kaspersky

Kaspersky Endpoint Security 14.0 for Windows

© 2026 AO Kaspersky Lab

목차

Kaspersky Endpoint Security for Windows 도움말
- 새로운 기능
- 자주 묻는 질문

Kaspersky Endpoint Security for Windows
- 애플리케이션 모드: Standard, EDR Agent, Light Agent
- 배포 패키지
- 하드웨어 및 소프트웨어 요구 사항
- 운영 체제 유형에 따라 사용 가능한 애플리케이션 기능 비교
- 관리 도구에 따른 애플리케이션 기능 비교
- 다른 애플리케이션과의 호환성

애플리케이션 설치 및 제거
- Kaspersky Security Center를 통한 배포
  - 애플리케이션 표준 설치
  - 설치 패키지 만들기
  - 설치 패키지에 내장된 데이터베이스 업데이트
  - 원격 설치 작업 만들기
- 마법사를 사용하여 로컬로 애플리케이션 설치
- System Center Configuration Manager를 사용하여 애플리케이션 원격 설치
- setup.ini 파일 설치 설정 설명
- 애플리케이션 구성 요소 변경
- 이전 버전의 애플리케이션 업그레이드 중
  - 다시 시작 없이 애플리케이션 업그레이드
  - 애플리케이션의 SMU 업데이트
- 애플리케이션 제거

애플리케이션 라이센스
- 최종 사용자 라이센스 계약서 정보
- 라이센스 정보
- 라이센스 인증서 정보
- 서브스크립션 정보
- 라이센스 키 정보
- 활성화 코드 정보
- 키 파일 정보
- 워크스테이션용 라이센스 유형에 따른 애플리케이션 기능 비교
- 서버용 라이센스 유형에 따른 애플리케이션 기능 비교
- 애플리케이션 활성화
- 라이센스 키 제거하기
- 라이센스 정보 보기
- 라이센스 구매
- 서브스크립션 갱신

데이터 제공
- 최종 사용자 라이센스 계약서에 따른 데이터 프로비전
- Kaspersky Security Network 사용 시 데이터 제공

Detection and Response 솔루션 사용 시 데이터 제공
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert(on-premise)
Kaspersky Network Detection and Response(KATA)
Kaspersky Unified Monitoring and Analysis Platform(KUMA)와 통합
유럽 연합 법규(GDPR) 준수
시작하기
Kaspersky Endpoint Security for Windows 관리 플러그인 정보
여러 버전의 관리 플러그인 사용 시의 특별 고려 사항
외부 서비스와 상호 작용하기 위해 암호화된 프로토콜을 사용할 때 특별히 고려해야 할 사항
애플리케이션 인터페이스
작업 표시줄 알림 영역의 애플리케이션 아이콘
간략한 애플리케이션 인터페이스
애플리케이션 인터페이스 표시 구성
애플리케이션 사용 준비
정책 관리
정책 만들기
정책 내보내기 및 가져오기
보안 레벨 표시기
작업 관리
로컬 애플리케이션 설정 구성
Kaspersky Endpoint Security 시작 및 중지
컴퓨터 보호 및 제어 일시 중지 및 다시 시작
구성 파일 만들기 및 사용
애플리케이션 기본 설정 복원
Kaspersky Endpoint Security 성능 및 다른 애플리케이션과의 호환성
절전 모드 작동 또는 중지
다른 애플리케이션에 컴퓨터 리소스 우선권 할당 작동 또는 중지
Kaspersky Endpoint Security 성능 최적화를 위한 모범 사례
악성 코드 검사
컴퓨터 검사
이동식 장치가 컴퓨터에 연결될 때 검사
백그라운드 검사
마우스 오른쪽 메뉴에서 검사
애플리케이션 무결성 검사
검사 범위 편집
스케줄된 검사 실행
다른 사용자로 검사 실행
검사 최적화
데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트
데이터베이스 및 애플리케이션 모듈 업데이트 시나리오
서버 저장소에서 업데이트
공유 폴더에서 업데이트
Kaspersky 업데이트 유틸리티를 사용하여 업데이트
모바일 모드에서 업데이트
업데이트 작업 시작 및 중지

다른 사용자 계정 권한으로 업데이트 작업 시작
업데이트 작업 스케줄 선택
업데이트 경로 추가
애플리케이션 모듈 업데이트
업데이트에 프록시 서버 사용
마지막 업데이트 롤백
고급 치료 기술
워크 스테이션의 처리 안 된 보안위협 치료
서버의 처리 안 된 보안위협 치료
처리되지 않은 위협 제거
컴퓨터 보호
파일 위협 보호
파일 위협 보호 사용 및 중지
파일 위협 보호 자동 일시 중지
파일 위협 보호 구성 요소가 감염된 파일에 수행하는 처리 방법 변경
파일 위협 보호 구성 요소의 보호 범위 구성
검사 방법 사용
파일 위협 보호 동작에 검사 기술 사용
파일 검사 최적화
복합 파일 검사
검사 모드 변경
컨테이너 검사
호스트 침입 방지
호스트 침입 방지 사용 및 중지
애플리케이션 제어 그룹 관리
애플리케이션의 제어 그룹 변경
제어 그룹 권한 구성
Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션에 대한 제어 그룹 선택
알 수 없는 애플리케이션에 대한 제어 그룹 선택
디지털 서명된 애플리케이션에 대한 제어 그룹 선택
애플리케이션 권한 관리
운영 체제 리소스 및 개인 데이터 보호
사용하지 않는 애플리케이션에 대한 정보 삭제
호스트 침입 방지 모니터링
오디오 및 비디오에 대한 접근 보호
BadUSB 공격 방지
BadUSB 공격 방지 사용 및 중지
USB 장치 인증 시 화상 키보드 사용
바코드 스캐너 인증
AMSI 보호
AMSI 보호 사용 및 중지
AMSI 보호로 파일 검사 최적화
웹 위협 보호
웹 위협 보호 사용 및 중지
악성 웹 주소 탐지 방법 구성
안티 피싱

- 신뢰하는 웹 주소 목록 생성
- 신뢰하는 웹 주소 목록 내보내기 및 가져오기

메일 위협 보호
- 메일 위협 보호 사용 및 중지
- 감염된 이메일 메시지에 수행할 처리 방법 변경
- 메일 위협 보호 구성 요소의 보호 범위 구성
- 이메일 메시지에 첨부된 복합 파일 검사
- 이메일 메시지 첨부파일 필터
- 첨부파일 필터링을 위한 확장 프로그램 내보내기 및 가져오기
- Microsoft Office Outlook의 이메일 검사
- Thunderbird, MyOffice, R7-Office에서 이메일 검사

네트워크 위협 보호
- 네트워크 위협 보호 사용 및 중지
- 공격 컴퓨터 차단
- 차단에서 예외할 주소 구성
- 차단 예외 규칙 목록 내보내기 및 가져오기
- 유형별 네트워크 위협 보호 구성

방화벽
- 방화벽 작동 또는 중지
- 네트워크 연결 유형 변경
- 네트워크 패킷 규칙 관리
  - 네트워크 패킷 규칙 생성
  - 네트워크 패킷 규칙 작동 또는 중지
  - 네트워크 패킷 규칙에 대한 방화벽 동작 변경
  - 네트워크 패킷 규칙의 우선 순위 변경
  - 네트워크 패킷 규칙 내보내기 및 가져오기
  - XML에서 네트워크 패킷 규칙 정의
- 애플리케이션 네트워크 규칙 관리
  - 애플리케이션 네트워크 규칙 만들기
  - 애플리케이션 네트워크 규칙 사용 및 중지
  - 애플리케이션 네트워크 규칙에 대한 방화벽 동작 변경
  - 애플리케이션 네트워크 규칙의 우선 순위 변경
- 네트워크 모니터

익스플로잇 방지
- 익스플로잇 방지 사용 및 중지
- 시스템 프로세스 메모리 보호

행동 탐지

Anti-Cryptor
- 외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 사용 및 중지
- 신뢰하지 않는 컴퓨터의 차단 기간 구성
- 보호 범위 편집
- 외부 데이터 암호화를 위해 신뢰하는 컴퓨터 추가
- 외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 시 예외 규칙 목록 내보내기 및 가져오기

복원 엔진

Kaspersky Security Network
- Kaspersky Security Network 사용 활성화 및 비활성화
- Kaspersky Private Security Network의 제한 사항

보호 구성 요소에서 클라우드 모드 사용 및 중지
KSN 프록시 설정
Kaspersky Security Network 내 파일의 평판 확인
암호화된 연결 검사
암호화된 연결 검사 활성화
신뢰할 수 있는 인증서 설치
신뢰할 수 없는 인증서로 암호화된 연결 검사
자체 인증서 저장소에 Kaspersky 인증서 추가
검사에서 암호화된 연결 제외
데이터 완전 삭제
컴퓨터 제어
웹 제어
웹 리소스 접근 규칙 추가
웹 리소스 주소별 필터링
웹 리소스 컨텐츠별 필터링
웹 리소스 접근 규칙 테스트
웹 제어 규칙 내보내기 및 가져오기
웹 제어 규칙의 웹 리소스 주소 내보내기 및 가져오기
사용자 인터넷 활동 모니터링
웹 제어 메시지 템플릿 편집
웹 리소스 주소 마스크 편집
가상 컴퓨터용 웹 제어
웹 제어 메시지 템플릿 변수
장치 제어
접근 규칙 정보
유형별 장치 접근 관리
연결 버스별 장치 접근 관리
장치에 대한 사용자 접근 권한의 구분
모바일 장치에 대한 액세스 관리
Bluetooth 장치에 대한 접근 관리
인쇄 제어
Wi-Fi 연결 제어
이동식 드라이브 사용 감시
캐싱 기간 변경
신뢰하는 장치와 관련된 처리 방법
애플리케이션 인터페이스에서 신뢰하는 목록에 장치 추가
Kaspersky Security Center에서 신뢰하는 목록에 장치 추가
신뢰하는 장치 목록 내보내기 및 가져오기
차단된 장치에 대한 접근 권한 획득
접근 권한 부여를 위한 온라인 모드
접근 권한 부여를 위한 오프라인 모드
장치 제어 메시지 템플릿 편집
안티 브리징
안티 브리징 활성화
연결 규칙 상태 변경
연결 규칙 우선 순위 변경

적응형 이상 행위 제어
적응형 이상 행위 제어 학습
적응형 이상 행위 제어 규칙 작동 및 중지
적응형 이상 행위 제어 규칙 작동 시에 수행되는 처리 수정
적응형 이상 행위 제어 규칙에 대한 예외 규칙 생성
적응형 이상 행위 제어 규칙에 대한 예외 규칙 내보내기 및 가져오기
적응형 이상 행위 제어 규칙용 업데이트 적용
적응형 이상 행위 제어 메시지 템플릿 편집
적응형 이상 행위 제어 작업 모니터링
애플리케이션 제어
애플리케이션 제어 기능 제한
사용자 컴퓨터에 설치된 애플리케이션에 대한 정보 수신
차단된 애플리케이션 모드를 활성화하는 방법
베이스라인 컴퓨터 기반 애플리케이션 제어
애플리케이션 제어 규칙 관리
애플리케이션 제어 규칙의 트리거 조건 추가
실행 파일 폴더에서 애플리케이션 카테고리로 실행 파일 추가
애플리케이션 카테고리에 이벤트 관련 실행 파일 추가
애플리케이션 제어 규칙 추가
Kaspersky Security Center를 사용해 애플리케이션 제어 규칙의 상태 변경
애플리케이션 제어 규칙 내보내기 및 가져오기
애플리케이션 제어 구성 요소의 동작에서 이벤트 결과 보기
차단된 애플리케이션 리포트 보기
애플리케이션 제어 규칙 테스트
애플리케이션 제어 규칙 테스트 활성화 및 비활성화
테스트 모드에서 차단된 애플리케이션 리포트 보기
애플리케이션 제어 구성 요소의 테스트 동작에서의 이벤트 결과 보기
애플리케이션 활동 모니터
파일 또는 폴더에 대한 이름 마스크 생성 규칙
애플리케이션 제어 메시지 템플릿 편집
애플리케이션 제어 메시지 템플릿 변수
허용된 애플리케이션 목록 구현의 모범 사례
애플리케이션에 대한 허용 목록 모드 구성
허용 목록 모드 테스트
허용 목록 모드 지원
네트워크 포트 모니터링
모든 네트워크 포트의 감시 작동
감시하는 네트워크 포트 목록 만들기
모든 네트워크 포트에 대한 감시를 받을 애플리케이션 목록 만들기
모니터링하는 포트 목록 내보내기 및 가져오기
로그 검사
사전 정의된 규칙 구성
사용자 지정 규칙 추가
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
- 시스템 무결성 상태 재설정
- Cloud Discovery

신뢰 구역
- 검사 예외 생성
- 탐지된 개체 유형별 예외 생성
- 신뢰하는 애플리케이션 목록 편집
- 로컬 신뢰 구역 생성
- 신뢰 구역 내보내기 및 가져오기
- 신뢰하는 디지털 서명으로 애플리케이션 처리
- 부록. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션
  - SQL 서버
  - Microsoft Exchange 서버
  - System Center Configuration Manager
  - Citrix
  - VMware

백업 저장소 관리
- 백업 저장소에 저장된 파일의 최대 저장 기간 구성
- 백업 저장소 최대 크기 구성
- 백업 저장소에서 파일 복원
- 백업 저장소에서 파일의 백업 복사본 삭제

알림 서비스
- 이벤트 로그 설정 구성
- 알림 표시 및 전달 구성
- 알림 영역의 애플리케이션 상태에 대한 경고 표시 구성
- 사용자와 관리자 간의 메시지

리포트 관리
- 리포트 보기
- 최대 리포트 저장 기간 구성
- 리포트 파일의 최대 크기 구성
- 파일에 리포트 저장
- 리포트 파일 삭제

Kaspersky Endpoint Security 자기 보호 기능
- 자기 보호 기능 작동 및 중지
- AM-PPL 지원 활성화 및 비활성화
- 외부 관리로부터 애플리케이션 서비스 보호
- 원격 관리 애플리케이션 지원
- 암호 보호
  - 암호 보호 사용
  - 개별 사용자 또는 그룹에 사용 권한 부여
  - 임시 암호를 사용해 권한 부여
  - 임시 암호 폐기
  - 암호 보호 권한의 특별한 점
  - KLAdmin 암호 재설정
- 중앙 관리 서버 연결 보호

데이터 암호화
- 암호화 기능 제한
- 암호화 키 길이 변경하기(AES56 / AES256)
- Kaspersky 디스크 암호화
  - SSD 드라이브 암호화의 특징
  - Kaspersky 디스크 암호화 시작
  - 암호화에서 제외할 하드 드라이브의 목록 작성
  - 암호화에서 제외할 하드 드라이브 목록 내보내기 및 가져오기
  - Single Sign-On(SSO) 기술 사용
  - 인증 에이전트 계정 관리
  - 인증 에이전트에서 토큰 및 스마트 카드 사용
  - 하드 드라이브 복호화
  - Kaspersky 디스크 암호화 기술로 보호되는 드라이브에 대한 접근 복원
  - 인증 에이전트 서비스 계정으로 로그인
  - 운영 체제 업데이트
  - 암호화 기능 업데이트의 오류 방지
  - 인증 에이전트 추적
  - 인증 에이전트 도움말 텍스트 편집
  - 인증 에이전트의 작동을 테스트한 후 남은 개체 및 데이터 제거
- BitLocker 관리
  - BitLocker 드라이브 암호화 시작
  - BitLocker로 보호되는 하드 드라이브 복호화
  - BitLocker로 보호되는 드라이브에 대한 접근 복원
  - 소프트웨어 업데이트를 위해 BitLocker 보호 일시 중지
- 로컬 컴퓨터 드라이브에 대한 파일 레벨 암호화
  - 로컬 컴퓨터 드라이브의 파일 암호화
  - 애플리케이션의 암호화된 파일 접근 규칙 작성
  - 특정 애플리케이션에서 만들어졌거나 수정된 파일 암호화
  - 복호화 규칙 생성
  - 로컬 컴퓨터 드라이브의 파일 복호화
  - 암호화 패키지 생성
  - 암호화된 파일에 대한 접근 복원
  - 운영 체제에 장애가 발생한 후 암호화된 데이터에 대한 접근 복원
  - 암호화된 파일 접근 메시지 템플릿 편집
- 이동식 드라이브 암호화
  - 이동식 드라이브 암호화 시작
  - 이동식 드라이브에 대한 암호화 규칙 추가
  - 이동식 드라이브에 대한 암호화 규칙 목록 내보내기 및 가져오기
  - 이동식 드라이브의 암호화된 파일 접근을 위한 휴대용 모드
  - 이동식 드라이브의 복호화
- 데이터 암호화 상세 정보 보기
  - 암호화 상태 보기
  - Kaspersky Security Center 대시보드에서 암호화 통계 보기
  - 로컬 컴퓨터 드라이브의 파일 암호화 오류 보기
  - 데이터 암호화 리포트 보기

암호화된 장치에 접근할 수 없는 경우 장치 사용
FDERT 복원 유틸리티를 사용하여 데이터 복원
운영 체제 응급 복구 디스크 만들기
Detection and Response 솔루션
MDR 및 EDR Optimum 라이센스
타사 EDR 솔루션과의 호환성
Kaspersky Endpoint Agent
[KES+KEA] 구성을 [KES+내장 에이전트] 구성으로 마이그레이션
Kaspersky Endpoint Agent의 정책 및 작업 마이그레이션
Endpoint Detection and Response Agent(EDR Agent)
EDR Agent 설치
EDR Agent를 MDR과 통합
EDR Agent를 EDR(KATA)와 통합
EDR Agent를 NDR(KATA)와 통합
EDR Agent를 EDR Expert(on-premise)와 통합
타사 EPP 애플리케이션과의 호환성
Managed Detection and Response
MDR과 내장 에이전트 통합
MDR용 KEA에서 KES로의 마이그레이션 가이드
Endpoint Detection and Response
EDR Optimum / EDR Expert와 내장 에이전트 통합
침해지표 검사(표준 작업) 검사
IOC 검사를 위한 확장 원격 측정
격리 저장소로 파일 이동
파일 가져오기
파일 삭제
프로세스 시작
프로세스 종료
실행 방지
컴퓨터 네트워크 격리
Cloud Sandbox
EDR Optimum용 KEA에서 KES로의 마이그레이션 가이드
Kaspersky Sandbox
Kaspersky Sandbox와 내장 에이전트 통합
침해 지표 검사(독립 실행형 작업)
Kaspersky Sandbox용 KEA에서 KES로의 마이그레이션 가이드
Kaspersky Anti Targeted Attack Platform
EDR / NDR (KATA)와 내장 에이전트 통합
EDR(KATA) 원격 측정 구성
EDR(KATA) 원격 측정 예외
예 1. 제외된 프로세스
예 2. 제외된 네트워크 통신
예 3. 제외된 파일 작업
예 4. 제외된 레지스트리 수정

KATA Sandbox
KATA Sandbox와 내장 에이전트 통합
보안 위협 대응 활동 구성
EDR(KATA)용 KEA에서 KES로의 마이그레이션 가이드
Endpoint Detection and Response Expert(on-premise)
EDR Expert(on-premise)와 내장 에이전트 통합
EDR Expert(on-premise) 원격 측정 설정 구성
EDR Expert(on-premise) 원격 측정 예외
EDR Expert(on-premise) 이벤트 필터 내보내기 및 가져오기
격리 저장소 관리
격리 저장소 최대 크기 구성
격리된 파일에 대한 데이터를 Kaspersky Security Center로 전송
격리 저장소에서 파일 복원
EDR 동작 모니터링
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Kaspersky Endpoint Security와 KUMA 통합
KUMA로 전송할 이벤트 필터링
KUMA 이벤트 필터 내보내기 및 가져오기
KSWS에서 KES로의 마이그레이션 가이드
KSWS 및 KES 구성 요소의 대응
KSWS 및 KES 설정의 대응
KSWS 구성 요소 마이그레이션
KSWS 작업 및 정책 마이그레이션
KSWS 신뢰 구역 마이그레이션
KSWS 애플리케이션 실행 제어 규칙 마이그레이션
KSWS 대신 KES 설치
[KSWS+KEA] 구성을 [KES+내장 에이전트] 구성으로 마이그레이션
Kaspersky Security for Windows Server가 성공적으로 제거되었는지 확인
KSWS 키로 KES 활성화
부하가 높은 서버 마이그레이션을 위한 특별 고려 사항
Server Core 모드에서 서버의 애플리케이션 관리
[KSWS+KEA]을 [KES+내장 에이전트]로 마이그레이션
가상 컴퓨터를 보호하는 Light Agent 모드
Light Agent 모드에 대한 특별 고려 사항
가상 컴퓨터 사전 구성
Citrix App Layering 기술과의 호환성
Citrix Provisioning(Citrix Provisioning Services) 기술과의 호환성
Omnissa App Volumes 기술과의 호환성
Light Agent 설치
Light Agent를 SVM에 연결
SVM 검색
Light Agent용 SVM 선택 알고리즘 구성
Light Agent와 SVM 연결 배포(태그)
Light Agent와 SVM 간의 연결 보호
Light Agent 활성화

KSVLA Light Agent에서 KES Light Agent로의 마이그레이션 가이드
KSVLA Light Agent 대신 KES Light Agent 설치
KSVLA Light Agent 및 KES Light Agent 구성 요소의 대응
KSVLA Light Agent 작업 및 정책 마이그레이션
[KSVLA Light Agent+KEA] 구성을 [KES Light Agent+내장 에이전트] 구성으로 마이그레이션
명령줄로 애플리케이션 관리
Setup. 애플리케이션 설치
Setup /x. 애플리케이션 제거
msiexec /i. 애플리케이션 복구
AVP 명령
SCAN. 악성 코드 검사
UPDATE. 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트
ROLLBACK. 마지막 업데이트 롤백
TRACES. 추적 로그
START. 프로필 시작
STOP. 프로필 중지
STATUS. 프로필 상태
STATISTICS. 프로필 동작 통계
RESTORE. 백업 저장소에서 파일 복원
EXPORT. 애플리케이션 설정 내보내기
IMPORT. 애플리케이션 설정 가져오기
ADDKEY. 키 파일 적용
LICENSE. 라이센스
RENEW. 라이센스 구매
PBATESTRESET. 디스크를 암호화하기 전에 디스크 검사 결과 재설정
EXIT. 애플리케이션 종료
EXITPOLICY. 정책 사용 안 함
STARTPOLICY. 정책 사용
DISABLE. 보호 중지
SPYWARE. 스파이웨어 탐지
KSN. KSN/KPSN 간 전환
SERVERBINDINGDISABLE. 서버 연결 보호 중지
KESCLI 명령
Scan. 악성 코드 검사
GetScanState. 검사 완료 상태
GetLastScanTime. 검사 완료 시간 확인
GetThreats. 삭제한 보안위협에 대한 데이터 불러오기
UpdateDefinitions. 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트
GetDefinitionState. 데이터베이스의 마지막 업데이트 날짜 및 시간 확인
EnableRTP. 보호 활성화
GetRealTimeProtectionState. 파일 위협 보호 상태
GetEncryptionState. 디스크 암호화 상태
Version. 애플리케이션 버전 확인
Detection and Response management 명령
SANDBOX. Sandbox 관리
PREVENTION. 실행 방지 관리
ISOLATION. 네트워크 격리 관리

RESTORE. 격리 저장소에서 파일 복원
IOCSCAN. 침해지표(IOC) 검사
MDRLICENSE. MDR 활성화
EDRKATA. EDR(KATA)과의 통합
KUMA. KUMA과 통합
YARA. YARA 검사 실행
TELEMETRYFILTERS. KUMA로 전송할 이벤트 필터링
Light Agent 관리 명령
KSVLAINFO. Light Agent 모드 확인
VIISINFO. 통합 서버에 대한 Light Agent 연결 상태
SVMINFO. 보호 서버에 대한 Light Agent 연결 상태
오류 코드
부록. 애플리케이션 프로필
REST API를 사용해 애플리케이션 관리
REST API를 사용해 애플리케이션 설치
API를 사용해 작업 수행
애플리케이션에 대한 정보 출처
기술 지원 서비스에 문의
추적 파일의 내용 및 저장
애플리케이션 동작 추적 로그
애플리케이션 성능 추적 로그
덤프 기록
덤프 파일 및 추적 파일 보호
OS 데이터 가져오기(Kaspersky Get System Info)
제한 및 경고
용어집
Cloud Discovery
IOC
IOC 파일
Kerberos 인증
Light Agent
OLE 개체
OpenIOC
SVM
감염 가능성이 있는 파일
감염된 파일
검사 범위
관리 그룹
네트워크 에이전트
라이센스 인증서
마스크
보호 범위
신뢰하는 플랫폼 모듈
악성 웹 주소 데이터베이스
안티 바이러스 데이터베이스
압축 파일
인증 에이전트

- 인증서 발급자
- 작업
- 정규화된 형태의 웹 리소스 주소
- 치료
- 통합 서버
- 피싱 웹 주소 데이터베이스
- 허위 경보
- 활성 키
- 휴대용 파일 관리자

부록

- 부록 1. 애플리케이션 설정
  - 파일 위협 보호
  - 웹 위협 보호
  - 메일 위협 보호
  - 네트워크 위협 보호
  - 방화벽
  - BadUSB 공격 방지
  - AMSI 보호
  - 익스플로잇 방지
  - 행동 탐지
  - 호스트 침입 방지
  - 복원 엔진
  - Kaspersky Security Network
  - 로그 검사
  - Anti-Cryptor
  - 웹 제어
  - 장치 제어
  - 애플리케이션 제어
  - 적응형 이상 행위 제어
  - 시스템 무결성 모니터링
  - Endpoint Sensor
  - Sandbox
  - Managed Detection and Response
  - Endpoint Detection and Response
  - Endpoint Detection and Response Expert(on-premise)
  - Network Detection and Response(KATA)
  - KUMA과 통합
  - 전체 디스크 암호화
  - 파일 레벨 암호화
  - 이동식 드라이브 암호화
  - 템플릿(데이터 암호화)
  - 예외 규칙
  - 애플리케이션 설정
  - 리포트 및 저장소
  - 네트워크 설정
  - 인터페이스

- 설정 관리
- 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트

부록 2. 애플리케이션 제어 그룹

부록 3. 빠른 이동식 드라이브 검사를 위한 파일 확장자

부록 4. 메일 위협 보호 첨부파일 필터의 파일 유형

부록 5. 외부 서비스와의 상호 작용을 위한 네트워크 설정

부록 6. 애플리케이션 이벤트

- 심각
- 기능 실패
- 경고
- 정보 메시지

부록 7. 지원하는 실행 방지 파일 확장자

부록 8. 실행 방지에서 지원되는 스크립트 인터프리터

부록 9. 레지스트리에서의 IOC 검사 범위(RegistryItem)

부록 10. IOC 파일 요구 사항

부록 11. 애플리케이션 구성 요소 규칙의 사용자 계정

부록 12. EDR 위협 대응을 위한 API

타사 코드에 대한 정보

상표 고지

Kaspersky Endpoint Security for Windows 도움말

새로운 기능

14.0 업데이트

Kaspersky Endpoint Security 14.0 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. 이제 Arm 기반 컴퓨터가 지원됩니다. 표준 모드 또는 EDR 에이전트 모드로 애플리케이션을 설치할 수 있습니다. 단, 애플리케이션에는 몇 가지 제한(예: 데이터 암호화 기술 중 BitLocker만 지원)이 있습니다.

2. 확장 정책 감사는 Kaspersky Security Center 웹 콘솔 15.0 버전 이상에서 지원됩니다. 이제 정책 수정 사항을 확인하고 파일에 저장할 수 있습니다. *수정본*은 사용자가 저장한 수정된 파라미터 값의 집합입니다. 수정본을 사용하면 정책 파라미터의 변경 사항을 비교하고 되돌릴 수 있습니다.

3. 이제 Kaspersky Endpoint Detection and Response 사용자는 새로운 원격 측정 이벤트를 사용할 수 있습니다. 이러한 새로운 이벤트는 Kaspersky EDR 솔루션의 위협 탐지 기능을 강화합니다.

4. 이 버전의 Kaspersky Endpoint Security for Windows를 개발할 때 다음 비공개 패치에 포함된 변경 사항을 통합했습니다: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051 , PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

12.12 업데이트

Kaspersky Endpoint Security 12.12 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. 행동 탐지 구성 요소의 일부였던 외부 암호화로부터 공유 폴더 보호가 이제는 별도의 구성 요소인 Anti-Cryptor입니다.

2. 인터넷 접근용 프록시 서버를 통해 애플리케이션을 인증할 수 있도록 Kerberos 프로토콜 지원이 추가되었습니다.

3. 이제 전체 경로가 아닌 신뢰하는 애플리케이션의 파일 해시를 지정할 수 있습니다.

4. Endpoint Detection and Response(EDR) 솔루션 사용자는 더 많은 더 *IOC 검사* 작업 기능을 사용할 수 있습니다. 이제 회고적 IOC 검사 기능을 사용할 수 있습니다. *회고적 IOC 검사*는 Kaspersky Endpoint Security가 특정 기간의 데이터를 사용하여 침해 지표를 검사하는 *IOC 검사* 작업의 모드 중 하나입니다. 이 모드는 컴퓨터의 네트워크 활동 데이터에서 침해 지표를 탐지하기 위한 것입니다. Kaspersky Endpoint Security가 컴퓨터에 설치된 운영 체제 로그 및 브라우저 로그의 데이터를 분석합니다.

5. Kaspersky Endpoint Detection and Response(EDR) 사용자는 격리 저장소 크기 제한을 제거할 수 있습니다. 이는 애플리케이션이 대규모 메모리 덤프 파일을 저장할 수 있기 때문에 YARA 검사에 필요할 수 있습니다. 이제 사용 가능한 디스크 공간을 모두 격리 저장소에 사용할 수 있습니다.

6. 이제 Kaspersky Unified Monitoring and Analysis Platform(KUMA)으로 이벤트 내보내기를 최적화할 수 있도록 HTTPS 압축이 지원됩니다. 이는 나가는 트래픽을 줄이는 데 도움이 됩니다.

7. 이 버전의 Kaspersky Endpoint Security for Windows를 개발할 때 다음 비공개 패치에 포함된 변경 사항을 통합했습니다: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051 , PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

12.11 업데이트

Kaspersky Endpoint Security 12.11 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. 애플리케이션은 설정을 저장하기 전에 제어 구성 요소의 구성을 확인합니다. 애플리케이션 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 제어의 경우, 허용한 애플리케이션을 제외한 모든 애플리케이션을 차단하는 모드를 선택하고 허용 규칙을 추가하지 않으면 이러한 구성이 시스템 오류를 유발할 수 있으므로 애플리케이션에서 경고를 표시합니다.

2. 검토를 위해 KATA Sandbox에 파일 자동 제출 지원을 추가했습니다. *KATA Sandbox*는 운영 체제의 가상 이미지에서 파일을 실행하는 Kaspersky Anti Targeted Attack Platform의 구성 요소입니다. Sandbox는 조직의 IT 인프라에 대한 표적 공격의 활동 특성 및 악성 활동 탐지를 위해 개체 행동을 분석합니다. Sandbox는 Microsoft Windows 운영 체제(Sandbox 서버)의 가상 이미지가 배포된 특수 서버의 개체를 분석하고 검사합니다. KATA Sandbox가 자동 모드에서 작동하려면 Kaspersky Anti Targeted Attack Platform 8.0 이상이 배포되어야 합니다.

3. EDR 원격 측정 전송을 최적화했습니다. 이제 최대 패킷 길이를 지정할 수 있습니다.

4. Kaspersky Security Network에 대한 연결 진단을 개선했습니다. 잠재적 문제를 해결하기 위해 Kaspersky Security Network의 연결 오류 세부 정보를 더욱 자세히 제공합니다.

5. Kaspersky Unified Monitoring and Analysis Platform(KUMA)으로 전송할 이벤트 목록 구성에 대한 지원이 추가되었습니다. 이제 KUMA 내 사전 정의된 이벤트 목록 외에도, 원격 측정에 이벤트를 수동으로 추가하거나 Windows 이벤트 로그에서 ID별로 이벤트를 제외할 수 있습니다.

6. 웹 콘솔의 정책 인터페이스를 업데이트했습니다. 정책 섹션의 레이아웃이 변경되어 필수 기능에 더 빠르게 접근할 수 있습니다.

7. Windows 11 25H2 지원

8. 이 버전의 Kaspersky Endpoint Security for Windows를 개발할 때 다음 비공개 패치에 포함된 변경 사항을 통합했습니다: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

12.10 업데이트

Kaspersky Endpoint Security 12.10 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. BadUSB 공격 방지 구성 요소에 화면에서 바코드를 읽어 바코드 스캐너를 인증하는 옵션이 추가되었습니다. 이제 바코드 스캐너 인증을 위해 화상 키보드로 코드를 입력할 필요가 없습니다.

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

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

   - 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.

3. 새 항목 암호 보호 권한인 *설정 내보내기*를 추가했습니다. 기본적으로 KLAdmin 사용자만 애플리케이션 인터페이스에서 Kaspersky Endpoint Security 설정을 사용하여 구성 파일을 생성할 수 있습니다. 다른 사용자에게 접근 권한을 부여하려면 해당 사용자에게 해당하는 권한을 부여해야 합니다.

4. 이 버전의 Kaspersky Endpoint Security for Windows를 개발할 때 다음 비공개 패치에 포함된 변경 사항을 통합했습니다: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

12.9 업데이트

Kaspersky Endpoint Security 12.9 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. *임시 암호 관리*를 위한 새로운 기능이 추가되었습니다. 임시 암호를 사용하면 암호 보호 활성화 상태로 별도의 컴퓨터에서 Kaspersky Endpoint Security에 접근할 수 있습니다. 임시 암호 관리는 암호 내역을 저장하고(최대 30일), 임시 암호 상태를 모니터링하고(*활성*, *만료됨*, *폐기됨*), 임시 암호를 폐기합니다.

2. 웹 제어 규칙이 금지하는 웹 리소스에 대한 연결을 정책이 적용된 직후에 종료하는 옵션이 추가되었습니다. 이전 버전의 애플리케이션에서는 웹 제어가 금지된 웹 리소스에 대한 새로운 연결만 제한했습니다.

3. Kaspersky Anti Targeted Attack Platform 사용자를 위해 컴퓨터에서 로컬로 YARA 검사를 실행하는 옵션이 추가되었습니다. 이렇게 하려면 YARA 규칙이 있는 파일을 다운로드하고 CMD에서 명령을 실행해야 합니다.

4. 타사 도구를 사용하여 드라이브가 이미 BitLocker로 보호됨 컴퓨터에서 BitLocker를 사용할 때 애플리케이션의 행동을 수정했습니다. Kaspersky Endpoint Security가 복구 절차를 시작하여 복구 키를 Kaspersky Security Center로 전송합니다. 따라서 BitLocker 관리는 Kaspersky Security Center 콘솔로 이전됩니다.

5. Kaspersky의 Detection and Response 솔루션 사용자에게 새로운 **응답 이력** 섹션이 제공됩니다. 이 섹션은 컴퓨터가 수행한 보안 위협 대응 활동의 정보를 담고 있습니다. 해당 활동에는 예시로는 *프로세스 종료* 작업을 실행하는 것이나 네트워크에서 컴퓨터를 격리하는 것이 포함됩니다. 응답 이력은 Kaspersky의 MDR, EDR, KATA 솔루션 사용자에게만 제공됩니다.

6. Kaspersky Unified Monitoring and Analysis Platform 사용자는 현재 EDR 보안 위협 대응 활동 지원이 이용 가능합니다. 위협 대응 시 KUMA는 해당하는 EDR 작업을 생성하는 스크립트를 실행합니다. EDR 작업을 수행하려면 KUMA 콘솔에서 사용자 지정 스크립트의 대응 규칙을 생성한 후 이벤트를 선택해야 합니다.

7. 이 버전의 Kaspersky Endpoint Security for Windows를 개발할 때 다음 비공개 패치에 포함된 변경 사항을 통합했습니다: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

12.8 업데이트

Kaspersky Endpoint Security 12.8 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. 애플리케이션은 이제 가상 환경 보호를 위한 Light Agent 모드를 지원합니다. 이제 Kaspersky Security for Virtualization Light Agent 6.2 솔루션의 일부로 Light Agent로 애플리케이션을 배포할 수 있습니다.

2. 이제 서버에서 Docker 컨테이너에서 파일 동작 가로채기가 지원됩니다. *컨테이너*는 운영 체제와 직접 상호작용하지 않고 애플리케이션을 실행할 수 있는 격리된 환경입니다. Kaspersky Endpoint Security는 사용자가 접근 권한을 가지고 있는 컨테이너 내의 파일을 검사합니다. 위협이 탐지되면 애플리케이션은 이 악성 활동을 차단하고 컨테이너 내의 파일을 치료하려고 시도합니다. 파일을 치료할 수 없는 경우 애플리케이션이 컨테이너를 중지합니다.

3. 이제 외부 암호화로부터 공유 폴더 보호에 대한 보호 범위를 정의할 수 있습니다(행동 탐지 구성 요소). 이제 애플리케이션이 파일 활동을 모니터링해야 하는 공유 폴더를 지정할 수 있습니다. 보호 범위에서 파일을 제외할 수도 있습니다. 이전 버전의 애플리케이션에서는 행동 탐지 구성 요소가 모든 공유 폴더의 파일 활동을 모니터링했습니다.

4. 이제 설치 패키지에서 다양한 운영 체제 유형에 대해 다양한 구성 요소 집합을 구성할 수 있습니다. 즉, 동일한 설치 패키지를 사용하여 워크스테이션과 서버에 애플리케이션을 배포할 수 있습니다. 특정 운영 체제 유형에서 사용할 수 없는 구성 요소는 설치 패키지 속성에서 자동으로 제외됩니다.

5. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 선택할 수 있는 옵션이 추가되었습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 가상 환경(Citrix, VMware)에서 애플리케이션에 대한 신뢰 구역을 빠르게 구성할 수 있습니다. 이러한 예외 규칙은 예를 들어 VHD 및 VHDX 가상 컴퓨터 파일이 포함됩니다. 애플리케이션 설치 패키지를 생성하거나 정책을 만들 때 또는 Kaspersky Endpoint Security 설치 시 예외 규칙을 추가할 수 있습니다.

6. 이제 EDR 원격 측정에 USB 연결 장치 작업을 위한 이벤트가 포함됩니다. 이러한 이벤트를 EDR 원격 측정 예외에 추가할 수도 있습니다.

7. 오래된 TLS 1.0 프로토콜을 통한 네트워크 연결을 차단하기 위한 옵션이 추가되었습니다. TLS 1.0은 보안 레벨이 낮기 때문에 이 프로토콜을 비활성화하고 최신 TLS 1.2 또는 TLS 1.3 버전을 사용하는 것이 좋습니다. 기본적으로 Kaspersky Endpoint Security는 TLS 1.0 연결을 차단합니다. 애플리케이션 버전을 업데이트하면 TLS 1.0 프로토콜을 사용하는 타사 서비스가 작동하지 않을 수 있습니다. 타사 서비스의 작동 문제를 방지하려면 애플리케이션 버전을 업데이트하기 전에 그룹 정책에서 TLS 1.0 프로토콜 사용을 허용하셔도 됩니다.

8. 이 버전의 Kaspersky Endpoint Security for Windows를 개발할 때 다음 비공개 패치에 포함된 변경 사항을 통합했습니다. PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

12.7 업데이트

Kaspersky Endpoint Security 12.7 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. 이제 *악성 코드 검사* 작업의 CPU 리소스 사용량을 제한할 수 있습니다. 이렇게 하려면 애플리케이션 설정에서 컴퓨터 검사 중에 활용할 수 있는 모든 코어에 대한 최대 CPU 로드를 퍼센트로 지정합니다.

2. 이제 수동으로 KATA Sandbox에서 검사를 위해 파일을 전송할 수 있습니다. *KATA Sandbox*는 운영 체제의 가상 이미지에서 파일을 실행하는 Kaspersky Anti Targeted Attack Platform의 구성 요소입니다. Sandbox는 조직의 IT 인프라에 대한 표적 공격의 활동 특성 및 악성 활동 탐지를 위해 개체 행동을 분석합니다. Sandbox는 Microsoft Windows 운영 체제(Sandbox 서버)의 가상 이미지가 배포된 특수 서버의 개체를 분석하고 검사합니다. 검사할 파일을 KATA Sandbox로 보내려면 파일의 마우스 오른쪽 메뉴에서 관련 명령을 선택합니다.

3. 이제 기업 LAN을 보호하는 솔루션인 *Kaspersky Network Detection and Response*와의 통합을 설정할 수 있습니다. Kaspersky Network Detection and Response(NDR)는 Kaspersky Anti Targeted Attack Platform의 일부입니다. 표준 모드 및 EDR Agent 모드에서 NDR과의 상호 작용을 구성할 수 있습니다.

4. 메일 위협 보호 확장 프로그램에 Microsoft Office Outlook 이메일 클라이언트 버전 2021에 대한 지원이 추가되었습니다. 확장 프로그램을 사용하면 프로토콜 수준이 아닌 메일 클라이언트 수준에서 메시지를 검색할 수 있습니다. 메시지 외에도 확장 프로그램을 사용하면 Microsoft Exchange 리포지토리에서 MAPI 인터페이스를 통해 받은 개체(예: 캘린더 내 개체)를 검색할 수 있습니다. 메일 클라이언트에서 이 검색이 수행됩니다.

5. Kaspersky Endpoint Security for Windows 버전을 개발할 때 비공개 패치(PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007)에 포함된 변경 사항을 통합했습니다.

12.6 업데이트

Kaspersky Endpoint Security 12.6 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. Kaspersky SIEM 솔루션*(Kaspersky Unified Monitoring and Analysis Platform(KUMA))*과의 통합 기능이 추가되었습니다. 이제 Windows 이벤트 로그에서 KUMA 수집기로 이벤트를 전송할 수 있습니다. 이렇게 하면 KUMA가 Kaspersky Endpoint Security가 설치된 모든 컴퓨터에서 KUMA 에이전트를 설치하지 않고 Windows 이벤트(일부의 EventID 집합 지원)를 수신할 수 있습니다.

2. 파일 무결성 모니터 구성 요소를 교체하기 위해 *시스템 무결성 모니터링*이 추가되었습니다. 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 Endpoint Security는 해당 이벤트를 생성하고 관리자에게 알립니다. 파일 무결성 모니터는 더 이상 애플리케이션에 포함되지 않습니다. 애플리케이션을 업데이트하면 파일 무결성 모니터 설정이 자동으로 시스템 무결성 모니터링으로 마이그레이션됩니다. 시스템 무결성 모니터링이 제대로 작동하려면 Kaspersky Endpoint Security 애플리케이션과 관리 플러그인 모두가 버전 12.6으로 업데이트되어야 합니다.

3. 설치된 내장 EDR Agent(KATA)의 상태가 Kaspersky Security Center 콘솔의 컴퓨터 속성에 추가되었습니다. 이제 내장 EDR Agent(KATA)가 설치되어 있다면 **Endpoint Sensor 상태** 열에 구성 요소의 현재 상태(예: *실행 중*, *중지됨*, *라이센스가 지원하지 않음* 등)가 표시됩니다.

4. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 선택할 수 있는 옵션이 추가되었습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 애플리케이션을 활용할 경우 신뢰하는 영역을 빠르게 구성할 수 있습니다. 이러한 예외 규칙은 예를 들어 MDF 및 LDF 데이터베이스 파일이 포함됩니다. 새 정책을 생성하거나 기존 정책 수정 시 또는 Kaspersky Endpoint Security 설치 시 예외 규칙이 추가될 수 있습니다.

5. Kaspersky Endpoint Detection and Response Optimum의 경고 세부 정보 표시가 Kaspersky Endpoint Security 관리 플러그인에서 별도의 Kaspersky Endpoint Detection and Response 관리 플러그인으로 이동되었습니다. EDR 관리 플러그인은 Windows, Mac 및 Linux 운영 체제에서 에이전트 작업을 위한 단일 플러그인입니다. 이제 EDR Optimum으로 작업할 때 보안 위협 대응 작업을 만들려면 Kaspersky Endpoint Security 관리 플러그인이 필요하고 경고 세부 정보를 보려면 EDR 관리 플러그인이 필요합니다.

6. Windows 11 24H2 지원

7. Kaspersky Endpoint Security for Windows 버전을 개발할 때 비공개 패치(pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002)에 포함된 변경 사항을 통합했습니다.

12.5 업데이트

Kaspersky Endpoint Security 12.5 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. 원격 측정 예외 규칙을 관리하는 옵션이 추가되었습니다. *원격 측정*은 보호된 컴퓨터에서 발생한 이벤트 목록입니다. 원격 측정 데이터는 Kaspersky Anti Targeted Attack Platform(EDR)에서 조직의 IT 인프라를 모니터링하고 보호하기 위해 사용됩니다. 원격 측정 예외 규칙 구성으로 컴퓨터 성능을 개선하고 원격 측정 수집 서버로의 데이터 전송을 최적화할 수 있습니다.

2. 애플리케이션의 신뢰 구역 인터페이스가 개선되었습니다. 사용자가 자신의(로컬) 검사 예외 및 신뢰하는 애플리케이션을 추가하지 못하도록 관리자가 금지한 경우, Kaspersky Endpoint Security는 사용자로부터 신뢰 구역 개체를 숨깁니다. 이는 침입자가 신뢰 구역에 무단으로 액세스하는 것을 방지하여 컴퓨터 보안 수준을 높일 수 있습니다.

3. MyOffice Mail 및 R7-Office Organizer 메일 클라이언트에 대한 트래픽을 검색하는 옵션이 추가되었습니다. 이제 메일 위협 보호 구성 요소는 다운로드 시 메시지 첨부 파일뿐만 아니라 주고받은 메시지도 검사합니다.

4. 웹 리소스 *생성형 AI 도구*의 새 카테고리가 추가되었습니다. 웹 제어를 사용하여 새 카테고리의 웹사이트에 대한 접근을 구성할 수 있습니다.

5. 이제 방화벽 목록에서 네트워크 패킷 규칙의 위치를 선택할 수 있습니다. 목록에서의 네트워크 패킷 규칙 위치가 우선순위를 결정합니다. 이전 버전의 애플리케이션에서는 새 규칙을 목록의 끝에 추가할 수만 있었으며, 그 후에는 목록에서 규칙을 직접 이동하여 우선순위를 지정해야 했습니다. 이제 규칙을 추가할 때 규칙을 목록의 시작, 끝 또는 선택한 규칙 옆에 배치할지 선택할 수 있습니다.

6. Kaspersky Endpoint Security 구성 요소의 규칙에 따라 이제 Active Directory뿐만 아니라 Kaspersky Security Center의 사용자 목록에서도 사용자를 선택할 수 있습니다. 로컬 사용자 계정 데이터를 직접 입력할 수도 있습니다. 이러한 수동 입력 기능은 애플리케이션 제어, 장치 제어, 웹 제어, 적응형 이상 행위 제어, 로그 검사 등과 같은 구성 요소의 규칙에 추가되었습니다.

7. 이제 네트워크 공격 탐지 리포트에는 공격하는 컴퓨터의 MAC 주소(네트워크 위협 보호 구성 요소)가 있는 열이 포함됩니다. 이제 리포트에서 공격 컴퓨터의 IP 주소 외에 MAC 주소도 확인할 수 있습니다. 이는 인시던트 조사에 유용합니다. 공격하는 컴퓨터의 MAC 주소를 포함한 리포트 또한 Kaspersky Security Center Linux 콘솔 버전 15.1 이상 버전에서 이용 가능합니다.

8. 컴퓨터 보호 요구 레벨이 높아졌습니다. 높은 보호 레벨을 위해서는 외부 관리로부터 애플리케이션 서비스 보호를 활성화해야 합니다. 정책 창 상단에서 보안 레벨 표시기를 확인하세요. 보안 레벨이 중간 또는 낮음일 경우, 보안 레벨 표시기 권장 사항 창에서 외부 관리로부터 애플리케이션 서비스 보호를 활성화할 수 있습니다.

9. 애플리케이션이 Endpoint Detection and Response Agent(EDR Agent) 구성에서 실행 중일 때 신규 개체 탐지 이벤트 지원이 추가되었습니다. 이러한 이벤트는 [KES+내장 에이전트] 구성에서 이미 지원되고 있습니다.

10. Kaspersky Endpoint Security for Windows 버전을 개발할 때 비공개 패치(pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013)에 포함된 변경 사항을 통합했습니다.

12.4 업데이트

Kaspersky Endpoint Security 12.4 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. Kaspersky Security Center에 컴퓨터가 연결되는 것을 보호하기 위한 새로운 기능이 추가되었습니다. 새로운 *중앙 관리 서버 연결 보호* 작업은 신뢰하는 서버에 연결하기 위한 암호 설정을 허용합니다. 이는 이 암호 없이 컴퓨터를 다시 연결하고 다른 서버에서 명령을 실행할 수 없다는 의미입니다.

2. 암호 보호 구성 요소에서 Active Directory 외의 사용자를 직접 선택하는 기능이 추가되었습니다. 따라서 수동으로 사용자 이름 및 암호를 지정하고 이 계정에 Kaspersky Endpoint Security 액세스 권한을 할당할 수 있습니다. 이렇게 하면 애플리케이션 접근 제어를 위해 다른 사용자와 KLAdmin 암호를 공유하거나 새 Active Directory 계정을 생성할 필요가 없습니다.

3. Windows 11 23H2 지원

12.3 업데이트

Kaspersky Endpoint Security 12.3 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. 이제 Endpoint Detection and Response Agent 구성에 애플리케이션을 설치할 수 있습니다. 이 구성을 사용하면 Kaspersky Detection and Response 솔루션(Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack Platform(EDR))에 필요한 구성 요소들이 갖춰진 애플리케이션을 설치할 수 있습니다. 타사 솔루션(예: Dr.Web, Dallas Lock, ESET)을 사용하여 이 구성에 애플리케이션을 설치할 수 있습니다. 이를 통해 Kaspersky Detection and Response와 함께 타사 인프라 보안 도구를 사용할 수 있습니다.

2. Kaspersky Endpoint Security의 Bluetooth 장치 작동이 개선되었습니다. 이제 예외 규칙 구성이나 입력 장치(무선 키보드, 마우스 등)를 제외한 모든 Bluetooth 장치에 액세스를 제한할 수 있습니다.

3. 실행 파일 데이터베이스가 있는 애플리케이션 제어 구성 요소 작업이 최적화되었습니다. 이제 파일이 컴퓨터에서 삭제되면 Kaspersky Endpoint Security가 자동으로 데이터베이스에서 파일 정보를 제거합니다. 이를 통해 데이터베이스를 최신 상태로 유지하고 Kaspersky Security Center 리소스를 절약할 수 있습니다.

4. 컴퓨터 보호 요구 레벨이 높아졌습니다. 보호 레벨을 높게 설정하려면 암호 보호 활성화를 해야 합니다. 정책 창 상단에서 보안 레벨 표시기를 확인하세요. 보호 레벨이 중간 또는 낮음일 경우, 보안 레벨 표시기 권장 창에서 암호 보호 사용을 활성화할 수 있습니다.

5. 애플리케이션이 Kaspersky Security Network에서 작동할 수 있도록 HTTPS 프로토콜 지원이 추가되었습니다. 중앙 관리 서버 속성의 KSN 프록시 서버 설정에서 HTTPS 사용을 활성화하십시오.

12.2 업데이트

Kaspersky Endpoint Security 12.2 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. Wi-Fi 네트워크에 대한 연결 제어(장치 제어)를 위해 WPA3 프로토콜 지원이 추가되었습니다. 이제 신뢰하는 Wi-Fi 네트워크 설정에서 WPA3 프로토콜을 선택하고 안전성이 떨어지는 프로토콜을 사용하는 네트워크 연결을 거부할 수 있습니다.

2. 이제 네트워크 위협 보호 제외를 위한 프로토콜 및 포트를 선택할 수 있습니다. 이제 신뢰하는 장치의 IP 주소를 지정하는 것 외에도 포트와 프로토콜을 선택할 수 있습니다. 이를 통해 개별 데이터 스트림을 제외하고 신뢰하는 IP 주소의 네트워크 공격을 방지할 수 있습니다.

3. 정책이 컴퓨터에 적용되는 경우 로컬 *데이터베이스 및 애플리케이션 모듈 업데이트 작업*의 업데이트 경로의 순서를 다르게 지정합니다. 이제 Kaspersky Security Center 서버가 기본적으로 Kaspersky 서버 대신 첫 번째 업데이트 경로로 사용됩니다. 이는 사용자가 로컬 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 실행할 때 트래픽을 절약하는 데 도움이 됩니다.

12.1 업데이트

Kaspersky Endpoint Security 12.1 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다.

1. Kaspersky Anti Targeted Attack Platform 솔루션용 내장 에이전트가 추가되었습니다. 이제 Kaspersky Endpoint Agent가 없어도 EDR(KATA)을 사용할 수 있습니다. Kaspersky Endpoint Agent의 모든 기능은 Kaspersky Endpoint Security에 의해 실행됩니다. Kaspersky Endpoint Agent 정책을 마이그레이션하려면 마이그레이션 마법사를 사용하십시오. 애플리케이션이 업데이트되면 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다. Kaspersky Endpoint Agent가 호환되지 않는 소프트웨어 목록에 추가되었습니다. Kaspersky Endpoint Security에 모든 Detection and Response 솔루션용 에이전트가 내장되므로 더 이상 이러한 솔루션과 통합하기 위해 Kaspersky Endpoint Agent를 설치할 필요가 없습니다.

2. 이제 Azure WVD 호환성 모드가 지원됩니다. 이 기능을 사용하면 Kaspersky Anti Targeted Attack Platform 콘솔에서 Azure 가상 컴퓨터 상태가 올바르게 표시됩니다. Azure WVD 호환성 모드를 사용하면 이러한 가상 컴퓨터에 영구적인 고유 센서 ID를 할당할 수 있습니다.

3. 이제 iTunes 또는 유사한 애플리케이션에서 모바일 장치에 대한 사용자 액세스를 구성할 수 있습니다. 예를 들어, 모바일 장치를 iTunes에서만 사용하도록 허용하고 모바일 장치를 이동식 드라이브로 사용하는 것을 차단할 수 있습니다. 그리고 이 애플리케이션은 Android 디버그 브리지(ADB) 애플리케이션에서도 이러한 규칙을 지원합니다.

4. Kaspersky Security Center 버전 11은 더 이상 지원되지 않습니다. Kaspersky Security Center를 최신 버전으로 업그레이드해야 합니다.

자주 묻는 질문

일반

Kaspersky Endpoint Security는 어떤 컴퓨터에서 작동할 수 있습니까?

마지막 버전 이후로 변경된 사항은 무엇입니까?

Kaspersky Endpoint Security에서 작동할 수 있는 다른 Kaspersky 애플리케이션에는 어떤 것이 있습니까?

Kaspersky Endpoint Security를 작동하면서 컴퓨터 리소스를 절약하려면 어떻게 해야 합니까?

배포

Kaspersky Endpoint Security를 조직 내 모든 컴퓨터에 설치하려면 어떻게 해야 합니까?

명령줄에서 구성할 수 있는 설치 설정에는 어떤 것이 있습니까?

Kaspersky Endpoint Security를 원격으로 제거하려면 어떻게 해야 합니까?

업데이트

데이터베이스를 업데이트하는 방법에는 어떤 것이 있습니까?

업데이트 후에 문제가 발생하면 어떻게 해야 합니까?

회사 네트워크 외부에 있는 데이터베이스는 어떻게 업데이트합니까?

업데이트 시 프록시 서버를 사용할 수 있나요?

보안

Kaspersky Endpoint Security는 어떤 방식으로 이메일을 검사합니까?

신뢰하는 파일을 검사에서 제외하려면 어떻게 해야 합니까?

플래시 드라이브를 통해 침투하는 바이러스로부터 컴퓨터를 보호하려면 어떻게 해야 합니까?

숨겨진 악성 코드 검사는 어떻게 실행합니까?

Kaspersky Endpoint Security의 보호를 일시 중지하려면 어떻게 해야 합니까?

Kaspersky Endpoint Security가 잘못 삭제한 파일을 복원하려면 어떻게 해야 합니까?

사용자가 Kaspersky Endpoint Security를 제거하지 못하도록 하려면 어떻게 해야 합니까?

인터넷

Kaspersky Endpoint Security는 암호화된 연결(HTTPS)을 검사합니까?

사용자가 신뢰하는 Wi-Fi 네트워크에만 연결할 수 있도록 하려면 어떻게 해야 합니까?

소셜 네트워크를 차단하려면 어떻게 해야 합니까?

애플리케이션

사용자의 컴퓨터에 설치된 애플리케이션(인벤토리)을 확인하려면 어떻게 해야 합니까?

컴퓨터 게임 실행을 차단하려면 어떻게 해야 합니까?

애플리케이션 제어가 올바르게 구성되었는지 확인하는 방법은 무엇입니까?

애플리케이션을 신뢰하는 목록에 추가하려면 어떻게 해야 합니까?

장치

플래시 드라이브 사용을 차단하려면 어떻게 해야 합니까?

장치를 신뢰하는 목록에 추가하려면 어떻게 해야 합니까?

차단된 장치에 대한 접근 권한을 획득할 수 있나요?

암호화

어떤 경우에 암호화가 불가능합니까?

암호를 사용하여 압축 파일에 대한 접근 권한을 제한하는 방법은 무엇입니까?

스마트 카드와 토큰을 사용하여 암호화할 수 있습니까?

Kaspersky Security Center와 연결하지 않고 암호화된 데이터에 대한 접근 권한을 받을 수 있습니까?

컴퓨터 운영 체제에 오류가 있는데 데이터가 암호화된 상태라면 어떻게 해야 합니까?

지원

리포트 파일은 어디에 저장됩니까?

추적 파일은 어떻게 생성합니까?

덤프 기록을 사용하려면 어떻게 해야 합니까?

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows(이하 Kaspersky Endpoint Security로도 지칭됨)에서는 다양한 유형의 위협, 네트워크 및 피싱 공격에 대한 포괄적인 컴퓨터 보호 기능을 제공합니다.

애플리케이션은 자동 제어 시스템과 관련된 기술적 프로세스에서 사용하도록 제작되지 않았습니다. 해당 시스템에서 장치를 보호하려면 Kaspersky Industrial CyberSecurity for Nodes 애플리케이션을 사용할 것을 권장합니다.

위협 탐지 기술

머신 러닝

Kaspersky Endpoint Security가 머신 러닝에 기반한 모델을 사용합니다. 이 모델은 Kaspersky 전문가가 개발한 모델입니다. 이 모델은 지속해서 KSN의 보안 위협 데이터를 받습니다(모델 훈련).

클라우드 분석

Kaspersky Endpoint Security가 Kaspersky Security Network에서 보안 위협 데이터를 수신합니다. *Kaspersky Security Network(KSN)*는 파일, 웹사이트 및 소프트웨어에 대한 정보가 포함된 Kaspersky의 온라인 기술 자료에 접속할 수 있는 클라우드 서비스 인프라입니다.

전문가 분석

Kaspersky Endpoint Security가 Kaspersky 바이러스 분석으로 추가된 보안 위협 데이터를 사용합니다. 바이러스 분석은 개체 평판을 자동으로 확인할 수 없을 시 개체를 평가합니다.

행동 분석

Kaspersky Endpoint Security가 개체의 활동을 실시간으로 분석합니다.

자동 분석

Kaspersky Endpoint Security가 자동 개체 분석 시스템의 데이터를 수신합니다. 이 시스템은 Kaspersky로 전송되는 모든 개체를 처리합니다. 시스템은 그 후 개체의 평판을 확인하고 개체 평판을 안티바이러스 데이터베이스에 추가합니다. 시스템이 개체 평판을 확인할 수 없는 시 시스템이 Kaspersky 바이러스 분석가에게 쿼리를 보냅니다.

Sandbox

Kaspersky Endpoint Security가 가상 머신에서 개체를 처리합니다. Kaspersky Sandbox가 개체 행동을 분석하여 개체 평판을 결정합니다. 이 기술은 Kaspersky Sandbox 솔루션을 사용하는 경우에만 이용할 수 있습니다.

Cloud Sandbox

Kaspersky Endpoint Security는 Kaspersky에서 제공하는 격리된 환경에서 개체를 검사합니다. Cloud Sandbox 기술은 영구적으로 활성화되며 사용 중인 라이센스 유형과 관계없이 모든 Kaspersky Security Network 사용자가 사용할 수 있습니다. Endpoint Detection and Response 솔루션을 이미 배포했다면 Cloud Sandbox에서 탐지한 위협에 대해 별도의 카운터를 활성화할 수 있습니다.

선택 트리

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

섹션	구성 요소
필수 위협 보호	**파일 위협 보호** 파일 위협 보호 구성 요소를 사용하면 컴퓨터 파일 시스템의 감염을 방지할 수 있습니다. 기본적으로 파일 위협 보호 구성 요소는 컴퓨터의 RAM에 영구적으로 상주하며 열려 있는 파일, 저장된 파일, 실행된 파일을 모두 실시간으로 검사합니다. 이 구성 요소는 연결된 드라이브를 포함하여 모든 컴퓨터 드라이브의 파일을 검사합니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다. **웹 위협 보호** 웹 위협 보호 구성 요소는 인터넷에서 악의적인 파일을 다운로드하지 못하도록 하며 악의적인 웹사이트와 피싱 웹사이트도 차단합니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다. **메일 위협 보호** 메일 위협 보호 구성 요소는 보내고 받는 이메일 메시지 첨부파일에 바이러스 및 기타 위협이 있는지 검사합니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다. 메일 위협 보호는 수신 및 발신 메시지를 모두 검사할 수 있습니다. 애플리케이션은 다음 메일 클라이언트에서 POP3, SMTP, IMAP 및 NNTP를 지원합니다. • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Mozilla Thunderbird, MyOffice Mail 및 R7-Office Organizer 메일 클라이언트의 트래픽을 검사하려면 인증서 저장소에 Kaspersky 인증서 추가하고 자체 인증서 저장소를 선택해야 합니다. 메일 위협 보호는 다른 프로토콜 및 메일 클라이언트를 지원하지 않습니다. 메일 위협 보호가 항상 메시지에 대해 *프로토콜 수준*의 액세스(예: Microsoft Exchange 솔루션을 사용하는 경우)를 얻을 수 있는 것은 아닙니다. 이러한 이유로 메일 위협 보호에는 Microsoft Office Outlook용 확장 프로그램이 포함됩니다. 확장 프로그램을 사용하면 *메일 클라이언트 수준*에서 메시지를 검색할 수 있습니다. 메일 위협 보호 확장 프로그램은 Outlook 2010, 2013, 2016, 2019, 2021, 2024 및 365의 32비트 버전을 지원합니다. Arm 기반 컴퓨터에서는 메일 위협 보호 확장 프로그램이 Arm64용 Outlook 2016, Outlook 2021, Outlook 2024 및 Outlook 365의 32비트 버전을 지원합니다. **네트워크 위협 보호** *네트워크 위협 보호* 구성 요소(침입 탐지 시스템, Intrusion Detection System, IDS라고도 함)는 인바운드 네트워크 트래픽에서 네트워크 공격의 활동 특성을 모니터링합니다. 애플리케이션은 사용자 컴퓨터에 시도된 네트워크 공격을 탐지하면 공격 컴퓨터와의 네트워크 연결을 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. **방화벽** 방화벽은 인터넷 또는 로컬 네트워크에서 작업하는 동안 컴퓨터에 대한 무단 연결을 차단합니다. 방화벽은 또한 컴퓨터에서 애플리케이션의 네트워크 활동을 제어합니다. 이를 통해 신원 도용 및 기타 공격으로부터 회사 LAN을 보호할 수 있습니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 사전 정의된 *네트워크 규칙*을 통해 컴퓨터 보호 기능을 제공합니다. **BadUSB 공격 방지** BadUSB 공격 방지 구성 요소는 키보드를 에뮬레이션하는 감염된 USB 장치가 컴퓨터에 연결하지 못하도록 차단합니다. **AMSI 보호** AMSI 보호 구성 요소는 Microsoft의 Antimalware Scan Interface를 지원합니다. *AMSI(Antimalware Scan Interface)*를 사용하는 경우 AMSI를 지원하는 타사 애플리케이션이 추가 검사를 위해 Kaspersky Endpoint Security에 PowerShell 스크립트 등의 개체를 전송하고 해당 개체에 대한 검사 결과를 받을 수 있습니다.

섹션	구성 요소
지능형 위협 보호 	**Kaspersky Security Network** *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 Endpoint Security에서 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 Endpoint Security는 검사한 웹 주소의 평판 정보는 물론이고 검사한 파일의 카테고리 및 평판 에 관한 정보도 수신하게 됩니다. **행동 탐지** 행동 탐지 구성 요소는 컴퓨터에 설치된 애플리케이션의 동작에 대한 데이터를 수신한 후 보호 구성 요소의 성능 향상을 위해 다른 구성 요소에 이 정보를 제공합니다. 행동 탐지 구성 요소는 애플리케이션의 행동 스트림 서명(BSS)을 활용합니다. 애플리케이션 동작이 행동 스트림 시그니처와 일치할 경우 Kaspersky Endpoint Security는 선택된 처리 방법을 수행합니다. Kaspersky Endpoint Security 기능은 행동 스트림 서명을 바탕으로 하며 컴퓨터에 대한 사전 방역을 제공합니다. 행동 탐지 구성 요소는 네트워크 포트에서 컴퓨터의 보안을 위협할 수 있는 애플리케이션 프로세스를 추가로 모니터링합니다. 애플리케이션은 안티 바이러스 데이터베이스를 사용하여 이러한 프로세스에 대한 정보를 가져옵니다. **Anti-Cryptor** Anti-Cryptor 구성 요소는 공유 폴더의 활동을 분석합니다. 이 활동이 외부 암호화에서 일반적으로 나타나는 행동 스트림 시그니처와 일치하면 Kaspersky Endpoint Security가 선택한 동작을 수행합니다. **익스플로잇 방지** 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 Endpoint Security가 해당 파일의 실행을 차단하거나 해당 사용자에게 알립니다. 익스플로잇 방지 구성 요소는 네트워크 포트에서 컴퓨터의 보안을 위협할 수 있는 애플리케이션 프로세스를 추가로 모니터링합니다. 애플리케이션은 안티 바이러스 데이터베이스를 사용하여 이러한 프로세스에 대한 정보를 가져옵니다. **호스트 침입 방지** 호스트 침입 방지 구성 요소는 애플리케이션이 운영 체제에 위험할 수 있는 작업을 수행하지 못하게 하고 운영 체제 리소스 및 개인 데이터에 대한 접근을 제어합니다. 이 구성 요소는 안티 바이러스 데이터베이스 및 Kaspersky Security Network 클라우드 서비스를 통해 컴퓨터를 보호합니다. **복원 엔진** 복원 엔진을 사용하면 Kaspersky Endpoint Security가 운영 체제에서 악성 코드에 의해 수행된 활동을 롤백합니다.
보안 제어 	**애플리케이션 제어** 애플리케이션 제어는 사용자 컴퓨터의 애플리케이션 시작을 관리합니다. 이를 통해 애플리케이션 사용에 대한 회사 보안 정책을 구현할 수 있습니다. 애플리케이션 제어는 애플리케이션에 대한 접근을 제한하여 컴퓨터 감염 위험을 줄입니다. **장치 제어** 장치 제어는 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. **웹 제어** 웹 제어는 웹 리소스에 대한 사용자의 접근을 관리합니다. 이렇게 하면 트래픽을 줄이고 업무 시간을 부적절하게 사용하는 것도 줄일 수 있습니다. 웹 제어가 제한한 웹사이트를 사용자가 열려고 하면 Kaspersky Endpoint Security가 접근을 차단하거나 경고를 표시합니다. **적응형 이상 행위 제어** 적응형 이상 행위 제어 구성 요소는 회사 네트워크의 컴퓨터에서 일반적이지 않은 활동을 감시하고 차단합니다. 적응형 이상 행위 제어는 일련의 규칙을 사용하여 비정상적인 동작을 추적합니다(예, *오피스 애플리케이션에서 Microsoft PowerShell 시작* 규칙). 규칙은 Kaspersky 전문가가 일반적인 악의적인 활동 시나리오를 기반으로 작성합니다. 적응형 이상 행위 제어에서 각 규칙을 처리하는 방법을 구성할 수 있습니다. 또한 예를 들어 특정 워크플로 작업을 자동화하는 PowerShell 스크립트를 실행을 허용할 수 있습니다. Kaspersky Endpoint Security는 규칙 세트와 애플리케이션 데이터베이스를 업데이트합니다. **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. **시스템 무결성 모니터링** 시스템 무결성 모니터링 구성 요소는 운영 체제에서 컴퓨터 보안 위반을 나타낼 수 있는 변경 사항을 모니터링합니다. 이러한 변경이 탐지되면 Kaspersky Endpoint Security는 해당 이벤트를 생성하고 관리자에게 알립니다.

섹션	구성 요소
작업 	**악성 코드 검사** Kaspersky Endpoint Security는 컴퓨터에서 바이러스 및 기타 보안 위협을 검사합니다. 따라서 낮은 보안 레벨 등으로 보호 구성 요소가 탐지하지 못한 악성 코드의 전파 가능성을 방지할 수 있습니다. **데이터베이스 및 애플리케이션 모듈 업데이트** Kaspersky Endpoint Security는 업데이트된 애플리케이션 데이터베이스 및 모듈을 다운로드합니다. 업데이트하면 최신 바이러스 및 기타 위협으로부터 컴퓨터가 계속 보호됩니다. 기본적으로 애플리케이션은 자동으로 업데이트되지만 필요시 데이터베이스 및 애플리케이션 모듈을 직접 업데이트할 수도 있습니다. **마지막 업데이트 롤백** Kaspersky Endpoint Security는 데이터베이스 및 모듈의 마지막 업데이트를 롤백합니다. 이렇게 하면 새 데이터베이스 버전에 잘못된 서명이 포함되어 있어 Kaspersky Endpoint Security가 안전한 애플리케이션을 차단하는 경우 등과 같이 필요 시에 데이터베이스 및 애플리케이션 모듈을 이전 버전으로 롤백할 수 있습니다. **애플리케이션 무결성 검사** Kaspersky Endpoint Security는 이 애플리케이션 설치 폴더에 있는 모듈의 손상 및 변경 여부를 확인합니다. 애플리케이션 모듈에 잘못된 디지털 서명이 포함되어 있으면 이 모듈은 손상된 것으로 간주됩니다.
데이터 암호화 	**파일 레벨 암호화** 이 구성 요소를 통해 파일 암호화 규칙을 생성할 수 있습니다. 암호화를 위해 미리 정의된 폴더를 선택하거나, 폴더를 직접 선택하거나, 확장자별로 개별 파일을 선택할 수 있습니다. **전체 디스크 암호화** 이 구성 요소를 사용하면 Kaspersky 디스크 암호화 또는 BitLocker 드라이브 암호화를 사용하여 하드 디스크를 암호화할 수 있습니다. **이동식 드라이브 암호화** 이 구성 요소를 사용하면 이동식 드라이브의 데이터를 보호할 수 있습니다. 전체 디스크 암호화(FDE) 또는 파일 수준 암호화(FLE)를 사용할 수 있습니다.
Detection and Response 	**Endpoint Detection and Response Optimum** Kaspersky Endpoint Detection and Response Optimum 솔루션(이하 "EDR Optimum"이라고도 함)용 내장 에이전트입니다. *Kaspersky Endpoint Detection and Response*는 지능형 사이버 위협으로부터 기업의 IT 인프라를 보호하기 위한 솔루션입니다. 이 솔루션의 기능은 위협 자동 탐지와 이에 대한 대응 능력을 결합하여 새로운 익스플로잇, 랜섬웨어, 파일리스 공격 및 합법적인 시스템 도구를 사용하는 방법 등 다양한 지능형 공격에 대처합니다. 솔루션에 대한 자세한 내용은 Kaspersky Endpoint Detection and Response Optimum 도움말 을 참조하십시오. **Endpoint Detection and Response Expert** Kaspersky Endpoint Detection and Response Expert 솔루션(이하 "EDR Expert"이라고도 함)용 내장 에이전트입니다. EDR Expert는 EDR Optimum보다 더 많은 보안위협 모니터링 및 대응 기능을 제공합니다. 솔루션에 대한 자세한 내용은 Kaspersky Endpoint Detection and Response Expert 도움말 을 참조하십시오. **Endpoint Detection and Response Expert(on-premise)** 및 **Network Detection and Response(KATA)** Kaspersky Anti Targeted Attack Platform 솔루션의 일부인 Endpoint Detection and Response 및 Network Detection and Response 구성 요소를 관리하기 위한 내장 에이전트입니다. *Kaspersky Anti Targeted Attack Platform*은 표적형 공격, APT(지능형 지속 위협), 제로 데이 공격 등 지능형 위협을 적시에 탐지하도록 설계된 솔루션입니다. Kaspersky Anti Targeted Attack Platform에는 다음 세 가지 기능 단위가 포함됩니다. • Kaspersky Anti Targeted Attack Platform(*KATA*) • Kaspersky Endpoint Detection and Response(*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) 모든 기능 단위를 구매하거나 개별 기능 단위를 따로 구매할 수 있습니다. 이 솔루션에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말 을 참조하십시오. **Sandbox** Sandbox용 내장 에이전트입니다. *Sandbox* 구성 요소는 컴퓨터에서 지능형 보안위협을 탐지하고 자동 차단합니다. Sandbox는 조직의 IT 인프라에 대한 표적 공격의 활동 특성 및 악성 활동 탐지를 위해 개체 행동을 분석합니다. Sandbox는 Microsoft Windows 운영 체제(Sandbox 서버)의 가상 이미지가 배포된 특수 서버의 개체를 분석하고 검사합니다. 이 솔루션에 대한 자세한 내용은 Kaspersky Sandbox 도움말 및 Kaspersky Anti Targeted Attack Platform 도움말 을 참조하십시오. **Managed Detection and Response** Kaspersky Managed Detection and Response 솔루션의 동작을 지원하는 내장 에이전트입니다. *Kaspersky Managed Detection and Response(MDR)* 솔루션은 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. 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 도움말 을 참조하십시오.

애플리케이션 모드: Standard, EDR Agent, Light Agent

Kaspersky Endpoint Security for Windows는 많은 Kaspersky 솔루션의 일부입니다. 솔루션에 따라 애플리케이션의 모드를 선택해야 합니다.



표준 모드

애플리케이션의 기본 모드입니다. Kaspersky EPP(Endpoint Protection Platform) 솔루션의 일부로 애플리케이션을 설치할 수 있습니다. 예를 들어 표준 모드의 Kaspersky Endpoint Security는 Kaspersky Endpoint Security for Business의 일부입니다. Kaspersky Endpoint Security는 다양한 위협, 네트워크 공격 및 사기로부터 워크스테이션과 서버를 포괄적으로 보호합니다. 표준 모드에서 EDR, MDR, KUMA 등을 포함한 Kaspersky Detection and Response 솔루션과의 통합에 내장 에이전트를 사용할 수도 있습니다.



EDR Agent

이 모드를 사용하면 Kaspersky Detection and Response 솔루션을 타사 EPP 솔루션과 함께 배포할 수 있습니다. Detection and Response 솔루션에는 Kaspersky Managed Detection and Response (MDR)와 Kaspersky Anti Targeted Attack Platform (KATA)가 포함됩니다. EDR Agent는 Kaspersky SIEM 솔루션인 Kaspersky Unified Monitoring and Analysis Platform (KUMA)도 지원합니다.

이 모드에서는 파일 위협 보호 또는 웹 위협 보호와 같은 표준 보호 구성 요소를 사용할 수 없습니다. 컴퓨터의 표준 보호는 타사 EPP 솔루션을 통해 제공됩니다. EDR Agent는 이러한 컴퓨터에서 실행 중인 프로세스, 개방형 네트워크 연결, 수정 중인 파일을 계속해서 모니터링하고 Detection and Response 솔루션과 상호 작용합니다.



Light Agent

이 모드는 가상 환경을 보호하는 데 사용됩니다. Light Agent 모드의 Kaspersky Endpoint Security는 Kaspersky Hybrid Cloud Security 솔루션의 일부입니다. Light Agent는 워크스테이션과 서버용 게스트 운영 체제가 설치된 가상 컴퓨터를 보호합니다. 이 모드에서도 표준 모드와 동일한 보호 및 제어 구성 요소를 사용할 수 있습니다. 차이점은 별도의 가상 컴퓨터인 SVM(Secure Virtual Machine)에 설치된 특수 솔루션 구성 요소를 통해 개체에서 바이러스 및 기타 악성 코드를 검사한다는 점입니다. 따라서 Light Agent는 가상 컴퓨터의 리소스 대신 SVM의 리소스를 사용하여 인프라 보안을 보장합니다.

배포 패키지

배포 키트에는 다음과 같은 배포 패키지가 포함되어 있습니다.

- **AES256**

  이 배포 패키지에는 256비트의 유효 키 길이를 가진 AES(Advanced Encryption Standard) 암호화 알고리즘을 구현하는 암호화 도구가 포함되어 있습니다.

- **AES56**

이 배포 패키지에는 56비트의 유효 키 길이로 AES 암호화 알고리즘을 구현하는 암호화 도구가 포함되어 있습니다.

AES256 및 AES56 배포 패키지는 Arm 기반 컴퓨터에 설치하도록 제작되지 않았습니다.

- **Arm64**

  이 배포 패키지는 Arm 기반 컴퓨터에 설치하기 위해 제작되었습니다.

  Arm64 배포 패키지는 Windows x86/x64 운영 체제 또는 서버용 Windows 운영 체제를 실행하는 컴퓨터에 설치하도록 제작되지 않았습니다.

각 배포 패키지에는 다음 파일이 포함되어 있습니다.

`kes_win.msi`	Kaspersky Endpoint Security 설치 패키지.
`setup_kes.exe`	이용 가능한 방법을 활용한 애플리케이션 설치에 필요한 파일.
`kes_win.kud`	Kaspersky Endpoint Security용 설치 패키지 생성용 파일.
`klcfginst.msi`	Kaspersky Security Center 관리 콘솔의 애플리케이션 관리 플러그인용 설치 패키지.
`bases.cab`	설치 시 사용되는 업데이트 패키지 파일.
`cleaner_v2.cab` `cleanerapi_v2.cab`	호환되지 않는 소프트웨어를 제거하는 파일.
`incompatible.txt`	Kaspersky Endpoint Security와 호환성 문제를 유발할 수 있는 소프트웨어 목록이 포함된 파일. Kaspersky는 목록에 있는 소프트웨어와 Kaspersky Endpoint Security의 호환성을 보장하지 않습니다.
`ksn_<language ID>.txt`	Kaspersky Security Network 참가 약관을 읽어볼 수 있는 파일.
`license.txt`	최종 사용자 라이센스 계약서 및 개인정보 취급방침을 읽어볼 수 있는 파일.
`installer.ini`	배포 패키지 내부 설정이 포함된 파일.
`kes.cab`	애플리케이션의 그래픽 인터페이스용 파일.
`aes256.cab` / `aes56.cab`	AES 암호화 알고리즘용 파일(Arm64 배포 패키지에 포함되지 않음).
`package.kcat`	애플리케이션 배포 키트의 서명이 있는 파일. 디지털 서명은 애플리케이션 배포 키트의 인증 및 무결성을 보장합니다.

이 설정 값을 변경하지 않는 것이 좋습니다. 설치 옵션을 변경하려면 setup.ini 파일을 사용합니다.

하드웨어 및 소프트웨어 요구 사항

Kaspersky Endpoint Security가 제대로 작동하려면 다음 요구사항이 충족되어야 합니다.

최소 일반 요구 사항:

- 2GB의 하드 드라이브 여유 공간
- CPU:
  - 워크스테이션: 1GHz
  - 서버: 1.4GHz
  - SSE2 명령어 지원(Arm 예외)
- RAM:
  - 워크스테이션(x86): 1GB
  - 워크스테이션(x64): 2GB
  - 서버: 2GB
  - Kaspersky Anti Targeted Attack Platform 통합용 내장 에이전트를 활용해 애플리케이션을 설치하기 위한 서버: 8GB
- Microsoft .NET Framework 4 이상

Arm 기반 컴퓨터 최소 일반 요구 사항:

- 2GB의 하드 드라이브 여유 공간
- CPU: 1GHz, Armv8.1 아키텍처
- RAM: 4 GB
- Microsoft .NET Framework 4.8 이상

애플리케이션을 설치하려면 컴퓨터에 대한 관리자 권한이 필요합니다.

워크스테이션

지원되는 워크스테이션 운영 체제:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise 멀티 세션

- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Windows 운영 체제는 버전 11 24H2부터 UDP Receive Segment Coalescing Offload(URO) 기술을 지원합니다. 호환 가능한 네트워크 카드 및 드라이버가 컴퓨터에 설치되어 있는 경우 이 기술은 기본적으로 활성화됩니다. 사용자 컴퓨터에서 URO를 사용하지 않도록 설정하면 애플리케이션의 성능이 크게 저하될 수 있습니다.

Kaspersky Endpoint Security가 올바르게 작동하려면 사용자 컴퓨터에서 Windows Security Center(wscsvc) 서비스가 실행되고 있어야 합니다.

Kaspersky Endpoint Security는 운영 체제 업데이트 KB4490628(2019년 3월 12일) 및 KB4474419(2019년 9월 23일) 없이는 Microsoft Windows 7에 설치할 수 없습니다. 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오.

Microsoft Windows 10 운영 체제 지원에 대한 상세 정보는 기술 지원 기술 자료 웹사이트를 참고하십시오.

Microsoft Windows 11 운영 체제 지원에 대한 상세 정보는 기술 지원 기술 자료 웹사이트를 참고하십시오.

서버

Kaspersky Endpoint Security는 서버용 Windows 운영 체제를 실행하는 컴퓨터의 애플리케이션 중요 구성 요소를 지원합니다. 조직의 서버 및 클러스터에서 Kaspersky Security for Windows Server 대신 Kaspersky Endpoint Security for Windows를 사용할 수 있습니다(Cluster Mode, 클러스터 모드). 또한, 애플리케이션은 Server Core Mode를 지원합니다(알려진 문제 참조).

지원되는 서버 운영 체제:

- Windows Small Business Server 2011 Essentials / Standard(64비트)

  Microsoft Small Business Server 2011 Standard(64비트)는 Microsoft Windows Server 2008 R2용 서비스 팩 1이 설치되었을 때만 지원됩니다.

- Windows MultiPoint Server 2011(64비트)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter(Server Core 모드 포함)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter(Server Core 모드 포함)
- Windows Server 2016 Essentials / Standard / Datacenter(Server Core 모드 포함)

- Windows Server 2019 Essentials / Standard / Datacenter(Server Core 모드 포함)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure 에디션(Server Core 모드 포함)
- Windows Server 2025 Standard / Datacenter

Kaspersky Endpoint Security는 운영 체제 업데이트 KB4490628(2019년 3월 12일) 및 KB4474419(2019년 9월 23일)를 설치하지 않으면 Microsoft Windows Server 2008 R2에 설치할 수 없습니다.

Microsoft Windows Server 2016 및 Microsoft Windows Server 2019 운영 체제 지원에 대한 상세 정보는 기술 지원 기술 자료 웹사이트를 참고하십시오.

Microsoft Windows Server 2022 운영 체제 지원에 대한 상세 정보는 기술 지원 기술 자료 웹사이트를 참고하십시오.

지원하지 않는 서버 운영 체제:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

가상 서버

표준 모드에서 애플리케이션 작동을 위해 지원되는 가상 플랫폼:

- VMware Workstation 17.6.4
- VMware ESXi 8.0 업데이트 3g
- Windows Server 2025
- Citrix Virtual Apps and Desktops 7 2507 LTSR
- Citrix Provisioning 2507 LTSR
- XenServer 8.4

애플리케이션은 Hyper-V를 사용하여 생성된 Windows 11 Pro Arm64를 실행하는 가상 컴퓨터를 지원합니다.

Light Agent 설치를 위한 가상 컴퓨터

Arm 기반 가상 컴퓨터에서는 Light Agent 모드의 Kaspersky Endpoint Security 설치를 지원하지 않습니다.

가상 컴퓨터의 BIOS는 SMBIOS 사양 버전 2.1 이상을 지원해야 합니다.

가상 컴퓨터에 다음 패키지 및 유틸리티가 설치되어 있어야 합니다 .

- Microsoft Hyper-V – 통합 서비스 패키지를 사용하는 경우.
- VMware vSphere – VMware Tools 패키지를 사용하는 경우.
- XenServer – XenTools 패키지를 사용하는 경우.
- HUAWEI FusionSphere – HUAWEI Tools 패키지를 사용하는 경우.
- KVM 기반 하이퍼바이저 – QEMU Guest Agent를 사용하는 경우.

Light Agent 모드에서 애플리케이션을 실행하기 위한 가상 인프라 요구 사항은 Kaspersky Security for Virtualization Light Agent 도움말 을 참조하십시오.

애플리케이션이 올바르게 작동하려면 최소 100Mbit/s 이상의 대역폭을 가진 가상 네트워크 인터페이스를 사용하십시오.

터미널 서버

지원하는 터미널 서버 유형:

- Windows Server 2008 R2 SP1 기반 Microsoft 원격 데스크톱 서비스
- Windows Server 2012 기반 Microsoft 원격 데스크톱 서비스
- Windows Server 2012 R2 기반 Microsoft 원격 데스크톱 서비스
- Windows Server 2016 기반 Microsoft 원격 데스크톱 서비스
- Windows Server 2019 기반 Microsoft 원격 데스크톱 서비스
- Windows Server 2022 기반 Microsoft 원격 데스크톱 서비스
- Windows Server 2025 기반 Microsoft 원격 데스크톱 서비스
- Citrix Virtual Apps and Desktops 7 2507 LTSR의 Citrix RDSH

Kaspersky Security Center 지원

Kaspersky Endpoint Security는 다음 버전 Kaspersky Security Center의 작동을 지원합니다:

- Kaspersky Security Center 14
- Kaspersky Security Center 14.1
- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16
- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2

운영 체제 유형에 따라 사용 가능한 애플리케이션 기능 비교

사용 가능한 Kaspersky Endpoint Security 기능 세트는 운영 체제 유형에 따라 달라집니다: 워크스테이션 또는 서버 (아래 표 참조).

Kaspersky Endpoint Security 12.8 for Windows부터 설치 패키지에서 운영 체제 유형별로 다른 구성 요소 세트를 구성할 수 있습니다. 즉, 동일한 설치 패키지를 사용하여 워크스테이션과 서버에 애플리케이션을 배포할 수 있습니다.

Arm 기반 가상 컴퓨터에서는 Light Agent 모드의 Kaspersky Endpoint Security 설치를 지원하지 않습니다.

Kaspersky Endpoint Security 기능 비교

기능	워크스테이션	Arm 기반 워크스테이션	서버	Server Core 모드
지능형 위협 보호				
Kaspersky Security Network	✓	✓	✓	✓

기능	워크스테이션	Arm 기반 워크스테이션	서버	Server Core 모드
행동 탐지	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓
익스플로잇 방지	✓	✓	✓	✓
호스트 침입 방지	✓	✓	–	–
복원 엔진	✓	✓	✓	✓
필수 위협 보호				
파일 위협 보호	✓	✓	✓	✓
웹 위협 보호	✓	✓	✓	–
메일 위협 보호	✓	✓	✓	–
방화벽	✓	✓	✓	✓
네트워크 위협 보호	✓	✓	✓	✓
BadUSB 공격 방지	✓	✓	✓	–
AMSI 보호	✓	✓	✓	✓
보안 제어				
로그 검사	–	–	✓	–
애플리케이션 제어	✓	✓	✓	✓
장치 제어	✓	✓	✓	✓
웹 제어	✓	✓	✓	–
적응형 이상 행위 제어	✓	✓	–	–
시스템 무결성 모니터링	–	–	✓	–
Cloud Discovery	✓	✓	–	–
데이터 암호화				
Kaspersky 디스크 암호화	✓	–	–	–
BitLocker 드라이브 암호화	✓	✓	✓	✓
파일 레벨 암호화	✓	–	–	–
이동식 드라이브 암호화	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert	✓	–	✓	✓
Endpoint Detection and Response(KATA)	✓	✓	✓	✓
Network Detection and Response(KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response(MDR)	✓	✓	✓	✓
KUMA 통합	✓	✓	✓	✓

관리 도구에 따른 애플리케이션 기능 비교

Kaspersky Endpoint Security에서 사용 가능한 기능은 관리 도구에 따라 다릅니다(아래 표 참조).

다음 Kaspersky Security Center 콘솔을 사용하여 애플리케이션을 관리할 수 있습니다:

- 관리 콘솔. 관리자 워크스테이션에 설치된 MMC(Microsoft Management Console) 스냅인.
- 웹 콘솔. 중앙 관리 서버에 설치된 Kaspersky Security Center의 구성 요소. 중앙 관리 서버에 접근할 수 있는 모든 컴퓨터에 설치된 브라우저를 사용해 웹 콘솔에서 작업할 수 있습니다.

또한, Kaspersky Security Center Cloud Console을 사용하여 애플리케이션을 관리할 수 있습니다. *Kaspersky Security Center Cloud Console*은 Kaspersky Security Center의 클라우드 버전입니다. 즉, 중앙 관리 서버와 Kaspersky Security Center의 기타 구성 요소가 Kaspersky의 클라우드 인프라에 설치됩니다. Kaspersky Security Center Cloud Console을 통한 애플리케이션 관리에 대한 상세 정보는 Kaspersky Security Center Cloud Console 도움말을 참조하십시오.

Kaspersky Endpoint Security는 Kaspersky Next Pro View 솔루션에 포함됩니다. 이 솔루션의 일부로 작동할 때 사용 가능한 애플리케이션 기능에 대한 자세한 내용은 Kaspersky Next 도움말을 참조하십시오.

Kaspersky Endpoint Security 기능 비교

기능	Kaspersky Security Center		Kaspersky Security Center
	관리 콘솔	웹 콘솔	Cloud Console
지능형 위협 보호			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
행동 탐지	✓	✓	✓
Anti-Cryptor			
익스플로잇 방지	✓	✓	✓
호스트 침입 방지	✓	✓	✓
복원 엔진	✓	✓	✓
필수 위협 보호			
파일 위협 보호	✓	✓	✓
웹 위협 보호	✓	✓	✓
메일 위협 보호	✓	✓	✓
방화벽	✓	✓	✓
네트워크 위협 보호	✓	✓	✓
BadUSB 공격 방지	✓	✓	✓
AMSI 보호	✓	✓	✓
보안 제어			
로그 검사	✓	✓	✓
애플리케이션 제어	✓	✓	✓
장치 제어	✓	✓	✓
웹 제어	✓	✓	✓
적응형 이상 행위 제어	✓	✓	✓
시스템 무결성 모니터링	✓	✓	✓
Cloud Discovery	–	–	✓
데이터 암호화			
Kaspersky 디스크 암호화	✓	✓	–
BitLocker 드라이브 암호화	✓	✓	✓

기능	Kaspersky Security Center		Kaspersky Security Center
	관리 콘솔	웹 콘솔	Cloud Console
파일 레벨 암호화	✓	✓	–
이동식 드라이브 암호화	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert	–	–	✓
Endpoint Detection and Response(KATA)	✓	✓	–
Network Detection and Response(KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response(MDR)	✓	✓	✓
KUMA 통합	✓	✓	✓
작업			
키 추가	✓	✓	✓
애플리케이션 구성 요소 변경	✓	✓	✓
인벤토리	✓	✓	✓
업데이트	✓	✓	✓
업데이트 롤백	✓	✓	✓
악성 코드 검사	✓	✓	✓
애플리케이션 무결성 검사	✓	✓	–
데이터 완전 삭제	✓	✓	✓
인증 에이전트 계정 관리(Kaspersky 디스크 암호화)	✓	✓	–
IOC 검사(EDR)	–	✓	✓
격리 저장소로 파일 이동(EDR)	–	✓	✓
파일 가져오기(EDR)	–	✓	✓
파일 삭제(EDR)	–	✓	✓
프로세스 시작(EDR)	–	✓	✓
프로세스 종료(EDR)	–	✓	✓

다른 애플리케이션과의 호환성

Kaspersky Endpoint Security는 일부 Kaspersky 애플리케이션 및 일부 타사 애플리케이션과 호환되지 않습니다. 따라서 설치, 애플리케이션 버전 업데이트, 애플리케이션 구성 요소 변경 전에, Kaspersky Endpoint Security가 컴퓨터를 검사하여 이러한 애플리케이션이 있는지 확인합니다.

타사 애플리케이션과의 호환성

Kaspersky Endpoint Security는 타사 엔드포인트 보호 시스템(Endpoint Protection Platform, EPP)의 일부인 애플리케이션과 호환되지 않습니다. Kaspersky Endpoint Security에는 다른 애플리케이션과의 호환성 문제가 발생할 수도 있습니다. 호환성을 확인하기 위해 Kaspersky Endpoint Security는 Kaspersky에서 준비한 소프트웨어 목록을 참조합니다. 이 목록은 incompatible.txt 파일에 포함되어 있습니다. 이 파일은 배포 키트에 포함되어 있습니다.

Kaspersky는 목록에 있는 소프트웨어와 Kaspersky Endpoint Security의 호환성을 보장하지 않습니다. 목록에 있는 애플리케이션이 검색되면 설치 프로그램이 Kaspersky Endpoint Security 배포를 중지합니다. 설치 프로그램은 목록에서 일부 애플리케이션을 자동으로 삭제할 수 있습니다. 위험을 무시하고 Kaspersky Endpoint Security와 목록에 있는 소프트웨어를 동일한 컴퓨터에 설치하려는 경우 컴퓨터 검사를 건너뛸 수 있습니다(아래 지침 참조).

INCOMPATIBLE.TXT 파일 다운로드

Kaspersky 애플리케이션과의 호환성

Kaspersky Endpoint Security는 다음 Kaspersky 애플리케이션과 호환되지 않습니다:

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security
- Kaspersky Internet Security
- Kaspersky Anti-Virus
- Kaspersky Total Security
- Kaspersky Safe Kids
- Kaspersky Free
- Kaspersky Anti-Ransomware Tool
- Kaspersky Anti Targeted Attack Platform 및 Kaspersky Endpoint Detection and Response 솔루션의 일부인 Endpoint Sensor.
- Kaspersky의 Detection and Response 솔루션의 일부인 Kaspersky Endpoint Agent.

  Kaspersky는 모든 Detection and Response 솔루션을 Kaspersky Endpoint Agent 대신 Kaspersky Endpoint Security 내장 에이전트를 사용하도록 전환하고 있습니다. 12.1 버전부터는 애플리케이션에서 모든 Detection and Response 솔루션을 지원합니다.

- Kaspersky Security for Virtualization Light Agent
- Kaspersky Fraud Prevention for Endpoint
- Kaspersky Security for Windows Server

  Kaspersky Endpoint Security 12.0부터 Kaspersky Security for Windows Server에서 Kaspersky Endpoint Security for Windows로 마이그레이션하고 동일 솔루션을 사용하여 워크스테이션과 서버를 보호할 수 있습니다.

- Kaspersky Embedded Systems Security

이 목록에 해당하는 Kaspersky 애플리케이션이 컴퓨터에 설치된 경우 Kaspersky Endpoint Security는 이러한 애플리케이션을 제거합니다. Kaspersky Endpoint Security 설치를 계속하기 전에 이 프로세스가 완료될 때까지 기다려 주십시오.

호환성 문제를 유발할 수 있는 소프트웨어 검사 건너뛰기

Kaspersky Endpoint Security가 incompatible.txt 목록에서 소프트웨어를 탐지하면 애플리케이션 설치가 종료됩니다. 설치를 계속하려면 해당 애플리케이션을 제거해야 합니다. 그러나 타사 소프트웨어 공급업체가 설명서에 해당 소프트웨어가 Endpoint Protection Platform(EPP)와 호환된다고 명시했다면 이 공급업체의 애플리케이션이 있는 컴퓨터에 Kaspersky Endpoint Security를 설치할 수 있습니다. 예를 들어, Endpoint Detection and Response(EDR) 솔루션 공급업체는 타사 EPP 시스템과의 호환성을 선언할 수 있습니다. 이때는 설치된 소프트웨어 검사를 실행하지 않고 Kaspersky Endpoint Security 설치를 시작해야 합니다. 이렇게 하려면 설치 프로그램에 다음 매개변수를 전달합니다.

- `SKIPPRODUCTCHECK=1`. 설치된 소프트웨어 검사를 비활성화합니다. 호환성 문제를 유발할 수 있는 소프트웨어 목록은 배포 키트에 포함된 incompatible.txt 파일에서 이용 가능합니다. 이 파라미터에 대해 설정된 값이 없고, 목록에 있는 소프트웨어가 탐지되면 Kaspersky Endpoint Security 설치가 종료됩니다.

- `SKIPPRODUCTUNINSTALL=1`. incompatible.txt 목록에서 탐지된 소프트웨어의 자동 제거를 비활성화합니다. 이 파라미터에 대해 설정된 값이 없으면 Kaspersky Endpoint Security에서 호환성 문제를 유발할 수 있는 소프트웨어를 제거하려고 시도합니다.

- `CLEANERSIGNCHECK=0`. 검사로 발견된 애플리케이션의 디지털 서명 확인을 비활성화합니다. 이 매개변수를 설정하지 않으면 Kaspersky Security Center를 통해 애플리케이션을 배포할 때 디지털 서명 확인이 비활성화됩니다. 애플리케이션을 로컬로 설치하면 디지털 서명 확인이 기본값으로 활성화됩니다.

애플리케이션을 로컬로 설치 시, 명령줄에서 매개변수를 전달할 수 있습니다.

설치 프로세스 중에 호환성 문제를 유발할 수 있는 소프트웨어 검사를 건너뛴 경우 Kaspersky Endpoint Security가 애플리케이션 구성 요소가 변경될 때 이 검사를 다시 수행할 수 있습니다. 설치된 소프트웨어에 대한 검사를 건너뛰려면 *애플리케이션 구성 요소 변경* 작업을 구성해야 합니다.

예:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Kaspersky Endpoint Security를 원격 설치하려면 `[Setup]`에서 `kes_win.kud`라는 이름의 설치 패키지 생성 파일에 적절한 매개변수를 추가해야 합니다(아래 참조). `kes_win.kud` 파일은 배포 키트에 포함되어 있습니다.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

애플리케이션 설치 및 제거

다음과 같은 여러 방법으로 Kaspersky Endpoint Security를 컴퓨터에서 설치할 수 있습니다:

- 로컬에서 설치 마법사 실행.
- 로컬에서 명령줄 실행.
- Kaspersky Security Center 원격 사용.
- Microsoft Windows 그룹 정책 관리 편집기를 사용해 원격으로 작업(자세한 내용은 Microsoft 기술 지원 웹사이트 참조).
- System Center Configuration Manager를 사용해 원격으로 작업.

애플리케이션 설치 설정은 여러 가지 방식으로 구성할 수 있습니다. 여러 가지 방식을 동시에 사용하여 설정을 구성하는 경우 Kaspersky Endpoint Security는 해당 설정에 가장 높은 우선 순위를 적용합니다. Kaspersky Endpoint Security는 다음 순서대로 우선 순위를 사용합니다:

1. setup.ini 파일에서 가져온 설정.
2. installer.ini 파일에서 가져온 설정.
3. 명령줄에서 가져온 설정.
4. 구성 파일(install.cfg)에서 가져온 설정.

Kaspersky Endpoint Security 설치(원격 설치 포함)를 시작하기 전에 열려 있는 모든 애플리케이션을 닫는 것이 좋습니다.

Kaspersky Endpoint Security를 설치할 때 운영 체제에서 자체 메시지를 표시할 수 있습니다. 애플리케이션을 설치하는 동안 네트워크 및 인터넷 연결이 중단될 수 있습니다.

Kaspersky Endpoint Security를 설치, 업데이트 또는 제거할 때 오류가 발생할 수 있습니다. 이러한 오류를 해결하는 방법에 대한 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오.

Kaspersky Security Center를 통한 배포

여러 가지 방식을 통해 기업 네트워크 내에서 Kaspersky Endpoint Security를 배포할 수 있습니다. 조직에 가장 적합한 배포 시나리오를 선택할 수도 있고, 여러 배포 시나리오를 동시에 사용할 수도 있습니다. 애플리케이션을 설치하기 전에 Kaspersky Security Center 네트워크 에이전트가 컴퓨터에 설치되었는지 확인해야 합니다. *네트워크 에이전트*를 설치하면 중앙 관리 서버와 클라이언트 컴퓨터가 원활하게 상호 작용할 수 있습니다.

Kaspersky Security Center는 다음과 같은 주요 배포 수단을 지원합니다:

- Kaspersky 소프트웨어 배포 마법사를 사용하여 애플리케이션 설치.

  Kaspersky Endpoint Security의 기본 설정이 적합하며 조직의 인프라가 단순하여 특수한 구성이 필요하지 않은 경우에는 표준 설치 방법을 사용하면 편리합니다.

- 원격 설치 작업을 사용하여 애플리케이션 설치.

  Kaspersky Endpoint Security 설정을 구성하고 원격 설치 작업을 유동적으로 관리할 수 있는 범용 설치 방법입니다. Kaspersky Endpoint Security를 설치할 때는 다음과 같은 단계를 수행합니다:

  1. 설치 패키지 만들기
  2. 원격 설치 작업 만들기

Kaspersky Security Center에서는 운영 체제 이미지 내의 배포 등 Kaspersky Endpoint Security를 설치하는 다른 방법도 지원합니다. 다른 배포 방법에 관한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.

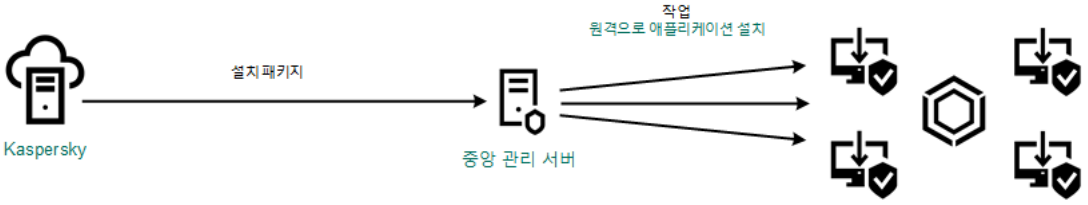
애플리케이션 표준 설치

Kaspersky Security Center에서는 기업 컴퓨터에 애플리케이션을 설치하기 위한 Kaspersky 소프트웨어 배포 마법사를 제공합니다. Kaspersky 소프트웨어 배포 마법사에는 다음과 같은 주요 동작을 실행할 수 있습니다:

1. Kaspersky Endpoint Security 설치 패키지 선택.

   *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 Endpoint Security 설치 패키지는 지원되는 모든 Windows 버전 및 프로세서 아키텍처 유형에 공통적으로 사용됩니다.

2. Kaspersky Security Center 중앙 관리 서버의 *원격으로 애플리케이션 설치* 작업 생성.



Kaspersky Endpoint Security 배포

관리 콘솔(MMC)에서 Kaspersky 소프트웨어 배포 마법사를 실행하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **고급** → **원격 설치**를 선택합니다.
3. **관리 중인 기기에 설치 패키지 배포(워크스테이션)** 링크를 클릭합니다.

그러면 Kaspersky 소프트웨어 배포 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

클라이언트 컴퓨터에서 139/445 TCP 포트와 137/138 UDP 포트가 열려 있어야 합니다.

1단계. 설치 패키지 선택

목록에서 Kaspersky Endpoint Security 설치 패키지를 선택합니다. 목록에 Kaspersky Endpoint Security용 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 Endpoint Security와 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.

2단계. 설치 패키지 경로 선택

Kaspersky Security Center 배포 패키지 소스를 선택합니다.

3단계. 설치할 장치 선택

Kaspersky Endpoint Security를 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.

4단계. 원격 설치 작업 설정 정의

다음과 같은 추가 애플리케이션 설정을 구성하십시오.

- **강제 설치 패키지 다운로드**. 애플리케이션 설치 방법 선택:
  - **네트워크 에이전트 이용**. 네트워크 에이전트는 Kaspersky Endpoint Security 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. 그런 다음 네트워크 에이전트의 도구를 통해 Kaspersky Endpoint Security가 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 Endpoint Security 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.
- **Active Directory 그룹 정책에 네트워크 에이전트 설치 지정**. Active Directory 리소스를 사용하여 네트워크 에이전트 수동 설치. 네트워크 에이전트를 설치하려면 도메인 관리자 권한으로 원격 설치 작업을 실행해야 합니다.

5단계. 라이센스 키 선택

애플리케이션 활성화용 키를 설치 패키지에 추가합니다. 이 단계는 선택입니다. 중앙 관리 서버에 자동 배포 기능이 있는 라이센스 키가 있으면 나중에 해당 키가 자동으로 추가됩니다. *키 추가* 작업을 사용하여 나중에 애플리케이션을 활성화할 수도 있습니다.

6단계. 운영 체제 재시작 설정 선택

컴퓨터를 다시 시작해야 하는 경우 수행할 처리 방법을 선택합니다. Kaspersky Endpoint Security를 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.

7단계. 애플리케이션을 설치하기 전에 호환되지 않는 애플리케이션 제거

호환되지 않는 애플리케이션 목록을 자세히 확인한 다음 이러한 애플리케이션의 제거를 허용합니다. 호환되지 않는 애플리케이션이 컴퓨터에 설치되어 있으면 Kaspersky Endpoint Security 설치가 종료되고 오류가 발생합니다.

8단계. 장치 접근용 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 Endpoint Security를 설치하는 경우에는 계정을 선택할 필요가 없습니다.

9단계. 설치 시작

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔 및 Cloud Console에서 Kaspersky 소프트웨어 배포 마법사를 시작하는 방법

웹 콘솔의 메인 창에서 **발견 및 배포 → 배포 및 할당 → 보호 배포 마법사**를 선택합니다.

그러면 Kaspersky 소프트웨어 배포 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

클라이언트 컴퓨터에서 139/445 TCP 포트와 137/138 UDP 포트가 열려 있어야 합니다.

1단계. 설치 패키지 선택

목록에서 Kaspersky Endpoint Security 설치 패키지를 선택합니다. 목록에 Kaspersky Endpoint Security용 설치 패키지가 포함되어 있지 않으면 마법사에서 패키지를 생성할 수 있습니다. 설치 패키지를 생성하기 위해 배포 패키지를 검색하여 컴퓨터 메모리에 저장할 필요가 없습니다. Kaspersky Security Center에서 Kaspersky 서버에 있는 배포 패키지 목록을 확인할 수 있으며, 설치 패키지는 자동으로 생성됩니다. Kaspersky는 새 버전의 애플리케이션 릴리즈 이후 목록을 업데이트합니다.

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

2단계. 라이센스 키 선택

애플리케이션 활성화용 키를 설치 패키지에 추가합니다. 이 단계는 선택입니다. 중앙 관리 서버에 자동 배포 기능이 있는 라이센스 키가 있으면 나중에 해당 키가 자동으로 추가됩니다. *키 추가* 작업을 사용하여 나중에 애플리케이션을 활성화할 수도 있습니다.

3단계. 네트워크 에이전트 선택

Kaspersky Endpoint Security와 함께 설치할 네트워크 에이전트 버전을 선택합니다. *네트워크 에이전트*를 설치하면 중앙 관리 서버와 클라이언트 컴퓨터가 원활하게 상호 작용할 수 있습니다. 네트워크 에이전트가 컴퓨터에 이미 설치되어 있으면 다시 설치되지 않습니다.

4단계. 설치할 장치 선택

Kaspersky Endpoint Security를 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.

5단계. 고급 설정 구성

다음과 같은 추가 애플리케이션 설정을 구성하십시오.

- **강제 설치 패키지 다운로드**. 애플리케이션 설치 방법 선택:
  - **네트워크 에이전트 이용**. 네트워크 에이전트는 Kaspersky Endpoint Security 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. 그런 다음 네트워크 에이전트의 도구를 통해 Kaspersky Endpoint Security가 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.
- **이미 설치한 애플리케이션은 설치하지 않음**. 이전 버전의 애플리케이션을 설치하려는 등의 경우 이 확인란의 선택을 취소합니다.
- **Active Directory 그룹 정책에 패키지 설치 지정**. Kaspersky Endpoint Security는 네트워크 에이전트를 통해 설치되거나 Active Directory를 통해 직접 설치됩니다. 네트워크 에이전트를 설치하려면 도메인 관리자 권한으로 원격 설치 작업을 실행해야 합니다.

6단계. 운영 체제 재시작 설정 선택

컴퓨터를 다시 시작해야 하는 경우 수행할 처리 방법을 선택합니다. Kaspersky Endpoint Security를 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.

7단계. 애플리케이션을 설치하기 전에 호환되지 않는 애플리케이션 제거

호환되지 않는 애플리케이션 목록을 자세히 확인한 다음 이러한 애플리케이션의 제거를 허용합니다. 호환되지 않는 애플리케이션이 컴퓨터에 설치되어 있으면 Kaspersky Endpoint Security 설치가 종료되고 오류가 발생합니다.

8단계. 관리 그룹에 할당

네트워크 에이전트를 설치한 후 컴퓨터를 이동할 관리 그룹을 선택합니다. 컴퓨터를 관리 그룹으로 이동하면 정책 및 그룹 작업을 적용할 수 있습니다. 컴퓨터가 이미 관리 그룹에 있으면 컴퓨터가 이동되지 않습니다. 관리 그룹을 선택하지 않으면 컴퓨터가 **미할당 기기** 그룹에 추가됩니다.

9단계. 장치 접근용 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 Endpoint Security를 설치하는 경우에는 계정을 선택할 필요가 없습니다.

10 단계. 설치 시작

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

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 Endpoint Security 설치 패키지는 지원되는 모든 Windows 버전 및 프로세서 아키텍처 유형에 공통적으로 사용됩니다.

관리 콘솔(MMC)에서 설치 패키지를 만드는 방법

1. 관리 콘솔에서 **중앙 관리 서버** → **고급** → **원격 설치** → **설치 패키지** 폴더로 이동합니다.
   Kaspersky Security Center로 다운로드한 설치 패키지 목록이 열립니다.
2. **설치 패키지 생성**을 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 Endpoint Security for Windows 14.0* 등).

3단계. 설치할 배포 패키지 선택

찾아보기 버튼을 누르고 배포 키트에 포함된 `kes_win.kud` 파일을 선택합니다.

필요시 **저장소에서 설치 패키지로 업데이트 파일 복사** 확인란을 사용하여 설치 패키지에서 안티 바이러스 데이터베이스를 업데이트합니다.

4단계. 최종 사용자 라이센스 계약서 및 개인정보취급방침

최종 사용자 사용권 라이센스 및 개인정보 취급방침의 약관을 읽고 수락합니다.

설치 패키지가 생성되어 Kaspersky Security Center에 추가됩니다. 설치 패키지를 사용하여 기업 네트워크 컴퓨터에 Kaspersky Endpoint Security를 설치하거나 애플리케이션 버전을 업데이트할 수 있습니다.

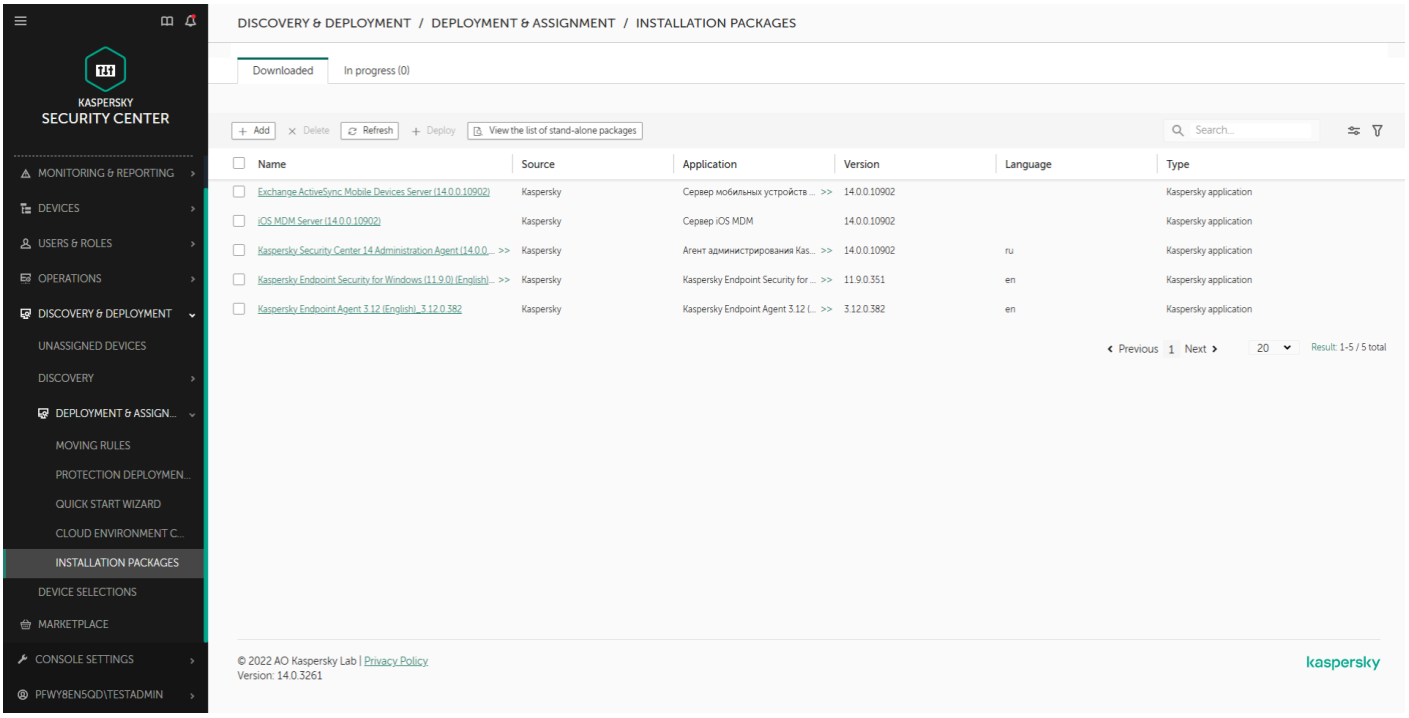
설치 패키지 설정에서 운영 체제 유형별로 애플리케이션 구성 요소를 선택할 수 있습니다. 즉, 설치 패키지에는 워크스테이션용과 서버용의 두 가지 구성 요소 세트가 포함되어 있습니다. 설치 패키지를 배포하기 전에, 설치 프로그램이 운영 체제 유형을 확인하고 해당 운영 체제 유형에 대해 사용자가 선택한 애플리케이션 구성 요소만 설치합니다. 이 방법으로 워크스테이션과 서버에 동일한 설치 패키지를 사용할 수 있습니다.

설치 패키지에는 중앙 관리 서버 저장소에서 복사한 안티 바이러스 데이터베이스가 포함되어 있습니다. Kaspersky Endpoint Security를 설치한 후 데이터베이스를 업데이트할 때 트래픽 소비를 줄이기 위해 설치 패키지에 데이터베이스를 업데이트할 수 있습니다.

웹 콘솔 및 Cloud Console에서 설치 패키지를 생성하는 방법

1. 웹 콘솔의 메인 창에서 **발견 및 배포 → 배포 및 할당 → 설치 패키지**를 클릭합니다.
   Kaspersky Security Center로 다운로드한 설치 패키지 목록이 열립니다.
2. **추가**를 클릭합니다.

   새 패키지 마법사가 시작됩니다. 마법사의 지침을 따릅니다.



설치 패키지 목록

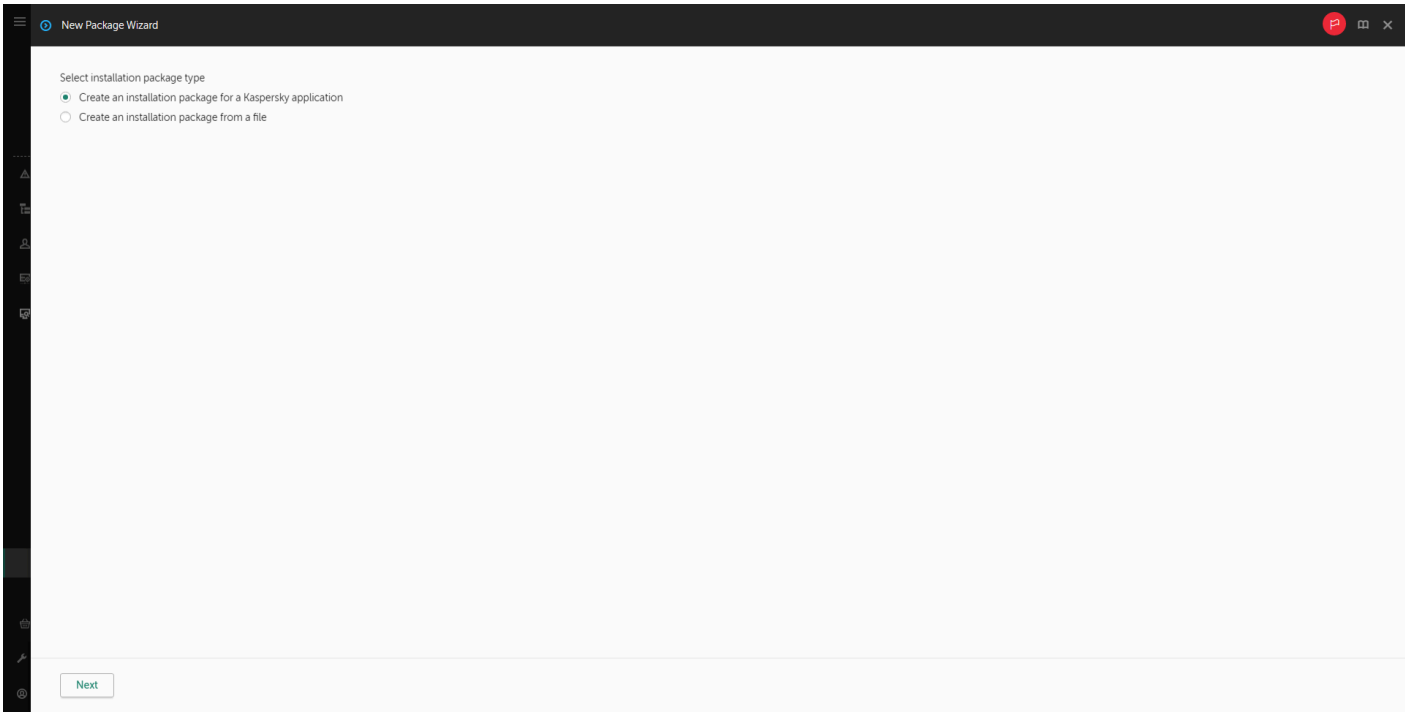
1단계. 설치 패키지 유형 선택

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. Kaspersky Endpoint Security 설치에 대해 이 옵션을 선택하는 것이 좋습니다.

파일로 설치 패키지를 생성할 수도 있습니다.

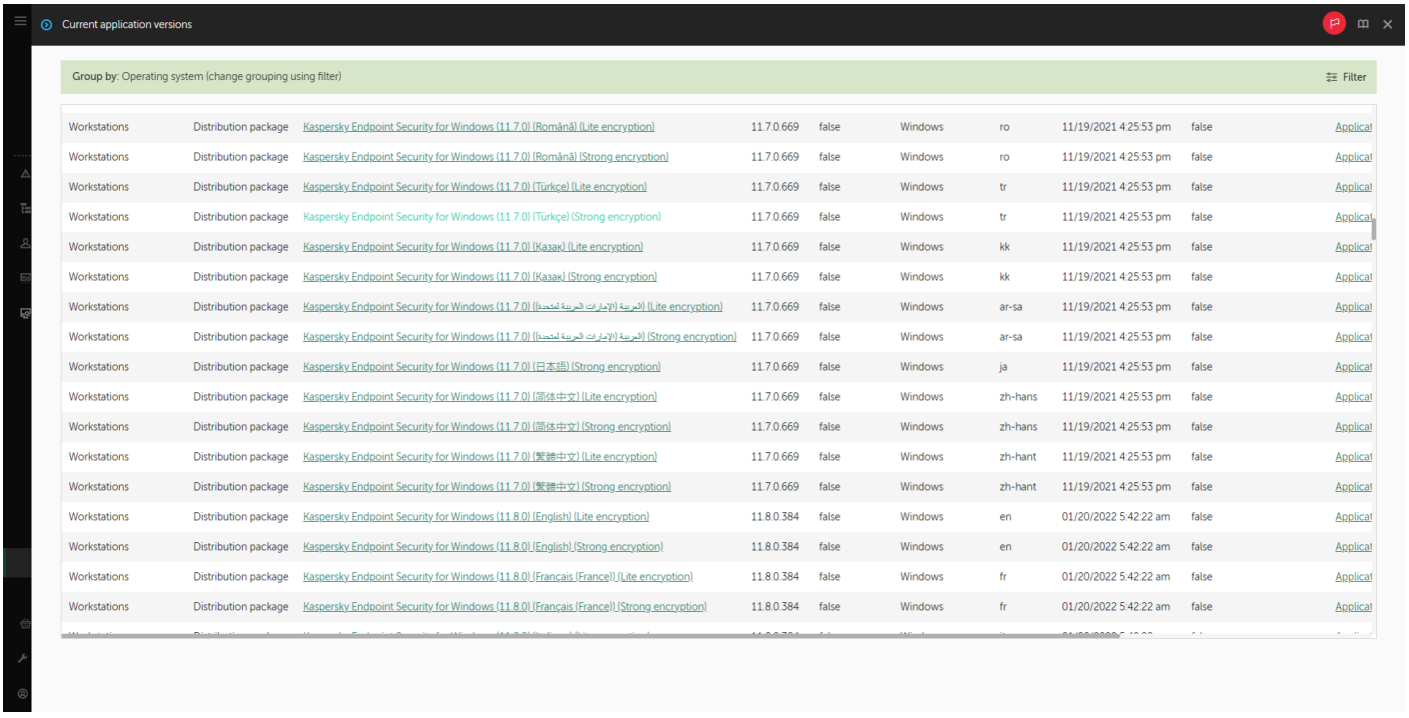
파일에서 Kaspersky Endpoint Security 설치 패키지를 생성하는 것은 Kaspersky Security Center 웹 콘솔에서만 가능합니다.



설치 패키지 유형

2단계. 설치 패키지

Kaspersky Endpoint Security for Windows 설치 패키지를 선택합니다. 설치 패키지 생성 프로세스가 시작됩니다. 설치 패키지를 생성하는 동안 최종 사용자 라이센스 계약서 및 개인정보 취급방침을 반드시 수락해야 합니다.

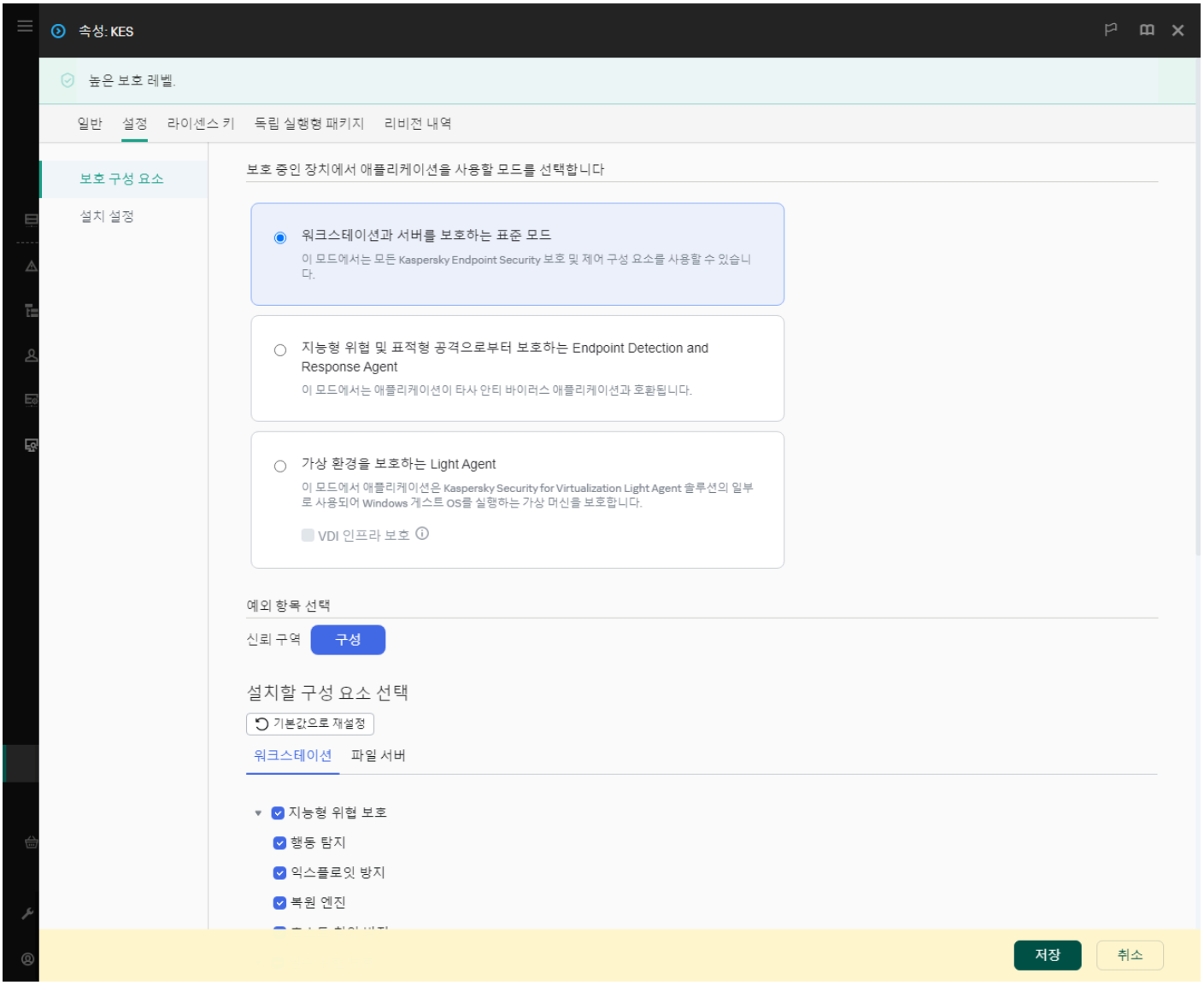


Kaspersky 서버의 설치 패키지 목록

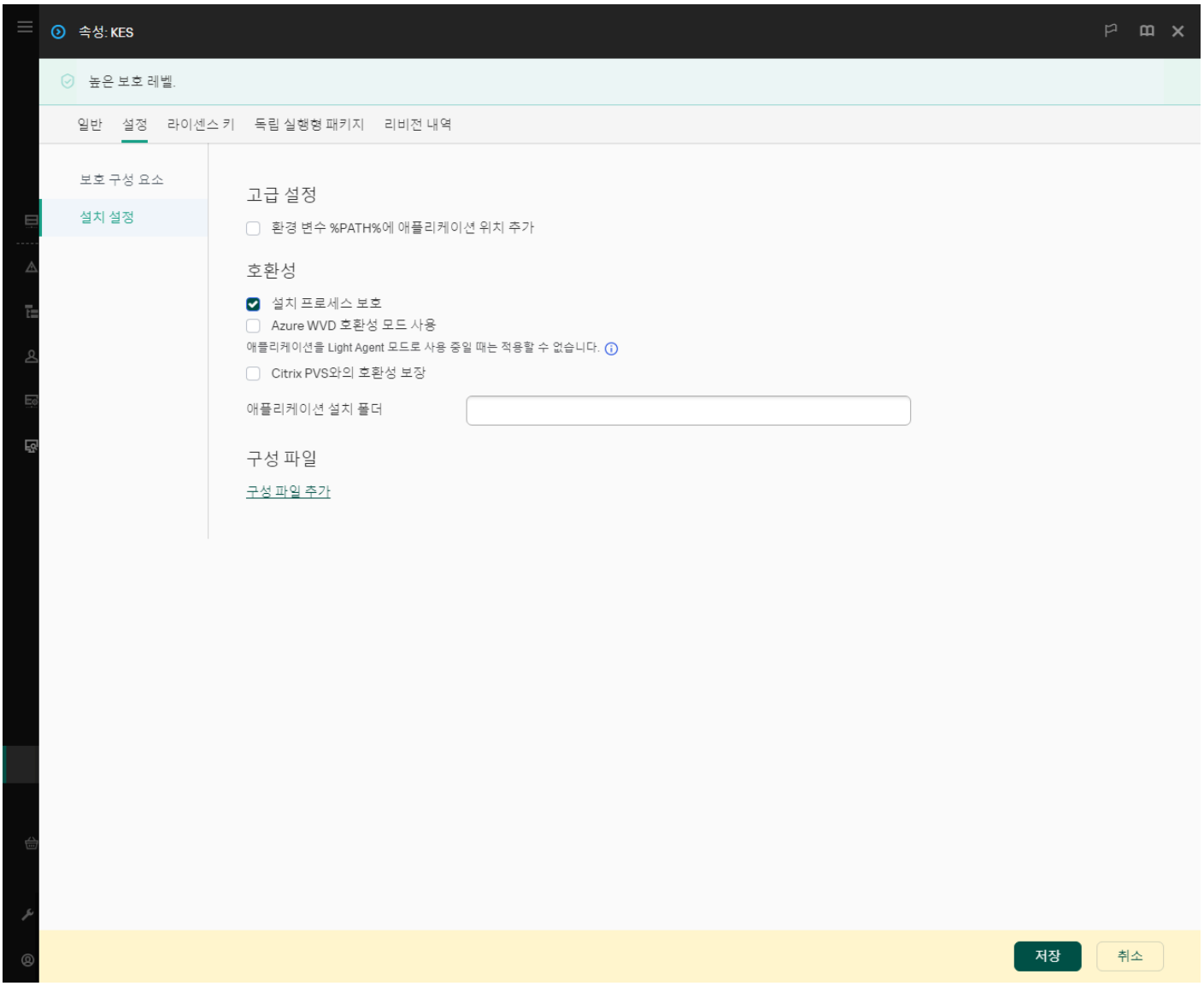
설치 패키지가 생성되어 Kaspersky Security Center에 추가됩니다. 설치 패키지를 사용하여 기업 네트워크 컴퓨터에 Kaspersky Endpoint Security를 설치하거나 애플리케이션 버전을 업데이트할 수 있습니다.

설치 패키지 설정에서 운영 체제 유형별로 애플리케이션 구성 요소를 선택할 수 있습니다. 즉, 설치 패키지에는 워크스테이션용과 서버용의 두 가지 구성 요소 세트가 포함되어 있습니다. 설치 패키지를 배포하기 전에, 설치 프로그램이 운영 체제 유형을 확인하고 해당 운영 체제 유형에 대해 사용자가 선택한 애플리케이션 구성 요소만 설치합니다. 이 방법으로 워크스테이션과 서버에 동일한 설치 패키지를 사용할 수 있습니다.

설치 패키지에는 중앙 관리 서버 저장소에서 복사한 안티 바이러스 데이터베이스가 포함되어 있습니다. Kaspersky Endpoint Security를 설치한 후 데이터베이스를 업데이트할 때 트래픽 소비를 줄이기 위해 설치 패키지에 데이터베이스를 업데이트할 수 있습니다.



설치 패키지에 포함된 구성 요소



설치 패키지의 설치 설정

설치 패키지 설정

섹션	설명
보호 구성 요소	**표준 모드**. 기본 제공 구성입니다. 이 구성을 사용하면 Detection and Response 솔루션을 지원하는 구성 요소들을 포함하여 애플리케이션의 모든 구성 요소를 사용할 수 있습니다. 이 구성은 다양한 유형의 위협, 네트워크 공격 및 사기 등으로부터 컴퓨터를 종합적으로 보호하는 데 사용됩니다. **Endpoint Detection and Response Agent**. 이 구성에서는 Detection and Response 솔루션을 지원하는 구성 요소만 설치할 수 있습니다. MDR, EDR(KATA), NDR(KATA), EDR Expert(on-premise) 및 KUMA. 조직에 타사 Endpoint Protection Platform(EPP)가 Kaspersky Detection and Response 솔루션과 함께 설치된 경우 이 구성이 필요합니다. 이를 통해 Endpoint Detection and Response Agent 구성의 Kaspersky Endpoint Security가 타사 EPP 애플리케이션과 호환됩니다. **가상 환경을 보호하는 Light Agent**. 이 구성은 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 사용되는 애플리케이션을 대상으로 합니다. 솔루션을 사용하여 보호해야 하는 각 가상 컴퓨터에 Light Agent를 설치해야 합니다. 이 구성에서는 데이터 암호화 구성 요소 또는 적응형 이상 행위 제어를 사용할 수 없습니다. *비영구 가상 컴퓨터*를 만드는데 사용될 가상 컴퓨터 템플릿에 Light Agent를 설치하는 경우, **VDI 인프라 보호** 확인란을 선택합니다(VDI는 Virtual Desktop Infrastructure). VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. 이 모드에서 Light Agent는 가상 컴퓨터를 다시 시작해야 하는 애플리케이션 업데이트를 거부합니다. 재시작이 필요한 애플리케이션 업데이트를 수신하면 Light Agent는 보호된 가상 컴퓨터의 템플릿을 업데이트해야 한다는 이벤트를 생성합니다.
예외 규칙	Kaspersky Endpoint Security 12.6 for Windows부터 검사 예외 및 신뢰하는 애플리케이션 이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다. Kaspersky Endpoint Security 12.8 for Windows부터 가상 환경 보호를 위한 Light Agent 모드로 애플리케이션을 설치할 수 있습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 나중에 정책 속성(검사 예외 및 신뢰하는 애플리케이션)에서 신뢰 구역을 구성할 수도 있습니다.

섹션	설명
설치할 구성 요소 선택	이 섹션에서는 제공할 애플리케이션 구성 요소를 선택할 수 있습니다. 나중에 *애플리케이션 구성 요소 변경* 작업을 사용하여 애플리케이션 구성 요소 세트를 변경할 수 있습니다. 워크스테이션과 서버를 위한 구성 요소 세트를 별도로 생성할 수 있습니다. 설치 패키지를 배포하기 전에, 설치 프로그램이 운영 체제 유형을 확인하고 해당 운영 체제 유형에 대해 사용자가 선택한 애플리케이션 구성 요소만 설치합니다. 이 방법으로 워크스테이션과 서버에 동일한 설치 패키지를 사용할 수 있습니다. 애플리케이션 구성에 따라 사용할 수 있는 구성 요소가 다릅니다. **표준 모드** BadUSB 공격 방지 구성 요소, Detection and Response 구성 요소, 데이터 암호화 구성 요소는 기본적으로 설치되지 않습니다. 이러한 구성 요소는 설치 패키지 설정에서 추가할 수 있습니다. **Endpoint Detection and Response Agent** 이 구성에서는 Kaspersky Detection and Response 솔루션용 내장 에이전트만 사용할 수 있습니다. **가상 환경을 보호하는 Light Agent** 이 구성에서는 데이터 암호화 구성 요소와 적응형 이상 제어 기능을 제외한 **표준 모드** 구성에서 사용할 수 있는 거의 모든 응용 프로그램 구성 요소를 사용할 수 있습니다.
라이센스 키	이 섹션에서 애플리케이션을 활성화할 수 있습니다. 애플리케이션을 활성화하려면 라이센스 키를 선택해야 합니다. 그러려면 먼저 키를 중앙 관리 서버에 추가해야 합니다. Kaspersky Security Center 중앙 관리 서버에 키를 추가하는 방법에 대한 자세한 내용은 Kaspersky Security Center 도움말 을 참조하시기 바랍니다.
호환되지 않는 애플리케이션	호환되지 않는 애플리케이션 목록을 자세히 확인한 다음 이러한 애플리케이션의 제거를 허용합니다. 호환되지 않는 애플리케이션이 컴퓨터에 설치되어 있으면 Kaspersky Endpoint Security 설치가 종료되고 오류가 발생합니다.
설치 설정	**시스템 변수 %PATH%에 avp.com 파일 경로 추가**. 명령줄 인터페이스를 편리하게 사용할 수 있도록 %PATH% 변수에 설치 경로를 추가할 수 있습니다. **설치 프로세스 보호**. 설치 보호는 악성 애플리케이션에 의한 배포 패키지 변조 차단, Kaspersky Endpoint Security 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. **Citrix PVS와의 호환성 보장**. 가상 컴퓨터에 Kaspersky Endpoint Security를 설치하기 위해 Citrix Provisioning Services 지원을 작동할 수 있습니다. **Azure WVD 호환성 모드 사용**. 이 기능을 사용하면 Kaspersky Anti Targeted Attack Platform 콘솔에서 Azure 가상 컴퓨터 상태가 올바르게 표시됩니다. 컴퓨터의 성능을 모니터링하기 위해 Kaspersky Endpoint Security는 원격 측정을 KATA 서버로 보냅니다. 원격 측정은 컴퓨터의 ID(Sensor ID)가 포함되어 있습니다. Azure WVD 호환성 모드를 사용하면 이러한 가상 컴퓨터에 영구적인 고유 Sensor ID를 할당할 수 있습니다. 호환성 모드가 꺼져 있으면 Azure 가상 컴퓨터의 작동 방식 때문에 컴퓨터를 다시 시작한 후 Sensor ID가 변경될 수 있습니다. 이로 인해 가상 컴퓨터의 복제본이 콘솔에 나타날 수 있습니다. **애플리케이션 설치 폴더**. 클라이언트 컴퓨터의 Kaspersky Endpoint Security 설치 경로를 변경할 수 있습니다. 애플리케이션은 기본적으로 `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.0` 폴더에 설치됩니다. **구성 파일**. 사전 정의된 설정을 사용하여 애플리케이션 설치. 이렇게 하려면 Kaspersky Endpoint Security의 설정을 정의하는 파일을 업로드해야 합니다. 애플리케이션의 로컬 인터페이스에서 구성 파일을 생성할 수 있습니다.

설치 패키지에 내장된 데이터베이스 업데이트

설치 패키지에는 그 설치 패키지를 생성할 때 중앙 관리 서버 저장소에 업데이트된 최신 안티 바이러스 데이터베이스가 포함되어 있습니다. 설치 패키지를 생성한 후 해당 설치 패키지에서 안티 바이러스 데이터베이스를 업데이트할 수 있습니다. 이렇게 하면 Kaspersky Endpoint Security를 설치한 후 안티 바이러스 데이터베이스를 업데이트할 때 트래픽 소비를 줄일 수 있습니다.

중앙 관리 서버 저장소에 안티 바이러스 데이터베이스를 업데이트하려면 중앙 관리 서버의 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 사용합니다. 중앙 관리 서버 저장소에 안티 바이러스 데이터베이스를 업데이트하는 것에 대한 자세한 내용은 Kaspersky Security Center 도움말 을 참조하시기 바랍니다.

설치 패키지 내의 데이터베이스는 관리 콘솔 및 Kaspersky Security Center 웹 콘솔에서만 업데이트할 수 있습니다. Kaspersky Security Center Cloud 콘솔에서는 설치 패키지의 데이터베이스를 업데이트할 수 없습니다.

관리 콘솔(MMC)을 통해 설치 패키지에서 안티 바이러스 데이터베이스를 업데이트하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔에서 **고급 → 원격 설치 → 설치 패키지** 폴더를 선택합니다.
   Kaspersky Security Center로 다운로드한 설치 패키지 목록이 열립니다.
3. 설치 패키지의 속성을 여십시오.
4. **일반** 섹션에서 **데이터베이스 업데이트** 버튼을 누릅니다.

그러면 설치 패키지 내의 안티 바이러스 데이터베이스가 중앙 관리 서버 저장소에서 업데이트됩니다. 배포 키트에 포함된 `bases.cab` 파일이 `bases` 폴더로 대체됩니다. 업데이트 패키지 파일은 그 폴더 안에 있습니다.

웹 콘솔을 통해 설치 패키지에서 안티 바이러스 데이터베이스를 업데이트하는 방법

1. 웹 콘솔의 메인 창에서 **발견 및 배포 → 배포 및 할당 → 설치 패키지**를 클릭합니다.
   그러면 웹 콘솔에 다운로드된 설치 패키지의 목록이 열립니다.
2. 안티 바이러스 데이터베이스를 업데이트할 Kaspersky Endpoint Security 설치 패키지의 이름을 클릭합니다.
   설치 패키지 속성 창이 열립니다.
3. **일반 정보** 탭에서 **데이터베이스 업데이트** 링크를 클릭합니다.

그러면 설치 패키지 내의 안티 바이러스 데이터베이스가 중앙 관리 서버 저장소에서 업데이트됩니다. 배포 키트에 포함된 `bases.cab` 파일이 `bases` 폴더로 대체됩니다. 업데이트 패키지 파일은 그 폴더 안에 있습니다.

원격 설치 작업 만들기

원격으로 애플리케이션 설치 작업은 Kaspersky Endpoint Security의 원격 설치를 위해 설계되었습니다. *원격으로 애플리케이션 설치* 작업을 통해 애플리케이션의 설치 패키지를 조직의 모든 컴퓨터에 배포할 수 있습니다. 설치 패키지를 배포하기 전에 패키지 내부의 안티 바이러스 데이터베이스를 업데이트하고 설치 패키지 속성에서 사용 가능한 애플리케이션 구성 요소를 선택할 수 있습니다.

관리 콘솔(MMC)에서 원격 설치 작업을 만드는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업**을 선택합니다.
   작업 목록이 열립니다.
3. **새 작업**을 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 Endpoint Security 설치 패키지를 선택합니다. 목록에 Kaspersky Endpoint Security용 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 Endpoint Security와 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 Endpoint Security와 함께 설치됩니다.

4단계. 설정

다음과 같은 추가 애플리케이션 설정을 구성하십시오.

- **강제 설치 패키지 다운로드**. 애플리케이션 설치 방법 선택:
  - **네트워크 에이전트 이용**. 네트워크 에이전트는 Kaspersky Endpoint Security 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. 그런 다음 네트워크 에이전트의 도구를 통해 Kaspersky Endpoint Security가 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 Endpoint Security 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 Endpoint Security를 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 Endpoint Security를 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 Endpoint Security를 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 Endpoint Security for Windows 14.0 설치* 등).

10 단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **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 콘솔 및 Cloud Console에서 원격 설치 작업을 생성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 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**를 선택합니다.
3. **작업 이름** 필드에 *Kaspersky Endpoint Security 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 Endpoint Security를 설치할 컴퓨터를 선택합니다.

3단계. 설치 패키지 구성

이 단계에서는 설치 패키지를 구성합니다:

1. Kaspersky Endpoint Security for Windows (14.0) 설치 패키지를 선택합니다.
2. 네트워크 에이전트 설치 패키지를 선택합니다.
   선택한 네트워크 에이전트 버전이 Kaspersky Endpoint Security와 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 Endpoint Security 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. 그런 다음 네트워크 에이전트의 도구를 통해 Kaspersky Endpoint Security가 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 Endpoint Security 설치 종료 시 오류가 발생하면 설치 작업에서 설치가 자동으로 다시 시작됩니다.

6. 필요시 **이미 설치한 애플리케이션은 설치하지 않음** 확인란 선택을 취소합니다. 그러면 애플리케이션의 이전 버전 중 하나를 설치하는 등의 작업을 수행할 수 있습니다.

7. 필요시 **다운로드하기 전에 운영 체제 유형 확인** 확인란 선택을 취소합니다. 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. 필요시 **Active Directory 그룹 정책에 패키지 설치 지정** 확인란을 선택합니다. Kaspersky Endpoint Security는 네트워크 에이전트를 통해 설치되거나 Active Directory를 통해 직접 설치됩니다. 네트워크 에이전트를 설치하려면 도메인 관리자 권한으로 원격 설치 작업을 실행해야 합니다.

9. 필요시 **실행 중인 애플리케이션의 종료 여부를 사용자에게 물어 보기** 확인란을 선택합니다. Kaspersky Endpoint Security를 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 Endpoint Security 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 Endpoint Security를 설치하는 경우에는 계정을 선택할 필요가 없습니다.

5단계. 작업 생성 완료

마침 버튼을 눌러 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.

마법사를 사용하여 로컬로 애플리케이션 설치

애플리케이션 설치 마법사의 인터페이스는 애플리케이션 설치 단계마다 나타나는 일련의 창으로 구성됩니다. 설치 마법사를 실행하는 데 사용되는 사용자 계정이 관리자 그룹에 있는지 확인합니다.

설치 마법사를 사용하여 애플리케이션을 설치하거나 이전 버전의 애플리케이션에서 업그레이드하려면 다음과 같이 하십시오.

1. 배포 키트 폴더를 사용자의 컴퓨터에 복사합니다.
2. setup_kes.exe를 실행합니다.

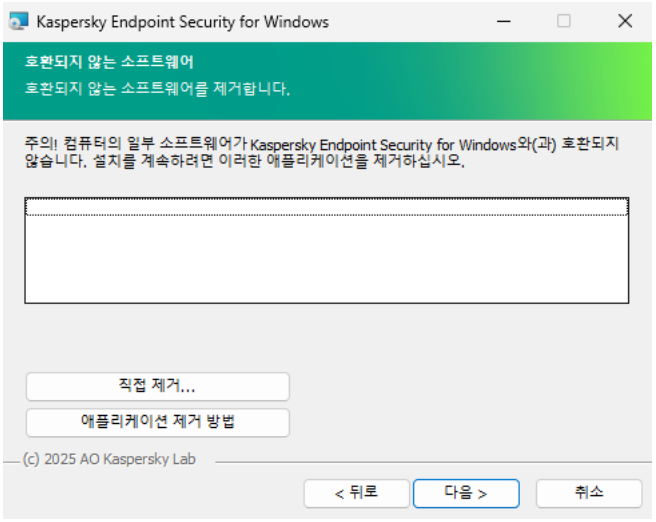
   설치 마법사가 시작됩니다.

설치 준비

컴퓨터에 Kaspersky Endpoint Security를 설치하거나 이전 버전에서 업그레이드하기 전에 다음 조건을 확인해야 합니다.

- Kaspersky Endpoint Security에 호환성 문제가 발생할 수 있는 소프트웨어 유무(소프트웨어 목록은 배포 키트에 포함된 incompatible.txt 파일에서 사용 가능).
- 하드웨어 및 소프트웨어 요구 사항이 충족되는지 여부.
- Microsoft .NET Framework가 존재하는지 여부
- 사용자에게 소프트웨어 제품의 설치 권한이 있는지 여부.

위의 요구 사항 중 어느 하나라도 충족되지 않으면 화면에 관련 알림 정보가 표시됩니다. 예를 들어, 호환되지 않는 소프트웨어에 관한 알림이 표시됩니다(아래 그림 참조).



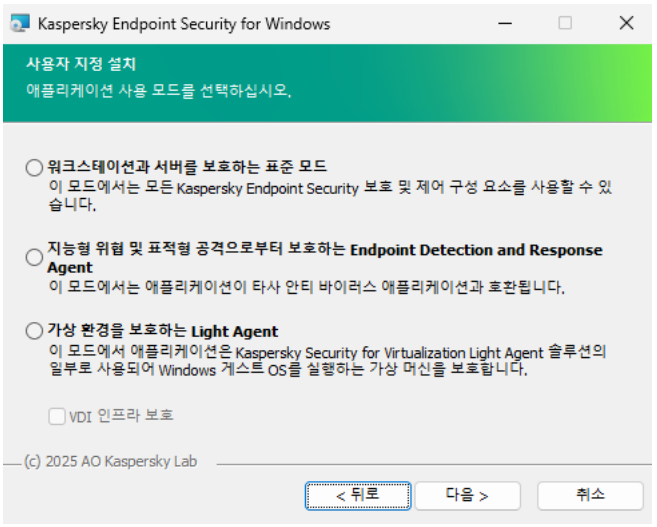
호환되지 않는 소프트웨어 제거

컴퓨터가 나열된 요구 사항을 충족하면 설치 마법사가 설치되는 애플리케이션과의 충돌을 유발할 수 있는 Kaspersky 애플리케이션을 검색합니다. 이러한 애플리케이션이 발견되면 해당 애플리케이션을 직접 제거하라는 메시지가 표시됩니다.

탐지된 애플리케이션에 Kaspersky Endpoint Security 이전 버전이 포함되어 있다면 Kaspersky Endpoint Security 14.0 for Windows 설치 동안 마이그레이션할 수 있는 모든 데이터(활성화 데이터 및 애플리케이션 설정 등)가 유지 및 사용되며 이전 애플리케이션 버전은 자동으로 제거됩니다. 이 내용은 다음 애플리케이션 버전에 적용됩니다:

- Kaspersky Endpoint Security 12.1 for Windows(빌드 12.1.0.506)
- Kaspersky Endpoint Security 12.2 for Windows(빌드 12.2.0.462)
- Kaspersky Endpoint Security 12.3 for Windows(빌드 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows(빌드 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows(빌드 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows(빌드 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows(빌드 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows(빌드 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows(빌드 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows(빌드 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows(빌드 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows(빌드 12.12.0.522)

Kaspersky Endpoint Security 구성



애플리케이션 구성 선택

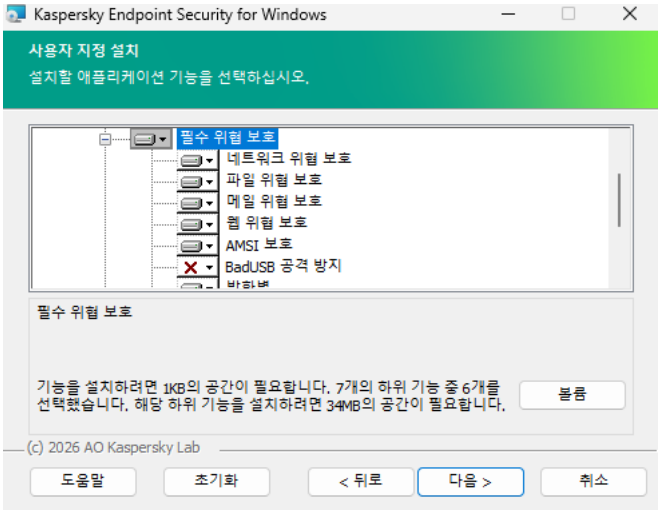
표준 모드. 기본 제공 구성입니다. 이 구성을 사용하면 Detection and Response 솔루션을 지원하는 구성 요소들을 포함하여 애플리케이션의 모든 구성 요소를 사용할 수 있습니다. 이 구성은 다양한 유형의 위협, 네트워크 공격 및 사기 등으로부터 컴퓨터를 종합적으로 보호하는 데 사용됩니다.

Endpoint Detection and Response Agent. 이 구성에서는 Detection and Response 솔루션을 지원하는 구성 요소만 설치할 수 있습니다. MDR, EDR(KATA), NDR(KATA), EDR Expert(on-premise) 및 KUMA. 조직에 타사 Endpoint Protection Platform(EPP)가 Kaspersky Detection and Response 솔루션과 함께 설치된 경우 이 구성이 필요합니다. 이를 통해 Endpoint Detection and Response Agent 구성의 Kaspersky Endpoint Security가 타사 EPP 애플리케이션과 호환됩니다.

가상 환경을 보호하는 Light Agent. 이 구성은 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 사용되는 애플리케이션을 대상으로 합니다. 솔루션을 사용하여 보호해야 하는 각 가상 컴퓨터에 Light Agent를 설치해야 합니다. 이 구성에서는 데이터 암호화 구성 요소 또는 적응형 이상 행위 제어를 사용할 수 없습니다. *비영구 가상 컴퓨터*를 만드는데 사용될 가상 컴퓨터 템플릿에 Light Agent를 설치하는 경우, **VDI 인프라 보호** 확인란을 선택합니다(VDI는 Virtual Desktop Infrastructure). VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. 이 모드에서 Light Agent는 가상 컴퓨터를 다시 시작해야 하는 애플리케이션 업데이트를 거부합니다. 재시작이 필요한 애플리케이션 업데이트를 수신하면 Light Agent는 보호된 가상 컴퓨터의 템플릿을 업데이트해야 한다는 이벤트를 생성합니다.

Kaspersky Endpoint Security 구성 요소

설치 과정 중 설치할 Kaspersky Endpoint Security의 구성 요소를 선택할 수 있습니다(아래 그림 참조). 파일 위협 보호 구성 요소는 반드시 설치해야 하는 필수 구성 요소입니다. 해당 구성 요소 설치를 취소할 수 없습니다.



설치할 애플리케이션 구성 요소 선택

기본적으로 다음 구성 요소를 제외한 모든 애플리케이션 구성 요소의 설치가 선택되어 있습니다:

- BadUSB 공격 방지
- 데이터 암호화 구성 요소
- Detection and Response 구성 요소

애플리케이션을 설치한 후 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다. 이렇게 하려면 설정 마법사를 다시 실행하고 사용 가능한 구성 요소를 변경하도록 선택해야 합니다.

Detection and Response 구성 요소를 설치할 시 Kaspersky Endpoint Security는 다음 구성을 지원합니다:

- Endpoint Detection and Response Optimum만
- Endpoint Detection and Response Expert만
- Endpoint Detection and Response(KATA)만
- Network Detection and Response(KATA)만
- Sandbox만
- Endpoint Detection and Response Optimum 및 Sandbox
- Endpoint Detection and Response Expert 및 Sandbox
- Endpoint Detection and Response(KATA) 및 Sandbox
- Network Detection and Response(KATA) 및 Endpoint Detection and Response(KATA)
- Network Detection and Response(KATA) 및 Managed Detection and Response

Kaspersky Endpoint Security는 애플리케이션을 설치하기 전에 구성 요소의 선택을 확인합니다. 지원하지 않는 Detection and Response 구성 요소의 구성을 선택했다면 Kaspersky Endpoint Security를 설치할 수 없습니다.

애플리케이션을 설치할 폴더 선택

클라이언트 컴퓨터의 Kaspersky Endpoint Security 설치 경로를 변경할 수 있습니다. 애플리케이션은 기본적으로 `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.0` 폴더에 설치됩니다.

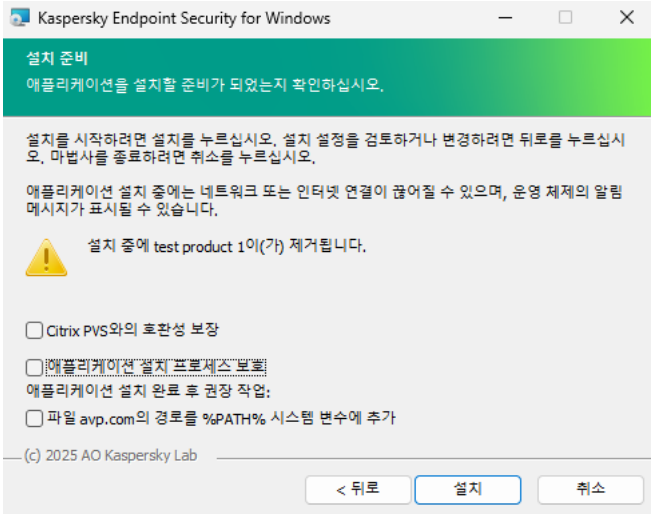
신뢰 구역 구성

Kaspersky Endpoint Security 12.6 for Windows부터 검사 예외 및 신뢰하는 애플리케이션 이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다.

Kaspersky Endpoint Security 12.8 for Windows부터 가상 환경 보호를 위한 Light Agent 모드로 애플리케이션을 설치할 수 있습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다.

나중에 정책 속성(검사 예외 및 신뢰하는 애플리케이션)에서 신뢰 구역을 구성할 수도 있습니다.

고급 설정



고급 애플리케이션 설치 설정

애플리케이션 설치 프로세스 보호. 설치 보호는 악성 애플리케이션에 의한 배포 패키지 변조 차단, Kaspersky Endpoint Security 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.

