 대한 대응

Kaspersky Industrial CyberSecurity for Nodes 4.0을 버전 5.0로 업그레이드하면, 애플리케이션이 로컬로 설치된 경우에만 구성 요소 및 작업 세트가 마이그레이션됩니다.

Kaspersky Industrial CyberSecurity for Nodes 버전 4.0 및 5.0의 구성 요소에 대한 대응

Kaspersky Industrial CyberSecurity for Nodes 4.0의 구성 요소	Kaspersky Industrial CyberSecurity for Nodes 5.0의 구성 요소
신뢰 구역	신뢰 구역
실시간 파일 보호	실시간 파일 보호
KSN 사용	KSN 사용
익스플로잇 방지	익스플로잇 방지
네트워크 위협 보호	네트워크 위협 보호
AMSI 스캐너	AMSI 스캐너
애플리케이션 실행 제어	애플리케이션 실행 제어
장치 제어	장치 제어
Wi-Fi 제어	장치 제어 the Wi-Fi 제어 구성 요소의 기능이 장치 제어 구성 요소에 병합되었습니다.
방화벽 관리	방화벽 Windows 방화벽은 Kaspersky Industrial CyberSecurity for Nodes 4.0의 방화벽 역할을 하며, 애플리케이션에서 Windows 방화벽을 관리합니다. Kaspersky Industrial CyberSecurity for Nodes 5.0에서는 별도의 구성 요소가 방화벽 기능을 담당합니다.
Anti-Cryptor	Anti-Cryptor
파일 무결성 모니터	시스템 무결성 모니터링 파일 무결성 모니터와 레지스트리 접근 모니터링 구성 요소의 기능이 시스템 무결성 모니터링 구성 요소에 병합되었습니다.
로그 검사	로그 검사
레지스트리 접근 모니터링	시스템 무결성 모니터링 파일 무결성 모니터와 레지스트리 접근 모니터링 구성 요소의 기능이 시스템 무결성 모니터링 구성 요소에 병합되었습니다.
휴대용 스캐너	Portable Auditor
(없음)	복원 엔진
(없음)	KICS for Networks와 통합 Kaspersky Endpoint Agent 역할을 하는 구성 요소.
(없음)	SIEM 통합 Kaspersky Endpoint Agent 역할을 하는 구성 요소.
(없음)	Managed Detection and Response(Industrial CyberSecurity) Kaspersky Endpoint Agent 역할을 하는 구성 요소.
(없음)	Endpoint Detection and Response Expert(on-premises) Kaspersky Endpoint Agent 역할을 하는 구성 요소.
(없음)	Endpoint Detection and Response(Industrial CyberSecurity)
(없음)	Sigma 규칙을 사용한 이상 행위 탐지 Kaspersky Endpoint Agent 역할을 하는 구성 요소.

Kaspersky Industrial CyberSecurity for Nodes 4.0의 구성 요소	Kaspersky Industrial CyberSecurity for Nodes 5.0의 구성 요소
Kaspersky Industrial CyberSecurity for Nodes 4.0의 작업	**Kaspersky Industrial CyberSecurity for Nodes 5.0의 작업**
애플리케이션 활성화	애플리케이션 활성화
업데이트 복사	업데이트 업데이트 복사 작업의 기능이 업데이트 작업에 병합되었습니다.
베이스라인 파일 무결성 모니터	베이스라인 시스템 무결성 모니터
데이터베이스 업데이트	업데이트 데이터베이스 업데이트 작업의 기능이 업데이트 작업에 병합되었습니다.
소프트웨어 모듈 업데이트	업데이트 소프트웨어 모듈 업데이트 작업의 기능이 업데이트 작업에 병합되었습니다.
애플리케이션 데이터베이스 업데이트 롤백	업데이트 롤백
온디맨드 검사	온디맨드 검사
애플리케이션 무결성 제어	애플리케이션 무결성 제어
애플리케이션 실행 제어를 위한 규칙 생성기	애플리케이션 실행 제어를 위한 규칙 생성기
장치 제어를 위한 규칙 생성기	장치 제어를 위한 규칙 생성기
(없음)	중앙 관리 서버 연결 보호
(없음)	Kaspersky Industrial CyberSecurity for Nodes 구성 요소 변경
(없음)	보안 감사 Kaspersky Endpoint Agent 기능을 구현하는 작업입니다.
(없음)	프로세스 종료 Kaspersky Endpoint Agent 기능을 구현하는 작업입니다.
(없음)	프로세스 시작 Kaspersky Endpoint Agent 기능을 구현하는 작업입니다.
(없음)	IOC 검사 Kaspersky Endpoint Agent 기능을 구현하는 작업입니다.
(없음)	파일 가져오기 Kaspersky Endpoint Agent 기능을 구현하는 작업입니다.
(없음)	격리 저장소로 파일 이동 Kaspersky Endpoint Agent 기능을 구현하는 작업입니다.
(없음)	파일 삭제 Kaspersky Endpoint Agent 기능을 구현하는 작업입니다.

Kaspersky Security Gateway 설치 및 제거

이 섹션에서는 Kaspersky Security Gateway 설치 및 제거 지침을 제공합니다.

Kaspersky Security Gateway 업데이트

Kaspersky Security Gateway 업데이트는 설치된 애플리케이션 버전 위에 새 버전을 설치하는 방식으로 수행되며 다시 시작할 필요가 없습니다.

Kaspersky Security Gateway를 버전 5.0로 업그레이드하면 이전에 설치한 애플리케이션 버전이 자동으로 삭제됩니다.

이전에 설치된 Kaspersky Security Gateway 버전의 설정 값이 변경되지 않고 Kaspersky Security Gateway 5.0로 전송됩니다.

Kaspersky Security Gateway를 4.5 이하 버전에서 5.0으로 업데이트하면 추적 파일 로그 기록이 중지됩니다. 필요하다면 다시 추적 파일 로그 기록을 구성합니다.

설치 마법사를 사용하여 Kaspersky Security Gateway 설치

Kaspersky Security Gateway를 설치하려면

배포 키트에 포함된 Security_gateway.msi 파일을 실행합니다.

해당 마법사가 설치 과정을 안내합니다. 마법사의 지침을 따릅니다.

Kaspersky Security Gateway 설치 마법사의 인터페이스는 일련의 창(단계)으로 구성됩니다. 설치 마법사 창 간에 이동하려면 **< 뒤로** 그리고 **다음 >** 버튼을 사용하십시오. 완료 후 설치 마법사를 닫으려면 **마침** 버튼을 클릭합니다. 설치 프로세스의 모든 단계에서 설치 마법사를 종료하려면 **취소** 버튼을 클릭합니다.

1단계. 설치 요구 사항 확인

탐지된 애플리케이션 중 Kaspersky Security Gateway 이전 버전이 있는 경우 설치 마법사가 이전 버전을 자동으로 제거하고 새 버전의 Kaspersky Security Gateway를 설치합니다.

Kaspersky Security Gateway 2.0 또는 이전 버전을 설치한 경우 설치 마법사는 이전 버전을 제거하지 않으며 설치를 취소합니다. Kaspersky Security Gateway 5.0를 설치하기 전에 Kaspersky Security Gateway 2.0 또는 이전 버전을 수동으로 제거하십시오.

Kaspersky Security Gateway를 설치하거나 업그레이드하기 전에 설치 마법사는 다음 요구 사항이 충족되는지 확인합니다:

- 컴퓨터와 설치된 소프트웨어가 하드웨어 및 소프트웨어 요구 사항을 충족합니다.
- 사용자 계정에는 애플리케이션을 설치하는 데 필요한 권한이 있습니다.

위의 요구 사항 중 어느 하나라도 충족되지 않으면 화면에 관련 알림 정보가 표시되며 설치 과정이 중단됩니다.

2단계. 설치 절차의 시작 페이지

Kaspersky Security Gateway를 설치하는 컴퓨터가 하드웨어 및 소프트웨어 요구 사항을 완전히 충족하면 설치 프로세스의 시작 페이지가 열립니다. 시작 페이지는 컴퓨터에 Kaspersky Security Gateway 설치가 시작되었음을 알립니다.

마법사의 다음 단계를 진행하십시오.

3단계. 최종 사용자 라이센스 계약서 및 개인정보취급방침 보기

이 단계에서 Kaspersky 최종 사용자 라이센스 계약서와 개인정보취급방침을 읽어야 합니다.

최종 사용자 라이센스 계약서와 개인정보취급방침의 약관에 동의하면 **I accept the terms of the End User License Agreement** 및 **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy** 확인란을 선택합니다.

최종 사용자 라이센스 계약서 또는 개인정보취급방침에 동의하지 않으면 설치가 중단됩니다.

마법사의 다음 단계를 진행하십시오.

4단계. 대상 폴더 선택

이 단계에서는 Kaspersky Security Gateway를 설치할 대상 폴더의 경로를 지정해야 합니다. 대상 폴더를 선택하려면 **찾아보기** 버튼을 클릭합니다.

마법사의 다음 단계를 진행하십시오.

5단계. 구성 요소 선택

이 단계에서 설치할 Kaspersky Security Gateway 구성 요소를 선택할 수 있습니다. 기본적으로 모든 구성 요소가 설치를 위해 선택되어 있습니다.

설치할 구성 요소를 선택하려면 구성 요소 이름 옆의 아이콘을 클릭해 마우스 오른쪽 메뉴를 엽니다. 그런 다음 **Feature will be installed on the local hard drive** 또는 **Entire feature and its subfeatures will be installed on local hard drive** 옵션을 선택합니다. 선택한 구성 요소가 수행하는 작업 및 구성 요소를 설치하는 데 필요한 디스크 공간에 관한 자세한 내용은 현재 설치 마법사 페이지 하단을 참조하십시오.

로컬 하드 드라이브의 사용 가능한 공간에 관한 자세한 정보를 보려면 **Volume** 버튼을 클릭합니다. **Disk Space Requirements** 창이 열리면 정보가 표시됩니다.

구성 요소 설치를 취소하려면 마우스 오른쪽 메뉴에서 **Feature will be unavailable** 옵션을 선택합니다.

기본적으로 설치되는 구성 요소 목록으로 돌아가려면 **초기화** 버튼을 클릭합니다.

마법사의 다음 단계를 진행하십시오.

6단계. SCADA 시스템에 대한 연결 구성

이 단계에서는 SCADA 연결 설정을 지정해야 합니다.

- IEC 60870-5-104 연결: Kaspersky Security Gateway를 설치할 컴퓨터의 주소(1부터 65535까지의 숫자) 및 TCP 포트(1부터 65535까지의 숫자).
- OPC UA 연결: Kaspersky Security Gateway를 설치할 컴퓨터의 TCP 포트(1부터 65535까지의 숫자).

프로그램을 설치하려면 **설치** 버튼을 클릭합니다.

컴퓨터에 Kaspersky Security Gateway를 설치하는 동안 현재 네트워크 연결이 종료될 수 있습니다. 종료된 연결은 대부분 잠시 후에 복원됩니다.

7단계. Kaspersky Security Gateway 설치

설치 마법사가 Kaspersky Security Gateway 파일을 컴퓨터로 복사합니다. 설치가 완료될 때까지 기다리십시오.

마법사를 완료합니다.

명령줄에서 Kaspersky Security Gateway 설치

명령줄에서 Kaspersky Security Gateway를 설치하려면 다음 명령을 실행합니다:

```
msiexec /i security_gateway.msi EULA=1 PRIVACYPOLICY=1 /qn
```

`EULA=1 PRIVACYPOLICY=1` – 사용자와 Kaspersky 간의 Kaspersky Security Gateway 최종 사용자 라이센스 계약서와 데이터 처리 및 전송을 설명하는 개인정보취급방침의 조항에 동의하십시오.

파라미터를 1로 설정하여 다음을 확인하십시오:

- 사용자는 최종 사용자 라이센스 계약서의 약관을 완전히 읽고 이해했으며 이에 동의합니다.
- 사용자는 개인정보취급방침을 완전히 읽고 이해했습니다. 사용자는 개인정보취급방침에 설명된 대로 자신의 데이터가 처리 및 전송(제삼국 포함)된다는 것을 인식하고 동의합니다.

Kaspersky Security Gateway를 설치하려면 최종 사용자 라이센스 계약서와 개인정보취급방침에 반드시 동의해야 합니다.

최종 사용자 라이센스 계약서 및 개인정보취급방침 텍스트는 배포 키트에 포함되어 있습니다.

Kaspersky Security Gateway 제거

Kaspersky Security Gateway를 제거하려면 관리자 계정 권한이 필요합니다.

Kaspersky Security Gateway를 제거하려면:

1. Microsoft Windows 제어판을 엽니다.
2. Microsoft Windows 제어판에서 **프로그램 및 기능** 아이콘을 클릭합니다.
   Microsoft Windows에서 **프로그램 제거 또는 변경** 창이 열립니다.
3. **프로그램 제거 또는 변경** 창에서 **Kaspersky Security Gateway**를 선택하고 **변경** 버튼을 클릭합니다.
   설치 마법사가 시작됩니다.
4. 설치 마법사의 **Modify, Repair, or Remove application** 창에서 **Remove** 버튼을 클릭합니다.

   설치 마법사가 제거 설정을 구성하라는 메시지를 표시합니다. 마법사의 지침을 따릅니다.

1단계. 나중에 사용하기 위해 Kaspersky Security Gateway 데이터 저장

이 단계에서 설치 마법사는 나중에 Kaspersky Security Gateway를 설치할 때(예: 새 버전 설치 시) 사용할 수 있도록 Kaspersky Security Gateway 구성 파일을 저장하라는 메시지를 표시합니다.

Kaspersky Security Gateway 구성 파일을 저장하려면,

Save application configuration file 확인란을 선택합니다.

Save application configuration file 옵션은 제어판의 **프로그램 및 기능** 섹션에 있는 **변경** 버튼을 클릭해 설치 마법사를 실행한 경우에만 이용할 수 있습니다.

마법사의 다음 단계를 진행하십시오.

2단계. Kaspersky Security Gateway 제거

이 단계에서 설치 마법사는 컴퓨터에서 Kaspersky Security Gateway를 제거합니다. 제거 프로세스가 완료될 때까지 기다리십시오.

마법사를 완료합니다.

Kaspersky Security Gateway를 제거할 때 운영 체제를 다시 시작해야 할 수 있습니다. 즉시 다시 시작하지 않기로 할 시 운영 체제를 다시 시작하거나 컴퓨터를 껐다가 다시 켤 때까지 Kaspersky Security Gateway 제거가 완료되지 않습니다.

OPC Core Components Redistributables 설치

Kaspersky Industrial CyberSecurity for Nodes 5.0 버전부터 OPC Core Components Redistributables 패키지는 Kaspersky Security Gateway 설치 패키지에 포함되지 않습니다.

데이터 전송에 OPC DA 프로토콜을 사용하려는 경우 Kaspersky Security Gateway 5.0 이상을 설치하거나 애플리케이션을 업그레이드할 때 다른 애플리케이션에서 OPC Core Components Redistributables 패키지를 설치하지 않았다면 이 패키지를 직접 설치해야 합니다. 배포 키트에 포함된 opc_redist.msi 파일을 사용할 수 있습니다.

Kaspersky Security Gateway를 설치한 후 OPC Core Components Redistributables를 설치한 경우 Kaspersky Security Gateway OPC 서비스를 다시 시작해야 합니다.

애플리케이션 인터페이스

다음 인터페이스를 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 제어할 수 있습니다:

- 애플리케이션 콘솔.
- Kaspersky Security Center 관리 콘솔
- Kaspersky Security Center 웹 콘솔

Kaspersky Security Center 관리 콘솔

Kaspersky Security Center는 원격에서 Kaspersky Industrial CyberSecurity for Nodes의 설치, 제거, 시작, 중지와 이용 가능한 애플리케이션 구성 요소 세트의 변경, 애플리케이션 설정 구성, 키 추가, 업데이트 및 검사 작업 시작/중지 등을 할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 관리 플러그인을 사용하여 Kaspersky Security Center를 통해 애플리케이션을 관리할 수 있습니다. Kaspersky Security Center 도움말에서 Kaspersky Security Center 인터페이스 관련 상세 정보를 참조하십시오.

Kaspersky Security Center 웹 콘솔

Kaspersky Security Center 웹 콘솔(이하 웹 콘솔로도 지칭함)은 조직 네트워크의 보안 시스템을 유지 및 관리하기 위한 주요 작업을 중앙에서 수행하는 데 사용할 수 있는 웹 애플리케이션입니다. Kaspersky Security Center 웹 콘솔은 사용자 인터페이스를 제공하는 Kaspersky Security Center 구성 요소입니다. Kaspersky Security Center 웹 콘솔에 대한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.

웹 콘솔에서 다음 동작을 수행할 수 있습니다:

- 조직의 보안 시스템 상태 감시
- 네트워크 내의 장치에 Kaspersky 애플리케이션 설치
- 설치한 애플리케이션 관리
- 보안 시스템 상태에 대한 리포트 보기

관리 플러그인 작업

이 섹션에서는 Kaspersky Industrial CyberSecurity for Nodes 관리 플러그인에 대한 정보를 제공하고, 보호 중인 장치 또는 보호 중인 장치 그룹에 설치된 애플리케이션을 관리하는 방법을 설명합니다.

Kaspersky Security Center에서 Kaspersky Industrial CyberSecurity for Nodes 관리

Kaspersky Industrial CyberSecurity for Nodes가 설치되어 있고 Kaspersky Industrial CyberSecurity for Nodes 관리 플러그인으로 같은 관리 그룹에 가입된 여러 보호 중인 장치를 중앙에서 관리할 수 있습니다. 또한 Kaspersky Security Center로 관리 그룹에 포함된 각 보호 중인 장치의 설정을 별도로 구성할 수 있습니다.

*관리 그룹*은 Kaspersky Security Center를 통해 직접 생성합니다. 이 그룹에는 Kaspersky Industrial CyberSecurity for Nodes가 설치된 장치가 여러 대 있어, 제어 및 보호 설정을 같게 구성할 수 있습니다. 관리 그룹 사용에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

보호 중인 장치의 Kaspersky Industrial CyberSecurity for Nodes 작업이 활성 Kaspersky Security Center 정책으로 제어된다면, 단일 보호 중인 장치에 대한 애플리케이션 설정을 사용할 수 없습니다.

Kaspersky Security Center에서 Kaspersky Industrial CyberSecurity for Nodes 관리 플러그인을 시작하기 위해 추가 작업은 필요하지 않습니다. 보호 중인 관리자의 장치에 관리 플러그인을 설치하면 모든 유형의 Kaspersky Security Center 관리 콘솔과 함께 시작합니다.

Kaspersky Industrial CyberSecurity for Nodes는 다음과 같은 방법으로 Kaspersky Security Center에서 관리할 수 있습니다.

- **Kaspersky Security Center 정책 사용**. Kaspersky Security Center 정책은 장치 그룹에 대해 같은 보호 설정을 원격 구성하는 데 사용할 수 있습니다. 활성 정책에서 지정된 작업 설정은 애플리케이션 콘솔에서 로컬로 구성된 설정 또는 Kaspersky Security Center의 **속성: <보호 중인 장치 이름>** 창에서 원격 구성된 작업 설정보다 우선합니다.

  정책을 사용하여 일반 애플리케이션 설정, 실시간 컴퓨터 보호 작업 설정, 장치의 활동 제어 작업, 네트워크 저장소 보호 작업, 스케줄에 따른 로컬 시스템 작업 시작 설정을 구성할 수 있습니다.

- **Kaspersky Security Center 그룹 작업 사용**. Kaspersky Security Center 그룹 작업을 통해 장치 그룹에 대해 만료 기간이 있는 작업의 공통 설정을 원격 구성할 수 있습니다.

  그룹을 사용하여 애플리케이션을 활성화하고, 온디맨드 검사 작업 설정을 구성하고 작업 설정 및 애플리케이션 실행 제어를 위한 규칙 생성기을 업데이트할 수 있습니다.

- **장치 세트에 작업 사용**. 장치 세트에 대한 작업을 사용하면, 관리 그룹에 속하지 않은 보호 중인 장치에 대해 실행 기간이 정해진 일반 작업 설정을 원격 구성할 수 있습니다.

- **단일 장치의 속성 창 사용**. **속성:<보호 중인 장치 이름>** 창에서 관리 그룹에 포함된 개별 보호 중인 장치에 대한 작업 설정을 원격 구성할 수 있습니다. 선택한 보호 중인 장치가 활성 Kaspersky Security Center 정책으로 제어되지 않는다면, 일반 애플리케이션 설정 및 Kaspersky Industrial CyberSecurity for Nodes 작업 전체의 설정을 모두 구성할 수 있습니다.

애플리케이션 설정 관리

이 섹션에는 Kaspersky Security Center 관리 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 일반 설정을 구성하는 방법에 관한 정보가 포함되어 있습니다.

Kaspersky Security Center에서 일반 애플리케이션 설정 구성

Kaspersky Security Center에서 보호 중인 장치 그룹 또는 보호 중인 장치 1대를 대상으로 Kaspersky Industrial CyberSecurity for Nodes 일반 설정을 구성할 수 있습니다.

Kaspersky Security Center에서 인터페이스 및 검사 설정 구성

확장성 설정 및 애플리케이션 인터페이스를 구성하려면:

1. Kaspersky Security Center 관리 콘솔 트리의 **관리 중인 기기** 노드를 확장합니다.
2. 애플리케이션 설정을 구성할 관리 그룹을 선택합니다.
3. 선택한 관리 그룹의 세부 정보 창에서 다음 동작 중 하나를 수행합니다.
   - 보호 중인 장치 그룹에 대한 애플리케이션 설정을 구성하려면 **정책** 탭을 선택하고 **속성: <정책 이름>** 창을 엽니다.
   - 개별 보호 중인 장치에 대한 작업 또는 애플리케이션의 설정을 구성하려면 **기기** 탭을 선택하고 로컬 작업 설정 또는 애플리케이션 설정으로 갑니다.
4. **애플리케이션 설정** 섹션에서 **인터페이스 설정** 하위 섹션의 **설정** 버튼을 클릭합니다.
5. **인터페이스 설정** 창의 **일반** 탭에서 다음 설정을 구성합니다.
   - **사용자와의 상호 작용** 섹션에서 애플리케이션이 시작할 때마다 작업 표시줄에 시스템 상자 아이콘을 표시할지 구성합니다.
     - **사용자 인터페이스 표시**. 클라이언트 컴퓨터의 Windows 트레이에서 아이콘을 사용할 수 있습니다. 아이콘의 마우스 오른쪽 메뉴에서 사용자는 Kaspersky Industrial CyberSecurity for Nodes로 작업을 수행할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes에서도 애플리케이션 아이콘 위에 알림을 표시합니다. Windows 시스템 트레이에 있는 아이콘의 마우스 오른쪽 메뉴를 사용하여 간편 진단 인터페이스를 열 수 있습니다. 간편 진단 인터페이스의 링크를 클릭하면 애플리케이션 콘솔이 열립니다.
     - **사용자 인터페이스 표시 안 함**. 클라이언트 컴퓨터에 Kaspersky Industrial CyberSecurity for Nodes 동작의 어떤 징후도 표시되지 않습니다. Windows 알림 영역의 아이콘과 알림을 사용할 수 없습니다.
   - **상태** 섹션에서 Kaspersky Industrial CyberSecurity for Nodes 시스템 트레이 아이콘에 표시할 경고를 지정할 수 있습니다.
6. **확인**을 누릅니다.

구성된 애플리케이션 설정이 저장됩니다.

Kaspersky Security Center에서 보안 설정 구성

보안 설정을 직접 구성하려면:

1. Kaspersky Security Center 관리 콘솔 트리의 **관리 중인 기기** 노드를 확장합니다.
2. 애플리케이션 설정을 구성할 관리 그룹을 선택합니다.
3. 선택한 관리 그룹의 세부 정보 창에서 다음 동작 중 하나를 수행합니다.
   - 보호 중인 장치 그룹에 대한 애플리케이션 설정을 구성하려면 **정책** 탭을 선택하고 **속성: <정책 이름>** 창을 엽니다.
   - 개별 보호 중인 장치에 대한 작업 또는 애플리케이션의 설정을 구성하려면 **기기** 탭을 선택하고 로컬 작업 설정 또는 애플리케이션 설정으로 갑니다.
4. **애플리케이션 설정** 섹션에서 **보안 및 신뢰성** 하위 섹션의 **설정** 버튼을 클릭합니다.
5. **보안 설정** 창의 **보안** 탭에서 다음 설정을 구성합니다.
   - **일반** 섹션에서 **컴퓨터 시작 시 애플리케이션 시작(권장)** 기능을 활성화(기본값) 상태로 둘 것을 권장합니다.
   - **자기 보호** 섹션에서 **외부 위협으로부터 애플리케이션 프로세스 보호** 기능을 활성화하거나 비활성화합니다.
   - **UPS 백업 전원으로 전환 시 동작** 섹션에서 UPS 전원으로 전환한 후 Kaspersky Industrial CyberSecurity for Nodes에서 생성하는 보호 중인 장치 부하에 대한 제한을 지정합니다.
     - **스케줄 지정된 검사 작업 시작 안 함**
     - **실행 중인 검사 작업 중단**
   - **설정 적용 시 컴퓨터 상태** 섹션에서 정책을 적용하거나 작업을 실행할 때 오류가 발생할 경우 애플리케이션이 설치된 클라이언트 컴퓨터의 상태 표시를 구성합니다.
   - **호환성 설정** 섹션에서 **원격 관리 소프트웨어와의 호환성** 설정을 구성합니다.

6. **검사 설정** 탭에서 다음 설정을 구성합니다:

   - **검사 작업을 위한 CPU 사용량 제한**. Kaspersky Industrial CyberSecurity for Nodes는 온디맨드 검사 작업 중 보호 중인 장치의 CPU 사용을 **상한** 필드에 지정된 값으로 제한합니다. 이 옵션을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes의 성능에 부정적인 영향을 미칠 수 있습니다.

   - **다른 애플리케이션에 컴퓨터 리소스 우선권 할당**. 컴퓨터 검사 시 Kaspersky Industrial CyberSecurity for Nodes의 컴퓨터 리소스 사용으로 CPU 및 하드 드라이브 서브시스템의 로드가 증가할 수 있습니다. 이렇게 되면 기타 애플리케이션의 속도가 저하될 수 있습니다. 성능을 최적화하기 위해 Kaspersky Industrial CyberSecurity for Nodes는 기타 애플리케이션으로 리소스를 전송하는 모드를 제공합니다. 이 모드에서는 CPU 로드가 높아지면 운영 체제에서 Kaspersky Industrial CyberSecurity for Nodes 검사 작업의 우선순위를 낮출 수 있습니다. 이 방법을 통해 운영 체제가 리소스를 기타 애플리케이션에 재분배할 수 있습니다. 따라서 검사 작업은 CPU 시간이 줄어듭니다. 결과적으로 Kaspersky Industrial CyberSecurity for Nodes가 컴퓨터를 검사하는 시간이 길어집니다. 기본적으로 이 애플리케이션은 컴퓨터 리소스 우선권을 다른 애플리케이션에 할당하도록 구성됩니다.

7. **확인** 버튼을 클릭합니다.

보안 및 신뢰성 설정이 저장됩니다.

Kaspersky Security Center를 사용하여 연결 설정 구성

구성된 연결 설정은 애플리케이션을 Kaspersky Security Network 서비스와 통합하는 중에, 그리고 Kaspersky Industrial CyberSecurity for Nodes를 업데이트 및 활성 서버에 연결하는 데 사용됩니다.

연결 설정을 구성하려면 다음 단계를 수행합니다.

1. Kaspersky Security Center 관리 콘솔 트리의 **관리 중인 기기** 노드를 확장합니다.

2. 애플리케이션 설정을 구성할 관리 그룹을 선택합니다.

3. 선택한 관리 그룹의 세부 정보 창에서 다음 동작 중 하나를 수행합니다.

   - 보호 중인 장치 그룹에 대한 애플리케이션 설정을 구성하려면 **정책** 탭을 선택하고 **속성: <정책 이름>** 창을 엽니다.

   - 개별 보호 중인 장치에 대한 작업 또는 애플리케이션의 설정을 구성하려면 **기기** 탭을 선택하고 로컬 작업 설정 또는 애플리케이션 설정으로 갑니다.

4. **애플리케이션 설정** 섹션에서 **연결 설정** 하위 섹션의 **설정** 버튼을 클릭합니다.
   연결 설정 창이 열립니다.

5. **프록시 서버** 섹션에서 **설정** 버튼을 클릭합니다.

6. 창이 열리면 **프록시 서버 설정** 섹션에서 프록시 설정 관리 옵션을 선택합니다.

   - **프록시 서버 사용 안 함**. 이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 프록시 서버를 사용하지 않습니다.

   - **프록시 서버 설정 자동 탐지.** 이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 운영 체제의 프록시 설정을 사용합니다.

- **지정한 프록시 서버 설정 사용**. 이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes는 수동으로 지정한 프록시 서버 설정을 사용합니다. 프록시 서버의 IP 주소 또는 기호 이름 및 포트 번호를 입력합니다

  필요하다면 **로컬 주소에 대해 프록시 서버 우회** 확인란을 선택 해제합니다. 이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 설치된 보호 중인 장치를 호스팅하는 네트워크에서 직접 장치에 접근합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

7. **프록시 서버 인증 설정** 섹션의 드롭다운 목록에서 프록시 서버에서의 인증 방법을 선택합니다.

   a. **프록시 서버 설정 자동 탐지**를 선택한 경우:

   - **인증 사용하지 않음**.
   - **NTLM 인증**. 현재 사용자 계정을 사용한 NTLM 인증(기본값).
   - **Kerberos 인증**. 현재 사용자 계정을 사용한 Kerberos 인증.

   b. **지정한 프록시 서버 설정 사용**를 선택한 경우:

   - **인증 사용하지 않음**.
   - **NTLM 인증**. 현재 사용자 계정을 사용한 NTLM 인증(기본값).
   - **사용자 이름 및 암호를 사용한 NTLM 인증**. 직접 지정한 자격 증명을 사용한 NTLM 인증.
   - **Kerberos 인증**. 현재 사용자 계정을 사용한 Kerberos 인증.

     > 프록시 서버 주소로 CNAME 레코드를 사용할 때 Kerberos 인증이 올바르게 작동하도록 하려면 각 CNAME 레코드에 대해 SPN(서비스 사용자 이름)을 등록해야 합니다.

   - **사용자 이름 및 암호를 사용한 Kerberos 인증**. 직접 지정한 자격 증명을 사용한 Kerberos 인증.
   - **사용자 이름 및 암호**. 직접 지정한 자격 증명을 사용한 인증.

   필요하다면 사용자 이름과 암호를 입력합니다.

   Kerberos 인증을 선택한 경우, 프록시 서버 설정에 따라 Kaspersky Industrial CyberSecurity for Nodes는 Kerberos 또는 NTLM 프로토콜을 사용하여 인증을 수행합니다.

8. **라이센스** 섹션에서 **애플리케이션을 활성화할 때 Kaspersky Security Center를 프록시 서버로 사용** 확인란을 선택하거나 선택 해제합니다.

9. **확인** 버튼을 클릭합니다.

10. **모니터링하는 포트** 섹션에서 네트워크 포트 옵션을 지정합니다.

- **모든 네트워크 포트 모니터**. 이 네트워크 포트 모니터링 모드에서는 보호 구성 요소가 컴퓨터의 열린 네트워크 포트를 통해 전송되는 데이터 스트림을 감시합니다.
- **선택한 네트워크 포트만 모니터**. 이 네트워크 포트 모니터링 모드에서 보호 구성 요소는 컴퓨터의 선택된 포트와 선택한 애플리케이션의 네트워크 활동을 모니터링합니다. 이메일 및 네트워크 트래픽의 전송에 일반적으로 사용되는 네트워크 포트 목록은 Kaspersky 전문가가 권장하는 것으로 구성됩니다. 필요하다면 네트워크 포트 목록을 편집할 수 있습니다.

11. **설정** 버튼을 클릭하고 다음 설정을 편집합니다.

    - **Kaspersky에서 권장하는 목록에 있는 애플리케이션의 모든 포트 모니터**. Kaspersky Industrial CyberSecurity for Nodes가 사전 정의된 목록에 있는 애플리케이션의 네트워크 포트를 모니터링합니다. 예를 들어, 이 목록에는 Google Chrome, Adobe Reader, Java 및 기타 애플리케이션이 포함됩니다.

    - **지정한 애플리케이션의 모든 포트 모니터**. Kaspersky Industrial CyberSecurity for Nodes가 목록에 추가된 애플리케이션의 네트워크 포트를 모니터링합니다.

12. **확인** 버튼을 클릭합니다.

    구성된 연결 설정이 저장됩니다.

로컬 작업 실행 모드 구성

정책을 사용하여 로컬 시스템 온디맨드 검사 작업과 업데이트 작업의 시작을 허용하거나 차단할 수 있습니다. 이는 관리 그룹의 각 보호 중인 장치에 로컬로 구성된 스케줄에 따라 수행합니다:

- 정책으로 특정 유형의 로컬 시스템 작업의 예약된 시작을 금지되어 있으면, 보호 중인 장치에서 일정에 따라 이 작업을 수행하지 않습니다. 로컬 시스템 작업을 수동으로 시작할 수 있습니다.

- 정책으로 특정 유형의 로컬 시스템 작업의 예약된 시작을 허용한다면, 해당 작업이 이 작업을 위해 로컬로 구성한 예약 파라미터에 따라 수행됩니다.

기본적으로 로컬 시스템 작업의 시작은 정책에 의해 금지됩니다.

업데이트 또는 온디맨드 검사가 Kaspersky Security Center 그룹 작업에 의해 관리되는 경우에는 로컬 시스템 작업 시작을 허용하지 않는 것이 좋습니다.

그룹 업데이트 또는 온디맨드 검사 작업을 사용하지 않는 경우에는 정책에서 로컬 시스템 작업이 시작되도록 허용합니다. Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 데이터베이스 및 모듈 업데이트를 수행하고 기본 일정에 따라 모든 로컬 시스템 온디맨드 검사 작업을 시작합니다.

정책을 사용하여 다음 로컬 시스템 작업의 예약된 시작을 허용 또는 차단할 수 있습니다.

- 온디맨드 검사 작업: *중요 영역 검사*, *운영 체제 시작 시 검사*, *애플리케이션 무결성 제어*, *베이스라인 시스템 무결성 모니터*.

- 업데이트 작업: *데이터베이스 및 애플리케이션 모듈 업데이트*, *애플리케이션 업데이트*.

보호 중인 장치가 관리 그룹에서 제외된 경우 로컬 시스템 작업 일정이 자동 활성화됩니다.

정책에서 애플리케이션 로컬 작업에 대한 시작 스케줄 관리를 허용하거나 차단하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 관련 그룹을 확장한 후, 결과 창에서 **정책** 탭을 선택합니다.

2. **정책** 탭의 보호 중인 장치 그룹에 대한 Kaspersky Industrial CyberSecurity for Nodes 로컬 시스템 작업을 스케줄할 정책의 마우스 오른쪽 메뉴에서 **속성** 항목을 선택합니다.

3. 정책 속성 창에서 **애플리케이션 설정** 섹션을 선택합니다.

4. **로컬 시스템 작업 실행** 하위 섹션에서 **설정** 버튼을 클릭합니다.

5. **로컬 작업 사용 허용** 확인란을 선택합니다.

6. **스케줄 관리 허용** 체크박스를 사용하여 애플리케이션 로컬 작업의 시작 스케줄 관리를 허용하거나 차단합니다.

Kaspersky Security Center에서 격리 및 백업 설정 구성

Kaspersky Security Center에서 일반 격리 저장소 및 백업 설정을 구성하려면:

1. Kaspersky Security Center 관리 콘솔 트리의 **관리 중인 기기** 노드를 확장합니다.

2. 애플리케이션 설정을 구성할 관리 그룹을 선택합니다.

3. 선택한 관리 그룹의 세부 정보 창에서 다음 동작 중 하나를 수행합니다.

   - 보호 중인 장치 그룹에 대한 애플리케이션 설정을 구성하려면 **정책** 탭을 선택하고 **속성: <정책 이름>** 창을 엽니다.
   - 개별 보호 중인 장치에 대한 작업 또는 애플리케이션의 설정을 구성하려면 **기기** 탭을 선택하고 로컬 작업 설정 또는 애플리케이션 설정으로 갑니다.

4. **보충** 섹션으로 갑니다.

5. **저장소** 하위 섹션에서 **설정** 버튼을 클릭합니다.

6. 아래 표에서 설명한 설정을 구성합니다.

저장소 설정

파라미터	설명
리포트 탭에서 리포트 설정을 구성합니다.	
리포트 저장 기간	이 확인란을 선택하면 최대 리포트 저장 기간이 정의한 시간 간격으로 제한됩니다. 리포트 최대 저장 기간의 기본값은 30일입니다. 이 기간이 지나면 Kaspersky Industrial CyberSecurity for Nodes가 리포트 파일에서 가장 오래된 항목을 자동으로 삭제합니다.
리포트 파일 크기 제한	이 확인란을 선택하면 최대 리포트 파일 크기가 정의된 값으로 제한됩니다. 최대 파일 크기의 기본값은 1024MB입니다. Kaspersky Industrial CyberSecurity for Nodes는 리포트 파일 크기가 최대한도에 도달하면 리포트 파일에서 가장 오래된 항목을 자동으로 삭제하여 최대한도를 넘지 않도록 관리합니다.
백업 탭에서 백업 설정을 지정합니다.	
개체 저장 기간	이 확인란을 선택하면 최대 파일 저장 기간이 정의한 시간 간격으로 제한됩니다. 파일 최대 저장 기간의 기본값은 30일입니다. 최대 저장 기간이 만료되면 Kaspersky Industrial CyberSecurity for Nodes가 백업에서 가장 오래된 파일을 삭제합니다.
백업 크기를 다음으로 제한	이 확인란을 선택하면 최대 저장소 크기가 정의된 값으로 제한됩니다. 최대 크기 기본값은 400MB입니다 Kaspersky Industrial CyberSecurity for Nodes는 저장소 크기가 최대한도에 도달하면 저장소에서 가장 오래된 파일을 자동으로 삭제하여 최대 저장소 크기를 넘지 않도록 관리합니다.
이용 가능 공간의 임계값	이 확인란은 백업의 최소 여유 공간(기본값: 100MB)을 모니터링하는 기능을 활성화 또는 비활성화합니다. 여유 공간이 지정된 한계값 아래로 줄어들면 Kaspersky Industrial CyberSecurity for Nodes는 *백업 여유 공간 한계값 초과* 이벤트를 로깅하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. 이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 백업의 여유 공간을 모니터링합니다. **백업 크기를 다음으로 제한** 확인란을 선택했다면 **이용 가능 공간의 임계값** 확인란이 활성화됩니다.
격리 저장소 탭에서 격리 설정을 구성합니다.	

파라미터	설명
격리 저장소 크기 제한	이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 격리 저장소에 있는 개체의 총 크기를 모니터링합니다. 지정된 값을 초과하면(기본값 1024MB) Kaspersky Industrial CyberSecurity for Nodes는 *최대 격리 저장소 크기 초과* 이벤트를 기록하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. 그동안 애플리케이션은 새 개체를 격리하지 않습니다. 격리 저장소를 직접 비워야 합니다. 이 기능을 사용하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 격리 저장소에 있는 개체의 총 크기를 모니터링하지 않습니다. 이 기능은 기본적으로 비활성화됩니다.
이용 가능 공간의 임계값	이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 백업의 최소 여유 공간(기본값 50MB)을 모니터링합니다. 여유 공간이 지정된 한계값 아래로 줄어들면 Kaspersky Industrial CyberSecurity for Nodes는 *격리 저장소 여유 공간 한계값 초과* 이벤트를 기록하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. **격리 저장소 크기 제한** 확인란을 선택했다면 **이용 가능 공간의 임계값** 확인란이 활성화됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

정책 만들기 및 구성

이 섹션에서는 여러 보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes 관리 시 Kaspersky Security Center 정책을 사용하는 방법에 대한 정보를 제공합니다.

Kaspersky Industrial CyberSecurity for Nodes를 설치한 여러 장치에서 보호 기능을 관리하기 위해 글로벌 Kaspersky Security Center 정책을 만들 수 있습니다.

정책은 관리 그룹 하나의 모든 보호 중인 장치에 대해 정책에 정의된 Kaspersky Industrial CyberSecurity for Nodes 설정, 기능, 작업을 강제 적용합니다.

관리자 그룹 하나에 대해 여러 정책을 만들어 차례로 적용할 수 있습니다. 그룹에 대해 현재 활성화된 정책은 관리 콘솔에서 *활성* 상태로 표시됩니다.

정책 적용에 대한 정보가 Kaspersky Industrial CyberSecurity for Nodes 시스템 감사 로그에 기록됩니다. 이 정보는 **로그 검사** 노드의 애플리케이션 콘솔에서 확인할 수 있습니다.

Kaspersky Security Center에는 보호 중인 장치에 정책을 적용할 수 있는 한 가지 방법인 *설정 편집 금지*가 있습니다. 정책을 적용하면 Kaspersky Industrial CyberSecurity for Nodes가 **편집 차단** 정책 속성에서 지정한 설정 값을 사용합니다. 이 경우 Kaspersky Industrial CyberSecurity for Nodes는 정책을 적용하기 전에 사용 중이던 설정 값을 사용하지 않습니다. Kaspersky Industrial CyberSecurity for Nodes는 **편집 허용** 정책 속성에서 사용자가 지정한 활성 정책 설정 값을 적용하지 않습니다.

정책이 활성 상태이면 정책에 아이콘이 표시된 설정값이 애플리케이션 콘솔에 표시되지만 편집할 수는 없습니다. 다른 설정의 값은 애플리케이션 콘솔에서 편집할 수 있습니다.

활성 정책에 구성되어 있고 아이콘이 표시된 설정은 **속성: <보호 중인 장치 이름>** 창에서 개별 보호 중인 장치에 대한 Kaspersky Security Center에서 변경사항을 차단합니다.

활성화된 정책을 이용하여 지정하고 보호 중인 장치로 전달한 설정은, 활성 정책 비활성화 시 로컬 작업 설정에 저장됩니다.

정책이 현재 실행 중인 실시간 컴퓨터 보호 작업 또는 네트워크 연결 스토리지 보호 작업의 설정을 정의한다면, 이 정책에서 정의한 설정은 정책이 적용된 직후 변경됩니다. 작업이 실행되고 있지 않으면 시작 시 설정이 적용됩니다.

정책 만들기

정책을 생성하기 전에 관리 플러그인 klcfginst.exe를 설치해야 합니다.

애플리케이션을 설치 및 실행하는 보호 중인 장치 그룹에 대한 정책을 생성하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 정책을 생성할 보호 중인 장치가 포함된 관리 그룹을 선택합니다.
2. 선택한 관리 그룹의 결과 창에서 **정책** 탭을 선택하고 **새 정책** 버튼을 클릭해 새 정책 마법사를 시작할 수 있습니다.

   새 정책 마법사 창이 열립니다.
3. **그룹 정책을 생성하기 원하는 애플리케이션 선택** 창에서 Kaspersky Industrial CyberSecurity for Nodes를 선택합니다.
4. **다음** 버튼을 클릭합니다.
5. **이름** 필드에 그룹 정책 이름을 입력합니다.

   정책 이름에 `" * < : > ? \ |` 기호는 포함할 수 없습니다.
6. 이전 버전의 애플리케이션에서 사용된 정책 구성을 적용하려면:
   a. **이전 애플리케이션 버전에 대한 정책 설정 사용** 확인란을 선택합니다.
   b. **찾기** 버튼을 클릭합니다.
   c. 적용할 정책을 선택합니다.
   d. **다음** 버튼을 클릭합니다.
7. **작업 유형 선택** 창의 **실시간 파일 보호 구성** 블록에서 **실시간 파일 보호 사용** 확인란을 선택하고 보안 레벨을 지정합니다.

   작업 실행 모드를 선택하지 않으면 새 정책 마법사의 다음 단계를 진행할 수 없습니다.
8. 실시간 컴퓨터 보호를 구성합니다.
9. 검사 예외 및 신뢰하는 애플리케이션을 구성합니다.
10. **그룹 정책 생성** 창에서 다음 정책 상태 중 하나를 선택합니다.

- **활성 정책**: 정책을 만든 직후 정책을 적용하려는 경우. 그룹에 이미 활성 정책이 이미 있다면 해당 정책이 비활성화되고 새 정책이 적용됩니다.
- **비활성 정책**: 만든 정책을 바로 적용하지 않으려는 경우. 이 경우 정책은 이후에 활성화할 수 있습니다.

- **이동 사용자 정책**: 컴퓨터가 조직 네트워크 외부로 이동하면 이 정책이 활성화됩니다.
- **정책이 생성된 직후 정책 속성 열기** 확인란을 선택해 **새 정책 마법사** 창을 자동으로 닫고 **다음** 버튼을 클릭한 후 새로 생성된 정책을 구성합니다.

11. **마침** 버튼을 클릭합니다.

만든 정책이 선택한 관리 그룹의 **정책** 탭에 있는 정책 목록에 나타납니다. **속성: <정책 이름>** 창에서 Kaspersky Industrial CyberSecurity for Nodes의 기타 설정, 작업 및 기능을 구성할 수 있습니다.

새 정책이 생성되면 허용 규칙 집합이 생성되어 애플리케이션 차단을 방지하고 매끄러운 작업을 보장합니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 새 정책을 생성할 때 인바운드 네트워크 트래픽에 대한 규칙 세트를 생성합니다:

- Kaspersky Security Center 네트워크 에이전트를 사용하여 Windows 바탕 화면을 공유하는 프로세스에 대한 두 가지 허용 규칙으로, %Program Files% 및 %Program Files (x86)% 폴더에 있습니다. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.
- 로컬 포트 15000에 대한 두 가지 허용 규칙. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 새 정책을 생성할 때 발신 네트워크 트래픽 규칙 세트를 생성합니다:

- Kaspersky Industrial CyberSecurity for Nodes service에 대한 두 가지 허용 규칙으로, %Program Files% 및 %Program Files (x86)% 폴더에 있습니다. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.
- Kaspersky Industrial CyberSecurity for Nodes의 작업자 프로세스에 대한 두 가지 허용 규칙으로, %Program Files% 및 %Program Files (x86)% 폴더에 있습니다. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.
- 로컬 포트 13000에 대한 두 가지 허용 규칙. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.

정책 구성

정책 설정을 구성하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장합니다.
2. 연관된 정책 설정을 구성할 관리 그룹을 확장하고 세부 정보 창에서 **정책** 탭을 엽니다.
3. 구성할 정책 이름을 클릭합니다.
   다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책 마우스 오른쪽 메뉴의 **속성** 옵션을 클릭합니다.
   - 선택한 정책을 더블 클릭합니다.

4. **정책 상태** 섹션의 **일반** 탭에서 정책을 활성화 또는 비활성화합니다. 이를 위해 아래 옵션 중 하나를 선택합니다:

   - **활성 정책**: 선택한 관리 그룹 내의 모든 장치에 정책을 적용하려는 경우입니다.
   - **이동 사용자 정책**: 컴퓨터가 조직 네트워크 외부로 이동하면 이 정책이 활성화됩니다.
   - **비활성 정책**: 선택한 관리 그룹 내의 모든 보호 중인 장치에 대해서 나중에 정책을 활성화하려는 경우입니다.

5. 정책의 다른 섹션에서 애플리케이션 설정을 구성합니다.

   Kaspersky Security Center 정책을 통해 관리 그룹 내 보호 중인 모든 장치에 대해 작업 실행을 활성화 또는 비활성화할 수 있습니다.

   모든 네트워크 내 보호 중인 장치에서 개별 소프트웨어 구성 요소에 대한 정책 설정 적용을 구성할 수 있습니다.

6. **확인**을 누릅니다.

   구성된 설정이 정책에 적용됩니다.

Kaspersky Security Center를 사용하여 작업 만들기 및 구성

이 절에는 Kaspersky Industrial CyberSecurity for Nodes 작업과 생성 방법, 작업 설정 구성, 시작 및 중지에 대한 정보가 포함되어 있습니다.

Kaspersky Security Center에서 작업 만들기 정보

관리 그룹 및 보호 중인 장치 세트에 대한 그룹 작업을 만들 수 있습니다. Kaspersky Security Center를 통해 다음 유형의 작업을 만들 수 있습니다.

- *애플리케이션 활성화*
- *보안 감사*
- *프로세스 종료*
- *프로세스 실행*
- *중앙 관리 서버 연결 보호*
- *Kaspersky Industrial CyberSecurity for Nodes 구성 요소 변경*
- *베이스라인 시스템 무결성 모니터*
- *업데이트*

- *업데이트 롤백*
- *IOC 검사*
- *파일 가져오기*
- *격리 저장소로 파일 이동*
- *온디맨드 검사*
- *애플리케이션 무결성 제어*
- *키 제거*
- *파일 삭제*
- *애플리케이션 실행 제어를 위한 규칙 생성기*
- *장치 제어를 위한 규칙 생성기.*

다음과 같은 방법으로 로컬 및 그룹 작업을 만들 수 있습니다.

- 개별 보호 중인 장치는 **작업** 섹션에서.
- 관리 그룹은 **작업** 탭에서 선택한 보호 중인 장치 그룹 노드의 세부 정보 창에서.
- 보호 중인 장치 세트는 **기기 조회** 노드의 세부 정보 창에서.

> 정책을 사용하면 같은 관리 그룹의 모든 보호 중인 장치에 대해 *업데이트* 및 *온디맨드 검사* 로컬 시스템 작업 스케줄을 비활성화할 수 있습니다.

Kaspersky Security Center의 작업에 대한 일반 정보는 Kaspersky Security Center 도움말 을 참조하십시오.

Kaspersky Security Center를 사용하여 작업 만들기

Kaspersky Security Center 관리 콘솔에서 새 작업을 생성하려면:

1. 다음 방법 중 하나로 작업 마법사를 시작합니다.
   - 로컬 작업을 만들려면:
     a. 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 보호 중인 서버가 속한 그룹을 선택합니다.
     b. **기기** 탭의 결과 창에서 보호 중인 장치의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
     c. 창이 열리면 **작업** 섹션에서 **추가** 버튼을 클릭합니다.

- 그룹 작업을 만들려면:

  a. Kaspersky Security Center 관리 콘솔 트리의 **관리 중인 기기** 노드를 확장합니다.

  b. 작업을 생성할 관리 그룹을 선택합니다.

  c. 결과 창에서 **작업** 탭하고 **새 작업**을 선택합니다.

작업 마법사 창이 열립니다.

2. **작업 유형 선택** 창의 **Kaspersky Industrial CyberSecurity for Nodes** 제목 아래에서 생성할 작업 유형을 선택합니다.

3. 작업 유형에 따라 설정이 다를 수 있습니다:

- 온디맨드 검사 작업 만들기.
- 업데이트 작업을 만들려면 요구사항에 따라 작업 설정을 구성합니다.

  a. **업데이트 경로** 블록에서 Kaspersky Security Center 중앙 관리 서버 또는 Kaspersky 업데이트 서버를 애플리케이션 업데이트 경로로 지정할 수 있습니다. 또한 사용자 지정 HTTP 및 FTP 서버 또는 네트워크 폴더를 수동으로 추가한 다음 업데이트 경로로 설정하여 업데이트 경로의 사용자 지정 목록을 만들 수도 있습니다.

  수동으로 사용자 지정한 서버를 사용할 수 없는 경우 Kaspersky 업데이트 서버를 사용하도록 지정할 수 있습니다.

  b. 디스크 하위 시스템의 부하를 줄이는 기능에 대한 설정을 구성합니다:

  c. 중요 애플리케이션 모듈 업데이트가 필요한 경우와 긴급 업데이트 설치가 완료된 후에 Kaspersky Industrial CyberSecurity for Nodes가 수행할 동작을 지정할 수 있습니다. 또한 Kaspersky Industrial CyberSecurity for Nodes가 사용 가능한 스케줄된 업데이트 정보를 받을지 지정할 수 있습니다.

  d. Kaspersky Industrial CyberSecurity for Nodes에서 복사한 업데이트를 저장할 폴더 경로와 복사할 업데이트 세트를 지정합니다.

- *애플리케이션 활성화* 작업을 생성하려면:

  a. **활성화 설정** 창에서 애플리케이션 활성화에 사용할 키 파일이나 활성화 코드를 지정합니다.

  b. 라이센스 갱신을 위한 작업을 만들려는 경우 **추가 키로 사용** 확인란을 선택합니다.

- 애플리케이션 실행 제어를 위한 규칙 생성기 작업을 생성합니다.
- 장치 제어를 위한 규칙 생성기 작업을 생성합니다.

4. 작업 스케줄을 구성합니다.

5. **확인**을 누릅니다.

6. 보호 중인 장치 세트에 대해 작업을 만든 경우 이 작업을 실행할 보호 중인 장치 네트워크(그룹)를 선택합니다.

7. **작업을 실행할 계정 선택** 창에서 작업 실행에 사용할 계정을 지정합니다.

8. **작업 이름 정의** 창에서 `" * < > ? \ | :` 기호를 포함하지 않고 작업 이름을 100자 이하로 입력합니다.

작업 이름에 작업 유형을 추가하는 것이 좋습니다(예: "공유 폴더 온디맨드 검사").

9. **작업 생성 마침** 창에서 다음을 수행합니다:

   a. 작업을 생성하는 즉시 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

   b. **마침** 버튼을 클릭합니다.

만든 작업이 **작업** 목록에 표시됩니다.

개별 컴퓨터에 대한 로컬 작업 설정 및 일반 애플리케이션 설정으로 이동

현재 애플리케이션에 Kaspersky Security Center 정책이 적용되고 이 정책이 애플리케이션 설정 변경을 금지한다면, 개별 컴퓨터에서 이러한 설정을 편집할 수 없습니다.

개별 컴퓨터의 로컬 작업 설정으로 이동하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장합니다.
2. 보호 중인 장치가 속한 그룹을 선택합니다.
3. 세부 정보 창에서 **장치** 탭을 선택합니다.
4. 다음 방법 중 하나로 **속성: <보호 중인 장치 이름>** 창을 엽니다.

   - 보호 중인 장치의 이름을 더블클릭합니다.
   - 선택한 작업 이름의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   속성: <보호 중인 장치 이름> 창이 열립니다.
5. **작업** 섹션으로 갑니다.
6. 다음 방법 중 하나로 작업 목록에서 구성할 로컬 작업을 선택합니다:

   - 작업 이름 더블클릭
   - 목록에서 작업을 선택하고 **속성** 버튼 더블클릭
   - 작업 이름의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   속성: <작업 이름> 창이 열립니다.

개인 컴퓨터의 일반 애플리케이션 설정으로 이동하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 보호 중인 장치가 속한 그룹을 선택합니다.
2. 세부 정보 창에서 **장치** 탭을 선택합니다.

3. 다음 방법 중 하나로 **속성: <보호 중인 장치 이름>** 창을 엽니다.

   - 보호 중인 장치의 이름을 더블클릭합니다.
   - 선택한 작업 이름의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   속성: <보호 중인 장치 이름> 창이 열립니다.

4. **애플리케이션** 섹션으로 갑니다.

5. 설치된 애플리케이션 목록에서 다음 방법 중 하나를 사용해 Kaspersky Industrial CyberSecurity for Nodes를 선택합니다.

   - Kaspersky Industrial CyberSecurity for Nodes 이름 더블클릭
   - 목록에서 Kaspersky Industrial CyberSecurity for Nodes 선택 후 **속성** 버튼 클릭.
   - Kaspersky Industrial CyberSecurity for Nodes 이름의 마우스 오른쪽 메뉴에서 **속성** 항목을 선택합니다.

   Kaspersky Industrial CyberSecurity for Nodes의 **설정** 창이 열립니다.

Kaspersky Security Center에서 그룹 작업 구성

여러 보호 중인 장치의 그룹 작업을 구성하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 애플리케이션 작업을 구성할 관리 그룹을 선택합니다.

2. 선택한 관리 그룹의 세부 정보 창에서 **작업** 탭을 엽니다.

3. 이전에 만든 그룹 작업 목록에서 구성하려는 작업을 선택합니다.

4. 다음 방법 중 하나로 **속성: <작업 이름>** 창을 엽니다.

   - 생성된 작업 목록에서 작업 이름 더블클릭.
   - 생성된 작업 목록에서 작업 이름을 선택하고 **작업 구성** 링크를 클릭합니다.
   - 생성된 작업 목록에서 작업 이름의 마우스 오른쪽 메뉴를 열고 **속성** 항목 선택.

5. **알림** 섹션에서 작업 이벤트 알림 설정을 구성합니다. 이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

6. 구성한 작업 유형에 따라 다음 중 하나를 수행합니다.

   - *온디맨드 검사* 작업을 구성하려면:
     - **검사 범위** 섹션에서 검사 범위를 생성합니다.
     - **설정** 섹션에서 작업 우선순위 레벨 및 다른 소프트웨어 구성 요소와의 통합을 구성합니다.

- *업데이트* 작업을 구성하려면:
  - **설정** 섹션으로 가서 **애플리케이션 데이터베이스 및 모듈 업데이트 설정**을 지정합니다.
  - 소프트웨어 모듈의 긴급 업데이트 복사 및 설치 또는 확인만 하기 중 수행할 동작을 선택합니다.
- *애플리케이션 활성화* 작업을 구성하려면:
  - **설정** 섹션에서 애플리케이션 활성화에 사용할 키 파일이나 활성화 코드를 지정합니다.
  - 라이센스 갱신을 위한 활성화 코드 또는 키 파일을 추가하려는 경우 **추가 키로 사용** 확인란을 선택합니다.
- *장치 제어를 위한 규칙 생성기* 작업을 구성하려면 **설정** 섹션에서 장치 제어 규칙 목록을 만드는 데 사용할 설정을 지정합니다.

7. **스케줄** 섹션에서 작업 스케줄을 구성합니다.
8. **계정** 섹션에서 작업 실행에 권한을 사용할 계정을 지정합니다. 이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.
9. 필요하다면 **작업 제외 그룹** 섹션에서 들어가 작업 범위에서 제외할 개체를 지정합니다. 이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.
10. **속성:<작업 이름>** 창의 **확인** 버튼을 클릭합니다.

    새로 구성된 그룹 작업 설정이 저장됩니다.

그룹 작업에 대해 구성할 수 있는 설정은 다음과 같습니다.

- 애플리케이션 실행 제어를 위한 규칙 생성기

  애플리케이션 실행 제어를 위한 규칙 생성기 작업 설정 구성 시, **규칙** 탭에서 허용 규칙 생성 방법을 선택할 수 있습니다.
  - **실행 중인 애플리케이션을 기반으로 허용 규칙 생성**
  - **폴더에서 애플리케이션에 대한 허용 규칙 생성**

  설정 탭에서 애플리케이션 실행 제어 허용 규칙을 생성하는 동안 수행할 다음 동작을 지정할 수 있습니다.
  - **디지털 인증서 사용**
  - **디지털 인증서 주체 및 지문 사용**
  - **인증서가 없다면 다음 사용**
  - **SHA256 해시 사용**
  - **사용자 또는 사용자 그룹을 위한 규칙 생성**

  작업 완료 시 Kaspersky Industrial CyberSecurity for Nodes가 생성하는 허용 규칙 목록을 사용해 구성 파일에 대한 설정을 구성할 수 있습니다.

  스케줄에 따라 작업을 시작하도록 설정을 구성할 수 있습니다.

- 장치 제어를 위한 규칙 생성기
  - 운영 모드 선택: 연결된 적이 있는 모든 외부 장치에 대한 시스템 데이터를 고려하거나 현재 연결된 외부 장치만 고려합니다.
  - 작업 완료 시 Kaspersky Industrial CyberSecurity for Nodes가 생성하는 허용 규칙 목록을 사용해 구성 파일에 대한 설정을 구성합니다.
  - 스케줄에 따라 작업을 시작하도록 설정을 구성할 수 있습니다.
- 애플리케이션 활성화
  - 애플리케이션 활성화나 라이센스 갱신을 위해 키 파일이나 활성화 코드를 추가할 수 있습니다.
  - 스케줄에 따라 작업을 시작하도록 설정을 구성할 수 있습니다.
- 데이터베이스 및 애플리케이션 모듈 업데이트
  - **업데이트 경로** 설정 블록에서 Kaspersky Security Center 중앙 관리 서버 또는 Kaspersky 업데이트 서버를 애플리케이션 업데이트 경로로 지정할 수 있습니다. 또한 사용자 지정 HTTP 및 FTP 서버 또는 네트워크 폴더를 수동으로 추가한 다음 업데이트 경로로 설정하여 업데이트 경로의 사용자 지정 목록을 만들 수도 있습니다.

    수동으로 사용자 지정한 서버를 사용할 수 없는 경우 Kaspersky 업데이트 서버를 사용하도록 지정할 수 있습니다.
  - 디스크 하위 시스템의 부하를 줄이는 기능에 대한 설정을 구성할 수 있습니다:
    - **디스크 I/O 부하 낮추기**
    - **최적화에 사용되는 RAM, MB**
  - 중요 애플리케이션 모듈 업데이트가 필요한 경우와 긴급 업데이트 설치가 완료된 후에 Kaspersky Industrial CyberSecurity for Nodes가 수행할 동작을 지정할 수 있습니다. 또한 Kaspersky Industrial CyberSecurity for Nodes가 사용 가능한 스케줄된 업데이트 정보를 받을지 지정할 수 있습니다.
  - Kaspersky Industrial CyberSecurity for Nodes에서 복사한 업데이트를 저장할 폴더 경로와 복사할 업데이트 세트를 지정할 수 있습니다.
  - 스케줄에 따라 작업을 시작하도록 설정을 구성할 수 있습니다.
- 온디맨드 검사
  - 온디맨드 검사 작업의 검사 범위를 지정하고 보안 레벨 설정을 구성할 수 있습니다.
  - **휴리스틱 분석기** 설정 블록에서 온디맨드 검사 작업에 대한 휴리스틱 분석기 사용을 활성화 또는 비활성화하고 슬라이더를 사용하여 분석 레벨을 설정할 수 있습니다.

- **다른 구성 요소와 통합** 블록에서 다음 설정을 구성할 수 있습니다:
  - 백그라운드 모드에서 검사 작업을 시작합니다.
  - 작업을 중요 영역 검사로 간주합니다.
  - 여러 검사 작업의 동시 실행을 비활성화합니다.
- 스케줄에 따라 작업을 시작하도록 설정을 구성할 수 있습니다.

- 애플리케이션 무결성 제어
  - 스케줄에 따라 작업을 시작하도록 설정을 구성할 수 있습니다.
- 베이스라인 시스템 무결성 모니터
  - 파일, 레지스트리, 장치에 수행할 동작을 지정하는 규칙과 모니터링 모드를 구성할 수 있습니다.
  - 스케줄에 따라 작업을 시작하도록 설정을 구성할 수 있습니다.

애플리케이션 활성화 작업

애플리케이션 활성화 작업을 구성하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 애플리케이션 작업을 구성할 관리 그룹을 선택합니다.
2. 선택한 관리 그룹의 세부 정보 창에서 **작업** 탭을 엽니다.
3. 이전에 만든 그룹 작업 목록에서 구성하려는 작업을 선택합니다.
4. 다음 방법 중 하나로 **속성: <작업 이름>** 창을 엽니다.
   - 생성된 작업 목록에서 작업 이름 더블클릭.
   - 생성된 작업 목록에서 작업 이름의 마우스 오른쪽 메뉴를 열고 **속성** 항목 선택.

   > **알림** 섹션에서 작업 이벤트 알림 설정을 구성합니다. 이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.
5. **활성화 설정** 섹션에서 애플리케이션을 활성화하는 데 사용할 키 파일을 지정합니다. 라이센스 갱신을 위해 키를 추가하려는 경우 **추가 키로 사용** 확인란을 선택합니다.
6. **스케줄** 섹션에서 작업 스케줄 설정을 구성합니다.
7. 필요하다면 **작업 제외 그룹** 섹션의 작업 범위에서 제외할 개체를 지정합니다.
   이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.
8. **속성:<작업 이름>** 창의 **확인** 버튼을 클릭합니다.

새로 구성된 그룹 작업 설정이 저장됩니다.

업데이트 작업

업데이트 작업을 구성하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 애플리케이션 작업을 구성할 관리 그룹을 선택합니다.
2. 선택한 관리 그룹의 세부 정보 창에서 **작업** 탭을 엽니다.
3. 이전에 만든 그룹 작업 목록에서 구성하려는 작업을 선택합니다.
4. 다음 방법 중 하나로 **속성: <작업 이름>** 창을 엽니다.
   - 생성된 작업 목록에서 작업 이름 더블클릭.
   - 생성된 작업 목록에서 작업 이름의 마우스 오른쪽 메뉴를 열고 **속성** 항목 선택.
5. **알림** 섹션에서 작업 이벤트 알림 설정을 구성합니다. 이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.
6. **설정** 섹션에서 다음을 수행합니다:
   a. **애플리케이션 데이터베이스 및 모듈 업데이트 설정** 섹션의 **설정** 버튼을 사용하여 업데이트 경로를 선택합니다:
      - Kaspersky Security Center 중앙 관리 서버.
      - Kaspersky 업데이트 서버.
      - 사용자 지정 HTTP 또는 FTP 서버 또는 네트워크 폴더.

      SMB 공유 폴더를 업데이트 경로로 사용하려면 작업을 시작할 사용자 계정을 지정할 필요가 있습니다.

      수동으로 사용자 지정한 서버를 사용할 수 없는 경우 Kaspersky 업데이트 서버를 사용하도록 지정할 수 있습니다.

   b. 디스크 하위 시스템의 부하를 줄이는 기능에 대한 설정을 구성합니다:
      - **디스크 I/O 부하 낮추기**. 이 확인란은 업데이트 파일을 RAM의 가상 드라이브에 저장하여 디스크 하위 시스템을 최적화하는 과정을 활성화 또는 비활성화합니다. 기본적으로 확인란의 선택이 취소됩니다.
      - **최적화에 사용되는 RAM, MB**

   c. 애플리케이션 모듈의 긴급 업데이트를 사용할 수 있거나 계획된 업데이트 정보가 있을 시 Kaspersky Industrial CyberSecurity for Nodes에서 수행할 동작을 지정합니다.

   d. 업데이트 복사 설정을 지정합니다.
7. **스케줄** 섹션에서 작업 일정을 구성합니다(데이터베이스 업데이트 롤백을 제외한 모든 작업 유형에 대한 일정을 구성할 수 있음).

8. **계정** 섹션에서 작업 실행에 권한을 사용할 계정을 지정합니다.

   이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

9. **속성: <작업 이름>** 창에서 **확인**을 클릭합니다.

업데이트 롤백 작업의 경우, Kaspersky Security Center에 의해 제어되는 표준 작업 설정만 **알림** 및 **작업 제외 그룹** 섹션에서 구성할 수 있습니다. 이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

애플리케이션 무결성 제어

애플리케이션 무결성 제어 그룹 작업을 구성하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 애플리케이션 작업을 구성할 관리 그룹을 선택합니다.
2. 선택한 관리 그룹의 세부 정보 창에서 **작업** 탭을 엽니다.
3. 이전에 만든 그룹 작업 목록에서 구성하려는 작업을 선택합니다.
4. 다음 방법 중 하나로 **속성: <작업 이름>** 창을 엽니다.
   - 생성된 작업 목록에서 작업 이름 더블클릭.
   - 생성된 작업 목록에서 작업 이름의 마우스 오른쪽 메뉴를 열고 **속성** 항목 선택.
5. **알림** 섹션에서 작업 이벤트 알림 설정을 구성합니다. 이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.
6. **장치** 섹션에서 *애플리케이션 무결성 제어* 작업을 구성할 장치를 선택합니다.
7. **스케줄** 섹션에서 작업 스케줄 설정을 구성합니다.
8. **계정** 섹션에서 작업 실행에 권한을 사용할 계정을 지정합니다.
9. 필요하다면 **작업 제외 그룹** 섹션의 작업 범위에서 제외할 개체를 지정합니다.

   이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

10. **속성:<작업 이름>** 창의 **확인** 버튼을 클릭합니다.

작업 예약

관리 플러그인을 사용하여 작업을 스케줄하려면 다음과 같이 하십시오.

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
2. 작업 공간에서 **기기** 탭을 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. **작업** 섹션으로 갑니다.
5. 스케줄을 구성할 작업의 속성 창을 두 번 클릭하여 엽니다.
6. **스케줄** 섹션을 선택합니다.
7. 필요에 따라 스케줄 설정(아래 표 참조)을 구성합니다.

   온디맨드 검사 및 업데이트 작업의 일정 설정 필드는 Kaspersky Security Center 정책에 의해 해당 작업 예약이 차단된 경우 사용할 수 없습니다.

8. **적용** 버튼을 클릭해 작업 시작 설정을 저장합니다.

Kaspersky Security Center를 사용하여 단일 작업의 애플리케이션 설정을 구성하려면 Kaspersky Security Center의 애플리케이션 설정 창에서 로컬 작업 구성 섹션을 엽니다.

작업 스케줄 설정

파라미터	설명
시작 스케줄	작업 실행 모드를 선택합니다: • **N시간마다**. 작업이 몇 시간마다 주기적으로 실행됩니다. 작업 시작 시간과 시간 단위의 주기를 지정합니다. • **N일마다**. 작업이 며칠마다 주기적으로 실행됩니다. 작업 시작 시간과 일 단위의 주기를 지정합니다. • **N분마다**. 작업이 몇 분마다 주기적으로 실행됩니다. 작업 시작 시간과 분 단위의 주기를 지정합니다. • **주별**. 작업이 매주 특정 요일에 실행됩니다. 요일과 시작 시간을 지정합니다. • **월별**. 작업이 매월 특정 일자에 실행됩니다. 시작 날짜와 시간을 지정합니다. • **한번만**. 작업이 지정된 날짜와 시간에 한 번 실행됩니다. • **수동**. 편리한 시간에 검사를 수동으로 시작할 수 있는 실행 모드입니다. • **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**. 저장소에서 업데이트가 다운로드될 때마다 작업이 실행됩니다. • **다른 작업 완료 시**. 다른 작업 완료 시 작업이 실행됩니다. 작업 및 완료 상태를 선택합니다. Kaspersky Industrial CyberSecurity for Nodes는 로컬 작업 스케줄에 **다른 작업 완료 시** 모드를 지원하지 않습니다. • **바이러스 발생 시**. 바이러스 공격이 탐지되면 작업이 실행됩니다. • **애플리케이션 시작 시**. 작업은 Kaspersky Industrial CyberSecurity for Nodes가 시작될 때마다 수행됩니다.
누락된 작업 실행	이 확인란을 선택하면, Kaspersky Industrial CyberSecurity for Nodes는 작업이 가능하자 마자 건너뛴 작업을 시작합니다. 스케줄된 작업 시작 시각에 컴퓨터가 꺼져 있는 등의 경우에는 작업을 건너뜁니다. 애플리케이션에 누락된 작업을 실행할 기회가 있다면 특정 시간 내에 무작위로 작업을 실행하여 컴퓨터의 로드를 분산합니다. 이 확인란을 선택 취소하면 Kaspersky Industrial CyberSecurity for Nodes가 건너뛴 작업을 실행하지 않습니다. 대신, 현재 스케줄에 따라 다음 작업을 실행합니다.

파라미터	설명
자동으로 작업 시작 임의 지연 사용	이 확인란을 선택하면 작업이 특정 시간 범위 내에서 임의의 시간에 컴퓨터에서 실행됩니다. 무작위 시작 시간은 스케줄에 따라 작업이 실행될 때, 중앙 관리 서버에 다수의 컴퓨터가 동시에 접근하는 것을 방지하는 데 도움이 됩니다. 확인란의 선택을 취소하면 작업이 정확히 스케줄된 시간에 실행됩니다.
다음 간격으로 작업 시작 임의 지연(분)	이 확인란을 선택하면 작업이 특정 시간 범위 내에서 임의의 시간에 컴퓨터에서 실행됩니다. 무작위 시작 시간은 스케줄에 따라 작업이 실행될 때, 중앙 관리 서버에 다수의 컴퓨터가 동시에 접근하는 것을 방지하는 데 도움이 됩니다. 확인란의 선택을 취소하면 작업이 정확히 스케줄된 시간에 실행됩니다.
작업 시작 전에 Wake-on-LAN 기능으로 기기 켜기	이 확인란을 선택하면 작업 실행 전에 컴퓨터 운영 체제에 시작 완료를 위해 지정된 리드 타임이 제공됩니다. 기본 리드 타임은 5분입니다. 전원이 꺼진 컴퓨터를 포함하여 모든 컴퓨터에서 작업을 실행하려면 확인란을 선택합니다.
작업 완료 후 기기 종료	이 확인란을 선택하면 작업이 완료된 후 컴퓨터가 종료됩니다. 예를 들어, 이 기능을 활성화하면 근무 시간이 끝난 금요일에 컴퓨터를 스캔할 수 있습니다. 작업이 완료되면 애플리케이션이 주말 동안 컴퓨터를 끕니다.
작업이 다음 시간보다 오래 실행되면 중지	작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Industrial CyberSecurity for Nodes가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Industrial CyberSecurity for Nodes가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.
작업 일시 중지	이전에 스케줄된 작업의 실행을 일시 중지할 시간 간격을 지정할 수 있습니다. 지정한 기간이 지나면 작업이 다시 시작됩니다. 이는 예를 들어 사용량이 가장 많은 기간에 Kaspersky Industrial CyberSecurity for Nodes가 컴퓨터 성능에 미치는 영향을 최소화하기 위해 필요할 수 있습니다. 이 기능은 온디맨드 검사 작업에만 사용할 수 있습니다.
다음부터 스케줄 비활성화	이 체크박스를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 지정한 날짜부터 스케줄된 작업의 실행을 중지합니다. 해당 작업은 **수동** 모드로 설정됩니다. 이 기능은 온디맨드 검사 작업에만 사용할 수 있습니다.

Kaspersky Security Center 리포트

Kaspersky Security Center의 리포트에는 관리 중인 장치의 상태 정보가 포함되어 있습니다. 리포트는 중앙 관리 서버에 저장된 정보를 기반으로 합니다.

Kaspersky Security Center 11부터 Kaspersky Industrial CyberSecurity for Nodes에서 다음 유형의 리포트를 사용할 수 있습니다.

- 애플리케이션 구성 요소 상태 리포트
- 금지한 애플리케이션에 대한 리포트
- 테스트 모드에서 금지한 애플리케이션에 대한 리포트

Kaspersky Security Center 리포트 사용에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Industrial CyberSecurity for Nodes 구성 요소 작동에 관한 리포트

모든 네트워크 장치의 보호 상태를 모니터링하고 각 장치의 구성 요소 집합에 대한 구조화된 개요를 확인할 수 있습니다.

리포트에는 각 구성 요소에 대해 다음 상태 중 하나가 표시됩니다: *실행 중*, *일시 중지됨*, *중지됨*, *라이센스에 포함되지 않음*.

설치되지 않음 상태는 애플리케이션 자체가 아닌 구성 요소를 말합니다. 애플리케이션이 설치되어 있지 않으면 Kaspersky Security Center가 N/A(사용할 수 없음) 상태를 할당합니다.

구성 요소 조회를 만들고 필터링을 사용하여 네트워크 장치를 지정된 구성 요소 및 상태 집합과 함께 표시할 수 있습니다.

만들기 및 조회 사용에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

애플리케이션 설정에서 구성 요소 상태를 검토하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 애플리케이션 설정을 구성하려는 관리 그룹을 선택합니다.
2. **장치** 탭을 선택하고 **애플리케이션 설정** 창을 엽니다.
3. **구성 요소** 섹션을 선택합니다.
4. 상태 표를 검토합니다.

Kaspersky Security Center 표준 리포트를 검토하려면:

1. 관리 콘솔 트리의 **중앙 관리 서버<중앙 관리 서버 이름>** 노드를 선택합니다.
2. **리포트** 탭을 선택합니다.
3. **애플리케이션 구성 요소 상태 리포트** 목록 항목을 더블클릭합니다.
   리포트가 생성됩니다.
4. 다음 리포트 세부 정보를 검토합니다:
   - 그래픽 다이어그램.
   - 각 구성 요소와 해당 구성 요소가 속한 그룹이 설치된 구성 요소와 네트워크 장치의 집계 수에 대한 요약표.
   - 구성 요소 상태, 버전, 장치, 그룹을 포함하는 상세표.

활성 및 테스트 모드에서 금지한 애플리케이션에 대한 리포트

애플리케이션 실행 제어 작업의 결과를 기반으로, 금지한 애플리케이션에 관한 리포트(작업이 활성 모드에서 시작된 경우)와 테스트 모드에서 금지한 애플리케이션에 관한 리포트(작업이 알림 모드에서 시작된 경우)의 두 가지 리포트가 생성될 수 있습니다. 이 리포트는 네트워크의 보호 중인 장치에서 차단된 애플리케이션에 대한 정보를 표시합니다. 모든 관리 그룹에 대해 각 리포트가 생성되며 보호 중인 장치에 설치된 모든 Kaspersky 애플리케이션의 데이터가 누적됩니다.

알림 모드에서 금지한 애플리케이션에 대한 리포트를 검토하려면:

1. 알림 모드에서 애플리케이션 실행 제어 작업을 시작합니다.
2. 관리 콘솔 트리의 **중앙 관리 서버<중앙 관리 서버 이름>** 노드를 선택합니다.
3. **리포트** 탭을 선택합니다.
4. **테스트 모드에서 금지한 애플리케이션에 대한 리포트** 항목을 더블클릭합니다.
   리포트가 생성됩니다.
5. 다음 리포트 세부 정보를 검토합니다:
   - 차단된 시작 횟수가 가장 많은 상위 10개 애플리케이션을 표시하는 그래픽 다이어그램.
   - 실행 파일 이름, 이유, 차단 시간, 차단이 발생한 장치 수를 지정하는 애플리케이션 차단 요약표입니다.
   - 장치, 파일 경로 및 차단 기준에 대한 데이터를 지정하는 상세표입니다.

활성 모드에서 금지한 애플리케이션에 대한 리포트를 검토하려면:

1. 활성 모드에서 애플리케이션 실행 제어 작업을 실행합니다.
2. 관리 콘솔 트리의 **중앙 관리 서버<중앙 관리 서버 이름>** 노드를 선택합니다.
3. **리포트** 탭을 선택합니다.
4. **금지한 애플리케이션에 대한 리포트** 항목을 더블클릭합니다.
   리포트가 생성됩니다.

이 리포트는 테스트 모드에서 금지한 애플리케이션에 대한 리포트와 같은 차단 데이터로 구성됩니다.

실시간 보호 상태

Kaspersky Industrial CyberSecurity for Nodes는 **실시간 보호 상태** 설정을 Kaspersky Security Center 중앙 관리 서버로 전송합니다. 이 설정의 값은 보호된 장치에서 애플리케이션 보호 구성 요소의 현재 상태에 따라 달라집니다(아래 표 참조).

Kaspersky Industrial CyberSecurity for Nodes는 다음 애플리케이션 구성 요소의 상태를 기반으로 실시간 보호 상태를 결정합니다.

- 실시간 파일 보호
- 장치 제어
- 방화벽
- 네트워크 위협 보호
- AMSI 스캐너
- Anti-Cryptor
- BadUSB 공격 방지
- 복원 엔진
- 익스플로잇 방지.

Kaspersky Security Center 콘솔에서 애플리케이션의 실시간 보호 상태를 확인할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 실시간 보호 상태를 확인하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **관리 중인 기기** 옵션을 선택합니다.

현재 실시간 보호 상태는 장치 목록의 **실시간 보호 상태** 열에 표시됩니다. **실시간 보호 상태** 열이 없으면 **열 추가/제거** 링크를 클릭하여 열 설정을 관리합니다.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **관리 중인 기기** 옵션을 선택합니다.

현재 실시간 보호 상태는 장치 목록의 **실시간 보호 상태** 열에 표시됩니다. **실시간 보호 상태** 열이 없으면 **열 추가/제거** 링크를 클릭하여 열 설정을 관리합니다.

웹 콘솔에서 실시간 컴퓨터 보호를 확인하는 방법

웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)** 옵션을 선택합니다.

현재 실시간 보호 상태는 장치 목록의 **실시간 보호 상태** 열에 표시됩니다. **실시간 보호 상태** 열이 없으면 열 설정을 관리합니다( ).

실시간 보호 상태 설정의 가능한 값

값	설명
알 수 없음	중앙 관리 서버에 이 장치의 실시간 보호 상태에 대한 정보가 없습니다.
설치 안 됨	설치된 구성 요소가 없습니다.
라이센스가 지원하지 않음	애플리케이션이 활성화되지 않았거나 라이선스가 설치된 구성 요소의 작동을 허용하지 않습니다.
실패	하나 이상의 구성 요소가 오작동했습니다.
중지됨	하나 이상의 구성 요소가 비활성화되어 있습니다.
일시 중지됨	하나 이상의 구성 요소가 일시 중지되었습니다.

값	설명
시작 중	하나 이상의 구성 요소를 켜는 중입니다.
실행 중	애플리케이션 구성 요소가 정상적으로 실행 중입니다.

Kaspersky Security Center의 **실시간 보호 상태** 설정값이 *실행 중*이 아닌 경우, 목록에 있는 Kaspersky Industrial CyberSecurity for Nodes의 설치된 구성 요소가 활성화되어 있고 애플리케이션이 활성화되어 있는지 확인하십시오.

Kaspersky Industrial CyberSecurity for Nodes 콘솔 작업

이 섹션에서는 Kaspersky Industrial CyberSecurity for Nodes 콘솔 정보를 제공하고, 보호 중인 장치 또는 다른 장치에 설치된 애플리케이션 콘솔로 애플리케이션을 관리하는 방법을 설명합니다.

애플리케이션 콘솔 시작

애플리케이션 콘솔을 시작하려면:

1. 다음 방법 중 하나로 간편 진단 인터페이스를 엽니다.

   - 보호 중인 장치의 애플리케이션 설치 폴더에 있는 avpui.exe 파일을 실행합니다. 기본적으로 파일은 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0에 있습니다.
   - 작업 표시줄 알림 영역의 애플리케이션 아이콘을 클릭합니다.

2. 간편 진단 인터페이스 창이 열리면 **Kaspersky Industrial CyberSecurity for Nodes 콘솔** 링크를 클릭합니다.

   보호 중인 장치에 대한 연결을 이미 구성했다면, 애플리케이션 콘솔이 열립니다.

   애플리케이션 콘솔을 처음 시작하면 **보호 중인 장치 선택** 창이 열리며, 여기서 보호 중인 컴퓨터에 대한 애플리케이션 콘솔의 연결을 구성해야 합니다.

   > 애플리케이션 콘솔 버전 4.5는 Kaspersky Industrial CyberSecurity for Nodes 버전 5.0 이상과 호환되지 않습니다. 연결을 시도하면 애플리케이션 콘솔용 호환성 팩을 설치하라는 메시지가 표시됩니다. 호환성 팩은 연결 대상 장치에서 다운로드됩니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔 인터페이스

이 섹션에서는 애플리케이션 인터페이스의 기본 요소에 대해 설명합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔 창

다른 보호 중인 장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes에 연결하면, 노드 이름에 애플리케이션이 설치된 보호 중인 장치 이름과 연결을 설정한 사용자 계정 이름이 더해집니다. 예: **Kaspersky Industrial CyberSecurity for Nodes <계정 이름>으로 <보호 중인 장치 이름>**. Kaspersky Industrial CyberSecurity for Nodes 콘솔이 있는 같은 보호 중인 장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes에 연결 시, 노드 이름은 Kaspersky Industrial CyberSecurity for Nodes가 됩니다.

콘솔 트리

애플리케이션 콘솔 트리가 Kaspersky Industrial CyberSecurity for Nodes 노드와 애플리케이션 기능 구성 요소의 하위 노드를 표시합니다.

Kaspersky Industrial CyberSecurity for Nodes 노드에는 다음 하위 노드가 포함됩니다.

- **실시간 컴퓨터 보호**는 다음 작업을 구성할 수 있습니다.
  - **실시간 파일 보호**
  - **Kaspersky Security Network**
  - **익스플로잇 방지**
  - **네트워크 위협 보호**
  - **Anti-Cryptor**
  - **복원 엔진**
  - **AMSI 스캐너**
- **원격 측정 설정**: 애플리케이션이 호환되는 Detection and Response 솔루션 및 SIEM 시스템으로 전송하는 텔레메트리 설정입니다.
- **컴퓨터 제어**: 보호 중인 장치 및 연결된 장치에서 실행 중인 애플리케이션 제어.
  - **애플리케이션 실행 제어**
  - **장치 제어**
  - **방화벽**
- **규칙 자동 생성**: 애플리케이션 실행 제어 구성 요소 및 장치 제어 구성 요소에 대한 그룹 및 시스템 규칙 자동 생성 구성.
  - **애플리케이션 실행 제어를 위한 규칙 생성기**
  - **장치 제어를 위한 규칙 생성기**
  - 규칙 생성 그룹 작업 **<작업 이름>**(해당하는 경우)

    그룹 작업은 Kaspersky Security Center를 이용하여 생성됩니다. Kaspersky Industrial CyberSecurity for Nodes 콘솔을 통해 그룹 작업을 관리할 수 없습니다.
- **시스템 점검**: 시스템 무결성 모니터링 및 Windows 이벤트 로그 분석 설정 구성.
  - **로그 검사**
  - **시스템 무결성 모니터링**

- **산업 네트워크 보호**: 보호 중인 PLC 정보를 수신하고 무결성을 모니터링합니다.
  - **PLC 프로젝트 무결성 검사**
  - **PLC 프로젝트 조사**
- **온디맨드 검사**: 온디맨드 검사 작업을 관리합니다. 각 작업에는 별도의 노드가 있습니다.
  - **운영 체제 시작 시 검사**
  - **중요 영역 검사**
  - **애플리케이션 무결성 제어**
  - **이동식 드라이브 검사**
  - **전체 검사**
  - 사용자 지정 작업 **<작업 이름>**(해당하는 경우)

  이 노드는 애플리케이션이 설치될 때 생성된 시스템 작업 사용자 정의 작업 및 Kaspersky Security Center를 사용하여 생성되어 보호 중인 장치로 전송된 그룹 온디맨드 검사 작업을 표시합니다.
- **업데이트**: Kaspersky Industrial CyberSecurity for Nodes 데이터베이스와 애플리케이션 모듈의 업데이트를 관리하고 마지막 업데이트를 롤백할 수 있습니다:
  - **데이터베이스 및 애플리케이션 모듈 업데이트**
  - **마지막 업데이트 롤백**
  - **애플리케이션 업데이트**

  이 노드는 Kaspersky Security Center를 이용하여 생성되어 보호 중인 장치로 전송된 모든 사용자 지정 작업과 그룹 업데이트 작업을 표시합니다.
- **저장소**: 백업 설정과 차단된 네트워크 세션 목록을 관리합니다.
  - **백업**
  - **차단된 네트워크 세션**
- **로그 및 알림**: 로컬 작업 로그 및 Kaspersky Industrial CyberSecurity for Nodes 시스템 감사 로그를 관리합니다.
  - **시스템 감사**
  - **산업 네트워크 보호**
  - **애플리케이션 실행 제어**
  - **장치 제어**
  - **애플리케이션 무결성 제어**
  - **로그 검사**

- **시스템 무결성 모니터링**
- **네트워크 위협 보호**
- **온디맨드 검사**
- **방화벽**
- **익스플로잇 방지**
- **Anti-Cryptor**
- **AMSI 스캐너**
- **업데이트**
- **실시간 파일 보호**
- **백업**
- **Endpoint Detection and Response(Industrial CyberSecurity)**

- **라이센스**: Kaspersky Industrial CyberSecurity for Nodes 키를 추가 또는 삭제하고 라이센스 세부 정보를 봅니다.

세부 정보 창

세부 정보 창에서는 선택 노드에 대한 정보를 표시합니다. **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하면 세부 정보 창에 현재 장치 보호 상태 및 Kaspersky Industrial CyberSecurity for Nodes에 대한 정보, 그 기능 구성 요소의 보호 상태, 키 상태 정보가 표시됩니다.

Kaspersky Industrial CyberSecurity for Nodes 노드의 마우스 오른쪽 메뉴

Kaspersky Industrial CyberSecurity for Nodes 노드의 마우스 오른쪽 메뉴 항목을 사용하여 다음 동작을 수행할 수 있습니다.

- **보호 일시 중지**.
- **신뢰 구역**. 신뢰 구역 설정 확인 및 구성.
- **KATA 통합 / KICS for Networks 통합 원격 측정 설정**.
- **이동식 드라이브 검사**. USB 포트를 통해 보호 중인 장치에 연결된 이동식 드라이브의 검사를 구성합니다.
- **애플리케이션 관리를 위한 사용자 접근 권한**. Kaspersky Industrial CyberSecurity for Nodes 기능에 접근할 수 있는 권한을 확인하고 구성합니다.
- **KICS for Nodes Service 관리를 위한 사용자 접근 권한**. Kaspersky Industrial CyberSecurity for Nodes 서비스 관리를 위한 사용자 권한을 보고 구성합니다.

- **저장소**.
- **설정 내보내기**. XML 형식 구성 파일에 애플리케이션 설정을 저장합니다. 애플리케이션 작업의 마우스 오른쪽 메뉴에서 이 동작을 수행할 수도 있습니다.
- **설정 가져오기**. XML 형식의 구성 파일에서 애플리케이션 설정을 가져옵니다. 애플리케이션 작업의 마우스 오른쪽 메뉴에서 이 동작을 수행할 수도 있습니다.
- **새로 고침**. Kaspersky Industrial CyberSecurity for Nodes 콘솔 창의 콘텐츠를 새로 고칩니다. 애플리케이션 작업의 마우스 오른쪽 메뉴에서 이 동작을 수행할 수도 있습니다.
- **애플리케이션 속성**. Kaspersky Industrial CyberSecurity for Nodes 또는 선택한 작업의 설정을 보고 구성합니다. 애플리케이션 작업의 마우스 오른쪽 메뉴에서 이 동작을 수행할 수도 있습니다.

  이렇게 하려면 Kaspersky Industrial CyberSecurity for Nodes 노드의 세부 정보 창에 있는 **애플리케이션 속성** 링크를 사용할 수도 있습니다.

- **도움말**. Kaspersky Industrial CyberSecurity for Nodes 도움말에서 정보를 봅니다. 애플리케이션 작업의 마우스 오른쪽 메뉴에서 이 동작을 수행할 수도 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 작업의 툴바 및 마우스 오른쪽 메뉴

Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 각 작업의 마우스 오른쪽 메뉴 항목을 사용하여 애플리케이션 작업을 관리할 수 있습니다.

마우스 오른쪽 메뉴 항목을 사용하여 다음 동작을 수행할 수 있습니다.

- **다시 시작/일시 중지**. 작업 실행 다시 시작 또는 일시 중지. 이러한 동작을 수행하기 위해 툴바의 버튼을 사용할 수도 있습니다. 이 동작은 실시간 보호 작업과 온디맨드 검사 작업에 사용할 수 있습니다.
- **작업 생성**. 새 사용자 지정 작업을 생성합니다.
- **작업 삭제**. 사용자 지정 작업을 삭제합니다.
- **설정 내보내기 / 설정 가져오기**. 작업 설정을 내보내거나 가져옵니다.
- **속성**. 작업 설정 창을 엽니다.
- **도움말**. 해당 온라인 도움말 항목을 엽니다.

알림 영역의 시스템 트레이 아이콘

Kaspersky Industrial CyberSecurity for Nodes를 설치하면 즉시 애플리케이션 아이콘이 Microsoft Windows 작업 표시줄 알림 영역에 나타납니다.

작업 표시줄 알림 영역의 애플리케이션 아이콘이 숨겨져 있으면 관리자가 정책에서 애플리케이션 인터페이스 표시를 비활성화한 것입니다.

알림 영역 아이콘의 용도는 다음과 같습니다:

- 애플리케이션 활동을 나타냅니다.
- 마우스 오른쪽 메뉴 및 메인 애플리케이션 창에 대한 바로가기 역할을 합니다.

애플리케이션 운영 정보를 표시하기 위해 다음과 같은 애플리케이션 아이콘 상태가 제공됩니다:

- 아이콘은 애플리케이션의 매우 중요한 보호 구성 요소가 작동 중임을 나타냅니다. 사용자가 애플리케이션 업데이트 후 컴퓨터를 다시 시작하는 등의 동작을 수행해야 할 때 Kaspersky Industrial CyberSecurity for Nodes에 경고가 표시됩니다.
- 아이콘은 애플리케이션의 매우 중요한 보호 구성 요소가 비활성화되었거나 오작동했음을 나타냅니다. 라이센스가 만료되었거나 애플리케이션 오류로 인해 보호 구성 요소가 오작동할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes에 컴퓨터 보호 문제에 대한 설명과 함께 경고가 표시됩니다.

시스템 트레이 아이콘을 우클릭하면 마우스 오른쪽 메뉴를 열 수 있습니다.

마우스 오른쪽 메뉴에는 애플리케이션 창을 표시할 수 있는 여러 명령이 있습니다(아래 표 참조).

시스템 트레이 아이콘의 마우스 오른쪽 메뉴 명령

명령	설명
애플리케이션 콘솔 열기	Kaspersky Industrial CyberSecurity for Nodes 콘솔을 엽니다(설치되어 있다면).
간편 진단 인터페이스 열기	간편 진단 인터페이스를 엽니다.
정보	Kaspersky Industrial CyberSecurity for Nodes 정보가 포함된 **정보** 창을 엽니다. Kaspersky Industrial CyberSecurity for Nodes 사용자라면 등록된 **정보** 창에 설치한 긴급 업데이트 정보가 포함됩니다.
숨기기	툴바 알림 영역에서 시스템 트레이 아이콘을 숨깁니다.

숨긴 시스템 트레이 아이콘은 언제든 다시 표시할 수 있습니다.

시스템 트레이 아이콘을 다시 표시하려면,

Microsoft Windows **시작** 메뉴에서, **모든 프로그램** > **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다. 아이콘이 Microsoft Windows 작업 표시줄의 알림 영역에 나타납니다.

설정 이름은 설치한 운영 체제마다 다를 수 있습니다.

애플리케이션 콘솔을 통해 일반 설정 구성

Kaspersky Industrial CyberSecurity for Nodes의 일반 설정 및 오작동 진단 설정은 애플리케이션의 일반 작동 조건을 구성합니다. 이 설정을 통해 Kaspersky Industrial CyberSecurity for Nodes에서 사용하는 작업 프로세스 수를 제어하고, 비정상 종료 후 Kaspersky Industrial CyberSecurity for Nodes 작업을 복구하고, 로그를 유지 관리하고, 비정상 종료 후 Kaspersky Industrial CyberSecurity for Nodes 프로세스의 덤프 파일을 생성하고, 기타 일반 설정을 구성할 수 있습니다.

활성 Kaspersky Security Center 정책이 설정에 대한 변경을 차단한다면 Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 애플리케이션 설정을 구성할 수 없습니다.

Kaspersky Industrial CyberSecurity for Nodes의 일반 설정을 구성하려면:

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 열고 다음 중 하나를 수행합니다:

   - 노드의 결과 창에서 **애플리케이션 속성** 링크를 클릭합니다.
   - 노드의 마우스 오른쪽 메뉴에서 **애플리케이션 속성** 항목을 선택합니다.

   애플리케이션 속성 창이 열립니다.

2. **인터페이스** 탭에서 Kaspersky Industrial CyberSecurity for Nodes 시스템 트레이 아이콘에 표시할 경고를 지정합니다.

3. **보안 설정** 탭에서 다음 설정을 구성합니다:

   - **일반** 섹션에서 **컴퓨터 시작 시 애플리케이션 시작(권장)** 옵션을 구성합니다.
   - **자기 보호**에서 애플리케이션 모듈 보호 및 운영 체제 서비스를 구성합니다.
   - **UPS 백업 전원으로 전환 시 동작** 섹션에서 UPS 전원으로 전환한 후 Kaspersky Industrial CyberSecurity for Nodes에서 생성하는 보호 중인 장치 부하에 대한 제한을 지정합니다.
     - **스케줄 지정된 검사 작업 시작 안 함**.
     - **실행 중인 검사 작업 중단**.
   - **호환성 설정** 섹션에서 **원격 관리 소프트웨어와의 호환성** 설정을 구성합니다.
   - **검사 설정** 섹션에서 검사 작업에 대한 CPU 사용량 제한을 구성하고 다른 애플리케이션에 리소스 양도를 허용합니다.

4. **네트워크 설정** 탭에서 다음 설정을 구성합니다:

   - **프록시 서버** 섹션에서 프록시 서버 설정 지정: 인증 유형 및 프록시 서버 인증에 필요한 세부 정보.
   - **모니터링하는 포트**에서 네트워크 포트 모니터링 옵션을 지정합니다:
     - **모든 네트워크 포트 모니터**. 이 네트워크 포트 모니터링 모드에서는 보호 구성 요소가 컴퓨터의 열린 네트워크 포트를 통해 전송되는 데이터 스트림을 감시합니다.
     - **선택한 네트워크 포트만 모니터**. 이 네트워크 포트 모니터링 모드에서 보호 구성 요소는 컴퓨터의 선택된 포트와 선택한 애플리케이션의 네트워크 활동을 모니터링합니다. 이메일 및 네트워크 트래픽의 전송에 일반적으로 사용되는 네트워크 포트 목록은 Kaspersky 전문가가 권장하는 것으로 구성됩니다. 필요하다면 네트워크 포트 목록을 편집할 수 있습니다.
   - **원격 연결용 포트**에서 필요하다면 애플리케이션 콘솔에서 애플리케이션이 설치된 컴퓨터에 연결하는 데 사용하는 포트를 변경합니다.

     Windows 자격 증명을 사용하여 연결하기 위한 기본 포트 번호는 13032이며, 수동 생성 사용자의 자격 증명을 사용하여 연결하기 위한 기본 포트 번호는 13031입니다. 가능한 포트 번호 범위: 1~65535.

     애플리케이션을 다시 시작할 때까지 이전에 저장한 포트 번호가 사용됩니다.

5. **오작동 진단** 탭에서 **설정** 버튼을 클릭한 후 애플리케이션의 메모리 덤프와 추적 로그를 구성합니다.

6. **확인** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes 설정을 저장했습니다.

Kaspersky Industrial CyberSecurity for Nodes 작업 관리

이 섹션에는 Kaspersky Industrial CyberSecurity for Nodes 작업을 생성과 구성, 시작, 중지하는 방법에 관한 정보가 포함되어 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 작업 카테고리

Kaspersky Industrial CyberSecurity for Nodes에서 실시간 컴퓨터 보호, 컴퓨터 제어, 규칙 자동 생성, 시스템 점검, 온디맨드 검사, 산업 네트워크 보호, 저장소 관리, 업데이트 작업을 사용할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리의 작업 마우스 오른쪽 메뉴와 결과 창을 사용하여 이러한 작업을 관리할 수 있습니다. 결과 창에서 작업 상태 정보를 볼 수 있습니다. 작업 관리는 시스템 감사 로그에 기록됩니다.

Kaspersky Industrial CyberSecurity for Nodes 작업에는 *로컬* 유형과 *그룹* 유형이 있습니다.

로컬 작업

로컬 작업은 로컬 작업이 생성된 보호 중인 장치에서만 실행할 수 있습니다. 시작 방법에 따른 로컬 작업 유형은 다음과 같습니다.

- **로컬 시스템 작업**. 이러한 작업은 Kaspersky Industrial CyberSecurity for Nodes를 설치하는 동안 자동 생성됩니다. *업데이트 롤백* 작업을 제외한 모든 로컬 시스템 작업의 설정을 변경할 수 있습니다. 로컬 시스템 작업은 이름을 변경하거나 삭제할 수 없습니다. 로컬 시스템 및 사용자 지정 온디맨드 검사 작업을 동시에 실행할 수 있습니다.

- **로컬 사용자 지정 작업**. 애플리케이션 콘솔에서 온디맨드 검사 작업, 업데이트 작업, 베이스라인 시스템 무결성 모니터 작업을 생성할 수 있습니다. Kaspersky Security Center에서는 온디맨드 검사 작업, 업데이트 작업 등을 생성할 수 있으며, 사용자 지정 작업의 이름을 바꾸고 구성하고 삭제할 수 있습니다. 여러 사용자 지정 작업을 동시에 실행할 수 있습니다.

그룹 작업

Kaspersky Security Center에서 그룹 작업 및 보호 중인 장치 세트에 대한 작업을 관리할 수 있습니다. 모든 그룹 작업은 사용자 지정 작업입니다. 그룹 작업은 애플리케이션 콘솔에도 표시됩니다. 애플리케이션 콘솔에서는 그룹 작업의 상태만 볼 수 있습니다. 애플리케이션 콘솔로는 그룹 작업을 관리하거나 구성할 수 없습니다.

수동으로 작업 시작, 일시 중지, 다시 시작, 중지

작업을 수동으로 시작, 일시 중지, 재개, 중지할 수 있습니다. 모든 Kaspersky Industrial CyberSecurity for Nodes 작업에서 이 옵션을 사용할 수 있는 것은 아닙니다.

작업을 시작, 일시 중지, 재시작, 중지하려면:

1. 애플리케이션 콘솔에서 작업의 마우스 오른쪽 메뉴를 엽니다.
2. **시작**, **일시 중지** 중 하나의 명령을 선택합니다.

작업이 수행되며 시스템 감사 로그에 기록됩니다.

작업 예약

Kaspersky Industrial CyberSecurity for Nodes Console에서 로컬 시스템 작업 및 사용자 작업의 실행 스케줄을 구성할 수 있습니다. 그러나 그룹 작업의 실행 스케줄은 구성할 수 없습니다.

작업을 스케줄하려면:

1. 콘솔 트리에서 스케줄을 구성할 작업을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.
3. 창이 열리면 **실행 모드** 섹션에서 다음 동작 중 하나를 수행합니다.
   - 원하는 시간에 작업을 수동으로 실행하려면 **수동** 체크박스를 선택합니다.
   - 예약된 작업 시작 설정을 사용하려는 경우 **스케줄에 따라** 확인란을 선택합니다.
4. **스케줄에 따라** 옵션을 선택한 경우 작업 스케줄 설정을 구성합니다(아래 표 참조).
5. 필요하다면 **다음 계정으로 작업 실행** 확인란을 선택하고 작업을 실행할 사용자 계정의 자격 증명을 지정합니다.
6. **확인** 버튼을 클릭합니다.

작업 스케줄 설정이 저장됩니다.

작업 스케줄 설정

파라미터	설명
실행 모드	작업 실행 모드를 선택합니다: • **분**. 작업이 몇 분마다 주기적으로 실행됩니다. 작업 시작 시간과 분 단위의 주기를 지정합니다. • **시간**. 작업이 몇 시간마다 주기적으로 실행됩니다. 작업 시작 시간과 시간 단위의 주기를 지정합니다. • **일**. 작업이 며칠마다 주기적으로 실행됩니다. 작업 시작 시간과 일 단위의 주기를 지정합니다. • **주**. 작업이 지정된 요일에 지정된 주 수 간격으로 실행됩니다. 스케줄을 지정하고 체크박스를 사용하여 작업을 실행할 요일을 선택한 다음 작업 시작 시간을 지정합니다. • **매달**. 작업이 매월 특정 일자에 실행됩니다. 시작 날짜와 시간을 지정합니다. • **지정한 시간**. 작업이 지정된 날짜와 시간에 한 번 실행됩니다. • **업데이트 후**. 저장소에서 업데이트가 다운로드될 때마다 작업이 실행됩니다. • **애플리케이션 시작 후**. 작업은 Kaspersky Industrial CyberSecurity for Nodes가 시작될 때마다 수행됩니다.

파라미터	설명
누락된 작업 실행	이 확인란을 선택하면, Kaspersky Industrial CyberSecurity for Nodes는 작업이 가능하자 마자 건너뛴 작업을 시작합니다. 스케줄된 작업 시작 시각에 컴퓨터가 꺼져 있는 등의 경우에는 작업을 건너뜁니다. 애플리케이션에 누락된 작업을 실행할 기회가 있다면 특정 시간 내에 무작위로 작업을 실행하여 컴퓨터의 로드를 분산합니다. 이 확인란을 선택 취소하면 Kaspersky Industrial CyberSecurity for Nodes가 건너뛴 작업을 실행하지 않습니다. 대신, 현재 스케줄에 따라 다음 작업을 실행합니다.
자동으로 작업 시작 임의 지연 사용	이 확인란을 선택하면 작업이 반드시 스케줄된 시간에 실행되는 것이 아니라, 일정 간격 내에서 무작위로 실행됩니다. 즉, 작업 시작 시간이 분산됩니다. 무작위 시작 시간은 스케줄에 따라 작업이 실행될 때, 중앙 관리 서버에 다수의 컴퓨터가 동시에 접근하는 것을 방지하는 데 도움이 됩니다. 무작위 시작 시간 범위는 작업이 할당된 컴퓨터 수에 따라 작업 생성 시 자동 계산됩니다. 결과적으로 작업은 항상 계산된 시작 시간에 실행됩니다. 그러나 계산된 시작 시간은 작업 설정을 수정하거나 작업을 수동으로 실행할 때마다 변경됩니다. 확인란의 선택을 취소하면 작업이 정확히 스케줄된 시간에 실행됩니다.
다음 간격으로 작업 시작 임의 지연(분)	이 확인란을 선택하면 작업이 특정 시간 범위 내에서 임의의 시간에 컴퓨터에서 실행됩니다. 무작위 시작 시간은 스케줄에 따라 작업이 실행될 때, 중앙 관리 서버에 다수의 컴퓨터가 동시에 접근하는 것을 방지하는 데 도움이 됩니다. 확인란의 선택을 취소하면 작업이 정확히 스케줄된 시간에 실행됩니다.
작업 일시 중지	이전에 스케줄된 작업의 실행을 일시 중지할 시간 간격을 지정할 수 있습니다. 지정한 기간이 지나면 작업이 다시 시작됩니다. 이는 예를 들어 사용량이 가장 많은 기간에 Kaspersky Industrial CyberSecurity for Nodes가 컴퓨터 성능에 미치는 영향을 최소화하기 위해 필요할 수 있습니다. 이 기능은 온디맨드 검사 작업에만 사용할 수 있습니다.
다음부터 스케줄 비활성화	이 체크박스를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 지정한 날짜부터 스케줄된 작업의 실행을 중지합니다. 해당 작업은 **수동** 모드로 설정됩니다. 이 기능은 온디맨드 검사 작업에만 사용할 수 있습니다.

사용자 계정을 사용하여 작업 시작

시스템 계정으로 작업을 시작하거나 다른 계정을 지정할 수 있습니다.

계정을 사용한 작업 시작 정보

계정을 지정하여 다음 Kaspersky Industrial CyberSecurity for Nodes 작업을 실행할 수 있습니다.

- *애플리케이션 실행 제어를 위한 규칙 생성기*
- *장치 제어를 위한 규칙 생성기*
- *로그 검사*
- *애플리케이션 무결성 제어*
- *업데이트.*

이러한 작업은 기본적으로 시스템 계정 권한을 사용하여 실행됩니다.

다음의 경우 적절한 접근 권한이 있는 다른 계정을 사용하도록 권장합니다.

- *업데이트* 작업의 경우:
  - 네트워크에 있는 다른 컴퓨터의 공유 폴더를 업데이트 경로로 지정한 경우.
  - 업데이트 경로에 접근하기 위해 NTLM 또는 Kerberos 인증이 있는 프록시 서버를 사용하는 경우.
- *애플리케이션 실행 제어를 위한 규칙 생성기* 작업의 경우: 생성된 규칙을 시스템 계정이 접근할 수 없는 구성 파일로 내보내는 경우(예: 보호 중인 장치의 공유 폴더).

시스템 계정 권한으로 나열된 작업을 시작할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 이러한 작업을 수행하고 네트워크에서 보호 중인 장치와 같은 도메인에 등록된 다른 장치가 있다면 해당 장치의 공유 폴더에 접근합니다. 이 경우, 시스템 계정에 해당 폴더에 대한 접근 권한이 있어야 합니다. Kaspersky Industrial CyberSecurity for Nodes는 **<도메인 이름 \ 장치_이름>** 계정에 대한 권한을 사용하여 장치에 접근합니다.

작업을 시작할 사용자 계정 지정

일부 작업에서는 애플리케이션 콘솔에서 계정을 지정하는 옵션을 사용할 수 없습니다.

작업을 시작할 계정을 지정하려면:

1. 애플리케이션 콘솔 트리에서 특정 계정의 권한으로 시작할 작업을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.
   속성: <작업 이름> 창이 열립니다.
3. **실행 모드** 탭으로 이동하고 다음을 수행합니다.
   a. **다음 계정으로 작업 실행** 확인란을 선택합니다.
   b. 사용하려는 계정의 사용자 이름과 암호를 입력합니다.

   선택한 사용자는 보호 중인 장치나 이 컴퓨터와 같은 도메인에 등록되어 있어야 합니다.
4. **확인**을 누릅니다.

설정 가져오기 및 내보내기

이 섹션에서는 Kaspersky Industrial CyberSecurity for Nodes 설정을 내보내는 방법을 설명합니다. 또한 특정 애플리케이션 구성 요소의 설정을 XML 구성 파일로 내보내는 방법과 이러한 설정을 구성 파일에서 애플리케이션으로 다시 가져오는 방법을 알아봅니다.

설정 가져오기 및 내보내기 정보

Kaspersky Industrial CyberSecurity for Nodes 설정을 XML 구성 파일로 내보내고 구성 파일에서 Kaspersky Industrial CyberSecurity for Nodes로 설정을 가져올 수 있습니다. 모든 애플리케이션 설정 또는 개별 구성 요소에 대한 설정만을 구성 파일에 저장할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes의 모든 설정을 파일로 내보내는 경우, 일반 애플리케이션 설정과 다음 Kaspersky Industrial CyberSecurity for Nodes 컴퓨터 구성 요소 및 기능의 설정이 저장됩니다.

- 실시간 파일 보호
- 익스플로잇 방지
- 네트워크 위협 보호
- Anti-Cryptor
- 복원 엔진
- AMSI 스캐너
- 애플리케이션 실행 제어
- 장치 제어
- 방화벽
- 애플리케이션 실행 제어를 위한 규칙 생성기
- 장치 제어를 위한 규칙 생성기
- 로그 검사
- 시스템 무결성 모니터링
- PLC 프로젝트 무결성 검사
- PLC 프로젝트 조사
- 운영 체제 시작 시 검사
- 중요 영역 검사
- 애플리케이션 무결성 제어
- 이동식 드라이브 검사
- 전체 검사
- 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트

- 마지막 업데이트 롤백
- 업데이트

사용자 계정 권한을 비롯한 Kaspersky Industrial CyberSecurity for Nodes의 일반 설정을 파일에 저장할 수 있습니다.

내보내기를 수행할 때 Kaspersky Security Center 정책이 활성화되어 있으면 애플리케이션은 해당 정책에서 사용하는 지정된 값을 내보냅니다.

그룹 작업 설정은 내보낼 수 없습니다.

Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션에서 사용하는 모든 암호(작업 실행 또는 프록시 서버 연결을 위한 사용자 계정 설정)를 내보냅니다. 내보낸 암호는 구성 파일에 암호화된 형식으로 저장됩니다. 재설치나 업데이트를 하지 않았다면 이 보호 중인 장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes를 통해서만 암호를 내보낼 수 있습니다.

다른 보호 중인 장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes를 사용하여 이전에 저장한 암호를 가져올 수는 없습니다. 다른 보호 중인 장치로 설정을 가져온 후에는 모든 암호를 직접 입력해야 합니다.

설정을 내보낼 때 **중요 작업을 확인하기 위한 암호 요청** 기능이 활성화되어 있으면 장치에 설정된 암호가 내보내지며, 다른 장치에서 설정을 가져올 때 자동으로 적용됩니다.

개별 Kaspersky Industrial CyberSecurity for Nodes 구성 요소에 대한 설정이 포함된 구성 파일에서 설정을 가져올 수 있습니다(예: 완료되지 않은 구성 요소 집합이 있는 Kaspersky Industrial CyberSecurity for Nodes가 설치한 파일에서). 설정을 가져온 후에는 구성 파일에 포함되어 있던 Kaspersky Industrial CyberSecurity for Nodes 설정만 변경됩니다. 기타 모든 설정은 그대로 유지됩니다.

차단된 Kaspersky Security Center의 활성 정책 설정은 설정을 가져올 때 변경되지 않습니다.

설정 내보내기

설정을 구성 파일로 내보내려면:

1. 모든 Kaspersky Industrial CyberSecurity for Nodes 설정을 내보내려면 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 마우스 오른쪽 메뉴에서 **설정 내보내기** 옵션을 선택합니다.

   개별 구성 요소의 설정을 내보내려면 **설정 내보내기**를 클릭합니다.

   Kaspersky Security Network 설정을 내보낼 수 없습니다. Kaspersky Security Network를 수동으로 구성해야 합니다.

2. 창이 열리면 설정 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

   경로 지정 시 시스템 환경 변수를 사용할 수 있지만 사용자 환경 변수는 사용할 수 없습니다.

   내보내기를 수행할 때 Kaspersky Security Center 정책이 활성화되어 있으면 애플리케이션은 해당 정책에서 사용하는 설정 값을 내보냅니다.

3. 파일을 저장합니다.

4. **설정 내보내기를 완료했습니다** 창의 **확인** 버튼을 클릭합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 설정 목록을 XML 파일로 내보냅니다.

신뢰하는 애플리케이션 목록을 내보내려면 다음을 수행합니다.

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 마우스 오른쪽 메뉴를 엽니다.
2. **신뢰 구역 설정 구성** 옵션을 선택합니다.
3. **신뢰 구역 설정 구성** 창이 열립니다.
4. **신뢰하는 애플리케이션** 섹션으로 가서 **설정**을 클릭합니다.

   신뢰하는 애플리케이션 목록이 포함된 창이 열립니다.
5. 내보낼 신뢰하는 애플리케이션을 선택합니다.

   신뢰하는 애플리케이션을 선택하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 신뢰하는 애플리케이션을 모두 내보냅니다.
6. 화살표를 클릭하고 드롭다운 목록에서 **내보내기** 옵션을 선택합니다.
7. 창이 열리면 신뢰하는 애플리케이션 목록을 내보낼 XML 파일의 이름을 입력하고 이 파일을 저장할 폴더를 선택합니다.
8. 파일을 저장합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 애플리케이션 목록을 XML 파일로 내보냅니다.

명령줄을 사용하여 Kaspersky Industrial CyberSecurity for Nodes 설정을 내보낼 수도 있습니다.

설정 가져오기

저장된 구성 파일에서 설정을 가져오려면:

1. Kaspersky Industrial CyberSecurity for Nodes 설정을 모두 가져오려면 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 컴퓨터의 마우스 오른쪽 메뉴에서 **설정 가져오기** 명령을 선택합니다.

   개별 구성 요소의 설정을 가져오려면 결과 창에서 **설정 가져오기**를 클릭합니다.

   > 전반적인 Kaspersky Industrial CyberSecurity for Nodes 설정이나 그 기능 구성 요소 설정을 보호 중인 장치로 가져온 후에는 이전 설정으로 되돌릴 수 없습니다.

   > Kaspersky Security Network 설정을 가져올 수 없습니다. Kaspersky Security Network를 수동으로 구성해야 합니다.
2. 표시된 창에서 설정을 가져올 XML 구성 파일을 선택하고 **열기**를 클릭합니다.

3. **설정 가져오기를 완료했습니다** 창의 **확인** 버튼을 클릭합니다.

4. 애플리케이션 콘솔 툴바에서 **업데이트** 버튼을 클릭합니다.

   애플리케이션 콘솔 창에 가져온 설정이 표시됩니다.

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Industrial CyberSecurity for Nodes를 재설치하거나 업데이트한 후에 다른 보호 중인 장치나 같은 보호 중인 장치에 생성한 파일에서 암호(작업 시작 또는 프록시 서버 연결을 위한 계정 정보)를 가져오지 않습니다. 가져오기가 완료되면 암호를 직접 입력해야 합니다.

신뢰하는 애플리케이션 목록을 가져오려면:

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 마우스 오른쪽 메뉴를 엽니다.

2. **신뢰 구역 설정 구성** 옵션을 선택합니다.

3. **신뢰 구역 설정 구성** 창이 열립니다.

4. **신뢰하는 애플리케이션** 섹션으로 가서 **설정**을 클릭합니다.

5. 화살표를 클릭하고 드롭다운 목록에서 **가져오기** 옵션을 선택합니다.

6. 창이 열리면 신뢰하는 애플리케이션 목록을 가져올 XML 파일을 선택합니다.

7. 파일을 엽니다.

   컴퓨터에 이미 신뢰하는 애플리케이션 목록이 있는 경우 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. **신뢰하는 애플리케이션** 탭에 목록이 표시됩니다. **확인** 버튼을 클릭합니다.

보호 상태 및 Kaspersky Industrial CyberSecurity for Nodes 정보 보기

장치 보호 상태 Kaspersky Industrial CyberSecurity for Nodes 정보를 보려면,

Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리의 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택합니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes 콘솔의 세부 정보 창에 포함된 정보는 자동으로 새로 고쳐집니다.

- 로컬 연결의 경우 10초마다.
- 원격 연결의 경우 15초마다.

수동으로 정보를 새로 고칠 수 있습니다.

*수동으로 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 정보를 새로 고치려면,*

Kaspersky Industrial CyberSecurity for Nodes 노드의 마우스 오른쪽 메뉴에서 **새로 고침** 명령을 선택합니다.

다음 애플리케이션 정보가 Kaspersky Industrial CyberSecurity for Nodes 콘솔의 세부 정보 창에 표시됩니다.

- Kaspersky Security Network 사용 상태.
- 장치 보호 상태.
- 데이터베이스 및 애플리케이션 모듈 업데이트 정보.
- 실제 진단 데이터.
- 보호 중인 장치 제어 작업에 관한 데이터.
- 라이센스 정보.
- 산업 네트워크 보호 상태.
- Kaspersky Security Center와의 통합 상태: 애플리케이션이 연결되고 Kaspersky Security Center가 설치된 서버의 세부사항, 활성 정책에서 제어하는 애플리케이션 작업 정보.

보호 상태를 표시하기 위해 색 구분이 사용됩니다.

- *초록색*. 구성된 설정에 따라 작업이 실행 중입니다. 보호가 활성 상태입니다.
- *노란색*. 작업이 시작되지 않았거나 일시 중지되었거나 중지되었습니다. 보안 위협이 있을 수 있습니다. 작업을 구성하고 시작하는 것이 좋습니다.
- *빨간색*. 작업이 완료되었지만 오류가 있거나 작업을 실행하는 동안 보안 위협이 탐지되었습니다. 작업을 시작하거나 탐지된 보안 위협을 제거하는 조치를 수행하는 것이 좋습니다.

이 블록에 있는 일부 세부사항(예: 작업 이름 또는 탐지한 위협 수)은 클릭하면 관련 작업 노드로 연결되거나 작업 로그를 여는 링크입니다.

KSN 사용 섹션은 *실행 중*, *중지됨*, *수행 안 함* 등으로 현재 작업 상태를 표시합니다. 표시기에서 사용되는 값은 다음과 같습니다.

- 초록색 패널 - **KSN 사용** 작업이 실행 중이며 상태에 대한 파일 요청이 KSN으로 전송되고 있음을 나타냅니다.
- 노란색 패널 - 진술문 중 하나를 수락했지만 작업이 실행 중이지 않거나, 작업이 실행 중이지만 파일 요청이 KSN으로 전송되지 않습니다.
- 빨간색 패널 - 작업이 실패했습니다.

컴퓨터 보호

컴퓨터 보호 섹션(아래 표 참조)에는 장치의 현재 보호 상태 정보가 표시됩니다.

장치 보호 상태 정보

보호 섹션	정보
장치 보호 상태 표시기	섹션 이름이 있는 패널의 색상은 섹션에서 수행 중인 작업의 상태를 반영합니다. 표시기에서 사용되는 값은 다음과 같습니다. • 초록색 패널 - 기본적으로 표시되며 실시간 파일 보호 구성 요소가 설치되어 있고 작업이 실행 중임을 나타냅니다. • 노란색 패널 - 실시간 파일 보호 구성 요소가 설치되지 않았으며 오랫동안 *중요 영역 검사* 작업이 수행되지 않았음을 의미합니다. • 빨간색 패널 - 실시간 파일 보호 작업을 실행 중이지 않습니다.
실시간 파일 보호	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태.
중요 영역 검사	**마지막 검사 날짜** – 바이러스 및 기타 컴퓨터 보안 위협에 대해 마지막 중요 영역 검사를 수행한 날짜 및 시간. *수행 안 함* – *중요 영역 검사* 작업이 30일 이상 수행되지 않으면 발생하는 이벤트(기본값). 이 이벤트가 생성되는 한계값은 변경할 수 있습니다.
네트워크 위협 보호	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태.
익스플로잇 방지	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태. **작업 모드** – 익스플로잇 방지에 사용 가능한 두 가지 모드 중 하나: **차단** 또는 **알림**.
Anti-Cryptor	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태. **작업 모드** – Anti-Cryptor 구성 요소에 가능한 세 가지 모드 중 하나: **삭제**, **차단**, 또는 **알림**.

업데이트

업데이트 섹션(아래 표 참조)에는 데이터베이스 및 애플리케이션 모듈의 상태 정보가 표시됩니다.

Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 모듈의 상태 정보

업데이트 섹션	정보
데이터베이스 및 애플리케이션 모듈의 상태 표시기	섹션 이름이 포함된 패널의 색상은 애플리케이션 데이터베이스 및 애플리케이션 모듈의 상태를 반영합니다. 표시기에서 사용되는 값은 다음과 같습니다. • 초록색 패널 - 기본적으로 표시되며 애플리케이션 데이터베이스가 최신 상태이며 마지막 데이터베이스 및 모듈 업데이트 작업이 완료되었음을 나타냅니다. • 노란색 패널 - 데이터베이스가 오래되었거나 마지막 데이터베이스 및 모듈 업데이트 작업이 실패했음을 나타냅니다. • 빨간색 패널 - *데이터베이스가 매우 오래됨* 또는 *데이터베이스가 최신입니다* 이벤트가 발생했습니다.
데이터베이스 상태	이 옵션은 다음과 같을 수 있습니다. • **데이터베이스가 최신입니다** – 애플리케이션 데이터베이스가 7일(기본값) 이내에 업데이트되었습니다. • **데이터베이스가 오래됨** – 애플리케이션 데이터베이스가 7일~14일(기본값) 전에 업데이트되었습니다. • **데이터베이스가 매우 오래됨** – 애플리케이션 데이터베이스가 업데이트된지 14일(기본값) 이상 지났습니다. *데이터베이스가 오래됨* 및 *데이터베이스가 매우 오래됨* 이벤트 생성 한계값을 변경할 수 있습니다.
데이터베이스 배포 날짜	최신 데이터베이스 업데이트의 릴리스 날짜와 시간. 날짜와 시간은 UTC 형식으로 지정됩니다.
가장 최근에 완료된 데이터베이스 업데이트 작업 상태	최신 데이터베이스 업데이트의 날짜와 시간. 보호 중인 장치의 로컬 시간에 따라 날짜 및 시간이 지정됩니다. 필드 값은 *실패했습니다* 이벤트가 발생하면 빨간색이 됩니다.

제어

제어 섹션(아래 표 참조)이 애플리케이션 실행 제어, 장치 제어, 방화벽 관리 작업의 정보를 표시합니다.

보호 중인 장치 제어 상태 정보

제어 섹션	정보
보호 중인 장치 제어 상태 표시기	섹션 이름이 있는 패널의 색상은 섹션에서 수행 중인 작업의 상태를 반영합니다. 표시기에서 사용되는 값은 다음과 같습니다. • 초록색 패널 - 기본적으로 표시되며 모든 애플리케이션 실행 제어 구성 요소가 설치되어 있고 작업이 활성 모드에서 실행 중임을 나타냅니다. 익스플로잇 방지 기능이 설치되었고 활성 상태입니다. • 다음 조건 중 하나 이상에서는 패널이 노란색입니다: 익스플로잇 방지가 실행되고 있지 않습니다, 애플리케이션 실행 제어가 알림 모드로 실행 중입니다, 익스플로잇 방지가 활성 모드로 실행 중이며 애플리케이션 실행 제어가 실행 중이 아니거나 실패했습니다. • 빨간색 패널 - 애플리케이션 실행 제어 작업이 실행 중이 아니거나 실패했으며, 익스플로잇 방지가 실행 중이지 않거나 **알림** 모드입니다.
애플리케이션 실행 제어	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태. **작업 모드** – 애플리케이션 실행 제어 작업에 사용할 수 있는 두 모드 중 하나: **알림** 또는 **차단**.
장치 제어	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태. **작업 모드** – 장치 제어 작업에 사용 가능한 두 가지 모드 중 하나: **규칙에 따라** 또는 **알림**.
방화벽	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태.

진단

진단 섹션(아래 표 참조)에는 시스템 무결성 모니터링 및 로그 검사 작업 정보가 표시됩니다.

시스템 점검 상태에 관한 정보

진단 섹션	정보
진단 상태 표시기	섹션 이름이 있는 패널의 색상은 섹션에서 수행 중인 작업의 상태를 반영합니다. 표시기에서 사용되는 값은 다음과 같습니다. • 녹색 – 기본적으로 표시되며 시스템 점검 구성 요소가 둘 중 하나 또는 둘 다 설치되었고 작업이 실행 중임을 나타냅니다. • 노란색 - 두 구성 요소가 모두 설치되었지만 시스템 점검 작업 중 하나가 실행되고 있지 않습니다. *실행 중이 아님* 이벤트가 발생합니다. • 빨간색 - 작업 중 하나가 실패했습니다.
시스템 무결성 모니터링	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태.
로그 검사	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태.

산업 네트워크 보호 탭

PLC 프로젝트 조사 섹션에는 보호 범위에 포함된 PLC 목록 정보가 표시됩니다.

PLC 데이터 수신 정보

PLC 프로젝트 조사 섹션	정보
보호 영역 내의 PLC 상태 표시기	섹션 이름이 있는 패널의 색상은 섹션에서 수행 중인 작업의 상태를 반영합니다. 표시기에서 사용되는 값은 다음과 같습니다. • 녹색 - 작업이 한 번 이상 성공적으로 완료되었음을 의미합니다. • 노란색 - 검사를 수행한 적이 없음을 나타냅니다. • 빨간색 - 작업이 실패했습니다.
PLC 프로젝트 조사	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태.

PLC 프로젝트 무결성 검사 섹션에는 보호 중인 PLC의 수와 무결성 위반 이벤트 정보가 표시됩니다.

PLC 프로젝트 무결성 검사 작업 정보

PLC 프로젝트 무결성 검사 섹션	정보
PLC 무결성 상태 표시기	섹션 이름이 있는 패널의 색상은 섹션에서 수행 중인 작업의 상태를 반영합니다. 표시기에서 사용되는 값은 다음과 같습니다. • 녹색 - 작업이 한 번 이상 성공적으로 완료되었음을 의미합니다. • 노란색 - 무결성 검사를 수행하지 않았음을 의미합니다. • 빨간색 - 작업이 실패했습니다.
PLC 프로젝트 무결성 검사	**상태** – *실행 중* 또는 *사용 안 함* 등과 같은 구성 요소의 현재 상태.

Kaspersky Industrial CyberSecurity for Nodes 노드의 세부 정보창 왼쪽 아래의 열에 Kaspersky Industrial CyberSecurity for Nodes 라이센스 정보가 표시됩니다.

애플리케이션 속성 링크를 따라 Kaspersky Industrial CyberSecurity for Nodes 속성을 구성할 수 있습니다.

원격 컴퓨터에 연결 링크를 따라 다른 보호 중인 장치에 연결할 수 있습니다.

애플리케이션 콘솔에서 백업 설정을 구성하는 방법

일반 백업 설정을 구성하려면 다음 단계를 따릅니다.

1. **Kaspersky Industrial CyberSecurity for Nodes** 노드의 마우스 오른쪽 메뉴에 있는 애플리케이션 콘솔 트리에서 **저장소** 링크를 클릭합니다.

2. 아래 표에서 설명한 설정을 구성합니다.

저장소 설정

파라미터	설명
리포트 탭에서 리포트 설정을 구성합니다.	
리포트 저장 기간	이 확인란을 선택하면 최대 리포트 저장 기간이 정의한 시간 간격으로 제한됩니다. 리포트 최대 저장 기간의 기본값은 30일입니다. 이 기간이 지나면 Kaspersky Industrial CyberSecurity for Nodes가 리포트 파일에서 가장 오래된 항목을 자동으로 삭제합니다.
리포트 파일 크기 제한	이 확인란을 선택하면 최대 리포트 파일 크기가 정의된 값으로 제한됩니다. 최대 파일 크기의 기본값은 1024MB입니다. Kaspersky Industrial CyberSecurity for Nodes는 리포트 파일 크기가 최대한도에 도달하면 리포트 파일에서 가장 오래된 항목을 자동으로 삭제하여 최대한도를 넘지 않도록 관리합니다.
백업 탭에서 백업 설정을 지정합니다.	
개체 저장 기간	이 확인란을 선택하면 최대 파일 저장 기간이 정의한 시간 간격으로 제한됩니다. 파일 최대 저장 기간의 기본값은 30일입니다. 최대 저장 기간이 만료되면 Kaspersky Industrial CyberSecurity for Nodes가 백업에서 가장 오래된 파일을 삭제합니다.
백업 크기를 다음으로 제한	이 확인란을 선택하면 최대 저장소 크기가 정의된 값으로 제한됩니다. 최대 크기 기본값은 400MB입니다 Kaspersky Industrial CyberSecurity for Nodes는 저장소 크기가 최대한도에 도달하면 저장소에서 가장 오래된 파일을 자동으로 삭제하여 최대 저장소 크기를 넘지 않도록 관리합니다.
이용 가능 공간의 임계값	이 확인란은 백업의 최소 여유 공간(기본값: 100MB)을 모니터링하는 기능을 활성화 또는 비활성화합니다. 여유 공간이 지정된 한계값 아래로 줄어들면 Kaspersky Industrial CyberSecurity for Nodes는 *백업 여유 공간 한계값 초과* 이벤트를 로깅하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. 이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 백업의 여유 공간을 모니터링합니다. **백업 크기를 다음으로 제한** 확인란을 선택했다면 **이용 가능 공간의 임계값** 확인란이 활성화됩니다.

웹 콘솔에서 웹 플러그인 작업

이 섹션에서는 웹 콘솔용 Kaspersky Industrial CyberSecurity for Nodes 관리 플러그인에 대한 정보를 제공하고 단일 보호 중인 장치 또는 보호 중인 장치 그룹에 설치된 애플리케이션 관리 방법을 설명합니다.

웹 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 관리

Kaspersky Industrial CyberSecurity for Nodes 웹 플러그인을 사용하여 Kaspersky Industrial CyberSecurity for Nodes가 설치되어 있고 관리 그룹에 가입된 여러 보호 중인 장치를 중앙에서 관리할 수 있습니다. Kaspersky Security Center 웹 콘솔은 관리 그룹에 포함된 보호된 보호 중인 각 장치의 설정을 별도로 구성할 수 있게도 합니다.

*관리 그룹*은 Kaspersky Security Center 웹 콘솔에서 직접 생성됩니다. 이 그룹에는 Kaspersky Industrial CyberSecurity for Nodes가 설치된 장치가 여러 대 있어, 제어 및 보호 설정을 같게 구성할 수 있습니다. 관리 그룹 사용에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

보호 중인 장치의 Kaspersky Industrial CyberSecurity for Nodes 작업이 활성 Kaspersky Security Center 정책으로 제어된다면, 단일 보호 중인 장치에 대한 애플리케이션 설정을 사용할 수 없습니다.

Kaspersky Industrial CyberSecurity for Nodes는 다음과 같은 방법으로 Kaspersky Security Center 웹 콘솔에서 관리할 수 있습니다.

- **Kaspersky Security Center 정책 사용**. Kaspersky Security Center 정책은 장치 그룹에 대해 같은 보호 설정을 원격 구성하는 데 사용할 수 있습니다. 활성 정책에서 지정된 작업 설정은 애플리케이션 콘솔에서 로컬로 구성되거나 Kaspersky Security Center 웹 콘솔의 속성: <보호 중인 장치 이름> 창에서 원격 구성된 작업 설정보다 우선합니다. 정책을 사용하여 일반 애플리케이션 설정, 실시간 컴퓨터 보호 작업 설정, 장치의 활동 제어 작업, 네트워크 저장소 보호 작업, 스케줄에 따른 로컬 시스템 작업 시작 설정을 구성할 수 있습니다.

- **Kaspersky Security Center 그룹 작업 사용**. Kaspersky Security Center 그룹 작업을 통해 장치 그룹에 대해 만료 기간이 있는 작업의 공통 설정을 원격 구성할 수 있습니다. 그룹을 사용하여 애플리케이션을 활성화하고, 온디맨드 검사 작업 설정을 구성하고 작업 설정 및 애플리케이션 실행 제어를 위한 규칙 생성기을 업데이트할 수 있습니다.

- **장치 세트에 작업 사용**. 장치 세트에 대한 작업을 사용하면, 관리 그룹에 속하지 않은 보호 중인 장치에 대해 실행 기간이 정해진 일반 작업 설정을 원격 구성할 수 있습니다.

- **단일 장치의 속성 창 사용**. 장치 속성 창에서 관리 그룹에 포함된 단일 보호 중인 장치에 대한 작업 설정을 원격 구성할 수 있습니다. 선택한 보호 중인 장치가 활성 Kaspersky Security Center 정책으로 제어되지 않는다면, 일반 애플리케이션 설정 및 Kaspersky Industrial CyberSecurity for Nodes 작업 전체의 설정을 모두 구성할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서는 애플리케이션 설정 및 고급 기능을 구성하고 로그 및 알림 작업을 수행할 수 있습니다. 보호 중인 장치 그룹 및 보호 중인 개별 장치에 대해 이러한 설정을 구성할 수 있습니다.

웹 플러그인 제한 사항

Kaspersky Industrial CyberSecurity for Nodes 웹 플러그인은 Kaspersky Industrial CyberSecurity for Nodes 관리 플러그인과 비교하여 다음 제한 사항이 있습니다.

- 애플리케이션 실행 제어 구성 요소 규칙은 디지털 인증서 또는 Kaspersky Security Center 이벤트를 사용하여 생성할 수 없습니다.
- 장치 제어 구성 요소 규칙은 연결된 장치 또는 시스템 데이터를 기반으로 생성할 수 없습니다.

애플리케이션 설정 관리

이 섹션에는 Kaspersky Security Center 웹 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes의 일반 설정을 구성하는 방법에 대한 정보가 포함되어 있습니다.

웹 플러그인에서 일반 애플리케이션 설정 구성

웹 플러그인에서 보호 중인 장치 그룹 또는 보호 중인 장치 1대를 대상으로 Kaspersky Industrial CyberSecurity for Nodes 일반 설정을 구성할 수 있습니다.

웹 플러그인에서 인터페이스 및 검사 설정 구성

애플리케이션 인터페이스 설정을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. 구성할 정책 이름을 클릭합니다.
3. **<정책 이름>** 창이 열리면 **애플리케이션 설정** 탭을 선택합니다.
4. **애플리케이션 설정** 섹션을 선택합니다.
5. **인터페이스 설정** 하위 섹션에서 **구성** 버튼을 클릭합니다.
6. 아래 표에서 설명한 설정을 구성합니다.

사용자 상호 작용 설정 및 검사 설정

파라미터	설명
사용자와의 상호 작용	**사용자 인터페이스 표시 안 함**. 클라이언트 컴퓨터에 Kaspersky Industrial CyberSecurity for Nodes 동작의 어떤 징후도 표시되지 않습니다. Windows 알림 영역의 아이콘과 알림을 사용할 수 없습니다. **사용자 인터페이스 표시**. 클라이언트 컴퓨터의 Windows 트레이에서 아이콘을 사용할 수 있습니다. 아이콘의 마우스 오른쪽 메뉴에서 사용자는 Kaspersky Industrial CyberSecurity for Nodes로 작업을 수행할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes에서도 애플리케이션 아이콘 위에 알림을 표시합니다. Windows 시스템 트레이에 있는 아이콘의 마우스 오른쪽 메뉴를 사용하여 간편 진단 인터페이스를 열 수 있습니다. 간편 진단 인터페이스의 링크를 클릭하면 애플리케이션 콘솔이 열립니다.
알림 영역에 애플리케이션 상태 표시	Microsoft Windows 알림 영역에 알림을 표시할 이벤트 카테고리 옆의 확인란을 선택합니다.

웹 플러그인에서 보안 및 신뢰성 설정 구성

보안 설정을 수동으로 구성하려면 다음 단계를 수행합니다.

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. 구성할 정책 이름을 클릭합니다.
3. **<정책 이름>** 창이 열리면 **애플리케이션 설정** 탭을 선택합니다.
4. **애플리케이션 설정** 섹션을 선택합니다.
5. **보안 및 신뢰성** 하위 섹션에서 **구성** 버튼을 클릭합니다.
6. 아래 표에서 설명한 설정을 구성합니다.

보안 및 신뢰성 설정

파라미터	설명
컴퓨터 시작 시 애플리케이션 시작(권장)	이 확인란을 선택하면 운영 체제가 로드된 후 Kaspersky Industrial CyberSecurity for Nodes가 시작되어 전체 세션 동안 컴퓨터를 보호합니다. 이 확인란을 선택 해제하면 운영 체제가 로드된 후 사용자가 수동으로 시작할 때까지 Kaspersky Industrial CyberSecurity for Nodes가 시작되지 않습니다. 컴퓨터 보호는 중단되며, 사용자 데이터는 위협에 노출 될 수 있습니다.
외부 위협으로부터 애플리케이션 프로세스 보호	이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 하드 드라이브의 애플리케이션 파일, 메모리 프로세스 및 시스템 레지스트리의 항목에 대한 변경이나 삭제를 방지합니다.
운영 체제 서비스 보호하기	운영 체제 서비스 보호를 활성화하면 타사 애플리케이션이 운영 체제의 프로세스를 작동할 수 없습니다. 운영 체제 서비스 보호가 비활성화되면 타사 애플리케이션이 운영 체제의 프로세스에 따라 작동할 수 있습니다.
배터리 전원으로 실행 중이면 스케줄된 작업 연기	이 옵션을 선택하면 절전 모드가 작동합니다. Kaspersky Industrial CyberSecurity for Nodes는 스케줄된 작업을 연기합니다. 필요할 경우 직접 검사 및 업데이트 작업을 시작할 수 있습니다. 절전 모드를 작동하고 컴퓨터가 배터리 전원으로 작동될 때 다음 작업은 예약되어 있더라도 실행되지 않습니다. • *데이터베이스 및 애플리케이션 모듈 업데이트* • *전체 검사* • *중요 영역 검사* • *사용자 지정 검사* • *애플리케이션 무결성 제어* • *IOC 검사.*

파라미터	설명
설정 적용 시 컴퓨터 상태	정책이나 작업 실행을 적용하는 중에 오류가 발생할 때 웹 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes가 설치된 클라이언트 컴퓨터의 상태를 표시하는 설정입니다. *정상*, *경고*, *심각* 상태를 이용할 수 있습니다.
원격 관리 소프트웨어와의 호환성	Kaspersky Industrial CyberSecurity for Nodes를 Remote Administration Tool(RAT)와 함께 사용할 때 문제가 발생하는 경우 호환 모드를 활성화할 수 있습니다. 애플리케이션의 Secure Desktop 기능과 RAT의 호환되지 않아서 문제가 발생했을 수 있습니다. 이는 컴퓨터의 보안 레벨을 낮출 가능성이 있는 잠재적인 작업들을 확인하기 위한 기능입니다. 이 기능을 사용하면 다른 여러 프로세스에서 격리된 확인 대화 상자를 애플리케이션에 표시할 수 있습니다. 이 기능은 높은 권한을 사용하여 요청을 보호합니다. 이런 방식으로는 사용자만이 작업을 확인할 수 있으며 악성 코드는 확인할 수 없습니다. 이 옵션을 선택하면 RAT 호환 모드가 활성화합니다. 애플리케이션은 이 기능 없이 확인 대화 상자를 표시합니다. 이는 컴퓨터의 보안 레벨을 낮출 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes가 RAT에 문제를 일으키지 않는 경우에는 호환 모드를 활성화하지 않는 것이 좋습니다. 이 확인란을 선택 해제하면 RAT 호환 모드가 비활성화됩니다. 기본적으로 확인란의 선택이 취소됩니다. 예: RemoteApp이 보안 데스크톱 기능을 지원하지 않기 때문에, RemoteApp 모드에서 브라우저를 사용하는 경우 신뢰할 수 없는 인증서가 있는 웹사이트를 방문할 때 Kaspersky Industrial CyberSecurity for Nodes가 확인 창을 표시하지 않을 수 있습니다. 이로 인해 브라우저가 응답하지 않을 수 있습니다. 브라우저가 RemoteApp 모드에서 올바르게 작동하려면 호환 모드를 활성화해야 합니다. 다른 타사 소프트웨어를 사용할 때 보안 데스크탑 기능에 문제가 발생하는 경우 호환 모드를 활성화해 보십시오.
검사 작업을 위한 CPU 사용량 제한	Kaspersky Industrial CyberSecurity for Nodes는 온디맨드 검사 작업 중 보호 중인 장치의 CPU 사용을 **상한** 필드에 지정한 값으로 제한합니다. 그러나 다른 구성 요소로 애플리케이션이 CPU 시간을 훨씬 더 사용할 수 있습니다. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes의 성능에 부정적인 영향을 미칠 수 있습니다. 이 기능은 기본적으로 비활성화됩니다.
다른 애플리케이션에 컴퓨터 리소스 우선권 할당	컴퓨터 검사 시 Kaspersky Industrial CyberSecurity for Nodes의 컴퓨터 리소스 사용으로 CPU 및 하드 드라이브 서브시스템의 로드가 증가할 수 있습니다. 이렇게 되면 기타 애플리케이션의 속도가 저하될 수 있습니다. 성능을 최적화하기 위해 Kaspersky Industrial CyberSecurity for Nodes는 기타 애플리케이션으로 리소스를 전송하는 모드를 제공합니다. 이 모드에서는 CPU 로드가 높아지면 운영 체제에서 Kaspersky Industrial CyberSecurity for Nodes 검사 작업의 우선순위를 낮출 수 있습니다. 이 방법을 통해 운영 체제가 리소스를 기타 애플리케이션에 재분배할 수 있습니다. 따라서 검사 작업은 CPU 시간이 줄어듭니다. 결과적으로 Kaspersky Industrial CyberSecurity for Nodes가 컴퓨터를 검사하는 시간이 길어집니다. 기본적으로 이 애플리케이션은 컴퓨터 리소스 우선권을 다른 애플리케이션에 할당하도록 구성됩니다.

웹 플러그인에서 연결 설정 구성

구성된 연결 설정은 애플리케이션을 Kaspersky Security Network 서비스와 통합하는 중에, 그리고 Kaspersky Industrial CyberSecurity for Nodes를 업데이트 및 활성 서버에 연결하는 데 사용됩니다.

연결 설정을 구성하려면 다음 단계를 수행합니다.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. 구성할 정책 이름을 클릭합니다.
3. **<정책 이름>** 창이 열리면 **애플리케이션 설정** 탭을 선택합니다.
4. **애플리케이션 설정** 섹션을 선택합니다.
5. **연결 설정** 하위 섹션에서 **구성** 버튼을 클릭합니다.
6. 아래 표에서 설명한 설정을 구성합니다.

파라미터	설명
데이터 통신 연결에서 트래픽 제한	이 확인란을 선택하면 인터넷 연결에 제한이 있을 경우 애플리케이션이 사용하는 자체 네트워크 트래픽을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 고속 모바일 인터넷 연결을 제한된 연결로, Wi-Fi 연결을 무제한 연결로 식별합니다. 비용 인식 네트워킹은 Windows 8 이상을 사용하는 컴퓨터에서 작동합니다.
프록시 서버 사용 안 함	이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 프록시 서버를 사용하지 않습니다.
프록시 서버 설정 자동 탐지	이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 운영 체제의 프록시 설정을 사용합니다.
지정한 프록시 서버 설정 사용	이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes는 수동으로 지정한 프록시 서버 설정을 사용합니다. 프록시 서버의 IP 주소 또는 기호 이름 및 포트 번호를 입력합니다
로컬 주소에 대해 프록시 서버 우회	이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 설치된 보호 중인 장치를 호스팅하는 네트워크에서 직접 장치에 접근합니다. 이 옵션은 기본적으로 활성화되어 있습니다.
프록시 서버 인증 설정	인터넷 접근을 위해 프록시 서버에서 애플리케이션을 인증하려면 사용자의 자격 증명을 입력해야 합니다. Kaspersky Industrial CyberSecurity for Nodes는 프록시 서버에서 자동 인증을 지원합니다. 자동 인증에 실패하면 애플리케이션이 자격 증명을 요청합니다. **인증 사용하지 않음**. **NTLM 인증**. 현재 사용자 계정을 사용한 NTLM 인증(기본값). **사용자 이름 및 암호를 사용한 NTLM 인증**. 직접 지정한 자격 증명을 사용한 NTLM 인증. **사용자 이름 및 암호**. 직접 지정한 자격 증명을 사용한 인증. **Kerberos 인증**. 현재 사용자 계정을 사용한 Kerberos 인증. 프록시 서버 주소로 CNAME 레코드를 사용할 때 Kerberos 인증이 올바르게 작동하도록 하려면 각 CNAME 레코드에 대해 SPN(서비스 사용자 이름)을 등록해야 합니다. **사용자 이름 및 암호를 사용한 Kerberos 인증**. 직접 지정한 자격 증명을 사용한 Kerberos 인증. Kerberos 인증을 선택한 경우, 프록시 서버 설정에 따라 Kaspersky Industrial CyberSecurity for Nodes는 Kerberos 또는 NTLM 프로토콜을 사용하여 인증을 수행합니다.
모든 네트워크 포트 모니터	이 네트워크 포트 모니터링 모드에서는 보호 구성 요소가 컴퓨터의 열린 네트워크 포트를 통해 전송되는 데이터 스트림을 감시합니다.
선택한 네트워크 포트만 모니터	이 네트워크 포트 모니터링 모드에서 보호 구성 요소는 컴퓨터의 선택된 포트와 선택한 애플리케이션의 네트워크 활동을 모니터링합니다. 이메일 및 네트워크 트래픽의 전송에 일반적으로 사용되는 네트워크 포트 목록은 Kaspersky 전문가가 권장하는 것으로 구성됩니다.
애플리케이션을 활성화할 때 Kaspersky Security Center를 프록시 서버로 사용	Kaspersky Security Center를 애플리케이션 활성화를 위한 프록시 서버로 이용할 것인지 지정합니다.

웹 플러그인에서 로컬 작업의 예약된 시작 구성

정책을 사용하여 로컬 시스템 온디맨드 검사 작업과 업데이트 작업의 시작을 허용하거나 차단할 수 있습니다. 이는 관리 그룹의 각 보호 중인 장치에 로컬로 구성된 스케줄에 따라 수행합니다:

- 정책으로 특정 유형의 로컬 시스템 작업의 예약된 시작을 금지되어 있으면, 보호 중인 장치에서 일정에 따라 이 작업을 수행하지 않습니다. 로컬 시스템 작업을 수동으로 시작할 수 있습니다.
- 정책으로 특정 유형의 로컬 시스템 작업의 예약된 시작을 허용한다면, 해당 작업이 이 작업을 위해 로컬로 구성한 예약 파라미터에 따라 수행됩니다.

기본적으로 로컬 시스템 작업의 시작은 정책에 의해 금지됩니다.

업데이트 또는 온디맨드 검사가 Kaspersky Security Center 그룹 작업에 의해 관리되는 경우에는 로컬 시스템 작업 시작을 허용하지 않는 것이 좋습니다.

그룹 업데이트 또는 온디맨드 검사 작업을 사용하지 않는 경우에는 정책에서 로컬 시스템 작업이 시작되도록 허용합니다. Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 데이터베이스 및 모듈 업데이트를 수행하고 기본 일정에 따라 모든 로컬 시스템 온디맨드 검사 작업을 시작합니다.

정책을 사용하여 다음 로컬 시스템 작업의 예약된 시작을 허용 또는 차단할 수 있습니다.

- 온디맨드 검사 작업: *중요 영역 검사*, *운영 체제 시작 시 검사*, *애플리케이션 무결성 제어*, *베이스라인 시스템 무결성 모니터*.
- *업데이트* 작업.

보호 중인 장치가 관리 그룹에서 제외된 경우 로컬 시스템 작업 일정이 자동 활성화됩니다.

정책에서 Kaspersky Industrial CyberSecurity for Nodes 로컬 시스템 작업의 예약된 시작을 허용하거나 차단하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. 구성할 정책 이름을 클릭합니다.
3. **<정책 이름>** 창이 열리면 **애플리케이션 설정** 탭을 선택합니다.
4. **애플리케이션 설정** 섹션을 선택합니다.
5. **로컬 시스템 작업 실행** 하위 섹션에서 **구성** 버튼을 클릭합니다.
6. 아래 표에서 설명한 설정을 구성합니다.

로컬 작업 시작을 위한 설정

파라미터	설명
로컬 작업 사용 허용	이 확인란을 선택한 경우 로컬 작업이 Kaspersky Industrial CyberSecurity for Nodes 로컬 인터페이스에 표시됩니다. 추가 정책 제한이 없는 경우 사용자가 작업을 구성 및 실행할 수 있습니다. 그러나 사용자는 작업 실행 스케줄을 구성할 수 없습니다. 사용자는 작업을 직접 실행할 수만 있습니다. 확인란을 선택 해제하면 로컬 작업 사용이 중지됩니다. 이 모드에서는 스케줄에 따라 로컬 작업이 실행되지 않습니다. Kaspersky Industrial CyberSecurity for Nodes 로컬 인터페이스에서 아니면 명령줄에서 작업할 때 작업을 시작하거나 구성할 수 없습니다.
스케줄 관리 허용	**로컬 작업 사용 허용** 확인란을 선택했다면 확인란이 활성화됩니다. 이 확인란을 선택하면 애플리케이션 콘솔의 로컬 작업 속성에서 스케줄 관리를 사용할 수 있게 됩니다. 기본적으로 확인란의 선택이 취소됩니다.
그룹 작업 표시 허용	이 확인란을 선택하면 그룹 작업이 Kaspersky Industrial CyberSecurity for Nodes 로컬 인터페이스에 표시됩니다. 사용자는 애플리케이션 콘솔에서 모든 작업 목록을 볼 수 있습니다. 이 확인란을 선택 해제하면, Kaspersky Industrial CyberSecurity for Nodes는 빈 작업 목록을 표시합니다.
그룹 작업 관리 허용	이 확인란을 선택하면 사용자는 Kaspersky Security Center에 지정된 그룹 작업을 시작 및 중지할 수 있습니다. 사용자는 애플리케이션 콘솔 또는 간략한 애플리케이션 인터페이스에서 작업을 시작 및 중지할 수 있습니다. 이 확인란을 선택 해제하면 Kaspersky Industrial CyberSecurity for Nodes가 예약된 작업을 자동으로 시작하거나 관리자가 Kaspersky Security Center에서 직접 작업을 시작합니다.

웹 플러그인에서 격리 및 백업 설정 구성

Kaspersky Security Center에서 일반 격리 저장소 및 백업 설정을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. 구성할 정책 이름을 클릭합니다.
3. **<정책 이름>** 창이 열리면 **애플리케이션 설정** 탭을 선택합니다.
4. **보충** 섹션을 선택합니다.
5. **저장소** 하위 섹션에서 **설정** 버튼을 클릭합니다.
6. 아래 표에서 설명한 설정을 구성합니다.

저장소 설정

파라미터	설명
리포트 탭에서 리포트 설정을 구성합니다.	
리포트 저장 기간	이 확인란을 선택하면 최대 리포트 저장 기간이 정의한 시간 간격으로 제한됩니다. 리포트 최대 저장 기간의 기본값은 30일입니다. 이 기간이 지나면 Kaspersky Industrial CyberSecurity for Nodes가 리포트 파일에서 가장 오래된 항목을 자동으로 삭제합니다.
리포트 파일 크기 제한	이 확인란을 선택하면 최대 리포트 파일 크기가 정의된 값으로 제한됩니다. 최대 파일 크기의 기본값은 1024MB입니다. Kaspersky Industrial CyberSecurity for Nodes는 리포트 파일 크기가 최대한도에 도달하면 리포트 파일에서 가장 오래된 항목을 자동으로 삭제하여 최대한도를 넘지 않도록 관리합니다.
백업 탭에서 백업 설정을 지정합니다.	
개체 저장 기간	이 확인란을 선택하면 최대 파일 저장 기간이 정의한 시간 간격으로 제한됩니다. 파일 최대 저장 기간의 기본값은 30일입니다. 최대 저장 기간이 만료되면 Kaspersky Industrial CyberSecurity for Nodes가 백업에서 가장 오래된 파일을 삭제합니다.
백업 크기를 다음으로 제한	이 확인란을 선택하면 최대 저장소 크기가 정의된 값으로 제한됩니다. 최대 크기 기본값은 400MB입니다 Kaspersky Industrial CyberSecurity for Nodes는 저장소 크기가 최대한도에 도달하면 저장소에서 가장 오래된 파일을 자동으로 삭제하여 최대 저장소 크기를 넘지 않도록 관리합니다.
이용 가능 공간의 임계값	이 확인란은 백업의 최소 여유 공간(기본값: 100MB)을 모니터링하는 기능을 활성화 또는 비활성화합니다. 여유 공간이 지정된 한계값 아래로 줄어들면 Kaspersky Industrial CyberSecurity for Nodes는 백업 저장소 여유 공간 한계값 초과 이벤트를 로깅하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. 이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 백업의 여유 공간을 모니터링합니다. **백업 크기를 다음으로 제한** 확인란을 선택했다면 **이용 가능 공간의 임계값** 확인란이 활성화됩니다. 기본적으로 확인란이 선택되어 있습니다.
격리 저장소 탭에서 격리 설정을 구성합니다.	
격리 저장소 크기 제한	이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 격리 저장소에 있는 개체의 총 크기를 모니터링합니다. 지정된 값을 초과하면(기본값 1024MB) Kaspersky Industrial CyberSecurity for Nodes는 *최대 격리 저장소 크기 초과* 이벤트를 기록하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. 그동안 애플리케이션은 새 개체를 격리하지 않습니다. 격리 저장소를 직접 비워야 합니다. 이 기능을 사용하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 격리 저장소에 있는 개체의 총 크기를 모니터링하지 않습니다. 이 기능은 기본적으로 비활성화됩니다.
이용 가능 공간의 임계값	이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 백업의 최소 여유 공간(기본값 50MB)을 모니터링합니다. 여유 공간이 지정된 한계값 아래로 줄어들면 Kaspersky Industrial CyberSecurity for Nodes는 *격리 저장소 여유 공간 한계값 초과* 이벤트를 기록하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. **격리 저장소 크기 제한** 확인란을 선택했다면 **이용 가능 공간의 임계값** 확인란이 활성화됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

정책 만들기 및 구성

이 섹션에서는 여러 보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes 관리 시 Kaspersky Security Center 정책을 사용하는 방법에 대한 정보를 제공합니다.

Kaspersky Industrial CyberSecurity for Nodes를 설치한 여러 장치에서 보호 기능을 관리하기 위해 글로벌 Kaspersky Security Center 정책을 만들 수 있습니다.

정책은 관리 그룹 하나의 모든 보호 중인 장치에 대해 정책에 정의된 Kaspersky Industrial CyberSecurity for Nodes 설정, 기능, 작업을 강제 적용합니다.

관리자 그룹 하나에 대해 여러 정책을 만들어 차례로 적용할 수 있습니다. 그룹에 대해 현재 활성화된 정책은 웹 콘솔에서 *활성* 상태로 표시됩니다.

정책 적용에 대한 정보가 Kaspersky Industrial CyberSecurity for Nodes 시스템 감사 로그에 기록됩니다. 이 정보는 **로그 및 알림** 노드의 애플리케이션 콘솔에서 확인할 수 있습니다.

Kaspersky Security Center에는 보호 중인 장치에 정책을 적용할 수 있는 한 가지 방법인 *설정 변경 금지*가 있습니다. 정책을 적용하면 Kaspersky Industrial CyberSecurity for Nodes가 보호 중인 장치의 정책 속성에서 사용자가 선택한 아이콘에 대한 설정을 사용합니다. 이 경우 정책 적용 전에 사용 중이던 설정 대신 선택한 설정이 사용됩니다. Kaspersky Industrial CyberSecurity for Nodes는 정책 속성에서 아이콘을 선택한 활성 정책 설정을 적용하지 않습니다.

정책이 활성 상태이면 정책에 아이콘이 표시된 설정값이 애플리케이션 콘솔에 표시되지만 편집할 수는 없습니다. 다른 설정의 값(정책에 아이콘이 표시됨)은 애플리케이션 콘솔에서 편집할 수 있습니다.

활성 정책에 구성되어 있고 아이콘이 표시된 설정은 **속성: <보호 중인 장치 이름>** 창에서 개별 보호 중인 장치에 대한 Kaspersky Security Center에서 변경사항을 차단합니다.

활성화된 정책을 이용하여 지정하고 보호 중인 장치로 전달한 설정은, 활성 정책 비활성화 시 로컬 작업 설정에 저장됩니다.

정책이 현재 실행 중인 실시간 컴퓨터 보호 작업 또는 네트워크 저장소 보호 작업의 설정을 정의하는 경우 정책이 정의한 설정은 정책 적용 직후 변경됩니다. 작업이 실행되고 있지 않으면 시작 시 설정이 적용됩니다.

Kaspersky Security Center 웹 콘솔에서 정책을 생성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. **추가** 버튼을 클릭합니다.
3. **새 정책** 창이 열립니다.
4. **애플리케이션 선택** 섹션에서 Kaspersky Industrial CyberSecurity for Nodes를 선택합니다.
5. 보호 중인 장치의 Kaspersky Industrial CyberSecurity for Nodes 모드를 지정합니다.
6. 필요하다면 전체 또는 일부 애플리케이션 구성 요소의 검사에서 제외할 파일 또는 폴더와 개체 이름(바이러스 백과사전을 따름)을 지정합니다.

7. **일반** 탭에서는 다음 처리를 수행할 수 있습니다.

   - 정책 이름을 변경합니다.

     정책 이름에 `" * < : > ? \ |` 기호는 포함할 수 없습니다.

   - 정책 상태를 선택합니다:

     - **활성**. 다음 동기화 이후 정책이 컴퓨터에서 활성 정책으로 사용됩니다.
     - **비활성**. 백업 정책입니다. 필요시 비활성 정책을 활성 상태로 전환할 수 있습니다.
     - **이동 사용자**. 컴퓨터가 조직 네트워크 외부로 이동하면 이 정책이 활성화됩니다.

   - 설정 상속을 구성합니다:

     - **상위 정책의 설정 상속**. 이 토글 버튼을 켜면 정책 설정 값이 상위 레벨 정책에서 상속됩니다. 부모 정책에 대해 이 설정되어 있으면 정책 설정을 편집할 수 없습니다.
     - **하위 정책에 설정 강제 상속**. 이 토글 버튼을 켜면 정책 설정의 값이 자식 정책으로 전파됩니다. 하위 정책 설정에서 **상위 정책의 설정 상속** 확인란이 자동 선택됩니다. 으로 표시된 설정을 제외한 자식 정책 설정이 부모 정책에서 상속됩니다. 부모 정책에 대해 이 설정되어 있으면 자식 정책 설정을 편집할 수 없습니다.

8. **애플리케이션 설정** 탭에서 필요에 따라 정책 설정을 구성합니다.

9. **저장** 버튼을 클릭합니다.

새 정책이 생성되면 허용 규칙 집합이 생성되어 애플리케이션 차단을 방지하고 매끄러운 작업을 보장합니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 새 정책을 생성할 때 인바운드 네트워크 트래픽에 대한 규칙 세트를 생성합니다:

- Kaspersky Security Center 네트워크 에이전트를 사용하여 Windows 바탕 화면을 공유하는 프로세스에 대한 두 가지 허용 규칙으로, %Program Files% 및 %Program Files (x86)% 폴더에 있습니다. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.
- 로컬 포트 15000에 대한 두 가지 허용 규칙. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 새 정책을 생성할 때 발신 네트워크 트래픽 규칙 세트를 생성합니다:

- Kaspersky Industrial CyberSecurity for Nodes service에 대한 두 가지 허용 규칙으로, %Program Files% 및 %Program Files (x86)% 폴더에 있습니다. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.
- Kaspersky Industrial CyberSecurity for Nodes의 작업자 프로세스에 대한 두 가지 허용 규칙으로, %Program Files% 및 %Program Files (x86)% 폴더에 있습니다. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.
- 로컬 포트 13000에 대한 두 가지 허용 규칙. 상태: 활성화됨. 허용 외부 주소: 모두. 프로토콜: TCP 및 UDP, 프로토콜당 규칙 하나.

Kaspersky Security Center를 사용하여 작업 만들기 및 구성

이 절에는 Kaspersky Industrial CyberSecurity for Nodes 작업과 생성 방법, 작업 설정 구성, 시작 및 중지에 대한 정보가 포함되어 있습니다.

웹 플러그인의 작업 생성 정보

다음과 같은 방법으로 로컬 및 그룹 작업을 만들 수 있습니다.

- 보호 중인 장치가 1대라면 **작업** 섹션의 **속성 <보호 중인 장치 이름>** 창에서.
- 관리 그룹은 **작업** 탭에서 선택한 보호 중인 장치 그룹 노드의 세부 정보 창에서.
- 보호 중인 장치 세트는 **기기 조회** 노드의 세부 정보 창에서.

정책을 사용하면 같은 관리 그룹의 모든 보호 중인 장치에 대해 *업데이트* 및 *온디맨드 검사* 로컬 시스템 작업 스케줄을 비활성화할 수 있습니다.

Kaspersky Security Center의 작업에 대한 일반 정보는 Kaspersky Security Center 도움말 을 참조하십시오.

웹 플러그인에서 작업 생성

Kaspersky Security Center 웹 콘솔에서 새 작업을 생성하려면:

1. 다음 방법 중 하나로 작업 마법사를 시작합니다.
   - 로컬 작업을 만들려면:
     a. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)** 옵션을 선택합니다.
     b. 보호 중인 장치 이름을 클릭합니다.
     c. **<장치 이름>** 창이 열리면 **작업** 탭을 선택합니다.
     d. **추가** 버튼을 클릭합니다.
   - 그룹 작업을 만들려면:
     a. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
     b. **추가** 버튼을 클릭합니다.

   작업 마법사 창이 열립니다.

2. **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다.

3. **작업 유형** 드롭다운 목록에서 생성할 작업의 유형을 선택합니다.

4. 선택한 작업 유형에 따라 다음 중 하나를 수행합니다.

   - 온디맨드 검사 작업 만들기.
   - 업데이트 작업을 만들려면 요구사항에 따라 작업 설정을 구성합니다.

     a. **업데이트 경로** 블록에서 Kaspersky Security Center 중앙 관리 서버 또는 Kaspersky 업데이트 서버를 애플리케이션 업데이트 경로로 지정할 수 있습니다. 또한 사용자 지정 HTTP 및 FTP 서버 또는 네트워크 폴더를 수동으로 추가한 다음 업데이트 경로로 설정하여 업데이트 경로의 사용자 지정 목록을 만들 수도 있습니다.

     수동으로 사용자 지정한 서버를 사용할 수 없는 경우 Kaspersky 업데이트 서버를 사용하도록 지정할 수 있습니다.

     b. 디스크 하위 시스템의 부하를 줄이는 기능에 대한 설정을 구성합니다:

     c. 중요 애플리케이션 모듈 업데이트가 필요한 경우와 긴급 업데이트 설치가 완료된 후에 Kaspersky Industrial CyberSecurity for Nodes가 수행할 동작을 지정할 수 있습니다. 또한 Kaspersky Industrial CyberSecurity for Nodes가 사용 가능한 스케줄된 업데이트 정보를 받을지 지정할 수 있습니다.

     d. Kaspersky Industrial CyberSecurity for Nodes에서 복사한 업데이트를 저장할 폴더 경로와 복사할 업데이트 세트를 지정합니다.

   - 애플리케이션 활성화 작업을 생성하려면:

     a. **라이센스 키 선택** 창에서 애플리케이션 활성화에 사용할 키 파일이나 활성화 코드를 지정합니다.

     b. 라이센스 갱신을 위한 작업을 만들려는 경우 **예비 키로 사용** 확인란을 선택합니다.

   - 애플리케이션 실행 제어를 위한 규칙 생성기 작업을 생성하고 구성합니다.
   - 장치 제어를 위한 규칙 생성기 작업을 생성하고 구성합니다.

5. **다음** 버튼을 클릭합니다.

6. 보호 중인 장치 세트에 대해 작업을 만든 경우 이 작업을 실행할 보호 중인 장치 네트워크(그룹)를 선택합니다.

7. **다음** 버튼을 클릭합니다.

8. 작업 설정을 구성하려면 **작업 생성 마침** 창에서 **생성이 완료되면 작업 세부 정보 열기** 확인란을 선택합니다.

9. **마침** 버튼을 클릭합니다.

만든 작업이 **작업** 목록에 표시됩니다.

웹 플러그인에서 그룹 작업 구성

여러 보호 중인 장치의 그룹 작업을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
2. Kaspersky Security Center 작업 목록에서 작업 이름을 클릭합니다.
   <작업 이름> 창이 열립니다.
3. **애플리케이션 설정** 탭으로 갑니다.
4. 구성한 작업 유형에 따라 다음 중 하나를 수행합니다.
   - *온디맨드 검사* 작업을 구성하려면:
     a. **검사 범위** 섹션에서 검사 범위를 생성합니다.
     b. **옵션** 섹션에서 휴리스틱 분석 수준 및 다른 애플리케이션 구성 요소와의 통합을 구성합니다.
   - *업데이트* 작업을 구성하려면 요구사항에 따라 작업 설정을 조정합니다.
     a. **업데이트 경로** 섹션에서 업데이트 경로 설정을 구성합니다.
     b. **업데이트 설정** 섹션에서, 디스크 하위 시스템 최적화 설정을 관리하고, 애플리케이션 모듈의 긴급 업데이트를 사용할 수 있거나 계획된 업데이트 정보가 있을 시 Kaspersky Industrial CyberSecurity for Nodes가 수행할 동작을 지정하고, 업데이트 복사 설정을 지정합니다.
   - *애플리케이션 활성화* 작업을 구성하려면 애플리케이션 활성화에 사용하려는 키 파일이나 활성화 코드를 적용합니다. 라이센스 갱신을 위한 활성화 코드 또는 키 파일을 추가하려는 경우 **추가 키로 사용** 확인란을 선택합니다.
   - 장치 제어에 대한 허용 규칙 자동 생성을 구성하려면 허용 규칙 목록을 만드는 데 사용할 설정을 지정합니다.
5. **스케줄** 섹션에서 작업 일정을 구성합니다(데이터베이스 *업데이트 롤백*을 제외한 모든 작업 유형에 대한 일정을 구성할 수 있음).
6. **설정** 섹션의 **계정** 탭에서 작업 실행에 권한을 사용할 계정을 지정합니다. 이 섹션의 설정 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.
7. **저장** 버튼을 클릭합니다.

새로 구성된 그룹 작업 설정이 저장됩니다.

웹 플러그인에서 애플리케이션 활성화 작업 구성

애플리케이션 활성화 작업을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
2. Kaspersky Security Center 작업 목록에서 작업 이름을 클릭합니다.
   <작업 이름> 창이 열립니다.
3. **애플리케이션 설정** 섹션에서 애플리케이션을 활성화하는 데 사용할 키 파일을 지정합니다. 라이센스 갱신을 위해 키를 추가하려는 경우 **예비 키로 사용** 확인란을 선택합니다.
4. **스케줄** 섹션에서 작업 스케줄을 구성합니다.
5. **<작업 이름>** 창의 **저장** 버튼을 클릭합니다.

웹 플러그인에서 업데이트 작업 구성

업데이트 작업을 구성하려면:

1. 웹 콘솔의 메인 창에서 **기기** → **작업**을 선택합니다.
2. Kaspersky Security Center 작업 목록에서 작업 이름을 클릭합니다.
   <작업 이름> 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **업데이트 경로** 섹션에서 업데이트 경로 설정을 구성합니다.
   a. Kaspersky Security Center 중앙 관리 서버나 Kaspersky 업데이트 서버를 애플리케이션 업데이트 경로로 지정합니다. 또한 사용자 지정 HTTP 및 FTP 서버 또는 네트워크 폴더를 수동으로 추가한 다음 업데이트 경로로 설정하여 업데이트 경로의 사용자 지정 목록을 만들 수도 있습니다.
   수동으로 사용자 지정한 서버를 사용할 수 없는 경우 Kaspersky 업데이트 서버를 사용하도록 지정할 수 있습니다.
   b. 디스크 하위 시스템의 부하를 줄이는 기능에 대한 설정을 구성합니다:
   - **디스크 I/O 부하 낮추기**
   - **최적화에 사용되는 RAM, MB**
   c. 애플리케이션 모듈의 긴급 업데이트를 사용할 수 있거나 계획된 업데이트 정보가 있을 시 Kaspersky Industrial CyberSecurity for Nodes에서 수행할 동작을 지정합니다.
   d. 업데이트 복사 설정을 지정합니다.
5. **스케줄** 섹션에서 작업 일정을 구성합니다(데이터베이스 *업데이트 롤백*을 제외한 모든 작업 유형에 대한 일정을 구성할 수 있음).
6. **<작업 이름>** 창에서 **확인**을 클릭합니다.

작업 예약

웹 콘솔에서 로컬 시스템 및 사용자 지정 작업을 스케줄할 수 있습니다.

웹 콘솔을 사용하여 그룹 작업을 스케줄하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
2. Kaspersky Security Center 작업 목록에서 작업 이름을 클릭합니다.
   <작업 이름> 창이 열립니다.
3. **스케줄** 섹션으로 이동하여 필요에 따라 스케줄 설정(아래 표 참조)을 구성합니다.

   온디맨드 검사 및 업데이트 작업의 일정 설정 필드는 Kaspersky Security Center 정책에 의해 해당 작업 예약이 차단된 경우 사용할 수 없습니다.

4. **저장** 버튼을 클릭해 작업 시작 설정을 저장합니다.

작업 스케줄 설정

파라미터	설명
시작 스케줄	작업 실행 모드를 선택합니다: • **N시간마다**. 작업이 몇 시간마다 주기적으로 실행됩니다. 작업 시작 시간과 시간 단위의 주기를 지정합니다. • **N일마다**. 작업이 며칠마다 주기적으로 실행됩니다. 작업 시작 시간과 일 단위의 주기를 지정합니다. • **N분마다**. 작업이 몇 분마다 주기적으로 실행됩니다. 작업 시작 시간과 분 단위의 주기를 지정합니다. • **요일별**. 작업이 지정된 요일에 실행됩니다. 요일을 선택하고 시작 시간을 지정합니다. 작업을 몇 주 간격으로 실행해야 하는 경우 **간격** 필드에 원하는 값을 입력합니다. • **월별**. 작업이 매월 특정 일자에 실행됩니다. 시작 날짜와 시간을 지정합니다. • **한번만**. 작업이 지정된 날짜와 시간에 한 번 실행됩니다. • **수동 시작**. 편리한 시간에 검사를 수동으로 시작할 수 있는 실행 모드입니다. • **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**. 저장소에서 업데이트가 다운로드될 때마다 작업이 실행됩니다. • **다른 작업 완료 시**. 다른 작업 완료 시 작업이 실행됩니다. 작업 및 완료 상태를 선택합니다. Kaspersky Industrial CyberSecurity for Nodes는 로컬 작업 스케줄에 **다른 작업 완료 시** 모드를 지원하지 않습니다. • **바이러스 발생 시**. 바이러스 공격이 탐지되면 작업이 실행됩니다. • **애플리케이션 시작 후 N분 내에 시작**. Kaspersky Industrial CyberSecurity for Nodes가 시작될 때마다 지정된 시간이 경과한 후 작업이 실행됩니다. **작업 시작 지연(분)** 필드에 분 단위의 값을 지정합니다.
누락된 작업 실행	이 확인란을 선택하면, Kaspersky Industrial CyberSecurity for Nodes는 작업이 가능하자 마자 건너뛴 작업을 시작합니다. 스케줄된 작업 시작 시각에 컴퓨터가 꺼져 있는 등의 경우에는 작업을 건너뜁니다. 애플리케이션에 누락된 작업을 실행할 기회가 있다면 특정 시간 내에 무작위로 작업을 실행하여 컴퓨터의 로드를 분산합니다. 이 확인란을 선택 취소하면 Kaspersky Industrial CyberSecurity for Nodes가 건너뛴 작업을 실행하지 않습니다. 대신, 현재 스케줄에 따라 다음 작업을 실행합니다.
자동으로 작업 시작 임의 지연 사용	이 확인란을 선택하면 작업이 특정 시간 범위 내에서 임의의 시간에 컴퓨터에서 실행됩니다. 무작위 시작 시간은 스케줄에 따라 작업이 실행될 때, 중앙 관리 서버에 다수의 컴퓨터가 동시에 접근하는 것을 방지하는 데 도움이 됩니다. 확인란의 선택을 취소하면 작업이 정확히 스케줄된 시간에 실행됩니다.
다음 간격으로 작업 시작 자동 임의 지연	이 확인란을 선택하면 작업이 특정 시간 범위 내에서 임의의 시간에 컴퓨터에서 실행됩니다. 무작위 시작 시간은 스케줄에 따라 작업이 실행될 때, 중앙 관리 서버에 다수의 컴퓨터가 동시에 접근하는 것을 방지하는 데 도움이 됩니다. 확인란의 선택을 취소하면 작업이 정확히 스케줄된 시간에 실행됩니다.
작업 시작 전에 Wake-on-LAN 기능으로 기기 켜기	이 확인란을 선택하면 작업 실행 전에 컴퓨터 운영 체제에 시작 완료를 위해 지정된 리드 타임이 제공됩니다. 기본 리드 타임은 5분입니다. 전원이 꺼진 컴퓨터를 포함하여 모든 컴퓨터에서 작업을 실행하려면 확인란을 선택합니다.

파라미터	설명
작업 완료 후 기기 종료	이 확인란을 선택하면 작업이 완료된 후 컴퓨터가 종료됩니다. 예를 들어, 이 기능을 활성화하면 근무 시간이 끝난 금요일에 컴퓨터를 스캔할 수 있습니다. 작업이 완료되면 애플리케이션이 주말 동안 컴퓨터를 끕니다.
작업이 다음 시간보다 오래 실행되면 중지	작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Industrial CyberSecurity for Nodes가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Industrial CyberSecurity for Nodes가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.
작업 실행 일시 중지	이전에 스케줄된 작업의 실행을 일시 중지할 시간 간격을 지정할 수 있습니다. 지정한 기간이 지나면 작업이 다시 시작됩니다. 이는 예를 들어 사용량이 가장 많은 기간에 Kaspersky Industrial CyberSecurity for Nodes가 컴퓨터 성능에 미치는 영향을 최소화하기 위해 필요할 수 있습니다. 이 기능은 온디맨드 검사 작업에만 사용할 수 있습니다.
종료일	이 체크박스를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 지정한 날짜부터 스케줄된 작업의 실행을 중지합니다. 해당 작업은 **수동** 모드로 설정됩니다. 이 기능은 온디맨드 검사 작업에만 사용할 수 있습니다.

Kaspersky Security Center 리포트

Kaspersky Security Center의 리포트에는 관리 중인 장치의 상태 정보가 포함되어 있습니다. 리포트는 중앙 관리 서버에 저장된 정보를 기반으로 합니다.

Kaspersky Security Center 11부터 Kaspersky Industrial CyberSecurity for Nodes에서 다음 유형의 리포트를 사용할 수 있습니다.

- 애플리케이션 구성 요소 상태 리포트
- 금지한 애플리케이션에 대한 리포트
- 테스트 모드에서 금지한 애플리케이션에 대한 리포트

모든 Kaspersky Security Center 리포트 및 구성 방법에 관한 자세한 정보는 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Industrial CyberSecurity for Nodes 구성 요소 작동에 관한 리포트

모든 네트워크 장치의 보호 상태를 모니터링하고 각 장치의 구성 요소 집합에 대한 구조화된 개요를 확인할 수 있습니다.

리포트에는 각 구성 요소에 대해 다음 상태 중 하나가 표시됩니다: *실행 중*, *일시 중지됨*, *중지됨*, *라이센스에 포함되지 않음*.

설치되지 않음 상태는 애플리케이션 자체가 아닌 구성 요소를 말합니다. 애플리케이션이 설치되어 있지 않은 경우 Kaspersky Security Center 웹 콘솔이 N/A(사용할 수 없음) 상태를 할당합니다.

구성 요소 조회를 만들고 필터링을 사용하여 네트워크 장치를 지정된 구성 요소 및 상태 집합과 함께 표시할 수 있습니다.

만들기 및 조회 사용에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Security Center 웹 콘솔에서 구성 요소의 상태를 보려면:

1. 웹 콘솔의 메인 창에서 **에셋(기기)** → **관리 중인 기기** 옵션을 선택합니다.
2. 장치 이름을 클릭하고 **애플리케이션** 섹션으로 갑니다.
3. Kaspersky Industrial CyberSecurity for Nodes의 애플리케이션 이름을 클릭합니다.
4. 창이 열리면 **일반** 탭에서 **구성 요소** 섹션으로 갑니다.
5. 상태 표를 검토합니다.

Kaspersky Security Center 웹 콘솔에서 표준 리포트를 검토하려면:

1. **모니터링** → **리포트**를 선택합니다.
2. 목록에서 **애플리케이션 구성 요소 상태 리포트** 항목을 선택하고 클릭합니다.
   리포트가 생성됩니다.
3. 다음 리포트 세부 정보를 검토합니다:
   - 그래픽 다이어그램.
   - 각 구성 요소와 해당 구성 요소가 속한 그룹이 설치된 구성 요소와 네트워크 장치의 집계 수에 대한 요약표.
   - 구성 요소 상태, 버전, 장치, 그룹을 포함하는 상세표.

활성 및 테스트 모드에서 금지한 애플리케이션에 대한 리포트

애플리케이션 실행 제어 작업의 결과를 기반으로, 금지한 애플리케이션에 관한 리포트(작업이 활성 모드에서 시작된 경우)와 테스트 모드에서 금지한 애플리케이션에 관한 리포트(작업이 알림 모드에서 시작된 경우)의 두 가지 리포트가 생성될 수 있습니다. 이 리포트는 네트워크의 보호 중인 장치에서 차단된 애플리케이션에 대한 정보를 표시합니다. 모든 관리 그룹에 대해 각 리포트가 생성되며 보호 중인 장치에 설치된 모든 Kaspersky 애플리케이션의 데이터가 누적됩니다.

알림 모드에서 금지한 애플리케이션에 대한 리포트를 검토하려면:

1. 알림 모드에서 애플리케이션 실행 제어 작업을 실행합니다.
2. **모니터링** → **리포트**를 선택합니다.
3. 목록에서 **테스트 모드에서 운영된 금지한 애플리케이션 리포트** 항목을 선택하고 클릭합니다.
   리포트가 생성됩니다.

4. 다음 리포트 세부 정보를 검토합니다:

   - 차단된 시작 횟수가 가장 많은 상위 10개 애플리케이션을 표시하는 그래픽 다이어그램.
   - 실행 파일 이름, 이유, 차단 시간, 차단이 발생한 장치 수를 지정하는 애플리케이션 차단 요약표입니다.
   - 장치, 파일 경로 및 차단 기준에 대한 데이터를 지정하는 상세표입니다.

활성 모드에서 금지한 애플리케이션에 대한 리포트를 검토하려면:

1. 활성 모드에서 애플리케이션 실행 제어 작업을 실행합니다.
2. **모니터링 → 리포트**를 선택합니다.
3. 목록에서 **금지한 애플리케이션 리포트** 항목을 선택하고 클릭합니다.
   리포트가 생성됩니다.

이 리포트는 테스트 모드에서 금지한 애플리케이션에 대한 리포트와 같은 차단 데이터로 구성됩니다.

애플리케이션 라이센스

이 섹션에서는 애플리케이션의 라이센스와 관련된 주요 개념을 설명합니다.

최종 사용자 라이센스 계약서 정보

*최종 사용자 라이센스 계약서*는 애플리케이션 사용 약관을 규정하고 있는 사용자와 AO Kaspersky Lab 간의 라이센스 계약서입니다.

애플리케이션을 사용하기 전에 최종 사용자 라이센스 계약 조항을 세심히 검토하십시오.

최종 사용자 라이센스 계약서의 조항과 데이터의 처리 및 전송이 설명된 개인정보취급방침을 다음과 같은 방법으로 읽을 수 있습니다:

- Kaspersky Industrial CyberSecurity for Nodes 설치 중.
- Kaspersky Industrial CyberSecurity for Nodes 콘솔 설치 중.
- Kaspersky Security Gateway 설치 중.
- 배포 키트에 포함된 파일인 license.txt 문서 읽기.
- Kaspersky 웹 사이트(https://www.kaspersky.com/business/eula).

애플리케이션을 설치할 때 최종 사용자 라이센스 계약서를 수락한다는 것은 최종 사용자 라이센스 계약서의 조건을 수락한다는 의미입니다. 최종 사용자 라이센스 계약 조항에 동의하지 않으면 애플리케이션 설치를 중단해야 하며 애플리케이션을 사용할 수 없습니다.

라이센스 정보

*라이센스*는 최종 사용자 라이센스 계약서에 따라 정해진 기간 동안 애플리케이션을 사용할 수 있도록 부여된 권한을 말합니다.

유효한 라이센스를 통해 최종 사용자 라이센스 계약서에 따라 애플리케이션을 사용하고 필요할 때 기술 지원을 받을 수 있습니다.

서비스 범위와 애플리케이션 사용 기간은 애플리케이션 활성화에 사용한 라이센스에 따라 달라집니다.

다음 두 가지 방법으로 애플리케이션을 활성화할 수 있습니다:

- 상업용 라이센스에 따른 사용 권한을 부여하는 키 파일 사용
- 활성화 코드를 사용하여 상업용 라이센스 구매.

상업용 라이센스가 만료되면 데이터베이스 업데이트 없이 다음 애플리케이션 구성 요소 및 작업만 계속 사용할 수 있습니다:

- 실시간 파일 보호
- 시스템 무결성 모니터링
- 온디맨드 검사 작업

Kaspersky Industrial CyberSecurity for Nodes의 모든 기능을 계속해서 사용하려면 상업용 라이센스를 갱신해야 합니다. 보호를 극대화하려면 만료 날짜 전에 라이센스의 유효 기간을 연장하는 것이 좋습니다.

라이센스 키를 제거해도 애플리케이션은 계속 실행됩니다. 시스템 무결성 모니터링 구성 요소는 계속 사용할 수 있으며, 나머지 구성 요소, 작업, Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 업데이트는 사용할 수 없습니다. Kaspersky가 사용자의 라이센스를 거부 목록에 추가해도 동일합니다.

라이센스 인증서 정보

*라이센스 인증서*는 키 파일 또는 활성화 코드와 함께 전달된 문서입니다.

이 라이센스 인증서에는 다음 라이센스 정보가 들어 있습니다:

- 라이센스 ID 또는 주문 번호.
- 라이센스가 부여된 사용자에 대한 세부 정보.
- 라이센스로 인증할 수 있는 애플리케이션에 대한 정보.
- 라이센스 구매 수량(예, 해당 라이센스로 애플리케이션을 사용할 수 있는 장치 개수).
- 라이센스 기간 시작 날짜.
- 라이센스 만료 날짜 또는 라이센스 기간.
- 라이센스 유형.

키 정보

*키*는 최종 사용자 라이센스 계약 조건에 따라 애플리케이션을 활성화한 후 사용할 수 있도록 해주는 일련의 비트입니다. 키는 Kaspersky에서 생성합니다.

키 파일 또는 활성화 코드를 사용하여 애플리케이션에 키를 추가할 수 있습니다. 애플리케이션에 키를 추가한 후에는 키가 고유한 영숫자로 애플리케이션 인터페이스에 표시됩니다.

라이센스 계약서 위반 시 Kaspersky는 거부 목록에 키를 추가할 수 있습니다. 키가 차단되면 다른 키를 추가해야 애플리케이션이 작동합니다.

라이센스 키에는 활성 키와 예약 키의 두 가지 유형이 있습니다.

*활성 키*는 현재 애플리케이션에서 사용 중인 라이센스입니다. 상업용 라이센스의 키는 활성 키로 추가할 수 있습니다. 애플리케이션은 하나 이상의 활성 키를 보유할 수 없습니다.

*예약 키*는 사용자에게 애플리케이션을 사용하기 위한 권한을 부여하지만 현재 사용하지는 않습니다. 현재 활성 키와 연관된 라이센스가 만료되면 예비 키가 자동으로 활성 키가 됩니다. 예약 키는 활성 키가 이미 추가된 경우에만 추가할 수 있습니다.

키 파일 정보

*키 파일*은 Kaspersky에서 받는 .key 확장자를 가진 파일입니다. 키 파일의 목적은 애플리케이션을 활성화하는 키를 추가하기 위한 것입니다.

Kaspersky Industrial CyberSecurity for Nodes 구매 후 지정한 이메일 주소로 키 파일을 받습니다.

키 파일로 애플리케이션을 활성화하려면, Kaspersky 활성화 서버에 연결할 필요가 없습니다.

만일 키 파일을 원치 않게 삭제했더라도 이를 복원할 수 있습니다. 예를 들어, Kaspersky CompanyAccount에 가입할 때 구입한 키 파일이 필요할 수 있습니다.

키 파일을 복원하려면 다음 중 하나를 수행하십시오.

- 라이센스 구매처로 문의.
- 기존 활성화 코드를 기반으로 Kaspersky 웹사이트에서 키 파일을 받습니다.

활성화 코드 정보

*활성화 코드*는 20개의 영숫자로 구성된 일련의 고유한 코드입니다. Kaspersky Industrial CyberSecurity for Nodes를 활성화하기 위한 키를 추가하려면 활성화 코드를 입력해야 합니다. Kaspersky Industrial CyberSecurity for Nodes 구매 후 지정한 이메일 주소로 활성화 코드를 받습니다.

활성화 코드를 사용하여 애플리케이션을 활성화할 때 Kaspersky 활성화 서버에 연결하기 위해 인터넷에 연결되어 있어야 합니다.

애플리케이션을 설치한 후 활성화 코드를 분실했다면 복구할 수 있습니다. 예를 들어, Kaspersky CompanyAccount 등록 시 활성화 코드가 필요할 수 있습니다. 활성화 코드를 복구하려면 라이센스를 구매한 Kaspersky Lab 협력사에 문의하십시오.

키 파일로 애플리케이션 활성화

키 파일을 적용하여 Kaspersky Industrial CyberSecurity for Nodes를 활성화할 수 있습니다.

키 파일을 적용하여 Kaspersky Industrial CyberSecurity for Nodes를 활성화하려면:

1. 애플리케이션 콘솔 트리에서 **라이센스** 노드를 확장합니다.
2. **라이센스** 노드의 결과 창에서 **키 추가** 링크를 클릭합니다.

3. 열리는 창에서 **찾아보기** 버튼을 클릭합니다.

4. 확장자가 .key인 키 파일을 선택합니다.

   키를 예비 키로 입력할 수도 있습니다. 추가 키로 키를 입력하려면 **추가 키로 사용** 확인란을 선택합니다.

5. **확인** 버튼을 클릭합니다.

선택한 키 파일이 적용됩니다. 이때:

- 애플리케이션 활성화를 위해 활성 키를 이미 추가한 상태에서 다른 키를 활성 키로 추가하면, 새 키가 이전에 추가한 키를 대체합니다. 이전에 추가한 키는 제거됩니다.
- 애플리케이션 활성화를 위해 예비 키를 이미 추가한 상태에서 다른 키를 예비 키로 추가하면, 새 키가 이전에 추가한 키를 대체합니다. 이전에 추가한 예비 키는 제거됩니다.
- 애플리케이션 활성화를 위해 활성 키와 예비 키를 이미 추가한 상태에서 새 키를 활성 키로 추가하면, 새 키가 이전에 추가한 활성 키를 대체하며 예비 키는 제거되지 않습니다.

추가된 키에 관한 정보는 **라이센스** 노드에서 확인할 수 있습니다.

활성화 코드로 애플리케이션 활성화

활성화 코드를 사용하여 애플리케이션을 활성화하려면, 보호 중인 장치가 인터넷에 연결되어 있어야 합니다.

활성화 코드를 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 활성화할 수 있습니다.

이 방법으로 애플리케이션을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 입력한 코드를 확인하기 위해 활성화 서버로 데이터를 전송합니다:

- 활성화 코드 검증이 성공적으로 완료되면 애플리케이션이 활성화됩니다.
- 활성화 코드 검증에 실패할 경우 대응하는 알림이 표시됩니다. 이 경우 Kaspersky Industrial CyberSecurity for Nodes 라이센스를 구매한 소프트웨어 제조업체에 문의해야 합니다.
- 활성화 코드의 활성화 횟수를 초과하면 대응하는 알림이 표시됩니다. 애플리케이션 활성화 절차가 중단되고 기술 지원에 문의하라는 메시지가 표시됩니다.

애플리케이션 콘솔을 사용하거나 관리 플러그인 또는 웹 플러그인을 통해 *애플리케이션 활성화* 그룹 작업을 생성하여 활성화 코드로 Kaspersky Industrial CyberSecurity for Nodes를 활성화할 수 있습니다.

애플리케이션 콘솔을 사용하여 활성화 코드로 Kaspersky Industrial CyberSecurity for Nodes 활성화하려면:

1. 애플리케이션 콘솔 트리에서 **라이센스** 노드를 확장합니다.
2. **라이센스** 노드의 결과 창에서 **활성화 코드 추가** 링크를 클릭합니다.

3. 창이 열리면 **활성화 코드** 필드에 활성화 코드를 입력합니다.

   - 활성화 코드를 예비 키로 사용하려면 **추가 키로 사용** 확인란을 선택합니다.
   - 라이센스에 관한 정보를 보려면 **라이센스 정보 보기** 버튼을 클릭합니다. 정보가 **라이센스 정보** 블록에 표시됩니다.

4. **확인** 버튼을 클릭합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 적용된 활성화 코드에 관한 정보를 활성화 서버로 보냅니다.

현재 라이센스 정보 보기

라이센스 상태 보기

현재 라이센스에 관한 상태 정보는 애플리케이션 콘솔의 **Kaspersky Industrial CyberSecurity for Nodes** 노드 세부 정보 창에 표시됩니다. 라이센스 상태 값은 다음과 같습니다.

- **키 상태를 확인 중입니다** – Kaspersky Industrial CyberSecurity for Nodes가 추가된 키 파일을 확인하고 현재 상태에 대한 응답을 기다리는 중입니다.
- **만료 날짜** – Kaspersky Industrial CyberSecurity for Nodes가 지정된 날짜까지 활성화되었습니다. 상태는 다음의 경우 노란색으로 강조 표시됩니다.
  - 라이센스가 30일 이내에 만료되고 입력된 예비 키가 없습니다.
  - 추가된 키가 거부 목록에 포함되어 곧 차단됩니다.
- **애플리케이션이 활성화되지 않았습니다** – 키가 추가되지 않았으므로 Kaspersky Industrial CyberSecurity for Nodes가 활성화되지 않습니다. 해당 상태는 빨간색으로 강조 표시됩니다.
- **라이센스가 만료되었습니다** – 라이센스가 만료되어 Kaspersky Industrial CyberSecurity for Nodes가 활성화되지 않습니다. 해당 상태는 빨간색으로 강조 표시됩니다.
- **최종 사용자 라이센스 계약이 위반됐습니다** – 최종 사용자 라이센스 계약서의 조건을 위반하여 Kaspersky Industrial CyberSecurity for Nodes가 활성화되지 않습니다. 해당 상태는 빨간색으로 강조 표시됩니다.
- **키가 거부 목록에 있습니다** – 추가된 키 파일이 차단되고 Kaspersky에 의해 거부 목록에 등록됩니다. 예: 타사가 불법적으로 애플리케이션을 활성화하기 위해 키를 사용한 경우. 해당 상태는 빨간색으로 강조 표시됩니다.

현재 라이센스 정보 보기

현재 라이센스에 관한 정보를 보려면,

애플리케이션 콘솔 트리에서 **라이센스** 노드를 확장합니다.

현재 라이센스에 관한 일반 정보가 **라이센스** 노드의 세부 정보 창에 표시됩니다(아래 표 참조).

라이센스 노드에 있는 라이센스에 관한 일반 정보

필드	설명
활성화 코드 상태 또는 키 상태	활성화 코드 상태 또는 키 상태: *활성 키* 또는 *예약*.
만료 날짜	활성 키와 연관된 라이센스의 만료 날짜 및 시간입니다.
라이센스 유형	라이센스 유형: *상업용 라이센스*.
활성화 상태	활성화 상태 정보는 다음 값을 사용할 수 있습니다: • **적용됨** – 키를 사용하여 애플리케이션을 활성화한 경우. • **애플리케이션 활성화** – 애플리케이션 활성화를 위해 활성화 코드를 적용했지만, 활성화 프로세스가 아직 완료되지 않은 경우. 애플리케이션 활성화가 완료되고 노드의 세부 정보 창 내용을 새로 고침하면 상태가 **적용됨**로 변경됩니다. • **활성화 오류** – 애플리케이션 활성화에 실패할 경우. 작업 로그에서 활성화 실패 원인을 볼 수 있습니다.
키	애플리케이션을 활성화하기 위해 사용한 키의 숫자입니다.

라이센스의 상세 정보를 보려면,

라이센스 노드의 세부 정보 창에서 원하는 라이센스의 마우스 오른쪽 메뉴를 열고 **속성**를 선택합니다.

속성 <키 번호> 창의 상세 라이센스 정보

필드	설명
키	애플리케이션을 활성화하기 위해 사용한 키의 숫자입니다.
애플리케이션	추가된 키로 활성화된 애플리케이션의 이름입니다.
라이센스 유형	라이센스 유형: 상업용 또는 체험판.
라이센스 기간	애플리케이션 활성화 날짜부터 라이센스가 유효한 일 수입니다.
활성화 날짜	애플리케이션에 키를 추가한 날짜입니다.
만료 날짜	활성 키와 연관된 라이센스의 만료 날짜입니다. 무제한 등록으로 애플리케이션을 활성화한 경우 필드 값은 *제한 없음*입니다. Kaspersky Industrial CyberSecurity for Nodes를 사용하여 라이센스 만료 날짜을 판별할 수 없으면 필드값은 *알 수 없음*으로 설정됩니다.
만료까지 남은 일수	활성 키와 연관된 라이센스 만료 날짜까지 남은 일 수입니다.
기술 지원 제공 대상	Kaspersky 또는 파트너사에서 라이센스 조항에 따른 고객 기술 지원 제공 여부 관련 정보입니다.
지원 정보	기술 지원을 제공하는 Kaspersky 또는 협력사의 연락처 상세 정보입니다. 기술 지원이 제공되지 않는 경우 이 필드는 비어 있을 수 있습니다.
소유자 정보	라이센스 고객에 관한 정보입니다. 라이센스를 취득한 고객의 이름 또는 조직의 이름입니다.
라이센스 정보	현재 라이센스의 번호와 유형입니다.
기능	라이센스에 따라 사용 가능한 애플리케이션 기능입니다.

라이센스 갱신

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 라이센스 만료가 30일 남았을 때 사용자에게 알립니다.

만료 날짜 전에 예비 키를 사용하여 라이센스를 갱신할 수 있습니다. 그러면 현재 라이센스가 만료된 후 새 라이센스로 애플리케이션을 활성화하기 전에도 장치의 보호 상태를 유지할 수 있습니다.

라이센스를 갱신하려면:

1. 새 활성화 코드나 키 파일을 받습니다.
2. 애플리케이션 콘솔 트리에서 **라이센스** 노드를 선택합니다.
3. **라이센스** 노드의 결과 창에서 다음 동작 중 하나를 수행합니다:
   - 키 파일을 사용하여 라이센스를 갱신하려면:
     a. **키 추가** 링크를 클릭합니다.
     b. 열리는 창에서 **찾아보기** 버튼을 클릭합니다.
     c. 확장자가 .key인 새 키 파일을 선택합니다.
     d. **추가 키로 사용** 확인란을 선택합니다.
   - 활성화 코드를 사용하여 라이센스를 갱신하려면:
     a. **활성화 코드 추가** 링크를 클릭합니다.
     b. 창이 열리면 구매한 활성화 코드를 입력합니다.
     c. **추가 키로 사용** 확인란을 선택합니다.

     활성화 코드를 적용하려면 인터넷 연결이 필요합니다.
4. **확인** 버튼을 클릭합니다.

예비 키가 추가되고 현재 Kaspersky Industrial CyberSecurity for Nodes 라이센스가 만료되면 자동으로 적용됩니다.

키 삭제

추가된 키를 삭제하면 키 파일을 다시 적용하여 복원할 수 있습니다.

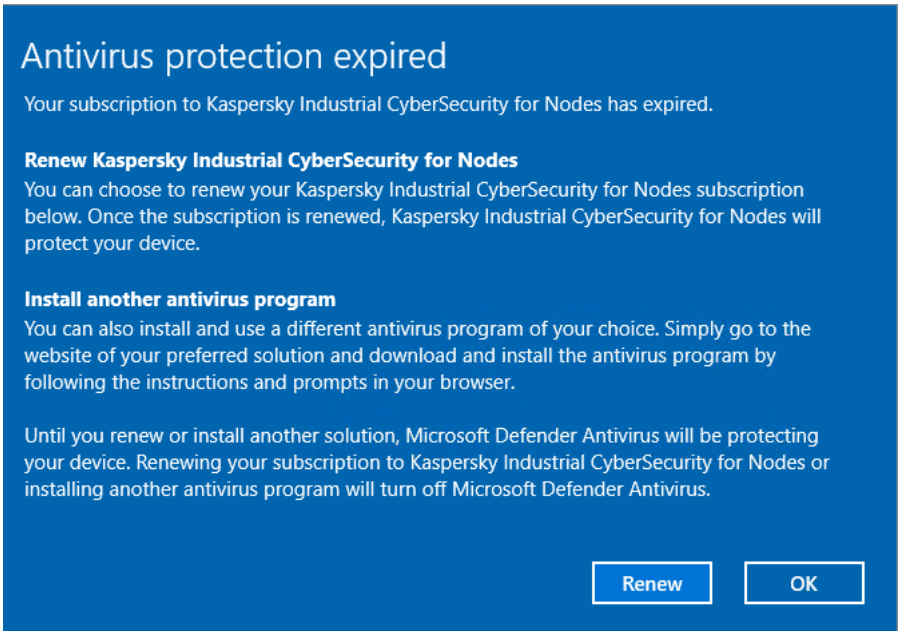
이전에 추가한 키를 제거하려면:

1. 애플리케이션 콘솔 트리에서 **라이센스** 노드를 선택합니다.
2. 추가된 키의 정보가 들어 있는 표의 **라이센스** 노드 결과 창에서 제거할 키를 선택합니다.
3. 선택한 키의 정보가 들어 있는 행의 마우스 오른쪽 메뉴에서 **제거** 옵션을 선택합니다.
4. 키 삭제를 확인하려면 확인 창에서 **예** 버튼을 클릭합니다.

선택한 키가 제거됩니다.

키를 제거하면 Kaspersky Industrial CyberSecurity for Nodes가 더는 컴퓨터를 보호하지 않습니다. 이 애플리케이션은 그 후 Windows Security Center(WSC)로 보호 상태 명령을 전송해 기본 제공 보호 도구를 활성화합니다. 이 애플리케이션은 이 과정에서 라이센스 갱신을 제안하는 창을 표시합니다(아래 그림 참조). 알림창이 다른 애플리케이션을 가려서 비활성화하고 싶다면 레지스트리에서 `NeedShowUPAOWindows=0` 키를 설정하십시오. 이 키는 `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.5.0\environment\`에 있습니다.

라이센스 갱신 창을 비활성화하면 Kaspersky Industrial CyberSecurity for Nodes가 Windows 보안 센터로 보호 상태 명령을 전송하지 않습니다. 즉, Windows 보안 센터가 기본 제공 보호 도구를 활성화하지 않습니다. 창을 비활성화할 때는 이 점을 염두에 두십시오.



라이센스 갱신을 제안하는 창

Kaspersky Industrial CyberSecurity for Nodes 시작 및 중지

이 섹션에는 Kaspersky Industrial CyberSecurity for Nodes 시작 및 중지에 관한 정보, Kaspersky Industrial CyberSecurity for Nodes 콘솔 및 Kaspersky Security Center 관리 콘솔용 관리 플러그인 시작에 관한 정보가 포함되어 있습니다.

애플리케이션 시작 및 중지

사용자 컴퓨터에 Kaspersky Industrial CyberSecurity for Nodes를 설치하고 나면 애플리케이션이 자동으로 시작됩니다. 기본적으로는 운영 체제를 시작하고 나면 Kaspersky Industrial CyberSecurity for Nodes가 자동으로 시작됩니다. 운영 체제 설정에서 애플리케이션의 자동 시작을 구성할 수 없습니다.

운영 체제가 시작된 후 Kaspersky Industrial CyberSecurity for Nodes 안티 바이러스 데이터베이스를 다운로드하면 컴퓨터 성능에 따라 최대 2분 정도 걸릴 수 있습니다. 이 시간 동안 컴퓨터 보호 레벨이 낮아집니다. 이미 시작된 운영 체제에서 Kaspersky Industrial CyberSecurity for Nodes가 시작될 때 안티 바이러스 데이터베이스를 다운로드하더라도 컴퓨터 보호 레벨이 낮아지지 않습니다.

Kaspersky Security Center 관리 콘솔에서 자동 애플리케이션 시작을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **애플리케이션 설정 → 보안 및 신뢰성** 옵션을 선택하고 **설정** 버튼을 클릭합니다.
4. **보안** 탭에서 **컴퓨터 시작 시 애플리케이션 시작(권장)** 확인란을 선택하거나 선택 해제하여, 애플리케이션의 자동 실행을 활성화하거나 비활성화합니다.
5. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 자동 애플리케이션 시작을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **애플리케이션 설정 → 보안 및 신뢰성**으로 갑니다.
5. **구성** 버튼을 클릭합니다.
   보안 및 신뢰성 창이 열립니다.

6. **컴퓨터 시작 시 애플리케이션 시작(권장)** 확인란을 사용하여 애플리케이션 자동 시작을 활성화하거나 비활성화합니다.

7. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 자동 애플리케이션 시작을 구성하는 방법

1. 애플리케이션 콘솔 트리의 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택합니다.

2. 노드의 마우스 오른쪽 메뉴에서 **애플리케이션 속성** 항목을 선택합니다.

3. 열린 창에서 **보안 설정** 탭을 선택합니다.

4. **컴퓨터 시작 시 애플리케이션 시작(권장)** 확인란을 사용하여 애플리케이션 자동 시작을 활성화하거나 비활성화합니다.

5. 변경 사항을 저장합니다.

사용자가 보호 중인 서버의 관리자 그룹 멤버인 경우 Kaspersky Industrial CyberSecurity for Nodes를 시작 및 중지할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 애플리케이션을 시작하거나 중지하는 방법

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.

2. 작업 공간에서 **기기** 탭을 선택합니다.

3. 더블 클릭해 컴퓨터 속성 창을 엽니다.

4. 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.

5. 컴퓨터에 설치된 Kaspersky 애플리케이션 목록에서 **Kaspersky Industrial CyberSecurity for Nodes(5.0.0)**를 선택합니다.

6. 다음 중 하나를 수행합니다:

   - 애플리케이션을 시작하려면 Kaspersky 애플리케이션 목록의 오른쪽에 있는 버튼을 클릭하거나 다음을 수행하십시오.

   - 애플리케이션을 중지하려면 Kaspersky 애플리케이션 목록의 오른쪽에 있는 버튼을 클릭하거나 다음을 수행하십시오.

Kaspersky Security Center 웹 콘솔에서 애플리케이션을 시작하거나 중지하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes를 시작하거나 중지할 컴퓨터의 이름을 누릅니다.
   컴퓨터 속성 창이 열립니다.

3. **애플리케이션** 탭을 선택합니다.

4. **Kaspersky Industrial CyberSecurity for Nodes(5.0.0)** 옆의 확인란을 선택합니다.

5. **시작** 또는 **중지** 버튼을 클릭합니다.

애플리케이션 콘솔에서 애플리케이션을 시작 또는 중지하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes를 중지하려면:

   a. 애플리케이션 콘솔을 엽니다.

   > 사용자 계정에는 **애플리케이션 종료** 기능에 액세스할 수 있는 권한이 있어야 합니다.

   b. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 마우스 오른쪽 메뉴를 엽니다.

   c. **애플리케이션 중지** 옵션을 선택합니다.

   d. 확인 창에서 **예** 버튼을 클릭하여 애플리케이션 중지를 확인합니다.
   애플리케이션이 중지됩니다.

2. **Kaspersky Industrial CyberSecurity for Nodes**를 시작하려면:

   a. 보호 중인 장치의 애플리케이션 콘솔 설치 폴더에 있는 avpui.exe 파일을 실행합니다. 기본적으로 파일은 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Console 폴더에 있습니다.
   보호 중인 장치 선택 창이 열립니다.

   b. Kaspersky Industrial CyberSecurity for Nodes와 애플리케이션 콘솔을 같은 컴퓨터에 설치했다면 **로컬 컴퓨터(애플리케이션 콘솔이 실행 중인 컴퓨터)** 옵션을 선택합니다.

   c. Kaspersky Industrial CyberSecurity for Nodes와 애플리케이션 콘솔이 다른 컴퓨터에 설치되어 있다면:

      1. **다른 장치** 옵션을 선택합니다.

      2. **찾아보기** 옵션을 클릭하고 애플리케이션을 설치한 컴퓨터의 이름을 지정합니다.

      3. 애플리케이션이 설치된 컴퓨터에 연결할 포트를 지정합니다.

         - **Windows 자격 증명 사용**. Windows 자격 증명을 사용하여 연결하는 포트. 기본값은 13032입니다.
         - **수동으로 생성된 사용자의 자격 증명을 사용**. 직접 생성한 사용자의 자격 증명을 사용하여 연결하는 포트. 기본값은 13031입니다.

   d. 필요한 경우 **인증 사용** 기능을 활성화하고 자격 증명을 입력하여 애플리케이션 콘솔을 애플리케이션이 설치된 컴퓨터에 연결합니다. 지정한 사용자 계정에는 애플리케이션이 설치된 컴퓨터에서 **설정 읽기** 및 **애플리케이션에 원격 연결** 기능에 액세스할 수 있는 권한이 있어야 합니다.

   e. **애플리케이션 관리 서비스** 버튼을 클릭합니다.

   f. 열리는 창에서 **시작** 버튼을 클릭합니다.
   애플리케이션이 시작됩니다.

보호 중인 장치 선택 창은 애플리케이션이 설치된 컴퓨터와의 연결이 끊기거나 KICS 서비스에 실패했을 때도 표시됩니다. **시작** 버튼을 클릭하면 KICS 서비스를 복원할 수 있습니다.

명령줄에서 애플리케이션을 시작하거나 중지할 수도 있습니다.

컴퓨터 보호 및 제어 일시 중지 및 다시 시작

컴퓨터 보호 및 제어 일시 중지는 Kaspersky Industrial CyberSecurity for Nodes의 모든 보호 및 제어 구성 요소를 잠시 동안 중지하는 것입니다.

애플리케이션 상태는 작업 표시줄 알림 영역의 애플리케이션 아이콘을 통해 표시됩니다.

- 아이콘은 컴퓨터 보호 및 제어가 일시 중지되었음을 나타냅니다.
- 아이콘은 컴퓨터 보호 및 제어가 활성화되었음을 나타냅니다.

컴퓨터 보호 및 제어를 일시 중지해도 검사 작업이나 업데이트 작업에 영향을 주지 않습니다.

컴퓨터 보호 및 제어를 일시 중지하거나 다시 시작할 때 네트워크 연결이 이미 설정되어 있는 경우 해당 네트워크 연결 종료에 대한 알림 메시지가 표시됩니다.

컴퓨터 보호 및 제어를 일시 중지하려면 다음과 같이 하십시오.

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 마우스 오른쪽 메뉴를 엽니다.
2. **보호 일시 중지** 옵션을 선택합니다.
3. 다음 옵션 중 하나를 선택합니다:
   - **지정된 시간 동안 일시 중지 <지정한 시간>** - 아래의 드롭다운 목록에서 지정한 시간이 지나면 컴퓨터 보호 및 제어가 다시 시작됩니다.
   - **재시작까지 일시 중지** - 애플리케이션을 종료한 후에 다시 열거나 운영 체제를 다시 시작하면 컴퓨터 보호 및 제어가 다시 시작됩니다. 이 옵션을 사용하려면 애플리케이션 자동 시작이 설정되어 있어야 합니다.
   - **일시 중지** - 사용자가 직접 컴퓨터 보호 및 제어를 다시 시작하도록 선택하면 다시 시작됩니다.

Kaspersky Industrial CyberSecurity for Nodes는 정책에서 자물쇠() 표시가 없는 모든 보호 및 제어 구성 요소의 작동을 일시 중지합니다.

컴퓨터 보호 및 제어를 다시 시작하려면 다음과 같이 하십시오.

1. 작업 표시줄 알림 영역에 있는 애플리케이션 아이콘의 마우스 오른쪽 메뉴를 엽니다.
2. 마우스 오른쪽 메뉴에서 **보호 다시 시작**를 선택합니다.

사용자가 컴퓨터 보호 및 제어를 다시 시작하기로 선택한 경우 이전에 선택한 컴퓨터 보호 및 제어 일시 중지 옵션에 상관없이 언제든지 다시 시작할 수 있습니다.

간편 진단 인터페이스

이 섹션에서는 간편 진단 인터페이스의 사용에 관해 설명합니다.

간편 진단 인터페이스 정보

간편 진단 인터페이스 구성 요소는 애플리케이션 콘솔과 별도로 시스템 트레이 아이콘 구성 요소와 함께 설치 및 제거되며, 보호 중인 장치에 애플리케이션 콘솔이 설치되어 있지 않은 경우에도 사용할 수 있습니다. 간편 진단 인터페이스는 시스템 트레이 아이콘에서 시작되거나, 보호 중인 장치의 애플리케이션 폴더에서 avpui.exe를 실행하여 시작됩니다.

간편 진단 인터페이스에서 다음을 수행할 수 있습니다:

- 설치된 업데이트 및 사용 가능한 패치 목록이 있는 **정보** 창 열기.
- 일반 애플리케이션 상태에 관한 정보 검토.
- 발생한 보안 인시던트 검토.
- 보호 중인 장치의 현재 동작 검토.
- 덤프 및 추적 파일 작성 시작 또는 중지.
- 휴대용 감사 도구 생성.
- 애플리케이션 콘솔을 엽니다.

간편 진단 인터페이스는 Kaspersky Industrial CyberSecurity for Nodes 기능에 대한 접근이 암호로 보호된 경우에도 사용할 수 있습니다. 암호는 필요하지 않습니다.

> 간편 진단 인터페이스 구성 요소는 Kaspersky Security Center를 통해서 구성할 수 없습니다.

간편 진단 인터페이스를 통해 Kaspersky Industrial CyberSecurity for Nodes 상태 검토

간편 진단 인터페이스를 사용하여 애플리케이션 상태를 보려면:

1. 다음 방법 중 하나로 간편 진단 인터페이스를 엽니다.
   - 보호 중인 장치의 애플리케이션 설치 폴더에 있는 avpui.exe 파일을 실행합니다. 기본적으로 파일은 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0에 있습니다.
   - 작업 표시줄 알림 영역의 애플리케이션 아이콘을 클릭합니다.

2. **보호 상태** 섹션에서 키, 실시간 컴퓨터 보호 작업, 업데이트 작업의 현재 상태를 검토하십시오. 다양한 색상이 사용자에게 보호 상태를 알리는 데 사용됩니다(아래 표 참조).

간편 진단 인터페이스 창의 색상 표시

섹션	상태
실시간 보호 상태	다음 조건이 충족되는 경우 패널은 *초록색*입니다: • 실시간 파일 보호 구성 요소가 활성화되어있습니다. • 애플리케이션 실행 제어 구성 요소는 **차단** 모드에서 실행 중입니다.
	다음 조건 중 하나 이상이 충족되는 경우 패널은 *노란색*입니다: • 실시간 파일 보호 구성 요소가 비활성화되어있습니다. • 애플리케이션 실행 제어 구성 요소는 **알림** 모드에서 실행 중입니다.
	다음 조건 중 하나 이상이 충족되는 경우 패널은 *빨간색*입니다: • 실시간 파일 보호 구성 요소가 비활성화되었거나 설치되지 않았습니다. • 애플리케이션 실행 제어 구성 요소가 설치되지 않았거나 **알림** 모드에서 실행 중입니다.
라이센스	현재 라이센스가 유효한 경우 패널은 *초록색*입니다.
	노란색 패널은 다음 이벤트 중 하나가 발생했음을 나타냅니다: • *라이센스 상태 확인.* • *라이센스가 14일 이내에 만료되고 입력된 추가 키나 활성화 코드가 없습니다.* • *추가된 키가 거부 목록에 포함되어 곧 차단됩니다.*
	빨간색 패널은 다음 이벤트 중 하나가 발생했음을 나타냅니다: • *애플리케이션이 활성화되지 않았습니다.* • *라이센스가 만료되었습니다.* • *최종 사용자 라이센스 계약이 위반됐습니다.* • *키가 거부 목록에 있습니다.*
업데이트	애플리케이션 데이터베이스가 최신 상태일 경우 패널은 *초록색*입니다.
	애플리케이션 데이터베이스가 오래된 경우 패널은 *노란색*입니다.
	애플리케이션 데이터베이스가 매우 오래된 경우 패널은 *빨간색*입니다.

보안 이벤트 통계 검토

통계 섹션에는 모든 보안 이벤트가 표시됩니다. 각 보호 작업 통계는 인시던트 수와 마지막 인시던트가 발생한 날짜 및 시간을 지정하는 별도의 블록에 표시됩니다. 인시던트가 기록되면 블록 색상이 빨간색으로 바뀝니다.

통계를 보려면:

1. 다음 방법 중 하나로 간편 진단 인터페이스를 엽니다.

   - 보호 중인 장치의 애플리케이션 설치 폴더에 있는 avpui.exe 파일을 실행합니다. 기본적으로 파일은 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0에 있습니다.
   - 작업 표시줄 알림 영역의 애플리케이션 아이콘을 클릭합니다.

2. **통계** 섹션으로 갑니다.

3. 보호 작업에 대한 보안 인시던트를 검토하십시오.

현재 애플리케이션 활동 검토

보호 중인 장치에서 현재 애플리케이션 활동을 검토하려면:

1. 다음 방법 중 하나로 간편 진단 인터페이스를 엽니다.
   - 보호 중인 장치의 애플리케이션 설치 폴더에 있는 avpui.exe 파일을 실행합니다. 기본적으로 파일은 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0에 있습니다.
   - 작업 표시줄 알림 영역의 애플리케이션 아이콘을 클릭합니다.
2. **현재 애플리케이션 활동** 섹션으로 갑니다.

다양한 색상이 애플리케이션 활동 상태를 표시하는 데 사용됩니다:

- **작업** 섹션에서:
  - *초록색.* 노란색이나 빨간색이 필요할 만한 조건이 없습니다.
  - *노란색.* 중요한 영역을 장기간 검사하지 않았습니다.
  - *빨간색.* 다음 조건 중 하나 이상이 충족됩니다:
    - 시작된 작업이 없으며 모든 작업에 대해 시작 스케줄이 설정되지 않았습니다.
    - 애플리케이션 실행 오류는 심각 이벤트로 기록됩니다.
- **Kaspersky Security Network** 섹션에서:
  - *초록색.* **KSN 사용** 작업이 시작됩니다.
  - *노란색.* KSN 진술문이 승인되었지만 작업이 시작되지 않았습니다.

애플리케이션 추적 로그 및 메모리 덤프 기록 구성

애플리케이션 추적 로그 및 메모리 덤프 기록을 구성하려면:

1. 다음 방법 중 하나로 간편 진단 인터페이스를 엽니다.
   - 보호 중인 장치의 애플리케이션 설치 폴더에 있는 avpui.exe 파일을 실행합니다. 기본적으로 파일은 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0에 있습니다.
   - 작업 표시줄 알림 영역의 애플리케이션 아이콘을 클릭합니다.
2. **오작동 진단** 섹션으로 갑니다.
3. **덤프 및 추적 파일 보호 사용** 확인란을 사용하여 덤프 파일 및 추적 파일 보호를 활성화하거나 비활성화합니다.