Citrix PVS와의 호환성 보장. 가상 컴퓨터에 Kaspersky Endpoint Security를 설치하기 위해 Citrix Provisioning Services 지원을 작동할 수 있습니다.

시스템 변수 %PATH%에 avp.com 파일 경로 추가. 명령줄 인터페이스를 편리하게 사용할 수 있도록 %PATH% 변수에 설치 경로를 추가할 수 있습니다.

System Center Configuration Manager를 사용하여 애플리케이션 원격 설치

이 안내는 System Center Configuration Manager 2012 R2에 해당되는 내용입니다.

System Center Configuration Manager를 사용하여 애플리케이션을 원격으로 설치하려면 다음을 수행합니다

1. Configuration Manager 콘솔을 엽니다.
2. 콘솔 오른쪽의 **앱 관리** 블록에서 **패키지**를 선택합니다.
3. 콘솔 위쪽 제어판에서 **패키지 생성** 버튼을 누릅니다.
   *새 패키지 및 애플리케이션 마법사*가 시작됩니다.
4. 새 패키지 및 애플리케이션 마법사:
   a. **패키지** 섹션에서 다음을 수행합니다:
      - **이름** 필드에서 설치 패키지 이름을 입력합니다.
      - **원본 폴더** 필드에 Kaspersky Endpoint Security 배포 패키지가 있는 폴더의 경로를 지정합니다.
   b. **애플리케이션 유형** 섹션에서 **표준 프로그램** 옵션을 선택합니다.
   c. **표준 프로그램** 섹션에서 다음을 수행합니다:
      - **이름** 필드에 설치 패키지 고유 이름을 입력합니다(예: 버전을 포함한 애플리케이션 이름).
      - **명령줄** 필드에서 명령줄의 Kaspersky Endpoint Security 설치 옵션을 지정합니다.
      - **찾아보기** 버튼을 눌러 애플리케이션 실행 파일의 경로를 지정합니다.
      - **실행 모드** 목록에 **관리자 권한으로 실행** 항목이 선택되어 있는지 확인합니다.
   d. **요구 사항** 섹션에서 다음을 수행합니다:
      - Kaspersky Endpoint Security를 설치하기 전 다른 애플리케이션이 먼저 시작하도록 하려면 **다른 프로그램 먼저 시작** 확인란을 선택합니다.
        애플리케이션 드롭다운 목록에서 애플리케이션을 선택하거나 **찾아보기** 버튼을 눌러 이 애플리케이션의 실행 파일 경로를 지정합니다.
      - 애플리케이션이 지정 운영 체제에서만 설치되도록 하려면 **플랫폼 요구 사항** 블록에서 **지정 플랫폼에서만 실행되는 프로그램** 옵션을 선택합니다.
        아래 목록에서 Kaspersky Endpoint Security를 설치할 운영 체제 옆의 확인란을 선택합니다.

이 단계는 선택입니다.

e. **요약** 섹션에서 입력한 모든 설정 값을 확인하고 **다음**을 누릅니다.

생성한 설치 패키지가 **패키지** 섹션의 사용 가능한 설치 패키지 목록에 표시됩니다.

5. 설치 패키지의 마우스 오른쪽 메뉴에서 **배포**를 선택합니다.
*배포 마법사*가 시작됩니다.

6. 배포 마법사:

a. **일반** 섹션에서:

- **소프트웨어** 필드에 설치 패키지 고유 이름을 입력하거나 **찾아보기** 버튼을 눌러 목록에서 설치 패키지를 선택합니다.
- **컬렉션** 필드에 애플리케이션을 설치할 컴퓨터 집합의 이름을 입력하거나 **찾아보기** 버튼을 눌러 컴퓨터 집합을 선택합니다.

b. **포함** 섹션에서 배포 지점을 추가합니다(자세한 내용은 System Center Configuration Manager 도움말 설명서 참조).

c. 필요시 배포 마법사의 다른 설정에 대한 값을 지정합니다. 이러한 설정은 Kaspersky Endpoint Security 원격 설치에 대해 선택적으로 지정합니다.

d. **요약** 섹션에서 입력한 모든 설정 값을 확인하고 **다음**을 누릅니다.

배포 마법사를 종료하면 Kaspersky Endpoint Security 원격 설치 작업이 생성됩니다.

setup.ini 파일 설치 설정 설명

명령줄로 애플리케이션을 설치 또는 Microsoft Windows의 그룹 정책 편집기를 사용하는 경우 setup.ini 파일이 사용됩니다. setup.ini 파일의 설정을 적용하려면 이 파일을 Kaspersky Endpoint Security 배포 패키지가 들어 있는 폴더에 넣습니다.

숨김 모드에서 애플리케이션 설치 시 setup.ini 파일만 사용합니다.

setup.ini 파일에 install.cfg 구성 파일의 경로를 추가할 수 없습니다. install.cfg 구성 파일을 Kaspersky Endpoint Security 배포 키트가 포함된 폴더에 넣으면 애플리케이션은 이 파일을 건너뜁니다. install.cfg 구성 파일의 설정을 적용하려면 다음 애플리케이션 설치 명령으로 파일 경로를 지정해야 합니다: `CONFIGPATH=<path to the configuration file>`.

SETUP.INI 파일 다운로드

setup.ini 파일은 다음 섹션으로 구성되어 있습니다:

- `[Setup]` – 애플리케이션 설치를 위한 일반 설정
- `[Components]` – 표준 모드에서 설치할 애플리케이션 구성 요소 선택. 어떤 구성 요소도 지정하지 않으면 운영 체제에서 지원하는 모든 구성 요소가 설치됩니다. 파일 위협 보호는 반드시 설치해야 하는 구성 요소이며 이 섹션에 표시된 설정에 관계없이 컴퓨터에 설치됩니다.
- `[Tasks]` - Kaspersky Endpoint Security 작업 목록에 포함시킬 작업 선택. 지정된 작업이 없으면 Kaspersky Endpoint Security 작업 목록에 모든 작업이 포함됩니다.

`1` 값을 대체하여 `yes`, `on`, `enable`, `enabled` 및 `true` 값을 사용할 수 있습니다. `0` 값을 대체하여 `no`, `off`, `disable`, `disabled` 및 `false` 값을 사용할 수 있습니다.

setup.ini 파일 설정

섹션	파라미터	설명
[Setup]	InstallDir	애플리케이션 설치 폴더 경로.
	ActivationCode	Kaspersky Endpoint Security 활성화 코드.
	Eula	최종 사용자 라이센스 계약서 조건 동의. 라이센스 계약서는 Kaspersky Endpoint Security 배포 키트에 포함되어 있습니다. 애플리케이션을 설치하거나 애플리케이션 버전을 업데이트하려면 최종 사용자 라이센스 계약서 조건에 동의해야 합니다.
	PrivacyPolicy	개인정보취급방침에 동의함. 개인정보취급방침 전문은 Kaspersky Endpoint Security 배포 키트에 포함되어 있습니다. 애플리케이션을 설치하거나 애플리케이션 버전을 업그레이드하려면 개인정보취급방침에 동의해야 합니다.
	KSN	Kaspersky Security Network(KSN) 참여 동의 또는 거부. 이 파라미터에 대해 값을 설정하지 않으면, Kaspersky Endpoint Security 처음 시작 시 Kaspersky Endpoint Security에서 KSN 참여에 대한 사용자의 동의 또는 거부를 확인하는 메시지가 표시됩니다. 사용 가능한 값: • `1` – KSN 참가 동의 • `0` - KSN 참가 거부(기본값) Kaspersky Endpoint Security 배포 패키지는 Kaspersky Security Network와 함께 사용할 수 있도록 최적화되었습니다. Kaspersky Security Network에 참여하지 않기로 선택한 경우에는 설치가 완료된 후 Kaspersky Endpoint Security를 즉시 업데이트해야 합니다.
	CLEANERSIGNCHECK	incompatible.txt 목록에서 탐지된 소프트웨어 파일의 디지털 서명을 확인합니다. 소프트웨어 제거를 위해 Kaspersky Endpoint Security는 소프트웨어 설치 프로그램 파일을 실행합니다. 설치 프로그램 파일에 디지털 서명이 없을 시, Kaspersky Endpoint Security는 해당 파일을 신뢰할 수 없는 것으로 간주하고 소프트웨어 제거를 중단하여 잠재적 악성 코드 실행을 방지합니다. 애플리케이션이 탐지된 소프트웨어 파일의 디지털 서명을 확인할 수 없을 시, Kaspersky Endpoint Security 설치가 오류와 함께 중지됩니다. 기본값은 소프트웨어 설치 방법에 따라 다릅니다: • `0`은 디지털 서명 확인이 비활성화되었음을 의미합니다(Kaspersky Security Center로 배포 시 기본값). • `1`은 디지털 서명 확인이 활성화되었음을 의미합니다(애플리케이션을 로컬에 설치 시 기본값).
	Login	Kaspersky Endpoint Security의 기능 및 설정에 접근하기 위한 사용자 이름 설정(암호 보호 구성 요소). 사용자 이름은 `Password` 및 `PasswordArea` 설정과 함께 설정됩니다. KLAdmin 사용자 이름이 기본값으로 사용됩니다.
	Password	Kaspersky Endpoint Security 기능 및 설정에 접근하기 위한 암호를 지정합니다(암호와 함께 `Login` 및 `PasswordArea` 파라미터 지정). 암호를 지정했지만 `Login` 변수와 함께 사용자 이름을 지정하지 않은 경우 KLAdmin 사용자 이름이 기본적으로 사용됩니다.

섹션	파라미터	설명
	`PasswordArea`	Kaspersky Endpoint Security에 접근하기 위한 암호 적용 영역을 지정합니다. 사용자가 이 범위에 포함된 동작을 수행하려고 하면 Kaspersky Endpoint Security에서 사용자의 계정 정보(`Login` 및 `Password` 파라미터)를 묻는 메시지를 표시합니다. 여러 값을 지정하려면 `;` 문자를 사용합니다. 사용 가능한 값: • `SET` – 애플리케이션 설정 수정 • `EXIT` – 애플리케이션 종료 • `DISPROTECT` - 보호 구성 요소 및 검사 작업 중지 • `DISPOLICY` - Kaspersky Security Center 정책 사용 안 함 • `UNINST` - 목록에서 애플리케이션 제거 • `DISCTRL` – 제어 구성 요소 중지 • `REMOVELIC` – 키 제거 • `REPORTS` – 리포트 보기 • `EXPORT` – 애플리케이션 설정 내보내기. 예: `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	애플리케이션 설치 보호 메커니즘을 사용하거나 사용하지 않습니다. 사용 가능한 값: • `1` - 애플리케이션 설치 보호 메커니즘이 활성화됩니다(기본 값). • `0` - 애플리케이션 설치 보호 메커니즘이 비활성됩니다. 설치 보호는 악성 애플리케이션에 의한 배포 패키지 변조 차단, Kaspersky Endpoint Security 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.
	`PROTECTOSSERVICES`	운영 체제 서비스 보호 기능입니다. 운영 체제 서비스 보호는 타사 애플리케이션이 운영 체제 서비스의 작동을 방해하는 것을 방지합니다. 예를 들어, 애플리케이션 자동 시작 서비스가 이러한 서비스에 포함됩니다. • `1`은 운영 체제 서비스 보호가 활성화되었음을 의미합니다(기본값). • `0`은 운영 체제 서비스 보호가 비활성화되었음을 의미합니다.
	`EnableAzureSupport`	Azure WVD 호환성 모드 활성화 또는 비활성화. 사용 가능한 값: • `1` – Azure WVD 호환성 모드가 활성화됩니다. • `0` – Azure WVD 호환성 모드가 비활성화됩니다(기본값). 이 기능을 사용하면 Kaspersky Anti Targeted Attack Platform 콘솔에서 Azure 가상 컴퓨터 상태가 올바르게 표시됩니다. 컴퓨터의 성능을 모니터링하기 위해 Kaspersky Endpoint Security는 원격 측정을 KATA 서버로 보냅니다. 원격 측정은 컴퓨터의 ID(Sensor ID)가 포함되어 있습니다. Azure WVD 호환성 모드를 사용하면 이러한 가상 컴퓨터에 영구적인 고유 Sensor ID를 할당할 수 있습니다. 호환성 모드가 꺼져 있으면 Azure 가상 컴퓨터의 작동 방식 때문에 컴퓨터를 다시 시작한 후 Sensor ID가 변경될 수 있습니다. 이로 인해 가상 컴퓨터의 복제본이 콘솔에 나타날 수 있습니다.
	`Reboot`	애플리케이션을 설치하거나 업그레이드한 후 필요시 컴퓨터를 자동으로 다시 시작합니다. 이 파라미터에 대해 설정된 값이 없으면 자동 컴퓨터 다시 시작이 차단됩니다. Kaspersky Endpoint Security를 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.
	`AddEnvironment`	%PATH% 시스템 변수에 Kaspersky Endpoint Security 설치 폴더에 있는 실행 파일 경로를 추가합니다. 사용 가능한 값: • `1` - %PATH% 시스템 변수에 Kaspersky Endpoint Security 설치 폴더에 있는 실행 파일 경로를 추가합니다. • `0` - %PATH% 시스템 변수에 Kaspersky Endpoint Security 설치 폴더에 있는 실행 파일 경로를 추가하지 않습니다.
	`AMPPL`	AM-PPL(Antimalware Protected Process Light) 기술을 사용한 Kaspersky Endpoint Security 프로세스 보호를 작동하거나 중지합니다. AM-PPL 기술에 대한 자세한 내용은 Microsoft 웹사이트를 방문하시기 바랍니다. AM-PPL 기술은 Windows 10 1703(RS2) 버전 이상 및 Windows Server 2019 운영 체제에서 사용할 수 있습니다. 사용 가능한 값: • `1` - AM-PPL 기술을 사용한 Kaspersky Endpoint Security 프로세스 보호가 작동됩니다. • `0` - AM-PPL 기술을 사용한 Kaspersky Endpoint Security 프로세스 보호가 중지됩니다.

섹션	파라미터	설명
	UPGRADEMODE	애플리케이션 업그레이드 모드: • Seamless는 컴퓨터 다시 시작을 포함하는 애플리케이션 업그레이드를 말합니다(기본값). • Force는 다시 시작 없는 애플리케이션 업그레이드를 말합니다. 11.10.0 버전부터 다시 시작 없이 애플리케이션을 업그레이드할 수 있습니다. 이전 버전의 애플리케이션을 업그레이드하려면, 컴퓨터를 다시 시작해야 합니다. 11.11.0 버전부터는 다시 시작 없이도 패치를 설치할 수 있습니다. Kaspersky Endpoint Security를 설치할 때 다시 시작할 필요가 없습니다. 즉, 애플리케이션 설정에서 애플리케이션의 업그레이드 모드를 지정합니다. 애플리케이션 설정 또는 정책에서 이 매개변수를 변경할 수 있습니다. 이미 설치된 애플리케이션 업그레이드 시, setup.ini 파일에 지정한 매개변수의 우선순위가 애플리케이션 설정이나 명령줄에 지정한 매개변수의 우선순위보다 높습니다. 예를 들어 setup.ini 파일에서 Force 업그레이드 모드를 지정하고 애플리케이션 설정에서 Seamless 모드를 지정하면 다시 시작 없이 업그레이드가 설치됩니다(Force). UPGRADEMODE 매개변수를 지정하지 않은 setup.ini 파일 사용 시, 설치 프로그램은 기본값(Seamless)을 사용하여 업그레이드를 설치하고 컴퓨터를 다시 시작합니다.
	SetupReg	setup.reg 파일에서 레지스트리로 레지스트리 키를 추가합니다. SetupReg: setup.reg 파라미터 값.
	EnableTraces	애플리케이션 추적 로그 활성화 또는 비활성화. Kaspersky Endpoint Security가 시작된 후 %ProgramData%\Kaspersky Lab\KES.14.0\Traces 폴더에 추적 파일을 저장합니다. 사용 가능한 값: • 1 - 추적 로그 활성화됨 • 0 – 추적 로그 비활성화됨(기본값)
	TracesLevel	추적로그 기록 레벨. 사용 가능한 값: • 100(심각). 치명적인 오류에 대한 메시지만 기록. • 200(높음). 치명적인 오류를 포함한 모든 오류에 대한 메시지 기록. • 300(진단). 모든 오류와 경고에 대한 메시지 기록. • 400(중요). 모든 오류, 경고 및 추가 정보 메시지 기록. • 500(일반). 모든 오류 및 경고에 대한 메시지뿐만 아니라 일반 모드에서 애플리케이션의 작동에 대한 자세한 정보도 제공합니다(기본값). • 600(낮음). 모든 메시지.
	RESTAPI	REST API를 통해 애플리케이션을 관리합니다. REST API를 통해 애플리케이션을 관리하려면 사용자 이름(RESTAPI_User 파라미터)을 지정해야 합니다. 사용 가능한 값: • 1 – REST API를 통한 관리가 가능합니다. • 0 – REST API를 통한 관리가 차단됩니다(기본값). REST API를 통해 애플리케이션을 관리하려면 관리 시스템을 사용한 관리가 허용되어야 합니다. 이렇게 하려면 AdminKitConnector=1 파라미터를 설정합니다. REST API를 통해 애플리케이션을 관리하면 Kaspersky의 관리 시스템을 사용하여 애플리케이션을 관리할 수 없습니다.
	RESTAPI_User	Windows 도메인 계정은 REST API로 애플리케이션을 관리하기 위해 사용되는 사용자 이름입니다. REST API를 통한 애플리케이션 관리는 이 사용자만 이용할 수 있습니다. 사용자 이름을 <DOMAIN>\<UserName> 형식으로 입력합니다(예: RESTAPI_User=COMPANY\Administrator). REST API로 작업할 사용자를 하나만 선택할 수 있습니다. REST API를 통해 애플리케이션을 관리하기 위해서는 사용자 이름을 추가해야 합니다.
	RESTAPI_Port	REST API를 통해 애플리케이션을 관리하는 데 사용되는 포트입니다. 기본적으로 포트 6782가 사용됩니다. 포트가 사용 가능한 상태인지 확인하십시오.
	RESTAPI_Certificate	요청 식별을 위한 인증서(예: RESTAPI_Certificate=C:\cert.pem). Kaspersky Endpoint Security와 REST 클라이언트의 안전한 상호 작용을 위해서는 요청 식별을 구성해야 합니다. 이렇게 하려면 인증서를 설치한 다음 각 요청의 페이로드에 서명해야 합니다.
	StandaloneMode	Endpoint Detection and Response Agent(EDR Agent) 모드로 애플리케이션 설치. *Endpoint Detection and Response Agent*는 조직의 IT 인프라에 있는 개별 워크스테이션 및 서버에 설치되어 Kaspersky Managed Detection and Response과 Kaspersky Anti Targeted Attack Platform 솔루션을 지원하는 애플리케이션입니다. EDR Agent는 타사 EPP 애플리케이션과 호환됩니다. 이를 통해 Kaspersky Detection and Response와 함께 타사 인프라 보안 도구를 사용할 수 있습니다. EDR Agent를 설치하려면 [Components] 섹션에서 StandaloneKATA, StandaloneNDR 또는 StandaloneMDR 구성 요소를 선택합니다. EDR Agent는 다른 애플리케이션 구성 요소를 지원하지 않습니다. 사용 가능한 값: • 1: EDR Agent 모드에서 애플리케이션을 설치합니다. • 0: 표준 모드(기본값)로 애플리케이션을 설치합니다.

섹션	파라미터	설명
	`KSVLAMode`	Light Agent 모드에서 애플리케이션 설치. 이 구성은 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 사용되는 애플리케이션을 대상으로 합니다. 솔루션을 사용하여 보호해야 하는 각 가상 컴퓨터에 Light Agent를 설치해야 합니다. 사용 가능한 값: • `1`: Light Agent 모드에서 애플리케이션 설치. • `0`: 표준 모드(기본값)로 애플리케이션을 설치합니다.
	`InstallOnVDI`	Light Agent 모드(`KSVLAMode=1`)로 애플리케이션을 설치할 때 VDI 보호 모드를 활성화합니다. VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. 이 모드에서 Light Agent는 가상 컴퓨터를 다시 시작해야 하는 애플리케이션 업데이트를 거부합니다. 재시작이 필요한 애플리케이션 업데이트를 수신하면 Light Agent는 보호된 가상 컴퓨터의 템플릿을 업데이트해야 한다는 이벤트를 생성합니다. 사용 가능한 값: • `1`: VDI 보호 모드를 활성화합니다. • `0`: VDI 보호 모드를 비활성화합니다(기본값).
	`KESExclusions`	서버에 애플리케이션을 설치할 때 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 추가합니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 예를 들어 SQL 서버에 대해 사전 정의된 검사 예외에는 MDF 및 LDF 데이터베이스 파일이 포함됩니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다. 사용 가능한 값: • `1`: 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 활성화합니다. • `0`: 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 비활성화 합니다(기본값).
	`LAExclusions`	가상 컴퓨터에 애플리케이션을 설치할 때 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 추가합니다(Light Agent 모드). 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 사용 가능한 값: • `1`: 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 활성화합니다. • `0`: 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 비활성화 합니다(기본값).
	`EnableUniqueSensorID`	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. 이 알고리즘은 고유한 Sensor ID를 보장합니다. 기본적으로 이 매개변수는 설정되어 있지 않습니다. 애플리케이션은 다음과 같은 경우에 Sensor ID를 상속합니다: • 애플리케이션 버전 업데이트 • [KES+KEA] 구성을 [KES+내장 에이전트] 구성으로 마이그레이션 애플리케이션 복구의 일부로 설치 프로그램은 Sensor ID 상속을 시도합니다. Sensor ID를 복원할 수 없는 경우, 애플리케이션이 새로운 Sensor ID를 생성합니다.
	`CitrixCompatibility`	Citrix Provisioning Services 지원을 활성화하여 가상 컴퓨터에 Kaspersky Endpoint Security를 설치할 수 있습니다.
`[Components]`	`ALL`	모든 구성 요소 설치. 파라미터 값 `1`을 지정하면 각 구성 요소의 설치 설정에 관계없이 모든 구성 요소가 설치됩니다. Detection and Response 솔루션을 지원하는 방식에 따라 Endpoint Detection and Response Optimum과 Kaspersky Sandbox 구성 요소가 컴퓨터에 설치됩니다. Endpoint Detection and Response Expert 구성 요소는 이 구성과 호환되지 않습니다.
	`MailThreatProtection`	메일 위협 보호.
	`WebThreatProtection`	웹 위협 보호.
	`AMSI`	AMSI 보호.
	`HostIntrusionPrevention`	호스트 침입 방지.

섹션	파라미터	설명
	`BehaviorDetection`	행동 탐지.
	`ExploitPrevention`	익스플로잇 방지.
	`RemediationEngine`	복원 엔진.
	`Firewall`	방화벽.
	`NetworkThreatProtection`	네트워크 위협 보호.
	`WebControl`	웹 제어.
	`DeviceControl`	장치 제어.
	`ApplicationControl`	애플리케이션 제어.
	`AdaptiveAnomaliesControl`	적응형 이상 행위 제어.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	로그 검사
	`AntiCryptor`	Anti-Cryptor
	`FileThreatProtection`	파일 위협 보호
	`SystemIntegrityMonitor`	시스템 무결성 모니터링.
	`FileEncryption`	파일 레벨 암호화 라이브러리.
	`DiskEncryption`	전체 디스크 암호화 라이브러리.
	`MSBitLocker`	BitLocker 암호화 관리 라이브러리.
	`BadUSBAttackPrevention`	BadUSB 공격 방지.
	`EDR`	Endpoint Detection and Response Optimum(EDR Optimum). 구성 요소는 EDR Expert(`EDRCloud`) 및 EDR(KATA)(`EDRKATA`) 구성 요소와 호환되지 않습니다.
	`EDRCloud`	Endpoint Detection and Response Expert(EDR Expert). 구성 요소는 EDR Optimum(`EDR`) 및 EDR(KATA)(`EDRKATA`) 구성 요소와 호환되지 않습니다.
	`AntiAPT`	Endpoint Detection and Response(KATA). 구성 요소는 EDR Expert(`EDRCloud`) 및 EDR Optimum(`EDR`) 구성 요소와 호환되지 않습니다.
	`SB`	Kaspersky Sandbox 또는 KATA Sandbox. *Kaspersky Sandbox*는 Kaspersky의 독립 실행형 Detection and Response 솔루션입니다. *KATA Sandbox*는 Kaspersky Anti Targeted Attack Platform 솔루션의 구성 요소입니다.
	`MDR`	Managed Detection and Response.
	`NDR`	Network Detection and Response(KATA). 구성 요소는 EDR Expert(`EDRCloud`) 및 EDR Optimum(`EDR`) 구성 요소와 호환되지 않습니다.

섹션	파라미터	설명
	`AdminKitConnector`	관리 시스템을 사용하여 애플리케이션을 관리합니다. 예를 들어 관리 시스템에는 Kaspersky Security Center가 포함됩니다. Kaspersky 관리 시스템 외에도 타사 솔루션을 사용할 수 있습니다. Kaspersky Endpoint Security는 이러한 용도로 API를 제공합니다. 사용 가능한 값: • `1` – 관리 시스템의 도움을 받아 애플리케이션을 관리할 수 있습니다(기본값). • `0` – 로컬 인터페이스를 통해서만 애플리케이션 관리가 가능합니다.
	`KUMAIntegration`	KUMA과 통합.
	`StandaloneKATA`	Kaspersky Anti Targeted Attack Platform(EDR)과의 통합을 위해 Endpoint Detection and Response Agent(EDR Agent) 모드에 애플리케이션 설치.
	`StandaloneMDR`	Kaspersky Managed Detection and Response와의 통합을 위해 Endpoint Detection and Response Agent(EDR Agent) 모드에 애플리케이션 설치.
	`StandaloneNDR`	Kaspersky Anti Targeted Attack Platform(NDR)과의 통합을 위해 Endpoint Detection and Response Agent(EDR Agent) 모드에 애플리케이션 설치.
	`StandaloneSiemTelemetry`	KUMA와의 통합을 위해 Endpoint Detection and Response Agent(EDR Agent) 모드에 애플리케이션 설치.
`[Tasks]`	`ScanMyComputer`	컴퓨터 전체 검사 작업. 사용 가능한 값: • `1` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함됩니다. • `0` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함되지 않습니다.
	`ScanCritical`	중요 영역 검사 작업. 사용 가능한 값: • `1` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함됩니다. • `0` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함되지 않습니다.
	`Updater`	업데이트 작업. 사용 가능한 값: • `1` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함됩니다. • `0` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함되지 않습니다.

애플리케이션 구성 요소 변경

애플리케이션을 설치하는 동안 사용 가능한 구성 요소를 선택할 수 있습니다. 다음과 같은 방법으로 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다.

- 로컬에서 설치 마법사 실행.

  애플리케이션 구성 요소가 Windows 운영 체제의 정상적인 방법, 즉 제어판을 통해 변경됩니다. 애플리케이션 설정 마법사를 실행하고 사용 가능한 애플리케이션 구성 요소를 변경하는 옵션을 선택합니다. 화면에 표시된 지침을 따릅니다.

  > Kaspersky Security Center를 통해 애플리케이션을 설치한 경우에는 이 방법을 사용할 수 없습니다. 로컬로 애플리케이션 설치 후에만 제어판의 애플리케이션 구성 요소 선택을 변경할 수 있습니다.

- Kaspersky Security Center 원격 사용.

  애플리케이션 구성 요소 변경 작업을 사용하면 애플리케이션을 설치한 이후에도 Kaspersky Endpoint Security의 구성 요소를 변경할 수 있습니다.

애플리케이션 구성 요소를 변경할 때는 다음 사항을 고려하시기 바랍니다:

- Windows Server를 실행하는 컴퓨터에서는 Kaspersky Endpoint Security의 모든 구성 요소를 설치할 수 없습니다(예: 적응형 이상 행위 제어 구성 요소를 사용할 수 없음).

- 컴퓨터의 하드 드라이브가 FDE(전체 디스크 암호화)로 보호되는 경우에는 전체 디스크 암호화 구성 요소를 제거할 수 없습니다. 전체 디스크 암호화 구성 요소를 제거하려면 컴퓨터의 모든 하드 드라이브의 복호화해야 합니다.

- 컴퓨터에 암호화된 파일(FLE)이 있거나 사용자가 암호화된 이동식 드라이브(FDE 또는 FLE)를 사용하는 경우에는 데이터 암호화 구성 요소가 제거된 후 파일 및 이동식 드라이브에 접근할 수 없습니다. 데이터 암호화 구성 요소를 다시 설치하여 파일 및 이동식 드라이브에 접근할 수 있습니다.

- VDI 인프라에 Light Agent 모드로 애플리케이션을 설치한 경우, 설정된 구성 요소를 변경하는 것은 지원되지 않습니다.

관리 콘솔(MMC)에서 애플리케이션 구성 요소를 추가하거나 제거하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **설치할 구성 요소 선택**을 선택합니다.

2단계. 애플리케이션 구성 요소 변경을 위한 작업 설정

애플리케이션 구성을 선택합니다.

- **호스트를 보호하는 표준 모드**. 기본 제공 구성입니다. 이 구성을 사용하면 Detection and Response 솔루션을 지원하는 구성 요소들을 포함하여 애플리케이션의 모든 구성 요소를 사용할 수 있습니다. 이 구성은 다양한 유형의 위협, 네트워크 공격 및 사기 등으로부터 컴퓨터를 종합적으로 보호하는 데 사용됩니다.

- **지능형 위협 및 표적형 공격으로부터 보호하는 Endpoint Detection and Response Agent**. 이 구성에서는 Detection and Response 솔루션을 지원하는 구성 요소만 설치할 수 있습니다. MDR, EDR(KATA), NDR(KATA), EDR Expert(on-premise) 및 KUMA. 조직에 타사 Endpoint Protection Platform(EPP)가 Kaspersky Detection and Response 솔루션과 함께 설치된 경우 이 구성이 필요합니다. 이를 통해 Endpoint Detection and Response Agent 구성의 Kaspersky Endpoint Security가 타사 EPP 애플리케이션과 호환됩니다.

  MDR과 함께 작동하도록 EDR 에이전트의 애플리케이션 구성을 변경할 때 원격 측정 수신을 담당하는 구성 요소가 활성화되었는지 확인하십시오.

- **가상 환경을 보호하는 Light Agent**. 이 구성은 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 사용되는 애플리케이션을 대상으로 합니다. 솔루션을 사용하여 보호해야 하는 각 가상 컴퓨터에 Light Agent를 설치해야 합니다. 이 구성에서는 데이터 암호화 구성 요소 또는 적응형 이상 행위 제어를 사용할 수 없습니다. *비영구 가상 컴퓨터*를 만드는데 사용될 가상 컴퓨터 템플릿에 Light Agent를 설치하는 경우, **VDI 인프라 보호** 확인란을 선택합니다(VDI는 Virtual Desktop Infrastructure). VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. 이 모드에서 Light Agent는 가상 컴퓨터를 다시 시작해야 하는 애플리케이션 업데이트를 거부합니다. 재시작이 필요한 애플리케이션 업데이트를 수신하면 Light Agent는 보호된 가상 컴퓨터의 템플릿을 업데이트해야 한다는 이벤트를 생성합니다.

사용자 컴퓨터에서 사용 가능한 애플리케이션 구성 요소를 선택합니다.

3단계. 고급 설정

작업에 대한 고급 설정을 구성합니다(아래 표 참조).

4단계. 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.

5 단계. 작업 시작 스케줄 구성

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

6단계. 작업 이름 정의

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

7단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔 및 Cloud Console에서 애플리케이션 구성 요소를 추가하거나 제거하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 일반 작업 설정 구성

일반 작업 설정을 구성하려면 다음을 수행하십시오.

1. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
2. **작업 유형** 드롭다운 목록에서 **애플리케이션 구성 요소 변경**을 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

생성이 완료되면 작업 세부 정보 열기 확인란을 선택하고 마법사를 완료하십시오.

작업 속성에서 **애플리케이션 설정** 탭을 선택합니다. 다음으로 애플리케이션 구성을 선택합니다.

- **워크스테이션과 서버를 보호하는 표준 모드**. 기본 제공 구성입니다. 이 구성을 사용하면 Detection and Response 솔루션을 지원하는 구성 요소들을 포함하여 애플리케이션의 모든 구성 요소를 사용할 수 있습니다. 이 구성은 다양한 유형의 위협, 네트워크 공격 및 사기 등으로부터 컴퓨터를 종합적으로 보호하는 데 사용됩니다.
- **지능형 위협 및 표적형 공격으로부터 보호하는 Endpoint Detection and Response Agent**. 이 구성에서는 Detection and Response 솔루션을 지원하는 구성 요소만 설치할 수 있습니다. MDR, EDR(KATA), NDR(KATA), EDR Expert(on-premise) 및 KUMA. 조직에 타사 Endpoint Protection Platform(EPP)가 Kaspersky Detection and Response 솔루션과 함께 설치된 경우 이 구성이 필요합니다. 이를 통해 Endpoint Detection and Response Agent 구성의 Kaspersky Endpoint Security가 타사 EPP 애플리케이션과 호환됩니다.

  MDR과 함께 작동하도록 EDR 에이전트의 애플리케이션 구성을 변경할 때 원격 측정 수신을 담당하는 구성 요소가 활성화되었는지 확인하십시오.

- **가상 환경을 보호하는 Light Agent**. 이 구성은 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 사용되는 애플리케이션을 대상으로 합니다. 솔루션을 사용하여 보호해야 하는 각 가상 컴퓨터에 Light Agent를 설치해야 합니다. 이 구성에서는 데이터 암호화 구성 요소 또는 적응형 이상 행위 제어를 사용할 수 없습니다. *비영구 가상 컴퓨터*를 만드는데 사용될 가상 컴퓨터 템플릿에 Light Agent를 설치하는 경우, **VDI 인프라 보호** 확인란을 선택합니다(VDI는 Virtual Desktop Infrastructure). VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. 이 모드에서 Light Agent는 가상 컴퓨터를 다시 시작해야 하는 애플리케이션 업데이트를 거부합니다. 재시작이 필요한 애플리케이션 업데이트를 수신하면 Light Agent는 보호된 가상 컴퓨터의 템플릿을 업데이트해야 한다는 이벤트를 생성합니다.

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

그 결과 사용자 컴퓨터의 Kaspersky Endpoint Security 구성 요소 세트가 숨김 모드로 변경됩니다. 사용 가능한 구성 요소의 설정이 애플리케이션의 로컬 인터페이스에 표시됩니다. 애플리케이션에 포함되지 않은 구성 요소는 사용할 수 없으며 해당 구성 요소의 설정을 사용할 수 없습니다.

Kaspersky Endpoint Security를 설치, 업데이트 또는 제거할 때 오류가 발생할 수 있습니다. 이러한 오류를 해결하는 방법에 대한 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오.

작업에 대한 고급 설정

파라미터	설명
작업 설정	**호환되지 않는 타사 애플리케이션 확인**. 기본적으로 Kaspersky Endpoint Security는 설치된 애플리케이션의 호환성을 확인합니다. 호환성 문제를 유발할 수 있는 소프트웨어 목록은 incompatible.txt 파일에서 이용 가능합니다. 이 파일은 배포 키트에 포함되어 있습니다. 설치된 소프트웨어 검사를 사용하는 경우 목록에 있는 애플리케이션이 탐지되면 Kaspersky Endpoint Security가 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 파일에 나열된 애플리케이션 자동 제거. 이 기능을 활성화하면 Kaspersky Endpoint Security는 작업을 계속하기 위해 호환성 문제를 유발할 수 있는 애플리케이션을 제거하려고 시도합니다. **Azure WVD 호환성 모드 사용**. 이 기능을 사용하면 Kaspersky Anti Targeted Attack Platform 콘솔에서 Azure 가상 컴퓨터 상태가 올바르게 표시됩니다. 컴퓨터의 성능을 모니터링하기 위해 Kaspersky Endpoint Security는 원격 측정을 KATA 서버로 보냅니다. 원격 측정은 컴퓨터의 ID(Sensor ID)가 포함되어 있습니다. Azure WVD 호환성 모드를 사용하면 이러한 가상 컴퓨터에 영구적인 고유 Sensor ID를 할당할 수 있습니다. 호환성 모드가 꺼져 있으면 Azure 가상 컴퓨터의 작동 방식 때문에 컴퓨터를 다시 시작한 후 Sensor ID가 변경될 수 있습니다. 이로 인해 가상 컴퓨터의 복제본이 콘솔에 나타날 수 있습니다.
예외 규칙	Kaspersky Endpoint Security 12.6 for Windows부터 검사 예외 및 신뢰하는 애플리케이션 이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다. Kaspersky Endpoint Security 12.8 for Windows부터 가상 환경 보호를 위한 Light Agent 모드로 애플리케이션을 설치할 수 있습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 나중에 정책 속성(검사 예외 및 신뢰하는 애플리케이션)에서 신뢰 구역을 구성할 수도 있습니다.
개별 모드 / 조합된 모드	워크스테이션과 서버를 위한 구성 요소 세트를 별도로 생성할 수 있습니다(**개별 모드**). 설치 패키지를 배포하기 전에, 설치 프로그램이 운영 체제 유형을 확인하고 해당 운영 체제 유형에 대해 사용자가 선택한 애플리케이션 구성 요소만 설치합니다. 이 방법으로 워크스테이션과 서버에 동일한 설치 패키지를 사용할 수 있습니다. **조합된 모드**에서는 워크스테이션 및 서버용 구성 요소의 일반 목록을 제공합니다. 개별 구성 요소의 사용 가능 여부는 운영 체제 유형에 따라 다릅니다. 이 모드에서는 워크스테이션용 설치 패키지와 서버용 설치 패키지를 별도로 생성하는 것이 좋습니다. 설치 패키지의 일반 구성 요소 목록은 표준 모드에서만 구성할 수 있습니다.
애플리케이션 구성 요소 변경 시 암호 사용	관리자는 일반적으로 암호 보호를 사용하여 Kaspersky Endpoint Security에 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.
Kaspersky Endpoint Agent 및 Kaspersky Security for Windows Server 제거 시 암호 사용	Kaspersky Endpoint Agent(KEA) 및 Kaspersky Security for Windows Server(KSWS)에 대한 액세스를 제한하기 위해 관리자는 일반적으로 이러한 작업에 대한 설정에서 암호 보호를 활성화합니다. 즉, [KES+KEA] 구성에서 [KES+내장 에이전트]로 마이그레이션하거나 KSWS에서 KES로 마이그레이션하는 경우 이러한 애플리케이션을 제거하려면 암호를 입력해야 합니다.

이전 버전의 애플리케이션 업그레이드 중

이전 버전의 애플리케이션을 최신 버전으로 업데이트할 때는 다음을 고려해야 합니다.

- Kaspersky Endpoint Security 새 버전의 언어와 설치한 버전의 애플리케이션 언어가 일치해야 합니다. 애플리케이션의 언어가 일치하지 않으면 애플리케이션 업그레이드가 오류와 함께 완료될 수 있습니다.
- 업데이트를 시작하기 전에 모든 실행 중인 애플리케이션을 종료하는 것이 좋습니다.
- 업데이트하기 전에 Kaspersky Endpoint Security는 전체 디스크 암호화 기능을 차단합니다. 전체 디스크 암호화를 잠글 수 없으면 업데이트 설치가 시작되지 않습니다. 애플리케이션을 업데이트하면 전체 디스크 암호화 기능이 복원됩니다.

Kaspersky Endpoint Security는 다음 버전의 애플리케이션에 대한 업데이트를 지원합니다:

- Kaspersky Endpoint Security 12.1 for Windows(빌드 12.1.0.506)
- Kaspersky Endpoint Security 12.2 for Windows(빌드 12.2.0.462)
- Kaspersky Endpoint Security 12.3 for Windows(빌드 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows(빌드 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows(빌드 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows(빌드 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows(빌드 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows(빌드 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows(빌드 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows(빌드 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows(빌드 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows(빌드 12.12.0.522)

Kaspersky Endpoint Security를 설치, 업데이트 또는 제거할 때 오류가 발생할 수 있습니다. 이러한 오류를 해결하는 방법에 대한 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오.

애플리케이션 업그레이드 방법

다음과 같은 여러 방법으로 Kaspersky Endpoint Security를 컴퓨터에서 업데이트할 수 있습니다:

- Kaspersky 업데이트 서비스 사용(Seamless Update – SMU).
- 로컬에서 설치 마법사 실행.
- 로컬에서 명령줄 실행.
- Kaspersky Security Center 원격 사용.
- Microsoft Windows 그룹 정책 관리 편집기를 사용해 원격으로 작업(자세한 내용은 Microsoft 기술 지원 웹사이트 참조).
- System Center Configuration Manager를 사용해 원격으로 작업.

기업 네트워크에 배포된 애플리케이션이 기본 구성 요소 집합 이외의 다른 구성 요소 집합이 있는 경우, 관리 콘솔(MMC)을 통한 애플리케이션 업데이트가 웹 콘솔 및 Cloud Console을 통한 애플리케이션 업데이트와 다릅니다. Kaspersky Endpoint Security를 업데이트할 때 고려할 사항은 다음과 같습니다.

- Kaspersky Security Center 웹 콘솔 또는 Kaspersky Security Center Cloud Console.

  기본 구성 요소 집합이 있는 애플리케이션의 새 버전을 설치하기 위해 설치 패키지를 만든 경우 사용자 컴퓨터에 있는 구성 요소 집합이 변경되지 않습니다. Kaspersky Endpoint Security를 기본 구성 요소 집합과 함께 사용하려면 설치 패키지 속성을 열고, 구성 요소 집합은 변경한 다음 원래 구성 요소 집합으로 복원한 후 변경 사항을 저장해야 합니다.

- Kaspersky Security Center 관리 콘솔

  업데이트 후 애플리케이션 구성 요소 집합은 설치 패키지의 구성 요소 집합과 일치하게 됩니다. 즉, 새 버전의 애플리케이션에 기본 구성 요소 집합이 있는 경우, 예를 들어, BadUSB 공격 방지 기능이 기본 구성 요소 집합에서 제외되기 때문에 컴퓨터에서도 해당 기능이 제거됩니다. 업데이트하기 전과 동일한 구성 요소 집합으로 애플리케이션을 계속 사용하려면 설치 패키지 설정에서 필요한 구성 요소를 선택하십시오.

다시 시작 없이 애플리케이션 업그레이드

다시 시작 없이 애플리케이션을 업그레이드하면 애플리케이션 버전이 업데이트될 때 서버가 중단 없이 작동합니다.

다시 시작 없이 애플리케이션을 업그레이드할 때는 다음 제한 사항이 따릅니다.

- 11.10.0 버전부터 다시 시작 없이 애플리케이션을 업그레이드할 수 있습니다. 이전 버전의 애플리케이션을 업그레이드하려면, 컴퓨터를 다시 시작해야 합니다.
- 11.11.0 버전부터는 다시 시작 없이 패치를 설치할 수 있습니다. 이전 버전의 애플리케이션용 패치를 설치하려면 컴퓨터를 다시 시작해야 합니다.

- 데이터 암호화(Kaspersky 암호화(FDE), BitLocker, 파일 레벨 암호화(FLE))를 활성화한 컴퓨터에서는 다시 시작 없이 애플리케이션을 업그레이드할 수 없습니다. 데이터 암호화를 활성화한 컴퓨터에서 애플리케이션을 업그레이드하려면 컴퓨터를 다시 시작해야 합니다.

- 다시 시작하지 않으면 가상 컴퓨터에서 애플리케이션을 업그레이드할 수 없습니다. 가상 컴퓨터에서 애플리케이션을 업그레이드하려면 가상 컴퓨터를 다시 시작해야 합니다.

애플리케이션 업그레이드, 패치 설치, 애플리케이션 구성 요소 세트 변경 또는 복원 후 Kaspersky Endpoint Security는 새 버전의 사용을 시작하기 위해 다시 시작됩니다. Kaspersky Endpoint Security 재시작은 1분 정도 걸릴 수 있습니다. 이 시간 동안 컴퓨터 보호 레벨이 낮아집니다. 애플리케이션을 재시작하면 컴퓨터의 보호 레벨이 복원됩니다.

관리 콘솔(MMC)에서 애플리케이션 업그레이드 모드를 선택하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **사용자 상호 작용**으로 갑니다.

5. **애플리케이션 업데이트 설정** 블록에서 **재시작 없이 애플리케이션 업데이트 설치** 확인란을 사용하여 애플리케이션 업그레이드 모드를 구성합니다.

6. 변경 사항을 저장합니다.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

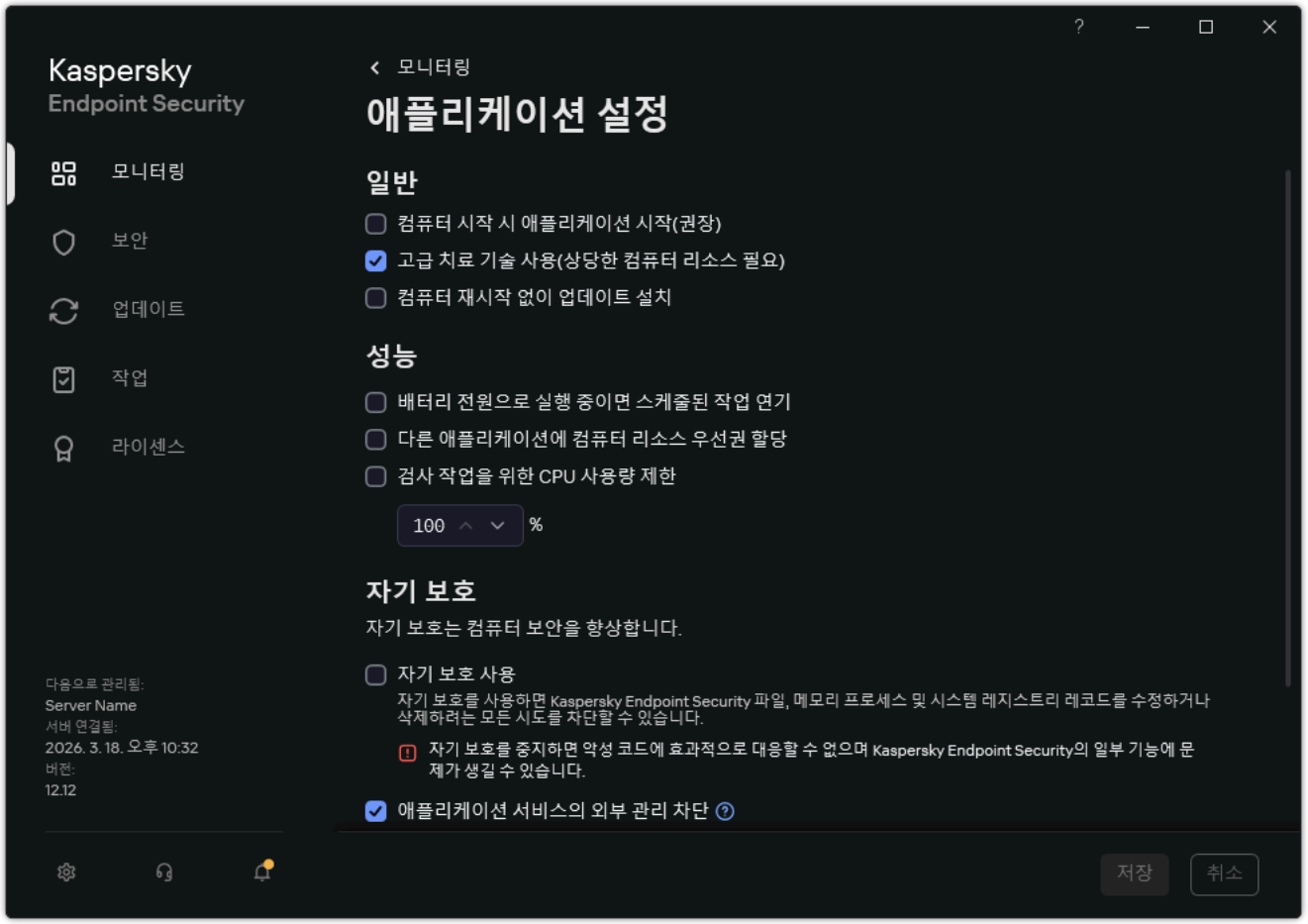
3. 정책 창에서 **일반 설정** → **애플리케이션 설정**을 차례로 선택합니다.

4. **고급 설정** 블록에서 **재시작 없이 애플리케이션 업데이트 설치** 확인란을 사용하여 애플리케이션 업그레이드 모드를 구성합니다.

5. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 애플리케이션 업그레이드 모드를 선택하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정 → 애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

3. **일반** 블록에서 **컴퓨터 재시작 없이 업데이트 설치** 확인란을 사용하여 애플리케이션 업그레이드 모드를 구성합니다.
4. 변경 사항을 저장합니다.

재시작 없이 애플리케이션을 업그레이드 절차가 완료되면, 컴퓨터에 최신 버전의 Kaspersky Endpoint Security가 설치됩니다. 이전 버전의 애플리케이션은 자동으로 삭제됩니다.

이전 업그레이드가 완료되기 전에는 애플리케이션 업그레이드를 시작할 수 없습니다.

Kaspersky Security Center 콘솔의 Kaspersky 애플리케이션 버전 리포트를 사용하여 Kaspersky Endpoint Security 업그레이드 상태를 확인할 수 있습니다.

애플리케이션의 SMU 업데이트

Kaspersky 업데이트 서비스(Seamless Update; SMU)를 사용하여 애플리케이션을 업데이트하면 다른 업데이트 방법과 달리 설치 프로그램을 실행할 필요가 없습니다. Kaspersky Endpoint Security는 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.

데이터베이스 및 애플리케이션 모듈 업데이트 작업을 사용하여 애플리케이션의 SMU 업데이트를 관리할 수 있습니다. 새 버전의 애플리케이션을 안티 바이러스 데이터베이스와 동일한 패키지에 포함하려면 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업 설정에서 *애플리케이션 모듈* 업데이트를 허용해야 합니다. 또한 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업 설정에서 재시작 없이 애플리케이션 업데이트를 허용할 수 있습니다.

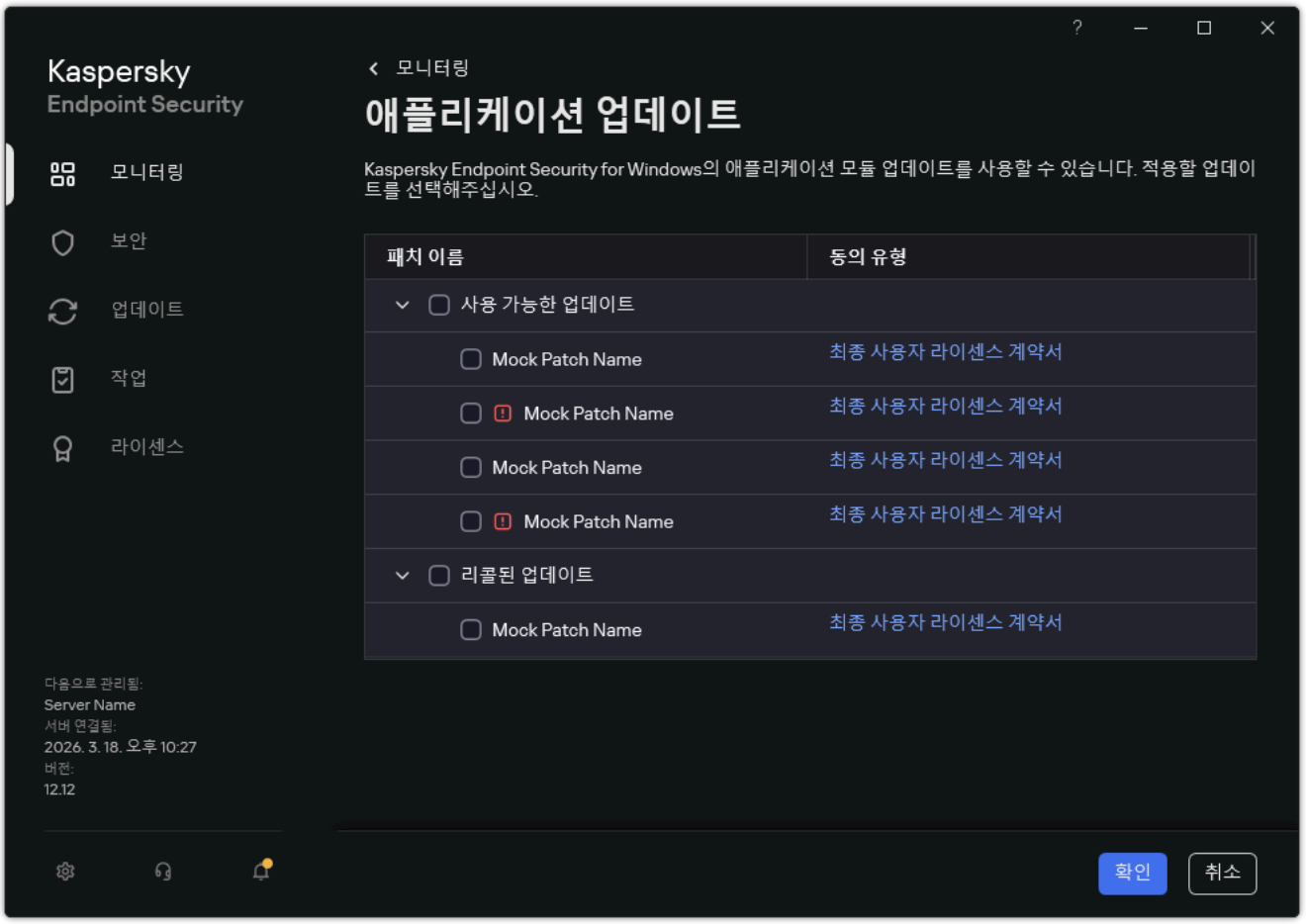
애플리케이션의 SMU 업데이트 단계

1. **애플리케이션의 새 버전이 출시된 후 Kaspersky에서 업데이트를 배포합니다.**
2. **사용자가 애플리케이션 업데이트를 승인합니다.**

   컴퓨터가 Kaspersky Security Center에 연결되어 있는 경우 Kaspersky Security Center의 **Kaspersky 데이터베이스 및 애플리케이션 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 인터페이스의 알림 섹션에서 업데이트할 수 있습니다: . 업데이트를 승인하려면 애플리케이션 버전을 선택하고 계약서의 약관에 동의합니다(아래 그림 참조).
3. **Kaspersky Endpoint Security는 구성된 스케줄에 따라 *데이터베이스 및 애플리케이션 모듈 업데이트*를 진행합니다.**

결과적으로 Kaspersky Endpoint Security는 "숨김" 모드로 애플리케이션을 업데이트합니다.



사용 가능한 애플리케이션 업데이트

애플리케이션 제거

Kaspersky Endpoint Security를 제거하면 컴퓨터 및 사용자 데이터가 보호되지 않는 상태로 위협에 노출됩니다.

Kaspersky Endpoint Security를 설치, 업데이트 또는 제거할 때 오류가 발생할 수 있습니다. 이러한 오류를 해결하는 방법에 대한 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오.

Kaspersky Security Center를 사용하여 애플리케이션 원격 제거

애플리케이션을 원격으로 제거 작업을 사용하면 애플리케이션을 원격으로 제거할 수 있습니다. 이 작업을 수행할 때 Kaspersky Endpoint Security는 애플리케이션 제거 유틸리티를 다운로드합니다. 애플리케이션 제거가 완료되면 이 유틸리티가 자동으로 제거됩니다.

관리 콘솔(MMC)을 통해 애플리케이션을 제거하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Security Center 중앙 관리 서버 → 고급 → 애플리케이션을 원격으로 제거를 선택합니다.

2단계. 제거할 애플리케이션 선택

Kaspersky Security Center에서 지원하는 애플리케이션 제거를 선택합니다.

3단계. 애플리케이션 제거를 위한 작업 설정

Kaspersky Endpoint Security for Windows (14.0)를 선택합니다.

4 단계. 유틸리티 설정 제거

다음과 같은 추가 애플리케이션 설정을 구성하십시오.

- **제거 유틸리티 강제 다운로드**. 유틸리티 제공 방법을 선택하십시오.
  - **네트워크 에이전트 이용**. 컴퓨터에 네트워크 에이전트를 설치하지 않은 경우 먼저 운영 체제의 도구를 사용하여 네트워크 에이전트가 설치됩니다. 그런 다음 네트워크 에이전트의 도구를 통해 Kaspersky Endpoint Security가 제거됩니다.
  - **중앙 관리 서버에서 대상 운영 체제의 관리 공유 폴더로 다운로드**. 중앙 관리 서버를 통해 운영 체제 리소스를 사용하여 클라이언트 컴퓨터로 유틸리티가 배달됩니다. 이 옵션은 클라이언트 컴퓨터에 네트워크 에이전트가 설치되어 있지 않아도 선택할 수 있지만, 이 경우 클라이언트 컴퓨터는 중앙 관리 서버와 같은 네트워크에 있어야 합니다.
  - **배포 지점에서 대상 운영 체제의 관리 공유 폴더로 다운로드**. 유틸리티가 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 도움말 을 참조하십시오.
- **다운로드하기 전에 운영 체제 유형 확인**. 필요시 이 확인란의 선택을 취소합니다. 이렇게 하면 컴퓨터의 운영 체제가 소프트웨어 요구 사항을 충족하지 않는 경우 제거 유틸리티가 다운로드되지 않습니다. 컴퓨터 운영 체제가 소프트웨어 요구 사항을 확실히 충족한다면 이 확인을 건너뛸 수 있습니다.

애플리케이션 제거 작업이 암호로 보호된 경우 다음을 수행하십시오.

1. **제거 암호 사용** 확인란을 선택합니다.
2. **편집** 버튼을 누릅니다.
3. KLAdmin 계정 암호를 입력합니다.

5단계. 운영 체제 재시작 설정 선택

애플리케이션을 제거한 후 다시 시작해야 합니다. 컴퓨터를 다시 시작하기 위해 수행할 작업을 선택하십시오.

6단계. 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.

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 Endpoint Security를 제거하는 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 Endpoint Security 14.0 제거* 등).

10 단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

애플리케이션이 숨김 모드로 제거됩니다.

웹 콘솔 및 Cloud Console을 통해 애플리케이션을 제거하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 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 **애플리케이션을 원격으로 제거**를 선택합니다.

3. **작업 이름** 필드에 *기술 지원 컴퓨터에서 Kaspersky Endpoint Security 제거*와 같은 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. 애플리케이션 제거 설정 구성

이 단계에서 다음과 같이 애플리케이션 제거 설정을 구성하십시오.

1. **관리 중인 애플리케이션 제거** 유형을 선택합니다.

2. **Kaspersky Endpoint Security for Windows**를 선택합니다.

3. **제거 유틸리티 강제 다운로드**. 유틸리티 제공 방법을 선택하십시오.

   - **네트워크 에이전트 이용**. 컴퓨터에 네트워크 에이전트를 설치하지 않은 경우 먼저 운영 체제의 도구를 사용하여 네트워크 에이전트가 설치됩니다. 그런 다음 네트워크 에이전트의 도구를 통해 Kaspersky Endpoint Security가 제거됩니다.

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

   - **배포 지점에서 대상 운영 체제의 관리 공유 폴더로 다운로드**. 유틸리티가 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.

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

5. **최대 제거 시도 횟수** 필드에서 애플리케이션 제거 시도 횟수의 제한을 설정합니다. Kaspersky Endpoint Security 제거 시 오류가 발생하면 해당 작업이 제거를 자동으로 다시 시작합니다.

6. 필요시 **다운로드하기 전에 운영 체제 유형 확인** 확인란 선택을 취소합니다. 이렇게 하면 컴퓨터의 운영 체제가 소프트웨어 요구 사항을 충족하지 않는 경우 제거 유틸리티가 다운로드되지 않습니다. 컴퓨터 운영 체제가 소프트웨어 요구 사항을 확실히 충족한다면 이 확인을 건너뛸 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 Endpoint Security를 제거하는 경우에는 계정을 선택할 필요가 없습니다.

5단계. 작업 생성 완료

마침 버튼을 눌러 마법사를 마칩니다. 작업 목록에 새 작업이 표시됩니다.

작업을 실행하려면 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다. 애플리케이션이 숨김 모드로 제거됩니다. 제거가 완료되면 Kaspersky Endpoint Security에서 컴퓨터 재시작하라는 메시지를 표시합니다.

애플리케이션 제거 작업이 암호로 보호되어 있는 경우에는 *애플리케이션을 원격으로 제거* 작업의 속성에 KLAdmin 계정 암호를 입력합니다. 암호를 입력하지 않으면 이 작업이 수행되지 않습니다.

애플리케이션을 원격으로 제거 작업에 KLAdmin 계정 암호를 입력하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. Kaspersky Security Center의 **애플리케이션을 원격으로 제거** 작업을 클릭합니다.
   작업 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **제거 암호 사용** 확인란을 선택합니다.
5. KLAdmin 계정 암호를 입력합니다.
6. 변경 사항을 저장합니다.

컴퓨터를 다시 시작하여 제거를 완료합니다. 네트워크 에이전트에 이를 위한 팝업 창이 표시됩니다.

Active Directory를 사용하여 애플리케이션 원격 제거

Microsoft Windows 그룹 정책을 사용하여 애플리케이션을 원격 제거할 수 있습니다. 애플리케이션을 제거하려면 그룹 정책 관리 콘솔(gpmc.msc)을 열고 그룹 정책 편집기를 사용하여 애플리케이션 제거 작업을 생성합니다(자세한 내용은 Microsoft 기술 지원 웹사이트를 방문하십시오).

애플리케이션 제거 동작에 암호가 걸려 있다면 다음을 수행해야 합니다.

1. 다음 내용으로 BAT 파일을 만듭니다.

```
msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
```

<GUID>는 애플리케이션의 고유 식별자입니다. 다음 명령을 사용하여 T기술 지원 기술 자료 웹사이트에서 애플리케이션의 GUID를 찾을 수 있습니다.

```
wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
```

예

```
msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

2. 그룹 정책 관리 콘솔(gpmc.msc)에서 컴퓨터에 대한 새 Microsoft Windows 정책을 생성합니다.

3. 새 정책을 사용하여 컴퓨터에서 생성된 BAT 파일을 실행합니다.

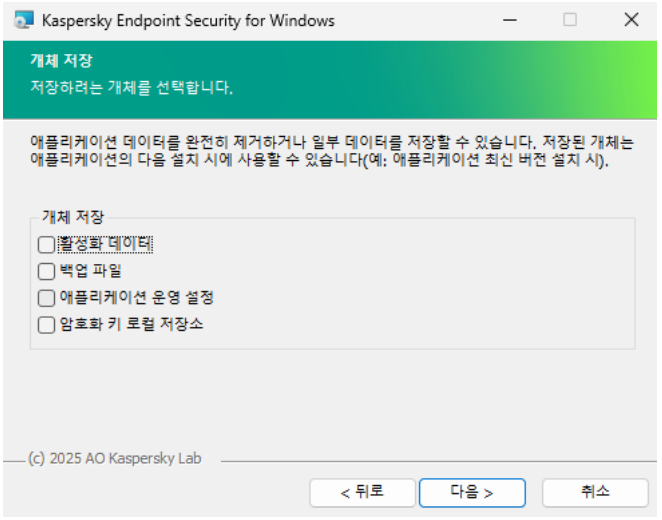
로컬에서 애플리케이션 제거

설치 마법사를 사용해 애플리케이션을 제거할 수도 있습니다. Kaspersky Endpoint Security가 Windows 운영 체제의 정상적인 방법, 즉 제어판을 통해 제거됩니다. 설치 마법사가 시작됩니다. 화면에 표시된 지침을 따릅니다.



애플리케이션 제거 작업 선택

다음 번 애플리케이션을 설치할 때(예: 새 버전의 애플리케이션으로 업그레이드 시) 애플리케이션에서 사용하는 데이터 중에서 나중에 사용하기 위해 저장할 데이터를 지정할 수 있습니다. 데이터를 지정하지 않으면 애플리케이션이 완전히 제거됩니다(아래 그림 참조).



제거 후 데이터 저장

다음과 같은 데이터를 저장할 수 있습니다.

- **활성화 데이터** - 애플리케이션을 다시 활성화할 필요가 없도록 해줍니다. Kaspersky Endpoint Security는 설치하기 전에 라이센스 기간이 만료되지 않았으면 라이센스 키를 자동으로 추가합니다.
- **백업 파일** - 이 파일은 애플리케이션에서 검사 후 백업 저장소로 이동된 파일입니다.

  애플리케이션을 제거한 후 저장된 백업 저장소 파일은 이러한 파일을 저장하는 데 사용된 애플리케이션 버전에서만 접근할 수 있습니다.

  애플리케이션을 제거한 후 백업 개체를 사용하려는 경우, 애플리케이션을 제거하기 전에 이러한 개체를 복원시켜야 합니다. 그러나, 이러한 경우 컴퓨터에 나쁜 영향을 미칠 수 있기 때문에 Kaspersky 전문가는 백업 저장소에서의 개체 복원을 권장하지 않습니다.

- **애플리케이션 운영 설정** - 애플리케이션 구성 중에 선택한 애플리케이션 설정 값입니다.
- **암호화 키 로컬 저장소** - 애플리케이션의 제거 전에 암호화된 파일 및 드라이브에 접근할 수 있는 데이터입니다. 암호화된 파일 및 드라이브에 접근할 수 있도록 하려면 Kaspersky Endpoint Security를 재설치할 때 데이터 암호화 기능을 선택했는지 확인하십시오. 이전에 암호화된 파일과 드라이브에 대한 접근을 위해 추가적인 조치가 필요하지 않습니다.

Kaspersky Endpoint Security는 데이터를 `C:\ProgramData\Kaspersky Lab\KES.14.0\QB`에 저장합니다.

명령줄을 사용해 로컬에서 애플리케이션을 삭제할 수도 있습니다.

애플리케이션 라이센스

이 섹션에는 Kaspersky Endpoint Security 라이센스와 관련된 전반적인 정보가 나와 있습니다.

최종 사용자 라이센스 계약서 정보

*최종 사용자 라이센스 계약서*는 애플리케이션 사용 약관을 규정하고 있는 사용자와 AO Kaspersky Lab 간의 라이센스 계약서입니다.

라이센스 계약서를 자세히 읽어본 후 애플리케이션을 사용하시기 바랍니다.

다음과 같은 방법으로 라이센스 계약서를 검토할 수 있습니다:

- 대화식 모드로 Kaspersky Endpoint Security를 설치할 때.
- license.txt 파일 읽기. 이 문서는 애플리케이션 배포 키트에 포함되어 있으며 애플리케이션 설치 폴더인 `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`에도 있습니다.

애플리케이션을 설치할 때 최종 사용자 라이센스 계약서를 수락한다는 것은 최종 사용자 라이센스 계약서의 조건을 수락한다는 의미입니다. 최종 사용자 라이센스 계약서에 동의하지 않으면 애플리케이션 설치가 중단됩니다.

라이센스 정보

*라이센스*는 최종 사용자 라이센스 계약서에 따라 정해진 기간 동안 애플리케이션을 사용할 수 있도록 부여된 권한을 말합니다.

라이센스를 통해 최종 사용자 라이센스 계약서에 따라 애플리케이션을 사용하고 기술 지원을 받을 수 있습니다. 사용 가능한 기능 목록과 애플리케이션 사용 기간은 애플리케이션 활성화에 사용된 라이센스 형태에 따라 달라집니다.

다음과 같은 라이센스 유형이 제공됩니다.

- *체험판* - 애플리케이션의 시범적인 사용을 위한 무료 라이센스입니다.

  체험판 라이센스는 보통 사용 기간이 짧습니다. 체험판 라이센스가 만료되면 모든 Kaspersky Endpoint Security 기능이 중지됩니다. 애플리케이션을 계속 사용하려면 상업용 라이센스를 구매해야 합니다.

  체험판 라이센스로 애플리케이션을 한 번만 활성화할 수 있습니다. 상업용 라이센스로 활성화한 애플리케이션은 체험판 라이센스로 활성화할 수 없습니다.

- *상업용* - Kaspersky Endpoint Security를 구매하면 제공되는 유료 라이센스입니다.

  상업용 라이센스로 사용 가능한 애플리케이션 기능은 제품 유형에 따라 다릅니다. 이용 가능한 제품은 라이센스 인증서에 표시되어 있습니다. 구매 가능한 제품에 관한 정보는 Kaspersky 웹사이트에서 확인하실 수 있습니다.

  상업용 라이센스가 만료되면 애플리케이션의 주요 기능을 이용할 수 없습니다. 애플리케이션을 계속 사용하려면 상업용 라이센스를 갱신해야 합니다. 라이센스를 갱신할 예정이 아닌 경우, 컴퓨터에서 애플리케이션을 제거해야 합니다.

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.

서브스크립션 정보

*Kaspersky Endpoint Security용 서브스크립션*은 특정 파라미터(예, 서브스크립션 만료일, 보호되는 장치 수)가 있는 애플리케이션에 대한 구매 주문입니다. ISP와 같은 서비스 제공업체로부터 Kaspersky Endpoint Security 서브스크립션을 주문할 수 있습니다. 서브스크립션은 수동 또는 자동으로 갱신할 수도 있고 취소할 수도 있습니다. 서비스 제공업체의 웹사이트에서 서브스크립션을 관리할 수 있습니다.

서브스크립션은 제한(1년 등) 또는 무제한(만료일 없음) 모두 가능합니다. Kaspersky Endpoint Security를 제한된 서브스크립션 기간이 만료한 후에도 계속 유지하려면 서브스크립션을 갱신해야 합니다. 무제한 서브스크립션은 공급업체의 서비스를 미리 적시에 지불한 경우 자동으로 갱신됩니다.

제한된 서브스크립션이 만료되면 서브스크립션 갱신 유예 기간이 주어질 수 있으며 이 기간 동안에는 애플리케이션을 계속해서 사용할 수 있습니다. 그러한 유예 기간의 제공 여부와 기간은 서비스 제공업체가 결정합니다.

서브스크립션으로 Kaspersky Endpoint Security를 사용하려면 서비스 공급업체로부터 받은 활성화 코드를 적용해야 합니다. 활성화 코드가 적용된 후에 활성 키가 추가됩니다. 활성 키는 서브스크립션 조건에서 애플리케이션을 사용하기 위한 라이센스를 결정합니다. 서브스크립션의 애플리케이션은 키 파일을 사용해서 활성화할 수 없습니다. 서비스 공급업체는 활성화 코드만 제공할 수 있습니다. 서브스크립션에서는 예비 키를 추가할 수 없습니다.

서브스크립션으로 구입한 활성화 코드를 사용하여 이전 버전의 Kaspersky Endpoint Security를 활성화하지 못할 수도 있습니다.

라이센스 키 정보

*라이센스 키*는 최종 사용자 라이센스 계약서 조건에 따라 애플리케이션을 활성화 및 사용할 수 있는 일련의 비트입니다.

라이센스 인증서는 서브스크립션 하에 추가된 라이센스 키에 대해서는 제공되지 않습니다.

키 파일을 적용하거나 활성화 코드를 입력하여 애플리케이션에 라이센스 키를 추가할 수 있습니다.

최종 사용자 라이센스 계약서의 조건을 위반했다면, 해당 키는 Kaspersky에 의해 차단될 수 있습니다. 라이센스 키가 차단되면 다른 키를 추가해야 계속해서 애플리케이션을 사용할 수 있습니다.

라이센스 키에는 활성 키와 예약 키의 두 가지 유형이 있습니다.

*활성 키*는 현재 애플리케이션에서 사용 중인 라이센스입니다. 체험판 또는 상업용 라이센스용 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. 활성 키가 만료되면 예약 키가 자동으로 활성화됩니다. 예약 키는 활성 키가 이미 추가된 경우에만 추가할 수 있습니다.

체험판 라이센스용 키는 활성 키로만 추가할 수 있습니다. 예약 키로는 추가할 수 없습니다. 체험판 라이센스 키는 상업용 라이센스에 대한 활성 키를 대체할 수 없습니다.

금지된 키 목록에 키가 추가되면 애플리케이션 활성화에 사용된 라이센스로 정의된 애플리케이션 기능을 8일 더 사용할 수 있습니다. 애플리케이션이 사용자에게 키가 금지된 키 목록에 추가되었음을 알립니다. 8일이 지나면 애플리케이션 기능은 라이센스 만료 후 사용 가능한 기능 수준으로 제한됩니다. 보호 및 제어 구성 요소를 사용하고 라이센스가 만료되기 전에 설치된 애플리케이션 데이터베이스를 사용하여 검사를 실행할 수 있습니다. 또한, 애플리케이션은 라이센스 만료 이전에 수정했거나 암호화한 파일은 계속 암호화하지만 새 파일은 암호화하지 않습니다. Kaspersky Security Network는 이용할 수 없습니다.

활성화 코드 정보

*활성화 코드*는 20개의 영숫자로 구성된 일련의 고유한 코드입니다. Kaspersky Endpoint Security를 활성화하는 라이센스 키를 추가하려면 활성화 코드를 입력합니다. Kaspersky Endpoint Security 구매 후 지정한 이메일 주소로 활성화 코드를 받습니다.

활성화 코드를 사용하여 애플리케이션을 활성화할 때 Kaspersky 활성화 서버에 연결하기 위해 인터넷에 연결되어 있어야 합니다.

애플리케이션이 활성화 코드를 사용하여 활성화 될 때, 활성 키가 추가됩니다. 예비 키는 활성화 코드로만 추가할 수 있으며 키 파일로는 추가할 수 없습니다.

만일 애플리케이션 활성화 후 활성화 코드를 분실했다면 해당 활성화 코드를 복원할 수 있습니다. 예를 들어 Kaspersky CompanyAccount를 등록하려면 활성화 코드가 필요할 수 있습니다. 애플리케이션 활성화 후 활성화 코드를 잃어버렸다면 라이센스를 구매한 Kaspersky 협력사에 문의하십시오.

키 파일 정보

*키 파일*은 Kaspersky에서 받는 .key 확장자를 가진 파일입니다. 키 파일의 목적은 애플리케이션을 활성화하는 키를 추가하기 위한 것입니다.

Kaspersky Endpoint Security를 구매하거나 Kaspersky Endpoint Security 체험판을 주문할 때 제공한 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.
- 다른 중앙 관리 서버에서 키 파일 가져오기.

애플리케이션이 키 파일을 사용하여 활성화 될 때, 활성 키가 추가됩니다. 예비 키는 키 파일로만 추가할 수 있으며 활성화 코드로는 추가할 수 없습니다.

워크스테이션용 라이센스 유형에 따른 애플리케이션 기능 비교

워크스테이션에서 사용 가능한 Kaspersky Endpoint Security 기능 세트는 라이센스 유형에 따라 다릅니다(아래 표 참조).

서버용 애플리케이션 기능 비교도 참조하십시오

Kaspersky Next 라이센스 유형에 따른 애플리케이션 기능 비교는 Kaspersky Next 도움말을 참조하십시오.

Kaspersky Endpoint Security 기능 비교

기능	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
지능형 위협 보호								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
행동 탐지	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓

기능	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
익스플로잇 방지	✓	✓	✓	✓	✓	✓	✓	✓
호스트 침입 방지	✓	✓	✓	✓	✓	✓	✓	✓
복원 엔진	✓	✓	✓	✓	✓	✓	✓	✓
필수 위협 보호								
파일 위협 보호	✓	✓	✓	✓	✓	✓	✓	✓
웹 위협 보호	✓	✓	✓	✓	✓	✓	✓	✓
메일 위협 보호	✓	✓	✓	✓	✓	✓	✓	✓
방화벽	✓	✓	✓	✓	✓	✓	✓	✓
네트워크 위협 보호	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB 공격 방지	✓	✓	✓	✓	✓	✓	✓	✓
AMSI 보호	✓	✓	✓	✓	✓	✓	✓	✓
보안 제어								
로그 검사	–	–	–	–	–	–	–	–
애플리케이션 제어	✓	✓	✓	✓	✓	✓	✓	✓
장치 제어	✓	✓	✓	✓	✓	✓	✓	✓
웹 제어	✓	✓	✓	✓	✓	✓	✓	✓
적응형 이상 행위 제어	–	✓	✓	✓	✓	✓	–	✓
시스템 무결성 모니터링	–	–	–	–	–	–	–	–
데이터 암호화								
Kaspersky 디스크 암호화	–	✓	✓	✓	✓	✓	–	✓
BitLocker 드라이브 암호화	–	✓	✓	✓	✓	✓	–	✓
파일 레벨 암호화	–	✓	✓	✓	✓	✓	–	✓
이동식 드라이브 암호화	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(Kaspersky Sandbox 라이센스는 별도로 구매해야 합니다)*	✓	✓	✓	✓	✓	✓	✓	✓

기능	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
KUMA과 통합 *(KUMA 통합용 라이센스는 별도로 구매해야 함)*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent 모드 *(애플리케이션을 활성화하려면 Light Agent가 연결된 SVM에 라이센스 키를 추가해야 합니다)*	–	–	–	–	–	–	✓	✓

서버용 라이센스 유형에 따른 애플리케이션 기능 비교

라이센스 유형에 따라 서버에서 사용 가능한 Kaspersky Endpoint Security 기능 세트(아래 표 참조).

워크스테이션용 애플리케이션 기능 비교도 참조하십시오

Kaspersky Next 라이센스 유형에 따른 애플리케이션 기능 비교는 Kaspersky Next 도움말을 참조하십시오.

Kaspersky Endpoint Security 기능 비교

기능	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
지능형 위협 보호								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
행동 탐지	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
익스플로잇 방지	✓	✓	✓	✓	✓	✓	✓	✓
호스트 침입 방지	–	–	–	–	–	–	–	–
복원 엔진	✓	✓	✓	✓	✓	✓	✓	✓
필수 위협 보호								
파일 위협 보호	✓	✓	✓	✓	✓	✓	✓	✓
웹 위협 보호	–	✓	✓	✓	✓	✓	✓	✓
메일 위협 보호	–	✓	✓	✓	✓	✓	✓	✓
방화벽	✓	✓	✓	✓	✓	✓	✓	✓
네트워크 위협 보호	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB 공격 방지	✓	✓	✓	✓	✓	✓	✓	✓

기능	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
AMSI 보호	✓	✓	✓	✓	✓	✓	✓	✓
보안 제어								
로그 검사	–	–	–	–	–	–	–	✓
애플리케이션 제어	–	✓	✓	✓	✓	✓	–	✓
장치 제어	–	✓	✓	✓	✓	✓	✓	✓
웹 제어	–	✓	✓	✓	✓	✓	✓	✓
적응형 이상 행위 제어	–	–	–	–	–	–	–	–
시스템 무결성 모니터링	–	–	–	–	–	–	–	✓
데이터 암호화								
Kaspersky 디스크 암호화	–	–	–	–	–	–	–	–
BitLocker 드라이브 암호화	–	✓	✓	✓	✓	✓	–	✓
파일 레벨 암호화	–	–	–	–	–	–	–	–
이동식 드라이브 암호화	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(Kaspersky Sandbox 라이센스는 별도로 구매해야 합니다)*	✓	✓	✓	✓	✓	✓	✓	✓
KUMA과 통합 *(KUMA 통합용 라이센스는 별도로 구매해야 함)*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent 모드 *(애플리케이션을 활성화하려면 Light Agent가 연결된 SVM에 라이센스 키를 추가해야 합니다)*	–	–	–	–	–	–	✓	✓

애플리케이션 활성화

*활성화*란 라이센스가 만료될 때까지 정식 애플리케이션 버전을 사용할 수 있도록 라이센스를 활성화하는 절차를 말합니다. 애플리케이션 활성화는 라이센스 키 추가를 포함합니다.

다음과 같은 방법으로 애플리케이션을 활성화할 수 있습니다:

- 활성화 마법사를 사용하여 애플리케이션 인터페이스에서 로컬로 작업합니다. 이 방법으로 활성 키와 예약 키 모두를 추가할 수 있습니다.
- Kaspersky Security Center 소프트웨어 제품군을 사용하여 원격으로 작업합니다.
  - *키 추가* 작업 사용.

    이 방법을 사용하면 특정 컴퓨터 또는 관리 그룹의 일부 컴퓨터에 키를 추가할 수 있습니다. 이 방법으로 활성 키와 예약 키 모두를 추가할 수 있습니다.
  - Kaspersky Security Center 중앙 관리 서버에 저장된 키를 컴퓨터에 배포.

    이 방법을 사용하면 Kaspersky Security Center에 이미 연결되어 있는 컴퓨터와 새 컴퓨터에 키를 자동으로 추가할 수 있습니다. 이 방법을 사용하려면 Kaspersky Security Center 중앙 관리 서버에 키를 먼저 추가해야 합니다. Kaspersky Security Center 중앙 관리 서버에 키를 추가하는 방법에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하시기 바랍니다.

    > 서브스크립션으로 구매한 활성화 코드는 우선 배포됩니다.

  - Kaspersky Endpoint Security 설치 패키지에 키 추가.

    이 방법을 사용하면 Kaspersky Endpoint Security 배포 중에 설치 패키지 속성에서 키를 추가할 수 있습니다. 애플리케이션이 설치 후 자동으로 활성화됩니다.
- 명령줄 사용.

> Kaspersky의 인증 서버 부하로 인해 활성화 코드로 애플리케이션이 활성화 될 때까지 시간이 좀 걸릴 수 있습니다(원격 또는 비대화식 설치). 바로 애플리케이션을 활성화해야 할 경우에는 진행 중인 활성화 프로세스를 중단하고 활성화 마법사를 사용해 활성화를 시작할 수 있습니다.

> Kaspersky Endpoint Security가 가상 환경 보호를 위한 Light Agent 모드에서 사용되는 경우에는 애플리케이션을 별도로 활성화할 필요가 없습니다.

애플리케이션 활성화

관리 콘솔(MMC)에서 애플리케이션을 활성화하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **키 추가**를 선택합니다.

2 단계. 키 추가

활성화 코드를 입력하거나 키 파일을 선택합니다.

Kaspersky Security Center 저장소에 키를 추가하는 방법에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

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 이름(예: *Kaspersky Endpoint Security for Windows 활성화*)을 입력하십시오.

6단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다. 결과적으로 사용자의 컴퓨터에서 Kaspersky Endpoint Security가 숨김 모드로 활성화됩니다.

웹 콘솔 및 Cloud Console에서 애플리케이션을 활성화하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 일반 작업 설정 구성

일반 작업 설정을 구성하려면 다음을 수행하십시오.

1. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
2. **작업 유형** 드롭다운 목록에서 **키 추가**를 선택합니다.
3. **작업 이름** 필드에 *Kaspersky Endpoint Security for Windows 활성화*와 같은 간단한 설명을 입력합니다.
4. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다. 다음 단계로 넘어갑니다.

2단계. 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.

3 단계. 라이센스 선택

애플리케이션을 활성화하는 데 사용할 라이센스를 선택합니다. 다음 단계로 넘어갑니다.

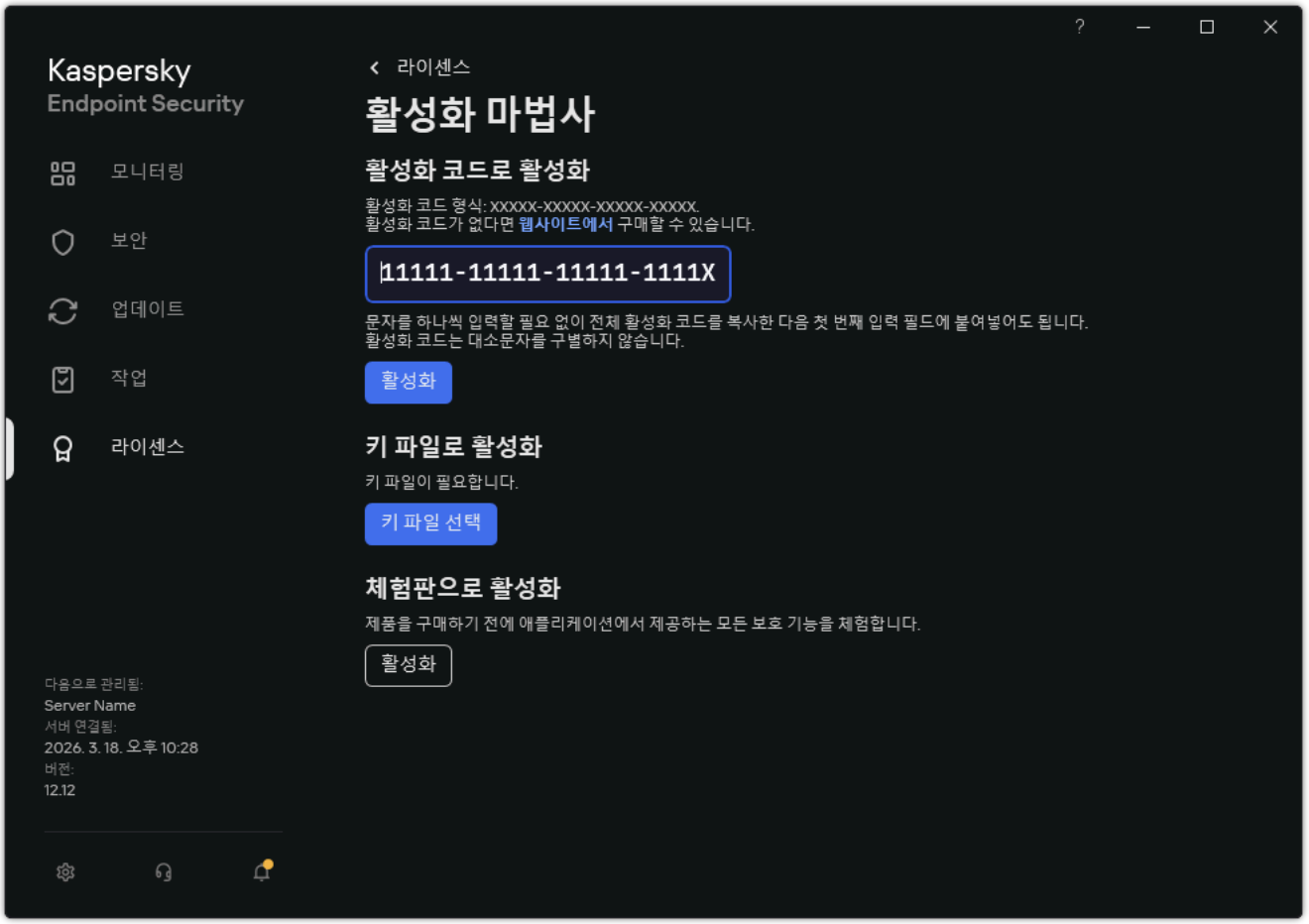
키를 웹 콘솔에 추가할 수 있습니다(**동작** → **라이센스**).

4단계. 작업 생성 완료

마침 버튼을 눌러 마법사를 마칩니다. 작업 목록에 새 작업이 표시됩니다. 작업을 실행하려면 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다. 결과적으로 사용자의 컴퓨터에서 Kaspersky Endpoint Security가 숨김 모드로 활성화됩니다.

애플리케이션 인터페이스에서 애플리케이션을 활성화하는 방법

1. 메인 애플리케이션 창에서 **라이센스** 섹션으로 이동합니다.
2. **새 라이센스로 애플리케이션 활성화**를 클릭합니다.
   애플리케이션 활성화 마법사가 시작됩니다. 활성화 마법사의 안내를 따릅니다.



애플리케이션 활성화

키 추가 작업 속성에서 컴퓨터에 예약 키를 추가할 수 있습니다. *예약 키*는 활성 키가 만료되거나 삭제되면 활성 키로 설정됩니다. 예약 키를 사용할 수 있으면 라이센스 만료 시 애플리케이션 기능 제한을 방지할 수 있습니다.

관리 콘솔(MMC)을 통해 컴퓨터에 라이센스 키를 자동으로 추가하는 방법

1. 관리 콘솔에서 **Kaspersky 라이센스** 폴더로 이동합니다.
   라이센스 키 목록이 열립니다.

2. 라이센스 키 속성을 엽니다.

3. **일반** 섹션에서 **관리 중인 기기에 자동으로 라이센스 키 배포** 확인란을 선택합니다.

4. 변경 사항을 저장합니다.

이렇게 하면 해당 컴퓨터에 키가 자동으로 배포됩니다. 키를 활성 키나 예약 키로 자동 배포할 때는 키의 속성에 설정된 컴퓨터 수에 대한 라이센스 제한을 고려합니다. 라이센스 제한에 도달하면 컴퓨터로의 이 키 배포는 자동으로 중단됩니다. 키가 추가된 컴퓨터의 수와 기타 데이터는 **기기** 섹션의 키 속성에서 확인할 수 있습니다.

웹 콘솔 및 Cloud Console을 통해 컴퓨터에 라이센스 키를 자동으로 추가하는 방법

1. 웹 콘솔의 기본 창에서 **동작 → 라이센스 → 라이센스**를 선택합니다.
   라이센스 키 목록이 열립니다.

2. 라이센스 키 속성을 엽니다.

3. **일반** 탭에서 **관리 중인 기기에 자동으로 라이센스 키 배포** 토글 스위치를 활성화합니다.

4. 변경 사항을 저장합니다.

이렇게 하면 해당 컴퓨터에 키가 자동으로 배포됩니다. 키를 활성 키나 예약 키로 자동 배포할 때는 키의 속성에 설정된 컴퓨터 수에 대한 라이센스 제한을 고려합니다. 라이센스 제한에 도달하면 컴퓨터로의 이 키 배포는 자동으로 중단됩니다. 키가 추가된 컴퓨터의 수와 기타 데이터는 **기기** 탭의 키 속성에서 확인할 수 있습니다.

*활성화 코드*를 사용하여 애플리케이션을 활성화하는 경우, Kaspersky 활성화 서버에 연결하려면 인터넷에 접속해야 합니다. *키 파일*을 사용하여 애플리케이션을 활성화하는 경우, 인터넷 접속이 필요하지 않습니다. 컴퓨터가 인터넷에 접속할 수 없는 격리된 네트워크 부분에 있는 경우 코드로 애플리케이션을 활성화하려면 Kaspersky Security Center 중앙 관리 서버를 프록시 서버로 사용하도록 허용해야 합니다. 즉, 애플리케이션은 인터넷에 연결된 중앙 관리 서버를 통해 활성화 서버에 접근할 수 있습니다.

관리 콘솔(MMC)에서 애플리케이션을 활성화하기 위해 중앙 관리 서버를 프록시 서버로 사용하도록 허용하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **일반 설정 → 애플리케이션 설정**을 차례로 선택합니다.

4. **활성화 시 프록시 서버로 Kaspersky Security Center 사용** 확인란을 선택합니다.

5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 애플리케이션을 활성화하기 위해 중앙 관리 서버를 프록시 서버로 사용하도록 허용하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **KSC 통합**으로 갑니다.

5. **활성화 시 프록시 서버로 Kaspersky Security Center 사용** 확인란을 선택합니다.

6. 변경 사항을 저장합니다.

*활성화 코드*로 애플리케이션을 활성화할 수 없는 경우, Kaspersky solution을 사용하여 *키 파일*을 가져와 다른 방법으로 애플리케이션을 다시 활성화해 볼 수 있습니다.

라이센스 사용량 모니터링

다음과 같은 방식으로 라이센스 사용을 감시할 수 있습니다:

- 조직 인프라에 대한 *라이센스 키 사용 리포트*를 봅니다(**모니터링** → **리포트**).
- **관리 중인 기기** → **기기** 탭에서 컴퓨터 상태를 확인합니다. 애플리케이션이 활성화되어 있지 않으면 컴퓨터에 ⚠ *애플리케이션이 활성화되지 않았습니다* 상태가 표시됩니다.
- 컴퓨터 속성에서 라이센스 정보를 봅니다.
- 키 속성을 봅니다(**동작** → **라이센스**).

Kaspersky Security Center Cloud Console의 일부로 애플리케이션을 활성화하는 세부 사항

Kaspersky Security Center Cloud 콘솔에 대한 체험판 버전이 제공됩니다. *체험판 버전*은 사용자가 애플리케이션 기능과 친숙해지도록 설계된 Kaspersky Security Center Cloud 콘솔의 특수 버전입니다. 이 버전에서는 30일 동안 작업 공간에서 작업을 수행할 수 있습니다. 관리되는 모든 애플리케이션은 Kaspersky Endpoint Security를 포함한 Kaspersky Security Center Cloud 콘솔의 체험판 라이센스에 따라 자동으로 실행됩니다. 그러나 Kaspersky Security Center Cloud Console의 체험판 라이센스가 만료되면 자체 체험판 라이센스를 사용하여 Kaspersky Endpoint Security를 활성화할 수 없습니다. Kaspersky Security Center 라이센스에 대한 상세 정보는 Kaspersky Security Center Cloud 콘솔 도움말을 참조하십시오.

> Kaspersky Security Center Cloud 콘솔의 체험판 버전은 이후 상업용 버전으로 전환할 수 없습니다. 모든 체험판 작업 공간은 30일 기간이 만료된 후 모든 내용과 함께 자동으로 삭제됩니다.

라이센스 키 제거하기

라이센스 키를 제거하려면, 컴퓨터에서 특수 작업을 실행해야 합니다. 예를 들어 라이센스 키를 제거하여 라이센스 단위를 재배치할 수 있습니다. 또한 라이센스가 만료되면 Kaspersky Endpoint Security가 알려줍니다. EDR Optimum 애드온과 같은 애플리케이션을 체험해 보기 위해 단기 라이센스 키를 추가한 경우 이 라이센스 키를 제거하여 알림을 받지 않고 컴퓨터 상태를 수정할 수 있습니다.

키 제거 작업을 통해 컴퓨터에서 모든 라이센스 키를 제거할 수 있습니다. 활성 라이센스 키와 예약된 라이센스 키를 제거할 수 있습니다. Kaspersky Endpoint Security 활성화 라이센스 키 외에도 EDR Optimum 애드온과 같은 Kaspersky Detection and Response 솔루션의 개별 라이센스 키를 제거할 수 있습니다.

관리 콘솔(MMC)에서 라이센스 키를 제거하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **키 제거**를 선택합니다.

2 단계. 라이센스 선택

제거하고자 하는 라이센스 키를 선택합니다. Kaspersky Security Center 키 스토어에서 라이센스 키를 선택하거나 키 파일을 선택할 수 있습니다.

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 이름(예: *베타용 키 제거*)을 입력합니다.

6단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔에서 라이센스 키를 제거하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 일반 작업 설정 구성

일반 작업 설정을 구성하려면 다음을 수행하십시오.

1. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
2. **작업 유형** 드롭다운 목록에서 **키 제거**를 선택합니다.
3. **작업 이름** 필드에 *베타용 키 제거* 등의 간단한 설명을 입력합니다.
4. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다. 다음 단계로 넘어갑니다.

2단계. 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.

3 단계. 라이센스 선택

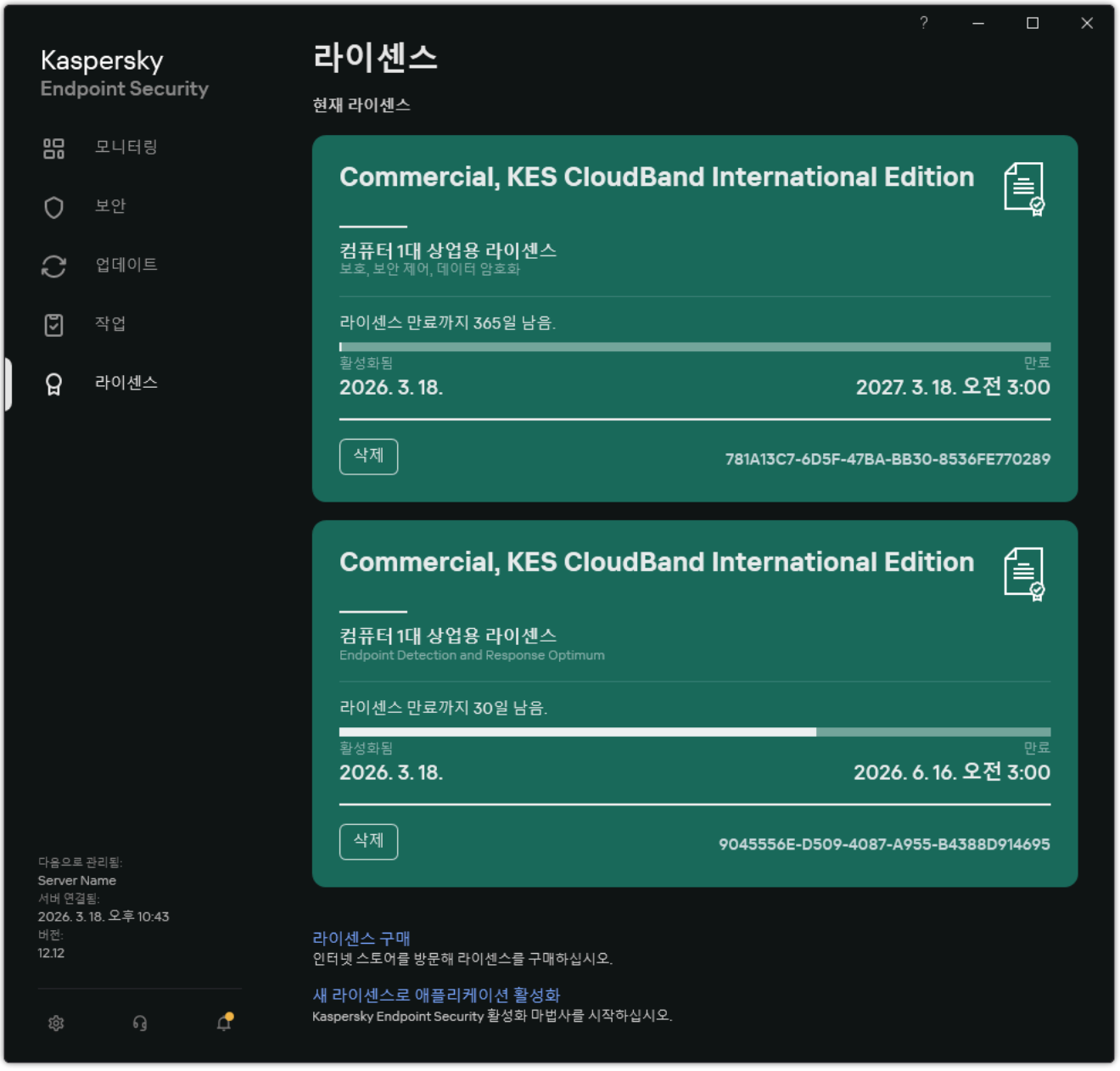
제거하고자 하는 라이센스 키를 선택합니다. Kaspersky Security Center 키 스토어에서 라이센스 키를 선택하거나 키 파일을 선택할 수 있습니다. 다음 단계로 넘어갑니다.

4단계. 작업 생성 완료

마침 버튼을 눌러 마법사를 마칩니다. 작업 목록에 새 작업이 표시됩니다. 작업을 실행하려면 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다.

애플리케이션 인터페이스에서 라이센스 키를 제거하는 방법

1. 메인 애플리케이션 창에서 **라이센스** 섹션으로 이동합니다.
2. 삭제하려는 키를 선택하고 **삭제**를 클릭합니다.



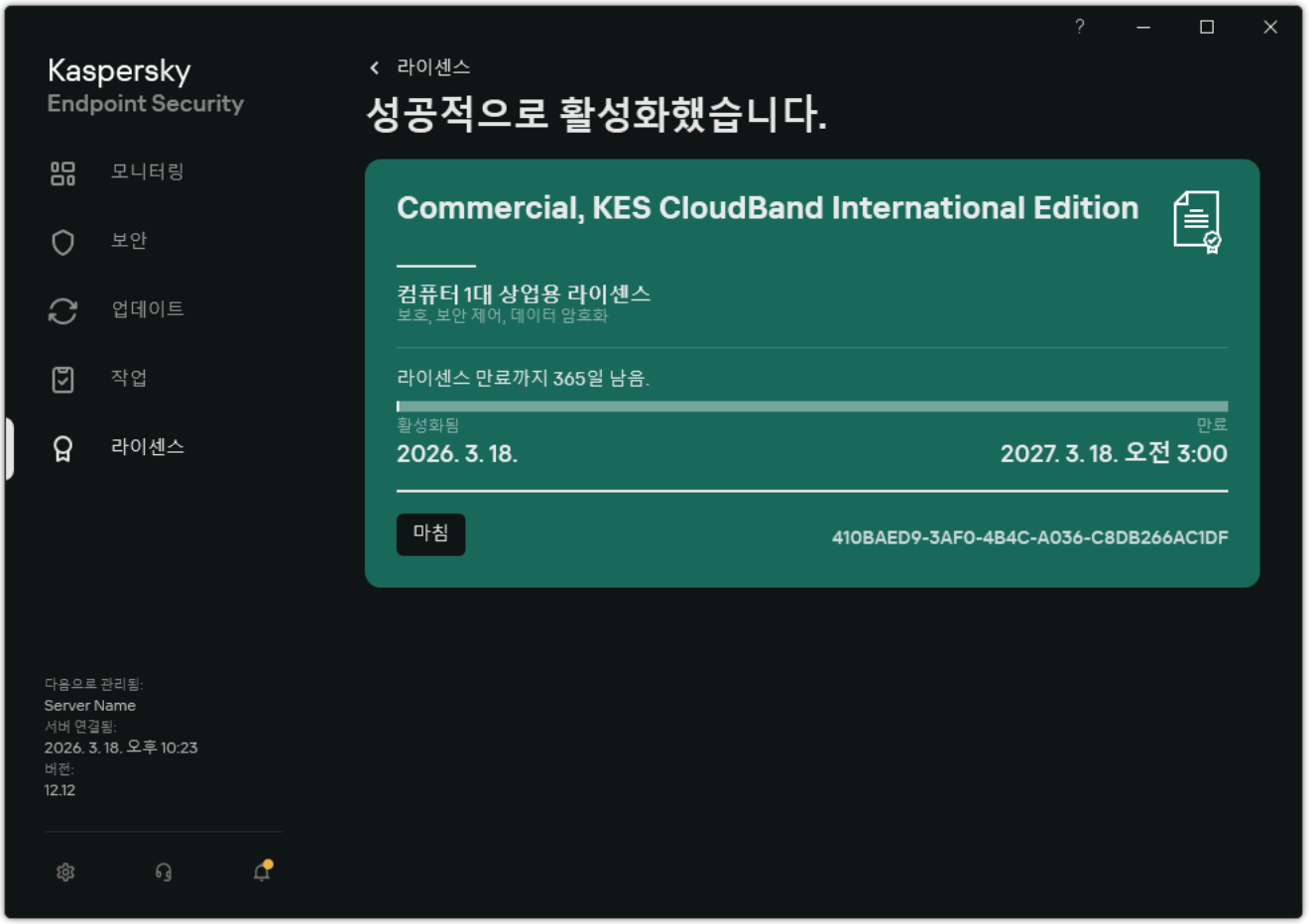
라이센스 창

명령줄에서 라이센스 키를 제거할 수도 있습니다.

라이센스 정보 보기

라이센스 관련 정보를 보려면 다음과 같이 하십시오:

메인 애플리케이션 창에서 **라이센스** 섹션으로 이동합니다(아래 그림 참조).



라이센스 창

섹션에 다음 세부 정보가 표시됩니다:

- *키 상태.* 컴퓨터에는 여러 키를 저장할 수 있습니다. 라이센스 키에는 활성 키와 예약 키의 두 가지 유형이 있습니다. 애플리케이션은 하나 이상의 활성 키를 보유할 수 없습니다. 예비 키는 활성 키가 만료되거나 **삭제** 버튼을 클릭하여 활성 키를 삭제한 후에만 활성화됩니다.
- *애플리케이션 이름.* 구매한 Kaspersky 애플리케이션의 전체 이름입니다.
- *라이센스 유형.* 사용 가능한 라이센스 유형은 체험판 및 상업용입니다.
- *기능.* 라이센스에 따라 사용 가능한 애플리케이션 기능입니다. 기능에는 보호, 보안 제어, 데이터 암호화 및 기타 기능이 포함될 수 있습니다. 사용 가능한 기능 목록은 라이센스 인증서에도 제공됩니다.

- *추가 라이센스 정보*. 라이센스 기간의 시작 날짜와 종료 날짜(활성 키만 해당), 남은 라이센스 기간

  라이센스 만료 시간은 운영 체제에 구성된 시간대에 따라 표시됩니다.

- *키*. 키는 활성화 코드 또는 키 파일에서 생성되는 고유한 영숫자 시퀀스입니다.

라이센스 창에서 다음 중 하나를 수행할 수도 있습니다:

- **라이센스 구매/라이센스 갱신**. 라이센스를 구매하거나 갱신할 수 있는 Kaspersky 온라인 스토어 웹사이트를 엽니다. 이렇게 하려면 회사 정보를 입력하고 주문을 결제하십시오.

- **새 라이센스로 애플리케이션 활성화**. 애플리케이션 활성화 마법사가 시작됩니다. 이 마법사에서 활성화 코드 또는 키 파일을 사용하여 키를 추가할 수 있습니다. 애플리케이션 활성화 마법사에서는 활성 키와 예약 키(하나만 추가할 수 있음)를 추가할 수 있습니다.

라이센스 구매

애플리케이션을 설치한 후 라이센스를 구매할 수 있습니다. 라이센스를 구매 시 애플리케이션을 활성화하는 활성화 코드 또는 키 파일을 받을 수 있습니다.

라이센스를 구매하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 **라이센스** 섹션으로 이동합니다.
2. 다음 중 하나를 수행합니다:
   - 추가된 키가 없거나 체험판이 설치되어 있다면, **라이센스 구매** 버튼을 클릭합니다.
   - 상업용 라이센스를 설치한 경우 **라이센스 갱신** 버튼을 누릅니다.

   라이센스를 구매할 수 있는 Kaspersky 온라인 스토어의 웹사이트 창이 열립니다.

서브스크립션 갱신

서브스크립션으로 애플리케이션을 사용할 때 Kaspersky Endpoint Security가 서브스크립션이 만료될 때까지 특정 간격으로 활성화 서버에 자동으로 접속합니다.

무제한 서브스크립션으로 애플리케이션을 사용하는 경우 Kaspersky Endpoint Security가 갱신된 라이센스 키에 대한 활성화 서버를 백그라운드 모드에서 자동으로 확인합니다. 활성화 서버에서 라이센스 키를 사용할 수 있다면 애플리케이션이 이전 키를 대체하는 방식으로 키를 추가합니다. 이러한 방식으로 Kaspersky Endpoint Security에 대한 무제한 서브스크립션이 사용자의 개입 없이 갱신됩니다.

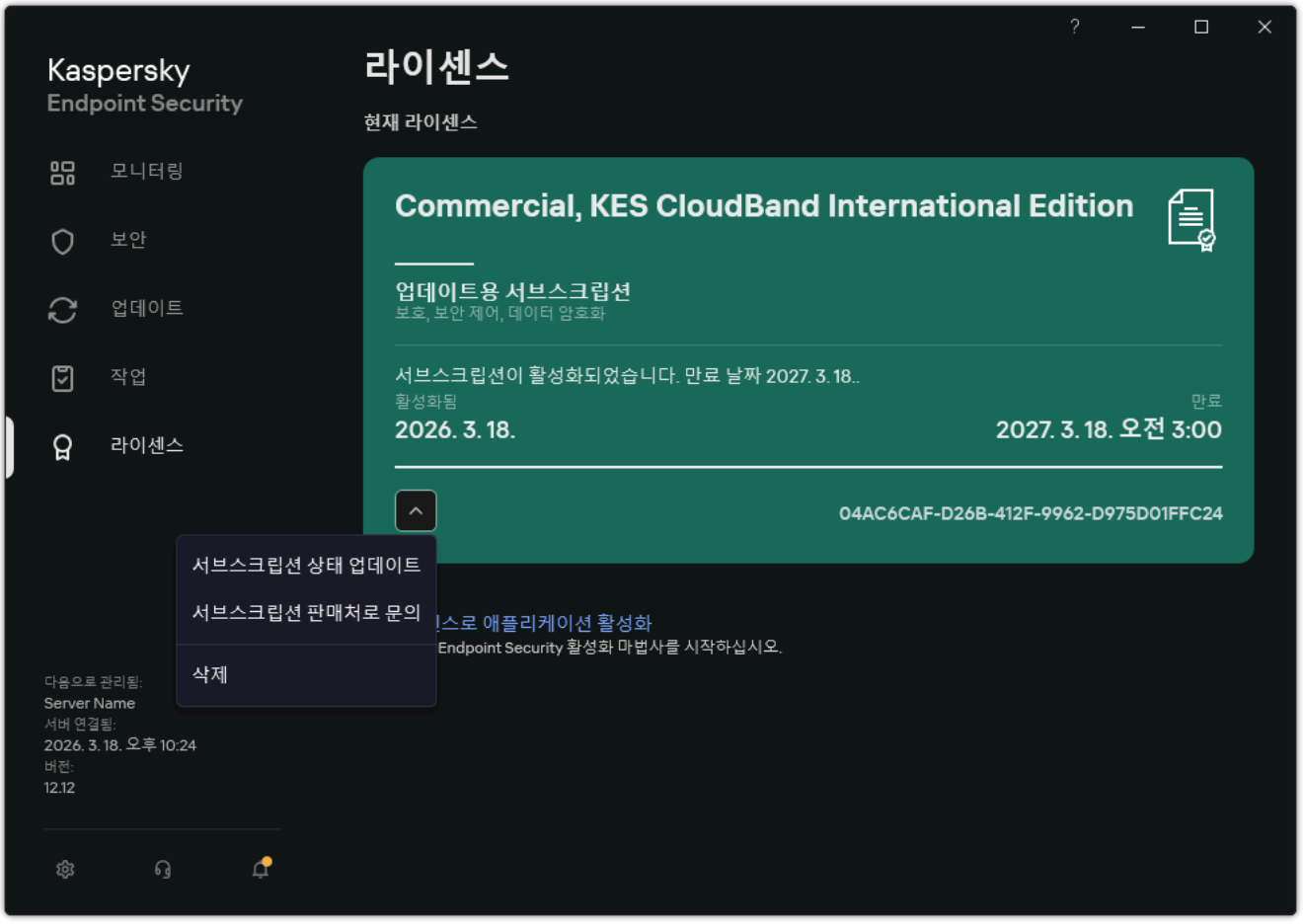
제한된 서브스크립션으로 애플리케이션을 사용하는 경우, 서브스크립션의 만료 날짜(또는 서브스크립션 갱신 유예 기간의 만료 날짜)가 되면 Kaspersky Endpoint Security에서 기간 만료를 알리고 서브스크립션의 자동 갱신 시도를 중단합니다. 이 경우 Kaspersky Endpoint Security는 애플리케이션의 상업용 라이센스가 만료될 때와 동일한 방식으로 동작합니다. 즉, 애플리케이션이 업데이트없이 실행되며 Kaspersky Security Network 서비스를 사용할 수 없게 됩니다.

서비스 제공업체의 웹사이트에서 서브스크립션을 갱신할 수 있습니다.

애플리케이션 인터페이스에서 해당 서비스 제공업체의 웹사이트를 방문하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 **라이센스** 섹션으로 이동합니다.
2. **서브스크립션 판매처로 문의**를 클릭합니다.

서브스크립션 상태를 직접 업데이트할 수 있습니다. 이것은 유예 기간이 지난 후에 애플리케이션이 갱신되었으며 애플리케이션이 서브스크립션 상태를 자동으로 업데이트하지 않은 경우에 필요할 수도 있습니다.



서브스크립션 갱신

데이터 제공

최종 사용자 라이센스 계약서에 따른 데이터 프로비전

활성화 코드를 적용하여 Kaspersky Endpoint Security를 활성화하면 애플리케이션의 올바른 사용을 확인하려는 목적으로 다음 정보를 정기적으로 Kaspersky에 자동 전송하는 데 동의하게 됩니다:

- Kaspersky Endpoint Security의 유형, 버전 및 현지화
- Kaspersky Endpoint Security의 설치된 업데이트 버전
- 컴퓨터 ID 및 컴퓨터에 설치된 특정 Kaspersky Endpoint Security의 ID
- 일련 번호 및 활성 키 식별자
- 운영 체제의 유형, 버전, 비트 및 가상 환경의 이름(Kaspersky Endpoint Security가 가상 환경에 설치된 경우)
- 권리 소유자 서비스에 대한 고유 요청 ID
- 정보가 전송될 때 활성화되는 Kaspersky Endpoint Security 구성 요소의 ID

Kaspersky는 Kaspersky 소프트웨어의 보급 및 사용에 관한 통계를 생성하기 위해 이 정보를 사용할 수도 있습니다.

활성화 코드를 사용하면 상기 나열된 데이터의 자동 전송에 동의하게 됩니다. 이 정보가 Kaspersky로 전송되는 데 동의하지 않으시면 키 파일을 사용하여 Kaspersky Endpoint Security를 활성화해야 합니다.

최종 사용자 라이센스 계약서의 조건에 동의하시면 다음 정보를 자동으로 전송하는 데 동의하게 됩니다:

- Kaspersky Endpoint Security 업그레이드 시:
  - Kaspersky Endpoint Security 버전
  - Kaspersky Endpoint Security ID
  - 활성 키
  - 업그레이드 작업 시작 고유 ID
  - Kaspersky Endpoint Security 설치 고유 ID
- Kaspersky Endpoint Security 인터페이스에서 링크로 이동할 때:
  - Kaspersky Endpoint Security 버전
  - 운영 체제 버전
  - Kaspersky Endpoint Security 활성화 날짜
  - 라이센스 만료 날짜
  - 키 생성 날짜

- Kaspersky Endpoint Security 설치 날짜
- Kaspersky Endpoint Security ID
- 운영 체제에서 탐지된 취약점 ID
- Kaspersky Endpoint Security에 설치된 마지막 업데이트 ID
- 위협을 포함하는 탐지된 파일의 해시, Kaspersky 분류에 따른 해당 위협의 이름
- Kaspersky Endpoint Security 활성화 오류 카테고리
- Kaspersky Endpoint Security 활성화 오류 코드
- 키 만료 전까지 남은 날짜
- 키 추가 후 경과된 날짜
- 라이센스 만료 후 경과된 날짜
- 현재 라이센스가 적용된 컴퓨터 수
- 활성 키
- Kaspersky Endpoint Security 라이센스 기간
- 라이센스의 현재 상태
- 현재 라이센스의 유형
- 애플리케이션 유형
- 업그레이드 작업 시작 고유 ID
- 컴퓨터의 Kaspersky Endpoint Security 설치 고유 ID
- Kaspersky Endpoint Security 인터페이스 언어

Kaspersky에 제공된 정보는 법률 및 요건, Kaspersky의 해당 규정에 따라 보호됩니다. 데이터는 암호화된 통신 채널을 통해 전송됩니다.

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.

Kaspersky Security Network 사용 시 데이터 제공

Kaspersky Endpoint Security가 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.

Detection and Response 솔루션 사용 시 데이터 제공

Kaspersky Endpoint Security가 설치된 컴퓨터에서 Kaspersky Endpoint Detection and Response, Kaspersky Sandbox 및 Kaspersky Anti Targeted Attack Platform 서버로 자동 전송하기 위한 데이터가 저장되었습니다. 파일은 일반적이고 암호화되지 않은 형태로 저장됩니다.

구체적인 데이터 집합은 Kaspersky Endpoint Security를 사용하는 솔루션에 따라 달라집니다.

Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Security가 제거되면 애플리케이션이 컴퓨터에 로컬로 저장한 모든 데이터가 삭제됩니다.

IOC 검사 작업 예외의 결과로 수신된 데이터(표준 작업)

Kaspersky Endpoint Security는 *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 Sandbox

Kaspersky Endpoint Security가 제거되면 애플리케이션이 컴퓨터에 로컬로 저장한 모든 데이터가 삭제됩니다.

서비스 데이터

Kaspersky Endpoint Security는 자동 응답 동안 처리된 데이터를 다음과 같이 저장합니다.

- Kaspersky Endpoint Security의 내장 에이전트를 구성하는 동안 사용자가 입력한 처리된 파일 및 데이터:
  - 격리된 파일
  - Kaspersky Sandbox와의 통합에 사용한 인증서의 공개 키
- Kaspersky Endpoint Security 내장 에이전트의 캐시:
  - 검사 결과가 캐시에 기록된 시간
  - 검사 작업의 MD5 해시
  - 검사 작업 식별자
  - 개체에 대한 검사 결과
- 개체 검사 요청 대기열:
  - 대기열에 있는 개체의 ID
  - 개체가 대기열에 배치된 시간
  - 대기열에 있는 개체의 처리 상태
  - 개체 검사 작업이 생성된 운영 체제의 사용자 세션 ID
  - 작업을 생성하기 위해 계정을 사용한 운영 체제 사용자의 시스템 식별자(SID)
  - 개체 검사 작업의 MD5 해시
- Kaspersky Endpoint Security의 내장 에이전트가 Kaspersky Sandbox의 검사 결과를 기다리고 있는 작업에 대한 정보:
  - 개체 검사 작업을 수신한 시간
  - 개체 처리 상태
  - 개체 검사 작업이 생성된 운영 체제의 사용자 세션 ID

- 개체 검사 작업의 식별자
- 개체 검사 작업의 MD5 해시
- 작업을 생성하기 위해 계정을 사용한 운영 체제 사용자의 시스템 식별자(SID)
- 자동으로 생성된 IOC의 XML 스키마
- 검사한 개체의 MD5 또는 SHA256 해시
- 처리 오류
- 검사 작업이 생성된 개체의 이름
- 개체에 대한 검사 결과

Kaspersky Sandbox에 대한 요청 관련 데이터

Kaspersky Endpoint Security 내장형 에이전트에서 Kaspersky Sandbox로 다음과 같은 데이터 요청은 컴퓨터에 로컬로 저장됩니다.

- 검사 작업의 MD5 해시
- 검사 작업 식별자
- 검사한 개체 및 모든 관련 파일

IOC 검사 작업 실행 결과 수신된 데이터(독립 실행형 과제)

Kaspersky Endpoint Security는 *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

Kaspersky Endpoint Detection and Response Expert(on-premise)

Kaspersky Endpoint Security가 제거되면 애플리케이션이 컴퓨터에 로컬로 저장한 모든 데이터가 삭제됩니다.

서비스 데이터

Kaspersky Endpoint Security의 내장 에이전트는 다음의 데이터를 로컬로 저장합니다.

- EDR Expert(온프레미스) 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 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 Endpoint Security의 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 Endpoint Security에서 EDR Expert 구성 요소로 전송한 요청의 데이터

EDR Expert(on-premise) 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 Endpoint Security의 자기 보호 상태
  - 컴퓨터에 설치된 운영 체제 이름 및 버전
  - Kaspersky Endpoint Security 버전
  - 애플리케이션 설정 및 작업 설정의 버전
  - 작업 상태: 작업 식별자, 실행 상태, 오류 코드
- 서버에서 파일을 얻기 위한 요청에서:
  - 파일의 고유 식별자
  - 고유한 Kaspersky Endpoint Security 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 Endpoint Security의 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 Network Detection and Response(KATA)

Kaspersky Endpoint Security가 제거되면 애플리케이션이 컴퓨터에 로컬로 저장한 모든 데이터가 삭제됩니다.

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
- 파일 서명이 생성된 날짜 및 시간
- 서명 파일에 사용된 인증서 체인
- 인증서 체인 유형
- 체인의 인증서
- 인증서 발급자 이름
- 인증서 보유자 이름
- 인증서 일련 번호
- 인증서 지문 알고리즘
- 인증서 지문
- 인증서 유효 기간

- **로그인 세션 데이터**
  - 로그인 세션 ID
  - 로그인한 사용자의 계정 이름
  - 사용자 계정 유형
  - 세션 유형
  - 로그인을 시도한 컴퓨터의 IP 주소
  - 로그인을 시도한 로컬 컴퓨터의 IP 주소
  - 이 이벤트가 나타내는 세션에 승격된 권한 및 관리자 권한이 있음을 나타내는 플래그
  - 다른 세션이 이 로그인 세션에 링크되어 있는지 여부를 나타내는 파라미터
  - 터미널 세션에 사용된 프로토콜
  - 터미널 세션에 사용된 IPv4 프로토콜

- **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
  - 이더넷 프레임 EtherType 필드
  - 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 메소드
  - 호스트 이름이 없는 경로
  - 호스트 이름
  - 연결 시 동적 프로세스 상태
  - 연결 방향
  - 동적 프로세스 상태
  - 이더넷 프레임 EtherType 필드

- **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

- **호스트의 프로세스 만들기에 대한 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
  - 프로세스 권한 토큰 목록
  - 속성 권한
  - 해석된 파일의 고유 식별자 목록
  - 프로세스 상태
  - 프로세스를 시작하는 데 사용된 명령
- **프로세스 종료 데이터**
  - 프로세스의 고유 식별자
- **탐지된 위협 데이터**
  - 위협 정보
  - 위협 평결
  - AMR 레코드 번호
  - 안티 바이러스 데이터베이스 버전
  - 위협 탐지 모드
  - 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
- 감염된 개체를 수신한 네트워크 프로토콜
- 감염된 개체를 수신한 로컬 주소
- 감염된 개체가 수신된 외부 주소
- 개체 콘텐츠 유형
- 탐지된 위협의 컨텍스트
- 개체 콘텐츠
- 위협 탐지가 백그라운드에서 실행되었음을 나타내는 플래그

- **위협 처리에 대한 데이터**
  - 위협 정보
  - 위협 평결
  - AMR 레코드 번호
  - 안티 바이러스 데이터베이스 버전
  - 위협 탐지 모드
  - 감염된 개체 이름
  - 개체의 MD5 및 SHA256 해시
  - 감염된 프로세스의 고유 식별자
  - 감염된 개체의 고유 식별자
  - 감염된 개체를 수신한 네트워크 프로토콜

- 감염된 개체를 수신한 로컬 주소
- 감염된 개체가 수신된 외부 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 차단 여부
  - 암호의 만료 여부
  - 암호 변경이 필요한지 여부
  - 암호 변경 허용 여부
  - 사용자 계정 유형
  - 이 계정에 대해 자동 로그인이 활성화되었는지 여부
  - 사용자가 속한 그룹 목록

Kaspersky Unified Monitoring and Analysis Platform(KUMA)와 통합

Kaspersky Endpoint Security가 제거되면 애플리케이션이 컴퓨터에 로컬로 저장한 모든 데이터가 삭제됩니다.

Kaspersky Unified Monitoring and Analysis Platform(KUMA)과 통합하면 연결 설정 데이터와 Windows 로그에 등록된 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.

유럽 연합 법규(GDPR) 준수

Kaspersky Endpoint Security는 다음 시나리오에서 Kaspersky로 데이터를 전송할 수 있습니다:

- Kaspersky Security Network 사용.
- 활성화 코드로 애플리케이션 활성화.
- 애플리케이션 모듈 및 안티 바이러스 데이터베이스 업데이트.
- 애플리케이션 인터페이스의 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 Endpoint Security를 사용하기 전에 최종 사용자 라이센스 계약서 및 Kaspersky Security Network 진술문에서 전송된 데이터에 대한 설명을 주의 깊게 읽으십시오. 설명된 시나리오에 따라 Kaspersky Endpoint Security에서 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. KPSN에 대한 자세한 내용은 Kaspersky Private Security Network 설명서를 참조하십시오.

활성화 코드로 애플리케이션 활성화

활성화 코드를 사용하면 최종 사용자 라이센스 계약서에 나열된 데이터를 자동으로 제공하는 데 동의하는 것입니다. 이 정보를 Kaspersky에 제공하는 데 동의하지 않으면 키 파일을 사용하여 Kaspersky Endpoint Security를 활성화해야 합니다.

애플리케이션 모듈 및 안티 바이러스 데이터베이스 업데이트

Kaspersky 서버를 사용하면 최종 사용자 라이센스 계약서에 나열된 데이터를 자동으로 제공하는 데 동의하는 것입니다. Kaspersky는 Kaspersky Endpoint Security가 합법적으로 사용되고 있는지 확인하기 위해 이 정보가 필요합니다. 이 정보를 Kaspersky에 제공하는 데 동의하지 않으면 Kaspersky Security Center를 사용하여 데이터베이스를 업데이트하거나 Kaspersky 업데이트 유틸리티를 사용하십시오.

애플리케이션 인터페이스의 링크를 따름

애플리케이션 인터페이스에서 링크를 사용하면 최종 사용자 라이센스 계약서에 나열된 데이터의 자동 제공에 동의하는 것입니다. 각 특정 링크에서 전송되는 정확한 데이터 목록은 링크가 애플리케이션 인터페이스에 있는 위치와 해결하려는 문제에 따라 다릅니다. 이 데이터를 Kaspersky에 제공하는 데 동의하지 않으면 간략한 애플리케이션 인터페이스를 사용하거나 애플리케이션 인터페이스를 숨깁니다.

덤프 기록

덤프 기록을 사용하는 경우 Kaspersky Endpoint Security는 이 덤프 파일이 생성된 시점에 애플리케이션 프로세스의 모든 메모리 데이터를 포함하는 덤프 파일을 생성합니다.

시작하기

Kaspersky Endpoint Security 설치 후 다음 인터페이스를 사용하여 애플리케이션을 관리할 수 있습니다.

- 로컬 애플리케이션 인터페이스
- Kaspersky Security Center 관리 콘솔
- Kaspersky Security Center 웹 콘솔
- Kaspersky Security Center Cloud Console

Kaspersky Security Center 관리 콘솔

Kaspersky Security Center는 원격으로 Kaspersky Endpoint Security의 설치, 제거, 시작 및 중지와 이용 가능한 애플리케이션 구성 요소 세트의 변경, 애플리케이션 설정 구성, 키 추가, 업데이트 및 검사 작업 시작/중지 등을 할 수 있습니다.

Kaspersky Endpoint Security 관리 플러그인을 사용하여 Kaspersky Security Center를 통해 애플리케이션을 관리할 수 있습니다.

Kaspersky Security Center를 통해 애플리케이션을 관리하는 방법에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Security Center 웹 콘솔 또는 Kaspersky Security Center Cloud Console

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

Kaspersky Security Center Cloud 콘솔(이하 "*Cloud Console*")은 조직의 네트워크를 보호하고 관리하기 위한 클라우드 기반 솔루션입니다. Kaspersky Security Center Cloud 콘솔에 대한 상세 정보는 Kaspersky Security Center Cloud 콘솔 도움말을 참조하십시오.

웹 콘솔 및 Cloud Console을 통해 다음을 수행할 수 있습니다:

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

웹 콘솔, Cloud Console 및 Kaspersky Security Center 관리 콘솔을 통해 Kaspersky Endpoint Security를 관리할 때 모두 다른 관리 범위를 제공합니다. 사용 가능한 구성 요소 및 작업은 콘솔마다 다릅니다.

Kaspersky Endpoint Security for Windows 관리 플러그인 정보

Kaspersky Endpoint Security for Windows 관리 플러그인은 Kaspersky Endpoint Security 및 Kaspersky Security Center 간의 상호 작용을 가능하게 합니다. 관리 플러그인을 사용하면 정책, 작업 및 로컬 애플리케이션 설정을 사용하여 Kaspersky Endpoint Security를 관리할 수 있습니다. Kaspersky Security Center 웹 콘솔과의 상호 작용은 웹 플러그인에서 제공됩니다.

관리 플러그인 버전은 클라이언트 컴퓨터에 설치된 Kaspersky Endpoint Security 애플리케이션 버전과 다를 수 있습니다. 설치된 관리 플러그인 버전에 포함된 기능이 설치된 Kaspersky Endpoint Security 버전보다 적으면 관리 플러그인을 통해 누락된 기능의 설정을 제어할 수 없습니다. 사용자는 Kaspersky Endpoint Security 로컬 인터페이스에서 이러한 설정을 수정할 수 있습니다.

웹 플러그인은 Kaspersky Security Center 웹 콘솔에 기본적으로 설치되지 않습니다. Kaspersky Security Center 웹 콘솔이 설치된 컴퓨터에 웹 플러그인이 설치되어 있어야 합니다. 브라우저에서 웹 콘솔에 접근할 수 있는 모든 관리자는 웹 플러그인의 기능을 사용할 수 있습니다. 웹 콘솔 인터페이스에서 설치된 웹 플러그인 목록을 확인할 수 있습니다(**콘솔 설정 → 웹 플러그인**). 웹 플러그인 버전과 웹 콘솔의 호환성에 대한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Endpoint Security를 Kaspersky Endpoint Detection and Response Optimum 솔루션의 일부로 사용하는 경우 Kaspersky Endpoint Detection and Response 관리 플러그인을 설치해야 합니다. 경고 세부 정보를 표시하려면 관리 플러그인이 필요합니다. *경고 세부 정보*는 탐지된 위협에서 수집한 전체 정보를 확인하는 도구입니다. 경고 세부 정보에는 컴퓨터에서의 파일 히스토리 등이 포함됩니다. 따라서 위협 대응 작업을 생성하려면 Kaspersky Endpoint Security 관리 플러그인이 필요하고 경고 세부 정보를 보려면 EDR 관리 플러그인이 필요합니다.

웹 플러그인 설치

웹 플러그인은 다음과 같이 설치할 수 있습니다:

- Kaspersky Security Center 웹 콘솔의 빠른 시작 마법사를 사용하여 웹 플러그인을 설치합니다.

  웹 콘솔을 중앙 관리 서버에 처음으로 연결하면 웹 콘솔에서 빠른 시작 마법사를 실행할지 묻는 메시지가 자동으로 표시됩니다. 웹 인터페이스에서 빠른 시작 마법사를 실행할 수도 있습니다(**발견 및 배포 → 배포 및 할당 → 빠른 시작 마법사**). 빠른 시작 마법사는 설치된 웹 플러그인이 최신 상태인지를 확인하고 필요한 업데이트를 다운로드할 수도 있습니다. Kaspersky Security Center 웹 콘솔의 빠른 시작 마법사에 대한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.

- 웹 콘솔에서 사용 가능한 배포 패키지 목록에서 웹 플러그인을 설치합니다.

  웹 플러그인을 설치하려면 웹 콘솔 인터페이스에서 Kaspersky Endpoint Security 웹 플러그인의 배포 패키지를 선택합니다(**콘솔 설정 → 웹 플러그인**). 새 버전의 Kaspersky 애플리케이션이 릴리즈되면 사용 가능한 배포 패키지 목록이 자동으로 업데이트됩니다.

- 외부 소스에서 웹 콘솔에 배포 패키지를 다운로드합니다.

  웹 플러그인을 설치하려면 웹 콘솔 인터페이스에서 Kaspersky Endpoint Security 웹 플러그인용 배포 패키지의 ZIP 압축파일을 선택합니다(**콘솔 설정 → 웹 플러그인**). 예를 들어 Kaspersky 웹사이트에서 웹 플러그인의 배포 패키지를 다운로드할 수 있습니다.

Kaspersky Endpoint Security 12.11 for Windows부터 웹 플러그인의 설치 절차가 변경되었습니다. 이제 배포 패키지에 *Kaspersky Endpoint Security for Windows 14.0.0*과 *통합 보호 및 관리 플러그인*에 해당하는 두 가지 웹 플러그인이 포함됩니다. 이는 Kaspersky 애플리케이션 관리를 위한 단일 통합 웹 플러그인으로의 전환 때문입니다. 통합 웹 플러그인을 사용하면 단일 정책을 생성하여 여러 Kaspersky 애플리케이션(Kaspersky Endpoint Security for Windows, macOS, Linux 등)을 관리할 수 있습니다. 통합 웹 플러그인으로 전환하는 데 여러 버전이 걸릴 수 있습니다. 전환이 완료되면 배포 패키지에는 *통합 보호 및 관리 플러그인*만 포함됩니다.

관리 플러그인 업데이트

Kaspersky Endpoint Security for Windows 관리 플러그인을 업데이트하려면, 최신 버전의 플러그인(배포 키트에 포함)을 다운로드하고 플러그인 설치 마법사를 실행하십시오.

새 버전의 웹 플러그인을 사용할 수 있게 되면 *활용된 플러그인에 대한 업데이트가 있음* 알림을 표시합니다. 이 웹 콘솔 알림에서 웹 플러그인 버전을 계속 업데이트할 수 있습니다. 웹 콘솔 인터페이스에서 새 웹 플러그인 업데이트를 직접 확인할 수도 있습니다(**콘솔 설정 → 웹 플러그인**). 업데이트하는 동안 이전 버전의 웹 플러그인이 자동으로 제거됩니다.

> 웹 플러그인이 업데이트되면 기존 항목(예, 정책 또는 작업)이 저장됩니다. Kaspersky Endpoint Security의 새 기능을 구현하는 항목의 새 설정이 기존 항목에 나타나며 기본값을 갖습니다.

웹 플러그인은 다음과 같이 업데이트할 수 있습니다:

- 온라인 모드의 웹 플러그인 목록에서 웹 플러그인을 업데이트합니다.

  웹 플러그인을 업데이트하려면 웹 콘솔 인터페이스에서 Kaspersky Endpoint Security 웹 플러그인의 배포 패키지를 선택합니다(**콘솔 설정 → 웹 플러그인**). 웹 콘솔은 Kaspersky 서버에서 사용 가능한 업데이트를 확인하고 관련 업데이트를 다운로드합니다.

- 파일에서 웹 플러그인을 업데이트합니다.

  웹 플러그인을 업데이트하려면 웹 콘솔 인터페이스에서 Kaspersky Endpoint Security 웹 플러그인용 배포 패키지의 ZIP 압축파일을 선택해야 합니다(**콘솔 설정 → 웹 플러그인**). 예를 들어 Kaspersky 웹사이트에서 웹 플러그인의 배포 패키지를 다운로드할 수 있습니다. Kaspersky Endpoint Security 웹 플러그인은 최신 버전으로만 업데이트할 수 있습니다. 웹 플러그인을 이전 버전으로 업데이트할 수 없습니다.

정책이나 작업과 같은 항목이 열리면 웹 플러그인이 호환성 정보를 확인합니다. 웹 플러그인 버전이 호환성 정보에 지정된 버전과 같거나 상위 버전인 경우 이 항목 설정을 변경할 수 있습니다. 그렇지 않으면 웹 플러그인을 사용해 선택한 항목의 설정을 변경할 수 없습니다. 이 경우 웹 플러그인을 업데이트하기를 권장합니다.

여러 버전의 관리 플러그인 사용 시의 특별 고려 사항

Kaspersky Endpoint Security 관리 플러그인 호환성에 관한 정보에 지정된 버전 이상의 관리 플러그인이 있을 때만 Kaspersky Security Center를 통해 Kaspersky Endpoint Security를 관리할 수 있습니다. 배포 키트에 포함된 installer.ini 파일에서 관리 플러그인의 최소 요구 버전을 확인할 수 있습니다.

정책이나 작업과 같은 항목이 열리면 관리 플러그인이 호환성 정보를 확인합니다. 관리 플러그인 버전이 호환성 정보에 지정된 버전과 같거나 상위 버전인 경우 이 항목 설정을 변경할 수 있습니다. 그렇지 않으면 관리 플러그인을 사용해 선택한 항목의 설정을 변경할 수 없습니다. 이 경우 관리 플러그인을 업그레이드하는 것이 좋습니다.

관리 콘솔에 Kaspersky Endpoint Security 관리 플러그인이 설치된 경우 새 버전의 관리 플러그인을 설치할 때는 다음을 고려해야 합니다.

- Kaspersky Endpoint Security 관리 플러그인의 이전 버전은 제거됩니다.
- 새 버전의 Kaspersky Endpoint Security 관리 플러그인은 사용자의 컴퓨터에 있는 Kaspersky Endpoint Security for Windows의 이전 버전을 관리할 수 있도록 지원합니다.
- 새 버전의 관리 플러그인을 사용하여 이전 버전의 관리 플러그인으로 생성한 정책, 작업 및 기타 항목의 설정을 변경할 수 있습니다.
- 새 설정의 경우 정책, 정책 프로필 또는 작업을 처음 저장할 때 새 버전의 관리 플러그인이 기본값을 지정합니다.

  관리 플러그인을 업그레이드한 후에는 정책 및 정책 프로필에 새 설정 값을 확인하고 저장하는 것이 좋습니다. 이렇게 하지 않으면 사용자 컴퓨터에 설치된 새로운 Kaspersky Endpoint Security 설정 그룹이 기본값을 적용하고 각종 설정이 편집 가능한 상태가 될 수 있습니다(속성). 계층 구조의 최상위 레벨에서 정책 및 정책 프로필로 시작하는 설정을 확인하는 것이 좋습니다. 또한 Kaspersky Security Center의 모든 기능 영역에 대한 접근 권한이 있는 사용자 계정을 사용하는 것이 좋습니다.

  애플리케이션의 새로운 기능에 대해 알아보려면 릴리스 정보 또는 애플리케이션 도움말을 참조하시기 바랍니다.

- 새 버전의 관리 플러그인에 있는 설정 그룹에 새 파라미터가 추가된 경우 이 설정 그룹에 대해 이전에 정의된 / 속성의 상태는 변경되지 않습니다.

외부 서비스와 상호 작용하기 위해 암호화된 프로토콜을 사용할 때 특별히 고려해야 할 사항

Kaspersky Endpoint Security 및 Kaspersky Security Center는 Kaspersky의 외부 서비스와 작업하기 위해 TLS(Transport Layer Security)로 암호화된 통신 채널을 사용합니다. Kaspersky Endpoint Security는 다음 기능을 위해 외부 서비스를 사용합니다:

- 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트
- 활성화 코드로 애플리케이션 활성화(활성화 2.0)
- Kaspersky Security Network 사용.

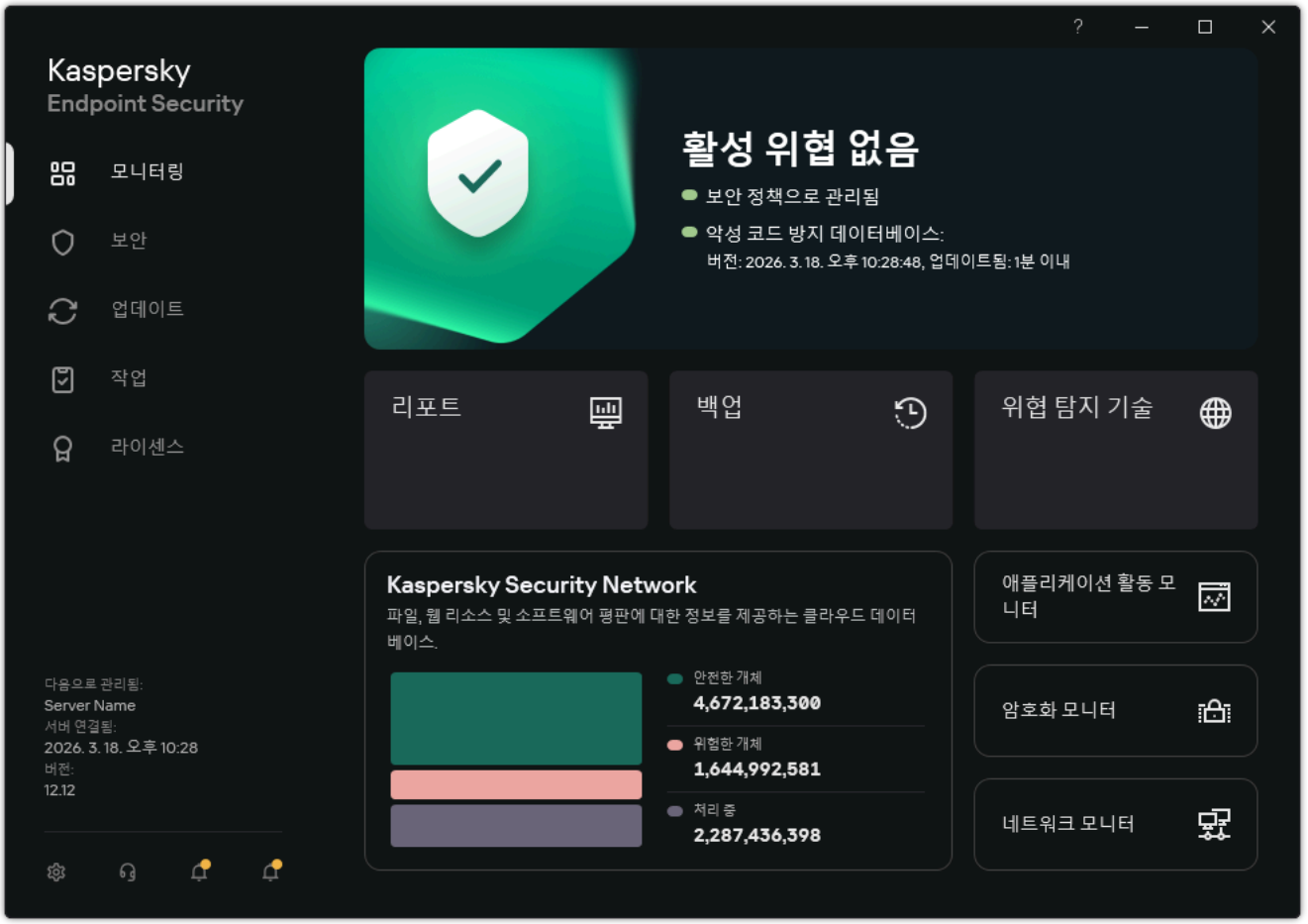
TLS를 사용하면 다음 기능을 제공하여 애플리케이션을 보호할 수 있습니다.

- 암호화. 메시지의 내용은 기밀이며 제삼자 사용자에게 공개되지 않습니다.
- 무결성. 메시지 수신자는 보낸 사람이 메시지를 전달한 이후 메시지 내용이 수정되지 않았음을 확신합니다.
- 인증. 수신자는 신뢰하는 Kaspersky 서버만을 통해 커뮤니케이션이 설정되었음을 확신합니다.

Kaspersky Endpoint Security는 서버 인증을 위해 공개 키 인증서를 사용합니다. 인증서를 사용하려면 PKI(Public Key Infrastructure)가 필요합니다. 인증 기관은 PKI의 일부입니다. Kaspersky 서비스는 상당히 기술적이며 일반에 공개되지 않기 때문에 Kaspersky에서는 자체 인증 기관을 사용합니다. 이 경우 Thawte, VeriSign, GlobalTrust 및 기타의 루트 인증서가 취소되어도 Kaspersky PKI는 중단없이 계속 작동합니다.

Kaspersky Endpoint Security는 MITM(HTTPS 프로토콜 구문 분석을 지원하는 소프트웨어 및 하드웨어 도구)이 있는 환경을 안전하지 않은 것으로 간주합니다. Kaspersky 서비스를 사용할 때 오류가 발생할 수 있습니다. 예를 들어 Self-Signed Certificate 사용과 관련된 오류가 발생할 수 있습니다. 이러한 오류가 발생할 수 있는 원인은 사용자 환경의 HTTPS 검사 도구가 Kaspersky PKI를 인식하지 못하기 때문입니다. 이러한 문제를 해결하려면 외부 서비스와의 상호 작용에 대한 예외 규칙을 구성해야 합니다.

애플리케이션 인터페이스



메인 애플리케이션 창

모니터링	• **리포트**. 애플리케이션, 개별 구성 요소 및 작업의 동작 중에 발생한 이벤트를 봅니다. • **백업**. 애플리케이션이 탐지한 감염 파일 복사본의 저장소를 봅니다. • **위협 탐지 기술**. 위협 탐지 기술에 대한 정보와 이러한 기술로 탐지된 보안 위협 수를 봅니다. • **Kaspersky Security Network** Kaspersky Endpoint Security와 Kaspersky Security Network간의 연결 상태 및 글로벌 KSN 통계. *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 Endpoint Security에서 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 Endpoint Security는 검사한 웹 주소의 평판 정보는 물론이고 검사한 파일의 카테고리 및 평판 에 관한 정보도 수신하게 됩니다. • **애플리케이션 활동 모니터**. 설치된 애플리케이션의 동작에 대한 정보를 봅니다. 애플리케이션 활동 모니터는 애플리케이션과 관련된 파일, 레지스트리 및 운영 체제 이벤트를 추적합니다. • **네트워크 모니터**. 컴퓨터의 네트워크 활동에 대한 정보를 실시간으로 봅니다. • **암호화 모니터**. 디스크 암호화 또는 복호화 프로세스를 실시간으로 모니터링합니다. 암호화 모니터는 Kaspersky 디스크 암호화 구성 요소 또는 BitLocker 드라이브 암호화 구성 요소가 설치된 경우 사용할 수 있습니다.
보안	설치된 구성 요소의 작동 상태. 구성 요소를 계속 구성하거나 리포트를 볼 수도 있습니다.
업데이트	Kaspersky Endpoint Security 업데이트 작업 관리. 안티 바이러스 데이터베이스 및 애플리케이션 모듈을 업데이트하고 마지막 업데이트를 롤백할 수 있습니다. 관리자는 사용자에게 섹션 숨기거나 작업 관리를 제한할 수 있습니다.
작업	Kaspersky Endpoint Security 검사 작업 관리. 악성 코드 검사 및 애플리케이션 무결성 검사를 실행할 수 있습니다. 관리자는 사용자로부터 작업을 숨기거나 작업 관리를 제한할 수 있습니다.
라이센스	애플리케이션 라이센스. 라이센스를 구매하거나, 애플리케이션을 활성화하거나 서브스크립션을 갱신할 수 있습니다. 현재 라이센스 정보를 확인할 수도 있습니다.
⚙	애플리케이션 설정 구성. 관리자는 Kaspersky Security Center의 설정 변경을 금지할 수 있습니다.

	애플리케이션에 대한 정보: Kaspersky Endpoint Security의 현재 버전, 데이터베이스 배포 날짜, 키 및 기타 정보. Kaspersky 정보 리소스로 이동하여 애플리케이션의 구매, 설치 및 사용에 관한 유용한 정보, 권장 사항 및 자주 묻는 질문에 대한 답변을 참조할 수 있습니다.
	사용 가능한 업데이트에 대한 정보와 암호화된 파일 및 장치에 대한 접근 요청이 포함된 메시지.

작업 표시줄 알림 영역의 애플리케이션 아이콘

Kaspersky Endpoint Security를 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 작업을 수행해야 할 때 Kaspersky Endpoint Security에  경고가 표시됩니다.
-  아이콘은 애플리케이션의 매우 중요한 보호 구성 요소가 비활성화되었거나 오작동했음을 나타냅니다. 라이센스가 만료되었거나 애플리케이션 오류로 인해 보호 구성 요소가 오작동할 수 있습니다. Kaspersky Endpoint Security에 컴퓨터 보호 문제에 대한 설명과 함께. 경고가 표시됩니다.

애플리케이션 아이콘의 마우스 오른쪽 메뉴는 다음 항목을 포함하고 있습니다:

- **Kaspersky Endpoint Security for Windows**. 메인 애플리케이션 창을 엽니다. 이 창에서 애플리케이션 구성 요소 및 작업의 작동을 조정하고 처리된 파일과 탐지된 위협 통계를 볼 수 있습니다.
- **보호 일시 중지 / 보호 다시 시작**. 정책에서 자물쇠() 표시가 없는 모든 보호 및 제어 구성 요소의 작동을 일시 중지합니다. 이 작업을 수행하기 전에 Kaspersky Security Center 정책을 비활성화하는 것이 좋습니다.

  보호 및 제어 구성 요소의 동작을 일시 중지하기 전에 애플리케이션이 Kaspersky Endpoint Security에 접근하기 위한 암호(계정 암호 또는 임시 암호)를 요청합니다. 일시 중지 기간은 지정된 시간 동안, 다시 시작할 때까지 또는 사용자 요청 시 중에서 선택할 수 있습니다.

  이 마우스 오른쪽 메뉴 항목은 암호 보호가 설정된 경우 사용할 수 있습니다. 보호 및 제어 구성 요소의 동작을 다시 시작하려면 애플리케이션의 마우스 오른쪽 메뉴에서 **보호 다시 시작**을 클릭합니다.

  보호 및 제어 구성 요소의 동작을 일시 중지해도 업데이트 및 악성 코드 검사 작업의 성능에 영향을 미치지 않습니다. 또한 애플리케이션은 계속해서 Kaspersky Security Network를 사용합니다.

- **정책 사용 안 함/정책 사용**. Kaspersky Security Center 정책을 비활성화합니다. 정책에 닫힌 자물쇠()가 있는 설정을 포함하여 모든 Kaspersky Endpoint Security 설정을 수정할 수 있습니다. 정책이 비활성화되면 애플리케이션은 Kaspersky Endpoint Security 접근용 암호(계정 암호 또는 임시 암호)를 요청합니다. 이 마우스 오른쪽 메뉴 항목은 암호 보호가 설정된 경우 사용할 수 있습니다. 정책을 사용하려면 애플리케이션의 마우스 오른쪽 메뉴에서 **정책 사용**을 선택합니다.

- **설정**. 애플리케이션 설정 창을 엽니다.
- **지원**. Kaspersky 기술 지원에 문의하는 데 필요한 정보가 담긴 창이 열립니다.
- **정보**. 이 항목은 애플리케이션 세부 내용이 나와 있는 정보 창을 엽니다.
- **종료**. 이 항목은 Kaspersky Endpoint Security를 종료합니다. 이 마우스 오른쪽 메뉴를 누르면 애플리케이션이 컴퓨터 RAM에서 언로드됩니다.



애플리케이션 아이콘 마우스 오른쪽 메뉴

간략한 애플리케이션 인터페이스

간략한 인터페이스 표시가 구성된 Kaspersky Security Center 정책이 Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터에 적용되면 이 클라이언트 컴퓨터에서는 메인 애플리케이션 창을 사용할 수 없습니다. Kaspersky Endpoint Security 아이콘(아래 그림 참조)을 마우스 오른쪽 버튼으로 눌러 다음 항목이 포함된 마우스 오른쪽 메뉴를 엽니다:

- **정책 사용 안 함/정책 사용**. Kaspersky Security Center 정책을 비활성화합니다. 정책에 닫힌 자물쇠()가 있는 설정을 포함하여 모든 Kaspersky Endpoint Security 설정을 수정할 수 있습니다. 정책이 비활성화되면 애플리케이션은 Kaspersky Endpoint Security 접근용 암호(계정 암호 또는 임시 암호)를 요청합니다. 이 마우스 오른쪽 메뉴 항목은 암호 보호가 설정된 경우 사용할 수 있습니다. 정책을 사용하려면 애플리케이션의 마우스 오른쪽 메뉴에서 **정책 사용**을 선택합니다.
- **작업**. 드롭다운 목록에 다음 항목이 있습니다:
  - **애플리케이션 무결성 검사**.
  - **데이터베이스를 이전 버전으로 롤백**.
  - **전체 검사**.
  - **사용자 지정 검사**.
  - **중요 영역 검사**.
  - **업데이트**.
- **지원**. Kaspersky 기술 지원에 문의하는 데 필요한 정보가 담긴 창이 열립니다.
- **종료**. 이 항목은 Kaspersky Endpoint Security를 종료합니다. 이 마우스 오른쪽 메뉴를 누르면 애플리케이션이 컴퓨터 RAM에서 언로드됩니다.



간략한 인터페이스를 표시할 때 애플리케이션 아이콘의 마우스 오른쪽 메뉴

애플리케이션 인터페이스 표시 구성

사용자에 대한 애플리케이션 인터페이스 표시 모드를 구성할 수 있습니다. 사용자는 다음과 같은 방법으로 애플리케이션과 상호 작용할 수 있습니다.

- **간략한 인터페이스 표시**. 클라이언트 컴퓨터에서 메인 애플리케이션 창에 접근할 수 없으며 Windows 알림 영역의 아이콘만 사용할 수 있습니다. 아이콘의 마우스 오른쪽 메뉴에서 사용자는 Kaspersky Endpoint Security로 제한된 수의 작업을 수행할 수 있습니다. Kaspersky Endpoint Security에서도 애플리케이션 아이콘 위에 알림을 표시합니다.

- **사용자 인터페이스 표시**. 클라이언트 컴퓨터에서 Kaspersky Endpoint Security의 메인 창과 Windows 알림 영역의 아이콘을 모두 사용할 수 있습니다. 아이콘의 마우스 오른쪽 메뉴에서 사용자는 Kaspersky Endpoint Security로 작업을 수행할 수 있습니다. Kaspersky Endpoint Security에서도 애플리케이션 아이콘 위에 알림을 표시합니다.

- **사용자 인터페이스 표시 안 함**. 클라이언트 컴퓨터에 Kaspersky Endpoint Security 동작의 어떤 징후도 표시되지 않습니다. Windows 알림 영역의 아이콘과 알림을 사용할 수 없습니다.

관리 콘솔(MMC)에서 애플리케이션 인터페이스 표시 모드를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **일반 설정 → 인터페이스**를 선택합니다.

4. **사용자와의 상호 작용** 블록에서 다음 중 하나를 수행합니다:

   - 다음 인터페이스 요소를 클라이언트 컴퓨터에 표시하려면 **사용자 인터페이스 표시** 확인란을 선택합니다:

     - **시작** 메뉴에 애플리케이션 이름이 포함된 폴더

     - Microsoft Windows 작업 표시줄 알림 영역에 있는 Kaspersky Endpoint Security 아이콘

     - 팝업 알림

     이 확인란을 선택하면 이용 가능한 권한에 따라 사용자가 애플리케이션 인터페이스에서 애플리케이션 설정을 보고 변경할 수 있습니다.

   - 클라이언트 컴퓨터에서 Kaspersky Endpoint Security의 모든 표시를 숨기려면 **사용자 인터페이스 표시** 확인란을 선택 해제합니다.

5. Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터에 간략한 애플리케이션 인터페이스를 표시하려면 **사용자와의 상호 작용** 블록에서 **간략한 인터페이스 표시** 확인란을 선택합니다.

웹 콘솔 및 Cloud Console에서 애플리케이션 인터페이스 표시 모드를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **사용자 상호 작용**으로 갑니다.

5. **사용자에 대한 표시 여부** 블록에서 애플리케이션 인터페이스가 표시되는 방법을 구성합니다.

   - **애플리케이션 아이콘 표시**. 클라이언트 컴퓨터의 알림 영역에는 애플리케이션 아이콘이 있습니다. 아이콘의 마우스 오른쪽 메뉴에서 사용자는 Kaspersky Endpoint Security로 작업을 수행할 수 있습니다. Kaspersky Endpoint Security에서도 애플리케이션 아이콘 위에 알림을 표시합니다.

   - **사용자를 위한 애플리케이션 인터페이스 표시 안 함**. 클라이언트 컴퓨터에서 Kaspersky Endpoint Security의 메인 창에 접근할 수 없으며 알림 영역의 아이콘만 사용할 수 있습니다. 아이콘의 마우스 오른쪽 메뉴에서 사용자는 Kaspersky Endpoint Security로 제한된 수의 작업을 수행할 수 있습니다. Kaspersky Endpoint Security에서도 애플리케이션 아이콘 위에 알림을 표시합니다.

6. 변경 사항을 저장합니다.

애플리케이션 사용 준비

클라이언트 컴퓨터에 애플리케이션을 배포한 후 Kaspersky Security Center 웹 콘솔에서 Kaspersky Endpoint Security를 사용하려면 다음 작업을 수행해야 합니다.

- 정책을 생성하고 구성합니다.

  정책을 사용하여 관리 그룹 내의 모든 클라이언트 컴퓨터에 동일한 Kaspersky Endpoint Security 설정을 적용할 수 있습니다. Kaspersky Security Center의 빠른 시작 마법사에서는 Kaspersky Endpoint Security용 정책을 자동으로 생성합니다.

- *데이터베이스 및 애플리케이션 모듈 업데이트* 및 *악성 코드 검사* 작업을 생성합니다.

  컴퓨터 보안을 최신 상태로 유지하려면 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 필요합니다. 이 작업을 수행하면 Kaspersky Endpoint Security가 안티 바이러스 데이터베이스와 애플리케이션 모듈을 업데이트합니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

  바이러스와 기타 악성 코드를 적시에 탐지하려면 *악성 코드 검사* 작업이 필요합니다. *악성 코드 검사* 작업을 직접 만들어야 합니다.

  관리 콘솔(MMC)에서 악성 코드 검사 작업을 만드는 방법

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

     작업 목록이 열립니다.

  2. **새 작업**을 클릭합니다.

     작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

  1단계. 작업 유형 선택

  Kaspersky Endpoint Security for Windows (14.0) → **악성 코드 검사**를 선택합니다.

2단계. 검사 범위

검사 작업을 수행하는 동안 Kaspersky Endpoint Security가 검사할 개체 목록을 만듭니다.

3단계. Kaspersky Endpoint Security 작업

위협 탐지 시 처리 방법을 선택합니다.

- **치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.
- **치료 - 불가능한 경우 알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 탐지된 모든 감염을 자동으로 치료합니다. 치료 실패 시 Kaspersky Endpoint Security는 탐지된 감염 파일에 대한 정보를 처리 안 된 위협 목록에 추가합니다.
- **알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 감염된 파일에 대한 정보를 해당 파일 탐지 시 처리 안 된 위협 목록에 추가합니다.
- **고급 치료 즉시 실행** 확인란을 선택한 경우 Kaspersky Endpoint Security는 고급 치료 기술을 사용하여 검사 중에 처리 안 된 위협을 치료합니다.

  *고급 치료 기술*은 RAM에서 프로세스를 시작하여 Kaspersky Endpoint Security가 일반적인 방법으로는 제거할 수 없는 악성 애플리케이션을 제거하기 위해 개발되었습니다. 위협은 이 기술로 처리됩니다. 고급 치료 기술을 사용하면 이러한 위협이 처리되며, 고급 치료 절차가 진행 중인 동안에는 새로운 프로세스를 시작하거나 운영 체제 레지스트리를 편집하지 않는 것이 좋습니다. 고급 치료 기술은 상당한 운영 체제 리소스를 사용하므로 다른 애플리케이션의 속도가 떨어질 수 있습니다. 고급 치료가 완료된 후, Kaspersky Endpoint Security는 사용자에게 확인을 요청하지 않고 컴퓨터를 다시 시작합니다.
- **컴퓨터가 유휴 상태일 때만 실행**. 컴퓨터 리소스가 사용 중일 때 작업 시작을 연기했습니다. Kaspersky Endpoint Security는 컴퓨터가 잠겨 있거나 화면 보호기가 켜져 있을 때 검사 작업을 시작합니다. 예를 들어 컴퓨터를 잠금 해제하는 등으로 작업 실행이 중단되면 Kaspersky Endpoint Security는 자동으로 중단된 지점부터 작업을 실행합니다. 이 예약 옵션을 사용하면 컴퓨터를 사용할 때 컴퓨터 리소스를 절약할 수 있습니다.

4단계. 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.

5단계. 작업을 실행할 계정 선택

악성 코드 검사 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다. 검사 범위에 네트워크 드라이브 또는 접근이 제한된 다른 개체가 포함된 경우 충분한 접근 권한이 있는 사용자 계정을 선택합니다.

6 단계. 작업 시작 스케줄 구성

예를 들어 안티 바이러스 데이터베이스를 저장소에 다운로드 한 후 또는 직접 작업 시작 스케줄을 구성합니다.

7단계. 작업 이름 정의

작업 이름을 입력합니다(예: *매일 전체 검사*).

8단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다. 이렇게 하면 지정한 스케줄에 따라 사용자 컴퓨터에서 악성 코드 검사 작업이 실행됩니다.

웹 콘솔에서 악성 코드 검사 작업을 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **악성 코드 검사**를 선택합니다.
   c. **작업 이름** 필드에 *주별 검사* 등의 간단한 설명을 입력합니다.
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.
5. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.
6. 마법사를 끝냅니다.
   작업 목록에 새 작업이 표시됩니다.

7. 작업 스케줄을 구성하려면 작업 속성으로 이동합니다.
   최소 일주일에 한 번은 작업 실행을 스케줄하는 것이 좋습니다.

8. 작업 옆의 확인란을 선택합니다.

9. **시작**을 클릭합니다.
   작업 상태와 작업이 정상적으로 완료되었거나 완료 시 오류가 발생한 장치의 수를 감시할 수 있습니다.

이렇게 하면 지정한 스케줄에 따라 사용자 컴퓨터에서 악성 코드 검사 작업이 실행됩니다.

- Kaspersky Endpoint Security 성능을 최적화합니다.

정책 관리

*정책*은 관리 그룹에 정의된 애플리케이션 설정의 모음입니다. 애플리케이션 하나에 대해 각기 다른 값을 사용해 여러 정책을 구성할 수 있습니다. 애플리케이션은 각 관리 그룹에 대해 다른 설정으로 실행할 수 있습니다. 각 관리 그룹에는 고유한 애플리케이션 정책이 있을 수 있습니다.

각 정책 설정에는 ('자물쇠') 속성이 있습니다. 이 속성의 상태에 따라 설정이 관리 그룹의 관리 중인 장치로 전달되는지 여부가 결정됩니다.

- '자물쇠'가 열려 있는 경우( ), 이 설정의 값은 관리 중인 장치로 전달되지 않습니다. 애플리케이션의 로컬 인터페이스에서 설정을 수정할 수 있습니다. 이러한 설정을 *잠금 해제*라고 합니다.

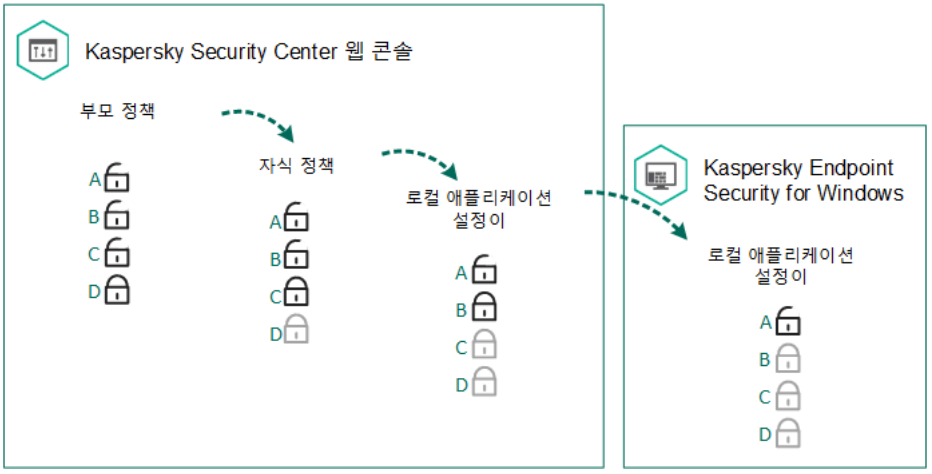
- '자물쇠'가 잠겨 있는 경우( ), 이 설정의 값은 전달되어 관리 중인 장치에 적용됩니다. 이러한 설정을 *잠금*이라고 합니다. 애플리케이션의 로컬 인터페이스에서는 차단된 설정을 수정할 수 없습니다.

동기화 중에 네트워크 에이전트가 클라이언트 컴퓨터로 정책 설정을 전송합니다. 기본적으로 중앙 관리 서버는 정책 설정이 변경된 직후에 동기화를 수행합니다. 클라이언트 컴퓨터의 UDP 포트 15000이 동기화에 사용됩니다. 중앙 관리 서버는 기본적으로 15분마다 동기화를 수행합니다. 정책 설정이 변경된 후 동기화가 실패하면 구성된 스케줄에 따라 다음 동기화 시도가 수행됩니다.

설정 상속

관리 그룹과 같은 정책은 계층 구조로 배열됩니다. *자식 정책*은 중첩된 계층 구조 레벨의 정책(중첩된 관리 그룹과 보조 중앙 관리 서버에 대한 정책)입니다.

기본적으로 자식 정책은 부모 정책의 설정을 상속합니다. 부모 정책의 설정에 (잠긴 '자물쇠') 속성이 지정되면 자식 정책 및 로컬 애플리케이션 설정에서 부모 정책에 따라 해당 설정의 값이 재정의되고 설정이 잠깁니다. 필요할 경우 부모 정책에서 설정의 상속을 비활성화할 수 있습니다. 이동 사용자 정책은 관리 그룹 계층 구조를 통해 다른 정책에 영향을 주지 않습니다.



설정 상속

정책 설정(읽기, 쓰기, 실행)에 접근할 수 있는 권한은 Kaspersky Endpoint Security 기능 범위 및 Kaspersky Security Center 중앙 관리 서버에 접근할 수 있는 개별 사용자를 위해 지정됩니다. 정책 설정에 대한 접근 권한을 구성하려면 Kaspersky Security Center 중앙 관리 서버 속성 창의 **보안** 섹션으로 이동합니다(기본적으로 이 섹션은 콘솔 인터페이스에서 숨겨져 있음).

정책 수정

Kaspersky Security Center 정책 수정 사항을 추적하고 수정본을 생성합니다. *수정본*은 사용자가 저장한 수정된 파라미터 값의 집합입니다. 수정본을 사용하면 정책 파라미터의 변경 사항을 비교하고 되돌릴 수 있습니다. 수정본에는 수정된 파라미터 집합 외에도 변경을 수행한 사용자에 대한 정보와 변경 시간, IP 주소, 사용자 설명 및 기타 관련 데이터가 포함됩니다.

수정 로그를 확인하려면 정책 속성을 열고 **수정 기록** 섹션으로 이동하십시오. 수정 처리에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

정책 만들기

정책을 생성할 때 마법사는 선택한 모드와 관련된 설정을 제안합니다. 예를 들어 Light Agent 모드의 경우 보호 서버(SVM)를 추가해야 합니다. 애플리케이션을 사용하여 SQL 서버를 보호할 때 서버 동작에 방해가 되지 않도록 사전 정의된 검사 예외를 추가해야 합니다. 마법사는 모드 선택 후 관련 정책 설정을 제안합니다. 그런 다음 정책 속성에서 이러한 설정을 편집할 수 있습니다.

관리 콘솔(MMC)에서 정책을 만드는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 선택합니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.

4. **새 정책**을 클릭합니다.
   정책 마법사가 시작됩니다.

5. 정책 마법사의 안내를 따릅니다.

1단계. 그룹 정책을 생성할 애플리케이션 선택

Kaspersky Endpoint Security for Windows (14.0) 애플리케이션을 선택합니다.

2단계. 그룹 정책 이름 지정

그룹 정책의 이름을 입력합니다(예: *오피스 정책*).

정책 마법사를 사용하여 기존 정책을 기반으로 새로운 정책을 만들 수도 있습니다. 그렇게 하려면 그룹 정책 이름을 지정할 때 **이전 애플리케이션 버전에 대한 정책 설정 사용(U)** 확인란을 선택합니다. 마법사를 사용하면 Kaspersky Endpoint Security(KES) 정책을 Kaspersky Security for Windows Server(KSWS) 또는 Kaspersky Security for Virtualization Light Agent for Windows와 같은 다른 솔루션의 정책을 기반으로 만들 수도 있습니다.

3단계. Kaspersky Security Network 참여

Kaspersky Security Network(KSN) 진술문 약관을 읽고 동의해 주십시오.

4단계. 컴퓨터의 애플리케이션 사용 모드 선택

Kaspersky Endpoint Security의 용도에 따라 다음 애플리케이션 모드에 대한 정책을 구성할 수 있습니다.

- 호스트를 보호하는 표준 모드
  이 모드에서는 정책 구성 방법을 선택할 수 있습니다.

  - **기본 설정으로 정책 생성**. 기본 설정은 최적의 설정을 사용합니다. Kaspersky 전문가가 권장하는 설정입니다. 기본 설정은 권장 보호 수준과 최적의 리소스 사용을 제공합니다.

  - **마법사를 사용해 정책 설정 변경**. 이 방법으로 마법사를 사용하여 정책 설정을 단계별로 관리할 수 있습니다. 애플리케이션의 구성 파일을 사용하여 정책 설정을 관리할 수도 있습니다(다음 단계 참조).

- 지능형 위협 및 표적형 공격으로부터 보호하는 Endpoint Detection and Response Agent.
  *Endpoint Detection and Response Agent*는 조직의 IT 인프라에 있는 개별 워크스테이션 및 서버에 설치되어 Kaspersky의 Detection and Response 솔루션을 지원하는 애플리케이션입니다. 다음 단계에서 EDR Agent 통합을 위한 솔루션을 선택해야 합니다.

- 가상 환경을 보호하는 Light Agent.
  Light Agent 모드에서 애플리케이션을 사용하려면 SVM 가상 컴퓨터와 연결을 구성해야 합니다. 애플리케이션이 Light Agent 모드에서 작동하려면 이러한 설정이 필요합니다.

Kaspersky Endpoint Security는 모든 애플리케이션 모드와 OS 유형에 대한 공통 정책을 제공합니다. 즉, 정책이 전체 설정에 적용됩니다. 그러나 Kaspersky Endpoint Security는 일부 기능을 사용할 수 없는 모드로 배포되기 때문에 애플리케이션이 일부 정책 설정을 무시할 수 있습니다. 예를 들어 Endpoint Detection and Response Agent 모드에서 애플리케이션을 사용하는 경우, Kaspersky Detection and Response 솔루션과의 통합 및 KUMA와의 통합과 관련된 설정만 사용할 수 있습니다.

모드 및 운영 체제 유형에 따라 다른 정책을 사용하는 것이 좋습니다.

5단계. 설정 가져오는

이 단계는 4단계에서 수동 정책 구성을 선택한 경우에 수행할 수 있습니다.

CFG 구성 파일에서 Kaspersky Endpoint Security 설정을 기반으로 정책을 생성할 수 있습니다. 애플리케이션 구성 파일을 가져올 때 마법사에서 모든 정책 설정을 사용할 수 있는 것은 아닙니다. 예를 들어 애플리케이션 설정에서 정책 프로필이 누락될 수 있습니다. 모든 설정과 프로필을 정책으로 전송하려면 KLP 파일에서 다른 정책 가져오기를 수행할 수 있습니다.

구성 파일을 가져올 때 Kaspersky Endpoint Security는 암호화 컨테이너의 암호를 전송하지 않습니다. 서버에 연결할 때 양방향 인증을 사용하는 경우 암호화 컨테이너의 암호를 처음부터 지정해야 합니다.

6단계 – 10단계. 정책 설정 구성

이 단계는 4단계에서 수동 정책 구성을 선택한 경우에 수행할 수 있습니다.

다음 단계에 따라 정책 설정을 관리합니다.

11 단계. 신뢰 구역 구성

신뢰 영역을 구성합니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 추가할 수 있습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션도 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security in Light Agent 모드를 빠르게 구성하는 데 도움이 될 수 있습니다.

12 단계. 정책 상태 선택

- **활성**. 다음 동기화 이후 정책이 컴퓨터에서 활성 정책으로 사용됩니다.

  활성 정책의 설정은 동기화 중에 클라이언트 컴퓨터에 저장됩니다. 여러 정책을 컴퓨터 한 대에 동시에 적용할 수는 없으므로 각 그룹에서는 정책 하나만 활성 상태일 수 있습니다.

- **비활성**. 백업 정책입니다. 필요시 비활성 정책을 활성 상태로 전환할 수 있습니다.

  비활성 정책은 수에 제한 없이 생성할 수 있습니다. 비활성 정책은 네트워크에 있는 컴퓨터의 애플리케이션 설정에 영향을 주지 않습니다. 비활성 정책은 바이러스 공격과 같은 비상 상황을 준비하기 위한 것입니다. 플래시 드라이브를 통한 공격이 진행되면 플래시 드라이브 접근을 차단하는 정책을 활성화할 수 있습니다. 이 경우 활성 상태였던 정책은 자동으로 비활성화됩니다.

- **이동 사용자**. 컴퓨터가 조직 네트워크 외부로 이동하면 이 정책이 활성화됩니다.

마법사를 끝냅니다.

웹 콘솔 및 Cloud Console에서 정책을 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. **추가**를 클릭합니다.

   정책 마법사가 시작됩니다.
3. Kaspersky Endpoint Security를 선택하고 **다음**을 누릅니다.
4. Kaspersky Security Network(KSN) 진술문 약관을 확인하고 동의한 후에 **다음**을 누릅니다.
5. 애플리케이션 모드를 선택합니다:

   - 워크스테이션과 서버를 보호하는 표준 모드
   - 지능형 위협 및 표적형 공격으로부터 보호하는 Endpoint Detection and Response Agent.

     이 모드를 선택하면 컴퓨터를 Kaspersky Detection and Response 솔루션과 통합하는 정책을 만들 수 있습니다. 마법사가 Kaspersky Managed Detection and Response와 Kaspersky Anti Targeted Attack Platform (EDR)에 대한 통합을 구성하라는 메시지를 표시합니다.
   - 가상 환경을 보호하는 Light Agent.

     이 모드를 선택하면 다음 단계에서 보호 서버(SVM)에 대한 연결을 구성해야 합니다. 애플리케이션이 Light Agent 모드에서 작동하려면 이러한 설정이 필요합니다.

   Kaspersky Endpoint Security는 모든 애플리케이션 모드와 OS 유형에 대한 공통 정책을 제공합니다. 즉, 정책이 전체 설정에 적용됩니다. 그러나 Kaspersky Endpoint Security는 일부 기능을 사용할 수 없는 모드로 배포되기 때문에 애플리케이션이 일부 정책 설정을 무시할 수 있습니다. 예를 들어 Endpoint Detection and Response Agent 모드에서 애플리케이션을 사용하는 경우, Kaspersky Detection and Response 솔루션과의 통합 및 KUMA와의 통합과 관련된 설정만 사용할 수 있습니다.

   > 모드 및 운영 체제 유형에 따라 다른 정책을 사용하는 것이 좋습니다.

6. 신뢰 영역을 구성합니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 추가할 수 있습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션도 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security in Light Agent 모드를 빠르게 구성하는 데 도움이 될 수 있습니다.

7. **일반** 탭에서는 다음 처리를 수행할 수 있습니다.

   - 정책 이름을 변경합니다.
   - 정책 상태를 선택합니다:
     - **활성**. 다음 동기화 이후 정책이 컴퓨터에서 활성 정책으로 사용됩니다.

       활성 정책의 설정은 동기화 중에 클라이언트 컴퓨터에 저장됩니다. 여러 정책을 컴퓨터 한 대에 동시에 적용할 수는 없으므로 각 그룹에서는 정책 하나만 활성 상태일 수 있습니다.

     - **비활성**. 백업 정책입니다. 필요시 비활성 정책을 활성 상태로 전환할 수 있습니다.

       비활성 정책은 수에 제한 없이 생성할 수 있습니다. 비활성 정책은 네트워크에 있는 컴퓨터의 애플리케이션 설정에 영향을 주지 않습니다. 비활성 정책은 바이러스 공격과 같은 비상 상황을 준비하기 위한 것입니다. 플래시 드라이브를 통한 공격이 진행되면 플래시 드라이브 접근을 차단하는 정책을 활성화할 수 있습니다. 이 경우 활성 상태였던 정책은 자동으로 비활성화됩니다.

     - **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. 자식 정책의 속성에서 **상위 정책의 설정 상속** 토글 버튼이 자동으로 켜지고 이를 끌 수 없습니다. 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 Kaspersky Endpoint Security 정책 설정을 구성할 수 있습니다.

9. 마법사를 끝냅니다.

그러면 다음 동기화 중에 클라이언트 컴퓨터에서 Kaspersky Endpoint Security 설정이 구성됩니다. 메인 화면에서 버튼을 클릭하여 Kaspersky Endpoint Security 인터페이스에서 컴퓨터에 적용되는 정책에 대한 정보를 볼 수 있습니다(예: 정책 이름). 그렇게 하려면 네트워크 에이전트 정책 설정에서 확장 정책 데이터 수신을 활성화해야 합니다. 네트워크 에이전트 정책에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

정책 내보내기 및 가져오기

Kaspersky Endpoint Security는 설정 및 프로필이 포함된 정책을 KLP 파일로 내보낼 수 있습니다. 그런 다음 정책 내보내기/가져오기 기능을 사용하여 정책을 백업하거나, 정책을 다른 서버로 마이그레이션합니다. 예를 들어 Kaspersky Security Center Windows에서 Kaspersky Security Center Linux로 정책을 마이그레이션할 수 있습니다. 정책 관리에 관한 자세한 정보는 Kaspersky Security Center 도움말을 참조하십시오.

관리 콘솔(MMC)에서 정책을 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 정책을 내보내기:
   a. 내보낼 정책을 클릭합니다.
   b. 창 오른쪽의 **정책을 파일로 내보내기** 링크를 클릭합니다.
   c. 창이 열리면 정책을 내보낼 KLP 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   d. 파일을 저장합니다.
5. 정책을 가져오기:
   a. **미리 만든 파일에서 정책 가져오기**를 클릭합니다.
   b. 창이 열리면 가져올 KLP 정책을 선택합니다.
   c. 파일을 엽니다.

   새 정책이 *비활성 정책* 상태로 추가됩니다.

웹 콘솔 및 Cloud Console에서 정책을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. 정책을 내보내기:
   a. 편집하려는 정책 옆의 확인란을 선택합니다.
   b. **내보내기** 버튼을 클릭합니다.
   c. 창이 열리면 정책을 내보낼 KLP 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   d. 파일을 저장합니다.
3. 정책을 가져오기:
   a. **가져오기**를 클릭합니다.
   b. 가져올 KLP 정책 파일을 선택합니다.
   c. 정책이 성공적으로 처리되면 정책을 적용할 관리 그룹을 선택합니다.
   d. **완료** 버튼을 클릭해 작업 생성을 완료합니다.

   새 정책이 *비활성* 상태로 추가됩니다.

보안 레벨 표시기

보안 레벨 표시기는 정책 속성 창의 상단에 표시됩니다. 표시기는 다음 값 중 하나를 사용할 수 있습니다:

- **높은 보호 레벨**. 디음 카테고리의 모든 구성 요소가 활성화된 경우 표시기는 이 값을 사용하고 초록색으로 바뀝니다:
  - **심각**. 이 카테고리에는 다음 구성 요소가 포함됩니다:
    - 파일 위협 보호
    - 행동 탐지
    - 익스플로잇 방지
    - 복원 엔진
    - 외부 관리로부터 애플리케이션 서비스 보호
  - **중요** 이 카테고리에는 다음 구성 요소가 포함됩니다:
    - Kaspersky Security Network
    - 웹 위협 보호
    - 메일 위협 보호
    - 호스트 침입 방지
    - 암호 보호
- **중간 보호 레벨**. 중요 구성 요소가 비활성된 경우 표시기는 이 값을 사용하고 노란색으로 바뀝니다.
- **낮은 보호 레벨**. 다음 경우 중 하나에 해당될 경우 표시기는 이 값을 사용하고 빨간색으로 바뀝니다:
  - 하나 이상의 중요 구성 요소가 비활성화됩니다.
  - 둘 이상의 중요 구성 요소가 비활성화됩니다.

표시기가 **중간 보호 레벨** 또는 **낮은 보호 레벨** 값을 갖는 경우 **권장하는 보호 구성 요소** 창을 여는 링크가 표시기 오른쪽에 나타납니다. 이 창에서 권장하는 보호 구성 요소를 활성화할 수 있습니다.

애플리케이션을 업그레이드한 후, 보호 레벨 표시기가 업그레이드 전보다 낮은 보호 레벨을 표시할 수 있습니다. 이는 컴퓨터 보안에 중요한 새로운 구성 요소 또는 기능이 애플리케이션의 최신 버전에 추가되었기 때문입니다. 애플리케이션을 업그레이드한 후, 높은 보호 레벨을 유지하도록 새 설정을 관리해야 합니다.



정책의 보안 레벨 표시기

작업 관리

다음과 같은 유형의 작업을 만들어 Kaspersky Security Center를 통해 Kaspersky Endpoint Security를 관리할 수 있습니다:

- 개별 클라이언트 컴퓨터에 대해 구성된 로컬 작업.
- 관리 그룹 내에 있는 클라이언트 컴퓨터에 대해 구성된 그룹 작업.
- 컴퓨터 조회를 위한 작업.

그룹 작업, 컴퓨터 조회를 위한 작업 또는 로컬 작업을 원하는 수만큼 생성할 수 있습니다. 관리 그룹, 컴퓨터 조회 작업과 관련한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Endpoint Security는 다음 작업을 지원합니다:

- **악성 코드 검사**. Kaspersky Endpoint Security는 바이러스 및 기타 위협에 대한 설정에 지정된 컴퓨터 영역을 검사합니다. Kaspersky Endpoint Security의 동작에 필요한 *악성 코드 검사* 작업은 빠른 시작 마법사를 실행하는 동안 생성됩니다. 최소 일주일에 한 번은 작업 실행을 스케줄하는 것이 좋습니다.
- **키 추가**. Kaspersky Endpoint Security는 애플리케이션 활성화를 위한 키(추가 키 포함)를 추가합니다. 작업을 실행하기 전에 해당 작업을 실행할 컴퓨터 수가 라이센스에서 허용되는 컴퓨터 수를 초과하지 않는지 확인하십시오.
- **애플리케이션 구성 요소 변경**. Kaspersky Endpoint Security는 작업 설정에 지정된 구성 요소 목록에 따라 클라이언트 컴퓨터에서 구성 요소를 설치 또는 제거합니다. 파일 위협 보호 구성 요소는 제거할 수 없습니다. Kaspersky Endpoint Security 구성 요소의 최적 집합을 사용하면 컴퓨터 리소스를 절약할 수 있습니다.

- **인벤토리**. Kaspersky Endpoint Security는 컴퓨터에 저장된 모든 애플리케이션 실행 파일에 대한 정보를 수신합니다. 애플리케이션 제어 구성 요소가 *인벤토리* 작업을 수행합니다. 애플리케이션 제어 구성 요소가 설치되어 있지 않으면 작업이 종료되며 오류가 발생합니다.

- **데이터베이스 및 애플리케이션 모듈 업데이트**. Kaspersky Endpoint Security는 데이터베이스 및 애플리케이션 모듈을 업데이트합니다. Kaspersky Endpoint Security의 동작에 필요한 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업은 빠른 시작 마법사를 실행하는 동안 생성됩니다. 매일 1회 이상 작업을 실행하는 스케줄을 구성하는 것이 좋습니다.

- **데이터 완전 삭제**. Kaspersky Endpoint Security는 Kaspersky Security Center에 오랫동안 연결되지 않는 경우 사용자의 컴퓨터에서 파일과 폴더를 즉시 삭제합니다.

- **업데이트 롤백**. Kaspersky Endpoint Security는 데이터베이스 및 애플리케이션 모듈의 마지막 업데이트를 롤백합니다. 예를 들어 Kaspersky Endpoint Security가 안전한 애플리케이션을 차단하도록 할 수 있는 잘못된 데이터가 새 데이터베이스에 포함되어 있는 경우 업데이트를 롤백해야 할 수 있습니다.

- **애플리케이션 무결성 검사**. Kaspersky Endpoint Security는 애플리케이션 파일을 분석하고, 파일의 손상 및 변경 여부를 확인하고, 애플리케이션 파일의 디지털 서명을 확인합니다.

- **인증 에이전트 계정 관리**. Kaspersky Endpoint Security는 인증 에이전트 계정 설정을 구성합니다. 암호화된 드라이브를 사용하려면 인증 에이전트가 필요합니다. 운영 체제가 로드되기 전에 사용자는 에이전트 인증을 완료해야 합니다.

애플리케이션이 Kaspersky의 Endpoint Detection and Response 솔루션의 일부로 작동하는 경우 탐지 대응 동작(responses)으로 추가 작업을 실행할 수 있습니다. 예를 들어 *프로세스 종료* 작업을 사용해 프로세스를 원격으로 종료할 수 있습니다.

> 작업은 Kaspersky Endpoint Security가 실행 중인 경우에만 컴퓨터에서 실행됩니다.

작업 생성

관리 콘솔(MMC)에서 작업을 만드는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **작업** 폴더를 선택합니다.
3. **새 작업**을 클릭합니다.
   작업 마법사가 시작됩니다.
4. 작업 마법사의 안내를 따릅니다.

웹 콘솔 및 Cloud Console에서 작업을 생성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 사용자 컴퓨터에서 실행할 작업을 선택합니다.

   c. **작업 이름** 필드에 간단한 설명을 입력합니다.

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

4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.

5. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.

6. 마법사를 끝냅니다.

작업 목록에 새 작업이 표시됩니다. 이 작업에는 기본 설정이 적용됩니다. 작업 설정을 구성하려면 작업 속성으로 이동합니다. 작업을 실행하려면 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다. 작업이 시작된 후 작업을 일시 중지했다가 나중에 다시 시작할 수 있습니다.

작업 목록에서 작업 결과를 모니터링할 수 있습니다. 여기에는 컴퓨터의 작업 성능에 대한 통계와 작업 상태가 포함됩니다. 작업 완료를 모니터할 이벤트 조회를 생성할 수도 있습니다(**모니터링 → 이벤트 선택**). 이벤트 선택에 대한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오. 작업 실행 결과는 Windows 이벤트 로그와 Kaspersky Endpoint Security 리포트에 로컬로도 저장됩니다.

작업 접근 관리

Kaspersky Endpoint Security 작업(읽기, 쓰기, 실행)에 접근할 수 있는 권한은 Kaspersky Endpoint Security 기능 영역으로의 접근 설정을 통해 Kaspersky Security Center 중앙 관리 서버에 접근할 수 있는 개별 사용자를 위해 정의됩니다. Kaspersky Endpoint Security의 기능 영역으로의 접근 권한을 구성하려면, Kaspersky Security Center 중앙 관리 서버의 속성 창의 **보안** 섹션으로 이동합니다. Kaspersky Security Center를 통해 작업을 관리하는 방법에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

정책(*작업 관리 모드*)을 사용하여 작업에 접근할 수 있는 사용자 권한을 구성할 수 있습니다. 예를 들어 Kaspersky Endpoint Security 인터페이스에서 그룹 작업을 숨길 수 있습니다.

관리 콘솔(MMC)을 통해 Kaspersky Endpoint Security 인터페이스에서 작업 관리 모드를 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 작업 → 작업 관리**를 선택합니다.

4. 작업 관리 모드를 구성합니다(아래 표 참조).

5. 변경 사항을 저장합니다.

웹 콘솔을 통해 Kaspersky Endpoint Security 인터페이스에서 작업 관리 모드를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **사용자 상호 작용**으로 갑니다.
5. **허용되는 작업**에서 작업 관리 모드를 구성합니다(아래 표 참조).
6. 변경 사항을 저장합니다.

작업 관리 설정

파라미터	설명
로컬 작업에 접근	이 확인란을 선택한 경우 로컬 작업이 Kaspersky Endpoint Security 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 Endpoint Security 로컬 인터페이스에서 아니면 명령줄에서 작업할 때 작업을 시작하거나 구성할 수 없습니다. 사용자는 파일 또는 폴더의 마우스 오른쪽 메뉴에서 **바이러스 검사** 옵션을 선택하여 파일 또는 폴더의 검사를 시작할 수는 있습니다. 사용자 지정 검사 작업의 경우 기본 설정 값을 사용한 검사 작업이 시작됩니다.
그룹 작업 보기	이 확인란을 선택하면 그룹 작업이 Kaspersky Endpoint Security 로컬 인터페이스에 표시됩니다. 사용자는 애플리케이션 인터페이스에서 모든 작업 목록을 볼 수 있습니다. 이 확인란을 선택 해제하면, Kaspersky Endpoint Security는 빈 작업 목록을 표시합니다.
그룹 작업 관리	이 확인란을 선택하면 사용자는 Kaspersky Security Center 콘솔에 지정된 그룹 작업을 시작 및 중지할 수 있습니다. 사용자는 애플리케이션 인터페이스 또는 간략한 애플리케이션 인터페이스에서 작업을 시작 및 중지할 수 있습니다. 이 확인란을 선택 해제하면 Kaspersky Endpoint Security가 예약된 작업을 자동으로 시작하거나 관리자가 Kaspersky Security Center 콘솔에서 직접 작업을 시작합니다.

로컬 애플리케이션 설정 구성

Kaspersky Security Center에서 특정 컴퓨터의 Kaspersky Endpoint Security 설정을 구성할 수 있습니다. 이러한 설정은 *로컬 애플리케이션 설정*입니다. 일부 설정은 편집할 수 없을 수 있습니다. 이러한 설정은 정책 속성에서 속성에 의해 차단됩니다.

관리 콘솔(MMC)에서 로컬 애플리케이션 설정을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **기기** 탭을 선택합니다.
4. 더블 클릭해 컴퓨터 속성 창을 엽니다.
5. 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.
6. 컴퓨터에 설치된 Kaspersky 애플리케이션 목록에서 **Kaspersky Endpoint Security for Windows (14.0)**를 선택하고 더블 클릭하여 애플리케이션 속성을 엽니다.

7. **일반 설정** 섹션에서 Kaspersky Endpoint Security와 리포트 및 저장소를 구성합니다.

   애플리케이션 속성 창의 나머지 섹션은 Kaspersky Security Center의 표준입니다. 이러한 섹션에 대한 설명은 Kaspersky Security Center 도움말에 나와 있습니다.

   > 애플리케이션에 특정 설정의 변경을 금지하는 정책이 적용된다면 **일반 설정** 섹션에서 해당 설정을 편집하거나 구성하지 못합니다.

8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 로컬 애플리케이션 설정을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)**를 선택합니다.
2. 로컬 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.

   그러면 컴퓨터 속성이 열립니다.
3. **애플리케이션** 탭을 선택합니다.
4. **Kaspersky Endpoint Security for Windows**를 누릅니다.

   그러면 로컬 애플리케이션 설정이 열립니다.
5. **애플리케이션 설정** 탭을 선택합니다.
6. 로컬 애플리케이션 설정을 구성합니다.
7. 변경 사항을 저장합니다.

암호화 설정을 제외한 로컬 애플리케이션 설정은 정책 설정과 동일합니다.

Kaspersky Endpoint Security 시작 및 중지

사용자 컴퓨터에 Kaspersky Endpoint Security를 설치하고 나면 애플리케이션이 자동으로 시작됩니다. 기본적으로는 운영 체제를 시작하고 나면 Kaspersky Endpoint Security가 자동으로 시작됩니다. 운영 체제 설정에서 애플리케이션의 자동 시작을 구성할 수 없습니다.

> 운영 체제가 시작된 후 Kaspersky Endpoint Security 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 Endpoint Security가 시작될 때 안티 바이러스 데이터베이스를 다운로드하더라도 컴퓨터 보호 레벨이 낮아지지 않습니다.

관리 콘솔(MMC)에서 Kaspersky Endpoint Security 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 **일반 설정** → **애플리케이션 설정**을 차례로 선택합니다.

4. **컴퓨터 시작 시 애플리케이션 시작(권장)** 확인란을 사용하여 애플리케이션 시작을 구성합니다.

5. 변경 사항을 저장합니다.

웹 콘솔에서 Kaspersky Endpoint Security 시작을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **사용자 상호 작용**으로 갑니다.

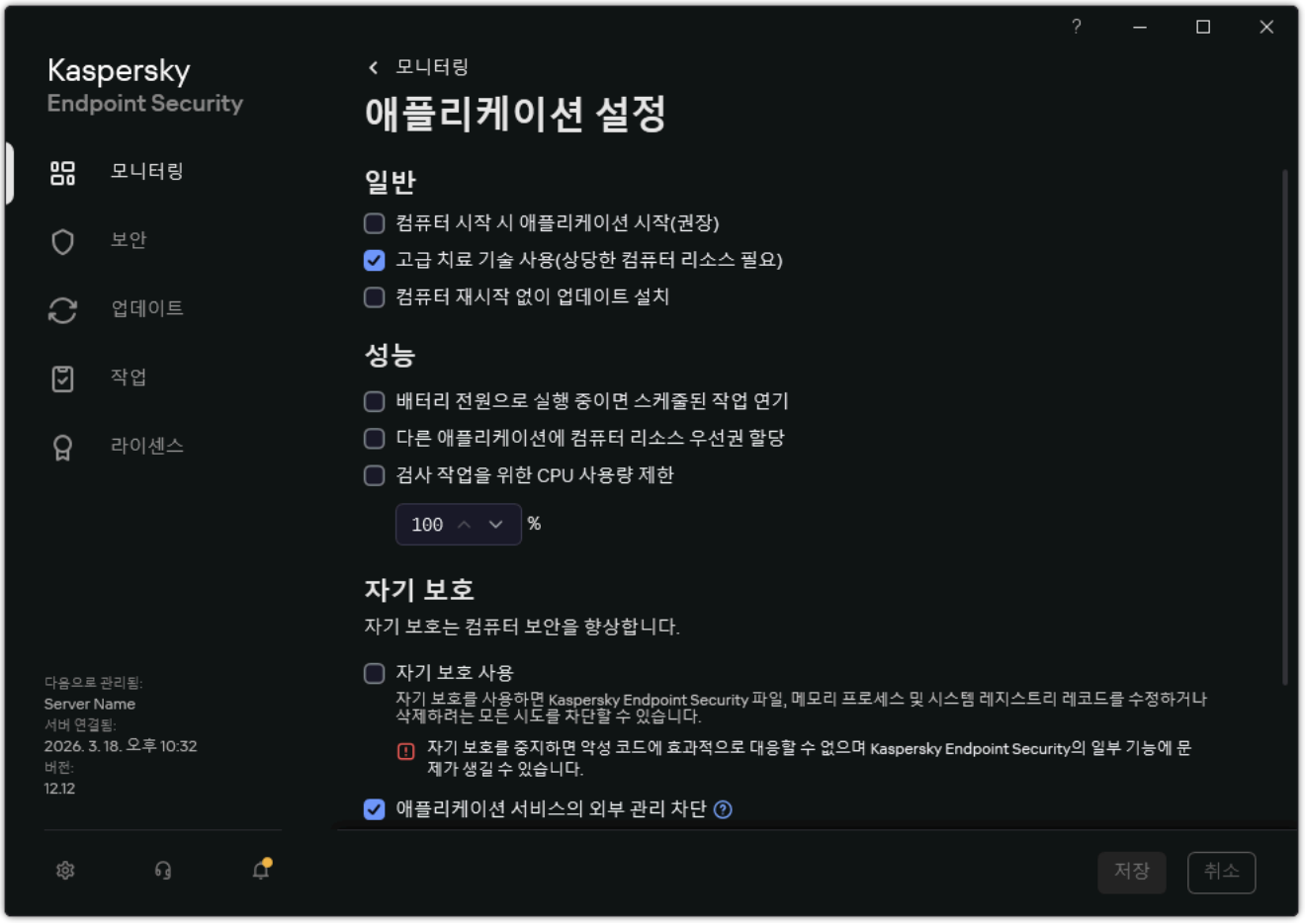
5. **컴퓨터 시작 시 Kaspersky Endpoint Security 시작(권장)** 확인란을 사용하여 애플리케이션 시작을 구성합니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 Kaspersky Endpoint Security 시작을 구성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **일반 설정** → **애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

3. **컴퓨터 시작 시 애플리케이션 시작(권장)** 확인란을 사용하여 애플리케이션 시작을 구성합니다.

4. 변경 사항을 저장합니다.

Kaspersky 전문가는 컴퓨터와 개인 데이터가 위협에 노출될 수 있으므로 Kaspersky Endpoint Security를 직접 중지하는 것을 권장하지 않습니다. 필요시에는 애플리케이션을 중지하지 않고 원하는 기간 동안 컴퓨터 보호를 일시 중지할 수 있습니다.

보호 상태 위젯을 사용하여 애플리케이션 상태를 모니터링할 수 있습니다.

관리 콘솔(MMC)에서 Kaspersky Endpoint Security를 시작 또는 중지하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.

3. 작업 공간에서 **기기** 탭을 선택합니다.

4. 더블 클릭해 컴퓨터 속성 창을 엽니다.

5. 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.

6. 컴퓨터에 설치된 Kaspersky 애플리케이션 목록에서 **Kaspersky Endpoint Security for Windows (14.0)**를 선택하고 더블 클릭하여 애플리케이션 속성을 엽니다.

7. 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.

웹 콘솔에서 Kaspersky Endpoint Security를 시작 또는 중지하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.

2. Kaspersky Endpoint Security를 시작하거나 중지할 컴퓨터의 이름을 누릅니다.
   컴퓨터 속성 창이 열립니다.

3. **애플리케이션** 탭을 선택합니다.

4. **Kaspersky Endpoint Security for Windows** 옆의 확인란을 선택합니다.

5. **시작** 또는 **중지** 버튼을 누릅니다.

명령줄에서 Kaspersky Endpoint Security를 시작 또는 중지하는 방법

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.

2. klpsm.exe 실행 파일이 있는 폴더로 이동합니다.

3. 명령줄에서 애플리케이션을 시작하려면 `klpsm.exe start_avp_service`를 입력합니다.

4. 명령줄에서 애플리케이션을 중지하려면 `klpsm.exe stop_avp_service`를 입력합니다.

명령줄에서 애플리케이션을 중지하려면 시스템 서비스의 외부 관리를 활성화합니다.



명령줄을 통해 애플리케이션 시작 및 중지

컴퓨터 보호 및 제어 일시 중지 및 다시 시작

컴퓨터 보호 및 제어 일시 중지는 Kaspersky Endpoint Security의 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. 작업 표시줄 알림 영역에 있는 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 눌러 마우스 오른쪽 메뉴를 엽니다.

2. 마우스 오른쪽 메뉴에서 **보호 일시 중지**를 선택합니다(아래 그림 참조).

   이 마우스 오른쪽 메뉴 항목은 암호 보호가 설정된 경우 사용할 수 있습니다.

3. 다음 옵션 중 하나를 선택합니다:

   - **다음 시간 동안 일시 중지: <지정한 시간>** - 아래의 드롭다운 목록에서 지정한 시간이 지나면 컴퓨터 보호 및 제어가 다시 시작됩니다.
   - **애플리케이션이 다시 시작될 때까지 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.

4. **보호 일시 중지**를 클릭합니다.

Kaspersky Endpoint Security는 정책에서 자물쇠(🔒) 표시가 없는 모든 보호 및 제어 구성 요소의 작동을 일시 중지합니다. 이 작업을 수행하기 전에 Kaspersky Security Center 정책을 비활성화하는 것이 좋습니다.



애플리케이션 아이콘 마우스 오른쪽 메뉴

컴퓨터 보호 및 제어를 다시 시작하려면 다음과 같이 하십시오.

1. 작업 표시줄 알림 영역에 있는 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 눌러 마우스 오른쪽 메뉴를 엽니다.
2. 마우스 오른쪽 메뉴에서 **보호 다시 시작**을 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.

구성 파일 만들기 및 사용

Kaspersky Endpoint Security 설정 구성 파일을 사용하면 다음 작업을 수행할 수 있습니다:

- 사전에 지정한 설정을 사용하여 명령줄에서 Kaspersky Endpoint Security 로컬 설치를 수행합니다.
- 사전에 지정한 설정을 사용하여 Kaspersky Security Center를 통해 Kaspersky Endpoint Security 원격 설치를 수행합니다.
- 애플리케이션 설정을 정책으로 전송합니다.
- 한 컴퓨터에서 다른 컴퓨터로 Kaspersky Endpoint Security 설정을 마이그레이션합니다(아래 지침 참조).

구성 파일 내보내기

구성 파일을 생성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **설정 관리**를 선택합니다.
3. **내보내기**를 클릭합니다.
4. 창이 열리면 구성 파일을 저장할 경로를 지정하고 파일 이름을 입력합니다.

   Kaspersky Endpoint Security의 로컬 또는 원격 설치에 구성 파일을 사용하려면 파일의 이름을 install.cfg로 지정해야 합니다.

5. 필요한 경우 애플리케이션 구성을 파일로 내보내기 위한 암호를 입력합니다.

   구성 파일을 저장하려면 암호 보호가 활성화되어야 합니다. 해당 사용자에게 **설정 내보내기** 권한이 있어야 합니다.

6. 파일을 저장합니다.

그러면 애플리케이션이 구성 파일을 생성합니다. 구성 파일에 사용자 계정 세부 정보가 포함될 수 있으므로 Kaspersky Endpoint Security가 파일을 암호화합니다. 구성 파일은 편집할 수 없습니다. 구성 파일을 수정하려고 하면 구성 파일이 손상됩니다.

구성 파일 가져오기

구성 파일에는 애플리케이션에 추가된 사용자 계정의 세부 정보가 포함될 수 있습니다. 파일을 해당 파일이 생성된 컴퓨터에서 가져오는 경우 Kaspersky Endpoint Security는 사용자 계정의 암호를 가져옵니다. 다른 컴퓨터에서 파일을 가져오는 경우 암호를 직접 입력해야 합니다.

구성 파일을 가져올 때 Kaspersky Endpoint Security는 암호화 컨테이너의 암호를 전송하지 않습니다. 서버에 연결할 때 양방향 인증을 사용하는 경우 암호화 컨테이너의 암호를 처음부터 지정해야 합니다.

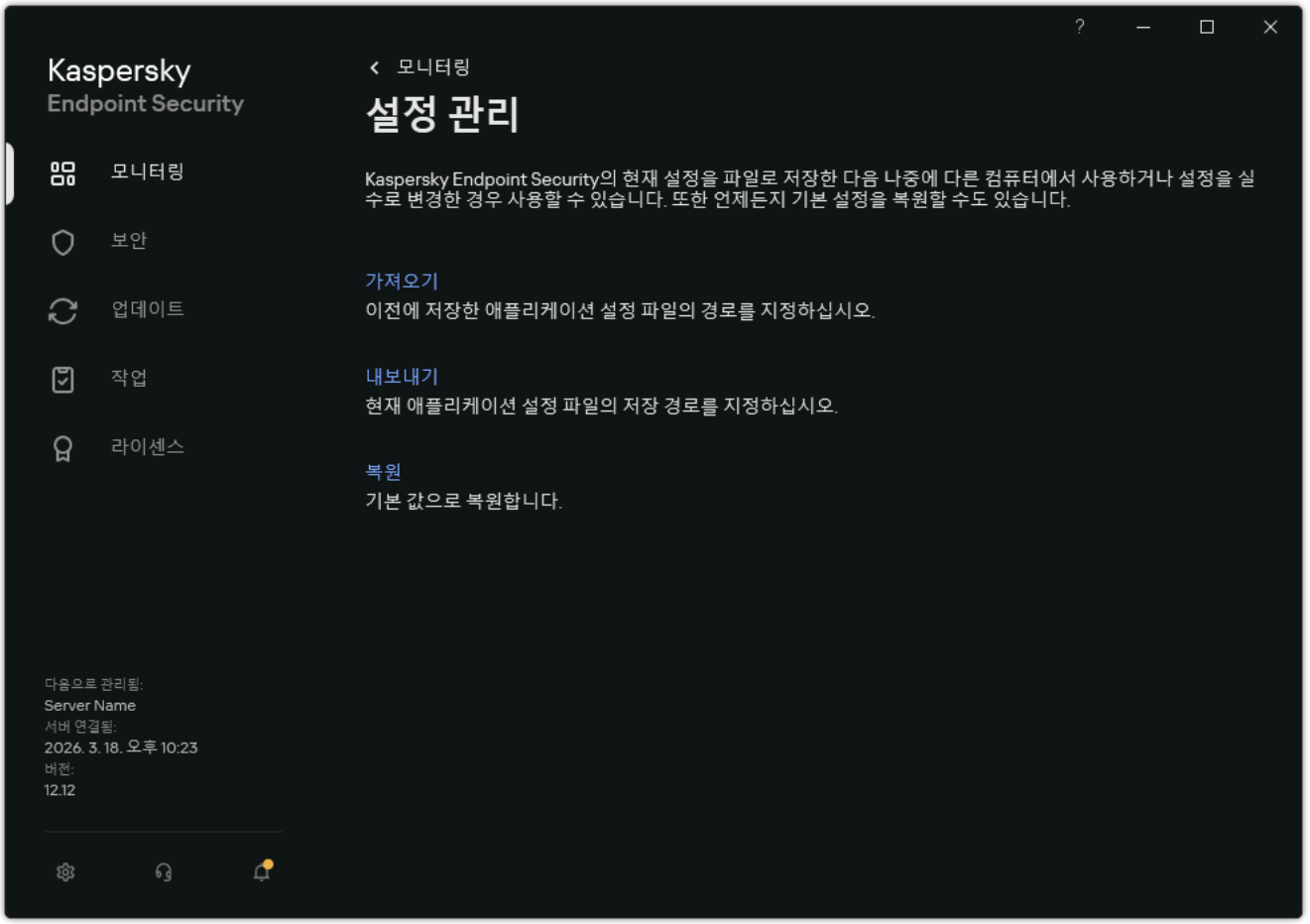
구성 파일의 Kaspersky Endpoint Security 설정을 가져오려면 다음을 수행합니다:

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **설정 관리**를 선택합니다.
3. **가져오기**를 클릭합니다.

4. 창이 열리면 구성 파일의 경로를 입력합니다.

5. 파일을 엽니다.

선택한 구성 파일에 따라 Kaspersky Endpoint Security의 모든 설정 값이 설정됩니다.



애플리케이션 설정 관리

애플리케이션 기본 설정 복원

언제든지 Kaspersky 권장 애플리케이션 설정을 복원할 수 있습니다. 설정을 복원하면 모든 보호 구성 요소에 대해 **권장** 보안 레벨이 설정됩니다.

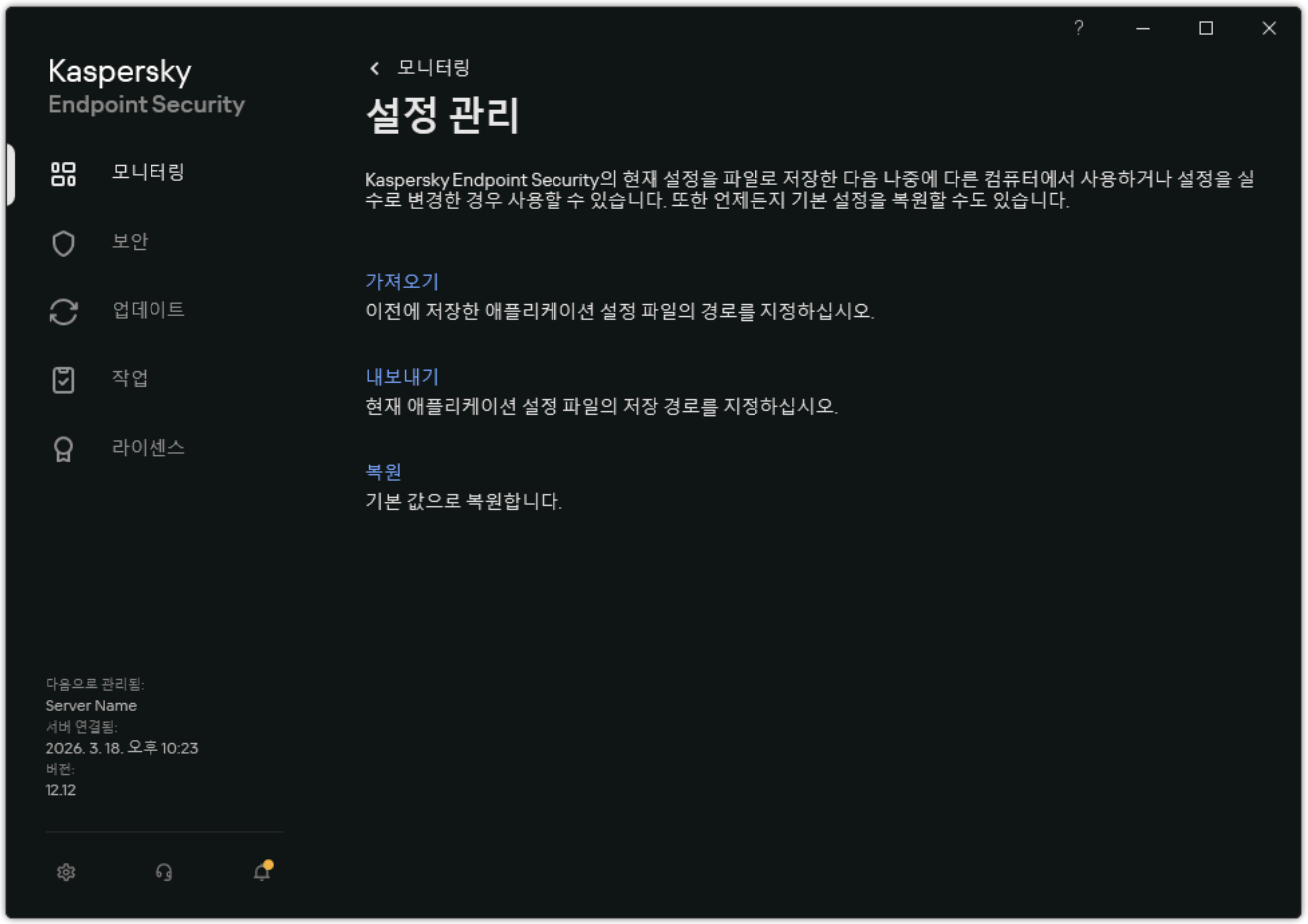
애플리케이션 설정을 기본값으로 복원하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **일반 설정** → **설정 관리**를 선택합니다.

3. **복원**을 클릭합니다.

4. 변경 사항을 저장합니다.



애플리케이션 설정 관리

Kaspersky Endpoint Security 성능 및 다른 애플리케이션과의 호환성

Kaspersky Endpoint Security의 성능은 컴퓨터를 손상시킬 수 있는 위협 중 탐지 가능한 유형의 수, 에너지 소비량 및 컴퓨터 리소스의 사용량을 의미합니다.

탐지 가능한 개체의 유형 선택

Kaspersky Endpoint Security를 통해 컴퓨터 보호를 유연하게 구성하고 작업 중 애플리케이션에서 탐지한 개체의 유형을 선택할 수 있습니다. Kaspersky Endpoint Security는 항상 운영 체제에서 바이러스, 웜 및 트로이목마를 검사합니다. 이 유형의 개체에 대한 검사는 중지할 수 없습니다. 이러한 악성 코드가 컴퓨터에 심각한 손상을 불러 일으킬 수 있기 때문입니다. 컴퓨터를 손상시키거나 개인 정보를 훔칠 목적으로 악용될 수 있는 정상적인 소프트웨어를 감시하도록 설정하면 탐지 가능 개체 유형의 범위를 확장하고 컴퓨터 보안을 더욱 철저히 유지할 수 있습니다.

절전 모드 사용

애플리케이션으로 인한 에너지 소비량은 휴대용 컴퓨터에서 중요한 고려 사항입니다. Kaspersky Endpoint Security의 예약된 작업은 일반적으로 상당한 자원을 사용합니다. 컴퓨터가 배터리 전원으로 실행되는 경우 절전 모드를 사용하여 전원 소모를 줄일 수 있습니다.

절전 모드에서는 다음과 같이 스케줄된 작업이 자동으로 연기됩니다:

- 업데이트 작업
- 컴퓨터 전체 검사 작업
- 중요 영역 검사 작업
- 사용자 지정 검사 작업
- 무결성 검사 작업

절전 모드의 설정 여부에 관계 없이 휴대용 컴퓨터가 배터리로 작동될 경우 Kaspersky Endpoint Security는 암호화된 작업을 일시 중지합니다. 휴대용 컴퓨터가 배터리 전원이 아닌 주 전원으로 작동하면 애플리케이션에서 다시 암호화 작업을 시작합니다.

다른 애플리케이션에 컴퓨터 리소스 우선권 할당

컴퓨터 검사 시 컴퓨터 리소스 사용으로 인해 CPU 및 하드 드라이브 서브시스템의 로드가 증가할 수 있습니다. CPU 및 하드 드라이브의 하위 시스템에 로드가 증가되는 동안 실행되는 작업의 문제를 해결하기 위해 Kaspersky Endpoint Security는 다른 애플리케이션에 컴퓨터 리소스 우선권을 할당할 수 있습니다.

고급 치료 기술 사용

오늘날의 악성 애플리케이션은 운영 체제의 최하위 계층에 침투하기 때문에 제거하기가 거의 불가능합니다. 운영 체제에서 악성 활동을 탐지한 후 Kaspersky Endpoint Security는 특수한 고급 치료 기술을 사용하는 포괄적인 치료 절차를 수행합니다. *고급 치료 기술*은 RAM에서 프로세스를 시작하여 Kaspersky Endpoint Security가 일반적인 방법으로는 제거할 수 없는 악성 애플리케이션을 제거하기 위해 개발되었습니다. 위협은 이 기술로 처리됩니다. 고급 치료 기술을 사용하면 이러한 위협이 처리되며, 고급 치료 절차가 진행 중인 동안에는 새로운 프로세스를 시작하거나 운영 체제 레지스트리를 편집하지 않는 것이 좋습니다. 고급 치료 기술은 상당한 운영 체제 리소스를 사용하므로 다른 애플리케이션의 속도가 떨어질 수 있습니다.

워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에서 고급 치료 기술이 실행 완료된 후 Kaspersky Endpoint Security는 사용자가 컴퓨터를 재부팅하도록 요청합니다. 시스템 재부팅 후 Kaspersky Endpoint Security는 악성 코드를 삭제하고 "빠른" 컴퓨터 전체 검사를 시작합니다.

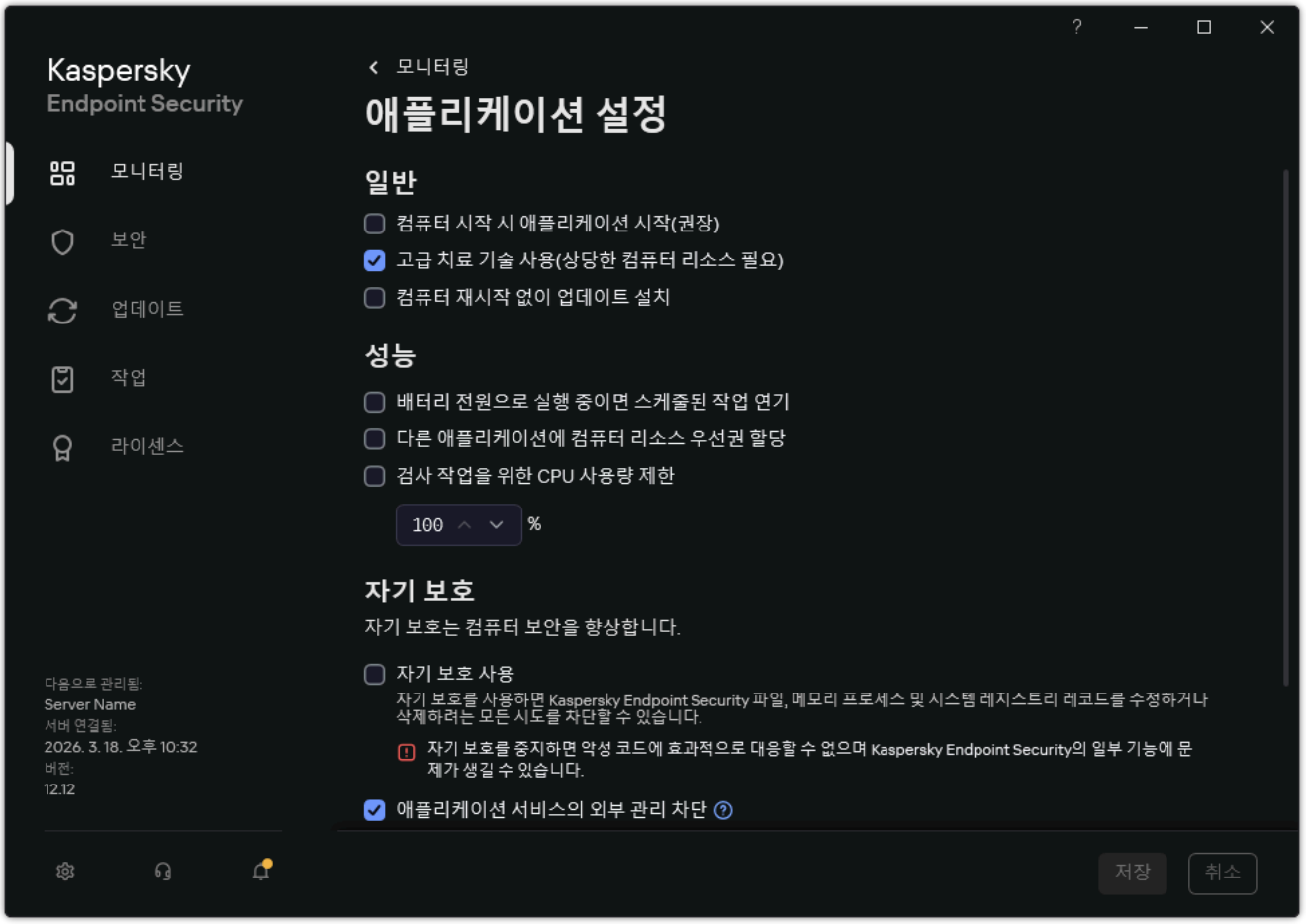
Kaspersky Endpoint Security의 특성으로 인해 서버용 Microsoft Windows를 실행 중인 컴퓨터는 재부팅할 수 없습니다. 파일 서버의 예기치 못한 재부팅은 파일 서버 데이터를 일시적으로 사용할 수 없거나 저장되지 않은 데이터가 손실되는 등의 문제로 이어질 수 있습니다. 따라서 정해진 스케줄에 따라 안전하게 파일 서버를 재부팅하는 것이 좋습니다. 파일 서버용에서는 고급 치료 기술이 기본적으로 사용 안 함 설정된 이유입니다.

파일 서버에서 활성 위협이 탐지될 경우 Kaspersky Security Center에 고급 치료가 필요하다는 정보와 함께 이벤트가 전달됩니다. 서버의 감염을 치료하기 위해 서버용 고급 치료 기술을 활성화하고 서버 사용자가 편리한 시간에 *악성 코드 검사* 그룹 작업을 시작합니다.

절전 모드 작동 또는 중지

절전 모드를 작동 또는 중지하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

3. **성능** 블록에서 **배터리 전원으로 실행 중이면 스케줄된 작업 연기** 확인란으로 절전 모드를 사용하거나 중지합니다.

   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 검사*
- *IOC 검사*

4. 변경 사항을 저장합니다.

다른 애플리케이션에 컴퓨터 리소스 우선권 할당 작동 또는 중지

사용자 컴퓨터 검사 시 Kaspersky Endpoint Security의 컴퓨터 리소스 사용으로 인해 CPU 및 하드 드라이브 서브시스템의 로드가 증가할 수 있습니다. 이렇게 되면 기타 애플리케이션의 속도가 저하될 수 있습니다. 성능을 최적화하기 위해 Kaspersky Endpoint Security는 *기타 애플리케이션으로 리소스를 전송하는 모드*를 제공합니다. 이 모드에서는 CPU 로드가 높아지면 운영 체제에서 Kaspersky Endpoint Security 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 Endpoint Security가 컴퓨터를 검사하는 시간이 길어집니다. 기본적으로 이 애플리케이션은 컴퓨터 리소스 우선권을 다른 애플리케이션에 할당하도록 구성됩니다.

관리 콘솔(MMC)에서 다른 애플리케이션에 컴퓨터 리소스 우선권 할당을 활성화 또는 비활성화하는 방법

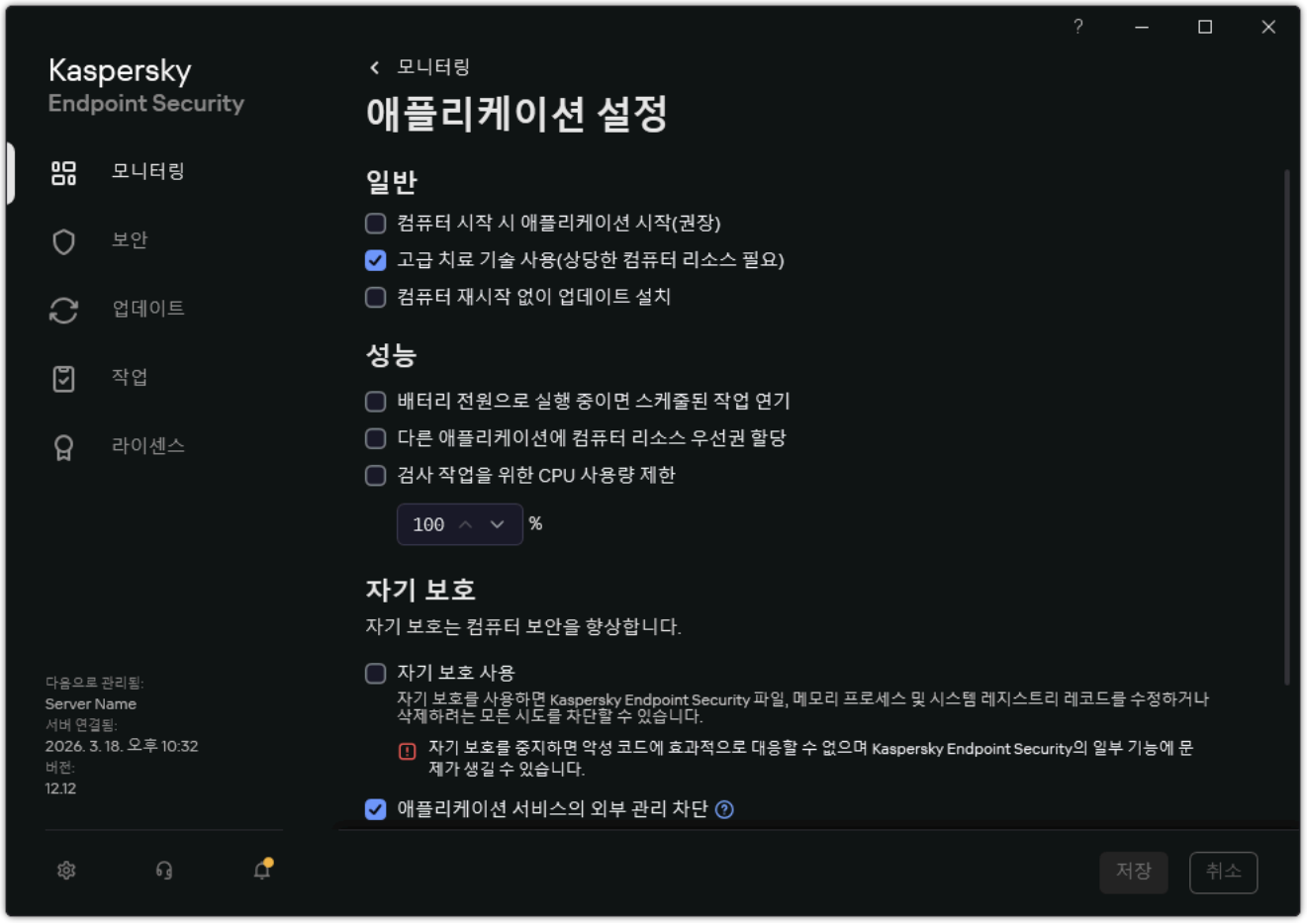
1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 애플리케이션 설정**을 차례로 선택합니다.
4. **성능** 블록에서 **다른 애플리케이션에 컴퓨터 리소스 우선권 할당** 확인란으로 다른 애플리케이션에 대한 리소스 할당을 사용하거나 중지합니다.
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 다른 애플리케이션에 컴퓨터 리소스 우선권 할당을 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 성능**으로 이동합니다.
5. **다른 애플리케이션에 리소스 우선권 할당** 블록에서 **다른 애플리케이션에 리소스 우선권 할당** 토글 스위치를 사용하여 다른 애플리케이션에 리소스 우선권 할당을 활성화하거나 비활성화합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 다른 애플리케이션에 컴퓨터 리소스 우선권 할당을 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

3. **성능** 블록에서 **다른 애플리케이션에 컴퓨터 리소스 우선권 할당** 확인란으로 다른 애플리케이션에 대한 리소스 할당을 사용하거나 중지합니다.
4. 변경 사항을 저장합니다.

Kaspersky Endpoint Security 성능 최적화를 위한 모범 사례