덤프 파일 및 추적 파일 보호를 작동한 경우 다음 사용자가 파일에 접근할 수 있습니다:

- 시스템 관리자와 로컬 관리자, 그리고 덤프 파일 및 추적 파일 쓰기가 설정된 사용자가 덤프 파일에 접근할 수 있습니다.
- 시스템 관리자와 로컬 관리자만 추적 파일에 접근할 수 있습니다.

4. **추적 파일에 디버그 정보를 씁니다** 확인란을 사용하여 애플리케이션 동작 추적을 활성화하거나 비활성화합니다.

   기본적으로 애플리케이션 동작 추적이 비활성화되었습니다.

5. 필요하다면 Kaspersky Industrial CyberSecurity for Nodes 추적 파일을 저장할 기본 폴더를 변경합니다. 변경하려면 **찾아보기** 버튼을 클릭하고 필요한 폴더를 선택합니다.

   > 폴더는 사전에 생성되어야 하고 SYSTEM 계정으로 작성 가능해야 합니다. 네트워크 폴더, 드라이브, 환경 변수는 지정할 수 없습니다.

   선택한 폴더에서 Kaspersky Industrial CyberSecurity for Nodes는 추적 파일을 저장하기 위해 logs-Kaspersky Industrial CyberSecurity for Nodes-<uid>라는 하위 폴더를 생성합니다. 여기서 <uid>는 8자의 고유 로그 식별자입니다.

6. 디버그 정보의 상세 수준을 선택합니다:

   - **일반**은 추적 파일이 모든 오류, 경고에 관한 메시지는 물론 애플리케이션의 정상 작동에 관한 정보도 저장한다는 뜻입니다(기본값).
   - **심각**은 추적 파일이 치명적인 오류에 관한 메시지만 저장한다는 뜻입니다.
   - **진단**은 추적 파일이 경고뿐만 아니라 모든 오류에 관한 메시지를 저장한다는 뜻입니다.
   - **중요**는 추적 파일이 모든 오류, 경고, 추가 정보에 관한 메시지를 저장한다는 뜻입니다.
   - **정밀**은 추적 파일이 애플리케이션의 작동에 관한 모든 정보를 저장한다는 뜻입니다.

   기술 지원 담당자가 잠재적 문제를 해결하는 데 필요한 상세 수준을 결정합니다.

7. 오래된 추적 파일을 삭제하려면 **가장 오래된 추적 파일 제거** 기능을 활성화합니다.

   이 기능이 활성화된 경우 추적 파일의 최대 크기와 개수를 구성합니다:

   a. **추적 파일 최대 크기(MB)** 값을 지정합니다.

      사용 가능한 값: 1~4095MB. 기본값은 100MB입니다.

   b. **최대 추적 파일 개수** 값을 지정합니다.

      사용 가능한 값: 1부터 999까지. 기본값은 5입니다.

8. **오작동 시 폴더로 덤프 파일 생성** 확인란을 사용하여 애플리케이션 동작 추적을 활성화하거나 비활성화합니다.

   기본적으로 메모리 덤프 기록이 비활성화되었습니다.

9. 필요하다면 Kaspersky Industrial CyberSecurity for Nodes 추적 파일을 저장할 기본 폴더를 변경합니다. 변경하려면 **찾아보기** 버튼을 클릭하고 필요한 폴더를 선택합니다.

   폴더는 사전에 생성되어야 하고 SYSTEM 계정으로 작성 가능해야 합니다. 네트워크 폴더, 드라이브, 환경 변수는 지정할 수 없습니다.

10. **적용** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes 자기 보호

자기 보호는 다른 애플리케이션이 Kaspersky Industrial CyberSecurity for Nodes의 작동을 방해할 수 있는 동작을 수행하지 못하도록 합니다. 애플리케이션에는 폴더와 메모리 프로세스, 시스템 레지스트리 항목의 수정이나 삭제로부터 애플리케이션을 보호하는 자기 보호 메커니즘이 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 Microsoft의 Antimalware Protected Process Light (AM-PPL) 기술을 지원하며, 이는 악성 활동으로부터 애플리케이션 프로세스를 보호합니다. 또한, 애플리케이션을 통해 애플리케이션 기능에 대한 사용자 접근 권한과 애플리케이션 서비스에 대한 사용자 접근 권한을 별도로 관리할 수 있습니다.

자기 보호 기능 작동 및 중지

Kaspersky Industrial CyberSecurity for Nodes가 하드 드라이브의 애플리케이션 파일, 메모리 프로세스 및 시스템 레지스트리의 항목에 대한 변경이나 삭제를 방지합니다.

이 기술은 다음 애플리케이션 구성 요소에 대한 접근을 차단합니다:

- Kaspersky Industrial CyberSecurity for Nodes 설치 폴더의 파일 및 애플리케이션의 기타 파일;
- 애플리케이션에 속한 레코드가 있는 레지스트리 키;
- 애플리케이션이 실행하는 프로세스.

> 신뢰할 수 없는 상위 프로세스에서 시작된 Kaspersky Industrial CyberSecurity for Nodes 프로세스에는 자기 보호 메커니즘이 적용되지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes의 자기 보호 메커니즘은 기본값으로 활성화됩니다.

Kaspersky Security Center 관리 콘솔에서 자기 보호를 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **애플리케이션 설정** 섹션으로 갑니다.
4. **보안 및 신뢰성** 블록에서 **설정** 버튼을 클릭합니다.
5. 열린 창에서 **보안** 탭을 선택합니다.
6. **자기 보호** 블록에서, **외부 위협으로부터 애플리케이션 프로세스 보호** 확인란으로 자기 보호를 활성화하거나 비활성화합니다.
7. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.
8. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

애플리케이션 콘솔에서 자기 보호를 활성화 또는 비활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고 결과 창에서 **애플리케이션 속성** 링크를 따라갑니다.
2. 열린 창에서 **보안 설정** 탭을 선택합니다.
3. **자기 보호** 블록에서, **외부 위협으로부터 애플리케이션 프로세스 보호** 확인란으로 자기 보호를 활성화하거나 비활성화합니다.
4. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 자기 보호를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **애플리케이션 설정** 섹션을 선택합니다.
5. **보안 및 신뢰성** 블록에서 **구성** 버튼을 클릭합니다.
   보안 및 신뢰성 창이 열립니다.
6. **자기 보호** 블록에서, **외부 위협으로부터 애플리케이션 프로세스 보호** 확인란으로 자기 보호를 활성화하거나 비활성화합니다.
7. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.
8. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

AM-PPL 기술 지원

Kaspersky Industrial CyberSecurity for Nodes는 Microsoft의 Antimalware Protected Process Light 기술(이하 "AM-PPL"이라고 함)을 지원합니다. AM-PPL은 Kaspersky Industrial CyberSecurity for Nodes 프로세스를 악의적인 작업(예: 애플리케이션 종료)으로부터 보호합니다. AM-PPL은 신뢰할 수 있는 프로세스만 실행할 수 있도록 허용합니다. Kaspersky Industrial CyberSecurity for Nodes 프로세스는 Windows 보안 요구 사항에 따라 서명되므로 신뢰할 수 있는 것입니다. AM-PPL 기술에 대한 자세한 내용은 Microsoft 웹사이트를 방문하시기 바랍니다. AM-PPL 기술은 기본값으로 활성화되어 있습니다.

또한 Kaspersky Industrial CyberSecurity for Nodes에는 애플리케이션 프로세스를 보호하기 위한 메커니즘이 내장되어 있습니다. AM-PPL 지원을 통해 프로세스 보안 기능을 운영 체제에 위임할 수 있습니다. 따라서 애플리케이션의 속도를 높이고 컴퓨터 리소스의 사용을 줄일 수 있습니다.

애플리케이션이 Kaspersky Industrial CyberSecurity for Nodes (AVP) 서비스 및 Kaspersky Seamless Update Service(AVPSUS) 서비스를 등록합니다. AM-PPL 기술은 AVP 서비스만 보호합니다.

AM-PPL 기술을 항상 활성 상태로 유지하십시오. AM-PPL은 운영 체제 보호에 중요한 구성 요소입니다. AM-PPL은 애플리케이션 문제 해결을 위해 별도의 테스트 환경에서만 비활성화할 수 있습니다.

AM-PPL 기술은 Windows 10 1703(RS2) 버전 이상 및 Windows Server 2019 운영 체제에서 사용할 수 있습니다.

AM-PPL 기술을 활성화하거나 비활성화하려면 다음을 수행합니다.

1. 애플리케이션의 자기 보호 메커니즘 끄기.

   자기 보호 메커니즘은 AM-PPL 상태 변경을 포함한 컴퓨터 메모리에서의 애플리케이션 프로세스 수정과 삭제를 방지합니다.

2. 명령줄 해석기(cmd)를 관리자 권한으로 실행합니다.
3. Kaspersky Industrial CyberSecurity for Nodes 실행 파일이 있는 폴더로 이동합니다.
4. AM-PPL 기술 지원을 활성화하려면 다음 명령을 실행합니다:

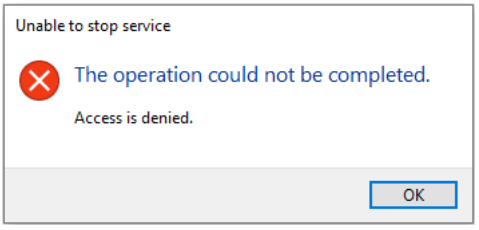
   ```
   klpsm.exe enable
   ```

5. AM-PPL 기술 지원을 비활성화하려면 다음 명령을 실행합니다:

   ```
   klpsm.exe disable
   ```

6. Kaspersky Industrial CyberSecurity for Nodes를 다시 시작합니다.
7. 애플리케이션의 자기 보호 메커니즘 다시 시작.

그 결과 사용자가 AVP 서비스를 중지하려고 하면 오류 메시지와 함께 시스템 창이 표시됩니다. 사용자는 Kaspersky Industrial CyberSecurity for Nodes 인터페이스에서만 애플리케이션 서비스를 관리할 수 있습니다.



애플리케이션 서비스 접근 오류

운영 체제 서비스 보호하기

운영 체제 서비스 보호하기 기능을 사용하여 타사 애플리케이션이 운영 체제 서비스에 영향을 주는 것을 허용하거나 금지할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 운영 체제 서비스 보호를 활성화하거나 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **애플리케이션 설정** 섹션으로 갑니다.
4. **보안 및 신뢰성** 블록에서 **설정** 버튼을 클릭합니다.
5. 열린 창에서 **보안** 탭을 선택합니다.
6. **운영 체제 서비스 보호하기** 확인란을 사용하여 운영 체제 서비스 보호를 활성화하거나 비활성화합니다.
   운영 체제 서비스 보호를 활성화하면 타사 애플리케이션이 운영 체제의 프로세스를 작동할 수 없습니다.
   운영 체제 서비스 보호가 비활성화되면 타사 애플리케이션이 운영 체제의 프로세스에 따라 작동할 수 있습니다.
   기능을 활성화 또는 비활성화한 후 변경 사항을 적용하려면 컴퓨터를 다시 시작해야 합니다.
7. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.
8. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

애플리케이션 콘솔에서 운영 체제 서비스 보호를 활성화하거나 비활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고 결과 창에서 **애플리케이션 속성** 링크를 따라갑니다.
2. 열린 창에서 **보안 설정** 탭을 선택합니다.
3. **운영 체제 서비스 보호하기** 확인란을 사용하여 운영 체제 서비스 보호를 활성화하거나 비활성화합니다.
   운영 체제 서비스 보호를 활성화하면 타사 애플리케이션이 운영 체제의 프로세스를 작동할 수 없습니다.
   운영 체제 서비스 보호가 비활성화되면 타사 애플리케이션이 운영 체제의 프로세스에 따라 작동할 수 있습니다.
   기능을 활성화 또는 비활성화한 후 변경 사항을 적용하려면 컴퓨터를 다시 시작해야 합니다.
4. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 운영 체제 서비스 보호를 활성화하거나 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **애플리케이션 설정** 섹션을 선택합니다.
5. **보안 및 신뢰성** 블록에서 **구성** 버튼을 클릭합니다.
   보안 및 신뢰성 창이 열립니다.
6. **운영 체제 서비스 보호하기** 확인란을 사용하여 운영 체제 서비스 보호를 활성화하거나 비활성화합니다.
   운영 체제 서비스 보호를 활성화하면 타사 애플리케이션이 운영 체제의 프로세스를 작동할 수 없습니다.

운영 체제 서비스 보호가 비활성화되면 타사 애플리케이션이 운영 체제의 프로세스에 따라 작동할 수 있습니다.

기능을 활성화 또는 비활성화한 후 변경 사항을 적용하려면 컴퓨터를 다시 시작해야 합니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

8. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes를 관리하기 위한 사용자 권한 구성

기본적으로 보호 중인 장치의 관리자 그룹 구성원, Kaspersky Industrial CyberSecurity for Nodes를 설치할 때 보호 중인 장치에서 생성되는 KICS 관리자 그룹의 구성원, SYSTEM 그룹은 Kaspersky Industrial CyberSecurity for Nodes의 모든 기능에 접근할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 사용자 목록에 등록되지 않은 사용자는 애플리케이션 콘솔을 열 수 없습니다.

개별 사용자 또는 사용자 그룹에 대해 Kaspersky Industrial CyberSecurity for Nodes의 특정 기능에 대한 접근을 허용하거나 차단할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 기능에 대한 접근 권한 정보

사용자 권한	설명
작업 관리	Kaspersky Industrial CyberSecurity for Nodes 작업을 시작/중지/일시 중지/다시 시작할 수 있습니다.
작업 생성 및 삭제	온디맨드 검사 작업을 만들고 삭제할 수 있습니다.
설정 편집	다음을 수행할 수 있습니다: • 구성 파일에서 Kaspersky Industrial CyberSecurity for Nodes 설정을 가져옵니다. • 애플리케이션 설정을 편집합니다.
설정 읽기	다음을 수행할 수 있습니다: • Kaspersky Industrial CyberSecurity for Nodes 일반 설정 및 작업 설정을 봅니다. • Kaspersky Industrial CyberSecurity for Nodes 설정을 구성 파일로 내보냅니다. • 작업 로그, 시스템 감사 로그, 알림의 설정을 봅니다.
저장소 관리	다음을 수행할 수 있습니다: • 격리 저장소로 개체를 이동시킵니다. • 격리 및 백업 저장소에서 개체를 제거합니다. • 격리 및 백업 저장소에서 개체를 복원합니다.
로그 관리	작업 로그를 삭제하고 시스템 감사 로그를 정리할 수 있습니다.
로그 읽기	작업 로그와 시스템 감사 로그에서 안티 바이러스 이벤트를 볼 수 있습니다.
통계 검색	각 Kaspersky Industrial CyberSecurity for Nodes 작업의 통계를 볼 수 있습니다.
애플리케이션 라이센스 관리	Kaspersky Industrial CyberSecurity for Nodes를 활성화할 수 있습니다.
애플리케이션 설치 제거	Kaspersky Industrial CyberSecurity for Nodes를 삭제할 수 있습니다.
권한 읽기	Kaspersky Industrial CyberSecurity for Nodes 사용자 및 사용자 접근 권한 목록을 볼 수 있습니다.
권한 편집	다음을 수행할 수 있습니다: • 애플리케이션 관리에 접근할 수 있는 사용자 목록을 편집합니다. • Kaspersky Industrial CyberSecurity for Nodes 기능에 대한 사용자 접근 권한을 편집합니다.
애플리케이션에 원격 연결	애플리케이션 콘솔을 사용하여 애플리케이션에 원격으로 연결할 수 있습니다. 원격 접근을 위해서는 사용자에게 **설정 읽기** 기능에 대한 접근 권한 또한 있어야 합니다.

사용자 권한	설명
애플리케이션 종료	애플리케이션 콘솔을 사용하여 애플리케이션을 종료할 수 있습니다.
Kaspersky Security Center 정책 비활성화	Kaspersky Security Center 정책을 비활성화할 수 있습니다.
설정 내보내기	Kaspersky Industrial CyberSecurity for Nodes 설정을 내보낼 수 있습니다.
오작동 진단 편집	애플리케이션 추적 로그 및 메모리 덤프 기록을 구성할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes를 관리하기 위해 사용자 권한을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **보충** 옵션을 선택합니다.
4. **애플리케이션 관리를 위한 사용자 접근 권한** 섹션에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면, 해당 창에서 **수동으로 생성된 사용자의 자격 증명을 사용하여 애플리케이션의 작업 확인 허용** 확인란을 클릭한 다음 KLAdmin 사용자 계정의 암호를 설정합니다. 사용자 계정이 사용자 계정 목록에 자동으로 추가됩니다.
6. 필요하다면 애플리케이션 관리 접근 권한을 부여할 사용자 계정을 추가합니다. 그렇게 하려면 사용자 계정 표에서 **추가**을(를) 클릭합니다.

   사용자 접근 권한 구성 양식이 열립니다.
7. 사용자를 추가할 때 사용할 방법을 선택합니다:

   - **Active Directory에서 사용자/그룹 선택**. Active Directory 도메인 내 개별 사용자 또는 그룹에 Kaspersky Industrial CyberSecurity for Nodes 접근을 허용할 수 있습니다. 예를 들어 Everyone 그룹에 대해 애플리케이션 종료가 차단된 경우 개별 사용자에게 **애플리케이션 종료** 권한을 부여할 수 있습니다.
   - **사용자/사용자 그룹 직접 추가**. Active Directory에 존재하지 않는 사용자 계정을 만들고 해당 사용자 계정에 개별 권한을 할당할 수 있습니다. 즉 *서비스 사용자 계정*을 만들고 KLAdmin 대신 사용할 수 있습니다. 이렇게 하면 다른 사용자와 KLAdmin 암호를 공유하거나 새 Active Directory 사용자 계정을 만들 필요가 없습니다. 사용자 이름 및 암호를 지정할 수 있습니다. 예를 들어 서비스 사용자 계정에 **로그 읽기** 권한을 부여할 수 있습니다. 그 결과 모든 그룹에서 리포트 보기가 금지된 경우 서비스 사용자 계정 또는 KLAdmin 사용자 계정으로 리포트를 열 수 있습니다.

     사용자 또는 사용자 그룹을 직접 추가하려면 암호 보호를 활성화해야 합니다.
8. 애플리케이션 관리에 대한 접근을 부여할 사용자 또는 사용자 그룹을 선택합니다.
9. **권한** 목록에서 애플리케이션 기능에 대한 사용자 접근 권한을 구성합니다.
10. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes를 관리하기 위한 사용자 권한을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **애플리케이션 관리를 위한 사용자 접근 권한** 옵션을 선택합니다.

2. 창이 열리면, 해당 창에서 **수동으로 생성된 사용자의 자격 증명을 사용하여 애플리케이션의 작업 확인 허용** 확인란을 클릭한 다음 KLAdmin 사용자 계정의 암호를 설정합니다. 사용자 계정이 사용자 계정 목록에 자동으로 추가됩니다.

3. 필요하다면 애플리케이션 관리 접근 권한을 부여할 사용자 계정을 추가합니다. 그렇게 하려면 사용자 계정 표에서 **추가**을(를) 클릭합니다.

   사용자 접근 권한 구성 양식이 열립니다.

4. 사용자를 추가할 때 사용할 방법을 선택합니다:

   - **Active Directory에서 사용자/그룹 선택**. Active Directory 도메인 내 개별 사용자 또는 그룹에 Kaspersky Industrial CyberSecurity for Nodes 접근을 허용할 수 있습니다. 예를 들어 Everyone 그룹에 대해 애플리케이션 종료가 차단된 경우 개별 사용자에게 **애플리케이션 종료** 권한을 부여할 수 있습니다.

   - **사용자/사용자 그룹 직접 추가**. Active Directory에 존재하지 않는 사용자 계정을 만들고 해당 사용자 계정에 개별 권한을 할당할 수 있습니다. 즉 *서비스 사용자 계정*을 만들고 KLAdmin 대신 사용할 수 있습니다. 이렇게 하면 다른 사용자와 KLAdmin 암호를 공유하거나 새 Active Directory 사용자 계정을 만들 필요가 없습니다. 사용자 이름 및 암호를 지정할 수 있습니다. 예를 들어 서비스 사용자 계정에 **로그 읽기** 권한을 부여할 수 있습니다. 그 결과 모든 그룹에서 리포트 보기가 금지된 경우 서비스 사용자 계정 또는 KLAdmin 사용자 계정으로 리포트를 열 수 있습니다.

     사용자 또는 사용자 그룹을 직접 추가하려면 암호 보호를 활성화해야 합니다.

5. 애플리케이션 관리에 대한 접근을 부여할 사용자 또는 사용자 그룹을 선택합니다.

6. **권한** 목록에서 애플리케이션 기능에 대한 사용자 접근 권한을 구성합니다.

7. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes를 관리하기 위한 사용자 접근 권한을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보충** → **애플리케이션 관리를 위한 사용자 접근 권한** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. 창이 열리면, 해당 창에서 **수동으로 생성된 사용자의 자격 증명을 사용하여 애플리케이션의 작업 확인 허용** 확인란을 클릭한 다음 KLAdmin 사용자 계정의 암호를 설정합니다. 사용자 계정이 사용자 계정 목록에 자동으로 추가됩니다.

6. 필요하다면 애플리케이션 관리 접근 권한을 부여할 사용자 계정을 추가합니다. 그렇게 하려면 사용자 계정 표에서 **추가**을(를) 클릭합니다.

   사용자 접근 권한 구성 양식이 열립니다.

7. 사용자를 추가할 때 사용할 방법을 선택합니다:

   - **Active Directory에서 사용자/그룹 선택**. Active Directory 도메인 내 개별 사용자 또는 그룹에 Kaspersky Industrial CyberSecurity for Nodes 접근을 허용할 수 있습니다. 예를 들어 Everyone 그룹에 대해 애플리케이션 종료가 차단된 경우 개별 사용자에게 **애플리케이션 종료** 권한을 부여할 수 있습니다.

   - **사용자/사용자 그룹 직접 추가**. Active Directory에 존재하지 않는 사용자 계정을 만들고 해당 사용자 계정에 개별 권한을 할당할 수 있습니다. 즉 *서비스 사용자 계정*을 만들고 KLAdmin 대신 사용할 수 있습니다. 이렇게 하면 다른 사용자와 KLAdmin 암호를 공유하거나 새 Active Directory 사용자 계정을 만들 필요가 없습니다. 사용자 이름 및 암호를 지정할 수 있습니다. 예를 들어 서비스 사용자 계정에 **로그 읽기** 권한을 부여할 수 있습니다. 그 결과 모든 그룹에서 리포트 보기가 금지된 경우 서비스 사용자 계정 또는 KLAdmin 사용자 계정으로 리포트를 열 수 있습니다.

     사용자 또는 사용자 그룹을 직접 추가하려면 암호 보호를 활성화해야 합니다.

8. 애플리케이션 관리에 대한 접근을 부여할 사용자 또는 사용자 그룹을 선택합니다.

9. **권한** 목록에서 애플리케이션 기능에 대한 사용자 접근 권한을 구성합니다.

10. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Industrial CyberSecurity for Nodes 서비스를 관리하기 위한 사용자 접근 권한 구성

설치 시 Kaspersky Industrial CyberSecurity for Nodes는 Windows에 애플리케이션 서비스(*Kaspersky Industrial CyberSecurity for Nodes 서비스*)를 등록합니다. 따라서 애플리케이션에는 운영 체제를 시작할 때 시작하는 기능 구성 요소가 포함됩니다. 애플리케이션 서비스를 사용하여 보호 중인 장치의 보안 설정 및 애플리케이션 기능에 제삼자가 접근할 수 있는 위험을 줄이기 위해 Kaspersky Industrial CyberSecurity for Nodes 서비스 관리 권한을 제한할 수 있습니다.

기본적으로 보호 중인 장치의 관리자 그룹에 속한 사용자에게 Kaspersky Industrial CyberSecurity for Nodes 서비스 관리 권한이 부여됩니다. SERVICE 및 INTERACTIVE 그룹에 읽기 권한이 부여되고 SYSTEM 그룹에 읽기 및 실행 권한이 부여됩니다.

SYSTEM 사용자 계정을 삭제하거나 이 계정의 권한을 편집할 수 없습니다. SYSTEM 사용자 계정 권한이 편집된 경우, 변경 사항을 저장할 때 해당 계정에 대한 최대 권한이 복원됩니다.

'권한 편집' 레벨의 기능에 접근할 수 있는 사용자는 보호 중인 장치에 등록되어 있거나 도메인에 포함된 다른 사용자에게 Kaspersky Industrial CyberSecurity for Nodes 서비스 관리 접근 권한을 부여할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 사용자 또는 그룹에 대해 다음과 같은 사전 설정된 Kaspersky Industrial CyberSecurity for Nodes 서비스 관리 접근 권한 레벨 중 하나를 선택할 수 있습니다:

- **전체 제어**: Kaspersky Industrial CyberSecurity for Nodes 서비스의 일반 설정 및 사용자 권한을 보고 편집하고 Kaspersky Industrial CyberSecurity for Nodes 서비스를 시작하고 중지하는 기능.

- **읽기**: Kaspersky Industrial CyberSecurity for Nodes 서비스의 일반 설정 및 사용자 권한을 보는 기능.

- **편집**: Kaspersky Industrial CyberSecurity for Nodes 서비스의 일반 설정 및 사용자 권한을 보고 편집하는 기능.
- **실행**: Kaspersky Industrial CyberSecurity for Nodes 서비스를 시작하고 중지하는 기능.

특정 Kaspersky Industrial CyberSecurity for Nodes 기능에 대한 접근을 허용하거나 거부하며 고급 접근 권한을 구성할 수도 있습니다(아래 표 참조).

Kaspersky Industrial CyberSecurity for Nodes 서비스 기능에 대한 접근 권한

기능	설명
읽기 서비스 설정	Kaspersky Industrial CyberSecurity for Nodes 서비스의 일반 설정 및 사용자 권한을 보는 기능.
서비스 제어 관리자에서 서비스 상태 요청	Microsoft Windows Service Control Manager에서 Kaspersky Industrial CyberSecurity for Nodes 서비스의 실행 상태를 요청하는 기능.
서비스 상태 요청	Kaspersky Industrial CyberSecurity for Nodes 서비스에서 서비스 실행 상태를 요청하는 기능.
종속 서비스 목록 읽기	Kaspersky Industrial CyberSecurity for Nodes 서비스가 의존하는 서비스와 Kaspersky Industrial CyberSecurity for Nodes 서비스에 의존하는 서비스의 목록을 보는 기능.
서비스 설정 수정	Kaspersky Industrial CyberSecurity for Nodes 서비스의 일반 설정 및 사용자 권한을 보고 편집하는 기능.
서비스 시작	Kaspersky Industrial CyberSecurity for Nodes 서비스를 시작하는 기능.
서비스 중단	Kaspersky Industrial CyberSecurity for Nodes 서비스를 중지하는 기능.
서비스 일시 정지/재개	Kaspersky Industrial CyberSecurity for Nodes 서비스를 일시 중지하고 다시 시작하는 기능.
권한 읽기	Kaspersky Industrial CyberSecurity for Nodes 서비스 사용자 목록 및 각 사용자의 접근 권한을 보는 기능.
권한 편집	다음을 수행할 수 있습니다: • Kaspersky Industrial CyberSecurity for Nodes 서비스 사용자를 추가하거나 제거합니다. • Kaspersky Industrial CyberSecurity for Nodes 서비스에 대한 사용자 접근 권한을 편집합니다.
서비스 제거	Microsoft Windows Service Control Manager에서 Kaspersky Industrial CyberSecurity for Nodes 서비스를 등록 해제하는 기능.
서비스에 대한 사용자 정의 요청	사용자 요청을 생성하여 Kaspersky Industrial CyberSecurity for Nodes 서비스에 전송하는 기능.

Kaspersky Industrial CyberSecurity for Nodes 서비스를 관리할 수 있는 사용자 및 사용자 그룹의 목록과 해당 사용자 및 사용자 그룹의 접근 권한을 편집할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 서비스를 관리하기 위한 사용자 권한을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **보충** 옵션을 선택합니다.
4. **KICS for Nodes Service 관리를 위한 사용자 접근 권한** 섹션에서 **설정** 버튼을 클릭합니다.

   사용자 접근 권한 구성 양식이 열립니다.
5. Kaspersky Industrial CyberSecurity for Nodes 서비스 사용자 권한을 구성할 Active Directory 사용자 또는 그룹을 추가합니다.
6. 애플리케이션 관리에 대한 접근을 부여할 사용자 또는 사용자 그룹을 선택합니다.
7. 권한 목록에서 Kaspersky Industrial CyberSecurity for Nodes 서비스를 관리하기 위한 사용자 권한을 구성합니다.

8. 필요하다면 사용자에 대한 특수 권한을 구성합니다:

   a. **추가**를 클릭합니다.

   b. 열린 창에서 사용자 계정을 선택합니다.

   c. 더블 클릭하여 사용자 계정 속성을 엽니다.

   d. 열린 창에서 **추가 권한 표시** 링크를 클릭합니다.

   e. 열린 창에서 사용자에 대한 특수 권한을 구성합니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 서비스를 관리하기 위한 사용자 권한을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **KICS for Nodes Service 관리를 위한 사용자 접근 권한** 옵션을 선택합니다.

2. 창이 열리면 **권한** 블록에서 **추가** 버튼을 클릭합니다.
   사용자 접근 권한 구성 양식이 열립니다.

3. Kaspersky Industrial CyberSecurity for Nodes 서비스 사용자 권한을 구성할 Active Directory 사용자 또는 그룹을 추가합니다.

4. 애플리케이션 관리에 대한 접근을 부여할 사용자 또는 사용자 그룹을 선택합니다.

5. 권한 목록에서 Kaspersky Industrial CyberSecurity for Nodes 서비스를 관리하기 위한 사용자 권한을 구성합니다.

6. 필요하다면 사용자에 대한 특수 권한을 구성합니다:

   a. **추가**를 클릭합니다.

   b. 열린 창에서 사용자 계정을 선택합니다.

   c. 더블 클릭하여 사용자 계정 속성을 엽니다.

   d. 열린 창에서 **추가 권한 표시** 링크를 클릭합니다.

   e. 열린 창에서 사용자에 대한 특수 권한을 구성합니다.

7. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 서비스를 관리하기 위한 사용자 권한을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보충 → KICS for Nodes Service 관리를 위한 사용자 접근 권한** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   KICS for Nodes Service 관리를 위한 사용자 접근 권한 창이 열립니다.

5. Kaspersky Industrial CyberSecurity for Nodes 서비스 사용자 권한을 구성할 Active Directory 사용자 또는 그룹을 추가합니다.

6. 애플리케이션 관리에 대한 접근을 부여할 사용자 또는 사용자 그룹을 선택합니다.

   웹 콘솔에서는 애플리케이션 서비스를 관리하기 위해 특수 권한을 구성할 수 없습니다.

7. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Industrial CyberSecurity for Nodes 기능 접근을 암호로 보호

사용자 권한을 구성하여 사용자 권한 구성을 통한 애플리케이션 관리와 등록 서비스 접근을 제한할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes 설정에서 암호 보호를 설정하여 중요 작업에 대한 추가 보호를 설정할 수도 있습니다.

사용자가 암호로 보호된 동작을 수행하려고 하면 Kaspersky Industrial CyberSecurity for Nodes는 사용자 이름과 암호를 입력하거나 토큰을 사용하여 인증하라는 메시지를 표시합니다.

사용자 이름 및 암호

암호 보호는 다음 계정을 지원합니다:

- **KLAdmin**. Kaspersky Industrial CyberSecurity for Nodes에 대한 무제한 접근 권한을 가진 관리자 계정. KLAdmin 계정에는 암호로 보호된 작업을 수행할 수 있는 권한이 있습니다. KLAdmin 계정에 대한 권한은 철회할 수 없습니다. 암호 보호를 사용하도록 설정하면 KLAdmin 계정의 암호를 설정하라는 메시지를 Kaspersky Industrial CyberSecurity for Nodes가 표시합니다.
- **계정 직접 추가됨**. Active Directory 도메인 외의 계정. 관리자 암호를 공유하고 싶지 않은 경우 KLAdmin 대신 이 서비스 계정을 사용할 수 있습니다. 사용자 이름 및 암호를 설정하고 개별 권한을 구성할 수 있습니다.
- **Everyone 그룹**. 회사 네트워크 내의 모든 사용자를 포함하는 기본 제공 Windows 그룹. Everyone 그룹의 사용자는 자신에게 부여된 권한에 따라 애플리케이션에 접근할 수 있습니다.
- **개별 사용자 또는 그룹**. 개별 권한을 구성할 수 있는 사용자 계정. 예를 들어 Everyone 그룹에 대해 동작이 차단된 경우 개별 사용자 또는 그룹에 대해 이 작업을 허용할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 인터페이스는 화면 상에서 지정된 암호를 숨깁니다. Kaspersky Industrial CyberSecurity for Nodes는 암호를 입력했을 때 계산된 체크섬으로 암호를 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes는 암호 강도를 확인하지 않으며 여러 번 실패해도 암호 입력을 차단하지 않습니다.

암호 생성 시 다음 조건을 충족하는 것이 좋습니다:

- 암호는 계정 이름이나 컴퓨터 이름을 포함하지 않습니다.
- 암호는 8자 이상이어야 합니다.
- 암호가 다음 카테고리에서 3개 이상에 해당하는 문자를 포함합니다.
  - 라틴 대문자(A~Z)
  - 라틴 소문자(a~z)
  - 숫자(0~9)
  - 느낌표(!), 달러 기호($), 파운드 기호(#), 퍼센트 기호(%)

토큰

Kaspersky Industrial CyberSecurity for Nodes 기능을 사용하려면 연결된 토큰에 저장된 인증서 목록에서 적절한 사용자 인증서를 선택하고 PIN을 입력해야 합니다. 토큰 기반 인증은 Active Directory 도메인에 속한 사용자만 사용할 수 있습니다. 관리자는 개별 사용자 또는 그룹의 권한을 구성할 수 있습니다. 토큰 기반 인증을 사용하려면 신뢰할 수 있는 PKI 인프라를 배포하고 토큰 관리용 특수 소프트웨어를 설치해야 합니다.

Kaspersky Security Center 관리 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 기능 접근을 암호로 보호하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **보충** 옵션을 선택합니다.
4. **애플리케이션 관리를 위한 사용자 접근 권한** 섹션에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **수동으로 생성된 사용자의 자격 증명을 사용하여 애플리케이션의 작업 확인 허용** 확인란을 선택합니다.
6. 필요하다면 **중요 작업을 확인하기 위한 암호 요청** 확인란을 선택 해제합니다.

   이 기능이 활성화될 경우, 애플리케이션 삭제, 수정, 복구, 장치의 보호 레벨을 낮출 수 있는 명령줄 동작 수행 시 애플리케이션에서 사용자 이름 및 암호를 요청합니다.

   이 기능이 비활성화되고, 현재 사용자에게 필요 권한이 있을 경우 Kaspersky Industrial CyberSecurity for Nodes에서 자격 증명을 요청하지 않습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

   > 현재 사용자에게 Windows 암호가 공란으로 설정되어 있다면, 필수 권한이 있으며 공란이 아닌 암호를 설정한 사용자의 자격 증명을 입력해야 합니다.

7. KLAdmin 사용자 계정의 암호를 지정합니다.

8. 필요하다면 애플리케이션 관리 접근 권한을 부여할 사용자 계정을 추가합니다.

   a. **추가** 버튼을 클릭합니다.
   사용자 접근 권한 구성 양식이 열립니다.

   b. 창이 열리면 사용자 추가 방법(**사용자/사용자 그룹 직접 추가**)을 선택합니다.

   c. 사용자 이름과 암호를 지정합니다.

   d. **권한** 목록에서 애플리케이션 기능에 대한 사용자 접근 권한을 구성합니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 기능 접근을 암호로 보호하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **애플리케이션 관리를 위한 사용자 접근 권한** 옵션을 선택합니다.

2. 창이 열리면 **수동으로 생성된 사용자의 자격 증명을 사용하여 애플리케이션의 작업 확인 허용** 확인란을 선택합니다.

3. 필요하다면 **중요 작업을 확인하기 위한 암호 요청** 확인란을 선택 해제합니다.
   이 기능이 활성화될 경우, 애플리케이션 삭제, 수정, 복구, 장치의 보호 레벨을 낮출 수 있는 명령줄 동작 수행 시 애플리케이션에서 사용자 이름 및 암호를 요청합니다.
   이 기능이 비활성화되고, 현재 사용자에게 필요 권한이 있을 경우 Kaspersky Industrial CyberSecurity for Nodes에서 자격 증명을 요청하지 않습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

   > 현재 사용자에게 Windows 암호가 공란으로 설정되어 있다면, 필수 권한이 있으며 공란이 아닌 암호를 설정한 사용자의 자격 증명을 입력해야 합니다.

4. KLAdmin 사용자 계정의 암호를 지정합니다.

5. 필요하다면 애플리케이션 관리 접근 권한을 부여할 사용자 계정을 추가합니다.

   a. **추가** 버튼을 클릭합니다.
   사용자 접근 권한 구성 양식이 열립니다.

   b. 창이 열리면 사용자 추가 방법(**사용자/사용자 그룹 직접 추가**)을 선택합니다.

   c. 사용자 이름과 암호를 지정합니다.

   d. **권한** 목록에서 애플리케이션 기능에 대한 사용자 접근 권한을 구성합니다.

6. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 기능 접근을 암호로 보호하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보충 → 애플리케이션 관리를 위한 사용자 접근 권한** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. 창이 열리면 **수동으로 생성된 사용자의 자격 증명을 사용하여 애플리케이션의 작업 확인 허용** 확인란을 선택합니다.

6. 필요하다면 **중요 작업을 확인하기 위한 암호 요청** 확인란을 선택 해제합니다.

   이 기능이 활성화될 경우, 애플리케이션 삭제, 수정, 복구, 장치의 보호 레벨을 낮출 수 있는 명령줄 동작 수행 시 애플리케이션에서 사용자 이름 및 암호를 요청합니다.

   이 기능이 비활성화되고, 현재 사용자에게 필요 권한이 있을 경우 Kaspersky Industrial CyberSecurity for Nodes에서 자격 증명을 요청하지 않습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

   > 현재 사용자에게 Windows 암호가 공란으로 설정되어 있다면, 필수 권한이 있으며 공란이 아닌 암호를 설정한 사용자의 자격 증명을 입력해야 합니다.

7. KLAdmin 사용자 계정의 암호를 지정합니다.

8. 필요하다면 애플리케이션 관리 접근 권한을 부여할 사용자 계정을 추가합니다.

   a. **추가** 버튼을 클릭합니다.
      사용자 접근 권한 구성 양식이 열립니다.

   b. 창이 열리면 사용자 추가 방법(**사용자/사용자 그룹 직접 추가**)을 선택합니다.

   c. 사용자 이름과 암호를 지정합니다.

   d. **권한** 목록에서 애플리케이션 기능에 대한 사용자 접근 권한을 구성합니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

> 이 암호는 복구할 수 없습니다. 암호를 잊으면 애플리케이션 통제권을 완전히 상실하게 됩니다. 또한 보호 중인 장치에서 애플리케이션을 제거할 수 없게 됩니다.

암호는 언제든지 초기화할 수 있습니다. 그러려면 **수동으로 생성된 사용자의 자격 증명을 사용하여 애플리케이션의 작업 확인 허용** 확인란을 선택 해제하고 변경 사항을 저장합니다. 암호 보호가 중지되고 이전 암호 체크섬이 제거됩니다. 새 암호로 암호 생성 프로세스를 반복합니다.

Secure Desktop 알림

Kaspersky Industrial CyberSecurity for Nodes는 *보안 데스크톱*(Secure Desktop) 기능을 지원합니다. 이는 컴퓨터의 보안 레벨을 낮출 가능성이 있는 잠재적인 작업들을 확인하기 위한 기능입니다. 이 기능을 사용하면 다른 여러 프로세스에서 격리된 확인 대화 상자를 애플리케이션에 표시할 수 있습니다. 이 기능은 높은 권한을 사용하여 요청을 보호합니다. 이런 방식으로는 사용자만이 작업을 확인할 수 있으며 악성 코드는 확인할 수 없습니다.

Kaspersky Industrial CyberSecurity for Nodes는 다음 동작을 확인하기 위해 보안 데스크톱 알림을 표시합니다.

- 추적 활성화됨 / 비활성화됨
- 애플리케이션 설정 내보냄 / 가져옴
- 보호 일시 중지됨
- 애플리케이션 종료됨
- 활성 키 삭제됨
- Kaspersky Industrial CyberSecurity for Nodes 제거됨
- 장치 제어 비활성화됨
- 실시간 파일 보호 비활성화됨
- Kaspersky Security Center 정책 비활성화됨
- 리포트 열람됨
- 백업 저장소에서 파일이 복원됨
- Kaspersky Industrial CyberSecurity for Nodes 설정 수정됨
- 시작 이외의 방법으로 관리되는 애플리케이션 작업

Kaspersky Security Center 관리 콘솔에서 Secure Desktop 알림을 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **애플리케이션 설정** 섹션으로 갑니다.
4. **보안 및 신뢰성** 블록에서 **설정** 버튼을 클릭합니다.
5. 열린 창에서 **보안** 탭을 선택합니다.
6. **자기 보호** 블록에서 **Secure Desktop 알림 활성화** 확인란을 선택하거나 선택 해제하여, Secure Desktop 알림을 활성화하거나 비활성화합니다.

   자기 보호 메커니즘이 비활성화되면 **Secure Desktop 알림 활성화** 확인란을 사용할 수 없습니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.
8. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

관리 콘솔에서 Secure Desktop 알림을 활성화 또는 비활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고 결과 창에서 **애플리케이션 속성** 링크를 따라갑니다.
2. 열린 창에서 **보안 설정** 탭을 선택합니다.
3. **자기 보호** 블록에서 **Secure Desktop 알림 활성화** 확인란을 선택하거나 선택 해제하여, Secure Desktop 알림을 활성화하거나 비활성화합니다.

   > 자기 보호 메커니즘이 비활성화되면 **Secure Desktop 알림 활성화** 확인란을 사용할 수 없습니다.

4. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 Secure Desktop 알림을 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **애플리케이션 설정** 섹션을 선택합니다.
5. **보안 및 신뢰성** 블록에서 **구성** 버튼을 클릭합니다.
   보안 및 신뢰성 창이 열립니다.
6. **자기 보호** 블록에서 **Secure Desktop 알림 활성화** 확인란을 선택하거나 선택 해제하여, Secure Desktop 알림을 활성화하거나 비활성화합니다.

   > 자기 보호 메커니즘이 비활성화되면 **Secure Desktop 알림 활성화** 확인란을 사용할 수 없습니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다 .
8. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

신뢰 구역

*신뢰 구역*은 Kaspersky Industrial CyberSecurity for Nodes에서 감시하지 않는 개체 및 애플리케이션을 시스템 관리자가 구성한 목록입니다.

관리자는 처리되는 개체와 컴퓨터에 설치된 애플리케이션의 기능을 고려하여 독립적으로 신뢰 구역을 형성합니다. 사용자가 안전하다고 확신하는 개체 또는 애플리케이션인데도 Kaspersky Industrial CyberSecurity for Nodes가 해당 개체 또는 애플리케이션에 대한 접근을 차단하면 개체와 애플리케이션을 신뢰 구역에 포함하는 것이 좋습니다. 관리자는 사용자가 특정 컴퓨터에 대해 자신의 로컬 신뢰 구역을 만들도록 허용할 수도 있습니다. 이러한 방식으로 사용자는 정책의 일반 신뢰 구역 외에도 자신의 로컬 예외 규칙 및 신뢰하는 애플리케이션 목록을 생성할 수 있습니다.

EDR 원격 측정을 신뢰 구역에 추가할 수도 있습니다. 이를 통해 애플리케이션이 Kaspersky Anti Targeted Attack Platform(EDR) 솔루션용 원격 측정 서버로 전송하는 데이터를 최적화할 수 있습니다.

사전 정의된 검사 예외 및 신뢰하는 애플리케이션이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 신뢰 구역을 수동으로 생성하지 않고도 Kaspersky Industrial CyberSecurity for Nodes를 빠르게 구성할 수 있습니다.

검사 예외 생성

*검사 예외*는 Kaspersky Industrial CyberSecurity for Nodes에서 특정 개체의 바이러스 및 기타 위협을 검사하지 않도록 하려면 충족해야 하는 조건 집합입니다.

검사 예외는 다음 애플리케이션 구성 요소 및 작업에서 사용할 수 있습니다.

- **실시간 파일 보호**
- **온디맨드 검사**
- **Anti-Cryptor**
- **AMSI 스캐너**
- **네트워크 위협 보호**

검사 작업 중 하나를 시작할 때 개체가 들어 있는 드라이브 또는 폴더가 검사 범위에 포함된 경우 Kaspersky Industrial CyberSecurity for Nodes는 해당 개체를 검사하지 않습니다. 그러나 이 개체에 대한 사용자 지정 검사 작업이 시작된 경우 검사 예외는 적용되지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes는 5,000개 이상의 개체가 포함된 예외 목록을 지원하지 않습니다.

Kaspersky Security Center 관리 콘솔에서 검사 예외를 생성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **보충 → 신뢰 구역** 옵션을 선택하고 **설정** 버튼을 클릭합니다.

4. **검사 예외** 탭을 선택합니다.

5. 회사의 모든 컴퓨터에 대해 예외의 통합 목록을 만들려면 **상속할 때 값 병합** 확인란을 선택합니다. 부모 및 자식 정책의 예외 규칙 목록이 병합됩니다. 상속할 때 값 병합이 활성화된 경우 목록이 병합됩니다. 부모 정책의 예외 규칙은 자식 정책에 읽기 전용 보기로 표시됩니다. 부모 정책의 예외 규칙은 변경하거나 삭제할 수 없습니다.

6. 사용자가 예외의 로컬 목록을 만들 수 있도록 하려면 **로컬 예외 항목 사용 허용** 확인란을 선택합니다. 이러한 방식으로 사용자는 정책에서 생성된 일반 예외 규칙 목록 외에도 로컬 예외 규칙 목록을 만들 수 있습니다. 관리자는 Kaspersky Security Center를 사용하여 컴퓨터 속성의 목록 항목을 확인, 추가, 편집 또는 삭제할 수 있습니다.

   확인란을 선택 취소하면 사용자는 정책에서 생성된 일반 예외 규칙 목록에만 접근할 수 있습니다. 또한 이 확인란을 선택 해제하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 콘솔에서 검사 예외 통합 목록을 숨깁니다.

7. **추가** 버튼을 클릭하고 동작을 선택합니다:

   - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.

   - **새로운 예외**. Kaspersky Industrial CyberSecurity for Nodes가 새 검사 예외를 목록의 루트에 추가합니다.

   - **선택한 카테고리에 대한 새로운 제외 사항**. 특정 카테고리에 새 검사 예외를 추가하려면 카테고리를 선택합니다.

   - **목록에서 예외 항목 선택**. Kaspersky Industrial CyberSecurity for Nodes를 빠르게 구성하려면 사전 정의된 검사 예외 목록에서 예외를 추가할 수 있습니다.

8. 파일이나 폴더를 검사에서 제외시키려면 **파일 또는 폴더** 확인란을 선택합니다. **파일 또는 폴더 선택** 링크를 클릭해 창을 열고 해당 창에서 **찾아보기**를 클릭해 파일 및 폴더를 선택합니다.

   경로를 수동으로 입력할 수도 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:

   - `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.

   - `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.

   - `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

     파일 경로 시작 부분, 중간 또는 끝 부분에서 마스크를 사용할 수 있습니다. 예를 들어, 모든 사용자용 폴더를 예외 조건에 추가하려면 `?:\Users\*\Folder\` 마스크를 입력합니다.

9. 사전 정의된 영역을 검사에서 제외하려면 **사전 정의된 범위** 확인란을 선택합니다. **사전 정의된 범위 선택** 링크를 클릭해 창을 열고 해당 창에서 보호 중인 장치의 표준 범위 중 하나를 선택합니다.

10. 검사에서 특정 개체를 제외하려면 **탐지된 개체 유형** 확인란을 선택합니다. **개체 이름 입력** 링크를 클릭하고 **추가** 버튼을 클릭해 표시된 창에서 Kaspersky 백과사전 분류에 따라 개체 유형의 이름을 입력합니다(예, `Email-Worm`, `Rootkit`, `RemoteAdmin`).

    `?` 문자(단일 문자 대체) 및 `*` 문자(모든 문자 대체)와 함께 마스크를 사용할 수 있습니다. 예를 들어 `Client*` 마스크가 지정된 경우 Kaspersky Industrial CyberSecurity for Nodes는 `Client-IRC`, `Client-P2P` 및 `Client-SMTP` 개체를 검사에서 제외합니다.

11. 개별 파일을 검사에서 제외하려면 **개체 해시** 확인란을 선택합니다. **개체 해시 입력** 링크를 클릭해 창을 열고 해당 창에 파일 해시를 입력합니다.

    파일이 수정되면 파일 해시도 수정됩니다. 이 경우 수정된 파일이 예외 규칙에 추가되지 않습니다.

12. **규칙 사용 범위** 블록에서 검사 예외를 적용할 구성 요소를 선택합니다.

13. 필요하다면 **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

14. 변경 사항을 저장하여 목록에 예외를 추가합니다. 개체 옆의 확인란을 사용해 언제든 예외를 비활성화할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서 검사 예외를 생성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

    정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보충** → **신뢰 구역** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. **검사 예외** 탭을 선택합니다.

6. 회사의 모든 컴퓨터에 대해 예외의 통합 목록을 만들려면 **상속할 때 값 병합** 확인란을 선택합니다. 부모 및 자식 정책의 예외 규칙 목록이 병합됩니다. 상속할 때 값 병합이 활성화된 경우 목록이 병합됩니다. 부모 정책의 예외 규칙은 자식 정책에 읽기 전용 보기로 표시됩니다. 부모 정책의 예외 규칙은 변경하거나 삭제할 수 없습니다.

7. 사용자가 예외의 로컬 목록을 만들 수 있도록 하려면 **로컬 예외 항목 사용 허용** 확인란을 선택합니다. 이러한 방식으로 사용자는 정책에서 생성된 일반 예외 규칙 목록 외에도 로컬 예외 규칙 목록을 만들 수 있습니다. 관리자는 Kaspersky Security Center를 사용하여 컴퓨터 속성의 목록 항목을 확인, 추가, 편집 또는 삭제할 수 있습니다.

    확인란을 선택 취소하면 사용자는 정책에서 생성된 일반 예외 규칙 목록에만 접근할 수 있습니다. 또한 이 확인란을 선택 해제하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 콘솔에서 검사 예외 통합 목록을 숨깁니다.

8. **추가** 버튼을 클릭하고 동작을 선택합니다:

    - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.
    - **새로운 예외**. Kaspersky Industrial CyberSecurity for Nodes가 새 검사 예외를 목록의 루트에 추가합니다.
    - **목록에서 예외 항목 선택**. Kaspersky Industrial CyberSecurity for Nodes를 빠르게 구성하려면 사전 정의된 검사 예외 목록에서 예외를 추가할 수 있습니다.

9. 파일 또는 폴더를 검사에서 제외하려면 **파일 또는 폴더**를 선택하고 이름이 같은 필드의 확인란을 선택합니다. 파일 또는 폴더로의 경로 지정.

Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:

- `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.

- `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.

- `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

  파일 경로 시작 부분, 중간 또는 끝 부분에서 마스크를 사용할 수 있습니다. 예를 들어, 모든 사용자용 폴더를 예외 조건에 추가하려면 `?:\Users\*\Folder\` 마스크를 입력합니다.

10. 검사에서 사전 정의된 범위를 제외하려면 **사전 정의된 범위**를 선택합니다. 드롭다운 목록에서 보호 중인 장치의 표준 범위 중 하나를 선택합니다.

11. 특정 개체를 검사에서 제외하려면 **탐지된 개체 유형** 확인란을 선택하고 Kaspersky 백과사전 분류에 따른 개체 유형의 이름을 입력합니다(예: `Email-Worm`, `Rootkit`, 또는 `RemoteAdmin`).

    `?` 문자(단일 문자 대체) 및 `*` 문자(모든 문자 대체)와 함께 마스크를 사용할 수 있습니다. 예를 들어 `Client*` 마스크가 지정된 경우 Kaspersky Industrial CyberSecurity for Nodes는 *Client-IRC*, *Client-P2P* 및 *Client-SMTP* 개체를 검사에서 제외합니다.

12. 개별 파일을 검사에서 제외하려면 **개체 해시** 확인란을 선택하고 파일 또는 이벤트 목록의 해시를 추가합니다.

    파일이 수정되면 파일 해시도 수정됩니다. 이 경우 수정된 파일이 예외 규칙에 추가되지 않습니다.

13. 필요하다면 **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

14. **보호 구성 요소** 블록에서 검사 예외를 적용할 구성 요소를 선택합니다.

15. 새로운 예외가 목록에 추가됩니다. **상태** 열의 확인란을 사용해 언제든 예외를 비활성화할 수 있습니다.

16. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 검사 예외를 생성하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **신뢰 구역** 옵션을 선택합니다.

   신뢰 구역 설정 구성 창이 열립니다.

2. **예외 규칙** 섹션에서 **검사 예외** 블록 옆에 있는 **설정** 버튼을 클릭합니다.

3. **추가** 버튼을 클릭하고 동작을 선택합니다:

   - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.

   - **새로운 예외**. Kaspersky Industrial CyberSecurity for Nodes가 새 검사 예외를 목록의 루트에 추가합니다.

- **선택한 카테고리에 대한 새로운 제외 사항**. 특정 카테고리에 새 검사 예외를 추가하려면 카테고리를 선택합니다.

- **목록에서 예외 항목 선택**. Kaspersky Industrial CyberSecurity for Nodes를 빠르게 구성하려면 사전 정의된 검사 예외 목록에서 예외를 추가할 수 있습니다.

4. 파일이나 폴더를 검사에서 제외시키려면 **파일 또는 폴더** 확인란을 선택합니다. **파일 또는 폴더를 선택하십시오** 링크를 클릭해 창을 열고 해당 창에서 **찾아보기** 버튼을 클릭해 파일 및 폴더를 선택합니다.

   경로를 수동으로 입력할 수도 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:

   - `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.

   - `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.

   - `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

     파일 경로 시작 부분, 중간 또는 끝 부분에서 마스크를 사용할 수 있습니다. 예를 들어, 모든 사용자용 폴더를 예외 조건에 추가하려면 `?:\Users\*\Folder\` 마스크를 입력합니다.

5. 사전 정의된 영역을 검사에서 제외하려면 **사전 정의된 범위** 확인란을 선택합니다. **사전 정의된 범위 선택** 링크를 클릭해 창을 열고 해당 창에서 보호 중인 장치의 표준 범위 중 하나를 선택합니다.

6. 검사에서 특정 개체를 제외하려면 **탐지된 개체 유형** 확인란을 선택합니다. **개체 이름 입력** 링크를 클릭하고 **추가** 버튼을 클릭해 표시된 창에서 Kaspersky 백과사전 분류에 따라 개체 유형의 이름을 입력합니다(예, `Email-Worm`, `Rootkit`, `RemoteAdmin`).

   `?` 문자(단일 문자 대체) 및 `*` 문자(모든 문자 대체)와 함께 마스크를 사용할 수 있습니다. 예를 들어 `Client*` 마스크가 지정된 경우 Kaspersky Industrial CyberSecurity for Nodes는 `Client-IRC`, `Client-P2P` 및 `Client-SMTP` 개체를 검사에서 제외합니다.

7. 개별 파일을 검사에서 제외하려면 **개체 해시** 확인란을 선택합니다. **개체 해시 입력** 링크를 클릭해 창을 열고 해당 창에 파일 해시를 입력합니다.

   파일이 수정되면 파일 해시도 수정됩니다. 이 경우 수정된 파일이 예외 규칙에 추가되지 않습니다.

8. **규칙 사용 범위** 블록에서 검사 예외를 적용할 구성 요소를 선택합니다.

9. 필요하다면 **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

10. 변경 사항을 저장하여 목록에 예외를 추가합니다. 개체 옆의 확인란을 사용해 언제든 예외를 비활성화할 수 있습니다.

경로 마스크 예시:
모든 폴더에 있는 파일에 대한 경로:

- `*.exe` 마스크는 exe 확장자를 가진 파일의 모든 경로를 포함합니다.
- `example*` 마스크는 EXAMPLE 이름을 가진 파일에 대한 모든 경로를 포함합니다.

지정한 폴더에 있는 파일에 대한 경로:

- `C:\dir\*.*` 마스크는 C:\dir\ 폴더에 있는 파일에 대한 모든 경로를 포함하지만 C:\dir\의 하위 폴더는 포함하지 않습니다.
- `C:\dir\*` 마스크는 C:\dir\ 폴더 및 하위 폴더에 있는 파일에 대한 모든 경로를 포함합니다.
- `C:\dir\` 마스크는 C:\dir\ 폴더 및 하위 폴더에 있는 파일에 대한 모든 경로를 포함합니다.
- `C:\dir\*.exe` 마스크에는 C:\dir\ 폴더에 있지만 C:\dir\의 하위 폴더에는 없는 .EXE 확장자 파일의 모든 경로가 포함됩니다.
- `C:\dir\test` 마스크는 C:\dir\ 폴더에 있으며 "test" 이름을 가진 파일에 대한 모든 경로를 포함하지만 C:\dir\의 하위 폴더는 포함하지 않습니다.
- `C:\dir\*\test` 마스크는 C:\dir\ 폴더와 C:\dir\의 하위 폴더에 있으며 "test" 이름을 가진 파일에 대한 모든 경로를 포함합니다.
- 마스크 `C:\dir1\*\dir3\`는 dir3 하위 폴더에 있는 파일의 모든 경로를 한 수준 높은 C:\dir1\ 폴더에 포함시킵니다.
- 마스크 `C:\dir1\**\dirN\`은 dirN 하위 폴더에 있는 파일의 모든 경로를 수준과 상관없이 C:\dir1\ 폴더에 포함시킵니다.

지정한 이름을 가진 모든 폴더에 있는 파일에 대한 경로:

- `dir\*.*` 마스크는 "dir" 이름을 가진 폴더에 있는 파일에 대한 모든 경로를 포함하지만 그 하위 폴더는 포함하지 않습니다.
- `dir\*` 마스크는 "dir" 이름을 가진 폴더에 있는 파일에 대한 모든 경로를 포함하지만 그 하위 폴더는 포함하지 않습니다.
- `dir\` 마스크는 "dir" 이름을 가진 폴더에 있는 파일에 대한 모든 경로를 포함하지만 그 하위 폴더는 포함하지 않습니다.
- `dir\*.exe` 마스크에는 "dir"이라는 이름의 폴더에 있지만 해당 폴더의 하위 폴더에는 없는 .EXE 확장자 파일의 모든 경로가 포함됩니다.
- `dir\test` 마스크는 "dir" 이름을 가진 폴더에 있으며 "test" 이름을 가진 파일에 대한 모든 경로를 포함하지만 그 하위 폴더는 포함하지 않습니다.

탐지 가능한 개체의 유형 선택

탐지 가능한 개체의 유형을 선택하려면 다음과 같이 하십시오.

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 열고 다음 중 하나를 수행합니다:

   - 노드의 결과 창에서 **신뢰 구역 설정 구성** 링크를 클릭합니다.
   - 노드의 마우스 오른쪽 메뉴에서 **신뢰 구역** 항목을 선택합니다.

   신뢰 구역 설정 구성 창이 열립니다.

2. **탐지된 개체 유형** 섹션에서 **설정** 버튼을 클릭합니다.

3. 창이 열리면 Kaspersky Industrial CyberSecurity for Nodes거 탐지할 개체 유형 옆의 확인란을 선택합니다:

   - **바이러스 및 웜**

     하위 카테고리: 바이러스, 웜(Viruses_and_Worms)

     위험도: 높음

클래식 바이러스 및 웜은 사용자가 승인하지 않은 동작을 수행합니다. 자체 복제 기능이 있는 경우 스스로를 복사할 수 있습니다.

클래식 바이러스

클래식 바이러스가 컴퓨터에 침투하면 파일을 감염시킨 후 활성화되어 악성 작업을 수행하고, 자신의 사본을 다른 파일에 추가합니다.

클래식 바이러스는 컴퓨터의 로컬 리소스에만 전파되므로 다른 컴퓨터에 침투할 수는 없습니다. 이 바이러스는 공유 폴더 또는 삽입된 CD에 저장된 파일에 자신의 사본을 추가하거나 사용자가 감염된 파일을 첨부한 이메일 메시지를 전달하는 경우에만 다른 컴퓨터로 이동할 수 있습니다.

클래식 바이러스 코드는 컴퓨터, 운영 체제 및 애플리케이션의 다양한 영역에 침투할 수 있습니다. 환경에 따라 바이러스는 *파일 바이러스*, *부트 바이러스*, *스크립트 바이러스* 및 *매크로 바이러스*로 나뉩니다.

바이러스는 다양한 기술을 동원하여 파일을 감염시킬 수 있습니다. *덮어쓰기 바이러스*는 감염된 파일 코드 위에 자신의 코드를 써서 파일의 컨텐츠를 지웁니다. 감염된 파일은 기능이 중지되며 복원할 수 없습니다. *기생 바이러스*는 파일을 수정한 다음 그냥 두거나 부분적으로만 기능하도록 둡니다. *동반 바이러스*는 파일을 수정하지는 않지만 자신의 복제를 만듭니다. 감염된 파일을 열면 바이러스의 복제가 시작됩니다. 다음과 같은 바이러스 유형 또한 발생됩니다: *링크 바이러스*, *OBJ 바이러스*, *LIB 바이러스*, *소스 코드 바이러스*, 기타 등등.

웜

웜 코드 역시 클래식 바이러스와 마찬가지로 컴퓨터에 침투한 후 활성화되어 악성 작업을 수행합니다. 웜이라는 이름은 한 컴퓨터에서 다른 컴퓨터로 "크롤링"하며 사용자의 허가 없이 다양한 데이터 채널을 통해 사본을 유포하는 기능 때문에 붙여졌습니다.

다양한 웜 유형을 구분하게 하는 주요 기능은 웜의 유포 방식입니다. 다음 표에는 유포되는 방식에 따라 분류된 다양한 형태의 웜에 대한 개요 정보가 나와 있습니다.

웜이 유포되는 방식

유형	이름	설명
Email-Worm	Email-Worm	이 형태의 웜은 이메일을 통해 유포됩니다. 감염된 이메일 메시지에는 웜의 사본이 포함된 첨부파일이나 웹사이트로 업로드된 파일 링크가 포함되어 있으며, 후자의 경우 해당 웹사이트는 감염의 목적으로 해킹되었거나 만들어진 것일 수 있습니다. 첨부파일을 열면 웜이 활성화됩니다. 링크를 누르거나 파일을 다운로드해서 열 경우에도 웜이 악성 작업을 시작합니다. 그런 다음 웜은 자신의 사본 유포, 다른 이메일 주소 검색 및 감염된 메시지 전송을 진행합니다.
IM-Worm	IM 클라이언트 웜	이것은 IM 클라이언트를 통해 퍼집니다. 일반적으로 이러한 웜은 사용자의 연락처 목록을 사용하여 웹사이트에 있는 웜의 사본을 포함한 파일 링크를 메시지에 포함시켜 보냅니다. 사용자가 파일을 다운로드하여 열면 웜이 활성화됩니다.
IRC-Worm	인터넷 채팅 웜	이 형태의 웜은 인터넷상의 다른 사용자와 실시간으로 통신할 수 있는 서비스 시스템인 인터넷 릴레이 채팅을 통해 유포됩니다. 이러한 웜은 인터넷 채팅 시 자신의 사본이 포함된 파일 또는 파일에 대한 링크를 게시합니다. 사용자가 파일을 다운로드하여 열면 웜이 활성화됩니다.
Net-Worm	네트워크 웜	이러한 웜은 컴퓨터 네트워크를 통해 유포됩니다. 다른 형태의 웜과 달리 일반적인 네트워크 웜은 사용자의 관여 없이 유포됩니다. 이 형태의 웜은 취약한 프로그램이 포함되어 있는 컴퓨터의 로컬 네트워크를 검색합니다. 이를 위해 웜 코드나 웜 코드 일부를 포함하는 특별한 형태의 네트워크 패킷(익스플로잇)을 보냅니다. 네트워크에 "취약한" 컴퓨터가 있으면 이 네트워크 패킷이 전송됩니다. 웜은 컴퓨터에 완전히 침투한 후 활성화됩니다.
P2P-Worm	파일 공유 네트워크 웜	이 형태의 웜은 P2P 파일 공유 네트워크를 통해 유포됩니다. P2P 네트워크에 침투하기 위해 웜은 일반적으로 사용자의 컴퓨터에 있는 파일 공유 폴더로 자신을 복사합니다. 그러면 P2P 네트워크에 이 파일에 대한 정보가 표시되므로 P2P 사용자가 네트워크에서 다른 파일과 마찬가지로 감염된 파일을 "찾아" 다운로드하여 열 수 있습니다. 보다 정교한 웜은 특정 P2P 네트워크의 네트워크 프로토콜을 에뮬레이션합니다: 쿼리 검색에 긍정적인 응답을 반환하고 웜 파일의 복사본을 다운로드하도록 합니다.

유형	이름	설명
웜	기타 웜 형태	그 외 다음과 같은 형태의 웜이 있습니다: • 네트워크 리소스를 통해 자신의 사본을 유포하는 웜. 이 형태의 웜은 운영 체제의 기능을 사용하여 사용 가능한 네트워크 폴더를 검색하고, 인터넷상의 컴퓨터에 연결하며, 디스크 드라이브에 대한 모든 권한을 얻으려고 시도합니다. 이전에 설명한 형태의 웜과 달리 다른 형태의 웜은 자체적으로 활성화되지 않고 사용자가 웜 사본이 포함된 파일을 열 때 활성화됩니다. • 즉, 이러한 웜은 위의 표에 설명되어 있는 방법을 사용하지 않고 전파됩니다(예: 휴대폰을 통해 전파되는 웜).

- **트로이목마**

  하위 카테고리: 트로이목마

  위험도: 높음

  웜 및 바이러스와 달리 트로이목마는 자체적으로 복제되지 않습니다. 예를 들어, 트로이목마는 사용자가 감염된 웹 페이지를 방문할 때 이메일 또는 브라우저를 통해 컴퓨터에 침투합니다. 트로이목마는 사용자의 참여를 통해 시작됩니다. 시작되는 즉시 악성 작업을 수행합니다.

  트로이목마의 형태에 따라 감염된 컴퓨터에서 수행하는 작업도 달라집니다. 트로이목마는 주로 정보의 차단과 수정, 제거 및 컴퓨터 또는 네트워크 중지를 주 목적으로 하지만. 파일 송수신 및 실행, 화면 메시지 표시, 웹 페이지 요청, 프로그램 다운로드 및 설치, 컴퓨터 다시 시작 등의 작업도 할 수 있습니다.

  해커는 일반적으로 여러 트로이목마의 "세트"를 사용합니다.

  트로이목마의 동작 유형이 다음 표에 설명되어 있습니다.

  감염된 컴퓨터에서 트로이목마의 동작 유형

유형	이름	설명
Trojan-ArcBomb	트로이목마 - "압축 파일 폭탄"	압축을 해제했을 때 이러한 압축 파일은 컴퓨터 작업에 영향을 미칠 만큼 크기가 증가합니다. 사용자가 이 파일을 압축 해제하면 컴퓨터의 성능이 저하되거나 아예 실행 중지될 수 있으며, 하드 디스크는 "빈" 데이터로 가득 찰 수 있습니다. "압축 파일 폭탄"은 특히 파일 및 메일 서버에 위험합니다. 서버에서 자동 시스템을 사용하여 들어오는 정보를 처리할 경우 "압축 파일 폭탄"으로 인해 서버가 중지될 수 있습니다.
Backdoor	원격 관리를 위한 트로이목마	이 형태의 트로이목마는 모든 트로이목마 중에서도 가장 위험한 형태로 간주됩니다. 그 기능을 봤을 때 컴퓨터에 설치된 원격 관리 애플리케이션과 비슷합니다. 이러한 프로그램은 침입자가 컴퓨터를 원격으로 관리할 수 있도록 사용자 모르게 컴퓨터에 프로그램을 설치합니다.
Trojan	트로이목마	이 형태의 트로이목마에는 다음과 같은 악성 애플리케이션이 포함됩니다. • **클래식 트로이목마**. 이 프로그램은 트로이목마의 주 기능만 수행합니다: 주로 정보의 차단과 수정, 제거 및 컴퓨터 또는 네트워크 중지. 표에 설명된 다른 형태의 트로이목마와 달리 고급 기능은 포함하지 않습니다. • **다용도 트로이목마**. 이 형태의 트로이목마는 여러 트로이목마에서 일반적으로 보여지는 고급 기능을 갖추고 있습니다.
Trojan-Ransom	랜섬 트로이목마	이 형태의 트로이목마는 사용자의 정보를 "인질"로 취하여 해당 정보를 수정 또는 차단하거나 사용자가 정보를 사용할 수 없도록 컴퓨터의 작동에 영향을 줍니다. 침입자는 컴퓨터 성능 및 컴퓨터에 저장된 데이터를 복원하는 애플리케이션을 보내준다는 약속을 하며 사용자에게 대가를 요구합니다.
Trojan-Clicker	트로이목마 클리커	자체적으로 브라우저에 명령을 보내거나 운영 체제 파일에 지정된 웹 주소를 변경하여 사용자 컴퓨터에서 웹 페이지에 접근합니다. 이러한 프로그램을 사용하여 침입자는 네트워크 공격을 침투시키고 웹사이트 방문 수를 증가시켜 배너 광고의 표시 횟수를 높입니다.
Trojan-Downloader	트로이목마 다운로드	침입자의 웹 페이지에 접근하여 다른 악성 애플리케이션을 다운로드한 후 이를 사용자 컴퓨터에 설치합니다. 이 형태의 트로이목마는 다운로드할 악성 애플리케이션의 파일 이름을 포함하고 있거나 접근하는 웹 페이지에서 파일 이름을 수신할 수 있습니다.

유형	이름	설명
Trojan-Dropper	트로이목마 드로퍼	하드 드라이브에 복사한 후 설치하는 다른 트로이목마를 포함합니다. 침입자는 다음과 같은 목적을 위해 트로이목마 드로퍼형 프로그램을 사용할 수 있습니다: • 사용자가 알아채지 못하게 악성 애플리케이션을 설치합니다. Trojan-Dropper형 프로그램은 메시지를 표시하지 않거나 아니면 압축 파일에 오류가 있다거나 호환되지 않는 버전의 운영 체제라는 오류를 알리는 허위 메시지를 표시합니다. • 다른 알려진 악성 애플리케이션으로부터 보호하십시오. 일부 안티 바이러스 소프트웨어는 Trojan-Dropper형 애플리케이션 내의 악성 애플리케이션을 탐지하지 못합니다.
Trojan-Notifier	트로이목마 알림 기능	이 트로이목마는 감염된 컴퓨터가 접근 가능하다는 것을 침입자에게 알리고 컴퓨터에 대한 정보를 침입자에게 전송합니다: IP 주소, 열린 포트 번호, 이메일 주소. 이메일, FTP, 침입자의 웹 페이지 접근 등의 방법을 사용하여 침입자와 연결합니다. Trojan-Notifier형 프로그램은 보통 여러 개의 트로이목마로 구성되며. 침입자에게 다른 트로이목마가 사용자의 컴퓨터에 설치되었음을 알려줍니다.
Trojan-Proxy	트로이목마 프록시	이 형태의 트로이목마는 침입자가 사용자의 컴퓨터를 사용하여 웹 페이지에 익명으로 접근하도록 하며, 일반적으로 스팸 전달에 사용됩니다.
Trojan-PSW	Password-stealing-ware	Password-stealing-ware는 소프트웨어 등록 데이터 등의 사용자 계정을 훔치는 형태의 트로이목마입니다. 이 형태의 트로이목마는 시스템 파일의 기밀 데이터를 찾아서 이메일, FTP, 침입자의 웹 페이지 접근 또는 기타 방법으로 "공격자"에게 해당 정보를 전송합니다. 이러한 트로이목마 중 일부는 이 표에서 기술된 별도 유형으로 분류됩니다. 은행 계정을 도용하는 트로이목마(Trojan-Banker), IM 클라이언트의 사용자 정보를 도용하는 트로이목마(Trojan-IM) 및 온라인 게임 사용자 정보를 도용하는 트로이목마(Trojan-GameThief)가 여기에 해당됩니다.
Trojan-Spy	트로이목마 스파이	이 형태의 트로이목마는 사용자가 컴퓨터에서 수행한 작업에 대한 정보를 수집하여 사용자를 정탐합니다. 이 트로이목마는 사용자가 키보드로 입력한 데이터를 가로채거나 스크린샷을 찍거나 활성 애플리케이션의 목록을 수집할 수 있습니다. 정보를 수신한 후에는 이메일, FTP, 침입자의 웹 페이지 접근 또는 기타 방법으로 침입자에게 해당 정보를 전송합니다.
Trojan-DDoS	트로이목마 네트워크 공격자	사용자 컴퓨터에서 원격 서버로 대량의 요청을 전송합니다. 서버는 모든 요청을 처리할 리소스가 부족하여 작동을 멈추게 됩니다(서비스 거부 또는 DoS). 해커들은 다수의 컴퓨터를 사용하여 한 대의 서버를 동시에 공격할 수 있도록 이러한 프로그램을 많은 컴퓨터에 감염시킵니다. DoS 프로그램은 사용자에 대한 정보가 있는 단일 컴퓨터에서 공격을 가합니다. DDoS(분산된 서비스 거부 공격) 프로그램은 사용자 모르게 여러 컴퓨터에서 감염 컴퓨터에 분산 공격을 가합니다.
Trojan-IM	IM 클라이언트의 사용자 정보를 훔치는 트로이목마	이러한 트로이목마는 IM 클라이언트 사용자의 계정과 암호를 도용합니다. 이메일, FTP, 침입자의 웹 페이지 접근 또는 기타 방법으로 침입자에게 데이터를 전송합니다.
Rootkit	루트킷	이 형태의 트로이목마는 다른 악성 애플리케이션과 그 활동을 마스킹하여 운영 체제에서 해당 애플리케이션의 지속 기간을 연장시킵니다. 또한 이 형태의 트로이목마는 감염된 컴퓨터의 메모리에 악성 애플리케이션을 실행하는 파일, 프로세스 또는 레지스트리 키를 숨길 수 있습니다. 루트킷은 사용자 컴퓨터와 네트워크에 있는 다른 컴퓨터의 애플리케이션 간에 데이터 교환을 마스킹할 수 있습니다.
Trojan-SMS	SMS 메시지 형태의 트로이목마	이 형태의 트로이목마는 특별 요금 전화번호로 SMS 메시지를 전송하여 휴대폰을 감염시킵니다.
Trojan-GameThief	온라인 게임 사용자의 정보를 훔치는 트로이목마	이러한 트로이목마는 온라인 게임 사용자의 계정 정보를 도용해 이메일, FTP, 침입자의 웹 페이지 접근 또는 기타 방법으로 해당 데이터를 전송합니다.
Trojan-Banker	은행 계정을 훔치는 트로이목마	은행 계좌 데이터 또는 이머니(emoney) 시스템 데이터를 도용하고 이메일, FTP, 침입자의 웹 페이지 접근 또는 기타 방법으로 해당 데이터를 전송합니다.
Trojan-Mailfinder	이메일 주소를 수집하는 트로이목마	이 형태의 트로이목마는 컴퓨터에 저장된 이메일 주소를 수집하여 이메일, FTP, 침입자의 웹 페이지 접근 또는 기타 방법으로 침입자에게 해당 정보를 전송합니다. 이 경우 침입자가 수집한 주소로 스팸을 보낼 수 있습니다.

- **악성 도구**

  하위 카테고리: 악성 도구

  위험도: 중간

  다른 종류의 악성 코드와 달리 악성 도구는 활동을 시작하는 즉시 작업을 수행하지 않습니다. 악성 툴은 사용자의 컴퓨터에 안전하게 저장되어 있다가 시작될 수 있습니다. 침입자는 보통 이러한 프로그램의 기능을 사용하여 바이러스, 웜 및 트로이목마를 만들거나, 원격 서버에 대한 네트워크 공격을 가하거나, 컴퓨터를 해킹하거나, 기타 악성 작업을 수행합니다.

악성 도구의 다양한 기능은 다음 표에 설명된 형태에 따라 분류할 수 있습니다.

악성 도구의 기능

유형	이름	설명
Constructor	바이러스 제작	이 형태의 악성 툴은 새 바이러스, 웜 및 트로이목마를 만들 수 있습니다. 일부 바이러스 제작 유틸리티는 일반적인 창 기반의 인터페이스를 제공하는데, 이러한 인터페이스를 통해 사용자는 제작할 악성 애플리케이션의 형태, 디버거 대응 방법 및 기타 기능을 선택할 수 있습니다.
Dos	네트워크 공격	사용자 컴퓨터에서 원격 서버로 대량의 요청을 전송합니다. 서버는 모든 요청을 처리할 리소스가 부족하여 작동을 멈추게 됩니다(서비스 거부 또는 DoS).
Exploit	익스플로잇	*익스플로잇은* 데이터 또는 프로그램 코드의 집합이며, 해당 데이터 또는 코드가 처리되는 애플리케이션의 취약점을 활용하여 컴퓨터에 대한 악성 작업을 수행합니다. 예를 들어 익스플로잇은 파일을 쓰거나 읽을 수 있으며 "감염된" 웹 페이지를 요청할 수 있습니다. 서로 다른 익스플로잇은 각기 다른 애플리케이션 또는 네트워크 서비스의 취약점을 활용합니다. 네트워크 패킷으로 위장된 익스플로잇은 네트워크를 통해 수많은 컴퓨터로 전송되어 취약한 네트워크 서비스가 포함된 컴퓨터를 검색합니다. DOC 파일의 익스플로잇은 텍스트 편집기의 취약점을 활용합니다. 이 형태의 익스플로잇은 사용자가 감염된 파일을 열었을 때 해커가 사전 프로그래밍해 놓은 작업을 수행할 수 있습니다. 이메일 메시지에 삽입된 익스플로잇은 모든 이메일 클라이언트의 취약점을 검색합니다. 이 형태의 악성 툴은 사용자가 이 이메일 클라이언트에서 감염된 메시지를 여는 즉시 악성 작업을 수행할 수 있습니다. 익스플로잇을 사용하여 네트워크를 통해 유포되는 Net-Worm. Nuker 익스플로잇은 컴퓨터를 중지시키는 네트워크 패킷입니다.
FileCryptor	암호화 프로그램	이 형태의 악성 툴은 다른 악성 애플리케이션을 암호화하여 안티 바이러스 애플리케이션에서 탐지하지 못하도록 합니다.
Flooder	네트워크 "감염"용 프로그램	이 형태의 악성 툴은 네트워크 채널을 통해 수많은 메시지를 전송합니다. 이 형태의 툴에는 인터넷 릴레이 채팅을 오염시키는 프로그램이 포함될 수 있습니다. 그러나 이메일, 메신저 클라이언트, 모바일 통신 시스템에 사용되는 채널을 "감염"시키는 프로그램은 이 Flooder형 툴에 포함되지 않습니다. 이러한 프로그램은 본 표에 설명된 다른 형태(Email-Flooder, IM-Flooder 및 SMS-Flooder)와 구분됩니다.
HackTool	해킹 툴	이 형태의 악성 툴은 해당 툴이 설치된 컴퓨터를 해킹하거나 다른 컴퓨터를 공격할 수 있습니다(예: 사용자 허가 없이 새로운 시스템 계정 추가, 시스템 로그를 삭제하여 운영 체제에 해당 악성 툴의 존재를 숨김). 이 형태의 툴에는 암호 가로채기와 같은 악성 기능을 특징으로 하는 일부 Sniffer가 포함됩니다. Sniffer는 네트워크 트래픽을 볼 수 있는 프로그램입니다.
Hoax	혹스	혹스는 감염되지 않은 파일에서 "바이러스를 탐지"하고 사용자에게 디스크가 포맷되었다는 허위 사실을 알립니다.
Spoofer	스푸핑 툴	이 형태의 악성 툴은 가짜 발신자 주소를 사용하여 메시지와 네트워크 요청을 전송합니다. 예를 들어, 침입자는 Spoofer형 툴을 사용하여 실제 메시지 발신자인 것처럼 행세합니다.
VirTool	악성 애플리케이션을 수정하는 툴	다른 악성 코드의 수정을 허용하여 안티 바이러스 애플리케이션으로부터 바이러스의 존재를 숨깁니다.
Email-Flooder	이메일 주소를 "오염"시키는 프로그램	이 형태의 악성 툴은 다양한 이메일 주소로 수많은 메시지를 전송하여 해당 이메일 주소를 "오염"시킵니다. 대용량의 메시지가 들어오면 사용자는 자신의 받은 편지함에서 정작 유용한 메시지를 볼 수 없게 됩니다.
IM-Flooder	IM 클라이언트의 트래픽을 "오염"시키는 프로그램	메신저 클라이언트 사용자에게 다량의 메시지를 보냅니다. 대용량의 메시지가 수신되어 사용자는 정작 유용한 메시지를 볼 수 없게 됩니다.
SMS-Flooder	SMS 메시지로 트래픽을 "오염"시키는 프로그램	이 형태의 악성 툴은 휴대폰으로 수많은 SMS 메시지를 전송합니다.

- **애드웨어**

  하위 카테고리: 광고 소프트웨어(Adware)

  위험도: 중간

애드웨어는 사용자에게 광고 정보를 표시하는 프로그램입니다. 애드웨어 프로그램은 다른 프로그램의 인터페이스에 배너 광고를 표시하고, 검색 쿼리를 광고 웹 페이지로 리다이렉트합니다. 그들 중 일부는 사용자에 대한 마케팅 정보를 수집하고, 개발자에게 이를 보냅니다: 이 정보는 사용자 또는 사용자의 검색 쿼리의 컨텐츠에 의해 방문하는 웹사이트의 이름을 포함할 수 있습니다. Trojan-Spy형 프로그램과 달리 애드웨어 프로그램은 사용자의 허가를 받아 개발자에게 이러한 정보를 전송합니다.

- **자동 다이얼러**

  하위 카테고리: 자동 다이얼러(Dialer).

  위험도: 중간

  자동 다이얼러는 모뎀을 사용하여 은밀하게 전화 연결을 구성할 수 있습니다.

- **침입자에게 악용되어 사용자의 컴퓨터나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어**

  하위 카테고리: 침입자에게 악용되어 사용자의 컴퓨터나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어.

  위험도: 중간

  이러한 애플리케이션 중 대부분은 유용하며 많은 사용자가 해당 프로그램을 사용합니다. 이러한 애플리케이션에는 IRC 클라이언트, 자동 다이얼러, 파일 다운로드 프로그램, 컴퓨터 시스템 활동 모니터, 암호 유틸리티, FTP, HTTP 및 Telnet용 인터넷 서버가 포함됩니다.

  그러나 침입자가 이러한 프로그램에 대한 접근 권한을 얻게 되거나 침입자가 사용자 컴퓨터에 이러한 형태의 프로그램을 이식하면 애플리케이션 기능 중 일부가 보안을 위협하는 데 활용될 수 있습니다.

  이러한 애플리케이션은 기능이 서로 다르며 다음 표에 그 유형이 설명되어 있습니다.

유형	이름	설명
Client-IRC	인터넷 채팅 클라이언트	인터넷 릴레이 채팅에서 다른 사용자와 대화하기 위해 이러한 프로그램을 설치합니다. 침입자는 이러한 프로그램을 통해 악성 코드를 유포합니다.
Downloader	다운로드용 프로그램	이러한 프로그램은 숨겨진 모드로 웹 페이지에서 파일을 다운로드할 수 있습니다.
Monitor	모니터링용 프로그램	해당 프로그램이 설치된 컴퓨터의 활동(활성 애플리케이션 확인 및 다른 컴퓨터에 설치된 애플리케이션과 데이터를 교환하는 방법)을 모니터링할 수 있습니다.
PSWTool	암호 복원툴	잊어버린 암호를 확인하고 복원하는 툴입니다. 침입자는 사용자 모르게 컴퓨터에 이러한 프로그램을 설치하여 암호를 확인합니다.
RemoteAdmin	원격 관리 프로그램	시스템 관리자에 의해 광범위하게 사용되는 프로그램입니다. 이러한 프로그램은 원격 컴퓨터의 모니터링 및 관리를 위해 원격 컴퓨터의 인터페이스에 대한 접근 권한을 제공합니다. 침입자도 이와 같은 목적으로 사용자 장치에 은밀히 침투합니다: 원격 컴퓨터를 감시하고 관리하기 위한 목적. 합법적인 원격 관리 프로그램은 원격 관리를 위한 backdoor형 트로이목마와 다릅니다. 트로이목마는 운영 체제에 독립적으로 침투하여 자신을 설치할 수 있지만 정상적 애플리케이션을 그럴 수 없습니다.
Server-FTP	FTP 서버	이 형태의 프로그램은 FTP 서버 기능을 합니다. 침입자는 사용자의 컴퓨터에 이러한 형태의 프로그램을 이식하여 FTP를 통해 사용자 컴퓨터에 대한 원격 접속 권한을 얻습니다.
Server-Proxy	프록시 서버	이 형태의 프로그램은 프록시 서버 기능을 합니다. 침입자가 이 유형의 리스크웨어를 사용자 컴퓨터에 심어 사용자 이름으로 스팸을 전송합니다.
Server-Telnet	Telnet 서버	이 형태의 프로그램은 Telnet 기능을 합니다. 침입자는 사용자의 컴퓨터에 이러한 형태의 프로그램을 이식하여 Telnet을 통해 사용자 컴퓨터에 대한 원격 접속 권한을 얻습니다.
Server-Web	웹 서버	이 형태의 프로그램은 웹 서버 기능을 합니다. 침입자는 사용자의 컴퓨터에 이러한 형태의 프로그램을 이식하여 HTTP를 통해 사용자 컴퓨터에 대한 원격 접속 권한을 얻습니다.
RiskTool	로컬 컴퓨터에서의 작업에 사용되는 툴	이 형태의 프로그램은 사용자가 자신의 컴퓨터에서 작업할 때 추가 옵션을 제공합니다. 이 툴을 통해 사용자는 활성 애플리케이션의 파일 또는 창을 숨기고 활성 프로세스를 종료할 수 있습니다.

유형	이름	설명
NetTool	네트워크 툴	이 형태의 프로그램은 사용자가 네트워크상의 다른 컴퓨터에 대해 작업할 때 추가 옵션을 제공합니다. 이러한 툴을 통해 컴퓨터를 다시 시작하고, 열린 포트를 탐지하고, 컴퓨터에 설치되어 있는 애플리케이션을 시작할 수 있습니다.
Client-P2P	P2P 네트워크 클라이언트	이 형태의 프로그램을 통해 피어 투 피어 네트워크에 대한 작업을 할 수 있습니다. 침입자도 악성 코드 유포에 이러한 프로그램을 활용할 수 있습니다.
Client-SMTP	SMTP 클라이언트	사용자가 알지 못하도록 이메일 메시지를 전송합니다. 침입자가 이 유형의 리스크웨어를 사용자 컴퓨터에 심어 사용자 이름으로 스팸을 전송합니다.
WebToolbar	웹 툴바	이 형태의 프로그램은 다른 애플리케이션의 인터페이스에 검색 엔진을 사용하는 툴바를 추가합니다.
FraudTool	의사 프로그램	이 형태의 프로그램은 다른 프로그램 행세를 합니다. 예를 들어, 악성 코드 탐지에 관한 메시지를 표시하는 의사 안티 바이러스 프로그램이 있습니다. 그러나, 실제로는 바이러스를 찾거나 치료하지 못합니다.

- **악성 코드를 숨기려는 목적으로 이용될 수 있는 실행 압축 개체**

  하위 카테고리: 피해를 줄 수 있는 실행 압축 파일.

  위험도: 중간.

  파일이 바이러스, 웜, 트로이목마 등 악성 코드를 압축하는 데 사용되는 특수 압축 프로그램을 사용하여 압축되었습니다. Kaspersky Industrial CyberSecurity for Nodes는 SFX(자동 압축 해제) 압축 파일에 들어 있는 압축 해제 모듈을 검사합니다.

  해커는 안티 바이러스가 탐지하지 못하도록 악성 코드를 숨기기 위해 특수 압축 프로그램을 사용하여 악성 코드를 압축합니다. Kaspersky 전문가들은 해커들 사이에 가장 인기가 많은 압축 프로그램에 대한 정보를 확보하고 있습니다.

- **다중 실행 압축 개체**

  하위 카테고리: 다중 실행 압축 파일.

  위험도: 중간.

  파일이 하나 이상의 압축 프로그램으로 세 번 이상 압축되었습니다.

  해커는 안티 바이러스가 탐지하지 못하도록 악성 코드를 숨기기 위해 특수 압축 프로그램을 사용하여 파일을 여러 번 압축할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 압축된 파일을 검사합니다.

4. 변경 사항을 저장합니다.

신뢰하는 애플리케이션 목록 편집

*신뢰하는 애플리케이션 목록*은 Kaspersky Industrial CyberSecurity for Nodes에서 파일 및 네트워크 활동(악성 활동 포함)과 시스템 레지스트리 접근을 감시하지 않는 애플리케이션 목록입니다. 기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 다른 애플리케이션 프로세스에서 열려 있거나 실행하거나 저장하는 개체를 검사하고 모든 애플리케이션 활동과 이에 따라 생성되는 네트워크 트래픽을 모니터링합니다. 신뢰하는 애플리케이션 목록에 애플리케이션이 추가되면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 활동의 모니터링을 중단합니다.

검사 예외 및 신뢰하는 애플리케이션의 차이는, 검사 예외는 Kaspersky Industrial CyberSecurity for Nodes가 해당 파일을 검사하지 않으며 신뢰하는 애플리케이션에서는 시작한 프로세스를 제어하지 않습니다. 신뢰하는 애플리케이션이 검사 예외에 포함되어 있지 않은 폴더에서 악성 파일을 생성할 경우, Kaspersky Industrial CyberSecurity for Nodes는 파일을 감지하고 위험을 제거합니다. 폴더가 예외로 추가되면 Kaspersky Industrial CyberSecurity for Nodes는 이 파일을 건너뜁니다.

예를 들어, 사용자가 표준 Microsoft Windows 메모장 애플리케이션에서 사용하는 개체가 안전하므로 검사가 필요 없다고 생각하는 경우, 즉 이 애플리케이션을 신뢰하는 경우, Microsoft Windows 메모장을 신뢰하는 애플리케이션 목록에 추가하면 이 애플리케이션에서 사용하는 개체는 모니터링하지 않습니다. 이렇게 하면 컴퓨터 성능이 향상되는데, 이것은 서버 애플리케이션을 사용할 때 특히 중요합니다.

또한, Kaspersky Industrial CyberSecurity for Nodes가 의심스러운 것으로 분류한 특정 동작이 다수 애플리케이션의 기능 맥락 내에서는 안전할 수 있습니다. 예를 들어, 키보드에서 입력된 문자를 가로채는 것은 자동 키보드 레이아웃 스위처(예, Punto Switcher)에 있어서 일반적인 과정입니다. 이러한 애플리케이션의 특성을 고려하여 이들의 활동을 감시 대상에서 예외시키려면 해당 애플리케이션을 신뢰하는 애플리케이션 목록에 추가하는 것이 좋습니다.

신뢰하는 애플리케이션은 Kaspersky Industrial CyberSecurity for Nodes와 다른 애플리케이션 사이의 호환성 문제를 방지합니다. 예를 들어, Kaspersky Industrial CyberSecurity for Nodes와 다른 안티 바이러스 애플리케이션에서 제3자 컴퓨터가 네트워크 트래픽을 이중으로 검사하는 문제를 방지합니다.

이렇게 해도 실행 파일과 신뢰하는 애플리케이션 프로세스에 대해서는 계속 바이러스와 기타 악성 코드 검사가 수행됩니다. 검사 예외를 사용하여 애플리케이션을 Kaspersky Industrial CyberSecurity for Nodes 검사에서 완전히 예외시킬 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 5,000개 이상의 개체가 포함된 신뢰하는 애플리케이션 목록을 지원하지 않습니다.

Kaspersky Security Center 관리 콘솔의 신뢰하는 목록에 애플리케이션을 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보충**를 선택합니다.
4. **신뢰 구역** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **신뢰하는 애플리케이션** 탭을 선택합니다.
   신뢰하는 애플리케이션 목록이 포함된 창이 열립니다.
6. 보호 중인 장치에 설치된 백업 도구가 파일 읽기 작업을 수행할 경우 해당 작업의 검사를 건너뛰려면 **파일 백업 작업 확인 안 함** 확인란을 선택합니다.
7. 회사의 모든 컴퓨터에 대해 신뢰하는 애플리케이션의 통합 목록을 만들려면 **상속할 때 값 병합** 확인란을 선택합니다. 부모 및 자식 정책의 신뢰하는 애플리케이션 목록이 병합됩니다. 상속할 때 값 병합이 활성화된 경우 목록이 병합됩니다. 부모 정책의 신뢰하는 애플리케이션은 자식 정책에 읽기 전용 보기로 표시됩니다. 상위 정책의 신뢰하는 애플리케이션은 변경하거나 삭제할 수 없습니다

8. 사용자가 신뢰하는 애플리케이션의 로컬 목록을 만들 수 있도록 하려면 **신뢰하는 로컬 애플리케이션 편집 허용** 확인란을 선택합니다. 이러한 방식으로 사용자는 정책에서 생성된 신뢰할 수 있는 애플리케이션의 일반 목록 외에도 신뢰하는 애플리케이션의 로컬 목록을 만들 수 있습니다. 관리자는 Kaspersky Security Center를 사용하여 컴퓨터 속성의 목록 항목을 확인, 추가, 편집 또는 삭제할 수 있습니다.

   확인란을 선택 취소하면 사용자는 정책에서 생성된 신뢰하는 애플리케이션의 일반 목록에만 접근할 수 있습니다. 또한 이 확인란을 선택 해제하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 콘솔에서 신뢰하는 애플리케이션의 통합 목록을 숨깁니다.

9. 신뢰하는 프로세스에 대한 파일 동작 검사를 건너뛰려면 **지정 프로세스의 파일 활동 확인 안 함** 확인란을 선택합니다.

10. **추가** 버튼을 클릭하고 동작을 선택합니다:

    - **카테고리**. 신뢰하는 애플리케이션을 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 만들려면 카테고리 이름을 입력하고 해당 카테고리에 신뢰하는 애플리케이션을 하나 이상 추가합니다.
    - **새로운 예외**. Kaspersky Industrial CyberSecurity for Nodes가 신뢰하는 새로운 애플리케이션을 목록의 루트에 추가합니다.
    - **선택한 카테고리에 대한 새로운 제외 사항**. 신뢰하는 새로운 애플리케이션을 특정 카테고리에 추가하려면 카테고리를 선택합니다.
    - **목록에서 예외 항목 선택**. Kaspersky Industrial CyberSecurity for Nodes를 빠르게 구성하려면 사전 정의된 신뢰하는 애플리케이션 목록에서 애플리케이션을 추가할 수 있습니다.

11. 창이 열리면 **디스크의 전체 프로세스 경로를 사용하여 신뢰할 수 있는 것으로 간주** 확인란을 선택하고 파일 경로를 입력하여 프로세스를 신뢰하는지 여부를 결정합니다.

    Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:

    > Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Center 콘솔에서 신뢰하는 애플리케이션 목록을 생성할 때 `%userprofile%` 환경 변수를 지원하지 않습니다. 항목을 모든 사용자 계정에 적용하려면 * 문자를 사용할 수 있습니다(예: `C:\Users\*\Documents\File.exe`). 환경 변수를 새로 추가할 때마다 애플리케이션을 다시 시작해야 합니다.

12. 신뢰하는 애플리케이션에 대한 고급 설정을 구성합니다(아래 표 참조).

13. **확인** 버튼을 클릭합니다.

    신뢰하는 새로운 애플리케이션이 목록에 추가됩니다. 개체 옆의 확인란을 사용하여 언제든지 신뢰 구역에서 애플리케이션을 제외할 수 있습니다.

14. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔의 신뢰하는 목록에 애플리케이션을 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

4. **애플리케이션 설정** 탭을 선택합니다.

5. **보충 → 신뢰 구역** 섹션으로 가서 **구성** 버튼을 클릭합니다.

6. 창이 열리면 **신뢰하는 애플리케이션** 탭을 선택합니다.

7. 보호 중인 장치에 설치된 백업 도구가 파일 읽기 작업을 수행할 경우 해당 작업의 검사를 건너뛰려면 **파일 백업 작업 확인 안 함** 확인란을 선택합니다.

8. 회사의 모든 컴퓨터에 대해 신뢰하는 애플리케이션의 통합 목록을 만들려면 **상속할 때 값 병합** 확인란을 선택합니다. 부모 및 자식 정책의 신뢰하는 애플리케이션 목록이 병합됩니다. 상속할 때 값 병합이 활성화된 경우 목록이 병합됩니다. 부모 정책의 신뢰하는 애플리케이션은 자식 정책에 읽기 전용 보기로 표시됩니다. 상위 정책의 신뢰하는 애플리케이션은 변경하거나 삭제할 수 없습니다

9. 사용자가 신뢰하는 애플리케이션의 로컬 목록을 만들 수 있도록 하려면 **신뢰하는 로컬 애플리케이션 편집 허용** 확인란을 선택합니다. 이러한 방식으로 사용자는 정책에서 생성된 신뢰할 수 있는 애플리케이션의 일반 목록 외에도 신뢰하는 애플리케이션의 로컬 목록을 만들 수 있습니다. 관리자는 Kaspersky Security Center를 사용하여 컴퓨터 속성의 목록 항목을 확인, 추가, 편집 또는 삭제할 수 있습니다.

   확인란을 선택 취소하면 사용자는 정책에서 생성된 신뢰하는 애플리케이션의 일반 목록에만 접근할 수 있습니다. 또한 이 확인란을 선택 해제하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 콘솔에서 신뢰하는 애플리케이션의 통합 목록을 숨깁니다.

10. 신뢰하는 프로세스에 대한 파일 동작 검사를 건너뛰려면 **지정 프로세스의 파일 활동 확인 안 함** 확인란을 선택합니다.

11. **추가** 버튼을 클릭하고 동작을 선택합니다:

    - **카테고리**. 신뢰하는 애플리케이션을 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 만들려면 카테고리 이름을 입력하고 해당 카테고리에 신뢰하는 애플리케이션을 하나 이상 추가합니다.
    - **새로운 예외**. Kaspersky Industrial CyberSecurity for Nodes가 신뢰하는 새로운 애플리케이션을 목록의 루트에 추가합니다.
    - **선택한 카테고리에 대한 새로운 제외 사항**. 신뢰하는 새로운 애플리케이션을 특정 카테고리에 추가하려면 카테고리를 선택합니다.
    - **목록에서 예외 항목 선택**. Kaspersky Industrial CyberSecurity for Nodes를 빠르게 구성하려면 사전 정의된 신뢰하는 애플리케이션 목록에서 애플리케이션을 추가할 수 있습니다.

12. 창이 열리면 **디스크의 전체 프로세스 경로를 사용하여 신뢰할 수 있는 것으로 간주** 확인란을 선택하고 파일 경로를 입력하여 프로세스를 신뢰하는지 여부를 결정합니다.

    Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:

    > Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Center 콘솔에서 신뢰하는 애플리케이션 목록을 생성할 때 `%userprofile%` 환경 변수를 지원하지 않습니다. 항목을 모든 사용자 계정에 적용하려면 * 문자를 사용할 수 있습니다(예: `C:\Users\*\Documents\File.exe`). 환경 변수를 새로 추가할 때마다 애플리케이션을 다시 시작해야 합니다.

13. 신뢰하는 애플리케이션에 대한 고급 설정을 구성합니다(아래 표 참조).

14. **정상** 버튼을 클릭합니다.

    신뢰하는 새로운 애플리케이션이 목록에 추가됩니다. **처리** 열의 확인란을 사용하여 언제든지 신뢰 구역에서 애플리케이션을 제외할 수 있습니다.

15. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 신뢰하는 목록에 애플리케이션을 추가하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **신뢰 구역** 옵션을 선택합니다.

   신뢰 구역 설정 구성 창이 열립니다.

2. **예외 규칙** 섹션에서 **신뢰하는 애플리케이션** 블록 옆에 있는 **설정** 버튼을 클릭합니다.

3. **추가** 버튼을 클릭하고 동작을 선택합니다:

   - **카테고리**. 신뢰하는 애플리케이션을 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 만들려면 카테고리 이름을 입력하고 해당 카테고리에 신뢰하는 애플리케이션을 하나 이상 추가합니다.
   - **새로운 예외**. Kaspersky Industrial CyberSecurity for Nodes가 신뢰하는 새로운 애플리케이션을 목록의 루트에 추가합니다.
   - **선택한 카테고리에 대한 새로운 제외 사항**. 신뢰하는 새로운 애플리케이션을 특정 카테고리에 추가하려면 카테고리를 선택합니다.
   - **목록에서 예외 항목 선택**. Kaspersky Industrial CyberSecurity for Nodes를 빠르게 구성하려면 사전 정의된 신뢰하는 애플리케이션 목록에서 애플리케이션을 추가할 수 있습니다.

4. 목록에서 파일을 선택하거나 신뢰하는 애플리케이션의 실행 파일 경로를 입력합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:

   > Kaspersky Industrial CyberSecurity for Nodes는 환경 변수를 지원합니다. 동시에 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션의 로컬 인터페이스에서 경로를 변환합니다. 즉, `%userprofile%\Documents\File.exe` 경로를 입력하면, Fred123 사용자의 애플리케이션 로컬 인터페이스에 `C:\Users\Fred123\Documents\File.exe` 기록이 추가됩니다. 따라서 Kaspersky Industrial CyberSecurity for Nodes는 다른 사용자에 대해 신뢰하는 프로그램 `File.exe`를 무시합니다. 항목을 모든 사용자 계정에 적용하려면 `*` 문자를 사용할 수 있습니다(예: `C:\Users\*\Documents\File.exe`).

   > 환경 변수를 새로 추가할 때마다 애플리케이션을 다시 시작해야 합니다.

5. 신뢰하는 애플리케이션에 대한 고급 설정을 구성합니다(아래 표 참조).

6. **확인** 버튼을 클릭합니다.

   신뢰하는 새로운 애플리케이션이 목록에 추가됩니다. 개체 이름 옆의 확인란을 사용하여 언제든지 신뢰 구역에서 애플리케이션을 제외할 수 있습니다.

7. 변경 사항을 저장합니다.

신뢰하는 애플리케이션 설정

파라미터	설명
디스크의 전체 프로세스 경로를 사용하여 신뢰할 수 있는 것으로 간주	Kaspersky Industrial CyberSecurity for Nodes는 파일의 전체 경로를 사용하여 프로세스가 신뢰할 수 있는지 여부를 결정합니다.
프로세스 파일 해시를 사용하여 신뢰할 수 있는 것으로 간주	Kaspersky Industrial CyberSecurity for Nodes는 선택한 파일의 해시를 사용하여 프로세스의 신뢰 상태를 결정합니다. 확인란을 선택 해제하면 파일의 해시는 프로세스의 신뢰 상태를 결정하는 데 사용되지 않습니다.

파라미터	설명
규칙 사용	신뢰하는 애플리케이션의 활동을 감시하지 않을 Kaspersky Industrial CyberSecurity for Nodes 구성 요소 목록을 구성할 수 있습니다. • **실시간 파일 보호**. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 애플리케이션을 사용하여 연 모든 파일을 검사에서 제외합니다. 이 옵션은 기본적으로 활성화되어 있습니다. • **레지스트리 접근 모니터링**. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 애플리케이션이 변경한 시스템 무결성 모니터링 구성 요소의 모니터링 범위 내 레지스트리 키를 감시하지 않습니다. 이 기능은 기본적으로 비활성화됩니다. • **행동 탐지 및 익스플로잇 방지**. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 Anti-Cryptor 및 익스플로잇 방지 구성 요소를 사용하여 운영 체제에서 신뢰하는 애플리케이션의 파일 및 네트워크 활동을 감시하지 않습니다. 이 기능은 기본적으로 비활성화됩니다. • **AMSI 스캐너 구성 요소와의 상호작용**. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 애플리케이션에서 AMSI 스캐너 구성 요소로 전송되는 요청을 감시하지 않습니다. 이 기능은 기본적으로 비활성화됩니다. • **파일 무결성 모니터**. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 애플리케이션이 변경한 시스템 무결성 모니터링 구성 요소의 모니터링 범위 내 파일을 감시하지 않습니다. 이 기능은 기본적으로 비활성화됩니다. • **Endpoint Agent 원격 측정**. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 애플리케이션의 활동에 관한 원격 측정 데이터를 전송하지 않습니다. 이 기능은 기본적으로 비활성화됩니다. 이 기능을 비활성화하면 **Endpoint Agent 원격 측정을 위한 콘솔 대화형 입력 가로채기** 체크박스를 선택하여 콘솔을 통한 신뢰하는 애플리케이션 관리에 관한 원격 측정 데이터 전송을 별도로 구성할 수 있습니다. • **애플리케이션 실행 제어**. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 구성 요소를 통한 신뢰하는 애플리케이션의 실행을 감시하지 않습니다. 이 기능은 기본적으로 비활성화됩니다. 사전 정의된 신뢰하는 애플리케이션의 경우 **애플리케이션 실행 제어** 기능을 제외한 모든 기능이 기본적으로 활성화됩니다. Sigma 규칙을 사용한 이상 행위 탐지 구성 요소가 설치되어 있으면 **Endpoint Agent 원격 측정** 기능도 기본적으로 비활성화됩니다.
애플리케이션 인터페이스와의 상호작용 허용	Kaspersky Industrial CyberSecurity for Nodes는 원격 컴퓨터에서 애플리케이션 서비스를 관리하려는 모든 시도를 차단합니다. 이 확인란을 선택하면 원격 접속 애플리케이션이 Kaspersky Industrial CyberSecurity for Nodes 인터페이스를 통해 Kaspersky Industrial CyberSecurity for Nodes 설정을 관리할 수 있습니다.
자식 애플리케이션의 활동 감시 안 함	Kaspersky Industrial CyberSecurity for Nodes는 이 애플리케이션이 시작한 애플리케이션의 파일 활동 또는 네트워크 활동을 모니터링하지 않습니다. 예외를 반복 적용할 수 있습니다. 이 경우 애플리케이션은 전체 자식 애플리케이션 체인의 활동을 감시하지 않습니다.
부모 프로세스(애플리케이션)의 제한을 상속하지 않음	Kaspersky Industrial CyberSecurity for Nodes는 상위 프로세스에 대해 구성된 제한을 하위 프로세스에 적용하지 않습니다. 상위 프로세스는 애플리케이션 권한 및 애플리케이션 네트워크 규칙이 구성된 애플리케이션에 의해 시작됩니다.
프로세스 메모리를 검사하지 않음	Kaspersky Industrial CyberSecurity for Nodes는 프로세스 메모리를 검사하지 않습니다.

로컬 신뢰 구역 생성

이제 사용자는 특정 컴퓨터에 대해 자신만의 로컬 신뢰 구역을 생성할 수 있습니다. 이러한 방식으로 사용자는 정책의 일반 신뢰 구역 외에도 자신의 로컬 검사 예외 및 신뢰하는 애플리케이션 목록을 생성할 수 있습니다. 관리자는 정책 설정에서 로컬 예외 항목 또는 신뢰하는 로컬 애플리케이션 사용을 허용하거나 차단할 수 있습니다. 이를 위해서는 정책의 **신뢰 구역** 섹션에 있는 **검사 예외** 및 **신뢰하는 애플리케이션** 탭에서 **로컬 예외 항목 사용 허용** 및 **신뢰하는 로컬 애플리케이션 편집 허용** 확인란을 사용합니다.

관리자가 로컬 신뢰 구역 생성을 허용한 경우 사용자는 애플리케이션 콘솔에서 자신의 검사 예외와 신뢰하는 애플리케이션을 추가할 수 있습니다. 반면, 사용자에게는 정책에 구성된 신뢰 구역에서 개체를 수정하거나 삭제할 수 있는 권한이 없습니다. 또한 개별 컴퓨터에 대해 예외 항목을 추가해야 하는 경우 관리자는 Kaspersky Security Center 콘솔에서 목록 항목을 확인하고 추가, 수정 또는 삭제할 수도 있습니다.

관리자가 콘솔에서 신뢰 구역의 구성을 차단하고('닫힌 자물쇠' 기호) 로컬 검사 예외 및 신뢰하는 애플리케이션이 금지된 경우, Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 콘솔에서 검사 예외 및 신뢰하는 애플리케이션의 목록을 숨깁니다.

Kaspersky Security Center 관리 콘솔의 로컬 신뢰 구역에 애플리케이션을 추가하는 방법

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
2. 작업 공간에서 **기기** 탭을 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.
5. 컴퓨터에 설치된 Kaspersky 애플리케이션 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택하고 더블 클릭하여 애플리케이션 속성을 엽니다.
6. 애플리케이션 설정 창에서 **보충 → 신뢰 구역**을 선택하고 **설정** 버튼을 클릭합니다.
7. **검사 예외** 탭에서 로컬 검사 예외 목록을 만듭니다.

   로컬 검사 예외 항목 생성 규칙은 일반 예외 항목 생성 규칙과 동일합니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:
8. **신뢰하는 애플리케이션** 탭에서 신뢰하는 로컬 애플리케이션 목록을 만듭니다. 신뢰하는 로컬 애플리케이션 목록을 포함한 창이 열립니다.

   신뢰하는 로컬 애플리케이션 목록에 애플리케이션을 추가하는 규칙은 일반 목록에 애플리케이션을 추가하는 규칙과 동일합니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:
9. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔의 로컬 신뢰 구역에 개체를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.
2. 사용자가 차단된 동작을 수행하도록 허용할 컴퓨터 이름을 클릭합니다.
3. **애플리케이션** 탭을 선택합니다.
4. **Kaspersky Industrial CyberSecurity for Nodes**를 클릭합니다.

   그러면 로컬 애플리케이션 설정이 열립니다.
5. **애플리케이션 설정** 탭을 선택합니다.
6. 애플리케이션 설정 창에서 **보충 → 신뢰 구역**을 선택하고 **구성** 버튼을 클릭합니다.

   예외 규칙 및 탐지된 개체의 유형 창이 열립니다.
7. **검사 예외** 탭에서 로컬 검사 예외 목록을 만듭니다.

   로컬 예외 항목 생성 규칙은 일반 예외 항목 생성 규칙과 같습니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:
8. **신뢰하는 애플리케이션** 탭에서 신뢰하는 로컬 애플리케이션 목록을 만듭니다.

   신뢰하는 로컬 애플리케이션 목록에 애플리케이션을 추가하는 규칙은 일반 목록에 애플리케이션을 추가하는 규칙과 동일합니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:
9. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 로컬 검사 예외를 생성하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **신뢰 구역** 옵션을 선택합니다.

   신뢰 구역 설정 구성 창이 열립니다.

2. **검사 예외 및 신뢰하는 애플리케이션** 섹션에서 **로컬 검사 예외 항목** 블록 옆에 있는 **설정** 버튼을 클릭합니다.

   > 관리자가 Kaspersky Security Center 관리 콘솔에서 검사 예외 구성을 차단하고('닫힌 자물쇠' 기호) 로컬 검사 예외가 금지된 경우(**로컬 예외 항목 사용 허용** 확인란이 선택 해제됨) Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 콘솔에서 검사 예외 목록을 숨깁니다.

3. **추가** 버튼을 클릭하고 동작을 선택합니다:

   - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.
   - **새로운 예외**. Kaspersky Industrial CyberSecurity for Nodes가 새 검사 예외를 목록의 루트에 추가합니다.
   - **선택한 카테고리에 대한 새로운 제외 사항**. 특정 카테고리에 새 검사 예외를 추가하려면 카테고리를 선택합니다.
   - **목록에서 예외 항목 선택**. Kaspersky Industrial CyberSecurity for Nodes를 빠르게 구성하려면 사전 정의된 검사 예외 목록에서 예외를 추가할 수 있습니다.

4. **새로운 예외** 옵션을 선택하면 **검사 예외** 창이 열립니다.

5. 파일이나 폴더를 검사에서 제외시키려면 **파일 또는 폴더** 확인란을 선택합니다. **파일 또는 폴더를 선택하십시오** 링크를 클릭해 창을 열고 해당 창에서 **찾아보기** 버튼을 클릭해 파일 및 폴더를 선택합니다.

   경로를 수동으로 입력할 수도 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:

   - `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.
   - `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.
   - `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

     파일 경로 시작 부분, 중간 또는 끝 부분에서 마스크를 사용할 수 있습니다. 예를 들어, 모든 사용자용 폴더를 예외 조건에 추가하려면 `?:\Users\*\Folder\` 마스크를 입력합니다.

6. 사전 정의된 영역을 검사에서 제외하려면 **사전 정의된 범위** 확인란을 선택합니다. **사전 정의된 범위 선택** 링크를 클릭해 창을 열고 해당 창에서 보호 중인 장치의 표준 범위 중 하나를 선택합니다.

7. 검사에서 특정 개체를 제외하려면 **탐지된 개체 유형** 확인란을 선택합니다. **개체 이름 입력** 링크를 클릭하고 **추가** 버튼을 클릭해 표시된 창에서 Kaspersky 백과사전 분류에 따라 개체 유형의 이름을 입력합니다(예, `Email-Worm`, `Rootkit`, `RemoteAdmin`).

   `?` 문자(단일 문자 대체) 및 `*` 문자(모든 문자 대체)와 함께 마스크를 사용할 수 있습니다. 예를 들어 `Client*` 마스크가 지정된 경우 Kaspersky Industrial CyberSecurity for Nodes는 `Client-IRC`, `Client-P2P` 및 `Client-SMTP` 개체를 검사에서 제외합니다.

8. 개별 파일을 검사에서 제외하려면 **개체 해시** 확인란을 선택합니다. **개체 해시 입력** 링크를 클릭해 창을 열고 해당 창에 파일 해시를 입력합니다.

   파일이 수정되면 파일 해시도 수정됩니다. 이 경우 수정된 파일이 예외 규칙에 추가되지 않습니다.

9. **규칙 사용 범위** 블록에서 검사 예외를 적용할 구성 요소를 선택합니다.

10. 필요하다면 **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

11. 변경 사항을 저장하여 목록에 예외를 추가합니다. 개체 옆의 확인란을 사용해 언제든 예외를 비활성화할 수 있습니다.

애플리케이션 콘솔에서 신뢰하는 로컬 애플리케이션 목록에 애플리케이션을 추가하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **신뢰 구역** 옵션을 선택합니다.

   신뢰 구역 설정 구성 창이 열립니다.

2. **예외 규칙** 섹션에서 **신뢰하는 로컬 애플리케이션** 블록 옆에 있는 **설정** 버튼을 클릭합니다.

   > Kaspersky Security Center 관리 콘솔에서 관리자가 신뢰하는 애플리케이션 구성을 차단하고('닫힌 자물쇠' 기호) 신뢰하는 로컬 애플리케이션이 금지된 경우(**신뢰하는 로컬 애플리케이션 편집 허용** 확인란이 선택 해제됨) Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 콘솔에서 신뢰하는 애플리케이션의 통합 목록을 숨깁니다.

3. **추가** 버튼을 클릭하고 동작을 선택합니다:

   - **카테고리**. 신뢰하는 애플리케이션을 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 만들려면 카테고리 이름을 입력하고 해당 카테고리에 신뢰하는 애플리케이션을 하나 이상 추가합니다.
   - **새로운 예외**. Kaspersky Industrial CyberSecurity for Nodes가 신뢰하는 새로운 애플리케이션을 목록의 루트에 추가합니다.
   - **선택한 카테고리에 대한 새로운 제외 사항**. 신뢰하는 새로운 애플리케이션을 특정 카테고리에 추가하려면 카테고리를 선택합니다.
   - **목록에서 예외 항목 선택**. Kaspersky Industrial CyberSecurity for Nodes를 빠르게 구성하려면 사전 정의된 신뢰하는 애플리케이션 목록에서 애플리케이션을 추가할 수 있습니다.

4. **새로운 예외** 옵션을 선택하면 **검사 예외** 창이 열립니다.

5. **디스크의 전체 프로세스 경로를 사용하여 신뢰할 수 있는 것으로 간주** 확인란을 선택하고 신뢰하는 애플리케이션의 실행 파일 경로를 입력합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다:

Kaspersky Industrial CyberSecurity for Nodes는 환경 변수를 지원합니다. 동시에 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션의 로컬 인터페이스에서 경로를 변환합니다. 즉, `%userprofile%\Documents\File.exe` 경로를 입력하면, Fred123 사용자의 애플리케이션 로컬 인터페이스에 `C:\Users\Fred123\Documents\File.exe` 기록이 추가됩니다. 따라서 Kaspersky Industrial CyberSecurity for Nodes는 다른 사용자에 대해 신뢰하는 프로그램 `File.exe`를 무시합니다. 항목을 모든 사용자 계정에 적용하려면 `*` 문자를 사용할 수 있습니다(예: `C:\Users\*\Documents\File.exe`).

환경 변수를 새로 추가할 때마다 애플리케이션을 다시 시작해야 합니다.

6. 신뢰하는 애플리케이션 속성 창에서 고급 설정을 구성합니다.

7. 변경 사항을 저장하여 목록에 예외를 추가합니다.

신뢰 구역 내보내기 및 가져오기

*신뢰 구역*은 Kaspersky Industrial CyberSecurity for Nodes에서 감시하지 않는 개체 및 애플리케이션을 시스템 관리자가 구성한 목록입니다. 신뢰 구역은 *검사 예외*와 *신뢰하는 애플리케이션*으로 구성됩니다. 그 후 파일을 수정하여 동일 유형의 예외 규칙을 여러 개 추가하는 등의 작업을 진행할 수 있습니다. 내보내기/가져오기 기능을 사용하여 예외 규칙 목록과 신뢰하는 애플리케이션 목록을 백업하거나, 목록을 다른 서버로 마이그레이션할 수도 있습니다.

애플리케이션은 신뢰하는 애플리케이션과 *예외 목록*의 내보내기 및 가져오기에 XML 형식을 사용합니다.

Kaspersky Industrial CyberSecurity for Nodes는 5,000개 이상의 개체가 포함된 예외 목록 및 신뢰하는 애플리케이션 목록을 지원하지 않습니다.

Kaspersky Security Center 관리 콘솔에서 신뢰 구역을 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **보충 → 신뢰 구역** 옵션을 선택하고 **설정** 버튼을 클릭합니다.

4. 규칙 목록을 내보내려면 다음을 수행합니다.

   a. **검사 예외** 탭을 선택합니다.

   b. 전체 목록을 내보내려면 버튼을 누르고 **내보내기**을 선택합니다.

   c. 목록의 일부만 내보내려면 다음 단계를 수행합니다.

      1. **Ctrl** 또는 **Shift** 키를 사용하여 내보낼 목록 항목을 선택합니다. 모든 항목을 선택하려면 **Ctrl+A**를 누릅니다.

      2. 버튼을 클릭하고 **선택 항목 내보내기**을 선택합니다.

d. 창이 열리면 내보낼 XML 파일의 이름을 지정하고 파일을 저장할 폴더를 선택합니다. **저장** 버튼을 누릅니다.

Kaspersky Industrial CyberSecurity for Nodes는 목록을 XML 파일로 내보냅니다.

5. 신뢰하는 애플리케이션 목록을 내보내려면 다음을 수행합니다.

a. **신뢰하는 애플리케이션** 탭을 선택합니다.

b. 전체 목록을 내보내려면 버튼을 누르고 **내보내기**을 선택합니다.

c. 목록의 일부만 내보내려면 다음 단계를 수행합니다.

1. **Ctrl** 또는 **Shift** 키를 사용하여 내보낼 목록 항목을 선택합니다. 모든 항목을 선택하려면 **Ctrl+A**를 누릅니다.

2. 버튼을 클릭하고 **선택 항목 내보내기**을 선택합니다.

d. 창이 열리면 내보낼 XML 파일의 이름을 지정하고 파일을 저장할 폴더를 선택합니다. **저장** 버튼을 누릅니다.

Kaspersky Industrial CyberSecurity for Nodes는 목록을 XML 파일로 내보냅니다.

6. 예외 목록을 가져오려면 다음을 수행합니다.

a. **검사 예외** 탭을 선택합니다.

예외 규칙 목록이 포함된 창이 열립니다.

b. 폴더 아이콘을 클릭하고 드롭다운 목록에서 **가져오기** 옵션을 선택합니다.

c. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.

d. 파일을 엽니다.

컴퓨터에 이미 예외 목록이 있으면 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 신뢰하는 애플리케이션 목록을 가져오려면 다음을 수행합니다.

a. **신뢰하는 애플리케이션** 탭을 선택합니다.

신뢰하는 애플리케이션 목록이 포함된 창이 열립니다.

b. **가져오기** 버튼을 클릭합니다.

c. 창이 열리면 신뢰하는 애플리케이션 목록을 가져올 XML 파일을 선택합니다.

d. 파일을 엽니다.

컴퓨터에 이미 신뢰하는 애플리케이션 목록이 있는 경우 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. 변경 사항을 저장합니다.

웹 콘솔에서 신뢰 구역을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보충 → 신뢰 구역** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. 규칙 목록을 내보내려면 다음을 수행합니다.

   a. **검사 예외 및 신뢰하는 애플리케이션** 탭에서 내보낼 예외를 선택합니다.

   b. 점 세 개를 클릭하고 **내보내기** 옵션을 선택합니다.

   c. 선택한 예외 규칙만 내보낼 것인지 전체 예외 규칙 목록을 내보낼 것인지 확인합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 목록을 XML 파일로 내보냅니다.

6. 신뢰하는 애플리케이션 목록을 내보내려면 다음을 수행합니다.

   a. **검사 예외 및 신뢰하는 애플리케이션** 탭에서 내보내려는 애플리케이션을 선택합니다.

   b. 점 세 개를 클릭하고 **내보내기** 옵션을 선택합니다.

   c. 선택한 애플리케이션만 내보낼 것인지 전체 목록을 내보낼 것인지 확인합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 목록을 XML 파일로 내보냅니다.

7. 예외 목록을 가져오려면 다음을 수행합니다.

   a. 애플리케이션 버전 4.0 이하에서 생성한 XML 파일에서 예외 목록을 가져오려는 경우 **검사 예외 및 신뢰하는 애플리케이션** 탭에서 **이전 버전에서 가져오기**을 클릭합니다.

   4.5 이상 버전에서 생성한 XML 파일에서 규칙을 가져오는 경우 **가져오기**를 클릭합니다.

   b. 컴퓨터에 이미 예외 목록이 있으면 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

   c. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.

   d. **가져오기** 버튼을 클릭합니다.

8. 신뢰하는 애플리케이션 목록을 가져오려면 다음을 수행합니다.

   a. 애플리케이션 버전 4.0 이하에서 생성한 XML 파일에서 신뢰하는 애플리케이션 목록을 가져오려는 경우 **검사 예외 및 신뢰하는 애플리케이션** 탭에서 **이전 버전에서 가져오기**을 클릭합니다.

   4.5 이상 버전에서 생성한 XML 파일에서 신뢰하는 애플리케이션을 가져오는 경우 **가져오기**를 클릭합니다.

   b. 컴퓨터에 이미 신뢰하는 애플리케이션 목록이 있는 경우 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

   c. 창이 열리면 신뢰하는 애플리케이션 목록을 가져올 XML 파일을 선택합니다.

   d. **가져오기** 버튼을 클릭합니다.

9. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 신뢰 구역을 내보내거나 가져오는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **신뢰 구역** 옵션을 선택합니다.

   신뢰 구역 설정 구성 창이 열립니다.

2. 예외 목록이나 신뢰하는 애플리케이션 목록을 내보내려면:

   a. **예외 규칙** 섹션에서 **검사 예외** 또는 **신뢰하는 애플리케이션** 블록 옆에 있는 **설정** 버튼을 클릭합니다.

   검사 예외 목록 또는 신뢰하는 애플리케이션 목록이 포함된 창이 열립니다.

   b. 전체 목록을 내보내려면 버튼을 누르고 **내보내기**을 선택합니다.

   c. 목록의 일부만 내보내려면 다음 단계를 수행합니다.

      1. **Ctrl** 또는 **Shift** 키를 사용하여 내보낼 목록 항목을 선택합니다. 모든 항목을 선택하려면 **Ctrl+A**를 누릅니다.

      2. 버튼을 클릭하고 **선택 항목 내보내기**을 선택합니다.

   d. 창이 열리면 내보낼 XML 파일의 이름을 지정하고 파일을 저장할 폴더를 선택합니다. **저장** 버튼을 누릅니다.

   Kaspersky Industrial CyberSecurity for Nodes는 목록을 XML 파일로 내보냅니다.

3. 예외 목록 및 신뢰하는 애플리케이션 목록을 가져오려면:

   a. **예외 규칙** 섹션에서 **검사 예외** 또는 **신뢰하는 애플리케이션** 블록 옆에 있는 **설정** 버튼을 클릭합니다.

   b. 가져올 예외 및 신뢰하는 애플리케이션을 선택합니다.

   c. 폴더 아이콘을 클릭하고 **가져오기** 옵션을 선택합니다.

   d. 열린 창에서 예외 목록 및 신뢰하는 애플리케이션 목록을 가져올 XML 파일을 선택합니다.

   e. 파일을 엽니다.

   컴퓨터에 이미 예외 목록이 있으면 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

4. 변경 사항을 저장합니다.

신뢰하는 시스템 인증서 저장소 사용

시스템 인증서 저장소를 사용하면 신뢰하는 디지털 서명으로 서명된 애플리케이션을 바이러스 검사에서 예외할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 이러한 애플리케이션을 *신뢰하는* 그룹에 자동으로 할당합니다.

Kaspersky Security Center 관리 콘솔에서 신뢰하는 시스템 인증서 저장소 사용을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **보충 → 신뢰 구역** 옵션을 선택하고 **설정** 버튼을 클릭합니다.

4. **신뢰하는 시스템 인증서 저장소** 탭을 선택합니다.

5. **신뢰하는 시스템 인증서 저장소 사용** 확인란을 선택하고 드롭다운 목록에서 Kaspersky Industrial CyberSecurity for Nodes가 신뢰하는 것으로 간주할 시스템 저장소를 선택합니다.

6. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 신뢰하는 시스템 인증서 저장소 사용을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보충** → **신뢰 구역** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. **신뢰하는 시스템 인증서 저장소** 탭을 선택합니다.

6. **신뢰하는 시스템 인증서 저장소 사용** 확인란을 선택하고 드롭다운 목록에서 Kaspersky Industrial CyberSecurity for Nodes가 신뢰하는 것으로 간주할 시스템 저장소를 선택합니다.

7. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 신뢰하는 시스템 인증서 저장소 사용을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **신뢰 구역** 옵션을 선택합니다.
   신뢰 구역 설정 구성 창이 열립니다.

2. **신뢰하는 시스템 인증서 저장소**에서 **신뢰하는 시스템 인증서 저장소 사용** 확인란을 선택하고 드롭다운 목록에서 Kaspersky Industrial CyberSecurity for Nodes가 신뢰하는 것으로 간주할 시스템 저장소를 선택합니다.

3. 변경 사항을 저장합니다.

사전 정의된 검사 예외 및 신뢰하는 애플리케이션

미리 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 다음 소프트웨어의 프로세스와 파일을 신뢰 구역에 빠르게 추가할 수 있습니다.

- 산업용 소프트웨어
- Microsoft Exchange Server
- Microsoft SQL Server
- Microsoft Hyper-V
- Microsoft Windows Server의 데이터 중복 제거 프로세스
- Microsoft System Center Configuration Manager

다음과 같은 방법으로 사전 정의된 예외 규칙 및 신뢰하는 애플리케이션을 선택할 수 있습니다.

- 애플리케이션을 설치합니다.
  - 마법사를 사용하여 로컬로 애플리케이션 설치
  - 설치 패키지 속성
- 정책을 설정합니다.
  - 새 정책 마법사
  - 정책 속성: 검사 예외 및 신뢰하는 애플리케이션
  - 명령줄에서.

산업용 소프트웨어 예외 프로필

*예외 프로필*은 특정 산업 애플리케이션의 프로세스와 파일을 신뢰하는 애플리케이션 및 검사 예외 목록에 추가하고 애플리케이션 실행 제어 규칙을 구성하기 위한 XML 형식의 예외 규칙 집합입니다.

아래 표에는 사용 가능한 모든 산업 애플리케이션 예외 프로필이 나열되어 있습니다.

각 예외 프로필에 대한 규칙은 산업 애플리케이션이 기본 폴더에 설치되어 있다고 가정합니다. 산업용 애플리케이션을 기본 폴더가 아닌 다른 폴더에 설치했다면 Kaspersky Industrial CyberSecurity for Nodes 설치 후 해당 예외 프로필의 규칙을 수동으로 조정해야 합니다.

산업용 소프트웨어 예외 프로필

예외 프로필	신뢰 구역 구성 규칙	애플리케이션 실행 제어 구성 규칙	명령줄 예외 프로필 이름
ABB 800xA DCS	예	아니오	ABB_800xA_DCS
ABB MicroSCADA	예	아니오	ABB_MicroSCADA
AVADS Archiving Server 1.2	예	아니오	AVADS_AS_1.2
AVADS SAR Expert 1.0	예	아니오	AVADS_SAR_Expert_1.0
Bently Nevada System 1	예	예	BakerHughes_BentlyNevadaSystem
Bosch Building Integration System	예	아니오	BOSCH_BIS
BRIC	예	아니오	BRIC_IDE
Consen SC9000	예	아니오	Consen
Emerson DeltaV	예	예	Emerson_DeltaV
Emerson OpenEnterprise	예	예	Emerson_OpenEnterprise
Emerson Ovation	예	아니오	Emerson_Ovation
Emerson PipelineManager	예	아니오	Emerson_Pipeline
GE Cimplicity	예	아니오	GE_Cimplicity
Honeywell Experion PKS	예	아니오	Honeywell_Experion_PKS
MasterSCADA4D	예	아니오	MasterSCADA4D
Mitsubishi MAPS	예	아니오	Mitsubishi_MAPS

예외 프로필	신뢰 구역 구성 규칙	애플리케이션 실행 제어 구성 규칙	명령줄 예외 프로필 이름
Nefteavtomatika “NaftaManagement PCM” 25.01	예	아니오	Nefteavtomatika_NaftaManagement_PCM_25.01
OMRON CX-Supervisor	예	아니오	OMRON_CX-Supervisor
PcVue Solutions 15	예	예	PcVue_PcVue15
RegLab PC “AstraRegul” 2025.08.15.00	예	아니오	RegLab_AstraRegul_2025.08.15.00
Rexroth IndraWorks	예	아니오	Rexroth_IndraWorks
Rockwell Automation FactoryTalk View	예	아니오	Rockwell_Automation_FactoryTalk_View
Schneider Electric Citect SCADA	예	아니오	Schneider_Electric_Citect_SCADA
Schneider Electric Clear SCADA	예	예	Schneider_Electric_Clear_SCADA
Schneider Electric EcoStruxure Foxboro DCS	예	아니오	Schneider_Electric_EcoStruxure_Foxboro_DCS
Schneider Electric Unity Pro	예	아니오	Schneider_Electric_Unity_Pro
Siemens SIMATIC PCS 7 v8.2	예	아니오	Siemens_SIMATICPCS7-8.2SP1
Siemens SIMATIC PCS 7 v9.0	예	아니오	Siemens_SIMATICPCS7-9.0SP2
Siemens SIMATIC PCS 7 v9.1	예	예	Siemens_SIMATICPCS7-9.1
Siemens SIMATIC WinCC OA	예	예	Siemens_SIMATIC_WinCC_OA
Siemens SIMATIC WinCC	예	아니오	Siemens_SIMATIC_WinCC
Siemens SIMATIC STEP7	예	아니오	Siemens_SIMATIC_STEP7
Siemens TIA Portal	예	아니오	Siemens_TIA_Portal
Siemens DIGSI	예	아니오	Siemens_DIGSI
Siemens SICAM PAS	예	아니오	Siemens_SICAM_PAS
Valmet DNA	예	예	Valmet_DNA
Wonderware InTouch	예	아니오	Wonderware_InTouch
Wonderware System Platform 2017	예	아니오	Wonderware_System-Platform-2017
Yokogawa CENTUM VP	예	아니오	Yokogawa_CENTUM_VP
Yokogawa ProSafe-RS	예	아니오	Yokogawa_ProSafe-RS
Yokogawa FAST/TOOLS	예	아니오	Yokogawa_FAST_TOOLS
AVADS SAR Expert 1.0	예	아니오	AVADS_SAR_Expert_1.0
AVADS Archiving Server 1.2	예	아니오	AVADS_AS_1.2
AVM-Energo SCADA Sonica 7.90.26	예	아니오	AVM_Energo_SCADA_Sonica_7.90.26
Alpha.Platform	예	예	AutomiqSoft_AlphaPlatform
VACS	예	예	SPEMT_VACSStandart
GAUS	예	아니오	GAUS
ISUB ARBITER	예	아니오	ARBITR
Concor_SP KT	예	아니오	Software_Platform_KT_1.2
PK AstraRegul	예	아니오	AstraRegul
NaftaProcess DCS	예	예	NaftaProcess_DCS
Supcon_SP i-OMC	예	아니오	SUPCON i-OMC_1.2
Sib MIR Sibmir_SCADA 1.3	예	아니오	SibMir_SCADA
SimpLight_Linux SimpLight_Linux	예	아니오	SIMP_Light

예외 프로필	신뢰 구역 구성 규칙	애플리케이션 실행 제어 구성 규칙	명령줄 예외 프로필 이름
TEKON	예	아니오	`TECON`
Tornado-N	예	예	`Tornado_Tornado-N`
TREI	예	아니오	`TREI`
CASCADE 3.18 Digital Platform	예	아니오	`Kaskad_3.18`
CASCADE 4 Digital Platform	예	아니오	`KASKAD_4.0`
EKRA (EKRASMS, EKRASMS-SP)	예	예	`EKRA`

Kaspersky Industrial CyberSecurity for Nodes을 설치하는 동안 산업용 소프트웨어 예외 프로필을 적용하려면:

- 설정 마법사의 해당하는 단계에서 필요한 예외 프로필을 선택합니다.
- 명령줄 설치 옵션을 입력합니다: `ADDEXCLUSION=<exclusion profile name 1>;<exclusion profile name 2>;...;<exclusion profile name n>`.

실시간 파일 보호

Kaspersky Industrial CyberSecurity for Nodes의 실시간 파일 보호 구성 요소는 다음과 같은 보호 중인 장치 개체에 접근할 때 해당 개체를 검사합니다:

- 파일
- NTFS 대체 데이터 스트림.
- 로컬 하드 드라이브와 외부 장치에 있는 마스터 부트 레코드 및 부팅 섹터.
- Windows Server 2016 및 Windows Server 2019 컨테이너 파일.

애플리케이션이 보호 중인 장치에 파일을 작성하거나 장치에서 파일을 읽는 경우, Kaspersky Industrial CyberSecurity for Nodes는 이 파일을 가로채 위협이 있는지 검사한 후 위협을 탐지하면 기본 동작 또는 사용자가 지정한 동작을 수행합니다. 즉 바이러스를 치료하거나 격리 저장소로 옮기거나 삭제합니다. Kaspersky Industrial CyberSecurity for Nodes는 치료 또는 삭제하기 전에 소스 파일의 암호화된 복사본을 백업 폴더에 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes는 Windows Server 2016 및 Windows Server 2019 컨테이너에서 실행되는 파일 동작을 가로챕니다.

*컨테이너*는 운영 체제와 직접 상호 작용하지 않고 애플리케이션을 실행할 수 있는 격리된 환경입니다. 컨테이너가 구성 요소 보호 범위에 포함된 경우 Kaspersky Industrial CyberSecurity for Nodes는 사용자가 접근하는 컨테이너 파일에 컴퓨터 위협이 있는지 검사합니다. 위협이 탐지되면 애플리케이션은 컨테이너 치료를 시도합니다. 치료에 성공하면 컨테이너는 계속 작동합니다. 치료에 실패하면 컨테이너의 전원이 꺼집니다.

Kaspersky Industrial CyberSecurity for Nodes는 Windows Subsystem for Linux®에서 실행되는 프로세스의 악성 코드도 탐지합니다. 이러한 프로세스의 경우 실시간 파일 보호 구성 요소는 현재 구성에서 정의한 동작을 적용합니다.

작업 보호 범위 및 보안 설정 정보

기본적으로 실시간 파일 보호 구성 요소는 장치 파일 시스템에 있는 모든 개체를 보호합니다. 파일 시스템의 모든 개체를 보호해야 하는 보안 요구 사항이 없거나 작업 범위에서 개체를 제외하려는 경우 보호 범위를 제한할 수 있습니다.

애플리케이션 콘솔에서 보호 범위는 Kaspersky Industrial CyberSecurity for Nodes가 모니터링할 수 있는 장치의 파일 리소스 목록으로 표시됩니다.

보안 설정

작업 보안 설정은 보호 범위에 포함된 모든 노드 또는 항목에 대한 공통 설정으로 구성하거나, 장치의 파일 리소스 목록에 있는 각 노드 또는 항목에 대한 다른 설정으로 구성할 수 있습니다.

선택한 상위 노드에 구성된 보안 설정은 모든 하위 노드에 자동으로 적용됩니다. 상위 노드의 보안 설정은 별도로 구성된 하위 노드에는 적용되지 않습니다.

선택한 보호 범위의 설정은 다음 중 한 가지 방법으로 구성할 수 있습니다:

- 세 사전 정의된 보안 레벨 중 하나를 선택합니다.
- 파일 리소스 목록에서 선택 노드 또는 항목에 대해 수동으로 보안 설정을 구성합니다(보안 레벨 **사용자 지정**로 변경).

사전 정의된 보호 범위

파일 리소스 목록은 구성된 Microsoft Windows 보안 설정을 기반으로 읽기 접근 권한을 가진 노드를 표시합니다.

Kaspersky Industrial CyberSecurity for Nodes는 다음과 같은 사전 정의된 보호 범위를 적용합니다:

- **로컬 하드 드라이브**. Kaspersky Industrial CyberSecurity for Nodes가 장치 하드 드라이브의 파일을 보호합니다.
- **이동식 드라이브**. Kaspersky Industrial CyberSecurity for Nodes가 외부 장치(예: CD 또는 이동식 드라이브)의 파일을 보호합니다. 모든 이동식 디스크나 개별 디스크, 폴더, 파일을 보호 범위에 포함하거나 제외할 수 있습니다.
- **네트워크**. Kaspersky Industrial CyberSecurity for Nodes가 장치에서 실행 중인 애플리케이션이 네트워크 폴더에 작성했거나 네트워크 폴더에서 읽은 파일을 보호합니다. Kaspersky Industrial CyberSecurity for Nodes는 보호 중인 다른 장치의 애플리케이션에서 접근한 파일은 보호하지 않습니다.

기본적으로 범위 목록에서 사전 정의된 보호 범위를 보고 구성할 수 있습니다. 보호 범위 설정에서 목록이 만들어지는 동안 목록에 사전 정의된 범위를 추가할 수도 있습니다.

연결된 네트워크 드라이브도 보호 중인 장치의 파일 리소스 목록에 표시되지 않습니다. 보호 범위에 네트워크 드라이브의 개체를 포함하려면 UNC(Universal Naming Convention) 형식으로 이 네트워크 드라이브에 해당하는 폴더 경로를 지정합니다.

사전 정의된 보안 레벨 정보

보호 중인 장치의 파일 리소스 트리나 파일 리소스 목록에서 선택 노드에 사전 정의된 보안 레벨 **최대 성능** 및 **권장**, **최대 보호**, **알림** 중 하나를 적용할 수 있습니다. 이러한 레벨 각각에는 자체적으로 사전 정의된 보안 설정 세트가 있습니다(아래 표 참조).

최대 성능

최대 성능 보안 레벨은 보호 중인 장치 및 워크스테이션에서 Kaspersky Industrial CyberSecurity for Nodes를 사용하는 것 외에도 네트워크에 방화벽 및 기존 보안 정책 등의 추가 보호 장치 보안 조치가 있을 때 권장합니다.

권장

권장 보안 레벨은 장치에 대한 보호 및 성능 영향을 가장 효과적으로 조합합니다. Kaspersky 전문가는 이 레벨을 대부분의 회사 네트워크에서 장치를 보호하는 데 적합한 것으로 권장합니다. 기본적으로 **권장** 보안 레벨이 설정됩니다.

최대 보호

최대 보호 보안 레벨은 조직의 네트워크에 필요한 장치 보안 요구 사항이 높을 때 권장합니다.

알림

알림 보안 레벨은 회사 네트워크에 감염될 수 있는 컴퓨터가 많고, 컴퓨터를 차단하면 조직의 운영에 큰 지장을 초래할 수 있을 때 권장합니다.

사전 설정된 보안 레벨과 대응하는 설정 값

옵션	보안 레벨			
	최대 성능	권장	최대 보호	알림
개체 보호	안티 바이러스 데이터베이스에 지정된 확장자 목록에 따라 검사한 개체	형식에 따라 검사한 개체	형식에 따라 검사한 개체	형식에 따라 검사한 개체
새로운 파일과 수정된 파일만 검사	활성화됨	활성화됨	비활성화됨	활성화됨
복합 파일 검사	비활성화됨	Microsoft Office 형식 파일 검사	Microsoft Office 형식 파일 검사	Microsoft Office 형식 파일 검사
감염된 개체 및 기타 개체에 수행할 동작	접근을 차단하고 치료합니다. 치료 불가능한 경우 삭제	Kaspersky 전문가가 권장하는 동작 수행 및 접근 차단	접근을 차단하고 치료합니다. 치료 불가능한 경우 삭제	알림
선택한 개체 유형에 동작 적용	비활성화됨	비활성화됨	비활성화됨	비활성화됨
내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거	비활성화됨	비활성화됨	활성화됨	비활성화됨
시스템 중요 개체는 운영 체제와 Kaspersky Industrial CyberSecurity for Nodes의 작동에 필요한 파일입니다. 이러한 파일은 삭제할 수 없습니다. 이러한 개체와 연결된 프로세스는 종료할 수 없습니다.				
다음보다 큰 복합 파일을 백그라운드에서 압축 해제(MB)				
검사 시간이 다음을 초과하면 검사 중지(초)	60초.	60초.	60초.	60초.
다음을 초과하는 복합 파일은 검사하지 않음(MB)	8MB	8MB	설정되지 않음	8MB
iSwift 기술 사용	활성화됨	활성화됨	활성화됨	활성화됨
iChecker 기술 사용	활성화됨	활성화됨	활성화됨	활성화됨

실시간 파일 보호 구성 요소에서 기본으로 검사하는 파일 확장자

Kaspersky Industrial CyberSecurity for Nodes는 기본적으로 다음 확장자를 가진 파일을 검사합니다.

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*

- *.exe*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*

- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*

- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?.*

실시간 파일 보호 구성 요소 구성

기본적으로 실시간 파일 보호 구성 요소에서는 아래 표에 설명된 설정이 사용됩니다. 사용자가 설정 값을 변경할 수 있습니다.

실시간 파일 보호 구성 요소의 기본 설정

파라미터	기본 값	설명
보호 범위	가상 드라이브를 제외한 보호 중인 장치 전체.	보호 범위를 변경하려면 이 옵션을 사용합니다.
보안 설정	전체 보호 범위에 대한 공통 설정이며, **권장** 보안 레벨에 해당합니다.	보호 중인 장치의 파일 리소스 목록 또는 트리에서 선택 노드에 대해 다음 작업을 수행할 수 있습니다: • 사전 정의된 다른 보안 레벨 선택 • 수동으로 보안 설정 변경 선택 노드의 보안 설정을 템플릿으로 저장하여 나중에 다른 노드에 사용할 수 있습니다.
개체 보호 모드	**스마트 모드**.	이 옵션을 사용하여 보호 모드를 선택합니다. 즉 Kaspersky Industrial CyberSecurity for Nodes가 개체를 검사할 접근 시도의 유형을 정의합니다.
휴리스틱 분석기	**보통** 보안 레벨이 적용됩니다.	휴리스틱 분석기를 활성화 또는 비활성화할 수 있고 분석 레벨을 구성할 수 있습니다.
악성 활동을 보이는 세션의 네트워크 공유 리소스 접근 차단	적용되지 않음.	이 옵션을 사용하여 현재 세션을 차단하고 차단된 호스트 저장소 섹션에서 악성 활동이 탐지된 호스트 IP 또는 호스트 LUID를 추가합니다.
활성 감염이 탐지되면 중요 영역 검사 실행	적용됨.	활성 감염이 탐지될 경우 Kaspersky Industrial CyberSecurity for Nodes는 중요 영역 검사 작업을 생성하고 실행합니다.

파라미터	기본 값	설명
치료가 실패하면 컨테이너 중지	적용됨.	애플리케이션이 탐지된 개체에 대해 충분한 읽기 및 쓰기 권한을 가지고 있지 않을 수 있습니다. 이때는 탐지된 개체를 치료하거나 삭제할 수 없습니다. 이 확인란을 선택하면 애플리케이션이 탐지된 개체를 차단하고 컨테이너를 중지합니다. 이 확인란을 선택하지 않으면 애플리케이션이 탐지된 개체만 차단합니다.
Windows 컨테이너에서 실행되는 파일 동작 검사 안 함	적용됨.	이 확인란을 선택하면 애플리케이션이 컨테이너가 시작될 때만 컨테이너를 검사합니다. 이 확인란을 선택하지 않으면 애플리케이션이 실시간으로 계속 컨테이너를 검사합니다.

Kaspersky Security Center 관리 콘솔에서 파일의 바이러스 검사를 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.
4. **실시간 파일 보호 설정** 섹션에서 **설정** 버튼을 클릭합니다.
5. **실시간 파일 보호** 확인란을 선택합니다.
6. **개체 보호 모드** 블록 **일반** 탭에서 실시간 파일 보호 운영 모드를 선택합니다:
   - **스마트 모드**. Kaspersky Industrial CyberSecurity for Nodes가 검사할 개체를 자동으로 선택합니다. 개체가 열려 있는 동안 검사하고 개체가 수정되면 저장 후 다시 검사합니다. 프로세스에서 개체에 여러 번 접근하고 수정할 경우 Kaspersky Industrial CyberSecurity for Nodes는 프로세스에서 마지막으로 개체를 저장한 후에만 개체를 다시 검사합니다.
   - **접근 및 수정 시**. Kaspersky Industrial CyberSecurity for Nodes는 개체를 열 때 검사하고 개체가 수정되면 저장 후 다시 검사합니다. 이 옵션은 기본적으로 선택되어 있습니다.
   - **접근 시**. Kaspersky Industrial CyberSecurity for Nodes가 읽거나 실행, 수정을 위해 열리는 모든 개체를 검사합니다.
   - **실행 시**. Kaspersky Industrial CyberSecurity for Nodes가 실행을 위한 파일 접근 시도가 있을 경우에만 파일을 검사합니다.
7. **휴리스틱 분석 사용** 확인란을 선택하거나 선택 해제합니다.
8. **악성 활동을 보이는 세션의 네트워크 공유 리소스 접근 차단** 확인란을 선택하거나 선택 해제합니다.
9. **활성 감염이 탐지되면 중요 영역 검사 실행** 확인란을 선택하거나 선택 해제합니다.

   이 확인란을 선택하면 활성 감염 탐지 시 Kaspersky Industrial CyberSecurity for Nodes가 사전 정의된 *중요 영역 검사* 작업을 수행합니다. 기본적으로 확인란이 선택되어 있습니다.
10. Windows 컨테이너에서 실행되는 파일 동작 검사의 설정을 지정합니다.
11. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 파일 바이러스 검사를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **실시간 컴퓨터 보호 → 실시간 파일 보호** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. **실시간 파일 보호 사용** 확인란을 선택합니다.

6. **개체 보호 모드** 블록 **일반** 탭에서 실시간 파일 보호 운영 모드를 선택합니다:

   - **스마트 모드**. Kaspersky Industrial CyberSecurity for Nodes가 검사할 개체를 자동으로 선택합니다. 개체가 열려 있는 동안 검사하고 개체가 수정되면 저장 후 다시 검사합니다. 프로세스에서 개체에 여러 번 접근하고 수정할 경우 Kaspersky Industrial CyberSecurity for Nodes는 프로세스에서 마지막으로 개체를 저장한 후에만 개체를 다시 검사합니다.

   - **접근 및 수정 시**. Kaspersky Industrial CyberSecurity for Nodes는 개체를 열 때 검사하고 개체가 수정되면 저장 후 다시 검사합니다. 이 옵션은 기본적으로 선택되어 있습니다.

   - **접근 시**. Kaspersky Industrial CyberSecurity for Nodes가 읽거나 실행, 수정을 위해 열리는 모든 개체를 검사합니다.

   - **실행 시**. Kaspersky Industrial CyberSecurity for Nodes가 실행을 위한 파일 접근 시도가 있을 경우에만 파일을 검사합니다.

7. **휴리스틱 분석 사용** 확인란을 선택하거나 선택 해제합니다.

8. **악성 활동을 보이는 네트워크 세션의 네트워크 공유 리소스에 대한 접근 차단** 확인란을 선택하거나 선택 해제합니다.

9. **활성 감염이 탐지되면 중요 영역 검사 실행** 확인란을 선택하거나 선택 해제합니다.

   이 확인란을 선택하면 활성 감염 탐지 시 Kaspersky Industrial CyberSecurity for Nodes가 사전 정의된 *중요 영역 검사* 작업을 수행합니다. 기본적으로 확인란이 선택되어 있습니다.

10. Windows 컨테이너에서 실행되는 파일 동작 검사의 설정을 지정합니다.

11. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 파일 바이러스 검사를 활성화하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호 → 실시간 파일 보호** 옵션을 선택합니다.

2. **실시간 파일 보호** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.

   속성: 실시간 파일 보호 창이 열립니다.

3. **실시간 파일 보호** 확인란을 선택합니다.

4. **개체 보호 모드** 블록 **일반** 탭에서 실시간 파일 보호 운영 모드를 선택합니다:

   - **스마트 모드**. Kaspersky Industrial CyberSecurity for Nodes가 검사할 개체를 자동으로 선택합니다. 개체가 열려 있는 동안 검사하고 개체가 수정되면 저장 후 다시 검사합니다. 프로세스에서 개체에 여러 번 접근하고 수정할 경우 Kaspersky Industrial CyberSecurity for Nodes는 프로세스에서 마지막으로 개체를 저장한 후에만 개체를 다시 검사합니다.

   - **접근 및 수정 시**. Kaspersky Industrial CyberSecurity for Nodes는 개체를 열 때 검사하고 개체가 수정되면 저장 후 다시 검사합니다. 이 옵션은 기본적으로 선택되어 있습니다.

- **접근 시**. Kaspersky Industrial CyberSecurity for Nodes가 읽거나 실행, 수정을 위해 열리는 모든 개체를 검사합니다.
- **실행 시**. Kaspersky Industrial CyberSecurity for Nodes가 실행을 위한 파일 접근 시도가 있을 경우에만 파일을 검사합니다.

5. **휴리스틱 분석 사용** 확인란을 선택하거나 선택 해제합니다.
6. **악성 활동을 보이는 세션의 네트워크 공유 리소스 접근 차단** 확인란을 선택하거나 선택 해제합니다.
7. **활성 감염이 탐지되면 중요 영역 검사 실행** 확인란을 선택하거나 선택 해제합니다.

   이 확인란을 선택하면 활성 감염 탐지 시 Kaspersky Industrial CyberSecurity for Nodes가 사전 정의된 *중요 영역 검사* 작업을 수행합니다. 기본적으로 확인란이 선택되어 있습니다.
8. Windows 컨테이너에서 실행되는 파일 동작 검사의 설정을 지정합니다.
9. 변경 사항을 저장합니다.

실시간 파일 보호 구성 요소의 보호 범위 구성

기본적으로 실시간 파일 보호 구성 요소에서는 전체 보호 범위에 대해 공통 보안 설정을 사용합니다. 이 설정은 **권장** 사전 설정된 보안 레벨에 해당합니다.

보안 설정의 기본값은 전체 보호 범위에 대해 공통 설정으로 구성하거나 장치 파일 리소스 목록에 있는 개별 항목에 대해 별도의 설정을 구성하는 방법으로 수정할 수 있습니다.

동일한 개체가 여러 보호 범위 항목에 포함되어 있고 이러한 항목의 보안 레벨이 서로 다른 경우 목록의 마지막 규칙이 우선 적용됩니다. 예를 들어 **모든 하드 드라이브**(보안 레벨 **알림**)와 `*\Users\*\Downloads\*`(보안 레벨 **사용자 지정**)이라는 두 항목이 포함된 보호 범위를 생각해 보십시오. 애플리케이션은 `Downloads` 폴더를 제외하고 Inform 레벨에 따라 하드 드라이브를 검사합니다. 이 항목이 보호 범위 목록의 마지막 항목이기 때문에 애플리케이션은 수동으로 지정된 설정에 따라 `Downloads` 폴더를 검사합니다.

Kaspersky Security Center 관리 콘솔에서 실시간 파일 보호의 보호 범위를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.
4. **실시간 파일 보호** 섹션에서 **설정** 버튼을 클릭합니다.
5. **보호 범위** 탭을 선택합니다.
6. 보호 중인 장치의 파일 리소스 목록에서 사전 정의된 보안 레벨을 설정할 항목을 선택합니다.
7. 파일 공유가 목록에 없으면 직접 추가합니다:
   a. **추가** 버튼을 클릭합니다.
   b. 폴더 트리를 사용하여 필요한 개체의 경로를 지정하거나 **개체** 필드에 경로를 입력합니다.

필요하다면 특수 문자를 사용하여 개체 경로 마스크를 입력합니다:

- `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.

- `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.

- `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

컴퓨터의 파일 리소스 목록에 있는 **내 PC** 개체에는 **모든 하드 드라이브**, **모든 네트워크 드라이브** 및 **모든 이동식 드라이브** 개체가 포함되어 있습니다.

c. **확인** 버튼을 클릭합니다.

8. 선택한 파일 리소스가 보호 범위에 포함되어 있는지 확인합니다.

9. **구성** 버튼을 클릭해 선택한 보호 범위에 대해 사전 정의된 보안 레벨을 지정합니다. 기본적으로는 전체 보호 범위에 같은 보안 설정이 적용됩니다. 이 설정은 **권장** 사전 설정된 보안 레벨에 해당합니다. 기본 보안 설정을 편집할 수도 있습니다.

10. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 실시간 파일 보호의 보호 범위를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **실시간 컴퓨터 보호** → **실시간 파일 보호** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. **보호 범위** 탭을 선택합니다.

6. 보호 중인 장치의 파일 리소스 목록에서 사전 정의된 보안 레벨을 설정할 항목을 선택합니다.

7. 파일 공유가 목록에 없으면 직접 추가합니다:

   a. **추가** 버튼을 클릭합니다.

   b. **개체 유형** 목록에서 옵션을 선택합니다.

마스크 옵션에서, 특수 문자를 사용하여 개체 경로 마스크를 입력합니다:

- `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.

- `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.

- `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

컴퓨터의 파일 리소스 목록에 있는 **내 PC** 개체에는 **모든 하드 드라이브**, **모든 네트워크 드라이브** 및 **모든 이동식 드라이브** 개체가 포함되어 있습니다.

c. **확인** 버튼을 클릭합니다.

8. 목록 항목 옆의 토글 스위치를 사용하여 선택한 파일 리소스가 보호 범위에 포함되었는지 확인합니다.

9. **편집** 버튼을 클릭해 선택한 보호 범위에 대해 사전 정의된 보안 레벨을 지정합니다. 기본적으로는 전체 보호 범위에 같은 보안 설정이 적용됩니다. 이 설정은 **권장** 사전 설정된 보안 레벨에 해당합니다. 기본 보안 설정을 편집할 수도 있습니다.

10. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 실시간 파일 보호의 보호 범위를 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호 → 실시간 파일 보호** 옵션을 선택합니다.

2. **실시간 파일 보호** 노드의 결과 창에서 **보호 범위 구성** 버튼을 클릭합니다.
   속성: 실시간 파일 보호 창이 열립니다.

3. 보호 중인 장치의 파일 리소스 목록에서 사전 정의된 보안 레벨을 설정할 항목을 선택합니다.

4. 파일 공유가 목록에 없으면 직접 추가합니다:

   a. **추가** 버튼을 클릭합니다.

   b. 폴더 트리를 사용하여 필요한 개체의 경로를 지정하거나 **개체** 필드에 경로를 입력합니다.

필요하다면 특수 문자를 사용하여 개체 경로 마스크를 입력합니다:

- `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.

- `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.

- `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

컴퓨터의 파일 리소스 목록에 있는 **내 PC** 개체에는 **모든 하드 드라이브**, **모든 네트워크 드라이브** 및 **모든 이동식 드라이브** 개체가 포함되어 있습니다.

c. **확인** 버튼을 클릭합니다.

5. 선택한 파일 리소스가 보호 범위에 포함되어 있는지 확인합니다.

6. **구성** 버튼을 클릭해 선택한 보호 범위에 대해 사전 정의된 보안 레벨을 지정합니다. 기본적으로는 전체 보호 범위에 같은 보안 설정이 적용됩니다. 이 설정은 **권장** 사전 설정된 보안 레벨에 해당합니다. 기본 보안 설정을 편집할 수도 있습니다.

7. 변경 사항을 저장합니다.

보안 설정 수동 구성

기본적으로 실시간 파일 보호 작업은 전체 보호 범위에 공통 보안 설정을 사용합니다. 이 설정은 **권장** 사전 설정된 보안 레벨에 해당합니다.

보안 설정의 기본값은 전체 보호 범위에 대한 공통 설정으로 구성하거나 장치의 파일 리소스 목록에 있는 개별 항목 또는 트리에 있는 노드별 별도의 설정으로 구성하는 방법으로 수정할 수 있습니다.

보호 중인 장치의 파일 리소스 트리로 작업할 시 선택한 상위 노드에 구성된 보안 설정이 모든 하위 노드에 자동으로 적용됩니다. 상위 노드의 보안 설정은 별도로 구성된 하위 노드에는 적용되지 않습니다.

Kaspersky Security Center 관리 콘솔에서 직접 보안 설정을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.

4. **실시간 파일 보호** 섹션에서 **설정** 버튼을 클릭합니다.

5. **실시간 파일 보호** 창에서 **보호 범위** 탭으로 갑니다.

6. 보안 설정을 구성할 리소스를 선택합니다.

7. **구성** 버튼을 클릭합니다.

8. 창이 열리면 필요한 보안 레벨을 선택하고 **설정** 버튼을 클릭합니다.

9. **일반** 탭에서 다음 설정을 지정합니다:

   - 보호 범위에 포함해야 하는 개체:

     - **모든 개체**. Kaspersky Industrial CyberSecurity for Nodes가 모든 개체를 검사합니다.

     - **형식에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 형식을 기준으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 형식 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.

     - **안티 바이러스 데이터베이스에 지정된 확장자 목록으로 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 확장자 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.

     - **지정된 확장자 목록에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. 확장자 목록은 사용자가 직접 지정합니다.

   - **최적화** 블록에서 **새로운 파일과 수정된 파일만 검사** 확인란을 선택하거나 선택 해제합니다.

   - **복합 파일 검사** 섹션에서 검사 범위에 포함할 복합 개체를 지정합니다:

     - **압축파일 검사**
     - **배포 패키지 검사**
     - **Microsoft Office 형식 파일 검사**
     - **이메일 형식 파일 검사**

10. **동작** 탭에서 다음 설정을 지정합니다:

    - 감염 및 기타 탐지된 개체에 수행할 동작을 선택합니다:

      - **알림**
      - **차단**
      - **추가 작업 수행**
        드롭다운 목록에서 동작을 선택합니다:

        - **치료**
        - **치료 - 불가능한 경우 삭제**
        - **삭제**
        - **권장**

- 탐지한 개체 유형에 따라 개체에 수행할 동작을 구성합니다:

  a. **선택한 개체 유형에 동작 적용** 확인란을 선택 해제하거나 선택합니다.

  b. **설정** 버튼을 클릭하고 탐지할 개체의 유형을 선택합니다.

- 수정할 수 없는 복합 파일에 대한 동작을 구성합니다. **내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거** 확인란을 선택 해제하거나 선택합니다.

11. **최적화** 탭에서 다음 설정을 지정합니다:

- **다음보다 큰 복합 파일을 백그라운드에서 압축 해제(MB)**
- **검사 시간이 다음을 초과하면 검사 중지(초)**
- **다음을 초과하는 복합 파일은 검사하지 않음(MB)**
- **iSwift 기술 사용**
- **iChecker 기술 사용**

12. 새 보안 설정을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 직접 보안 설정을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호** → **실시간 파일 보호** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. **보호 범위** 탭을 선택합니다.
6. 다음 중 하나를 수행합니다:

   - **추가** 버튼을 클릭해 새 규칙을 추가하고 이에 대한 보안 설정을 지정합니다.
   - 기존 규칙을 선택하고 **편집** 버튼을 클릭합니다.

   범위 편집 창이 열립니다.
7. 토글 스위치를 **활성**으로 설정합니다.
8. 보안 레벨을 선택하고 필요에 따라 보안 설정을 지정합니다.

9. **개체 보호 모드** 섹션에서 검사 범위에 포함할 개체 유형을 지정합니다:

   - 보호 범위에 포함해야 하는 개체:

     - **모든 개체**. Kaspersky Industrial CyberSecurity for Nodes가 모든 개체를 검사합니다.

     - **형식에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 형식을 기준으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 형식 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.

     - **안티 바이러스 데이터베이스에 지정된 확장자 목록으로 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 확장자 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.

     - **지정된 확장자 목록에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. 확장자 목록은 사용자가 직접 지정합니다.

10. **최적화** 섹션에서 **새로운 파일과 수정된 파일만 보호** 확인란을 선택하거나 선택 해제합니다.

11. **복합 개체 보호** 섹션에서 검사 범위에 포함할 복합 개체를 지정합니다:

    - **압축파일 검사**
    - **배포 패키지 검사**
    - **Microsoft Office 형식 파일 검사**
    - **이메일 형식 파일 검사**

12. 감염 및 기타 탐지된 개체에 수행할 동작을 선택합니다:

    - **알림**
    - **차단**
    - **추가 작업 수행**
      드롭다운 목록에서 동작을 선택합니다:

      - **치료**
      - **치료 - 불가능한 경우 삭제**
      - **삭제**
      - **권장**

13. 탐지한 개체 유형에 따라 개체에 수행할 동작을 구성합니다:

    a. **선택한 개체 유형에 동작 적용** 확인란을 선택 해제하거나 선택합니다.

    b. 이 확인란이 선택되어 있으면 **설정**을 클릭해 탐지할 개체의 유형을 선택합니다.

14. 수정할 수 없는 복합 파일에 대한 동작을 구성합니다. **내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거** 확인란을 선택 해제하거나 선택합니다.

15. **최적화** 섹션에서 다음 설정을 구성할 수 있습니다.

- **백그라운드에서 복합 파일 압축 해제**
- **검사 시간이 다음을 초과하면 검사 중지(초)**
- **다음을 초과하는 복합 파일은 검사하지 않음(MB)**
- **iSwift 기술 사용**
- **iChecker 기술 사용**

16. 새 보안 설정을 저장합니다.

애플리케이션 콘솔에서 직접 보안 설정을 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호** → **실시간 파일 보호** 옵션을 선택합니다.
2. **실시간 파일 보호** 노드의 결과 창에서 **보호 범위 구성** 버튼을 클릭합니다.
   속성: 실시간 파일 보호 창이 열립니다.
3. 보안 설정을 구성할 리소스를 선택합니다.
4. **구성** 버튼을 클릭합니다.
5. 창이 열리면 필요한 보안 레벨을 선택하고 **설정** 버튼을 클릭합니다.
6. **일반** 탭에서 다음 설정을 지정합니다:
   - 보호 범위에 포함해야 하는 개체:
     - **모든 개체**. Kaspersky Industrial CyberSecurity for Nodes가 모든 개체를 검사합니다.
     - **형식에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 형식을 기준으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 형식 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
     - **안티 바이러스 데이터베이스에 지정된 확장자 목록으로 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 확장자 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
     - **지정된 확장자 목록에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. 확장자 목록은 사용자가 직접 지정합니다.
   - **최적화** 블록에서 **새로운 파일과 수정된 파일만 보호** 확인란을 선택하거나 선택 해제합니다.
   - **복합 파일 검사** 섹션에서 검사 범위에 포함할 복합 개체를 지정합니다:
     - **압축파일 검사**. ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE 및 다른 압축 파일 검사. 애플리케이션은 확장자뿐만 아니라 형식으로도 압축 파일을 검사합니다. 압축 파일을 확인할 때 애플리케이션은 재귀 압축 해제를 수행합니다. 이로 인해 다중 구조 압축 파일(압축 파일 내 압축 파일) 내에서 위협을 탐지할 수 있습니다.
     - **배포 패키지 검사**. 이 확인란은 타사 애플리케이션 배포 패키지 검사를 작동 또는 중지합니다.

- **Microsoft Office 형식 파일 검사**. Microsoft Office 파일(DOC, DOCX, XLS, PPT 및 기타 Microsoft 확장자)을 검사합니다. Office 형식 파일에는 OLE 개체도 포함됩니다. Kaspersky Industrial CyberSecurity for Nodes는 확인란 선택 여부와 관계없이 1MB보다 작은 오피스 형식 파일을 검사합니다.

- **이메일 형식 파일 검사**.

7. **동작** 탭에서 다음 설정을 지정합니다:

- 감염 및 기타 탐지된 개체에 수행할 동작을 선택합니다:

  - **알림**

  - **차단**

  - **추가 작업 수행**.
    드롭다운 목록에서 동작을 선택합니다:

    - **치료**

    - **치료 - 불가능한 경우 삭제**

    - **삭제**

    - **권장**

- 탐지한 개체 유형에 따라 개체에 수행할 동작을 구성합니다:

  a. **선택한 개체 유형에 동작 적용** 확인란을 선택 해제하거나 선택합니다.

  b. **설정** 버튼을 클릭하고 탐지할 개체의 유형을 선택합니다.

- 수정할 수 없는 복합 파일에 대한 동작을 구성합니다. **내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거** 확인란을 선택 해제하거나 선택합니다.

8. **최적화** 탭에서 다음 설정을 지정합니다:

- **다음보다 큰 복합 파일을 백그라운드에서 압축 해제(MB)**

- **검사 시간이 다음을 초과하면 검사 중지(초)**

- **다음을 초과하는 복합 파일은 검사하지 않음(MB)**

- **iSwift 기술 사용**

- **iChecker 기술 사용**

9. 새 보안 설정을 저장합니다.

컨테이너 검사

*컨테이너*는 운영 체제와 직접 상호 작용하지 않고 애플리케이션을 실행할 수 있는 격리된 환경입니다. 컨테이너를 사용하면 다음과 같은 위험이 따릅니다.

- 해커가 컨테이너화 취약점을 악용하여 컨테이너 내의 애플리케이션을 침해할 수 있습니다.
- 해커는 컨테이너 환경의 안전하지 않은 구성을 악용하여 컴퓨터의 데이터에 무단으로 접근하거나 시스템의 무결성을 손상할 수 있습니다.
- 컨테이너에 대한 공격이 성공하면 해커가 컴퓨터의 데이터에 접근할 수 있습니다.
- 해커가 네트워크 취약점을 악용하여 네트워크 트래픽을 가로챌 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 컨테이너 내의 악성 활동을 탐지하기 위한 외부 도구입니다. 이를 통해 컨테이너의 성능을 유지하고 컨테이너 내의 다른 애플리케이션과의 충돌을 방지할 수 있습니다. 컨테이너 내에 Kaspersky Industrial CyberSecurity for Nodes 설치는 지원하지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes는 컨테이너 보안 외에도 애플리케이션 실행 제어 구성 요소를 사용한 컨테이너 내부 애플리케이션 관리 기능도 제공합니다. 애플리케이션 실행 제어 구성 요소는 컴퓨터에 설치된 애플리케이션에 대해 구성되는 것과 동일한 방식으로 컨테이너에 대해 구성됩니다. 시스템 무결성 모니터링 구성 요소는 컨테이너도 지원합니다.

컨테이너 요구 사항

- 컨테이너가 Docker 컨테이너여야 합니다. 다른 컨테이너화 도구는 지원하지 않습니다.
- 컨테이너를 프로세스 격리 모드에서 실행해야 합니다. Hyper-V 격리 모드는 지원하지 않습니다.
- 컨테이너가 Windows Server 2016, 2019 또는 2022 서버(Docker Host)에 배치되어야 합니다.
- 컨테이너가 Windows 이미지(Docker Image)를 포함해야 합니다. Windows 10 및 11은 지원하지 않습니다. Linux 이미지는 지원하지 않습니다.
- WSL2에서 실행 중인 컨테이너 검사 – Windows Subsystem for Linux v2 (Docker Wine) 모드는 지원하지 않습니다.

위협 탐지 시 처리 방법

컨테이너 내부에서 위협이 탐지되면 애플리케이션은 실시간 파일 보호 구성 요소에 대해 선택된 동작을 적용합니다. 컨테이너 검사에는 추가 설정이 있습니다(아래 지침 참조). 위협이 탐지되면 애플리케이션은 악성 활동을 차단하고 선택한 작업(예: 개체 치료 시도)을 수행합니다. Kaspersky Industrial CyberSecurity for Nodes는 탐지된 개체 치료에 실패 시 컨테이너를 중지할 수 있습니다. 컨테이너 중지는 기본적으로 활성화됩니다.

Kaspersky Security Center 관리 콘솔에서 컨테이너 검사를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.
4. **실시간 파일 보호** 섹션에서 **설정** 버튼을 클릭합니다.
5. **Windows 컨테이너에서 실행되는 파일 동작 검사** 블록에서 검사 설정을 구성합니다:
   - **치료가 실패하면 컨테이너 중지**. 애플리케이션이 탐지된 개체에 대해 충분한 읽기 및 쓰기 권한을 가지고 있지 않을 수 있습니다. 이때는 탐지된 개체를 치료하거나 삭제할 수 없습니다. 이 확인란을 선택하면 애플리케이션이 탐지된 개체를 차단하고 컨테이너를 중지합니다. 이 확인란을 선택하지 않으면 애플리케이션이 탐지된 개체만 차단합니다.
   - **Windows 컨테이너에서 실행되는 파일 동작 검사 안 함**. 이 확인란을 선택하면 애플리케이션이 컨테이너가 시작될 때만 컨테이너를 검사합니다. 이 확인란을 선택하지 않으면 애플리케이션이 실시간으로 계속 컨테이너를 검사합니다.
6. 새 보안 설정을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 컨테이너 검사를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호** → **실시간 파일 보호** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. **Windows 컨테이너에서 실행되는 파일 동작 검사** 블록에서 검사 설정을 구성합니다:
   - **치료가 실패하면 컨테이너 중지**. 애플리케이션이 탐지된 개체에 대해 충분한 읽기 및 쓰기 권한을 가지고 있지 않을 수 있습니다. 이때는 탐지된 개체를 치료하거나 삭제할 수 없습니다. 이 확인란을 선택하면 애플리케이션이 탐지된 개체를 차단하고 컨테이너를 중지합니다. 이 확인란을 선택하지 않으면 애플리케이션이 탐지된 개체만 차단합니다.
   - **Windows 컨테이너에서 실행되는 파일 동작 검사 안 함**. 이 확인란을 선택하면 애플리케이션이 컨테이너가 시작될 때만 컨테이너를 검사합니다. 이 확인란을 선택하지 않으면 애플리케이션이 실시간으로 계속 컨테이너를 검사합니다.
6. 새 보안 설정을 저장합니다.

애플리케이션 콘솔에서 컨테이너 검사를 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호** → **실시간 파일 보호** 옵션을 선택합니다.
2. **실시간 파일 보호** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 실시간 파일 보호 창이 열립니다.

3. **Windows 컨테이너에서 실행되는 파일 동작 검사** 블록에서 검사 설정을 구성합니다:

- **치료가 실패하면 컨테이너 중지**. 애플리케이션이 탐지된 개체에 대해 충분한 읽기 및 쓰기 권한을 가지고 있지 않을 수 있습니다. 이때는 탐지된 개체를 치료하거나 삭제할 수 없습니다. 이 확인란을 선택하면 애플리케이션이 탐지된 개체를 차단하고 컨테이너를 중지합니다. 이 확인란을 선택하지 않으면 애플리케이션이 탐지된 개체만 차단합니다.

- **Windows 컨테이너에서 실행되는 파일 동작 검사 안 함**. 이 확인란을 선택하면 애플리케이션이 컨테이너가 시작될 때만 컨테이너를 검사합니다. 이 확인란을 선택하지 않으면 애플리케이션이 실시간으로 계속 컨테이너를 검사합니다.

4. 변경 사항을 저장합니다.

KSN 사용

Kaspersky Industrial CyberSecurity for Nodes는 사용자 컴퓨터를 보다 효과적으로 보호하기 위해 전 세계 사용자에게 수신한 데이터를 사용합니다. Kaspersky Security Network는 이러한 사용자 데이터를 수집하기 위한 네트워크입니다.

미국 내 소프트웨어에서 KSN 기능이 제공되지 않을 수도 있습니다.

*Kaspersky Security Network(KSN)*는 파일, 웹사이트 및 소프트웨어에 대한 정보가 포함된 Kaspersky의 온라인 기술 자료에 접속할 수 있는 클라우드 서비스 인프라입니다. Kaspersky Security Network의 데이터를 사용하면 Kaspersky Industrial CyberSecurity for Nodes에서 새로운 위협에 대해 신속하게 대응할 수 있으며, 일부 보호 구성 요소의 성능이 향상되고 정상적인 개체를 바이러스로 탐지하는 가능성을 줄입니다. Kaspersky Security Network에 참여하는 경우, KSN 서비스를 통해 Kaspersky Industrial CyberSecurity for Nodes는 검사한 웹 주소의 평판 정보는 물론이고 검사한 파일의 카테고리 및 평판에 관한 정보도 수신하게 됩니다. KSN 액세스 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Security Network 사용은 사용자의 의사에 따라 결정합니다. 애플리케이션 초기 구성 시 KSN을 사용하라는 메시지가 표시됩니다. 사용자는 아무 때나 KSN 참가를 시작 또는 중단할 수 있습니다.

KSN에 참여하는 동안 생성된 Kaspersky 통계 정보의 전송 및 그러한 정보의 보관 및 파기에 대한 자세한 내용은 Kaspersky Security Network 진술문을 검토하거나 Kaspersky 웹사이트에서 확인하십시오. Kaspersky Security Network 진술문인 ksn_ <언어 ID>.txt 파일은 애플리케이션 배포 키트에 포함되어 있습니다.

Kaspersky 평판 데이터베이스의 인프라

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky 평판 데이터베이스 작업을 위해 다음과 같은 인프라 솔루션을 지원합니다.

- *Kaspersky Security Network(KSN)*은 대부분의 Kaspersky 애플리케이션에서 사용하는 솔루션입니다. KSN 참여자는 Kaspersky로부터 정보를 수신하며, Kaspersky 분석가의 추가 분석이 필요하고 평판 및 통계 데이터베이스에 포함해야 하는 사용자 컴퓨터에서 탐지된 개체에 관한 Kaspersky 정보를 전송합니다.
- *Kaspersky Private Security Network(KPSN)*는 Kaspersky Industrial CyberSecurity for Nodes 또는 기타 Kaspersky 애플리케이션을 호스팅하는 컴퓨터의 사용자가 자신의 컴퓨터에서 Kaspersky로 데이터를 보내지 않고도 Kaspersky 평판 데이터베이스 및 기타 통계 데이터에 접근할 수 있게 해주는 솔루션입니다. KPSN은 다음과 같은 이유로 Kaspersky Security Network에 참여할 수 없는 기업 고객용으로 제공됩니다:
  - 로컬 워크스테이션이 인터넷에 연결되어 있지 않습니다.
  - 국외 또는 기업 LAN 외부로의 데이터 전송이 법률이나 기업 보안 정책에 의해 금지되어 있습니다.

Kaspersky Security Network 사용 활성화

Kaspersky Security Center 관리 콘솔에서 Kaspersky Security Network 사용을 활성화하는 방법

1. Kaspersky Security Network 관리 콘솔 트리에서 **정책** 폴더를 선택합니다.
2. 필요한 Kaspersky Industrial CyberSecurity for Nodes 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 열린 창의 섹션 목록에서 **실시간 컴퓨터 보호 → KSN 사용** 옵션을 선택합니다.
4. **설정** 버튼을 클릭합니다.
5. **Kaspersky Security Network** 확인란을 선택하여 구성 요소를 활성화합니다.

   KSN을 사용한다면 Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky Security Network 진술문을 표시합니다. Kaspersky Security Network(KSN) 진술문 약관을 읽어 보고, 동의한다면 수락하십시오.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Network의 확장 모드를 사용합니다. 확장 Kaspersky Security Network 모드는 Kaspersky Industrial CyberSecurity for Nodes가 추가 데이터를 Kaspersky로 전송하는 모드입니다.
6. 필요하다면 **확장 KSN 모드 사용** 확인란을 선택 해제합니다.
7. 변경 사항을 저장합니다.

Kaspersky Security Network 사용이 활성화된 경우, Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Network에서 받은 파일과 웹 리소스, 애플리케이션의 평판 정보를 사용합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 Kaspersky Security Network 사용을 활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호** 노드를 확장합니다.
2. **Kaspersky Security Network** 하위 노드를 선택합니다.
3. 메인 애플리케이션 창에서 **속성** 옵션을 클릭합니다.
4. **Kaspersky Security Network** 확인란을 선택하여 구성 요소를 활성화합니다.

   KSN을 사용한다면 Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky Security Network 진술문을 표시합니다. Kaspersky Security Network(KSN) 진술문 약관을 읽어 보고, 동의한다면 수락하십시오.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Network의 확장 모드를 사용합니다. 확장 Kaspersky Security Network 모드는 Kaspersky Industrial CyberSecurity for Nodes가 추가 데이터를 Kaspersky로 전송하는 모드입니다.
5. 필요하다면 **확장 KSN 모드 사용** 확인란을 선택 해제합니다.
6. 변경 사항을 저장합니다.

Kaspersky Security Network 사용이 활성화된 경우, Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Network에서 받은 파일과 웹 리소스, 애플리케이션의 평판 정보를 사용합니다.

Kaspersky Security Center 웹 콘솔에서 Kaspersky Security Network 사용을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호 → KSN 사용** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. 표시된 창에서 **Kaspersky Security Network 사용** 확인란을 선택하여 구성 요소를 활성화합니다.
   KSN을 사용한다면 Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky Security Network 진술문을 표시합니다. 동의한다면 Kaspersky Security Network 사용 약관에 동의합니다.
   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Network의 확장 모드를 사용합니다. 확장 Kaspersky Security Network 모드는 Kaspersky Industrial CyberSecurity for Nodes가 추가 데이터를 Kaspersky로 전송하는 모드입니다.
6. 필요하다면 **확장 KSN 모드 사용** 확인란을 선택 해제합니다.
7. 변경 사항을 저장합니다.

그 결과 Kaspersky Security Network 사용을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky Security Network에서 받은 파일, 웹 리소스, 애플리케이션의 평판 정보를 사용합니다.

Kaspersky Security Network 사용 통계

KSN 사용 작업이 실행 중인 동안 작업이 시작된 순간부터 지금까지 Kaspersky Industrial CyberSecurity for Nodes가 처리한 개체 수에 대한 실시간 정보를 볼 수 있습니다.

KSN 사용 통계를 보려면:

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호** 섹션을 선택합니다.
2. **Kaspersky Security Network** 하위 노드를 선택합니다.
   결과 창의 **통계** 섹션에 작업 통계가 표시됩니다(아래 표 참조).

KSN 통계

필드	설명
파일 요청 전송됨	Kaspersky Industrial CyberSecurity for Nodes가 KSN에 전송한 개체 평판 쿼리의 수입니다.
KSN에서 신뢰하지 않는 파일	KSN이 할당한 신뢰할 수 없는 평판이 있는 개체의 수입니다.
요청 전송 오류	오류와 함께 처리된 KSN 요청 수입니다.
통계 형성됨	KSN에 전송된 생성된 통계 패키지의 수입니다.
삭제된 개체	Kaspersky Industrial CyberSecurity for Nodes가 삭제한 개체의 수입니다.
삭제되지 않은 개체	다른 애플리케이션의 개체 접근 차단 등의 이유로 Kaspersky Industrial CyberSecurity for Nodes의 삭제 시도가 실패한 개체 수입니다.
백업으로 이동됨	Kaspersky Industrial CyberSecurity for Nodes가 백업에 복사한 개체 수입니다.

필드	설명
백업으로 이동되지 않은 개체	Kaspersky Industrial CyberSecurity for Nodes가 디스크 공간 부족 등의 이유로 백업에 복사하지 못한 개체 수입니다. 애플리케이션은 백업으로 이동할 수 없는 파일을 치료하거나 삭제하지 않습니다.
제한된 모드	상태는 애플리케이션이 제한 모드에서 파일 평판 요청을 보낼지 여부를 나타냅니다. 제한 모드에서 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky 전문가 권장 사항에 따라 파일 평판 요청의 일부만 전송합니다.

삭제된 개체, **삭제되지 않은 개체**, **백업으로 이동됨**, **백업으로 이동되지 않은 개체** 필드의 값은 실시간 파일 보호 구성 요소의 통계에서 생성됩니다.

Kaspersky Private Security Network의 제한 사항

*Kaspersky Private Security Network(KPSN)*는 Kaspersky Industrial CyberSecurity for Nodes 또는 기타 Kaspersky 애플리케이션을 호스팅하는 컴퓨터의 사용자가 자신의 컴퓨터에서 Kaspersky로 데이터를 보내지 않고도 Kaspersky 평판 데이터베이스 및 기타 통계 데이터에 접근할 수 있게 해주는 솔루션입니다. Kaspersky Private Security Network을 사용하면 자체 로컬 평판 데이터베이스를 사용하여 개체(파일 또는 웹 주소)의 평판을 확인할 수 있습니다. 로컬 평판 데이터베이스에 추가된 개체의 평판은 KSN/KPSN에 추가된 것보다 우선순위가 높습니다. 예를 들어 Kaspersky Industrial CyberSecurity for Nodes가 컴퓨터를 검사하고 KSN/KPSN에 있는 파일의 평판을 요청한다고 가정해 봅시다. 파일의 평판이 로컬 평판 데이터베이스에서는 *신뢰하지 않음*지만 KSN/KPSN에서는 *신뢰함*라면, Kaspersky Industrial CyberSecurity for Nodes는 파일을 *신뢰하지 않음*로 탐지하고 탐지된 위협에 대해 정의된 동작을 수행합니다.

그러나 경우에 따라 Kaspersky Industrial CyberSecurity for Nodes가 KSN/KPSN에 있는 개체의 평판을 요청하지 않을 수 있습니다. 이 경우 Kaspersky Industrial CyberSecurity for Nodes는 KPSN의 로컬 평판 데이터베이스에서 데이터를 수신하지 않습니다. Kaspersky Industrial CyberSecurity for Nodes는 다음과 같은 이유로 KSN/KPSN에 있는 개체의 평판을 요청하지 않을 수 있습니다:

- Kaspersky 애플리케이션이 오프라인 평판 데이터베이스를 사용하고 있습니다. 오프라인 평판 데이터베이스는 Kaspersky 애플리케이션이 작동하는 동안 리소스를 최적화하고 컴퓨터에서 매우 중요한 개체를 보호하도록 설계되었습니다. 오프라인 평판 데이터베이스는 Kaspersky 전문가가 Kaspersky Security Network의 데이터를 기반으로 생성합니다. Kaspersky 애플리케이션은 특정 애플리케이션의 안티 바이러스 데이터베이스로 오프라인 평판 데이터베이스를 업데이트합니다. 오프라인 평판 데이터베이스에 검사 중인 개체에 대한 정보가 포함된 경우 애플리케이션이 KSN/KPSN에서 이 개체에 대한 평판을 요청하지 않습니다.

- 검사 예외(신뢰 구역)는 애플리케이션 설정에서 구성됩니다. 이 경우 애플리케이션은 로컬 평판 데이터베이스에 있는 개체의 평판을 고려하지 않습니다.

- 이 애플리케이션은 iSwift 또는 iChecker와 같은 검사 최적화 기술을 사용하거나 KSN/KPSN으로 평판 요청을 캐싱합니다. 이 경우 애플리케이션은 이전에 검사한 개체의 평판을 요청하지 않을 수 있습니다.

- 작업량을 최적화하기 위해 애플리케이션은 특정 형식과 크기의 파일을 검사합니다. 관련 형식 및 크기 제한 목록은 Kaspersky 전문가가 결정합니다. 이 목록은 애플리케이션의 안티 바이러스 데이터베이스로 업데이트합니다.

KSN 프록시 설정

Kaspersky Security Center 중앙 관리 서버가 관리하는 사용자 컴퓨터는 KSN 프록시 서비스를 통해 KSN과 통신할 수 있습니다.

KSN 프록시는 다음과 같은 기능을 제공합니다:

- 직접 인터넷을 통하지 않고 사용자의 컴퓨터에서 KSN으로 쿼리를 전송하고 정보를 제출합니다.
- KSN 프록시 서비스는 처리된 데이터를 캐시하므로 외부 네트워크 통신 채널의 부하를 줄이고 사용자의 컴퓨터에서 신속하게 요청한 정보를 받아볼 수 있습니다.

KSN을 활성화하고 KSN 진술문을 수락하면, 기본적으로 애플리케이션은 프록시 서버를 사용하여 Kaspersky Security Network에 연결합니다. 애플리케이션에서 사용하는 프록시 서버는 TCP 포트 13111을 통한 Kaspersky Security Center 중앙 관리 서버입니다. 따라서 KSN 프록시를 사용할 수 없다면 장치가 KSN 프록시 서버로 작동하는지 확인해야 합니다. 다음을 확인해야 합니다:

- *ksnproxy* 서비스가 중앙 관리 서버에서 실행 중입니다.
- 포트 13111이 컴퓨터의 방화벽에 차단되지 않았습니다.

KSN 프록시를 활성화 또는 비활성화하고 연결을 위한 포트를 구성하여 KSN 프록시 사용을 구성할 수 있습니다. 이렇게 하려면 중앙 관리 서버 속성을 열어야 합니다. KSN 프록시 구성에 대한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오. Kaspersky Industrial CyberSecurity for Nodes 정책에서 개별 컴퓨터에 대해 KSN 프록시를 활성화 또는 비활성화할 수도 있습니다.

Kaspersky Security Center 관리 콘솔에서 KSN Proxy를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 Kaspersky Industrial CyberSecurity for Nodes 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 열린 창의 섹션 목록에서 **실시간 컴퓨터 보호** → **KSN 사용**를 선택합니다.
4. **설정** 버튼을 클릭합니다.
5. **KSN 프록시 설정** 블록에서 **중앙 관리 서버를 KSN 프록시 서버로 사용** 확인란을 사용하여 KSN 프록시를 활성화하거나 비활성화합니다.
6. 필요하다면 **KSN 프록시 서버를 이용할 수 없는 경우 Kaspersky Security Network 서버 사용** 확인란을 선택합니다.

   이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 KSN 프록시 서비스를 사용할 수 없을 때 KSN 서버를 사용합니다. KSN 서버는 Kaspersky 서버 측과 타사 서버(Kaspersky Private Security Network 사용 시) 측 모두에 둘 수 있습니다.
7. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 KSN 프록시를 활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호** 노드를 확장합니다.
2. **Kaspersky Security Network** 하위 노드를 선택합니다.
3. 메인 애플리케이션 창에서 **속성** 옵션을 클릭합니다.
4. **KSN 프록시 설정** 블록에서 **중앙 관리 서버를 KSN 프록시 서버로 사용** 확인란을 사용하여 KSN 프록시를 활성화하거나 비활성화합니다.

5. 필요하다면 **KSN 프록시 서버를 이용할 수 없는 경우 Kaspersky Security Network 서버 사용** 확인란을 선택합니다.

   이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 KSN 프록시 서비스를 사용할 수 없을 때 KSN 서버를 사용합니다. KSN 서버는 Kaspersky 서버 측과 타사 서버(Kaspersky Private Security Network 사용 시) 측 모두에 둘 수 있습니다.

6. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 KSN 프록시를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **실시간 컴퓨터 보호** → **KSN 사용** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. **중앙 관리 서버를 KSN 프록시 서버로 사용** 확인란을 선택하거나 선택 해제하여 KSN 프록시를 활성화하거나 비활성화합니다.

6. 필요하다면 **KSN 프록시 서버를 이용할 수 없는 경우 Kaspersky Security Network 서버 사용** 확인란을 선택합니다.

   이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 KSN Proxy 서비스를 사용할 수 없을 때 KSN 서버를 사용합니다. KSN 서버는 Kaspersky 서버 측과 타사 서버(Kaspersky Private Security Network 사용 시) 측 모두에 둘 수 있습니다.

7. 변경 사항을 저장합니다.

KSN 프록시 주소는 중앙 관리 서버 주소와 일치합니다. 중앙 관리 서버 도메인 이름이 변경되면 KSN 프록시 주소를 직접 업데이트해야 합니다.

익스플로잇 방지

Kaspersky Industrial CyberSecurity for Nodes는 프로세스 메모리를 악용으로부터 보호하는 기능을 제공합니다. 이 기능은 익스플로잇 방지 구성 요소에서 구현하며, 이 구성 요소를 사용하여 구성 요소의 활동 상태를 변경하고 익스플로잇으로부터 프로세스 보호를 구성할 수 있습니다.

익스플로잇 방지 구성 요소는 컴퓨터의 취약점을 활용하여 관리자 권한을 악용하거나 악성 활동을 수행하는 프로그램 코드를 탐지합니다. 예를 들어 익스플로잇은 버퍼 오버플로우 공격을 활용할 수 있습니다. 이를 위해 익스플로잇은 다량의 데이터를 취약한 애플리케이션에 전송합니다. 취약한 애플리케이션은 이 데이터를 처리하는 과정에서 악성 코드를 실행하게 됩니다. 이 공격이 이루어지면 익스플로잇은 악성 코드를 무단으로 설치할 수 있습니다. 취약점이 있는 애플리케이션의 실행 파일을 무단으로 실행하려는 시도가 있으면 Kaspersky Industrial CyberSecurity for Nodes가 해당 파일의 실행을 차단하거나 해당 사용자에게 알립니다. 구성 요소는 보호 중인 프로세스에 외부 프로세스 보호 에이전트를 삽입하여 프로세스 메모리를 악용으로부터 보호합니다.

프로세스 보호 에이전트(이하 *에이전트*라고도 함)는 동적으로 로드된 Kaspersky Industrial CyberSecurity for Nodes 모듈로서 보호 중인 프로세스에 삽입되어 무결성을 모니터링하고 악용될 위험을 줄입니다.

에이전트가 보호 중인 프로세스 내에서 작동하려면 프로세스 시작 및 중지가 필요합니다. 보호 중인 프로세스 목록에 추가된 프로세스에 에이전트를 처음 로드하는 것은 프로세스가 다시 시작될 경우에만 가능합니다. 또한 프로세스가 보호 중인 프로세스 목록에서 제거 된 후에는 프로세스가 다시 시작된 후에만 에이전트를 언로드할 수 있습니다.

보호 중인 프로세스에서 에이전트를 언로드하려면 에이전트를 중지해야 합니다. 익스플로잇 방지 구성 요소가 제거되면 애플리케이션은 환경을 동결시키고 에이전트가 보호 중인 프로세스로부터 언로드되도록 강제합니다. 구성 요소를 제거하는 동안 에이전트가 보호 중인 프로세스에 삽입되면, 영향을 받는 프로세스를 종료해야 합니다. 보호 중인 장치를 다시 시작해야 할 수 있습니다(예: 시스템 프로세스를 보호하는 경우).

보호 중인 프로세스에서 악의적인 공격의 증거가 발견되면 Kaspersky Industrial CyberSecurity for Nodes는 다음 동작 중 하나를 수행합니다.

- 악의적인 시도가 있을 경우 프로세스를 종료합니다.
- 프로세스가 손상되었다는 사실을 보고합니다.

다음 방법 중 하나를 사용하여 프로세스 보호를 중지할 수 있습니다.

- 구성 요소 제거.
- 보호 중인 프로세스 목록에서 프로세스를 제거 및 프로세스 다시 시작.

익스플로잇 방지 모드

다음 모드 중 하나를 선택하여 보호 중인 프로세스에서 취약점 악용 위험을 줄이기 위한 동작을 구성할 수 있습니다.

- **차단**. 이 모드가 선택되면 Kaspersky Industrial CyberSecurity for Nodes는 프로세스에 충격 감소 기술이 적용된 경우 악용 시도를 감지하면 프로세스를 종료합니다.

  보호 중인 중요한 운영 체제 프로세스의 취약점을 악용하려는 시도를 감지하면, Kaspersky Industrial CyberSecurity for Nodes는 익스플로잇 방지 구성 요소 설정에 표시된 모드와 상관 없이 프로세스를 종료하지 않습니다.

- **알림**(Kaspersky Security Center 웹 콘솔에서 작업 시 – **알림**). 보안 로그의 이벤트를 사용하여 보호 중인 프로세스의 악용 사례에 대한 정보를 받으려면 이 모드를 적용합니다. 악용된 프로세스가 계속 실행됩니다.

  이 모드를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트를 생성하여 취약점을 악용하려는 모든 시도를 기록합니다. 기본적으로 선택됩니다.

익스플로잇 방지 사용 및 중지

Kaspersky Industrial CyberSecurity for Nodes로 취약한 애플리케이션이 실행 중인 실행 파일을 모니터링할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes가 취약한 애플리케이션의 실행 파일이 사용자 이외의 주체에 의해 실행된 것을 탐지하면 Kaspersky Industrial CyberSecurity for Nodes는 동작 차단 등 선택된 동작을 수행합니다.

Kaspersky Security Center 관리 콘솔에서 익스플로잇 방지를 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 Kaspersky Industrial CyberSecurity for Nodes 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 열린 창의 섹션 목록에서 **실시간 컴퓨터 보호** → **익스플로잇 방지** 옵션을 선택합니다.
4. **설정** 버튼을 클릭합니다.
5. **익스플로잇 방지** 확인란을 선택하여 구성 요소를 활성화합니다.
6. **일반** 탭에서 익스플로잇 방지 모드를 선택합니다: **차단** 또는 **알림**.
7. 필요하다면 **익스플로잇 방지** 확인란을 선택 해제하여 구성 요소를 비활성화합니다.
8. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 익스플로잇 방지를 활성화 또는 비활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호** 노드를 확장합니다.
2. **익스플로잇 방지** 하위 노드를 선택합니다.

3. 메인 애플리케이션 창에서 **속성** 옵션을 클릭합니다.
4. **익스플로잇 방지** 확인란을 선택하여 구성 요소를 활성화합니다.
5. **일반** 탭에서 익스플로잇 방지 모드를 선택합니다: **차단** 또는 **알림**.
6. 필요하다면 **익스플로잇 방지** 확인란을 선택 해제하여 구성 요소를 비활성화합니다.
7. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 익스플로잇 방지를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호** → **익스플로잇 방지** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. 창이 열리면 **익스플로잇 방지 모드**에서 **취약한 프로세스 익스플로잇 방지** 확인란을 선택하여 구성 요소를 활성화합니다.
6. 익스플로잇 방지 모드를 **차단** 또는 **알림**으로 선택합니다.
7. 필요하다면 **취약한 프로세스 익스플로잇 방지** 확인란을 선택 해제하여 구성 요소를 비활성화합니다.
8. 변경 사항을 저장합니다.

메모리 보호 활성화 및 비활성화

Kaspersky Industrial CyberSecurity for Nodes는 시스템 프로세스에 접근하려는 외부 프로세스의 시도를 차단합니다. 기본 값으로 시스템 프로세스 메모리 보호가 사용됩니다.

Kaspersky Security Center 관리 콘솔에서 메모리 보호를 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 Kaspersky Industrial CyberSecurity for Nodes 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 열린 창의 섹션 목록에서 **실시간 컴퓨터 보호** → **익스플로잇 방지** 옵션을 선택합니다.
4. **설정** 버튼을 클릭합니다.
5. **일반** 탭에서 **시스템 프로세스 메모리 보호 사용** 확인란을 선택합니다.
6. 필요하다면 **시스템 프로세스 메모리 보호 사용** 확인란을 선택 해제합니다.
7. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 메모리 보호를 활성화 또는 비활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호** 노드를 확장합니다.
2. **익스플로잇 방지** 하위 노드를 선택합니다.
3. 메인 애플리케이션 창에서 **속성** 옵션을 클릭합니다.
4. **일반** 탭에서 **시스템 프로세스 메모리 보호 사용** 확인란을 선택합니다.
5. 필요하다면 **시스템 프로세스 메모리 보호 사용** 확인란을 선택 해제합니다.
6. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 메모리 보호를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호 → 익스플로잇 방지** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. 열린 창의 **시스템 프로세스 메모리 보호** 블록에서 **시스템 프로세스 메모리 보호** 확인란을 클릭합니다.
6. 필요하다면 **시스템 프로세스 메모리 보호** 확인란을 선택 해제하여 시스템 프로세스 메모리 보호를 비활성화합니다.
7. 변경 사항을 저장합니다.

보호 중인 프로세스 목록 생성

기본적으로 익스플로잇 방지 구성 요소는 여러 프로세스를 보호합니다. 애플리케이션은 보호 프로세스 목록을 자동 생성할 수 있습니다. 프로세스를 직접 추가하거나 제거할 수도 있습니다.

Kaspersky Security Center 관리 콘솔에서 보호 프로세스 목록을 관리하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 Kaspersky Industrial CyberSecurity for Nodes 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 열린 창의 섹션 목록에서 **실시간 컴퓨터 보호 → 익스플로잇 방지** 옵션을 선택합니다.
4. **설정** 버튼을 클릭합니다.
5. **보호 중인 프로세스** 탭에서 다음 옵션 중 하나를 선택하여 프로세스 악성 코드 삽입을 방지합니다.
   - **보호 중인 프로세스 자동 탐지**. 이 옵션을 선택하면 애플리케이션이 보호 프로세스 목록을 자동 생성합니다.
   - **아래 목록의 프로세스만 보호**. 이 옵션을 선택하면 보호할 프로세스를 선택할 수 있습니다.

6. **아래 목록의 프로세스만 보호** 옵션을 선택했다면, 다음 중 하나를 수행하여 보호 프로세스 목록을 편집할 수 있습니다:

   - 필요하다면 **추가** 버튼을 클릭하고 보호 중인 프로세스 목록에 추가할 프로세스를 선택합니다.
   - 생성한 보호 프로세스 목록에서 프로세스를 삭제하려면 목록에서 프로세스를 선택하고 **삭제** 버튼을 클릭합니다.

     삭제 버튼은 목록에서 프로세스를 하나 이상 선택하면 활성화됩니다.

7. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔을 사용하여 보호 프로세스 목록을 관리하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호** 노드를 확장합니다.
2. **익스플로잇 방지** 하위 노드를 선택합니다.
3. 메인 애플리케이션 창에서 **속성** 옵션을 클릭합니다.
4. **보호 중인 프로세스** 탭에서 다음 옵션 중 하나를 선택하여 프로세스 악성 코드 삽입을 방지합니다.

   - **보호 중인 프로세스 자동 탐지**. 이 옵션을 선택하면 애플리케이션이 보호 프로세스 목록을 자동 생성합니다.
   - **아래 목록의 프로세스만 보호**. 이 옵션을 선택하면 보호할 프로세스를 선택할 수 있습니다.

5. **아래 목록의 프로세스만 보호** 옵션을 선택했다면, 다음 중 하나를 수행하여 보호 프로세스 목록을 편집할 수 있습니다:

   - 필요하다면 **추가** 버튼을 클릭하고 보호 중인 프로세스 목록에 추가할 프로세스를 선택합니다.
   - 생성한 보호 프로세스 목록에서 프로세스를 삭제하려면 목록에서 프로세스를 선택하고 **삭제** 버튼을 클릭합니다.

     삭제 버튼은 목록에서 프로세스를 하나 이상 선택하면 활성화됩니다.

6. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 보호 프로세스 목록을 관리하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호** → **익스플로잇 방지** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. **보호 중인 프로세스 목록**에서 다음 옵션 중 하나를 선택해 프로세스 악성 코드 삽입을 방지합니다.

   - **보호 중인 프로세스 자동 탐지**. 이 옵션을 선택하면 애플리케이션이 보호 프로세스 목록을 자동 생성합니다.
   - **아래 목록의 프로세스만 보호**. 이 옵션을 선택하면 보호할 프로세스를 추가, 편집, 제거할 수 있습니다.

6. **아래 목록의 프로세스만 보호** 옵션을 선택했다면, 다음 중 하나를 수행합니다.

- **추가** 버튼을 클릭해 **보호 중인 프로세스** 창을 열고 해당 창에서:

  a. **보호 중인 프로세스** 확인란을 선택합니다.

  b. **프로세스 이름** 필드에서 프로세스 이름을 입력합니다.

  c. 변경 사항을 저장합니다.

- 필요하다면 보호 프로세스 목록에서 프로세스 설정을 편집합니다. 이를 위해서는 다음 동작을 수행합니다.

  a. 보호 중인 프로세스 목록에 프로세스를 추가하려면:

  b. **편집** 버튼을 클릭합니다. **편집** 버튼은 목록에서 프로세스를 하나 이상 선택하면 활성화됩니다.

  c. **보호 중인 프로세스** 창에서 **보호 중인 프로세스** 확인란을 선택하거나 선택 해제합니다.

  d. 필요하다면 **프로세스 이름** 필드에서 프로세스 이름을 편집합니다.

  e. 변경 사항을 저장합니다.

- 필요하다면 보호 프로세스 목록에서 프로세스를 제거할 수 있습니다. 이를 위해서는 다음 동작을 수행합니다.

  a. 보호 중인 프로세스 목록에서 프로세스를 하나 이상 선택합니다.

  b. **삭제** 버튼을 클릭합니다. **삭제** 버튼은 목록에서 프로세스를 하나 이상 선택하면 활성화됩니다.

7. 변경 사항을 저장합니다.

복원 엔진

복원 엔진을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 운영 체제에서 악성 코드에 의해 수행된 활동을 롤백합니다.

Kaspersky Industrial CyberSecurity for Nodes는 운영 체제에서 악성 코드가 수행한 동작을 롤백할 때 다음 동작을 수행합니다.

- **파일 활동**
  - 네트워크 드라이브를 제외한 모든 미디어에서 악성 코드에 의해 생성된 실행 파일을 삭제합니다.
  - 악성 코드에 의해 침입된 프로그램이 생성한 실행 파일을 삭제합니다.
  - 악성 코드에 의해 수정되거나 삭제된 파일을 복원합니다.

  파일 복구 기능에는 **여러 가지 제한**이 있습니다.

  - 애플리케이션은 NTFS 또는 FAT32 파일 시스템을 사용하는 장치에서만 파일을 복원합니다.
  - 애플리케이션은 다음 확장명을 가진 파일을 복원할 수 있습니다: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
  - 네트워크 드라이브 또는 다시 쓰기 가능한 CD/DVD 디스크에 있는 파일을 복원할 수 없습니다.
  - EFS(암호화 파일 시스템)로 암호화된 파일은 복원할 수 없습니다. EFS 동작에 대한 자세한 내용은 Microsoft 웹사이트를 방문하시기 바랍니다.
  - 애플리케이션은 운영 체제 커널 레벨에서 프로세스에 의해 수행된 파일의 변경 사항을 모니터링하지 않습니다.
  - 애플리케이션은 네트워크 인터페이스를 통한 파일의 변경 사항을 모니터링하지 않습니다(예: 파일이 공유 폴더에 있고 프로세스가 다른 컴퓨터에서 원격으로 시작되는 경우).
- **레지스트리 활동**
  - 악성 코드에서 생성한 레지스트리 키를 삭제합니다.

  Kaspersky Industrial CyberSecurity for Nodes는 악성 코드에서 변경하거나 삭제한 레지스트리 키는 복원하지 않습니다.
- **시스템 활동**
  - 악성 코드에 의해 시작된 프로세스를 종료합니다.
  - 악성 애플리케이션이 침투한 프로세스를 종료합니다.

  Kaspersky Industrial CyberSecurity for Nodes는 악성 코드에 의해 중지된 프로세스는 재시작하지 않습니다.

- **네트워크 활동**
  - 악성 코드의 네트워크 활동을 차단합니다.
  - 악성 코드가 침투한 프로세스의 네트워크 활동을 차단합니다.

악성 애플리케이션 동작의 롤백은 실시간 파일 보호 구성 요소가 시작하거나 온디맨드 검사 중에 시작됩니다.

악성 코드 활동을 롤백하면 엄격하게 정의된 데이터 집합에는 영향을 줍니다. 롤백은 운영 체제 또는 컴퓨터 데이터의 무결성에는 악영향이 없습니다.

Kaspersky Security Center 관리 콘솔에서 복원 엔진 구성 요소를 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 섹션으로 갑니다.
4. **복원 엔진** 블록에서 **설정** 버튼을 클릭합니다.
5. **일반** 탭에서 **복원 엔진** 창이 열립니다.
6. 다음 중 하나를 수행합니다:
   - 복원 엔진 구성 요소를 활성화하려면 **복원 엔진** 확인란을 선택합니다.
   - 복원 엔진 구성 요소를 비활성화하려면 **복원 엔진** 확인란을 선택 해제합니다.
7. **복원 엔진** 창의 **확인** 버튼을 클릭합니다.
8. **속성: <정책 이름>** 창에서 **확인** 버튼을 클릭합니다.

Kaspersky Security Center 웹 콘솔에서 복원 엔진 구성 요소를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호** 섹션을 선택합니다.
5. **복원 엔진** 블록에서 **구성** 버튼을 클릭합니다.
6. **복원 엔진** 창이 열립니다.
7. 다음 중 하나를 수행합니다:
   - 복원 엔진 구성 요소를 활성화하려면 **복원 엔진** 확인란을 선택합니다.
   - 복원 엔진 구성 요소를 비활성화하려면 **복원 엔진** 확인란을 선택 해제합니다.

8. **복원 엔진** 창의 **확인** 버튼을 클릭합니다.

9. **<정책 이름>** 창의 **저장** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 복원 엔진 구성 요소를 활성화 또는 비활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호** → **복원 엔진** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.
   일반 탭에서 **복원 엔진** 창이 열립니다.

3. 다음 중 하나를 수행합니다:

   - 복원 엔진 구성 요소를 활성화하려면 **복원 엔진** 확인란을 선택합니다.
   - 복원 엔진 구성 요소를 비활성화하려면 **복원 엔진** 확인란을 선택 해제합니다.

4. **복원 엔진** 창의 **확인** 버튼을 클릭합니다.

Anti-Cryptor

Anti-Cryptor 구성 요소는 컴퓨터에서 애플리케이션의 동작에 대한 데이터를 수신한 후 이 정보를 다른 보호 구성 요소에 제공하여 성능을 개선합니다. Anti-Cryptor 구성 요소는 애플리케이션의 행동 스트림 서명(BSS)을 활용합니다. 애플리케이션 활동이 행동 스트림 서명과 일치할 경우 Kaspersky Industrial CyberSecurity for Nodes는 선택된 대응 조치를 수행합니다. 행동 스트림 서명을 바탕으로 한 Kaspersky Industrial CyberSecurity for Nodes 기능은 컴퓨터에 대한 사전 방역을 제공합니다.

로컬 폴더에 대한 암호화 보호 활성화 및 비활성화

Kaspersky Security Center 관리 콘솔에서 Anti-Cryptor를 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.
4. **Anti-Cryptor** 섹션에서 **설정** 옵션을 클릭합니다.
5. **Anti-Cryptor** 확인란으로 구성 요소를 사용하거나 중지합니다.
6. **일반** 탭으로 갑니다.
7. **외부 컴퓨터에서 시도하는 암호화로부터 로컬 폴더 보호 사용** 확인란으로 구성 요소를 사용하거나 중지합니다. 이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 아래 지정된 동작으로 악성 활동에 대응합니다.
8. **악성 코드 활동 탐지 시 처리 방법** 블록에서 필요한 동작을 선택합니다:
   - **삭제**. 이 항목을 선택하면 악성 코드 활동 탐지 시 Kaspersky Industrial CyberSecurity for Nodes가 악성 코드의 실행 파일을 삭제하고 백업 저장소에 백업 복사본을 생성합니다.
   - **차단**. 이 항목을 선택한 경우 Kaspersky Industrial CyberSecurity for Nodes는 악성 코드 활동 탐지 시 해당 애플리케이션을 종료합니다.
   - **알림**. 이 항목을 선택하고 애플리케이션의 악성코드 활동이 탐지되면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션의 악성 코드 활동에 대한 정보를 처리 안 된 위협 목록에 추가합니다.
9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 Anti-Cryptor를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.

4. **실시간 컴퓨터 보호** → **Anti-Cryptor** 섹션으로 가서 **구성** 버튼을 클릭합니다.

   Anti-Cryptor 창이 열립니다.

5. **Anti-Cryptor 사용** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.

6. **일반** 탭으로 갑니다.

7. **외부 컴퓨터에서 시도하는 암호화로부터 로컬 폴더 보호 사용** 확인란으로 구성 요소를 사용하거나 중지합니다. 이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 아래 지정된 동작으로 악성 활동에 대응합니다.

8. **공유 폴더에 대한 외부 컴퓨터에서의 암호화 시도 탐지 시** 블록에서 필요한 동작을 선택합니다:

   - **삭제**. 이 항목을 선택하면 악성 코드 활동 탐지 시 Kaspersky Industrial CyberSecurity for Nodes가 악성 코드의 실행 파일을 삭제하고 백업 저장소에 백업 복사본을 생성합니다.

   - **차단**. 이 항목을 선택한 경우 Kaspersky Industrial CyberSecurity for Nodes는 악성 코드 활동 탐지 시 해당 애플리케이션을 종료합니다.

   - **알림**. 이 항목을 선택하고 애플리케이션의 악성코드 활동이 탐지되면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션의 악성 코드 활동에 대한 정보를 처리 안 된 위협 목록에 추가합니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 Anti-Cryptor를 활성화 또는 비활성화하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호** → **Anti-Cryptor** 옵션을 선택합니다.

2. **Anti-Cryptor** 노드 결과 창에서 **속성**을 클릭합니다.

   속성: Anti-Cryptor 창이 열립니다.

3. **Anti-Cryptor** 확인란을 선택합니다.

4. **일반** 탭으로 갑니다.

5. **외부 컴퓨터에서 시도하는 암호화로부터 로컬 폴더 보호 사용** 확인란으로 구성 요소를 사용하거나 중지합니다. 이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 아래 지정된 동작으로 악성 활동에 대응합니다.

6. **공유 폴더에 대한 외부 컴퓨터에서의 암호화 시도 탐지 시** 블록에서 필요한 동작을 선택합니다:

   - **삭제**. 이 항목을 선택하면 악성 코드 활동 탐지 시 Kaspersky Industrial CyberSecurity for Nodes가 악성 코드의 실행 파일을 삭제하고 백업 저장소에 백업 복사본을 생성합니다.

   - **차단**. 이 항목을 선택한 경우 Kaspersky Industrial CyberSecurity for Nodes는 악성 코드 활동 탐지 시 해당 애플리케이션을 종료합니다.

   - **알림**. 이 항목을 선택하고 애플리케이션의 악성코드 활동이 탐지되면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션의 악성 코드 활동에 대한 정보를 처리 안 된 위협 목록에 추가합니다.

7. 변경 사항을 저장합니다.

외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호

이 구성 요소는 NTFS 파일 시스템을 사용하는 대용량 저장소에 저장되고 EFS로 암호화되지 않은 파일만을 사용하여 수행된 작업을 감시합니다.

외부 암호화로부터 공유 폴더를 보호하는 기능을 사용할 때는 공유 폴더의 활동을 분석할 수 있습니다. 이 활동이 외부 암호화에서 일반적으로 나타나는 행동 스트림 서명과 일치하면 Kaspersky Industrial CyberSecurity for Nodes가 선택한 동작을 수행합니다.

Kaspersky Industrial CyberSecurity for Nodes는 공유 폴더에서 파일 수정 시도가 탐지되면 다음 동작을 수행합니다.

- 악성 활동을 시작한 세션의 파일 수정 액세스를 차단합니다(파일이 읽기 전용이 됩니다).
- 수정되고 있는 파일에 대한 백업 사본을 만듭니다.
- 로컬 애플리케이션 인터페이스 리포트에 항목을 추가하고 탐지된 악성 활동에 대한 정보를 Kaspersky Security Center로 전송합니다.
- 또한 복원 엔진 구성 요소가 활성화되었다면, 수정된 파일이 백업 복사본에서 복원됩니다.

외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 사용 및 중지

기본적으로 외부 암호화로부터 공유 폴더를 보호하는 기능이 활성화되어 있으며 Kaspersky 전문가의 권장 사항에 따라 작동합니다. 이 기능을 구성하려면 보호 범위를 만들고 필요한 경우 예외 규칙을 구성할 수 있습니다. 기본적으로 애플리케이션은 공유 폴더를 자동으로 식별하고 모든 폴더의 파일 활동을 모니터링합니다. 공유 폴더 내의 파일 외부 암호화 시도가 탐지되면, Kaspersky Industrial CyberSecurity for Nodes가 1시간 동안 원격 사용자의 세션을 차단합니다(기본값).

Kaspersky Industrial CyberSecurity for Nodes가 설치된 후 외부 암호화로부터 공유 폴더 보호는 컴퓨터를 다시 시작하기 전까지 제한됩니다.

Kaspersky Security Center 관리 콘솔에서 외부 암호화로부터 공유 폴더 보호 기능을 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.
4. **Anti-Cryptor** 섹션에서 **설정** 옵션을 클릭합니다.
5. **Anti-Cryptor** 확인란으로 구성 요소를 사용하거나 중지합니다.
6. **공유 폴더 보호** 탭으로 갑니다.

7. **공유 폴더 보호** 확인란으로 구성 요소를 사용하거나 중지합니다.

8. **외부 암호화로부터 공유 폴더 보호** 블록에서 필요한 동작을 선택합니다:

   - **다음 시간 동안 연결 차단: N분**. 이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 공유 폴더의 파일 수정 시도 탐지 시, 악의적 행위를 시작한 세션의 파일 수정 접근 권한을 차단하고(읽기 전용) 수정된 파일의 백업 복사본을 생성합니다.

     > 복원 엔진 구성 요소를 활성화하고 **다음 시간 동안 연결 차단: N분** 옵션을 선택하면 수정된 파일을 백업 복사본에서 복원합니다.

   - **알림**. 이 옵션을 선택하면 공유 폴더의 파일 수정 시도 탐지 시 Kaspersky Industrial CyberSecurity for Nodes가 이 공유 폴더의 파일 수정 시도 정보를 처리 안 된 위협 목록에 추가하고, 로컬 인터페이스의 리포트에 기록을 추가하며, 악성 활동 탐지 정보를 Kaspersky Security Center로 보냅니다.

9. 필요하다면 보호 범위를 변경하고 예외를 정의합니다.

10. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 외부 암호화로부터 공유 폴더 보호 기능을 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **실시간 컴퓨터 보호** → **Anti-Cryptor** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   Anti-Cryptor 창이 열립니다.

5. **Anti-Cryptor 사용** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.

6. **공유 폴더 보호** 탭으로 갑니다.

7. **외부 암호화로부터 공유 폴더 보호 사용** 확인란으로 구성 요소를 사용하거나 중지합니다.

8. **외부 암호화 탐지** 블록에서 필요한 동작을 선택합니다:

   - **연결 차단**. 이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 공유 폴더의 파일 수정 시도 탐지 시, 악의적 행위를 시작한 세션의 파일 수정 접근 권한을 차단하고(읽기 전용) 수정된 파일의 백업 복사본을 생성합니다.

     > 복원 엔진 구성 요소를 활성화하고 **연결 차단** 옵션을 선택하면 수정된 파일을 백업 복사본에서 복원합니다.

   - **알림**. 이 옵션을 선택하면 공유 폴더의 파일 수정 시도 탐지 시 Kaspersky Industrial CyberSecurity for Nodes가 이 공유 폴더의 파일 수정 시도 정보를 처리 안 된 위협 목록에 추가하고, 로컬 인터페이스의 리포트에 기록을 추가하며, 악성 활동 탐지 정보를 Kaspersky Security Center로 보냅니다.

9. 필요하다면 보호 범위를 변경하고 예외를 정의합니다.

10. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 외부 암호화로부터 공유 폴더 보호 기능을 활성화 또는 비활성화하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호** → **Anti-Cryptor** 옵션을 선택합니다.

2. **Anti-Cryptor** 노드 결과 창에서 **속성**을 클릭합니다.

   속성: Anti-Cryptor 창이 열립니다.

3. **Anti-Cryptor** 확인란을 선택합니다.

4. **공유 폴더 보호** 탭으로 갑니다.

5. **공유 폴더 보호** 확인란으로 구성 요소를 사용하거나 중지합니다.