Kaspersky Endpoint Security for Windows 배포 시 다음 권장 사항을 사용하여 컴퓨터 보호를 구성하고 성능을 최적화할 수 있습니다. 컴퓨터 성능 오류를 해결하는 방법에 대한 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오.

일반

다음 권장 사항에 따라 애플리케이션의 일반 설정을 구성합니다:

1. Kaspersky Endpoint Security를 최신 버전으로 업그레이드.
   최신 버전의 애플리케이션은 오류가 수정되고 안정성이 높으며 성능도 최적화되어있습니다.

2. 기본 설정으로 보호 구성 요소 활성화.

   기본 설정은 최적의 설정을 사용합니다. Kaspersky 전문가가 권장하는 설정입니다. 기본 설정은 권장 보호 수준과 최적의 리소스 사용을 제공합니다. 필요하다면 기본 애플리케이션 설정을 복원할 수 있습니다.

3. 애플리케이션 성능 최적화 기능 활성화.

   애플리케이션에는 에너지 절약 모드 및 다른 애플리케이션에 리소스 양도 등의 성능 최적화 기능이 있습니다. 이러한 옵션이 활성화되어 있는지 확인하십시오.

워크스테이션에서 악성 코드 검사

워크스테이션에서 악성 코드 검사 시 백그라운드 검사를 권장합니다. *백그라운드 검사*는 사용자에 대한 알림을 표시하지 않는 Kaspersky Endpoint Security의 검사 모드입니다. 백그라운드 검사는 다른 유형의 검사(예: 전체 검사)보다 적은 컴퓨터 리소스를 사용합니다. 이 모드에서 Kaspersky Endpoint Security는 시작 개체, 부트 섹터, 시스템 메모리 및 시스템 파티션을 검사합니다. 백그라운드 검사 설정은 최적의 설정을 사용합니다. Kaspersky 전문가가 권장하는 설정입니다. 따라서 컴퓨터의 악성 코드 검사를 수행할 때 다른 검사 작업을 사용하지 않고 백그라운드 검사 모드만 사용해도 됩니다.

백그라운드 검색만으로는 부족하다면 다음 권장 사항에 따라 *악성 코드 검사* 작업을 구성하십시오:

1. 컴퓨터 검사 중 CPU 리소스 소비 제한을 설정합니다.

   악성 코드 검사 작업을 실행할 때 CPU 사용량을 제한할 수 있습니다. 이렇게 하려면 애플리케이션 설정에서 컴퓨터 검사 중에 활용할 수 있는 모든 코어에 대한 최대 CPU 로드를 퍼센트로 지정합니다. 이는 컴퓨터를 검사하는 데 걸리는 시간을 늘릴 수 있습니다.

2. 최적의 컴퓨터 검사 스케줄 구성.

   컴퓨터의 부하가 최소 수준일 때 작업을 실행하도록 구성할 수 있습니다. 예를 들어 작업을 야간이나 주말에 실행하도록 구성할 수 있습니다.

   사용자가 업무 시간 외에 컴퓨터를 끄는 경우 Wake-on-LAN 기능을 활성화할 수 있습니다. Wake-on-LAN 기능을 사용하면 로컬 네트워크를 통해 특수 신호를 보내 원격으로 컴퓨터 전원을 켤 수 있습니다. 이 기능을 사용하려면 BIOS 설정에서 Wake-on-LAN을 활성화해야 합니다. 검사를 완료한 후 컴퓨터가 자동으로 꺼지도록 할 수도 있습니다.

   최적의 검사 스케줄을 구성할 수 없다면 컴퓨터가 유휴 상태일 때만 작업이 실행되도록 설정하십시오. Kaspersky Endpoint Security는 컴퓨터가 잠겨 있거나 화면 보호기가 켜져 있을 때 검사 작업을 시작합니다. 예를 들어 컴퓨터를 잠금 해제하는 등으로 작업 실행이 중단되면 Kaspersky Endpoint Security는 자동으로 중단된 지점부터 작업을 실행합니다.

3. 검사 범위 정의.

   검사할 다음 개체를 선택합니다(최소 검사 범위 세트):

   - 커널 메모리
   - 실행 중인 프로세스 및 시작 개체
   - 부트 섹터
   - %systemroot% (하위 폴더 제외)
   - %systemroot%\System (하위 폴더 제외)
   - %systemroot%\System32 (하위 폴더 제외)

- %systemroot%\System32\drivers (하위 폴더 제외)
- %systemroot%\SysWOW64 (하위 폴더 제외)
- %systemroot%\SysWOW64\drivers (하위 폴더 제외)

4. iSwift 및 iChecker 기술을 켭니다.

   - iSwift 기술.

     이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.

   - iChecker 기술.

     이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.

   관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 iSwift 및 iChecker 기술을 켤 수 있습니다. Kaspersky Security Center 웹 콘솔에서는 이러한 기술을 켤 수 없습니다.

5. 암호로 보호된 압축파일 검사 비활성화.

   암호로 보호된 압축파일 스캔이 활성화되면 압축파일을 검사하기 전에 암호 프롬프트가 표시됩니다. 본 작업은 업무 외 시간에 스케줄할 것을 권장하는 만큼 사용자가 매번 암호를 입력하기는 힘듭니다. 암호가 걸려 있는 압축 파일은 수동으로 검사할 수 있습니다.

6. 여러 검사 작업의 동시 실행을 비활성화합니다.

   Kaspersky Endpoint Security는 현재 검사가 진행 중이면 새 검사 작업을 대기열에 넣습니다. 이렇게 하면 컴퓨터 부하 최적화에 도움이 됩니다.

서버 상의 악성 코드 검사

다음 권장 사항에 따라 *악성 코드 검사* 작업을 구성합니다:

1. 컴퓨터 검사 중 CPU 리소스 소비 제한을 설정합니다.

   악성 코드 검사 작업을 실행할 때 CPU 사용량을 제한할 수 있습니다. 이렇게 하려면 애플리케이션 설정에서 컴퓨터 검사 중에 활용할 수 있는 모든 코어에 대한 최대 CPU 로드를 퍼센트로 지정합니다. 이는 컴퓨터를 검사하는 데 걸리는 시간을 늘릴 수 있습니다.

2. 최적의 컴퓨터 검사 스케줄 구성.

   컴퓨터의 부하가 최소 수준일 때 작업을 실행하도록 구성할 수 있습니다. 예를 들어 작업을 야간이나 주말에 실행하도록 구성할 수 있습니다.

3. iSwift 및 iChecker 기술을 켭니다.

   - iSwift 기술.

     이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.

   - iChecker 기술.

     이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.

   관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 iSwift 및 iChecker 기술을 켤 수 있습니다. Kaspersky Security Center 웹 콘솔에서는 이러한 기술을 켤 수 없습니다.

4. 암호로 보호된 압축파일 검사 비활성화.

   암호로 보호된 압축파일 스캔이 활성화되면 압축파일을 검사하기 전에 암호 프롬프트가 표시됩니다. 본 작업은 업무 외 시간에 스케줄할 것을 권장하는 만큼 사용자가 매번 암호를 입력하기는 힘듭니다. 암호가 걸려 있는 압축 파일은 수동으로 검사할 수 있습니다.

5. 여러 검사 작업의 동시 실행을 비활성화합니다.

   Kaspersky Endpoint Security는 현재 검사가 진행 중이면 새 검사 작업을 대기열에 넣습니다. 이렇게 하면 컴퓨터 부하 최적화에 도움이 됩니다.

Kaspersky Security Network

Kaspersky Endpoint Security는 사용자 컴퓨터를 보다 효과적으로 보호하기 위해 전세계 사용자로부터 수신한 데이터를 사용합니다. Kaspersky Security Network는 이러한 사용자 데이터를 수집하기 위한 네트워크입니다.

*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 Endpoint Security에서 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 Endpoint Security는 검사한 웹 주소의 평판 정보는 물론이고 검사한 파일의 카테고리 및 평판에 관한 정보도 수신하게 됩니다.

다음 권장 사항에 따라 Kaspersky Security Network 설정을 편집합니다:

1. 확장 KSN 모드 비활성화.

   *확장 KSN 모드*는 Kaspersky Endpoint Security가 추가 데이터를 Kaspersky로 전송하는 모드입니다.

2. Kaspersky Private Security Network 구성.

   *Kaspersky Private Security Network(KPSN)*는 Kaspersky Endpoint Security 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.

3. 클라우드 모드 사용.

   클라우드 모드 Kaspersky Endpoint Security가 경량 버전의 안티 바이러스 데이터베이스를 사용하는 애플리케이션 운영 모드를 의미합니다. Kaspersky Security Network는 경량의 안티 바이러스 데이터베이스가 사용 중일 때 애플리케이션의 운영을 지원합니다. 경량 버전의 안티 바이러스 데이터베이스를 사용하면 일반 데이터베이스에 비해 절반 가량의 컴퓨터 RAM을 사용하게 됩니다. Kaspersky Security Network에 참여하지 않거나 클라우드 모드를 사용하지 않는 경우 Kaspersky Endpoint Security는 Kaspersky 서버에서 전체 버전의 안티 바이러스 데이터베이스를 다운로드합니다.

악성 코드 검사

악성 코드 검사는 컴퓨터 보안에 있어 매우 중요합니다. 정기적인 악성 코드 검사 실행은 낮은 보안 레벨 설정이나 다른 이유로 인해 보호 구성 요소에서 탐지하지 못하는 악성 코드가 확산되는 것을 막을 수 있습니다.

Kaspersky Endpoint Security는 컨텐츠가 OneDrive 클라우드 저장소에 있는 파일을 검사하지 않으며 이러한 파일이 검사되지 않았음을 나타내는 로그 항목을 생성합니다.

전체 검사

전체 컴퓨터를 완전히 검사합니다. Kaspersky Endpoint Security는 다음과 같은 개체를 검사합니다:

- 커널 메모리
- 운영 체제를 시작할 때 로드되는 개체
- 부트 섹터
- 운영 체제 백업
- 모든 하드 및 이동식 드라이브

Kaspersky 전문가는 *전체 검사* 작업의 검사 범위를 변경하지 않는 것을 권장합니다.

컴퓨터 리소스를 절약하려면 전체 검사 작업 대신 백그라운드 검사 작업을 사용하는 것이 좋습니다. 이는 컴퓨터의 보안 레벨에 영향을 주지 않습니다.

중요 영역 검사

Kaspersky Endpoint Security는 기본적으로 커널 메모리, 실행 중인 프로세스 및 디스크 부트 섹터를 검사합니다.

Kaspersky 전문가는 *중요 영역 검사* 작업의 검사 범위를 변경하지 않는 것을 권장합니다.

사용자 지정 검사

Kaspersky Endpoint Security에서 사용자가 선택한 개체를 검사합니다. 다음 목록의 개체를 검사할 수 있습니다:

- 시스템 메모리
- 운영 체제를 시작할 때 로드되는 개체
- 운영 체제 백업
- 하드, 이동식 및 네트워크 드라이브
- 모든 선택 파일

백그라운드 검사

*백그라운드 검사*는 사용자에 대한 알림을 표시하지 않는 Kaspersky Endpoint Security의 검사 모드입니다. 백그라운드 검사는 다른 유형의 검사(예: 전체 검사)보다 적은 컴퓨터 리소스를 사용합니다. 이 모드에서 Kaspersky Endpoint Security는 시작 개체, 부트 섹터, 시스템 메모리 및 시스템 파티션을 검사합니다.

애플리케이션 무결성 검사

Kaspersky Endpoint Security는 그 애플리케이션 모듈의 손상 및 변경 여부를 확인합니다.

컴퓨터 검사

검사는 컴퓨터 보안에 있어 매우 중요합니다. 정기적인 악성 코드 검사 실행은 낮은 보안 레벨 설정이나 다른 이유로 인해 보호 구성 요소에서 탐지하지 못하는 악성 코드가 확산되는 것을 막을 수 있습니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다.

Kaspersky Endpoint Security에는 사전 정의된 표준 작업인 *전체 검사*, *중요 영역 검사*, *사용자 지정 검사*가 있습니다. 조직에 Kaspersky Security Center 관리 시스템이 배포되어 있다면 *악성 코드 검사* 작업 생성과 검사 구성이 가능합니다.

관리 콘솔(MMC)에서 검사 작업을 실행하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업**을 선택합니다.
3. 검사 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.
   필요하다면 *악성 코드 검사* 작업을 생성합니다.

4. 작업 속성 창에서 **설정** 섹션을 선택합니다.

5. 검사 작업을 구성합니다(아래 표 참조).
   필요하다면, 검사 작업 스케줄을 구성합니다.

6. 변경 사항을 저장합니다.

7. 검사 작업을 실행합니다.

   Kaspersky Endpoint Security가 컴퓨터 검사를 시작합니다. 사용자가 작업 실행을 중단했다면(컴퓨터 전원 끄기 등) Kaspersky Endpoint Security는 검사가 중단된 지점부터 계속 작업을 자동으로 실행합니다.

웹 콘솔 및 Cloud Console에서 검사 작업을 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. 검사 작업을 클릭합니다.
   작업 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. 검사 작업을 구성합니다(아래 표 참조).
   필요하다면, 검사 작업 스케줄을 구성합니다.

5. 변경 사항을 저장합니다.

6. 검사 작업을 실행합니다.

   Kaspersky Endpoint Security가 컴퓨터 검사를 시작합니다. 사용자가 작업 실행을 중단했다면(컴퓨터 전원 끄기 등) Kaspersky Endpoint Security는 검사가 중단된 지점부터 계속 작업을 자동으로 실행합니다.

애플리케이션 인터페이스에서 검사 작업을 실행하는 방법

1. 메인 애플리케이션 창에서 **작업** 섹션으로 이동합니다.

2. 작업 목록에서 검사 작업을 선택하고 ⚙ 클릭합니다.

3. 검사 작업을 구성합니다(아래 표 참조).
   필요하다면, 검사 작업 스케줄을 구성합니다.

4. 변경 사항을 저장합니다.

5. 검사 작업을 실행합니다.

   Kaspersky Endpoint Security가 컴퓨터 검사를 시작합니다. 애플리케이션은 검사 진행률, 검사한 파일 수 및 남은 검사 시간을 표시합니다. **중지** 버튼을 클릭하여 언제든지 작업을 중지할 수 있습니다. 검사 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

컴퓨터를 검사하는 동안 Kaspersky Endpoint Security 성능을 최적화기 위해 *전체 검사* 작업의 고급 설정을 관리하고 CPU 리소스 사용을 제한할 수 있습니다.

Kaspersky Security Center에서 *백그라운드 검사* 작업을 *전체 검사* 작업 대신 사용하여 애플리케이션의 성능을 최적화할 수 있습니다. 이는 컴퓨터의 보안 레벨에 영향을 주지 않습니다. 백그라운드 검사를 구성할 수 없습니다.

그에 따라 Kaspersky Endpoint Security는 컴퓨터를 검사하고 위협이 탐지되면 애플리케이션 설정에서 구성한 처리 방법을 실행합니다. 일반적으로 애플리케이션은 감염된 파일 치료를 시도합니다. 그에 따라 감염된 파일은 다음 상태를 수신할 수 있습니다:

- **연기**. 감염된 파일을 치료할 수 없습니다. 애플리케이션이 컴퓨터를 다시 시작한 후 감염된 파일을 삭제합니다.
- **리포트에만 기록**. 감염된 파일을 치료할 수 없습니다. 애플리케이션이 처리 안 된 보안위협 목록에 탐지된 감염 파일에 대한 정보를 추가합니다.
- **쓰기 지원 안 됨** 또는 **쓰기 오류**. 감염된 파일을 치료할 수 없습니다. 애플리케이션에 쓰기 권한이 없습니다.
- **이미 처리됨**. 이전에 애플리케이션이 감염된 파일을 탐지했습니다. 애플리케이션이 컴퓨터를 다시 시작한 후 감염된 파일을 치료하거나 삭제합니다.

검사 설정

파라미터	설명
보안 레벨	Kaspersky Endpoint Security는 다양한 설정 그룹을 사용해 검사를 실행할 수 있습니다. 애플리케이션에 저장된 설정 집합을 *보안 레벨*이라고 합니다: • **높음**. Kaspersky Endpoint Security는 모든 유형의 파일을 검사합니다. 복합 파일을 검사할 때 애플리케이션은 압축 파일, 배포 패키지, 오피스 형식의 파일을 검사하지만, 암호가 걸린 압축 파일은 검사하지 않습니다. 이 보안 레벨을 설정하면 애플리케이션은 휴리스틱 분석과 **정밀 검사** 세부 정보 수준을 사용합니다. • **권장**. Kaspersky Endpoint Security는 모든 유형의 파일을 검사합니다. 복합 파일을 검사할 때 애플리케이션은 압축 파일, 배포 패키지, 오피스 형식의 파일을 검사하지만, 암호가 걸린 압축 파일은 검사하지 않습니다. 이 보안 레벨을 설정하면 애플리케이션이 휴리스틱 분석과 **보통 검사** 세부 정보 수준을 사용합니다. • **낮음**. Kaspersky Endpoint Security가 지정된 파일 형식만 검사합니다. 복합 파일을 검사할 때 애플리케이션은 압축 파일, 배포 패키지, 오피스 형식의 파일을 검사하지만, 암호가 걸린 압축 파일은 검사하지 않습니다. 이 보안 레벨을 설정하면 애플리케이션이 휴리스틱 분석과 **빠른 검사** 세부 정보 수준을 사용합니다. 미리 설정된 보안 레벨 중 하나를 선택하거나 직접 보안 레벨 설정을 구성할 수 있습니다. 보안 레벨 설정을 변경한 경우 언제든지 권장 보안 레벨로 되돌릴 수 있습니다.
위협 탐지 시 처리 방법	**치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다. **치료 - 불가능한 경우 알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 탐지된 모든 감염을 자동으로 치료합니다. 치료 실패 시 Kaspersky Endpoint Security는 탐지된 감염 파일에 대한 정보를 처리 안 된 위협 목록에 추가합니다. **알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 감염된 파일에 대한 정보를 해당 파일 탐지 시 처리 안 된 위협 목록에 추가합니다. 감염된 파일을 치료하거나 삭제하기 전에 애플리케이션이 파일을 복원하거나 나중에 치료할 수 있을 때에 대비하여 파일의 복사본을 만듭니다. Windows Store 애플리케이션에서 감염된 파일이 탐지되면 Kaspersky Endpoint Security는 해당 파일의 삭제를 시도합니다.
고급 치료 즉시 실행 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이 컴퓨터에 적용된 정책의 속성에서 고급 치료 기능을 사용하는 경우에만 컴퓨터에서 바이러스 검사 작업 중 고급 치료가 수행됩니다. 이 확인란을 선택하면 Kaspersky Endpoint Security는 바이러스 검사 작업 실행 중에 탐지된 실행 중인 악성 코드를 즉시 치료합니다. 실행 중인 악성 코드 치료 후 Kaspersky Endpoint Security는 사용자에게 메시지를 표시하지 않고 컴퓨터를 재부팅합니다. 확인란을 선택 해제하면 Kaspersky Endpoint Security는 바이러스 검사 작업 실행 중에 탐지된 실행 중인 악성 코드를 즉시 치료하지 않습니다. Kaspersky Endpoint Security는 로컬 애플리케이션 리포트와 Kaspersky Security Center에서 실행 중인 악성 코드 이벤트를 생성합니다. 고급 치료 기능이 켜진 상태에서 바이러스 검사 작업을 다시 실행하면 실행 중인 악성 코드를 치료할 수 있습니다. 이러한 방식으로 시스템 관리자는 고급 치료를 수행할 적절한 시간을 선택한 다음 컴퓨터를 자동으로 재부팅할 수 있습니다.

파라미터	설명
검사 범위	Kaspersky Endpoint Security가 검사 작업을 수행할 때 검사하는 개체 목록입니다. 검사 범위 내의 개체에는 커널 메모리, 실행 중인 프로세스, 부트 섹터, 시스템 백업 저장소, 하드 드라이브, 이동식 드라이브, 네트워크 드라이브, 폴더 또는 파일 등이 포함될 수 있습니다. Kaspersky Endpoint Security for Windows 12.12에서는 이메일은 애플리케이션 검사 범위에서 제외됩니다. 수신 및 발신되는 이메일 메시지의 검사는 메일 위협 보호 구성 요소에서 수행합니다. 이전 버전의 관리 플러그인을 사용하는 경우 애플리케이션은 정책에 포함되어 있더라도 이메일을 검사 범위에서 제외합니다.
검사 스케줄	**수동**. 편리한 시간에 검사를 수동으로 시작할 수 있는 실행 모드입니다. **스케줄에 따라**. 이 검사 작업 스케줄에서는 애플리케이션이 사용자가 만드는 스케줄에 따라 검사 작업을 시작합니다. 이 검사 작업 스케줄이 선택되면 검사 작업을 수동으로 시작할 수도 있습니다.
애플리케이션 시작 후 다음 시간 동안 작업 실행 연기: N분	애플리케이션 시작 시 일정 시간 후에 검사 작업 시작. 운영 체제 시작 시 많은 프로세스가 실행 중이므로 Kaspersky Endpoint Security 시작 직후에 검사 작업을 실행하는 것보다 검사 작업을 잠시 연기하는 것이 좋습니다.
건너뛴 작업 실행	이 확인란을 선택하면, Kaspersky Endpoint Security는 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 Endpoint Security가 건너뛴 작업을 실행하지 않습니다. 대신, 현재 스케줄에 따라 다음 작업을 실행합니다.
컴퓨터가 유휴 상태일 때만 실행	컴퓨터 리소스가 사용 중일 때 작업 시작을 연기했습니다. Kaspersky Endpoint Security는 컴퓨터가 잠겨 있거나 화면 보호기가 켜져 있을 때 검사 작업을 시작합니다. 예를 들어 컴퓨터를 잠금 해제하는 등으로 작업 실행이 중단되면 Kaspersky Endpoint Security는 자동으로 중단된 지점부터 작업을 실행합니다. 이 예약 옵션을 사용하면 컴퓨터를 사용할 때 컴퓨터 리소스를 절약할 수 있습니다.
다음으로 검사 실행	기본적으로 검사 작업이 운영 체제에 등록된 권한을 가진 사용자의 이름으로 실행됩니다. 보호 범위에는 특수 접근 권한이 필요한 네트워크 드라이브 또는 기타 개체가 포함될 수 있습니다. 애플리케이션 설정에서 필요한 권한이 있는 사용자를 지정하여 이 사용자의 계정으로 검사 작업을 실행할 수 있습니다.
파일 유형	Kaspersky Endpoint Security는 확장자가 없는 파일을 실행 파일로 간주합니다. 애플리케이션은 검사하도록 선택한 파일 형태에 상관없이 항상 실행 파일을 검사합니다. **모든 파일**. 이 설정을 사용하면 Kaspersky Endpoint Security가 예외 없이 모든 형식과 확장자의 파일을 검사합니다. **형식에 따라 검사한 파일**. 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일에 악성 코드가 있는지 검사하기 전에 파일의 내부 헤더를 분석하여 파일 형식을 결정합니다(예: txt, .doc 또는 .exe). 또한 이 검사에서는 특정 파일 확장자를 가진 파일도 찾습니다. **확장자에 따라 검사한 파일** 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일 형식은 파일 확장자를 기반으로 결정됩니다. Kaspersky Endpoint Security는 기본적으로 파일 유형으로 파일을 검사합니다. 확장자로 파일 검색 시 악성 파일이 감염 가능 확장자 목록에 없는 확장자를 취할 수 있으므로(예: `.123`) 안전성이 떨어집니다.
새로운 파일과 수정된 파일만 검사	새로운 파일과 마지막 검사 이후 수정된 파일만 검사합니다. 이는 검사 시간을 줄이는 것입니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.
다음보다 오래 검사하는 파일은 건너뛰기: N초	작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.
여러 검사 작업을 동시에 실행하지 않음	검사가 이미 실행 중이라면 검사 작업 시작을 연기합니다. Kaspersky Endpoint Security는 현재 검사가 진행 중이면 새 검사 작업을 대기열에 넣습니다. 이렇게 하면 컴퓨터 부하 최적화에 도움이 됩니다. 예를 들어 애플리케이션이 스케줄에 따라 전체 검색 작업을 시작했다고 가정해봅시다. 사용자가 애플리케이션 인터페이스에서 빠른 검사를 시작하려고 하면 Kaspersky Endpoint Security는 이 파일 검사 작업을 대기열에 넣은 후 전체 검사 작업 완료 후에 이 작업을 자동으로 시작합니다. 그러나 Kaspersky Endpoint Security는 다음 검사 작업 중 하나가 실행 중일 때도 즉시 검사 작업을 시작합니다. • 이동식 드라이브 연결 시 검사 • 마우스 오른쪽 메뉴에서 검사 • 침해 지표(IoC) 탐지로 시작된 중요 영역 검사 이 확인란을 선택 취소하면 Kaspersky Endpoint Security에서 동시에 여러 검사 작업을 실행할 수 있습니다. 여러 검사 작업을 실행하려면 컴퓨터 리소스가 더 많이 필요합니다.
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	타사 애플리케이션의 배포 패키지 검사.

파라미터	설명
Microsoft Office 형식 파일 검사	Microsoft Office 파일(DOC, DOCX, XLS, PPT 및 기타 Microsoft 확장자)을 검사합니다. Office 형식 파일에는 OLE 개체도 포함됩니다. 애플리케이션이 확인란 선택 여부와 상관없이 1MB보다 작은 오피스 형식 파일을 검사합니다.
이메일 형식 파일 검사	이메일 형식 파일 및 이메일 데이터베이스 검사. 이 애플리케이션은 MS Outlook 및 Windows Mail 메일 클라이언트에서 사용하는 PST 및 OST 파일과 EML 파일을 검색합니다. Kaspersky Endpoint Security는 64비트 버전의 Microsoft Outlook 이메일 클라이언트를 지원하지 않습니다. 따라서 Kaspersky Endpoint Security는 64비트 버전의 Microsoft Outlook이 컴퓨터에 설치된 경우 메일이 검사 범위에 포함되어도 Microsoft Outlook 파일(PST 및 OST 파일)을 검사하지 않습니다. 이 확인란을 선택하면 Kaspersky Endpoint Security가 메일 형식 파일을 각 구성 요소로 나누고(헤더, 본문, 첨부파일) 각각의 보안위협을 검사합니다. 이 확인란을 선택 취소하면 Kaspersky Endpoint Security가 메일 형식 파일을 단일 파일로 검사합니다. PST 또는 OST 파일에서 악성 개체가 탐지되면 Kaspersky Endpoint Security는 선택한 작업(예: 파일 치료 또는 삭제)에 따라 해당 개체를 무해한 상태로 만듭니다. 다른 메일 클라이언트(예: Mozilla Thunderbird)의 파일에서 악성 파일이 탐지되면 Kaspersky Endpoint Security는 감염된 메시지를 표시만 합니다. 첨부 파일의 감염된 메시지를 직접 삭제해야 합니다.
암호로 보호된 압축 파일 검사	이 확인란을 선택하면 애플리케이션이 암호가 걸려 있는 압축 파일을 검사합니다. 압축 파일 내의 파일을 검사하기 전에 먼저 암호 입력 화면이 표시됩니다. 이 확인란을 선택 해제하면 애플리케이션이 암호가 걸려 있는 압축 파일의 검사를 건너뜁니다.
큰 복합 파일은 압축 해제 안 함	이 확인란을 선택하면 애플리케이션이 지정된 크기를 초과하는 복합 파일을 검사하지 않습니다. 이 확인란을 선택하지 않으면 애플리케이션이 크기에 자격 증명 공급업체이 모든 파일을 검사합니다. 애플리케이션은 확인란의 선택 여부와 관계없이 압축 파일에서 압축 해제한 대용량 파일을 검사합니다.
머신 러닝 및 시그니처 분석	머신 러닝 및 시그니처 분석 기법은 알려진 위협과 이를 처리하는 방법에 대한 설명이 포함된 Kaspersky Endpoint Security 데이터베이스를 사용합니다. 이 방법을 사용하는 보호는 허용되는 최소한의 보안 레벨을 제공합니다. Kaspersky 전문가의 권고에 따라 기본적으로 머신 러닝과 시그니처 분석이 사용되도록 선택되어 있습니다.
휴리스틱 분석	현재 버전의 Kaspersky 애플리케이션 데이터베이스를 사용하여 식별할 수 없는 위협을 탐지하기 위해 개발된 기술입니다. 알려지지 않은 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 파일을 탐지합니다. 파일에서 악성 코드를 검사할 때 휴리스틱 분석기는 실행 파일의 명령을 실행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
iSwift 기술 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.
iChecker 기술 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.

이동식 장치가 컴퓨터에 연결될 때 검사

Kaspersky Endpoint Security는 이동식 드라이브에 있는 파일을 포함하여 사용자가 실행하거나 복사하는 모든 파일을 검사합니다(파일 위협 보호 구성 요소). 이동식 드라이브를 컴퓨터에 연결했을 때 자동으로 검사하도록 구성하여 바이러스 및 기타 악성 코드의 확산을 방지할 수 있습니다. Kaspersky Endpoint Security가 탐지된 모든 감염 파일을 자동으로 치료합니다. 치료에 실패할 경우 Kaspersky Endpoint Security는 파일을 삭제합니다. 이 구성 요소는 머신 러닝과 휴리스틱 분석(높음 레벨), 시그니처 분석을 구현한 검사를 실행하여 컴퓨터를 안전하게 보호합니다. 또한 Kaspersky Endpoint Security는 iSwift 및 iChecker 검사 최적화 기술도 사용합니다. 이 기술은 항상 켜져 있으며 비활성화할 수 없습니다.

관리 콘솔(MMC)에서 이동식 드라이브 검사 실행을 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 작업 → 이동식 드라이브 검사**를 선택합니다.
4. **이동식 드라이브 연결 시 처리 방법** 드롭다운 목록에서 **상세 검사** 또는 **빠른 검사**를 선택합니다.
5. 이동식 드라이브 검사에 대한 고급 옵션을 구성합니다(아래 표 참조).
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 이동식 드라이브 검사 실행을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 이동식 드라이브 검사**로 갑니다.
5. **이동식 드라이브 검사 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.
6. **검사 유형** 블록에서 **상세 검사** 또는 **빠른 검사**를 선택합니다.
7. 이동식 드라이브 검사에 대한 고급 옵션을 구성합니다(아래 표 참조).
8. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 이동식 드라이브 검사 실행을 구성하는 방법

1. 메인 애플리케이션 창에서 **작업** 섹션으로 이동합니다.
2. 작업 목록에서 검사 작업을 선택하고 ⚙ 클릭합니다.
3. **이동식 드라이브 검사** 토글로 컴퓨터에 이동식 드라이브 연결 시 검사를 사용하거나 중지합니다.
4. 이동식 드라이브 검사에 대한 고급 옵션을 구성합니다(아래 표 참조).
5. 변경 사항을 저장합니다.

결과적으로 Kaspersky Endpoint Security는 지정한 최대 크기보다 작은 이동식 드라이브에 대해 이동식 드라이브 검사를 실행합니다. *이동식 드라이브 검사* 작업이 표시되지 않는다면 관리자가 정책에서 로컬 작업 사용을 금지했다는 뜻입니다.

파라미터	설명
검사 유형	**상세 검사**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 이동식 드라이브가 연결될 때 복합 개체, 압축 파일, 배포 패키지, Office 형식 파일 내에 중첩된 파일을 포함하여 모든 파일을 검사합니다. Kaspersky Endpoint Security는 메일 형식의 파일이나 암호로 보호된 압축 파일은 검사하지 않습니다. **빠른 검사**. 이 옵션을 선택하면 이동식 드라이브가 연결된 후 Kaspersky Endpoint Security가 감염에 가장 취약한 특정 형식을 가진 파일만 검사하고 복합 개체의 압축을 풀지 않습니다.
최대 드라이브 크기(MB)	이 확인란을 선택하면 Kaspersky Endpoint Security가 지정된 최대 드라이브 크기보다 작은 이동식 드라이브를 대상으로 선택한 작업을 수행합니다. 이동식 드라이브의 크기가 구성된 값을 초과하면 Kaspersky Endpoint Security가 검사를 건너뜁니다. 이 확인란을 선택 해제하면 Kaspersky Endpoint Security가 모든 크기의 이동식 드라이브를 대상으로 선택한 작업을 수행합니다.
검사 진행률 표시줄 숨기기	이 확인란을 선택하면 Kaspersky Endpoint Security가 별도의 창과 **작업** 섹션에서 이동식 드라이브 검사의 진행률을 표시합니다. 이 확인란의 선택을 취소하면 Kaspersky Endpoint Security가 백그라운드에서 이동식 드라이브 검사를 수행합니다.
사용자의 검사 중지 방지	이 확인란을 선택하면 Kaspersky Endpoint Security의 로컬 인터페이스에서 이동식 드라이브 검사 작업 시, **작업** 섹션의 **중지** 버튼과 이동식 드라이브 검사 창의 **중지** 버튼을 사용할 수 없습니다.

백그라운드 검사

*백그라운드 검사*는 사용자에 대한 알림을 표시하지 않는 Kaspersky Endpoint Security의 검사 모드입니다. 백그라운드 검사는 다른 유형의 검사(예: 전체 검사)보다 적은 컴퓨터 리소스를 사용합니다. 이 모드에서 Kaspersky Endpoint Security는 시작 개체, 부트 섹터, 시스템 메모리 및 시스템 파티션을 검사합니다.

컴퓨터 리소스를 절약하려면 전체 검사 작업 대신 백그라운드 검사 작업을 사용하는 것이 좋습니다. 이는 컴퓨터의 보안 레벨에 영향을 주지 않습니다. 이 작업은 검사 범위가 같습니다. 컴퓨터 부하 최적화를 위해 애플리케이션은 전체 검색 작업과 백그라운드 검색 작업을 동시에 실행하지 않습니다. 전체 검사 작업을 이미 실행했다면 Kaspersky Endpoint Security는 전체 검사 작업 완료 후 7일간 백그라운드 검사 작업을 시작하지 않습니다.

백그라운드 검사는 다음과 같은 경우에 시작됩니다:

- 안티 바이러스 데이터베이스 업데이트 후.
- Kaspersky Endpoint Security가 시작되고 30분 후.
- 매 6시간마다.
- 컴퓨터가 5분 이상 유휴 상태일 때(컴퓨터가 잠겨 있거나 화면 보호기가 켜져 있음).

다음 조건 중 하나가 참일 경우, 컴퓨터가 유휴 상태에서 백그라운드 검사가 중단됩니다:

- 컴퓨터가 활성 모드로 전환된 경우.

  > 백그라운드 검사를 10일 이상 실행하지 않은 경우 해당 검사는 중단됨.

- 컴퓨터(노트북)가 배터리 모드로 전환된 경우.

> 백그라운드 검사 작업을 수행할 때 Kaspersky Endpoint Security는 컨텐츠가 OneDrive 클라우드 스토리지에 있는 파일을 검사하지 않습니다.

관리 콘솔(MMC)에서 백그라운드 검사를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **로컬 작업 → 백그라운드 검사**를 선택합니다.
4. **백그라운드 검사 사용** 확인란으로 백그라운드 검사를 활성화 또는 비활성화합니다.
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 백그라운드 검사를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 파일 위협 보호**로 갑니다.
5. **백그라운드 검사**에서 **백그라운드 검사 활성화됨** 토글 스위치를 사용하여 백그라운드 검사를 활성화 또는 비활성화합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 백그라운드 검사를 활성화하는 방법

1. 메인 애플리케이션 창에서 **작업** 섹션으로 이동합니다.
2. 작업 목록에서 검사 작업을 선택하고 ⚙ 클릭합니다.
3. **백그라운드 검사** 토글로 백그라운드 검사를 사용하거나 중지합니다.
4. 변경 사항을 저장합니다.

*백그라운드 검사*가 표시되지 않는다면 관리자가 정책에서 로컬 작업 사용을 금지했다는 뜻입니다.

마우스 오른쪽 메뉴에서 검사

Kaspersky Endpoint Security에서는 마우스 오른쪽 메뉴를 통해 바이러스 및 기타 악성 코드를 검사하는 개별 파일 검사를 실행할 수 있습니다.

마우스 오른쪽 메뉴에서 검사를 수행할 때 Kaspersky Endpoint Security는 컨텐츠가 OneDrive 클라우드 저장소에 있는 파일을 검사하지 않습니다.



마우스 오른쪽 메뉴에서 검사

관리 콘솔(MMC)에서 마우스 오른쪽 메뉴 검사를 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 작업 → 마우스 오른쪽 메뉴에서 검사**를 선택합니다.
4. 마우스 오른쪽 메뉴에서 검사를 구성합니다(아래 표 참조).
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 마우스 오른쪽 메뉴 검사를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 파일 위협 보호**로 갑니다.
5. **마우스 오른쪽 메뉴에서 검사**에서 마우스 오른쪽 메뉴에서 검사를 구성합니다(아래 표 참조).
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 마우스 오른쪽 메뉴 검사를 구성하는 방법

1. 메인 애플리케이션 창에서 **작업** 섹션으로 이동합니다.
2. 작업 목록에서 검사 작업을 선택하고 ⚙ 클릭합니다.

3. 마우스 오른쪽 메뉴에서 검사를 구성합니다(아래 표 참조).

4. 변경 사항을 저장합니다.

마우스 오른쪽 메뉴에서 검사 작업이 표시되지 않는다면 관리자가 정책에서 로컬 작업 사용을 금지했다는 뜻입니다.

마우스 오른쪽 메뉴에서 검사 작업 설정

파라미터	설명
보안 레벨	Kaspersky Endpoint Security는 다양한 설정 그룹을 사용해 검사를 실행할 수 있습니다. 애플리케이션에 저장된 설정 집합을 *보안 레벨*이라고 합니다: • **높음**. Kaspersky Endpoint Security는 모든 유형의 파일을 검사합니다. 복합 파일을 검사할 때 애플리케이션은 압축 파일, 배포 패키지, 오피스 형식의 파일을 검사하지만, 암호가 걸린 압축 파일은 검사하지 않습니다. 이 보안 레벨을 설정하면 애플리케이션은 휴리스틱 분석과 **정밀 검사** 세부 정보 수준을 사용합니다. • **권장**. Kaspersky Endpoint Security는 모든 유형의 파일을 검사합니다. 복합 파일을 검사할 때 애플리케이션은 압축 파일, 배포 패키지, 오피스 형식의 파일을 검사하지만, 암호가 걸린 압축 파일은 검사하지 않습니다. 이 보안 레벨을 설정하면 애플리케이션이 휴리스틱 분석과 **보통 검사** 세부 정보 수준을 사용합니다. • **낮음**. Kaspersky Endpoint Security가 지정된 파일 형식만 검사합니다. 복합 파일을 검사할 때 애플리케이션은 압축 파일, 배포 패키지, 오피스 형식의 파일을 검사하지만, 암호가 걸린 압축 파일은 검사하지 않습니다. 이 보안 레벨을 설정하면 애플리케이션이 휴리스틱 분석과 **빠른 검사** 세부 정보 수준을 사용합니다.
위협 탐지 시 처리 방법	**치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다. **치료 - 불가능한 경우 알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 탐지된 모든 감염을 자동으로 치료합니다. 치료 실패 시 Kaspersky Endpoint Security는 탐지된 감염 파일에 대한 정보를 처리 안 된 위협 목록에 추가합니다. **알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 감염된 파일에 대한 정보를 해당 파일 탐지 시 처리 안 된 위협 목록에 추가합니다.
파일 유형	Kaspersky Endpoint Security는 확장자가 없는 파일을 실행 파일로 간주합니다. 애플리케이션은 검사하도록 선택한 파일 형태에 상관없이 항상 실행 파일을 검사합니다. **모든 파일**. 이 설정을 사용하면 Kaspersky Endpoint Security가 예외 없이 모든 형식과 확장자의 파일을 검사합니다. **형식에 따라 검사한 파일**. 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일에 악성 코드가 있는지 검사하기 전에 파일의 내부 헤더를 분석하여 파일 형식을 결정합니다(예: txt, .doc 또는 .exe). 또한 이 검사에서는 특정 파일 확장자를 가진 파일도 찾습니다. **확장자에 따라 검사한 파일** 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일 형식은 파일 확장자를 기반으로 결정됩니다. Kaspersky Endpoint Security는 기본적으로 파일 유형으로 파일을 검사합니다. 확장자로 파일 검색 시 악성 파일이 감염 가능 확장자 목록에 없는 확장자를 취할 수 있으므로(예: `.123`) 안전성이 떨어집니다.
새로운 파일과 수정된 파일만 검사	새로운 파일과 마지막 검사 이후 수정된 파일만 검사합니다. 이는 검사 시간을 줄이는 것입니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.
다음보다 오래 검사하는 파일은 건너뛰기: N초	작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.
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 배포 패키지의 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. 애플리케이션이 확인란 선택 여부와 상관없이 1MB보다 작은 오피스 형식 파일을 검사합니다.

파라미터	설명
이메일 형식 파일 검사	이메일 형식 파일 및 이메일 데이터베이스 검사. 이 애플리케이션은 MS Outlook 및 Windows Mail 메일 클라이언트에서 사용하는 PST 및 OST 파일과 EML 파일을 검색합니다. Kaspersky Endpoint Security는 64비트 버전의 Microsoft Outlook 이메일 클라이언트를 지원하지 않습니다. 따라서 Kaspersky Endpoint Security는 64비트 버전의 Microsoft Outlook이 컴퓨터에 설치된 경우 메일이 검사 범위에 포함되어도 Microsoft Outlook 파일(PST 및 OST 파일)을 검사하지 않습니다. 이 확인란을 선택하면 Kaspersky Endpoint Security가 메일 형식 파일을 각 구성 요소로 나누고(헤더, 본문, 첨부파일) 각각의 보안위협을 검사합니다. 이 확인란을 선택 취소하면 Kaspersky Endpoint Security가 메일 형식 파일을 단일 파일로 검사합니다. PST 또는 OST 파일에서 악성 개체가 탐지되면 Kaspersky Endpoint Security는 선택한 작업(예: 파일 치료 또는 삭제)에 따라 해당 개체를 무해한 상태로 만듭니다. 다른 메일 클라이언트(예: Mozilla Thunderbird)의 파일에서 악성 파일이 탐지되면 Kaspersky Endpoint Security는 감염된 메시지를 표시만 합니다. 첨부 파일의 감염된 메시지를 직접 삭제해야 합니다.
암호로 보호된 압축 파일 검사	이 확인란을 선택하면 애플리케이션이 암호가 걸려 있는 압축 파일을 검사합니다. 압축 파일 내의 파일을 검사하기 전에 먼저 암호 입력 화면이 표시됩니다. 이 확인란을 선택 해제하면 애플리케이션이 암호가 걸려 있는 압축 파일의 검사를 건너뜁니다.
큰 복합 파일은 압축 해제 안 함	이 확인란을 선택하면 애플리케이션이 지정된 크기를 초과하는 복합 파일을 검사하지 않습니다. 이 확인란을 선택하지 않으면 애플리케이션이 크기에 자격 증명 공급업체이 모든 파일을 검사합니다. 애플리케이션은 확인란의 선택 여부와 관계없이 압축 파일에서 압축 해제한 대용량 파일을 검사합니다.
머신 러닝 및 시그니처 분석	머신 러닝 및 시그니처 분석 기법은 알려진 위협과 이를 처리하는 방법에 대한 설명이 포함된 Kaspersky Endpoint Security 데이터베이스를 사용합니다. 이 방법을 사용하는 보호는 허용되는 최소한의 보안 레벨을 제공합니다. Kaspersky 전문가의 권고에 따라 기본적으로 머신 러닝과 시그니처 분석이 사용되도록 선택되어 있습니다.
휴리스틱 분석	현재 버전의 Kaspersky 애플리케이션 데이터베이스를 사용하여 식별할 수 없는 위협을 탐지하기 위해 개발된 기술입니다. 알려지지 않은 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 파일을 탐지합니다. 파일에서 악성 코드를 검사할 때 휴리스틱 분석기는 실행 파일의 명령을 실행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
iSwift 기술	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.
iChecker 기술	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.

애플리케이션 무결성 검사

Kaspersky Endpoint Security는 그 애플리케이션 모듈의 손상 및 변경 여부를 확인합니다. 예를 들어, 애플리케이션 라이브러리에 잘못된 디지털 서명이 포함되어 있으면 이 라이브러리는 손상된 것으로 간주됩니다. *애플리케이션 무결성 검사* 작업은 애플리케이션 파일을 확인하기 위해 수행됩니다. Kaspersky Endpoint Security가 악성 개체를 탐지했으나 처리하지 않은 경우 *애플리케이션 무결성 검사* 작업을 실행하십시오.

애플리케이션 무결성 검사 작업은 Kaspersky Security Center 웹 콘솔 및 관리 콘솔에서 생성할 수 있습니다. Kaspersky Security Center Cloud Console에서는 작업을 생성할 수 없습니다.

다음과 같은 경우에 애플리케이션 무결성 위반이 발생할 수 있습니다:

- 악성 개체가 Kaspersky Endpoint Security 파일을 수정했습니다. 이 경우, 운영 체제의 도구를 사용하여 Kaspersky Endpoint Security 복원 절차를 수행하십시오. 복원이 완료되면 컴퓨터에 대한 전체 검사를 실행하고 무결성 검사를 반복합니다.
- 디지털 서명이 만료되었습니다. 이 경우 Kaspersky Endpoint Security를 업데이트하십시오.

관리 콘솔(MMC)을 통해 애플리케이션 무결성 검사를 실행하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **애플리케이션 무결성 검사**를 선택합니다.

2단계. 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.

3 단계. 작업 시작 스케줄 구성

작업 시작 스케줄(예: 직접 또는 바이러스 발생이 탐지될 때)을 구성하십시오.

4단계. 작업 이름 정의

작업 이름을 입력합니다(예: *컴퓨터가 감염된 후 무결성 검사*).

5단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다. 그러면 Kaspersky Endpoint Security에서 애플리케이션의 무결성을 검사합니다. 작업 속성에서 애플리케이션 무결성 검사 스케줄을 구성할 수도 있습니다(아래 표 참조).

웹 콘솔을 통해 애플리케이션 무결성 검사를 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **애플리케이션 무결성 검사**를 선택합니다.
   c. **작업 이름** 필드에 간략한 설명을 입력합니다(예: *컴퓨터 감염 후 애플리케이션에 대한 무결성 검사*).
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.
5. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.
6. 마법사를 끝냅니다.
   작업 목록에 새 작업이 표시됩니다.
7. 작업 옆의 확인란을 선택합니다.

그러면 Kaspersky Endpoint Security에서 애플리케이션의 무결성을 검사합니다. 작업 속성에서 애플리케이션 무결성 검사 스케줄을 구성할 수도 있습니다(아래 표 참조).

애플리케이션 인터페이스에서 무결성 검사를 실행하는 방법

1. 메인 애플리케이션 창에서 **작업** 섹션으로 이동합니다.
2. 작업 목록이 열리면 *애플리케이션 무결성 검사* 작업을 선택하고 **실행**을 클릭합니다.

그러면 Kaspersky Endpoint Security에서 애플리케이션의 무결성을 검사합니다. 작업 속성에서 애플리케이션 무결성 검사 스케줄을 구성할 수도 있습니다(아래 표 참조). *애플리케이션 무결성 검사* 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

파라미터	설명
검사 스케줄	**수동**. 편리한 시간에 검사를 수동으로 시작할 수 있는 실행 모드입니다. **스케줄에 따라**. 이 검사 작업 스케줄에서는 애플리케이션이 사용자가 만드는 스케줄에 따라 검사 작업을 시작합니다. 이 검사 작업 스케줄이 선택되면 검사 작업을 수동으로 시작할 수도 있습니다.
건너뛴 작업 실행	이 확인란을 선택하면, Kaspersky Endpoint Security는 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 Endpoint Security가 건너뛴 작업을 실행하지 않습니다. 대신, 현재 스케줄에 따라 다음 작업을 실행합니다.
컴퓨터가 유휴 상태일 때만 실행	컴퓨터 리소스가 사용 중일 때 작업 시작을 연기했습니다. Kaspersky Endpoint Security는 컴퓨터가 잠겨 있거나 화면 보호기가 켜져 있을 때 검사 작업을 시작합니다. 예를 들어 컴퓨터를 잠금 해제하는 등으로 작업 실행이 중단되면 Kaspersky Endpoint Security는 자동으로 중단된 지점부터 작업을 실행합니다. 이 예약 옵션을 사용하면 컴퓨터를 사용할 때 컴퓨터 리소스를 절약할 수 있습니다.

검사 범위 편집

*검사 범위*는 Kaspersky Endpoint Security가 작업을 실행할 때 검색하는 폴더 및 경로에 대한 경로 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.

검사 범위를 편집하려면 *사용자 지정 검사* 작업을 사용할 것을 권장합니다. Kaspersky 전문가는 *전체 검사* 및 *중요 영역 검사* 작업의 검사 범위를 변경하지 않을 것을 권장합니다.

Kaspersky Endpoint Security의 검사 범위에는 다음과 같은 사전 정의된 개체가 포함됩니다.

- **시스템 메모리**.
- **실행 중인 프로세스 및 시작 개체**.
  시스템 시작 시 실행되는 프로세스 및 애플리케이션 실행 파일이 차지하는 메모리.
- **디스크 부트 섹터**.
  하드 디스크 및 이동식 디스크 부트 섹터.
- **시스템 백업**.
  시스템 볼륨 정보 폴더의 컨텐츠.
- **모든 외부 장치**.
- **모든 하드 드라이브**.
- **모든 네트워크 드라이브**.

Kaspersky Endpoint Security for Windows 12.12에서는 이메일은 애플리케이션 검사 범위에서 제외됩니다. 수신 및 발신되는 이메일 메시지의 검사는 메일 위협 보호 구성 요소에서 수행합니다. 이전 버전의 관리 플러그인을 사용하는 경우 애플리케이션은 정책에 포함되어 있더라도 이메일을 검사 범위에서 제외합니다.

네트워크 드라이브 또는 공유 폴더를 검사하기 위해 별도의 검사 작업을 생성하는 것이 좋습니다. *악성 코드 검사* 작업 설정에서는 사용자에게 이 드라이브에 대한 쓰기 권한을 지정합니다. 이는 탐지된 위협을 완화하는 데 필요합니다. 네트워크 드라이브가 있는 서버에 자체 보안 도구가 있는 경우 해당 드라이브에 검사 작업을 실행하지 마십시오. 이렇게 하면 개체를 두 번 확인하지 않고도 서버 성능을 향상시킬 수 있습니다.

검사 범위에서 폴더 또는 파일을 제외하려면 폴더 또는 파일을 신뢰 구역에 추가합니다.

관리 콘솔(MMC)에서 검사 범위를 편집하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업**을 선택합니다.
3. 검사 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.
   필요하다면 *악성 코드 검사* 작업을 생성합니다.
4. 작업 속성 창에서 **설정** 섹션을 선택합니다.
5. **검사 범위** 섹션에서, **설정**을 클릭합니다.
6. 창이 열리면 검사 범위에 추가하거나 제외할 개체를 선택합니다.
7. 검사 범위에 새로운 개체를 추가하려면 다음과 같이 하십시오.
   a. **추가**를 클릭합니다.
   b. **개체** 필드에서 폴더 또는 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.

      파일 또는 폴더 경로 어디서든 마스크를 사용할 수 있습니다. 예를 들어, 컴퓨터에 있는 모든 사용자 계정의 다운로드 폴더를 검사 범위에 포함시키려면 `C:\Users\*\Downloads\` 마스크를 입력합니다.

      컴퓨터 내 파일 리소스 목록의 **내 PC** 개체는 **모든 하드 드라이브**, **모든 네트워크 드라이브**, **모든 이동식 드라이브**를 포함합니다.

   검사 범위의 개체 목록에서 개체를 삭제하지 않고도 검사에서 개체를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.
8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 검사 범위를 편집하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. 검사 작업을 클릭합니다.
   작업 속성 창이 열립니다. 필요하다면 *악성 코드 검사* 작업을 생성합니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **검사 범위** 섹션에서 검사 범위에 추가하거나 제외할 개체를 선택합니다.

5. 검사 범위에 새로운 개체를 추가하려면 다음과 같이 하십시오.

   a. **추가**를 클릭합니다.

   b. 폴더 또는 파일 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.

      파일 또는 폴더 경로 어디서든 마스크를 사용할 수 있습니다. 예를 들어, 컴퓨터에 있는 모든 사용자 계정의 다운로드 폴더를 검사 범위에 포함시키려면 `C:\Users\*\Downloads\` 마스크를 입력합니다.

   검사 범위의 개체 목록에서 개체를 삭제하지 않고도 검사에서 개체를 제외할 수 있습니다. 이렇게 하려면 옆의 토글 스위치를 끄기로 설정합니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 검사 범위를 편집하는 방법

1. 메인 애플리케이션 창에서 **작업** 섹션으로 이동합니다.

2. 작업 목록이 열리면 *사용자 지정 검사* 작업을 선택하고 **선택**을 클릭합니다.
   다른 작업에 대한 검사 범위를 편집할 수도 있습니다. Kaspersky 전문가는 *전체 검사* 및 *중요 영역 검사* 작업의 검사 범위를 변경하지 않을 것을 권장합니다.

3. 창이 열리면 검사 범위에 추가할 개체를 선택합니다.

4. 변경 사항을 저장합니다.

검사 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

스케줄된 검사 실행

악성 코드 검사 작업을 사용하여 악성 코드 검사하는 과정은 시간이 오래 걸릴 수 있으며 Kaspersky Endpoint Security의 컴퓨터 리소스 사용량이 증가할 수 있습니다. 따라서 다른 애플리케이션의 성능에 미치는 영향을 최소화할 수 있는 최적의 작업 실행 시간을 선택하는 것이 좋습니다.

예를 들어 조직의 직원이 고정된 스케줄에 따라 작업하는 경우 야간이나 주말에 컴퓨터 검사를 실행하도록 구성할 수 있습니다. 컴퓨터의 전원이 켜져 있지 않는 등의 이유로 작업을 실행할 수 없는 경우 컴퓨터의 전원이 켜지면 건너뛴 작업을 자동으로 시작하도록 구성할 수 있습니다. 이 기능을 사용하면 아침에 사용자 컴퓨터의 전원을 켤 때 해당 컴퓨터의 애플리케이션 속도가 저하될 수 있으므로 주의하여 사용해야 합니다.

필요에 맞는 최적의 검사 스케줄을 결정할 수 없는 경우 다음 특수 조건 중 하나를 충족할 때 검사를 실행하도록 구성할 수 있습니다.

- 데이터베이스 업데이트 후.

  Kaspersky Endpoint Security는 업데이트된 서명 데이터베이스로 컴퓨터 검사를 실행합니다.

- 애플리케이션 시작 후.

  Kaspersky Endpoint Security는 애플리케이션 시작 후 지정된 시간이 경과하면 컴퓨터 검사를 실행합니다. 운영 체제 시작 시 많은 프로세스가 실행 중이므로 Kaspersky Endpoint Security 시작 직후에 검사 작업을 실행하는 것보다 검사 작업을 잠시 연기하는 것이 좋습니다.

- Wake-on-LAN 기능.

  Kaspersky Endpoint Security는 컴퓨터의 전원이 꺼져 있어도 스케줄에 따라 컴퓨터 검사를 실행합니다. 이를 위해 애플리케이션은 운영 체제의 Wake-on-LAN 기능을 사용합니다. Wake-on-LAN 기능을 사용하면 로컬 네트워크를 통해 특수 신호를 보내 원격으로 컴퓨터 전원을 켤 수 있습니다. 이 기능을 사용하려면 BIOS 설정에서 Wake-on-LAN을 활성화해야 합니다.

  Kaspersky Security Center에서 Wake-on-LAN을 사용하여 검사 실행을 구성할 수 있으며 *악성 코드 검사* 작업만 가능합니다. 애플리케이션 인터페이스에서는 컴퓨터 검사를 위해 Wake-on-LAN을 활성화할 수 없습니다.

- 컴퓨터가 유휴 상태일 때.

  Kaspersky Endpoint Security는 화면 보호기가 활성화 중이거나 화면이 잠겨 있을 때 스케줄에 따라 컴퓨터 검사를 실행합니다. 사용자가 컴퓨터의 잠금을 해제하면 Kaspersky Endpoint Security가 검사를 일시 중지합니다. 이 경우 전체 검사를 완료하는 데 며칠이 걸릴 수 있습니다.

- 작업을 건너뛰었을 때.

  Kaspersky Endpoint Security는 건너뛴 작업을 실행할 수 있게 되면 곧바로 작업을 실행합니다. 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.

웹 콘솔 및 Cloud Console에서 검사 스케줄을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.

   작업 목록이 열립니다.

2. 검사 작업을 클릭합니다.

   작업 속성 창이 열립니다.

3. 작업 속성 창에서 **스케줄** 탭을 선택합니다.

4. 검사 작업 스케줄을 구성합니다.

5. 선택한 빈도에 따라 작업 실행 스케줄을 지정하는 고급 설정을 구성합니다(아래 표 참조).

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 검사 스케줄을 구성하는 방법

컴퓨터에 정책이 적용되지 않을 때만 검사 스케줄을 구성할 수 있습니다. 정책이 적용되는 컴퓨터에서는 Kaspersky Security Center에서 *악성 코드 검사* 작업 스케줄을 구성할 수 있습니다.

1. 메인 애플리케이션 창에서 **작업** 섹션으로 이동합니다.

2. 작업 목록에서 검사 작업을 선택하고 ⚙ 클릭합니다.

   전체 검사, 중요 영역 검사, 무결성 검사 실행 스케줄을 구성할 수 있습니다. 사용자 지정 검사는 수동으로만 실행할 수 있습니다.

3. **검사 스케줄**을 클릭합니다.

4. 창이 열리면 검사 작업 실행 스케줄을 구성합니다.

5. 선택한 빈도에 따라 작업 실행 스케줄을 지정하는 고급 설정을 구성합니다(아래 표 참조).

6. 변경 사항을 저장합니다.

검사 스케줄 설정

파라미터	설명
검사 스케줄	**수동**. 편리한 시간에 검사를 수동으로 시작할 수 있는 실행 모드입니다. **스케줄에 따라**. 이 검사 작업 스케줄에서는 애플리케이션이 사용자가 만드는 스케줄에 따라 검사 작업을 시작합니다. 이 검사 작업 스케줄이 선택되면 검사 작업을 수동으로 시작할 수도 있습니다.
애플리케이션 시작 후 다음 시간 동안 작업 실행 연기: N분	애플리케이션 시작 시 일정 시간 후에 검사 작업 시작. 운영 체제 시작 시 많은 프로세스가 실행 중이므로 Kaspersky Endpoint Security 시작 직후에 검사 작업을 실행하는 것보다 검사 작업을 잠시 연기하는 것이 좋습니다.
건너뛴 작업 실행	이 확인란을 선택하면, Kaspersky Endpoint Security는 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 Endpoint Security가 건너뛴 작업을 실행하지 않습니다. 대신, 현재 스케줄에 따라 다음 작업을 실행합니다.
컴퓨터가 유휴 상태일 때만 실행	컴퓨터 리소스가 사용 중일 때 작업 시작을 연기했습니다. Kaspersky Endpoint Security는 컴퓨터가 잠겨 있거나 화면 보호기가 켜져 있을 때 검사 작업을 시작합니다. 예를 들어 컴퓨터를 잠금 해제하는 등으로 작업 실행이 중단되면 Kaspersky Endpoint Security는 자동으로 중단된 지점부터 작업을 실행합니다. 이 예약 옵션을 사용하면 컴퓨터를 사용할 때 컴퓨터 리소스를 절약할 수 있습니다.
랜덤하게 작업 시작 시간을 자동으로 조절하는 기능 사용 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	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.
작업이 다음 시간보다 오래 실행되면 중지(분) *(Kaspersky Security Center 콘솔에서만 사용 가능)*	작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다. 작업 실행 시간을 줄이기 위해 검사 범위 구성이나 검사 최적화 등을 수행할 수 있습니다.

파라미터	설명
작업 시작 전에 Wake-on-LAN 기능으로 장치 켜기(분) *(Kaspersky Security Center 콘솔에서만 사용 가능)*	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 장치 종료 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	예를 들어, 이 기능을 활성화하면 근무 시간이 끝난 금요일에 컴퓨터를 스캔할 수 있습니다. 작업이 완료되면 애플리케이션이 주말 동안 컴퓨터를 끕니다.

다른 사용자로 검사 실행

기본적으로 검사 작업이 운영 체제에 등록된 권한을 가진 사용자의 이름으로 실행됩니다. 보호 범위에는 특수 접근 권한이 필요한 네트워크 드라이브 또는 기타 개체가 포함될 수 있습니다. 애플리케이션 설정에서 필요한 권한이 있는 사용자를 지정하여 이 사용자의 계정으로 검사 작업을 실행할 수 있습니다.

다른 사용자로 다음 검사를 실행할 수 있습니다.

- 중요 영역 검사
- 전체 검사.
- 사용자 지정 검사
- 마우스 오른쪽 메뉴에서 검사

이동식 드라이브 검사, 백그라운드 검사, 무결성 검사 실행에 대해서는 사용자 권한을 구성할 수 없습니다.

관리 콘솔(MMC)에서 다른 사용자로 검사를 실행하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **작업** 탭을 선택합니다.
4. 검사 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.
5. 작업 속성 창에서 **계정** 섹션을 선택합니다.
6. 검사 작업을 실행하는 데 사용할 권한이 있는 사용자의 계정 자격 증명을 입력합니다.
7. 변경 사항을 저장합니다.

웹 콘솔 또는 Cloud Console에서 다른 사용자로 검사를 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. 검사 작업을 클릭합니다.
   작업 속성 창이 열립니다.
3. **설정** 탭을 선택합니다.
4. **계정** 블록에서 **설정** 버튼을 누릅니다.
5. 검사 작업을 실행하는 데 사용할 권한이 있는 사용자의 계정 자격 증명을 입력합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 다른 사용자로 검사를 실행하는 방법

1. 메인 애플리케이션 창에서 **작업** 섹션으로 이동합니다.
2. 작업 목록에서 검사 작업을 선택하고 ⚙ 클릭합니다.
3. 작업 속성에서 **고급 설정 → 다음으로 검사 실행**을 선택합니다.
4. 창이 열리면 검사 작업을 실행하는 데 사용할 권한이 있는 사용자의 계정 자격 증명을 입력합니다.
5. 변경 사항을 저장합니다.

검사 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

검사 최적화

컴퓨터 검사 중 CPU 사용량 제한

악성 코드 검사 작업을 실행할 때 CPU 사용량을 제한할 수 있습니다. 이는 컴퓨터를 검사하는 데 걸리는 시간을 늘릴 수 있습니다.

관리 콘솔(MMC)에서 컴퓨터를 검사할 때 CPU 사용량을 제한하는 방법

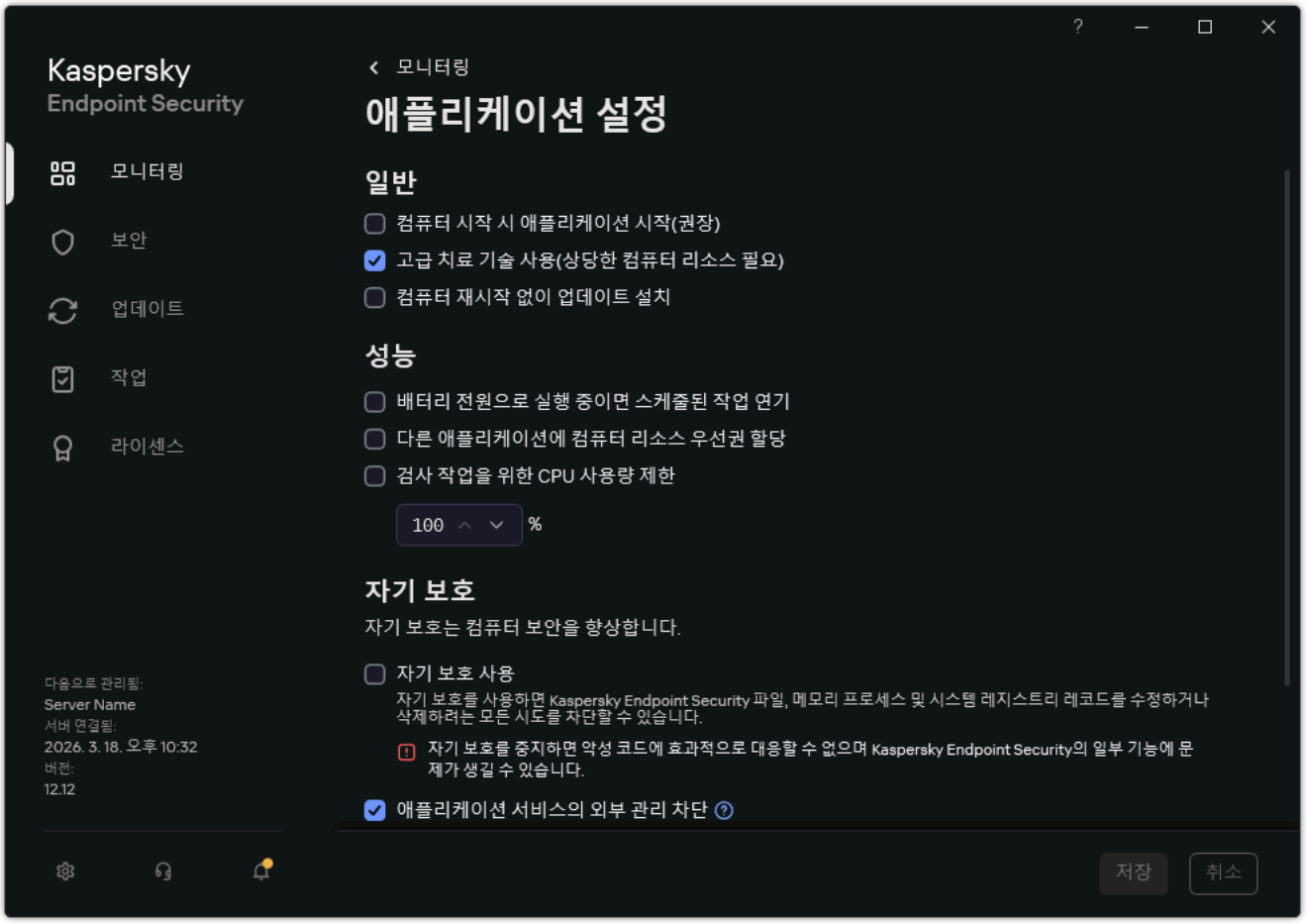
1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 애플리케이션 설정**을 차례로 선택합니다.
4. **성능**에서 **검사 작업을 위한 CPU 사용량 제한** 확인란을 선택하고 CPU 리소스 소비의 평균값을 백분율로 입력합니다.
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 컴퓨터를 검사할 때 CPU 사용량을 제한하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **성능**으로 이동합니다.
5. **검사 작업을 위한 CPU 사용량 제한**에서 **검사 작업을 위한 CPU 사용량 제한** 토글 스위치를 사용하고 CPU 리소스 소비의 평균값을 백분율로 입력합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 컴퓨터를 검사할 때 CPU 사용량을 제한하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

3. **성능**에서 **검사 작업을 위한 CPU 사용량 제한** 확인란을 선택하고 CPU 리소스 소비의 평균값을 백분율로 입력합니다.
4. 변경 사항을 저장합니다.

악성 코드 검사에 대한 고급 작업 설정을 구성합니다.

파일 검사를 최적화할 수 있습니다: 검사 시간을 단축하고 Kaspersky Endpoint Security의 작업 속도를 높일 수 있습니다. 검사 최적화는 새 파일과 마지막 검사 후 변경된 파일만 검사하는 방법으로 이루어집니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다. 단일 파일 검사에 대한 제한을 설정할 수도 있습니다. 지정한 시간이 경과되면 Kaspersky Endpoint Security는 현재 검사에서 해당 파일을 예외합니다(압축 파일 및 여러 파일로 이루어진 파일은 예외).

바이러스나 기타 악성 코드를 숨기는 일반적인 방법은 압축 파일이나 데이터베이스와 같은 복합 파일에 심는 것입니다. 이런 방법으로 숨겨진 바이러스나 기타 악성 코드를 탐지하려면 복합 파일을 압축 해제 해야 하는데 그러면 검사 속도가 느려질 수 있습니다. 검사할 복합 파일의 유형을 제한하는 방법으로 검사 속도를 높일 수 있습니다.

또한 iChecker 및 iSwift 기술을 활성화할 수 있습니다. iChecker 및 iSwift 기술은 최근에 검사된 후로 변경되지 않은 파일을 제외하여 파일 검사 속도를 최적화합니다.

관리 콘솔(MMC)에서 검사를 최적화하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업**을 선택합니다.
3. 검사 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.
   필요하다면 *악성 코드 검사* 작업을 생성합니다.
4. 작업 속성 창에서 **설정** 섹션을 선택합니다.
5. **보안 레벨** 블록에서 **설정** 버튼을 클릭합니다.
   검사 작업 설정 창이 열립니다.
6. **최적화** 블록에서 검사 설정을 구성합니다:
   - **새로운 파일과 수정된 파일만 검사**. 새로운 파일과 마지막 검사 이후 수정된 파일만 검사합니다. 이는 검사 시간을 줄이는 것입니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.
     유형별로 새 파일 검색을 구성할 수도 있습니다. 예를 들어, 배포 패키지는 모두 검사하고 압축 파일 및 오피스 형식 파일은 새로운 것만 검사할 수 있습니다.
   - **다음보다 오래 검사하는 파일은 건너뛰기: N초**. 작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.
   - **여러 검사 작업을 동시에 실행하지 않음**. 검사가 이미 실행 중이라면 검사 작업 시작을 연기합니다. Kaspersky Endpoint Security는 현재 검사가 진행 중이면 새 검사 작업을 대기열에 넣습니다. 이렇게 하면 컴퓨터 부하 최적화에 도움이 됩니다. 예를 들어 애플리케이션이 스케줄에 따라 전체 검색 작업을 시작했다고 가정해봅시다. 사용자가 애플리케이션 인터페이스에서 빠른 검사를 시작하려고 하면 Kaspersky Endpoint Security는 이 파일 검사 작업을 대기열에 넣은 후 전체 검사 작업 완료 후에 이 작업을 자동으로 시작합니다.
7. **추가**를 클릭합니다.
   복합 파일 검사 설정 창이 열립니다.

8. **크기 제한** 블록에서 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택합니다. 작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.

   Kaspersky Endpoint Security는 **큰 복합 파일은 압축 해제 안 함** 확인란의 선택 여부에 관계 없이 압축 해제된 대용량 파일을 검사합니다.

9. **확인**을 누릅니다.

10. **추가** 탭으로 갑니다.

11. **검사 기술** 블록에서 검사가 진행되는 동안 사용할 기술 이름 옆의 확인란을 선택합니다:

    - **iSwift 기술**. 이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.

    - **iChecker 기술**. 이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.

12. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 검사를 최적화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.

   작업 목록이 열립니다.

2. 검사 작업을 클릭합니다.

   작업 속성 창이 열립니다. 필요하다면 *악성 코드 검사* 작업을 생성합니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **위협 탐지 시 처리 방법** 블록에서 **새로운 파일과 수정된 파일만 검사** 확인란을 선택합니다. 새로운 파일과 마지막 검사 이후 수정된 파일만 검사합니다. 이는 검사 시간을 줄이는 것입니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.

   유형별로 새 파일 검색을 구성할 수도 있습니다. 예를 들어, 배포 패키지는 모두 검사하고 압축 파일 및 오피스 형식 파일은 새로운 것만 검사할 수 있습니다.

5. **검사 최적화** 블록에서 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택합니다. 작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.

   Kaspersky Endpoint Security는 **큰 복합 파일은 압축 해제 안 함** 확인란의 선택 여부에 관계 없이 압축 해제된 대용량 파일을 검사합니다.

6. **여러 검사 작업을 동시에 실행하지 않음** 확인란을 선택합니다. 검사가 이미 실행 중이라면 검사 작업 시작을 연기합니다. Kaspersky Endpoint Security는 현재 검사가 진행 중이면 새 검사 작업을 대기열에 넣습니다. 이렇게 하면 컴퓨터 부하 최적화에 도움이 됩니다. 예를 들어 애플리케이션이 스케줄에 따라 전체 검색 작업을 시작했다고 가정해봅시다. 사용자가 애플리케이션 인터페이스에서 빠른 검사를 시작하려고 하면 Kaspersky Endpoint Security는 이 파일 검사 작업을 대기열에 넣은 후 전체 검사 작업 완료 후에 이 작업을 자동으로 시작합니다.

7. **고급 설정** 블록에서 **다음보다 오래 검사하는 파일은 건너뛰기(초)** 확인란을 선택합니다. 작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.

8. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 검사를 최적화하는 방법

1. 메인 애플리케이션 창에서 **작업** 섹션으로 이동합니다.

2. 작업 목록에서 검사 작업을 선택하고 ⚙ 클릭합니다.

3. **고급 설정**을 클릭합니다.

4. **최적화** 블록에서 검사 설정을 구성합니다:

   - **새로운 파일과 수정된 파일만 검사**. 새로운 파일과 마지막 검사 이후 수정된 파일만 검사합니다. 이는 검사 시간을 줄이는 것입니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.

     유형별로 새 파일 검색을 구성할 수도 있습니다. 예를 들어, 배포 패키지는 모두 검사하고 압축 파일 및 오피스 형식 파일은 새로운 것만 검사할 수 있습니다.

   - **다음보다 오래 검사하는 파일은 건너뛰기: N초**. 작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.

   - **여러 검사 작업을 동시에 실행하지 않음**. 검사가 이미 실행 중이라면 검사 작업 시작을 연기합니다. Kaspersky Endpoint Security는 현재 검사가 진행 중이면 새 검사 작업을 대기열에 넣습니다. 이렇게 하면 컴퓨터 부하 최적화에 도움이 됩니다. 예를 들어 애플리케이션이 스케줄에 따라 전체 검색 작업을 시작했다고 가정해봅시다. 사용자가 애플리케이션 인터페이스에서 빠른 검사를 시작하려고 하면 Kaspersky Endpoint Security는 이 파일 검사 작업을 대기열에 넣은 후 전체 검사 작업 완료 후에 이 작업을 자동으로 시작합니다.

5. **크기 제한** 블록에서 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택합니다. 작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.

   Kaspersky Endpoint Security는 **큰 복합 파일은 압축 해제 안 함** 확인란의 선택 여부에 관계 없이 압축 해제된 대용량 파일을 검사합니다.

6. **검사 기술** 블록에서 검사가 진행되는 동안 사용할 기술 이름 옆의 확인란을 선택합니다:

- **iSwift 기술**. 이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.

- **iChecker 기술**. 이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.

7. 변경 사항을 저장합니다.

검사 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트

Kaspersky Endpoint Security의 데이터베이스 및 애플리케이션 모듈을 업데이트함으로써 컴퓨터를 최신 상태로 보호할 수 있습니다. 전 세계적으로 날마다 수많은 신종 바이러스 및 기타 형태의 악성 코드가 나타나고 있습니다. Kaspersky Endpoint Security 데이터베이스에는 위협에 대한 정보와 이를 처리하는 방법이 포함되어 있습니다. 위협을 신속하게 탐지하려면 데이터베이스 및 애플리케이션 모듈을 정기적으로 업데이트해야 합니다.

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)이 제공되지 않을 수도 있습니다.

정기적인 업데이트는 유효한 라이센스를 요구합니다. 활성화된 라이센스가 없는 경우 업데이트를 한 번만 수행할 수 있습니다.

Kaspersky 업데이트 서버에서 업데이트 패키지를 성공적으로 다운로드하려면 컴퓨터를 인터넷에 연결해야 합니다. 기본적으로 인터넷 연결 설정은 자동으로 결정됩니다. 프록시 서버를 사용할 시 프록시 서버 설정을 구성해야 합니다.

업데이트는 HTTPS 프로토콜을 통해 다운로드됩니다. HTTPS 프로토콜을 통해 업데이트를 다운로드할 수 없을 때는 HTTP 프로토콜을 통해 다운로드할 수도 있습니다.

업데이트를 수행하면 다음과 같은 개체가 다운로드되어 컴퓨터에 설치됩니다:

- Kaspersky Endpoint Security 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 Endpoint Security 데이터베이스 외에도 애플리케이션 구성 요소가 네트워크 트래픽을 가로챌 수 있도록 하는 네트워크 드라이버가 업데이트됩니다.

- 애플리케이션 모듈. Kaspersky Endpoint Security 데이터베이스 외에도 애플리케이션 모듈을 업데이트할 수 있습니다. 이 애플리케이션 모듈을 업데이트하면 Kaspersky Endpoint Security의 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 Endpoint Security 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 대한 정보는 Kaspersky Endpoint Security 리포트에 기록됩니다.

애플리케이션이 Light Agent 모드로 작동하는 경우, 애플리케이션 데이터베이스와 모듈을 업데이트할 때 특별한 고려 사항이 필요합니다.

데이터베이스 및 애플리케이션 모듈 업데이트 시나리오

Kaspersky Endpoint Security의 데이터베이스 및 애플리케이션 모듈을 업데이트함으로써 컴퓨터를 최신 상태로 보호할 수 있습니다. 전 세계적으로 날마다 수많은 신종 바이러스 및 기타 형태의 악성 코드가 나타나고 있습니다. Kaspersky Endpoint Security 데이터베이스에는 위협에 대한 정보와 이를 처리하는 방법이 포함되어 있습니다. 위협을 신속하게 탐지하려면 데이터베이스 및 애플리케이션 모듈을 정기적으로 업데이트해야 합니다.

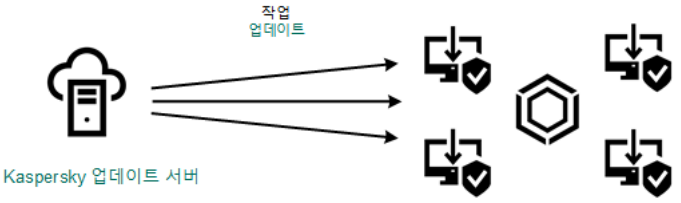
사용자 컴퓨터에서 업데이트되는 개체는 다음과 같습니다:

- 안티 바이러스 데이터베이스. 안티 바이러스 데이터베이스에는 악성 코드 서명 데이터베이스, 네트워크 공격 설명, 악성/피싱 웹 주소 데이터베이스, 배너 데이터베이스, 스팸 데이터베이스 및 기타 데이터가 포함됩니다.
- 애플리케이션 모듈. 모듈 업데이트는 애플리케이션의 취약점을 없애고 컴퓨터 보호 방법을 개선하기 위한 것입니다. 모듈 업데이트로 인해 애플리케이션 구성 요소의 동작이 변경되고 새 기능이 추가될 수 있습니다.

Kaspersky Endpoint Security는 데이터베이스 및 애플리케이션 모듈 업데이트를 위한 다음 시나리오를 지원합니다:

- Kaspersky 서버에서 업데이트.

  전 세계 여러 국가에 Kaspersky 업데이트 서버가 있습니다. 그러므로 업데이트의 신뢰성이 높습니다. 특정 서버에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 서버로 전환합니다.



Kaspersky 서버에서 업데이트

- 중앙 집중식 업데이트.

  중앙 집중식 업데이트를 수행하면 외부 인터넷 트래픽이 감소하며 업데이트를 편리하게 감시할 수 있습니다.

  중앙 집중식 업데이트는 다음 단계로 구성되어 있습니다:

  1. 조직 네트워크 내의 저장소에 업데이트 패키지를 다운로드합니다.

     업데이트 패키지는 *중앙 관리 서버 저장소에 업데이트 다운로드*라는 관리 서버 작업에 의해 저장소에 다운로드됩니다.

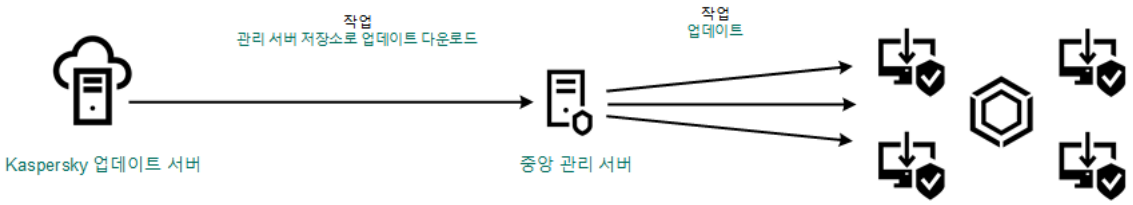
  2. 업데이트 패키지를 공유 폴더에 다운로드합니다(선택사항).

다음 방법을 사용하여 공유 폴더에 업데이트 패키지를 다운로드할 수 있습니다:

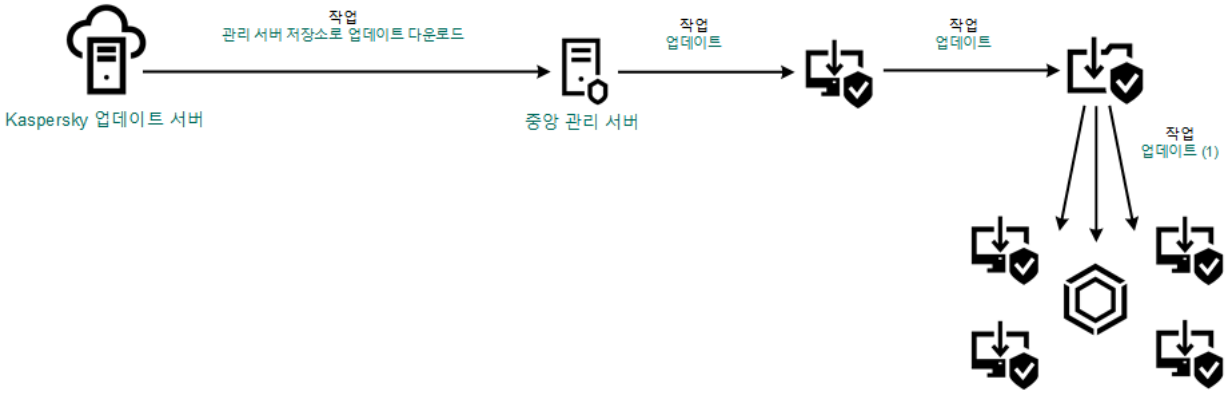
- Kaspersky Endpoint Security의 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업 사용하기. 로컬 회사 네트워크의 컴퓨터 중 한 대에서 이 작업을 수행할 수 있습니다.
- Kaspersky 업데이트 유틸리티 사용. Kaspersky 업데이트 유틸리티 사용에 대한 자세한 내용은 Kaspersky 기술 자료를 참조하십시오.

3. 클라이언트 컴퓨터로 업데이트 패키지 배포.

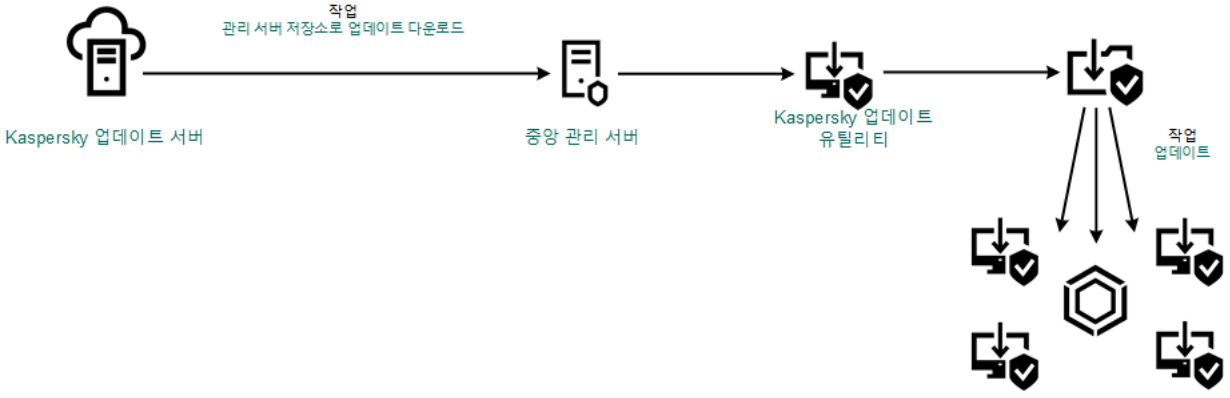
업데이트 패키지는 Kaspersky Endpoint Security *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 통해 클라이언트 컴퓨터로 배포됩니다. 각 관리 그룹에 대해 업데이트 작업을 수에 제한 없이 생성할 수 있습니다.



서버 저장소에서 업데이트



공유 폴더에서 업데이트



Kaspersky 업데이트 유틸리티를 사용하여 업데이트

Kaspersky Security Center의 경우, 기본 업데이트 경로 목록에는 Kaspersky Security Center 중앙 관리 서버 및 Kaspersky 업데이트 서버가 포함되어 있습니다. Kaspersky Security Center Cloud 콘솔의 경우 기본 업데이트 경로 목록에는 배포 지점 및 Kaspersky 업데이트 서버가 포함됩니다. 배포 지점에 대한 상세 정보는 Kaspersky Security Center Cloud Console 도움말을 참조하십시오. 다른 업데이트 경로를 목록에 추가할 수도 있습니다. 업데이트 경로는 HTTP/FTP 서버 및 공유 폴더가 될 수 있습니다. 하나의 업데이트 서버에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 업데이트 서버로 전환합니다.

업데이트는 표준 네트워크 프로토콜을 통해 Kaspersky 업데이트 서버 또는 기타 FTP/HTTP 서버에서 다운로드됩니다. 업데이트 경로에 접근하려면 프록시 서버에 연결해야 하는 경우 Kaspersky Endpoint Security 정책 설정에서 프록시 서버 설정을 지정합니다.

서버 저장소에서 업데이트

인터넷 트래픽을 절약하려는 경우 서버 저장소에서 조직 LAN의 컴퓨터에 대한 데이터베이스 및 애플리케이션 모듈 업데이트를 구성할 수 있습니다. 이렇게 하려면 Kaspersky Security Center가 Kaspersky 업데이트 서버에서 저장소(FTP/HTTP 서버, 네트워크 또는 로컬 폴더)에 업데이트 패키지를 다운로드해야 합니다. 그러면 조직 LAN의 다른 컴퓨터가 서버 저장소에서 업데이트 패키지를 받을 수 있습니다.

서버 저장소에서 데이터베이스 및 애플리케이션 모듈 업데이트를 구성하는 과정은 다음 단계로 구성됩니다:

1. 중앙 관리 서버 저장소로의 업데이트 패키지 다운로드를 구성합니다(*중앙 관리 서버 저장소에 업데이트 다운로드* 작업).

   중앙 관리 서버 빠른 시작 마법사에서 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 자동으로 생성합니다. 이 작업은 인스턴스를 하나만 포함할 수 있습니다. 기본적으로 Kaspersky Security Center는 `\\<server name>\KLSHARE\Updates` 폴더에 업데이트 패키지를 복사합니다. 중앙 관리 서버 저장소 업데이트를 다운로드하는 것에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하시기 바랍니다.

2. 지정한 서버 저장소에서 조직 LAN에 있는 나머지 컴퓨터로의 데이터베이스 및 애플리케이션 모듈 업데이트를 구성합니다(*데이터베이스 및 애플리케이션 모듈 업데이트* 작업).

   관리 콘솔(MMC)의 지정된 서버 저장소에서 Kaspersky Endpoint Security 업데이트를 구성하는 방법

   1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

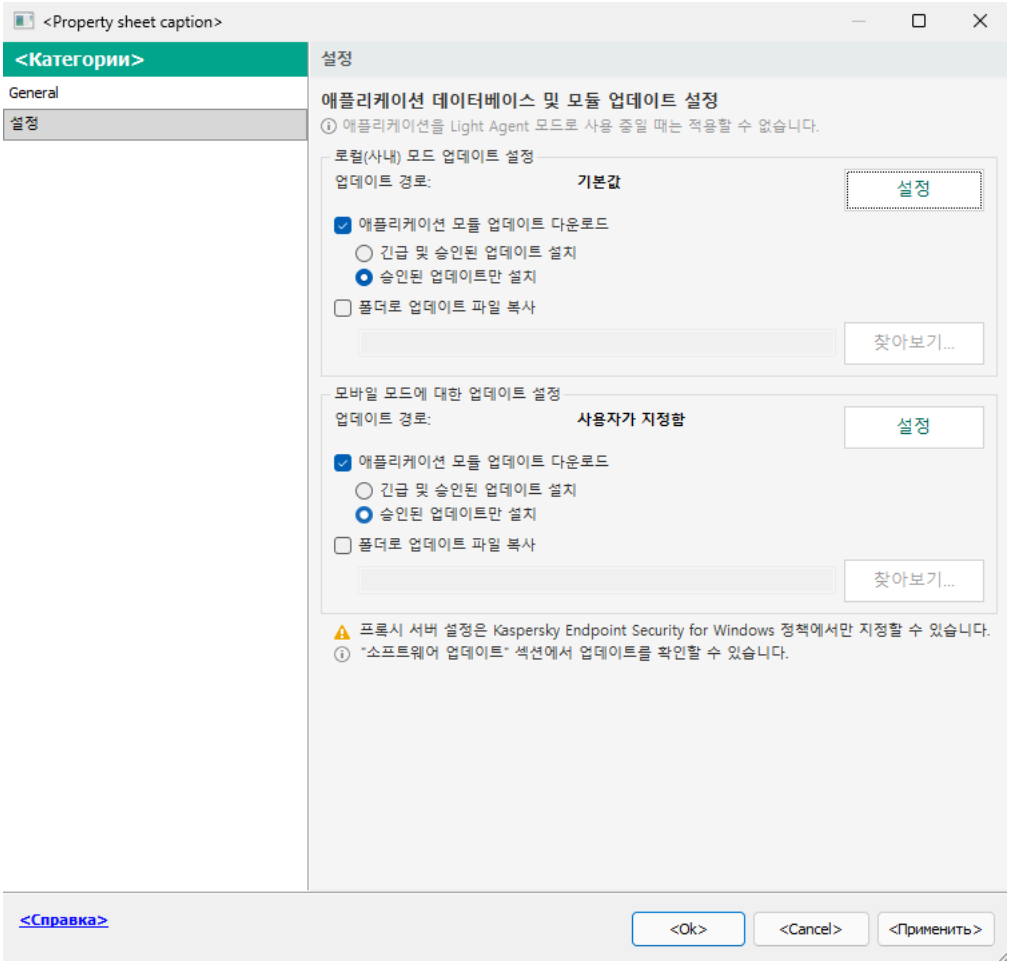
      콘솔 트리에서 **작업**을 선택합니다.

   2. Kaspersky Endpoint Security의 **데이터베이스 및 애플리케이션 모듈 업데이트** 작업을 클릭합니다.

      작업 속성 창이 열립니다.

      데이터베이스 및 애플리케이션 모듈 업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

3. 작업 속성 창에서 **설정** 섹션을 선택합니다.



데이터베이스 및 애플리케이션 모듈 업데이트 작업 설정

4. **로컬(사내) 모드 업데이트 설정** 블록에서 **설정** 버튼을 클릭합니다.

5. 업데이트 경로 목록에서 **Kaspersky Security Center** 경로 업데이트가 활성화되어 있는지 확인하십시오. 또한, **Kaspersky Security Center** 경로의 우선순위가 가장 높아야 합니다.

6. 필요하다면 다음 업데이트 경로를 추가합니다.

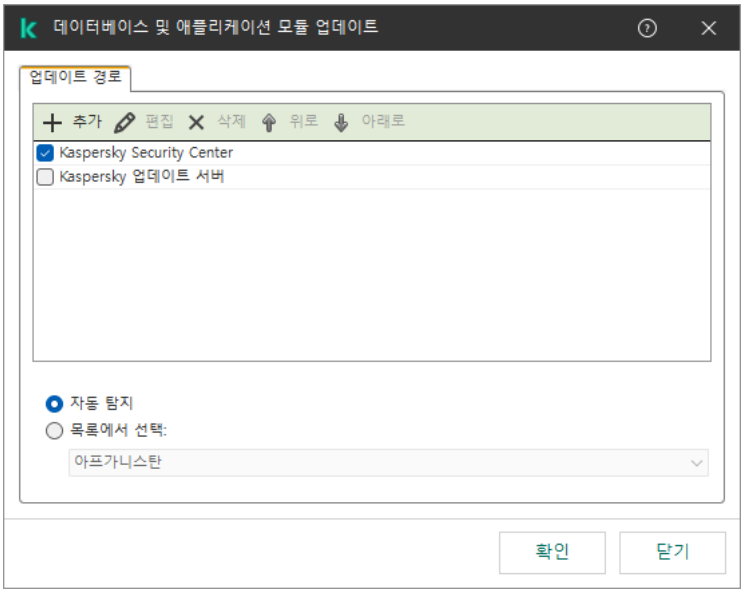
   a. 업데이트 경로 목록에서 **추가** 버튼을 누릅니다.

   b. **업데이트 경로** 필드에서 Kaspersky Security Center가 Kaspersky 서버에서 받은 업데이트 패키지를 복사하는 FTP/HTTP 서버, 네트워크 폴더 또는 로컬 폴더의 주소를 지정합니다.

   > 업데이트 경로의 주소는 서버 저장소로의 업데이트 다운로드를 구성할 때 **업데이트 저장 폴더** 필드에 지정한 주소와 일치해야 합니다(*중앙 관리 서버 저장소에 업데이트 다운로드* 작업).

   c. **확인**을 누릅니다.

업데이트 경로 목록에서 제거하지 않고 업데이트 경로를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.



업데이트 경로

7. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

   첫 번째 업데이트 경로에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 경로로 자동 전환합니다.

8. 작업 속성 창에서 **스케줄** 섹션을 선택하고 작업 실행 모드를 구성합니다.

9. 기본적으로 Kaspersky Endpoint Security는 수동 모드에서 작업을 실행합니다.

10. 변경 사항을 저장합니다.

웹 콘솔에서 지정한 서버 저장소에서의 Kaspersky Endpoint Security 업데이트를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.

   작업 목록이 열립니다.

2. Kaspersky Endpoint Security의 **업데이트** 작업을 누릅니다.

   작업 속성 창이 열립니다.

   업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

3. **애플리케이션 설정** → **로컬 모드** 탭을 선택합니다.

4. 업데이트 경로 목록에서 **Kaspersky Security Center** 경로 업데이트가 활성화되어 있는지 확인하십시오. 또한, **Kaspersky Security Center** 경로의 우선순위가 가장 높아야 합니다.

5. 필요하다면 다음 업데이트 경로를 추가합니다.

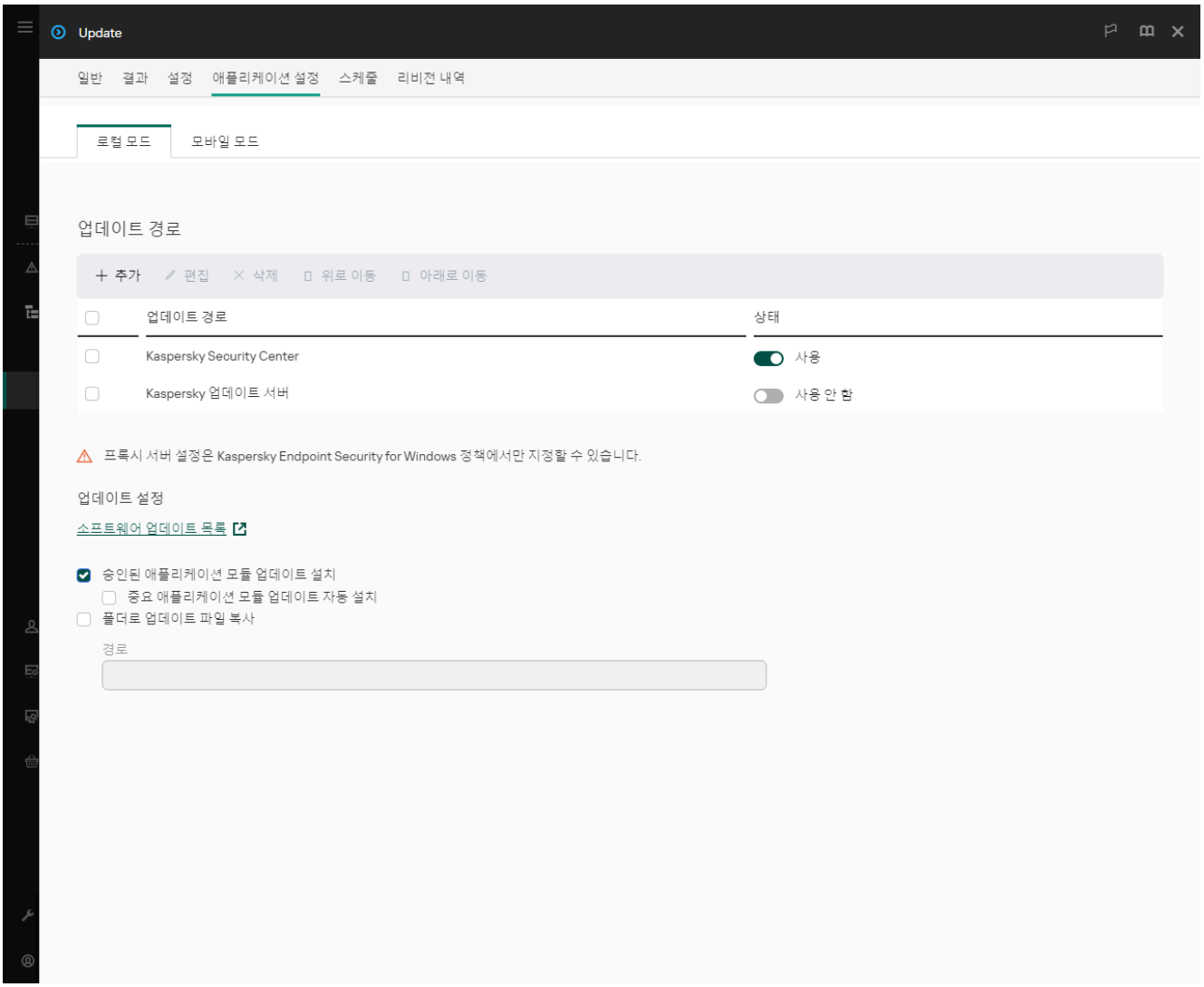
   a. 업데이트 경로 목록에서 **추가** 버튼을 누릅니다.

   b. **업데이트 경로** 필드에서 Kaspersky Security Center가 Kaspersky 서버에서 받은 업데이트 패키지를 복사하는 FTP/HTTP 서버, 네트워크 폴더 또는 로컬 폴더의 주소를 지정합니다.

      업데이트 경로의 주소는 서버 저장소로의 업데이트 다운로드를 구성할 때 **업데이트 저장 폴더** 필드에 지정한 주소와 일치해야 합니다(*중앙 관리 서버 저장소에 업데이트 다운로드* 작업).

   c. **저장**을 클릭합니다.

   업데이트 경로 목록에서 제거하지 않고 업데이트 경로를 제외할 수 있습니다. 이렇게 하려면 옆의 토글 스위치를 끄기로 설정합니다.



업데이트 경로

6. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

   첫 번째 업데이트 경로에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 경로로 자동 전환합니다.

7. 작업 속성 창에서 **스케줄** 섹션을 선택하고 작업 실행 모드를 구성합니다.

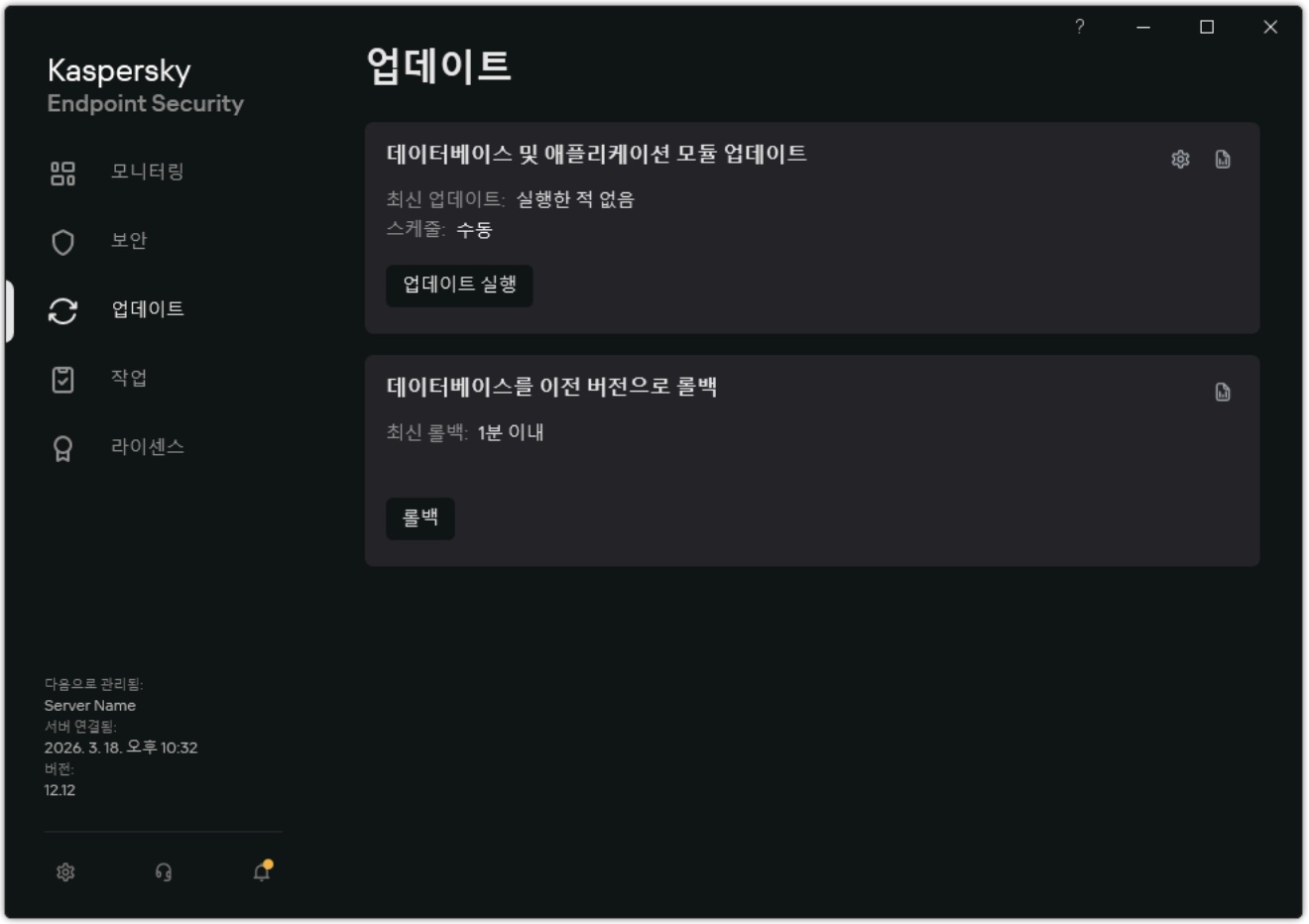
8. 기본적으로 Kaspersky Endpoint Security는 수동 모드에서 작업을 실행합니다.

9. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 지정한 서버 저장소에서의 Kaspersky Endpoint Security 업데이트를 구성하는 방법

애플리케이션 인터페이스에서 *데이터베이스 및 애플리케이션 모듈 업데이트* 그룹 작업을 구성할 수 없습니다. 로컬 업데이트 작업인 *데이터베이스 및 애플리케이션 모듈 업데이트*만 사용자가 이용할 수 있습니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.



로컬 업데이트 작업

2. 작업 목록이 열립니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 선택하고 ⚙ 클릭합니다.

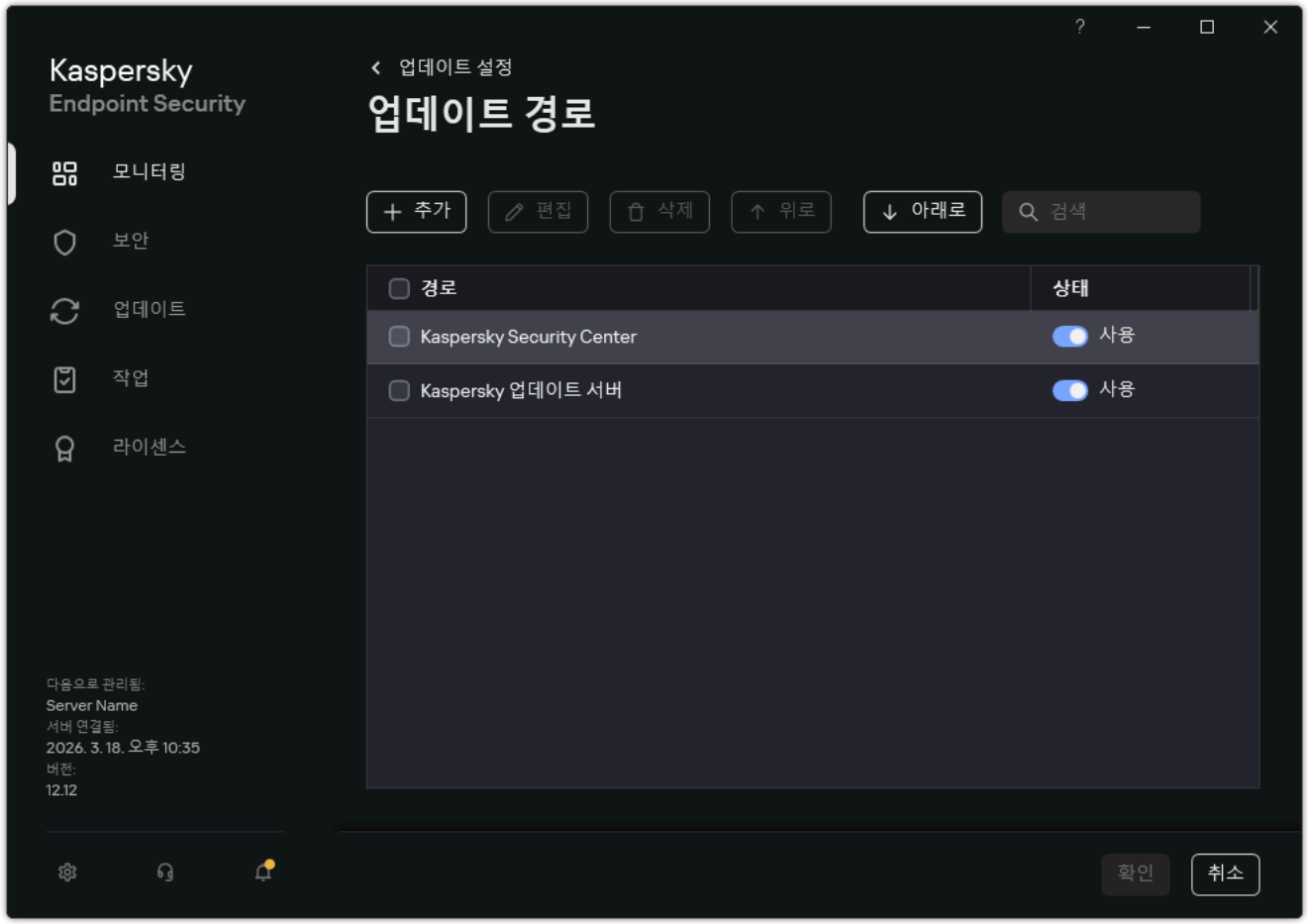
   작업 속성 창이 열립니다.

3. 작업 속성 창에서 **업데이트 경로 선택**을 클릭합니다.

4. 업데이트 경로 목록에서 **Kaspersky Security Center** 경로 업데이트가 활성화되어 있는지 확인하십시오. 또한, **Kaspersky Security Center** 경로의 우선순위가 가장 높아야 합니다.

5. 필요하다면 다음 업데이트 경로를 추가합니다.

a. 업데이트 경로 목록에서 **추가** 버튼을 누릅니다.



업데이트 경로

a. Kaspersky Security Center가 Kaspersky 업데이트 서버에서 받은 업데이트 패키지를 복사하는 FTP/HTTP 서버, 네트워크 폴더 또는 로컬 폴더의 주소를 지정합니다.

> 업데이트 경로의 주소는 서버 저장소로의 업데이트 다운로드를 구성할 때 **업데이트 저장 폴더** 필드에 지정한 주소와 일치해야 합니다(*중앙 관리 서버 저장소에 업데이트 다운로드* 작업).

b. **선택**을 클릭합니다.

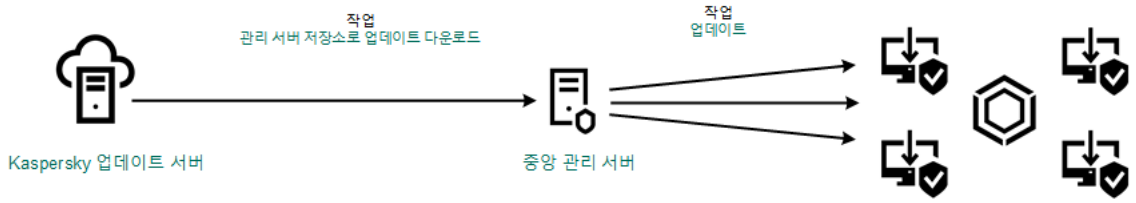
업데이트 경로 목록에서 제거하지 않고 업데이트 경로를 제외할 수 있습니다. 이렇게 하려면 옆의 토글 스위치를 끄기로 설정합니다.

6. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

첫 번째 업데이트 경로에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 경로로 자동 전환합니다.

> 컴퓨터가 Kaspersky Security Center에서 관리되는 경우 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업에 대해 실행 모드를 구성할 수 없습니다. 작업은 수동으로만 실행할 수 있습니다.

7. 변경 사항을 저장합니다.



서버 저장소에서 업데이트

공유 폴더에서 업데이트

인터넷 트래픽을 절약하려는 경우 공유 폴더에서 조직 LAN의 컴퓨터에 대한 데이터베이스 및 애플리케이션 모듈 업데이트를 구성할 수 있습니다. 그러려면 조직 LAN의 컴퓨터 중 한 대가 Kaspersky Security Center 중앙 관리 서버 또는 Kaspersky 업데이트 서버에서 업데이트 패키지를 받은 다음 공유 폴더에 해당 업데이트 패키지를 복사해야 합니다. 그러면 조직 LAN의 다른 컴퓨터가 이 공유 폴더에서 업데이트 패키지를 받을 수 있습니다.

업데이트 패키지를 공유 폴더에 복사하는 Kaspersky Endpoint Security 애플리케이션의 버전 및 언어는 공유 폴더에서 데이터베이스를 업데이트하는 애플리케이션의 버전 및 언어와 일치해야 합니다. 애플리케이션의 버전 또는 언어가 일치하지 않으면 데이터베이스 업데이트가 오류와 함께 종료될 수 있습니다.

공유 폴더에서 데이터베이스 및 애플리케이션 모듈 업데이트를 구성하는 과정은 다음 단계로 구성됩니다:

1. 서버 저장소에서 데이터베이스 및 애플리케이션 모듈 업데이트 구성.

2. LAN(Local Area Network)에 있는 컴퓨터 중 하나의 공유 폴더로 업데이트 패키지를 복사하는 기능을 작동합니다.

   관리 콘솔(MMC) 내 공유 폴더에 업데이트 패키지를 복사하는 것을 활성화하는 방법

   1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

   2. 콘솔 트리에서 **작업**을 선택합니다.

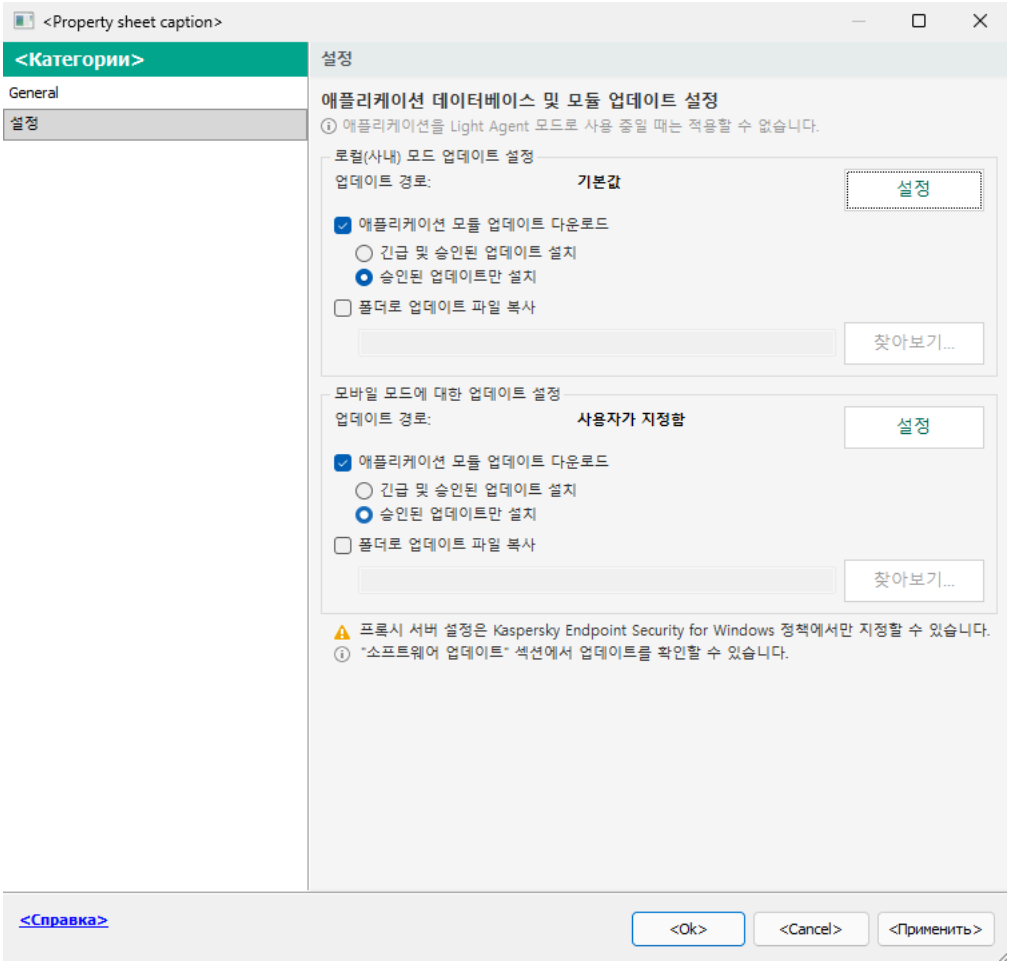
      업데이트 경로로 사용할 컴퓨터 한 대에 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 지정해야 합니다.

   3. Kaspersky Endpoint Security의 **데이터베이스 및 애플리케이션 모듈 업데이트** 작업을 클릭합니다.

      작업 속성 창이 열립니다.

      데이터베이스 및 애플리케이션 모듈 업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

4. 작업 속성 창에서 **설정** 섹션을 선택합니다.



데이터베이스 및 애플리케이션 모듈 업데이트 작업 설정

5. **로컬(사내) 모드 업데이트 설정** 블록에서 **설정** 버튼을 클릭합니다.

6. 업데이트 경로를 구성합니다.

   업데이트 경로는 Kaspersky 업데이트 서버, Kaspersky Security Center 중앙 관리 서버, 기타 FTP/HTTP 서버, 로컬 폴더 또는 네트워크 폴더일 수 있습니다.

7. **폴더로 업데이트 파일 복사** 확인란을 선택합니다.

8. **폴더 경로** 필드에 UNC 경로를 공유 폴더에 입력합니다(예: `\\<server name>\KLSHARE\Updates`).

   이 필드를 비워 두면 Kaspersky Endpoint Security는 `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\` 폴더로 업데이트 패키지를 복사합니다.

9. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console 내 공유 폴더에 업데이트 패키지를 복사하는 것을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.

   작업 목록이 열립니다.

   > 업데이트 경로로 사용할 컴퓨터 한 대에 *업데이트* 작업을 지정해야 합니다.

2. Kaspersky Endpoint Security의 **업데이트** 작업을 누릅니다.

   작업 속성 창이 열립니다.

업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

3. **애플리케이션 설정 → 로컬 모드** 탭을 선택합니다.

4. 업데이트 경로를 구성합니다.

   업데이트 경로는 Kaspersky 업데이트 서버, Kaspersky Security Center 중앙 관리 서버, 기타 FTP/HTTP 서버, 로컬 폴더 또는 네트워크 폴더일 수 있습니다.

5. **폴더로 업데이트 파일 복사** 확인란을 선택합니다.

6. **경로** 필드에 UNC 경로를 공유 폴더에 입력합니다(예: `\\<server name>\KLSHARE\Updates`).

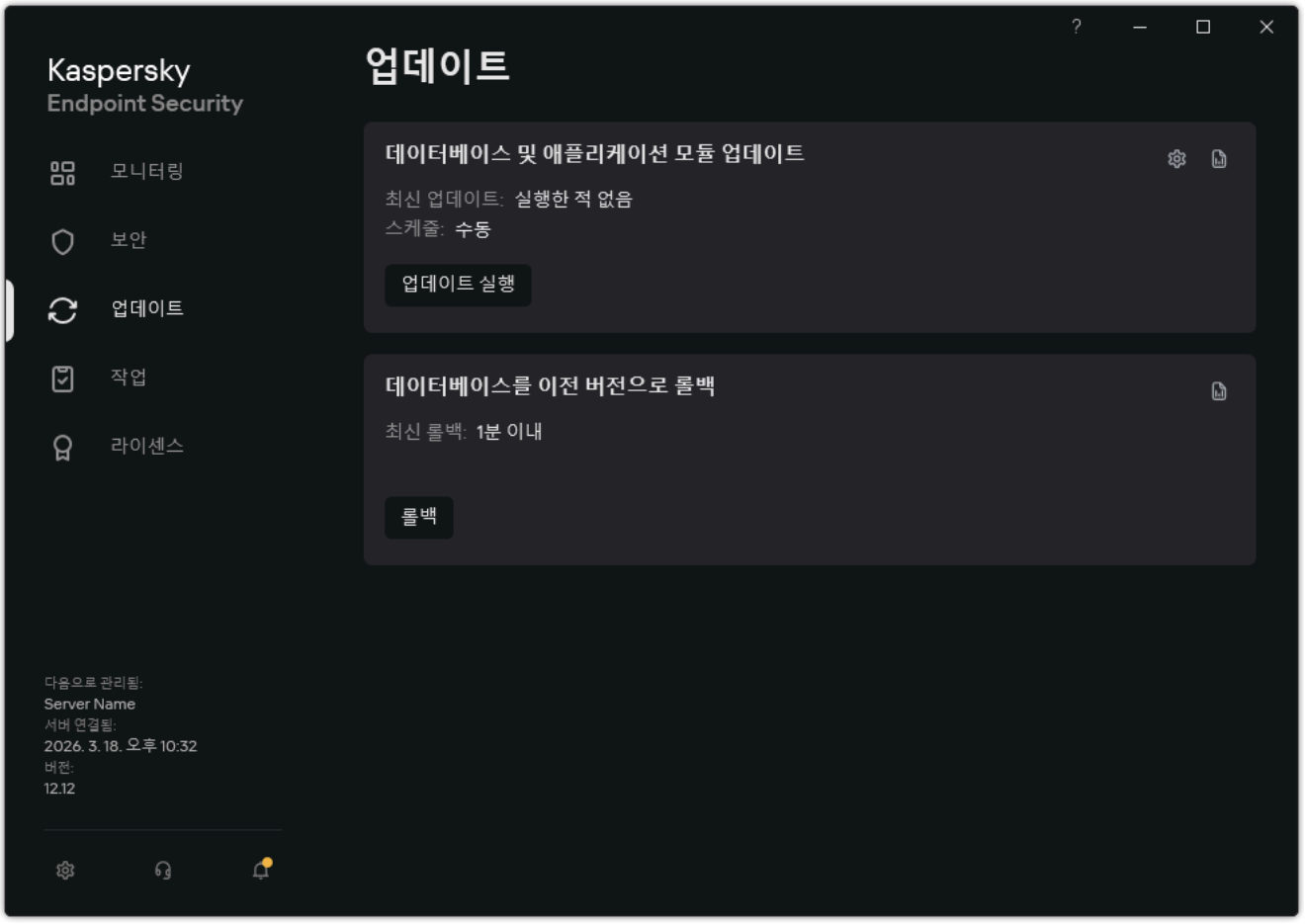
   이 필드를 비워 두면 Kaspersky Endpoint Security는 `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\` 폴더로 업데이트 패키지를 복사합니다.

7. 변경 사항을 저장합니다.

애플리케이션 인터페이스 내 공유 폴더에 업데이트 패키지를 복사하는 것을 활성화하는 방법

애플리케이션 인터페이스에서 *데이터베이스 및 애플리케이션 모듈 업데이트* 그룹 작업을 구성할 수 없습니다. 로컬 업데이트 작업인 *데이터베이스 및 애플리케이션 모듈 업데이트*만 사용자가 이용할 수 있습니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.



로컬 업데이트 작업

2. 작업 목록이 열립니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 선택하고 ⚙ 클릭합니다.
   작업 속성 창이 열립니다.

3. **업데이트 배포** 섹션에서 **폴더로 업데이트 파일 복사** 확인란을 선택합니다.

4. UNC 경로를 공유 폴더에 입력합니다(예: `\\<server name>\KLSHARE\Updates`).

5. 변경 사항을 저장합니다.

3. 지정한 공유 폴더에서 조직 LAN에 있는 나머지 컴퓨터로의 데이터베이스 및 애플리케이션 모듈 업데이트를 구성합니다.

관리 콘솔(MMC)에서 공유 폴더의 업데이트를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **데이터베이스 및 애플리케이션 모듈 업데이트**를 선택합니다.

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

5. **새 작업**을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **데이터베이스 및 애플리케이션 모듈 업데이트**를 선택합니다.

2단계. 업데이트 경로 선택

새 업데이트 경로 추가: 공유 폴더. 이 경로 주소는 공유 폴더로의 업데이트 패키지 복사를 구성할 때 **폴더 경로** 필드에 지정한 주소와 일치해야 합니다. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

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.

업데이트 경로로 사용되는 컴퓨터를 제외한 조직 LAN의 컴퓨터에 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 지정해야 합니다.

4단계. 작업을 실행할 계정 선택

데이터베이스 및 애플리케이션 모듈 업데이트 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.

5 단계. 작업 시작 스케줄 구성

예를 들어 안티 바이러스 데이터베이스를 저장소에 다운로드 한 후 또는 직접 작업 시작 스케줄을 구성합니다.

6단계. 작업 이름 정의

*공유 폴더에서 업데이트*와 같이 작업 이름을 입력합니다.

7단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다. 이렇게 하면 지정한 스케줄에 따라 사용자 컴퓨터에서 업데이트 작업이 실행됩니다.

웹 콘솔 및 Cloud Console에서 공유 폴더의 업데이트를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **업데이트**를 선택합니다.

   c. **작업 이름** 필드에 *공유 폴더에서 업데이트* 등의 간단한 설명을 입력합니다.

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

   > 업데이트 경로로 사용되는 컴퓨터를 제외한 조직 LAN의 컴퓨터에 *업데이트* 작업을 지정해야 합니다.

4. 선택한 작업 범위 옵션에 따라 장치를 선택하고 다음 단계로 넘어갑니다.

5. 마법사를 끝냅니다.
   작업 표에 새 작업이 표시됩니다.

6. 새롭게 생성된 *업데이트* 작업을 누릅니다.
   작업 속성 창이 열립니다.

7. **애플리케이션 설정** → 로컬 모드 탭을 선택합니다.

8. **업데이트 경로** 블록에서 **추가** 버튼을 누릅니다.

9. 열리는 창에서 공유 폴더의 경로를 입력합니다.

   > 이 경로 주소는 공유 폴더로의 업데이트 패키지 복사를 구성할 때 **경로** 필드에 지정한 주소와 일치해야 합니다(위 지침 참조).

10. **확인**을 누릅니다.

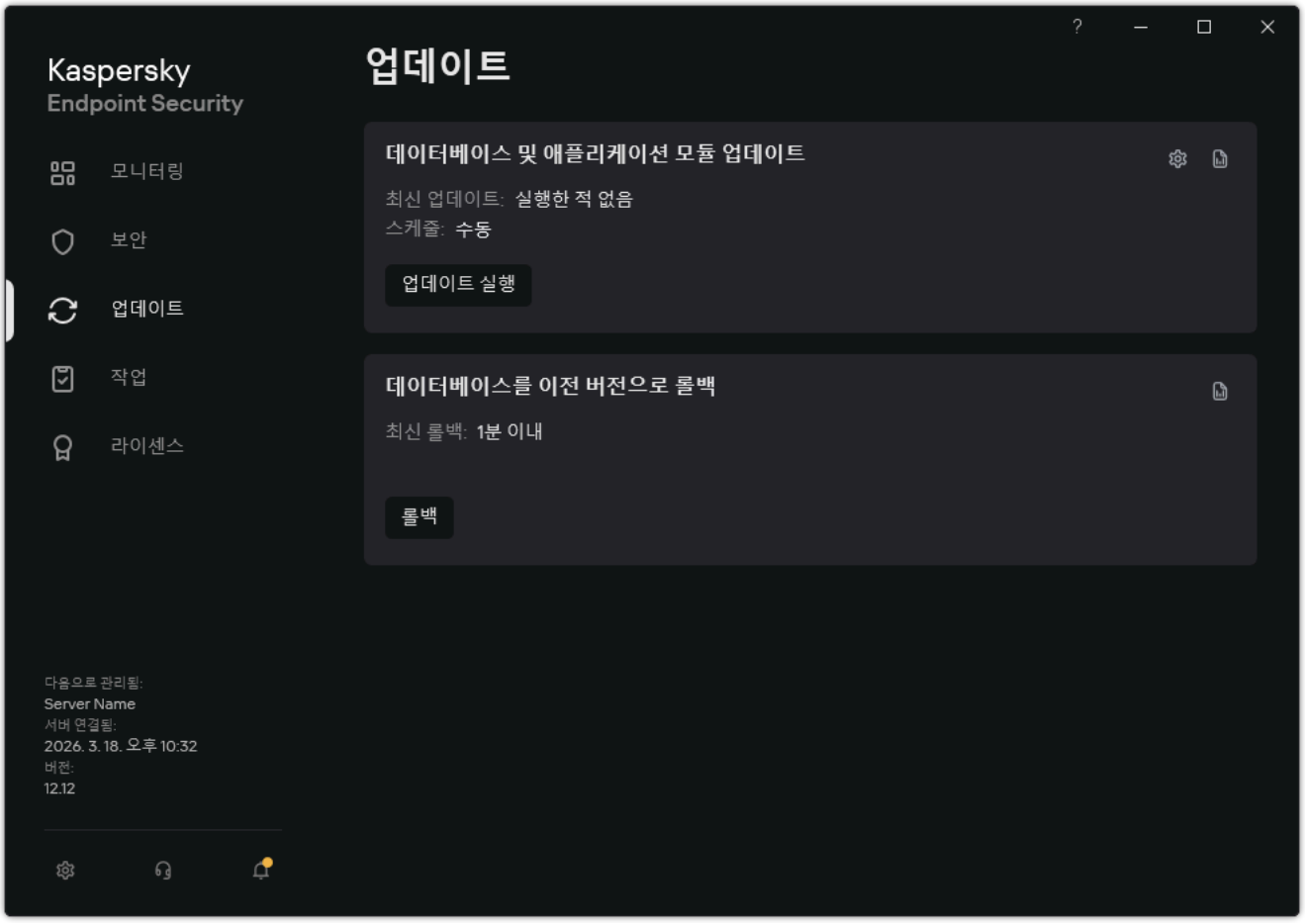
11. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

12. 변경 사항을 저장합니다.

애플리케이션 인터페이스의 공유 폴더에서 업데이트를 구성하는 방법

애플리케이션 인터페이스에서 *데이터베이스 및 애플리케이션 모듈 업데이트* 그룹 작업을 구성할 수 없습니다. 로컬 업데이트 작업인 *데이터베이스 및 애플리케이션 모듈 업데이트*만 사용자가 이용할 수 있습니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.



로컬 업데이트 작업

2. 작업 목록이 열립니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 선택하고 ⚙ 클릭합니다. 작업 속성 창이 열립니다.
3. **업데이트 경로 선택**을 클릭합니다.
4. 열리는 창에서 **추가** 버튼을 누릅니다.
5. 열리는 창에서 공유 폴더의 경로를 입력합니다.

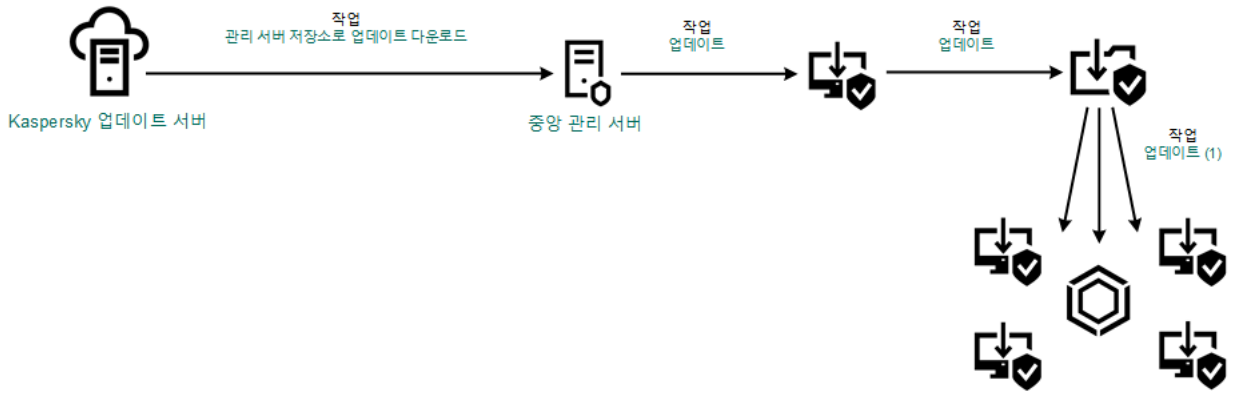
   이 경로 주소는 공유 폴더로의 업데이트 패키지 복사를 구성할 때 지정한 주소와 일치해야 합니다(위 지침 참조).

6. **선택**을 클릭합니다.

7. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

   첫 번째 업데이트 경로에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 경로로 자동 전환합니다.

8. 변경 사항을 저장합니다.



공유 폴더에서 업데이트

Kaspersky 업데이트 유틸리티를 사용하여 업데이트

인터넷 트래픽을 절약하려는 경우 Kaspersky Update Utility를 사용해 공유 폴더에서 조직 LAN의 컴퓨터에 대한 데이터베이스 및 애플리케이션 모듈 업데이트를 구성할 수 있습니다. 그러려면 조직 LAN의 컴퓨터 중 한 대가 Kaspersky Security Center 중앙 관리 서버 또는 Kaspersky 업데이트 서버에서 업데이트 패키지를 받은 다음 이 유틸리티를 사용해 공유 폴더에 해당 업데이트 패키지를 복사해야 합니다. 그러면 조직 LAN의 다른 컴퓨터가 이 공유 폴더에서 업데이트 패키지를 받을 수 있습니다.

업데이트 패키지를 공유 폴더에 복사하는 Kaspersky Endpoint Security 애플리케이션의 버전 및 언어는 공유 폴더에서 데이터베이스를 업데이트하는 애플리케이션의 버전 및 언어와 일치해야 합니다. 애플리케이션의 버전 또는 언어가 일치하지 않으면 데이터베이스 업데이트가 오류와 함께 종료될 수 있습니다.

공유 폴더에서 데이터베이스 및 애플리케이션 모듈 업데이트를 구성하는 과정은 다음 단계로 구성됩니다:

1. 서버 저장소에서 데이터베이스 및 애플리케이션 모듈 업데이트 구성.

2. 조직 LAN에 있는 컴퓨터 한 대에 Kaspersky 업데이트 유틸리티를 설치합니다.

3. Kaspersky 업데이트 유틸리티 설정에서 공유 폴더로의 업데이트 패키지 복사를 구성합니다.

   Kaspersky 기술 지원 웹사이트에서 Kaspersky 업데이트 유틸리티 배포 패키지를 다운로드할 수 있습니다. 유틸리티 설치 후 업데이트 경로(예: 중앙 관리 서버 저장소) 및 Kaspersky 업데이트 유틸리티가 업데이트 패키지를 복사해 넣을 공유 폴더를 선택합니다. Kaspersky 업데이트 유틸리티 사용에 대한 자세한 내용은 Kaspersky 기술 자료를 참조하십시오.

4. 지정한 공유 폴더에서 조직 LAN에 있는 나머지 컴퓨터로의 데이터베이스 및 애플리케이션 모듈 업데이트를 구성합니다.

   관리 콘솔(MMC)에서 공유 폴더의 업데이트를 구성하는 방법

   1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

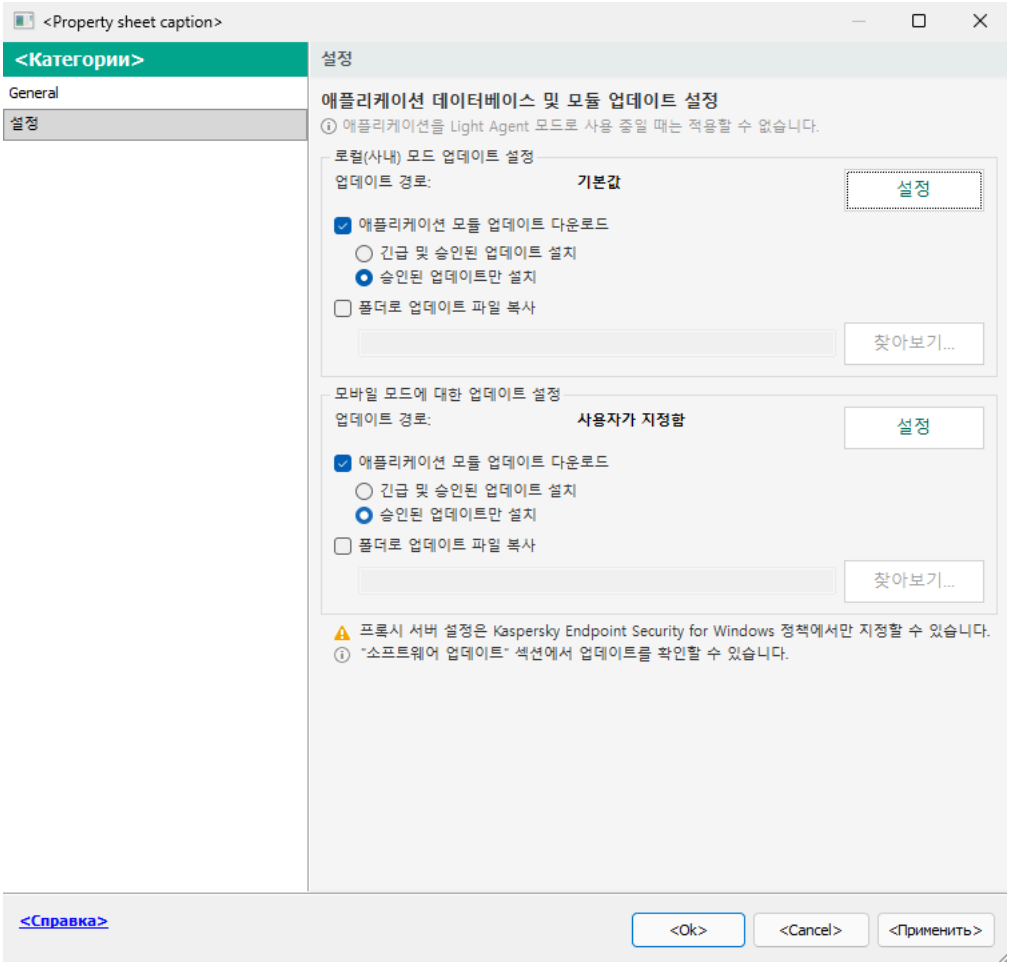
   2. 콘솔 트리에서 **작업**을 선택합니다.

3. Kaspersky Endpoint Security의 **데이터베이스 및 애플리케이션 모듈 업데이트** 작업을 클릭합니다.

   작업 속성 창이 열립니다.

   데이터베이스 및 애플리케이션 모듈 업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

4. 작업 속성 창에서 **설정** 섹션을 선택합니다.



데이터베이스 및 애플리케이션 모듈 업데이트 작업 설정

5. **로컬(사내) 모드 업데이트 설정** 블록에서 **설정** 버튼을 클릭합니다.

6. 업데이트 경로 목록에서 **추가** 버튼을 누릅니다.

7. 창이 열리면 업데이트 경로 필드에 UNC 경로를 공유 폴더에 입력합니다(예: `\\<server name>\KLSHARE\Updates`).

   이 경로 주소는 Kaspersky 업데이트 유틸리티 설정에 나와 있는 주소와 일치해야 합니다.

8. **확인**을 누릅니다.

9. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

   첫 번째 업데이트 경로에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 경로로 자동 전환합니다.

10. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 공유 폴더의 업데이트를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. Kaspersky Endpoint Security의 **업데이트** 작업을 누릅니다.
   작업 속성 창이 열립니다.
   업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

3. **애플리케이션 설정** → **로컬 모드** 탭을 선택합니다.

4. 업데이트 경로 목록에서 **추가** 버튼을 누릅니다.

5. 창이 열리면 업데이트 경로 필드에 UNC 경로를 공유 폴더에 입력합니다(예: `\\<server name>\KLSHARE\Updates`).

   > 이 경로 주소는 Kaspersky 업데이트 유틸리티 설정에 나와 있는 주소와 일치해야 합니다.

6. **확인**을 누릅니다.

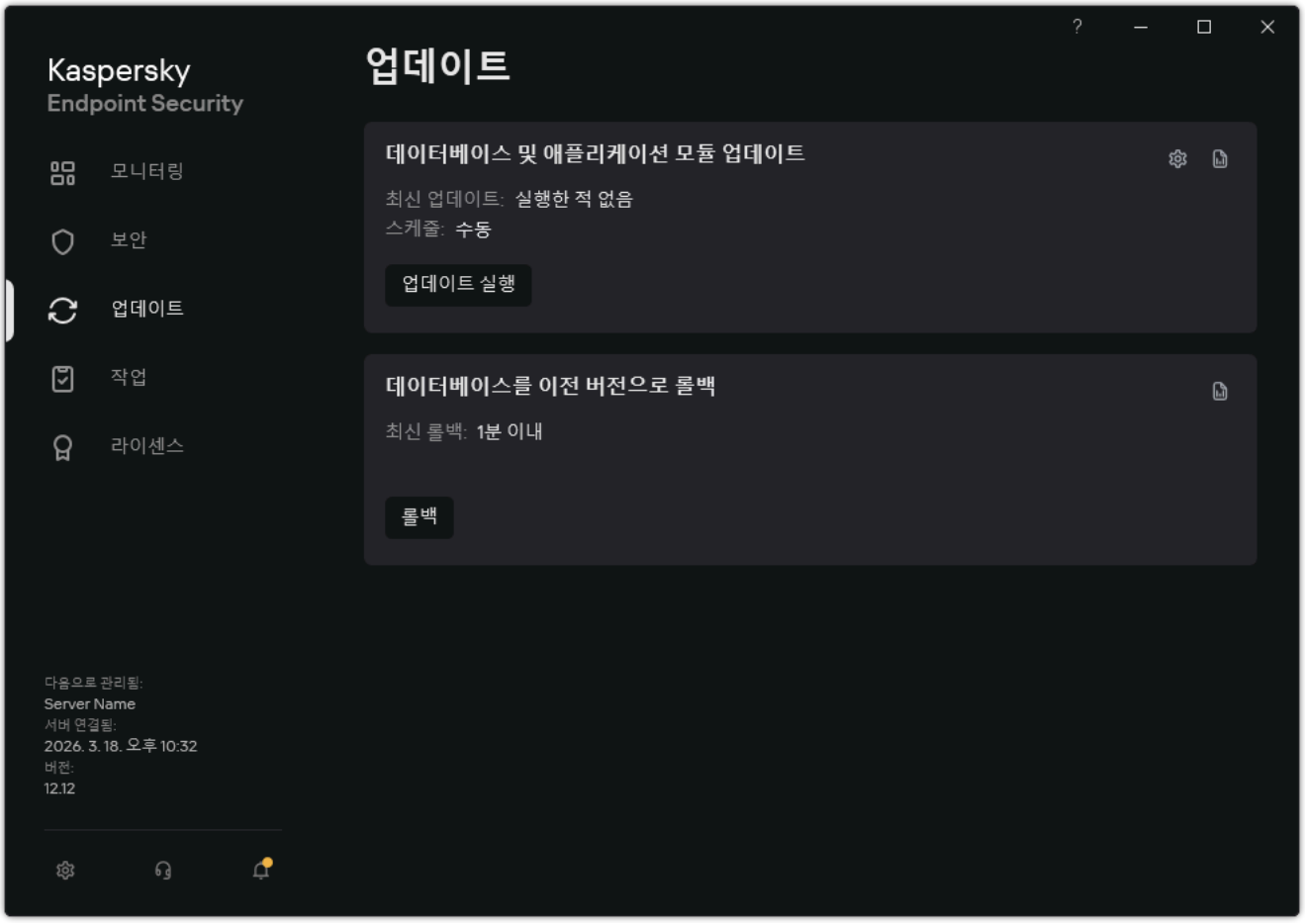
7. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.
   첫 번째 업데이트 경로에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 경로로 자동 전환합니다.

8. 변경 사항을 저장합니다.

애플리케이션 인터페이스의 공유 폴더에서 업데이트를 구성하는 방법

애플리케이션 인터페이스에서 *데이터베이스 및 애플리케이션 모듈 업데이트* 그룹 작업을 구성할 수 없습니다. 로컬 업데이트 작업인 *데이터베이스 및 애플리케이션 모듈 업데이트*만 사용자가 이용할 수 있습니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.

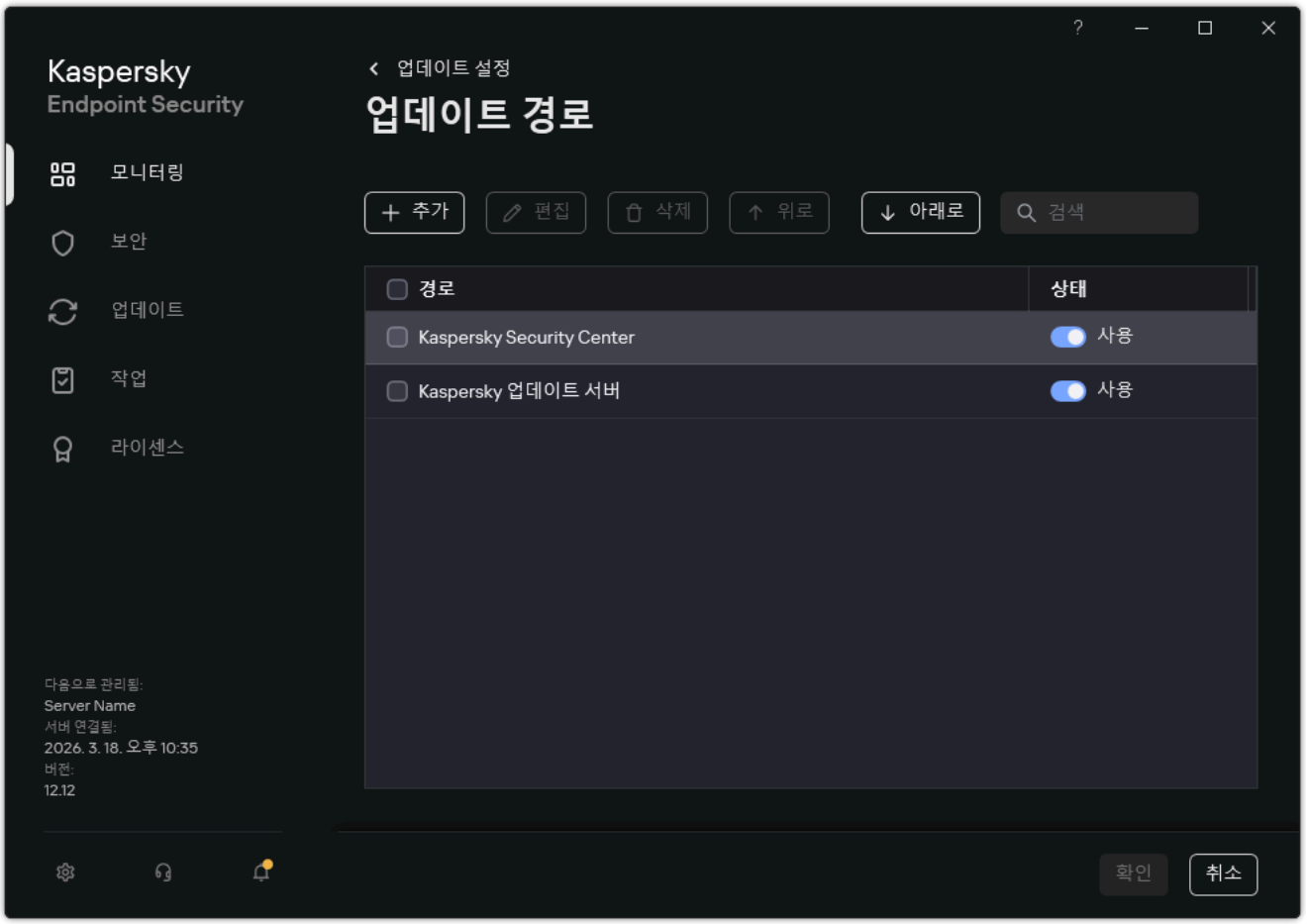


로컬 업데이트 작업

2. 작업 목록이 열립니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 선택하고 ⚙ 클릭합니다. 작업 속성 창이 열립니다.

3. 작업 속성 창에서 **업데이트 경로 선택**을 클릭합니다.

4. 업데이트 경로 목록에서 **추가** 버튼을 누릅니다.



업데이트 경로

5. UNC 경로를 공유 폴더에 입력합니다(예: `\\<server name>\KLSHARE\Updates`).

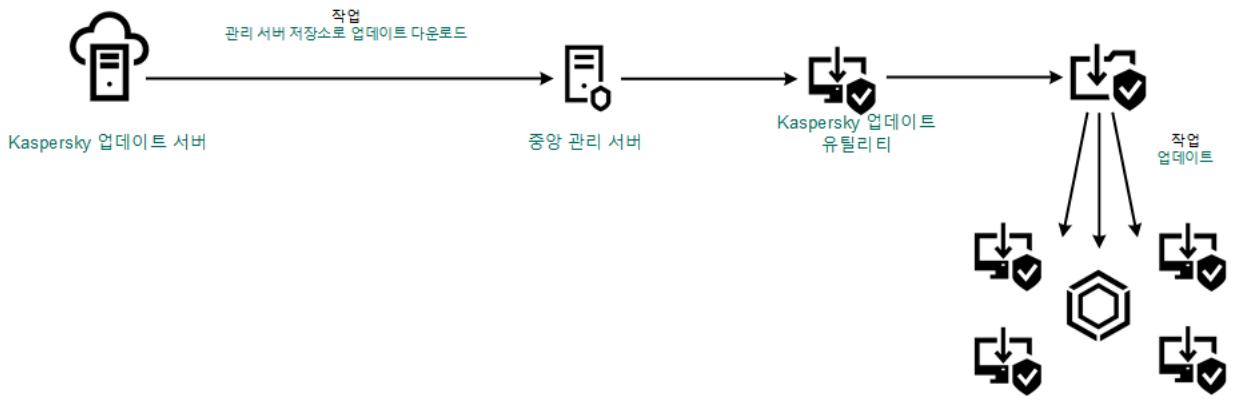
이 경로 주소는 Kaspersky 업데이트 유틸리티 설정에 나와 있는 주소와 일치해야 합니다.

6. **선택**을 클릭합니다.

7. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

   첫 번째 업데이트 경로에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 경로로 자동 전환합니다.

8. 변경 사항을 저장합니다.



Kaspersky 업데이트 유틸리티를 사용하여 업데이트

모바일 모드에서 업데이트

*모바일 모드*는 컴퓨터가 조직 네트워크 경계를 벗어날 때(*오프라인 컴퓨터*)의 Kaspersky Endpoint Security 동작 모드입니다. 오프라인 컴퓨터 및 이동 사용자 작업과 관련한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.

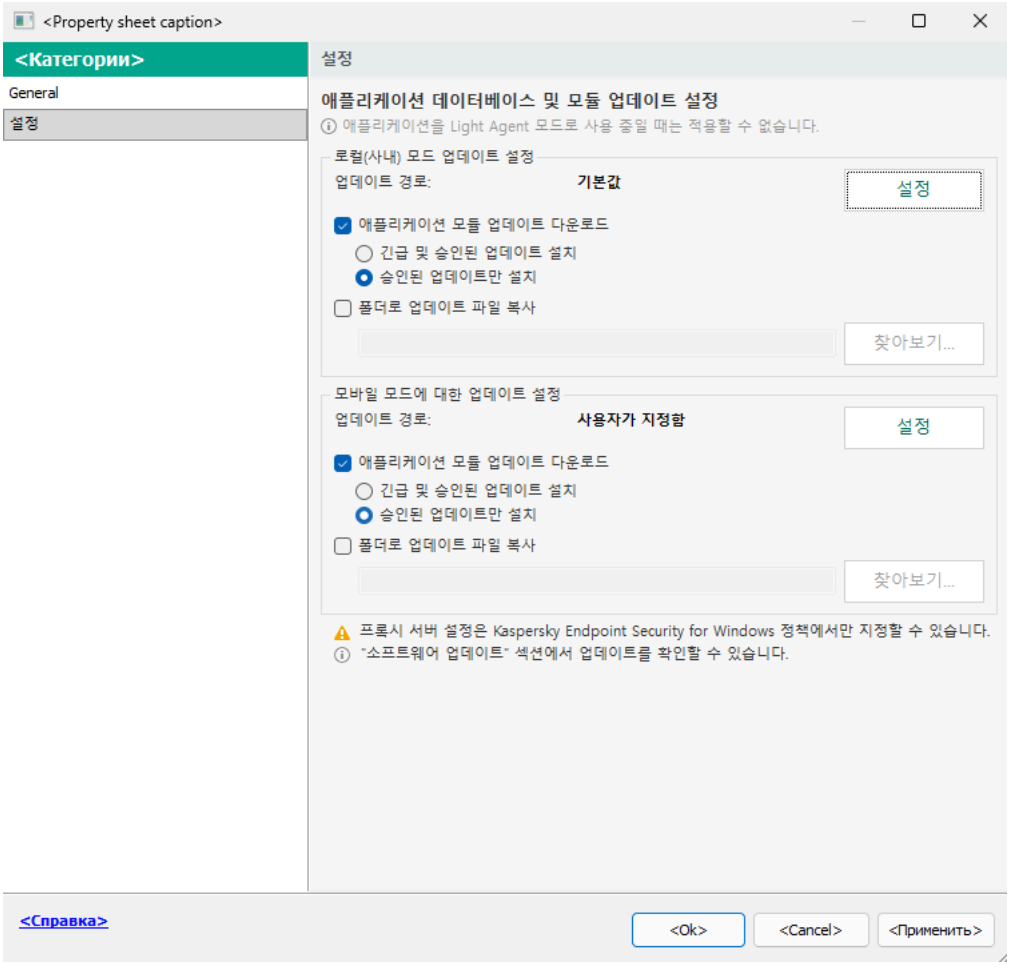
조직 네트워크 외부의 오프라인 컴퓨터는 중앙 관리 서버에 연결하여 데이터베이스 및 애플리케이션 모듈을 업데이트할 수 없습니다. 기본적으로는 Kaspersky 업데이트 서버만 모바일 모드에서 데이터베이스 및 애플리케이션 모듈 업데이트를 위한 업데이트 경로로 사용됩니다. 인터넷 연결을 위한 프록시 서버 사용 여부는 특수 이동 사용자 정책을 통해 결정됩니다. 이동 사용자 정책은 별도로 생성해야 합니다. Kaspersky Endpoint Security를 모바일 모드로 전환하면 업데이트 작업이 2시간마다 시작됩니다.

관리 콘솔(MMC)에서 모바일 모드에 대한 업데이트 설정을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업**을 선택합니다.
3. Kaspersky Endpoint Security의 **데이터베이스 및 애플리케이션 모듈 업데이트** 작업을 클릭합니다.

   작업 속성 창이 열립니다.

   데이터베이스 및 애플리케이션 모듈 업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.
4. 작업 속성 창에서 **설정** 섹션을 선택합니다.



데이터베이스 및 애플리케이션 모듈 업데이트 작업 설정

5. **모바일 모드에 대한 업데이트 설정** 블록에서 **설정** 버튼을 클릭합니다.

6. 업데이트 경로를 구성합니다. 업데이트 경로는 Kaspersky 업데이트 서버, 기타 FTP/HTTP 서버, 로컬 폴더 또는 네트워크 폴더일 수 있습니다.

7. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 모바일 모드 업데이트 설정을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.

   작업 목록이 열립니다.

2. Kaspersky Endpoint Security의 **업데이트** 작업을 누릅니다.

   작업 속성 창이 열립니다.

   업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

3. **애플리케이션 설정** → **모바일 모드** 탭을 선택합니다.

4. 업데이트 경로를 구성합니다. 업데이트 경로는 Kaspersky 업데이트 서버, 기타 FTP/HTTP 서버, 로컬 폴더 또는 네트워크 폴더일 수 있습니다.

5. 변경 사항을 저장합니다.

그러면 사용자 컴퓨터가 모바일 모드로 전환될 때 데이터베이스 및 애플리케이션 모듈이 업데이트됩니다.

업데이트 작업 시작 및 중지

선택한 업데이트 작업 스케줄에 관계 없이 언제라도 Kaspersky Endpoint Security 업데이트 작업을 시작 또는 중지할 수 있습니다.

업데이트 작업을 시작 또는 중지하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.

2. 업데이트 작업을 시작하려면 **데이터베이스 및 애플리케이션 모듈 업데이트** 타일에서 **업데이트** 버튼을 클릭합니다.

   Kaspersky Endpoint Security가 애플리케이션 모듈 및 데이터베이스 업데이트를 시작합니다. 애플리케이션이 작업 진행률, 다운로드 한 파일의 크기 및 업데이트 경로를 표시합니다. **업데이트 중지** 버튼을 클릭하여 언제든지 작업을 중지할 수 있습니다.

간략한 애플리케이션 인터페이스가 표시될 때 업데이트 작업을 시작하거나 중지하려면 다음과 같이 하십시오.

1. 작업 표시줄 알림 영역에 있는 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 눌러 마우스 오른쪽 메뉴를 엽니다.

2. 마우스 오른쪽 메뉴에 있는 **작업** 드롭다운 목록에서 다음 중 하나를 수행하십시오:

   - 실행하지 않은 업데이트 작업을 선택하여 시작합니다
   - 실행 중인 업데이트 작업을 선택하여 중지합니다
   - 일시 중지된 업데이트 작업을 선택하여 재시작하거나 다시 시작하십시오

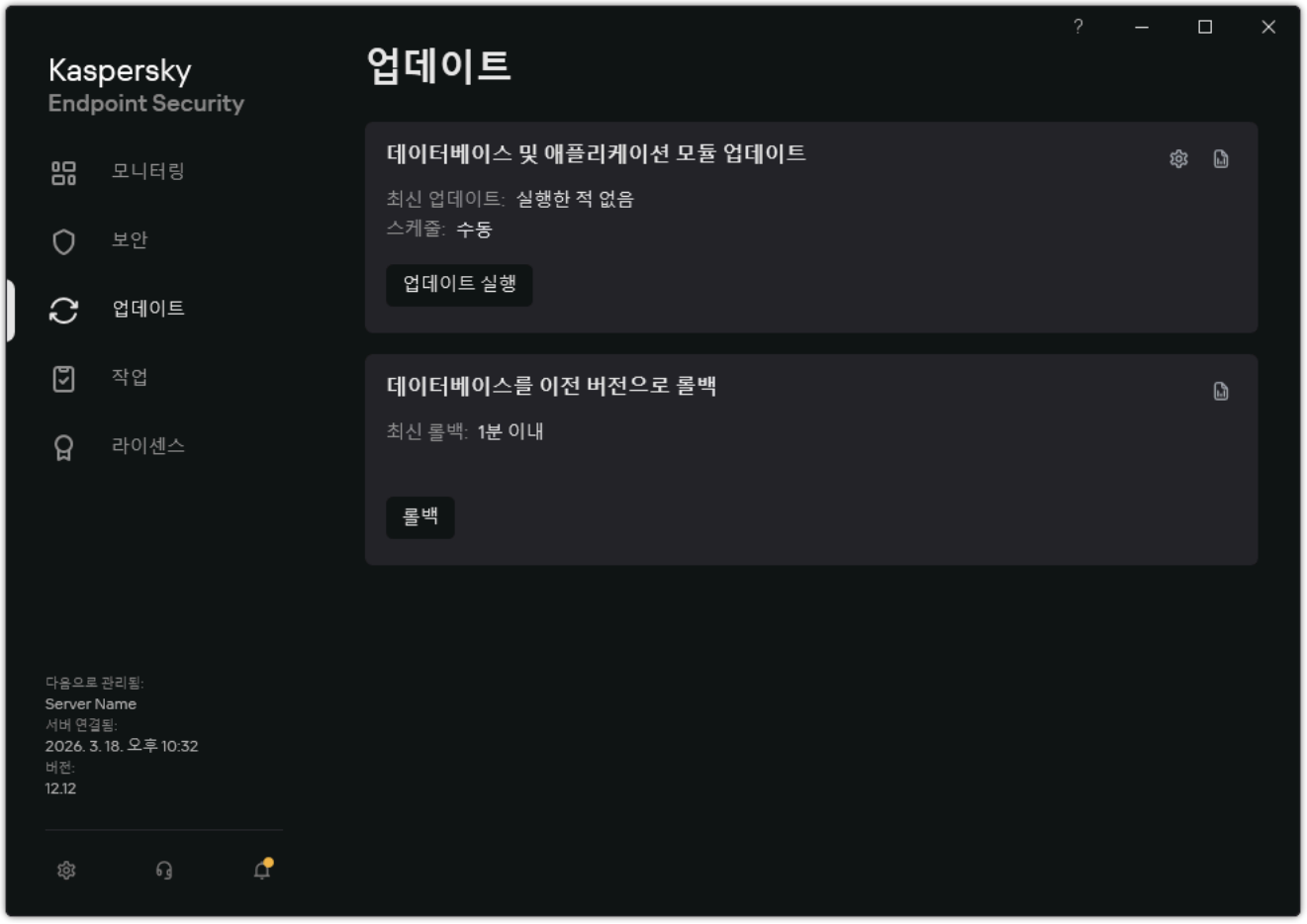
다른 사용자 계정 권한으로 업데이트 작업 시작

기본적으로 Kaspersky Endpoint Security 업데이트 작업은 운영 체제에 로그인하는 데 사용했던 계정의 사용자 권한으로 시작됩니다. 그러나 Kaspersky Endpoint Security는 필요한 권한이 없어 접근할 수 없는 업데이트 경로(예: 업데이트 패키지가 포함된 공유 폴더) 또는 인증된 프록시 서버 인증이 구성되지 않은 업데이트 경로에서도 업데이트할 수 있습니다. 애플리케이션 설정에서 그러한 권한을 가진 사용자를 지정하여 해당 사용자 계정으로 Kaspersky Endpoint Security 업데이트 작업을 시작할 수 있습니다.

다른 사용자 계정으로 업데이트 작업을 시작하려면 다음과 같이 하십시오.

애플리케이션 인터페이스에서 *데이터베이스 및 애플리케이션 모듈 업데이트* 그룹 작업을 구성할 수 없습니다. 로컬 업데이트 작업인 *데이터베이스 및 애플리케이션 모듈 업데이트*만 사용자가 이용할 수 있습니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.



로컬 업데이트 작업

2. 작업 목록이 열립니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 선택하고 ⚙ 클릭합니다.
   작업 속성 창이 열립니다.

3. **사용자 권한으로 데이터베이스 업데이트 실행**을 클릭합니다.

4. 창이 열리면 **다른 사용자**를 선택합니다.

5. 업데이트 소스에 접근하는 데 필요한 권한이 있는 사용자의 계정 정보를 입력합니다.

6. 변경 사항을 저장합니다.

업데이트 작업 스케줄 선택

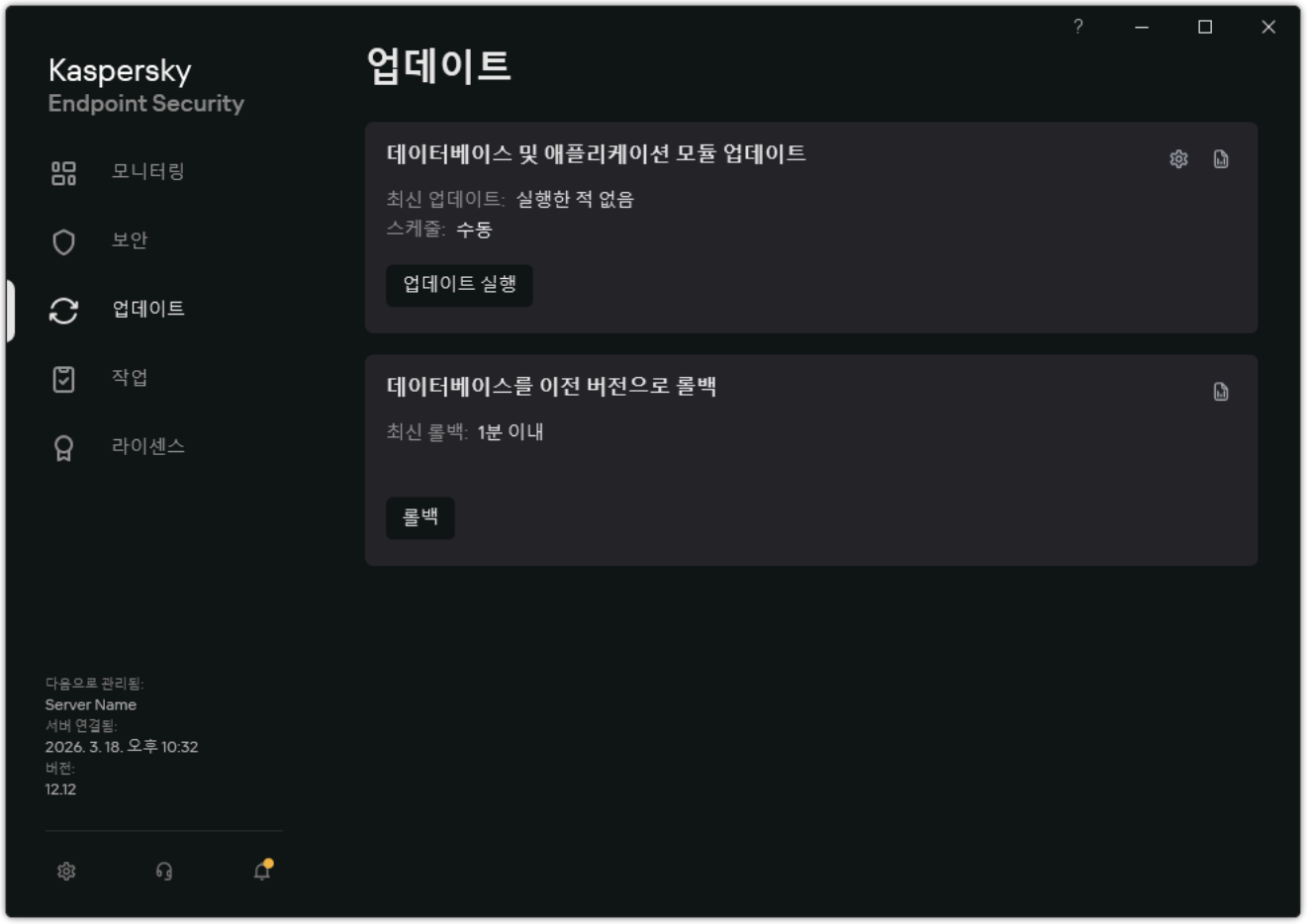
컴퓨터의 전원이 켜져 있지 않는 등의 이유로 업데이트 작업을 실행할 수 없는 경우 컴퓨터의 전원이 켜지면 건너뛴 작업을 자동으로 시작하도록 구성할 수 있습니다.

스케줄에 따라 업데이트 작업 스케줄을 선택했고 Kaspersky Endpoint Security의 시작 시간이 업데이트 작업 시작 스케줄과 일치하는 경우 애플리케이션이 시작된 후에 업데이트 작업을 시작하도록 연기할 수 있습니다. 업데이트 작업은 Kaspersky Endpoint Security가 시작된 후 지정된 시간 간격이 경과해야만 실행할 수 있습니다.

업데이트 작업 스케줄을 선택하려면 다음과 같이 하십시오.

애플리케이션 인터페이스에서 *데이터베이스 및 애플리케이션 모듈 업데이트* 그룹 작업을 구성할 수 없습니다. 로컬 업데이트 작업인 *데이터베이스 및 애플리케이션 모듈 업데이트*만 사용자가 이용할 수 있습니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.



로컬 업데이트 작업

2. 작업 목록이 열립니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 선택하고 ⚙ 클릭합니다.
   작업 속성 창이 열립니다.

3. **실행 모드**를 클릭합니다.

4. 창이 열리면 업데이트 작업 실행 모드를 선택합니다.

   - 업데이트 경로에서 업데이트 패키지를 사용할 수 있는지 여부에 따라 Kaspersky Endpoint Security에서 업데이트 작업을 실행하도록 하려면 **자동**을 선택합니다. Kaspersky Endpoint Security의 업데이트 패키지 검사 빈도는 바이러스 급증 시 증가하고 다른 경우에는 줄어듭니다.

   - 업데이트 작업을 직접 시작하려면 **수동**을 선택합니다.

   - 업데이트 작업의 시작 스케줄을 구성하려면 다른 옵션을 선택합니다. 업데이트 작업을 시작하기 위한 고급 설정을 구성합니다:

     - **애플리케이션 시작 후 다음 시간 동안 작업 실행 연기: N분** 필드에서 Kaspersky Endpoint Security 시작 후 업데이트 작업의 시작을 연기할 시간 간격을 지정합니다.

     - Kaspersky Endpoint Security에서 누락된 업데이트 작업을 기회가 될 때 바로 실행하도록 하려면 **컴퓨터가 꺼져 있으면 스케줄된 검사를 다음 날 실행**을 선택합니다. 애플리케이션에 누락된 작업을 실행할 기회가 있다면 특정 시간 내에 무작위로 작업을 실행하여 컴퓨터의 로드를 분산합니다.

5. 변경 사항을 저장합니다.

업데이트 경로 추가

*업데이트 경로*는 Kaspersky Endpoint Security의 데이터베이스 및 애플리케이션 모듈 업데이트가 포함된 리소스입니다.

업데이트 경로에는 Kaspersky Security Center 서버, Kaspersky 업데이트 서버, 네트워크 또는 로컬 폴더가 있습니다.

Kaspersky 업데이트 서버를 사용할 수 없는 경우 Kaspersky Endpoint Security는 대체 도메인을 사용하여 데이터베이스 및 애플리케이션 소프트웨어 모듈을 업데이트할 수 있습니다. 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오.

기본 업데이트 경로 목록에는 Kaspersky Security Center 및 Kaspersky 업데이트 서버가 포함되어 있습니다. 다른 업데이트 경로를 목록에 추가할 수도 있습니다. 업데이트 경로는 HTTP/FTP 서버 및 공유 폴더가 될 수 있습니다.

Kaspersky Endpoint Security Kaspersky의 업데이트 서버를 제외한 HTTPS 서버에서의 업데이트를 지원하지 않습니다.

여러 리소스를 업데이트 경로로 선택한 경우 Kaspersky Endpoint Security는 목록 위부터 아래 순서로 하나씩 연결해 보고 가장 먼저 가능한 경로에서 업데이트 패키지를 가져와서 업데이트 작업을 수행합니다.

기본적으로 Kaspersky Endpoint Security는 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 Kaspersky 서버는 *데이터베이스 및 애플리케이션 모듈 업데이트* 설정에서 첫 번째 업데이트 경로로 선택됩니다.

애플리케이션이 Light Agent 모드로 실행중인 경우, SVM의 폴더가 업데이트 경로로 선택됩니다.

관리 콘솔(MMC)에서 업데이트 경로를 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

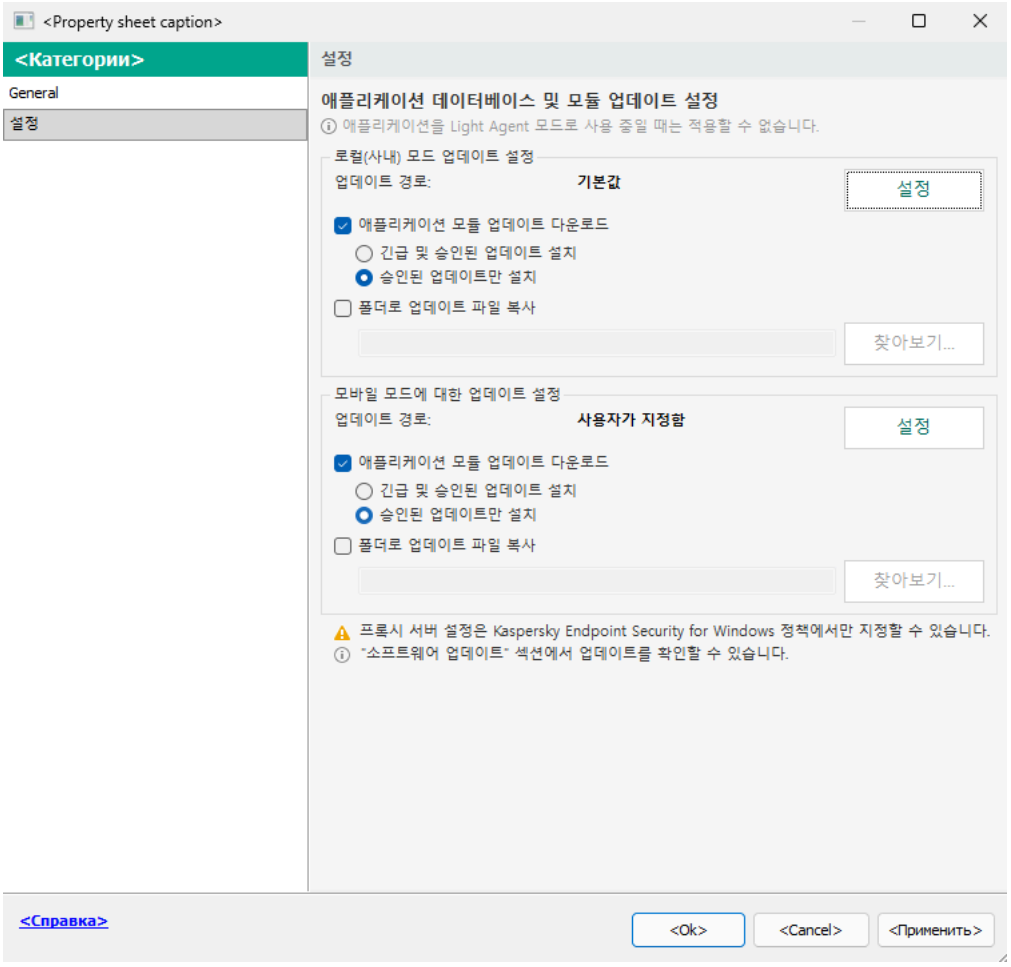
   콘솔 트리에서 **작업**을 선택합니다.

2. Kaspersky Endpoint Security의 **데이터베이스 및 애플리케이션 모듈 업데이트** 작업을 클릭합니다.

   작업 속성 창이 열립니다.

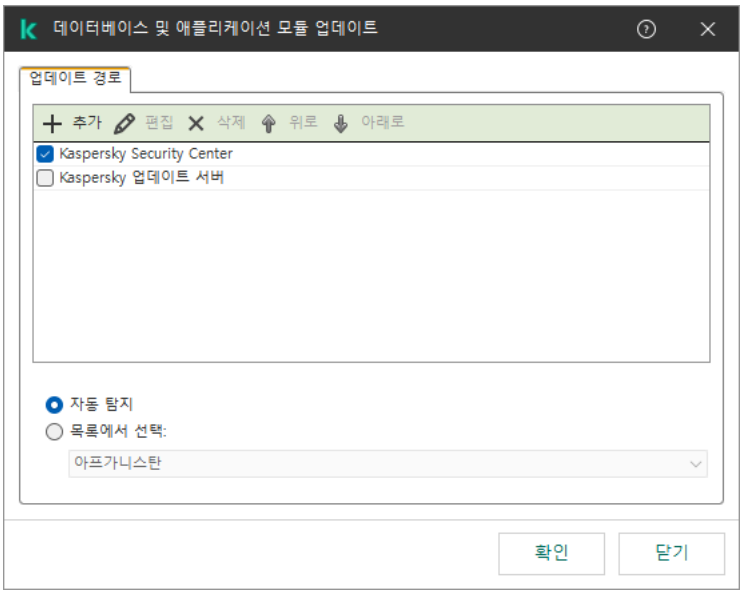
   데이터베이스 및 애플리케이션 모듈 업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

3. 작업 속성 창에서 **설정** 섹션을 선택합니다.



데이터베이스 및 애플리케이션 모듈 업데이트 작업 설정

4. **로컬(사내) 모드 업데이트 설정** 블록에서 **설정** 버튼을 클릭합니다.



업데이트 경로

5. 업데이트 경로 목록에서 **추가** 버튼을 누릅니다.

6. **업데이트 경로** 필드에서 업데이트 패키지가 포함된 FTP 또는 HTTP 서버, 네트워크 폴더 또는 로컬 폴더의 주소를 지정합니다.

   각 업데이트 경로에 다음과 같은 형식을 사용해야 합니다:

   - FTP 또는 HTTP 서버를 선택할 경우 해당 웹 주소 또는 IP 주소를 입력합니다.

     예를 들어 `http://dnl-01.geo.kaspersky.com/` 또는 `93.191.13.103`과 같이 입력할 수 있습니다.

     FTP 서버를 선택할 경우 이 주소에 인증 설정을 지정할 수 있으며, 그 형식은 다음과 같습니다: `ftp://<user name>:<password>@<node>:<port>`.

   - 네트워크 폴더의 경우 UNC 경로를 입력합니다.

     예: `\\Server\Share\Update distribution`.

   - 로컬 폴더의 경우 해당 폴더의 전체 경로를 입력합니다.

     예: `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   업데이트 경로 목록에서 제거하지 않고 업데이트 경로를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.

7. **확인**을 누릅니다.

8. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

   첫 번째 업데이트 경로에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 경로로 자동 전환합니다.

9. 필요한 경우 모바일 모드 업데이트 소스를 추가합니다. *모바일 모드*는 컴퓨터가 조직 네트워크 경계를 벗어날 때(*오프라인 컴퓨터*)의 Kaspersky Endpoint Security 동작 모드입니다.

10. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 업데이트 경로를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.

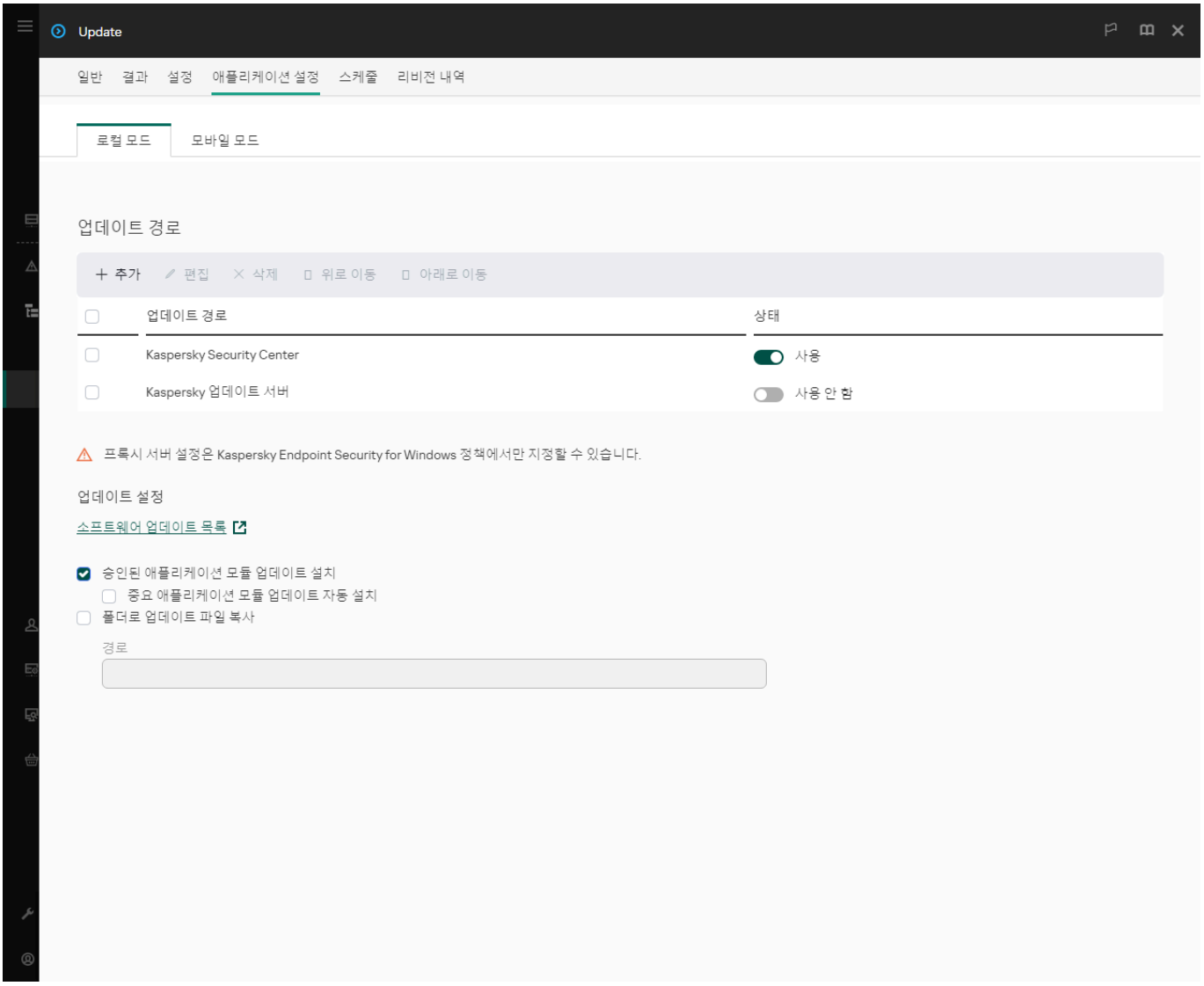
   작업 목록이 열립니다.

2. Kaspersky Endpoint Security의 **업데이트** 작업을 누릅니다.

   작업 속성 창이 열립니다.

   업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

3. **애플리케이션 설정** → **로컬 모드** 탭을 선택합니다.



업데이트 경로

4. 업데이트 경로 목록에서 **추가** 버튼을 누릅니다.

5. 열리는 창에서 업데이트 패키지가 포함된 FTP 또는 HTTP 서버, 네트워크 폴더 또는 로컬 폴더의 주소를 지정합니다.

   각 업데이트 경로에 다음과 같은 형식을 사용해야 합니다:

   - FTP 또는 HTTP 서버를 선택할 경우 해당 웹 주소 또는 IP 주소를 입력합니다.

     예를 들어 `http://dnl-01.geo.kaspersky.com/` 또는 `93.191.13.103`과 같이 입력할 수 있습니다.

     FTP 서버를 선택할 경우 이 주소에 인증 설정을 지정할 수 있으며, 그 형식은 다음과 같습니다:
     `ftp://<user name>:<password>@<node>:<port>`.

- 네트워크 폴더의 경우 UNC 경로를 입력합니다.

  예: `\\Server\Share\Update distribution`.

- 로컬 폴더의 경우 해당 폴더의 전체 경로를 입력합니다.

  예: `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

업데이트 경로 목록에서 제거하지 않고 업데이트 경로를 제외할 수 있습니다. 이렇게 하려면 옆의 토글 스위치를 끄기로 설정합니다.

6. **확인**을 누릅니다.

7. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

   첫 번째 업데이트 경로에서 업데이트를 수행할 수 없으면 Kaspersky Endpoint Security는 다음 경로로 자동 전환합니다.

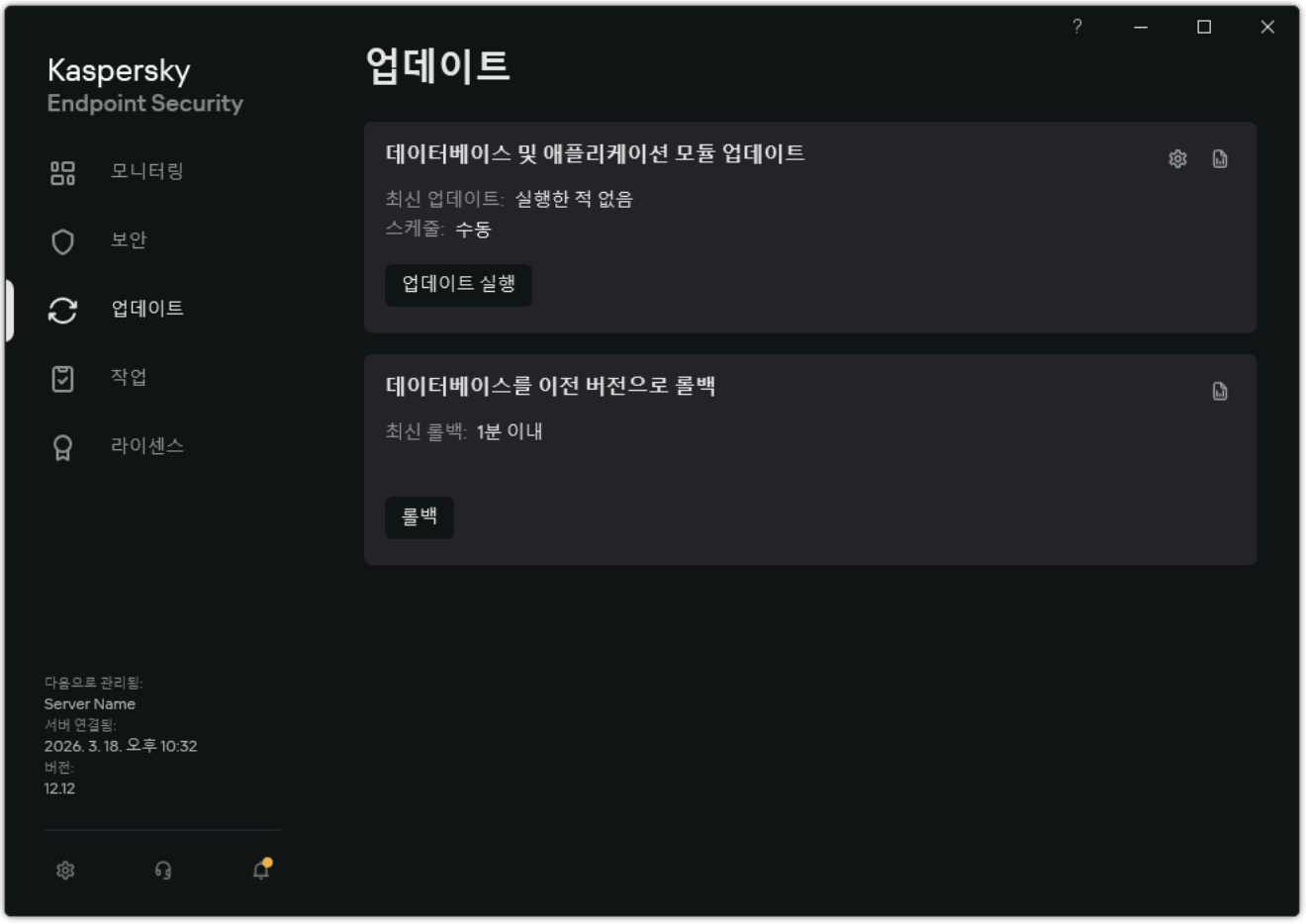
8. 필요한 경우 모바일 모드 업데이트 소스를 추가합니다. *모바일 모드*는 컴퓨터가 조직 네트워크 경계를 벗어날 때(*오프라인 컴퓨터*)의 Kaspersky Endpoint Security 동작 모드입니다.

9. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 업데이트 경로를 추가하는 방법

애플리케이션 인터페이스에서 *데이터베이스 및 애플리케이션 모듈 업데이트* 그룹 작업을 구성할 수 없습니다. 로컬 업데이트 작업인 *데이터베이스 및 애플리케이션 모듈 업데이트*만 사용자가 이용할 수 있습니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.

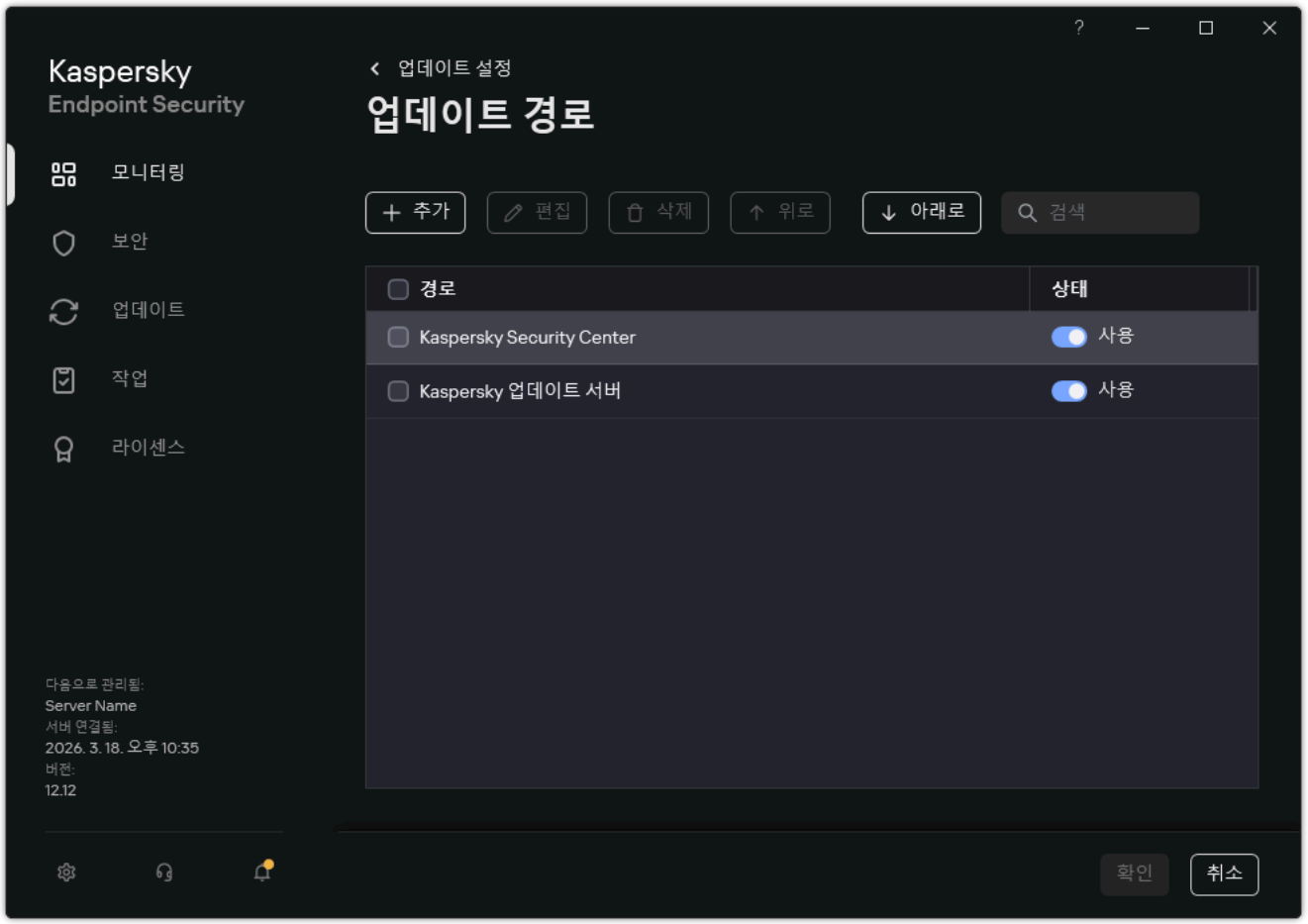


로컬 업데이트 작업

2. 작업 목록이 열립니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 선택하고 ⚙ 클릭합니다.
   작업 속성 창이 열립니다.

3. **업데이트 경로 선택**을 클릭합니다.

4. 열리는 창에서 **추가** 버튼을 누릅니다.



업데이트 경로

5. 열리는 창에서 업데이트 패키지가 포함된 FTP 또는 HTTP 서버, 네트워크 폴더 또는 로컬 폴더의 주소를 지정합니다.

   각 업데이트 경로에 다음과 같은 형식을 사용해야 합니다:

   - FTP 또는 HTTP 서버를 선택할 경우 해당 웹 주소 또는 IP 주소를 입력합니다.

     예를 들어 `http://dnl-01.geo.kaspersky.com/` 또는 `93.191.13.103`과 같이 입력할 수 있습니다.

     FTP 서버를 선택할 경우 이 주소에 인증 설정을 지정할 수 있으며, 그 형식은 다음과 같습니다: `ftp://<user name>:<password>@<node>:<port>`.

   - 네트워크 폴더의 경우 UNC 경로를 입력합니다.

     예: `\\Server\Share\Update distribution`.

   - 로컬 폴더의 경우 해당 폴더의 전체 경로를 입력합니다.

     예: `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. **선택**을 클릭합니다.

7. **위로** 및 **아래로** 버튼을 사용하여 업데이트 경로의 우선순위를 구성합니다.

8. 변경 사항을 저장합니다.

애플리케이션 모듈 업데이트

애플리케이션 모듈 업데이트는 오류를 수정하고 성능을 개선하며 새 기능을 추가합니다. 새 애플리케이션 모듈 업데이트를 사용할 수 있게 되면 업데이트 설치를 확인해야 합니다. 애플리케이션 인터페이스 또는 Kaspersky Security Center에서 애플리케이션 모듈 업데이트 설치를 확인할 수 있습니다. 업데이트를 이용할 수 있으면 애플리케이션이 Kaspersky Endpoint Security의 메인 창에 알림을 표시합니다: . 애플리케이션 모듈 업데이트를 검토하고 최종 사용자 라이센스 계약서 조항을 승인하면, 애플리케이션은 최종 사용자 라이센스 계약서가 사용자에 의해 수락된 후 업데이트를 설치합니다.

애플리케이션 업데이트 설치 시 컴퓨터를 다시 시작해야 할 수 있습니다.

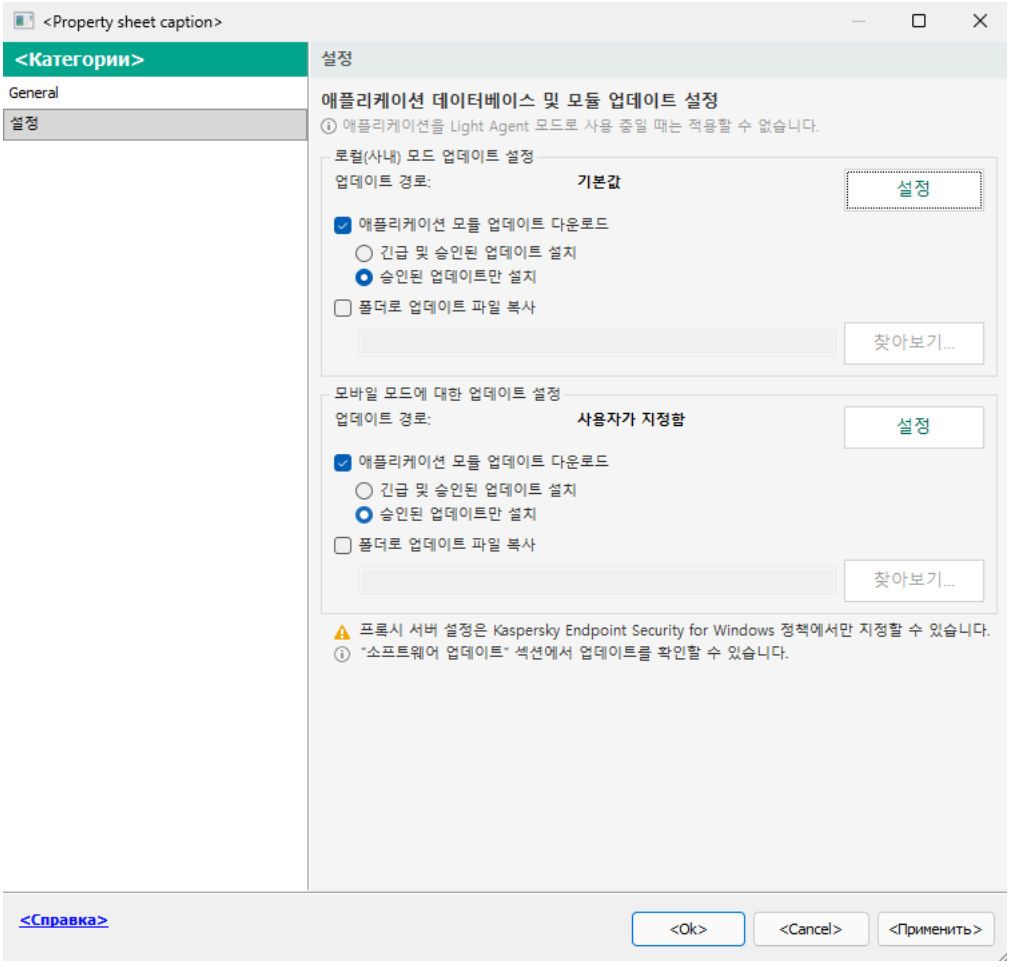
관리 콘솔(MMC)에서 애플리케이션 모듈 업데이트를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업**을 선택합니다.
3. Kaspersky Endpoint Security의 **데이터베이스 및 애플리케이션 모듈 업데이트** 작업을 클릭합니다.

   작업 속성 창이 열립니다.

   데이터베이스 및 애플리케이션 모듈 업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

4. 작업 속성 창에서 **설정** 섹션을 선택합니다.



데이터베이스 및 애플리케이션 모듈 업데이트 작업 설정

5. **로컬(사내) 모드 업데이트 설정** 차단에서 **애플리케이션 모듈 업데이트 다운로드** 확인란을 선택합니다.

   애플리케이션 모듈 업데이트가 다운로드되지 않도록 하려면 **애플리케이션 모듈 업데이트 다운로드** 확인란의 선택을 취소하고 사용자의 로컬 작업 사용을 금지합니다.

6. 설치할 애플리케이션 모듈 업데이트를 선택합니다.

   - **긴급 및 승인된 업데이트 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Endpoint Security는 자동으로 중요 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 Endpoint Security는 애플리케이션 모듈은 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다. 이 옵션은 기본적으로 선택되어 있습니다.