6. **외부 암호화로부터 공유 폴더 보호** 블록에서 필요한 동작을 선택합니다:

   - **다음 시간 동안 연결 차단: N분**. 이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 공유 폴더의 파일 수정 시도 탐지 시, 악의적 행위를 시작한 세션의 파일 수정 접근 권한을 차단하고(읽기 전용) 수정된 파일의 백업 복사본을 생성합니다.

     복원 엔진 구성 요소를 활성화하고 **다음 시간 동안 연결 차단: N분** 옵션을 선택하면 수정된 파일을 백업 복사본에서 복원합니다.

   - **알림**. 이 옵션을 선택하면 공유 폴더의 파일 수정 시도 탐지 시 Kaspersky Industrial CyberSecurity for Nodes가 이 공유 폴더의 파일 수정 시도 정보를 처리 안 된 위협 목록에 추가하고, 로컬 인터페이스의 리포트에 기록을 추가하며, 악성 활동 탐지 정보를 Kaspersky Security Center로 보냅니다.

7. 필요하다면 보호 범위를 변경하고 예외를 정의합니다.

8. 변경 사항을 저장합니다.

보호 범위 편집

*보호 범위*는 Kaspersky Industrial CyberSecurity for Nodes가 파일 활동을 감시하는 공유 폴더의 경로 목록입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크 입력 시 환경 변수와 `*` 및 `?` 문자를 지원합니다. 기본적으로 애플리케이션은 공유 폴더를 자동 식별하고 모든 폴더의 파일 활동을 모니터링합니다.

공유 폴더를 통해 파일을 교환할 때 데이터 암호화를 사용하는 조직에서는 보호 범위에서 폴더를 제외하면 오탐의 수를 줄일 수 있습니다. 예를 들어 사용자가 공유 폴더에서 ENC 확장자의 파일로 작업할 때, Anti-Cryptor 구성 요소가 오탐의 수를 늘릴 수 있습니다. 이러한 활동은 외부 암호화의 전형적인 행동 패턴과 일치합니다. 공유 폴더에서 데이터 보호를 위해 암호화한 파일이 있다면, 해당 폴더를 예외 규칙에 추가합니다.

컴퓨터에서 전송되는 외부 암호화 시도를 무시하려면 컴퓨터를 제외할 수도 있습니다.

Kaspersky Security Center 관리 콘솔에서 보호 범위 구성 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.
4. **Anti-Cryptor** 섹션에서 **설정** 옵션을 클릭합니다.
5. **Anti-Cryptor** 확인란으로 구성 요소를 사용하거나 중지합니다.
6. **공유 폴더 보호** 탭으로 갑니다.
7. **보호 범위** 블록에서 **구성** 버튼을 클릭합니다.
8. 창이 열리면 **지정된 공유 폴더만 해당** 모드를 선택합니다.
9. **추가** 버튼을 클릭합니다.
10. 그러면 창이 열립니다. 이 창에서 보호 범위에 포함할 공유 폴더의 경로를 입력합니다(예, `C:\Share`).

    > 공유 폴더를 보호 범위에 추가하려면 로컬 경로를 사용하십시오.

11. **확인** 버튼을 클릭합니다.
12. 필요한 경우 보호 범위 예외 규칙을 정의하십시오.
    a. **예외** 블록에서 **구성** 버튼을 클릭합니다.
    b. 열리는 창에서 **추가** 버튼을 클릭합니다.
    c. 창이 표시되면 폴더나 파일의 경로를 입력합니다.
    마스크 사용:

    - `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.
    - `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.
    - `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

    보호 범위의 개체 목록에서 개체를 삭제하지 않고도 보호 대상에서 개체를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.
13. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 보호 범위 구성 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호** → **Anti-Cryptor** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   Anti-Cryptor 창이 열립니다.
5. **Anti-Cryptor 사용** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.
6. **공유 폴더 보호** 탭으로 갑니다.
7. **보호 범위**에서 **지정된 공유 폴더만 해당** 모드를 선택합니다.
8. **추가** 버튼을 클릭합니다.
9. 그러면 창이 열립니다. 이 창에서 보호 범위에 포함할 공유 폴더의 경로를 입력합니다(예, `C:\Share`).

   > 공유 폴더를 보호 범위에 추가하려면 로컬 경로를 사용하십시오.

10. **확인** 버튼을 클릭합니다.
11. 필요한 경우 보호 범위 예외 규칙을 정의하십시오.

    a. **제외할 개체** 블록에서 **추가** 버튼을 클릭합니다.

    b. 창이 표시되면 폴더나 파일의 경로를 입력합니다.
    마스크 사용:

    - `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.
    - `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.
    - `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

    보호 범위의 개체 목록에서 개체를 삭제하지 않고도 보호 대상에서 개체를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.

12. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 보호 범위 구성 방법

1. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.
2. **Anti-Cryptor** 섹션에서 **설정** 옵션을 클릭합니다.
3. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호** → **Anti-Cryptor** 옵션을 선택합니다.
4. **Anti-Cryptor** 노드 결과 창에서 **속성**을 클릭합니다.
   속성: Anti-Cryptor 창이 열립니다.
5. **Anti-Cryptor** 확인란으로 구성 요소를 사용하거나 중지합니다.
6. **공유 폴더 보호** 탭으로 갑니다.
7. **보호 범위** 블록에서 **구성** 버튼을 클릭합니다.
8. 창이 열리면 **지정된 공유 폴더만 해당** 모드를 선택합니다.
9. **보호 범위** 블록에서 **추가** 버튼을 클릭합니다.
10. 그러면 창이 열립니다. 이 창에서 보호 범위에 포함할 공유 폴더의 경로를 입력합니다(예, `C:\Share`).

    > 공유 폴더를 보호 범위에 추가하려면 로컬 경로를 사용하십시오.

11. **확인** 버튼을 클릭합니다.
12. 필요한 경우 보호 범위 예외 규칙을 정의하십시오.
    a. **예외** 블록에서 **설정** 버튼을 클릭합니다.
    b. 표시된 **마스크로 예외 설정** 창에서 **추가** 버튼을 클릭합니다.
    c. 창이 표시되면 폴더나 파일의 경로를 입력합니다.
    마스크 사용:

    - `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.
    - `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다.
    - `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.

보호 범위의 개체 목록에서 개체를 삭제하지 않고도 보호 대상에서 개체를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.

13. 변경 사항을 저장합니다.

외부 데이터 암호화를 위해 신뢰하는 컴퓨터 추가

조직에서 파일 공유 과정에 외부 데이터 암호화를 사용하는 경우, 신뢰하는 컴퓨터 목록을 만들어야 합니다. Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 컴퓨터의 데이터 암호화를 모니터링하지 않습니다.

Windows XP 또는 Windows Server 2003을 실행하는 보호 대상 장치에서 Kaspersky Industrial CyberSecurity for Nodes는 원격 컴퓨터를 신뢰하는 컴퓨터 목록에 추가하더라도 공유 폴더 암호화 시도를 감시합니다.

외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 기능에서 주소로 제외하기 위해 로그온 감사 서비스를 사용해야 합니다. 기본적으로 로그온 감사 서비스는 비활성되어 있습니다(로그온 감사 서비스를 활성하는 방법에 대한 자세한 내용은 Microsoft 웹사이트를 방문하십시오).

공유 폴더 보호 시 특정 주소를 예외 처리하는 기능은 Kaspersky Industrial CyberSecurity for Nodes를 시작하기 전에 원격 컴퓨터가 꺼진 경우에는 원격 컴퓨터에서 작동하지 않습니다. Kaspersky Industrial CyberSecurity for Nodes가 시작된 후 이 원격 컴퓨터를 다시 시작하면 공유 폴더 보호 시 특정 주소를 예외 처리하는 기능이 이 원격 컴퓨터에서 작동하도록 할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 외부 데이터 암호화를 위해 신뢰하는 컴퓨터를 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.
4. **Anti-Cryptor** 섹션에서 **설정** 옵션을 클릭합니다.
5. **공유 폴더 보호** 탭으로 갑니다.
6. **IP 주소 예외** 블록에서 **구성** 버튼을 클릭합니다.
7. 열리는 창에서 **추가** 버튼을 클릭합니다.
8. 외부에서의 암호화 시도를 처리하지 말아야 하는 컴퓨터의 이름 또는 IP 주소를 입력합니다.
9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 외부 데이터 암호화를 위해 신뢰하는 컴퓨터를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **실시간 컴퓨터 보호** → **Anti-Cryptor** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   Anti-Cryptor 창이 열립니다.

5. **공유 폴더 보호** 탭으로 갑니다.

6. **예외 규칙** 블록에서 **추가** 버튼을 클릭합니다.

7. 외부에서의 암호화 시도를 처리하지 말아야 하는 컴퓨터의 이름 또는 IP 주소를 입력합니다.

8. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 외부 데이터 암호화를 위해 신뢰하는 컴퓨터를 추가하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호** → **Anti-Cryptor** 옵션을 선택합니다.

2. **Anti-Cryptor** 노드 결과 창에서 **속성**을 클릭합니다.
   속성: Anti-Cryptor 창이 열립니다.

3. **공유 폴더 보호** 탭으로 갑니다.

4. **IP 주소 예외** 블록에서 **구성** 버튼을 클릭합니다.

5. 열리는 창에서 **추가** 버튼을 클릭합니다.

6. 외부에서의 암호화 시도를 처리하지 말아야 하는 컴퓨터의 이름 또는 IP 주소를 입력합니다.

7. 변경 사항을 저장합니다.

신뢰하지 않는 컴퓨터의 차단 기간 구성

*신뢰할 수 없는 컴퓨터*는 악성 활동 또는 데이터 암호화를 수행하는 원격 컴퓨터입니다. 기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 원격 사용자의 세션을 1시간 동안 차단합니다. 차단 기간이 만료되면 Kaspersky Industrial CyberSecurity for Nodes는 차단 목록에서 해당 컴퓨터를 제거하고 공유 폴더에 대한 접근 권한을 복원합니다.

Kaspersky Security Center 관리 콘솔에서 신뢰할 수 없는 컴퓨터의 차단 기간을 설정하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.

4. **Anti-Cryptor** 섹션에서 **설정** 옵션을 클릭합니다.

5. **Anti-Cryptor** 확인란으로 구성 요소를 사용하거나 중지합니다.

6. **공유 폴더 보호** 탭으로 갑니다.

7. **공유 폴더에 대한 외부 컴퓨터에서의 암호화 시도 탐지 시**에서 악성 활동 또는 데이터 암호화에 연루된 신뢰할 수 없는 컴퓨터의 차단 기간을 설정합니다.

8. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 신뢰할 수 없는 컴퓨터의 차단 기간을 설정하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **실시간 컴퓨터 보호** → **Anti-Cryptor** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   Anti-Cryptor 창이 열립니다.

5. **Anti-Cryptor 사용** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.

6. **공유 폴더 보호** 탭으로 갑니다.

7. **외부 암호화 탐지**에서 악성 활동 또는 데이터 암호화에 연루된 신뢰할 수 없는 컴퓨터의 차단 기간을 설정합니다.

8. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 신뢰할 수 없는 컴퓨터의 차단 기간을 설정하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호** → **Anti-Cryptor** 옵션을 선택합니다.

2. **Anti-Cryptor** 노드 결과 창에서 **속성**을 클릭합니다.
   속성: Anti-Cryptor 창이 열립니다.

3. **Anti-Cryptor** 확인란을 선택합니다.

4. **공유 폴더 보호** 탭으로 갑니다.

5. **외부 암호화로부터 공유 폴더 보호**에서 악성 활동 또는 데이터 암호화에 연루된 신뢰할 수 없는 컴퓨터의 차단 기간을 설정합니다.

6. 변경 사항을 저장합니다.

외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 시 예외 규칙 목록 내보내기 및 가져오기

예외 목록을 XML 파일로 내보낼 수 있습니다. 그 후 같은 유형의 주소를 여러 개 추가하는 등 파일을 수정할 수 있습니다. 내보내기/가져오기 기능을 사용하여 예외 규칙 목록을 백업하거나 목록을 다른 서버로 마이그레이션할 수도 있습니다.

Kaspersky Security Center 관리 콘솔에서 예외 목록을 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 옵션을 선택합니다.
4. **Anti-Cryptor** 섹션에서 **설정** 옵션을 클릭합니다.
5. **공유 폴더 보호** 탭으로 갑니다.
6. **IP 주소 예외** 블록에서 **구성** 버튼을 클릭합니다.
7. 규칙 목록을 내보내려면 다음을 수행합니다.
   a. 필요하다면 내보낼 예외를 선택합니다.
   b. 버튼을 클릭하고 내보내기 모드를 선택하여, 전체 예외 목록을 내보내거나 선택한 예외만 내보냅니다.
   c. 창이 열리면 예외 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   d. 파일을 저장합니다.
   Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 예외 목록을 XML 파일로 내보냅니다.
8. 예외 목록을 가져오려면 다음을 수행합니다.
   a. → **가져오기** 버튼을 클릭합니다.
   창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.
   b. 파일을 엽니다.
   Kaspersky Industrial CyberSecurity for Nodes가 예외를 가져옵니다.
9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

웹 콘솔에서 예외 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호** → **Anti-Cryptor** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   Anti-Cryptor 창이 열립니다.
5. **Anti-Cryptor 사용** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.
6. **공유 폴더 보호** 탭으로 갑니다.

7. **예외 규칙** 블록에서 예외 목록을 내보내려면 다음을 수행합니다.

   a. 필요하다면 내보낼 예외를 선택합니다.

   b. **내보내기** 버튼을 클릭하고 내보내기 모드를 선택하여, 전체 예외 목록을 내보내거나 선택한 예외만 내보냅니다.

   c. 파일을 저장합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 예외 목록을 XML 파일로 내보냅니다.

8. **예외 규칙** 블록에서 예외 목록을 가져오려면 다음을 수행합니다.

   a. **가져오기** 버튼을 클릭하고 추가 또는 교체 중에서 가져오기 모드를 선택합니다.

   b. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.

   c. 파일을 엽니다.

   Kaspersky Industrial CyberSecurity for Nodes가 선택한 모드에 따라 예외를 가져옵니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다 .

네트워크 위협 보호

네트워크 위협 보호 구성 요소는 인바운드 네트워크 트래픽에 네트워크 공격을 위한 일반적인 활동이 있는지 검사합니다. 사용자 컴퓨터를 표적으로 하는 네트워크 공격 시도가 탐지되면 Kaspersky Industrial CyberSecurity for Nodes가 공격 컴퓨터의 네트워크 활동을 차단합니다. 현재 알려진 네트워크 공격 유형과 이에 대응하는 방법에 대한 설명은 애플리케이션 데이터베이스에서 제공합니다. 네트워크 위협 보호 구성 요소가 탐지하는 네트워크 공격 목록은 데이터베이스 및 애플리케이션 모듈 업데이트 중에 업데이트됩니다.

기본적으로 네트워크 위협 보호 작업은 **알림** 모드에서 실행됩니다. 이 모드에서는 Kaspersky Industrial CyberSecurity for Nodes가 인바운드 네트워크 트래픽에서 일반적인 네트워크 공격 활동을 검색하고 탐지된 활동에 해당하는 이벤트를 로깅하지만, 이러한 활동에 관련된 컴퓨터의 연결을 차단하지 않으며, 해당 컴퓨터의 IP 주소를 차단된 네트워크 세션 목록에 추가하지 않습니다.

차단 모드에서 Kaspersky Industrial CyberSecurity for Nodes는 일반적인 네트워크 공격 활동을 보이는 컴퓨터의 연결을 차단하고, 때에 따라 이러한 컴퓨터의 IP 주소를 차단된 네트워크 세션 목록에 추가합니다.

차단된 호스트 저장소에서 차단된 호스트 목록을 볼 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션이 다시 시작될 때와 네트워크 위협 보호 설정이 변경될 때 차단 목록을 지웁니다.

차단된 호스트 저장소 설정을 구성하여 차단된 호스트에 대한 접근을 복원하고, 호스트가 차단된 후 네트워크 파일 리소스에 다시 접근할 수 있는 기간을 일, 시간, 분으로 지정할 수 있습니다.

다음 경우에는 일반적인 네트워크 공격의 활동을 보이는 호스트의 IP 주소를 차단된 호스트 목록에서 삭제합니다.

- Kaspersky Industrial CyberSecurity for Nodes가 제거되었습니다.
- 차단된 호스트 목록에서 IP 주소를 수동으로 삭제했습니다.
- 호스트 차단 기간이 만료되었습니다.
- **차단** 모드가 꺼졌습니다.

Kaspersky Industrial CyberSecurity for Nodes가 Microsoft Hyper-V 인프라의 가상 컴퓨터에서 올바르게 작동하려면 Hyper-V 가상 스위치를 구성하기 전에 Kaspersky Industrial CyberSecurity for Nodes를 설치해야 합니다.

네트워크 위협 보호 사용 및 구성

Kaspersky Security Center 관리 콘솔에서 네트워크 위협 보호를 활성화하고 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **네트워크 활동 제어** 섹션으로 갑니다.

4. **네트워크 위협 보호** 블록에서 **설정** 버튼을 클릭합니다.

5. 창이 열리면 **네트워크 위협 보호** 확인란을 선택합니다.

6. **운영 모드** 섹션에서 작업 모드를 선택합니다.

   - **차단**. 이 모드를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 인바운드 네트워크 트래픽에서 일반적인 네트워크 공격 활동을 검사하고, 이러한 활동을 보이는 컴퓨터의 연결을 차단하며, 때에 따라 컴퓨터의 IP 주소를 차단된 네트워크 세션 목록에 추가합니다. 또한 애플리케이션이 구성 요소 로그에 일반적인 네트워크 공격의 탐지된 활동에 대한 이벤트를 기록합니다.

   - **알림**. 이 모드를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 인바운드 네트워크 트래픽에서 일반적인 네트워크 공격 활동을 검색하지만 이러한 활동을 보이는 컴퓨터의 연결을 차단하지 않으며 컴퓨터의 IP 주소를 차단된 네트워크 세션 목록에 추가하지 않습니다. 애플리케이션은 구성 요소 로그에 일반적인 네트워크 공격으로 탐지된 활동에 대한 이벤트를 기록합니다.

7. **포트 검사와 네트워크 플러딩을 공격으로 간주** 확인란으로 해당 공격의 탐지를 활성화하거나 비활성화합니다.

8. 필요하다면 **다음 시간 동안 공격 장치 차단: N분** 확인란을 선택합니다.

9. **MAC 스푸핑 보호** 블록에서 **MAC 스푸핑 공격에 대한 보호 활성화** 확인란을 선택하거나 선택 해제합니다.

10. 필요하다면 차단 예외를 추가할 수 있습니다.

11. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 네트워크 위협 보호를 활성화하고 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호 → 네트워크 위협 보호** 노드를 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.
   속성: 네트워크 위협 보호 창이 열립니다.

3. **네트워크 위협 보호** 확인란을 선택합니다.

4. **작업 모드** 섹션에서 작업 모드를 선택합니다.

   - **차단**. 이 모드를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 인바운드 네트워크 트래픽에서 일반적인 네트워크 공격 활동을 검사하고, 이러한 활동을 보이는 컴퓨터의 연결을 차단하며, 때에 따라 컴퓨터의 IP 주소를 차단된 네트워크 세션 목록에 추가합니다. 또한 애플리케이션이 구성 요소 로그에 일반적인 네트워크 공격의 탐지된 활동에 대한 이벤트를 기록합니다.

   - **알림**. 이 모드를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 인바운드 네트워크 트래픽에서 일반적인 네트워크 공격 활동을 검색하지만 이러한 활동을 보이는 컴퓨터의 연결을 차단하지 않으며 컴퓨터의 IP 주소를 차단된 네트워크 세션 목록에 추가하지 않습니다. 애플리케이션은 구성 요소 로그에 일반적인 네트워크 공격으로 탐지된 활동에 대한 이벤트를 기록합니다.

5. **포트 검사와 네트워크 플러딩을 공격으로 간주** 확인란으로 해당 공격의 탐지를 활성화하거나 비활성화합니다.

6. 필요하다면 **다음 시간 동안 공격 장치 차단: N분** 확인란을 선택합니다.

7. **MAC 스푸핑 보호** 블록에서 **MAC 스푸핑 공격에 대한 보호 활성화** 확인란을 선택하거나 선택 해제합니다.

8. 필요하다면 차단 예외를 추가할 수 있습니다.

9. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 네트워크 위협 보호를 활성화하고 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **네트워크 활동 제어** → **네트워크 위협 보호**를 선택합니다.

5. **일반** 탭에서 **네트워크 위협 보호 사용** 확인란을 선택합니다.

6. 작업 운영 모드를 선택합니다:

   - **차단**. 이 모드를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 인바운드 네트워크 트래픽에서 일반적인 네트워크 공격 활동을 검사하고, 이러한 활동을 보이는 컴퓨터의 연결을 차단하며, 때에 따라 컴퓨터의 IP 주소를 차단된 네트워크 세션 목록에 추가합니다. 또한 애플리케이션이 구성 요소 로그에 일반적인 네트워크 공격의 탐지된 활동에 대한 이벤트를 기록합니다.

   - **알림**. 이 모드를 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 인바운드 네트워크 트래픽에서 일반적인 네트워크 공격 활동을 검색하지만 이러한 활동을 보이는 컴퓨터의 연결을 차단하지 않으며 컴퓨터의 IP 주소를 차단된 네트워크 세션 목록에 추가하지 않습니다. 애플리케이션은 구성 요소 로그에 일반적인 네트워크 공격으로 탐지된 활동에 대한 이벤트를 기록합니다.

7. **포트 검사와 네트워크 플러딩을 공격으로 간주** 확인란으로 해당 공격의 탐지를 활성화하거나 비활성화합니다.

8. 필요하다면 **다음 시간 동안 공격 장치 차단: N분** 확인란을 선택합니다.

9. **MAC 스푸핑 공격에 대한 보호 활성화** 확인란을 선택하거나 선택 해제합니다.

10. 필요하다면 차단 예외를 추가할 수 있습니다.

11. 변경 사항을 저장합니다.

차단 예외 생성

Kaspersky Industrial CyberSecurity for Nodes는 네트워크 공격을 인식하고 대량의 패킷을 전송하는 보안 되지 않은 네트워크 연결(감시 카메라 등)을 차단할 수 있습니다. 신뢰하는 장치로 작업하려면 이러한 장치의 IP 주소를 예외 규칙 목록에 추가할 수 있습니다. 커뮤니케이션에 사용되는 프로토콜과 포트를 선택하고 특정 네트워크 활동을 허용할 수도 있습니다.

제외할 프로토콜과 포트를 선택하는 기능이 Kaspersky Industrial CyberSecurity for Nodes 4.0에 추가되었습니다. 애플리케이션과 관리 플러그인이 버전 4.0 이상으로 업데이트되었는지 확인하십시오. 이전 버전의 애플리케이션 또는 관리 플러그인을 사용 중이라면 Kaspersky Industrial CyberSecurity for Nodes는 IP 주소로만 네트워크 활동을 허용할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 차단 예외를 생성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **네트워크 활동 제어** 섹션으로 갑니다.
4. **네트워크 위협 보호** 블록에서 **설정** 버튼을 클릭합니다.
   네트워크 위협 보호 창이 열립니다.
5. **예외** 탭으로 갑니다.
6. **제외된 주소를 제어하지 않음** 확인란을 선택하면, Kaspersky Industrial CyberSecurity for Nodes가 제외된 IP 주소의 인바운드 네트워크 트래픽을 검사하지 않습니다.
7. **추가** 버튼을 클릭합니다.
8. **예외** 창에 네트워크 공격을 차단하지 않을 기기의 IP 주소를 입력합니다.
9. 필요한 경우 데이터가 전송되는 프로토콜과 포트를 지정합니다.
10. **확인**을 누릅니다.
11. 추가한 예외마다 c~f 단계를 수행합니다.
12. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 차단 예외를 생성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **네트워크 활동 제어 → 네트워크 위협 보호** 옵션을 선택하고 **구성** 버튼을 클릭합니다.
5. **예외 규칙** 탭으로 갑니다.
6. **제외된 IP 주소를 제어하지 않음** 확인란을 선택하면, Kaspersky Industrial CyberSecurity for Nodes가 제외된 IP 주소의 인바운드 네트워크 트래픽을 검사하지 않습니다.
7. **추가** 버튼을 클릭합니다.
8. **예외 규칙 추가** 창에 네트워크 공격을 차단하지 않을 기기의 IP 주소를 입력합니다.
9. 필요한 경우 데이터가 전송되는 프로토콜과 포트를 지정합니다.
10. **확인**을 누릅니다.
11. 추가한 예외마다 c~f 단계를 수행합니다.
12. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 차단 예외를 생성하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호 → 네트워크 위협 보호** 노드를 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.
   속성: 네트워크 위협 보호 창이 열립니다.
3. **예외** 탭으로 갑니다.
4. **제외된 주소를 제어하지 않음** 확인란을 선택하면, Kaspersky Industrial CyberSecurity for Nodes가 제외된 IP 주소의 인바운드 네트워크 트래픽을 검사하지 않습니다.
5. **추가** 버튼을 클릭합니다.
6. **예외** 창에 네트워크 공격을 차단하지 않을 기기의 IP 주소를 입력합니다.
7. 필요한 경우 데이터가 전송되는 프로토콜과 포트를 지정합니다.
8. **확인**을 누릅니다.
9. 추가한 예외마다 c~f 단계를 수행합니다.
10. 변경 사항을 저장합니다.

외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 시 예외 규칙 목록 내보내기 및 가져오기

예외 목록을 XML 파일로 내보낼 수 있습니다. 그 후 같은 유형의 주소를 여러 개 추가하는 등 파일을 수정할 수 있습니다. 내보내기/가져오기 기능을 사용하여 예외 규칙 목록을 백업하거나 목록을 다른 서버로 마이그레이션할 수도 있습니다.

Kaspersky Security Center 관리 콘솔에서 예외 목록을 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **네트워크 활동 제어** 섹션으로 갑니다.
4. **네트워크 위협 보호** 블록에서 **설정** 버튼을 클릭합니다.
   네트워크 위협 보호 창이 열립니다.
5. **예외** 탭으로 갑니다.

6. 규칙 목록을 내보내려면 다음 동작 중 하나를 수행합니다.

   - 확인란을 사용해 내보낼 예외를 선택합니다. 화살표를 클릭하고 드롭다운 목록에서 **선택 항목 내보내기** 옵션을 선택합니다.
   - 예외 규칙 목록 전체를 내보내려면 화살표를 클릭하고 드롭다운 목록에서 **내보내기**를 선택합니다.

     Kaspersky Industrial CyberSecurity for Nodes는 표준 다운로드 폴더에 networkExclusions.xml이라는 파일을 저장합니다.

7. 예외 목록을 가져오려면 다음을 수행합니다.

   a. 화살표를 클릭하고 **가져오기**를 선택합니다.

   b. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.

   c. 파일을 엽니다.

      컴퓨터에 이미 예외 목록이 있으면 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. 변경 사항을 저장합니다.

웹 콘솔에서 예외 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호** → **네트워크 위협 보호** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. 창이 열리면 **예외 규칙** 탭을 선택합니다.
6. 규칙 목록을 내보내려면 다음을 수행합니다.

   a. 필요하다면 내보낼 예외를 선택합니다.

   b. **내보내기** 버튼을 클릭하고 내보내기 모드를 선택하여, 전체 예외 목록을 내보내거나 선택한 예외만 내보냅니다.

   c. **내보내기** 버튼을 클릭합니다.

      Kaspersky Industrial CyberSecurity for Nodes는 표준 다운로드 폴더에 networkExclusions.xml이라는 파일을 저장합니다.

7. 예외 목록을 가져오려면 다음을 수행합니다.

   a. **가져오기** 버튼을 클릭하고 **기존 항목에 추가** 또는 **기존 항목 덮어쓰기** 중에서 가져오기 모드를 선택합니다.

   b. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.

c. 파일을 엽니다.

Kaspersky Industrial CyberSecurity for Nodes가 선택한 모드에 따라 예외를 가져옵니다.

8. 변경 사항을 저장합니다.

AMSI 스캐너

AMSI 스캐너 작업이 실행 중일 때 Kaspersky Industrial CyberSecurity for Nodes가 VBScript 또는 JScript와 같은 Microsoft Windows 스크립팅 기술(액티브 스크립팅, Active Scripting)을 사용하여 생성된 스크립트의 실행을 제어합니다. 또한 애플리케이션은 AMSI(Antimalware Scan Interface)가 설치된 운영 체제의 Microsoft Office 애플리케이션에서 실행되는 스크립트 및 PowerShell 스크립트를 처리할 수 있습니다.

AMSI를 사용하면 애플리케이션 및 서비스를 장치에 설치된 모든 악성 코드 방지 애플리케이션과 통합할 수 있으며, 이를 통해 악성 코드 방지 프로그램이 실행 중인 모든 스크립트를 가로채서 검사할 수 있습니다. AMSI 기능에 대한 자세한 내용은 Microsoft 웹사이트에서 확인할 수 있습니다.

구성 요소 설정에서 위험한 스크립트 실행을 허용하거나 거부할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes가 스크립트를 위험한 것으로 식별하면 사용자가 선택한 동작에 따라 스크립트의 실행을 차단하거나 허용합니다. **차단** 동작을 선택하면 애플리케이션이 위험한 스크립트를 차단하고 다른 스크립트를 허용합니다.

Kaspersky Industrial CyberSecurity for Nodes는 Microsoft Windows 10 및 Microsoft Windows Server 2016 이상에서 AMSI 기술을 지원합니다.

AMSI 스캐너 사용 및 중지

Kaspersky Security Center 관리 콘솔에서 AMSI 스캐너를 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 섹션으로 갑니다.
4. **AMSI 스캐너** 블록에서 **설정** 버튼을 클릭합니다.
   일반 탭에서 **AMSI 스캐너** 창이 열립니다.
5. 다음 중 하나를 수행합니다:
   - AMSI 스캐너를 활성화하려는 경우 **AMSI 스캐너** 확인란을 선택합니다.
   - AMSI 스캐너를 비활성화하려는 경우 **AMSI 스캐너** 확인란을 선택 해제합니다.
6. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 AMSI 스캐너를 활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호** → **AMSI 스캐너** 섹션을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.
   일반 탭에서 **AMSI 스캐너** 창이 열립니다.

3. 다음 중 하나를 수행합니다:

   - AMSI 스캐너를 활성화하려는 경우 **AMSI 스캐너** 확인란을 선택합니다.
   - AMSI 스캐너를 비활성화하려는 경우 **AMSI 스캐너** 확인란을 선택 해제합니다.

4. **AMSI 스캐너** 창에서 **확인** 버튼을 클릭합니다.

Kaspersky Security Center 웹 콘솔에서 AMSI 스캐너를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **실시간 컴퓨터 보호** 섹션을 선택합니다.
5. **AMSI 스캐너** 블록에서 **구성** 버튼을 클릭합니다.
   AMSI 스캐너 창이 열립니다.
6. 다음 중 하나를 수행합니다:

   - AMSI 스캐너를 활성화하려는 경우 **AMSI 스캐너** 확인란을 선택합니다.
   - AMSI 스캐너를 비활성화하려는 경우 **AMSI 스캐너** 확인란을 선택 해제합니다.

7. 변경 사항을 저장합니다.

AMSI 스캐너 설정

Kaspersky Security Center 관리 콘솔에서 AMSI 스캐너 설정을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **실시간 컴퓨터 보호** 섹션으로 갑니다.
4. **AMSI 스캐너** 블록에서 **설정** 버튼을 클릭합니다.
   일반 탭에서 **AMSI 스캐너** 창이 열립니다.
5. 위험한 스크립트가 실행될 때 Kaspersky Industrial CyberSecurity for Nodes가 수행할 동작을 선택합니다:

   - **알림**. 애플리케이션이 위험할 수 있는 스크립트의 실행을 허용합니다. 해당 이벤트가 작업 로그에 기록됩니다.
   - **차단**. 애플리케이션이 위험할 수 있는 스크립트를 차단합니다.

6. **복합 파일 검사** 블록에서 압축 파일, 배포 패키지, 오피스 형식의 파일 등 검사할 복합 파일의 유형을 지정합니다.

7. **크기 제한** 블록에서 다음 중 하나를 수행합니다:

   - AMSI 스캐너 구성 요소가 대용량 복합 파일을 압축 해제하지 않게 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택하고 **최대 파일 크기(MB)** 필드에 필요한 값을 지정합니다. AMSI 스캐너 구성 요소는 지정한 크기보다 큰 복합 파일을 압축 해제하지 않습니다.

   - AMSI 스캐너 구성 요소가 대용량 복합 파일을 압축 해제하게 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택 해제합니다.

   AMSI 스캐너 구성 요소는 **큰 복합 파일은 압축 해제 안 함** 확인란의 선택 여부와 관계없이 압축 파일에서 추출한 대용량 파일을 검사합니다.

8. **AMSI 스캐너** 창에서 **확인** 버튼을 클릭합니다.

9. **속성: <정책 이름>** 창에서 **확인** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 AMSI 스캐너 설정을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **실시간 컴퓨터 보호 → AMSI 스캐너** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.

   일반 탭에서 **AMSI 스캐너** 창이 열립니다.

3. 위험한 스크립트가 실행될 때 Kaspersky Industrial CyberSecurity for Nodes가 수행할 동작을 선택합니다:

   - **알림**. 애플리케이션이 위험할 수 있는 스크립트의 실행을 허용합니다. 해당 이벤트가 작업 로그에 기록됩니다.

   - **차단**. 애플리케이션이 위험할 수 있는 스크립트를 차단합니다.

4. **복합 파일 검사** 블록에서 압축 파일, 배포 패키지, 오피스 형식의 파일 등 검사할 복합 파일의 유형을 지정합니다.

5. **크기 제한** 블록에서 다음 중 하나를 수행합니다:

   - AMSI 스캐너 구성 요소가 대용량 복합 파일을 압축 해제하지 않게 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택하고 **최대 파일 크기(MB)** 필드에 필요한 값을 지정합니다. AMSI 스캐너 구성 요소는 지정한 크기보다 큰 복합 파일을 압축 해제하지 않습니다.

   - AMSI 스캐너 구성 요소가 대용량 복합 파일을 압축 해제하게 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택 해제합니다.

   AMSI 스캐너 구성 요소는 **큰 복합 파일은 압축 해제 안 함** 확인란의 선택 여부와 관계없이 압축 파일에서 추출한 대용량 파일을 검사합니다.

6. **AMSI 스캐너** 창에서 **확인** 버튼을 클릭합니다.

Kaspersky Security Center 웹 콘솔에서 AMSI 스캐너 설정을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **실시간 컴퓨터 보호** 섹션을 선택합니다.

5. **AMSI 스캐너** 블록에서 **구성** 버튼을 클릭합니다.
   AMSI 스캐너 창이 열립니다.

6. 위험한 스크립트가 실행될 때 Kaspersky Industrial CyberSecurity for Nodes가 수행할 동작을 선택합니다:

   - **알림**. 애플리케이션이 위험할 수 있는 스크립트의 실행을 허용합니다. 해당 이벤트가 작업 로그에 기록됩니다.

   - **차단**. 애플리케이션이 위험할 수 있는 스크립트를 차단합니다.

7. **복합 파일 검사** 블록에서 압축 파일, 배포 패키지, 오피스 형식의 파일 등 검사할 복합 파일의 유형을 지정합니다.

8. **크기 제한** 블록에서 다음 중 하나를 수행합니다:

   - AMSI 스캐너 구성 요소가 대용량 복합 파일을 압축 해제하지 않게 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택하고 **최대 파일 크기(MB)** 필드에 필요한 값을 지정합니다. AMSI 스캐너 구성 요소는 지정한 크기보다 큰 복합 파일을 압축 해제하지 않습니다.

   - AMSI 스캐너 구성 요소가 대용량 복합 파일을 압축 해제하게 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택 해제합니다.

   > AMSI 스캐너 구성 요소는 **큰 복합 파일은 압축 해제 안 함** 확인란의 선택 여부와 관계없이 압축 파일에서 추출한 대용량 파일을 검사합니다.

9. **AMSI 스캐너** 창의 **확인** 버튼을 클릭합니다.

10. **<정책 이름>** 창의 **저장** 버튼을 클릭합니다.

애플리케이션 실행 제어

Kaspersky Industrial CyberSecurity for Nodes의 애플리케이션 실행 제어 구성 요소는 무단 애플리케이션 실행으로부터 장치를 보호합니다. 애플리케이션 실행 제어 구성 요소는 기본 거부 원칙을 기반으로 합니다. 즉, 구성 요소 설정에서 허용하지 않은 애플리케이션은 자동으로 차단됩니다. 애플리케이션에 대한 구성 요소 허용 규칙을 만들어 애플리케이션 실행을 허용할 수 있습니다.

애플리케이션 실행 제어 규칙을 최대한 완전하게 생성하면 Kaspersky Industrial CyberSecurity for Nodes는 조직의 로컬 네트워크 관리자가 확인하지 않은 모든 새 애플리케이션의 실행을 차단하는 동시에 운영 체제와 사용자가 업무를 수행하는 데 필요한 검증된 애플리케이션의 정상 작동을 보장합니다. *애플리케이션 실행 제어를 위한 규칙 생성기* 작업을 사용하여 보호 중인 장치에 설치된 애플리케이션에 대한 정보를 확인할 수 있습니다.

애플리케이션 실행 제어 구성 요소를 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 보호 중인 장치에서 실행 파일이 실행될 때 발생하는 프로세스 생성 요청과 관련된 모든 운영 체제 이벤트를 가로챕니다. 그런 다음 애플리케이션은 실행되는 실행 파일, 스크립트 또는 MSI 패키지에 대한 정보를 수집하고 이를 애플리케이션 실행 제어 규칙의 트리거 조건과 비교합니다. 하나 이상의 허용 규칙에 지정된 모든 조건이 충족되면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행을 허용합니다. 실행되는 애플리케이션이 어떤 허용 규칙의 조건도 충족하지 않거나 차단 규칙이 트리거되면 Kaspersky Industrial CyberSecurity for Nodes는 프로세스 생성을 취소하여 애플리케이션 실행 시도를 차단합니다.

애플리케이션의 모든 시작 시도는 구성 요소의 로그에 기록됩니다.

애플리케이션 실행 제어 구성 요소는 두 가지 모드 중 하나에서 작동할 수 있습니다:

- **차단**. Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 규칙을 사용하여 애플리케이션 실행을 제어합니다. 애플리케이션 실행 제어 규칙의 범위는 애플리케이션 실행 제어 구성 요소 일반 설정에서 지정됩니다. 애플리케이션이 애플리케이션 실행 제어 규칙을 충족하지만 애플리케이션 실행 제어 규칙의 범위와 일치하는 규칙이 없으면 해당 애플리케이션이 실행되지 않습니다.

  애플리케이션 실행 제어 규칙이 적용되지 않는 애플리케이션을 실행하는 것은 금지됩니다.

  > 애플리케이션 실행 제어 구성 요소는 생성된 애플리케이션 실행 제어 규칙이 없거나 보호 중인 장치 하나에 대해 65,535개보다 많은 애플리케이션 실행 제어 규칙이 있는 경우에는 활성 모드에서 시작할 수 없습니다.

- **알림**. Kaspersky Industrial CyberSecurity for Nodes이 모든 애플리케이션의 시작을 허용합니다. 모든 애플리케이션 실행, 실행 중인 애플리케이션에 적용되는 규칙, **차단** 모드에서 작업이 실행 중일 경우 수행될 처리에 관한 정보만 기록됩니다. 기본적으로 이 모드가 설정됩니다.

> 애플리케이션 실행 제어 규칙을 생성할 때 운영 체제의 애플리케이션 실행을 차단하지 않는지 확인하는 것이 좋습니다.

Kaspersky Industrial CyberSecurity for Nodes는 Windows Subsystem for Linux에서 실행된 프로세스도 가로챌 수 있습니다(UNIX™ 셸 또는 명령줄 해석기에서 실행되는 스크립트 예외). 이러한 프로세스에 대해 애플리케이션 실행 제어 구성 요소는 현재 구성에서 정의한 동작을 적용합니다. *애플리케이션 실행 제어를 위한 규칙 생성기* 작업은 애플리케이션 실행을 탐지하고 Windows Subsystem for Linux에서 실행되는 애플리케이션에 대응하는 규칙을 생성합니다.

애플리케이션 실행 제어 규칙 정보

애플리케이션 실행 제어 규칙의 작동 방식

애플리케이션 실행 제어 규칙은 다음 구성 요소를 기반으로 작동합니다:

- 규칙 유형.

  애플리케이션 실행 제어 규칙은 애플리케이션 시작을 허용하거나 거부할 수 있습니다. 따라서, 애플리케이션 실행 규칙은 *허용* 또는 *거부* 규칙이라고 불립니다.

- 규칙 사용 범위.

  애플리케이션 실행 제어 규칙은 *실행 파일, 스크립트, MSI 패키지*에 적용할 수 있습니다.

- 규칙 트리거 조건.

  애플리케이션 실행 제어 규칙은 규칙 설정에 지정된 트리거 조건을 하나 이상 충족하는 파일 실행을 규제합니다. 예를 들어 실행 파일은 지정된 *디지털 인증서*로 서명되고, 지정된 *SHA256 해시*를 가지며, 지정된 *경로*에 있고, 지정된 *명령줄* 인수와 일치합니다. 규칙 트리거 조건을 하나 이상 추가해야 합니다. 아니면 애플리케이션 실행 제어 규칙이 추가되지 않습니다.

- 규칙 예외.

  애플리케이션 실행 제어 규칙에 대한 예외를 구성할 수 있으며, 이는 규칙 트리거 조건과 같은 기준에 기반할 수 있습니다. 애플리케이션 실행 제어 규칙에서 예외는 특정 허용 규칙에 필요할 수 있습니다. 예를 들어 Regedit.exe 파일의 실행은 차단하면서 C:\Windows 경로에서 사용자가 프로그램을 시작할 수 있도록 하려는 경우입니다.

- 사용자 또는 사용자 그룹.

  애플리케이션 실행 제어 규칙은 지정된 사용자 또는 사용자 그룹이 지정된 애플리케이션을 시작하는 것을 제어할 수 있습니다.

애플리케이션 실행 제어 규칙을 생성할 때 새 규칙이 운영 체제의 애플리케이션 실행을 차단하지 않는지 확인하는 것이 좋습니다.

애플리케이션 실행 제어 규칙 관리

애플리케이션 실행 제어 규칙으로 다음 동작을 수행할 수 있습니다.

- 직접 추가.
- 자동으로 규칙 생성 및 추가.
- 삭제.

- 가져오기 및 내보내기.
- 규칙 목록을 필터링.

소프트웨어 배포 제어 정보

소프트웨어 배포를 제어할 경우 애플리케이션 실행 제어 생성이 더 복잡해질 수 있습니다. 예를 들어, 설치된 소프트웨어가 정기적으로 자동 업데이트되는 보호 중인 장치에서 이를 수행할 수 있습니다. 이 경우 애플리케이션 실행 제어 구성 요소 설정에서 새로 생성된 파일을 고려하려면 각 소프트웨어 업데이트 후 허용 규칙 목록을 업데이트해야 합니다. 소프트웨어 배포 시나리오에서 실행 제어를 간소화하기 위해 소프트웨어 배포 제어를 사용할 수 있습니다.

설치 패키지(이하 "패키지"라고 함)는 보호 중인 장치에 설치되는 하나 이상의 애플리케이션을 나타냅니다. 설치 패키지에는 특정 업데이트 및 개별 명령이 포함될 수도 있습니다.

소프트웨어 배포 제어 서브시스템은 예외의 추가 목록으로 구현됩니다. 목록에 추가된 설치 패키지는 신뢰하는 패키지가 됩니다. 신뢰하는 패키지는 압축 해제가 허용되며 신뢰하는 패키지에서 설치하거나 업데이트한 애플리케이션은 자동 시작할 수 있습니다. 압축 해제된 파일은 기본 배포 패키지의 신뢰 속성을 상속할 수 있습니다. *기본 배포 패키지*는 사용자가 소프트웨어 배포 제어 예외 목록에 추가하여 신뢰하는 패키지가 된 패키지입니다.

Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 배포의 전체 주기만 제어하며, 패키지를 처음 시작할 때 소프트웨어 배포 제어가 꺼져 있거나 애플리케이션 실행 제어 구성 요소가 설치되지 않은 경우 신뢰하는 패키지에서 수정한 파일의 시작을 올바르게 처리할 수 없습니다.

소프트웨어 배포 제어를 사용하려면 애플리케이션 실행 제어 구성 요소 일반 설정의 **실행 파일에 규칙 적용** 기능을 활성화해야 합니다.

소프트웨어 배포 캐시

Kaspersky Industrial CyberSecurity for Nodes는 동적으로 생성된 소프트웨어 배포 캐시(이하 "배포 캐시"라고 함)를 사용하여 신뢰하는 패키지와 소프트웨어 배포 중에 생성된 파일 간의 관계를 설정합니다. 패키지를 처음 시작하면 Kaspersky Industrial CyberSecurity for Nodes는 소프트웨어 배포 프로세스 중에 패키지에서 생성한 모든 파일을 탐지하고 파일 체크섬과 경로를 배포 캐시에 저장합니다. 그런 다음 기본적으로 배포 캐시에 저장된 정보가 있는 모든 파일의 시작이 허용됩니다.

사용자 인터페이스를 통해 배포 캐시를 검토하거나 삭제하거나 직접 수정할 수 없습니다. 캐시는 Kaspersky Industrial CyberSecurity for Nodes에서 채우고 제어합니다.

배포 캐시를 구성 파일(XML 형식)로 내보내거나 명령줄에서 배포 캐시를 삭제할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 24시간마다 배포 캐시를 업데이트합니다. 이전에 허용된 파일의 체크섬이 변경되면 애플리케이션은 배포 캐시에서 이 파일에 대한 레코드를 삭제합니다. 애플리케이션 실행 제어 구성 요소가 활성 모드에서 실행 중이면 이 파일을 시작하려는 이후의 시도가 차단됩니다. 체크섬이 배포 캐시 내에 저장되므로 이전에 허용된 파일의 전체 경로가 변경되어도 이 파일을 시작하려는 이후의 시도가 차단되지 않습니다.

압축 해제된 파일 처리

압축 해제 파일 및 기본 신뢰하는 배포 패키지(첫 번째 중첩 수준)에서 만든 패키지는 예외 목록의 소프트웨어 배포 패키지를 처음 열 때 배포 캐시에 체크섬이 추가되면서 신뢰하는 속성을 상속합니다. 따라서 배포 패키지 자체와 이 패키지에서 압축 해제된 모든 파일도 신뢰합니다.

예를 들어 여러 패키지와 애플리케이션을 포함한 패키지인 test.msi를 예외 목록에 추가하고 **모든 자식 파일을 신뢰하는 배포 패키지로 실행 허용** 기능이 활성화되면, 다른 중첩 파일을 포함하는 경우에도 test.msi 패키지에 포함된 모든 패키지와 애플리케이션을 압축 해제하고 실행할 수 있습니다. 이 시나리오는 모든 중첩 수준의 압축 해제 파일에 적용됩니다.

test.msi 패키지가 예외 목록에 추가되고 **모든 자식 파일을 신뢰하는 배포 패키지로 실행 허용** 기능이 비활성화되면, 애플리케이션은 신뢰하는 패킷(첫 번째 중첩 수준)에서 직접 압축 해제된 패킷 및 실행 파일에만 신뢰 속성을 할당합니다. 이러한 파일의 체크섬은 배포 캐시에 저장됩니다. 기본 거부 원칙에 따라 두 번째 수준 이상의 모든 파일이 차단됩니다.

압축 해제된 파일은 운영 체제를 다시 시작한 후에도 신뢰 속성을 유지합니다.

압축 해제된 모든 파일에서 상속 속성을 제거하려면 신뢰하는 설치 패키지를 다시 실행하기 전에 배포 캐시를 삭제하고 **모든 자식 파일을 신뢰하는 배포 패키지로 실행 허용** 기능을 비활성화합니다.

애플리케이션 실행 제어 규칙 목록 작업 방법

소프트웨어 배포 제어의 신뢰하는 패키지 목록은 예외 목록으로, 애플리케이션 실행 제어 규칙의 일반 목록을 증폭시키지만 교체하지는 않습니다.

애플리케이션 실행 제어 규칙 거부의 우선순위가 가장 높습니다. 신뢰하는 패키지 압축 해제와 새로운 파일 또는 수정된 파일의 시작은 이러한 패키지 및 파일이 애플리케이션 실행 제어 거부 규칙의 영향을 받는 경우 차단됩니다.

애플리케이션 실행 제어 목록의 거부 규칙이 해당 패키지 및 파일에 적용되지 않는 경우, 신뢰하는 패키지와 이러한 패키지에 의해 만들어졌거나 수정된 파일에 소프트웨어 배포 제어 예외가 적용됩니다.

애플리케이션 실행 제어를 위한 규칙 생성기 정보

회사 네트워크의 모든 보호 중인 장치 및 보호 중인 장치 그룹에 대해 Kaspersky Security Center 작업 및 정책을 동시에 사용하여 애플리케이션 실행 제어 규칙 목록을 만들 수 있습니다. 회사 네트워크에 참조 머신이 없고 템플릿 머신에 설치된 애플리케이션을 기반으로 허용 규칙 목록을 만들 수 없는 경우 아래 나열된 시나리오를 사용하는 것이 좋습니다.

애플리케이션 콘솔을 통해 로컬에서 *애플리케이션 실행 제어를 위한 규칙 생성기* 작업을 실행하여 보호 중인 단일 장치에서 실행 중인 애플리케이션을 기반으로 규칙 목록을 생성할 수 있습니다.

Kaspersky Security Center에서는 다음 방법의 하나로 애플리케이션 실행 제어 규칙 목록을 만들 수 있습니다:

- *애플리케이션 실행 제어를 위한 규칙 생성기* 그룹 작업 사용.

애플리케이션 실행 제어를 위한 규칙 생성기 작업은 설정에 따라 보호 중인 장치에서 실행되는 애플리케이션에 대한 정보뿐 아니라 지정된 범위에 있는 실행 파일 및 스크립트에 대한 정보도 수집할 수 있습니다. 수집된 정보를 기반으로 작업에서 애플리케이션 실행 제어 구성 요소에 대한 허용 규칙 목록을 생성합니다.

생성된 규칙을 애플리케이션 실행 제어 구성 요소 규칙 목록으로 자동 가져오도록 구성하거나 수동으로 가져올 수 있습니다.

이 시나리오는 촉박하게 애플리케이션 실행 제어 규칙 목록을 만들어야 하는 경우 권장됩니다. 허용 규칙의 사용 범위에 안전한 것으로 확인된 폴더 및 파일이 포함된 경우에만 *애플리케이션 실행 제어를 위한 규칙 생성기* 작업의 예약 실행을 구성하는 것이 좋습니다.

- *알림* 모드에서 실행 중인 애플리케이션 실행 제어 구성 요소에 대해 Kaspersky Security Center에서 생성한 이벤트 리포트를 기반으로 합니다.

  이 시나리오에서 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행을 거부하지 않습니다. 대신, 애플리케이션 실행 제어 구성 요소가 *알림* 모드에서 실행되면 모든 네트워크 보호 장치에서 허용되거나 거부된 모든 애플리케이션 실행을 Kaspersky Security Center의 중앙 관리 서버 노드 작업 공간에 있는 **이벤트** 탭에 보고합니다. Kaspersky Security Center는 리포트를 사용하여 애플리케이션 실행이 거부된 이벤트의 단일 목록을 생성합니다.

  구성 요소가 실행되는 동안 보호 중인 장치 및 보호 중인 장치 그룹에 대해 가능한 모든 시나리오(보호 중인 장치를 한 번 이상 다시 시작하는 경우 포함)를 실행해야 합니다. 저장된 Kaspersky Security Center 이벤트 리포트 파일(TXT 형식)에서 애플리케이션 실행 데이터를 가져와 이 데이터를 기반으로 이러한 애플리케이션에 대한 애플리케이션 실행 제어 허용 규칙을 생성할 수 있습니다.

  이 시나리오는 회사 네트워크에 다양한 유형의 보호 중인 장치(다양한 소프트웨어 설치)가 다수 포함된 경우에 권장됩니다.

- 구성 파일을 생성하거나 가져오지 않고 Kaspersky Security Center를 통해 수신한 애플리케이션 실행 거부 이벤트를 기반으로 합니다.

  이 기능을 사용하려면 보호 중인 장치에서 애플리케이션 실행 제어 구성 요소가 Kaspersky Security Center 정책에 따라 실행되고 있어야 합니다. 이 경우 보호 중인 장치의 모든 이벤트가 중앙 관리 서버로 전송됩니다.

네트워크 보호 중인 장치에 설치된 애플리케이션 세트가 변경된 경우(예: 업데이트 설치 또는 운영 체제 다시 설치) 규칙 목록을 업데이트하는 것이 좋습니다. 테스트 관리 그룹의 보호 중인 장치에서 *애플리케이션 실행 제어를 위한 규칙 생성기* 작업 또는 애플리케이션 실행 제어 구성 요소를 *알림* 모드로 실행하여 업데이트된 규칙 목록을 생성하는 것이 좋습니다. 테스트 관리 그룹에는 네트워크 보호 중인 장치에 설치되기 전에 새 애플리케이션의 실행을 테스트하는 데 필요한 보호 중인 장치가 포함되어 있습니다.

허용 규칙 목록이 포함된 XML 파일은 보호 중인 장치에서 시작된 애플리케이션에 대한 분석을 기반으로 생성됩니다. 규칙 목록 생성 시 네트워크에서 사용 중인 모든 애플리케이션을 고려하려면 *애플리케이션 실행 제어를 위한 규칙 생성기* 작업 및 애플리케이션 실행 제어 구성 요소를 템플릿 머신의 *알림* 모드에서 시작하는 것이 좋습니다.

참조 머신에서 실행된 애플리케이션을 기반으로 허용 규칙 생성을 시작하기 전에 템플릿 머신이 안전하고 악성 코드가 없는지 확인합니다.

허용 규칙을 추가하기 전에 이용 가능한 규칙 적용 모드 중 하나를 선택합니다. Kaspersky Security Center 정책 규칙 목록에는 규칙 적용 모드와 관계없이 정책에 지정된 규칙만 표시됩니다. 로컬 규칙 목록에는 적용된 모든 규칙(로컬 규칙과 정책을 통해 추가된 규칙 모두)이 표시됩니다.

애플리케이션 실행 제어 활성화 및 구성

Kaspersky Security Center 관리 콘솔에서 애플리케이션 실행 제어 일반 설정을 활성화하고 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 섹션으로 갑니다.
4. **애플리케이션 실행 제어** 블록에서 **설정** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
5. **애플리케이션 실행 제어** 확인란을 선택합니다.
6. **차단 규칙 운영 모드** 블록에서, 구성 요소 운영 모드를 선택합니다:
   - **차단**. Kaspersky Industrial CyberSecurity for Nodes가 생성된 모든 애플리케이션 실행 제어 규칙을 적용합니다.
   - **알림**. Kaspersky Industrial CyberSecurity for Nodes가 애플리케이션 실행 제어 규칙을 사용하지 않습니다. 구성 요소의 로그에는 애플리케이션 시작에 관한 정보만 기록합니다. 모든 애플리케이션을 시작할 수 있습니다. 이 모드를 사용하면 구성 요소의 로그에 기록된 거부 애플리케이션 실행 정보를 기반으로 애플리케이션 실행 제어 규칙 목록을 생성할 수 있습니다.
7. 구성 요소 설정을 구성합니다(아래 표 참조).
8. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes가 구성 요소 설정을 즉시 적용합니다. 설정을 수정한 날짜 및 시간에 관한 정보 및 수정 전후의 설정값이 시스템 감사 로그에 저장됩니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 애플리케이션 실행 제어에 대한 일반 설정을 활성화하고 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **컴퓨터 제어 → 애플리케이션 실행 제어** 섹션을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
3. **애플리케이션 실행 제어** 확인란을 선택합니다.
4. **차단 규칙 운영 모드** 블록에서, 구성 요소 운영 모드를 선택합니다:
   - **차단**. Kaspersky Industrial CyberSecurity for Nodes가 생성된 모든 애플리케이션 실행 제어 규칙을 적용합니다.
   - **알림**. Kaspersky Industrial CyberSecurity for Nodes가 애플리케이션 실행 제어 규칙을 사용하지 않습니다. 구성 요소의 로그에는 애플리케이션 시작에 관한 정보만 기록합니다. 모든 애플리케이션을 시작할 수 있습니다. 이 모드를 사용하면 구성 요소의 로그에 기록된 거부 애플리케이션 실행 정보를 기반으로 애플리케이션 실행 제어 규칙 목록을 생성할 수 있습니다.

5. 구성 요소 설정을 구성합니다(아래 표 참조).

6. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes가 구성 요소 설정을 즉시 적용합니다. 설정을 수정한 날짜 및 시간에 관한 정보 및 수정 전후의 설정값이 시스템 감사 로그에 저장됩니다.

Kaspersky Security Center 웹 콘솔에서 애플리케이션 실행 제어 일반 설정을 활성화하고 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어** 섹션을 선택합니다.

5. **애플리케이션 실행 제어** 블록에서 **구성** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.

6. **애플리케이션 실행 제어 사용** 확인란을 선택합니다.

7. **차단 규칙 운영 모드** 블록에서, 구성 요소 운영 모드를 선택합니다:

   - **차단**. Kaspersky Industrial CyberSecurity for Nodes가 생성된 모든 애플리케이션 실행 제어 규칙을 적용합니다.

   - **알림**. Kaspersky Industrial CyberSecurity for Nodes가 애플리케이션 실행 제어 규칙을 사용하지 않습니다. 구성 요소의 로그에는 애플리케이션 시작에 관한 정보만 기록합니다. 모든 애플리케이션을 시작할 수 있습니다. 이 모드를 사용하면 구성 요소의 로그에 기록된 거부 애플리케이션 실행 정보를 기반으로 애플리케이션 실행 제어 규칙 목록을 생성할 수 있습니다.

8. 구성 요소 설정을 구성합니다(아래 표 참조).

9. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes가 구성 요소 설정을 즉시 적용합니다. 설정을 수정한 날짜 및 시간에 관한 정보 및 수정 전후의 설정값이 시스템 감사 로그에 저장됩니다.

애플리케이션 실행 제어 일반 설정

파라미터	설명
이 파일의 모든 후속 실행에서 첫 번째 파일 실행 시 수행한 동작 반복	이 옵션은 캐시에 저장된 이벤트 정보를 기반으로 애플리케이션을 시작하려는 두 번째 이후의 시도에 대한 실행 제어를 활성화하거나 비활성화합니다. 이 옵션을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션의 첫 번째 실행 관련 구성 요소의 결론을 기반으로 애플리케이션의 후속 실행을 허용하거나 거부합니다. 예를 들어 규칙에서 첫 번째 애플리케이션 시작을 허용하면, 이 판단에 관한 정보가 캐시에 저장되고 두 번째 이후 실행은 재확인 없이 허용됩니다. Windows XP를 실행하는 컴퓨터에 애플리케이션을 설치한 경우, 탐색기를 통해 파일 작업을 할 때 첫 번째 애플리케이션 시작 결론을 덮어쓰게 되어 기능이 제대로 작동하지 않을 수 있습니다. 이 옵션을 비활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 실행을 시도할 때마다 애플리케이션을 분석합니다.

파라미터	설명
실행할 명령이 없는 명령 해석기 실행 거부	이 기능을 활성화하면 다음 조건 중 하나라도 충족되는 경우 Kaspersky Industrial CyberSecurity for Nodes는 명령줄 해석기 시작을 거부합니다. • 애플리케이션 실행 제어 규칙에 따라 명령줄 해석기 시작이 거부됩니다. • 명령줄 해석기는 파라미터 없이 시작됩니다. 이 옵션을 비활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 명령줄 해석기를 실행할 때 허용 규칙만 고려합니다. 적용할 수 있는 애플리케이션 실행 제어 허용 규칙이 없으면 실행이 차단됩니다. 애플리케이션 실행 제어의 허용 규칙을 적용하면 실행할 명령의 유무와 관계없이 명령줄 해석기를 실행할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 다음 명령 해석기의 실행을 제어합니다: • cmd.exe • powershell.exe • python.exe • perl.exe • wscript.exe 이 기능은 기본적으로 비활성화됩니다.
실행 파일에 규칙 적용	이 옵션은 실행 파일의 실행 제어를 활성화하거나 비활성화합니다. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 규칙을 사용하여 실행 파일의 실행을 허용하거나 거부합니다. 이 기능을 비활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 규칙을 사용하여 실행 파일의 실행을 제어하지 않습니다. 실행 파일의 시작이 허용됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.
DLL 모듈 로드 모니터링	DLL 모듈의 로드를 제어하면 운영 체제 성능에 영향을 미칠 수 있습니다. 이 기능은 **실행 파일에 규칙 적용** 기능이 활성화된 경우에 사용할 수 있습니다. 이 기능은 DLL 모듈의 로드 제어를 활성화하거나 비활성화합니다. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 규칙을 사용하여 DLL 모듈의 로드를 허용하거나 거부합니다. 이 기능을 비활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 규칙을 사용하여 DLL 모듈의 로드를 제어하지 않습니다. DLL 모듈 로드가 허용됩니다. 이 기능은 기본적으로 비활성화됩니다.
스크립트 및 MSI 패키지에 규칙 적용	이 옵션은 스크립트 및 MSI 패키지의 실행을 활성화하거나 비활성화합니다. 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 규칙을 사용하여 스크립트 및 MSI 패키지의 실행을 허용하거나 거부합니다. 이 확인란을 선택 해제하면 Kaspersky Industrial CyberSecurity for Nodes가 애플리케이션 실행 제어 규칙을 사용하여 스크립트 및 MSI 패키지의 실행을 제어하지 않습니다. 스크립트 및 MSI 패키지의 시작이 허용됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.
인증서 유효성을 검사할 때 누락된 서명 타임스탬프 무시	이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 만료되었거나 만료 날짜가 정의되지 않은 인증서로 서명된 애플리케이션의 실행을 허용합니다. 이 기능을 비활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 만료되었거나 만료 날짜가 정의되지 않은 인증서로 서명된 애플리케이션 실행을 거부합니다. 이 기능은 기본적으로 비활성화됩니다.

소프트웨어 배포 제어 구성

Kaspersky Security Center 관리 콘솔에서 소프트웨어 배포 제어를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 섹션으로 갑니다.
4. **애플리케이션 실행 제어** 블록에서 **설정** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.

5. **소프트웨어 배포 제어** 탭을 선택합니다.

6. **나열된 애플리케이션과 패키지를 통한 소프트웨어 배포 자동 허용** 기능을 활성화하십시오. 이 기능은 목록에 지정된 실행 파일 및 설치 패키지를 사용하여 실행된 모든 파일에 대해 자동으로 예외를 생성합니다.

   일반 탭에서 **실행 파일에 규칙 적용** 기능이 활성화되어 있는 경우 **나열된 애플리케이션과 패키지를 통한 소프트웨어 배포 자동 허용** 기능을 활성화할 수 있습니다.

7. 필요하다면 **Windows Installer를 통한 소프트웨어 배포 항상 허용** 기능을 비활성화하십시오. 이 기능은 Windows Installer을 사용하여 실행된 모든 파일에 대해 예외를 자동으로 생성합니다.

   이 기능을 끄면 운영 체제 파일 업데이트에 문제가 발생하고 배포 패키지에서 추출한 파일의 실행이 차단될 수 있습니다.

8. 필요하다면 **Background Intelligent Transfer Service를 사용하여 SCCM을 통한 소프트웨어 배포 항상 허용** 기능을 활성화하십시오. 이 기능을 사용하면 System Center Configuration Manager 솔루션을 통해 소프트웨어를 배포할 수 있습니다.

   이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes에서 System Center Configuration Manager을 사용하여 Microsoft Windows를 배포할 수 있습니다. 애플리케이션은 Background Intelligent Transfer Service를 통해서만 소프트웨어를 배포할 수 있습니다. 애플리케이션이 .EXE 및 .MSI 확장자 실행 파일의 실행을 제어합니다.

   애플리케이션은 패키지 전달에서 설치/업데이트에 이르기까지 보호 중인 장치의 소프트웨어 배포 주기를 제어합니다. 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치하기 전에 배포 단계가 수행된 경우에는 애플리케이션이 프로세스를 제어하지 않습니다.

9. 실행을 허용할 실행 파일 및 설치 패키지를 추가하십시오:

   - **수동으로 하나 추가**

     a. **추가** 버튼의 마우스 오른쪽 메뉴에서 **배포 패키지 하나 추가** 옵션을 선택합니다.

     b. 열리는 창에서 **찾아보기** 버튼을 클릭합니다.

     c. 실행 파일 또는 배포 패키지를 선택합니다.

     신뢰 기준의 필드가 자동으로 선택 파일에 관한 정보로 채워집니다.

     d. 필요하다면 **모든 자식 파일을 신뢰하는 배포 패키지로 실행 허용** 기능을 활성화하십시오.

     e. 실행 파일 또는 설치 패키지를 신뢰할 수 있는지 결정하는 기준을 선택합니다: **인증서 세부 정보** 또는 **SHA256 해시**.

     f. **확인**을 누릅니다.

     실행 파일 또는 설치 패키지가 목록에 추가됩니다.

- **해시로 여러 개 추가**

  a. **추가** 버튼의 마우스 오른쪽 메뉴에서 **해시를 기준으로 여러 패키지 추가** 옵션을 선택합니다.

  b. 열린 창에서 파일 또는 설치 패키지를 원하는 수만큼 선택합니다.

  c. **열기**를 클릭합니다.

  실행 파일 또는 설치 패키지가 목록에 추가됩니다. SHA256 해시는 해당 속성에 지정됩니다.

- **파일에서 가져오기**

  a. **가져오기** 버튼을 클릭합니다.

  b. 창이 열리면 실행 파일 및 설치 패키지에 관한 정보가 포함된 .TXT 파일을 선택합니다.

  c. **열기**를 클릭합니다.

  실행 파일 또는 설치 패키지가 목록에 추가됩니다. SHA256 해시는 해당 속성에 지정됩니다.

> 실행 파일을 기반으로 신뢰 배포 패키지를 생성하고, 동일한 실행 파일을 기반으로 하는 신뢰 구역 설정에 프로세스를 추가하여 애플리케이션 실행 제어 구성 요소에 대해 신뢰하도록 설정하는 경우, 신뢰 구역 설정이 더 높은 우선순위를 가집니다. Kaspersky Industrial CyberSecurity for Nodes는 이 실행 파일의 시작을 차단하지만 실행 파일의 프로세스를 신뢰할 수 있는 것으로 간주합니다.

10. 필요하다면 **편집** 버튼을 클릭해 추가된 실행 파일 및 설치 패키지 목록을 편집하십시오.

11. 필요하다면 **삭제** 버튼을 클릭해 추가된 실행 파일 및 설치 패키지 목록을 제거하십시오. 이 경우 압축이 해제된 실행 파일을 실행할 수 있습니다.

> 압축 해제된 실행 파일이 실행되지 않도록 하려면 보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes를 제거하거나 압축 해제 파일에 대한 애플리케이션 실행 제어 거부 규칙을 생성해야 합니다.

12. **확인** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 소프트웨어 배포 제어를 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **컴퓨터 제어 → 애플리케이션 실행 제어** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.

3. **소프트웨어 배포 제어** 탭을 선택합니다.

4. **나열된 애플리케이션과 패키지를 통한 소프트웨어 배포 자동 허용** 기능을 활성화하십시오. 이 기능은 목록에 지정된 실행 파일 및 설치 패키지를 사용하여 실행된 모든 파일에 대해 자동으로 예외를 생성합니다.

> **일반** 탭에서 **실행 파일에 규칙 적용** 기능이 활성화되어 있는 경우 **나열된 애플리케이션과 패키지를 통한 소프트웨어 배포 자동 허용** 기능을 활성화할 수 있습니다.

5. 필요하다면 **Windows Installer를 통한 소프트웨어 배포 항상 허용** 기능을 비활성화하십시오. 이 기능은 Windows Installer을 사용하여 실행된 모든 파일에 대해 예외를 자동으로 생성합니다.

   이 기능을 끄면 운영 체제 파일 업데이트에 문제가 발생하고 배포 패키지에서 추출한 파일의 실행이 차단될 수 있습니다.

6. 필요하다면 **Background Intelligent Transfer Service를 사용하여 SCCM을 통한 소프트웨어 배포 항상 허용** 기능을 활성화하십시오. 이 기능을 사용하면 System Center Configuration Manager 솔루션을 통해 소프트웨어를 배포할 수 있습니다.

   이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes에서 System Center Configuration Manager을 사용하여 Microsoft Windows를 배포할 수 있습니다. 애플리케이션은 Background Intelligent Transfer Service를 통해서만 소프트웨어를 배포할 수 있습니다. 애플리케이션이 .EXE 및 .MSI 확장자 실행 파일의 실행을 제어합니다.

   애플리케이션은 패키지 전달에서 설치/업데이트에 이르기까지 보호 중인 장치의 소프트웨어 배포 주기를 제어합니다. 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치하기 전에 배포 단계가 수행된 경우에는 애플리케이션이 프로세스를 제어하지 않습니다.

7. 실행을 허용할 실행 파일 및 설치 패키지를 추가하십시오:

   - **수동으로 하나 추가**

     a. **추가** 버튼의 마우스 오른쪽 메뉴에서 **배포 패키지 하나 추가** 옵션을 선택합니다.

     b. 열리는 창에서 **찾아보기** 버튼을 클릭합니다.

     c. 실행 파일 또는 배포 패키지를 선택합니다.

     신뢰 기준의 필드가 자동으로 선택 파일에 관한 정보로 채워집니다.

     d. 필요하다면 **모든 자식 파일을 신뢰하는 배포 패키지로 실행 허용** 기능을 활성화하십시오.

     e. 실행 파일 또는 설치 패키지를 신뢰할 수 있는지 결정하는 기준을 선택합니다: **인증서 세부 정보** 또는 **SHA256 해시**.

     f. **확인**을 누릅니다.

     실행 파일 또는 설치 패키지가 목록에 추가됩니다.

   - **해시로 여러 개 추가**

     a. **추가** 버튼의 마우스 오른쪽 메뉴에서 **해시를 기준으로 여러 패키지 추가** 옵션을 선택합니다.

     b. 열린 창에서 파일 또는 설치 패키지를 원하는 수만큼 선택합니다.

     c. **열기**를 클릭합니다.

     실행 파일 또는 설치 패키지가 목록에 추가됩니다. SHA256 해시는 해당 속성에 지정됩니다.

- **파일에서 가져오기**

  a. **가져오기** 버튼을 클릭합니다.

  b. 창이 열리면 실행 파일 및 설치 패키지에 관한 정보가 포함된 .TXT 파일을 선택합니다.

  c. **열기**를 클릭합니다.

  실행 파일 또는 설치 패키지가 목록에 추가됩니다. SHA256 해시는 해당 속성에 지정됩니다.

실행 파일을 기반으로 신뢰 배포 패키지를 생성하고, 동일한 실행 파일을 기반으로 하는 신뢰 구역 설정에 프로세스를 추가하여 애플리케이션 실행 제어 구성 요소에 대해 신뢰하도록 설정하는 경우, 신뢰 구역 설정이 더 높은 우선순위를 가집니다. Kaspersky Industrial CyberSecurity for Nodes는 이 실행 파일의 시작을 차단하지만 실행 파일의 프로세스를 신뢰할 수 있는 것으로 간주합니다.

8. 필요하다면 **편집** 버튼을 클릭해 추가된 실행 파일 및 설치 패키지 목록을 편집하십시오.
9. 필요하다면 **삭제** 버튼을 클릭해 추가된 실행 파일 및 설치 패키지 목록을 제거하십시오. 이 경우 압축이 해제된 실행 파일을 실행할 수 있습니다.

압축 해제된 실행 파일이 실행되지 않도록 하려면 보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes를 제거하거나 압축 해제 파일에 대한 애플리케이션 실행 제어 거부 규칙을 생성해야 합니다.

10. **확인** 버튼을 클릭합니다.

Kaspersky Security Center 웹 콘솔에서 소프트웨어 배포 제어를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **로컬 활동 제어** 섹션을 선택합니다.
5. **애플리케이션 실행 제어** 블록에서 **구성** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
6. **소프트웨어 배포 제어** 탭을 선택합니다.
7. **나열된 애플리케이션과 패키지를 통한 소프트웨어 배포 자동 허용** 기능을 활성화하십시오. 이 기능은 목록에 지정된 실행 파일 및 설치 패키지를 사용하여 실행된 모든 파일에 대해 자동으로 예외를 생성합니다.

일반 탭에서 **실행 파일에 규칙 적용** 기능이 활성화되어 있는 경우 **나열된 애플리케이션과 패키지를 통한 소프트웨어 배포 자동 허용** 기능을 활성화할 수 있습니다.

8. 필요하다면 **Windows Installer를 통한 소프트웨어 배포 항상 허용** 기능을 비활성화하십시오. 이 기능은 Windows Installer을 사용하여 실행된 모든 파일에 대해 예외를 자동으로 생성합니다.

   이 기능을 끄면 운영 체제 파일 업데이트에 문제가 발생하고 배포 패키지에서 추출한 파일의 실행이 차단될 수 있습니다.

9. 필요하다면 **Background Intelligent Transfer Service를 사용하여 SCCM을 통한 소프트웨어 배포 항상 허용** 기능을 활성화하십시오. 이 기능을 사용하면 System Center Configuration Manager 솔루션을 통해 소프트웨어를 배포할 수 있습니다.

   이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes에서 System Center Configuration Manager을 사용하여 Microsoft Windows를 배포할 수 있습니다. 애플리케이션은 Background Intelligent Transfer Service를 통해서만 소프트웨어를 배포할 수 있습니다. 애플리케이션이 .EXE 및 .MSI 확장자 실행 파일의 실행을 제어합니다.

   애플리케이션은 패키지 전달에서 설치/업데이트에 이르기까지 보호 중인 장치의 소프트웨어 배포 주기를 제어합니다. 보호 중인 장치에 Kaspersky Industrial CyberSecurity for Nodes를 설치하기 전에 배포 단계가 수행된 경우에는 애플리케이션이 프로세스를 제어하지 않습니다.

10. 실행을 허용할 실행 파일 및 설치 패키지를 추가하십시오:

    - **수동**

      a. **추가** 버튼을 누릅니다.

      b. **신뢰 기준**에서 실행 파일 또는 설치 패키지를 신뢰할 수 있는지 결정하는 기준을 선택합니다: **디지털 인증서 사용** 또는 **SHA256 해시 사용**.

      c. **디지털 인증서 사용** 옵션을 선택했다면 실행 파일 또는 설치 패키지 서명에 사용된 인증서의 헤더 및 지문과 실행 파일 또는 설치 패키지의 이름을 입력합니다.

      d. **SHA256 해시 사용** 옵션을 선택했다면 **찾아보기**를 클릭해 실행 파일 또는 설치 패키지를 선택합니다.

      e. 필요하다면 **모든 자식 파일을 신뢰하는 배포 패키지로 실행 허용** 기능을 활성화하십시오.

      f. **확인**을 누릅니다.

      실행 파일 또는 설치 패키지가 목록에 추가됩니다.

    - **파일에서 가져오기**

      a. **가져오기** 버튼을 클릭합니다.

      b. 창이 열리면 실행 파일 및 설치 패키지에 관한 정보가 포함된 .TXT 파일을 선택합니다.

      c. **열기** 버튼을 클릭합니다.

      실행 파일 또는 설치 패키지가 목록에 추가됩니다. SHA256 해시는 해당 속성에 지정됩니다.

실행 파일을 기반으로 신뢰 배포 패키지를 생성하고, 동일한 실행 파일을 기반으로 하는 신뢰 구역 설정에 프로세스를 추가하여 애플리케이션 실행 제어 구성 요소에 대해 신뢰하도록 설정하는 경우, 신뢰 구역 설정이 더 높은 우선순위를 가집니다. Kaspersky Industrial CyberSecurity for Nodes는 이 실행 파일의 시작을 차단하지만 실행 파일의 프로세스를 신뢰할 수 있는 것으로 간주합니다.

11. 필요하다면 **편집** 버튼을 클릭해 추가된 실행 파일 및 설치 패키지 목록을 편집하십시오.
12. 필요하다면 **삭제** 버튼을 클릭해 추가된 실행 파일 및 설치 패키지 목록을 제거하십시오. 이 경우 압축이 해제된 실행 파일을 실행할 수 있습니다.

압축 해제된 실행 파일이 실행되지 않도록 하려면 보호 중인 장치에서 Kaspersky Industrial CyberSecurity for Nodes를 제거하거나 압축 해제 파일에 대한 애플리케이션 실행 제어 거부 규칙을 생성해야 합니다.

13. **확인** 버튼을 클릭합니다.
14. **애플리케이션 실행 제어** 창의 **확인** 버튼을 클릭합니다.

애플리케이션 실행 제어 규칙 작업 방법

이 섹션에서는 애플리케이션 실행 제어에 대한 규칙 목록을 생성하는 방법이 제공됩니다.

애플리케이션 실행 제어 규칙 추가

Kaspersky Security Center 관리 콘솔에 애플리케이션 실행 제어 규칙을 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 섹션으로 갑니다.
4. **애플리케이션 실행 제어** 블록에서 **설정** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
5. **규칙** 탭을 선택합니다.
6. **규칙 사용** 드롭다운 목록에서 규칙 적용 모드를 선택합니다.
   - **로컬 규칙에 정책 규칙 추가**. 애플리케이션은 로컬 규칙 목록과 함께 정책에 지정된 규칙 목록을 적용합니다.
   - **로컬 규칙을 정책 규칙으로 교체**. 애플리케이션은 보호 중인 장치 그룹에서 애플리케이션 실행 제어를 위해 정책에 지정된 규칙 목록을 적용합니다. 로컬 규칙 목록은 작성, 편집 또는 적용될 수 없습니다.
7. 필요하다면 **사용자의 로컬 규칙 수정 거부** 기능을 활성화하십시오.
   이 기능을 활성화하면 애플리케이션이 애플리케이션 콘솔에서 로컬로 애플리케이션 실행 제어 규칙을 편집하는 것을 허용하지 않습니다. 이 기능은 기본적으로 비활성화됩니다.

8. 다음 방법 중 하나를 사용하여 애플리케이션 실행 제어 규칙을 추가하십시오.

- **수동**

  a. **추가** 버튼을 클릭합니다.
  애플리케이션 실행 제어 창이 열립니다.

  b. **이름** 필드에서 규칙의 이름을 입력합니다.

  c. 필요하다면 **설명** 필드에서 규칙의 설명을 입력합니다.

  d. **유형** 드롭다운 목록에서 규칙 유형을 선택합니다:

  - **허용** 규칙에 설명된 애플리케이션 실행을 허용하는 규칙이 필요한 경우.
  - **거부** 규칙에 설명된 애플리케이션 실행을 차단하는 규칙이 필요한 경우.

  e. **범위** 드롭다운 목록에서 규칙에 따라 실행을 제어할 파일 유형을 선택합니다:

  - **실행 파일**: 실행 파일의 실행을 제어하는 규칙이 필요한 경우.
  - **스크립트 및 MSI 패키지**: 스크립트 및 MSI 패키지의 실행을 제어하는 규칙이 필요한 경우. 확장자가.js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct인 파일이 지원됩니다.

  f. Kaspersky Industrial CyberSecurity for Nodes가 규칙 트리거 조건과 일치하는 애플리케이션을 신뢰하는 업데이터로 간주하도록 하려면 **신뢰하는 업데이터** 확인란을 선택합니다. 신뢰하는 업데이터는 이후에 실행할 수 있는 다른 실행 파일을 생성할 수 있는 애플리케이션입니다.
  애플리케이션이 여러 규칙을 트리거한다면, Kaspersky Industrial CyberSecurity for Nodes는 다음 조건 충족 시에 *신뢰하는 업데이터* 플래그를 설정합니다.

  - 모든 규칙은 애플리케이션 실행을 허용합니다.
  - 적어도 하나의 규칙에 **신뢰하는 업데이터** 확인란이 선택되어 있습니다.

  g. 애플리케이션 실행 제어 규칙에 대한 트리거 조건을 추가하십시오.

  h. 애플리케이션 실행 제어 규칙의 트리거 조건에서 예외를 추가하십시오.

  i. 규칙을 충족하는 애플리케이션 실행을 허용하거나 금지하는 사용자 또는 사용자 그룹을 추가하십시오.

  j. **확인**을 누릅니다.

- **애플리케이션 실행 제어 규칙이 포함된 XML 파일을 가져옵니다**

  a. 버튼의 마우스 오른쪽 메뉴에서 **가져오기 → XML 파일로부터** 항목을 선택합니다.

  b. XML 파일에서 정책에 적용할 수 있는 장치 제어 규칙을 추가하는 방법을 선택합니다:

  - **기존 규칙 교체**: 가져온 규칙으로 기존 규칙을 바꾸려는 경우.
  - **기존 규칙에 추가**: 기존 규칙 목록에 가져온 규칙을 추가하려는 경우. 설정이 같은 규칙은 중복됩니다.
  - **기존 규칙과 병합**: 기존 규칙 목록에 가져온 규칙을 추가하려는 경우. 설정이 같은 규칙이 중복되지 않습니다. 하나 이상의 규칙 설정이 고유하면 규칙이 추가됩니다.

  c. 창이 열리면 *애플리케이션 실행 제어를 위한 규칙 생성기*에 대한 로컬 작업 또는 그룹 작업 완료 후 생성된 XML 파일의 경로를 지정합니다.

  d. **열기** 버튼을 클릭합니다.

- **요청을 사용하는 Kaspersky Security Center 이벤트 기준**

  a. 버튼의 마우스 오른쪽 메뉴에서 **가져오기 → Kaspersky Security Center 이벤트를 기반으로 허용 규칙 생성(요청)** 항목을 선택합니다.

  b. 이전에 생성된 애플리케이션 실행 제어 규칙 목록에 규칙을 추가하는 원칙을 선택합니다.

  - **기존 규칙에 추가**: 기존 규칙 목록에 가져온 규칙을 추가하려는 경우. 설정이 같은 규칙은 중복됩니다.
  - **기존 규칙 교체**: 가져온 규칙으로 기존 규칙을 바꾸려는 경우.
  - **기존 규칙과 병합**: 기존 규칙 목록에 가져온 규칙을 추가하려는 경우. 동일한 설정이 추가되지 않은 규칙, 한 개 이상의 규칙 파라미터가 고유하다면 규칙이 추가됩니다.

  애플리케이션 실행 제어 규칙 생성 창이 열립니다.

  c. 애플리케이션이 애플리케이션 실행 제어 규칙을 생성할 때 사용할 이벤트 유형을 선택합니다.

  - **애플리케이션 실행 거부됨**.
  - **통계 전용 모드: 애플리케이션 실행이 거부됨**.

  d. **기간 내에 생성된 요청 이벤트** 드롭다운 목록에서 기간을 선택합니다.

  e. **규칙 생성 시 해시 사용에 우선 순위 부여** 확인란을 선택 해제하거나 선택합니다.

  이 확인란을 선택하면 파일의 체크섬과 인증서를 모두 사용할 수 있을 때 Kaspersky Industrial CyberSecurity for Nodes가 파일의 체크섬을 사용하여 규칙을 생성합니다.

  이 확인란을 선택 해제하면 파일의 체크섬과 인증서를 모두 사용할 수 있을 때 Kaspersky Industrial CyberSecurity for Nodes가 파일의 디지털 인증서를 사용하여 규칙을 생성합니다.

  f. **규칙 생성** 버튼을 클릭합니다.

  g. **확인** 버튼을 클릭합니다.

- **Kaspersky Security Center 차단된 애플리케이션 이벤트 조회가 포함된 텍스트 파일을 가져오기**

  1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
  2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
  3. 정책 속성 창에서 **로그 및 알림** 섹션으로 갑니다.
  4. **작업 로그** 블록에서 **설정** 버튼을 클릭합니다.
     알림 창이 열립니다.
  5. **로컬 활동 제어** 노드를 확장합니다.
  6. **애플리케이션 실행 제어** 섹션을 선택합니다.
  7. 애플리케이션 실행 제어 이벤트 목록에서, **Kaspersky Security Center로 이벤트 전송** 열에서 *애플리케이션 시작이 금지됨* 그리고 *테스트 모드에서 애플리케이션 시작이 금지됨* 옆에 있는 확인란을 선택합니다.
  8. 변경 사항을 저장합니다.
  9. 정책의 **이벤트 구성** 섹션에서 **다음 기간만큼 중앙 관리 서버에 저장(일)** 필드에 지정된 이벤트 저장 기간이 차단된 애플리케이션 실행에 관한 정보를 수집할 기간(기본값은 30일)보다 긴지 확인하십시오.

     > 애플리케이션 실행 제어 구성 요소 로그 보존 기간이 만료되면 기록된 이벤트는 삭제되며 리포트에 표시되지 않습니다.

  10. 거부된 애플리케이션 실행에 관한 데이터를 수집하도록 구성된 정책을 활성화하십시오.
  11. 필요하다면 애플리케이션 실행 제어 모드를 수정하십시오.
  12. 차단된 애플리케이션 실행에 관한 정보 수집 기간이 만료되면 *애플리케이션 시작이 금지됨* 그리고 *테스트 모드에서 애플리케이션 시작이 금지됨* 이벤트 중에서 선택하여 텍스트 파일로 내보내십시오. 자세한 내용은 Kaspersky Security Center 도움말의 "이벤트 조회" 섹션을 참조하십시오.
  13. 내보낸 텍스트 파일을 엽니다.
  14. 필요하다면 이벤트 목록을 편집하십시오.

  추가된 애플리케이션 실행 제어 규칙이 목록에 표시됩니다.

9. 필요하다면 5단계를 수행하여 애플리케이션 실행 제어 규칙을 더 추가하십시오.
10. 필요하다면 **편집** 버튼을 클릭해 추가된 애플리케이션 실행 제어 규칙을 편집하십시오.
11. 필요하다면 **삭제** 버튼을 클릭해 추가된 애플리케이션 실행 제어 규칙을 삭제하십시오.
12. **확인** 버튼을 클릭합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 애플리케이션 실행 제어 규칙을 추가하는 방법

1. 애플리케이션 콘솔 트리에서 **컴퓨터 제어** → **애플리케이션 실행 제어** 섹션을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
3. **규칙** 탭을 선택합니다.
4. 다음 방법 중 하나를 사용하여 애플리케이션 실행 제어 규칙을 추가하십시오.

- **수동**

  a. **추가** 버튼을 클릭합니다.
  애플리케이션 실행 제어 창이 열립니다.

  b. **이름** 필드에서 규칙의 이름을 입력합니다.

  c. 필요하다면 **설명** 필드에서 규칙의 설명을 입력합니다.

  d. **유형** 드롭다운 목록에서 규칙 유형을 선택합니다:

  - **허용** 규칙에 설명된 애플리케이션 실행을 허용하는 규칙이 필요한 경우.
  - **거부** 규칙에 설명된 애플리케이션 실행을 차단하는 규칙이 필요한 경우.

  e. **범위** 드롭다운 목록에서 규칙에 따라 실행을 제어할 파일 유형을 선택합니다:

  - **실행 파일**: 실행 파일의 실행을 제어하는 규칙이 필요한 경우.
  - **스크립트 및 MSI 패키지**: 스크립트 및 MSI 패키지의 실행을 제어하는 규칙이 필요한 경우. 확장자가.js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct인 파일이 지원됩니다.

  f. Kaspersky Industrial CyberSecurity for Nodes가 규칙 트리거 조건과 일치하는 애플리케이션을 신뢰하는 업데이터로 간주하도록 하려면 **신뢰하는 업데이터** 확인란을 선택합니다. 신뢰하는 업데이터는 이후에 실행할 수 있는 다른 실행 파일을 생성할 수 있는 애플리케이션입니다.
  애플리케이션이 여러 규칙을 트리거한다면, Kaspersky Industrial CyberSecurity for Nodes는 다음 조건 충족 시에 *신뢰하는 업데이터* 플래그를 설정합니다.

  - 모든 규칙은 애플리케이션 실행을 허용합니다.
  - 적어도 하나의 규칙에 **신뢰하는 업데이터** 확인란이 선택되어 있습니다.

  g. 애플리케이션 실행 제어 규칙에 대한 트리거 조건을 추가하십시오.

  h. 애플리케이션 실행 제어 규칙의 트리거 조건에서 예외를 추가하십시오.

  i. 규칙을 충족하는 애플리케이션 실행을 허용하거나 금지하는 사용자 또는 사용자 그룹을 추가하십시오.

  j. **확인**을 누릅니다.

- **애플리케이션 실행 제어 규칙이 포함된 XML 파일을 가져옵니다**

  a. 버튼의 마우스 오른쪽 메뉴에서 **가져오기 → XML 파일로부터** 항목을 선택합니다.

  b. XML 파일에서 정책에 적용할 수 있는 장치 제어 규칙을 추가하는 방법을 선택합니다:

  - **기존 규칙 교체**: 가져온 규칙으로 기존 규칙을 바꾸려는 경우.
  - **기존 규칙에 추가**: 기존 규칙 목록에 가져온 규칙을 추가하려는 경우. 설정이 같은 규칙은 중복됩니다.
  - **기존 규칙과 병합**: 기존 규칙 목록에 가져온 규칙을 추가하려는 경우. 설정이 같은 규칙이 중복되지 않습니다. 하나 이상의 규칙 설정이 고유하면 규칙이 추가됩니다.

  c. 창이 열리면 *애플리케이션 실행 제어를 위한 규칙 생성기*에 대한 로컬 작업 또는 그룹 작업 완료 후 생성된 XML 파일의 경로를 지정합니다.

  d. **열기** 버튼을 클릭합니다.

추가된 애플리케이션 실행 제어 규칙이 목록에 표시됩니다.

5. 필요하다면 5단계를 수행하여 애플리케이션 실행 제어 규칙을 더 추가하십시오.
6. 필요하다면 **편집** 버튼을 클릭해 추가된 애플리케이션 실행 제어 규칙을 편집하십시오.
7. 필요하다면 **삭제** 버튼을 클릭해 추가된 애플리케이션 실행 제어 규칙을 삭제하십시오.
8. **확인** 버튼을 클릭합니다.

Kaspersky Security Center 웹 콘솔에서 애플리케이션 실행 제어 규칙을 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **로컬 활동 제어** 섹션을 선택합니다.
5. **애플리케이션 실행 제어** 블록에서 **구성** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
6. **규칙** 탭을 선택합니다.
7. **규칙 적용** 드롭다운 목록에서 규칙 적용 모드를 선택합니다.
   - **로컬 규칙에 정책 규칙 추가**. 애플리케이션은 로컬 규칙 목록과 함께 정책에 지정된 규칙 목록을 적용합니다.
   - **로컬 규칙을 정책 규칙으로 교체**. 애플리케이션은 보호 중인 장치 그룹에서 애플리케이션 실행 제어를 위해 정책에 지정된 규칙 목록을 적용합니다. 로컬 규칙 목록은 작성, 편집 또는 적용될 수 없습니다.
8. 필요하다면 **사용자의 로컬 규칙 수정 거부** 기능을 활성화하십시오.
   이 기능을 활성화하면 애플리케이션이 애플리케이션 콘솔에서 로컬로 애플리케이션 실행 제어 규칙을 편집하는 것을 허용하지 않습니다. 이 기능은 기본적으로 비활성화됩니다.

9. 다음 방법 중 하나를 사용하여 애플리케이션 실행 제어 규칙을 추가하십시오.

- **수동**

  a. **추가** 버튼을 클릭합니다.
  규칙 설정 창이 열립니다.

  b. **이름** 필드에서 규칙의 이름을 입력합니다.

  c. **유형** 드롭다운 목록에서 규칙 유형을 선택합니다:

  - **허용** 규칙에 설명된 애플리케이션 실행을 허용하는 규칙이 필요한 경우.
  - **거부** 규칙에 설명된 애플리케이션 실행을 차단하는 규칙이 필요한 경우.

  d. **범위** 드롭다운 목록에서 규칙에 따라 실행을 제어할 파일 유형을 선택합니다:

  - **실행 파일**: 실행 파일의 실행을 제어하는 규칙이 필요한 경우.
  - **스크립트 및 MSI 패키지**: 스크립트 및 MSI 패키지의 실행을 제어하는 규칙이 필요한 경우.

  e. **사용자/그룹** 탭에 나열되지 않은 모든 사용자에 대해 규칙에 설명된 애플리케이션의 실행을 애플리케이션이 차단하게 하려면 **다른 사용자 거부** 확인란을 선택합니다.

  f. Kaspersky Industrial CyberSecurity for Nodes가 규칙 트리거 조건과 일치하는 애플리케이션을 신뢰하는 업데이터로 간주하도록 하려면 **신뢰하는 업데이터** 확인란을 선택합니다. 신뢰하는 업데이터는 이후에 실행할 수 있는 다른 실행 파일을 생성할 수 있는 애플리케이션입니다.
  애플리케이션이 여러 규칙을 트리거한다면, Kaspersky Industrial CyberSecurity for Nodes는 다음 조건 충족 시에 *신뢰하는 업데이터* 플래그를 설정합니다.

  - 모든 규칙은 애플리케이션 실행을 허용합니다.
  - 적어도 하나의 규칙에 **신뢰하는 업데이터** 확인란이 선택되어 있습니다.

  g. 애플리케이션 실행 제어 규칙에 대한 트리거 조건을 추가하십시오.

  h. 애플리케이션 실행 제어 규칙의 트리거 조건에서 예외를 추가하십시오.

  i. **규칙을 충족하는 애플리케이션 실행을 허용하거나 금지하는 사용자 또는 사용자 그룹을 추가하십시오**.

  a. **사용자/그룹** 탭을 선택합니다.

  b. **추가** 버튼을 클릭합니다.

  c. 열린 창에서 사용자 또는 사용자 그룹의 이름을 입력하거나 선택합니다.

  d. **선택** 버튼을 클릭합니다.

  e. 모든 사용자 또는 사용자 그룹에 대해 b~d 단계를 완료하십시오.

  j. **확인**을 누릅니다.

  추가된 애플리케이션 실행 제어 규칙이 목록에 표시됩니다.

- **애플리케이션 실행 제어 규칙이 포함된 XML 파일을 가져옵니다**

  a. **가져오기** 버튼을 클릭합니다.

  b. 표시된 **파일에서 가져오기** 창에서 **선택** 버튼을 클릭합니다.

  c. *애플리케이션 실행 제어를 위한 규칙 생성기*에 대한 로컬 작업 또는 그룹 작업 완료 후 생성된 XML 파일의 경로를 지정합니다.

  d. **열기** 버튼을 클릭합니다.

  e. **가져오기** 버튼을 클릭합니다.

  가져온 애플리케이션 실행 제어 규칙이 기존 규칙 목록에 추가됩니다. 설정이 같은 규칙이 중복되지 않습니다. 하나 이상의 규칙 설정이 고유하면 규칙이 추가됩니다.

- **Kaspersky Industrial CyberSecurity for Nodes 4.0 애플리케이션 실행 제어 규칙이 포함된 XML 파일을 가져옵니다**

  a. **이전 버전에서 가져오기** 버튼을 클릭합니다.

  b. 표시된 **파일에서 가져오기** 창에서 **선택** 버튼을 클릭합니다.

  c. Kaspersky Industrial CyberSecurity for Nodes 4.0에서 내보낸 애플리케이션 실행 제어 규칙이 포함된 XML 파일의 경로를 지정합니다.

  d. **열기**를 클릭합니다.

  e. **가져오기** 버튼을 클릭합니다.

  가져온 애플리케이션 실행 제어 규칙이 기존 규칙 목록에 추가됩니다. 설정이 같은 규칙이 중복되지 않습니다. 하나 이상의 규칙 설정이 고유하면 규칙이 추가됩니다.

- **Kaspersky Security Center 리포트 파일에서 규칙을 가져옵니다**

  a. **KSC 리포트에서 가져오기** 버튼을 클릭합니다.

  b. 열린 창에서 리포트의 이벤트를 내보낸 TXT 파일을 선택합니다.

  c. **열기**를 클릭합니다.

  Kaspersky Security Center 리포트 기반 규칙이 정책의 규칙 목록에 추가됩니다.

- **요청을 사용하는 Kaspersky Security Center 이벤트 기준**

  a. **KSC 이벤트의 허용 규칙** 버튼을 클릭합니다.
  애플리케이션 실행 제어를 위한 규칙 생성기 창이 열립니다.

  b. 애플리케이션이 애플리케이션 실행 제어 규칙을 생성할 때 사용할 이벤트 유형을 선택합니다.

  - **모든 이벤트**.
  - **애플리케이션 실행 거부됨**.
  - **통계 전용 모드: 애플리케이션 실행이 거부됨**.

c. **기간 내에 생성된 이벤트 사용** 드롭다운 목록에서 기간을 선택합니다.

d. **규칙 생성 시 해시 사용에 우선 순위 부여** 확인란을 선택 해제하거나 선택합니다.

이 확인란을 선택하면 파일의 체크섬과 인증서를 모두 사용할 수 있을 때 Kaspersky Industrial CyberSecurity for Nodes가 파일의 체크섬을 사용하여 규칙을 생성합니다.

이 확인란을 선택 해제하면 파일의 체크섬과 인증서를 모두 사용할 수 있을 때 Kaspersky Industrial CyberSecurity for Nodes가 파일의 디지털 인증서를 사용하여 규칙을 생성합니다.

e. 필요하다면 **관리 중인 장치 그룹에 대해 생성된 이벤트 사용** 필드에서 관리 중인 장치 그룹 이름을 지정합니다.

f. **규칙 생성** 버튼을 클릭합니다.

g. **주 목록에 추가하기 위한 규칙** 드롭다운 목록에서 이전에 생성된 애플리케이션 실행 제어 규칙 목록에 규칙을 추가하는 원칙을 선택합니다.

- **기존 규칙에 추가**: 기존 규칙 목록에 가져온 규칙을 추가하려는 경우. 설정이 같은 규칙은 중복됩니다.
- **기존 규칙 교체**: 가져온 규칙으로 기존 규칙을 바꾸려는 경우.

h. 정책의 애플리케이션 시작 제어 규칙으로 내보낼 규칙을 선택하고 **내보내기** 버튼을 클릭합니다.

i. 변경 사항을 저장합니다.

10. 필요하다면 5단계를 수행하여 애플리케이션 실행 제어 규칙을 더 추가하십시오.
11. 필요하다면 **편집** 버튼을 클릭해 추가된 애플리케이션 실행 제어 규칙을 편집하십시오.
12. 필요하다면 **삭제** 버튼을 클릭해 추가된 애플리케이션 실행 제어 규칙을 삭제하십시오.
13. **확인** 버튼을 클릭합니다.

애플리케이션 실행 제어 규칙의 트리거 조건 추가

Kaspersky Security Center 관리 콘솔에서 애플리케이션 실행 제어 규칙의 트리거 조건을 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 섹션으로 갑니다.
4. **애플리케이션 실행 제어** 블록에서 **설정** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
5. **규칙** 탭을 선택합니다.

6. 다음 중 하나를 수행합니다:

   a. 새 애플리케이션 실행 제어 규칙을 추가하는 경우 **추가** 버튼을 클릭합니다.

   b. 애플리케이션 실행 제어 규칙 목록에서 트리거 조건을 추가할 규칙을 선택하고 **편집** 버튼을 클릭합니다.

   애플리케이션 실행 제어 창이 열립니다.

7. **조건** 탭의 **추가** 버튼 마우스 오른쪽 메뉴에서 애플리케이션 실행 제어 규칙의 트리거 조건을 선택합니다:

- **파일의 정보**. **선택한 파일의 정보**가 규칙 트리거 조건으로 사용됩니다.

  a. **파일의 정보** 창의 **찾아보기** 버튼을 클릭합니다.
  표준 Microsoft Windows **파일 열기** 창이 열립니다.

  b. 파일을 선택합니다.

  c. **열기**를 클릭합니다.
  선택한 파일에 관한 정보가 **파일의 정보** 창에 표시됩니다.

  d. 옵션을 하나 이상 선택합니다:

  - **인증서 세부 정보**. 이 확인란을 선택하면 지정된 데이터가 있는 디지털 인증서로 서명된 애플리케이션의 실행을 규칙이 제어하지 않습니다.
  - **메타데이터**. 이 확인란을 선택하면 지정된 메타데이터가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
  - **파일 해시**. 이 확인란을 선택하면 지정된 SHA256 해시가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
  - **파일 경로**. 이 확인란을 선택하면 지정된 경로에서의 애플리케이션 실행을 규칙이 제어하지 않습니다.

  e. 필요하다면 **명령줄** 필드에 명령줄에서 애플리케이션을 시작하기 위한 명령을 입력합니다. 해당 규칙은 이 애플리케이션의 실행을 제어합니다. ? 및 * 문자를 사용하여 마스크를 입력할 수 있습니다.

  > Kaspersky Industrial CyberSecurity for Nodes는 슬래시("/")가 포함된 경로를 인식하지 못합니다. 경로에 백슬래시 문자("\")를 사용합니다.

  f. **확인** 버튼을 클릭합니다.

- **드라이브 유형**. 이 규칙은 보호 중인 컴퓨터에 연결된 모든 이동식 드라이브의 애플리케이션 실행을 제어합니다.
- **KL 카테고리**. 이 규칙은 선택한 KL 카테고리에 속하는 애플리케이션의 실행을 제어합니다.
- **KSN이 신뢰함**. 이 규칙은 KSN에서 신뢰하는 애플리케이션의 실행을 제어합니다.
- **KSN이 신뢰하지 않음**. 이 규칙은 KSN에서 신뢰하지 않는 애플리케이션의 실행을 제어합니다.
- **OS가 신뢰함**. 이 규칙은 운영 체제에서 신뢰하는 애플리케이션의 실행을 제어합니다.

추가된 조건이 목록에 표시됩니다.

8. 필요하다면 각 후속 규칙 트리거 조건에 지침의 이전 단계를 수행합니다.

9. 필요하다면 **편집** 버튼을 클릭해 규칙 트리거 조건을 편집합니다.

10. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 애플리케이션 실행 제어 규칙의 트리거 조건을 추가하는 방법

1. 애플리케이션 콘솔 트리에서 **컴퓨터 제어 → 애플리케이션 실행 제어** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.

3. **규칙** 탭을 선택합니다.

4. 다음 중 하나를 수행합니다:

   a. 새 애플리케이션 실행 제어 규칙을 추가하는 경우 **추가** 버튼을 클릭합니다.

   b. 애플리케이션 실행 제어 규칙 목록에서 트리거 조건을 추가할 규칙을 선택하고 **편집** 버튼을 클릭합니다.

   애플리케이션 실행 제어 창이 열립니다.

5. **조건** 탭의 **추가** 버튼 마우스 오른쪽 메뉴에서 애플리케이션 실행 제어 규칙의 트리거 조건을 선택합니다:

   - **파일의 정보**. **선택한 파일의 정보**가 규칙 트리거 조건으로 사용됩니다.

     a. **파일의 정보** 창의 **찾아보기** 버튼을 클릭합니다.
     표준 Microsoft Windows **파일 열기** 창이 열립니다.

     b. 파일을 선택합니다.

     c. **열기**를 클릭합니다.
     선택한 파일에 관한 정보가 **파일의 정보** 창에 표시됩니다.

     d. 옵션을 하나 이상 선택합니다:

     - **인증서 세부 정보**. 이 확인란을 선택하면 지정된 데이터가 있는 디지털 인증서로 서명된 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **메타데이터**. 이 확인란을 선택하면 지정된 메타데이터가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **파일 해시**. 이 확인란을 선택하면 지정된 SHA256 해시가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **파일 경로**. 이 확인란을 선택하면 지정된 경로에서의 애플리케이션 실행을 규칙이 제어하지 않습니다.

e. 필요하다면 **명령줄** 필드에 명령줄에서 애플리케이션을 시작하기 위한 명령을 입력합니다. 해당 규칙은 이 애플리케이션의 실행을 제어합니다. ? 및 * 문자를 사용하여 마스크를 입력할 수 있습니다.

> Kaspersky Industrial CyberSecurity for Nodes는 슬래시("/")가 포함된 경로를 인식하지 못합니다. 경로에 백슬래시 문자("\")를 사용합니다.

f. **확인** 버튼을 클릭합니다.

- **드라이브 유형**. 이 규칙은 보호 중인 컴퓨터에 연결된 모든 이동식 드라이브의 애플리케이션 실행을 제어합니다.
- **KL 카테고리**. 이 규칙은 선택한 KL 카테고리에 속하는 애플리케이션의 실행을 제어합니다.
- **KSN이 신뢰함**. 이 규칙은 KSN에서 신뢰하는 애플리케이션의 실행을 제어합니다.
- **KSN이 신뢰하지 않음**. 이 규칙은 KSN에서 신뢰하지 않는 애플리케이션의 실행을 제어합니다.
- **OS가 신뢰함**. 이 규칙은 운영 체제에서 신뢰하는 애플리케이션의 실행을 제어합니다.

추가된 조건이 목록에 표시됩니다.

6. 필요하다면 각 후속 규칙 트리거 조건에 지침의 이전 단계를 수행합니다.
7. 필요하다면 **편집** 버튼을 클릭해 규칙 트리거 조건을 편집합니다.
8. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 애플리케이션 실행 제어 규칙에 대한 트리거 조건을 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **로컬 활동 제어** 섹션을 선택합니다.
5. **애플리케이션 실행 제어** 블록에서 **구성** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
6. **규칙** 탭을 선택합니다.
7. **추가** 버튼을 클릭합니다.
   규칙 설정 창이 열립니다.
8. **조건** 탭에서 **추가** 버튼을 클릭합니다.
   규칙 설정 창이 열립니다.

9. 애플리케이션 실행 제어 규칙의 트리거 조건을 선택합니다:

   - **파일의 정보**. **파일의 정보**가 규칙 트리거 조건으로 사용됩니다.

     a. **규칙 트리거 기준**에서 하나 이상의 기준에 값을 지정합니다:

     - **디지털 인증서**. 이 확인란을 선택하면 지정된 데이터가 있는 디지털 인증서로 서명된 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **메타데이터**. 이 확인란을 선택하면 지정된 메타데이터가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **SHA256 해시**. 이 확인란을 선택하면 지정된 SHA256 해시가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **파일 경로**. 이 확인란을 선택하면 지정된 경로에서의 애플리케이션 실행을 규칙이 제어하지 않습니다.

     b. **확인** 버튼을 클릭합니다.

   - **KL 카테고리에서**. 이 규칙은 선택한 KL 카테고리에 속하는 애플리케이션의 실행을 제어합니다.
   - **이동식 드라이브**. 이 규칙은 보호 중인 컴퓨터에 연결된 모든 이동식 드라이브의 애플리케이션 실행을 제어합니다.
   - **OS가 신뢰함**. 이 규칙은 운영 체제에서 신뢰하는 애플리케이션의 실행을 제어합니다.

   추가된 조건이 목록에 표시됩니다.

10. 필요하다면 각 후속 규칙 트리거 조건에 지침의 4~5단계를 수행합니다.
11. 필요하다면 **편집** 버튼을 클릭해 규칙 트리거 조건을 편집합니다.
12. 변경 사항을 저장합니다.

애플리케이션 실행 제어 규칙 범위에서 예외 추가

Kaspersky Security Center 관리 콘솔에서 애플리케이션 실행 제어 규칙 범위에 예외를 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 섹션으로 갑니다.
4. **애플리케이션 실행 제어** 블록에서 **설정** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
5. **규칙** 탭을 선택합니다.

6. 다음 중 하나를 수행합니다:

   a. 새 애플리케이션 실행 제어 규칙을 추가하는 경우 **추가** 버튼을 클릭합니다.

   b. 애플리케이션 실행 제어 규칙 목록에서 예외를 추가할 규칙을 선택하고 **편집** 버튼을 클릭합니다.

   애플리케이션 실행 제어 창이 열립니다.

7. **예외 규칙** 탭의 **추가** 버튼의 마우스 오른쪽 메뉴에서 애플리케이션 실행 제어 규칙의 범위에 예외를 생성하는 기준을 선택합니다:

   - **파일의 정보**. **선택한 파일의 정보**가 기준으로 사용됩니다.

     a. **파일의 정보** 창의 **찾아보기** 버튼을 클릭합니다.
     표준 Microsoft Windows **파일 열기** 창이 열립니다.

     b. 파일을 선택합니다.

     c. **열기**를 클릭합니다.
     선택한 파일에 관한 정보가 **파일의 정보** 창에 표시됩니다.

     d. 옵션을 하나 이상 선택합니다:

     - **인증서 세부 정보**. 이 확인란을 선택하면 지정된 데이터가 있는 디지털 인증서로 서명된 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **메타데이터**. 이 확인란을 선택하면 지정된 메타데이터가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **파일 해시**. 이 확인란을 선택하면 지정된 SHA256 해시가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **파일 경로**. 이 확인란을 선택하면 지정된 경로에서의 애플리케이션 실행을 규칙이 제어하지 않습니다.

     e. 필요하다면 **명령줄** 필드에 명령줄에서 애플리케이션을 시작하기 위한 명령을 입력합니다. 해당 규칙은 이 애플리케이션의 실행을 제어하지 않습니다. ? 및 * 문자를 사용하여 마스크를 입력할 수 있습니다.

     > Kaspersky Industrial CyberSecurity for Nodes는 슬래시("/")가 포함된 경로를 인식하지 못합니다. 경로에 백슬래시 문자("\")를 사용합니다.

     f. **확인** 버튼을 클릭합니다.

   - **드라이브 유형**. 이 규칙은 보호 중인 컴퓨터에 연결된 모든 이동식 드라이브의 애플리케이션 실행을 제어하지 않습니다.
   - **KL 카테고리**. 이 규칙은 선택한 KL 카테고리에 속하는 애플리케이션의 실행을 제어하지 않습니다.
   - **KSN이 신뢰함**. 이 규칙은 KSN에서 신뢰하는 애플리케이션의 실행을 제어하지 않습니다.
   - **KSN이 신뢰하지 않음**. 이 규칙은 KSN에서 신뢰하지 않는 애플리케이션의 실행을 제어하지 않습니다.
   - **OS가 신뢰함**. 이 규칙은 운영 체제에서 신뢰하는 애플리케이션의 실행을 제어하지 않습니다.

새로운 예외가 목록에 표사됩니다.

8. 필요하다면 지침의 이전 단계를 수행하여 애플리케이션 실행 제어 규칙의 범위에 다음 각 예외를 추가합니다.

9. 필요하다면 **편집** 버튼을 클릭해 예외를 편집합니다.

10. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 애플리케이션 실행 제어 규칙의 범위에 예외를 추가하는 방법

1. 애플리케이션 콘솔 트리에서 **컴퓨터 제어 → 애플리케이션 실행 제어** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.

3. **규칙** 탭을 선택합니다.

4. 다음 중 하나를 수행합니다:

   a. 새 애플리케이션 실행 제어 규칙을 추가하는 경우 **추가** 버튼을 클릭합니다.

   b. 애플리케이션 실행 제어 규칙 목록에서 예외를 추가할 규칙을 선택하고 **편집** 버튼을 클릭합니다.

   애플리케이션 실행 제어 창이 열립니다.

5. **예외 규칙** 탭의 **추가** 버튼의 마우스 오른쪽 메뉴에서 애플리케이션 실행 제어 규칙의 범위에 예외를 생성하는 기준을 선택합니다:

   - **파일의 정보**. **선택한 파일의 정보**가 기준으로 사용됩니다.

     a. **파일의 정보** 창의 **찾아보기** 버튼을 클릭합니다.
        표준 Microsoft Windows **파일 열기** 창이 열립니다.

     b. 파일을 선택합니다.

     c. **열기**를 클릭합니다.
        선택한 파일에 관한 정보가 **파일의 정보** 창에 표시됩니다.

     d. 옵션을 하나 이상 선택합니다:

     - **인증서 세부 정보**. 이 확인란을 선택하면 지정된 데이터가 있는 디지털 인증서로 서명된 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **메타데이터**. 이 확인란을 선택하면 지정된 메타데이터가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **파일 해시**. 이 확인란을 선택하면 지정된 SHA256 해시가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
     - **파일 경로**. 이 확인란을 선택하면 지정된 경로에서의 애플리케이션 실행을 규칙이 제어하지 않습니다.

e. 필요하다면 **명령줄** 필드에 명령줄에서 애플리케이션을 시작하기 위한 명령을 입력합니다. 해당 규칙은 이 애플리케이션의 실행을 제어하지 않습니다. ? 및 * 문자를 사용하여 마스크를 입력할 수 있습니다.

> Kaspersky Industrial CyberSecurity for Nodes는 슬래시("/")가 포함된 경로를 인식하지 못합니다. 경로에 백슬래시 문자("\")를 사용합니다.

f. **확인** 버튼을 클릭합니다.

- **드라이브 유형**. 이 규칙은 보호 중인 컴퓨터에 연결된 모든 이동식 드라이브의 애플리케이션 실행을 제어하지 않습니다.
- **KL 카테고리**. 이 규칙은 선택한 KL 카테고리에 속하는 애플리케이션의 실행을 제어하지 않습니다.
- **KSN이 신뢰함**. 이 규칙은 KSN에서 신뢰하는 애플리케이션의 실행을 제어하지 않습니다.
- **KSN이 신뢰하지 않음**. 이 규칙은 KSN에서 신뢰하지 않는 애플리케이션의 실행을 제어하지 않습니다.
- **OS가 신뢰함**. 이 규칙은 운영 체제에서 신뢰하는 애플리케이션의 실행을 제어하지 않습니다.

새로운 예외가 목록에 표시됩니다.

6. 필요하다면 지침의 이전 단계를 수행하여 애플리케이션 실행 제어 규칙의 범위에 다음 각 예외를 추가합니다.
7. 필요하다면 **편집** 버튼을 클릭해 예외를 편집합니다.
8. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 애플리케이션 실행 제어 규칙의 범위에 예외를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **로컬 활동 제어** 섹션을 선택합니다.
5. **애플리케이션 실행 제어** 블록에서 **구성** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
6. **규칙** 탭을 선택합니다.
7. **추가** 버튼을 클릭합니다.
   규칙 설정 창이 열립니다.
8. **예외 규칙** 탭에서 **추가** 버튼을 클릭합니다.
   규칙 설정 창이 열립니다.

9. 애플리케이션 실행 제어 규칙 범위에서 예외 규칙을 생성하는 기준을 선택합니다:

   - **파일의 정보**. 이 규칙은 **파일의 데이터**와 일치하는 데이터가 있는 애플리케이션의 실행을 제어하지 않습니다.

     a. **규칙 트리거 기준**에서 하나 이상의 기준에 값을 지정합니다:

        - **디지털 인증서**. 이 확인란을 선택하면 지정된 데이터가 있는 디지털 인증서로 서명된 애플리케이션의 실행을 규칙이 제어하지 않습니다.
        - **메타데이터**. 이 확인란을 선택하면 지정된 메타데이터가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
        - **SHA256 해시**. 이 확인란을 선택하면 지정된 SHA256 해시가 있는 애플리케이션의 실행을 규칙이 제어하지 않습니다.
        - **파일 경로**. 이 확인란을 선택하면 지정된 경로에서의 애플리케이션 실행을 규칙이 제어하지 않습니다.

     b. **확인** 버튼을 클릭합니다.

   - **KL 카테고리**. 이 규칙은 선택한 KL 카테고리에 속하는 애플리케이션의 실행을 제어하지 않습니다.
   - **드라이브 유형**. 이 규칙은 보호 중인 컴퓨터에 연결된 모든 이동식 드라이브의 애플리케이션 실행을 제어하지 않습니다.
   - **OS가 신뢰함**. 이 규칙은 운영 체제에서 신뢰하는 애플리케이션의 실행을 제어하지 않습니다.

   추가된 조건이 목록에 표시됩니다.

10. 필요하다면 지침의 4~5단계를 수행하여 애플리케이션 실행 제어 규칙의 범위에 다음 예외를 추가합니다.
11. 필요하다면 **편집** 버튼을 클릭해 예외를 편집합니다.
12. 변경 사항을 저장합니다.

모든 애플리케이션 실행 허용

특별히 구성된 애플리케이션 실행 제어 허용 규칙을 사용하여 모든 애플리케이션 실행을 허용할 수 있습니다.

모든 애플리케이션 실행을 허용하려면:

1. 다음 파라미터를 사용하여 2개의 애플리케이션 실행 제어 허용 규칙을 직접 추가하십시오:

   - 규칙 유형: *허용*, 범위: *실행 파일*, 파일 경로: `?:\`.
   - 규칙 유형: *허용*, 범위: *스크립트 및 MSI 패키지*, 파일 경로: `?:\`.

2. 애플리케이션 실행 제어 거부 규칙이 추가된 경우 이 거부 규칙을 삭제하십시오.
3. 이전에 생성된 모든 애플리케이션 실행 제어 허용 규칙에 대해 예외를 삭제하십시오.
4. 변경 사항을 저장합니다.

애플리케이션 실행 제어 규칙 내보내기

애플리케이션 실행 제어 규칙 목록과 소프트웨어 배포 제어의 신뢰할 수 있는 설치 패키지 목록을 XML 파일로 내보낼 수 있습니다. 내보내기 기능을 사용하여 애플리케이션 실행 제어 규칙 목록을 백업하거나 다른 서버로 마이그레이션할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 애플리케이션 실행 제어 규칙 내보내기

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 섹션으로 갑니다.
4. **애플리케이션 실행 제어** 블록에서 **설정** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
5. 애플리케이션 실행 제어 규칙을 내보내려면 **규칙** 탭으로 이동하고, 소프트웨어 배포 제어 규칙을 내보내려면 **소프트웨어 배포 제어** 탭으로 이동합니다.
6. 전체 목록을 내보내려면 버튼을 누르고 **내보내기**을 선택합니다.
7. 목록의 일부만 내보내려면 다음 단계를 수행합니다.
   a. **Ctrl** 또는 **Shift** 키를 사용하여 내보낼 목록 항목을 선택합니다. 모든 항목을 선택하려면 **Ctrl+A**를 누릅니다.
   b. 버튼을 클릭하고 **선택 항목 내보내기**을 선택합니다.
8. 창이 열리면 내보낼 XML 파일의 이름을 지정하고 파일을 저장할 폴더를 선택합니다. **저장** 버튼을 누릅니다.

Kaspersky Industrial CyberSecurity for Nodes는 규칙 목록을 XML 파일로 내보냅니다.

Kaspersky Industrial CyberSecurity for Nodes Console에서 애플리케이션 실행 제어 규칙 내보내기

1. 애플리케이션 콘솔 트리에서 **컴퓨터 제어 → 애플리케이션 실행 제어** 섹션을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.
3. 애플리케이션 실행 제어 규칙을 내보내려면 **규칙** 탭으로 이동하고, 소프트웨어 배포 제어 규칙을 내보내려면 **소프트웨어 배포 제어** 탭으로 이동합니다.
4. 전체 목록을 내보내려면 버튼을 누르고 **내보내기**을 선택합니다.

5. 목록의 일부만 내보내려면 다음 단계를 수행합니다.

   a. **Ctrl** 또는 **Shift** 키를 사용하여 내보낼 목록 항목을 선택합니다. 모든 항목을 선택하려면 **Ctrl+A**를 누릅니다.

   b. 버튼을 클릭하고 **선택 항목 내보내기**을 선택합니다.

6. 창이 열리면 내보낼 XML 파일의 이름을 지정하고 파일을 저장할 폴더를 선택합니다. **저장** 버튼을 누릅니다.

Kaspersky Industrial CyberSecurity for Nodes는 규칙 목록을 XML 파일로 내보냅니다.

웹 콘솔에서 애플리케이션 실행 제어 규칙 내보내기

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어** 섹션을 선택합니다.

5. **애플리케이션 실행 제어** 블록에서 **구성** 버튼을 클릭합니다.
   일반 탭에서 **애플리케이션 실행 제어** 창이 열립니다.

6. 애플리케이션 실행 제어 규칙을 내보내려면 **규칙** 탭으로 이동하고, 소프트웨어 배포 제어 규칙을 내보내려면 **소프트웨어 배포 제어** 탭으로 이동합니다.

7. 체크박스를 사용해 내보낼 규칙을 선택합니다.

8. **내보내기** 버튼을 클릭합니다. 열린 창에서 선택한 규칙을 내보낼 것인지 모든 규칙을 내보낼 것인지를 지정한 후 **내보내기**를 클릭합니다.
   규칙을 선택하지 않은 경우 Kaspersky Industrial CyberSecurity for Nodes는 모든 규칙을 내보냅니다.

Kaspersky Industrial CyberSecurity for Nodes는 규칙 목록을 XML 파일로 내보냅니다.

Kaspersky Security Center에서 차단된 애플리케이션 이벤트를 선택하여 텍스트 파일 생성

Kaspersky Security Center 차단된 애플리케이션 이벤트 조회 항목을 텍스트 파일로 내보낸 다음, 이 데이터를 가져와 구성 중인 정책에서 애플리케이션 실행 제어 허용 규칙의 목록을 생성할 수 있습니다.

Kaspersky Security Center 관리 콘솔을 사용하여 Kaspersky Security Center 차단된 애플리케이션 이벤트 조회 항목으로 텍스트 파일을 생성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **로그 및 알림** 섹션으로 갑니다.

4. **작업 로그** 블록에서 **설정** 버튼을 클릭합니다.
   알림 창이 열립니다.

5. **로컬 활동 제어** 노드를 확장합니다.

6. **애플리케이션 실행 제어** 섹션을 선택합니다.

7. 애플리케이션 실행 제어 이벤트 목록에서, **Kaspersky Security Center로 이벤트 전송** 열에서 *애플리케이션 시작이 금지됨* 그리고 *테스트 모드에서 애플리케이션 시작이 금지됨* 옆에 있는 확인란을 선택합니다.

8. 변경 사항을 저장합니다.

9. 정책의 **이벤트 구성** 섹션에서 **다음 기간만큼 중앙 관리 서버에 저장(일)** 필드에 지정된 이벤트 저장 기간이 차단된 애플리케이션 실행에 관한 정보를 수집할 기간(기본값은 30일)보다 긴지 확인하십시오.

   애플리케이션 실행 제어 구성 요소 로그 보존 기간이 만료되면 기록된 이벤트는 삭제되며 리포트에 표시되지 않습니다.

10. 거부된 애플리케이션 실행에 관한 데이터를 수집하도록 구성된 정책을 활성화하십시오.

11. 필요하다면 애플리케이션 실행 제어 모드를 수정하십시오.

12. 차단된 애플리케이션 실행에 관한 정보 수집 기간이 만료되면 *애플리케이션 시작이 금지됨* 그리고 *테스트 모드에서 애플리케이션 시작이 금지됨* 이벤트 중에서 선택하여 텍스트 파일로 내보내십시오. 자세한 내용은 Kaspersky Security Center 도움말의 "이벤트 조회" 섹션을 참조하십시오.

13. 내보낸 텍스트 파일을 엽니다.

14. 필요하다면 이벤트 목록을 편집하십시오.

Kaspersky Security Center 웹 콘솔 사용하여 Kaspersky Security Center 차단된 애플리케이션 이벤트 조회 항목으로 TXT 파일을 생성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로그 및 알림** 섹션을 선택합니다.

5. **작업 로그** 블록에서 **구성** 버튼을 클릭합니다.
   작업 로그 창이 열립니다.

6. **애플리케이션 실행 제어** 섹션을 선택합니다.

7. 애플리케이션 실행 제어 이벤트 목록에서, **Kaspersky Security Center로 이벤트 전송** 열에서 *애플리케이션 시작이 금지됨* 그리고 *테스트 모드에서 애플리케이션 시작이 금지됨* 옆에 있는 확인란을 선택합니다.

8. 변경 사항을 저장합니다.

9. 구성 중인 정책의 **이벤트 구성** 탭에서 **다음 기간만큼 중앙 관리 서버에 저장(일)** 필드에서 지정된 이벤트 저장 기간이 차단된 애플리케이션 실행에 관한 정보를 수집할 기간(기본값은 30일)보다 길게 하십시오.

   애플리케이션 실행 제어 구성 요소 로그 보존 기간이 만료되면 기록된 이벤트는 삭제되며 리포트에 표시되지 않습니다.

10. 거부된 애플리케이션 실행에 관한 데이터를 수집하도록 구성된 정책을 활성화하십시오.

11. 필요하다면 애플리케이션 실행 제어 모드를 수정하십시오.

12. 차단된 애플리케이션 실행에 관한 정보 수집 기간이 만료되면 *애플리케이션 시작이 금지됨* 그리고 *테스트 모드에서 애플리케이션 시작이 금지됨* 이벤트 중에서 선택하여 텍스트 파일로 내보내십시오. 자세한 내용은 Kaspersky Security Center 도움말의 "이벤트 조회" 섹션을 참조하십시오.

13. 내보낸 텍스트 파일을 엽니다.

14. 필요하다면 이벤트 목록을 편집하십시오.

애플리케이션 실행 제어를 위한 규칙 생성기 그룹 작업 구성

Kaspersky Security Center 관리 콘솔에서 애플리케이션 실행 제어를 위한 규칙 생성기 그룹 작업을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장합니다.

2. 작업을 구성할 관리 그룹을 선택합니다.

3. **작업** 탭을 선택합니다.

4. 그룹 작업 목록에서 작업 이름을 더블 클릭하여 *애플리케이션 실행 제어를 위한 규칙 생성기* 작업을 엽니다.
   속성: 애플리케이션 실행 제어를 위한 규칙 생성기 창이 열립니다.

5. **옵션** 섹션으로 갑니다.

6. 필요하다면 **규칙** 탭에서 규칙 이름 접두사를 입력합니다.

7. **허용 규칙 사용 범위**에서 허용 규칙을 만드는 데 사용할 방법을 지정합니다:

   - **실행 중인 애플리케이션을 기반으로 허용 규칙 생성**.
   - **폴더에서 애플리케이션에 대한 허용 규칙 생성**.

8. **설정** 탭에서 애플리케이션 실행 제어 허용 규칙을 만들 때 작업이 적용할 기준을 선택합니다:

   - **디지털 인증서 사용**.

     이 옵션을 선택하면 애플리케이션 실행 제어에 대해 새로 생성되는 허용 규칙의 설정에서 디지털 인증서의 유무를 규칙 트리거 기준으로 지정합니다. Kaspersky Industrial CyberSecurity for Nodes는 디지털 인증서가 있는 파일을 허용합니다. 이 옵션은 운영 체제에서 신뢰하는 애플리케이션의 시작을 허용하려는 경우 사용하는 것이 좋습니다. 이 옵션은 기본적으로 선택되어 있습니다.

- **디지털 인증서 주체 및 지문 사용**.
- **인증서가 없다면 다음 사용**.
- **SHA256 해시 사용**.

  이 옵션을 선택하면 규칙 생성에 사용된 파일의 체크섬이 새로 생성되는 애플리케이션 실행 제어용 허용 규칙의 설정에서 규칙 트리거 기준으로 지정됩니다. Kaspersky Industrial CyberSecurity for Nodes는 지정된 체크섬이 있는 파일을 사용하여 실행된 애플리케이션을 허용합니다. SHA256 체크섬을 규칙 트리거 기준으로 사용하면 규칙 사용 범위가 파일 1개로 제한됩니다.

9. **해시 섬을 기반으로 생성된 규칙의 파일 경로 추가** 설정을 구성합니다.

   이 확인란을 선택하면 규칙을 내보낼 때 Kaspersky Industrial CyberSecurity for Nodes가 실행 파일의 전체 경로를 XML 파일에 추가합니다. 전체 경로를 통해 실행 파일이 속한 소프트웨어를 찾을 수 있습니다.

   이 확인란을 선택 해제하면 실행 파일의 이름과 SHA256 해시만 XML 파일에 포함됩니다. 기본적으로 확인란의 선택이 취소됩니다.

10. 작업을 사용하여 만든 규칙을 충족하는 애플리케이션을 실행할 수 있는 사용자 또는 사용자 그룹을 추가하십시오.

    a. **추가** 버튼의 마우스 오른쪽 메뉴에서 사용자 또는 그룹을 추가하는 방법을 선택합니다.

    b. 열린 창에서 사용자 또는 사용자 그룹의 이름을 입력하거나 선택합니다.

    c. **확인** 버튼을 클릭합니다.

    d. 모든 사용자 또는 사용자 그룹에 대해 a~c 단계를 완료하십시오.

11. **작업 완료 후** 블록에서 다음 설정을 구성합니다.
    - **허용 규칙을 애플리케이션 실행 제어 규칙 목록에 추가**.
    - **추가 원칙**.
    - **파일에 허용 규칙 내보내기**.
    - **파일 이름에 보호 중인 장치 세부 정보 추가**.
12. 필요하다면 **예외** 탭으로 들어가 작업 범위에서 제외할 개체를 지정합니다.
13. **속성: 애플리케이션 실행 제어를 위한 규칙 생성기** 창에서 **확인** 버튼을 클릭합니다.

Kaspersky Security Center 웹 콘솔에서 애플리케이션 실행 제어를 위한 규칙 생성기 그룹 작업을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
2. 그룹 작업 목록에서 애플리케이션 실행 제어를 위한 규칙 생성기 작업을 엽니다.

   애플리케이션 실행 제어를 위한 규칙 생성기 창이 열립니다.
3. **애플리케이션 설정** 탭을 엽니다.
4. 필요하다면 **허용 규칙 사용 범위** 섹션에서 규칙 이름 접두사를 입력합니다.

5. **허용 규칙 사용 범위**에서 허용 규칙을 만드는 데 사용할 방법을 지정합니다:

   - **실행 중인 애플리케이션을 기반으로 허용 규칙 생성**
   - **폴더에서 애플리케이션에 대한 허용 규칙 생성**

6. **파라미터** 탭에서 애플리케이션 실행 제어 허용 규칙을 만들 때 작업이 적용할 기준을 선택합니다:

   - **디지털 인증서 사용**.
   - **디지털 인증서 주체 및 지문 사용**.
   - **인증서가 없다면 다음 사용**.
   - **SHA256 해시 사용**.

7. **해시 섬을 기반으로 생성된 규칙의 파일 경로 추가** 설정을 구성합니다.

   이 확인란을 선택하면 규칙을 내보낼 때 Kaspersky Industrial CyberSecurity for Nodes가 실행 파일의 전체 경로를 XML 파일에 추가합니다. 전체 경로를 통해 실행 파일이 속한 소프트웨어를 찾을 수 있습니다.

   이 확인란을 선택 해제하면 실행 파일의 이름과 SHA256 해시만 XML 파일에 포함됩니다. 기본적으로 확인란의 선택이 취소됩니다.

8. 작업을 사용하여 만든 규칙을 충족하는 애플리케이션을 실행할 수 있는 사용자 또는 사용자 그룹을 추가하십시오.

   a. **사용자 또는 그룹 추가** 버튼을 클릭합니다.

   b. 열린 창에서 사용자 또는 사용자 그룹의 이름을 입력하거나 선택합니다.

   c. **선택** 버튼을 클릭합니다.

   d. 모든 사용자 또는 사용자 그룹에 대해 a~c 단계를 완료하십시오.

9. **작업 완료 후** 블록에서 다음 설정을 구성합니다.

   - **허용 규칙을 애플리케이션 실행 제어 규칙 목록에 추가**.
   - **추가 원칙**.
   - **허용 규칙을 파일로 내보냅니다**. **.xml 확장자가 있는 파일의 전체 경로를 지정합니다** 필드에서 애플리케이션 실행 제어를 위한 규칙 생성기 작업이 완료될 때 Kaspersky Industrial CyberSecurity for Nodes가 허용 규칙을 XML 파일로 내보낼 경로를 지정할 수 있습니다.
   - **파일 이름에 보호 중인 장치 세부 정보 추가**.

10. 필요하다면 **예외 규칙** 탭으로 들어가 작업 범위에서 제외할 개체를 지정합니다.

11. **애플리케이션 실행 제어를 위한 규칙 생성기** 창의 **확인** 버튼을 클릭합니다.

애플리케이션 실행 제어를 위한 규칙 생성기 그룹 작업을 사용하여 규칙 생성.

애플리케이션 실행 제어를 위한 규칙 생성기 그룹 작업을 사용하여 규칙을 생성하려면:

1. *애플리케이션 실행 제어를 위한 규칙 생성기* 그룹 작업을 생성하거나 기존 작업을 선택합니다.
2. 애플리케이션 실행 제어를 위한 규칙 생성기 작업을 구성합니다.
3. 애플리케이션 실행 제어를 위한 규칙 생성기 작업을 실행합니다.

작업 종료 후 작업 설정에 따라:

- 작업 완료 후 **허용 규칙을 애플리케이션 실행 제어 규칙 목록에 추가** 동작을 지정하면 생성된 애플리케이션 실행 제어 규칙이 애플리케이션 콘솔의 애플리케이션 실행 제어 설정 목록에 추가됩니다.
- 작업 완료 후 **허용 규칙을 파일로 내보냅니다** 동작을 지정하면 생성된 애플리케이션 실행 제어 규칙이 작업 설정에 지정된 경로에 있는 XML 파일에 저장됩니다.

목록에는 애플리케이션 실행 제어를 위한 규칙 생성기 그룹 작업의 설정과 일치하는 유형의 애플리케이션 실행에 대한 허용 규칙이 포함됩니다.

장치 제어

장치 제어 구성 요소는 컴퓨터에 설치되거나 컴퓨터에 연결된 장치(예: 하드 드라이브, 카메라 또는 Wi-Fi 모듈)에 대한 사용자 접근을 관리합니다. 이는 이러한 장치가 연결될 때 컴퓨터를 감염으로부터 보호하고 데이터 손실 또는 유출을 방지할 수 있습니다.

장치 제어 구성 요소는 다음 기능을 제공합니다.

- 저장 장치(이동식 드라이브, 휴대전화, CD/DVD 드라이브 등)에 대한 사용자 접근 권한 관리.
- 파일 시스템이 없는 장치(외부 모뎀, Bluetooth 어댑터, USB 키보드 등) 연결 제어.
- Wi-Fi 연결 관리.

기본적으로 장치 제어 구성 요소는 비활성화됩니다. 장치 제어 구성 요소를 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 다음 장치 유형에 대한 접근을 기본적으로 거부합니다.

- 이동식 드라이브(USB 플래시 드라이브 포함)
- 플로피 디스크
- CD/DVD 드라이브
- 휴대용 장치(MTP)
- 모뎀
- 스마트 카드 리더기
- 외부 네트워크 어댑터
- Bluetooth(입력 장치 제외)

장치 제어 레벨

Kaspersky Industrial CyberSecurity for Nodes는 다음 수준에서 장치 접근을 제어합니다.

1. **장치 유형**.

   장치를 컴퓨터에 연결할 때 운영 체제에 따라 프린터, 이동식 드라이브, CD/DVD 드라이브 등의 유형이 결정됩니다. 이 레벨에서 유형별로 장치 연결을 허용 또는 거부할 수 있습니다.

2. **연결 버스**.

   *연결 버스*는 장치를 컴퓨터에 연결하는 데 사용되는 인터페이스입니다. 일부 장치 유형에는 여러 연결 인터페이스가 있습니다. 예를 들어 프린터를 USB 또는 직렬(COM) 포트에 연결할 수 있습니다.

   이 레벨에서 연결 버스에 따라 장치에 대한 접근을 허용하거나 거부할 수 있습니다.

   예를 들어 USB를 통한 접근을 거부했다고 가정해 보십시오. Kaspersky Industrial CyberSecurity for Nodes는 USB를 통해 연결될 때 **연결 버스에 종속** 모드를 사용하여 모든 장치 유형에 대한 접근을 거부합니다.

장치에 대해 접근 **허용** 또는 **차단** 모드가 선택되면 접근 제어가 장치의 연결 버스를 무시합니다.

3. **신뢰하는 장치**.

   *신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.

장치 제어 운영 모드

장치 제어 구성 요소는 다음 모드에서 작동할 수 있습니다.

- **활성 모드**.

  Kaspersky Industrial CyberSecurity for Nodes 구성된 장치 접근 규칙에 따라 장치를 거부하거나 허용합니다. 또한, 애플리케이션이 신뢰하는 장치에 대한 접근을 허용합니다. 애플리케이션이 장치 연결 및 연결 해제 이벤트를 등록합니다.

- **알림**.

  Kaspersky Industrial CyberSecurity for Nodes는 모든 장치를 허용하고 해당 이벤트를 기록합니다. 모든 장치가 허용됩니다. 기본적으로 이 모드가 설정됩니다. 이 모드를 활성화하여 조직 내 장치 감사를 수행하고, 이 정보를 사용하여 신뢰하는 장치 목록을 작성합니다.

장치 접근 규칙

*장치 접근 규칙*은 컴퓨터에 설치되거나 연결된 장치에 대한 사용자의 접근을 결정합니다. 이러한 설정에는 특정 장치에 대한 접근, 접근 스케줄, 읽기 또는 쓰기 권한 등이 포함됩니다. 접근 규칙에 대한 설정 그룹은 장치 유형에 따라 다릅니다.

접근 규칙 설정

장치	사용자 및 사용자 그룹 할당	장치 접근 스케줄	읽기/쓰기 권한	연결 버스 모니터링
하드 드라이브	✓	✓	✓	✓
이동식 드라이브(USB 플래시 드라이브 포함)	✓	✓	✓	✓
플로피 디스크	✓	✓	✓	✓
CD/DVD 드라이브	✓	✓	✓	✓
휴대용 장치(MTP)	✓	✓	✓	✓
로컬 프린터	✓	–	–	✓
네트워크 프린터	✓	–	–	–
모뎀	–	–	–	✓
스트리머	–	–	–	✓
다기능 장치	–	–	–	✓
스마트 카드 리더기	–	–	–	✓
Windows CE USB ActiveSync 장치	–	–	–	✓
외부 네트워크 어댑터	–	–	–	✓
Bluetooth	–	–	–	–
카메라 및 스캐너	–	–	–	✓

장치	사용자 및 사용자 그룹 할당	장치 접근 스케줄	읽기/쓰기 권한	연결 버스 모니터링
Wi-Fi	–	–	–	–
USB 키보드	–	–	–	✓
USB 마우스	–	–	–	✓

유형별 장치 접근 관리

장치 제어 구성 요소를 통해 장치에 대한 접근을 유형별로 관리할 수 있습니다. 장치 유형은 장치가 연결될 때 운영 체제가 결정합니다. 운영 체제에 내장된 장치 관리자 도구를 사용하여 장치 유형을 조회할 수 있습니다. 장치에 대한 접근을 관리하려면 규칙을 구성해야 합니다. *장치 접근 규칙*은 컴퓨터에 설치되거나 연결된 장치에 대한 사용자의 접근을 결정합니다. 이러한 설정에는 특정 장치에 대한 접근, 접근 스케줄, 읽기 또는 쓰기 권한 등이 포함됩니다. 접근 규칙에 대한 설정 그룹은 장치 유형에 따라 다릅니다.

다음과 같이 장치 접근 설정을 구성할 수 있습니다:

- **허용**.

  Kaspersky Industrial CyberSecurity for Nodes가 모든 사용자에게 장치에 대한 전체 접근 권한을 부여합니다.

- **차단**.

  Kaspersky Industrial CyberSecurity for Nodes가 장치 연결을 차단합니다. 애플리케이션이 신뢰하는 장치의 연결만 허용합니다.

- **연결 버스에 종속**.

  Kaspersky Industrial CyberSecurity for Nodes가 장치의 연결 버스를 식별하고 연결 버스의 접근 모드에 따라 접근 제어를 수행합니다. 또한 애플리케이션은 신뢰하는 장치 연결을 허용합니다.

- **규칙에 따라**.

  일부 장치 유형의 경우 장치 사용, 장치 접근 스케줄 구성, 읽기 및 쓰기 권한을 구성할 수 있는 사용자 또는 사용자 그룹을 선택할 수 있습니다. 애플리케이션이 신뢰하는 장치의 연결도 허용합니다.

하드 드라이브 유형의 장치에 대한 접근을 설정할 때는 주의해야 합니다. 시스템 디스크에 대한 접근을 차단하면 운영 체제를 부팅할 때 애플리케이션이 충돌(BSOD)을 일으킬 수 있습니다.

장치가 장치 제어 분류 구성표에 해당하지 않는다면 해당 장치에 대한 접근을 제한할 수 없습니다.

Kaspersky Security Center 관리 콘솔에서 유형별로 장치에 대한 접근을 제어하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.
4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.
5. **장치 제어** 확인란을 선택합니다.
6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.

7. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   장치 유형 탭에는 장치 제어 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.

8. 장치 접근 규칙을 구성합니다:

   a. 접근 모드를 **허용**, **차단**, **연결 버스에 종속**, **규칙에 따라** 중에서 선택합니다.
      규칙에 따라 접근 모드를 선택하려면 더블 클릭하여 접근 규칙 속성을 열어야 합니다.

   b. **연결 버스에 종속** 접근 모드를 선택했다면, **연결 버스** 탭을 누르고 연결 인터페이스에 대한 접근 규칙을 구성합니다.

   c. 저장 장치(예: 이동식 드라이브)의 경우 개별 사용자의 접근 권한을 구성할 수 있습니다. 사용자가 장치 접근 스케줄과 읽기 및 쓰기 권한을 구성할 수도 있습니다.

   d. 필요하다면 인쇄 규칙을 구성합니다.

   e. 필요하다면 Wi-Fi 연결 규칙을 구성합니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 유형별로 장치에 대한 접근을 제어하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어** → **장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.

5. **장치 제어 사용** 확인란을 선택합니다.

6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.

7. **장치 제어 설정** 블록에서 **장치 및 Wi-Fi 네트워크에 대한 접근 규칙** 옵션을 클릭합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.

8. 장치 접근 규칙을 구성합니다:

   a. 접근 모드를 **허용**, **차단**, **연결 버스에 종속**, **규칙에 따라** 중에서 선택합니다.
      드롭다운 메뉴에서 접근 모드를 사용할 수 없는 경우 장치 유형을 더블 클릭하여 접근 규칙의 속성을 엽니다.

   b. **연결 버스에 종속** 접근 모드를 선택하는 경우 일반 장치 제어 설정이 있는 창으로 돌아가서 **연결 버스**를 클릭하고 연결 인터페이스에 대한 접근 규칙을 구성합니다.

   c. 저장 장치(예: 이동식 드라이브)의 경우 개별 사용자의 접근 권한을 구성할 수 있습니다. 사용자가 장치 접근 스케줄과 읽기 및 쓰기 권한을 구성할 수도 있습니다.

d. 필요하다면 인쇄 규칙을 구성합니다.

e. 필요하다면 Wi-Fi 연결 규칙을 구성합니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 유형별로 장치 접근을 제어하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **장치 제어** 옵션을 선택합니다.

2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.

3. **장치 제어** 확인란을 선택합니다.

4. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.

5. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.

6. 장치 접근 규칙을 구성합니다:

   a. 접근 모드를 **허용**, **차단**, **연결 버스에 종속**, **규칙에 따라** 중에서 선택합니다.
      규칙에 따라 접근 모드를 선택하려면 더블 클릭하여 접근 규칙 속성을 열어야 합니다.

   b. **연결 버스에 종속** 접근 모드를 선택하면 **연결 버스** 탭에서 연결 인터페이스에 대한 접근 규칙을 구성해야 합니다.

   c. 저장 장치(예: 이동식 드라이브)의 경우 개별 사용자의 접근 권한을 구성할 수 있습니다. 사용자가 장치 접근 스케줄과 읽기 및 쓰기 권한을 구성할 수도 있습니다.

   d. 필요하다면 인쇄 규칙을 구성합니다.

   e. 필요하다면 Wi-Fi 연결 규칙을 구성합니다.

7. 변경 사항을 저장합니다.

결과적으로, 사용자가 장치 접근 권한을 획득하려고 하면 애플리케이션이 규칙에 따라 접근을 차단합니다. Kaspersky Industrial CyberSecurity for Nodes는 해당 이벤트도 기록합니다. 개별 장치에 대한 접근 권한을 부여하려면 해당 장치를 신뢰하는 장치 목록에 추가할 수 있습니다.

Wi-Fi 연결 제어

장치 제어 구성 요소를 통해 컴퓨터(터미널)의 Wi-Fi 연결을 관리할 수 있습니다. 공용 Wi-Fi 네트워크는 안전하지 않을 수 있으며 이러한 네트워크를 사용하면 데이터가 손실될 수 있습니다. 장치 제어 구성 요소를 사용하면 사용자가 Wi-Fi에 연결하지 못하도록 차단하거나 신뢰할 수 있는 네트워크에만 연결하도록 허용할 수 있습니다. 예를 들어, 보안이 확보된 회사 Wi-Fi 네트워크에만 연결하도록 허용할 수 있습니다. 장치 제어 구성 요소는 신뢰 목록에 지정된 네트워크를 예외한 모든 Wi-Fi 네트워크에 대한 접근을 차단합니다.

Windows 11을 실행하는 컴퓨터에서 Wi-Fi 연결을 제어하려면 위치 서비스를 활성화해야 합니다. 이렇게 하려면 운영 체제 설정(**설정 → 개인 정보 및 보안 → 위치**)에서 **위치 서비스** 스위치를 활성화해야 합니다. 위치 서비스가 비활성화되면 Kaspersky Industrial CyberSecurity for Nodes가 Wi-Fi 네트워크에 대한 연결을 제어하지 않습니다.

Kaspersky Security Center 관리 콘솔에서 Wi-Fi 연결을 제한하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.
4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.
5. **장치 제어** 확인란을 선택합니다.
6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.
7. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   장치 유형 탭에는 장치 제어 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
8. **Wi-Fi** 장치의 경우 접근 규칙을 구성합니다:
   a. 접근 모드를 **허용**, **차단**, **예외를 제외하고 차단** 중에서 선택합니다.
   b. **예외를 제외하고 차단** 모드를 선택한 경우 신뢰하는 Wi-Fi 네트워크 목록을 생성해야 합니다:
      1. **Wi-Fi** 장치 유형을 더블 클릭하여 신뢰하는 Wi-Fi 네트워크 목록을 엽니다.
      2. 열리는 창에서 **추가** 버튼을 클릭합니다.
      3. 열린 창에서 신뢰하는 Wi-Fi 네트워크를 구성합니다:
         - **네트워크 이름**. Wi-Fi 네트워크의 이름 또는 SSID(Service Set Identifier).
         - **인증 유형**. Wi-Fi 네트워크 연결에 사용되는 인증 유형.
         - **암호화 유형**. Wi-Fi 트래픽 보호에 사용되는 암호화 유형.
         - **설명**. 추가한 Wi-Fi 네트워크에 대한 추가 정보.

라우터 설정에서 신뢰하는 Wi-Fi 네트워크의 설정을 볼 수 있습니다.

Wi-Fi 네트워크의 설정이 규칙에 지정된 모든 설정과 일치하는 경우 신뢰할 수 있는 네트워크로 간주됩니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 Wi-Fi 연결을 제한하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **로컬 활동 제어** → **장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.
5. **장치 제어 사용** 확인란을 선택합니다.
6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.
7. **장치 제어 설정** 블록에서 **장치 및 Wi-Fi 네트워크에 대한 접근 규칙** 옵션을 클릭합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
8. **Wi-Fi** 장치 유형을 더블 클릭하여 접근 규칙 속성을 엽니다.
9. 접근 모드를 **허용**, **차단**, **예외를 제외하고 차단** 중에서 선택합니다.
10. **예외를 제외하고 차단** 모드를 선택한 경우 신뢰하는 Wi-Fi 네트워크 목록을 생성해야 합니다:
    1. **신뢰하는 Wi-Fi 네트워크** 블록에서 **추가** 버튼을 클릭합니다.
    2. 열린 창에서 신뢰하는 Wi-Fi 네트워크를 구성합니다:
       - **네트워크 이름**. Wi-Fi 네트워크의 이름 또는 SSID(Service Set Identifier).
       - **인증 유형**. Wi-Fi 네트워크 연결에 사용되는 인증 유형.
       - **암호화 유형**. Wi-Fi 트래픽 보호에 사용되는 암호화 유형.
       - **설명**. 추가한 Wi-Fi 네트워크에 대한 추가 정보.

    라우터 설정에서 신뢰하는 Wi-Fi 네트워크의 설정을 볼 수 있습니다.

    Wi-Fi 네트워크의 설정이 규칙에 지정된 모든 설정과 일치하는 경우 신뢰할 수 있는 네트워크로 간주됩니다.

11. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 Wi-Fi 연결을 제한하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **장치 제어** 옵션을 선택합니다.
2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.
3. **장치 제어** 확인란을 선택합니다.
4. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.
5. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
6. **Wi-Fi** 장치의 경우 접근 규칙을 구성합니다:
   a. 접근 모드를 **허용**, **차단**, **예외를 제외하고 차단** 중에서 선택합니다.
   b. **예외를 제외하고 차단** 모드를 선택한 경우 신뢰하는 Wi-Fi 네트워크 목록을 생성해야 합니다:
      1. **Wi-Fi** 장치 유형을 더블 클릭하여 신뢰하는 Wi-Fi 네트워크 목록을 엽니다.
      2. 열리는 창에서 **추가** 버튼을 클릭합니다.
      3. 열린 창에서 신뢰하는 Wi-Fi 네트워크를 구성합니다:
         - **네트워크 이름**. Wi-Fi 네트워크의 이름 또는 SSID(Service Set Identifier).
         - **인증 유형**. Wi-Fi 네트워크 연결에 사용되는 인증 유형.
         - **암호화 유형**. Wi-Fi 트래픽 보호에 사용되는 암호화 유형.
         - **설명**. 추가한 Wi-Fi 네트워크에 대한 추가 정보.

   라우터 설정에서 신뢰하는 Wi-Fi 네트워크의 설정을 볼 수 있습니다.

   > Wi-Fi 네트워크의 설정이 규칙에 지정된 모든 설정과 일치하는 경우 신뢰할 수 있는 네트워크로 간주됩니다.

7. 변경 사항을 저장합니다.

그 결과 사용자가 신뢰 목록에 없는 Wi-Fi 네트워크에 연결을 시도하면 애플리케이션이 연결을 차단합니다.

인쇄 제어

장치 제어 구성 요소를 통해 로컬 및 네트워크 프린터에 대한 사용자 접근을 구성할 수 있습니다.

로컬 프린터 제어

Kaspersky Industrial CyberSecurity for Nodes는 USB, 직렬 포트(COM), 병렬 포트(LPT) 버스를 통해 로컬 프린터 연결을 제어합니다.

Kaspersky Industrial CyberSecurity for Nodes는 버스 레벨에서만 로컬 프린터와 COM 및 LPT 포트의 연결을 제어합니다. 즉, COM 및 LPT 포트에 대한 프린터 연결을 방지하려면 **로컬 프린터** 장치 유형의 경우 **연결 버스에 종속** 모드를 선택하고 COM 및 LPT 버스에 대한 장치의 연결을 금지합니다.

USB에 연결된 프린터에 대해서는, 애플리케이션이 장치 유형(로컬 프린터)과 연결 버스(USB)의 두 가지 수준에서 제어를 실행합니다.

USB를 통한 다음 로컬 프린터 접근 모드 중 하나를 선택할 수 있습니다.

- **허용**. Kaspersky Industrial CyberSecurity for Nodes가 모든 사용자에게 로컬 프린터에 대한 전체 접근 권한을 부여합니다. 사용자는 운영 체제가 제공하는 수단을 사용하여 프린터를 연결하고 문서를 인쇄할 수 있습니다.
- **차단**. Kaspersky Industrial CyberSecurity for Nodes가 로컬 프린터 연결을 차단합니다. 애플리케이션이 신뢰하는 프린터의 연결만 허용합니다.
- **연결 버스에 종속**. Kaspersky Industrial CyberSecurity for Nodes가 USB 버스 연결 상태(**허용** 또는 **차단**)에 따라 로컬 프린터 연결을 허용합니다.
- **규칙에 따라**. 인쇄를 제어하려면 *인쇄 규칙*을 추가해야 합니다. 규칙을 통해 로컬 프린터에서 문서 인쇄에 대한 액세스를 허용하거나 차단할 사용자 또는 사용자 그룹을 선택할 수 있습니다.

네트워크 프린터 제어

Kaspersky Industrial CyberSecurity for Nodes를 통해 네트워크 프린터의 인쇄에 대한 접근을 구성할 수 있습니다. 네트워크 프린터에 대한 다음 접근 모드 중 하나를 선택할 수 있습니다:

- **허용하고 기록하지 않음**. Kaspersky Industrial CyberSecurity for Nodes가 네트워크 프린터의 인쇄를 제어하지 않습니다. 애플리케이션이 모든 사용자에게 인쇄에 대한 접근 권한을 부여하고 인쇄에 관한 정보를 이벤트 로그에 저장하지 않습니다.
- **허용**. Kaspersky Industrial CyberSecurity for Nodes가 모든 사용자에게 네트워크 프린터에서 인쇄할 수 있는 접근 권한을 부여합니다.
- **차단**. Kaspersky Industrial CyberSecurity for Nodes가 모든 사용자의 네트워크 프린터 접근을 제한합니다. 애플리케이션은 신뢰하는 프린터에만 접근을 허용합니다.
- **규칙에 따라**. 인쇄를 제어하려면 *인쇄 규칙*을 추가해야 합니다. 규칙을 통해 네트워크 프린터의 문서 인쇄에 대한 접근을 허용하거나 차단할 사용자 또는 사용자 그룹을 선택할 수 있습니다.

프린터에 대한 인쇄 규칙 추가

Kaspersky Security Center 관리 콘솔에서 인쇄 규칙을 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.
4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.
5. **장치 제어** 확인란을 선택합니다.
6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.
7. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   장치 유형 탭에는 장치 제어 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
8. 프린터 접근 규칙을 구성합니다:
   a. **로컬 프린터** 및 **네트워크 프린터** 장치 유형의 경우 **허용**, **차단**, **허용하고 기록하지 않음**(네트워크 프린터만 해당), **연결 버스에 종속**(로컬 프린터만 해당), **규칙에 따라** 등의 접근 규칙을 구성합니다.
   b. **연결 버스에 종속** 접근 모드를 선택했다면, **연결 버스** 탭을 누르고 연결 인터페이스에 대한 접근 규칙을 구성합니다.
   c. **규칙에 따라** 접근 모드를 선택하면 인쇄 규칙을 구성해야 합니다:
      1. **로컬 프린터** 및 **네트워크 프린터** 장치 유형을 더블 클릭하고 접근 규칙 속성을 엽니다.
      2. 인쇄 규칙을 적용할 사용자 또는 사용자 그룹을 선택합니다. 이를 위해서는 **추가** 버튼을 클릭합니다.
         새 인쇄 규칙을 추가할 수 있는 창이 열립니다.
      3. *규칙 항목*에 우선순위를 할당합니다. 규칙 항목에는 사용자 계정, 작업(허용/차단), 우선순위 특성이 포함됩니다.
         규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Industrial CyberSecurity for Nodes는 우선순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Industrial CyberSecurity for Nodes는 0부터 10,000까지 우선순위를 할당할 수 있습니다. 값이 클수록 우선순위가 높습니다. 다시 말해, 값이 0인 항목은 우선순위가 가장 낮습니다.
         예를 들어 Everyone 그룹에 읽기 전용 권한을 부여하고 관리자 그룹에 읽기/쓰기 권한을 부여할 수 있습니다. 이렇게 하려면 관리자 그룹에 우선 순위 1을 할당하고 Everyone 그룹에 우선 순위 0을 할당합니다.
         차단 규칙이 허용 규칙보다 우선합니다. 즉, 사용자가 여러 그룹에 추가된 상태에서 모든 규칙의 우선순위가 동일하다면 Kaspersky Industrial CyberSecurity for Nodes가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.
      4. **처리**에서 프린터 인쇄에 대한 사용자 접근을 구성합니다.

5. **사용자 및 그룹** 버튼을 클릭하고 인쇄에 접근할 사용자 또는 사용자 그룹을 선택합니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.

6. **확인** 버튼을 클릭합니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 인쇄 규칙을 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어** → **장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.

5. **장치 제어 사용** 확인란을 선택합니다.

6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.

7. **장치 제어 설정** 블록에서 **장치 및 Wi-Fi 네트워크에 대한 접근 규칙** 옵션을 클릭합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.

8. 프린터 접근 규칙을 구성합니다:

   a. **로컬 프린터** 및 **네트워크 프린터** 장치 유형의 경우 접근 모드를 **허용**, **차단**, **허용하고 기록하지 않음**(네트워크 프린터만 해당), **연결 버스에 종속**(로컬 프린터만 해당), **규칙에 따라** 중에서 선택합니다.

   드롭다운 메뉴에서 접근 모드를 사용할 수 없는 경우 장치 유형을 더블 클릭하여 접근 규칙의 속성을 엽니다.

   b. **연결 버스에 종속** 접근 모드를 선택하는 경우 장치 제어 구성 요소 일반 설정이 있는 창으로 돌아가서 **연결 버스**를 클릭하고 연결 인터페이스에 대한 접근 규칙을 구성합니다.

   c. 인쇄를 구성하려면:

      1. **로컬 프린터** 또는 **네트워크 프린터** 장치 유형을 더블 클릭하고 접근 규칙 속성을 엽니다.

      2. **규칙에 따라** 접근 모드를 선택합니다.

      3. 인쇄 규칙을 적용할 사용자 또는 사용자 그룹을 선택합니다. 이를 위해서는 **추가** 버튼을 클릭합니다.
         새 인쇄 규칙을 추가할 수 있는 창이 열립니다.

      4. *규칙 항목*에 우선순위를 할당합니다. 규칙 항목에는 사용자 계정, 작업(허용/차단), 우선순위 특성이 포함됩니다.

         규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Industrial CyberSecurity for Nodes는 우선순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Industrial CyberSecurity for Nodes는 0부터 10,000까지 우선순위를 할당할 수 있습니다. 값이 클수록 우선순위가 높습니다. 다시 말해, 값이 0인 항목은 우선순위가 가장 낮습니다.

예를 들어 Everyone 그룹에 읽기 전용 권한을 부여하고 관리자 그룹에 읽기/쓰기 권한을 부여할 수 있습니다. 이렇게 하려면 관리자 그룹에 우선 순위 1을 할당하고 Everyone 그룹에 우선 순위 0을 할당합니다.

차단 규칙이 허용 규칙보다 우선합니다. 즉, 사용자가 여러 그룹에 추가된 상태에서 모든 규칙의 우선순위가 동일하다면 Kaspersky Industrial CyberSecurity for Nodes가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.

5. **처리**에서 프린터 인쇄에 대한 사용자 접근을 구성합니다.

6. **사용자 및 그룹**에서 **추가**를 클릭하고 인쇄에 접근할 사용자 또는 사용자 그룹을 선택합니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.

7. **확인** 버튼을 클릭합니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 인쇄 규칙을 추가하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **장치 제어** 옵션을 선택합니다.

2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.

3. **장치 제어** 확인란을 선택합니다.

4. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.

5. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.

6. 프린터 접근 규칙을 구성합니다:

   a. **로컬 프린터** 및 **네트워크 프린터** 장치 유형의 경우 **허용**, **차단**, **허용하고 기록하지 않음**(네트워크 프린터만 해당), **연결 버스에 종속**(로컬 프린터만 해당), **규칙에 따라** 등의 접근 규칙을 구성합니다.

   b. **연결 버스에 종속** 접근 모드를 선택했다면, **연결 버스** 탭을 누르고 연결 인터페이스에 대한 접근 규칙을 구성합니다.

   c. **규칙에 따라** 접근 모드를 선택하면 인쇄 규칙을 구성해야 합니다:

      1. **로컬 프린터** 및 **네트워크 프린터** 장치 유형을 더블 클릭하고 접근 규칙 속성을 엽니다.

      2. 인쇄 규칙을 적용할 사용자 또는 사용자 그룹을 선택합니다. 이를 위해서는 **추가** 버튼을 클릭합니다.
         새 인쇄 규칙을 추가할 수 있는 창이 열립니다.

      3. *규칙 항목*에 우선순위를 할당합니다. 규칙 항목에는 사용자 계정, 작업(허용/차단), 우선순위 특성이 포함됩니다.

         규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Industrial CyberSecurity for Nodes는 우선순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Industrial CyberSecurity for Nodes는 0부터 10,000까지 우선순위를 할당할 수 있습니다. 값이 클수록 우선순위가 높습니다. 다시 말해, 값이 0인 항목은 우선순위가 가장 낮습니다.

         예를 들어 Everyone 그룹에 읽기 전용 권한을 부여하고 관리자 그룹에 읽기/쓰기 권한을 부여할 수 있습니다. 이렇게 하려면 관리자 그룹에 우선 순위 1을 할당하고 Everyone 그룹에 우선 순위 0을 할당합니다.

차단 규칙이 허용 규칙보다 우선합니다. 즉, 사용자가 여러 그룹에 추가된 상태에서 모든 규칙의 우선순위가 동일하다면 Kaspersky Industrial CyberSecurity for Nodes가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.

4. **처리**에서 프린터 인쇄에 대한 사용자 접근을 구성합니다.

5. **사용자 및 그룹** 버튼을 클릭하고 인쇄에 접근할 사용자 또는 사용자 그룹을 선택합니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.

6. **확인** 버튼을 클릭합니다.

7. 변경 사항을 저장합니다.

입력 장치 제어(HID)

입력 장치에는 키보드와 마우스, 트랙볼, 터치패드, 기타 장치가 포함됩니다. USB, Bluetooth, PS/2 포트, RS-232(COM) 포트, IR 포트 등의 인터페이스를 사용하여 입력 장치를 연결할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes를 사용하면 USB 및 Bluetooth 마우스와 키보드를 제어할 수 있습니다. 장치 제어 구성 요소는 입력 장치 연결 장치와 연결 해제 장치를 기록합니다.

Bluetooth 장치가 연결되거나 연결 해제되면 애플리케이션은 장치에 대한 여러 이벤트를 생성할 수 있습니다. 운영 체제가 Bluetooth 장치를 서로 다른 유형의 여러 장치로 감지할 수 있기 때문입니다. 또한 Kaspersky Industrial CyberSecurity for Nodes는 장치가 연결되는 Bluetooth 어댑터도 별도의 장치로 관리합니다. 이것이 바로 애플리케이션이 탐지하는 장치마다 이벤트를 생성하는 이유입니다.

Kaspersky Industrial CyberSecurity for Nodes는 입력 장치의 사용과 신뢰하는 장치 목록 작성을 허용하거나 금지할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 장치 제어를 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.

4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.

5. **장치 제어** 확인란을 선택합니다.

6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.

7. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.

   장치 유형 탭에는 장치 제어 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.

8. **Bluetooth** 장치 유형의 경우 **허용**, **차단**, **허용하고 기록하지 않음** 등의 접근 모드를 선택합니다.

   모든 Bluetooth 장치를 차단 또는 허용하거나, Bluetooth 입력 장치(HID(휴먼 인터페이스 장치) 클래스)의 연결만 허용할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서만 입력 장치 연결을 허용할 수 있습니다. 관리 콘솔(MMC)이나 Kaspersky Industrial CyberSecurity for Nodes 콘솔에서는 입력 장치 연결을 허용할 수 없습니다.

9. **USB 키보드** 및 **USB 마우스** 장치 유형의 경우, **허용**, **차단**, **연결 버스에 종속** 등의 접근 모드를 선택합니다.
10. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 장치 제어를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **로컬 활동 제어** → **장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.
5. **장치 제어 사용** 확인란을 선택합니다.
6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.
7. **장치 제어 설정** 블록에서 **장치 및 Wi-Fi 네트워크에 대한 접근 규칙** 옵션을 클릭합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
8. **Bluetooth** 장치 유형을 클릭해 접근 규칙 속성을 엽니다.
9. 접근 모드를 **허용**, **차단**, **허용하고 기록하지 않음** 중에서 선택합니다.
   모든 Bluetooth 장치를 차단 또는 허용하거나, Bluetooth 입력 장치(HID(휴먼 인터페이스 장치) 클래스)의 연결만 허용할 수 있습니다.
10. **USB 키보드** 및 **USB 마우스** 장치 유형의 경우, **허용**, **차단**, **연결 버스에 종속** 등의 접근 모드를 선택합니다.
11. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 장치 제어를 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **장치 제어** 옵션을 선택합니다.
2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.
3. **장치 제어** 확인란을 선택합니다.
4. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.
5. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
6. **Bluetooth** 장치 유형의 경우 **허용**, **차단**, **허용하고 기록하지 않음** 등의 접근 모드를 선택합니다.

모든 Bluetooth 장치를 차단 또는 허용하거나, Bluetooth 입력 장치(HID(휴먼 인터페이스 장치) 클래스)의 연결만 허용할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서만 입력 장치 연결을 허용할 수 있습니다. 관리 콘솔(MMC)이나 Kaspersky Industrial CyberSecurity for Nodes 콘솔에서는 입력 장치 연결을 허용할 수 없습니다.

7. **USB 키보드** 및 **USB 마우스** 장치 유형의 경우, **허용**, **차단**, **연결 버스에 종속** 등의 접근 모드를 선택합니다.

8. 변경 사항을 저장합니다.

모바일 장치에 대한 액세스 관리

Kaspersky Industrial CyberSecurity for Nodes를 사용하면 Android 및 iOS를 실행하는 모바일 장치의 데이터에 대한 접근을 제어할 수 있습니다. 모바일 장치는 휴대용 장치(MTP) 범주에 속합니다. 따라서 모바일 장치에서 데이터 접근을 구성하려면 휴대용 장치(MTP)에 대한 접근 설정을 편집해야 합니다.

모바일 장치가 컴퓨터에 연결되면 운영 체제가 장치 유형을 결정합니다. 컴퓨터에 iTunes 또는 유사한 애플리케이션이 설치되어 있으면 Android Debug Bridge(ADB 애플리케이션에 대한 자세한 내용은 기술 자료 및 Android 기술 지원 웹사이트 참조), 운영 체제는 모바일 장치를 ADB 또는 iTunes 장치로 식별합니다. 다른 모든 경우 운영 체제는 모바일 장치 유형을 파일 전송을 위한 휴대용 장치(MTP), 이미지 전송을 위한 PTP 장치(카메라) 또는 다른 장치로 식별할 수 있습니다. 장치 유형은 모바일 장치의 모델과 선택한 USB 연결 모드에 따라 다릅니다. Kaspersky Industrial CyberSecurity for Nodes를 사용하면 ADB 애플리케이션, iTunes 또는 파일 관리자에서 모바일 장치의 데이터에 대한 개별 접근 권한을 구성할 수 있습니다. 그 외의 경우, 장치 제어는 휴대용 장치(MTP) 접근 규칙에 따라 모바일 장치에 대한 접근을 허용합니다.

모바일 장치에 대한 접근

모바일 장치는 휴대용 장치(MTP) 범주에 속하므로 설정이 같습니다. 모바일 장치에 대한 다음 접근 모드 중 하나를 선택할 수 있습니다:

- **허용**. Kaspersky Industrial CyberSecurity for Nodes는 모바일 장치에 대한 모든 접근 권한을 부여합니다. 파일 관리자 또는 ADB 및 iTunes 애플리케이션을 사용하여 모바일 장치에서 파일을 열거나 생성, 수정, 복사 또는 삭제할 수 있습니다. 모바일 장치를 컴퓨터의 USB 포트에 연결하여 장치의 배터리를 충전할 수도 있습니다.

- **차단**. Kaspersky Industrial CyberSecurity for Nodes는 파일 관리자와 ADB 및 iTunes 애플리케이션에서 모바일 장치에 대한 접근을 제한합니다. 애플리케이션은 신뢰하는 모바일 장치에만 접근을 허용합니다. 모바일 장치를 컴퓨터의 USB 포트에 연결하여 장치의 배터리를 충전할 수도 있습니다.

- **연결 버스에 종속**. Kaspersky Industrial CyberSecurity for Nodes는 USB 버스 연결 상태(**허용** 또는 **차단**)에 따라 모바일 장치 연결을 허용합니다.

- **규칙에 따라**. Kaspersky Industrial CyberSecurity for Nodes는 규칙에 따라 모바일 장치에 대한 접근을 제한합니다. 규칙에서 접근 권한(읽기/쓰기)을 구성하고, 모바일 장치에 접근할 수 있는 사용자 또는 사용자 그룹을 선택하고, 모바일 장치에 대한 접근 스케줄을 구성할 수 있습니다. ADB 및 iTunes 애플리케이션을 통해 모바일 장치의 데이터에 대한 접근을 제한할 수도 있습니다.

모바일 장치 접근 규칙 구성

휴대용 장치(MTP), ADB 장치 및 iTunes 장치에 대한 접근 규칙은 다르게 구성됩니다. 휴대용 장치(MTP) 및 ADB 장치용 개별 사용자 또는 사용자 그룹에 대한 규칙을 구성하고 규칙이 적용되는 스케줄을 만들 수 있습니다. iTunes 장치의 경우에는 할 수 없습니다. 모든 사용자의 iTunes 애플리케이션을 통한 데이터로의 접근만 허용하거나 거부할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 모바일 장치 접근 규칙을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.
4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.
5. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.
6. **휴대용 장치(MTP)** 장치 유형의 마우스 오른쪽 메뉴에서 모바일 장치 접근 모드를 구성합니다: **허용**, **차단** 또는 **연결 버스에 종속**.
7. 모바일 장치 접근 규칙을 구성하려면 더블 클릭하여 규칙 목록을 엽니다.
8. 모바일 장치 접근 규칙 구성:
   a. **접근 규칙** 블록에서 **추가** 버튼을 클릭합니다.
      새 모바일 장치 접근 규칙을 추가할 수 있는 창이 열립니다.
   b. **우선순위** 필드에서 규칙 쓰기 우선순위를 설정합니다. 규칙에는 사용자 계정, 스케줄, 권한(읽기/쓰기/ADB 접근), 우선순위 속성이 포함됩니다.
      규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Industrial CyberSecurity for Nodes는 우선순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Industrial CyberSecurity for Nodes는 0부터 10,000까지 우선순위를 할당할 수 있습니다. 값이 클수록 우선순위가 높습니다. 다시 말해, 값이 0인 항목은 우선순위가 가장 낮습니다.
      예를 들어 Everyone 그룹에 읽기 전용 권한을 부여하고 관리자 그룹에 읽기/쓰기 권한을 부여할 수 있습니다. 이렇게 하려면 관리자 그룹에 우선 순위 1을 할당하고 Everyone 그룹에 우선 순위 0을 할당합니다.
      차단 규칙이 허용 규칙보다 우선합니다. 즉, 사용자가 여러 그룹에 추가된 상태에서 모든 규칙의 우선순위가 동일하다면 Kaspersky Industrial CyberSecurity for Nodes가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.
   c. **사용자 및 그룹 규칙**에서 사용자 또는 사용자 그룹을 선택합니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.
   d. **확인** 버튼을 클릭합니다.

9. **선택한 접근 규칙에 대한 스케줄**에서 사용자에 대한 모바일 장치 접근 스케줄을 구성합니다.

   ADB 장치에 대해 별도의 접근 스케줄을 구성할 수는 없습니다. ADB 장치 및 휴대용 장치(MTP)에 대한 공통 접근 스케줄을 구성할 수 있습니다.

10. 파일 관리자에서 모바일 장치에 대한 사용자의 접근 권한을 구성합니다(**읽기** / **쓰기**).

11. **ADB를 통한 액세스** 체크박스를 사용하여 ADB 애플리케이션을 통한 모바일 장치 데이터 접근을 구성합니다.
    확인란을 선택 취소하면 모바일 장치가 연결될 때 ADB 애플리케이션이 장치를 감지하지 못합니다.

12. **iTunes를 통한 액세스**에서 iTunes 애플리케이션을 통한 모바일 장치 데이터 접근을 구성합니다.

    Kaspersky Industrial CyberSecurity for Nodes는 모든 사용자의 iTunes 애플리케이션을 통한 모바일 장치 접근 권한 설정을 적용합니다. iTunes 장치에 대해 별도의 접근 스케줄을 구성할 수는 없습니다.

13. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 모바일 장치 접근 규칙을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어** → **장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.

5. **장치 제어 설정** 블록에서 **장치 및 Wi-Fi 네트워크에 대한 접근 규칙** 링크를 클릭합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.

6. **휴대용 장치(MTP)** 장치 유형을 선택합니다.
   이렇게 하면 휴대용 장치(MTP) 접근 권한이 열립니다.

7. 모바일 장치 접근 모드를 구성합니다: **허용**, **차단**, **연결 버스에 종속** 또는 **규칙에 따라**.

8. **iTunes를 통한 액세스**에서 iTunes 애플리케이션을 통한 모바일 장치 데이터 접근을 구성합니다.

   Kaspersky Endpoint Security는 모든 사용자의 iTunes 애플리케이션을 통한 모바일 장치 접근 권한 설정을 적용합니다. iTunes 장치에 대해 별도의 접근 스케줄을 구성할 수는 없습니다.

9. **규칙에 따라** 모드를 선택하면 장치 접근 규칙을 추가해야 합니다. 그러려면 **사용자**에서 **추가** 버튼을 클릭하고 모바일 장치 접근 규칙을 구성합니다.

   a. **우선순위** 필드에서 규칙 쓰기 우선순위를 설정합니다. 규칙에는 사용자 계정, 스케줄, 권한(읽기/쓰기/ADB 접근), 우선순위 속성이 포함됩니다.

규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Industrial CyberSecurity for Nodes는 우선순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Industrial CyberSecurity for Nodes는 0부터 10,000까지 우선순위를 할당할 수 있습니다. 값이 클수록 우선순위가 높습니다. 다시 말해, 값이 0인 항목은 우선순위가 가장 낮습니다.

예를 들어 Everyone 그룹에 읽기 전용 권한을 부여하고 관리자 그룹에 읽기/쓰기 권한을 부여할 수 있습니다. 이렇게 하려면 관리자 그룹에 우선 순위 1을 할당하고 Everyone 그룹에 우선 순위 0을 할당합니다.

차단 규칙이 허용 규칙보다 우선합니다. 즉, 사용자가 여러 그룹에 추가된 상태에서 모든 규칙의 우선순위가 동일하다면 Kaspersky Industrial CyberSecurity for Nodes가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.

b. **사용자**에서 모바일 장치에 접근할 사용자 또는 사용자 그룹을 선택합니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.

c. **장치 접근 스케줄**에서 사용자에 대한 모바일 장치 접근 스케줄을 구성합니다.

> ADB 장치에 대해 별도의 접근 스케줄을 구성할 수는 없습니다. ADB 장치 및 휴대용 장치(MTP)에 대한 공통 접근 스케줄을 구성할 수 있습니다.

d. 파일 관리자에서 모바일 장치에 대한 사용자의 접근 권한을 구성합니다(**읽기** / **쓰기**).

e. **ADB를 통한 액세스** 체크박스를 사용하여 ADB 애플리케이션을 통한 모바일 장치 데이터 접근을 구성합니다.

확인란을 선택 취소하면 모바일 장치가 연결될 때 ADB 애플리케이션이 장치를 감지하지 못합니다.

10. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 모바일 장치 접근 규칙을 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어 → 장치 제어** 옵션을 선택합니다.
2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.

   속성: 장치 제어 창이 열립니다.
3. **장치 유형** 탭을 선택합니다.

   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
4. **휴대용 장치(MTP)** 장치 유형의 마우스 오른쪽 메뉴에서 모바일 장치 접근 모드를 구성합니다: **허용**, **차단** 또는 **연결 버스에 종속**.
5. 모바일 장치 접근 규칙을 구성하려면 더블 클릭하여 규칙 목록을 엽니다.
6. 모바일 장치 접근 규칙 구성:

   a. **접근 규칙** 블록에서 **추가** 버튼을 클릭합니다.

   새 모바일 장치 접근 규칙을 추가할 수 있는 창이 열립니다.

   b. **우선순위** 필드에서 규칙 쓰기 우선순위를 설정합니다. 규칙에는 사용자 계정, 스케줄, 권한(읽기/쓰기/ADB 접근), 우선순위 속성이 포함됩니다.

규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Industrial CyberSecurity for Nodes는 우선순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Industrial CyberSecurity for Nodes는 0부터 10,000까지 우선순위를 할당할 수 있습니다. 값이 클수록 우선순위가 높습니다. 다시 말해, 값이 0인 항목은 우선순위가 가장 낮습니다.

예를 들어 Everyone 그룹에 읽기 전용 권한을 부여하고 관리자 그룹에 읽기/쓰기 권한을 부여할 수 있습니다. 이렇게 하려면 관리자 그룹에 우선 순위 1을 할당하고 Everyone 그룹에 우선 순위 0을 할당합니다.

차단 규칙이 허용 규칙보다 우선합니다. 즉, 사용자가 여러 그룹에 추가된 상태에서 모든 규칙의 우선순위가 동일하다면 Kaspersky Industrial CyberSecurity for Nodes가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.

c. **사용자 및 그룹 규칙**에서 사용자 또는 사용자 그룹을 선택합니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.

d. **확인** 버튼을 클릭합니다.

7. **선택한 접근 규칙에 대한 스케줄**에서 사용자에 대한 모바일 장치 접근 스케줄을 구성합니다.

ADB 장치에 대해 별도의 접근 스케줄을 구성할 수는 없습니다. ADB 장치 및 휴대용 장치(MTP)에 대한 공통 접근 스케줄을 구성할 수 있습니다.

8. 파일 관리자에서 모바일 장치에 대한 사용자의 접근 권한을 구성합니다(**읽기** / **쓰기**).

9. **ADB를 통한 액세스** 체크박스를 사용하여 ADB 애플리케이션을 통한 모바일 장치 데이터 접근을 구성합니다.

확인란을 선택 취소하면 모바일 장치가 연결될 때 ADB 애플리케이션이 장치를 감지하지 못합니다.

10. **iTunes를 통한 액세스**에서 iTunes 애플리케이션을 통한 모바일 장치 데이터 접근을 구성합니다.

Kaspersky Industrial CyberSecurity for Nodes는 모든 사용자의 iTunes 애플리케이션을 통한 모바일 장치 접근 권한 설정을 적용합니다. iTunes 장치에 대해 별도의 접근 스케줄을 구성할 수는 없습니다.

11. 변경 사항을 저장합니다.

결과적으로 규칙에 따라 모바일 장치에 대한 사용자 접근이 제한됩니다. ADB 및 iTunes 애플리케이션에서 모바일 장치에 대한 접근을 금지한 경우 모바일 장치를 연결할 때 ADB 및 iTunes 애플리케이션이 모바일 장치를 감지하지 못합니다.

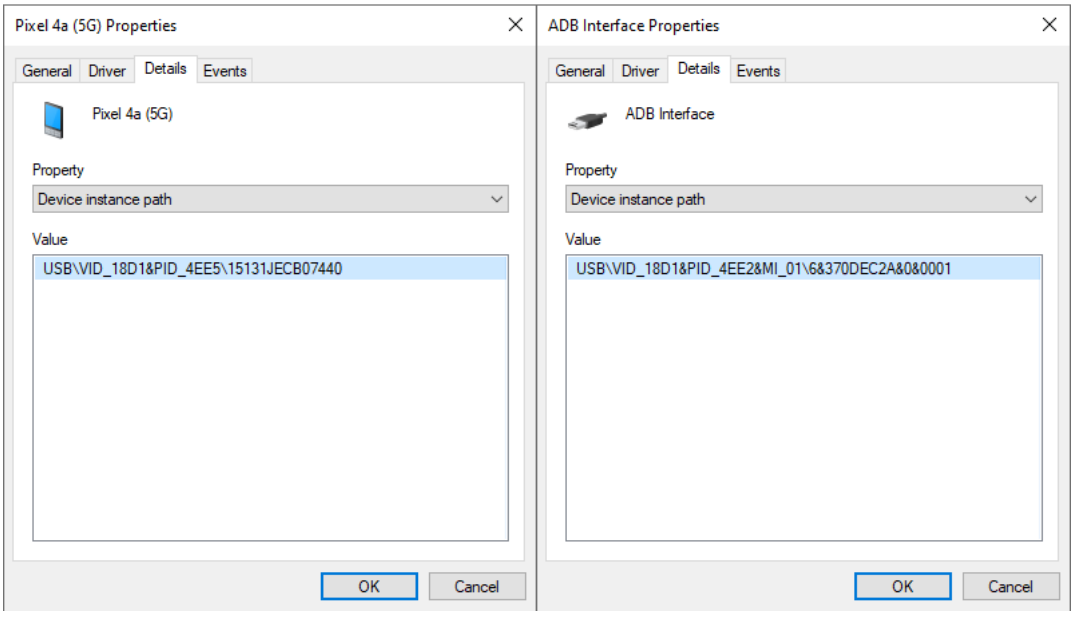
신뢰하는 모바일 장치

신뢰하는 모바일 장치 추가 절차는 다른 유형의 신뢰하는 장치에서와 같습니다. ID 또는 장치 모델별로 모바일 장치를 추가할 수 있습니다.

ID로 신뢰하는 모바일 장치를 추가하려면 고유 ID(하드웨어 ID, Hardware ID – HWID)가 필요합니다. 운영 체제 도구를 사용하여 장치 속성에서 ID를 찾을 수 있습니다(아래 그림 참조). 장치 관리자(Device Manager) 도구로 이 작업을 수행할 수 있습니다. 같은 모바일 장치라도 휴대용 장치(MTP)와 ADB, iTunes 장치의 ID는 서로 다릅니다. 휴대용 장치(MTP)의 ID 형식은 다음과 같습니다: `15131JECB07440`. ADB 장치의 ID 형식은 다음과 같습니다: `6&370DEC2A&0&0001`. 여러 특정 장치를 추가하려는 경우 ID별로 장치를 추가하는 것이 편리합니다. 마스크를 사용할 수도 있습니다.

장치를 컴퓨터에 연결한 후 ADB 또는 iTunes 애플리케이션을 설치한 경우 장치의 고유 ID가 재설정될 수 있습니다. 즉, Kaspersky Industrial CyberSecurity for Nodes는 이 장치를 새 장치로 식별합니다. 장치를 신뢰하는 경우 장치를 신뢰하는 목록에 다시 추가하십시오.

장치 모델별로 신뢰하는 모바일 장치를 추가하려면 공급사 ID(Vendor ID – VID) 및 제품 ID(Product ID – PID)가 필요합니다. 운영 체제 도구를 사용하여 장치 속성에서 ID를 찾을 수 있습니다(아래 그림 참조). VID 및 PID 입력을 위한 템플릿: `VID_18D1&PID_4EE5`. 조직에서 특정 모델의 장치를 사용하는 경우 모델별로 장치를 추가하는 것이 편리합니다. 이런 식으로 이 모델의 모든 장치를 추가할 수 있습니다.



장치 관리자의 장치 ID

이동식 드라이브 사용 감시

이동식 드라이브 사용 감시는 다음을 포함합니다:

- 이동식 드라이브의 파일에 대한 동작 모니터링.
- 신뢰하는 이동식 드라이브의 연결 및 연결 해제 모니터링.

  Kaspersky Industrial CyberSecurity for Nodes를 사용하면 이동식 드라이브뿐만 아니라 모든 신뢰하는 장치의 연결 및 연결 해제를 모니터링할 수 있습니다. 장치 제어 구성 요소에 대한 이벤트 기록은 알림 설정에서 켤 수 있습니다. 이벤트에는 *정보* 심각도가 있습니다.

Kaspersky Security Center 관리 콘솔에서 이동식 드라이브의 파일 동작 모니터링을 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.

4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.

5. **장치 제어** 확인란을 선택합니다.

6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.

7. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   장치 유형 탭에는 장치 제어 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.

8. **이동식 드라이브** 장치 유형을 선택하고 **로그 기록** 버튼을 클릭합니다.
   그러면 이벤트 기록 창이 열립니다.

9. **로그 기록 사용** 확인란을 선택합니다.

10. **파일 동작** 블록에서 **쓰기**, **삭제** 등 감시할 동작을 선택합니다.

11. **파일 형식 필터링** 블록에서 장치 제어 구성 요소를 통해 연관된 동작을 기록할 파일 형식을 선택합니다.

12. 감시할 이동식 드라이브를 사용하는 사용자 또는 사용자 그룹을 선택합니다.

13. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 이동식 드라이브의 파일 동작 모니터링을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어** → **장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.

5. **장치 제어 사용** 확인란을 선택합니다.

6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.

7. **장치 제어 설정** 블록에서 **장치 및 Wi-Fi 네트워크에 대한 접근 규칙** 옵션을 클릭합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.

8. **이동식 드라이브** 장치 유형을 더블 클릭하여 접근 규칙 속성을 엽니다.

9. 창이 열리면 **로그 기록** 탭을 선택합니다.

10. 토글 스위치를 **로그 기록 활성화됨**으로 설정합니다.

11. **파일 동작** 블록에서 **쓰기**, **삭제** 등 감시할 동작을 선택합니다.

12. **파일 형식 필터링** 블록에서 장치 제어 구성 요소를 통해 연관된 동작을 기록할 파일 형식을 선택합니다.

13. 감시할 이동식 드라이브를 사용하는 사용자 또는 사용자 그룹을 선택합니다.

14. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 이동식 드라이브의 파일 동작 모니터링을 활성화하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **장치 제어** 옵션을 선택합니다.

2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.

3. **장치 제어** 확인란을 선택합니다.

4. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.

5. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.

6. **이동식 드라이브** 장치 유형을 선택하고 **로그 기록** 버튼을 클릭합니다.
   그러면 이벤트 기록 창이 열립니다.

7. **로그 기록 사용** 확인란을 선택합니다.

8. **파일 동작** 블록에서 **쓰기**, **삭제** 등 감시할 동작을 선택합니다.

9. **파일 형식 필터링** 블록에서 장치 제어 구성 요소를 통해 연관된 동작을 기록할 파일 형식을 선택합니다.

10. 감시할 이동식 드라이브를 사용하는 사용자 또는 사용자 그룹을 선택합니다.

11. 변경 사항을 저장합니다.

그 결과 사용자가 이동식 드라이브에 있는 파일에 쓰기 또는 삭제 동작을 하면 Kaspersky Industrial CyberSecurity for Nodes는 해당 동작에 관한 정보를 이벤트 로그에 저장하고 Kaspersky Security Center로 이벤트를 전송합니다. **이벤트** 탭에서 **중앙 관리 서버** 노드의 작업 영역에 있는 Kaspersky Security Center 콘솔에서 이동식 드라이브의 파일 관련 이벤트를 확인할 수 있습니다. 로컬 Kaspersky Industrial CyberSecurity for Nodes 이벤트 로그에 이벤트가 표시되려면 장치 제어 구성 요소의 알림 설정에서 **파일 동작이 수행됨** 확인란을 선택해야 합니다.

Bluetooth 장치에 대한 접근 관리

Kaspersky Industrial CyberSecurity for Nodes는 Bluetooth 장치에 대한 접근을 관리합니다. Bluetooth 장치에는 무선 키보드, 마우스, 헤드셋, 프린터 등이 포함됩니다. Bluetooth를 사용하여 모바일 장치와 통신할 수도 있습니다.

Bluetooth 장치가 연결되거나 연결 해제되면 애플리케이션은 장치에 대한 여러 이벤트를 생성할 수 있습니다. 운영 체제가 Bluetooth 장치를 서로 다른 유형의 여러 장치로 감지할 수 있기 때문입니다. 또한 Kaspersky Industrial CyberSecurity for Nodes는 장치가 연결되는 Bluetooth 어댑터도 별도의 장치로 관리합니다. 이것이 바로 애플리케이션이 탐지하는 장치마다 이벤트를 생성하는 이유입니다.

Bluetooth 장치에 대한 다음 접근 모드 중 하나를 선택할 수 있습니다.

- **허용하고 기록하지 않음**. Kaspersky Industrial CyberSecurity for Nodes가 모든 Bluetooth 장치의 연결을 허용하며, 연결에 대한 정보를 이벤트 로그에 저장하지 않습니다. Bluetooth 입력 장치(키보드, 마우스 등)를 연결하고, Bluetooth를 통해 데이터를 전송하고, 다른 Bluetooth 장치(헤드셋, 헤드폰 등)를 관리할 수 있습니다.
- **허용**. Kaspersky Industrial CyberSecurity for Nodes가 모든 Bluetooth 장치의 연결을 허용합니다. Bluetooth 입력 장치(키보드, 마우스 등)를 연결하고, Bluetooth로 데이터를 전송하고, 기타 Bluetooth 장치(헤드셋, 헤드폰 등)를 관리할 수 있습니다.
- **차단**. Kaspersky Industrial CyberSecurity for Nodes가 Bluetooth 장치에 대한 접근을 제한합니다. Bluetooth 입력 장치(휴먼 인터페이스 장치 클래스) 연결만 허용됩니다. 이러한 장치에는 키보드, 마우스, 조이스틱 등이 포함됩니다.

신뢰하는 Bluetooth 장치 목록을 생성할 수 없습니다. Bluetooth 장치 접근을 제한했을 경우, Bluetooth 입력 장치 연결만 가능합니다.

Kaspersky Security Center 웹 콘솔이나 애플리케이션 콘솔에서만 입력 장치 연결을 허용할 수 있습니다. Kaspersky Security Center 관리 콘솔에서는 입력 장치 연결을 허용할 수 없습니다.

Kaspersky Security Center 관리 콘솔에서 Bluetooth 장치 접근 규칙을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **로컬 활동 제어** → **장치 제어** 옵션을 선택하고 **설정** 버튼을 클릭합니다.
4. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.
5. **Bluetooth** 장치 유형의 마우스 오른쪽 메뉴에서, Bluetooth 장치 접근 모드를 구성합니다: **허용**, **차단**, **허용하고 기록하지 않음**.

   Bluetooth 장치에 대한 접근을 차단한 경우 애플리케이션 콘솔이나 Kaspersky Security Center 웹 콘솔에서 입력 장치(키보드, 마우스 등)만 연결하도록 허용할 수 있습니다. Kaspersky Security Center 관리 콘솔에서는 입력 장치 연결을 허용할 수 없습니다.
6. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 Bluetooth 장치 접근 규칙을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. 정책 창에서 **로컬 활동 제어** → **장치 제어** 옵션을 선택하고 **설정** 버튼을 클릭합니다.

5. **장치 제어 설정** 블록에서 **장치 및 Wi-Fi 네트워크에 대한 접근 규칙** 링크를 클릭합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.

6. **Bluetooth** 장치 유형을 선택합니다.
   이것을 선택하면 Bluetooth 장치 접근 설정이 열립니다.

7. Bluetooth 장치 접근 모드를 구성합니다: **허용**, **차단**, **허용하고 기록하지 않음**.

8. **차단** 모드를 선택하면 Bluetooth 입력 장치(키보드, 마우스 등)만 연결하도록 허용할 수 있습니다. 이렇게 하려면 **예외**에서 **입력 장치(마우스 및 키보드)** 확인란을 선택합니다.

9. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 Bluetooth 장치 접근 규칙을 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어 → 장치 제어** 옵션을 선택합니다.

2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.

3. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.

4. **접근**에서 Bluetooth 장치 접근 모드를 구성합니다: **허용**, **차단**, **허용하고 기록하지 않음**.

5. **차단** 모드를 선택하면 Bluetooth 입력 장치(키보드, 마우스 등)만 연결하도록 허용할 수 있습니다. 이렇게 하려면 **예외 규칙**에서 **입력 장치(마우스 및 키보드)** 확인란을 선택합니다.

6. 변경 사항을 저장합니다.

장치에 대한 사용자 접근 권한의 구분

장치 유형이나 신뢰하는 장치에 대한 사용자 접근 권한을 구성할 수 있습니다.

장치 유형에 따른 사용자 접근 권한의 구분

장치 제어 구성 요소를 통해 *저장 장치*의 데이터에 대한 사용자 접근 권한을 구성할 수 있습니다. 이러한 장치에 쓰기 및 읽기 권한을 구성할 수 있습니다. 장치 제어 구성 요소는 다음 유형의 저장 장치를 지원합니다:

- 하드 드라이브
- 이동식 드라이브
- 플로피 디스크
- CD/DVD 드라이브
- 휴대용 장치(MTP) 휴대용 장치(MTP)는 예를 들어 모바일 장치, 사진 카메라, 미디어 플레이어 등을 포함합니다.

이러한 방식으로 관리자 그룹에만 이동식 미디어를 사용하도록 허용하거나 할 수 있습니다. 다른 장치 유형에는 모든 사용자의 접근을 거부하거나 허용할 수 있습니다. 프린터를 사용하기 위한 사용자 접근 권한도 구성할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 이동식 드라이브의 데이터에 대한 사용자 접근 권한을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.
4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.
5. **장치 제어** 확인란을 선택합니다.
6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.
7. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   장치 유형 탭에는 장치 제어 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
8. 저장 장치 접근 규칙을 구성하려면 더블 클릭하여 규칙 목록을 엽니다.
9. 저장 장치 접근 규칙 구성:
   a. **접근 규칙** 블록에서 **추가** 버튼을 클릭합니다.
      새 저장 장치 접근 규칙을 추가할 수 있는 창이 열립니다.
   b. **우선순위** 필드에서 *규칙 쓰기*/ 우선순위를 설정합니다. 규칙에는 사용자 계정, 스케줄, 권한(읽기/쓰기), 우선순위 속성이 포함됩니다.
      규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Industrial CyberSecurity for Nodes는 우선순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Industrial CyberSecurity for Nodes는 0부터 10,000까지 우선순위를 할당할 수 있습니다. 값이 클수록 우선순위가 높습니다. 다시 말해, 값이 0인 항목은 우선순위가 가장 낮습니다.
      예를 들어 Everyone 그룹에 읽기 전용 권한을 부여하고 관리자 그룹에 읽기/쓰기 권한을 부여할 수 있습니다. 이렇게 하려면 관리자 그룹에 우선 순위 1을 할당하고 Everyone 그룹에 우선 순위 0을 할당합니다.
      차단 규칙이 허용 규칙보다 우선합니다. 즉, 사용자가 여러 그룹에 추가된 상태에서 모든 규칙의 우선순위가 동일하다면 Kaspersky Industrial CyberSecurity for Nodes가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.
   c. **사용자 및 그룹 규칙**에서 사용자 또는 사용자 그룹을 선택합니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.
   d. **확인** 버튼을 클릭합니다.
10. **선택한 접근 규칙에 대한 스케줄**에서 사용자에 대한 저장 장치 접근 스케줄을 구성합니다.
    예를 들어 사용자가 작업 시간에만 저장 장치를 사용하도록 허용할 수 있습니다.
11. 파일 관리자에서 저장 장치에 대한 사용자의 접근 권한을 구성합니다(**읽기** / **쓰기**).
12. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔 에서 저장 장치의 데이터에 대한 사용자 접근 권한을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **로컬 활동 제어** → **장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.
5. **장치 제어 사용** 확인란을 선택합니다.
6. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.
7. **장치 제어 설정** 블록에서 **장치 및 Wi-Fi 네트워크에 대한 접근 규칙** 옵션을 클릭합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
8. **저장 장치에 대한 접근** 블록에서 저장 장치 접근 규칙의 속성을 엽니다.
9. 저장 장치 접근 규칙 구성:
   a. **사용자** 블록에서 **추가** 버튼을 클릭합니다.
      새 저장 장치 접근 규칙을 추가할 수 있는 창이 열립니다.
   b. **우선순위** 필드에서 *규칙 쓰기* 우선순위를 설정합니다. 규칙에는 사용자 계정, 스케줄, 권한(읽기/쓰기), 우선순위 속성이 포함됩니다.
      규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Industrial CyberSecurity for Nodes는 우선순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Industrial CyberSecurity for Nodes는 0부터 10,000까지 우선순위를 할당할 수 있습니다. 값이 클수록 우선순위가 높습니다. 다시 말해, 값이 0인 항목은 우선순위가 가장 낮습니다.
      예를 들어 Everyone 그룹에 읽기 전용 권한을 부여하고 관리자 그룹에 읽기/쓰기 권한을 부여할 수 있습니다. 이렇게 하려면 관리자 그룹에 우선 순위 1을 할당하고 Everyone 그룹에 우선 순위 0을 할당합니다.
      차단 규칙이 허용 규칙보다 우선합니다. 즉, 사용자가 여러 그룹에 추가된 상태에서 모든 규칙의 우선순위가 동일하다면 Kaspersky Industrial CyberSecurity for Nodes가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.
   c. **사용자**에서 사용자 또는 사용자 그룹을 선택합니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.
   d. **장치 접근 스케줄**에서 사용자에 대한 저장 장치 접근 스케줄을 구성합니다.
      예를 들어 사용자가 작업 시간에만 저장 장치를 사용하도록 허용할 수 있습니다.
   e. 파일 관리자에서 저장 장치에 대한 사용자의 접근 권한을 구성합니다(**읽기** / **쓰기**).
   f. **확인** 버튼을 클릭합니다.
10. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 저장 장치의 데이터에 대한 사용자 접근 권한을 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **장치 제어** 옵션을 선택합니다.
2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.
3. **장치 제어** 확인란을 선택합니다.
4. **차단 규칙 운영 모드** 블록에서 **차단** 또는 **알림** 옵션을 선택합니다.
5. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
6. 저장 장치 접근 규칙을 구성하려면 더블 클릭하여 규칙 목록을 엽니다.
7. 저장 장치 접근 규칙 구성:
   a. **접근 규칙** 블록에서 **추가** 버튼을 클릭합니다.
      새 저장 장치 접근 규칙을 추가할 수 있는 창이 열립니다.
   b. **규칙 우선순위** 필드에서 *규칙 쓰기* 우선순위를 설정합니다. 규칙에는 사용자 계정, 스케줄, 권한(읽기/쓰기), 우선 순위 속성이 포함됩니다.
      규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Industrial CyberSecurity for Nodes는 우선순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Industrial CyberSecurity for Nodes는 0부터 10,000까지 우선순위를 할당할 수 있습니다. 값이 클수록 우선순위가 높습니다. 다시 말해, 값이 0인 항목은 우선순위가 가장 낮습니다.
      예를 들어 Everyone 그룹에 읽기 전용 권한을 부여하고 관리자 그룹에 읽기/쓰기 권한을 부여할 수 있습니다. 이렇게 하려면 관리자 그룹에 우선 순위 1을 할당하고 Everyone 그룹에 우선 순위 0을 할당합니다.
      차단 규칙이 허용 규칙보다 우선합니다. 즉, 사용자가 여러 그룹에 추가된 상태에서 모든 규칙의 우선순위가 동일하다면 Kaspersky Industrial CyberSecurity for Nodes가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.
   c. **사용자 및 그룹 규칙**에서 사용자 또는 사용자 그룹을 선택합니다. Active Directory에서 사용자를 선택하거나 로컬 사용자 이름을 직접 입력할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.
   d. **확인** 버튼을 클릭합니다.
8. **선택한 접근 규칙에 대한 스케줄**에서 사용자에 대한 저장 장치 접근 스케줄을 구성합니다.
   예를 들어 사용자가 작업 시간에만 저장 장치를 사용하도록 허용할 수 있습니다.
9. 파일 관리자에서 저장 장치에 대한 사용자의 접근 권한을 구성합니다(**읽기** / **쓰기**).
10. 변경 사항을 저장합니다.

신뢰하는 장치에 대한 사용자 접근 권한 구분

*신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다. 신뢰하는 장치를 사용하려면 개별 사용자, 사용자 그룹 또는 조직의 모든 사용자에게 접근 권한을 부여할 수 있습니다. 신뢰하는 장치의 속성에 대한 사용자 접근 권한을 구성할 수 있습니다.

장치 제어를 위한 규칙 생성기 정보

회사 네트워크의 모든 보호 중인 장치 및 보호 중인 장치 그룹에 대해 Kaspersky Security Center 작업 및 정책을 동시에 사용하여 장치 제어 규칙을 생성할 수 있습니다. 신뢰하는 장치 목록을 만들려면 조직의 외부 장치에 대한 감사를 수행해야 합니다.

개별 보호 중인 장치에 연결된 장치 목록을 기반으로 규칙 목록을 생성하려면 애플리케이션 콘솔을 사용하여 *장치 제어를 위한 규칙 생성기* 작업을 로컬에서 실행할 수 있습니다.

Kaspersky Security Center를 사용하여 다음과 같은 방법으로 장치 제어 규칙을 생성할 수 있습니다.

- *장치 제어를 위한 규칙 생성기* 작업을 사용합니다.

  설정에 따라 *장치 제어를 위한 규칙 생성기* 작업은 컴퓨터에 연결된 적이 있고 운영 체제에 정보가 저장되어 있는 모든 장치에 대한 정보 또는 작업이 시작되는 시점에 연결되어 있는 장치에 대한 정보를 수집할 수 있습니다. 수집된 정보를 기반으로 작업에서 장치 제어 구성 요소에 대한 허용 규칙 목록을 생성합니다. 생성된 규칙을 장치 제어 구성 요소 규칙 목록으로 자동 가져오도록 구성하거나 수동으로 가져올 수 있습니다.

  예를 들어 장치 제어 구성 요소를 처음 실행하기 전에 과거에 사용한 신뢰하는 장치에 대한 허용 규칙을 빠르게 생성해야 하는 경우 이 시나리오를 사용할 수 있습니다.

  Kaspersky Security Center 관리 콘솔에서 장치 제어를 위한 규칙 생성기 작업을 실행하는 방법

  1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
  2. 콘솔 트리에서 **작업** 옵션을 선택합니다.
  3. *장치 제어를 위한 규칙 생성기* 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.

     필요하다면 새 작업을 만듭니다.
  4. **모드** 섹션에서 작업 모드를 선택합니다:

     - **지금까지 연결된 모든 외부 장치에 대해 시스템 데이터 고려**.

       애플리케이션은 운영 체제 메모리에서 컴퓨터에 연결된 적이 있는 모든 장치에 관한 정보를 가져옵니다.
     - **현재 연결된 외부 장치만 고려**.

       애플리케이션은 작업이 시작될 때 연결된 장치에 관한 정보를 가져옵니다.
  5. 데이터와 함께 파일을 저장할 경로를 입력합니다.
  6. 여러 컴퓨터에서 작업을 실행하는 경우 **파일 이름에 보호 중인 장치 세부 정보 추가** 확인란을 선택하는 것이 좋습니다.

7. 변경 사항을 저장합니다.

8. 작업을 실행합니다.

웹 콘솔에서 장치 제어를 위한 규칙 생성기 작업을 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
   작업 목록이 열립니다.

2. *장치 제어를 위한 규칙 생성기* 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.
   필요하다면 새 작업을 만듭니다.

3. **모드** 섹션에서 작업 모드를 선택합니다:

   - **지금까지 연결된 모든 외부 장치에 대해 시스템 데이터 고려**.
     애플리케이션은 운영 체제 메모리에서 컴퓨터에 연결된 적이 있는 모든 장치에 관한 정보를 가져옵니다.

   - **현재 연결된 외부 장치만 고려**.
     애플리케이션은 작업이 시작될 때 연결된 장치에 관한 정보를 가져옵니다.

4. 데이터와 함께 파일을 저장할 경로를 입력합니다.

5. 여러 컴퓨터에서 작업을 실행하는 경우 **파일 이름에 보호 중인 장치 세부 정보 추가** 확인란을 선택하는 것이 좋습니다.

6. 변경 사항을 저장합니다.

7. 작업을 실행합니다.

웹 콘솔에서 장치 제어를 위한 규칙 생성기 작업을 실행하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **규칙 자동 생성** → **장치 제어를 위한 규칙 생성기** 옵션을 선택합니다.

2. **장치 제어를 위한 규칙 생성기** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어를 위한 규칙 생성기 창이 열립니다.

3. **모드** 섹션에서 작업 모드를 선택합니다:

   - **지금까지 연결된 모든 외부 장치에 대해 시스템 데이터 고려**.
     애플리케이션은 운영 체제 메모리에서 컴퓨터에 연결된 적이 있는 모든 장치에 관한 정보를 가져옵니다.

   - **현재 연결된 외부 장치만 고려**.
     애플리케이션은 작업이 시작될 때 연결된 장치에 관한 정보를 가져옵니다.

4. **작업 완료 후** 섹션에서 작업 완료 후 애플리케이션 동작을 선택합니다:

   - **장치 제어 규칙 목록에 허용 규칙 추가**. 장치 제어 규칙 목록은 장치 제어 구성 요소 설정에서 사용할 수 있습니다.

     이 확인란을 선택하면 애플리케이션이 선택된 규칙 추가 원칙을 기반으로 작업이 생성한 규칙을 장치 제어 규칙 목록에 추가합니다.

     이 확인란을 선택 해제하면 애플리케이션이 장치 제어 규칙 목록에 새로 생성된 허용 규칙을 추가하지 않습니다. 애플리케이션은 규칙을 파일로 내보내기만 합니다.

- **추가 원칙**. 장치 제어 규칙 목록에 새로 생성된 허용 규칙을 추가하는 데 사용하는 방법입니다:
  - **기존 규칙에 추가**. 애플리케이션이 규칙을 기존 규칙 목록에 추가합니다. 이 경우 애플리케이션은 동일한 규칙을 복제합니다.
  - **기존 규칙 교체**. 애플리케이션이 기존 규칙 대신 새 규칙을 추가합니다.
  - **기존 규칙과 병합**. 애플리케이션이 규칙을 기존 규칙 목록에 추가합니다. 이 경우 애플리케이션은 동일한 규칙을 병합합니다.
- **파일에 허용 규칙 내보내기**. 애플리케이션이 아래 필드에 지정된 파일로 허용 규칙을 내보냅니다. 그런 다음 다른 컴퓨터의 애플리케이션 설정에서 파일을 가져와 허용 규칙을 배포할 수 있습니다. 이 파일을 사용하여 허용 규칙을 백업할 수도 있습니다.
- **파일 이름에 보호 중인 장치 세부 정보 추가**. 애플리케이션은 날짜 및 시간 외에도 내보낸 파일 이름에 컴퓨터 이름을 추가합니다. 여러 컴퓨터에서 허용 규칙을 수집하면 편리합니다.

5. 변경 사항을 저장합니다.

그 결과 Kaspersky Industrial CyberSecurity for Nodes는 외부 장치를 감사하고 Kaspersky Security Center의 레지스트리에 정보를 저장합니다. 외부 장치 목록은 신뢰하는 장치 추가 시 사용할 수 있습니다.

장치 제어를 위한 규칙 생성기 작업은 장치에 연결된 네트워크 프린터 및 Wi-Fi 네트워크에 대한 정보를 수집하지 않습니다. 이러한 유형의 장치에 대해서는 규칙을 수동으로 생성해야 합니다.

- **알림** 모드에서 실행 중인 장치 제어 구성 요소에 대해 Kaspersky Security Center에서 생성한 이벤트 리포트를 기반으로 합니다.

  이 시나리오에서 Kaspersky Industrial CyberSecurity for Nodes는 장치에 대한 접근을 차단하지 않습니다. 장치 제어 구성 요소가 **알림** 모드로 실행되면 애플리케이션은 모든 장치의 사용을 허용하고 외부 장치 연결 및 연결 해제 이벤트를 기록합니다.

  Kaspersky Security Center 관리 콘솔에서 알림 모드로 장치 제어를 활성화하는 방법

  1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
  2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
  3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.
  4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.
  5. **장치 제어** 확인란을 선택합니다.
  6. **차단 규칙 운영 모드**에서 **알림** 옵션을 선택합니다.
  7. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

  Kaspersky Security Center 웹 콘솔에서 알림 모드로 장치 제어를 활성화하는 방법

  1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
  2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

     정책 속성 창이 열립니다.
  3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어** → **장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.

5. **장치 제어 사용** 확인란을 선택합니다.

6. **차단 규칙 운영 모드**에서 **알림** 옵션을 선택합니다.

7. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 알림 모드로 장치 제어를 활성화하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **장치 제어** 옵션을 선택합니다.

2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.

3. **장치 제어** 확인란을 선택합니다.

4. **차단 규칙 운영 모드**에서 **알림** 옵션을 선택합니다.

5. 변경 사항을 저장합니다.

구성 요소가 실행되는 동안 보호 중인 장치 및 보호 중인 장치 그룹에 대해 가능한 모든 시나리오를 실행해야 합니다. 그런 다음 Kaspersky Security Center 이벤트 리포트의 정보를 TXT 파일로 가져오고 리포트를 검토한 후 신뢰하는 장치를 추가할 수 있습니다.

이 시나리오는 회사 네트워크에 유형이 다양하고 서로 다른 외부 장치 집합을 사용하는 보호 중인 장치가 다수 포함된 경우에 권장됩니다.

신뢰하는 장치 추가

*신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.

신뢰하는 장치를 사용하려면 개별 사용자, 사용자 그룹 또는 조직의 모든 사용자에게 접근 권한을 부여할 수 있습니다.

예를 들어 조직에서 이동식 드라이브 사용을 허용하지 않지만 관리자가 작업 중 이동식 드라이브를 사용하는 경우 관리자 그룹에 대해서만 이동식 드라이브를 허용할 수 있습니다. 그렇게 하려면 신뢰하는 목록에 이동식 드라이브를 추가하고 사용자 접근 권한을 구성합니다.

> 신뢰할 수 있는 장치를 1000개 이상 추가할 경우 시스템이 불안정해질 수 있으므로 권장하지 않습니다.

Kaspersky Security Center 관리 콘솔의 신뢰하는 목록에 신뢰하는 장치를 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.

4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.

5. **장치 모니터링 설정**에서 **신뢰하는 장치** 탭을 선택합니다.
   그러면 신뢰하는 장치 목록이 열립니다.

6. 회사의 모든 컴퓨터에 대해 신뢰하는 장치의 통합 목록을 만들려면 **상속할 때 값 병합** 확인란을 선택합니다.
   부모 및 자식 정책의 신뢰하는 장치 목록이 병합됩니다. 상속할 때 값 병합이 활성화된 경우 목록이 병합됩니다. 부모 정책의 신뢰하는 장치는 자식 정책에 읽기 전용 보기로 표시됩니다. 부모 정책의 신뢰하는 장치를 변경하거나 삭제할 수 없습니다.

7. **추가** 버튼을 클릭하고 신뢰하는 목록에 장치를 추가하는 방법을 선택합니다:

   - **연결된 장치를 기반으로 규칙 생성**.
   - **시스템 데이터를 기반으로 규칙 생성**.
   - **Kaspersky Security Center 레지스트리를 기반으로 규칙 생성**.

   장치 목록이 비어 있으면 외부 장치 감사를 수행해야 합니다. 이를 위해서는 *장치 제어를 위한 규칙 생성기* 작업을 실행합니다.

   > Kaspersky Industrial CyberSecurity for Nodes는 **플로피 디스크** 유형의 장치를 신뢰하는 목록에 추가하는 것을 지원하지 않습니다.

8. **선택한 장치에 규칙 추가** 버튼을 클릭합니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 신뢰하는 장치를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어** → **장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.

5. **장치 제어 설정** 블록에서 **신뢰하는 장치** 옵션을 클릭합니다.
   그러면 신뢰하는 장치 목록이 열립니다.

6. 회사의 모든 컴퓨터에 대해 신뢰하는 장치의 통합 목록을 만들려면 **상속할 때 값 병합** 확인란을 선택합니다.
   부모 및 자식 정책의 신뢰하는 장치 목록이 병합됩니다. 상속할 때 값 병합이 활성화된 경우 목록이 병합됩니다. 부모 정책의 신뢰하는 장치는 자식 정책에 읽기 전용 보기로 표시됩니다. 부모 정책의 신뢰하는 장치를 변경하거나 삭제할 수 없습니다.

7. **KSC 레지스트리에서** 버튼을 클릭합니다.
   장치 목록이 비어 있으면 외부 장치 감사를 수행해야 합니다. 이를 위해서는 *장치 제어를 위한 규칙 생성기* 작업을 실행합니다.

Kaspersky Industrial CyberSecurity for Nodes는 **플로피 디스크** 유형의 장치를 신뢰하는 목록에 추가하는 것을 지원하지 않습니다.

8. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 신뢰하는 장치를 추가하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **장치 제어** 옵션을 선택합니다.
2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.
3. **장치 제어 설정**에서 **신뢰하는 장치** 탭을 선택합니다.
   그러면 신뢰하는 장치 목록이 열립니다.
4. **추가** 버튼을 클릭하고 신뢰하는 목록에 장치를 추가하는 방법을 선택합니다:
   - **연결된 장치를 기반으로 규칙 생성**.
   - **시스템 데이터를 기반으로 규칙 생성**.
   - **Kaspersky Security Center 레지스트리를 기반으로 규칙 생성**.

   장치 목록이 비어 있으면 외부 장치 감사를 수행해야 합니다. 이를 위해서는 *장치 제어를 위한 규칙 생성기* 작업을 실행합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 **플로피 디스크** 유형의 장치를 신뢰하는 목록에 추가하는 것을 지원하지 않습니다.

5. **선택한 장치에 규칙 추가** 버튼을 클릭합니다.
6. 변경 사항을 저장합니다.

신뢰하는 장치 목록 내보내기 및 가져오기

신뢰하는 장치 목록을 조직의 모든 컴퓨터에 배포하려면 내보내기/가져오기 절차를 사용합니다. 신뢰하는 장치 목록을 XML 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 동일 유형의 장치를 여러 개 추가하는 등의 작업을 진행할 수 있습니다. 내보내기/가져오기 기능을 사용하여 신뢰하는 장치 목록을 백업하거나 목록을 다른 서버로 마이그레이션할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes를 사용하면 Kaspersky Endpoint Security for Windows에서 신뢰하는 장치 목록을 가져올 수 있습니다. 이러한 애플리케이션의 XML 파일 형식은 동일합니다.

Kaspersky Security Center 관리 콘솔에서 신뢰하는 장치 목록을 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **로컬 활동 제어** 옵션을 선택합니다.

4. **장치 제어** 섹션에서 **설정** 버튼을 클릭합니다.

5. **장치 제어 설정**에서 **신뢰하는 장치** 탭을 선택합니다.
   그러면 신뢰하는 장치 목록이 열립니다.

6. 신뢰하는 장치 목록을 내보내려면 다음을 수행합니다:

   a. 전체 목록을 내보내려면 버튼을 누르고 **내보내기**을 선택합니다.

   b. 목록의 일부만 내보내려면 다음 단계를 수행합니다.

      1. **Ctrl** 또는 **Shift** 키를 사용하여 내보낼 목록 항목을 선택합니다. 모든 항목을 선택하려면 **Ctrl+A**를 누릅니다.

      2. 버튼을 클릭하고 **선택 항목 내보내기**을 선택합니다.

   c. 창이 열리면 내보낼 XML 파일의 이름을 지정하고 파일을 저장할 폴더를 선택합니다. **저장** 버튼을 누릅니다.
      Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 장치 목록을 XML 파일로 내보냅니다.

7. 신뢰하는 장치 목록을 가져오려면 다음과 같이 진행합니다:

   a. **추가 → XML 파일에서 규칙 가져오기** 버튼을 클릭하고 추가 또는 교체 중에서 가져오기 모드를 선택합니다.
      창이 열리면 신뢰하는 장치 목록을 가져올 XML 파일을 선택합니다.
      병합 모드에서 애플리케이션은 신뢰하는 장치 목록을 확인하고 중복 항목을 제거합니다. 추가 모드에서 애플리케이션은 중복을 확인하지 않고 신뢰하는 애플리케이션 목록에 항목을 추가합니다.

   b. 파일을 엽니다.
      Kaspersky Industrial CyberSecurity for Nodes는 선택된 모드에 따라 신뢰하는 장치를 가져옵니다.

8. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

웹 콘솔에서 신뢰하는 장치 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어 → 장치 제어** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   장치 제어 창이 열립니다.

5. **장치 제어 설정** 블록에서 **신뢰하는 장치** 옵션을 클릭합니다.
   그러면 신뢰하는 장치 목록이 열립니다.

6. 신뢰하는 장치 목록을 내보내려면 다음을 수행합니다:

   a. 내보낼 신뢰하는 장치를 선택합니다.

   b. **내보내기** 버튼을 클릭하고 신뢰하는 장치의 전체 목록을 내보내기 및 선택한 신뢰하는 장치만 내보내기 중에서 내보내기 모드를 선택합니다.

   c. 파일을 저장합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 웹 리소스 주소 목록을 XML 파일로 내보냅니다.

7. 신뢰하는 장치 목록을 가져오려면 다음과 같이 진행합니다:

   a. **가져오기** 버튼을 클릭하고 추가 또는 교체 중에서 가져오기 모드를 선택합니다.

   b. 창이 열리면 웹 리소스 목록을 가져올 XML 파일을 선택합니다.

   c. 파일을 엽니다.

   Kaspersky Industrial CyberSecurity for Nodes는 선택된 모드에 따라 신뢰하는 장치를 가져옵니다.

8. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 콘솔에서 신뢰하는 장치 목록을 내보내고 가져오는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **장치 제어** 옵션을 선택합니다.

2. **장치 제어** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 장치 제어 창이 열립니다.

3. **장치 제어 설정**에서 **신뢰하는 장치** 탭을 선택합니다.
   그러면 신뢰하는 장치 목록이 열립니다.

4. 신뢰하는 장치 목록을 내보내려면 다음을 수행합니다:

   a. 전체 목록을 내보내려면 버튼을 누르고 **내보내기**을 선택합니다.

   b. 목록의 일부만 내보내려면 다음 단계를 수행합니다.

      1. **Ctrl** 또는 **Shift** 키를 사용하여 내보낼 목록 항목을 선택합니다. 모든 항목을 선택하려면 **Ctrl+A**를 누릅니다.

      2. 버튼을 클릭하고 **선택 항목 내보내기**을 선택합니다.

   c. 창이 열리면 내보낼 XML 파일의 이름을 지정하고 파일을 저장할 폴더를 선택합니다. **저장** 버튼을 누릅니다.

   Kaspersky Industrial CyberSecurity for Nodes는 신뢰하는 장치 목록을 XML 파일로 내보냅니다.

5. 신뢰하는 장치 목록을 가져오려면 다음과 같이 진행합니다:

   a. **추가** → **XML 파일에서 규칙 가져오기** 버튼을 클릭하고 추가 또는 교체 중에서 가져오기 모드를 선택합니다.
   창이 열리면 웹 리소스 목록을 가져올 XML 파일을 선택합니다.
   병합 모드에서 애플리케이션은 신뢰하는 장치 목록을 확인하고 중복 항목을 제거합니다. 추가 모드에서 애플리케이션은 중복을 확인하지 않고 신뢰하는 애플리케이션 목록에 항목을 추가합니다.

b. 파일을 엽니다.

Kaspersky Industrial CyberSecurity for Nodes는 선택된 모드에 따라 신뢰하는 장치를 가져옵니다.

6. 변경 사항을 저장합니다.

방화벽

방화벽 구성 요소는 다음 모드에서 작동할 수 있습니다.

- **Windows 방화벽 상태 관찰**. 애플리케이션 버전 4.0 이하의 방화벽 관리 작업 로직을 애플리케이션 버전 4.5 버전 이상의 방화벽 기능 전체로 원활하게 전환하기 위한 모드입니다. 애플리케이션 버전 4.0 이하를 업그레이드하면 Windows 방화벽에 통합된 방화벽 관리 작업의 규칙이 유지됩니다. 그러나 방화벽 구성 요소가 더는 Windows 방화벽과 상호작용을 하지 않으며, Windows 방화벽 트래픽 필터링만 모니터링하고 구성 요소의 작업 로그에 해당 이벤트를 기록합니다. 그런 다음 방화벽 규칙을 만들거나, Windows 방화벽 규칙을 가져오거나 방화벽 운영 모드를 **알림**으로 변경할 수 있습니다.

- **알림**. 애플리케이션은 방화벽 규칙의 작동을 모니터링하기만 하며 구성 요소의 작업 로그에 해당 이벤트를 기록합니다. 방화벽 규칙을 테스트하기 위한 모드입니다. 방화벽 작업 로그를 사용하여 적용 가능성을 평가할 수 있습니다. 그런 다음 필요하다면 방화벽 규칙을 조정하고 방화벽 작동 모드를 **차단**으로 변경할 수 있습니다.

- **차단**. 애플리케이션이 구성 요소 설정에 따라 네트워크 트래픽을 필터링하고 구성 요소의 작업 로그에 해당 이벤트를 기록합니다.

방화벽 규칙 정보

차단 모드를 선택하면 방화벽 구성 요소가 방화벽 규칙을 사용하여 네트워크 트래픽을 필터링합니다.

애플리케이션에 대한 방화벽 규칙은 지정된 애플리케이션의 네트워크 연결을 제어합니다. 이러한 규칙의 작동 기준은 실행 가능한 애플리케이션 파일의 경로를 기준으로 합니다.

방화벽 포트 규칙은 지정된 포트와 프로토콜(TCP / UDP)의 네트워크 연결을 제어합니다. 이러한 규칙의 트리거링 기준은 프로토콜 유형 및 포트 또는 포트 범위입니다.

포트 규칙은 애플리케이션 규칙보다 광범위합니다. 포트 규칙을 기준으로 한 네트워크 연결을 허용하면 보호 중인 컴퓨터의 보안 레벨이 낮아집니다.

방화벽 구성

이 섹션에서는 방화벽 구성 요소의 일반 설정 구성과 방화벽 규칙 생성 및 구성 방법에 관한 지침을 제공합니다.

일반 방화벽 설정 구성

Kaspersky Security Center 관리 콘솔에서 방화벽 구성 요소의 일반 설정 구성

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. **네트워크 활동 제어** 섹션에서 **방화벽** 하위 섹션의 **설정** 버튼을 클릭합니다.
   방화벽 창이 열립니다.

4. **차단 규칙 운영 모드** 블록의 **일반** 탭에서 구성 요소 운영 모드를 선택합니다:

   - **Windows 방화벽 상태 관찰**. 애플리케이션 버전 4.0 이하의 방화벽 관리 작업 로직을 애플리케이션 버전 4.5 버전 이상의 방화벽 기능 전체로 원활하게 전환하기 위한 모드입니다. 애플리케이션 버전 4.0 이하를 업그레이드하면 Windows 방화벽에 통합된 방화벽 관리 작업의 규칙이 유지됩니다. 그러나 방화벽 구성 요소가 더는 Windows 방화벽과 상호작용을 하지 않으며, Windows 방화벽 트래픽 필터링만 모니터링하고 구성 요소의 작업 로그에 해당 이벤트를 기록합니다. 그런 다음 방화벽 규칙을 만들거나, Windows 방화벽 규칙을 가져오거나 방화벽 운영 모드를 **알림**으로 변경할 수 있습니다.

   - **알림**. 애플리케이션은 방화벽 규칙의 작동을 모니터링하기만 하며 구성 요소의 작업 로그에 해당 이벤트를 기록합니다. 방화벽 규칙을 테스트하기 위한 모드입니다. 방화벽 작업 로그를 사용하여 적용 가능성을 평가할 수 있습니다. 그런 다음 필요하다면 방화벽 규칙을 조정하고 방화벽 작동 모드를 **차단**으로 변경할 수 있습니다.

   - **차단**. 애플리케이션이 구성 요소 설정에 따라 네트워크 트래픽을 필터링하고 구성 요소의 작업 로그에 해당 이벤트를 기록합니다.

5. **인바운드 연결** 블록에서 수신 네트워크 연결에 대한 설정을 구성합니다.

   - 수신 연결에 대한 방화벽 규칙에 달리 정의되어 있지 않는 한, **인바운드 연결을 위한 처리** 드롭다운 목록을 사용하여 들어오는 모든 네트워크 연결에 대해 애플리케이션이 수행할 작업을 지정합니다.

   - 필요하다면 수신 연결에 대한 방화벽 규칙을 추가합니다.
     수신 연결에 대한 방화벽 규칙은 예외의 역할을 수행합니다. 예를 들어 수신 네트워크 연결에 대한 허용 규칙을 구성하고 **인바운드 연결을 위한 처리** 드롭다운 목록에서 **차단** 옵션을 선택하하면, 애플리케이션이 규칙 기준과 일치하는 수신 네트워크 연결을 허용합니다.

6. **아웃바운드 연결** 블록에서 발신 네트워크 연결 설정을 구성합니다.

   - 발신 연결에 대한 방화벽 규칙에 달리 정의되어 있지 않는 한, **아웃바운드 연결을 위한 처리** 드롭다운 목록을 사용하여 모든 발신 네트워크 연결에 대해 애플리케이션에서 수행할 작업을 지정합니다.

   - 필요하다면 발신 연결에 대한 방화벽 규칙을 추가합니다.
     발신 연결에 대한 방화벽 규칙은 예외의 역할을 수행합니다. 예를 들어 발신 네트워크 연결에 대한 차단 규칙을 구성하고 **아웃바운드 연결을 위한 처리** 드롭다운 목록에서 **허용** 옵션을 선택하면, 애플리케이션이 규칙 기준과 일치하는 보내는 네트워크 연결을 차단합니다.

7. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes가 새 설정을 적용합니다. 설정이 변경된 날짜와 시간은 시스템 감사 로그에 저장됩니다.

Kaspersky Security Center 웹 콘솔에서 방화벽 구성 요소의 일반 설정 구성

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **네트워크 활동 제어** 섹션에서 **방화벽** 하위 섹션의 **구성** 버튼을 클릭합니다.
   방화벽 창이 열립니다.

5. 토글 스위치를 **방화벽 활성화됨**으로 설정합니다.

6. **차단 규칙 운영 모드** 블록에서, 구성 요소 운영 모드를 선택합니다:

   - **Windows 방화벽 상태 관찰**. 애플리케이션 버전 4.0 이하의 방화벽 관리 작업 로직을 애플리케이션 버전 4.5 버전 이상의 방화벽 기능 전체로 원활하게 전환하기 위한 모드입니다. 애플리케이션 버전 4.0 이하를 업그레이드하면 Windows 방화벽에 통합된 방화벽 관리 작업의 규칙이 유지됩니다. 그러나 방화벽 구성 요소가 더는 Windows 방화벽과 상호작용을 하지 않으며, Windows 방화벽 트래픽 필터링만 모니터링하고 구성 요소의 작업 로그에 해당 이벤트를 기록합니다. 그런 다음 방화벽 규칙을 만들거나, Windows 방화벽 규칙을 가져오거나 방화벽 운영 모드를 **알림**으로 변경할 수 있습니다.

   - **알림**. 애플리케이션은 방화벽 규칙의 작동을 모니터링하기만 하며 구성 요소의 작업 로그에 해당 이벤트를 기록합니다. 방화벽 규칙을 테스트하기 위한 모드입니다. 방화벽 작업 로그를 사용하여 적용 가능성을 평가할 수 있습니다. 그런 다음 필요하다면 방화벽 규칙을 조정하고 방화벽 작동 모드를 **차단**으로 변경할 수 있습니다.

   - **차단**. 애플리케이션이 구성 요소 설정에 따라 네트워크 트래픽을 필터링하고 구성 요소의 작업 로그에 해당 이벤트를 기록합니다.

7. **인바운드 연결** 블록에서 수신 네트워크 연결에 대한 설정을 구성합니다.

   - 수신 연결에 대한 방화벽 규칙에 달리 정의되어 있지 않는 한, **인바운드 연결을 위한 동작** 드롭다운 목록을 사용하여 들어오는 모든 네트워크 연결에 대해 애플리케이션이 수행할 작업을 지정합니다.

   - 필요하다면 수신 연결에 대한 방화벽 규칙을 추가합니다.
     수신 연결에 대한 방화벽 규칙은 예외의 역할을 수행합니다. 예를 들어 수신 네트워크 연결에 대한 허용 규칙을 구성하고 **인바운드 연결을 위한 동작** 드롭다운 목록에서 **차단** 옵션을 선택하하면, 애플리케이션이 규칙 기준과 일치하는 수신 네트워크 연결을 허용합니다.

8. **아웃바운드 연결** 블록에서 발신 네트워크 연결 설정을 구성합니다.

   - 발신 연결에 대한 방화벽 규칙에 달리 정의되어 있지 않는 한, **아웃바운드 연결을 위한 동작** 드롭다운 목록을 사용하여 모든 발신 네트워크 연결에 대해 애플리케이션에서 수행할 작업을 지정합니다.

   - 필요하다면 발신 연결에 대한 방화벽 규칙을 추가합니다.
     발신 연결에 대한 방화벽 규칙은 예외의 역할을 수행합니다. 예를 들어 발신 네트워크 연결에 대한 차단 규칙을 구성하고 **아웃바운드 연결을 위한 동작** 드롭다운 목록에서 **허용** 옵션을 선택하면, 애플리케이션이 규칙 기준과 일치하는 보내는 네트워크 연결을 차단합니다.

9. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes가 새 설정을 적용합니다. 설정이 변경된 날짜와 시간은 시스템 감사 로그에 저장됩니다.

애플리케이션 콘솔에서 방화벽 구성 요소의 일반 설정 구성

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **방화벽** 옵션을 선택합니다.

2. **방화벽** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 방화벽 창이 열립니다.

3. **방화벽** 확인란을 선택합니다.

4. **차단 규칙 운영 모드** 블록에서, 구성 요소 운영 모드를 선택합니다:

   - **Windows 방화벽 상태 관찰**. 애플리케이션 버전 4.0 이하의 방화벽 관리 작업 로직을 애플리케이션 버전 4.5 버전 이상의 방화벽 기능 전체로 원활하게 전환하기 위한 모드입니다. 애플리케이션 버전 4.0 이하를 업그레이드하면 Windows 방화벽에 통합된 방화벽 관리 작업의 규칙이 유지됩니다. 그러나 방화벽 구성 요소가 더는 Windows 방화벽과 상호작용을 하지 않으며, Windows 방화벽 트래픽 필터링만 모니터링하고 구성 요소의 작업 로그에 해당 이벤트를 기록합니다. 그런 다음 방화벽 규칙을 만들거나, Windows 방화벽 규칙을 가져오거나 방화벽 운영 모드를 **알림**으로 변경할 수 있습니다.

   - **알림**. 애플리케이션은 방화벽 규칙의 작동을 모니터링하기만 하며 구성 요소의 작업 로그에 해당 이벤트를 기록합니다. 방화벽 규칙을 테스트하기 위한 모드입니다. 방화벽 작업 로그를 사용하여 적용 가능성을 평가할 수 있습니다. 그런 다음 필요하다면 방화벽 규칙을 조정하고 방화벽 작동 모드를 **차단**으로 변경할 수 있습니다.

   - **차단**. 애플리케이션이 구성 요소 설정에 따라 네트워크 트래픽을 필터링하고 구성 요소의 작업 로그에 해당 이벤트를 기록합니다.

5. **인바운드 연결** 블록에서 수신 네트워크 연결에 대한 설정을 구성합니다.

   - 수신 연결에 대한 방화벽 규칙에 달리 정의되어 있지 않는 한, **인바운드 연결을 위한 처리** 드롭다운 목록을 사용하여 들어오는 모든 네트워크 연결에 대해 애플리케이션이 수행할 작업을 지정합니다.

   - 필요하다면 수신 연결에 대한 방화벽 규칙을 추가합니다.

     수신 연결에 대한 방화벽 규칙은 예외의 역할을 수행합니다. 예를 들어 수신 네트워크 연결에 대한 허용 규칙을 구성하고 **인바운드 연결을 위한 처리** 드롭다운 목록에서 **차단** 옵션을 선택하하면, 애플리케이션이 규칙 기준과 일치하는 수신 네트워크 연결을 허용합니다.

6. **아웃바운드 연결** 블록에서 발신 네트워크 연결 설정을 구성합니다.

   - 발신 연결에 대한 방화벽 규칙에 달리 정의되어 있지 않는 한, **아웃바운드 연결을 위한 처리** 드롭다운 목록을 사용하여 모든 발신 네트워크 연결에 대해 애플리케이션에서 수행할 작업을 지정합니다.

   - 필요하다면 발신 연결에 대한 방화벽 규칙을 추가합니다.

     발신 연결에 대한 방화벽 규칙은 예외의 역할을 수행합니다. 예를 들어 발신 네트워크 연결에 대한 차단 규칙을 구성하고 **아웃바운드 연결을 위한 처리** 드롭다운 목록에서 **허용** 옵션을 선택하면, 애플리케이션이 규칙 기준과 일치하는 보내는 네트워크 연결을 차단합니다.

7. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes가 새 설정을 적용합니다. 설정이 변경된 날짜와 시간은 시스템 감사 로그에 저장됩니다.

방화벽 규칙 생성 및 구성

Kaspersky Security Center 관리 콘솔에서 방화벽 규칙 생성 및 구성

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. **네트워크 활동 제어** 섹션에서 **방화벽** 하위 섹션의 **설정** 버튼을 클릭합니다.

   방화벽 창이 열립니다.

4. **인바운드 연결** 블록에서 **규칙 목록** 버튼을 클릭합니다.
   인바운드 연결 규칙 창이 열립니다.

5. **수신 연결에 대한 방화벽 규칙을 생성하고 구성합니다**.

   1. **애플리케이션** 탭에서 **추가** 버튼을 클릭합니다.
      애플리케이션 규칙 창이 열립니다.

   2. 규칙 설정을 구성합니다:

      a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

      > 규칙 이름은 대소문자에 상관없이 기존의 이름인 All, ICMPv4 및 ICMPv6과 같아서는 안 되며, 인바운드 네트워크 연결에 대한 모든 규칙 목록에서 고유해야 합니다.

      b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

      - **허용**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 수신 네트워크 연결을 허용합니다.
      - **차단**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 수신 네트워크 연결을 차단합니다.

      c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

      d. **포트** 및 **포트** 블록에서 포트나 포트 범위를 지정합니다.

      e. **애플리케이션 경로** 필드에서 직접 또는 **찾아보기** 버튼으로 규칙을 구성할 실행 가능한 애플리케이션 파일 경로를 지정합니다.

      f. **서비스 이름** 필드에서 필요하다면 규칙이 적용될 서비스의 이름을 지정합니다.

      g. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션이 규칙 설정에 따라 지정된 네트워크 주소에서 들어오는 연결을 모니터링합니다.

      > IP 주소에 대해 IPv4 형식만 지원합니다.

      h. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

      i. **확인** 버튼을 클릭해 규칙을 저장합니다.

   3. **포트** 탭에서 **추가** 버튼을 클릭합니다.
      포트 규칙 창이 열립니다.

4. 규칙 설정을 구성합니다:

   a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

   b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

      - **허용**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 수신 네트워크 연결을 허용합니다.
      - **차단**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 수신 네트워크 연결을 차단합니다.

   c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

   d. **포트** 및 **포트** 블록에서 포트나 포트 범위를 지정합니다.

   e. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션이 규칙 설정에 따라 지정된 네트워크 주소에서 들어오는 연결을 모니터링합니다.

      IP 주소에 대해 IPv4 형식만 지원합니다.

   f. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

   g. **확인** 버튼을 클릭해 규칙을 저장합니다.

5. **인바운드 연결 규칙** 창의 **확인** 버튼을 클릭합니다.

6. **아웃바운드 연결** 블록에서 **규칙 목록** 버튼을 클릭합니다.
   아웃바운드 연결 규칙 창이 열립니다.

7. **송신 연결에 대한 방화벽 규칙을 생성하고 구성합니다**.

   1. **애플리케이션** 탭에서 **추가** 버튼을 클릭합니다.
      애플리케이션 규칙 창이 열립니다.

   2. 규칙 설정을 구성합니다:

      a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

         규칙 이름은 대소문자에 상관없이 기존의 이름인 All, ICMPv4 및 ICMPv6과 같아서는 안 되며, 송신 네트워크 연결에 대한 모든 규칙 목록에서 고유해야 합니다.

      b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

         - **허용**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 송신 네트워크 연결을 허용합니다.
         - **차단**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 송신 네트워크 연결을 차단합니다.

      c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

      d. **포트** 및 **포트** 블록에서 포트나 포트 범위를 지정합니다.

e. **애플리케이션 경로** 필드에서 직접 또는 **찾아보기** 버튼으로 규칙을 구성할 실행 가능한 애플리케이션 파일 경로를 지정합니다.

f. **서비스 이름** 필드에서 필요하다면 규칙이 적용될 서비스의 이름을 지정합니다.

g. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션은 규칙 설정에 따라 지정된 네트워크 주소로 송신하는 연결을 모니터링합니다.

> IP 주소에 대해 IPv4 형식만 지원합니다.

h. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

i. **확인** 버튼을 클릭해 규칙을 저장합니다.

3. **포트** 탭에서 **추가** 버튼을 클릭합니다.
   포트 규칙 창이 열립니다.

4. 규칙 설정을 구성합니다:

a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

- **허용**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 송신 네트워크 연결을 허용합니다.
- **차단**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 송신 네트워크 연결을 차단합니다.

c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

d. **포트** 및 **포트** 블록에서 포트나 포트 범위를 지정합니다.

e. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션은 규칙 설정에 따라 지정된 네트워크 주소로 송신하는 연결을 모니터링합니다.

> IP 주소에 대해 IPv4 형식만 지원합니다.

f. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

g. **확인** 버튼을 클릭해 규칙을 저장합니다.

5. **아웃바운드 연결 규칙** 창의 **확인** 버튼을 클릭합니다.

8. XML 파일에서 사용자 지정 규칙을 가져오거나 내보내려면 **규칙 가져오기 및 내보내기** 블록의 **가져오기** 또는 **내보내기** 버튼을 사용합니다.

9. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes가 새 설정을 적용합니다. 설정이 변경된 날짜와 시간은 시스템 감사 로그에 저장됩니다.

Kaspersky Security Center 웹 콘솔에서 방화벽 규칙 생성 및 구성

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **네트워크 활동 제어** 섹션에서 **방화벽** 하위 섹션의 **구성** 버튼을 클릭합니다.
   방화벽 창이 열립니다.
5. 토글 스위치를 **방화벽 활성화됨**으로 설정합니다.
6. **인바운드 연결** 블록에서 **구성** 버튼을 클릭합니다.
   인바운드 연결 규칙 창이 열립니다.
7. **수신 연결에 대한 방화벽 규칙을 생성하고 구성합니다**.
   1. **포트** 탭에서 **추가** 버튼을 클릭합니다.
      포트 규칙 창이 열립니다.
   2. 규칙 설정을 구성합니다:
      a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.
      b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.
      - **허용**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 수신 네트워크 연결을 허용합니다.
      - **거부**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 수신 네트워크 연결을 차단합니다.

      c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.
      d. **로컬 포트** 및 **원격 포트** 블록에서 포트나 포트 범위를 지정합니다.
      e. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션은 규칙 설정에 따라 지정된 네트워크 주소로 수신되는 연결을 모니터링합니다.

      > IP 주소에 대해 IPv4 형식만 지원합니다.

      f. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.
      g. **확인** 버튼을 클릭해 규칙을 저장합니다.
   3. **애플리케이션** 탭에서 **추가** 버튼을 클릭합니다.
      애플리케이션 규칙 창이 열립니다.

4. 규칙 설정을 구성합니다:

   a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

   > 규칙 이름은 대소문자에 상관없이 기존의 이름인 All, ICMPv4 및 ICMPv6과 같아서는 안 되며, 인바운드 네트워크 연결에 대한 모든 규칙 목록에서 고유해야 합니다.

   b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

   - **허용**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 수신 네트워크 연결을 허용합니다.
   - **거부**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 수신 네트워크 연결을 차단합니다.

   c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

   d. **로컬 포트** 및 **원격 포트** 블록에서 포트나 포트 범위를 지정합니다.

   e. **애플리케이션 경로** 필드에서 규칙을 구성할 애플리케이션의 실행 파일 경로를 직접 지정합니다.

   f. **서비스 이름** 필드에서 필요하다면 규칙이 적용될 서비스의 이름을 지정합니다.

   g. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션이 규칙 설정에 따라 지정된 네트워크 주소에서 들어오는 연결을 모니터링합니다.

   > IP 주소에 대해 IPv4 형식만 지원합니다.

   h. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

   i. **확인** 버튼을 클릭해 규칙을 저장합니다.

5. **인바운드 연결 규칙** 창의 **확인** 버튼을 클릭합니다.

8. **아웃바운드 연결** 블록에서 **구성** 버튼을 클릭합니다.
   아웃바운드 연결 규칙 창이 열립니다.

9. **송신 연결에 대한 방화벽 규칙을 생성하고 구성합니다**.

   1. **포트** 탭에서 **추가** 버튼을 클릭합니다.
      포트 규칙 창이 열립니다.

   2. 규칙 설정을 구성합니다:

      a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

      b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

      - **허용**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 송신 네트워크 연결을 허용합니다.
      - **거부**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 송신 네트워크 연결을 차단합니다.

c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

d. **로컬 포트** 및 **원격 포트** 블록에서 포트나 포트 범위를 지정합니다.

e. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션은 규칙 설정에 따라 지정된 네트워크 주소로 송신하는 연결을 모니터링합니다.

> IP 주소에 대해 IPv4 형식만 지원합니다.

f. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

g. **확인** 버튼을 클릭해 규칙을 저장합니다.

3. **애플리케이션** 탭에서 **추가** 버튼을 클릭합니다.
   애플리케이션 규칙 창이 열립니다.

4. 규칙 설정을 구성합니다:

a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

> 규칙 이름은 대소문자에 상관없이 기존의 이름인 All, ICMPv4 및 ICMPv6과 같아서는 안 되며, 송신 네트워크 연결에 대한 모든 규칙 목록에서 고유해야 합니다.

b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

- **허용**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 송신 네트워크 연결을 허용합니다.
- **거부**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 송신 네트워크 연결을 차단합니다.

c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

d. **로컬 포트** 및 **원격 포트** 블록에서 포트나 포트 범위를 지정합니다.

e. **애플리케이션 경로** 필드에서 규칙을 구성할 애플리케이션의 실행 파일 경로를 직접 지정합니다.

f. **서비스 이름** 필드에서 필요하다면 규칙이 적용될 서비스의 이름을 지정합니다.

g. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션은 규칙 설정에 따라 지정된 네트워크 주소로 송신하는 연결을 모니터링합니다.

> IP 주소에 대해 IPv4 형식만 지원합니다.

h. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

i. **확인** 버튼을 클릭해 규칙을 저장합니다.

5. **아웃바운드 연결 규칙** 창의 **확인** 버튼을 클릭합니다.

10. XML 파일에서 사용자 지정 규칙을 가져오거나 내보내려면 **규칙 가져오기 및 내보내기** 블록의 **규칙 가져오기** 또는 **규칙 내보내기** 버튼을 사용합니다.

11. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes가 새 설정을 적용합니다. 설정이 변경된 날짜와 시간은 시스템 감사 로그에 저장됩니다.

애플리케이션 콘솔에서 방화벽 규칙 생성 및 구성

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **방화벽** 옵션을 선택합니다.

2. **방화벽** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 방화벽 창이 열립니다.

3. **인바운드 연결** 블록에서 **규칙 목록** 버튼을 클릭합니다.
   인바운드 연결 규칙 창이 열립니다.

4. **수신 연결에 대한 방화벽 규칙을 생성하고 구성합니다**.

   1. **애플리케이션** 탭에서 **추가** 버튼을 클릭합니다.
      애플리케이션 규칙 창이 열립니다.

   2. 규칙 설정을 구성합니다:

      a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

      > 규칙 이름은 대소문자에 상관없이 기존의 이름인 All, ICMPv4 및 ICMPv6과 같아서는 안 되며, 인바운드 네트워크 연결에 대한 모든 규칙 목록에서 고유해야 합니다.

      b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

      - **허용**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 수신 네트워크 연결을 허용합니다.
      - **차단**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 수신 네트워크 연결을 차단합니다.

      c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

      d. **포트** 및 **포트** 블록에서 포트나 포트 범위를 지정합니다.

      e. **애플리케이션 경로** 필드에서 직접 또는 **찾아보기** 버튼으로 규칙을 구성할 실행 가능한 애플리케이션 파일 경로를 지정합니다.

      f. **서비스 이름** 필드에서 필요하다면 규칙이 적용될 서비스의 이름을 지정합니다.

      g. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션이 규칙 설정에 따라 지정된 네트워크 주소에서 들어오는 연결을 모니터링합니다.

      > IP 주소에 대해 IPv4 형식만 지원합니다.

h. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

i. **확인** 버튼을 클릭해 규칙을 저장합니다.

3. **포트** 탭에서 **추가** 버튼을 클릭합니다.
포트 규칙 창이 열립니다.

4. 규칙 설정을 구성합니다:

a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

- **허용**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 수신 네트워크 연결을 허용합니다.
- **차단**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 수신 네트워크 연결을 차단합니다.

c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

d. **포트** 및 **포트** 블록에서 포트나 포트 범위를 지정합니다.

e. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션이 규칙 설정에 따라 지정된 네트워크 주소에서 들어오는 연결을 모니터링합니다.

> IP 주소에 대해 IPv4 형식만 지원합니다.

f. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

g. **확인** 버튼을 클릭해 규칙을 저장합니다.

5. **인바운드 연결 규칙** 창의 **확인** 버튼을 클릭합니다.

5. **아웃바운드 연결** 블록에서 **규칙 목록** 버튼을 클릭합니다.
아웃바운드 연결 규칙 창이 열립니다.

6. **송신 연결에 대한 방화벽 규칙을 생성하고 구성합니다**.

1. **애플리케이션** 탭에서 **추가** 버튼을 클릭합니다.
애플리케이션 규칙 창이 열립니다.

2. 규칙 설정을 구성합니다:

a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

> 규칙 이름은 대소문자에 상관없이 기존의 이름인 All, ICMPv4 및 ICMPv6과 같아서는 안 되며, 송신 네트워크 연결에 대한 모든 규칙 목록에서 고유해야 합니다.

b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

- **허용**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 송신 네트워크 연결을 허용합니다.
- **차단**. 이 옵션을 선택하면 애플리케이션이 애플리케이션의 송신 네트워크 연결을 차단합니다.

c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

d. **포트** 및 **포트** 블록에서 포트나 포트 범위를 지정합니다.

e. **애플리케이션 경로** 필드에서 직접 또는 **찾아보기** 버튼으로 규칙을 구성할 실행 가능한 애플리케이션 파일 경로를 지정합니다.

f. **서비스 이름** 필드에서 필요하다면 규칙이 적용될 서비스의 이름을 지정합니다.

g. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션은 규칙 설정에 따라 지정된 네트워크 주소로 송신하는 연결을 모니터링합니다.

> IP 주소에 대해 IPv4 형식만 지원합니다.

h. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

i. **확인** 버튼을 클릭해 규칙을 저장합니다.

3. **포트** 탭에서 **추가** 버튼을 클릭합니다.
   포트 규칙 창이 열립니다.

4. 규칙 설정을 구성합니다:

a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

b. **처리** 목록에서 다음 옵션 중 하나를 선택합니다.

- **허용**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 송신 네트워크 연결을 허용합니다.
- **차단**. 이 옵션을 선택하면 애플리케이션이 해당 포트의 송신 네트워크 연결을 차단합니다.

c. **프로토콜** 확인란을 선택하여 애플리케이션이 수신 네트워크 연결을 제어할 프로토콜 유형을 선택합니다.

d. **포트** 및 **포트** 블록에서 포트나 포트 범위를 지정합니다.

e. **규칙 사용 범위** 필드에서 네트워크 주소를 지정합니다. 애플리케이션은 규칙 설정에 따라 지정된 네트워크 주소로 송신하는 연결을 모니터링합니다.

> IP 주소에 대해 IPv4 형식만 지원합니다.

f. **네트워크 어댑터** 블록에서 네트워크 어댑터 목록을 지정합니다.

g. **확인** 버튼을 클릭해 규칙을 저장합니다.

5. **아웃바운드 연결 규칙** 창의 **확인** 버튼을 클릭합니다.

7. XML 파일에서 사용자 지정 규칙을 가져오거나 내보내려면 **규칙 가져오기 및 내보내기** 블록의 **가져오기** 또는 **내보내기** 버튼을 사용합니다.

8. Windows 방화벽 규칙을 가져오려면 **Windows 방화벽 규칙 가져오기** 버튼을 클릭합니다.

Windows 11 24H2 컴퓨터에서는 애플리케이션이 특정 Windows 방화벽 규칙을 건너뛸 수 있습니다. 이 운영 체제 버전의 특별한 기능으로 인해 Kaspersky Industrial CyberSecurity for Nodes가 일부 애플리케이션 패킷 규칙의 파라미터를 인식하지 못할 수 있습니다.

9. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes가 새 설정을 적용합니다. 설정이 변경된 날짜와 시간은 시스템 감사 로그에 저장됩니다.

방화벽 규칙의 활성화와 비활성화

Kaspersky Security Center 관리 콘솔에서 방화벽 규칙 사용 및 중지

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. **네트워크 활동 제어** 섹션에서 **방화벽** 하위 섹션의 **설정** 버튼을 클릭합니다.
   방화벽 창이 열립니다.

4. 창이 열리면 상태를 변경하려는 규칙 유형에 따라 **인바운드 연결** 또는 **아웃바운드 연결** 섹션의 **규칙 목록** 버튼을 클릭합니다.

5. 창이 열리면 **애플리케이션** 또는 **포트** 탭을 선택합니다.
   규칙 목록에서 수정하고자 하는 상태의 규칙을 선택하고 다음 중 한 가지 조치를 수행합니다.

   - 비활성화된 규칙을 활성화하려면 규칙 이름 왼쪽의 체크박스를 선택합니다.
     선택된 규칙이 활성화됩니다.

   - 활성화된 규칙을 비활성화하려면 규칙 이름 왼쪽의 체크박스를 해제합니다.
     선택된 규칙이 비활성화됩니다.

6. 목록에서 규칙을 삭제하려면, 규칙을 선택하고 **삭제** 버튼을 클릭합니다.

7. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 방화벽 규칙 사용 및 중지

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **네트워크 활동 제어** 섹션에서 **방화벽** 하위 섹션의 **구성** 버튼을 클릭합니다.
   방화벽 창이 열립니다.
5. 창이 열리면 상태를 변경하려는 규칙 유형에 따라 **인바운드 연결** 또는 **아웃바운드 연결** 섹션의 **구성** 버튼을 클릭합니다.
6. 창이 열리면 **포트** 또는 **애플리케이션** 탭을 선택합니다.
   규칙 목록에서 수정하고자 하는 상태의 규칙을 선택하고 다음 중 한 가지 조치를 수행합니다.
   - 비활성화된 규칙을 활성화하려면 규칙 이름 왼쪽의 체크박스를 선택합니다.
     선택된 규칙이 활성화됩니다.
   - 활성화된 규칙을 비활성화하려면 규칙 이름 왼쪽의 체크박스를 해제합니다.
     선택된 규칙이 비활성화됩니다.
7. 목록에서 규칙을 삭제하려면, 규칙을 선택하고 **삭제** 버튼을 클릭합니다.
8. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 방화벽 규칙 사용 및 중지

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **컴퓨터 제어** → **방화벽** 옵션을 선택합니다.
2. **방화벽** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 방화벽 창이 열립니다.
3. 창이 열리면 상태를 변경하려는 규칙 유형에 따라 **인바운드 연결** 또는 **아웃바운드 연결** 섹션의 **규칙 목록** 버튼을 클릭합니다.
4. 창이 열리면 **애플리케이션** 또는 **포트** 탭을 선택합니다.
   규칙 목록에서 수정하고자 하는 상태의 규칙을 선택하고 다음 중 한 가지 조치를 수행합니다.
   - 비활성화된 규칙을 활성화하려면 규칙 이름 왼쪽의 체크박스를 선택합니다.
     선택된 규칙이 활성화됩니다.
   - 활성화된 규칙을 비활성화하려면 규칙 이름 왼쪽의 체크박스를 해제합니다.
     선택된 규칙이 비활성화됩니다.
5. 목록에서 규칙을 삭제하려면, 규칙을 선택하고 **삭제** 버튼을 클릭합니다.
6. 변경 사항을 저장합니다.

BadUSB 공격 방지

BadUSB 공격 방지 구성 요소는 기본적으로 설치되지 않습니다. 애플리케이션 설치 중에 구성 요소를 추가하거나 애플리케이션을 설치한 후 애플리케이션 구성 요소 집합을 변경할 수 있습니다.

일부 바이러스는 USB 장치의 펌웨어를 수정해 운영 체제가 USB 장치를 키보드를 인식하도록 속입니다. 결과적으로 바이러스는 사용자 계정에서 명령을 실행하여 악성 코드를 다운로드하는 등의 작업을 할 수 있습니다.

BadUSB 공격 방지 구성 요소는 키보드를 에뮬레이션하는 감염된 USB 장치가 컴퓨터에 연결하지 못하도록 차단합니다.

USB 장치가 컴퓨터에 연결되고 운영 체제가 이를 키보드로 인식하면 애플리케이션은 사용자에게 이 키보드 또는 화상 키보드(가능할 경우)를 이용해 애플리케이션이 생성한 숫자로 이루어진 코드를 입력하도록 요청합니다. 이 절차는 키보드 인증을 의미합니다.

만일 해당 코드를 올바르게 입력했다면, 이 애플리케이션은 인증된 키보드 목록에 식별 파라미터(키보드의 VID/PID와 키보드가 연결된 포트 번호)를 저장합니다. 키보드를 다시 연결하거나 운영 체제를 재시작된 이후에는 키보드 인증을 반복할 필요가 없습니다.

인증된 키보드가 다른 USB 포트에 연결되면, 애플리케이션은 해당 키보드에 대한 인증을 다시 요구합니다.

만일 숫자 코드가 부정확하게 입력되었다면, 애플리케이션은 새 코드를 만듭니다. 숫자 코드 입력 시도 횟수를 구성할 수 있습니다. 숫자 코드를 여러 번 잘못 입력하거나 키보드 인증 창을 닫으면 애플리케이션 해당 키보드의 입력을 차단합니다. USB 장치 차단 시간이 지나거나 운영 체제가 재시작되면, 애플리케이션은 키보드 인증을 사용자에게 다시 요구합니다.

애플리케이션은 인증된 키보드만 사용할 수 있도록 허용하고 인증 안 된 키보드는 차단합니다.

BadUSB 공격 방지 구성 요소가 설치되기 전에 컴퓨터에 연결되고 운영 체제에 의해 키보드로 식별된 USB 장치는 이 구성 요소가 설치된 이후에 인증된 것으로 간주됩니다.

Kaspersky Security Center 관리 콘솔에서 BadUSB 공격 방지 구성 요소를 활성화하고 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로컬 활동 제어** 섹션으로 갑니다.
4. **BadUSB 공격 방지** 블록에서 **설정** 버튼을 클릭합니다.
   BadUSB 공격 방지 창이 열립니다.
5. **BadUSB 공격 방지** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.

6. **USB 장치 인증** 섹션에서 다음 설정을 구성할 수 있습니다.

   - **USB 장치 인증 최대 시도 횟수**. 인증 코드를 지정된 횟수만큼 잘못 입력하면 USB 장치를 자동으로 차단합니다. 유효한 값은 1~10입니다. 예를 들어 인증 코드 입력을 5회 허용하는 경우 애플리케이션은 인증 코드 입력 5회 실패 후 USB 장치를 차단합니다. Kaspersky Industrial CyberSecurity for Nodes는 USB 장치의 차단 시간을 표시합니다. 이 시간이 지나면 인증 코드 입력 가능 횟수가 다시 5회 생깁니다.

   - **최대 시도 횟수 도달 시 타임아웃(분)**. 인증 코드 입력 시도가 지정된 횟수만큼 실패할 시 USB 장치를 차단하는 시간. 유효한 값은 1~180(분)입니다.

7. **연결 시 USB 장치 인증** 섹션에서 다음 설정을 구성할 수 있습니다.

   - **USB 장치 인증 시 화상 키보드 사용 차단**. 이 확인란이 선택되면, 애플리케이션은 인증 코드를 입력할 수 없는 USB 장치의 인증을 위한 화상 키보드의 사용을 차단합니다(바코드 스캐너 등).

   - **USB 장치 인증에 바코드 사용 금지**. 이 확인란을 선택하면 애플리케이션이 바코드 스캐너 인증 알림에 바코드를 표시하지 않습니다.

8. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다 .

9. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 BadUSB 공격 방지 구성 요소를 활성화하고 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로컬 활동 제어** 섹션을 선택합니다.

5. **BadUSB 공격 방지** 블록에서 **구성** 버튼을 클릭합니다.
   BadUSB 공격 방지 창이 열립니다.

6. **BadUSB 공격 방지** 토글로 구성 요소를 사용하거나 중지합니다.

7. 인증 코드를 입력할 수 없는 USB 장치(예: 바코드 스캐너)의 인증을 위한 화상 키보드 사용을 허용하거나 차단하려면 **USB 장치 인증 시 화상 키보드 사용 금지 활성화됨** 토글 스위치를 활성화하거나 비활성화합니다.

8. 바코드 스캐너 권한 부여를 위한 알림에 바코드 표시를 허용하거나 차단하려면 **USB 장치 인증에 바코드 사용 금지 활성화됨** 토글 스위치를 활성화하거나 비활성화합니다.

9. **USB 장치 인증** 섹션에서 다음 설정을 구성할 수 있습니다.

   - **USB 장치 인증 최대 시도 횟수(1~10)**. 인증 코드를 지정된 횟수만큼 잘못 입력하면 USB 장치를 자동으로 차단합니다. 유효한 값은 1~10입니다. 예를 들어 인증 코드 입력을 5회 허용하는 경우 애플리케이션은 인증 코드 입력 5회 실패 후 USB 장치를 차단합니다. Kaspersky Industrial CyberSecurity for Nodes는 USB 장치의 차단 시간을 표시합니다. 이 시간이 지나면 인증 코드 입력 가능 횟수가 다시 5회 생깁니다.

   - **다음 시간 내에 최대 시도 횟수 도달 시 타임아웃(분, 1~180)**. 인증 코드 입력 시도가 지정된 횟수만큼 실패할 시 USB 장치를 차단하는 시간. 유효한 값은 1~180(분)입니다.

10. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다 .

11. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

애플리케이션 콘솔에서 BadUSB 공격 방지 구성 요소를 활성화 및 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **컴퓨터 제어** → **BadUSB 공격 방지** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.
   BadUSB 공격 방지 창이 열립니다.

3. **BadUSB 공격 방지** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.

4. **USB 장치 인증** 섹션에서 다음 설정을 구성할 수 있습니다.

   - **USB 장치 인증 최대 시도 횟수**. 인증 코드를 지정된 횟수만큼 잘못 입력하면 USB 장치를 자동으로 차단합니다. 유효한 값은 1~10입니다. 예를 들어 인증 코드 입력을 5회 허용하는 경우 애플리케이션은 인증 코드 입력 5회 실패 후 USB 장치를 차단합니다. Kaspersky Industrial CyberSecurity for Nodes는 USB 장치의 차단 시간을 표시합니다. 이 시간이 지나면 인증 코드 입력 가능 횟수가 다시 5회 생깁니다.

   - **최대 시도 횟수 도달 시 타임아웃(분)**. 인증 코드 입력 시도가 지정된 횟수만큼 실패할 시 USB 장치를 차단하는 시간. 유효한 값은 1~180(분)입니다.

5. **연결 시 USB 장치 인증** 섹션에서 다음 설정을 구성할 수 있습니다.

   - **USB 장치 인증 시 화상 키보드 사용 차단**. 이 확인란이 선택되면, 애플리케이션은 인증 코드를 입력할 수 없는 USB 장치의 인증을 위한 화상 키보드의 사용을 차단합니다(바코드 스캐너 등).

   - **USB 장치 인증에 바코드 사용 금지**. 이 확인란을 선택하면 애플리케이션이 바코드 스캐너 인증 알림에 바코드를 표시하지 않습니다.

6. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

시스템 무결성 모니터링

Kaspersky Industrial CyberSecurity for Nodes 4.5에 이제 별도의 파일 무결성 모니터와 레지스트리 접근 모니터 구성 요소가 아닌 시스템 무결성 모니터링 구성 요소가 포함됩니다. 시스템 무결성 모니터링 구성 요소에는 파일 무결성 모니터의 모든 기능이 포함되어 있으며 추가로 레지스트리 변경 사항 및 외부 장치의 연결을 모니터링할 수 있습니다.

시스템 무결성 모니터링 구성 요소는 운영 체제에서 컴퓨터 보안 위반을 나타낼 수 있는 변경 사항을 모니터링합니다. 이러한 변경이 탐지되면 Kaspersky Industrial CyberSecurity for Nodes는 해당 이벤트를 생성하고 관리자에게 알립니다. 시스템 무결성 모니터링 구성 요소는 실시간 모드에서 작동할 수 있으며 필요에 따라 시스템 무결성 검사를 수행할 수도 있습니다.

실시간 시스템 무결성 모니터링

실시간 모드에서 시스템 무결성 모니터링 구성 요소는 구성 요소의 범위(모니터링 범위)에 포함된 개체의 변경 사항을 추적합니다. 또한 시스템 무결성 모니터링 구성 요소를 사용하면 해당 개체에 대한 무단 접근을 실시간으로 차단할 수 있습니다.

온디맨드 시스템 무결성 검사

수동 시스템 무결성 검사는 수동으로 또는 스케줄에 따라 실행할 수 있는 작업입니다. *베이스라인 시스템 무결성 모니터* 작업을 실행하려면 구성 요소의 범위(모니터링 범위)를 설정하고 베이스라인을 생성해야 합니다. 베이스라인은 시스템 내 객체의 기록된 상태로 애플리케이션이 현재 상태와 비교할 때 참조합니다. 베이스라인은 처음 작업을 시작할 때 생성됩니다.

파일 무결성 모니터 설정 마이그레이션

Kaspersky Industrial CyberSecurity for Nodes 버전 4.0 이하를 버전 5.0로 업데이트하면 파일 무결성 모니터와 레지스트리 접근 모니터링 설정이 자동으로 마이그레이션됩니다. 마이그레이션 과정에서 애플리케이션이 모니터링 규칙을 시스템 무결성 모니터링 구성 요소로 이동합니다.

시스템 무결성 모니터링 규칙 정보

시스템 무결성 모니터링 기능이 작동하려면 적어도 하나 이상의 규칙을 추가해야 합니다. *시스템 무결성 모니터링 규칙*은 파일이나 레지스트리에 대한 사용자의 접근을 정의하는 기준 세트입니다. 시스템 무결성 모니터링 기능은 지정된 *모니터링 범위* 내에서 파일 또는 레지스트리의 변경 사항을 탐지합니다. 모니터링 범위는 시스템 무결성 모니터링 규칙의 기준 중 하나입니다.

시스템 무결성 모니터링 기능을 통해 다음 개체를 모니터링할 수 있습니다:

- 파일
- 레지스트리
- 외부 장치

파일 모니터링과 관련된 특별 고려 사항

시스템 무결성 모니터링 기능은 파일 및 폴더의 변경 사항뿐만 아니라 모니터링 범위에 추가되거나 제거되는 파일을 모니터링합니다. 이러한 변동은 컴퓨터 보안 위반을 의미할 수 있습니다. 관리자만 액세스할 수 있는 개체나 수정된 개체만 추가하는 것이 좋습니다. 이렇게 하면 시스템 무결성 모니터링 이벤트의 수가 줄어듭니다.

Kaspersky Industrial CyberSecurity for Nodes는 실시간 시스템 무결성 모니터링이 작동하기 시작할 때 연결된 디스크의 파일 및 폴더 변경 사항만 모니터링합니다. 실시간 시스템 무결성 모니터가 작동하기 시작할 때 디스크가 연결되어 있지 않은 경우 파일 및 폴더가 모니터링 범위에 추가되더라도 애플리케이션은 해당 디스크의 파일 및 폴더의 변경 사항을 모니터링하지 않습니다.

애플리케이션은 파일 생성, 파일 크기 증가, 파일 데이터 다시 쓰기, 파일 자르기 작업 중 하나가 기록될 때 개체 생성 이벤트를 생성합니다. 따라서 애플리케이션 실행 제어 차단 규칙 동작 중에 파일의 개체 생성 이벤트가 생성되는 경우, 이는 파일 크기 증가, 데이터 다시 쓰기, 자르기 같은 동작을 포함한 금지된 파일 생성 또는 금지된 파일 수정으로 인해 발생할 수 있습니다.

레지스트리 모니터링과 관련된 특별 고려 사항

시스템 무결성 모니터링 기능은 레지스트리를 모니터링합니다. 이러한 변동은 컴퓨터 보안 위반을 의미할 수 있습니다.

시스템 무결성 모니터는 레지스트리의 다음 루트 키를 모니터링합니다:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`

- HKEY_USERS
- HKEY_CURRENT_CONFIG

시스템 무결성 모니터는 HKEY_CURRENT_USER 키를 지원하지 않습니다. HKEY_USERS 항목에서 HKEY_USERS\<user profile ID>\<key>로 키를 지정할 수 있습니다.

외부 장치 모니터링과 관련된 특별 고려 사항

시스템 무결성 모니터링은 외부 장치의 연결 및 연결 해제를 모니터링합니다. 이는 이러한 장치와의 파일 교환으로 인해 발생할 수 있는 보안 위협으로부터 컴퓨터를 보호하기 위해 필요합니다. 시스템 무결성 모니터는 외부 장치에 대한 접근을 모니터링하지 않으며 파일 교환을 차단하지 않습니다. 다른 애플리케이션 구성 요소인 장치 제어 구성 요소를 사용하여 장치에 대한 접근을 설정할 수 있습니다.

베이스라인 시스템 무결성 모니터 작업을 실행할 때, 운영 체제에서 같은 드라이브 문자를 사용하는 외부 장치가 다시 연결되더라도 애플리케이션은 이를 무시합니다. 로그에 기록하려면, 다시 연결된 장치의 드라이브 문자가 달라야 합니다.

시스템 무결성 모니터링 기능은 다음 유형의 외부 장치의 연결을 모니터링합니다.

- 이동식 드라이브(USB 플래시 드라이브 포함)
- 하드 드라이브
- 외부 네트워크 어댑터
- CD/DVD/Blu-ray 드라이브
- 스캐너/카메라

실시간 시스템 무결성 모니터링

시스템 무결성 모니터링을 사용하면 운영 체제의 변경 사항을 실시간으로 추적할 수 있습니다. 컴퓨터에서 보안 위반을 나타낼 수 있는 변경 사항을 추적할 수 있습니다. 이 구성 요소를 사용하면 이러한 변경을 차단하거나 단순히 변경 이벤트를 로그 기록할 수 있습니다.

시스템 무결성 모니터링이 작동하려면 적어도 하나 이상의 규칙을 추가해야 합니다. 시스템 무결성 모니터링 규칙은 파일 및 레지스트리에 대한 사용자의 접근을 정의하는 기준 세트입니다. 시스템 무결성 모니터링은 지정된 모니터링 범위 내에서 파일 및 레지스트리의 변경 사항을 탐지합니다. 모니터링 범위는 시스템 무결성 모니터링 규칙의 기준 중 하나입니다.

Kaspersky Security Center 관리 콘솔에서 실시간 시스템 무결성 모니터링을 활성화하고 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **시스템 점검** 옵션을 선택합니다.

4. **시스템 무결성 모니터링** 섹션에서 **설정** 버튼을 클릭합니다.

5. **시스템 무결성 모니터링** 확인란을 선택합니다.

6. 파일 무결성 모니터 구성:

   a. **파일** 탭에서 **파일 모니터** 확인란을 선택합니다.

   b. **차단 규칙 운영 모드**에서 파일 무결성 모니터 모드를 선택합니다:

   - **차단**. 이 모드에서는 애플리케이션이 파일 무결성 모니터 규칙에 따라 파일에 작업을 수행하고 시스템 무결성 모니터링 로그에 해당 이벤트를 생성합니다.

   - **알림**. 이 모드에서는 애플리케이션이 시스템 무결성 모니터링 로그에서 트리거된 파일 무결성 모니터 규칙에 대한 이벤트만 생성합니다.

   c. **추가** 버튼을 사용하거나 XML 파일에서 가져와서 파일 무결성 모니터 규칙을 직접 추가합니다. 다음 표에는 파일 무결성 모니터 규칙 설정에 대한 설명이 나와 있습니다.

   d. 파일 무결성 모니터 규칙 목록에서 확인란을 관리하여 필요한 규칙을 활성화된 상태로 둡니다.

7. 레지스트리 접근 모니터 구성:

   a. **레지스트리** 탭에서 **레지스트리 모니터** 확인란을 선택합니다.

   b. **차단 규칙 운영 모드**에서 레지스트리 접근 모니터 모드를 선택합니다:

   - **차단**. 이 모드에서 애플리케이션은 레지스트리 접근 모니터 규칙에 따라 레지스트리를 사용한 작업을 차단하고 시스템 무결성 모니터링 로그에 해당 이벤트를 생성합니다.

   - **알림**. 이 모드에서 애플리케이션은 시스템 무결성 모니터링 로그에 트리거된 레지스트리 접근 모니터 규칙에 대한 이벤트만 생성합니다.

   c. **추가** 버튼을 사용하거나 XML 파일에서 가져와서 레지스트리 접근 모니터 규칙을 직접 추가합니다. 다음 표에는 레지스트리 접근 규칙 설정에 대한 설명이 나와 있습니다.

   d. 레지스트리 접근 모니터 규칙 목록에서 확인란을 관리하여 필요한 규칙을 활성화된 상태로 둡니다.

8. 외부 장치 모니터링 구성:

   a. **장치** 탭에서 **장치 모니터** 확인란을 선택합니다.

   b. **이벤트 심각도** 드롭다운 목록에서 외부 장치 모니터링 이벤트의 중요도(*정보*, *경고*, *심각*)를 선택합니다.

   외부 장치 모니터링 설정을 적용하면 애플리케이션이 현재 외부 장치 연결을 기억합니다. 이후, 외부 장치가 연결되거나 연결 해제되면 애플리케이션이 해당 이벤트를 생성합니다.

9. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 실시간 시스템 무결성 모니터링을 활성화하고 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **시스템 점검** → **시스템 무결성 모니터링** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. **시스템 무결성 모니터링** 확인란을 선택합니다.
6. 파일 무결성 모니터 구성:
   a. **파일** 탭에서 **파일 모니터** 확인란을 선택합니다.
   b. **차단 규칙 운영 모드**에서 파일 무결성 모니터 모드를 선택합니다:
      - **차단**. 이 모드에서는 애플리케이션이 파일 무결성 모니터 규칙에 따라 파일에 작업을 수행하고 시스템 무결성 모니터링 로그에 해당 이벤트를 생성합니다.
      - **알림**. 이 모드에서는 애플리케이션이 시스템 무결성 모니터링 로그에서 트리거된 파일 무결성 모니터 규칙에 대한 이벤트만 생성합니다.
   c. **추가** 버튼을 사용하거나 XML 파일에서 가져와서 파일 무결성 모니터 규칙을 직접 추가합니다. 다음 표에는 파일 무결성 모니터 규칙 설정에 대한 설명이 나와 있습니다.
   d. 파일 무결성 모니터 규칙 목록에서 **상태** 열의 확인란을 관리하여 필요한 규칙을 활성화된 상태로 둡니다.
7. 레지스트리 접근 모니터 구성:
   a. **레지스트리** 탭에서 **레지스트리 모니터** 확인란을 선택합니다.
   b. **차단 규칙 운영 모드**에서 레지스트리 접근 모니터 모드를 선택합니다:
      - **차단**. 이 모드에서 애플리케이션은 레지스트리 접근 모니터 규칙에 따라 레지스트리를 사용한 작업을 차단하고 시스템 무결성 모니터링 로그에 해당 이벤트를 생성합니다.
      - **알림**. 이 모드에서 애플리케이션은 시스템 무결성 모니터링 로그에 트리거된 레지스트리 접근 모니터 규칙에 대한 이벤트만 생성합니다.
   c. **추가** 버튼을 사용하거나 XML 파일에서 가져와서 레지스트리 접근 모니터 규칙을 직접 추가합니다. 다음 표에는 레지스트리 접근 규칙 설정에 대한 설명이 나와 있습니다.
   d. 레지스트리 접근 모니터 규칙 목록에서 **상태** 열의 확인란을 관리하여 필요한 규칙을 활성화된 상태로 둡니다.

8. 외부 장치 모니터링 구성:

   a. **장치** 탭에서 **장치 모니터** 확인란을 선택합니다.

   b. **이벤트 심각도** 드롭다운 목록에서 외부 장치 모니터링 이벤트의 중요도(*정보*, *경고*, *심각*)를 선택합니다.

   시스템 무결성 모니터링은 외부 장치의 현재 연결 상태를 기록합니다. 애플리케이션 설정에서 구성 요소를 활성화하면 애플리케이션이 외부 장치의 연결 및 연결 해제를 모니터링하기 시작합니다. 이후, 외부 장치가 연결 또는 연결 해제되면 애플리케이션은 해당 이벤트를 생성합니다.

9. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 실시간 시스템 무결성 모니터링을 활성화하고 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **시스템 점검** → **시스템 무결성 모니터링** 옵션을 선택합니다.

2. **시스템 무결성 모니터링** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.

   속성: 시스템 무결성 모니터링 창이 열립니다.

3. **시스템 무결성 모니터링** 확인란을 선택합니다.

4. 파일 무결성 모니터 구성:

   a. **파일** 탭에서 **파일 모니터** 확인란을 선택합니다.

   b. **차단 규칙 운영 모드**에서 파일 무결성 모니터 모드를 선택합니다:

   - **차단**. 이 모드에서는 애플리케이션이 파일 무결성 모니터 규칙에 따라 파일에 작업을 수행하고 시스템 무결성 모니터링 로그에 해당 이벤트를 생성합니다.

   - **알림**. 이 모드에서는 애플리케이션이 시스템 무결성 모니터링 로그에서 트리거된 파일 무결성 모니터 규칙에 대한 이벤트만 생성합니다.

   c. **추가** 버튼을 사용하거나 XML 파일에서 가져와서 파일 무결성 모니터 규칙을 직접 추가합니다. 다음 표에는 파일 무결성 모니터 규칙 설정에 대한 설명이 나와 있습니다.

   d. 파일 무결성 모니터 규칙 목록에서 확인란을 관리하여 필요한 규칙을 활성화된 상태로 둡니다.

5. 레지스트리 접근 모니터 구성:

   a. **레지스트리** 탭에서 **레지스트리 모니터** 확인란을 선택합니다.

   b. **차단 규칙 운영 모드**에서 레지스트리 접근 모니터 모드를 선택합니다:

   - **차단**. 이 모드에서 애플리케이션은 레지스트리 접근 모니터 규칙에 따라 레지스트리를 사용한 작업을 차단하고 시스템 무결성 모니터링 로그에 해당 이벤트를 생성합니다.

   - **알림**. 이 모드에서 애플리케이션은 시스템 무결성 모니터링 로그에 트리거된 레지스트리 접근 모니터 규칙에 대한 이벤트만 생성합니다.

   c. **추가** 버튼을 사용하거나 XML 파일에서 가져와서 레지스트리 접근 모니터 규칙을 직접 추가합니다. 다음 표에는 레지스트리 접근 규칙 설정에 대한 설명이 나와 있습니다.

   d. 레지스트리 접근 모니터 규칙 목록에서 확인란을 관리하여 필요한 규칙을 활성화된 상태로 둡니다.

6. 외부 장치 모니터링 구성:

   a. **장치** 탭에서 **장치 모니터** 확인란을 선택합니다.

   b. **이벤트 심각도** 드롭다운 목록에서 외부 장치 모니터링 이벤트의 중요도(*정보*, *경고*, *심각*)를 선택합니다.

   외부 장치 모니터링 설정을 적용하면 애플리케이션이 현재 외부 장치 연결을 기억합니다. 이후, 외부 장치가 연결되거나 연결 해제되면 애플리케이션이 해당 이벤트를 생성합니다.

7. 변경 사항을 저장합니다.

시스템 무결성 모니터링 규칙 설정

파라미터	설명
파일 동작에서 범위 모니터링	파일 무결성 모니터링을 적용할 범위입니다. 이 필드는 필수입니다. 마스크 사용: Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다. `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다. `?`(물음표) 문자는 \ 및 / 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.
모니터링한 개체	여기에서 레지스트리 키의 이름이나 값을 지정할 수 있습니다. 마스크 사용: Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다:
파일 작업	• **탐지**. 애플리케이션이 모니터링 범위의 파일에 대한 처리를 허용합니다. • **탐지 및 차단**. 선택한 파일 무결성 모니터 모드에 따라 애플리케이션의 행동도 다릅니다. *차단* 모드를 선택한 경우 시스템 무결성 모니터링은 모니터링 범위에 있는 파일에 대한 동작을 차단합니다. *알림* 모드를 선택한 경우 시스템 무결성 모니터링은 모니터링 범위에 있는 파일에 대한 동작을 허용합니다.
신뢰하는 사용자 및/또는 사용자 그룹	신뢰하는 사용자는 모니터링 범위에서 파일 및 레지스트리 키로 동작을 수행할 수 있는 사용자입니다. Kaspersky Industrial CyberSecurity for Nodes가 신뢰하는 사용자가 수행한 동작을 탐지하면 시스템 무결성 모니터링이 정보 이벤트를 생성합니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다.
파일 동작 표식 / 동작	애플리케이션이 모니터링할 파일 또는 레지스트리 키로 작업을 특성화하는 마커입니다.
인식한 모든 마커를 기준으로 파일 동작 탐지 / 인식한 모든 마커를 기준으로 레지스트리 작업 탐지	기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 모든 파일/레지스트리 작업 마커를 탐지합니다.
다음 마커를 기준으로 파일 동작 탐지 / 다음 마커를 기준으로 레지스트리 작업 탐지	사용 가능한 파일/레지스트리 작업 목록에서 모니터링할 작업 옆의 확인란을 선택합니다.
가능한 경우 파일 동작 후 체크섬을 계산합니다. 체크섬은 작업 로그에 표시됩니다	이 확인란이 선택된 경우, 적어도 하나의 선택된 마커와 파일 동작이 탐지되면 Kaspersky Industrial CyberSecurity for Nodes는 수정된 파일의 체크섬을 계산합니다. 여러 마커에서 파일 동작을 탐지하면 모든 수정이 완료된 최종 파일의 체크섬만 계산됩니다. 이 확인란이 선택 해제된 경우, Kaspersky Industrial CyberSecurity for Nodes는 수정된 파일의 체크섬을 계산하지 않습니다. 다음과 같은 경우에는 체크섬 계산이 수행되지 않습니다: • 파일을 사용할 수 없게 된 경우(예: 접근 권한 변경). • 이후에 제거된 파일에서 파일 동작이 탐지된 경우. 기본적으로 확인란의 선택이 취소됩니다.
체크섬 계산 알고리즘	드롭다운 목록에서 체크섬 계산 알고리즘 중 하나를 선택합니다: • MD5 해시 • SHA256 해시

파라미터	설명
예외 규칙	**예외 규칙** 탭에서 모니터링 범위에서 제외할 개체를 추가할 수 있습니다: • 파일 무결성 모니터 규칙에 대해 폴더 목록을 지정할 수 있습니다. • 레지스트리 접근 모니터링 규칙에 대해 레지스트리 키 또는 값을 지정할 수 있습니다. 마스크 사용: **파일** 구성 요소가 모니터링하는 파일 및 폴더 목록입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다. `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다. `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다. **레지스트리** Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 `*` 및 `?`를 지원하며, 예외 항목은 모니터링 범위 항목보다 우선순위가 높습니다.
이벤트 심각도	Kaspersky Industrial CyberSecurity for Nodes는 모니터링 범위 내 파일 또는 레지스트리 키가 수정될 때마다 파일 수정 이벤트를 기록합니다. 사용할 수 있는 이벤트 심각도는 **정보**, **경고**, **심각**입니다.

온디맨드 시스템 무결성 검사

온디맨드 시스템 무결성 검사는 수동으로 또는 스케줄에 따라 실행할 수 있는 작업입니다. *베이스라인 시스템 무결성 모니터* 작업을 실행할 때 애플리케이션은 모니터링 범위에 포함된 개체의 현재 상태를 *베이스라인* 상태와 비교합니다. 베이스라인은 처음 작업을 시작할 때 생성됩니다.

시스템 무결성 모니터가 작동하려면 적어도 하나 이상의 규칙을 추가해야 합니다. 시스템 무결성 모니터링 규칙은 파일 및 레지스트리에 대한 사용자의 접근을 정의하는 기준 세트입니다. 시스템 무결성 모니터링은 지정된 모니터링 범위 내에서 파일 및 레지스트리의 변경 사항을 탐지합니다. 모니터링 범위는 시스템 무결성 모니터링 규칙의 기준 중 하나입니다.

베이스라인 시스템 무결성 모니터 작업에 대한 모니터링 범위 구성

베이스라인 시스템 무결성 모니터 작업의 모니터링 범위는 기본값으로 실시간 시스템 무결성 모니터링의 모니터링 범위와 같습니다. 작업에 대해 다른 모니터링 범위를 구성할 수 있습니다.

시스템 무결성 모니터링은 `HKEY_CURRENT_USER` 및 `HKEY_CURRENT_CONFIG` 키 가져오기를 *시스템 무결성 검사* 작업에서 지원하지 않습니다. 작업 모니터링 범위에 이러한 키가 포함되어 있으면, 애플리케이션이 *잘못된 개체를 포함한 모니터링 범위* 이벤트를 생성합니다.

Kaspersky Security Center 관리 콘솔에서 베이스라인 시스템 무결성 모니터 작업에 대해 다른 모니터링 범위를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **작업**을 선택합니다.
2. 필요한 *베이스라인 시스템 무결성 모니터* 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.

3. 창이 열리면 **설정** 옵션을 선택합니다.

4. 파일 모니터링 구성:

   a. **파일** 탭에서 **파일 모니터** 확인란을 선택합니다.

   b. 목록에서 확인란을 선택하여 규칙을 선택합니다.

   c. 필요하다면 **추가** 버튼을 클릭해 새로운 규칙을 추가합니다. 다음 표에는 베이스라인 시스템 무결성 모니터 규칙 설정에 관한 설명이 나와 있습니다.

   d. 다른 소스에서 규칙을 가져올 수도 있습니다.

5. 레지스트리 모니터링을 구성합니다:

   a. **레지스트리** 탭에서 **레지스트리 모니터** 확인란을 선택합니다.

   b. 목록에서 확인란을 선택하여 규칙을 선택합니다.

   c. 필요하다면 **추가** 버튼을 클릭해 새로운 규칙을 추가합니다. 다음 표에는 베이스라인 시스템 무결성 모니터 규칙 설정에 관한 설명이 나와 있습니다.

   d. 다른 소스에서 규칙을 가져올 수도 있습니다.

6. 외부 장치 모니터링 구성:

   a. **장치** 탭에서 **장치 모니터** 확인란을 선택합니다.

   b. **이벤트 심각도** 드롭다운 목록에서 외부 장치 모니터링 이벤트의 중요도(*정보*, *경고*, *심각*)를 선택합니다.

   베이스라인 시스템 무결성 모니터 작업은 베이스라인이 생성된 시점에 연결된 외부 장치에 대한 정보를 기록합니다. 이후, 외부 장치가 연결되면, 애플리케이션이 해당 이벤트를 생성합니다. 작업을 실행할 때 애플리케이션은 외부 장치의 연결 해제를 모니터링하지 않습니다.

7. 변경 사항을 저장합니다.

웹 콘솔에서 베이스라인 시스템 무결성 모니터 작업에 대해 다른 모니터링 범위를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.

2. 필요한 *베이스라인 시스템 무결성 모니터* 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.

3. 창이 열리면 **애플리케이션 설정** 옵션을 선택합니다.

4. 파일 모니터링 구성:

   a. **파일 모니터** 확인란을 선택합니다.

   b. 목록에서 확인란을 선택하여 규칙을 선택합니다.

   c. 필요하다면 **추가** 버튼을 클릭해 새로운 규칙을 추가합니다. 다음 표에는 베이스라인 시스템 무결성 모니터 규칙 설정에 관한 설명이 나와 있습니다.

   d. 다른 소스에서 규칙을 가져올 수도 있습니다.

5. 레지스트리 모니터링을 구성합니다:

   a. **레지스트리 모니터** 확인란을 선택합니다.

   b. 목록에서 확인란을 선택하여 규칙을 선택합니다.

   c. 필요하다면 **추가** 버튼을 클릭해 새로운 규칙을 추가합니다. 다음 표에는 베이스라인 시스템 무결성 모니터 규칙 설정에 관한 설명이 나와 있습니다.

   d. 다른 소스에서 규칙을 가져올 수도 있습니다.

6. 외부 장치 모니터링 구성:

   a. **장치 모니터** 확인란을 선택합니다.

   b. **이벤트 심각도** 드롭다운 목록에서 외부 장치 모니터링 이벤트의 중요도(*정보*, *경고*, *심각*)를 선택합니다.

   베이스라인 시스템 무결성 모니터 작업은 베이스라인이 생성된 시점에 연결된 외부 장치에 대한 정보를 기록합니다. 이후, 외부 장치가 연결되면, 애플리케이션이 해당 이벤트를 생성합니다. 작업을 실행할 때 애플리케이션은 외부 장치의 연결 해제를 모니터링하지 않습니다.

7. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 베이스라인 시스템 무결성 모니터 작업에 대해 다른 모니터링 범위를 구성하는 방법

작업이 로컬로 생성되거나 정책 속성의 **애플리케이션 설정 → 로컬 시스템 작업 실행** 섹션에서 **로컬 작업 사용 허용** 확인란이 선택되어 있는 경우 **베이스라인 시스템 무결성 모니터** 작업의 속성을 Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 편집할 수 있습니다.

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **시스템 점검 → 베이스라인 시스템 무결성 모니터** 옵션을 선택합니다.

2. **베이스라인 시스템 무결성 모니터** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.

   속성: 베이스라인 시스템 무결성 모니터 창이 열립니다.

3. 파일 모니터링 구성:

   a. **파일** 탭에서 **파일 모니터** 확인란을 선택합니다.

   b. 목록에서 확인란을 선택하여 규칙을 선택합니다.

   c. 필요하다면 **추가** 버튼을 클릭해 새로운 규칙을 추가합니다. 다음 표에는 베이스라인 시스템 무결성 모니터 규칙 설정에 관한 설명이 나와 있습니다.

   d. 다른 소스에서 규칙을 가져올 수도 있습니다.

4. 레지스트리 모니터링을 구성합니다:

   a. **레지스트리** 탭에서 **레지스트리 모니터** 확인란을 선택합니다.

   b. 목록에서 확인란을 선택하여 규칙을 선택합니다.

   c. 필요하다면 **추가** 버튼을 클릭해 새로운 규칙을 추가합니다. 다음 표에는 베이스라인 시스템 무결성 모니터 규칙 설정에 관한 설명이 나와 있습니다.

   d. 다른 소스에서 규칙을 가져올 수도 있습니다.

5. 외부 장치 모니터링 구성:

   a. **장치** 탭에서 **장치 모니터** 확인란을 선택합니다.

   b. **이벤트 심각도** 드롭다운 목록에서 외부 장치 모니터링 이벤트의 중요도(*정보*, *경고*, *심각*)를 선택합니다.

   베이스라인 시스템 무결성 모니터 작업은 베이스라인이 생성된 시점에 연결된 외부 장치에 대한 정보를 기록합니다. 이후, 외부 장치가 연결되면, 애플리케이션이 해당 이벤트를 생성합니다. 작업을 실행할 때 애플리케이션은 외부 장치의 연결 해제를 모니터링하지 않습니다.

6. 변경 사항을 저장합니다.

베이스라인 시스템 무결성 모니터 작업 규칙 설정

파라미터	설명
파일 동작에서 범위 모니터링	파일 무결성 모니터링을 적용할 범위입니다. 이 필드는 필수입니다. 마스크 사용: Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다. `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다. `?`(물음표) 문자는 \ 및 / 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다.
모니터링한 개체	여기에서 레지스트리 키의 이름이나 값을 지정할 수 있습니다. 마스크 사용: Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다:
예외 규칙	**예외 규칙** 탭에서 모니터링 범위에서 제외할 개체를 추가할 수 있습니다: • 파일 무결성 모니터 규칙에 대해 폴더 목록을 지정할 수 있습니다. • 레지스트리 접근 모니터링 규칙에 대해 레지스트리 키 또는 값을 지정할 수 있습니다. 마스크 사용: **파일** 구성 요소가 모니터링하는 파일 및 폴더 목록입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: `*`(별표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 문자의 조합을 나타낼 수 있습니다. 예를 들어 `C:\*\*.txt` 마스크에는 C: 드라이브의 폴더(하위 폴더 제외)에 있는 TXT 확장자를 가진 파일에 대한 모든 경로가 포함됩니다. `*` 문자를 두 번 연속 사용하면 파일 또는 폴더 이름에서 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 포함하여 모든 문자(공백 포함)의 조합을 나타낼 수 있습니다. 예를 들어, `C:\Folder\**\*.txt` 마스크는 `Folder`라는 이름의 폴더를 제외하고 `Folder` 내에 포함된 폴더에 있는 TXT 확장자 파일에 대한 모든 경로를 포함합니다. 마스크에는 적어도 하나의 하위 레벨이 포함되어야 합니다. `C:\**\*.txt` 마스크는 하위 레벨의 폴더가 없어 유효한 마스크가 아닙니다. `?`(물음표) 문자는 `\` 및 `/` 문자(파일 및 폴더에 대한 경로에서 파일 및 폴더 이름의 구분 기호)를 제외한 모든 단일 문자를 나타낼 수 있습니다. 예를 들어 `C:\Folder\???.txt` 마스크는 TXT 확장자를 가지고 있으며 세 개 문자를 가진 `Folder` 폴더 내의 모든 파일에 대한 경로를 포함하게 됩니다. **레지스트리** Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 `*` 및 `?`를 지원하며, 예외 항목은 모니터링 범위 항목보다 우선순위가 높습니다.
이벤트 심각도	Kaspersky Industrial CyberSecurity for Nodes는 모니터링 범위 내 파일 또는 레지스트리 키가 수정될 때마다 파일 수정 이벤트를 기록합니다. 사용할 수 있는 이벤트 심각도는 **정보**, **경고**, **심각**입니다.

베이스라인 시스템 무결성 모니터 작업 실행

베이스라인 시스템 무결성 모니터 작업을 통해 파일 또는 레지스트리 키 변경 사항과 외부 장치 연결 상태를 확인할 수 있습니다. 파일의 변경 사항을 확인하려면 다음 모드에서 **베이스라인 시스템 무결성 모니터** 작업을 실행합니다:

- **전체 검사**. 이 모드에서는 애플리케이션이 파일의 모든 속성과 해시를 확인합니다.
- **빠른 검사**. 이 모드에서는 애플리케이션이 파일의 속성만 확인합니다.

작업이 실행되는 모드는 레지스트리나 외부 장치의 검사에 영향을 미치지 않습니다.

Kaspersky Security Center 관리 콘솔에서 베이스라인 시스템 무결성 모니터 작업을 실행하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **새 작업** 버튼을 클릭합니다.
   작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
3. Kaspersky Industrial CyberSecurity for Nodes → **베이스라인 시스템 무결성 모니터** 옵션을 선택합니다. 시스템 무결성 모니터링 모드를 선택합니다:
   - **전체 검사**. 이 모드에서는 애플리케이션이 파일의 모든 속성과 해시를 확인합니다.
   - **빠른 검사**. 이 모드에서는 애플리케이션이 파일의 속성만 확인합니다.
4. 작업을 수행할 컴퓨터를 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.
   - 네트워크에서 중앙 관리 서버가 탐지한 컴퓨터 선택: 미할당 기기. 이 특정 장치에는 관리 그룹에 속하는 장치와 미할당 장치가 포함될 수 있습니다.
   - 장치 주소를 직접 지정하거나 주소 목록에서 가져옵니다. 작업을 할당할 장치의 NetBIOS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.
   - 작업을 실행할 장치를 지정합니다.
   - 관리 그룹에 작업 할당. 이 경우 이전에 만든 관리 그룹에 포함된 컴퓨터에 작업이 할당됩니다.
5. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 로컬 사용자 계정의 권한으로 작업을 시작합니다.
6. 예를 들어 직접 또는 특정 요일에 작업 스케줄을 구성합니다.
7. 작업 이름을 입력합니다.
8. 마법사를 완료합니다. 필요하다면 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔에서 베이스라인 시스템 무결성 모니터 작업을 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
   작업 목록이 열립니다.

2. **추가** 버튼을 클릭합니다.
   작업 마법사가 시작됩니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 Kaspersky Industrial CyberSecurity for Nodes를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **베이스라인 시스템 무결성 모니터** 옵션을 선택합니다.

   c. **작업 이름** 필드에 *주별 시스템 무결성 검사* 등의 간단한 설명을 입력합니다.

4. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.

5. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.

6. 체크섬 계산 알고리즘을 선택합니다.

7. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 로컬 사용자 계정의 권한으로 작업을 시작합니다.

8. 마법사를 완료합니다.
   작업 목록에 새 작업이 표시됩니다.

9. 새 작업을 클릭합니다.
   작업 속성 창이 열립니다.

10. **애플리케이션 설정** 탭을 선택합니다.

11. 시스템 무결성 검사 모드 선택:

    - **전체 검사**. 이 모드에서는 애플리케이션이 파일의 모든 속성과 해시를 확인합니다.
    - **빠른 검사**. 이 모드에서는 애플리케이션이 파일의 속성만 확인합니다.

12. 변경 사항을 저장합니다.

13. 작업 옆의 확인란을 선택합니다.

14. **시작** 버튼을 클릭합니다.

시스템 무결성 모니터링 규칙 내보내기 및 가져오기

시스템 무결성 모니터링 규칙 목록을 XML 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 동일 유형의 기록을 여러 개 추가하는 등의 작업을 진행할 수 있습니다. 내보내기/가져오기 기능을 사용하여 시스템 무결성 모니터링 규칙 목록을 백업하거나 다른 서버로 마이그레이션할 수 있습니다.

시스템 무결성 모니터링은 `HKEY_CURRENT_USER` 및 `HKEY_CURRENT_CONFIG` 키 가져오기를 *시스템 무결성 검사* 작업에서 지원하지 않습니다. 작업 모니터링 범위에 이러한 키가 포함되어 있으면, 애플리케이션이 *잘못된 개체를 포함한 모니터링 범위* 이벤트를 생성합니다.

Kaspersky Security Center 관리 콘솔에서 시스템 무결성 모니터링 규칙 목록을 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **시스템 점검** 옵션을 선택합니다.
4. **시스템 무결성 모니터링** 섹션에서 **설정** 버튼을 클릭합니다.
5. 내보내거나 가져올 규칙에 따라 **파일** 또는 **레지스트리** 탭으로 이동합니다.
6. 파일 규칙 및 레지스트리 규칙 목록을 내보내려면:
   a. 전체 목록을 내보내려면 버튼을 누르고 **내보내기**을 선택합니다.
   b. 목록의 일부만 내보내려면 다음 단계를 수행합니다.
      1. **Ctrl** 또는 **Shift** 키를 사용하여 내보낼 목록 항목을 선택합니다. 모든 항목을 선택하려면 **Ctrl+A**를 누릅니다.
      2. 버튼을 클릭하고 **선택 항목 내보내기**을 선택합니다.
   c. 창이 열리면 내보낼 XML 파일의 이름을 지정하고 파일을 저장할 폴더를 선택합니다. **저장** 버튼을 누릅니다.
   Kaspersky Industrial CyberSecurity for Nodes는 규칙 목록을 XML 파일로 내보냅니다.
7. 파일/레지스트리 규칙을 가져오려면:
   a. **가져오기** 버튼을 클릭합니다.
   창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.
   b. 파일을 엽니다.
   컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에서 새 항목을 추가하라는 메시지를 표시합니다.
8. 변경 사항을 저장합니다.

웹 콘솔에서 시스템 무결성 모니터링 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **시스템 점검** → **시스템 무결성 모니터링** 섹션으로 가서 **구성** 버튼을 클릭합니다.
   시스템 무결성 모니터링 설정 창이 열립니다.
5. 파일/레지스트리 규칙을 내보내려면:
   a. **파일** 또는 **레지스트리** 탭에서 내보내려는 규칙을 선택합니다.
   b. **내보내기** 버튼을 클릭합니다. 열린 창에서 선택한 규칙을 내보낼 것인지 모든 규칙을 내보낼 것인지를 지정한 후 **내보내기**를 클릭합니다.
      규칙을 선택하지 않은 경우 Kaspersky Industrial CyberSecurity for Nodes는 모든 규칙을 내보냅니다.
      Kaspersky Industrial CyberSecurity for Nodes는 규칙 목록을 XML 파일로 내보냅니다.
6. 파일/레지스트리 규칙을 가져오려면:
   a. 4.0 이하 버전의 애플리케이션에서 만든 XML 파일에서 규칙을 가져오려면 **파일** 또는 **레지스트리** 탭에서 **이전 버전에서 가져오기** 버튼을 클릭합니다.
      4.5 이상 버전에서 생성한 XML 파일에서 규칙을 가져오는 경우 **가져오기**를 클릭합니다.
   b. 컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에서 새 항목을 추가하라는 메시지를 표시합니다.
   c. 창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.
   d. **가져오기** 버튼을 클릭합니다.
7. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 시스템 무결성 모니터링 규칙 목록을 내보내고 가져오는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **시스템 점검** → **시스템 무결성 모니터링** 옵션을 선택합니다.
2. **시스템 무결성 모니터링** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 시스템 무결성 모니터링 창이 열립니다.
3. 내보내거나 가져올 규칙에 따라 **파일** 또는 **레지스트리** 탭으로 이동합니다.

4. 파일 규칙 및 레지스트리 규칙 목록을 내보내려면:

   a. 전체 목록을 내보내려면 버튼을 누르고 **내보내기**을 선택합니다.

   b. 목록의 일부만 내보내려면 다음 단계를 수행합니다.

      1. **Ctrl** 또는 **Shift** 키를 사용하여 내보낼 목록 항목을 선택합니다. 모든 항목을 선택하려면 **Ctrl+A**를 누릅니다.

      2. 버튼을 클릭하고 **선택 항목 내보내기**을 선택합니다.

   c. 창이 열리면 내보낼 XML 파일의 이름을 지정하고 파일을 저장할 폴더를 선택합니다. **저장** 버튼을 누릅니다.

   Kaspersky Industrial CyberSecurity for Nodes는 규칙 목록을 XML 파일로 내보냅니다.

5. 파일/레지스트리 규칙을 가져오려면:

   a. **가져오기** 버튼을 클릭합니다.

   창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.

   b. 파일을 엽니다.

   컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Industrial CyberSecurity for Nodes는 기존 목록을 삭제하거나 XML 파일에서 새 항목을 추가하라는 메시지를 표시합니다.

6. 변경 사항을 저장합니다.

시스템 무결성 모니터링 리포트 보기

시스템 무결성 모니터링 규칙의 성능을 분석하기 위해 애플리케이션에서 생성된 리포트 및 이벤트를 확인할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 구성 요소에 대해 다음과 같은 리포트를 생성합니다.

- 모니터링 규칙이 가장 많이 트리거된 컴퓨터에 대한 리포트
- 가장 자주 트리거되는 모니터링 규칙에 대한 리포트

  이 애플리케이션은 가장 자주 실행되는 모니터링 규칙의 리포트 생성을 위해 다음 이벤트를 기록합니다.

  - *파일 또는 폴더 변경이 탐지됨*
  - *통계 전용: 제어 영역에서 금지된 파일 동작*
  - *신뢰할 수 있는 사용자가 제어 영역에서 파일 동작을 수행하도록 허용됨*
  - *제어 영역에서 미관리 파일 동작.*

> 이러한 이벤트의 저장 기간을 구성하려면 정책의 **이벤트 구성** 섹션에서 일반 시스템 무결성 모니터링 이벤트: *파일 또는 폴더 변경이 탐지됨*의 지속 시간을 지정합니다.

기본 설정으로 리포트가 생성된 날짜를 포함하여 지난 30일 동안의 리포트가 생성됩니다.

Kaspersky Security Center 관리 콘솔에서 시스템 무결성 모니터링 리포트를 확인하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **중앙 관리 서버** 노드에서 **리포트** 탭을 선택합니다.
3. **새 리포트 템플릿** 버튼을 클릭합니다.
   새 리포트 템플릿 마법사가 시작됩니다.
4. 리포트 템플릿 마법사의 안내를 따릅니다. **리포트 템플릿 유형 선택** 단계에서 시스템 무결성 모니터링 리포트(**기타** 섹션)를 선택합니다:
   - **파일 무결성 모니터/시스템 무결성 모니터링 규칙이 가장 자주 트리거되는 상위 10개 기기**.
   - **가장 자주 트리거된 파일 무결성 모니터/시스템 무결성 모니터링의 상위 10개 규칙**.

   새 리포트 템플릿 마법사를 종료하면 **리포트** 탭에 표로 새 리포트 템플릿이 나타납니다.
5. 더블 클릭으로 리포트를 엽니다.

리포트 생성 프로세스가 시작됩니다. 리포트가 새 창으로 표시됩니다.

웹 콘솔에서 시스템 무결성 모니터링 리포트를 확인하는 방법

1. 웹 콘솔의 메인 창에서 **모니터링** → **리포트** 옵션을 선택합니다.
2. **추가** 버튼을 클릭합니다.
   새 리포트 템플릿 마법사가 시작됩니다.
3. **템플릿**의 **기타** 섹션에서 시스템 무결성 모니터링 리포트를 선택합니다:
   - **파일 무결성 모니터/시스템 무결성 모니터링 규칙이 가장 자주 트리거되는 상위 10개 기기**.
   - **가장 자주 트리거된 파일 무결성 모니터/시스템 무결성 모니터링의 상위 10개 규칙**.

   새 리포트 템플릿 마법사를 종료하면 새 리포트 템플릿이 표에 나타납니다.
4. 리포트를 선택하고 실행합니다.

리포트 생성 프로세스가 시작됩니다. 리포트가 새 창으로 표시됩니다.

애플리케이션에서 생성된 이벤트를 보려면 Kaspersky Security Center 콘솔에서 이벤트 선택을 사용할 수도 있습니다.

로그 검사

로그 검사는 Windows 이벤트 로그 분석 결과를 바탕으로 보호 중인 환경의 무결성을 모니터링합니다. 이 애플리케이션이 시스템에서 비정상적인 행동 징후를 감지하면 이것이 사이버 공격 시도를 의미할 수 있으므로 관리자에게 알립니다.

Kaspersky Industrial CyberSecurity for Nodes는 규칙에 따라 Windows 이벤트 로그를 분석하여 위반 사항을 탐지합니다. 이 구성 요소에는 사전 정의된 규칙이 포함되어 있습니다. 사전 정의된 규칙은 휴리스틱 분석으로 작동합니다. 사용자 자신의 규칙을 추가할 수도 있습니다(사용자 지정 규칙). 규칙이 트리거되면 애플리케이션이 *심각* 상태의 이벤트를 생성합니다.

로그 검사를 사용할 경우에는 보안 감사 정책이 구성되어 시스템이 관련 이벤트를 기록하는지 확인해야 합니다(자세한 내용은 Microsoft 기술 지원 웹사이트 참조).

파라미터	설명
사전 정의된 규칙	로그 검사 규칙 목록입니다. 사전 정의된 규칙에는 보호 대상 컴퓨터에서 일어나는 비정상 활동 템플릿이 포함됩니다. 비정상 활동은 공격 시도를 의미할 수 있습니다.
사용자 지정 규칙	사용자가 추가한 로그 검사 규칙 목록입니다. 사용자 자신의 로그 검사 규칙 트리거 기준을 설정할 수 있습니다. 이를 위해서는 이벤트 ID를 입력하고 이벤트 소스를 선택해야 합니다. 표준 로그인 *Application*, *Security*, *System* 중에서 이벤트 소스를 선택할 수 있습니다. 타사 애플리케이션 로그를 지정할 수도 있습니다.

사용자 지정 규칙 추가

사용자 자신의 로그 검사 규칙 트리거 기준을 설정할 수 있습니다. 이를 위해서는 이벤트 ID를 입력하고 이벤트 소스를 선택해야 합니다. Microsoft 기술 지원 웹사이트에서 이벤트 ID를 조회할 수 있습니다. 표준 로그인 *Application*, *Security*, *System* 중에서 이벤트 소스를 선택할 수 있습니다. 타사 애플리케이션 로그를 지정할 수도 있습니다. 이벤트 뷰어 도구를 사용해 타사 애플리케이션 로그의 이름을 검색할 수 있습니다. 타사 애플리케이션 로그는 애플리케이션 및 서비스 로그 폴더에 있습니다(예: *Windows PowerShell* 로그).

이 애플리케이션은 지정된 로그가 실제로 Windows 이벤트 로그에 있는지 여부는 확인하지 않습니다. 로그 이름에 실수가 있는 경우 이 애플리케이션은 해당 로그의 이벤트를 모니터링하지 않습니다.

Kaspersky 전문가가 생성한 여러 규칙이 이미 사용자 지정 규칙 목록에 포함되어 있습니다.

Kaspersky Security Center 관리 콘솔에서 사용자 지정 규칙을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **시스템 점검** 옵션을 선택합니다.
4. **로그 검사** 섹션에서 **설정** 버튼을 클릭합니다.
5. **로그 검사** 확인란을 선택합니다.
6. **사용자 지정 규칙** 탭에서 **로그 검사에 사용자 지정 규칙 적용** 확인란을 선택합니다.

7. 활성화하려는 사용자 지정 규칙 옆의 확인란을 선택합니다.

8. 필요하다면 **추가** 버튼을 클릭해 사용자 자신의 사용자 지정 규칙을 생성합니다.

9. 그러면 창이 열립니다. 이 창에서 사용자 지정 규칙을 구성합니다.

   - **규칙 이름**.
   - **로그 이름**. Windows 이벤트 로그. *Application*, *Security*, *System* 로그를 사용할 수 있습니다.
   - **경로**. 타사 애플리케이션 로그입니다. 이벤트 뷰어 도구를 사용해 타사 애플리케이션 로그의 이름을 검색할 수 있습니다. 타사 애플리케이션 로그는 애플리케이션 및 서비스 로그 폴더에 있습니다(예: Windows PowerShell 로그).
   - **이벤트 식별자**. Windows 이벤트 로그에 있는 이벤트 ID입니다. Microsoft 기술 문서에서 이벤트 ID를 조회할 수 있습니다.

10. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 사용자 지정 규칙을 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **시스템 점검** → **로그 검사** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. **로그 검사 사용** 확인란을 선택합니다.

6. **사용자 지정 규칙** 탭에서 **로그 검사에 사용자 지정 규칙 적용** 확인란을 선택합니다.

7. 토글을 사용하여 사용자 지정 규칙을 구성합니다:

8. 필요하다면 **추가** 버튼을 클릭해 사용자 자신의 사용자 지정 규칙을 생성합니다.

9. 그러면 창이 열립니다. 이 창에서 사용자 지정 규칙을 구성합니다.

   - **규칙 이름**.
   - **Windows 이벤트 로그 이름**. Windows 이벤트 로그. *Application*, *Security*, *System* 로그를 사용할 수 있습니다.
   - **출처**. 타사 애플리케이션 로그입니다. 이벤트 뷰어 도구를 사용해 타사 애플리케이션 로그의 이름을 검색할 수 있습니다. 타사 애플리케이션 로그는 애플리케이션 및 서비스 로그 폴더에 있습니다(예: Windows PowerShell 로그).
   - **이벤트 ID**. Windows 이벤트 로그에 있는 이벤트 ID입니다. Microsoft 기술 문서에서 이벤트 ID를 조회할 수 있습니다.

10. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 사용자 지정 규칙을 추가하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **시스템 점검** → **로그 검사** 옵션을 선택합니다.
2. **로그 검사** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   이는 **속성: 로그 검사** 창을 엽니다.
3. **로그 검사** 확인란을 선택합니다.
4. **사용자 지정 규칙** 탭에서 **로그 검사에 사용자 지정 규칙 적용** 확인란을 선택합니다.
5. 활성화하려는 사용자 지정 규칙 옆의 확인란을 선택합니다.
6. 필요하다면 **추가** 버튼을 클릭해 사용자 자신의 사용자 지정 규칙을 생성합니다.
7. 그러면 창이 열립니다. 이 창에서 사용자 지정 규칙을 구성합니다.
   - **규칙 이름**.
   - **로그 이름**. Windows 이벤트 로그. *Application*, *Security*, *System* 로그를 사용할 수 있습니다.
   - **경로**. 타사 애플리케이션 로그입니다. 이벤트 뷰어 도구를 사용해 타사 애플리케이션 로그의 이름을 검색할 수 있습니다. 타사 애플리케이션 로그는 애플리케이션 및 서비스 로그 폴더에 있습니다(예: Windows PowerShell 로그).
   - **이벤트 식별자**. Windows 이벤트 로그에 있는 이벤트 ID입니다. Microsoft 기술 문서에서 이벤트 ID를 조회할 수 있습니다.
8. 변경 사항을 저장합니다.

이후 규칙이 트리거되면 Kaspersky Industrial CyberSecurity for Nodes가 *심각* 이벤트를 생성합니다.

사전 정의된 규칙 구성

사전 정의된 규칙에는 보호 대상 컴퓨터에서 일어나는 비정상 활동 템플릿이 포함됩니다. 비정상 활동은 공격 시도를 의미할 수 있습니다. 사전 정의된 규칙은 휴리스틱 분석으로 작동합니다. 7가지 사전 정의된 규칙을 로그 검사에서 사용할 수 있습니다. 규칙을 활성화하거나 비활성화할 수 있습니다. 사전 정의된 규칙은 삭제할 수 없습니다.

다음 작업의 이벤트를 모니터링하는 규칙의 트리거 기준을 구성할 수 있습니다.

- 무차별 암호 대입 감지
- 네트워크 로그인 감지

Kaspersky Security Center 관리 콘솔에서 사전 정의된 규칙을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **시스템 점검** 옵션을 선택합니다.
4. **로그 검사** 섹션에서 **설정** 버튼을 클릭합니다.

5. **로그 검사** 확인란을 선택합니다.

6. **사전 정의된 규칙** 탭에서 **로그 검사를 위한 사전 정의된 규칙을 적용합니다** 확인란을 선택합니다.

7. 사전 정의된 규칙을 구성하는 확인란을 선택하거나 선택을 해제합니다.

   - **시스템에서 무차별 대입 공격 의심 패턴이 발견되었습니다**.
   - **네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다**.
   - **Windows 이벤트 로그 남용 패턴이 발견되었습니다**.
   - **설치된 새 서비스에서 이례적 작업이 감지되었습니다**.
   - **명시적 자격 증명을 사용하는 이례적 로그인이 감지되었습니다**.
   - **시스템에서 Kerberos 위조 PAC(MS14-068) 공격 의심 패턴이 발견되었습니다**.
   - **권한이 있는 내장 관리자 그룹에서 의심스러운 변경 사항이 감지되었습니다**.

8. 필요하다면 **시스템에서 무차별 대입 공격 의심 패턴이 발견되었습니다** 규칙을 구성합니다:

   a. 규칙 밑에 있는 **설정** 버튼을 클릭합니다.

   b. 열린 창에서 규칙 트리거에 필요한 암호 입력 횟수와 시간을 지정합니다.

   c. **확인**을 누릅니다.

9. **네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다** 규칙을 선택한 관련 설정을 구성해야 합니다:

   a. 규칙 밑에 있는 **설정** 버튼을 클릭합니다.

   b. 창이 열리면 **네트워크 로그인 탐지** 블록에서 시간 간격의 시작과 끝을 지정합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 정의된 간격 도중 수행한 로그인 시도를 비정상 활동으로 간주합니다.

   기본적으로 간격은 설정되지 않으며 애플리케이션은 로그인 시도를 모니터링하지 않습니다. 애플리케이션이 로그인 시도를 계속 모니터링하도록 하려면 간격을 오전 12:00~오후 11:59로 설정합니다. 간격의 시작과 끝은 다르게 설정해야 합니다. 시작과 끝을 같게 설정 시 애플리케이션이 로그인 시도를 모니터링하지 않습니다.

   c. 신뢰하는 사용자와 신뢰하는 IP 주소(IPv4 및 IPv6)의 목록을 생성합니다.

   Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다. Kaspersky Industrial CyberSecurity for Nodes는 이러한 사용자와 컴퓨터에 대한 로그온 시도는 모니터링하지 않습니다.

   > Windows XP에서 실행 중인 애플리케이션에서는 IP 주소로 신뢰하는 컴퓨터를 제외할 수 없습니다.

   d. **확인** 버튼을 클릭합니다.

10. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 사전 정의된 규칙을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **시스템 점검** → **로그 검사** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. **로그 검사 사용** 확인란을 선택합니다.
6. **사전 정의된 규칙** 탭에서 **로그 검사를 위한 사전 정의된 규칙을 적용합니다** 확인란을 선택합니다.
7. 토글을 사용하여 사전 정의된 규칙을 구성합니다:
   - **시스템에서 무차별 대입 공격 의심 패턴이 발견되었습니다**.
   - **네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다**.
   - **Windows 이벤트 로그 남용 패턴이 발견되었습니다**.
   - **설치된 새 서비스에서 이례적 작업이 감지되었습니다**.
   - **명시적 자격 증명을 사용하는 이례적 로그인이 감지되었습니다**.
   - **시스템에서 Kerberos 위조 PAC(MS14-068) 공격 의심 패턴이 발견되었습니다**.
   - **권한이 있는 내장 관리자 그룹에서 의심스러운 변경 사항이 감지되었습니다**.
8. **확장됨** 탭에서 다음 설정을 구성합니다:
   - **시스템에서 무차별 대입 공격 의심 패턴이 발견되었습니다** 규칙이 트리거되게 하려면 암호 입력 시도 횟수와 시간을 설정합니다.
   - **네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다** 규칙이 트리거되게 하려면 애플리케이션이 모든 로그인 시도를 비정상 활동으로 간주하는 시간 간격의 시작과 끝을 지정합니다.
     기본적으로 간격은 설정되지 않으며 애플리케이션은 로그인 시도를 모니터링하지 않습니다. 애플리케이션이 로그인 시도를 계속 모니터링하도록 하려면 간격을 오전 12:00~오후 11:59로 설정합니다. 간격의 시작과 끝은 다르게 설정해야 합니다. 시작과 끝을 같게 설정 시 애플리케이션이 로그인 시도를 모니터링하지 않습니다.
9. 신뢰하는 사용자와 신뢰하는 IP 주소(IPv4 및 IPv6)의 목록을 대응하는 탭에 생성합니다.
   계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 직접 입력할 수 있습니다.

   > Windows XP에서 실행 중인 애플리케이션에서는 IP 주소로 신뢰하는 컴퓨터를 제외할 수 없습니다.

10. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 사전 정의된 규칙을 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **시스템 점검** → **로그 검사** 옵션을 선택합니다.
2. **로그 검사** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   이는 **속성: 로그 검사** 창을 엽니다.
3. **로그 검사** 확인란을 선택합니다.
4. **사전 정의된 규칙** 탭에서 **로그 검사를 위한 사전 정의된 규칙을 적용합니다** 확인란을 선택합니다.
5. 사전 정의된 규칙을 구성하는 확인란을 선택하거나 선택을 해제합니다.
   - **시스템에서 무차별 대입 공격 의심 패턴이 발견되었습니다**.
   - **네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다**.
   - **Windows 이벤트 로그 남용 패턴이 발견되었습니다**.
   - **설치된 새 서비스에서 이례적 작업이 감지되었습니다**.
   - **명시적 자격 증명을 사용하는 이례적 로그인이 감지되었습니다**.
   - **시스템에서 Kerberos 위조 PAC(MS14-068) 공격 의심 패턴이 발견되었습니다**.
   - **권한이 있는 내장 관리자 그룹에서 의심스러운 변경 사항이 감지되었습니다**.
6. 필요하다면 **시스템에서 무차별 대입 공격 의심 패턴이 발견되었습니다** 규칙을 구성합니다:
   a. 규칙 밑에 있는 **설정** 버튼을 클릭합니다.
   b. 열린 창에서 규칙 트리거에 필요한 암호 입력 횟수와 시간을 지정합니다.
   c. **확인**을 누릅니다.
7. **네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다** 규칙을 선택한 관련 설정을 구성해야 합니다:
   a. 규칙 밑에 있는 **설정** 버튼을 클릭합니다.
   b. 창이 열리면 **네트워크 로그인 탐지** 블록에서 시간 간격의 시작과 끝을 지정합니다.
      Kaspersky Industrial CyberSecurity for Nodes는 정의된 간격 도중 수행한 로그인 시도를 비정상 활동으로 간주합니다.
      기본적으로 간격은 설정되지 않으며 애플리케이션은 로그인 시도를 모니터링하지 않습니다. 애플리케이션이 로그인 시도를 계속 모니터링하도록 하려면 간격을 오전 12:00~오후 11:59로 설정합니다. 간격의 시작과 끝은 다르게 설정해야 합니다. 시작과 끝을 같게 설정 시 애플리케이션이 로그인 시도를 모니터링하지 않습니다.
   c. 신뢰하는 사용자와 신뢰하는 IP 주소(IPv4 및 IPv6)의 목록을 생성합니다.
      Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다. Active Directory에서 사용자 목록을 생성합니다. Kaspersky Industrial CyberSecurity for Nodes는 이러한 사용자와 컴퓨터에 대한 로그온 시도는 모니터링하지 않습니다.

Windows XP에서 실행 중인 애플리케이션에서는 IP 주소로 신뢰하는 컴퓨터를 제외할 수 없습니다.

d. **확인** 버튼을 클릭합니다.

8. 변경 사항을 저장합니다.

이후 규칙이 트리거되면 Kaspersky Industrial CyberSecurity for Nodes가 *심각* 이벤트를 생성합니다.

성능 분석기

성능 분석기 작업은 가장 활성화된 애플리케이션과 접근 시도가 가장 많은 파일의 목록을 생성합니다. 이 정보는 애플리케이션이 산업용 소프트웨어 성능에 미치는 영향을 최소화하기 위해 신뢰 구역을 정의하는 데 도움이 될 수 있습니다.

성능 분석기 작업이 올바르게 작동하려면 작업이 시작된 컴퓨터가 Windows Vista 이상을 실행해야 합니다.

이 작업은 Kaspersky Security Center 웹 콘솔과 애플리케이션 콘솔에서만 관리할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서 작업 설정 및 성능 분석기 작업 실행

1. 새 작업 마법사를 시작합니다.
2. **작업 유형** 드롭다운 목록에서 **성능 분석기** 옵션을 선택합니다.
3. 작업 이름을 입력하거나 기본 이름을 유지합니다.
4. 작업을 할당할 장치를 선택하고 **다음** 버튼을 클릭합니다.
5. **작업 범위** 창에서 작업 범위를 지정하고 **다음**를 클릭합니다.
6. **작업을 실행할 계정 선택** 창에서 계정을 지정하고 **다음** 버튼을 클릭합니다.
7. **작업 생성 마침** 창에서 **생성이 완료되면 작업 세부 정보 열기** 확인란을 선택하고 **마침** 버튼을 클릭합니다.
8. 열린 창에서 **애플리케이션 설정** 탭을 선택합니다.
9. **성능 분석기 설정** 섹션으로 갑니다.
10. **다음 시간 후 작업 자동 중지** 필드에서 경과 후 Kaspersky Industrial CyberSecurity for Nodes 분석을 중지해야 하는 시간 간격을 시간(1~168시간) 또는 일(1~7일)로 설정합니다.
11. 필요하다면 **규칙 생성 범위 제한**에서 Kaspersky Industrial CyberSecurity for Nodes가 예외 규칙 생성을 위한 분석을 수행할 폴더 목록을 생성합니다.

    Kaspersky Industrial CyberSecurity for Nodes는 마스크 입력 시 환경 변수와 `*` 및 `?` 문자를 지원합니다. UNC(범용 이름 지정 규칙) 형식으로 경로를 지정하여 네트워크 폴더나 파일을 검사 범위에 추가할 수도 있습니다.

    기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 범위 제한 없이 작업을 실행합니다.
12. **스케줄** 탭을 선택하고 작업 스케줄을 구성합니다.
13. 변경 사항을 저장합니다.
14. 생성된 작업 이름 옆의 확인란을 선택하고 **시작** 버튼을 클릭합니다.

애플리케이션 콘솔에서 설정 관리 및 성능 분석기 작업 실행

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **시스템 점검** → **성능 분석기** 옵션을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.

3. 창이 열리면 **작업 설정** 탭의 **다음 시간 후 작업 중지** 필드에서 경과 후 Kaspersky Industrial CyberSecurity for Nodes 분석을 중지해야 하는 시간 간격을 시간(1~168시간) 또는 일(1~7일)로 설정합니다.

4. 필요하다면 **규칙 생성 범위**에서 Kaspersky Industrial CyberSecurity for Nodes가 예외 규칙 생성을 위한 분석을 수행할 폴더 목록을 생성합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 마스크 입력 시 환경 변수와 `*` 및 `?` 문자를 지원합니다. UNC(범용 이름 지정 규칙) 형식으로 경로를 지정하여 네트워크 폴더나 파일을 검사 범위에 추가할 수도 있습니다.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 범위 제한 없이 작업을 실행합니다.

5. **실행 모드** 탭으로 갑니다.

6. **수동**를 선택하거나 작업 실행 모드를 구성합니다.

7. 필요한 경우 **사용자**에서 작업을 실행할 사용자 계정을 지정합니다.

8. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

9. **관리** 블록에서 **시작** 링크를 클릭합니다.

성능 분석기 작업 결과를 Kaspersky Industrial CyberSecurity for Nodes 정책의 신뢰 구역 설정 또는 애플리케이션의 로컬 신뢰 구역 설정으로 직접 내보내거나, 리포트의 개체 정보를 XML 파일에 저장한 다음 이 파일을 설정으로 가져올 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 리포트의 파일을 검사 예외 목록에 추가하고, 신뢰 구역의 신뢰하는 애플리케이션 목록에 추가합니다.

Kaspersky Security Center 웹 콘솔에서 성능 분석기 작업 결과 내보내기

1. 로컬 작업 결과를 내보내려면:

   a. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)** 옵션을 선택합니다.

   b. 작업 설정을 구성할 장치의 이름을 클릭합니다.

   c. **<장치 이름>** 창이 열리면 **작업** 탭을 선택합니다.

   d. 관련 있는 성능 분석기 작업을 클릭합니다.

2. 그룹 작업 결과를 내보내려면:

   a. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.

   b. 관련 있는 성능 분석기 작업을 클릭합니다.

3. 열린 창에서 **애플리케이션 설정** 탭을 선택합니다.
   작업 속성 창이 열립니다.

4. **성능 분석기 결과** 섹션으로 갑니다.

5. 리포트에 해시를 포함하려면 **파일 해시 고려** 확인란을 선택합니다. 기본적으로 확인란의 선택이 취소됩니다.

6. 필요하다면 **파일 경로 고려** 확인란을 선택 해제하여 리포트에서 파일 경로를 제외합니다. 기본적으로 확인란이 선택되어 있습니다.

   파일 해시 고려 확인란과 **파일 경로 고려** 확인란 중 하나 이상을 선택해야 합니다.

7. **파일** 탭과 **애플리케이션** 탭에서 내보낼 개체를 선택합니다.
   전체 리포트를 내보내거나 리포트를 확장하고 내보낼 개별 개체를 선택할 수 있습니다.

8. 정책의 신뢰 구역 설정으로 작업 결과를 내보내려면:

   a. **설정으로 내보내기** 버튼을 클릭합니다.

   b. 열린 창에서 설정을 내보낼 정책 이름 옆의 확인란을 선택한 다음 **내보내기** 버튼을 클릭합니다.
      정책에 이미 예외 목록이 구성되어 있는 경우 Kaspersky Industrial CyberSecurity for Nodes는 이 목록에 새 항목을 추가합니다.

9. 작업 결과를 XML 파일로 내보내려면:

   a. **파일로 내보내기** 버튼을 클릭합니다.

   b. **내보내기** 버튼을 클릭합니다. 열린 창에서 선택한 개체를 내보낼 것인지 모든 개체를 내보낼 것인지를 지정한 후 **내보내기** 버튼을 클릭합니다.

애플리케이션 콘솔에서 성능 분석기 작업 결과 내보내기

Kaspersky Industrial CyberSecurity for Nodes의 로컬 신뢰 구역 설정으로 성능 분석기 작업 결과 내보내기는 **로컬 예외 항목 사용 허용** 및 **신뢰하는 로컬 애플리케이션 편집 허용**가 **검사 예외** 및 **신뢰하는 애플리케이션** 탭(정책의 **보충 → 신뢰 구역** 섹션에 있음)에서 선택되어 있는 경우 Kaspersky Industrial CyberSecurity for Nodes 콘솔에서 사용할 수 있습니다.

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **시스템 점검 → 성능 분석기** 옵션을 선택합니다.

2. 결과 창에서 **결과** 링크를 클릭합니다.
   성능 분석기 결과 창이 열립니다.

3. 리포트에 해시를 포함하려면 **파일 해시 고려** 확인란을 선택합니다. 기본적으로 확인란의 선택이 취소됩니다.

4. 필요하다면 **파일 경로 고려** 확인란을 선택 해제하여 리포트에서 파일 경로를 제외합니다. 기본적으로 확인란이 선택되어 있습니다.

   파일 해시 고려 확인란과 **파일 경로 고려** 확인란 중 하나 이상을 선택해야 합니다.

5. **파일** 탭과 **애플리케이션** 탭에서 내보낼 개체를 선택합니다.
   전체 리포트를 내보내거나 리포트를 확장하고 내보낼 개별 개체를 선택할 수 있습니다.

6. 작업 결과를 애플리케이션의 신뢰 구역 설정으로 내보내려면:

   a. **설정으로 내보내기** 버튼을 클릭합니다.

   b. 선택한 개체를 신뢰 구역 설정으로 내보낼 것인지 확인합니다.

      설정에 이미 예외 목록이 구성되어 있는 경우 Kaspersky Industrial CyberSecurity for Nodes는 이 목록에 새 항목을 추가합니다.

7. 작업 결과를 XML 파일로 내보내려면:

   a. **파일로 내보내기** 버튼을 클릭합니다.

   b. 창이 열리면 개체 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

온디맨드 검사

이 섹션에서는 온디맨드 검사 작업에 대한 정보와 보호 중인 장치에서의 온디맨드 검사 작업 설정 및 보안 설정 구성에 대한 지침을 제공합니다.

온디맨드 검사 작업 정보

Kaspersky Industrial CyberSecurity for Nodes는 지정된 영역에서 바이러스 및 기타 컴퓨터 보안 위협을 검사합니다. Kaspersky Industrial CyberSecurity for Nodes는 보호 중인 장치 파일, RAM 및 자동 실행 개체를 검사합니다.

Kaspersky Industrial CyberSecurity for Nodes에서 다음과 같은 온디맨드 검사 작업을 사용할 수 있습니다:

- *운영 체제 시작 시 검사* 작업은 Kaspersky Industrial CyberSecurity for Nodes가 시작될 때마다 수행됩니다. 애플리케이션이 하드 드라이브, 이동식 드라이브, 시스템 메모리 및 프로세스 메모리의 부트 섹터와 마스터 부트 레코드를 검사합니다. 이 작업을 실행할 때마다 Kaspersky Industrial CyberSecurity for Nodes는 감염되지 않은 부팅 섹터의 사본을 만듭니다. 다음에 작업이 시작될 때 해당 섹터에서 보안위협을 탐지하면, 백업 복사본으로 교체합니다.

  운영 체제 시작 시 검사 작업은 설치 후 자동 생성됩니다. **알림** 모드는 기본적으로 적용됩니다. 이 경우, 장치에 Kaspersky Industrial CyberSecurity for Nodes를 배포한 후에, 검사에서 시스템 서비스 문제가 발견되지 않으면 *운영 체제 시작 시 검사* 작업을 활성화할 수 있습니다. 애플리케이션이 중요 시스템 서비스를 감염되었거나 감염 의심 개체로 탐지하면 **알림** 모드가 원인을 파악하고 문제를 해결할 시간을 제공합니다. 시스템 파일을 치료하거나 제거하면 운영 체제 시작에 심각한 문제가 발생할 수 있습니다. 애플리케이션이 **권장** 모드를 적용하면, 다음 동작이 수행됩니다: **권장 작업 수행**.

  > 보호 중인 장치가 절전 또는 최대 절전 모드였다가 켜지면 *운영 체제 시작 시 검사* 작업이 수행되지 않을 수 있습니다. 이 작업은 보호 중인 장치를 다시 시작하거나 완전히 종료된 상태에서 시작할 때만 수행됩니다.

- *중요 영역 검사* 작업은 기본적으로 매주 스케줄에 따라 수행됩니다. Kaspersky Industrial CyberSecurity for Nodes는 운영 체제의 중요한 영역에 있는 개체(자동 실행 개체, 하드 드라이브 및 이동식 드라이브의 부팅 섹터와 마스터 부팅 레코드, 시스템 메모리, 프로세스 메모리)를 검사합니다. Kaspersky Industrial CyberSecurity for Nodes는 **알림** 레벨에 해당하는 보안 설정을 적용합니다. *중요 영역 검사* 작업의 설정을 수정할 수 있습니다.

- *애플리케이션 무결성 제어* 작업이 매일 수행됩니다. 이 작업은 손상 및 수정 사항이 있는지 Kaspersky Industrial CyberSecurity for Nodes 모듈을 검사하는 옵션을 제공합니다. 애플리케이션 설치 폴더가 검사됩니다. 작업 실행 통계는 확인한 모듈 수와 손상된 것으로 파악된 모듈의 수를 나타냅니다. 이 작업 설정의 값은 기본적으로 정의되어 있으며 편집할 수 없습니다. 작업 시작 스케줄 설정은 편집할 수 있습니다.

- *이동식 드라이브 검사* 작업은 이동식 드라이브에 있는 파일을 포함하여 사용자가 실행하거나 복사하는 모든 파일을 검사합니다. 이동식 드라이브를 컴퓨터에 연결했을 때 자동으로 검사하도록 구성하여 바이러스 및 기타 악성 코드의 확산을 방지할 수 있습니다.

- *전체 검사* 작업은 매주 수행됩니다. 이 작업은 시스템 백업 저장소, 부트 섹터, 메일 데이터베이스를 포함하여 보호 중인 장치를 철저히 검사합니다.

또한 사용자 지정 온디맨드 검사 작업을 생성할 수 있습니다(예: 보호 중인 장치의 공유 폴더 검사 작업).

Kaspersky Industrial CyberSecurity for Nodes는 동시에 여러 온디맨드 검사 작업을 실행할 수 있습니다.

작업 검사 범위 및 보안 설정 정보

애플리케이션 콘솔에서 선택한 온디맨드 검사 작업의 검사 범위는 Kaspersky Industrial CyberSecurity for Nodes가 제어할 수 있는 보호 중인 장치 파일 리소스의 목록으로 표시됩니다.

항목 또는 노드는 보호 중인 장치 파일 리소스의 목록 보기 모드로 다음과 같이 표시됩니다.

☑ 해당 노드가 검사 범위에 포함됩니다.

☐ 해당 노드가 검사 범위에서 제외됩니다.

보안 설정

선택된 온디맨드 검사 작업에서 기본 보안 설정을 전체 보호 또는 검사 범위에 대해 공통 설정으로 구성하거나, 장치 파일 리소스 목록에서 노드나 항목마다 다른 설정으로 구성하여 수정할 수 있습니다.

> 동일한 개체가 여러 보호 범위 항목에 포함되어 있고 이러한 항목의 보안 레벨이 서로 다른 경우 목록의 마지막 규칙이 우선 적용됩니다. 예를 들어 **모든 하드 드라이브**(보안 레벨 **알림**)와 `*\Users\*\Downloads\*`(보안 레벨 **사용자 지정**)이라는 두 항목이 포함된 보호 범위를 생각해 보십시오. 애플리케이션은 `Downloads` 폴더를 제외하고 Inform 레벨에 따라 하드 드라이브를 검사합니다. 이 항목이 보호 범위 목록의 마지막 항목이기 때문에 애플리케이션은 수동으로 지정된 설정에 따라 `Downloads` 폴더를 검사합니다.

선택한 상위 노드에 대해 구성된 보안 설정은 모든 하위 노드에 자동 적용됩니다. 상위 노드의 보안 설정은 별도로 구성된 하위 노드에는 적용되지 않습니다.

선택한 검사 범위 또는 보호 범위의 설정은 다음 중 한가지 방법으로 구성할 수 있습니다.

- 사전 정의된 세 가지 보안 레벨(**최대 성능**, **권장**, **최대 보호**) 중 하나를 선택합니다.
- 보호 중인 장치 파일 리소스의 목록에서 선택한 노드나 항목의 보안 설정을 직접 변경합니다(보안 레벨이 **사용자 지정**으로 변경됨).

사전 정의된 검사 범위

선택한 온디맨드 검사 작업에 대해 보호 중인 장치 파일 리소스 목록이 **검사 범위** 창에 표시됩니다.

> 파일 리소스 목록은 구성된 Microsoft Windows 보안 설정을 기반으로 읽기 접근 권한을 가진 노드를 표시합니다.

Kaspersky Industrial CyberSecurity for Nodes는 다음과 같은 사전 정의된 검사 범위를 포함합니다.

- **모든 하드 드라이브**. Kaspersky Industrial CyberSecurity for Nodes가 보호 중인 장치 하드 드라이브의 개체를 검사합니다. 검사 범위에서 모든 하드 드라이브, 개별 디스크, 폴더 또는 파일을 포함하거나 제외할 수 있습니다.
- **모든 이동식 드라이브**. Kaspersky Industrial CyberSecurity for Nodes가 외부 장치(예: CD 또는 이동식 드라이브)의 파일을 검사합니다. 검사 범위에서 모든 이동식 드라이브, 개별 디스크, 폴더 또는 파일을 포함하거나 제외할 수 있습니다.
- **모든 네트워크 드라이브**. 네트워크 폴더 또는 파일의 경로를 범용 명명 규칙(UNC) 형식으로 지정하면 이러한 항목을 검사 범위에 추가할 수 있습니다. 작업을 실행하는 데 사용되는 계정에는 추가된 네트워크 폴더 및 파일에 대한 접근 권한이 있어야 합니다. 기본적으로 온디맨드 검사 작업은 시스템 계정으로 실행됩니다.

  연결된 네트워크 드라이브도 보호 중인 장치의 파일 리소스 트리에 표시되지 않습니다. 검사 범위에 네트워크 드라이브의 개체를 포함하려면 UNC(Universal Naming Convention) 형식으로 이 네트워크 드라이브에 해당하는 폴더 경로를 지정합니다.

- **커널 메모리**. Kaspersky Industrial CyberSecurity for Nodes가 검사 시작 시 운영 체제에서 실행 중인 프로세스의 실행 파일 및 모듈을 검사합니다.
- **실행 중인 프로세스 및 시작 개체**. Kaspersky Industrial CyberSecurity for Nodes가 레지스트리 키 및 구성 파일(예: WIN.INI 또는 SYSTEM.INI)은 물론, 보호 중인 장치 시작 시 자동 시작되는 애플리케이션 모듈을 검사합니다.
- **디스크 부트 섹터**. Kaspersky Industrial CyberSecurity for Nodes가 하드 드라이브 및 이동식 미디어의 부트 섹터를 검사합니다.
- **시스템 백업**. Kaspersky Industrial CyberSecurity for Nodes가 System Volume Information 폴더의 내용을 검사합니다.

  Kaspersky Industrial CyberSecurity for Nodes 5.0에서는 이메일은 애플리케이션 검사 범위에서 제외됩니다. 이전 버전의 관리 플러그인을 사용하는 경우 애플리케이션은 정책에 포함되어 있더라도 이메일을 검사 범위에서 제외합니다.

표준 검사 범위는 기본적으로 네트워크 파일 리소스 트리에 표시됩니다. 검사 범위 설정에서 생성 시 네트워크 파일 리소스 목록에 추가할 수 있습니다.

기본적으로 온디맨드 검사 작업은 다음 범위에서 실행됩니다.

- *운영 체제 시작 시 검사* 작업:
  - **커널 메모리**.
  - **디스크 부트 섹터**.
- *중요 영역 검사* 작업:
  - **모든 하드 드라이브**(Windows 폴더 제외)
  - **모든 이동식 드라이브**.
  - **커널 메모리**.
  - **실행 중인 프로세스 및 시작 개체**.

- *온디맨드 검사* 작업:
  - **모든 하드 드라이브**(Windows 폴더 제외)
  - **모든 이동식 드라이브**.
  - **커널 메모리**.
  - **실행 중인 프로세스 및 시작 개체**.
- *전체 검사* 작업:
  - **모든 하드 드라이브**(Windows 폴더 제외)
  - **모든 이동식 드라이브**.
  - **커널 메모리**.
  - **실행 중인 프로세스 및 시작 개체**.
  - **시스템 백업**.
  - **디스크 부트 섹터**.

온라인 저장소 파일 검사

클라우드 파일 정보

Kaspersky Industrial CyberSecurity for Nodes는 Microsoft OneDrive 클라우드 파일과 상호 작용할 수 있습니다. 애플리케이션은 새로운 OneDrive Files On-Demand 기능을 지원합니다.

> Kaspersky Industrial CyberSecurity for Nodes는 다른 온라인 저장소를 지원하지 않습니다.

OneDrive 파일 온디맨드를 사용하면 장치의 저장 공간을 사용해 모든 OneDrive 파일을 다운로드할 필요 없이 모든 OneDrive 파일에 접근할 수 있습니다. 필요할 때 하드 드라이브에 파일을 다운로드할 수 있습니다.

OneDrive 파일 온디맨드 기능이 켜지면 파일 탐색기에서 각 파일의 **상태** 열 옆에 상태 아이콘이 표시됩니다. 각 파일의 상태는 다음 중 하나입니다:

이 상태 아이콘은 파일이 *온라인에서만 이용 가능*함을 뜻합니다. 온라인 전용 파일은 하드 드라이브에 실제로 저장되지 않습니다. 장치가 인터넷에 연결되어 있지 않으면 온라인 전용 파일을 열 수 없습니다.

이 상태 아이콘은 파일이 *로컬에서 사용 가능*함을 뜻합니다. 이는 온라인 전용 파일을 열었고 사용자의 장치에 다운로드한 경우입니다. 인터넷에 연결하지 않고도 언제든지 로컬에서 사용 가능한 파일을 열 수 있습니다. 공간을 확보하려면 파일을 다시 온라인 전용으로 변경할 수 있습니다.

이 상태 아이콘은 파일이 *하드 드라이브에 저장되며 항상 사용 가능*함을 뜻합니다.

클라우드 파일 검사

Kaspersky Industrial CyberSecurity for Nodes는 보호 중인 장치에 로컬로 저장된 클라우드 파일만 검사할 수 있습니다. 이러한 OneDrive 파일에는 및 상태입니다. 파일은 보호 중인 장치에 실제로 있지 않기 때문에 검사하는 동안 건너뜁니다.

Kaspersky Industrial CyberSecurity for Nodes는 검사 범위에 파일이 있더라도 검사 중 클라우드에서 자동으로 다운로드하지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes 작업은 클라우드 파일을 다양한 시나리오에 따라 처리합니다.

- 실시간 클라우드 파일 검사: 클라우드 파일이 포함된 폴더를 실시간 파일 보호 구성 요소 보호 범위에 추가할 수 있습니다. 사용자가 파일에 접근하면 파일을 검사합니다. 사용자가 파일에 접근하여 다운로드하고 로컬에서 사용 가능하게 되면 파일이 상태로 바뀝니다. 이렇게 하면 실시간 파일 보호 구성 요소에서 파일을 처리할 수 있습니다.

- 주문형 클라우드 파일 검사: 클라우드 파일이 포함된 폴더를 온디맨드 검사 작업의 검사 범위에 추가할 수 있습니다. 이 작업은 및 상태의 파일을 검사합니다. 검사 도중 범위 내에서 파일이 발견되면 건너뛰며, 작업 로그에 검사한 파일이 클라우드 파일의 자리 표시자이며 로컬 드라이브에 존재하지 않음을 나타내는 정보 이벤트가 기록됩니다.

- 애플리케이션 실행 제어 규칙 생성 및 사용: *애플리케이션 실행 제어를 위한 규칙 생성기* 작업을 사용하여 및 파일에 대한 허용 및 거부 규칙을 생성할 수 있습니다. 애플리케이션 실행 제어 구성 요소는 기본 거부 원칙과 생성 규칙을 적용하여 클라우드 파일을 처리하고 차단합니다.

  애플리케이션 실행 제어 구성 요소는 상태에 관계없이 모든 클라우드 파일의 시작을 차단합니다. 파일은 하드 드라이브에 실제로 저장되지 않기 때문에 애플리케이션의 규칙 생성 범위에 포함되지 않습니다. 이러한 파일에 대한 허용 규칙을 만들 수 없으므로 기본 거부 원칙이 적용됩니다.

OneDrive 클라우드 파일에서 위협이 탐지되면 애플리케이션이 검사 수행 작업의 설정에 지정된 동작을 적용합니다. 따라서 파일이 제거, 치료되거나, 격리 저장소나 백업 저장소로 이동될 수 있습니다.

로컬 파일에 대한 변경 사항은 관련 Microsoft OneDrive 설명서의 원칙에 따라 OneDrive에 저장된 복사본과 동기화됩니다.

사전 정의된 보안 레벨 정보

휴리스틱 분석 사용 보안 설정은 사전 설정된 보안 레벨 설정에 포함되지 않습니다. 이 설정을 변경해도 선택한 기본 보안 레벨은 변경되지 않습니다.

장치의 파일 리소스 트리에서 선택 노드에 사전 정의된 네 가지 보안 레벨인 **최대 성능**, **권장**, **최대 보호**, **알림** 중 하나를 적용할 수 있습니다. 이러한 레벨에는 각 사전 정의된 보안 설정이 있습니다(아래 표 참조).

최대 성능

최대 성능 보안 레벨은 보호 중인 장치 및 워크스테이션에서 Kaspersky Industrial CyberSecurity for Nodes를 사용하는 것 외에도 네트워크에 방화벽 및 기존 보안 정책 등의 추가 보호 장치 보안 조치가 있을 때 권장합니다.

권장

권장 보안 레벨은 장치에 대한 보호 및 성능 영향을 가장 효과적으로 조합합니다. Kaspersky 전문가는 이 레벨을 대부분의 회사 네트워크에서 장치를 보호하는 데 적합한 것으로 권장합니다. 기본적으로 **권장** 보안 레벨이 설정됩니다.

최대 보호

최대 보호 보안 레벨은 조직의 네트워크에 필요한 장치 보안 요구 사항이 높을 때 권장합니다.

알림

알림 보안 레벨은 회사 네트워크에 감염될 수 있는 컴퓨터가 많고, 컴퓨터를 차단하면 조직의 운영에 큰 지장을 초래할 수 있을 때 권장합니다.

사전 정의된 보안 레벨과 해당하는 보안 설정 값

옵션	보안 레벨			
	최대 성능	권장	최대 보호	알림
개체 유형	형식에 따라 검사한 개체	모든 개체	모든 개체	모든 개체
새로운 파일과 수정된 파일만 검사	활성화됨	비활성화됨	비활성화됨	비활성화됨
감염된 개체 및 기타 개체에 수행할 동작	치료. 치료 불가능한 경우 삭제	Kaspersky 전문가가 권장하는 동작 수행	치료. 치료 불가능한 경우 삭제	알림
복합 파일 검사	Microsoft Office 형식 배포 패키지 및 파일 검사	모든 압축 파일, 배포 패키지, Microsoft Office 형식 파일 검사	모든 압축 파일, 배포 패키지, Microsoft Office 형식 파일 검사	모든 압축 파일, 배포 패키지, Microsoft Office 형식 파일 검사
시스템 중요 개체는 운영 체제와 Kaspersky Industrial CyberSecurity for Nodes의 작동에 필요한 파일입니다. 이러한 파일은 삭제할 수 없습니다. 이러한 개체와 연결된 프로세스는 종료할 수 없습니다.				
선택한 개체 유형에 동작 적용	기본적으로 모든 개체 유형을 검사합니다	기본적으로 모든 개체 유형을 검사합니다	기본적으로 모든 개체 유형을 검사합니다	기본적으로 모든 개체 유형을 검사합니다
내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거	아니오	아니오	아니오	아니오
파일 예외	아니오	아니오	아니오	아니오
유형 기준으로 개체 탐지 안 함	아니오	아니오	아니오	아니오
검사 시간이 다음을 초과하면 검사 중지(초)	60초.	아니오	아니오	아니오
다음을 초과하는 복합 파일은 검사하지 않음(MB)	8MB	아니오	아니오	아니오
iSwift 기술 사용	예	예	예	예
iChecker 기술 사용	예	예	예	예

이동식 드라이브 검사

USB 포트를 통해 보호 중인 장치에 연결된 이동식 드라이브의 검색을 구성할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 운영 체제에 USB 외부 장치로 등록된 연결된 이동식 드라이브를 검사합니다. 장치 제어 구성 요소에 의해 연결이 차단되면 애플리케이션은 이동식 드라이브를 검사하지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes는 검사 중에 이동식 드라이브 접근을 허용합니다.

각 이동식 드라이브의 검사 결과는 이동식 드라이브 연결 시 생성되는 온디맨드 검사 작업의 작업 로그에서 이용할 수 있습니다.

이동식 드라이브 검사 구성 요소의 설정을 변경할 수 있습니다(아래 표 참조).

이동식 드라이브 검사 설정

파라미터	기본 값	설명
USB를 통해 연결 시 이동식 드라이브 검사	정리됨	USB를 통해 보호 중인 장치에 연결된 이동식 드라이브 검사를 켜거나 끌 수 있습니다.
크기(MB)가 다음 이하이면 이동식 드라이브 검사	4096MB	사용자는 검사된 드라이브의 데이터 최대 볼륨을 설정하여 구성 요소의 범위를 축소할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 저장된 데이터의 양이 지정된 값을 초과할 경우 이동식 드라이브를 검사하지 않습니다.
보안 레벨로 검사	최대 보호	사용자는 세 가지 보안 레벨 중 하나를 선택하여 생성된 온디맨드 검사 작업을 구성할 수 있습니다. • **최대 보호** • **권장** • **최대 성능** • **알림**. 감염되었을 때와 감염되었을 가능성이 있을 때, 그리고 다른 개체가 감지되었을 때 사용되는 알고리즘과 각 보안 레벨에 대한 다른 검사 설정은 온디맨드 검사 작업의 사전 정의된 보안 레벨에 해당합니다.

온디맨드 검사 작업 설정 기본값

온디맨드 검사 작업은 아래 표에서 설명하는 기본 설정을 사용합니다. 로컬 시스템 및 사용자 지정 온디맨드 검사 작업을 구성할 수 있습니다.

온디맨드 검사 작업 설정 기본값

파라미터	기본 값	설명
검사 범위	로컬 시스템 및 사용자 지정 작업에서 적용: • **운영 체제 시작 시 검사**: 공유 폴더 및 자동 실행 개체를 제외한 보호 중인 장치 전체. • **중요 영역 검사**: 공유 폴더 및 특정 운영 체제 파일을 제외한 보호 중인 장치 전체. • **온디맨드 검사**(사용자 지정 작업): 보호 중인 전체 장치. • **전체 검사**: 보호 중인 장치 전체를 검사합니다.	검사 범위를 변경할 수 있습니다. **이동식 드라이브 검사** 및 **애플리케이션 무결성 제어** 로컬 시스템 작업에 대한 검사 범위는 구성할 수 없습니다.
보안 설정	**권장** 보안 레벨에 해당하는 전체 검사 범위에 대한 공통 설정입니다.	보호 중인 장치의 파일 리소스 목록에서 선택된 노드에 대해 다음을 수행할 수 있습니다. • 사전 정의된 다른 보안 레벨 선택 • 수동으로 보안 설정 변경

파라미터	기본 값	설명
휴리스틱 분석 사용	*중요 영역 검사*, *운영 체제 시작 시 검사*, *온디맨드 검사*, *전체 검사* 작업에 **보통** 분석 레벨로 적용됩니다.	휴리스틱 분석기를 활성화 또는 비활성화할 수 있고 분석 레벨을 구성할 수 있습니다.
특정 권한으로 작업을 시작하는 설정	작업이 시스템 계정으로 시작됩니다.	*애플리케이션 무결성 제어* 작업을 제외한 모든 시스템 및 사용자 지정 온디맨드 검사 작업은 특정 계정 권한으로 시작 설정을 편집할 수 있습니다.
백그라운드 모드에서 작업 수행	적용되지 않음.	온디맨드 검사 작업의 우선 순위 레벨을 구성할 수 있습니다.
작업을 중요 영역 검사로 간주	*온디맨드 검사*, *운영 체제 시작 시 검사*, *중요 영역 검사*, *전체 검사* 작업에 적용됩니다.	온디맨드 검사 작업의 우선 순위 레벨을 구성할 수 있습니다.
여러 검사 작업을 동시에 실행하지 않음	적용되지 않음.	온디맨드 검사 작업의 우선 순위 레벨을 구성할 수 있습니다.
작업 실행 스케줄	로컬 시스템 작업에서 적용: • *운영 체제 시작 시 검사* – **애플리케이션 시작 후**. • *중요 영역 검사*, *애플리케이션 무결성 제어*, *전체 검사* – **매주**.	스케줄된 작업 시작에 대한 설정을 구성할 수 있습니다.

온디맨드 검사 작업 관리

이 섹션에서는 보호 중인 장치에서 *온디맨드 검사* 작업을 생성하고 구성하는 방법을 설명합니다.

온디맨드 검사 작업 만들기

Kaspersky Security Center 관리 콘솔에서 온디맨드 검사 작업 생성

1. 새 작업 마법사를 시작합니다.
2. **작업 유형 선택** 창에서, **온디맨드 검사**을 선택하고 **다음**을 클릭합니다.
3. **검사 범위** 창에서 검사 범위를 만듭니다.

   기본적으로 검사 범위에는 보호 중인 장치의 중요한 영역이 포함됩니다. 검사 범위는 테이블에 아이콘 ☑과 함께 표시됩니다. 제외된 검사 범위가 테이블에 ☐ 아이콘과 함께 표시됩니다. 사전 설정된 특정 검사 범위, 디스크, 폴더, 네트워크 개체 및 파일을 추가하여 검사 범위를 변경하고 추가된 각 범위에 대해서는 특정 보안 설정을 할당할 수 있습니다.

   - 검사에서 일부 범위를 제외하려면 해당 목록 항목을 선택하고 **삭제**를 클릭합니다.
   - 사전 정의된 검사 범위, 디스크, 폴더, 네트워크 개체 또는 파일을 포함하려면:
     a. **추가** 버튼을 클릭합니다.
     b. **검사 범위 선택** 창의 목록에서 사전 정의된 검사 범위를 선택하고 **확인**를 클릭합니다.

- 검사 범위에서 하위 폴더 또는 파일을 제외하려면:

  a. **검사 범위** 창에서 추가된 폴더(디스크)를 선택합니다.

  b. **편집** 버튼을 클릭합니다.

  c. **하위 폴더 포함** 확인란 비활성화

- 검사 범위 보안 설정을 변경하려면:

  a. 설정을 편집할 검사 범위를 선택하고 **구성**을 클릭합니다.

  b. 열린 창에서 사전 정의된 보안 레벨 중 하나를 선택하거나 **설정** 버튼을 클릭하여 보안 설정을 직접 구성합니다.

> 보안 설정은 실시간 파일 보호 작업과 같은 방식으로 구성됩니다.

4. 휴리스틱 분석기 및 다른 구성 요소와의 통합 구성:

- 휴리스틱 분석기의 사용을 구성합니다.
- 작업이 실행될 작업 프로세스에 *낮음* 우선순위를 할당하려면 **백그라운드 모드에서 작업 수행** 확인란을 선택합니다.

> 기본적으로 Kaspersky Industrial CyberSecurity for Nodes 작업이 실행되는 작업 프로세스에는 *중간*(보통) 우선순위가 할당됩니다.

- 작업을 *중요 영역 검사* 작업으로 사용하려면 **작업을 중요 영역 검사로 간주** 확인란을 선택합니다.
- 컴퓨터 부하를 최적화하려면 **여러 검사 작업을 동시에 실행하지 않음** 확인란을 선택합니다.

5. **이 작업이 할당되는 기기 선택** 창에서 장치 목록을 지정하고 **다음**를 클릭합니다.

6. **작업을 실행할 계정 선택** 창에서 계정을 지정하고 **다음** 버튼을 클릭합니다.

7. **작업 스케줄 구성** 창에서 작업 스케줄을 구성하고 **다음**을 클릭합니다.

8. 작업 이름을 입력합니다.

> 작업 이름은 100자 이하여야 하며 다음 기호는 사용할 수 없습니다: " * < > & \ : |

9. **작업 생성 마침** 창이 열립니다. **마침** 버튼을 클릭해 작업 생성을 완료합니다.

선택한 보호 중인 장치 또는 보호 중인 장치 그룹에 대해 새로운 *온디맨드 검사* 작업이 생성됩니다.

Kaspersky Security Center 웹 콘솔에서 온디맨드 검사 작업 생성

1. 새 작업 마법사를 시작합니다.

2. **새 작업** 창의 **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다.

3. **작업 유형** 드롭다운 목록에서 **온디맨드 검사**를 선택하고 **다음**을 클릭합니다.

4. 작업 범위를 선택하고 **다음**을 클릭합니다.

5. **작업을 실행할 계정 선택** 창에서 계정을 지정하고 **다음** 버튼을 클릭합니다.

6. 작업 이름을 입력합니다.

   작업 이름은 100자 이하여야 하며 다음 기호는 사용할 수 없습니다: " * < > & \ : |

7. **작업 생성 마침** 창이 열립니다. **마침** 버튼을 클릭해 작업 생성을 완료합니다.

선택한 보호 중인 장치 또는 보호 중인 장치 그룹에 대해 새로운 *온디맨드 검사* 작업이 생성됩니다.

애플리케이션 콘솔에서 온디맨드 검사 작업 생성

보호 중인 단일 장치에 대한 사용자 지정 작업은 **온디맨드 검사** 노드에서 생성할 수 있습니다.

새 온디맨드 검사 작업을 생성하고 구성하려면:

1. 애플리케이션 콘솔 트리에서 **온디맨드 검사** 노드의 마우스 오른쪽 메뉴를 엽니다.

2. **작업 생성** 옵션을 선택합니다.
   작업 생성 창이 열립니다.

3. 작업 이름을 입력하고 **확인**을 클릭합니다.

보호 중인 개별 장치에 대한 *온디맨드 검사* 작업이 생성됩니다.

백그라운드에서 온디맨드 검사 작업 실행

기본적으로 Kaspersky Industrial CyberSecurity for Nodes 작업이 실행되는 프로세스에는 *중간(보통)* 우선순위를 할당됩니다.

온디맨드 검사 작업을 실행할 프로세스에는 *낮음* 우선순위를 할당할 수 있습니다. 프로세스 우선 순위를 낮추면 작업을 실행하는 데 필요한 시간이 늘어나지만, 다른 실행 프로그램의 프로세스 성능 향상에 도움이 될 수 있습니다.

우선순위가 낮은 작동 중인 프로세스 하나에서 여러 백그라운드 작업을 실행할 수 있습니다.

기존 *온디맨드 검사* 작업의 우선 순위를 변경하려면, 작업 설정의 **백그라운드 모드에서 작업 수행** 확인란을 선택합니다.

구성된 작업 설정이 저장되고 실행 중인 작업에 즉시 적용됩니다. 작업이 실행되지 않는 경우 다음 시작 시 수정된 설정이 적용됩니다.

중요 영역 검사 실행 등록

기본적으로 장치 보호 상태는 **Kaspersky Industrial CyberSecurity for Nodes** 노드의 결과 창에 표시되고 *중요 영역 검사* 작업이 수행된 후 매주 업데이트됩니다.

장치 보호 상태가 업데이트되는 시간은 **작업을 중요 영역 검사로 간주** 확인란이 선택된 온디맨드 검사 작업의 스케줄과 연동됩니다.

온디맨드 검사 작업의 검사 범위 구성

*운영 체제 시작 시 검사*와 *중요 영역 검사* 작업에서 검사 범위를 수정하는 경우, 설치 마법사를 사용해 Kaspersky Industrial CyberSecurity for Nodes를 복구하여 이러한 작업에 대한 기본 검사 범위를 복원할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 온디맨드 검사 작업에 대한 검사 범위 구성

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
2. 작업 공간에서 **기기** 탭을 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. **작업** 섹션으로 갑니다.
5. **온디맨드 검사** 작업의 속성 창을 두 번 클릭하여 엽니다.
6. **검사 범위** 섹션을 선택합니다.
7. 검사 범위에 범위를 추가하려면 범위 옆의 확인란을 선택합니다.
8. 목록에 없는 검사 범위를 추가하려면:
   a. **추가** 버튼을 클릭합니다.
   b. 표시된 창에서 범위, 개별 디스크, 폴더, 네트워크 위치 등을 선택합니다.
   c. 검사 범위에 하위 폴더를 포함하려면 **하위 폴더 포함** 확인란을 선택합니다.
9. 검사 범위에서 개별 노드를 제외하려면 노드 이름 옆에 있는 확인란을 선택 해제합니다.
10. 검사 범위를 편집하려면 목록에서 검사 범위를 선택하고 **편집**을 클릭합니다.
11. 네트워크 파일 리소스 목록에서 이전에 추가한 검사 범위를 숨기려면 검사 범위를 선택하고 **삭제**를 클릭합니다.

    검사 범위를 네트워크 파일 리소스 목록에서 제거하면 온디맨드 검사 작업 범위에서 제외됩니다.

12. **확인**을 누릅니다.

검사 범위 설정 창이 닫힙니다. 새로 구성된 설정이 저장됩니다.

Kaspersky Security Center 웹 콘솔에서 온디맨드 검사 작업에 대한 검사 범위 구성

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)** 옵션을 선택합니다.
2. 작업을 구성할 컴퓨터 이름을 클릭합니다.

3. **작업** 섹션을 선택합니다.
4. 열린 창에서 **온디맨드 검사** 작업을 더블 클릭하여 속성을 엽니다.
5. **애플리케이션 설정** 탭을 선택합니다.
6. 검사 범위에 범위를 추가하려면 범위 옆의 스위치를 사용합니다.
7. 목록에 없는 검사 범위를 추가하려면:
   a. **추가** 버튼을 클릭합니다.
   b. 표시된 창에서 범위, 개별 디스크, 폴더, 네트워크 위치 등을 선택합니다.
   c. 검사 범위에 하위 폴더를 포함하려면 **하위 폴더** 확인란을 선택합니다.
8. 검사 범위에서 개별 노드를 제외하려면 노드 이름 옆에 있는 확인란을 선택 해제합니다.
9. 검사 범위를 편집하려면 목록에서 검사 범위를 선택하고 **범위 편집** 버튼을 클릭합니다.
10. 네트워크 파일 리소스 목록에서 이전에 추가한 검사 범위를 숨기려면 검사 범위를 선택하고 **삭제**를 클릭합니다.

    검사 범위를 네트워크 파일 리소스 목록에서 제거하면 온디맨드 검사 작업 범위에서 제외됩니다.

11. **저장** 버튼을 클릭합니다.

검사 범위 설정 창이 닫힙니다. 새로 구성된 설정이 저장됩니다.

애플리케이션 콘솔에서 온디맨드 검사 작업의 검사 범위 구성

1. 애플리케이션 콘솔 트리에서 **온디맨드 검사** 노드를 확장합니다.
2. 구성하려는 온디맨드 검사 작업에 해당하는 하위 노드를 선택합니다.
3. 선택한 노드의 결과 창에서 **보호 범위 구성** 링크를 클릭합니다.
4. 표시된 창에서 검사 범위에 범위를 추가하려면 옆에 있는 확인란을 선택합니다.
5. 목록에 없는 검사 범위를 추가하려면:
   a. **추가** 버튼을 클릭합니다.
   b. 표시된 창에서 범위, 개별 디스크, 폴더, 네트워크 위치 등을 선택합니다.
   c. 검사 범위에 하위 폴더를 포함하려면 **하위 폴더 포함** 확인란을 선택합니다.
6. 검사 범위에서 개별 노드를 제외하려면 노드 이름 옆에 있는 확인란을 선택 해제합니다.
7. 검사 범위를 편집하려면 목록에서 검사 범위를 선택하고 **범위 편집** 버튼을 클릭합니다.

8. 네트워크 파일 리소스 목록에서 이전에 추가한 검사 범위를 숨기려면 검사 범위를 선택하고 **삭제**를 클릭합니다.

   검사 범위를 네트워크 파일 리소스 목록에서 제거하면 온디맨드 검사 작업 범위에서 제외됩니다.

9. **확인** 버튼을 클릭합니다.

검사 범위 설정 창이 닫힙니다. 새로 구성된 설정이 저장됩니다.

온디맨드 검사 작업 설정 구성

Kaspersky Security Center 관리 콘솔에서 온디맨드 검사 작업을 구성하는 방법

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
2. 작업 공간에서 **기기** 탭을 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. **작업** 섹션으로 갑니다.
5. **온디맨드 검사** 작업의 속성 창을 두 번 클릭하여 엽니다.
6. **옵션** 섹션을 선택합니다.
7. **휴리스틱 분석 사용** 확인란을 선택하거나 선택 해제합니다.
8. 필요하다면 분석 레벨을 변경합니다.
9. 작업이 실행될 작업 프로세스에 *낮음* 우선순위를 할당하려면 **백그라운드 모드에서 작업 수행** 확인란을 선택합니다.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes 작업이 실행되는 작업 프로세스에는 *중간*(보통) 우선순위가 할당됩니다.

10. 작업을 *중요 영역 검사* 작업으로 사용하려면 **작업을 중요 영역 검사로 간주** 확인란을 선택합니다.
11. 컴퓨터 부하를 최적화하려면 **여러 검사 작업을 동시에 실행하지 않음** 확인란을 선택합니다.
12. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 온디맨드 검사 작업을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)** 옵션을 선택합니다.
2. 작업을 구성할 컴퓨터 이름을 클릭합니다.
3. **작업** 섹션을 선택합니다.

4. 열린 창에서 **온디맨드 검사** 작업을 더블 클릭하여 속성을 엽니다.
5. **애플리케이션 설정** 섹션을 선택합니다.
6. **설정** 섹션으로 갑니다.
7. **휴리스틱 분석 사용** 확인란을 선택하거나 선택 해제합니다.
8. 필요하다면 **휴리스틱 분석 레벨** 드롭다운 목록에서 분석 레벨을 선택합니다.
9. 작업이 실행될 작업 프로세스에 *낮음* 우선순위를 할당하려면 **컴퓨터가 유휴 상태일 때만 실행** 확인란을 선택합니다.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes 작업이 실행되는 작업 프로세스에는 *중간*(보통) 우선순위가 할당됩니다.

10. 작업을 *중요 영역 검사* 작업으로 사용하려면 **작업을 중요 영역 검사로 간주** 확인란을 선택합니다.
11. 컴퓨터 부하를 최적화하려면 **여러 검사 작업을 동시에 실행하지 않음** 확인란을 선택합니다.
12. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 온디맨드 검사 작업을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **온디맨드 검사** 노드를 확장합니다.
2. 구성하려는 온디맨드 검사 작업에 해당하는 하위 노드를 선택합니다.
3. 선택한 노드의 결과 창에서 **속성**을 클릭합니다.
4. **작업 설정** 탭을 선택합니다.
5. **휴리스틱 분석 사용** 확인란을 선택하거나 선택 해제합니다.
6. 필요하다면 분석 레벨을 변경합니다.
7. 작업이 실행될 작업 프로세스에 *낮음* 우선순위를 할당하려면 **백그라운드 모드에서 작업 수행** 확인란을 선택합니다.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes 작업이 실행되는 작업 프로세스에는 *중간*(보통) 우선순위가 할당됩니다.

8. 작업을 *중요 영역 검사* 작업으로 사용하려면 **작업을 중요 영역 검사로 간주** 확인란을 선택합니다.
9. 컴퓨터 부하를 최적화하려면 **여러 검사 작업을 동시에 실행하지 않음** 확인란을 선택합니다.
10. 변경 사항을 저장합니다.

이동식 드라이브 검사 구성

Kaspersky Security Center 관리 콘솔에서 이동식 드라이브 검사 구성

1. Kaspersky Security Center 관리 콘솔 트리의 **관리 중인 기기** 노드를 확장합니다.
2. 작업을 구성할 관리 그룹을 선택합니다.
3. **정책** 탭을 선택합니다.
4. 구성할 정책 이름을 더블클릭합니다.
   정책 속성 창에서 **보충** 섹션으로 갑니다.
5. **이동식 드라이브 검사** 하위 섹션에서 **설정** 버튼을 클릭합니다.
   이동식 드라이브 검사 창이 열립니다.
6. 다음을 수행합니다:
   - 이동식 드라이브가 연결될 때 Kaspersky Industrial CyberSecurity for Nodes가 자동으로 검사하도록 설정하려면 **USB를 통해 연결 시 이동식 드라이브 검사** 확인란을 선택합니다.
   - 필요하다면 **크기(MB)가 다음 이하이면 이동식 드라이브 검사** 옵션을 선택하고 오른쪽 필드에 최대값을 지정합니다.
   - **보안 레벨로 검사** 드롭다운 목록에서 이동식 드라이브 검사 작업에 사용할 설정으로 보안 레벨을 지정합니다.
7. **확인**을 누릅니다.

지정된 설정이 저장되고 적용됩니다.

Kaspersky Security Center 웹 콘솔에서 이동식 드라이브 검사 구성

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보충** 섹션으로 갑니다.
5. **이동식 드라이브 검사**의 **구성** 버튼을 클릭합니다.
   이동식 드라이브 검사 창이 열립니다.

6. 다음을 수행합니다:

   - 이동식 드라이브가 연결될 때 Kaspersky Industrial CyberSecurity for Nodes가 자동으로 검사하도록 설정하려면 **USB를 통해 연결 시 이동식 드라이브 검사** 확인란을 선택합니다.
   - 필요하다면 **크기(MB)가 다음 이하이면 이동식 드라이브 검사** 옵션을 선택하고 오른쪽 필드에 최대값을 지정합니다.
   - **보안 레벨로 검사** 드롭다운 목록에서 이동식 드라이브 검사 작업에 사용할 설정으로 보안 레벨을 지정합니다.

7. **확인**을 누릅니다.

지정된 설정이 저장되고 적용됩니다.

애플리케이션 콘솔에서 이동식 드라이브 검사 구성

1. **Kaspersky Industrial CyberSecurity for Nodes** 노드의 마우스 오른쪽 메뉴에 있는 애플리케이션 콘솔 트리에서 **이동식 드라이브 검사** 링크를 클릭합니다.

   이동식 드라이브 검사 창이 열립니다.

2. 다음을 수행합니다:

   - 이동식 드라이브가 연결될 때 Kaspersky Industrial CyberSecurity for Nodes가 자동으로 검사하도록 설정하려면 **USB를 통해 연결 시 이동식 드라이브 검사** 확인란을 선택합니다.
   - 필요하다면 **크기(MB)가 다음 이하이면 이동식 드라이브 검사** 옵션을 선택하고 오른쪽 필드에 최대값을 지정합니다.
   - **보안 레벨로 검사** 드롭다운 목록에서 이동식 드라이브 검사 작업에 사용할 설정으로 보안 레벨을 지정합니다.

3. **확인** 버튼을 클릭합니다.

온디맨드 검사 작업에 대해 사전 정의된 보안 레벨 선택

보호 중인 장치의 파일 리소스 목록에서 선택한 노드에 다음 사전 정의된 보안 레벨 세 가지 중 하나를 적용할 수 있습니다: **최대 성능**, **권장**, **최대 보호**.

Kaspersky Security Center 관리 콘솔에서 사전 정의된 보안 레벨 중 하나 선택

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
2. 작업 공간에서 **기기** 탭을 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. **작업** 섹션으로 갑니다.
5. **온디맨드 검사** 작업의 속성 창을 두 번 클릭하여 엽니다.
6. **검사 범위** 섹션을 선택합니다.

7. 보호 중인 장치 목록에서, 검사 범위에 포함된 항목을 선택하여 사전 정의된 보안 레벨을 설정합니다.

8. **구성** 버튼을 클릭합니다.

9. 열린 창에서 **보안 레벨** 탭에서 적용할 보안 레벨을 선택합니다.

10. **확인** 버튼을 클릭합니다.

11. **속성의 온디맨드 검사** 창에서 **확인** 버튼을 클릭합니다.

구성된 작업 설정이 저장되고 실행 중인 작업에 즉시 적용됩니다. 작업이 실행되지 않는 경우 다음 시작 시 수정된 설정이 적용됩니다.

애플리케이션 콘솔에서 사전 정의된 보안 레벨 중 하나 선택

1. 애플리케이션 콘솔 트리에서 **온디맨드 검사** 노드를 확장합니다.

2. 구성하려는 온디맨드 검사 작업에 해당하는 하위 노드를 선택합니다.

3. 선택한 노드의 결과 창에서 **보호 범위 구성**을 클릭합니다.

4. 보호 중인 장치의 네트워크 파일 리소스 목록에서 사전 정의된 보안 레벨을 설정할 노드 또는 항목을 선택합니다.

5. 선택한 노드나 항목이 검사 범위에 포함되는지 확인합니다.

6. **구성** 버튼을 클릭합니다.

7. 열린 창에서 원하는 보안 레벨을 선택합니다.
   선택한 보안 레벨에 해당하는 보안 설정 목록이 표시됩니다.

8. **확인** 버튼을 클릭합니다.

작업 설정이 저장되고 실행 중인 작업에 즉시 적용됩니다. 작업이 실행되지 않는 경우 다음 시작 시 수정된 설정이 적용됩니다.

보안 설정 수동 구성

기본적으로 온디맨드 검사 작업에서는 전체 검사 범위에 공통 보안 설정을 사용합니다.

이 설정은 **권장** 사전 설정된 보안 레벨에 해당합니다.

전체 검사 범위에 공통 기본값 설정 구성하거나 보호 중인 장치의 파일 리소스 목록이나 트리의 노드마다 별도의 설정을 구성하는 방법으로 보안 설정의 기본값을 수정할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 보안 설정 수동 관리

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.

2. 작업 공간에서 **기기** 탭을 선택합니다.

3. 더블 클릭해 컴퓨터 속성 창을 엽니다.

4. **작업** 섹션으로 갑니다.
5. **온디맨드 검사** 작업의 속성 창을 두 번 클릭하여 엽니다.
6. **검사 범위** 섹션을 선택합니다.
7. 보호 중인 장치 목록에서 보안 설정을 관리할 검사의 범위에 포함된 항목을 선택합니다.
8. **구성** 버튼을 클릭합니다.
9. 열린 창에서 **보안 레벨** 탭에서 적용할 보안 레벨을 선택합니다.
10. 보안 설정을 구성할 리소스를 선택합니다.
11. **구성** 버튼을 클릭합니다.
12. 창이 열리면 필요한 보안 레벨을 선택하고 **설정** 버튼을 클릭합니다.
13. **일반** 탭에서 다음 설정을 지정합니다:
    - 보호 범위에 포함해야 하는 개체:
      - **모든 개체**. Kaspersky Industrial CyberSecurity for Nodes가 모든 개체를 검사합니다.
      - **형식에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 형식을 기준으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 형식 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
      - **안티 바이러스 데이터베이스에 지정된 확장자 목록으로 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 확장자 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
      - **지정된 확장자 목록에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. 확장자 목록은 사용자가 직접 지정합니다.
    - **최적화** 블록에서 **새로운 파일과 수정된 파일만 보호** 확인란을 선택하거나 선택 해제합니다.
    - **복합 파일 검사** 섹션에서 검사 범위에 포함할 복합 개체를 지정합니다:
      - **압축파일 검사**
      - **배포 패키지 검사**
      - **Microsoft Office 형식 파일 검사**
      - **이메일 형식 파일 검사**
14. **동작** 탭에서 다음 설정을 지정합니다:
    - 감염 및 기타 탐지된 개체에 수행할 동작을 선택합니다:
      - **치료**
      - **치료 - 불가능한 경우 삭제**

- **삭제**
- **권장**
- **알림**

- 탐지한 개체 유형에 따라 개체에 수행할 동작을 구성합니다:

  a. **선택한 개체 유형에 동작 적용** 확인란을 선택 해제하거나 선택합니다.

  b. **설정** 버튼을 클릭하고 탐지할 개체의 유형을 선택합니다.

- 수정할 수 없는 복합 파일에 대한 동작을 구성합니다. **내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거** 확인란을 선택 해제하거나 선택합니다.

15. **최적화** 탭에서 다음 설정을 지정합니다:

- **예외 규칙** 블록에서:
  - **파일 예외** 확인란을 선택 해제하거나 선택합니다.
  - **유형 기준으로 개체 탐지 안 함** 확인란을 선택 해제하거나 선택합니다.
    각 설정의 **편집** 버튼을 클릭해 예외를 추가합니다.
- **고급 설정** 블록에서:
  - **검사 시간이 다음을 초과하면 검사 중지(초)**
  - **다음을 초과하는 복합 파일은 검사하지 않음(MB)**
  - **iSwift 기술 사용**
  - **iChecker 기술 사용**

16. 새 보안 설정을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 보안 설정 수동 관리

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.
2. 작업을 구성할 컴퓨터 이름을 클릭합니다.
3. **작업** 섹션을 선택합니다.
4. 열린 창에서 **온디맨드 검사** 작업을 더블 클릭하여 속성을 엽니다.
5. **애플리케이션 설정** 섹션을 선택합니다.
6. **검사 범위** 섹션으로 갑니다.
7. 보호 중인 장치의 네트워크 파일 리소스 목록에서 보안 설정을 관리할 항목을 선택합니다. 선택한 항목이 검사 범위에 포함되어 있는지 확인합니다.
8. **편집** 버튼을 클릭합니다.

9. 드롭다운 목록에서 개체 보호 모드를 선택합니다.

   - **모든 개체**. Kaspersky Industrial CyberSecurity for Nodes가 모든 개체를 검사합니다.
   - **형식에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 형식을 기준으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 형식 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
   - **안티 바이러스 데이터베이스에 지정된 확장자 목록으로 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 확장자 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
   - **지정된 확장자 목록에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. 확장자 목록은 사용자가 직접 지정합니다.

10. **새로운 파일과 수정된 파일만 보호** 확인란을 선택하거나 선택 해제하고 검사에서 하위 폴더 포함 여부를 지정합니다.

11. 복합 개체 보호 설정 관리:

    - **압축파일 검사**
    - **배포 패키지 검사**
    - **Microsoft Office 형식 파일 검사**
    - **이메일 형식 파일 검사**

12. 감염 및 기타 탐지된 개체에 수행할 동작을 선택합니다:

    - **치료**
    - **치료 - 불가능한 경우 삭제**
    - **삭제**
    - **권장**
    - **알림**

13. 탐지한 개체 유형에 따라 개체에 수행할 동작을 구성합니다:

    a. **선택한 개체 유형에 동작 적용** 확인란을 선택 해제하거나 선택합니다.

    b. **설정** 버튼을 클릭하고 탐지할 개체의 유형을 선택합니다.

14. 수정할 수 없는 복합 파일에 대한 동작을 구성합니다. **내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거** 확인란을 선택 해제하거나 선택합니다.

15. **예외 규칙** 블록에서:

    - **파일 예외** 확인란을 선택 해제하거나 선택합니다.
    - **유형 기준으로 개체 탐지 안 함** 확인란을 선택 해제하거나 선택합니다.

16. **키 추가** 블록에서:

- **검사 시간이 다음을 초과하면 검사 중지(초)**
- **다음을 초과하는 복합 파일은 검사하지 않음(MB)**
- **iSwift 기술 사용**
- **iChecker 기술 사용**

17. 새 보안 설정을 저장합니다.

애플리케이션 콘솔에서 보안 설정 수동 관리

1. 애플리케이션 콘솔 트리에서 **온디맨드 검사** 노드를 확장합니다.
2. 구성하려는 온디맨드 검사 작업에 해당하는 하위 노드를 선택합니다.
3. 선택한 노드의 결과 창에서 **보호 범위 구성**을 클릭합니다.
4. 보호 중인 장치의 네트워크 파일 리소스 목록에서 보안 설정을 관리할 항목을 선택합니다.
5. 선택한 항목이 검사 범위에 포함되어 있는지 확인합니다.
6. **구성** 버튼을 클릭합니다.
7. 창이 열리면 필요한 보안 레벨을 선택하고 **설정** 버튼을 클릭합니다.
8. **일반** 탭에서 다음 설정을 지정합니다:
   - 보호 범위에 포함해야 하는 개체:
     - **모든 개체**. Kaspersky Industrial CyberSecurity for Nodes가 모든 개체를 검사합니다.
     - **형식에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 형식을 기준으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 형식 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
     - **안티 바이러스 데이터베이스에 지정된 확장자 목록으로 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. Kaspersky는 확장자 목록을 컴파일합니다. 이는 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
     - **지정된 확장자 목록에 따라 검사한 개체**. Kaspersky Industrial CyberSecurity for Nodes가 파일 확장자를 기반으로 감염 가능성이 있는 개체만 검사합니다. 확장자 목록은 사용자가 직접 지정합니다.
   - **최적화** 블록에서 **새로운 파일과 수정된 파일만 보호** 확인란을 선택하거나 선택 해제합니다.
   - **복합 파일 검사** 섹션에서 검사 범위에 포함할 복합 개체를 지정합니다:
     - **압축파일 검사**
     - **배포 패키지 검사**

- **Microsoft Office 형식 파일 검사**
- **이메일 형식 파일 검사**

9. **동작** 탭에서 다음 설정을 지정합니다:

- 감염 및 기타 탐지된 개체에 수행할 동작을 선택합니다:
  - **치료**
  - **치료 - 불가능한 경우 삭제**
  - **삭제**
  - **권장**
  - **알림**
- 탐지한 개체 유형에 따라 개체에 수행할 동작을 구성합니다:
  a. **선택한 개체 유형에 동작 적용** 확인란을 선택 해제하거나 선택합니다.
  b. **설정** 버튼을 클릭하고 탐지할 개체의 유형을 선택합니다.
- 수정할 수 없는 복합 파일에 대한 동작을 구성합니다. **내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거** 확인란을 선택 해제하거나 선택합니다.

10. **최적화** 탭에서 다음 설정을 지정합니다:

- **예외 규칙** 블록에서:
  - **파일 예외** 확인란을 선택 해제하거나 선택합니다.
  - **유형 기준으로 개체 탐지 안 함** 확인란을 선택 해제하거나 선택합니다.

  각 설정의 **편집** 버튼을 클릭해 예외를 추가합니다.
- **고급 설정** 블록에서:
  - **검사 시간이 다음을 초과하면 검사 중지(초)**
  - **다음을 초과하는 복합 파일은 검사하지 않음(MB)**
  - **iSwift 기술 사용**
  - **iChecker 기술 사용**

11. 새 보안 설정을 저장합니다.

온디맨드 검사 작업 통계

온디맨드 검사 작업이 실행되는 동안 Kaspersky Industrial CyberSecurity for Nodes를 시작한 후 지금까지 이 애플리케이션이 처리한 개체 수에 대한 정보를 볼 수 있습니다.

작업이 일시 중지된 경우에도 이 정보를 사용할 수 있습니다. 작업 로그에서 작업 통계를 볼 수 있습니다.

온디맨드 검사 작업 통계를 보려면:

1. 애플리케이션 콘솔 트리에서 **온디맨드 검사** 노드를 확장합니다.
2. 통계를 보려는 온디맨드 검사 작업을 선택합니다.

   선택한 노드의 결과 창에 있는 **통계** 섹션에 작업 통계가 표시됩니다.

Kaspersky Industrial CyberSecurity for Nodes가 시작된 이후 처리된 개체에 대한 정보는 아래 표에 나와 있습니다.

온디맨드 검사 작업 통계

필드	설명
탐지	Kaspersky Industrial CyberSecurity for Nodes에서 탐지한 개체의 수입니다. 예를 들어 Kaspersky Industrial CyberSecurity for Nodes가 5개 파일에서 하나의 악성 개체를 탐지한 경우 이 필드 값이 1증가합니다.
감염된 개체 및 기타 개체	Kaspersky Industrial CyberSecurity for Nodes가 발견하고 감염으로 분류한 개체 수 또는 검사 범위에서 제외되지 않았지만 침입자가 사용하여 장치나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어로 분류된 합법적인 소프트웨어 파일의 수입니다.
치료되지 않은 개체	Kaspersky Industrial CyberSecurity for Nodes가 다음의 이유로 치료하지 않은 개체 수입니다. • 탐지된 개체는 치료할 수 없는 유형입니다. • 바이러스 치료 중 오류 발생.
치료된 개체	Kaspersky Industrial CyberSecurity for Nodes에서 치료한 개체의 수입니다.
삭제된 개체	Kaspersky Industrial CyberSecurity for Nodes가 삭제한 개체의 수입니다.
검사되지 않은 개체	보호 범위에 속하지만 다른 애플리케이션의 개체 접근 차단과 같은 이유로 Kaspersky Industrial CyberSecurity for Nodes가 검사하지 못한 개체 수입니다.
압축 파일	Kaspersky Industrial CyberSecurity for Nodes에서 검사한 압축 파일의 수입니다.
압축된 개체	Kaspersky Industrial CyberSecurity for Nodes에서 검사한 실행 압축 개체의 수입니다.
암호로 보호된 개체	암호로 보호되어 Kaspersky Industrial CyberSecurity for Nodes에서 검사하지 못한 개체(예: 압축파일) 수입니다.
손상된 개체	손상된 형식으로 Kaspersky Industrial CyberSecurity for Nodes가 건너뛴 개체의 수입니다.
처리 오류	처리 중에 오류가 발생한 개체 수입니다.
삭제되지 않은 개체	다른 애플리케이션의 개체 접근 차단 등의 이유로 Kaspersky Industrial CyberSecurity for Nodes의 삭제 시도가 실패한 개체 수입니다.
개체 처리 안 됨	Kaspersky Industrial CyberSecurity for Nodes에서 처리하지 않은 총 개체 수입니다.

결과 창의 **관리** 섹션에서 **작업 로그 열기** 링크를 클릭해 선택한 작업 로그에서 온디맨드 검사 작업 통계를 볼 수도 있습니다.

작업 완료 시 작업 로그의 **이벤트** 탭에 기록된 이벤트를 수동으로 처리할 것을 권장합니다.

산업 네트워크 보호

이 섹션에서는 프로그래밍 가능한 논리 컨트롤러 프로젝트(이하 "PLC 프로젝트") 조사 및 무결성 검사 작업을 설명하고 구성 방법에 대한 지침을 제공합니다.

PLC 프로젝트 무결성 검사 정보

이 기능은 산업 시스템에서 사용되는 PLC 프로젝트의 무결성을 검사하도록 설계되었습니다.

PLC 프로젝트는 PLC용으로 작성된 마이크로 프로그램입니다. PLC 프로젝트는 PLC의 메모리에 저장되며 PLC를 사용하는 생산 프로세스의 일부로 실행됩니다.

PLC 프로젝트 무결성 검사를 사용하려면 Kaspersky Industrial CyberSecurity for Nodes가 설치된 보호 중인 장치 네트워크에서 PLC에 접근할 수 있어야 합니다.

이 기능을 사용하기 전에 다음 준비 작업을 수행합니다.

1. 애플리케이션 콘솔**PLC 프로젝트 조사** 로컬 작업을 을 사용하여 PLC 프로젝트에 대한 정보를 가져옵니다.
2. 애플리케이션 콘솔 **PLC 프로젝트 무결성 검사** 로컬 작업 설정에서, 이전 단계에서 얻은 프로젝트 목록에서 PLC 참조 프로젝트를 나타냅니다.

PLC 프로젝트 무결성 검사 작업에서 PLC 프로젝트에 대한 정보를 보려면:

정책 속성에서 **중앙 관리 서버와 상호 작용** 창을 열고 **PLC 프로젝트의 버전** 확인란을 선택하여 중앙 관리 서버로의 데이터 전송을 구성합니다.

PLC 프로젝트 무결성 검사 로컬 작업이 시작된 후에 PLC 참조 프로젝트를 기준으로 PLC 프로젝트가 변경되면 애플리케이션이 경고를 표시합니다.

PLC 프로젝트 무결성 검사는 기본적으로 비활성화되어 있습니다.

리포트

보고는 Kaspersky Security Center 중앙 관리 서버의 기본 기능 중 하나입니다. 이 기능은 Kaspersky Security Center의 관리 콘솔을 통해서만 사용할 수 있습니다.

PLC 프로젝트 무결성 검사 작업이 완료된 후에는 다음 정보가 포함된 리포트를 생성하고 검토할 수 있습니다:

- *PLC 프로젝트 무결성 검사*가 완료된 컴퓨터 이름.
- 무결성을 모니터링하는 PLC.
- 마지막 검사 날짜.
- 무결성 검사 결과.

Kaspersky Security Center 중앙 관리 서버에서 리포트를 생성하려면,

리포트 탭을 열고 **PLC(Programmable Logic Controller) 무결성 검사 리포트**를 선택합니다.

리포트 생성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

PLC 프로젝트 무결성 검사 작업 구성

이 섹션에서는 PLC 프로젝트 제어 작업의 일반 설정 구성을 위한 지침을 제공합니다.

PLC 프로젝트 조사 구성

PLC 프로젝트 무결성 검사를 실행하기 전에 현재 산업 네트워크에서 사용되는 PLC 프로젝트에 대한 정보를 받아야 합니다. PLC 프로젝트에 대한 정보는 *PLC 프로젝트 조사* 로컬 작업을 사용하여 얻습니다.

Kaspersky Security Center 관리 콘솔에서 PLC 프로젝트 조사 구성

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
2. 작업 공간에서 **기기** 탭을 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. **작업** 섹션으로 갑니다.
5. 창이 열리면 **PLC 프로젝트 조사** 작업을 선택하고 **속성** 버튼을 클릭합니다.
   속성: PLC 프로젝트 조사 창이 열립니다.
6. **설정** 섹션으로 가서 **작업 설정** 탭의 **PLC 레지스트리에서 추가** 버튼을 클릭합니다.
   PLC 레지스트리 관리 5.0.0 창이 열립니다.
7. **추가** 버튼을 클릭합니다.
8. **일반 설정**에서 PLC 구성 이름을 입력하고 **PLC 유형** 드롭다운 목록에서 PLC 유형을 선택합니다.
   PLC 유형은 PLC 제조업체에서 제공하는 모델 및 시리즈를 나타냅니다.
9. **설명** 필드에 PLC 설명을 입력합니다.
   애플리케이션은 *PLC 프로젝트 조사* 작업을 실행하는 동안 얻은 새 버전의 각 PLC 펌웨어에 지정된 설명을 링크합니다.
10. **연결 대기** 필드에서 대기 시간 값(초)을 지정합니다.
11. 선택한 PLC 유형에 따라 **연결 설정**에서 다음 필드를 작성합니다: **IP 주소**, **포트**, **랙, Telnet 포트, 컨트롤러 가상 주소**, **슬롯**.

12. PLC에 대한 연결을 보호하려면 선택한 PLC 유형에 따라 인증 방법을 선택합니다.

    - **암호**.

      이 확인란을 선택하면 애플리케이션이 사용자가 PLC에 연결할 때 지정한 암호를 사용하여 쿼리합니다.

      이 확인란을 선택 해제하면 애플리케이션이 암호를 사용하지 않고 PLC에 연결합니다. 기본적으로 확인란의 선택이 취소됩니다.

      > 이 확인란은 PLC 연결을 위해 새 암호를 할당하지 않습니다. 암호는 PLC 측에서 설정해야 합니다.

    - **컨트롤러에 인증 사용**.

13. **데이터 블록 읽기** 확인란을 선택하거나 선택 해제합니다.

    이 확인란을 선택하면 애플리케이션이 PLC 프로젝트 체크섬을 계산할 때 데이터 블록을 고려합니다. 검사 보안 레벨 개선을 위해 데이터 블록에 통계 값만 포함된 경우, 이 확인란을 선택하는 것이 좋습니다.

    이 확인란을 선택 해제하면 애플리케이션이 데이터 블록을 고려하지 않습니다. *PLC 프로젝트 무결성 검사* 작업에서 오탐을 방지하기 위해 데이터 블록에 동적 값이 포함되어 있으면, 확인란을 선택하지 않는 것이 좋습니다. 선택한 PLC 프로젝트는 참조 프로젝트와 비교됩니다.

    기본적으로 확인란의 선택이 취소됩니다.

14. **확인** 버튼을 클릭합니다.

    > 중복 컨트롤러는 지원하지 않습니다.

    추가된 PLC 구성은 **작업 설정** 탭에 표시됩니다.

15. Kaspersky Industrial CyberSecurity for Nodes 콘솔이 설치된 로컬 컴퓨터에서 *PLC 프로젝트 조사* 작업이 완료된 후 수신된 PLC 구성을 추가하려면:

    a. PLC 구성 목록에서 PLC 레지스트리에 추가할 구성을 선택합니다.

    b. **PLC 레지스트리 링크** 버튼을 클릭합니다.

    > 레지스트리의 각 PLC 구성에는 고유한 ID 번호가 마지막 열에 지정되어 있습니다. 로컬 컴퓨터 작업의 PLC 구성을 PLC 레지스트리에 추가하면 이 구성에 ID 번호가 할당됩니다.

16. 선택한 PLC 구성을 작업 목록에서 삭제하려면 **삭제** 버튼을 클릭합니다.

    > PLC 구성은 PLC 레지스트리에서 삭제되지 않으며 언제든지 다시 추가할 수 있습니다.

17. 변경 사항을 저장합니다.

PLC 프로젝트 조사 작업을 실행하여 얻은 PLC 프로젝트 정보는 PLC 참조 프로젝트 선택 및 *PLC 프로젝트 무결성 검사* 작업 구성에 사용됩니다.

Kaspersky Security Center 웹 콘솔에서 PLC 프로젝트 조사 구성

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.
2. *PLC 프로젝트 조사* 작업을 구성할 컴퓨터 이름을 클릭합니다.
3. **작업** 탭을 선택합니다.
4. 열린 창에서 **PLC 프로젝트 조사** 작업을 더블 클릭하여 속성을 엽니다.
5. **애플리케이션 설정** 탭을 선택하고 **PLC 레지스트리에서 추가** 버튼을 클릭합니다.
   PLC 구성 창이 열립니다.
6. **PLC 설정** 섹션의 **PLC 유형** 드롭다운 목록에서 PLC 유형을 선택합니다.
   PLC 유형은 PLC 제조업체에서 제공하는 모델 및 시리즈를 나타냅니다.
7. **설명** 필드에 PLC 설명을 입력합니다.
   애플리케이션은 *PLC 프로젝트 조사* 작업을 실행하는 동안 얻은 새 버전의 각 PLC 펌웨어에 지정된 설명을 링크합니다.
8. **연결 시간 초과(초)** 필드에서 대기 시간 값(초)을 지정합니다.
9. **연결 설정** 섹션에서 선택한 PLC 유형에 따라 다음 필드를 작성합니다: **컨트롤러 주소**, **포트**, **랙, Telnet 포트, 컨트롤러 가상 주소**, **슬롯**.
10. PLC에 대한 연결을 보호하려면 선택한 PLC 유형에 따라 인증 방법을 선택합니다.
    - **암호 적용**.
      이 확인란을 선택하면 애플리케이션이 사용자가 PLC에 연결할 때 지정한 암호를 사용하여 쿼리합니다.
      이 확인란을 선택 해제하면 애플리케이션이 암호를 사용하지 않고 PLC에 연결합니다. 기본적으로 확인란의 선택이 취소됩니다.

      > 이 확인란은 PLC 연결을 위해 새 암호를 할당하지 않습니다. 암호는 PLC 측에서 설정해야 합니다.

    - **컨트롤러에 인증 사용**.
11. **데이터 블록 읽기** 확인란을 선택하거나 선택 해제합니다.
    이 확인란을 선택하면 애플리케이션이 PLC 프로젝트 체크섬을 계산할 때 데이터 블록을 고려합니다. 검사 보안 레벨 개선을 위해 데이터 블록에 통계 값만 포함된 경우, 이 확인란을 선택하는 것이 좋습니다.
    이 확인란을 선택 해제하면 애플리케이션이 데이터 블록을 고려하지 않습니다. *PLC 프로젝트 무결성 검사* 작업에서 오탐을 방지하기 위해 데이터 블록에 동적 값이 포함되어 있으면, 확인란을 선택하지 않는 것이 좋습니다. 선택한 PLC 프로젝트는 참조 프로젝트와 비교됩니다.
    기본적으로 확인란의 선택이 취소됩니다.
12. **확인** 버튼을 클릭합니다.

> 중복 컨트롤러는 지원하지 않습니다.

추가된 PLC 구성은 **애플리케이션 설정** 탭에 표시됩니다.

13. Kaspersky Industrial CyberSecurity for Nodes 콘솔이 설치된 로컬 컴퓨터에서 *PLC 프로젝트 조사* 작업이 완료된 후 수신된 PLC 구성을 추가하려면:

    a. PLC 구성 목록에서 PLC 레지스트리에 추가할 구성을 선택합니다.

    b. **PLC 레지스트리 링크** 버튼을 클릭합니다.

    > 레지스트리의 각 PLC 구성에는 고유한 ID 번호가 마지막 열에 지정되어 있습니다. 로컬 컴퓨터 작업의 PLC 구성을 PLC 레지스트리에 추가하면 이 구성에 ID 번호가 할당됩니다.

14. 선택한 PLC 구성을 작업 목록에서 삭제하려면 **삭제** 버튼을 클릭합니다.

    > PLC 구성은 PLC 레지스트리에서 삭제되지 않으며 언제든지 다시 추가할 수 있습니다.

15. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 PLC 프로젝트 조사 구성

1. 애플리케이션 콘솔 트리에서 **산업 네트워크 보호** 노드를 확장합니다.
2. **PLC 프로젝트 조사** 하위 노드를 선택합니다.
3. **PLC 프로젝트 조사** 노드의 세부 정보 창에서 **속성** 링크를 클릭합니다.
   속성: PLC 프로젝트 조사 창이 열립니다.
4. **작업 설정** 탭에서 **추가** 버튼을 클릭합니다.
   PLC 구성 창이 열립니다.
5. **PLC 유형** 드롭다운 목록의 **일반 설정**에서 PLC 유형을 선택합니다.
   PLC 유형은 PLC 제조업체에서 제공하는 모델 및 시리즈를 나타냅니다.
6. **설명** 필드에 PLC 설명을 입력합니다.
   애플리케이션은 *PLC 프로젝트 조사* 작업을 실행하는 동안 얻은 새 버전의 각 PLC 펌웨어에 지정된 설명을 링크합니다.
7. **연결 대기** 필드에서 대기 시간 값(초)을 지정합니다.
8. 선택한 PLC 유형에 따라 **연결 설정**에서 다음 필드를 작성합니다: **IP 주소**, **포트**, **랙, Telnet 포트, 컨트롤러 가상 주소**, **슬롯**.
9. PLC에 대한 연결을 보호하려면 선택한 PLC 유형에 따라 인증 방법을 선택합니다.

   - **암호**.
     이 확인란을 선택하면 애플리케이션이 사용자가 PLC에 연결할 때 지정한 암호를 사용하여 쿼리합니다.
     이 확인란을 선택 해제하면 애플리케이션이 암호를 사용하지 않고 PLC에 연결합니다. 기본적으로 확인란의 선택이 취소됩니다.

이 확인란은 PLC 연결을 위해 새 암호를 할당하지 않습니다. 암호는 PLC 측에서 설정해야 합니다.

- **컨트롤러에 인증 사용**.

10. **데이터 블록 읽기** 확인란을 선택하거나 선택 해제합니다.

    이 확인란을 선택하면 애플리케이션이 PLC 프로젝트 체크섬을 계산할 때 데이터 블록을 고려합니다. 검사 보안 레벨 개선을 위해 데이터 블록에 통계 값만 포함된 경우, 이 확인란을 선택하는 것이 좋습니다.

    이 확인란을 선택 해제하면 애플리케이션이 데이터 블록을 고려하지 않습니다. *PLC 프로젝트 무결성 검사* 작업에서 오탐을 방지하기 위해 데이터 블록에 동적 값이 포함되어 있으면, 확인란을 선택하지 않는 것이 좋습니다. 선택한 PLC 프로젝트는 참조 프로젝트와 비교됩니다.

    기본적으로 확인란의 선택이 취소됩니다.

11. **확인** 버튼을 클릭합니다.

    중복 컨트롤러는 지원하지 않습니다.

    추가된 PLC 구성은 **작업 설정** 탭에 표시됩니다.

12. 선택한 PLC 구성을 작업 목록에서 삭제하려면 **삭제** 버튼을 클릭합니다.

    PLC 구성은 PLC 레지스트리에서 삭제되지 않으며 언제든지 다시 추가할 수 있습니다.

13. 변경 사항을 저장합니다.

PLC 프로젝트 조사 작업을 실행하여 얻은 PLC 프로젝트 정보는 PLC 참조 프로젝트 선택 및 *PLC 프로젝트 무결성 검사* 작업 구성에 사용됩니다.

PLC 프로젝트 무결성 검사 구성

Kaspersky Security Center 관리 콘솔에서 PLC 프로젝트 무결성 검사 구성

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
2. 작업 공간에서 **장치** 탭을 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. **작업** 섹션으로 갑니다.
5. 창이 열리면 **PLC 프로젝트 무결성 검사** 작업을 선택하고 **속성** 버튼을 클릭합니다.

   속성: PLC 프로젝트 무결성 검사 창이 열립니다.
6. **설정** 섹션으로 갑니다.
7. 열린 창에서 **추가** 버튼을 클릭해 *PLC 프로젝트 무결성 검사* 작업을 실행할 구성을 목록에 추가합니다.

   PLC 프로젝트 무결성 검사용 데이터 창이 열립니다.

이 창에 있는 모든 정보는 Kaspersky Security Center의 *PLC 프로젝트 조사* 작업을 실행한 결과로 얻은 것입니다.

8. **PLC 유형** 드롭다운 목록에서 프로젝트 무결성을 확인할 PLC 유형을 선택합니다.

9. 목록에서 선택한 PLC 유형에 대한 구성을 선택하고 PLC 프로젝트의 참조 버전을 지정합니다. 애플리케이션은 PLC 참조 프로젝트의 설정과 비교한 결과를 기반으로 PLC 프로젝트의 무결성에 관한 결론을 내립니다.

10. **PLC 프로젝트 무결성 검사용 데이터** 창에서 **확인** 버튼을 클릭하여 변경 사항을 저장합니다. PLC 프로젝트 정보가 작업에 추가됩니다.

11. **속성: PLC 프로젝트 무결성 검사** 창의 목록에서 추가된 PLC 구성을 선택합니다.

    - **PLC 구성** 탭에는 PLC 프로젝트의 해시에 관한 정보와 해시를 받은 날짜가 표시됩니다.
    - **PLC 프로젝트의 참조 버전** 탭에는 PLC 구성에 대한 상세 정보가 포함되어 있습니다.

12. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 PLC 프로젝트 무결성 검사 구성

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.

2. *PLC 프로젝트 무결성 검사* 작업을 구성할 컴퓨터 이름을 클릭합니다.

3. **작업** 섹션을 선택합니다.

4. 열린 창에서 **PLC 프로젝트 무결성 검사** 작업을 더블 클릭하여 속성을 엽니다.

5. **애플리케이션 설정** 탭을 선택하고 **추가** 버튼을 클릭합니다.

   PLC 프로젝트 무결성 검사용 데이터 창이 열립니다.

   이 창에 있는 모든 정보는 Kaspersky Security Center의 *PLC 프로젝트 조사* 작업을 실행한 결과로 얻은 것입니다.

6. **PLC 구성을 선택하십시오** 버튼을 클릭해 PLC 구성을 선택합니다.

7. 애플리케이션이 PLC 프로젝트에 대한 정보를 요청할 때 준수할 시간 간격을 선택합니다.

8. **참조 PLC 프로젝트 선택** 버튼을 클릭하고 PLC 프로젝트의 참조 버전을 지정합니다. 애플리케이션은 PLC 참조 프로젝트의 설정과 비교한 결과를 기반으로 PLC 프로젝트의 무결성에 관한 결론을 내립니다.

9. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

10. 목록에서 추가된 PLC 구성을 선택합니다.

11. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 PLC 프로젝트 무결성 검사 구성

1. 애플리케이션 콘솔 트리에서 **산업 네트워크 보호** 노드를 확장합니다.

2. **PLC 프로젝트 무결성 검사** 하위 노드를 선택합니다.

3. **PLC 프로젝트 무결성 검사** 노드의 세부 정보 창에서 **속성** 링크를 클릭합니다.

   스케줄 및 실행 모드 창이 열립니다.

4. 창이 열리면 다음 설정을 구성합니다.

   - 작업 스케줄 설정 관리.
   - 필요한 경우 **사용자 계정으로 작업 실행** 기능을 활성화하고 작업 실행에 사용할 사용자 계정의 사용자 이름과 암호를 지정합니다.

5. **PLC 프로젝트 무결성 검사** 노드의 결과 창에서 **보호 범위 구성** 링크를 클릭합니다.

6. 열린 창에서 **추가** 버튼을 클릭해 *PLC 프로젝트 무결성 검사* 작업을 실행할 구성을 목록에 추가합니다.

   PLC 프로젝트 무결성 검사용 데이터 창이 열립니다. 이 창에 있는 모든 정보는 Kaspersky Security Center의 *PLC 프로젝트 조사* 작업을 실행한 결과로 얻은 것입니다.

7. **PLC 유형** 드롭다운 목록에서 프로젝트 무결성을 확인할 PLC 유형을 선택합니다.

8. 목록에서 선택한 PLC 유형에 대한 구성을 선택하고 PLC 프로젝트의 참조 버전을 지정합니다. 애플리케이션은 PLC 참조 프로젝트의 설정과 비교한 결과를 기반으로 PLC 프로젝트의 무결성에 관한 결론을 내립니다.

9. **PLC 프로젝트 무결성 검사용 데이터** 창에서 **확인** 버튼을 클릭하여 변경 사항을 저장합니다. PLC 프로젝트 정보가 작업에 추가됩니다.

10. **속성: PLC 프로젝트 무결성 검사** 창의 목록에서 추가된 PLC 구성을 선택합니다.

    - **PLC 구성** 탭에는 PLC 프로젝트의 해시에 관한 정보와 해시를 받은 날짜가 표시됩니다.
    - **PLC 프로젝트의 참조 버전** 탭에는 PLC 구성에 대한 상세 정보가 포함되어 있습니다.

11. 변경 사항을 저장합니다.

PLC 프로젝트 무결성 검사 활성화 및 비활성화

PLC 프로젝트 무결성 검사 작업은 Kaspersky Industrial CyberSecurity for Nodes가 *PLC 프로젝트 조사* 작업을 사용하여 펌웨어 정보를 받은 후에만 실행됩니다.

Kaspersky Security Center 관리 콘솔에서 PLC 프로젝트 무결성 검사 활성화 또는 비활성화

1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
2. 작업 공간에서 **장치** 탭을 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. **작업** 섹션으로 갑니다.
5. 창이 열리면 **PLC 프로젝트 조사** 작업을 선택하고 다음 동작 중 하나를 수행합니다.

   - PLC 프로젝트 무결성 검사를 활성화하려면 작업의 마우스 오른쪽 메뉴에서 **시작**를 선택합니다.

     PLC 프로젝트 무결성 검사 작업이 시작됩니다.

- PLC 프로젝트 무결성 검사를 비활성화하려면, 작업의 마우스 오른쪽 메뉴에서 **중지**를 선택합니다.
  PLC 프로젝트 무결성 검사 작업이 중지됩니다.

Kaspersky Security Center 웹 콘솔에서 PLC 프로젝트 무결성 검사 활성화 또는 비활성화

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.
2. *PLC 프로젝트 무결성 검사* 작업을 구성할 컴퓨터 이름을 클릭합니다.
3. **작업** 탭을 선택합니다.
4. **PLC 프로젝트 조사** 작업 옆의 확인란을 선택하고 다음 중 하나를 수행합니다.
   - PLC 프로젝트 무결성 검사를 활성화하려면 **시작** 버튼을 클릭합니다.
     PLC 프로젝트 무결성 검사 작업이 시작됩니다.
   - PLC 프로젝트 무결성 검사를 비활성화하려면 **중지** 버튼을 클릭합니다.
     PLC 프로젝트 무결성 검사 작업이 중지됩니다.

애플리케이션 콘솔에서 PLC 프로젝트 무결성 검사 활성화 또는 비활성화

1. 애플리케이션 콘솔 트리에서 **산업 네트워크 보호** 노드를 확장합니다.
2. **PLC 프로젝트 조사** 하위 노드를 선택합니다.
3. **PLC 프로젝트 조사** 노드의 세부 정보 창에 있는 **관리** 섹션에서 **시작** 링크를 클릭합니다.
4. **PLC 프로젝트 무결성 검사** 하위 노드를 선택합니다.
5. **PLC 프로젝트 무결성 검사** 노드의 세부 정보 창에 있는 **관리** 섹션에서 다음 단계 중 하나를 수행합니다.
   - PLC 프로젝트 무결성 검사를 활성화하려면 **시작** 링크를 클릭합니다.
     PLC 프로젝트 무결성 검사 작업이 시작됩니다.
   - PLC 프로젝트 무결성 검사를 비활성화하려면 **중지** 링크를 클릭합니다.
     PLC 프로젝트 무결성 검사 작업이 중지됩니다.

PLC 구성 레지스트리 정보

PLC 구성 레지스트리(이하 레지스트리)는 Kaspersky Industrial CyberSecurity for Nodes가 사용하는 모든 PLC 구성의 공유 목록입니다. *PLC 구성*은 PLC의 개별 속성의 집합이며, 설정에서 지정할 수 있습니다(IP 주소, 랙 번호, 모델 등). 레지스트리로 작업하는 동안 PLC 구성을 추가, 수정, 제거할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 4.5에서 Siemens SIMATIC S7-300/400/400H 유형의 PLC 구성 해시를 계산하는 절차가 변경되었습니다. 따라서 애플리케이션을 업그레이드한 후 *PLC 프로젝트 조사* 작업을 재시작하여 이 PLC 프로젝트에 대한 새 베이스라인을 생성해야 합니다.

PLC 구성 레지스트리를 직접 채울 수도 있고, PLC 구성 데이터가 포함된 구성 파일을 가져올 수도 있습니다.

레지스트리에서 PLC 구성 목록은 Kaspersky Security Center 관리 콘솔을 통해 구성되는 *PLC 프로젝트 무결성 검사* 작업의 보호 범위 생성에 사용됩니다. *PLC 프로젝트 조사* 작업 목록을 생성할 때 레지스트리에 추가된 PLC 구성을 추가하고 제거할 수 있습니다. 작업 목록에서 PLC 구성을 제거해도 레지스트리에서 이 구성이 제거되지는 않습니다.

레지스트리에 추가된 각 PLC 구성은 고유 식별 번호를 획득합니다. PLC 구성이 변경되면 식별 번호도 변경됩니다. Kaspersky Industrial CyberSecurity for Nodes 콘솔의 *PLC 프로젝트 조사* 작업 목록에 추가된 PLC 구성에는 식별 번호가 없습니다. Kaspersky Security Center에서 *PLC 프로젝트 조사* 작업 보호 범위를 생성할 때 이러한 PLC 구성을 레지스트리에 직접 추가할 수 있습니다.

Kaspersky Security Center에 있는 *PLC 프로젝트 조사* 작업의 PLC 구성 목록은 다음 두 경로에서 채워집니다.

- 애플리케이션 콘솔을 통해 로컬 작업 목록에 추가된 ID가 없는 PLC 구성(목록은 자동 동기화됨).
- 관리자가 레지스트리에서 추가한, ID가 있는 PLC 구성.

PLC 프로젝트 조사 작업 목록에 추가된 PLC 구성이 레지스트리에서 제거되면, Kaspersky Industrial CyberSecurity for Nodes에서 무결성 검사 결과가 왜곡될 수 있음을 알립니다. *PLC 프로젝트 조사* 작업 목록의 모든 PLC 구성이 레지스트리에 있는지 확인하고 PLC 프로젝트 조사 작업을 다시 시작합니다.

PLC 레지스트리 구성

PLC 레지스트리를 구성하려면:

1. 다음 방법 중 하나로 **PLC 레지스트리 관리** 창을 엽니다.

   - **로컬 PLC 프로젝트 조사 작업 설정에서**

     1. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
     2. 작업 공간에서 **기기** 탭을 선택합니다.
     3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
     4. **작업** 섹션으로 갑니다.
     5. 창이 열리면 **PLC 프로젝트 조사** 작업을 선택하고 **속성** 버튼을 클릭합니다.
        속성: PLC 프로젝트 조사 창이 열립니다.
     6. **설정** 섹션으로 가서 **작업 설정** 탭의 **PLC 레지스트리에서 추가** 버튼을 클릭합니다.
        PLC 레지스트리 관리 5.0.0 창이 열립니다.

   - **Kaspersky Security Center 관리 콘솔 하드웨어 폴더에서**

     a. Kaspersky Security Center 관리 콘솔 트리에서 **중앙 관리 서버 <서버 이름>** 노드를 확장합니다.

     b. **고급** 노드를 확장합니다.

c. **저장소** 폴더에서 **하드웨어** 하위 폴더를 선택합니다.

> **하드웨어** 폴더가 보이지 않는다면, 중앙 관리 서버 인터페이스 설정에서 **취약점 및 패치 관리 표시** 확인란을 선택합니다.

d. **하드웨어** 폴더 작업 공간에 있는 **추가 조치** 버튼의 마우스 오른쪽 메뉴에서 **PLC 레지스트리 관리 5.0.0** 옵션을 선택합니다.

PLC 레지스트리 관리 5.0.0 창이 열립니다.

2. 필요한 PLC 구성을 직접 추가합니다.

3. 필요하다면 **XML 파일에서 PLC 프로젝트 구성 데이터를 가져옵니다**.

a. **가져오기** 버튼을 클릭합니다.

표준 Microsoft Windows **파일 열기** 창이 열립니다.

b. PLC 설정 XML 파일의 경로를 지정합니다.

c. **열기**를 클릭합니다.

새 PLC 구성 데이터 항목이 **PLC 레지스트리 관리** 창의 목록에 표시됩니다.

4. 필요하다면 **PLC 프로젝트 구성 데이터를 XML 파일로 내보냅니다**.

a. **내보내기** 버튼을 클릭합니다.

b. 팝업 창에서 PLC 프로젝트 구성 데이터를 저장할 XML 파일의 위치와 파일 이름을 제공합니다.

c. **저장** 버튼을 누릅니다.

5. PLC 구성 설정을 변경하려면 **편집**을 클릭합니다.

PLC 레지스트리에서 PLC 구성을 수정하면 *PLC 프로젝트 무결성 검사* 작업이 영향을 받습니다. *PLC 프로젝트 조사* 작업을 실행하여 업데이트된 데이터를 가져온 후 *PLC 프로젝트 무결성 검사*를 다시 실행해야 실제 결과를 얻을 수 있습니다.

1. PLC 프로젝트 구성을 더 이상 사용하지 않는다면 **삭제** 버튼을 클릭합니다.

> PLC 프로젝트가 PLC 레지스트리에서 삭제되면 추가 조사 및 무결성 검사에 사용할 수 없습니다.

2. **필터** 필드를 사용하여 필요한 값으로 PLC 구성을 검토합니다.

3. 필요하다면 **Kaspersky Industrial CyberSecurity for Nodes(으)로 보호할 수 있는 PLC 구성만 표시합니다** 확인란을 선택합니다.

4. **닫기** 버튼을 클릭합니다.

PLC 레지스트리가 저장됩니다.

보안 감사

이 작업은 ICS 감사 라이센스가 부여된 개체를 포함한 활성 Kaspersky Industrial CyberSecurity for Nodes 라이센스 키가 있는 경우에만 실행할 수 있습니다.

보안 감사 작업은 장치의 취약점을 검색하고 장치의 운영 체제 표준 준수를 평가하기 위한 그룹 또는 로컬 작업입니다. Kaspersky Industrial CyberSecurity for Nodes는 보안 감사 작업을 수행하기 위해 제품과 함께 제공되는 XML 형식 데이터베이스 또는 사용자 지정 데이터베이스를 사용합니다.

- 장치의 취약점을 검색하기 위해 애플리케이션은 OVAL 언어로 작성된 규칙을 사용합니다.
- 운영 체제의 장치 보안 및 표준 준수를 평가하기 위해 애플리케이션은 OVAL 및 XCCDF 언어로 작성된 규칙 구성을 사용합니다.

보안 감사 규칙은 여러 클래스로 구분됩니다:

- 규정 준수 – 이 규칙은 시스템 구성 설정이 보안 정책을 준수하는지 확인합니다.
- 인벤토리 – 이 규칙은 규칙에 지정된 소프트웨어 또는 하드웨어가 시스템에 있는지 확인합니다.
- 기타 – 이 규칙에는 사용자 지정 검사가 포함됩니다.
- 패치 – 이 규칙은 규칙에 지정된 패치가 시스템에 설치되었는지 확인합니다.
- 취약점 – 이 규칙은 규칙에 지정된 취약점이 시스템에 있는지 확인합니다.

보안 감사 작업 설정 제한 사항

보안 감사 작업을 생성 및 구성할 때 다음 제한 사항을 고려합니다:

- **파일의 사용자 지정 규칙 기반** 경로를 선택할 때 사용되는 파일의 누적 크기에 대한 총 제한은 2MB입니다.
- 작업 실행 결과 리포트의 크기 제한은 7.5MB입니다.

지원하는 OVAL 검사 유형

보안 감사 작업은 다음 유형의 OVAL 검사를 지원합니다:

- accesstoken
- auditeventpolicy
- auditeventpolicysubcategories
- cmdlet - Windows Vista / Server 2008 이상에서 사용 가능

- environmentvariable58
- environmentvariable
- family
- file
- fileauditedpermissions53
- filehash58
- filehash
- group_sid
- interface
- lockoutpolicy
- passwordpolicy
- 포트
- process58
- process
- registry
- rpmverifyfile
- service
- sid
- textfilecontent54
- 사용자
- user_sid
- variable
- wmi57
- wmi
- xmlfilecontent

지원되지 않는 OVAL 검사의 경우 보안 감사 결과 리포트에 오류가 표시됩니다.

보안 감사 작업 관리

이 작업은 ICS 감사 라이센스가 부여된 개체를 포함한 활성 Kaspersky Industrial CyberSecurity for Nodes 라이센스 키가 있는 경우에만 실행할 수 있습니다.

보안 감사 작업은 Kaspersky Security Center 웹 콘솔 또는 명령줄 인터페이스를 사용하여 만들고 구성하는 로컬 작업 또는 그룹 작업입니다. 이러한 작업은 취약점을 검색하고 기업 시스템의 보안 표준 준수를 평가하는 데 사용됩니다.

이 섹션에서는 보안 감사 작업을 관리하는 방법에 대한 지침을 제공합니다.

기본 설정으로 보안 감사 작업 생성 및 구성

기본 설정으로 보안 감사 작업을 생성하고 구성하려면:

1. Kaspersky Security Center 웹 콘솔 메인 창에서 **에셋 관리** → **작업** 섹션을 선택합니다.
2. **추가** 버튼을 클릭합니다.
   작업 마법사가 시작됩니다.
3. **애플리케이션** 드롭다운 목록에서 Kaspersky Industrial CyberSecurity for Nodes를 선택합니다.
4. **작업 유형** 드롭다운 목록에서 **보안 감사** 옵션을 선택합니다.
5. 작업 이름을 입력하거나 기본 이름을 유지합니다.
6. 이 작업이 할당되는 장치를 선택합니다.
7. **다음** 버튼을 클릭합니다.
8. **작업을 실행할 계정 선택** 창에서 다음 중 하나를 수행합니다:
   - 기본 계정을 선택합니다.
   - 작업을 시작하는 데 계정 권한을 사용할 사용자의 이름과 암호를 입력합니다.
9. **다음** 버튼을 클릭합니다.
10. **작업 생성 마침** 창에서 **생성이 완료되면 작업 세부 정보 열기** 확인란을 선택합니다.
11. **마침** 버튼을 클릭합니다.
    기본 설정이 포함된 작업 속성 창이 열립니다.
12. **애플리케이션 설정** 탭을 엽니다.
    규칙 소스 섹션에서 **파일의 사용자 지정 규칙 기반** 옵션이 기본으로 선택됩니다.
13. **파일에서 규칙 기반 가져오기** 버튼을 클릭합니다.

14. 창이 열리면 규칙 데이터베이스가 있는 파일을 지정합니다.

    OVAL 규칙 및 XCCDF 규칙이 들어 있는 XML 파일이 포함된 압축 파일을 하나만 로드할 수 있습니다.

    > 압축 파일 크기는 2MB를 초과할 수 없습니다.

15. **열기** 버튼을 클릭합니다.

    규칙 소스 섹션에는 로드한 규칙에 관한 정보가 표시됩니다. **플랫폼** 필드의 **더 알아보기** 링크를 따라서 선택한 경로의 규칙에 언급된 운영 체제 및 제품 목록이 있는 창을 엽니다.

16. 필요하다면 외부 변수를 사용하여 파일을 로드합니다:

    > 선택한 규칙 소스에 XCCDF 규칙이 포함되어 있는 경우 외부 변수를 사용할 수 없습니다.

    a. **사용자 지정 데이터베이스가 있는 외부 변수 데이터 사용** 확인란을 선택합니다.

    b. **파일에서 외부 변수 가져오기** 링크를 클릭합니다.

    c. 창이 열리면 외부 변수가 들어 있는 파일의 경로를 지정합니다.

    d. **열기** 버튼을 클릭합니다.

17. **범위** 섹션에서 필요하다면 취약점 검사 모드를 변경합니다:

    > 선택한 규칙 소스에 XCCDF 규칙이 포함된 경우 **범위** 섹션은 사용할 수 없습니다.

    a. 모드 중 하나를 선택합니다:

    - **모든 취약점 검사**.

      Kaspersky Industrial CyberSecurity for Nodes는 취약점 데이터베이스의 규칙에 설명된 모든 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

    - **목록에 추가된 항목을 제외한 모든 취약점 검사**.

      Kaspersky Industrial CyberSecurity for Nodes는 아래 목록에 추가된 취약점을 제외하고 취약점 데이터베이스의 규칙에 설명된 모든 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

    - **목록에 추가된 취약점 검사**.

      Kaspersky Industrial CyberSecurity for Nodes는 아래 목록에 추가된 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

    b. **목록에 추가된 항목을 제외한 모든 취약점 검사** 및 **목록에 추가된 취약점 검사** 모드를 선택한 경우 **추가** 및 **조건별 추가** 버튼을 사용하여 취약점 목록을 생성합니다.

18. **고급 설정** 섹션에서 필요하다면 보안 감사 작업 리포트에 포함할 지시어 기반 검사의 상태를 결정합니다:

    > 선택한 규칙 소스에 XCCDF 규칙이 포함되어 있는 경우 지시어를 적용할 수 없습니다.

    a. **지시어 사용** 확인란을 선택합니다.

b. 각 지시어 옆의 스위치를 사용하여 보안 감사 작업 리포트에 표시할 지시어 기반 검사의 상태를 결정합니다.

지시어 상태 옆의 스위치가 켜져 있으면 이 상태를 가진 지시어의 규칙에 따른 검사 결과가 보안 감사 작업 리포트에 표시됩니다.

기본적으로 모든 지시어에 대해서 **True** 그리고 **False** 검사 결과 옆의 확인란이 선택됩니다.

19. **고급 설정** 섹션에서 필요하다면 작업 완료 이벤트 기록을 위한 설정을 구성합니다:

a. **로그 기록 사용** 확인란을 선택합니다.

b. 목록에서 원하는 **로그 기록 수준**을 선택합니다.

기본적으로 로그는 C:\Program Files\ Kaspersky Lab\ Kaspersky Security Center Web Console\logs 폴더에 저장됩니다.

다음 기록 레벨을 사용할 수 있습니다:

- **심각 수준** – 심각 이벤트만
- **경고 수준** – 심각 및 경고 이벤트만
- **정보 수준** – 모든 심각, 경고, 정보 이벤트
- **디버그 수준** – 모든 심각, 경고, 정보, 디버그 이벤트

20. **저장** 버튼을 클릭해 변경 사항을 저장합니다.

생성된 작업을 수동으로 시작하거나 스케줄에 따라 시작되도록 구성할 수 있습니다. 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

SCADA용 Kaspersky ICS CERT 취약점 데이터베이스를 사용하여 보안 감사 작업 설정 구성

Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 모듈 업데이트와 함께 SCADA용 Kaspersky ICS CERT 취약점 데이터베이스가 제공 및 업데이트됩니다. 따라서 SCADA용 Kaspersky ICS CERT 취약점 데이터베이스를 규칙 경로로 사용해 보안 감사 작업 설정을 구성하기 전에 애플리케이션 데이터베이스 및 모듈을 업데이트합니다.

SCADA용 Kaspersky ICS CERT 취약점 데이터베이스를 규칙 경로로 사용하여 보안 감사 작업 설정을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
2. 보안 감사 작업의 이름을 클릭해 작업 설정 창을 엽니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **규칙 소스** 섹션에서 **SCADA용 Kaspersky ICS CERT 취약점 데이터베이스** 옵션을 선택합니다.

취약점 데이터베이스 정보가 표시됩니다. **플랫폼** 필드의 **상세 정보** 링크를 따라서 선택한 경로의 규칙에 언급된 운영 체제 및 제품 목록이 있는 창을 엽니다.

5. **범위** 섹션에서 필요하다면 취약점 검사 모드를 변경합니다:

   a. 모드 중 하나를 선택합니다:

   - **모든 취약점 검사**.

     Kaspersky Industrial CyberSecurity for Nodes는 SCADA용 Kaspersky ICS CERT 취약점 데이터베이스의 규칙에 설명된 모든 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

   - **목록에 추가된 항목을 제외한 모든 취약점 검사**.

     Kaspersky Industrial CyberSecurity for Nodes는 아래 목록에 추가된 취약점을 제외하고 SCADA용 Kaspersky ICS CERT 취약점 데이터베이스의 규칙에 설명된 모든 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

   - **목록에 추가된 취약점 검사**.

     Kaspersky Industrial CyberSecurity for Nodes는 아래 목록에 추가된 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

   b. **목록에 추가된 항목을 제외한 모든 취약점 검사** 및 **목록에 추가된 취약점 검사** 모드를 선택한 경우 **추가** 및 **조건별 추가** 버튼을 사용하여 취약점 목록을 생성합니다.

6. **고급 설정** 섹션에서 필요하다면 보안 감사 작업 리포트에 포함할 지시어 기반 검사의 상태를 결정합니다:

   a. **지시어 사용** 확인란을 선택합니다.

   b. 각 지시어 옆의 스위치를 사용하여 보안 감사 작업 리포트에 표시할 지시어 기반 검사의 상태를 결정합니다.

   지시어 상태 옆의 스위치가 켜져 있으면 이 상태를 가진 지시어의 규칙에 따른 검사 결과가 보안 감사 작업 리포트에 표시됩니다.

   기본적으로 모든 지시어에 대해서 **True** 그리고 **False** 검사 결과 옆의 확인란이 선택됩니다.

7. **고급 설정** 섹션에서 필요하다면 작업 완료 이벤트 기록을 위한 설정을 구성합니다:

   a. **로그 기록 사용** 확인란을 선택합니다.

   b. 목록에서 원하는 **로그 기록 수준**을 선택합니다.

   기본적으로 로그는 C:\Program Files\ Kaspersky Lab\ Kaspersky Security Center Web Console\logs 폴더에 저장됩니다.

   다음 기록 레벨을 사용할 수 있습니다:

   - **심각 수준** – 심각 이벤트만
   - **경고 수준** – 심각 및 경고 이벤트만
   - **정보 수준** – 모든 심각, 경고, 정보 이벤트
   - **디버그 수준** – 모든 심각, 경고, 정보, 디버그 이벤트

8. **저장** 버튼을 클릭해 작업 설정을 저장합니다.

보안 및 표준 준수 구성을 사용하여 보안 감사 작업 설정 구성

Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 모듈 업데이트를 통해 보안 및 표준 준수 구성이 설정되고 업데이트됩니다. 따라서 보안 및 표준 준수 구성을 사용하여 보안 감사 작업 설정을 구성하기 전에 애플리케이션 데이터베이스 및 모듈을 업데이트합니다.

보안 및 표준 준수 구성을 규칙 경로로 사용하여 보안 감사 작업 설정을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
2. 보안 감사 작업의 이름을 클릭해 작업 설정 창을 엽니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **규칙 소스** 섹션에서 **운영 체제용 규정 준수 및 보안 구성** 옵션을 선택합니다.
5. **규칙 구성 선택** 버튼을 클릭합니다.
6. 창이 열리면 보안 및 표준 준수 구성 중 하나를 선택합니다.
7. **확인** 버튼을 클릭합니다.

   규칙 소스 선택 항목은 선택한 보안 및 표준 준수 구성의 정보를 표시합니다. **규칙** 섹션에는 경로로 선택한 보안 및 표준 준수 구성에 포함된 규칙 목록이 표시됩니다.
8. **고급 설정** 섹션에서 필요하다면 작업 완료 이벤트 기록을 위한 설정을 구성합니다:

   a. **로그 기록 사용** 확인란을 선택합니다.

   b. 목록에서 원하는 **로그 기록 수준**을 선택합니다.

   기본적으로 로그는 C:\Program Files\ Kaspersky Lab\ Kaspersky Security Center Web Console\logs 폴더에 저장됩니다.

   다음 기록 레벨을 사용할 수 있습니다:

   - **심각 수준** – 심각 이벤트만
   - **경고 수준** – 심각 및 경고 이벤트만
   - **정보 수준** – 모든 심각, 경고, 정보 이벤트
   - **디버그 수준** – 모든 심각, 경고, 정보, 디버그 이벤트
9. **규칙** 섹션에서 선택한 보안 및 표준 준수 구성에 포함된 규칙 목록을 검토합니다:
   - 규칙 이름을 클릭해 규칙 설명을 엽니다.
   - **필터** 버튼을 클릭해 필터링 규칙 창을 엽니다.
10. **저장** 버튼을 클릭해 작업 설정을 저장합니다.

Kaspersky Security Center 저장소에서 사용자 지정 규칙 데이터베이스를 사용하여 보안 감사 작업 설정 구성

Kaspersky Security Center 저장소를 사용하여 사용자 지정 데이터베이스를 통한 보안 감사 작업 설정을 구성하기 전에:

1. 명령줄 인터페이스에서 사용자 지정 데이터베이스 서명용 인증서의 지문을 생성합니다.

   사용자 지정 데이터베이스 서명용 인증서에 기존 지문을 사용할 수 있습니다.

2. 명령줄 인터페이스를 사용하여 package.zip 이름의 Kaspersky Security Center 설치 패키지를 생성합니다.

3. 이전 단계에서 생성된 OVAL 및 XCCDF 규칙이 포함된 package.zip 압축 파일을 Kaspersky Security Center 저장소에 추가합니다. 이를 위해서 다음 설정을 사용해 설치 패키지를 설치하는 작업을 생성하고 실행합니다:

   - 설치 패키지는 이전 단계에서 생성된 package.zip 압축 파일의 파일을 기반으로 생성되어야 합니다.
   - 설치 패키지 설치 작업을 할당할 장치 선택 창에서 Kaspersky Security Center 중앙 관리 서버가 설치된 컴퓨터의 주소를 직접 지정합니다.

Kaspersky Industrial CyberSecurity for Nodes에서는 설치 및 배포된 패키지를 사용자 지정 규칙 데이터베이스로만 업데이트할 수 있습니다. 규칙 패키지는 삭제할 수 없습니다.

Kaspersky Security Center 저장소의 사용자 지정 규칙 데이터베이스를 사용하여 보안 감사 작업 설정을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
2. 작업 이름을 클릭해 작업 설정 창을 엽니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **규칙 소스** 섹션에서 **Kaspersky Security Center 리포지토리의 사용자 지정 규칙 기반** 옵션을 선택합니다.
5. **사용자 지정 컬렉션에서 파일 선택** 버튼을 클릭합니다.
6. 창이 열리면 규칙 데이터베이스가 있는 압축 파일을 지정합니다.
   OVAL 규칙 및 XCCDF 규칙이 포함된 XML 파일이 들어 있는 압축 파일을 하나만 로드할 수 있습니다.

   압축 파일 크기는 2MB를 초과할 수 없습니다.

7. **열기** 버튼을 클릭합니다.
   규칙 소스 섹션에는 로드한 규칙에 관한 정보가 표시됩니다. **플랫폼** 필드의 **상세 정보** 링크를 따라서 선택한 경로의 규칙에 언급된 운영 체제 및 제품 목록이 있는 창을 엽니다.

8. 필요하다면 사용자 지정 규칙 데이터베이스 서명용 인증서의 지문을 지정합니다:

   a. **지문 사용** 확인란을 선택합니다. 이 기능을 활성화하면 작업 실행 시 Kaspersky Security Center에서 지문을 확인합니다. 지문이 작업 설정에 지정된 지문과 일치하지 않은 경우 작업 실행이 오류를 발생시키며 종료됩니다.

   이 기능을 비활성화하면 Kaspersky Security Center에서 지문을 확인하지 않습니다.

   b. **지문** 필드에 명령줄 인터페이스를 사용하여 얻은 지문을 입력합니다.

9. 필요하다면 외부 변수를 사용하여 파일을 로드합니다:

   선택한 규칙 소스에 XCCDF 규칙이 포함되어 있는 경우 외부 변수를 사용할 수 없습니다.

   a. **사용자 지정 데이터베이스가 있는 외부 변수 데이터 사용** 확인란을 선택합니다.

   b. **파일에서 외부 변수 가져오기** 버튼을 클릭합니다.

   c. 창이 열리면 외부 변수가 들어 있는 파일의 경로를 지정합니다.

   d. **확인** 버튼을 클릭합니다.

10. **범위** 섹션에서 필요하다면 취약점 검사 모드를 변경합니다:

    선택한 규칙 소스에 XCCDF 규칙이 포함된 경우 **범위** 섹션은 사용할 수 없습니다.

    a. 모드 중 하나를 선택합니다:

    - **모든 취약점 검사**.

      Kaspersky Industrial CyberSecurity for Nodes는 SCADA용 Kaspersky ICS CERT 취약점 데이터베이스의 규칙에 설명된 모든 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

    - **목록에 추가된 항목을 제외한 모든 취약점 검사**.

      Kaspersky Industrial CyberSecurity for Nodes는 아래 목록에 추가된 취약점을 제외하고 SCADA용 Kaspersky ICS CERT 취약점 데이터베이스의 규칙에 설명된 모든 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

    - **목록에 추가된 취약점 검사**.

      Kaspersky Industrial CyberSecurity for Nodes는 아래 목록에 추가된 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

    b. **목록에 추가된 항목을 제외한 모든 취약점 검사** 및 **목록에 추가된 취약점 검사** 모드를 선택한 경우 **추가** 및 **조건별 추가** 버튼을 사용하여 취약점 목록을 생성합니다.

11. **고급 설정** 섹션에서 필요하다면 보안 감사 작업 리포트에 포함할 지시어 기반 검사의 상태를 결정합니다:

    선택한 규칙 소스에 XCCDF 규칙이 포함되어 있는 경우 지시어를 적용할 수 없습니다.

    a. **지시어 사용** 확인란을 선택합니다.

    b. 각 지시어 옆의 스위치를 사용하여 보안 감사 작업 리포트에 표시할 지시어 기반 검사의 상태를 결정합니다.

지시어 상태 옆의 스위치가 켜져 있으면 이 상태를 가진 지시어의 규칙에 따른 검사 결과가 보안 감사 작업 리포트에 표시됩니다.

기본적으로 모든 지시어에 대해서 **True** 그리고 **False** 검사 결과 옆의 확인란이 선택됩니다.

12. **고급 설정** 섹션에서 필요하다면 작업 완료 이벤트 기록을 위한 설정을 구성합니다:

    a. **로그 기록 사용** 확인란을 선택합니다.

    b. 목록에서 원하는 **로그 기록 수준**을 선택합니다.

    기본적으로 로그는 C:\Program Files\ Kaspersky Lab\ Kaspersky Security Center Web Console\logs 폴더에 저장됩니다.

    다음 기록 레벨을 사용할 수 있습니다:

    - **심각 수준** – 심각 이벤트만
    - **경고 수준** – 심각 및 경고 이벤트만
    - **정보 수준** – 모든 심각, 경고, 정보 이벤트
    - **디버그 수준** – 모든 심각, 경고, 정보, 디버그 이벤트

13. **저장** 버튼을 클릭해 작업 설정을 저장합니다.

파일에서 사용자 지정 데이터베이스를 사용하여 보안 감사 작업 설정 구성

파일에서 사용자 지정 데이터베이스를 사용하여 보안 감사 작업 설정을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 작업** 옵션을 선택합니다.
2. 작업 이름을 클릭해 작업 설정 창을 엽니다.
3. **애플리케이션 설정** 탭을 엽니다.
4. **규칙 소스** 섹션에서 **파일의 사용자 지정 규칙 기반** 옵션을 선택합니다.
5. **파일에서 규칙 기반 가져오기** 버튼을 클릭합니다.
6. 창이 열리면 규칙 데이터베이스가 있는 파일을 지정합니다.

   OVAL 규칙 및 XCCDF 규칙이 들어 있는 XML 파일이 포함된 압축 파일을 하나만 로드할 수 있습니다.

   > 압축 파일 크기는 2MB를 초과할 수 없습니다.

7. **열기** 버튼을 클릭합니다.

   규칙 소스 섹션에는 로드한 규칙에 관한 정보가 표시됩니다. **플랫폼** 필드의 **더 알아보기** 링크를 따라서 선택한 경로의 규칙에 언급된 운영 체제 및 제품 목록이 있는 창을 엽니다.

8. 필요하다면 외부 변수를 사용하여 파일을 로드합니다:

선택한 규칙 소스에 XCCDF 규칙이 포함되어 있는 경우 외부 변수를 사용할 수 없습니다.

a. **사용자 지정 데이터베이스가 있는 외부 변수 데이터 사용** 확인란을 선택합니다.

b. **파일에서 외부 변수 가져오기** 링크를 클릭합니다.

c. 창이 열리면 외부 변수가 들어 있는 파일의 경로를 지정합니다.

d. **열기** 버튼을 클릭합니다.