7. 필요 시 모바일 모드용 애플리케이션 모듈 업데이트를 구성합니다. *모바일 모드*는 컴퓨터가 조직 네트워크 경계를 벗어날 때(*오프라인 컴퓨터*)의 Kaspersky Endpoint Security 동작 모드입니다.

8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 애플리케이션 모듈 업데이트를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.

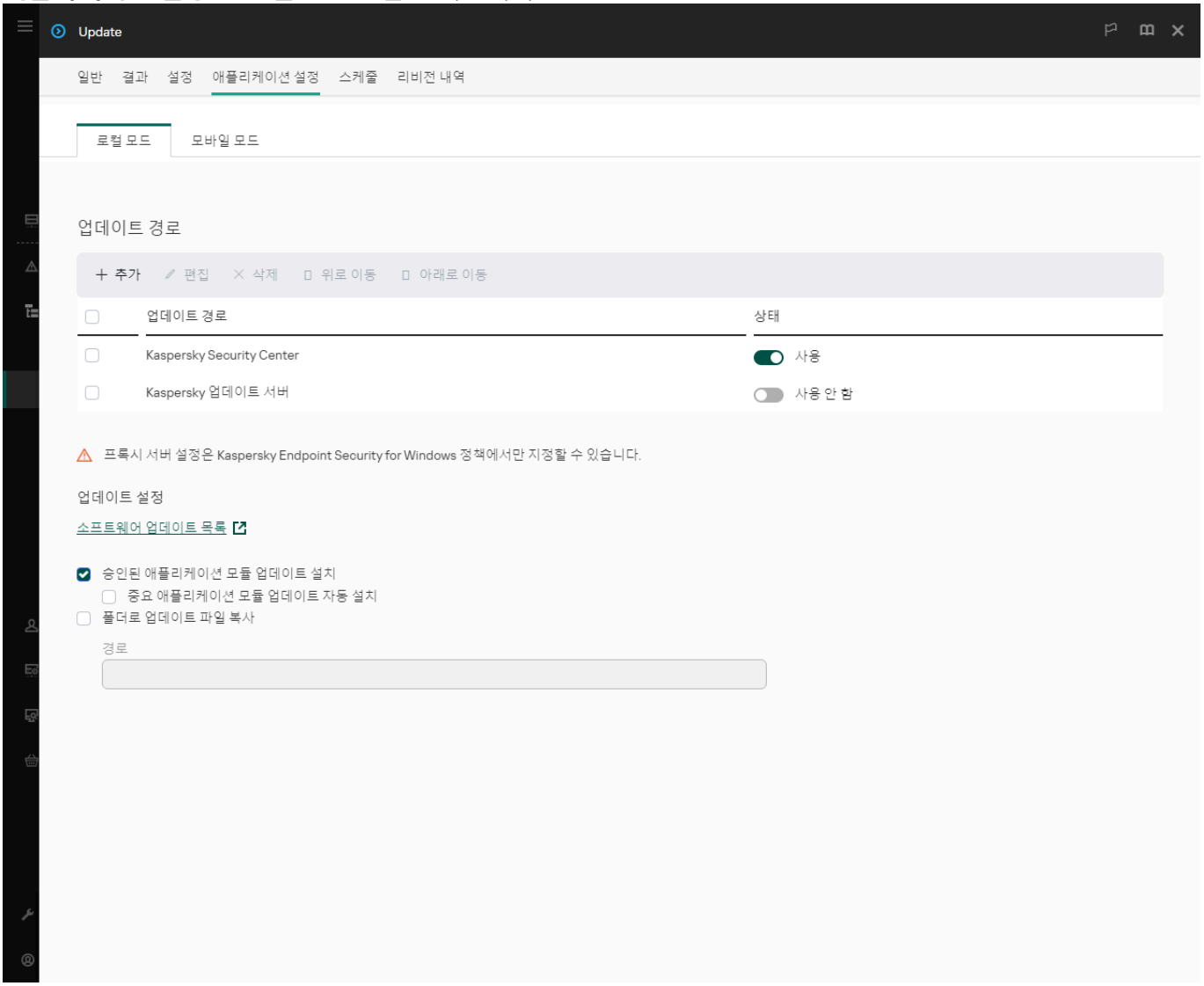
   작업 목록이 열립니다.

2. Kaspersky Endpoint Security의 **데이터베이스 및 애플리케이션 모듈 업데이트** 작업을 클릭합니다.

   작업 속성 창이 열립니다.

데이터베이스 및 애플리케이션 모듈 업데이트 작업은 중앙 관리 서버 빠른 시작 마법사로 자동으로 생성됩니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 생성하려면 마법사를 실행하는 동안 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치합니다.

3. **애플리케이션 설정 → 로컬 모드** 탭을 선택합니다.



업데이트 작업 설정

4. **업데이트 설정**에서 설치할 애플리케이션 모듈 업데이트를 선택합니다:

   - **승인된 애플리케이션 모듈 업데이트 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Endpoint Security는 애플리케이션 모듈은 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다. 이 옵션은 기본적으로 선택되어 있습니다.

   - **중요 애플리케이션 모듈 업데이트 자동 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Endpoint Security는 자동으로 중요 업데이트를 설치하고 나머지 모든 애플리케이션 모듈은 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다.

   애플리케이션 모듈 업데이트가 다운로드되지 않도록 하려면 **승인된 애플리케이션 모듈 업데이트 설치** 및 **중요 애플리케이션 모듈 업데이트 자동 설치** 확인란의 선택을 취소하고 사용자의 로컬 작업 사용을 금지합니다.

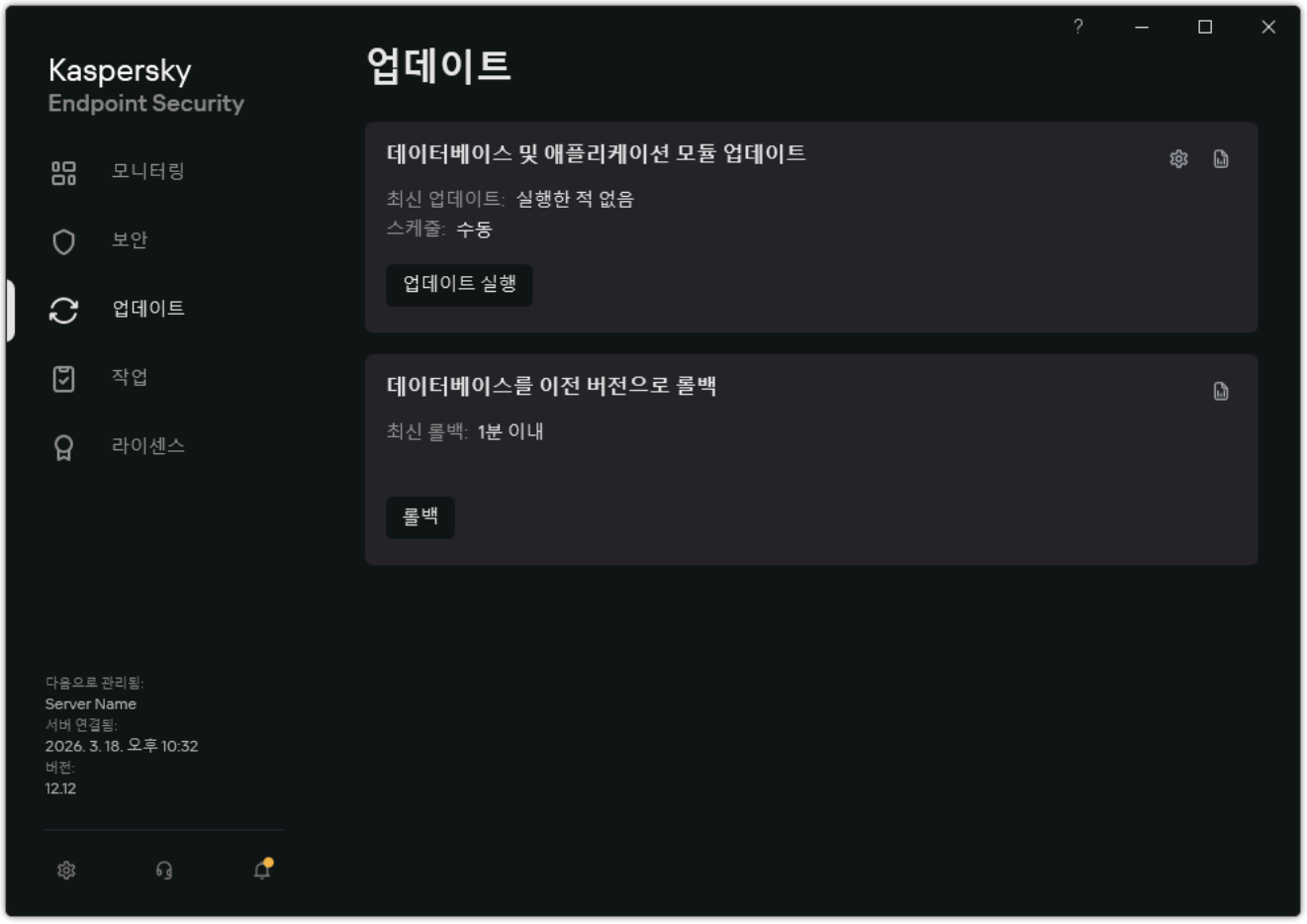
5. 필요 시 모바일 모드용 애플리케이션 모듈 업데이트를 구성합니다. *모바일 모드*는 컴퓨터가 조직 네트워크 경계를 벗어날 때(*오프라인 컴퓨터*)의 Kaspersky Endpoint Security 동작 모드입니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 애플리케이션 모듈 업데이트를 구성하는 방법

애플리케이션 인터페이스에서 *데이터베이스 및 애플리케이션 모듈 업데이트* 그룹 작업을 구성할 수 없습니다. 로컬 업데이트 작업인 *데이터베이스 및 애플리케이션 모듈 업데이트*만 사용자가 이용할 수 있습니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 표시되지 않으면 관리자가 정책에서 로컬 작업의 사용을 금지했다는 뜻입니다.

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.



로컬 업데이트 작업

2. 작업 목록이 열립니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 선택하고 ⚙ 클릭합니다.
   작업 속성 창이 열립니다.

3. **애플리케이션 모듈 업데이트 다운로드 및 설치** 블록에서 **애플리케이션 모듈 업데이트 다운로드** 확인란을 선택합니다.

4. 설치할 애플리케이션 모듈 업데이트를 선택합니다.

   - **긴급 및 승인된 업데이트 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Endpoint Security는 자동으로 중요 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 Endpoint Security는 애플리케이션 모듈은 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다. 이 옵션은 기본적으로 선택되어 있습니다.

5. 변경 사항을 저장합니다.

업데이트에 프록시 서버 사용

업데이트 경로에서 데이터베이스 및 애플리케이션 모듈 업데이트를 다운로드하려면 프록시 서버 설정을 지정해야 할 수 있습니다. 업데이트 경로가 여러 개이면 모든 경로에 프록시 서버 설정이 적용됩니다. 일부 업데이트 경로에는 프록시 서버가 필요하지 않은 경우 정책 속성에서 프록시 서버 사용을 중지할 수 있습니다. 또한 Kaspersky Endpoint Security는 프록시 서버를 사용하여 Kaspersky Security Network 및 활성화 서버에 접근합니다.

프록시 서버를 통해 업데이트 경로 연결을 구성하려면 다음과 같이 하십시오.

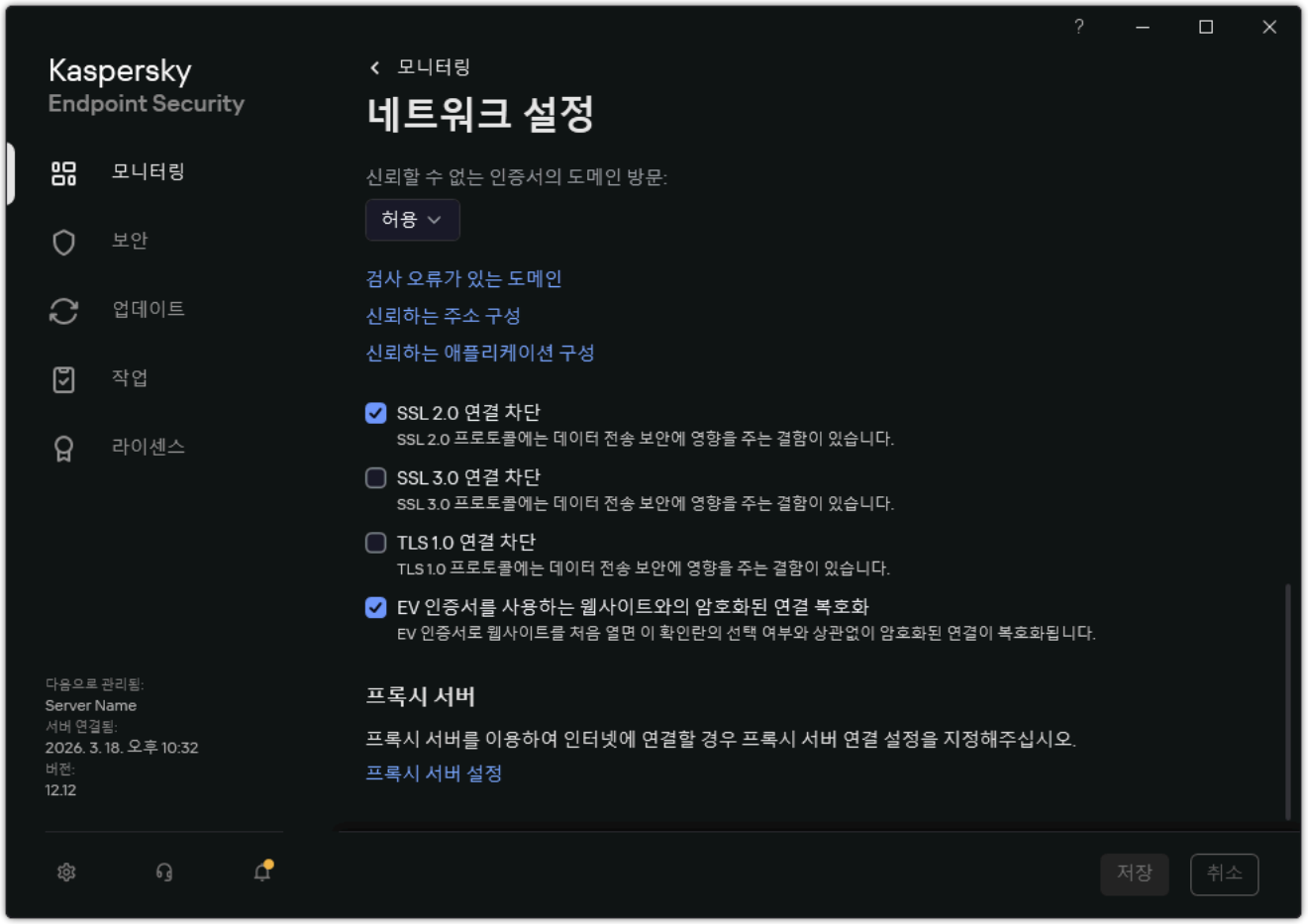
1. 웹 콘솔의 메인 창에서 ⚙ 클릭합니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **인터넷 연결 구성** 섹션으로 갑니다.
3. **프록시 서버 사용** 확인란을 선택합니다.
4. 프록시 서버 연결 설정을 구성합니다: 프록시 서버 주소, 포트 및 인증 설정(사용자 이름 및 암호).
5. 변경 사항을 저장합니다.

특정 관리 그룹에 대해 프록시 서버 사용을 중지하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **네트워크 설정**으로 갑니다.
5. **프록시 서버** 블록에서 **설정** 버튼을 누릅니다.
6. 창이 열리면 **로컬 주소에 대해 프록시 서버 우회** 확인란을 선택합니다.
7. 변경 사항을 저장합니다.

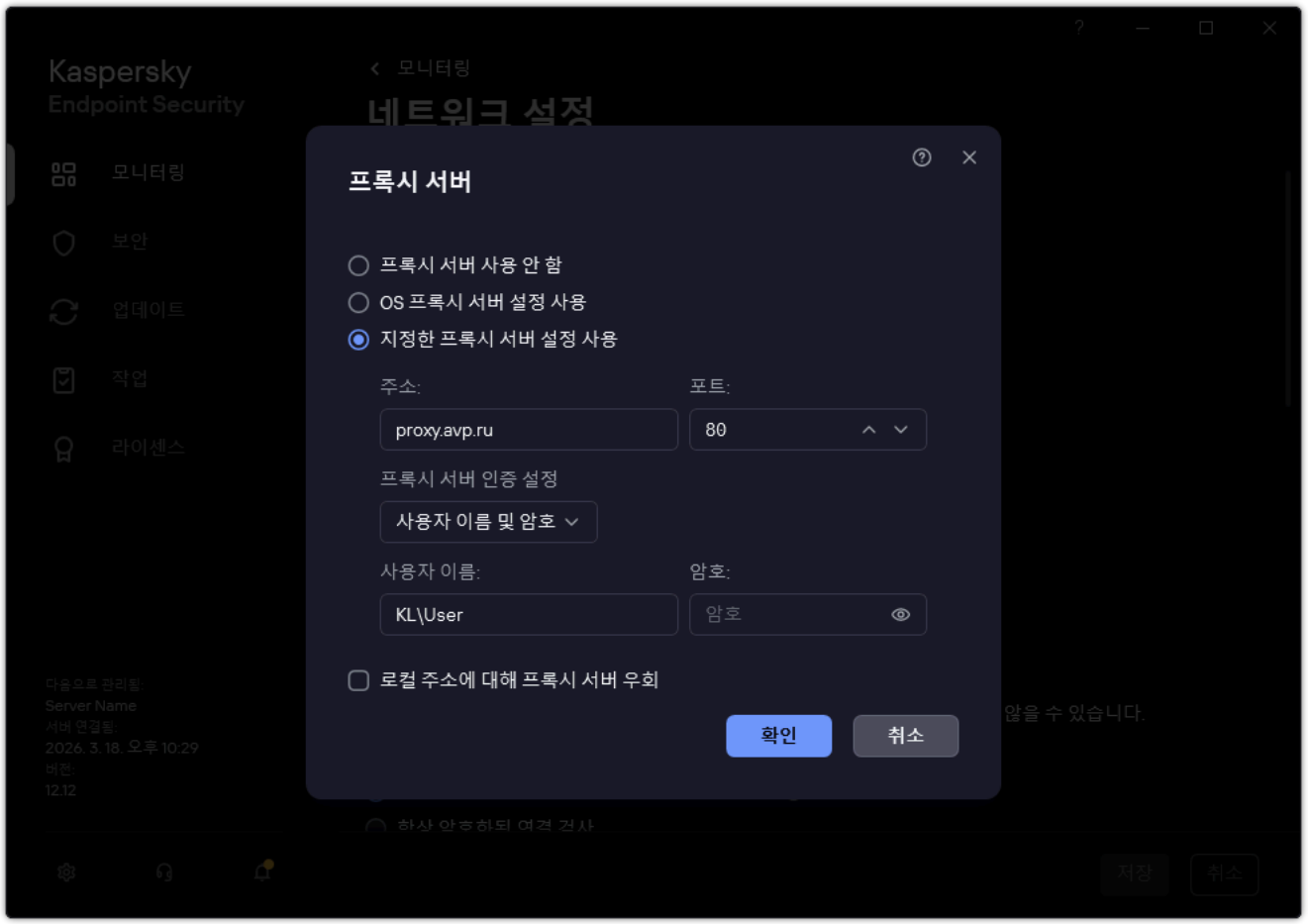
애플리케이션 인터페이스에서 프록시 서버 설정을 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.



애플리케이션 네트워크 설정

3. **프록시 서버** 블록에서 **프록시 서버 설정** 링크를 클릭합니다.



프록시 서버 연결 설정

4. 창이 열리면 다음 옵션 중 하나를 선택하여 프록시 서버 주소를 결정합니다:

- **OS 프록시 서버 설정 사용**.

  이 옵션은 기본적으로 선택되어 있습니다. Kaspersky Endpoint Security는 운영 체제 설정에 정의된 프록시 서버 설정을 사용합니다.

- **지정한 프록시 서버 설정 사용**.

  이 옵션을 선택하면 프록시 서버 연결 설정(프록시 서버 주소 및 포트)을 구성합니다.

5. 프록시 서버에서 애플리케이션이 인증하는 방식을 선택합니다. 기본적으로 애플리케이션은 현재 사용자의 도메인 NTLM 인증을 사용합니다.

6. 공유 폴더에서 데이터베이스 및 애플리케이션 모듈을 업데이트할 때 프록시 서버 사용을 중지하려면 **로컬 주소에 대해 프록시 서버 우회** 확인란을 선택합니다.

7. 변경 사항을 저장합니다.

결과적으로 Kaspersky Endpoint Security는 프록시 서버를 사용하여 애플리케이션 모듈 및 데이터베이스 업데이트를 다운로드합니다. 또한 Kaspersky Endpoint Security는 프록시 서버를 사용하여 KSN 서버 및 활성화 서버에 접근합니다. 프록시 서버에서 인증이 필요하지만 사용자 계정 정보가 제공되지 않았거나 올바르지 않을 시 Kaspersky Endpoint Security는 사용자 이름과 비밀번호를 입력하라는 메시지를 표시합니다.

마지막 업데이트 롤백

처음으로 데이터베이스 및 애플리케이션 모듈을 업데이트하면 데이터베이스 및 애플리케이션 모듈을 이전 버전으로 롤백하는 기능을 사용할 수 있습니다.

사용자가 업데이트 프로세스를 시작할 때마다 Kaspersky Endpoint Security는 현재 데이터베이스 및 애플리케이션 모듈의 백업 복사본을 생성합니다. 필요시 데이터베이스 및 애플리케이션 모듈을 이전 버전으로 롤백할 수 있습니다. 마지막으로 성공한 업데이트로 롤백하는 기능은 새로운 데이터베이스 버전에 잘못된 서명이 포함되어 Kaspersky Endpoint Security에서 안전한 애플리케이션을 차단하는 등의 경우에 유용합니다.

Light Agent 모드의 Kaspersky Endpoint Security는 *업데이트 롤백* 작업을 지원하지 않습니다.

관리 콘솔(MMC)에서 마지막 업데이트를 롤백하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

1. **Kaspersky Endpoint Security for Windows (14.0) → 업데이트 롤백**을 선택합니다.

2단계. 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.

3 단계. 작업 시작 스케줄 구성

작업 일정을 설정합니다(예: 수동).

4단계. 작업 이름 정의

작업 이름을 입력합니다.

7단계. 작업 생성 완료

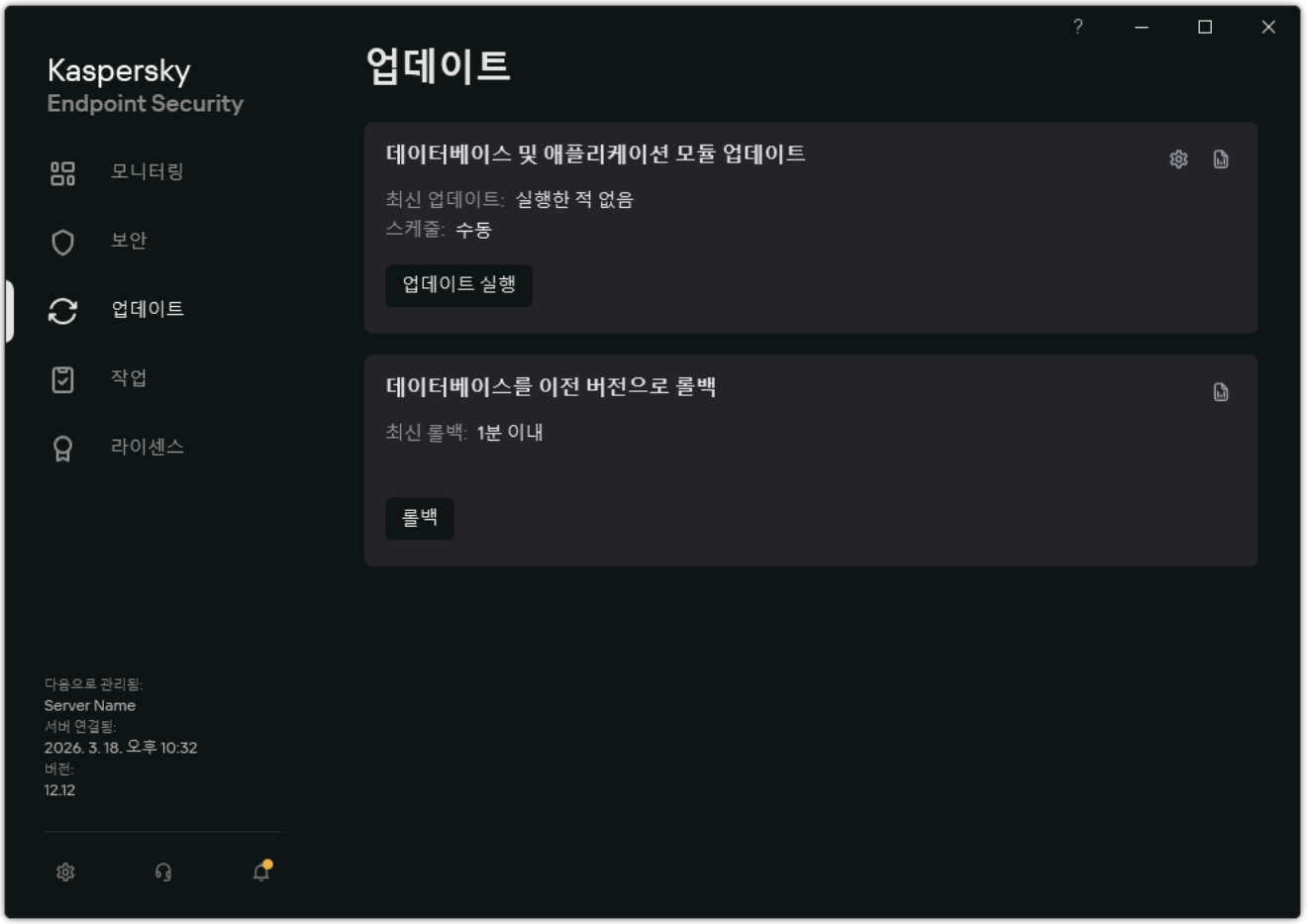
마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔에서 마지막 업데이트를 롤백하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **데이트 롤백**을 선택합니다.
   c. **작업 이름** 필드에 *데이트 롤백* 등과 같은 간단한 설명을 입력합니다.
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.
5. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.
6. 마법사를 끝냅니다.
7. 작업 목록에 새 작업이 표시됩니다.
8. 작업 옆의 확인란을 선택합니다.
9. **시작**을 클릭합니다.

애플리케이션 인터페이스에서 마지막 업데이트를 롤백하는 방법

1. 메인 애플리케이션 창에서 **업데이트** 섹션으로 이동합니다.



로컬 업데이트 작업

2. **데이터베이스를 이전 버전으로 롤백** 타일에서 **롤백** 버튼을 클릭합니다.

Kaspersky Endpoint Security는 마지막 데이터베이스 업데이트 롤백을 시작합니다. 애플리케이션은 롤백 진행률, 다운로드한 파일의 크기 및 업데이트 경로를 표시합니다. **업데이트 중지** 버튼을 클릭하여 언제든지 작업을 중지할 수 있습니다.

고급 치료 기술

Kaspersky Endpoint Security는 처리 안 된 보안 위협을 처리하기 위해 고급 치료 기술을 사용합니다. 고급 치료는 워크 스테이션 및 서버에서 다른 방식으로 작동합니다. *악성 코드 검사* 작업 설정과 애플리케이션 설정에서 고급 치료를 구성할 수 있습니다.

Kaspersky Endpoint Security가 악성 코드의 실행을 막을 수 없다면 고급 치료 기술을 사용할 수 있습니다. 정책이 적용된 컴퓨터에서 고급 치료는 컴퓨팅 리소스를 상당히 많이 사용하므로 기본적으로 비활성화되어 있습니다. 정책을 적용하지 않은 컴퓨터에서는 고급 치료가 기본적으로 활성화됩니다.

> 고급 치료는 워크 스테이션 및 서버에서 다른 방식으로 작동합니다. 서버에서 이 기술을 사용하려면 *악성 코드 검사* 작업의 속성에서 즉각적인 고급 치료를 활성화해야 합니다. 워크 스테이션에서 이 기술을 사용할 때는 이 절차가 필요하지 않습니다.

관리 콘솔(MMC)에서 고급 치료 기술을 활성화 또는 비활성화하는 방법

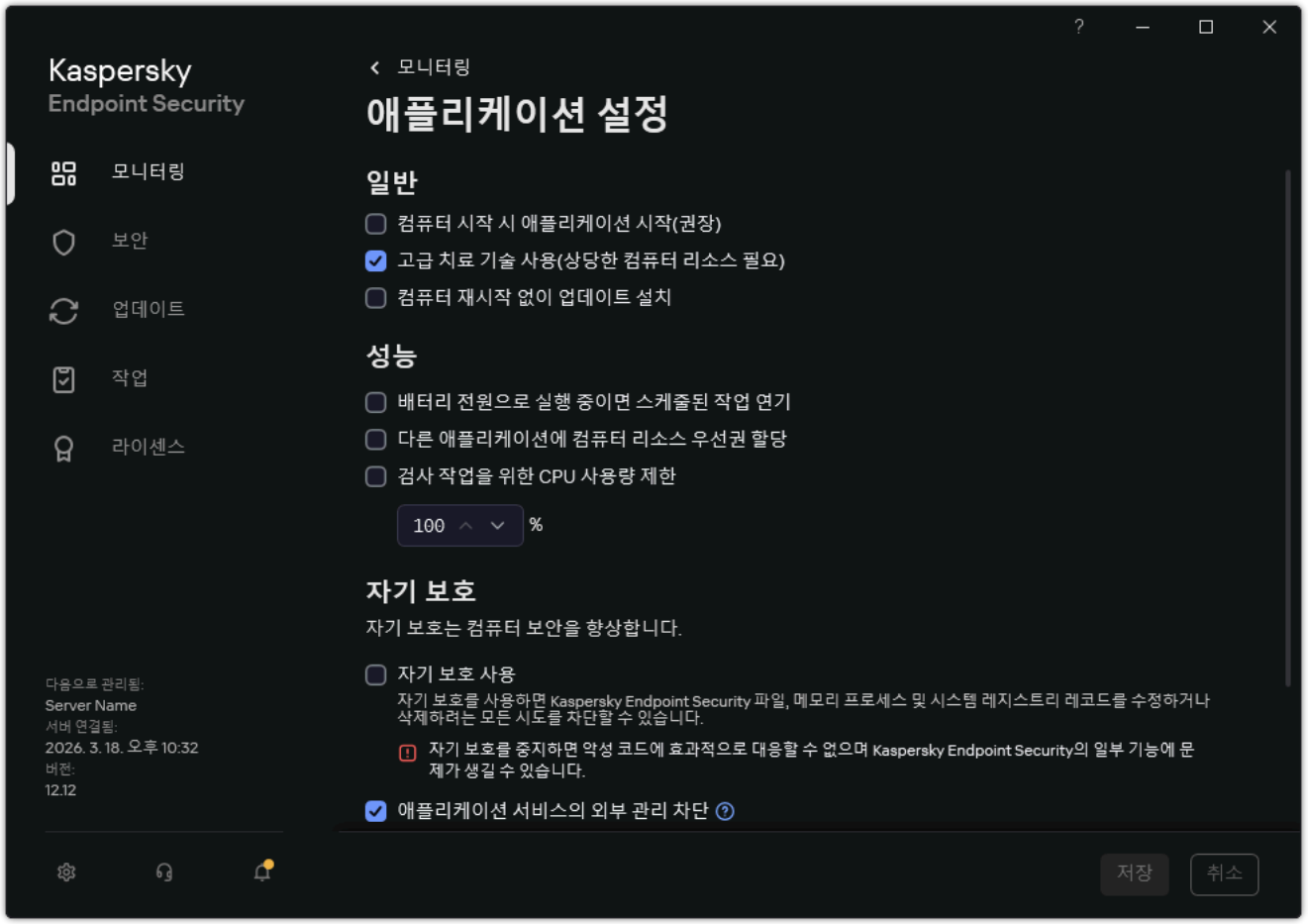
1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 애플리케이션 설정**을 차례로 선택합니다.
4. **일반** 블록에서 **고급 치료 기술 사용** 확인란으로 고급 치료 기술을 활성화 또는 비활성화합니다.
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 고급 치료 기술을 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 탐지 설정**을 선택합니다.
5. **고급 치료 기술** 블록에서 **고급 치료 기술 사용** 토글 스위치로 고급 치료 기술을 활성화하거나 비활성화합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 고급 치료 기술을 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정 → 애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

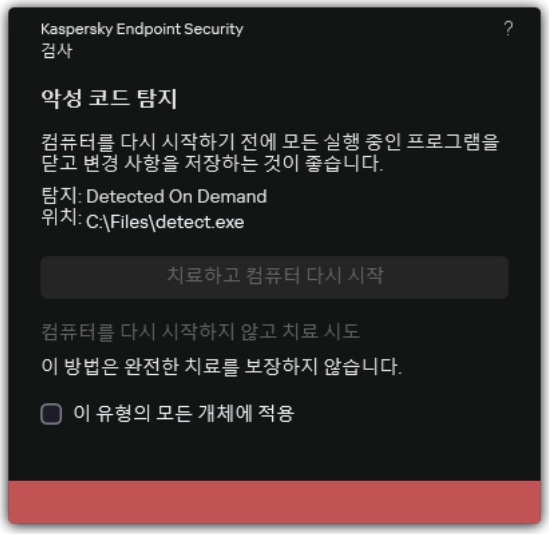
3. **일반** 블록에서 **고급 치료 기술 사용(상당한 컴퓨터 리소스 필요)** 확인란으로 고급 치료 기술을 활성화 또는 비활성화합니다.
4. 변경 사항을 저장합니다.

고급 치료가 진행 중일 때는 운영 체제 기능 대부분을 사용할 수 없게 됩니다. 치료가 완료되면 컴퓨터가 재부팅됩니다.

워크 스테이션의 처리 안 된 보안위협 치료

워크 스테이션의 처리 안 된 보안위협을 처리하려면, 애플리케이션 설정에서 고급 치료 기술을 활성화합니다. 그다음 *악성 코드 검사* 작업 속성에서 사용자 경험을 구성합니다. 작업 속성의 **고급 치료 즉시 실행** 확인란을 선택합니다. 플래그를 설정하면 Kaspersky Endpoint Security가 사용자에게 알리지 않고 치료를 수행합니다. 치료가 완료되면 컴퓨터가 재부팅됩니다. 플래그 설정을 해제하면 Kaspersky Endpoint Security가 처리 안 된 보안위협에 대한 알림을 표시합니다(아래 그림을 참조하십시오). 파일을 처리해야만 이 알림창을 닫을 수 있습니다.

이 컴퓨터에 적용된 정책의 속성에서 고급 치료 기능을 사용하는 경우에만 컴퓨터에서 바이러스 검사 작업 중 고급 치료가 수행됩니다.



처리 안 된 보안위협에 대한 알림

서버의 처리 안 된 보안위협 치료

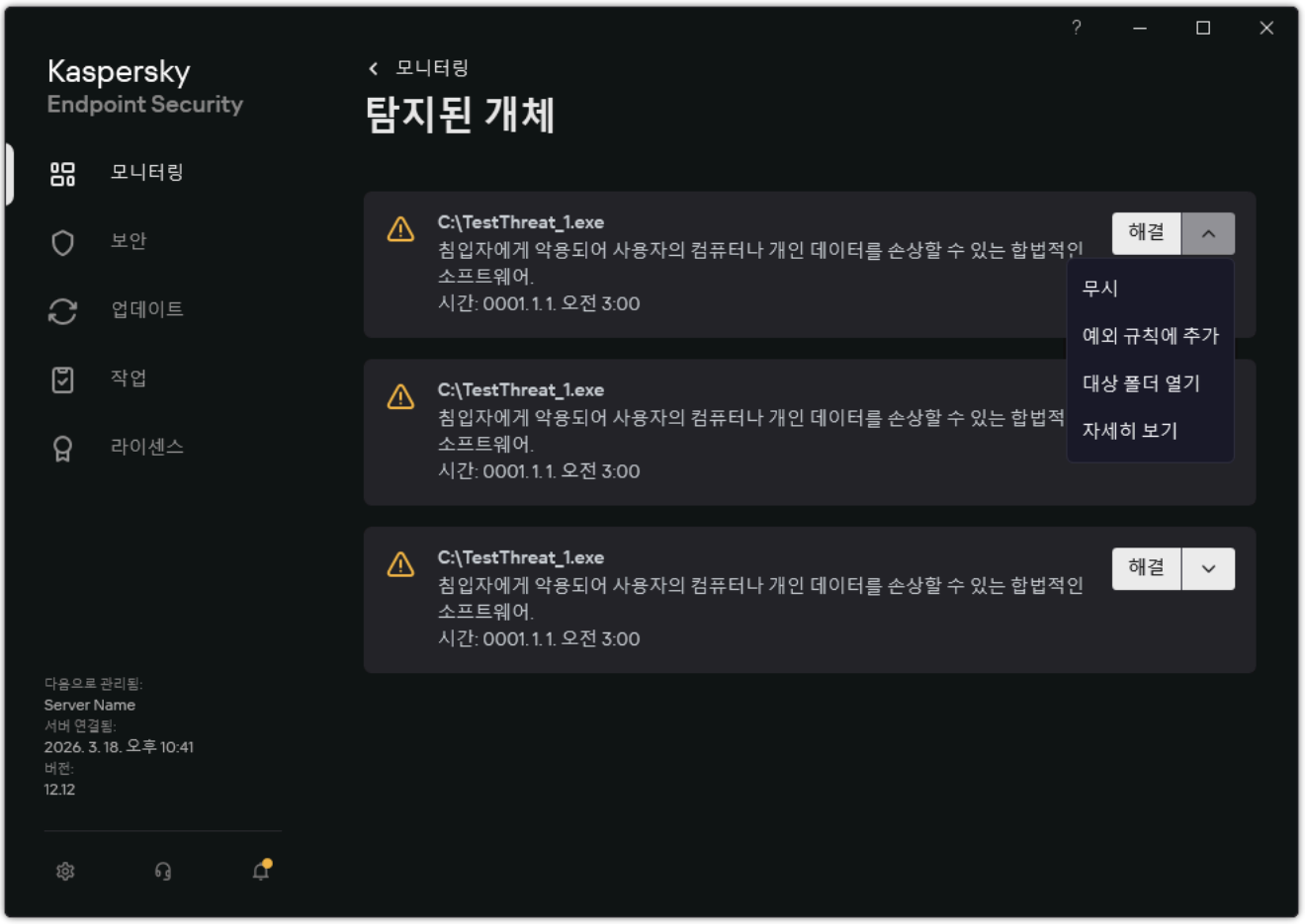
서버의 처리 안 된 보안위협을 처리하려면 다음을 수행해야 합니다.

- 애플리케이션 설정에서 고급 치료 기술을 활성화합니다.
- *악성 코드 검사* 작업 속성에서 즉각적인 고급 치료를 활성화합니다.

Kaspersky Endpoint Security를 서버용 Windows를 사용하는 컴퓨터에 설치하면 Kaspersky Endpoint Security가 알림을 표시하지 않습니다. 따라서 사용자가 처리 안 된 보안위협 치료를 위한 동작을 선택할 수 없습니다. 보안위협을 치료하려면 애플리케이션 설정에서 고급 치료 기술을 활성화하고 *악성 코드 검사* 작업 설정에서 즉각적인 고급 치료를 활성화해야 합니다. 그다음 *악성 코드 검사* 작업을 시작해야 합니다.

처리되지 않은 위협 제거

Kaspersky Endpoint Security는 어떤 이유로 인해 처리 안 된 파일에 대한 정보를 기록합니다. 이 정보는 처리 안 된 보안 위협 목록에서 이벤트 형식으로 기록됩니다(아래 그림 참조).



처리 안 된 보안위협 목록

Kaspersky Endpoint Security가 컴퓨터에서 바이러스 및 기타 악성 코드 검사 중 파일을 치료하거나 위협 요소를 제거했다면 감염된 파일이 *처리*로 간주됩니다.

어떤 이유로 Kaspersky Endpoint Security가 바이러스 및 기타 위협이 있는지 컴퓨터를 검사하는 동안 지정된 애플리케이션 설정에 따라 이 파일에 대한 처리 방법을 수행하지 못했다면 Kaspersky Endpoint Security는 해당 파일을 처리 안 된 위협 목록으로 이동합니다.

다음과 같은 경우에 이런 상황이 발생할 수 있습니다:

- 검사한 파일을 사용할 수 없습니다. 예를 들어 파일이 쓰기 권한이 없는 네트워크 드라이브 또는 이동식 드라이브에 있습니다.
- *악성 코드 검사* 작업 설정에서 보안위협 탐지 시 동작 작업이 **알림**으로 설정되어 있습니다. 그런 다음 화면에 감염된 파일 알림이 표시되고 사용자가 **무시**를 선택합니다.

처리되지 않은 보안위협이 있다면 Kaspersky Endpoint Security가 아이콘을 으로 변경합니다. 메인 애플리케이션 창에서 보안위협 알림이 표시됩니다(아래 그림 참조). Kaspersky Security Center 콘솔에서 컴퓨터 상태가 *심각*()으로 변경됩니다.

관리 콘솔(MMC)에서 보안위협을 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**를 선택합니다.

웹 콘솔 및 Cloud Console에서 보안위협을 처리하는 방법

1. 웹 콘솔의 기본 창에서 **동작** → **저장소** → **처리 안 된 위협**을 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**를 선택합니다.

애플리케이션 인터페이스에서 보안위협을 처리하는 방법

1. 메인 애플리케이션 창의 **모니터링** 섹션에서 **위험한 상태** 타일을 클릭합니다.
   처리 안 된 보안위협 목록이 열립니다.
2. 처리할 개체를 선택합니다.
3. 보안 위협을 처리할 방법을 선택합니다:
   - **해결**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.
   - **예외 규칙에 추가**. 이 작업을 선택하면 Kaspersky Endpoint Security가 파일을 검사 예외 목록에 추가할 것을 제안합니다. 예외 설정은 자동으로 구성됩니다. 예외 추가를 사용할 수 없다면 관리자가 정책 설정에서 예외 추가를 비활성화했다는 뜻입니다.
   - **무시**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 처리 안 된 보안위협 목록에서 해당 항목을 삭제합니다. 목록에 남아있는 처리 안 된 보안위협이 없으면 컴퓨터 상태가 *정상*으로 바뀝니다. 개체가 다시 탐지되면 Kaspersky Endpoint Security가 처리 안 된 보안위협 목록에 새 항목을 추가합니다.

- **대상 폴더 열기**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 파일 관리자의 개체가 있는 폴더를 엽니다. 그 후 직접 해당 개체를 삭제하거나 보호 범위 밖의 폴더로 옮길 수 있습니다.

- **자세히 보기**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 Kaspersky 취약점 및 위협 데이터베이스 웹사이트를 엽니다.

Kaspersky Security Center 콘솔에서 처리 안 된 위협을 처리하려면 처리되지 않은 파일 정보의 중앙 관리 서버 전송을 활성화해야 합니다. 데이터 전송은 기본적으로 활성화되어 있습니다.

관리 콘솔(MMC)에서 처리 안 된 파일 데이터 전송을 활성화하는 방법

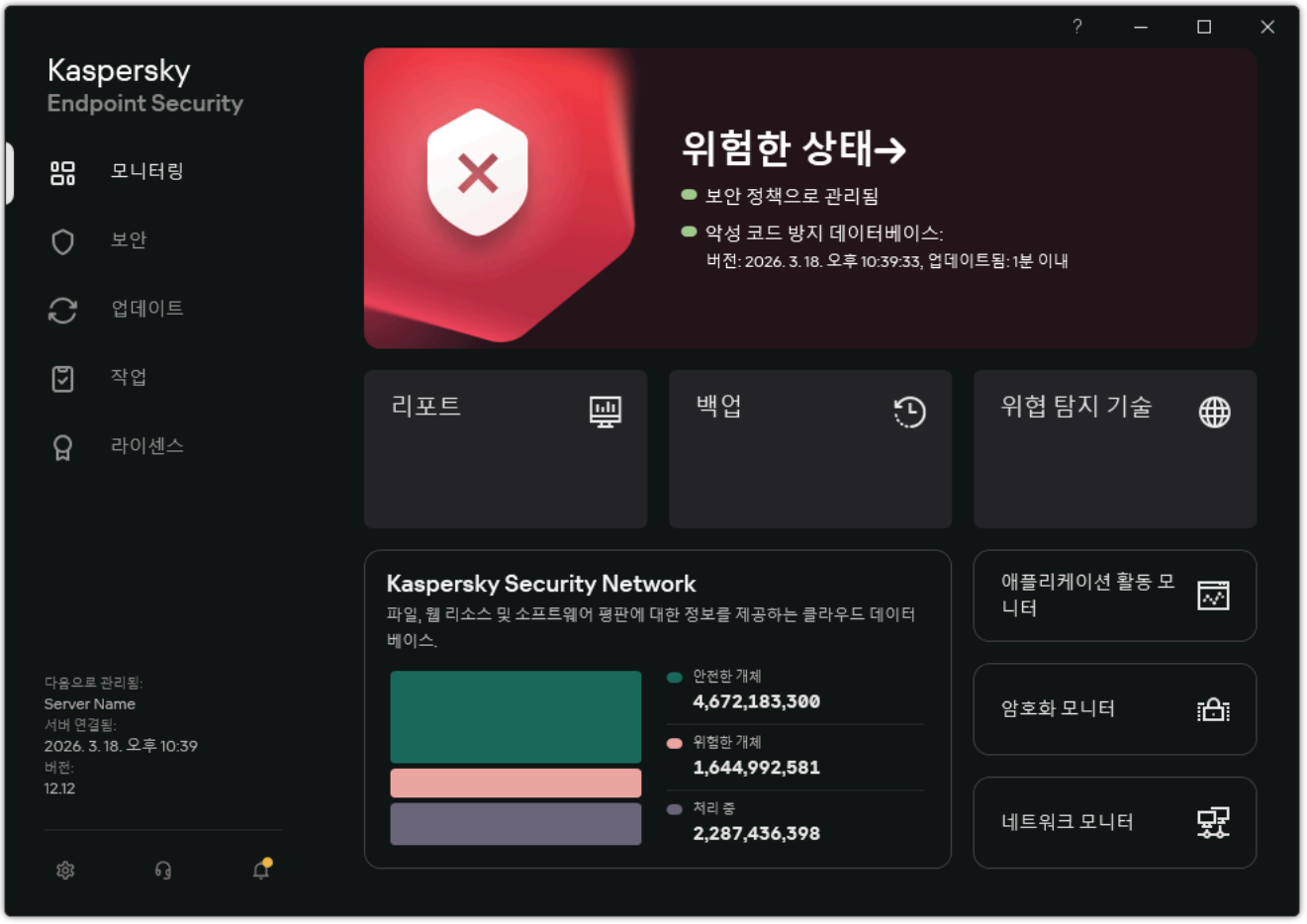
1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정** → **리포트 및 저장소**를 선택합니다.
4. **중앙 관리 서버로의 데이터 전송** 블록에서 **설정** 버튼을 클릭합니다.
5. **처리 안 된 파일** 확인란을 선택합니다.
6. 변경 사항을 저장합니다.

웹 콘솔에서 처리 안 된 파일 데이터 전송을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **KSC 통합**으로 갑니다.

5. **중앙 관리 서버로의 데이터 전송** 블록에서 **처리 안 된 파일 정보** 확인란을 선택합니다.

6. 변경 사항을 저장합니다.



위협 감지 시 메인 애플리케이션 창

컴퓨터 보호

파일 위협 보호

파일 위협 보호 구성 요소를 사용하면 컴퓨터 파일 시스템의 감염을 방지할 수 있습니다. 기본적으로 파일 위협 보호 구성 요소는 컴퓨터의 RAM에 영구적으로 상주하며 열려 있는 파일, 저장된 파일, 실행된 파일을 모두 실시간으로 검사합니다. 이 구성 요소는 연결된 드라이브를 포함하여 모든 컴퓨터 드라이브의 파일을 검사합니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다.

이 구성 요소는 사용자 또는 애플리케이션이 접근한 파일을 검사합니다. 악성 파일이 탐지되면 Kaspersky Endpoint Security가 파일 동작을 차단합니다. 그런 다음 애플리케이션은 파일 위협 보호 구성 요소의 설정에 따라 악성 파일을 치료하거나 삭제합니다.

OneDrive 클라우드 저장소에 내용을 보관하는 파일에 접근을 시도하면 Kaspersky Endpoint Security는 파일 내용을 다운로드하여 검사합니다.

파일 위협 보호 사용 및 중지

기본적으로 파일 위협 보호 구성 요소는 작동되며 Kaspersky 전문가가 권장하는 모드에서 실행됩니다. Kaspersky Endpoint Security는 파일 위협 보호에 대해 다양한 설정 그룹을 적용할 수 있습니다. 애플리케이션에 저장된 이러한 설정 그룹을 *보안 레벨*이라고 하며 **높음**, **권장**, **낮음**으로 설정할 수 있습니다. **권장** 보안 레벨 설정은 Kaspersky 전문가가 권장하는 최적의 설정입니다(아래 표를 참고하십시오). 미리 설정된 보안 레벨 중 하나를 선택하거나 직접 보안 레벨 설정을 구성할 수 있습니다. 보안 레벨 설정을 변경한 경우 언제든지 권장 보안 레벨로 되돌릴 수 있습니다.

파일 위협 보호 구성 요소는 다른 애플리케이션 구성 요소로부터 받은 데이터를 사용합니다. 해당 구성 요소의 활성화는 선택 사항입니다. 추가 데이터를 제공하는 구성 요소는 다음을 포함합니다:

- Kaspersky Security Network
- 호스트 침입 방지
- 행동 탐지

관리 콘솔(MMC)에서 파일 위협 보호 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 창에서 **필수 위협 보호** → **파일 위협 보호**를 선택합니다.
4. **파일 위협 보호** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.

5. 구성 요소를 활성화했다면 **보안 레벨** 블록에서 다음 중 하나를 수행합니다.

   - 미리 설정된 보안 레벨 중 하나를 적용하려면 슬라이더로 레벨을 선택합니다.

     - **높음**. 이 파일 보안 레벨을 선택하는 경우 파일 위협 보호 구성 요소가 열려 있거나 저장 또는 시작되는 모든 파일을 가장 엄격하게 제어합니다. 파일 위협 보호 구성 요소가 컴퓨터의 모든 하드 드라이브, 이동식 드라이브, 네트워크 드라이브에서 모든 파일 유형을 검사합니다. 또한 압축 파일, 설치 프로그램 패키지 및 삽입된 OLE 개체에 대한 검사도 수행합니다.

     - **권장**. 이 파일 보안 레벨은 Kaspersky Lab 전문가가 권장하는 레벨입니다. 파일 위협 보호 구성 요소가 컴퓨터의 모든 하드 드라이브, 이동식 드라이브, 네트워크 드라이브에서 지정된 파일 형식과 삽입된 OLE 개체만 검사합니다. 파일 위협 보호 구성 요소가 압축 파일이나 설치 패키지는 검사하지 않습니다.

     - **낮음**. 이 파일 보안 레벨 설정에서 검사 속도가 가장 빠릅니다. 파일 위협 보호 구성 요소는 컴퓨터의 모든 하드 드라이브, 이동식 드라이브 및 네트워크 드라이브에서 지정된 확장자를 가진 파일만 검사합니다. 파일 위협 보호 구성 요소가 복합 파일은 검사하지 않습니다.

   - 사용자 지정 보안 레벨을 구성하려면 **설정** 버튼을 클릭하고 직접 구성 요소 설정을 정의합니다.

     보안 레벨에서 **기본값**을 클릭하여 사전 설정된 보안 수준 값을 복원할 수 있습니다.

6. **위협 탐지 시 처리 방법** 블록에서는 악성 개체 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:

   - **치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.

   - **치료 - 불가능한 경우 차단**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 탐지된 모든 감염을 자동으로 치료합니다. 치료에 실패하면 Kaspersky Endpoint Security가 파일을 차단합니다(읽기/쓰기).

   - **차단**. 이 옵션을 선택한 경우 파일 위협 보호 구성 요소가 탐지된 모든 감염 파일을 치료하려고 시도하지 않고 자동으로 차단합니다.

   - **알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 감염된 파일에 대한 정보를 해당 파일 탐지 시 처리 안 된 위협 목록에 추가합니다.

   > 감염된 파일을 치료하거나 삭제하기 전에 애플리케이션이 파일을 복원하거나 나중에 치료할 수 있을 때에 대비하여 파일의 복사본을 만듭니다.

7. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 파일 위협 보호 구성 요소를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **호스트 위협 보호** → **파일 위협 보호**로 갑니다.

5. **파일 위협 보호 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.

6. 보호 범위에 새로운 개체를 추가하려면 다음과 같이 하십시오.

   a. **고급 설정**에서 **보호 범위** 탭을 선택합니다.

   b. **추가**를 클릭합니다.

   c. 창이 열립니다. 이 창에서 보호 범위에 추가할 개체를 선택합니다.

   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.

   파일 또는 폴더 경로 어디서든 마스크를 사용할 수 있습니다. 예를 들어, 컴퓨터에 있는 모든 사용자 계정의 다운로드 폴더를 검사 범위에 포함시키려면 `C:\Users\*\Downloads\` 마스크를 입력합니다.

   보호 범위의 개체 목록에서 개체를 삭제하지 않고도 보호 대상에서 개체를 제외할 수 있습니다. 이렇게 하려면 옆의 토글 스위치를 끄기로 설정합니다.

   d. 변경 사항을 저장합니다.

7. **위협 탐지 시 처리 방법** 블록에서는 악성 개체 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:

   - **치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.

   - **치료 - 불가능한 경우 차단**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 탐지된 모든 감염을 자동으로 치료합니다. 치료에 실패하면 Kaspersky Endpoint Security가 파일을 차단합니다(읽기/쓰기).

   - **차단**. 이 옵션을 선택한 경우 파일 위협 보호 구성 요소가 탐지된 모든 감염 파일을 치료하려고 시도하지 않고 자동으로 차단합니다.

   > 감염된 파일을 치료하거나 삭제하기 전에 애플리케이션이 파일을 복원하거나 나중에 치료할 수 있을 때에 대비하여 파일의 복사본을 만듭니다.

8. 필요하다면 파일 위협 보호의 고급 설정을 편집합니다.

9. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 파일 위협 보호 구성 요소를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.

3. **파일 위협 보호** 토글로 구성 요소를 사용하거나 중지합니다.

4. 구성 요소를 활성화했다면 **보안 레벨** 블록에서 다음 중 하나를 수행합니다.

   - 미리 설정된 보안 레벨 중 하나를 적용하려면 슬라이더로 레벨을 선택합니다.

     - **높음**. 이 파일 보안 레벨을 선택하는 경우 파일 위협 보호 구성 요소가 열려 있거나 저장 또는 시작되는 모든 파일을 가장 엄격하게 제어합니다. 파일 위협 보호 구성 요소가 컴퓨터의 모든 하드 드라이브, 이동식 드라이브, 네트워크 드라이브에서 모든 파일 유형을 검사합니다. 또한 압축 파일, 설치 프로그램 패키지 및 삽입된 OLE 개체에 대한 검사도 수행합니다.

     - **권장**. 이 파일 보안 레벨은 Kaspersky Lab 전문가가 권장하는 레벨입니다. 파일 위협 보호 구성 요소가 컴퓨터의 모든 하드 드라이브, 이동식 드라이브, 네트워크 드라이브에서 지정된 파일 형식과 삽입된 OLE 개체만 검사합니다. 파일 위협 보호 구성 요소가 압축 파일이나 설치 패키지는 검사하지 않습니다.

     - **낮음**. 이 파일 보안 레벨 설정에서 검사 속도가 가장 빠릅니다. 파일 위협 보호 구성 요소는 컴퓨터의 모든 하드 드라이브, 이동식 드라이브 및 네트워크 드라이브에서 지정된 확장자를 가진 파일만 검사합니다. 파일 위협 보호 구성 요소가 복합 파일은 검사하지 않습니다.

   - 사용자 지정 보안 레벨을 구성하려면 **고급 설정** 버튼을 클릭하고 고유 구성 요소 설정을 정의합니다.

     권장 보안 레벨 복원 버튼을 클릭하여 미리 설정된 보안 레벨을 복원할 수 있습니다.

5. **위협 탐지 시 처리 방법** 블록에서는 악성 개체 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:

   - **치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.

   - **치료 - 불가능한 경우 차단**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 탐지된 모든 감염을 자동으로 치료합니다. 치료에 실패하면 Kaspersky Endpoint Security가 파일을 차단합니다(읽기/쓰기).

   - **차단**. 이 옵션을 선택한 경우 파일 위협 보호 구성 요소가 탐지된 모든 감염 파일을 치료하려고 시도하지 않고 자동으로 차단합니다.

   - **알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 감염된 파일에 대한 정보를 해당 파일 탐지 시 처리 안 된 위협 목록에 추가합니다.

   > 감염된 파일을 치료하거나 삭제하기 전에 애플리케이션이 파일을 복원하거나 나중에 치료할 수 있을 때에 대비하여 파일의 복사본을 만듭니다.

6. 변경 사항을 저장합니다.

Kaspersky 전문가가 권장하는 파일 위협 보호 설정(권장 보안 레벨)

파라미터	값	설명
파일 유형	**형식에 따라 검사한 파일**	이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일에 악성 코드가 있는지 검사하기 전에 파일의 내부 헤더를 분석하여 파일 형식을 결정합니다(예: txt, .doc 또는 .exe). 또한 이 검사에서는 특정 파일 확장자를 가진 파일도 찾습니다.
휴리스틱 분석	**빠른 검사**	현재 버전의 Kaspersky 애플리케이션 데이터베이스를 사용하여 식별할 수 없는 위협을 탐지하기 위해 개발된 기술입니다. 알려지지 않은 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 파일을 탐지합니다. 파일에서 악성 코드를 검사할 때 휴리스틱 분석기는 실행 파일의 명령을 실행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
새로운 파일과 수정된 파일만 검사	**켜기**	새로운 파일과 마지막 검사 이후 수정된 파일만 검사합니다. 이는 검사 시간을 줄이는 것입니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.

파라미터	값	설명
iSwift 기술 사용	**켜기**	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.
iChecker 기술 사용	**켜기**	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.
Microsoft Office 형식 파일 검사	**켜기**	Microsoft Office 파일(DOC, DOCX, XLS, PPT 및 기타 Microsoft 확장자)을 검사합니다. Office 형식 파일에는 OLE 개체도 포함됩니다. 애플리케이션이 확인란 선택 여부와 상관없이 1MB보다 작은 오피스 형식 파일을 검사합니다.
이메일 형식 파일 검사	**켜기**	이메일 형식 파일 검사. 애플리케이션이 MSG 및 EML 파일을 검사합니다. 이메일 형식 파일에는 OLE 개체 및 MHT 파일도 포함됩니다. Kaspersky Endpoint Security는 확인란 선택 여부와 상관없이 1MB보다 작은 이메일 형식 파일을 검사합니다.
검사 모드	**스마트 모드**	이 모드에서 파일 위협 보호는 개체에 대해 수행된 처리의 분석 내용에 따라 개체를 검사합니다. 예를 들어 Microsoft Office 문서 작업의 경우 Kaspersky Endpoint Security는 파일이 처음 열릴 때와 마지막에 닫힐 때 파일을 검사합니다. 그 사이에 파일에 쓰는 작업은 검사되지 않습니다.
위협 탐지 시 처리 방법	**치료 - 불가능한 경우 삭제**	이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.

파일 위협 보호 자동 일시 중지

지정한 시간이 되거나 특정 애플리케이션을 작동할 때 자동으로 파일 위협 보호가 일시 중지하도록 구성할 수 있습니다.

파일 위협 보호는 일부 애플리케이션과 충돌할 때 마지막 수단으로만 일시 중지해야 합니다. 구성 요소 실행 중 충돌이 발생하면 Kaspersky 기술 지원에 문의해주시기 바랍니다. 지원 전문가는 파일 위협 보호 구성 요소가 컴퓨터의 다른 애플리케이션과 동시에 실행되도록 설정하는 것을 도와줍니다.

파일 위협 보호를 자동으로 일시 중지하도록 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. **파일 위협 보호 일시 중지** 블록에서 **파일 위협 보호 일시 중지** 링크를 클릭합니다.
5. 창이 열리면 파일 위협 보호 일시 중지 설정을 구성합니다.
   a. 파일 위협 보호 자동 일시 중지 스케줄을 구성합니다.
   b. 파일 위협 보호가 작업을 일시 중지할 애플리케이션 목록을 만듭니다.
6. 변경 사항을 저장합니다.

파일 위협 보호 구성 요소가 감염된 파일에 수행하는 처리 방법 변경

기본적으로 파일 위협 보호 구성 요소는 탐지된 모든 감염 파일을 자동으로 치료합니다. 치료에 실패할 경우 파일 위협 보호 구성 요소가 이러한 파일을 삭제합니다.

파일 위협 보호 구성 요소가 감염된 파일에 취하는 조치를 변경하려면 다음과 같이 진행합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.
3. **위협 탐지 시 처리 방법** 블록에서 관련 옵션을 선택합니다:
   - **치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다.
   - **치료 - 불가능한 경우 차단**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 탐지된 모든 감염을 자동으로 치료합니다. 치료에 실패하면 Kaspersky Endpoint Security가 파일을 차단합니다(읽기/쓰기).
   - **차단**. 이 옵션을 선택한 경우 파일 위협 보호 구성 요소가 탐지된 모든 감염 파일을 치료하려고 시도하지 않고 자동으로 차단합니다.

   감염된 파일을 치료하거나 삭제하기 전에 애플리케이션이 파일을 복원하거나 나중에 치료할 수 있을 때에 대비하여 파일의 복사본을 만듭니다.
4. 변경 사항을 저장합니다.

파일 위협 보호 구성 요소의 보호 범위 구성

보호가 작동되는 경우 구성 요소가 검사하는 개체를 보호 범위이라고 합니다. 각 구성 요소의 보호 범위는 서로 다른 속성을 가집니다. 검사되는 파일의 유형과 위치는 파일 위협 보호 구성 요소의 보호 범위 속성입니다. 기본적으로 파일 위협 보호 구성 요소는 하드 드라이브, 이동식 드라이브 및 네트워크 드라이브에서 실행되는 감염 의심 파일만 검사합니다.

검사할 파일 유형을 선택할 때 다음을 고려하십시오.

1. 특정 형식의 파일(예: TXT 형식)에 악성 코드를 포함시키고 추후 이를 활성화할 가능성은 낮습니다. 반면, 실행 코드(예: .exe, .dll)를 포함하는 파일 형식도 있습니다. 실행 코드에는 이러한 목적으로 사용되지 않는 파일 형식(예: DOC 형식)에도 포함될 수 있습니다. 악성 코드가 침투하여 활성화될 위험이 높습니다.
2. 침입자가 실행 파일의 이름을 .txt 확장명으로 변경하고 컴퓨터에 바이러스나 기타 악성 애플리케이션을 보낼 수도 있습니다. 만일 확장자로 파일 검사를 선택하면 애플리케이션은 검사하는 동안 이 파일은 건너뜁니다. 파일 형식별 검사를 선택하면 Kaspersky Endpoint Security가 확장자와 상관없이 파일 헤더를 분석합니다. 이 분석에서 파일이 실행 파일 형식(예: EXE)으로 확인되면 애플리케이션은 해당 파일을 검사합니다.

보호 범위를 만들려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. **파일 유형** 블록에서 파일 위협 보호 구성 요소가 검사 작업을 수행할 파일 유형을 지정합니다.
   - **모든 파일**. 이 설정을 사용하면 Kaspersky Endpoint Security가 예외 없이 모든 형식과 확장자의 파일을 검사합니다.
   - **형식에 따라 검사한 파일**. 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일에 악성 코드가 있는지 검사하기 전에 파일의 내부 헤더를 분석하여 파일 형식을 결정합니다(예: txt, .doc 또는 .exe). 또한 이 검사에서는 특정 파일 확장자를 가진 파일도 찾습니다.
   - **확장자에 따라 검사한 파일** 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일 형식은 파일 확장자를 기반으로 결정됩니다.
5. **보호 범위 편집** 링크를 클릭합니다.
6. 창이 열리면 보호 범위에 추가하거나 제외할 개체를 선택합니다.

   > 기본 검사 범위에 포함된 개체는 삭제하거나 편집할 수 없습니다.

7. 보호 범위에 새로운 개체를 추가하려면 다음과 같이 하십시오.
   a. **추가**를 클릭합니다.
   폴더 트리가 열립니다.
   b. **경로** 필드에 폴더 또는 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.

   파일 또는 폴더 경로 어디서든 마스크를 사용할 수 있습니다. 예를 들어, 컴퓨터에 있는 모든 사용자 계정의 다운로드 폴더를 검사 범위에 포함시키려면 `C:\Users\*\Downloads\` 마스크를 입력합니다.
   컴퓨터 내 파일 리소스 목록의 **내 PC** 개체는 **모든 하드 드라이브**, **모든 네트워크 드라이브**, **모든 이동식 드라이브**를 포함합니다.

검사 범위의 개체 목록에서 개체를 삭제하지 않고도 검사에서 개체를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.

8. 변경 사항을 저장합니다.

검사 방법 사용

Kaspersky Endpoint Security는 머신 러닝 및 시그니처 분석이라는 검사 기술을 사용합니다. 시그니처 분석 시 Kaspersky Endpoint Security는 데이터베이스의 기록과 탐지된 개체가 일치하는지 확인합니다. Kaspersky 전문가의 권고에 따라 기본적으로 머신 러닝과 시그니처 분석이 사용되도록 선택되어 있습니다.

보호의 효율성을 높이려면 휴리스틱 분석을 사용합니다. 파일에서 악성 코드를 검사할 때 휴리스틱 분석기는 실행 파일의 명령을 실행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.

파일 위협 보호 구성 요소의 작업에 휴리스틱 분석 기술을 사용하도록 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. 애플리케이션이 파일 위협 보호를 위해 휴리스틱 분석을 사용하도록 하려면 **검사 방법** 블록에서 **휴리스틱 분석** 확인란을 선택합니다. 그런 다음 슬라이더를 사용하여 휴리스틱 분석 레벨을 설정합니다: **빠른 검사**, **보통 검사**, **상세 검사**.
5. 변경 사항을 저장합니다.

파일 위협 보호 동작에 검사 기술 사용

파일 위협 보호 작업에 검사 기술을 사용하도록 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.

4. **검사 기술** 블록에서 파일 위협 보호에 사용할 기술 이름 옆의 확인란을 선택합니다:

   - **iSwift 기술 사용**. 이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.

   - **iChecker 기술 사용**. 이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.

5. 변경 사항을 저장합니다.

파일 검사 최적화

파일 위협 보호 구성 요소에서 수행하는 파일 검사를 최적화하여 검사 시간을 단축하고 Kaspersky Endpoint Security의 작업 속도를 높일 수 있습니다. 검사 최적화는 새 파일과 마지막 검사 후 변경된 파일만 검사하는 방법으로 이루어집니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.

또한, iChecker 및 iSwift 기술을 사용하면 최근에 검사된 후로 수정되지 않은 파일을 제외하여 파일 검사 속도를 최적화할 수 있습니다.

파일 검사를 최적화하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. **최적화** 블록에서 **새로운 파일과 수정된 파일만 검사** 확인란을 선택합니다.
5. 변경 사항을 저장합니다.

복합 파일 검사

바이러스나 기타 악성 코드를 숨기는 일반적인 방법은 압축 파일이나 데이터베이스와 같은 복합 파일에 심는 것입니다. 이런 방법으로 숨겨진 바이러스나 기타 악성 코드를 탐지하려면 복합 파일을 압축 해제 해야 하는데 그러면 검사 속도가 느려질 수 있습니다. 검사할 복합 파일의 유형을 제한하는 방법으로 검사 속도를 높일 수 있습니다.

감염된 복합 파일을 처리하는 방법(치료 또는 삭제)은 파일 유형에 따라 달라집니다.

파일 위협 보호 구성 요소는 ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR 및 ICE 형식의 복합 파일을 치료하고 다른 모든 형식의 파일을 삭제합니다(메일 데이터베이스 예외).

복합 파일 검사를 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. **복합 파일 검사** 블록에서 압축 파일, 배포 패키지, 메일 또는 오피스 형식의 파일 등 검사할 복합 파일의 유형을 지정합니다.
5. 새로운 파일 및 수정된 파일만 검사를 중지하면 유형별 복합 파일 검사에 대한 설정을 구성합니다(이 유형의 모든 파일 또는 새로운 파일 만 검사).

   새로운 파일 및 수정된 파일만 검사를 사용하면 Kaspersky Endpoint Security는 모든 유형의 복합 파일에 대해 새로운 파일 및 수정된 파일만 검사합니다.
6. 복합 파일 검사를 위한 고급 설정을 구성합니다.
   - **큰 복합 파일은 압축 해제 안 함**.

     이 확인란을 선택하면 Kaspersky Endpoint Security는 크기가 지정된 값을 초과하는 복합 파일을 검사하지 않습니다.

     이 확인란을 선택하지 않으면 Kaspersky Endpoint Security는 크기에 관계 없이 모든 파일을 검사합니다.

     > Kaspersky Endpoint Security는 **큰 복합 파일은 압축 해제 안 함** 확인란의 선택 여부에 관계 없이 압축 해제된 대용량 파일을 검사합니다.

   - **백그라운드에서 복합 파일 압축 해제**.

     이 확인란을 선택하면 Kaspersky Endpoint Security는 파일을 검사하기 전에 지정된 값보다 큰 복합 파일에 대한 접근을 제공합니다. 이 경우 Kaspersky Endpoint Security는 백그라운드에서 복합 파일을 압축 해제하고 검사합니다.

     Kaspersky Endpoint Security는 파일을 압축 해제하고 검사한 후에만 이 값보다 작은 복합 파일에 접근할 수 있습니다.

     이 확인란을 선택하지 않으면 Kaspersky Endpoint Security는 모든 크기의 파일을 압축 해제하고 검사한 후에만 복합 파일에 접근할 수 있습니다.
7. 변경 사항을 저장합니다.

검사 모드 변경

*검사 모드*는 파일 위협 보호 구성 요소에서 파일 검사를 시작하는 조건입니다. Kaspersky Endpoint Security는 기본적으로 스마트 모드로 실행됩니다. 이 파일 검사 모드에서는 사용자, 사용자를 대신한 애플리케이션(로그인에 사용된 계정 또는 다른 사용자 계정 사용) 또는 운영 체제에 의해 파일에서 수행된 작업을 분석한 후에 파일 위협 보호 구성 요소가 파일의 감시 여부를 결정합니다. 예를 들어 Microsoft Office Word 문서 작업의 경우 Kaspersky Endpoint Security는 파일이 처음 열릴 때와 마지막에 닫힐 때 파일을 검사합니다. 그 사이에 파일에 쓰는 작업은 검사되지 않습니다.

파일 검사 모드를 변경하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.

3. **고급 설정**을 클릭합니다.

4. **검사 모드** 블록에서 필요한 방식을 선택합니다.

   - **스마트 모드**. 이 모드에서 파일 위협 보호는 개체에 대해 수행된 처리의 분석 내용에 따라 개체를 검사합니다. 예를 들어 Microsoft Office 문서 작업의 경우 Kaspersky Endpoint Security는 파일이 처음 열릴 때와 마지막에 닫힐 때 파일을 검사합니다. 그 사이에 파일에 쓰는 작업은 검사되지 않습니다.

   - **접근 및 수정 시** 이 모드에서는 개체를 열거나 수정하려는 시도가 있을 때 파일 위협 보호가 개체를 검사합니다.

   - **접근 시**. 이 모드에서는 개체를 열려는 시도가 있을 때만 파일 위협 보호가 개체를 검사합니다.

   - **실행 시**. 이 모드에서는 개체를 실행하려는 시도가 있을 때만 파일 위협 보호가 개체를 검사합니다.

5. 변경 사항을 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 Endpoint Security는 디스크의 파일뿐만 아니라 컨테이너 내부의 파일도 검사합니다. 즉, Kaspersky Endpoint Security는 컨테이너 내의 악성 활동을 탐지하기 위한 외부 도구입니다. 이를 통해 컨테이너의 성능을 유지하고 컨테이너 내의 다른 애플리케이션과의 충돌을 방지할 수 있습니다. 컨테이너 내에 Kaspersky Endpoint Security 설치는 지원하지 않습니다.

Kaspersky Endpoint Security는 컨테이너 보안 외에도 애플리케이션 제어를 사용한 컨테이너 내부 애플리케이션 관리 기능도 제공합니다. 애플리케이션 제어는 컴퓨터에 설치된 애플리케이션에 대해 구성되는 것과 동일한 방식으로 컨테이너에 대해 구성됩니다. 시스템 무결성 모니터링 기능은 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.

위협 탐지 시 처리 방법

컨테이너 내부에서 위협이 탐지되면 애플리케이션은 파일 위협 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 Endpoint Security는 탐지된 개체를 치료할 수 없는 경우 컨테이너를 중지할 수 있습니다. 기본적으로 컨테이너 중지 기능은 비활성화되어 있습니다.

관리 콘솔(MMC)에서 컨테이너 검사 스케줄을 설정하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.
4. **설정**을 클릭합니다.
5. 열린 창에서 **추가** 탭을 선택합니다.
6. **Windows 컨테이너에서 실행되는 파일 동작 검사**에서 컨테이너 검사를 설정합니다:
   - **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.
7. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 컨테이너 검사를 설정하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 파일 위협 보호**로 갑니다.
5. **고급 설정**에서 **성능** 탭을 선택합니다.

6. **검사 최적화** 블록에서 컨테이너 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.

7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 컨테이너 검사를 설정하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **필수 위협 보호 → 파일 위협 보호**를 선택합니다.

3. **Windows 컨테이너에서 실행되는 파일 동작 검사**에서 컨테이너 검사를 설정합니다:

   - **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.

호스트 침입 방지

이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

호스트 침입 방지 구성 요소는 애플리케이션이 운영 체제에 위험할 수 있는 작업을 수행하지 못하게 하고 운영 체제 리소스 및 개인 데이터에 대한 접근을 제어합니다. 이 구성 요소는 안티 바이러스 데이터베이스 및 Kaspersky Security Network 클라우드 서비스를 통해 컴퓨터를 보호합니다.

이 구성 요소는 *애플리케이션 권한*을 사용하여 애플리케이션의 작동을 제어합니다. 애플리케이션 권한에는 다음과 같은 접근 파라미터가 포함됩니다.

- 운영 체제 리소스에 접근(예: 자동 시작 옵션, 레지스트리 키)
- 개인 데이터에 접근(예: 파일 및 애플리케이션)

애플리케이션의 네트워크 활동은 *네트워크 규칙*을 사용하여 방화벽 구성 요소에 의해 제어됩니다.

애플리케이션을 처음 시작하는 동안 호스트 침입 방지 구성 요소는 다음 작업을 수행합니다.

1. 다운로드한 안티 바이러스 데이터베이스를 사용하여 애플리케이션의 보안을 확인합니다.
2. Kaspersky Security Network에서 애플리케이션의 보안을 확인합니다.

   Kaspersky Security Network 참가를 활성화 해 호스트 침입 방지 구성 요소가 보다 효과적으로 작동하도록 도와주십시오.

3. 애플리케이션을 다음 중 하나의 신뢰 그룹에 배치합니다: *신뢰함*, *낮은 제한*, *높은 제한*, *신뢰하지 않음*.

   Kaspersky Endpoint Security가 애플리케이션 동작을 제어할 때 참조하는 권한은 제어 그룹이 정의합니다. Kaspersky Endpoint Security는 애플리케이션이 컴퓨터에 미칠 수 있는 위험 수준에 따라 해당 애플리케이션을 신뢰 그룹에 배치합니다.

   Kaspersky Endpoint Security는 방화벽 및 호스트 침입 방지 구성 요소의 제어 그룹에 애플리케이션을 배치합니다. 방화벽 또는 호스트 침입 방지에 대해서만 제어 그룹을 변경할 수 없습니다.

   KSN 참여를 거부하거나 네트워크가 없는 경우 Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 설정에 따라 애플리케이션을 제어 그룹에 배치합니다. KSN으로부터 애플리케이션의 평판을 받은 후 제어 그룹이 자동으로 변경될 수 있습니다.

4. 제어 그룹에 따라 애플리케이션 작업을 차단합니다. 예를 들어 *높은 제한* 제어 그룹의 애플리케이션은 운영 체제 모듈에 대한 접근이 거부됩니다.

다음 번 애플리케이션을 시작할 때 Kaspersky Endpoint Security가 애플리케이션의 무결성을 확인합니다. 애플리케이션에 변화가 없으면 구성 요소가 애플리케이션에 현재 애플리케이션 권한을 사용합니다. 애플리케이션이 수정되었으면 Kaspersky Endpoint Security가 애플리케이션을 처음으로 시작하는 것처럼 다시 검사합니다.

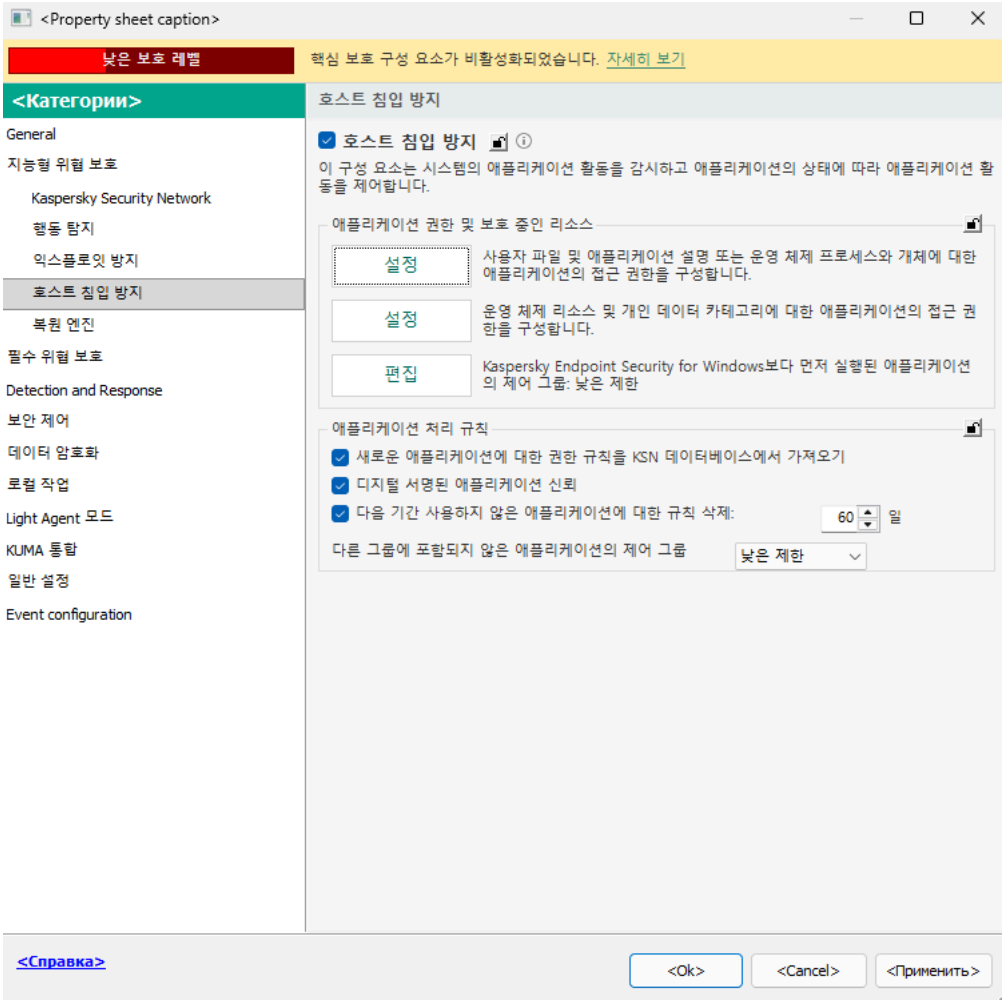
호스트 침입 방지 사용 및 중지

기본적으로 호스트 침입 방지 구성 요소는 작동되며 Kaspersky 전문가가 권장하는 모드에서 실행됩니다.

관리 콘솔(MMC)에서 호스트 침입 방지 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 창에서 **지능형 위협 보호 → 호스트 침입 방지**를 선택합니다.



침입 방지 설정

4. **호스트 침입 방지** 확인란으로 구성 요소를 사용하거나 중지합니다.

5. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 호스트 침입 방지 구성 요소를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **호스트 위협 보호 → 호스트 침입 방지**로 이동합니다.

5. **호스트 침입 방지 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 호스트 침입 방지 구성 요소를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 호스트 침입 방지**을 선택합니다.

3. **호스트 침입 방지** 토글로 구성 요소를 사용하거나 중지합니다.

4. 변경 사항을 저장합니다.

호스트 침입 방지 구성 요소를 활성화하면 Kaspersky Endpoint Security가 애플리케이션이 컴퓨터에 미칠 수 있는 위험 수준에 따라 해당 애플리케이션을 제어 그룹에 배치합니다. 그러면 Kaspersky Endpoint Security는 제어 그룹에 따라 애플리케이션의 동작을 차단합니다.

애플리케이션 제어 그룹 관리

애플리케이션이 처음 시작될 때 호스트 침입 방지 구성 요소는 애플리케이션 보안을 확인하고 애플리케이션을 제어 그룹 중 하나로 이동합니다.

Kaspersky Endpoint Security는 애플리케이션 검사의 첫 단계에서 알려진 애플리케이션의 내부 데이터베이스에서 일치하는 항목을 검사하는 동시에 Kaspersky Security Network 데이터베이스에 요청을 보냅니다(인터넷에 연결된 경우). 내부 데이터베이스 및 Kaspersky Security Network 데이터베이스의 검색 결과를 기준으로 애플리케이션이 제어 그룹에 지정됩니다. 그 후에는 애플리케이션이 시작할 때마다 Kaspersky Endpoint Security는 KSN 데이터베이스에 새로 쿼리를 보내서 KSN 데이터베이스의 애플리케이션 평판이 달라진 경우 애플리케이션을 다른 제어 그룹에 포함시킵니다.

Kaspersky Endpoint Security가 알 수 없는 모든 애플리케이션을 자동으로 배치할 제어 그룹을 선택할 수 있습니다. Kaspersky Endpoint Security가 시작되기 전에 실행 중이던 애플리케이션은 자동으로 호스트 침입 방지 설정에서 지정한 신뢰 그룹에 배치됩니다.

Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션에 대해서는 네트워크 동작만 제어됩니다. 방화벽 설정에서 정의한 네트워크 규칙에 따라 제어를 수행합니다.

애플리케이션의 제어 그룹 변경

애플리케이션이 처음 시작될 때 호스트 침입 방지 구성 요소는 애플리케이션 보안을 확인하고 애플리케이션을 제어 그룹 중 하나로 이동합니다.

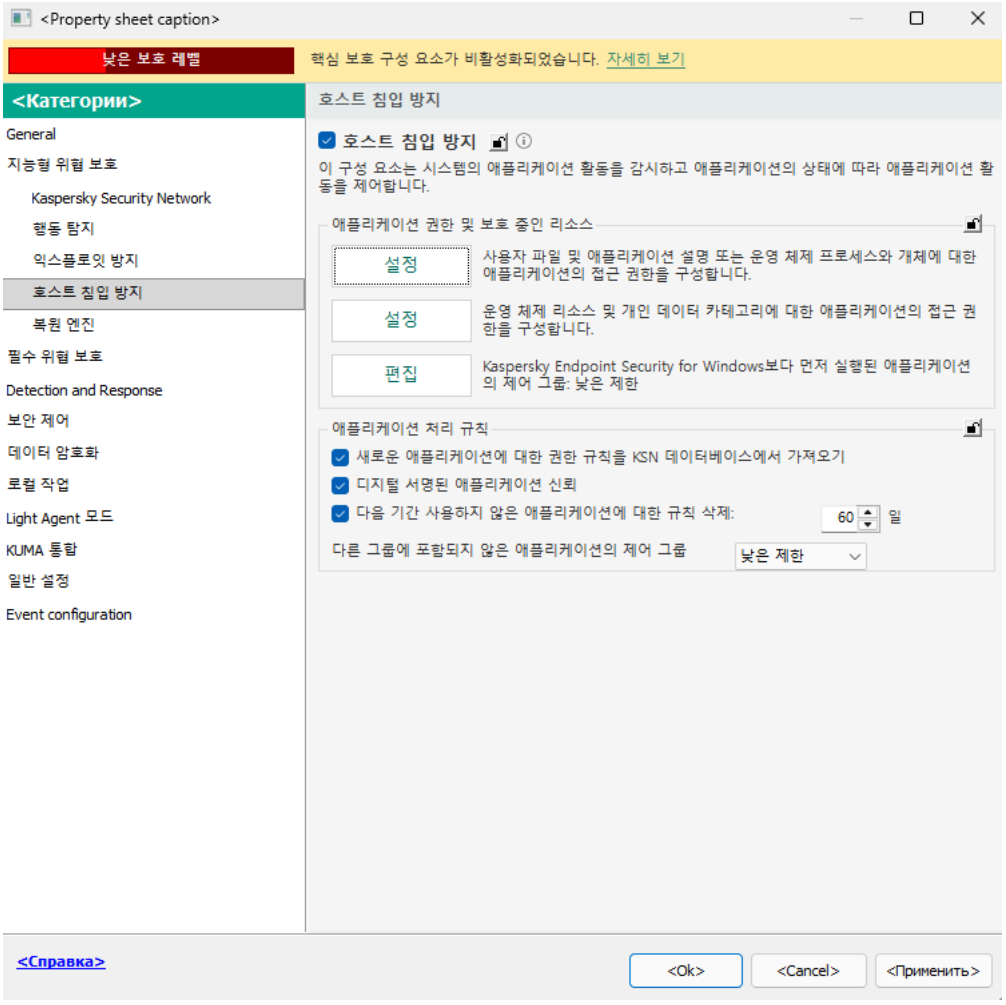
Kaspersky 전문가는 자동으로 할당된 제어 그룹의 애플리케이션을 다른 제어 그룹으로 이동하는 것을 권장하지 않습니다. 대신 필요시 개별 애플리케이션의 권한을 수정할 수 있습니다.

관리 콘솔(MMC)에서 애플리케이션의 제어 그룹을 변경하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **지능형 위협 보호 → 호스트 침입 방지**를 선택합니다.



침입 방지 설정

4. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **설정** 버튼을 클릭합니다.

   그러면 애플리케이션 권한 구성 창과 보호 중인 리소스 목록이 열립니다.

5. **애플리케이션 권한** 탭을 선택합니다.

6. **추가**를 클릭합니다.

7. 창이 열리면 제어 그룹을 변경하려는 애플리케이션에 대한 검색 기준을 입력합니다.

   애플리케이션 이름 또는 공급업체 이름을 입력할 수 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.

8. **새로 고침**을 클릭합니다.

   Kaspersky Endpoint Security는 관리 컴퓨터에 설치된 애플리케이션 통합 목록에서 애플리케이션을 검색합니다. Kaspersky Endpoint Security는 검색 기준을 충족하는 애플리케이션 목록을 표시합니다.

9. 필요한 애플리케이션을 선택합니다.

10. **선택한 애플리케이션을 제어 그룹에 추가** 드롭다운 목록에서 애플리케이션에 필요한 제어 그룹을 선택합니다.

11. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 애플리케이션의 제어 그룹을 변경하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호** → **호스트 침입 방지**로 이동합니다.
5. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **애플리케이션 권한 및 보호 중인 리소스** 링크를 클릭합니다.
   그러면 애플리케이션 권한 구성 창과 보호 중인 리소스 목록이 열립니다.
6. **애플리케이션 권한** 탭을 선택합니다.
   창의 왼쪽에는 제어 그룹 목록이, 오른쪽에는 해당 속성이 표시됩니다.
7. **추가**를 클릭합니다.
   제어 그룹에 애플리케이션을 추가하기 위한 마법사가 시작됩니다.
8. 애플리케이션에 해당하는 제어 그룹을 선택합니다.
9. **애플리케이션** 유형을 선택합니다. 다음 단계로 넘어갑니다.
   여러 애플리케이션에 대한 제어 그룹을 변경하려면 **그룹** 유형을 선택하고 애플리케이션 그룹의 이름을 정의합니다.
10. 애플리케이션 목록이 열리면 제어 그룹을 변경하려는 애플리케이션을 선택합니다.
    필터를 사용합니다. 애플리케이션 이름 또는 공급업체 이름을 입력할 수 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.
11. 마법사를 끝냅니다.
    애플리케이션이 제어 그룹에 추가됩니다.
12. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 애플리케이션의 제어 그룹을 변경하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호** → **호스트 침입 방지**을 선택합니다.
3. **애플리케이션 관리**를 클릭합니다.
   그러면 설치된 애플리케이션의 목록이 열립니다.
4. 필요한 애플리케이션을 선택합니다.
5. 애플리케이션의 마우스 오른쪽 메뉴에서 **제한** → **<제어 그룹>**을 클릭합니다.
6. 변경 사항을 저장합니다.

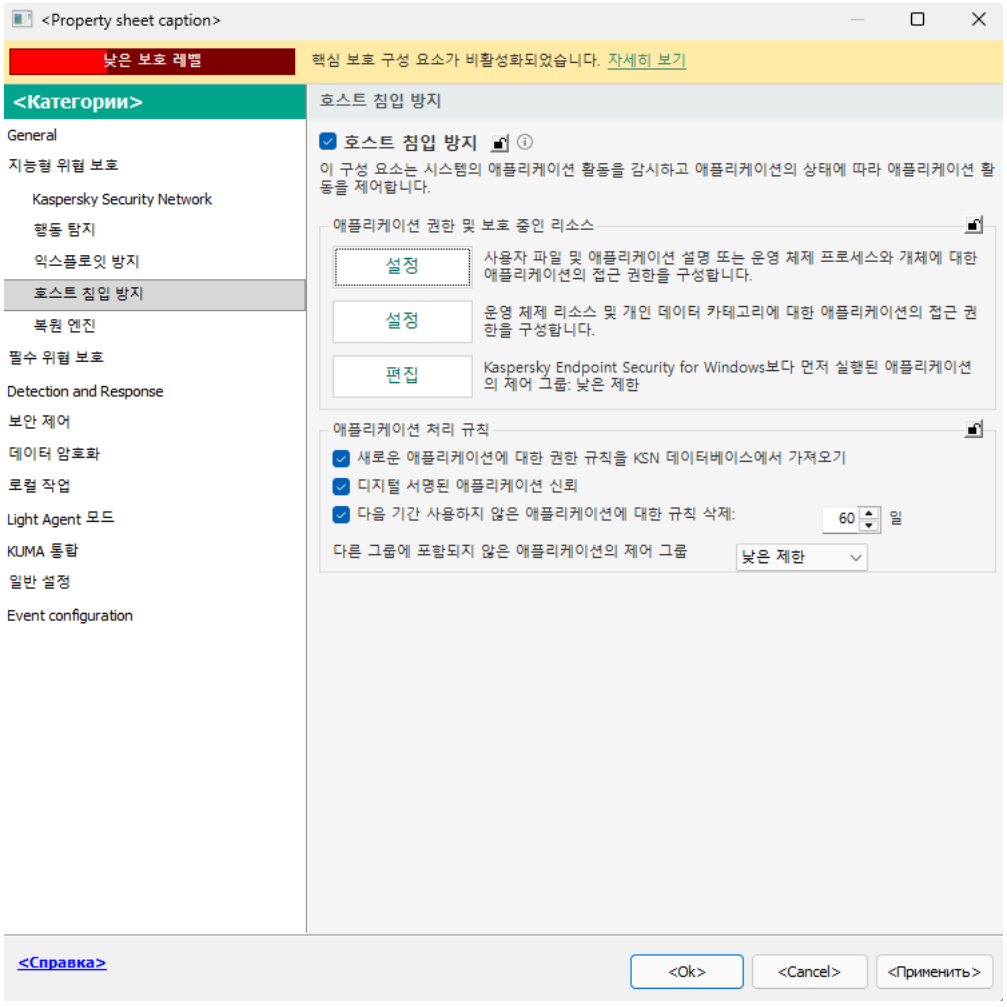
결과적으로 애플리케이션이 다른 제어 그룹에 배치됩니다. 그러면 Kaspersky Endpoint Security는 제어 그룹에 따라 애플리케이션의 동작을 차단합니다. *(사용자가 정의함)* 상태가 애플리케이션에 배정됩니다. Kaspersky Security Network에서 애플리케이션의 평판이 변경되면 호스트 침입 방지 구성 요소가 이 애플리케이션의 제어 그룹을 변경하지 않고 그대로 둡니다.

제어 그룹 권한 구성

기본적으로 다양한 제어 그룹에 대한 최적의 애플리케이션 권한이 생성됩니다. 제어 그룹에 있는 애플리케이션 그룹의 권한 설정은 제어 그룹 권한의 설정에서 값을 상속합니다.

관리 콘솔(MMC)에서 제어 그룹 권한을 변경하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **지능형 위협 보호 → 호스트 침입 방지**를 선택합니다.



침입 방지 설정

4. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **설정** 버튼을 클릭합니다.
   그러면 애플리케이션 권한 구성 창과 보호 중인 리소스 목록이 열립니다.
5. **애플리케이션 권한** 탭으로 이동합니다.
6. 필요한 제어 그룹을 선택합니다.

7. 제어 그룹의 마우스 오른쪽 메뉴에서 **그룹 권한**을 선택합니다.
   제어 그룹 속성이 열립니다.

8. 다음 중 하나를 수행합니다:

   - 운영 체제 레지스트리, 사용자 파일 및 애플리케이션 설정에 대한 작업을 규제하는 제어 그룹 권한을 편집하려면 **파일 및 시스템 레지스트리**를 선택합니다.
   - 운영 체제 프로세스 및 개체에 대한 접근을 규제하는 제어 그룹 권한을 편집하려면 **권한**을 선택합니다.

   애플리케이션의 네트워크 활동은 *네트워크 규칙*을 사용하여 방화벽 구성 요소에 의해 제어됩니다.

9. 관련 리소스가 필요하면 해당 처리 열에서 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 열고 **상속**, **허용**(), 또는 **차단**() 등 필요한 옵션을 선택합니다.

10. 컴퓨터 리소스 사용을 모니터링하려면 **이벤트 기록**(/)을 선택합니다.
    Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 작동에 대한 정보를 기록합니다. 리포트에는 애플리케이션에서 수행하는 컴퓨터 리소스 작업(허용 또는 금지)에 대한 정보가 포함됩니다. 리포트에는 각 리소스를 활용하는 애플리케이션에 대한 정보도 포함됩니다.

11. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 제어 그룹을 변경하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호** → **호스트 침입 방지**로 이동합니다.
5. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **애플리케이션 권한 및 보호 중인 리소스** 링크를 클릭합니다.
   그러면 애플리케이션 권한 구성 창과 보호 중인 리소스 목록이 열립니다.
6. **애플리케이션 권한** 탭으로 이동합니다.
   창의 왼쪽에는 제어 그룹 목록이, 오른쪽에는 해당 속성이 표시됩니다.
7. 창 왼쪽에서 관련 제어 그룹을 선택합니다.
8. 창 오른쪽의 드롭다운 목록에서 다음 중 하나를 수행합니다:

   - 운영 체제 레지스트리, 사용자 파일 및 애플리케이션 설정에 대한 작업을 규제하는 제어 그룹 권한을 편집하려면 **파일 및 시스템 레지스트리**를 선택합니다.
   - 운영 체제 프로세스 및 개체에 대한 접근을 규제하는 제어 그룹 권한을 편집하려면 **권한**을 선택합니다.

   애플리케이션의 네트워크 활동은 *네트워크 규칙*을 사용하여 방화벽 구성 요소에 의해 제어됩니다.

9. 관련 리소스가 필요하면 해당 작업 열에서 **상속**, **허용**(), **차단**() 등 필요한 옵션을 선택합니다.

10. 컴퓨터 리소스 사용을 모니터링하려면 **이벤트 기록**(/)을 선택합니다.

    Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 작동에 대한 정보를 기록합니다. 리포트에는 애플리케이션에서 수행하는 컴퓨터 리소스 작업(허용 또는 금지)에 대한 정보가 포함됩니다. 리포트에는 각 리소스를 활용하는 애플리케이션에 대한 정보도 포함됩니다.

11. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 제어 그룹 권한을 변경하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 호스트 침입 방지**을 선택합니다.
3. **애플리케이션 관리**를 클릭합니다.

   그러면 설치된 애플리케이션의 목록이 열립니다.
4. 필요한 제어 그룹을 선택합니다.
5. 제어 그룹의 마우스 오른쪽 메뉴에서 **상세 정보 및 규칙**을 선택합니다.

   제어 그룹 속성이 열립니다.
6. 다음 중 하나를 수행합니다:

   - 운영 체제 레지스트리, 사용자 파일 및 애플리케이션 설정에 대한 작업을 규제하는 제어 그룹 권한을 편집하려면 **파일 및 시스템 레지스트리**를 선택합니다.
   - 운영 체제 프로세스 및 개체에 대한 접근을 규제하는 제어 그룹 권한을 편집하려면 **권한**을 선택합니다.

   애플리케이션의 네트워크 활동은 *네트워크 규칙*을 사용하여 방화벽 구성 요소에 의해 제어됩니다.
7. 관련 리소스가 필요하면 해당 처리 열에서 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 열고 **상속**, **허용**(), 또는 **거부**() 등 필요한 옵션을 선택합니다.
8. 컴퓨터 리소스 사용을 모니터링하려면 **이벤트 기록**()을 선택합니다.

   Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 작동에 대한 정보를 기록합니다. 리포트에는 애플리케이션에서 수행하는 컴퓨터 리소스 작업(허용 또는 금지)에 대한 정보가 포함됩니다. 리포트에는 각 리소스를 활용하는 애플리케이션에 대한 정보도 포함됩니다.
9. 변경 사항을 저장합니다.

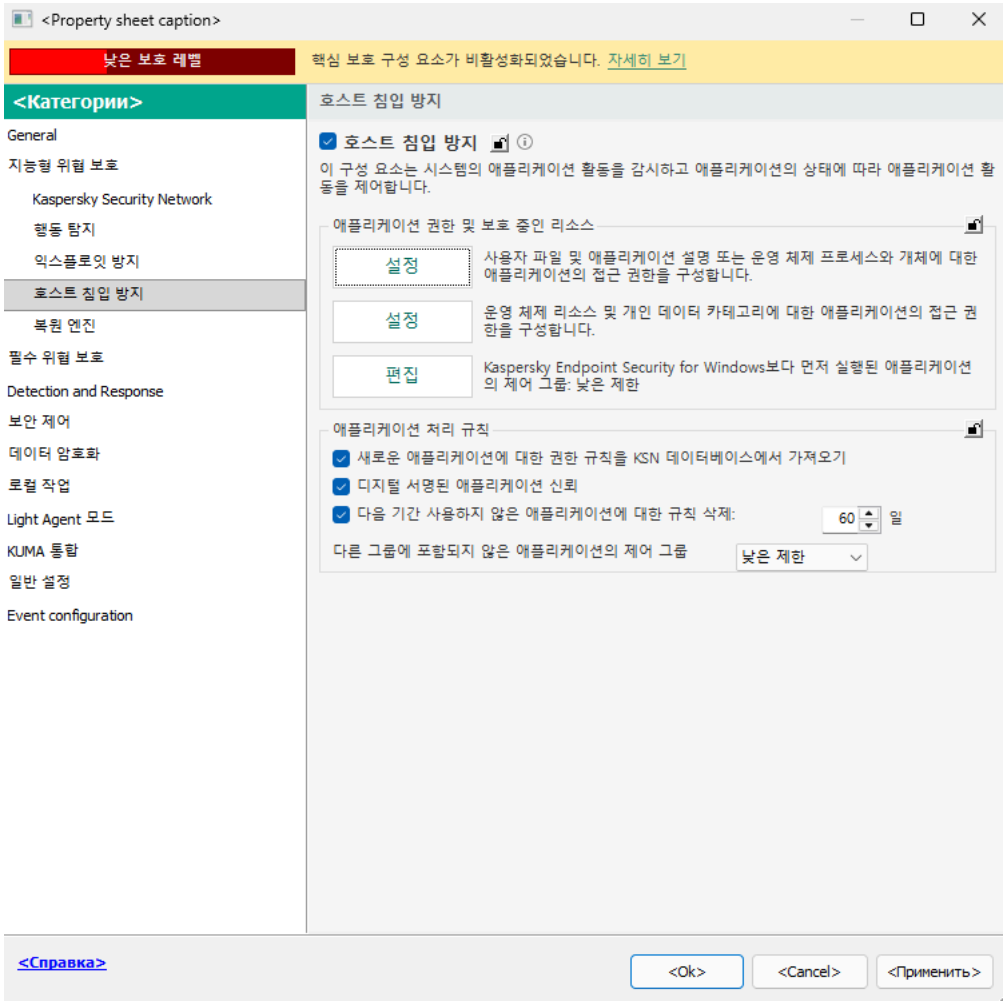
제어 그룹 권한이 변경됩니다. 그러면 Kaspersky Endpoint Security는 제어 그룹에 따라 애플리케이션의 동작을 차단합니다. 상태(*사용자 지정 설정*)가 제어 그룹에 할당됩니다.

Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션에 대한 제어 그룹 선택

Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션에 대해서는 네트워크 동작만 제어됩니다. 방화벽 설정에서 정의한 네트워크 규칙에 따라 제어를 수행합니다. 그러한 애플리케이션을 모니터링하는 네트워크 활동에 적용해야 하는 네트워크 규칙을 지정하려면 제어 그룹을 선택해야 합니다.

관리 콘솔(MMC)에서 Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션에 대한 제어 그룹을 선택하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **지능형 위협 보호 → 호스트 침입 방지**를 선택합니다.



침입 방지 설정

4. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **편집** 버튼을 클릭합니다.
5. **Kaspersky Endpoint Security 보다 먼저 실행된 애플리케이션의 제어 그룹** 설정에 대해 적절한 제어 그룹을 선택합니다.
6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션에 대한 제어 그룹을 선택하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 호스트 침입 방지**로 이동합니다.

5. **Kaspersky Endpoint Security 보다 먼저 실행된 애플리케이션의 제어 그룹** 설정에 대해 적절한 제어 그룹을 선택합니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션에 대한 제어 그룹을 선택하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 호스트 침입 방지**을 선택합니다.

3. **Kaspersky Endpoint Security 보다 먼저 실행된 애플리케이션의 제어 그룹** 블록에서 해당하는 제어 그룹을 선택하십시오.

4. 변경 사항을 저장합니다.

결과적으로 Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션은 다른 제어 그룹에 포함됩니다. 그러면 Kaspersky Endpoint Security는 제어 그룹에 따라 애플리케이션의 동작을 차단합니다.

알 수 없는 애플리케이션에 대한 제어 그룹 선택

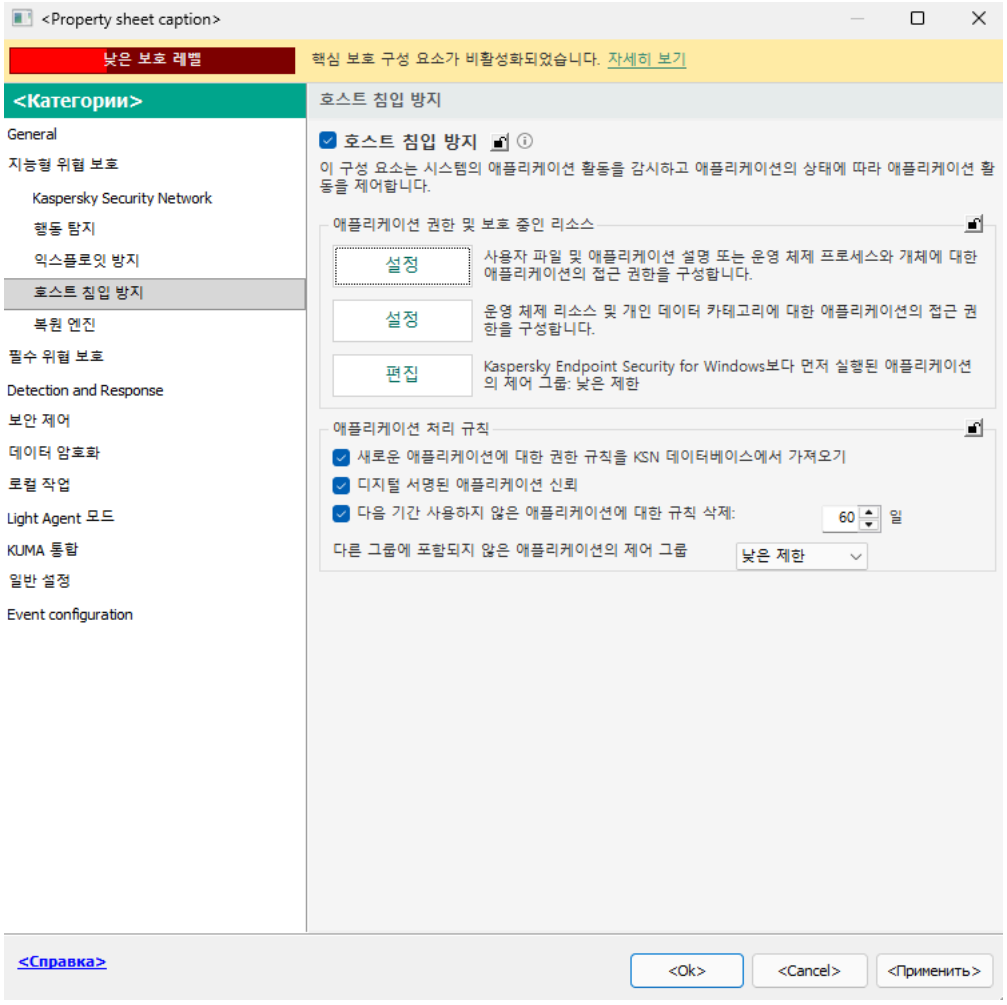
애플리케이션을 처음 시작하는 동안 호스트 침입 방지 구성 요소는 애플리케이션의 제어 그룹을 결정합니다. 인터넷에 접근할 수 없거나 Kaspersky Security Network에 이 애플리케이션에 대한 정보가 없는 경우 Kaspersky Endpoint Security는 기본적으로 애플리케이션을 *낮은 제한* 그룹에 배치합니다. KSN에서 이전에 알려지지 않은 애플리케이션에 대한 정보가 탐지되면 Kaspersky Endpoint Security는 이 애플리케이션의 권한을 업데이트합니다. 그리고 나면 애플리케이션 권한을 직접 편집할 수 있습니다.

관리 콘솔(MMC)에서 알 수 없는 애플리케이션에 대한 제어 그룹을 선택하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **지능형 위협 보호 → 호스트 침입 방지**를 선택합니다.



침입 방지 설정

4. **애플리케이션 처리 규칙** 블록에서 **다른 그룹에 포함되지 않은 애플리케이션의 제어 그룹** 드롭다운 목록을 사용하여 필요한 제어 그룹을 선택합니다.

   Kaspersky Security Network 참여가 활성화된 후 Kaspersky Endpoint Security는 애플리케이션을 시작할 때마다 KSN에 애플리케이션 평판에 대한 쿼리를 전송합니다. 수신한 응답을 근거로 호스트 침입 방지 구성 요소 설정에 지정된 것과 달리 애플리케이션을 제어 그룹으로 이동할 수 있습니다.

5. **새로운 애플리케이션에 대한 권한 규칙을 KSN 데이터베이스에서 가져오기** 확인란을 사용하여 알 수 없는 애플리케이션 권한의 자동 업데이트를 구성합니다.

6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 알 수 없는 애플리케이션에 대한 제어 그룹을 선택하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **호스트 위협 보호 → 호스트 침입 방지**로 이동합니다.

5. **애플리케이션 처리 규칙** 블록에서 **다른 그룹에 포함되지 않은 애플리케이션의 제어 그룹** 드롭다운 목록을 사용하여 필요한 제어 그룹을 선택합니다.

   Kaspersky Security Network 참여가 활성화된 후 Kaspersky Endpoint Security는 애플리케이션을 시작할 때마다 KSN에 애플리케이션 평판에 대한 쿼리를 전송합니다. 수신한 응답을 근거로 호스트 침입 방지 구성 요소 설정에 지정된 것과 달리 애플리케이션을 제어 그룹으로 이동할 수 있습니다.

6. **새로운 애플리케이션에 대한 권한 규칙을 KSN 데이터베이스에서 가져오기** 확인란을 사용하여 알 수 없는 애플리케이션 권한의 자동 업데이트를 구성합니다.

7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 알 수 없는 애플리케이션에 대한 제어 그룹을 선택하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 호스트 침입 방지**을 선택합니다.

3. **애플리케이션 처리 규칙** 블록에서 적절한 제어 그룹을 선택합니다.

   Kaspersky Security Network 참여가 활성화된 후 Kaspersky Endpoint Security는 애플리케이션을 시작할 때마다 KSN에 애플리케이션 평판에 대한 쿼리를 전송합니다. 수신한 응답을 근거로 호스트 침입 방지 구성 요소 설정에 지정된 것과 달리 애플리케이션을 제어 그룹으로 이동할 수 있습니다.

4. **KSN에 등록되지 않은 애플리케이션에 대한 권한 업데이트** 확인란을 사용하여 알 수 없는 애플리케이션의 권한 자동 업데이트를 구성합니다.

5. 변경 사항을 저장합니다.

디지털 서명된 애플리케이션에 대한 제어 그룹 선택

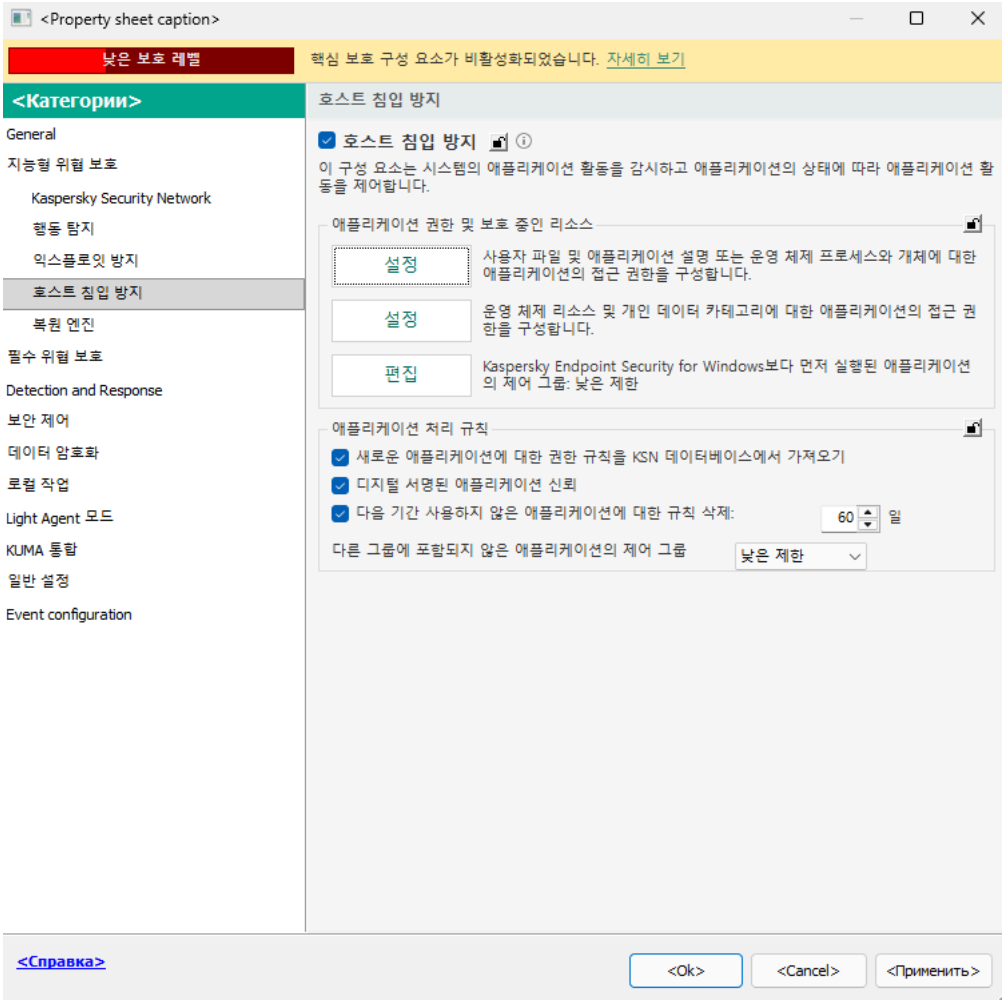
Kaspersky Endpoint Security는 항상 Microsoft 인증서 또는 Kaspersky 인증서가 서명한 애플리케이션을 *신뢰하는* 그룹에 배치합니다.

관리 콘솔(MMC)에서 디지털 서명된 애플리케이션에 대한 제어 그룹을 선택하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **지능형 위협 보호 → 호스트 침입 방지**를 선택합니다.



침입 방지 설정

4. **애플리케이션 처리 규칙** 블록에서 **디지털 서명된 애플리케이션 신뢰** 확인란을 사용하여 신뢰하는 공급업체의 디지털 서명이 포함된 애플리케이션을 Trusted 신뢰 그룹에 자동 배정할 수 있습니다.

   *신뢰하는 공급업체*는 Kaspersky에서 신뢰하는 그룹에 포함된 소프트웨어 공급 업체입니다. 공급 업체 인증서를 신뢰하는 시스템 인증서 저장소에 직접 추가할 수도 있습니다.

   이 확인란을 선택 해제하면 호스트 침입 방지 구성 요소가 디지털로 서명한 애플리케이션을 신뢰하지 않으며 다른 파라미터를 사용하여 제어 그룹을 결정합니다.

5. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 디지털 서명된 애플리케이션에 대한 제어 그룹을 선택하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **호스트 위협 보호 → 호스트 침입 방지**로 이동합니다.

5. **애플리케이션 처리 규칙** 블록에서 **디지털 서명된 애플리케이션 신뢰** 확인란을 사용하여 신뢰하는 공급업체의 디지털 서명이 포함된 애플리케이션을 Trusted 신뢰 그룹에 자동 배정할 수 있습니다.

   *신뢰하는 공급업체*는 Kaspersky에서 신뢰하는 그룹에 포함된 소프트웨어 공급 업체입니다. 공급 업체 인증서를 신뢰하는 시스템 인증서 저장소에 직접 추가할 수도 있습니다.

이 확인란을 선택 해제하면 호스트 침입 방지 구성 요소가 디지털로 서명한 애플리케이션을 신뢰하지 않으며 다른 파라미터를 사용하여 제어 그룹을 결정합니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 디지털 서명된 애플리케이션에 대한 제어 그룹을 선택하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 호스트 침입 방지**을 선택합니다.
3. **애플리케이션 처리 규칙** 블록에서 **디지털 서명된 애플리케이션 신뢰** 확인란을 사용하여 신뢰하는 공급업체의 디지털 서명이 포함된 애플리케이션을 Trusted 신뢰 그룹에 자동 배정할 수 있습니다.

   *신뢰하는 공급업체*는 Kaspersky에서 신뢰하는 그룹에 포함된 소프트웨어 공급 업체입니다. 공급 업체 인증서를 신뢰하는 시스템 인증서 저장소에 직접 추가할 수도 있습니다.

   이 확인란을 선택 해제하면 호스트 침입 방지 구성 요소가 디지털로 서명한 애플리케이션을 신뢰하지 않으며 다른 파라미터를 사용하여 제어 그룹을 결정합니다.

4. 변경 사항을 저장합니다.

애플리케이션 권한 관리

기본적으로 애플리케이션 활동은 Kaspersky Endpoint Security가 처음 시작할 때 애플리케이션에 배정한 특정 제어 그룹에 대해 정의한 애플리케이션 권한을 기반으로 제어됩니다. 필요시 전체 제어 그룹에 대한 애플리케이션 권한을 편집하거나, 개별 애플리케이션 또는 제어 그룹에 속한 애플리케이션 그룹에 대해 애플리케이션 권한을 편집할 수 있습니다.

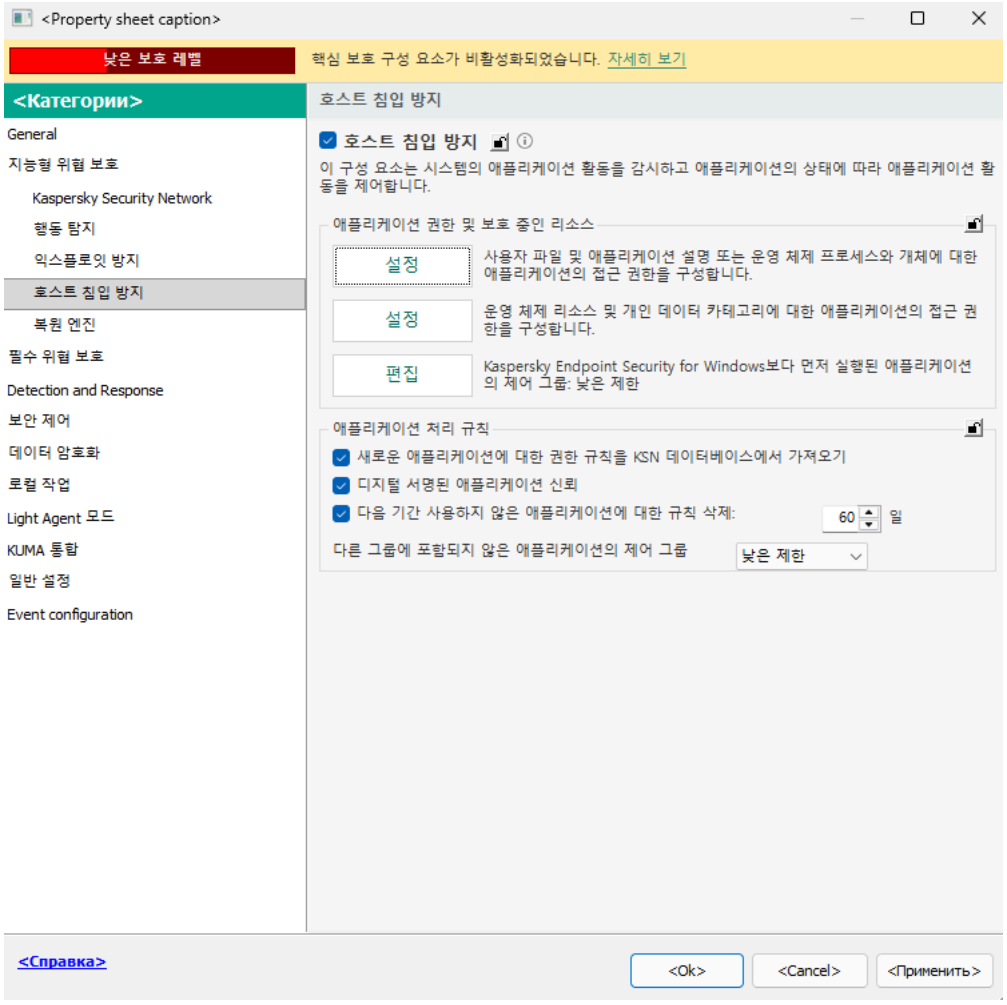
직접 정의한 애플리케이션 권한은 제어 그룹에 대해 정의한 애플리케이션 권한보다 우선순위가 높습니다. 즉, 직접 정의한 애플리케이션 권한이 제어 그룹에 대해 정의한 애플리케이션 권한과 다른 경우 호스트 침입 방지 구성 요소는 직접 정의한 애플리케이션 권한에 따라 애플리케이션 활동을 제어합니다.

애플리케이션에 대해 생성하는 규칙은 자식 애플리케이션에 상속됩니다. 예를 들어, cmd.exe에 대한 모든 네트워크 활동을 거부하면 cmd.exe를 사용하여 시작한 notepad.exe에 대해서도 모든 네트워크 활동이 거부됩니다. 애플리케이션이 실행의 기반이 되는 애플리케이션의 자식 애플리케이션이 아니라면 규칙이 상속되지 않습니다.

관리 콘솔(MMC)에서 애플리케이션 권한을 변경하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **지능형 위협 보호 → 호스트 침입 방지**를 선택합니다.



침입 방지 설정

4. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **설정** 버튼을 클릭합니다.
   그러면 애플리케이션 권한 구성 창과 보호 중인 리소스 목록이 열립니다.

5. **애플리케이션 권한** 탭으로 이동합니다.

6. **추가**를 클릭합니다.

7. 창이 열리면 애플리케이션 권한을 변경할 애플리케이션의 검색 기준을 입력합니다.
   애플리케이션 이름 또는 공급업체 이름을 입력할 수 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.

8. **새로 고침**을 클릭합니다.
   Kaspersky Endpoint Security는 관리 컴퓨터에 설치된 애플리케이션 통합 목록에서 애플리케이션을 검색합니다. Kaspersky Endpoint Security는 검색 기준을 충족하는 애플리케이션 목록을 표시합니다.

9. 필요한 애플리케이션을 선택합니다.

10. **선택한 애플리케이션을 제어 그룹에 추가** 드롭다운 목록에서 **초기 상태 그룹**을 선택하고 **확인**을 클릭합니다.
    애플리케이션이 기본 그룹에 추가됩니다.

11. 관련 애플리케이션을 선택한 다음 애플리케이션의 마우스 오른쪽 메뉴에서 **애플리케이션 권한**을 선택합니다.
    애플리케이션 속성이 열립니다.

12. 다음 중 하나를 수행합니다:

    - 운영 체제 레지스트리, 사용자 파일 및 애플리케이션 설정에 대한 작업을 규제하는 제어 그룹 권한을 편집하려면 **파일 및 시스템 레지스트리**를 선택합니다.
    - 운영 체제 프로세스 및 개체에 대한 접근을 규제하는 제어 그룹 권한을 편집하려면 **권한**을 선택합니다.

    애플리케이션의 네트워크 활동은 *네트워크 규칙*을 사용하여 방화벽 구성 요소에 의해 제어됩니다.

13. 관련 리소스가 필요하면 해당 처리 열에서 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 열고 **상속**, **허용**( ), 또는 **차단**( ) 등 필요한 옵션을 선택합니다.

14. 컴퓨터 리소스 사용을 모니터링하려면 **이벤트 기록**(/)을 선택합니다.

    Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 작동에 대한 정보를 기록합니다. 리포트에는 애플리케이션에서 수행하는 컴퓨터 리소스 작업(허용 또는 금지)에 대한 정보가 포함됩니다. 리포트에는 각 리소스를 활용하는 애플리케이션에 대한 정보도 포함됩니다.

15. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 애플리케이션 권한을 변경하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호** → **호스트 침입 방지**로 이동합니다.
5. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **애플리케이션 권한 및 보호 중인 리소스** 링크를 클릭합니다.

   그러면 애플리케이션 권한 구성 창과 보호 중인 리소스 목록이 열립니다.
6. **애플리케이션 권한** 탭으로 이동합니다.

   창의 왼쪽에는 제어 그룹 목록이, 오른쪽에는 해당 속성이 표시됩니다.
7. **추가**를 클릭합니다.

   제어 그룹에 애플리케이션을 추가하기 위한 마법사가 시작됩니다.
8. 애플리케이션에 해당하는 제어 그룹을 선택합니다.
9. **애플리케이션** 유형을 선택합니다. 다음 단계로 넘어갑니다.

   여러 애플리케이션에 대한 제어 그룹을 변경하려면 **그룹** 유형을 선택하고 애플리케이션 그룹의 이름을 정의합니다.
10. 애플리케이션 목록이 열리면 애플리케이션 권한을 변경하려는 애플리케이션을 선택합니다.

    필터를 사용합니다. 애플리케이션 이름 또는 공급업체 이름을 입력할 수 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.
11. 마법사를 끝냅니다.

    애플리케이션이 제어 그룹에 추가됩니다.

12. 창 왼쪽에서 관련 애플리케이션을 선택합니다.

13. 창 오른쪽의 드롭다운 목록에서 다음 중 하나를 수행합니다:

    - 운영 체제 레지스트리, 사용자 파일 및 애플리케이션 설정에 대한 작업을 규제하는 제어 그룹 권한을 편집하려면 **파일 및 시스템 레지스트리**를 선택합니다.
    - 운영 체제 프로세스 및 개체에 대한 접근을 규제하는 제어 그룹 권한을 편집하려면 **권한**을 선택합니다.

    애플리케이션의 네트워크 활동은 *네트워크 규칙*을 사용하여 방화벽 구성 요소에 의해 제어됩니다.

14. 관련 리소스가 필요하면 해당 작업 열에서 **상속**, **허용**(), **차단**() 등 필요한 옵션을 선택합니다.

15. 컴퓨터 리소스 사용을 모니터링하려면 **이벤트 기록**(/)을 선택합니다.

    Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 작동에 대한 정보를 기록합니다. 리포트에는 애플리케이션에서 수행하는 컴퓨터 리소스 작업(허용 또는 금지)에 대한 정보가 포함됩니다. 리포트에는 각 리소스를 활용하는 애플리케이션에 대한 정보도 포함됩니다.

16. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 애플리케이션 권한을 변경하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 호스트 침입 방지**을 선택합니다.
3. **애플리케이션 관리**를 클릭합니다.

   그러면 설치된 애플리케이션의 목록이 열립니다.
4. 필요한 애플리케이션을 선택합니다.
5. 애플리케이션의 마우스 오른쪽 메뉴에서 **상세 정보 및 규칙**을 선택합니다.

   애플리케이션 속성이 열립니다.
6. 다음 중 하나를 수행합니다:

    - 운영 체제 레지스트리, 사용자 파일 및 애플리케이션 설정에 대한 작업을 규제하는 제어 그룹 권한을 편집하려면 **파일 및 시스템 레지스트리**를 선택합니다.
    - 운영 체제 프로세스 및 개체에 대한 접근을 규제하는 제어 그룹 권한을 편집하려면 **권한**을 선택합니다.

7. 관련 리소스가 필요하면 해당 처리 열에서 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 열고 **상속**, **허용**(), 또는 **거부**() 등 필요한 옵션을 선택합니다.
8. 컴퓨터 리소스 사용을 모니터링하려면 **이벤트 기록**()을 선택합니다.

   Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 작동에 대한 정보를 기록합니다. 리포트에는 애플리케이션에서 수행하는 컴퓨터 리소스 작업(허용 또는 금지)에 대한 정보가 포함됩니다. 리포트에는 각 리소스를 활용하는 애플리케이션에 대한 정보도 포함됩니다.
9. **예외 규칙** 탭을 선택하고 애플리케이션의 고급 설정을 구성합니다(아래 표 참조).
10. 변경 사항을 저장합니다.

파라미터	설명
애플리케이션에서 연 파일 검사 안 함	Kaspersky Endpoint Security의 검사에서 제외한 애플리케이션이 여는 모든 파일. 예를 들어, 애플리케이션을 사용하여 파일을 백업할 때 이 기능이 Kaspersky Endpoint Security의 리소스 소모를 줄이는 데 도움이 됩니다.
애플리케이션 활동 감시 안 함	Kaspersky Endpoint Security는 운영 체제에서 애플리케이션의 파일 및 네트워크 활동을 감시하지 않습니다. Kaspersky Endpoint Security의 여러 구성 요소에 대한 애플리케이션 활동 모니터를 구성할 수 있습니다. • **보호 및 제어 구성 요소 감시 안 함**. 애플리케이션 활동은 행동 탐지, 익스플로잇 방지, 호스트 침입 방지, 복원 엔진 및 방화벽 구성 요소가 감시합니다. • **Managed Detection and Response와 Endpoint Detection and Response 감시 안 함**. 애플리케이션 활동은 내장형 MDR 에이전트 및 내장형 EDR(KATA) 에이전트로 모니터링됩니다. • **Endpoint Detection and Response에 대한 콘솔 대화형 입력 가로채지 않음**. Kaspersky Endpoint Security는 콘솔에서 애플리케이션 관리에 대한 원격 측정 데이터를 전송하지 않습니다. 원격 측정 데이터는 Kaspersky Anti Targeted Attack Platform(EDR)에서 사용됩니다.
부모 프로세스(애플리케이션)의 제한을 상속하지 않음	Kaspersky Endpoint Security는 부모 프로세스에 대해 구성된 제한을 자식 프로세스에 적용하지 않습니다. 부모 프로세스는 애플리케이션 권한(호스트 침입 방지) 및 애플리케이션 네트워크 규칙(방화벽)이 구성된 애플리케이션에 의해 시작됩니다.
자녀 애플리케이션의 활동 감시 안 함	Kaspersky Endpoint Security는 이 애플리케이션이 시작한 애플리케이션의 파일 활동 또는 네트워크 활동을 모니터링하지 않습니다. 예외를 반복 적용할 수 있습니다. 따라서 애플리케이션은 전체 자식 애플리케이션 체인 활동을 모니터링하지 않습니다.
Kaspersky Endpoint Security for Windows 인터페이스와의 상호작용 허용	Kaspersky Endpoint Security의 자기 보호는 원격 컴퓨터에서 애플리케이션 서비스를 관리하려는 모든 시도를 차단합니다. 이 확인란을 선택하면 원격 접속 애플리케이션이 Kaspersky Endpoint Security 인터페이스를 통해 Kaspersky Endpoint Security 설정을 관리할 수 있습니다.
암호화된 트래픽 검사 안 함/모든 트래픽 검사 안 함	애플리케이션이 시작한 네트워크 트래픽은 Kaspersky Endpoint Security의 검사에서 제외됩니다. 모든 트래픽을 검사에서 제외하거나 암호화된 트래픽만 제외할 수 있습니다. 스캔에서 개별 IP 주소 및 포트 번호를 제외할 수도 있습니다. 해시가 경로가 아닌 신뢰하는 애플리케이션에 대해 지정된 경우 애플리케이션은 네트워크 트래픽 예외를 지원하지 않습니다.

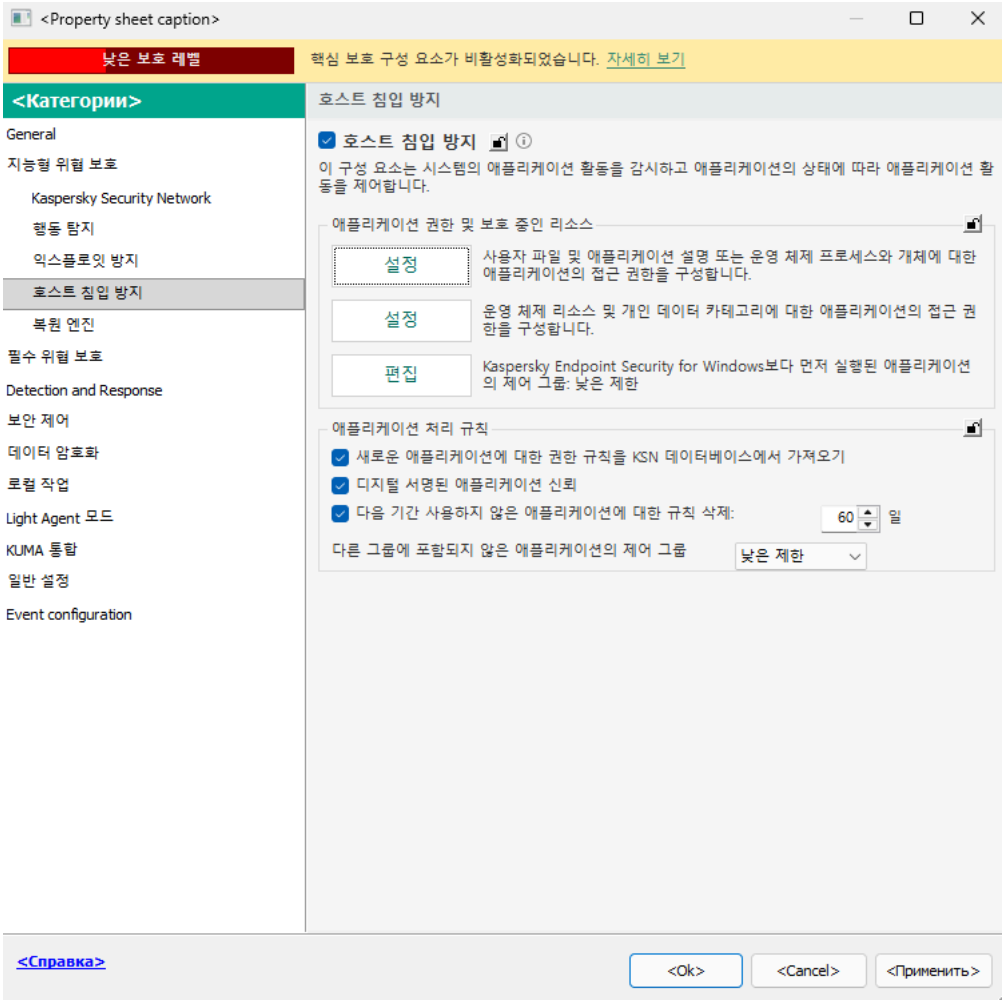
운영 체제 리소스 및 개인 데이터 보호

호스트 침입 방지 구성 요소는 운영 체제 리소스 및 개인 데이터에 대한 다양한 카테고리에 대한 작업을 처리하는 애플리케이션 권한을 관리합니다. Kaspersky 전문가가 지정한 보호되는 리소스 카테고리가 사전 설정되어 있습니다. 예를 들어, *운영 체제* 카테고리에는 애플리케이션 자동 실행과 관련된 모든 레지스트리 키를 나열하는 *시작 설정* 하위 카테고리가 있습니다. 사전 설정된 보호되는 리소스 카테고리 및 이 카테고리에 속하는 보호되는 리소스는 편집하거나 삭제할 수 없습니다.

관리 콘솔(MMC)에서 보호 중인 리소스를 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **지능형 위협 보호 → 호스트 침입 방지**를 선택합니다.



침입 방지 설정

4. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **설정** 버튼을 클릭합니다.

   그러면 애플리케이션 권한 구성 창과 보호 중인 리소스 목록이 열립니다.

5. **보호 중인 리소스** 탭을 선택합니다.

   창 왼쪽에 보호 중인 리소스 목록과 특정 제어 그룹에 따라 해당 리소스에 접근할 수 있는 해당 권한이 표시됩니다.

6. 새 보호 리소스를 추가할 보호되는 리소스 카테고리를 선택합니다.

   하위 카테고리를 추가하려면 **추가 → 카테고리**를 클릭합니다.

7. **추가** 버튼을 누릅니다. 드롭다운 목록에서 **파일 또는 폴더** 또는 **레지스트리 키** 등 추가할 리소스 유형을 선택합니다.

8. 창이 열리면 파일, 폴더 또는 레지스트리 키를 선택합니다.

   추가된 리소스에 접근할 수 있는 애플리케이션의 권한을 볼 수 있습니다. 이를 위해 창 왼쪽에서 추가된 리소스를 선택하면 Kaspersky Endpoint Security가 각 제어 그룹에 대한 접근 권한을 표시합니다. 새 리소스 옆의 확인란을 사용하여 리소스에 대한 애플리케이션 활동 제어를 비활성화할 수도 있습니다.

9. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 보호 중인 리소스를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호** → **호스트 침입 방지**로 이동합니다.
5. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **애플리케이션 권한 및 보호 중인 리소스** 링크를 클릭합니다.
   그러면 애플리케이션 권한 구성 창과 보호 중인 리소스 목록이 열립니다.
6. **보호 중인 리소스** 탭을 선택합니다.
   창 왼쪽에 보호 중인 리소스 목록과 특정 제어 그룹에 따라 해당 리소스에 접근할 수 있는 해당 권한이 표시됩니다.
7. **추가**를 클릭합니다.
   새 리소스 마법사가 시작됩니다.
8. **그룹 이름** 블록에서 새 보호되는 리소스를 추가할 보호되는 리소스 카테고리를 선택합니다.
   하위 카테고리를 추가하려면 **보호되는 리소스 카테고리** 옵션을 선택합니다.
9. **파일 또는 폴더** 또는 **레지스트리 키** 등 추가할 리소스 유형을 선택합니다.
10. 파일, 폴더 또는 레지스트리 키를 선택합니다.
11. 마법사를 끝냅니다.
    추가된 리소스에 접근할 수 있는 애플리케이션의 권한을 볼 수 있습니다. 이를 위해 창 왼쪽에서 추가된 리소스를 선택하면 Kaspersky Endpoint Security가 각 제어 그룹에 대한 접근 권한을 표시합니다. 또한 **상태** 열의 확인란을 사용하여 리소스에 대한 애플리케이션 활동 제어를 비활성화할 수 있습니다.
12. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 보호 중인 리소스를 추가하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호** → **호스트 침입 방지**을 선택합니다.
3. **리소스 관리**를 클릭합니다.
   보호되는 리소스 목록이 열립니다.
4. 새 보호 리소스를 추가할 보호되는 리소스 카테고리를 선택합니다.
   하위 카테고리를 추가하려면 **추가** → **카테고리**를 클릭합니다.
5. **추가** 버튼을 누릅니다. 드롭다운 목록에서 **파일 또는 폴더** 또는 **레지스트리 키** 등 추가할 리소스 유형을 선택합니다.

6. 창이 열리면 파일, 폴더 또는 레지스트리 키를 선택합니다.

   추가된 리소스에 접근할 수 있는 애플리케이션의 권한을 볼 수 있습니다. 이를 위해 창 왼쪽에서 추가된 리소스를 선택하면 Kaspersky Endpoint Security에 애플리케이션 목록과 각 애플리케이션에 대한 접근 권한이 표시됩니다. **상태** 열에서 **제어 사용** 버튼을 사용하여 리소스를 사용하는 애플리케이션 활동에 대한 제어를 중지할 수 있습니다.

7. 변경 사항을 저장합니다.

Kaspersky Endpoint Security는 추가된 운영 체제 리소스 및 개인 데이터에 대한 접근을 제어합니다. Kaspersky Endpoint Security는 애플리케이션에 할당한 제어 그룹을 기반으로 리소스에 대한 애플리케이션의 접근을 제어합니다. 애플리케이션의 제어 그룹을 변경할 수도 있습니다.

사용하지 않는 애플리케이션에 대한 정보 삭제

Kaspersky Endpoint Security는 애플리케이션 권한을 사용하여 애플리케이션 활동을 제어합니다. 애플리케이션 권한은 해당 제어 그룹에 의해 결정됩니다. Kaspersky Endpoint Security는 애플리케이션 최초 시작 애플리케이션을 제어 그룹에 넣습니다. 애플리케이션의 제어 그룹을 직접 변경할 수 있습니다. 개별 애플리케이션의 권한을 직접 구성할 수도 있습니다. Kaspersky Endpoint Security는 애플리케이션에 대한 다음 정보를 저장합니다: 애플리케이션의 제어 그룹 및 애플리케이션의 권한.

Kaspersky Endpoint Security는 컴퓨터 리소스를 절약하기 위해 사용하지 않는 애플리케이션에 대한 정보를 자동으로 삭제합니다. Kaspersky Endpoint Security는 다음 규칙에 따라 애플리케이션 정보를 삭제합니다.

- 애플리케이션의 제어 그룹과 권한이 자동으로 결정되면 Kaspersky Endpoint Security는 30일 후 이 애플리케이션에 대한 정보를 삭제합니다. 애플리케이션 정보의 저장 기간을 변경하거나 자동 삭제를 해제할 수 없습니다.

- 직접 애플리케이션을 제어 그룹에 넣거나 애플리케이션의 접근 권한을 구성하면 Kaspersky Endpoint Security는 60일 후에 이 애플리케이션에 대한 정보를 삭제합니다(기본 저장 기간). 애플리케이션 정보의 저장 기간을 변경하거나 자동 삭제를 해제할 수 있습니다(아래 지침 참조).

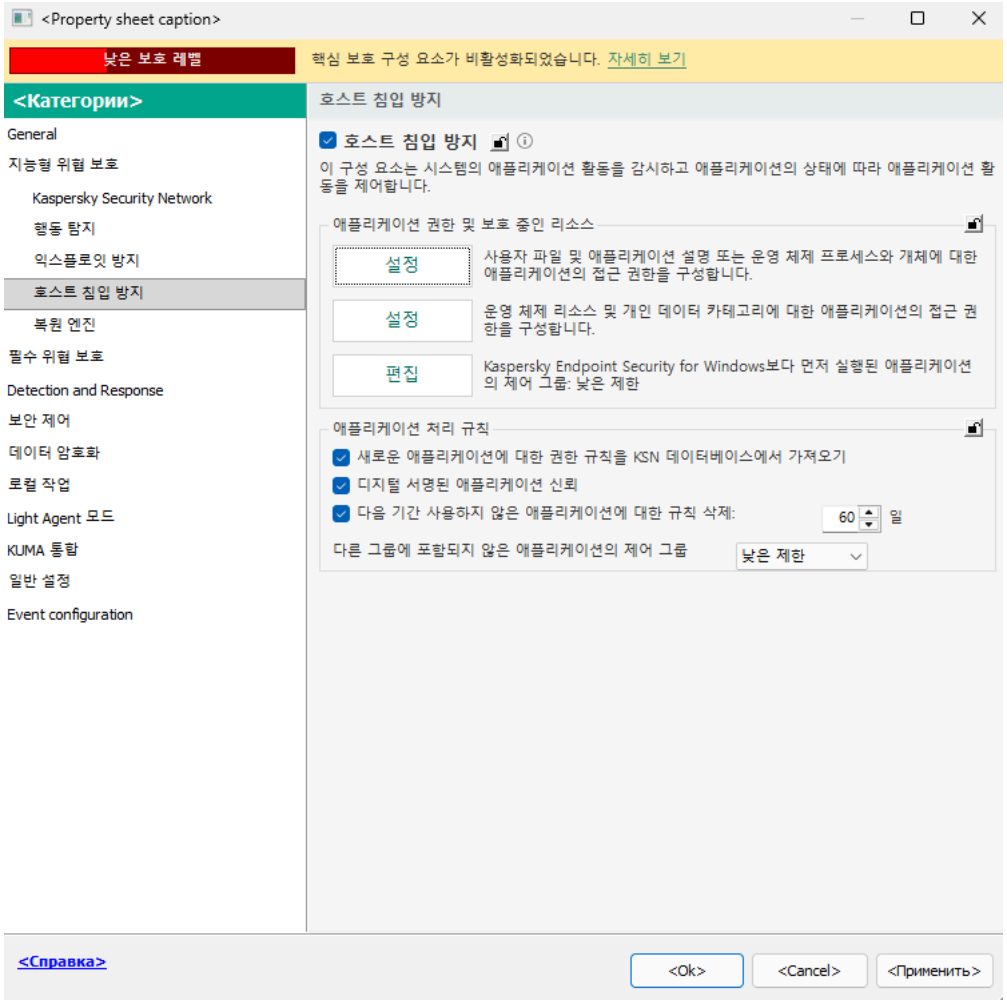
정보가 삭제된 애플리케이션을 시작하면 Kaspersky Endpoint Security는 애플리케이션을 처음으로 시작하는 것처럼 다시 검사합니다.

관리 콘솔(MMC)에서 사용하지 않는 애플리케이션에 대한 정보 자동 삭제 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **지능형 위협 보호 → 호스트 침입 방지**를 선택합니다.



침입 방지 설정

4. **애플리케이션 처리 규칙** 블록에서 다음 중 하나를 수행합니다:

   - 자동 삭제를 구성하려면 **다음 기간 동안 사용하지 않은 애플리케이션에 대한 규칙 삭제: N일** 확인란을 선택하고 필요한 기간을 지정합니다.

     제어 그룹에 직접 넣거나 직접 구성한 접근 권한을 가진 애플리케이션에 대한 정보는 지정된 날짜가 지난 후 Kaspersky Endpoint Security에 의해 삭제됩니다. 제어 그룹과 애플리케이션 권한이 자동으로 결정된 애플리케이션에 대한 정보도 30일 후에 Kaspersky Endpoint Security에서 삭제됩니다.

   - 자동 삭제를 끄려면 **다음 기간 동안 사용하지 않은 애플리케이션에 대한 규칙 삭제: N일** 확인란의 선택을 취소합니다.

     제어 그룹에 직접 넣거나 직접 구성한 접근 권한을 가진 애플리케이션에 대한 정보는 저장 기간 제한없이 Kaspersky Endpoint Security에 의해 무기한 저장됩니다. Kaspersky Endpoint Security는 30일 후 제어 그룹과 애플리케이션 권한이 자동으로 결정된 애플리케이션에 대한 정보만 삭제합니다.

5. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 사용하지 않는 애플리케이션에 대한 정보 자동 삭제 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **호스트 위협 보호 → 호스트 침입 방지**로 이동합니다.

5. **애플리케이션 처리 규칙** 블록에서 다음 중 하나를 수행합니다:

   - 자동 삭제를 구성하려면 **다음 기간 이상 시작하지 않은 애플리케이션에 대한 규칙 삭제(일, 1~90)** 확인란을 선택하고 필요한 기간을 지정합니다.

     제어 그룹에 직접 넣거나 직접 구성한 접근 권한을 가진 애플리케이션에 대한 정보는 지정된 날짜가 지난 후 Kaspersky Endpoint Security에 의해 삭제됩니다. 제어 그룹과 애플리케이션 권한이 자동으로 결정된 애플리케이션에 대한 정보도 30일 후에 Kaspersky Endpoint Security에서 삭제됩니다.

   - 자동 삭제를 끄려면 **다음 기간 이상 시작하지 않은 애플리케이션에 대한 규칙 삭제(일, 1~90)** 확인란의 선택을 취소합니다.

     제어 그룹에 직접 넣거나 직접 구성한 접근 권한을 가진 애플리케이션에 대한 정보는 저장 기간 제한없이 Kaspersky Endpoint Security에 의해 무기한 저장됩니다. Kaspersky Endpoint Security는 30일 후 제어 그룹과 애플리케이션 권한이 자동으로 결정된 애플리케이션에 대한 정보만 삭제합니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 사용하지 않는 애플리케이션에 대한 정보 자동 삭제 구성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 호스트 침입 방지**을 선택합니다.

3. **애플리케이션 처리 규칙** 블록에서 다음 중 하나를 수행합니다:

   - 자동 삭제를 구성하려면 **다음 기간 사용하지 않은 애플리케이션에 대한 규칙 삭제 N일(1~90)** 확인란을 선택하고 필요한 기간을 지정합니다.

     제어 그룹에 직접 넣거나 직접 구성한 접근 권한을 가진 애플리케이션에 대한 정보는 지정된 날짜가 지난 후 Kaspersky Endpoint Security에 의해 삭제됩니다. 제어 그룹과 애플리케이션 권한이 자동으로 결정된 애플리케이션에 대한 정보도 30일 후에 Kaspersky Endpoint Security에서 삭제됩니다.

   - 자동 삭제를 끄려면 **다음 기간 사용하지 않은 애플리케이션에 대한 규칙 삭제 N일(1~90)** 확인란의 선택을 취소합니다.

     제어 그룹에 직접 넣거나 직접 구성한 접근 권한을 가진 애플리케이션에 대한 정보는 저장 기간 제한없이 Kaspersky Endpoint Security에 의해 무기한 저장됩니다. Kaspersky Endpoint Security는 30일 후 제어 그룹과 애플리케이션 권한이 자동으로 결정된 애플리케이션에 대한 정보만 삭제합니다.

4. 변경 사항을 저장합니다.

호스트 침입 방지 모니터링

호스트 침입 방지 구성 요소의 작동에 대한 리포트를 받을 수 있습니다. 리포트에는 애플리케이션에서 수행하는 컴퓨터 리소스 작업(허용 또는 금지)에 대한 정보가 포함됩니다. 리포트에는 각 리소스를 활용하는 애플리케이션에 대한 정보도 포함됩니다.

호스트 침입 방지 작업을 모니터링하려면 리포트 쓰기를 활성화해야 합니다. 예를 들어, 호스트 침입 방지 구성 요소 설정에서 개별 애플리케이션에 대한 리포트 전달을 활성화할 수 있습니다.

호스트 침입 방지 모니터링을 구성할 때는, Kaspersky Security Center로 이벤트 전달 시 발생할 수 있는 네트워크 로드를 고려하십시오. Kaspersky Endpoint Security의 로컬 로그에서만 리포트 저장을 활성화할 수도 있습니다.

오디오 및 비디오에 대한 접근 보호

오디오 신호 보호 기능 및 웹캠 접근 보호 기능은 Arm 기반 컴퓨터에서 지원하지 않습니다.

사이버 범죄자는 특수 프로그램을 사용하여 오디오 및 비디오 기록 장치(마이크나 웹캠 등)에 접근하려고 할 수 있습니다. Kaspersky Endpoint Security는 애플리케이션이 오디오 스트림 또는 비디오 스트림을 수신하는 시기를 제어하고 무단 가로채기로부터 데이터를 보호합니다.

기본적으로 Kaspersky Endpoint Security는 *신뢰하는* 그룹의 애플리케이션에 대한 오디오 및 비디오 스트림 수신만 허용합니다. *낮은 제한*, *높은 제한* 및 *신뢰하지 않음* 그룹의 애플리케이션은 장치로부터 오디오 스트림 및 비디오 스트림을 수신할 수 없습니다. 애플리케이션이 오디오 스트림 및 비디오 스트림을 수신하도록 직접 허용할 수 있습니다.

오디오 스트림 보호의 특수 기능

오디오 스트림 보호에는 다음과 같은 특별한 기능이 있습니다:

- 이 기능이 작동하려면 호스트 침입 방지를 사용하도록 설정해야 합니다.
- 호스트 침입 방지 구성 요소를 시작하기 전에 애플리케이션이 오디오 스트림 수신을 시작한 경우 Kaspersky Endpoint Security는 해당 애플리케이션의 오디오 스트림 수신을 허용하며 알림을 표시하지 않습니다.
- 애플리케이션이 오디오 스트림 수신을 시작한 후 사용자가 애플리케이션을 *신뢰하지 않음* 또는 *높은 제한* 그룹으로 이동한 경우 Kaspersky Endpoint Security는 오디오 스트림 수신을 허용하고 알림을 표시하지 않습니다.
- 사운드 녹음 장치에 대한 애플리케이션 접근 설정이 변경된 후에는(애플리케이션의 오디오 스트림 수신이 차단된 경우 등) 애플리케이션을 다시 시작해야 오디오 스트림 수신이 중지됩니다.
- 사운드 녹음 장치에서 전송되는 오디오 스트림에 대한 접근 제어는 애플리케이션의 웹캠 접근 설정과는 관련이 없습니다.
- Kaspersky Endpoint Security는 기본 제공 마이크 및 외부 마이크에 대한 접근만 보호합니다. 다른 오디오 스트리밍 장치는 지원되지 않습니다.
- Kaspersky Endpoint Security는 DSLR 카메라, 휴대용 비디오 카메라, 액션 카메라 등의 장치에서 전송되는 오디오 스트림에 대한 보호를 보장하지 못합니다.
- Kaspersky Endpoint Security를 설치한 후 오디오 및 비디오 또는 재생 애플리케이션을 처음으로 실행하면 오디오 및 비디오 또는 재생이 중단될 수 있습니다. 이는 애플리케이션의 사운드 녹음 장치 접근을 제어하는 기능을 설정하는 과정에서 불가피합니다. 따라서 Kaspersky Endpoint Security를 처음 실행할 때 오디오 하드웨어를 제어하는 시스템 서비스가 다시 시작됩니다.

애플리케이션 웹캠 접근 보호의 특수 기능

웹캠 접근 보호 기능에는 다음 특별 고려 사항과 제한이 있습니다:

- 애플리케이션은 비디오와 웹캠 데이터 처리를 통해 생성되는 정지 이미지를 제어합니다.
- 애플리케이션은 웹캠에서 수신된 비디오 스트림의 일부분인 오디오 스트림을 제어합니다.
- 애플리케이션은 Windows 장치 관리자에 이미징 장치로 표시되는 USB 또는 IEEE1394를 통해 연결된 웹캠만 제어합니다.
- Kaspersky Endpoint Security는 다음 웹캠을 지원합니다:
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800
  - Microsoft LifeCam Cinema

  Kaspersky는 이 목록에 지정되어 있지 않은 웹캠의 경우 지원을 보장하지 못합니다.

BadUSB 공격 방지

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(아래 그림 참조). 이 절차는 키보드 인증을 의미합니다.

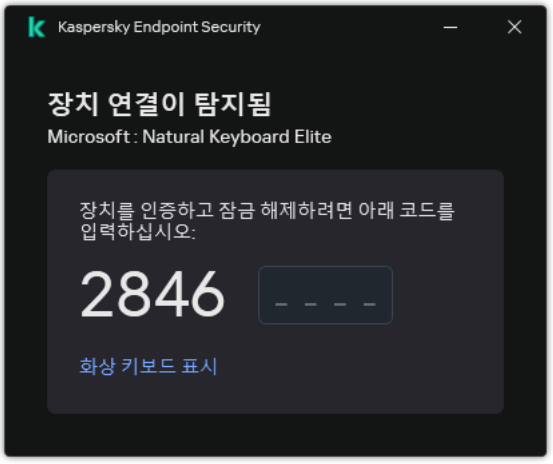
만일 해당 코드를 올바르게 입력했다면, 이 애플리케이션은 인증된 키보드 목록에 식별 파라미터(키보드의 VID/PID와 키보드가 연결된 포트 번호)를 저장합니다. 키보드를 다시 연결하거나 운영 체제를 재시작된 이후에는 키보드 인증을 반복할 필요가 없습니다.

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(아래 그림 참조) 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 요소는 기본적으로 설치되지 않습니다. BadUSB 공격 방지 구성 요소가 필요한 경우 애플리케이션을 설치하기 전에 설치 패키지 속성에 구성 요소를 추가하거나 애플리케이션을 설치한 후 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다.



키보드 인증

BadUSB 공격 방지 사용 및 중지

BadUSB 공격 방지 구성 요소가 설치되기 전에 컴퓨터에 연결되고 운영 체제에 의해 키보드로 식별된 USB 장치는 이 구성 요소가 설치된 이후에 인증된 것으로 간주됩니다.

관리 콘솔(MMC)에서 BadUSB 공격 방지 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 창에서 **필수 위협 보호** → **BadUSB 공격 방지**를 선택합니다.
4. **BadUSB 공격 방지** 확인란으로 구성 요소를 사용하거나 중지합니다.

5. **연결 시 USB 장치 인증** 블록에서 인증 코드 입력에 대한 보안 설정을 조정합니다:

   - **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 Endpoint Security는 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 장치 차단 시간. 유효한 값은 1~180(분)입니다.

6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 BadUSB 공격 방지 구성 요소를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **호스트 위협 보호** → **BadUSB 공격 방지**로 갑니다.

5. **BadUSB 공격 방지** 토글로 구성 요소를 사용하거나 중지합니다.

6. **USB 장치 인증** 블록에서 인증 코드 입력에 대한 보안 설정을 조정합니다:

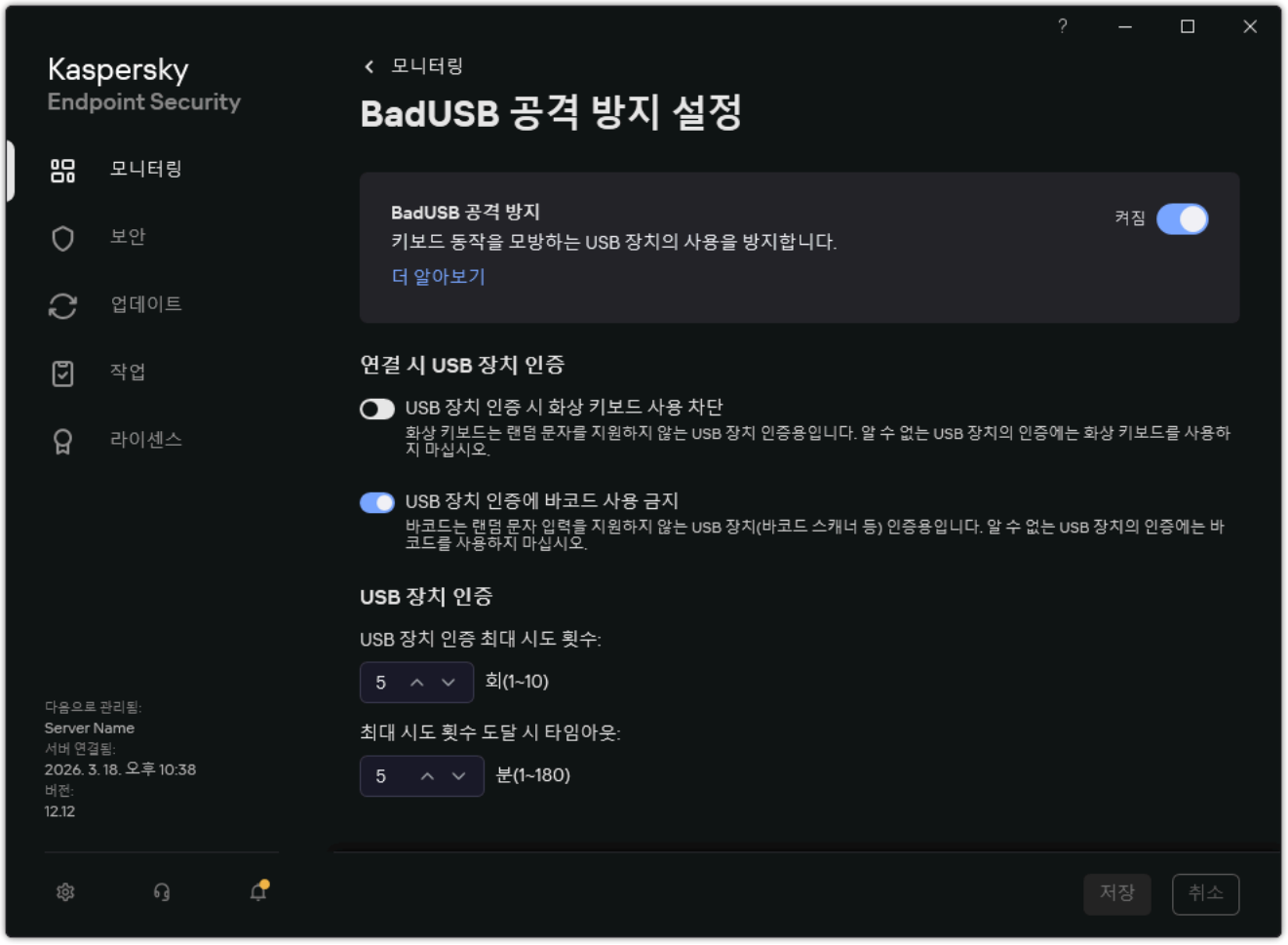
   - **USB 장치 인증 최대 시도 횟수**. 인증 코드를 지정된 횟수만큼 잘못 입력하면 USB 장치를 자동으로 차단합니다. 유효한 값은 1~10입니다. 예를 들어 인증 코드 입력을 5회 허용하는 경우 애플리케이션은 인증 코드 입력 5회 실패 후 USB 장치를 차단합니다. Kaspersky Endpoint Security는 USB 장치의 차단 시간을 표시합니다. 이 시간이 지나면 인증 코드 입력 가능 횟수가 다시 5회 생깁니다.

   - **최대 시도 횟수 도달 시 타임아웃(분)**. 인증 코드 입력 시도가 지정된 횟수만큼 실패할 시 USB 장치 차단 시간. 유효한 값은 1~180(분)입니다.

7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 BadUSB 공격 방지 구성 요소를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → BadUSB 공격 방지**를 선택합니다.



BadUSB 공격 방지 구성 요소 설정

3. **BadUSB 공격 방지** 토글로 구성 요소를 사용하거나 중지합니다.
4. **연결 시 USB 장치 인증** 블록에서 인증 코드 입력에 대한 보안 설정을 조정합니다:
   - **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 Endpoint Security는 USB 장치의 차단 시간을 표시합니다. 이 시간이 지나면 인증 코드 입력 가능 횟수가 다시 5회 생깁니다.
   - **최대 시도 횟수 도달 시 타임아웃**. 인증 코드 입력 시도가 지정된 횟수만큼 실패할 시 USB 장치 차단 시간. 유효한 값은 1~180(분)입니다.
5. 변경 사항을 저장합니다.

결과적으로 BadUSB 공격 방지를 사용하면 Kaspersky Endpoint Security는 운영 체제에서 키보드로 식별한 연결된 USB 장치의 인증을 요구합니다. 사용자는 키보드가 인증될 때까지 미인증 키보드를 사용할 수 없습니다.

USB 장치 인증 시 화상 키보드 사용

화상 키보드는 무작위 문자 입력을 지원하지 않는 USB 장치의 인증을 위해서만 사용됩니다(바코드 스캐너 등). 알려지지 않은 USB 장치의 인증에서는 화상 키보드 사용을 권장하지 않습니다.

관리 콘솔(MMC)에서 인증 시 화상 키보드 사용을 허용 또는 금지하는 방법

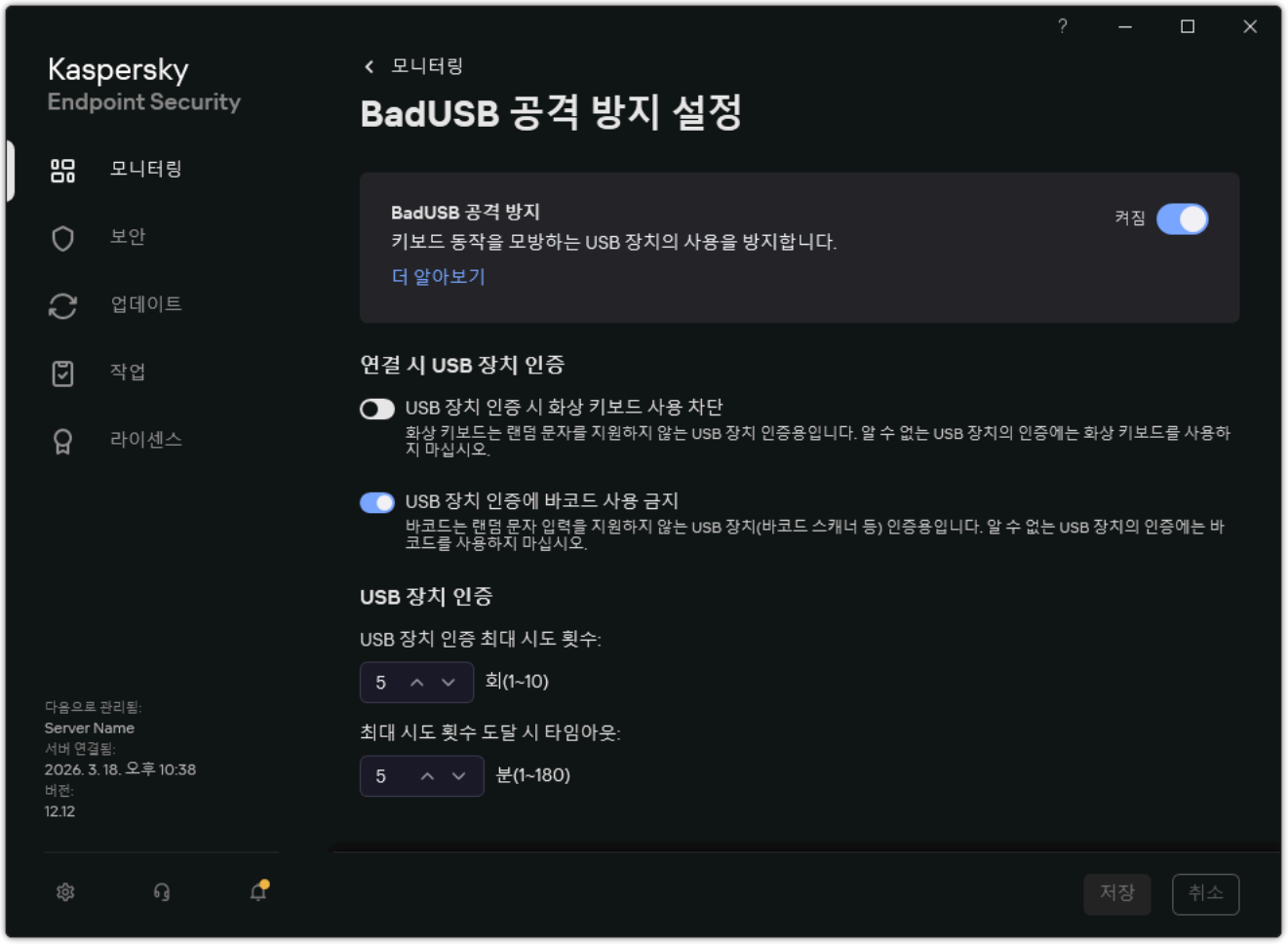
1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **필수 위협 보호 → BadUSB 공격 방지**를 선택합니다.
4. 인증 시 화상 키보드 사용을 차단하거나 허용하려면 **USB 장치 인증 시 화상 키보드 사용 차단** 확인란을 사용합니다.
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 인증 시 화상 키보드 사용을 허용 또는 금지하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → BadUSB 공격 방지**로 갑니다.
5. 인증 시 화상 키보드 사용을 차단하거나 허용하려면 **USB 장치 인증 시 화상 키보드 사용 차단** 토글을 사용합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 인증 시 화상 키보드의 사용을 허용 또는 금지하는 방법

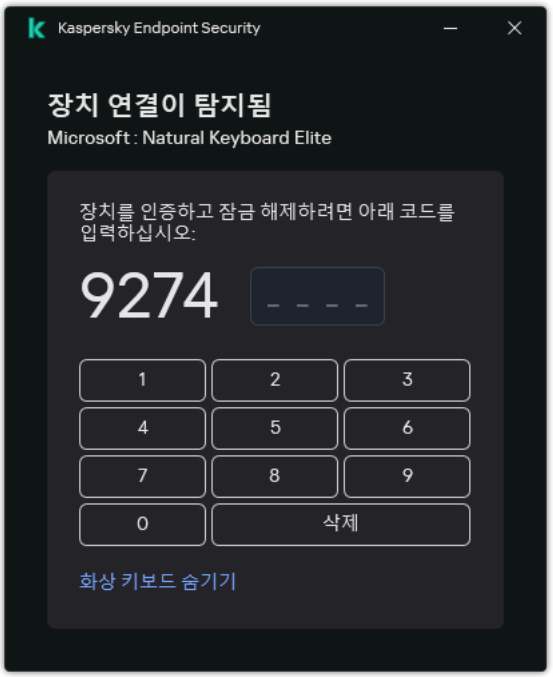
1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **BadUSB 공격 방지**를 선택합니다.



BadUSB 공격 방지 구성 요소 설정

3. 인증 시 화상 키보드 사용을 차단하거나 허용하려면 **USB 장치 인증 시 화상 키보드 사용 차단** 토글을 사용합니다.

4. 변경 사항을 저장합니다.



USB 장치 인증

바코드 스캐너 인증

바코드 스캐너를 컴퓨터에 연결하면, BadUSB 공격 방지 구성 요소가 이 장치를 입력 장치로 식별하고 인증을 하라는 메시지를 표시합니다. 바코드 스캐너를 인증하려면 화면에 표시된 바코드를 스캔해야 합니다. 애플리케이션은 바코드 및 QR 코드 스캐너 대부분에서 지원하는 Code39 형식으로 컴퓨터에서 바코드를 생성합니다.

Kaspersky Endpoint Security는 다른 바코드 스캐너 인증 방법도 지원합니다. 터치스크린 장치를 사용한다면 화상 키보드를 사용하여 코드를 입력할 수 있습니다. 그러려면 화상 키보드를 허용해야 합니다. 이 방법은 금전 등록기에 내장된 고정 바코드 스캐너 등을 사용할 때 편리합니다. 다른 바코드 스캐너 인증 방법은 사용할 수 없습니다.

기본적으로 애플리케이션은 USB 장치 인증에 바코드를 사용하지 않습니다.

관리 콘솔(MMC)에서 바코드로 USB 장치 인증을 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 콘솔 트리에서 **정책**을 선택합니다.

3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

4. 정책 창에서 **필수 위협 보호 → BadUSB 공격 방지**를 선택합니다.

5. 인증 시 바코드 사용을 차단하거나 허용하려면 **USB 장치 인증에 바코드 사용 금지** 확인란을 사용합니다.

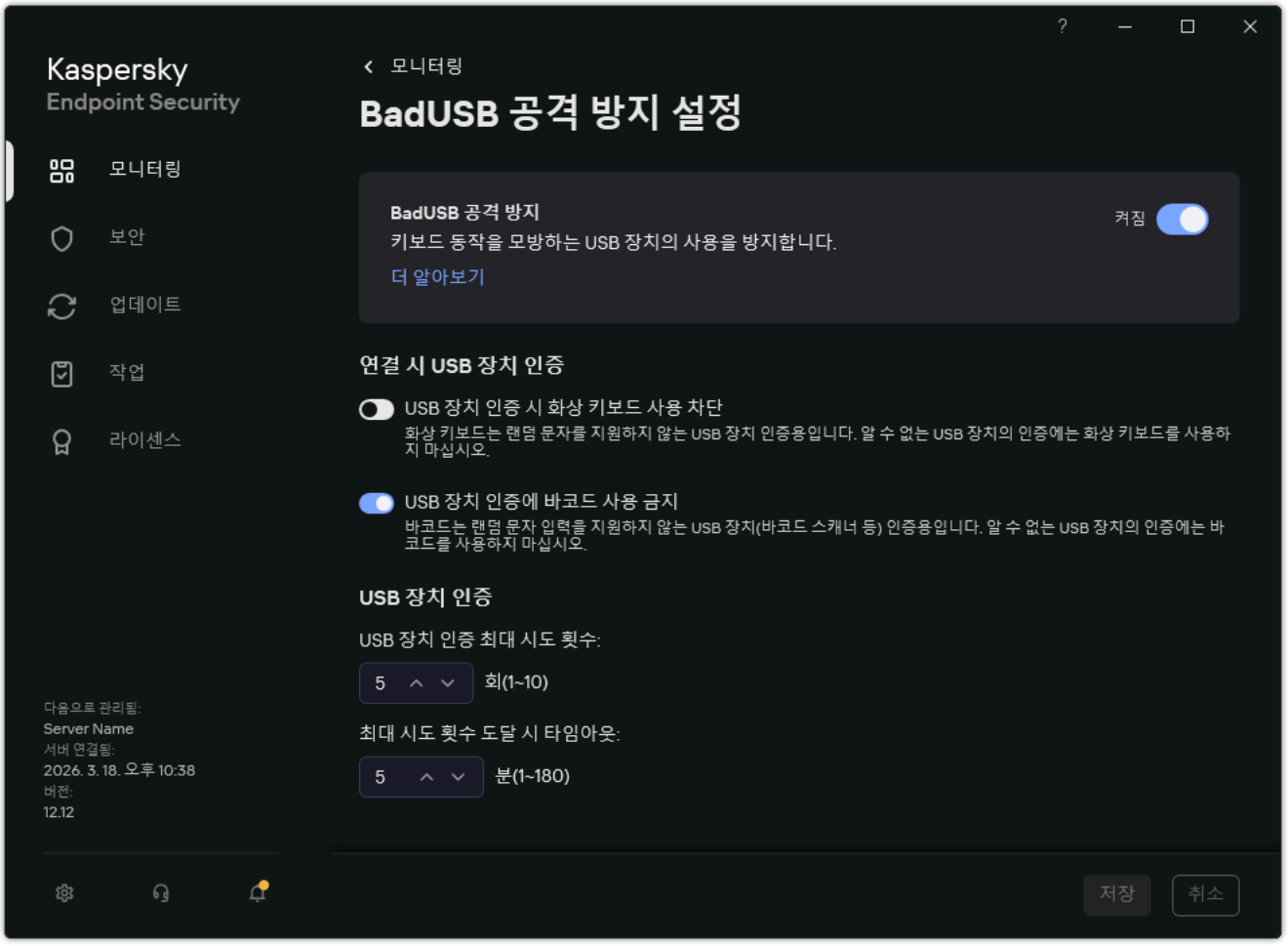
6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 바코드로 USB 장치 인증을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호** → **BadUSB 공격 방지**로 갑니다.
5. 인증 시 바코드 사용을 차단하거나 허용하려면 **USB 장치 인증에 바코드 사용 금지** 토글을 사용합니다.
6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 바코드로 USB 장치 인증을 활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **BadUSB 공격 방지**를 선택합니다.



BadUSB 공격 방지 구성 요소 설정

3. 인증 시 바코드 사용을 차단하거나 허용하려면 **USB 장치 인증에 바코드 사용 금지** 토글을 사용합니다.

4. 변경 사항을 저장합니다.

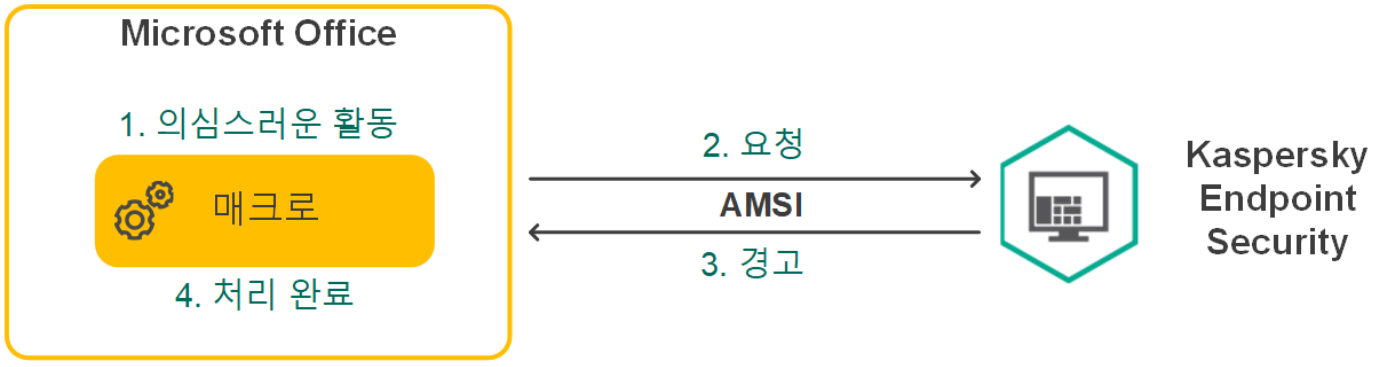


바코드 스캐너 인증

AMSI 보호

AMSI 보호 구성 요소는 Microsoft의 Antimalware Scan Interface를 지원합니다. *AMSI(Antimalware Scan Interface)*를 사용하는 경우 AMSI를 지원하는 타사 애플리케이션이 추가 검사를 위해 Kaspersky Endpoint Security에 PowerShell 스크립트 등의 개체를 전송하고 해당 개체에 대한 검사 결과를 받을 수 있습니다. 타사 애플리케이션에는 Microsoft Office 애플리케이션 등이 포함됩니다(아래 그림 참조). AMSI에 대한 자세한 정보는 Microsoft 설명서를 참조하십시오.

AMSI 보호는 위협을 탐지하기만 하며 제삼자 애플리케이션에 탐지된 위협에 대해 알립니다. 위협 알림을 수신한 타사 애플리케이션은 악성 동작을 허용하지 않습니다.(예: 해당 동작을 종료함)



AMSI 작동 모드

AMSI 보호 구성 요소는 제삼자 애플리케이션의 요청 수가 지정된 간격 내의 최대 횟수를 초과하는 등의 경우에 해당 애플리케이션의 요청을 거부할 수 있습니다. Kaspersky Endpoint Security는 타사 애플리케이션에서 전송했으나 거부된 요청에 대한 정보를 중앙 관리 서버로 전송합니다. AMSI 보호 구성 요소는 AMSI 보호 구성 요소와의 지속적 통합이 활성화된 타사 애플리케이션의 요청을 거부하지 않습니다.

AMSI 보호를 사용할 수 있는 워크 스테이션 및 서버용 운영 체제는 다음과 같습니다:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise 멀티 세션
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise

- Windows Server 2016 Essentials / Standard / Datacenter(Server Core 모드 포함)
- Windows Server 2019 Essentials / Standard / Datacenter(Server Core 모드 포함)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure 에디션(Server Core 모드 포함)
- Windows Server 2025 Standard / Datacenter

AMSI 보호 사용 및 중지

기본적으로 AMSI 보호를 사용하며 Kaspersky가 권장하는 모드에서 작동합니다(아래 표 참조).

관리 콘솔(MMC)에서 AMSI 보호를 활성화 또는 비활성화하는 방법

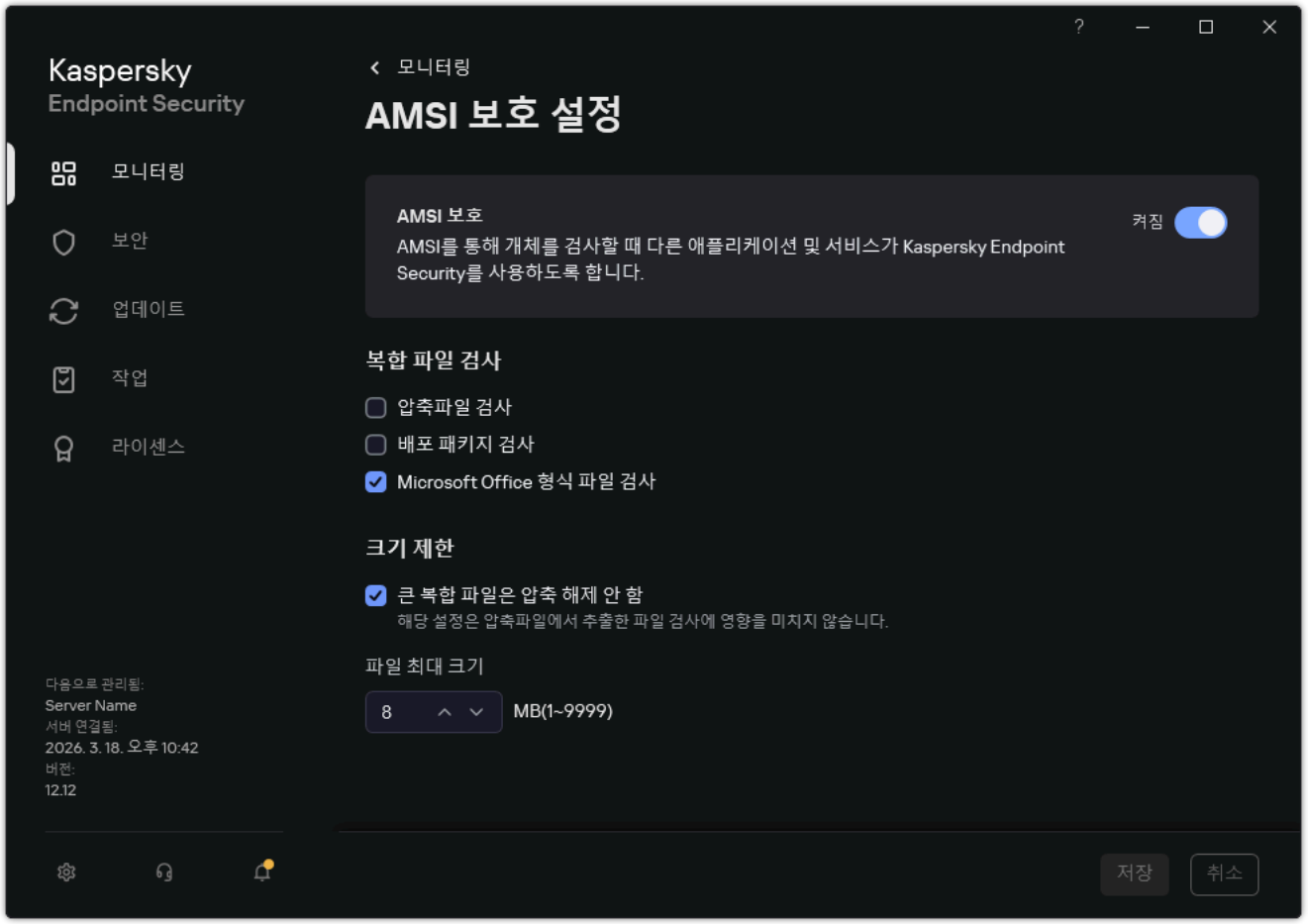
1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **필수 위협 보호** → **AMSI 스캐너**를 선택합니다.
4. **AMSI 스캐너** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.
5. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 AMSI 보호를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호** → **AMSI 보호**로 갑니다.
5. **AMSI 보호 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.
6. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 인터페이스에서 AMSI 보호를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **AMSI 보호**를 선택합니다.



AMSI 보호 설정

3. **AMSI 보호** 토글로 구성 요소를 사용하거나 중지합니다.
4. 변경 사항을 저장합니다.

Kaspersky 전문가가 권장하는 AMSI 보호 설정

파라미터	값	설명
압축파일 검사	**꺼짐**	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	**꺼짐**	타사 애플리케이션의 배포 패키지 검사.
Microsoft Office 형식 파일 검사	**켜기**	Microsoft Office 파일(DOC, DOCX, XLS, PPT 및 기타 Microsoft 확장자)을 검사합니다. Office 형식 파일에는 OLE 개체도 포함됩니다. 애플리케이션이 확인란 선택 여부와 상관없이 1MB보다 작은 오피스 형식 파일을 검사합니다.
큰 복합 파일은 압축 해제 안 함	**최대 파일 크기 8MB**	이 확인란을 선택하면 애플리케이션이 지정된 크기를 초과하는 복합 파일을 검사하지 않습니다. 이 확인란을 선택하지 않으면 애플리케이션이 크기에 자격 증명 공급업체이 모든 파일을 검사합니다. 애플리케이션은 확인란의 선택 여부와 관계없이 압축 파일에서 압축 해제한 대용량 파일을 검사합니다.

AMSI 보호로 파일 검사 최적화

파일 검사를 최적화할 수 있습니다: 검사 시간을 단축하고 Kaspersky Endpoint Security의 작업 속도를 높일 수 있습니다. 압축 파일, 배포 패키지, 오피스 형식 파일 등 검사가 필요한 복합 파일을 선택할 수 있습니다. 검사할 복합 파일의 크기를 제한할 수도 있습니다. AMSI 보호 구성 요소는 지정한 크기보다 큰 복합 파일을 압축 해제하지 않습니다.

바이러스나 기타 악성 코드를 숨기는 일반적인 방법은 압축 파일 같은 복합 파일에 심는 것입니다. 이런 방법으로 숨겨진 바이러스나 기타 악성 코드를 탐지하려면 복합 파일을 압축 해제 해야 하는데 그러면 검사 속도가 느려질 수 있습니다. 검사할 복합 파일의 유형을 제한하는 방법으로 검사 속도를 높일 수 있습니다.

관리 콘솔(MMC)에서 AMSI 보호로 파일 검사를 최적화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **필수 위협 보호** → **AMSI 스캐너**를 선택합니다.
4. **복합 파일 검사** 블록에서 압축 파일, 설치 패키지, 오피스 형식의 파일 등 검사할 복합 파일의 유형을 지정합니다.
5. **크기 제한** 블록에서 다음 중 하나를 수행합니다:
   - AMSI 보호 구성 요소가 대용량 복합 파일을 압축 해제하지 않게 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택하고 필요한 값을 지정합니다. AMSI 보호 구성 요소는 지정한 크기보다 큰 복합 파일을 압축 해제하지 않습니다.
   - AMSI 보호 구성 요소가 대용량 복합 파일을 압축 해제하도록 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택 해제합니다.

   AMSI 보호 구성 요소는 **큰 복합 파일은 압축 해제 안 함** 확인란의 선택 여부에 관계없이 압축 파일에서 나온 대용량 파일을 검사합니다.
6. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

웹 콘솔 및 Cloud Console에서 AMSI 보호로 파일 검사를 최적화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호** → **AMSI 보호**로 갑니다.
5. **복합 파일 검사** 블록에서 압축 파일, 설치 패키지, 오피스 형식의 파일 등 검사할 복합 파일의 유형을 지정합니다.

6. **검사 최적화** 블록에서 다음 중 하나를 수행합니다:

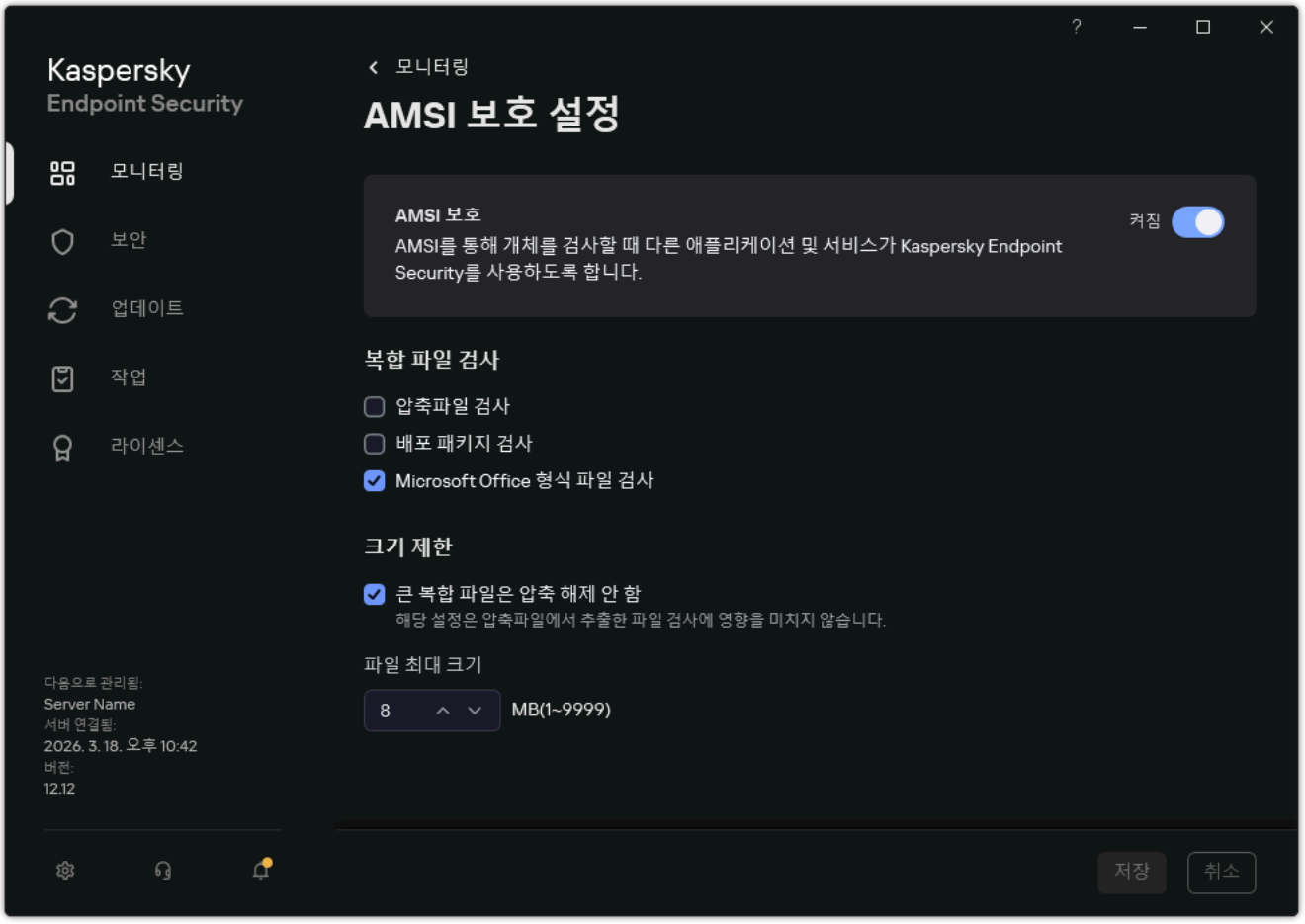
   - AMSI 보호 구성 요소가 대용량 복합 파일을 압축 해제하지 않게 하려면 **크기 제한 사용** 확인란을 선택하고 필요한 값을 지정합니다. AMSI 보호 구성 요소는 지정한 크기보다 큰 복합 파일을 압축 해제하지 않습니다.
   - AMSI 보호 구성 요소가 대용량 복합 파일을 압축 해제하도록 하려면 **크기 제한 사용** 확인란을 선택 해제합니다.

   AMSI 보호 구성 요소는 **크기 제한 사용** 확인란의 선택 여부와 관계없이 압축 파일에서 추출한 대용량 파일을 검사합니다.

7. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

애플리케이션 인터페이스에서 AMSI 보호로 파일 검사를 활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **AMSI 보호**를 선택합니다.



AMSI 보호 설정

3. **복합 파일 검사** 블록에서 압축 파일, 설치 패키지, 오피스 형식의 파일 등 검사할 복합 파일의 유형을 지정합니다.

4. **크기 제한** 블록에서 다음 중 하나를 수행합니다:

   - AMSI 보호 구성 요소가 대용량 복합 파일을 압축 해제하지 않게 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택하고 필요한 값을 지정합니다. AMSI 보호 구성 요소는 지정한 크기보다 큰 복합 파일을 압축 해제하지 않습니다.

   - AMSI 보호 구성 요소가 대용량 복합 파일을 압축 해제하도록 하려면 **큰 복합 파일은 압축 해제 안 함** 확인란을 선택 해제합니다.

   AMSI 보호 구성 요소는 **큰 복합 파일은 압축 해제 안 함** 확인란의 선택 여부에 관계없이 압축 파일에서 나온 대용량 파일을 검사합니다.

5. 변경 사항을 저장합니다.

웹 위협 보호

웹 위협 보호 구성 요소는 인터넷에서 악의적인 파일을 다운로드하지 못하도록 하며 악의적인 웹사이트와 피싱 웹사이트도 차단합니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다.

Kaspersky Endpoint Security는 HTTP-, HTTPS-, FTP-트래픽만 모니터링합니다. Kaspersky Endpoint Security는 URL 및 IP 주소를 검사합니다.

웹 위협 보호를 사용하려면 애플리케이션의 초기 구성을 완료해야 합니다.

- HTTPS 트래픽 모니터링의 경우, 암호화된 연결 검사를 활성화합니다(기본적으로 활성화되어 있습니다).

- Kaspersky Endpoint Security가 모니터링해야 하는 포트를 선택합니다(기본적으로 애플리케이션은 모든 포트를 모니터링합니다).

- Kaspersky Endpoint Security가 트래픽을 모니터링할 애플리케이션을 선택합니다. 대부분의 브라우저는 Kaspersky에서 권장하는 애플리케이션 목록에 이미 있습니다. 사용 중인 브라우저가 목록에 없는 경우 수동으로 추가하세요.

- 웹 트래픽에 웹 페이지 상호 작용 스크립트 삽입하는 것을 권장합니다(기본적으로 스크립트 삽입은 비활성화되어 있습니다). 이 스크립트를 사용하면 애플리케이션 이벤트 로그, OS 이벤트 로그 및 리포트에 대한 웹 위협 보호 이벤트를 등록할 수 있습니다.

사용자가 악성 및 피싱 웹사이트를 열려고 하면 Kaspersky Endpoint Security가 접근을 차단하고 경고를 표시합니다.

웹 위협 보호 사용 및 중지

기본적으로 웹 위협 보호 구성 요소는 작동되며 Kaspersky 전문가가 권장하는 모드에서 실행됩니다. 애플리케이션은 웹 위협 보호에 대해 다양한 설정 그룹을 적용할 수 있습니다. 애플리케이션에 저장된 이러한 설정 그룹을 *보안 레벨*이라고 하며 **높음**, **권장**, **낮음**으로 설정할 수 있습니다. **권장** 웹 트래픽 보안 레벨 설정은 Kaspersky 전문가가 권장하는 최적의 설정입니다. HTTP 및 FTP 프로토콜을 통해 송수신되는 웹 트래픽에 대해 기본 제공되는 보안 레벨 중 하나를 선택하거나 사용자 지정 웹트래픽 보안 레벨을 구성할 수 있습니다. 웹 트래픽 보안 레벨 설정을 변경한 경우 언제든지 권장 웹 트래픽 보안 레벨로 되돌릴 수 있습니다.

관리 콘솔(MMC) 또는 애플리케이션의 로컬 인터페이스에서만 보안 레벨을 선택하거나 구성할 수 있습니다. 웹 콘솔 또는 Cloud Console에서 보안 레벨을 선택하거나 구성할 수 없습니다.

관리 콘솔(MMC)에서 웹 위협 보호 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 창에서 **필수 위협 보호** → **웹 위협 보호**를 선택합니다.
4. **웹 위협 보호** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.
5. 구성 요소를 활성화했다면 **보안 레벨** 블록에서 다음 중 하나를 수행합니다.
   - 미리 설정된 보안 레벨 중 하나를 적용하려면 슬라이더로 레벨을 선택합니다.
     - **높음**. 웹 위협 보호 구성 요소가 HTTP 및 FTP를 통해 컴퓨터에 도착하는 웹 트래픽을 최대한 자세히 검사하는 보안 레벨입니다. 웹 위협 보호는 전체 애플리케이션 데이터베이스를 사용하여 모든 웹 트래픽 개체를 자세히 검사하고 가능한 정밀하게 휴리스틱 분석을 수행합니다.
     - **권장**. 애플리케이션의 성능과 웹 트래픽 보안 간에 최적의 균형을 유지하는 보안 레벨입니다. 웹 위협 보호 구성 요소는 보통 검사 레벨의 휴리스틱 분석을 수행합니다. 이 웹 트래픽 보안 레벨은 Kaspersky 전문가가 권장한 것입니다. 권장 보안 레벨 설정값은 아래 표에 나와 있습니다.
     - **낮음**. 이 웹 트래픽 보안 레벨 설정은 최대 속도의 웹 트래픽 검사를 보장합니다. 웹 위협 보호 구성 요소는 빠른 검사 레벨의 휴리스틱 분석을 수행합니다.
   - 사용자 지정 보안 레벨을 구성하려면 **설정** 버튼을 클릭하고 직접 구성 요소 설정을 정의합니다.

     보안 레벨에서 **기본값**을 클릭하여 사전 설정된 보안 수준 값을 복원할 수 있습니다.
6. **위협 탐지 시 처리 방법** 블록에서는 악성 웹 트래픽 개체 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:
   - **차단**. 이 옵션을 선택하고 감염된 개체가 웹 트래픽에서 탐지되면 웹 위협 보호 구성 요소는 개체에 대한 접근을 차단하고 브라우저에 메시지를 표시합니다.
   - **알림**. 이 옵션을 선택하고 웹 트래픽에서 감염된 개체가 탐지되면 Kaspersky Endpoint Security는 이 개체를 컴퓨터로 다운로드할 수 있도록 허용하지만 감염된 개체에 대한 정보를 처리 안 된 위협 목록에 추가합니다.
7. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 웹 위협 보호 구성 요소를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **통신 및 웹 보호** → **웹 위협 보호**로 갑니다.
5. **웹 위협 보호 활성화됨** 토글로 구성 요소를 활성화하거나 비활성화합니다.
6. **위협 탐지 시 처리 방법** 블록에서는 악성 웹 트래픽 개체 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:
   - **차단**. 이 옵션을 선택하고 감염된 개체가 웹 트래픽에서 탐지되면 웹 위협 보호 구성 요소는 개체에 대한 접근을 차단하고 브라우저에 메시지를 표시합니다.
   - **허용, 알림 또는 조치 확인(OS에 따라 다름)**. 이 옵션을 선택하고 웹 트래픽에서 감염된 개체가 탐지되면 Kaspersky Endpoint Security는 이 개체를 컴퓨터로 다운로드할 수 있도록 허용하지만 감염된 개체에 대한 정보를 처리 안 된 위협 목록에 추가합니다.
7. 필요하다면 신뢰하는 웹 주소 목록을 작성합니다.
8. 변경 사항을 저장합니다.

웹 위협 보호 구성 요소를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **웹 위협 보호**를 선택합니다.
3. **웹 위협 보호** 토글로 구성 요소를 사용하거나 중지합니다.
4. 구성 요소를 활성화했다면 **보안 레벨** 블록에서 다음 중 하나를 수행합니다.
   - 미리 설정된 보안 레벨 중 하나를 적용하려면 슬라이더로 레벨을 선택합니다.
     - **높음**. 웹 위협 보호 구성 요소가 HTTP 및 FTP를 통해 컴퓨터에 도착하는 웹 트래픽을 최대한 자세히 검사하는 보안 레벨입니다. 웹 위협 보호는 전체 애플리케이션 데이터베이스를 사용하여 모든 웹 트래픽 개체를 자세히 검사하고 가능한 정밀하게 휴리스틱 분석을 수행합니다.
     - **권장**. 애플리케이션의 성능과 웹 트래픽 보안 간에 최적의 균형을 유지하는 보안 레벨입니다. 웹 위협 보호 구성 요소는 보통 검사 레벨의 휴리스틱 분석을 수행합니다. 이 웹 트래픽 보안 레벨은 Kaspersky 전문가가 권장한 것입니다. 권장 보안 레벨 설정값은 아래 표에 나와 있습니다.
     - **낮음**. 이 웹 트래픽 보안 레벨 설정은 최대 속도의 웹 트래픽 검사를 보장합니다. 웹 위협 보호 구성 요소는 빠른 검사 레벨의 휴리스틱 분석을 수행합니다.
   - 사용자 지정 보안 레벨을 구성하려면 **고급 설정** 버튼을 클릭하고 고유 구성 요소 설정을 정의합니다.
     권장 보안 레벨 복원 버튼을 클릭하여 미리 설정된 보안 레벨을 복원할 수 있습니다.

5. **위협 탐지 시 처리 방법** 블록에서는 악성 웹 트래픽 개체 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:

   - **차단**. 이 옵션을 선택하고 감염된 개체가 웹 트래픽에서 탐지되면 웹 위협 보호 구성 요소는 개체에 대한 접근을 차단하고 브라우저에 메시지를 표시합니다.

   - **알림**. 이 옵션을 선택하고 웹 트래픽에서 감염된 개체가 탐지되면 Kaspersky Endpoint Security는 이 개체를 컴퓨터로 다운로드할 수 있도록 허용하지만 감염된 개체에 대한 정보를 처리 안 된 위협 목록에 추가합니다.

6. 변경 사항을 저장합니다.

Kaspersky 전문가가 권장하는 웹 위협 보호 설정(권장 보안 레벨)

파라미터	값	설명
악성 웹 주소 데이터베이스에서 웹 주소 확인	**켜기**	링크를 검사하여 악성 웹 주소 데이터베이스에 포함되어 있는지 확인하면 거부 목록에 등록된 웹사이트를 추적할 수 있습니다. 악성 웹 주소 데이터베이스는 Kaspersky에서 관리하는 것으로 애플리케이션 설치 프로그램 패키지에 포함되어 있으며 Kaspersky Endpoint Security 데이터베이스 업데이트와 함께 사용하여 보완할 수 있습니다.