9. **범위** 섹션에서 필요하다면 취약점 검사 모드를 변경합니다:

선택한 규칙 소스에 XCCDF 규칙이 포함된 경우 **범위** 섹션은 사용할 수 없습니다.

a. 모드 중 하나를 선택합니다:

- **모든 취약점 검사**.

  Kaspersky Industrial CyberSecurity for Nodes는 취약점 데이터베이스의 규칙에 설명된 모든 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

- **목록에 추가된 항목을 제외한 모든 취약점 검사**.

  Kaspersky Industrial CyberSecurity for Nodes는 아래 목록에 추가된 취약점을 제외하고 취약점 데이터베이스의 규칙에 설명된 모든 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

- **목록에 추가된 취약점 검사**.

  Kaspersky Industrial CyberSecurity for Nodes는 아래 목록에 추가된 취약점을 탐지하기 위해 작업이 할당된 장치를 검사합니다.

b. **목록에 추가된 항목을 제외한 모든 취약점 검사** 및 **목록에 추가된 취약점 검사** 모드를 선택한 경우 **추가** 및 **조건별 추가** 버튼을 사용하여 취약점 목록을 생성합니다.

10. **고급 설정** 섹션에서 필요하다면 보안 감사 작업 리포트에 포함할 지시어 기반 검사의 상태를 결정합니다:

선택한 규칙 소스에 XCCDF 규칙이 포함되어 있는 경우 지시어를 적용할 수 없습니다.

a. **지시어 사용** 확인란을 선택합니다.

b. 각 지시어 옆의 스위치를 사용하여 보안 감사 작업 리포트에 표시할 지시어 기반 검사의 상태를 결정합니다.

지시어 상태 옆의 스위치가 켜져 있으면 이 상태를 가진 지시어의 규칙에 따른 검사 결과가 보안 감사 작업 리포트에 표시됩니다.

기본적으로 모든 지시어에 대해서 **True** 그리고 **False** 검사 결과 옆의 확인란이 선택됩니다.

11. **고급 설정** 섹션에서 필요하다면 작업 완료 이벤트 기록을 위한 설정을 구성합니다:

a. **로그 기록 사용** 확인란을 선택합니다.

b. 목록에서 원하는 **로그 기록 수준**을 선택합니다.

기본적으로 로그는 C:\Program Files\ Kaspersky Lab\ Kaspersky Security Center Web Console\logs 폴더에 저장됩니다.

다음 기록 레벨을 사용할 수 있습니다:

- **심각 수준** – 심각 이벤트만
- **경고 수준** – 심각 및 경고 이벤트만
- **정보 수준** – 모든 심각, 경고, 정보 이벤트
- **디버그 수준** – 모든 심각, 경고, 정보, 디버그 이벤트

12. **저장** 버튼을 클릭해 작업 설정을 저장합니다.

보안 감사 작업 실행 결과 보기

보안 감사 작업 실행 결과를 보려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
2. 작업 이름을 클릭해 작업 설정 창을 엽니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **리포트** 섹션을 선택합니다.

리포트 목록에는 날짜별로 정렬된 작업 실행 결과가 포함됩니다. 목록의 각 줄에는 작업 설정에서 지정한 노드의 **작업 실행 상태**와 작업 실행이 완료되는 날짜 및 시간이 포함됩니다.

Kaspersky Industrial CyberSecurity for Nodes는 보안 감사 작업 실행 결과를 반환합니다:

- *통과함*.

  보안 감사 작업은 **Vulnerability** 지시어에 대한 검사 결과가 *False*이고 나머지 지시어는 *True*인 경우 이 상태를 획득합니다.

- *통과하지 못함*.

  보안 감사 작업은 **Vulnerability** 지시어에 대한 검사 결과가 *True*이고 나머지 지시어는 *False*인 경우 이 상태를 획득합니다.

- *경고*.

  보안 감사 작업은 모든 지시어에 대한 검사 결과가 *오류*인 경우 이 상태를 획득합니다.

- *기타*.

  보안 감사 작업은 모든 지시어에 대한 검사 결과가 *알 수 없음*, *Not evaluated*, *Not applicable*인 경우 이 상태를 획득합니다.

필터를 사용하여 리포트의 데이터를 필터링할 수 있습니다.

보안 감사 작업 실행 결과에 대한 리포트는 작업 완료 후 7일간 또는 작업이 제거될 때까지 Kaspersky Security Center에서 볼 수 있습니다.

보안 감사 작업 실행 결과를 별도의 파일로 내보내기

보안 감사 작업 실행 결과를 별도의 파일로 내보내려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
2. 작업 이름을 클릭해 작업 설정 창을 엽니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **리포트** 탭에서 원하는 리포트를 선택하고 **상세 정보** 버튼을 클릭합니다.
5. **보안 감사 결과** 창이 열리면 다음 동작 중 하나를 수행합니다:

   - 모든 작업 실행 결과에 대한 XML 형식 리포트가 들어 있는 압축 파일을 받으려면 **내보내기**를 클릭합니다.

     XML 형식 리포트가 포함된 ZIP 압축 파일은 다운로드한 파일용 표준 운영 체제 폴더에 저장됩니다. 작업 설정에서 보안 감사 이벤트 기록을 활성화한 경우 TXT 형식 로그가 포함된 ZIP 압축 파일도 추가됩니다.

   - HTML 형식의 작업 실행 결과 리포트가 포함된 압축 파일을 받으려면:

     a. 필요하다면 **필터** 버튼을 사용하여 리포트 데이터를 필터링합니다.

     b. **리포트 생성** 버튼을 클릭합니다.

     HTML 형식 리포트가 포함된 ZIP 압축 파일은 다운로드한 파일용 표준 운영 체제 폴더에 저장됩니다. 리포트에는 필터와 일치하는 줄만 포함됩니다.

   리포트가 포함된 압축 파일의 이름에는 작업이 실행된 노드의 이름과 작업이 실행된 날짜 및 시간이 포함됩니다.

OVAL 및 XCCDF 규칙을 사용하는 파일 서명용 인증서 지문 생성

OVAL 또는 XCCDF 규칙이 있는 파일 서명용 인증서 지문을 생성하려면:

1. 장치에서 로컬 관리자 권한으로 명령줄 해석기(명령 프롬프트 `cmd.exe` 등)를 실행합니다.
2. `cd` 명령을 사용하여 ovaldbmgr.exe 파일이 있는 폴더로 갑니다.

   기본적으로 파일은 배포 패키지의 \tools\ovaldbmgr 폴더에 있습니다.
3. 인증서의 위치에 따라 다음 명령 중 하나를 실행하고 Enter를 누릅니다.

   - 인증서를 생성한 다음 System Storage Local Machine에 저장하려면:

     ```
     ovaldbmgr.exe --signer=make-cert --subject=<certificate name>
     ```

- 인증서를 생성한 다음 PFX 컨테이너에 저장하려면:

```
ovaldbmgr.exe --signer=make-cert --subject=<certificate_name> --export --pwd=
<password_for_accessing_the_PFX_container> --pfx=<full_path_and_file_name_of_the_PFX_container>
```

인증서가 성공적으로 생성되면 인증서의 지문이 명령줄에 반환됩니다.

사용자 지정 OVAL 및 XCCDF 규칙을 사용하여 Kaspersky Security Center 설치 패키지 생성

서명된 압축 파일로 OVAL 또는 XCCDF 규칙이 포함된 Kaspersky Security Center 설치 패키지를 생성하려면:

1. 장치에서 로컬 관리자 권한으로 명령줄 해석기(명령 프롬프트 `cmd.exe` 등)를 실행합니다.
2. `cd` 명령을 사용하여 ovaldbmgr.exe 파일이 있는 폴더로 갑니다.
   기본적으로 파일은 배포 패키지의 \tools\ovaldbmgr 폴더에 있습니다.
3. OVAL 또는 XCCDF 규칙 파일의 서명 인증서 위치에 따라 다음 명령 중 하나를 실행합니다:
   - 서명 인증서가 시스템 저장소 로컬 머신에 있는 경우:

```
ovaldbmgr.exe --make-package --command={replace|merge} --subject=<certificate name> --output=<full path> --
source=<full path> <full path to the file with OVAL or XCCDF rules>
```

   - 서명 인증서가 PFX 컨테이너에 있는 경우:

```
ovaldbmgr.exe --make-package --command={replace|merge} --pfx=<full path to the PFX container> --pwd=
<password to access the PFX container> --output=<full path> --source=<full path> <full path to the file
with OVAL or XCCDF rules>
```

Kaspersky Security Center 설치 패키지 생성을 위한 명령 파라미터

옵션	설명
`--make-package`	필수 인수입니다. 파일이 포함된 압축 파일을 생성합니다.
`--command={replace|merge}`	필수 인수입니다. 이 파라미터는 Kaspersky Security Center의 패키지 배포 모드를 정의합니다. 사용 가능한 값: • `replace` – Kaspersky Security Center 저장소의 설치 패키지를 생성 중인 패키지로 교체합니다. • `merge` – 생성할 설치 패키지를 Kaspersky Security Center 저장소에 이미 있는 패키지와 병합합니다. 파라미터 값을 지정하지 않으면 작업이 오류를 일으키며 종료됩니다.
`--pfx=<full path to the PFX container>`	필수 인수입니다. 파라미터는 OVAL 또는 XCCDF 규칙 파일의 서명 인증서 설치 공간이 있는 PFX 컨테이너의 전체 경로를 지정합니다.
`--pwd=<password to access the PFX container>`	필수 인수입니다. 이 파라미터는 PFX 컨테이너에 접근하기 위한 암호를 정의합니다.
`--subject=<certificate name>`	필수 인수입니다. 이 파라미터는 서명용 인증서 이름을 전달합니다. 존재하지 않는 인증서의 이름을 서명에 지정하면 명령이 오류를 일으키며 종료됩니다.

옵션	설명
`--output=<full path>`	필수 인수입니다. 이 파라미터는 명령을 실행한 결과로 설치 패키지가 생성될 폴더의 전체 경로를 지정합니다.
`--source=<full path>`	이 파라미터는 Kaspersky Security Center 패키지에 포함할 OVAL 및 XCCDF 규칙이 있는 폴더를 포함한 폴더의 전체 경로를 지정합니다.
`<full path to the file with OVAL or XCCDF rules>`	이 파라미터는 Kaspersky Security Center 패키지에 포함할 OVAL 또는 XCCDF 규칙이 있는 XML 형식 파일의 전체 경로를 정의합니다. OVAL 및 XCCDF 규칙은 BOM 없이 UTF-8로 저장해야 합니다. OVAL 또는 XCCDF 규칙이 있는 파일은 다른 폴더 내의 폴더에 있어야 합니다. 예: C:\Users\UserName\Desktop\folder\subfolder\OvalRules.xml 스페이스로 구분된 여러 파라미터 값을 지정할 수 있습니다. OVAL 또는 XCCDF 규칙이 있는 파일을 지정하려면 다음 옵션 중 하나를 선택합니다: • `--source=<full path>` 인수만 설정합니다. • 하나 이상의 `<full path to OVAL or XCCDF rules>` 값을 공백으로 구분하여 지정합니다. • `--source=<full path>` 를 설정하고, 동시에 하나 이상의 `<full path to the file with OVAL or XCCDF rules>` 값을 공백으로 구분하여 지정합니다. `<full path to the file with OVAL or XCCDF rules>` 값을 지정하지 않고 `--source=<full path>` 파라미터를 생략하면 작업이 오류를 일으키며 종료됩니다.

명령을 실행하면 Kaspersky Industrial CyberSecurity for Nodes가 다음을 생성합니다:

- `--output=<full path>` 파라미터의 값에 의해 지정된 폴더에 package.zip 이름의 압축 파일이 생성됩니다. 압축 파일은 다음 파일을 포함합니다:
  - OVAL 또는 XCCDF 규칙이 있는 사용자 지정 파일 각각에 대한 하나 이상의 ZIP 파일. 각 압축 파일은 규칙이 포함된 XML 파일 하나와 해당 XML 파일용 서명 파일을 포함합니다.
  - Kaspersky Security Center 패키지 배포를 위한 ovaldbmgr.kud 파일.
  - ovaldbmgr.exe 배포 유틸리티.
- package.zip 압축 파일 서명에 사용되는 서명 지문.

  규칙 경로로 Kaspersky Security Center 저장소의 사용자 지정 규칙 데이터베이스를 사용하여 보안 감사 작업 설정에서 지문을 지정할 수 있습니다.

Kaspersky Security Gateway 사용

이 애플리케이션은 Kaspersky Security Gateway 버전 4.0 이상과 호환됩니다.

Kaspersky Security Gateway는 Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Industrial CyberSecurity for Networks에서 받은 진단 정보를 Kaspersky Security Center에서 SCADA 시스템으로 전송하거나 Kaspersky Industrial CyberSecurity for Networks에서 직접 SCADA 시스템으로 전송하도록 설계되었습니다. 산업 네트워크 및 네트워크의 개별 컴퓨터 보호 상태에 관한 정보가 SCADA 시스템 화면에 표시되어 SCADA 시스템 운영자가 산업 네트워크 보호 문제에 신속히 대응할 수 있습니다.

Kaspersky Security Gateway는 다음 통신 프로토콜을 사용하여 SCADA 시스템과 상호 작용합니다:

- **IEC 60870-5-104**. 자동화 시스템을 위한 통합 개방형 프로토콜입니다.
- **OPC DA**. Microsoft COM 기술 기반의 산업용 네트워크를 위한 장치 상호 작용 사양입니다.
- **OPC UA**. 플랫폼 간 호환성을 제공하는 산업용 네트워크를 위한 장치 상호 작용 사양입니다.

Kaspersky Security Gateway 그래픽 사용자 인터페이스 또는 표준 Microsoft Windows 도구를 사용하여 데이터 전송 설정 구성을 할 수 있습니다.

진단 정보

Kaspersky Security Gateway는 다음 정보를 SCADA 시스템으로 전송합니다:

- **SecurityServerAvailable**. Kaspersky Security Center 중앙 관리 서버의 가용성입니다. 가능한 값:
  - `1` Kaspersky Security Gateway가 Kaspersky Security Center 중앙 관리 서버에 성공적으로 연결되었습니다.
  - `0` Kaspersky Security Gateway가 Kaspersky Security Center 중앙 관리 서버에 연결할 수 없습니다.
- **AllSecuredHostAvailable**. 네트워크의 모든 보호 중인 컴퓨터의 가용성입니다. 컴퓨터는 보호 애플리케이션과 네트워크 에이전트가 실행 중인 경우 이용할 수 있습니다. 가능한 값:
  - `0` Kaspersky Security Center 중앙 관리 서버에서 관리하고 Kaspersky Security Gateway 설정에서 모니터링하도록 선택된 하나 이상의 컴퓨터가 상태를 확인하는 시점에서 이용 불가능한 상태입니다.
  - `1` Kaspersky Security Center 중앙 관리 서버에서 관리하고 Kaspersky Security Gateway 설정에서 모니터링하도록 선택된 모든 컴퓨터가 상태를 확인하는 시점에서 이용 가능한 상태입니다.

  하나 이상의 컴퓨터와 Kaspersky Security Center 중앙 관리 서버가 연결되어 있지 않으면 값 `0`(이용 불가)이 전송됩니다.

- **GeneralizedThreatOccured**. 네트워크의 보호 상태입니다. 가능한 값:
  - `0` 네트워크의 모든 컴퓨터에서 탐지된 위협이 없습니다.
  - `1` 네트워크에 있는 하나 이상의 컴퓨터에서 위협이 탐지되었습니다.
  - `2` 네트워크에 있는 하나 이상의 컴퓨터에 경고가 발생했습니다.

  네트워크 보호 상태 확인 시 Kaspersky Security Gateway는 Kaspersky Security Gateway 설정에서 SCADA 시스템에 표시하도록 선택된 컴퓨터의 상태 정보만 사용합니다.
- **<컴퓨터 이름>**. 컴퓨터의 가용성 및 보호 상태입니다. 컴퓨터에서 이용 가능한 보호 애플리케이션과 네트워크 에이전트가 실행 중입니다. 가능한 값:
  - `-1` 컴퓨터 상태를 검색할 수 없습니다.
  - `0` 컴퓨터를 사용할 수 있습니다.
  - `1` 컴퓨터에서 위협이 탐지되었습니다.
  - `2` 컴퓨터에 경고가 발행했습니다.
  - `3` 컴퓨터를 사용할 수 없습니다.

  Kaspersky Security Gateway는 Kaspersky Security Gateway 설정에서 SCADA 시스템에 표시하도록 선택된 컴퓨터의 상태 정보만 전송합니다.

  > 컴퓨터 또는 Kaspersky Security Gateway와 Kaspersky Security Center 중앙 관리 서버가 연결되어 있지 않으면 값 `-1`(컴퓨터 상태를 검색할 수 없음)이 전송됩니다.
- **<PLC 이름>**. Kaspersky Security Center에 연결된 PLC 상태:
  - `-1` 상태를 검색할 수 없습니다.
  - `0` 오류 메시지가 없거나 PLC를 검사하지 않았습니다.
  - `1` 심각 오류(예: PLC 프로젝트가 참조 프로젝트와 일치하지 않음).
  - `2` 경고.
  - `3` PLC 이용 불가.
- **<장치 이름>**. Kaspersky Industrial CyberSecurity for Networks에 연결된 장치(PLC 또는 IED)의 상태:
  - `-1` 상태를 검색할 수 없습니다.
  - `0` 오류 메시지가 없거나 장치를 검사하지 않았습니다.
  - `1` 심각 오류(예: PLC 프로젝트가 참조 프로젝트와 일치하지 않음).
  - `2` 경고.
  - `3` 장치를 사용할 수 없습니다.

- **UnauthorizedSystemCommandCount**. Kaspersky Industrial CyberSecurity for Networks에 연결된 장치의 새 이벤트 카운터. 가능한 값:
  - `<number>` 새 이벤트 수.
  - `-1` 상태를 검색할 수 없습니다.

Kaspersky Security Gateway의 제한 사항 및 알려진 문제

- Windows 7, Windows Server 2008, Windows Server 2012 중 하나를 실행하는 장치에 설치된 Kaspersky Security Gateway를 Kaspersky Security Center 14 이상에 연결하려면, 운영 체제에서 TLS 1.1 및 1.2를 기본 보안 프로토콜로 활성화해야 합니다. 자세한 정보는 Microsoft 설명서를 참조하십시오.
- `gateway_service.exe` 긴급 종료는 타사 grpc 라이브러리의 오류에 따라 발생할 수 있습니다. 서비스 긴급 종료는 애플리케이션 확인(Application Verifier) 유틸리티를 사용하여 동적 코드 분석을 수행하는 동시에 Kaspersky Industrial CyberSecurity for Networks에 대한 연결이 설정될 시 발생합니다.
- Kaspersky Security Gateway는 Kaspersky Industrial CyberSecurity for Networks 4.2 버전 이상과 호환됩니다.
- KSG OPC UA 서버를 PcVue 16.2와 함께 사용하면, SessionsDiagnosticsSummary 노드를 열 때 PcVue 16.2에 크래시가 발생할 수 있습니다.
- OPC DA 및 OPC UA 프로토콜을 사용 중인 경우 태그 값이 int 유형이어야 합니다.
- Quality 태그 상태는 사용되지 않으며 항상 GOOD 값을 가집니다. 태그 추적이 중지되면 전송되는 데이터에서 제외됩니다. 상태가 변경된 태그(BAD 또는 COM_FAILURE)는 전송할 수 없습니다.
- Kaspersky Security Gateway는 시작된 후 Kaspersky Security Center 또는 Kaspersky Industrial CyberSecurity for Networks에서 데이터를 수신할 때까지 SCADA 시스템으로 태그 값을 전송하지 않습니다.

  Kaspersky Security Gateway를 4.5 이하 버전에서 5.0으로 업데이트하면 추적 파일 로그 기록이 중지됩니다. 필요하다면 다시 추적 파일 로그 기록을 구성합니다.
- 모니터링되는 장치가 Kaspersky Industrial CyberSecurity for Networks에서 제거되면 해당 장치는 Kaspersky Security Gateway 콘솔의 **Tracked data** 섹션에 더 이상 표시되지 않습니다. 그러나 해당 장치에 대해서는 **<Device name>**의 값이 `-1`인 태그와 **UnauthorizedSystemCommandCount**의 값이 `0`인 태그가 계속 전송됩니다. 원격 장치에 대한 데이터 전송을 중지하려면 다음과 같이 하십시오.

  1. Kaspersky Security Gateway 콘솔 열기
  2. **Kaspersky Security Gateway** 노드에서 사용되는 프로토콜을 선택합니다.
  3. 결과 창의 **Tracked data**에서 **Change** 링크를 클릭합니다.

     Selecting tracked data 창이 열립니다.
  4. 변경할 필요가 없습니다. **OK**을 클릭하여 창을 닫습니다.

Kaspersky Security Gateway Console 인터페이스

Kaspersky Security Gateway Console은 **Kaspersky Security Gateway**라는 이름의 노드 형식으로 Microsoft Management Console(Microsoft 관리 콘솔) 트리에 표시됩니다.

콘솔 트리에는 SCADA 시스템에서 사용할 데이터 전송 프로토콜을 구성하기 위한 **Kaspersky Security Gateway** 노드 및 하위 노드가 표시됩니다:

- **IEC 60870-5-104**.
- **OPC DA**.
- **OPC UA**.

Kaspersky Security Gateway 노드의 결과 창은 다음을 표시합니다:

- Kaspersky Security Gateway에 관한 일반 정보.
- Kaspersky Security Center 및 Kaspersky Industrial CyberSecurity for Networks에 연결하기 위한 설정 그리고 설정 창으로의 링크에 관한 상세 정보.
- 현재 Kaspersky Security Gateway 추가 설정 및 설정 창으로의 링크에 관한 세부 정보.

Kaspersky Security Center와의 연결 구성

Kaspersky Security Center에 대한 연결을 구성하려면:

1. Kaspersky Security Gateway 콘솔 열기
2. **Kaspersky Security Gateway** 노드를 선택합니다.
3. 결과 창의 **Connection Settings** 섹션에서 **Configure connection** 링크를 클릭합니다.

   Connection Settings 창이 열립니다.
4. **Kaspersky Security Center**에서 Kaspersky Security Center 중앙 관리 서버 연결 설정을 지정합니다.
   - **Server**. Kaspersky Security Center 중앙 관리 서버의 IP 주소나 도메인 이름과 해당 연결에 사용된 포트 번호. 중앙 관리 서버 연결 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오. 포트 번호로 가능한 값 범위: 1~65535.
   - **User name**. Kaspersky Security Center 중앙 관리 서버 관리자의 계정 이름입니다.
   - **Password**. Kaspersky Security Center 중앙 관리 서버 관리자의 계정 암호입니다.

5. 연결 유형:

- **Disabled**. Kaspersky Security Center 중앙 관리 서버에 연결할 수 없습니다.
- **Open API**. Open API 인터페이스를 데이터 공급자로 선택하면, 신뢰하는 루트 인증 기관(CA)의 인증서 저장소에 **Kaspersky Security Center 루트 인증서를 내보내고** 설치해야 합니다. Open API 데이터 공급자의 경우 기본 포트 번호는 13299입니다.

  1. 브라우저에서 `https://<Web Console address>:13299`를 입력합니다.
  2. 브라우저에서 Kaspersky Security Center 웹 콘솔에 설정한 연결의 인증서 정보를 엽니다.
  3. **인증서** 창에서 **인증서 경로** 탭을 선택합니다.
  4. 루트 인증서를 선택합니다.
  5. **상세 정보** 탭으로 갑니다.
  6. **파일에 복사** 버튼을 클릭하여 선택한 인증서를 내보냅니다.

- **klakaut**. *klakaut*는 Kaspersky Security Center 자동화 유틸리티로, COM(Component Object Model) 개체를 사용하여 외부 API를 통해 Kaspersky Security Center 중앙 관리 서버를 관리할 수 있습니다. klakaut 유틸리티를 데이터 공급자로 선택한 경우 Kaspersky Security Center 관리 콘솔을 설치한 후 같은 컴퓨터에 Kaspersky Security Gateway를 설치합니다. Klakaut 데이터 공급자의 기본 포트 번호는 13291입니다. 이 옵션은 기본적으로 선택되어 있습니다.

  Kaspersky Security Gateway 설치 후에 Kaspersky Security Center 관리 콘솔을 설치하면 Kaspersky Security Gateway와 Kaspersky Security Center 중앙 관리 서버 간의 연결을 구성할 수 없습니다.

- **Automatically**. 애플리케이션은 klakaut 및 Open API을 사용하여 Kaspersky Security Center 중앙 관리 서버에 연결을 시도합니다. 버전 4.5 이하에서 버전 5.0으로 Kaspersky Security Gateway를 업데이트한 후에는 이 옵션이 기본적으로 선택됩니다.

  Automatic 연결 유형은 이전 버전 위에 새 버전의 Kaspersky Security Gateway를 설치한 후에만 사용할 수 있습니다. 연결 유형을 변경하면 이 옵션은 더 이상 드롭다운 목록에 표시되지 않습니다.

6. **Connection scan** 버튼을 클릭합니다.

   연결이 설정되면 *Connected* 상태가 표시됩니다.

7. **OK** 버튼을 클릭합니다.

8. **OK** 버튼을 클릭해 **Kaspersky Security Gateway** 창을 닫습니다.

`C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 폴더에 있는 `ConnectionSettings.xml` 구성 파일을 사용하여 연결 설정을 구성할 수도 있습니다. 구성 파일에서는 암호를 설정할 수 없습니다. Kaspersky Security Gateway Console을 사용하여 암호를 설정하십시오.

Kaspersky Industrial CyberSecurity for Networks와의 연결 구성

Kaspersky Industrial CyberSecurity for Networks와의 연결을 구성하려면

1. Kaspersky Security Gateway 콘솔 열기
2. **Kaspersky Security Gateway** 노드를 선택합니다.
3. 결과 창의 **Connection Settings** 섹션에서 **Configure connection** 링크를 클릭합니다.

   Connection Settings 창이 열립니다.
4. **Kaspersky Industrial CyberSecurity for Networks**에서, Kaspersky Industrial CyberSecurity for Networks 서버 하나 이상에 대한 연결 설정을 추가합니다:

   a. **Add** 버튼을 클릭합니다.

   Kaspersky Industrial CyberSecurity for Networks connection settings 창이 열립니다.

   b. 이전에 Kaspersky Industrial CyberSecurity for Networks에 추가한 일반 유형 커넥터의 IP 주소를 연결에 사용한 포트 번호와 함께 입력합니다. 포트 번호로 가능한 값 범위: 1~65535.

   > 커넥터 연결 설정이 Kaspersky Industrial CyberSecurity for Networks 통합 서버의 연결 설정과 다릅니다. 커넥터에 대한 자세한 내용은 Kaspersky Industrial CyberSecurity for Networks 도움말을 참조하십시오.

   c. Kaspersky Industrial CyberSecurity for Networks와 신뢰할 수 있는 연결을 구성하려면:

      1. **Use pinned certificate to secure connection** 확인란을 선택합니다.
      2. **Load** 버튼을 클릭합니다.
      3. 창이 열리면 TLS 인증서가 있는 파일을 선택합니다.
      4. **열기**를 클릭합니다.

   추가된 TLS 인증서에 관한 정보는 **TLS certificate data**에 표시됩니다.

   > 연결 보호를 위해 고정 인증서를 지정했다면, 클라이언트 인증서도 지정해야 합니다. 그렇지 않으면 Kaspersky Industrial CyberSecurity for Networks와의 연결을 설정할 수 없습니다.

   d. 클라이언트 인증서를 사용하여 연결 보호를 추가로 구성하려면:

      1. **Secure connection with client certificate** 확인란을 선택합니다.
      2. **Load** 버튼을 클릭합니다.
      3. 창이 열리면 클라이언트 인증서가 있는 PFX 파일을 선택합니다.

4. **열기**를 클릭합니다.

5. 이름이 같은 필드에 클라이언트 인증서의 암호(있다면)를 입력합니다.

e. **Test connection** 버튼을 클릭합니다.
연결이 설정되면 *Connected* 상태가 표시됩니다.

f. **OK** 버튼을 클릭합니다.

g. 필요하다면, a~f 단계를 반복하여 다른 Kaspersky Industrial CyberSecurity for Networks 서버를 위한 연결 설정을 추가합니다.

Kaspersky Industrial CyberSecurity for Networks 연결 정보는 **Connection settings** 창의 목록에 표시됩니다.

5. **확인**을 누릅니다.

`C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 폴더에 있는 `ConnectionSettings.xml` 구성 파일을 사용하여 연결 설정을 구성할 수도 있습니다. 구성 파일에서는 암호를 설정할 수 없습니다. Kaspersky Security Gateway Console을 사용하여 암호를 설정하십시오.

DCOM 프로토콜 구성

OPC DA 프로토콜을 통해 데이터를 주고받는 데 관련된 컴퓨터가 Active Directory 도메인에 가입되어 있지 않은 경우, 이러한 각 컴퓨터에 대해 같은 이름과 암호의 사용자 계정을 만드십시오.

OPC DA 연결을 설정하려면 분산 구성 요소 개체 모델(DCOM) 프로토콜에 대한 접근 권한을 구성합니다.

한 컴퓨터에 설치된 Kaspersky Security Gateway와 SCADA 시스템 간의 상호 작용을 위해 DCOM 프로토콜을 구성하는 방법

1. Kaspersky Security Gateway와 SCADA 시스템이 설치된 컴퓨터에서 상호 작용을 구성할 컴퓨터에서 **Win+R** 키 조합을 누릅니다.
표준 Microsoft Windows **실행** 창이 열립니다.

2. **열기** 필드에 *dcomcnfg*를 입력하고 **확인**을 클릭합니다.
구성 요소 서비스 창이 열립니다.

3. 창 왼쪽의 폴더 트리에서 **구성 요소 서비스** → **컴퓨터** → **내 컴퓨터**를 선택합니다.

4. **내 컴퓨터** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.

5. **내 컴퓨터 속성** 창의 **COM 보안** 탭을 선택합니다.

6. **접근 권한**에서 **기본값 편집**을 클릭합니다.
접근 권한 창이 열립니다.

7. **그룹 또는 사용자 이름**에서, **네트워크 서비스** 그룹을 선택합니다.

8. **네트워크 서비스** 그룹의 권한 표의 **허용** 열에서, **로컬 접근** 및 **원격 접근** 확인란을 선택합니다.

9. **기본 속성** 탭을 선택하고 다음 값을 구성했는지 확인합니다: **기본 인증 레벨 –** *연결*, **기본 사칭 레벨** – *식별*.

10. **확인**을 누릅니다.

11. **속성: 내 컴퓨터** 창의 **확인** 버튼을 클릭합니다.

12. 컴퓨터 다시 시작.

Kaspersky Security Gateway와 다른 컴퓨터에 설치된 SCADA 시스템 간의 상호 작용을 위해 DCOM 프로토콜을 구성하는 방법

두 컴퓨터에서:

1. **Win+R** 키 조합을 누릅니다.
   표준 Microsoft Windows **실행** 창이 열립니다.

2. **열기** 필드에 *dcomcnfg*를 입력하고 **확인**을 클릭합니다.
   구성 요소 서비스 창이 열립니다.

3. 창 왼쪽의 폴더 트리에서 **구성 요소 서비스** → **컴퓨터** → **내 컴퓨터**를 선택합니다.

4. **내 컴퓨터** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.

5. **내 컴퓨터 속성** 창의 **COM 보안** 탭을 선택합니다.

6. **접근 권한** 섹션에서 **제한 편집** 버튼을 클릭합니다.
   접근 권한 창이 열립니다.

7. **그룹 또는 사용자 이름** 섹션에서 **ANONYMOUS LOGON** 그룹을 선택합니다.

8. **익명 로그인** 그룹의 권한 표의 **허용** 열에서, **로컬 접근** 및 **원격 접근** 확인란을 선택합니다.

   ANONYMOUS LOGON 그룹에 대한 원격 접근을 허용하면 시스템의 보안 레벨에 영향을 줍니다. 이 권한 없이 OPC DA 프로토콜의 기능을 테스트하는 것이 좋습니다. 이 권한 없이 작업이 불가능한 경우에만 권한을 부여하십시오.

9. **접근 권한**에서, **기본값 편집**을 클릭하고 지침의 7~8단계를 반복합니다.

10. **시작 및 활성화 권한**에서 **제한 편집**을 클릭하고 지침의 7~8단계를 반복합니다.

11. **시작 및 활성화 권한**에서 **기본값 편집**을 클릭하고 지침의 7~8단계를 반복합니다.

12. **기본 속성** 탭에서 다음 값을 구성했는지 확인합니다: **기본 인증 레벨 –** *연결*, **기본 사칭 레벨** – *식별*.

13. **확인**을 누릅니다.

14. **속성: 내 컴퓨터** 창의 **확인** 버튼을 클릭합니다.

15. OPCEnum 애플리케이션을 구성합니다.

    a. 창 왼쪽의 폴더 트리에서 **구성 요소 서비스** → **컴퓨터** → **내 컴퓨터** → **DCOM 구성** → **OPCEnum**을 선택합니다.

    b. 마우스 오른쪽 버튼을 클릭해 **OPCEnum**의 마우스 오른쪽 메뉴를 표시하고 **속성**을 선택합니다.

    이는 **속성: OPCEnum** 창을 엽니다.

    c. **일반** 탭에서 **기본 인증 레벨**을 *연결*로 설정했는지 확인합니다.

    d. **보안** 탭의 **시작 및 활성화 권한**에서 **편집**을 클릭합니다.

    e. **그룹 또는 사용자 이름**에서 **전체** 그룹을 선택합니다.

    f. **전체** 그룹 권한 표의 **허용** 열에서 **로컬 접근**, **원격 접근**, **로컬 활성화**, **원격 활성화** 확인란을 선택합니다.

    g. **접근 권한** 섹션에서 **편집** 버튼을 클릭합니다.

    h. **그룹 또는 사용자 이름**에서 **전체** 그룹을 선택합니다.

    i. **전체** 그룹의 권한 표의 **허용** 열에서 **로컬 접근** 및 **원격 접근** 확인란을 선택합니다.

    j. **신원** 탭에서 **시스템 계정**을 선택합니다.

    k. **확인**을 누릅니다.

16. 컴퓨터 다시 시작.

Kaspersky Security Gateway 유틸리티가 설치된 컴퓨터에서:

1. **Win+R** 키 조합을 누릅니다.

   표준 Microsoft Windows **실행** 창이 열립니다.

2. **열기** 필드에 *dcomcnfg*를 입력하고 **확인**을 클릭합니다.

   구성 요소 서비스 창이 열립니다.

3. 창 왼쪽의 폴더 트리에서 **구성 요소 서비스** → **컴퓨터** → **내 컴퓨터** → **DCOM 구성** → **Kaspersky Gateway OPC Service**를 선택합니다.

4. **Kaspersky Gateway OPC Service**의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.

   속성: Kaspersky Gateway OPC Service 창이 열립니다.

5. **일반** 탭에서 **기본 인증 레벨**을 *연결*로 설정했는지 확인합니다.

6. **확인**을 누릅니다.

7. Kaspersky Security Gateway와 SCADA 시스템을 다른 도메인에 속하는 컴퓨터에 설치했다면:

   a. 운영 체제에서 **제어판 – 관리 도구 – 로컬 보안 정책**을 엽니다.

   b. 로컬 보안 정책 콘솔 트리에서 **로컬 정책 – 보안 옵션** 섹션을 선택합니다.

   c. **보안 옵션** 섹션의 작업 영역에서, **네트워크 액세스: 모든 사용자 권한을 익명의 사용자에게 적용하도록 허용** 로컬 정책의 마우스 오른쪽 메뉴에서 **사용**을 선택합니다.

8. 컴퓨터 다시 시작.

통신 프로토콜을 사용하여 데이터 전송 설정 구성

이 섹션에서는 이용 가능한 통신 프로토콜을 사용하여 데이터 전송을 구성하는 방법에 대한 지침을 제공합니다.

IEC 60870-5-104 프로토콜을 사용하여 데이터 전송 구성

Kaspersky Security Gateway Console을 사용해 IEC 60870-5-104 프로토콜을 통한 데이터 전송을 구성하려면:

1. Kaspersky Security Gateway 콘솔 열기
2. **Kaspersky Security Gateway** 노드에서 **IEC 60870-5-104**를 선택합니다.
3. 결과 창의 **Data transmission settings** 섹션에서 **Change** 링크를 클릭합니다.
   Settings 창이 열립니다.
4. **Transmission settings** 섹션에서 **Enable data transmission** 옵션을 활성화하거나 비활성화합니다.
   이 기능을 활성화하면 Kaspersky Security Gateway는 산업 네트워크 노드의 보호 상태를 SCADA 시스템으로 전송합니다. 이 기능은 기본적으로 비활성화됩니다.
5. **Connection settings** 그룹 상자에서 다음을 구성할 수 있습니다:
   - **Device address**. SCADA 시스템에서 컴퓨터에 할당된 보조 주소입니다. 가능한 값 범위: 1~65535.
   - **Device port**. SCADA 시스템 연결을 설정하기 위한 포트 번호입니다. 가능한 값 범위: 1~65535.
   - **TCP connection timeout**. 값은 초 단위로 지정됩니다. 가능한 값 범위: 1~255.
   - **Message send timeout**. 값은 초 단위로 지정됩니다. 가능한 값 범위: 1~255.
   - **Message confirmation timeout**. 값은 초 단위로 지정됩니다. 가능한 값 범위: 1~255.
   - **Test connection timeout**. 값은 초 단위로 지정됩니다. 가능한 값 범위: 1~255.
   - **Maximum unconfirmed received messages allowed**. 가능한 값 범위: 1~32767.
   - **Maximum unconfirmed sent messages allowed**. 가능한 값 범위: 1~32767.
6. **OK** 버튼을 클릭합니다.

7. 결과 창의 **Tracked data** 섹션에서 **Change** 링크를 클릭합니다.

   Selecting tracked data 창이 열립니다. 이 목록은 Kaspersky Security Center 및 Kaspersky Industrial CyberSecurity for Networks와 같은 데이터 소스에 연결한 후 자동으로 추가된 추적 데이터를 표시합니다.

8. 컴퓨터 이름 옆의 확인란을 선택하거나 선택 해제하여 컴퓨터의 가용성 및 보호 상태 추적을 활성화하거나 비활성화합니다. 컴퓨터에서 이용 가능한 보호 애플리케이션과 네트워크 에이전트가 실행 중입니다.

   추적이 활성화되면 데이터가 SCADA 시스템으로 전송됩니다.

   추적이 비활성화되면 데이터가 SCADA 시스템으로 전송되지 않습니다.

   > 컴퓨터 또는 Kaspersky Security Gateway와 Kaspersky Security Center 중앙 관리 서버가 연결되어 있지 않으면 값 `-1`(컴퓨터 상태를 검색할 수 없음)이 전송됩니다.

9. 필요하다면 **Service tag** 열에서 서비스 태그를 편집하거나 추가하십시오. 서비스 태그를 사용하여 SCADA 시스템에서 받은 데이터를 필터링할 수 있습니다. 태그는 숫자로만 구성할 수 있습니다.

10. **OK** 버튼을 클릭합니다.

`ProtocolEICSettings.xml` 구성 파일(`C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 폴더에 있음)을 사용하여 IEC 60870-5-104 프로토콜을 통한 데이터 전송을 구성할 수 있습니다.

OPC DA 프로토콜을 사용하여 데이터 전송 구성

OPC DA 프로토콜을 통해 데이터를 성공적으로 전송하려면 다음 사전 요구 사항이 충족되어야 합니다.

- 필요한 DCOM 권한이 SCADA 시스템과 Kaspersky Security Gateway 양쪽에서 OPCEnum에 할당됩니다.
- Kaspersky Security Gateway가 설치된 컴퓨터와 SCADA 시스템에 대해 통합 인증이 설정됩니다. 도메인 인증을 사용하거나 작업 그룹의 모든 컴퓨터에 같은 사용자 이름/암호를 사용합니다.

Kaspersky Security Gateway Console을 사용하여 OPC DA 프로토콜을 통한 데이터 전송을 구성하려면:

1. Kaspersky Security Gateway 콘솔 열기
2. **Kaspersky Security Gateway** 노드에서 **OPC DA**를 선택합니다.
3. 결과 창의 **Data transmission settings** 섹션에서 **Change** 링크를 클릭합니다.

   Settings 창이 열립니다.

4. **Enable data transmission** 옵션을 비활성화 또는 활성화하십시오.

   이 기능을 활성화하면 Kaspersky Security Gateway는 산업 네트워크 노드의 보호 상태를 SCADA 시스템으로 전송합니다. 이 기능은 기본적으로 비활성화됩니다.

5. **OK** 버튼을 클릭합니다.
6. 결과 창의 **Tracked data** 섹션에서 **Change** 링크를 클릭합니다.

   Selecting tracked data 창이 열립니다. 이 목록은 Kaspersky Security Center 및 Kaspersky Industrial CyberSecurity for Networks와 같은 데이터 소스에 연결한 후 자동으로 추가된 추적 데이터를 표시합니다.

7. 컴퓨터 이름 옆의 확인란을 선택하거나 선택 해제하여 컴퓨터의 가용성 및 보호 상태 추적을 활성화하거나 비활성화합니다. 컴퓨터에서 이용 가능한 보호 애플리케이션과 네트워크 에이전트가 실행 중입니다.

   추적이 활성화되면 데이터가 SCADA 시스템으로 전송됩니다.

   추적이 비활성화되면 데이터가 SCADA 시스템으로 전송되지 않습니다.

   > 컴퓨터 또는 Kaspersky Security Gateway와 Kaspersky Security Center 중앙 관리 서버가 연결되어 있지 않으면 값 `-1`(컴퓨터 상태를 검색할 수 없음)이 전송됩니다.

8. 필요하다면 **Service tag** 열에서 서비스 태그를 편집하거나 추가하십시오. 서비스 태그를 사용하여 SCADA 시스템에서 받은 데이터를 필터링할 수 있습니다. 태그는 숫자 또는 문자를 포함할 수 있습니다.

9. **OK** 버튼을 클릭합니다.

`ProtocolOPCSettings.xml` 구성 파일(`C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 폴더에 있음)을 사용하여 OPC DA 프로토콜을 통한 데이터 전송을 구성할 수 있습니다.

OPC UA 프로토콜을 사용하여 데이터 전송 구성

Kaspersky Security Gateway Console을 사용하여 OPC UA 프로토콜을 통한 데이터 전송을 구성하려면:

1. Kaspersky Security Gateway 콘솔 열기

2. **Kaspersky Security Gateway** 노드에서 **OPC UA**를 선택합니다.

3. 결과 창의 **Data transmission settings** 섹션에서 **Change** 링크를 클릭합니다.

   Settings 창이 열립니다.

4. **Enable data transmission** 옵션을 비활성화 또는 활성화하십시오.

   이 기능을 활성화하면 Kaspersky Security Gateway는 산업 네트워크 노드의 보호 상태를 SCADA 시스템으로 전송합니다. 이 기능은 기본적으로 비활성화됩니다.

5. **Connection settings**에서 SCADA 시스템 연결을 설정하기 위한 포트 번호입니다. 포트 번호로 가능한 값 범위: 1~65535.

6. **OK** 버튼을 클릭합니다.

7. 결과 창의 **Tracked data** 섹션에서 **Change** 링크를 클릭합니다.

   Selecting tracked data 창이 열립니다. 이 목록은 Kaspersky Security Center 및 Kaspersky Industrial CyberSecurity for Networks와 같은 데이터 소스에 연결한 후 자동으로 추가된 추적 데이터를 표시합니다.

8. 컴퓨터 이름 옆의 확인란을 선택하거나 선택 해제하여 컴퓨터의 가용성 및 보호 상태 추적을 활성화하거나 비활성화합니다. 컴퓨터에서 이용 가능한 보호 애플리케이션과 네트워크 에이전트가 실행 중입니다.

   추적이 활성화되면 데이터가 SCADA 시스템으로 전송됩니다.

   추적이 비활성화되면 데이터가 SCADA 시스템으로 전송되지 않습니다.

   > 컴퓨터 또는 Kaspersky Security Gateway와 Kaspersky Security Center 중앙 관리 서버가 연결되어 있지 않으면 값 `-1`(컴퓨터 상태를 검색할 수 없음)이 전송됩니다.

9. 필요하다면 **Service tag** 열에서 서비스 태그를 편집하거나 추가하십시오. 서비스 태그를 사용하여 SCADA 시스템에서 받은 데이터를 필터링할 수 있습니다. 태그는 숫자 또는 문자를 포함할 수 있습니다.

10. **OK** 버튼을 클릭합니다.

`ProtocolOPCUASettings.xml` 구성 파일(`C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 폴더에 있음)을 사용하여 OPC UA 프로토콜을 통한 데이터 전송을 구성할 수 있습니다.

구성 파일을 사용하여 데이터 전송 구성

구성 파일을 편집하려면 전문 지식이 필요합니다. 구성 파일을 잘못 편집하면 Kaspersky Security Gateway 오류가 발생할 수 있습니다.

구성 파일을 사용하여 데이터 전송을 구성하려면:

1. 텍스트 편집기에서 `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 폴더의 Kaspersky Security Gateway 설정이 있는 구성 파일을 엽니다.
   - `ProtocolIECSettings.xml`은 IEC 60870-5-104 프로토콜의 구성 파일입니다.
   - `ProtocolOPCSettings.xml`은 OPC DA 프로토콜의 구성 파일입니다.
   - `ProtocolOPCUASettings.xml`은 OPC UA 프로토콜의 구성 파일입니다.
2. 데이터 전송 설정을 구성합니다.
3. 구성 파일을 저장합니다.
4. Kaspersky Security Gateway 서비스를 다시 시작하여 새 설정을 적용하십시오.

Kaspersky Security Gateway 추가 설정 구성

Kaspersky Security Gateway의 추가 설정을 구성하려면:

1. Kaspersky Security Gateway 콘솔 열기
2. **Kaspersky Security Gateway** 노드를 선택합니다.
3. 결과 창의 **Application Settings** 섹션에서 **Configure application settings** 링크를 클릭합니다.
   Application settings 창이 열립니다.
4. **Interrogation** 섹션에서 **Interrogation period (sec)** 값을 설정하십시오.

5. **System tracing** 섹션에서:

   - **Enable tracing** 확인란을 선택하거나 선택 해제합니다.
   - 드롭다운 목록에서 기록할 정보의 **Level**을 선택합니다.

6. **Application settings** 창에서 **OK** 버튼을 클릭합니다.

`AppSettings.xml` 구성 파일(`C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 폴더에 있음)을 사용하여 Kaspersky Security Gateway의 고급 설정을 구성할 수 있습니다.

Kaspersky Security Gateway 이벤트 보기

Kaspersky Security Gateway 동작 중에는 다음 이벤트가 발생할 수 있습니다:

- Kaspersky Security Gateway 서비스를 활성화 및 비활성화합니다.
- Kaspersky Security Gateway와 SCADA 시스템 간의 통신에 문제가 있습니다.
- Kaspersky Security Center 중앙 관리 서버에 연결하고 중앙 관리 서버에서 데이터를 수신하는 데 문제가 있습니다.
- Kaspersky Security Gateway 구성 파일에 접근하는 데 문제가 있습니다.

이러한 이벤트에 대한 정보는 `%ProgramData%\Kaspersky Lab\Security Gateway\Traces` 폴더에 저장된 추적 파일에 기록됩니다.

BitLocker 전체 디스크 암호화 관리

*BitLocker*는 Windows 운영 체제에 내장된 암호화 기술입니다. Kaspersky Industrial CyberSecurity for Nodes를 사용하면 Kaspersky Security Center를 통해 Bitlocker를 제어하고 관리할 수 있습니다. BitLocker는 논리 볼륨을 암호화합니다. BitLocker에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

Kaspersky Industrial CyberSecurity for Nodes는 Windows Vista 및 Windows Server 2008 컴퓨터에서 BitLocker 관리를 지원하지 않습니다.

디스크를 암호화할 때 BitLocker는 부트 로더 및 기타 보조 파일을 system partition에 넣습니다. 이 파티션은 암호화되지 않았습니다. 운영 체제는 Windows 설치 중 시스템 파티션을 자동 생성합니다. Windows를 설치하기 전에 디스크를 완전히 분할하면 운영 체제가 시스템 파티션을 생성할 수 없습니다. 이때는 BitLocker 디스크 암호화를 시작하면 운영 체제에서 사용자에게 디스크를 다시 분할하고 시스템 파티션을 만들라는 메시지를 표시합니다. 시스템 파티션을 생성하면 운영 체제가 BitLocker 암호화를 시작합니다.

Kaspersky Industrial CyberSecurity for Nodes는 이동식 드라이브의 BitLocker 암호화를 지원하지 않습니다.

BitLocker는 신뢰하는 플랫폼 모듈을 사용하여 접근 허용 키를 안전하게 저장합니다. *Trusted Platform Module* (TPM, 신뢰하는 플랫폼 모듈)은 보안 관련 기본 기능을 제공하도록 개발된 마이크로칩(예: 암호화 키 저장)입니다. 신뢰하는 플랫폼 모듈은 보통 컴퓨터 마더보드에 설치하고 하드웨어 버스를 통해 다른 모든 시스템 구성 요소와 상호 작용합니다. TPM은 시작 전 시스템 무결성 확인을 제공하므로 TPM을 사용하는 것이 BitLocker 접근 허용 키를 저장하는 가장 안전한 방법입니다. TPM 없이도 여전히 컴퓨터에서 드라이브를 암호화할 수 있습니다. 이 경우 접근 허용 키는 암호로 암호화됩니다. BitLocker는 다음 인증 방법을 사용합니다:

- TPM
- TPM 및 PIN
- 암호

드라이브를 암호화하기 전에 BitLocker는 복구 키를 생성합니다. Kaspersky Industrial CyberSecurity for Nodes는 복구 키를 읽어 Kaspersky Security Center로 전송하므로, 예를 들어 사용자가 암호를 잊어버린 경우 디스크에 대한 접근을 복원할 수 있습니다.

시스템 하드 드라이브를 암호화한 후, 운영체제를 부팅하려면 BitLocker 인증을 거쳐야 합니다. 인증 후 BitLocker가 사용자의 로그인을 허용합니다. BitLocker는 SSO(single sign-on) 기술을 지원하지 않습니다.

사용자가 BitLocker를 사용하여 디스크를 암호화하는 경우 Kaspersky Industrial CyberSecurity for Nodes는 디스크 암호화 정보와 복구 키를 Kaspersky Security Center로 전송합니다.

Windows 그룹 정책을 사용하는 경우 정책 설정에서 BitLocker 매니지먼트를 해제합니다. Windows 정책 설정이 Kaspersky Industrial CyberSecurity for Nodes 정책 설정과 충돌할 수 있습니다. 드라이브를 암호화할 때 오류가 발생할 수 있습니다.

BitLocker 드라이브 암호화 시작

전체 디스크 암호화를 시작하기 전에 컴퓨터가 감염되지는 않았는지 확인하는 것이 좋습니다. 그렇게 하려면, 전체 검사 또는 중요 영역 검사 작업을 시작합니다. 루트킷에 감염된 컴퓨터에서 전체 디스크 암호화를 수행하면 컴퓨터가 작동하지 않을 수 있습니다.

서버용 Windows 운영 체제를 실행하는 컴퓨터에서 BitLocker 드라이브 암호화를 사용하려면 BitLocker 드라이브 암호화 구성 요소를 설치해야 합니다. 운영 체제 도구(역할 및 구성 요소 추가 마법사)를 사용하여 구성 요소를 설치합니다. BitLocker 드라이브 암호화에 대한 자세한 내용은 Microsoft 문서를 참조하십시오.

Kaspersky Security Center 관리 콘솔에서 BitLocker 드라이브 암호화 작업을 실행하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **데이터 암호화** 섹션을 선택합니다.
4. **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 암호화** 옵션을 선택합니다.

   여러 운영 체제가 설치된 컴퓨터인 경우 암호화 후 암호화가 수행된 운영 체제만 로드할 수 있습니다.

5. 고급 BitLocker 드라이브 암호화 옵션을 구성하십시오(아래 표 참조).
6. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 BitLocker 드라이브 암호화 작업을 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **데이터 암호화** 섹션으로 갑니다.
5. **전체 디스크 암호화** 하위 섹션에서 **구성** 버튼을 클릭합니다.
6. **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 암호화** 옵션을 선택합니다.

   여러 운영 체제가 설치된 컴퓨터인 경우 암호화 후 암호화가 수행된 운영 체제만 로드할 수 있습니다.

7. 고급 BitLocker 드라이브 암호화 옵션을 구성하십시오(아래 표 참조).
8. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

애플리케이션 콘솔을 사용하여 사용자 컴퓨터의 디스크 암호화 또는 복호화 프로세스를 제어할 수 있습니다.

정책을 적용한 후 인증 설정에 따라 애플리케이션은 간편 진단 인터페이스 창 또는 애플리케이션 콘솔에 다음 요청을 표시합니다.

- TPM만. 사용자 입력 필요 없음. 컴퓨터 다시 시작 시 디스크가 암호화됩니다.
- TPM + PIN/암호. TPM 모듈을 사용할 수 있는 경우 PIN 코드 프롬프트 창이 나타납니다. TPM 모듈을 사용할 수 없는 경우 preboot 인증을 위한 암호 프롬프트 창이 표시됩니다.
- 암호만. 사전 부팅 인증을 위한 암호 프롬프트 창이 표시됩니다.

컴퓨터 운영 체제에 연방 정보 처리 표준 호환 모드가 설정되어 있으면 Windows 8 이하 버전의 운영 체제에서 복구 키 파일을 저장할 저장 장치를 연결하라는 요청이 표시됩니다. 단일 저장 장치에 여러 복구 키 파일을 저장할 수 있습니다.

암호 또는 PIN 코드를 설정한 후 BitLocker는 컴퓨터와 BitLocker의 호환성을 확인하기 위해 사용자의 컴퓨터를 다시 시작할지 묻는 메시지를 표시합니다. Kaspersky Industrial CyberSecurity for Nodes는 간편 진단 인터페이스 창 또는 애플리케이션 콘솔에 해당 알림을 표시합니다. 다음으로, 사용자는 BitLocker 인증 절차를 거쳐야 합니다. 인증 절차 후 사용자는 시스템에 로그온해야 합니다. 운영 체제가 로드된 후 BitLocker가 암호화를 시작합니다.

사용자는 암호화 키에 접근할 수 없는 경우 로컬 네트워크 관리자에게 복구 키를 제공하도록 요청할 수 있습니다 (복구 키를 이전에 저장 장치에 저장하지 않았거나 분실한 경우).

BitLocker 드라이브 암호화 구성 요소 설정

파라미터	설명
태블릿에서 사전 부팅 키보드 입력이 필요한 BitLocker 인증 사용 활성화	플랫폼에서 부팅 전 입력 기능을 제공하지 않을 때(태블릿에서 터치스크린 키보드 사용 등)도 포함하여, 부팅 전 환경에서 데이터 입력이 필요한 인증 사용. 태블릿 컴퓨터의 터치 스크린은 preboot 환경에서 사용할 수 없습니다. 예를 들어 태블릿 컴퓨터에서 BitLocker 인증을 완료하려면 사용자가 USB 키보드를 연결해야 합니다. 이 확인란을 선택하면 부팅 전 입력이 필요한 인증 사용이 허용됩니다. 부팅 전 환경에서 대안적 데이터 입력 도구(예: 터치스크린 키보드 외에 USB 키보드)가 있는 장치에 한해 이 설정을 사용하는 것이 좋습니다. 확인란을 선택 취소하면 태블릿에서 BitLocker 드라이브 암호화를 사용할 수 없습니다.
하드웨어 암호화 사용 (Windows 8 이상)	이 확인란을 선택하면 애플리케이션이 하드웨어 암호화를 적용합니다. 이 방법을 사용하면 암호화 속도가 빨라지고 컴퓨터 리소스를 적게 사용합니다.
사용한 디스크 공간만 암호화 (Windows 8 이상)	이 확인란은 사용된 하드 드라이브 섹터 영역만 암호화하도록 제한하는 옵션을 작동하거나 중지합니다. 이렇게 제한하면 암호화 시간을 줄일 수 있습니다. 암호화 시작 후 **사용한 디스크 공간만 암호화(Windows 8 이상)** 기능을 활성화 또는 비활성화해도 하드 드라이브를 복호화하기 전까지는 이 설정이 수정되지 않습니다. 암호화를 시작하기 전에 확인란을 선택 또는 선택 해제해야 합니다. 이 확인란을 선택하면 하드 드라이브에서 파일이 저장되어 있는 부분만 암호화됩니다. Kaspersky Industrial CyberSecurity for Nodes는 추가되는 새 데이터를 자동으로 데이터를 암호화합니다. 확인란이 비어 있으면 이전에 삭제 및 수정되고 남은 파일 조각을 포함하여 전체 하드 드라이브가 암호화됩니다. 이 옵션은 데이터를 수정하거나 삭제하지 않은 새 하드 드라이브에 사용하는 것이 좋습니다. 이미 사용 중인 하드 드라이브에 암호화를 적용할 경우 전체 하드 드라이브를 암호화하는 것이 좋습니다. 이를 통해 복구 가능한 삭제된 데이터까지 포함하여 모든 데이터를 보호할 수 있습니다. 기본적으로 확인란의 선택이 취소됩니다.

파라미터	설명
인증 방법	**신뢰하는 플랫폼 모듈(TPM)** 이 옵션을 선택하면 BitLocker가 신뢰하는 플랫폼 모듈(TPM)을 사용합니다. 신뢰하는 플랫폼 모듈(TPM)은 보안 관련 기본 기능을 제공하도록 개발된 마이크로칩(예: 암호화 키 저장)입니다. 신뢰하는 플랫폼 모듈은 보통 컴퓨터 마더보드에 설치하고 하드웨어 버스를 통해 다른 모든 시스템 구성 요소와 상호 작용합니다. Windows 7 또는 Windows Server 2008 R2를 실행하는 컴퓨터의 경우 TPM 모듈을 사용한 암호화만 수행할 수 있습니다. TPM 모듈이 설치되어 있지 않으면 BitLocker 암호화를 사용할 수 없습니다. 이러한 컴퓨터에서 암호를 사용하는 것은 지원되지 않습니다. 신뢰하는 플랫폼 모듈이 설치된 장치는 장치에서만 복호화할 수 있는 암호화 키를 만들 수 있습니다. 신뢰하는 플랫폼 모듈은 고유의 루트 스토리지 키를 사용하여 암호화 키를 암호화합니다. 루트 스토리지 키는 신뢰하는 플랫폼 모듈 내에 저장됩니다. 암호화 키 해킹 시도에 맞서 추가적인 보호 수준을 제공할 수 있습니다. 이 처리 방법은 기본적으로 선택되어 있습니다. 암호화 키 접근에 대해 추가적으로 보호를 설정할 수 있으며, 키를 암호나 PIN로 암호화할 수 있습니다. **TPM에 PIN 사용**. 이 확인란을 선택하면, 사용자는 PIN 코드를 사용하여 신뢰하는 플랫폼 모듈(TPM) 내에 저장된 암호화 키에 접근할 수 있습니다. 이 확인란을 선택 해제하면 사용자는 PIN 코드를 사용할 수 없습니다. 암호화 키에 접근하려면 사용자가 암호를 입력해야 합니다. **신뢰하는 플랫폼 모듈(TPM), TPM을 사용할 수 없을 시 암호** 이 옵션을 선택하면 사용자는 신뢰하는 플랫폼 모듈(TPM)을 사용할 수 없을 때 암호화 키에 접근하기 위한 암호를 사용할 수 있습니다. 확인란의 선택을 취소하고 TPM를 사용할 수 없는 경우 전체 디스크 암호화가 시작되지 않습니다. **암호만(Windows 8 이상)** 이 옵션을 선택하면 사용자가 암호화된 드라이브에 접근하려고 시도할 때 Kaspersky Industrial CyberSecurity for Nodes가 사용자에게 암호 입력을 요구합니다. 신뢰하는 플랫폼 모듈(TPM)을 사용하지 않는 경우 이 옵션을 선택할 수 있습니다. 선택된 인증 방법은 암호 또는 PIN 요구 사항을 지정하여 구성해야 합니다. • **최소 PIN 길이(문자 수)**. • **강화 PIN(문자와 숫자) 사용**. 강화 PIN은 대문자와 소문자, 라틴 문자, 특수 문자 및 공백 등 숫자 외의 다른 문자도 사용할 수 있습니다. • **최소 암호 길이(문자 수)**. • **TPM에 대한 암호/PIN 유효 기간 제한(일)**.
자동으로 복구 키 재생성(일)	BitLocker로 보호되는 드라이브에 대한 접근 복원을 위한 암호를 자동으로 업데이트합니다. 확인란이 선택되면 복구 키 암호 유효 기간을 지정합니다.

BitLocker로 보호되는 하드 드라이브 복호화

사용자는 운영 체제를 사용하여 디스크를 복호화할 수 있습니다(*BitLocker 끄기* 기능). 그 후 Kaspersky Industrial CyberSecurity for Nodes는 디스크를 다시 암호화하라는 메시지를 표시합니다. 정책에서 디스크 복호화를 활성화하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 디스크를 암호화하라는 메시지를 표시합니다.

Kaspersky Security Center 관리 콘솔을 사용하여 BitLocker로 보호되는 하드 드라이브를 복호화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **데이터 암호화** 섹션을 선택합니다.
4. **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 복호화** 옵션을 선택합니다.
5. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔을 사용하여 BitLocker로 보호되는 하드 드라이브를 복호화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **데이터 암호화** 섹션으로 갑니다.
5. **전체 디스크 암호화** 하위 섹션에서 **구성** 버튼을 클릭합니다.
6. **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 복호화** 옵션을 선택합니다.
7. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

애플리케이션 콘솔을 사용하여 디스크 암호화 또는 복호화 프로세스를 제어할 수 있습니다.

BitLocker로 보호되는 드라이브에 대한 접근 복원

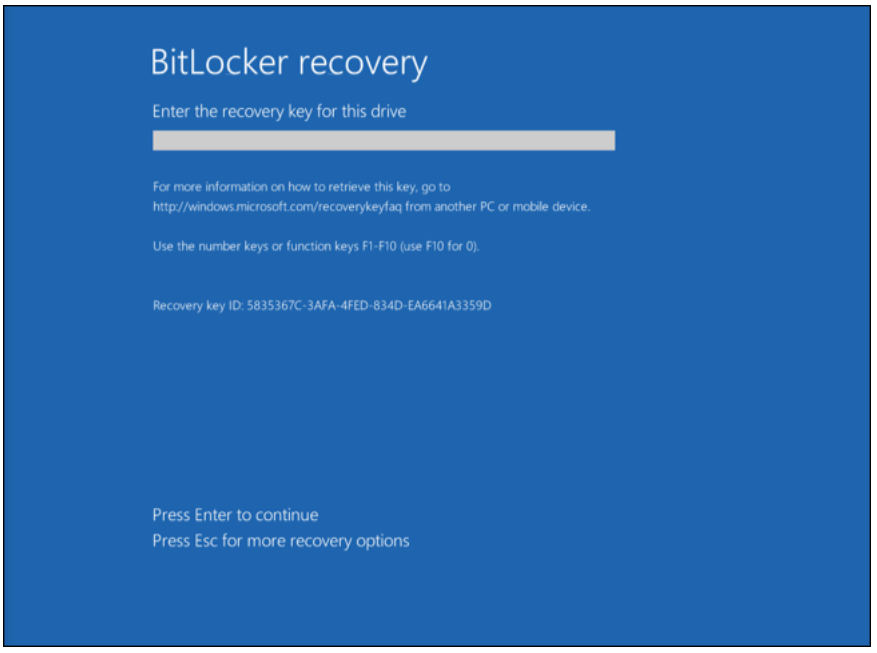
사용자가 BitLocker로 암호화된 하드 드라이브에 접근하기 위한 암호를 잊어버린 경우 복원 절차(요청-응답)를 시작해야 합니다.

> 컴퓨터 운영 체제에 FIPS(연방 정보 처리 표준) 호환 모드가 설정되어 있는 경우 Windows 8 이하 버전에서는 복구 키 파일이 암호화 전에 이동식 드라이브에 저장됩니다. 드라이브에 대한 접근을 복원하려면 이동식 드라이브를 삽입하고 화면의 지침을 따릅니다.

BitLocker로 암호화된 하드 드라이브에 대한 접근 복원은 다음 단계로 구성됩니다.

1. 사용자는 관리자에게 복구 키 ID를 알려줍니다(아래 그림 참조).
2. 관리자는 Kaspersky Security Center의 컴퓨터 속성에서 복구 키의 ID를 확인합니다. 사용자가 제공한 ID는 컴퓨터 속성에 표시된 ID와 일치해야 합니다.
   복구 키 ID가 일치하면 관리자가 복구 키를 사용자에게 전달합니다.

3. 사용자는 복구 키를 입력하고 하드 드라이브에 접근할 수 있습니다.



BitLocker로 암호화된 하드 드라이브에 대한 접근 복원

시스템 드라이브에 대한 접근 복원

복원 절차를 시작하려면 부팅 전 인증 단계에서 **Esc** 키를 눌러야 합니다.

Kaspersky Security Center 관리 콘솔에서 BitLocker로 암호화된 시스템 드라이브의 복구 키를 보는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기**을 선택합니다.
2. **기기** 탭으로 갑니다.
3. 암호화된 데이터 접근 복구를 요청한 사용자 컴퓨터의 마우스 오른쪽 메뉴를 엽니다.
4. 마우스 오른쪽 메뉴에서 **오프라인 모드에서의 접근 권한 부여**를 선택합니다.
5. 사용자에게 BitLocker 암호 입력 창에 표시된 복구 키 ID를 묻고 **복구 키 ID** 필드(**BitLocker로 보호된 시스템 드라이브에 접근** 탭에 있음)에 있는 ID와 비교합니다.

   ID가 일치하지 않으면 지정된 시스템 드라이브에 대한 접근을 복원하는 데 이 키를 사용할 수 없습니다. 선택한 컴퓨터 이름이 사용자 컴퓨터의 이름이 맞는지 확인합니다.

6. 사용자에게 **복구 키** 필드에 표시된 키를 전송합니다.

Kaspersky Security Center 웹 콘솔에서 BitLocker로 암호화된 시스템 드라이브의 복구 키를 보는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.
2. 드라이브에 대한 접근을 복원하려는 컴퓨터 이름 옆의 확인란을 선택합니다.
3. **오프라인 모드인 기기에 접근 권한 부여** 버튼을 클릭합니다.

4. 복구 키 ID를 확인합니다. 사용자가 제공한 ID는 컴퓨터 설정에 표시된 ID와 일치해야 합니다.

   ID가 일치하지 않으면 지정된 시스템 드라이브에 대한 접근을 복원하는 데 이 키를 사용할 수 없습니다. 선택한 컴퓨터 이름이 사용자 컴퓨터의 이름이 맞는지 확인합니다.

5. **키 받기** 버튼을 클릭합니다.

6. 사용자에게 **복구 키** 필드에 표시된 키를 전송합니다.

운영 체제 로드 후 Kaspersky Industrial CyberSecurity for Nodes는 사용자에게 비밀번호나 PIN 코드를 변경하라는 메시지를 표시합니다. 새 암호나 PIN 코드를 설정하면 BitLocker가 새 복구 암호를 생성하고 애플리케이션은 Kaspersky Security Center에 해당 암호를 전송합니다.

비시스템 드라이브에 대한 접근 복원

복원 절차를 시작하려면 사용자는 드라이브에 대한 접근을 제공하는 창에서 **암호를 잊으셨습니까** 링크를 클릭해야 합니다. 암호화된 드라이브에 대한 접근을 획득한 후 사용자는 BitLocker 설정에서 Windows 인증 중에 드라이브의 자동 잠금 해제를 활성화할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 BitLocker로 암호화된 비시스템 드라이브의 복구 키를 보는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **고급 → 데이터 암호화 및 보호 → 암호화된 드라이브** 폴더를 선택합니다.

2. 작업 공간에서 접근 허용 키 파일을 생성할 암호화된 장치를 선택하고 장치의 마우스 오른쪽 메뉴에서 **Kaspersky Industrial CyberSecurity for Nodes에서 장치에 대한 접근 권한 가져오기** 옵션을 클릭합니다.

3. 사용자에게 BitLocker 암호 입력 창에 표시된 복구 키 ID를 확인하고 **복구 키 ID** 필드의 ID와 비교합니다.

   ID가 일치하지 않으면 지정된 드라이브에 대한 접근을 복원하는 데 이 키를 사용할 수 없습니다. 선택한 컴퓨터 이름이 사용자 컴퓨터의 이름이 맞는지 확인합니다.

4. 사용자에게 **복구 키** 필드에 표시된 키를 전송합니다.

Kaspersky Security Center 웹 콘솔에서 BitLocker로 암호화된 비시스템 드라이브의 복구 키를 보는 방법

1. 웹 콘솔의 메인 창에서 **동작 → 데이터 암호화 및 보호 → 암호화된 드라이브** 옵션을 선택합니다.

2. 드라이브에 대한 접근을 복원하려는 컴퓨터 이름 옆의 확인란을 선택합니다.

3. **오프라인 모드인 기기에 접근 권한 부여** 버튼을 클릭합니다.
   장치에 대한 접근 권한을 부여하는 마법사가 시작됩니다.

4. 장치에 대한 접근 권한을 부여하려면 마법사의 지침을 따릅니다.

   a. Kaspersky Industrial CyberSecurity for Nodes 플러그인을 선택합니다.

   b. 복구 키 ID를 확인합니다. 사용자가 제공한 ID는 컴퓨터 설정에 표시된 ID와 일치해야 합니다.

   > ID가 일치하지 않으면 지정된 시스템 드라이브에 대한 접근을 복원하는 데 이 키를 사용할 수 없습니다. 선택한 컴퓨터 이름이 사용자 컴퓨터의 이름이 맞는지 확인합니다.

   c. **키 받기** 버튼을 클릭합니다.

5. 사용자에게 **복구 키** 필드에 표시된 키를 전송합니다.

소프트웨어 업데이트를 위해 BitLocker 보호 일시 중지

BitLocker 보호가 켜진 상태로 운영 체제 업데이트, 운영 체제 업데이트 패키지 설치 또는 다른 소프트웨어 업데이트 시 특별히 고려할 사항이 많습니다. 업데이트 설치 시 컴퓨터를 여러 번 다시 시작해야 할 수 있습니다. 다시 시작할 때마다 사용자는 BitLocker 인증을 완료해야 합니다. 업데이트를 올바르게 설치하기 위해 BitLocker 인증을 일시적으로 끌 수 있습니다. 이 경우 디스크는 암호화된 상태로 유지되고 사용자는 시스템에 로그인한 후 데이터에 접근할 수 있습니다. BitLocker 인증을 관리하려면 *BitLocker 보호 관리* 작업을 사용할 수 있습니다. 이 작업을 사용하여 BitLocker 인증을 거치지 않고 컴퓨터를 다시 시작할 횟수를 지정할 수 있습니다. 이 방법을 사용해 업데이트를 설치하고 *BitLocker 보호 관리* 작업을 완료하면, BitLocker 인증이 자동으로 활성화됩니다. BitLocker 인증은 언제든지 활성화할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 BitLocker 보호를 일시 중지하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **작업**을 선택합니다.
   작업 목록이 열립니다.

2. **새 작업** 버튼을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Industrial CyberSecurity for Nodes (5.0) → BitLocker 보호 관리 옵션을 선택합니다.

2단계. BitLocker 보호 관리

BitLocker 인증을 구성합니다. BitLocker 보호를 일시 중지하려면 **BitLocker 인증 건너뛰기 임시 허용** 옵션을 선택하고 BitLocker 인증 없이 다시 시작할 횟수를 입력합니다(1~15회). 필요하면 작업의 만료 날짜와 시간을 입력합니다. 지정한 시간이 되면 작업이 자동으로 꺼지고, 컴퓨터를 다시 시작할 때 사용자가 BitLocker 인증을 완료해야 합니다.

3단계. 작업을 할당할 장치 선택

작업을 수행할 컴퓨터를 선택합니다. 다음과 같은 옵션을 사용할 수 있습니다.

- 관리 그룹에 작업 할당. 이 경우 이전에 만든 관리 그룹에 포함된 컴퓨터에 작업이 할당됩니다.
- 네트워크에서 중앙 관리 서버가 탐지한 컴퓨터 선택: *미할당 장치*. 이 특정 장치에는 관리 그룹에 속하는 장치와 미할당 장치가 포함될 수 있습니다.
- 장치 주소를 직접 지정하거나 주소 목록에서 가져옵니다. 작업을 할당할 장치의 NetBIOS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

4단계. 작업 이름 정의

*Windows 10으로 업데이트*와 같이 작업 이름을 입력합니다.

5단계. 작업 생성 완료

마법사를 완료합니다. 필요하다면 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔로 BitLocker 보호를 일시 중지하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 작업** 옵션을 선택합니다.
   작업 목록이 열립니다.
2. **추가** 버튼을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 일반 작업 설정 구성

일반 작업 설정을 구성하려면 다음을 수행하십시오.

1. **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다.
2. **작업 유형** 드롭다운 목록에서 **BitLocker 보호 관리** 옵션을 선택합니다.
3. **작업 이름** 필드에 *Windows 10으로 업데이트*와 같은 간단한 설명을 입력합니다.
4. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.

2단계. BitLocker 보호 관리

BitLocker 인증을 구성합니다. BitLocker 보호를 일시 중지하려면 **BitLocker 인증 건너뛰기 임시 허용** 옵션을 선택하고 BitLocker 인증 없이 다시 시작할 횟수를 입력합니다(1~15회). 필요하면 작업의 만료 날짜와 시간을 입력합니다. 지정한 시간이 되면 작업이 자동으로 꺼지고, 컴퓨터를 다시 시작할 때 사용자가 BitLocker 인증을 완료해야 합니다.

3단계. 작업 생성 완료

마법사를 완료합니다. 작업 목록에 새 작업이 표시됩니다.

작업을 실행하려면 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다.

결과적으로 이 작업이 실행 중일 때는 컴퓨터를 다시 시작한 후에도 BitLocker가 사용자에게 인증을 요청하지 않습니다. BitLocker 인증 없이 컴퓨터를 다시 시작할 때마다 Kaspersky Industrial CyberSecurity for Nodes는 해당 이벤트를 생성하고 남은 다시 시작 횟수를 기록합니다.

지정한 다시 시작 횟수나 작업 만료 시간에 도달하면 BitLocker 인증이 자동으로 설정됩니다. 데이터에 접근하려면 사용자가 BitLocker 인증을 완료해야 합니다.

Windows 7을 사용하는 컴퓨터에서는 BitLocker가 컴퓨터 다시 시작을 카운트할 수 없습니다. Windows 7 컴퓨터에서는 Kaspersky Industrial CyberSecurity for Nodes에서 다시 시작 횟수 카운트를 처리합니다. 따라서 다시 시작할 때마다 BitLocker 인증을 자동으로 켜려면 Kaspersky Industrial CyberSecurity for Nodes를 시작해야 합니다.

BitLocker 인증을 미리 켜려면 *BitLocker 보호 관리* 작업 속성을 열고 **부팅 전에 항상 인증 요청**을 선택합니다.

타사 시스템과 통합

이 섹션에서는 Kaspersky Industrial CyberSecurity for Nodes와 타사 기능 및 기술의 통합에 대해 설명합니다.

시스템 모니터용 성능 카운터

Performance Counters는 Kaspersky Industrial CyberSecurity for Nodes의 구성 요소로서, 보호 구성 요소 작동 중 애플리케이션 성능을 모니터링하는 데 사용할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 설치하는 동안 성능 카운터를 등록합니다.

애플리케이션 성능 카운터는 Windows 제어판에서 사용할 수 있는 "시스템 모니터" 애플리케이션을 사용하여 확인할 수 있습니다. 성능 카운터 사용에 대한 자세한 내용은 Microsoft 기술 지원 웹사이트를 참조하십시오.

성능 카운터를 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 다른 애플리케이션과 함께 실행될 때 리소스 부족을 식별할 수 있을 뿐만 아니라 충돌을 진단하고 Kaspersky Industrial CyberSecurity for Nodes의 바람직하지 않은 설정을 식별할 수도 있습니다.

리소스 부족으로 처리되지 않은 요청 수

리소스 부족으로 처리되지 않은 요청 수

설명	시스템 리소스(예: RAM) 부족으로 처리되지 않은 파일 가로채기 드라이버의 총 요청 건수입니다. Kaspersky Industrial CyberSecurity for Nodes가 마지막으로 시작된 시점부터 집계됩니다. Kaspersky Industrial CyberSecurity for Nodes는 파일 가로채기 드라이버에서 처리되지 않은 개체 처리 요청을 건너뜁니다.
용도	이 카운터를 사용하면 시스템 리소스 부족으로 인해 발생할 수 있는 실시간 컴퓨터 보호 성능 저하를 탐지하고 해결할 수 있습니다.
정상 / 한계값	0 / 1
권장 읽기 간격	1시간.
한계값 초과 시 구성 권장 사항	카운터 값이 0이 아닌 경우에는 Kaspersky Industrial CyberSecurity for Nodes 프로세스가 요청을 처리하는 데 더 많은 RAM이 필요합니다. 다른 애플리케이션의 활성 프로세스가 가용 RAM을 모두 점유하고 있을 수 있습니다.

처리 제출 요청 수

처리 제출 요청 수

설명	작업 프로세스에서 처리 대기 중인 개체의 수입니다.
용도	이 카운터를 사용하면 Kaspersky Industrial CyberSecurity for Nodes 작업 프로세스의 부하와 보호 중인 장치의 전반적인 파일 활동 수준을 모니터링할 수 있습니다.
정상 / 한계값	카운터는 보호 중인 장치의 파일 활동 수준에 따라 다를 수 있습니다.
권장 읽기 간격	1분.
한계값 초과 시 구성 권장 사항	해당 없음

초당 처리된 개체 수

초당 처리된 개체 수

설명	처리된 개체 수를 해당 개체를 처리하는 데 걸린 시간으로 나눈 값입니다(동일한 시간 간격으로 계산).
용도	이 카운터는 개체 처리 속도를 보여줍니다. Kaspersky Industrial CyberSecurity for Nodes 프로세스에 할당된 프로세서 시간이 부족하거나 Kaspersky Industrial CyberSecurity for Nodes 작동 오류가 발생하여 보호 중인 장치 성능이 저하되는 지점을 탐지하고 해결하는 데 사용할 수 있습니다.
정상 / 한계값	변동 / 없음
권장 읽기 간격	1분.
한계값 초과 시 구성 권장 사항	이 카운터의 값은 Kaspersky Industrial CyberSecurity for Nodes 설정에 지정된 값과 다른 애플리케이션 프로세스가 보호 중인 장치에 미치는 부하에 따라 달라집니다. 장기간에 걸쳐 카운터 평균값을 확인하십시오. 카운터 평균값이 감소하는 경우 다음 상황 중 하나에 해당할 수 있습니다: • Kaspersky Industrial CyberSecurity for Nodes 프로세스에 개체를 처리할 프로세서 시간이 부족합니다. Kaspersky Industrial CyberSecurity for Nodes에 추가 프로세서 시간이 할당되었는지 확인합니다(예: 보호 중인 장치에서 타 애플리케이션의 부하를 줄이는 방식). • Kaspersky Industrial CyberSecurity for Nodes에서 오류(일부 스트림이 유휴 상태)가 발생했습니다. Kaspersky Industrial CyberSecurity for Nodes를 다시 시작합니다.

감염된 개체 대기열의 요소 수

감염된 개체 대기열의 요소 수

설명	처리(치료 또는 삭제) 대기 중인 감염된 개체 수입니다.
용도	이 카운터로 다음을 탐지할 수 있습니다: • 파일 가로채기 디스패처의 잠재적 오류로 인한 실시간 컴퓨터 보호 중단. • 여러 작업 프로세스와 Kaspersky Industrial CyberSecurity for Nodes 간에 프로세서 시간이 고르게 분산되지 않아 발생하는 프로세스 과부하. • 바이러스 확산.
정상 / 한계값	Kaspersky Industrial CyberSecurity for Nodes가 감염되었거나 감염이 의심되는 개체를 처리하는 동안에는 값이 0이 아닐 수 있으나 처리가 완료되면 0으로 돌아옵니다. / 장기간 0이 아닌 값으로 유지됩니다.
권장 읽기 간격	1분.
한계값 초과 시 구성 권장 사항	카운터 값이 장기간 0으로 돌아오지 않는 경우: • Kaspersky Industrial CyberSecurity for Nodes가 개체를 처리하지 않고 있습니다(파일 가로채기 디스패처가 충돌했을 수 있음). Kaspersky Industrial CyberSecurity for Nodes를 다시 시작합니다. • 개체를 처리할 프로세서 시간이 부족할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes에 추가 프로세서 시간이 할당되었는지 확인합니다(예: 보호 중인 장치에서 타 애플리케이션의 부하를 줄이는 방식). • 바이러스 확산이 발생했습니다. 실시간 파일 보호 구성 요소에 감염된 개체 또는 감염 의심 개체가 많은 경우도 바이러스 확산의 징후입니다. 탐지된 개체 수에 대한 정보는 구성 요소 통계 또는 구성 요소 로그에서 확인할 수 있습니다.

거부된 총 요청 수

거부된 총 요청 수

설명	**파일 가로채기 드라이버가 생성했으나 애플리케이션 프로세스에서 수락하지 않은 개체 처리 요청의 총 건수입니다. Kaspersky Industrial CyberSecurity for Nodes가 마지막으로 시작된 시점부터 집계됩니다.** **애플리케이션은 Kaspersky Industrial CyberSecurity for Nodes 프로세스에서 처리 요청이 거부된 개체는 건너뜁니다.**
용도	이 카운터로 다음을 탐지할 수 있습니다: • Kaspersky Industrial CyberSecurity for Nodes 프로세스의 과부하로 인한 실시간 컴퓨터 보호 성능 저하. • 파일 가로채기 디스패처 오류로 인한 실시간 컴퓨터 보호 중단.

설명	**파일 가로채기 드라이버가 생성했으나 애플리케이션 프로세스에서 수락하지 않은 개체 처리 요청의 총 건수입니다. Kaspersky Industrial CyberSecurity for Nodes가 마지막으로 시작된 시점부터 집계됩니다.** **애플리케이션은 Kaspersky Industrial CyberSecurity for Nodes 프로세스에서 처리 요청이 거부된 개체는 건너뜁니다.**
정상 / 한계값	0 / 1
권장 읽기 간격	1시간.
한계값 초과 시 구성 권장 사항	거부된 처리 요청 수는 건너뛴 개체 수와 일치합니다. 카운터 동작에 따라 발생 가능한 경우는 다음과 같습니다: • 카운터에 거부된 요청 일부가 장기간 표시되는 경우: Kaspersky Industrial CyberSecurity for Nodes 프로세스가 최대 부하 상태로 작동 중입니다. 애플리케이션이 개체를 검사할 수 없습니다. 개체 건너뛰기를 방지하려면 애플리케이션에 할당된 시스템 리소스를 늘리십시오. • 거부된 요청 수가 한계값을 크게 초과하고 급증하는 경우: 파일 가로채기 디스패처가 충돌했습니다. Kaspersky Industrial CyberSecurity for Nodes가 개체에 접근할 때 검사를 수행하지 않습니다. Kaspersky Industrial CyberSecurity for Nodes를 다시 시작합니다.

건너뛴 총 요청 수

건너뛴 총 요청 수

설명	파일 가로채기 드라이버가 생성하고 Kaspersky Industrial CyberSecurity for Nodes에서 수신했지만 처리 완료를 알리는 이벤트는 생성되지 않은 요청의 총 건수입니다. 이 값은 애플리케이션이 마지막으로 시작된 시점부터 집계됩니다 개체 처리 요청이 작업 프로세스 중 하나에서 수락되었지만 처리 완료를 알리는 이벤트를 보내지 않는 경우, 드라이버는 해당 요청을 다른 프로세스로 전달하며 **건너뛴 총 요청 수** 카운터 값이 1 증가합니다. 드라이버가 모든 작업 프로세스를 확인했음에도 요청을 수락한 프로세스가 없거나(모두 사용 중) 처리 완료를 알리는 이벤트를 보내지 않은 경우, Kaspersky Industrial CyberSecurity for Nodes는 해당 개체를 건너뜁니다. 이로 인해 **건너뛴 총 요청 수** 카운터 값이 1 증가합니다.
용도	이 카운터를 사용하면 파일 가로채기 디스패처 오류로 인한 성능 저하를 탐지할 수 있습니다.
정상 / 한계값	0 / 1
권장 읽기 간격	1시간.
한계값 초과 시 구성 권장 사항	카운터 값이 0이 아닌 경우는 하나 이상의 파일 가로채기 디스패처 스트림이 멈춰 응답하지 않는 상태입니다. 카운터 값은 현재 작동이 중단된 스트림 수와 일치합니다. 사 속도가 만족스럽지 않은 경우, Kaspersky Industrial CyberSecurity for Nodes를 다시 시작하여 오프라인 스트림을 복원해야 합니다.

최대 파일 가로채기 디스패처 스트림 수

Kaspersky Industrial CyberSecurity for Nodes 버전 5.0부터 "파일 가로채기 디스패처 스트림의 최대 수" 카운터는 지원되지 않습니다.

평균 파일 가로채기 디스패처 스트림 수

Kaspersky Industrial CyberSecurity for Nodes 버전 5.0부터 "파일 가로채기 디스패처 스트림의 평균 수" 카운터는 지원되지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes SNMP 카운터 및 트랩

설치할 안티 바이러스 구성 요소 세트에 SNMP 프로토콜 지원 구성 요소를 포함한 경우 Simple Network Management Protocol(SNMP)를 사용하여 Kaspersky Industrial CyberSecurity for Nodes 카운터 및 트랩을 볼 수 있습니다.

관리자 워크스테이션에서 Kaspersky Industrial CyberSecurity for Nodes 카운터 및 트랩을 보려면 보호 장치에서 SNMP 서비스를 시작하고 관리자 워크스테이션에서 SNMP 서비스와 SNMP Trap 서비스를 시작하십시오.

Kaspersky Industrial CyberSecurity for Nodes SNMP 카운터

이 섹션에는 Kaspersky Industrial CyberSecurity for Nodes SNMP 카운터 설정을 설명하는 표가 포함되어 있습니다.

성능 카운터

성능 카운터

카운터	정의
currentRequestsAmount	처리를 위해 제출된 요청 수
currentInfectedQueueLength	감염된 개체 대기열의 요소 수
currentObjectProcessingRate	초당 처리된 개체 수
currentWorkProcessesNumber	Kaspersky Industrial CyberSecurity for Nodes에서 현재 사용하는 작업 프로세스 수

백업 카운터

백업 카운터

카운터	정의
currentBackupStorageSize	백업의 총 데이터 양(MB)

일반 카운터

일반 카운터

카운터	정의
lastCriticalAreasScanAge	작업 *중요 영역 검사*이 완료된 후 경과한 시간(초)입니다.
licenseExpirationDate	라이선스 만료 날짜입니다. 활성 키와 추가 키가 모두 추가된 경우 추가 키와 연결된 라이선스의 만료 날짜가 표시됩니다.
currentApplicationUptime	Kaspersky Industrial CyberSecurity for Nodes가 마지막으로 시작된 후 실행된 시간이며, 1/100초 단위로 표시됩니다.

업데이트 카운터

업데이트 카운터

카운터	정의
avBasesAge	가장 최근에 설치된 데이터베이스 업데이트의 생성 날짜 이후 100분의 1초 단위로 경과한 시간.

실시간 파일 보호 카운터

실시간 파일 보호 카운터

카운터	정의
totalObjectsProcessed	실시간 파일 보호 구성 요소를 마지막으로 실행한 이후 검사한 총 개체 수
totalInfectedObjectsFound	실시간 파일 보호 구성 요소를 마지막으로 실행한 이후 탐지한 감염된 개체 및 기타 개체의 총수
totalSuspiciousObjectsFound	실시간 파일 보호 구성 요소를 마지막으로 실행한 이후 탐지한 감염 의심 개체의 총수
totalVirusesFound	실시간 파일 보호 구성 요소를 마지막으로 실행한 이후 탐지한 총 개체 수
totalObjectsQuarantined	Kaspersky Industrial CyberSecurity for Nodes가 격리에 저장한 감염된 개체, 감염 의심 개체 및 기타 개체의 총수. 실시간 파일 보호 구성 요소를 마지막으로 실행한 시점부터 계산됨
totalObjectsNotQuarantined	Kaspersky Industrial CyberSecurity for Nodes가 격리에 저장하려고 시도했지만 저장하지 못한 감염된 개체 또는 감염 의심 개체의 총수. 실시간 파일 보호 구성 요소를 마지막으로 실행한 시점부터 계산됨
totalObjectsDisinfected	Kaspersky Industrial CyberSecurity for Nodes가 치료한 감염된 개체의 총수. 실시간 파일 보호 구성 요소를 마지막으로 실행한 시점부터 계산됨
totalObjectsNotDisinfected	Kaspersky Industrial CyberSecurity for Nodes가 치료하려고 시도했지만 치료하지 못한 감염된 개체 및 기타 개체의 총수. 실시간 파일 보호 구성 요소를 마지막으로 실행한 시점부터 계산됨
totalObjectsDeleted	Kaspersky Industrial CyberSecurity for Nodes가 삭제한 감염된 개체, 감염 의심 개체 및 기타 개체의 총수. 실시간 파일 보호 구성 요소를 마지막으로 실행한 시점부터 계산됨
totalObjectsNotDeleted	Kaspersky Industrial CyberSecurity for Nodes가 삭제하려고 시도했지만 삭제하지 못한 감염된 개체, 감염 의심 개체 및 기타 개체의 총수. 실시간 파일 보호 구성 요소를 마지막으로 실행한 시점부터 계산됨
totalObjectsBackedUp	Kaspersky Industrial CyberSecurity for Nodes가 백업에 저장한 감염된 개체 및 기타 개체의 총수. 실시간 파일 보호 구성 요소를 마지막으로 실행한 시점부터 계산됨
totalObjectsNotBackedUp	Kaspersky Industrial CyberSecurity for Nodes가 백업에 저장하려고 시도했지만 저장하지 못한 감염된 개체 및 기타 개체의 총수. 실시간 파일 보호 구성 요소를 마지막으로 실행한 시점부터 계산됨
currentFileMonitorTaskStatus	실시간 파일 보호 구성 요소의 상태: • `1`은 구성 요소가 활성화되어 보호 기능을 제공하고 있음을 의미합니다. • `0`은 구성 요소가 보호 기능을 제공하지 않음을 의미합니다. 예: 비활성화됨, 설치되지 않음, 라이선스 계약 위반.

AMSI 스캐너 카운터

AMSI 스캐너 카운터

카운터	정의
currentScriptCheckerTaskStatus	AMSI 스캐너 구성 요소의 상태: • `1`은 구성 요소가 활성화되어 보호 기능을 제공하고 있음을 의미합니다. • `0`은 구성 요소가 보호 기능을 제공하지 않음을 의미합니다. 예: 비활성화됨, 설치되지 않음, 라이선스 계약 위반.
totalScriptsProcessed	AMSI 스캐너 구성 요소를 마지막으로 실행한 이후 처리된 스크립트 수.
totalInfectedlDangerousScriptsFound	AMSI 스캐너 구성 요소를 마지막으로 실행한 이후 탐지된 위험한 스크립트 수.

카운터	정의
totalSuspiciousScriptsFound	AMSI 스캐너 구성 요소를 마지막으로 실행한 이후 탐지된 의심스러운 스크립트의 총수.
totalScriptsBlocked	AMSI 스캐너 구성 요소를 마지막으로 실행한 이후 차단된 스크립트의 총수. **차단**에서 구성 요소가 활성화된 경우 카운터 값이 변경되며 totalInfectedIDangerousScriptsFound 카운터 값과 같습니다.

Kaspersky Industrial CyberSecurity for Nodes SNMP 트랩 및 해당 옵션

Kaspersky Industrial CyberSecurity for Nodes의 SNMP 트랩 옵션은 다음과 같습니다.

- eventThreatDetected: 개체 탐지됨.
  트랩의 옵션은 다음과 같습니다.
  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty
- eventBackupStorageSizeExceeds: 최대 백업 크기 초과. 백업의 총 데이터 양이 **백업 크기를 다음으로 제한**에 지정된 값을 초과합니다. Kaspersky Industrial CyberSecurity for Nodes는 감염된 개체를 계속 백업합니다.
  트랩의 옵션은 다음과 같습니다.
  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventThresholdBackupStorageSizeExceeds: 백업 여유 공간 한계값 초과. 백업의 여유 공간이 **이용 가능 공간의 임계값(MB)**에 지정된 값 이하입니다. Kaspersky Industrial CyberSecurity for Nodes는 감염된 개체를 계속 백업합니다.
  트랩의 옵션은 다음과 같습니다.
  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventObjectNotBackuped: 개체 백업되지 않음.

트랩의 옵션은 다음과 같습니다.

- eventSeverity
- eventDateAndTime
- eventSource
- objectName
- userName
- computerName
- storageObjectNotAddedEventReason

- eventBackupInternalError: 백업 오류입니다.
  트랩의 옵션은 다음과 같습니다.
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventAVBasesOutdated: 데이터베이스가 오래되었습니다. *업데이트* 작업(로컬 작업, 그룹 작업 또는 보호 장치 세트에 대한 작업)을 마지막으로 실행한 후 경과한 일수입니다.
  트랩의 옵션은 다음과 같습니다.
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventAVBasesTotallyOutdated: 데이터베이스가 매우 오래되었습니다. *업데이트* 작업(로컬 작업, 그룹 작업 또는 보호 장치 세트에 대한 작업)을 마지막으로 실행한 후 경과한 일수입니다.
  트랩의 옵션은 다음과 같습니다.
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventApplicationStarted: 애플리케이션 시작.

트랩의 옵션은 다음과 같습니다.

- eventSeverity
- eventDateAndTime
- eventSource

- eventApplicationShutdown: 애플리케이션 중지.
  트랩의 옵션은 다음과 같습니다.
  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventCriticalAreasScanWasntPerformForALongTime: 중요 영역 검사를 장기간 수행하지 않았습니다. *중요 영역 검사* 작업을 마지막으로 완료한 후 경과한 일수입니다.
  트랩의 옵션은 다음과 같습니다.
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventLicenseHasExpired: 라이센스가 만료되었습니다.
  트랩의 옵션은 다음과 같습니다.
  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventLicenseExpiresSoon: 라이센스가 곧 만료됨. 라이선스 만료일까지 남은 일수로 계산됩니다.
  트랩의 옵션은 다음과 같습니다.
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventTaskInternalError: 작업 완료 오류입니다.

트랩의 옵션은 다음과 같습니다.

- eventSeverity
- eventDateAndTime
- eventSource
- errorCode
- knowledgeBaseId
- taskName

- eventUpdateError: *업데이트* 작업 실행 중 오류가 발생했습니다.
  트랩의 옵션은 다음과 같습니다.
  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason
  - eventSource

Kaspersky Industrial CyberSecurity for Nodes SNMP 트랩 옵션 설명 및 가능한 값

트랩 옵션과 가능한 값에 대한 설명은 다음과 같습니다.

- eventDateAndTime: 이벤트 날짜 및 시간
- eventSeverity: 중요도
  이 옵션은 다음과 같을 수 있습니다.
  - critical (1) – 심각
  - warning (2) – 경고
  - info (3) – 알림
- userName: 사용자 이름(예: 감염된 파일에 접근을 시도한 사용자의 이름).
- computerName: 보호되는 장치 이름(예: 사용자가 감염된 파일에 접근을 시도한 보호되는 장치의 이름).
- eventSource: 이벤트를 생성한 기능 구성 요소.

이 옵션은 다음과 같을 수 있습니다.

- unknown (0) – 알 수 없는 기능 구성 요소
- quarantine (1) – 격리
- backup (2) – 백업
- reporting (3) – 작업 로그
- updates (4) – 업데이트
- realTimeProtection (5) – 실시간 파일 보호
- onDemandScanning (6) – 온디맨드 검사
- product (7) – 개별 구성 요소의 작동이 아닌 Kaspersky Industrial CyberSecurity for Nodes 전체의 작동과 관련된 이벤트
- systemAudit (8) – 시스템 감사 로그

- eventReason: 이벤트 트리거: 이벤트를 트리거한 항목.
  이 옵션은 다음과 같을 수 있습니다.
  - reasonUnknown (0) – 원인을 알 수 없습니다.
  - reasonInvalidSettings (1) – 백업 및 격리 이벤트에만 해당합니다. 격리 또는 백업 폴더를 사용할 수 없는 경우(접근 권한이 부족하거나 격리 설정에 잘못된 폴더가 지정된 경우(예: 네트워크 경로가 지정된 경우)) 표시됩니다. 이 경우 Kaspersky Industrial CyberSecurity for Nodes는 기본 백업 또는 격리 폴더를 사용합니다.
- objectName: 개체 이름(예: 바이러스가 탐지된 파일의 이름).
- threatName: 바이러스 백과사전 분류에 따른 개체 이름. 이 이름은 Kaspersky Industrial CyberSecurity for Nodes가 개체를 탐지할 때 반환하는 전체 이름에 포함됩니다. 작업 로그에서 탐지된 개체의 전체 이름을 볼 수 있습니다.
- detectType: 탐지된 개체의 유형.
  이 옵션은 다음과 같을 수 있습니다.
  - undefined (0) – 정의되지 않음
  - virware – 클래식 바이러스 및 네트워크 웜
  - trojware – 트로이목마
  - malware – 기타 악성 애플리케이션
  - adware – 광고 소프트웨어
  - pornware – 음란물 소프트웨어
  - riskware – 침입자가 사용자의 장치나 개인 데이터를 손상하는 데 사용할 수 있는 합법적인 애플리케이션
- detectCertainty: 위협 탐지 확실도.

이 옵션은 다음과 같을 수 있습니다.

- Suspicion (감염 가능성 있음) – Kaspersky Industrial CyberSecurity for Nodes가 개체 코드의 한 섹션과 알려진 악성 코드 섹션이 부분적으로 일치하는 것을 탐지했습니다.
- Sure (감염됨) – Kaspersky Industrial CyberSecurity for Nodes가 개체의 한 코드 섹션과 알려진 악성 코드 섹션이 완전히 일치하는 것을 탐지했습니다.

- days: 일수(예: 라이선스 만료일까지 남은 일수).
- errorCode: 오류 코드.
- taskName: 작업 이름.
- updaterErrorEventReason: 업데이트 오류의 원인.
  이 옵션은 다음과 같을 수 있습니다.
  - reasonUnknown(0) – 원인을 알 수 없습니다.
  - reasonAccessDenied – 접근이 거부되었습니다.
  - reasonUrlsExhausted – 업데이트 소스 목록이 모두 소진되었습니다.
  - reasonInvalidConfig – 잘못된 구성 파일.
  - reasonInvalidSignature – 잘못된 서명.
  - reasonCantCreateFolder – 폴더를 생성할 수 없습니다.
  - reasonFileOperError – 파일 오류.
  - reasonDataCorrupted – 개체가 손상되었습니다.
  - reasonConnectionReset – 연결이 재설정되었습니다.
  - reasonTimeOut – 연결 시간이 초과되었습니다.
  - reasonProxyAuthError – 프록시 인증 오류.
  - reasonServerAuthError – 서버 인증 오류.
  - reasonHostNotFound – 장치를 찾을 수 없습니다.
  - reasonServerBusy – 서버를 사용할 수 없습니다.
  - reasonConnectionError – 연결 오류.
  - reasonModuleNotFound – 개체를 찾을 수 없습니다.
  - reasonBlstCheckFailed (16) – 키 거부 목록을 확인하는 동안 오류가 발생했습니다. 업데이트 시점에 데이터베이스 업데이트가 게시 중이었을 수 있습니다. 몇 분 후에 업데이트를 다시 수행하십시오.
- storageObjectNotAthreatddedEventReason: 개체가 백업 또는 격리에 저장되지 않은 이유.

이 옵션은 다음과 같을 수 있습니다.

- reasonUnknown (0) – 원인을 알 수 없습니다.
- reasonStorageInternalError – 데이터베이스 오류. Kaspersky Industrial CyberSecurity for Nodes를 복원해야 합니다.
- reasonStorageReadOnly – 데이터베이스가 읽기 전용입니다. Kaspersky Industrial CyberSecurity for Nodes를 복원해야 합니다.
- reasonStorageIOError – 입출력 오류: a) Kaspersky Industrial CyberSecurity for Nodes가 손상되어 복원해야 합니다. b) Kaspersky Industrial CyberSecurity for Nodes 파일이 저장된 디스크가 손상되었습니다.
- reasonStorageCorrupted – 스토리지가 손상되었습니다. Kaspersky Industrial CyberSecurity for Nodes를 복원해야 합니다.
- reasonStorageFull – 데이터베이스가 가득 찼습니다. 디스크 여유 공간이 필요합니다.
- reasonStorageOpenError – 데이터베이스 파일을 열 수 없습니다. Kaspersky Industrial CyberSecurity for Nodes를 복원해야 합니다.
- reasonStorageOSFeatureError – 일부 운영 체제 기능이 Kaspersky Industrial CyberSecurity for Nodes 요구 사항을 충족하지 않습니다.
- reasonObjectNotFound – 격리에 저장하려는 개체가 디스크에 없습니다.
- reasonObjectAccessError – 백업 API를 사용할 권한이 부족합니다. 작업 수행에 사용되는 계정에 백업 운영자 권한이 없습니다.
- reasonDiskOutOfSpace – 디스크 공간이 부족합니다.

WMI 통합

Kaspersky Industrial CyberSecurity for Nodes는 Windows Management Instrumentation(WMI)와의 통합을 지원합니다. WMI를 사용하는 클라이언트 시스템에서 Web-Based Enterprise Management(WBEM) 표준을 통해 Kaspersky Industrial CyberSecurity for Nodes 및 해당 구성 요소의 상태 정보를 받을 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes를 설치하면 보호 장치에 Kaspersky Industrial CyberSecurity for Nodes 네임스페이스를 생성하기 위한 전용 모듈이 시스템에 등록됩니다. Kaspersky Industrial CyberSecurity for Nodes 네임스페이스를 사용하면 Kaspersky Industrial CyberSecurity for Nodes 클래스와 인스턴스 및 해당 속성을 사용할 수 있습니다.

일부 인스턴스 속성의 값은 작업 유형에 따라 달라집니다.

*비주기적 작업*은 실행 시간이 제한되지 않으며 계속 실행되거나 중지된 상태일 수 있는 애플리케이션 작업입니다. 이러한 작업에는 실행 진행률이 없습니다. 작업이 실행되는 동안 작업 결과는 단일 이벤트로 계속 기록됩니다(예: 실시간 컴퓨터 보호 작업에서 감염된 개체 탐지). 이러한 유형의 작업은 Kaspersky Security Center 정책을 통해 관리됩니다.

*주기적 작업*은 실행 시간이 제한되며 실행 진행률이 백분율로 표시되는 애플리케이션 작업입니다. 작업 결과는 작업이 완료될 때 생성되며 단일 항목 또는 변경된 애플리케이션 상태로 표시됩니다(예: 완료된 애플리케이션 데이터베이스 업데이트, 규칙 생성 작업을 위해 생성된 구성 파일). 동일한 유형의 주기적 작업 여러 개를 하나의 보호 장치에서 동시에 실행할 수 있습니다(예: 검사 범위가 서로 다른 온디맨드 검사 작업 3개). 주기적 작업은 Kaspersky Security Center를 통해 그룹 작업으로 관리할 수 있습니다.

도구를 사용하여 WMI 네임스페이스 쿼리를 생성하고 회사 네트워크의 WMI 네임스페이스에서 동적 데이터를 수신하면 현재 애플리케이션 상태에 대한 정보를 확인할 수 있습니다(아래 표 참조).

애플리케이션 상태 정보

인스턴스 속성	설명	값
`ProductName`	설치된 애플리케이션의 이름입니다.	버전 번호를 제외한 애플리케이션의 전체 이름입니다.
`ProductVersion`	설치된 애플리케이션의 전체 버전 번호입니다.	빌드 번호를 포함한 전체 애플리케이션 버전 번호입니다.
`InstalledPatches`	설치된 패치의 표시 이름 집합입니다.	애플리케이션에 설치된 중요 수정 사항 목록입니다.
`IsLicenseInstalled`	애플리케이션 활성화 상태입니다.	애플리케이션 활성화에 사용되는 키의 상태입니다. 가능한 값: • `False` 라이선스 키가 추가되지 않았습니다. • `True` 라이선스 키가 추가되었습니다.
`LicenseDaysLeft`	현재 라이선스가 만료될 때까지 남은 일수를 표시합니다.	현재 라이선스가 만료될 때까지 남은 일수입니다. 가능한 0 이하의 값: • `0` 라이선스가 만료되었습니다. • `-1` 현재 키에 대한 정보를 가져올 수 없거나 지정된 키를 애플리케이션 활성화에 사용할 수 없습니다(예: 키 거부 목록에 따라 차단된 경우).
`AVBasesDatetime`	현재 안티 바이러스 데이터베이스 버전의 타임스탬프입니다.	현재 사용 중인 안티 바이러스 데이터베이스가 생성된 날짜와 시간입니다. 설치된 애플리케이션에서 안티 바이러스 데이터베이스를 사용하지 않는 경우 필드 값은 `{Not installed}` 입니다.
`IsExploitPreventionEnabled`	익스플로잇 방지 구성 요소의 상태입니다.	익스플로잇 방지 구성 요소의 상태입니다. 가능한 값: • `True` 익스플로잇 방지 구성 요소가 활성화되어 보호 기능을 제공하고 있습니다. • `False` 익스플로잇 방지 구성 요소가 보호 기능을 제공하지 않고 있습니다. 예: 비활성화됨, 설치되지 않음, 라이선스 계약 위반.
`ProtectionTasksRunning`	현재 실행 중인 보호 작업 집합입니다.	현재 실행 중인 보호, 제어 및 모니터링 작업 목록입니다. 이 필드에는 실행 중인 모든 비정기 작업이 포함되어야 합니다. 실행 중인 비정기 작업이 없는 경우 필드 값은 `{No}` 입니다.
`IsAppControlRunning`	애플리케이션 실행 제어 구성 요소의 상태입니다.	가능한 값 • `True` 애플리케이션 실행 제어 구성 요소가 활성화되어 보호 기능을 제공하고 있습니다. • `False` 애플리케이션 실행 제어 구성 요소가 보호 기능을 제공하지 않고 있습니다. 예: 비활성화됨, 설치되지 않음, 라이선스 계약 위반.
`AppControlMode`	애플리케이션 실행 제어 구성 요소의 운영 모드입니다.	가능한 값: • `Active` 구성 요소 설정에 **차단** 모드가 지정되어 있습니다. • `Statistics Only` 구성 요소 설정에 **알림** 모드가 지정되어 있습니다. • `Not installed` 애플리케이션 실행 제어 구성 요소가 설치되어 있지 않습니다. • `Unknown` 구성 요소가 비활성화되어 있습니다.
`AppControlRulesNumber`	애플리케이션 실행 제어 규칙의 총 수입니다.	현재 애플리케이션 실행 제어 구성 요소 설정에 지정된 규칙 수입니다.
`AppControlLastBlocking`	모든 모드에서 애플리케이션 실행 제어 구성 요소가 마지막으로 애플리케이션 실행을 차단한 타임스탬프입니다.	애플리케이션 실행 제어 구성 요소가 마지막으로 애플리케이션 실행을 차단한 날짜와 시간입니다. 이 필드에는 구성 요소의 운영 모드와 관계없이 차단된 모든 애플리케이션이 포함됩니다. WMI 쿼리가 처리될 때 차단된 애플리케이션 실행 인스턴스가 등록되어 있지 않으면 필드 값은 `{No}` 입니다.
`PeriodicTasksRunning`	현재 실행 중인 정기 작업 집합입니다.	현재 실행 중인 온디맨드 검사, 업데이트 및 인벤토리 수집 작업 목록입니다. 이 필드에는 실행 중인 모든 정기 작업이 포함되어야 합니다. 현재 실행 중인 정기 작업이 없으면 필드 값은 `{No}` 입니다.

인스턴스 속성	설명	값
`ConnectionState`	WMI Provider 구성 요소와 Kaspersky Industrial CyberSecurity for Nodes 서비스 간의 연결 상태입니다.	WMI Provider 구성 요소와 Kaspersky Industrial CyberSecurity for Nodes 서비스 간의 연결 상태에 대한 정보입니다. 가능한 값: • `Success` 연결이 성공적으로 설정되어 WMI 클라이언트가 애플리케이션 상태를 수신할 수 있습니다. • `Failed. Error Code: <code>` 지정된 코드의 오류로 인해 연결을 설정할 수 없습니다.
`IsDumpingEnabled`	메모리 덤프 기록 상태입니다.	가능한 값 • `True` 메모리 덤프 기록이 활성화되어 있습니다. • `False` 메모리 덤프 기록이 비활성화되어 있습니다.
`DumpsFolder`	덤프 파일 저장 폴더입니다.	전체 폴더 경로입니다. 덤프 기록이 비활성화되어 있으면 이 필드는 비어 있습니다.
`IsTracingEnabled`	애플리케이션 추적 상태입니다.	가능한 값 • `True` 애플리케이션 추적이 활성화되어 있습니다. • `False` 애플리케이션 추적이 비활성화되어 있습니다.
`TraceFolder`	추적 파일 저장 폴더입니다.	전체 폴더 경로입니다. 애플리케이션 추적이 비활성화되어 있으면 이 필드는 비어 있습니다.
`AllTasksState`	모든 작업의 상태입니다.	`{<profile-name_1>, <profile-type_1>, <profile-state_1>,...<profile-name_N>, <profile-type_N>, <profile-state_N>}` 형식의 작업 상태 정보입니다. 여기서 `profile-name`은 작업 이름, `profile-type`은 작업 유형, `profile-state`은 작업의 현재 상태입니다. 가능한 상태 값: • `not started` 작업이 아직 시작되지 않았습니다. • `running` 작업이 실행 중입니다. • `running ma` 작업이 실행 중이며 실행 중에 장애가 발생했습니다. • `paused` 작업이 일시 중지되었습니다. • `stopped` 작업이 중지되었습니다. • `completed` 작업이 성공적으로 완료되었습니다. • `failed` 작업이 오류로 인해 종료되었습니다. • `disabled` 작업이 비활성화되어 실행할 수 없습니다. • `starting` 작업이 시작되는 중입니다. • `pausing` 작업이 일시 중지되는 중입니다. • `stopping` 작업이 중지되는 중입니다. • `<unknown>` 상태를 확인할 수 없습니다.
`IsDevControlRunning`	장치 제어 구성 요소의 상태입니다.	가능한 값: • `True` 장치 제어 구성 요소가 활성화되어 보호 기능을 제공하고 있습니다. • `False` 장치 제어 구성 요소가 보호 기능을 제공하지 않고 있습니다. 예: 비활성화됨, 설치되지 않음, 라이선스 계약 위반.
`IsKSNRunning`	Kaspersky Security Network 구성 요소의 상태입니다.	가능한 값: • `True` Kaspersky Security Network 구성 요소가 활성화되어 보호 기능을 제공하고 있습니다. • `False` Kaspersky Security Network 구성 요소가 보호 기능을 제공하지 않고 있습니다. 예: 비활성화됨, 설치되지 않음, 라이선스 계약 위반.
`IsOASRunning`	실시간 파일 보호 구성 요소의 상태입니다.	가능한 값: • `True` 실시간 파일 보호 구성 요소가 활성화되어 보호 기능을 제공하고 있습니다. • `False` 실시간 파일 보호 구성 요소가 보호 기능을 제공하지 않고 있습니다. 예: 비활성화됨, 설치되지 않음, 라이선스 계약 위반.

이 데이터는 인스턴스 속성 `KasperskySecurity_ProductInfo.ProductName=Kaspersky Industrial CyberSecurity for Nodes`을 나타내며, 각 속성은 다음과 같습니다.

- `KasperskySecurity_ProductInfo`은 Kaspersky Industrial CyberSecurity for Nodes 클래스의 이름입니다.
- `.ProductName=Kaspersky Industrial CyberSecurity for Nodes`은 Kaspersky Industrial CyberSecurity for Nodes의 키 속성입니다.

이 클래스는 `ROOT\Kaspersky\Security` 네임스페이스에서 인스턴스화됩니다.

Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 소프트웨어 모듈 업데이트

이 섹션에는 Kaspersky Industrial CyberSecurity for Nodes 업데이트의 업데이트 작업과 롤백에 관한 정보와 작업 구성 지침이 포함되어 있습니다.

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)이 제공되지 않을 수도 있습니다.

데이터베이스 및 애플리케이션 모듈 업데이트

Kaspersky Industrial CyberSecurity for Nodes의 데이터베이스 및 애플리케이션 모듈을 업데이트하면 컴퓨터를 최신 상태로 보호할 수 있습니다. 전 세계적으로 날마다 수많은 신종 바이러스 및 기타 형태의 악성 코드가 나타나고 있습니다. Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에는 위협에 대한 정보와 이를 처리하는 방법이 포함되어 있습니다. 위협을 신속하게 탐지하려면 데이터베이스 및 애플리케이션 모듈을 정기적으로 업데이트해야 합니다.

정기적인 업데이트는 유효한 라이센스를 요구합니다. 활성화된 라이센스가 없는 경우 업데이트를 한 번만 수행할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky의 HTTP 또는 FTP 업데이트 서버, Kaspersky Security Center 중앙 관리 서버, 기타 업데이트 경로에서 애플리케이션 데이터베이스 및 모듈 업데이트를 다운로드합니다.

보호된 각 장치에 대한 업데이트를 다운로드하거나 보호된 장치 하나를 중개 장치로 사용할 수 있습니다. 업데이트가 여기에 복사된 다음 보호 중인 장치에 배포됩니다. Kaspersky Security Center 사용하여 조직의 장치 보안을 중앙에서 관리하는 경우 중앙 관리 서버를 업데이트 다운로드용 프록시로 활용할 수 있습니다.

업데이트 다운로드 프로세스가 중단되거나 오류를 일으키면 Kaspersky Industrial CyberSecurity for Nodes는 마지막으로 설치된 업데이트가 적용된 데이터베이스를 사용하도록 자동으로 다시 전환합니다. Kaspersky Industrial CyberSecurity for Nodes 데이터베이스가 손상되었다면 이전에 설치된 업데이트에 수동으로 롤백할 수 있습니다.

업데이트를 수행하면 다음과 같은 개체가 다운로드되어 컴퓨터에 설치됩니다:

- Kaspersky Industrial CyberSecurity for Nodes 데이터베이스. 악성 코드를 처리하는 방법에 대한 정보 및 바이러스 및 기타 위협의 시그니처가 담긴 데이터베이스를 사용해 컴퓨터 보호가 이뤄집니다. 보호 구성 요소는 이 정보를 사용하여 컴퓨터에서 감염된 파일을 검색하고 치료합니다. 데이터베이스는 신종 위협 레코드와 그 대응 방법으로 계속 업데이트됩니다. 데이터베이스를 정기적으로 업데이트하는 것이 좋습니다.

  Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 외에도 애플리케이션 구성 요소가 네트워크 트래픽을 가로챌 수 있도록 하는 네트워크 드라이버가 업데이트됩니다.

- 애플리케이션 모듈. 이 애플리케이션 모듈을 업데이트하면 Kaspersky Industrial CyberSecurity for Nodes의 취약점이 수정되거나, 새로운 기능이 추가되거나, 기존 기능이 향상됩니다.

업데이트 시 컴퓨터에 있는 애플리케이션 모듈 및 데이터베이스는 업데이트 경로에 있는 최신 버전과 비교됩니다. 사용자의 현재 데이터베이스 및 애플리케이션 모듈이 최신 버전과 다른 경우 누락된 부분에 대한 업데이트가 컴퓨터에 설치됩니다.

데이터베이스가 오래된 경우 업데이트 패키지가 커질 수 있고 그에 따라 인터넷 트래픽이 최대 수십 MB까지 증가할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 데이터베이스의 현재 상태에 대한 정보는 알림 영역에서 애플리케이션 아이콘 위로 커서를 이동하면 표시되는 툴팁 또는 메인 애플리케이션 창에 표시됩니다.

업데이트 결과와 업데이트 작업 동안 발생한 모든 이벤트에 관한 정보는 업데이트 작업 로그에 기록됩니다.

업데이트 작업 정보

Kaspersky Industrial CyberSecurity for Nodes에는 *업데이트*와 *업데이트 롤백*이라는 두 가지 업데이트 작업이 있습니다.

업데이트

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 업데이트 경로에서 데이터베이스와 애플리케이션 모듈(사용 가능한 경우)을 장치로 복사하며, 보호 구성 요소에서 이를 즉시 사용하기 시작합니다. 온디맨드 검사 작업은 다음 시작 시부터 업데이트된 데이터베이스를 사용합니다.

업데이트 작업의 설정을 구성할 수 있습니다. 작업 설정이 수정되면 Kaspersky Industrial CyberSecurity for Nodes는 다음 작업 시작 시 새 값을 적용합니다.

기본적으로 *업데이트* 작업은 **수동** 모드로 설정됩니다. 업데이트 작업은 일시 중지 후 다시 시작할 수 없습니다.

업데이트 롤백

이 작업으로 Kaspersky Industrial CyberSecurity for Nodes는 이전 데이터베이스 및 애플리케이션 모듈로 돌아갑니다.

기본적으로 *업데이트 롤백* 작업은 비활성화되어 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 모듈 업데이트 구성

업데이트 작업의 업데이트 경로는 조직에서 사용하는 데이터베이스 및 소프트웨어 모듈의 업데이트 구성에 따라 선택합니다.

Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 모듈은 보호 중인 장치에서 다음 구성을 사용하여 업데이트할 수 있습니다:

- 인터넷에서 보호 중인 각 장치로 직접 업데이트를 다운로드합니다(구성 1).
- 인터넷에서 중계 장치로 업데이트를 다운로드한 후 보호 중인 장치로 업데이트를 배포합니다.
  다음 애플리케이션이 설치된 모든 장치가 중계 기능을 할 수 있습니다:
  - Kaspersky Industrial CyberSecurity for Nodes(구성 2).
  - Kaspersky Security Center 중앙 관리 서버(구성 3).

  > 중계 장치를 사용하여 업데이트하면 인터넷 트래픽이 줄어들 뿐만 아니라 네트워크 보호 중인 장치에 대한 보안이 추가로 제공됩니다.

- 보안 이동식 드라이브를 통해 보호 중인 각 장치에 데이터베이스 업데이트를 다운로드하십시오(구성 4).

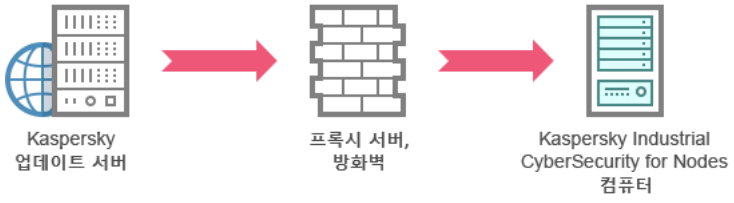
나열된 업데이트 구성에 대한 설명은 다음과 같습니다.

구성 1. 인터넷에서 직접 데이터베이스 및 모듈 업데이트

인터넷에서 직접 Kaspersky Industrial CyberSecurity for Nodes 업데이트를 구성하려면:

보호 중인 각 장치의 *업데이트* 작업의 설정에서 Kaspersky의 업데이트 서버를 업데이트 경로로 지정합니다.

업데이트 폴더가 있는 기타 HTTPS 또는 HTTP 서버는 업데이트 경로로 구성할 수 있습니다.



구성 1: 인터넷에서 직접 데이터베이스 및 모듈 업데이트

구성 2. 보호 중인 장치 하나를 통해 데이터베이스 및 모듈 업데이트

보호 중인 장치 하나를 통해 Kaspersky Industrial CyberSecurity for Nodes 업데이트 수신을 구성하려면:

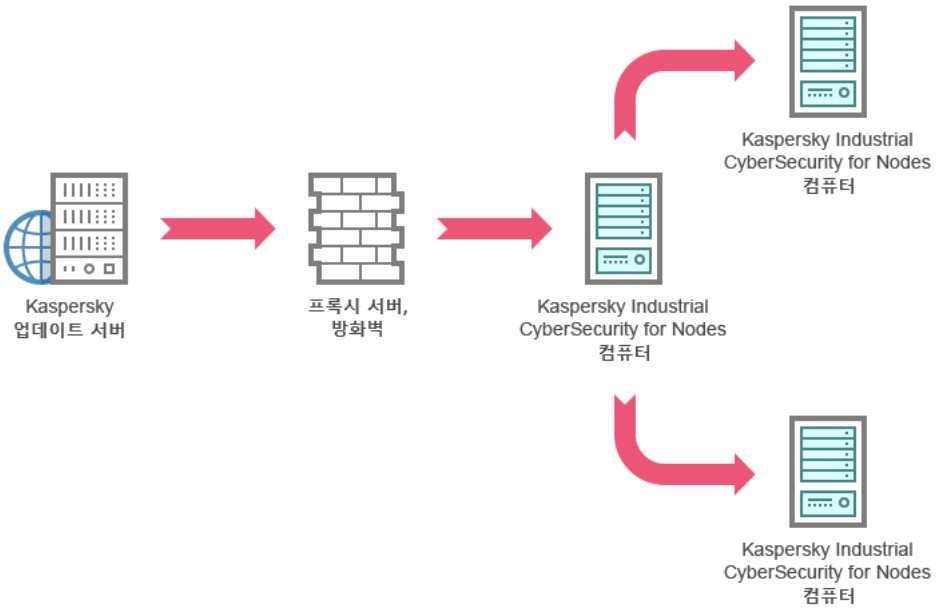
1. 선택한 보호 중인 장치로 업데이트를 복사합니다.
   - 선택한 보호 중인 장치에서 *업데이트* 작업 설정을 구성합니다:
     a. Kaspersky의 업데이트 서버를 업데이트 경로로 지정합니다.
     b. 공유 폴더를 업데이트가 저장될 폴더로 사용하도록 지정합니다.

2. 다른 보호 중인 장치에 업데이트를 배포합니다.

- 보호 중인 각 장치에서 *업데이트* 작업을 구성합니다:

  a. 업데이트 경로의 경우 업데이트를 다운로드할 중계 장치의 드라이브에 있는 폴더를 지정합니다.

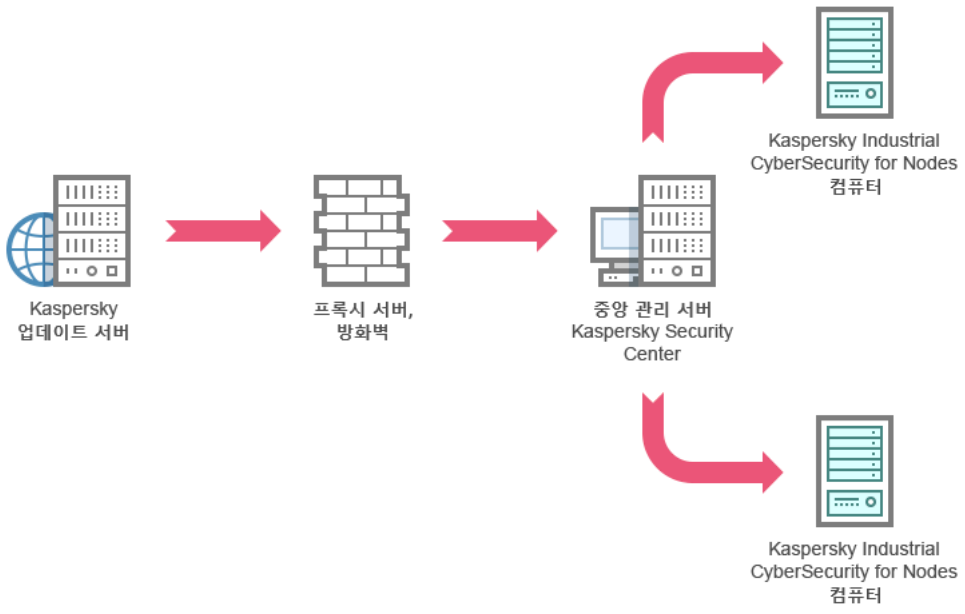
Kaspersky Industrial CyberSecurity for Nodes는 보호 중인 장치 하나를 통해 업데이트를 가져옵니다.



구성 2: 보호 중인 장치 하나를 통해 데이터베이스 및 모듈 업데이트

구성 3. Kaspersky Security Center 중앙 관리 서버를 통해 데이터베이스 및 모듈 업데이트

Kaspersky Security Center를 사용하여 장치의 안티 바이러스 보호를 중앙에서 관리하는 경우, 로컬 네트워크에 설치된 Kaspersky Security Center 중앙 관리 서버를 통해 업데이트를 다운로드할 수 있습니다.



구성 3: Kaspersky Security Center 중앙 관리 서버를 통해 데이터베이스 및 모듈 업데이트

Kaspersky Security Center 중앙 관리 서버를 통해 Kaspersky Industrial CyberSecurity for Nodes의 업데이트 수신을 구성하려면:

1. 보호 중인 각 장치에 네트워크 에이전트를 설치하십시오. 네트워크 에이전트는 Kaspersky Security Center 배포 키트에 포함된 소프트웨어 구성 요소입니다. 이는 중앙 관리 서버와 보호 중인 장치의 Kaspersky Industrial CyberSecurity for Nodes 간 상호 작용을 보장합니다. 네트워크 에이전트와 Kaspersky Security Center를 사용한 네트워크 에이전트의 구성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

2. Kaspersky의 업데이트 서버에서 Kaspersky Security Center 중앙 관리 서버로 업데이트를 다운로드합니다.

   - 지정된 보호 중인 장치 집합에 대해 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 구성합니다:

     a. Kaspersky의 업데이트 서버를 업데이트 경로로 지정합니다.

3. 보호 중인 장치에 업데이트를 배포합니다. 이를 위해서는 다음 동작 중 하나를 수행합니다:

   - Kaspersky Security Center 중앙 관리 서버에서 *업데이트* 그룹 작업을 구성하여 보호 중인 장치로 업데이트를 배포합니다:

   - 보호 중인 각 장치에서 *업데이트* 작업을 구성합니다:

     a. Kaspersky Security Center 중앙 관리 서버를 업데이트 경로로 지정합니다.

     b. 필요한 경우 작업 스케줄을 구성합니다.

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Center 중앙 관리 서버를 통해 업데이트를 확보합니다.

구성 4. 보안 이동식 드라이브에서 애플리케이션 데이터베이스 업데이트

보안 이동식 드라이브를 사용하여 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스를 업데이트하려면:

1. Kaspersky Industrial CyberSecurity for Nodes가 설치되어 있고 애플리케이션 데이터베이스 업데이트에 접근할 수 있는 장치에 보안 이동식 드라이브를 연결합니다.

2. 연결된 이동식 드라이브에 대해 장치 제어 구성 요소의 허용 규칙을 추가합니다.

3. 애플리케이션 콘솔에서 *애플리케이션 데이터베이스의 안전한 복사* 작업을 구성하고 실행합니다.

4. 데이터베이스 업데이트가 포함된 보안 이동식 드라이브를 애플리케이션 데이터베이스를 업데이트해야 하는 장치에 연결합니다.

5. 애플리케이션 콘솔에서 *애플리케이션 데이터베이스의 안전한 업데이트* 작업을 구성하고 실행합니다.

Kaspersky Industrial CyberSecurity for Nodes가 보안 이동식 드라이브에서 업데이트된 애플리케이션 데이터베이스를 수신합니다.

업데이트 작업 구성

Kaspersky Security Center 관리 콘솔에서 업데이트 작업을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔에서 구성하려는 로컬 또는 그룹 업데이트 작업으로 갑니다.
2. **설정** 섹션을 엽니다.
3. Kaspersky Security Center 중앙 관리 서버에 연결된 Kaspersky Industrial CyberSecurity for Nodes에 대한 **로컬 (사내) 모드 업데이트 설정**에서 업데이트 경로를 구성합니다:
   a. **설정** 버튼을 클릭합니다.
   데이터베이스 및 애플리케이션 모듈 업데이트 창이 열립니다.
   b. 사용하려는 업데이트 경로 옆의 확인란을 선택합니다.
   - Kaspersky Security Center 중앙 관리 서버
   - Kaspersky 업데이트 서버

   필요하다면 **추가** 버튼을 클릭해 사용자 지정 업데이트 경로를 추가하십시오.
   c. 여러 업데이트 경로를 선택하는 경우 **위로** 그리고 **아래로** 버튼을 사용하여 우선순위에 따라 업데이트 경로를 정렬하십시오. Kaspersky Industrial CyberSecurity for Nodes는 엄격하게 구성된 순서에 따라 업데이트 경로에 접근하고, 이용 가능한 첫 번째 업데이트 경로의 업데이트 패키지를 사용하여 업데이트 작업을 수행합니다.
   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Center 서버를 첫 번째 업데이트 경로로 사용합니다. 이는 업데이트 시 트래픽을 절약하는 데 도움이 됩니다. 정책이 컴퓨터에 적용되지 않은 경우 애플리케이션이 Kaspersky Security Center 서버에 접근할 수 없기 때문에 로컬 *업데이트* 작업 설정에서 Kaspersky 서버가 첫 번째 업데이트 경로로 선택됩니다.
   d. 업데이트 경로로 **Kaspersky 업데이트 서버**를 선택했다면, Kaspersky 업데이트 서버 선택 시 Kaspersky Industrial CyberSecurity for Nodes가 따라야 하는 원칙을 선택합니다:
   - **자동 탐지**. 애플리케이션이 가장 가까운 Kaspersky 업데이트 서버를 사용합니다.
   - **목록에서 선택**. 애플리케이션이 목록에서 선택한 국가의 Kaspersky 업데이트 서버를 사용합니다.

   e. **데이터베이스 및 애플리케이션 모듈 업데이트** 창에서 **확인** 버튼을 클릭합니다.
4. 애플리케이션 데이터베이스 업데이트를 구성하려면:
   a. **애플리케이션 데이터베이스 업데이트 다운로드** 확인란을 선택하거나 선택 해제합니다.
   b. **디스크 I/O 부하 낮추기** 확인란을 선택하거나 선택 해제합니다. 이 확인란은 업데이트 파일을 RAM의 가상 드라이브에 저장하여 디스크 하위 시스템을 최적화하는 과정을 활성화 또는 비활성화합니다. 기본적으로 확인란의 선택이 취소됩니다.
   c. **디스크 I/O 부하 낮추기** 확인란을 선택했다면 **최적화에 사용되는 RAM, MB** 필드에서 RAM 크기(MB)를 지정합니다. 작업 실행 시 운영 체제에서 지정된 RAM 볼륨을 업데이트 파일 저장을 위해 일시적으로 할당합니다. 기본 RAM 크기는 640MB입니다. 최소 RAM 크기는 400MB입니다.

디스크 하위 시스템 최적화 기능을 활성화한 상태에서 *업데이트* 작업을 실행하면 다음 중 하나가 발생할 수 있습니다.

- 값이 너무 작은 경우 할당된 RAM이 데이터베이스 업데이트 작업을 완료하는 데 부족하여(예: 첫 번째 업데이트 중) 오류가 발생하며 작업이 완료될 수 있습니다.

  이 경우 디스크 하위 시스템 최적화 기능에 할당할 RAM을 늘리는 것이 좋습니다.

- 값이 너무 크면 데이터베이스 업데이트 작업 시작 시 RAM에서 선택한 크기의 가상 드라이브를 만드는 것이 불가능할 수 있습니다. 결과적으로 디스크 하위 시스템 최적화 기능이 자동으로 비활성화되고 데이터베이스 업데이트 작업이 최적화 기능 없이 실행됩니다.

  이 경우 디스크 하위 시스템 최적화 기능에 할당할 RAM을 줄이는 것이 좋습니다.

5. 애플리케이션 소프트웨어 모듈 업데이트를 구성합니다:

   a. **애플리케이션 모듈 업데이트 다운로드** 확인란을 선택하거나 선택 해제합니다.

   확인란이 선택되어 있다면, Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 모듈 업데이트가 있을 경우 이를 사용자에게 알리고 *업데이트* 작업 실행 시 업데이트 패키지 안에 애플리케이션 모듈 업데이트를 포함합니다. 적용할 애플리케이션 모듈 업데이트의 유형은 별도로 구성됩니다. 기본적으로 확인란이 선택되어 있습니다.

   b. 적용할 애플리케이션 모듈 업데이트를 선택합니다.

   - **긴급 및 승인된 업데이트 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Industrial CyberSecurity for Nodes는 자동으로 긴급 업데이트를 설치하고 나머지 모든 애플리케이션 모듈은 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다.

   - **승인된 업데이트만 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Industrial CyberSecurity for Nodes는 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다. 이 옵션은 기본적으로 선택되어 있습니다.

   애플리케이션 모듈 업데이트를 검토하고 최종 사용자 라이센스 계약서 조항을 승인하면, 애플리케이션은 최종 사용자 라이센스 계약서가 사용자에 의해 수락된 후 업데이트를 설치합니다.

6. 로컬 저장소용 폴더에 업데이트 복사를 구성합니다:

   a. **로컬 저장소용 폴더에 업데이트 복사** 확인란을 선택하거나 선택 해제합니다.

   b. 애플리케이션이 로컬 저장소 폴더에 복사할 업데이트 컨텐츠를 선택합니다:

   - **데이터베이스 업데이트 복사**. 애플리케이션은 데이터베이스 업데이트만 다운로드합니다.

   - **중요 애플리케이션 모듈 업데이트 복사**. 애플리케이션은 중요한 애플리케이션 모듈 업데이트만 다운로드합니다.

   - **데이터베이스 업데이트와 애플리케이션 모듈의 중요 업데이트 복사**. 애플리케이션이 데이터베이스 업데이트 및 중요 애플리케이션 모듈 업데이트를 다운로드합니다.

   c. Kaspersky Industrial CyberSecurity for Nodes가 다운로드된 업데이트를 배포할 로컬 또는 네트워크 폴더를 지정합니다.

7. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 업데이트 작업을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **업데이트 → 데이터베이스 및 애플리케이션 모듈 업데이트** 노드를 엽니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.

   속성: 데이터베이스 및 애플리케이션 모듈 업데이트 창이 열립니다.

3. Kaspersky Security Center 중앙 관리 서버에 연결된 Kaspersky Industrial CyberSecurity for Nodes에 대한 **로컬 (사내) 모드 업데이트 설정**에서 업데이트 경로를 구성합니다:

   a. **설정** 버튼을 클릭합니다.

   데이터베이스 및 애플리케이션 모듈 업데이트 창이 열립니다.

   b. 사용하려는 업데이트 경로 옆의 확인란을 선택합니다.

   - Kaspersky Security Center 중앙 관리 서버
   - Kaspersky 업데이트 서버

   필요하다면 **추가** 버튼을 클릭해 사용자 지정 업데이트 경로를 추가하십시오.

   c. 여러 업데이트 경로를 선택하는 경우 **위로** 그리고 **아래로** 버튼을 사용하여 우선순위에 따라 업데이트 경로를 정렬하십시오. Kaspersky Industrial CyberSecurity for Nodes는 엄격하게 구성된 순서에 따라 업데이트 경로에 접근하고, 이용 가능한 첫 번째 업데이트 경로의 업데이트 패키지를 사용하여 업데이트 작업을 수행합니다.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Center 서버를 첫 번째 업데이트 경로로 사용합니다. 이는 업데이트 시 트래픽을 절약하는 데 도움이 됩니다. 정책이 컴퓨터에 적용되지 않은 경우 애플리케이션이 Kaspersky Security Center 서버에 접근할 수 없기 때문에 로컬 *업데이트* 작업 설정에서 Kaspersky 서버가 첫 번째 업데이트 경로로 선택됩니다.

   d. 업데이트 경로로 **Kaspersky 업데이트 서버**를 선택했다면, Kaspersky 업데이트 서버 선택 시 Kaspersky Industrial CyberSecurity for Nodes가 따라야 하는 원칙을 선택합니다:

   - **자동 탐지**. 애플리케이션이 가장 가까운 Kaspersky 업데이트 서버를 사용합니다.
   - **목록에서 선택**. 애플리케이션이 목록에서 선택한 국가의 Kaspersky 업데이트 서버를 사용합니다.

   e. **데이터베이스 및 애플리케이션 모듈 업데이트** 창에서 **확인** 버튼을 클릭합니다.

4. 애플리케이션 데이터베이스 업데이트를 구성하려면:

   a. **애플리케이션 데이터베이스 업데이트 다운로드** 확인란을 선택하거나 선택 해제합니다.

   b. **디스크 I/O 부하 낮추기** 확인란을 선택하거나 선택 해제합니다. 이 확인란은 업데이트 파일을 RAM의 가상 드라이브에 저장하여 디스크 하위 시스템을 최적화하는 과정을 활성화 또는 비활성화합니다. 기본적으로 확인란의 선택이 취소됩니다.

   c. **디스크 I/O 부하 낮추기** 확인란을 선택했다면 **최적화에 사용되는 RAM, MB** 필드에서 RAM 크기(MB)를 지정합니다. 작업 실행 시 운영 체제에서 지정된 RAM 볼륨을 업데이트 파일 저장을 위해 일시적으로 할당합니다. 기본 RAM 크기는 640MB입니다. 최소 RAM 크기는 400MB입니다.

디스크 하위 시스템 최적화 기능을 활성화한 상태에서 *업데이트* 작업을 실행하면 다음 중 하나가 발생할 수 있습니다.

- 값이 너무 작은 경우 할당된 RAM이 데이터베이스 업데이트 작업을 완료하는 데 부족하여(예: 첫 번째 업데이트 중) 오류가 발생하며 작업이 완료될 수 있습니다.

  이 경우 디스크 하위 시스템 최적화 기능에 할당할 RAM을 늘리는 것이 좋습니다.

- 값이 너무 크면 데이터베이스 업데이트 작업 시작 시 RAM에서 선택한 크기의 가상 드라이브를 만드는 것이 불가능할 수 있습니다. 결과적으로 디스크 하위 시스템 최적화 기능이 자동으로 비활성화되고 데이터베이스 업데이트 작업이 최적화 기능 없이 실행됩니다.

  이 경우 디스크 하위 시스템 최적화 기능에 할당할 RAM을 줄이는 것이 좋습니다.

5. 애플리케이션 소프트웨어 모듈 업데이트를 구성합니다:

   a. **애플리케이션 모듈 업데이트 다운로드** 확인란을 선택하거나 선택 해제합니다.

   확인란이 선택되어 있다면, Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 모듈 업데이트가 있을 경우 이를 사용자에게 알리고 *업데이트* 작업 실행 시 업데이트 패키지 안에 애플리케이션 모듈 업데이트를 포함합니다. 적용할 애플리케이션 모듈 업데이트의 유형은 별도로 구성됩니다. 기본적으로 확인란이 선택되어 있습니다.

   b. 적용할 애플리케이션 모듈 업데이트를 선택합니다.

   - **긴급 및 승인된 업데이트 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Industrial CyberSecurity for Nodes는 자동으로 긴급 업데이트를 설치하고 나머지 모든 애플리케이션 모듈은 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다.

   - **승인된 업데이트만 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Industrial CyberSecurity for Nodes는 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다. 이 옵션은 기본적으로 선택되어 있습니다.

   애플리케이션 모듈 업데이트를 검토하고 최종 사용자 라이센스 계약서 조항을 승인하면, 애플리케이션은 최종 사용자 라이센스 계약서가 사용자에 의해 수락된 후 업데이트를 설치합니다.

6. 로컬 저장소용 폴더에 업데이트 복사를 구성합니다:

   a. **로컬 저장소용 폴더에 업데이트 복사** 확인란을 선택하거나 선택 해제합니다.

   b. 애플리케이션이 로컬 저장소 폴더에 복사할 업데이트 컨텐츠를 선택합니다:

   - **데이터베이스 업데이트 복사**. 애플리케이션은 데이터베이스 업데이트만 다운로드합니다.

   - **중요 애플리케이션 모듈 업데이트 복사**. 애플리케이션은 중요한 애플리케이션 모듈 업데이트만 다운로드합니다.

   - **데이터베이스 업데이트와 애플리케이션 모듈의 중요 업데이트 복사**. 애플리케이션이 데이터베이스 업데이트 및 중요 애플리케이션 모듈 업데이트를 다운로드합니다.

   c. Kaspersky Industrial CyberSecurity for Nodes가 다운로드된 업데이트를 배포할 로컬 또는 네트워크 폴더를 지정합니다.

7. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 업데이트 작업을 구성하는 방법

1. 웹 콘솔에서 구성할 로컬 또는 그룹 *업데이트* 작업으로 갑니다.
2. **설정** 섹션을 엽니다.
3. **로컬 모드** 탭을 선택하여 Kaspersky Security Center 중앙 관리 서버에 연결된 Kaspersky Industrial CyberSecurity for Nodes의 *업데이트* 작업을 구성합니다.
4. 업데이트 경로 구성:
   a. **업데이트 경로**에서 사용할 업데이트 경로 옆의 확인란을 선택합니다:
      - **Kaspersky Security Center 중앙 관리 서버**
      - **Kaspersky 업데이트 서버**

      필요하다면 **추가** 버튼을 클릭해 사용자 지정 업데이트 경로를 추가하십시오.
   b. 여러 업데이트 경로를 선택하는 경우 **위로** 그리고 **아래로** 버튼을 사용하여 우선순위에 따라 업데이트 경로를 정렬하십시오. Kaspersky Industrial CyberSecurity for Nodes는 엄격하게 구성된 순서에 따라 업데이트 경로에 접근하고, 이용 가능한 첫 번째 업데이트 경로의 업데이트 패키지를 사용하여 업데이트 작업을 수행합니다.

      기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Security Center 서버를 첫 번째 업데이트 경로로 사용합니다. 이는 업데이트 시 트래픽을 절약하는 데 도움이 됩니다. 정책이 컴퓨터에 적용되지 않은 경우 애플리케이션이 Kaspersky Security Center 서버에 접근할 수 없기 때문에 로컬 *업데이트* 작업 설정에서 Kaspersky 서버가 첫 번째 업데이트 경로로 선택됩니다.
5. 애플리케이션 데이터베이스 업데이트를 구성하려면:
   a. **애플리케이션 데이터베이스 업데이트 다운로드** 확인란을 선택하거나 선택 해제합니다.
   b. **디스크 I/O 부하 낮추기** 확인란을 선택하거나 선택 해제합니다. 이 확인란은 업데이트 파일을 RAM의 가상 드라이브에 저장하여 디스크 하위 시스템을 최적화하는 과정을 활성화 또는 비활성화합니다. 기본적으로 확인란의 선택이 취소됩니다.
   c. **디스크 I/O 부하 낮추기** 확인란을 선택했다면 **최적화에 사용되는 RAM, MB** 필드에서 RAM 크기(MB)를 지정합니다. 작업 실행 시 운영 체제에서 지정된 RAM 볼륨을 업데이트 파일 저장을 위해 일시적으로 할당합니다. 기본 RAM 크기는 640MB입니다. 최소 RAM 크기는 400MB입니다.

      디스크 하위 시스템 최적화 기능을 활성화한 상태에서 *업데이트* 작업을 실행하면 다음 중 하나가 발생할 수 있습니다.

      - 값이 너무 작은 경우 할당된 RAM이 작업을 완료하는 데 부족하여(예: 첫 번째 업데이트 중) 오류가 발생하며 작업이 완료될 수 있습니다.

        이 경우 디스크 하위 시스템 최적화 기능에 할당할 RAM을 늘리는 것이 좋습니다.
      - 값이 너무 크면 작업 시작 시 RAM에서 선택한 크기의 가상 드라이브를 만드는 것이 불가능할 수 있습니다. 결과적으로 디스크 하위 시스템 최적화 기능이 자동으로 비활성화되고 데이터베이스 업데이트 작업이 최적화 기능 없이 실행됩니다.

        이 경우 디스크 하위 시스템 최적화 기능에 할당할 RAM을 줄이는 것이 좋습니다.

6. 애플리케이션 소프트웨어 모듈 업데이트를 구성합니다:

   a. **애플리케이션 모듈 업데이트 다운로드** 확인란을 선택하거나 선택 해제합니다.

      확인란이 선택되어 있다면, Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 모듈 업데이트가 있을 경우 이를 사용자에게 알리고 *업데이트* 작업 실행 시 업데이트 패키지 안에 애플리케이션 모듈 업데이트를 포함합니다. 적용할 애플리케이션 모듈 업데이트의 유형은 별도로 구성됩니다. 기본적으로 확인란이 선택되어 있습니다.

   b. 적용할 애플리케이션 모듈 업데이트를 선택합니다.

      - **긴급 및 승인된 업데이트 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Industrial CyberSecurity for Nodes는 자동으로 긴급 업데이트를 설치하고 나머지 모든 애플리케이션 모듈은 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다.

      - **승인된 업데이트만 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Industrial CyberSecurity for Nodes는 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다. 이 옵션은 기본적으로 선택되어 있습니다.

      애플리케이션 모듈 업데이트를 검토하고 최종 사용자 라이센스 계약서 조항을 승인하면, 애플리케이션은 최종 사용자 라이센스 계약서가 사용자에 의해 수락된 후 업데이트를 설치합니다.

7. 로컬 저장소용 폴더에 업데이트 복사를 구성합니다:

   a. **폴더로 업데이트 파일 복사** 확인란을 선택하거나 선택 해제합니다.

   b. 애플리케이션이 로컬 저장소 폴더에 복사할 업데이트 컨텐츠를 선택합니다:

      - **데이터베이스 업데이트 복사**. 애플리케이션은 데이터베이스 업데이트만 다운로드합니다.

      - **중요 애플리케이션 모듈 업데이트 복사**. 애플리케이션은 중요한 애플리케이션 모듈 업데이트만 다운로드합니다.

      - **데이터베이스 업데이트와 애플리케이션 모듈의 중요 업데이트 복사**. 애플리케이션이 데이터베이스 업데이트 및 중요 애플리케이션 모듈 업데이트를 다운로드합니다.

   c. Kaspersky Industrial CyberSecurity for Nodes가 다운로드된 업데이트를 배포할 로컬 또는 네트워크 폴더를 지정합니다.

8. 변경 사항을 저장합니다.

애플리케이션의 SMU 업데이트

Kaspersky 업데이트 서비스(Seamless Update; SMU)를 사용하여 애플리케이션을 업데이트하면 다른 업데이트 방법과 달리 설치 프로그램을 실행할 필요가 없습니다. Kaspersky Industrial CyberSecurity for Nodes는 동일한 경로에서 안티 바이러스 데이터베이스와 함께 새 버전의 애플리케이션을 가져옵니다.

SMU 업데이트를 사용하면 조직 내 모든 컴퓨터의 애플리케이션을 최신 버전으로 업데이트할 수 있습니다. SMU 업데이트를 적용하기 전에 몇 대의 컴퓨터에서 새 버전의 애플리케이션을 테스트하는 것을 권장합니다. 이렇게 하려면 컴퓨터에서 수동으로 애플리케이션을 업데이트해야 합니다(예: 로컬에서 설치 마법사를 사용). SMU 업데이트를 수행할 때는 개별 컴퓨터를 선택할 수 없습니다.

애플리케이션의 업데이트 스케줄은 Kaspersky 직원이 결정합니다. 새 버전의 애플리케이션이 원활하게 실행될 수 있도록 Kaspersky는 단계별로 업데이트를 제공합니다. 따라서 새 버전이 출시되는 것보다 최대 2개월 늦게 SMU 업데이트를 받을 수 있습니다.

업데이트 작업을 사용하여 애플리케이션의 SMU 업데이트를 관리할 수 있습니다. 새 버전의 애플리케이션을 안티 바이러스 데이터베이스와 동일한 패키지에 포함하려면 *업데이트* 작업 설정에서 *애플리케이션 모듈* 업데이트를 허용해야 합니다.

애플리케이션의 SMU 업데이트 단계

1. **애플리케이션의 새 버전이 출시되거나 모듈이 업데이트되면 Kaspersky에서 업데이트를 배포합니다.**
2. **사용자가 애플리케이션 업데이트를 승인합니다.**

   컴퓨터가 Kaspersky Security Center에 연결되어 있는 경우 Kaspersky Security Center의 **Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트** 섹션에서 업데이트할 수 있습니다. 업데이트 승인에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

   컴퓨터가 Kaspersky Security Center에 연결되어 있지 않은 경우 애플리케이션 콘솔에서 업데이트를 사용할 수 있습니다. 업데이트를 승인하려면 **업데이트 → 애플리케이션 업데이트** 섹션에서 애플리케이션 버전을 선택하고, 필요한 경우 계약 약관 및 조건에 동의합니다.
3. **Kaspersky Industrial CyberSecurity for Nodes는 스케줄에 따라 업데이트 작업을 실행합니다.**

결과적으로 Kaspersky Industrial CyberSecurity for Nodes는 "숨김" 모드로 애플리케이션을 업데이트합니다.

애플리케이션 데이터베이스의 보안 복사

이 작업은 애플리케이션 콘솔에서만 구성할 수 있습니다. Kaspersky Security Center 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서는 이 작업을 구성할 수 없습니다.

애플리케이션 데이터베이스 보안 복사 작업을 구성하고 시작하려면:

1. 애플리케이션 콘솔 트리에 있는 **업데이트** 노드의 마우스 오른쪽 메뉴에서, **데이터베이스를 안전하게 복사하기 시작** 옵션을 선택합니다.

   보안 애플리케이션 데이터베이스 복사 마법사의 시작 창이 열립니다.

2. **다음(N) >** 버튼을 클릭합니다.

3. **업데이트 경로**에서 업데이트 경로를 선택합니다:

   - **Kaspersky Security Center 중앙 관리 서버**.

     네트워크의 Kaspersky 애플리케이션이 Kaspersky Security Center 원격 접근 시스템으로 관리되는 경우 및 네트워크 에이전트(보호 중인 장치와 중앙 관리 서버 간의 연결을 제공하는 Kaspersky Security Center 구성 요소)가 보호 중인 장치에 설치된 경우에만 이 옵션을 선택할 수 있습니다.

     이 옵션은 기본적으로 선택되어 있습니다.

   - **Kaspersky 업데이트 서버**.

     Kaspersky 애플리케이션이 데이터베이스 및 애플리케이션 모듈 업데이트를 다운로드하는 Kaspersky HTTP 및 HTTPS 서버.

   - **사용자 지정 HTTP 또는 FTP 서버 또는 네트워크 폴더**.

4. 이전 단계에서 **Kaspersky Security Center 중앙 관리 서버**을(를) 선택한 경우 **지정된 서버를 사용할 수 없는 경우 Kaspersky 업데이트 서버 사용** 기능을 구성합니다. 이 옵션을 활성화하면 Kaspersky Security Center 중앙 관리 서버를 사용할 수 없는 경우 Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky 업데이트 서버를 업데이트 경로로 사용합니다.

5. **소스 연결 설정 업데이트**에서 업데이트 경로에 연결하기 위한 프록시 서버 사용을 구성합니다.

6. **다음(N) >** 버튼을 클릭합니다.

7. 드롭다운 목록에서 애플리케이션 안티 바이러스 데이터베이스를 저장할 연결된 보안 Rutoken 이동식 드라이브를 선택합니다.

   Portable Auditor 생성과 애플리케이션 데이터베이스의 안전한 복사에 동일한 Rutoken 이동식 드라이브를 동시에 사용할 수 없습니다.

   장치 제어 구성 요소의 규칙을 통해 특별히 승인된 Rutoken 이동식 드라이브만 보안 이동식 드라이브로 사용할 수 있습니다.

8. 잠재적 침입자가 Rutoken 이동식 드라이브의 콘텐츠를 읽거나 복사하거나 쓰지 못하도록 **보안 설정**의 **현재 관리자 PIN 코드 입력** 필드에 Rutoken 이동식 드라이브에 설정된 관리자 PIN 코드를 입력합니다.

9. 현재 관리자 PIN을 변경하려면:

   a. **관리자의 현재 PIN 코드 변경(숫자와 라틴 문자만 허용)** 확인란을 선택합니다.

   b. 새 PIN을 입력합니다.

   c. 새 PIN을 확인합니다.

10. 사용자 PIN을 설정합니다. 이 PIN은 *애플리케이션 데이터베이스의 안전한 업데이트* 작업 및 선택한 Rutoken 이동식 드라이브를 사용하여 애플리케이션 데이터베이스를 업데이트할 직원에게 필요합니다.

    a. 사용자 PIN을 입력합니다.

    b. 사용자 PIN을 확인합니다.

11. **다음(N) >** 버튼을 클릭합니다.

Rutoken 이동식 드라이브로 애플리케이션 데이터베이스의 보안 복사가 시작됩니다. 설정은 작업이 실행되는 동안 저장 및 적용됩니다.

두 개의 Rutoken 이동식 드라이브를 동일한 장치에 연결하여 애플리케이션 데이터베이스의 안전한 복사 작업과 Portable Auditor 생성 작업을 동시에 실행하는 것은 권장되지 않습니다. 이 경우 작업이 오류로 종료될 수 있습니다.

애플리케이션 데이터베이스의 보안 업데이트

애플리케이션 데이터베이스의 안전한 업데이트 작업은 폐쇄된 회사 네트워크와 애플리케이션 데이터베이스에 접근할 수 없는 장치에서 잠재적 침입자의 읽기, 복사 및 쓰기로부터 보호되는 보안 이동식 드라이브를 사용하여 애플리케이션 데이터베이스를 업데이트하는 데 필요합니다.

이 작업은 Kaspersky Industrial CyberSecurity for Nodes와 동일한 장치에 설치된 애플리케이션 콘솔을 통해서만 시작할 수 있습니다. 관리 콘솔 또는 웹 콘솔에서는 작업을 구성할 수 없습니다.

애플리케이션 데이터베이스의 안전한 업데이트 작업을 실행하려면:

1. 애플리케이션 콘솔 트리에 있는 **업데이트** 노드의 마우스 오른쪽 메뉴에서, **데이터베이스를 안전하게 업데이트하기 시작** 옵션을 선택합니다.

   보안 애플리케이션 데이터베이스 업데이트 마법사의 시작 창이 열립니다. **다음(N) >** 버튼을 클릭합니다.

2. 드롭다운 목록에서 애플리케이션 안티 바이러스 데이터베이스가 들어 있는 연결된 보안 이동식 드라이브를 선택합니다.

   장치 제어 구성 요소의 규칙을 통해 특별히 승인된 Rutoken 이동식 드라이브만 보안 이동식 드라이브로 사용할 수 있습니다.

3. 애플리케이션 데이터베이스 복사 단계에서 지정한 Rutoken 이동식 드라이브의 PIN을 입력합니다.

4. **마침** 버튼을 클릭합니다.

애플리케이션 데이터베이스의 보안 업데이트 작업이 시작됩니다. 애플리케이션 데이터베이스가 Rutoken 이동식 드라이브에서 복사됩니다.

Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 업데이트 롤백

데이터베이스 업데이트를 수행하기 전에 Kaspersky Industrial CyberSecurity for Nodes는 이전에 사용된 데이터베이스의 백업 복사본을 생성합니다. 업데이트가 중단되거나 오류를 일으키면 Kaspersky Industrial CyberSecurity for Nodes는 이전에 설치된 데이터베이스를 자동으로 사용합니다.

데이터베이스 업데이트 후 문제가 발생하면 *마지막 업데이트 롤백* 작업을 통해 이전에 설치된 업데이트로 롤백할 수 있습니다.

마지막 업데이트 롤백 작업을 실행하려면:

1. 애플리케이션 콘솔 트리에서 **업데이트 → 마지막 업데이트 롤백** 섹션을 엽니다.
2. 결과 창에서 **시작** 링크를 클릭합니다.

업데이트 작업 통계

업데이트 작업이 실행되는 동안 작업 시작 이후 다운로드된 데이터의 양과 기타 작업 실행 통계에 관한 실시간 정보가 표시됩니다.

작업이 완료되었거나 정지된 경우 이 정보를 작업 로그에서 볼 수 있습니다.

업데이트 작업 통계를 보려면:

애플리케이션 콘솔 트리에서 **업데이트 → 데이터베이스 및 애플리케이션 모듈 업데이트** 섹션을 엽니다.

결과 창의 **통계**에서 수집 데이터의 총량에 관한 정보를 찾을 수 있습니다.

Detection and Response 솔루션

Kaspersky Detection and Response 솔루션은 조직 인프라의 다양한 수준에서 지능형 위협 및 공격 지표를 탐지하기 위한 보안 시스템입니다. Detection and Response 솔루션은 탐지된 위협에 대한 정보를 제공하고 위협 대응 조치를 관리할 수 있도록 합니다.

이에 따라 Detection and Response 솔루션은 다음을 수행합니다.

- 컴퓨터, 서버 또는 기타 장치(원격 측정)의 작동에 대한 정보를 받습니다.
- 정보를 자동으로 분석하여 위협을 탐지합니다.
- 분석 및 위협 대응 조치 선택을 위해 경보 세부 정보를 위협 개발 체인의 열로 생성합니다.
- 위협 대응 조치를 수행합니다(예: 컴퓨터의 네트워크 격리).

Kaspersky Industrial CyberSecurity for Nodes는 *Endpoint Agent* 내장 에이전트(이하 *내장 에이전트*)를 사용하는 Detection and Response 솔루션을 지원합니다. 내장 에이전트는 솔루션 서버에 원격 측정을 전송하고 위협 대응 조치를 수행합니다. 내장 에이전트 지원 사항:

- Kaspersky Managed Detection and Response(MDR)
- Kaspersky Industrial CyberSecurity Endpoint Detection and Response
- Kaspersky Endpoint Detection and Response Expert(on-premise)
- Kaspersky Anti Targeted Attack Platform(원격 측정만 해당)

Kaspersky Industrial CyberSecurity Endpoint Detection and Response

Kaspersky Industrial CyberSecurity Endpoint Detection and Response는 지능형 사이버 위협으로부터 조직의 IT 인프라를 보호하기 위한 솔루션입니다. 이 솔루션은 자동 위협 탐지 기능과 보안 위협 대응 기능을 결합하여 신종 익스플로잇, 랜섬웨어, 파일리스 공격 및 합법적인 시스템 도구를 사용하는 기법을 비롯한 복합 공격에 대응합니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response는 위협의 진행 과정을 검토하고 분석하며, 보안 담당자 또는 관리자에게 위협에 적시에 대응할 수 있도록 잠재적 공격에 대한 정보를 제공하거나 지정된 대응 작업을 자동으로 수행합니다.

Kaspersky Security for Business Professional 라이선스 사용자는 분석 및 대응 기능을 확장하는 Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 추가 기능을 사용할 수 있습니다.

- 격리에서 Kaspersky TIP으로 파일 전송
- 경고 세부 정보에서 Active Directory 사용자에 대한 대응 작업 수행
- 경고 세부 정보에서 사용자에게 Kaspersky ASAP 교육 과정 할당

업데이트 기능(안티바이러스 서명 업데이트 및 코드베이스 업데이트 제공이 포함)과 KSN 기능이 미국 내 솔루션에서 제공되지 않을 수 있습니다.

솔루션 아키텍처

Kaspersky Industrial CyberSecurity Endpoint Detection and Response에는 다음 구성 요소가 포함됩니다.

- Kaspersky Industrial CyberSecurity Endpoint Detection and Response 기능을 지원하며 조직의 IT 인프라 내 개별 장치에 설치되는 EPP Kaspersky 애플리케이션(Kaspersky Industrial CyberSecurity for Nodes 또는 Kaspersky Industrial CyberSecurity for Linux Nodes). 이 애플리케이션은 보호 대상 장치에서 실행 중인 프로세스, 열린 네트워크 연결 및 파일 변경 사항을 지속적으로 모니터링합니다.
- Kaspersky Endpoint Agent는 장치에서 실행 중인 프로세스, 열린 네트워크 연결 및 수정된 파일에 대한 정보를 지속적으로 모니터링하여 Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0으로 전송하는 애플리케이션입니다. Kaspersky Industrial CyberSecurity for Linux Nodes 또는 Kaspersky Industrial CyberSecurity for Nodes 버전 4.5 이상을 사용하는 경우 Kaspersky Endpoint Agent를 설치할 필요가 없습니다.
- 중앙 집중식 네트워크 보안 관리를 위한 솔루션(Kaspersky Security Center).
- 위협 인텔리전스 도구:
  - 파일, 웹사이트 및 소프트웨어에 대한 정보가 포함된 Kaspersky의 온라인 기술 자료에 접속할 수 있는 Kaspersky Security Network(KSN) 클라우드 서비스 인프라입니다. Kaspersky Security Network의 데이터를 사용하면 Kaspersky 애플리케이션에서 보안 위협에 신속하게 대응할 수 있으며, 일부 보호 구성 요소의 성능을 향상하고 오탐의 가능성을 줄입니다.
  - Kaspersky Private Security Network(KPSN)와의 통합을 통해 사용자는 자신의 장치에서 KSN으로 데이터를 전송하지 않고도 KSN 평판 데이터베이스 및 기타 통계에 접근할 수 있습니다.
  - 파일 및 URL의 평판에 대한 정보를 포함하고 표시하는 Kaspersky Threat Intelligence Portal과의 통합. Kaspersky Threat Intelligence Portal과의 통합을 통해 수행할 수 있는 작업:
    - 경고 세부 정보에서 개체에 대한 추가 정보를 검색합니다.
    - 격리된 파일을 위협 분석을 위해 전송합니다(Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 확장 기능을 사용하는 경우).
  - Kaspersky 보안 위협 데이터베이스.

다중 테넌트 지원

*다중 테넌트 지원*은 솔루션을 사용하여 여러 조직의 인프라를 동시에 보호하는 운영 모드입니다.

Kaspersky Security Center를 사용하면 Kaspersky Industrial CyberSecurity Endpoint Detection and Response를 통해 여러 조직의 인프라를 동시에 보호할 수 있습니다. 이를 위해 Kaspersky Industrial CyberSecurity Endpoint Detection and Response를 사용하여 보호할 각 조직의 가상 중앙 관리 서버를 생성합니다. 이러한 가상 중앙 관리 서버는 서비스 제공자 조직의 물리적 중앙 관리 서버 아래에 생성해야 합니다. 가상 중앙 관리 서버 생성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

각 테넌트 조직마다 별도의 가상 중앙 관리 서버를 생성해야 합니다. 물리적 중앙 관리 서버의 관리자는 해당 서버에서 관리하는 모든 장치의 솔루션을 관리할 수 있습니다. 가상 중앙 관리 서버의 관리자는 자신이 관리하는 서버에 연결된 장치에서만 솔루션을 관리할 수 있습니다.

Kaspersky 애플리케이션과의 호환성

Kaspersky Industrial CyberSecurity Endpoint Detection and Response는 다음 버전의 Kaspersky 애플리케이션과 호환됩니다.

- Kaspersky Industrial CyberSecurity for Linux Nodes 1.5 이상

  Kaspersky Industrial CyberSecurity for Linux® Nodes는 다음 버전의 Kaspersky Security Center가 필요합니다:

  - Kaspersky Security Center Windows 14.2 이상
  - Kaspersky Security Center Linux 15.1 이상

- Kaspersky Industrial CyberSecurity for Nodes 3.1 이상

  Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우 Kaspersky Industrial CyberSecurity for Nodes를 사용하려면 Kaspersky Endpoint Agent도 설치해야 합니다. Kaspersky Endpoint Agent는 Microsoft® Windows® 운영 체제가 설치된 조직의 IT 인프라 내 개별 장치에 설치할 수 있습니다. 이 애플리케이션은 Kaspersky Industrial CyberSecurity for Nodes용 Kaspersky Industrial CyberSecurity Endpoint Detection and Response를 지원합니다. Kaspersky Industrial CyberSecurity Endpoint Detection and Response는 Kaspersky Endpoint Agent 3.13 이상과의 통합을 지원합니다.

  Kaspersky Industrial CyberSecurity for Nodes 4.5 이상에는 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 솔루션에서 작동하는 내장 에이전트가 도입되었습니다.

  지정된 버전의 Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Endpoint Agent와 함께 사용해야 하는 Kaspersky Security Center 버전은 다음과 같습니다.

  - Kaspersky Security Center 버전 10.5~12.1은 Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 일부 기능만 지원합니다(Kaspersky Security Center 버전별 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 기능에 대한 자세한 내용은 라이선스를 구매한 Kaspersky 파트너에게 문의하십시오).
  - Kaspersky Security Center Windows 12.1 이상은 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 기능을 완전히 지원합니다.
  - Kaspersky Security Center Linux 15.1 이상

Kaspersky Security for Business Professional 라이선스 사용자를 위한 Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 확장 기능은 다음 버전의 Kaspersky 애플리케이션과 호환됩니다.

- Kaspersky Industrial CyberSecurity for Nodes 4.5 이상
- Endpoint Detection and Response 플러그인 버전 15.4 이상이 설치된 Kaspersky Security Center Linux 버전 15.4 이상.

배포 및 초기 설정

Kaspersky Industrial CyberSecurity Endpoint Detection and Response가 작동하려면 다음 조건을 충족해야 합니다.

- 웹 콘솔이 포함된 Kaspersky Security Center 지원 버전이 설치되어 있습니다.

  Kaspersky Security Center 설치에 대한 자세한 내용은 Kaspersky Security Center 도움말 및 Kaspersky Security Center Linux 도움말을 참조하십시오.

- Kaspersky Industrial CyberSecurity for Nodes 또는 Kaspersky Industrial CyberSecurity for Linux Nodes가 보호 대상 장치에 설치되어 있습니다(Kaspersky Industrial CyberSecurity for Linux Nodes 설치에 대한 자세한 내용은 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오).

- Kaspersky Industrial CyberSecurity for Nodes 또는 Kaspersky Industrial CyberSecurity for Linux Nodes 관리 웹 플러그인이 설치되어 있습니다.

  관리 웹 플러그인 설치에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

- Endpoint Detection and Response 웹 플러그인이 설치되어 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 4.5 이상을 사용한 솔루션 배포 및 초기 설정

배포 및 초기 구성 시나리오는 다음 단계로 구성됩니다.

1. **Endpoint Detection and Response(Industrial CyberSecurity) 구성 요소 설치**

   설치 패키지 설정이나 설치 마법사에서, 또는 Windows 제어판의 애플리케이션 구성 요소 집합 변경을 통해, 설치할 애플리케이션 구성 요소 선택 단계에서 다음을 선택합니다: **전체 기능** → **Endpoint Agent** → **Endpoint Detection and Response(Industrial CyberSecurity)**.

   > 애플리케이션 구성 요소 집합 변경을 완료하려면 컴퓨터를 다시 시작해야 합니다.

2. **Kaspersky Industrial CyberSecurity Endpoint Detection and Response 활성화**

3. **Kaspersky Industrial CyberSecurity for Nodes의 필수 구성 요소 활성화**

   Kaspersky Industrial CyberSecurity for Nodes의 다음 구성 요소가 활성화되어 실행 중인지 확인합니다.

   - 실시간 파일 보호
   - 익스플로잇 방지

- Anti-Cryptor
- 복원 엔진

4. **Endpoint Detection and Response(Industrial CyberSecurity) 구성 요소 활성화 및 구성**

   Kaspersky Security Center 웹 콘솔에서 Endpoint Detection and Response(Industrial CyberSecurity) 구성 요소를 활성화하고 구성하는 방법

   1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
   2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
      정책 속성 창이 열립니다.
   3. **애플리케이션 설정** 탭을 선택합니다.
   4. **원격 측정 수집 서버** 섹션을 선택합니다.
   5. **Endpoint Detection and Response(Industrial CyberSecurity)** 블록에서 **설정** 버튼을 클릭합니다.
      Endpoint Detection and Response(Industrial CyberSecurity) 창이 열립니다.
   6. **Endpoint Detection and Response(Industrial CyberSecurity) 사용** 확인란을 선택합니다.
   7. 네트워크 격리 설정을 구성합니다.
   8. 실행 방지 설정을 구성합니다.
   9. 필요하다면 Cloud Sandbox가 탐지한 위협과 같은 이름의 토글을 사용하여 해당 위협의 카운터를 활성화합니다.
   10. 변경 사항을 저장합니다.

   Kaspersky Industrial CyberSecurity for Linux Nodes에서 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 통합을 활성화하고 구성하는 방법에 대한 자세한 내용은 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

5. **Kaspersky Security Center 중앙 관리 서버로의 데이터 전송 활성화**

   모든 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 기능을 활성화하려면 다음 유형의 데이터 전송을 활성화해야 합니다.

   - 격리 파일 데이터.

     Kaspersky Security Center 웹 콘솔에서 분석을 위해 격리 저장소의 파일을 다운로드할 수 있습니다.

   - 보안 위협 개발 체인 데이터.

     웹 콘솔에서 경고 세부 정보를 확인하고 대응할 수 있습니다.

   웹 콘솔에서 중앙 관리 서버로의 데이터 전송을 활성화하는 방법

   1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
   2. 구성할 정책 이름을 클릭합니다.
   3. **<정책 이름>** 창이 열리면 **애플리케이션 설정** 탭을 선택합니다.
   4. **로그 및 알림** 섹션으로 갑니다.

5. **중앙 관리 서버와 상호 작용** 블록에서 **설정** 버튼을 클릭합니다.

6. 창이 열리면 다음 확인란을 선택합니다.

   - **격리 저장소 파일**.
   - **보안 위협 개발 체인**.

7. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response 솔루션이 Kaspersky Security Center 웹 콘솔을 통해 관리 서버를 사용하려면 새로운 보안 연결인 *백그라운드 연결*을 구성해야 합니다.

웹 콘솔에서 백그라운드 연결 구성

1. 웹 콘솔의 메인 창에서 **설정** → **통합** 옵션을 선택합니다.
2. **통합** 섹션으로 갑니다.
3. **통합을 위한 백그라운드 연결 활성화됨** 토글을 켭니다.
4. 변경 사항을 저장합니다.

6 **보안 위협 리포트 구성**

인시던트 카드를 보려면 보안 위협 리포트를 구성합니다.

7 **위젯 추가**

경고를 모니터링하려면 대시보드에 EDR 경고 위젯을 추가합니다.

8 **경고 목록 표시**

Kaspersky Security Center 웹 콘솔에서 경고 섹션 표시를 활성화합니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response를 사용할 준비가 되었습니다.

Kaspersky Industrial CyberSecurity for Nodes 3.1~4.0 버전을 사용한 솔루션 배포 및 초기 설정

Kaspersky Industrial CyberSecurity for Nodes 3.1~4.0 버전을 사용하는 경우 보호 대상 장치에 Kaspersky Endpoint Agent를 추가로 설치하고 활성화한 후, Kaspersky Endpoint Agent 관리 웹 플러그인을 설치하고 해당 정책을 생성해야 합니다. 자세한 내용은 Kaspersky Endpoint Agent 도움말을 참조하십시오.

Kaspersky Industrial CyberSecurity for Linux Nodes를 사용한 솔루션 배포 및 초기 설정

Kaspersky Industrial CyberSecurity for Linux Nodes에서 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 통합을 활성화하고 구성하는 방법에 대한 자세한 내용은 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

솔루션 활성화

Kaspersky Industrial CyberSecurity Endpoint Detection and Response를 활성화하려면 다음 애플리케이션을 활성화해야 합니다.

- Kaspersky Industrial CyberSecurity for Nodes

  > Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우 Kaspersky Endpoint Agent도 활성화해야 합니다.

- Kaspersky Industrial CyberSecurity for Linux Nodes.

이러한 애플리케이션은 보호 대상 장치에 설치하고 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 기능이 포함된 라이선스를 사용하여 활성화해야 합니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response 라이선스 구매 방법:

- Kaspersky Industrial CyberSecurity for Nodes 사용 라이선스에 포함하여.

  이 경우 솔루션 초기 설정을 완료하면 Kaspersky Industrial CyberSecurity Endpoint Detection and Response를 사용할 수 있습니다.

- 기존에 구매한 Kaspersky Industrial CyberSecurity for Nodes 사용 라이선스에 추가하여 별도로.

  Kaspersky Industrial CyberSecurity Endpoint Detection and Response 사용 라이선스를 별도로 구매한 경우 장치에 Kaspersky Industrial CyberSecurity for Nodes 애플리케이션을 설치하고 활성화한 후 새 활성화 코드 또는 키 파일을 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 활성화해야 합니다(애플리케이션 버전 3.1~4.0을 사용하는 경우 Kaspersky Endpoint Agent도 활성화해야 함).

애플리케이션을 활성화한 후 솔루션 초기 설정을 수행합니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 확장 기능을 활성화하려면 Kaspersky Security for Business Professional 라이선스로 Kaspersky Security Center Linux를 활성화해야 합니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 확장 기능을 사용하기 위한 Kaspersky Security for Business Professional 라이선스 구매 방법:

- EPP 애플리케이션 및 Kaspersky Security Center 사용 라이선스에 포함하여.

  이 경우 솔루션 초기 설정을 완료하면 솔루션을 사용할 수 있습니다.

- 기존에 구매한 Kaspersky Security Center 사용 라이선스에 추가하여 별도로.

  Kaspersky Security for Business Professional 라이선스를 별도로 구매한 경우 장치에 Kaspersky 애플리케이션을 설치하고 활성화한 후 새 활성화 코드 또는 키 파일을 사용하여 Kaspersky Security Center Linux를 다시 활성화해야 합니다. 그런 다음 솔루션 초기 설정을 수행합니다.

솔루션 활성화에 대한 자세한 내용은 Kaspersky 애플리케이션 도움말을 참조하십시오.

- Kaspersky Security Center.
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Endpoint Agent

경고 세부 정보를 보기 위한 위협 리포트 구성

위협 리포트에서 경고 세부 정보 창을 여는 기능을 구성하려면 다음을 수행합니다.

1. 웹 콘솔의 메인 창에서 **모니터링 → 리포트** 옵션을 선택합니다.
2. 리포트 목록에서 **위협 처리 리포트** 템플릿 리포트 옆의 체크박스를 선택하고 **리포트 템플릿 속성 열기** 버튼을 클릭합니다.
3. 열리는 리포트 속성 창에서 **필드** 탭으로 이동합니다.
4. **상세 정보 필드** 설정 블록의 리포트 필드 목록에 **경고 열기** 필드가 있는지 확인합니다.
5. 목록에 **경고 열기** 필드가 없으면 다음 단계를 수행합니다.
   a. **추가** 버튼을 클릭합니다.
   b. 창 오른쪽의 드롭다운 목록에서 **경고 열기** 필드를 선택합니다.
   c. **확인**을 누릅니다.
6. **저장** 버튼을 클릭합니다.

EDR 경고 위젯 추가

EDR 경고 위젯에는 지난 한 달 동안 장치에서 발생한 경고 수에 대한 정보가 표시됩니다. 이 위젯은 Kaspersky Security Center 웹 콘솔의 **대시보드** 탭에서 사용할 수 있습니다. 이 위젯을 사용하면 장치의 경고 목록이 표시되는 **경고** 섹션으로 이동할 수 있습니다.

대시보드에 EDR 경고 위젯을 추가하려면 다음과 같이 하십시오.

1. **모니터링 → 대시보드**으로 갑니다.
2. **웹 위젯 추가 또는 복원** 버튼을 클릭합니다.
3. 사용 가능한 위젯 목록의 **위협 통계** 카테고리에서 **경고** 위젯을 선택합니다.
4. **추가** 버튼을 누릅니다.
   웹 위젯이 대시보드 끝에 추가됩니다.

위젯 사용에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

장치에서 솔루션 성능 모니터링

Kaspersky Security Center 기능을 사용하면 장치의 현재 보호 상태와 인프라에서 Kaspersky Industrial CyberSecurity Endpoint Detection and Response를 지원하는 EPP 애플리케이션이 설치되지 않은 장치에 대한 정보를 확인할 수 있습니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response 구성 요소의 상태를 기준으로 장치 선택을 생성하여 이 정보를 확인할 수 있습니다.

장치 선택을 생성하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 웹 콘솔에서 **에셋 관리 → 기기 조회** 섹션으로 이동합니다.
2. 다음 조건으로 새 장치 선택을 생성합니다.
   a. **Kaspersky 애플리케이션 세부 정보** 섹션을 선택합니다.
   b. **애플리케이션 구성 요소** 목록에서 다음 옵션 중 하나를 선택합니다.
      - Kaspersky Industrial CyberSecurity for Nodes 버전 4.5 이상용 **Endpoint Detection and Response(Industrial CyberSecurity)** 구성 요소.
      - Kaspersky Endpoint Agent용 **Endpoint Detection and Response Optimum** 구성 요소(Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0이 장치에 설치된 경우).
      - Kaspersky Industrial CyberSecurity for Linux Nodes용 **Kaspersky Industrial CyberSecurity Endpoint Detection and Response 통합** 구성 요소.
   c. **상태** 드롭다운 목록에서 이 작업 상태의 장치가 표시되도록 필요한 선택 기준 값을 선택합니다.
   d. **저장** 버튼을 클릭합니다.

새 선택에는 Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 선택한 작업 상태에 해당하는 장치 목록이 표시됩니다.

확장 기능이 포함된 Kaspersky Industrial CyberSecurity Endpoint Detection and Response로 업그레이드

Kaspersky Security for Business Professional 라이선스를 구매한 경우 확장 기능이 포함된 Kaspersky Industrial CyberSecurity Endpoint Detection and Response를 사용할 수 있습니다.

확장 기능이 포함된 Kaspersky Industrial CyberSecurity Endpoint Detection and Response로 업그레이드하는 단계는 다음과 같습니다.

1. **사용자 컴퓨터의 네트워크 에이전트 구성 요소 및 Linux용 Kaspersky Security Center 웹 콘솔을 포함하여 Kaspersky Security Center Linux를 버전 15.4 이상으로 업데이트**

   자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

2. **보호 장치의 EPP 애플리케이션을 확장 기능이 포함된 Kaspersky Industrial CyberSecurity Endpoint Detection and Response를 지원하는 버전으로 업데이트**

3. **Kaspersky Security Center에 Endpoint Detection and Response 웹 플러그인 버전 15.4 이상 설치**

   플러그인 설치에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

4. **Kaspersky Security for Business Professional 라이선스로 솔루션 활성화**

5. **보안 위협 대응을 위해 Active Directory와의 통합 구성**

   통합 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

6. **보안 위협 대응을 위해 Kaspersky Automated Security Awareness Platform과의 통합 구성**

   통합 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

7. **보안 위협 대응을 위해 Kaspersky Threat Intelligence Portal과의 통합 구성**

   통합 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

대응 조치

이 섹션에는 Kaspersky Industrial CyberSecurity Endpoint Detection and Response에서 사용할 수 있는 탐지된 위협에 대한 대응 조치 정보가 포함되어 있습니다.

장치의 네트워크 격리

Kaspersky Industrial CyberSecurity Endpoint Detection and Response는 필요에 따라 장치를 네트워크에서 격리하거나(수동) 탐지된 위협에 대응하기 위한 자동 조치로 격리하는 기능을 제공합니다.

자동 대응의 경우 운영자의 확인 없이 장치에서 해당 명령이 실행됩니다. 표준 운영 체제 메커니즘을 사용하더라도 예기치 않은 문제가 발생할 수 있습니다. 이러한 문제는 잘못되었거나 특정 용도에만 맞춰진 장치 구성, 호환성 문제 또는 정상적인 사용 중에는 드러나지 않는 장치나 산업 제어 시스템(ICS)의 소프트웨어 오류로 인해 발생할 수 있습니다. 예를 들어 다음과 같은 문제가 발생할 수 있습니다: 장치 전원 꺼짐, 장치와의 통신 끊김, 장치 작동 불능, 기타 솔루션 및 장비 작동 장애. 또한 ICS 운영에 의도치 않은 영향을 미칠 수 있습니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response 관리자는 탐지된 위협에 대응하는 솔루션의 자동 조치가 ICS 및 기술 프로세스의 안정성에 미치는 영향에 대해 전적으로 책임을 집니다.

네트워크 격리를 활성화하면 애플리케이션은 모든 활성 TCP/IP 연결을 끊고 아래에 나열된 연결을 제외한 장치의 모든 새 TCP/IP 네트워크 연결을 차단합니다:

- 네트워크 격리 예외로 지정된 연결
- Kaspersky Industrial CyberSecurity for Nodes 또는 Kaspersky Industrial CyberSecurity for Linux Nodes의 서비스에서 시작된 연결
- Kaspersky Security Center 네트워크 에이전트가 시작한 연결

웹 콘솔에서 네트워크 격리를 관리할 수 있습니다.

네트워크 격리 작업 시 사용 가능한 옵션

네트워크 격리 작업 시 다음 옵션을 사용할 수 있습니다.

- IOC 탐지 시 네트워크 격리 자동 활성화.
- 장치의 네트워크 격리 수동 활성화.
- 경고 세부 정보 카드에서 네트워크 격리 활성화.
- 장치의 네트워크 격리 수동 비활성화.
- Kaspersky Industrial CyberSecurity 정책을 사용하여 네트워크 격리 간격 구성.
- 장치의 네트워크 격리 간격 구성.

자동 네트워크 격리 모드

IOC 탐지 시 네트워크 격리가 자동으로 켜지도록 구성할 수 있습니다. 그룹 정책을 사용하여 자동 네트워크 격리 모드를 구성할 수 있습니다.

IOC 탐지 시 네트워크 격리 자동 활성화를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
   작업 목록이 열립니다.
2. Kaspersky Industrial CyberSecurity for Nodes **IOC 검사** 작업을 클릭합니다.
   작업 속성 창이 열립니다.
   필요한 경우 *IOC 검사* 작업을 생성합니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **IOC 탐지 시 동작** 블록에서 **IOC 발견 후 대응 동작 수행** 및 **네트워크에서 컴퓨터 격리** 확인란을 선택합니다.
5. 변경 사항을 저장합니다.

결과적으로 IOC가 탐지되면 애플리케이션이 컴퓨터를 네트워크에서 격리해 보안위협의 확산을 방지합니다.

특정 기간 후에 자동 네트워크 격리를 비활성화하도록 구성할 수 있습니다. 기본적으로 애플리케이션은 네트워크 격리가 켜지고 8시간이 지나면 자동으로 격리를 해제합니다. 네트워크 격리를 수동으로 끌 수 있습니다(아래 지침 참조). 네트워크 격리가 꺼지고 나면 컴퓨터가 네트워크를 제한 없이 사용할 수 있습니다.

컴퓨터에서 네트워크 격리를 자동 모드로 끌 시간을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.

4. **원격 측정 수집 서버 → Endpoint Detection and Response(Industrial CyberSecurity)**로 가서 **구성** 버튼을 클릭합니다.

5. **네트워크 격리** 블록에서 **컴퓨터 잠금 해제 설정 구성** 옵션을 클릭합니다.

6. 창이 열리면 **다음 시간 후 격리된 컴퓨터 자동 잠금 해제** 확인란을 선택하고 자동으로 네트워크 격리를 끌 시간을 입력합니다.

7. 변경 사항을 저장합니다.

수동 네트워크 격리 모드

네트워크 격리는 수동으로 켜고 끌 수 있습니다. Kaspersky Security Center 관리 콘솔의 컴퓨터 속성을 사용하여 수동 네트워크 격리 모드를 구성할 수 있습니다.

다음 방법으로 네트워크 격리를 활성화할 수 있습니다:

- 경고 세부 정보에서.
- 로컬 애플리케이션 설정 사용.

컴퓨터에서 네트워크 격리를 수동으로 켜는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.

2. 로컬 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.
   그러면 컴퓨터 속성이 열립니다.

3. **애플리케이션** 탭을 선택합니다.

4. **Kaspersky Industrial CyberSecurity for Nodes**를 클릭합니다.
   그러면 로컬 애플리케이션 설정이 열립니다.

5. **애플리케이션 설정** 탭을 선택합니다.

6. **원격 측정 수집 서버 → Endpoint Detection and Response(Industrial CyberSecurity)**로 가서 **구성** 버튼을 클릭합니다.

7. **네트워크 격리**에서 **네트워크에서 컴퓨터 격리** 버튼을 클릭합니다.

8. **확인** 버튼을 클릭합니다.

특정 기간 후에 자동 네트워크 격리를 비활성화하도록 구성할 수 있습니다. 기본적으로 애플리케이션은 네트워크 격리가 켜지고 8시간이 지나면 자동으로 격리를 해제합니다. 네트워크 격리가 꺼지고 나면 컴퓨터가 네트워크를 제한 없이 사용할 수 있습니다.

컴퓨터에서 네트워크 격리를 수동 모드로 끌 시간을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.

2. 로컬 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.
   그러면 컴퓨터 속성이 열립니다.

3. **작업** 탭을 선택합니다.
   이렇게 하면 컴퓨터에서 사용할 수 있는 작업 목록이 표시됩니다.

4. **네트워크 격리** 작업을 선택합니다.

5. **애플리케이션 설정** 탭을 선택합니다.

6. 창이 열립니다. 이 창에서 네트워크 격리를 끌 시간을 선택합니다.

7. 변경 사항을 저장합니다.

컴퓨터에서 네트워크 격리를 수동으로 끄는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)** 옵션을 선택합니다.

2. 로컬 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.
   그러면 컴퓨터 속성이 열립니다.

3. **애플리케이션** 탭을 선택합니다.

4. **Kaspersky Industrial CyberSecurity for Nodes**를 클릭합니다.
   그러면 로컬 애플리케이션 설정이 열립니다.

5. **애플리케이션 설정** 탭을 선택합니다.

6. **원격 측정 수집 서버** → **Endpoint Detection and Response(Industrial CyberSecurity)**로 가서 **구성** 버튼을 클릭합니다.

7. **네트워크 격리**에서 **네트워크에서 격리된 컴퓨터 차단 해제** 버튼을 클릭합니다.

8. 변경 사항을 저장합니다.

명령줄을 사용하여 로컬에서 네트워크 격리를 비활성화할 수도 있습니다.

네트워크 격리 예외

네트워크 격리 예외를 구성할 수 있습니다. 규칙과 일치하는 네트워크 연결은 컴퓨터에서 네트워크 격리를 켜도 차단되지 않습니다.

네트워크 격리 예외를 구성하려면 표준 네트워크 프로필 목록을 사용할 수 있습니다. 기본적으로 예외는 DNS/DHCP 서버 및 DNS/DHCP 클라이언트 역할을 하는 장치의 중단 없는 작동을 보장하는 규칙이 포함된 네트워크 프로필을 포함합니다. 표준 네트워크 프로필 설정을 수정하거나 수동으로 예외를 정의할 수도 있습니다(아래 지침 참조).

정책 속성에 지정된 예외는 보안위협 탐지 시 자동으로 네트워크 격리가 켜질 때만 적용됩니다. 컴퓨터 속성에 지정된 예외는 Kaspersky Security Center 콘솔의 컴퓨터 속성이나 경고 세부 정보에서 네트워크 격리가 수동으로 켜질 때만 적용됩니다.

활성 정책은 컴퓨터 속성에서 구성한 네트워크 격리 예외의 적용에 영향을 주지 않는데, 이는 해당 파라미터에 다른 사용 시나리오가 적용되기 때문입니다.

자동 모드에서 네트워크 격리 예외를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **원격 측정 수집 서버** → **Endpoint Detection and Response(Industrial CyberSecurity)**로 가서 **구성** 버튼을 클릭합니다.
5. **네트워크 격리 예외** 블록에서 **예외 규칙** 옵션을 클릭합니다.
6. 창이 열리면 **프로필 추가**을 클릭하고 예외 구성에 대한 표준 네트워크 프로필을 선택합니다.
   프로필의 네트워크 격리 예외가 네트워크 격리 예외 목록에 추가됩니다. 네트워크 연결 속성을 볼 수 있습니다. 필요시 네트워크 연결 설정을 수정할 수 있습니다.
7. 필요시 네트워크 격리 예외를 수동으로 추가합니다. 그렇게 하려면 예외 규칙 창에서 **추가** 버튼을 클릭하고 네트워크 연결 설정을 수동으로 편집합니다.
8. 변경 사항을 저장합니다.

수동 모드에서 네트워크 격리 예외를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)** 옵션을 선택합니다.
2. 로컬 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.
   그러면 컴퓨터 속성이 열립니다.
3. **작업** 탭을 선택합니다.
   이렇게 하면 컴퓨터에서 사용할 수 있는 작업 목록이 표시됩니다.
4. **네트워크 격리** 작업을 선택합니다.
5. **애플리케이션 설정** 탭을 선택합니다.
6. 창이 열립니다. 이 창에서 **예외 규칙** 버튼을 클릭합니다.
7. 창이 열리면 **프로필 추가**을 클릭하고 예외 구성에 대한 표준 네트워크 프로필을 선택합니다.
   프로필의 네트워크 격리 예외가 네트워크 격리 예외 목록에 추가됩니다. 네트워크 연결 속성을 볼 수 있습니다. 필요시 네트워크 연결 설정을 수정할 수 있습니다.
8. 필요시 네트워크 격리 예외를 수동으로 추가합니다. 그렇게 하려면 예외 규칙 창에서 **추가** 버튼을 클릭하고 네트워크 연결 설정을 수동으로 편집합니다.
9. 변경 사항을 저장합니다.

명령줄을 사용해 로컬에서 네트워크 격리 예외 목록을 볼 수도 있습니다. 이 경우, 컴퓨터는 격리되어야 합니다.

격리된 장치의 태그

격리된 모든 장치에 ISOLATED FROM NETWORK 태그가 추가됩니다. 장치가 격리된 동안에는 이 태그를 제거할 수 없습니다.

> 이 태그를 수동으로 추가하면 장치가 네트워크에서 격리되지 않습니다.

ISOLATED FROM NETWORK 태그를 사용하면 격리된 장치를 탐지할 수 있습니다. 자세한 내용은 격리된 장치 목록 보기 섹션을 참조하십시오.

Kaspersky Endpoint Agent(Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우) 및 Kaspersky Industrial CyberSecurity for Linux Nodes에서 네트워크 격리를 관리하는 방법에 대한 자세한 내용은 Kaspersky Endpoint Agent 도움말 및 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

IOC 검사

*침해지표(IOC)*는 장치에 대한 무단 접근(데이터 침해)을 나타내는 개체 또는 활동에 관한 데이터 집합입니다. 예를 들어, 시스템 로그인 시도가 여러 번 실패하면 침해지표가 될 수 있습니다.

IOC 파일은 IOC를 검색하는 데 사용됩니다. IOC 파일에는 이벤트의 지표와 비교되는 지표 집합이 포함되어 있습니다. 비교한 지표가 일치하면 EPP 애플리케이션은 해당 이벤트를 경고로 간주합니다.

Kaspersky Industrial CyberSecurity for Nodes에는 IOC 파일을 사용하는 그룹 또는 로컬 작업인 *IOC 검사* 작업이 포함되어 있습니다. 일치하는 침해지표가 있으면 애플리케이션은 *IOC 검사* 작업 속성에 지정된 조치를 수행합니다. 탐지된 IOC에 대해 다음 대응 조치를 사용할 수 있습니다.

- 네트워크에서 장치 격리.
- 중요 영역 검사 실행.
- 개체의 복사본을 격리로 이동하고 개체 삭제.

다음과 같은 방법으로 *IOC 검사* 작업을 생성할 수 있습니다.

- 경고 세부 정보에서.
- **웹 콘솔에서.**

  1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
     작업 목록이 열립니다.
  2. **추가** 버튼을 클릭합니다.
     작업 마법사가 시작됩니다.
  3. 검사 설정을 구성합니다:
     a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다.
     b. **작업 유형** 드롭다운 목록에서 **IOC 검사** 옵션을 선택합니다.

c. 필요하다면 **작업 이름** 필드에서 작업 이름을 편집합니다.

d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.

4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다.

5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다.

> 기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

시스템 계정(SYSTEM)은 네트워크 드라이브에서 *IOC 검사* 작업을 수행할 권한이 없습니다. 네트워크 드라이브에 대한 작업을 실행하려면 해당 드라이브에 대한 접근 권한이 있는 사용자의 계정을 선택하십시오.

6. 마법사를 완료합니다.
생성된 작업이 작업 목록에 표시됩니다.

7. 생성한 작업의 이름을 클릭합니다.
작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. **IOC 검사 설정** 섹션으로 갑니다.

10. IOC 파일 업로드하여 침해지표를 검색합니다.

> 작업을 시작한 후에는 IOC 파일을 추가하거나 제거하지 않는 것이 좋습니다. 이로 인해 작업의 이전 실행에 대한 IOC 검사 결과가 잘못 표시될 수 있습니다. 새 IOC 파일로 침해지표를 검색하려면, 새 작업을 추가하는 것이 좋습니다.

11. 필요하다면 소급 IOC 검사를 구성합니다. *IOC 검사* 작업의 이 모드에서는, Kaspersky Industrial CyberSecurity for Nodes가 지정된 기간에 받은 보호 중인 장치의 데이터에서 침해지표를 검색합니다. 애플리케이션이 보호 중인 컴퓨터에 설치된 운영 체제 로그 및 브라우저 로그의 데이터를 분석합니다.

> *회고적 IOC 검사* 모드에서 작업을 시작하려면, 업로드된 IOC 파일이 이 목록의 용어를 하나 이상 포함해야 합니다: *FileItem/**, *Network/**, *PortItem/**, *ProcessItem/**, *RegistryItem/**, *UrlHistoryItem/**.

다음을 수행합니다:

a. **회고적 IOC 검사 활성화** 확인란을 선택합니다.

b. 검색 기간을 일 단위로 지정합니다. 최대값은 14일입니다.
작업 실행 중에 애플리케이션은 작업이 시작된 시간부터 지정된 기간 동안 수집된 정보를 분석합니다.
기본 설정은 1일입니다.

c. 작업 속성의 **고급** 섹션에서 업로드된한 IOC 파일에 언급된 모든 데이터 유형의 확인란이 선택되어 있는지 확인합니다.

d. 업로드한 IOC 파일이 *Network/** 용어가 있는 침해지표를 포함한다면, *네트워크 데이터 - NetworkItem* 데이터 유형 옆의 확인란을 선택합니다. 이 확인란은 기본적으로 선택 해제되어 있습니다.

IOC 검사 작업은 소급 검사 모드에서 시작됩니다. 이 모드에서 애플리케이션은 각 파일에 대해 정상 작업 결과와 소급 IOC 검사 결과를 게시합니다.

Kaspersky Industrial CyberSecurity for Nodes는 소급 검사 결과에 대해서만 PID 필드와 UPID 필드를 표시합니다. 또한 확장 원격 측정이 비활성화된 경우 소급 IOC 검사의 제한 사항은 다음과 같습니다.

- 애플리케이션은 FileItem 레코드의 Created, Modified, Changed, Accessed, FileAttributes 필드를 채우지 않습니다.
- 실행되지 않은 기존 파일의 경우 소급 검사 결과의 Md5sum, Sha256sum, SizeInBytes 필드는 0으로 설정됩니다.
- 삭제된 탐지된 파일의 경우 애플리케이션은 해시를 계산하지 않습니다.

12. 필요하다면 침해지표 탐지 시 Kaspersky Industrial CyberSecurity for Nodes 수행할 동작을 구성합니다.

    a. **IOC 발견 후 대응 동작 수행** 확인란을 선택합니다.

    b. Kaspersky Industrial CyberSecurity for Nodes가 침해지표 탐지 시 수행할 처리 방법 옆의 확인란을 선택합니다:

    - **네트워크에서 컴퓨터 격리**. 이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 위협 확산을 방지하기 위해 컴퓨터를 네트워크에서 격리합니다. Endpoint Detection and Response(KSC) 구성 요소 설정에서 격리 기간을 구성할 수 있습니다.
    - **격리 저장소로 사본을 옮기고 개체 삭제**. 이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 컴퓨터에서 발견된 악성 개체를 삭제합니다. Kaspersky Industrial CyberSecurity for Nodes는 개체 삭제 전에 백업 복사본을 생성하여 격리 저장소에 넣습니다.
    - **중요 영역 검사 실행**. 이 옵션을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 사전 정의된 *중요 영역 검사* 작업을 실행합니다.

13. **고급** 섹션으로 갑니다.

14. 작업 시 분석해야 하는 데이터 유형(IOC 문서)을 선택합니다.

    Kaspersky Industrial CyberSecurity for Nodes는 불러온 IOC 파일의 내용에 따라 *IOC 검사* 작업에 대한 데이터 유형(IOC 문서)을 자동으로 선택합니다. 직접 선택한 데이터 유형을 선택 해제하는 것은 권장하지 않습니다.

    Kaspersky Industrial CyberSecurity for Nodes는 *Windows 레지스트리 – RegistryItem* 데이터 유형에 대해 사전 정의된 레지스트리 키 세트를 분석합니다.

15. 필요하다면 파일 – FileItem 데이터 유형에 추가 설정을 지정합니다.

    a. **IOC 문서** 버튼을 클릭합니다.

    파일 검사 설정 - FileItem 창이 열립니다.

    b. **다음 영역에서 IOC 검사**에서 작업으로 분석할 데이터를 선택합니다.

c. **사용자 지정 검사 영역**에서 침해지표를 찾을 보호 중인 장치의 디스크 영역을 선택합니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 다운로드 폴더, 바탕화면, 운영 체제 임시 파일이 있는 폴더 등 컴퓨터의 중요한 영역에서만 IOC를 검사합니다. 필요한 영역의 경로를 지정할 수 있습니다.

d. **확인**을 누릅니다.

16. 필요하다면 Windows 이벤트 로그 - EventLogItem 데이터 유형에 추가 설정을 지정합니다.

a. **로그 및 날짜** 버튼을 클릭합니다.

Windows 이벤트 로그 검사 설정 - EventLogItem 창이 열립니다.

b. 작업이 특정 시점 이전에 등록된 이벤트를 무시하도록 하려면 **지정한 기간 내에 기록된 이벤트만 검사** 확인란을 선택하고 날짜 및 시간을 지정합니다.

c. **다음 채널에 속하는 이벤트 검사**에서 작업으로 분석할 Windows 이벤트 로그를 선택합니다.

d. **확인**을 누릅니다.

EventLogItem\source IOC 용어에는 이벤트의 XML 스키마에 있는 **공급자 이름** 값을 사용합니다.

17. **스케줄** 탭에서 작업 시작 스케줄을 구성합니다.

18. 변경 사항을 저장합니다.

19. 작업 옆의 확인란을 선택합니다.

20. **시작** 버튼을 클릭합니다.

- 명령줄 사용.

결과 섹션의 작업 속성에서 작업 결과를 볼 수 있습니다. 작업 속성에서 탐지된 침해지표에 관한 정보를 볼 수 있습니다: **애플리케이션 설정 → IOC 검사 결과**.

Kaspersky Industrial CyberSecurity for Nodes는 동일한 IOC 파일에 대해 생성된 레코드 중에서 중복 레코드를 찾고 작업 결과에서 고유한 레코드만 유지합니다. 중복은 비교된 모든 필드의 값이 같은 동일 유형의 레코드입니다. 또한 애플리케이션은 **하나 이상의 필드**에 값이 없는 경우 레코드를 생성하지 않을 수 있습니다.

유형	비교 필드	레코드를 생성하지 않기 위한 조건
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• FullPath, Md5sum, Sha256sum 필드의 값 누락. • FullPath 필드의 값과 Md5sum, Sha256sum 필드의 동일한 값 누락.
RegistryItem	• 하이브 • KeyPath • ValueName • 텍스트 • 유형	Hive, KeyPath, ValueName 필드 중 하나 이상의 값 누락.
ProcessItem	• startTime • PID	startTime 또는 PID 필드의 값 누락.

경고 세부 정보 창에 필드 값이 동일한 RegistryItem 레코드가 표시될 수 있습니다. 이러한 레코드는 인터페이스에 표시되지 않는 Text 필드의 값이 서로 다르기 때문에 중복이 아닙니다.

IOC 검사 결과는 30일간 보관됩니다. 이 기간 후에는 Kaspersky Industrial CyberSecurity for Nodes가 가장 오래된 항목을 자동으로 삭제합니다.

IOC 검사는 IOC 파일에 설명된 침해지표와 일치하는 항목 128개를 찾으면 중단됩니다. 이는 *IOC 검사* 작업 리포트의 항목 수를 제한하여 분석을 더 쉽게 하고, 정확하지 않게 정의된 침해지표로 인해 비정상적으로 많은 일치 항목이 생성되어 리포트가 너무 커지는 것을 방지하기 위함입니다.

Kaspersky Endpoint Agent(Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우) 및 Kaspersky Industrial CyberSecurity for Linux Nodes에서 IOC 검사 작업을 생성하는 방법에 대한 자세한 내용은 Kaspersky Endpoint Agent 도움말 및 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

IOC 파일 요구 사항

IOC 검사 작업 생성 시 다음 IOC 파일 관련 요구 사항 및 제한 사항을 고려합니다.

- 애플리케이션은 침해지표 표시에 대해 개방형 표준 OpenIOC 버전 1.0 및 1.1에서 IOC 및 XML 확장자의 IOC 파일을 지원합니다.
- IOC 파일을 업로드한 후 작업 속성의 내장 편집기에서 직접 파일을 편집할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 OpenIOC 버전 1.1을 준수하는 IOC 파일의 내용 변경을 지원합니다. OpenIOC 버전 1.0과 호환되는 IOC 파일의 내용은 수정할 수 없습니다.
- 명령줄에서 *IOC 검사* 작업 생성 시 업로드한 IOC 파일 중 지원하지 않는 파일이 있으면, 작업 실행 시 애플리케이션이 지원하는 IOC 파일만을 사용합니다. 명령줄에서 *IOC 검사* 작업 생성 시 업로드한 IOC 파일 전체가 지원하지 않는 파일이라면, 작업을 계속 실행할 수는 있지만 침해 지표를 전혀 탐지하지 못합니다. 웹 콘솔이나 Cloud Console을 사용하여 지원하지 않는 IOC 파일을 업로드할 수 없습니다.
- IOC 파일에서 의미 오류나 지원하지 않은 IOC 용어 및 태그가 있어도 작업 실행이 실패하지는 않습니다. 이러한 IOC 파일 섹션에서는 애플리케이션이 아무것도 탐지하지 않습니다.

- 단일 IOC 검사 작업에 사용된 모든 IOC 파일의 ID는 고유해야 합니다. 식별자가 같은 IOC 파일이 있다면 작업 실행 결과에 영향을 미칠 수 있습니다.
- 단일 IOC 파일의 크기는 2MB를 넘지 않아야 합니다. 더 큰 파일을 사용하면 IOC 검사 작업 시 오류가 발생할 수 있습니다. IOC 컬렉션에 추가한 모든 파일의 총 크기는 10MB를 초과할 수 없습니다. 모든 파일의 총 크기가 10MB를 초과하면 IOC 컬렉션을 분할하고 여러 개의 IOC 검사 작업을 생성해야 합니다.
- 보안위협 하나당 IOC 파일 하나를 생성할 것을 권장합니다. 이를 통해 *IOC 검사* 작업 결과를 더 쉽게 분석할 수 있습니다.

아래의 링크를 클릭해 다운로드할 수 있는 파일에는 OpenIOC 표준의 전체 IOC 용어 목록이 포함되어 있습니다.

IOC_TERMS.XLSX 파일 다운로드

OpenIOC 표준에 대한 애플리케이션 지원의 기능 및 제한 사항은 다음 표에 나와 있습니다.

OpenIOC 버전 1.0 및 1.1 지원의 기능 및 제한 사항.

지원 조건	OpenIOC 1.0:
	
	`is`
	`isnot`(세트의 예외)
	`contains`
	`containsnot`(세트의 예외)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

지원 조건 속성	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

지원 연산자	`AND` `OR`
지원 데이터 유형	`"date"`: 날짜(적용 조건: `is`, `greater-than`, `less-than`) `"int"`: 정수(적용 조건: `is`, `greater-than`, `less-than`) `"string"`: 스트링(적용 조건: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: 기간(초)(적용 조건: `is`, `greater-than`, `less-than`)

데이터 유형 해석 기능	`"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` 데이터 유형은 스트링으로 해석됩니다.
	
	이 애플리케이션은 `int` 및 `date` 데이터 유형에 대한 `Content` 설정이 시간 간격의 형태로 설정되었을 때 이 설정의 해석을 지원합니다:
	
	OpenIOC 1.0:
	`Content` 필드에서 `TO` 연산자 사용:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	`greater-than` 및 `less-than` 조건 사용
	`Content` 필드에서 `TO` 연산자 사용
	지표가 `ISO 8601, Zulu time zone, UTC` 형식으로 설정되어 있으면 애플리케이션이 `date` 및 `duration` 데이터 유형의 해석을 지원합니다.

IOC 검사를 위한 확장 원격 측정

회고적 IOC 검사를 위해 컴퓨터에서 확장 원격 측정을 활성화하는 것이 좋습니다. 확장 원격 측정은 IOC 탐지의 정확도를 개선하지만 컴퓨터 리소스를 더 많이 사용합니다.

확장 원격 측정에는 다음 추가 용어 지원이 포함됩니다.

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

확장 원격 측정이 비활성화되면 Kaspersky Industrial CyberSecurity for Nodes는 탐지된 침해 지표에 대한 정보를 교체할 수 있습니다.

확장 원격 측정을 활성화하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **원격 측정 수집 서버** → **Endpoint Detection and Response(Industrial CyberSecurity)**로 가서 **구성** 버튼을 클릭합니다.
5. **고급 시스템 활동 로그 활성화** 확인란을 선택합니다.
6. 변경 사항을 저장합니다.