피싱 웹 주소 데이터베이스에서 웹 주소 확인	**켜기**	피싱 웹 주소 데이터베이스에는 피싱 공격을 실행할 때 사용된 현재 알려진 웹사이트의 웹 주소가 포함되어 있습니다. Kaspersky는 이 피싱 링크 데이터베이스를 국제피싱대응협의체(APWG: Anti Phising Working Group)에서 받은 주소로 보완합니다. 피싱 URL 데이터베이스는 애플리케이션 설치 프로그램 패키지에 포함되어 있으며 Kaspersky Endpoint Security 데이터베이스 업데이트와 함께 사용하여 보완할 수 있습니다.
휴리스틱 분석 사용(웹 위협 보호)	**보통 검사**	현재 버전의 Kaspersky 애플리케이션 데이터베이스를 사용하여 식별할 수 없는 위협을 탐지하기 위해 개발된 기술입니다. 알려지지 않은 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 파일을 탐지합니다. 웹 트래픽에서 바이러스 및 보안위협이 있는 애플리케이션이 검사되면 휴리스틱 분석기는 실행 파일의 명령을 수행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
휴리스틱 분석 사용(안티 피싱)	**켜기**	현재 버전의 Kaspersky 애플리케이션 데이터베이스를 사용하여 식별할 수 없는 위협을 탐지하기 위해 개발된 기술입니다. 알려지지 않은 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 파일을 탐지합니다.
위협 탐지 시 처리 방법	**차단**	이 옵션을 선택하고 감염된 개체가 웹 트래픽에서 탐지되면 웹 위협 보호 구성 요소는 개체에 대한 접근을 차단하고 브라우저에 메시지를 표시합니다.

악성 웹 주소 탐지 방법 구성

웹 위협 보호는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스, 휴리스틱 분석을 사용하여 악성 웹 주소를 탐지합니다.

악성 웹 주소 탐지 방법은 관리 콘솔(MMC) 또는 애플리케이션의 로컬 인터페이스에서만 선택할 수 있습니다. 웹 콘솔 또는 Cloud Console에서는 악성 웹 주소 탐지 방법을 선택할 수 없습니다. 기본 옵션은 휴리스틱 분석(보통 검사)으로 악성 주소 데이터베이스에 대해 웹 주소를 확인하는 것입니다.

악성 주소 데이터베이스를 이용한 검사

링크를 검사하여 악성 웹 주소 데이터베이스에 포함되어 있는지 확인하면 거부 목록에 등록된 웹사이트를 추적할 수 있습니다. 악성 웹 주소 데이터베이스는 Kaspersky에서 관리하는 것으로 애플리케이션 설치 프로그램 패키지에 포함되어 있으며 Kaspersky Endpoint Security 데이터베이스 업데이트와 함께 사용하여 보완할 수 있습니다.

Kaspersky Endpoint Security는 모든 링크를 검사하여 악성 웹 주소 데이터베이스에 등록되어 있는지 확인합니다. 애플리케이션의 보안 연결 검사 설정은 링크 검사 기능에 영향을 주지 않습니다. 즉, 암호화된 연결 검사가 중지되면 Kaspersky Endpoint Security는 네트워크 트래픽이 암호화된 연결을 통해 전송될 때에도 악성 웹 주소의 데이터베이스에서 링크를 확인합니다.

관리 콘솔(MMC)을 사용하여 악성 웹 주소 데이터베이스에서의 웹 주소 확인을 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 창에서 **필수 위협 보호 → 웹 위협 보호**를 선택합니다.
4. **보안 레벨** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **검사 방법** 블록에서 **악성 웹 주소 데이터베이스에서 웹 주소 확인** 확인란을 선택하거나 선택 해제하여 악성 웹 주소 데이터베이스에서의 주소 확인을 활성화 또는 비활성화합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 악성 주소 데이터베이스에서의 주소 확인을 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 웹 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. **검사 방법** 블록에서 **악성 웹 주소 데이터베이스에서 웹 주소 확인** 확인란을 선택하거나 선택 해제하여 악성 웹 주소 데이터베이스에서의 주소 확인을 활성화 또는 비활성화합니다.
5. 변경 사항을 저장합니다.

휴리스틱 분석

휴리스틱 분석 시 Kaspersky Endpoint Security는 운영 체제의 애플리케이션 활동을 분석합니다. 휴리스틱 분석을 사용하면 현재 Kaspersky Endpoint Security 데이터베이스에 기록이 없는 위협도 탐지할 수 있습니다.

웹 트래픽에서 바이러스 및 보안위협이 있는 애플리케이션이 검사되면 휴리스틱 분석기는 실행 파일의 명령을 수행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.

관리 콘솔(MMC)에서 휴리스틱 분석을 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 창에서 **필수 위협 보호 → 웹 위협 보호**를 선택합니다.
4. **보안 레벨** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 웹 트래픽에서 바이러스 및 기타 악성 코드를 검사할 때 애플리케이션이 휴리스틱 분석을 사용하도록 하려면 열린 창에서 **검사 방법** 블록에서 **휴리스틱 분석 사용** 확인란을 선택합니다.
6. 슬라이더를 사용하여 휴리스틱 분석 레벨을 설정합니다: **빠른 검사**, **보통 검사**, **상세 검사**.

   웹 트래픽에서 바이러스 및 보안위협이 있는 애플리케이션이 검사되면 휴리스틱 분석기는 실행 파일의 명령을 수행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 휴리스틱 분석을 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 웹 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. 웹 트래픽에서 바이러스 및 기타 악성 코드를 검사할 때 애플리케이션이 휴리스틱 분석을 사용하도록 하려면 **검사 방법** 블록에서 **휴리스틱 분석 사용** 확인란을 선택합니다.

   웹 트래픽에서 바이러스 및 보안위협이 있는 애플리케이션이 검사되면 휴리스틱 분석기는 실행 파일의 명령을 수행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
5. 변경 사항을 저장합니다.

안티 피싱

웹 위협 보호는 링크가 피싱 웹 주소에 해당하는지 확인합니다. 이는 *피싱 공격* 방지에 도움이 됩니다. 피싱 공격은 거래 은행에서 온 이메일 메시지로 사칭할 수 있습니다. 해당 은행의 공식 웹사이트 링크가 이메일에 포함되어 있습니다. 링크를 누르면 은행 웹사이트와 똑같은 복제 사이트로 이동하고 브라우저의 주소 창에도 은행 웹사이트 주소가 나타납니다. 그러나 그것은 위장 사이트입니다. 이때부터 해당 사이트에서 수행하는 모든 작업이 추적되어 돈을 훔치는 데 사용될 수 있습니다.

피싱 웹사이트로 연결되는 링크는 이메일 메시지뿐만 아니라 메신저와 같은 다른 출처에서도 받을 수 있으므로, 웹 위협 보호 구성 요소는 웹 트래픽 검사 레벨에서 피싱 웹사이트에 대한 접근 시도를 모니터링하고 해당 웹사이트에 대한 접근을 차단합니다. 피싱 URL 목록은 Kaspersky Endpoint Security 배포 키트에 포함되어 있습니다.

안티 피싱은 관리 콘솔(MMC)이나 애플리케이션의 로컬 인터페이스에서만 구성할 수 있습니다. 웹 콘솔 또는 Cloud Console에서는 안티 피싱을 구성할 수 없습니다. 기본적으로 휴리스틱 분석이 포함된 안티 피싱이 활성화됩니다.

관리 콘솔(MMC)에서 안티 피싱을 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 창에서 **필수 위협 보호 → 웹 위협 보호**를 선택합니다.
4. **보안 레벨** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **안티 피싱 설정** 블록에서 **피싱 웹 주소 데이터베이스에서 웹 주소 확인** 확인란을 선택하거나 선택 해제하여 안티 피싱을 활성화하거나 비활성화합니다.

   피싱 웹 주소 데이터베이스에는 피싱 공격을 실행할 때 사용된 현재 알려진 웹사이트의 웹 주소가 포함되어 있습니다. Kaspersky는 이 피싱 링크 데이터베이스를 국제피싱대응협의체(APWG: Anti Phising Working Group)에서 받은 주소로 보완합니다. 피싱 URL 데이터베이스는 애플리케이션 설치 프로그램 패키지에 포함되어 있으며 Kaspersky Endpoint Security 데이터베이스 업데이트와 함께 사용하여 보완할 수 있습니다.
6. 웹 페이지에서 피싱 링크를 검사할 때 휴리스틱 분석을 사용하도록 하려면 안티 피싱 블록에서 **휴리스틱 분석 사용** 확인란을 선택합니다.

   휴리스틱 분석 시 Kaspersky Endpoint Security는 운영 체제의 애플리케이션 활동을 분석합니다. 휴리스틱 분석을 사용하면 현재 Kaspersky Endpoint Security 데이터베이스에 기록이 없는 위협도 탐지할 수 있습니다.

   안티 바이러스 데이터베이스 및 휴리스틱 분석 외에도 Kaspersky Security Network 평판 데이터베이스를 사용하여 링크를 검사할 수 있습니다.
7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 안티 피싱을 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 웹 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. 웹 위협 보호 구성 요소가 피싱 웹 주소 데이터베이스에서 링크를 확인하도록 하려면 **안티 피싱** 블록에서 **피싱 웹 주소 데이터베이스에서 웹 주소 확인** 확인란을 선택합니다. 피싱 웹 주소 데이터베이스에는 피싱 공격을 실행할 때 사용된 현재 알려진 웹사이트의 웹 주소가 포함되어 있습니다. Kaspersky는 이 피싱 링크 데이터베이스를 국제피싱대응협의체(APWG: Anti Phising Working Group)에서 받은 주소로 보완합니다. 피싱 URL 데이터베이스는 애플리케이션 설치 프로그램 패키지에 포함되어 있으며 Kaspersky Endpoint Security 데이터베이스 업데이트와 함께 사용하여 보완할 수 있습니다.
5. 웹 페이지에서 피싱 링크를 검사할 때 휴리스틱 분석을 사용하도록 하려면 안티 피싱 블록에서 **휴리스틱 분석 사용** 확인란을 선택합니다.

   휴리스틱 분석 시 Kaspersky Endpoint Security는 운영 체제의 애플리케이션 활동을 분석합니다. 휴리스틱 분석을 사용하면 현재 Kaspersky Endpoint Security 데이터베이스에 기록이 없는 위협도 탐지할 수 있습니다.

안티 바이러스 데이터베이스 및 휴리스틱 분석 외에도 Kaspersky Security Network 평판 데이터베이스를 사용하여 링크를 검사할 수 있습니다.

6. 변경 사항을 저장합니다.

신뢰하는 웹 주소 목록 생성

웹 위협 보호는 악성 및 피싱 웹사이트 외에 다른 웹사이트도 차단할 수 있습니다. 예를 들어 웹 위협 보호는 RFC 표준에 맞지 않는 HTTP 트래픽을 차단합니다. 신뢰할 수 있는 컨텐츠가 포함된 URL의 목록을 작성할 수 있습니다. 웹 위협 보호 구성 요소가 신뢰하는 웹 주소의 정보에 대해서는 바이러스 및 기타 위협 검사를 실시하지 않습니다. 예를 들어, 이 옵션은 공신력 있는 웹사이트에서 파일을 다운로드할 때 웹 위협 보호 구성 요소가 개입하지 않도록 하는데 유용할 수 있습니다.

URL은 특정 웹페이지의 주소 또는 웹사이트의 주소일 수 있습니다.

정책에서 신뢰하는 웹 주소 목록을 변경하면 부모 정책의 속성에 따라 차단될 수 있습니다. 목록을 변경하려면 웹 콘솔의 신뢰 구역('자물쇠'가 잠금 해제되어야 함) 설정 변경을 허용해야 합니다.

신뢰 구역은 관리 콘솔(MMC)과 웹 콘솔에서 다르게 그룹화됩니다. 마찬가지로, 신뢰 구역 파라미터의 변경을 방지하는 방법도 다릅니다('자물쇠'가 다름). 웹 콘솔만 사용하여 애플리케이션을 관리하는 것이 좋습니다. 서로 다른 콘솔에서 신뢰 구역을 구성하는 경우 관리 플러그인이 '자물쇠'를 기본 상태로 재설정할 수 있습니다.

관리 콘솔(MMC)에서 신뢰하는 웹 주소를 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **필수 위협 보호** → **웹 위협 보호**를 선택합니다.
4. **보안 레벨** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **신뢰하는 웹 주소** 탭을 선택합니다.
6. **신뢰하는 웹 주소의 웹 트래픽은 검사 안 함** 확인란을 선택합니다.

   이 옵션을 선택한 경우 웹 위협 보호 구성 요소는 주소가 신뢰하는 웹 주소 목록에 포함되어 있는 웹 페이지/웹사이트의 컨텐츠를 검사하지 않습니다. 웹 페이지/웹사이트의 지정 주소와 주소 마스크를 신뢰하는 웹 주소 목록에 추가할 수 있습니다.
7. 신뢰하는 컨텐츠가 있는 URL 및 웹페이지 목록을 만듭니다.

   Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.

   XML 파일에서 신뢰하는 웹 주소 목록 가져오기를 할 수도 있습니다.
8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 신뢰하는 웹 주소를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **통신 및 웹 보호** → **웹 위협 보호**로 갑니다.
5. **신뢰하는 웹 주소**를 클릭합니다.
6. 신뢰하는 컨텐츠가 있는 URL 및 웹페이지 목록을 만듭니다.
   Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.
   XML 파일에서 신뢰하는 웹 주소 목록 가져오기를 할 수도 있습니다.
7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 신뢰하는 웹 주소를 추가하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **웹 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. **신뢰하는 URL의 웹 트래픽은 검사 안 함** 확인란을 선택합니다.
   이 옵션을 선택한 경우 웹 위협 보호 구성 요소는 주소가 신뢰하는 웹 주소 목록에 포함되어 있는 웹 페이지/웹사이트의 컨텐츠를 검사하지 않습니다. 웹 페이지/웹사이트의 지정 주소와 주소 마스크를 신뢰하는 웹 주소 목록에 추가할 수 있습니다.
5. 신뢰하는 컨텐츠가 있는 URL 및 웹페이지 목록을 만듭니다.
   Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.
   XML 파일에서 신뢰하는 웹 주소 목록 가져오기를 할 수도 있습니다.
6. 변경 사항을 저장합니다.

결과적으로 웹 위협 보호는 신뢰할 수 있는 웹 주소의 트래픽을 검색하지 않습니다. 사용자는 언제든지 신뢰하는 웹사이트를 열고 해당 웹사이트에서 파일을 다운로드할 수 있습니다. 웹사이트에 액세스할 수 없을 시, 암호화된 연결 검사, 웹 제어, 네트워크 포트 모니터링 구성 요소의 설정을 확인하십시오. Kaspersky Endpoint Security가 신뢰할 수 있는 웹사이트에서 다운로드한 파일을 악성 파일로 감지하면 이 파일을 예외 규칙에 추가할 수 있습니다.

또한 암호화된 연결에 대한 일반 예외 규칙 목록을 생성할 수도 있습니다. 이때, Kaspersky Endpoint Security는 웹 위협 보호, 메일 위협 보호, 웹 제어 구성 요소가 작업을 수행할 때 신뢰하는 웹 주소의 HTTPS 트래픽을 검사하지 않습니다.

신뢰하는 웹 주소 목록 내보내기 및 가져오기

신뢰하는 웹 주소 목록을 XML 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 동일 유형의 웹 주소를 다수 추가하는 등의 작업을 진행할 수 있습니다. 내보내기/가져오기 기능을 사용하여 신뢰하는 웹 주소 목록을 백업하거나 목록을 다른 서버로 마이그레이션할 수도 있습니다.

관리 콘솔(MMC)에서 신뢰하는 웹 주소 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 창에서 **필수 위협 보호 → 웹 위협 보호**를 선택합니다.
4. **보안 레벨** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **신뢰하는 웹 주소** 탭을 선택합니다.
6. 신뢰하는 웹 주소 목록을 내보내려면 다음을 수행합니다.
   a. 내보낼 신뢰하는 주소를 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
      신뢰하는 웹 주소를 선택하지 않은 경우 Kaspersky Endpoint Security는 모든 웹 주소를 내보냅니다.
   b. **내보내기** 링크를 클릭합니다.
   c. 창이 열리면 신뢰하는 웹 주소 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   d. 파일을 저장합니다.
      Kaspersky Endpoint Security는 신뢰하는 웹 주소의 전체 목록을 XML 파일로 내보냅니다.
7. 신뢰하는 주소 목록을 가져오려면 다음과 같이 진행합니다:
   a. **가져오기** 링크를 클릭합니다.
      창이 열리면 신뢰하는 주소 목록을 가져올 XML 파일을 선택합니다.
   b. 파일을 엽니다.
      컴퓨터에 이미 신뢰하는 주소 목록이 있는 경우 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.
8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 신뢰하는 웹 주소 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **통신 및 웹 보호 → 웹 위협 보호**로 갑니다.

5. 예외 목록을 내보내려면 **규칙 목록** 블록에서:

   a. 내보낼 신뢰하는 주소를 선택합니다.

   b. → **내보내기** 버튼을 클릭합니다.

      Kaspersky Endpoint Security는 신뢰하는 웹 주소 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.

6. 예외 목록을 가져오려면 **규칙 목록** 블록에서:

   a. → **가져오기** 버튼을 클릭합니다.

      창이 열리면 신뢰하는 주소 목록을 가져올 JSON 파일을 선택합니다.

   b. 파일을 엽니다.

      컴퓨터에 이미 신뢰하는 주소 목록이 있는 경우 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 변경 사항을 저장합니다.

메일 위협 보호

메일 위협 보호 구성 요소는 보내고 받는 이메일 메시지 첨부파일에 바이러스 및 기타 위협이 있는지 검사합니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다.

메일 위협 보호는 수신 및 발신 메시지를 모두 검사할 수 있습니다. 애플리케이션은 다음 메일 클라이언트에서 POP3, SMTP, IMAP 및 NNTP를 지원합니다.

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Mozilla Thunderbird, MyOffice Mail 및 R7-Office Organizer 메일 클라이언트의 트래픽을 검사하려면 인증서 저장소에 Kaspersky 인증서 추가하고 자체 인증서 저장소를 선택해야 합니다.

메일 위협 보호는 다른 프로토콜 및 메일 클라이언트를 지원하지 않습니다.

메일 위협 보호가 항상 메시지에 대해 *프로토콜 수준*의 액세스(예: Microsoft Exchange 솔루션을 사용하는 경우)를 얻을 수 있는 것은 아닙니다. 이러한 이유로 메일 위협 보호에는 Microsoft Office Outlook용 확장 프로그램이 포함됩니다. 확장 프로그램을 사용하면 *메일 클라이언트 수준*에서 메시지를 검색할 수 있습니다. 메일 위협 보호 확장 프로그램은 Outlook 2010, 2013, 2016, 2019, 2021, 2024 및 365의 32비트 버전을 지원합니다. Arm 기반 컴퓨터에서는 메일 위협 보호 확장 프로그램이 Arm64용 Outlook 2016, Outlook 2021, Outlook 2024 및 Outlook 365의 32비트 버전을 지원합니다.

메일 클라이언트가 브라우저에서 열려 있으면 메일 위협 보호 구성 요소가 메시지를 검사하지 않습니다.

첨부 파일에서 악성 파일이 탐지되면 Kaspersky Endpoint Security는 메시지 제목에 *[메시지가 처리되었습니다] <메시지 제목>*과 같이 수행 작업에 대한 정보를 추가합니다.

메일 위협 보호 사용 및 중지

기본적으로 메일 위협 보호 구성 요소는 작동되며 Kaspersky 전문가가 권장하는 모드에서 실행됩니다. 애플리케이션은 메일 위협 보호에 대해 다양한 설정 그룹을 적용할 수 있습니다. 애플리케이션에 저장된 이러한 설정 그룹을 *보안 레벨*이라고 하며 **높음**, **권장**, **낮음**으로 설정할 수 있습니다. **권장** 메일 보안 레벨 설정은 Kaspersky 전문가가 권장하는 최적의 설정입니다(아래 표를 참고하십시오). 기본 제공되는 이메일 보안 레벨 중 하나를 선택하거나 사용자 지정 이메일 보안 레벨을 구성할 수 있습니다. 이메일 보안 레벨 설정을 변경한 경우 언제든지 권장 이메일 보안 레벨로 되돌릴 수 있습니다.

Mozilla Thunderbird 메일 클라이언트에서 사서함 폴더에서 메시지를 이동하는 필터를 사용하면 메일 위협 보호 구성 요소가 IMAP 프로토콜을 통해 전송되는 메시지에 대해 바이러스 및 기타 위협 검사를 수행하지 않습니다.

관리 콘솔(MMC)에서 메일 위협 보호 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 창에서 **필수 위협 보호 → 메일 위협 보호**를 선택합니다.
4. **메일 위협 보호** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.

5. 구성 요소를 활성화했다면 **보안 레벨** 블록에서 다음 중 하나를 수행합니다.

   - 미리 설정된 보안 레벨 중 하나를 적용하려면 슬라이더로 레벨을 선택합니다.

     - **높음**. 이 이메일 보안 레벨을 선택하면 메일 위협 보호 구성 요소가 이메일 메시지를 철저히 검사합니다. 메일 위협 보호 구성 요소는 수신 및 발신 이메일 메시지를 검사하고 정밀 휴리스틱 분석을 수행합니다. 높음 메일 보안 레벨은 위험도가 높은 환경에 권장합니다. 예를 들어, 중앙 집중식 이메일 보호로 보호되지 않는 홈 네트워크에서 무료 이메일 서비스에 연결하는 경우가 위험한 환경에 해당합니다.

     - **권장**. 애플리케이션의 성능과 이메일 보안 간에 최적의 균형을 유지하는 이메일 보안 레벨입니다. 메일 위협 보호 구성 요소는 수신 및 발신 이메일 메시지를 검사하고 보통 수준의 휴리스틱 분석을 수행합니다. 이 메일 트래픽 보안 레벨은 Kaspersky 전문가가 권장한 것입니다. 권장 보안 레벨 설정값은 아래 표에 나와 있습니다.

     - **낮음**. 이 이메일 보안 레벨을 선택하는 경우 메일 위협 보호 구성 요소가 받는 이메일 메시지만 검사하고 간단한 휴리스틱 분석을 수행하며 이메일 메시지에 첨부된 압축 파일을 검사하지 않습니다. 이 메일 보안 레벨에서는 메일 위협 보호 구성 요소가 운영 체제 리소스를 가장 적게 사용하며 가장 빠른 속도로 이메일 메시지를 검사합니다. 낮음 메일 보안 레벨은 확실하게 보호되는 안전한 환경에서 사용하는 경우 권장됩니다. 중앙 집중식 이메일 보안을 사용하는 기업 LAN이 그러한 환경에 속합니다.

   - 사용자 지정 보안 레벨을 구성하려면 **설정** 버튼을 클릭하고 직접 구성 요소 설정을 정의합니다.

     보안 레벨에서 **기본값**을 클릭하여 사전 설정된 보안 수준 값을 복원할 수 있습니다.

6. **위협 탐지 시 처리 방법** 블록에서는 악성 개체 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:

   - **치료 - 불가능한 경우 삭제**. 감염된 개체가 인바운드 또는 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 감염된 개체를 삭제합니다. 애플리케이션은 수행된 작업에 대한 정보를 *[메시지가 처리됨] <메시지 제목>* 등의 형식으로 메시지 제목에 추가합니다.

   - **치료 - 불가능한 경우 차단**. 감염된 개체가 인바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 감염된 개체가 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 개체를 치료할 수 없는 경우 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다.

   - **차단**. 인바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 아웃바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 메일 위협 보호 구성 요소를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **통신 및 웹 보호 → 메일 위협 보호**로 갑니다.

5. **메일 위협 보호 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.

6. **위협 탐지 시 처리 방법** 블록에서는 악성 개체 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:

   - **치료 - 불가능한 경우 삭제**. 감염된 개체가 인바운드 또는 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 감염된 개체를 삭제합니다. 애플리케이션은 수행된 작업에 대한 정보를 *[메시지가 처리됨] <메시지 제목>* 등의 형식으로 메시지 제목에 추가합니다.

   - **치료 - 불가능한 경우 차단**. 감염된 개체가 인바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 감염된 개체가 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 개체를 치료할 수 없는 경우 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다.

   - **차단**. 인바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 아웃바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다.

7. 필요하다면 메일 위협 보호의 고급 설정을 편집합니다.

8. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 메일 위협 보호 구성 요소를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **필수 위협 보호 → 메일 위협 보호**를 선택합니다.

3. **메일 위협 보호** 토글로 구성 요소를 사용하거나 중지합니다.

4. 구성 요소를 활성화했다면 **보안 레벨** 블록에서 다음 중 하나를 수행합니다.

   - 미리 설정된 보안 레벨 중 하나를 적용하려면 슬라이더로 레벨을 선택합니다.

     - **높음**. 이 이메일 보안 레벨을 선택하면 메일 위협 보호 구성 요소가 이메일 메시지를 철저히 검사합니다. 메일 위협 보호 구성 요소는 수신 및 발신 이메일 메시지를 검사하고 정밀 휴리스틱 분석을 수행합니다. 높음 메일 보안 레벨은 위험도가 높은 환경에 권장합니다. 예를 들어, 중앙 집중식 이메일 보호로 보호되지 않는 홈 네트워크에서 무료 이메일 서비스에 연결하는 경우가 위험한 환경에 해당합니다.

     - **권장**. 애플리케이션의 성능과 이메일 보안 간에 최적의 균형을 유지하는 이메일 보안 레벨입니다. 메일 위협 보호 구성 요소는 수신 및 발신 이메일 메시지를 검사하고 보통 수준의 휴리스틱 분석을 수행합니다. 이 메일 트래픽 보안 레벨은 Kaspersky 전문가가 권장한 것입니다. 권장 보안 레벨 설정값은 아래 표에 나와 있습니다.

     - **낮음**. 이 이메일 보안 레벨을 선택하는 경우 메일 위협 보호 구성 요소가 받는 이메일 메시지만 검사하고 간단한 휴리스틱 분석을 수행하며 이메일 메시지에 첨부된 압축 파일을 검사하지 않습니다. 이 메일 보안 레벨에서는 메일 위협 보호 구성 요소가 운영 체제 리소스를 가장 적게 사용하며 가장 빠른 속도로 이메일 메시지를 검사합니다. 낮음 메일 보안 레벨은 확실하게 보호되는 안전한 환경에서 사용하는 경우 권장됩니다. 중앙 집중식 이메일 보안을 사용하는 기업 LAN이 그러한 환경에 속합니다.

   - 사용자 지정 보안 레벨을 구성하려면 **고급 설정** 버튼을 클릭하고 고유 구성 요소 설정을 정의합니다.

     권장 보안 레벨 복원 버튼을 클릭하여 미리 설정된 보안 레벨을 복원할 수 있습니다.

5. **위협 탐지 시 처리 방법** 블록에서는 악성 개체 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:

   - **치료 - 불가능한 경우 삭제**. 감염된 개체가 인바운드 또는 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 감염된 개체를 삭제합니다. 애플리케이션은 수행된 작업에 대한 정보를 *[메시지가 처리됨] <메시지 제목>* 등의 형식으로 메시지 제목에 추가합니다.

   - **치료 - 불가능한 경우 차단**. 감염된 개체가 인바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 감염된 개체가 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 개체를 치료할 수 없는 경우 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다.

   - **차단**. 인바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 아웃바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다.

6. 변경 사항을 저장합니다.

Kaspersky 전문가가 권장하는 메일 위협 보호 설정(권장 보안 레벨)

파라미터	값	설명
보호 범위	**보내고 받는 메시지**	*보호 범위*에는 보내고 받는 메시지 또는 받는 메시지만과 같이 구성 요소에서 실행 시 확인하는 개체가 포함됩니다. 컴퓨터를 보호하려면 받는 메시지만 검사하면 됩니다. 보내는 메시지 검사를 켜서 감염된 파일이 압축 파일로 전송되지 않도록 할 수 있습니다. 예를 들어 오디오 및 비디오 파일과 같은 특정 형식의 파일이 전송되지 않도록 하려는 경우에도 보내는 메시지 검사를 켤 수 있습니다.
Microsoft Outlook 확장 프로그램 연결	**켜기**	이 확인란을 선택하면 POP3, SMTP, NNTP, IMAP 프로토콜을 통해 전송된 이메일 메시지의 검사를 Microsoft Outlook에 통합된 확장 프로그램에서 작동할 수 있습니다. Microsoft Outlook용 확장 프로그램을 사용하여 메일을 검사하는 경우 Cached Exchange Mode를 사용하는 것이 좋습니다. Exchange 캐싱 모드에 대한 자세한 내용 및 모드 사용 관련 권장 사항은 Microsoft 기술 자료 를 참조하십시오.
첨부된 압축파일 검사	**켜기**	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.
Microsoft Office 형식의 첨부 파일 검사	**켜기**	Microsoft Office 파일(DOC, DOCX, XLS, PPT 및 기타 Microsoft 확장자)을 검사합니다. Office 형식 파일에는 OLE 개체도 포함됩니다. 애플리케이션이 확인란 선택 여부와 상관없이 1MB보다 작은 오피스 형식 파일을 검사합니다.
첨부 파일 필터	**선택한 유형의 첨부 파일 이름 바꾸기**	이 옵션을 선택하면 메일 위협 보호 구성 요소가 지정된 유형의 첨부파일 확장자의 마지막 문자를 밑줄 문자(예: attachment.doc_)로 바꿉니다. 따라서 파일을 열려면 파일 이름을 바꿔야 합니다.
휴리스틱 분석	**보통 검사**	현재 버전의 Kaspersky 애플리케이션 데이터베이스를 사용하여 식별할 수 없는 위협을 탐지하기 위해 개발된 기술입니다. 알려지지 않은 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 파일을 탐지합니다. 파일에서 악성 코드를 검사할 때 휴리스틱 분석기는 실행 파일의 명령을 실행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
위협 탐지 시 처리 방법	**치료 - 불가능한 경우 삭제**	감염된 개체가 인바운드 또는 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 감염된 개체를 삭제합니다. 애플리케이션은 수행된 작업에 대한 정보를 *[메시지가 처리됨] <메시지 제목>* 등의 형식으로 메시지 제목에 추가합니다.

감염된 이메일 메시지에 수행할 처리 방법 변경

기본적으로 메일 위협 보호 구성 요소는 탐지된 모든 감염 이메일 메시지를 자동으로 치료합니다. 치료에 실패할 경우 메일 위협 보호 구성 요소가 감염된 이메일 메시지를 삭제합니다.

감염된 이메일 메시지에 수행할 처리 방법을 변경하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 메일 위협 보호**를 선택합니다.
3. **위협 탐지 시 처리 방법** 블록에서는 감염된 메시지 탐지 시 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:
   - **치료 - 불가능한 경우 삭제**. 감염된 개체가 인바운드 또는 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 감염된 개체를 삭제합니다. 애플리케이션은 수행된 작업에 대한 정보를 *[메시지가 처리됨]<메시지 제목>* 등의 형식으로 메시지 제목에 추가합니다.
   - **치료 - 불가능한 경우 차단**. 감염된 개체가 인바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 감염된 개체가 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 개체를 치료할 수 없는 경우 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다.
   - **차단**. 인바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 아웃바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다.
4. 변경 사항을 저장합니다.

메일 위협 보호 구성 요소의 보호 범위 구성

*보호 범위*란 활성 상태의 구성 요소에서 검사되는 개체를 말합니다. 각 구성 요소의 보호 범위는 서로 다른 속성을 가집니다. 메일 위협 보호 구성 요소의 보호 범위 속성에는 메일 위협 보호 구성 요소를 메일 클라이언트에 통합하는 설정 및 메일 위협 보호에서 트래픽을 검사할 이메일 메시지의 유형과 이메일 프로토콜 등이 포함됩니다. 기본적으로 Kaspersky Endpoint Security는 보내고 받는 모든 이메일 메시지와 POP3, SMTP, NNTP 및 IMAP 프로토콜을 통과하는 트래픽을 검사하며, Microsoft Office Outlook 메일 클라이언트와 통합됩니다.

메일 위협 보호 구성 요소의 보호 범위를 구성하려면 다음과 같이 진행합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 메일 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.

4. **보호 범위** 블록에서 검사할 메시지를 선택합니다:

   - **보내고 받는 메시지**
   - **수신 메시지만**

   컴퓨터를 보호하려면 받는 메시지만 검사하면 됩니다. 보내는 메시지 검사를 켜서 감염된 파일이 압축 파일로 전송되지 않도록 할 수 있습니다. 예를 들어 오디오 및 비디오 파일과 같은 특정 형식의 파일이 전송되지 않도록 하려는 경우에도 보내는 메시지 검사를 켤 수 있습니다.

   받는 메시지만 검사하도록 설정하는 경우 내 컴퓨터에 메일을 통해 유포되는 이메일 웜이 있을 수 있으므로 모든 보내는 메시지에 대해 1회 검사를 수행하는 것이 좋습니다. 그러면 자신의 컴퓨터에서 감염된 메시지가 포함된 이메일이 검사되지 않은 상태로 전달되는 결과를 막을 수 있습니다.

5. **연결성** 블록에서는 다음을 수행합니다.

   - POP3, SMTP, NNTP 및 IMAP 프로토콜을 통해 전송되는 메시지를 컴퓨터로 수신하기 전에 메일 위협 보호 구성 요소에서 이러한 이메일 메시지를 검사하도록 하려면 **POP3, SMTP, NNTP, IMAP 트래픽 검사** 확인란을 선택합니다.

     POP3, SMTP, NNTP 및 IMAP 프로토콜을 통해 전송되는 메시지가 컴퓨터에 도착하기 전에 메일 위협 보호 구성 요소에서 이러한 이메일 메시지를 검사하지 않도록 하려면 **POP3, SMTP, NNTP, IMAP 트래픽 검사** 확인란을 선택 해제합니다. 이 때, **Microsoft Outlook 확장 프로그램 연결** 확인란을 선택하면 사용자의 컴퓨터에 메시지가 도착했을 때 Microsoft Office Outlook 메일 클라이언트에 내장된 메일 위협 보호 확장 프로그램이 메시지를 검사합니다.

     Microsoft Office Outlook 이외의 메일 클라이언트 사용 시 **POP3, SMTP, NNTP, IMAP 트래픽 검사** 확인란을 선택 해제하면 메일 위협 보호 구성 요소가 POP3, SMTP, NNTP 및 IMAP 프로토콜을 통해 전송되는 메시지를 검색하지 않습니다.

   - Microsoft Office Outlook에서 메일 위협 보호 구성 요소 설정에 접근할 수 있도록 허용하고, POP3, SMTP, NNTP, IMAP 및 MAPI 프로토콜을 통해 전송되는 메일 메시지가 컴퓨터가 도착한 후에 Microsoft Office Outlook에 통합된 확장 프로그램에서 이를 검사하도록 하려면 **Microsoft Outlook 확장 프로그램 연결** 확인란을 선택합니다.

     Microsoft Office Outlook에서 메일 위협 보호 구성 요소 설정에 대한 접근을 차단하고 POP3, SMTP, NNTP, IMAP 및 MAPI 프로토콜을 통해 전송되는 메일 메시지가 컴퓨터가 도착한 후에 Microsoft Office Outlook에 통합된 확장 프로그램에서 이를 검사하지 않도록 하려면 **Microsoft Outlook 확장 프로그램 연결** 확인란을 선택 해제합니다.

     메일 위협 보호 확장 프로그램은 Kaspersky Endpoint Security가 설치될 때 Microsoft Office Outlook 메일 클라이언트에 통합됩니다.

6. 변경 사항을 저장합니다.

이메일 메시지에 첨부된 복합 파일 검사

이메일 첨부파일 검사를 작동 또는 중지하거나, 검사되는 첨부파일의 최대 크기 및 첨부파일 검사에 걸리는 최대 시간을 제한할 수 있습니다.

이메일 메시지에 첨부된 복합 파일의 검사를 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 메일 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.
4. **복합 파일 검사** 블록에서 검사 설정을 구성합니다:
   - **Microsoft Office 형식의 첨부 파일 검사**. Microsoft Office 파일(DOC, DOCX, XLS, PPT 및 기타 Microsoft 확장자)을 검사합니다. Office 형식 파일에는 OLE 개체도 포함됩니다. 애플리케이션이 확인란 선택 여부와 상관없이 1MB보다 작은 오피스 형식 파일을 검사합니다.
   - **첨부된 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.

     검사 과정에서 애플리케이션이 메시지 텍스트에 있는 압축 파일의 암호를 감지하면 이 암호를 사용하여 악성 애플리케이션용 압축 파일의 내용을 검사합니다. 이 경우 암호는 저장되지 않습니다. 검사할 때 압축 파일의 압축이 해제됩니다. 압축을 풀 때 애플리케이션 오류가 발생하는 경우에는 %systemroot%\temp 경로에 저장된 압축이 풀린 파일을 사용자가 직접 삭제할 수 있습니다. 이 파일의 접두사는 PR입니다.

   - **다음보다 큰 압축파일 검사 안 함: NMB(1~9999)**. 이 확인란을 선택하면 메일 위협 보호 구성 요소는 압축된 이메일 첨부 메시지의 크기가 지정된 값을 초과하는 경우 해당 파일을 검사 대상에서 예외합니다. 만일 확인란이 선택 해제되면 메일 위협 보호 구성 요소는 모든 크기의 이메일 첨부파일을 검사합니다.
   - **압축파일 확인 시간을 다음으로 한정: N초(1~9999)**. 이 확인란을 선택한 경우 압축된 이메일 첨부 메시지를 검사하는 데 할당된 시간은 지정된 시간으로 제한됩니다.
5. 변경 사항을 저장합니다.

이메일 메시지 첨부파일 필터

첨부파일 필터링 기능은 보내는 이메일 메시지에는 적용되지 않습니다.

악성 애플리케이션은 이메일 첨부파일의 형태로 유포될 수 있습니다. 이메일 첨부파일의 형식을 기준으로 필터링하도록 구성하면 지정된 파일 유형이 자동으로 이름이 변경되거나 삭제됩니다. 어떤 유형의 첨부파일의 이름을 바꿔, Kaspersky Endpoint Security가 악성 애플리케이션의 자동 실행으로부터 컴퓨터를 보호할 수 있습니다.

첨부파일 필터링을 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 메일 위협 보호**를 선택합니다.
3. **고급 설정**을 클릭합니다.

4. **첨부 파일 필터** 블록에서 다음 중 하나를 수행합니다:

   - **필터링 비활성화**. 이 옵션을 선택한 경우 메일 위협 보호 구성 요소는 이메일 메시지에 첨부된 파일을 필터링하지 않습니다.
   - **선택한 유형의 첨부 파일 이름 바꾸기**. 이 옵션을 선택하면 메일 위협 보호 구성 요소가 지정된 유형의 첨부 파일 확장자의 마지막 문자를 밑줄 문자(예: attachment.doc_)로 바꿉니다. 따라서 파일을 열려면 파일 이름을 바꿔야 합니다.
   - **선택한 유형의 첨부 파일 삭제**. 이 옵션을 선택한 경우 메일 위협 보호 구성 요소는 이메일 메시지에서 지정한 유형의 첨부파일을 삭제합니다.

5. 이전 단계에서 **선택한 유형의 첨부 파일 이름 바꾸기** 옵션 또는 **선택한 유형의 첨부 파일 삭제** 옵션을 선택한 경우 관련 파일 형식 옆의 확인란을 선택합니다.

6. 변경 사항을 저장합니다.

첨부파일 필터링을 위한 확장 프로그램 내보내기 및 가져오기

첨부파일 필터 확장 프로그램 목록을 XML 파일로 내보낼 수 있습니다. 내보내기/가져오기 기능을 사용하여 확장 프로그램 목록을 백업하거나 목록을 다른 서버로 마이그레이션할 수 있습니다.

관리 콘솔(MMC)에서 첨부파일 필터 확장 프로그램 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **통신 및 웹 보호 → 메일 위협 보호**로 갑니다.

5. **첨부 파일 필터** 블록의 확장 프로그램 목록을 내보내려면 다음을 수행합니다.

   a. 내보낼 확장 프로그램을 선택합니다.

   b. **내보내기** 링크를 클릭합니다.

   c. 창이 열리면 확장 프로그램 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

   d. 파일을 저장합니다.
      Kaspersky Endpoint Security는 확장 프로그램의 전체 목록을 XML 파일로 내보냅니다.

6. **첨부 파일 필터** 블록의 확장 프로그램 목록을 가져오려면 다음을 수행합니다.

   a. **가져오기** 링크를 클릭합니다.

   b. 창이 열리면 확장 프로그램 목록을 가져올 XML 파일을 선택합니다.

c. 파일을 엽니다.

컴퓨터에 이미 확장 프로그램 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 변경 사항을 저장합니다.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **필수 위협 보호 → 메일 위협 보호**를 선택합니다.

4. **보안 레벨** 블록에서 **설정** 버튼을 클릭합니다.

5. 열린 창에서 **첨부 파일 필터** 탭을 선택합니다.

6. 확장 프로그램 목록을 내보내려면 다음을 수행합니다.

a. 내보낼 확장 프로그램을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.

b. **내보내기** 링크를 클릭합니다.

c. 창이 열리면 확장 프로그램 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

d. 파일을 저장합니다.

Kaspersky Endpoint Security는 확장 프로그램의 전체 목록을 XML 파일로 내보냅니다.

7. 확장 프로그램 목록을 가져오려면 다음을 수행합니다.

a. **가져오기** 링크를 클릭합니다.

b. 창이 열리면 확장 프로그램 목록을 가져올 XML 파일을 선택합니다.

c. 파일을 엽니다.

컴퓨터에 이미 확장 프로그램 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. 변경 사항을 저장합니다.

Microsoft Office Outlook의 이메일 검사

Kaspersky Endpoint Security를 설치하는 동안 Microsoft Office Outlook(이하 Outlook)에 내장된 메일 위협 보호 확장 프로그램이 설치됩니다. 확장 프로그램을 사용하면 프로토콜 수준이 아닌 메일 클라이언트 수준에서 메시지를 검색할 수 있습니다. 메시지 외에도 확장 프로그램을 사용하면 Microsoft Exchange 리포지토리에서 MAPI 인터페이스를 통해 받은 개체(예: 캘린더 내 개체)를 검색할 수 있습니다. 메일 클라이언트에서 이 검색이 수행됩니다.

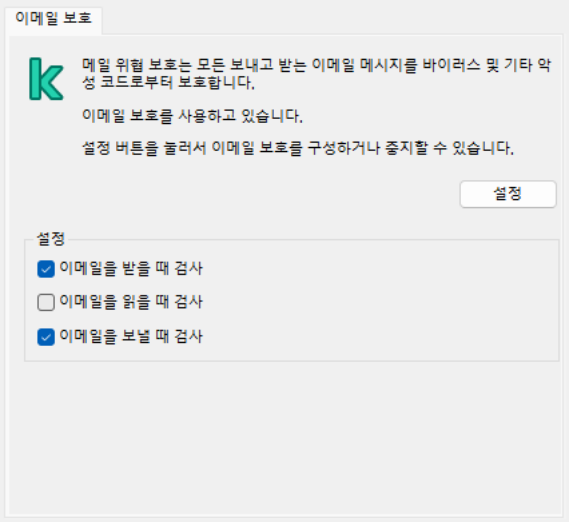
Outlook 내에서 메일 위협 보호 구성 요소 설정을 열 수 있으며, 이메일 메시지에 바이러스 및 기타 위협이 있는지 검사하는 시기도 지정할 수 있습니다.

메일 위협 보호 확장 프로그램은 Outlook 2010, 2013, 2016, 2019, 2021, 2024 및 365의 32비트 버전을 지원합니다.

Arm 기반 컴퓨터에서는 메일 위협 보호 확장 프로그램이 Arm64용 Outlook 2016, Outlook 2021, Outlook 2024 및 Outlook 365의 32비트 버전을 지원합니다.

Outlook에서 받는 메시지는 먼저 메일 위협 보호 구성 요소(Kaspersky Endpoint Security 인터페이스에서 POP3, SMTP, NNTP, IMAP 트래픽 검사 확인란을 선택한 경우)에서 검사한 다음 Outlook에 통합된 메일 위협 보호 확장 프로그램에서 검사합니다. 메일 위협 보호 구성 요소가 메시지에서 악성 개체를 탐지할 경우 이를 사용자에게 알립니다.

Kaspersky Endpoint Security 인터페이스에서 Microsoft Outlook 확장 프로그램이 연결되었을 때 Outlook에서 직접 메일 위협 보호 구성 요소 설정을 구성할 수 있습니다(아래 그림 참조).



Outlook의 메일 위협 보호 구성 요소 설정

보내는 메시지는 먼저 Outlook에 통합된 메일 위협 보호 확장 프로그램에서 검사한 다음 메일 위협 보호 구성 요소에서 검사합니다.

Outlook용 메일 위협 보호 구성 요소 확장 프로그램을 사용하여 메일을 검사하는 경우 Exchange 캐싱 모드를 사용하는 것이 좋습니다. Exchange 캐싱 모드에 대한 자세한 내용 및 모드 사용 관련 권장 사항은 Microsoft 기술 자료를 참조하십시오.

Outlook용 메일 위협 보호 확장 프로그램의 운영 모드를 구성하려면 다음을 수행합니다.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **필수 위협 보호 → 메일 위협 보호**를 선택합니다.
4. **보안 레벨** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **연결성** 블록에서, **설정** 버튼을 클릭합니다.

6. **이메일 보호** 창에서 다음을 수행합니다:

   - Outlook용 메일 위협 보호 확장 프로그램이 받는 메일이 사서함에 도착할 때 메일을 검사하도록 설정하려면 **이메일을 받을 때 검사** 확인란을 선택합니다.
   - Outlook용 메일 위협 보호 확장 프로그램이 사용자가 받은 메일을 열 때 메일을 검사하도록 설정하려면 **이메일을 읽을 때 검사** 확인란을 선택합니다.
   - Outlook용 메일 위협 보호 확장 프로그램이 보내는 메일을 보낼 때 메일을 검사하도록 설정하려면 **이메일을 보낼 때 검사** 확인란을 선택합니다.

7. 변경 사항을 저장합니다.

Thunderbird, MyOffice, R7-Office에서 이메일 검사

메일 위협 보호 구성 요소는 보내고 받는 이메일 메시지 첨부파일에 바이러스 및 기타 위협이 있는지 검사합니다. Mozilla Thunderbird, MyOffice Mail 및 R7-Office Organizer 메일 클라이언트의 경우 애플리케이션은 *프로토콜 수준* (POP3, SMTP, IMAP, NNTP)에서만 메시지에 접근할 수 있습니다.

Mozilla Thunderbird, MyOffice Mail 및 R7-Office Organizer 메일 클라이언트의 트래픽을 검사하려면 인증서 저장소에 Kaspersky 인증서 추가하고 자체 인증서 저장소를 선택해야 합니다.

메일 클라이언트가 브라우저에서 열려 있으면 메일 위협 보호 구성 요소가 메시지를 검사하지 않습니다.

실시간 메일 위협 보호

메일 위협 보호는 수신 및 발신 메시지를 모두 검사할 수 있습니다. 기본적으로 메일 위협 보호 구성 요소는 탐지된 모든 감염 이메일 메시지를 자동으로 치료합니다. 치료에 실패할 경우 메일 위협 보호 구성 요소가 감염된 이메일 메시지를 삭제합니다. 첨부 파일에서 악성 파일이 탐지되면 Kaspersky Endpoint Security는 메시지 제목에 *[메시지가 처리되었습니다] <메시지 제목>*과 같이 수행 작업에 대한 정보를 추가합니다.

Mozilla Thunderbird 메일 클라이언트에서 사서함 폴더에서 메시지를 이동하는 필터를 사용하면 메일 위협 보호 구성 요소가 IMAP 프로토콜을 통해 전송되는 메시지에 대해 바이러스 및 기타 위협 검사를 수행하지 않습니다.

메일 데이터베이스의 악성 코드 검사

악성 코드 검사 작업을 사용하면 메일 형식 파일을 검사할 수 있습니다. 이러한 메일 클라이언트의 파일에서 악성 개체가 탐지되면 Kaspersky Endpoint Security는 탐지한 개체에 대한 정보만 활성 위협 목록에 추가합니다. 애플리케이션은 작업 설정에 관계없이 메일 데이터베이스에서 감염된 파일을 치료하거나 삭제하지 않습니다.

활성 위협 제거

메일 위협 보호는 프로토콜 수준에서 컴퓨터의 감염을 방지하지만, Kaspersky Endpoint Security를 설치하기 전에 컴퓨터가 감염되었다면 애플리케이션은 메일 데이터베이스에서 위협을 탐지할 수만 있습니다. 메일 위협 보호에는 Microsoft Office Outlook과 같은 메시지를 여러 부분(헤더, 본문, 첨부 파일)으로 분해할 수 있는 구성 요소는 포함되지 않습니다. 따라서 애플리케이션이 탐지된 개체를 삭제하거나 치료할 수 없습니다. Kaspersky Endpoint Security는 탐지된 개체에 대한 정보만 활성 위협 목록에 추가합니다.

활성 위협을 제거하려면:

1. 메일 클라이언트 인터페이스에서 탐지된 개체가 포함된 메시지를 직접 찾아 삭제합니다.

   애플리케이션은 탐지된 개체에 대한 정보를 활성 위협 목록에 표시합니다.

   탐지된 개체 카드의 예:

   HEUR:Trojan.PDF.Phish.gen
   개체:`C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. 데이터베이스 압축 작업을 수행합니다.

   사용자 인터페이스에서 메시지가 삭제되면 메일 클라이언트는 삭제 표시만 추가합니다. 메일 클라이언트는 데이터베이스를 압축한 후에만 메시지를 삭제합니다. 데이터베이스 압축에 대한 자세한 내용은 메일 클라이언트(예: Mozilla Thunderbird)의 도움말을 참조하십시오.

3. *악성 코드 검사* 작업을 다시 실행하고 보안 위협이 더 이상 존재하지 않는지 확인합니다.

네트워크 위협 보호

네트워크 위협 보호 구성 요소(침입 탐지 시스템, Intrusion Detection System, IDS라고도 함)는 인바운드 네트워크 트래픽에서 네트워크 공격의 활동 특성을 모니터링합니다. 애플리케이션은 사용자 컴퓨터에 시도된 네트워크 공격을 탐지하면 공격 컴퓨터와의 네트워크 연결을 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.

네트워크 위협 보호 사용 및 중지

기본적으로 네트워크 위협 보호는 작동되어 있으며 최적 모드가 사용됩니다. Kaspersky Endpoint Security는 인바운드 네트워크 트래픽에서 네트워크 공격의 활동 특성에 대해 모니터링하고 공격을 차단합니다.

관리 콘솔(MMC)에서 네트워크 위협 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 창에서 **필수 위협 보호 → 네트워크 위협 보호**를 선택합니다.

4. **네트워크 위협 보호** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.

5. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 네트워크 위협 보호를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **통신 및 웹 보호** → **네트워크 위협 보호**로 갑니다.

5. **네트워크 위협 보호 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 네트워크 위협 보호를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **필수 위협 보호** → **네트워크 위협 보호**를 선택합니다.



네트워크 위협 보호 설정

3. **네트워크 위협 보호** 토글로 구성 요소를 사용하거나 중지합니다.

4. 변경 사항을 저장합니다.

공격 컴퓨터 차단

네트워크 위협 보호 구성 요소를 활성화하면 Kaspersky Endpoint Security가 자동으로 네트워크 위협을 차단합니다. 또한 애플리케이션은 컴퓨터 공격을 차단하고 특정 시간 동안 네트워크 패킷 전송을 제한할 수 있습니다. 기본적으로 Kaspersky Endpoint Security는 1시간 동안 컴퓨터를 차단합니다.

관리 콘솔(MMC)에서 컴퓨터 공격을 차단하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **필수 위협 보호 → 네트워크 위협 보호**를 선택합니다.
4. **네트워크 위협 보호 설정**에서 **다음 시간 동안 공격 장치 차단: N 분** 확인란을 선택합니다.

   이 옵션이 활성화되면 네트워크 위협 보호 구성 요소가 차단 목록에 컴퓨터 공격을 추가합니다. 이렇게 되면 첫 번째 네트워크 공격 시도가 발생한 후 지정된 기간 동안 네트워크 위협 보호 구성 요소에서 공격 컴퓨터와의 네트워크 연결을 차단합니다. 이를 통해 향후 동일한 주소에서 발생하는 네트워크 공격으로부터 사용자의 컴퓨터를 자동으로 보호할 수 있습니다. 공격 컴퓨터가 차단 목록에서 보내야 하는 최소 시간은 1분입니다. 최대 시간은 999분입니다.
5. **다음 시간 동안 공격 장치 차단: N분** 확인란 오른쪽 필드에서 공격 컴퓨터에 대한 차단 기간을 다양하게 설정할 수 있습니다.
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 컴퓨터 공격을 차단하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **통신 및 웹 보호 → 네트워크 위협 보호**로 갑니다.
5. **위협 탐지 시 처리 방법** 블록에서 **다음 시간 동안 공격 및 공격 장치 차단(분)** 확인란을 선택합니다.

   이 옵션이 활성화되면 네트워크 위협 보호 구성 요소가 차단 목록에 컴퓨터 공격을 추가합니다. 이렇게 되면 첫 번째 네트워크 공격 시도가 발생한 후 지정된 기간 동안 네트워크 위협 보호 구성 요소에서 공격 컴퓨터와의 네트워크 연결을 차단합니다. 이를 통해 향후 동일한 주소에서 발생하는 네트워크 공격으로부터 사용자의 컴퓨터를 자동으로 보호할 수 있습니다. 공격 컴퓨터가 차단 목록에서 보내야 하는 최소 시간은 1분입니다. 최대 시간은 999분입니다.
6. 공격 컴퓨터의 차단 지속 시간을 변경합니다.
7. 변경 사항을 저장합니다.

애플리케이션의 사용자 인터페이스에서 컴퓨터 공격을 차단하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 네트워크 위협 보호**를 선택합니다.



네트워크 위협 보호 설정

3. **다음 시간 동안 공격 장치 차단: N분** 토글을 켭니다.

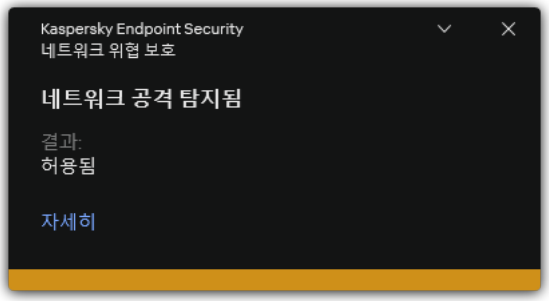
   이 옵션이 활성화되면 네트워크 위협 보호 구성 요소가 차단 목록에 컴퓨터 공격을 추가합니다. 이렇게 되면 첫 번째 네트워크 공격 시도가 발생한 후 지정된 기간 동안 네트워크 위협 보호 구성 요소에서 공격 컴퓨터와의 네트워크 연결을 차단합니다. 이를 통해 향후 동일한 주소에서 발생하는 네트워크 공격으로부터 사용자의 컴퓨터를 자동으로 보호할 수 있습니다. 공격 컴퓨터가 차단 목록에서 보내야 하는 최소 시간은 1분입니다. 최대 시간은 999분입니다.

4. **다음 시간 동안 공격 장치 차단: N분** 토글 스위치 아래의 필드에서 컴퓨터 공격에 대한 차단 기간을 다양하게 설정할 수 있습니다.

5. 변경 사항을 저장합니다.

결과적으로 Kaspersky Endpoint Security는 사용자 컴퓨터에 대한 네트워크 공격 시도를 탐지하면 공격 컴퓨터와의 모든 연결을 차단합니다. Kaspersky Endpoint Security에서 *네트워크 공격 탐지* 이벤트를 띄웁니다. 이벤트에는 공격을 시도한 컴퓨터의 정보(IP 및 MAC 주소)가 포함됩니다.

애플리케이션의 사용자 인터페이스 또는 Kaspersky Security Center 콘솔 버전 15.1 이상에서만 공격하는 컴퓨터의 MAC 주소를 볼 수 있습니다.



네트워크 공격 탐지 알림

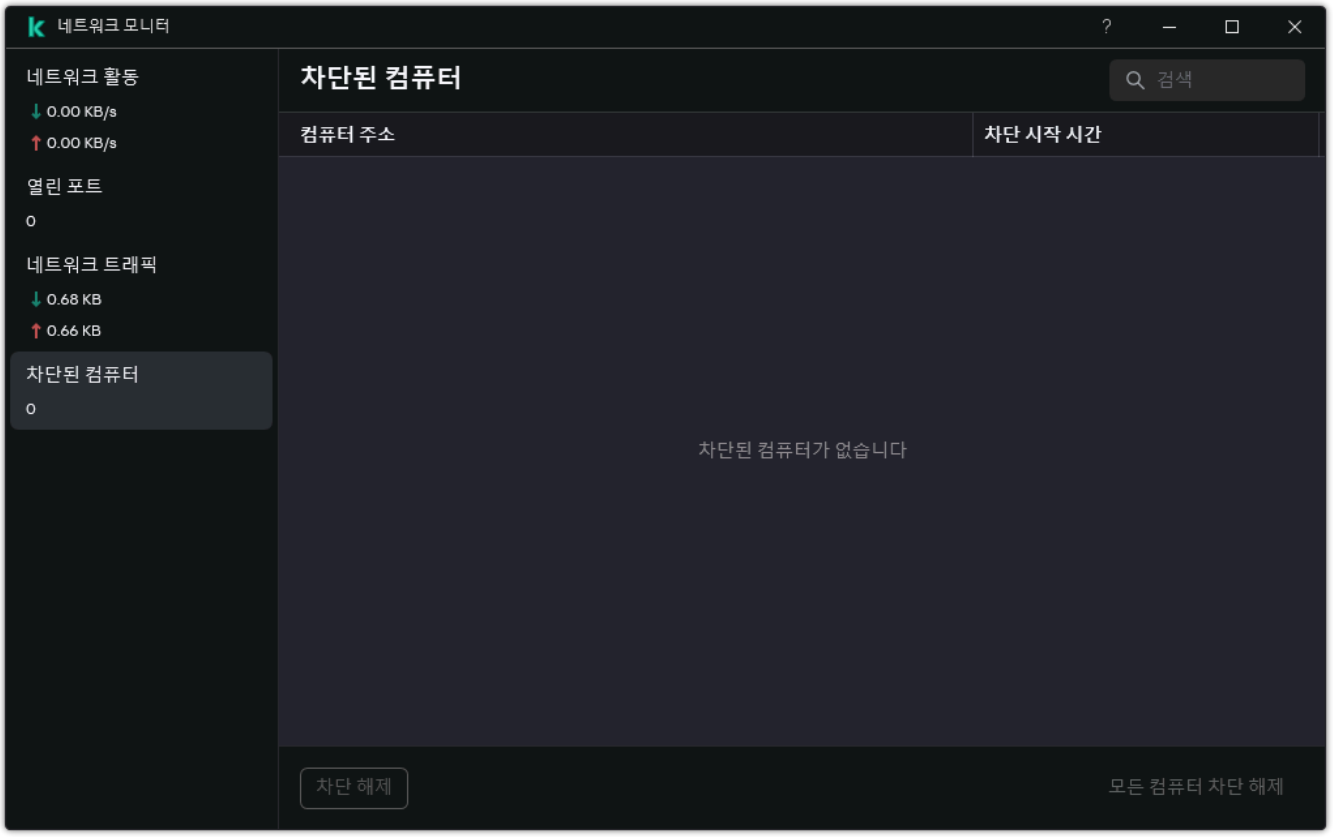
Kaspersky Endpoint Security는 지정된 시간이 지나면 컴퓨터 차단을 해제합니다. Kaspersky Security Center 콘솔은 리포트의 *네트워크 공격이 탐지됨* 이벤트 외에는 차단된 컴퓨터를 모니터링하는 도구를 제공하지 않습니다. 애플리케이션 인터페이스에서는 차단된 컴퓨터 목록만 볼 수 있습니다. 이 기능은 *네트워크 모니터* 도구에서 제공합니다. 네트워크 모니터 도구를 사용하여 컴퓨터 차단을 해제할 수도 있습니다.

컴퓨터 차단을 해제하는 방법:

1. 메인 애플리케이션 창의 **모니터링** 섹션에서 **네트워크 모니터** 타일을 클릭합니다.
2. **차단한 컴퓨터** 탭을 선택합니다.
   그러면 차단된 컴퓨터 목록이 열립니다(아래 그림 참조).

Kaspersky Endpoint Security는 애플리케이션이 다시 시작될 때와 네트워크 위협 보호 설정이 변경될 때 차단 목록을 지웁니다.

3. 차단을 해제할 컴퓨터를 선택하고 **차단 해제**를 클릭합니다.



차단된 컴퓨터 목록

차단에서 예외할 주소 구성

Kaspersky Endpoint Security는 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 Endpoint Security 12.2에 추가되었습니다. 애플리케이션과 관리 플러그인이 버전 12.2 이상으로 업데이트되었는지 확인하십시오. 이전 버전의 애플리케이션 또는 관리 플러그인을 사용 중인 경우 Kaspersky Endpoint Security는 IP 주소로만 네트워크 활동을 허용할 수 있습니다.

차단 예외 목록을 변경하면 부모 정책의 속성에 따라 차단될 수 있습니다. 목록을 변경하려면 웹 콘솔의 신뢰 구역('자물쇠'가 잠금 해제되어야 함) 설정 변경을 허용해야 합니다.

신뢰 구역은 관리 콘솔(MMC)과 웹 콘솔에서 다르게 그룹화됩니다. 마찬가지로, 신뢰 구역 파라미터의 변경을 방지하는 방법도 다릅니다('자물쇠'가 다름). 웹 콘솔만 사용하여 애플리케이션을 관리하는 것이 좋습니다. 서로 다른 콘솔에서 신뢰 구역을 구성하는 경우 관리 플러그인이 '자물쇠'를 기본 상태로 재설정할 수 있습니다.

관리 콘솔(MMC)의 차단에서 예외 주소를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **필수 위협 보호 → 네트워크 위협 보호**를 선택합니다.
4. **네트워크 위협 보호 설정** 블록에서 **예외** 버튼을 클릭합니다.
5. 열리는 창에서 **추가** 버튼을 누릅니다.
6. 네트워크 공격을 차단해야 하는 컴퓨터의 IP 주소를 입력합니다.
   필요한 경우 데이터가 전송되는 프로토콜과 포트를 선택합니다.
7. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console의 차단에서 예외 주소를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **통신 및 웹 보호 → 네트워크 위협 보호**로 갑니다.
5. 창 상단에서 **신뢰하는 IP 주소** 링크를 클릭합니다.
6. 열리는 창에서 **추가** 버튼을 누릅니다.
7. 네트워크 공격을 차단해야 하는 컴퓨터의 IP 주소를 입력합니다.
   필요한 경우 데이터가 전송되는 프로토콜과 포트를 선택합니다.
8. 변경 사항을 저장합니다.

애플리케이션의 사용자 인터페이스의 차단에서 예외 주소를 구성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 네트워크 위협 보호**를 선택합니다.



네트워크 위협 보호 설정

3. **예외 규칙 관리** 링크를 클릭합니다.
4. 열리는 창에서 **추가** 버튼을 누릅니다.
5. 네트워크 공격을 차단해야 하는 컴퓨터의 IP 주소를 입력합니다.
   필요한 경우 데이터가 전송되는 프로토콜과 포트를 선택합니다.
6. 변경 사항을 저장합니다.

차단 예외 규칙 목록 내보내기 및 가져오기

예외 규칙 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.

관리 콘솔(MMC)에서 예외 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 창에서 **필수 위협 보호 → 네트워크 위협 보호**를 선택합니다.

4. **네트워크 위협 보호 설정** 블록에서 **예외** 버튼을 클릭합니다.

5. 규칙 목록을 내보내려면 다음을 수행합니다.

   a. 내보낼 예외 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
   예외 규칙을 아무 것도 선택하지 않으면 Kaspersky Endpoint Security가 모든 예외 규칙을 내보냅니다.

   b. → **내보내기** 버튼을 클릭합니다.

   c. 창이 열리면 예외 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

   d. 파일을 저장합니다.
   Kaspersky Endpoint Security는 예외 규칙의 전체 목록을 XML 파일로 내보냅니다.

6. 예외 목록을 가져오려면 다음을 수행합니다.

   a. → **가져오기** 버튼을 클릭합니다.

   b. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.

   c. 파일을 엽니다.
   컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 예외 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **통신 및 웹 보호 → 네트워크 위협 보호**로 갑니다.

5. 창 상단에서 **신뢰하는 IP 주소** 링크를 클릭합니다.
   예외 규칙 목록이 열립니다.

6. 규칙 목록을 내보내려면 다음을 수행합니다.

   a. 내보낼 예외 규칙을 선택합니다.

   b. → **내보내기** 버튼을 클릭합니다.
   Kaspersky Endpoint Security는 예외 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.

7. 예외 목록을 가져오려면 다음을 수행합니다.

   a. → **가져오기** 버튼을 클릭합니다.
   창이 열리면 예외 규칙 목록을 가져올 JSON 파일을 선택합니다.

   b. 파일을 엽니다.
   컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. 변경 사항을 저장합니다.

유형별 네트워크 위협 보호 구성

Kaspersky Endpoint Security에서 다음 유형의 네트워크 공격에 대한 보호를 관리할 수 있습니다:

- *네트워크 플러딩*은 조직의 네트워크 리소스(웹 서버 등)에 대한 공격입니다. 이 공격은 많은 양의 요청을 보내 네트워크 리소스 대역폭의 과부하를 유발합니다. 이러면 사용자가 조직의 네트워크 리소스에 접근할 수 없게 됩니다.

- *포트 검사* 공격은 컴퓨터의 UDP 포트, TCP 포트, 네트워크 서비스에 대한 검사로 구성됩니다. 공격자는 이 공격을 통해 컴퓨터의 취약점을 파악한 후 더 위험한 유형의 네트워크 공격을 수행할 수 있습니다. 또한 컴퓨터의 운영 체제를 식별하여 이 운영 체제에 적합한 네트워크 공격을 선택할 수 있습니다.

- *MAC 스푸핑 공격*에서는 네트워크 장치(네트워크 카드)의 MAC 주소를 변경합니다. 그러면 공격자는 장치로 전송된 데이터를 다른 장치로 리다이렉트하고 이 데이터에 접근할 수 있습니다. Kaspersky Endpoint Security에서는 MAC 스푸핑 공격을 차단하고 공격 관련 알림을 수신할 수 있습니다.

허용된 애플리케이션 중 일부가 이러한 유형의 공격에서 일반적으로 발견되는 작업을 수행하면 이러한 유형의 공격 탐지를 비활성화할 수 있습니다. 이는 잘못된 알림을 방지하는 데 도움이 됩니다.

기본적으로 Kaspersky Endpoint Security는 네트워크 플러딩, 포트 검사 및 MAC 스푸핑 공격을 모니터링하지 않습니다.

Microsoft Hyper-V 인프라의 가상 컴퓨터에서는 MAC 스푸핑 보호를 사용하지 않는 것이 좋습니다. Microsoft Hyper-V 플랫폼의 특성에 따라, Kaspersky Industrial CyberSecurity for Nodes가 오탐으로 하이퍼바이저를 차단할 수 있습니다.

관리 콘솔(MMC)에서 유형별로 네트워크 위협 보호를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **필수 위협 보호 → 네트워크 위협 보호**를 선택합니다.

4. 이러한 공격의 탐지를 활성화하거나 비활성화하려면 **포트 검사와 네트워크 플러딩을 공격으로 간주** 확인란을 사용합니다.

   이 기능이 활성화되면 Kaspersky Endpoint Security는 네트워크 트래픽에서 포트 스캐닝 및 네트워크 플러딩을 모니터링합니다. 이러한 행동이 탐지되면 애플리케이션은 사용자에게 위험을 알리고 해당 이벤트를 Kaspersky Security Center로 보냅니다. 애플리케이션은 요청을 전송하는 컴퓨터에 대한 정보를 제공합니다. 이 정보는 적시 대응에 필요합니다. 하지만 이러한 트래픽은 회사 네트워크에서 정상적으로 발생할 수 있으므로 Kaspersky Endpoint Security는 요청을 전송하는 컴퓨터를 차단하지 않습니다.

5. **MAC 스푸핑 보호 모드** 블록에서 다음 옵션 중 하나를 선택합니다:

   - **MAC 스푸핑 공격 추적 안 함**
   - **알림**
   - **차단**.

6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 유형별로 네트워크 위협 보호를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **통신 및 웹 보호** → **네트워크 위협 보호**로 갑니다.

5. 이러한 공격의 탐지를 활성화하거나 비활성화하려면 **포트 검사와 네트워크 플러딩을 공격으로 간주** 확인란을 사용합니다.

   이 기능이 활성화되면 Kaspersky Endpoint Security는 네트워크 트래픽에서 포트 스캐닝 및 네트워크 플러딩을 모니터링합니다. 이러한 행동이 탐지되면 애플리케이션은 사용자에게 위험을 알리고 해당 이벤트를 Kaspersky Security Center로 보냅니다. 애플리케이션은 요청을 전송하는 컴퓨터에 대한 정보를 제공합니다. 이 정보는 적시 대응에 필요합니다. 하지만 이러한 트래픽은 회사 네트워크에서 정상적으로 발생할 수 있으므로 Kaspersky Endpoint Security는 요청을 전송하는 컴퓨터를 차단하지 않습니다.

6. **MAC 스푸핑 보호** 블록에서 다음 옵션 중 하나를 선택합니다:

   - **MAC 스푸핑 보호 활성화됨**
   - **알림**
   - **차단**.

7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 유형별로 네트워크 위협 보호를 구성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 네트워크 위협 보호**를 선택합니다.



네트워크 위협 보호 설정

3. 이러한 공격의 탐지를 활성화하거나 비활성화하려면 **포트 검사와 네트워크 플러딩을 공격으로 간주** 토글을 사용합니다.

   이 기능이 활성화되면 Kaspersky Endpoint Security는 네트워크 트래픽에서 포트 스캐닝 및 네트워크 플러딩을 모니터링합니다. 이러한 행동이 탐지되면 애플리케이션은 사용자에게 위험을 알리고 해당 이벤트를 Kaspersky Security Center로 보냅니다. 애플리케이션은 요청을 전송하는 컴퓨터에 대한 정보를 제공합니다. 이 정보는 적시 대응에 필요합니다. 하지만 이러한 트래픽은 회사 네트워크에서 정상적으로 발생할 수 있으므로 Kaspersky Endpoint Security는 요청을 전송하는 컴퓨터를 차단하지 않습니다.

4. 토글 **MAC 스푸핑 보호**를 사용하여 이러한 공격 탐지를 활성화 또는 비활성화합니다.
5. **MAC 스푸핑 공격 탐지에 대한 조치** 블록에서 다음 옵션 중 하나를 선택합니다:
   - **알림**.
   - **차단**.
6. 변경 사항을 저장합니다.

방화벽

방화벽은 인터넷 또는 로컬 네트워크에서 작업하는 동안 컴퓨터에 대한 무단 연결을 차단합니다. 방화벽은 또한 컴퓨터에서 애플리케이션의 네트워크 활동을 제어합니다. 이를 통해 신원 도용 및 기타 공격으로부터 회사 LAN을 보호할 수 있습니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 사전 정의된 *네트워크 규칙*을 통해 컴퓨터 보호 기능을 제공합니다.

네트워크 에이전트는 Kaspersky Security Center와 상호 작용 시 사용됩니다. 방화벽은 애플리케이션 네트워크 에이전트가 작동하는 데 필요한 네트워크 규칙을 자동으로 생성합니다. 결과적으로 방화벽은 컴퓨터에서 여러 포트를 엽니다. 열리는 포트는 컴퓨터의 역할(예: 배포 지점)에 따라 다릅니다. 컴퓨터에서 열리는 포트에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

네트워크 규칙

다음 레벨로 네트워크 규칙을 구성할 수 있습니다.

- *네트워크 패킷 규칙*. 네트워크 패킷 규칙은 애플리케이션에 관계없이 네트워크 패킷을 제한합니다. 이러한 규칙은 선택한 데이터 프로토콜의 특정 포트를 통과하는 인바운드 및 아웃바운드 트래픽을 제한합니다. Kaspersky Endpoint Security에는 Kaspersky 전문가가 권장하는 권한으로 네트워크 패킷 규칙이 사전 정의되어 있습니다.

- *애플리케이션 네트워크 규칙*. 애플리케이션 네트워크 규칙은 특정 애플리케이션의 네트워크 활동을 제한합니다. 이 규칙은 네트워크 패킷의 특성뿐 아니라 해당 네트워크 패킷의 주소로 지정되거나 네트워크 패킷을 발행한 특정 애플리케이션까지 고려합니다.

호스트 침입 방지 구성 요소는 *애플리케이션 권한*을 사용하여 운영 체제 리소스, 프로세스 및 개인 데이터에 대한 애플리케이션의 접근 제어를 제공합니다.

애플리케이션을 처음 시작할 때 방화벽은 다음 작업을 수행합니다.

1. 다운로드한 안티 바이러스 데이터베이스를 사용하여 애플리케이션의 보안을 확인합니다.

2. Kaspersky Security Network에서 애플리케이션의 보안을 확인합니다.

   Kaspersky Security Network 참가를 활성화 해 방화벽이 보다 효과적으로 작동하도록 도와주십시오.

3. 애플리케이션을 다음 중 하나의 신뢰 그룹에 배치합니다: *신뢰함*, *낮은 제한*, *높은 제한*, *신뢰하지 않음*.

   Kaspersky Endpoint Security가 애플리케이션 동작을 제어할 때 참조하는 권한은 제어 그룹이 정의합니다. Kaspersky Endpoint Security는 애플리케이션이 컴퓨터에 미칠 수 있는 위험 수준에 따라 해당 애플리케이션을 신뢰 그룹에 배치합니다.

   Kaspersky Endpoint Security는 방화벽 및 호스트 침입 방지 구성 요소의 제어 그룹에 애플리케이션을 배치합니다. 방화벽 또는 호스트 침입 방지에 대해서만 제어 그룹을 변경할 수 없습니다.

KSN 참여를 거부하거나 네트워크가 없는 경우 Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 설정에 따라 애플리케이션을 제어 그룹에 배치합니다. KSN으로부터 애플리케이션의 평판을 받은 후 제어 그룹이 자동으로 변경될 수 있습니다.

4. 제어 그룹에 따라 애플리케이션의 네트워크 활동을 차단합니다. 예를 들어 *높은 제한* 제어 그룹의 애플리케이션은 네트워크 연결을 사용할 수 없습니다.

다음 번 애플리케이션을 시작할 때 Kaspersky Endpoint Security가 애플리케이션의 무결성을 확인합니다. 애플리케이션이 변경되지 않은 경우 구성 요소는 현재 네트워크 규칙을 사용합니다. 애플리케이션이 수정되었으면 Kaspersky Endpoint Security가 애플리케이션을 처음으로 시작하는 것처럼 다시 검사합니다.

네트워크 규칙 우선 순위

각 규칙에는 우선 순위가 있습니다. 규칙 목록에서 순위가 높을수록 그 우선 순위도 높습니다. 네트워크 활동이 여러 규칙에 추가되면 방화벽은 우선 순위가 가장 높은 규칙에 따라 네트워크 활동을 통제합니다.

네트워크 패킷 규칙은 애플리케이션 네트워크 규칙보다 우선합니다. 같은 네트워크 활동 유형에 대해 네트워크 패킷 규칙과 애플리케이션 네트워크 규칙이 모두 지정된 경우, 네트워크 패킷 규칙에 따라 네트워크 활동이 처리됩니다.

애플리케이션용 네트워크 규칙은 특정 방식으로 작동합니다. 애플리케이션용 네트워크 규칙에는 네트워크 상태, 즉 *공용 네트워크*, *로컬 네트워크*, *신뢰하는 네트워크*에 따른 접근 규칙이 포함되어 있습니다. 예를 들어 *높은 제한* 제어 그룹의 애플리케이션은 기본적으로 모든 상태의 네트워크에서 네트워크 활동이 허용되지 않습니다. 네트워크 규칙이 개별 애플리케이션(상위 애플리케이션)에 대해 지정되어 있는 경우, 다른 애플리케이션의 하위 프로세스가 상위 애플리케이션의 네트워크 규칙에 따라 실행됩니다. 애플리케이션에 대한 네트워크 규칙이 없으면 자식 프로세스는 애플리케이션 제어 그룹의 네트워크 접근 규칙에 따라 실행됩니다.

예를 들어, 브라우저 X를 제외한 모든 애플리케이션에 대해 모든 상태의 네트워크에서 네트워크 활동을 금지했습니다. 브라우저 X(부모 애플리케이션)에서 브라우저 Y 설치(자식 프로세스)를 시작하면 브라우저 Y 설치 프로그램이 네트워크에 접근하여 필요한 파일을 다운로드합니다. 설치 후 브라우저 Y는 방화벽 설정에 따라 네트워크 연결이 거부됩니다. 자식 프로세스로서 브라우저 Y 설치 프로그램의 네트워크 활동을 금지하려면 브라우저 Y 설치 프로그램에 대한 네트워크 규칙을 추가해야 합니다.

네트워크 연결 유형

방화벽을 사용하면 네트워크 연결 유형에 따라 네트워크 활동을 제어할 수 있습니다. Kaspersky Endpoint Security는 컴퓨터 운영 체제에서 네트워크 연결 유형을 수신합니다. 운영 체제의 네트워크 연결 유형은 사용자가 연결을 설정할 때 설정됩니다. Kaspersky Endpoint Security 설정에서 네트워크 연결 유형을 변경할 수 있습니다. 방화벽은 운영 체제가 아닌 Kaspersky Endpoint Security 설정에 지정된 네트워크 유형에 따라 네트워크 활동을 모니터링합니다.

다음 네트워크 연결 유형을 사용할 수 있습니다.

- **공용 네트워크**. 안티 바이러스 애플리케이션, 방화벽 또는 필터(예: 카페의 Wi-Fi)로 네트워크는 보호되지 않습니다. 방화벽은 이러한 네트워크에 연결된 컴퓨터의 사용자가 이 컴퓨터의 파일 및 프린터에 접근하지 못하게 차단합니다. 외부 사용자도 이 컴퓨터의 데스크톱에 원격 접근하여 공유 폴더의 데이터에 접근할 수 없습니다. 방화벽은 각 애플리케이션에 설정된 네트워크 규칙에 따라 이러한 애플리케이션의 네트워크 활동을 필터링합니다.

  방화벽은 기본적으로 인터넷에 *공용 네트워크* 유형을 할당합니다. 인터넷의 유형은 변경할 수 없습니다.

- **로컬 네트워크**. 이 컴퓨터의 파일 및 프린터에 대한 접근이 제한된 사용자를 위한 네트워크(예: 회사 LAN 또는 홈 네트워크).
- **신뢰하는 네트워크**. 컴퓨터가 공격이나 무단 데이터 접근 시도에 노출되지 않는 안전한 네트워크. 이 상태의 네트워크에서는 모든 네트워크 활동이 허용됩니다.

방화벽 작동 또는 중지

기본적으로 방화벽은 작동되며 최적 모드가 사용됩니다.

관리 콘솔(MMC)에서 방화벽을 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 창에서 **필수 위협 보호 → 방화벽**을 선택합니다.
4. **방화벽** 확인란으로 구성 요소를 사용하거나 중지합니다.
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 방화벽을 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **통신 및 웹 보호 → 방화벽**을 선택합니다.
5. **방화벽** 토글로 구성 요소를 사용하거나 중지합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 방화벽을 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 방화벽**을 선택합니다.
3. **방화벽** 토글로 구성 요소를 사용하거나 중지합니다.
4. 변경 사항을 저장합니다.

따라서 방화벽이 작동할 경우 Kaspersky Endpoint Security가 네트워크 활동을 제어하며 사용자의 컴퓨터에 대한 무단 네트워크 연결을 차단하는 것은 물론 사용자 컴퓨터에 있는 애플리케이션의 무단 네트워크 활동도 차단합니다. 네트워크 위협 보호 구성 요소도 네트워크 활동을 제어합니다. 네트워크 위협 보호 구성 요소(침입 탐지 시스템, IDS라고도 함)는 인바운드 네트워크 트래픽에서 네트워크 공격의 활동 특성을 모니터링합니다.

Kaspersky Endpoint Security는 방화벽 설정과 상관없이 그 리포트에 네트워크 공격 이벤트를 기록합니다. 방화벽이 규칙을 사용해 네트워크 연결을 차단하여 네트워크 공격이 방지되더라도 네트워크 위협 보호 구성 요소가 네트워크 공격 이벤트를 등록합니다. 조직 내 컴퓨터에 대한 네트워크 공격에 관한 통계 정보가 생성되어야 합니다.

네트워크 연결 유형 변경

방화벽은 기본적으로 인터넷에 *공용 네트워크* 유형을 할당합니다. 인터넷의 유형은 변경할 수 없습니다.

네트워크 연결 유형을 변경하려면:

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **방화벽**을 선택합니다.
3. **사용 가능한 네트워크**를 클릭합니다.
4. 유형을 변경하고 싶은 네트워크 연결을 선택합니다.
5. **네트워크 유형** 열에서 네트워크 연결 유형을 선택합니다:
   - **공용 네트워크**. 안티 바이러스 애플리케이션, 방화벽 또는 필터(예: 카페의 Wi-Fi)로 네트워크는 보호되지 않습니다. 방화벽은 이러한 네트워크에 연결된 컴퓨터의 사용자가 이 컴퓨터의 파일 및 프린터에 접근하지 못하게 차단합니다. 외부 사용자도 이 컴퓨터의 데스크톱에 원격 접근하여 공유 폴더의 데이터에 접근할 수 없습니다. 방화벽은 각 애플리케이션에 설정된 네트워크 규칙에 따라 이러한 애플리케이션의 네트워크 활동을 필터링합니다.
   - **로컬 네트워크**. 이 컴퓨터의 파일 및 프린터에 대한 접근이 제한된 사용자를 위한 네트워크(예: 회사 LAN 또는 홈 네트워크).
   - **신뢰하는 네트워크**. 컴퓨터가 공격이나 무단 데이터 접근 시도에 노출되지 않는 안전한 네트워크. 이 상태의 네트워크에서는 모든 네트워크 활동이 허용됩니다.
6. 변경 사항을 저장합니다.

네트워크 패킷 규칙 관리

네트워크 패킷 규칙을 관리할 때 다음 작업도 수행할 수 있습니다:

- 새 네트워크 패킷 규칙 만들기.

  네트워크 패킷 및 데이터 스트림에 적용되는 조건 및 처리 방법 집합을 만들어 새 네트워크 패킷 규칙을 만들 수 있습니다.

- 네트워크 패킷 규칙을 작동하거나 중지합니다.

기본적으로 방화벽에 의해 만들어지는 모든 네트워크 패킷 규칙에는 *사용* 상태가 지정됩니다. 네트워크 패킷 규칙이 작동하면 방화벽이 이 규칙을 적용합니다.

네트워크 패킷 규칙 목록에서 선택한 네트워크 패킷 규칙은 중지시킬 수 있습니다. 네트워크 패킷 규칙이 중지되면 방화벽은 일시적으로 이 규칙을 적용하지 않습니다.

새 사용자 지정 네트워크 패킷 규칙은 *사용* 상태가 기본 적용되어 네트워크 패킷 규칙 목록에 추가됩니다.

- 기존 네트워크 패킷 규칙의 설정을 편집합니다.

  새 네트워크 패킷 규칙을 만든 후에는 항상 설정 편집으로 돌아가 필요에 따라 설정을 수정할 수 있습니다.

- 네트워크 패킷 규칙에 대한 방화벽 동작을 변경합니다.

  특정 네트워크 패킷 규칙과 일치하는 네트워크 활동이 탐지되었을 때 방화벽이 취하는 동작을 네트워크 패킷 규칙 목록에서 편집할 수 있습니다.

- 네트워크 패킷 규칙 우선 순위 변경.

  목록에서 선택된 네트워크 패킷 규칙의 우선 순위를 높이거나 낮출 수 있습니다.

- 네트워크 패킷 규칙 제거.

  네트워크 패킷 규칙을 제거하여 네트워크 활동이 탐지 되었을 때 방화벽이 이 규칙을 적용하지 않도록 하고 *사용 안 함* 상태의 네트워크 패킷 규칙 목록에 이 규칙이 표시되지 않게 할 수 있습니다.

네트워크 패킷 규칙 생성

방화벽은 네트워크 패킷 규칙에 따라 컴퓨터의 모든 네트워크 동작을 필터링합니다. 네트워크 패킷 규칙에는 방화벽이 컴퓨터의 네트워크 연결을 제어하기 위해 적용하는 조건(예: 방향, 프로토콜)이 포함되어 있습니다. 네트워크 패킷 규칙은 규칙과 일치하는 연결을 사용하여 방화벽에서 수행하는 동작(연결 허용 또는 차단)도 지정합니다.

네트워크 패킷 규칙 생성을 위한 권장 사항

IP 주소 또는 IP 주소 범위를 지정하여 네트워크 활동을 필터링할 수 있습니다. DNS 이름을 지정할 수도 있지만 IP 주소와 IP 주소 범위를 사용하는 것을 권장합니다. 네트워크 패킷 이름에 DNS 이름을 사용하면 DNS 서버 소유자가 DNS 기록의 파라미터를 수정할 수 있기 때문에 안전하지 않을 수 있습니다. 또한 악성 행위자는 DNS 메시지를 스푸핑하고 방화벽 규칙을 우회할 수 있습니다.

웹 제어 규칙을 사용하여 DNS 이름으로 네트워크 연결을 제어할 수 있습니다. 방화벽 규칙에 DNS 이름을 지정해야 하는 경우:

- 회사 LAN의 보안을 보장합니다.
- 캐싱 및 권한 있는 DNS 서버의 보안을 보장합니다.
- DNS 기록이 수정되지 않도록 하는 보호가 활성화됩니다.

네트워크 패킷 규칙을 생성할 때 네트워크 패킷 규칙이 애플리케이션 네트워크 규칙보다 우선 순위가 높다는 점을 기억하십시오.

네트워크 패킷 규칙을 생성하는 방법

다음과 같이 네트워크 패킷 규칙을 생성할 수 있습니다:

- 네트워크 모니터 도구를 사용합니다.

  *네트워크 모니터*는 네트워크 활동에 대한 정보를 실시간으로 확인하기 위해 개발된 도구입니다. 모든 규칙 설정을 구성할 필요가 없어 편리합니다. 일부 방화벽 설정은 네트워크 모니터 데이터에서 자동으로 삽입됩니다. 네트워크 모니터는 애플리케이션 인터페이스에서만 사용할 수 있습니다.

- 방화벽 설정을 구성합니다.

  이를 통해 방화벽 설정을 상세 조정할 수 있습니다. 현재 네트워크 활동이 없더라도 모든 네트워크 활동에 대한 규칙을 만들 수 있습니다.

네트워크 모니터 도구를 사용하여 애플리케이션 인터페이스에서 네트워크 패킷 규칙을 만드는 방법

1. 메인 애플리케이션 창의 **모니터링** 섹션에서 **네트워크 모니터** 타일을 클릭합니다.
2. **네트워크 활동** 탭을 선택합니다.

   네트워크 활동 탭에는 컴퓨터의 현재 활성된 네트워크 연결이 모두 나타납니다. 이때, 아웃바운드 및 인바운드 네트워크 연결이 모두 표시됩니다.
3. 네트워크 연결의 마우스 오른쪽 메뉴에서 **네트워크 패킷 규칙 만들기**를 선택합니다.

   네트워크 규칙 속성이 열립니다.
4. 패킷 규칙의 **활성** 상태를 설정합니다.
5. **이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.
6. 네트워크 규칙 설정을 구성합니다(아래 표 참조).

   네트워크 규칙 템플릿 링크를 클릭하여 미리 정의된 규칙 템플릿을 선택할 수 있습니다. 규칙 템플릿은 가장 자주 사용하는 네트워크 연결을 표시합니다.

   모든 네트워크 규칙 설정이 자동으로 입력됩니다.
7. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 기록** 확인란을 선택합니다.
8. **저장**을 클릭합니다.

   새 네트워크 규칙이 목록에 추가됩니다.
9. **위로/아래로** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.
10. 변경 사항을 저장합니다.

방화벽 설정을 사용하여 애플리케이션 인터페이스에서 네트워크 패킷 규칙을 만드는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **방화벽**을 선택합니다.
3. **패킷 규칙**을 클릭합니다.

   방화벽에서 설정한 기본 네트워크 규칙의 목록이 열립니다.

4. **추가** 드롭다운 목록을 사용하여 목록의 규칙 위치를 선택합니다(목록 상단, 목록 하단, 선택한 규칙 옆).

   목록의 규칙 위치에 따라 규칙의 우선순위가 결정됩니다. 목록 상단에 있는 규칙이 가장 높은 우선순위를 가집니다.

5. 패킷 규칙의 **활성** 상태를 설정합니다.

6. **이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.

7. 네트워크 규칙 설정을 구성합니다(아래 표 참조).

   네트워크 규칙 템플릿 링크를 클릭하여 미리 정의된 규칙 템플릿을 선택할 수 있습니다. 규칙 템플릿은 가장 자주 사용하는 네트워크 연결을 표시합니다.

   모든 네트워크 규칙 설정이 자동으로 입력됩니다.

8. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 기록** 확인란을 선택합니다.

9. **저장**을 클릭합니다.

   새 네트워크 규칙이 목록에 추가됩니다.

10. **위로/아래로** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.

11. 변경 사항을 저장합니다.

관리 콘솔(MMC)에서 네트워크 패킷 규칙을 만드는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **필수 위협 보호** → **방화벽**을 선택합니다.

4. **방화벽 설정** 블록에서 **설정** 버튼을 누릅니다.

   그러면 네트워크 패킷 규칙 목록과 애플리케이션 네트워크 규칙 목록이 열립니다.

5. **네트워크 패킷 규칙** 탭으로 이동합니다.

   방화벽에서 설정한 기본 네트워크 규칙의 목록이 열립니다.

6. **추가** 드롭다운 목록을 사용하여 목록의 규칙 위치를 선택합니다(목록 상단, 목록 하단, 선택한 규칙 옆).

   목록의 규칙 위치에 따라 규칙의 우선순위가 결정됩니다. 목록 상단에 있는 규칙이 가장 높은 우선순위를 가집니다.

7. **이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.

8. 네트워크 규칙 설정을 구성합니다(아래 표 참조).

   버튼을 클릭하여 미리 정의된 규칙 템플릿을 선택할 수 있습니다. 규칙 템플릿은 가장 자주 사용하는 네트워크 연결을 표시합니다.

   모든 네트워크 규칙 설정이 자동으로 입력됩니다.

9. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 기록** 확인란을 선택합니다.

10. 새 네트워크 규칙을 저장합니다.

11. **위로/아래로** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.

12. 변경 사항을 저장합니다.

방화벽은 규칙에 따라 네트워크 패킷을 제어합니다. 패킷 규칙을 목록에서 삭제하지 않고 방화벽 작업에서 비활성화할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.

웹 콘솔 및 Cloud Console에서 네트워크 패킷 규칙을 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **통신 및 웹 보호** → **방화벽**을 선택합니다.

5. **네트워크 패킷 규칙** 탭을 선택합니다.
   방화벽에서 설정한 기본 네트워크 규칙의 목록이 열립니다.

6. **추가**를 클릭합니다.
   새 네트워크 규칙 양식이 열립니다.

7. **규칙 이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.

8. 네트워크 규칙 설정을 구성합니다(아래 표 참조).
   규칙 템플릿 선택 링크를 클릭하여 미리 정의된 규칙 템플릿을 선택할 수 있습니다. 규칙 템플릿은 가장 자주 사용하는 네트워크 연결을 표시합니다.
   모든 네트워크 규칙 설정이 자동으로 입력됩니다.

9. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 기록** 확인란을 선택합니다.

10. 네트워크 규칙을 저장합니다.
    새 네트워크 규칙이 목록에 추가됩니다.

11. **이동** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.

12. 변경 사항을 저장합니다.

방화벽은 규칙에 따라 네트워크 패킷을 제어합니다. 패킷 규칙을 목록에서 삭제하지 않고 방화벽 작업에서 비활성화할 수 있습니다. **상태** 열의 토글로 패킷 규칙을 사용하거나 중지합니다.

네트워크 패킷 규칙 설정

파라미터	설명
처리	**허용**. **차단**. **애플리케이션 규칙에 따라 처리**. 이 옵션을 선택하면 방화벽이 네트워크 연결에 애플리케이션 네트워크 규칙을 적용합니다.
프로토콜	선택한 프로토콜(TCP, UDP, ICMP, ICMPv6, IGMP, GRE)을 통해 네트워크 활동을 제어합니다. ICMP 또는 ICMPv6를 프로토콜로 선택하면 ICMP 패킷 유형과 코드를 지정할 수 있습니다: TCP 또는 UDP를 프로토콜 유형으로 선택한 경우 연결을 모니터링할 로컬 및 원격 컴퓨터의 포트 번호를 쉼표로 구분하여 지정할 수 있습니다.

파라미터	설명
방향	**인바운드(패킷)**. 방화벽은 모든 인바운드 네트워크 패킷에 네트워크 규칙을 적용합니다. **인바운드**. 방화벽이 원격 컴퓨터에서 시작된 연결을 통해 전송된 모든 네트워크 패킷에 네트워크 규칙을 적용합니다. **인바운드/아웃바운드**. 방화벽은 모든 인바운드 및 아웃바운드 네트워크 패킷에 네트워크 규칙을 적용합니다. **아웃바운드(패킷)**. 방화벽은 모든 아웃바운드 네트워크 패킷에 네트워크 규칙을 적용합니다. **아웃바운드**. 방화벽이 사용자의 컴퓨터에서 시작된 연결을 통해 전송된 모든 네트워크 패킷에 네트워크 규칙을 적용합니다.
네트워크 어댑터	네트워크 패킷을 송신 및/또는 수신할 수 있는 네트워크 어댑터. 네트워크 어댑터의 설정을 지정함으로써 동일한 IP 주소를 가지고 있는 네트워크 어댑터로 인해 보내거나 또는 받는 네트워크 패킷을 구별할 수 있습니다.
TTL(Time to live)	네트워크 패킷의 수명(Time to Live, TTL)을 기준으로 제어를 제한합니다.
원격 주소	네트워크 패킷을 주고받는 원격 컴퓨터의 네트워크 주소. 방화벽은 원격 네트워크 주소의 지정된 범위에 대해 네트워크 규칙을 적용합니다. 모든 IP 주소를 네트워크 규칙에 포함하거나, 별도의 IP 주소 목록을 만들거나, IP 주소 범위를 지정하거나, 하위 네트워크(신뢰하는 네트워크, 로컬 네트워크, 공용 네트워크)를 선택할 수 있습니다. IP 주소 대신 컴퓨터의 DNS 이름을 지정할 수도 있습니다. LAN 컴퓨터 또는 내부 서비스에 대해서만 DNS 이름을 사용해야 합니다. 클라우드 서비스(Microsoft Azure 등) 및 기타 인터넷 리소스와의 상호 작용은 웹 제어 구성 요소에서 처리해야 합니다. 네트워크 패킷 규칙에서 IP 주소를 확인할 수 없는 DNS 이름을 추가한 경우 Kaspersky Endpoint Security가 경고를 표시합니다. 웹 콘솔의 네트워크 패킷 규칙 목록에 오류 설명을 포함한 열이 추가됩니다. 관리 콘솔(MMC)에서는 오류설명을 사용할 수 없습니다. 이러한 패킷 규칙은 색상으로 강조 표시됩니다.
로컬 주소	네트워크 패킷을 주고받는 컴퓨터의 네트워크 주소. 방화벽은 네트워크 주소의 지정된 범위에 대해 로컬 네트워크 규칙을 적용합니다. 네트워크 규칙에 모든 IP 주소를 포함하거나, 별도의 IP 주소 목록을 만들거나, IP 주소 범위를 지정할 수 있습니다. 원격 주소 목록이 지정된 경우에만 애플리케이션이 로컬 주소를 저장합니다. 즉, **목록의 주소** 값이 **원격 주소**에 대해 선택되어 있고 한 개 이상의 주소가 추가된 경우입니다. 가끔 애플리케이션의 로컬 주소를 불러올 수 없습니다. 이 경우 이 파라미터는 무시됩니다.

네트워크 패킷 규칙 작동 또는 중지

네트워크 패킷 규칙을 작동하거나 중지하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 방화벽**을 선택합니다.
3. **패킷 규칙**을 클릭합니다.
   방화벽에서 설정한 기본 네트워크 패킷 규칙의 목록이 열립니다.
4. 목록에서 원하는 네트워크 패킷 규칙을 선택합니다.
5. **상태** 열의 토글로 규칙을 사용하거나 중지합니다.
6. 변경 사항을 저장합니다.

네트워크 패킷 규칙에 대한 방화벽 동작 변경

네트워크 패킷 규칙에 적용되는 방화벽 동작을 변경하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **방화벽**을 선택합니다.
3. **패킷 규칙**을 클릭합니다.
   방화벽에서 설정한 기본 네트워크 패킷 규칙의 목록이 열립니다.
4. 네트워크 패킷 규칙 목록에서 해당 규칙을 선택하고 **편집** 버튼을 누릅니다.
5. **처리** 드롭다운 목록에서, 이러한 종류의 네트워크 활동을 감지할 경우 방화벽에서 수행할 처리 방법을 선택합니다:
   - **허용**.
   - **차단**.
   - **애플리케이션 규칙에 따라 처리**. 이 옵션을 선택하면 방화벽이 네트워크 연결에 애플리케이션 네트워크 규칙을 적용합니다.
6. 변경 사항을 저장합니다.

네트워크 패킷 규칙의 우선 순위 변경

네트워크 패킷 규칙의 우선 순위는 네트워크 패킷 규칙 목록에서의 위치에 따라 결정됩니다. 즉, 네트워크 패킷 규칙 목록의 맨 위에 위치한 규칙이 우선 순위가 가장 높습니다.

직접 만든 각 네트워크 패킷 규칙은 목록의 끝에 추가되며 가장 낮은 우선순위가 지정됩니다.

방화벽은 네트워크 패킷 규칙 목록에서 위에서 아래로 표시되는 순서에 따라 규칙을 실행합니다. 방화벽은 특정 네트워크 연결에 적용되는 각 네트워크 패킷 규칙의 처리에 따라, 해당 네트워크 연결의 설정에 지정된 주소 및 포트에 대한 네트워크 접근을 허용하거나 차단합니다.

네트워크 패킷 규칙의 우선 순위를 변경하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호** → **방화벽**을 선택합니다.
3. **패킷 규칙**을 클릭합니다.
   방화벽에서 설정한 기본 네트워크 패킷 규칙의 목록이 열립니다.
4. 목록에서 우선 순위를 변경할 네트워크 패킷 규칙을 선택합니다.
5. **위로/아래로** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.
6. 변경 사항을 저장합니다.

네트워크 패킷 규칙 내보내기 및 가져오기

네트워크 패킷 규칙 목록을 XML 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 동일 유형의 규칙을 여러 개 추가하는 등의 작업을 진행할 수 있습니다. 내보내기/가져오기 기능을 사용하여 네트워크 패킷 규칙 목록을 백업하거나 목록을 다른 서버로 마이그레이션할 수 있습니다.

관리 콘솔(MMC)에서 네트워크 패킷 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 창에서 **필수 위협 보호 → 방화벽**을 선택합니다.
4. **방화벽 설정** 블록에서 **설정** 버튼을 누릅니다.
   그러면 네트워크 패킷 규칙 목록과 애플리케이션 네트워크 규칙 목록이 열립니다.
5. **네트워크 패킷 규칙** 탭으로 이동합니다.
6. 네트워크 패킷 규칙 목록을 내보내려면 다음을 수행합니다.
   a. 내보낼 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
      규칙을 선택하지 않으면 Kaspersky Endpoint Security는 모든 규칙을 내 보냅니다.
   b. **내보내기** 링크를 클릭합니다.
   c. 창이 열리면 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   d. 파일을 저장합니다.
      Kaspersky Endpoint Security는 신뢰하는 규칙 목록을 XML 파일로 내보냅니다.
7. 네트워크 패킷 규칙 목록을 가져오려면 다음을 수행합니다.
   a. **가져오기** 링크를 클릭합니다.
      창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.
   b. 파일을 엽니다.
      컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.
8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 네트워크 패킷 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.

4. **통신 및 웹 보호** → **방화벽**을 선택합니다.

5. 규칙 목록을 내보내려면 **네트워크 패킷 규칙** 블록에서:

   a. 내보낼 규칙을 선택합니다.

   b. → **내보내기** 버튼을 클릭합니다.

   Kaspersky Endpoint Security는 규칙 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.

6. 규칙 목록을 가져오려면 **네트워크 패킷 규칙** 블록에서:

   a. → **가져오기** 버튼을 클릭합니다.

   창이 열리면 규칙 목록을 가져올 JSON 파일을 선택합니다.

   b. 파일을 엽니다.

   컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 변경 사항을 저장합니다.

XML에서 네트워크 패킷 규칙 정의

XML 형식에서 방화벽이 네트워크 패킷 내보내기를 허용합니다. 그 후 파일을 수정하여 동일 유형의 규칙을 여러 개 추가하는 등의 작업을 진행할 수 있습니다.

XML 파일에는 `Rules`과 `Resources`라는 두 개의 기본 노드가 포함되어 있습니다. `Rules` 노드는 네트워크 패킷 규칙을 나열합니다. 이 노드에는 기본 구성 규칙(*사전 정의된 규칙*)과 사용자가 추가한 규칙(*사용자 지정 규칙*)이 포함됩니다.

네트워크 패킷 규칙 마크업

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

파라미터	설명	값
`<key name="0000">`	규칙의 우선순위입니다. 값이 낮을수록 우선순위가 높습니다.	정수 우선순위 값은 4자리 수로 구성되어야 합니다. XML 파일의 노드는 `0000`으로 시작하는 우선순위 값에 따라 정렬되어야 합니다.
`RuleId`	규칙의 ID입니다.	**사전 정의된 규칙** `100` – **TCP를 통해 DNS 서버에 요청** `101` – **UDP를 통해 DNS 서버에 요청** `102` – **이메일 메시지 보내기** `110` – **모든 네트워크 활동**(신뢰하는 네트워크) `125` – **모든 네트워크 활동**(로컬 네트워크) `130` – **Remote Desktop 네트워크 활동** `131` – **로컬 포트를 통한 TCP 연결** `132` – **로컬 포트를 통한 UDP 연결** `133` – **받는 TCP 스트림** `134` – **받는 UDP 스트림** `137` – **ICMP Destination Unreachable - 받는 응답** `138` – **ICMP Echo Reply - 받는 패킷** `140` – **ICMP Time Exceeded - 받는 응답** `142` – **받는 ICMP 스트림** `266` – **ICMPv6 Echo Request - 받는 패킷**
`RuleState`	규칙의 상태입니다.	`0` – 사전 정의된 규칙이 비활성화됩니다 `1` – 사전 정의된 규칙이 활성화됩니다 `2` – 사용자 지정 규칙이 비활성화됩니다 `3` – 사용자 지정 규칙이 활성화됩니다
`RuleTypeId`	규칙 유형의 ID입니다.	`4` – 네트워크 패킷 규칙
`AppIdEx`	네트워크 패킷 규칙이 속한 애플리케이션 ID입니다.	규칙이 애플리케이션에 속하지 않은 경우 값은 `0`입니다.
`ResIdEx`	규칙 설정이 있는 리소스의 메인 ID입니다. 이 식별자를 사용해 `Resources` 노드에서 규칙 설정이 있는 블록의 위치를 찾을 수 있습니다.	정수
`ResIdEx2`	네트워크 유형의 ID입니다.	`0` – **모든 주소** `50` – **신뢰하는 네트워크** `51` – **로컬 네트워크** `52` – **공용 네트워크** `<Network Identifier>` – **목록의 주소**(주소는 수동으로 정의됩니다).
`AccessFlag`	**처리** 파라미터의 값입니다.	`0` – **허용** `2` **애플리케이션 규칙에 따라 처리** `3` – **차단** `4` – **허용** 및 **이벤트 기록** `6` – **애플리케이션 규칙에 따라 처리** 및 **이벤트 기록** `7` – **차단** 및 **이벤트 기록**
`</key>`		

`Resources` 노드에는 네트워크 패킷 규칙 설정이 포함됩니다. 사용자 지정 네트워크 패킷 규칙 설정은 `<key name="0004">` 블록에 나열됩니다.

커스텀 네트워크 패킷 규칙 마크업

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

사용자 지정 네트워크 패킷 규칙 설정

파라미터	설명	값
`<key name="Data">`	파라미터 블록의 ID입니다.	정수
RemotePorts	**원격 포트** 파라미터의 값입니다.	원격 포트 범위의 목록입니다.
LocalPorts	**로컬 포트** 파라미터의 값입니다.	로컬 포트 범위의 목록입니다.

파라미터	설명	값
`AdapterBindings`	**네트워크 어댑터** 파라미터의 값입니다.	`IpAddresses` – **IP 주소** 파라미터의 값입니다. `MacAddresses` – **MAC 주소** 파라미터의 값입니다. `AdapterName` – 네트워크 어댑터의 이름입니다. `InterfaceType` – **인터페이스 유형** 파라미터의 값입니다: • `0` – **기타** • `1` – **루프백** • `2` – **유선 네트워크(이더넷)** • `3` – **무선 네트워크(Wi-Fi)** • `4` – **터널** • `5` – **PPP 연결** • `6` – **PPPoE 연결** • `7` – **VPN 연결** • `8` – **모뎀 연결**
`unique`	구조의 내부 ID입니다.	정수 이 파라미터는 그대로 두는 것이 좋습니다.
`Proto`	**프로토콜** 파라미터의 값입니다.	`0` – 비활성화됨 `1` – **ICMP** `2` – **IGMP** `6` – **TCP** `17` – **UDP** `47` – **GRE** `58` – **ICMPv6**
`Direction`	**방향** 파라미터의 값입니다.	`1` – **인바운드(패킷)** `2` – **아웃바운드(패킷)** `3` – **인바운드/아웃바운드** `4` – **인바운드** `5` – **아웃바운드**

파라미터	설명	값
`IcmpType`	**ICMP 유형** 파라미터의 값입니다.	**ICMP 프로토콜** `0` – **에코 응답**(ICMP) 또는 비활성화됨 `3` – **대상에 연결할 수 없음**(ICMP) `4` – **원본 억제** `5` – **리디렉션** `6` – **Alternate Host Address** `8` – **에코 요청** `9` – **라우터 알림** `10` – **라우터 요청** `11` – **시간 초과** `12` – **매개 변수 문제** `13` – **타임스탬프** `14` – **타임스탬프 응답** `15` – **정보 요청** `16` – **정보 응답** `17` – **주소 마스크 요청** `18` – **주소 마스크 응답** `30` – **경로 추적** `31` – **Datagram Conversion Error** `32` – **Mobile Host Redirect** `33` – **IPv6 WAY(Where-Are-You)** `34` – **IPv6 IAH(I-Am-Here)** `35` – **Mobile Registration Request** `36` – **Mobile Registration Reply** `37` – **도메인 이름 요청** `38` – **도메인 이름 응답** `40` – **Photuris** **ICMPv6 프로토콜** `1` – **대상에 연결할 수 없음** `2` – **패킷이 너무 큼** `3` – **시간 초과** `4` – **매개 변수 문제** `128` – **에코 요청** `129` – **에코 응답** `130` – **멀티캐스트 수신기 쿼리** `131` – **멀티캐스트 수신기 리포트** `132` – **멀티캐스트 수신기 완료** `133` – **라우터 요청** `134` – **라우터 알림** `135` – **인접 항목 요청** `136` – **인접 항목 알림** `137` – **리다이렉트 메시지** `138` – **라우터 번호 재지정** `139` – **ICMP 노드 정보 쿼리** `141` – **역방향 인접 항목 탐색 요청 메시지** `142` – **역방향 인접 항목 탐색 알림 메시지** `143` – **버전 2 멀티캐스트 수신기 리포트**

파라미터	설명	값
		144 – **홈 에이전트 주소 탐색 요청 메시지** 145 – **홈 에이전트 주소 탐색 응답 메시지** 146 – **모바일 접두사 요청** 147 – **모바일 접두사 알림** 148 – **인증 경로 요청 메시지** 149 – **인증 경로 알림 메시지** 151 – **멀티캐스트 라우터 알림** 152 – **멀티캐스트 라우터 요청** 153 – **멀티캐스트 라우터 종료**
`IcmpCode`	**ICMP 코드** 파라미터의 값입니다.	`0` – **코드 0** 또는 비활성화 `1` – **코드 1** `2` – **코드 2**
`Flags`	구조 속성 포인터입니다.	정수 이 파라미터는 그대로 두는 것이 좋습니다.
`TTL`	**TTL(Time to live)** 파라미터의 값입니다.	값의 단위는 초입니다. 비활성화되면 값은 `0`입니다.
`</key>`		
`Id`	리소스의 메인 ID입니다(`Rules` 노드 참조).	정수
`ParentID`	상위 그룹의 ID입니다.	정수 이 파라미터는 그대로 두는 것이 좋습니다.
`Flags`	규칙의 상태입니다.	`6` – 규칙이 비활성화됩니다. `38` – 규칙이 활성화됩니다.
`Name`	네트워크 패킷 규칙의 이름입니다.	문자열

애플리케이션 네트워크 규칙 관리

기본적으로 Kaspersky Endpoint Security는 파일이나 네트워크를 감시하는 해당 소프트웨어의 공급업체 이름을 기준으로 컴퓨터에 설치된 모든 애플리케이션을 그룹화 합니다. 그런 다음 애플리케이션 그룹은 제어 그룹으로 분류됩니다. 모든 애플리케이션 및 애플리케이션 그룹은 그 상위 그룹에서 속성이 상속됩니다: 애플리케이션 제어 규칙, 애플리케이션 네트워크 규칙 및 그 실행 우선 순위.

호스트 침입 방지 구성 요소와 마찬가지로 기본 값으로 방화벽 구성 요소는 그룹 내의 모든 애플리케이션의 네트워크 활동을 필터링할 때 애플리케이션 그룹에 대해 네트워크 규칙을 적용합니다. 애플리케이션 그룹 네트워크 규칙은 그룹 내의 애플리케이션이 다른 네트워크 연결에 접근할 수 있는 권한을 정의합니다.

기본적으로 방화벽은 컴퓨터에서 Kaspersky Endpoint Security에 의해 탐지된 각 애플리케이션 그룹에 대해 네트워크 규칙 집합을 만듭니다. 기본 생성된 애플리케이션 그룹 네트워크 규칙에 적용되는 방화벽 동작은 변경이 가능합니다. 기본 애플리케이션 그룹 네트워크 규칙의 우선 순위는 편집하거나 제거, 중지 또는 변경할 수 없습니다.

개별 애플리케이션에 대해 네트워크 규칙을 만들 수도 있습니다. 그러한 규칙은 그 애플리케이션이 속한 그룹의 네트워크 규칙보다 우선합니다.

애플리케이션 네트워크 규칙 만들기

기본적으로 애플리케이션 동작은 Kaspersky Endpoint Security가 처음 실행 시 애플리케이션을 할당한 제어 그룹에 대해 정의된 네트워크 규칙에 따라 제어됩니다. 필요할 경우 전체 제어 그룹, 개별 애플리케이션 또는 제어 그룹에 속한 애플리케이션 그룹에 대해 네트워크 규칙을 생성할 수 있습니다.

직접 정의한 네트워크 규칙은 제어 그룹을 대상으로 결정된 네트워크 규칙보다 우선순위가 높습니다. 즉, 직접 정의한 애플리케이션 규칙이 제어 그룹을 대상으로 결정된 애플리케이션 규칙과 다른 경우 방화벽은 직접 정의한 애플리케이션 규칙에 따라 애플리케이션 활동을 제어합니다.

기본적으로 방화벽은 각 애플리케이션에 대해 다음 네트워크 규칙을 만듭니다:

- 신뢰하는 네트워크의 모든 네트워크 활동.
- 로컬 네트워크의 모든 네트워크 활동.
- 공용 네트워크의 모든 네트워크 활동.

Kaspersky Endpoint Security는 다음과 같이 사전 정의한 네트워크 규칙에 따라 애플리케이션의 네트워크 활동을 제어합니다:

- 신뢰 및 낮은 제한: 모든 네트워크 활동을 허용합니다.
- 높은 제한 및 신뢰하지 않음: 모든 네트워크 활동을 차단합니다.

사전 정의한 애플리케이션 규칙은 편집하거나 삭제할 수 없습니다.

다음과 같은 방법으로 애플리케이션 네트워크 규칙을 만들 수 있습니다:

- 네트워크 모니터 도구를 사용합니다.

  *네트워크 모니터*는 네트워크 활동에 대한 정보를 실시간으로 확인하기 위해 개발된 도구입니다. 모든 규칙 설정을 구성할 필요가 없어 편리합니다. 일부 방화벽 설정은 네트워크 모니터 데이터에서 자동으로 삽입됩니다. 네트워크 모니터는 애플리케이션 인터페이스에서만 사용할 수 있습니다.

- 방화벽 설정을 구성합니다.

  이를 통해 방화벽 설정을 상세 조정할 수 있습니다. 현재 네트워크 활동이 없더라도 모든 네트워크 활동에 대한 규칙을 만들 수 있습니다.

애플리케이션에 대한 네트워크 규칙을 만들 때 네트워크 패킷 규칙을 애플리케이션 네트워크 규칙보다 우선합니다.

네트워크 모니터 도구를 사용하여 애플리케이션 인터페이스에서 애플리케이션 네트워크 규칙을 만드는 방법

1. 메인 애플리케이션 창의 **모니터링** 섹션에서 **네트워크 모니터** 타일을 클릭합니다.
2. **네트워크 활동** 또는 **열린 포트** 탭으로 이동합니다.

네트워크 활동 탭에는 컴퓨터의 현재 활성된 네트워크 연결이 모두 나타납니다. 이때, 아웃바운드 및 인바운드 네트워크 연결이 모두 표시됩니다.

열린 포트 탭에는 컴퓨터의 열린 네트워크 포트가 모두 나열됩니다.

3. 네트워크 연결의 마우스 오른쪽 메뉴에서 **애플리케이션 네트워크 규칙을 생성합니다** 선택합니다.
   애플리케이션 규칙 및 속성 창이 열립니다.
4. **네트워크 규칙** 탭을 선택합니다.
   방화벽에서 설정한 기본 네트워크 규칙의 목록이 열립니다.
5. **추가**를 클릭합니다.
   네트워크 규칙 속성이 열립니다.
6. **이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.
7. 네트워크 규칙 설정을 구성합니다(아래 표 참조).
   네트워크 규칙 템플릿 링크를 클릭하여 미리 정의된 규칙 템플릿을 선택할 수 있습니다. 규칙 템플릿은 가장 자주 사용하는 네트워크 연결을 표시합니다.
   모든 네트워크 규칙 설정이 자동으로 입력됩니다.
8. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 기록** 확인란을 선택합니다.
9. **저장**을 클릭합니다.
   새 네트워크 규칙이 목록에 추가됩니다.
10. **위로/아래로** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.
11. 변경 사항을 저장합니다.

방화벽 설정을 사용하여 애플리케이션 인터페이스에서 애플리케이션 네트워크 규칙을 만드는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 방화벽**을 선택합니다.
3. **애플리케이션 규칙**을 선택합니다.
   방화벽에서 설정한 기본 네트워크 규칙의 목록이 열립니다.
4. 애플리케이션 목록에서 네트워크 규칙을 만들 애플리케이션 또는 애플리케이션 그룹을 선택합니다.
5. 마우스 오른쪽 메뉴를 열어 **상세 정보 및 규칙**을 선택합니다.
   애플리케이션 규칙 및 속성 창이 열립니다.
6. **네트워크 규칙** 탭을 선택합니다.
7. **추가**를 클릭합니다.
   네트워크 규칙 속성이 열립니다.
8. **이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.
9. 네트워크 규칙 설정을 구성합니다(아래 표 참조).

네트워크 규칙 템플릿 링크를 클릭하여 미리 정의된 규칙 템플릿을 선택할 수 있습니다. 규칙 템플릿은 가장 자주 사용하는 네트워크 연결을 표시합니다.

모든 네트워크 규칙 설정이 자동으로 입력됩니다.

10. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 기록** 확인란을 선택합니다.

11. **저장**을 클릭합니다.

    새 네트워크 규칙이 목록에 추가됩니다.

12. **위로/아래로** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.

13. 변경 사항을 저장합니다.

관리 콘솔(MMC)에서 애플리케이션 네트워크 규칙을 만드는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **필수 위협 보호** → **방화벽**을 선택합니다.

4. **방화벽 설정** 블록에서 **설정** 버튼을 누릅니다.

   그러면 네트워크 패킷 규칙 목록과 애플리케이션 네트워크 규칙 목록이 열립니다.

5. **애플리케이션 네트워크 규칙** 탭으로 이동합니다.

6. **추가**를 클릭합니다.

7. 창이 열리면 네트워크 규칙을 만들 애플리케이션에 대한 검색 기준을 입력합니다.

   애플리케이션 이름 또는 공급업체 이름을 입력할 수 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 * 및 ? 문자를 지원합니다.

8. **새로 고침**을 클릭합니다.

   Kaspersky Endpoint Security는 관리 컴퓨터에 설치된 애플리케이션 통합 목록에서 애플리케이션을 검색합니다. Kaspersky Endpoint Security는 검색 기준을 충족하는 애플리케이션 목록을 표시합니다.

9. 필요한 애플리케이션을 선택합니다.

10. **선택한 애플리케이션을 제어 그룹에 추가** 드롭다운 목록에서 **초기 상태 그룹**을 선택하고 **확인**을 클릭합니다.

    애플리케이션이 기본 그룹에 추가됩니다.

11. 관련 애플리케이션을 선택한 다음 애플리케이션의 마우스 오른쪽 메뉴에서 **애플리케이션 권한**을 선택합니다.

    애플리케이션 규칙 및 속성 창이 열립니다.

12. **네트워크 규칙** 탭을 선택합니다.

    방화벽에서 설정한 기본 네트워크 규칙의 목록이 열립니다.

13. **추가**를 클릭합니다.

    네트워크 규칙 속성이 열립니다.

14. **이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.

15. 네트워크 규칙 설정을 구성합니다(아래 표 참조).

버튼을 클릭하여 미리 정의된 규칙 템플릿을 선택할 수 있습니다. 규칙 템플릿은 가장 자주 사용하는 네트워크 연결을 표시합니다.

모든 네트워크 규칙 설정이 자동으로 입력됩니다.

16. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 기록** 확인란을 선택합니다.

17. 새 네트워크 규칙을 저장합니다.

18. **위로/아래로** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.

19. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 애플리케이션 네트워크 규칙을 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **통신 및 웹 보호** → **방화벽**을 선택합니다.

5. **애플리케이션 권한 및 보호 중인 리소스** 블록에서 **애플리케이션 권한** 링크를 클릭합니다.

   그러면 애플리케이션 권한 구성 창과 보호 중인 리소스 목록이 열립니다.

6. **애플리케이션 권한** 탭으로 이동합니다.

   창의 왼쪽에는 제어 그룹 목록이, 오른쪽에는 해당 속성이 표시됩니다.

7. **애플리케이션** 블록에서 **추가** 버튼을 누릅니다.

   제어 그룹에 애플리케이션을 추가하기 위한 마법사가 시작됩니다.

8. 애플리케이션에 해당하는 제어 그룹을 선택합니다.

9. **애플리케이션** 유형을 선택합니다. 다음 단계로 넘어갑니다.

   여러 애플리케이션에 대한 네트워크 규칙을 만들려면 **그룹** 유형을 선택하고 애플리케이션 그룹의 이름을 정의합니다.

10. 애플리케이션 목록이 열리면 네트워크 규칙을 만들 애플리케이션을 선택합니다.

    필터를 사용합니다. 애플리케이션 이름 또는 공급업체 이름을 입력할 수 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 * 및 ? 문자를 지원합니다.

11. 마법사를 끝냅니다.

    애플리케이션이 제어 그룹에 추가됩니다.

12. 창 왼쪽에서 관련 애플리케이션을 선택합니다.

13. 창 오른쪽의 드롭다운 목록에서 **네트워크 규칙**을 선택합니다.

    방화벽에서 설정한 기본 네트워크 규칙의 목록이 열립니다.

14. **추가**를 클릭합니다.

    애플리케이션 규칙 속성이 열립니다.

15. **규칙 이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.

16. 네트워크 규칙 설정을 구성합니다(아래 표 참조).

    규칙 템플릿 선택 링크를 클릭하여 미리 정의된 규칙 템플릿을 선택할 수 있습니다. 규칙 템플릿은 가장 자주 사용하는 네트워크 연결을 표시합니다.

    모든 네트워크 규칙 설정이 자동으로 입력됩니다.

17. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 기록** 확인란을 선택합니다.

18. 네트워크 규칙을 저장합니다.

    새 네트워크 규칙이 목록에 추가됩니다.

19. **이동** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.

20. 변경 사항을 저장합니다.

애플리케이션 네트워크 규칙 설정

파라미터	설명
처리	**허용**. **차단**.
프로토콜	선택한 프로토콜(TCP, UDP, ICMP, ICMPv6, IGMP, GRE)을 통해 네트워크 활동을 제어합니다. ICMP 또는 ICMPv6를 프로토콜로 선택하면 ICMP 패킷 유형과 코드를 지정할 수 있습니다: TCP 또는 UDP를 프로토콜 유형으로 선택한 경우 연결을 모니터링할 로컬 및 원격 컴퓨터의 포트 번호를 쉼표로 구분하여 지정할 수 있습니다.
방향	**인바운드**. **인바운드/아웃바운드**. **아웃바운드**.
원격 주소	네트워크 패킷을 주고받는 원격 컴퓨터의 네트워크 주소. 방화벽은 원격 네트워크 주소의 지정된 범위에 대해 네트워크 규칙을 적용합니다. 모든 IP 주소를 네트워크 규칙에 포함하거나, 별도의 IP 주소 목록을 만들거나, IP 주소 범위를 지정하거나, 하위 네트워크(신뢰하는 네트워크, 로컬 네트워크, 공용 네트워크)를 선택할 수 있습니다. IP 주소 대신 컴퓨터의 DNS 이름을 지정할 수도 있습니다. LAN 컴퓨터 또는 내부 서비스에 대해서만 DNS 이름을 사용해야 합니다. 클라우드 서비스(Microsoft Azure 등) 및 기타 인터넷 리소스와의 상호 작용은 웹 제어 구성 요소에서 처리해야 합니다. 네트워크 패킷 규칙에서 IP 주소를 확인할 수 없는 DNS 이름을 추가한 경우 Kaspersky Endpoint Security가 경고를 표시합니다. 웹 콘솔의 네트워크 패킷 규칙 목록에 오류 설명을 포함한 열이 추가됩니다. 관리 콘솔(MMC)에서는 오류설명을 사용할 수 없습니다. 이러한 패킷 규칙은 색상으로 강조 표시됩니다.
로컬 주소	네트워크 패킷을 주고받는 컴퓨터의 네트워크 주소. 방화벽은 네트워크 주소의 지정된 범위에 대해 로컬 네트워크 규칙을 적용합니다. 네트워크 규칙에 모든 IP 주소를 포함하거나, 별도의 IP 주소 목록을 만들거나, IP 주소 범위를 지정할 수 있습니다. 원격 주소 목록이 지정된 경우에만 애플리케이션이 로컬 주소를 저장합니다. 즉, **목록의 주소** 값이 **원격 주소**에 대해 선택되어 있고 한 개 이상의 주소가 추가된 경우입니다. 가끔 애플리케이션의 로컬 주소를 불러올 수 없습니다. 이 경우 이 파라미터는 무시됩니다.

애플리케이션 네트워크 규칙 사용 및 중지

애플리케이션 네트워크 규칙을 작동 또는 중지시키려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **필수 위협 보호** → **방화벽**을 선택합니다.

3. **애플리케이션 규칙**을 선택합니다.
   애플리케이션 규칙 목록이 열립니다.

4. 애플리케이션 목록에서 네트워크 규칙을 만들거나 편집할 애플리케이션 또는 애플리케이션 그룹을 선택합니다.

5. 마우스 오른쪽 메뉴를 열어 **상세 정보 및 규칙**을 선택합니다.
   애플리케이션 규칙 및 속성 창이 열립니다.

6. **네트워크 규칙** 탭을 선택합니다.

7. 애플리케이션 그룹에 대한 네트워크 규칙 목록에서 관련 네트워크 규칙을 선택합니다.
   네트워크 규칙 속성 창이 열립니다.

8. 네트워크 규칙의 **활성** 또는 **비활성** 상태를 설정합니다.
   방화벽에 의해 기본적으로 만들어지는 애플리케이션 그룹 네트워크 규칙은 중지시킬 수 없습니다.

9. 변경 사항을 저장합니다.

애플리케이션 네트워크 규칙에 대한 방화벽 동작 변경

애플리케이션 또는 애플리케이션 그룹에 대해 기본적으로 만들어지는 네트워크 규칙에 적용되는 방화벽 동작은 물론 하나의 애플리케이션 또는 애플리케이션 그룹에 대한 사용자 지정 네트워크 규칙 방화벽 동작도 변경할 수 있습니다.

애플리케이션 또는 애플리케이션 그룹에 대한 모든 네트워크 규칙의 방화벽 동작을 변경하려면 다음을 수행합니다:

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **필수 위협 보호** → **방화벽**을 선택합니다.

3. **애플리케이션 규칙**을 선택합니다.
   애플리케이션 규칙 목록이 열립니다.

4. 기본 생성된 모든 네트워크 규칙에 적용되는 방화벽 동작을 변경하려면 목록에서 애플리케이션 또는 애플리케이션 그룹을 선택합니다. 직접 생성된 네트워크 규칙은 변경되지 않습니다.

5. 마우스 오른쪽 메뉴를 열고 **네트워크 규칙**을 선택한 후 할당할 작업을 선택합니다:

   - **상속**.
   - **허용**.
   - **차단**.

6. 변경 사항을 저장합니다.

애플리케이션 또는 애플리케이션 그룹의 네트워크 규칙에 대한 방화벽 동작을 수정하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 방화벽**을 선택합니다.
3. **애플리케이션 규칙**을 선택합니다.
   애플리케이션 규칙 목록이 열립니다.
4. 목록에서 네트워크 규칙 한 개에 적용되는 동작을 변경할 애플리케이션 또는 애플리케이션 그룹을 선택합니다.
5. 마우스 오른쪽 메뉴를 열어 **상세 정보 및 규칙**을 선택합니다.
   애플리케이션 규칙 및 속성 창이 열립니다.
6. **네트워크 규칙** 탭을 선택합니다.
7. 방화벽 동작을 변경할 네트워크 규칙을 선택합니다.
8. **권한** 열에서 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 열고 할당할 동작을 선택합니다:
   - **상속**.
   - **허용**.
   - **거부**.
   - **이벤트 기록**.
9. 변경 사항을 저장합니다.

애플리케이션 네트워크 규칙의 우선 순위 변경

네트워크 규칙의 우선 순위는 네트워크 규칙 목록에서의 위치로 결정됩니다. 방화벽은 네트워크 규칙 목록에서 위에서 아래로 표시되는 순서에 따라 규칙을 실행합니다. 방화벽은 특정 네트워크 연결에 적용되는 각 네트워크 규칙의 처리에 따라, 해당 네트워크 연결의 설정에 표시된 주소 및 포트에 대한 네트워크 접근을 허용하거나 차단합니다.

직접 만든 네트워크 규칙은 기본 네트워크 규칙보다 우선합니다.

기본 애플리케이션 그룹 네트워크 규칙의 우선 순위는 변경할 수 없습니다.

네트워크 규칙의 우선 순위를 변경하려면 다음을 수행합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **필수 위협 보호 → 방화벽**을 선택합니다.
3. **애플리케이션 규칙**을 선택합니다.
   애플리케이션 규칙 목록이 열립니다.

4. 애플리케이션 목록에서 네트워크 규칙의 우선 순위를 변경할 애플리케이션 또는 애플리케이션 그룹을 선택합니다.

5. 마우스 오른쪽 메뉴를 열어 **상세 정보 및 규칙**을 선택합니다.
   애플리케이션 규칙 및 속성 창이 열립니다.

6. **네트워크 규칙** 탭을 선택합니다.

7. 우선 순위를 변경할 네트워크 규칙을 선택합니다.

8. **위로/아래로** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.

9. 변경 사항을 저장합니다.

네트워크 모니터

*네트워크 모니터*는 네트워크 활동에 대한 정보를 실시간으로 확인하기 위해 개발된 도구입니다.

네트워크 모니터를 시작하려면 다음과 같이 하십시오.

메인 애플리케이션 창의 **모니터링** 섹션에서 **네트워크 모니터** 타일을 클릭합니다.

네트워크 모니터 창이 열립니다. 이 창에는 컴퓨터의 네트워크 활동에 대한 정보가 다음 4가지 탭에 표시됩니다:

- **네트워크 활동** 탭에는 컴퓨터의 현재 활성된 네트워크 연결이 모두 나타납니다. 이때, 아웃바운드 및 인바운드 네트워크 연결이 모두 표시됩니다. 이 탭에서 방화벽 작동에 대한 네트워크 패킷 규칙을 생성할 수도 있습니다.
- **열린 포트** 탭에는 컴퓨터의 열린 네트워크 포트가 모두 나열됩니다. 이 탭에서 방화벽 작동에 대한 네트워크 패킷 규칙 및 애플리케이션 규칙을 생성할 수도 있습니다.
- **네트워크 트래픽** 탭에는 사용자 컴퓨터와 현재 사용자가 연결된 네트워크에 있는 다른 컴퓨터 사이의 인바운드 및 아웃바운드 네트워크 트래픽 양이 표시됩니다.
- **차단된 컴퓨터** 탭에는 해당 IP 주소에서 네트워크 공격을 시도한 것으로 탐지되어 네트워크 위협 보호 구성 요소에 의해 네트워크 활동이 차단된 원격 컴퓨터의 IP 주소가 표시됩니다.

익스플로잇 방지

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 Endpoint Security가 해당 파일의 실행을 차단하거나 해당 사용자에게 알립니다.

익스플로잇 방지 구성 요소는 네트워크 포트에서 컴퓨터의 보안을 위협할 수 있는 애플리케이션 프로세스를 추가로 모니터링합니다. 애플리케이션은 안티 바이러스 데이터베이스를 사용하여 이러한 프로세스에 대한 정보를 가져옵니다.

익스플로잇 방지 사용 및 중지