레지스트리에서의 IOC 검사 범위(RegistryItem)

IOC 검사 범위에 RegistryItem 데이터 유형을 추가하면 Kaspersky Industrial CyberSecurity for Nodes가 다음 레지스트리 키를 검사합니다:

```
HKEY_CLASSES_ROOT\htafile
```

```
HKEY_CLASSES_ROOT\batfile
```

```
HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

중요 영역 검사 실행

위협이 탐지될 때 수행할 수 있는 대응 작업 중 하나는 장치에서 중요 영역 검사를 실행하는 것입니다.

중요 영역 검사를 수동으로 실행하거나 경고 대응 작업의 결과로 검사가 자동 실행되도록 구성할 수 있습니다.

Kaspersky Endpoint Agent(Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우) 및 Kaspersky Industrial CyberSecurity for Linux Nodes의 중요 영역 검사에 대한 자세한 내용은 Kaspersky Endpoint Agent 도움말 및 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

실행 방지

실행 방지를 통해 실행 파일 및 스크립트 실행과 오피스 형식 파일 열기를 관리할 수 있습니다. 이를 통해 안전하지 않다고 판단되는 애플리케이션의 실행을 방지하는 등의 작업을 할 수 있습니다. 결과적으로 보안위협의 확산을 막을 수 있습니다. 실행 방지는 **오피스 파일 확장자 세트**와 **스크립트 인터프리터 세트**를 지원합니다.

실행 방지는 다음 스크립트 인터프리터를 지원합니다:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe

- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

실행 방지는 Java 런타임 환경에서의 Java 애플리케이션 사용을 지원합니다(java.exe 및 javaw.exe 프로세스).

Kaspersky Industrial CyberSecurity for Nodes는 특정 애플리케이션에서 오피스 형식의 파일을 열지 못하게 차단할 수 있습니다. 지원하는 파일 확장자와 애플리케이션에 관한 정보는 다음 표를 확인하십시오.

지원하는 실행 방지 파일 확장자

애플리케이션 이름	실행 파일	파일 확장자
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw

애플리케이션 이름	실행 파일	파일 확장자
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

실행 방지 규칙

실행 방지는 실행 방지 규칙으로 파일에 대한 사용자 접근을 관리합니다. *실행 방지 규칙*은 개체 실행 차단 등과 같이 개체 실행에 반응할 때 애플리케이션이 고려하는 기준 집합입니다. 애플리케이션은 MD5 및 SHA256 해싱 알고리즘을 사용하여 계산된 경로 또는 체크섬으로 파일을 식별합니다.

실행 방지 규칙은 다음에서 생성할 수 있습니다:

- 경고 세부 정보에서.

  Kaspersky Industrial CyberSecurity for Linux Nodes 버전 1.5가 설치된 Linux 운영 체제 기반 컴퓨터에서는 이 작업을 사용할 수 없습니다.

- 그룹 정책 또는 로컬 애플리케이션 설정 사용.

  파일 경로와 해시(SHA256 또는 MD5)를 입력하거나 둘 중 하나를 입력해야 합니다.

실행 방지에는 다음 제한이 있습니다.

1. CD나 ISO 이미지 내의 파일은 방지 규칙의 범위에 포함되지 않습니다. 이 애플리케이션은 해당 파일의 실행이나 열기를 차단하지 않습니다.
2. 시스템 중요 개체(SCO)의 시작 차단은 불가능합니다. SCO는 운영 체제 및 Kaspersky Industrial CyberSecurity for Nodes 애플리케이션을 실행하는 데 필요한 파일입니다.
3. 실행 방지 규칙을 5,000개 이상 생성 시 시스템이 불안정해질 수 있으므로 권장하지 않습니다.

실행 방지 규칙 모드

실행 방지는 다음 두 가지 모드로 작동할 수 있습니다:

- **알림**

  이 모드에서는 Kaspersky Industrial CyberSecurity for Nodes가 방지 규칙의 기준과 일치하는 실행 개체 실행 또는 문서 열기 시도 이벤트를 Windows 이벤트 로그 및 Kaspersky Security Center에 게시하지만, 개체나 문서에 대한 실행 또는 열기 시도를 차단하지 않습니다. 기본적으로 이 모드가 선택되어 있습니다.

- **차단**

  이 모드에서는 애플리케이션이 방지 규칙의 기준과 일치하는 개체 실행 또는 문서 열기를 차단합니다. 또한 애플리케이션은 개체 실행 또는 문서 열기 시도 이벤트를 Windows 이벤트 로그 및 Kaspersky Security Center 이벤트 로그에 게시합니다.

실행 방지 관리

구성 요소 설정은 Kaspersky Security Center 웹 콘솔 이나 로컬에서 명령줄을 통해 구성할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서 개체 실행을 방지하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **원격 측정 수집 서버** → **Endpoint Detection and Response(Industrial CyberSecurity)**로 가서 **구성** 버튼을 클릭합니다.
5. **실행 방지 사용** 확인란을 선택합니다.
6. **금지된 개체 실행 또는 열기 시 동작** 블록에서, 구성 요소 운영 모드를 선택합니다:

   - **차단**. 이 모드에서는 애플리케이션이 방지 규칙의 기준과 일치하는 개체 실행 또는 문서 열기를 차단합니다. 또한 애플리케이션은 개체 실행 또는 문서 열기 시도 이벤트를 Windows 이벤트 로그 및 Kaspersky Security Center 이벤트 로그에 게시합니다.

   - **알림**. 이 모드에서는 Kaspersky Industrial CyberSecurity for Nodes가 방지 규칙의 기준과 일치하는 실행 개체 실행 또는 문서 열기 시도 이벤트를 Windows 이벤트 로그 및 Kaspersky Security Center에 게시하지만, 개체나 문서에 대한 실행 또는 열기 시도를 차단하지 않습니다. 기본적으로 이 모드가 선택되어 있습니다.
7. 실행 방지 규칙 목록을 생성합니다:

   a. **추가** 버튼을 클릭합니다.

   b. 창이 열리면 실행 방지 규칙의 이름을 입력합니다.

c. **유형** 드롭다운 목록에서 차단할 개체를 선택합니다: **실행 파일**, **스크립트**, **Microsoft Office 문서**.

잘못된 개체 유형을 Kaspersky Industrial CyberSecurity for Nodes가 해당 파일 또는 스크립트를 차단하지 않습니다.

d. 파일을 추가하려면 파일의 해시(SHA256 또는 MD5)와 파일의 전체 경로를 입력하거나 둘 중 하나를 입력해야 합니다.

> 파일이 네트워크 드라이브에 있다면 드라이브 문자가 아닌 `\\` 문자로 시작하는 파일 경로를 입력합니다. 예: `\\server\shared_folder\file.exe`. 파일 경로에 네트워크 드라이브 문자가 포함되면 Kaspersky Industrial CyberSecurity for Nodes가 해당 파일 또는 스크립트를 차단하지 않습니다.

e. **확인** 버튼을 클릭합니다.

8. 변경 사항을 저장합니다.

결과적으로 Kaspersky Industrial CyberSecurity for Nodes가 개체의 실행을 차단합니다: 실행 파일 및 스크립트 실행, 오피스 형식 파일 열기. 스크립트 실행이 차단되어도 텍스트 에디터 등으로 스크립트 파일을 열 수는 있습니다. 알림이 애플리케이션 설정에서 활성화되어 있다면 개체 실행 차단 시 Kaspersky Industrial CyberSecurity for Nodes가 기본 알림을 표시합니다.

Kaspersky Endpoint Agent(Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우) 및 Kaspersky Industrial CyberSecurity for Linux Nodes에서 실행 방지를 구성하는 방법에 대한 자세한 내용은 Kaspersky Endpoint Agent 도움말 및 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

프로세스 시작

프로세스 시작 작업을 사용하여 파일을 원격으로 실행할 수 있습니다. 예를 들어, 컴퓨터 구성 파일을 생성하는 유틸리티를 원격으로 실행할 수 있습니다. 다음으로 *파일 가져오기* 작업을 사용하여 Kaspersky Security Center 웹 콘솔에서 생성된 파일을 수신합니다.

프로세스 시작 작업을 생성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.

   작업 목록이 열립니다.

2. **추가** 버튼을 클릭합니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **프로세스 시작** 옵션을 선택합니다.

   c. **작업 이름** 필드에 작업에 대한 간단한 설명을 입력하고 **다음** 버튼을 클릭합니다.

4. **작업 범위** 섹션에서 관리 중인 장치를 선택하고 **다음** 버튼을 클릭합니다.

5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음** 버튼을 클릭합니다.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. **마침** 버튼을 클릭해 마법사를 마칩니다. 작업 목록에 새 작업이 표시됩니다.

7. 새 작업을 클릭합니다. 작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. **설정 시작** 섹션을 선택하고 프로세스 시작 명령을 입력합니다:

   컴퓨터 구성에 대한 정보를 `conf.txt`라는 이름의 파일을 현재 폴더에(기본값으로) 저장하는 유틸리티(`utility.exe`)를 실행하려면 다음과 같이 진행합니다. 유틸리티는 `C:\Users\admin\Diagnostic\` 폴더에 있습니다. 구성 파일을 `C:\Users\admin\Documents\Configuration` 폴더에 저장해야 합니다. 다음 값을 입력합니다.

   - **실행 가능 명령** – `C:\Users\admin\Diagnostic\utility.exe`
   - **명령줄 인수(선택사항)** – `/R conf.txt`
   - **작업 폴더 경로(선택사항)** – `C:\Users\admin\Documents\Configuration`

10. 작업 속성 창에서 **스케줄** 탭을 선택합니다.

11. 작업 스케줄을 구성합니다.

    이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.

12. **저장** 버튼을 클릭합니다.

13. 작업 옆의 확인란을 선택하고 **시작** 버튼을 클릭합니다.

    결과적으로 Kaspersky Industrial CyberSecurity for Nodes는 숨김 모드에서 명령을 실행하고 프로세스를 시작합니다. **실행 결과** 섹션의 작업 속성에서 작업 결과를 볼 수 있습니다.

Kaspersky Endpoint Agent(Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우) 및 Kaspersky Industrial CyberSecurity for Linux Nodes에서 *프로세스 시작* 작업을 실행하는 방법에 대한 자세한 내용은 Kaspersky Endpoint Agent 도움말 및 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

프로세스 종료

프로세스 종료 작업을 사용해 프로세스를 원격으로 종료할 수 있습니다. 예를 들어, *프로세스 실행* 작업을 사용하여 시작된 인터넷 속도 테스트 유틸리티를 원격으로 종료할 수 있습니다.

파일 실행을 금지하려면 실행 방지를 구성할 수 있습니다. 실행 파일, 스크립트, 오피스 형식 파일의 실행을 금지할 수 있습니다.

SCO(시스템 중요 개체) 프로세스는 종료할 수 없습니다. SCO는 운영 체제 및 Kaspersky Industrial CyberSecurity for Nodes 애플리케이션을 실행하는 데 필요한 파일입니다.

프로세스 종료 작업을 생성하려면:

1. 웹 콘솔의 메인 창에서 **장치** → **작업** 옵션을 선택합니다.
   작업 목록이 열립니다.
2. **추가** 버튼을 클릭합니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **프로세스 종료** 옵션을 선택합니다.
   c. **작업 이름** 필드에 작업에 대한 간단한 설명을 입력하고 **다음** 버튼을 클릭합니다.
4. **작업 범위** 섹션에서 관리 중인 장치를 선택하고 **다음** 버튼을 클릭합니다.
5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음** 버튼을 클릭합니다.
   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.
6. **마침** 버튼을 클릭해 마법사를 마칩니다. 작업 목록에 새 작업이 표시됩니다.
7. 새 작업을 클릭합니다. 작업 속성 창이 열립니다.
8. **애플리케이션 설정** 탭을 선택합니다.
9. 프로세스를 완료하려면 종료할 파일을 선택해야 합니다. 다음과 같은 방법으로 파일을 선택할 수 있습니다:
   - 파일의 전체 이름을 입력합니다.
   - 파일의 해시와 파일 경로를 입력합니다.
   - 프로세스의 PID를 입력합니다(로컬 작업에만 해당).

   파일이 네트워크 드라이브에 있다면 드라이브 문자가 아닌 `\\` 문자로 시작하는 파일 경로를 입력합니다. 예: `\\server\shared_folder\file.exe`. 파일 경로에 네트워크 드라이브 문자가 포함되어 있으면 *파일이 없음* 오류가 발생할 수 있습니다.
10. 작업 속성 창에서 **스케줄** 탭을 선택합니다.
11. 작업 스케줄을 구성합니다.

    이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.
12. **저장** 버튼을 클릭합니다.
13. 작업 옆의 확인란을 선택하고 **시작** 버튼을 클릭합니다.

결과적으로 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터에서 프로세스를 종료합니다. 예를 들어 'GAME' 애플리케이션이 실행 중일 때 game.exe 프로세스를 종료하면, 데이터가 저장되지 않은 채 애플리케이션이 닫힙니다. **결과** 섹션의 작업 속성에서 작업 결과를 볼 수 있습니다.

Kaspersky Endpoint Agent(Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우) 및 Kaspersky Industrial CyberSecurity for Linux Nodes에서 *프로세스 종료* 작업을 실행하는 방법에 대한 자세한 내용은 Kaspersky Endpoint Agent 도움말 및 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

파일 가져오기

사용자 컴퓨터에서 파일을 가져올 수 있습니다. 예를 들어 타사 애플리케이션에서 만든 이벤트 로그 파일을 가져오도록 구성할 수 있습니다. 파일을 가져오려면 전용 작업을 만들어야 합니다. 작업 실행에 따른 파일은 격리 저장소에 저장됩니다. 웹 콘솔을 사용하여 격리 저장소에서 컴퓨터로 이 파일을 다운로드할 수 있습니다. 이 파일은 사용자 컴퓨터의 원래 폴더에 남습니다.

작업을 성공적으로 완료하려면 결과 파일의 크기가 2GB 미만이어야 합니다.

파일 가져오기 작업을 생성하려면:

1. 웹 콘솔의 메인 창에서 **장치** → **작업** 옵션을 선택합니다.
   작업 목록이 열립니다.
2. **추가** 버튼을 클릭합니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **파일 가져오기** 옵션을 선택합니다.
   c. **작업 이름** 필드에 작업에 대한 간단한 설명을 입력하고 **다음** 버튼을 클릭합니다.
4. **작업 범위** 섹션에서 관리 중인 장치를 선택하고 **다음** 버튼을 클릭합니다.
5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음** 버튼을 클릭합니다.
   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.
6. **마침** 버튼을 클릭해 마법사를 마칩니다. 작업 목록에 새 작업이 표시됩니다.
7. 새 작업을 클릭합니다. 작업 속성 창이 열립니다.
8. **애플리케이션 설정** 탭을 선택합니다.
9. 파일 목록에서 **추가** 버튼을 클릭합니다. 파일 추가 마법사가 시작됩니다.
10. 파일을 추가하려면 파일의 전체 경로를 입력하거나, 체크섬과 폴더 경로를 입력해야 합니다.

    파일이 네트워크 드라이브에 있다면 드라이브 문자가 아닌 `\\` 문자로 시작하는 파일 경로를 입력합니다. 예: `\\server\shared_folder\file.exe`. 파일 경로에 네트워크 드라이브 문자가 포함되어 있으면 *파일이 없음* 오류가 발생할 수 있습니다.

11. 작업 속성 창에서 **스케줄** 탭을 선택합니다. 작업 스케줄을 구성합니다.

    이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.

12. **저장** 버튼을 클릭합니다.

13. 작업 옆의 확인란을 선택하고 **시작** 버튼을 클릭합니다.

결과적으로 Kaspersky Industrial CyberSecurity for Nodes는 파일의 사본을 생성하고 이 사본을 격리 저장소로 이동합니다.

Kaspersky Endpoint Agent에서 파일의 사본을 받으려면 **파일 격리** 작업을 생성하고 **파일 격리 후 처리 방법** 섹션에서 파일을 격리로 이동할 때 삭제하지 않도록 지정합니다. 자세한 내용은 Kaspersky Endpoint Agent 도움말 (Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우)을 참조하십시오.

Kaspersky Industrial CyberSecurity for Linux Nodes에서 파일의 사본을 받으려면 **장치에서 파일 받기** 유형의 작업을 생성합니다. 자세한 내용은 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

Kaspersky Endpoint Security 12.1 for Linux를 사용하는 경우 작업이 Kaspersky Security Center의 백업 폴더로 이동됩니다.

파일 삭제

Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky Industrial CyberSecurity Endpoint Detection and Response와 통합된 경우 파일 삭제 작업을 사용하여 보호되는 장치에서 파일을 삭제할 수 있습니다.

SCO(시스템 중요 개체)는 삭제할 수 없습니다. SCO는 운영 체제 및 Kaspersky Industrial CyberSecurity for Nodes 애플리케이션을 실행하는 데 필요한 파일입니다.

파일 삭제 작업을 생성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업** 옵션을 선택합니다.
   작업 목록이 열립니다.

2. **추가** 버튼을 클릭합니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **파일 삭제** 옵션을 선택합니다.

   c. **작업 이름** 필드에 작업에 대한 간단한 설명을 입력하고 **다음** 버튼을 클릭합니다.

4. **작업 범위** 섹션에서 관리 중인 장치를 선택하고 **다음** 버튼을 클릭합니다.

5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음** 버튼을 클릭합니다.
   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. **마침** 버튼을 클릭해 마법사를 마칩니다. 작업 목록에 새 작업이 표시됩니다.

7. 새 작업을 클릭합니다. 작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. 파일을 삭제하려면 파일의 전체 경로를 입력하거나, 폴더 경로가 있는 체크섬을 입력해야 합니다.

   파일이 네트워크 드라이브에 있다면 드라이브 문자가 아닌 \\ 문자로 시작하는 파일 경로를 입력합니다. 예: `\\server\shared_folder\file.exe`. 파일 경로에 네트워크 드라이브 문자가 포함되어 있으면 *파일이 없음* 오류가 발생할 수 있습니다.

10. 작업 속성 창에서 **스케줄** 탭을 선택합니다. 작업 스케줄을 구성합니다.

    이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.

11. **저장** 버튼을 클릭합니다.

12. 작업 옆의 확인란을 선택하고 **시작** 버튼을 클릭합니다.

    결과적으로 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터에서 파일을 삭제합니다. 다른 프로세스가 파일을 잠갔다면, 작업은 *완료*으로 표시되지만 파일 자체는 컴퓨터가 다시 시작된 후에만 삭제됩니다. 컴퓨터를 다시 시작한 후 파일이 삭제되었는지 확인하십시오.

현재 실행 중인 실행 파일을 삭제할 시 *파일 삭제* 작업이 *접근 거부됨* 오류와 함께 끝납니다. 파일에 대해 프로세스 종료 작업을 생성한 후 다시 시도하십시오.

Kaspersky Endpoint Agent(Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우) 및 Kaspersky Industrial CyberSecurity for Linux Nodes에서 파일을 삭제하는 방법에 대한 자세한 내용은 Kaspersky Endpoint Agent 도움말 (Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우) 및 Kaspersky Industrial CyberSecurity for Linux Nodes 도움말을 참조하십시오.

격리 저장소로 파일 이동

위협이 탐지되었을 때 가능한 대응 작업 중 하나는 파일을 격리하는 것입니다.

*격리*는 Kaspersky Industrial CyberSecurity Endpoint Detection and Response가 설치된 장치의 특수 로컬 저장소로, 바이러스에 감염되었을 가능성이 있거나 탐지 시 치료할 수 없는 파일을 저장하는 데 사용됩니다. 격리 설정을 구성할 수 있습니다. 격리된 파일은 보호되는 장치에 암호화된 형식으로 저장되므로 장치의 보안을 손상시키지 않습니다.

파일을 수동으로 격리하거나 경고 대응 작업의 결과로 파일이 자동 격리되도록 구성할 수 있습니다. 또한 경고 세부 정보 창에서 파일을 격리할 수 있습니다.

Kaspersky Industrial CyberSecurity for Linux Nodes 버전 1.5가 설치된 Linux 운영 체제 기반 컴퓨터에서는 이 작업을 사용할 수 없습니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 확장 기능을 사용하면 분석을 위해 격리된 파일을 Kaspersky TIP에 전송할 수 있습니다. 이 기능을 사용하려면 Kaspersky TIP과의 통합을 구성해야 합니다. 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Security for Business Professional 라이선스에는 Kaspersky TIP 요청이 제한된 횟수만큼 포함됩니다.

격리 관리에 관한 자세한 내용은 Kaspersky 애플리케이션 도움말을 참조하십시오.

- Kaspersky Security Center 도움말
- Kaspersky Endpoint Agent 도움말 (Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우).
- Kaspersky Industrial CyberSecurity for Linux Nodes 도움말

격리된 파일 보기

격리된 파일 목록을 보려면 다음과 같이 하십시오.

웹 콘솔의 메인 창에서 **동작** → **저장소** → **격리** 옵션을 선택합니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response에서 격리한 개체는 검사할 수 없습니다.

개체는 시스템 계정 권한으로 격리됩니다. Kaspersky Endpoint Agent를 사용하는 경우 격리에서 복원된 파일은 원래 위치가 아니라 장치의 특수 폴더에 저장되며, 이 폴더에서 대상 폴더로 직접 이동할 수 있습니다.

격리에서 Kaspersky TIP으로 파일 전송

Kaspersky Security for Business Professional 라이선스에는 Kaspersky TIP 요청이 제한된 횟수만큼 포함됩니다.

격리에서 Kaspersky TIP으로 파일을 전송하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **동작** → **저장소** → **격리** 옵션을 선택합니다.
2. 파일을 선택합니다.
   분석을 위해 한 번에 하나의 파일만 보낼 수 있습니다.

3. 도구 모음에서 **위협 분석을 위해 전송** 버튼을 클릭합니다.

   Kaspersky Security Center는 관리 중인 장치에서 Kaspersky TIP으로 파일을 전송합니다. 이렇게 하려면 관리 중인 장치가 네트워크에서 표시되어야 합니다.

   파일이 Kaspersky TIP으로 전송됩니다. 분석 결과를 보려면 알림에서 **Kaspersky TIP에서 보기** 버튼을 클릭한 다음 Kaspersky TIP에 로그인합니다.

Kaspersky Security Center는 Kaspersky TIP 분석 결과를 저장하지 않습니다.

Cloud Sandbox

Cloud Sandbox는 사용자 컴퓨터에서 복잡한 위협을 탐지하는 클라우드 기반 기술입니다. Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Industrial CyberSecurity for Linux Nodes는 확인이 필요한 파일을 분석을 위해 Cloud Sandbox로 자동 전송합니다. Cloud Sandbox는 이러한 파일을 격리된 환경에서 실행하여 악성 활동을 식별하고 평판을 결정합니다. 그다음 이 파일의 데이터가 Kaspersky Security Network로 전송됩니다.

Cloud Sandbox가 작동하려면 Kaspersky Security Network 사용을 활성화해야 합니다.

Kaspersky Private Security Network를 사용하는 경우 Cloud Sandbox 기술을 사용할 수 없습니다.

Linux를 실행하는 장치에서 Cloud Sandbox 기술을 사용하려면 다음 조건을 충족해야 합니다.

- 컴퓨터에 Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 이상이 설치되어 있어야 합니다.
- KSN 지원은 Kaspersky Industrial CyberSecurity for Linux Nodes 버전 2.0 이상에 포함되어 있습니다.

Cloud Sandbox 지원에 대한 자세한 내용은 *Kaspersky Industrial CyberSecurity for Linux Nodes 도움말*을 참조하십시오.

Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Industrial CyberSecurity for Linux Nodes 버전 2.0 이상에서는 Cloud Sandbox에서 탐지한 위협에 대한 별도 카운터를 활성화할 수 있습니다. 이 카운터를 사용하여 탐지된 보안 위협을 분석하는 동안 통계를 생성할 수 있습니다.

Cloud Sandbox에서 탐지한 경고에 대한 리포트를 보려면(**위협 처리 리포트** → **상세 정보** 탭 → **Cloud Sandbox 기술에 의해 감지됨** 열) Kaspersky Security Center for Windows 버전 14.2 이상, Kaspersky Security Center for Linux 버전 15.1 이상 또는 Kaspersky Security Center Cloud Console이 있어야 합니다.

경고 세부 정보 작업

이 섹션에는 경고 세부 정보 창에서 직접 수행할 수 있는 작업에 대한 정보가 포함되어 있습니다.

경고 세부 정보 정보

경고 세부 정보에는 탐지된 위협에 대해 제공되는 모든 정보가 포함되며, 경고 대응 작업을 관리할 수 있습니다.

경고 세부 정보에는 다음 정보가 포함됩니다.

- **보안 위협 개발 체인 그래프**. 엔드포인트 장치를 표적으로 하는 공격 수명 주기를 표시합니다. 경고 세부 정보 카드에는 축약 버전과 전체 버전의 두 가지 그래프가 표시됩니다.
  - 축약 버전에는 다음과 같은 주요 요소가 포함됩니다.
    - **에셋**는 경고가 탐지된 장치입니다.
    - **사용자**는 경고와 관련된 사용자입니다.
    - **근본 원인**는 이벤트의 근본 원인입니다.
    - **탐지된 개체**는 위협 이름입니다.
    - **판단**는 EPP 프로그램이 위협에 대해 내린 판정입니다.
    - 작업 수행 결과
  - 전체 그래프에는 공격과 관련된 전체 이벤트 체인이 포함되며, 공격이 확대되는 경로, 공격에 관련된 프로세스 및 해당 프로세스가 수행한 작업이 표시됩니다.
- **권장**. 경고 대응을 위한 권장 사항입니다.

  권장 사항은 Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Industrial CyberSecurity for Linux Nodes 1.5 이상에서 제공됩니다.
- **경고 세부 정보**. 처리 결과, 카테고리 및 탐지 모드(예: 온디맨드 검사 또는 자동 검사 중 탐지)를 포함한 경고 관련 일반 정보입니다.
- **기기**. 경고가 발생한 보호 대상 장치에 대한 정보입니다. 예: 장치 이름, IP 주소, MAC 주소 및 운영 체제.
- **프로세스**. 악성으로 분류된 프로세스에 대한 정보입니다.
- **파일**. 탐지한 개체에 대한 정보.
- **다운로드**. 네트워크 리소스에 액세스하여 경고를 발생시킨 프로세스에 대한 정보입니다.
- **Kaspersky TIP의 데이터**. 신뢰 그룹, 디지털 서명, 파일 배포 데이터 및 경고 분석 링크를 포함한 파일 평판 정보입니다.

  이 정보는 탐지 시점에 Kaspersky Industrial CyberSecurity for Linux Nodes 애플리케이션에서 Kaspersky Security Network 기능이 활성화된 경우에 제공됩니다.

  나열된 데이터는 위협이 탐지된 시점의 데이터입니다. 솔루션은 나열된 데이터를 업데이트하지 않으므로 Kaspersky Threat Intelligence Portal에 표시되는 데이터와 다를 수 있습니다. 최신 데이터를 보려면 경고 세부 정보에서 Kaspersky Threat Intelligence Portal 데이터 링크를 사용하십시오.

다음 두 애플리케이션을 Kaspersky Security Center와 함께 사용하는 경우 보안 위협 개발 체인의 개체에 수행된 대응 작업에 대한 추가 정보가 제공됩니다.

- Kaspersky Industrial CyberSecurity for Nodes 4.5 이상
- Endpoint Detection and Response 웹 플러그인 버전 15.4 이상

경고 세부 정보에서 다음 대응 작업을 수행할 수 있습니다.

- 경고가 발생한 장치 격리.
- 격리 저장소 파일.

  Kaspersky Industrial CyberSecurity for Linux Nodes 버전 1.5가 설치된 Linux 운영 체제 기반 컴퓨터에서는 이 작업을 사용할 수 없습니다.

- IOC 검사 작업 생성.
- 탐지된 파일의 실행 방지.

  Kaspersky Industrial CyberSecurity for Linux Nodes 버전 1.5가 설치된 Linux 운영 체제 기반 컴퓨터에서는 이 작업을 사용할 수 없습니다.

EPP 애플리케이션은 위협 탐지 이벤트와 위협 데이터 처리 결과를 기반으로 경고를 생성합니다. 이벤트 스토리지 기간은 EPP 애플리케이션에서 구성할 수 있습니다.

기본적으로 EPP 애플리케이션은 경고 세부 정보를 30일 동안 저장합니다. 이 기간이 지나면 경고 세부 정보가 자동으로 삭제됩니다.

경고 목록에는 최근 30일 동안의 경고가 표시됩니다.

경고 세부 정보 보기

경고 세부 정보는 경고 목록에서 확인할 수 있습니다. 경고 목록은 Kaspersky Security Center 웹 콘솔의 **위협 처리 리포트**에서 또는 **모니터링** 섹션의 **경고** 하위 섹션에서 확인할 수 있습니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response용 라이선스 키를 추가하면 기본 메뉴의 **모니터링** 섹션에 **경고** 하위 섹션이 자동으로 나타납니다. Kaspersky Security Center 속성에서 **경고** 하위 섹션의 표시 여부를 구성할 수도 있습니다.

경고 세부 정보를 보려면 다음과 같이 하십시오.

1. Kaspersky Security Center 웹 콘솔 메인 창에서 **모니터링** → **경고** 섹션으로 이동합니다.

   Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 확장 기능을 사용하면 **경고 집계** 토글 스위치를 사용하여 유사한 경고를 그룹화할 수 있습니다.

2. 경고를 선택하고 **강화됨** 링크를 클릭합니다.

   경고 세부 정보가 표시됩니다.

보안위협 리포트에서 경고 세부 정보를 보려면 다음과 같이 하십시오.

1. Kaspersky Security Center 웹 콘솔 메인 창에서 **모니터링 → 리포트** 섹션으로 이동합니다.
2. **위협 처리 리포트** 템플릿을 선택하고 **리포트 표시** 버튼을 클릭합니다.
3. 리포트 창의 **상세 정보** 탭에서 경고를 선택하고 **경고 세부 정보 열기** 링크를 클릭합니다.
   경고 세부 정보가 표시됩니다.

경고 세부 정보를 표시하려면 Kaspersky Industrial CyberSecurity Endpoint Detection and Response가 경고가 발생한 장치에서 데이터를 가져와야 합니다. 데이터 또는 장치를 사용할 수 없으면 오류 메시지가 표시됩니다. 장치가 응답하는 데 몇 분이 걸릴 수 있습니다.

네트워크 격리 적용 및 제거

경고 세부 정보 창에서 장치를 네트워크로부터 격리하려면 다음과 같이 하십시오.

1. 경고 세부 정보 창을 엽니다.
2. **기기**에서 **대응 작업** 드롭다운 목록의 **네트워크에서 기기 격리** 옵션을 선택합니다.

   Kaspersky Industrial CyberSecurity for Nodes 4.5 이상 버전에서는 장치의 네트워크 격리 설정을 구성할 수 있습니다.

3. 사용자 지정 네트워크 격리 간격을 지정하려면 **기본 잠금 해제 설정 사용** 체크박스의 선택을 취소한 다음 **다음 후 잠금 해제(시간)** 필드에 원하는 시간 수를 입력합니다.
4. **격리** 버튼을 클릭합니다.
5. 작업을 확인합니다.

애플리케이션이 장치를 격리하고 장치에 네트워크에서 격리됨 태그를 할당합니다.

장치에서 네트워크 격리를 제거하려면 다음과 같이 하십시오.

1. 경고 세부 정보 창을 엽니다.
2. **기기**에서 **대응 작업** 드롭다운 목록의 **네트워크에서 기기 재활성화** 옵션을 선택합니다.

   Kaspersky Industrial CyberSecurity for Nodes 4.5 이상 버전 또는 Kaspersky Industrial CyberSecurity for Linux Nodes 1.5 이상 버전에서 경고를 수신한 경우 **네트워크에서 기기 재활성화** 버튼을 사용할 수 있습니다.

3. 작업을 확인합니다.

장치의 네트워크 격리가 제거되고 장치에 할당된 네트워크에서 격리됨 태그가 삭제됩니다.

장치에서 네트워크 격리를 활성화 및 비활성화하고 네트워크 격리 예외를 구성하는 방법에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- Kaspersky Endpoint Agent 도움말 (Kaspersky Industrial CyberSecurity for Nodes 버전 3.1~4.0을 사용하는 경우).
- Kaspersky Industrial CyberSecurity for Linux Nodes 도움말

경고 세부 정보에서 파일을 격리로 이동

경고 세부 정보에서 파일을 격리로 이동하려면 다음과 같이 하십시오.

1. 경고 세부 정보를 엽니다.
2. **파일**에서 **대응 작업** 드롭다운 목록의 **격리 저장소로 이동** 버튼을 클릭합니다.
   파일이 장치에서 삭제되고 파일의 사본은 격리됩니다.

Kaspersky Industrial CyberSecurity for Linux Nodes 버전 1.5가 설치된 Linux 운영 체제 기반 컴퓨터에서는 이 작업을 사용할 수 없습니다.

경고 세부 정보에서 IOC 검사 작업 생성

경고 세부 정보에서 IOC 검사 작업을 생성하려면 다음과 같이 하십시오.

1. 경고 세부 정보를 엽니다.
2. **모든 경고 이벤트** 탭에서 IOC 검사 작업을 생성할 항목을 선택합니다.
3. **IOC 생성** 버튼을 클릭합니다.
4. 침해지표의 트리거 조건을 선택합니다.
   - 선택한 개체 중 하나라도 탐지될 때 침해지표가 트리거되도록 하려면 화면 오른쪽에서 **OR(발견한 IOC)**을 선택합니다.
   - 선택한 모든 개체가 탐지될 때 침해지표가 트리거되도록 하려면 화면 오른쪽에서 **AND(발견한 IOC 전체)**을 선택합니다.
5. IOC가 트리거될 때 수행할 작업을 선택합니다.
   - 네트워크에서 장치 격리.
   - 중요 영역 검사 시작.
   - 사본 격리 및 개체 삭제.
6. **작업 생성** 버튼을 클릭합니다.

생성된 작업은 **장치** → **작업** 섹션에서 확인할 수 있습니다.

경고 세부 정보에서 선택한 개체(파일 또는 프로세스)에 대한 IOC 검사 작업을 생성하면 FileItem 용어가 포함된 IOC가 자동으로 생성됩니다.

경고 세부 정보에서 개체 실행 방지

경고가 발생한 장치에 Kaspersky Industrial CyberSecurity for Nodes의 활성 정책이 적용된 경우 해당 장치에 실행 방지 규칙이 적용됩니다. 경고가 발생한 장치가 활성 정책으로 관리되지 않는 경우 실행 방지 규칙이 생성되지 않습니다.

경고 세부 정보에서 개체 실행을 방지하려면 다음과 같이 하십시오.

1. 경고 세부 정보를 엽니다.
2. **파일** 섹션에서 **실행 방지** 버튼을 클릭합니다.

개체 실행이 방지됩니다. 장치가 속한 그룹의 정책에 실행 방지 규칙이 추가됩니다.

Kaspersky Industrial CyberSecurity for Linux Nodes 버전 1.5가 설치된 Linux 운영 체제 기반 컴퓨터에서는 이 작업을 사용할 수 없습니다.

경고 세부 정보에서 Active Directory 사용자에 대한 대응 조치

Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 확장 기능을 사용하면 경고의 영향을 받거나 경고에 관련된 Active Directory 사용자에 대한 대응 조치를 수행할 수 있습니다. 다음 대응 조치를 수행할 수 있습니다.

- 사용자 암호 재설정.
- 사용자 계정 차단.
- 보안 그룹에 사용자 추가.
- 보안 그룹에서 사용자 제거.

이러한 대응 조치는 Kaspersky Industrial CyberSecurity for Nodes 4.5 이상이 설치된 보호 장치에서만 사용할 수 있습니다.

이 기능을 사용하려면 Active Directory와의 통합을 구성해야 합니다. 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

사용자 암호 재설정

Active Directory 계정 속성에서 **사용자가 암호를 변경할 수 없음** 설정이 활성화된 사용자의 경우 **암호 초기화** 대응 조치가 실행되지 않습니다.

경고 세부 정보에서 Active Directory 사용자 암호를 재설정하려면 다음과 같이 하십시오.

1. 경고 세부 정보를 엽니다.
2. **경고 세부 정보 → 파일** 설정 그룹으로 이동한 다음 **소유자** 필드의 드롭다운 목록에서 **암호 초기화**을 선택합니다.

   Active Directory 사용자 암호가 재설정됩니다.

Active Directory 사용자 계정 속성에서 **암호 사용 기간 제한 없음** 설정이 활성화된 경우 **암호 초기화** 대응 조치가 실행되면 **암호 사용 기간 제한 없음** 설정이 비활성화되고 사용자는 다음 로그인 시 도메인 암호를 변경해야 합니다.

사용자 계정 차단

경고 세부 정보에서 Active Directory 사용자 계정을 차단하려면 다음과 같이 하십시오.

1. 경고 세부 정보를 엽니다.
2. **경고 세부 정보 → 파일** 설정 그룹으로 이동한 다음 **소유자** 필드의 드롭다운 목록에서 **사용자 계정 차단**을 선택합니다.

   Active Directory 사용자 계정이 차단됩니다.

보안 그룹에 사용자 추가

경고 세부 정보에서 Active Directory 사용자를 보안 그룹에 추가하려면 다음과 같이 하십시오.

1. 경고 세부 정보를 엽니다.
2. **경고 세부 정보 → 파일** 설정 그룹으로 이동한 다음 **소유자** 필드의 드롭다운 목록에서 **보안 그룹에 사용자 추가**를 선택합니다.

   보안 그룹에 사용자 추가 창이 열립니다.
3. 보안 그룹의 전체 경로를 입력합니다.
4. **추가** 버튼을 누릅니다.

   사용자가 보안 그룹에 추가됩니다. 사용자 보안 그룹 정보가 업데이트되는 데 최대 12시간이 걸릴 수 있습니다.

보안 그룹에서 사용자 제거

경고 세부 정보에서 Active Directory 사용자를 보안 그룹에서 제거하려면 다음과 같이 하십시오.

1. 경고 세부 정보를 엽니다.
2. **경고 세부 정보 → 파일** 설정 그룹으로 이동한 다음 **소유자** 필드의 드롭다운 목록에서 **보안 그룹에서 사용자 제거**를 선택합니다.

   보안 그룹에서 사용자 제거 창이 열립니다.
3. 보안 그룹의 전체 경로를 입력합니다.
4. **삭제** 버튼을 클릭합니다.

   사용자가 보안 그룹에서 제거됩니다. 사용자 보안 그룹 정보가 업데이트되는 데 최대 12시간이 걸릴 수 있습니다.

경고 세부 정보에서 사용자에게 Kaspersky ASAP 교육 과정 할당

Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 확장 기능을 사용하면 경고 세부 정보에서 직접 경고를 처리하는 사용자에게 Kaspersky Automated Security Awareness Platform 교육 과정을 할당할 수 있습니다.

이 기능을 사용하려면 Active Directory 및 Kaspersky ASAP과의 통합을 구성해야 합니다. 자세한 내용은 다음 Kaspersky Security Center 도움말 문서를 참조하십시오: Active Directory와의 통합 구성, Kaspersky Automated Security Awareness Platform과의 통합 구성.

경고 세부 정보에서 Kaspersky ASAP 교육 과정을 할당하려면 다음과 같이 하십시오.

1. 경고 세부 정보를 엽니다.
2. **경고 세부 정보 → 파일** 설정 그룹으로 이동한 다음 **소유자** 필드의 드롭다운 목록에서 **KASAP 과정 할당**을 선택합니다.

   사용자 세부 창이 열립니다.
3. **KASAP 그룹 할당** 드롭다운 목록에서 사용자의 교육 그룹을 선택합니다.

   선택한 그룹이 사용자에게 할당됩니다.

할당된 교육 과정은 **사용자 세부** 창의 **할당된 과정** 섹션에서 확인할 수 있습니다.

모니터링 및 리포트

Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 작동을 모니터링하는 데 다음 기능을 사용할 수 있습니다.

- EDR 경고 위젯
- 경고 목록
- Kaspersky Security Center 리포트 및 선택 항목

경고 목록 보기

모든 경고를 목록으로 보려면,

웹 콘솔에서 **모니터링** → **경고**을 선택합니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response 활성화 후 **경고** 섹션이 자동으로 표시됩니다. Kaspersky Security Center에서 이 섹션이 표시되도록 설정할 수도 있습니다.

경고 목록에서 선택한 경고의 세부 정보를 열 수 있습니다.

실행 방지 규칙 트리거 정보 보기

Kaspersky Security Center 기능을 사용하면 Kaspersky Industrial CyberSecurity Endpoint Detection and Response에서 실행 방지 규칙이 작동하여 실행이 차단된 애플리케이션에 대한 정보를 확인할 수 있습니다.

실행이 차단된 애플리케이션에 대한 리포트를 보려면 다음과 같이 하십시오.

1. 웹 콘솔에서 **모니터링** → **리포트**을 선택합니다.
2. 목록에서 필요한 리포트를 선택합니다.
   - **금지한 애플리케이션 리포트** – 차단 및 리포트에 기록 모드에서 실행이 차단된 애플리케이션에 대한 정보를 봅니다.
   - **테스트 모드에서 운영된 금지한 애플리케이션 리포트** – 이벤트만 기록 모드에서 실행이 차단된 애플리케이션에 대한 정보를 봅니다.

격리된 장치 목록 보기

Kaspersky Security Center 기능을 사용하면 네트워크 격리가 활성화된 장치에 대한 정보를 확인할 수 있습니다.

ISOLATED FROM NETWORK 태그를 사용하여 장치 선택을 생성하면 이 정보를 확인할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서는 이 서버에 네트워크 격리를 한 번 이상 적용한 후에만 물리적 중앙 관리 서버에서 격리된 장치 선택을 생성할 수 있습니다.

네트워크에서 격리된 장치 목록을 보려면 다음과 같이 하십시오.

1. **에셋 관리** → **태그** → **기기 태그** 항목으로 이동합니다.
2. ISOLATED FROM NETWORK 태그 필드에서 **기기 보기** 버튼을 클릭합니다.

   그러면 격리된 장치 목록이 열립니다.

네트워크에서 격리된 장치 선택을 생성하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 웹 콘솔에서 **에셋 관리** → **기기 조회** 섹션으로 이동합니다.
2. 장치 선택을 생성하려면 **추가** 버튼을 클릭합니다.
3. 새 조건을 만들고 **태그** 탭을 선택합니다.
4. **추가** 버튼을 클릭합니다.
5. **태그 추가** 창에서 **이 태그가 있는 모든 기기**을 선택한 다음, **태그** 드롭다운 목록에서 ISOLATED FROM NETWORK을 선택합니다.
6. 열려 있는 모든 창에서 **저장**을 클릭합니다.
7. 생성된 선택을 열지 묻는 메시지가 표시되면 확인합니다.

   새 선택에는 네트워크에서 격리된 장치 목록이 표시됩니다.

Endpoint Agent 모드

Endpoint Agent 모드의 Kaspersky Industrial CyberSecurity for Nodes를 사용하면 타사 EPP 애플리케이션과 함께 Kaspersky Detection and Response 솔루션을 배포할 수 있습니다. Endpoint Agent 구성은 조직의 IT 인프라에 있는 개별 워크스테이션과 서버에 설치되며 컴퓨터에서 실행 중인 프로세스, 열린 네트워크 연결 및 수정 중인 파일을 지속적으로 모니터링합니다. 이 모드에서는 Kaspersky Industrial CyberSecurity for Nodes의 보호 및 제어 구성 요소를 사용할 수 없습니다.

Endpoint Agent 모드의 Kaspersky Industrial CyberSecurity for Nodes는 다음 Kaspersky 솔루션을 지원합니다.

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection and Response Expert(on-premise)

또한 Endpoint Agent 모드는 Kaspersky Industrial CyberSecurity for Networks 애플리케이션과의 통합과 Sigma 규칙을 사용한 이상 행위 탐지 기능을 포함합니다.

Endpoint Agent 모드로 Kaspersky Industrial CyberSecurity for Nodes 설치

Endpoint Agent 모드의 Kaspersky Industrial CyberSecurity for Nodes 설치 프로세스는 Kaspersky Industrial CyberSecurity for Nodes를 설치하는 것과 같습니다. 설치 패키지 설정 또는 설치 마법사의 애플리케이션 구성 요소 선택 단계에서 Endpoint Agent를 선택합니다.

Endpoint Agent 모드로 Kaspersky Industrial CyberSecurity for Nodes를 설치하고 나면 애플리케이션 콘솔과 시스템 트레이의 애플리케이션 아이콘 을 사용할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 Endpoint Agent 모드로 애플리케이션이 설치된 컴퓨터에는 *심각* 상태()가 표시됩니다. 실시간 파일 보호 구성 요소가 없기 때문에 컴퓨터에 이러한 상태가 표시됩니다. 별도의 조치를 취할 필요가 없습니다.

설치 프로그램이 타사 EPP 애플리케이션이 있는 컴퓨터에서 호환되지 않는 소프트웨어를 발견하여 Endpoint Agent 모드로 Kaspersky Industrial CyberSecurity for Nodes를 설치할 수 없다면 애플리케이션을 설치할 때 호환되지 않는 소프트웨어 검사를 비활성화할 수 있습니다.

타사 EPP 애플리케이션과의 호환성

Endpoint Agent 모드의 Kaspersky Industrial CyberSecurity for Nodes는 다음 공급업체의 EPP 애플리케이션과 호환됩니다.

- **Bitdefender**

  Bitdefender Endpoint Security Tools 버전 8.26.7.647.

- **Dallas Lock**

  Dallas Lock 8.0-C 버전 843.2.

- **ESET**

  ESET Endpoint Security 버전 13.0.2044.0 및 ESET Management Agent 버전 13.2.1189.0.

- **Secret Net Studio**

  Secret Net Studio 버전 8.11(20851).

  안티 바이러스 구성 요소와 함께 Secret Net Studio가 배포된 컴퓨터에는 애플리케이션을 설치할 수 없습니다. 상호 운용이 가능하게 하려면 Secret Net Studio에서 안티 바이러스 구성 요소를 제거해야 합니다.

- **Sophos**

  Sophos Intercept X 버전 2024.1.2 이상(Endpoint Agent 포함 및 Sophos Core Agent 버전 2026.2.1.3).

- **Trend Micro**

  Trend Micro Vision One Apex One(Security Agent 14.0.20731 포함).

Trend Micro Deep Security 버전 20.0.3-18160(Security Agent 포함).

- **마이크로소프트**

  Microsoft Defender Antivirus, Windows 보안의 일부(이전 명칭: Windows Defender).

애플리케이션은 다음 순서대로 설치해야 합니다. 먼저 EPP 애플리케이션을 설치한 다음 Kaspersky Security Center 네트워크 에이전트를 설치하고 마지막으로 Endpoint Agent 모드의 Kaspersky Industrial CyberSecurity for Nodes를 설치합니다. 이 과정이 필요한 이유는 EPP 애플리케이션 설치 프로그램이 Endpoint Agent 모드의 Kaspersky Industrial CyberSecurity for Nodes 및 네트워크 에이전트를 호환되지 않는 소프트웨어로 감지하여 제거할 수 있기 때문입니다. 타사 EPP 애플리케이션을 업데이트한 후에는 Endpoint Agent 모드의 애플리케이션 및 네트워크 에이전트가 제대로 작동하는지도 확인해야 합니다. 해당 설치 프로그램이 컴퓨터에서 호환되지 않는 소프트웨어를 다시 검사하여 애플리케이션을 제거할 수 있기 때문입니다.

Managed Detection and Response

Kaspersky Industrial CyberSecurity for Nodes는 Managed Detection and Response 솔루션과의 통합을 지원합니다.

Kaspersky Managed Detection and Response(이하 MDR)는 전문 기술과 직원을 확보하기 어렵거나 내부 리소스가 제한적인 조직을 위해 자동화된 보안 장벽을 우회하는 위협으로부터 24시간 보호 기능을 제공합니다. 시장에 나와 있는 유사한 솔루션과 달리 이 서비스는 효과적인 표적 공격 연구의 검증된 추적 기록을 활용하여 가장 복잡한 위협에 대한 지속적인 보호를 보장합니다. 이 서비스는 사이버 위협에 대한 기업의 복원력을 개선하는 동시에 기존 리소스를 다른 작업에 집중할 수 있도록 도와줍니다.

MDR은 엔드포인트 및 기계 학습에서 수신한 원격 측정 데이터를 사용합니다. MDR은 인시던트 데이터를 Kaspersky 전문가에게 보냅니다. 그러면 전문가는 인시던트를 처리하고, 안티 바이러스 데이터베이스에 새 항목 추가 등의 행동을 할 수 있습니다. 또는 전문가가 인시던트 처리에 대한 권장 사항을 발표하고 예를 들어 네트워크에서 컴퓨터를 격리하도록 제안할 수 있습니다. 솔루션 작동 방식에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

MDR과 통합하기 위한 Kaspersky Industrial CyberSecurity for Nodes 구성

MDR 작업에는 다음 구성을 사용할 수 있습니다.

- **[KICS+내장 에이전트]**. 이 구성에서 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터 보안을 책임지는 애플리케이션이자 MDR 작업을 위한 애플리케이션으로서 작동합니다. 이 내장 에이전트는 Kaspersky Industrial CyberSecurity for Nodes 4.5 버전부터 사용할 수 있습니다.

- **[타사 EPP+Endpoint Agent 모드의 KICS]**. 이 구성에서는 타사 EPP(Endpoint Protection Platform)를 통해 IT 인프라 보안이 제공됩니다. Kaspersky Industrial CyberSecurity for Nodes는 Endpoint Agent 모드에서 MDR과 통합할 수 있습니다. Endpoint Agent 모드는 Kaspersky Industrial CyberSecurity for Nodes 4.5 버전부터 사용할 수 있습니다.

MDR 통합 구성

Kaspersky Managed Detection and Response와의 통합은 다음 단계로 구성됩니다:

1. **Managed Detection and Response(Industrial CyberSecurity) 구성 요소 설치**

   Kaspersky Industrial CyberSecurity for Nodes와 Managed Detection and Response 솔루션의 통합을 위해 Managed Detection and Response(Industrial CyberSecurity) 구성 요소가 사용됩니다. 설치 패키지 설정이나 설치 마법사를 사용하여 이 구성 요소를 설치하거나 Windows 제어판에서 애플리케이션 구성 요소의 구성을 변경할 때 다음을 선택합니다.

   - **전체 기능** → **Endpoint Agent** → 내장 에이전트를 위한 **Managed Detection and Response(Industrial CyberSecurity)**
   - **Endpoint Agent** → Endpoint Agent 구성을 위한 **Managed Detection and Response(Industrial CyberSecurity)**

   또한 *Kaspersky Industrial CyberSecurity for Nodes 구성 요소 변경* 작업을 사용하여 구성 요소를 설치할 수 있습니다.

   > *Kaspersky Industrial CyberSecurity for Nodes 구성 요소 변경* 작업을 사용하여 컴퓨터를 다시 시작하지 않고 Managed Detection and Response(Industrial CyberSecurity) 구성 요소를 설치하려면 작업 설정에서 **호환되지 않는 타사 애플리케이션 확인** 옵션을 비활성화해야 합니다.

2. **Kaspersky Private Security Network**

   2025년 7월 업데이트부터 Managed Detection and Response 솔루션이 KPSN 구성 파일 없는 작동을 지원합니다. MDR 솔루션이 Kaspersky Security Network를 사용하는 방식에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

   구성이 KPSN 구성 파일 없이 실행하기 위한 요구 사항을 충족하지 않으면 중앙 관리 서버 속성에서 KPSN 구성 파일을 업로드합니다. KPSN 구성 파일은 MDR 구성 파일의 ZIP 압축파일 안에 있습니다. 명령줄을 사용하여 KPSN 구성 파일을 업로드할 수도 있습니다.

   Kaspersky Private Security Network 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

3. **Kaspersky Managed Detection and Response 활성화**

   > Kaspersky Industrial CyberSecurity for Nodes를 이전 버전에서 버전 4.5 이상으로 업그레이드하면 이전에 MDR 구성 파일(BLOB 파일)을 사용하여 활성화했던 Managed Detection and Response 솔루션이 자동으로 활성화되지 않습니다. 키 파일 또는 활성화 코드를 사용하여 Managed Detection and Response 솔루션을 다시 활성화해야 합니다.

   Kaspersky Industrial CyberSecurity for Nodes에서 Managed Detection and Response 솔루션을 활성화하려면 Kaspersky Managed Detection and Response for Industrial CyberSecurity 애드온에 대한 별도 라이센스가 필요합니다.

   > 버전 4.5부터 Kaspersky Industrial CyberSecurity for Nodes MDR 구성 파일(BLOB 파일)만 사용하여 Managed Detection and Response 솔루션을 활성화하는 것을 지원하지 않습니다.

   MDR 테넌트를 사용하는 경우 BLOB 파일이 만료되었더라도 활성화 코드를 적용하기 전에 테넌트의 BLOB 파일을 업로드해야 합니다.

MDR 테넌트를 사용하지 않고 생성한 적도 없다면 BLOB 파일을 업로드할 필요가 없습니다.

솔루션 활성화에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

4. **Managed Detection and Response(Industrial CyberSecurity) 구성 요소 활성화**

Kaspersky Security Center 관리 콘솔에서 Managed Detection and Response(Industrial CyberSecurity) 구성 요소를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **원격 측정 수집 서버** 섹션을 선택합니다.
4. **Managed Detection and Response(Industrial CyberSecurity)** 블록에서 **설정** 버튼을 클릭합니다.
   Managed Detection and Response(Industrial CyberSecurity) 창이 열립니다.
5. **Managed Detection and Response** 확인란을 선택합니다.
6. 필요한 경우 **업로드** 버튼을 클릭하여 MDR 구성 파일을 업로드합니다. MDR 구성 파일에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

   Managed Detection and Response 구성 파일을 업로드하면, Kaspersky Industrial CyberSecurity for Nodes가 사전 설치된 장치에서 처리를 위해 Kaspersky에 지정된 데이터를 자동 전송하는 데 동의하는 것입니다. 지정된 정보가 처리되지 않도록 하려면 구성 파일을 업로드하지 마십시오.

7. 변경 사항을 저장합니다.

웹 콘솔에서 Managed Detection and Response(Industrial CyberSecurity) 구성 요소를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **원격 측정 수집 서버** 섹션을 선택합니다.
5. **Managed Detection and Response(Industrial CyberSecurity)** 블록에서 **설정** 버튼을 클릭합니다.
   Managed Detection and Response(Industrial CyberSecurity) 창이 열립니다.
6. **Managed Detection and Response(Industrial CyberSecurity) 비활성화됨** 확인란을 선택합니다.
7. 필요한 경우 **업로드** 버튼을 클릭하여 MDR 구성 파일을 업로드합니다. MDR 구성 파일에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

   Managed Detection and Response 구성 파일을 업로드하면, Kaspersky Industrial CyberSecurity for Nodes가 사전 설치된 장치에서 처리를 위해 Kaspersky에 지정된 데이터를 자동 전송하는 데 동의하는 것입니다. 지정된 정보가 처리되지 않도록 하려면 구성 파일을 업로드하지 마십시오.

8. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 Managed Detection and Response(Industrial CyberSecurity) 구성 요소를 활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **원격 측정 수집 서버** → **Managed Detection and Response(Industrial CyberSecurity)** 섹션을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.

   일반 탭에서 **Managed Detection and Response(Industrial CyberSecurity)** 창이 열립니다.
3. **Managed Detection and Response** 확인란을 선택합니다.
4. 필요한 경우 **업로드** 버튼을 클릭하여 MDR 구성 파일을 업로드합니다. MDR 구성 파일에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

   > Managed Detection and Response 구성 파일을 업로드하면, Kaspersky Industrial CyberSecurity for Nodes가 사전 설치된 장치에서 처리를 위해 Kaspersky에 지정된 데이터를 자동 전송하는 데 동의하는 것입니다. 지정된 정보가 처리되지 않도록 하려면 구성 파일을 업로드하지 마십시오.
5. 변경 사항을 저장합니다.

명령줄을 사용하여 Managed Detection and Response(Industrial CyberSecurity) 구성 요소를 활성화할 수도 있습니다.

5 원격 측정을 수신하도록 애플리케이션의 다른 구성 요소 구성

Kaspersky Managed Detection and Response가 작동하려면 다음 구성 요소를 활성화해야 합니다.

- Kaspersky Security Network(확장 모드)
- 실시간 파일 보호.
- AMSI 스캐너.
- Anti-Cryptor
- 익스플로잇 방지.
- 네트워크 위협 보호.
- 방화벽.
- 온디맨드 검사.

Kaspersky Managed Detection and Response가 Kaspersky Security Center 웹 콘솔을 통해 관리 서버를 사용하려면 새로운 보안 연결인 *백그라운드 연결*도 구성해야 합니다. 솔루션 배포 시 Kaspersky Managed Detection and Response가 백그라운드 연결을 구성할 것인지 묻는 메시지를 표시합니다. 백그라운드 연결을 구성해야 합니다.

Kaspersky Security Center 웹 콘솔에서 백그라운드 연결 구성

1. 웹 콘솔의 메인 창에서 **설정** → **통합** 옵션을 선택합니다.
2. **통합** 섹션으로 갑니다.

3. **통합을 위한 백그라운드 연결 활성화됨** 토글을 켭니다.

4. 변경 사항을 저장합니다.

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform은 조직의 IT 인프라를 보호하고 제로 데이 공격, 표적형 공격, 지능형 지속 위협(이하 APT) 등의 위협을 조기에 탐지하기 위한 솔루션입니다.

Kaspersky Anti Targeted Attack Platform 솔루션에는 다음 세 가지 기능 단위가 포함됩니다.

- Kaspersky Anti Targeted Attack(이하 KATA) – 기업의 IT 인프라 경계를 보호합니다.
- Kaspersky Endpoint Detection and Response(이하 KEDR) – 조직 로컬 네트워크의 컴퓨터를 보호합니다.
- Network Detection and Response – 기업 LAN을 보호합니다.

이 솔루션에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

솔루션 작동 원리

Kaspersky Industrial CyberSecurity for Nodes는 조직의 IT 인프라에 포함된 Windows를 실행하는 개별 컴퓨터에 설치됩니다. 애플리케이션은 프로세스, 개방형 네트워크 연결, 수정 중인 파일을 계속해서 모니터링합니다. 컴퓨터 이벤트, 애플리케이션에서 탐지한 위협 및 이러한 위협 처리 결과에 대한 정보는 Central Node 서버로 전송됩니다.

KEDR(KATA)과의 통합은 Kaspersky Security Center 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 구성됩니다. 그러면 내장 에이전트 또는 Endpoint Agent 모드의 애플리케이션이 Kaspersky Anti Targeted Attack Platform 콘솔을 통해 관리됩니다. 여기에는 작업 실행, 격리된 개체 관리, 리포트 보기 및 기타 동작이 포함됩니다.

Kaspersky Anti Targeted Attack Platform과의 통합을 위한 Kaspersky Industrial CyberSecurity for Nodes 구성

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Anti Targeted Attack Platform 솔루션의 일부인 Kaspersky Endpoint Detection and Response와 통합할 수 있습니다. 다음 구성이 가능합니다.

- **[KICS+내장 에이전트]**. 이 구성에서 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터 보안을 책임지는 애플리케이션이자 KEDR 작업을 위한 애플리케이션으로서 작동합니다. 이 내장 에이전트는 Kaspersky Industrial CyberSecurity for Nodes 4.5 버전부터 사용할 수 있습니다.
- **[타사 EPP+Endpoint Agent 모드의 KICS]**. 이 구성에서는 타사 EPP(Endpoint Protection Platform)를 통해 IT 인프라 보안이 제공됩니다. Kaspersky Industrial CyberSecurity for Nodes는 Endpoint Agent 모드에서 KEDR과 통합할 수 있습니다. Endpoint Agent 모드는 Kaspersky Industrial CyberSecurity for Nodes 4.5 버전부터 사용할 수 있습니다.

이전 버전의 Kaspersky Industrial CyberSecurity for Nodes 지원

Kaspersky Industrial CyberSecurity for Nodes 4.5는 내장 에이전트 또는 Endpoint Agent 모드를 사용하여 Kaspersky Anti Targeted Attack Platform(EDR) 솔루션과의 통합을 지원합니다. Kaspersky Endpoint Agent는 설치할 필요가 없습니다.

Kaspersky Anti Targeted Attack Platform(EDR)과의 통합을 위해 4.5 이전 버전의 Kaspersky Industrial CyberSecurity for Nodes 사용한다면, Kaspersky Endpoint Agent를 별도로 설치해야 합니다.

KATA 통합 구성

Kaspersky Industrial CyberSecurity for Nodes 4.5부터 KATA 통합 구성 요소의 이름이 Endpoint Detection and Response Expert(on-premises)로 바뀌었습니다. 이 버전의 애플리케이션에서 구성 요소는 Kaspersky Anti Targeted Attack Platform 7.1 이하 버전 및 Kaspersky Endpoint Detection and Response Expert(on-premises)와 호환됩니다.

Endpoint Detection and Response(Industrial CyberSecurity) 및 Endpoint Detection and Response Expert(on-premises) 구성 요소는 서로 호환되지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes 내장 에이전트와 KATA를 통합하려면 다음 조건을 충족해야 합니다.

- 기업 IT 인프라에 Kaspersky Anti Targeted Attack Platform 5.0 이상을 배포해야 합니다.
- 기업 IT 인프라에 Kaspersky Security Center 14.2 이상을 배포해야 합니다.
- KATA로 데이터를 전송하는 애플리케이션 구성 요소가 활성화되고 작동해야 합니다.
  - 실시간 파일 보호
  - 익스플로잇 방지
  - Anti-Cryptor
  - AMSI 스캐너
  - Kaspersky Security Network

기업 IT 인프라에서 Endpoint Agent 구성을 KATA와 통합하려면 다음을 배포해야 합니다:

- Kaspersky Anti Targeted Attack Platform 버전 5.0 이상.
- Kaspersky Security Center 버전 14.2 이상.

KATA 통합 설정에는 다음 단계가 포함됩니다.

1. **Endpoint Detection and Response Expert(on-premises) 구성 요소 설치**

설치 패키지 설정이나 설치 마법사에서, 또는 Windows 제어판의 애플리케이션 구성 요소 집합 변경을 통해, 설치할 애플리케이션 구성 요소 선택 단계에서 다음을 선택합니다:

- **전체 기능** → **Endpoint Agent** → 내장 에이전트를 위한 **Endpoint Detection and Response Expert(on-premises)**
- **Endpoint Agent** → Endpoint Agent 구성을 위한 **Endpoint Detection and Response Expert(on-premises)**

애플리케이션 구성 요소 집합 변경을 완료하려면 컴퓨터를 다시 시작해야 합니다.

2 Endpoint Detection and Response Expert(on-premises) 활성화

KATA용 별도 라이센스를 구매해야 합니다(Kaspersky Endpoint Detection and Response(KATA) 애드온 등).

독립 실행형 Endpoint Detection and Response Expert(on-premises) 기능의 라이센스는 Kaspersky Industrial CyberSecurity for Nodes의 라이센스와 같습니다. 이 기능은 Kaspersky Endpoint Detection and Response(KATA)의 키를 별도로 추가한 후에 이용할 수 있습니다. 결과적으로 Kaspersky Industrial CyberSecurity for Nodes 키와 Endpoint Detection and Response Expert(on-premises) 키가 컴퓨터에 추가됩니다.

라이센스에 Endpoint Detection and Response Expert(on-premises) 기능이 포함되었는지 확인합니다.

3 Central Node에 연결

Kaspersky Anti Targeted Attack Platform에서 Kaspersky Industrial CyberSecurity for Nodes와 Central Node 구성 요소 간에 신뢰할 수 있는 연결을 설정할 수 있습니다. 신뢰할 수 있는 연결을 구성하려면 TLS 인증서를 사용해야 합니다. Kaspersky Anti Targeted Attack Platform 콘솔에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Anti Targeted Attack Platform 도움말의 지침 참조). 그런 다음 Kaspersky Industrial CyberSecurity for Nodes에 TLS 인증서를 추가해야 합니다(아래 지침 참조).

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 Central Node의 TLS 인증서만 확인합니다. 더 안전한 연결을 위해, Central Node에서 컴퓨터 확인을 추가로 활성화할 수 있습니다. 이 확인을 활성화하려면 Central Node와 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증을 켜야 합니다. 양방향 인증을 사용하려면 암호화 컨테이너도 필요합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Anti Targeted Attack Platform 콘솔에서 암호화 컨테이너를 얻을 수 있습니다(Kaspersky Anti Targeted Attack Platform 도움말의 지침 참조).

Kaspersky Security Center 관리 콘솔을 사용하여 Kaspersky Industrial CyberSecurity for Nodes 컴퓨터를 Central Node에 연결하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책** 폴더를 엽니다.
3. 애플리케이션 관리 정책을 선택하고 더블클릭하여 설정 창을 엽니다.
4. **원격 측정 수집 서버** 섹션을 선택합니다.
5. **Endpoint Detection and Response Expert(on-premises)** 블록에서 **설정** 버튼을 클릭합니다.

   Endpoint Detection and Response Expert(on-premises) 창이 열립니다.
6. **Endpoint Detection and Response Expert(버전 7.1 이하)** 확인란을 선택합니다.
7. **연결 설정**에서 **추가** 버튼을 클릭하여 하나 이상의 Central Node 서버를 추가합니다. 각 서버에 서버 연결을 위한 주소(IPv4, IPv6)와 포트를 지정합니다.

   Kaspersky Industrial CyberSecurity for Nodes가 첫 번째 IP 주소에서 서버와의 연결 설정을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Industrial CyberSecurity for Nodes는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

8. **서버 연결 설정** 버튼을 클릭합니다.

9. 창이 열리면 서버에 대한 연결을 구성합니다.

   - **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 다른 Central Node 서버에 연결을 시도합니다.

   - **서버 TLS 인증서**. Central Node 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Anti Targeted Attack Platform 콘솔에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Anti Targeted Attack Platform 도움말 의 지침 참조).

   - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 Central Node 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Anti Targeted Attack Platform 콘솔에서 암호화 컨테이너를 얻을 수 있습니다(Kaspersky Anti Targeted Attack Platform 도움말 의 지침 참조). Central Node 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

     암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

10. **확인** 버튼을 클릭합니다.

11. 필요한 경우 원격 측정을 구성합니다.

12. 변경 사항을 저장합니다.

애플리케이션 콘솔을 사용하여 Kaspersky Industrial CyberSecurity for Nodes 컴퓨터를 Central Node에 연결하는 방법

1. 애플리케이션 콘솔 트리에서 **원격 측정 수집 서버 → Endpoint Detection and Response Expert(on-premises)** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.

   일반 탭에서 **속성: Endpoint Detection and Response Expert(on-premises)** 창이 열립니다.

3. **Endpoint Detection and Response Expert(버전 7.1 이하)** 확인란을 선택합니다.

4. **연결 설정**에서 **추가** 버튼을 클릭하여 하나 이상의 Central Node 서버를 추가합니다. 각 서버에 서버 연결을 위한 주소(IPv4, IPv6)와 포트를 지정합니다.

   Kaspersky Industrial CyberSecurity for Nodes가 첫 번째 IP 주소에서 서버와의 연결 설정을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Industrial CyberSecurity for Nodes는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

5. **서버 연결 설정** 버튼을 클릭합니다.

6. 창이 열리면 서버에 대한 연결을 구성합니다.

   - **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 다른 Central Node 서버에 연결을 시도합니다.

   - **서버 TLS 인증서**. Central Node 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Anti Targeted Attack Platform 콘솔에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Anti Targeted Attack Platform 도움말의 지침 참조).

   - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 Central Node 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Anti Targeted Attack Platform 콘솔에서 암호화 컨테이너를 얻을 수 있습니다(Kaspersky Anti Targeted Attack Platform 도움말의 지침 참조). Central Node 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

     암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

7. **확인** 버튼을 클릭합니다.

8. 필요한 경우 원격 측정을 구성합니다.

9. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔을 사용하여 Kaspersky Industrial CyberSecurity for Nodes 컴퓨터를 Central Node에 연결하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **원격 측정 수집 서버** 섹션을 선택합니다.

5. **Endpoint Detection and Response Expert(on-premises)** 블록에서 **구성** 버튼을 클릭합니다.
   Endpoint Detection and Response Expert(on-premises) 창이 열립니다.

6. **Endpoint Detection and Response Expert(on-premises) 사용** 확인란을 선택합니다.

7. **Endpoint Detection and Response Expert(버전 7.1 이하)** 모드를 선택합니다.

8. **연결 설정**에서 **추가** 버튼을 클릭하여 하나 이상의 Central Node 서버를 추가합니다. 각 서버에 서버 연결을 위한 주소(IPv4, IPv6)와 포트를 지정합니다.
   Kaspersky Industrial CyberSecurity for Nodes가 첫 번째 IP 주소에서 서버와의 연결 설정을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Industrial CyberSecurity for Nodes는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

9. **KATA 서버 연결 설정** 버튼을 클릭합니다.

10. 창이 열리면 서버에 대한 연결을 구성합니다.

    - **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 다른 Central Node 서버에 연결을 시도합니다.

    - **서버 TLS 인증서**. Central Node 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Anti Targeted Attack Platform 콘솔에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Anti Targeted Attack Platform 도움말의 지침 참조).

    - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 Central Node 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Anti Targeted Attack Platform 콘솔에서 암호화 컨테이너를 얻을 수 있습니다(Kaspersky Anti Targeted Attack Platform 도움말의 지침 참조). Central Node 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

      암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

11. **확인** 버튼을 클릭합니다.

12. 필요한 경우 원격 측정을 구성합니다.

13. 변경 사항을 저장합니다.

결과적으로 Kaspersky Industrial CyberSecurity for Nodes 컴퓨터가 Kaspersky Anti Targeted Attack Platform 콘솔을 사용하여 추가됩니다.

원격 측정 구성

*원격 측정*은 보호된 컴퓨터에서 발생한 이벤트 목록입니다. Kaspersky Industrial CyberSecurity for Nodes는 원격 측정 데이터를 분석하여 동기화 시 Kaspersky Anti Targeted Attack Platform에 보냅니다. 원격 측정 이벤트는 거의 지속적으로 서버에 도착합니다. Kaspersky Industrial CyberSecurity for Nodes는 다음 조건 중 하나라도 충족되면 서버와의 동기화를 시작합니다.

- 동기화 주기가 되었습니다.
- 버퍼의 이벤트 개수가 상한을 초과합니다.

Kaspersky Industrial CyberSecurity for Nodes 정책에서 동기화 동작을 구성하고 네트워크 부하에 맞는 최적의 값을 선택할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes와 서버가 서로 연결되어 있지 않으면 애플리케이션이 새 이벤트를 대기시킵니다. 연결이 복원되면 Kaspersky Industrial CyberSecurity for Nodes가 대기열에 있는 이벤트들을 적절한 순서로 서버에 보냅니다. 서버 과부하를 방지하기 위해 Kaspersky Industrial CyberSecurity for Nodes는 일부 이벤트를 건너뛸 수 있습니다. 이를 활성화하기 위해 이벤트 전송 설정을 최적화할 수 있습니다. 예를 들어, 시간당 이벤트 값을 최대로 설정합니다.

Kaspersky Anti Targeted Attack Platform을 원격 측정을 사용하는 다른 솔루션과 함께 사용할 경우 KATA의 원격 측정을 끌 수 있습니다. 이렇게 하면 솔루션의 서버 로드를 최적화할 수 있습니다. 예를 들어 Managed Detection and Response와 Kaspersky Anti Targeted Attack Platform 솔루션이 배포되어 있다면, Managed Detection and Response 원격 측정을 사용하면서 Kaspersky Anti Targeted Attack Platform에서 보안 위협 대응 작업을 생성할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 원격 측정을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 콘솔 트리에서 **정책** 폴더를 엽니다.

3. 애플리케이션 관리 정책을 선택하고 더블클릭하여 설정 창을 엽니다.

4. **원격 측정 수집 서버** 섹션을 선택합니다.

5. **Endpoint Detection and Response Expert(on-premises)** 블록에서 **설정** 버튼을 클릭합니다.

6. 창이 열리면 **다음 시간마다 KATA 서버로 동기화 요청 보내기(분)** 설정을 구성합니다. 서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Industrial CyberSecurity for Nodes는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.

7. **데이터 전송 설정** 블록에서 **KATA로 원격 측정 전송** 확인란이 선택되었는지 확인합니다.

8. 필요하다면 **최대 이벤트 전송 지연(초)** 설정을 구성합니다. 지정된 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 같은 서버에 다시 연결을 시도하거나, 서버가 여러 개라면 목록의 다음 서버에 연결합니다. 기본 설정은 30초입니다.

9. 필요한 경우 **최대 이벤트 패키지 수** 설정을 구성합니다. 이 설정은 한 트랜잭션의 일부로 전송할 수 있는 패킷의 최대 수를 조절합니다. 기본값은 1024입니다.

10. 필요하다면 **요청 제한** 블록에서 **요청 제한 사용** 확인란을 선택합니다.

    이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다.

11. 이벤트를 서버로 전송하기 위한 최적화 설정을 구성합니다.

    - **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

    - **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 기본 설정은 15%입니다.

12. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 원격 측정을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **원격 측정 수집 서버** → **Endpoint Detection and Response Expert(on-premises)** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.

3. 창이 열리면 **다음 시간마다 KATA 서버로 동기화 요청 보내기(분)** 설정을 구성합니다. 서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Industrial CyberSecurity for Nodes는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.

4. **데이터 전송 설정** 블록에서 **KATA로 원격 측정 전송** 확인란이 선택되었는지 확인합니다.

5. 필요하다면 **최대 이벤트 전송 지연(초)** 설정을 구성합니다. 지정된 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 같은 서버에 다시 연결을 시도하거나, 서버가 여러 개라면 목록의 다음 서버에 연결합니다. 기본 설정은 30초입니다.

6. 필요한 경우 **최대 이벤트 패키지 수** 설정을 구성합니다. 이 설정은 한 트랜잭션의 일부로 전송할 수 있는 패킷의 최대 수를 조절합니다. 기본값은 1024입니다.

7. 필요하다면 **요청 제한** 블록에서 **요청 제한 사용** 확인란을 선택합니다.

   이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다.

8. 이벤트를 서버로 전송하기 위한 최적화 설정을 구성합니다.

   - **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

   - **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 기본 설정은 15%입니다.

9. 변경 사항을 저장합니다.

웹 콘솔에서 원격 측정을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **원격 측정 수집 서버** 섹션을 선택합니다.

5. **Endpoint Detection and Response Expert(on-premises)** 블록에서 **구성** 버튼을 클릭합니다.

6. 창이 열리면 **다음 시간마다 서버로 동기화 요청 보내기(분)** 설정을 구성합니다. 서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Industrial CyberSecurity for Nodes는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.

7. **데이터 전송 설정** 블록에서 **KATA로 원격 측정 전송** 확인란이 선택되었는지 확인합니다.

8. 필요하다면 **최대 이벤트 전송 지연(초)** 설정을 구성합니다. 지정된 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 같은 서버에 다시 연결을 시도하거나, 서버가 여러 개라면 목록의 다음 서버에 연결합니다. 기본 설정은 30초입니다.

9. 필요한 경우 **최대 이벤트 패키지 수** 설정을 구성합니다. 이 설정은 한 트랜잭션의 일부로 전송할 수 있는 패킷의 최대 수를 조절합니다. 기본값은 1024입니다.

10. 필요하다면 **제한** 블록에서 **제한 사용** 확인란을 선택합니다.

    이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다.

11. 이벤트를 서버로 전송하기 위한 최적화 설정을 구성합니다.

    - **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

    - **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 기본 설정은 15%입니다.

12. 변경 사항을 저장합니다.

Endpoint Detection and Response Expert(on-premises)

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Endpoint Detection and Response Expert (on-premises) 솔루션과의 통합을 지원합니다. Kaspersky Endpoint Detection and Response Expert (on-premises)는 기업 사이버 보안 솔루션으로, Kaspersky 애플리케이션을 통해 조직에서 대부분의 사이버 위험에 대응하고 가장 중요한 위협 전파 시나리오를 처리하도록 지원합니다. EDR Expert(on-premises) 구성 요소는 Open Single Management Platform(OSMP)에 배포됩니다. 이 플랫폼은 단일 인터페이스에서 크로스 플랫폼 시나리오를 실행하며, Kaspersky 애플리케이션과 타사 애플리케이션을 포괄적인 보안 시스템으로 통합할 수 있도록 합니다.

이 솔루션의 핵심 요소 중 하나는 *SIEM*입니다. SIEM은 모든 구성 요소에서 발생하는 이벤트를 추적하고 공급업체 및 사용자 정의 규칙을 사용하여 이러한 이벤트의 상관관계를 파악합니다. EDR Expert(on-premises)는 기업 인프라에서 수신한 로그 및 원격 측정을 확인하여 공격을 자동으로 탐지하며, Kaspersky 애플리케이션 타사 정보 보안 제품의 이벤트를 포함하여 EDR Expert(on-premises)에 수집된 모든 이벤트를 결합한 조사 그래프를 통해 사고를 조사하도록 지원합니다.

고급 인시던트에 대응하기 위해 EDR Expert(on-premises)는 사전 설정 및 사용자 정의 시나리오를 사용합니다. 또한 타사 애플리케이션 및 여러 애플리케이션이 관련된 대응 시나리오의 대응 작업을 사용할 수 있습니다.

위협 인텔리전스 도구

Kaspersky Endpoint Detection and Response는 다음 위협 인텔리전스 툴을 사용합니다:

- 파일 및 웹 주소의 평판에 대한 정보를 포함하고 표시하는 Kaspersky Threat Intelligence Portal과의 통합.
- Kaspersky 보안 위협 데이터베이스.
- Kaspersky 기술 자료에 있는 파일, 웹사이트 및 소프트웨어의 실시간 평판 정보에 대한 접근을 제공하는 Kaspersky Security Network 클라우드 서비스 인프라. Kaspersky Security Network의 데이터를 사용하면 Kaspersky 애플리케이션에서 보안 위협에 신속하게 대응할 수 있으며, 일부 보호 구성 요소의 성능을 향상하고 오탐의 가능성을 줄입니다.

솔루션 작동 원리

Kaspersky Industrial CyberSecurity for Nodes는 조직의 IT 인프라에 포함된 Windows를 실행하는 개별 컴퓨터에 설치됩니다. 애플리케이션은 프로세스, 개방형 네트워크 연결, 수정 중인 파일을 계속해서 모니터링합니다. 컴퓨터 이벤트, 애플리케이션에서 탐지한 위협 및 이러한 위협 처리 결과에 대한 정보는 EDR Expert (on-premises) 서버로 전송됩니다.

EDR Expert (on-premises) 통합은 Kaspersky Security Center 웹 콘솔에서 구성됩니다. 그러면 내장 에이전트 또는 Endpoint Agent 모드의 애플리케이션은 Open Single Management Platform(OSMP)을 사용하여 관리됩니다. 여기에는 작업 실행, 격리된 개체 관리, 리포트 보기 및 기타 동작이 포함됩니다.

Kaspersky Anti Targeted Attack Platform과의 통합을 위한 Kaspersky Industrial CyberSecurity for Nodes 구성

EDR Expert(on-premises) 작업에 다음 구성을 사용할 수 있습니다.

- **[KICS+내장 에이전트]**. 이 구성에서 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터 보안을 보장하는 애플리케이션이자 EDR Expert (on-premises)와 연동하는 애플리케이션으로 작동합니다. 내장 에이전트는 버전 4.5부터 EDR Expert (on-premises)와의 통합을 지원합니다.
- **[타사 EPP+Endpoint Agent 모드의 KICS]**. 이 구성에서는 타사 EPP(Endpoint Protection Platform)를 통해 IT 인프라 보안이 제공됩니다. Endpoint Agent 구성의 Kaspersky Industrial CyberSecurity for Nodes에서 EDR Expert (on-premises)와의 통합을 제공합니다. Endpoint Agent 구성은 버전 4.5부터 EDR Expert (on-premises)와의 통합을 지원합니다.

EDR Expert (on-premises) 통합 구성

Endpoint Detection and Response(Industrial CyberSecurity) 및 Endpoint Detection and Response Expert(on-premises) 구성 요소는 서로 호환되지 않습니다.

Endpoint Detection and Response Expert(on-premises)의 작동을 위해서는 다음 조건을 만족해야 합니다:

- OSMP(Open Single Management Platform)가 설치되어 있습니다.
- 애플리케이션이 활성화되고 해당 기능에 라이센스가 적용됩니다.
- Endpoint Detection and Response Expert(on-premises) 구성 요소가 활성화되어있습니다.
- EDR Expert(on-premises)의 동작을 보장하는 애플리케이션 구성 요소가 활성화되고 작동합니다. EDR Expert(on-premises)의 동작을 보장하는 구성 요소는 다음과 같습니다.
  - 실시간 파일 보호
  - 익스플로잇 방지
  - Anti-Cryptor
  - AMSI 스캐너
  - Kaspersky Security Network

EDR Expert(on-premises) 통합 설정에는 다음 단계가 포함됩니다:

1. **Endpoint Detection and Response Expert(on-premises) 구성 요소 설치**

   설치 패키지 설정이나 설치 마법사에서, 또는 Windows 제어판의 애플리케이션 구성 요소 집합 변경을 통해, 설치할 애플리케이션 구성 요소 선택 단계에서 다음을 선택합니다:

   - **전체 기능** → **Endpoint Agent** → 내장 에이전트를 위한 **Endpoint Detection and Response Expert(on-premises)**
   - **Endpoint Agent** → Endpoint Agent 구성을 위한 **Endpoint Detection and Response Expert(on-premises)**

   애플리케이션 구성 요소 집합 변경을 완료하려면 컴퓨터를 다시 시작해야 합니다.

2. **Endpoint Detection and Response Expert(on-premises) 활성화**

   EDR Expert(on-premise)(Kaspersky Endpoint Detection and Response(on-premises) 애드온) 사용을 위해 별도 라이센스 구매해야 합니다.

   독립 실행형 Endpoint Detection and Response Expert(on-premises) 기능의 라이센스는 Kaspersky Industrial CyberSecurity for Nodes의 라이센스와 같습니다. 이 기능은 Kaspersky Endpoint Detection and Response (on-premises)의 키를 별도로 추가한 후 사용할 수 있습니다. 결과적으로 Kaspersky Industrial CyberSecurity for Nodes 키와 Endpoint Detection and Response Expert(on-premises) 키가 컴퓨터에 추가됩니다.

   라이센스에 Endpoint Detection and Response Expert(on-premises) 기능이 포함되었는지 확인합니다.

3. **원격 측정 수집 서버 및 응답 서버에 연결**

   Kaspersky Endpoint Detection and Response Expert(on-premises)를 사용하려면 Kaspersky Endpoint Security와 두 서버 간의 신뢰할 수 있는 연결이 필요합니다.

   - *원격 측정 수집 서버*는 컴퓨터에서 발생하는 이벤트에 대한 정보를 수집, 정규화, 상관관계 파악, 분석, 저장하는 SIEM 솔루션에 포함된 서버입니다.
   - *응답 서버*는 데이터를 수신 및 검사하고, 개체의 동작을 조사하고, 조사 결과를 게시하기 위한 서버입니다.

신뢰할 수 있는 연결을 구성하려면 TLS 인증서를 사용해야 합니다. Open Single Management Platform에서 TLS 인증서를 받을 수 있습니다(Kaspersky Endpoint Detection and Response Expert (on-premises) 도움말의 지침 참조). 그런 다음 Kaspersky Industrial CyberSecurity for Nodes에 TLS 인증서를 추가해야 합니다(아래 지침 참조).

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 서버의 TLS 인증서만 확인합니다. 보다 안전한 연결을 위해, 서버에서 컴퓨터 확인을 추가로 활성화할 수 있습니다(양방향 인증). 이 확인을 활성화하려면 서버와 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증을 켜야 합니다. 양방향 인증을 사용하려면 암호화 컨테이너도 필요합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Open Single Management Platform에서 암호화 컨테이너를 받을 수 있습니다(Kaspersky Endpoint Detection and Response Expert (on-premises) 도움말의 지침 참조).

웹 콘솔을 사용하여 Kaspersky Industrial CyberSecurity for Nodes 컴퓨터를 EDR Expert(on-premises)에 연결하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **원격 측정 수집 서버** 섹션을 선택합니다.
5. **Endpoint Detection and Response Expert(on-premises)** 블록에서 **구성** 버튼을 클릭합니다.
   Endpoint Detection and Response Expert(on-premises) 창이 열립니다.
6. **Endpoint Detection and Response Expert(on-premises) 사용** 확인란을 선택합니다.
7. **Endpoint Detection and Response Expert(버전 8.0 이상)** 모드를 선택합니다.
8. 원격 측정 수집 서버 연결을 구성합니다.
   a. **원격 측정 수집 서버에 연결** 블록에서 **KATA 서버 연결 설정** 링크를 클릭합니다.
   b. 창이 열리면 원격 측정 수집 서버에 대한 연결을 구성합니다.
      - **시간 초과(초)**. 최대 서버 응답 시간 초과. 제한 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 다른 서버에 연결을 시도합니다.
      - **서버 TLS 인증서**. 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Open Single Management Platform에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Endpoint Detection and Response Expert(on-premises) 도움말의 지침 참조).
      - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 서버 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Open Single Management Platform에서 암호화 컨테이너를 얻을 수 있습니다(Kaspersky Endpoint Detection and Response Expert(on-premises) 도움말의 지침 참조). 서버 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

        암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

   c. **확인** 버튼을 클릭합니다.

d. 원격 측정 수집 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.

여러 개의 원격 측정 수집 서버 주소를 추가할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes가 첫 번째 IP 주소에서 서버와의 연결 설정을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Industrial CyberSecurity for Nodes는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

e. 필요한 경우 원격 측정을 구성합니다.

9. 응답 서버 연결 구성:

a. **응답 서버에 연결** 블록에서 **다음 시간마다 서버로 동기화 요청 보내기(분)** 설정을 구성합니다. 서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Industrial CyberSecurity for Nodes가 보안 위협 대응 작업을 수신하고 작업 결과를 전송합니다.

b. **KATA 서버 연결 설정** 링크를 클릭합니다.

c. 창이 열리면 응답 서버에 대한 연결을 구성합니다.

- **시간 초과(초)**. 최대 서버 응답 시간 초과. 제한 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 다른 서버에 연결을 시도합니다.
- **서버 TLS 인증서**. 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Open Single Management Platform에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Endpoint Detection and Response Expert(on-premises) 도움말의 지침 참조).
- **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 서버 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Open Single Management Platform에서 암호화 컨테이너를 얻을 수 있습니다(Kaspersky Endpoint Detection and Response Expert(on-premises) 도움말의 지침 참조). 서버 설정을 구성한 후 Kaspersky Endpoint Security 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

  암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

d. **확인** 버튼을 클릭합니다.

e. 응답 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.

여러 개의 원격 측정 수집 서버 주소를 추가할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes가 첫 번째 IP 주소에서 서버와의 연결 설정을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Industrial CyberSecurity for Nodes는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

10. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

그러면 컴퓨터가 Open Single Management Platform(OSMP)에 추가됩니다.

EDR Expert(on-premises) 원격 측정 설정 구성

*원격 측정*은 보호된 컴퓨터에서 발생한 이벤트 목록입니다. Kaspersky Industrial CyberSecurity for Nodes는 원격 측정 데이터를 분석하여 동기화하는 동안 원격 측정 수집 서버로 보냅니다. 전송되는 텔레메트리 이벤트에 대한 자세한 내용은 Kaspersky Endpoint Detection and Response Expert(on-premises) 도움말을 참조하십시오.

원격 측정 이벤트는 거의 지속적으로 서버에 도착합니다. Kaspersky Industrial CyberSecurity for Nodes는 다음 조건 중 하나라도 충족되면 서버와의 동기화를 시작합니다.

- 동기화 주기가 되었습니다.
- 버퍼의 이벤트 개수가 상한을 초과합니다.

따라서 기본적으로 애플리케이션은 30초마다, 또는 버퍼에 이벤트가 1024개 있을 때마다 동기화를 합니다. Kaspersky Industrial CyberSecurity for Nodes 정책에서 동기화 동작을 구성하고 네트워크 부하에 맞는 최적의 값을 선택할 수 있습니다(아래 지침 참조).

Kaspersky Industrial CyberSecurity for Nodes와 서버가 서로 연결되어 있지 않으면 애플리케이션이 새 이벤트를 대기시킵니다. 연결이 복원되면 Kaspersky Industrial CyberSecurity for Nodes가 대기열에 있는 이벤트들을 적절한 순서로 서버에 보냅니다. 서버 과부하를 방지하기 위해 Kaspersky Industrial CyberSecurity for Nodes는 일부 이벤트를 건너뛸 수 있습니다. 이를 활성화하기 위해 이벤트 전송 설정을 최적화할 수 있습니다. 예를 들어, 시간당 이벤트 값을 최대로 설정합니다(아래 지침 참조).

원격 측정 설정을 구성하려면 다음 단계를 수행합니다.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **원격 측정 수집 서버** 섹션을 선택합니다.
5. **Endpoint Detection and Response Expert(on-premises)** 블록에서 **구성** 버튼을 클릭합니다.
   Endpoint Detection and Response Expert(on-premises) 창이 열립니다.
6. **데이터 전송 설정** 블록에서 **원격 측정 수집 서버로 원격 측정 전송** 확인란이 선택되었는지 확인합니다.
7. 필요하다면 **IOA만 포함한 원격 측정 전송** 확인란을 선택합니다. *공격 지표(IOA)*는 시스템의 의심스러운 동작에 대한 설명을 포함하는 규칙으로, 표적 공격의 가능성을 표시합니다. 애플리케이션은 시스템에서 진행 중인 동작을 이러한 규칙과 비교하여 표적 공격을 표시하는 이벤트를 로그에 기록합니다. 애플리케이션은 스트리밍 검사 기술을 사용하며, 이를 통해 해당 이벤트를 실시간으로 추적할 수 있습니다.
8. 필요한 경우, **데이터 전송 설정** 블록에서 서버 설정과 동기화를 구성합니다.
   - **최대 이벤트 전송 지연(초)**. 애플리케이션이 서버와 동기화하여 동기화 주기가 만료된 후 이벤트를 보냅니다. 기본 설정은 30초입니다.
   - **트랜잭션의 일부로 전송된 이벤트 패키지의 수 관리**. 버퍼가 이벤트로 가득 차면 애플리케이션이 서버와 동기화를 수행합니다. 기본 설정은 이벤트 1024개입니다.

9. 필요한 경우 **제한** 블록에서 **제한 사용** 체크박스를 선택 해제합니다.

   이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

10. 이벤트를 서버로 전송하기 위한 최적화 설정을 구성합니다.

    - **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

    - **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 기본 설정은 15%입니다.

11. **응답 서버에 연결** 블록에서 **다음 시간마다 서버로 동기화 요청 보내기(분)** 파라미터의 값을 입력합니다.

12. 서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Industrial CyberSecurity for Nodes는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.

13. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

EDR Expert(on-premises) 원격 측정 예외

성능을 개선하고 원격 측정 수집 서버로의 데이터 전송을 최적화하기 위해 원격 측정 예외 규칙을 구성할 수 있습니다. 예를 들어 개별 애플리케이션의 네트워크 통신 데이터를 전송하지 않도록 선택할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 총 최대 10,000개의 EDR Expert (on-premises) 포함 및 예외 이벤트 필터링 규칙을 지원합니다.

저장된 필터링 규칙의 지원 한도를 초과할 경우 EDR Expert(on-premises) 이벤트 필터링 규칙이 정책에서 Kaspersky Industrial CyberSecurity for Nodes 4.5 이하 버전을 실행하는 관리 장치로 전달되지 않습니다. 애플리케이션은 해당 경고를 표시합니다.

웹 콘솔에서 원격 측정 예외를 생성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보충** 섹션으로 갑니다.

5. **원격 측정 설정** 블록에서 **구성** 버튼을 클릭합니다.

6. **EDR Expert(on-premises) 원격 측정** 탭을 선택합니다.

7. **일반 예외** 블록에서 **추가** 버튼을 클릭합니다.
   예외 규칙 추가 창이 열립니다.

8. 필요시 규칙의 상태를 변경합니다. 기본적으로 규칙이 활성화됩니다.

9. 규칙의 이름을 입력합니다.

10. 규칙이 트리거될 때 수행할 작업 선택:

    - **수집하지 않음**. 필터링된 이벤트가 전송되는 원격 측정에서 제외됩니다.
    - **IOA 제외**. IOA 규칙 트리거 이벤트가 전송되는 원격 측정에서 제외됩니다.

11. **IOA 제외** 옵션을 선택한 경우 예외에 추가할 IOA 규칙을 지정합니다.

    - **전체 제외**. 지정된 조건이 충족되면 애플리케이션은 모든 IOA 규칙에 따라 생성된 이벤트를 원격 측정에서 제외합니다.
    - **GUID별 제외**. IOA 규칙의 GUID를 지정합니다. `,`를 사용하여 여러 GUID를 지정할 수 있습니다. IOA 규칙에 대한 자세한 내용은 EDR Expert(on-premises) 도움말을 참조하십시오.

12. 필터링 조건 지정:

    a. 필터링에 사용할 필드 이름을 선택합니다.

    b. 연산자(아래 표 참조)를 선택하고 이벤트의 필드 값을 비교할 값을 지정합니다.

조건 연산자 목록

연산자	설명
<	필드 값이 조건에 지정된 값보다 작으면 이벤트가 필터링되어 제외됩니다.
≤	필드 값이 조건에 지정된 값보다 작거나 같으면 이벤트가 필터링되어 제외됩니다.
=	필드 값이 조건에 지정된 값과 같으면 이벤트가 필터링되어 제외됩니다.
≥	필드 값이 조건에 지정된 값보다 크거나 같으면 이벤트가 필터링되어 제외됩니다.
>	필드 값이 조건에 지정된 값보다 크면 이벤트가 필터링되어 제외됩니다.
≠	필드 값이 조건에 지정된 값과 같지 않으면 이벤트가 필터링되어 제외됩니다.
같음	필드 값이 조건에 지정된 마스크와 일치하면 이벤트가 필터링되어 제외됩니다. 애플리케이션은 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.
같지 않음	필드 값이 조건에 지정된 마스크와 일치하지 않으면 이벤트가 필터링되어 제외됩니다. 애플리케이션은 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.
다음 중 하나	필드 값이 조건에 지정된 목록의 값 중 하나와 일치하면 이벤트가 필터링된 것으로 간주됩니다.
다음 중 해당 없음	필드 값이 조건에 지정된 목록의 어떤 값과도 일치하지 않으면 이벤트가 필터링된 것으로 간주됩니다.
다음 중 하나와 같음	필드 값이 조건에 지정된 마스크 중 하나와 일치하면 이벤트가 필터링되어 제외됩니다. 애플리케이션은 마스크를 입력할 때 * 및 ? 문자를 지원합니다.
다음 중 하나와 같지 않음	필드 값이 조건에 지정된 마스크 중 어느 것과도 일치하지 않으면 이벤트가 필터링되어 제외됩니다. 애플리케이션은 마스크를 입력할 때 * 및 ? 문자를 지원합니다.
존재함	조건에 지정된 필드가 이벤트에 포함되어 있으면 해당 이벤트가 필터링되어 제외됩니다.
존재하지 않음	조건에 지정된 필드가 이벤트에 포함되어 있지 않으면 해당 이벤트가 필터링되어 제외됩니다.
포함	조건에 지정된 값이 필드 값에 포함되어 있으면 해당 이벤트가 필터링되어 제외됩니다.

연산자	설명
다음과 같음	필드 값이 조건에 지정된 값과 같으면 이벤트가 필터링되어 제외됩니다. 이 검사는 대소문자를 구분하지 않습니다.
비트 AND 연산자	필드 값과 조건에 지정된 값 간의 비트 AND(&) 연산 결과가 1이면 이벤트가 필터링되어 제외됩니다.

13. 필요에 따라 여러 필터 조건과 조건 그룹을 추가하여 복합 필터 기준을 생성할 수 있습니다. 조건 그룹에 중첩 조건 및 조건 그룹을 추가할 수도 있습니다. 다음 연산자를 사용할 수 있습니다.

    - **AND**는 필터가 지정된 조건을 모두 충족하는 이벤트를 선택함을 의미합니다.
    - **OR**는 필터가 지정된 조건 중 하나라도 충족하는 이벤트를 선택함을 의미합니다.
    - **NOT**(이 연산자를 사용하려면 **NOT을 앞에 추가** 옵션 선택)는 필터가 지정된 조건 중 어느 것도 충족하지 않는 이벤트를 선택함을 의미합니다.

    조건과 1단계 조건 그룹은 **AND** 연산자를 사용하여 결합됩니다.

14. 컴퓨터에서 Open Single Management Platform(OSMP)을 실행하는 경우 생성한 필터링 규칙을 검사할 수 있습니다. 검사를 실행하려면 **규칙 확인** 버튼을 클릭합니다.

    창이 열리면 생성된 규칙을 사용하여 필터링된 이벤트 표가 표시됩니다. 자세한 내용은 EDR Expert(on-premises) 도움말을 참조하십시오.

15. 필요한 경우 **모든 이벤트 유형**에서 이벤트 유형별로 원격 측정 예외를 추가합니다.

    a. 이벤트 유형 이름을 클릭합니다.

    b. 열리는 창에서 **수동 설정** 버튼을 클릭합니다.

    c. 필요한 경우 **이벤트 전송** 토글 스위치를 사용하여 선택한 이벤트 유형에 대한 원격 측정 전송을 구성합니다. 기본적으로 원격 측정 전송은 모든 이벤트 유형에 대해 활성화됩니다.

    d. **예외 규칙** 블록에서 **추가** 버튼을 클릭합니다.
    예외 규칙 추가 창이 열립니다.

    e. 추가하는 각 규칙에 대해 7~13단계에 설명된 작업을 수행합니다.

16. 일부 이벤트 유형의 경우 포함 규칙을 추가하여 수집되는 원격 측정을 확장할 수도 있습니다.

    a. **예외 규칙** 블록에서 **추가** 버튼을 클릭합니다.
    포함 규칙 추가 창이 열립니다.

    b. 규칙의 이름을 입력합니다.

    c. **조건**에서 표시된 필드에 값을 입력합니다. 사용 가능한 필드 유형은 선택한 이벤트에 따라 다릅니다.

> 제외 규칙은 포함 규칙보다 우선합니다.

17. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

EDR Expert(on-premises) 이벤트 필터 내보내기 및 가져오기

Kaspersky Industrial CyberSecurity for Nodes는 총 최대 10,000개의 EDR Expert (on-premises) 포함 및 예외 이벤트 필터링 규칙을 지원합니다.

저장된 필터링 규칙의 지원 한도를 초과할 경우 EDR Expert(on-premises) 이벤트 필터링 규칙이 정책에서 Kaspersky Industrial CyberSecurity for Nodes 4.5 이하 버전을 실행하는 관리 장치로 전달되지 않습니다. 애플리케이션은 해당 경고를 표시합니다.

예외 규칙 목록을 JSON 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 이벤트 ID를 여러 개 추가할 수 있습니다. 내보내기 및 가져오기 기능을 사용하여 이벤트 필터를 백업하거나 목록을 다른 서버로 마이그레이션할 수도 있습니다.

Kaspersky Security Center 관리 콘솔에서 이벤트 필터를 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **보충** 섹션으로 갑니다.
4. **EDR Expert(on-premises) 원격 측정 설정** 블록에서 **설정** 버튼을 클릭합니다.
5. EDR Expert (on-premises) 원격 측정 설정을 내보내려면 다음과 같이 진행합니다.
   a. **내보내기** 버튼을 클릭합니다.
   b. 창이 열리면 설정을 내보낼 JSON 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   c. 파일을 저장합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 설정을 JSON 파일로 내보냅니다.
6. 원격 측정 설정을 가져오려면 다음과 같이 진행합니다:
   a. **가져오기** 버튼을 클릭합니다.
   b. 이벤트 필터를 가져올 JSON 파일을 선택합니다.
   c. 파일을 엽니다.
   d. 표시되는 대화 상자에서 EDR Expert (on-premises) 원격 측정 설정의 수정 사항을 확인합니다.
7. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

웹 콘솔에서 이벤트 필터를 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보충** 섹션으로 갑니다.
5. **원격 측정 설정** 블록에서 **구성** 버튼을 클릭합니다.
6. **EDR Expert(on-premises) 원격 측정** 탭을 선택합니다.
7. EDR Expert (on-premises) 원격 측정 설정을 내보내려면 **내보내기**을 클릭합니다.
   Kaspersky Industrial CyberSecurity for Nodes는 표준 다운로드 폴더에 filterExport.json이라는 파일을 저장합니다.
8. 원격 측정 설정을 가져오려면 다음과 같이 진행합니다:
   a. **가져오기** 버튼을 클릭합니다.
   b. 이벤트 필터를 가져올 JSON 파일을 선택합니다.
   c. 파일을 엽니다.
   d. 이벤트 필터링 규칙을 가져올 방법을 선택합니다. 기존 규칙에 추가할 수도 있고 기존 규칙을 폐기하고 새 규칙으로 교체할 수도 있습니다.
   e. 변경 사항을 저장합니다.
      JSON 파일에 포함된 규칙이 목록에 표시됩니다.

애플리케이션 콘솔에서 이벤트 필터를 내보내고 가져오는 방법

1. 애플리케이션 콘솔 트리에서 **원격 측정 설정** 노드를 선택합니다.
2. **EDR Expert(on-premises) 원격 측정 설정** 블록에서 **설정** 버튼을 클릭합니다.
3. EDR Expert (on-premises) 원격 측정 설정을 내보내려면 다음과 같이 진행합니다.
   a. **내보내기** 버튼을 클릭합니다.
   b. 창이 열리면 설정을 내보낼 JSON 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   c. 파일을 저장합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 설정을 JSON 파일로 내보냅니다.
4. 원격 측정 설정을 가져오려면 다음과 같이 진행합니다:
   a. **가져오기** 버튼을 클릭합니다.
   b. 이벤트 필터를 가져올 JSON 파일을 선택합니다.

c. 파일을 엽니다.

d. 표시되는 대화 상자에서 EDR Expert (on-premises) 원격 측정 설정의 수정 사항을 확인합니다.

5. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

명령줄에서 이벤트 필터 내보내기 또는 가져오기를 수행할 수도 있습니다.

YARA 검사

*YARA 검사*는 Kaspersky Industrial CyberSecurity for Nodes가 YARA 파일을 사용하여 장치에서 악성 활동의 시그니처를 찾는 프로세스입니다. 이 검사는 로컬 디스크에서 반복 수행됩니다. 네트워크, 이동식 드라이브, 클라우드 리소스 검사는 지원하지 않습니다.

YARA 검사를 실행하려면 EDR Expert(온프레미스)의 유효한 라이선스가 필요합니다.

*YARA 파일*은 YARA 규칙을 포함하는 .YARA 또는 .YAR 확장자의 파일입니다. *YARA 규칙*은 표적형 공격의 서명과 기업 IT 인프라에 대한 침입을설명합니다. Kaspersky Industrial CyberSecurity for Nodes는 이러한 규칙을 사용하여 개체를 검사합니다. 개체가 규칙과 일치하면 분석기는 감염을 진단하고 로그에 세부 정보를 기록합니다.

YARA 파일 사용과 관련된 다음 요구 사항 및 제한 사항을 고려해야 합니다.

- Kaspersky Industrial CyberSecurity for Nodes는 침해지표 설명을 위한 YARA 4.2.3 공개 표준을 따르는 .YARA 또는 .YAR 확장자의 YARA 파일을 지원합니다.
- Kaspersky Industrial CyberSecurity for Nodes에서 지원하지 않거나 구문 오류가 포함된 YARA 파일로 YARA 검사를 실행하면, 검사가 중단되고 해당 오류 알림이 표시됩니다.
- YARA 검사 작업에 사용된 모든 YARA 파일의 ID는 고유해야 합니다. 식별자가 같은 YARA 파일이 있다면 작업 실행 결과에 영향을 미칠 수 있습니다.
- YARA 검사는 YARA 규칙에 설명된 지표와 128개가 일치 시 중단됩니다. 이는 YARA 검사 리포트의 항목 수를 제한하여 분석을 더 쉽게 하고, 정확하지 않게 공식화된 YARA 규칙으로 대량의 일치 항목이 생성되어 리포트가 오버플로되는 것을 방지하기 위함입니다.

YARA 파일당 규칙 하나를 생성하는 것이 좋습니다. 이 접근 방식은 YARA 검사 결과의 가독성을 높입니다.

YARA 검사는 명령줄 인터페이스를 통해서만 실행할 수 있습니다.

YARA 검사는 오래 걸릴 수 있습니다. 드라이브 크기, 작업 설정 및 디스크에 있는 개체 수에 따라 YARA 검사는 몇 분에서 몇 시간까지 걸릴 수 있습니다. 애플리케이션은 진행률 표시기를 표시하지 않습니다. YARA 검사를 중지하거나 취소할 수 없습니다. YARA 검사 결과가 나올 때까지 기다리는 것이 좋습니다.

명령이 완료되었고(반환 값 `0`) 도중에 침해지표가 감지되면, Kaspersky Industrial CyberSecurity for Nodes가 명령줄에 다음 작업 결과 정보를 출력합니다:

`Started at <time>` `Finished at <time>`	검사 시작 시간과 완료 시간입니다.
`Host name: <computer name>`	해당 개체가 탐지된 컴퓨터의 이름입니다.

`Result: <error>`	작업을 실행하는 동안 발생한 오류의 오류 코드입니다. 오류가 없으면 애플리케이션이 `0x00000000`을 출력합니다.
`Comment: <comment text>`	작업을 실행하는 동안 발생한 오류의 오류 설명입니다. 예: `Operation timeout`.
`Object Name:` 또는 `Process:`(프로세스 메모리를 검사하는 경우)	YARA 규칙이 트리거된 개체 또는 프로세스의 이름입니다.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	YARA 규칙이 트리거된 개체의 해시입니다.
`Rule Name`	트리거된 YARA 규칙의 이름입니다.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	YARA 규칙에 지정된 메타데이터.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	YARA 규칙 조건을 충족하는 개체 내에서 일치하는 항목을 찾았습니다.
	• 일치가 탐지된 프로세스 메모리 또는 파일의 오프셋(`Offset`).
	• YARA 규칙에서 일치하는 문자열의 이름(`String name`).
	• 프로세스 메모리 또는 파일에서 일치하는 문자열(`String data`).

EDR 원격 측정 예외 규칙

성능을 개선하고 원격 측정 수집 서버로의 데이터 전송을 최적화하기 위해 원격 측정 예외 규칙을 구성할 수 있습니다. 예를 들어 개별 애플리케이션의 네트워크 통신 데이터를 전송하지 않도록 선택할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 EDR 원격 측정 예외 생성

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보충 → KATA 통합 / KICS for Networks 통합 원격 측정 설정** 옵션을 선택하고 **설정** 버튼을 클릭합니다.
4. 창이 열리면 원격 측정 예외 규칙을 구성합니다(아래 표 참조).
5. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 EDR 원격 측정 예외 생성

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보충 → KATA 통합 / KICS for Networks 통합 원격 측정 설정** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. 창이 열리면 원격 측정 예외 규칙을 구성합니다(아래 표 참조).
6. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 EDR 원격 측정 예외 생성

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 선택하고, 노드의 마우스 오른쪽 메뉴에서 **KATA 통합 / KICS for Networks 통합 원격 측정 설정** 옵션을 선택합니다.

2. 창이 열리면 원격 측정 예외 규칙을 구성합니다(아래 표 참조).

3. 변경 사항을 저장합니다.

파라미터	설명
제외된 프로세스	**전송할 원격 측정 크기 최적화**. Kaspersky Industrial CyberSecurity for Nodes를 사용하면 전송된 데이터의 양을 최적화하고 원격 측정에서 특정 코드(Microsoft SMB 프로토콜, WinRM 서비스, 네트워크 에이전트의 klnagent.exe 프로세스, 모든 유형의 네트워크 프로토콜의 네트워크 패킷 유형에 대한 확장 정보에 대한 코드 102(기본 통신) 및 8(프로세스의 네트워크 활동))가 있는 이벤트를 제외할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스 상세 정보** 및 **부모 프로세스 상세 정보**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다. • **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다. • **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다. • **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다. • **파일 체크섬**. MD5 및 SHA256. 파일을 직접 선택할 수도 있으며, 그러면 애플리케이션이 선택한 파일의 필드를 자동으로 채웁니다. 64비트 운영 체제에서는 애플리케이션이 실행 파일 파라미터 필드를 `C:\windows\syswow64` 폴더에 있는 동일한 실행 파일의 32비트 버전 속성의 데이터로 채우기 때문에 `C:\windows\system32` 폴더에서 프로세스 실행 파일의 64비트 버전 파라미터를 수동으로 입력해야 합니다. 예를 들어 `C:\windows\system32\cmd.exe`를 선택하면 플러그인이 `C:\windows\syswow64\cmd.exe`의 파라미터를 표시합니다. 이러한 동작은 운영 체제의 특성에 따라 달라집니다. **다음 이벤트 유형에 사용**: • **파일 수정**. • **네트워크 이벤트**. • **프로세스: 콘솔 대화형 입력**. • **모듈 로드됨**. • **레지스트리 수정됨**. • **DNS 로그**. • **프로세스 접근**. • **코드 삽입**. • **WMI 쿼리**. • **파이프**. • **LDAP**. • **AMSI**.
제외된 네트워크 통신	• **규칙 이름**. 규칙 이름입니다. • **방향**. 수신 또는 발신 이벤트입니다. • **프로토콜**. 프로토콜 유형입니다. • **원시 소켓**. 원시 소켓 사용 여부입니다. • **프로토콜 번호**. 프로토콜 번호입니다. • **TLS 인증서**. TLS 프로토콜을 사용하여 클라이언트와 서버 간의 연결을 암호화하는 데 사용되는 디지털 인증서입니다. • **로컬 포트 또는 범위**. 특정 포트 또는 가능한 로컬 포트의 범위입니다. • **원격 포트 또는 범위**. 특정 포트 또는 가능한 원격 포트의 범위입니다. • **로컬 주소**. Kaspersky Industrial CyberSecurity for Nodes가 네트워크 트래픽에서 원격 측정을 제외하는 컴퓨터의 네트워크 주소입니다. • **원격 주소**. Kaspersky Industrial CyberSecurity for Nodes가 네트워크 트래픽에서 원격 측정을 제외하는 컴퓨터의 네트워크 주소입니다. IP 주소에 대해 IPv4 형식만 지원합니다. • **애플리케이션**. Kaspersky Industrial CyberSecurity for Nodes가 네트워크 트래픽에서 EDR 원격 측정을 제외하는 애플리케이션의 실행 파일 목록입니다.
제외된 파일 동작	• **규칙 이름**. 규칙 이름입니다. • **파일 이름 또는 마스크**. 파일 또는 폴더의 이름이나 마스크; Kaspersky Industrial CyberSecurity for Nodes는 이 파일 또는 폴더에 접근할 때 예외를 적용합니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다: • **작업 유형**. 파일 동작 유형(예: 파일 생성 또는 파일 속성 편집)입니다. • **이전 경로**. 파일의 이전 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스 상세 정보** 및 **부모 프로세스 상세 정보**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다.

파라미터	설명
	• **부모 경로**. 파일이 있는 폴더 경로입니다. • **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다. • **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다. • **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다. • **파일 체크섬**. MD5 및 SHA256. 파일을 직접 선택할 수도 있으며, 그러면 애플리케이션이 선택한 파일의 필드를 자동으로 채웁니다. 64비트 운영 체제에서는 애플리케이션이 실행 파일 파라미터 필드를 `C:\windows\syswow64` 폴더에 있는 동일한 실행 파일의 32비트 버전 속성의 데이터로 채우기 때문에 `C:\windows\system32` 폴더에서 프로세스 실행 파일의 64비트 버전 파라미터를 수동으로 입력해야 합니다. 예를 들어 `C:\windows\system32\cmd.exe`를 선택하면 플러그인이 `C:\windows\syswow64\cmd.exe`의 파라미터를 표시합니다. 이러한 동작은 운영 체제의 특성에 따라 달라집니다.
제외된 DNS 작업	• **규칙 이름**. 규칙 이름입니다. Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스 상세 정보** 및 **부모 프로세스 상세 정보**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다. • **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다. • **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다. • **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다. • **파일 체크섬**. MD5 및 SHA256. 파일을 직접 선택할 수도 있으며, 그러면 애플리케이션이 선택한 파일의 필드를 자동으로 채웁니다. 64비트 운영 체제에서는 애플리케이션이 실행 파일 파라미터 필드를 `C:\windows\syswow64` 폴더에 있는 동일한 실행 파일의 32비트 버전 속성의 데이터로 채우기 때문에 `C:\windows\system32` 폴더에서 프로세스 실행 파일의 64비트 버전 파라미터를 수동으로 입력해야 합니다. 예를 들어 `C:\windows\system32\cmd.exe`를 선택하면 플러그인이 `C:\windows\syswow64\cmd.exe`의 파라미터를 표시합니다. 이러한 동작은 운영 체제의 특성에 따라 달라집니다. DNS: • **DNS 서버 IP 주소**. DNS 쿼리를 처리하는 서버의 주소입니다. • **쿼리 옵션**. DNS 쿼리의 형식과 조건을 규제하는 파라미터입니다. • **상태**. DNS 작업의 현재 상태입니다. • **도메인 이름**. 쿼리가 처리되는 도메인 이름입니다. • **설정 유형 ID**. DNS 설정 유형의 고유 ID입니다. • **응답 데이터**. DNS 쿼리에 대한 응답으로 서버에서 반환한 데이터입니다.
제외된 LDAP 작업	• **규칙 이름**. 규칙 이름입니다. • **LDAP 검색 범위**. LDAP 검색이 수행되는 범위입니다. • **필터**. LDAP 개체 필터링을 위한 검색 기준입니다. • **LDAP 개체 검색을 위한 고유 이름**. LDAP 검색에 대한 개체의 고유 이름입니다. • **개체 속성**. LDAP 쿼리에서 추출할 개체의 속성입니다. Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스 상세 정보** 및 **부모 프로세스 상세 정보**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다. • **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다. • **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다. • **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다. • **파일 체크섬**. MD5 및 SHA256. 파일을 직접 선택할 수도 있으며, 그러면 애플리케이션이 선택한 파일의 필드를 자동으로 채웁니다. 64비트 운영 체제에서는 애플리케이션이 실행 파일 파라미터 필드를 `C:\windows\syswow64` 폴더에 있는 동일한 실행 파일의 32비트 버전 속성의 데이터로 채우기 때문에 `C:\windows\system32` 폴더에서 프로세스 실행 파일의 64비트 버전 파라미터를 수동으로 입력해야 합니다. 예를 들어 `C:\windows\system32\cmd.exe`를 선택하면 플러그인이 `C:\windows\syswow64\cmd.exe`의 파라미터를 표시합니다. 이러한 동작은 운영 체제의 특성에 따라 달라집니다.

파라미터	설명
제외된 프로세스 접근 쿼리	**규칙 이름**. 규칙 이름입니다. **작업 유형**. 프로세스 접근 작업의 유형입니다(예: "모두" 또는 "열림"). **프로세스에 대한 접근 권한 요청**. 프로세스에 대한 접근 수준입니다. **호출 스택 추적**. 프로세스 접근과 관련된 함수 호출의 순서에 대한 정보입니다. Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스 상세 정보**, **부모 프로세스 상세 정보**, **대상 프로세스의 파일**, **소스 프로세스에 대한 핸들**, **대상 프로세스에 대한 핸들**. • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다. • **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다. • **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다. • **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다. • **파일 체크섬**. MD5 및 SHA256. 파일을 직접 선택할 수도 있으며, 그러면 애플리케이션이 선택한 파일의 필드를 자동으로 채웁니다. 64비트 운영 체제에서는 애플리케이션이 실행 파일 파라미터 필드를 `C:\windows\syswow64` 폴더에 있는 동일한 실행 파일의 32비트 버전 속성의 데이터로 채우기 때문에 `C:\windows\system32` 폴더에서 프로세스 실행 파일의 64비트 버전 파라미터를 수동으로 입력해야 합니다. 예를 들어 `C:\windows\system32\cmd.exe`를 선택하면 플러그인이 `C:\windows\syswow64\cmd.exe`의 파라미터를 표시합니다. 이러한 동작은 운영 체제의 특성에 따라 달라집니다.
제외된 코드 삽입	• **규칙 이름**. 규칙 이름입니다. • **접근 방법**. 코드 삽입에 사용된 접근 방법입니다. • **호출 스택**. 코드 삽입과 관련된 함수 호출 순서입니다. • **수정된 명령줄**. 삽입으로 수정된 명령줄입니다. • **삽입 주소**. 삽입이 발생한 메모리 위치입니다. • **삽입된 DLL 이름**. 삽입에 사용된 DLL(동적 링크 라이브러리)의 이름입니다. Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스 상세 정보** 및 **부모 프로세스 상세 정보**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다. • **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다. • **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다. • **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다. • **파일 체크섬**. MD5 및 SHA256. 파일을 직접 선택할 수도 있으며, 그러면 애플리케이션이 선택한 파일의 필드를 자동으로 채웁니다. 64비트 운영 체제에서는 애플리케이션이 실행 파일 파라미터 필드를 `C:\windows\syswow64` 폴더에 있는 동일한 실행 파일의 32비트 버전 속성의 데이터로 채우기 때문에 `C:\windows\system32` 폴더에서 프로세스 실행 파일의 64비트 버전 파라미터를 수동으로 입력해야 합니다. 예를 들어 `C:\windows\system32\cmd.exe`를 선택하면 플러그인이 `C:\windows\syswow64\cmd.exe`의 파라미터를 표시합니다. 이러한 동작은 운영 체제의 특성에 따라 달라집니다.
제외된 WMI 쿼리	• **규칙 이름**. 규칙 이름입니다. • **WMI 작업 유형**. WMI를 사용하여 수행하는 작업 유형입니다. • **원격 쿼리**. WMI 쿼리의 원격 실행 여부 정보입니다. • **WMI 명령을 실행한 컴퓨터의 이름**. 쿼리를 시작한 컴퓨터 이름입니다. • **WMI 사용자 계정**. WMI 쿼리에 사용된 사용자 계정입니다. • **실행된 WMI 명령**. WMI를 통해 실행된 특정 명령입니다. • **WMI 네임스페이스**. WMI 작업이 수행된 네임스페이스입니다. • **WMI 이벤트 소비자 필터**. WMI에서 이벤트 처리에 사용하는 필터입니다. • **생성된 WMI 이벤트 소비자의 이름**. WMI를 사용하여 만든 이벤트 소비자의 이름입니다. • **WMI 이벤트 소비자의 소스 코드**. WMI 이벤트 소비자를 만드는 데 사용되는 코드입니다. Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스 상세 정보** 및 **부모 프로세스 상세 정보:** • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다.

파라미터	설명
	• **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다. • **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다. • **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다. • **파일 체크섬**. MD5 및 SHA256. 파일을 직접 선택할 수도 있으며, 그러면 애플리케이션이 선택한 파일의 필드를 자동으로 채웁니다. 64비트 운영 체제에서는 애플리케이션이 실행 파일 파라미터 필드를 `C:\windows\syswow64` 폴더에 있는 동일한 실행 파일의 32비트 버전 속성의 데이터로 채우기 때문에 `C:\windows\system32` 폴더에서 프로세스 실행 파일의 64비트 버전 파라미터를 수동으로 입력해야 합니다. 예를 들어 `C:\windows\system32\cmd.exe`를 선택하면 플러그인이 `C:\windows\syswow64\cmd.exe`의 파라미터를 표시합니다. 이러한 동작은 운영 체제의 특성에 따라 달라집니다.
제외된 파이프 작업	• **규칙 이름**. 규칙 이름입니다. • **파이프 이름**. 파이프의 이름입니다. • **작업 유형**. 파이프가 있는 작업 유형입니다(예: 생성 또는 연결). Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스 상세 정보** 및 **부모 프로세스 상세 정보**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다. • **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다. • **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다. • **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다. • **파일 체크섬**. MD5 및 SHA256. 파일을 직접 선택할 수도 있으며, 그러면 애플리케이션이 선택한 파일의 필드를 자동으로 채웁니다. 64비트 운영 체제에서는 애플리케이션이 실행 파일 파라미터 필드를 `C:\windows\syswow64` 폴더에 있는 동일한 실행 파일의 32비트 버전 속성의 데이터로 채우기 때문에 `C:\windows\system32` 폴더에서 프로세스 실행 파일의 64비트 버전 파라미터를 수동으로 입력해야 합니다. 예를 들어 `C:\windows\system32\cmd.exe`를 선택하면 플러그인이 `C:\windows\syswow64\cmd.exe`의 파라미터를 표시합니다. 이러한 동작은 운영 체제의 특성에 따라 달라집니다.
제외된 레지스트리 변경	• **규칙 이름**. 규칙 이름입니다. • **작업 유형**. 레지스트리에서 수행되는 작업 유형입니다(예: 추가, 삭제, 수정). • **경로**. 변경이 발생한 레지스트리 키의 경로입니다. • **값 이름**. 수정된 레지스트리 값의 이름입니다. • **값**. 새롭거나 수정된 레지스트리 값입니다. • **레지스트리 파일의 전체 이름**. 수정된 레지스트리 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스 상세 정보** 및 **부모 프로세스 상세 정보**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Industrial CyberSecurity for Nodes는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다: • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다. • **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다. • **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다. • **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다. • **파일 체크섬**. MD5 및 SHA256. 파일을 직접 선택할 수도 있으며, 그러면 애플리케이션이 선택한 파일의 필드를 자동으로 채웁니다. 64비트 운영 체제에서는 애플리케이션이 실행 파일 파라미터 필드를 `C:\windows\syswow64` 폴더에 있는 동일한 실행 파일의 32비트 버전 속성의 데이터로 채우기 때문에 `C:\windows\system32` 폴더에서 프로세스 실행 파일의 64비트 버전 파라미터를 수동으로 입력해야 합니다. 예를 들어 `C:\windows\system32\cmd.exe`를 선택하면 플러그인이 `C:\windows\syswow64\cmd.exe`의 파라미터를 표시합니다. 이러한 동작은 운영 체제의 특성에 따라 달라집니다.
장치 사용 시 제외되는 동작	• **규칙 이름**. 규칙 이름입니다. • **장치 유형**. 장치 유형: 로컬 프린터, 이동식 드라이브, CD/DVD 드라이브 등. 자세한 내용은 장치 접근 규칙을 참조하십시오.

파라미터	설명
	• **장치 ID**. 장치의 특정 인스턴스 식별에 사용하는 고유 ID입니다. • **장치 이름**. 장치의 이름입니다. Kaspersky Industrial CyberSecurity for Nodes는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다.

Kaspersky Industrial CyberSecurity for Networks 통합

Kaspersky Industrial CyberSecurity for Networks는 정보 보안 위협으로부터 기업의 인프라를 보호하고 기술 프로세스의 연속성을 보장하도록 설계되었습니다. Kaspersky Industrial CyberSecurity for Networks는 산업 네트워크 트래픽을 분석하여 기술 파라미터 값의 편차를 탐지하고, 네트워크 공격의 징후를 탐지하며, 네트워크의 장치의 작동 및 현재 상태를 모니터링합니다. 이 애플리케이션은 Kaspersky Industrial CyberSecurity 솔루션의 일부입니다. Kaspersky Industrial CyberSecurity for Networks에 대한 전체 정보는 Kaspersky Industrial CyberSecurity for Networks 도움말을 참조하십시오.

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Industrial CyberSecurity for Networks와의 통합을 지원합니다. Kaspersky Industrial CyberSecurity for Nodes에서 받은 장치 이벤트에 대한 데이터는 Kaspersky Industrial CyberSecurity for Networks 서버로 전송됩니다. 애플리케이션 간의 통합을 통해 Kaspersky Industrial CyberSecurity for Networks 기능이 향상되어 산업 네트워크의 위협을 조사하고 대응할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes와의 통합을 위한 Kaspersky Industrial CyberSecurity for Networks for Nodes 구성

다음 구성이 가능합니다.

- **[KICS+내장 에이전트]**. 이 구성에서 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터 보안을 책임지는 애플리케이션이자 Kaspersky Industrial CyberSecurity for Networks와의 작업을 위한 애플리케이션 역할을 합니다. 이 내장 에이전트는 Kaspersky Industrial CyberSecurity for Nodes 4.5 버전부터 사용할 수 있습니다.
- **[타사 EPP+Endpoint Agent 모드의 KICS]**. 이 구성에서는 타사 EPP(Endpoint Protection Platform)를 통해 컴퓨터 보안이 제공됩니다. Kaspersky Industrial CyberSecurity for Nodes는 Endpoint Agent 모드에서 Kaspersky Industrial CyberSecurity for Networks와 통합할 수 있습니다. Endpoint Agent 모드는 Kaspersky Industrial CyberSecurity for Nodes 4.5 버전부터 사용할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 내장 에이전트와 Kaspersky Industrial CyberSecurity for Networks 통합하려면 다음 조건을 충족해야 합니다:

- Kaspersky Industrial CyberSecurity for Networks가 배포되었습니다.
- Kaspersky Security Center 버전 14.2 이상이 배포되었습니다.
- 다음 보호 구성 요소가 활성화되어 작동합니다: 익스플로잇 방지, 복원 엔진, Anti-Cryptor.

Endpoint Agent 구성을 Kaspersky Industrial CyberSecurity for Networks와 통합하려면 다음을 배포해야 합니다:

- Kaspersky Industrial CyberSecurity for Networks.
- Kaspersky Security Center 버전 14.2 이상.

이전 버전의 Kaspersky Industrial CyberSecurity for Nodes 지원

Kaspersky Industrial CyberSecurity for Nodes 4.5는 내장 에이전트 또는 Endpoint Agent 모드를 사용하여 Kaspersky Industrial CyberSecurity for Networks와의 통합을 지원합니다. Kaspersky Endpoint Agent를 설치할 필요가 없습니다.

Kaspersky Industrial CyberSecurity for Networks와의 통합을 위해 4.5 이전 버전의 Kaspersky Industrial CyberSecurity for Nodes를 사용한다면 Kaspersky Endpoint Agent를 별도로 설치해야 합니다.

Kaspersky Industrial CyberSecurity for Networks와의 통합 구성

Kaspersky Industrial CyberSecurity for Networks와의 통합은 다음 단계를 포함합니다.

1. **Kaspersky Industrial CyberSecurity for Networks 통합 구성 요소 설치**

   설치 패키지 설정이나 설치 마법사에서, 또는 Windows 제어판의 애플리케이션 구성 요소 집합 변경을 통해, 설치할 애플리케이션 구성 요소 선택 단계에서 다음을 선택합니다:

   - **전체 기능** → **Endpoint Agent** → 내장 에이전트를 위한 **KICS for Networks와 통합**
   - **Endpoint Agent** → Endpoint Agent 모드용 **KICS for Networks와 통합**

   > 애플리케이션 구성 요소 집합 변경을 완료하려면 컴퓨터를 다시 시작해야 합니다.

2. **Kaspersky Industrial CyberSecurity for Networks 통합 구성 요소 활성화**

   라이센스가 Kaspersky Industrial CyberSecurity for Networks 통합 기능 활성화에 적용되는지 확인.

3. **Kaspersky Industrial CyberSecurity for Networks 통합 구성 요소 활성화 및 구성**

   Kaspersky Industrial CyberSecurity for Nodes는 KICS for Networks 서버로 텔레메트리를 전송하기 위해 TCP 및 UDP 프로토콜을 지원합니다. 연결할 KICS for Networks 통합 서버의 설정에 따라 해당 프로토콜을 선택하고 연결 설정을 지정해야 합니다. 통합 서버 설정에 대한 상세 정보는 KICS for Networks 도움말을 참조하십시오.

   애플리케이션은 데이터 다이오드가 있는 네트워크에서도 KICS for Networks와의 통합을 지원합니다. 데이터 다이오드는 보호 중인 네트워크 세그먼트와 외부 장치 간의 통신을 위한 단방향 게이트웨이입니다. 애플리케이션이 데이터 다이오드를 통해 텔레메트리를 전송할 때 사용할 수 있는 프로토콜:

   - MQTT
   - UDP

   데이터 다이오드를 통해 KICS for Networks로 텔레메트리를 전송하는 방법에 대한 자세한 내용은 KICS for Networks 도움말을 참조하십시오.

   Kaspersky Industrial CyberSecurity for Nodes는 소프트웨어 MQTT 서버(예: Mosquitto)를 MQTT 브로커로 지원합니다. 애플리케이션을 구독자 모드와 게시자 모드 모두에서 사용할 수 있습니다. MQTT 게시자 모드로 작동하는 애플리케이션은 데이터 다이오드를 통해 MQTT 브로커로 텔레메트리를 전송합니다.

   > MQTT 중개 서버로 전송된 원격 측정에는 기밀 정보가 포함될 수 있습니다. 데이터 접근을 제어하려면 원격 측정 보안을 보장하도록 조처해야 합니다.

Kaspersky Security Center 관리 콘솔에서 Kaspersky Industrial CyberSecurity for Networks와의 통합을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **원격 측정 수집 서버** 섹션을 선택합니다.
4. **KICS for Networks와 통합** 블록에서 **설정** 버튼을 클릭합니다.
   KICS for Networks와 통합 창이 열립니다.
5. **KICS for Networks와 통합** 확인란을 선택합니다.
6. **일반** 탭에서 원격 측정 모드를 선택합니다:
   - **TCP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송**. Kaspersky Industrial CyberSecurity for Nodes는 TCP 프로토콜을 통해 Kaspersky Industrial CyberSecurity for Networks 서버로 텔레메트리를 직접 전송합니다.
   - **원격 측정을 데이터 다이오드로 MQTT 게시자로 전송**. Kaspersky Industrial CyberSecurity for Nodes가 원격 측정을 소프트웨어 데이터 다이오드에 내장된 MQTT 중개 서버로 전송합니다.
   - **UDP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송**. Kaspersky Industrial CyberSecurity for Nodes는 UDP 프로토콜을 사용하여 데이터 다이오드를 통해 Kaspersky Industrial CyberSecurity for Networks 서버로 텔레메트리를 전송합니다.
7. **TCP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송** 모드에서 관리할 설정:
   - **주소** 및 **포트**. 원격 측정을 전송할 Kaspersky Industrial CyberSecurity for Networks 서버의 IP 주소 및 포트. 가능한 포트 값 범위: 1~65535. 기본 포트는 8081입니다.
   - **요청 간격(분)**. Kaspersky Industrial CyberSecurity for Networks 서버에 요청을 보내는 간격(분)입니다. Kaspersky Industrial CyberSecurity for Nodes가 MQTT 게시자로 작동할 때 브로커와의 연결이 끊어지면 이 설정에 따라 MQTT 브로커에 대한 요청 간격이 설정됩니다. 사용 가능한 값 범위는 1–60분입니다. 기본값은 1분입니다.
   - **서버 연결 설정**. 다음 설정을 관리합니다:
     - **시간 초과(초)**. 최대 서버 응답 시간 초과. 시간 초과 시 Kaspersky Industrial CyberSecurity for Nodes가 서버에 다시 연결합니다. 사용 가능한 값 범위: 1~60000초. 기본값은 10초입니다.
     - **서버 TLS 인증서**. Kaspersky Industrial CyberSecurity for Networks 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Industrial CyberSecurity for Networks 관리 인터페이스를 사용하여 TLS 인증서를 얻을 수 있습니다.
     - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Kaspersky Industrial CyberSecurity for Networks 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Industrial CyberSecurity for Networks 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

       암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

8. **원격 측정을 데이터 다이오드로 MQTT 게시자로 전송** 모드에서 관리할 설정:

   a. **서버 연결 설정** 버튼을 클릭합니다.

   b. MQTT 중개 서버에서 인증을 위한 자격 증명을 입력합니다.

   c. MQTT 중개 서버의 IP 주소와 포트를 입력합니다.

9. **UDP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송** 모드에서 관리할 설정:

   a. 서버의 IP 주소와 포트를 입력합니다.

   b. 데이터 암호화를 사용하려면 **서버 연결 설정** 버튼을 클릭하고 **UDP 프로토콜을 통해 데이터를 전송할 때 암호화 사용** 체크박스를 선택합니다.

   > 전송되는 데이터의 암호화가 필요한지 평가해야 합니다.

   c. 암호화 키 암호를 입력하고 확장자가 .PEM인 암호화 키 파일을 업로드합니다.

10. **데이터 전송** 탭으로 갑니다.

11. 데이터 전송 설정:

- **최대 이벤트 전송 지연(초)**. 애플리케이션이 서버와 동기화하여 지정한 시간 후 이벤트를 보냅니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.

  > Kaspersky Industrial CyberSecurity for Nodes를 MQTT 구독자로 사용하는 경우 MQTT 게시자의 설정에서 최소 **최대 이벤트 전송 지연(초)** 값인 1초를 지정했다면 MQTT 게시자로 구성된 Kaspersky Industrial CyberSecurity for Nodes 장치 250대 이상에서 원격 측정을 수신하도록 구성하지 않는 것이 좋습니다. 설정값이 30초 이상인 경우 MQTT 게시자 1,000개 이상에서 데이터를 수신하도록 구성하지 않는 것이 좋습니다.

- **요청 제한 사용**. 이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다.

- **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 사용 가능한 값 범위는 10–65535입니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

- **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 사용 가능한 값 범위: 5~100%. 기본값은 15%입니다

필요하다면 무차별 모드에서 원격 측정 구성. 기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터의 네트워크 인터페이스에 도착하고 애플리케이션이 설치된 컴퓨터로 주소가 지정되는 네트워크 트래픽을 수집합니다. 무차별 모드에서 애플리케이션은 사용 가능한 모든 서브넷에서 컴퓨터의 네트워크 인터페이스에 대한 네트워크 트래픽을 수집합니다. 애플리케이션은 수집된 트래픽을 사용하여 확장 원격 측정을 생성합니다.

모든 네트워크 어댑터가 무차별 모드(Promiscuous mode)를 지원하지는 않습니다. 이러한 네트워크 어댑터에서는 확장 원격 측정 수집이 작동하지 않습니다.

a. 애플리케이션이 설치된 컴퓨터의 모든 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 오는 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **원격 측정 수집** 탭에서 **애플리케이션 및 호스트 네트워크 인터페이스에 무차별 모드 사용** 확인란을 선택합니다.

b. 아래 목록의 서브넷에 대해 구성된 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **지정된 서브넷에 대해 구성된 호스트 네트워크 인터페이스만 무차별 모드에서 사용** 확인란을 선택합니다.

c. 필요하다면 서브넷 목록을 생성합니다.

12. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 Kaspersky Industrial CyberSecurity for Networks와의 통합을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **원격 측정 수집 서버** 섹션을 선택합니다.
5. **KICS for Networks와 통합** 블록에서 **구성** 버튼을 클릭합니다.
   KICS for Networks와 통합 창이 열립니다.
6. **KICS for Networks와 통합 사용** 확인란을 선택합니다.
7. **연결 설정**에서 텔레메트리 모드를 선택합니다.
   - **TCP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송**. Kaspersky Industrial CyberSecurity for Nodes는 TCP 프로토콜을 통해 Kaspersky Industrial CyberSecurity for Networks 서버로 텔레메트리를 직접 전송합니다.
   - **원격 측정을 데이터 다이오드로 MQTT 게시자로 전송**. Kaspersky Industrial CyberSecurity for Nodes가 원격 측정을 소프트웨어 데이터 다이오드에 내장된 MQTT 중개 서버로 전송합니다.
   - **UDP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송**. Kaspersky Industrial CyberSecurity for Nodes는 UDP 프로토콜을 사용하여 데이터 다이오드를 통해 Kaspersky Industrial CyberSecurity for Networks 서버로 텔레메트리를 전송합니다.
8. **TCP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송** 모드에서 관리할 설정:
   - **주소** 및 **포트**. 원격 측정을 전송할 Kaspersky Industrial CyberSecurity for Networks 서버의 IP 주소 및 포트. 가능한 포트 값 범위: 1~65535. 기본 포트는 8081입니다.
   - **요청 간격(분)**. Kaspersky Industrial CyberSecurity for Networks 서버에 요청을 보내는 간격(분)입니다. Kaspersky Industrial CyberSecurity for Nodes가 MQTT 게시자로 작동할 때 브로커와의 연결이 끊어지면 이 설정에 따라 MQTT 브로커에 대한 요청 간격이 설정됩니다. 사용 가능한 값 범위는 1–60분입니다. 기본값은 1분입니다.

- **서버 연결 설정**. 다음 설정을 관리합니다:

  - **시간 초과(초)**. 최대 서버 응답 시간 초과. 시간 초과 시 Kaspersky Industrial CyberSecurity for Nodes가 서버에 다시 연결합니다. 사용 가능한 값 범위: 1~60000초. 기본값은 10초입니다.

  - **서버 TLS 인증서**. Kaspersky Industrial CyberSecurity for Networks 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Industrial CyberSecurity for Networks 관리 인터페이스를 사용하여 TLS 인증서를 얻을 수 있습니다.

  - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Kaspersky Industrial CyberSecurity for Networks 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Industrial CyberSecurity for Networks 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

    암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

9. **원격 측정을 데이터 다이오드로 MQTT 게시자로 전송** 모드에서 관리할 설정:

   a. MQTT 중개 서버에서 인증을 위한 자격 증명을 입력합니다.

   b. MQTT 중개 서버의 IP 주소와 포트를 입력합니다.

10. **UDP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송** 모드에서 관리할 설정:

    a. 서버의 IP 주소와 포트를 입력합니다.

    b. 데이터 암호화를 사용하려면 **서버 연결 설정** 버튼을 클릭하고 **UDP 프로토콜을 통해 데이터를 전송할 때 암호화 사용** 체크박스를 선택합니다.

    > 전송되는 데이터의 암호화가 필요한지 평가해야 합니다.

    c. 암호화 키 암호를 입력하고 확장자가 .PEM인 암호화 키 파일을 업로드합니다.

11. 데이터 전송 설정:

- **최대 이벤트 전송 지연(초)**. 애플리케이션이 서버와 동기화하여 지정한 시간 후 이벤트를 보냅니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.

  > Kaspersky Industrial CyberSecurity for Nodes를 MQTT 구독자로 사용하는 경우 MQTT 게시자의 설정에서 최소 **최대 이벤트 전송 지연(초)** 값인 1초를 지정했다면 MQTT 게시자로 구성된 Kaspersky Industrial CyberSecurity for Nodes 장치 250대 이상에서 원격 측정을 수신하도록 구성하지 않는 것이 좋습니다. 설정값이 30초 이상인 경우 MQTT 게시자 1,000개 이상에서 데이터를 수신하도록 구성하지 않는 것이 좋습니다.

- **요청 제한 사용**. 이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다.

- **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 사용 가능한 값 범위는 10–65535입니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

- **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 사용 가능한 값 범위: 5~100%. 기본값은 15%입니다

필요하다면 무차별 모드에서 원격 측정 구성. 기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터의 네트워크 인터페이스에 도착하고 애플리케이션이 설치된 컴퓨터로 주소가 지정되는 네트워크 트래픽을 수집합니다. 무차별 모드에서 애플리케이션은 사용 가능한 모든 서브넷에서 컴퓨터의 네트워크 인터페이스에 대한 네트워크 트래픽을 수집합니다. 애플리케이션은 수집된 트래픽을 사용하여 확장 원격 측정을 생성합니다.

> 모든 네트워크 어댑터가 무차별 모드(Promiscuous mode)를 지원하지는 않습니다. 이러한 네트워크 어댑터에서는 확장 원격 측정 수집이 작동하지 않습니다.

a. 애플리케이션이 설치된 컴퓨터의 모든 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 오는 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **애플리케이션 및 호스트 네트워크 인터페이스에 무차별 모드 사용** 확인란을 선택합니다.

b. 아래 목록의 서브넷에 대해 구성된 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **지정된 서브넷에 대해 구성된 호스트 네트워크 인터페이스만 무차별 모드에서 사용** 확인란을 선택합니다.

c. 필요하다면 서브넷 목록을 생성합니다.

12. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 Kaspersky Industrial CyberSecurity for Networks와의 통합을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **원격 측정 수집 서버 → KICS for Networks와 통합** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.
   일반 탭에서 **속성: KICS for Networks와 통합** 창이 열립니다.

3. **KICS for Networks와 통합** 확인란을 선택합니다.

4. **일반** 탭에서 원격 측정 모드를 선택합니다:

   - **TCP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송**. Kaspersky Industrial CyberSecurity for Nodes는 TCP 프로토콜을 통해 Kaspersky Industrial CyberSecurity for Networks 서버로 텔레메트리를 직접 전송합니다.

   - **원격 측정을 데이터 다이오드로 MQTT 게시자로 전송**. Kaspersky Industrial CyberSecurity for Nodes가 원격 측정을 소프트웨어 데이터 다이오드에 내장된 MQTT 중개 서버로 전송합니다.

   - **UDP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송**. Kaspersky Industrial CyberSecurity for Nodes는 UDP 프로토콜을 사용하여 데이터 다이오드를 통해 Kaspersky Industrial CyberSecurity for Networks 서버로 텔레메트리를 전송합니다.

5. **TCP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송** 모드에서 관리할 설정:

   - **주소** 및 **포트**. 원격 측정을 전송할 Kaspersky Industrial CyberSecurity for Networks 서버의 IP 주소 및 포트. 가능한 포트 값 범위: 1~65535. 기본 포트는 8081입니다.

   - **요청 간격(분)**. Kaspersky Industrial CyberSecurity for Networks 서버에 요청을 보내는 간격(분)입니다. Kaspersky Industrial CyberSecurity for Nodes가 MQTT 게시자로 작동할 때 브로커와의 연결이 끊어지면 이 설정에 따라 MQTT 브로커에 대한 요청 간격이 설정됩니다. 사용 가능한 값 범위는 1–60분입니다. 기본값은 1분입니다.

   - **서버 연결 설정**. 다음 설정을 관리합니다:

     - **시간 초과(초)**. 최대 서버 응답 시간 초과. 시간 초과 시 Kaspersky Industrial CyberSecurity for Nodes가 서버에 다시 연결합니다. 사용 가능한 값 범위: 1~60000초. 기본값은 10초입니다.

     - **서버 TLS 인증서**. Kaspersky Industrial CyberSecurity for Networks 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Industrial CyberSecurity for Networks 관리 인터페이스를 사용하여 TLS 인증서를 얻을 수 있습니다.

     - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Kaspersky Industrial CyberSecurity for Networks 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Industrial CyberSecurity for Networks 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

       암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

6. **원격 측정을 데이터 다이오드로 MQTT 게시자로 전송** 모드에서 관리할 설정:

   a. **서버 연결 설정** 버튼을 클릭합니다.

   b. MQTT 중개 서버에서 인증을 위한 자격 증명을 입력합니다.

   c. MQTT 중개 서버의 IP 주소와 포트를 입력합니다.

7. **UDP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송** 모드에서 관리할 설정:

   a. 서버의 IP 주소와 포트를 입력합니다.

   b. 데이터 암호화를 사용하려면 **서버 연결 설정** 버튼을 클릭하고 **UDP 프로토콜을 통해 데이터를 전송할 때 암호화 사용** 체크박스를 선택합니다.

      전송되는 데이터의 암호화가 필요한지 평가해야 합니다.

   c. 암호화 키 암호를 입력하고 확장자가 .PEM인 암호화 키 파일을 업로드합니다.

8. **데이터 전송** 탭으로 갑니다.

9. 데이터 전송 설정:

- **최대 이벤트 전송 지연(초)**. 애플리케이션이 서버와 동기화하여 지정한 시간 후 이벤트를 보냅니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.

  > Kaspersky Industrial CyberSecurity for Nodes를 MQTT 구독자로 사용하는 경우 MQTT 게시자의 설정에서 최소 **최대 이벤트 전송 지연(초)** 값인 1초를 지정했다면 MQTT 게시자로 구성된 Kaspersky Industrial CyberSecurity for Nodes 장치 250대 이상에서 원격 측정을 수신하도록 구성하지 않는 것이 좋습니다. 설정값이 30초 이상인 경우 MQTT 게시자 1,000개 이상에서 데이터를 수신하도록 구성하지 않는 것이 좋습니다.

- **요청 제한 사용**. 이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다.

- **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 사용 가능한 값 범위는 10–65535입니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

- **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 사용 가능한 값 범위: 5~100%. 기본값은 15%입니다

필요하다면 무차별 모드에서 원격 측정 구성. 기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터의 네트워크 인터페이스에 도착하고 애플리케이션이 설치된 컴퓨터로 주소가 지정되는 네트워크 트래픽을 수집합니다. 무차별 모드에서 애플리케이션은 사용 가능한 모든 서브넷에서 컴퓨터의 네트워크 인터페이스에 대한 네트워크 트래픽을 수집합니다. 애플리케이션은 수집된 트래픽을 사용하여 확장 원격 측정을 생성합니다.

> 모든 네트워크 어댑터가 무차별 모드(Promiscuous mode)를 지원하지는 않습니다. 이러한 네트워크 어댑터에서는 확장 원격 측정 수집이 작동하지 않습니다.

a. 애플리케이션이 설치된 컴퓨터의 모든 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 오는 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **원격 측정 수집** 탭에서 **애플리케이션 및 호스트 네트워크 인터페이스에 무차별 모드 사용** 확인란을 선택합니다.

b. 아래 목록의 서브넷에 대해 구성된 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **지정된 서브넷에 대해 구성된 호스트 네트워크 인터페이스만 무차별 모드에서 사용** 확인란을 선택합니다.

c. 필요하다면 서브넷 목록을 생성합니다.

10. 변경 사항을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes를 MQTT 구독자로 구성할 수도 있습니다. 이 모드에서 애플리케이션은 데이터 다이오드를 통해 MQTT 브로커로부터 텔레메트리를 수신한 다음 KICS for Networks로 전달합니다.

Kaspersky Security Center 관리 콘솔에서 애플리케이션을 MQTT 구독자로 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **관리 중인 기기** 노드를 확장하고 컴퓨터가 속한 그룹을 선택합니다.
2. 세부 정보 창에서 **기기** 탭을 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. **애플리케이션** 섹션으로 갑니다.
5. 컴퓨터에 설치된 Kaspersky 애플리케이션 목록에서 Kaspersky Industrial CyberSecurity for Nodes를 선택하고 더블 클릭하여 애플리케이션 속성을 엽니다.
6. **원격 측정 수집 서버** 섹션을 선택합니다.
7. **KICS for Networks와 통합** 블록에서 **설정** 버튼을 클릭합니다.

   KICS for Networks와 통합 창이 열립니다.
8. **KICS for Networks와 통합** 확인란을 선택합니다.
9. **일반** 탭에서 **TCP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송** 옵션을 선택합니다.
10. 다음 설정을 관리합니다:

    - **주소** 및 **포트**. 원격 측정을 전송할 Kaspersky Industrial CyberSecurity for Networks 서버의 IP 주소 및 포트.
    - **요청 간격(분)**. Kaspersky Industrial CyberSecurity for Networks 서버에 요청을 보내는 간격(분)입니다. Kaspersky Industrial CyberSecurity for Nodes가 MQTT 게시자로 작동할 때 브로커와의 연결이 끊어지면 이 설정에 따라 MQTT 브로커에 대한 요청 간격이 설정됩니다. 사용 가능한 값 범위는 1–60분입니다. 기본값은 1분입니다.
    - **서버 연결 설정**. 다음 설정을 관리합니다:
      - **시간 초과(초)**. 최대 서버 응답 시간 초과. 시간 초과 시 Kaspersky Industrial CyberSecurity for Nodes가 서버에 다시 연결합니다. 사용 가능한 값 범위: 1~60000초. 기본값은 10초입니다.
      - **서버 TLS 인증서**. Kaspersky Industrial CyberSecurity for Networks 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Industrial CyberSecurity for Networks 관리 인터페이스를 사용하여 TLS 인증서를 얻을 수 있습니다.
      - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Kaspersky Industrial CyberSecurity for Networks 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Industrial CyberSecurity for Networks 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

        암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.
    - **원격 측정을 데이터 다이오드에서 MQTT 서브스크라이버로 수신** 확인란을 선택합니다.

- MQTT 중개 서버에서 인증을 위한 자격 증명을 입력합니다.
- MQTT 중개 서버의 IP 주소와 포트를 입력합니다.

11. **데이터 전송** 탭으로 갑니다.

12. 데이터 전송 설정:

    - **최대 이벤트 전송 지연(초)**. 애플리케이션이 서버와 동기화하여 지정한 시간 후 이벤트를 보냅니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.

      Kaspersky Industrial CyberSecurity for Nodes를 MQTT 구독자로 사용하는 경우 MQTT 게시자의 설정에서 최소 **최대 이벤트 전송 지연(초)** 값인 1초를 지정했다면 MQTT 게시자로 구성된 Kaspersky Industrial CyberSecurity for Nodes 장치 250대 이상에서 원격 측정을 수신하도록 구성하지 않는 것이 좋습니다. 설정값이 30초 이상인 경우 MQTT 게시자 1,000개 이상에서 데이터를 수신하도록 구성하지 않는 것이 좋습니다.

    - **요청 제한 사용**. 이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다.

    - **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 사용 가능한 값 범위는 10–65535입니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

    - **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 사용 가능한 값 범위: 5~100%. 기본값은 15%입니다

13. 필요하다면 무차별 모드에서 원격 측정 구성.

    기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터의 네트워크 인터페이스에 도착하고 애플리케이션이 설치된 컴퓨터로 주소가 지정되는 네트워크 트래픽을 수집합니다. 무차별 모드에서 애플리케이션은 사용 가능한 모든 서브넷에서 컴퓨터의 네트워크 인터페이스에 대한 네트워크 트래픽을 수집합니다. 애플리케이션은 수집된 트래픽을 사용하여 확장 원격 측정을 생성합니다.

    모든 네트워크 어댑터가 무차별 모드(Promiscuous mode)를 지원하지는 않습니다. 이러한 네트워크 어댑터에서는 확장 원격 측정 수집이 작동하지 않습니다.

    a. 애플리케이션이 설치된 컴퓨터의 모든 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 오는 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **원격 측정 수집** 탭에서 **애플리케이션 및 호스트 네트워크 인터페이스에 무차별 모드 사용** 확인란을 선택합니다.

    b. 아래 목록의 서브넷에 대해 구성된 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **지정된 서브넷에 대해 구성된 호스트 네트워크 인터페이스만 무차별 모드에서 사용** 확인란을 선택합니다.

    c. 필요하다면 서브넷 목록을 생성합니다.

14. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 애플리케이션을 MQTT 구독자로 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)** 옵션을 선택합니다.
2. 컴퓨터 이름을 클릭합니다.
3. 표시된 컴퓨터 속성 창에서 **애플리케이션** 탭을 선택합니다.
4. **Kaspersky Industrial CyberSecurity for Nodes(5.0.0)**를 클릭합니다.
5. **애플리케이션 설정** 탭을 선택합니다.
6. **원격 측정 수집 서버** 섹션을 선택합니다.
7. **KICS for Networks와 통합** 블록에서 **구성** 버튼을 클릭합니다.
   KICS for Networks와 통합 창이 열립니다.
8. **KICS for Networks와 통합** 확인란을 선택합니다.
9. **일반** 탭에서 **TCP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송** 옵션을 선택합니다.
10. 다음 설정을 관리합니다:

    - **주소** 및 **포트**. 원격 측정을 전송할 Kaspersky Industrial CyberSecurity for Networks 서버의 IP 주소 및 포트.
    - **요청 간격(분)**. Kaspersky Industrial CyberSecurity for Networks 서버에 요청을 보내는 간격(분)입니다. Kaspersky Industrial CyberSecurity for Nodes가 MQTT 게시자로 작동할 때 브로커와의 연결이 끊어지면 이 설정에 따라 MQTT 브로커에 대한 요청 간격이 설정됩니다. 사용 가능한 값 범위는 1–60분입니다. 기본값은 1분입니다.
    - **서버 연결 설정**. 다음 설정을 관리합니다:
      - **시간 초과(초)**. 최대 서버 응답 시간 초과. 시간 초과 시 Kaspersky Industrial CyberSecurity for Nodes가 서버에 다시 연결합니다. 사용 가능한 값 범위: 1~60000초. 기본값은 10초입니다.
      - **서버 TLS 인증서**. Kaspersky Industrial CyberSecurity for Networks 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Industrial CyberSecurity for Networks 관리 인터페이스를 사용하여 TLS 인증서를 얻을 수 있습니다.
      - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Kaspersky Industrial CyberSecurity for Networks 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Industrial CyberSecurity for Networks 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

        암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.
    - **원격 측정을 데이터 다이오드에서 MQTT 서브스크라이버로 수신** 확인란을 선택합니다.
    - MQTT 중개 서버에서 인증을 위한 자격 증명을 입력합니다.
    - MQTT 중개 서버의 IP 주소와 포트를 입력합니다.

11. 데이터 전송 설정:

- **최대 이벤트 전송 지연(초)**. 애플리케이션이 서버와 동기화하여 지정한 시간 후 이벤트를 보냅니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.

  Kaspersky Industrial CyberSecurity for Nodes를 MQTT 구독자로 사용하는 경우 MQTT 게시자의 설정에서 최소 **최대 이벤트 전송 지연(초)** 값인 1초를 지정했다면 MQTT 게시자로 구성된 Kaspersky Industrial CyberSecurity for Nodes 장치 250대 이상에서 원격 측정을 수신하도록 구성하지 않는 것이 좋습니다. 설정값이 30초 이상인 경우 MQTT 게시자 1,000개 이상에서 데이터를 수신하도록 구성하지 않는 것이 좋습니다.

- **요청 제한 사용**. 이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다.

- **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 사용 가능한 값 범위는 10–65535입니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

- **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 사용 가능한 값 범위: 5~100%. 기본값은 15%입니다

12. 필요하다면 무차별 모드에서 원격 측정 구성.

    기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터의 네트워크 인터페이스에 도착하고 애플리케이션이 설치된 컴퓨터로 주소가 지정되는 네트워크 트래픽을 수집합니다. 무차별 모드에서 애플리케이션은 사용 가능한 모든 서브넷에서 컴퓨터의 네트워크 인터페이스에 대한 네트워크 트래픽을 수집합니다. 애플리케이션은 수집된 트래픽을 사용하여 확장 원격 측정을 생성합니다.

    모든 네트워크 어댑터가 무차별 모드(Promiscuous mode)를 지원하지는 않습니다. 이러한 네트워크 어댑터에서는 확장 원격 측정 수집이 작동하지 않습니다.

    a. 애플리케이션이 설치된 컴퓨터의 모든 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 오는 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **애플리케이션 및 호스트 네트워크 인터페이스에 무차별 모드 사용** 확인란을 선택합니다.

    b. 아래 목록의 서브넷에 대해 구성된 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **지정된 서브넷에 대해 구성된 호스트 네트워크 인터페이스만 무차별 모드에서 사용** 확인란을 선택합니다.

    c. 필요하다면 서브넷 목록을 생성합니다.

13. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 애플리케이션을 MQTT 구독자로 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **원격 측정 수집 서버 → KICS for Networks와 통합** 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.

   일반 탭에서 **속성: KICS for Networks와 통합** 창이 열립니다.

3. **KICS for Networks와 통합** 확인란을 선택합니다.

4. **일반** 탭에서 **TCP 프로토콜을 통해 KICS for Networks 서버에 원격 측정 전송** 옵션을 선택합니다.

5. 다음 설정을 관리합니다:

   - **주소** 및 **포트**. 원격 측정을 전송할 Kaspersky Industrial CyberSecurity for Networks 서버의 IP 주소 및 포트.

   - **요청 간격(분)**. Kaspersky Industrial CyberSecurity for Networks 서버에 요청을 보내는 간격(분)입니다. Kaspersky Industrial CyberSecurity for Nodes가 MQTT 게시자로 작동할 때 브로커와의 연결이 끊어지면 이 설정에 따라 MQTT 브로커에 대한 요청 간격이 설정됩니다. 사용 가능한 값 범위는 1–60분입니다. 기본값은 1분입니다.

   - **서버 연결 설정**. 다음 설정을 관리합니다:

     - **시간 초과(초)**. 최대 서버 응답 시간 초과. 시간 초과 시 Kaspersky Industrial CyberSecurity for Nodes가 서버에 다시 연결합니다. 사용 가능한 값 범위: 1~60000초. 기본값은 10초입니다.

     - **서버 TLS 인증서**. Kaspersky Industrial CyberSecurity for Networks 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Industrial CyberSecurity for Networks 관리 인터페이스를 사용하여 TLS 인증서를 얻을 수 있습니다.

     - **양방향 인증 사용**. Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Kaspersky Industrial CyberSecurity for Networks 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. Kaspersky Industrial CyberSecurity for Networks 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

       암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

   - **원격 측정을 데이터 다이오드에서 MQTT 서브스크라이버로 수신** 확인란을 선택합니다.

   - MQTT 중개 서버에서 인증을 위한 자격 증명을 입력합니다.

   - MQTT 중개 서버의 IP 주소와 포트를 입력합니다.

6. **데이터 전송** 탭으로 갑니다.

7. 데이터 전송 설정:

- **최대 이벤트 전송 지연(초)**. 애플리케이션이 서버와 동기화하여 지정한 시간 후 이벤트를 보냅니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.

  Kaspersky Industrial CyberSecurity for Nodes를 MQTT 구독자로 사용하는 경우 MQTT 게시자의 설정에서 최소 **최대 이벤트 전송 지연(초)** 값인 1초를 지정했다면 MQTT 게시자로 구성된 Kaspersky Industrial CyberSecurity for Nodes 장치 250대 이상에서 원격 측정을 수신하도록 구성하지 않는 것이 좋습니다. 설정값이 30초 이상인 경우 MQTT 게시자 1,000개 이상에서 데이터를 수신하도록 구성하지 않는 것이 좋습니다.

- **요청 제한 사용**. 이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 이벤트 전송을 중지합니다.

- **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 1시간 후에 이벤트 전송을 재개합니다. 사용 가능한 값 범위는 10–65535입니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

- **이벤트 제한 초과율**. 애플리케이션은 이벤트를 유형별로 정렬하고(예: "레지스트리 변경 사항" 이벤트) 총 이벤트 수에 대한 동일한 유형의 이벤트 비율이 설정된 제한(백분율)을 초과할 경우 이벤트 전송을 제한합니다. Kaspersky Industrial CyberSecurity for Nodes는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 사용 가능한 값 범위: 5~100%. 기본값은 15%입니다

8. 필요하다면 무차별 모드에서 원격 측정 구성.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터의 네트워크 인터페이스에 도착하고 애플리케이션이 설치된 컴퓨터로 주소가 지정되는 네트워크 트래픽을 수집합니다. 무차별 모드에서 애플리케이션은 사용 가능한 모든 서브넷에서 컴퓨터의 네트워크 인터페이스에 대한 네트워크 트래픽을 수집합니다. 애플리케이션은 수집된 트래픽을 사용하여 확장 원격 측정을 생성합니다.

   모든 네트워크 어댑터가 무차별 모드(Promiscuous mode)를 지원하지는 않습니다. 이러한 네트워크 어댑터에서는 확장 원격 측정 수집이 작동하지 않습니다.

   a. 애플리케이션이 설치된 컴퓨터의 모든 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 오는 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **원격 측정 수집** 탭에서 **애플리케이션 및 호스트 네트워크 인터페이스에 무차별 모드 사용** 확인란을 선택합니다.

   b. 아래 목록의 서브넷에 대해 구성된 네트워크 인터페이스에 대해 사용 가능한 모든 서브넷에서 네트워크 트래픽 수집의 무차별 모드를 활성화하려면 **지정된 서브넷에 대해 구성된 호스트 네트워크 인터페이스만 무차별 모드에서 사용** 확인란을 선택합니다.

   c. 필요하다면 서브넷 목록을 생성합니다.

9. 변경 사항을 저장합니다.

필요한 경우 명령줄 인터페이스를 사용하여 Kaspersky Industrial CyberSecurity for Networks와의 통합을 구성할 수 있습니다.

Kaspersky Industrial CyberSecurity for Networks 통합 관련 특별 고려 사항 및 제한 사항

감사 정책 설정 수정

Kaspersky Industrial CyberSecurity for Networks와의 통합이 올바르게 작동하도록 하려면 감사 정책 설정을 수정해야 합니다. 애플리케이션의 동작은 장치가 도메인에 속하는지 여부에 따라 다릅니다.

- 장치가 도메인에 속하지 않으면 애플리케이션이 필요에 따라 로컬 정책 설정을 자동으로 수정합니다.
- 장치가 도메인에 속하면 애플리케이션이 도메인 그룹 정책 설정을 수정하지 않습니다. 이러한 장치를 도메인에서 제외하거나 도메인 그룹 정책 설정을 직접 구성할 수 있습니다.
  - **사용자 계정 관리 감사** 하위 범주에서 **성공** 설정을 활성화합니다.
  - **로그온 감사**, **로그오프 감사** 및 **기타 로그온/로그오프 이벤트 감사** 하위 범주에서 **성공** 및 **실패** 설정을 활성화합니다.

Kaspersky Industrial CyberSecurity for Networks 통합 제한 사항

Kaspersky Industrial CyberSecurity for Networks 통합 기능에는 다음과 같은 제한 사항이 있습니다.

- Windows XP 컴퓨터에서는 MQTT 중개 서버로 원격 측정을 전송할 수 없습니다.
- Kaspersky Industrial CyberSecurity for Networks 서버와 연결되어 있지 않으면 데이터 다이오드를 통해 Kaspersky Industrial CyberSecurity for Nodes에서 수신한 메시지의 전달이 보장되지 않습니다.
- Wi-Fi 네트워크 모니터링 기능은 IPv4 프로토콜을 사용하는 네트워크에서 지원됩니다. IPv6 주소가 있는 장치는 탐지되지 않습니다.
- SSID가 숨겨진 Wi-Fi 네트워크에서는 사용되는 보호 표준과 암호화 프로토콜 및 로밍 표준에 대한 정보를 수집할 수 없습니다.
- Wi-Fi 네트워크를 검사할 때 애플리케이션은 DHCP, ICMP, ARP, mDNS, UPnP 및 NetBIOS 프로토콜을 사용합니다. 애플리케이션이 올바르게 작동하려면 네트워크에서 이러한 프로토콜의 사용을 허용해야 합니다.
- Windows 11, Windows Server 2025 이상을 실행하는 보호된 장치에서 Wi-Fi 네트워크에 대한 데이터를 수집하려면 운영 체제 설정에서 위치 서비스를 활성화해야 합니다. 위치 서비스가 꺼져 있으면 Kaspersky Industrial CyberSecurity for Nodes는 Wi-Fi 네트워크에 대한 데이터를 수집하거나 Kaspersky Industrial CyberSecurity for Networks로 전송하지 않습니다.
- Windows Vista 이전 버전의 운영 체제를 실행하는 장치에서는 Wi-Fi 데이터를 수집할 수 없습니다.

Wi-Fi 네트워크 모니터링 구성

Kaspersky Industrial CyberSecurity for Nodes가 실행 중인 보호 대상 장치에서 탐지된 Wi-Fi 네트워크에 대한 데이터와 보호 대상 장치와 동일한 Wi-Fi 네트워크에 연결된 장치에 대한 데이터를 Kaspersky Industrial CyberSecurity for Networks 서버로 보내도록 구성할 수 있습니다. Kaspersky Industrial CyberSecurity for Networks는 수집된 데이터를 사용하여 인프라 내 Wi-Fi 네트워크를 중앙에서 모니터링합니다. 자세한 내용은 Kaspersky Industrial CyberSecurity for Networks 도움말을 참조하십시오.

네트워크 인프라의 부하를 줄이려면 수집 데이터의 완전성을 보장하는 데 필요한 장치에서만 Wi-Fi 데이터 수집을 활성화하는 것이 좋습니다.

Wi-Fi 네트워크 데이터의 수집 및 전송은 Kaspersky Security Center 관리 콘솔에서만 구성할 수 있습니다. 애플리케이션 콘솔에서는 현재 설정만 볼 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 Wi-Fi 네트워크 데이터 수집 및 전송을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **원격 측정 수집 서버** 섹션을 선택합니다.
4. **KICS for Networks와 통합** 블록에서 **설정** 버튼을 클릭합니다.

   KICS for Networks와 통합 창이 열립니다.
5. **네트워크 및 기기 검색 설정** 탭으로 갑니다.
6. Wi-Fi 네트워크 설정 구성:

   - **Wi-Fi 네트워크 검색**. 이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 보호 대상 장치에서 사용할 수 있는 Wi-Fi 네트워크에 대한 정보를 수집하여 Kaspersky Industrial CyberSecurity for Networks로 전송합니다. 이 기능은 기본적으로 비활성화됩니다.
   - **연결된 네트워크에서 유선 또는 무선 기기 검색**. 이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 보호 대상 장치와 동일한 Wi-Fi 네트워크에 연결된 장치에 대한 정보를 수집하여 Kaspersky Industrial CyberSecurity for Networks로 전송합니다. 이 기능은 기본적으로 비활성화됩니다.
7. 필요한 경우 데이터 수집 및 전송의 기본 설정을 변경합니다.

   - **실행 주기(분)**. 검사 간격을 분 단위로 지정합니다. 사용 가능한 값 범위: 1–150분. 기본값은 5분입니다.
   - **(분)마다 서버에 데이터 전송**. 데이터를 서버로 전송하는 간격을 분 단위로 지정합니다. 사용 가능한 값 범위: 1–150분. 기본값은 10분입니다.

     검사 간격은 데이터 전송 간격보다 짧아야 합니다.

애플리케이션이 단일 데이터 전송 간격 동안 여러 번 검사하는 경우 수집된 데이터는 다음 규칙에 따라 집계됩니다.

- 집계된 데이터에서 MAC 주소는 검사된 개체의 고유 식별자로 사용됩니다.
- 검사된 각 개체에 대해 집계된 데이터에는 해당 간격 내 마지막 검사에서 얻은 정보가 포함됩니다.
- 검사 장치가 여러 Wi-Fi 네트워크 간에 전환된 경우 집계된 데이터에는 현재 전송 간격 동안 가장 최근의 네트워크에서 수집된 정보만 포함됩니다.
- 검사된 개체가 더 이상 탐지되지 않으면 집계된 데이터에는 해당 개체에 대해 수집된 최신 정보와 마지막 탐지 타임스탬프가 포함됩니다.
- Wi-Fi 네트워크의 SSID를 변경하면 이전 SSID와 연결된 데이터는 유지되지 않습니다. 집계된 데이터에는 마지막 SSID와 관련된 정보만 포함됩니다.

8. 변경 사항을 저장합니다.

웹 콘솔에서 Wi-Fi 네트워크 정보 수집 및 전송을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **원격 측정 수집 서버** 섹션을 선택합니다.
5. **KICS for Networks와 통합** 블록에서 **구성** 버튼을 클릭합니다.
   KICS for Networks와 통합 창이 열립니다.
6. **네트워크 및 기기 검색 설정**에서 Wi-Fi 네트워크 설정을 구성합니다.
   - **Wi-Fi 네트워크 검색**. 이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 보호 대상 장치에서 사용할 수 있는 Wi-Fi 네트워크에 대한 정보를 수집하여 Kaspersky Industrial CyberSecurity for Networks로 전송합니다. 이 기능은 기본적으로 비활성화됩니다.
   - **연결된 네트워크에서 유선 또는 무선 기기 검색**. 이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 보호 대상 장치와 동일한 Wi-Fi 네트워크에 연결된 장치에 대한 정보를 수집하여 Kaspersky Industrial CyberSecurity for Networks로 전송합니다. 이 기능은 기본적으로 비활성화됩니다.
7. 필요한 경우 데이터 수집 및 전송의 기본 설정을 변경합니다.
   - **실행 주기(분)**. 검사 간격을 분 단위로 지정합니다. 사용 가능한 값 범위: 1–150분. 기본값은 5분입니다.
   - **(분)마다 서버에 데이터 전송**. 데이터를 서버로 전송하는 간격을 분 단위로 지정합니다. 사용 가능한 값 범위: 1–150분. 기본값은 10분입니다.

     검사 간격은 데이터 전송 간격보다 짧아야 합니다.

애플리케이션이 단일 데이터 전송 간격 동안 여러 번 검사하는 경우 수집된 데이터는 다음 규칙에 따라 집계됩니다.

- 집계된 데이터에서 MAC 주소는 검사된 개체의 고유 식별자로 사용됩니다.
- 검사된 각 개체에 대해 집계된 데이터에는 해당 간격 내 마지막 검사에서 얻은 정보가 포함됩니다.
- 검사 장치가 여러 Wi-Fi 네트워크 간에 전환된 경우 집계된 데이터에는 현재 전송 간격 동안 가장 최근의 네트워크에서 수집된 정보만 포함됩니다.
- 검사된 개체가 더 이상 탐지되지 않으면 집계된 데이터에는 해당 개체에 대해 수집된 최신 정보와 마지막 탐지 타임스탬프가 포함됩니다.
- Wi-Fi 네트워크의 SSID를 변경하면 이전 SSID와 연결된 데이터는 유지되지 않습니다. 집계된 데이터에는 마지막 SSID와 관련된 정보만 포함됩니다.

8. 변경 사항을 저장합니다.

EDR 동작 모니터링

*EDR 동작 모니터링 센터*는 모든 Kaspersky Detection and Response 솔루션의 위협 대응 기록을 볼 수 있는 콘솔입니다. 조직에 여러 Detection and Response를 배포했다면 Kaspersky Industrial CyberSecurity for Nodes가 모든 솔루션의 위협 대응 기록을 표시합니다. 이를 통해 별도의 컴퓨터에서 Detection and Response 솔루션의 성능을 분석하고 이 솔루션의 설정을 최적화할 수 있습니다.

모니터링 센터는 다음 정보를 제공합니다:

- 위협 대응 작업 정보(*프로세스 종료* 작업 등)
- 네트워크 격리 및 실행 방지 규칙의 변경

위협 대응이 네트워크 공유 접근과 관련된 오류를 발견하면, 위협 대응 이력에서 해당 오류가 표시되지 않습니다.

EDR 동작 모니터링 센터 콘솔이 열립니다.

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)** 옵션을 선택합니다.
2. 위협 대응 이력을 보려는 컴퓨터의 이름을 클릭합니다.
   컴퓨터 속성 창이 열립니다.
3. **애플리케이션** 탭을 선택합니다.
4. **Kaspersky Industrial CyberSecurity for Nodes(5.0.0)**를 클릭합니다.
   그러면 로컬 애플리케이션 설정이 열립니다.

5. **애플리케이션 설정** 탭을 선택합니다.

6. **원격 측정 수집 서버 → 응답 이력**으로 갑니다.

EDR 동작 모니터링 센터 콘솔이 열립니다. 콘솔을 사용하여 위협 대응 작업 상태, 작업 지속 시간, 규칙 변경 사항, 개시자 세부 정보를 볼 수 있습니다.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent는 지능형 위협을 탐지하기 위해 이 애플리케이션과 다른 Kaspersky 솔루션(Kaspersky Anti Targeted Attack Platform 등) 간의 상호 작용을 지원합니다. Kaspersky 솔루션은 특정 버전의 Kaspersky Endpoint Agent와 호환됩니다.

Kaspersky 솔루션의 일부로 Kaspersky Endpoint Agent를 사용하려면 해당하는 라이센스 키로 이 솔루션을 활성화해야 합니다.

Kaspersky Endpoint Agent는 지능형 위협(예: 표적형 공격)을 탐지를 위해 다음 Kaspersky 솔루션과의 상호 작용을 지원합니다:

- Kaspersky Industrial CyberSecurity Endpoint Detection and Response(Kaspersky Endpoint Agent 3.9 이상 지원)
- Kaspersky Anti Targeted Attack Platform(Kaspersky Endpoint Agent 3.8 이상 지원)
- Kaspersky Managed Detection and Response

Kaspersky Industrial CyberSecurity for Nodes 4.0 배포 키트는 Kaspersky Endpoint Agent 애플리케이션을 포함합니다. 이전 버전에서는 기술 계정 관리자(TAM)에게 Kaspersky Endpoint Agent 배포 키트를 요청할 수 있습니다. 4.5 버전부터 Kaspersky Industrial CyberSecurity for Nodes 배포 키트에 Kaspersky Endpoint Agent 배포 키트가 포함되지 않습니다. Kaspersky Industrial CyberSecurity for Nodes 4.5에는 애플리케이션이 Detection and Response 솔루션과의 통합을 지원하는 데 사용하는 내장 에이전트가 포함되어 있습니다. 이 두 애플리케이션을 한 컴퓨터에 모두 설치할 수는 없습니다.

[KICS+KEA] 구성을 [KICS+내장 Endpoint Agent] 구성으로 마이그레이션

Kaspersky Industrial CyberSecurity for Nodes는 버전 4.5부터 Detection and Response 솔루션을 지원하기 위한 내장 에이전트를 포함합니다. 이제 Kaspersky Endpoint Agent 애플리케이션이 없어도 이 솔루션을 이용할 수 있습니다. Kaspersky Endpoint Agent가 설치된 컴퓨터에 Kaspersky Industrial CyberSecurity for Nodes를 배포하면, Detection and Response 솔루션이 Kaspersky Industrial CyberSecurity for Nodes와 계속해서 작동하며 Kaspersky Endpoint Agent 애플리케이션이 컴퓨터에서 제거됩니다.

[KICS+KEA] 구성을 [KICS+내장 에이전트]로 마이그레이션하는 단계는 다음과 같습니다:

1. **Kaspersky Security Center 업그레이드**

   사용자 컴퓨터의 네트워크 에이전트를 포함하여 Kaspersky Security Center 구성 요소 전체를 버전 14.2 이상으로 업그레이드합니다.

2 Kaspersky Industrial CyberSecurity for Nodes 설치/버전 5.0로 업그레이드

애플리케이션을 설치하는 경우 설치 패키지 설정 또는 에서 설치 마법사, 다른 필요한 구성 요소와 함께 **전체 기능 → Endpoint Agent**를 선택합니다.

애플리케이션을 업데이트하면 Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky Endpoint Agent가 설치된 컴퓨터에서 자동 구성 요소 선택을 지원합니다. 구성 요소의 자동 선택은 애플리케이션을 업그레이드하는 사용자 계정의 권한에 달려 있습니다.

시스템 계정(SYSTEM)의 EXE 또는 MSI 파일을 사용해 Kaspersky Industrial CyberSecurity for Nodes를 업그레이드한다면 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky 솔루션의 현재 라이센스에 대한 접근 권한을 획득합니다. 따라서 컴퓨터에 Kaspersky Endpoint Agent가 설치되어 있고 EDR Optimum 솔루션이 활성화되어 있는 것 같은 경우에 Kaspersky Industrial CyberSecurity for Nodes 설치 프로그램은 자동으로 구성 요소의 세트를 구성하고 EDR Optimum 구성 요소를 선택합니다. 이에 따라 Kaspersky Industrial CyberSecurity for Nodes는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다. 시스템 계정(SYSTEM)에서 MSI 설치 프로그램을 실행하면 주로 Kaspersky 업데이트 서비스(SMU)를 통해 업그레이드하거나 Kaspersky Security Center를 통해 설치 패키지를 배포할 때 수행됩니다.

별도의 권한이 없는 사용자 계정으로 MSI 파일을 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 업그레이드한다면, Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky 솔루션의 현재 라이센스에 접근할 권한이 없습니다. 이때 Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Endpoint Agent 구성에 기반하여 자동으로 구성 요소를 선택합니다. 그리고 나서 Kaspersky Industrial CyberSecurity for Nodes는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다.

3 라이센싱 기능

Kaspersky Endpoint Detection and Response Optimum 공통 라이센스를 사용하여 Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Endpoint Agent를 활성화하면 애플리케이션을 버전 5.0로 업그레이드한 후 EDR Optimum 기능이 자동으로 활성화됩니다. 별도의 작업이 필요하지 않습니다.

독립 실행형 Kaspersky EDR Optimum 애드온 라이센스로 EDR Optimum 기능을 활성화하면 EDR Optimum 애드온 키가 Kaspersky Security Center 저장소에 추가되었으며 자동 라이센스 키 배포 기능이 활성화되었는지 확인해야 합니다. 애플리케이션을 버전 5.0로 업그레이드하면 EDR Optimum 기능이 자동으로 활성화됩니다.

Kaspersky Endpoint Detection and Response Optimum 라이센스로 Kaspersky Endpoint Agent를 활성화한 후 다른 라이센스로 Kaspersky Industrial CyberSecurity for Nodes를 활성화하면 Kaspersky Industrial CyberSecurity for Nodes 키를 Kaspersky Endpoint Detection and Response Optimum 또는 Kaspersky Optimum Security 공통 키로 교체해야 합니다. 키는 *키 추가* 작업으로 교체할 수 있습니다.

4 Kaspersky Industrial CyberSecurity for Nodes 웹 플러그인 업그레이드

Kaspersky Security Center 웹 콘솔에서 Kaspersky Industrial CyberSecurity for Nodes 웹 플러그인을 5.0로 업그레이드합니다.

5 정책 및 작업 마이그레이션

정책 및 작업 마이그레이션 마법사를 사용하여 Kaspersky Endpoint Agent 설정을 Kaspersky Industrial CyberSecurity for Nodes로 마이그레이션합니다.

[KICS+KEA] 구성의 정책 및 작업을 [KICS+내장 에이전트] 구성으로 마이그레이션

Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Endpoint Agent 4.0 이하의 정책 및 작업 마이그레이션 마법사를 사용하여 내장 에이전트가 있는 Kaspersky Industrial CyberSecurity for Nodes 5.0를 거쳐 다음 솔루션에 정책과 작업 설정을 마이그레이션할 수 있습니다:

- Kaspersky Industrial CyberSecurity Endpoint Detection and Response
- Kaspersky Anti Targeted Attack Platform(EDR).

정책 및 작업 마이그레이션 마법사는 웹 콘솔과 Cloud Console에서만 사용할 수 있습니다.

우선 하나의 컴퓨터에서 [KICS+KEA] 구성의 정책 및 작업을 [KICS+내장 에이전트]로 마이그레이션한 다음, 컴퓨터 그룹을 거쳐 조직의 모든 컴퓨터로 마이그레이션할 것을 권장합니다.

[KICS+KEA] 구성에서 [KICS+내장 에이전트] 구성으로 정책 및 작업을 마이그레이션하려면:

웹 콘솔 또는 Cloud Console의 메인 창에서 **동작** → **Kaspersky Industrial CyberSecurity for Nodes 5.0.0으로 마이그레이션** 옵션을 선택합니다.

정책 및 작업 마이그레이션 마법사가 열립니다. 마법사의 지침을 따릅니다.

1단계. 정책 마이그레이션

설정을 병합하려는 Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Endpoint Agent 정책을 선택합니다.

알맞은 정책을 선택했는지 확인하고 다음 단계로 넘어갑니다.

2단계. 정책 마이그레이션

작업 목록에서 Kaspersky Industrial CyberSecurity for Nodes 5.0에 생성하고자 하는 Kaspersky Industrial CyberSecurity for Nodes 작업을 선택합니다.

다음 단계로 넘어갑니다.

3단계. 마법사 완료

마법사를 완료합니다. 결과적으로 마법사는 다음을 수행합니다.

- Kaspersky Industrial CyberSecurity for Nodes 5.0에 대한 새 정책이 생성됩니다.

  이 정책은 Kaspersky Industrial CyberSecurity for Nodes 및 Kaspersky Endpoint Agent 이전 버전의 설정을 결합합니다. 새 정책 이름은 병합 전의 Kaspersky Industrial CyberSecurity for Nodes 정책 이름에 "KICS에서 복사됨" 문구가 추가된 것입니다. 새 정책은 *비활성* 상태입니다. 새로 병합된 정책을 적용하려면 활성화합니다.

  Kaspersky Anti Targeted Attack Platform(EDR) 솔루션을 위해 Kaspersky Endpoint Agent에서 Kaspersky Industrial CyberSecurity for Nodes로 마이그레이션하는 경우, 컴퓨터를 KATA 서버로 연결할 때 오류가 발생할 수도 있습니다. 그 이유는 마이그레이션 마법사가 다음 정책 설정을 건너뛰고 마이그레이션하지 않기 때문입니다.

  - 연결 설정 수정 금지("잠금").

    설정은 기본적으로 수정할 수 있습니다("자물쇠"가 열려 있음). 따라서 설정이 컴퓨터에서 적용되지 않습니다. 설정 수정을 금지하고 "자물쇠"를 닫아야 합니다.

  - 암호화 컨테이너.

    KATA 서버로 연결하기 위해 양방향 인증을 사용하는 경우, 암호화 컨테이너를 다시 추가해야 합니다. 마이그레이션 마법사는 서버의 TLS 인증서를 올바로 마이그레이션합니다.

- Kaspersky Industrial CyberSecurity for Nodes 5.0에 대한 새 작업이 생성됩니다.

  새 작업에는 마이그레이션된 Kaspersky Industrial CyberSecurity for Nodes 작업의 설정과 Kaspersky Industrial CyberSecurity for Nodes 5.0에 도입된 새 설정이 포함됩니다. 새 작업 이름은 병합 전의 Kaspersky Industrial CyberSecurity for Nodes 작업 이름에 "KICS에서 복사됨" 문구가 추가된 것입니다.

SIEM 통합

Kaspersky Industrial CyberSecurity for Nodes를 사용하면 SIEM 시스템에 연결하여 잠재적 위협 분석 및 대응을 위해 이벤트를 보낼 수 있습니다. SIEM 시스템을 사용하면 보안 위협이 조직에 피해를 주기 전에 탐지, 분석, 제거할 수 있습니다.

SIEM 통합을 사용하면 Windows 운영 체제가 실행되는 보호 대상 장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes에서 다음 Kaspersky Industrial CyberSecurity for Nodes 이벤트를 SIEM 서버로 보낼 수 있습니다:

- 보안 이벤트. 이벤트를 JSON Lines 및 Syslog(RFC 5424) 형식으로 변환할 수 있습니다. 애플리케이션에서 SIEM 서버로 보낼 이벤트를 선택할 수 있습니다.
- Windows 이벤트 로그 이벤트. 애플리케이션이 Windows 이벤트 로그 이벤트를 JSON Lines 형식으로 변환합니다. 필요하다면 필터링 규칙을 사용하여 전송된 원격 측정에서 이벤트를 제외할 수 있습니다.

  Kaspersky Industrial CyberSecurity for Nodes는 Windows XP를 실행하는 보호 대상 장치에 설치된 경우 Windows 이벤트 로그 이벤트 전송을 지원하지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes는 SIEM 서버로 이벤트를 전송하기 위해 다음 프로토콜을 지원합니다:

- TCP
- UDP
- HTTP/HTTPS(Windows 이벤트 로그 이벤트 전송 전용)

SIEM 통합 설정에는 다음 단계가 포함됩니다.

1. **SIEM 통합 구성 요소 설치**

   설치 패키지 설정이나 설치 마법사에서, 또는 Windows 제어판의 애플리케이션 구성 요소 집합 변경을 통해, 설치할 애플리케이션 구성 요소 선택 단계에서 다음을 선택합니다: **전체 기능** → **Endpoint Agent** → **SIEM 통합**.

2. **SIEM 통합 구성 요소 활성화 및 구성**

   기본적으로 SIEM 통합은 사용되지 않습니다. SIEM 통합을 활성화 및 비활성화하고 관련 설정을 구성할 수 있습니다.

   여러 SIEM 서버에 대한 연결을 구성하여 SIEM 서버로의 이벤트 전송 실패 위험을 줄일 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes가 목록에서 첫 번째 SIEM 서버에 연결합니다. 연결 시도가 실패하면 Kaspersky Industrial CyberSecurity for Nodes는 목록에 있는 다른 서버에 하나씩 연결을 시도합니다. Kaspersky Industrial CyberSecurity for Nodes는 시스템 감사 이벤트를 사용하여 사용자에게 SIEM 서버 연결 시도의 실패와 SIEM 서버로 이벤트 전송 중 발생한 오류를 알립니다.

   Kaspersky Security Center 관리 콘솔에서 SIEM 통합을 구성하는 방법

   1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
   2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
   3. **원격 측정 수집 서버** 섹션을 선택합니다.

4. **SIEM 통합** 블록에서 **설정** 버튼을 클릭합니다.
   SIEM 통합 창이 열립니다.

5. **SIEM 통합** 확인란을 선택합니다.

6. 보안 이벤트를 전송하도록 SIEM 서버 연결을 구성합니다.

   a. **보안 이벤트 전송 설정** 탭으로 갑니다.

   b. **추가** 버튼을 클릭합니다.

   c. **서버 추가** 창이 열리면 SIEM 서버 주소(IPv4, DNS), 포트 및 연결 프로토콜을 입력합니다.

   d. **TCP 연결 보안 설정** 버튼을 클릭합니다.

   e. 이렇게 하면 **TCP 연결 보안 설정** 창이 열립니다. 해당 창에서 SIEM 서버 연결 설정을 관리합니다(아래 표 참조).

   f. 필요하다면 **SIEM 서버로 이벤트 전송 설정** 블록에서 **원격 syslog 서버로 전송된 이벤트의 로컬 복사본 제거** 확인란을 선택합니다. 이 확인란을 선택하면 애플리케이션은 SIEM 서버에 성공적으로 게시된 이벤트의 로컬 복사본을 삭제합니다. 이 모드는 성능이 낮은 장치에서 권장됩니다. 확인란을 선택 해제하면 애플리케이션이 SIEM 서버에 이벤트를 전송하기만 합니다. 로그 복사본은 계속해서 로컬에 저장됩니다. 기본적으로 확인란의 선택이 취소됩니다.

      애플리케이션은 보안 로그의 로컬 버전을 절대로 삭제하지 않습니다.

   g. **이벤트 형식** 블록에서 애플리케이션 이벤트를 SIEM 서버로 보낼 수 있도록 변환할 형식을 선택합니다.

      - **정형 데이터로 이벤트 변환**(기본 값). 애플리케이션이 이벤트를 Syslog 형식(RFC 5424)으로 전송합니다.
      - **JSON으로 이벤트 변환**. 애플리케이션이 이벤트를 JSON Lines 형식으로 전송합니다.

      사용된 SIEM 서버의 구성에 따라 이벤트 형식을 선택하는 것이 좋습니다.

7. Windows 이벤트 로그 이벤트를 전송하도록 SIEM 서버 연결을 구성합니다.

   a. **Windows 이벤트 전송 설정** 탭으로 갑니다.

   b. Kaspersky Industrial CyberSecurity for Nodes와 SIEM 서버 간의 연결 암호화를 활성화해야 하는 경우, **SIEM 서버 연결 설정**에서 **TLS 암호화 사용** 확인란을 선택합니다.

   c. **추가** 버튼을 클릭합니다.

   d. **SIEM 서버** 창이 열리면 SIEM 서버 주소(IPv4, DNS), 포트 및 연결 프로토콜을 입력합니다.

   e. **SIEM 서버 연결 설정** 버튼을 클릭합니다.

   f. 이렇게 하면 **SIEM 서버 연결 설정** 창이 열립니다. 해당 창에서 SIEM 서버 연결 설정을 관리합니다(아래 표 참조).

g. 필요하다면 **데이터 전송 설정** 블록에서 **최대 이벤트 전송 지연(초)** 설정을 구성합니다. 지정된 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 같은 서버에 연결을 시도하거나, 서버가 여러 개라면 목록의 다음 서버에 연결합니다. 기본 설정은 30초입니다.

애플리케이션이 Windows 이벤트 로그 이벤트를 SIEM에 JSON Lines 형식으로 전송합니다.

8. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

9. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 SIEM 통합을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **원격 측정 수집 서버** 섹션을 선택합니다.

5. **SIEM 통합** 블록에서 **구성** 버튼을 클릭합니다.

SIEM 통합 창이 열립니다.

6. **SIEM 통합 사용** 확인란을 선택합니다.

7. 보안 이벤트를 전송하도록 SIEM 서버 연결을 구성합니다.

a. **보안 이벤트 전송 설정** 탭으로 갑니다.

b. **추가** 버튼을 클릭합니다.

c. **SIEM 서버** 창이 열리면 SIEM 서버 주소(IPv4, DNS), 포트 및 연결 프로토콜을 입력합니다.

d. **연결 보호** 블록에서 **SIEM 서버 연결 설정** 링크를 클릭합니다.

e. 이렇게 하면 **SIEM 서버 연결 설정** 창이 열립니다. 해당 창에서 SIEM 서버 연결 설정을 관리합니다(아래 표 참조).

f. **이벤트 형식** 섹션에서 애플리케이션 이벤트를 SIEM 서버로 보낼 수 있도록 변환할 형식을 지정합니다.

- **정형 데이터로 이벤트 변환**(기본 값). 애플리케이션이 이벤트를 Syslog 형식(RFC 5424)으로 전송합니다.
- **JSON으로 이벤트 변환**. 애플리케이션이 이벤트를 JSON Lines 형식으로 전송합니다.

사용된 SIEM 서버의 구성에 따라 이벤트 형식을 선택하는 것이 좋습니다.

g. 필요하다면 **연결 설정** 블록에서 **원격 syslog 서버로 전송된 이벤트의 로컬 복사본 제거** 확인란을 선택합니다. 이 확인란을 선택하면 애플리케이션은 SIEM 서버에 성공적으로 게시된 이벤트의 로컬 복사본을 삭제합니다. 이 모드는 성능이 낮은 장치에서 권장됩니다. 확인란을 선택 해제하면 애플리케이션이 SIEM 서버에 이벤트를 전송하기만 합니다. 로그 복사본은 계속해서 로컬에 저장됩니다. 기본적으로 확인란의 선택이 취소됩니다.

애플리케이션은 보안 로그의 로컬 버전을 절대로 삭제하지 않습니다.

8. Windows 이벤트 로그 이벤트를 전송하도록 SIEM 서버 연결을 구성합니다.

a. **Windows 이벤트 전송 설정** 탭으로 갑니다.

b. **추가** 버튼을 클릭합니다.

c. **SIEM 서버** 창이 열리면 SIEM 서버 주소(IPv4, DNS), 포트 및 연결 프로토콜을 입력합니다.

d. **연결 보호** 블록에서 **SIEM 서버 연결 설정** 링크를 클릭합니다.

e. 이렇게 하면 **SIEM 서버 연결 설정** 창이 열립니다. 해당 창에서 SIEM 서버 연결 설정을 관리합니다(아래 표 참조).

f. 필요하다면 **연결 설정** 블록에서 **최대 이벤트 전송 지연(초)** 설정을 구성합니다. 지정된 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 같은 서버에 연결을 시도하거나, 서버가 여러 개라면 목록의 다음 서버에 연결합니다. 기본 설정은 30초입니다.

애플리케이션이 Windows 이벤트 로그 이벤트를 SIEM에 JSON Lines 형식으로 전송합니다.

9. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

애플리케이션 콘솔에서 SIEM 통합을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **Endpoint Agent 원격 측정** → SIEM 통합 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.
속성: SIEM 통합 창이 열립니다.

3. **SIEM 통합** 확인란을 선택합니다.

4. 보안 이벤트를 전송하도록 SIEM 서버 연결을 구성합니다.

a. **보안 이벤트 전송 설정** 탭으로 갑니다.

b. **추가** 버튼을 클릭합니다.

c. **서버 추가** 창이 열리면 SIEM 서버 주소(IPv4, DNS), 포트 및 연결 프로토콜을 입력합니다.

d. **TCP 연결 보안 설정** 버튼을 클릭합니다.

e. 이렇게 하면 **TCP 연결 보안 설정** 창이 열립니다. 해당 창에서 SIEM 서버 연결 설정을 관리합니다(아래 표 참조).

f. 필요하다면 **SIEM 서버로 이벤트 전송 설정** 블록에서 **원격 syslog 서버로 전송된 이벤트의 로컬 복사본 제거** 확인란을 선택합니다. 이 확인란을 선택하면 애플리케이션은 SIEM 서버에 성공적으로 게시된 이벤트의 로컬 복사본을 삭제합니다. 이 모드는 성능이 낮은 장치에서 권장됩니다. 확인란을 선택 해제하면 애플리케이션이 SIEM 서버에 이벤트를 전송하기만 합니다. 로그 복사본은 계속해서 로컬에 저장됩니다. 기본적으로 확인란의 선택이 취소됩니다.

애플리케이션은 보안 로그의 로컬 버전을 절대로 삭제하지 않습니다.

g. **이벤트 형식** 블록에서 애플리케이션 이벤트를 SIEM 서버로 보낼 수 있도록 변환할 형식을 선택합니다.

- **정형 데이터로 이벤트 변환**(기본 값). 애플리케이션이 이벤트를 Syslog 형식(RFC 5424)으로 전송합니다.
- **JSON으로 이벤트 변환**. 애플리케이션이 이벤트를 JSON Lines 형식으로 전송합니다.

사용된 SIEM 서버의 구성에 따라 이벤트 형식을 선택하는 것이 좋습니다.

5. Windows 이벤트 로그 이벤트를 전송하도록 SIEM 서버 연결을 구성합니다.

a. **Windows 이벤트 전송 설정** 탭으로 갑니다.

b. Kaspersky Industrial CyberSecurity for Nodes와 SIEM 서버 간의 연결 암호화를 활성화해야 하는 경우, **SIEM 서버 연결 설정**에서 **TLS 암호화 사용** 확인란을 선택합니다.

c. **추가** 버튼을 클릭합니다.

d. **SIEM 서버** 창이 열리면 SIEM 서버 주소(IPv4, DNS), 포트 및 연결 프로토콜을 입력합니다.

e. **SIEM 서버 연결 설정** 버튼을 클릭합니다.

f. 이렇게 하면 **SIEM 서버 연결 설정** 창이 열립니다. 해당 창에서 SIEM 서버 연결 설정을 관리합니다(아래 표 참조).

g. 필요하다면 **데이터 전송 설정** 블록에서 **최대 이벤트 전송 지연(초)** 설정을 구성합니다. 지정된 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 같은 서버에 연결을 시도하거나, 서버가 여러 개라면 목록의 다음 서버에 연결합니다. 기본 설정은 30초입니다.

애플리케이션이 Windows 이벤트 로그 이벤트를 SIEM에 JSON Lines 형식으로 전송합니다.

6. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

SIEM 서버 연결 설정

파라미터	설명
시간 초과(초)	최대 SIEM 서버 응답 시간 초과. 제한 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 다른 SIEM 서버에 연결을 시도합니다.
서버 TLS 인증서	SIEM 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. SIEM 관리 인터페이스를 사용하여 TLS 인증서를 얻을 수 있습니다.
양방향 인증 사용	Kaspersky Industrial CyberSecurity for Nodes와 SIEM 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 SIEM 설정에서 양방향 인증을 활성화한 다음 암호화 컨테이너를 가져오고 암호를 설정하여 암호화 컨테이너를 보호해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. SIEM 설정을 구성한 후 Kaspersky Industrial CyberSecurity for Nodes 설정에서 확인란을 사용하여 양방향 인증을 활성화하고 암호로 보호되는 암호화 컨테이너를 로드해야 합니다. 암호화 컨테이너는 암호로 보호되어야 합니다. 빈 암호로 암호화 컨테이너를 추가할 수 없습니다.

SIEM로 전송할 이벤트 필터링

성능을 개선하고 SIEM 서버로 데이터 전송을 최적화하기 위해, 원격 측정에서 개별 Windows 이벤트 로그 이벤트를 수동으로 추가하거나 제외할 수 있습니다. 그 예로, Sysmon 이벤트를 제외할 수 있습니다.

SIEM 통합 구성 요소가 올바르게 작동하도록 필요한 이벤트 전송을 활성화합니다. 기본적으로 모든 이벤트 전송은 비활성화되어 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 SIEM 원격 측정을 위한 WEL 이벤트 필터링에 최대 1,500개의 포함 및 예외 규칙을 지원합니다.

Kaspersky Security Center 관리 콘솔에서 SIEM로 전송할 이벤트 목록을 만드는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **보충** 섹션으로 갑니다.
4. **SIEM 원격 측정 설정** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 표시되면 SIEM로 전송할 이벤트 필터를 구성합니다.

   표준 *Application*, *Security*, *System* 로그에 대한 이벤트 필터링을 구성하거나 다른 로그를 수동으로 추가할 수 있습니다.

   a. 로그 속성을 열거나 **추가** 버튼을 클릭하고 로그 이름을 입력합니다.

   b. 이벤트 전송 모드를 선택합니다.

   - **모든 이벤트 전송**. 이 모드에서는 애플리케이션이 예외 규칙에 추가된 이벤트를 제외하고 Windows 로그의 모든 이벤트를 전송합니다.
   - **선택한 이벤트만 전송**. 이 모드에서는 애플리케이션이 포함 규칙에 추가된 이벤트만 전송합니다.

   c. 관련 이벤트 전송 모드에 대한 예외 규칙 또는 포함 규칙 목록을 만듭니다.

   규칙을 추가하려면 Windows 이벤트 로그에서 이벤트 ID를 지정해야 합니다. 하나의 규칙에 여러 이벤트 ID의 목록을 만들 수 있습니다. 여러 이벤트 ID를 지정하려면 쉼표(`,`)로 구분하십시오.

   d. 필요한 경우 로그 이름 옆의 확인란을 사용하여 이벤트 기록을 활성화합니다.

6. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

웹 콘솔에서 SIEM로 전송할 이벤트 목록을 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보충** 섹션을 선택합니다.

5. **원격 측정 설정** 블록에서 **구성** 버튼을 클릭합니다.
   원격 측정 설정 창이 열립니다.

6. **SIEM 원격 측정** 탭으로 갑니다.

7. SIEM로 전송할 이벤트 필터를 구성합니다.

   표준 *Application*, *Security*, *System* 로그에 대한 이벤트 필터링을 구성하거나 다른 로그를 수동으로 추가할 수 있습니다.

   a. 로그 속성을 열거나 **추가** 버튼을 클릭하고 로그 이름을 입력합니다.

   b. 이벤트 전송 모드를 선택합니다.

   - **모든 이벤트 전송**. 이 모드에서는 애플리케이션이 예외 규칙에 추가된 이벤트를 제외하고 Windows 로그의 모든 이벤트를 전송합니다.
   - **선택한 이벤트만 전송**. 이 모드에서는 애플리케이션이 포함 규칙에 추가된 이벤트만 전송합니다.

   c. 관련 이벤트 전송 모드에 대한 예외 규칙 또는 포함 규칙 목록을 만듭니다.

   규칙을 추가하려면 Windows 이벤트 로그에서 이벤트 ID를 지정해야 합니다. 하나의 규칙에 여러 이벤트 ID의 목록을 만들 수 있습니다. 여러 이벤트 ID를 지정하려면 쉼표(`,`)로 구분하십시오.

   d. 필요한 경우 로그 이름 옆의 토글 스위치를 사용하여 이벤트 기록을 활성화합니다.

8. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

원격 측정 이벤트 필터링 규칙 내보내기 및 가져오기

Kaspersky Industrial CyberSecurity for Nodes에서 원격 측정 이벤트 필터링 규칙을 사용하여 JSON 파일을 가져오고 내보낼 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 SIEM 원격 측정을 위한 WEL 이벤트 필터링에 최대 1,500개의 포함 및 예외 규칙을 지원합니다.

이벤트 필터링 규칙이 컴퓨터에 이미 있는 경우, Kaspersky Industrial CyberSecurity for Nodes는 가져오기를 수행할 때 이 규칙을 교체합니다.

예를 들어 예외 목록을 JSON 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 이벤트 ID를 여러 개 추가할 수 있습니다. 내보내기 및 가져오기 기능을 사용하여 이벤트 필터를 백업하거나 목록을 다른 서버로 마이그레이션할 수도 있습니다.

Kaspersky Security Center 관리 콘솔에서 이벤트 필터링 규칙을 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **보충** 섹션으로 갑니다.
4. **SIEM 원격 측정** 블록에서 **설정** 버튼을 클릭합니다.
5. 이벤트 필터를 내보내려면,
   a. 내보낼 필터를 포함하는 이벤트 로그를 선택합니다.
   b. 버튼을 클릭하여 마우스 오른쪽 메뉴를 열고 **내보내기**를 선택합니다.
   c. 창이 열리면 신뢰하는 이벤트 필터를 내보낼 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   d. 파일을 저장합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 이벤트 필터를 JSON 파일로 내보냅니다.
6. 이벤트 필터를 가져오려면,
   a. 버튼을 클릭하여 마우스 오른쪽 메뉴를 열고 **가져오기**를 선택합니다.
   b. 창이 열리면 이벤트 필터를 가져올 JSON 파일을 선택합니다.
   c. 파일을 엽니다.
7. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Security Center 웹 콘솔에서 이벤트 필터링 규칙을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보충** 섹션을 선택합니다.
5. **원격 측정 설정** 블록에서 **구성** 버튼을 클릭합니다.
   원격 측정 설정 창이 열립니다.
6. **SIEM 원격 측정** 탭으로 갑니다.
7. 이벤트 필터를 내보내려면,
   a. 내보낼 필터를 포함하는 이벤트 로그를 선택합니다.
   b. **내보내기** 버튼을 클릭합니다.

c. 창이 열리면 신뢰하는 이벤트 필터를 내보낼 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

d. 파일을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes는 이벤트 필터를 JSON 파일로 내보냅니다.

8. 이벤트 필터를 가져오려면,

a. **가져오기** 버튼을 클릭합니다.

b. 창이 열리면 이벤트 필터를 가져올 JSON 파일을 선택합니다.

c. 파일을 엽니다.

9. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

Kaspersky Industrial CyberSecurity for Nodes 애플리케이션 콘솔에서 이벤트 필터링 규칙을 내보내거나 가져오는 방법

1. 애플리케이션 콘솔 트리에서 **원격 측정 설정** 노드를 선택합니다.

2. **SIEM 원격 측정** 블록에서 **설정** 버튼을 클릭합니다.

3. 이벤트 필터를 내보내려면,

a. **내보내기** 버튼을 클릭합니다.

b. 창이 열리면 이벤트 필터를 내보낼 JSON 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

c. 파일을 저장합니다.

Kaspersky Industrial CyberSecurity for Nodes는 이벤트 필터를 JSON 파일로 내보냅니다.

4. 이벤트 필터를 가져오려면,

a. **가져오기** 버튼을 클릭합니다.

b. 표시되는 대화 상자에서 SIEM 원격 측정 설정의 수정 사항을 확인합니다.

c. 이벤트 필터를 가져올 JSON 파일을 선택합니다.

d. 파일을 엽니다.

5. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

명령줄 인터페이스를 사용하여 원격 측정 이벤트 필터링 규칙을 내보내거나 가져올 수도 있습니다.

Sigma 규칙을 사용한 이상 행위 탐지

이 기능은 Windows 7 이상 또는 Windows Server 2008 R2 이상을 실행하는 컴퓨터에서 EDR Optimum 및 ICS 원격 측정 라이센스 개체와 함께 활성화된 Kaspersky Industrial CyberSecurity for Nodes 라이센스 키가 있는 경우 사용할 수 있습니다.

Sigma 규칙을 사용하여 이상 행위를 탐지하려면 실시간 파일 보호, 익스플로잇 방지, 복원 엔진 구성 요소를 활성화해야 합니다.

*Sigma*는 Kaspersky Industrial CyberSecurity for Nodes가 내부 이벤트 및 이벤트 로그의 데이터를 분석하기 위해 사용하는 이상 행위 탐지 규칙의 설명 형식입니다. Sigma 형식으로 작성된 규칙을 Sigma 규칙이라고 합니다.

Sigma 규칙은 YAML로 작성되며 통합 구조를 갖습니다. 이를 통해 특수하게 만들어진 변환기가 Sigma 규칙을 기반으로 하는 다양한 SIEM 시스템의 구문으로 규칙을 생성할 수 있습니다. 각 Sigma 규칙은 별도의 YAML 파일에 저장됩니다.

Sigma 규칙 구조

이 표에는 Kaspersky Industrial CyberSecurity for Nodes가 해석하는 Sigma 규칙의 섹션 및 속성에 대한 기본 정보가 포함되어 있습니다. 자세한 내용을 보려면 이 링크를 확인하십시오.

속성 값은 대소문자를 구분합니다. 예를 들어 Kaspersky Industrial CyberSecurity for Nodes는 AnyDesk.exe 및 AnyDesk.exe 실행 파일의 이름을 다르게 처리합니다.

<table>
<tr><th>특성/섹션</th><th>필수</th><th>설명</th></tr>
<tr><td>logsource</td><td>예</td><td>
이 섹션에서는 애플리케이션이 이상 행위를 검색할 이벤트의 경로를 정의할 수 있습니다. 이 섹션의 주요 속성은 category, product, service 입니다.
Kaspersky Industrial CyberSecurity for Nodes가 지원하는 이벤트 경로
Kaspersky Industrial CyberSecurity for Nodes가 지원하는 이벤트 경로
<table>
<tr><th>경로(logsource)</th><th>이벤트</th></tr>
<tr><td>category: process_creation
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 1에 해당하는 내용의 내부 프로세스 시작 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: driver_load
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 6에 해당하는 내용의 내부 드라이버 로드 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: image_load
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 7에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: registry_event
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 12, EventID 13, EventID 14에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: dns_query
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 22에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: file_rename
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Windows 추적 서비스 공급자 Microsoft-Windows-Kernel-File 로그의 이벤트에 해당하는 내용의 내부 이벤트를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: file_event
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 11에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>product: windows
service: application</td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/애플리케이션 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>product: windows
service: security</td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/보안 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>product: windows
service: system</td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/시스템 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>category: chronicle_journal
product: deltav</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Emerson DeltaV 시스템 이벤트 로그의 정규화된 데이터와 관련된 내부 이벤트 인스턴스를 분석합니다.
출처 이벤트는 외부 이벤트 로그에 연결되지 않습니다.</td></tr>
<tr><td>product: windows
service: powershell-classic</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Windows PowerShell 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>product: windows
service: powershell</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-PowerShell/작업 로그에서 이벤트를 분석합니다.</td></tr>
</table>
Microsoft Windows 7의 category: dns_query, service: powershell-classic, service: powershell 공급자에서는 일부 내부 이벤트가 누락되었거나 이벤트에서 일부 필드 또는 필요한 데이터가 누락될 수 있습니다. 결과적으로 Sigma 규칙이 트리거되지 않을 수 있습니다.
이 링크에서 더 확인할 수 있습니다.
</td></tr>
<tr><td>title</td><td>예</td><td>탐지된 항목을 나타내는 규칙 이름입니다. 최대 길이는 256자입니다.
예:
title: 새로운 RAT 서비스 생성</td></tr>
<tr><td>id</td><td>아니오</td><td>규칙의 전역 고유 식별자입니다. 예:
id: 929a690e-bef0-4204-a928-ef5e620d6fcc</td></tr>
<tr><td>status</td><td>아니오</td><td>규칙 상태. 가능한 값: stable, test, experimental, deprecated, unsupported.
예:
status: test</td></tr>
<tr><td>description</td><td>아니오</td><td>규칙 및 규칙이 탐지할 수 있는 악성 활동에 대한 설명입니다. 최대 길이는 65,535자입니다.
예:
description: 새로운 원격 유틸리티 호스트 애플리케이션 서비스 설치를 탐지합니다.</td></tr>
<tr><td>license</td><td>아니오</td><td>SPDX ID 사양에 따른 라이센스 ID입니다. 지정된 라이센스 유형의 조건에 따라 규칙이 게시되었습니다.</td></tr>
<tr><td>author</td><td>아니오</td><td>규칙의 작성자를 나타내는 지정자입니다. 예: 이름과 성, 닉네임, 소셜 네트워크 ID.</td></tr>
</table>

reference	아니오	규칙을 가져온 출처에 대한 링크입니다. 블로그 기사나 백서를 예로 들 수 있습니다.
date	아니오	규칙이 만들어진 날짜는 YYYY/MM/DD 형식입니다.
modified	아니오	다음 규칙 속성 중 하나가 변경된 날짜(YYYY/MM/DD 형식): `title`, `status`, `logsource`, `detection`, `level`.
tags	아니오	규칙 분류를 위한 태그입니다. 이 링크에서 더 확인할 수 있습니다.

category	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 제품의 카테고리를 정의합니다. 예: 방화벽, 인터넷, 안티바이러스, 일반 등.
		
		`logsource:`
		`  category: firewall`

product	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 소프트웨어 제품 또는 운영 체제를 정의합니다. 예:
		
		`logsource:`
		`  product: Windows`

service	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 서비스를 정의합니다. 예:
		
		`logsource:`
		`  service: AppLocker`

definition	아니오	애플리케이션이 이상 행위를 검색할 이벤트 로그의 세부 출처에 관한 설명입니다.
detection	예	이 섹션은 이벤트 로그에서 이상 행위를 검색하기 위한 하나 이상의 기준과 규칙 트리거 조건을 포함합니다. 검색 기준으로 리스트나 딕셔너리, 또는 이 둘의 조합을 사용할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 `windash` 값 수정자를 지원하지 않습니다.

목록	아니오	이벤트 로그에 있는 파라미터 값의 목록으로, 논리합으로 결합합니다. 예:
		
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: `OriginalFileName='AnyDesk.exe'` 또는 `OriginalFileName='TeamViewer.exe'`.

딕셔너리	아니오	*이벤트 로그 파라미터 - 값* 쌍. 둘은 논리곱으로 연결됩니다. 예:
		
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: EventLog='Security' AND Event ID=517.

리스트와 딕셔너리의 조합	아니오	이벤트 로그 설정 값과 딕셔너리로 구성된 리스트입니다. 예:
		
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: EventLog='Security' AND (Event ID=517 OR Event ID=1102)

condition	예	규칙 트리거 조건. 예:
		
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

fields	아니오	분석가가 이벤트의 후속 분석을 위해 관심을 가질 수 있는 이벤트 로그의 열.

falsepositives	아니오	규칙을 잘못 트리거할 수 있다고 알려진 시나리오 목록입니다. 예:
		
		`falsepositives:`
		`- 시스템 관리자의 유틸리티 사용`

level	아니오	규칙을 사용하여 찾을 수 있는 이상 행위의 심각도를 나타내는 지표입니다. 가능한 값: `informational`, `low`, `medium`, `high`, `critical`.

Sigma 규칙의 예

```
title: CertUtil.exe를 사용한 파일 다운로드
id: 89346938-3b2f-46c7-bb38-b9f244e3fad0
status: test
description: Detects file downloads using CertUtil.exe.
```

```
references:
  - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
author: Kaspersky
date: 2024-05-22
tags:
  - attack.defense_evasion
  - attack.t1027
logsource:
  category: process_creation
  product: windows
detection:
  selection_image:
    - Image|endswith: '\certutil.exe'
    - OriginalFileName: 'CertUtil.exe'
  selection_http:
    CommandLine|contains: 'http'
condition: all of selection_*
falsepositives:
  - Legitimate actions of the system administrator.
level: low
```

*Sigma 규칙 컬렉션*은 유사한 이벤트를 정의하는 Sigma 규칙 집합입니다.

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky에서 제공하는 Sigma 규칙 컬렉션과 애플리케이션 데이터베이스, 사용자가 생성한 Sigma 규칙 컬렉션을 사용하여 내부 이벤트 및 이벤트 로그의 데이터를 분석하고 이상 행위를 찾습니다.

애플리케이션 버전에 따라 Kaspersky Industrial CyberSecurity for Nodes는 아래 표에 나열된 사전 정의된 Sigma 규칙 모음의 사용을 지원합니다.

사전 정의된 Sigma 규칙 모음

Sigma 규칙 모음	애플리케이션 버전	
	4.5	5.0
원격 관리 도구(RAT) 탐지	✓	✓
Emerson DeltaV용 이상 행위 탐지	✓	✓
사용자 계정 컨트롤(UAC)	✓	✓
Siemens SIMATIC WinCC, Siemens TIA Portal, Siemens SIMATIC STEP 7용 이상 행위 탐지	✓	✓
Yokogawa CENTUM VP용 이상 행위 탐지	✓	✓
네트워크 및 이동식 미디어를 통한 파일 공유 감사	–	✓

일부 시그마 규칙을 사용할 때 애플리케이션은 보호 중인 컴퓨터의 보안 감사 정책을 변경할 수 있습니다(로컬 Windows 보안 정책의 일부).

시그마 규칙을 사용한 이상 행위 탐지의 특별 고려 사항 및 제한 사항

일부 Sigma 규칙 컬렉션은 감사 정책 설정을 수정해야 제대로 작동합니다. 애플리케이션의 동작은 컴퓨터가 도메인에 속하는지 여부에 따라 다릅니다.

- 컴퓨터가 도메인에 속하지 않으면 애플리케이션이 도메인 그룹 정책 설정을 수정하지 않습니다. 이러한 컴퓨터를 도메인에서 제외하거나 도메인 그룹 정책 설정을 직접 구성할 수 있습니다.
- 컴퓨터가 도메인에 속하지 않으면 Sigma 규칙 컬렉션이 올바르게 작동하는 데 필요한 경우 애플리케이션이 로컬 정책 설정을 자동으로 편집합니다.

로컬 정책 설정을 자동으로 수정하려면 로컬 보안 감사 정책 변경 사항 자동 적용 기능을 사용해야 합니다. 이 기능이 중지되어 있는 경우 Sigma 규칙이 제대로 작동하도록 로컬 정책 설정을 수동으로 구성하는 단계를 수행하십시오.

애플리케이션은 Sigma 규칙의 사용자 지정 컬렉션에 대한 로컬 정책 설정을 수정하지 않습니다. 로컬 정책 설정을 수동으로 구성해야 사용자 지정 Sigma 규칙이 제대로 작동합니다.

Sigma 규칙 컬렉션이 중지되면 애플리케이션은 로컬 정책 설정을 원래 값으로 되돌리지 않습니다. 필요하다면 원래 로컬 정책 설정을 수동으로 복원할 수 있습니다.

Sigma 규칙을 사용한 이상 행위 탐지 기능에는 다음 제한 사항이 있습니다.

- "DeltaV 호스트에서 Windows 이벤트 로그 수정 또는 삭제" Sigma 규칙이 작동하려면 "Sigma 규칙을 사용한 이상 행위 탐지" 구성 요소를 설치한 직후 컴퓨터를 다시 시작하거나 **Windows 이벤트 로그 서비스를 중지했다가 다시 시작해야 합니다**.

  1. Windows 서비스 애플리케이션(service.msc)을 시작합니다.
  2. 서비스 목록에서 Windows 이벤트 로그를 찾습니다.
  3. Windows 이벤트 로그 서비스의 마우스 오른쪽 메뉴에서 **중지**를 선택해 서비스를 중지합니다.
  4. Windows 이벤트 로그 서비스의 마우스 오른쪽 메뉴에서 **시작**을 선택해 서비스를 시작합니다.

- 다음 값 수정자는 지원하지 않습니다: `base64offset`, `cidr`, `lt`, `windash`.
- 정규식은 지원하지 않습니다.
- 와일드카드 문자의 이스케이프는 지원하지 않습니다.
- 이 애플리케이션은 `?` 와일드 카드를 `*`로 사용합니다.
- "`condition: not selection`" 구성은 지원하지 않습니다. 그러나 "`condition: selection and not filter`" 구성은 지원됩니다.
- Windows 이벤트 로그에서 이상 행위 검색 기준으로 지정된 `EventID` 파라미터 값을 하나 이상 갖지 않는 규칙은 지원하지 않습니다.
- 파일 작업을 설명하는 시그마 규칙은 리포트에 처음 50건의 탐지가 포함됩니다. 프로세스가 경로가 유사한 파일에 대해 작업을 수행하면 각 프로세스에 대해 별도로 탐지가 계산됩니다.
- 애플리케이션은 몇 가지 제한과 함께 Windows XP 및 Windows Server 2003 컴퓨터에서 Sigma 규칙을 지원합니다. 이러한 운영 체제를 실행하는 컴퓨터에서 탐지의 경고 세부 정보를 열려고 하면 *경고 세부 정보를 열지 못했습니다. 가능한 사유: 호스트 오프라인, 네트워크 문제, 경고 저장소 시간 만료* 오류와 함께 실패할 수 있습니다. Kaspersky Industrial CyberSecurity for Networks를 사용하여 경고 세부 정보를 열 수 있습니다.
- 애플리케이션은 Siemens SIMATIC PCS 7 버전 9.0 SP1 이상과의 통합을 지원합니다.
- 네트워크 및 이동식 미디어를 통한 파일 공유 감사 사전 정의 컬렉션의 "이동식 드라이브 파일 쓰기 탐지" Sigma 규칙이 제대로 작동하려면 컴퓨터를 다시 시작해야 합니다.

Sigma 규칙을 사용한 이상 행위 탐지 활성화

Kaspersky Security Center 관리 콘솔에서 Sigma 규칙을 사용한 이상 행위 탐지 활성화

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션을 선택합니다.
4. **Sigma 규칙을 사용한 이상 행위 탐지** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **Sigma 규칙을 사용한 이상 행위 탐지** 확인란을 선택합니다.
6. 하나 이상의 Sigma 규칙 컬렉션을 추가합니다.
   a. **추가** 버튼을 클릭합니다.
   규칙 컬렉션 추가 창이 열립니다.
   b. **규칙 컬렉션 선택** 드롭다운 목록을 사용해 다음 중 하나를 수행합니다.
   - 사전 정의된 Sigma 규칙 컬렉션 중 하나를 선택합니다.
     사전 정의된 Sigma 규칙 컬렉션이 표시되지 않으면 애플리케이션이 EDR Optimum 및 ICS 원격 측정 개체가 있는 라이센스 키로 활성화되었는지 확인하십시오. *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 실행하여 사전 정의된 컬렉션을 업데이트할 수도 있습니다.

     > 사전 정의된 Sigma 규칙 모음을 추가할 때는 선택한 모음이 관리 중인 기기에 설치된 모든 버전의 Kaspersky Industrial CyberSecurity for Nodes에서 지원되는지 확인해야 합니다.

   - **사용자 지정 규칙 컬렉션** 옵션을 선택하여 Sigma 규칙의 사용자 지정 컬렉션을 추가합니다.
     사용자 지정 Sigma 규칙 컬렉션을 추가하는 경우 해당 필드에 컬렉션의 고유 이름을 입력합니다. 생성된 사용자 지정 컬렉션에 포함된 규칙이 없습니다.

   c. **확인**을 누릅니다.
   새로운 컬렉션이 목록에 표시됩니다. 기본적으로 추가된 Sigma 규칙 컬렉션이 사용됩니다. 필요한 경우 컬렉션 이름 왼쪽에 있는 확인란을 사용하여 Sigma 규칙 컬렉션의 상태를 관리합니다.
7. 필요하다면 **로컬 보안 감사 정책 변경 사항 자동 적용** 확인란을 선택 해제합니다. 이 기능을 사용하면 추가된 Sigma 규칙 컬렉션이 제대로 작동하는 데 필요한 경우 애플리케이션이 로컬 정책 설정을 자동으로 편집합니다. 이 기능이 중지되어 있는 경우 Sigma 규칙이 제대로 작동하도록 로컬 정책 설정을 수동으로 구성하는 단계를 수행하십시오. 이 옵션은 기본적으로 활성화되어 있습니다.

   > 애플리케이션은 Sigma 규칙의 사용자 지정 컬렉션에 대한 로컬 정책 설정을 수정하지 않습니다. 로컬 정책 설정을 수동으로 구성해야 사용자 지정 Sigma 규칙이 제대로 작동합니다.

8. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

9. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 활성화된 Sigma 규칙 컬렉션을 사용하여 이상 행위를 검색합니다.

웹 콘솔에서 Sigma 규칙을 사용한 이상 행위 탐지 활성화

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션에서 **Sigma 규칙을 사용한 이상 행위 탐지 사용** 확인란을 선택합니다.

5. 필요하다면 **로컬 보안 감사 정책 변경 사항 자동 적용** 확인란을 선택 해제합니다. 이 기능을 사용하면 추가된 Sigma 규칙 컬렉션이 제대로 작동하는 데 필요한 경우 애플리케이션이 로컬 정책 설정을 자동으로 편집합니다. 이 기능이 중지되어 있는 경우 Sigma 규칙이 제대로 작동하도록 로컬 정책 설정을 수동으로 구성하는 단계를 수행하십시오. 이 옵션은 기본적으로 활성화되어 있습니다.

   > 애플리케이션은 Sigma 규칙의 사용자 지정 컬렉션에 대한 로컬 정책 설정을 수정하지 않습니다. 로컬 정책 설정을 수동으로 구성해야 사용자 지정 Sigma 규칙이 제대로 작동합니다.

6. 하나 이상의 Sigma 규칙 컬렉션을 추가합니다.

   a. **추가** 버튼을 클릭합니다.

      규칙 컬렉션 추가 창이 열립니다.

   b. **규칙 컬렉션 선택** 드롭다운 목록을 사용해 다음 중 하나를 수행합니다.

      - 사전 정의된 Sigma 규칙 컬렉션 중 하나를 선택합니다.

        사전 정의된 Sigma 규칙 컬렉션이 표시되지 않으면 애플리케이션이 EDR Optimum 및 ICS 원격 측정 개체가 있는 라이센스 키로 활성화되었는지 확인하십시오. *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 실행하여 사전 정의된 컬렉션을 업데이트할 수도 있습니다.

        > 사전 정의된 Sigma 규칙 모음을 추가할 때는 선택한 모음이 관리 중인 기기에 설치된 모든 버전의 Kaspersky Industrial CyberSecurity for Nodes에서 지원되는지 확인해야 합니다.

      - **사용자 지정 규칙 컬렉션** 옵션을 선택하여 Sigma 규칙의 사용자 지정 컬렉션을 추가합니다.

        사용자 지정 Sigma 규칙 컬렉션을 추가하는 경우 해당 필드에 컬렉션의 고유 이름을 입력합니다. 생성된 사용자 지정 컬렉션에 포함된 규칙이 없습니다.

   c. **확인**을 누릅니다.

      새로운 컬렉션이 목록에 표사됩니다. 기본적으로 추가된 Sigma 규칙 컬렉션이 사용됩니다. 필요한 경우 컬렉션 이름 왼쪽에 있는 토글 스위치를 사용하여 Sigma 규칙 컬렉션의 상태를 관리합니다.

   d. **저장** 버튼을 클릭합니다.

      Kaspersky Industrial CyberSecurity for Nodes는 활성화된 Sigma 규칙 컬렉션을 사용하여 이상 행위를 검색합니다.

애플리케이션 콘솔에서 Sigma 규칙을 사용한 이상 행위 탐지 활성화

1. 애플리케이션 콘솔 트리에서 **Detection and Response** → Sigma 규칙을 사용한 이상 행위 탐지 섹션을 선택합니다.

   결과 창에서 **속성** 링크를 클릭합니다.

2. **Sigma 규칙을 사용한 이상 행위 탐지** 확인란을 선택합니다.

3. 하나 이상의 Sigma 규칙 컬렉션을 추가합니다.

   a. **추가** 버튼을 클릭합니다.

   규칙 컬렉션 추가 창이 열립니다.

   b. **규칙 컬렉션 선택** 드롭다운 목록을 사용해 다음 중 하나를 수행합니다.

   - 사전 정의된 Sigma 규칙 컬렉션 중 하나를 선택합니다.

     사전 정의된 Sigma 규칙 컬렉션이 표시되지 않으면 애플리케이션이 EDR Optimum 및 ICS 원격 측정 개체가 있는 라이센스 키로 활성화되었는지 확인하십시오. *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 실행하여 사전 정의된 컬렉션을 업데이트할 수도 있습니다.

   - **사용자 지정 규칙 컬렉션** 옵션을 선택하여 Sigma 규칙의 사용자 지정 컬렉션을 추가합니다.

     사용자 지정 Sigma 규칙 컬렉션을 추가하는 경우 해당 필드에 컬렉션의 고유 이름을 입력합니다. 생성된 사용자 지정 컬렉션에 포함된 규칙이 없습니다.

     > 애플리케이션 콘솔을 사용하여 생성된 Sigma 규칙의 사용자 지정 컬렉션은 Kaspersky Security Center 관리 콘솔 및 웹 콘솔에서 사용할 수 없습니다.

   c. **확인**을 누릅니다.

   새로운 컬렉션이 목록에 표사됩니다. 기본적으로 추가된 Sigma 규칙 컬렉션이 사용됩니다. 필요한 경우 컬렉션 이름 왼쪽에 있는 확인란을 사용하여 Sigma 규칙 컬렉션의 상태를 관리합니다.

4. 필요하다면 **로컬 보안 감사 정책 변경 사항 자동 적용** 확인란을 선택 해제합니다. 이 기능을 사용하면 추가된 Sigma 규칙 컬렉션이 제대로 작동하는 데 필요한 경우 애플리케이션이 로컬 정책 설정을 자동으로 편집합니다. 이 기능이 중지되어 있는 경우 Sigma 규칙이 제대로 작동하도록 로컬 정책 설정을 수동으로 구성하는 단계를 수행하십시오. 이 옵션은 기본적으로 활성화되어 있습니다.

   > 애플리케이션은 Sigma 규칙의 사용자 지정 컬렉션에 대한 로컬 정책 설정을 수정하지 않습니다. 로컬 정책 설정을 수동으로 구성해야 사용자 지정 Sigma 규칙이 제대로 작동합니다.

5. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 활성화된 Sigma 규칙 컬렉션을 사용하여 이상 행위를 검색합니다.

또한 명령줄에서 Sigma 규칙을 사용한 이상 행위 탐지를 활성화할 수 있습니다.

사용자 지정 컬렉션에 Sigma 규칙 추가

Kaspersky Security Center 관리 콘솔에서 사용자 지정 컬렉션에 Sigma 규칙 추가

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션을 선택합니다.
4. **Sigma 규칙을 사용한 이상 행위 탐지** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 하나 이상의 Sigma 규칙을 추가할 사용자 지정 Sigma 규칙 컬렉션을 선택합니다.
6. **편집** 버튼을 클릭합니다.
7. 창이 열리면 다음 방법 중 하나로 Sigma 규칙을 컬렉션에 추가합니다.

- 수동:

  a. **추가** 버튼을 클릭합니다.

  b. 편집기 양식이 열리면 **Sigma 형식**의 규칙을 설명합니다.

  이 표에는 Kaspersky Industrial CyberSecurity for Nodes가 해석하는 Sigma 규칙의 섹션 및 속성에 대한 기본 정보가 포함되어 있습니다. 자세한 내용을 보려면 이 링크를 확인하십시오.

  > 속성 값은 대소문자를 구분합니다. 예를 들어 Kaspersky Industrial CyberSecurity for Nodes는 AnyDesk.exe 및 AnyDesk.exe 실행 파일의 이름을 다르게 처리합니다.

<table>
<tr><th>특성/섹션</th><th>필수</th><th>설명</th></tr>
<tr><td><code>logsource</code></td><td>예</td><td>
이 섹션에서는 애플리케이션이 이상 행위를 검색할 이벤트의 경로를 정의할 수 있습니다. 이 섹션의 주요 속성은 <code>category</code>, <code>product</code>, <code>service</code> 입니다.

Kaspersky Industrial CyberSecurity for Nodes가 지원하는 이벤트 경로

Kaspersky Industrial CyberSecurity for Nodes가 지원하는 이벤트 경로

<table>
<tr><th>경로(logsource)</th><th>이벤트</th></tr>
<tr><td><code>category: process_creation</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 1에 해당하는 내용의 내부 프로세스 시작 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td><code>category: driver_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 6에 해당하는 내용의 내부 드라이버 로드 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td><code>category: image_load</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 7에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td><code>category: registry_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 12, EventID 13, EventID 14에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td><code>category: dns_query</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 22에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td><code>category: file_rename</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Windows 추적 서비스 공급자 Microsoft-Windows-Kernel-File 로그의 이벤트에 해당하는 내용의 내부 이벤트를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td><code>category: file_event</code>
<code>product: windows</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 11에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td><code>product: windows</code>
<code>service: application</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/애플리케이션 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td><code>product: windows</code>
<code>service: security</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/보안 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td><code>product: windows</code>
<code>service: system</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/시스템 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td><code>category: chronicle_journal</code>
<code>product: deltav</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Emerson DeltaV 시스템 이벤트 로그의 정규화된 데이터와 관련된 내부 이벤트 인스턴스를 분석합니다.
출처 이벤트는 외부 이벤트 로그에 연결되지 않습니다.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell-classic</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Windows PowerShell 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td><code>product: windows</code>
<code>service: powershell</code></td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-PowerShell/작업 로그에서 이벤트를 분석합니다.</td></tr>
</table>

Microsoft Windows 7의 <code>category: dns_query</code>, <code>service: powershell-classic</code>, <code>service: powershell</code> 공급자에서는 일부 내부 이벤트가 누락되었거나 이벤트에서 일부 필드 또는 필요한 데이터가 누락될 수 있습니다. 결과적으로 Sigma 규칙이 트리거되지 않을 수 있습니다.

이 링크에서 더 확인할 수 있습니다.
</td></tr>
<tr><td><code>title</code></td><td>예</td><td>
탐지된 항목을 나타내는 규칙 이름입니다. 최대 길이는 256자입니다.
예:

<code>title: 새로운 RAT 서비스 생성</code>
</td></tr>
<tr><td><code>id</code></td><td>아니오</td><td>
규칙의 전역 고유 식별자입니다. 예:

<code>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</code>
</td></tr>
<tr><td><code>status</code></td><td>아니오</td><td>
규칙 상태. 가능한 값: <code>stable</code>, <code>test</code>, <code>experimental</code>, <code>deprecated</code>, <code>unsupported</code>.
예:

<code>status: test</code>
</td></tr>
<tr><td><code>description</code></td><td>아니오</td><td>
규칙 및 규칙이 탐지할 수 있는 악성 활동에 대한 설명입니다. 최대 길이는 65,535자입니다.
예:

<code>description: 새로운 원격 유틸리티 호스트 애플리케이션 서비스 설치를 탐지합니다.</code>
</td></tr>
</table>

`license`	아니오	SPDX ID 사양에 따른 라이센스 ID입니다. 지정된 라이센스 유형의 조건에 따라 규칙이 게시되었습니다.
`author`	아니오	규칙의 작성자를 나타내는 지정자입니다. 예: 이름과 성, 닉네임, 소셜 네트워크 ID.
`reference`	아니오	규칙을 가져온 출처에 대한 링크입니다. 블로그 기사나 백서를 예로 들 수 있습니다.
`date`	아니오	규칙이 만들어진 날짜는 YYYY/MM/DD 형식입니다.
`modified`	아니오	다음 규칙 속성 중 하나가 변경된 날짜(YYYY/MM/DD 형식): `title`, `status`, `logsource`, `detection`, `level`.
`tags`	아니오	규칙 분류를 위한 태그입니다. 이 링크에서 더 확인할 수 있습니다.

`category`	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 제품의 카테고리를 정의합니다. 예: 방화벽, 인터넷, 안티 바이러스, 일반 등.
		`logsource:`
		`  category: firewall`

`product`	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 소프트웨어 제품 또는 운영 체제를 정의합니다. 예:
		`logsource:`
		`  product: Windows`

`service`	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 서비스를 정의합니다. 예:
		`logsource:`
		`  service: AppLocker`

`definition`	아니오	애플리케이션이 이상 행위를 검색할 이벤트 로그의 세부 출처에 관한 설명입니다.
`detection`	예	이 섹션은 이벤트 로그에서 이상 행위를 검색하기 위한 하나 이상의 기준과 규칙 트리거 조건을 포함합니다. 검색 기준으로 리스트나 딕셔너리, 또는 이 둘의 조합을 사용할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 `windash` 값 수정자를 지원하지 않습니다.

목록	아니오	이벤트 로그에 있는 파라미터 값의 목록으로, 논리합으로 결합합니다. 예:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: `OriginalFileName='AnyDesk.exe'` 또는 `OriginalFileName='TeamViewer.exe'`.

딕셔너리	아니오	*이벤트 로그 파라미터 - 값* 쌍. 둘은 논리곱으로 연결됩니다. 예:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: EventLog='Security' AND Event ID=517.

리스트와 딕셔너리의 조합	아니오	이벤트 로그 설정 값과 딕셔너리로 구성된 리스트입니다. 예:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: EventLog='Security' AND (Event ID=517 OR Event ID=1102)

`condition`	예	규칙 트리거 조건. 예:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	아니오	분석가가 이벤트의 후속 분석을 위해 관심을 가질 수 있는 이벤트 로그의 열.

`falsepositives`	아니오	규칙을 잘못 트리거할 수 있다고 알려진 시나리오 목록입니다. 예:
		`falsepositives:`
		`- 시스템 관리자의 유틸리티 사용`

`level`	아니오	규칙을 사용하여 찾을 수 있는 이상 행위의 심각도를 나타내는 지표입니다. 가능한 값: `informational`, `low`, `medium`, `high`, `critical`.

c. **확인**을 누릅니다.
설명된 Sigma 규칙이 컬렉션의 규칙 목록에 표시됩니다.

d. 규칙을 직접 추가할 때마다 a~c 단계를 반복합니다.

- 파일에서:

a. **파일 추가** 버튼을 클릭합니다.

b. 창이 열리면 Sigma 규칙을 설명하는 YAML 파일을 하나 이상 선택합니다.
YAML 파일에 설명된 Sigma 규칙이 컬렉션의 규칙 목록에 표시됩니다.

> Sigma 규칙에 구문 오류가 포함되어 있거나 필수 속성이 누락된 경우에는 규칙이 컬렉션에 추가되지 않습니다.

8. 기본적으로 추가된 규칙이 사용됩니다. 필요한 경우 컬렉션 이름 왼쪽에 있는 확인란을 사용하여 Sigma 규칙의 상태를 관리합니다. **모두 사용** 버튼과 **모두 사용 안 함** 버튼을 사용하여 컬렉션에 있는 모든 규칙의 상태를 변경할 수 있습니다.

9. 목록에서 규칙을 삭제하려면, 규칙을 선택하고 **제거**를 클릭합니다.

10. 변경 사항을 저장합니다.

웹 콘솔에서 사용자 지정 컬렉션에 Sigma 규칙 추가

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션을 선택합니다.

5. **Sigma 규칙을 사용한 이상 행위 탐지** 블록에서 컬렉션 이름 옆의 확인란을 사용하여 하나 이상의 Sigma 규칙을 추가할 사용자 지정 Sigma 규칙 컬렉션을 선택합니다.

6. **편집** 버튼을 클릭합니다.

7. 창이 열리면 다음 방법 중 하나로 Sigma 규칙을 컬렉션에 추가합니다.

- 수동:

a. **추가** 버튼을 클릭합니다.

b. 편집기 양식이 열리면 **Sigma 형식**의 규칙을 설명합니다.

이 표에는 Kaspersky Industrial CyberSecurity for Nodes가 해석하는 Sigma 규칙의 섹션 및 속성에 대한 기본 정보가 포함되어 있습니다. 자세한 내용을 보려면 이 링크를 확인하십시오.

> 속성 값은 대소문자를 구분합니다. 예를 들어 Kaspersky Industrial CyberSecurity for Nodes는 AnyDesk.exe 및 AnyDesk.exe 실행 파일의 이름을 다르게 처리합니다.

<table>
<tr><th>특성/섹션</th><th>필수</th><th>설명</th></tr>
<tr><td>logsource</td><td>예</td><td>
이 섹션에서는 애플리케이션이 이상 행위를 검색할 이벤트의 경로를 정의할 수 있습니다. 이 섹션의 주요 속성은 category, product, service 입니다.
Kaspersky Industrial CyberSecurity for Nodes가 지원하는 이벤트 경로
Kaspersky Industrial CyberSecurity for Nodes가 지원하는 이벤트 경로
<table>
<tr><th>경로(logsource)</th><th>이벤트</th></tr>
<tr><td>category: process_creation
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 1에 해당하는 내용의 내부 프로세스 시작 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: driver_load
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 6에 해당하는 내용의 내부 드라이버 로드 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: image_load
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 7에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: registry_event
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 12, EventID 13, EventID 14에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: dns_query
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 22에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: file_rename
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Windows 추적 서비스 공급자 Microsoft-Windows-Kernel-File 로그의 이벤트에 해당하는 내용의 내부 이벤트를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: file_event
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 11에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>product: windows
service: application</td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/애플리케이션 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>product: windows
service: security</td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/보안 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>product: windows
service: system</td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/시스템 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>category: chronicle_journal
product: deltav</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Emerson DeltaV 시스템 이벤트 로그의 정규화된 데이터와 관련된 내부 이벤트 인스턴스를 분석합니다.
출처 이벤트는 외부 이벤트 로그에 연결되지 않습니다.</td></tr>
<tr><td>product: windows
service: powershell-classic</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Windows PowerShell 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>product: windows
service: powershell</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-PowerShell/작업 로그에서 이벤트를 분석합니다.</td></tr>
</table>
Microsoft Windows 7의 category: dns_query, service: powershell-classic, service: powershell 공급자에서는 일부 내부 이벤트가 누락되었거나 이벤트에서 일부 필드 또는 필요한 데이터가 누락될 수 있습니다. 결과적으로 Sigma 규칙이 트리거되지 않을 수 있습니다.
이 링크에서 더 확인할 수 있습니다.
</td></tr>
<tr><td>title</td><td>예</td><td>
탐지된 항목을 나타내는 규칙 이름입니다. 최대 길이는 256자입니다.
예:
<pre>title: 새로운 RAT 서비스 생성</pre>
</td></tr>
<tr><td>id</td><td>아니오</td><td>
규칙의 전역 고유 식별자입니다. 예:
<pre>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</pre>
</td></tr>
<tr><td>status</td><td>아니오</td><td>
규칙 상태. 가능한 값: stable, test, experimental, deprecated, unsupported.
예:
<pre>status: test</pre>
</td></tr>
<tr><td>description</td><td>아니오</td><td>
규칙 및 규칙이 탐지할 수 있는 악성 활동에 대한 설명입니다. 최대 길이는 65,535자입니다.
예:
<pre>description: 새로운 원격 유틸리티 호스트 애플리케이션 서비스 설치를 탐지합니다.</pre>
</td></tr>
</table>

`license`	아니오	SPDX ID 사양에 따른 라이센스 ID입니다. 지정된 라이센스 유형의 조건에 따라 규칙이 게시되었습니다.
`author`	아니오	규칙의 작성자를 나타내는 지정자입니다. 예: 이름과 성, 닉네임, 소셜 네트워크 ID.
`reference`	아니오	규칙을 가져온 출처에 대한 링크입니다. 블로그 기사나 백서를 예로 들 수 있습니다.
`date`	아니오	규칙이 만들어진 날짜는 YYYY/MM/DD 형식입니다.
`modified`	아니오	다음 규칙 속성 중 하나가 변경된 날짜(YYYY/MM/DD 형식): `title`, `status`, `logsource`, `detection`, `level`.
`tags`	아니오	규칙 분류를 위한 태그입니다. 이 링크에서 더 확인할 수 있습니다.

`category`	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 제품의 카테고리를 정의합니다. 예: 방화벽, 인터넷, 안티 바이러스, 일반 등.
		`logsource:`
		`  category: firewall`

`product`	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 소프트웨어 제품 또는 운영 체제를 정의합니다. 예:
		`logsource:`
		`  product: Windows`

`service`	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 서비스를 정의합니다. 예:
		`logsource:`
		`  service: AppLocker`

`definition`	아니오	애플리케이션이 이상 행위를 검색할 이벤트 로그의 세부 출처에 관한 설명입니다.
`detection`	예	이 섹션은 이벤트 로그에서 이상 행위를 검색하기 위한 하나 이상의 기준과 규칙 트리거 조건을 포함합니다. 검색 기준으로 리스트나 딕셔너리, 또는 이 둘의 조합을 사용할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 `windash` 값 수정자를 지원하지 않습니다.

목록	아니오	이벤트 로그에 있는 파라미터 값의 목록으로, 논리합으로 결합합니다. 예:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: `OriginalFileName='AnyDesk.exe'` 또는 `OriginalFileName='TeamViewer.exe'`.

딕셔너리	아니오	*이벤트 로그 파라미터 - 값* 쌍. 둘은 논리곱으로 연결됩니다. 예:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: EventLog='Security' AND Event ID=517.

리스트와 딕셔너리의 조합	아니오	이벤트 로그 설정 값과 딕셔너리로 구성된 리스트입니다. 예:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: EventLog='Security' AND (Event ID=517 OR Event ID=1102)

`condition`	예	규칙 트리거 조건. 예:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	아니오	분석가가 이벤트의 후속 분석을 위해 관심을 가질 수 있는 이벤트 로그의 열.

`falsepositives`	아니오	규칙을 잘못 트리거할 수 있다고 알려진 시나리오 목록입니다. 예:
		`falsepositives:`
		`- 시스템 관리자의 유틸리티 사용`

`level`	아니오	규칙을 사용하여 찾을 수 있는 이상 행위의 심각도를 나타내는 지표입니다. 가능한 값: `informational`, `low`, `medium`, `high`, `critical`.

c. **확인**을 누릅니다.

설명된 Sigma 규칙이 컬렉션의 규칙 목록에 표시됩니다.

d. 규칙을 직접 추가할 때마다 a~c 단계를 반복합니다.

- 파일에서:

a. **파일 추가** 버튼을 클릭합니다.

b. 창이 열리면 Sigma 규칙을 설명하는 YAML 파일을 하나 이상 선택합니다.

YAML 파일에 설명된 Sigma 규칙이 컬렉션의 규칙 목록에 표시됩니다.

> Sigma 규칙에 구문 오류가 포함되어 있거나 필수 속성이 누락된 경우에는 규칙이 컬렉션에 추가되지 않습니다.

8. 기본적으로 추가된 규칙이 사용됩니다. 필요한 경우 컬렉션 이름 왼쪽에 있는 토글 스위치를 사용하여 Sigma 규칙 컬렉션의 상태를 관리합니다. **모두 사용** 버튼과 **모두 사용 안 함** 버튼을 사용하여 컬렉션에 있는 모든 규칙의 상태를 변경할 수 있습니다.

9. 목록에서 규칙을 삭제하려면, 규칙을 선택하고 **삭제**를 클릭합니다.

10. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 사용자 지정 컬렉션에 Sigma 규칙 추가

1. 애플리케이션 콘솔 트리에서 **Detection and Response** → Sigma 규칙을 사용한 이상 행위 탐지 섹션을 선택합니다.

2. 결과 창에서 **속성** 링크를 클릭합니다.

3. 창이 열리면 하나 이상의 Sigma 규칙을 추가할 사용자 지정 Sigma 규칙 컬렉션을 선택합니다.

4. **편집** 버튼을 클릭합니다.

5. 창이 열리면 다음 방법 중 하나로 Sigma 규칙을 컬렉션에 추가합니다.

- 수동:

a. **추가** 버튼을 클릭합니다.

b. 편집기 양식이 열리면 **Sigma 형식**의 규칙을 설명합니다.

이 표에는 Kaspersky Industrial CyberSecurity for Nodes가 해석하는 Sigma 규칙의 섹션 및 속성에 대한 기본 정보가 포함되어 있습니다. 자세한 내용을 보려면 이 링크를 확인하십시오.

> 속성 값은 대소문자를 구분합니다. 예를 들어 Kaspersky Industrial CyberSecurity for Nodes는 AnyDesk.exe 및 AnyDesk.exe 실행 파일의 이름을 다르게 처리합니다.

<table>
<tr><th>특성/섹션</th><th>필수</th><th>설명</th></tr>
<tr><td>logsource</td><td>예</td><td>
이 섹션에서는 애플리케이션이 이상 행위를 검색할 이벤트의 경로를 정의할 수 있습니다. 이 섹션의 주요 속성은 category, product, service 입니다.
Kaspersky Industrial CyberSecurity for Nodes가 지원하는 이벤트 경로
Kaspersky Industrial CyberSecurity for Nodes가 지원하는 이벤트 경로
<table>
<tr><th>경로(logsource)</th><th>이벤트</th></tr>
<tr><td>category: process_creation
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 1에 해당하는 내용의 내부 프로세스 시작 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: driver_load
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 6에 해당하는 내용의 내부 드라이버 로드 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: image_load
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 7에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: registry_event
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 12, EventID 13, EventID 14에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: dns_query
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 22에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: file_rename
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Windows 추적 서비스 공급자 Microsoft-Windows-Kernel-File 로그의 이벤트에 해당하는 내용의 내부 이벤트를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>category: file_event
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-Sysmon/동작 로그의 EventID 11에 해당하는 내용의 내부 이벤트 인스턴스를 분석하고 Kaspersky Industrial CyberSecurity for Nodes 필드에 인리치먼트를 적용합니다.</td></tr>
<tr><td>product: windows
service: application</td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/애플리케이션 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>product: windows
service: security</td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/보안 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>product: windows
service: system</td><td>Kaspersky Industrial CyberSecurity for Nodes가 WEL/시스템 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>category: chronicle_journal
product: deltav</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Emerson DeltaV 시스템 이벤트 로그의 정규화된 데이터와 관련된 내부 이벤트 인스턴스를 분석합니다.
출처 이벤트는 외부 이벤트 로그에 연결되지 않습니다.</td></tr>
<tr><td>product: windows
service: powershell-classic</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Windows PowerShell 로그에서 이벤트를 분석합니다.</td></tr>
<tr><td>product: windows
service: powershell</td><td>Kaspersky Industrial CyberSecurity for Nodes가 Microsoft-Windows-PowerShell/작업 로그에서 이벤트를 분석합니다.</td></tr>
</table>
Microsoft Windows 7의 category: dns_query, service: powershell-classic, service: powershell 공급자에서는 일부 내부 이벤트가 누락되었거나 이벤트에서 일부 필드 또는 필요한 데이터가 누락될 수 있습니다. 결과적으로 Sigma 규칙이 트리거되지 않을 수 있습니다.
이 링크에서 더 확인할 수 있습니다.
</td></tr>
<tr><td>title</td><td>예</td><td>
탐지된 항목을 나타내는 규칙 이름입니다. 최대 길이는 256자입니다.
예:
<pre>title: 새로운 RAT 서비스 생성</pre>
</td></tr>
<tr><td>id</td><td>아니오</td><td>
규칙의 전역 고유 식별자입니다. 예:
<pre>id: 929a690e-bef0-4204-a928-ef5e620d6fcc</pre>
</td></tr>
<tr><td>status</td><td>아니오</td><td>
규칙 상태. 가능한 값: stable, test, experimental, deprecated, unsupported.
예:
<pre>status: test</pre>
</td></tr>
<tr><td>description</td><td>아니오</td><td>
규칙 및 규칙이 탐지할 수 있는 악성 활동에 대한 설명입니다. 최대 길이는 65,535자입니다.
예:
<pre>description: 새로운 원격 유틸리티 호스트 애플리케이션 서비스 설치를 탐지합니다.</pre>
</td></tr>
</table>

`license`	아니오	SPDX ID 사양에 따른 라이센스 ID입니다. 지정된 라이센스 유형의 조건에 따라 규칙이 게시되었습니다.
`author`	아니오	규칙의 작성자를 나타내는 지정자입니다. 예: 이름과 성, 닉네임, 소셜 네트워크 ID.
`reference`	아니오	규칙을 가져온 출처에 대한 링크입니다. 블로그 기사나 백서를 예로 들 수 있습니다.
`date`	아니오	규칙이 만들어진 날짜는 YYYY/MM/DD 형식입니다.
`modified`	아니오	다음 규칙 속성 중 하나가 변경된 날짜(YYYY/MM/DD 형식): `title`, `status`, `logsource`, `detection`, `level`.
`tags`	아니오	규칙 분류를 위한 태그입니다. 이 링크에서 더 확인할 수 있습니다.

`category`	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 제품의 카테고리를 정의합니다. 예: 방화벽, 인터넷, 안티 바이러스, 일반 등.
		`logsource:`
		`  category: firewall`

`product`	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 소프트웨어 제품 또는 운영 체제를 정의합니다. 예:
		`logsource:`
		`  product: Windows`

`service`	아니오	애플리케이션이 이벤트 로그에서 이상 행위를 검색할 서비스를 정의합니다. 예:
		`logsource:`
		`  service: AppLocker`

`definition`	아니오	애플리케이션이 이상 행위를 검색할 이벤트 로그의 세부 출처에 관한 설명입니다.
`detection`	예	이 섹션은 이벤트 로그에서 이상 행위를 검색하기 위한 하나 이상의 기준과 규칙 트리거 조건을 포함합니다. 검색 기준으로 리스트나 딕셔너리, 또는 이 둘의 조합을 사용할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 `windash` 값 수정자를 지원하지 않습니다.

목록	아니오	이벤트 로그에 있는 파라미터 값의 목록으로, 논리합으로 결합합니다. 예:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: `OriginalFileName='AnyDesk.exe'` 또는 `OriginalFileName='TeamViewer.exe'`.

딕셔너리	아니오	*이벤트 로그 파라미터 - 값* 쌍. 둘은 논리곱으로 연결됩니다. 예:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: EventLog='Security' AND Event ID=517.

리스트와 딕셔너리의 조합	아니오	이벤트 로그 설정 값과 딕셔너리로 구성된 리스트입니다. 예:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		조건에 따라 다음과 같이 일치하는 항목을 검색합니다: EventLog='Security' AND (Event ID=517 OR Event ID=1102)

`condition`	예	규칙 트리거 조건. 예:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	아니오	분석가가 이벤트의 후속 분석을 위해 관심을 가질 수 있는 이벤트 로그의 열.

`falsepositives`	아니오	규칙을 잘못 트리거할 수 있다고 알려진 시나리오 목록입니다. 예:
		`falsepositives:`
		`- 시스템 관리자의 유틸리티 사용`

`level`	아니오	규칙을 사용하여 찾을 수 있는 이상 행위의 심각도를 나타내는 지표입니다. 가능한 값: `informational`, `low`, `medium`, `high`, `critical`.

c. **확인**을 누릅니다.
설명된 Sigma 규칙이 컬렉션의 규칙 목록에 표시됩니다.

d. 규칙을 직접 추가할 때마다 a~c 단계를 반복합니다.

- 파일에서:

a. **파일 추가** 버튼을 클릭합니다.

b. 창이 열리면 Sigma 규칙을 설명하는 YAML 파일을 하나 이상 선택합니다.
YAML 파일에 설명된 Sigma 규칙이 컬렉션의 규칙 목록에 표시됩니다.

> Sigma 규칙에 구문 오류가 포함되어 있거나 필수 속성이 누락된 경우에는 규칙이 컬렉션에 추가되지 않습니다.

6. 기본적으로 추가된 규칙이 사용됩니다. 필요한 경우 컬렉션 이름 왼쪽에 있는 확인란을 사용하여 Sigma 규칙의 상태를 관리합니다. **모두 사용** 버튼과 **모두 사용 안 함** 버튼을 사용하여 컬렉션에 있는 모든 규칙의 상태를 변경할 수 있습니다.

7. 목록에서 규칙을 삭제하려면, 규칙을 선택하고 **제거**를 클릭합니다.

8. 변경 사항을 저장합니다.

규칙 컬렉션 내에서 Sigma 규칙 필터링

컬렉션에 있는 Sigma 규칙의 수가 많고 특정 파라미터와 함께 Sigma 규칙 목록을 표시해야 하는 경우 필터를 사용할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 Sigma 규칙 필터링

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션을 선택합니다.

4. **Sigma 규칙을 사용한 이상 행위 탐지** 블록에서 **설정** 버튼을 클릭합니다.

5. 창이 열리면 규칙 필터를 적용할 컬렉션을 선택합니다.

6. **편집** 버튼을 클릭합니다.
편집 창이 열립니다.

7. **필터** 버튼을 클릭합니다.
필터링 기준이 있는 창이 열립니다.

8. 필요한 필터링 기준 값을 지정합니다:

   - **규칙에 텍스트가 포함됨** 기준은 대소문자를 구분하지 않는 부분 일치를 기반으로 규칙을 선택합니다. 모든 규칙 속성 또는 해당 값을 입력할 수 있습니다.
   - **규칙 상태** 기준은 상태에 따라 규칙을 선택합니다.
   - **예외 사용 가능성** 기준은 예외의 존재에 따라 규칙을 선택합니다.

     이 기준은 Kaspersky 에서 제공하는 컬렉션의 필터링 규칙에만 사용할 수 있습니다.

9. **확인**을 누릅니다.

   필터링 기준과 일치하는 규칙이 컬렉션의 규칙 목록에 표시됩니다.

웹 콘솔에서 Sigma 규칙 필터링

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션을 선택합니다.
5. **Sigma 규칙을 사용한 이상 행위 탐지** 블록에서 컬렉션 이름 옆의 확인란을 사용하여 규칙 필터를 적용할 컬렉션을 선택합니다.
6. **편집** 버튼을 클릭합니다.

   편집 창이 열립니다.
7. **필터** 버튼을 클릭합니다.

   필터링 기준이 있는 창이 열립니다.
8. 필요한 필터링 기준 값을 지정합니다:

   - **규칙에 텍스트가 포함됨** 기준은 대소문자를 구분하지 않는 부분 일치를 기반으로 규칙을 선택합니다. 모든 규칙 속성 또는 해당 값을 입력할 수 있습니다.
   - **규칙 상태** 기준은 상태에 따라 규칙을 선택합니다.
   - **예외 사용 가능성** 기준은 예외의 존재에 따라 규칙을 선택합니다.

     이 기준은 Kaspersky 에서 제공하는 컬렉션의 필터링 규칙에만 사용할 수 있습니다.

9. **확인**을 누릅니다.
10. 필터링 기준과 일치하는 규칙이 컬렉션의 규칙 목록에 표시됩니다.

애플리케이션 콘솔에서 Sigma 규칙 필터링

1. 애플리케이션 콘솔 트리에서 **Detection and Response** → Sigma 규칙을 사용한 이상 행위 탐지 섹션을 선택합니다.

   결과 창에서 **속성** 링크를 클릭합니다.

2. 창이 열리면 규칙 필터를 적용할 컬렉션을 선택합니다.

3. **편집** 버튼을 클릭합니다.

   편집 창이 열립니다.

4. **필터** 버튼을 클릭합니다.

   필터링 기준이 있는 창이 열립니다.

5. 필요한 필터링 기준 값을 지정합니다:

   - **규칙에 텍스트가 포함됨** 기준은 대소문자를 구분하지 않는 부분 일치를 기반으로 규칙을 선택합니다. 모든 규칙 속성 또는 해당 값을 입력할 수 있습니다.
   - **규칙 상태** 기준은 상태에 따라 규칙을 선택합니다.
   - **예외 사용 가능성** 기준은 예외의 존재에 따라 규칙을 선택합니다.

     이 기준은 Kaspersky 에서 제공하는 컬렉션의 필터링 규칙에만 사용할 수 있습니다.

6. **확인**을 누릅니다.

   필터링 기준과 일치하는 규칙이 컬렉션의 규칙 목록에 표시됩니다.

사용자 지정 컬렉션의 Sigma 규칙 내보내기 및 가져오기

Kaspersky Security Center 관리 콘솔에서 Sigma 규칙 내보내기 및 가져오기

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션을 선택합니다.
4. **Sigma 규칙을 사용한 이상 행위 탐지** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 사용자 지정 Sigma 규칙 컬렉션을 선택합니다.
6. **편집** 버튼을 클릭합니다.
7. **내보내기** 버튼을 클릭해 사용자 지정 컬렉션에서 Sigma 규칙을 내보냅니다.

   Kaspersky Industrial CyberSecurity for Nodes는 표준 다운로드 폴더에 sigma.zip이라는 압축 파일을 저장합니다.

8. 사용자 지정 컬렉션으로 Sigma 규칙 가져오려면 다음과 같이 진행합니다:

   a. **가져오기** 버튼을 클릭합니다.

   b. 창이 열리면 설명된 Sigma 규칙을 가진 YAML 파일이 포함된 ZIP 압축파일을 선택합니다.

   > Sigma 규칙에 구문 오류가 포함되어 있거나 필수 속성이 누락된 경우에는 규칙이 컬렉션에 추가되지 않습니다.

   압축 파일에 포함된 Sigma 규칙이 컬렉션의 규칙 목록에 표시됩니다.

   > 가져온 ZIP 압축파일에 컬렉션에 이미 있는 중복 Sigma 규칙이 포함된 경우 이러한 규칙을 덮어쓰지 않습니다.

9. 변경 사항을 저장합니다.

웹 콘솔에서 Sigma 규칙 내보내기 및 가져오기

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션을 선택합니다.
5. **Sigma 규칙을 사용한 이상 행위 탐지** 블록에서 컬렉션 이름 옆의 확인란을 사용하여 사용자 지정 Sigma 규칙 컬렉션을 선택합니다.
6. **편집** 버튼을 클릭합니다.
7. **내보내기** 버튼을 클릭해 사용자 지정 컬렉션에서 Sigma 규칙을 내보냅니다.
   Kaspersky Industrial CyberSecurity for Nodes는 표준 다운로드 폴더에 sigma.zip이라는 압축 파일을 저장합니다.
8. 사용자 지정 컬렉션으로 Sigma 규칙 가져오려면 다음과 같이 진행합니다:

   a. **가져오기** 버튼을 클릭합니다.

   b. 창이 열리면 설명된 Sigma 규칙을 가진 YAML 파일이 포함된 ZIP 압축파일을 선택합니다.

   > Sigma 규칙에 구문 오류가 포함되어 있거나 필수 속성이 누락된 경우에는 규칙이 컬렉션에 추가되지 않습니다.

   압축 파일에 포함된 Sigma 규칙이 컬렉션의 규칙 목록에 표시됩니다.

가져온 ZIP 압축파일에 컬렉션에 이미 있는 중복 Sigma 규칙이 포함된 경우 이러한 규칙을 덮어쓰지 않습니다.

9. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 Sigma 규칙 내보내기 및 가져오기

1. 애플리케이션 콘솔 트리에서 **Detection and Response** → Sigma 규칙을 사용한 이상 행위 탐지 섹션을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.
3. 창이 열리면 사용자 지정 Sigma 규칙 컬렉션을 선택합니다.
4. **편집** 버튼을 클릭합니다.
5. **내보내기** 버튼을 클릭해 사용자 지정 컬렉션에서 Sigma 규칙을 내보냅니다.

   Kaspersky Industrial CyberSecurity for Nodes는 표준 다운로드 폴더에 sigma.zip이라는 압축 파일을 저장합니다.
6. 사용자 지정 컬렉션으로 Sigma 규칙 가져오려면 다음과 같이 진행합니다:

   a. **가져오기** 버튼을 클릭합니다.

   b. 창이 열리면 설명된 Sigma 규칙을 가진 YAML 파일이 포함된 ZIP 압축파일을 선택합니다.

   Sigma 규칙에 구문 오류가 포함되어 있거나 필수 속성이 누락된 경우에는 규칙이 컬렉션에 추가되지 않습니다.

   압축 파일에 포함된 Sigma 규칙이 컬렉션의 규칙 목록에 표시됩니다.

   가져온 ZIP 압축파일에 컬렉션에 이미 있는 중복 Sigma 규칙이 포함된 경우 이러한 규칙을 덮어쓰지 않습니다.
7. 변경 사항을 저장합니다.

Sigma 규칙 변경

사용자 지정 Sigma 규칙을 원하는 대로 변경할 수 있습니다. Kaspersky Lab에서 사전 정의된 컬렉션의 일부로 제공하는 Sigma 규칙의 경우 예외 추가 또는 제거와 규칙 상태 변경만 허용됩니다.

Kaspersky Security Center 관리 콘솔에서 Sigma 규칙 변경

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션을 선택합니다.

4. **Sigma 규칙을 사용한 이상 행위 탐지** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 하나 이상의 Sigma 규칙을 편집할 사용자 지정 Sigma 규칙 컬렉션을 선택합니다.
6. **편집** 버튼을 클릭합니다.
7. 창이 열리면 편집할 규칙을 선택합니다.
8. 필요한 경우 규칙 이름 왼쪽에 있는 확인란을 사용하여 규칙 상태를 변경합니다.
9. **편집** 버튼을 클릭합니다.
10. 창이 열리면 Sigma 규칙을 필요에 따라 편집합니다.

    Kaspersky Lab에서 컬렉션의 일부로 제공하는 Sigma 규칙을 편집하는 경우 규칙 예외만 편집할 수 있습니다.

11. 변경 사항을 저장합니다.

웹 콘솔에서 Sigma 규칙 편집

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **Sigma 규칙을 사용한 이상 행위 탐지** 섹션을 선택합니다.
5. **Sigma 규칙을 사용한 이상 행위 탐지** 블록에서 컬렉션 이름 옆의 확인란을 사용하여 하나 이상의 Sigma 규칙을 추가할 사용자 지정 Sigma 규칙 컬렉션을 선택합니다.
6. **편집** 버튼을 클릭합니다.
7. 창이 열리면 확인란을 사용하여 편집할 규칙을 선택합니다.
8. 필요하다면 규칙 이름 위의 **사용** / **사용 안 함** 토글 버튼을 사용하여 규칙 상태를 변경합니다.
9. **편집** 버튼을 클릭합니다.
10. 창이 열리면 Sigma 규칙을 필요에 따라 편집합니다.

    Kaspersky Lab에서 컬렉션의 일부로 제공하는 Sigma 규칙을 편집하는 경우 규칙 예외만 편집할 수 있습니다.

11. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 Sigma 규칙 편집

1. 애플리케이션 콘솔 트리에서 **Detection and Response** → Sigma 규칙을 사용한 이상 행위 탐지 섹션을 선택합니다.
2. 결과 창에서 **속성** 링크를 클릭합니다.
3. 창이 열리면 하나 이상의 Sigma 규칙을 편집할 사용자 지정 Sigma 규칙 컬렉션을 선택합니다.
4. **편집** 버튼을 클릭합니다.
5. 창이 열리면 편집할 규칙을 선택합니다.
6. 필요한 경우 규칙 이름 왼쪽에 있는 확인란을 사용하여 규칙 상태를 변경합니다.
7. **편집** 버튼을 클릭합니다.
8. 창이 열리면 Sigma 규칙을 필요에 따라 편집합니다.

   > Kaspersky Lab에서 컬렉션의 일부로 제공하는 Sigma 규칙을 편집하는 경우 규칙 예외만 편집할 수 있습니다.

9. 변경 사항을 저장합니다.

Sigma 규칙의 예외

사용자는 애플리케이션 데이터베이스와 함께 제공된 Sigma 규칙의 컨텐츠를 사용할 수 없습니다. 이는 이러한 규칙의 트리거 조건이 Kaspersky의 지적 자산이며 공개할 수 없기 때문입니다.

애플리케이션 데이터베이스와 함께 제공되는 Sigma 규칙 편집용 편집기의 경우 `detection` 섹션에서 규칙 예외만 추가할 수 있습니다.

예외 템플릿은 다음과 같이 정의됩니다:

```
detection:
   exclude1:
        - ...
   조건: exclude* 중 1이 아님
```

이 템플릿은 `exclude*` 특성을 사용해 예외가 지정된다고 가정하며, 규칙 트리거 조건은 사용자에게 숨긴 조건을 만족하며 지정한 예외와 일치하는 것이 없다고 가정합니다.

예:

```
detection:
   exclude1:
     Image|endswith:
       - '\chrome.exe'
       - '\tor.exe'
   exclude2:
     QueryName|endswith: 'api.parsec.app'
   조건: exclude* 중 1이 아님
```

개체 격리 및 백업

이 섹션에서는 바이러스 치료 또는 제거 전 탐지된 악성 개체의 백업 및 감염 의심 개체의 격리에 관한 정보를 설명합니다.

감염 의심 개체 격리. 격리 저장소

위협에 대응할 때 Kaspersky Industrial CyberSecurity for Nodes는 *격리 저장소로 파일 이동* 작업을 생성할 수 있습니다. 이는 보안위협의 결과를 최소화하는 데 필요합니다. 격리 저장소는 컴퓨터의 특수 로컬 저장소입니다. 관리자는 컴퓨터에 위험하다고 판단되는 파일을 격리할 수 있습니다. 격리된 파일은 암호화된 상태로 저장되며 장치 보안에 위협이 되지 않습니다. Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Industrial CyberSecurity Endpoint Detection and Response, Endpoint Detection and Response Expert(온프레미스) 또는 Kaspersky Industrial CyberSecurity for Networks와 함께 작동할 때만 격리를 사용합니다. 그 외에는 Kaspersky Industrial CyberSecurity for Nodes가 관련 파일을 백업에 저장합니다.

다음 방법으로 *격리 저장소로 파일 이동* 작업을 생성할 수 있습니다.

- 경고 세부 정보(Kaspersky Industrial CyberSecurity Endpoint Detection and Response 만 해당) 사용.

  *경고 세부 정보*는 탐지된 위협에서 수집한 전체 정보를 확인하는 도구입니다. 경고 세부 정보에는 컴퓨터에서의 파일 히스토리 등이 포함됩니다. 경고 세부 정보 관리에 관한 자세한 정보는 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 도움말을 참조하십시오.

- 작업 마법사 사용.

  파일 경로 또는 체크섬과 폴더 경로를 입력해야 합니다.

격리 저장소로 파일 이동 작업에는 다음 제한 사항이 있습니다.

- 파일 크기는 100MB를 초과할 수 없습니다.
- SCO(시스템 중요 개체)는 격리할 수 없습니다. SCO는 운영 체제 및 Kaspersky Industrial CyberSecurity for Nodes 애플리케이션을 실행하는 데 필요한 파일입니다.
- 웹 콘솔에서 Kaspersky Industrial CyberSecurity Endpoint Detection and Response의 작업 설정을 관리할 수 있습니다.

웹 콘솔에서 격리 저장소로 파일 이동 작업을 만드는 방법

1. 웹 콘솔의 메인 창에서 **장치** → **작업** 옵션을 선택합니다.

   작업 목록이 열립니다.

2. **추가** 버튼을 클릭합니다.
3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Industrial CyberSecurity for Nodes**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **격리 저장소로 파일 이동** 옵션을 선택합니다.

   c. **작업 이름** 필드에 작업에 대한 간단한 설명을 입력하고 **다음** 버튼을 클릭합니다.

4. **작업 범위** 섹션에서 관리 중인 장치를 선택하고 **다음** 버튼을 클릭합니다.

5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음** 버튼을 클릭합니다.

   기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. **마침** 버튼을 클릭해 마법사를 마칩니다. 작업 목록에 새 작업이 표시됩니다.

7. 새 작업을 클릭합니다. 작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. 파일 목록에서 **추가** 버튼을 클릭합니다. 파일 추가 마법사가 시작됩니다.

10. 파일을 추가하려면 파일의 전체 경로를 입력하거나, 체크섬과 폴더 경로를 입력해야 합니다.

    > 파일이 네트워크 드라이브에 있다면 드라이브 문자가 아닌 \\ 문자로 시작하는 파일 경로를 입력합니다. 예: `\\server\shared_folder\file.exe`. 파일 경로에 네트워크 드라이브 문자가 포함되어 있으면 파일이 없음 오류가 발생할 수 있습니다.

11. 작업 속성 창에서 **스케줄** 탭을 선택합니다. 작업 스케줄을 구성합니다.

    > 이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.

12. **저장** 버튼을 클릭합니다.

13. 작업 옆의 확인란을 선택하고 **시작** 버튼을 클릭합니다.

결과적으로 Kaspersky Industrial CyberSecurity for Nodes는 파일을 격리 저장소로 이동합니다.

다른 프로세스가 파일을 잠갔다면 작업은 **통과함**으로 표시되지만 파일 자체는 컴퓨터가 다시 시작된 후에만 격리됩니다. 컴퓨터를 다시 시작한 후 파일이 삭제되었는지 확인하십시오.

용량이 너무 큰 파일을 격리할 경우 *격리 저장소에 공간이 부족합니다* 오류가 발생하며 *격리 저장소로 파일 이동* 작업이 종료됩니다. 격리 저장소를 비우거나 크기를 늘리십시오. 그 후 다시 시도합니다.

격리 저장소에서 파일을 복원하거나 웹 콘솔을 사용하여 격리 저장소를 비울 수 있습니다.

격리 개체 보기

Kaspersky Security Center 관리 콘솔 및 웹 콘솔에서 격리된 개체를 볼 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 격리된 개체를 보는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 콘솔 트리에서 **추가** → **저장소** 폴더를 선택합니다.

3. **격리 저장소** 폴더로 갑니다.

4. 격리된 개체 정보가 콘솔의 오른쪽 창에 표시됩니다.

Kaspersky Security Center 웹 콘솔에서 격리된 개체를 보는 방법

1. 웹 콘솔을 엽니다.

2. 콘솔 트리에서 **동작** → **저장소** 폴더를 선택합니다.

3. **격리 저장소** 폴더로 갑니다.

4. 격리된 개체 정보가 콘솔의 오른쪽 창에 표시됩니다.

격리된 개체 목록에서 필요한 개체를 찾으려면,

개체를 정렬하거나 필터링하십시오.

격리된 개체 정렬

기본적으로 격리 개체 목록의 개체는 최근에 격리된 개체부터 격리 날짜별로 정렬되어 있습니다. 필요한 개체를 찾기 위해 개체 정보가 있는 열을 기준으로 개체를 정렬할 수 있습니다. 개체를 정렬하려면:

Kaspersky Security Center 관리 콘솔에서 격리 저장소의 파일을 정렬하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 콘솔 트리에서 **추가** → **격리 저장소** 폴더를 선택합니다.

3. 파일 목록에서 개체를 정렬하는데 사용하려는 열 제목을 선택합니다.

선택한 조건에 따라 격리 저장소의 파일이 정렬됩니다.

Kaspersky Security Center 웹 콘솔에서 격리 저장소의 파일을 정렬하는 방법

1. 웹 콘솔을 엽니다.

2. 콘솔 트리에서 **동작** → **격리 저장소** 폴더를 선택합니다.

3. 파일 목록에서 개체를 정렬하는데 사용하려는 열 제목을 선택합니다.

선택한 조건에 따라 격리 저장소의 파일이 정렬됩니다.

격리된 개체 필터링

필요한 격리 개체를 찾기 위해 목록에서 개체를 필터링할 수 있습니다. 그러면 지정한 필터링 기준(필터)을 충족하는 개체만 표시됩니다.

Kaspersky Security Center 관리 콘솔에서 격리 저장소 파일을 필터링하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **추가** → **저장소** 폴더를 선택합니다.
3. **격리 저장소** 폴더로 갑니다.
4. 오른쪽 창에서 **필터 지정 안 됨,** 링크를 클릭합니다.
5. **필터링 설정** 링크를 클릭하고 **필터링 설정** 창에서 필터링할 열을 선택합니다.
6. 선택한 열에 대한 연산자와 값을 지정합니다.
7. 생성된 필터가 저장됩니다.
8. 모든 격리 개체를 다시 표시하려면 **필터링 설정** 창에서 **모두 지우기**를 클릭합니다.

Kaspersky Security Center 웹 콘솔에서 격리 저장소의 파일을 정렬하는 방법

1. 웹 콘솔을 엽니다.
2. 콘솔 트리에서 **동작** → **저장소** 폴더를 선택합니다.
3. **격리 저장소** 폴더로 갑니다.
4. 필터 아이콘을 클릭하고 **필터** 탭의 **추가** 버튼을 클릭합니다.
5. 필터링할 속성을 선택합니다.
6. 선택한 속성의 조건과 값을 지정합니다.
7. **적용** 버튼을 클릭합니다.
   필터 설정이 저장됩니다.
8. 격리된 모든 개체의 표시를 복원하려면 **필터** 탭의 **모두 지우기**를 클릭합니다.

격리된 개체 복원

Kaspersky Industrial CyberSecurity for Nodes는 감염 의심 개체를 격리 폴더에 암호화된 형식으로 저장하여 이러한 개체가 미칠 수 있는 유해한 영향으로부터 보호 중인 장치를 방어합니다.

보호 중인 장치에 안전한 개체로 간주되고 사용하려는 경우 격리 저장소에서 개체를 복원할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes가 후속 검사 중에 개체를 격리하지 않도록 하려면 실시간 파일 보호 구성 요소와 온디맨드 검사 작업의 처리에서 개체를 제외하거나 신뢰 구약에 개체를 추가할 수 있습니다.

격리 저장소에서 개체를 복원하면 보호 붕인 장치가 감염될 수 있습니다.

하나 이상의 개체를 복원할 수 있습니다.

Kaspersky Security Center 관리 콘솔의 격리 저장소에서 개체 복원

1. Kaspersky Security Center 관리 콘솔 트리에서 **추가** → **저장소** 폴더를 선택합니다.
2. **격리 저장소** 폴더로 갑니다.
3. 다음 중 하나를 수행합니다:
   - 개체 하나를 복원하려면 해당 개체 이름의 마우스 오른쪽 메뉴에서 **복원** 옵션을 선택합니다.
   - 여러 개체를 복원하려면 Ctrl 또는 Shift 키를 사용하여 복원하려는 개체를 선택하고, 선택한 개체 중 하나를 마우스 오른쪽 버튼으로 클릭해 마우스 오른쪽 메뉴에서 **복원** 옵션을 선택합니다.
4. 개체가 원래 폴더로 복원됩니다.

Kaspersky Security Center 웹 콘솔 격리 저장소에서 개체 복원

1. 웹 콘솔을 엽니다.
2. 콘솔 트리에서 **동작** → **저장소** 폴더를 선택합니다.
3. **격리 저장소** 폴더로 갑니다.
4. 목록에서 개체를 선택하고 **복원** 버튼을 클릭합니다.
5. 개체가 원래 폴더로 복원됩니다.

격리 저장소에서 개체 삭제

Kaspersky Security Center 관리 콘솔 및 웹 콘솔의 격리 저장소에서 개체를 삭제할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 격리 개체를 삭제하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **추가** → **저장소** 폴더를 선택합니다.
3. **격리 저장소** 폴더로 갑니다.
4. 다음 중 하나를 수행합니다:
   - 개체 하나를 삭제하려면 개체의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
   - 여러 개체를 삭제하려면 Ctrl 또는 Shift 키를 사용하여 삭제하려는 개체를 선택하고, 선택한 개체 중 하나를 마우스 오른쪽 버튼으로 클릭해 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
5. 선택한 개체가 격리 저장소에서 제거됩니다.

Kaspersky Security Center 웹 콘솔에서 격리 저장소 개체를 삭제하는 방법

1. 웹 콘솔을 엽니다.
2. 콘솔 트리에서 **동작** → **저장소** 폴더를 선택합니다.

3. **격리 저장소** 폴더로 갑니다.

4. 목록에서 개체를 선택하고 **삭제** 버튼을 클릭합니다.

5. 삭제를 확인합니다.

6. 선택한 개체가 백업 저장소에서 삭제됩니다.

분석을 위해 Kaspersky로 감염 의심 개체 보내기

개체의 동작이 해당 개체에 위협이 포함되어 있다는 의심을 불러일으킬 만한 이유를 제공하는 경우 Kaspersky Industrial CyberSecurity for Nodes는 이 개체를 정리 대상으로 간주합니다. 서명이 아직 데이터베이스에 추가되지 않은 알려지지 않은 새로운 위협이 발생했을 수 있습니다. 이러한 개체는 분석을 위해 Kaspersky로 보낼 수 있습니다. Kaspersky의 안티 바이러스 분석가가 이러한 개체를 분석하고 개체 내에서 새로운 위협을 탐지하면 데이터베이스에 해당 위협을 식별하는 레코드를 추가합니다. 데이터베이스를 업데이트한 후 개체를 다시 검사하면 Kaspersky Industrial CyberSecurity for Nodes는 해당 개체를 감염된 것으로 식별하고 치료할 수 있습니다. 이러한 개체를 보관할 수 있을 뿐만 아니라 바이러스 급증을 방지할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 분석용 개체를 Kaspersky 전문가에게 전송하려면

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 콘솔 트리에서 **추가** → **저장소** 폴더를 선택합니다.

3. **격리 저장소** 또는 **백업** 폴더로 갑니다.

4. 다음 중 하나를 수행합니다:

   - 개체를 하나 보내려면 해당 개체 이름의 마우스 오른쪽 메뉴에서 **Kaspersky에 전송** 옵션을 선택합니다.
   - 여러 개체를 보내려면 Ctrl 또는 Shift 키를 사용하여 보내려는 개체를 선택하고, 선택한 개체 중 하나를 마우스 오른쪽 버튼으로 클릭해 마우스 오른쪽 메뉴에서 **Kaspersky에 전송** 옵션을 선택합니다.

5. 컴퓨터에 개체를 저장할 폴더를 선택합니다.

6. 그러면 Kaspersky Threat Intelligence Portal로 이동하라는 메시지가 표시됩니다. 저장된 개체를 업로드하여 해당 개체에 관한 전체 정보를 얻을 수 있습니다.

Kaspersky Security Center 웹 콘솔에서 분석용 개체를 Kaspersky 전문가에게 보내려면

1. 웹 콘솔을 엽니다.

2. 콘솔 트리에서 **동작** → **저장소** 폴더를 선택합니다.

3. **격리 저장소** 또는 **파일 백업** 폴더로 갑니다.

4. 목록에서 개체를 선택하고 **Kaspersky에 전송** 버튼을 클릭합니다.

5. 컴퓨터에 개체를 저장할 폴더를 선택합니다.

6. 그러면 Kaspersky Threat Intelligence Portal로 이동하라는 메시지가 표시됩니다. 저장된 개체를 업로드하여 해당 개체에 관한 전체 정보를 얻을 수 있습니다.

애플리케이션을 버전 4.0 이하에서 4.5 이상으로 업그레이드한 후에 격리 저장소 및 백업 저장소의 개체를 마이그레이션했거나, Kaspersky Anti Targeted Attack Platform 또는 Kaspersky Industrial CyberSecurity for Networks 시나리오에 따라 해당 개체를 저장소에 넣었다면, 분석을 위해 이 개체를 Kaspersky로 보낼 때 Kaspersky Security Center 웹 콘솔이나 관리 콘솔을 사용할 수 없습니다.

격리 설정 구성

격리 설정을 구성할 수 있습니다. 새 격리 저장소 설정은 저장 후 즉시 적용됩니다.

Kaspersky Security Center 관리 콘솔에서 격리 저장소 설정을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **보충 → 저장소** 옵션을 선택하고 **설정** 버튼을 클릭합니다.

4. **격리 저장소** 탭을 선택합니다.

5. 격리 설정을 지정합니다(아래 표 참조).

6. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 격리 설정을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보충 → 저장소** 옵션을 선택하고 **구성** 버튼을 클릭합니다.

5. **격리 저장소** 탭으로 갑니다.

6. 격리 설정을 지정합니다(아래 표 참조).

7. 변경 사항을 저장합니다.

파라미터	설명
격리 저장소 크기 제한	이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 격리 저장소에 있는 개체의 총 크기를 모니터링합니다. 지정된 값을 초과하면(기본값 1024MB) Kaspersky Industrial CyberSecurity for Nodes는 *최대 격리 저장소 크기 초과* 이벤트를 기록하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. 그동안 애플리케이션은 새 개체를 격리하지 않습니다. 격리 저장소를 직접 비워야 합니다. 이 기능을 사용하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 격리 저장소에 있는 개체의 총 크기를 모니터링하지 않습니다. 이 기능은 기본적으로 비활성화됩니다.
이용 가능 공간의 임계값	이 확인란을 선택하면 Kaspersky Industrial CyberSecurity for Nodes가 백업의 최소 여유 공간(기본값 50MB)을 모니터링합니다. 여유 공간이 지정된 한계값 아래로 줄어들면 Kaspersky Industrial CyberSecurity for Nodes는 *격리 저장소 여유 공간 한계값 초과* 이벤트를 기록하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. **격리 저장소 크기 제한** 확인란을 선택했다면 **이용 가능 공간의 임계값** 확인란이 활성화됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

개체의 백업 복사본 만들기. 백업

Kaspersky Industrial CyberSecurity for Nodes는 치료되거나 삭제된 개체의 암호화된 복사본을 백업 폴더에 저장합니다.

개체가 복합 개체의 일부인 경우(예: 압축 파일의 일부) Kaspersky Industrial CyberSecurity for Nodes는 해당 복합 개체 전체를 백업 저장소에 저장합니다. 예를 들어 Kaspersky Industrial CyberSecurity for Nodes가 메일 데이터베이스의 개체 중 하나가 감염되었음을 탐지하면 메일 데이터베이스 전체를 백업합니다.

Kaspersky Industrial CyberSecurity for Nodes가 백업 저장소에 저장한 대용량 개체는 시스템 속도를 저하시키고 하드 드라이브의 디스크 공간을 줄일 수 있습니다.

백업의 파일은 원래 폴더나 보호 중인 장치의 다른 폴더로 복원할 수 있습니다. 예를 들어 감염된 파일에 중요 정보가 포함되어 있지만 Kaspersky Industrial CyberSecurity for Nodes가 무결성 손상 및 정보 손실 없이 파일을 치료할 수 없는 경우 해당 파일을 백업 저장소에서 복원할 수 있습니다.

백업 저장소에서 파일을 복원하면 보호 중인 장치가 감염될 수 있습니다.

백업에서 개체 보기

이 섹션에서는 백업의 파일 목록을 보는 방법에 관한 정보를 제공합니다.

Kaspersky Security Center 관리 콘솔에서 백업 개체를 보는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **추가** → **저장소** 폴더를 선택합니다.
3. **백업** 폴더로 갑니다.
4. 백업 저장소에 저장된 개체 정보가 콘솔의 오른쪽 창에 표시됩니다.

Kaspersky Security Center 웹 콘솔에서 백업 개체를 보는 방법

1. 웹 콘솔을 엽니다.
2. 콘솔 트리에서 **동작** → **저장소** 폴더를 선택합니다.
3. **백업** 폴더로 갑니다.
4. 백업 저장소에 저장된 개체 정보가 콘솔의 오른쪽 창에 표시됩니다.

애플리케이션 콘솔에서 백업 개체를 보는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **저장소** → **백업** 옵션을 선택합니다.
2. 백업 저장소에 저장된 개체 정보가 콘솔의 오른쪽 창에 표시됩니다.

백업에 저장된 개체 목록에서 필수 개체를 찾으려면,

개체를 정렬하거나 필터링하십시오.

백업에서 파일 정렬

기본적으로 백업의 파일은 저장된 백업 날짜별로 최근에 저장된 파일부터 정렬되어 있습니다. 필요한 파일을 찾기 위해 결과 창에서 열의 콘텐츠에 따라 파일을 정렬할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 백업의 파일을 정렬하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **추가** → **저장소** 폴더를 선택합니다.
3. **백업** 폴더로 갑니다.
4. 파일 목록에서 개체를 정렬하는데 사용하려는 열 제목을 선택합니다.

선택한 조건에 따라 백업의 파일이 정렬됩니다.

Kaspersky Security Center 웹 콘솔에서 백업의 파일을 정렬하는 방법

1. 웹 콘솔을 엽니다.
2. 콘솔 트리에서 **동작** → **저장소** 폴더를 선택합니다.
3. **백업** 폴더로 갑니다.
4. 파일 목록에서 개체를 정렬하는데 사용하려는 열 제목을 선택합니다.

선택한 조건에 따라 백업의 파일이 정렬됩니다.

애플리케이션 콘솔에서 백업의 파일을 정렬하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **저장소 → 백업** 옵션을 선택합니다.
2. 파일 목록에서 개체를 정렬하는데 사용하려는 열 제목을 선택합니다.

선택한 조건에 따라 백업의 파일이 정렬됩니다.

백업에서 파일 필터링

백업 저장소에서 파일을 찾기 위해 지정한 필터링 기준(필터)을 충족하는 파일만 목록에 표시되도록 파일을 필터링할 수 있습니다.

Kaspersky Security Center 관리 콘솔의 백업 저장소에서 파일 필터링

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **보충 → 저장소** 폴더를 선택합니다.
3. **백업** 폴더로 갑니다.
4. 오른쪽 창에서 **필터 지정 안 됨,** 링크를 클릭합니다.
5. **필터링 설정** 링크를 클릭하고 **필터링 설정** 창에서 필터링할 열을 선택합니다.
6. 선택한 열에 대한 연산자와 값을 지정합니다.
7. 생성된 필터가 저장됩니다.
8. 백업의 모든 개체를 다시 표시하려면 **필터링 설정** 창에서 **모두 지우기**를 클릭합니다.

Kaspersky Security Center 웹 콘솔 백업 저장소에서 파일 필터링

1. 웹 콘솔을 엽니다.
2. 콘솔 트리에서 **동작 → 저장소** 폴더를 선택합니다.
3. **백업** 폴더로 갑니다.
4. 필터 아이콘을 클릭하고 **필터** 탭의 **추가** 버튼을 클릭합니다.
5. 필터링할 속성을 선택합니다.
6. 선택한 속성의 조건과 값을 지정합니다.
7. **적용** 버튼을 클릭합니다.
   필터 설정이 저장됩니다.
8. 백업의 모든 개체를 다시 표시하려면 **필터** 탭에서 **모두 지우기**를 클릭합니다.

애플리케이션 콘솔에서 백업 파일을 필터링하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **저장소** → **백업** 옵션을 선택합니다.
2. 파일 테이블에서 열 제목을 선택하고 왼쪽 상단에 있는 필터 아이콘을 클릭합니다.
3. 필터를 구성하고 **확인** 버튼을 클릭합니다.
   필터 설정이 저장됩니다.

백업 저장소에서 파일 복원

Kaspersky Industrial CyberSecurity for Nodes는 백업 폴더에 암호화된 형식으로 파일을 저장하여 유해한 영향으로부터 보호 중인 장치를 방어합니다.

어떠한 파일도 백업 저장소에서 복원할 수 있습니다.

다음과 같은 경우 파일을 복원해야 할 수 있습니다.

- 원본 감염 파일에 중요한 정보가 포함되어 있는데 Kaspersky Industrial CyberSecurity for Nodes가 이 파일의 무결성을 유지하지 못해 파일에 포함된 정보를 사용할 수 없게 된 경우.
- 이 파일이 보호 중인 장치에 무해한 것으로 간주되어 해당 파일을 사용하려는 경우. Kaspersky Industrial CyberSecurity for Nodes에서 후속 검사 중 이 파일을 감염된 것으로 간주하지 않도록 하기 위해 실시간 파일 보호 작업과 온디맨드 검사 작업에서 처리되지 않도록 해당 파일을 제외할 수 있습니다.

백업 저장소에서 파일을 복원하면 보호 중인 장치가 감염될 수 있습니다.

파일을 복원할 때 복원 중인 파일을 저장할 위치를 선택할 수 있습니다. 기본적으로 원래 위치에 복원되지만, 복원된 개체를 위한 보호 중인 장치의 특수 폴더에 복원하거나 애플리케이션 콘솔이 설치된 보호 중인 장치의 사용자 지정 폴더에 복원할 수 있습니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 파일을 복원하는 경우 백업 저장소에 사본을 만듭니다. 파일 사본은 복원이 끝난 후 백업 저장소에서 삭제할 수 있습니다.

Kaspersky Security Center 관리 콘솔의 백업 저장소에서 파일 복원

1. Kaspersky Security Center 관리 콘솔 트리에서 **추가** → **저장소** 폴더를 선택합니다.
2. **백업** 폴더로 갑니다.
3. 다음 중 하나를 수행합니다:
   - 개체 하나를 복원하려면 해당 개체 이름의 마우스 오른쪽 메뉴에서 **복원** 옵션을 선택합니다.
   - 여러 개체를 복원하려면 **Ctrl** 또는 **Shift** 키를 사용하여 삭제하려는 개체를 선택하고, 선택한 개체 중 하나를 마우스 오른쪽 버튼으로 클릭한 다음 마우스 오른쪽 메뉴에서 **복원**를 선택합니다.
4. 개체가 원래 폴더로 복원됩니다.

Kaspersky Security Center 웹 콘솔 백업 저장소에서 파일 복원

1. 웹 콘솔을 엽니다.
2. 콘솔 트리에서 **동작** → **저장소** 폴더를 선택합니다.
3. **백업** 폴더로 갑니다.
4. 목록에서 개체를 선택하고 **복원** 버튼을 클릭합니다.
5. 개체가 원래 폴더로 복원됩니다.

애플리케이션 콘솔의 백업 저장소에서 파일 복원

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **저장소** → **백업** 옵션을 선택합니다.
2. **백업** 노드의 결과 창에서 다음 동작 중 하나를 수행합니다:
   - 개체 하나를 복원하려면 복원하려는 개체의 마우스 오른쪽 메뉴에서 **복원** 옵션을 선택합니다.
   - 여러 개체를 복원하려면 **Ctrl** 또는 **Shift** 키를 사용하여 복원하려는 개체를 선택하고, 선택한 개체 중 하나를 마우스 오른쪽 버튼으로 클릭한 다음 마우스 오른쪽 메뉴에서 **복원**를 선택합니다.
3. **개체 복원** 창에서 선택한 각 개체에 대해 복원 중인 개체를 저장할 폴더를 지정합니다.

   개체 이름이 창 위쪽에 있는 **개체** 필드에 표시됩니다. 여러 개체를 선택한 경우 선택한 개체 목록의 맨 처음에 있는 개체의 이름이 표시됩니다.

4. 다음 중 하나를 수행합니다:
   - 개체를 원래 위치로 복원하려면 **소스 폴더로 복원** 옵션을 선택합니다.
   - 애플리케이션 설치 중 복원된 개체의 위치로 지정된 폴더에 개체를 복원하려면 **복원을 위해 기본 폴더로 복원** 옵션을 선택합니다.
   - 애플리케이션 콘솔이 설치된 보호 중인 장치의 다른 폴더에 개체를 저장하려면 **로컬 컴퓨터의 폴더로 복원** 옵션을 선택한 다음 필요한 폴더를 선택하거나 경로를 지정합니다.
5. 복원한 후 백업 폴더에 파일 사본을 저장하지 않으려는 경우 **복원 후 저장소에서 개체 제거** 확인란을 선택합니다(기본적으로 이 확인란은 선택 해제되어 있음).
6. 지정된 복원 조건을 선택한 나머지 개체에 적용하려면 **선택된 모든 개체에 적용** 확인란을 선택합니다.
7. **확인** 버튼을 클릭합니다.
8. Kaspersky Industrial CyberSecurity for Nodes가 선택한 개체 중 첫 번째 개체의 복원을 시작합니다.

9. 지정된 위치에 이 이름을 가진 개체가 이미 있는 경우 **이 이름을 가진 개체가 이미 존재합니다** 창이 열립니다.

   a. 다음 Kaspersky Industrial CyberSecurity for Nodes 동작 중 하나를 선택합니다.

   - **교체**: 기존 개체를 복원된 개체로 대치합니다.
   - **이름 바꾸기**: 복원된 개체를 다른 이름으로 저장합니다. 입력 필드에 복원된 새 개체의 파일 이름과 개체의 전체 경로를 입력합니다.
   - **접미사 추가로 이름 변경**: 파일 이름에 접미사를 추가하여 복원된 개체의 이름을 바꿉니다. 입력 필드에 접미사를 입력합니다.

   b. 복원할 개체를 여러 개 선택한 경우 **선택된 모든 개체에 적용** 확인란을 선택하여 선택된 동작(**교체** 또는 **이름 바꾸기**)을 나머지 선택한 개체에 적용하십시오. **이름 바꾸기** 옵션을 선택했다면 **선택된 모든 개체에 적용** 확인란을 사용할 수 없습니다.

   c. **확인** 버튼을 클릭합니다.

   파일이 복원됩니다. 복원 작업에 관한 정보는 시스템 감사 로그에 기록됩니다.

개체 복원 창에서 **선택된 모든 개체에 적용** 옵션을 선택하지 않은 경우, **개체 복원** 창이 다시 열릴 수 있습니다. 이 창을 사용하여 다음 선택한 개체를 저장할 위치를 지정합니다.

백업에서 파일 삭제

Kaspersky Security Center 관리 콘솔의 백업 저장소에서 파일 삭제

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **추가** → **저장소** 폴더를 선택합니다.
3. **백업** 폴더로 갑니다. 오른쪽 창에 백업 저장소에 있는 개체 목록이 표시됩니다.
4. 다음 중 하나를 수행합니다:
   - 개체 하나를 삭제하려면 개체의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
   - 여러 개체를 삭제하려면 **Ctrl** 또는 **Shift** 키를 사용하여 삭제하려는 개체를 선택하고, 선택한 개체 중 하나를 마우스 오른쪽 버튼으로 클릭한 다음 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
5. 선택한 개체가 백업 저장소에서 삭제됩니다.

Kaspersky Security Center 웹 콘솔의 백업 저장소에서 파일 삭제

1. 웹 콘솔을 엽니다.
2. 콘솔 트리에서 **동작** → **저장소** 폴더를 선택합니다.
3. **백업** 폴더로 갑니다.
4. 목록에서 개체를 선택하고 **삭제** 버튼을 클릭합니다.
5. 선택한 개체가 백업 저장소에서 삭제됩니다.

애플리케이션 콘솔의 백업 저장소에서 파일 제거

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **저장소** → **백업** 옵션을 선택합니다.
2. 오른쪽 창에 백업 저장소에 있는 개체 목록이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 개체 하나를 삭제하려면 개체의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
   - 여러 개체를 삭제하려면 **Ctrl** 또는 **Shift** 키를 사용하여 삭제하려는 개체를 선택하고, 선택한 개체 중 하나를 마우스 오른쪽 버튼으로 클릭한 다음 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
4. 선택한 개체가 백업 저장소에서 삭제됩니다.

백업 설정 구성

Kaspersky Security Center 관리 콘솔에서 백업 설정을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보충** → **저장소** 옵션을 선택하고 **설정** 버튼을 클릭합니다.
4. **백업** 탭으로 갑니다.
5. 백업 설정을 지정합니다(아래 표 참조).
6. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 백업 설정을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보충** → **저장소** 옵션을 선택하고 **구성** 버튼을 클릭합니다.
5. **백업** 탭으로 갑니다.
6. 백업 설정을 지정합니다(아래 표 참조).
7. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 백업 설정을 구성하는 방법

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **저장소** → **백업** 옵션을 선택합니다.
2. **백업** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.

3. **속성: 백업** 창에서 백업 설정을 지정합니다(아래 표 참조).

4. 변경 사항을 저장합니다.

백업 설정

파라미터	설명
개체 저장 기간	이 기능을 사용하면 최대 파일 저장 기간이 정의된 시간 간격으로 제한됩니다. 파일 최대 저장 기간의 기본값은 30일입니다. 최대 저장 기간이 만료되면 Kaspersky Industrial CyberSecurity for Nodes가 백업에서 가장 오래된 파일을 삭제합니다.
백업 크기를 다음으로 제한	이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes가 백업 저장소에 있는 개체의 총 크기를 모니터링합니다. 지정된 값을 초과하면(기본값 400MB) Kaspersky Industrial CyberSecurity for Nodes는 *최대 백업 크기 초과* 이벤트를 기록하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. 이 기능을 사용하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 백업 저장소에 있는 개체의 총 크기를 모니터링하지 않습니다. 이 기능은 기본적으로 비활성화됩니다.
다음 이용 가능 공간의 임계값 제한	이 기능을 사용하면 Kaspersky Industrial CyberSecurity for Nodes는 백업의 최소 여유 공간(기본값 100MB)을 모니터링합니다. 여유 공간이 지정된 한계값 아래로 줄어들면 Kaspersky Industrial CyberSecurity for Nodes는 *백업 여유 공간 한계값 초과* 이벤트를 기록하고 이러한 유형의 이벤트에 대한 알림 설정에 따라 알림을 보냅니다. **백업 크기를 다음으로 제한** 확인란을 선택했다면 **다음 이용 가능 공간의 임계값 제한** 확인란이 활성화됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

백업 저장소의 개체 크기가 최대 백업 크기를 초과하거나 사용 가능한 공간의 한계값을 초과하면 Kaspersky Industrial CyberSecurity for Nodes가 계속 백업 저장소에 개체를 저장하면서 알림을 발행합니다.

백업 통계

백업의 현재 상태, 즉 백업 통계에 관한 정보를 확인할 수 있습니다.

백업 통계를 보려면:

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **저장소** → **백업** 옵션을 선택합니다.

2. **백업** 노드의 결과 창에서 **통계** 버튼을 클릭합니다.

백업. 통계 창이 열립니다. **백업: 통계** 창에는 현재 백업 상태에 관한 정보가 표시됩니다(아래 테이블 참조).

현재 백업 상태에 관한 정보

필드	설명
현재 백업 크기	백업 폴더에 있는 데이터의 총 크기입니다. 애플리케이션은 암호화된 형식으로 파일 크기를 계산합니다
전체 개체 수	현재 백업 저장소에 있는 개체의 총 수.

처리되지 않은 위협 제거

Kaspersky Industrial CyberSecurity for Nodes는 어떤 이유로든 처리되지 않은 파일에 대한 정보를 기록합니다. 이 정보는 처리 안 된 보안 위협 목록에 이벤트 형식으로 기록됩니다.

Kaspersky Industrial CyberSecurity for Nodes가 컴퓨터에서 바이러스 및 기타 악성 코드를 검사하는 중에 감염된 파일을 치료하거나 위협을 제거한 경우 해당 파일은 *처리*된 것으로 간주됩니다. Kaspersky Industrial CyberSecurity for Nodes가 지정된 애플리케이션 설정에 따라 이 파일에 대한 동작을 수행하지 않으면 해당 파일이 처리 안 된 보안 위협 목록에 추가됩니다.

Kaspersky Industrial CyberSecurity for Nodes에 처리되지 않은 위협이 있으면 Kaspersky Security Center 콘솔에서 장치 상태가 *심각*로 변경됩니다.

관리 콘솔과 웹 콘솔에서 처리 안 된 보안 위협을 처리할 수 있습니다.

Kaspersky Security Center 콘솔에서 처리 안 된 보안 위협을 처리하려면 처리되지 않은 파일에 대한 데이터를 중앙 관리 서버로 전송하는 기능을 활성화해야 합니다. 데이터 전송은 기본적으로 활성화되어 있습니다.

Kaspersky Security Center 관리 콘솔에서 보안 위협을 처리하는 방법

1. 관리 콘솔에서 **중앙 관리 서버** → **고급** → **저장소** → **처리 안 된 위협** 폴더로 이동합니다.
   처리 안 된 보안위협 목록이 열립니다.
2. 처리할 개체를 선택합니다.
3. 보안 위협을 처리할 방법을 선택합니다:
   - **치료**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.
   - **삭제**. 이 옵션을 선택하면 애플리케이션이 처리 안 된 위협 저장소에서 탐지한 감염 파일을 삭제합니다. 이 경우 애플리케이션은 탐지한 파일을 컴퓨터 메모리에 보관합니다. 컴퓨터에서 위협을 제거하려면 **치료**을 선택합니다.

웹 콘솔에서 보안 위협을 처리하는 방법

1. 웹 콘솔의 메인 창에서 **동작** → **저장소** → **처리 안 된 위협** 옵션을 선택합니다.
   처리 안 된 보안위협 목록이 열립니다.
2. 처리할 개체를 선택합니다.
3. 보안 위협을 처리할 방법을 선택합니다:
   - **치료**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.
   - **삭제**. 이 옵션을 선택하면 애플리케이션이 처리 안 된 위협 저장소에서 탐지한 감염 파일을 삭제합니다. 이 경우 애플리케이션은 탐지한 파일을 컴퓨터 메모리에 보관합니다. 컴퓨터에서 위협을 제거하려면 **치료**을 선택합니다.

네트워크 리소스에 대한 접근을 차단합니다. 차단된 네트워크 세션

이 섹션에서는 원격 장치를 차단하고 차단된 네트워크 세션 목록의 설정을 구성하는 방법을 설명합니다.

차단된 네트워크 세션 목록

네트워크 위협 보호 또는 Anti-Cryptor 구성 요소가 설치되어 있는 경우 기본적으로 차단된 네트워크 세션 목록을 사용할 수 있습니다. 이러한 구성 요소는 차단된 네트워크 세션 목록에 따라 보호 중인 장치 또는 네트워크 연결 스토리지 공유 폴더에서 개체를 암호화, 열기, 실행하려는 원격 시도를 검색합니다. 보호 중인 모든 장치에서 차단된 네트워크 세션에 관한 정보는 Kaspersky Security Center로 전송됩니다. Kaspersky Industrial CyberSecurity for Nodes는 현재 세션을 차단하고 현재 세션과 관련하여 공유 폴더 또는 네트워크 연결 저장소 폴더를 사용할 수 없게 만듭니다.

차단된 네트워크 세션 목록은 다음 작업 중 하나 이상이 활성 모드에서 시작되면 (지정된 조건에서) 채워집니다:

- *네트워크 위협 보호* 작업: 네트워크 공격의 일반적인 활동이 탐지됩니다.

  Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션이 다시 시작될 때와 네트워크 위협 보호 설정이 변경될 때 차단 목록을 지웁니다.

- *Anti-Cryptor* 작업: 네트워크 파일 리소스에 접근하는 장치의 악성 암호화가 탐지됩니다.

악성 활동 또는 암호화 시도가 탐지된 후, 작업은 공격 네트워크 세션에 관한 정보를 차단된 네트워크 세션 목록으로 보내고 애플리케이션은 공격 호스트의 현재 세션에 대한 *경고* 이벤트를 생성합니다. 보호 중인 공유 네트워크 폴더에 접근하려는 이 세션의 모든 시도가 차단됩니다.

공격 네트워크 세션을 시작한 호스트의 로컬 고유 식별자(LUID)가 차단된 네트워크 세션 목록에 추가되면 Kaspersky Industrial CyberSecurity for Nodes는 공격 호스트의 LUID 대신 호스트의 IP 주소를 확인하여 차단된 네트워크 세션 목록에 추가합니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 차단된 네트워크 세션을 목록에 추가한 지 30분 후에 목록에서 제거합니다. 차단된 네트워크 세션 목록에서 네트워크 세션을 삭제하면 네트워크 파일 리소스에 대한 접근이 자동으로 복원됩니다. 차단된 네트워크 세션을 자동으로 차단 해제할 시간을 지정할 수 있습니다.

모든 사용자 계정의 저장소 관리 접근을 제한해도 차단된 네트워크 세션 목록은 계속 사용할 수 있습니다. 차단된 네트워크 세션에 대한 설정은 선택한 사용자 계정에 Kaspersky Industrial CyberSecurity for Nodes를 관리할 수 있는 **권한 편집**이 없으면 변경할 수 없습니다.

차단된 네트워크 세션 목록 관리

악성 활동 또는 암호화 활동을 보이는 네트워크 세션을 차단된 네트워크 세션 목록에 추가하고 해당 세션의 네트워크 파일 리소스에 대한 접근을 차단하려면 다음 구성 요소 중 하나 이상을 활성화해야 합니다:

- 네트워크 위협 보호
- Anti-Cryptor

Kaspersky Security Center 관리 콘솔에서 신뢰하지 않는 호스트 차단 활성화

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **네트워크 활동 제어 → 네트워크 위협 보호 설정** 옵션을 선택하고 **설정** 버튼을 클릭합니다.
4. 창이 열리면 **네트워크 위협 보호** 확인란을 선택합니다.
5. **일반** 탭에서 **차단** 모드를 활성화합니다.
6. **다음 시간 동안 공격 장치 차단** 확인란을 선택하고 차단 시간을 지정합니다.
7. 변경 사항을 저장합니다.

정책 속성에서 Anti-Cryptor 구성 요소에 대한 신뢰할 수 없는 네트워크 세션 차단을 구성하려면:

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **실시간 컴퓨터 보호 → Anti-Cryptor** 옵션을 선택하고 **설정** 버튼을 클릭합니다.
4. 창이 열리면 **Anti-Cryptor** 확인란을 선택합니다.
5. **공유 폴더 보호** 탭으로 이동하고 **공유 폴더 보호** 확인란을 선택합니다.
6. **다음 시간 동안 연결 차단** 확인란을 선택하고 차단 시간을 지정합니다.
7. 필요하다면 IP 주소와 마스크로 보호 범위 및 예외를 지정합니다.
8. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 신뢰하지 않는 호스트 차단 활성화

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **네트워크 활동 제어 → 네트워크 위협 보호** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. 창이 열리면 **네트워크 위협 보호 사용** 확인란을 선택합니다.
6. **차단** 모드 활성화.
7. **다음 시간 동안 공격 장치 차단** 확인란을 선택하고 차단 시간을 지정합니다.
8. 필요하다면 IP 주소로 예외를 지정합니다.
9. 변경 사항을 저장합니다.

Anti-Cryptor 구성 요소에 대해 신뢰할 수 없는 네트워크 세션 차단을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **실시간 컴퓨터 보호** → **Anti-Cryptor** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. 창이 열리면 **Anti-Cryptor 사용** 확인란을 선택합니다.

6. **공유 폴더 보호** 탭으로 이동하고 **외부 암호화로부터 공유 폴더 보호 사용** 확인란을 선택합니다.

7. **연결 차단** 옵션을 선택하고 **공유 폴더에 대한 외부 컴퓨터에서의 암호화 시도 탐지 시.** 섹션에서 차단 시간을 지정합니다.

8. 필요하다면 IP 주소와 마스크로 보호 범위 및 예외를 지정합니다.

9. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 신뢰하지 않는 호스트 차단 활성화

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호** → **네트워크 위협 보호** 옵션을 선택합니다.

2. **네트워크 위협 보호** 노드의 결과 창에서 **속성** 버튼을 클릭합니다.
   속성: 네트워크 위협 보호 창이 열립니다.

3. 창이 열리면 **네트워크 위협 보호** 확인란을 선택합니다.

4. **일반** 탭에서 **차단** 모드를 활성화합니다.

5. **다음 시간 동안 공격 장치 차단** 확인란을 선택하고 차단 시간을 지정합니다.

6. 변경 사항을 저장합니다.

Anti-Cryptor 구성 요소에 대해 신뢰할 수 없는 네트워크 세션 차단을 구성하려면:

1. Kaspersky Industrial CyberSecurity for Nodes 콘솔 트리에서 **실시간 컴퓨터 보호** → **Anti-Cryptor** 옵션을 선택합니다.

2. **Anti-Cryptor** 노드 결과 창에서 **속성**을 클릭합니다.

3. 창이 열리면 **Anti-Cryptor** 확인란을 선택합니다.

4. **공유 폴더 보호** 탭으로 이동하고 **공유 폴더 보호** 확인란을 선택합니다.

5. **다음 시간 동안 연결 차단** 확인란을 선택하고 차단 시간을 지정합니다.

6. 필요하다면 IP 주소와 마스크로 보호 범위 및 예외를 지정합니다.

7. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 차단된 세션 목록 구성

1. 애플리케이션 콘솔 트리에서 **저장소** 노드를 확장합니다.

2. **차단된 네트워크 세션** 하위 노드를 선택합니다.

3. 결과 창에서 **속성** 버튼을 클릭합니다.

4. 창이 열리면 **다음 시간 동안 공격 장치 차단** 확인란을 선택하고 차단 시간을 지정합니다.

5. 차단된 모든 네트워크 세션에 대한 접근을 복원하려면 창 위쪽 **모두 차단 해제**를 클릭합니다.
   모든 네트워크 세션이 목록에서 제거되고 차단이 해제됩니다.

6. 차단된 네트워크 세션 목록에서 네트워크 세션을 제거하려면 결과 창의 목록에서 세션을 하나 이상 선택하고 창 위쪽 **선택한 항목 차단 해제**를 클릭합니다.
   선택한 네트워크 세션의 차단이 해제됩니다.

이벤트 등록. Kaspersky Industrial CyberSecurity for Nodes 로그

이 섹션에는 Kaspersky Industrial CyberSecurity for Nodes 로그를 사용하는 방법에 관한 정보가 나와있습니다.

Kaspersky Industrial CyberSecurity for Nodes 이벤트를 등록하는 방법

Kaspersky Industrial CyberSecurity for Nodes의 이벤트는 다음과 같은 두 가지 그룹으로 나뉩니다.

- 애플리케이션 구성 요소의 작동, Kaspersky Industrial CyberSecurity for Nodes 작업의 개체 처리와 관련된 이벤트입니다.
- 애플리케이션 시작, 작업 생성 또는 삭제, 작업 설정 편집과 같은 Kaspersky Industrial CyberSecurity for Nodes의 관리와 관련된 이벤트입니다.

Kaspersky Industrial CyberSecurity for Nodes는 다음 방법을 사용하여 이벤트를 기록합니다:

- **애플리케이션 구성 요소 작업 로그**. 로그에는 애플리케이션 구성 요소의 작동 중에 발생한 이벤트에 대한 정보가 포함됩니다.
- **시스템 감사 로그**. 시스템 감사 로그는 Kaspersky Industrial CyberSecurity for Nodes 관리와 관련된 이벤트 관련 정보를 포함합니다. 또한 보호 중인 장치의 보안 위반 또는 보안 위반 시도와 관련된 이벤트에 관한 정보도 포함되어 있습니다.
- **이벤트 로그**. 이벤트 로그는 Kaspersky Industrial CyberSecurity for Nodes의 작동 오류 진단에 필요한 이벤트 관련 정보가 포함합니다. 이벤트 로그는 Microsoft Windows 이벤트 뷰어에서 확인할 수 있습니다.

다음 링크에서 다운로드할 수 있는 파일에는 다음 카테고리의 Kaspersky Industrial CyberSecurity for Nodes 이벤트 목록 전체가 포함되어 있습니다.

- Kaspersky Industrial CyberSecurity for Nodes가 이벤트 로그에 기록하는 이벤트입니다.

  WEL-EVENTS.ZIP 다운로드
- Kaspersky Industrial CyberSecurity for Nodes가 중앙 관리 서버로 전송하는 이벤트입니다.

  DOWNLOAD KSC-EVENTS.ZIP

로그 설정 구성

Kaspersky Industrial CyberSecurity for Nodes는 로그의 다음 설정을 편집할 수 있습니다.

- 작업 로그 및 시스템 감사 로그의 이벤트 보관 기간.
- Kaspersky Industrial CyberSecurity for Nodes가 작업 로그 파일 및 시스템 감사 로그 파일을 저장하는 폴더의 위치.
- *데이터베이스가 오래되었습니다*, *데이터베이스가 매우 오래됨*, *중요 영역 검사를 장기간 수행하지 않았습니다* 에 대한 이벤트 생성 한계값.
- Kaspersky Industrial CyberSecurity for Nodes가 작업 로그, 시스템 감사 로그 및 이벤트 뷰어의 Kaspersky Industrial CyberSecurity for Nodes 이벤트 로그에 저장하는 이벤트.
- Kaspersky Industrial CyberSecurity for Nodes가 SIEM 서버로 전송하는 이벤트입니다.

Kaspersky Security Center 관리 콘솔에서 로그 설정을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로그 및 알림** 옵션을 선택합니다.
4. **작업 로그** 섹션에서 **설정** 버튼을 클릭합니다.
   알림 창이 열립니다.
5. 이 창에서 구성할 로그를 선택하고 개별 이벤트에 대한 설정을 지정합니다:
   - 이벤트 저장 위치: 로컬 리포트 또는 Windows 이벤트 로그.
   - 이벤트 알림: 이메일로 알림, 터미널 서비스를 사용하여 알림, 실행 파일을 실행하여 알림.
   - SIEM 서버나 Kaspersky Security Center로의 이벤트 전송 여부.
6. **이벤트 생성 한계값 설정** 버튼을 클릭해 이벤트 생성 한계값을 구성합니다.
7. 열린 창에서 경과 후 *데이터베이스가 오래되었습니다*, *데이터베이스가 매우 오래됨*, *중요 영역 검사를 장기간 수행하지 않았습니다* 이벤트를 등록해야 하는 일수를 지정합니다.
8. **이메일 알림 설정** 버튼을 클릭하여 이메일 알림을 구성합니다.
9. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 로그 설정을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로그 및 알림** → **작업 로그** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. 열린 창의 **알림** 탭에서 구성할 로그를 선택하고 개별 이벤트에 대한 설정을 지정합니다:

   - 이벤트 저장 위치: 로컬 리포트 또는 Windows 이벤트 로그.
   - 이벤트 알림: 이메일로 알림, 터미널 서비스를 사용하여 알림, 실행 파일을 실행하여 알림.
   - SIEM 서버나 Kaspersky Security Center로의 이벤트 전송 여부.

6. **이메일 알림 설정** 탭에서 이메일 알림을 구성합니다.

7. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 로그 설정을 구성하는 방법:

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드의 마우스 오른쪽 메뉴를 엽니다.

2. **속성** 옵션을 선택합니다.
   알림 창이 열립니다.

3. 이 창에서 구성할 로그를 선택하고 개별 이벤트에 대한 설정을 지정합니다:

   - 이벤트 저장 위치: 로컬 리포트 또는 Windows 이벤트 로그.
   - 이벤트 알림: 이메일로 알림, 터미널 서비스를 사용하여 알림, 실행 파일을 실행하여 알림.
   - SIEM 서버나 Kaspersky Security Center로의 이벤트 전송 여부.

4. **이벤트 생성 한계값 설정** 버튼을 클릭해 이벤트 생성 한계값을 구성합니다.

5. 열린 창에서 경과 후 *데이터베이스가 오래되됨(일)*, *데이터베이스가 매우 오래됨(일)*, *중요 영역 검사를 장기간 수행하지 않았음(일)* 이벤트를 등록해야 하는 일수를 지정합니다.

6. **이메일 알림 설정** 버튼을 클릭하여 이메일 알림을 구성합니다.

7. 변경 사항을 저장합니다.

로그에서 이벤트 정렬

기본적으로 로그의 이벤트는 가장 최근에 발생한 이벤트가 가장 먼저 표시됩니다.

로그에서 이벤트 정렬하기:

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드의 마우스 오른쪽 메뉴를 엽니다.

2. 필요한 로그를 선택합니다.

3. 결과 창에서 목록의 이벤트를 정렬하는 데 사용하려는 열 머리글을 선택합니다.

   정렬한 결과는 다음에 로그를 볼 때도 반영됩니다.

로그에서 이벤트 필터링

지정한 필터링 조건(필터)을 충족하는 이벤트의 레코드만 표시하도록 로그를 구성할 수 있습니다.

로그에서 이벤트 필터링하려면:

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드를 확장합니다.
2. 필터를 구성할 로그를 선택하고 결과 창에서 **필터**를 클릭합니다.
   필터 설정 창이 열립니다.
3. 필터를 추가하려면 다음 단계를 수행합니다.
   a. **필드 이름** 목록에서 이벤트 필터링에 사용할 열을 선택합니다.
   b. **작업자** 목록에서 필터링 조건을 선택합니다. 필터링 조건은 **필드 이름** 목록에서 선택된 항목에 따라 달라집니다.
   c. **필드 값**에서 필터에 대한 값을 선택합니다.
   d. **추가** 버튼을 클릭합니다.

   추가한 필터가 **필터 설정** 창의 필터 목록에 나타납니다.
4. 필요하다면 다음 동작 중 하나를 수행합니다.
   - 논리 연산자 "AND"를 사용하여 여러 필터를 결합하려면 **모든 조건이 충족되는 경우** 옵션을 선택합니다.
   - 논리 연산자 "OR"를 사용하여 여러 필터를 결합하려면 **어떤 조건이든 충족되는 경우** 옵션을 선택합니다.
5. **확인** 버튼을 클릭하여 로그 이벤트의 필터링 조건을 저장합니다.

   로그의 이벤트 목록에 필터링 조건을 충족하는 이벤트만 표시됩니다. 필터링된 결과는 다음에 로그를 볼 때도 반영됩니다.

필터 비활성화:

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드를 확장합니다.
2. 필터를 제거할 로그를 선택하고 **필터 제거**를 클릭합니다.

   그러면 로그에 모든 이벤트가 표시됩니다.

로그에서 이벤트 삭제

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 30일 동안 로그 기록을 유지합니다. 로그의 레코드에 대한 보관 기간은 사용자가 변경할 수 있습니다.

로그에서 이벤트를 삭제하려면:

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드를 확장합니다.
2. 이벤트를 삭제할 로그를 선택하고 결과 창에서 **지우기** 버튼을 클릭합니다.
3. 삭제 작업을 확인합니다.

로그가 삭제됩니다.

로그에서 정보 내보내기

로그에서 CSV 또는 TXT 파일로 데이터를 내보낼 수 있습니다.

로그에서 이벤트를 내보내려면:

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드를 확장합니다.
2. 로그를 선택하고 결과 창에서 **로그 내보내기** 버튼을 클릭합니다.
   저장 창이 열립니다.
3. 작업 로그에서 데이터를 내보내려는 파일의 이름, 위치 및 유형을 지정합니다.
4. **저장** 버튼을 클릭합니다.

지정한 파일에 로그의 정보가 저장됩니다.

시스템 감사 로그

Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Industrial CyberSecurity for Nodes의 관리와 관련된 이벤트의 시스템 감사를 수행합니다. 이 애플리케이션은 애플리케이션 시작, Kaspersky Industrial CyberSecurity for Nodes 작업 시작 및 중지, 작업 설정 변경, 온디맨드 검사 작업 생성 및 삭제 등에 관한 정보를 로깅합니다. 또한 보호 중인 장치의 보안 위반 또는 보안 위반 시도와 관련된 이벤트에 대한 정보도로깅합니다. 애플리케이션 콘솔에서 **시스템 감사** 노드를 선택하면 이러한 모든 이벤트의 레코드가 결과 창에 표시됩니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 시스템 감사 로그에 30일 동안 레코드를 저장합니다. 로그의 레코드에 대한 보관 기간은 사용자가 변경할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes가 기본 파일이 아니라 시스템 감사 로그가 포함된 파일을 저장하는 데 사용할 폴더를 지정할 수 있습니다.

구성 요소 및 작업 로그

Kaspersky Industrial CyberSecurity for Nodes 구성 요소 및 작업의 작동에 대한 정보는 구성 요소 또는 **로그 및 알림** 섹션의 작업 이름이 있는 노드를 선택하면 결과 창의 애플리케이션 콘솔에 표시됩니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 구성 요소 및 작업 로그에 30일 동안 레코드를 저장합니다. 작업 - 완료한 순간부터. 작업 로그 및 구성 요소 로그의 레코드 저장 기간은 변경할 수 있습니다.

기본 폴더 외에도, Kaspersky Industrial CyberSecurity for Nodes가 작업 로그 및 구성 요소 로그가 포함된 파일을 저장할 폴더를 지정할 수 있습니다. 또한 Kaspersky Industrial CyberSecurity for Nodes가 작업 로그 및 구성 요소 로그에 기록할 이벤트를 선택할 수도 있습니다.

작업 로그에서는 시작된 이후부터 지금까지 실행된 작업에서 발생한 모든 이벤트에 관한 자세한 정보와 작업 실행 통계 및 작업 설정을 볼 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 작업에 대한 통계 및 정보를 보려면:

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드를 확장합니다.
2. 작업을 선택하고 결과 창에서 **통계** 탭을 선택합니다.

작업 로그에서 Kaspersky Industrial CyberSecurity for Nodes 작업에 대한 통계 및 정보 보기

작업 로그에서는 시작된 이후부터 지금까지 실행된 작업에서 발생한 모든 이벤트에 관한 자세한 정보와 작업 실행 통계 및 작업 설정을 볼 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 작업에 대한 통계 및 정보를 보려면:

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드를 확장합니다.
2. 작업을 선택하고 결과 창에서 **통계** 탭을 선택합니다.

이벤트 뷰어에서 Kaspersky Industrial CyberSecurity for Nodes의 이벤트 로그 보기

Microsoft Management Console용 Microsoft Windows 이벤트 뷰어 스냅인을 사용하여 Kaspersky Industrial CyberSecurity for Nodes의 이벤트 로그를 볼 수 있습니다. 로그에는 Kaspersky Industrial CyberSecurity for Nodes에 등록되고 작동 장애를 진단하는 데 필요한 이벤트가 포함됩니다.

이벤트 로그에 등록할 이벤트를 다음 기준에 따라 선택할 수 있습니다.

- **이벤트 유형 기준**.
- **상세 정보 레벨 기준**. 상세 정보 레벨은 로그에 등록된 이벤트의 중요도에 해당합니다(정보, 중요, 심각 이벤트). 정보 레벨은 모든 이벤트를 등록하므로 가장 상세합니다. 심각 수준은 심각 이벤트만 등록하므로 가장 간결합니다.

Kaspersky Industrial CyberSecurity for Nodes 이벤트 로그를 보려면:

1. **시작** 버튼을 클릭한 다음, 검색 창에 `mmc` 명령을 입력하고 **ENTER** 키를 누릅니다.
   Microsoft 관리 콘솔이 열립니다.
2. **파일** > **스냅인 추가/제거**를 선택합니다.
   스냅인 추가/제거 창이 열립니다.

3. 사용 가능한 스냅인 목록에서 **이벤트 뷰어 스냅인**을 선택하고 **추가** 버튼을 클릭합니다.

   컴퓨터 선택 창이 열립니다.

4. **컴퓨터 선택** 창에서 Kaspersky Industrial CyberSecurity for Nodes가 설치된 보호 중인 장치를 지정하고 **확인**을 클릭합니다.

5. **스냅인 추가/제거** 창에서 **확인**을 클릭합니다.

   Microsoft Management Console 트리에 **이벤트 뷰어** 노드가 나타납니다.

6. **이벤트 뷰어** 노드를 확장하고 **애플리케이션 및 서비스 로그** > **Kaspersky Industrial CyberSecurity for Nodes** 하위 노드를 선택합니다.

Kaspersky Industrial CyberSecurity for Nodes 이벤트 로그가 열립니다.

관리자 및 사용자 알림 방법

Kaspersky Industrial CyberSecurity for Nodes 동작 시 다음 이벤트와 장치의 안티 바이러스 보호 상태를 관리자와 장치에 접근하는 사용자에게 알리도록 애플리케이션을 구성할 수 있습니다.

- 관리자가 선택한 유형의 이벤트에 대한 정보를 받을 수 있습니다.
- 보호 중인 장치 및 터미널 장치 사용자에게 접근하는 LAN 사용자가 실시간 파일 보호 작업에서 *개체 탐지됨* 유형의 이벤트에 대한 정보를 받을 수 있습니다.

관리자 또는 사용자 알림은 다양한 방법으로 활성화할 수 있습니다.

- 터미널 서비스 도구.

  이 방법은 보호 중인 장치를 터미널로 사용되는 경우 보호 중인 터미널 장치 사용자에게 알리는 데 적용할 수 있습니다.

- 실행 파일 실행.

  이 방법은 이벤트 발생 시 보호 중인 장치의 로컬 드라이브에 저장된 실행 파일을 실행합니다.

- 이메일로 보내기.

  이 방법은 이메일을 사용하여 메시지를 전송합니다.

개별 이벤트 유형에 대해 메시지 텍스트를 생성할 수 있습니다. 이 텍스트에는 이벤트에 대해 설명하는 정보 필드를 포함할 수 있습니다. 기본적으로 이 애플리케이션에서는 사전 정의된 메시지를 사용하여 사용자에게 알립니다.

관리자 및 사용자 알림 구성

이벤트 알림 설정에서는 메시지 텍스트를 구성 및 작성하는 방법을 선택할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 이벤트 알림을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **로그 및 알림** 옵션을 선택합니다.

4. **작업 로그** 섹션에서 **설정** 버튼을 클릭합니다.

   알림 창이 열립니다.

5. 알림 방법을 선택할 이벤트를 선택하고 **알림 설정** 버튼을 클릭합니다.

   알림 설정 창이 열립니다.

6. 이메일 알림은 **이메일** 탭에서 이벤트 알림 메시지의 텍스트를 추가할 수 있습니다.

   이벤트에 대한 정보가 포함된 필드를 추가하려면 **변수** 버튼을 클릭하고 드롭 다운 목록에서 관련 필드를 선택합니다. 이 절의 표에는 이벤트 정보가 포함된 필드에 대한 설명이 들어 있습니다.

   기본 이벤트 메시지 텍스트를 복원하려면 **기본값** 버튼을 클릭합니다.

7. 실행 파일을 실행하여 알림을 받으려면 **실행 파일** 탭에서 보호 중인 장치의 로컬 드라이브에 있는 파일을 선택하거나 전체 경로를 입력합니다. 이벤트가 발생하면 보호 중인 장치에서 이 파일이 실행됩니다. 파일을 실행하는 데 사용할 사용자 이름 및 암호를 입력합니다.

   실행 파일의 경로를 지정할 때 시스템 환경 변수를 사용할 수 있지만 사용자 환경 변수는 허용되지 않습니다.

8. 터미널 서비스를 활용한 알림은 **터미널 서비스** 탭에서 이벤트 알림 메시지의 텍스트를 추가할 수 있습니다.

   이벤트에 대한 정보가 포함된 필드를 추가하려면 **변수** 버튼을 클릭하고 드롭 다운 목록에서 관련 필드를 선택합니다. 이 절의 표에는 이벤트 정보가 포함된 필드에 대한 설명이 들어 있습니다.

   기본 이벤트 메시지 텍스트를 복원하려면 **기본값** 버튼을 클릭합니다.

9. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 이벤트 알림을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **로그 및 알림** → **작업 로그** 섹션으로 가서 **구성** 버튼을 클릭합니다.

5. 열린 창에서 알림 방법을 선택할 이벤트를 클릭합니다.

   알림 설정 창이 열립니다.

6. 이메일 알림은 **사용자에게 알림** 섹션에서 **이메일 전송** 확인란을 선택하고 이벤트 알림 메시지의 텍스트를 추가합니다.

   이벤트에 대한 정보가 포함된 필드를 추가하려면 **변수 추가** 버튼을 클릭하고 목록에서 관련 항목을 선택합니다. 이 절의 표에는 이벤트 정보가 포함된 필드에 대한 설명이 들어 있습니다.

   기본 이벤트 메시지 텍스트를 복원하려면 **초기화** 버튼을 클릭합니다.

7. 실행 파일을 실행하여 알림을 받으려면 **관리자에게 알림** 섹션에서 **실행 파일 실행** 확인란을 선택하고 보호 중인 장치의 로컬 디스크에 있는 파일의 전체 경로를 입력합니다. 이벤트가 발생하면 보호 중인 장치에서 이 파일이 실행됩니다. 파일을 실행하는 데 사용할 사용자 이름 및 암호를 입력합니다.

   실행 파일의 경로를 지정할 때 시스템 환경 변수를 사용할 수 있지만 사용자 환경 변수는 허용되지 않습니다.

8. 터미널 서비스를 사용하는 알림은 **관리자에게 알림** 섹션에서 **터미널 서비스 사용** 확인란을 선택하고 이벤트 알림 메시지의 텍스트를 추가합니다.

이벤트에 대한 정보가 포함된 필드를 추가하려면 **변수 추가** 버튼을 클릭하고 목록에서 관련 항목을 선택합니다. 이 절의 표에는 이벤트 정보가 포함된 필드에 대한 설명이 들어 있습니다.

기본 이벤트 메시지 텍스트를 복원하려면 **초기화** 버튼을 클릭합니다.

9. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 이벤트 알림을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드의 마우스 오른쪽 메뉴를 엽니다.
2. **속성** 옵션을 선택합니다.

   알림 창이 열립니다.
3. 알림 방법을 선택할 이벤트를 선택하고 **알림 설정** 버튼을 클릭합니다.

   알림 설정 창이 열립니다.
4. 이메일 알림은 **이메일** 탭에서 이벤트 알림 메시지의 텍스트를 추가할 수 있습니다.

   이벤트에 대한 정보가 포함된 필드를 추가하려면 **변수** 버튼을 클릭하고 드롭 다운 목록에서 관련 필드를 선택합니다. 이 절의 표에는 이벤트 정보가 포함된 필드에 대한 설명이 들어 있습니다.

   기본 이벤트 메시지 텍스트를 복원하려면 **기본값** 버튼을 클릭합니다.
5. 실행 파일을 실행하여 알림을 받으려면 **실행 파일** 탭에서 보호 중인 장치의 로컬 드라이브에 있는 파일을 선택하거나 전체 경로를 입력합니다. 이벤트가 발생하면 보호 중인 장치에서 이 파일이 실행됩니다. 파일을 실행하는 데 사용할 사용자 이름 및 암호를 입력합니다.

   실행 파일의 경로를 지정할 때 시스템 환경 변수를 사용할 수 있지만 사용자 환경 변수는 허용되지 않습니다.
6. 터미널 서비스를 활용한 알림은 **터미널 서비스** 탭에서 이벤트 알림 메시지의 텍스트를 추가할 수 있습니다.

   이벤트에 대한 정보가 포함된 필드를 추가하려면 **변수** 버튼을 클릭하고 드롭 다운 목록에서 관련 필드를 선택합니다. 이 절의 표에는 이벤트 정보가 포함된 필드에 대한 설명이 들어 있습니다.

   기본 이벤트 메시지 텍스트를 복원하려면 **기본값** 버튼을 클릭합니다.
7. 변경 사항을 저장합니다.

이벤트 정보가 포함된 필드

변수	설명
%EVENT_TYPE%	이벤트 유형.
%EVENT_TIME%	이벤트 시간
%EVENT_SEVERITY%	중요도.
%OBJECT%	개체 이름(실시간 컴퓨터 보호 및 온디맨드 검사 작업). 소프트웨어 모듈 업데이트 작업에는 업데이트에 대한 정보와 함께 업데이트 이름 및 웹 페이지 주소가 포함됩니다.
%VIRUS_NAME%	바이러스 백과사전 분류에 따른 개체의 이름. 이 이름은 Kaspersky Industrial CyberSecurity for Nodes가 개체 탐지 시 반환하는 탐지 개체의 전체 이름에 포함됩니다. 작업 로그에서 탐지된 개체의 전체 이름을 볼 수 있습니다.
%VIRUS_TYPE%	Kaspersky 분류에 따라 탐지된 개체의 유형(예: "바이러스" 또는 "트로이 목마"). 이 유형은 Kaspersky Industrial CyberSecurity for Nodes가 감염되었거나 감염 의심 개체를 찾은 경우 반환하는 탐지 개체의 전체 이름에 포함됩니다. 작업 로그에서 탐지된 개체의 전체 이름을 볼 수 있습니다.
%USER_COMPUTER%	*실시간 파일 보호* 작업에서, 장치의 개체에 접근한 사용자의 보호 중인 장치의 이름입니다.
%USER_NAME%	*실시간 파일 보호* 작업에서 장치의 개체에 접근한 사용자의 이름입니다.
%FROM_COMPUTER%	알림이 발생한 보호 중인 장치의 이름.
%EVENT_REASON%	이벤트 발생 사유(일부 이벤트에는 이 필드가 없음).
%ERROR_CODE%	오류 코드("내부 작업 오류" 이벤트에만 해당).

변수	설명
%TASK_NAME%	작업 이름(작업 성능과 관련된 이벤트에만 해당).
%PROTOCOL%	사용 중인 프로토콜입니다.
%MESSAGE%	메시지의 텍스트.
%DEVICE_INSTANCEPATH%	장치 인스턴스의 경로입니다.
%DEVICE_VID%	장치 공급업체
%DEVICE_PID%	컨트롤러의 유형입니다.
%DEVICE_SERIALNUMBER%	장치의 일련 번호입니다.

이메일 알림 구성

Kaspersky Security Center 관리 콘솔에서 이메일 알림을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로그 및 알림** 옵션을 선택합니다.
4. **작업 로그** 섹션에서 **설정** 버튼을 클릭합니다.
   알림 창이 열립니다.
5. **이메일 알림 설정** 버튼을 클릭합니다.
6. 창이 열리면 **이벤트 알림 전송** 확인란을 선택합니다.
7. **보낸 사람**에서 발신자 정보를 지정합니다: 발신자 주소, SMTP 서버, SMTP 서버 포트, 사용자 이름 및 암호.
8. **받는 사람**에서 수신자 이메일 주소를 지정합니다.
9. 설정을 테스트하려면 **테스트 메시지 발송** 버튼을 클릭합니다.

   테스트 메시지 기능은 Kaspersky Security Center 관리 콘솔 및 애플리케이션 콘솔에서만 사용할 수 있습니다.

10. 전송 모드를 지정합니다: **이벤트 발생 즉시 발송** 또는 **스케줄 사용(스케줄이 지정 안 됨)**. 스케줄을 구성하려면 **편집** 버튼을 클릭합니다.
11. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 이메일 알림을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.

4. **로그 및 알림 → 작업 로그** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. 열린 창에서 **이메일 알림 설정** 탭을 선택합니다.
6. **이벤트 알림 전송** 확인란을 선택합니다.
7. 발신자 정보를 지정합니다: 발신자 주소, SMTP 서버, SMTP 서버 포트, 사용자 이름 및 암호.
8. 수신자 이메일 주소를 지정합니다.
9. 전송 모드를 지정합니다: **이벤트 발생 시** 또는 **스케줄에 따라**. 해당한다면 스케줄을 구성합니다.
10. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 이메일 알림을 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **로그 및 알림** 노드의 마우스 오른쪽 메뉴를 엽니다.
2. **속성** 옵션을 선택합니다.
   알림 창이 열립니다.
3. **이메일 알림 설정** 버튼을 클릭합니다.
4. 창이 열리면 **이벤트 알림 전송** 확인란을 선택합니다.
5. **보낸 사람**에서 발신자 정보를 지정합니다: 발신자 주소, SMTP 서버, SMTP 서버 포트, 사용자 이름 및 암호.
6. **받는 사람**에서 수신자 이메일 주소를 지정합니다.
7. 설정을 테스트하려면 **테스트 메시지 발송** 버튼을 클릭합니다.

   테스트 메시지 기능은 Kaspersky Security Center 관리 콘솔 및 애플리케이션 콘솔에서만 사용할 수 있습니다.

8. 전송 모드를 지정합니다: **이벤트 발생 즉시 발송** 또는 **스케줄 사용(스케줄이 지정 안 됨)**. 스케줄을 구성하려면 **편집** 버튼을 클릭합니다.
9. 변경 사항을 저장합니다.

관리 서버와의 상호 작용 구성

Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky Security Center 중앙 관리 서버로 정보를 전송할 개체 유형을 선택합니다.

Kaspersky Security Center 관리 콘솔에서 중앙 관리 서버와의 통합을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. **로그 및 알림** 섹션에서 **중앙 관리 서버와 상호 작용** 하위 섹션의 **설정** 버튼을 클릭합니다.

4. 열린 창에서 Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky Security Center 중앙 관리 서버로 정보를 전송할 다음 개체 유형을 선택합니다.
   - **격리 저장소 파일 정보**
   - **백업된 파일 정보**
   - **처리 안 된 파일 정보**
   - **설치된 장치 정보**
   - **보안 위협 개발 체인 정보**
   - **PLC 프로젝트 정보**
5. 변경 사항을 저장합니다.

   Kaspersky Industrial CyberSecurity for Nodes는 선택된 개체 유형에 대한 정보를 관리 서버로 보냅니다.

Kaspersky Security Center 웹 콘솔에서 중앙 관리 서버로의 통합을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **로그 및 알림** 섹션에서 **중앙 관리 서버와 상호 작용** 하위 섹션의 **구성** 버튼을 클릭합니다.
5. 열린 창에서 Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky Security Center 중앙 관리 서버로 정보를 전송할 다음 개체 유형을 선택합니다.
   - **격리 저장소 파일**
   - **백업 파일**
   - **처리 안 된 파일 정보**
   - **차단된 네트워크 세션**
   - **설치된 장치**
   - **보안 위협 개발 체인**
   - **PLC 프로젝트의 버전**
6. 변경 사항을 저장합니다.

인시던트 생성 구성

중앙 관리 서버 데이터베이스에는 관리되는 보호 중인 장치에서 발생하는 애플리케이션 이벤트에 관한 정보가 저장됩니다.

Kaspersky Security Center 관리 콘솔에서 인시던트 생성을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **로그 및 알림** 옵션을 선택합니다.
4. **인시던트** 섹션에서 **설정** 버튼을 클릭합니다.
5. 열린 창에서 필요하다면 아래 표의 이벤트 조회를 편집합니다. 그러면 Kaspersky Industrial CyberSecurity for Nodes가 이를 사용해 인시던트를 생성합니다.
6. 변경 사항을 저장합니다.
   인시던트 생성 설정이 저장됩니다.

Kaspersky Security Center 웹 콘솔에서 인시던트 생성을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **로그 및 알림** → **인시던트** 섹션으로 가서 **구성** 버튼을 클릭합니다.
5. 열린 창에서 필요하다면 아래 표의 이벤트 조회를 편집합니다. 그러면 Kaspersky Industrial CyberSecurity for Nodes가 이를 사용해 인시던트를 생성합니다.
6. 변경 사항을 저장합니다.
   인시던트 생성 설정이 저장됩니다.

인시던트 생성을 위한 이벤트 목록

이벤트	기본 값
PLC 프로젝트가 참조 프로젝트와 일치하지 않음	선택됨
PLC 프로젝트와 참조 프로젝트를 연결하는 중 오류 발생	선택됨
PLC 프로젝트 정보를 가져오는 중 오류 발생	선택됨
라이센스가 만료되었습니다	선택되지 않음
최종 사용자 라이센스 계약서가 위반됨	선택됨
업데이트 실패	선택되지 않음
데이터베이스가 손상됨	선택되지 않음
데이터베이스가 매우 오래됨	선택되지 않음
데이터베이스가 오래되었습니다	선택되지 않음
네트워크 세션이 신뢰할 수 없는 것으로 표시됨	선택됨
애플리케이션 실행 거부됨	선택되지 않음
통계 전용 모드: 애플리케이션 실행이 거부됨	선택됨
애플리케이션 실행 처리 중 오류 발생	선택되지 않음
신뢰하지 않는 외부 장치 탐지 및 제한됨	선택됨
통계 전용: 신뢰할 수 없는 외부 장치가 탐지됨	선택됨

장치 연결 처리 중 오류 발생	선택됨
감염 또는 기타 개체 탐지됨	선택됨
개체 탐지됨(KSN 신뢰할 수 없는 개체 발견)	선택됨
개체 치료되지 않음	선택되지 않음
개체 백업되지 않음	선택되지 않음
네트워크 공격 탐지됨	선택되지 않음

Portable Auditor

Portable Auditor는 장치의 악성 코드 및 취약점을 검사하고 보안 설정 감사를 수행하며 수신 및 송신 트래픽을 기록할 수 있는 애플리케이션입니다. Portable Auditor는 장치에 연결된 이동식 드라이브에서 실행되며 검사할 장치에 설치할 필요가 없습니다. 따라서 어떤 이유로 Kaspersky Industrial CyberSecurity for Nodes 애플리케이션을 설치할 수 없는 장치도 Portable Auditor를 사용하여 검사할 수 있습니다.

- 격리된 장치
- 다음과 같은 이유로 Kaspersky Industrial CyberSecurity for Nodes를 설치할 수 없는 장치:
  - 조직의 보안 정책
  - 장치 공급업체에서 적용한 제한 사항
  - 장치의 기술적 제한 사항 및 기타 요인
- 게스트 장치

Portable Auditor는 검사한 장치에 작업 흔적을 남기지 않습니다. 기본적으로 애플리케이션이 실행 중에 생성한 모든 파일은 이동식 드라이브에 저장됩니다. 필요한 경우 Portable Auditor를 보호된 이동식 드라이브에 기록할 수 있습니다. 이 경우 애플리케이션 파일은 읽기 전용 파티션에 있으므로 Portable Auditor 이동식 드라이브를 감염된 장치에 연결해도 파일을 보호할 수 있습니다. 검사 결과는 이동식 드라이브의 보호된 영역에 저장되므로 무단 접근으로부터 보호할 수 있습니다.

Portable Auditor가 장치 검사에 사용하는 작업:

- *악성 코드 검사*. 기본적으로 Portable Auditor는 로컬 하드 드라이브, RAM 및 시작 개체에서 바이러스 및 기타 위협 프로그램을 검사합니다. 필요한 경우 검사 범위를 직접 구성할 수 있습니다. 감염된 개체가 탐지되면 애플리케이션은 작업 설정에 지정된 처리 방법을 수행합니다.
- *보안 감사*. Portable Auditor는 장치의 취약점을 검사하고, 운영 체제 보안 요구 사항에 대한 장치의 준수 여부를 평가하며, **장치 구성 정보를** 수집합니다.

  Portable Auditor가 수집하는 장치 관련 정보:

  - 실행 중인 서비스
  - 설치된 드라이버
  - 예약된 작업
  - 설치된 애플리케이션 및 패치
  - 공유 네트워크 리소스의 이름
  - 시작 항목
  - 장치 정보(IP 주소, DNS 이름)

  - 로컬 사용자 및 그룹
  - 하드웨어
- *네트워크 트래픽 기록*. Portable Auditor는 지정된 기간 동안 검사 중인 장치의 수신 및 송신 트래픽을 기록하여 PcapNG 형식의 파일에 저장합니다.

동일한 Portable Auditor 인스턴스를 사용하여 여러 장치를 연속으로 검사할 수 있습니다. 이후 Portable Auditor Console을 사용하여 각 장치의 검사 결과를 개별적으로 관리할 수 있습니다.

애플리케이션은 각 작업의 결과를 바탕으로 내보낼 수 있는 별도의 리포트를 생성합니다. 탐지된 위협 리포트는 Portable Auditor Console에서 볼 수도 있습니다.

Portable Auditor Console 또는 명령줄을 사용하여 Portable Auditor를 관리할 수 있습니다.

하드웨어 및 소프트웨어 요구 사항

이 문서에는 해당 애플리케이션이 테스트를 거쳤으며 정상적으로 작동하는 것이 보장되는 소프트웨어 버전이 나와 있습니다. 애플리케이션이 다른 소프트웨어 버전에서 작동할 수도 있지만, 이러한 구성은 전체 테스트를 거치지 않았으므로 지원 보장 버전 목록에 포함되지 않습니다.

Portable Auditor 생성

휴대용 감사기를 생성하려면 다음이 필요합니다.

- 유효한 라이센스가 적용된 Kaspersky Industrial CyberSecurity for Nodes 애플리케이션이 설치된 장치.
- Kaspersky Industrial CyberSecurity for Nodes 휴대용 감사기 라이센스.
- 2GB 이상의 USB 이동식 드라이브 또는 지원되는 보안 이동식 드라이브:
  - Rutoken EDS 2.0 Flash
  - Rutoken EDS 3.0 Flash

검사 대상 장치의 하드웨어 요구 사항

다음 최소 요구 사항을 충족하는 장치를 검사할 수 있습니다.

- 프로세서: 1GHz 싱글 코어 프로세서, Celeron III 이상 또는 VIA C3
- RAM: 256 MB
- 하드 드라이브 여유 공간: 2GB

보호 중인 장치의 소프트웨어 요구 사항

다음 32비트 또는 64비트 Microsoft Windows 운영 체제 중 하나를 실행하는 장치를 검사할 수 있습니다.

- Windows 2000 Professional SP4 32비트
- Windows XP Professional SP2 32비트/64비트
- Windows XP Professional SP3 32비트
- Windows Vista SP2 32비트/64비트
- Windows 7 SP1 Home / Pro / Enterprise / Ultimate 32비트/64비트
- Windows 8 Pro / Enterprise 32비트/64비트
- Windows 8.1 Pro / Enterprise 32비트/64비트
- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32비트/64비트
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트

- Windows 11 25H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트
- Windows 11 26H2 Home / Pro / Pro for Workstations / Education / Enterprise 64비트

서버 운영 체제:

- Windows Server 2003 SP1 Standard / Enterprise 32비트/64비트
- Windows Server 2008 R2 SP1 Foundation / Standard / Enterprise 64비트
- Windows Server 2008 R2 SP2 Foundation / Standard / Enterprise 64비트
- Windows Server 2008 SP2 Standard / Enterprise 64비트
- Windows Small Business Server 2011 Essentials / Standard 64비트
- Windows MultiPoint Server 2011 64비트
- Windows Server 2012 Foundation / Essentials / Standard 64비트
- Windows Server 2012 R2 Foundation / Essentials / Standard 64비트
- Windows Server 2016 Essentials / Standard 64비트
- Windows Server 2019 RS5 Essentials / Standard 64비트
- Windows Server 2022 21H2 64비트
- Windows Server 2022 버전 20348.350 64비트
- Windows Server 2025 버전 26100.1742 64비트

임베디드 시스템:

- Windows XP Embedded Service Pack 3 32비트
- Windows Embedded POSReady 7 32비트/64비트
- Windows Embedded Standard 7 Service Pack 1 32비트/64비트
- Windows Embedded 8 Standard 32비트/64비트
- Windows Embedded 8.1 Industry Pro 32비트/64비트
- Windows 10 IoT Enterprise 버전 1507 32비트/64비트
- Windows 10 IoT Enterprise 버전 1607 32비트/64비트
- Windows 10 IoT Enterprise 버전 1803 32비트/64비트
- Windows 10 IoT Enterprise 버전 1809 32비트/64비트
- Windows 10 IoT Enterprise 버전 1903 32비트/64비트
- Windows 10 IoT Enterprise 버전 2004 32비트/64비트

- Windows 10 IoT Enterprise 버전 20H2 32비트/64비트
- Windows 10 IoT Enterprise 버전 21H1 32비트/64비트
- Windows 10 IoT Enterprise 버전 21H2 32비트/64비트
- Windows 10 IoT Enterprise 버전 22H2 32비트/64비트
- Windows 11 IoT Enterprise 버전 21H2 64비트
- Windows 11 IoT Enterprise 버전 22H2 64비트
- Windows 11 IoT Enterprise 버전 23H2 64비트
- Windows 11 IoT Enterprise 버전 24H2 64비트
- Windows 11 IoT Enterprise 버전 25H2 64비트

Portable Auditor 기능 제한

Portable Auditor에는 다음과 같은 제한이 있습니다.

- Windows 2000 Professional 장치에서는 *악성 코드 검사* 작업만 실행할 수 있습니다. 운영 체제 제한으로 인해 *보안 감사* 및 *네트워크 트래픽 기록* 작업을 실행할 수 없습니다.
- Windows XP Professional, Windows Vista, Windows Server 2003 및 Windows XP Embedded 장치에서는 운영 체제 제한으로 인해 *네트워크 트래픽 기록* 작업을 실행할 수 없습니다.
- Windows 2000 Professional, Windows XP Professional, Windows Vista, Windows Server 2003 및 Windows XP Embedded 장치에서는 보안 이동식 드라이브에 Portable Auditor를 만들거나 해당 드라이브에서 Portable Auditor를 실행할 수 없습니다.

Portable Auditor 생성

휴대용 감사기를 생성하려면 다음과 같이 하십시오.

1. 유효한 라이선스가 있는 Kaspersky Industrial CyberSecurity for Nodes가 설치된 장치에 지원되는 이동식 드라이브를 연결합니다.

   Windows Server 2022를 실행하는 컴퓨터의 연결 중인 이동식 미디어 목록에 Rutoken 이동식 드라이브가 표시되도록 하려면 USB 카드 판독기용 UMDF2 드라이버를 WUDF 드라이버로 바꿔야 합니다.

2. 알림 영역 애플리케이션 아이콘의 마우스 오른쪽 메뉴에서 **간편 진단 인터페이스** 옵션을 선택합니다.

3. 간편 진단 인터페이스 창이 열리면 **Portable Auditor 생성** 링크를 클릭합니다.

   휴대용 감사기 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

마법사의 다음 단계로 진행하려면 **다음 >** 버튼을 클릭합니다.

1단계. 설정 가져오는

필요한 경우 이전에 생성한 XML 파일에서 휴대용 감사기 설정을 가져옵니다.

1. **설정 가져오기** 버튼을 클릭합니다.

2. 창이 열리면 휴대용 감사기 설정이 포함된 XML 파일을 선택합니다.

3. **열기**를 클릭합니다.

   XML 파일로부터 가져온 설정이 이후 마법사 단계에서 표시됩니다. 해당 설정은 필요에 따라 변경할 수 있습니다.

2단계. 키 파일 추가

휴대용 감사기를 생성하려면 유효한 Kaspersky Industrial CyberSecurity for Nodes 휴대용 감사기 라이선스가 필요합니다.

키 파일 추가:

1. **라이센스 파일 선택** 버튼을 클릭합니다.

2. 창이 열리면 휴대용 감사기의 키 파일을 선택합니다.

3. **열기**를 클릭합니다.

   라이센스 정보가 현재 마법사 창에 표시됩니다.

3단계. 휴대용 감사기 작업 선택

장치에서 휴대용 감사기를 시작할 때 수행할 작업을 선택합니다.

- **안티바이러스 데이터베이스로 선택한 영역 검사**. 이 기능을 활성화하면 휴대용 감사기가 선택한 영역에서 바이러스 및 기타 위협을 검사합니다. 휴대용 감사기는 기본 보안 수준인 **알림**을 적용합니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- **모든 네트워크 인터페이스에서 트래픽 기록**. 이 기능을 활성화하면 휴대용 감사기가 지정된 시간 동안 검사 중인 장치의 인바운드 및 아웃바운드 트래픽을 기록합니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- **보안 감사 실행**. 이 기능을 활성화하면 휴대용 감사기는 설정에 따라 장치의 취약점을 검사하거나, 장치 보안 및 운영 체제 규정 준수를 평가하거나, OVAL 및 XCCDF로 작성된 규칙을 사용하여 장치 구성 데이터를 수집할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

필요한 경우 휴대용 감사기가 검사를 실행할 때 수행할 작업을 선택하도록 구성할 수 있습니다.

4단계. 검사 작업 설정 구성

이 단계는 3단계에서 **안티바이러스 데이터베이스로 선택한 영역 검사** 동작을 선택한 경우에 진행할 수 있습니다.

1. 기본적으로 **로컬 하드 드라이브**, **시스템 메모리 및 프로세스** 및 **시작 개체** 개체가 검사 범위에 추가됩니다.

   개체를 삭제하지 않고 검사 범위에서 제외할 수 있습니다. 개체를 제외하려면 개체 이름 왼쪽에 있는 체크박스를 선택 해제합니다. 작업 설정에서 원하는 개체를 검사 범위에 포함할 수 있습니다.

   검사 범위에서 제외된 개체는 예외 목록에 추가되지 않으며 *악성 코드 검사* 작업의 검사 범위에 포함될 수 있습니다. 예를 들어 로컬 하드 드라이브의 폴더를 제외했지만 **로컬 하드 드라이브** 개체가 검사 범위에 포함된 경우 작업에서 해당 폴더를 검사합니다.

2. 필요한 경우 다음 절차에 따라 검사 범위에 개체를 추가할 수 있습니다.

   a. **추가** 버튼을 클릭합니다.

   b. **검사 범위** 창이 열리면 추가할 개체 유형을 선택합니다:

   - **사전 정의된 범위**, 보호 중인 장치에 대한 사전 정의된 범위 중 하나를 검사 범위에 포함하려는 경우에 선택합니다. 그런 다음 드롭다운 목록에서 필요한 검사 범위를 선택합니다.
   - **디스크, 폴더 또는 네트워크 위치**, 검사 범위에 단일 드라이브 또는 폴더를 포함하려는 경우에 선택합니다. **찾아보기** 버튼을 클릭해 창이 열리면 필요한 범위를 선택합니다.

     로컬 하드 드라이브가 검사 범위에 추가된 경우 Portable Auditor는 해당 드라이브에 연결된 공유 폴더를 검사하지 않습니다. 공유 폴더까지 포함하려면 별도로 추가해야 합니다.

   - **파일**, 검사 범위에 단일 파일을 포함하려는 경우입니다. 그런 다음 열리는 **찾아보기** 창에서 파일을 선택합니다.

   c. **확인** 버튼을 클릭합니다.

   d. 추가하는 각 검사 개체에 대해 a에서 c 단계를 반복합니다.

   추가된 개체는 기본적으로 검사 범위에 포함됩니다. 필요한 경우 항목 이름 왼쪽에 있는 체크박스를 사용하여 검사 범위에서 해당 항목을 제외합니다.

   e. 필요한 경우 **삭제** 버튼을 클릭하여 목록에서 개체를 제거합니다.

3. 검사 설정을 구성합니다:

   a. **검사 설정** 버튼을 클릭합니다.

   b. **일반** 탭의 **개체 검사**에서 검사 범위에 포함할 개체를 선택합니다.

   - **모든 개체**. Portable Auditor가 모든 개체를 검사합니다.
   - **형식에 따라 검사한 개체**. Portable Auditor가 파일 형식에 따라 감염될 수 있는 개체만 검사합니다. 파일 형식은 Kaspersky 전문가가 목록에 추가하며, 해당 목록은 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
   - **안티 바이러스 데이터베이스에 지정된 확장자 목록으로 검사한 개체**. Portable Auditor가 파일 확장자에 따라 감염될 수 있는 개체만 검사합니다. 확장자는 Kaspersky 전문가가 목록에 추가하며, 해당 목록은 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
   - **지정된 확장자 목록에 따라 검사한 개체**. Portable Auditor가 파일 확장자에 따라 감염될 수 있는 개체만 검사합니다. **편집**을 클릭하여 사용자 정의 확장자 목록을 만들 수 있습니다.
   - **디스크 부트 섹터 검사**. 이 체크박스를 선택하면 휴대용 감사기가 보호 중인 장치의 하드 드라이브 및 이동식 드라이브에서 부트 섹터와 마스터 부트 레코드를 검사합니다. 기본적으로 확인란이 선택되어 있습니다.
   - **대체 NTFS 스트림 검사**. NTFS 파일 시스템을 사용하는 드라이브의 대체 파일 및 폴더 스트림 검사. 이 체크박스를 선택하면 휴대용 감사기가 감염 의심 개체 및 해당 개체와 관련된 모든 NTFS 스트림을 검사합니다. 이 확인란을 선택 해제하면 애플리케이션은 탐지 후 감염 의심 개체로 간주한 개체만 검사합니다. 기본적으로 확인란이 선택되어 있습니다.

c. **복합 개체 검사** 섹션에서 검사 범위에 포함할 복합 개체의 유형을 지정합니다:

- **압축 파일**. ZIP, CAB, RAR, ARJ 압축 파일과 기타 압축 파일 형식 검사.
- **SFX 압축파일**. 자동 압축 해제 파일 검사.
- **압축된 개체**. UPX 또는 ASPack과 같은 이진 코드 압축 프로그램으로 압축된 실행 파일 검사.
- **일반 이메일**. Microsoft Outlook 및 Microsoft Outlook Express 메시지와 같은 메일 형식의 파일 검사.
- **이메일 데이터베이스**. Microsoft Outlook 및 Microsoft Outlook Express 메일 데이터베이스 파일 검사. **일반 이메일** 체크박스를 선택하면 이 옵션을 사용할 수 있습니다.
- **삽입된 OLE 개체**. 파일에 삽입된 개체(예: Microsoft Word 매크로 또는 이메일 메시지 첨부 파일) 검사.

d. **추가** 탭으로 갑니다.

e. **일반 설정** 블록에서:

- **검사 후 파일 속성 복원**. 검사 중에 파일을 열면 파일에 마지막으로 접근한 시간이 업데이트됩니다. 따라서 압축 프로그램 및 클라우드 저장소는 파일 데이터를 다시 계산하여 클라우드 또는 백업 저장소로 전송합니다. 다시 계산하는 프로세스를 방지하기 위해 검사를 수행한 후 마지막으로 접근한 시간을 복원할 수 있습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.
- **검사 작업을 위한 CPU 사용량 제한**. 설정은 검사 중에 컴퓨터가 중단되는 것을 방지하는 데 사용됩니다. 이 옵션은 메인 소프트웨어가 중지되지 않아야 하는 산업 시스템에서 매우 중요할 수 있습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.
- **검사 중에 생성된 임시 파일용 폴더**. 기본적으로 임시 파일은 Portable Auditor가 있는 이동식 드라이브의 kavscan\Results\<검사한 장치 이름>\<날짜_시간>\Temp 폴더에 저장됩니다. 필요한 경우 임시 파일을 저장할 폴더를 변경할 수 있습니다. 예를 들어 검사 중 이동식 드라이브의 여유 공간이 부족해지거나 읽기/쓰기 속도가 느려 검사에 너무 오래 걸리는 경우, 검사 중인 장치의 폴더에 임시 파일을 저장하도록 구성할 수 있습니다.

f. **탐지된 개체에 수행할 작업**에서 Portable Auditor가 감염된 개체 및 기타 탐지된 개체에 수행할 동작을 선택합니다.

- **치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지된 모든 감염을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.
- **알림**(기본 값). 이 동작을 선택하면 Portable Auditor는 감염된 개체 또는 기타 탐지된 개체에 아무런 동작도 수행하지 않습니다. 애플리케이션은 리포트에 이벤트만 기록합니다. 이 옵션은 빠른 검사를 수행하거나, 산업용 소프트웨어 모듈을 절대 삭제하면 안 되는 시스템을 검사할 때 사용할 수 있습니다.

g. **치료 - 불가능한 경우 삭제** 옵션이 선택된 경우 **내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거** 기능을 구성합니다. 이 기능을 활성화하면 악성 개체 또는 기타 중첩 개체가 탐지될 때마다 Portable Auditor가 상위 복합 개체 전체를 강제로 삭제합니다. 애플리케이션이 탐지된 하위 개체만 제거할 수 없는 경우(예: 상위 개체를 수정할 수 없는 경우) 상위 파일과 그 모든 컨텐츠가 강제로 제거됩니다. 이 기능을 비활성화하면 Portable Auditor가 상위 개체를 삭제하지 않습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

h. **성능** 탭으로 갑니다.

i. 필요한 경우 **예외**에서 경우 검사 범위에서 제외할 항목을 추가합니다:

- **파일 예외**. 파일을 검사 범위에서 제외하고 탐지 시 제거하지 않으려면 이 기능을 사용하십시오. 전체 경로를 지정하고 마스크를 사용할 수 있습니다. 이 기능은 기본적으로 비활성화됩니다.

- **유형 기준으로 개체 탐지 안 함**. 이 기능을 사용하여 특정 유형의 개체가 탐지되어 추후 삭제되는 것을 방지할 수 있습니다. 개체 이름을 지정하거나 마스크를 사용할 수 있습니다. 이 기능은 기본적으로 비활성화됩니다.

j. **고급 설정**의 설정을 사용하면 검사를 더 빠르게 완료하고 Portable Auditor의 처리 속도를 높일 수 있습니다.

- **검사 시간이 다음을 초과하면 검사 중지(초)**. 이 기능을 활성화한 상태에서 개체 검사 시간이 너무 오래 걸릴 경우 Portable Auditor는 해당 개체 검사를 중지하고 영역 검사를 이어갑니다. 예를 들어 Portable Auditor가 대용량 파일이나 네트워크 환경을 검사하는 데 너무 오래 걸리는 경우 이 옵션을 사용할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다. 60초로 기본 설정되어 있습니다.

- **다음을 초과하는 복합 파일은 검사하지 않음(MB)**. 이 옵션을 활성화하면 Portable Auditor는 지정된 크기보다 큰 개체를 검사에서 제외합니다. 이 옵션은 기본적으로 활성화되어 있습니다. 기본값은 100MB입니다.

- **iChecker 기술 사용**. 이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Portable Auditor 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iChecker 기술에는 제한이 있습니다. 즉, 대용량 파일에서는 사용할 수 없으며 애플리케이션에서 인지하는 구조로 된 파일(예: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR)에만 적용됩니다.

4. 검사 예외를 생성하려면 **예외 설정** 버튼을 클릭합니다.

검사 예외 창이 열립니다.

> Portable Auditor는 예외 목록에 있는 폴더와 개체가 검사 범위에 포함되어 있어도 검사하지 않습니다. 예를 들어 하드 드라이브를 예외 목록에 추가하면 Portable Auditor는 해당 드라이브에 있으며 검사 범위에 포함된 폴더를 검사하지 않습니다.

5. 검사 예외 생성:

a. **추가** 버튼을 클릭합니다.

b. **검사 예외 추가** 창이 열리면 추가할 개체 유형을 선택합니다:

- **사전 정의된 범위**: 보호 중인 장치에 사전 정의된 범위 중 하나를 예외 목록에 포함하려는 경우 선택합니다. 그런 다음 드롭다운 목록에서 필요한 검사 범위를 선택합니다.

- **디스크, 폴더 또는 네트워크 위치**: 검사 범위의 드라이브 또는 폴더 하나를 예외 목록에 포함하려는 경우 선택합니다. **찾아보기** 버튼을 클릭해 창이 열리면 필요한 범위를 선택합니다.

  > 로컬 하드 드라이브를 예외 목록에 추가해도 휴대용 감사기는 이 드라이브에 연결된 공유 폴더를 검사 범위에서 제외하지 않습니다. 공유 폴더를 예외 목록에 포함하려면 별도로 추가해야 합니다.

- **파일**, 검사 범위에 단일 파일을 포함하려는 경우입니다. 그런 다음 열리는 **찾아보기** 창에서 파일을 선택합니다.

c. **확인**을 누릅니다.

d. 추가할 모든 예외에 대해 a–c단계를 반복합니다.

e. **삭제** 버튼을 사용하여 추가한 예외를 삭제할 수 있습니다.

5단계. 네트워크 트래픽 기록 구성

이 단계는 3단계에서 **모든 네트워크 인터페이스에서 트래픽 기록** 동작을 선택한 경우에 진행할 수 있습니다.

필요한 경우 **다음 시간 간격(초) 동안 검사 대상 호스트의 인바운드 및 아웃바운드 네트워크 트래픽 기록** 필드에서 휴대용 감사기가 검사 중인 장치의 인바운드 및 아웃바운드 트래픽을 기록하는 기간을 변경합니다. 30초로 기본 설정되어 있습니다.

6단계. 보안 감사 설정 구성

이 단계는 3단계에서 **보안 감사 실행** 동작을 선택한 경우에 진행할 수 있습니다.

Portable Auditor가 장치 보안을 감사하는 데 사용할 OVAL 및 XCCDF 규칙 소스를 선택합니다.

- **SCADA용 Kaspersky ICS CERT 취약점 데이터베이스**. Portable Auditor는 Kaspersky ICS CERT for ICS 취약점 데이터베이스의 OVAL 규칙에 설명된 모든 취약점이 있는지 장치를 검사합니다. 기본적으로 옵션이 선택되어 있습니다.
- **호스트 구성 데이터를 수집하기 위한 규칙**. Portable Auditor는 장치 구성 정보를 수집합니다. 기본적으로 옵션이 선택되어 있습니다.
- **운영 체제용 규정 준수 및 보안 구성**. Portable Auditor는 장치의 운영 체제 설정이 보안 벤치마크를 준수하는지 확인합니다. 기본적으로 옵션이 선택되어 있습니다.

  검사 대상 장치에 설치된 운영 체제를 미리 알 수 없는 경우가 있으므로 지원되는 모든 운영 체제의 구성이 기본적으로 선택됩니다. 필요한 경우 **구성 선택**를 클릭하여 사용하지 않는 구성을 제외할 수 있습니다.

  SCADA용 Kaspersky ICS CERT 취약점 데이터베이스, 호스트 구성 데이터를 수집하기 위한 규칙, 운영 체제용 규정 준수 및 보안 구성은 Portable Auditor 데이터베이스와 함께 제공됩니다. 따라서 나열된 규칙 소스 중 하나 이상을 사용하여 Portable Auditor를 시작하기 전에 Portable Auditor 데이터베이스가 최신 상태인지 확인하십시오.

- **사용자 지정 규칙 데이터베이스**. Portable Auditor는 사용자 지정 OVAL 및 XCCDF 규칙에 설명된 취약점이 있는지 장치를 검사합니다. 이 옵션을 선택하면 규칙 데이터베이스가 포함된 ZIP 압축 파일을 업로드해야 합니다.

7단계. 이동식 드라이브 선택

휴대용 감사기를 생성할 이동식 드라이브를 선택합니다.

- **이동식 드라이브**. 이동식 USB 드라이브. 드롭다운 목록에서 이동식 드라이브를 선택합니다.
- **보안 이동식 드라이브**. 관리자 암호로 읽기, 복사 및 쓰기가 방지되는 이동식 USB 드라이브입니다. 이 옵션을 선택했다면 다음 마법사 단계에서 보안 이동식 드라이브를 선택합니다.

> 휴대용 감사기를 생성하고 애플리케이션 데이터베이스를 안전하게 복사하는 데 동일한 보안 이동식 드라이브를 동시에 사용할 수 없습니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 휴대용 감사기 데이터를 확인합니다. 여러 이동식 드라이브에 동일한 설정으로 휴대용 감사기를 생성하려는 경우 첫 번째 휴대용 감사기의 데이터를 확인하여 불일치를 조기에 탐지하면 시간을 절약할 수 있습니다. 필요하다면 **생성 후 Portable Auditor 데이터 확인** 확인란을 선택 해제하여 이 기능을 비활성화합니다.

8단계. 보안 이동식 드라이브 구성

> 이 단계는 7단계에서 **보안 이동식 드라이브** 옵션을 선택한 경우에 진행할 수 있습니다.

보안 이동식 드라이브 설정을 구성합니다.

1. 연결된 보안 이동식 드라이브 중 휴대용 감사기를 생성할 드라이브를 선택합니다.
2. 보안 이동식 드라이브의 콘텐츠를 보호하려면 **보안 설정**의 **현재 관리자 PIN 코드 입력** 필드에 해당 드라이브에 설정된 관리자 PIN 코드를 입력합니다.

   > 이 PIN 코드는 나중에 휴대용 감사기와 관련된 작업을 수행할 때 입력해야 합니다.

3. 필요한 경우 현재 관리자 PIN을 변경합니다.

   a. **현재 PIN 코드 변경(숫자와 라틴 문자만 허용)** 확인란을 선택합니다.

   b. 해당 필드에 새 PIN 코드를 입력합니다.

   c. 새 PIN을 확인합니다.

9단계. 이동식 드라이브에 휴대용 감사기 쓰기

이 단계에서는 휴대용 감사기를 생성하기 전에 모든 설정을 검토할 수 있습니다. 필요하다면 **내보내기**를 클릭하여 이 설정을 XML 파일로 내보낼 수 있습니다.

마침 버튼을 클릭하여 지정된 설정으로 휴대용 감사기를 생성합니다.

두 개의 Rutoken 이동식 드라이브를 동일한 장치에 연결하여 애플리케이션 데이터베이스의 안전한 복사 작업과 Portable Auditor 생성 작업을 동시에 실행하는 것은 권장되지 않습니다. 이 경우 작업이 오류로 종료될 수 있습니다.

선택한 이동식 드라이브에 휴대용 감사기가 기록됩니다. 휴대용 감사기가 작동하는 데 필요한 파일과 폴더가 들어 있는 kavscan 폴더가 이동식 드라이브에 생성됩니다.

휴대용 감사기가 이동식 드라이브에 이미 설치되어 있는 경우 마법사는 kavscan 폴더에 있는 기존 휴대용 감사기의 모든 파일을 덮어씁니다. 쓰기를 중단하면 설치 마법사가 변경 사항을 롤백하지 않고 쓰기 작업을 종료합니다.

설정을 완료하면 마법사가 다른 휴대용 감사기를 생성하라는 메시지를 표시합니다.

이동식 드라이브의 데이터 손상을 방지하려면 Portable Auditor로 작업할 때 안전 제거 기능을 사용하십시오.

명령줄 인터페이스를 사용하여 휴대용 감사기를 생성할 수도 있습니다.

Portable Auditor 업데이트

Portable Auditor를 최신 버전으로 업그레이드하려면 현재 버전의 Kaspersky Industrial CyberSecurity for Nodes가 설치된 장치에 이동식 드라이브를 연결하고 Portable Auditor를 새로 생성해야 합니다.

Portable Auditor를 업그레이드하면 이동식 디스크에 저장된 검사 결과가 삭제됩니다.

Portable Auditor 콘솔 사용

Portable Auditor가 있는 이동식 드라이브의 여유 공간이 200KB 미만이면 Portable Auditor 콘솔을 실행할 수 없습니다.

검사할 장치에서 Portable Auditor 콘솔을 시작하려면 다음과 같이 하십시오.

1. Portable Auditor 이동식 드라이브를 장치에 연결합니다.
2. Portable Auditor 이동식 드라이브의 kavscan 폴더로 이동합니다.

3. kavscan_ui.exe 실행 파일을 실행합니다.

> Portable Auditor 작업을 실행하려면 사용자에게 검사할 장치의 관리자 권한이 있어야 합니다.

4. Portable Auditor가 보안 이동식 드라이브에 기록된 경우 PIN을 입력합니다.

Portable Auditor 콘솔 창이 열립니다.

> 검사 중인 장치에서는 Portable Auditor 콘솔 인스턴스를 하나만 실행할 수 있습니다.

Portable Auditor 콘솔을 시작하면 **대시보드** 섹션이 표시됩니다. 이 섹션에는 애플리케이션에 대한 다음 정보가 표시됩니다.

- **작업**에서 Portable Auditor 작업의 현재 상태를 확인할 수 있습니다.
- **통계**에서 이 Portable Auditor 인스턴스가 생성된 이후의 전체 통계를 확인할 수 있습니다.
  - **최근 실행**은 마지막으로 시작한 작업의 완료 날짜입니다.
  - **호스트 검사함**은 하나 이상의 작업이 실행된 고유 장치 수입니다.
  - **위협이 탐지된 호스트**은 보안 위협이 탐지된 검사 장치 수입니다.
  - **악성 코드 검사 작업**은 실행 중인 *악성 코드 검사* 작업의 총수입니다.
  - **보안 감사 작업**은 실행 중인 *보안 감사* 작업의 총수입니다.
  - **네트워크 트래픽 기록 작업**은 실행 중인 *네트워크 트래픽 기록* 작업의 총수입니다.
- **디스크 공간**에서 이동식 드라이브의 여유 공간 및 사용 중인 공간에 대한 정보를 확인할 수 있습니다.

이동식 드라이브에서 Portable Auditor가 생성한 파일을 삭제하려면 다음과 같이 하십시오.

a. **디스크 공간** 블록에서 **저장공간 확보** 링크를 클릭합니다.
   표시된 창에서 이동식 드라이브의 Portable Auditor 작업 리포트, 덤프 파일 및 추적 파일이 차지하는 공간(MB)에 대한 자세한 정보를 확인할 수 있습니다.

b. 해당 섹션에서 **삭제** 버튼을 클릭하고 작업을 확인합니다.

c. 모든 파일을 삭제하려면 **모두 삭제** 버튼을 클릭하고 작업을 확인합니다.

Portable Auditor가 이동식 드라이브에서 선택한 파일을 삭제합니다.

리포트 섹션에서 개별 장치의 작업 리포트 파일을 삭제할 수도 있습니다.

Portable Auditor 콘솔을 종료하려면 다음과 같이 하십시오.

시스템 트레이에 있는 Portable Auditor 아이콘의 마우스 오른쪽 메뉴에서 **종료**를 선택합니다.

Portable Auditor 콘솔 창을 닫아도 애플리케이션은 백그라운드에서 계속 실행됩니다.

이동식 드라이브의 데이터 손상을 방지하려면 Portable Auditor로 작업할 때 안전 제거 기능을 사용하십시오.

장치 검사

Portable Auditor가 있는 이동식 드라이브의 여유 공간이 100 MB 미만이면 작업을 실행할 수 없습니다.

Portable Auditor를 사용하여 장치 검사를 실행하려면 다음 단계를 수행하십시오.

1. 검사할 장치에서 Portable Auditor 콘솔을 시작합니다.

   Portable Auditor 작업을 실행하려면 사용자에게 검사할 장치의 관리자 권한이 있어야 합니다.

2. **작업** 섹션으로 갑니다.

   표시된 창에서 각 작업의 현재 상태, 마지막으로 시작된 날짜와 시간 및 선택한 구성 방법(**기본값** 또는 **사용자 지정**)을 확인할 수 있습니다.

   기본 작업 설정은 Portable Auditor를 만들 때 지정한 설정입니다.

3. 현재 설정으로 작업을 시작하려면 시작할 작업의 체크박스를 선택하고 **선택된 작업 실행** 버튼을 클릭합니다. 기본적으로 Portable Auditor를 만들 때 실행되도록 구성한 작업이 선택됩니다.

   해당 섹션에서 **실행** 버튼을 클릭하여 개별 작업을 시작할 수도 있습니다.

4. 작업의 사용자 지정 설정을 지정하려면 해당 섹션에서 **설정** 버튼을 클릭합니다. 기본 설정을 복원하려면 **기본 설정으로 복원** 링크를 클릭합니다.

   필요한 경우 작업 설정을 내보내고 가져올 수 있습니다.

5. 작업을 시작하면 애플리케이션에 작업의 현재 진행률이 표시됩니다. 여러 작업을 동시에 실행하면 Portable Auditor가 각 작업을 하나씩 순차적으로 실행합니다. **취소** 버튼을 사용하여 작업 실행을 중지할 수 있습니다.

작업이 완료되면 Portable Auditor가 보고서 파일을 이동식 드라이브에 저장하고 **상태** 필드에 결과 정보를 표시합니다. 현재 장치에서 검사 결과를 확인하거나 Portable Auditor를 종료할 수 있습니다.

이동식 드라이브의 데이터 손상을 방지하려면 Portable Auditor로 작업할 때 안전 제거 기능을 사용하십시오.

명령줄을 사용하여 장치 검사를 실행할 수도 있습니다.

악성 코드 검사 작업 설정

악성 코드 검사 작업을 구성하려면:

1. **악성 코드 검사** 블록에서 **설정** 버튼을 클릭합니다.

   검사 설정 창이 열립니다.

2. **설정** 필드에서 **사용자 지정** 옵션을 선택합니다.

3. **검사 범위** 탭에서 검사 범위를 구성합니다. 기본적으로 검사 범위에는 Portable Auditor를 생성할 때 포함된 개체가 포함됩니다.

   개체를 삭제하지 않고 검사 범위에서 제외할 수 있습니다. 개체를 제외하려면 개체 이름 왼쪽에 있는 체크박스를 선택 해제합니다.

   > 검사 범위에서 제외된 개체는 예외 목록에 추가되지 않으며 *악성 코드 검사* 작업의 검사 범위에 포함될 수 있습니다. 예를 들어 로컬 하드 드라이브의 폴더를 제외했지만 **로컬 하드 드라이브** 개체가 검사 범위에 포함된 경우 작업에서 해당 폴더를 검사합니다.

4. 필요한 경우 다음 절차에 따라 검사 범위에 개체를 추가할 수 있습니다.

   a. **추가** 버튼을 클릭합니다.

   b. 열리는 **검사 범위 추가** 창에서 범위, 개별 디스크, 폴더 또는 네트워크 위치를 선택합니다.

   > 로컬 하드 드라이브가 검사 범위에 추가된 경우 Portable Auditor는 해당 드라이브에 연결된 공유 폴더를 검사하지 않습니다. 공유 폴더까지 포함하려면 별도로 추가해야 합니다.

   c. **확인**을 누릅니다.

   추가된 개체가 목록에 표시됩니다.

   d. 추가하는 각 개체에 대해 a-d 단계를 반복합니다.

   추가된 개체는 기본적으로 검사 범위에 포함됩니다. 필요한 경우 항목 이름 왼쪽에 있는 체크박스를 사용하여 검사 범위에서 해당 항목을 제외합니다.

   e. 필요한 경우 **삭제** 버튼을 클릭하여 검사 범위에서 개체를 제거합니다.

   f. 필요한 경우 **편집** 버튼을 클릭하여 기존 검사 범위 개체를 편집할 수 있습니다.

5. 각 검사 범위 개체에 대해 *악성 코드 검사* 작업 설정을 개별적으로 구성할 수 있습니다.

   a. 작업 설정을 구성할 검사 범위 개체를 선택하고 **범위 설정** 버튼을 클릭합니다.

   b. **일반** 탭에서 **범위 설정** 창이 열립니다.

c. **탐지된 개체에 수행할 작업**에서 Portable Auditor가 감염된 개체 및 기타 탐지된 개체에 수행할 동작을 선택합니다.

- **치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지된 모든 감염을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.
- **알림**(기본 값). 이 동작을 선택하면 Portable Auditor는 감염된 개체 또는 기타 탐지된 개체에 아무런 동작도 수행하지 않습니다. 애플리케이션은 리포트에 이벤트만 기록합니다. 이 옵션은 빠른 검사를 수행하거나, 산업용 소프트웨어 모듈을 절대 삭제하면 안 되는 시스템을 검사할 때 사용할 수 있습니다.

d. **개체 검사** 섹션에서 검사 범위에 포함할 개체를 선택합니다:

- **모든 개체**. Portable Auditor가 모든 개체를 검사합니다.
- **형식에 따라 검사한 개체**. Portable Auditor가 파일 형식에 따라 감염될 수 있는 개체만 검사합니다. 파일 형식은 Kaspersky 전문가가 목록에 추가하며, 해당 목록은 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
- **안티 바이러스 데이터베이스에 지정된 확장자 목록으로 검사한 개체**. Portable Auditor가 파일 확장자에 따라 감염될 수 있는 개체만 검사합니다. 확장자는 Kaspersky 전문가가 목록에 추가하며, 해당 목록은 Kaspersky Industrial CyberSecurity for Nodes 데이터베이스에 포함되어 있습니다.
- **지정된 확장자 목록에 따라 검사한 개체**. Portable Auditor가 파일 확장자에 따라 감염될 수 있는 개체만 검사합니다. **찾아보기**을 클릭하여 사용자 정의 확장자 목록을 만들 수 있습니다.

e. **복합 개체 검사** 섹션에서 검사 범위에 포함할 복합 개체의 유형을 지정합니다:

- **압축 파일**. ZIP, CAB, RAR, ARJ 압축 파일과 기타 압축 파일 형식 검사.
- **SFX 압축 파일**. 자동 압축 해제 파일 검사.
- **압축된 개체**. UPX 또는 ASPack과 같은 이진 코드 압축 프로그램으로 압축된 실행 파일 검사.
- **일반 이메일**. Microsoft Outlook 및 Microsoft Outlook Express 메시지와 같은 메일 형식의 파일 검사.
- **이메일 데이터베이스**. Microsoft Outlook 및 Microsoft Outlook Express 메일 데이터베이스 파일 검사. **일반 이메일** 체크박스를 선택하면 이 옵션을 사용할 수 있습니다.
- **삽입된 OLE 개체**. 파일에 삽입된 개체(예: Microsoft Word 매크로 또는 이메일 메시지 첨부 파일) 검사.

f. **치료 - 불가능한 경우 삭제** 옵션이 선택된 경우 **내장 개체 탐지 시 애플리케이션에서 수정할 수 없는 복합 파일을 완전히 제거** 기능을 구성합니다. 이 기능을 활성화하면 악성 개체 또는 기타 중첩 개체가 탐지될 때마다 Portable Auditor가 상위 복합 개체 전체를 강제로 삭제합니다. 애플리케이션이 탐지된 하위 개체만 제거할 수 없는 경우(예: 상위 개체를 수정할 수 없는 경우) 상위 파일과 그 모든 컨텐츠가 강제로 제거됩니다. 이 기능을 비활성화하면 Portable Auditor가 상위 개체를 삭제하지 않습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

g. **추가** 탭으로 갑니다.

h. **검사 최적화**의 설정을 사용하면 검사를 더 빠르게 완료하고 Portable Auditor의 처리 속도를 높일 수 있습니다.

- **검사 시간이 다음을 초과하면 검사 중지(초)**. 이 기능을 활성화한 상태에서 개체 검사 시간이 너무 오래 걸릴 경우 Portable Auditor는 해당 개체 검사를 중지하고 영역 검사를 이어갑니다. 예를 들어 Portable Auditor가 대용량 파일이나 네트워크 환경을 검사하는 데 너무 오래 걸리는 경우 이 옵션을 사용할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다. 1부터 6000초까지의 값을 사용할 수 있습니다. 60초로 기본 설정되어 있습니다.

- **다음을 초과하는 복합 파일은 검사하지 않음(MB)**. 이 옵션을 활성화하면 Portable Auditor는 지정된 크기보다 큰 개체를 검사에서 제외합니다. 이 옵션은 기본적으로 활성화되어 있습니다. 사용 가능한 값: 1~10,000MB. 기본값은 100MB입니다.

- **iChecker 기술 사용**. 이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Portable Auditor 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iChecker 기술에는 제한이 있습니다. 즉, 대용량 파일에서는 사용할 수 없으며 애플리케이션에서 인지하는 구조로 된 파일(예: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR)에만 적용됩니다.

i. 필요한 경우 **검사 예외**에서 경우 검사 범위에서 제외할 항목을 추가합니다:

- **파일 예외**. 파일을 검사 범위에서 제외하고 탐지 시 제거하지 않으려면 이 기능을 사용하십시오. 전체 파일 경로를 지정할 수도 있고 마스크를 사용할 수도 있습니다. 이 기능은 기본적으로 비활성화됩니다.

- **유형 기준으로 개체 탐지 안 함**. 이 기능을 사용하여 특정 유형의 개체가 탐지되어 추후 삭제되는 것을 방지할 수 있습니다. 개체 이름을 지정하거나 마스크를 사용할 수 있습니다. 이 기능은 기본적으로 비활성화됩니다.

6. 필요한 경우 한 검사 범위 개체에서 다른 개체로 사용자 지정 작업 설정을 전송할 수 있습니다.

a. 설정을 전송하려는 검사 범위를 선택합니다.

b. **설정 복제** 버튼을 클릭합니다.

c. 창이 열립니다. 이 창에서 설정을 적용할 검사 범위를 선택합니다.

d. **확인**을 누릅니다.

작업 설정이 선택한 검사 범위로 전송됩니다.

7. 검사 예외를 생성하려면 **예외** 탭으로 이동합니다.

Portable Auditor는 예외 목록에 있는 폴더와 개체가 검사 범위에 포함되어 있어도 검사하지 않습니다. 예를 들어 하드 드라이브를 예외 목록에 추가하면 Portable Auditor는 해당 드라이브에 있으며 검사 범위에 포함된 폴더를 검사하지 않습니다.

8. 검사 예외 생성:

   a. **추가** 버튼을 클릭합니다.

   b. 창이 열립니다. 이 창에서 예외를 지정할 방법을 선택합니다.

   - **카테고리 제외**. 이 옵션을 사용하면 특정 유형의 개체가 탐지된 후 삭제되는 것을 방지할 수 있습니다.
   - **개체 경로 지정**. 파일을 검사 범위에서 제외하고 탐지되더라도 제거하지 않으려면 이 옵션을 사용하십시오. 전체 파일 경로를 지정할 수도 있고 마스크를 사용할 수도 있습니다.

   c. **확인**을 누릅니다.

   d. 추가할 모든 예외에 대해 a–c단계를 반복합니다.

9. **일반 설정** 탭으로 갑니다.

10. **개체 검사** 섹션에서 검사 범위에 포함할 개체 유형을 지정합니다.

    - **디스크 부트 섹터 검사**. 이 기능을 활성화하면 Portable Auditor가 보호 중인 장치의 하드 드라이브 및 이동식 드라이브에 있는 부트 섹터와 마스터 부트 레코드를 검사합니다. 이 옵션은 기본적으로 활성화되어 있습니다.
    - **대체 NTFS 스트림 검사**. NTFS 파일 시스템을 사용하는 드라이브의 대체 파일 및 폴더 스트림 검사. 이 기능을 활성화하면 Portable Auditor가 감염 의심 개체와 해당 개체에 연결된 모든 NTFS 스트림을 검사합니다. 이 기능을 활성화하면 애플리케이션은 탐지된 개체 중 감염 의심 개체로 간주된 개체만 검사합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

11. **컴퓨터 자원 사용**에서 필요한 경우 **검사 작업을 위한 CPU 사용량 제한** 기능을 활성화하십시오. 이 기능을 활성화하면 Portable Auditor가 검사 작업이 검사 대상 장치에서 사용하는 CPU 사용량을 제한합니다. 이 기능은 기본적으로 비활성화됩니다.

    이 기능을 활성화한 경우 **상한** 설정을 관리합니다. 사용 가능한 값 범위: 10~100%. 기본값은 50%입니다

보안 감사 작업 설정

보안 감사 작업을 구성하려면:

1. **보안 감사** 블록에서 **설정** 버튼을 클릭합니다.

   보안 감사 설정 창이 열립니다.

2. **설정** 필드에서 **사용자 지정** 옵션을 선택합니다.

3. Portable Auditor가 장치 보안을 감사하는 데 사용할 OVAL 및 XCCDF 규칙 소스를 선택합니다.

   - **SCADA용 Kaspersky ICS CERT 취약점 데이터베이스**. Portable Auditor는 Kaspersky ICS CERT for ICS 취약점 데이터베이스의 OVAL 규칙에 설명된 모든 취약점이 있는지 장치를 검사합니다. 기본적으로 옵션이 선택되어 있습니다.
   - **호스트 구성 데이터를 수집하기 위한 규칙**. Portable Auditor는 장치 구성 정보를 수집합니다. 기본적으로 옵션이 선택되어 있습니다.
   - **운영 체제용 규정 준수 및 보안 구성**. Portable Auditor는 장치의 운영 체제 설정이 보안 벤치마크를 준수하는지 확인합니다. 기본적으로 옵션이 선택되어 있습니다.

검사 대상 장치에 설치된 운영 체제를 미리 알 수 없는 경우가 있으므로 지원되는 모든 운영 체제의 구성이 기본적으로 선택됩니다. 필요한 경우 **구성 선택**를 클릭하여 사용하지 않는 구성을 제외할 수 있습니다.

SCADA용 Kaspersky ICS CERT 취약점 데이터베이스, 호스트 구성 데이터를 수집하기 위한 규칙, 운영 체제용 규정 준수 및 보안 구성은 Portable Auditor 데이터베이스와 함께 제공됩니다. 따라서 나열된 규칙 소스 중 하나 이상을 사용하여 Portable Auditor를 시작하기 전에 Portable Auditor 데이터베이스가 최신 상태인지 확인하십시오.

- **사용자 지정 규칙 데이터베이스**. Portable Auditor는 사용자 지정 OVAL 및 XCCDF 규칙에 설명된 취약점이 있는지 장치를 검사합니다.

4. **사용자 지정 규칙 데이터베이스** 옵션을 선택한 경우 규칙 데이터베이스를 다운로드합니다.

   a. **구성** 버튼을 클릭합니다.

   b. 창이 열리면 규칙 데이터베이스가 포함된 ZIP 압축 파일을 지정합니다.

   c. OVAL 규칙 및 XCCDF 규칙이 들어 있는 XML 파일이 포함된 압축 파일을 하나만 로드할 수 있습니다.

   d. **열기** 버튼을 클릭합니다.

5. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

네트워크 트래픽 기록 작업 설정

네트워크 트래픽 기록 작업을 구성하려면:

1. **네트워크 트래픽 기록** 블록에서 **설정** 버튼을 클릭합니다.
   네트워크 트래픽 기록 설정 창이 열립니다.

2. **설정** 필드에서 **사용자 지정** 옵션을 선택합니다.

3. **다음 시간 간격(초) 동안 검사 대상 호스트의 인바운드 및 아웃바운드 네트워크 트래픽 기록** 필드에서 Portable Auditor가 검사 대상 장치의 인바운드 및 아웃바운드 트래픽을 기록하는 기간을 변경합니다. 사용 가능한 값 범위: 1~1800초. 기본값은 30초입니다.

4. **확인** 버튼을 클릭해 변경 사항을 저장합니다.

작업 설정 가져오기 및 내보내기

내보내기/가져오기 기능을 사용하여 Portable Auditor 인스턴스 간에 작업 설정을 전송할 수 있습니다.

작업 설정을 구성 파일로 내보내려면 다음을 수행합니다.

1. **작업** 섹션에서 **설정 내보내기** 링크를 클릭합니다.

2. 열리는 창에서 **찾아보기** 버튼을 클릭합니다.

3. 작업 설정을 내보낼 XML 파일의 이름을 입력하고 이 파일을 저장할 폴더를 선택합니다.

4. **내보내기** 버튼을 클릭합니다.

   Portable Auditor는 사용자 지정 작업 설정, 기본 작업 설정 및 사용자 지정 OVAL 또는 XCCDF 규칙(있는 경우)을 XML 파일로 내보냅니다.

구성 파일에서 작업 설정을 가져오려면 다음을 수행합니다.

1. **작업** 섹션으로 갑니다.

2. **설정 가져오기** 링크를 클릭합니다.

3. 창이 열리면 **찾아보기** 버튼을 클릭하고 Portable Auditor 설정이 포함된 XML 파일을 선택합니다.

4. **가져오기** 버튼을 클릭합니다.

   파일의 작업 설정이 Portable Auditor의 사용자 지정 작업 설정을 재정의합니다.

라이센스 정보 보기

현재 라이센스에 관한 정보를 보려면,

Portable Auditor 콘솔에서 **라이센스** 섹션으로 이동합니다.

현재 라이센스에 관한 일반 정보가 결과 창에 표시됩니다(아래 표 참조).

라이센스에 관한 일반 정보

필드	설명
키 상태	키 상태 및 라이센스 유형
라이센스 키	Portable Auditor를 활성화하는 데 사용한 키의 번호입니다.
남은 일수	라이센스가 만료될 때까지 남은 일수입니다.
만료 날짜	라이센스 만료 날짜 및 시간입니다.
활성화 날짜	애플리케이션 활성화 날짜입니다.

라이센스 섹션에서는 만료 알림에 색상 표시도 사용됩니다.

- *빨간색*은 라이센스가 만료될 때까지 남은 기간이 10일 미만임을 의미합니다.
- *노란색*은 라이센스가 만료될 때까지 11~30일이 남았음을 의미합니다.
- *녹색*은 라이센스가 만료될 때까지 30일 넘게 남았음을 의미합니다.

라이센스가 만료되면 새 키 파일을 사용하여 Portable Auditor를 처음부터 생성해야 합니다.

검사 결과 보기

Portable Auditor 작업 결과를 보려면:

1. **리포트** 섹션으로 갑니다.
   결과 창에는 Portable Auditor가 작업 결과를 저장한 장치 목록이 표로 표시됩니다.
2. 검사 결과를 내보낼 수 있습니다.
   a. 검사 결과를 내보낼 장치를 하나 이상 선택합니다. **CTRL** 또는 **SHIFT** 키를 누른 상태에서 클릭하여 여러 장치를 선택할 수 있습니다. 모든 장치를 선택하려면 **모두 선택** 버튼을 클릭합니다.
   b. **내보내기** 버튼을 클릭하고 내보낼 폴더를 선택합니다.
   Portable Auditor는 kavscan\Results\<검사한 장치 이름> 폴더의 내용을 선택한 폴더로 내보냅니다.
3. 내보낸 후 **지우기** 버튼을 클릭하여 이동식 드라이브에서 검사 결과 파일을 삭제할 수 있습니다.
4. 작업 리포트를 보려면 장치를 선택하고 **보기** 버튼을 클릭합니다.
5. 창이 열리면 리포트를 보려는 작업의 이름을 클릭합니다.
   작업이 성공적으로 완료되면 창 오른쪽에 리포트가 표시됩니다.
   - *악성 코드 검사* 작업의 경우 위협 정보가 포함된 표가 표시됩니다.
     - **개체 이름**은 감염된 파일의 이름입니다.
     - **위협 이름**은 Kaspersky IT 백과사전에 등재된 보안 위협의 이름입니다.
     - **개체 경로**은 검사한 장치에서 탐지된 개체의 전체 경로입니다.
     - **검사 시간**은 개체가 탐지된 시간입니다.
     - **이유**은 탐지된 개체를 애플리케이션이 탐지하지 못한 이유입니다.

     악성 코드 검사 작업 리포트 내보내기 버튼을 사용하여 작업 리포트를 내보낼 수 있습니다. Portable Auditor는 탐지된 보안 위협에 대한 리포트가 포함된 ZIP 압축 파일을 내보내 지정된 폴더에 저장합니다.
   - *보안 감사* 및 *네트워크 트래픽 기록* 작업의 경우 Portable Auditor 콘솔에서 리포트를 볼 수 없습니다. 이러한 작업의 결과를 보려면 **내보내기** 버튼을 클릭하여 리포트를 내보내야 합니다.

휴대용 감사기 결과 파일 및 스토리지

보안 이동식 드라이브에 기록된 휴대용 감사기 결과는 숨겨져 있습니다. 이러한 휴대용 감사기의 결과에 접근하려면 휴대용 감사기 콘솔 또는 명령줄에서 사용 가능한 다른 매체로 결과를 내보내야 합니다.

검사가 완료되면 kavscan 폴더에 결과 폴더가 생성됩니다. 이는 다음과 같은 구조를 가지고 있습니다:

- <검사한 장치 이름>: 검사하는 장치의 이름을 딴 폴더로 다음 하위 폴더를 포함합니다:
  - <날짜_시간>: YYYY-MM-DD_HH-MM-SS 형식으로 장치 검사 날짜 및 시간이 이름에 포함된 폴더. 검사 설정에 따라 다음 하위 폴더를 포함할 수 있습니다:
    - 검사 작업이 **치료 - 불가능한 경우 삭제** 모드로 실행된 경우 백업 폴더에는 애플리케이션에서 치료를 시도한 원본 파일의 백업 복사본이 포함됩니다. 각 파일의 이름에는 검사한 장치에서 해당 파일이 있는 경로가 포함됩니다. 각 파일은 암호가 걸려 있는 .ZIP 압축 파일로 압축되어 있습니다. `infected`를 파일에 접근하기 위한 암호로 사용하십시오.
    - 탐지: 탐지에 관한 서비스 정보가 포함된 폴더. 폴더의 컨텐츠는 Kaspersky Industrial CyberSecurity for Networks에서 경고 세부 정보를 표시하는 데 필요합니다.
    - Oval: 감사 보안 규칙의 각 소스에 대한 XML 및 HTML 리포트가 있는 ZIP 압축 파일이 포함된 폴더. 보안 감사 수행 시 폴더가 존재합니다.
    - 네트워크: 장치의 인바운드 및 아웃바운드 트래픽 덤프가 포함된 폴더. *네트워크 트래픽 기록* 작업이 실행된 경우 폴더가 존재합니다.
    - Report 폴더에는 휴대용 감사기 보고서가 포함된 report.txt 파일이 있습니다.
    - 결과: 완료한 검사 결과가 포함된 아티팩트가 들어 있는 결과_<검사한 장치 이름> _<검사 날짜_시간>.zip 압축 파일이 포함된 폴더. 이 압축 파일은 검사 결과를 Kaspersky Industrial CyberSecurity for Networks로 가져오는 데 필요합니다.
    - Temp: 검사 중에 생성된 임시 데이터가 들어 있는 폴더.

일반 휴대용 감사기 리포트 보기

작업이 완료되면 kavscan\Results\<검사한 장치 이름>\<날짜_시간>\Reports에 report.txt 파일이 생성됩니다.

이 리포트는 다음 섹션으로 구성되어 있습니다:

- **제목**
  - 휴대용 감사기 버전
  - 검사가 시작된 날짜 및 시간
  - 검사를 시작하는 데 사용된 명령
  - 검사를 시작한 장치의 이름
  - 검사한 장치의 운영 체제
  - 네트워크 인터페이스: 이름, MAC 주소, IP 주소
  - 검사를 시작한 사용자
  - 데이터베이스가 생성된 날짜 및 시간
  - *보안 감사* 작업이 수행된 날짜 및 시간

- 휴대용 감사기가 장치 보안을 감사하는 데 사용할 규칙 소스
- *보안 감사* 작업이 완료된 날짜 및 시간
- *악성 코드 검사* 작업이 수행된 날짜 및 시간
- 검사 범위

- **이벤트 목록**

  이벤트 목록에는 `/type=full` 및 `/type=critical` 모드의 검사 세부 정보가 포함됩니다. 여기에는 검사한 장치의 이름과 탐지된 개체에 수행된 처리가 포함됩니다.
  `/type=short` 모드에서는 이벤트 목록이 생성되지 않습니다.

- **통계**

  리포트의 이 섹션은 검사가 완료된 날짜 및 시간과 다음 카테고리의 개체 수를 포함합니다:

  - 탐지됨
  - 탐지된 감염 개체 및 기타 개체
  - 치료되지 않은 개체
  - 검사되지 않은 개체
  - 처리 오류
  - 치료된 개체
  - 개체 삭제 완료
  - 암호로 보호된 개체
  - 개체 처리 완료.
  - 검사가 완료된 날짜 및 시간

일반 검사 리포트의 세부 정보를 구성하려면 다음과 같이 하십시오.

1. Portable Auditor 콘솔에서 **오작동 진단** 섹션으로 이동합니다.
2. **리포트 유형** 블록에서 적절한 세부 정보 수준을 선택합니다.
   - **전체**: 모든 이벤트 유형이 포함된 전체 검사 리포트
   - **심각**: 심각 이벤트만 포함된 검사 리포트
   - **요약**: 이벤트 없이 일반 통계만 포함된 검사 리포트

Portable Auditor 데이터베이스 업데이트

Portable Auditor 콘솔의 **업데이트** 섹션에서 애플리케이션 데이터베이스의 릴리스 날짜와 시간을 확인할 수 있습니다.

Portable Auditor 데이터베이스를 업데이트하려면:

1. 다음 방법 중 하나로 업데이트된 애플리케이션 데이터베이스를 다운로드하십시오:

   - 배포 지점 저장소 사용.

     Kaspersky Industrial CyberSecurity for Nodes가 설치된 장치에서 장치 또는 장치 그룹에 대한 기존 *배포 지점의 저장소로 업데이트 다운로드* 작업을 생성하거나 구성합니다. 작업 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오. 작업을 시작하십시오.

     장치에 설치된 Kaspersky Industrial CyberSecurity for Nodes 버전은 Portable Auditor를 생성하는 데 사용된 Kaspersky Industrial CyberSecurity for Nodes 버전과 일치하거나 그 이상이어야 합니다. 그렇지 않으면 업데이트된 애플리케이션 데이터베이스에 Portable Auditor를 제대로 실행하는 데 필요한 특정 파일이 포함되지 않을 수 있습니다.

   - Kaspersky Updater Utility 사용.

     Kaspersky Updater Utility를 사용하여 장치의 폴더에 최신 애플리케이션 데이터베이스를 다운로드하십시오. Kaspersky 업데이트 유틸리티 사용에 대한 자세한 내용은 Kaspersky 기술 자료를 참조하십시오.

2. Portable Auditor가 포함된 이동식 드라이브를 업데이트된 애플리케이션 데이터베이스가 있는 장치에 연결합니다.

3. Portable Auditor 콘솔 시작.

4. **업데이트** 섹션으로 갑니다.

5. **소스를 선택하고 업데이트** 버튼을 클릭합니다.

6. 창이 열립니다. 이 창에서 1단계에서 다운로드한 애플리케이션 데이터베이스가 있는 폴더를 지정합니다.

Portable Auditor는 Bases 폴더의 애플리케이션 데이터베이스를 업데이트하고 데이터베이스를 검사합니다. **상태** 필드에서 업데이트 작업의 상태를 확인할 수 있습니다. 작업 상태는 색상으로도 표시됩니다.

- *빨간색*은 업데이트가 오류로 완료되었음을 의미합니다.
- *녹색*은 업데이트가 완료되었거나 Portable Auditor를 생성한 후 업데이트가 시작되지 않았음을 의미합니다.

Portable Auditor 추적 로그 및 메모리 덤프 기록 구성

Portable Auditor의 추적 및 덤프를 구성하려면 다음과 같이 하십시오.

1. Portable Auditor 콘솔에서 **오작동 진단** 섹션으로 이동합니다.

2. **덤프 설정**에서 **덤프 파일 생성** 체크박스를 선택하여 덤프 생성을 활성화합니다. 기본적으로 메모리 덤프 기록이 비활성화되었습니다.

   Portable Auditor는 Portable Auditor 콘솔 덤프 파일을 kavscan\Crash Dumps\Application Console Crash Dumps 폴더에 저장하고 애플리케이션 덤프 파일을 kavscan\Crash Dumps\Application Crash Dumps 폴더에 저장합니다.

3. **추적 로그 설정**에서 **추적 활성화** 체크박스를 선택하여 Portable Auditor 추적을 활성화합니다. 기본적으로 Portable Auditor 작업 추적은 비활성화되어 있습니다.

4. 필요한 경우 디버그 정보의 상세 수준을 변경합니다.

   - **보통**은 추적 파일이 모든 오류 및 경고에 관한 메시지와 Portable Auditor의 정상 작동에 관한 정보를 저장한다는 뜻입니다(기본값).
   - **중요**는 추적 파일이 모든 오류, 경고, 추가 정보에 관한 메시지를 저장한다는 뜻입니다.
   - **자세히**은 추적 파일이 Portable Auditor 작업에 관한 모든 정보를 저장한다는 뜻입니다.

   Portable Auditor는 Portable Auditor 콘솔 추적 파일을 kavscan\Traces\Application Console Traces 폴더에 저장하고 애플리케이션 추적 파일을 kavscan\Traces\Application Traces 폴더에 저장합니다.

5. 덤프 및 추적 파일을 내보내려면 **덤프 및 추적 파일 내보내기** 버튼을 클릭하고 열리는 창에서 내보낼 폴더를 선택합니다.

명령줄을 사용하여 Portable Auditor Console 사용

Portable Auditor를 시작하려면 다음과 같이 하십시오.

1. Portable Auditor가 포함된 이동식 드라이브를 검사할 장치에 연결합니다.
2. 장치에 대한 로컬 관리자 권한으로 명령줄 해석기를 시작하십시오.
3. `cd /d` 명령을 사용하여(예: `cd /d "E:\kavscan"`, 여기서 `E`는 이동식 드라이브의 문자) kavscan.exe 파일이 포함된 폴더로 변경합니다.
4. 다음 중 하나를 수행합니다:

   - Portable Auditor를 기록하기 전에 지정한 설정으로 Portable Auditor를 시작하려면 다음 명령을 실행합니다.

     ```
     KAVSCAN SCAN
     ```

   - Portable Auditor를 생성할 때 지정한 옵션과 다른 옵션으로 Portable Auditor를 실행하려면 다음 명령을 실행합니다.

     ```
     KAVSCAN SCAN [/AV] [/TRAFFIC=<기간(초)>] [/OVAL=<보안 감사 규칙이 포함된 ZIP 압축 파일의 전체 경로>]
     [/MYCOMPUTER] [/FIXED] [/REMOVABLE] [/REMOTE] [/SHARED] [/MEMORY] [/STARTUP] [/DRIVE=<디스크>] [/FOLDER=<검
     사할 폴더의 전체 경로>] [/FILE=<이름을 포함한 파일의 전체 경로>] [/CURE=<yes|no>] [/TRACE=
     <important|normal|detailed>] [/DUMP] [/REPORT=<full|critical|short>] [/SETTINGS=<사용자 지정 설정 파일의 전체
     경로>]
     ```

     대화 상자 대신 명령줄에 `?` 문자가 표시된다면, 운영 체제와 Kaspersky Industrial CyberSecurity for Nodes의 인코딩이 일치하지 않는다는 뜻입니다. 대화 상자를 올바르게 표시하려면 유니코드를 지원하지 않는 애플리케이션의 언어를 선택하도록 운영 체제 설정을 관리해야 합니다. Kaspersky Industrial CyberSecurity for Nodes에서 사용 중인 언어를 선택해야 합니다.

     명령 도움말을 보려면 `KAVSCAN HELP` 명령을 실행합니다.

/CURE, /TRACE, /DUMP, /REPORT를 제외한 모든 KAVSCAN SCAN 스위치는 원래 Portable Auditor 설정을 재정의합니다. 예를 들어 KAVSCAN SCAN 스위치 /AV, /TRAFFIC, /OVAL 이 어떤 조합으로든 또는 단독으로 지정된 경우, 원래 Portable Auditor 설정에 모든 처리가 포함되어 있더라도 Portable Auditor는 지정된 키로 정의된 처리만 수행합니다.

5. 보안 이동식 드라이브에서 Portable Auditor를 시작하는 경우 Portable Auditor를 처음 구성할 때 설정한 관리자 암호를 입력합니다.

Portable Auditor 시작 명령 옵션

파라미터	설명
/AV	바이러스 및 기타 위협에 대한 검사를 시작하십시오.
/TRAFFIC=<duration in seconds>	지정된 시간 동안 검사 중인 장치의 인바운드 및 아웃바운드 트래픽을 기록합니다. 1부터 1800까지의 값을 사용할 수 있습니다. 명령에서 기록 기간을 설정하지 않으면 Portable Auditor는 기본 기록 기간을 사용합니다. Portable Auditor 설정에 값을 지정하지 않으면 기본값인 30초가 사용됩니다.
/OVAL=<full path to the ZIP archive containing security audit rules>	지정된 ZIP 압축 파일 내의 규칙에 따라 보안 감사 작업을 시작하십시오. ZIP 압축 파일에는 OVAL로 작성된 규칙이 있는 XML 파일 또는 XCCDF로 작성된 규칙이 있는 XML 파일 세트가 포함되어야 합니다. 이름을 포함하여 ZIP 파일의 전체 경로를 제공해야 합니다. 규칙이 포함된 ZIP 압축 파일의 전체 경로를 지정하지 않으면 Portable Auditor가 원래 설정에 따라 보안 감사를 실행합니다.
/MYCOMPUTER	전체 컴퓨터 검사를 시작하십시오.
/FIXED	모든 로컬 하드 드라이브의 검사를 시작하십시오.
/REMOVABLE	모든 이동식 드라이브의 검사를 시작하십시오.
/REMOTE	모든 원격 드라이브의 검사를 시작하십시오.
/SHARED	공유 폴더 검사를 시작하십시오.
/MEMORY	모든 메모리 프로세스의 검사를 시작하십시오.
/STARTUP	시작 개체 검사를 시작하십시오.
/DRIVE=<drive>	지정된 드라이브의 모든 부팅 섹터와 파일의 검사를 시작하십시오.
/FOLDER=<full path to the folder to be scanned>	지정된 폴더의 검사를 시작하십시오. 폴더 라벨 템플릿은 파라미터값으로 사용할 수 없습니다.
/FILE=<full path to the file including its name>	지정된 파일의 검사를 시작하십시오. 파일 이름을 포함하여 파일의 전체 경로를 지정해야 합니다.
/CURE=<yes|no>	검사 모드를 정의하십시오. 다음과 같은 값을 사용할 수 있습니다. • yes: 검사하고 치료합니다. 파리미터를 설정하지 않으면 설정에서 구성한 모드를 적용합니다. • no: 탐지 모드로 검사합니다. 파리미터를 설정하지 않으면 설정에서 구성한 모드를 적용합니다.
/TRACE=<important|normal|detailed>	Portable Auditor 작업의 추적을 활성화합니다. • important은 추적 파일이 모든 오류, 경고 및 추가 정보에 관한 메시지를 저장한다는 뜻입니다. • normal은 추적 파일이 모든 오류 및 경고에 관한 메시지와 Portable Auditor의 정상 작동에 관한 정보를 기록한다는 뜻입니다. • detailed은 Portable Auditor 작업에 관한 모든 정보가 추적 파일에 저장된다는 뜻입니다(기본값).
/DUMP	덤프 기록을 활성화하십시오.

`/REPORT=<full|critical|short>`	검사 완료 후 Kavscan\Report\report.txt에 생성되는 리포트 유형을 정의하십시오. 다음과 같은 값을 사용할 수 있습니다. • `full`: 모든 이벤트 유형이 포함된 전체 검사 리포트 • `critical`: 심각 이벤트만 포함하는 검사 리포트 • `short`: 일반 통계만 포함하고 이벤트는 포함하지 않는 검사 리포트입니다. 기본적으로는 `short` 유형이 적용됩니다.
`/SETTINGS=<full path to the file containing custom settings>`	파일 이름을 포함하는 전체 경로에 있는 파일의 사용자 지정 설정을 적용하십시오. 값을 지정하지 않으면 Portable Auditor가 원래 설정을 적용합니다. 이러한 설정은 Kavscan\settings.dat에 있습니다.

`KAVSCAN SCAN` 명령의 반환 코드:

- `0` – 명령이 성공적으로 실행되었습니다.
- `1`는 일반적인 오류가 발생했음을 의미합니다.

보안 이동식 드라이브에서 Portable Auditor 결과 내보내기

휴대용 감사기가 보안 이동식 드라이브에 기록된 경우 kavscan\Results 폴더에 표시되는 휴대용 감사기 결과는 드라이브의 숨겨진 파티션에 기록됩니다. 따라서 휴대용 감사기에서 생성된 결과를 직접 보거나 복사하거나 다른 매체로 전송할 수 없습니다.

보안 이동식 드라이브에서 휴대용 감사기 결과를 내보내려면 다음과 같이 하십시오.

1. 휴대용 감사기 결과를 내보낼 장치에 보안 이동식 드라이브를 연결하십시오.

   Kaspersky Industrial CyberSecurity for Nodes는 타사 프로세스가 보안 이동식 드라이브에 접근하는 것을 차단합니다. 휴대용 감사기 결과를 내보내려면 Kaspersky Industrial CyberSecurity for Nodes가 설치되지 않은 장치를 사용하거나 차단을 비활성화하십시오.

2. 장치에 대한 로컬 관리자 권한으로 명령줄 해석기를 시작하십시오.

3. `cd /d` 명령을 사용하여(예: `cd /d "E:\kavscan"`, 여기서 `E`는 이동식 드라이브의 문자) kavscan.exe 파일이 포함된 폴더로 변경합니다.

4. 다음 명령을 실행합니다:

   ```
   KAVSCAN EXPORT /FOLDER=<full path to folder> [/CLEAN]
   ```

   위치:

   `/FOLDER=<full path to folder>`는 휴대용 감사기 결과를 복사할 폴더의 전체 경로를 지정합니다. 이는 장치의 폴더, 장치에 연결된 이동식 드라이브, 네트워크 공유 폴더일 수 있습니다.

   `/CLEAN`은 휴대용 감사기 결과를 보안 이동식 드라이브에서 삭제해야 함을 나타냅니다. 애플리케이션이 내보내기 폴더에 접근할 수 없거나 파일이 해당 폴더로 복사되지 않은 경우 휴대용 감사기 결과를 삭제하지 않습니다.

5. 메시지가 표시되면 휴대용 감사기를 만들기 전에 설정한 관리자 PIN을 입력하십시오.

kavscan\Results에 표시된 휴대용 감사기 결과가 지정된 경로의 폴더에 복사되고 폴더 구조가 저장됩니다. `/CLEAN` 매개 변수를 추가하면 휴대용 감사기 결과가 삭제됩니다.

Portable Auditor 데이터베이스를 업데이트하려면:

1. 장치에 대한 로컬 관리자 권한으로 명령줄 해석기를 시작하십시오.
2. `cd /d` 명령을 사용하여(예: `cd /d "E:\kavscan"`, 여기서 `E`는 이동식 드라이브의 문자) kavscan.exe 파일이 포함된 폴더로 변경합니다.
3. Portable Auditor가 포함된 이동식 드라이브를 데이터베이스 업데이트 폴더가 있는 장치에 연결합니다.
4. 다음 명령을 실행합니다:

   ```
   KAVSCAN UPDATE /SOURCE=<폴더의 전체 경로>
   ```

   여기서 `<full path to folder>`은 배포 지점의 저장소 또는 다운로드한 애플리케이션 데이터베이스가 있는 로컬 폴더입니다.

   Portable Auditor는 Bases 폴더에 있는 애플리케이션 데이터베이스를 업데이트한 후 데이터베이스 무결성 검사를 실행합니다. 이 검사 결과는 명령줄 인터페이스에 메시지로 표시됩니다.

보안 이동식 드라이브 접근 차단

Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션이 설치된 장치에 연결된 보안 이동식 드라이브에 대한 접근을 차단할 수 있습니다. 차단을 사용하면 장치 사용자는 Portable Auditor를 생성하고 장치에서 *애플리케이션 데이터베이스 보안 복사* 및 *애플리케이션 데이터베이스의 안전한 업데이트*, 작업만 실행할 수 있습니다. 운영 체제의 표준 수단을 통한 보호된 이동식 드라이브 접근은 차단됩니다.

명령줄에서 보호된 이동식 드라이브에 대한 접근 차단을 구성할 수 있습니다.

명령줄에서 Kaspersky Industrial CyberSecurity for Nodes 관리

명령줄에서 Kaspersky Industrial CyberSecurity for Nodes를 관리하고 운영할 수 있습니다.

명령줄에서 Kaspersky Industrial CyberSecurity for Nodes를 관리하려면:

1. 장치에서 로컬 관리자 권한으로 명령줄 해석기(cmd.exe 등)를 실행합니다.
2. cd 명령으로 kavshell.exe 파일이 있는 폴더로 갑니다.

   예

   ```
   cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0
   ```

   애플리케이션 설치 단계에서 %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.
3. 다음 템플릿을 사용하여 명령을 실행합니다.

   ```
   KAVSHELL <command> [options]
   ```

   `KAVSHELL HELP` 명령을 실행하여 애플리케이션을 관리하기 위한 명령 목록을 볼 수 있습니다. 특정 명령의 구문을 읽으려면 `KAVSHELL HELP <command>`을 입력합니다.

결과적으로 Kaspersky Industrial CyberSecurity for Nodes는 지정된 작업을 수행합니다.

APPCONTROL. 애플리케이션 실행 제어 규칙 가져오기

`KAVSHELL APPCONTROL` 명령을 사용하면 XML 파일에서 애플리케이션 실행 제어 구성 요소의 규칙을 가져오고 구성 요소의 규칙 목록에서 모든 규칙을 제거할 수 있습니다. 규칙이 포함된 XML 파일을 생성하려면 로컬 또는 그룹 *애플리케이션 실행 제어를 위한 규칙 생성기* 작업을 사용할 수 있습니다.

명령 구문

```
KAVSHELL APPCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/APPEND | /REPLACE | /MERGE | /CLEAR`	필수 인수입니다. 지정한 XML 파일에서 애플리케이션 실행 제어 규칙 가져오기: • `/APPEND`: 파일의 모든 규칙을 구성 요소의 규칙 목록에 추가합니다. 규칙이 목록에 이미 있으면 중복해서 추가됩니다. • `/REPLACE`: 구성 요소의 기존 규칙 목록 전체를 파일의 규칙으로 대체합니다. • `/MERGE`: 파일의 규칙을 기존 규칙 목록과 병합합니다. 규칙이 목록에 이미 있으면 중복해서 추가되지 않습니다. 애플리케이션 실행 제어 구성 요소의 모든 규칙을 제거하려면 `/CLEAR`를 사용합니다.
`<path to XML file>`	`/APPEND`, `/REPLACE` 및 `/MERGE`가 전달된 경우 필수입니다. 규칙이 포함된 XML 파일의 전체 경로.

파라미터	설명
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL APPCONTROL /APPEND c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

APPCONTROL /CONFIG. 애플리케이션 실행 제어 구성 요소 구성

`KAVSHELL APPCONTROL /CONFIG` 명령을 사용하여 애플리케이션 실행 제어 구성 요소의 설정을 관리할 수 있습니다.

명령 구문

```
KAVSHELLKAVSHELL APPCONTROL /CONFIG [/MODE:<applyrules|statistics>] [/DLL:<no|yes>] [/SAVETOFILE:<path to XML file>] [/SDC] [/CLEARSDC] /PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/MODE: <applyrules|statistics>`	선택 인수입니다. 애플리케이션 실행 제어 구성 요소 운영 모드: • `applyrules`: Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 규칙을 사용하여 애플리케이션 실행을 제어합니다. • `statistics` (기본값): Kaspersky Industrial CyberSecurity for Nodes는 모든 애플리케이션의 실행을 허용합니다. 이 모드에서 애플리케이션은 모든 애플리케이션 실행, 실행된 애플리케이션에 적용되는 규칙 및 구성 요소가 `applyrules` 모드에서 실행 중이었다면 수행되었을 작업에 대한 정보만 기록합니다.
`/DLL:<no|yes>`	선택 인수입니다. DDL 로드 모니터링: • no (기본값): Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 규칙을 사용하여 DLL 모듈의 로드를 제어하지 않습니다. DLL 모듈 로드가 허용됩니다. • `yes`: 이 기능을 활성화하면 Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 실행 제어 규칙을 사용하여 DLL 모듈의 로드를 허용하거나 거부합니다.
`/SAVETOFILE:<path to XML file>`	선택 인수입니다. 애플리케이션 실행 제어 규칙 목록을 지정된 XML 파일에 저장합니다.
`/SDC`	선택 인수입니다. 애플리케이션 배포 캐시를 `/SAVETOFILE` 옵션으로 지정된 XML 구성 파일로 내보냅니다.
`/CLEARSDC`	선택 인수입니다. 소프트웨어 배포 캐시를 삭제합니다.
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.

/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no> /savetofile:c:\appcontrol\config.xml /PWD:p@ssw0rd
```

APPCONTROL /GENERATE. 애플리케이션 실행 제어를 위한 규칙 생성기

KAVSHELL APPCONTROL /GENERATE 명령을 사용하여 *애플리케이션 실행 제어를 위한 규칙 생성기* 작업을 관리할 수 있습니다.

명령 구문

```
KAVSHELL APPCONTROL /GENERATE <path to folder> | /SOURCE:<path to file with folders list> [/MASKS:<edms>]
[/RUNAPP] [/RULES:<ch|cp|h>] [/STRONG] [/USER:<user or group of users>] [/EXPORT:<path to XML file>] [/IMPORT:
<a|r|m>] [/PREFIX:<prefix for rules names>] [/UNIQUE] [/ADDPATH] /PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
<path to folder>	/SOURCE를 전달하지 않은 경우 필수입니다. 실행 파일, MSI 패키지 및 스크립트가 있는 폴더의 경로. 지정된 유형이며 지정된 폴더에 있는 파일이 실행될 경우 작업은 허용 규칙을 생성합니다.
/SOURCE:<path to file with folders list>	<path to folder>를 전달하지 않은 경우 필수입니다. 허용 규칙을 자동으로 생성할 실행 파일이 있는 폴더 목록이 포함된 TXT 파일의 경로.
/MASKS:<edms>	선택 인수입니다. 허용 규칙을 자동으로 생성할 실행 파일의 확장자. 작업 범위에 다음 확장자의 파일을 포함할 수 있습니다. • e: EXE 파일 • d: DLL 파일 • m: MSI 파일 • s: 스크립트
/RUNAPP	선택 인수입니다. 실행 중인 애플리케이션을 기반으로 허용 규칙을 생성합니다.
/RULES:<ch|cp|h>	선택 인수입니다. 애플리케이션 실행 제어 허용 규칙을 생성할 때 작업이 적용할 기준: • ch: 디지털 인증서를 사용합니다. 인증서가 없으면 SHA256 해시를 사용합니다. • cp: 디지털 인증서를 사용합니다. 인증서가 없으면 실행 파일의 경로를 사용합니다. • h: SHA256 해시를 사용합니다.
/STRONG	선택 인수입니다. 애플리케이션 실행 제어 허용 규칙을 트리거하는 기준으로 파일 디지털 인증서의 주체 및 지문 사용. /RULES:<ch|cp> 파라미터와 함께 사용됩니다.
/USER:<user or group of users>	선택 인수입니다. 규칙을 적용할 사용자 또는 사용자 그룹의 이름.
/EXPORT:<path to XML file>	선택 인수입니다. 지정한 규칙을 저장할 XML 파일의 경로와 이름.

`/IMPORT:<a|r|m>`	선택 인수입니다. 생성된 규칙을 애플리케이션 실행 제어 규칙 목록으로 가져오기: • `a`: 파일의 모든 규칙을 구성 요소의 규칙 목록에 추가합니다. 규칙이 목록에 이미 있으면 중복해서 추가됩니다. • `r`: 구성 요소의 기존 규칙 목록 전체를 파일의 규칙으로 대체합니다. • `m`: 파일의 규칙을 기존 규칙 목록과 병합합니다. 규칙이 목록에 이미 있으면 중복해서 추가되지 않습니다.
`/PREFIX:<prefix for rules names>`	애플리케이션 실행 제어 허용 규칙 이름의 접두사 지정.
`/UNIQUE`	애플리케이션 실행 제어 허용 규칙 생성의 기반이 된 보호 대상 장치에 대한 정보를 규칙에 추가.
`/ADDPATH`	해시를 기반으로 생성된 규칙에 실행 파일의 경로를 추가합니다.
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml /PWD:p@ssw0rd
```

CONFIG. AM-PPL 기술 지원

`KAVSHELL CONFIG` 명령을 사용하면 AM-PPL 기술을 사용하여 애플리케이션 프로세스 보호를 관리할 수 있습니다.

명령이 올바르게 작동하려면 자기 보호 메커니즘을 비활성화해야 합니다.

명령 구문

```
KAVSHELL CONFIG /PPL:<ON|OFF> /PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/PPL:<ON|OFF>`	필수 인수입니다. AM-PPL 기술 지원 활성화 또는 비활성화: • `ON` – AM-PPL 기술 지원을 활성화합니다. • `OFF` – AM-PPL 기술 지원을 비활성화합니다.
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.

`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL CONFIG /PPL:ON
KAVSHELL CONFIG /PPL:OFF
```

CREATEPORTABLE. Portable Auditor 생성

`KAVSHELL CREATEPORTABLE` 명령을 사용하면 이동식 드라이브에 Portable Auditor를 생성할 수 있습니다.

명령 구문

```
KAVSHELL CREATEPORTABLE /DRIVE=<name of the removable drive or serial number of the Rutoken removable drive>
/LICENSE=<path to the license key file> [/TOKENPIN=<password> [/NEWTOKENPIN=<password>]] [/VERIFY] [/AV <settings
of the scan for viruses and other threatening programs>] [/TRAFFIC=<duration in seconds>] [/OVAL <settings of the
security audit task>]
```

명령 옵션

파라미터	설명
`/DRIVE=<name of the removable drive or serial number of the Rutoken removable drive>`	필수 인수입니다. Portable Auditor를 생성할 이동식 드라이브를 선택할 수 있습니다. Portable Auditor를 Rutoken 이동식 드라이브에 쓰려면 Rutoken 드라이브의 10자리 일련 번호를 입력해야 합니다. 현재 장치에 연결된 Rutoken 드라이브의 일련 번호는 `KAVSHELL TOKEN /ENUMERATE` 명령을 실행하여 확인할 수 있습니다.
`/LICENSE=<path to the license key file>`	필수 인수입니다. Portable Auditor를 생성하는 데 필요한 키 파일의 경로를 지정합니다.
`/TOKENPIN=<password>`	Rutoken 이동식 드라이브를 사용하는 경우 필수 인수입니다. Rutoken 드라이브에 접근하기 위한 관리자 암호를 설정합니다.
`/NEWTOKENPIN=<password>`	선택 인수입니다. Rutoken 드라이브에 접근하기 위한 새 관리자 암호를 설정합니다.
`/VERIFY`	선택 인수입니다. Portable Auditor를 이동식 드라이브에 쓴 후 확인합니다.
`/AV <settings of the scan for viruses and other threatening programs>`	선택 인수입니다. `/av`, `/oval` 또는 `/traffic` 인수 중 하나 이상을 지정해야 합니다. 바이러스 및 기타 위협적 프로그램을 검사합니다.
`/TRAFFIC=<duration in seconds>`	선택 인수입니다. 지정된 시간 동안 검사 중인 장치의 인바운드 및 아웃바운드 트래픽을 기록합니다. 1부터 1800까지의 값을 사용할 수 있습니다. 30초로 기본 설정되어 있습니다.
`/OVAL <settings of the security audit task>`	선택 인수입니다. 보안 감사 작업을 활성화합니다.
바이러스 및 기타 위협적 프로그램 검사 설정	
`<list of files>`	파일, 폴더, 네트워크 경로 또는 사전 정의된 검사 범위를 공백으로 구분한 목록입니다.

`/L=<path to file with a list of scan scopes>`	검사 범위 목록이 있는 파일 경로입니다. 파일을 직접 생성하고 TXT 형식으로 저장해야 합니다. 파일은 BOM 없이 UTF-8 인코딩으로 저장해야 합니다.
`/MEMORY`	모든 메모리 프로세스의 검사를 시작하십시오. 이 검사 범위는 기본적으로 활성화되어 있습니다.
`/SHARED`	공유 폴더 검사를 시작하십시오.
`/STARTUP`	시작 개체 검사를 시작하십시오. 이 검사 범위는 기본적으로 활성화되어 있습니다.
`/REMDRIVES`	모든 이동식 드라이브의 검사를 시작하십시오.
`/NETDRIVES`	네트워크 드라이브 검사
`/FIXDRIVES`	모든 로컬 하드 드라이브의 검사를 시작하십시오. 이 검사 범위는 기본적으로 활성화되어 있습니다.
`/MYCOMP`	전체 컴퓨터 검사를 시작하십시오.
`/F<A|C|E>`	검사 범위에 포함해야 하는 개체: • `/FA`: 모든 개체를 검사합니다. 애플리케이션은 예외 없이 모든 파일(모든 형식 및 확장자)을 검사합니다. • `/FC`: 형식에 따라 개체를 검사합니다. 애플리케이션은 감염 가능한 개체의 형식 목록에 포함된 형식의 개체만 검사합니다. • `/FE`: 확장자에 따라 개체를 검사합니다. 애플리케이션이 감염될 수 있는 개체의 확장자 목록에 포함된 확장자를 가진 개체만 검사합니다.
`/AI=<action>`	탐지된 감염 개체에 적용할 처리입니다. 가능한 값: • `DISINFDEL` – **치료 - 불가능한 경우 삭제** • `REPORT`(기본 값) – **알림**
`/E=ABMSPO`	지정한 개체 유형을 제외합니다. 가능한 값: • `A`: ZIP, CAB, RAR, ARJ 압축 파일 및 기타 압축 파일 형식. • `B`: Microsoft Outlook 및 Microsoft Outlook Express 메일 데이터베이스 파일. • `M`: Microsoft Outlook 및 Microsoft Outlook Express 메시지와 같은 메일 형식의 파일. • `S`: 자동 압축 해제 압축 파일. • `P`: UPX 또는 ASPack과 같은 이진 코드 압축 프로그램으로 압축된 실행 파일. • `O`: 파일에 삽입된 개체(예: Microsoft Word 매크로 또는 이메일 메시지 첨부 파일). 여러 파라미터 값을 지정할 수 있습니다.
`/EM=<file mask>`	파일 마스크와 일치하는 파일은 검사 범위에서 제외됩니다. 예: • `*.exe` 마스크는 exe 확장자를 가진 파일의 모든 경로를 포함합니다. • `example*` 마스크는 EXAMPLE 이름을 가진 파일에 대한 모든 경로를 포함합니다.
`/ET=<scan duration in seconds>`	지정된 시간 제한(초)보다 검사하는 데 오래 걸리는 파일은 검사 범위에서 제외됩니다. 60초로 기본 설정되어 있습니다.
`/ES=<size in megabytes>`	지정된 크기 제한(MB)보다 큰 파일은 검사 범위에서 제외됩니다. 기본값은 100MB입니다.
`/NOICHECKER`	iChecker를 비활성화합니다. 이 옵션은 기본적으로 활성화되어 있습니다.
`/EXCLUDE=<list of exlusions>`	검사 작업 범위에서 제외할 파일, 폴더 또는 네트워크 경로의 목록입니다. 공백으로 구분된 여러 값을 지정할 수 있습니다.
`/W=<file path>`	검사 로그 파일의 경로 및 이름입니다.
보안 감사 작업 설정	
`/SOURCE=<kl|kl-compl|file>`	보안 감사에 필요한 규칙의 소스를 결정합니다. 가능한 파라미터 값: • `kl`(기본적으로 활성화되어 있음) – 배포 패키지에 포함된 Kaspersky ICS CERT 취약점 데이터베이스입니다. • `kl-compl`(기본적으로 활성화되어 있음) – 배포 패키지에 포함된 운영 체제용 보안 구성 및 표준 준수입니다. • `file` – 파일의 사용자 지정 규칙 데이터베이스입니다.

`/PATH=<full path to ZIP archive with security audit rules>`	이 파라미터는 **사용자 지정 규칙 데이터베이스** 경로에 대한 규칙이 있는 파일의 경로를 전달합니다(`/SOURCE=file`. 지정된 ZIP 압축 파일 내의 규칙에 따라 보안 감사 작업을 시작하십시오. ZIP 압축 파일에는 OVAL 언어 규칙이 있는 XML 파일이 포함되어야 합니다. 이름을 포함하여 ZIP 파일의 전체 경로를 제공해야 합니다. OVAL 규칙은 BOM 없이 UTF-8 인코딩으로 저장해야 합니다.
`/MODE=<all|exclude|include>`	이 파라미터는 취약점 검사 모드를 정의합니다. 가능한 파라미터 값: • `all` – 경로에 나열된 모든 취약점을 검사합니다. • `exclude` – `/DEFINITIONS` 파라미터에 의해 지정된 취약점을 제외하고 경로에 나열된 취약점을 검사합니다. • `include` – `/DEFINITIONS` 파라미터에 의해 지정된 취약점 `/SOURCE=kl` 파라미터와 함께 사용됩니다.
`/DEFINITIONS=<vuln_type_01;...;vuln_type_N>`	검사해야 하거나 검사에서 제외해야 하는 취약점 유형을 세미콜론으로 구분한 목록입니다. 예: `oval:org.mitre.oval.test:def:998;oval:org.mitre.oval.test:def:999`. `/MODE=include` 또는 `/MODE=exclude` 파라미터와 함께 사용됩니다.

예:

```
KAVSHELL CREATEPORTABLE /DRIVE=E: /LICENSE=C:\0000000A.key /VERIFY /AV /l="C:\Documents and Settings\file.txt"
/ai=DISINFDEL
```

DEVCONTROL. 장치 제어 규칙 가져오기

`KAVSHELL DEVCONTROL` 명령을 사용하면 *장치 제어를 위한 규칙 생성기* 명령으로 생성된 XML 파일에서 장치 제어 구성 요소의 규칙을 가져오거나 구성 요소의 규칙 목록에서 모든 규칙을 제거할 수 있습니다.

명령 구문

```
KAVSHELL DEVCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/APPEND | /REPLACE | /MERGE | /CLEAR`	필수 인수입니다. 지정한 XML 파일에서 장치 제어 규칙 가져오기: • `/APPEND`: 파일의 모든 규칙을 구성 요소의 규칙 목록에 추가합니다. 규칙이 목록에 이미 있으면 중복해서 추가됩니다. • `/REPLACE`: 구성 요소의 기존 규칙 목록 전체를 파일의 규칙으로 대체합니다. • `/MERGE`: 파일의 규칙을 기존 규칙 목록과 병합합니다. 규칙이 목록에 이미 있으면 중복해서 추가되지 않습니다. 장치 제어 구성 요소의 모든 규칙을 제거하려면 `/CLEAR`를 사용합니다.
`<path to XML file>`	`/APPEND`, `/REPLACE` 및 `/MERGE`가 전달된 경우 필수입니다. 규칙이 포함된 XML 파일의 전체 경로.
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.

파라미터	설명
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL DEVCONTROL /MERGE c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

DUMP. 메모리 덤프 기록

`KAVSHELL DUMP` 명령을 사용하면 메모리 덤프를 활성화하거나 비활성화할 수 있습니다.

명령 구문

```
KAVSHELL DUMP </ON /F:<dump_file_folder> | /SNAPSHOT /F:<dump_file_folder> /P:<process_ID> | /OFF > [/PWD:
<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
/ON	덤프 파일 생성을 활성화합니다.
/F:<dump_file_folder>	필수 인수입니다. 덤프 파일이 저장되는 폴더를 설정합니다.
/SNAPSHOT	지정된 ID로 실행 중인 프로세스의 메모리 덤프를 생성합니다. 덤프 파일은 `/F` 옵션으로 지정한 폴더에 저장됩니다.
/P:<process_ID>	`/SNAPSHOT`가 통과되면 필요합니다. 프로세스 ID를 설정합니다. `tasklist` 명령을 사용하여 프로세스 ID를 확인할 수 있습니다.
/OFF	덤프 파일 생성을 비활성화합니다.
/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL DUMP /ON /F:"C:\Dumps and others"
KAVSHELL DUMP /SNAPSHOT /F:"C:\Dumps and others" /P:1234 /PWD:p@ssw0rd
KAVSHELL DUMP /OFF
```

EDR_EXPERT_ON_PREM. EDR Expert(on-premises) 통합

`KAVSHELL EDR_EXPERT_ON_PREM` 명령을 사용하여 Kaspersky Endpoint Detection and Response Expert(on-premises) 통합을 구성할 수 있습니다.

명령 구문

```
KAVSHELL EDR_EXPERT_ON_PREM /ENABLE /MODE:<EDRKATA|ERDExpertOnPrem> /SERVERS:<address>:<port> [/PINNED-
CERTIFICATE:<full path to the TLS certificate file>] [/CLIENT-CERTIFICATE:<full path to the certificate file>]
[/CLIENT-PASSWORD:<password for the client certificate>] [/TIMEOUT:<server connection timeout, in seconds>]
[/SYNC-PERIOD":<synchronization period with the server, in minutes> [/EVENTS-SEND-PERIOD:<period of send events to
server, in seconds>] [/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or
0>] [/EVENTS-PER-HOUR:<events count limit: max events per hour>] [/MAX-PACKET-LENGTH:<Maximum number of event
packets transmitted within a transaction>] [/TELEMETRY-SERVERS:<address>:<port>] [/TELEMETRY-PINNED-CERTIFICATE:
<full path to the telemetry server TLS certificate file>] [/TELEMETRY-CLIENT-CERTIFICATE:<full path to the
telemetry certificate file>] [/TELEMETRY-CLIENT-PASSWORD:<password for the client certificate>] [/TELEMETRY-
TIMEOUT:<Telemetry server connection timeout, in seconds>] [/TELEMETRY-ONLY-TAGGED-EVENTS:<0|1>] [/PWD:<password>]
[/LOGIN:<user name>]
| /DISABLE [/PWD:<password>] [/LOGIN:<user name>]
| /SHOW
```

명령 옵션

파라미터	설명
`/<ENABLE|DISABLE|SHOW>`	필수 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 Endpoint Detection and Response Expert(on-premises) 솔루션의 통합 활성화, 비활성화 또는 상태 조회.
`/MODE:<EDRKATA|ERDExpertOnPrem>`	필수 인수입니다. 통합할 솔루션 선택: • `EDRKATA`: Kaspersky Anti Targeted Attack Platform. • `ERDExpertOnPrem`: Kaspersky Endpoint Detection and Response Expert(on-premises)
`/SERVERS:<address>:<port>`	필수 인수입니다. 응답 서버 주소 및 서버 연결에 사용할 포트. `;`로 구분된 여러 값을 지정할 수 있습니다.
`/PINNED-CERTIFICATE:<full path to the TLS certificate file>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 응답 서버 간에 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서.
`/CLIENT-CERTIFICATE:<full path to the certificate file>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 SIEM 서버 간의 연결을 보호하기 위한 암호화된 클라이언트 인증서를 저장하는 PFX 파일인 *암호화 컨테이너*를 추가할 수 있습니다.
`/CLIENT-PASSWORD:<password for the client certificate>`	`/CLIENT-CERTIFICATE`가 통과되면 필요합니다. 암호화 컨테이너의 암호를 지정할 수 있습니다.
`/TIMEOUT:<server connection timeout, in seconds>`	선택 인수입니다. 응답 서버의 최대 응답 대기 시간(초). 사용 가능한 값 범위: 1~3600초. 기본값은 10초입니다.
`/SYNC-PERIOD:<synchronization period with the server, in minutes>`	선택 인수입니다. 응답 서버에 요청을 보내는 간격(분). 사용 가능한 값 범위는 1–60분입니다. 기본값은 5분입니다.
`/EVENTS-SEND-PERIOD:<period of send events to server, in seconds>`	선택 인수입니다. 응답 서버로 이벤트를 전송할 때의 최대 지연 시간. 지정된 시간이 만료되면 애플리케이션이 같은 서버에 다시 연결을 시도하거나, 서버가 여러 개일 경우 목록에 있는 다음 서버에 연결합니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.

`/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or 0>`	선택 인수입니다. 전송되는 이벤트 수 제한: • `1`: 활성화됨. • `0`: 비활성화됨(기본값). 이벤트 수가 구성된 제한을 초과하면 애플리케이션이 이벤트 전송을 중지합니다.
`/EVENTS-PER-HOUR:<events count limit: max events per hour>`	선택 인수입니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.
`/TELEMETRY-SERVERS:<address>:<port>`	필수 인수입니다. 원격 측정 서버의 주소 및 포트. `;`로 구분된 여러 값을 지정할 수 있습니다.
`/TELEMETRY-PINNED-CERTIFICATE:<full path to the telemetry server TLS certificate file>`	선택 인수입니다. 원격 측정 수집 서버와 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서.
`/TELEMETRY-CLIENT-CERTIFICATE:<full path to the telemetry certificate file>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 원격 측정 수집 서버 간의 연결을 보호하기 위한 암호화된 클라이언트 인증서를 저장하는 *암호화 컨테이너*를 추가할 수 있습니다.
`/TELEMETRY-CLIENT-PASSWORD:<password for the client certificate>`	`/CLIENT-CERTIFICATE`가 통과되면 필요합니다. 암호화 컨테이너의 암호를 지정할 수 있습니다.
`/TELEMETRY-TIMEOUT:<Telemetry server connection timeout, in seconds>`	선택 인수입니다. 원격 측정 수집 서버의 최대 응답 대기 시간(초). 사용 가능한 값 범위: 1~3600초. 기본값은 10초입니다.
`/TELEMETRY-ONLY-TAGGED-EVENTS:<0|1>`	선택 인수입니다. IOA만 포함한 원격 측정 전송: • `1`: 활성화됨. • `0`: 비활성화됨(기본값).
`/PWD:<password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL EDR_EXPERT_ON_PREM /MODE=EDRKATA /ENABLE /SERVERS:123.4.5.6:8080 /EVENTS-LIMIT=1 /EVENTS-PER-HOUR=3000
/PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /ENABLE /SERVERS:123.4.5.6:8080 /PINNED-CERTIFICATE:c:\user\certs\cetr.pfx
/PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /MODE=EDRExpertOnPrem /ENABLE /SERVERS:123.4.5.6:8080 /EVENTS-LIMIT=1 /EVENTS-PER-
HOUR=3000 /telemetry-SERVERS:127.0.0.1:8080;telemetry.server.ru:8080 /telemetry-TIMEOUT=30 /PINNED-
CERTIFICATE:c:\user\certs\telemetry_cert.pfx /PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /DISABLE /PWD:p@ssw0rd
KAVSHELL EDR_EXPERT_ON_PREM /SHOW
```

EDRKATA. KATA 통합

`KAVSHELL EDRKATA` 명령을 사용하여 Kaspersky Anti Targeted Attack Platform 솔루션과의 통합을 구성할 수 있습니다.

명령 구문

```
KAVSHELL EDRKATA /ENABLE /SERVERS:<address>:<port> [/PINNED-CERTIFICATE:<full path to the TLS certificate file>] [/CLIENT-CERTIFICATE:<full path to the certificate file>] [/CLIENT-PASSWORD:<password for the client certificate>] [/TIMEOUT:<server connection timeout, in seconds>] [/SYNC-PERIOD:<synchronization period with the server, in minutes> [/EVENTS-SEND-PERIOD:<period of send events to server, in seconds>] [/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or 0>] [/EVENTS-PER-HOUR:<events count limit: max events per hour>] [/PWD:<password>] [/LOGIN:<user name>] | /DISABLE [/PWD:<current password>] [/LOGIN:<user name>] | /SHOW
```

명령 옵션

파라미터	설명
`/<ENABLE|DISABLE|SHOW>`	필수 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Anti Targeted Attack Platform 솔루션 간 통합을 활성화 또는 비활성화하거나 통합 상태를 확인합니다.
`/SERVERS:<address>:<port>`	필수 인수입니다. KATA Central Node 서버 주소(IPv4, IPv6) 및 포트. `;`로 구분된 여러 값을 지정할 수 있습니다.
`/PINNED-CERTIFICATE:<full path to the TLS certificate file>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 Central Node 서버 간에 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서.
`/CLIENT-CERTIFICATE:<full path to the certificate file>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 Central Node 서버 간의 연결을 보호하기 위한 암호화된 클라이언트 인증서를 저장하는 PFX 파일인 *암호화 컨테이너*를 추가할 수 있습니다.
`/CLIENT-PASSWORD:<password for the client certificate>`	`/CLIENT-CERTIFICATE`가 통과되면 필요합니다. 암호화 컨테이너의 암호를 지정할 수 있습니다.
`/TIMEOUT:<server connection timeout, in seconds>`	선택 인수입니다. 원격 측정 수집 서버의 최대 응답 대기 시간(초). 사용 가능한 값 범위: 1~3600초. 기본값은 10초입니다.
`/SYNC-PERIOD:<synchronization period with the server, in minutes>`	선택 인수입니다. Central Node 서버에 요청을 보내는 간격(분). 사용 가능한 값 범위는 1–60분입니다. 기본값은 5분입니다.
`/EVENTS-SEND-PERIOD:<period of send events to server, in seconds>`	선택 인수입니다. Central Node 서버로 이벤트를 전송할 때의 최대 지연 시간. 지정된 시간이 만료되면 애플리케이션이 같은 서버에 다시 연결을 시도하거나, 서버가 여러 개일 경우 목록에 있는 다음 서버에 연결합니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.
`/EVENTS-LIMIT:<events count limit: enable (1) or disable (0) events count limit, value 1 or 0>`	선택 인수입니다. 전송되는 이벤트 수 제한: • `1`: 활성화됨. • `0`: 비활성화됨(기본값). 이벤트 수가 구성된 제한을 초과하면 애플리케이션이 이벤트 전송을 중지합니다.
`/EVENTS-PER-HOUR:<events count limit: max events per hour>`	선택 인수입니다. 기본 설정은 시간당 이벤트 3000개입니다. 애플리케이션이 서버에 설치된 경우 원격 측정 데이터 스트림은 더 높습니다. 서버의 경우 이 값을 시간당 60,000개 이벤트로 늘리는 것이 좋습니다.

/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL EDRKATA /ENABLE /SERVERS:123.4.5.6:8080 /EVENTS-LIMIT=1 /EVENTS-PER-HOUR=3000 /PWD:p@ssw0rd
KAVSHELL EDRKATA /ENABLE /SERVERS:123.4.5.6:8080 /PINNED-CERTIFICATE:c:\user\certs\cetr.pfx /PWD:p@ssw0rd
KAVSHELL EDRKATA /DISABLE /PWD:p@ssw0rd
KAVSHELL EDRKATA /SHOW
```

EXITPOLICY. 장치에서 정책 비활성화

KAVSHELL EXITPOLICY 명령은 장치에서 Kaspersky Security Center 정책을 비활성화합니다. 정책을 비활성화하면 정책에서 닫힌 자물쇠(🔒)로 표시된 설정을 포함하여 모든 Kaspersky Industrial CyberSecurity for Nodes 설정을 구성할 수 있습니다.

명령 구문

```
KAVSHELL EXITPOLICY [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL EXITPOLICY /PWD:p@ssw0rd
```

EXPORT. 애플리케이션 설정 내보내기

KAVSHELL EXPORT 명령을 사용하면 XML 형식의 구성 파일에서 Kaspersky Industrial CyberSecurity for Nodes 설정을 내보낼 수 있습니다. 모든 애플리케이션 설정 또는 개별 구성 요소에 대한 설정만을 구성 파일에 저장할 수 있습니다.

명령 구문

```
KAVSHELL EXPORT <profile> <file name> [/LOGIN:<user name>] [/PWD:<password>]
```

명령 옵션

파라미터	설명
`<profile>`	필수 인수입니다. 내보내기 설정 프로필 이름을 입력합니다. 프로필은 Kaspersky Industrial CyberSecurity for Nodes의 구성 요소, 작업 또는 기능입니다. `KAVSHELL EXPORT /?` 명령을 실행하여 사용 가능한 프로필 목록을 볼 수 있습니다. 모든 애플리케이션 설정을 내보내려면 `product` 프로필을 지정합니다.
`<file name>`	필수 인수입니다. 프로필 설정을 내보낼 XML 형식의 파일 이름을 지정합니다. 파일 경로를 지정할 수도 있습니다. 예: `C:\Test\settings.xml` • 명령에 파일 이름만 지정하면 애플리케이션은 해당 파일을 애플리케이션 설치 폴더에 저장하려고 시도합니다. 애플리케이션의 자체 보호 메커니즘이 활성화되어 있으면 애플리케이션의 자체 보호 기능이 애플리케이션 폴더에 새 파일이 생성되는 것을 차단하므로 내보내기에 실패합니다. 애플리케이션 설정을 내보내려면 파일 경로를 지정합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.
`/PWD: <password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.

예

```
KAVSHELL EXPORT product C:\Test\settings.xml /LOGIN:Admin /PWD:p@ssw0rd
```

FBRESET. iSwift 데이터베이스 지우기

Kaspersky Industrial CyberSecurity for Nodes는 마지막 검사 이후 수정되지 않은 파일을 다시 검사하지 않도록 해주는 iSwift 기술을 사용할 수 있습니다. `KAVSHELL FBRESET` 명령은 검사되었으며 감염되지 않은 파일에 대한 정보를 저장하는 데이터베이스를 지웁니다. 데이터베이스를 지운 후 Kaspersky Industrial CyberSecurity for Nodes는 각 파일에 처음 접근할 때 해당 파일을 검사합니다.

명령 구문

```
KAVSHELL FBRESET
```

FIM /BASELINE. 베이스라인 시스템 무결성 모니터

`KAVSHELL FIM /BASELINE` 명령을 사용하여 *베이스라인 시스템 무결성 모니터* 작업을 관리할 수 있습니다.

```
KAVSHELL FIM /BASELINE [[/CREATE {<monitoring scope>|/L:<path to TXT file containing the list of monitoring areas>}] [/MD5 | /SHA256] [/SF] [/W:<file name>] [/ANSI]] [/SCAN {[/BL:<id baseline>] | [/ALIAS:<existing task id>]} [/W:<file name>] [/ANSI]] [/CLEAR [/BL:<id baseline>] | [/ALIAS:<existing task id>]] [/SHOW [[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/EXPORT:<path to folder>[[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/CREATE`	새 *베이스라인 시스템 무결성 모니터* 작업을 시작하여 시스템 상태의 스냅샷을 생성합니다.

/SCAN	시스템 스냅샷 ID 또는 기존 작업의 대체 이름을 사용하여 *베이스라인 시스템 무결성 모니터* 작업을 실행합니다.
/CLEAR	기준선을 삭제하는 중입니다. 시스템 스냅샷의 ID 또는 스냅샷을 생성한 작업의 대체 이름을 지정합니다. 대체 작업 이름과 스냅샷 ID를 모두 지정하지 않으면 애플리케이션이 모든 스냅샷을 삭제합니다.
/EXPORT	모든 스냅샷 또는 /BL 옵션을 사용하여 지정한 스냅샷의 데이터를 TXT 파일로 지정된 폴더에 내보냅니다.
/SHOW	모든 시스템 상태 스냅샷 또는 /BL 옵션으로 지정한 스냅샷의 데이터를 표시합니다.
<monitoring scope>	/L을 지정하지 않은 경우 필수 인수입니다. 작업의 모니터링 범위를 설정합니다. * 및 ? 문자를 사용하여 경로 마스크를 입력할 수 있습니다.
/L	<monitoring scope>를 지정하지 않았을 때의 필수 인수입니다. 모니터링 범위 목록이 포함된 TXT 파일의 경로를 지정할 수 있습니다.
/MD5	선택 인수입니다. /SHA256 파라미터와 함께 사용할 수 없습니다. 체크섬 계산에 사용할 MD5 알고리즘을 설정합니다. 기본적으로 MD5 알고리즘이 사용됩니다.
/SHA256	선택 인수입니다. /MD5 파라미터와 함께 사용할 수 없습니다. 체크섬 계산에 사용할 SHA256 알고리즘을 설정합니다. 기본적으로 MD5 알고리즘이 사용됩니다.
/SF	선택 인수입니다. 작업의 모니터링 범위에 모든 하위 폴더를 포함합니다. 기본적으로 하위 폴더는 모니터링 범위에 포함되지 않습니다.
/ALIAS:<existing task id>	/BL를 지정하지 않았을 때의 필수 인수입니다. 작업 별칭. KAVSHELL FIM /BASELINE /SHOW 명령을 사용하여 작업 별칭을 확인할 수 있습니다.
/BL:<id baseline>	/ALIAS를 지정하지 않았을 때의 필수 인수입니다. 시스템 스냅샷의 ID를 설정합니다. KAVSHELL FIM /BASELINE /SHOW 명령을 사용하여 기준선 ID를 확인할 수 있습니다.
/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL FIM /BASELINE /CREATE "c:\program files\*" /MD5 /SF
KAVSHELL FIM /BASELINE /CREATE /L:c:\programdata\mytask\list.txt /ALIAS:SystemIntegrityMonitorOnDemandTask$001
/MD5 /SF
KAVSHELL FIM /BASELINE /SCAN /ALIAS:SystemIntegrityMonitorOnDemandTask$001
KAVSHELL FIM /BASELINE /EXPORT:c:\programdata\mytask\baselines\
```

HELP. 명령 도움말 표시

사용 가능한 모든 Kaspersky Industrial CyberSecurity for Nodes 명령 목록을 표시하려면 다음 명령 중 하나를 실행합니다.

```
KAVSHELL
KAVSHELL HELP
```

```
KAVSHELL /?
```

명령 및 해당 구문에 대한 설명을 표시하려면 다음 명령 중 하나를 실행합니다.

```
KAVSHELL HELP <command>
KAVSHELL <command> /?
```

예

```
KAVSHELL HELP SCAN
```

IMPORT. 애플리케이션 설정 가져오기

`KAVSHELL IMPORT` 명령을 사용하면 XML 형식의 구성 파일에서 Kaspersky Industrial CyberSecurity for Nodes 설정을 가져올 수 있습니다. `KAVSHELL EXPORT` 명령을 사용하여 구성 파일을 생성할 수 있습니다.

명령 구문

```
KAVSHELL IMPORT <file_name> /PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`<file name>`	필수 인수입니다. 설정을 가져올 XML 파일의 이름과 확장자를 포함한 전체 경로를 지정합니다.
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL IMPORT C:\Test\settings.xml /PWD:p@ssw0rd
```

명령 반환 값:

- 0: 작업을 완료했습니다.
- -2: 서비스가 실행되고 있지 않습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -4: 개체를 찾을 수 없습니다.
- -9: 관리 대상 장치를 다른 사용자 계정으로 실행하려는 시도가 실패했습니다.
- -99: 알 수 없는 오류.
- -501: 작업은 성공적으로 완료되었지만 실행 중 오류 또는 경고가 발생했습니다(예: 애플리케이션에서 일부 구성 요소의 설정을 가져오지 못함).

- -502: 가져오기 파일이 없거나 인식할 수 없는 형식입니다.
- -503: 설정이 호환되지 않습니다(다른 애플리케이션 또는 호환되지 않는 최신 버전의 Kaspersky Industrial CyberSecurity for Nodes에서 내보낸 구성 파일).

KICS. Kaspersky Industrial CyberSecurity for Networks 통합

`KAVSHELL KICS` 명령을 사용하여 Kaspersky Industrial CyberSecurity for Networks와의 통합을 구성할 수 있습니다.

1. TCP 프로토콜을 통해 Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks의 통합을 구성하려면 다음 명령을 실행합니다.

```
KAVSHELL KICS /ENABLE /SERVERS:<address>:<port> [/PINNED-CERTIFICATE:<full path to the TLS certificate file>]
[/CLIENT-CERTIFICATE:<full path to the crypto-container>] [/CLIENT-PASSWORD:<password for the crypto-
container>] [/TIMEOUT:<maximum server response timeout>] [/SYNC-PERIOD:<synchronization request period>]
[/EVENTS-SENT-PERIOD:<maximum delay when sending events>] [/EVENTS-LIMIT:<1|0>] [/EVENTS-PER-HOUR:<maximum
number of events per hour>] [/VIRTUAL-SPAN-ENABLE] [/VIRTUAL-SPAN-DISABLE] [/VIRTUAL-SPAN-ADD-RULES:<subnet
IDs>] [/VIRTUAL-SPAN-REMOVE-RULES:<subnet IDs>] [/LOGIN:<user name>] [/PWD:<password>]
```

2. MQTT 게시자 모드에서 Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks의 통합을 구성하려면 다음 명령을 실행하십시오.

```
KAVSHELL KICS /ENABLE /KICS-MODE:MQTT-PUBLISHER /MQTT-SERVER:<address>:<port> [/MQTT-USER:<login name for
authorization at the MQTT broker>] [/MQTT-PASSWORD:<password for authorization at the MQTT broker>] [/LOGIN:
<user name>] [/PWD:<password>]
```

3. UDP 프로토콜을 통해 Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks의 통합을 구성하려면 다음 명령을 실행합니다.

```
KAVSHELL KICS /ENABLE /KICS-MODE:UDP-DATA-DIODE /UDP-SERVER:<address>:<port> [/UDP-ENCRYPTION-DISABLE] [/UDP-
ENCRYPTION-ENABLE] [/UDP-ENCRYPTION-KEY:<full path to the encryption key>] [/UDP-ENCRYPTION-PASSWORD:<password
to the encryption key>]
```

4. Kaspersky Industrial CyberSecurity for Nodes 통합을 MQTT 구독자로 구성하려면 다음 명령을 실행합니다.

```
KAVSHELL KICS /ENABLE /KICS-MODE:TELEMETRY /SERVERS:<address>:<port> [/PINNED-CERTIFICATE:<full path to the TLS
certificate file>] [/CLIENT-CERTIFICATE:<full path to the crypto-container>] [/CLIENT-PASSWORD:<password for
the crypto-container>] [/TIMEOUT:<maximum server response timeout>] [/SYNC-PERIOD:<synchronization request
period>] [/EVENTS-SENT-PERIOD:<maximum delay when sending events>] [/EVENTS-LIMIT:<1|0>] [/EVENTS-PER-HOUR:
<maximum number of events per hour>] [/VIRTUAL-SPAN-ENABLE] [/VIRTUAL-SPAN-DISABLE] [/VIRTUAL-SPAN-ADD-RULES:
<subnet IDs>] [/VIRTUAL-SPAN-REMOVE-RULES:<subnet IDs>] /MQTT-SUBSCRIBER-ENABLE /MQTT-SERVER:<address>:<port>
[/MQTT-USER:<login name for authorization at the MQTT broker>] [/MQTT-PASSWORD:<password for authorization at
the MQTT broker>] [/LOGIN:<user name>] [/PWD:<password>]
```

명령 옵션

파라미터	설명
`/<ENABLE|DISABLE|SHOW>`	필수 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks의 통합을 활성화 또는 비활성화하거나 통합 상태를 볼 수 있습니다.
`/SERVERS:<address>:<port>`	필수 인수입니다. Kaspersky Industrial CyberSecurity for Networks 서버의 주소와 포트 또는 MQTT 게시자의 주소를 지정할 수 있습니다. 가능한 포트 값 범위: 1~65535.

`/KICS-MODE:<TELEMETRY|MQTT-PUBLISHER|UDP-DATA-DIODE>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Networks와 애플리케이션의 통합 모드를 선택할 수 있습니다. • `TELEMETRY`는 TCP 프로토콜을 통해 원격 측정을 Kaspersky Industrial CyberSecurity for Networks 서버로 직접 전송하는 모드입니다. • `MQTT-PUBLISHER`는 MQTT 중개 서버에 원격 측정을 전송하는 데 사용되는 모드입니다. • `UDP-DATA-DIODE`는 UDP 프로토콜을 사용하여 데이터 다이오드를 통해 원격 측정을 전송하는 모드입니다. 기본값은 `TELEMETRY`입니다.
`/PINNED-CERTIFICATE:<full path to the TLS certificate file>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Nodes를 Kaspersky Industrial CyberSecurity for Networks 서버에 연결하기 위한 TLS 인증서를 추가할 수 있습니다.
`/CLIENT-CERTIFICATE:<full path to the crypto-container>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 Kaspersky Industrial CyberSecurity for Networks 서버 간의 연결을 보호하기 위한 암호화된 클라이언트 인증서를 저장할 *암호화 컨테이너*를 추가할 수 있습니다.
`/CLIENT-PASSWORD:<password for the crypto-container>`	`/CLIENT-CERTIFICATE`가 통과되면 필요합니다. 암호화 컨테이너의 암호를 지정할 수 있습니다.
`/TIMEOUT:<maximum server response timeout>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Networks 서버의 최대 응답 시간을 초 단위로 지정할 수 있습니다. 제한 시간이 초과되면 다른 Industrial CyberSecurity for Networks 서버가 하나 이상 있을 경우 Kaspersky Industrial CyberSecurity for Nodes가 해당 서버에 연결을 시도합니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.
`/SYNC-PERIOD:<synchronization request period>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Networks 서버에 대한 요청 간격을 분 단위로 지정할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes가 MQTT 게시자로 작동할 때 브로커와의 연결이 끊어지면 이 설정에 따라 MQTT 브로커에 대한 요청 간격이 설정됩니다. 사용 가능한 값 범위는 1–60분입니다. 기본값은 1분입니다.
`/EVENTS-SENT-PERIOD:<maximum delay when sending events>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Networks 서버로 이벤트 전송 시의 최대 지연을 지정할 수 있습니다. 지정된 시간이 만료되면 애플리케이션이 같은 서버에 다시 연결을 시도하거나, 서버가 여러 개일 경우 목록에 있는 다음 서버에 연결합니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다. Kaspersky Industrial CyberSecurity for Nodes를 MQTT 구독자로 사용하는 경우 MQTT 게시자의 설정에서 최소 **`/EVENTS-SENT-PERIOD`** 값인 1초를 지정했다면 MQTT 게시자로 구성된 Kaspersky Industrial CyberSecurity for Nodes 장치 250대 이상에서 원격 측정을 수신하도록 구성하지 않는 것이 좋습니다. 설정값이 30초 이상인 경우 MQTT 게시자 1,000개 이상에서 데이터를 수신하도록 구성하지 않는 것이 좋습니다.
`/EVENTS-LIMIT:<1|0>`	선택 인수입니다. 전송되는 이벤트 수를 제한할 수 있습니다. 이벤트 수가 구성된 제한을 초과하면 애플리케이션이 이벤트 전송을 중지합니다.
`/EVENTS-PER-HOUR:<maximum number of events per hour>`	`/EVENTS-LIMIT:1`가 통과되면 필요합니다. 시간당 전송할 최대 이벤트 수를 지정할 수 있습니다. 사용 가능한 값 범위는 10–65535입니다. 기본 설정은 시간당 이벤트 3000개입니다.
`/PWD:<password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

/VIRTUAL-SPAN-ENABLE	선택 인수입니다. 무차별 원격 측정 모드를 활성화합니다. 기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 컴퓨터의 네트워크 인터페이스에 도착하고 애플리케이션이 설치된 컴퓨터로 주소가 지정되는 네트워크 트래픽을 수집합니다. 무차별 모드에서 애플리케이션은 사용 가능한 모든 서브넷에서 컴퓨터의 네트워크 인터페이스에 대한 네트워크 트래픽을 수집합니다. 애플리케이션은 수집된 트래픽을 사용하여 확장 원격 측정을 생성합니다. 모든 네트워크 어댑터가 무차별 모드(Promiscuous mode)를 지원하지는 않습니다. 이러한 네트워크 어댑터에서는 확장 원격 측정 수집이 작동하지 않습니다.
/VIRTUAL-SPAN-DISABLE	선택 인수입니다. 무차별 원격 측정 모드를 비활성화합니다.
/VIRTUAL-SPAN-ADD-RULES:<IPv4 addresses of the computer's network interfaces>	선택 인수입니다. 서브넷을 컴퓨터 네트워크 인터페이스의 주소(애플리케이션이 네트워크 인터페이스의 서브넷 마스크로 해당 서브넷 식별) 또는 IPv4 형식 서브넷이 있는 네트워크 인터페이스의 주소로 추가할 수 있습니다. 애플리케이션은 지정된 서브넷에 대해 구성된 네트워크 인터페이스에 대해서만 무차별 모드로 네트워크 트래픽을 수집합니다. 예: /VIRTUAL-SPAN-ADD-RULES:198.51.100.0; 198.51.100.0/24.
/VIRTUAL-SPAN-REMOVE-RULES: <subnet IDs>	선택 인수입니다. 지정된 ID를 가진 서브넷을 삭제할 수 있습니다. 추가된 서브넷 및 해당 ID 목록은 KAVSHELL KICS /SHOW 명령을 사용하여 표시할 수 있습니다.
/MQTT-SUBSCRIBER-ENABLE	선택 인수입니다. 데이터 다이오드에서 원격 측정을 수신하기 위해 MQTT 구독자 모드를 활성화합니다. 기본적으로 MQTT 구독자 모드는 비활성화되어 있습니다.
/MQTT-SUBSCRIBER-DISABLE	선택 인수입니다. MQTT 구독자 모드를 비활성화합니다.
/MQTT-SERVER:<address>:<port>	/KICS-MODE:MQTT-PUBLISHER 또는 /MQTT-SUBSCRIBER:ENABLE 파라미터가 전달되면 필수 파라미터입니다. MQTT 중개자의 주소 및 포트를 지정합니다. MQTT 중개자의 기본 포트는 1883입니다.
/MQTT-USER:<login>	로그인 및 암호 인증의 필수 파라미터는 MQTT 중개자에서 구성됩니다. MQTT 중개자에서의 인증을 위한 로그인 이름을 지정합니다.
/MQTT-PASSWORD:<password>	로그인 및 암호 인증의 필수 파라미터는 MQTT 중개자에서 구성됩니다. MQTT 중개자에서의 인증을 위한 암호를 지정합니다.
/UDP-SERVER:<address>:<port>	/KICS-MODE:UDP-DATA-DIODE 가 통과되면 필요합니다. Kaspersky Industrial CyberSecurity for Networks 서버의 주소와 포트를 지정할 수 있습니다.
/UDP-ENCRYPTION-ENABLE	선택 인수입니다. UDP 프로토콜을 통해 전송되는 데이터의 암호화를 활성화합니다.
/UDP-ENCRYPTION-DISABLE	선택 인수입니다. UDP 프로토콜을 통해 전송되는 데이터의 암호화를 비활성화합니다.
/UDP-ENCRYPTION-KEY:<full path to the encryption key>	/UDP-ENCRYPTION-ENABLE 가 통과되면 필요합니다. .PEM 확장자를 사용하는 암호화 키 파일의 경로를 지정할 수 있습니다.
/UDP-ENCRYPTION-PASSWORD: <password to the encryption key>	/UDP-ENCRYPTION-ENABLE 가 통과되면 필요합니다. 암호화 키의 암호를 지정할 수 있습니다.

예

```
KAVSHELL KICS /ENABLE /SERVERS:123.4.5.6:8080 /PINNED-CERTIFICATE:c:\user\certs\cetr.pfx /PWD:p@ssw0rd
KAVSHELL KICS /DISABLE /PWD:p@ssw0rd
KAVSHELL KICS /SHOW
KAVSHELL KICS /VIRTUAL-SPAN-ENABLE /PWD:p@ssw0rd
KAVSHELL KICS /VIRTUAL-SPAN-REMOVE-RULES:1,2,3 /PWD:p@ssw0rd
KAVSHELL KICS /VIRTUAL-SPAN-ADD-RULES:192.168.73.0/24;192.168.73.0/24 /PWD:p@ssw0rd
KAVSHELL KICS /ENABLE /KICS-MODE:MQTT-PUBLISHER /MQTT-SERVER:1.2.3.4:1218 /MQTT-USER:User /MQTT-PASSWORD:p@ssw0rd
```

```
/PWD:p@ssw0rd
KAVSHELL KICS /ENABLE /KICS-MODE:TELEMETRY /SERVERS:123.4.5.6:8080 /MQTT-SUBSCRIBER-ENABLE /MQTT-
SERVER:1.2.3.4:1218 /MQTT-USER:User /MQTT-PASSWORD:p@ssw0rd /PWD:p@ssw0rd
KAVSHELL KICS /MQTT-SUBSCRIBER-DISABLE
KAVSHELL KICS /ENABLE /KICS-MODE:UDP-DATA-DIODE /UDP-SERVER:1.2.3.4:1234 /UDP-ENCRYPTION-ENABLE /UDP-ENCRYPTION-
KEY:c:\user\username\123e4567-e89b-12d3-a456-426655440990.pem /UDP-ENCRYPTION-PASSWORD:p@ssw0rd
```

명령 반환 값:

- 0: 명령을 완료했습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -5: 구문 오류.

ISOLATION. 네트워크 격리 관리

`KAVSHELL ISOLATION` 명령을 사용하여 로컬에서 장치 네트워크 격리를 관리할 수 있습니다.

명령 구문

```
KAVSHELL ISOLATION [/DISABLE] [/SHOW] [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/DISABLE`	`/SHOW`를 전달하지 않은 경우 필수입니다. 장치 네트워크 격리를 비활성화합니다.
`/SHOW`	`/DISABLE`를 전달하지 않은 경우 필수입니다. 장치의 현재 네트워크 격리 설정을 콘솔에 출력합니다.
`/PWD:<password>`	`KAVSHELL ISOLATION /DISABLE` 명령의 필수 옵션입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

명령 반환 값:

- 0: 작업을 완료했습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -5: 구문 오류.
- -6: 잘못된 작업(이미 비활성화된 구성 요소를 비활성화하려는 시도 등).
- -7: 서비스가 등록되지 않았습니다
- -8: 서비스 자동 시작이 비활성화되었습니다.
- -9: 관리 대상 장치를 다른 사용자 계정으로 실행하려는 시도가 실패했습니다.
- -99: 알 수 없는 오류.

KSN. KSN/KPSN 사용

`KAVSHELL KSN` 명령을 사용하여 파일 또는 웹사이트의 평판을 확인할 Kaspersky 솔루션을 선택할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky 평판 데이터베이스 작업을 위해 다음과 같은 인프라 솔루션을 지원합니다.

- *Kaspersky Security Network(KSN)*은 대부분의 Kaspersky 애플리케이션에서 사용하는 솔루션입니다. KSN 참여자는 Kaspersky로부터 정보를 수신하며, Kaspersky 분석가의 추가 분석이 필요하고 평판 및 통계 데이터베이스에 포함해야 하는 사용자 컴퓨터에서 탐지된 개체에 관한 Kaspersky 정보를 전송합니다.

- *Kaspersky Private Security Network(KPSN)*는 Kaspersky Industrial CyberSecurity for Nodes 또는 기타 Kaspersky 애플리케이션을 호스팅하는 컴퓨터의 사용자가 자신의 컴퓨터에서 Kaspersky로 데이터를 보내지 않고도 Kaspersky 평판 데이터베이스 및 기타 통계 데이터에 접근할 수 있게 해주는 솔루션입니다. KPSN은 다음과 같은 이유로 Kaspersky Security Network에 참여할 수 없는 기업 고객용으로 제공됩니다:

  - 로컬 워크스테이션이 인터넷에 연결되어 있지 않습니다.

  - 국외 또는 기업 LAN 외부로의 데이터 전송이 법률이나 기업 보안 정책에 의해 금지되어 있습니다.

명령 구문

```
KAVSHELL KSN /GLOBAL|/PRIVATE <settings-file> /PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/GLOBAL`	Kaspersky Security Network 사용으로 전환합니다.
`/PRIVATE <settings-file>`	Kaspersky Private Security Network 사용으로 전환합니다. Kaspersky Private Security Network 설정이 포함된 구성 파일의 이름을 지정합니다. 이 파일의 확장자는 .PKCS7 또는 .PEM입니다.
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL KSN /GLOBAL /PWD:p@ssw0rd
KAVSHELL KSN /PRIVATE c:\settings.pkcs7 /PWD:p@ssw0rd
```

LICENSE. 애플리케이션 활성화

Kaspersky Industrial CyberSecurity for Nodes 키 및 활성화 코드는 `KAVSHELL LICENSE` 명령을 사용하여 관리할 수 있습니다.

명령 구문

```
KAVSHELL LICENSE [/ADD:<key_file | activation code> [/R]|/DEL:<license key serial number>|/REFRESH:<license id>]
/PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
지정된 옵션이 없습니다.	이 명령은 추가된 키에 대한 다음 정보를 반환합니다. • 키. • 라이센스 유형(상용). • 키와 연결된 라이센스 기간. • 키 상태(활성 또는 추가). 상태가 *이면 키가 추가 키로 추가된 것입니다.
`/ADD:<key_file | activation code>`	키 파일을 사용한 Kaspersky Industrial CyberSecurity for Nodes 활성화. 애플리케이션이 이미 활성화된 경우 이 키는 예약 키로 추가됩니다.
`/R`	`/R` 옵션을 전달하면 활성화 코드 또는 키가 예비 코드 또는 키로 추가됩니다.
`/DEL:<license key serial number>`	지정된 키 또는 활성화 코드를 삭제합니다.
`/REFRESH:<license id>`	지정된 라이센스의 상태를 업데이트합니다.
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

명령 반환 값:

- 0: 작업을 완료했습니다.
- -2: 서비스가 실행되고 있지 않습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -4: 지정된 번호의 키를 찾을 수 없습니다.
- -5: 구문 오류.
- -6: 잘못된 작업(키가 이미 추가됨).
- -99: 알 수 없는 오류.
- -301: 라이센스가 유효하지 않습니다.
- -303: 다른 애플리케이션용 라이센스입니다.

MDR. Managed Detection and Response 통합 구성

`KAVSHELL MDR` 명령을 사용하여 Kaspersky Industrial CyberSecurity for Nodes와 Managed Detection and Response 솔루션의 통합을 구성할 수 있습니다.

명령 구문

```
KAVSHELL MDR /ENABLE /BLOB:<path to pkcs7> [/PWD:<password>] [/LOGIN:<user name>] | /DISABLE [/BLOB:<path to pkcs7>] [/PWD:<password>] [/LOGIN:<user name>] | /SHOW
```

명령 옵션

파라미터	설명
`MDR /<enable|disable|show>`	필수 인수입니다. Managed Detection and Response(Industrial CyberSecurity) 구성 요소를 활성화 또는 비활성화하거나 현재 설정을 확인할 수 있습니다.
`/BLOB:<full path to the MDR configuration file>`	필수 인수입니다. MDR 구성 파일의 경로를 지정할 수 있습니다.
`/PWD:<password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL MDR /ENABLE /BLOB:C:\some\folder\blob.pkcs7 /PWD:p@ssw0rd
KAVSHELL MDR /DISABLE /PWD:p@ssw0rd
KAVSHELL MDR /SHOW
```

네트워크 차단. 네트워크 차단 관리

`KAVSHELL NETWORKBLOCKING` 명령을 사용하여 기기의 네트워크 연결 차단을 로컬에서 비활성화할 수 있습니다. 연결 차단에 대한 자세한 내용은 Kaspersky Industrial CyberSecurity for Networks 도움말을 참조하십시오.

명령 구문

```
KAVSHELL NETWORKBLOCKING /DISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/DISABLE`	필수 인수입니다. 기기의 네트워크 연결 차단을 비활성화합니다.
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.

`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

명령 반환 값:

- 0: 명령을 완료했습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -5: 구문 오류.
- -6: 잘못된 작업(이미 비활성화된 구성 요소를 비활성화하려는 시도 등).
- -9: 관리 대상 장치를 다른 사용자 계정으로 실행하려는 시도가 실패했습니다.
- -99: 알 수 없는 오류.

OMSINFO. 애플리케이션 정보가 포함된 JSON 파일 생성

`KAVSHELL OMSINFO` 명령을 사용하면 애플리케이션의 현재 상태와 탐지된 위협에 대한 정보가 포함된 JSON 파일을 생성한 후 모니터링 시스템에 업로드할 수 있습니다.

명령 구문

```
KAVSHELL OMSINFO <oms_info_json_file_name>
```

명령 옵션

파라미터	설명
`<oms_info_json_file_name>`	이름과 확장자를 포함한 JSON 파일의 전체 경로입니다.

예

```
KAVSHELL OMSINFO "C:\Dumps and others\omsinfo.json"
```

암호. Kaspersky Industrial CyberSecurity for Nodes 기능 접근을 암호로 보호

`KAVSHELL PASSWORD` 명령을 사용하면 Kaspersky Industrial CyberSecurity for Nodes 기능에 대한 암호로 보호된 접근을 관리할 수 있습니다. 이 기능이 활성화될 경우, 애플리케이션 삭제, 수정, 복구, 장치의 보호 레벨을 낮출 수 있는 명령줄 동작 수행 시 애플리케이션에서 사용자 이름 및 암호를 요청합니다.

명령 구문

```
KAVSHELL PASSWORD /SET /NEW:<new password> | /RESET /PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/SET`	중요한 작업을 확인하기 위한 암호 입력 요청을 활성화합니다.

`/NEW:<new password>`	`/SET`가 통과되면 필요합니다.
	새 암호를 설정합니다.
	암호 생성 시 다음 조건을 충족하는 것이 좋습니다:
	• 암호는 계정 이름이나 컴퓨터 이름을 포함하지 않습니다.
	• 암호는 8자 이상이어야 합니다.
	• 암호가 다음 카테고리에서 3개 이상에 해당하는 문자를 포함합니다.
	  • 라틴 대문자(A~Z)
	  • 라틴 소문자(a~z)
	  • 숫자(0~9)
	  • 느낌표(!), 달러 기호($), 파운드 기호(#), 퍼센트 기호(%)

`/RESET`	중요한 작업을 확인하기 위한 암호 입력 요청을 비활성화합니다.
`/PWD:<password>`	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

PATCHCOMPATIBILITYRESET. 호환되지 않는 패치 목록에서 패치 제거

`KAVSHELL PATCHCOMPATIBILITYRESET` 명령을 사용하면 호환되지 않는 패치 목록에서 지정된 GUID의 패치를 제거할 수 있습니다. 공백으로 구분된 여러 GUID를 지정할 수 있습니다.

명령 구문

```
KAVSHELL PATCHCOMPATIBILITYRESET <GUID> [GUID...]
```

예

```
KAVSHELL PATCHCOMPATIBILITYRESET 01234567-890A-BCDE-F012-34567890ABCD
```

성능 분석기. 성능 분석기 작업 결과 내보내기

`KAVSHELL PERFANALYZER` 명령을 사용하여 *성능 분석기* 작업 결과를 JSON 파일로 내보낼 수 있습니다.

명령 구문

```
KAVSHELL PERFANALYZER /EXPORT:<path to destination directory> [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
/EXPORT:<path to destination directory>	필수 인수입니다. .JSON 확장자의 파일을 내보낼 폴더 경로를 지정합니다.
/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL PERFANALYZER /EXPORT:C:\PerfAnalyzer
```

명령 반환 값:

- 0: 명령을 완료했습니다.
- -2: 서비스가 실행되고 있지 않습니다.
- -4: 개체를 찾을 수 없습니다.
- -5: 구문 오류.
- -99: 알 수 없는 오류.

PREVENTION. 실행 방지

KAVSHELL PREVENTION 명령을 사용하여 개체 실행 방지를 관리할 수 있습니다.

명령 구문

```
KAVSHELL PREVENTION /SHOW | /DISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
/SHOW	/DISABLE를 지정하지 않았을 때의 필수 인수입니다. 현재 실행 방지 설정 보기. 명령을 실행하면 다음 응답을 받습니다. prevention.enabled=true|false prevention.mode=audit|prevent prevention.rules id: <rule ID> target: script|process|document md5: <MD5 hash of the file> sha256: <SHA256 hash of the file> pattern: <path to the object> case-sensitive: true|false
/DISABLE	/SHOW를 지정하지 않았을 때의 필수 인수입니다. 실행 방지 비활성화.

/PWD:<password>	KAVSHELL PREVENTION /DISABLE 명령의 필수 옵션입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL PREVENTION /DISABLE /LOGIN:Admin /PWD:p@ssw0rd
```

명령 반환 값:

- 0: 작업을 완료했습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -5: 구문 오류.
- -6: 잘못된 작업(이미 비활성화된 구성 요소를 비활성화하려는 시도 등).
- -7: 서비스가 등록되지 않았습니다
- -8: 서비스 자동 시작이 비활성화되었습니다.
- -9: 관리 대상 장치를 다른 사용자 계정으로 실행하려는 시도가 실패했습니다.
- -99: 알 수 없는 오류.

REMOTEACCESS. 애플리케이션 콘솔 원격 연결 설정 관리

KAVSHELL REMOTEACCESS 명령을 사용하여 Kaspersky Industrial CyberSecurity for Nodes가 설치된 장치에 대한 애플리케이션 콘솔의 원격 연결 설정을 관리할 수 있습니다.

명령 구문

```
KAVSHELL REMOTEACCESS /SET /PORT=<new_port> [/PWD:<password>] [/LOGIN:<user name>] | /RESET UIKLPORT [/PWD:
<password>] [/LOGIN:<user name>] | /SHOW
```

명령 옵션

파라미터	설명
/SET [UIPORT | UIKLPORT]	포트 번호 설정: • UIPORT 은 Windows 자격 증명을 사용하여 연결하는 포트입니다. • UIKLPORT 은 수동으로 생성한 사용자가 자격 증명을 사용하여 연결하는 포트입니다.
/PORT=<new_port>	/SET 가 통과되면 필요합니다. 포트 번호. 가능한 값 범위: 1~65535.
/RESET UIKLPORT	수동으로 생성한 사용자가 자격 증명을 사용하여 연결하는 포트를 닫습니다.
/SHOW	현재 포트 번호를 출력합니다.

/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL REMOTEACCESS /SET UIPORT /PORT=50000
KAVSHELL REMOTEACCESS /RESET UIKLPORT
KAVSHELL REMOTEACCESS /SHOW
```

RESETMDRMACHINEID. 장치 ID 재설정

KAVSHELL RESETMDRMACHINEID 명령을 사용하면 Managed Detection and Response 솔루션에서 사용하는 장치 ID를 재설정할 수 있습니다.

명령 구문

```
KAVSHELL RESETMDRMACHINEID [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

RESTORE. 파일 복원

KAVSHELL RESTORE 명령을 사용하여 백업 및 격리에서 파일을 복원할 수 있습니다.

명령 구문

```
KAVSHELL RESTORE <filename> [/REPLACE][/QUARANTINE][/BACKUP]/PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
<file name>	필수 인수입니다. 복원할 파일의 전체 경로.
/REPLACE	선택 인수입니다. 기존 파일 덮어쓰기 이 옵션을 전달하지 않으면 충돌이 없는 경우에만 파일이 복원됩니다.

/QUARANTINE	선택 인수입니다. 격리에서 파일을 복원합니다.
/BACKUP	선택 인수입니다. 백업에서 파일을 복원합니다(기본값).
/PWD:<password>	필수 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

명령 구문

```
KAVSHELL RESTORE /REPLACE C:\\eicar.com
KAVSHELL RESTORE /QUARANTINE C:\\test\eicar.com /PWD=1234 /LOGIN=user
```

명령 반환 값:

- 0: 작업을 완료했습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -5: 구문 오류.
- -6: 잘못된 작업입니다.
- -7: 서비스가 등록되지 않았습니다
- -8: 서비스 자동 시작이 비활성화되었습니다.
- -9: 관리 대상 장치를 다른 사용자 계정으로 실행하려는 시도가 실패했습니다.
- -99: 알 수 없는 오류.

ROLLBACK. 마지막 업데이트 롤백

KAVSHELL ROLLBACK 명령은 *마지막 업데이트 롤백* 작업을 시작합니다.

명령 구문

```
KAVSHELL ROLLBACK [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.

`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL ROLLBACK
```

명령 반환 값:

- 0: 작업을 완료했습니다.
- -2: 서비스가 실행되고 있지 않습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -99: 알 수 없는 오류.
- -221: 데이터베이스 백업 복사본을 찾을 수 없거나 복사본이 손상되었습니다.
- -222: 데이터베이스 백업 복사본이 손상되었습니다.

RTP. 실시간 파일 보호

`KAVSHELL RTP` 명령을 사용하면 실시간 파일 보호 구성 요소를 활성화하거나 비활성화할 수 있습니다.

명령 구문

```
KAVSHELL RTP </START|/STOP> [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`</START|/STOP>`	실시간 파일 보호 구성 요소 활성화 또는 비활성화: • `/START`은 구성 요소를 활성화합니다. • `/STOP`은 구성 요소를 비활성화합니다.
`/PWD:<password>`	`KAVSHELL RTP /STOP` 명령의 필수 옵션입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL RTP STOP /PWD:p@ssw0rd
```

SCAN. 온디맨드 검사

KAVSHELL SCAN 명령을 사용하여 *온디맨드 검사* 작업을 만들고 시작할 수 있습니다. 명령줄에서 기존 온디맨드 검사 작업을 시작하려면 KAVSHELL TASK 명령을 사용하십시오.

명령 구문

```
KAVSHELL SCAN <scan_scope> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<file_name>][/F<A|C|E>]
[/NEWONLY][/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|DELETE]
[/E:<ABMSPO>] [/EM:<"masks">] [/ES:<size>] [/ET:<s>][/TZOFF] [/NOICHECKER][/NOISWIFT][/NOCHECKMSSIGN]
[/ANALYSERLEVEL] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

명령 옵션

파라미터	설명
<scan_scope>	필수 인수입니다. 파일, 폴더, 네트워크 경로 또는 표준 검사 범위를 공백으로 구분한 목록입니다. 표준 검사 범위: • /MEMORY 은(는) 모든 메모리 프로세스를 검사합니다. • /SHARED 은(는) 공유 폴더를 검사합니다. • /STARTUP 은(는) 시작 개체를 검사합니다. • /REMDRIVES 은(는) 이동식 드라이브를 검사합니다. • /FIXDRIVES 은(는) 모든 로컬 하드 드라이브를 검사합니다. • /MYCOMP 은(는) 전체 컴퓨터를 검사합니다. 공백으로 구분된 여러 값을 지정할 수 있습니다.
/L:<file_name>	선택 인수입니다. 검사 범위 목록이 있는 파일 경로입니다. 파일을 직접 생성하고 TXT 형식으로 저장해야 합니다. 파일은 BOM 없이 UTF-8 인코딩으로 저장해야 합니다.
/F<A|C|E>	선택 인수입니다. 검사 범위에 포함해야 하는 개체: • /FA: 모든 개체를 검사합니다. 애플리케이션은 예외 없이 모든 파일(모든 형식 및 확장자)을 검사합니다. • /FC: 형식에 따라 개체를 검사합니다. 애플리케이션은 감염 가능한 개체의 형식 목록에 포함된 형식의 개체만 검사합니다. • /FE: 확장자에 따라 개체를 검사합니다. 애플리케이션이 감염될 수 있는 개체의 확장자 목록에 포함된 확장자를 가진 개체만 검사합니다.
/NEWONLY	선택 인수입니다. 새 파일과 수정된 파일만 검사합니다. 이 인수를 전달하지 않으면 Kaspersky Industrial CyberSecurity for Nodes는 모든 개체를 검사합니다.
/AI: <DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>	선택 인수입니다. 감염된 개체 및 기타 개체에 대해 애플리케이션이 수행할 처리 방법: • DISINFECT: 치료 - 불가능한 경우 알림. • DISINFDEL: 치료 - 불가능한 경우 삭제. • DELETE: 삭제. • REPORT(기본값): 알림. • AUTO: 권장.

파라미터	설명
/AS:<QUARANTINE|DELETE|REPORT|AUTO>	선택 인수입니다. 감염된 개체에 대해 애플리케이션이 수행할 처리 방법: • QUARANTINE: 격리로 이동합니다. • DELETE: 삭제. • REPORT(기본값): 알림. • AUTO: 권장.
/E:<ABMSPO>	지정한 개체 유형을 제외합니다. 가능한 값: • A: ZIP, CAB, RAR, ARJ 압축 파일 및 기타 압축 파일 형식. • B: Microsoft Outlook 및 Microsoft Outlook Express 메일 데이터베이스 파일. • M: Microsoft Outlook 및 Microsoft Outlook Express 메시지와 같은 메일 형식의 파일. • S: 자동 압축 해제 압축 파일. • P: UPX 또는 ASPack과 같은 이진 코드 압축 프로그램으로 압축된 실행 파일. • O: 파일에 삽입된 개체(예: Microsoft Word 매크로 또는 이메일 메시지 첨부 파일). 여러 파라미터 값을 지정할 수 있습니다.
/EM=<file mask>	파일 마스크와 일치하는 파일은 검사 범위에서 제외됩니다. 예: • *.exe 마스크는 EXE 확장자를 가진 파일의 모든 경로를 포함합니다. • example* 마스크는 이름이 EXAMPLE인 파일의 모든 경로를 포함합니다.
/ET=<scan duration in seconds>	지정된 시간 제한(초)보다 검사하는 데 오래 걸리는 파일은 검사 범위에서 제외됩니다. 60초로 기본 설정되어 있습니다.
/ES=<size in megabytes>	지정된 크기 제한(MB)보다 큰 파일은 검사 범위에서 제외됩니다. 기본값은 100MB입니다.
/TZOFF	신뢰 구역 예외 규칙을 적용하지 않습니다.
/NOICHECKER	iChecker 사용 중지(기본적으로 활성화됨).
/NOISWIFT	iSwift 사용 중지(기본적으로 활성화됨).
/NOCHECKMSSIGN	Microsoft에서 디지털 서명한 파일은 검사하지 않습니다.
/ANALYSERLEVEL	휴리스틱 분석기를 활성화하고 분석 레벨을 구성합니다. 사용 가능한 휴리스틱 분석 레벨은 다음과 같습니다. • 1: 빠름. • 2: 보통. • 3: 정밀. 이 인수를 전달하지 않으면 애플리케이션에서 휴리스틱 분석기를 사용하지 않습니다.
/EXCLUDE=<list of exlusion	검사 작업 범위에서 제외할 파일, 폴더 또는 네트워크 경로의 목록입니다. 공백으로 구분된 여러 값을 지정할 수 있습니다.
/W=<file path>	작업 로그 파일의 경로 및 이름입니다. 동일한 로그 설정으로 명령을 다시 시작하면 기존 로그 파일을 덮어씁니다.
/ANSI	작업 로그에 기록되는 이벤트에 ANSI 인코딩을 사용합니다. /W 파라미터를 전달하지 않으면 /ANSI 파라미터가 적용되지 않습니다. /ANSI 파라미터를 지정하지 않으면 Unicode을 사용하여 작업 로그를 생성합니다.
/ALIAS:<alternate name>	실행 중인 작업을 참조하는 데 사용할 임시 이름을 작업에 할당합니다. 예를 들어 KAVSHELL TASK 명령을 사용하여 작업 통계를 볼 수 있습니다. 대체 작업 이름은 애플리케이션의 모든 대체 작업 이름 중에서 고유해야 합니다. 이 인수를 전달하지 않으면 작업 이름이 다음과 같이 할당됩니다: scan_<kavshell_pid>. 예: scan_1234.

예

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\003.exe "\\another server\Shared\"
F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER
/NOISWIFT /W:log.log
KAVSHELL SCAN /L:scan_objects.lst /W:log.log
```

명령 반환 값:

- 0: 작업이 성공적으로 완료되었습니다(탐지된 위협 없음).
- 1: 작업이 취소되었습니다.
- -2: 서비스가 실행되고 있지 않습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -4: 개체를 찾을 수 없습니다(검사 범위 목록이 포함된 파일을 찾을 수 없음).
- -5: 구문 오류가 발생했거나 검사 범위가 설정되지 않았습니다.
- -80: 감염된 개체가 탐지되었습니다.
- -81: 감염 의심 개체가 탐지되었습니다.
- -82: 검사 중 개체 처리 오류가 발생했습니다.
- -83: 검사되지 않은 개체가 탐지되었습니다.
- -84: 손상된 개체가 탐지되었습니다.
- -85: 작업 로그를 생성하지 못했습니다.
- -99: 알 수 없는 오류.
- -301: 라이센스가 유효하지 않습니다.

SCAN-IOC. IOC 검사

`KAVSHELL SCAN-IOC` 명령을 사용하여 *IOC 검사* 작업을 구성하고 시작할 수 있습니다.

명령 구문

```
KAVSHELL SCAN-IOC <full path to IOC file> [/PATH:<path to folder with IOC files>] [/PROCESS=no] [/HINT=<full path
to the executable file of the process|full path to file>]
[/REGISTRY=no] [/DNSENTRY=no] [/ARPENTRY=no] [/PORTS=no] [/SERVICES=no] [/SYSTEM=no] [/USERS=no] [/VOLUMES=no]
[/EVENTLOG=no] [/DATETIME=<event publication date>] [/CHANNELS=<list of channels>]
[/FILES=no] [/DRIVES=<all|system|critical|custom>] [/NETWORK=no] [/URL=no] [/EMAIL=no] [/ROUTE=no] [/RETRO]
[/DEPTH=<1-14>] [/EXCLUDES=<list of exclusions>] [/SCOPE=<configurable list of folders>]
```

명령 옵션

옵션	설명
`<full path to IOC file>`	검색에 사용할 IOC 또는 xml 확장자가 있는 IOC 파일의 전체 경로입니다. `/PATH:<path to the folder with IOC files>`를 지정하지 않았을 때의 필수 인수입니다.
`/PATH:<path to the folder with IOC files>`	검사에 사용할 IOC 파일이 있는 폴더의 경로입니다. `<full path to IOC file>`를 지정하지 않았을 때의 필수 인수입니다.

`/PROCESS=no`	선택 인수입니다. 검사 중에는 프로세스 정보 분석을 비활성화합니다. 인수의 값이 <no>라면 Kaspersky Industrial CyberSecurity for Nodes는 검사를 수행할 때 컴퓨터에서 실행 중인 프로세스를 분석하지 않습니다. IOC 파일에 ProcessItem IOC 문서의 IOC 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 ProcessItem IOC 문서가 설명된 경우에만 프로세스 데이터를 분석합니다.
`/HINT=<full path to the executable file of the process|full path to the file>`	선택 인수입니다. 이 인수를 사용하면 개별 파일을 지정하여 ProcessItem 및 FileItem IOC 문서를 사용하는 검사에서 분석할 데이터 범위를 줄일 수 있습니다. 다음을 이 인수의 값으로 전달할 수 있습니다: • `<full path to executable file of the process (ProcessItem)>` – ProcessItem • `<full path to file>` – FileItem 이 인수는 `/PROCESS=yes` 및 `/FILES=yes` 인수와 결합해서만 전달할 수 있습니다.
`/REGISTRY=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 레지스트리 키(IOC 문서 RegistryItem)의 분석을 비활성화합니다. 이 인수의 값이 <no>라면 Kaspersky Industrial CyberSecurity for Nodes가 레지스트리 키 관련 정보를 분석하지 않습니다. IOC 파일에 RegistryItem IOC 문서 용어가 포함되어 있으면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes는 검사를 위해 제공된 IOC 파일에 RegistryItem IOC 문서가 설명된 경우에만 레지스트리를 분석합니다.
`/DNSENTRY=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 로컬 DNS 캐시 레코드(IOC 문서 DnsEntryItem)의 분석을 비활성화합니다. 인수의 값이 <no>라면 Kaspersky Industrial CyberSecurity for Nodes가 로컬 DNS 캐시를 검사하지 않습니다. IOC 파일에 DnsEntryItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 DnsEntryItem IOC 문서가 설명된 경우에만 로컬 DNS 캐시를 검사합니다.
`/ARPENTRY=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 로컬 ARP 테이블 레코드(IOC 문서 ArpEntryItem)의 분석을 비활성화합니다. 인수의 값이 <no>라면 Kaspersky Industrial CyberSecurity for Nodes가 로컬 ARP 테이블을 검사하지 않습니다. IOC 파일에 ArpEntryItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 ArpEntryItem IOC 문서가 설명된 경우에만 로컬 ARP 테이블을 검사합니다.
`/PORTS=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 수신 대기 중인 포트(IOC 문서 PortItem)에 대한 정보 분석을 비활성화합니다. 인수의 값이 <no>라면 Kaspersky Industrial CyberSecurity for Nodes가 장치의 활성 연결 테이블을 검사하지 않습니다. IOC 파일에 PortItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 PortItem IOC 문서가 설명된 경우에만 활성 연결 테이블을 검사합니다.
`/SERVICES=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 장치에 설치된 서비스(IOC 문서 ServiceItem)에 대한 정보 분석을 비활성화합니다. 인수의 값이 <no>라면 Kaspersky Industrial CyberSecurity for Nodes가 장치에 설치된 서비스의 정보를 검사하지 않습니다. IOC 파일에 ServiceItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 ServiceItem IOC 문서가 설명된 경우에만 서비스 정보를 분석합니다.

/SYSTEM=no	선택 인수입니다. 이 인수는 IOC 검사 중 환경 관련 정보(IOC 문서 SystemInfoItem) 분석을 비활성화합니다. 이 인수의 값이 <no> 라면 Kaspersky Industrial CyberSecurity for Nodes는 환경 관련 정보를 분석하지 않습니다. IOC 파일에 SystemInfoItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 SystemInfoItem IOC 문서가 설명된 경우에만 환경 정보를 분석합니다.
/USERS=no	선택 인수입니다. 이 인수는 IOC 검사 중에 사용자 관련 정보(IOC 문서 UserItem) 분석을 비활성화합니다. 이 인수의 값이 <no> 라면 Kaspersky Industrial CyberSecurity for Nodes가 시스템에서 생성한 사용자 관련 데이터를 분석하지 않습니다. IOC 파일에 UserItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 UserItem IOC 문서가 설명된 경우에만 시스템에서 생성한 사용자 관련 정보를 분석합니다.
/VOLUMES=no	선택 인수입니다. 이 인수는 IOC 검사 중에 볼륨(IOC 문서 VolumeItem)에 대한 정보 분석을 비활성화합니다. 인수의 값이 <no> 라면 Kaspersky Industrial CyberSecurity for Nodes가 장치 볼륨 정보를 검사하지 않습니다. IOC 파일에 VolumeItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 VolumeItem IOC 문서가 설명된 경우에만 볼륨 정보를 분석합니다.
/EVENTLOG=no	선택 인수입니다. 이 인수는 IOC 검사 중에 Windows 이벤트 로그 레코드(IOC 문서 EventLogItem)의 분석을 비활성화합니다. 이 인수의 값이 <no> 라면 Kaspersky Industrial CyberSecurity for Nodes가 Windows 이벤트 로그 레코드를 검사하지 않습니다. IOC 파일에 EventLogItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 EventLogItem IOC 문서가 설명된 경우에만 Windows 이벤트 로그 레코드를 분석합니다. EventLogItem\source IOC 용어에는 이벤트의 XML 스키마에 있는 공급자 이름 값을 사용합니다.
/DATETIME=<event publication date>	선택 인수입니다. 이 파라미터는 해당 IOC 문서에 대한 IOC 검사 범위를 결정할 때 이벤트가 Windows 이벤트 로그에 게시된 날짜를 고려하는 것을 활성화하거나 비활성화할 수 있습니다. IOC 검사 수행 시 Kaspersky Industrial CyberSecurity for Nodes는 지정된 시간 및 날짜부터 작업이 실행되는 순간까지의 기간에 게시된 이벤트만 검사합니다. Kaspersky Industrial CyberSecurity for Nodes에서는 이벤트 게시 날짜를 인수 값으로 지정할 수 있습니다. 지정된 날짜 이후와 검색 실행 전 Windows 이벤트 로그에 게시된 이벤트에 대해서만 검색을 수행합니다. 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes는 모든 게시 날짜의 이벤트를 검색합니다. 이 설정은 검사를 위해 제공된 IOC 파일에 EventLogItem IOC 문서가 설명된 경우에만 사용됩니다.
/CHANNELS=<list of channels>	선택 인수입니다. 이 인수를 사용하면 IOC 검사를 수행하려는 채널(로그) 이름 목록을 전달할 수 있습니다. 이 인수가 전달되면 IOC 검사 작업 실행 시 Kaspersky Industrial CyberSecurity for Nodes가 지정된 로그에 게시된 이벤트만 고려합니다. 로그 이름은 로그 속성(전체 이름 / Full Name 파라미터) 또는 이벤트 속성(이벤트의 xml 스키마에 있는 <Channel></Channel> 파라미터)에 지정된 로그(채널) 이름에 따라 스트링으로 지정됩니다. 기본적으로(이 인수가 전달되지 않은 경우 포함) IOC 검사는 Application, System, Security 채널을 대상으로 수행됩니다. 이 인수에 여러 값을 전달할 수 있습니다(공백으로 구분). 이 설정은 검사를 위해 제공된 IOC 파일에 EventLogItem IOC 문서가 설명된 경우에만 사용됩니다.

`/FILES=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 파일(IOC 문서 FileItem)에 대한 정보 분석을 비활성화합니다. 이 인수의 값이 <no> 라면 Kaspersky Industrial CyberSecurity for Nodes가 파일 관련 정보를 분석하지 않습니다. IOC 파일에 FileItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 FileItem IOC 문서가 설명된 경우에만 파일 정보를 분석합니다.
`/DRIVES=<all|system|critical|custom>`	선택 인수입니다. 이 인수를 사용하면 FileItem IOC 문서에 대한 데이터를 분석할 때 IOC 검사 범위를 지정할 수 있습니다. 다음 값 중 하나를 사용할 수 있습니다: • `all`은 애플리케이션이 사용 가능한 모든 파일 영역을 검사하도록 합니다. • `system`은 애플리케이션이 운영 체제가 설치된 폴더의 파일만 검사하도록 합니다. • `critical`은 애플리케이션이 사용자 및 시스템 폴더에 있는 임시 파일만 검사하도록 합니다. • `custom`은 애플리케이션이 사용자가 지정한 범위에 있는 파일만 검사하도록 합니다. 인수를 지정하지 않으면 중요 영역을 검사합니다.
`/NETWORK=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 Network IOC 문서 기반의 위협 검사를 사용하지 않습니다. 인수의 값이 <no>라면 Kaspersky Industrial CyberSecurity for Nodes가 Network IOC 문서를 기반으로 위협을 검사하지 않습니다. IOC 파일에 Network IOC 문서의 용어가 포함되어 있다면, 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 Network IOC 문서가 설명된 경우에만 Network IOC 문서 기반의 위협 검사를 활성화합니다.
`/URL=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 UrlHistoryItem IOC 문서 기반의 위협 검사를 사용하지 않습니다. 인수의 값이 <no>라면 Kaspersky Industrial CyberSecurity for Nodes가 UrlHistoryItem IOC 문서를 기반으로 위협을 검사하지 않습니다. IOC 파일에 UrlHistoryItem IOC 문서의 용어가 포함되어 있다면, 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 UrlHistoryItem IOC 문서가 설명된 경우에만 UrlHistoryItem IOC 문서 기반의 위협 검사를 활성화합니다.
`/EMAIL=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 메일 개체(IOC 문서 Email)의 분석을 비활성화합니다. 이 인수의 값이 <no> 라면 Kaspersky Industrial CyberSecurity for Nodes가 메일 개체를 분석하지 않습니다. IOC 파일에 이메일 IOC 문서의 용어가 포함되어 있다면, 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes는 검사를 위해 제공된 IOC 파일에 Email IOC 문서가 설명된 경우에만 메일 개체를 분석합니다.
`/ROUTE=no`	선택 인수입니다. 이 인수는 IOC 검사 중에 RouteEntryItem IOC 문서 기반의 위협 검사를 활성화합니다. 인수의 값이 <no>라면 Kaspersky Industrial CyberSecurity for Nodes가 RouteEntryItem IOC 문서를 기반으로 위협을 검사하지 않습니다. IOC 파일에 UrlHistoryItem IOC 문서의 용어가 포함되어 있다면, 이 용어를 무시합니다(불일치로 탐지). 이 인수를 지정하지 않으면 Kaspersky Industrial CyberSecurity for Nodes가 검사를 위해 제공된 IOC 파일에 RouteEntryItem IOC 문서가 설명된 경우에만 RouteEntryItem IOC 문서 기반의 위협 검사를 활성화합니다.
`/RETRO`	선택 인수입니다. 이 인수는 *회고적 IOC 검사* 모드에서 작업을 실행합니다. `/DEPTH=<interval in days>`를 사용하면 애플리케이션에서 소급 IOC 검사를 수행할 기간을 추가로 전달할 수 있습니다. 최대값은 14일입니다. 시간은 작업이 시작된 순간부터 계산됩니다. 예: `KAVSHELL SCAN-IOC /PATH=<path to a folder with IOC files> /RETRO /DEPTH=2` 이 시간 간격이 경과되지 않으면 기본값은 1일로 설정됩니다.
`/EXCLUDES=<list of exclusions>`	선택 인수입니다. 이 인수를 사용하면 FileItem IOC 문서에 대한 데이터를 분석할 때 예외 범위를 지정할 수 있습니다. 이 인수에 공백으로 구분된 여러 경로를 전달할 수 있습니다. 이 인수를 지정하지 않으면 예외 없이 검사를 수행합니다.

`/SCOPE=<configurable list of folders>`	선택 인수입니다. `/DRIVES=custom` 인수를 지정했다면 이 인수가 필요합니다. 이 인수를 사용하면 검사 범위 목록을 지정할 수 있습니다. 이 인수에 공백으로 구분된 여러 경로를 전달할 수 있습니다.

명령이 완료되었고(반환 값 `0`) 도중에 침해지표가 감지되면, Kaspersky Industrial CyberSecurity for Nodes가 명령줄에 다음 작업 결과 정보를 출력합니다:

침해지표 탐지 시 애플리케이션이 명령줄에 출력하는 정보

`Uuid`	IOC 파일 구조의 헤더에서 IOC 파일의 ID(`<ioc id="">` 태그)
`Name`	IOC 파일 구조의 헤더에서 IOC 파일에 대한 설명(`<description></description>` 태그)
`Matched Indicator Items`	일치하는 모든 지표의 ID 목록입니다.
`Matched objects`	일치 항목이 있는 각 IOC 문서에 대한 데이터입니다.
`Date`	침해지표가 발견된 파일의 생성 날짜입니다.
`Created`	FileItem에만 해당합니다. 침해지표가 발견된 개체의 생성 날짜입니다.
`Pid`	침해지표가 발견된 프로세스의 ID입니다.
`Upid`	침해지표가 발견된 프로세스의 고유 ID입니다.
`ParentPid`	침해지표가 발견된 프로세스가 포함된 상위 개체 ID입니다.
`Username`	검사한 개체를 수정한 사용자의 이름입니다.
`StartTime`	침해지표가 발견된 프로세스의 시작 시간입니다.

SCAN-OVAL. 보안 감사

`KAVSHELL SCAN-OVAL` 명령을 사용하여 *보안 감사* 작업을 구성하고 시작할 수 있습니다. 다음 규칙 경로의 경우 명령줄 인터페이스를 사용하여 보안 감사 작업을 구성하고 실행할 수 있습니다:

- **SCADA용 Kaspersky ICS CERT 취약점 데이터베이스**
- **운영 체제용 규정 준수 및 보안 구성**
- **파일의 사용자 지정 규칙 기반**.

명령 구문

```
KAVSHELL SCAN-OVAL [/SOURCE:<kl|kl-compl|file>] [/REPOSITORY:show] [/PATH:<full path to the folder>] [/EXTERNAL-VARS:<full path and name of ZIP archive with external variables>] [/MODE:<all|exclude|include>] [/DEFINITIONS:<vuln_type_01;...;vuln_type_N>] /RESULT-PATH:<path to the folder with the report> [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/SOURCE:<kl|kl-compl|file>`	선택 인수입니다. 보안 감사에 필요한 규칙의 소스: • `kl` – 배포 패키지에 포함된 Kaspersky ICS CERT 취약점 데이터베이스입니다. Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 모듈을 성공적으로 업데이트한 후 명령줄에서 사용할 수 있습니다. • `kl-compl` – 배포 패키지에 포함된 운영 체제용 보안 구성 및 표준 준수입니다. Kaspersky Industrial CyberSecurity for Nodes 데이터베이스 및 모듈을 성공적으로 업데이트한 후 명령줄에서 사용할 수 있습니다. • `file` – 파일의 사용자 지정 규칙 데이터베이스입니다. 파라미터 값을 지정하지 않을 경우 기본적으로 다음 경로가 사용됩니다: **SCADA용 Kaspersky ICS CERT 취약점 데이터베이스** (`/SOURCE=kl`).

`/REPOSITORY:show`	선택 인수입니다. 이 파라미터는 선택한 규칙 경로가 운영 체제용 보안 구성 및 표준 준수일 경우 사용 가능합니다 (`/SOURCE=kl-compl`). 이 파라미터를 지정할 경우 Kaspersky Industrial CyberSecurity for Nodes는 보안 감사 작업을 실행하는 대신 기존 보안 구성의 이름이 나열된 XML 파일을 `/RESULT-PATH` 파라미터에 의해 지정된 폴더에 저장합니다.
`/PATH:<full path to the folder>`	선택 인수입니다. 이 파라미터는 OVAL 규칙이 있는 XML 파일이 포함된 압축 파일 또는 **운영 체제용 규정 준수 및 보안 구성**(`/SOURCE=kl-compl`) 및 **파일의 사용자 지정 규칙 기반**(`/SOURCE=file`) 소스에 대한 OVAL 및 XCCDF 규칙이 있는 XML 파일이 포함된 압축 파일에 대한 전체 경로를 지정합니다. OVAL 및 XCCDF 규칙은 BOM 없이 UTF-8로 저장해야 합니다.
`/EXTERNAL-VARS:<full path and name of ZIP archive with external variables>`	선택 인수입니다. 이 파라미터는 OVAL 규칙용 외부 변수가 있는 XML 파일이 포함된 ZIP 압축파일의 이름과 전체 경로를 지정합니다. 경로에 OVAL 규칙만 포함된 경우 파라미터를 사용할 수 있습니다.
`/MODE:<all|exclude|include>`	선택 인수입니다. 이 파라미터는 취약점 검사 모드를 정의합니다. 경로에 OVAL 규칙만 포함된 경우 파라미터를 사용할 수 있습니다. 가능한 파라미터 값: • `all` – 경로에 나열된 모든 취약점을 검사합니다. • `exclude` – `/definitions` 파라미터에 의해 지정된 취약점을 제외하고 경로에 나열된 취약점을 검사합니다. • `include` – `/definitions` 파라미터에 의해 지정된 취약점 파라미터 값을 지정하지 않으면 `all` 모드가 기본적으로 사용됩니다.
`/DEFINITIONS:<vuln_type_01;...;vuln_type_N>`	선택 인수입니다. 검사해야 하거나 검사에서 제외해야 하는 취약점 유형을 세미콜론으로 구분한 목록입니다. 경로에 OVAL 규칙만 포함된 경우 파라미터를 사용할 수 있습니다. 예: `oval:org.mitre.oval.test:def:998;oval:org.mitre.oval.test:def:999`. `/MODE=include` 또는 `/MODE=exclude` 파라미터와 함께 사용됩니다.
`/RESULT-PATH`	필수 인수입니다. XML 형식 검사 리포트가 저장되는 폴더의 경로를 지정합니다. 파일 이름에는 노드 이름과 작업이 실행된 날짜 및 시간이 포함됩니다. 파라미터를 지정하지 않으면 작업 실행이 실패합니다.
`/PWD:<password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL SCAN-OVAL /SOURCE:kl /RESULT-PATH:c:\storage\reports
KAVSHELL SCAN-OVAL /SOURCE:kl-comp /REPOSITORY:show /RESULT-PATH:c:\storage\reports
```

SCANCRITICAL. 중요 영역 검사

`KAVSHELL SCANCRITICAL` 명령은 *중요 영역 검사* 작업을 시작합니다.

명령 구문

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>] [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/W`	선택 인수입니다. 내보낸 작업 로그의 파일 이름을 .LOG 확장자로 지정합니다. 파일 경로를 지정할 수도 있습니다. 명령에 파일 이름만 지정하면 애플리케이션은 해당 파일을 애플리케이션 설치 폴더에 저장하려고 시도합니다. 애플리케이션의 자체 보호 메커니즘이 활성화되어 있으면 애플리케이션의 자체 보호 기능이 애플리케이션 폴더에 새 파일이 생성되는 것을 차단하므로 내보내기에 실패합니다. 로그를 내보내려면 파일 경로를 지정합니다.
`/PWD:<password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

SERVERBINDINGDISABLE. 중앙 관리 서버 연결 보호 중지

`KAVSHELL SERVERBINDINGDISABLE` 명령은 중앙 관리 서버 연결 보호를 로컬에서 중지합니다. 이 명령은 컴퓨터의 중앙 관리 서버 연결 암호를 제거하는 *중앙 관리 서버 연결 보호* 작업을 시작합니다.

명령 구문

```
KAVSHELL SERVERBINDINGDISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/PWD:<password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

SIEM. SIEM 시스템 통합

`KAVSHELL SIEM` 명령을 사용하면 텔레메트리를 전송하기 위해 SIEM 시스템과의 통합을 구성할 수 있습니다.

명령 구문

```
KAVSHELL SIEM /ENABLE /TLS /SERVERS=<protocol://server:port;protocol://server:port...> /TIMEOUT=<seconds> /PWD:
<password> /LOGIN:<user name> /PINNED-CERTIFICATE=<path> /CLIENT-CERTIFICATE=<path> /CLIENT-PASSWORD=<password>
/MAXIMUM-DATA-TRANSFER-TIME=<seconds> | /DISABLE | /SHOW
```

명령 옵션

파라미터	설명
`/<ENABLE|DISABLE|SHOW>`	필수 인수입니다. SIEM 통합 구성 요소 설정을 활성화 또는 비활성화하거나 확인합니다.
`/TLS`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 SIEM 서버 간 연결 암호화를 활성화합니다.
`/SERVERS=<protocol://server:port;protocol://server:port...>`	필수 인수입니다. 서버 주소 및 포트를 지정합니다. 가능한 포트 값 범위: 1~65535.
`/TIMEOUT=<seconds>`	선택 인수입니다. SIEM 서버의 응답을 기다리는 최대 시간(초)입니다. 사용 가능한 값 범위: 1~3600초. 기본값은 30초입니다.
`/PINNED-CERTIFICATE=<path>`	`/TLS`가 통과되면 필요합니다. Kaspersky Industrial CyberSecurity for Nodes와 SIEM 서버 간에 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다.
`/CLIENT-CERTIFICATE=<path>`	선택 인수입니다. Kaspersky Industrial CyberSecurity for Nodes와 SIEM 서버 간의 연결을 보호하기 위한 암호화된 클라이언트 인증서를 저장하는 PFX 파일인 *암호화 컨테이너*를 추가할 수 있습니다.
`/CLIENT-PASSWORD=<password>`	`/CLIENT-CERTIFICATE`가 통과되면 필요합니다. 암호화 컨테이너의 암호를 지정할 수 있습니다.
`/MAXIMUM-DATA-TRANSFER-TIME=<seconds>`	SIEM 서버의 응답을 기다리는 최대 시간(초)입니다. 지정된 시간을 초과하면 Kaspersky Industrial CyberSecurity for Nodes는 같은 서버에 연결을 시도하거나, 서버가 여러 개라면 목록의 다음 서버에 연결합니다. 사용 가능한 값 범위: 1~3600초. 기본값은 5초입니다.
`/PWD:<password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL SIEM /ENABLE /SERVERS="tcp://server1:1234;udp://server2:5678;http://server3:9012" /TIMEOUT=10 /MAXIMUM-
DATA-TRANSFER-TIME=20"
KAVSHELL SIEM /DISABLE
KAVSHELL SIEM /SHOW
```

SIGMA. Sigma 규칙을 사용한 이상 행위 탐지

`KAVSHELL SIGMA` 명령을 사용하여 Sigma 규칙을 사용한 이상 행위 탐지 구성 요소를 관리할 수 있습니다.

명령 구문

```
KAVSHELL SIGMA /<ENABLE|DISABLE|ADD|REMOVE|SHOW> [/COLLECTION:<rat|deltav|uac|siemens|yokogawa|nfta|custom>]
[/NAME:<collection name>] [/SOURCE:<full path to the folder with the YAML files>] [/PWD:<password> [/LOGIN:<user
name>]
```

명령 옵션

파라미터	설명
`/<ENABLE|DISABLE|ADD|REMOVE|SHOW>`	필수 인수입니다. 다음 동작 중 하나를 지정합니다. • `ENABLE` – Sigma 규칙을 사용한 이상 행위 탐지 활성화 • `DISABLE` – Sigma 규칙을 사용한 이상 행위 탐지 비활성화 • `ADD` – Sigma 규칙 컬렉션 추가 • `REMOVE` – Sigma 규칙 컬렉션 제거 • `SHOW` – Sigma 규칙을 사용한 이상 행위 탐지의 현재 설정 표시
`/COLLECTION:` `<rat|deltav|uac|siemens|yokogawa|nfta|custom>`	`SIGMA /<ADD|REMOVE>`을(를) 지정하면 이 파라미터가 필요합니다. 추가하거나 제거할 Sigma 규칙 컬렉션의 유형을 지정합니다: • `rat`: 원격 관리 도구(RAT) 탐지. • `deltaV`: Emerson DeltaV용 이상 행위 탐지. • `uac`: 사용자 계정 컨트롤(UAC). • `siemens`: Siemens SIMATIC WinCC, Siemens TIA Portal, Siemens SIMATIC STEP 7용 이상 행위 탐지. • `yokogawa`: Yokogawa CENTUM VP용 이상 행위 탐지. • `nfta`: 네트워크 및 이동식 미디어를 통한 파일 공유 감사. • `custom`: 사용자 지정 규칙 컬렉션. `test`를 지정할 수도 있습니다. AO Kaspersky Lab의 내부 테스트를 위해 설계된 규칙 하나가 추가되거나 제거됩니다.
`/NAME:<collection name>`	`SIGMA /<ADD|REMOVE>` 및 `/COLLECTION:custom`을(를) 지정하면 이 파라미터가 필요합니다. 사용자 지정 Sigma 규칙 컬렉션의 이름을 지정합니다.
`/SOURCE:<full path to the folder with the YAML files>`	`SIGMA /ADD` 및 `/COLLECTION:custom`을(를) 지정하면 이 파라미터가 필요합니다. 사용자 지정 Sigma 규칙을 설명하는 YAML 파일이 있는 폴더의 전체 경로를 지정합니다.
`/PWD:<password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL SIGMA /ENABLE
KAVSHELL SIGMA /ADD /COLLECTION:deltav
KAVSHELL SIGMA /REMOVE /COLLECTION:custom /NAME:rules.yaml
```

START. 애플리케이션 서비스 시작

`KAVSHELL START` 명령은 Kaspersky Industrial CyberSecurity for Nodes 서비스 서비스를 시작합니다.

명령 구문

```
KAVSHELL START
```

STARTPOLICY. 정책 사용

`KAVSHELL STARTPOLICY` 명령은 보호된 장치에서 Kaspersky Security Center 정책을 활성화합니다. 정책에 따라 애플리케이션 설정이 구성됩니다.

명령 구문

```
KAVSHELL STARTPOLICY
```

STOP. 애플리케이션 서비스 중지

`KAVSHELL STOP` 명령은 Kaspersky Industrial CyberSecurity for Nodes 서비스 서비스를 중지합니다.

명령 구문

```
KAVSHELL STOP [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/PWD:<password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

명령 반환 값:

- 0: 작업을 완료했습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -5: 구문 오류.
- -6: 잘못된 작업입니다(Kaspersky Industrial CyberSecurity for Nodes 서비스이(가) 이미 중지됨).

- -7: 서비스가 등록되지 않았습니다
- -8: 서비스 자동 시작이 비활성화되었습니다.
- -9: 관리 대상 장치를 다른 사용자 계정으로 실행하려는 시도가 실패했습니다.
- -99: 알 수 없는 오류.

작업. 작업 관리

`KAVSHELL TASK` 명령을 사용하여 Kaspersky Industrial CyberSecurity for Nodes 작업을 실행, 일시 중지, 재개 및 중지하고 현재 작업 상태와 통계를 확인할 수 있습니다.

명령 구문

```
KAVSHELL TASK [<alternative name> </START | /STOP | /STATE | /STATISTICS>] /PWD:<password> [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
매개변수 없음	기존의 모든 Kaspersky Industrial CyberSecurity for Nodes 작업 목록을 반환합니다. 목록에는 작업의 대체 이름(Kaspersky Industrial CyberSecurity for Nodes for Windows에서 작업에 할당하는 추가적인 짧은 이름), 작업 카테고리(시스템 또는 사용자), 작업의 현재 상태 필드가 포함됩니다.
`<alternative name>`	관리할 작업의 대체 이름입니다. Kaspersky Industrial CyberSecurity for Nodes 작업 별칭을 보려면 `KAVSHELL TASK` 명령을 매개변수 없이 입력합니다.
`/START`	작업 시작.
`/STOP`	작업 중지.
`/STATE`	작업의 현재 상태를 표시합니다.
`/STATISTICS`	작업 통계를 표시합니다.
`/PWD:<password>`	`KAVSHELL TASK /STOP` 명령의 필수 옵션입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

명령 구문

```
KAVSHELL TASK on-access /START
KAVSHELL TASK user-task_1 /STOP
KAVSHELL TASK scan-critical /STATE
```

명령 반환 값:

- 0: 작업을 완료했습니다.
- -2: 서비스가 실행되고 있지 않습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -4: 개체를 찾을 수 없습니다(작업을 찾을 수 없음).

- -5: 구문 오류가 발생했거나 검사 범위가 설정되지 않았습니다.
- -6: 유효하지 않은 작업입니다(예: 작업이 실행 중이 아니거나 이미 실행 중이거나 일시 중지할 수 없음).
- -99: 알 수 없는 오류.
- -301: 라이센스가 유효하지 않습니다.
- 401: 작업이 시작되지 않았습니다(`KAVSHELL TASK <task name> /STATE` 명령의 경우).
- 402: 작업이 이미 시작되었습니다(`KAVSHELL TASK <task name> /STATE` 명령의 경우).
- 403: 작업이 일시 중지되었습니다(`KAVSHELL TASK <task name> /STATE` 명령의 경우).
- -404: 작업에 실패했습니다(작업 상태 변경으로 인해 비정상 종료가 발생했습니다).

TELEMETRYFILTERS. 원격 측정 이벤트 필터링 규칙 내보내기 및 가져오기

`KAVSHELL TELEMETRYFILTERS` 명령을 사용하여 원격 분석 이벤트 필터링 규칙을 내보내거나 가져올 수 있습니다.

명령 구문

```
KAVSHELL TELEMETRYFILTERS [/IMPORT /EXPORT] <file_path> [/PWD:<password>] [/LOGIN:<user name>]
```

명령 옵션

파라미터	설명
`/IMPORT <file_path>`	`/EXPORT`를 전달하지 않은 경우 필수입니다. 파일에서 원격 분석 이벤트 필터링 규칙을 가져옵니다. 규칙이 포함된 JSON 파일의 이름과 확장자를 포함한 전체 경로를 지정합니다. 이벤트 필터링 규칙이 컴퓨터에 이미 있는 경우, Kaspersky Industrial CyberSecurity for Nodes는 가져오기를 수행할 때 이 규칙을 교체합니다.
`/EXPORT <file_path>`	`/IMPORT`를 전달하지 않은 경우 필수입니다. 원격 분석 이벤트 필터링 규칙을 JSON 파일로 내보냅니다. • 명령에 파일 이름만 지정하면 애플리케이션은 해당 파일을 애플리케이션 설치 폴더에 저장하려고 시도합니다. 애플리케이션의 자체 보호 메커니즘이 활성화되어 있으면 애플리케이션의 자체 보호 기능이 애플리케이션 폴더에 새 파일이 생성되는 것을 차단하므로 내보내기에 실패합니다. 규칙을 내보내려면 파일 경로를 지정합니다.
`/PWD: <password>`	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
`/LOGIN:<user name>`	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL TELEMETRYFILTERS /IMPORT "C:\some\folder\telemetry_filers.json" /LOGIN:Admin /PWD:p@ssw0rd
```

토큰. 보안 이동식 드라이브에 대한 접근 차단 관리

`KAVSHELL TOKEN` 명령을 사용하면 보호된 이동식 드라이브에 대한 접근 차단을 관리하고 장치에 연결된 보호된 이동식 드라이브에 대한 정보를 볼 수 있습니다.

명령 구문

```
KAVSHELL TOKEN [/ENUMERATE | /PROTECTION:<status|enable|disable>]
```

명령 옵션

파라미터	설명
`/ENUMERATE`	연결된 보호된 이동식 드라이브를 나열합니다.
`/PROTECTION:<status|enable|disable>]`	보안 이동식 드라이브에 대한 접근 차단 관리: • `status`는 현재 보호 상태를 표시합니다. • `enable`는 보호를 활성화합니다. • `disable`는 보호를 중지합니다.

예

```
KAVSHELL TOKEN /ENUMERATE
KAVSHELL TOKEN /PROTECTION:status
KAVSHELL TOKEN /PROTECTION:enable
KAVSHELL TOKEN /PROTECTION:disable
```

TRACE. 애플리케이션 동작 추적

`KAVSHELL TRACE` 명령을 사용하면 애플리케이션 동작 추적을 사용하거나 중지할 수 있습니다.

명령 구문

```
KAVSHELL TRACE </ON /F:<traces_folder:>[/S:<traces_size_in_MB>] [/LVL:<debug|info|warning|error|critical>] /R:<max
trace files to rotate> | /OFF > [/LOGIN:<user name>] [/PWD:<password>]
```

명령 옵션

파라미터	설명
`</ON | /OFF>`	필수 인수입니다. 애플리케이션 동작 추적을 사용하거나 중지합니다.
`/F:<traces_folder>`	`/ON`가 통과되면 필요합니다. 추적 파일을 저장할 폴더의 경로입니다.
`/S:<traces_size_in_MB>`	선택 인수입니다. 추적 파일의 최대 크기(MB)입니다. 사용 가능한 값: 1~4095MB. 기본값은 100MB입니다.

/LVL: <debug|info|warning|error|critical>	선택 인수입니다. 디버그 정보의 상세 수준. • critical은 추적 파일이 치명적인 오류에 관한 메시지만 저장한다는 뜻입니다. • error은 추적 파일이 경고뿐만 아니라 모든 오류에 관한 메시지를 저장한다는 뜻입니다. • warning은 추적 파일이 모든 오류, 경고 및 추가 정보에 관한 메시지를 저장한다는 뜻입니다. • info(기본값)은 추적 파일이 모든 오류 및 경고에 관한 메시지는 물론 애플리케이션의 정상 작동에 관한 정보도 저장한다는 뜻입니다. • debug은 추적 파일이 애플리케이션 작동에 관한 모든 정보를 저장한다는 뜻입니다.
/R:<max trace files to rotate>	선택 인수입니다. 추적 로그의 최대 파일 수. 사용 가능한 값: 1부터 999까지. 기본값은 5입니다.
/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:info /R:50 /PWD:p@ssw0rd
KAVSHELL TRACE /OFF
```

UPDATE. 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트

KAVSHELL UPDATE 명령을 사용하여 *업데이트* 작업을 관리할 수 있습니다.

명령 구문

```
KAVSHELL UPDATE <update_source | /AK | /KL> [/NOUSEKL] [/PROXY:<IP address>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:
<user_name>] [/PROXYPWD:<password>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE]
[/TIMEOUT:<s>] [/REG:<code_by_iso3166>] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

명령 옵션

파라미터	설명
<update_source | /AK | /KL>	필수 인수입니다. 업데이트 경로 선택: • <update_source> 사용자 지정 업데이트 경로를 사용합니다. 보호된 장치의 폴더 경로, UNC 형식의 네트워크 폴더 경로 또는 업데이트 폴더가 있는 HTTP 또는 FTP 서버의 주소를 지정할 수 있습니다. • /AK Kaspersky Security Center 중앙 관리 서버를 업데이트 경로로 사용합니다. • /KL Kaspersky 업데이트 서버를 업데이트 경로로 사용합니다. 공백으로 구분된 여러 값을 지정할 수 있습니다.
/NOUSEKL	선택 인수입니다. 다른 업데이트 경로를 사용할 수 없는 경우에도 Kaspersky 업데이트 서버를 사용하지 않습니다(기본값).
/PROXY:<IP address>:<port>	선택 인수입니다. 프록시 서버의 IP 주소 또는 기호 이름 및 포트 번호.

/AUTHTYPE:<0-2>	선택 인수입니다. 프록시 서버 인증 유형: • 0은 현재 사용자 계정을 사용한 NTLM 인증입니다. • 1은 /PROXYUSER 및 /PROXYPWD 옵션으로 사용자 이름과 암호를 지정한 사용자 계정을 사용한 NTLM 인증입니다. • 2은 /PROXYUSER 및 /PROXYPWD 옵션으로 지정한 사용자 이름과 암호를 사용한 인증입니다.
/PROXYUSER:<user_name>	/AUTHTYPE:1 또는 /AUTHTYPE:2 파라미터가 전달되면 필수 파라미터입니다. 프록시 서버에 접근하는 데 사용할 사용자 이름입니다. /AUTHTYPE:0을 지정하면 /PROXYUSER:<user_name> 및 /PROXYPWD:<password> 옵션이 무시됩니다.
/PROXYPWD:<password>	/AUTHTYPE:1 또는 /AUTHTYPE:2 파라미터가 전달되면 필수 파라미터입니다. 프록시 서버에 접근하는 데 사용할 사용자 암호입니다. /AUTHTYPE:0을 지정하면 /PROXYUSER:<user_name> 및 /PROXYPWD:<password> 옵션이 무시됩니다. /PROXYUSER 파라미터를 지정하고 /PROXYPWD 파라미터를 생략하면 암호가 빈 문자열로 간주됩니다.
/NOPROXYFORKL	선택 인수입니다. Kaspersky 업데이트 서버에 연결할 때 프록시 서버 설정을 사용하지 않습니다.
/USEPROXYFORCUSTOM	선택 인수입니다. 프록시 서버 설정을 사용하여 사용자 지정 업데이트 경로에 연결합니다.
/USEPROXYFORLOCAL	선택 인수입니다. 프록시 서버 설정을 사용하여 로컬 업데이트 경로에 연결합니다.
/NOFTPPASSIVE	선택 인수입니다. 이 옵션을 지정하면 Kaspersky Industrial CyberSecurity for Nodes에서 FTP 서버 연결에 활성 모드를 사용합니다. 이 옵션을 전달하지 않으면 Kaspersky Industrial CyberSecurity for Nodes에서 가능한 경우 수동 연결 모드를 사용합니다.
/TIMEOUT:<s>	선택 인수입니다. FTP 또는 HTTP 서버 연결 시간 제한(초)입니다. 기본값: 10초.
/REG:<code_by_iso3166>	선택 인수입니다. ISO 3166-1 표준에 따른 보호된 장치가 위치한 국가의 코드입니다. 예: /REG:GR. 이 파라미터를 생략하거나 잘못된 국가 코드를 지정하면 Kaspersky Industrial CyberSecurity for Nodes에서 애플리케이션 콘솔이 설치된 보호된 장치의 지역 설정을 기준으로 위치를 확인합니다. 애플리케이션은 업데이트 서버를 선택할 때 위치 정보를 사용합니다.
/W=<file path>	작업 로그 파일의 경로 및 이름입니다. 동일한 로그 설정으로 명령을 다시 시작하면 기존 로그 파일을 덮어씁니다.
/ANSI	작업 로그에 기록되는 이벤트에 ANSI 인코딩을 사용합니다. /W 파라미터를 전달하지 않으면 /ANSI 파라미터가 적용되지 않습니다. /ANSI 파라미터를 지정하지 않으면 Unicode을 사용하여 작업 로그를 생성합니다.
/ALIAS:<alternate name>	실행 중인 작업을 참조하는 데 사용할 임시 이름을 작업에 할당합니다. 예를 들어 KAVSHELL TASK 명령을 사용하여 작업 통계를 볼 수 있습니다. 대체 작업 이름은 애플리케이션의 모든 대체 작업 이름 중에서 고유해야 합니다. 이 인수를 전달하지 않으면 작업 이름이 다음과 같이 할당됩니다: update_<kavshell_pid>. 예: update_1234.
/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

명령 구문

```
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /USEPROXYFORCUSTOM /PROXY:proxy.company.com:8080
/AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd /TIMEOUT:100 /REG:ru /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /NOUSEKL /USEPROXYFORCUSTOM
/PROXY:proxy.company.com:8080 /AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
KAVSHELL UPDATE /AK /NOUSEKL
```

```
KAVSHELL UPDATE /KL /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE /AK /W:"C:\KAVREPORTS\daily update.log"
```

명령 반환 값:

- 0: 작업을 완료했습니다.
- 200: 모든 개체가 최신 상태입니다.
- -2: 서비스가 실행되고 있지 않습니다.
- -3: 명령을 실행할 권한이 부족합니다.
- -5: 구문 오류.
- -99: 알 수 없는 오류.
- -206: 지정한 업데이트 경로에 확장 파일이 없거나 형식을 알 수 없습니다.
- -209: 업데이트 경로에 연결하는 중 오류가 발생했습니다.
- -232: 프록시 서버에 연결하는 중 인증 오류가 발생했습니다.
- -234: Kaspersky Security Center 연결 오류.
- -235: Kaspersky Industrial CyberSecurity for Nodes가 업데이트 경로에 연결할 때 인증되지 않았습니다.
- -236: 애플리케이션 데이터베이스가 손상되었습니다.
- -301: 라이센스가 유효하지 않습니다.

YARA. YARA 검사 실행

`KAVSHELL YARA` 명령을 사용하여 YARA 검사를 실행할 수 있습니다.

명령 구문

```
KAVSHELL YARA <full path to a YARA file> | /PATH=<path to a folder with YARA files> [<additional arguments>]
```

명령 옵션

필수 인수	설명
`<full path to a YARA file>`	검사에 사용할 YARA 파일의 전체 경로입니다. 공백으로 구분된 여러 YARA 파일 경로를 지정할 수 있습니다. `/PATH`를 전달하지 않은 경우 필수입니다. 예: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/PATH=<path to a folder with YARA files>`	검사에 사용할 YARA 파일이 있는 폴더의 전체 경로입니다. `<full path to a YARA file>`를 전달하지 않은 경우 필수입니다. 예: `/PATH=C:\Users\Admin\Desktop\YARA`

`/FASTSCAN=<on|off>`	선택 인수입니다. 빠른 YARA 검사. 애플리케이션은 각 개체에 대해 탐지된 지표의 발생을 한 번만 기록합니다. 또한 애플리케이션은 로그에서 탐지된 지표의 중복 파일을 숨깁니다. 빠른 YARA 검사를 사용하면 대용량 파일을 더 빠르게 검사할 수 있습니다. 이 설정을 지정하지 않으면 애플리케이션이 표준 YARA 검사를 수행합니다. 이 모드에서는 애플리케이션이 중복으로 탐지된 지표를 로그에 반영합니다.
`/MAXRULES=<maximum number of scan rules>`	선택 인수입니다. 한도에 도달하면 애플리케이션이 YARA 검사를 중지하도록 하는 고유한 규칙 트리거 한도입니다. 이 설정의 값이 지정되지 않거나 `0`이 지정되면 애플리케이션은 제한 없이 YARA 검사를 수행합니다.
`/TIMEOUT=<N seconds>`	선택 인수입니다. YARA 검사에 걸리는 시간(초). 이 시간이 초과되면 애플리케이션은 YARA 검사를 중지합니다. 이 설정의 값이 지정되지 않거나 `0`이 지정되면 애플리케이션은 제한 없이 YARA 검사를 수행합니다.
`/RECURSIVE=<on|off>`	선택 인수입니다. 이 인수는 `/SCANFOLDERS)` 사용자 지정 검사 내 하위 폴더에 반복 검사를 시작합니다.
`/SCANFOLDERS=<path to folders for the YARA scan>`	선택 인수입니다. 이 인수는 지정된 폴더 목록에 있는 파일에 YARA 검사를 시작합니다. 공백으로 구분된 여러 값을 지정할 수 있습니다. Kaspersky Industrial CyberSecurity for Nodes는 폴더 경로 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다. 이 설정이 지정되지 않으면 애플리케이션은 네트워크 공유, 클라우드 드라이브 및 이동식 미디어를 제외한 모든 로컬 디스크에 대해 YARA 검사를 수행합니다.
`/SCANMEMORY=<on|off>`	선택 인수입니다. 실행 중인 모든 프로세스의 메모리를 검사합니다.
`/SCANPROCESS=<full paths to executable files of processes>`	선택 인수입니다. 지정된 프로세스에 대해서만 메모리를 검사합니다. 프로세스 실행 파일의 공백으로 구분된 전체 경로를 지정합니다. `*` 및 `?` 문자로 마스크를 입력할 수 있습니다.
`/MAXSIZE=<size in bytes>`	선택 인수입니다. YARA 검사를 위한 파일 크기를 제한합니다. 애플리케이션은 더 큰 파일은 건너뜁니다.
`/INCLUDES=<list of objects for the YARA scan>`	선택 인수입니다. 검사 범위 편집. 공백으로 구분된 여러 값을 지정할 수 있습니다. 다음과 같은 값을 사용할 수 있습니다. • 파일 이름 • 파일 확장자 검사 범위는 `/SCANFOLDERS` 파라미터와 함께 지정되어야 합니다. 예: `/SCANFOLDERS C:\*.* /includes=*.exe *.dll` – 애플리케이션이 디스크 C에서 .EXE 및 .DLL 확장자를 사용하는 모든 파일을 검사합니다.
`/EXCLUDES=<paths to objects to be excluded from the YARA scan>`	선택 인수입니다. YARA 검사에서 파일을 제외합니다. 공백으로 구분된 여러 값을 지정할 수 있습니다. 다음과 같은 값을 사용할 수 있습니다. • 파일 경로 • 파일 경로 마스크 예외 규칙은 `/SCANFOLDERS` 파라미터와 함께 지정되어야 합니다. 예: `/SCANFOLDERS C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – 애플리케이션은 readme.txt 파일, C:\trusted folder 폴더의 모든 파일 및 C 드라이브의 루트 폴더에 xml 확장자를 가진 모든 파일을 건너뜁니다.
`/SCANAUTORUNS=<on|off>`	선택 인수입니다. 자동 실행 지점 개체에 대한 YARA 검사를 수행합니다.
`/EXCLUDEAUTORUNS=<list of autorun point objects to exclude from the YARA scan>`	선택 인수입니다. 검사 범위에서 자동 실행 지점 개체를 제외합니다. 프로세스 실행 파일의 공백으로 구분된 전체 경로를 지정합니다. `*` 및 `?` 문자로 마스크를 입력할 수 있습니다.

/LOGFOLDER=<path for saving scan results>	선택 인수입니다. 폴더의 경로를 지정하면 애플리케이션이 yara_<컴퓨터 이름>_<검사 완료 시각>.txt 파일의 지정된 경로에 있는 검사 결과를 저장합니다. 특정 TXT 파일의 경로를 지정하면 애플리케이션이 해당 파일에 검사 결과를 저장합니다. 예를 들어 /LOGFOLDER=C:\test 또는 /LOGFOLDER=C:\test\abc.txt 입니다. 검사 결과는 /LOGFOLDER 옵션 지정 여부와 관계없이 명령줄에 출력됩니다.
/PWD:<password>	선택 인수입니다. KLAdmin 사용자 계정 또는 충분한 권한이 있는 사용자 계정의 암호입니다. 이 옵션을 지정하지 않으면 애플리케이션은 다음 줄에서 암호를 입력하라는 메시지를 표시합니다.
/LOGIN:<user name>	선택 인수입니다. 충분한 권한이 있는 사용자 계정 이름입니다. 이 옵션을 지정하지 않으면 애플리케이션이 다음 줄에서 사용자 이름을 입력하라는 메시지를 표시합니다. KLAdmin 암호를 입력한 경우 이 값을 입력할 필요가 없습니다.

예

```
KAVSHELL YARA C:\rule.yara /SCANFOLDERS=c:\scanFolder\ /RECURSIVE=on
KAVSHELL YARA /PATH=c:\rules\ /SCANFOLDERS=c:\scanFolder\ /FASTSCAN=on
KAVSHELL YARA c:\rules\rule1.yara c:\rules\rule2.yara /SCANFOLDERS=c:\scanFolder\ /LOGFOLDER=c:\yara_logs\
KAVSHELL YARA /PATH=c:\rules\ /SCANFOLDERS=c:\scanFolder\ c:\scanFolder2\ /LOGFOLDER=c:\yara_logs\
```

기술 지원 서비스에 문의

이 섹션에서는 기술 지원을 받는 방법과 그 조건에 관해 설명합니다.

기술 지원을 요청하는 방법

애플리케이션 문서 또는 그 외 Kaspersky Industrial CyberSecurity for Nodes에 대한 정보 출처에서 문제에 대한 해결 방법을 찾을 수 없을 시 기술 지원에 문의할 것을 권장합니다. 기술 지원에서 Kaspersky Industrial CyberSecurity for Nodes 설치 및 사용에 관한 질문에 답해 드립니다.

Kaspersky는 애플리케이션 수명 주기 동안 Kaspersky Industrial CyberSecurity for Nodes에 대한 지원을 제공합니다(애플리케이션 수명 주기 페이지 참조). 기술 지원 서비스에 문의하기 전에 지원 규칙을 읽어보시기 바랍니다.

다음 방법 중 하나로 기술 지원에 문의할 수 있습니다:

- 기술 지원 웹사이트 방문
- Kaspersky CompanyAccount 포털을 통해 Kaspersky 기술 지원 요청

Kaspersky CompanyAccount를 통한 기술 지원

Kaspersky CompanyAccount는 Kaspersky 애플리케이션을 사용하는 기업용 포털입니다. Kaspersky CompanyAccount는 온라인 요청을 통해 사용자와 Kaspersky 전문가가 원활하게 소통하도록 하기 위해 마련되었습니다. Kaspersky CompanyAccount를 사용하면 Kaspersky 전문가가 처리하는 전자 요청의 진행 상황을 모니터링하고 전자 요청 내역을 저장할 수 있습니다.

또한 Kaspersky CompanyAccount에서 단일 사용자 계정으로 조직의 모든 직원을 등록할 수 있습니다. 단일 계정을 사용하면 등록된 직원이 Kaspersky로 보낸 전자 요청을 중앙에서 관리할 수 있으며 Kaspersky CompanyAccount를 통해 직원의 권한을 관리할 수도 있습니다.

Kaspersky CompanyAccount는 다음 언어로 제공됩니다.

- 영어
- 스페인어
- 이탈리아어
- 독일어
- 폴란드어
- 포르투갈어
- 러시아어

- 프랑스어
- 일본어

기술 지원 웹사이트에서 Kaspersky CompanyAccount에 관해 저 자세히 알아볼 수 있습니다.

기술 지원 전문가에게 확장 진단 정보 제공

애플리케이션 문제에 대한 보다 효율적인 지원 및 문제 해결을 위해 기술 지원 전문가는 진단 중 디버깅을 목적으로 애플리케이션 설정을 일시적으로 변경하도록 요청할 수 있습니다. 이때, 다음 작업을 수행해야 할 수 있습니다:

- 확장 진단 정보를 처리하고 저장하는 기능을 활성화합니다.
- 표준 사용자 인터페이스 요소를 통해서는 사용할 수 없는 개별 소프트웨어 구성 요소의 설정을 미세 조정합니다.
- 처리된 진단 정보의 저장 및 전송 설정을 변경합니다.
- 네트워크 트래픽 차단 및 로깅 구성.

나열된 동작을 수행하는 데 필요한 모든 정보(단계 순서 설명, 변경 가능한 설정, 구성 파일, 스크립트, 추가 명령줄 기능, 디버깅 모듈, 전용 유틸리티 등) 및 디버깅 목적으로 분석된 데이터의 구성은 기술 지원 전문가가 알립니다. 고급 진단 정보는 사용자의 컴퓨터에 저장됩니다. 저장된 데이터를 Kaspersky로 자동 전송하는 작업은 수행되지 않습니다.

기술 지원 전문가에게 문제를 보고하면 기술 지원 전문가는 Kaspersky Industrial CyberSecurity for Nodes의 작동에 관한 정보가 포함된 리포트를 생성하여 기술 지원으로 보내달라고 요청할 수 있습니다. Kaspersky 기술 지원 전문가가 추적 파일 생성, 메모리 덤프 파일 전송, Kaspersky Get System Info 유틸리티의 리포트 제공을 요청할 수도 있습니다.

사용자가 보낸 데이터를 분석한 후 기술 지원 전문가는 AVZ 스크립트를 만들어 사용자에게 보낼 수 있습니다. AVZ 스크립트를 사용하면 활성 프로세스에 위협이 있는지 분석하고, 컴퓨터에 위협이 있는지 검사하며, 감염된 파일을 치료 또는 삭제하고, 시스템 검사 리포트를 만들 수 있습니다.

위에서 나열된 동작은 기술 지원 전문가의 지침에 따라 제공된 안내를 통해서만 수행할 수 있습니다. 애플리케이션 문서 또는 기술 지원 전문가의 권장 사항에 설명되지 않은 방법으로 애플리케이션 설정을 도움 없이 수정하면 운영 체제의 속도 저하 및 오작동, 컴퓨터 보호 수준 저하, 처리 중인 정보의 가용성 및 무결성 위반이 발생할 수 있습니다.

애플리케이션 동작 추적

*애플리케이션 추적 로그*는 애플리케이션에서 수행한 동작과 해당 애플리케이션 동작 시 발생한 이벤트의 메시지에 관한 정밀 기록입니다. 추적 로그 프로세스 중에 애플리케이션은 서로 다른 애플리케이션 구성 요소의 작동에 대한 데이터가 포함된 파일 세트를 생성합니다.

애플리케이션 추적 로그는 Kaspersky 기술 지원의 감독하에 수행해야 합니다.

추적 파일을 통해 애플리케이션의 단계별 수행 과정을 추적하여 오류가 발생한 애플리케이션 동작 구간을 파악할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 애플리케이션 추적을 활성화하고 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **오작동 진단** 섹션으로 갑니다.
4. **오작동 진단 설정** 블록에서 **설정** 버튼을 클릭합니다.
   애플리케이션 추적 설정 탭에서 **오작동 진단 설정** 창이 열립니다.
5. **추적 활성화** 확인란을 사용하여 애플리케이션 동작 추적을 활성화하거나 비활성화합니다.
   기본적으로 애플리케이션 동작 추적이 비활성화되었습니다.
6. 필요하다면 Kaspersky Industrial CyberSecurity for Nodes 추적 파일을 저장할 기본 폴더를 변경합니다. 변경하려면 **추적 파일 폴더** 필드에 로컬 폴더의 전체 경로를 지정합니다.

   > 폴더는 사전에 생성되어야 하고 SYSTEM 계정으로 작성 가능해야 합니다. 네트워크 폴더, 드라이브, 환경 변수는 지정할 수 없습니다.

   선택한 폴더에서 Kaspersky Industrial CyberSecurity for Nodes는 추적 파일을 저장하기 위해 logs-Kaspersky Industrial CyberSecurity for Nodes-<uid>라는 하위 폴더를 생성합니다. 여기서 <uid>는 8자의 고유 로그 식별자입니다.
7. 디버그 정보의 상세 수준을 선택합니다:
   - **일반**은 추적 파일이 모든 오류, 경고에 관한 메시지는 물론 애플리케이션의 정상 작동에 관한 정보도 저장한다는 뜻입니다(기본값).
   - **심각**은 추적 파일이 치명적인 오류에 관한 메시지만 저장한다는 뜻입니다.
   - **진단**은 추적 파일이 경고뿐만 아니라 모든 오류에 관한 메시지를 저장한다는 뜻입니다.
   - **중요**는 추적 파일이 모든 오류, 경고, 추가 정보에 관한 메시지를 저장한다는 뜻입니다.
   - **정밀**은 추적 파일이 애플리케이션의 작동에 관한 모든 정보를 저장한다는 뜻입니다.

   기술 지원 담당자가 잠재적 문제를 해결하는 데 필요한 상세 수준을 결정합니다.
8. 오래된 추적 파일을 삭제하려면 **가장 오래된 추적 파일 제거** 기능을 활성화합니다.
   이 기능이 활성화된 경우 추적 파일의 최대 크기와 개수를 구성합니다:
   a. **추적 파일 최대 크기(MB)** 값을 지정합니다.
      사용 가능한 값: 1~4095MB. 기본값은 100MB입니다.
   b. **한 추적 로그의 최대 파일 개수** 값을 지정합니다.
      사용 가능한 값: 1부터 999까지. 기본값은 5입니다.
9. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 애플리케이션 추적을 활성화 및 구성하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 열고 다음 중 하나를 수행합니다:

   - 노드의 결과 창에서 **애플리케이션 속성** 링크를 클릭합니다.
   - 노드의 마우스 오른쪽 메뉴에서 **애플리케이션 속성** 항목을 선택합니다.

   애플리케이션 속성 창이 열립니다.

2. **오작동 진단** 탭을 선택합니다.
3. **오작동 진단 설정** 블록에서 **설정** 버튼을 클릭합니다.
   오작동 진단 설정 창이 열립니다.
4. 추적 설정 탭을 선택합니다.

   - **애플리케이션 추적 설정**. Kaspersky Industrial CyberSecurity for Nodes가 애플리케이션에 대한 추적을 시작합니다.
   - **애플리케이션 콘솔 추적 설정**. 애플리케이션 콘솔과 Kaspersky Industrial CyberSecurity for Nodes가 서로 다른 컴퓨터에 설치된 경우 애플리케이션 콘솔의 추적만 시작할 수 있습니다.

5. **추적 활성화** 확인란을 사용하여 애플리케이션 동작 추적을 활성화하거나 비활성화합니다.
   기본적으로 애플리케이션 동작 추적이 비활성화되었습니다.
6. 필요하다면 Kaspersky Industrial CyberSecurity for Nodes 추적 파일을 저장할 기본 폴더를 변경합니다. 변경하려면 **찾아보기** 버튼을 클릭하고 필요한 폴더를 선택합니다.

   > 폴더는 사전에 생성되어야 하고 SYSTEM 계정으로 작성 가능해야 합니다. 네트워크 폴더, 드라이브, 환경 변수는 지정할 수 없습니다.

   선택한 폴더에서 Kaspersky Industrial CyberSecurity for Nodes는 추적 파일을 저장하기 위해 logs-Kaspersky Industrial CyberSecurity for Nodes-<uid>라는 하위 폴더를 생성합니다. 여기서 <uid>는 8자의 고유 로그 식별자입니다.

7. 디버그 정보의 상세 수준을 선택합니다:

   - **보통**은 추적 파일이 모든 오류, 경고에 관한 메시지는 물론 애플리케이션의 정상 작동에 관한 정보도 저장한다는 뜻입니다(기본값).
   - **심각**은 추적 파일이 치명적인 오류에 관한 메시지만 저장한다는 뜻입니다.
   - **진단**은 추적 파일이 경고뿐만 아니라 모든 오류에 관한 메시지를 저장한다는 뜻입니다.
   - **중요**는 추적 파일이 모든 오류, 경고, 추가 정보에 관한 메시지를 저장한다는 뜻입니다.
   - **자세히**은 추적 파일이 애플리케이션의 작동에 관한 모든 정보를 저장한다는 뜻입니다.

   기술 지원 담당자가 잠재적 문제를 해결하는 데 필요한 상세 수준을 결정합니다.

8. 오래된 추적 파일을 삭제하려면 **가장 오래된 추적 파일 제거** 기능을 활성화합니다.

이 기능이 활성화된 경우 추적 파일의 최대 크기와 개수를 구성합니다:

a. **추적 파일 최대 크기(MB)** 값을 지정합니다.
   사용 가능한 값: 1~4095MB. 기본값은 100MB입니다.

b. **한 추적 로그의 최대 파일 개수** 값을 지정합니다.
   사용 가능한 값: 1부터 999까지. 기본값은 5입니다.

9. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 애플리케이션 추적을 활성화하고 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **오작동 진단** 섹션을 선택합니다.

5. **오작동 진단 설정** 블록에서 **애플리케이션 추적 로그 사용** 확인란으로 애플리케이션 동작 추적을 활성화하거나 비활성화합니다.
   기본적으로 애플리케이션 동작 추적이 비활성화되었습니다.

6. 필요하다면 Kaspersky Industrial CyberSecurity for Nodes 추적 파일을 저장할 기본 폴더를 변경합니다. 변경하려면 **추적 폴더(폴더의 전체 경로, 예: C:\\Traces\\)** 필드에 로컬 폴더의 전체 경로를 지정합니다.

   > 폴더는 사전에 생성되어야 하고 SYSTEM 계정으로 작성 가능해야 합니다. 네트워크 폴더, 드라이브, 환경 변수는 지정할 수 없습니다.

   선택한 폴더에서 Kaspersky Industrial CyberSecurity for Nodes는 추적 파일을 저장하기 위해 logs-Kaspersky Industrial CyberSecurity for Nodes-<uid>라는 하위 폴더를 생성합니다. 여기서 <uid>는 8자의 고유 로그 식별자입니다.

7. 디버그 정보의 상세 수준을 선택합니다:

   - **보통**은 추적 파일이 모든 오류, 경고에 관한 메시지는 물론 애플리케이션의 정상 작동에 관한 정보도 저장한다는 뜻입니다(기본값).
   - **심각**은 추적 파일이 치명적인 오류에 관한 메시지만 저장한다는 뜻입니다.
   - **진단**은 추적 파일이 경고뿐만 아니라 모든 오류에 관한 메시지를 저장한다는 뜻입니다.
   - **중요**는 추적 파일이 모든 오류, 경고, 추가 정보에 관한 메시지를 저장한다는 뜻입니다.
   - **정밀**은 추적 파일이 애플리케이션의 작동에 관한 모든 정보를 저장한다는 뜻입니다.

   기술 지원 담당자가 잠재적 문제를 해결하는 데 필요한 상세 수준을 결정합니다.

8. 오래된 추적 파일을 삭제하려면 **오래된 추적 파일 제거** 기능을 활성화합니다.

이 기능이 활성화된 경우 추적 파일의 최대 크기와 개수를 구성합니다:

a. **추적 파일 최대 크기(MB)** 값을 지정합니다.
사용 가능한 값: 1~4095MB. 기본값은 100MB입니다.

b. **한 추적 로그의 최대 파일 개수** 값을 지정합니다.
사용 가능한 값: 1부터 999까지. 기본값은 5입니다.

9. 변경 사항을 저장합니다.

간편 진단 인터페이스 및 명령줄에서도 애플리케이션 추적을 활성화하고 구성할 수 있습니다.

추적 파일의 내용 및 저장

사용자는 자신의 컴퓨터에 저장된 데이터의 보안에 대해 스스로 책임을 져야 하며, 특히 Kaspersky에 제출될 때까지 데이터에 대한 접근을 모니터링하고 제한해야 합니다.

추적 파일은 애플리케이션이 사용 중일 때는 컴퓨터에 저장되며 애플리케이션이 제거되면 영구적으로 삭제됩니다.

추적 파일은 %ProgramData%\Kaspersky Lab\KICS.5.0\Traces 폴더에 저장됩니다.

추적 파일은 다음 이름 형식을 가집니다: KICS<5.0_dateXX.XX_timeXX.XX_pidXXX.><추적 파일 유형>.log.

추적 파일에 저장된 데이터를 볼 수 있습니다.

모든 추적 파일에는 다음 일반 데이터가 포함됩니다.

- 이벤트 시간
- 실행 스레드 수
- 이벤트를 발생시킨 애플리케이션 구성 요소
- 이벤트의 심각도(정보 이벤트, 경고, 심각 이벤트, 오류)
- 애플리케이션의 구성 요소에 의한 명령 실행 및 이 명령 실행의 결과에 연관된 이벤트 설명

SRV.log, GUI.log, ALL.log 추적 파일 내용

SRV.log, GUI.log, ALL.log 추적 파일은 일반적인 데이터 이외에 다음 정보를 저장할 수도 있습니다.

- 성, 이름 등 개인 데이터(이러한 데이터가 로컬 컴퓨터에서 파일 경로에 포함된 경우).
- 사용자 이름과 암호(공개적으로 전송된 경우). 이 데이터는 인터넷 트래픽 검사 중에 추적 파일에 기록될 수 있습니다.
- 사용자 이름 및 암호(HTTP 헤더에 포함된 경우).

- Microsoft Windows 계정 이름(계정 이름이 파일 이름에 포함된 경우).
- 사용자의 계정 이름과 암호가 포함된 이메일 주소나 웹 주소(이들이 발견된 개체의 이름에 포함된 경우).
- 프록시 서버 주소, 컴퓨터 이름, 포트, IP 주소, 프록시 서버에 로그인할 때 사용되는 사용자 이름. 이 데이터는 애플리케이션이 프록시 서버를 사용하는 경우 추적 파일에 작성됩니다.
- 컴퓨터가 연결을 구축한 원격 IP 주소.
- 네트워크 트래픽 데이터. 이 데이터는 트래픽 모니터링 구성 요소가 활성화된 경우 추적 파일에 작성됩니다.
- Kaspersky 서버로부터 수신된 데이터(예: 안티바이러스 데이터베이스 버전).
- Kaspersky Industrial CyberSecurity for Nodes 구성 요소 및 해당 운영 데이터 상태.
- 애플리케이션의 사용자 활동에 대한 데이터.
- 운영 체제 이벤트.

HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log 추적 파일의 내용

일반 데이터 이외에도 HST.log 추적 파일에는 데이터베이스의 실행 및 애플리케이션 모듈 업데이트 작업에 대한 정보가 포함됩니다.

일반 데이터 이외에도 BL.log 추적 파일에는 애플리케이션의 작동 중에 발생한 이벤트에 대한 정보 및 애플리케이션 오류의 문제 해결에 필요한 데이터가 포함됩니다. 이 파일은 애플리케이션이 avp.exe –bl 파라미터로 시작된 경우에 생성됩니다.

일반 데이터 이외에도 Dumpwriter.log 추적 파일에는 애플리케이션 덤프 파일이 작성될 때 발생하는 오류의 문제 해결에 필요한 서비스 정보가 포함됩니다.

일반 데이터 이외에도 WD.log 추적 파일에는 애플리케이션 모듈 업데이트 이벤트를 비롯한 avpsus 서비스의 작동 중에 발생하는 이벤트에 대한 정보가 포함되어 있습니다.

일반 데이터 이외에도 AVPCon.dll.log 추적 파일에는 Kaspersky Security Center 연결 모듈 작동 중에 발생하는 이벤트에 대한 정보가 포함되어 있습니다.

AMSI 스캐너 구성 요소 추적 파일의 내용

AMSI.log 추적 파일에는 일반 데이터 외에도 타사 애플리케이션의 요청에 대해 수행된 검색 결과에 대한 정보가 포함되어 있습니다.

애플리케이션 웹 플러그인의 추적 파일 내용

애플리케이션 웹 플러그인의 추적 파일은 Kaspersky Security Center 웹 콘솔이 배포된 컴퓨터의 Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs 폴더에 저장됩니다.

애플리케이션 웹 플러그인의 추적 로그 파일 이름은 다음과 같습니다: logs-kics_windows-<추적 파일 유형>.DESKTOP-<파일 업데이트 날짜>.log. 웹 콘솔은 설치 후 데이터 쓰기를 시작하고 웹 콘솔을 제거한 이후에는 추적 파일을 삭제합니다.

애플리케이션 웹 플러그인의 추적 파일에는 일반 데이터 이외에도 다음 정보가 포함되어 있습니다.

- Kaspersky Industrial CyberSecurity for Nodes 인터페이스의 잠금을 해제하기 위한 KLAdmin 사용자 암호.
- Kaspersky Industrial CyberSecurity for Nodes 인터페이스의 잠금을 해제하기 위한 임시 암호.
- SMTP 메일 서버에 대한 사용자 이름 및 암호.
- 프록시 서버에 대한 사용자 이름 및 암호.
- *애플리케이션 구성 요소 변경* 작업에 대한 사용자 이름 및 암호.
- Kaspersky Industrial CyberSecurity for Nodes 작업 및 정책 속성에 지정된 계정 인증 정보 및 경로.

메모리 덤프 기록

메모리 덤프 파일에는 애플리케이션 오작동 당시 Kaspersky Industrial CyberSecurity for Nodes 프로세스의 작동 메모리에 관한 모든 정보가 포함됩니다.

메모리 덤프 파일은 애플리케이션이 사용 중일 때는 컴퓨터에 저장되며 애플리케이션이 제거되면 영구적으로 삭제됩니다.

> 저장된 덤프 파일에는 기밀 데이터가 포함되어 있을 수 있습니다. 데이터에 대한 접근을 제어하려면 메모리 덤프 파일의 보안을 독립적으로 보장해야 합니다.

기본적으로 메모리 덤프 파일은 %ProgramData%\Kaspersky Lab\KICS.5.0\Traces 폴더에 저장됩니다.

Kaspersky Security Center 관리 콘솔에서 메모리 덤프 기록을 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 속성 창에서 **오작동 진단** 섹션으로 갑니다.
4. **오작동 진단 설정** 블록에서 **설정** 버튼을 클릭합니다.
   애플리케이션 추적 설정 탭에서 **오작동 진단 설정** 창이 열립니다.
5. **애플리케이션 덤프 설정** 탭을 선택합니다.
6. **덤프 파일 생성** 확인란을 사용하여 애플리케이션 동작 추적을 활성화하거나 비활성화합니다.
   기본적으로 메모리 덤프 기록이 비활성화되었습니다.

7. 필요하다면 Kaspersky Industrial CyberSecurity for Nodes 추적 파일을 저장할 기본 폴더를 변경합니다. 변경하려면 **덤프 파일 폴더** 필드에 로컬 폴더의 전체 경로를 지정합니다.

   폴더는 사전에 생성되어야 하고 SYSTEM 계정으로 작성 가능해야 합니다. 네트워크 폴더, 드라이브, 환경 변수는 지정할 수 없습니다.

8. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 메모리 덤프 기록을 활성화 또는 비활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 열고 다음 중 하나를 수행합니다:

   - 노드의 결과 창에서 **애플리케이션 속성** 링크를 클릭합니다.
   - 노드의 마우스 오른쪽 메뉴에서 **애플리케이션 속성** 항목을 선택합니다.

   애플리케이션 속성 창이 열립니다.

2. **오작동 진단** 탭을 선택합니다.
3. **오작동 진단 설정** 블록에서 **설정** 버튼을 클릭합니다.
   오작동 진단 설정 창이 열립니다.
4. 덤프 설정 탭을 선택합니다.

   - **애플리케이션 덤프 설정**. Kaspersky Industrial CyberSecurity for Nodes가 애플리케이션의 모든 덤프를 기록합니다.
   - **애플리케이션 콘솔 덤프 설정**. 애플리케이션 콘솔과 Kaspersky Industrial CyberSecurity for Nodes가 서로 다른 컴퓨터에 설치된 경우 애플리케이션 콘솔의 덤프만 기록할 수 있습니다.

5. **덤프 파일 생성** 확인란을 사용하여 애플리케이션 동작 추적을 활성화하거나 비활성화합니다.
   기본적으로 메모리 덤프 기록이 비활성화되었습니다.
6. 필요하다면 Kaspersky Industrial CyberSecurity for Nodes 추적 파일을 저장할 기본 폴더를 변경합니다. 변경하려면 **찾아보기** 버튼을 클릭하고 필요한 폴더를 선택합니다.

   폴더는 사전에 생성되어야 하고 SYSTEM 계정으로 작성 가능해야 합니다. 네트워크 폴더, 드라이브, 환경 변수는 지정할 수 없습니다.

7. 변경 사항을 저장합니다.

Kaspersky Security Center 웹 콘솔에서 메모리 덤프 기록을 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.
2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.

4. **오작동 진단** 섹션을 선택합니다.

5. **덤프 파일 설정** 블록에서 **덤프 파일 생성** 확인란으로 애플리케이션 동작 추적을 활성화하거나 비활성화합니다.
   기본적으로 메모리 덤프 기록이 비활성화되었습니다.

6. 필요하다면 Kaspersky Industrial CyberSecurity for Nodes 추적 파일을 저장할 기본 폴더를 변경합니다. 변경하려면 **덤프 파일 폴더(폴더의 전체 경로, 예: C:\\Dumps\\)** 필드에 로컬 폴더의 전체 경로를 지정합니다.

   > 폴더는 사전에 생성되어야 하고 SYSTEM 계정으로 작성 가능해야 합니다. 네트워크 폴더, 드라이브, 환경 변수는 지정할 수 없습니다.

7. 변경 사항을 저장합니다.

간편 진단 인터페이스에서 메모리 덤프 기록을 활성화 또는 비활성화할 수도 있습니다.

덤프 파일 및 추적 파일 보호

덤프 파일과 추적 파일에는 운영 체제에 관한 정보가 포함되며 사용자 데이터도 포함될 수 있습니다. 그러한 데이터에 무단으로 접근하지 못하게 하기 위해 덤프 파일 및 추적 파일 보호를 작동할 수 있습니다.

덤프 파일 및 추적 파일 보호를 작동한 경우 다음 사용자가 파일에 접근할 수 있습니다:

- 시스템 관리자와 로컬 관리자, 그리고 덤프 파일 및 추적 파일 쓰기가 설정된 사용자가 덤프 파일에 접근할 수 있습니다.
- 시스템 관리자와 로컬 관리자만 추적 파일에 접근할 수 있습니다.

Kaspersky Security Center 관리 콘솔에서 덤프 파일 및 추적 파일 보호를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 옵션을 선택합니다.

2. Kaspersky Industrial CyberSecurity for Nodes 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **오작동 진단** 섹션을 선택합니다.

5. **덤프 및 추적 파일 보호 사용** 확인란을 사용하여 덤프 파일 및 추적 파일 보호를 활성화하거나 비활성화합니다.

6. 변경 사항을 저장합니다.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 속성 창에서 **오작동 진단** 섹션으로 갑니다.

4. **오작동 진단 설정** 블록에서 **설정** 버튼을 클릭합니다.

5. **오작동 진단 설정** 창이 열립니다.

6. **덤프 및 추적 파일 보호 사용** 확인란을 사용하여 덤프 파일 및 추적 파일 보호를 활성화하거나 비활성화합니다.

7. 변경 사항을 저장합니다.

애플리케이션 콘솔에서 덤프 파일 및 추적 파일 보호를 활성화하는 방법

1. 애플리케이션 콘솔 트리에서 **Kaspersky Industrial CyberSecurity for Nodes** 노드를 열고 다음 중 하나를 수행합니다:

   - 노드의 결과 창에서 **애플리케이션 속성** 링크를 클릭합니다.
   - 노드의 마우스 오른쪽 메뉴에서 **애플리케이션 속성** 항목을 선택합니다.

   애플리케이션 속성 창이 열립니다.

2. **오작동 진단** 탭을 선택합니다.

3. **오작동 진단 설정** 블록에서 **설정** 버튼을 클릭합니다.
   오작동 진단 설정 창이 열립니다.

4. **덤프 및 추적 파일 보호 사용** 확인란을 사용하여 덤프 파일 및 추적 파일 보호를 활성화하거나 비활성화합니다.

5. 변경 사항을 저장합니다.

간편 진단 인터페이스에서 덤프 파일 및 추적 파일 보호를 활성화 또는 비활성화할 수도 있습니다.

보호가 활성일 때 쓰여진 덤프 및 추적 파일은 보호 기능이 중지된 후에도 계속 보호됩니다.

OS 데이터 가져오기(Kaspersky Get System Info)

Kaspersky Industrial CyberSecurity for Nodes 애플리케이션을 설치한 후 운영 체제 또는 애플리케이션이 제대로 작동하지 않을 수 있습니다. 애플리케이션과 컴퓨터 구성 요소의 소프트웨어 또는 드라이버 간에 충돌이 있는 것입니다.

Kaspersky 기술 지원에서 문제의 원인을 확인하려면 Kaspersky Get System Info 유틸리티(이하 GSI)의 리포트가 필요합니다. 이 유틸리티를 사용하는 방법에 대한 자세한 내용은 Kaspersky 기술 자료를 참조하십시오.

Kaspersky Industrial CyberSecurity for Nodes에 관한 정보 출처

다음 소스를 사용하여 Kaspersky Industrial CyberSecurity for Nodes에 관한 정보를 찾을 수 있습니다:

- Kaspersky 웹사이트의 Kaspersky Industrial CyberSecurity for Nodes 페이지
- 기술 지원 웹 사이트의 Kaspersky Embedded Systems Security 페이지(기술 자료)
- 온라인 도움말
- 포럼의 애플리케이션에 대해 토론

온라인 정보 소스를 사용하려면 인터넷에 연결해야 합니다.

최신 암호화 프로토콜을 지원하지 않는 브라우저에서는 온라인 도움말을 보지 못할 수 있습니다.

문제에 대한 해결 방법을 찾지 못한 경우 Kaspersky 기술 지원에 문의하십시오.

Kaspersky 웹사이트의 Kaspersky Industrial CyberSecurity for Nodes 페이지

Kaspersky Industrial CyberSecurity for Nodes 페이지에서 애플리케이션과 그 기능, 특징과 같은 일반적인 정보를 확인할 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 페이지에는 온라인 스토어로의 링크를 포함하고 있습니다. 여기에서 애플리케이션을 구입하거나 라이센스를 갱신할 수 있습니다.

기술 지원 기술 자료 웹사이트의 Kaspersky Industrial CyberSecurity for Nodes 페이지

기술 자료는 기술 지원 웹사이트의 한 섹션입니다.

기술 자료의 Kaspersky Industrial CyberSecurity for Nodes 페이지에서는 애플리케이션의 구매와 설치, 사용에 관한 유용한 정보와 권장 사항, 자주 하는 질문에 대한 답변을 확인할 수 있습니다.

기술 자료 문서에는 Kaspersky Industrial CyberSecurity for Nodes뿐만 아니라 다른 Kaspersky 애플리케이션에 관련된 질문에 대한 답변이 있습니다. 기술 지원 관련 뉴스도 포함될 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes 도움말

온라인 도움말은 Kaspersky Industrial CyberSecurity for Nodes의 구성 및 사용에 관한 정보를 포함합니다.

포럼의 애플리케이션에 대해 토론

긴급하게 답변이 필요한 것이 아니라면 Kaspersky 전문가 또는 포럼 사용자와 해당 질문에 대해 토론할 수 있습니다.

포럼에서는 이미 게시된 주제를 보고, 의견을 남기고, 새 논제를 작성할 수 있습니다.

부록

이 섹션에는 문서의 본문을 보완하는 정보가 포함되어 있습니다.

빠른 검사를 위한 파일 확장자

com - 64KB보다 크지 않은 애플리케이션 실행 파일

exe - 실행 파일 또는 자동으로 압축이 해제되는 압축파일

sys - Microsoft Windows 시스템 파일

prg - dBase™, Clipper 또는 Microsoft Visual FoxPro®용 프로그램 텍스트 또는 WAVmaker 프로그램

bin - 이진 파일

bat - 배치 파일

cmd - Microsoft Windows NT(DOS용 BAT 파일과 유사) 또는 OS/2용 명령 파일

dpl - 압축된 Borland Delphi(볼랜드 델파이) 라이브러리

dll - 동적 링크 라이브러리

scr - Microsoft Windows 시작 화면

cpl - Microsoft Windows 제어판 모듈

ocx - Microsoft OLE(개체 연결 및 포함) 개체

tsp - 스플릿 타임(split-time) 모드에서 실행 중인 프로그램

drv - 장치 드라이버

vxd - Microsoft Windows 가상 장치 드라이버

pif - 프로그램 정보 파일

lnk - Microsoft Windows 링크 파일

reg - Microsoft Windows 시스템 레지스트리 키 파일

ini - Microsoft Windows, Windows NT 및 일부 애플리케이션용 설정 데이터가 포함되어 있는 구성 파일

cla - Java 클래스

vbs - Visual Basic® 스크립트

vbe - BIOS 비디오 확장자

js, jse - JavaScript 소스 텍스트

htm - 하이퍼텍스트 문서

htt - Microsoft Windows 하이퍼텍스트 헤더

hta - Microsoft Internet Explorer용 하이퍼텍스트 프로그램®

asp - Active Server Pages 스크립트

chm - 컴파일된 HTML 파일

pht - PHP 스크립트와 통합된 HTML 파일

php - HTML 파일과 통합된 스크립트

wsh - Microsoft Windows 스크립트 호스트 파일

wsf - Microsoft Windows 스크립트

the - Microsoft Windows 95 데스크톱 배경 무늬 파일

hlp - Win 도움말 파일

msg - Microsoft Mail 이메일 메시지

plg - 이메일 메시지

mbx – 저장된 Microsoft Office Outlook 이메일 메시지

dot* - Microsoft Office Word 문서(예: dot - Microsoft Office Word 문서, dotx - XML을 지원하는 Microsoft Office Word 2007 문서, dotm - 매크로 지원이 포함된 Microsoft Office Word 2007 문서)

dot* - Microsoft Office Word 문서 템플릿(예: dot - Microsoft Office Word 문서 템플릿, dotx - Microsoft Office Word 2007 문서 템플릿, dotm - 매크로 지원이 포함된 Microsoft Office Word 2007 문서 템플릿)

fpm - 데이터베이스 프로그램, Microsoft Visual FoxPro 시작 파일

rtf - 서식 있는 텍스트 문서

shs - 셸 스크랩 개체 핸들러(Shell Scrap Object Handler) 조각

dwg - AutoCAD® 드로잉 데이터베이스

msi - Microsoft Windows Installer 패키지

otm - Microsoft Office Outlook용 VBA 프로젝트

pdf - Adobe Acrobat 문서

swf - Shockwave® Flash 패킷 개체

jpg, jpeg - 압축된 이미지 그래픽 형식

emf - 확장 메타파일 형식(EMF) 파일

ico - 개체 아이콘 파일

ov? – Microsoft Office Word 실행 파일

xl* – Microsoft Office Excel 문서 및 파일, 예: xla - Microsoft Office Excel 확장자, xlc - 다이어그램, xlt - 문서 템플릿, xlsx - Microsoft Office Excel 2007 통합 문서, xltm - 매크로 지원이 포함된 Microsoft Office Excel 2007 통합 문서, xlsb - 이진(XML 아님) 형식의 Microsoft Office Excel 2007 통합 문서, xltx - Microsoft Office Excel 2007 템플릿, xlsm - 매크로 지원이 포함된 Microsoft Office Excel 2007 템플릿, xlam - 매크로 지원이 포함된 Microsoft Office Excel 2007 플러그인

pp* – Microsoft Office PowerPoint® 문서 및 파일, 예:pps - Microsoft Office PowerPoint 슬라이드, ppt - 프레젠테이션, pptx - Microsoft Office PowerPoint 2007 프레젠테이션, pptm - 매크로 지원이 포함된 Microsoft Office PowerPoint 2007 프레젠테이션, potx - Microsoft Office PowerPoint 2007 프레젠테이션 템플릿, potm - 매크로 지원이 포함된 Microsoft Office PowerPoint 2007 프레젠테이션 템플릿, ppsx - Microsoft Office PowerPoint 2007 슬라이드쇼, ppsm - 매크로 지원이 포함된 Microsoft Office PowerPoint 2007 슬라이드쇼, ppam - 매크로 지원이 포함된 Microsoft Office PowerPoint 2007 플러그인

md* – Microsoft Office Access® 문서 파일, 예: Microsoft Office Access 워크 그룹용 mda 및 데이터베이스용 mdb

sldx - Microsoft PowerPoint 2007 슬라이드

sldm - 매크로 지원이 포함된 Microsoft PowerPoint 2007 슬라이드

thmx – Microsoft Office 2007 테마

애플리케이션 구성 요소 규칙의 사용자 계정

일부 애플리케이션 구성 요소를 구성하려면 애플리케이션에서 규칙을 적용할 사용자를 선택할 수 있는 특수 규칙을 추가해야 합니다.

다음 애플리케이션 구성 요소를 구성하려면 규칙을 추가해야 합니다.

- 애플리케이션 실행 제어
- 장치 제어
- Anti-Cryptor
- 시스템 무결성 모니터링

다음과 같은 방법으로 사용자를 추가할 수 있습니다.

- Active Directory에서 선택(권장)
- Kaspersky Security Center 사용자 목록에서 선택
- 직접 추가

Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다. 로컬 계정 사용 시의 보안 위험에 관한 자세한 내용은 Microsoft 기술 자료를 참조하십시오. 로컬 사용자 계정을 사용하는 경우 컴퓨터 보안에 대한 모든 책임은 사용자에게 있습니다. 특히 여기에는 애플리케이션 설정에 대한 접근을 제어하고 제한하는 책임이 포함됩니다.

애플리케이션은 사용자의 SID(보안 식별자)를 사용하여 사용자를 식별합니다. Active Directory 또는 Kaspersky Security Center 사용자 목록의 사용자 계정을 사용할 때 애플리케이션이 중앙 관리 서버의 SID를 결정합니다. 즉, 애플리케이션이 사용자 식별을 위해 컴퓨터에 추가 로드를 가하지 않습니다. 애플리케이션 규칙에 1000개 이상의 로컬 사용자 계정을 추가했다면 애플리케이션이 도메인 컨트롤러에 접속하여 사용자를 식별합니다. 즉, 컴퓨터의 로드가 증가합니다. 컴퓨터에 미치는 성능 영향을 최적화하려면 Active Directory 또는 Kaspersky Security Center 사용자 목록의 사용자 계정을 사용하는 것이 좋습니다.

Kaspersky Industrial CyberSecurity for Nodes는 규칙에 포함된 사용자 및 그룹 계정(예: "Everyone" 그룹)을 지원합니다. 사용자 SID 탐지의 특성에 따라, 애플리케이션이 Active Directory 또는 Kaspersky Security Center 사용자 목록에서 추가된 내장 계정의 사용만 허용합니다. 내장 계정을 직접 추가하는 규칙이 작동하지 않습니다.

법률 정보

데이터 제공

이 섹션에는 Kaspersky Industrial CyberSecurity for Nodes 애플리케이션이 장치에 저장하고 작동 중 Kaspersky에 자동으로 전송할 수 있는 데이터에 대한 정보가 포함되어 있습니다.

Kaspersky에 제공된 정보는 법률 및 요건, Kaspersky의 해당 규정에 따라 보호됩니다. 데이터는 암호화된 통신 채널을 통해 전송됩니다.

최종 사용자 라이센스 계약서에 따른 데이터 프로비전

최종 사용자 라이센스 계약서의 조항에 동의하면 Kaspersky에 다음 정보를 자동으로 전송하는 데 동의하게 됩니다:

- 업데이트 수신 메커니즘 지원 목적: 설치된 애플리케이션 및 라이센스 인증서의 정보: 설치 중인 애플리케이션 및 정식 버전의 식별자(빌드 번호, 유형, 라이센스 식별자, 설치 식별자, 고유 업데이트 작업 식별자 포함).
- 데이터 처리 확인 관리 목적: 데이터 전송 조건을 규정하는 라이센스 계약서 및 기타 문서의 수락 상태 정보: 데이터 처리 조건을 수락하거나 거부하는 기타 문서 또는 라이센스 계약서의 식별자 및 버전, 사용자의 처리를 나타내는 속성(약관 동의에 관한 확인 또는 상기), 데이터 처리 약관 동의의 상태 변경 날짜 및 시간.
- 활성화 코드로 애플리케이션 활성화 목적: 설치된 애플리케이션의 유형과 버전, 현지화, 설치된 업데이트의 버전, 보호 중인 장치의 식별자 및 보호 중인 장치에 설치된 애플리케이션의 식별자, 활성화 코드 및 현재 라이센스의 고유 식별자, 운영 체제의 유형과 버전, 단어 크기, 가상 환경에 애플리케이션이 설치될 시의 가상 환경의 이름, 정보가 제공된 시점에 활성화된 애플리케이션 구성 요소의 식별자 정보.

사용자가 애플리케이션 사용 시 Kaspersky 수신하는 데이터는 법률 및 현재 Kaspersky 규칙이 설정한 요구 사항에 따라 보호되고 처리됩니다. 데이터는 암호화된 통신 채널을 통해 전송됩니다. 애플리케이션 사용 중에 획득하여 Kaspersky로 전송된 정보의 처리와 저장, 파기에 관한 자세한 내용은 www.kaspersky.com/Products-and-Services-Privacy-Policy 의 개인정보취급방침을 참조하십시오.

로컬 데이터 처리

이 가이드에 설명된 애플리케이션의 기본 기능을 실행하는 동안 Kaspersky Industrial CyberSecurity for Nodes는 보호 중인 장치에서 일련의 데이터를 로컬로 처리하고 저장합니다.

아래 표에는 리포트에 포함된 Kaspersky Industrial CyberSecurity for Nodes의 로컬 데이터 처리 및 저장 정보가 포함되어 있습니다.

기능 영역	감사.
사용 유형	Kaspersky Industrial CyberSecurity for Nodes는 데이터를 로컬에 저장했다가 중앙 관리 서버로 전송합니다. 중앙 관리 서버 데이터베이스에는 관리되는 보호 중인 장치에서 발생하는 애플리케이션 이벤트에 관한 정보가 저장됩니다.
스토리지	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<제품 버전>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • 중앙 관리 서버의 데이터베이스
보안 조치	접근 제어 목록.
보관 기간	Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Industrial CyberSecurity for Nodes를 제거할 때까지 데이터를 저장합니다. Kaspersky Industrial CyberSecurity for Nodes를 제거하는 동안 Kaspersky Industrial CyberSecurity for Nodes가 보호 중인 장치에 저장한 모든 데이터가 삭제됩니다.
용도	기본 기능을 제공합니다.

Kaspersky Industrial CyberSecurity for Nodes는 Windows 이벤트 로그에서 이벤트를 삭제하지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes는 다음 데이터를 로컬로 처리하고 리포트에 저장합니다:

- 처리된 파일의 이름 및 속성과 검사된 미디어에서 해당 파일의 전체 경로.
- Kaspersky Industrial CyberSecurity for Nodes에서 검사된 파일에 수행된 조치.
- 보호 중인 장치의 검사된 파일에 수행된 사용자 조치.
- 보호 중인 네트워크 또는 보호 중인 장치에서 조치를 수행하는 사용자 계정 정보.
- 장치 제어 규칙에 추가된 장치의 장치 인스턴스 경로 값.
- 시스템에서 실행 중인 프로세스 및 스크립트 정보: 체크섬(MD5, SHA-256) 및 실행 파일의 전체 경로, 디지털 인증서 정보.
- Windows 방화벽 설정.
- Windows 이벤트 로그 항목.
- 보호 중인 장치에서 검사된 파일에 조치를 수행하는 사용자 계정의 이름.
- 시작되는 실행 파일의 인스턴스와 이러한 파일의 유형, 이름, 체크섬, 속성.
- 네트워크 활동 정보: 차단된 외부 장치의 IP 주소, 보호 중인 공유 리소스에 대한 접근이 수행된 유출된 로그인 세션의 식별자.
- 보호 중인 장치가 연결되는 Wi-Fi 네트워크 정보: 네트워크 이름 및 네트워크 식별자.
- PLC 연결 설정(IP, 랙 및 슬롯 번호, 암호), 펌웨어 체크섬을 포함하여 보호 범위에 추가되는 PLC 프로젝트 정보.
- Windows USN 저널 상태 정보.

아래 표에는 사용자가 지정한 파라미터에 관한 데이터에 대한 Kaspersky Industrial CyberSecurity for Nodes의 로컬 처리 및 저장 정보가 포함되어 있습니다.

Kaspersky Industrial CyberSecurity for Nodes는 사용자가 지정한 파라미터의 데이터만 처리하고 저장합니다.

사용자가 지정한 파라미터에 관한 데이터 처리 및 저장

기능 영역	자동 복원, Sandbox 통합.
사용 유형	Kaspersky Industrial CyberSecurity for Nodes는 파라미터에 관한 데이터를 로컬에 저장했다가 중앙 관리 서버로 전송합니다. 중앙 관리 서버의 데이터베이스에는 관리되는 보호 중인 장치의 파라미터에 관한 정보가 저장됩니다.
스토리지	%ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<제품 버전>\
보안 조치	접근 제어 목록.
보관 기간	Kaspersky Industrial CyberSecurity for Nodes는 Kaspersky Industrial CyberSecurity for Nodes를 제거할 때까지 데이터를 저장합니다. Kaspersky Industrial CyberSecurity for Nodes를 제거하는 동안 Kaspersky Industrial CyberSecurity for Nodes가 보호 중인 장치에 저장한 모든 데이터가 삭제됩니다.
용도	기본 기능을 제공합니다.

Kaspersky Industrial CyberSecurity for Nodes는 구성 파일로 내보낸 파라미터에 관한 데이터를 삭제하지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes는 설치 마법사에서 **격리된 개체 내보내기** 그리고 **백업 개체 내보내기** 확인란이 선택된 경우 격리 저장소 개체 및 백업 개체를 삭제하지 않습니다.

Kaspersky Industrial CyberSecurity for Nodes는 사용자가 지정한 파라미터에 관해 다음 데이터를 로컬로 처리 및 저장합니다:

- 격리 저장소 또는 백업 저장소에 저장된 개체 정보.
- 애플리케이션 콘솔 또는 관리 플러그인을 통해 구성된 설정 정보는 예를 들어 다음과 같습니다:
  - Kaspersky Industrial CyberSecurity for Nodes 암호, Kaspersky Industrial CyberSecurity for Nodes 작업이 실행되는 사용자 계정의 이름.
  - 프록시 서버 인증에 사용되는 사용자 계정의 이름.
  - 사용자 정의 업데이트 경로로 사용되는 HTTP 또는 FTP 서버의 폴더 또는 네트워크 폴더 주소.
  - Wi-Fi 네트워크 정보.
  - PLC 연결 설정 및 펌웨어 체크섬을 포함하여 보호 범위에 추가되는 PLC 프로젝트 정보.
  - 차단된 로그인 세션의 IP 주소 및 식별자.
  - Windows 방화벽 설정.
  - 애플리케이션 실행 제어 작업 규칙에 추가된 체크섬(MD5, SHA-256) 및 실행 파일 경로.
  - 장치 제어 규칙에 추가된 장치의 장치 인스턴스 경로 값.

- Kaspersky Industrial CyberSecurity for Nodes 작업의 범위에 포함된 폴더 정보.
- Windows 이벤트 로그의 이벤트 정보.
- iSwift 또는 iChecker 기술을 사용하여 탐지된 파일 정보.
- 체크섬(MD5, SHA-256) 및 신뢰 구역에 추가된 파일의 경로.
- 추가된 라이센스 키 정보.
- 디지털 인증서 정보.
- 파일의 체크섬, 디지털 인증서 데이터, 파일에 대한 전체 경로(SDC 데이터베이스, 베이스라인 파일 무결성 모니터 작업용 파일).
- 애플리케이션이 압축 파일 검사 시 생성되는 임시 파일.
- %SystemRoot% 정보.

- Kaspersky Industrial CyberSecurity for Nodes에서 처리된 파일에 관한 데이터(예: 파일의 체크섬(MD5, SHA-256), 디지털 인증서 정보, 파일의 전체 경로).

Kaspersky Industrial CyberSecurity for Nodes는 애플리케이션 이벤트 기록 및 진단 데이터 수신을 포함하여 애플리케이션의 기본 기능의 일부로 데이터를 처리하고 저장합니다. 로컬에서 처리된 데이터는 구성 및 적용된 애플리케이션 설정에 따라 처리되고 보호됩니다.

Kaspersky Industrial CyberSecurity for Nodes를 사용하면 로컬에서 처리되는 데이터에 대한 보호 수준을 구성할 수 있습니다. 프로세스 데이터에 접근하기 위한 사용자 권한 변경, 해당 데이터의 데이터 저장 기간 변경, 데이터 기록과 관련된 기능의 전체 또는 일부 비활성화, 데이터가 기록되는 드라이브 내 폴더의 속성 및 경로 변경 등의 작업을 수행할 수 있습니다.

데이터 처리와 관련된 애플리케이션 기능 구성에 관한 자세한 내용은 이 가이드의 해당 섹션을 참조하십시오.

애플리케이션 보조 구성 요소를 통한 로컬 데이터 처리

Kaspersky Industrial CyberSecurity for Nodes 설치 패키지는 애플리케이션 보조 구성 요소로 구성되며, 이 구성 요소는 Kaspersky Industrial CyberSecurity for Nodes가 설치되어 있지 않은 장치에도 설치할 수 있습니다.

이 가이드에 설명된 애플리케이션의 주요 기능을 수행하는 동안 애플리케이션 보조 구성 요소는 Kaspersky Industrial CyberSecurity for Nodes와 별도로 설치되었더라도 애플리케이션 보조 구성 요소가 설치된 보호 중인 장치에서 로컬로 데이터 집합을 처리하고 저장합니다.

아래 표에는 덤프 및 추적 파일에 작성된 데이터에 대한 Kaspersky Industrial CyberSecurity for Nodes의 로컬 처리 및 저장 정보가 포함되어 있습니다.

기본적으로 Kaspersky Industrial CyberSecurity for Nodes는 덤프 및 추적 파일을 작성하지 않습니다.

덤프 및 추적 파일에 작성된 데이터의 처리 및 저장

스토리지	기본적으로 덤프 및 추적 파일이 저장되는 폴더는 지정되지 않습니다. 폴더는 지정할 수 있습니다
보안 조치	Kaspersky Industrial CyberSecurity for Nodes는 덤프 및 추적 파일에 대한 접근을 제한하지 않습니다.

보관 기간	Kaspersky Industrial CyberSecurity for Nodes는 덤프 및 추적 파일을 삭제하지 않습니다.
용도	기술 지원 제공.

Kaspersky Industrial CyberSecurity for Nodes는 덤프 및 추적 파일에 작성된 다음 데이터를 로컬로 처리 및 저장합니다:

- Kaspersky Industrial CyberSecurity for Nodes가 보호 중인 장치에서 수행한 처리 정보.
- Kaspersky Industrial CyberSecurity for Nodes에서 처리한 개체 정보.
- Kaspersky Industrial CyberSecurity for Nodes 실행 동안 발생한 오류 정보.

보조 구성 요소에서 처리한 데이터는 Kaspersky 또는 기타 타사 시스템으로 자동 전송되지 않습니다.

기본적으로 작동 중 애플리케이션 보조 구성 요소에서 로컬로 처리한 모든 데이터는 해당 구성 요소 제거 후 삭제됩니다.

보조 애플리케이션 구성 요소의 추적 파일은 예외입니다. 이러한 파일을 직접 삭제하는 것이 좋습니다.

애플리케이션 보조 구성 요소의 진단 데이터가 포함된 파일 작업에 관한 자세한 내용은 이 가이드의 해당 섹션을 참조하십시오.

Detection and Response 솔루션 사용 시 데이터 제공

Kaspersky Industrial CyberSecurity for Nodes 설치된 컴퓨터에는 Detection and Response 솔루션 서버로 자동 전송되도록 준비된 데이터가 축적됩니다. 파일은 일반적이고 암호화되지 않은 형태로 저장됩니다.

구체적인 데이터 세트는 Kaspersky Industrial CyberSecurity Endpoint Detection and Response가 어떤 솔루션과 함께 사용되는지에 따라 달라집니다.

Kaspersky Industrial CyberSecurity Endpoint Detection and Response

Kaspersky Industrial CyberSecurity for Nodes가 제거되면 애플리케이션이 컴퓨터에 로컬로 저장한 모든 데이터가 삭제됩니다.

IOC 검사 작업 예외의 결과로 수신된 데이터(표준 작업)

Kaspersky Industrial CyberSecurity for Nodes는 *IOC 검사* 작업 실행 결과 데이터를 Kaspersky Security Center에 자동으로 제출합니다.

IOC 검사 작업 실행 결과의 데이터에는 다음 정보가 포함될 수 있습니다.

- ARP 테이블의 IP 주소
- ARP 테이블의 물리적 주소

- DNS 레코드 유형 및 이름
- 보호 대상 컴퓨터의 IP 주소
- 보호 대상 컴퓨터의 물리적 주소(MAC 주소)
- 이벤트 로그 항목 내 식별자
- 로그에 있는 데이터 소스 이름
- 로그 이름
- 이벤트 시간
- 파일의 MD5 및 SHA256 해시
- 파일의 전체 이름(경로 포함)
- 파일 크기
- 검사 중에 연결이 설정된 원격 IP 주소 및 포트
- 로컬 어댑터 IP 주소
- 로컬 어댑터에서 열린 포트
- 숫자로서의 프로토콜(IANA 표준에 따름)
- 프로세스 이름
- 프로세스 인수
- 프로세스 파일 경로
- 프로세스의 Windows 식별자(PID)
- 부모 프로세스의 Windows 식별자(PID)
- 프로세스가 시작된 사용자 계정
- 프로세스가 시작된 날짜 및 시간
- 서비스 이름
- 서비스 설명
- DLL 서비스의 경로 및 이름(svchost용)
- 서비스 실행 파일의 경로 및 이름
- 서비스의 Windows 식별자(PID)
- 서비스 유형(예: 커널 드라이버 또는 어댑터)
- 서비스 상태

- 서비스 시작 모드
- 사용자 계정 이름.
- 볼륨 이름
- 볼륨 문자
- 볼륨 유형
- Windows 레지스트리 값
- 레지스트리 하이브 값
- 레지스트리 키 경로(하이브 및 값 이름 없음)
- 레지스트리 설정
- 시스템(환경)
- 컴퓨터에 설치된 운영 체제 이름 및 버전
- 보호 대상 컴퓨터의 네트워크 이름
- 보호 대상 컴퓨터가 속한 도메인 또는 그룹
- 브라우저 이름
- 브라우저 버전
- 웹 리소스에 마지막으로 액세스한 시간
- HTTP 요청의 URL
- HTTP 요청에 사용하는 계정의 이름
- HTTP 요청을 수행한 프로세스의 파일 이름
- HTTP 요청을 수행한 프로세스 파일의 전체 경로
- HTTP 요청을 수행한 프로세스의 Windows 식별자(PID)
- HTTP 리퍼러(HTTP 요청 소스 URL)
- HTTP를 통해 요청된 리소스의 URI
- HTTP 사용자 에이전트(HTTP 요청을 수행한 애플리케이션) 관련 정보
- HTTP 요청 실행 시간
- HTTP 쿼리를 수행한 프로세스의 고유 식별자

보안 위협 개발 체인 생성용 데이터

보안 위협 개발 체인 생성용 데이터는 기본적으로 7일 동안 저장됩니다. 데이터는 Kaspersky Security Center로 자동 전송됩니다.

보안 위협 개발 체인 생성용 데이터에는 다음 정보가 포함될 수 있습니다.

- 사건 날짜 및 시간
- 탐지 이름
- 검사 모드
- 탐지와 관련된 마지막 조치의 상태
- 탐지 처리가 실패한 이유
- 탐지된 개체 유형
- 탐지된 개체 이름
- 개체 처리 후 보안 위협 상태
- 개체에 대한 작업 실행이 실패한 이유
- 악의적인 작업을 롤백하기 위해 수행되는 작업
- 처리된 개체 관련 정보:
  - 프로세스의 고유 식별자
  - 부모 프로세스의 고유 식별자
  - 프로세스 파일의 고유 식별자
  - Windows 프로세스 식별자(PID)
  - 프로세스 명령줄
  - 프로세스가 시작된 사용자 계정
  - 프로세스가 실행 중인 로그온 세션의 코드
  - 프로세스가 실행 중인 세션 유형
  - 처리 중인 프로세스의 통합 레벨
  - 권한 있는 로컬 및 도메인 그룹에서 프로세스를 시작한 사용자 계정의 멤버십
  - 처리된 개체의 식별자
  - 처리된 개체의 전체 이름

- 보호 대상 장치의 식별자
- 개체의 전체 이름(로컬 파일 이름 또는 다운로드한 파일 웹 주소)
- 처리된 개체의 MD5 또는 SHA256 해시
- 처리된 개체의 유형
- 처리된 개체를 만든 날짜
- 처리된 객체가 마지막으로 수정된 날짜
- 처리된 개체의 크기
- 처리된 객체의 특성
- 처리된 개체를 서명한 조직
- 처리된 개체 전자 인증서 검증 결과
- 처리된 개체의 보안 식별자(SID)
- 처리된 개체의 시간대 식별자
- 처리된 개체 다운로드의 웹 주소(디스크에 있는 파일만 해당)
- 파일을 다운로드한 애플리케이션의 이름
- 파일을 다운로드한 애플리케이션의 MD5 및 SHA256 해시
- 파일을 마지막으로 수정한 애플리케이션의 이름
- 파일을 마지막으로 수정한 애플리케이션의 MD5 및 SHA256 해시
- 처리된 개체 시작 수
- 처리된 개체가 처음 시작된 날짜 및 시간
- 파일의 고유 식별자
- 파일의 전체 이름(로컬 파일 이름 또는 다운로드한 파일 웹 주소)
- 처리된 Windows 레지스트리 변수의 경로
- 처리된 Windows 레지스트리 변수의 이름
- 처리된 Windows 레지스트리 변수의 값
- 처리된 Windows 레지스트리 변수의 유형
- 자동 실행 포인트에 있는 처리된 레지스트리 키 멤버십의 표시기
- 처리된 웹 요청의 웹 주소
- 처리된 웹 요청의 링크 소스

- 처리된 웹 요청의 사용자 에이전트
- 처리된 웹 요청 유형(GET 또는 POST)
- 처리된 웹 요청의 로컬 IP 포트
- 처리된 웹 요청의 원격 IP 포트
- 처리된 웹 요청의 연결 방향(인바운드 또는 아웃바운드)
- 악성 코드가 포함된 프로세스의 식별자

Kaspersky Endpoint Detection and Response Expert(on-premises)

Kaspersky Industrial CyberSecurity for Nodes가 제거되면 애플리케이션이 컴퓨터에 로컬로 저장한 모든 데이터가 삭제됩니다.

서비스 데이터

Kaspersky Industrial CyberSecurity for Nodes의 내장 에이전트는 다음의 데이터를 로컬로 저장합니다.

- EDR Expert(on-premises) 구성 요소와의 통합에 필요한 데이터:
  - KATA Central Node 서버 연결 주소 및 포트
  - 원격 측정 전송 서버 연결 주소 및 포트
  - 응답 서버 연결 주소 및 포트
  - KATA Central Node와의 통합에 사용된 인증서 관련 정보
  - 원격 측정 전송 서버와의 통합에 사용된 인증서 관련 정보
  - 응답 서버와의 통합에 사용된 인증서 관련 정보
- 격리된 파일

전송된 원격 측정 이벤트의 데이터

- **원격 측정 데이터**
  - 파일 데이터:
    - 파일의 고유 식별자
    - 파일 유형

    - 전체 파일 경로
    - 파일 크기
    - 파일 특성
    - 영역 ID
    - 파일이 생성된 날짜 및 시간
    - 파일이 마지막으로 수정된 날짜 및 시간
    - 원본 파일 이름
    - 애플리케이션 이름
    - 애플리케이션 버전
    - 애플리케이션 공급업체
    - 파일 설명
    - 파일 버전
    - 개체의 MD5 및 SHA256 해시
    - 파일 서명 확인 결과
    - 인증서 발급자 이름
    - 인증서 보유자 이름
    - 인증서 일련 번호
- AMSI 검사 관련 데이터:
    - 활동을 시작한 프로세스의 고유 식별자
    - AMSI로 전달된 개체의 컨텐츠 유형
    - AMSI로 전달된 개체의 컨텐츠
    - 개체 이름
    - 개체의 MD5 및 SHA256 해시
- 애플리케이션 차단 관련 데이터:
    - 애플리케이션 차단을 시작한 프로세스의 고유 식별자
    - 부모 프로세스의 고유 식별자
    - 프로세스의 고유 시스템 식별자
    - 프로세스를 시작하는 데 사용된 명령

    - 로그인 세션 ID
    - 프로세스 통합 레벨
    - 프로세스 상태
    - 프로세스 파일의 고유 식별자
    - 프로세스 명령줄
    - 해석된 파일의 고유 식별자 목록
- 차단된 파일 열기 관련 데이터:
    - 파일 열기를 시작한 프로세스의 고유 식별자
    - 파일의 고유 식별자
- 드라이버 로딩 관련 데이터:
    - 로드한 드라이버의 고유 식별자
- 이벤트 관련 데이터:
    - 이벤트의 고유 식별자
    - 이벤트 날짜 및 시간
- 파일 수정 관련 데이터:
    - 파일 수정을 시작한 프로세스의 고유 식별자
    - 파일의 고유 식별자
    - 수정 작업 유형
    - 컴퓨터를 다시 시작한 후 파일이 삭제됨을 나타내는 플래그
    - 수정된 파일의 고유 식별자
    - 수정 전 파일의 고유 식별자
    - 파일 열기 방법을 결정하는 비트 플래그 집합
    - 접근 제어 목록의 동작에 대한 데이터
    - 파일의 소유권 또는 부모 그룹의 변경 사항 관련 데이터
- 로그인 세션 데이터:
    - 로그인 세션 ID
    - 로그인한 사용자의 사용자 이름

    - 사용자 계정 유형
    - 세션 유형
- 네트워크 연결 데이터:
    - 연결을 시작한 프로세스의 고유 식별자
    - 연결을 시작하는 데 사용된 로컬 IP 주소
    - 연결 엔드포인트의 원격 IP 주소
    - 연결 방향
    - 데이터 전송 프로토콜
    - HTTP 메소드
    - 호스트 이름이 없는 경로
    - 호스트 이름
    - 연결 시 동적 프로세스 상태
    - 연결이 원시 소켓 레벨에서 열려 있음을 나타내는 플래그
    - 연결 세션에 사용된 TLS 버전
    - TLS 서버 이름
    - TLS 서버 인증서의 MD5 및 SHA1 해시
    - 인증서의 주체 대체 이름(SAN) 목록
    - TLS 인증서 발급자 이름
    - 인증서 일련 번호
    - 사용된 암호화 알고리즘
    - 인증서의 시작 날짜와 종료 날짜
    - TLS 클라이언트의 JA3 지문
    - 서버의 JA3S 지문
- 네트워크 포트에서 수신 중 캡처된 데이터:
    - 연결을 시작한 프로세스의 고유 식별자

- 명령줄 입력 데이터:
  - 콘솔 입력을 시작한 프로세스의 고유 식별자
  - 콘솔 입력 유형
  - 사용자 또는 프로세스가 입력한 텍스트
- 프로세스 생성 관련 데이터:
  - 프로세스의 고유 식별자
  - 부모 프로세스의 고유 식별자
  - 프로세스의 고유 시스템 식별자
  - 프로세스를 시작하는 데 사용된 명령
  - 로그인 세션 ID
  - 프로세스 통합 레벨
  - 프로세스 파일의 고유 식별자
  - 해석된 파일의 고유 식별자 목록
  - 프로세스 유형
- 프로세스에서 로드한 모듈 관련 데이터:
  - 다운로드를 시작한 프로세스의 고유 식별자
  - 프로세스에 업로드된 파일의 전체 경로
  - 모듈 파일의 고유 식별자
  - .NET 어셈블리의 정규화된 전체 이름(로드된 파일이 .NET 모듈인 경우)
  - 매니페스트에 정의된 .NET 어셈블리의 플래그
- 프로세스 종료 데이터:
  - 종료된 프로세스 고유 식별자
- 레지스트리 수정 관련 데이터:
  - 레지스트리 수정을 시작한 프로세스의 고유 식별자
  - 레지스트리 동작 유형
  - 레지스트리 키의 전체 경로
  - 레지스트리 키에 있는 값의 이름
  - 레지스트리 키 값에 저장된 데이터 유형

    - 레지스트리 키 값에 지정된 데이터
    - 이름을 바꾸기 전 키의 이름
    - 키 또는 기본 키 그룹의 소유권 변경에 관한 정보
    - 키의 접근 제어 목록(ACL)에 대한 변경 사항 목록
- 탐지된 위협 및 그 처리 관련 데이터:
    - 위협 탐지가 백그라운드에서 실행되었음을 나타내는 플래그
    - 위협 평결
    - 판정 이름
    - 데이터베이스 레코드의 고유 식별자
    - 위협 레코드가 데이터베이스에 저장된 시간
    - 위협 처리 모드
    - 감염된 개체 유형
    - 감염된 개체 이름
    - 개체의 MD5 및 SHA256 해시
    - 감염된 개체의 고유 식별자
    - 인터넷에서 감염된 개체를 다운로드한 프로세스의 고유 식별자
    - 감염된 개체가 다운로드된 URL
    - 감염된 개체를 전송한 발신자 이메일 주소
    - 감염된 개체를 수신한 네트워크 프로토콜
    - 감염된 개체를 수신한 로컬 주소
    - 감염된 개체가 수신된 외부 주소
    - 개체 콘텐츠 유형
    - 개체 콘텐츠
- 프로세스 접근 관련 데이터:
    - 접근을 시도한 프로세스의 고유 식별자
    - 접근한 대상 프로세스의 고유 식별자
    - 대상 프로세스에서 요청된 권한 집합
    - 작업 유형

    - 프로세스 접근 시점의 호출 집합
    - 소스 프로세스 서술자
    - 대상 프로세스 서술자
- DNS 관련 데이터:
    - DNS 쿼리를 시작한 프로세스의 고유 식별자
    - DNS 서버 IP 주소
    - DNS 쿼리의 동작을 관리하는 플래그
    - 요청 완료 상태
    - DNS 쿼리에 지정된 정규화된 전체 도메인 이름
    - DNS 쿼리의 데이터 유형
    - DNS 서버 응답
- 코드 삽입 관련 데이터:
    - 코드 삽입을 시도한 프로세스의 고유 식별자
    - 사용된 접근 방법
    - 삽입된 코드가 탐지된 시점의 호출 집합
    - 코드가 업로드된 대상 프로세스의 고유 식별자
    - 대상 프로세스의 명령 순서 변경 관련 데이터
    - 대상 프로세스 주소
    - 대상 프로세스에 업로드된 DLL 라이브러리의 이름
    - DDL 파일 전체 경로
- 이름이 지정된 채널을 사용한 작업 관련 데이터:
    - 채널을 만들거나 채널에 연결된 프로세스의 고유 식별자
    - 이름이 지정된 채널의 전체 이름
    - 작업 유형(생성 또는 연결)
- WMI 쿼리 관련 데이터:
    - WMI 작업을 시작한 프로세스의 고유 식별자
    - WMI 작업 유형
    - WMI 쿼리의 대상 장치의 이름

    - WMI 쿼리를 시작한 사용자 계정
    - WMI 쿼리 텍스트
    - WMI 작업이 수행된 네임스페이스
    - WMI 필터 이름
    - 소비자 개체의 이름
    - 소비자 개체의 작업을 설명하는 텍스트
- LDAP 쿼리 관련 데이터:
    - LDAP 쿼리를 수행한 프로세스의 고유 식별자
    - LDAP 쿼리 검색 범위
    - LDAP 필터
    - 쿼리가 전송된 Active Directory 파티션을 지정하는 파라미터
    - LDAP 검색 특성
- 연결된 USB 장치에 대한 데이터:
    - USB 장치 작업 유형
    - USB 장치 유형
    - USB 장치의 식별자
    - USB 장치 이름
    - USB 장치의 경로
    - USB 장치가 시스템 드라이브임을 나타내는 플래그
- 예약된 작업의 생성, 삭제 및 수정 관련 데이터
- 서비스 생성, 삭제 및 수정 관련 데이터
- 파일 시스템의 마운트/마운트 해제 관련 데이터
- EDR Expert 온프레미스 구성 요소의 작동 관련 데이터:
    - 에이전트 시작/중지 관련 정보
    - 에이전트 설치/제거 관련 정보
    - 에이전트 시작의 고유 식별자
    - 에이전트 프로세스의 시스템 식별자
    - 에이전트 프로세스의 고유 식별자

    - 에이전트 종료 이유
    - 에이전트 프로세스 종료 코드
- 이벤트 필터링 설정:
    - 모듈 이름
    - 개체에 대한 전체 경로
    - 개체의 MD5 및 SHA256 해시
    - Windows 이벤트 로그 항목의 식별자
    - 디지털 인증서 설정
    - 트래픽 방향, IP 주소, 포트, 프로토콜, 실행 파일 전체 경로
    - 사용자 이름
    - 사용자 로그온 유형
    - 필터가 적용되는 원격 분석 이벤트 유형

Kaspersky Industrial CyberSecurity for Nodes의 내장 에이전트에 대한 EDR Expert 구성 요소에서 요청된 데이터

- 일반 작업 설정:
    - 작업 유형
    - 작업 스케줄 설정
    - 작업을 실행할 수 있는 계정의 이름과 암호
    - 설정 버전
    - 격리된 개체의 식별자
    - 개체 경로
    - 개체의 MD5 및 SHA256 해시
    - 인수를 이용해 프로세스를 시작하는 명령줄
    - 작업 완료 시 수행되는 추가 작업의 플래그
    - 서버에서 검색할 IOC 파일 식별자
    - IOC 파일
    - 서비스 이름

- 서비스 시작 유형
- *포렌식 가져오기* 작업 결과를 수신해야 하는 폴더
- *포렌식 가져오기* 작업에 대한 개체 이름 및 확장자 마스크

- 네트워크 격리 설정:
  - 설정 유형
  - 설정 버전
  - 네트워크 격리 예외 및 예외 설정 목록: 트래픽 방향, IP 주소, 포트, 프로토콜 및 실행 파일 전체 경로
  - 추가 작업의 플래그
  - 자동 격리 비활성화 시간
- 실행 방지 알림:
  - 설정 유형
  - 설정 버전
  - 실행 방지 규칙 및 규칙 설정 목록: 개체 경로, 개체 유형, 개체의 MD5 및 SHA256 해시
  - 추가 작업의 플래그

Kaspersky Industrial CyberSecurity for Nodes에서 EDR Expert 구성 요소로 전송한 쿼리 데이터

EDR Expert(on-premises) 솔루션과 통합하려면 다음의 데이터가 컴퓨터에 로컬로 저장됩니다.

- 동기화 요청에서:
  - 고유 ID
  - 서버 웹 주소의 기본 부분
  - 컴퓨터 이름
  - 컴퓨터 IP 주소
  - 컴퓨터 MAC 주소
  - 컴퓨터의 현지 시간
  - Kaspersky Industrial CyberSecurity for Nodes 자기 보호 상태
  - 컴퓨터에 설치된 운영 체제 이름 및 버전
  - Kaspersky Industrial CyberSecurity for Nodes 버전

- 애플리케이션 설정 및 작업 설정의 버전
- 작업 상태: 작업 식별자, 실행 상태, 오류 코드

- 서버에서 파일을 얻기 위한 요청에서:
  - 파일의 고유 식별자
  - Kaspersky Industrial CyberSecurity for Nodes 고유 식별자
  - 인증서의 고유 식별자
  - Central Node 구성 요소가 설치된 서버의 웹 주소 기본 부분
  - 호스트 IP 주소
- 작업 실행 결과 리포트에서:
  - 호스트 IP 주소
  - IOC 검사 또는 YARA 검사 중에 감지된 개체 관련 정보
  - 작업 완료 시 수행되는 추가 작업의 플래그
  - 작업 실행 오류 및 반환 코드
  - 작업 완료 상태
  - 작업 완료 시간
  - 작업 실행에 사용하는 설정 버전
  - 서버에 제출된 개체, 격리된 개체 및 격리 저장소에서 복원된 개체 관련: 개체 경로, MD5 및 SHA256 해시, 격리된 개체의 식별자
  - 서버의 요청에 따라 컴퓨터에서 시작되거나 중지된 프로세스 관련 정보: 개체의 PID 및 UniquePID, 오류 코드, MD5 및 SHA256 해시
  - 서버의 요청에 따라 컴퓨터에서 시작되거나 중지된 서비스 관련 정보: 서비스 이름, 시작 유형, 오류 코드, 서비스 파일 이미지의 MD5 및 SHA256 해시
  - YARA 검사를 위해 메모리 덤프가 생성된 개체 관련 정보(경로, 덤프 파일 식별자)
  - 서버에서 요청한 파일
- 실행 중인 프로세스에 대한 데이터:
  - 전체 경로 및 확장자를 포함한 실행 파일 이름
  - 프로세스 자동 실행 매개변수
  - 프로세스 ID
  - 로그인 세션 ID

- 로그인 세션 이름
- 프로세스가 시작된 날짜 및 시간
- 개체의 MD5 및 SHA256 해시

- 파일 데이터:
  - 파일 경로
  - 파일 이름
  - 파일 크기
  - 파일 특성
  - 파일이 생성된 날짜 및 시간
  - 파일이 마지막으로 수정된 날짜 및 시간
  - 파일 설명
  - 회사 이름
  - 개체의 MD5 및 SHA256 해시
  - 레지스트리 키(자동 실행 포인트용)
- 개체 관련 정보를 검색할 때 발생한 오류 데이터:
  - 오류 발생 시 처리된 개체의 전체 이름
  - 오류 코드
- YARA 검사 결과 데이터:

  Kaspersky Industrial CyberSecurity for Nodes의 내장 에이전트는 보안 위협 개발 체인을 구축하기 위해 YARA 검사 결과를 Kaspersky Anti Targeted Attack Platform으로 자동 전송합니다.

  데이터는 작업 실행 결과를 Kaspersky Anti Targeted Attack Platform 서버로 전송하기 위해 대기열에 로컬로 임시로 저장됩니다. 전송된 데이터는 임시 저장소에서 삭제됩니다.

  - 파일의 MD5 및 SHA256 해시
  - 파일의 전체 이름
  - 파일 경로
  - 파일 크기
  - 프로세스 이름
  - 프로세스 인수
  - 프로세스 파일 경로
  - 프로세스의 Windows 식별자(PID)

    - 부모 프로세스의 Windows 식별자(PID)
    - 프로세스가 시작된 사용자 계정
    - 프로세스가 시작된 날짜 및 시간
- IOC 검사 결과 데이터:
    - ARP 테이블의 IP 주소
    - ARP 테이블의 물리적 주소
    - DNS 레코드 이름
    - DNS 레코드 유형
    - 호스트 이름
    - IP 주소
    - 로그에 있는 이벤트 ID
    - 로그에 있는 데이터 소스 이름
    - 로그 이름
    - 사용자 이름
    - 이벤트가 생성된 날짜 및 시간(ISO 형식)
    - 파일의 MD5 및 SHA256 해시
    - 파일의 전체 이름
    - 파일 크기
    - 검사 중에 연결이 설정된 원격 IP 주소 및 포트
    - 로컬 어댑터의 IP 주소 및 포트
    - 프로토콜
    - 프로세스 이름
    - 프로세스 인수
    - 프로세스 파일 경로
    - 프로세스의 Windows 식별자(PID)
    - 부모 프로세스의 Windows 식별자(PID)
    - 프로세스가 시작된 사용자 계정
    - 프로세스가 시작된 날짜 및 시간

- 레지스트리 키의 경로
- 레지스트리 키 이름
- 레지스트리 키의 텍스트 값
- 서비스 이름
- 서비스 설명
- DLL 서비스의 경로 및 이름
- 서비스 실행 파일의 경로 및 이름
- 서비스의 Windows 식별자(PID)
- 서비스 유형
- 서비스 상태
- 서비스 시작 모드
- 운영 체제 이름
- 운영 체제 버전
- 도메인이 없는 컴퓨터 네트워크 이름
- 도메인 또는 작업 그룹
- 사용자 이름
- 볼륨 이름
- 볼륨 문자
- 볼륨 유형

Kaspersky Industrial CyberSecurity for Networks 통합

Kaspersky Industrial CyberSecurity for Nodes가 제거되면 애플리케이션이 컴퓨터에 로컬로 저장한 모든 데이터가 삭제됩니다.

서비스 데이터

Kaspersky Industrial CyberSecurity for Nodes의 내장 에이전트는 다음의 데이터를 로컬로 저장합니다.

- Kaspersky Industrial CyberSecurity for Networks와의 통합에 필요한 데이터:
  - Kaspersky Industrial CyberSecurity for Networks 서버 연결 주소 및 포트
  - Kaspersky Industrial CyberSecurity for Networks와의 통합에 사용되는 인증서 관련 정보
- 격리된 파일

전송된 원격 측정 이벤트의 데이터

- **파일 데이터**
  - 파일의 고유 식별자
  - 파일 유형
  - 전체 파일 경로
  - 파일 크기
  - 파일 특성
  - ZoneId
  - 파일이 생성된 날짜 및 시간
  - 파일이 마지막으로 수정된 날짜 및 시간
  - 파일 특성이 수정된 날짜 및 시간
  - 원본 파일 이름
  - 애플리케이션 이름
  - 애플리케이션 버전
  - 애플리케이션 공급업체
  - 파일 설명
  - 파일 버전
  - 개체의 MD5 및 SHA256 해시
  - 파일 서명 확인 결과

- 파일 서명이 생성된 날짜 및 시간
- 서명 파일에 사용된 인증서 체인:
  - 인증서 체인 유형
  - 체인 내 인증서 관련 정보:
    - 인증서 발급자 이름
    - 인증서 보유자 이름
    - 인증서 일련 번호
    - 인증서 지문 알고리즘
    - 인증서 지문
    - 인증서 유효 기간

- **HTTP 쿼리 관련 데이터**
  - DNS 쿼리를 보낸 프로세스의 고유 식별자
  - 로컬 IP 주소 및 포트
  - 원격 IP 주소 및 포트
  - 데이터 전송 프로토콜
  - 연결 방향
  - HTTP 요청에 대한 정보:
    - HTTP 메소드
    - 도메인 이름이 없는 경로
    - 호스트 이름
    - HTTP 헤더 목록:
      - 이름
      - 값

- **경고 세부 정보**
  - 탐지 ID
  - 탐지 날짜 및 시간
  - 탐지 이름
  - 암호화 모드

- 탐지와 관련된 마지막 조치의 상태
- 탐지 처리가 실패한 이유
- 개체 유형
- 개체 이름
- 개체의 MD5 및 SHA256 해시
- 위협 제거 동작
- Kaspersky Security Network 내 개체 평판 정보:
  - 애플리케이션이 속한 그룹
  - 애플리케이션을 사용하는 Kaspersky Security Network 사용자 수
  - 애플리케이션이 가장 널리 사용되는 국가
  - Kaspersky Security Network에 애플리케이션이 처음 확인된 날짜 및 시간
  - Kaspersky Security Network로부터 정보를 수신한 날짜 및 시간

- **로그인 세션 데이터**
  - 세션 ID
  - 로그인에 사용된 사용자 계정의 이름
  - 사용자 계정 유형
  - 세션 유형
  - 로그인을 시도한 장치의 IP 주소
  - 로그인 시도가 발생한 장치의 IP 주소
  - 이 세션의 상승된 권한 및 관리자 권한 보유 여부에 대한 정보
  - 연결된 로그인 세션에 대한 정보
  - 원격 세션 애플리케이션 프로토콜
  - 원격 접근 세션 프로토콜
- **세션 종료 데이터**
  - 세션 ID
  - 로그인에 사용된 사용자 계정의 이름
  - 사용자 계정 유형
  - 세션 유형

- 로그인을 시도한 장치의 IP 주소
- 로그인 시도가 발생한 장치의 IP 주소
- 이 세션의 상승된 권한 및 관리자 권한 보유 여부에 대한 정보
- 연결된 로그인 세션에 대한 정보
- 원격 세션 애플리케이션 프로토콜
- 원격 접근 세션 프로토콜
- 세션 ID

- **네트워크 통신 데이터**
  - 데이터가 수집된 시간 간격의 시작 및 끝
  - 연결 목록:
    - 컴퓨터의 로컬 IP 주소
    - 컴퓨터의 로컬 MAC 주소
    - 컴퓨터의 원격 IP 주소
    - 컴퓨터의 원격 MAC 주소
    - 게이트웨이 IP 주소
    - 전송된 데이터 패킷 수
    - 수신된 데이터 패킷 수.
    - 전송된 총 바이트 수
    - 데이터 전송 프로토콜
    - EtherType
    - 간격 내 첫 번째 패킷의 페이로드 접두사
    - 통신이 캡처된 네트워크 인터페이스의 IPv4 주소

- **네트워크 연결 데이터**
  - 연결을 시작한 프로세스의 고유 식별자
  - 데이터 전송 프로토콜
  - 연결을 시작하는 데 사용된 로컬 IP 주소
  - 연결 엔드포인트의 원격 IP 주소

- HTTP 요청에 대한 정보:
  - HTTP 메소드
  - 도메인 이름이 없는 경로
  - 호스트 이름
  - HTTP 헤더 목록:
    - 이름
    - 값
- 연결 시 동적 프로세스 상태
- 연결 방향
- 동적 프로세스 상태
- EtherType

- **네트워크 포트에서 수신 중 캡처된 데이터**
  - 연결을 시작한 프로세스의 고유 식별자
  - 데이터 전송 프로토콜
  - 로컬 주소
  - 연결 시 동적 프로세스 상태

- **연결 확인 결과**
  - 호스트 네트워크 설정:
    - 네트워크 인터페이스 설명
    - DNS 도메인 이름
    - 컴퓨터의 로컬 MAC 주소
    - IP 연결 지표 번호
    - IP 주소 목록:
      - IP 주소
      - 네트워크 마스크
      - 게이트웨이 IP 주소
      - 게이트웨이 MAC 주소

- 설치된 패치 목록:
  - 패치 번호
  - 패치 설치 날짜
- 장치 모델
- 장치 공급업체
- Kaspersky Security Center 호스트 ID
- 설치된 Kaspersky 안티 바이러스에 대한 설명:
  - 설치된 Kaspersky 안티 바이러스의 구성 요소 이름
  - 설치된 Kaspersky 안티 바이러스의 구성 요소 버전
  - 설치된 Kaspersky 안티 바이러스 구성 요소의 데이터베이스 버전
  - 설치된 Kaspersky 안티 바이러스 구성 요소의 마지막 데이터베이스 업데이트 날짜
  - 설치된 Kaspersky 안티 바이러스의 구성 요소 상태
  - 라이센스 키 목록:
    - 키 일련 번호
    - 키 유형
    - 키 만료 날짜
    - 키 상태
- **프로세스 생성 관련 데이터**
  - 프로세스의 고유 식별자
  - 부모 프로세스의 고유 식별자
  - 프로세스의 고유 시스템 식별자
  - 프로세스를 시작하는 데 사용된 명령
  - 로그인 세션 ID
  - 터미널 세션 ID
  - 프로세스 파일의 고유 식별자
  - 프로세스 통합 레벨

- 토큰 권한 목록:
  - 권한
  - 권한 속성
- 해석된 파일의 고유 식별자 목록
- 프로세스 상태
- 프로세스를 시작하는 데 사용된 명령

- **프로세스 종료 데이터**
  - 감염된 개체의 고유 식별자

- **탐지된 위협 데이터**
  - 위협 정보:
    - 위협 평결
    - AMR 레코드 번호
    - 안티 바이러스 데이터베이스 버전
    - 위협 탐지 모드
    - 위협 UUID
    - 보호 기술
    - 위협의 고유 식별자
    - 보호 기술
  - 감염된 개체에 대한 정보:
    - 감염된 개체 유형
    - 감염된 개체 이름
    - 개체의 MD5 및 SHA256 해시
    - 감염된 프로세스의 고유 식별자
    - 감염된 개체의 고유 식별자
    - 인터넷에서 감염된 개체를 다운로드한 프로세스의 고유 식별자
    - 감염된 개체가 다운로드된 URL
    - 감염된 개체를 전송한 발신자 이메일 주소
    - 네트워크 프로토콜 유형(IANA에 따르면)

        - 로컬 네트워크 주소
        - 감염된 개체가 수신된 외부 네트워크 주소
        - 개체 콘텐츠 유형
        - 탐지된 위협의 컨텍스트
        - 개체 콘텐츠
    - 위협 탐지가 백그라운드에서 실행되었음을 나타내는 플래그
    - 로컬 물리적 주소
    - 감염된 개체를 수신한 물리적 주소
- **위협 처리에 대한 데이터**
    - 위협 정보:
        - 위협 평결
        - AMR 레코드 번호
        - 안티 바이러스 데이터베이스 버전
        - 위협 탐지 모드
        - 위협 UUID
        - 보호 기술
    - 감염된 개체에 대한 정보:
        - 감염된 개체 유형
        - 감염된 개체 이름
        - 개체의 MD5 및 SHA256 해시
        - 감염된 프로세스의 고유 식별자
        - 감염된 개체의 고유 식별자
        - 네트워크 프로토콜 유형(IANA에 따르면)
        - 감염된 개체가 수신된 외부 네트워크 주소
        - 로컬 네트워크 주소
    - 위협 처리 상태
    - 보안위협을 치료할 수 없는 이유
    - 로컬 물리적 주소

- **사용자 데이터**
  - 사용자 SID
  - 사용자 ID
  - 사용자 이름
  - 사용자의 전체 이름
  - 사용자 설명
  - 계정의 활성 또는 비활성 여부
  - 계정의 차단 여부
  - 암호의 만료 여부
  - 암호 변경이 필요한지 여부
  - 사용자가 암호를 변경할 수 있는지 여부
  - 사용자 계정 유형
  - 이 계정에 대해 자동 로그인이 활성화되었는지 여부
  - 사용자가 속한 그룹 목록
  - 마지막으로 암호를 변경한 날짜입니다.
  - 마지막 세션이 종료된 날짜입니다.

Kaspersky Industrial CyberSecurity for Nodes의 내장 에이전트에 대한 Kaspersky Industrial CyberSecurity for Networks에서 요청된 데이터

- 일반 작업 설정:
  - 작업 유형
  - 작업 스케줄 설정
  - 작업을 실행할 수 있는 계정의 이름과 암호
  - 설정 버전
  - 격리된 개체의 식별자
  - 개체 경로
  - 개체의 MD5 및 SHA256 해시
  - 인수를 이용해 프로세스를 시작하는 명령줄

- 작업 완료 시 수행되는 추가 작업의 플래그
- 서비스 이름
- 서비스 시작 유형

- 네트워크 격리 설정:
  - 설정 유형
  - 설정 버전
  - 네트워크 격리 예외 및 예외 설정 목록: 트래픽 방향, IP 주소, 포트, 프로토콜 및 실행 파일 전체 경로
  - 추가 작업의 플래그
  - 자동 격리 비활성화 시간
- 실행 방지 알림:
  - 설정 유형
  - 설정 버전
  - 실행 방지 규칙 및 규칙 설정 목록: 개체 경로, 개체 유형, 개체의 MD5 및 SHA256 해시
  - 추가 작업의 플래그

Kaspersky Industrial CyberSecurity for Nodes에서 Kaspersky Industrial CyberSecurity for Networks로 보내는 요청 데이터

Kaspersky Industrial CyberSecurity for Networks와 통합하려면 다음의 데이터가 컴퓨터에 로컬로 저장됩니다.

- 동기화 요청에서:
  - 고유 ID
  - 서버 웹 주소의 기본 부분
  - 컴퓨터 이름
  - 컴퓨터 IP 주소
  - 컴퓨터 MAC 주소
  - 컴퓨터의 현지 시간
  - Kaspersky Industrial CyberSecurity for Nodes 자기 보호 상태
  - 컴퓨터에 설치된 운영 체제 이름 및 버전
  - Kaspersky Industrial CyberSecurity for Nodes 버전

- 애플리케이션 설정 및 작업 설정의 버전
- 작업 상태: 작업 식별자, 실행 상태, 오류 코드

- 서버에서 파일을 얻기 위한 요청에서:
  - 파일의 고유 식별자
  - Kaspersky Industrial CyberSecurity for Nodes 고유 식별자
  - 인증서의 고유 식별자
  - Central Node 구성 요소가 설치된 서버의 웹 주소 기본 부분
  - 호스트 IP 주소
- 작업 실행 결과 리포트에서:
  - 호스트 IP 주소
  - 작업 완료 시 수행되는 추가 작업의 플래그
  - 작업 실행 오류 및 반환 코드
  - 작업 완료 상태
  - 작업 완료 시간
  - 작업 실행에 사용하는 설정 버전
  - 서버에 제출된 개체, 격리된 개체 및 격리 저장소에서 복원된 개체 관련: 개체 경로, MD5 및 SHA256 해시, 격리된 개체의 식별자
  - 서버의 요청에 따라 컴퓨터에서 시작되거나 중지된 프로세스 관련 정보: 개체의 PID 및 UniquePID, 오류 코드, MD5 및 SHA256 해시
  - 서버의 요청에 따라 컴퓨터에서 시작되거나 중지된 서비스 관련 정보: 서비스 이름, 시작 유형, 오류 코드, 서비스 파일 이미지의 MD5 및 SHA256 해시
  - 서버에서 요청한 파일
- 실행 중인 프로세스에 대한 데이터:
  - 전체 경로 및 확장자를 포함한 실행 파일 이름
  - 프로세스 자동 실행 매개변수
  - 프로세스 ID
  - 로그인 세션 ID
  - 로그인 세션 이름

- 프로세스가 시작된 날짜 및 시간
- 개체의 MD5 및 SHA256 해시

- 파일 데이터:
  - 파일 경로
  - 파일 이름
  - 파일 크기
  - 파일 특성
  - 파일이 생성된 날짜 및 시간
  - 파일이 마지막으로 수정된 날짜 및 시간
  - 파일 설명
  - 회사 이름
  - 개체의 MD5 및 SHA256 해시
  - 레지스트리 키(자동 실행 포인트용)
- 개체 관련 정보를 검색할 때 발생한 오류 데이터:
  - 오류 발생 시 처리된 개체의 전체 이름
  - 오류 코드

SIEM 통합

Kaspersky Industrial CyberSecurity for Nodes가 제거되면 애플리케이션이 컴퓨터에 로컬로 저장한 모든 데이터가 삭제됩니다.

SIEM 시스템과 통합되면 연결 설정에 대한 정보와 Windows 로그의 모든 이벤트가 전송됩니다.

기본 Windows 이벤트 로그는 시스템, 보안, 애플리케이션, 전달 이벤트 및 하드웨어 이벤트입니다. 사용자는 특정 요구 사항을 충족하는 사용자 지정 로그를 만들고 사용할 수도 있습니다.

Kaspersky Security Network 사용 시 데이터 제공

Kaspersky Industrial CyberSecurity for Nodes가 Kaspersky로 보내는 데이터 세트는 라이센스 유형 및 Kaspersky Security Network 사용 설정에 따라 다릅니다.

최대 4대의 컴퓨터에서 라이센스에 따라 KSN 사용

Kaspersky Security Network 진술문에 동의하시면 다음 정보를 자동으로 전송하는 데 동의하게 됩니다:

- KSN 구성 업데이트 관련 정보: 활성 구성의 식별자, 수신된 구성의 식별자, 구성 업데이트의 오류 코드;
- 검사할 파일과 URL 주소 관련 정보: 검사한 파일의 체크섬(MD5, SHA2-256, SHA1) 및 파일 패턴(MD5), 패턴의 크기, 탐지된 보안위협의 유형과 권리 소유자 분류에 따른 보안위협 이름, 안티 바이러스 데이터베이스의 식별자, 평판 요청 대상 URL 주소와 리퍼러 URL 주소, 연결의 프로토콜 식별자 및 사용 중인 포트 번호;
- 위협을 탐지한 검사 작업 ID;
- 인증 확인에 필요한 사용 중인 디지털 인증서 관련 정보: 검사한 개체의 서명에 사용되는 인증서의 체크섬(SHA256) 및 인증서의 공개 키;
- 검사를 수행 중인 소프트웨어 구성 요소의 식별자;
- 안티 바이러스 데이터베이스 및 이러한 데이터베이스의 레코드 ID;
- 컴퓨터의 소프트웨어 활성화 관련 정보: 활성화 서비스에서 전송된 티켓의 서명된 헤더(지역별 활성화 센터의 식별자, 활성화 코드의 체크섬, 티켓의 체크섬, 티켓 생성 날짜, 티켓의 고유 식별자, 티켓 버전, 라이센스 상태, 티켓 유효 기간 시작/종료 날짜와 시간, 라이센스의 고유 식별자, 라이센스 버전), 티켓 헤더에 서명하는 데 사용되는 인증서의 식별자, 키 파일의 체크섬(MD5);
- 권리 소유자 소프트웨어 관련 정보: 전체 버전, 유형, Kaspersky 서비스에 연결하는 데 사용되는 프로토콜의 버전.

최대 5대의 컴퓨터에서 라이센스에 따라 KSN 사용

Kaspersky Security Network 진술문에 동의하시면 다음 정보를 자동으로 전송하는 데 동의하게 됩니다:

Kaspersky Security Network 확인란을 선택하고 **확장 KSN 모드 사용** 확인란을 선택 해제하면 애플리케이션이 다음 정보를 전송합니다:

- KSN 구성 업데이트 관련 정보: 활성 구성의 식별자, 수신된 구성의 식별자, 구성 업데이트의 오류 코드;
- 검사할 파일과 URL 주소 관련 정보: 검사한 파일의 체크섬(MD5, SHA2-256, SHA1) 및 파일 패턴(MD5), 패턴의 크기, 탐지된 보안위협의 유형과 권리 소유자 분류에 따른 보안위협 이름, 안티 바이러스 데이터베이스의 식별자, 평판 요청 대상 URL 주소와 리퍼러 URL 주소, 연결의 프로토콜 식별자 및 사용 중인 포트 번호;
- 위협을 탐지한 검사 작업 ID;
- 인증 확인에 필요한 사용 중인 디지털 인증서 관련 정보: 검사한 개체의 서명에 사용되는 인증서의 체크섬(SHA256) 및 인증서의 공개 키;
- 검사를 수행 중인 소프트웨어 구성 요소의 식별자;
- 안티 바이러스 데이터베이스 및 이러한 데이터베이스의 레코드 ID;

- 컴퓨터의 소프트웨어 활성화 관련 정보: 활성화 서비스에서 전송된 티켓의 서명된 헤더(지역별 활성화 센터의 식별자, 활성화 코드의 체크섬, 티켓의 체크섬, 티켓 생성 날짜, 티켓의 고유 식별자, 티켓 버전, 라이센스 상태, 티켓 유효 기간 시작/종료 날짜와 시간, 라이센스의 고유 식별자, 라이센스 버전), 티켓 헤더에 서명하는 데 사용되는 인증서의 식별자, 키 파일의 체크섬(MD5);

- 권리 소유자 소프트웨어 관련 정보: 전체 버전, 유형, Kaspersky 서비스에 연결하는 데 사용되는 프로토콜의 버전.

확장 KSN 모드 사용 확인란과 **Kaspersky Security Network** 확인란을 선택하면 애플리케이션이 상기 나열된 정보와 함께 다음 정보를 전송합니다:

- 요청한 웹 리소스 분류 결과 관련 정보(호스트의 IP 주소와 처리된 URL, 분류를 수행한 소프트웨어 구성 요소의 버전, 분류 방법 및 웹 리소스에 대해 정의된 카테고리 집합 포함);

- 컴퓨터에 설치된 소프트웨어 관련 정보: 소프트웨어 애플리케이션의 이름 및 소프트웨어 공급업체, 레지스트리 키와 해당 값, 설치된 소프트웨어 구성 요소의 파일 관련 정보(체크섬(MD5, SHA2-256, SHA1), 이름, 컴퓨터의 파일 경로, 크기, 버전 및 디지털 서명);

- 컴퓨터의 안티 바이러스 보호 상태에 대한 정보: 사용 중인 안티 바이러스 데이터베이스의 버전 및 배포 타임 스탬프, 작업 ID 및 검사를 수행하는 소프트웨어의 ID;

- 최종 사용자가 다운로드 중인 파일 관련 정보: 다운로드 및 다운로드 페이지의 URL과 IP 주소, 다운로드 프로토콜 식별자 및 연결 포트 번호, URL의 상태(악성 여부), 파일 특성, 크기와 체크섬(MD5, SHA2-256, SHA1), 파일을 다운로드한 프로세스 관련 정보(체크섬(MD5, SHA2-256, SHA1), 만든 날짜/빌드 날짜, 자동 재생 상태, 특성, 실행 압축 프로그램 이름, 서명 관련 정보, 실행 파일 플래그, 형식 식별자, 엔트로피), 파일 이름 및 컴퓨터의 경로, 파일의 디지털 서명 및 생성 타임 스탬프, 파일이 탐지된 URL 주소, 의심스럽거나 유해한 것으로 확인된 페이지의 스크립트 번호, 생성된 HTTP 요청 및 해당 요청에 대한 응답 관련 정보;

- 실행 중인 애플리케이션 및 해당 모듈 관련 정보: 시스템에서 실행 중인 프로세스 관련 데이터(프로세스 ID(PID), 프로세스 이름, 프로세스가 시작된 계정 관련 정보, 프로세스를 시작한 애플리케이션과 명령, 신뢰하는 프로그램이나 프로세스의 기호, 프로세스의 파일 전체 경로와 그 체크섬(MD5, SHA2-256, SHA1), 시작 명령줄, 프로세스 무결성 레벨, 프로세스가 속하는 제품의 설명(제품 이름 및 게시자 관련 정보), 사용 중인 디지털 인증서 및 해당 인증서의 신뢰성 확인에 필요한 정보나 파일의 디지털 서명 누락 관련 정보), 프로세스에 로드된 모듈 관련 정보(모듈 이름, 크기, 유형, 생성 날짜, 특성, 체크섬(MD5, SHA2-256, SHA1), 컴퓨터의 모듈 경로), PE-파일 헤더 정보, 실행 압축 프로그램 이름(파일이 압축된 경우);

- 모든 잠재적인 악성 개체와 활동에 관한 정보: 탐지한 개체의 이름 및 컴퓨터상 개체의 전체 경로, 처리한 파일의 체크섬(MD5, SHA2-256, SHA1), 탐지 날짜 및 시간, 감염된 파일의 이름 및 크기와 경로, 경로 템플릿 코드, 실행 파일 플래그, 개체가 컨테이너인지 여부, 실행 파일 압축 프로그램의 이름(파일 압축 시), 파일 유형 코드, 파일 형식 ID, 악성 코드가 수행한 작업 목록 및 이에 대한 대응으로 소프트웨어 및 사용자가 내린 결정, 결정을 내리는 데 사용된 안티 바이러스 데이터베이스 및 이러한 데이터베이스에 포함된 레코드의 ID, 악성일 가능성이 있는 개체를 나타내는 표시기, 권리자의 분류에 따라 탐지된 위협의 이름, 위험 수준, 탐지 상태 및 탐지 방법, 분석된 컨텍스트 내로 포함한 이유와 컨텍스트 내 파일의 시퀀스 번호, 체크섬(MD5, SHA2-256, SHA1), 감염된 메시지 또는 링크가 전송된 애플리케이션의 실행 파일의 이름과 특성, 차단된 개체에 대한 호스트의 익명 처리된 IP 주소(IPv4 및 IPv6), 파일 엔트로피, 파일 자동 실행 표시, 시스템에서 파일을 처음 탐지한 시간, 마지막 통계 전송 이후 파일 실행 횟수, 악성 개체가 수신된 메일 클라이언트의 이름, 체크섬(MD5, SHA2-256, SHA1) 및 크기에 관한 정보, 검사를 수행한 소프트웨어 작업 ID, 파일 평판 또는 서명의 검사 여부, 파일 처리 결과, 개체에 대해 수집된 패턴의 체크섬(MD5), 패턴 크기(단위: 바이트), 적용한 탐지 기술의 기술 사양;

- 검사한 개체 관련 정보: 검사한 파일이 원래 포함되어 있었거나 검사 후에 포함된 제어 그룹, 파일이 해당 카테고리에 포함된 이유, 카테고리 식별자, 카테고리 소스 및 카테고리 데이터베이스 버전 관련 정보, 파일의 신뢰하는 인증서 플래그, 파일 공급업체 이름, 파일 버전, 파일을 포함하는 소프트웨어 애플리케이션의 이름과 버전;

- 탐지된 취약점 관련 정보: 취약점 데이터베이스의 취약점 ID, 취약점 위험 등급;

- 실행 파일 에뮬레이션 관련 정보: 파일 크기와 해당 체크섬(MD5, SHA2-256, SHA1), 에뮬레이션 구성 요소의 버전, 에뮬레이션 수준, 에뮬레이션 중에 가져온 논리 블록 내의 기능과 논리 블록 속성의 배열, 실행 파일 PE 헤더의 데이터;

- 공격하는 컴퓨터의 IP 주소(IPv4 및 IPv6), 네트워크 공격의 대상인 컴퓨터의 포트 번호, 공격을 포함하는 IP 패킷의 프로토콜 식별자, 공격 대상(조직 이름, 웹사이트), 공격에 대한 대응 플래그, 공격의 가중치, 신뢰 레벨;

- 스푸핑된 네트워크 리소스와 관련된 공격 관련 정보, 방문한 웹사이트의 DNS 및 IP 주소(IPv4 및 IPv6);

- 요청된 웹사이트의 DNS 및 IP 주소(IPv4 또는 IPv6), 웹사이트에 접근하는 파일 및 웹 클라이언트에 관한 정보, 파일의 이름, 크기 및 체크섬(MD5, SHA2-256, SHA1), 파일 및 경로 템플릿 코드에 대한 전체 경로, 디지털 서명 검사 결과, KSN의 상태;

- 악성 코드 활동의 롤백에 관한 정보: 활동이 롤백된 파일에 관한 데이터(파일 이름, 파일 전체 경로, 크기 및 체크섬(MD5, SHA2-256, SHA1)), 파일 삭제, 이름 바꾸기, 복사 및 레지스트리의 값 복구를 위한 작업 성공 또는 실패 날짜(레지스트리 키 이름 및 값), 롤백 전후 악성 코드가 수정한 시스템 파일에 관한 정보;

- 적응형 이상 행위 제어 구성 요소에 대해 설정된 예외 규칙 정보: 트리거된 규칙의 ID와 상태, 규칙 트리거 시 소프트웨어가 수행한 처리, 프로세스 또는 스레드가 의심스러운 활동을 수행하는 사용자 계정의 유형, 의심스러운 활동을 수행했거나 그 대상이었던 프로세스에 대한 정보(스크립트 ID 또는 프로세스 파일 이름, 프로세스 파일의 전체 경로, 경로 템플릿 코드, 프로세스 파일의 체크섬(MD5, SHA2-256, SHA1)) 의심스러운 활동을 수행한 개체 및 의심스러운 활동 수행 대상 개체 관련 정보(레지스트리 키 이름 또는 파일 이름, 파일의 전체 경로, 경로 템플릿 코드, 파일의 체크섬(MD5, SHA2-256, SHA1));

- 로드된 소프트웨어 모듈에 관한 정보: 모듈 파일의 이름, 크기 및 체크섬(MD5, SHA2-256, SHA1), 파일 전체 경로와 파일 템플릿 코드, 모듈 파일의 디지털 서명 설정, 서명 생성 날짜 및 시간, 모듈 파일을 서명한 조직 및 주체 이름, 모듈이 로드된 프로세스의 ID, 모듈 제공자 이름, 로딩 대기열 내 모듈의 시퀀스 번호;

- KSN 서비스와 소프트웨어의 상호 작용 품질 관련 정보: 통계 생성 기간의 시작 및 종료 날짜와 시간, 요청 품질과 사용되는 각 KSN 서비스에 대한 연결 관련 정보(KSN 서비스 ID, 성공한 요청 수, 캐시에서 응답을 받은 요청 수, 실패한 요청 수(네트워크 문제, 소프트웨어 설정에서 KSN이 중지됨, 잘못된 라우팅), 성공한 요청의 시간 분산, 취소한 요청의 시간 분산, 시간 제한을 초과한 요청의 시간 분산, 캐시에서 가져온 KSN으로의 연결 수, 성공한 KSN으로의 연결 수, 실패한 KSN으로의 연결 수, 성공한 트랜잭션 수, 실패한 트랜잭션 수, 성공한 KSN으로의 연결 시간 분산, 실패한 KSN으로의 연결 시간 분산, 성공한 트랜잭션의 시간 분산, 실패한 트랜잭션의 시간 분산);

- 잠재적 악성 개체가 탐지되면 프로세스 메모리에서 데이터 관련 정보가 제공됩니다: 시스템 개체 계층 구조의 요소(ObjectManager), UEFI BIOS 메모리의 데이터, 레지스트리 키의 이름과 해당 값;

- 시스템 로그의 이벤트 관련 정보: 이벤트 타임 스탬프, 이벤트가 발견된 로그 이름, 이벤트 유형 및 카테고리, 이벤트 소스 이름 및 이벤트 설명;

- 네트워크 연결 관련 정보: 포트를 연 프로세스가 시작된 파일의 버전 및 체크섬(MD5, SHA2-256, SHA1), 프로세스 파일 경로 및 디지털 서명, 로컬 및 원격 IP 주소, 로컬 및 원격 연결 포트 수, 연결 상태, 포트 열기 타임 스탬프;

- 컴퓨터에 소프트웨어를 설치 및 활성화한 날짜에 대한 정보: 라이센스를 판매한 파트너의 ID, 라이센스 일련번호, 활성화 서비스 티켓의 서명된 헤더(지역별 활성화 센터의 ID, 활성화 코드의 체크섬, 티켓의 체크섬, 티켓 생성 날짜, 티켓의 고유 ID, 티켓 버전, 라이센스 상태, 티켓 시작/종료 날짜 및 시간, 라이센스 고유 ID, 라이센스 버전), 티켓 헤더에 서명하는 데 사용된 인증서 ID, 키 파일의 체크섬(MD5), 컴퓨터에 설치된 소프트웨어의 고유 ID, 업데이트되는 애플리케이션의 유형 및 ID, 업데이트 작업;

- 설치된 모든 업데이트 집합 및 가장 최근에 설치/제거된 업데이트 집합 관련 정보, 업데이트 정보 전송의 원인이 된 이벤트의 유형, 마지막 업데이트 설치 이후에 경과한 시간, 현재 설치되어 있는 안티 바이러스 데이터베이스 관련 정보;

- 컴퓨터의 소프트웨어 동작 관련 정보: CPU 사용량 정보, 메모리 사용량 정보(전용 바이트, 비페이징 풀, 페이징 풀), 소프트웨어 프로세스의 활성 스레드 수와 보류 중인 스레드 수, 오류 발생 전까지 소프트웨어 동작 시간;

- 소프트웨어 설치 이후 그리고 마지막 업데이트 시간 이후 소프트웨어 덤프 및 시스템 덤프(BSOD) 횟수, 작동이 중단된 소프트웨어 모듈의 식별자와 버전, 소프트웨어 프로세스의 메모리 스택, 작동 중단 발생 시 안티 바이러스 데이터베이스에 관한 정보;

- 시스템 덤프(BSOD) 관련 데이터: 컴퓨터에서 BSOD가 발생했음을 나타내는 플래그, BSOD의 원인이 된 드라이버의 이름, 드라이버의 주소와 메모리 스택, BSOD 발생 전의 OS 세션 지속 시간을 나타내는 플래그, 작동이 중단된 드라이버의 메모리 스택, 저장된 메모리 덤프의 유형, BSOD가 10분 이상 지속되기 전의 OS 세션 플래그, 덤프의 고유 식별자, BSOD의 타임 스탬프;

- 소프트웨어 구성 요소 동작 중에 발생한 오류 또는 성능 문제 관련 정보: 소프트웨어의 상태 ID, 오류 유형, 코드와 원인, 오류 발생 시간, 구성 요소 ID, 오류가 발생한 제품의 모듈과 프로세스, 오류가 발생한 작업 또는 업데이트 카테고리의 ID, 소프트웨어에서 사용하는 드라이버의 로그(오류 코드, 모듈 이름, 소스 파일 이름, 오류가 발생한 줄);

- 안티 바이러스 데이터베이스 및 소프트웨어 구성 요소 업데이트 관련 정보: 마지막 업데이트 중에 다운로드되었으며 현재 업데이트 중에 다운로드 중인 색인 파일의 이름, 날짜 및 시간;

- 소프트웨어 동작의 비정상 종료 관련 정보: 덤프의 생성 타임 스탬프, 해당 유형, 소프트웨어 동작 비정상 종료의 원인이 된 이벤트의 유형(예기치 않은 전원 꺼짐, 타사 애플리케이션 작동 중단), 예기치 않은 전원 꺼짐 날짜 및 시간;

- 하드웨어 및 소프트웨어와 소프트웨어 드라이버의 호환성 관련 정보: 소프트웨어 구성 요소 기능을 제한하는 OS 속성 관련 정보(보안 부팅, KPTI, WHQL 적용, BitLocker, 대/소문자 구분), 설치된 다운로드 소프트웨어의 유형(UEFI, BIOS), 신뢰하는 플랫폼 모듈(TPM) 식별자, TPM 사양 버전, 컴퓨터에 설치된 CPU 관련 정보, 코드 무결성 및 Device Guard 운영 모드 및 파라미터, 드라이버 운영 모드 및 현재 모드 사용 이유, 소프트웨어 드라이버 버전, 컴퓨터의 소프트웨어 및 하드웨어 가상화 지원 상태;

- 오류를 발생시킨 제삼자 애플리케이션에 관한 정보: 이름, 버전 및 현지화, 오류 코드 및 애플리케이션의 시스템 로그에 기재된 오류 관련 정보, 제삼자 애플리케이션의 메모리 스택 및 오류 주소, 소프트웨어 구성 요소의 오류 발생을 나타내는 플래그, 오류 발생 전까지 제삼자 애플리케이션이 동작한 시간, 오류가 발생한 애플리케이션 프로세스 이미지의 체크섬(MD5, SHA2-256, SHA1), 이 애플리케이션 프로세스 이미지의 경로 및 경로 템플릿 코드, 시스템 로그의 정보와 애플리케이션과 관련된 오류 설명, 오류가 발생한 애플리케이션 모듈에 관한 정보(제외 식별자, 작동 중단된 메모리 주소(애플리케이션 모듈의 오프셋), 모듈의 이름과 버전, 권리 소유자의 플러그인 내 애플리케이션 작동 중단 식별자 및 작동 중단된 메모리 스택, 작동 중단 전까지의 애플리케이션 세션 지속 시간);

- 소프트웨어 업데이터 구성 요소의 버전, 구성 요소 수명 동안 업데이트 작업을 실행하는 중에 업데이터 구성 요소의 작동이 중단된 수, 업데이트 작업 유형의 ID, 업데이터 구성 요소의 업데이트 작업 완료 시도가 실패한 수;

- 소프트웨어 시스템 감시 구성 요소의 동작 관련 정보: 구성 요소의 전체 버전, 구성 요소가 시작된 날짜와 시간, 이벤트 대기열 초과의 원인이 된 이벤트 코드와 해당 이벤트의 수, 대기열 초과 이벤트의 총 수, 이벤트 게시자 프로세스의 파일 관련 정보(파일 이름과 컴퓨터의 파일 경로, 파일 경로의 템플릿 코드, 파일과 연결된 프로세스의 체크섬(MD5, SHA2-256, SHA1), 파일 버전), 발생한 이벤트 가로채기의 식별자, 가로채기 필터의 전체 버전, 가로챈 이벤트의 유형 식별자, 이벤트 대기열의 크기 및 대기열의 첫 번째 이벤트와 현재 이벤트 사이 이벤트 수, 대기열의 지연된 이벤트 수, 현재 이벤트 개시자 프로세스의 파일 관련 정보(파일 이름과 컴퓨터의 파일 경로, 파일 경로의 템플릿 코드, 파일과 연결된 프로세스의 체크섬(MD5, SHA2-256, SHA1)), 이벤트 처리의 지속 시간, 이벤트 처리의 최대 지속 시간, 통계 전송 가능성, 처릴 시간 제한이 초과된 OS 이벤트 관련 정보(이벤트의 날짜와 시간, 안티 바이러스 데이터베이스의 반복 초기화 수, 업데이트 이후 마지막으로 반복된 안티 바이러스 데이터베이스 초기화의 날짜와 시간, 각 시스템 감시 구성 요소의 이벤트 처리 지연 시간, 대기된 이벤트의 수, 처리된 이벤트의 수, 현재 유형의 지연되는 이벤트 수, 현재 유형 이벤트의 총 지연 시간, 모든 이벤트의 총 지연 시간);

- 소프트웨어 성능 문제 이벤트 발생 시 Microsoft의 SysConfig/SysConfigEx/WinSATAssessment 이벤트 공급자인 Windows 이벤트 추적 도구(ETW, Windows용 이벤트 추적)에서 생성되는 정보: 컴퓨터 관련 정보(모델, 하우징 폼 팩터, 버전), Windows 성능 메트릭 관련 정보(WinSAT 평가, Windows 성능 지수), 도메인 이름, 실제/논리 프로세서 관련 정보(실제/논리 프로세서의 수, 제조업체, 모델, 스태핑 레벨, 코어 수, 클록 주파수, CPUID, 캐시 특성, 논리 프로세서 특성, 지원되는 모드와 명령 표시기), RAM 모듈 관련 정보(유형, 폼 팩터, 제조업체, 모델, 용량, 메모리 할당 세분성), 네트워크 인터페이스 관련 정보(IP 및 MAC 주소, 이름, 설명, 네트워크 인터페이스 구성, 유형별 네트워크 패키지 수와 크기 구분, 네트워크 교환 속도, 유형별 네트워크 오류 수 구분), IDE 컨트롤러 구성, DNS 서버의 IP 주소, 비디오 카드 관련 정보(모델, 설명, 제조업체, 호환성, 비디오 메모리 용량, 화면 권한, 픽셀당 비트 수, BIOS 버전) 플러그 앤 플레이 장치 관련 정보(이름, 설명, 장치 식별자 [PnP, ACPI], 디스크 및 저장 장치 관련 정보(디스크 또는 플래시 드라이브 수, 제조업체, 모델, 디스크 용량, 실린더 수, 실린더당 트랙 수, 트랙당 섹터 수, 섹터 용량, 캐시 특성, 시퀀스 번호, 파티션 수, SCSI 컨트롤러 구성), 논리 디스크 관련 정보(시퀀스 번호, 파티션 용량, 볼륨 용량, 볼륨 문자, 파티션 유형, 파일 시스템 유형, 클러스터 수, 클러스터 크기, 클러스터당 섹터 수, 비어 있는/사용된 클러스터 수, 부팅 가능 볼륨 문자, 디스크 시작 관련 파티션 오프셋 주소), BIOS 마더보드 관련 정보(제조업체, 배포 날짜, 버전), 마더보드 관련 정보(제조업체, 모델, 유형), 실제 메모리 관련 정보(공유 및 사용 가능 용량), 운영 체제 서비스 관련 정보(이름, 설명, 상태, 태그, 프로세스 관련 정보 [이름 및 PID]), 컴퓨터의 에너지 소비량 파라미터, 인터럽트 컨트롤러 구성, Windows 시스템 폴더 경로(Windows 및 System32), OS 관련 정보(버전, 빌드, 배포 날짜, 이름, 유형, 설치 날짜), 페이지 파일 크기, 모니터 관련 정보(수, 제조업체, 화면 권한, 해상도 용량, 유형), 비디오 카드 드라이버 관련 정보(제조업체, 배포 날짜, 버전);

- Microsoft의 EventTrace/EventMetadata 이벤트 공급자인 ETW의 정보: 시스템 이벤트 시퀀스 관련 정보(유형, 시간, 날짜, 표준 시간대), 추적 결과가 포함된 파일 관련 메타데이터(이름, 구조, 추적 파라미터, 유형별 추적 동작 수 구분), OS 관련 정보(이름, 유형, 버전, 빌드, 배포 날짜, 시작 시각);

- Microsoft의 프로세스/Microsoft Windows 커널 프로세스/Microsoft Windows 커널 프로세서 전원 이벤트 공급자인 ETW의 정보: 시작/완료된 프로세스 관련 정보(이름, PID, 시작 파라미터, 명령줄, 반환 코드, 전원 관리 파라미터, 시작/완료 시간, 액세스 토큰 유형, SID, SessionID, 설치된 설명자 수), 스레드 우선 순위 변경 관련 정보(TID, 우선 순위, 시간), 프로세스의 디스크 작동 관련 정보(유형, 시간, 용량, 수), 사용 가능한 메모리 프로세스의 구조와 용량 변경 기록;

- Microsoft의 StackWalk/Perfinfo 이벤트 공급자인 ETW의 정보: 성능 카운트 관련 정보(개별 코드 섹션의 성능, 함수 호출 시퀀스, PID, TID, ISR과 DPC의 주소와 특성);

- Microsoft의 KernelTraceControl-ImageID 이벤트 공급자인 ETW의 정보: 실행 파일과 동적 라이브러리 관련 정보(이름, 이미지 크기, 전체 경로), PDB 파일 관련 정보(이름, 식별자), 실행 파일의 VERSIONINFO 리소스 데이터(이름, 설명, 작성자, 위치, 애플리케이션 버전과 식별자, 파일 버전과 식별자);

- Microsoft의 FileIo/DiskIo/Image/Windows 커널 디스크 이벤트 공급자인 ETW의 정보: 파일 및 디스크 동작 관련 정보(유형, 용량, 시작 시간, 완료 시간, 지속 시간, 완료 상태, PID, TID, 드라이버 함수 호출 주소, IRP(I/O 요청 패킷), Windows 파일 개체 특성), 파일 및 디스크 동작에서 사용된 파일 관련 정보(이름, 버전, 크기, 전체 경로, 특성, 오프셋, 이미지 체크섬, 열기 및 액세스 옵션);

- Microsoft의 PageFault 이벤트 공급자인 ETW의 정보: 메모리 페이지 액세스 오류 관련 정보(주소, 시간, 용량, PID, TID, Windows 파일 개체 특성, 메모리 할당 파라미터);

- Microsoft의 스레드 이벤트 공급자인 ETW의 정보: 스레드 생성/완료 관련 정보, 시작된 스레드 관련 정보(PID, TID, 스택 크기, CPU 리소스 우선 순위와 할당, I/O 리소스, 스레드 간의 메모리 페이지, 스택 주소, init 함수 주소, TEB(스레드 환경 블록)의 주소, Windows 서비스 태그);

- Microsoft Windows 커널 메모리 이벤트의 공급자인 ETW의 정보: 메모리 관리 동작 관련 정보(완료 상태, 시간, 수량, PID), 메모리 할당 구조(유형, 용량, SessionID, PID);

- 성능 문제 발생 시 소프트웨어 작동에 대한 정보: 소프트웨어 설치 식별자, 성능 저하 유형과 값, 소프트웨어 내 이벤트 시퀀스 관련 정보(시간, 표준 시간대, 유형, 완료 상태, 소프트웨어 구성 요소 식별자, 소프트웨어 작동 시나리오 식별자, TID, PID, 함수 호출 주소), 확인할 네트워크 연결 관련 정보(URL, 연결 방향, 네트워크 패키지 크기), PDB 파일 관련 정보(이름, 식별자, 실행 파일의 이미지 크기), 확인할 파일 관련 정보(이름, 전체 경로, 체크섬), 소프트웨어 성능 모니터링 파라미터';

- 마지막으로 실패한 OS 다시 시작 관련 정보: OS 설치 이후 실패한 다시 시작 수, 시스템 덤프의 데이터(오류의 코드와 파라미터, OS 동작에서 오류를 발생시킨 모듈의 이름, 버전 및 체크섬(CRC32), 오류 주소(모듈의 오프셋), 시스템 덤프의 체크섬(MD5, SHA2-256, SHA1));

- 파일에 서명하는 데 사용 중인 디지털 인증서의 신뢰성을 확인하기 위한 정보: 인증서의 지문, 체크섬 알고리즘, 인증서의 공개 키와 일련번호, 인증서 발급 기관의 이름, 인증서 검증 결과, 인증서 데이터베이스 식별자;

- 소프트웨어 자기 보호에 공격을 가한 프로세스 관련 정보: 프로세스 파일의 이름 및 크기, 체크섬(MD5, SHA2-256, SHA1), 프로세스 파일의 전체 경로 및 파일 경로의 템플릿 코드, 생성/작성 타임 스탬프, 실행 파일 플래그, 프로세스 파일의 특성, 프로세스 파일에 서명하는 데 사용된 인증서 관련 정보, 프로세스를 시작하는 데 사용한 계정의 코드, 프로세스 접근을 위해 수행된 동작의 ID, 동작 수행에 사용된 리소스 유형(프로세스, 파일, 레지스트리 개체, FindWindow 검색 기능), 동작 수행에 사용된 리소스 이름, 동작 성공을 나타내는 플래그, 프로세스의 파일 상태 및 KSN의 파일 서명;

- 권리 소유자 소프트웨어에 관한 정보: 사용한 소프트웨어의 전체 버전, 유형, 현지화 및 동작 상태, 설치된 소프트웨어 구성 요소의 버전 및 동작 상태, 설치된 소프트웨어 업데이트 날짜, TARGET 필터값, 권리 소유자 서비스에 연결하는 데 사용한 프로토콜 버전.

- 컴퓨터에 설치된 하드웨어 관련 정보: 유형, 이름, 모델 이름, 펌웨어 버전, 기본 제공 장치와 연결된 장치의 파라미터, 소프트웨어가 설치된 컴퓨터의 고유 식별자;

- 운영 체제와 설치된 업데이트의 버전 관련 정보, 단어 크기, OS 실행 모드의 버전과 파라미터, OS 커널 파일의 버전과 체크섬(MD5, SHA2-256, SHA1), OS 시작 시간과 날짜;

- 전체 또는 일부 실행 파일 및 비 실행 파일;

- 컴퓨터의 RAM 일부;

- OS 부팅 프로세스와 관련된 섹터;

- 네트워크 트래픽 데이터 패킷;

- 의심스러운 악성 개체가 포함된 웹 페이지와 이메일;

- WMI 저장소 클래스 및 해당 인스턴스에 관한 설명;

- 애플리케이션 활동 리포트:

  - 전송할 파일의 이름, 크기 및 버전, 설명 및 체크섬(MD5, SHA2-256, SHA1), 파일 형식 식별자, 파일 공급 업체 이름, 파일이 속한 제품 이름, 컴퓨터의 파일 전체 경로, 경로의 템플릿 코드, 파일의 생성 및 수정 타임 스탬프;

  - 인증서 유효 기간의 시작 및 종료 날짜/시간(디지털 서명이 있는 파일의 경우), 서명 날짜 및 시간, 인증서 발급자 이름, 인증서 소유자 관련 정보, 지문, 인증서의 공개 키 및 적절한 알고리즘, 인증서 일련번호;

  - 프로세스가 실행 중인 계정의 이름;

  - 프로세스가 시작된 컴퓨터의 이름에 대한 체크섬(MD5, SHA2-256, SHA1);

  - 프로세스 창 제목;

  - 안티 바이러스 데이터베이스의 식별자, 권리 소유자의 분류에 따른 탐지된 보안위협의 이름;

  - 설치된 라이센스, ID, 유형 및 만료 날짜에 대한 데이터;

  - 정보 제공 시점의 컴퓨터 로컬 시간;

- 프로세스에서 접근한 파일의 이름과 경로;
- 프로세스에서 접근한 레지스트리 키 이름과 값;
- 프로세스에서 접근한 URL 및 IP 주소;
- 실행 중인 파일을 다운로드한 URL 및 IP 주소.

유럽 연합 법규(GDPR) 준수

Kaspersky Industrial CyberSecurity for Nodes는 다음 시나리오에서 Kaspersky로 데이터를 전송할 수 있습니다:

- Kaspersky Security Network 사용.
- 활성화 코드로 애플리케이션 활성화.
- 애플리케이션 모듈 및 안티 바이러스 데이터베이스 업데이트.
- 애플리케이션 콘솔의 링크를 따릅니다.

데이터 분류 및 데이터 수신 지역에 관계없이 Kaspersky는 데이터 보안에 대한 높은 표준을 준수하고 사용자의 데이터를 보호하고 데이터 보안 및 기밀성을 보장하며 해당 법률에 의해 보장되는 사용자 권리의 이행을 보장하기 위해 다양한 법적, 조직적, 기술적 조치를 취합니다. 개인정보취급방침의 텍스트는 애플리케이션 배포 키트에 포함되어 있으며 Kaspersky 웹사이트에서 볼 수 있습니다.

Kaspersky Industrial CyberSecurity for Nodes를 사용하기 전에 최종 사용자 라이센스 계약서 및 Kaspersky Security Network 진술문(Kaspersky Security Network 진술문에 나열됨)에서 전송된 데이터에 대한 설명을 주의 깊게 읽으십시오. 설명된 시나리오에 따라 Kaspersky Industrial CyberSecurity for Nodes에서 전송된 특정 데이터가 현지 법률 또는 표준에 따라 개인 데이터로 분류될 수 있는 경우 해당 데이터가 합법적으로 처리되는지 확인하고 이러한 데이터의 수집 및 전송에 대한 최종 사용자의 동의를 얻어야합니다.

최종 사용자 라이센스 계약서와 Kaspersky Security Network 진술문에 동의한 이후에 애플리케이션 사용에 대한 정보를 당사가 수신, 처리, 저장 방법에 대한 자세한 내용을 보려면 최종 사용자 라이센스 계약서를 읽고 Kaspersky 웹사이트에 방문하십시오. 애플리케이션 배포 키트에 포함된 license.txt 및 ksn_<언어 ID>.txt 파일에는 최종 사용자 라이센스 계약서 전문과 Kaspersky Security Network 진술문이 들어 있습니다.

Kaspersky로 데이터를 전송하지 않으려면 데이터 제공을 중지할 수 있습니다.

Kaspersky Security Network 사용

Kaspersky Security Network를 사용하면 Kaspersky Security Network 진술문에 나열된 데이터의 자동 제공에 동의하는 것입니다. 이 데이터를 Kaspersky에 제공하는 데 동의하지 않으면 Kaspersky Private Security Network(KPSN)를 사용하거나 KSN 사용을 중지하십시오.

활성화 코드로 애플리케이션 활성화

활성화 코드를 사용하면 최종 사용자 라이센스 계약서에 따라 데이터를 자동 제공하는 데 동의하는 것입니다. 이 정보를 Kaspersky에 제공하는 데 동의하지 않으면 키 파일을 사용하여 Kaspersky Industrial CyberSecurity for Nodes를 활성화해야 합니다.

애플리케이션 모듈 및 안티 바이러스 데이터베이스 업데이트

Kaspersky 서버를 사용하면 최종 사용자 라이센스 계약서에 따라 데이터를 자동 제공하는 데 동의하는 것입니다. Kaspersky는 Kaspersky Industrial CyberSecurity for Nodes가 합법적으로 사용되고 있는지 확인하기 위해 이 정보가 필요합니다. 이 정보를 Kaspersky에 제공하는 데 동의하지 않으면 Kaspersky Security Center를 사용하여 데이터베이스를 업데이트하십시오.

애플리케이션 콘솔의 링크를 따릅니다.

애플리케이션 콘솔에서 링크를 사용하면 최종 사용자 라이센스 계약서에 따라 데이터를 자동 제공하는 데 동의하는 것입니다. 각 특정 링크에서 전송되는 정확한 데이터 목록은 링크가 애플리케이션 콘솔에 있는 위치와 해결하려는 문제에 따라 다릅니다. 이 정보를 Kaspersky에 제공하는 데 동의하지 않으면, 애플리케이션 인터페이스 표시를 비활성화하십시오.

타사 코드에 대한 정보

타사 코드에 대한 정보는 애플리케이션 설치 폴더에 있는 legal_notices.txt 파일에서 확인할 수 있습니다.

상표 고지

등록된 상표 및 서비스 마크는 해당 소유주의 재산입니다.

Bluetooth 단어, 마크 및 로고는 Bluetooth SIG, Inc.의 소유입니다.

Pentium은 Intel Corporation 또는 그 자회사의 상표입니다.

Linux는 미국 및 기타 국가에서 Linus Torvalds의 등록 상표입니다.

Microsoft, Active Directory, Excel, Forefront, Hyper-V, Internet Explorer, JScript, Lync, Outlook, PowerShell, SharePoint, SQL Server, Windows, Windows Server, Windows Vista 및 Windows XP는 Microsoft 그룹의 상표입니다.

Schneider Electric은 Schneider Electric의 상표입니다.

Siemens, Simatic, WinCC는 Siemens AG의 등록 상표입니다.

UNIX는 미국 및 기타 국가에서 등록된 상표이며 X/Open Company Limited를 통해서만 라이센스가 부여됩니다.