기본적으로 익스플로잇 방지가 작동되며 최적 모드가 사용됩니다. Kaspersky Endpoint Security는 취약한 애플리케이션이 실행 중인 실행 파일을 모니터링합니다. Kaspersky Endpoint Security가 취약한 애플리케이션의 실행 파일이 사용자 이외의 주체에 의해 실행된 것을 탐지하면 Kaspersky Endpoint Security는 작업 차단 등 선택된 동작을 수행합니다.

관리 콘솔(MMC)에서 익스플로잇 방지를 활성화 또는 비활성화하는 방법

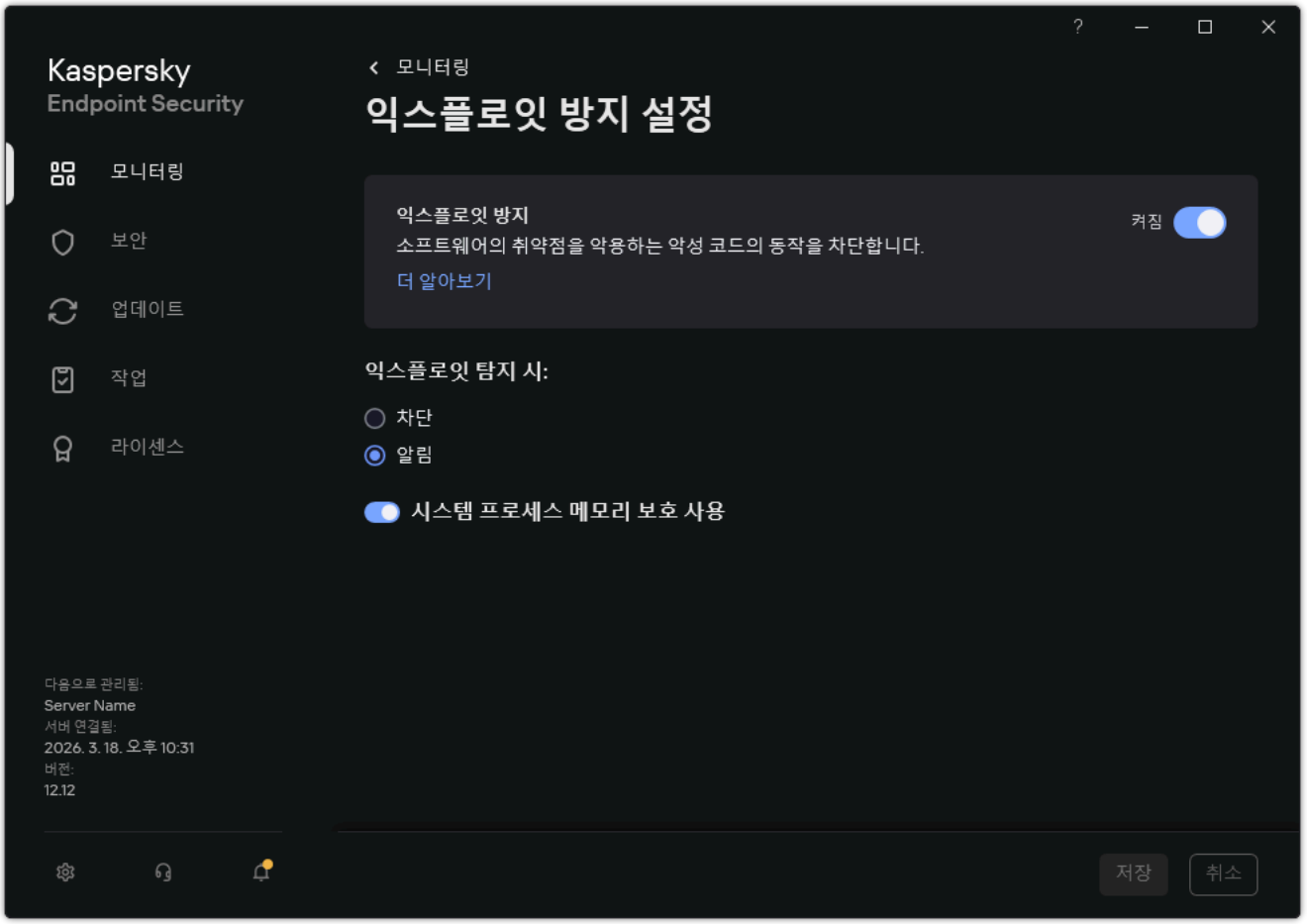
1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **지능형 위협 보호 → 익스플로잇 방지**를 선택합니다.
4. **익스플로잇 방지** 확인란으로 구성 요소를 사용하거나 중지합니다.
5. **익스플로잇 탐지 시** 블록에서 필요한 동작을 선택합니다:
   - **차단**. 이 항목을 선택하면 익스플로잇 탐지 시 Kaspersky Endpoint Security가 이 익스플로잇의 동작을 차단하고 이 익스플로잇에 관한 정보가 포함된 로그 항목을 만듭니다.
   - **알림**. 이 항목을 선택하면 Kaspersky Endpoint Security가 익스플로잇 탐지 시 이 익스플로잇에 관한 정보가 포함된 로그 항목을 만들고 이 익스플로잇에 관한 정보를 처리 안 된 보안위협 목록에 추가합니다.
6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 익스플로잇 방지를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 행동 분석 → 익스플로잇 방지**로 이동합니다.
5. **익스플로잇 방지 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.
6. **위협 탐지 시 처리 방법** 블록에서 필요한 동작을 선택합니다.
   - **차단**. 이 항목을 선택하면 익스플로잇 탐지 시 Kaspersky Endpoint Security가 이 익스플로잇의 동작을 차단하고 이 익스플로잇에 관한 정보가 포함된 로그 항목을 만듭니다.
   - **조치 알림 또는 확인**. 이 항목을 선택하면 Kaspersky Endpoint Security가 익스플로잇 탐지 시 이 익스플로잇에 관한 정보가 포함된 로그 항목을 만들고 이 익스플로잇에 관한 정보를 처리 안 된 보안위협 목록에 추가합니다.
7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 익스플로잇 방지를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 익스플로잇 방지**를 선택합니다.



익스플로잇 방지 설정

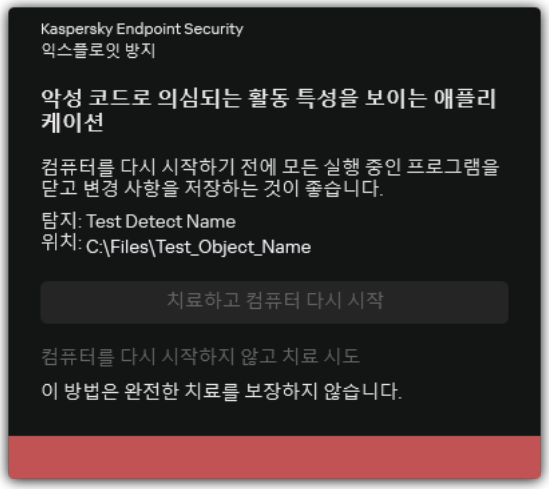
3. **익스플로잇 방지** 토글로 구성 요소를 사용하거나 중지합니다.

4. **익스플로잇 탐지 시** 블록에서 필요한 동작을 선택합니다:

   - **차단**. 이 항목을 선택하면 익스플로잇 탐지 시 Kaspersky Endpoint Security가 이 익스플로잇의 동작을 차단하고 이 익스플로잇에 관한 정보가 포함된 로그 항목을 만듭니다.

   - **알림**. 이 항목을 선택하면 Kaspersky Endpoint Security가 익스플로잇 탐지 시 이 익스플로잇에 관한 정보가 포함된 로그 항목을 만들고 이 익스플로잇에 관한 정보를 처리 안 된 보안위협 목록에 추가합니다.

5. 변경 사항을 저장합니다.



처리 안 된 보안위협에 대한 알림

시스템 프로세스 메모리 보호

기본 값으로 시스템 프로세스 메모리 보호가 사용됩니다. Kaspersky Endpoint Security는 시스템 프로세스에 접근하려는 외부 프로세스의 시도를 차단합니다.

관리 콘솔(MMC)에서 시스템 프로세스 메모리 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 창에서 **지능형 위협 보호 → 익스플로잇 방지**를 선택합니다.

4. **시스템 프로세스 메모리 보호 사용** 확인란을 사용하여 이 옵션을 활성화하거나 비활성화합니다.

5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 시스템 프로세스 메모리 보호를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **호스트 위협 보호 → 행동 분석 → 익스플로잇 방지**로 이동합니다.

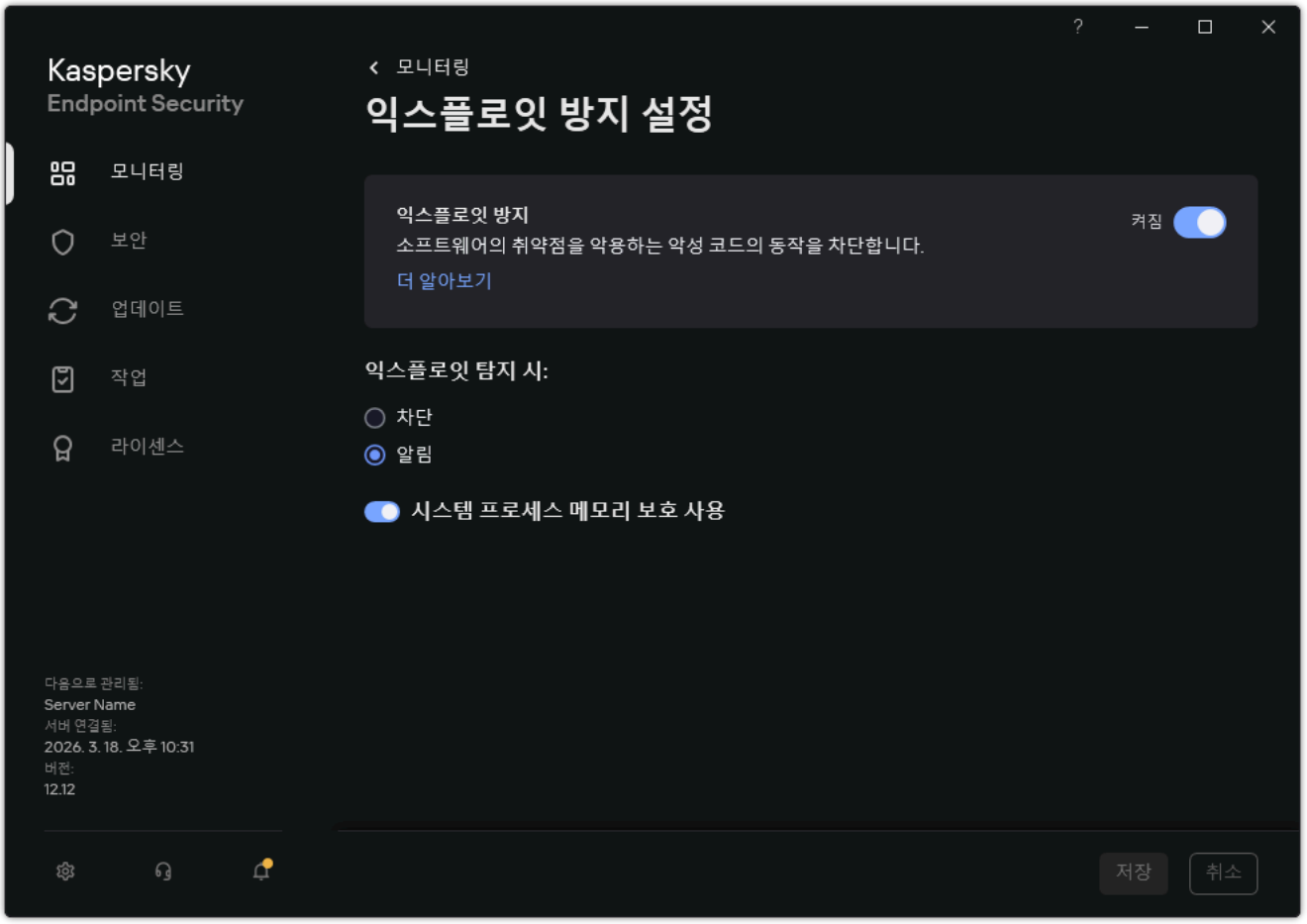
5. **시스템 프로세스 메모리 보호 활성화됨** 토글로 이 기능을 사용하거나 중지합니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 시스템 프로세스 메모리 보호를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 익스플로잇 방지**를 선택합니다.



익스플로잇 방지 설정

3. **시스템 프로세스 메모리 보호 사용** 토글로 이 기능을 사용하거나 중지합니다.

4. 변경 사항을 저장합니다.

행동 탐지

행동 탐지 구성 요소는 컴퓨터에 설치된 애플리케이션의 동작에 대한 데이터를 수신한 후 보호 구성 요소의 성능 향상을 위해 다른 구성 요소에 이 정보를 제공합니다. 행동 탐지 구성 요소는 애플리케이션의 행동 스트림 서명(BSS)을 활용합니다. 애플리케이션 동작이 행동 스트림 시그니처와 일치할 경우 Kaspersky Endpoint Security는 선택된 처리 방법을 수행합니다. Kaspersky Endpoint Security 기능은 행동 스트림 서명을 바탕으로 하며 컴퓨터에 대한 사전 방역을 제공합니다.

행동 탐지 구성 요소는 네트워크 포트에서 컴퓨터의 보안을 위협할 수 있는 애플리케이션 프로세스를 추가로 모니터링합니다. 애플리케이션은 안티 바이러스 데이터베이스를 사용하여 이러한 프로세스에 대한 정보를 가져옵니다.

기본적으로 행동 탐지는 작동되며 Kaspersky 전문가가 권장하는 모드에서 실행됩니다. 악성 활동이 탐지되면 Kaspersky Endpoint Security가 악성 애플리케이션의 실행 파일을 삭제합니다.

반드시 필요할 때가 아니라면 행동 탐지를 중지하는 것은 권장하지 않습니다. 중지할 경우 보호 구성 요소의 효율성이 저하될 수 있기 때문입니다. 보호 구성 요소는 위협 탐지를 위해 행동 탐지 구성 요소가 수집한 데이터를 사용할 수 있습니다.

관리 콘솔(MMC)에서 행동 탐지를 활성화 또는 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **지능형 위협 보호 → 행동 탐지**를 선택합니다.
5. **행동 탐지** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.
6. **악성 코드 활동 감지 시 처리 방법** 블록에서 필요한 동작을 선택합니다:
   - **삭제**. 이 항목을 선택하면 악성 코드 활동 탐지 시 Kaspersky Endpoint Security가 악성 코드의 실행 파일을 삭제하고 백업 저장소에 백업 복사본을 생성합니다.
   - **차단**. 이 항목을 선택한 경우 Kaspersky Endpoint Security는 악성 코드 활동 탐지 시 해당 애플리케이션을 종료합니다.
   - **알림**. 이 항목을 선택하고 애플리케이션의 악성코드 활동이 탐지되면 Kaspersky Endpoint Security는 애플리케이션의 악성 코드 활동에 대한 정보를 처리 안 된 위협 목록에 추가합니다.
7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 행동 탐지를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 행동 분석 → 행동 탐지**로 이동합니다.
5. **행동 탐지 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.

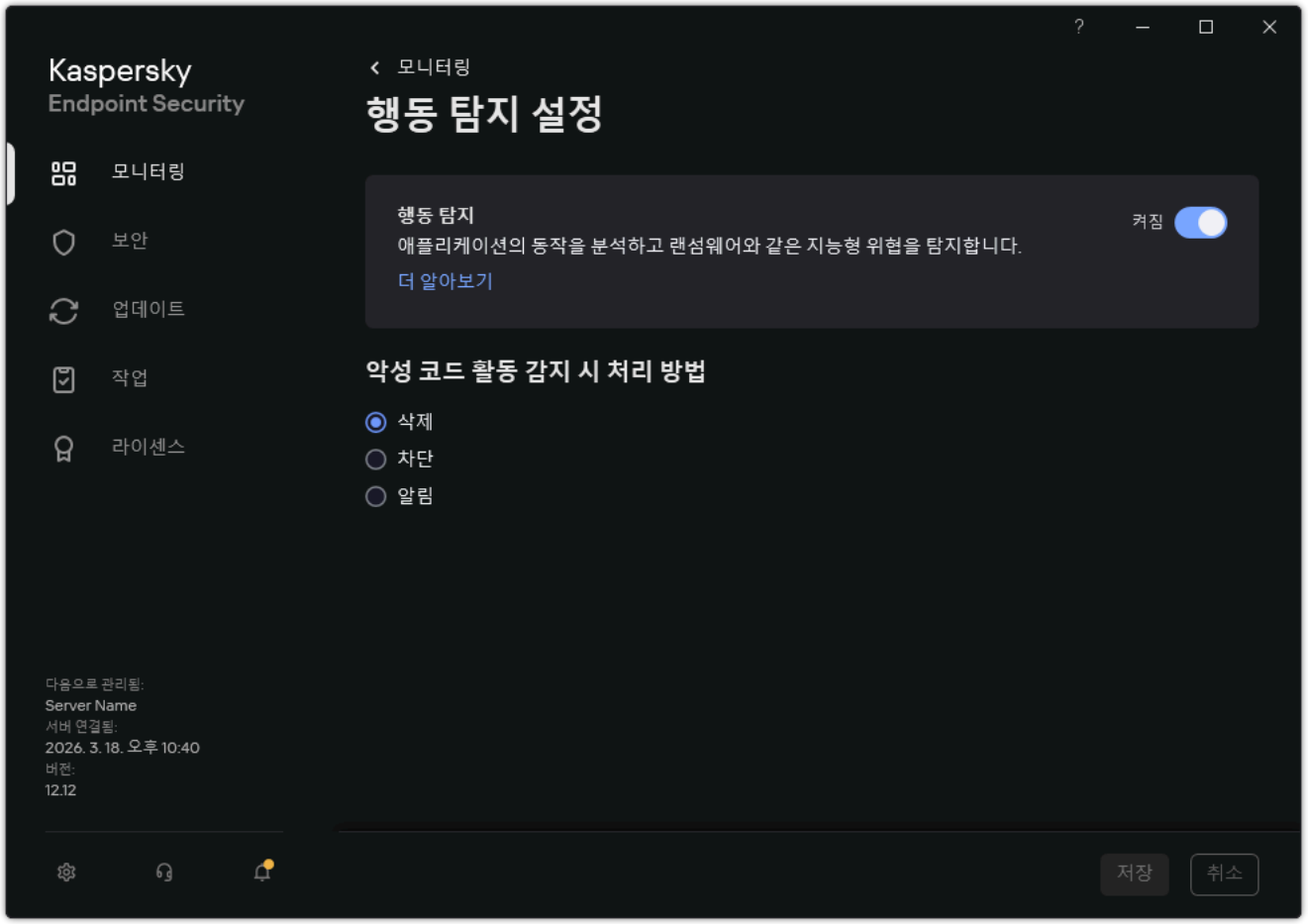
6. **위협 탐지 시 처리 방법** 블록에서 필요한 동작을 선택합니다.

   - **삭제**. 이 항목을 선택하면 악성 코드 활동 탐지 시 Kaspersky Endpoint Security가 악성 코드의 실행 파일을 삭제하고 백업 저장소에 백업 복사본을 생성합니다.
   - **차단**. 이 항목을 선택한 경우 Kaspersky Endpoint Security는 악성 코드 활동 탐지 시 해당 애플리케이션을 종료합니다.
   - **알림**. 이 항목을 선택하고 애플리케이션의 악성코드 활동이 탐지되면 Kaspersky Endpoint Security는 애플리케이션의 악성 코드 활동에 대한 정보를 처리 안 된 위협 목록에 추가합니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 행동 탐지를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 행동 탐지**를 선택합니다.



행동 탐지 설정

3. **행동 탐지** 토글로 구성 요소를 사용하거나 중지합니다.

4. **악성 코드 활동 감지 시 처리 방법** 블록에서 필요한 동작을 선택합니다:

   - **삭제**. 이 항목을 선택하면 악성 코드 활동 탐지 시 Kaspersky Endpoint Security가 악성 코드의 실행 파일을 삭제하고 백업 저장소에 백업 복사본을 생성합니다.
   - **차단**. 이 항목을 선택한 경우 Kaspersky Endpoint Security는 악성 코드 활동 탐지 시 해당 애플리케이션을 종료합니다.
   - **알림**. 이 항목을 선택하고 애플리케이션의 악성코드 활동이 탐지되면 Kaspersky Endpoint Security는 애플리케이션의 악성 코드 활동에 대한 정보를 처리 안 된 위협 목록에 추가합니다.

5. 변경 사항을 저장합니다.

결과적으로 행동 탐지를 사용하면 Kaspersky Endpoint Security는 행동 스트림 서명을 사용하여 운영 체제에서 애플리케이션의 활동을 분석합니다.

Anti-Cryptor

Kaspersky Endpoint Security 12.12 for Windows부터 행동 탐지 구성 요소의 일부였던 외부 암호화로부터 공유 폴더 보호는 별도의 구성 요소인 Anti-Cryptor입니다.

이 구성 요소는 NTFS 파일 시스템을 사용하는 대용량 저장소에 저장되고 EFS로 암호화되지 않은 파일만을 사용하여 수행된 작업을 감시합니다.

Anti-Cryptor 구성 요소는 공유 폴더의 활동을 분석합니다. 이 활동이 외부 암호화에서 일반적으로 나타나는 행동 스트림 시그니처와 일치하면 Kaspersky Endpoint Security가 선택한 동작을 수행합니다.

Anti-Cryptor 구성 요소가 작동하려면 행동 탐지 구성 요소를 활성화해야 합니다.

Kaspersky Endpoint Security가 공유 폴더에서의 파일 수정 시도 탐지 시 다음 작업을 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 Center 로 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 파일을 외부에서 암호화하려는 시도가 탐지되면 Kaspersky Endpoint Security가 1시간 동안 원격 사용자의 세션을 차단합니다(기본값).

Kaspersky Endpoint Security가 설치된 후 외부 암호화로부터 공유 폴더 보호는 컴퓨터를 다시 시작하기 전까지 제한됩니다.

관리 콘솔(MMC)에서 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 창에서 **지능형 위협 보호** → **Anti-Cryptor**를 선택합니다.
4. **Anti-Cryptor** 확인란으로 외부 컴퓨터에서 시도하는 일반적인 암호화 활동에 대한 탐지를 활성화하거나 비활성화합니다.
5. 공유 폴더의 파일 수정 시도가 탐지될 경우 애플리케이션에서 취할 조치 방법을 선택합니다:
   - **다음 시간 동안 연결 차단: N분**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 공유 폴더의 파일 수정 시도 탐지 시, 악의적 행위를 시작한 세션의 파일 수정 접근 권한을 차단하고 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 폴더에 있는 파일에 대한 수정 시도가 탐지될 때 Kaspersky Endpoint Security가 해당 시도에 대한 정보를 활성 위협 목록에 추가하고, 로컬 애플리케이션 인터페이스 리포트에 항목을 추가하고, 탐지된 악성 활동에 대한 정보를 Kaspersky Security Center로 전송합니다.
6. 필요한 경우 보호 범위를 변경하고 예외 규칙을 정의합니다.
7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 외부 암호화로부터 공유 폴더 보호 기능을 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.

4. **호스트 위협 보호** → **행동 분석** → **Anti-Cryptor**으로 이동합니다.

5. **Anti-Cryptor 사용** 토글로 외부 컴퓨터에서 시도하는 일반적인 암호화 활동에 대한 탐지를 활성화하거나 비활성화합니다.

6. 공유 폴더의 파일 수정 시도가 탐지될 경우 애플리케이션에서 취할 조치 방법을 선택합니다:

   - **다음 시간 동안 연결 차단(분) N분**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 공유 폴더의 파일 수정 시도 탐지 시, 악의적 행위를 시작한 세션의 파일 수정 접근 권한을 차단하고 수정된 파일의 백업 복사본을 생성합니다.

     복원 엔진 구성 요소를 활성화하고 **다음 시간 동안 연결 차단(분) N분** 옵션을 선택하면 수정된 파일을 백업 복사본에서 복원합니다.

   - **알림**. 이 옵션을 선택하면 공유 폴더에 있는 파일에 대한 수정 시도가 탐지될 때 Kaspersky Endpoint Security가 해당 시도에 대한 정보를 활성 위협 목록에 추가하고, 로컬 애플리케이션 인터페이스 리포트에 항목을 추가하고, 탐지된 악성 활동에 대한 정보를 Kaspersky Security Center로 전송합니다.

7. 필요한 경우 보호 범위를 변경하고 예외 규칙을 정의합니다.

8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 외부 암호화로부터 공유 폴더 보호 기능을 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **지능형 위협 보호** → **Anti-Cryptor**를 선택합니다.

3. **외부 암호화로부터 공유 폴더 보호** 확인란을 사용하여 외부 컴퓨터에서 시도하는 일반적인 암호화 활동에 대한 탐지를 활성화하거나 비활성화합니다.

4. **외부 암호화로부터 공유 폴더 보호** 확인란을 사용하여 외부 컴퓨터에서 시도하는 일반적인 암호화 활동에 대한 탐지를 활성화하거나 비활성화합니다.

5. 공유 폴더의 파일 수정 시도가 탐지될 경우 애플리케이션에서 취할 조치 방법을 선택합니다:

   - **다음 시간 동안 연결 차단(분) N분**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 공유 폴더의 파일 수정 시도 탐지 시, 악의적 행위를 시작한 세션의 파일 수정 접근 권한을 차단하고 수정된 파일의 백업 복사본을 생성합니다.

     복원 엔진 구성 요소를 활성화하고 **다음 시간 동안 연결 차단(분) N분** 옵션을 선택하면 수정된 파일을 백업 복사본에서 복원합니다.

   - **알림**. 이 옵션을 선택하면 공유 폴더에 있는 파일에 대한 수정 시도가 탐지될 때 Kaspersky Endpoint Security가 해당 시도에 대한 정보를 활성 위협 목록에 추가하고, 로컬 애플리케이션 인터페이스 리포트에 항목을 추가하고, 탐지된 악성 활동에 대한 정보를 Kaspersky Security Center로 전송합니다.

6. 필요한 경우 보호 범위를 변경하고 예외 규칙을 정의합니다.

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 Endpoint Security는 원격 사용자의 세션을 1시간 동안 차단합니다. 차단 기간이 만료되면 Kaspersky Endpoint Security는 차단 목록에서 해당 컴퓨터를 제거하고 공유 폴더에 대한 접근 권한을 복원합니다.

관리 콘솔(MMC)에서 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 창에서 **지능형 위협 보호 → Anti-Cryptor**를 선택합니다.
4. **위협 탐지 시 처리 방법** 블록에서 **다음 시간 동안 연결 차단 N분**을 선택합니다.
5. 악성 활동 또는 데이터 암호화에 연루된 신뢰할 수 없는 컴퓨터의 차단 기간을 설정합니다.
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 신뢰할 수 없는 컴퓨터의 차단 기간을 설정하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 행동 분석 → Anti-Cryptor**으로 이동합니다.
5. **위협 탐지 시 처리 방법**에서 악성 활동 또는 데이터 암호화에 연루된 신뢰할 수 없는 컴퓨터의 차단 기간을 설정합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 신뢰할 수 없는 컴퓨터의 차단 기간을 설정하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호 → Anti-Cryptor**를 선택합니다.
3. **위협 탐지 시 처리 방법** 블록에서 **다음 시간 동안 연결 차단(분)**을 선택합니다.
4. 악성 활동 또는 데이터 암호화에 연루된 신뢰할 수 없는 컴퓨터의 차단 기간을 설정합니다.
5. 변경 사항을 저장합니다.

그러면 원격 컴퓨터가 잠깁니다. 원격 컴퓨터의 잠금을 해제하려면 Kaspersky Endpoint Security를 다시 시작하면 됩니다.

보호 범위 편집

*보호 범위*는 Kaspersky Endpoint Security가 파일 활동을 감시하는 공유 폴더의 경로 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다. 기본적으로 애플리케이션은 공유 폴더를 자동으로 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, 행동 탐지가 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.

> 외부 암호화 시도를 처리되지 않아야 하는 컴퓨터를 제외할 수도 있습니다.

관리 콘솔(MMC)에서 보호 범위를 편집하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **지능형 위협 보호** → **Anti-Cryptor**를 선택합니다.
4. **보호 범위** 블록에서 **지정된 공유 폴더만 해당**을 선택합니다.
5. 폴더 목록에서 **추가**를 클릭합니다.
6. 그러면 창이 열립니다. 이 창에서 보호 범위에 포함할 공유 폴더의 경로를 입력합니다(예, `C:\Share`).

   > 공유 폴더를 보호 범위에 추가하려면 로컬 경로를 사용하십시오.

7. **확인**을 누릅니다.
8. 필요한 경우 보호 범위 예외 규칙을 정의하십시오.
   a. **검사 예외** 창에서 **마스크 사용** 버튼을 누릅니다.
   b. 열리는 창에서 **추가** 버튼을 누릅니다.
   c. 표시된 창의 `*.<file extension>` 형식 또는 폴더 경로에서 파일 확장자를 지정합니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.
      애플리케이션이 일부 예외 파일 확장자를 지원하지 않습니다. 따라서 `*.docx` 또는 `**\Folder\**`로 예외 규칙을 지정할 수 있습니다.

   보호 범위의 개체 목록에서 개체를 삭제하지 않고도 보호 대상에서 개체를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.
9. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 보호 범위를 편집하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호** → **행동 분석** → **Anti-Cryptor**으로 이동합니다.
5. **보호 범위** 블록에서 **지정된 공유 폴더만 해당**을 선택합니다.
6. 폴더 목록에서 **추가**를 클릭합니다.
7. 그러면 창이 열립니다. 이 창에서 보호 범위에 포함할 공유 폴더의 경로를 입력합니다(예, `C:\Share`).

   > 공유 폴더를 보호 범위에 추가하려면 로컬 경로를 사용하십시오.

8. **확인**을 누릅니다.
9. 필요한 경우 보호 범위 예외 규칙을 정의하십시오.
   a. 창 상단에서 **검사 예외** 링크를 클릭합니다.
   b. 열리는 창에서 **추가** 버튼을 누릅니다.
   c. 표시된 창의 `*.<file extension>` 형식 또는 폴더 경로에서 파일 확장자를 지정합니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.
   애플리케이션이 일부 예외 파일 확장자를 지원하지 않습니다. 따라서 `*.docx` 또는 `**\Folder\**`로 예외 규칙을 지정할 수 있습니다.

   보호 범위의 개체 목록에서 개체를 삭제하지 않고도 보호 대상에서 개체를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.
10. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 보호 범위를 편집하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호** → **Anti-Cryptor**를 선택합니다.
3. **보호 범위** 블록에서 **지정된 공유 폴더만 해당**을 선택합니다.
4. 폴더 목록에서 **추가**를 클릭합니다.
5. 그러면 창이 열립니다. 이 창에서 보호 범위에 포함할 공유 폴더의 경로를 입력합니다(예, `C:\Share`).

   > 공유 폴더를 보호 범위에 추가하려면 로컬 경로를 사용하십시오.

6. **확인**을 누릅니다.

7. 필요한 경우 보호 범위 예외 규칙을 정의하십시오.

   a. 창 상단에서 **마스크로 예외 설정** 링크를 클릭합니다.

   b. 열리는 창에서 **추가** 버튼을 누릅니다.

   c. 표시된 창의 `*.<file extension>` 형식 또는 폴더 경로에서 파일 확장자를 지정합니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.

      애플리케이션이 일부 예외 파일 확장자를 지원하지 않습니다. 따라서 `*.docx` 또는 `**\Folder\**`로 예외 규칙을 지정할 수 있습니다.

   보호 범위의 개체 목록에서 개체를 삭제하지 않고도 보호 대상에서 개체를 제외할 수 있습니다. 이렇게 하려면 개체 옆의 확인란을 선택 해제합니다.

8. 변경 사항을 저장합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **일반 설정** → **예외 규칙 및 탐지된 개체의 유형**을 선택합니다.

3. **예외 규칙** 블록에서 **예외 규칙 관리** 링크를 클릭합니다.

4. **추가**를 클릭합니다.

5. **찾아보기**를 클릭하고 공유 폴더를 선택합니다.

   경로를 수동으로 입력할 수도 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 * 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. **보호 구성 요소** 블록에서, **행동 탐지** 구성 요소를 선택합니다.

7. 필요하면, **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

8. 제외할 **활성** 상태를 선택합니다.
   토글을 사용하여 언제든지 예외를 중지할 수 있습니다.

9. 변경 사항을 저장합니다.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **신뢰 구역** 섹션으로 이동합니다.

5. 창이 열리면 **악성 코드 검사 예외** 링크를 누릅니다.

6. 회사의 모든 컴퓨터에 대해 통합 예외 규칙 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 예외 규칙의 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 취소하면 Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 검사 예외 통합 목록을 숨깁니다.

8. **추가**를 클릭하고 작업을 선택합니다:

   - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.
   - **새로운 예외**. Kaspersky Endpoint Security가 새 검사 예외를 목록의 루트에 추가합니다.
   - **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 검사 예외*가 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 검사 예외가 추가되었습니다. 보호하는 서버의 용도에 따라 사전 정의된 검사 예외를 선택해야 합니다.

9. **파일 또는 폴더 경로**로 예외 규칙을 어떻게 추가할지 선택합니다.

10. 경로를 공유 폴더에 입력합니다.

경로를 수동으로 입력할 수도 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 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 `C:\Users\*\Folder\` 마스크를 입력합니다.

11. **예외 적용 대상** 블록에서, **행동 탐지** 구성 요소를 선택합니다.

12. 필요하면, **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

13. 제외할 **예외 규칙에 추가** 상태를 선택합니다.
    토글을 사용하여 언제든지 예외를 중지할 수 있습니다.

14. 변경 사항을 저장합니다.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **일반 설정** → **예외 및 개체 유형**을 선택합니다.

4. **검사 예외 및 신뢰하는 애플리케이션** → **검사 예외** 블록에서 **설정** 버튼을 누릅니다.
   예외 규칙 목록이 포함된 창이 열립니다.

5. 회사의 모든 컴퓨터에 대해 통합 예외 규칙 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 예외 규칙의 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 취소하면 Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 검사 예외 통합 목록을 숨깁니다.

7. **추가**를 클릭하고 작업을 선택합니다:

   - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.

   - **새로운 예외**. Kaspersky Endpoint Security가 새 검사 예외를 목록의 루트에 추가합니다.

   - **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 검사 예외*가 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 검사 예외가 추가되었습니다. 보호하는 서버의 용도에 따라 사전 정의된 검사 예외를 선택해야 합니다.

8. **추가**를 클릭합니다.

9. **속성** 블록에서 **파일 또는 폴더** 확인란을 선택합니다.

10. **파일 또는 폴더 선택**의 이름 창을 열려면, **검사 예외 설명(편집하려면 밑줄 친 항목을 눌러 주십시오)** 블록에 있는 **파일 또는 폴더 이름** 링크를 클릭합니다.

11. **찾아보기**를 클릭하고 공유 폴더를 선택합니다.

    경로를 수동으로 입력할 수도 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 * 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.

12. 필요하면, **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

13. **보호 구성 요소** 창을 열려면 **검사 예외 설명(편집하려면 밑줄 친 항목을 눌러 주십시오)** 블록에 있는 링크를 클릭합니다.

14. **행동 탐지** 구성 요소 옆의 확인란을 선택합니다.

15. 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 Endpoint Security는 신뢰하는 컴퓨터의 데이터 암호화를 모니터링하지 않습니다.

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 Endpoint Security를 시작하기 전에 원격 컴퓨터가 꺼진 경우에는 원격 컴퓨터에서 작동하지 않습니다. Kaspersky Endpoint Security가 시작된 후 이 원격 컴퓨터를 다시 시작하면 공유 폴더 보호 시 특정 주소를 예외 처리하는 기능이 이 원격 컴퓨터에서 작동하도록 할 수 있습니다.

신뢰하는 컴퓨터 목록의 변경은 부모 정책의 속성에 따라 차단될 수 있습니다. 목록을 변경하려면 웹 콘솔의 신뢰 구역('자물쇠'가 잠금 해제되어야 함) 설정 변경을 허용해야 합니다.

신뢰 구역은 관리 콘솔(MMC)과 웹 콘솔에서 다르게 그룹화됩니다. 마찬가지로, 신뢰 구역 파라미터의 변경을 방지하는 방법도 다릅니다('자물쇠'가 다름). 웹 콘솔만 사용하여 애플리케이션을 관리하는 것이 좋습니다. 서로 다른 콘솔에서 신뢰 구역을 구성하는 경우 관리 플러그인이 '자물쇠'를 기본 상태로 재설정할 수 있습니다.

관리 콘솔(MMC)에서 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 창에서 **지능형 위협 보호** → **Anti-Cryptor**를 선택합니다.
4. **검사 예외** 창에서 **이름 또는 IP 주소 사용** 버튼을 누릅니다.
5. 창이 열리면 **이름 또는 IP 주소 사용** 버튼을 클릭합니다.
6. 외부에서의 암호화 시도를 처리하지 말아야 하는 IP 주소, IP 주소 범위 또는 컴퓨터 이름을 입력합니다.

   예:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`

- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

7. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 외부 데이터 암호화를 위해 신뢰하는 컴퓨터를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호** → **행동 분석** → **Anti-Cryptor**으로 이동합니다.
5. 창 상단에서 **이름 또는 IP 주소로 예외 설정** 링크를 클릭합니다.
6. 열리는 창에서 **추가** 버튼을 누릅니다.
7. 외부에서의 암호화 시도를 처리하지 말아야 하는 IP 주소, IP 주소 범위 또는 컴퓨터 이름을 입력합니다.
   예:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 외부 데이터 암호화를 위해 신뢰하는 컴퓨터를 추가하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호** → **Anti-Cryptor**를 선택합니다.
3. 창 상단에서 **이름 또는 IP 주소로 예외 설정** 링크를 클릭합니다.
4. 열리는 창에서 **추가** 버튼을 누릅니다.
5. 외부에서의 암호화 시도를 처리하지 말아야 하는 IP 주소, IP 주소 범위 또는 컴퓨터 이름을 입력합니다.
   예:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`

- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

6. 변경 사항을 저장합니다.

외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호 시 예외 규칙 목록 내보내기 및 가져오기

예외 규칙 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.

관리 콘솔(MMC)에서 예외 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 창에서 **지능형 위협 보호** → **Anti-Cryptor**를 선택합니다.
4. **검사 예외** 창에서 **이름 또는 IP 주소 사용** 버튼을 누릅니다.
5. 규칙 목록을 내보내려면 다음을 수행합니다.
   a. 내보낼 예외 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
      예외 규칙을 아무 것도 선택하지 않으면 Kaspersky Endpoint Security가 모든 예외 규칙을 내보냅니다.
   b. → **내보내기** 버튼을 클릭합니다.
   c. 창이 열리면 예외 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   d. 파일을 저장합니다.
      Kaspersky Endpoint Security는 예외 규칙의 전체 목록을 XML 파일로 내보냅니다.
6. 예외 목록을 가져오려면 다음을 수행합니다.
   a. → **가져오기** 버튼을 클릭합니다.
   b. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.
   c. 파일을 엽니다.
      컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.
7. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 예외 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 행동 분석 → Anti-Cryptor**으로 이동합니다.
5. **이름 또는 IP 주소로 예외 설정** 링크를 클릭합니다.
6. 규칙 목록을 내보내려면 다음을 수행합니다.
   a. 내보낼 예외 규칙을 선택합니다.
   b. → **내보내기** 버튼을 클릭합니다.
      Kaspersky Endpoint Security는 예외 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.
7. 예외 목록을 가져오려면 다음을 수행합니다.
   a. → **가져오기** 버튼을 클릭합니다.
      창이 열리면 예외 규칙 목록을 가져올 JSON 파일을 선택합니다.
   b. 파일을 엽니다.
      컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.
8. 변경 사항을 저장합니다.

복원 엔진

복원 엔진을 사용하면 Kaspersky Endpoint Security가 운영 체제에서 악성 코드에 의해 수행된 활동을 롤백합니다.

운영 체제에서 악성 코드가 수행한 동작을 롤백할 때 Kaspersky Endpoint Security는 다음과 같은 유형의 악성 코드를 처리합니다:

- **파일 활동**
  Kaspersky Endpoint Security는 다음 동작을 수행합니다:
  - 악성 코드에 의해 생성된 실행 파일을 삭제합니다(네트워크 드라이브를 제외한 모든 미디어에서).
  - 악성 코드에 의해 침입된 프로그램이 생성한 실행 파일을 삭제합니다.
  - 악성 코드에 의해 수정되거나 삭제된 파일을 복원합니다.

  파일 복구 기능에는 여러 가지 제한이 있습니다.
- **레지스트리 활동**

Kaspersky Endpoint Security는 다음 동작을 수행합니다:

- 악성 코드에서 생성한 레지스트리 키를 삭제합니다.
- 악성 코드에서 변경하거나 삭제한 레지스트리 키는 복원하지 않습니다.

- **시스템 활동**

  Kaspersky Endpoint Security는 다음 동작을 수행합니다:

  - 악성 코드에 의해 시작된 프로세스를 종료합니다.
  - 악성 애플리케이션이 침투한 프로세스를 종료합니다.
  - 악성 코드에 의해 중지된 프로세스는 재시작하지 않습니다.

- **네트워크 활동**

  Kaspersky Endpoint Security는 다음 동작을 수행합니다:

  - 악성 코드의 네트워크 활동을 차단합니다.
  - 악성 코드가 침투한 프로세스의 네트워크 활동을 차단합니다.

악성 코드 활동의 롤백은 파일 위협 보호, 행동 탐지 구성 요소 또는 악성 코드 검사에 의해 시작됩니다.

악성 코드 활동을 롤백하면 엄격하게 정의된 데이터 집합에는 영향을 줍니다. 롤백은 운영 체제 또는 컴퓨터 데이터의 무결성에는 악영향이 없습니다.

관리 콘솔(MMC)에서 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 창에서 **지능형 위협 보호 → 복원 엔진**을 선택합니다.
4. **복원 엔진** 확인란으로 구성 요소를 사용하거나 중지합니다.
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 복원 엔진 구성 요소를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **호스트 위협 보호 → 행동 분석 → 복원 엔진**으로 이동합니다.
5. **복원 엔진 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 복원 엔진 구성 요소를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호 → 복원 엔진**을 선택합니다.
3. **복원 엔진** 토글로 구성 요소를 사용하거나 중지합니다.
4. 변경 사항을 저장합니다.

결과적으로 복원 엔진을 사용하면 Kaspersky Endpoint Security는 운영 체제에서 악성 애플리케이션이 수행한 작업을 롤백합니다.

Kaspersky Security Network



Kaspersky Endpoint Security는 사용자 컴퓨터를 보다 효과적으로 보호하기 위해 전세계 사용자로부터 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 Endpoint Security에서 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 Endpoint Security는 검사한 웹 주소의 평판 정보는 물론이고 검사한 파일의 카테고리 및 평판에 관한 정보도 수신하게 됩니다.

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 Endpoint Security는 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 Endpoint Security 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 및 비활성화

기본적으로 Kaspersky Endpoint Security는 확장 KSN 모드를 사용합니다. *확장 KSN 모드*는 Kaspersky Endpoint Security가 추가 데이터를 Kaspersky로 전송하는 모드입니다.

관리 콘솔(MMC)에서 KSN 사용을 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 설정 창에서 **지능형 위협 보호 → Kaspersky Security Network**를 선택합니다.
4. **Kaspersky Security Network** 토글로 구성 요소를 사용하거나 중지합니다.

   KSN을 사용한다면 Kaspersky Endpoint Security가 Kaspersky Security Network 진술문을 표시합니다. Kaspersky Security Network(KSN) 진술문 약관을 읽어 보고, 동의한다면 수락하십시오.
5. 필요한 경우 **확장 KSN 모드 사용** 확인란 선택을 취소합니다.
6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 KSN 사용을 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → Kaspersky Security Network**으로 이동합니다.

5. **Kaspersky Security Network(KSN) 사용 활성화됨** 토글로 구성 요소를 사용하거나 중지합니다.

   KSN을 사용한다면 Kaspersky Endpoint Security가 Kaspersky Security Network 진술문을 표시합니다. Kaspersky Security Network(KSN) 진술문 약관을 읽어 보고, 동의한다면 수락하십시오.

6. 필요에 따라 **확장 KSN 모드 사용** 확인란의 토글을 해제합니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 KSN 사용을 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **지능형 위협 보호** → **Kaspersky Security Network**를 선택합니다.

3. **Kaspersky Security Network** 토글로 구성 요소를 사용하거나 중지합니다.

   KSN을 사용한다면 Kaspersky Endpoint Security가 Kaspersky Security Network 진술문을 표시합니다. Kaspersky Security Network(KSN) 진술문 약관을 읽어 보고, 동의한다면 수락하십시오.

4. 필요에 따라 **확장 KSN 모드 사용** 확인란의 토글을 해제합니다.

5. 변경 사항을 저장합니다.

결과적으로 KSN을 사용하면 Kaspersky Endpoint Security가 Kaspersky Security Network에서 받은 파일, 웹 리소스, 애플리케이션의 평판에 대한 정보를 사용합니다.

Kaspersky Private Security Network의 제한 사항

*Kaspersky Private Security Network(KPSN)*는 Kaspersky Endpoint Security 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 Endpoint Security가 컴퓨터를 검사하고 KSN/KPSN에있는 파일의 평판을 요청한다고 가정해봅시다. 파일의 평판이 로컬 평판 데이터베이스에서는 *신뢰하지 않음*이지만 KSN/KPSN에서는 *신뢰함*이라면, Kaspersky Endpoint Security는 파일을 *신뢰하지 않음*으로 탐지하고 탐지된 보안위협에 대해 정의된 조치를 취합니다.

그러나 경우에 따라 Kaspersky Endpoint Security가 KSN/KPSN에서 개체에 대한 평판을 요청하지 않을 수 있습니다. 이 경우 Kaspersky Endpoint Security는 KPSN의 로컬 평판 데이터베이스에서 데이터를 수신하지 않습니다. Kaspersky Endpoint Security는 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(신뢰하는 영역)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. 애플리케이션 인터페이스에서 파일 위협 방지 구성 요소 등에 대한 검색 최적화 설정을 구성할 수도 있습니다.

- Light Agent 모드의 Kaspersky Endpoint Security는 KSN 프록시 서버를 통해 KSN 서버와 통신합니다. KSN과의 직접 통신은 지원되지 않습니다.

보호 구성 요소에서 클라우드 모드 사용 및 중지

클라우드 모드 Kaspersky Endpoint Security가 경량 버전의 안티 바이러스 데이터베이스를 사용하는 애플리케이션 운영 모드를 의미합니다. Kaspersky Security Network는 경량의 안티 바이러스 데이터베이스가 사용 중일 때 애플리케이션의 운영을 지원합니다. 경량 버전의 안티 바이러스 데이터베이스를 사용하면 일반 데이터베이스에 비해 절반 가량의 컴퓨터 RAM을 사용하게 됩니다. Kaspersky Security Network에 참여하지 않거나 클라우드 모드를 사용하지 않는 경우 Kaspersky Endpoint Security는 Kaspersky 서버에서 전체 버전의 안티 바이러스 데이터베이스를 다운로드합니다.

Kaspersky Private Security Network 사용 시 Kaspersky Private Security Network 버전 3.0부터 클라우드 모드 기능을 이용할 수 있습니다.

애플리케이션이 Light Agent 모드로 작동하는 경우, 클라우드 모드를 사용할 수 없습니다.

관리 콘솔(MMC)에서 보호 구성 요소의 클라우드 모드를 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 설정 창에서 **지능형 위협 보호** → **Kaspersky Security Network**를 선택합니다.
4. **클라우드 모드 사용** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.
5. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 보호 구성 요소의 클라우드 모드를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **Kaspersky Security Network**으로 이동합니다.
5. **클라우드 모드 사용** 토글로 구성 요소를 사용하거나 중지합니다.
6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 보호 구성 요소의 클라우드 모드를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **지능형 위협 보호** → **Kaspersky Security Network**를 선택합니다.
3. **클라우드 모드 사용** 토글로 구성 요소를 사용하거나 중지합니다.
4. 변경 사항을 저장합니다.

결과적으로 Kaspersky Endpoint Security는 다음 업데이트 중에 가벼운 버전 또는 전체 버전의 안티 바이러스 데이터베이스를 다운로드합니다.

가벼운 버전의 안티 바이러스 데이터베이스를 사용할 수 없다면 Kaspersky Endpoint Security는 자동으로 안티 바이러스 데이터베이스의 프리미엄 버전으로 전환합니다.

KSN 프록시 설정

Kaspersky Security Center 중앙 관리 서버가 관리하는 사용자 컴퓨터는 KSN과 직접 상호작용하거나 KSN Proxy 서비스를 통해 상호작용할 수 있습니다.

애플리케이션이 Light Agent 모드로 실행 중인 경우, KSN과의 직접적인 통신은 지원되지 않습니다. Kaspersky Endpoint Security는 KSN 프록시 서버를 통해 KSN 서버와 통신합니다.

KSN Proxy(KSN 프록시)는 다음과 같은 기능을 제공합니다:

- 직접 인터넷을 통하지 않고 사용자의 컴퓨터에서 KSN으로 쿼리를 전송하고 정보를 제출합니다.
- KSN Proxy 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 다음을 확인해야 합니다.

- `ksnproxy` 서비스가 중앙 관리 서버에서 실행 중입니다.
- 포트 13111이 컴퓨터의 방화벽에 차단되지 않았습니다.

KSN Proxy를 활성화 또는 비활성화하고 연결을 위한 포트를 구성하여 KSN Proxy 사용을 구성할 수 있습니다. 이렇게 하려면 중앙 관리 서버 속성을 열어야 합니다. KSN Proxy 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.. Kaspersky Endpoint Security 정책에서 개별 컴퓨터에 대해 KSN Proxy를 활성화 또는 비활성화할 수도 있습니다.

관리 콘솔(MMC)에서 KSN 프록시를 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 설정 창에서 **지능형 위협 보호** → **Kaspersky Security Network**를 선택합니다.

4. **KSN 프록시 설정** 블록에서 **중앙 관리 서버를 KSN 프록시 서버로 사용** 확인란을 선택하여 KSN 프록시를 활성화하거나 비활성화합니다.

5. 필요하다면 **KSN 프록시 서버를 이용할 수 없는 경우 Kaspersky Security Network 서버 사용** 확인란을 선택합니다.

   이 확인란을 선택하면 Kaspersky Endpoint Security가 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.

6. 변경 사항을 저장합니다.

웹 콘솔에서 KSN 프록시를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정 → Kaspersky Security Network**으로 이동합니다.

5. **중앙 관리 서버를 KSN 프록시 서버로 사용** 확인란으로 KSN Proxy를 활성화하거나 비활성화합니다.

6. 필요하다면 **KSN 프록시 서버를 이용할 수 없는 경우 Kaspersky Security Network 서버 사용** 확인란을 선택합니다.

   이 확인란을 선택하면 Kaspersky Endpoint Security가 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 Proxy 주소는 중앙 관리 서버 주소와 일치합니다. 중앙 관리 서버 도메인 이름이 변경되면 KSN Proxy 주소를 직접 업데이트해야 합니다.

KSN 프록시 주소를 구성하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 콘솔에서 **고급 → 원격 설치 → 설치 패키지** 폴더를 선택합니다.

3. **설치 패키지** 폴더의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

4. 열린 창의 **일반** 탭에서 KSN 프록시 서버의 새 주소를 지정합니다.

5. 변경 사항을 저장합니다.

Kaspersky Security Network 내 파일의 평판 확인

파일의 보안이 의심스러운 경우 Kaspersky Security Network에서 파일의 평판을 확인할 수 있습니다.

Kaspersky Security Network 진술문의 약관에 동의한 경우 파일의 평판을 확인할 수 있습니다.

Kaspersky Security Network 내 파일의 평판을 확인하려면 다음을 수행합니다.

파일의 마우스 오른쪽 메뉴를 열고 **KSN에서 평판 확인** 옵션을 선택합니다(아래 그림 참조).



파일 마우스 오른쪽 메뉴

Kaspersky Endpoint Security는 파일 평판을 표시합니다.

신뢰함(Kaspersky Security Network). 애플리케이션은 다음 조건 중 하나 이상이 충족되는 경우 파일을 신뢰할 수 있는 것으로 간주합니다.

- 신뢰하는 공급업체가 파일에 디지털 서명한 경우
- 파일이 Kaspersky Security Network에서 신뢰하는 평판을 가지고 있는 경우
- 사용자가 신뢰하는 그룹에 애플리케이션을 추가한 경우

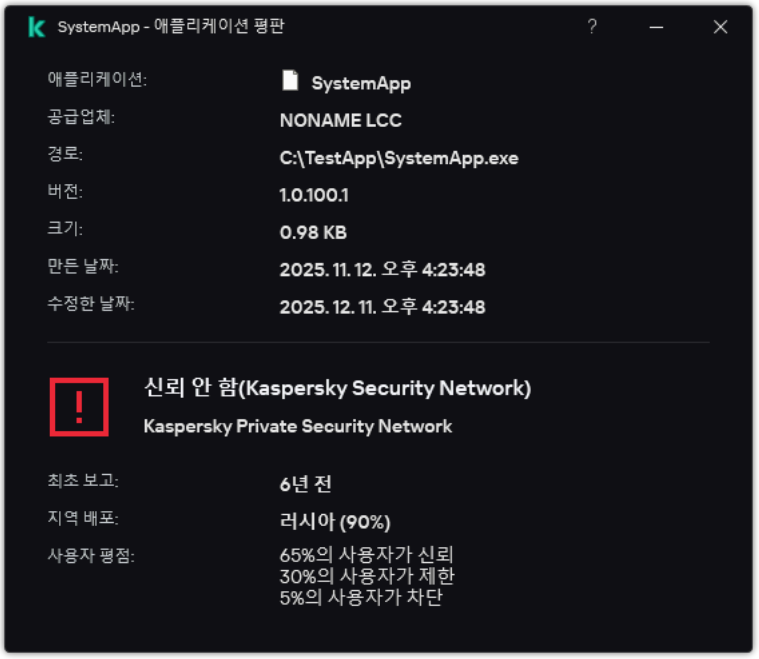
침입자에게 악용되어 사용자의 컴퓨터나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어. 해당 애플리케이션은 악성 기능을 갖지 않지만 침입자가 악용할 수 있습니다. 범죄자들이 사용자의 개인 데이터나 컴퓨터를 손상시키는 데 사용할 수 있는 합법적 소프트웨어에 대한 상세 정보는 Kaspersky IT 백과사전을 참조하십시오. 이러한 애플리케이션을 신뢰하는 목록에 추가할 수 있습니다.

신뢰 안 함(Kaspersky Security Network). 위협이 되는 바이러스 또는 기타 애플리케이션.

알 수 없음(Kaspersky Security Network). Kaspersky Security Network에 파일에 대한 정보가 없습니다. 안티 바이러스 데이터베이스를 사용하여 파일을 검사할 수 있습니다(마우스 오른쪽 메뉴의 **바이러스 검사** 옵션).

Kaspersky Endpoint Security는 파일의 평판을 결정하는 데 사용된 KSN 솔루션(*Kaspersky Security Network* 또는 *Kaspersky Private Security Network*)을 표시합니다.

Kaspersky Endpoint Security는 파일에 대한 추가 정보도 표시합니다(아래 그림 참조).



Kaspersky Security Network 내 파일의 평판

암호화된 연결 검사

설치 후 Kaspersky Endpoint Security는 신뢰하는 인증서의 시스템 저장소(Windows 인증서 저장소)에 Kaspersky 인증서를 추가합니다. Kaspersky Endpoint Security는 이 인증서를 사용하여 암호화된 연결을 검사합니다. Kaspersky Endpoint Security는 Firefox 및 Thunderbird에서 신뢰하는 인증서의 시스템 저장소를 사용하여 이러한 애플리케이션의 트래픽을 검사하는 것도 포함합니다.

웹 제어, 메일 위협 보호, 웹 위협 보호, 행동 탐지 및 익스플로잇 방지 구성 요소는 다음 프로토콜을 사용하여 암호화된 연결을 통해 전송되는 네트워크 트래픽을 복호화하고 검사할 수 있습니다:

- SSL 3.0
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3

암호화된 연결 검사 활성화

기본적으로 Kaspersky Endpoint Security는 항상 암호화된 연결을 검사하는 것이 아니라 보호 구성 요소가 요청할 경우에만 검사합니다.

관리 콘솔(MMC)에서 암호화된 연결 검사를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

4. 정책 창에서 **일반 설정 → 네트워크 설정**을 선택합니다.

5. **암호화된 연결 검사** 블록에서 암호화된 연결 검사 모드를 선택합니다:

   - **암호화된 연결 검사**. Kaspersky Endpoint Security가 `https://`로 시작하는 주소의 웹사이트 컨텐츠에 접근하지 못합니다.
   - **보호 구성 요소의 요청 하에 암호화된 연결 검사**. Kaspersky Endpoint Security가 웹 위협 보호, 메일 위협 보호, 웹 제어 구성 요소의 요청을 통해서만 암호화된 트래픽을 검사합니다.
   - **항상 암호화된 연결 검사**. 보호 구성 요소가 중지된 상태에서도 Kaspersky Endpoint Security가 암호화된 네트워크 트래픽을 검사합니다.

   Kaspersky Endpoint Security는 트래픽 검사가 중지된 신뢰하는 애플리케이션에 따라 설정된 암호화된 연결을 검사하지 않습니다. Kaspersky Endpoint Security는 미리 정의된 신뢰하는 웹사이트 목록에서의 암호화된 연결을 검사하지 않습니다. 미리 정의된 신뢰하는 웹사이트 목록은 Kaspersky 전문가가 작성합니다. 이 목록은 애플리케이션의 안티 바이러스 데이터베이스로 업데이트합니다. Kaspersky Endpoint Security 인터페이스에서만 사전 정의된 신뢰하는 웹사이트 목록을 볼 수 있습니다. Kaspersky Security Center 콘솔에서는 목록을 볼 수 없습니다.

6. 필요시 검사 예외: 신뢰하는 주소 및 애플리케이션을 추가합니다.

7. 암호화된 연결 검사를 위한 설정을 구성합니다(아래 표를 참조하십시오).

8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 암호화된 연결 검사를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 탭을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정 → 네트워크 설정**으로 갑니다.

5. **암호화된 연결 검사**에서 **암호화된 연결 검사 활성화됨** 토글 스위치를 켭니다.

   이 토글 버튼을 끄면 Kaspersky Endpoint Security가 `https://`로 시작하는 주소의 웹사이트 컨텐츠에 접근하지 못합니다.

6. **설정**을 클릭하고 암호화된 연결 검사 모드를 선택합니다.

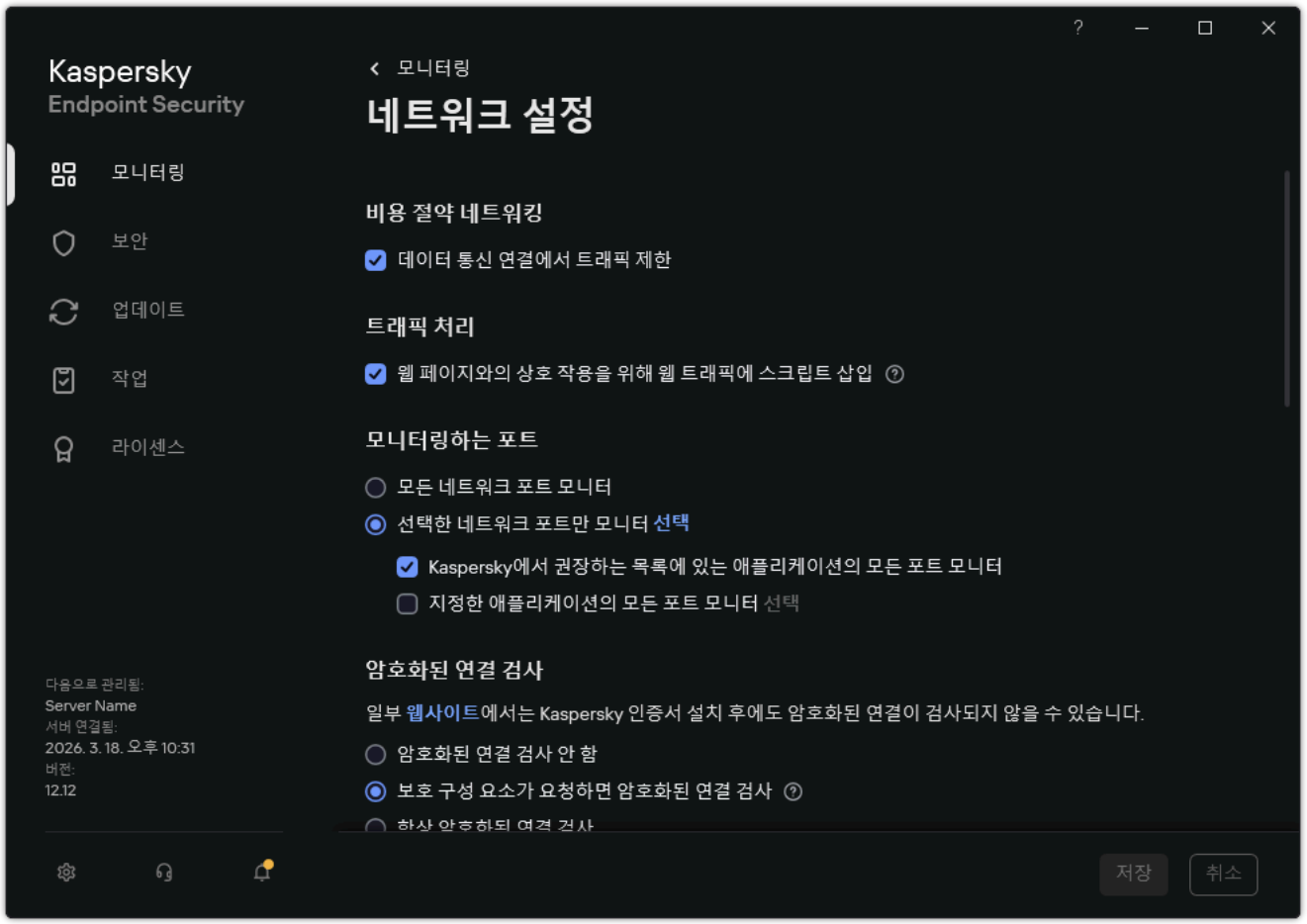
   - **보호 구성 요소의 요청 하에 암호화된 연결 검사**. Kaspersky Endpoint Security가 웹 위협 보호, 메일 위협 보호, 웹 제어 구성 요소의 요청을 통해서만 암호화된 트래픽을 검사합니다.
   - **항상 암호화된 연결 검사**. 보호 구성 요소가 중지된 상태에서도 Kaspersky Endpoint Security가 암호화된 네트워크 트래픽을 검사합니다.

Kaspersky Endpoint Security는 트래픽 검사가 중지된 신뢰하는 애플리케이션에 따라 설정된 암호화된 연결을 검사하지 않습니다. Kaspersky Endpoint Security는 미리 정의된 신뢰하는 웹사이트 목록에서의 암호화된 연결을 검사하지 않습니다. 미리 정의된 신뢰하는 웹사이트 목록은 Kaspersky 전문가가 작성합니다. 이 목록은 애플리케이션의 안티 바이러스 데이터베이스로 업데이트합니다. Kaspersky Endpoint Security 인터페이스에서만 사전 정의된 신뢰하는 웹사이트 목록을 볼 수 있습니다. Kaspersky Security Center 콘솔에서는 목록을 볼 수 없습니다.

7. 필요시 검사 예외: 신뢰하는 주소 및 애플리케이션을 추가합니다.
8. 암호화된 연결 검사를 위한 설정을 구성합니다(아래 표를 참조하십시오).
9. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 암호화된 연결 검사를 활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.



암호화된 연결 검사 설정

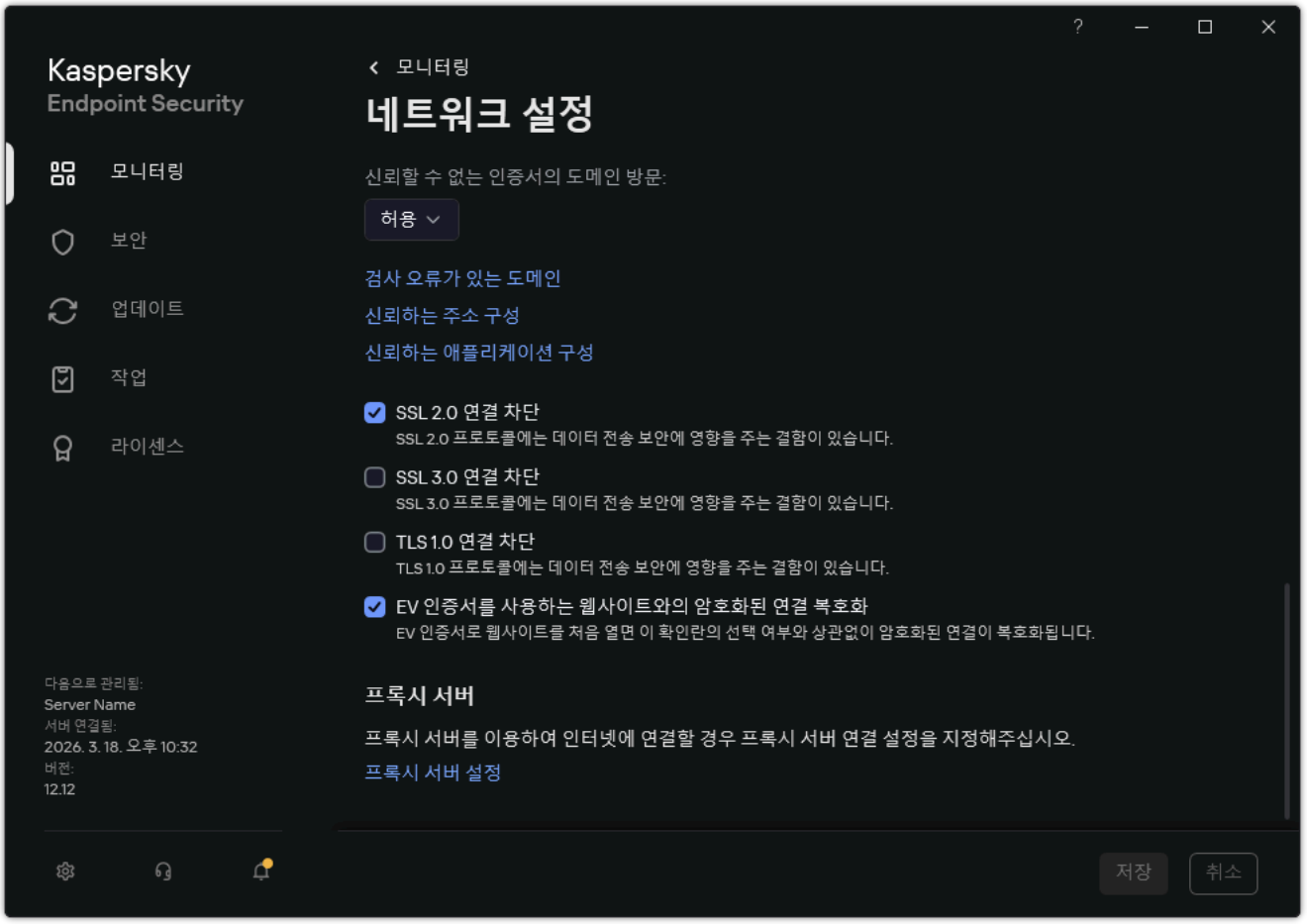
3. **암호화된 연결 검사** 블록에서 암호화된 연결 검사 모드를 선택합니다:

- **암호화된 연결 검사 안 함**. Kaspersky Endpoint Security가 `https://`로 시작하는 주소의 웹사이트 컨텐츠에 접근하지 못합니다.
- **보호 구성 요소의 요청 하에 암호화된 연결 검사**. Kaspersky Endpoint Security가 웹 위협 보호, 메일 위협 보호, 웹 제어 구성 요소의 요청을 통해서만 암호화된 트래픽을 검사합니다.
- **항상 암호화된 연결 검사**. 보호 구성 요소가 중지된 상태에서도 Kaspersky Endpoint Security가 암호화된 네트워크 트래픽을 검사합니다.

Kaspersky Endpoint Security는 트래픽 검사가 중지된 신뢰하는 애플리케이션에 따라 설정된 암호화된 연결을 검사하지 않습니다. Kaspersky Endpoint Security는 미리 정의된 신뢰하는 웹사이트 목록에서의 암호화된 연결을 검사하지 않습니다. 미리 정의된 신뢰하는 웹사이트 목록은 Kaspersky 전문가가 작성합니다. 이 목록은 애플리케이션의 안티 바이러스 데이터베이스로 업데이트합니다. Kaspersky Endpoint Security 인터페이스에서만 사전 정의된 신뢰하는 웹사이트 목록을 볼 수 있습니다. Kaspersky Security Center 콘솔에서는 목록을 볼 수 없습니다.

4. 필요시 검사 예외: 신뢰하는 주소 및 애플리케이션을 추가합니다.

5. 암호화된 연결 검사를 위한 설정을 구성합니다(아래 표를 참조하십시오).



암호화된 연결의 검사를 위한 추가 설정

6. 변경 사항을 저장합니다.

파라미터	설명
신뢰할 수 있는 루트 인증서	신뢰할 수 있는 루트 인증서 목록. Kaspersky Endpoint Security는 필요 시(새 인증 센터 배포 필요 등) 사용자 컴퓨터에 신뢰할 수 있는 루트 인증서를 설치할 수 있도록 허용합니다. 애플리케이션에서 특별한 Kaspersky Endpoint Security 인증서 스토어에 인증서를 추가할 수 있도록 허용합니다. 이때, 이 인증서는 Kaspersky Endpoint Security 애플리케이션에서만 신뢰할 수 있는 것으로 간주합니다. 다시 말해, 사용자는 브라우저에서 새 인증서가 있는 웹사이트에 액세스할 수 있습니다. 다른 애플리케이션이 해당 웹사이트에 액세스하려고 하면, 인증서 문제로 연결 오류가 발생합니다. 시스템 인증서 스토어에 추가하려면, Active Directory 그룹 정책을 사용할 수 있습니다.
신뢰할 수 없는 인증서의 도메인 방문	• **허용**. 신뢰하지 않는 인증서를 사용하는 도메인을 방문할 때 Kaspersky Endpoint Security가 네트워크 연결을 허용합니다. 브라우저에서 신뢰하지 않는 인증서를 사용하는 도메인을 열 때 Kaspersky Endpoint Security는 경고 및 해당 도메인을 방문하지 않는 것이 좋은 이유를 보여 주는 HTML 페이지를 표시합니다. 사용자는 HTML 경고 페이지의 링크를 눌러 요청한 웹사이트에 접근할 수 있습니다. 타사 애플리케이션 또는 서비스가 신뢰할 수 없는 인증서를 사용하는 도메인과 연결을 구성하면 Kaspersky Endpoint Security는 트래픽 검사를 위해 자체 인증서를 생성합니다. 새 인증서는 *신뢰하지 않음* 상태입니다. 이는 신뢰할 수 없는 연결에 대해 타사 애플리케이션에 경고하는 데 필요한데, 이 경우 HTML 페이지를 표시할 수 없고 백그라운드 모드에서 연결을 설정할 수 있기 때문입니다. • **차단**. 이 옵션을 선택하면 신뢰하지 않는 인증서를 사용하는 도메인 방문 시 Kaspersky Endpoint Security가 네트워크 연결을 차단합니다. 브라우저에서 신뢰하지 않는 인증서를 사용하는 도메인을 열 때 Kaspersky Endpoint Security는 해당 도메인이 차단된 이유를 보여 주는 HTML 페이지를 표시합니다.
암호화된 연결 검사 오류가 있는 도메인 방문	• **차단**. 이 항목을 선택하면 암호화된 연결 검사 오류 발생 시 Kaspersky Endpoint Security가 네트워크 연결을 차단합니다. • **예외 규칙에 도메인 허용 및 추가**. 이 항목을 선택하면 암호화된 연결 검사 오류 발생 시 Kaspersky Endpoint Security가 오류 발생 도메인을 검사 오류가 있는 도메인 목록에 추가하고 이 도메인을 방문할 때 암호화된 네트워크 트래픽을 감시하지 않습니다. 애플리케이션의 로컬 인터페이스에서만 암호화된 연결 검사 오류가 있는 도메인 목록을 볼 수 있습니다. 목록 내용을 지우려면 **차단**을 선택해야 합니다. Kaspersky Endpoint Security는 암호화된 연결 검사 오류에 대한 이벤트도 생성합니다.
SSL 2.0 연결 차단	이 확인란을 선택하면 애플리케이션이 SSL 2.0 프로토콜을 통해 설정된 네트워크 연결을 모니터링 및 차단합니다. 이 확인란을 선택 해제하면 애플리케이션이 SSL 2.0 프로토콜을 통해 설정된 네트워크 연결을 차단하지 않습니다. 그러나 애플리케이션은 이 프로토콜을 통한 네트워크 트래픽을 모니터링하지 않습니다.
SSL 3.0 연결 차단	이 확인란을 선택하면 애플리케이션이 SSL 3.0 프로토콜을 통해 설정된 네트워크 연결을 차단합니다. 이 확인란을 선택 해제하면 애플리케이션이 SSL 3.0 프로토콜을 통해 설정된 네트워크 연결을 차단하지 않습니다. 애플리케이션이 이 프로토콜을 통한 네트워크 트래픽을 모니터링합니다. 애플리케이션의 모든 구성 요소가 제한 없이 작동합니다.
TLS 1.0 연결 차단	이 확인란을 선택하면 애플리케이션이 TLS 1.0 프로토콜을 통해 설정된 네트워크 연결을 차단합니다. 이 확인란을 선택 해제하면 애플리케이션이 TLS 1.0 프로토콜을 통해 설정된 네트워크 연결을 차단하지 않습니다. 애플리케이션이 이 프로토콜을 통한 네트워크 트래픽을 모니터링합니다. 애플리케이션의 모든 구성 요소가 제한 없이 작동합니다.
EV 인증서를 사용하는 웹사이트와의 암호화된 연결 복호화	EV 인증서(Extended Validation Certificate)는 웹사이트의 신뢰성을 확인하고 연결 보안을 강화합니다. 브라우저는 주소 표시줄의 잠금 아이콘을 사용하여 웹사이트에 EV 인증서가 있음을 나타냅니다. 또한 브라우저가 주소 표시줄을 전부 또는 그 일부를 녹색으로 표시할 수도 있습니다. 이 확인란을 선택하면 애플리케이션이 EV 인증서를 사용하는 웹사이트에 대한 암호화된 연결을 복호화하고 모니터링하게 됩니다. 이 확인란을 선택 해제하면 애플리케이션이 HTTPS 트래픽 컨텐츠에 접근할 수 없게 됩니다. 이 경우 애플리케이션은 `https://bing.com`과 같은 웹사이트 주소를 기반으로만 HTTPS 트래픽을 모니터링합니다. EV 인증서로 웹사이트를 처음 열면, 이 확인란의 선택 여부와 상관없이 암호화된 연결이 복호화됩니다.

신뢰할 수 있는 인증서 설치

Kaspersky Endpoint Security는 필요 시(새 인증 센터 배포 필요 등) 사용자 컴퓨터에 신뢰할 수 있는 루트 인증서를 설치할 수 있도록 허용합니다. 애플리케이션에서 특별한 Kaspersky Endpoint Security 인증서 스토어에 인증서를 추가할 수 있도록 허용합니다. 이때, 이 인증서는 Kaspersky Endpoint Security 애플리케이션에서만 신뢰할 수 있는 것으로 간주합니다. 다시 말해, 사용자는 브라우저에서 새 인증서가 있는 웹사이트에 액세스할 수 있습니다. 다른 애플리케이션이 해당 웹사이트에 액세스하려고 하면, 인증서 문제로 연결 오류가 발생합니다. 시스템 인증서 스토어에 추가하려면, Active Directory 그룹 정책을 사용할 수 있습니다.

신뢰할 수 있는 루트 인증서 목록을 변경하는 것은 부모 정책의 속성에 따라 차단될 수 있습니다. 목록을 변경하려면 웹 콘솔의 신뢰 구역('자물쇠'가 잠금 해제되어야 함) 설정 변경을 허용해야 합니다.

신뢰 구역은 관리 콘솔(MMC)과 웹 콘솔에서 다르게 그룹화됩니다. 마찬가지로, 신뢰 구역 파라미터의 변경을 방지하는 방법도 다릅니다('자물쇠'가 다름). 웹 콘솔만 사용하여 애플리케이션을 관리하는 것이 좋습니다. 서로 다른 콘솔에서 신뢰 구역을 구성하는 경우 관리 플러그인이 '자물쇠'를 기본 상태로 재설정할 수 있습니다.

관리 콘솔(MMC)에 신뢰할 수 있는 루트 인증서를 설치하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 네트워크 설정**을 선택합니다.
4. **신뢰할 수 있는 루트 인증서** 블록에서 **추가** 버튼을 클릭합니다.
5. 창이 열리면 신뢰할 수 있는 인증서를 선택합니다.
   Kaspersky Endpoint Security는 PEM, DER, CRT 확장자의 인증서를 지원합니다.
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 신뢰할 수 있는 루트 인증서를 설치하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 네트워크 설정**으로 갑니다.
5. **신뢰할 수 있는 루트 인증서** 링크를 클릭합니다.
6. 창이 열리면 **추가**를 클릭하고 신뢰할 수 있는 루트 인증서를 선택합니다.
   Kaspersky Endpoint Security는 PEM, DER, CRT 확장자의 인증서를 지원합니다.
7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 신뢰할 수 있는 루트 인증서를 설치하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정 → 네트워크 설정**을 선택합니다.
3. **암호화된 연결 검사** 블록에서 **인증서 보기** 버튼을 클릭합니다.
4. 창이 열리면 **추가**를 클릭하고 신뢰할 수 있는 루트 인증서를 선택합니다.

   Kaspersky Endpoint Security는 PEM, DER, CRT 확장자의 인증서를 지원합니다.
5. 변경 사항을 저장합니다.

결과적으로 트래픽 검사 시, Kaspersky Endpoint Security가 시스템 인증서 스토어와 함께 자체 인증서 스토어도 사용합니다.

신뢰할 수 없는 인증서로 암호화된 연결 검사

설치 후 Kaspersky Endpoint Security는 신뢰하는 인증서의 시스템 저장소(Windows 인증서 저장소)에 Kaspersky 인증서를 추가합니다. Kaspersky Endpoint Security는 이 인증서를 사용하여 암호화된 연결을 검사합니다. 신뢰할 수 없는 인증서가 있는 도메인 방문 시, 해당 도메인에 대한 사용자 액세스를 허용하거나 거부할 수 있습니다(아래 지침 참조).

사용자가 신뢰할 수 없는 인증서를 사용하는 도메인을 방문하도록 허용했다면, Kaspersky Endpoint Security는 다음 작업을 수행합니다.

- *브라우저*에서 신뢰할 수 없는 인증서를 사용하는 도메인 방문 시, Kaspersky Endpoint Security는 Kaspersky 인증서를 사용하여 트래픽을 검사합니다. Kaspersky Endpoint Security는 경고 및 관련 도메인 방문을 권장하지 않는 이유에 대한 정보가 포함된 HTML 페이지를 표시합니다(아래 그림 참조). 사용자는 HTML 경고 페이지의 링크를 눌러 요청한 웹사이트에 접근할 수 있습니다. 이 링크를 따라 이동하고 나면 다음 1시간 동안은 동일 도메인에서 다른 리소스를 방문할 때 Kaspersky Endpoint Security가 신뢰하지 않는 인증서 관련 경고를 표시하지 않습니다. Kaspersky Endpoint Security는 또한 신뢰할 수 없는 인증서를 사용하는 암호화된 연결 설정에 대한 이벤트를 생성합니다.

  경우에 따라 Kaspersky Endpoint Security는 브라우저에 경고가 포함된 HTML 페이지를 기술적으로 표시할 수 없습니다(아래 그림 참조). 예를 들어 웹 리소스가 오래된 버전의 네트워크 프로토콜과 비표준 포트를 사용하는 경우입니다. 이러한 경우 Kaspersky Endpoint Security는 이 도메인에 대한 접근을 차단하고 브라우저에 표준 `ERR_CONNECTION_RESET` 창을 표시합니다. 웹 리소스에 접근하려면 예외 규칙에 도메인 추가 또는 신뢰하는 인증서를 사용합니다.

- *타사 애플리케이션 또는 서비스*가 신뢰할 수 없는 인증서를 사용하는 도메인과 연결을 구성하면 Kaspersky Endpoint Security는 트래픽 검사를 위해 자체 인증서를 생성합니다. 새 인증서는 *신뢰하지 않음* 상태입니다. 이는 신뢰할 수 없는 연결에 대해 타사 애플리케이션에 경고하는 데 필요한데, 이 경우 HTML 페이지를 표시할 수 없고 백그라운드 모드에서 연결을 설정할 수 있기 때문입니다. 따라서 타사 애플리케이션에 인증서 확인 도구가 내장되어 있을 시, 연결이 종료될 수 있습니다. 이때는 도메인 소유자에게 연락하여 신뢰할 수 있는 연결을 설정해야 합니다. 신뢰할 수 있는 연결을 설정할 수 없다면 신뢰하는 애플리케이션 목록에 해당 타사 애플리케이션을 추가할 수 있습니다. Kaspersky Endpoint Security는 또한 신뢰할 수 없는 인증서를 사용하는 암호화된 연결 설정에 대한 이벤트를 생성합니다.

관리 콘솔(MMC)에서 신뢰할 수 없는 인증서를 사용하는 암호화된 연결 검사를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 네트워크 설정**을 선택합니다.
4. **암호화된 연결 검사** 블록에서 **고급 설정** 버튼을 클릭합니다.
5. 창이 열리면 신뢰할 수 없는 인증서를 사용하는 도메인을 방문할 때의 애플리케이션 운영 모드(**허용** 또는 **차단**)를 선택합니다.
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 신뢰할 수 없는 인증서를 사용하는 암호화된 연결 검사를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 네트워크 설정**으로 갑니다.
5. **암호화된 연결 검사** 블록에서 **설정** 링크를 누릅니다.
6. 창이 열리면 신뢰할 수 없는 인증서를 사용하는 도메인을 방문할 때의 애플리케이션 운영 모드를 선택합니다: **연결 허용** 또는 **연결 차단**.
7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 신뢰할 수 없는 인증서를 사용하는 암호화된 연결 검사를 구성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정 → 네트워크 설정**을 선택합니다.

3. **암호화된 연결 검사** 블록에서 신뢰할 수 없는 인증서를 사용하는 도메인 방문 시의 애플리케이션 운영 모드(**허용** 또는 **차단**)를 선택합니다.

4. 변경 사항을 저장합니다.



신뢰하지 않는 인증서를 사용하는 도메인 방문 시 경고

자체 인증서 저장소에 Kaspersky 인증서 추가

브라우저 및 메일 클라이언트는 인증서를 사용하여 웹 리소스의 보안 및 신뢰성을 확인합니다. 인증서는 또한 웹 리소스와 사용자 간의 데이터 암호화를 제공합니다. 대부분의 브라우저 및 메일 클라이언트는 신뢰하는 인증서 저장소(Windows 인증서 저장소)를 사용합니다. 예를 들어 Google Chrome가 있습니다. 일부 브라우저 및 메일 클라이언트는 기본적으로 Windows 인증서 저장소 대신 자체 인증서 저장소를 사용합니다. 예를 들어 Firefox 및 Thunderbird가 있습니다.

설치 후 Kaspersky Endpoint Security는 신뢰하는 인증서의 시스템 저장소(Windows 인증서 저장소)에 Kaspersky 인증서를 추가합니다. Kaspersky Security Center를 조직에 배포하고 컴퓨터에 정책을 적용하는 경우 Kaspersky Endpoint Security는 자동으로 브라우저 및 메일 클라이언트의 Windows 인증서 저장소를 사용하여 이러한 애플리케이션의 트래픽을 검사합니다. 정책을 컴퓨터에 적용하지 않는 경우 브라우저 및 메일 클라이언트에서 사용할 인증서 저장소를 선택할 수 있습니다. 자체 인증서 저장소를 선택한 경우 Kaspersky 인증서를 저장소에 직접 추가합니다. 이렇게 하면 HTTPS 트래픽으로 작업할 때 오류를 방지할 수 있습니다.

Mozilla Firefox 브라우저와 Thunderbird 메일 클라이언트의 트래픽을 검사하려면 암호화된 연결 검사를 활성화해야 합니다. 암호화된 연결 검사를 비활성화하면 애플리케이션이 Mozilla Firefox 브라우저 및 Thunderbird 메일 클라이언트에서 트래픽을 검사하지 않습니다. MyOffice Mail 및 R7-Office Organizer 메일 클라이언트의 트래픽을 검사하려면 암호화된 연결 검사도 활성화해야 합니다.

브라우저 또는 메일 에이전트 자체 인증서 저장소에 인증서를 추가하기 전에 Windows 제어판(인터넷 속성)에서 Kaspersky 인증서를 내보냅니다. Kaspersky 인증서에 대한 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오. 저장소에 인증서를 추가하는 방법에 대한 자세한 내용은 Mozilla 기술 지원 웹사이트와 같은 곳에서 확인하실 수 있습니다.

애플리케이션의 로컬 인터페이스에서만 인증서 저장소를 선택할 수 있습니다.

브라우저 및 메일 클라이언트에서 암호화된 연결을 검사하기 위한 인증서 저장소를 선택하려면 다음을 수행합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정 → 네트워크 설정**을 선택합니다.
3. **암호화된 연결 검사** 블록에서 **자체 인증서 저장소가 있는 애플리케이션에서 암호화된 연결을 검사하려면 다음을 사용합니다** 확인란을 선택합니다.
4. 인증서 저장소 선택:
   - **Windows 인증서 저장소(권장)**. Kaspersky Endpoint Security 설치 중 이 저장소에 Kaspersky 루트 인증서가 추가됩니다.
   - **자체 인증서 저장소**. Mozilla Firefox 및 Thunderbird는 자체 인증서 저장소를 사용합니다. Mozilla 인증서 저장소를 선택했다면 브라우저 속성을 통해 이 저장소에 Kaspersky 루트 인증서를 직접 추가해야 합니다.

     MyOffice Mail 및 R7-Office Organizer 메일 클라이언트도 자체 인증서 저장소를 사용합니다.
5. 변경 사항을 저장합니다.

검사에서 암호화된 연결 제외

대부분의 웹 리소스는 암호화된 연결을 사용합니다. Kaspersky 전문가는 암호화된 연결 검사를 활성화할 것을 권장합니다. 암호화된 연결 검사가 작업 관련 활동에 방해된다면 *신뢰하는 주소*로 불리는 예외 규칙에 웹사이트를 추가할 수 있습니다. 이때, Kaspersky Endpoint Security는 웹 위협 보호, 메일 위협 보호, 웹 제어 구성 요소가 작업을 수행할 때 신뢰하는 웹 주소의 HTTPS 트래픽을 검사하지 않습니다.

신뢰하는 애플리케이션이 암호화된 연결을 사용하는 경우 이 애플리케이션에 대한 암호화된 연결 검사를 비활성화할 수 있습니다. 예를 들어 자체 인증서로 2단계 인증을 사용하는 클라우드 스토리지 애플리케이션에 대해 암호화된 연결 검사를 비활성화 할 수 있습니다.

신뢰하는 주소 목록의 변경은 부모 정책의 속성에 따라 차단될 수 있습니다. 목록을 변경하려면 웹 콘솔의 신뢰 구역('자물쇠'가 잠금 해제되어야 함) 설정 변경을 허용해야 합니다.

신뢰 구역은 관리 콘솔(MMC)과 웹 콘솔에서 다르게 그룹화됩니다. 마찬가지로, 신뢰 구역 파라미터의 변경을 방지하는 방법도 다릅니다('자물쇠'가 다름). 웹 콘솔만 사용하여 애플리케이션을 관리하는 것이 좋습니다. 서로 다른 콘솔에서 신뢰 구역을 구성하는 경우 관리 플러그인이 '자물쇠'를 기본 상태로 재설정할 수 있습니다.

관리 콘솔(MMC)의 암호화된 연결 검사에서 웹 주소를 제외하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 네트워크 설정**을 선택합니다.
4. **암호화된 연결 검사** 블록에서 **신뢰하는 주소 구성** 버튼을 클릭합니다.
5. **추가**를 클릭합니다.

6. 특정 도메인을 방문할 때 설정되는 암호화된 연결을 Kaspersky Endpoint Security가 검사하지 않도록 하려면 해당 도메인 이름 또는 IP 주소를 입력합니다.

   Kaspersky Endpoint Security는 도메인 이름에 마스크 입력 시 `*` 문자를 지원합니다.

   > Kaspersky Endpoint Security는 IP 주소에 대해 `*` 기호를 지원하지 않습니다. 서브넷 마스크를 사용하여 IP 주소 범위를 선택할 수 있습니다(예: 198.51.100.0/24).

   예:

   - `domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. 이 레코드는 하위 도메인을 제외합니다(예: `subdomain.domain.com`).
   - `subdomain.domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. 이 레코드는 `domain.com` 도메인을 제외합니다.
   - `*.domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://movies.domain.com`, `https://images.domain.com/page123`. 이 레코드는 `domain.com` 도메인을 제외합니다.

7. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console의 암호화된 연결 검사에서 웹 주소를 제외하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **네트워크 설정**으로 갑니다.
5. **암호화된 연결 검사** 블록에서 **신뢰하는 주소** 버튼을 클릭합니다.
6. **추가**를 클릭합니다.
7. 특정 도메인을 방문할 때 설정되는 암호화된 연결을 Kaspersky Endpoint Security가 검사하지 않도록 하려면 해당 도메인 이름 또는 IP 주소를 입력합니다.

   Kaspersky Endpoint Security는 도메인 이름에 마스크 입력 시 `*` 문자를 지원합니다.

   > Kaspersky Endpoint Security는 IP 주소에 대해 `*` 기호를 지원하지 않습니다. 서브넷 마스크를 사용하여 IP 주소 범위를 선택할 수 있습니다(예: 198.51.100.0/24).

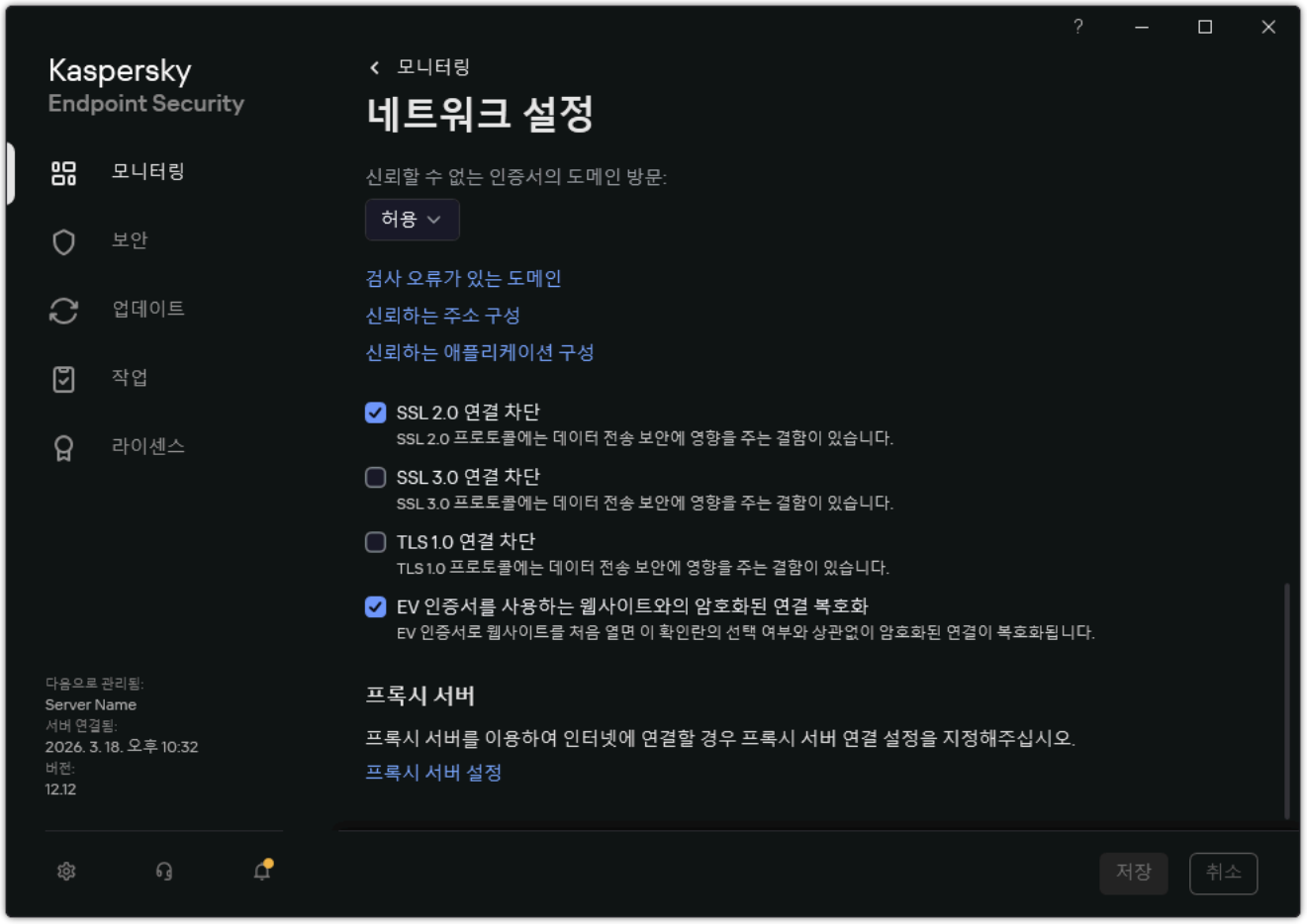
예:

- `domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. 이 레코드는 하위 도메인을 제외합니다(예: `subdomain.domain.com`).
- `subdomain.domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. 이 레코드는 `domain.com` 도메인을 제외합니다.
- `*.domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://movies.domain.com`, `https://images.domain.com/page123`. 이 레코드는 `domain.com` 도메인을 제외합니다.

8. 변경 사항을 저장합니다.

애플리케이션 인터페이스의 암호화된 연결 검사에서 웹 주소를 제외하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.



애플리케이션 네트워크 설정

3. **암호화된 연결 검사** 블록에서 **신뢰하는 주소 구성** 버튼을 클릭합니다.
4. **추가**를 클릭합니다.
5. 특정 도메인을 방문할 때 설정되는 암호화된 연결을 Kaspersky Endpoint Security가 검사하지 않도록 하려면 해당 도메인 이름 또는 IP 주소를 입력합니다.

   Kaspersky Endpoint Security는 도메인 이름에 마스크 입력 시 `*` 문자를 지원합니다.

Kaspersky Endpoint Security는 IP 주소에 대해 `*` 기호를 지원하지 않습니다. 서브넷 마스크를 사용하여 IP 주소 범위를 선택할 수 있습니다(예: 198.51.100.0/24).

예:

- `domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. 이 레코드는 하위 도메인을 제외합니다(예: `subdomain.domain.com`).
- `subdomain.domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. 이 레코드는 `domain.com` 도메인을 제외합니다.
- `*.domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://movies.domain.com`, `https://images.domain.com/page123`. 이 레코드는 `domain.com` 도메인을 제외합니다.

6. 변경 사항을 저장합니다.

기본적으로 Kaspersky Endpoint Security는 오류가 발생할 때 암호화된 연결을 검사하지 않으며 *검사 오류가 있는 도메인* 목록에 웹사이트를 추가합니다. Kaspersky Endpoint Security는 각 사용자에 대해 별도의 목록을 컴파일하고 Kaspersky Security Center로 데이터를 전송하지 않습니다. 검사 오류가 발생할 때 연결 차단을 활성화할 수 있습니다. 애플리케이션의 로컬 인터페이스에서만 암호화된 연결 검사 오류가 있는 도메인 목록을 볼 수 있습니다.

검사 오류가 있는 도메인 목록을 보려면 다음을 수행합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.
3. **암호화된 연결 검사** 블록에서 **검사 오류가 있는 도메인** 버튼을 클릭합니다.

검사 오류가 있는 도메인 목록이 열립니다. 목록을 재설정하려면, 정책에서 검사 오류가 발생할 때 연결 차단을 활성화하고 정책을 적용한 다음 파라미터를 초기 값으로 재설정하고 정책을 다시 적용하십시오.

Kaspersky 전문가는 Kaspersky Endpoint Security가 애플리케이션 설정에 관계없이 확인하지 않는 신뢰하는 웹사이트인 *전역 예외* 목록을 만듭니다.

암호화된 트래픽 검사에서 예외를 확인하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.
3. **암호화된 연결 검사** 블록에서 신뢰하는 웹사이트 링크 목록을 클릭합니다.

Kaspersky 전문가가 편집한 웹사이트 목록이 열립니다. Kaspersky Endpoint Security는 목록에 있는 웹사이트에 대해 보호된 연결을 검사하지 않습니다. Kaspersky Endpoint Security 데이터베이스와 모듈이 업데이트되면 이 목록도 업데이트될 수 있습니다.

데이터 완전 삭제

Kaspersky Endpoint Security에서는 사용자 컴퓨터에 있는 데이터를 원격으로 삭제할 수 있습니다.

Kaspersky Endpoint Security는 다음과 같이 데이터를 삭제합니다:

- 숨김 모드로 데이터를 삭제
- 하드 드라이브 및 이동식 드라이브에 있는 데이터를 삭제
- 컴퓨터에 있는 모든 사용자 계정에 대한 데이터를 삭제

Kaspersky Endpoint Security는 사용 중인 라이센스 유형에 상관없이 라이센스가 만료되었더라도 *데이터 완전 삭제* 작업을 수행합니다.

데이터 완전 삭제 모드

이 작업을 수행하면 다음 모드로 데이터를 삭제할 수 있습니다:

- 데이터 즉시 삭제.

  이 모드에서는 예를 들어 오래된 데이터를 삭제하여 디스크에 여유 공간을 확보할 수 있습니다.

- 연기된 데이터 삭제.

  이 모드는 예를 들어 노트북을 도난 또는 분실한 경우 노트북의 데이터를 보호하기 위해 사용됩니다. 노트북이 회사 네트워크 경계를 벗어나고 오랫동안 Kaspersky Security Center와 동기화되지 않는 경우 자동으로 데이터를 삭제하도록 구성할 수 있습니다.

작업 속성에서 데이터를 삭제하기 위한 스케줄을 설정할 수 없습니다. 작업을 직접 시작한 직후에만 데이터를 삭제하거나, Kaspersky Security Center와 연결이 없는 경우에만 지연된 데이터 삭제를 구성할 수 있습니다.

제한 사항

데이터 완전 삭제에는 다음과 같은 제한이 있습니다:

- Kaspersky Security Center 관리자만이 *데이터 완전 삭제* 작업을 관리할 수 있습니다. Kaspersky Endpoint Security의 로컬 인터페이스에서는 작업을 구성하거나 시작할 수 없습니다.
- NTFS 파일 시스템의 경우 Kaspersky Endpoint Security는 주 데이터 스트림의 이름만 삭제합니다. 대체 데이터 스트림 이름은 삭제할 수 없습니다.
- 심볼릭 링크 파일을 삭제하면 Kaspersky Endpoint Security는 경로에 심볼릭 링크가 지정된 파일도 삭제합니다.

데이터 완전 삭제 작업 생성

사용자 컴퓨터에서 데이터를 삭제하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **데이터 완전 삭제**를 선택합니다.
   c. **작업 이름** 필드에 *데이터 완전 삭제(도난 방지)*와 같은 간단한 설명을 입력합니다.
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.

   새 컴퓨터가 작업 범위 내에서 관리 그룹에 추가되었고 새 컴퓨터를 추가한지 5분 내에 데이터 즉시 삭제 작업이 완료된 경우에 한해 이 작업은 새 컴퓨터에서만 실행됩니다.

5. 마법사를 끝냅니다.
   작업 목록에 새 작업이 표시됩니다.
6. Kaspersky Endpoint Security의 **데이터 완전 삭제** 작업을 클릭합니다.
   작업 속성 창이 열립니다.
7. **애플리케이션 설정** 탭을 선택합니다.
8. 데이터 삭제 방법을 선택합니다:
   - **운영 체제를 사용해 삭제**. Kaspersky Endpoint Security가 운영 체제 리소스를 사용하여 파일을 휴지통으로 보내지 않고 파일을 삭제합니다.
   - **완전 삭제, 복구 불가능**. Kaspersky Endpoint Security가 임의 데이터로 파일을 덮어씁니다. 데이터를 삭제한 후 복원하는 것은 사실상 불가능합니다.
9. 데이터 삭제를 연기하려면 **다음보다 긴 시간 동안 Kaspersky Security Center와 연결할 수 없을 때 자동으로 데이터 완전 삭제: N일** 확인란을 선택합니다. 기간 정의.

   정의된 기간 동안 Kaspersky Security Center에 연결이 이루어지지 않을 때마다 연기된 데이터 삭제 작업이 수행됩니다.

연기된 데이터 삭제를 구성할 때 직원마다 작업 스케줄이 다를 수 있음에 유의하십시오. 오프라인 사용자의 업무 스케줄도 고려하시기 바랍니다. 오프라인 컴퓨터 및 이동 사용자 작업과 관련한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.

컴퓨터의 전원이 꺼져 있고 구성한 시간보다 오랫동안 연결되지 않았다면, 컴퓨터의 전원을 켰을 때 Kaspersky Endpoint Security가 데이터를 즉시 삭제하지 않습니다. 애플리케이션이 Kaspersky Security Center와의 동기화를 1시간 동안 기다립니다. 이는 휴가 등을 이유로 컴퓨터 전원을 끈 사용자의 컴퓨터에서 데이터가 무단 삭제되는 것을 방지하기 위함입니다.

이 확인란을 선택 해제하면 Kaspersky Security Center와 동기화가 이루어진 직후에 이 작업이 수행됩니다.

10. 삭제할 개체 목록 생성:

- **폴더**. Kaspersky Endpoint Security는 폴더와 하위 폴더 내 모든 파일을 삭제합니다. Kaspersky Endpoint Security는 폴더 경로 입력을 위한 마스크를 지원하지 않습니다.
- **파일 확장자로**. Kaspersky Endpoint Security는 이동식 드라이브를 포함해 모든 컴퓨터 드라이브에 있는 지정된 확장자의 파일을 검색합니다. 여러 확장자를 지정하려면 "`;`" 또는 "`,`" 문자를 사용합니다.
- **사전 정의된 범위**. Kaspersky Endpoint Security는 다음 영역에서 파일을 삭제합니다.
  - **문서**. 운영 체제의 표준 *문서* 폴더에 있는 파일 및 해당 하위 폴더.
  - **쿠키**. 브라우저가 사용자의 방문 웹사이트 데이터를 저장하는 파일(예: 사용자 인증 데이터).
  - **바탕 화면**. 운영 체제의 표준 *바탕 화면* 폴더에 있는 파일 및 해당 하위 폴더.
  - **임시 Internet Explorer 파일**. 웹 페이지 사본, 이미지 및 미디어 파일과 같은 Internet Explorer 작동과 관련된 임시 파일.
  - **임시 파일**. 컴퓨터에 설치된 애플리케이션 작동과 관련된 임시 파일. 예를 들어 Microsoft Office 애플리케이션은 문서의 백업 복사본이 포함된 임시 파일을 만듭니다.
  - **Outlook 파일**. 데이터 파일(PST), 오프라인 데이터 파일(OST), 오프라인 주소록 파일(OAB) 및 개인 주소록 파일(PAB)과 같은 Outlook 메일 클라이언트 작동과 관련된 파일.
  - **사용자 프로필**. 로컬 사용자 계정을 위한 운영 체제 설정을 저장하는 파일 및 폴더 세트.

각 탭에서 삭제할 개체 목록을 생성할 수 있습니다. Kaspersky Endpoint Security는 작업이 완료되면 통합 목록을 생성하고 이 목록에서 파일을 삭제합니다.

Kaspersky Endpoint Security 작동에 필요한 파일은 삭제할 수 없습니다.

11. 변경 사항을 저장합니다.

12. 작업 옆의 확인란을 선택합니다.

13. **시작**을 클릭합니다.

그러면 사용자 컴퓨터에 저장된 데이터가 선택한 모드(즉시 또는 연결 부재 시)에 따라 삭제됩니다. 사용자가 현재 사용 중인 이유 등으로 Kaspersky Endpoint Security가 파일을 삭제할 수 없는 경우 애플리케이션이 해당 파일 삭제를 다시 시도하지 않습니다. 데이터 삭제를 완료하려면 이 작업을 다시 실행하십시오.

컴퓨터 제어

웹 제어

웹 제어는 웹 리소스에 대한 사용자의 접근을 관리합니다. 이렇게 하면 트래픽을 줄이고 업무 시간을 부적절하게 사용하는 것도 줄일 수 있습니다. 사용자가 웹 제어에 의해 제한되는 웹사이트를 열려고 하면 Kaspersky Endpoint Security가 접근을 차단하거나 경고를 표시합니다(아래 그림 참조).

웹 제어를 사용하려면 애플리케이션의 초기 구성을 완료해야 합니다:

- HTTPS 트래픽 모니터링의 경우, 암호화된 연결 검사를 활성화합니다(기본적으로 활성화되어 있습니다).
- Kaspersky Endpoint Security가 모니터링해야 하는 포트를 선택합니다(기본적으로 애플리케이션은 모든 포트를 모니터링합니다).
- Kaspersky Endpoint Security가 트래픽을 모니터링할 애플리케이션을 선택합니다. 대부분의 브라우저는 Kaspersky에서 권장하는 애플리케이션 목록에 이미 있습니다. 사용 중인 브라우저가 목록에 없는 경우 수동으로 추가하세요.
- 웹 트래픽에 웹 페이지 상호 작용 스크립트 삽입하는 것을 권장합니다(기본적으로 스크립트 삽입은 비활성화되어 있습니다). 이 스크립트를 사용하면 애플리케이션 이벤트 로그, OS 이벤트 로그 및 리포트에 대한 웹 제어 이벤트를 등록할 수 있습니다.

웹사이트 접근을 관리하는 방법

웹 제어에서는 다음 방법으로 웹사이트에 대한 접근을 구성할 수 있습니다:

- **웹사이트 카테고리**. 웹사이트는 Kaspersky Security Network 클라우드 서비스, 휴리스틱 분석 및 알려진 웹사이트 데이터베이스(애플리케이션 데이터베이스에 포함)에 따라 분류됩니다. 예를 들어, *소셜 네트워크* 카테고리 또는 다른 카테고리에 대한 사용자 접근을 제한할 수 있습니다.
- **데이터 유형**. 이미지를 숨기는 등 웹사이트의 데이터에 대한 사용자 접근을 제한할 수 있습니다. Kaspersky Endpoint Security는 파일 확장자가 아니라 파일 형식에 따라 데이터 유형을 결정합니다.

  > Kaspersky Endpoint Security는 압축 파일에 포함된 파일을 검사하지 않습니다. 예를 들어, 이미지 파일이 압축 파일에 있는 경우 Kaspersky Endpoint Security는 *그래픽* 데이터 유형이 아니라 *압축 파일* 데이터 유형을 식별합니다.

- **개별 주소**. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다.

여러 가지 방법을 동시에 사용하여 웹사이트에 대한 접근을 제어할 수 있습니다. 예를 들어 *웹 기반 이메일* 웹사이트 카테고리에 대해서만 *오피스 애플리케이션 파일* 데이터 유형에 대한 접근을 제한할 수 있습니다.

웹사이트 접속 규칙

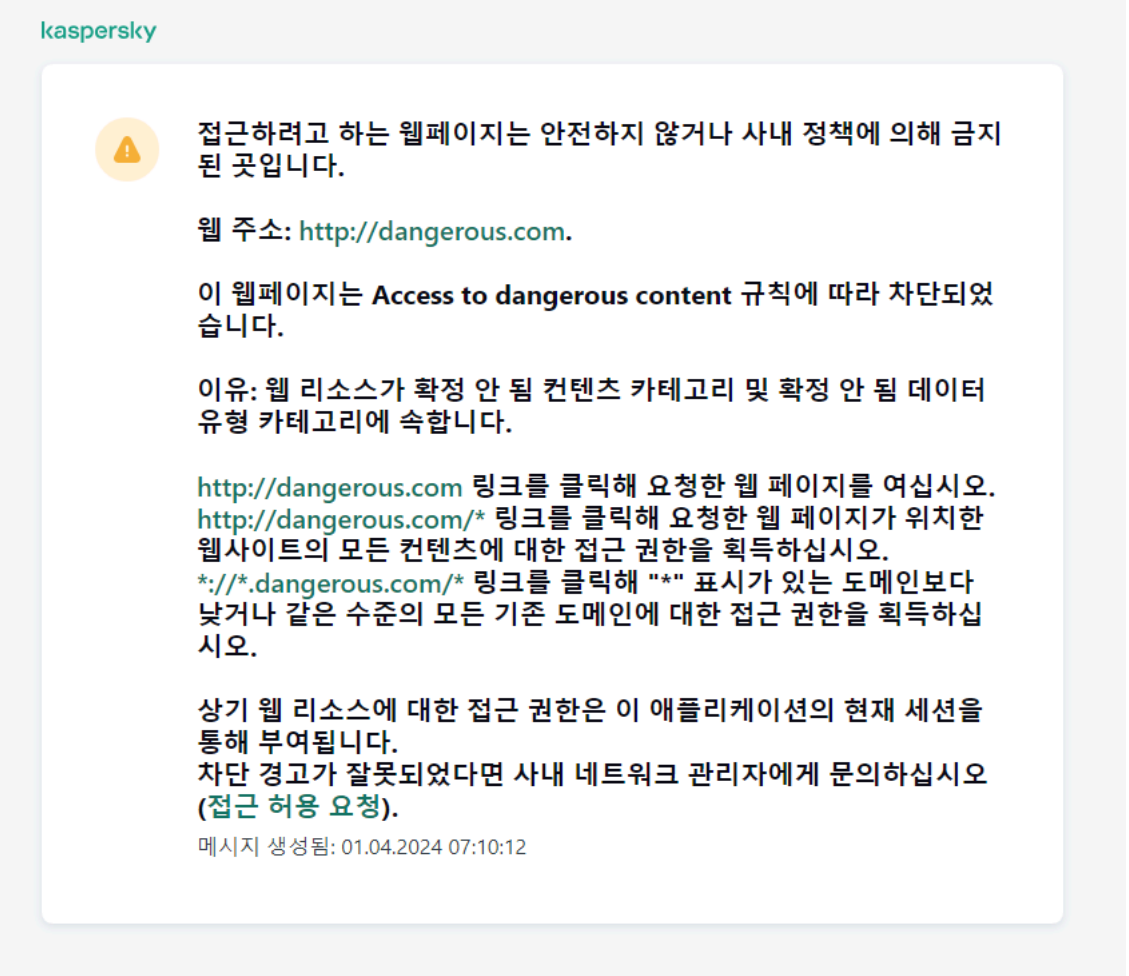
웹 제어는 *접근 규칙*을 사용하여 웹사이트에 대한 사용자 접근을 관리합니다. 웹사이트 접근 규칙을 위한 다음과 같은 고급 설정을 구성할 수 있습니다:

- 규칙을 적용할 사용자
  예를 들어, IT 부서를 제외한 회사의 모든 사용자의 브라우저를 통한 인터넷 접근을 제한할 수 있습니다.
- 규칙 스케줄
  예를 들어, 업무 시간 동안에만 브라우저를 통한 인터넷 접근을 제한할 수 있습니다.

접근 규칙 우선 순위

각 규칙에는 우선 순위가 있습니다. 규칙 목록에서 순위가 높을수록 그 우선 순위도 높습니다. 웹사이트가 여러 규칙에 추가된 경우 웹 제어는 가장 높은 우선 순위를 가진 규칙에 따라 웹사이트에 대한 접근을 제어합니다. 예를 들어 Kaspersky Endpoint Security가 회사 포털을 소셜 네트워크로 식별할 수 있습니다. 소셜 네트워크에 대한 접근을 제한하고 회사 웹 포털에 대한 접근을 허용하려면 두 가지 규칙 즉, *소셜 네트워크* 웹사이트 카테고리에 대한 차단 규칙과 회사 웹 포털에 대한 허용 규칙을 하나씩 생성하면 됩니다. 회사 웹 포털에 대한 접근 규칙은 소셜 네트워크에 대한 접근 규칙보다 우선 순위가 높아야 합니다.





웹 제어 메시지

웹 리소스 접근 규칙 추가

*웹 리소스 접근 규칙*은 사용자가 웹 리소스에 방문할 때 Kaspersky Endpoint Security가 적용되는 필터 및 동작 세트입니다. 접근 규칙에는 규칙 스케줄이 포함될 수 있습니다.

시스템이 불안정해 질 수 있으므로 웹 리소스 접근 규칙을 1000개 이상 생성하는 것은 권장하지 않습니다.

웹 리소스 접근 규칙이란 사용자가 규칙 스케줄에 표시된 시간 동안 규칙에 설명되어 있는 웹 리소스를 방문할 때 Kaspersky Endpoint Security에서 수행하는 필터 및 처리의 집합입니다. 필터를 사용하면 웹 제어 구성 요소에 의해 접근이 제어되는 웹 리소스 풀을 정확하게 지정할 수 있습니다.

다음과 같은 필터를 사용할 수 있습니다.

- **컨텐츠별 필터링**. 웹 제어는 컨텐츠 및 데이터 유형별로 웹 리소스를 분류합니다. 해당 카테고리에 정의된 유형에 속하는 컨텐츠 및 데이터가 포함된 웹 리소스에 대한 사용자 접근을 제어할 수 있습니다. 선택한 컨텐츠 카테고리 및/또는 데이터 유형 카테고리에 속하는 웹리소스를 방문하는 경우 Kaspersky Endpoint Security는 규칙에 지정된 처리를 수행합니다.

- **웹 리소스 주소별 필터링**. 모든 웹 리소스 주소 또는 개별 웹 리소스 주소 및/또는 웹 리소스 주소 그룹에 대한 사용자 접근을 제어할 수 있습니다.

  컨텐츠별 필터링 및 웹 리소스 주소별 필터링이 설정된 경우 지정된 웹 리소스 주소 및/또는 주소 그룹이 선택한 컨텐츠 카테고리나 데이터 유형 카테고리에 속하면 Kaspersky Endpoint Security는 선택한 컨텐츠 및/또는 데이터 유형 카테고리에서 모든 웹 리소스에 대한 접근을 제어하지 않습니다. 대신 애플리케이션은 지정된 웹 리소스 주소 및/또는 주소 그룹에 대한 접근만 제어합니다.

- **사용자 및 사용자 그룹 이름별 필터링**. 웹 리소스 접근이 규칙에 따라 제어되는 사용자 또는 사용자 그룹의 이름을 지정할 수 있습니다.

- **규칙 스케줄**. 규칙 스케줄을 지정할 수 있습니다. 규칙 스케줄은 Kaspersky Endpoint Security가 규칙이 적용되는 웹 리소스에 대한 접근을 감시하는 시간을 결정합니다.

Kaspersky Endpoint Security가 설치되면 웹 제어 구성 요소의 규칙 목록이 빈 상태에서 채워집니다. *기본 규칙*은 사전 설정되어 있습니다. 이 규칙은 다른 규칙이 적용되지 않는 웹사이트에 적용되며 모든 사용자의 이러한 웹사이트 접근을 허용하거나 차단합니다.

각 규칙에는 우선 순위가 있습니다. 규칙 목록에서 순위가 높을수록 그 우선 순위도 높습니다. 웹사이트가 여러 규칙에 추가된 경우 웹 제어는 가장 높은 우선 순위를 가진 규칙에 따라 웹사이트에 대한 접근을 제어합니다. 예를 들어 Kaspersky Endpoint Security가 회사 포털을 소셜 네트워크로 식별할 수 있습니다. 소셜 네트워크에 대한 접근을 제한하고 회사 웹 포털에 대한 접근을 허용하려면 두 가지 규칙 즉, *소셜 네트워크* 웹사이트 카테고리에 대한 차단 규칙과 회사 웹 포털에 대한 허용 규칙을 하나씩 생성하면 됩니다. 회사 웹 포털에 대한 접근 규칙은 소셜 네트워크에 대한 접근 규칙보다 우선 순위가 높아야 합니다.

관리 콘솔(MMC)에서 웹 리소스 접근 규칙을 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보안 제어 → 웹 제어**를 선택합니다.
4. **웹 제어** 확인란을 선택합니다.
5. **웹 제어 설정** 블록에서 **추가** 버튼을 클릭합니다.
   웹사이트 접근 규칙 창이 열립니다.
6. 웹 리소스 접근 규칙을 구성합니다(아래 표 참조).
7. 정책이 적용된 직후 웹 제어가 금지된 웹 리소스와의 연결을 종료하도록 하려면 **규칙이 적용된 후 활성 사용자 브라우저 세션 종료** 확인란을 선택합니다.

> 웹 제어를 사용하면 웹 브라우저에서만 웹 리소스 연결을 즉시 해제할 수 있습니다. 다른 애플리케이션은 웹 제어가 새 연결만 제한합니다.

이 확인란을 선택하지 않으면, 웹 제어는 금지된 웹 리소스에 대한 새로운 연결만 제한합니다. 웹 제어는 활성화된 연결을 종료하지 않습니다.

8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 웹 리소스 접근 규칙을 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **웹 제어**로 이동합니다
5. **웹 제어 활성화됨** 토글을 켭니다.
6. **규칙 목록** 블록에서 **추가** 버튼을 클릭합니다.
7. 웹 리소스 접근 규칙을 구성합니다(아래 표 참조).
8. 정책이 적용된 직후 웹 제어가 금지된 웹 리소스와의 연결을 종료하도록 하려면 **규칙이 적용된 후 활성 사용자 브라우저 세션 종료** 확인란을 선택합니다.

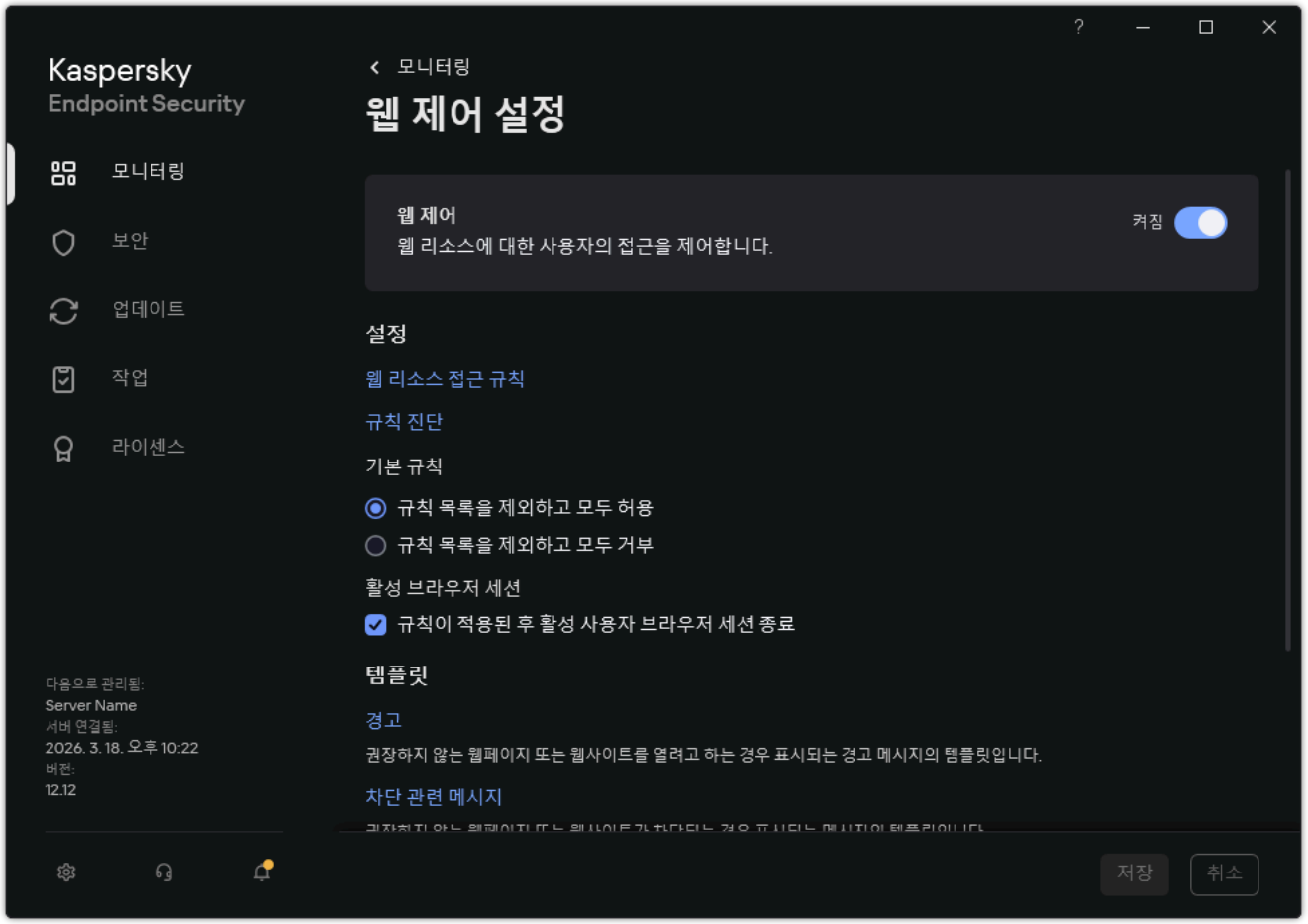
   웹 제어를 사용하면 웹 브라우저에서만 웹 리소스 연결을 즉시 해제할 수 있습니다. 다른 애플리케이션은 웹 제어가 새 연결만 제한합니다.

   이 확인란을 선택하지 않으면, 웹 제어는 금지된 웹 리소스에 대한 새로운 연결만 제한합니다. 웹 제어는 활성화된 연결을 종료하지 않습니다.

9. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 웹 리소스 접근 규칙을 추가하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **웹 제어**를 선택합니다.



웹 제어 설정

3. **웹 제어** 토글을 켭니다.
4. **설정** 블록에서, **웹 리소스 접근 규칙** 버튼을 클릭합니다.
5. 열리는 창에서 **추가** 버튼을 누릅니다.
   웹사이트 접근 규칙 창이 열립니다.
6. 웹 리소스 접근 규칙을 구성합니다(아래 표 참조).
7. 정책이 적용된 직후 웹 제어가 금지된 웹 리소스와의 연결을 종료하도록 하려면 **규칙이 적용된 후 활성 사용자 브라우저 세션 종료** 확인란을 선택합니다.

   웹 제어를 사용하면 웹 브라우저에서만 웹 리소스 연결을 즉시 해제할 수 있습니다. 다른 애플리케이션은 웹 제어가 새 연결만 제한합니다.

   이 확인란을 선택하지 않으면, 웹 제어는 금지된 웹 리소스에 대한 새로운 연결만 제한합니다. 웹 제어는 활성화된 연결을 종료하지 않습니다.
8. 변경 사항을 저장합니다.

그러면 새로운 웹 제어 규칙이 목록에 추가됩니다. 필요한 경우 웹 제어 규칙의 우선 순위를 변경합니다. 또한 토글 스위치로 목록에서 제거하지 않고도 웹 리소스 접근 규칙을 언제든지 중지할 수 있습니다.

파라미터	설명
규칙 이름	웹 제어 규칙의 이름입니다.
상태	• **켜짐**. • **꺼짐**. 언제든지 토글로 웹 리소스 접근 규칙을 중지할 수 있습니다.
처리	• **허용**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 허용합니다. • **차단**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 차단하고 웹사이트 접근 거부 메시지를 표시합니다. • **경고**. 사용자가 규칙과 일치하는 웹 리소스에 접근하려 할 때 웹 제어는 웹 리소스 방문을 철회할 수 없다는 경고를 표시합니다. 사용자는 경고 메시지의 링크를 사용하여 요청한 웹 리소스에 대한 접근 권한을 얻을 수 있습니다.
필터 콘텐츠	• **컨텐츠 카테고리별**. 카테고리 (*소셜 네트워크* 카테고리 등)별로 웹 리소스에 대한 사용자의 접근을 제어할 수 있습니다. • **데이터 유형별**. 게시된 데이터의 특정 데이터 유형(*그래픽* 등)을 기반으로 웹 리소스에 대한 사용자의 접근을 제어할 수 있습니다.
주소	• **모든 주소로**. 웹 제어는 주소별로 웹 리소스를 필터링하지 않습니다. • **개별 주소로**. 웹 제어는 목록에서 웹 리소스 주소만 필터링합니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다. 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. 암호화된 연결 검사를 중지하면 HTTPS 프로토콜에 대해 서버 이름으로만 필터링할 수 있습니다.
사용자	• **모든 사용자로**. 웹 제어는 특정 사용자에 대한 웹 리소스를 필터링하지 않습니다. • **개별 사용자 및/또는 그룹으로**. 웹 제어는 특정 사용자에 대해서만 웹 리소스를 필터링합니다. 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.
규칙 스케줄	규칙 스케줄은 Kaspersky Endpoint Security가 규칙이 적용되는 웹 리소스에 대한 접근을 감시하는 시간을 결정합니다. 예를 들어, 업무 시간 동안에만 브라우저를 통한 인터넷 접근을 제한할 수 있습니다.

웹 리소스 주소별 필터링

개별 웹 리소스 접근을 제어하려면 웹 제어 규칙을 만들고, 웹 주소 목록을 만들고, 웹 제어 동작을 선택해야 합니다. 웹 주소 목록을 만들 때 URL 주소를 입력하거나 마스크를 사용해야 합니다.

규칙에는 규칙 스케줄과 규칙이 적용되는 사용자 목록이 포함될 수 있습니다. 예를 들어 근무 시간만으로 웹사이트 접근을 제한하거나 특정 그룹의 사용자에게 웹사이트 방문을 허용할 수 있습니다.

관리 콘솔(MMC)에서 웹 리소스 주소 필터를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보안 제어 → 웹 제어**를 선택합니다.
4. **웹 제어** 확인란을 선택합니다.
5. **웹 제어 설정** 블록에서 **추가** 버튼을 클릭합니다.
   웹사이트 접근 규칙 창이 열립니다.
6. 웹 리소스 접근 규칙을 구성합니다:
   a. **이름** 필드에서 규칙의 이름을 입력합니다.
   b. **주소에 적용** 드롭다운 목록에서 **개별 주소로** 옵션을 선택합니다.

c. 웹 리소스 주소 목록을 만듭니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다.

> 암호화된 연결 검사를 중지하면 HTTPS 프로토콜에 대해 서버 이름으로만 필터링할 수 있습니다.

d. **사용자에게 적용** 드롭다운 목록에서 사용자에 해당하는 필터를 선택합니다:

- **모든 사용자로**. 웹 제어는 주소별로 웹 리소스를 필터링하지 않습니다.
- **개별 사용자 또는 그룹으로**. 웹 제어는 목록에서 웹 리소스 주소만 필터링합니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다. 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.

e. **처리** 드롭다운 목록에서 옵션을 선택합니다:

- **허용**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 허용합니다.
- **차단**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 차단하고 웹사이트 접근 거부 메시지를 표시합니다.
- **경고**. 사용자가 규칙과 일치하는 웹 리소스에 접근하려 할 때 웹 제어는 웹 리소스 방문을 철회할 수 없다는 경고를 표시합니다. 사용자는 경고 메시지의 링크를 사용하여 요청한 웹 리소스에 대한 접근 권한을 얻을 수 있습니다.

f. **규칙 스케줄** 드롭다운 목록에서 스케줄을 선택하거나 새 스케줄을 생성합니다.

7. 정책이 적용된 직후 웹 제어가 금지된 웹 리소스와의 연결을 종료하도록 하려면 **규칙이 적용된 후 활성 사용자 브라우저 세션 종료** 확인란을 선택합니다.

> 웹 제어를 사용하면 웹 브라우저에서만 웹 리소스 연결을 즉시 해제할 수 있습니다. 다른 애플리케이션은 웹 제어가 새 연결만 제한합니다.

이 확인란을 선택하지 않으면, 웹 제어는 금지된 웹 리소스에 대한 새로운 연결만 제한합니다. 웹 제어는 활성화된 연결을 종료하지 않습니다.

8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 웹 리소스 주소 필터를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **웹 제어**로 이동합니다
5. **웹 제어 활성화됨** 토글을 켭니다.
6. **규칙 목록** 블록에서 **추가** 버튼을 클릭합니다.

7. 웹 리소스 접근 규칙을 구성합니다:

   a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.

   b. 웹 리소스 접근 규칙에 대해 **활성화됨** 상태를 선택합니다.
   토글 스위치로 목록에서 제거하지 않고도 웹 리소스 접근 규칙을 언제든지 중지할 수 있습니다.

   c. **처리** 블록에서 관련 옵션을 선택합니다.

   - **허용**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 허용합니다.
   - **차단**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 차단하고 웹사이트 접근 거부 메시지를 표시합니다.
   - **알림**. 사용자가 규칙과 일치하는 웹 리소스에 접근하려 할 때 웹 제어는 웹 리소스 방문을 철회할 수 없다는 경고를 표시합니다. 사용자는 경고 메시지의 링크를 사용하여 요청한 웹 리소스에 대한 접근 권한을 얻을 수 있습니다.

   d. **범위**에서 **개별 웹사이트** 옵션을 선택합니다.

   e. 컨텐츠 필터를 구성합니다.

   - **개별 주소**. 웹 리소스 주소 목록을 만듭니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다.

     > 암호화된 연결 검사를 중지하면 HTTPS 프로토콜에 대해 서버 이름으로만 필터링할 수 있습니다.

   - **데이터 유형**. 게시된 데이터의 특정 데이터 유형(*그래픽* 등)을 기반으로 웹 리소스에 대한 사용자의 접근을 제어할 수 있습니다.

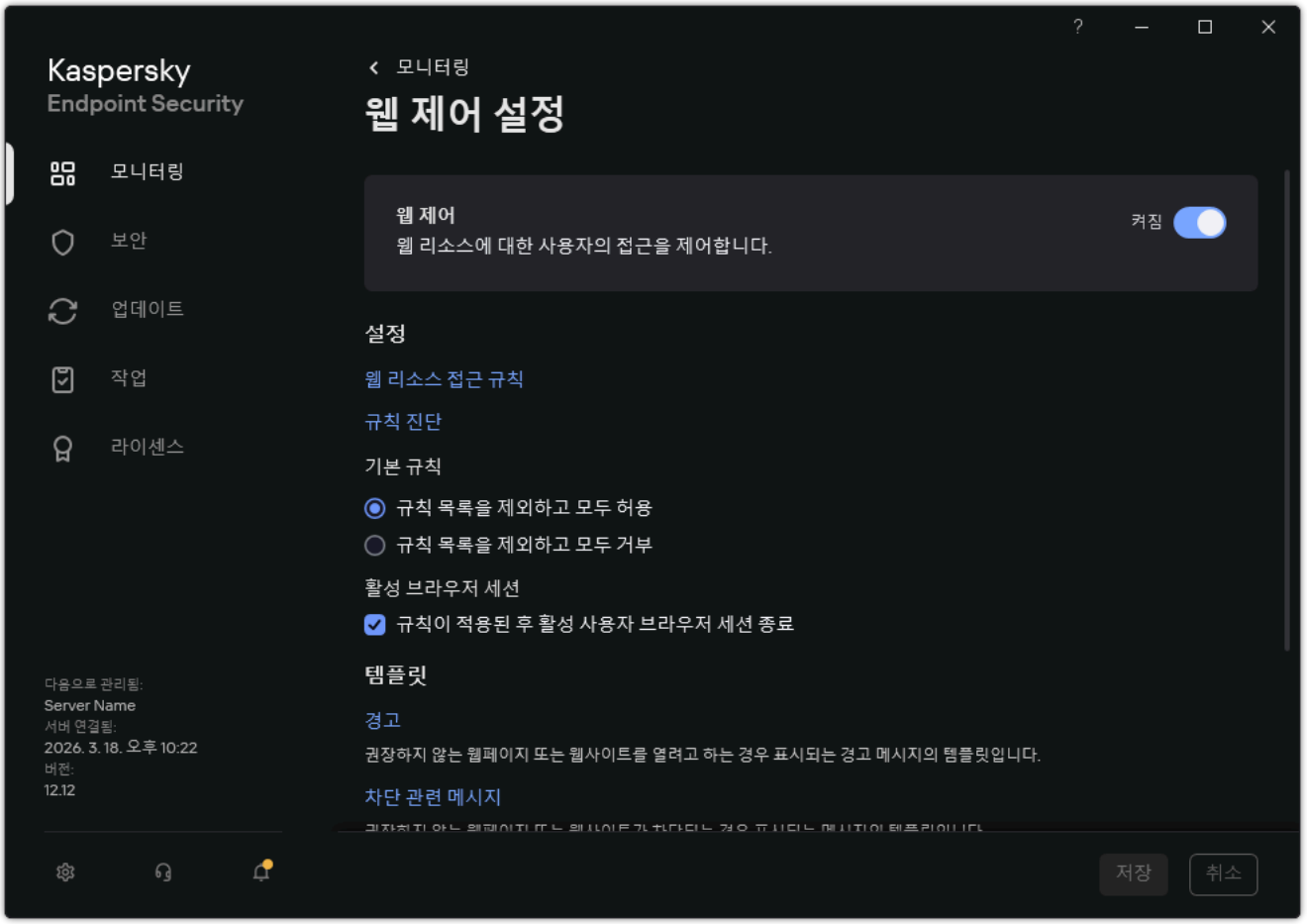
   f. **사용자 또는 그룹**에서 웹 제어를 통해 규칙을 적용할 사용자를 선택합니다.
   웹 제어는 목록에서 웹 리소스 주소만 필터링합니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.

   g. **접근 스케줄** 블록에서 스케줄을 선택하거나 새 스케줄을 생성합니다.

8. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 웹 리소스 주소 필터를 활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **웹 제어**를 선택합니다.



웹 제어 설정

3. **설정** 블록에서, **웹 리소스 접근 규칙** 버튼을 클릭합니다.
4. 열리는 창에서 **추가** 버튼을 누릅니다.
   웹사이트 접근 규칙 창이 열립니다.
5. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.
6. 웹 리소스 접근 규칙에 대해 **켜짐** 상태를 선택합니다.
   언제든지 토글로 웹 리소스 접근 규칙을 중지할 수 있습니다.
7. **처리** 블록에서 관련 옵션을 선택합니다.
   - **허용**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 허용합니다.
   - **차단**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 차단하고 웹사이트 접근 거부 메시지를 표시합니다.
   - **경고**. 사용자가 규칙과 일치하는 웹 리소스에 접근하려 할 때 웹 제어는 웹 리소스 방문을 철회할 수 없다는 경고를 표시합니다. 사용자는 경고 메시지의 링크를 사용하여 요청한 웹 리소스에 대한 접근 권한을 얻을 수 있습니다.
8. **주소**에서 **개별 주소로** 옵션을 선택합니다.

웹 리소스 주소 목록을 만듭니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다.

> 암호화된 연결 검사를 중지하면 HTTPS 프로토콜에 대해 서버 이름으로만 필터링할 수 있습니다.

9. **사용자** 블록에서 사용자에 대한 관련 필터를 선택합니다:

   - **모든 사용자로**. 웹 제어는 특정 사용자에 대한 웹 리소스를 필터링하지 않습니다.
   - **개별 사용자 및/또는 그룹으로**. 웹 제어는 목록에서 웹 리소스 주소만 필터링합니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다. 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.

10. **규칙 스케줄** 드롭다운 목록에서 스케줄을 선택하거나 새 스케줄을 생성합니다.

11. 정책이 적용된 직후 웹 제어가 금지된 웹 리소스와의 연결을 종료하도록 하려면 **규칙이 적용된 후 활성 사용자 브라우저 세션 종료** 확인란을 선택합니다.

    > 웹 제어를 사용하면 웹 브라우저에서만 웹 리소스 연결을 즉시 해제할 수 있습니다. 다른 애플리케이션은 웹 제어가 새 연결만 제한합니다.

    이 확인란을 선택하지 않으면, 웹 제어는 금지된 웹 리소스에 대한 새로운 연결만 제한합니다. 웹 제어는 활성화된 연결을 종료하지 않습니다.

12. 변경 사항을 저장합니다.

그러면 새로운 웹 제어 규칙이 목록에 추가됩니다. 필요한 경우 웹 제어 규칙의 우선 순위를 변경합니다. 또한 토글 스위치로 목록에서 제거하지 않고도 웹 리소스 접근 규칙을 언제든지 중지할 수 있습니다.

웹 리소스 컨텐츠별 필터링

웹 리소스 컨텐츠별 접근을 제어하려면 웹 제어는 카테고리 필터 및 데이터 유형 필터를 제공합니다.

웹사이트는 Kaspersky Security Network 클라우드 서비스, 휴리스틱 분석 및 알려진 웹사이트 데이터베이스(애플리케이션 데이터베이스에 포함)에 따라 분류됩니다. 예를 들어, *소셜 네트워크* 카테고리 또는 다른 카테고리에 대한 사용자 접근을 제한할 수 있습니다.

데이터 유형을 기반으로 웹사이트의 사용자 접근을 제한할 수 있습니다(예: 이미지 숨김). Kaspersky Endpoint Security는 파일 확장자가 아니라 파일 형식에 따라 데이터 유형을 결정합니다. 웹 제어는 다음 데이터 유형을 구분합니다:

- 비디오
- 소리
- 오피스 애플리케이션 파일
- 실행 파일

- 압축 파일
- 그래픽
- 스크립트

Kaspersky Endpoint Security는 압축 파일에 포함된 파일을 검사하지 않습니다. 예를 들어, 이미지 파일이 압축 파일에 있는 경우 Kaspersky Endpoint Security는 *그래픽* 데이터 유형이 아니라 *압축 파일* 데이터 유형을 식별합니다.

규칙에는 규칙 스케줄과 규칙이 적용되는 사용자 목록이 포함될 수 있습니다. 예를 들어 근무 시간만으로 웹사이트 접근을 제한하거나 특정 그룹의 사용자에게 웹사이트 방문을 허용할 수 있습니다.

관리 콘솔(MMC)의 웹 리소스 컨텐츠 필터를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보안 제어 → 웹 제어**를 선택합니다.
4. **웹 제어** 확인란을 선택합니다.
5. **웹 제어 설정** 블록에서 **추가** 버튼을 클릭합니다.
   웹사이트 접근 규칙 창이 열립니다.
6. 웹 리소스 접근 규칙을 구성합니다:
   a. **이름** 필드에서 규칙의 이름을 입력합니다.
   b. **컨텐츠 필터** 드롭다운 목록에서 관련 컨텐츠 필터를 선택합니다.
      - **컨텐츠 카테고리별**. 카테고리(*소셜 네트워크* 카테고리 등)별로 웹 리소스에 대한 사용자의 접근을 제어할 수 있습니다.
      - **데이터 유형별**. 게시된 데이터의 특정 데이터 유형(*그래픽* 등)을 기반으로 웹 리소스에 대한 사용자의 접근을 제어할 수 있습니다.
      - **컨텐츠 카테고리 및 데이터 유형별**. 컨텐츠 카테고리 및 데이터 유형별 필터가 활성화됩니다.

      필터를 선택한 후 필터 파라미터를 구성합니다.
   c. **사용자에게 적용** 드롭다운 목록에서 사용자에 해당하는 필터를 선택합니다:
      - **모든 사용자로**. 웹 제어는 주소별로 웹 리소스를 필터링하지 않습니다.
      - **개별 사용자 또는 그룹으로**. 웹 제어는 목록에서 웹 리소스 주소만 필터링합니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다. 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. **처리** 드롭다운 목록에서 옵션을 선택합니다:

- **허용**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 허용합니다.
- **차단**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 차단하고 웹사이트 접근 거부 메시지를 표시합니다.
- **경고**. 사용자가 규칙과 일치하는 웹 리소스에 접근하려 할 때 웹 제어는 웹 리소스 방문을 철회할 수 없다는 경고를 표시합니다. 사용자는 경고 메시지의 링크를 사용하여 요청한 웹 리소스에 대한 접근 권한을 얻을 수 있습니다.

e. **규칙 스케줄** 드롭다운 목록에서 스케줄을 선택하거나 새 스케줄을 생성합니다.

7. 정책이 적용된 직후 웹 제어가 금지된 웹 리소스와의 연결을 종료하도록 하려면 **규칙이 적용된 후 활성 사용자 브라우저 세션 종료** 확인란을 선택합니다.

웹 제어를 사용하면 웹 브라우저에서만 웹 리소스 연결을 즉시 해제할 수 있습니다. 다른 애플리케이션은 웹 제어가 새 연결만 제한합니다.

이 확인란을 선택하지 않으면, 웹 제어는 금지된 웹 리소스에 대한 새로운 연결만 제한합니다. 웹 제어는 활성화된 연결을 종료하지 않습니다.

8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 웹 리소스 컨텐츠 필터를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **웹 제어**로 이동합니다
5. **웹 제어 활성화됨** 토글을 켭니다.
6. **규칙 목록** 블록에서 **추가** 버튼을 클릭합니다.
7. 웹 리소스 접근 규칙을 구성합니다:
   a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.
   b. 웹 리소스 접근 규칙에 대해 **활성화됨** 상태를 선택합니다.
      언제든지 토글로 웹 리소스 접근 규칙을 중지할 수 있습니다.

c. **처리** 블록에서 관련 옵션을 선택합니다.

- **허용**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 허용합니다.
- **차단**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 차단하고 웹사이트 접근 거부 메시지를 표시합니다.
- **알림**. 사용자가 규칙과 일치하는 웹 리소스에 접근하려 할 때 웹 제어는 웹 리소스 방문을 철회할 수 없다는 경고를 표시합니다. 사용자는 경고 메시지의 링크를 사용하여 요청한 웹 리소스에 대한 접근 권한을 얻을 수 있습니다.

d. **범위**에서 **컨텐츠 카테고리**를 선택합니다.

e. 컨텐츠 필터를 구성합니다.

- **컨텐츠 카테고리**. 카테고리(*소셜 네트워크* 카테고리 등)별로 웹 리소스에 대한 사용자의 접근을 제어할 수 있습니다.
- **데이터 유형**. 게시된 데이터의 특정 데이터 유형(*그래픽* 등)을 기반으로 웹 리소스에 대한 사용자의 접근을 제어할 수 있습니다.

f. **사용자 또는 그룹**에서 웹 제어를 통해 규칙을 적용할 사용자를 선택합니다.

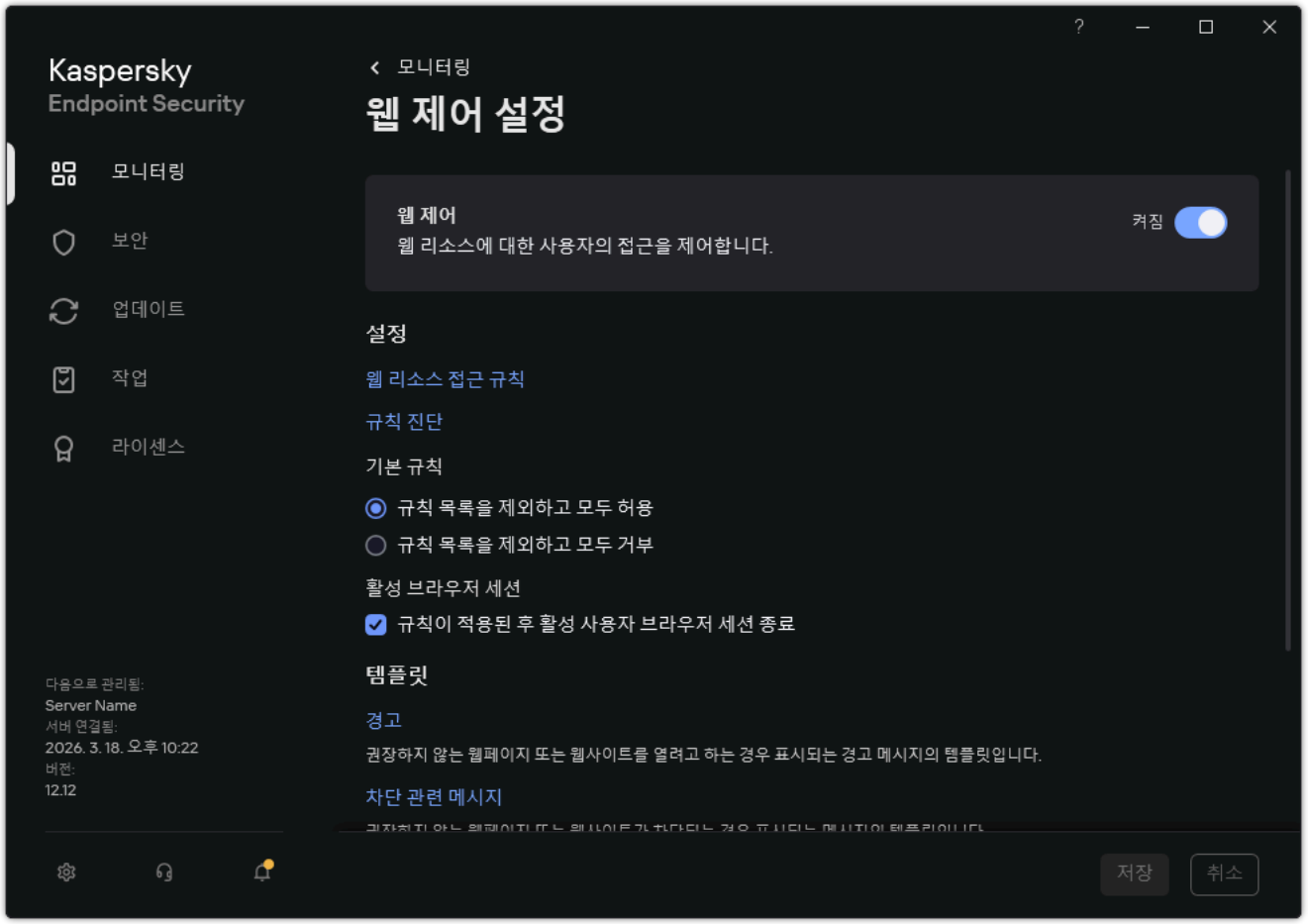
웹 제어는 목록에서 웹 리소스 주소만 필터링합니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다. Active Directory와 Kaspersky Security Center의 계정 목록에서 사용자를 선택하거나 로컬 사용자 이름을 수동으로 입력하여 사용자를 선택할 수 있습니다. Kaspersky는 도메인 사용자 계정을 사용할 수 없는 특별한 경우에만 로컬 사용자 계정을 사용할 것을 권장합니다.

g. **접근 스케줄** 블록에서 스케줄을 선택하거나 새 스케줄을 생성합니다.

8. 변경 사항을 저장합니다.

애플리케이션 인터페이스의 웹 리소스 컨텐츠 필터를 활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **웹 제어**를 선택합니다.



웹 제어 설정

3. **설정** 블록에서, **웹 리소스 접근 규칙** 버튼을 클릭합니다.
4. 열리는 창에서 **추가** 버튼을 누릅니다.
   웹사이트 접근 규칙 창이 열립니다.
5. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.
6. 웹 리소스 접근 규칙에 대해 **켜짐** 상태를 선택합니다.
   언제든지 토글로 웹 리소스 접근 규칙을 중지할 수 있습니다.
7. **처리** 블록에서 관련 옵션을 선택합니다.

   - **허용**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 허용합니다.
   - **차단**. 웹 제어는 규칙 파라미터와 일치하는 웹 리소스 접근을 차단하고 웹사이트 접근 거부 메시지를 표시합니다.
   - **경고**. 사용자가 규칙과 일치하는 웹 리소스에 접근하려 할 때 웹 제어는 웹 리소스 방문을 철회할 수 없다는 경고를 표시합니다. 사용자는 경고 메시지의 링크를 사용하여 요청한 웹 리소스에 대한 접근 권한을 얻을 수 있습니다.

8. **필터 콘텐츠** 블록에서 관련 콘텐츠 필터 선택합니다:

   - **컨텐츠 카테고리별**. 카테고리(*소셜 네트워크* 카테고리 등)별로 웹 리소스에 대한 사용자의 접근을 제어할 수 있습니다.
   - **데이터 유형별**. 게시된 데이터의 특정 데이터 유형(*그래픽* 등)을 기반으로 웹 리소스에 대한 사용자의 접근을 제어할 수 있습니다.

   컨텐츠 필터를 구성하려면 다음과 같이 하십시오.

   a. **설정** 링크를 클릭합니다.

   b. 필요한 컨텐츠 카테고리 및/또는 데이터 유형 카테고리 이름 옆의 확인란을 선택합니다.

   컨텐츠 카테고리 및/또는 데이터 유형 이름 옆의 확인란을 선택하면 Kaspersky Endpoint Security에서 선택한 컨텐츠 카테고리 및/또는 데이터 유형에 속해 있는 웹 리소스에 대한 접근을 제어하는 규칙을 적용합니다.

   c. 웹 리소스 접근 규칙 구성 창으로 돌아갑니다.

9. **사용자** 블록에서 사용자에 대한 관련 필터를 선택합니다:

   - **모든 사용자로**. 웹 제어는 주소별로 웹 리소스를 필터링하지 않습니다.
   - **개별 사용자 및/또는 그룹으로**. 웹 제어는 목록에서 웹 리소스 주소만 필터링합니다. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다. TXT 파일에서 웹 리소스 주소 목록 내보내기를 할 수도 있습니다. 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. 규칙을 적용할 사용자 목록을 만들려면 다음과 같이 하십시오.

     a. **추가**를 클릭합니다.

     b. 열린 창에서 웹 리소스 접근 규칙을 적용할 사용자 또는 사용자 그룹을 선택합니다.

     c. 웹 리소스 접근 규칙 구성 창으로 돌아갑니다.

10. **규칙 스케줄** 드롭다운 목록에서 필요한 스케줄의 이름을 선택하거나 선택한 규칙 스케줄을 기반으로 새 스케줄을 만듭니다. 이를 위해서는 다음과 같이 하십시오.

    a. **편집 또는 새로 추가**를 클릭합니다.

    b. 열리는 창에서 **추가** 버튼을 누릅니다.

    c. 열린 창에서 규칙 스케줄 이름을 입력합니다.

    d. 사용자에 대한 웹 리소스 접근 스케줄을 구성합니다.

    e. 웹 리소스 접근 규칙 구성 창으로 돌아갑니다.

11. 정책이 적용된 직후 웹 제어가 금지된 웹 리소스와의 연결을 종료하도록 하려면 **규칙이 적용된 후 활성 사용자 브라우저 세션 종료** 확인란을 선택합니다.

    웹 제어를 사용하면 웹 브라우저에서만 웹 리소스 연결을 즉시 해제할 수 있습니다. 다른 애플리케이션은 웹 제어가 새 연결만 제한합니다.

이 확인란을 선택하지 않으면, 웹 제어는 금지된 웹 리소스에 대한 새로운 연결만 제한합니다. 웹 제어는 활성화된 연결을 종료하지 않습니다.

12. 변경 사항을 저장합니다.

그러면 새로운 웹 제어 규칙이 목록에 추가됩니다. 필요한 경우 웹 제어 규칙의 우선 순위를 변경합니다. 또한 토글 스위치로 목록에서 제거하지 않고도 웹 리소스 접근 규칙을 언제든지 중지할 수 있습니다.

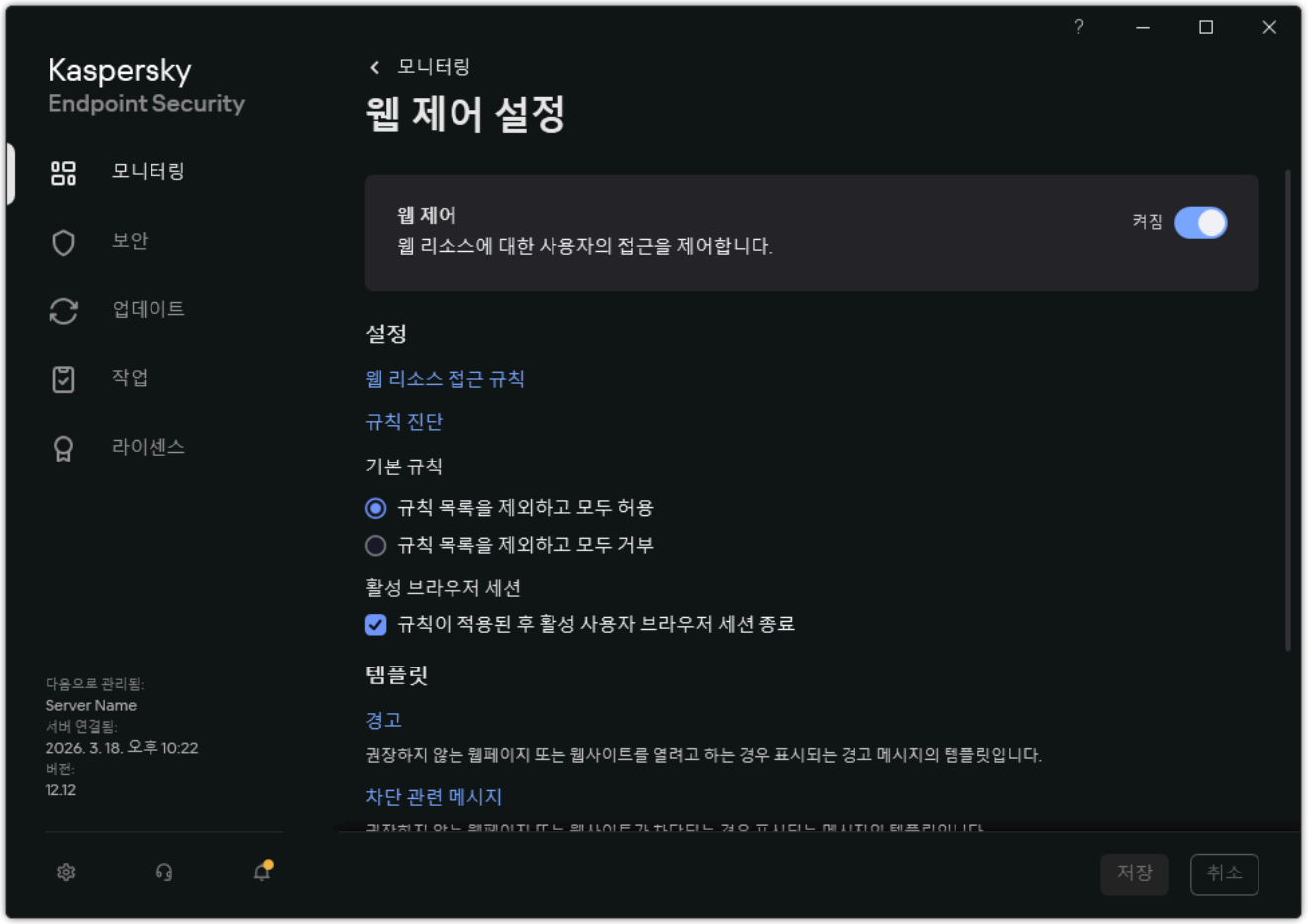
웹 리소스 접근 규칙 테스트

웹 제어를 구성할 때 의도치 않게 사용자가 작업에 필요한 웹 리소스 접근을 차단할 수 있습니다. 웹 리소스 접근을 차단하는 웹 제어 규칙을 찾으려면 *웹 제어 규칙 진단* 도구를 사용할 수 있습니다. 웹 제어 규칙 진단은 Kaspersky Endpoint Security 인터페이스에서만 사용 가능합니다. Kaspersky Security Center 콘솔에서 해당 리소스를 포함하는 웹 제어 규칙을 찾을 수 없습니다.

웹 리소스가 잘못 차단되었다고 판단되는 경우 웹 리소스 차단에 대해 알리는 메시지의 링크를 눌러 사전에 작성된 메시지를 사내 네트워크 관리자에게 보내 주십시오.

웹 리소스 접근 규칙을 테스트하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **웹 제어**를 선택합니다.



웹 제어 설정

3. **설정** 블록에서 **규칙 진단** 링크를 클릭합니다.

   규칙 진단 창이 열립니다.

4. Kaspersky Endpoint Security에서 특정 웹 리소스에 대한 접근을 제어하는 데 사용하는 규칙을 테스트하려면 **주소 지정** 확인란을 선택합니다. 아래 필드에 웹 리소스 주소를 입력합니다.

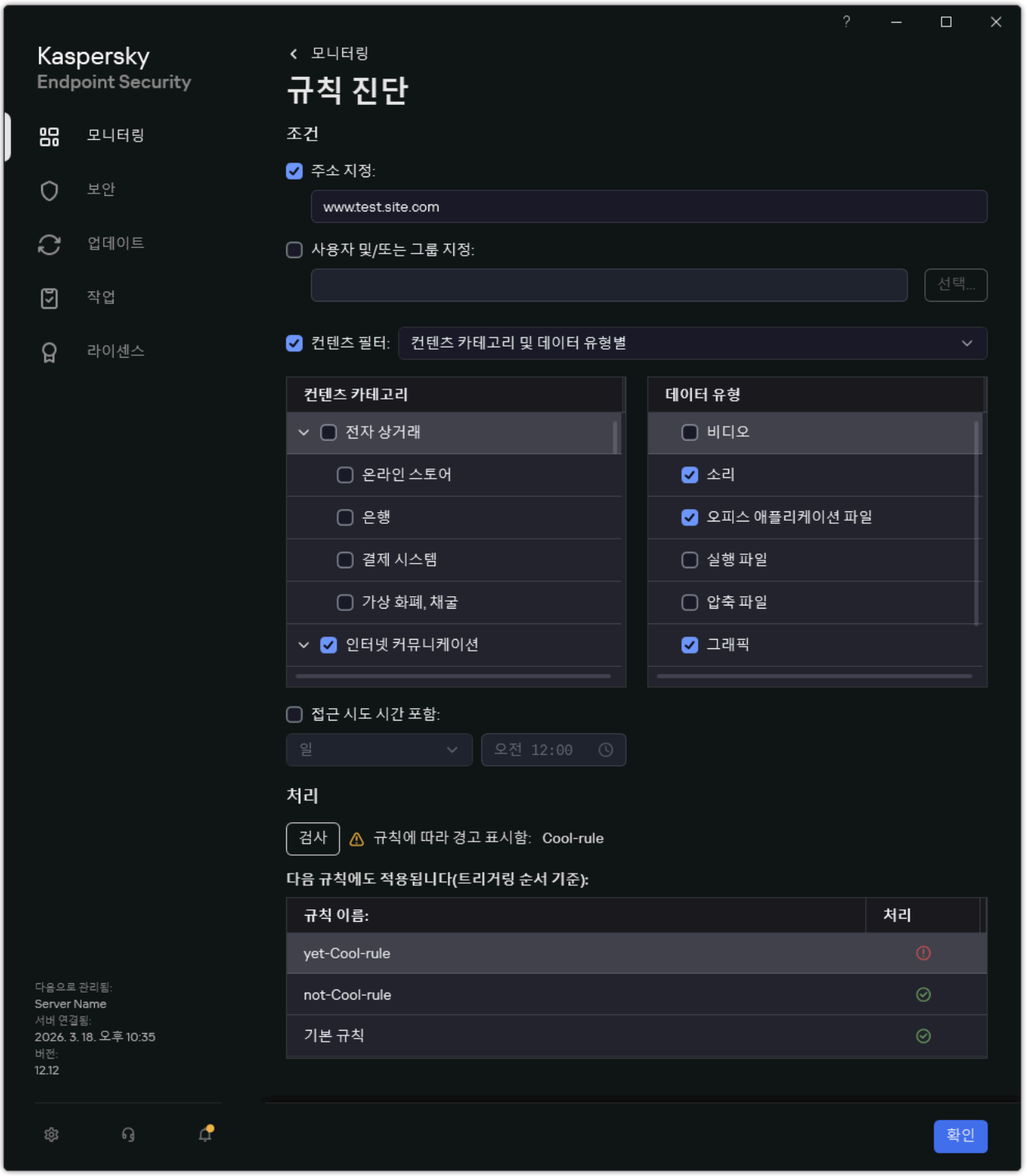
5. Kaspersky Endpoint Security에서 특정 사용자 또는 사용자 그룹의 웹 리소스 접근을 제어하는 데 사용하는 규칙을 테스트하려면 사용자 또는 사용자 그룹의 목록을 지정합니다.

6. Kaspersky Endpoint Security에서 특정 컨텐츠 카테고리 및/또는 데이터 유형 카테고리의 웹 리소스 접근을 제어하는 데 사용하는 규칙을 테스트하려면 **컨텐츠 필터** 확인란을 선택하고 드롭다운 목록에서 필요한 옵션을 선택합니다(**컨텐츠 카테고리별**, **데이터 유형별** 또는 **컨텐츠 카테고리 및 데이터 유형별**).

7. 규칙 진단 조건에 지정된 웹 리소스에 대해 접근하려는 시도가 발생한 요일 및 시간을 고려하여 규칙을 테스트하려면 **접근 시도 시간 포함** 확인란을 선택합니다. 그런 다음, 요일과 시간을 지정합니다.

8. **검사**를 클릭합니다.

테스트가 완료되면, 누군가 지정된 웹 리소스에 접근하려고 했을 때 가장 먼저 트리거되는 규칙에 따라 Kaspersky Endpoint Security에서 수행한 처리 방법에 대한 정보가 들어 있는 메시지가 표시됩니다(허용, 차단 또는 경고). 가장 먼저 트리거되는 규칙은 웹 제어 규칙 목록에서 해당 진단 조건을 충족하는 다른 규칙보다 순위가 높은 규칙입니다. 이 메시지는 **검사** 버튼 오른쪽에 표시됩니다. 다음 표에는 트리거된 나머지 규칙이 나열되어 Kaspersky Endpoint Security에서 수행하는 처리 방법이 명시됩니다. 이러한 규칙은 우선순위가 높은 순으로 나열됩니다.



웹 리소스 접근 테스트 결과

웹 제어 규칙 내보내기 및 가져오기

웹 제어 규칙 목록을 XML 또는 JSON 파일로 내보낼 수 있습니다. 그 후 같은 유형의 주소를 여러 개 추가하는 등 파일을 수정할 수 있습니다. 내보내기/가져오기 기능을 사용하여 웹 제어 규칙 목록을 백업하거나 다른 서버로 마이그레이션할 수 있습니다.

관리 콘솔(MMC)에서 웹 제어 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 창에서 **보안 제어 → 웹 제어**를 선택합니다.

4. 웹 제어 규칙 목록을 내보내려면 다음을 수행합니다.

   a. 내보낼 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
   규칙을 선택하지 않으면 Kaspersky Endpoint Security는 모든 규칙을 내 보냅니다.

   b. **내보내기** 링크를 클릭합니다.

   c. 창이 열리면 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

   d. 파일을 저장합니다.
   Kaspersky Endpoint Security는 신뢰하는 규칙 목록을 XML 파일로 내보냅니다.

5. 웹 제어 규칙 목록을 가져오려면 다음을 수행합니다.

   a. **가져오기** 링크를 클릭합니다.
   창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.

   b. 파일을 엽니다.
   컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 웹 제어 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어 → 웹 제어**로 이동합니다

5. 규칙 목록을 내보내려면 **규칙 목록** 블록에서:

   a. 내보낼 규칙을 선택합니다.

   b. → **내보내기** 버튼을 클릭합니다.
   Kaspersky Endpoint Security는 규칙 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.

6. 규칙 목록을 가져오려면 **규칙 목록** 블록에서:

   a. → **가져오기** 버튼을 클릭합니다.
   창이 열리면 규칙 목록을 가져올 JSON 파일을 선택합니다.

   b. 파일을 엽니다.
   컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 변경 사항을 저장합니다.

웹 제어 규칙의 웹 리소스 주소 내보내기 및 가져오기

웹 리소스 접근 규칙에서 웹 리소스 주소 목록을 만든 경우 다음 파일로 내보낼 수 있습니다.

- 관리 콘솔(MMC)에서 TXT 형식
- 애플리케이션 인터페이스에서 CSV 형식

이후에 접근 규칙을 구성할 때 이 파일에서 목록을 가져올 수 있으므로 직접 웹 리소스 주소 목록을 새로 작성할 필요가 없습니다. 웹 리소스 주소 목록 내보내기 및 가져오기 옵션은 파라미터가 유사한 접근 규칙을 만들 때 유용할 수 있습니다.

개별 규칙의 웹 리소스 주소만이 아니라 모든 웹 제어 규칙 내보내기/가져오기도 가능합니다.

웹 콘솔 또는 Cloud Console에서는 웹 제어 규칙의 웹 리소스 주소 내보내기/가져오기를 할 수 없습니다.

관리 콘솔(MMC)에서 웹 제어 규칙의 웹 리소스 주소를 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 **보안 제어** → **웹 제어**를 선택합니다.
4. **웹 제어 설정** 블록에서 내보내거나 가져올 웹 리소스 주소 목록에 대한 규칙을 선택합니다.
   웹 제어 규칙 속성이 표시됩니다.
5. 웹 리소스 목록을 내보내려면 주소 목록에서 다음을 수행합니다.
   a. 내보낼 주소를 선택합니다.
      주소를 선택하지 않으면 Kaspersky Endpoint Security는 모든 주소를 내보냅니다.
   b. 버튼을 클릭합니다.
   c. 창이 열리면 웹 리소스 주소 목록을 내보낼 TXT 파일의 이름을 입력하고 이 파일을 저장할 폴더를 선택합니다.
   d. 파일을 저장합니다.
      Kaspersky Endpoint Security는 웹 리소스 주소 목록을 TXT 파일로 내보냅니다.
6. 웹 리소스 목록을 가져오려면 주소 목록에서 다음을 수행합니다.
   a. 버튼을 클릭합니다.
      창이 열리면 웹 리소스 목록을 가져올 TXT 파일을 선택합니다.

b. 파일을 엽니다.

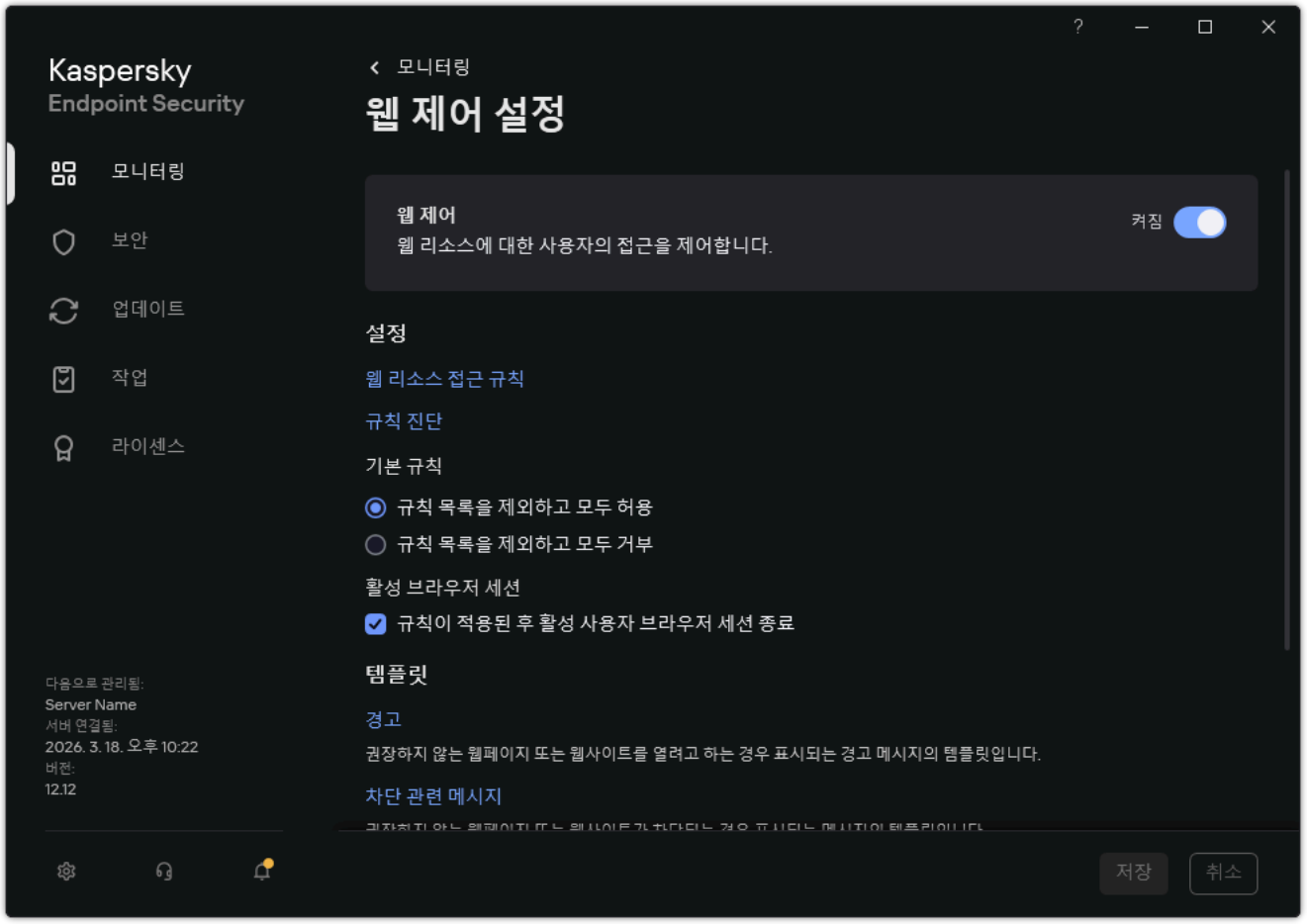
컴퓨터에 이미 주소 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 TXT 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 웹 제어 규칙의 웹 리소스 주소를 내보내고 가져오는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **보안 제어** → **웹 제어**를 선택합니다.



웹 제어 설정

3. **설정** 블록에서, **웹 리소스 접근 규칙** 버튼을 클릭합니다.

4. 내보내거나 가져올 웹 리소스 주소 목록에 대한 규칙을 선택합니다.

5. 신뢰하는 웹 주소 목록을 내보내려면 **주소** 블록에서 다음을 수행합니다:

a. 내보낼 주소를 선택합니다.

주소를 선택하지 않으면 Kaspersky Endpoint Security는 모든 주소를 내보냅니다.

b. **내보내기**를 클릭합니다.

c. 창이 열리면 웹 리소스 주소 목록을 내보낼 CSV 파일의 이름을 입력하고 이 파일을 저장할 폴더를 선택합니다.

d. 파일을 저장합니다.

Kaspersky Endpoint Security는 웹 리소스 주소 목록을 CSV 파일로 내보냅니다.

6. 웹 리소스 목록을 가져오려면 **주소** 블록에서 다음을 수행합니다.

   a. **가져오기**를 클릭합니다.

      창이 열리면 웹 리소스 목록을 가져올 CSV 파일을 선택합니다.

   b. 파일을 엽니다.

      컴퓨터에 이미 주소 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 CSV 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 변경 사항을 저장합니다.

사용자 인터넷 활동 모니터링

Kaspersky Endpoint Security에서는 허용된 웹사이트를 포함한 모든 웹사이트에 대한 사용자 방문 데이터를 기록할 수 있습니다. 따라서 사용자는 브라우저 보기에 대한 전체 기록을 획득할 수 있습니다. Kaspersky Endpoint Security는 Kaspersky Security Center, Kaspersky Endpoint Security의 로컬 로그 및 Windows 이벤트 로그에 사용자 활동 이벤트를 보냅니다. Kaspersky Security Center에서 이벤트를 받으려면 관리 콘솔 또는 웹 콘솔의 정책에서 이벤트 설정을 구성해야 합니다. 웹 콘솔 이벤트를 이메일로 수신하고 사용자 컴퓨터에 이벤트 알림을 표시하도록 구성할 수도 있습니다.

이 모니터링 기능이 지원되는 브라우저는 Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox입니다. 그 외 브라우저에서는 사용자 활동 모니터링이 작동하지 않습니다.

Kaspersky Endpoint Security는 다음과 같은 사용자 인터넷 활동 이벤트를 생성합니다:

- 웹사이트 차단(*심각* 상태 ⓘ).
- 권장하지 않는 웹사이트 방문(*경고* 상태 ⚠).
- 허용된 웹사이트 방문(*정보* 상태 ⓘ).

사용자 인터넷 활동 감시를 사용하기 전에 다음을 수행해야 합니다:

- 웹 트래픽에 웹 페이지 상호 작용 스크립트를 삽입합니다(아래 설명을 참조하십시오). 이 스크립트를 사용하면 웹 제어 이벤트를 등록할 수 있습니다.
- HTTPS 트래픽을 모니터링하려면 암호화된 연결 검사를 사용하도록 설정해야 합니다.

웹 페이지 상호작용 스크립트 삽입

관리 콘솔(MMC)에서 웹 트래픽에 웹 페이지 상호작용 스크립트를 삽입하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 네트워크 설정**을 선택합니다.

4. **암호화된 연결 검사** 블록에서 **웹 페이지와의 상호 작용을 위해 웹 트래픽에 스크립트 삽입** 확인란을 선택합니다.

5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 웹 트래픽에 웹 페이지 상호작용 스크립트를 삽입하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. 정책 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.

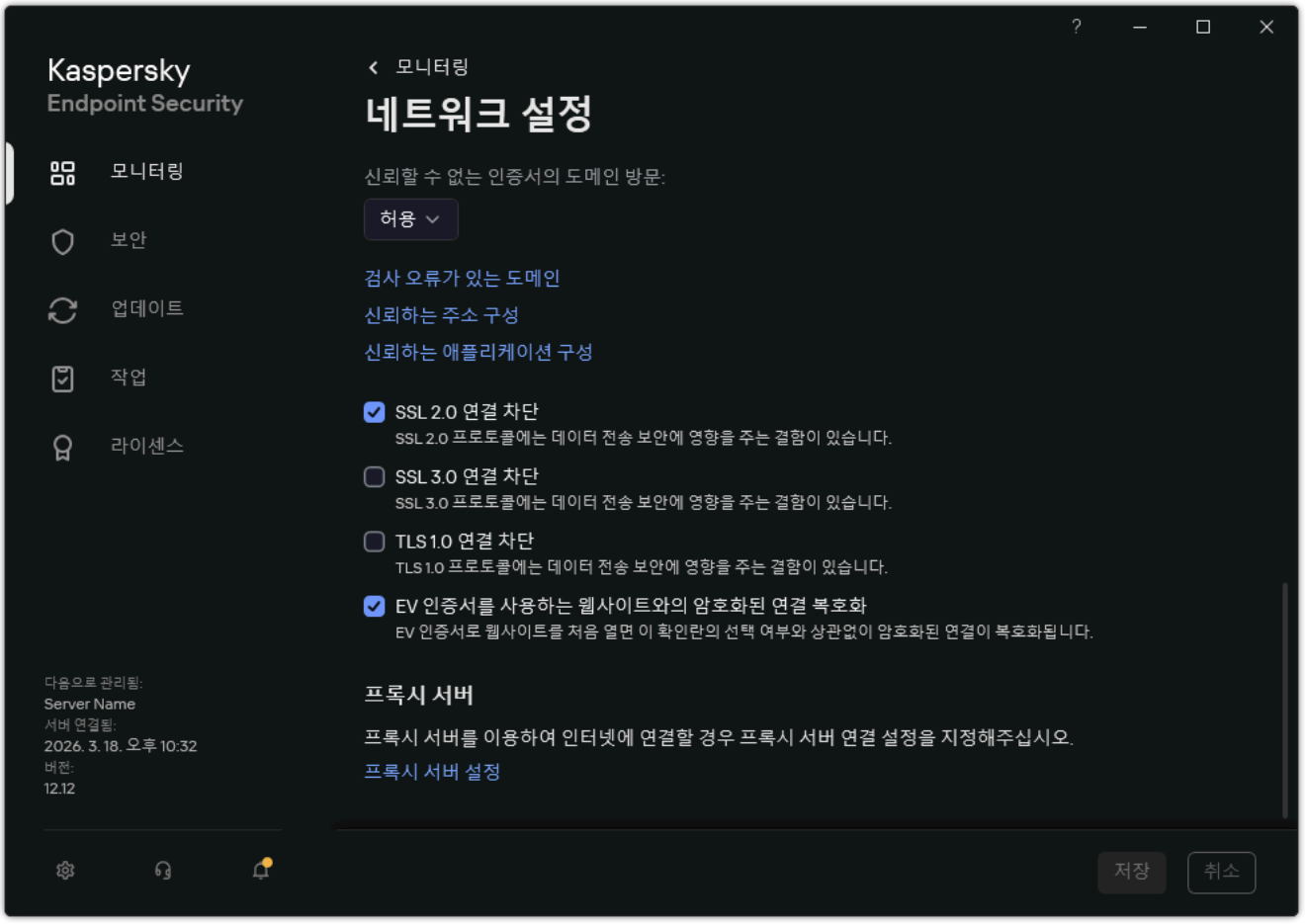
5. **인터넷 연결 모니터링**에서, **인터넷 연결 모니터링 활성화됨** 토글 스위치를 켭니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 웹 페이지 상호작용 스크립트를 웹 트래픽에 삽입하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.



애플리케이션 네트워크 설정

3. **트래픽 처리** 블록에서 **웹 페이지와의 상호 작용을 위해 웹 트래픽에 스크립트 삽입** 확인란을 선택합니다.

4. 변경 사항을 저장합니다.

결과적으로 Kaspersky Endpoint Security는 웹 트래픽에 웹 페이지 상호 작용 스크립트를 삽입합니다. 이 스크립트를 사용하면 애플리케이션 이벤트 로그, OS 이벤트 로그 및 리포트에 대한 웹 제어 이벤트를 등록할 수 있습니다.

웹 제어 이벤트 로그 기록 구성

사용자의 컴퓨터에서 웹 제어 이벤트에 대한 로그를 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **인터페이스**를 차례로 선택합니다.
3. **알림** 블록에서 **알림 구성** 버튼을 클릭합니다.
4. 창이 열리면 **웹 제어** 섹션을 선택합니다.
   웹 제어 이벤트와 알림 방법이 나와 있는 표가 열립니다.
5. 각 이벤트에 대한 알림 방법 구성: **로컬 리포트에 저장** 또는 **Windows 이벤트 로그에 저장**.
   허용된 웹사이트 방문 이벤트 로그를 기록하려면 웹 제어도 구성해야 합니다(아래 지침 참조).
   또한 이벤트 표에서 화면 알림 및 이메일 알림을 사용하도록 설정할 수 있습니다. 이메일로 알림을 전송하려면 SMTP 서버 설정을 구성해야 합니다. 이메일 알림 전송에 대한 자세한 정보는 Kaspersky Security Center 도움말을 참조하십시오.
6. 변경 사항을 저장합니다.

그러면 Kaspersky Endpoint Security가 사용자 인터넷 활동 이벤트 로그를 기록하기 시작합니다.

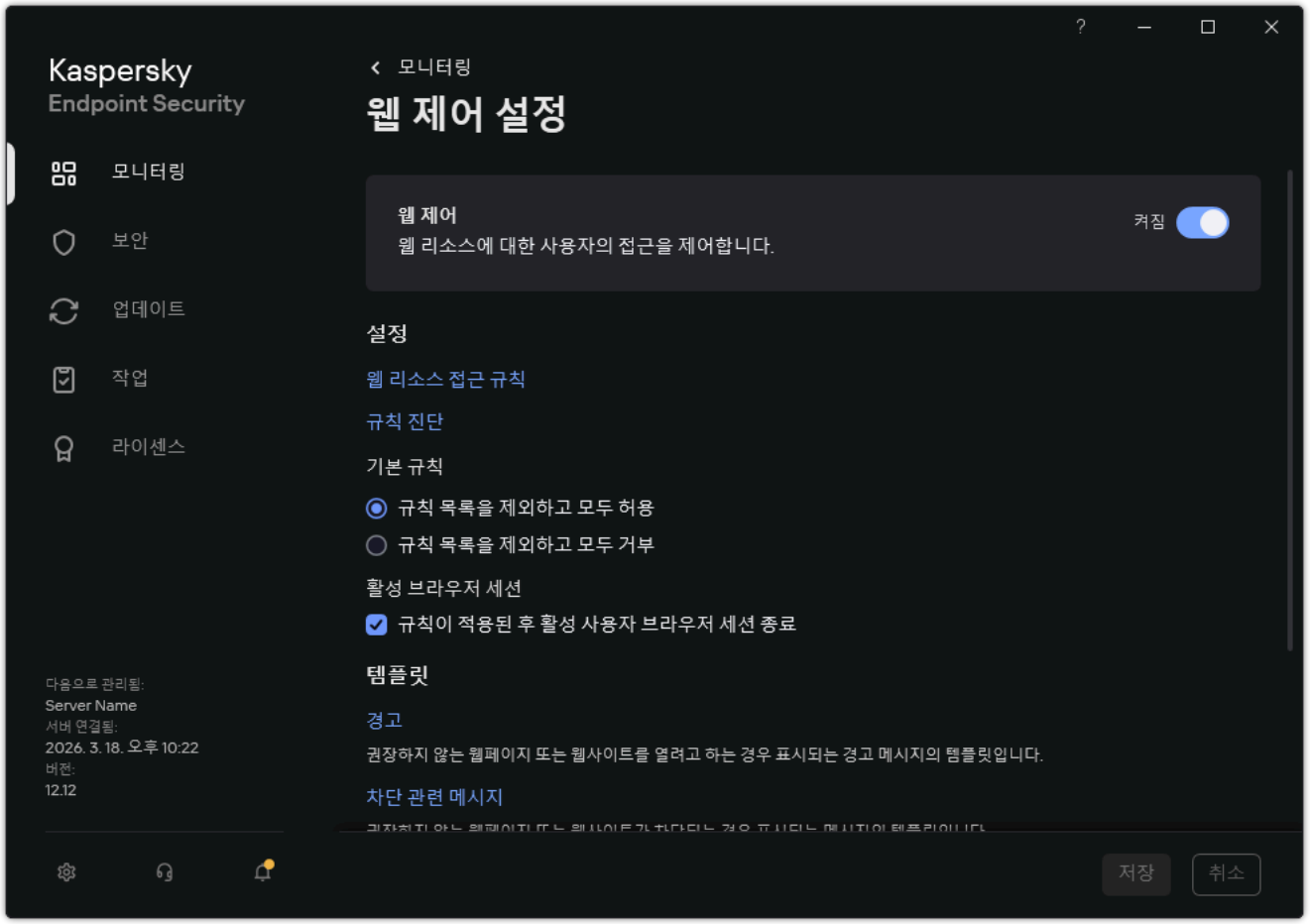
웹 제어는 다음과 같이 사용자 활동 이벤트를 Kaspersky Security Center로 전송합니다.

- Kaspersky Security Center를 사용하는 경우 웹 제어는 웹 페이지를 구성하는 모든 개체에 대한 이벤트를 전송합니다. 따라서 한 웹 페이지가 차단되면 여러 개의 이벤트가 생성될 수 있습니다. 예를 들어 http://www.example.com이라는 웹 페이지를 차단하는 경우 Kaspersky Endpoint Security는 http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js 같은 개체에 대한 이벤트를 전달할 수 있습니다.
- Kaspersky Security Center Cloud Console을 사용하는 경우 웹 제어는 이벤트를 그룹화하고 웹사이트의 프로토콜 및 도메인만을 전송합니다. 예를 들어 사용자가 권장하지 않는 웹 페이지 http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery를 방문하면 Kaspersky Endpoint Security는 http://www.example.com 개체와 함께 하나의 이벤트만 전송합니다.

허용된 웹사이트를 방문할 때 이벤트 로그 기록

허용된 웹사이트의 방문할 때 이벤트 로그 기록을 사용하려면 다음과 같이 하십시오.

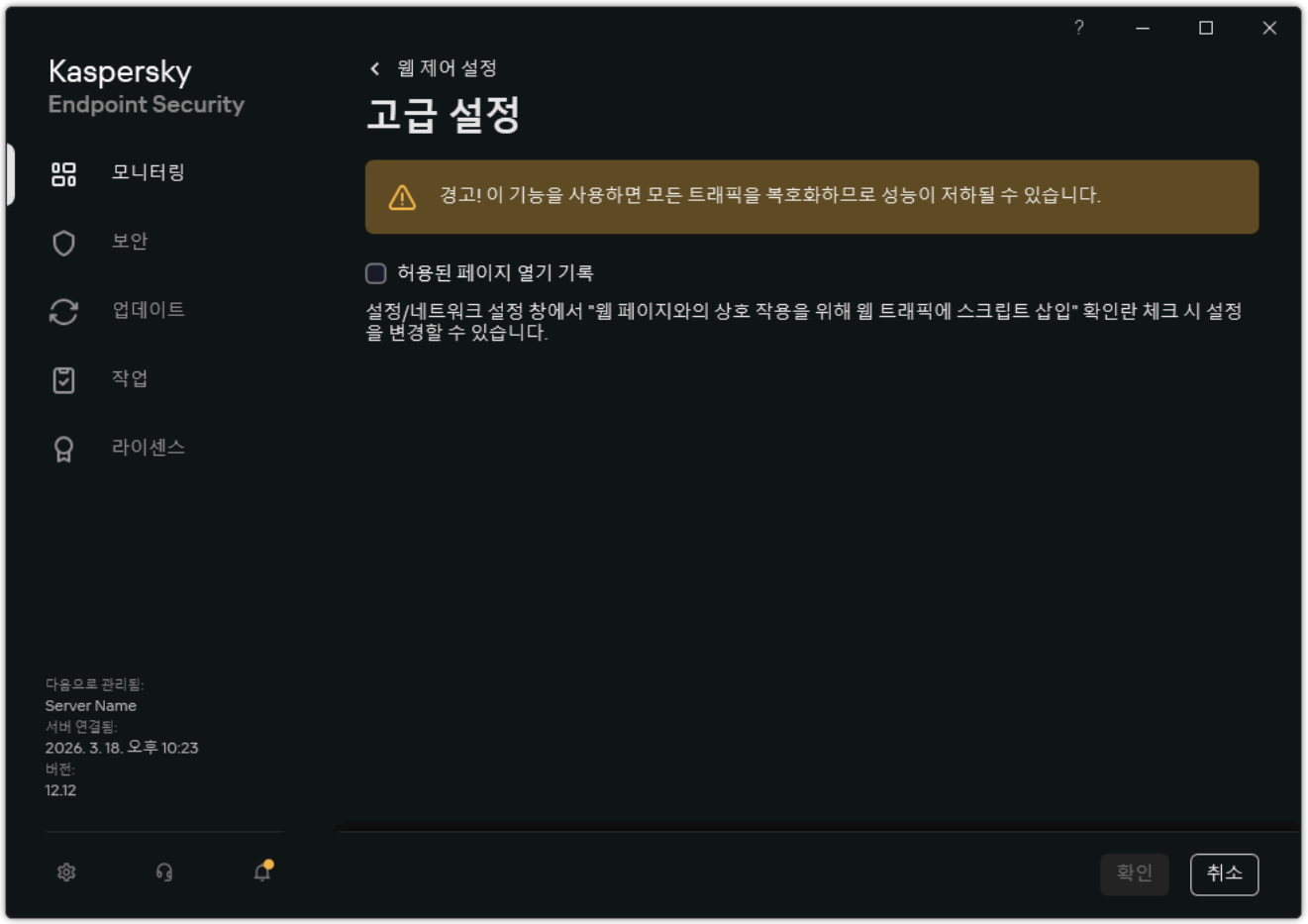
1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **웹 제어**를 선택합니다.



웹 제어 설정

3. **추가** 블록에서 **고급 설정** 버튼을 클릭합니다.

4. 창이 열리면 **허용된 페이지 열기 기록** 확인란을 선택합니다.



웹 제어 고급 설정

5. 변경 사항을 저장합니다.

이렇게 하면 전체 브라우저 기록을 볼 수 있습니다.

웹 제어 메시지 템플릿 편집

웹 제어 규칙 속성에 지정된 처리 방법의 유형에 따라, Kaspersky Endpoint Security에서는 사용자가 인터넷 리소스에 접근하려고 할 때 다음 유형 중 하나의 메시지가 표시됩니다(애플리케이션이 HTML 페이지를 HTTP 서버 응답에 대한 메시지로 대체):

- 경고 메시지. 이 메시지는 해당 웹 리소스를 방문하는 사용자에게 권장하지 않거나 또는 기업 보안 정책을 위반하는 것이라고 경고합니다. Kaspersky Endpoint Security는 해당 웹 리소스를 설명하는 규칙 설정에서 **경고** 옵션을 선택하면 경고 메시지를 표시합니다.

  경고 메시지가 잘못 표시되었다고 판단되는 경우 경고 메시지의 링크를 눌러 사전 생성된 메시지를 사내 네트워크 관리자에게 보내 주십시오.

- 웹 리소스 차단에 대해 알리는 메시지. Kaspersky Endpoint Security는 해당 웹 리소스를 설명하는 규칙 설정에서 **차단** 옵션을 선택하면 웹 리소스가 차단되었음을 알리는 메시지를 표시합니다(아래 그림 참조).

웹 리소스가 잘못 차단되었다고 판단되는 경우 웹 리소스 차단에 대해 알리는 메시지의 링크를 눌러 사전 생성된 메시지를 사내 네트워크 관리자에게 보내 주십시오.



웹 리소스 차단 관련 메시지

경고 메시지, 웹 리소스 차단에 대해 알리는 메시지, LAN 관리자에게 보낼 메시지에 사용할 수 있는 특별 템플릿이 제공됩니다. 메시지 템플릿(예: %USER_NAME%)을 관리하기 위해 특수 변수가 제공됩니다. 변수를 사용하면 다른 컴퓨터에서 단일 메시지 템플릿을 사용할 수 있습니다. 메시지 생성 시 Kaspersky Endpoint Security는 운영 체제 설정에서 변수 값을 검색하여 특정 컴퓨터, 사용자 및 이벤트와 일치하는 메시지에 삽입합니다.

관리 콘솔(MMC)에서 웹 제어 메시지 템플릿을 변경하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보안 제어 → 웹 제어**를 선택합니다.
4. **메시지 템플릿 설정** 블록에서 **템플릿** 버튼을 클릭합니다.
5. 웹 제어 메시지 템플릿을 구성합니다:

   - **경고**. 원하지 않는 웹 리소스에 대한 접근을 경고하는 규칙이 작동할 때 표시되는 메시지의 템플릿을 지정하는 입력 필드입니다.
   - **차단 관련 메시지**. 웹 리소스 접근을 차단하는 규칙이 작동될 때 나타나는 메시지의 템플릿을 지정하는 입력 필드입니다.
   - **관리자에게 메시지 보내기**. 사용자가 차단을 실수로 간주하는 경우 LAN 관리자에게 전송되는 메시지의 템플릿입니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 웹 페이지 접근 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다.

   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

기본적으로 버튼을 사용하여 기본 템플릿 텍스트를 복원할 수도 있습니다.

6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 웹 제어 메시지 템플릿을 변경하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어** → **웹 제어**로 이동합니다

5. **메시지 템플릿** 블록에서 **웹사이트 차단 관련 메시지** 링크를 클릭하고 웹 제어 메시지용 템플릿을 구성합니다.

   - **경고**. 원하지 않는 웹 리소스에 대한 접근을 경고하는 규칙이 작동할 때 표시되는 메시지의 템플릿을 지정하는 입력 필드입니다.

   - **차단 관련 메시지**. 웹 리소스 접근을 차단하는 규칙이 작동될 때 나타나는 메시지의 템플릿을 지정하는 입력 필드입니다.

   - **관리자에게 메시지 보내기**. 사용자가 차단을 실수로 간주하는 경우 LAN 관리자에게 전송되는 메시지의 템플릿입니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 웹 페이지 접근 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다.

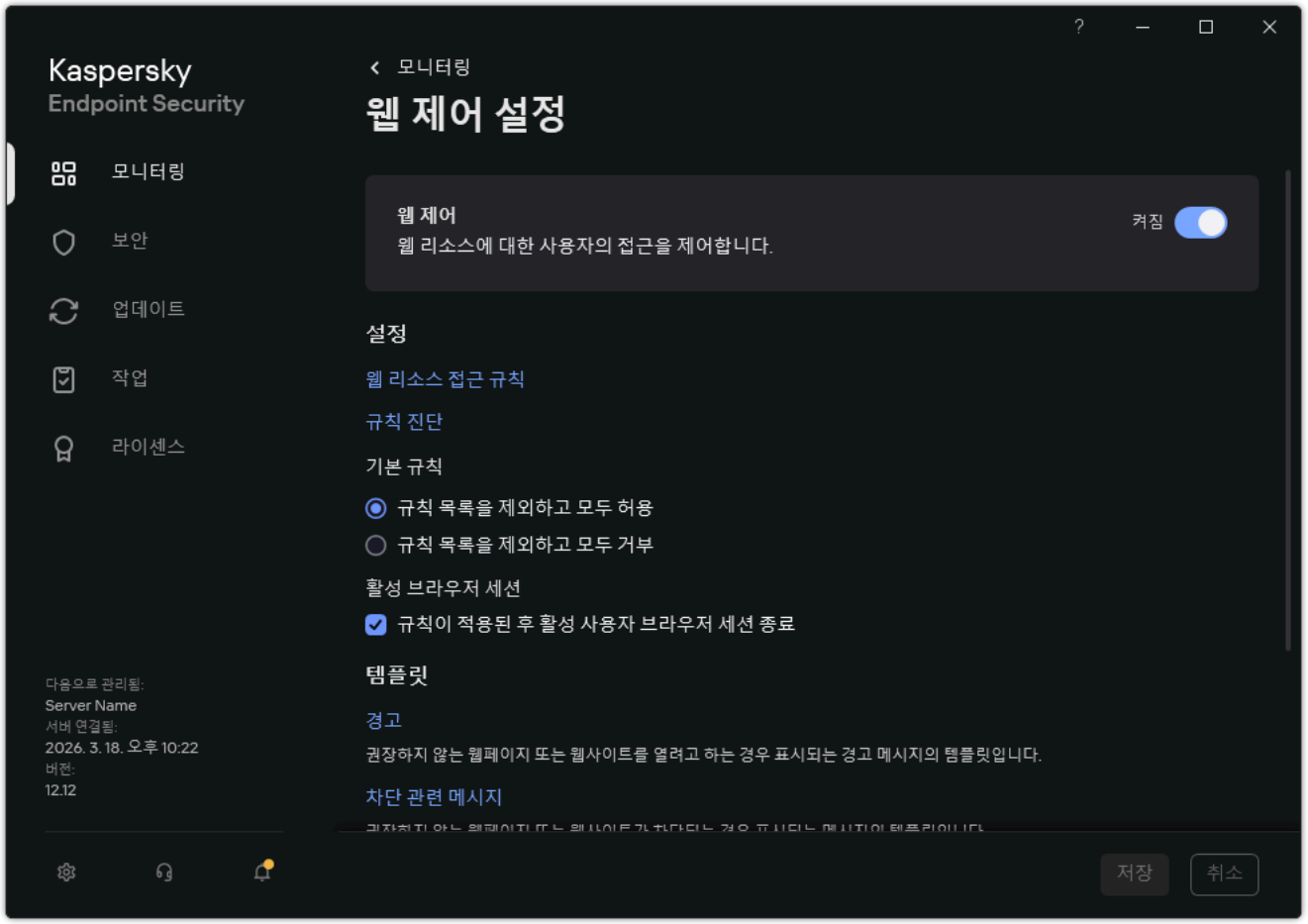
   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수 추가**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

   기본값으로 재설정 버튼을 사용하여 기본 템플릿 텍스트를 복원할 수도 있습니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 웹 제어 메시지 템플릿을 변경하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **웹 제어**를 선택합니다.



웹 제어 설정

3. **템플릿** 블록에서 웹 제어 메시지에 대한 템플릿을 구성합니다:

   - **경고**. 원하지 않는 웹 리소스에 대한 접근을 경고하는 규칙이 작동할 때 표시되는 메시지의 템플릿을 지정하는 입력 필드입니다.
   - **차단 관련 메시지**. 웹 리소스 접근을 차단하는 규칙이 작동될 때 나타나는 메시지의 템플릿을 지정하는 입력 필드입니다.
   - **관리자에게 메시지 보내기**. 사용자가 차단을 실수로 간주하는 경우 LAN 관리자에게 전송되는 메시지의 템플릿입니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 웹 페이지 접근 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다.

   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수 추가**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

   초기화 버튼을 사용하여 기본 템플릿 텍스트를 복원할 수도 있습니다.

4. 변경 사항을 저장합니다.

웹 리소스 주소 마스크 편집

웹 리소스 주소 마스크("주소 마스크"라고도 함)를 사용하면 웹 리소스 접근 규칙을 생성할 때 수많은 유사한 웹 리소스를 입력해야 할 경우 유용할 수 있습니다. 제대로 만들어진 주소 마스크 하나가 다수의 웹 리소스 주소를 대체할 수 있습니다.

주소 마스크를 만들 때, 다음 규칙을 따릅니다:

1. `*` 문자는 0자 이상의 문자를 대체합니다.

   예를 들어, 주소 마스크로 `*abc*`를 입력하는 경우 `abc`가 포함되어 있는 모든 웹 리소스에 접근 규칙이 적용됩니다. 예: `http://www.example.com/page_0-9abcdef.html`.

2. `*.` 문자열(*도메인 마스크*)로 주소의 모든 도메인을 선택할 수 있습니다. `*.` 도메인 마스크는 모든 도메인 이름, 하위 도메인 이름 또는 빈 줄을 나타냅니다.

   예: `*.example.com` 마스크는 다음 주소를 나타냅니다:

   - `http://pictures.example.com`. 도메인 마스크 `*.`는 `pictures.`를 나타냅니다.
   - `http://user.pictures.example.com`. 도메인 마스크 `*.`는 `pictures.`와 `user.`를 나타냅니다.
   - `http://example.com`. 도메인 마스크 `*.`은 빈 줄로 해석됩니다.

3. 주소 마스크 처음에 나오는 `www.`문자는 `*.` 순서로 해석됩니다.

   예: 주소 마스크 `www.example.com`은 `*.example.com`으로 해석됩니다. 이 마스크는 `www2.example.com` 및 `www.pictures.example.com` 주소를 포함합니다.

4. 주소 마스크가 `*` 문자로 시작되지 않는 경우 주소 마스크의 컨텐츠는 `*.` 접두사가 있는 컨텐츠와 동일합니다.

5. 주소 마스크가`/` 또는 `*` 이외의 문자로 끝나는 경우 주소 마스크의 컨텐츠는 `/*`접미사가 있는 컨텐츠와 동일합니다.

   예: 주소 마스크 `http://www.example.com`에는 `http://www.example.com/abc`와 같은 주소가 포함됩니다. 여기서 `a`, `b`, `c`는 아무 문자나 상관 없습니다.

6. 주소 마스크가 `/` 문자로 끝나는 경우 주소 마스크의 컨텐츠는 `/*` 접미사가 있는 컨텐츠와 동일합니다.

7. 주소 마스크 끝에 나오는 `/*` 문자는 `/*` 또는 빈 문자열로 해석됩니다.

8. 웹 리소스 주소는 주소 마스크와 비교하여 확인됩니다. 이때 프로토콜(http 또는 https) 또한 고려합니다:

   - 주소 마스크에 네트워크 프로토콜이 포함되어 있지 않은 경우 이 주소 마스크는 네트워크 프로토콜에 상관없이 모든 주소를 포함합니다.

     예: 주소 마스크 `example.com`은 `http://`example.com 및 `https://`example.com 주소를 포함합니다.

   - 주소 마스크에 네트워크 프로토콜이 포함되어 있는 경우 이 주소 마스크는 네트워크 프로토콜이 동일한 주소만 포함합니다.

     예: 주소 마스크 `http://*.example.com`에는 `http://www.example.com` 주소는 포함되지만 `https://www.example.com` 주소는 포함되지 않습니다.

9. 큰따옴표로 묶여 있는 주소 마스크는 * 문자가 주소 마스크에 처음부터 포함되어 있는 경우 해당 문자를 예외한 다른 추가 교체 문자를 고려하지 않고 처리됩니다. 규칙 5와 7은 큰 따옴표 안에 있는 주소 마스크에 적용되지 않습니다(아래 테이블에서 14~18 예시 참조).

10. 웹 리소스의 주소 마스크를 비교할 때 사용자 이름과 암호, 연결 포트 및 대소문자는 고려하지 않습니다.

주소 마스크를 만들 때 규칙을 사용하는 방법에 대한 예

번호	주소 마스크	확인해야 할 웹 리소스 주소	주소 마스크가 적용되는 주소인지 여부	설명
1	*.example.com	http://www.123example.com	아니오	규칙 1 참조.
2	*.example.com	http://www.123.example.com	예	규칙 2 참조.
3	*example.com	http://www.123example.com	예	규칙 1 참조.
4	*example.com	http://www.123.example.com	예	규칙 1 참조.
5	http://www.*.example.com	http://www.123example.com	아니오	규칙 1 참조.
6	www.example.com	http://www.example.com	예	규칙 3, 2, 1 참조.
7	www.example.com	https://www.example.com	예	규칙 3, 2, 1 참조.
8	http://www.*.example.com	http://123.example.com	예	규칙 3, 4, 1 참조.
9	www.example.com	http://www.example.com/abc	예	규칙 3, 5, 1 참조.
10	example.com	http://www.example.com	예	규칙 3 및 1 참조.
11	http://example.com/	http://example.com/abc	예	규칙 6 참조.
12	http://example.com/*	http://example.com	예	규칙 7 참조.
13	http://example.com	https://example.com	아니오	규칙 8 참조.
14	"example.com"	http://www.example.com	아니오	규칙 9 참조.
15	"http://www.example.com"	http://www.example.com/abc	아니오	규칙 9 참조.
16	"*.example.com"	http://www.example.com	예	규칙 1 및 9 참조.
17	"http://www.example.com/*"	http://www.example.com/abc	예	규칙 1 및 9 참조.
18	"www.example.com"	http://www.example.com; https://www.example.com	예	규칙 9 및 8 참조.
19	www.example.com/abc/123	http://www.example.com/abc	아니오	주소 마스크에는 웹 리소스 주소외에 추가 정보가 포함되어 있습니다.

가상 컴퓨터용 웹 제어

웹 제어는 컴퓨터 및 컴퓨터에 로컬로 배포된 가상 컴퓨터에서 트래픽을 제어합니다. 이 제어는 로컬 가상 컴퓨터에 Kaspersky Endpoint Security 애플리케이션을 설치하지 않고도 작동합니다. 즉, 사용자가 *가상 컴퓨터*의 브라우저에서 웹 제어 규칙에 의해 차단된 웹사이트를 하면, *컴퓨터*의 호스트 운영 체제에 설치된 애플리케이션이 해당 웹사이트에 대한 접근을 거부합니다.

웹 제어는 가상 컴퓨터에 따라 다르게 작동합니다.

Oracle VM VirtualBox

Kaspersky Endpoint Security는 Oracle VM VirtualBox 가상 컴퓨터에 대한 웹 제어 규칙을 제한 없이 지원합니다. 애플리케이션은 가상 컴퓨터의 모든 트래픽을 제어할 수 있습니다. 웹 제어 규칙에서 사용자별 필터를 구성하면 가상 컴퓨터의 모든 프로세스가 로컬 사용자에 의해 시작되므로 애플리케이션이 올바르게 작동합니다.

VMware Workstation

Kaspersky Endpoint Security는 VMware Workstation 가상 컴퓨터에 대한 웹 제어 규칙을 제한적으로 지원합니다. 애플리케이션은 사용자별 필터가 구성된 규칙을 지원하지 않습니다. 가상 컴퓨터 프로세스가 시스템 사용자(SYSTEM)로 실행 중입니다. 따라서 가상 컴퓨터에서 웹사이트를 열려고 하는 사용자를 식별할 수 없습니다.

Microsoft Hyper-V

Kaspersky Endpoint Security는 Microsoft Hyper-V 가상 컴퓨터에 대한 웹 제어 규칙을 지원하지 않습니다.

웹 제어 메시지 템플릿 변수

사용자 메시지 템플릿 또는 관리자 메시지 템플릿에서 다음 변수를 사용할 수 있습니다.

- **사용자** – `%USER_NAME%`.

  메시지가 생성된 컴퓨터의 현재 사용자 이름으로, `<device name>\<user alias>` 형식으로 표시됩니다(예: `DESKTOP-123\John.Smith`).

- **웹 리소스 주소** – `%CANONIC_REQUEST_URL%`.

  차단된 웹 리소스의 주소입니다.

- **규칙 이름** – `%RULE%`.

  웹 리소스를 차단한 규칙의 이름입니다.

- **메시지 전송 이메일** – `%COMPLAIN_EMAIL%`.

  웹 리소스 차단 관련 피드백 제출용 이메일 주소입니다. 이메일 주소를 클릭하면 관리자에게 메시지를 작성할 수 있는 창이 열립니다.

- **콘텐츠 카테고리 이름** – `%CONTENT_CATEGORY_LIST%`.

  차단된 리소스가 속한 웹사이트 카테고리입니다(예, *결제 시스템*).

- **데이터 유형 카테고리 이름** – `%TYPE_CATEGORY_LIST%`.

  차단된 웹 리소스의 데이터 유형 카테고리입니다(예, *그래픽 파일*).

- **요청한 웹 리소스 링크** – `%CONTINUE_PAGE%`.

  요청한 웹 페이지 링크(예, `http://www.example.com/pagename.html`).

- **웹사이트 링크** – %CONTINUE_SITE%.

  요청한 웹 페이지가 포함된 웹사이트 링크(예, http://www.example.com/).

- **도메인 접근용 링크** – %CONTINUE_DOMAIN%.

  도메인 이름에 해당하는 모든 기존 웹 페이지에 접근할 수 있는 클릭 가능한 링크입니다. 예를 들어 차단된 웹 페이지의 주소가 http://www.example.com인 경우, %CONTINUE_DOMAIN% 변수는 http://*.example.com 링크로 대체됩니다. 이 링크를 클릭하면 기본 도메인 이름인 http://www.example.com/의 모든 웹 주소에 접근할 수 있으며, 이는 http://start.example.com/* 또는 http://domain.domain.example.com/* 등의 하위 도메인을 포함합니다. 여기에서 * 문자는 모든 문자열(빈 문자열 포함)을 의미합니다.

장치 제어

장치 제어는 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 제어를 사용하면 애플리케이션이 연결된 장치에 대한 정보를 Kaspersky Security Center에 중계합니다. **고급 → 저장소 → 하드웨어** 폴더의 Kaspersky Security Center에서 연결된 장치 목록을 볼 수 있습니다.

장치 접근 레벨

장치 제어는 다음 레벨에서 접근을 제어합니다:

- **장치 유형**. 예: 프린터, 이동식 드라이브 및 CD/DVD 드라이브.

  다음과 같이 장치 접근 설정을 구성할 수 있습니다:

  - 허용 - .
  - 차단 - .
  - 규칙에 따라(프린터 및 휴대용 장치만) – .
  - 연결 버스에 종속(Wi-Fi 제외) - .
  - 예외를 제외하고 차단(Wi-Fi 전용) - .

- **연결 버스**. *연결 버스*는 장치를 컴퓨터에 연결하는 데 사용하는 인터페이스입니다(USB 또는 FireWire 등). 장치 유형에 **연결 버스에 종속** 모드가 선택되면 애플리케이션이 연결 인터페이스(예: USB)에 따라 장치에 대한 접근을 허용하거나 거부합니다.

  다음과 같이 장치 접근 설정을 구성할 수 있습니다:

  - 허용 - .
  - 차단 - .

- **신뢰하는 장치**. *신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.

다음 데이터를 기반으로 신뢰하는 장치를 추가할 수 있습니다:

- **ID로 장치 추가**. 각 장치에는 고유 ID가 있습니다(하드웨어 ID 또는 HWID). 운영 체제 도구를 사용하여 장치 속성에서 ID를 볼 수 있습니다. 장치 ID의 예: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. 여러 특정 장치를 추가하려는 경우 ID별로 장치를 추가하는 것이 편리합니다.

- **모델로 장치 추가**. 각 장치에는 공급업체 ID(VID) 및 제품 ID(PID)가 있습니다. 운영 체제 도구를 사용하여 장치 속성에서 ID를 볼 수 있습니다. VID 및 PID 입력을 위한 템플릿: `VID_1234&PID_5678`. 조직에서 특정 모델의 장치를 사용하는 경우 모델별로 장치를 추가하는 것이 편리합니다. 이런 식으로 이 모델의 모든 장치를 추가할 수 있습니다.

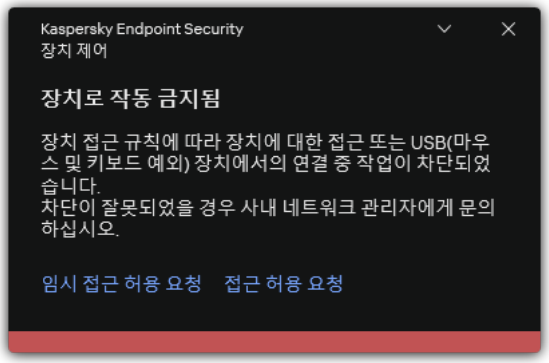
- **ID 마스크로 장치 추가**. 비슷한 ID를 가진 여러 장치를 사용하는 경우 마스크를 사용하여 신뢰하는 목록에 장치를 추가할 수 있습니다. `*` 문자는 모든 문자의 조합을 나타냅니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `?` 문자를 지원하지 않습니다. 예: `WDC_C*`.

- **모델 마스크로 장치 추가**. 비슷한 VID 또는 PID를 가진 여러 장치를 사용하는 경우(예: 동일한 제조업체의 장치), 마스크를 사용하여 신뢰하는 목록에 장치를 추가할 수 있습니다. `*` 문자는 모든 문자의 조합을 나타냅니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `?` 문자를 지원하지 않습니다. 예: `VID_05AC&PID_*`.

장치 제어는 *접근 규칙*을 사용하여 장치에 대한 사용자 접근을 규제합니다. 장치 제어를 사용하면 장치 연결/연결 끊김 이벤트도 저장할 수 있습니다. 이벤트를 저장하려면 정책에서 이벤트 등록을 구성해야 합니다.

장치에 대한 접근이 연결 버스(상태)에 따른다면 Kaspersky Endpoint Security는 장치 연결/연결 끊김 이벤트를 저장하지 않습니다. Kaspersky Endpoint Security를 사용하여 장치 연결/연결 끊김 이벤트를 저장하려면 해당 장치에 대한 접근을 허용하거나(상태) 장치를 신뢰하는 목록에 추가합니다.

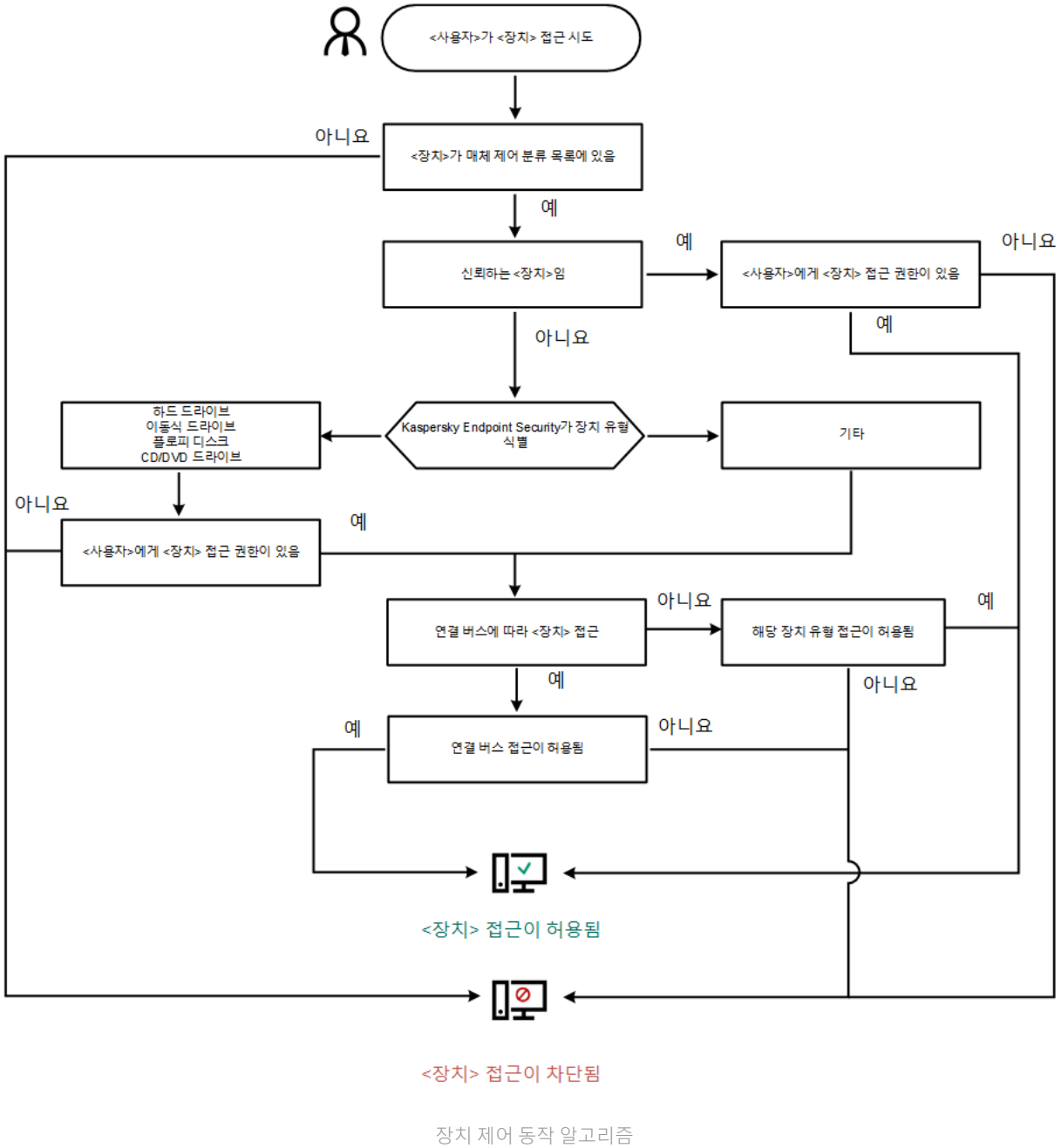
장치 제어로 차단된 장치가 컴퓨터에 연결되면 Kaspersky Endpoint Security가 접근을 차단하고 알림을 표시합니다(아래 그림 참조).



장치 제어 알림

장치 제어 동작 알고리즘

Kaspersky Endpoint Security는 사용자가 장치를 컴퓨터에 연결한 후 장치에 대한 접근을 허용할지 여부를 결정합니다(아래 그림 참조).



장치 제어 동작 알고리즘

장치가 연결되고 접근이 허용되는 경우에는 접근 규칙을 편집하고 접근을 차단할 수 있습니다. 이 경우 다음 번에 누군가가 이 장치에 접근을 시도하면(폴더 트리 보기, 읽기/쓰기 작업 수행 등) Kaspersky Endpoint Security에서 접근을 차단합니다. 파일 시스템이 없는 장치는 다음 번에 장치가 연결되는 경우에만 차단됩니다.

Kaspersky Endpoint Security가 설치된 컴퓨터의 사용자가 본인이 실수로 차단되었다고 생각하는 장치에 접근을 요청해야 하는 경우 사용자에게 접근 허용 요청 안내를 전송합니다.

접근 규칙 정보

*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. 장치 제어 분류를 벗어나는 장치는 추가할 수 없습니다. 그러한 장치에 대한 접근은 모든 사용자에게 허용됩니다.

장치 접근 규칙

접근 규칙에 대한 설정 그룹은 장치 유형에 따라 다릅니다(아래 표 참조).

접근 규칙 설정

장치	접근 제어	장치 접근 스케줄	사용자 및 사용자 그룹 할당	우선순위	읽기/쓰기 권한
하드 드라이브	✓	✓	✓	✓	✓
이동식 드라이브(USB 플래시 드라이브 포함)	✓	✓	✓	✓	✓
플로피 디스크	✓	✓	✓	✓	✓
CD/DVD 드라이브	✓	✓	✓	✓	✓
휴대용 장치(MTP)	✓	✓	✓	✓	✓
로컬 프린터	✓	–	✓	✓	–
네트워크 프린터	✓	–	✓	✓	–
모뎀	✓	–	–	–	–
테이프 장치	✓	–	–	–	–
다기능 장치	✓	–	–	–	–
스마트 카드 리더기	✓	–	–	–	–
Windows CE USB ActiveSync 장치	✓	–	–	–	–
외부 네트워크 어댑터	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
카메라 및 스캐너	✓	–	–	–	–

Wi-Fi 네트워크에 대한 접근 규칙

Wi-Fi 네트워크 접근 규칙은 Wi-Fi 네트워크 사용이 허용되는지(✓ 상태) 또는 금지되는지(⊘ 상태)를 결정합니다. *신뢰하는 Wi-Fi 네트워크*(상태)를 규칙에 추가할 수 있습니다. 신뢰하는 Wi-Fi 네트워크의 사용은 제한 없이 허용됩니다. 기본적으로 Wi-Fi 네트워크 접근 규칙은 모든 Wi-Fi 네트워크에 대한 접근을 허용합니다.

연결 버스 접근 규칙

장치 유형별 접근 규칙에 **연결 버스에 종속** 값이 선택되면 애플리케이션이 연결 인터페이스에 따라 장치에 대한 접근을 허용하거나 거부합니다. 기본적으로 장치 제어 구성 요소의 분류에 포함되는 모든 연결 버스에 대해 버스 접근을 허용하는 규칙이 생성됩니다.

연결 버스 접근 규칙은 장치 연결이 허용되는지(상태) 또는 금지되는지(상태)를 결정합니다. 장치 유형 접근 규칙의 우선순위가 연결 버스 접근 규칙의 우선순위보다 높습니다.

장치 제어 사용 중에는 키보드와 마우스를 잠글 수 없습니다. USB 연결 버스 접근을 금지하면 사용자는 계속해서 USB로 연결된 키보드와 마우스로 작업하게 됩니다. BadUSB 공격 방지 구성 요소는 키보드를 모방하는 감염된 USB 장치가 컴퓨터에 연결되는 것을 방지하도록 설계되었습니다.

유형별 장치 접근 관리

장치 제어를 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. 장치 제어 분류를 벗어나는 장치는 추가할 수 없습니다. 그러한 장치에 대한 접근은 모든 사용자에게 허용됩니다.

기본적으로 장치 제어는 모든 사용자의 모든 장치에 대한 접근을 허용합니다.

다음과 같이 장치에 대한 접근을 구성할 수 있습니다:

- **허용**.

  Kaspersky Endpoint Security가 모든 사용자에게 장치에 대한 전체 접근 권한을 부여합니다.

- **차단**.

  Kaspersky Endpoint Security가 장치 연결을 차단합니다. 애플리케이션이 신뢰하는 장치의 연결만 허용합니다.

- **연결 버스에 종속**.

  Kaspersky Endpoint Security가 장치의 연결 인터페이스를 결정하고 버스 연결 상태에 따라 장치에 대한 접근을 제한합니다. 애플리케이션이 신뢰하는 장치의 연결도 허용합니다.

- **규칙에 따라**.

  일부 장치 유형에서는 장치 사용이 허용된 개별 사용자나 사용자 그룹을 지정하고, 장치 접근 스케줄을 설정하고, 읽기 및 쓰기 권한을 구성할 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.

관리 콘솔(MMC)에서 유형별로 장치 접근을 관리하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **보안 제어 → 장치 제어**를 선택합니다.

5. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   장치 유형 탭에는 장치 제어 분류에 포함된 모든 장치의 접근 규칙이 표시됩니다.

6. 장치 접근 규칙 구성:

   a. **허용**, **차단**, **연결 버스에 종속**, **규칙에 따라** 등 접근 모드를 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(이동식 미디어 등)는 개별 사용자의 접근 권한을 구성할 수 있습니다. 또한, 장치 접근 스케줄을 설정하고 읽기 및 쓰기 권한을 구성할 수 있습니다.
      장치를 신뢰함 목록에 추가할 수 있습니다. *신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.

   d. 필요하다면 인쇄 규칙을 구성합니다.

   e. 필요하다면 Bluetooth 장치 접근 규칙을 구성합니다.

   f. 필요하다면 컴퓨터 Wi-Fi 연결 규칙을 구성합니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 유형별 장치 접근 관리 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어** → **장치 제어**로 이동합니다.

5. **장치 접근 규칙**에서, **장치 및 Wi-Fi 네트워크** 탭을 선택합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.

6. 장치 접근 규칙 구성:

   a. **허용**, **차단**, **버스에 따라 다름**, **사용자 지정** 등 접근 모드를 선택합니다.
      드롭다운 메뉴에 접근 모드가 없다면 장치 유형을 더블 클릭하여 접근 규칙 속성을 엽니다.

   b. **버스에 따라 다름** 접근 모드를 선택하면 **연결 버스** 탭에서 연결 인터페이스에 대한 접근 규칙을 구성해야 합니다.

   c. 저장 장치(이동식 미디어 등)는 개별 사용자의 접근 권한을 구성할 수 있습니다. 또한, 장치 접근 스케줄을 설정하고 읽기 및 쓰기 권한을 구성할 수 있습니다.
      장치를 신뢰함 목록에 추가할 수 있습니다. *신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.

   d. 필요하다면 인쇄 규칙을 구성합니다.

e. 필요하다면 Bluetooth 장치 접근 규칙을 구성합니다.

f. 필요하다면 컴퓨터 Wi-Fi 연결 규칙을 구성합니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 장치 접근을 관리하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **장치 및 Wi-Fi 네트워크** 링크를 클릭합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.
4. 장치 접근 규칙 구성:
   a. **허용**, **차단**, **연결 버스에 종속**, **규칙에 따라** 등 접근 모드를 선택합니다.
      드롭다운 메뉴에 접근 모드가 없다면 장치 유형을 더블 클릭하여 접근 규칙 속성을 엽니다.
   b. **연결 버스에 종속** 접근 모드를 선택하면 **연결 버스** 탭에서 연결 인터페이스에 대한 접근 규칙을 구성해야 합니다.
   c. 저장 장치(이동식 미디어 등)는 개별 사용자의 접근 권한을 구성할 수 있습니다. 또한, 장치 접근 스케줄을 설정하고 읽기 및 쓰기 권한을 구성할 수 있습니다.
      장치를 신뢰함 목록에 추가할 수 있습니다. *신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.
   d. 필요하다면 인쇄 규칙을 구성합니다.
   e. 필요하다면 Bluetooth 장치 접근 규칙을 구성합니다.
   f. 필요하다면 컴퓨터 Wi-Fi 연결 규칙을 구성합니다.
5. 변경 사항을 저장합니다.

결과적으로, 사용자가 장치 접근 권한을 획득하려고 하면 애플리케이션이 규칙에 따라 접근을 차단합니다. Kaspersky Endpoint Security는 해당 이벤트도 기록합니다. 개별 장치에 대한 접근 권한을 부여하려면 해당 장치를 신뢰하는 장치 목록에 추가할 수 있습니다.

연결 버스별 장치 접근 관리

연결 버스 접근 규칙을 편집하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **연결 버스** 버튼을 클릭합니다.
   창이 열리면 장치 제어 구성 요소 분류에 포함된 모든 연결 버스에 대한 접근 규칙이 표시됩니다.
4. 편집할 접근 규칙을 선택합니다.

5. **접근** 열에서 연결 버스에 대한 접근 허용 여부를 선택합니다(**허용** 또는 **차단**).

> 연결 버스에 대한 액세스 권한 변경 시, **직렬 포트**(COM) 또는 **병렬 포트**(LPT) 접근 규칙을 활성화하려면 컴퓨터를 다시 시작해야 합니다.

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 제어를 통해 *저장 장치*의 데이터에 대한 사용자 접근 권한을 구성할 수 있습니다. 이러한 장치에 쓰기 및 읽기 권한을 구성할 수 있습니다. 장치 제어는 다음 유형의 *저장 장치*를 지원합니다:

- 하드 드라이브
- 이동식 드라이브(USB 플래시 드라이브 포함)
- 플로피 디스크
- CD/DVD 드라이브
- 휴대용 장치(MTP). 휴대용 장치(MTP)는 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.

관리 콘솔(MMC)에서 저장 장치의 데이터에 대한 사용자 접근 권한을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **보안 제어 → 장치 제어**를 선택합니다.
5. **장치 제어 설정**에서 **장치 유형** 탭을 선택합니다.
   장치 유형 탭에는 장치 제어 분류에 포함된 모든 장치의 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 누릅니다.

      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 Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Endpoint Security는 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 Endpoint Security가 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**을 누릅니다.

8. **선택한 접근 규칙에 대한 스케줄**에서, 사용자의 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. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 저장 장치의 데이터에 대한 사용자 접근 권한을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어** → **장치 제어**로 이동합니다.

5. **장치 접근 규칙** 블록의 접근 규칙 표에서 저장 장치에 대한 접근 규칙의 속성을 엽니다.

6. **장치 접근 규칙** 블록에서 **사용자 지정**을 선택합니다.

7. 저장 장치 접근 규칙 구성:

   a. **사용자 및 권한** 블록에서 **추가** 버튼을 누릅니다.

      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 Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Endpoint Security는 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 Endpoint Security가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.

c. **사용자/그룹**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. **접근 스케줄**에서 사용자의 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. **저장**을 클릭합니다.

8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 저장 장치의 데이터에 대한 사용자 접근 권한을 구성하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **장치 및 Wi-Fi 네트워크** 링크를 클릭합니다.

이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.

4. 저장 장치 접근 규칙을 구성하려면 오른쪽 클릭하여 규칙 목록을 엽니다.
5. 저장 장치 접근 규칙 구성:

a. **사용자 권한** 블록에서 **추가** 버튼을 누릅니다.

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 Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Endpoint Security는 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 Endpoint Security가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.

c. **사용자**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**을 누릅니다.

6. **장치 접근 스케줄**에서 사용자의 저장 장치 접근 스케줄을 구성합니다.
   예를 들어 사용자가 작업 시간에만 저장 장치를 사용하도록 허용할 수 있습니다.

7. 파일 관리자에서 저장 장치에 대한 사용자의 접근 권한을 구성합니다(**읽기/쓰기**).

8. 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.

모바일 장치에 대한 액세스 관리

Kaspersky Endpoint Security를 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. ADB(Android Debug Bridge), iTunes 또는 이와 동등한 애플리케이션이 컴퓨터에 설치된 경우 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 Endpoint Security를 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 Endpoint Security는 모바일 장치에 대한 전체 접근을 허용합니다. 파일 관리자 또는 ADB 및 iTunes 애플리케이션을 사용하여 모바일 장치에서 파일을 열거나 생성, 수정, 복사, 삭제할 수 있습니다. 모바일 장치를 컴퓨터의 USB 포트에 연결하여 장치의 배터리를 충전할 수도 있습니다.

- **차단** ⊘. Kaspersky Endpoint Security는 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 Endpoint Security는 USB 연결 상태(**허용** 또는 **차단**)에 따라 모바일 장치에 대한 연결을 허용합니다.
- **규칙에 따라**. Kaspersky Endpoint Security는 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 접근 권한을 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.

관리 콘솔(MMC)에서 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 창에서 **보안 제어** → **장치 제어**를 선택합니다.
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. **휴대용 장치(MTP)** 장치 유형의 마우스 오른쪽 메뉴에서, 모바일 장치 접근 모드를 **허용**(), **차단**(), **연결 버스에 종속**() 등으로 구성합니다.
6. 모바일 장치 접근 규칙을 구성하려면 더블 클릭하여 규칙 목록을 엽니다.
7. 모바일 장치 접근 규칙 구성:

   a. **접근 규칙** 블록에서 **추가** 버튼을 누릅니다.

   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 Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Endpoint Security는 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 Endpoint Security가 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**을 누릅니다.

8. **선택한 접근 규칙에 대한 스케줄**에서, 사용자의 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.

9. 파일 관리자에서 모바일 장치에 대한 사용자의 접근 권한을 구성합니다(**읽기/쓰기**).

10. **ADB를 통한 액세스** 확인란을 선택하여 ADB 애플리케이션을 통해 모바일 장치의 데이터에 대한 권한을 구성합니다.

    확인란을 선택 취소하면 모바일 장치가 연결될 때 ADB 애플리케이션이 장치를 감지하지 못합니다.

11. **iTunes를 통한 액세스**에서 iTunes 애플리케이션을 통해 모바일 장치의 데이터에 대한 접근 권한을 구성합니다.

> Kaspersky Endpoint Security는 모든 사용자의 iTunes 애플리케이션을 통한 모바일 장치 접근 권한 설정을 적용합니다. iTunes 장치에 대해 별도의 접근 스케줄을 구성할 수는 없습니다.

12. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 모바일 장치 접근 규칙을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어** → **장치 제어**로 이동합니다.

5. **장치 접근 규칙** 블록에서 **장치 및 Wi-Fi 네트워크** 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 **허용**, **차단**, **버스에 따라 다름** 또는 **사용자 지정** 중 하나로 구성합니다.

8. **모든 사용자의 iTunes를 통한 접근 활성화됨** 토글 스위치를 사용하여 iTunes 애플리케이션을 통한 모바일 장치의 데이터에 대한 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. **사용자 지정** 모드를 선택하면 장치 접근 규칙을 추가해야 합니다. 그러려면 **사용자 및 권한**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 Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Endpoint Security는 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 Endpoint Security가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.

   b. **사용자/그룹**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. **규칙 스케줄**에서 사용자의 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** 확인란을 선택하여 ADB 애플리케이션을 통해 모바일 장치의 데이터에 대한 권한을 구성합니다.

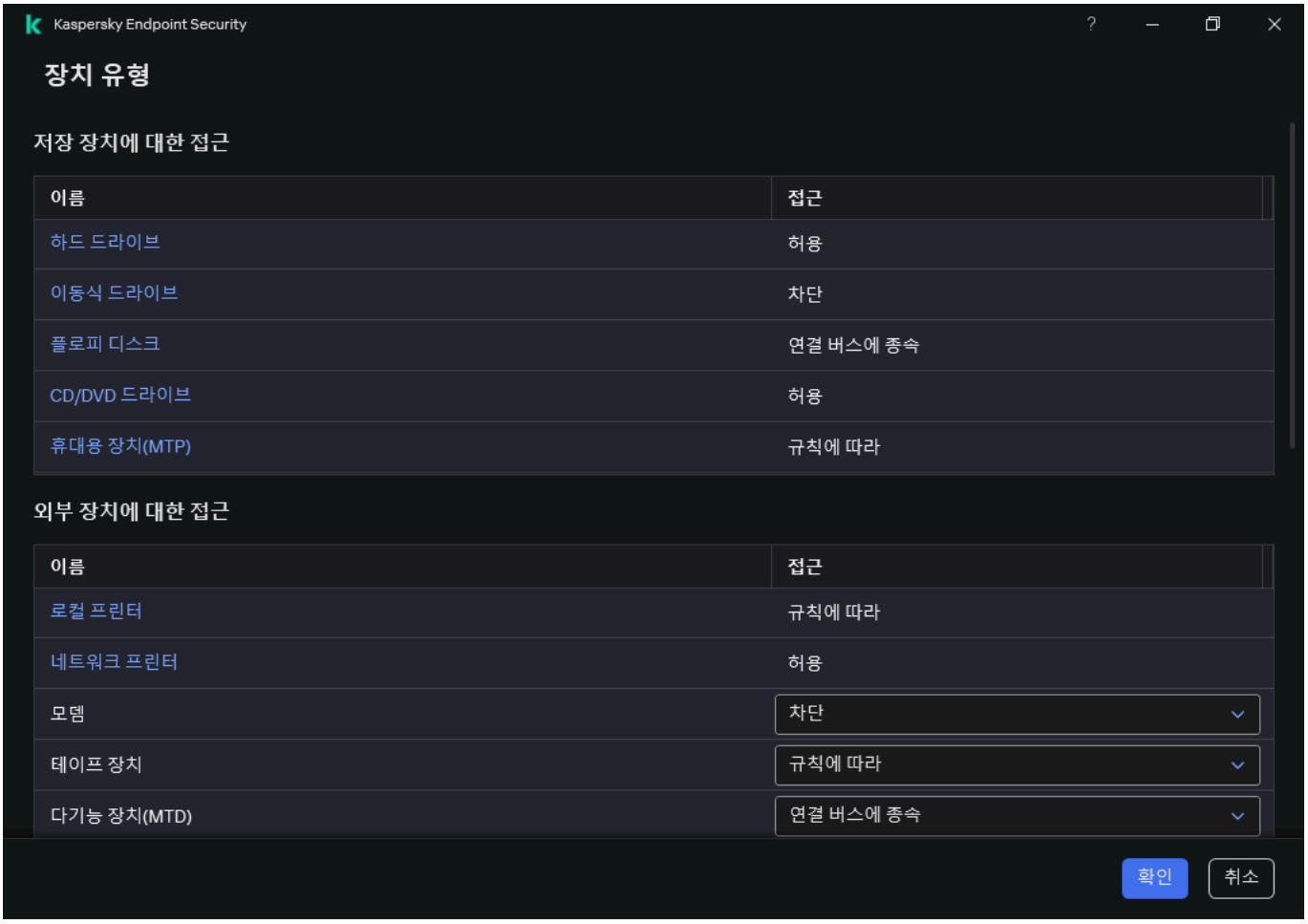
   확인란을 선택 취소하면 모바일 장치가 연결될 때 ADB 애플리케이션이 장치를 감지하지 못합니다.

10. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 모바일 장치 접근 규칙을 구성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **장치 및 Wi-Fi 네트워크** 버튼을 클릭합니다.

열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.



장치 제어 구성 요소의 장치 유형

4. **저장 장치에 대한 접근** 블록에서, **휴대용 장치(MTP)** 링크를 클릭합니다.
   그러면 휴대용 장치(MTP) 접근 규칙이 포함된 창이 열립니다.

5. **접근**에서, **허용**, **차단**, **연결 버스에 종속**, **규칙에 따라** 중 하나로 모바일 장치 접근 모드를 구성합니다.

6. **규칙에 따라** 모드를 선택하면 장치 접근 규칙을 추가해야 합니다:

   a. **사용자 권한** 블록에서 **추가** 버튼을 누릅니다.
      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 Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Endpoint Security는 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 Endpoint Security가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.

   c. **상태**에서, 모바일 장치 접근 규칙을 켭니다.

d. **접근 규칙**에서 사용자의 모바일 장치 접근 권한을 구성합니다.

- 파일 관리자에서 모바일 장치에 대한 사용자의 접근 권한을 구성합니다(**읽기/쓰기**).
- **ADB를 통한 액세스** 확인란을 선택하여 ADB 애플리케이션을 통해 모바일 장치의 데이터에 대한 권한을 구성합니다.

  확인란을 선택 취소하면 모바일 장치가 연결될 때 ADB 애플리케이션이 장치를 감지하지 못합니다.

e. **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.

f. **장치 접근 스케줄**에서 사용자의 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.

g. **iTunes를 통한 액세스**에서 iTunes 애플리케이션을 통해 모바일 장치의 데이터에 대한 접근 권한을 구성합니다.

> Kaspersky Endpoint Security는 모든 사용자의 iTunes 애플리케이션을 통한 모바일 장치 접근 권한 설정을 적용합니다. iTunes 장치에 대해 별도의 접근 스케줄을 구성할 수는 없습니다.

7. 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

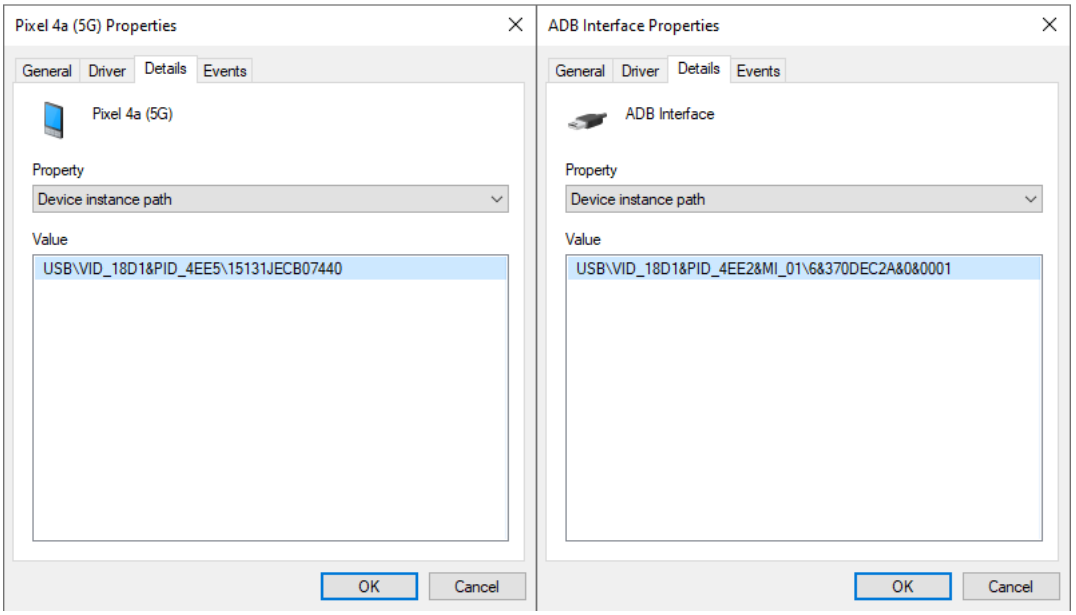
*신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.

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 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. 이는 Kaspersky Endpoint Security가 해당 장치를 새로운 장치로 식별함을 의미합니다. 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

Bluetooth 장치에 대한 접근 관리

Kaspersky Endpoint Security는 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 Endpoint Security는 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 Endpoint Security는 모든 Bluetooth 장치의 연결을 허용하며 연결 정보를 이벤트 로그에 저장하지 않습니다. 사용자는 Bluetooth 입력 장치(키보드, 마우스 등)를 연결하고, Bluetooth로 데이터를 전송하고, 기타 Bluetooth 장치(헤드셋, 헤드폰 등)를 관리할 수 있습니다.
- **허용**. Kaspersky Endpoint Security에서 Bluetooth 장치에 대한 접근을 허용합니다. 사용자는 Bluetooth 입력 장치(키보드, 마우스 등)를 연결하고, Bluetooth로 데이터를 전송하고, 기타 Bluetooth 장치(헤드셋, 헤드폰 등)를 관리할 수 있습니다.
- **차단**. Kaspersky Endpoint Security에서 Bluetooth 장치에 대한 접근을 제한합니다. Bluetooth 입력 장치(Human Interface Devices class)만 연결하도록 허용할 수 있습니다. 이러한 장치로는 키보드, 마우스 장치, 조이스틱 등이 포함됩니다.

신뢰하는 Bluetooth 장치 목록을 생성할 수 없습니다. Bluetooth 장치 접근을 제한했을 경우, Bluetooth 입력 장치 연결만 가능합니다.

관리 콘솔(MMC)에서 Bluetooth 장치 접근 규칙을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **보안 제어 → 장치 제어**를 선택합니다.
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. **Bluetooth** 장치 유형에 맞는 메뉴에서 Bluetooth 장치 액세스 모드를 구성합니다: **허용**, **차단**, **허용하고 기록하지 않음**.
7. **차단** 모드를 선택하면 Bluetooth 입력 장치(키보드, 마우스 등)만 연결하도록 허용할 수 있습니다. 그러려면 **예외** 항목에서 **입력 장치(마우스 및 키보드)** 확인란을 선택합니다.
8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

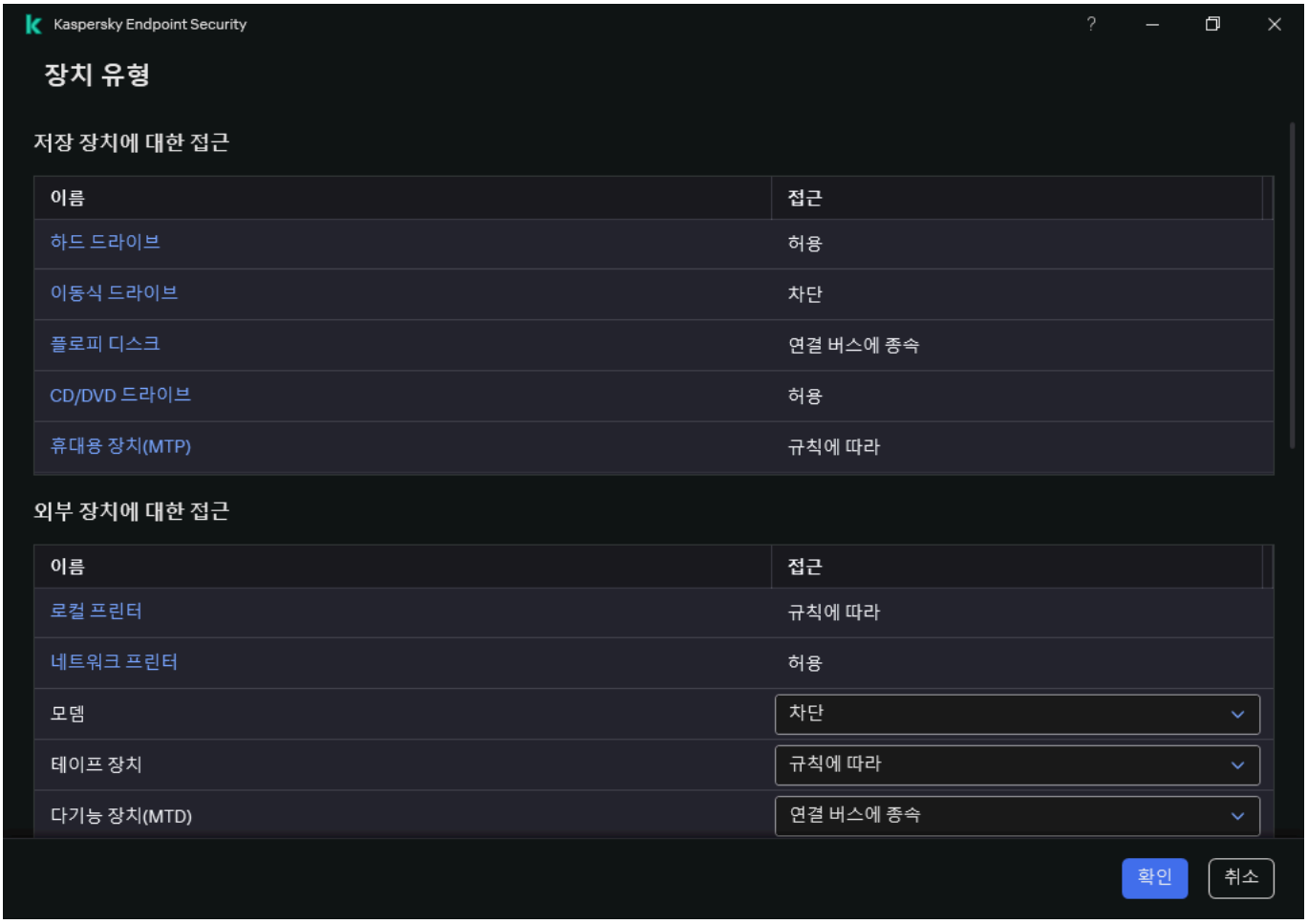
웹 콘솔 및 Cloud Console에서 Bluetooth 장치 접근 규칙을 설정하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어 → 장치 제어**로 이동합니다.
5. **장치 접근 규칙** 블록에서 **장치 및 Wi-Fi 네트워크** 링크를 클릭합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.
6. **Bluetooth 장치** 장치 유형을 선택합니다.
   이것을 선택하면 Bluetooth 장치 접근 설정이 열립니다.
7. Bluetooth 장치 접근 모드를 다음과 같이 설정합니다. **허용**, **차단**, **허용하고 기록하지 않음**.
8. **차단** 모드를 선택하면 Bluetooth 입력 장치(키보드, 마우스 등)만 연결하도록 허용할 수 있습니다. 그러려면 **예외** 항목에서 **입력 장치(마우스 및 키보드)** 확인란을 선택합니다.
9. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 Bluetooth 장치 접근 규칙을 구성하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어 → 장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **장치 및 Wi-Fi 네트워크** 버튼을 클릭합니다.

열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.



장치 제어 구성 요소의 장치 유형

4. **외부 장치에 대한 접근** 블록에서 **Bluetooth** 링크를 클릭합니다.
   이것을 선택하면 Bluetooth 장치 접근 설정이 열립니다.

5. **접근** 항목에서 Bluetooth 장치 액세스 모드를 다음과 같이 설정합니다: **허용**, **차단**, **허용하고 기록하지 않음**.

6. **차단** 모드를 선택하면 Bluetooth 입력 장치(키보드, 마우스 등)만 연결하도록 허용할 수 있습니다. 그러려면 **예외** 항목에서 **입력 장치(마우스 및 키보드)** 확인란을 선택합니다.

7. 변경 사항을 저장합니다.

인쇄 제어

Arm 기반 컴퓨터에서는 인쇄 제어를 지원하지 않습니다.

인쇄 제어를 사용하여 로컬 및 네트워크 프린터에 대한 사용자 액세스를 구성할 수 있습니다.

로컬 프린터 제어

Kaspersky Endpoint Security는 *연결*과 *인쇄*, 두 가지 수준에서 로컬 프린터에 대한 접근을 구성할 수 있습니다.

Kaspersky Endpoint Security는 USB, 직렬 포트(COM), 병렬 포트(LPT) 버스를 통해 로컬 프린터 연결을 제어합니다.

Kaspersky Endpoint Security는 로컬 프린터의 COM 및 LPT 포트 연결을 버스 수준에서만 제어합니다. 따라서 COM 및 LPT 포트를 통한 프린터 연결을 방지하려면 로컬 프린터에 대한 연결 버스에 종속 접근 모드를 선택하고 COM 및 LPT 버스에 대한 연결을 금지해야 합니다.

USB에 연결된 프린터에 대해서는, 애플리케이션이 장치 유형(로컬 프린터)과 연결 버스(USB)의 두 가지 수준에서 제어를 실행합니다.

USB를 통한 다음 로컬 프린터 액세스 모드 중 하나를 선택할 수 있습니다.

- **허용**. Kaspersky Endpoint Security가 모든 사용자에게 로컬 프린터에 대한 전체 액세스 권한을 부여합니다. 사용자는 운영 체제가 제공하는 수단을 사용하여 프린터를 연결하고 문서를 인쇄할 수 있습니다.
- **차단**. Kaspersky Endpoint Security가 로컬 프린터 연결을 차단합니다. 애플리케이션이 신뢰하는 프린터의 연결만 허용합니다.
- **연결 버스에 종속**. Kaspersky Endpoint Security는 USB 버스 연결 상태(**허용** 또는 **차단**)에 따라 로컬 프린터에 연결할 수 있습니다.
- **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 Endpoint Security를 통해 네트워크 프린터에서 인쇄에 대한 액세스를 구성할 수 있습니다. 다음 네트워크 프린터 액세스 모드 중 하나를 선택할 수 있습니다.

- **허용하고 기록하지 않음**. Kaspersky Endpoint Security는 네트워크 프린터의 인쇄를 제어하지 않습니다. 애플리케이션은 모든 사용자에게 인쇄 접근 권한을 부여하며 인쇄 정보를 이벤트 로그에 저장하지 않습니다.
- **허용**. Kaspersky Endpoint Security가 모든 사용자에게 네트워크 프린터에서 인쇄할 수 있는 액세스 권한을 부여합니다.
- **차단**. Kaspersky Endpoint Security가 모든 사용자의 네트워크 프린터 접근을 제한합니다. 애플리케이션은 신뢰하는 프린터에만 액세스를 허용합니다.
- **규칙에 따라**. Kaspersky Endpoint Security가 인쇄 규칙에 따라 인쇄에 대한 접근 권한을 부여합니다. 규칙을 통해 네트워크 프린터에서 문서 인쇄를 허용하거나 금지할 사용자 또는 사용자 그룹을 선택할 수 있습니다.

프린터에 대한 인쇄 규칙 추가

관리 콘솔(MMC)에서 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 창에서 **보안 제어 → 장치 제어**를 선택합니다.
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. **로컬 프린터** 및 **네트워크 프린터** 장치 유형 메뉴에서 관련 프린터에 대한 액세스 모드를 **허용**, **차단**, **허용하고 기록하지 않음**(네트워크 프린터 전용) 또는 **연결 버스에 종속**(로컬 프린터 전용)으로 구성합니다.
6. 로컬 및 네트워크 프린터에서 인쇄 규칙을 구성하려면 규칙 목록을 두 번 클릭하여 엽니다.
7. 프린터 접근 모드로 **규칙에 따라**를 선택합니다.
8. 인쇄 규칙을 적용할 사용자 또는 사용자 그룹을 선택합니다.
   a. **추가**를 클릭합니다.
      새 인쇄 규칙을 추가할 수 있는 창이 열립니다.
   b. 규칙 항목에 우선순위를 할당합니다. 규칙 항목에는 사용자 계정, 작업(허용/차단), 우선순위 특성이 포함됩니다.
      규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Endpoint Security는 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 Endpoint Security가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.
   c. **처리**에서 프린터 인쇄에 대한 사용자 접근을 구성합니다.
   d. **사용자 및 그룹**을 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.
   e. **확인**을 누릅니다.
9. 변경 사항을 저장합니다.

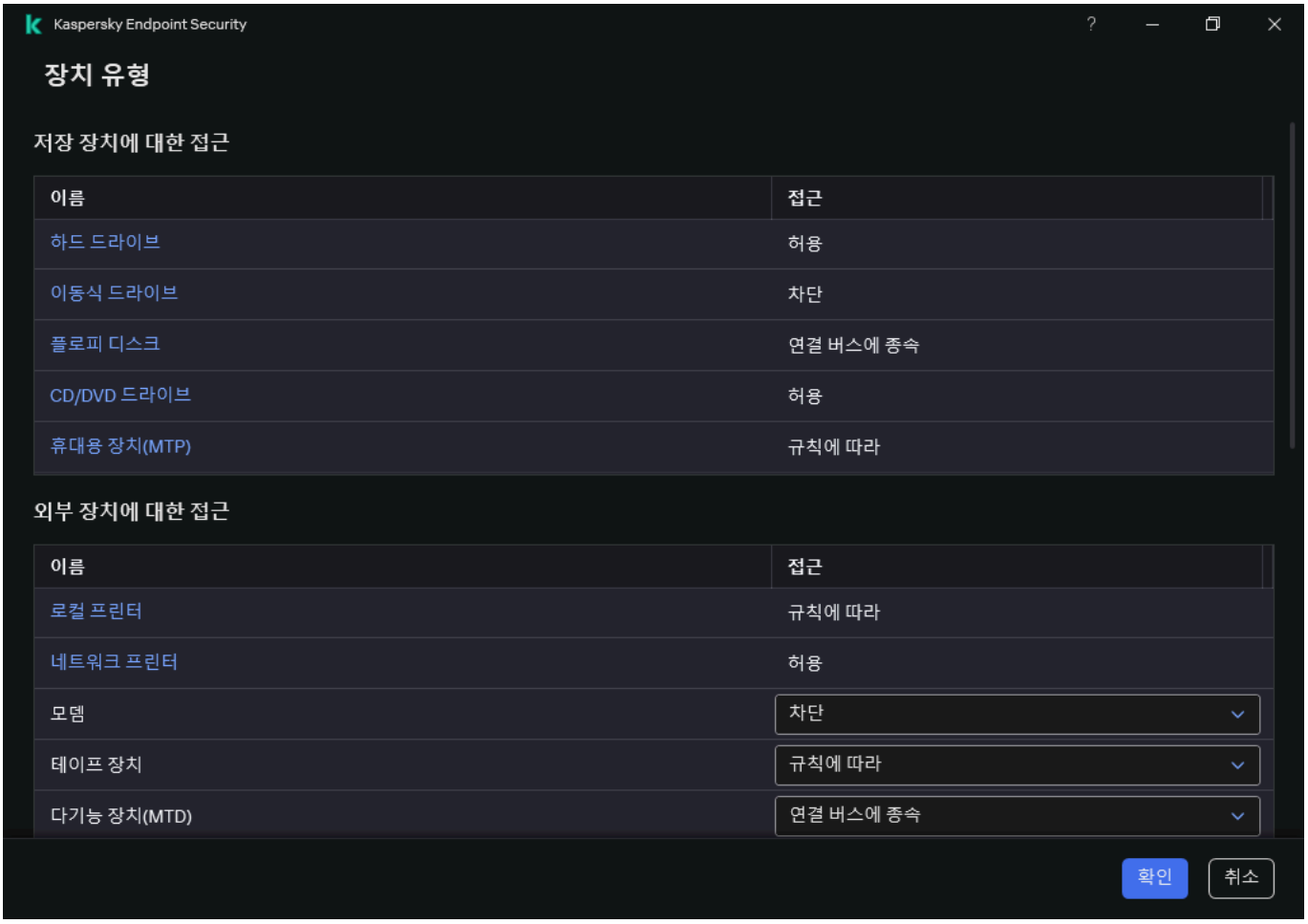
웹 콘솔 및 Cloud Console에서 인쇄 규칙을 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **장치 제어**로 이동합니다.
5. **장치 접근 규칙** 블록에서 **장치 및 Wi-Fi 네트워크** 링크를 클릭합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.
6. **로컬 프린터** 또는 **네트워크 프린터** 장치 유형을 선택합니다.
   프린터 접근 규칙이 열립니다.
7. 관련 프린터의 액세스 모드를 **허용**, **차단**, **허용하고 기록하지 않음**(네트워크 프린터 전용), **버스에 따라 다름**(로컬 프린터 전용) 또는 **사용자 지정**으로 설정합니다.
8. **사용자 지정** 모드를 선택하면 로컬 또는 네트워크 프린터에 대한 인쇄 규칙을 추가해야 합니다. 이렇게 하려면 인쇄 규칙 테이블에서 **추가** 버튼을 클릭합니다.
   그러면 새 인쇄 규칙의 설정이 열립니다.
9. 규칙 항목에 우선순위를 할당합니다. 규칙 항목에는 사용자 계정, 작업(허용/차단), 우선순위 특성이 포함됩니다.
   규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Endpoint Security는 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 Endpoint Security가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.
10. **처리**에서 프린터 인쇄에 대한 사용자 접근을 구성합니다.
11. **사용자/그룹**에서 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.
12. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 인쇄 규칙을 추가하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **장치 및 Wi-Fi 네트워크** 버튼을 클릭합니다.

열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.



장치 제어 구성 요소의 장치 유형

4. **외부 장치에 대한 접근**에서 **로컬 프린터** 또는 **네트워크 프린터**를 클릭합니다.

   그러면 프린터 접근 규칙이 있는 창이 열립니다.

5. **로컬 프린터에 액세스** 또는 **네트워크 프린터에 액세스** 메뉴에서 프린터의 액세스 모드를 **허용**, **차단**, **허용하고 기록하지 않음**(네트워크 프린터 전용), **연결 버스에 종속**(로컬 프린터 전용) 또는 **규칙에 따라**로 구성합니다.

6. **규칙에 따라** 모드를 선택하면 프린터에 대한 인쇄 규칙을 추가해야 합니다. 인쇄 규칙을 적용할 사용자 또는 사용자 그룹을 선택합니다.

   a. **추가**를 클릭합니다.

      새 인쇄 규칙을 추가할 수 있는 창이 열립니다.

   b. 규칙 항목에 우선순위를 할당합니다. 규칙 항목에는 사용자 계정, 권한(읽기/쓰기), 우선순위 특성이 포함됩니다.

      규칙에는 우선순위가 있습니다. 사용자가 여러 그룹에 추가된 경우 Kaspersky Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 장치 접근을 규제합니다. Kaspersky Endpoint Security는 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 Endpoint Security가 기존의 차단 규칙을 기반으로 장치 접근을 규제합니다.

c. **처리**에서 인쇄 액세스에 대한 사용자 권한을 구성합니다.

d. **사용자 및 그룹**에서 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. 변경 사항을 저장합니다.

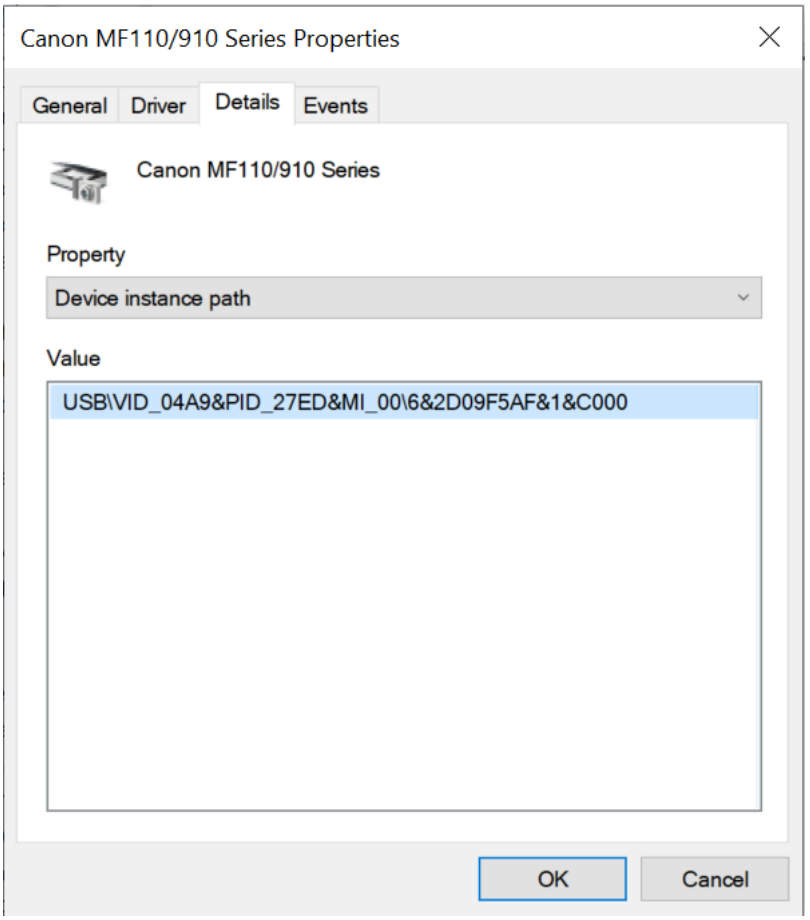
신뢰하는 프린터

*신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.

신뢰하는 프린터 추가 절차는 다른 유형의 신뢰하는 장치에서와 같습니다. ID 또는 장치 모델별로 로컬 프린터를 추가할 수 있습니다. 네트워크 프린터는 장치 ID로만 추가할 수 있습니다.

ID로 신뢰하는 로컬 프린터를 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. 로컬 프린터의 ID 형식은 다음과 같습니다: `6&2D09F5AF&1&C000`. 여러 특정 장치를 추가하려는 경우 ID별로 장치를 추가하는 것이 편리합니다. 마스크를 사용할 수도 있습니다.

장치 모델별로 신뢰하는 로컬 프린터를 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_04A9&PID_27FD`. 조직에서 특정 모델의 장치를 사용하는 경우 모델별로 장치를 추가하는 것이 편리합니다. 이런 식으로 이 모델의 모든 장치를 추가할 수 있습니다.



장치 관리자의 장치 ID

신뢰하는 네트워크 프린터를 추가하려면 장치 ID가 필요합니다. 네트워크 프린터에서 장치 ID는 프린터의 네트워크 이름(공유 프린터의 이름)이나 프린터의 IP 주소, 또는 프린터의 URL일 수 있습니다.

Wi-Fi 연결 제어

장치 제어를 통해 컴퓨터(랩톱)의 Wi-Fi 연결을 관리할 수 있습니다. 공용 Wi-Fi 네트워크는 안전하지 않을 수 있으며 이러한 네트워크를 사용하면 데이터가 손실될 수 있습니다. 장치 제어를 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 제어는 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 Endpoint Security가 Wi-Fi 네트워크에 대한 연결을 제어하지 않습니다.

관리 콘솔(MMC)에서 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 창에서 **보안 제어 → 장치 제어**를 선택합니다.
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. **Wi-Fi** 장치 유형의 마우스 오른쪽 메뉴에서, Wi-Fi에 연결 시 수행할 장치 제어 작업으로 **허용** (), **차단** (), **예외를 제외하고 차단** () 중 하나를 선택합니다.
6. **예외를 제외하고 차단** 옵션 선택 시, 신뢰하는 Wi-Fi 네트워크 목록을 생성합니다:
   a. 신뢰하는 Wi-Fi 네트워크 목록을 두 번 클릭하여 엽니다.
   b. **신뢰하는 Wi-Fi 네트워크** 블록에서 **추가** 버튼을 클릭합니다.
   c. 창이 열리면 신뢰하는 Wi-Fi 네트워크를 구성합니다(아래 그림 참조):
      - **네트워크 이름**. Wi-Fi 네트워크의 이름 또는 SSID(Service Set Identifier).
      - **인증 유형**. Wi-Fi 네트워크 연결에 사용되는 인증 유형.

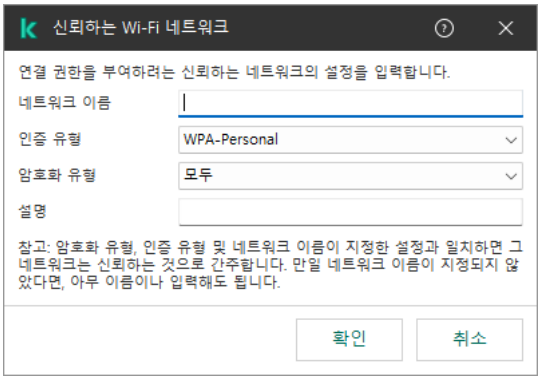
        Kaspersky Endpoint Security for Windows 버전 12.0부터 WPA3 프로토콜 지원이 애플리케이션에 추가되었습니다. Kaspersky Endpoint Security 버전 12.2 정책이 컴퓨터에 적용될 경우, WPA2 프로토콜은 Kaspersky Endpoint Security 버전 11.11.0 이하의 컴퓨터에서 선택됩니다. WPA2 / WPA3은 버전 12.0 ~ 12.1로 선택됩니다. WPA3은 버전 12.2 이상으로 선택됩니다.

      - **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.



신뢰하는 Wi-Fi 네트워크 설정

웹 콘솔 및 Cloud Console에서 Wi-Fi 연결을 제한하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **장치 제어**로 이동합니다.
5. **장치 접근 규칙**에서, **장치 및 Wi-Fi 네트워크** 탭을 선택합니다.
   이 표에는 장치 제어 구성 요소의 분류에 있는 모든 장치에 대한 접근 규칙이 나열되어 있습니다.
6. **Wi-Fi 네트워크** 블록에서 **Wi-Fi** 링크를 클릭합니다.
7. 열린 창에서, **허용**, **차단**, **예외와 함께 차단** 중 Wi-Fi 연결 시 수행할 장치 제어 작업을 선택합니다.
8. **예외와 함께 차단** 옵션 선택 시, 신뢰하는 Wi-Fi 네트워크 목록을 생성합니다:
   a. 신뢰하는 Wi-Fi 네트워크 목록을 두 번 클릭하여 엽니다.
   b. **신뢰하는 Wi-Fi 네트워크** 블록에서 **추가** 버튼을 클릭합니다.
   c. 창이 열리면 신뢰하는 Wi-Fi 네트워크를 구성합니다(아래 그림 참조):
      - **이름**. Wi-Fi 네트워크의 이름 또는 SSID(Service Set Identifier).
      - **인증 유형**. Wi-Fi 네트워크 연결에 사용되는 인증 유형.

Kaspersky Endpoint Security for Windows 버전 12.0부터 WPA3 프로토콜 지원이 애플리케이션에 추가되었습니다. Kaspersky Endpoint Security 버전 12.2 정책이 컴퓨터에 적용될 경우, WPA2 프로토콜은 Kaspersky Endpoint Security 버전 11.11.0 이하의 컴퓨터에서 선택됩니다. WPA2 / WPA3은 버전 12.0 ~ 12.1로 선택됩니다. WPA3은 버전 12.2 이상으로 선택됩니다.

- **암호화 유형**. Wi-Fi 트래픽 보호에 사용되는 암호화 유형.
- **설명**. 추가한 Wi-Fi 네트워크에 대한 추가 정보.

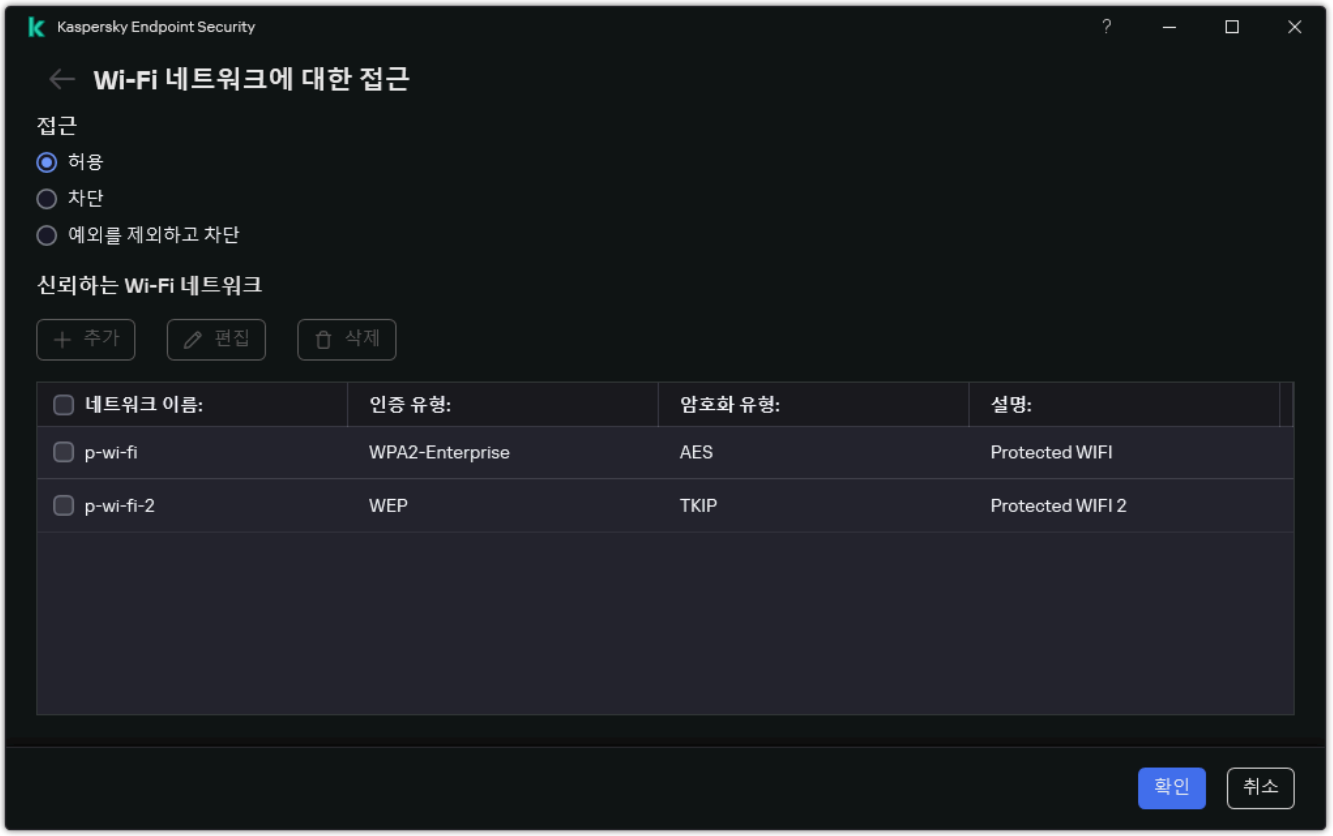
라우터 설정에서 신뢰하는 Wi-Fi 네트워크의 설정을 볼 수 있습니다.

> Wi-Fi 네트워크의 설정이 규칙에 지정된 모든 설정과 일치하는 경우 신뢰할 수 있는 네트워크로 간주됩니다.

9. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 Wi-Fi 연결을 제한하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **장치 및 Wi-Fi 네트워크** 버튼을 클릭합니다.
   열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.
4. **Wi-Fi 네트워크에 대한 접근** 블록에서 **Wi-Fi** 링크를 클릭합니다.
   Wi-Fi 네트워크 접근 규칙을 표시하는 창이 열립니다.



Wi-Fi 접근 설정

5. **접근**에서, **허용**, **차단**, **예외를 제외하고 차단** 중 Wi-Fi에 연결할 때 수행되는 장치 제어 작업을 선택합니다.

6. **예외를 제외하고 차단** 옵션 선택 시, 신뢰하는 Wi-Fi 네트워크 목록을 생성합니다:

   a. **신뢰하는 Wi-Fi 네트워크** 블록에서 **추가** 버튼을 클릭합니다.

   b. 창이 열리면 신뢰하는 Wi-Fi 네트워크를 구성합니다(아래 그림 참조):

   - **네트워크 이름**. Wi-Fi 네트워크의 이름 또는 SSID(Service Set Identifier).
   - **인증 유형**. Wi-Fi 네트워크 연결에 사용되는 인증 유형.

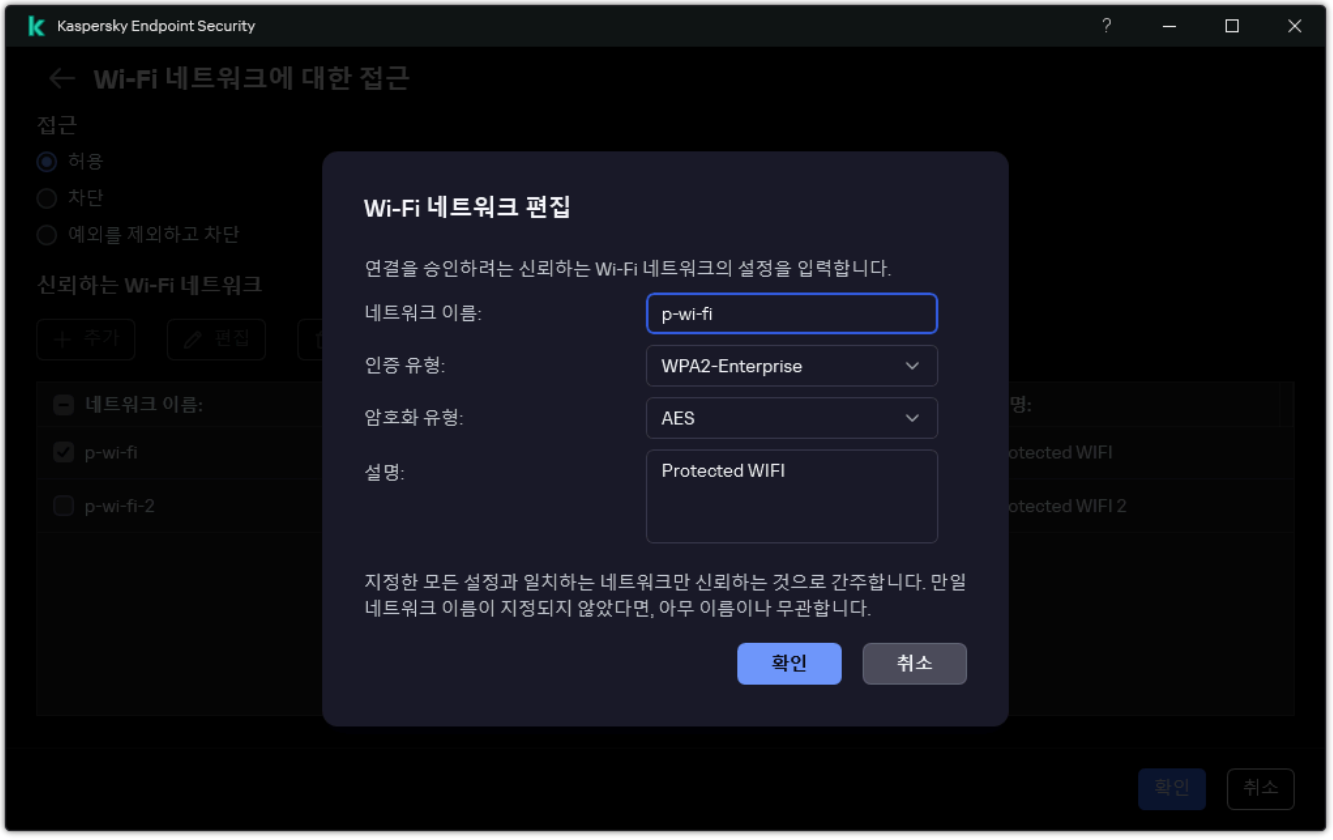
     > Kaspersky Endpoint Security for Windows 버전 12.0부터 WPA3 프로토콜 지원이 애플리케이션에 추가되었습니다. Kaspersky Endpoint Security 버전 12.2 정책이 컴퓨터에 적용될 경우, WPA2 프로토콜은 Kaspersky Endpoint Security 버전 11.11.0 이하의 컴퓨터에서 선택됩니다. WPA2 / WPA3은 버전 12.0 ~ 12.1로 선택됩니다. WPA3은 버전 12.2 이상으로 선택됩니다.

   - **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.

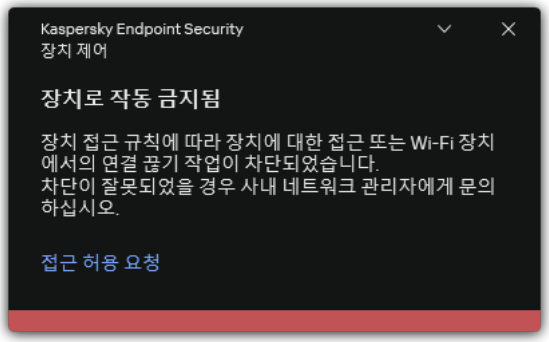
   > Wi-Fi 네트워크의 설정이 규칙에 지정된 모든 설정과 일치하는 경우 신뢰할 수 있는 네트워크로 간주됩니다.

7. 변경 사항을 저장합니다.



신뢰하는 Wi-Fi 네트워크 설정

따라서 신뢰 목록에 없는 Wi-Fi 네트워크에 연결을 시도하면 애플리케이션이 연결을 차단하고 알림을 표시합니다(아래 그림 참조).



장치 제어 알림

이동식 드라이브 사용 감시

이동식 드라이브 사용 감시는 다음을 포함합니다:

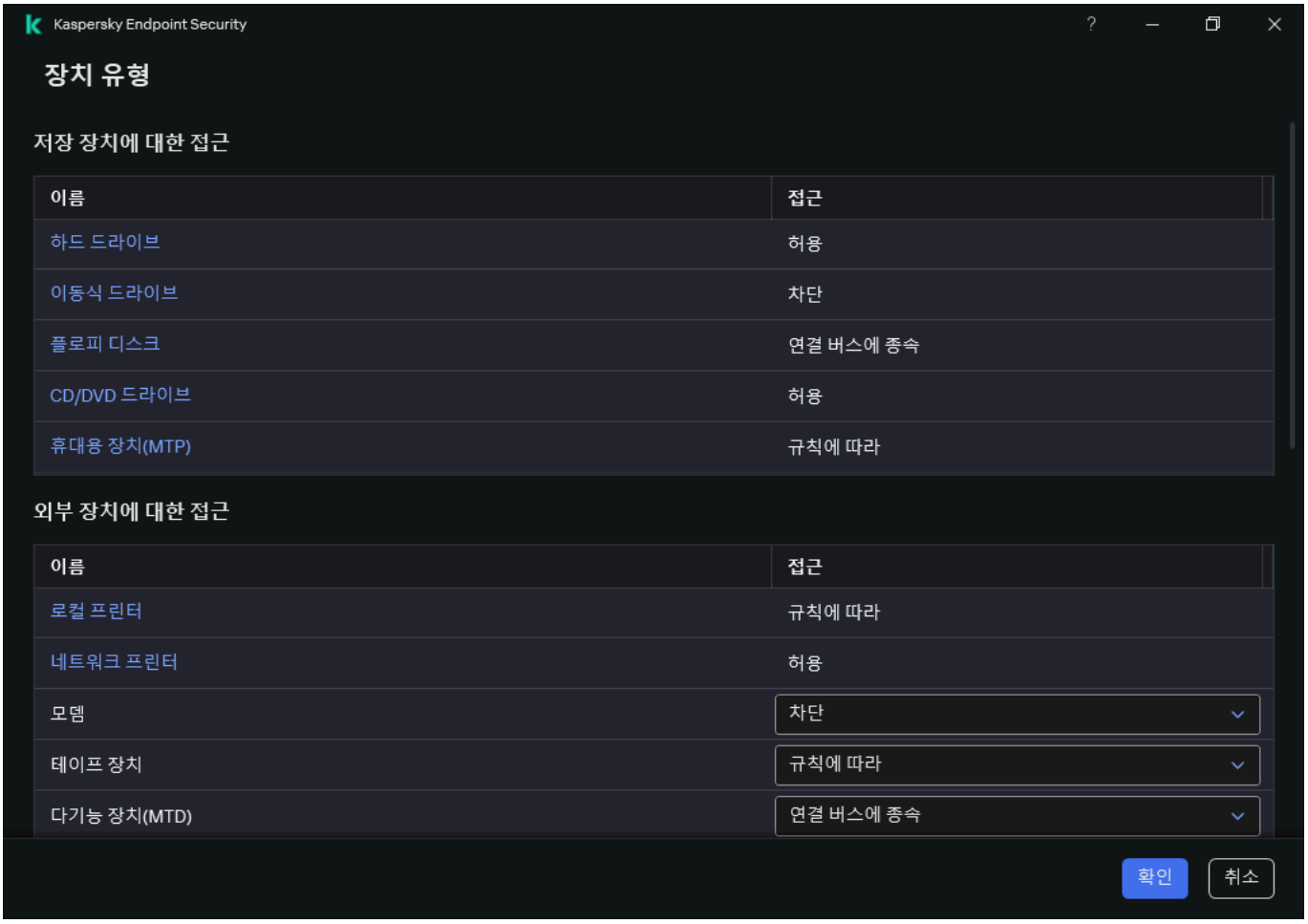
- 이동식 드라이브의 파일에 대한 동작 모니터링.
- 신뢰하는 이동식 드라이브의 연결 및 연결 해제 모니터링.

  Kaspersky Endpoint Security를 사용하면 이동식 드라이브뿐만 아니라 신뢰하는 장치 전체의 연결 및 연결 해제를 모니터링할 수 있습니다. 장치 제어 구성 요소에 대한 이벤트 기록은 알림 설정에서 켤 수 있습니다. 이벤트에는 *정보 메시지*의 심각도가 있습니다.

이동식 드라이브 사용 감시를 사용하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **장치 및 Wi-Fi 네트워크** 버튼을 클릭합니다.

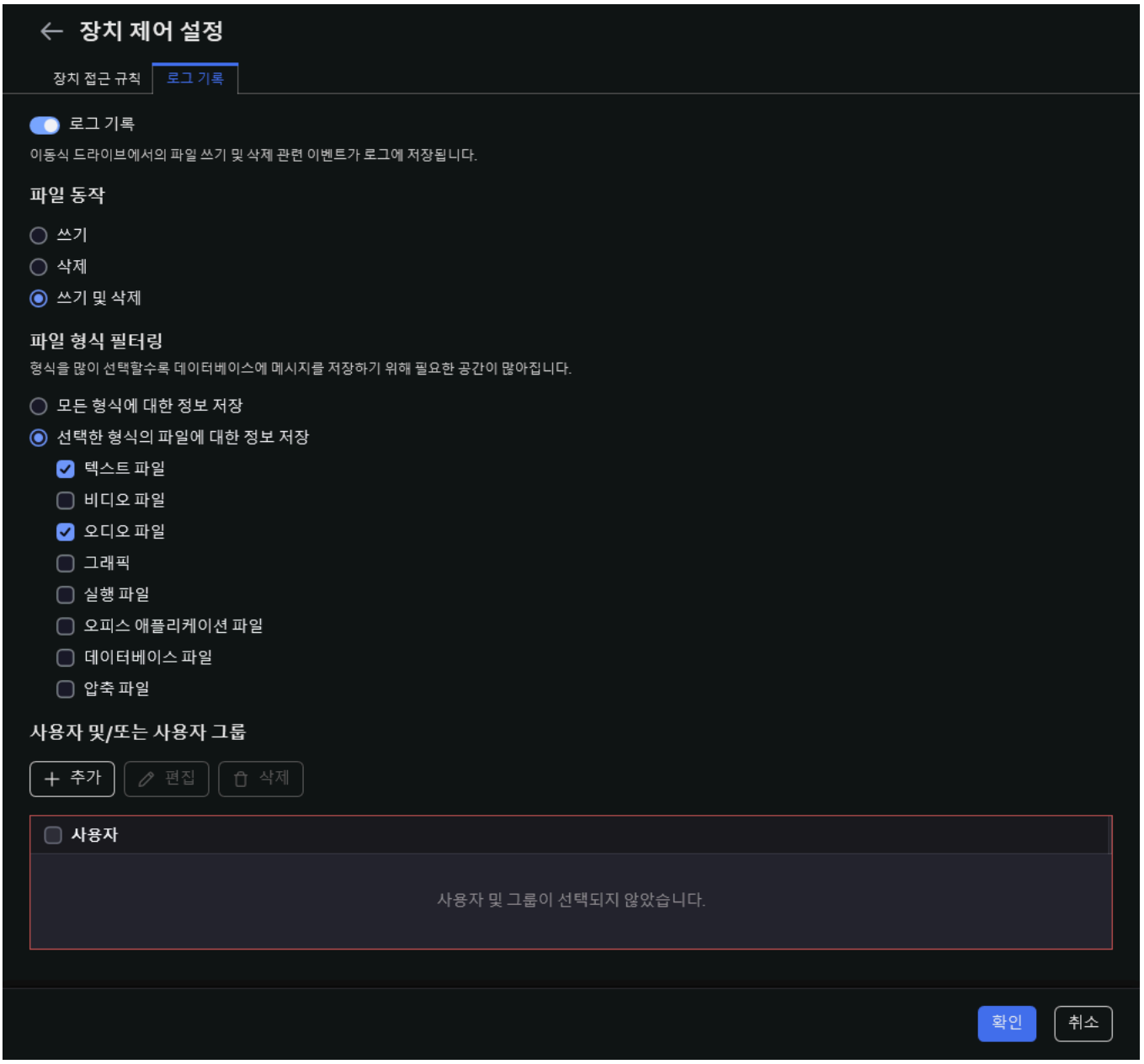
열린 창에는 장치 제어 구성 요소 분류에 포함된 모든 장치에 대한 접근 규칙이 표시됩니다.



장치 제어 구성 요소의 장치 유형

4. **저장 장치에 대한 접근** 블록에서 **이동식 드라이브**를 선택합니다.

5. 창이 열리면 **로그 기록** 탭을 선택합니다.



이동식 드라이브 사용량 모니터링 설정

6. **로그 기록** 토글을 켭니다.

7. **파일 동작** 블록에서 **쓰기**, **삭제** 등 감시할 작업을 선택합니다:

8. **파일 형식 필터링** 블록에서 장치 제어를 통해 연관된 작업을 기록할 파일 형식을 선택합니다.

9. 감시할 이동식 드라이브를 사용하는 사용자 또는 사용자 그룹을 선택합니다.

10. 변경 사항을 저장합니다.

결과적으로 사용자가 이동식 드라이브에 있는 파일에 쓰기 또는 삭제 작업을 하면 Kaspersky Endpoint Security는 해당 작업에 대한 정보를 이벤트 로그에 저장하고 Kaspersky Security Center 중앙 관리 서버로 전송합니다. Kaspersky Security Center 관리 콘솔에 있는 **중앙 관리 서버** 노드의 **이벤트** 탭에서 이동식 드라이브에 저장된 파일 관련 이벤트를 확인할 수 있습니다. 로컬 Kaspersky Endpoint Security 이벤트 로그에 이벤트가 표시되려면 장치 제어 구성 요소의 알림 설정에서 **파일 동작이 수행됨** 확인란을 선택해야 합니다.

캐싱 기간 변경

장치 제어 구성 요소는 장치 연결 및 연결 해제, 장치에서 파일 읽기, 장치에 파일 쓰기 및 기타 이벤트와 같이 감시하는 장치와 관련된 이벤트를 등록합니다. 그런 다음 장치 제어는 Kaspersky Endpoint Security 설정에 따라 작업을 허용하거나 차단합니다.

장치 제어는 *캐싱 기간*이라고 하는 특정 기간 동안 이벤트에 대한 정보를 저장합니다. 이벤트에 대한 정보가 캐싱되고 이 이벤트가 반복되는 경우, Kaspersky Endpoint Security에 이를 알리거나 장치 연결 등의 관련 작업에 대한 접근 권한을 부여하기 위해 또 다른 프롬프트를 표시할 필요가 없습니다. 이렇게 하면 장치 작업이 더 편해집니다.

다음 이벤트 설정이 캐시의 레코드와 모두 일치하는 경우 이벤트를 중복 이벤트로 간주합니다:

- 장치 ID
- 접근을 시도하는 사용자 계정의 SID
- 장치 카테고리
- 장치에서 취한 조치
- 이 작업에 대한 애플리케이션 권한(허용 또는 거부)
- 조치를 취하는 데 사용되는 프로세스 경로
- 접근 중인 파일

> 캐싱 기간을 변경하기 전에 Kaspersky Endpoint Security 자기 보호를 중지합니다. 캐싱 기간 변경 후에 자기 보호를 사용합니다.

캐싱 기간을 변경하려면 다음과 같이 하십시오.

1. 컴퓨터에서 레지스트리 편집기를 엽니다.
2. 레지스트리 편집기에서 다음 섹션으로 이동합니다:
   - 64비트 운영 체제: `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]`
   - 32비트 운영 체제: `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`
3. 편집을 위해 `DeviceControlEventsCachePeriod`를 엽니다.
4. 이벤트에 대한 정보가 삭제되기 전에 장치 제어가 이 정보를 저장해야 하는 시간(분)을 정의합니다.

신뢰하는 장치와 관련된 처리 방법

*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 Endpoint Security를 사용하면 다음과 같은 방법으로 신뢰하는 목록에 장치를 추가할 수 있습니다.

- Kaspersky Security Center가 조직에 배포되어 있지 않은 경우 장치를 컴퓨터에 연결하고 애플리케이션 설정의 신뢰하는 목록에 추가할 수 있습니다. 신뢰하는 장치 목록을 조직의 모든 컴퓨터에 배포하려면 정책에서 신뢰하는 장치 목록 병합을 활성화하거나 내보내기/가져오기 절차를 사용할 수 있습니다.
- Kaspersky Security Center가 조직에 배포된 경우 연결된 모든 장치를 원격으로 탐지하고 정책에서 신뢰하는 장치 목록을 생성할 수 있습니다. 신뢰하는 장치 목록은 정책이 적용되는 모든 컴퓨터에서 사용할 수 있습니다.

Kaspersky Endpoint Security를 사용하면 신뢰하는 장치(연결 및 연결 해제)의 사용을 제어할 수 있습니다. 장치 제어 구성 요소에 대한 이벤트 기록은 알림 설정에서 켤 수 있습니다. 이벤트에는 *정보*의 심각도가 있습니다.

애플리케이션 인터페이스에서 신뢰하는 목록에 장치 추가

기본적으로 신뢰하는 목록에 장치를 추가하면 해당 장치에 대한 접근 권한이 모든 사용자('누구나'사용자 그룹)에게 부여됩니다.

애플리케이션 인터페이스에서 신뢰하는 목록에 장치를 추가하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **신뢰하는 장치** 버튼을 클릭합니다.
   그러면 신뢰하는 장치 목록이 열립니다.
4. **선택**을 클릭합니다.
   그러면 연결된 장치 목록이 열립니다. 장치 목록은 **연결된 장치 표시** 드롭다운 목록에서 선택한 값에 따라 달라집니다.
5. 장치 목록에서 신뢰하는 목록에 추가할 장치를 선택합니다.

   Kaspersky Endpoint Security는 **플로피 디스크** 유형의 장치를 신뢰하는 목록에 추가하는 것을 지원하지 않습니다.

6. **설명** 필드에서 신뢰하는 장치에 대한 관련 정보를 추가할 수 있습니다.

7. 신뢰하는 장치에 대한 접근을 허용할 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.

8. 변경 사항을 저장합니다.

Kaspersky Security Center에서 신뢰하는 목록에 장치 추가

Kaspersky Security Center는 컴퓨터에 Kaspersky Endpoint Security가 설치되어 있고 장치 제어가 활성화된 경우 장치에 대한 정보를 받습니다. Kaspersky Security Center에서 해당 장치에 대한 정보를 사용할 수 없는 경우 신뢰할 수 있는 목록에 장치를 추가할 수 없습니다.

다음 데이터에 따라 신뢰할 수 있는 목록에 장치를 추가할 수 있습니다.

- **ID로 장치 추가**. 각 장치에는 고유 ID가 있습니다(하드웨어 ID 또는 HWID). 운영 체제 도구를 사용하여 장치 속성에서 ID를 볼 수 있습니다. 장치 ID의 예: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. 여러 특정 장치를 추가하려는 경우 ID별로 장치를 추가하는 것이 편리합니다.

- **모델로 장치 추가**. 각 장치에는 공급업체 ID(VID) 및 제품 ID(PID)가 있습니다. 운영 체제 도구를 사용하여 장치 속성에서 ID를 볼 수 있습니다. VID 및 PID 입력을 위한 템플릿: `VID_1234&PID_5678`. 조직에서 특정 모델의 장치를 사용하는 경우 모델별로 장치를 추가하는 것이 편리합니다. 이런 식으로 이 모델의 모든 장치를 추가할 수 있습니다.

- **ID 마스크로 장치 추가**. 비슷한 ID를 가진 여러 장치를 사용하는 경우 마스크를 사용하여 신뢰하는 목록에 장치를 추가할 수 있습니다. `*` 문자는 모든 문자의 조합을 나타냅니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `?` 문자를 지원하지 않습니다. 예: `WDC_C*`.

- **모델 마스크로 장치 추가**. 비슷한 VID 또는 PID를 가진 여러 장치를 사용하는 경우(예: 동일한 제조업체의 장치), 마스크를 사용하여 신뢰하는 목록에 장치를 추가할 수 있습니다. `*` 문자는 모든 문자의 조합을 나타냅니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `?` 문자를 지원하지 않습니다. 예: `VID_05AC&PID_*`.

신뢰하는 장치 목록을 변경하는 것은 부모 정책의 속성에 따라 차단될 수 있습니다. 목록을 변경하려면 웹 콘솔의 신뢰 구역('자물쇠'가 잠금 해제되어야 함) 설정 변경을 허용해야 합니다.

신뢰 구역은 관리 콘솔(MMC)과 웹 콘솔에서 다르게 그룹화됩니다. 마찬가지로, 신뢰 구역 파라미터의 변경을 방지하는 방법도 다릅니다('자물쇠'가 다름). 웹 콘솔만 사용하여 애플리케이션을 관리하는 것이 좋습니다. 서로 다른 콘솔에서 신뢰 구역을 구성하는 경우 관리 플러그인이 '자물쇠'를 기본 상태로 재설정할 수 있습니다.

신뢰하는 장치 목록에 장치를 추가하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **보안 제어 → 장치 제어**를 선택합니다.

4. 창 오른쪽에서 **신뢰하는 장치** 탭을 선택합니다.

5. 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.

6. **추가** 버튼을 클릭하고 신뢰하는 목록에 장치를 추가하는 방법을 선택합니다.

7. 장치를 필터링하려면 **장치 유형** 드롭다운 목록에서 장치 유형을 선택합니다(예: **이동식 드라이브**).

   Kaspersky Endpoint Security는 **플로피 디스크** 유형의 장치를 신뢰하는 목록에 추가하는 것을 지원하지 않습니다.

8. **이름/모델** 필드에, 선택한 추가 방법에 따라 장치 ID, 모델(VID 및 PID) 또는 마스크를 입력합니다.

   모델 마스크(VID 및 PID)에 의한 장치 추가는 다음과 같이 작동합니다. 모델과 일치하지 않는 모델 마스크를 입력하는 경우 Kaspersky Endpoint Security는 장치 ID(HWID)가 마스크와 일치하는지 확인합니다. Kaspersky Endpoint Security는 제조업체 및 장치 유형을 결정하는 장치 ID의 일부만을 확인합니다 (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). 모델 마스크가 장치 ID의 해당 부분과 일치하는 경우 마스크와 일치하는 장치가 컴퓨터의 신뢰하는 장치 목록에 추가됩니다. 반면, **새로 고침** 버튼을 클릭할 때 Kaspersky Security Center의 장치 목록은 여전히 비어 있습니다. 장치 목록을 올바르게 표시하기 위해 장치 ID 마스크로 장치를 추가할 수 있습니다.

9. 장치를 필터링하려면 **컴퓨터** 필드에 장치가 연결된 컴퓨터 이름 또는 컴퓨터 이름에 대한 마스크를 입력합니다.

   `*` 문자는 모든 문자의 조합을 나타냅니다. `?` 문자는 임의의 문자 하나를 나타냅니다.

10. **새로 고침** 버튼을 누릅니다.

    이 표에는 정의된 필터링 기준을 만족하는 장치 목록이 표시됩니다.

11. 신뢰하는 목록에 추가할 장치의 이름 옆에 있는 확인란을 선택합니다.

12. **설명** 필드에 신뢰하는 목록에 장치를 추가한 이유에 대한 설명을 입력합니다.

13. **다음 사용자 또는 사용자 그룹에 대해 허용** 필드 오른쪽의 **선택** 버튼을 클릭합니다.

14. 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.

    기본적으로 Everyone 그룹에는 신뢰하는 장치에 대한 접근이 허용됩니다.

15. 변경 사항을 저장합니다.

    장치가 연결되면 Kaspersky Endpoint Security는 승인된 사용자의 신뢰하는 장치 목록을 확인합니다. 장치를 신뢰하는 경우 Kaspersky Endpoint Security는 장치 유형 또는 연결 버스에 대한 접근이 거부된 경우에도 모든 권한과 함께 장치에 대한 접근을 허용합니다. 장치를 신뢰할 수 없고 접근이 거부된 경우 잠겨있는 장치에 대한 접근을 요청할 수 있습니다.

신뢰하는 장치 목록 내보내기 및 가져오기

신뢰하는 장치 목록을 조직의 모든 컴퓨터에 배포하려면 내보내기/가져오기 절차를 사용할 수 있습니다.

예를 들어 신뢰하는 이동식 드라이브 목록을 배포해야 하는 경우 다음을 수행해야 합니다.

1. 이동식 드라이브를 컴퓨터에 순차적으로 연결합니다.
2. Kaspersky Endpoint Security 설정에서 이동식 드라이브를 신뢰하는 목록에 추가합니다. 필요시 사용자 접근 권한을 구성합니다. 예를 들어 관리자만 이동식 드라이브에 접근하도록 합니다.
3. Kaspersky Endpoint Security 설정에서 신뢰하는 장치 목록을 내보냅니다(아래 지침 참조).
4. 신뢰하는 장치 목록 파일을 조직의 다른 컴퓨터에 배포합니다. 예를 들어 파일을 공유 폴더에 넣습니다.
5. 조직 내 다른 컴퓨터의 Kaspersky Endpoint Security 설정에서 신뢰하는 장치 목록을 가져옵니다(아래 지침 참조).

신뢰하는 장치 목록을 가져오거나 내보내려면 다음을 수행합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **신뢰하는 장치** 버튼을 클릭합니다.
   그러면 신뢰하는 장치 목록이 열립니다.
4. 신뢰하는 장치 목록을 내보내려면 다음을 수행합니다:
   a. 내보낼 신뢰하는 장치를 선택합니다.
   b. **내보내기**를 클릭합니다.
   c. 창이 열리면 신뢰하는 장치 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   d. 파일을 저장합니다.
      Kaspersky Endpoint Security는 신뢰하는 장치의 전체 목록을 XML 파일로 내보냅니다.
5. 신뢰하는 장치 목록을 가져오려면 다음과 같이 진행합니다:
   a. **가져오기** 드롭 다운 목록에서 **가져와서 기존 항목에 추가** 또는 **가져와서 기존 항목 교체** 등 필요한 작업을 선택합니다.
   b. 창이 열리면 신뢰하는 장치 목록을 가져올 XML 파일을 선택합니다.
   c. 파일을 엽니다.
6. 변경 사항을 저장합니다.

장치가 연결되면 Kaspersky Endpoint Security는 승인된 사용자의 신뢰하는 장치 목록을 확인합니다. 장치를 신뢰하는 경우 Kaspersky Endpoint Security는 장치 유형 또는 연결 버스에 대한 접근이 거부된 경우에도 모든 권한과 함께 장치에 대한 접근을 허용합니다.

차단된 장치에 대한 접근 권한 획득

장치 제어를 구성할 때 업무에 필요한 장치에 대한 접근을 실수로 차단할 수 있습니다.

Kaspersky Security Center가 조직에 배포되지 않은 경우에는 Kaspersky Endpoint Security의 설정에서 장치에 대한 접근을 허용할 수 있습니다. 예를 들어 해당 장치를 신뢰하는 목록에 추가하거나 일시적으로 장치 제어를 중지할 수 있습니다.

Kaspersky Security Center가 조직에 배포되어 있고 컴퓨터에 정책이 적용된 경우에는 관리 콘솔에서 장치에 대한 접근을 허용할 수 있습니다.

접근 권한 부여를 위한 온라인 모드

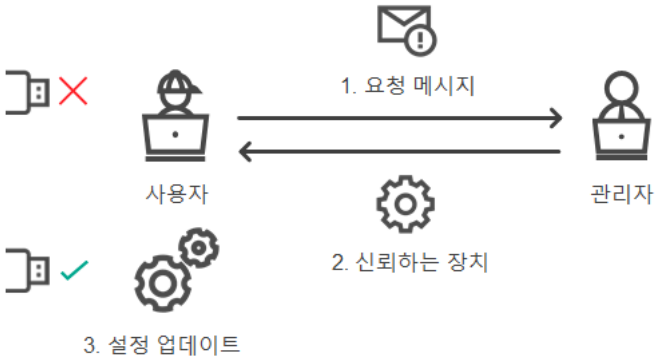
Kaspersky Security Center가 조직에 배포되어 있고 컴퓨터에 정책이 적용된 경우에 한해 온라인 모드에서 차단된 장치에 대한 접근을 허용할 수 있습니다. 컴퓨터에 중앙 관리 서버와 연결하는 기능이 있어야 합니다.

온라인 모드에서 접근 권한을 부여하는 작업은 다음 단계로 구성됩니다:

1. 사용자가 관리자에게 접근 요청이 포함된 메시지를 전송합니다.
2. 관리자가 Kaspersky Security Center 콘솔에서 요청 메시지를 수신합니다.

   Kaspersky Security Center 콘솔에는 사용자의 메시지들을 쉽게 추적할 수 있도록 하기 위해 *사용자 개선 요청 사항*이라는 사전 설정 이벤트 선택 항목이 있습니다.
3. 관리자가 해당 장치를 신뢰하는 목록에 추가합니다.

   관리 그룹에 대한 정책에 또는 개인 컴퓨터의 로컬 애플리케이션 설정에 신뢰하는 장치를 추가할 수 있습니다.
4. 관리자가 사용자 컴퓨터의 Kaspersky Endpoint Security의 설정을 업데이트합니다.



온라인 모드에서 장치에 대한 접근 권한을 부여하는 절차 설명

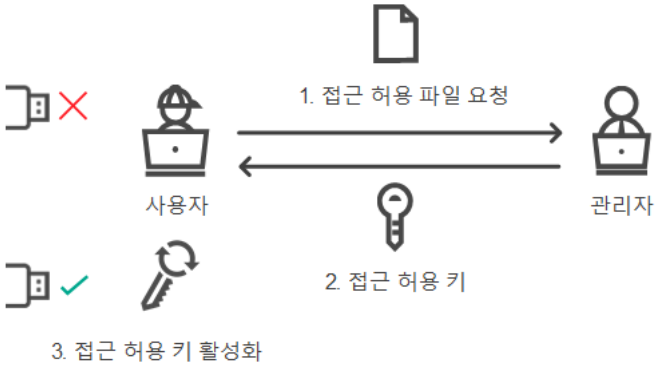
접근 권한 부여를 위한 오프라인 모드

Kaspersky Security Center가 조직에 배포되어 있고 컴퓨터에 정책이 적용된 경우에 한해 오프라인 모드에서 차단된 장치에 대한 접근을 허용할 수 있습니다. 정책 설정의 **장치 제어** 섹션에서 **임시 접근 요청 허용** 확인란을 반드시 선택해야 합니다.

차단된 장치에 임시 접근을 허용해야 하는데 해당 장치를 신뢰하는 목록에 추가할 수 없는 경우에는 오프라인 모드에서 해당 장치에 대한 접근 권한을 부여할 수 있습니다. 이 방법을 사용하면 컴퓨터가 네트워크에 접근할 수 없거나 컴퓨터가 회사 네트워크 외부에 있는 경우에도 차단된 장치에 대한 접근 권한을 부여할 수 있습니다.

오프라인 모드에서 접근 권한을 부여하는 작업은 다음 단계로 구성됩니다:

1. 사용자가 접근 허용 요청 파일을 생성하여 관리자에게 전송합니다.
2. 관리자가 접근 허용 요청 파일에서 접근 허용 키를 생성하여 사용자에게 전송합니다.
3. 사용자가 접근 허용 키를 활성화합니다.



오프라인 모드에서 장치에 대한 접근 권한을 부여하는 절차 설명

접근 권한 부여를 위한 온라인 모드

Kaspersky Security Center가 조직에 배포되어 있고 컴퓨터에 정책이 적용된 경우에 한해 온라인 모드에서 차단된 장치에 대한 접근을 허용할 수 있습니다. 컴퓨터에 중앙 관리 서버와 연결하는 기능이 있어야 합니다.

사용자가 다음과 같이 차단된 장치에 대한 접근 권한을 요청합니다:

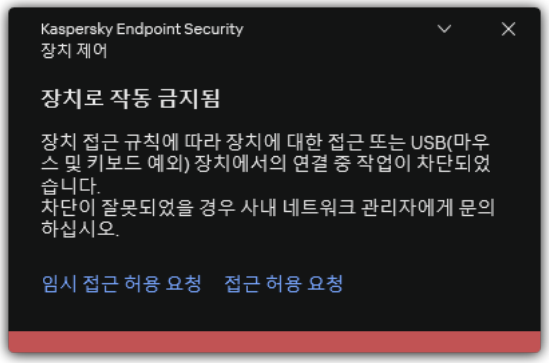
1. 장치를 컴퓨터에 연결합니다.

   Kaspersky Endpoint Security에서 해당 장치에 대한 접근이 차단되었다는 알림을 표시합니다(아래 그림 참조).

2. **접근 허용 요청** 링크를 클릭합니다.

   관리자용 메시지 창이 열립니다. 이 메시지에는 차단된 장치에 대한 정보가 포함됩니다.

3. **전송**을 클릭합니다.



장치 제어 알림

이어서 Kaspersky Security Center 콘솔 관리자가 *관리자에게 장치 접근 차단 메시지 보내기* 이벤트를 수신합니다. 이벤트에는 사용자 이름, 컴퓨터 이름, 사용자가 접근하려는 장치에 대한 정보와 다른 정보가 포함됩니다. 관리자가 이러한 이벤트 알림이 표시되는 방식을 구성할 수 있습니다(예: 이메일 알림 선택). Kaspersky Security Center 콘솔에는 사용자의 메시지들을 쉽게 추적할 수 있도록 하기 위해 *사용자 개선 요청 사항*이라는 사전 설정 이벤트 선택 항목이 있습니다.

접근을 허용하려면 신뢰하는 목록에 장치 추가를 해야 합니다. 컴퓨터에서 Kaspersky Endpoint Security 설정을 업데이트하면 사용자는 장치에 접근할 수 있습니다.

접근 권한 부여를 위한 오프라인 모드

Kaspersky Security Center가 조직에 배포되어 있고 컴퓨터에 정책이 적용된 경우에 한해 오프라인 모드에서 차단된 장치에 대한 접근을 허용할 수 있습니다. 정책 설정의 **장치 제어** 섹션에서 **임시 접근 요청 허용** 확인란을 반드시 선택해야 합니다.

사용자가 다음과 같이 차단된 장치에 대한 접근 권한을 요청합니다:

1. 장치를 컴퓨터에 연결합니다.

   Kaspersky Endpoint Security에서 해당 장치에 대한 접근이 차단되었다는 알림을 표시합니다(아래 그림 참조).

2. **임시 접근 허용 요청** 링크를 클릭합니다.

   연결된 장치 목록이 포함된 창이 열립니다.

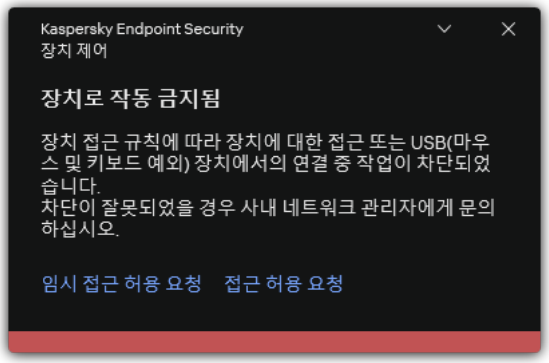
3. 연결된 장치 목록에서 접근 권한을 얻을 장치를 선택합니다.

4. **접근 허용 요청 파일 생성**을 클릭합니다.

5. **접근 지속 시간** 필드에서 장치에 접근하고자 하는 시간의 간격을 지정합니다.

6. 파일을 컴퓨터 메모리에 저장합니다.

그러면 확장자가 *.akey인 접근 허용 요청 파일이 컴퓨터 메모리에 다운로드됩니다. 이용 가능한 방법을 활용하여 장치 접근 허용 요청 파일을 회사 LAN 관리자에게 전송합니다.



장치 제어 알림

관리자가 관리 콘솔(MMC)에서 차단된 장치의 접근 허용 키를 만드는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.

3. 작업 공간에서 **기기** 탭을 선택합니다.

4. 클라이언트 컴퓨터 목록에서 차단된 장치에 대한 임시 접근을 허용할 사용자의 컴퓨터를 선택합니다.

5. 컴퓨터의 마우스 오른쪽 메뉴에서 **오프라인 모드에서의 접근 권한 부여** 항목을 선택합니다.

6. 열린 창에서 **장치 제어** 탭을 선택합니다.

7. **찾아보기** 버튼을 클릭하고 사용자로부터 받은 접근 허용 요청 파일을 다운로드합니다.
   사용자가 접근 권한을 요청한 차단된 장치에 대한 정보를 확인할 수 있습니다.

8. 필요할 경우 **접근 지속 시간** 설정 값을 변경합니다.
   기본적으로 **접근 지속 시간** 설정은 사용자가 접근 허용 요청 파일을 생성할 때 지정한 값을 사용합니다.

9. **활성화 유효 시간** 설정의 값을 지정합니다.
   이 설정은 제공된 접근 허용 키를 사용해 잠겨 있는 장치에 대한 사용자의 접근 허용 시간을 정의합니다.

10. 접근 허용 키 파일을 컴퓨터 메모리에 저장합니다.

관리자가 웹 콘솔 및 Cloud Console에서 차단된 장치의 접근 허용 키를 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.

2. 클라이언트 컴퓨터 목록에서 차단된 장치에 대한 임시 접근을 허용할 사용자의 컴퓨터를 선택합니다.

3. 컴퓨터 목록 위의 줄임표 버튼(...)을 클릭한 다음 **오프라인 모드인 기기에 접근 권한 부여** 버튼을 클릭합니다.

4. 창이 열리면 **장치 제어** 섹션을 선택합니다.

5. **찾아보기** 버튼을 클릭하고 사용자로부터 받은 접근 허용 요청 파일을 다운로드합니다.
   사용자가 접근 권한을 요청한 차단된 장치에 대한 정보를 확인할 수 있습니다.

6. 필요할 경우 **접근 지속 시간(시)** 설정 값을 변경합니다.
   기본적으로 **접근 지속 시간(시)** 설정은 사용자가 접근 허용 요청 파일을 생성할 때 지정한 값을 사용합니다.

7. 장치에서 접근 허용 키를 활성화할 수 있는 기간을 지정합니다.
   이 설정은 제공된 접근 허용 키를 사용해 잠겨 있는 장치에 대한 사용자의 접근 허용 시간을 정의합니다.

8. 접근 허용 키 파일을 컴퓨터 메모리에 저장합니다.

그러면 차단된 장치의 접근 허용 키가 컴퓨터 메모리에 다운로드됩니다. 접근 허용 키 파일의 확장자는 *.acode입니다. 이용 가능한 방법을 활용하여 차단된 장치의 접근 허용 키 파일을 사용자에게 전송합니다.

사용자가 다음과 같이 접근 허용 키를 활성화합니다:

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **보안 제어 → 장치 제어**를 선택합니다.

3. **접근 요청** 블록에서 **장치 접근 허용 요청** 버튼을 클릭합니다.

4. 창이 열리면 **접근 허용 키 활성화** 버튼을 클릭합니다.

5. 창이 열리면 기업 LAN 관리자로부터 받은 장치 접근 허용 키가 포함된 파일을 선택합니다.

   접근 제공 정보가 포함된 창이 열립니다.

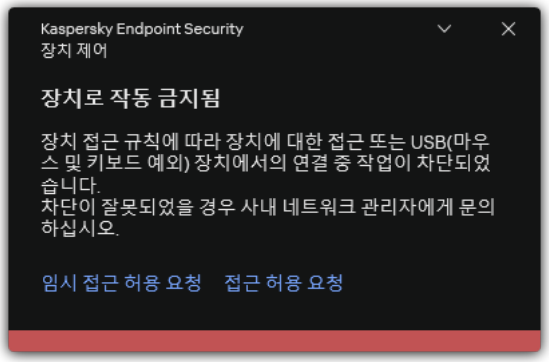
6. **확인**을 누릅니다.

그러면 사용자는 관리자가 설정한 기간 동안 장치에 대한 접근 권한을 받게 됩니다. 사용자는 장치 접근에 대한 모든 권한(읽기 및 쓰기)를 획득합니다. 이 키가 만료되면 장치에 대한 접근이 차단됩니다. 장치에 대한 영구 접근 권한을 받으려면 해당 장치를 신뢰하는 목록에 추가하십시오.

장치 제어 메시지 템플릿 편집

사용자가 차단된 장치에 접근하려고 하면 Kaspersky Endpoint Security에서는 장치에 대한 접근이 차단되었거나 해당 장치 컨텐츠의 작업이 금지되었다는 메시지가 표시됩니다. Kaspersky 전문가는 사용자에게 장치에 대한 액세스가 차단된 이유를 설명하는 메시지 템플릿을 제공합니다(아래 그림 참조).

메시지 템플릿(예: %USER_NAME%)을 관리하기 위해 특수 변수가 제공됩니다. 변수를 사용하면 다른 컴퓨터에서 단일 메시지 템플릿을 사용할 수 있습니다. 메시지 생성 시 Kaspersky Endpoint Security는 운영 체제 설정에서 변수 값을 검색하여 특정 컴퓨터, 사용자 및 이벤트와 일치하는 메시지에 삽입합니다.



장치 제어 알림

장치에 대한 접근이 잘못 차단되었거나 장치 컨텐츠의 작업이 실수로 금지되었다고 생각하면 차단 처리에 대해 표시된 메시지의 링크를 눌러 회사 로컬 네트워크 관리자에게 메시지를 보낼 수 있습니다. 이렇게 하려면, 사용자는 **접근 허용 요청** 또는 **임시 접근 허용 요청** 버튼을 누르고 관리자에게 상황을 설명하는 메시지를 보내야 합니다. 또한 관리자에게 보낼 메시지 템플릿을 준비하여 장치에 대한 접근을 허용할지 또는 차단할지 결정하는 데 도움이 되는 데이터를 추가할 수 있습니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 장치 접근 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다.

관리 콘솔(MMC)에서 장치 제어 메시지 템플릿을 변경하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **보안 제어** → **장치 제어**를 선택합니다.

4. **메시지 템플릿 설정** 블록에서 **템플릿** 버튼을 클릭합니다.

5. 그러면 창이 열립니다. 이 창에서 애플리케이션 제어 템플릿을 구성합니다.

   - **차단 관련 메시지**. 사용자가 차단된 장치에 접근하려고 할 때 표시되는 메시지의 템플릿입니다. 이 메시지는 사용자가 해당 사용자에 대해 차단된 장치 컨텐츠에 대한 작업을 수행하려고 할 때도 나타납니다.

   - **관리자에게 메시지 보내기**. 사용자가 장치 접근이 잘못 차단되었거나 장치 컨텐츠 작업이 잘못 금지되었다고 생각하는 경우 LAN 관리자에게 보내는 메시지 템플릿입니다.

   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

   기본 템플릿 텍스트를 복원할 수도 있습니다.

6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 장치 제어 메시지 템플릿을 변경하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어** → **장치 제어**로 이동합니다.

5. **메시지 템플릿** 블록에서 애플리케이션 제어 메시지에 대한 템플릿을 구성합니다.

   - **사용자에게 보내는 메시지**. 사용자가 차단된 장치에 접근하려고 할 때 표시되는 메시지의 템플릿입니다. 이 메시지는 사용자가 해당 사용자에 대해 차단된 장치 컨텐츠에 대한 작업을 수행하려고 할 때도 나타납니다.

   - **관리자에게 메시지 보내기**. 사용자가 장치 접근이 잘못 차단되었거나 장치 컨텐츠 작업이 잘못 금지되었다고 생각하는 경우 LAN 관리자에게 보내는 메시지 템플릿입니다.

   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수 추가**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

   기본 템플릿 텍스트를 복원할 수도 있습니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 장치 제어 메시지 템플릿을 변경하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **보안 제어** → **애플리케이션 제어**를 선택합니다.

3. **메시지 템플릿** 블록에서 애플리케이션 제어 메시지에 대한 템플릿을 구성합니다.

   - **차단 관련 메시지**. 사용자가 차단된 장치에 접근하려고 할 때 표시되는 메시지의 템플릿입니다. 이 메시지는 사용자가 해당 사용자에 대해 차단된 장치 컨텐츠에 대한 작업을 수행하려고 할 때도 나타납니다.

   - **관리자에게 메시지 보내기**. 사용자가 장치 접근이 잘못 차단되었거나 장치 컨텐츠 작업이 잘못 금지되었다고 생각하는 경우 LAN 관리자에게 보내는 메시지 템플릿입니다.

   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수 추가**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

기본 템플릿 텍스트를 복원할 수도 있습니다.

4. 변경 사항을 저장합니다.

안티 브리징

안티 브리징은 네트워크 브리지가 생성되는 것을 막아 컴퓨터에서 여러 개의 네트워크에 동시에 연결되지 않도록 합니다. 따라서 보호되지 않는 무단 네트워크를 통한 공격으로부터 회사 네트워크를 보호할 수 있습니다.

안티 브리징은 *연결 규칙*을 사용하여 네트워크 연결을 제어합니다.

미리 정의된 다음 유형의 장치에 대한 연결 규칙이 만들어집니다:

- 네트워크 어댑터
- Wi-Fi 어댑터
- 모뎀

연결 규칙을 사용할 경우 Kaspersky Endpoint Security는 다음을 수행합니다:

- 규칙에 지정된 장치 유형이 두 연결에 모두 사용되면 새 연결을 시작할 때 활성 연결을 차단합니다.
- 우선 순위가 낮은 규칙이 사용된 장치 유형을 사용하여 시작되는 연결을 차단합니다.

안티 브리징 활성화

기본적으로 안티 브리징은 중지되어 있습니다.

안티 브리징을 사용하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **안티 브리징** 버튼을 클릭합니다.
4. **안티 브리징 사용** 토글로 이 기능을 사용하거나 중지합니다.
5. 변경 사항을 저장합니다.

이미 안티 브리징이 사용 중이면 Kaspersky Endpoint Security는 연결 규칙에 따라 이미 확립된 연결을 차단합니다.

연결 규칙 상태 변경

연결 제어 규칙 상태를 변경하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **안티 브리징** 버튼을 클릭합니다.
4. **장치 규칙** 블록에서 상태를 변경할 규칙을 선택합니다.
5. **제어** 열의 토글로 규칙을 사용하거나 중지합니다.
6. 변경 사항을 저장합니다.

연결 규칙 우선 순위 변경

연결 제어 우선 순위를 변경하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **장치 제어**를 선택합니다.
3. **접근 설정** 블록에서 **안티 브리징** 버튼을 클릭합니다.
4. **장치 규칙** 블록에서 우선순위를 변경할 규칙을 선택합니다.
5. **위로/아래로** 버튼을 사용하여 연결 규칙의 우선순위를 설정합니다.

   규칙 표에서 위쪽에 있을수록 규칙의 우선 순위도 높습니다. 안티 브리징은 우선 순위가 가장 높은 규칙이 적용된 장치 유형을 사용하여 이루어진 하나의 연결을 제외하고 모든 연결을 차단합니다.
6. 변경 사항을 저장합니다.

적응형 이상 행위 제어

이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

적응형 이상 행위 제어 구성 요소는 회사 네트워크의 컴퓨터에서 일반적이지 않은 활동을 감시하고 차단합니다. 적응형 이상 행위 제어는 일련의 규칙을 사용하여 비정상적인 동작을 추적합니다(예, *오피스 애플리케이션에서 Microsoft PowerShell 시작* 규칙). 규칙은 Kaspersky 전문가가 일반적인 악의적인 활동 시나리오를 기반으로 작성합니다. 적응형 이상 행위 제어에서 각 규칙을 처리하는 방법을 구성할 수 있습니다. 또한 예를 들어 특정 워크플로 작업을 자동화하는 PowerShell 스크립트를 실행을 허용할 수 있습니다. Kaspersky Endpoint Security는 규칙 세트와 애플리케이션 데이터베이스를 업데이트합니다. 규칙 세트에 대한 업데이트를 직접 확인해야 합니다.

적응형 이상 행위 제어 설정

적응형 이상 행위 제어의 구성은 다음 단계로 구성됩니다:

1. 적응형 이상 행위 제어 학습.

   적응형 이상 행위 제어를 활성화하면 해당 규칙은 *학습 모드*로 작동합니다. 학습하는 동안 적응형 이상 행위 제어는 규칙 트리거링을 모니터링하고 트리거링 이벤트를 Kaspersky Security Center로 전송합니다. 각 규칙은 개별적으로 학습 모드 지속 시간을 갖습니다. 학습 모드 지속 시간은 Kaspersky 전문가가 설정합니다. 일반적으로 학습 모드는 2주 동안 진행됩니다.

   학습 중에 규칙이 전혀 트리거되지 않은 경우 적응형 이상 행위 제어는 이후 이 규칙과 관련된 작업을 일반적이지 않은 것으로 간주합니다. Kaspersky Endpoint Security는 해당 규칙과 관련된 모든 작업을 차단합니다.

   학습 중에 규칙이 트리거되면 Kaspersky Endpoint Security는 규칙 트리거링 리포트 및 **스마트 학습 상태에서 트리거된 규칙** 저장소에 이벤트를 기록합니다.

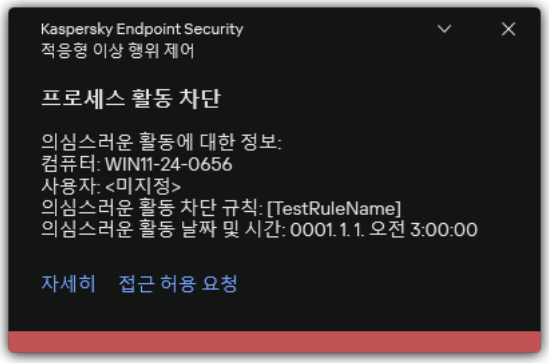
2. 규칙 트리거링 리포트 분석.

   관리자는 규칙 트리거링 리포트 또는 **스마트 학습 상태에서 트리거된 규칙** 저장소의 내용을 분석합니다. 그런 다음 관리자는 규칙이 트리거될 때 적응형 이상 행위 제어의 동작을 선택할 수 있습니다: 차단 또는 허용. 또한 관리자는 규칙의 작동 방식을 계속 모니터링하고 학습 모드의 기간을 연장할 수 있습니다. 관리자가 아무런 조치를 취하지 않으면 애플리케이션도 학습 모드에서 계속 작동합니다. 학습 모드 기간이 재시작되었습니다.

적응형 이상 행위 제어는 다음 채널을 통해 실시간으로 구성됩니다.

- 적응형 이상 행위 제어는 학습 모드에서 트리거되지 않은 규칙과 관련된 작업을 자동으로 차단하기 시작합니다.
- Kaspersky Endpoint Security는 새 규칙을 추가하거나 오래된 규칙을 제거합니다.
- 관리자는 규칙 트리거링 리포트와 **스마트 학습 상태에서 트리거된 규칙** 저장소의 내용을 검토한 후 적응형 이상 행위 제어의 작업을 구성합니다. 트리거하는 규칙과 **스마트 학습 상태에서 트리거된 규칙** 저장소의 내용에 대한 리포트를 확인하는 것이 좋습니다.

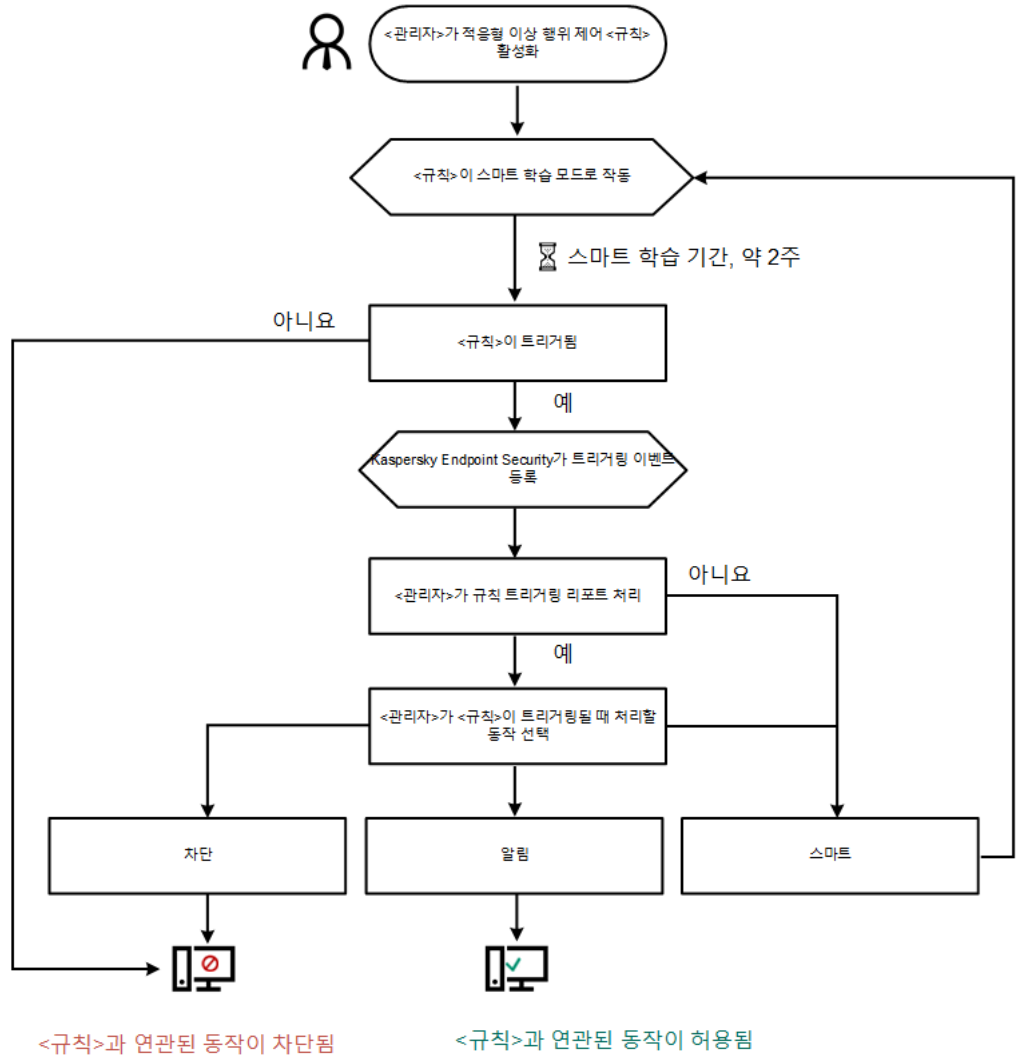
악성 애플리케이션이 동작을 수행하려고 하면 Kaspersky Endpoint Security가 해당 동작을 차단하고 알림을 표시합니다(아래 그림 참조).



적응형 이상 행위 제어 알림

적응형 이상 행위 제어 운영 알고리즘

Kaspersky Endpoint Security는 다음 알고리즘을 기반으로 한 규칙과 연관된 동작을 허용할지 또는 차단할지 결정합니다(아래 그림 참조).



적응형 이상 행위 제어 운영 알고리즘

적응형 이상 행위 제어 학습

적응형 이상 행위 제어에는 일련의 규칙(동작 패턴)이 포함되어 있습니다. 적응형 이상 행위 제어를 활성화하면 해당 규칙은 *학습 모드*로 작동합니다. 학습하는 동안 적응형 이상 행위 제어는 규칙 트리거링을 모니터링하고 트리거링 이벤트를 Kaspersky Security Center로 전송합니다. 적응형 이상 행위 제어는 컴퓨터에서 애플리케이션 활동을 차단하지 않으며 관리자에게 알리기만 합니다. 적응형 이상 행위 제어 규칙이 트리거되면 적용되는 처리 방법을 수동으로 선택할 수도 있습니다.

관리 콘솔(MMC)에서 적응형 이상 행위 제어 규칙 목록을 확인하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

4. 정책 창에서 **보안 제어 → 적응형 이상 행위 제어**를 선택합니다.

5. **적응형 이상 행위 제어** 확인란을 선택합니다.

6. **적응형 이상 행위 제어 규칙 설정** 아래에서 규칙 목록을 확인합니다.
   기본적으로 모든 규칙은 **스마트** 모드에서 작동합니다.

7. 필요한 경우 적응형 이상 행위 제어 규칙의 업데이트를 확인합니다.

8. 필요한 경우 적응형 이상 행위 제어 규칙이 트리거될 때 적용되는 처리 방법을 선택합니다.

   - **차단**. 이 작업을 선택하면 적응형 이상 행위 제어 규칙이 트리거될 때 Kaspersky Endpoint Security가 규칙이 적용되는 활동을 차단하고 활동 관련 정보가 포함된 항목을 기록합니다.

   - **알림**. 이 작업을 선택하면 적응형 이상 행위 제어 규칙이 트리거될 때 Kaspersky Endpoint Security가 규칙이 적용되는 활동을 허용하고 활동 관련 정보가 포함된 항목을 기록합니다.

9. 필요한 경우 사용하지 않을 규칙을 비활성화합니다.

10. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 적응형 이상 행위 제어 규칙을 확인하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 탭을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어 → 적응형 이상 행위 제어**로 이동합니다.

5. **적응형 이상 행위 제어** 토글을 켭니다.

6. **규칙** 아래에서 규칙 목록을 확인합니다.
   기본적으로 모든 규칙은 **스마트** 모드에서 작동합니다.

7. 필요한 경우 적응형 이상 행위 제어 규칙의 업데이트를 확인합니다.

8. 필요한 경우 적응형 이상 행위 제어 규칙이 트리거될 때 적용되는 처리 방법을 선택합니다.

   - **차단**. 이 작업을 선택하면 적응형 이상 행위 제어 규칙이 트리거될 때 Kaspersky Endpoint Security가 규칙이 적용되는 활동을 차단하고 활동 관련 정보가 포함된 항목을 기록합니다.

   - **알림**. 이 작업을 선택하면 적응형 이상 행위 제어 규칙이 트리거될 때 Kaspersky Endpoint Security가 규칙이 적용되는 활동을 허용하고 활동 관련 정보가 포함된 항목을 기록합니다.

9. 필요한 경우 사용하지 않을 규칙을 비활성화합니다.

10. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 적응형 이상 행위 제어 규칙 목록을 확인하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **적응형 이상 행위 제어**를 선택합니다.
3. **적응형 이상 행위 제어** 토글을 켭니다.
4. **규칙** 블록에서 **규칙 편집** 링크를 클릭합니다.
   적응형 이상 행위 제어 규칙 목록이 열립니다. 기본적으로 모든 규칙은 **스마트** 모드에서 작동합니다.
5. 필요한 경우 적응형 이상 행위 제어 규칙의 업데이트를 확인합니다.
6. 필요한 경우 적응형 이상 행위 제어 규칙이 트리거될 때 적용되는 처리 방법을 선택합니다.
   - **차단**. 이 작업을 선택하면 적응형 이상 행위 제어 규칙이 트리거될 때 Kaspersky Endpoint Security가 규칙이 적용되는 활동을 차단하고 활동 관련 정보가 포함된 항목을 기록합니다.
   - **알림**. 이 작업을 선택하면 적응형 이상 행위 제어 규칙이 트리거될 때 Kaspersky Endpoint Security가 규칙이 적용되는 활동을 허용하고 활동 관련 정보가 포함된 항목을 기록합니다.
7. 필요한 경우 사용하지 않을 규칙을 비활성화합니다.
8. 변경 사항을 저장합니다.

각 규칙은 개별적으로 학습 모드 지속 시간을 갖습니다. 학습 모드 지속 시간은 Kaspersky 전문가가 설정합니다. 일반적으로 학습 모드는 2주 동안 진행됩니다.

학습 중에 규칙이 트리거되지 않으면 적응형 이상 행위 제어는 이러한 동작을 이례적으로 간주하고 규칙 상태를 **스마트 차단**으로 변경합니다. 그러면 애플리케이션은 이 규칙과 일치하는 모든 활동을 차단합니다.

학습 중에 규칙이 트리거되면 애플리케이션이 이 규칙과 일치하는 탐지된 활동에 적용할 처리 방법을 직접 구성해야 합니다. 규칙이 트리거될 때 적용되는 처리 방법을 선택하지 않으면 적응형 이상 행위 제어가 계속 학습 모드에서 작동합니다.

적응형 이상 행위 제어 규칙 작동 및 중지

적응형 이상 행위 제어 규칙을 작동하거나 중지하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **적응형 이상 행위 제어**를 선택합니다.
3. **규칙** 블록에서 **규칙 편집** 버튼을 클릭합니다.
   적응형 이상 행위 제어 규칙 목록이 열립니다.
4. 테이블에서 규칙 세트(*오피스 애플리케이션 활동* 등)를 선택하고 세트를 펼칩니다.
5. 규칙을 선택합니다(예: *오피스 애플리케이션에서 Microsoft PowerShell 시작*).
6. **상태** 열의 토글 스위치로 적응형 이상 행위 제어 규칙을 활성화 또는 비활성화합니다.
7. 변경 사항을 저장합니다.

적응형 이상 행위 제어 규칙 작동 시에 수행되는 처리 수정

적응형 이상 행위 제어 규칙 작동 시에 수행되는 처리를 편집하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **적응형 이상 행위 제어**를 선택합니다.
3. **규칙** 블록에서 **규칙 편집** 버튼을 클릭합니다.
   적응형 이상 행위 제어 규칙 목록이 열립니다.
4. 표에서 규칙을 선택합니다.
5. **편집**을 클릭합니다.
   적응형 이상 행위 제어 규칙 속성 창이 열립니다.
6. **처리** 섹션에서 다음 옵션 중 하나를 선택합니다:
   - **스마트**. 이 옵션을 선택하면 Kaspersky 전문가가 정의한 기간에 적응형 이상 행위 제어 규칙이 스마트 학습 상태로 작동합니다. 이 모드에서는 적응형 이상 행위 제어 규칙이 트리거될 때 Kaspersky Endpoint Security가 규칙이 적용되는 활동을 허용하며 Kaspersky Security Center 중앙 관리 서버의 **스마트 학습 상태에서 트리거된 규칙** 스토리지에 항목을 기록합니다. 스마트 학습 상태로 작동하도록 설정된 기간이 끝나면 Kaspersky Endpoint Security는 적응형 이상 행위 제어 규칙이 적용되는 활동을 차단하며 활동 관련 정보가 포함된 항목을 기록합니다.
   - **차단**. 이 작업을 선택하면 적응형 이상 행위 제어 규칙이 트리거될 때 Kaspersky Endpoint Security가 규칙이 적용되는 활동을 차단하고 활동 관련 정보가 포함된 항목을 기록합니다.
   - **알림**. 이 작업을 선택하면 적응형 이상 행위 제어 규칙이 트리거될 때 Kaspersky Endpoint Security가 규칙이 적용되는 활동을 허용하고 활동 관련 정보가 포함된 항목을 기록합니다.
7. 변경 사항을 저장합니다.

적응형 이상 행위 제어 규칙에 대한 예외 규칙 생성

적응형 이상 행위 제어 규칙에 대한 예외는 1,000개보다 많이 생성할 수 없습니다. 예외는 200개보다 많이 생성하지 않는 것이 좋습니다. 사용되는 예외 수를 줄이려면 예외 설정에서 마스크를 사용하는 것이 좋습니다.

적응형 이상 행위 제어 규칙에 대한 예외에는 소스 및 대상 개체에 대한 설명이 포함됩니다. 소스 *개체*는 작업을 수행하는 개체입니다. *대상 개체*는 작업이 수행되는 개체입니다. 예를 들어 `file.xlsx`라는 파일을 열었습니다. 따라서 DLL 확장자를 가진 라이브러리 파일이 컴퓨터 메모리에 로드됩니다. 이 라이브러리는 브라우저에서 사용됩니다(`browser.exe`라는 실행 파일). 이 예에서 `file.xlsx`는 소스 개체이며 Excel은 소스 프로세스, `browser.exe`는 대상 개체이고 Browser는 대상 프로세스입니다.

적응형 이상 행위 제어 규칙의 예외 규칙을 생성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어 → 적응형 이상 행위 제어**를 선택합니다.
3. **규칙** 블록에서 **규칙 편집** 버튼을 클릭합니다.
   적응형 이상 행위 제어 규칙 목록이 열립니다.
4. 표에서 규칙을 선택합니다.
5. **편집**을 클릭합니다.
   적응형 이상 행위 제어 규칙 속성 창이 열립니다.
6. **예외 규칙** 창에서 **추가** 버튼을 누릅니다.
   예외 규칙 속성 창이 열립니다.
7. 예외 규칙을 구성할 사용자를 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.

   > 적응형 이상 행위 제어는 사용자 그룹 예외 규칙을 지원하지 않습니다. 사용자 그룹을 선택하면 Kaspersky Endpoint Security가 예외 규칙을 적용하지 않습니다.

8. **설명** 필드에 예외 규칙의 설명을 입력합니다.
9. 개체에 의해 시작된 소스 개체 또는 소스 프로세스의 설정 정의:

   - **소스 프로세스**. 파일이 포함된 파일 또는 폴더의 경로 또는 마스크(`C:\Dir\File.exe` 또는 `Dir\*.exe` 등).
   - **소스 프로세스 해시**. 파일 해시 코드.
   - **소스 개체**. 파일이 포함된 파일 또는 폴더의 경로 또는 마스크(`C:\Dir\File.exe` 또는 `Dir\*.exe` 등). 예, 스크립트 또는 매크로를 사용하여 대상 프로세스를 시작하는 `document.docm` 파일 경로.

     또한 웹 주소, 매크로, 명령줄의 명령, 레지스트리 경로 등의 제외할 다른 개체를 지정할 수도 있습니다. 다음 템플릿에 따라 개체를 지정합니다: `object://<object>`, 여기서 `<object>`는 개체 이름을 나타냅니다. 예, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. 마스크를 사용할 수도 있습니다. 예, `object://*C:\Windows\temp\*`.
   - **소스 개체 해시**. 파일 해시 코드.

   적응형 이상 행위 제어 규칙은 개체에 의해 수행된 작업 또는 개체에 의해 시작된 프로세스에 적용되지 않습니다.
10. 개체에서 시작된 대상 개체 또는 대상 프로세스의 설정을 지정합니다.

    - **대상 프로세스**. 파일이 포함된 파일 또는 폴더의 경로 또는 마스크(`C:\Dir\File.exe` 또는 `Dir\*.exe` 등).
    - **대상 프로세스 해시**. 파일 해시 코드.

- **대상 개체**. 대상 프로세스를 시작하는 명령. `object://<command>` 패턴을 사용하여 명령을 지정합니다. 예, `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. 마스크를 사용할 수도 있습니다. 예, `object://*C:\Windows\temp\*`.

- **대상 개체 해시**. 파일 해시 코드.

적응형 이상 행위 제어 규칙은 개체에서 행한 작업 또는 개체에서 시작된 프로세스에 적용되지 않습니다.

11. 변경 사항을 저장합니다.

적응형 이상 행위 제어 규칙에 대한 예외 규칙 내보내기 및 가져오기

선택한 규칙에 대한 예외 규칙 목록을 내보내거나 가져오려면 다음을 수행합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **보안 제어** → **적응형 이상 행위 제어**를 선택합니다.

3. **규칙** 블록에서 **규칙 편집** 버튼을 클릭합니다.
   적응형 이상 행위 제어 규칙 목록이 열립니다.

4. 규칙 목록을 내보내려면 다음을 수행합니다.

   a. 예외 규칙을 내보낼 규칙을 선택합니다.

   b. **내보내기**를 클릭합니다.

   c. 창이 열리면 예외 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

   d. 선택한 예외 규칙만 내보낼 것인지 전체 예외 규칙 목록을 내보낼 것인지 확인합니다.

   e. 파일을 저장합니다.

5. 예외 목록을 가져오려면 다음을 수행합니다.

   a. **가져오기**를 클릭합니다.

   b. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.

   c. 파일을 엽니다.
      컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

6. 변경 사항을 저장합니다.

적응형 이상 행위 제어 규칙용 업데이트 적용

안티 바이러스 데이터베이스가 업데이트되면 새 적응형 이상 행위 제어 규칙을 규칙 표에 추가할 수 있으며 기존 적응형 이상 행위 제어 규칙을 규칙 표에서 삭제할 수 있습니다. 표에 추가하거나 표에서 삭제할 적응형 이상 행위 제어 규칙의 업데이트가 적용되지 않은 경우 Kaspersky Endpoint Security가 해당 규칙을 구분합니다.

업데이트가 적용될 때까지 Kaspersky Endpoint Security는 규칙 표에서 업데이트에 의해 삭제되도록 설정된 적응형 이상 행위 제어 규칙을 표시하며 해당 규칙에 *사용 안 함* 상태를 할당합니다. 이러한 규칙의 설정은 변경할 수 없습니다.

적응형 이상 행위 제어 규칙용 업데이트를 적용하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **적응형 이상 행위 제어**를 선택합니다.
3. **규칙** 블록에서 **규칙 편집** 버튼을 클릭합니다.
   적응형 이상 행위 제어 규칙 목록이 열립니다.
4. 열리는 창에서 **업데이트 승인** 버튼을 클릭합니다.
   업데이트 승인 버튼은 적응형 이상 행위 제어 규칙용 업데이트를 사용할 수 있는 경우에 사용 가능합니다.
5. 변경 사항을 저장합니다.

적응형 이상 행위 제어 메시지 템플릿 편집

사용자가 적응형 이상 행위 제어 규칙으로 차단된 작업 수행을 시도하면 Kaspersky Endpoint Security에는 해로울 수 있는 작업이 차단된다는 메시지가 표시됩니다. 사용자는 작업이 잘못 차단되었다고 생각되면 메시지 텍스트의 링크를 사용하여 사내 네트워크 관리자에게 메시지를 전송할 수 있습니다.

잠재적으로 유해한 행동 차단과 관련하여 관리자에게 보내는 메시지를 위한 특수 템플릿이 제공됩니다. 메시지 템플릿(예: `%USER_NAME%`)을 관리하기 위해 특수 변수가 제공됩니다. 변수를 사용하면 다른 컴퓨터에서 단일 메시지 템플릿을 사용할 수 있습니다. 메시지 생성 시 Kaspersky Endpoint Security는 운영 체제 설정에서 변수 값을 검색하여 특정 컴퓨터, 사용자 및 이벤트와 일치하는 메시지에 삽입합니다.

메시지 템플릿을 편집하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **적응형 이상 행위 제어**를 선택합니다.

3. **템플릿** 블록에서 적응형 이상 행위 제어 메시지에 대한 템플릿을 구성합니다.

   - **차단 관련 메시지**. 일반적이지 않은 동작을 차단하는 적응형 이상 행위 제어 규칙이 트리거될 때 사용자에게 표시되는 메시지 템플릿입니다.

   - **관리자에게 메시지 보내기**. 사용자가 차단이 잘못된 것으로 판단한 경우 로컬 네트워크 관리자에게 사용자가 보낼 수 있는 메시지 템플릿입니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 애플리케이션 활동 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다.

   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수 추가**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

   초기화 버튼을 사용하여 기본 템플릿 텍스트를 복원할 수도 있습니다.

4. 변경 사항을 저장합니다.

적응형 이상 행위 제어 작업 모니터링

적응형 이상 행위 제어는 여러 모니터링 도구를 포함합니다. 적응형 이상 행위 제어 모니터링의 주요 목적은 학습하면서 구성 요소를 구성하는 것입니다.

적응형 이상 행위 제어 리포트

적응형 이상 행위 제어는 다음 리포트를 사용합니다:

- **적응형 이상 행위 제어 규칙 상태 리포트**. 리포트에는 적응형 이상 행위 제어 규칙(*끄기*, *스마트 학습*, *스마트 차단*, *알림*, *차단*). 이 리포트를 통해 적응형 이상 행위 제어의 학습 레벨을 분석하고 *스마트 학습* 모드에서 일반 운영 모드(*스마트 차단* 등)로 전환한 규칙의 수를 검토할 수 있습니다.

- **트리거된 적응형 이상 행위 제어 규칙 리포트**. 리포트에는 규칙 트리거 정보가 포함됩니다. 리포트에는 *차단*(*스마트 차단* 포함)이나 *알림* 등의 규칙 트리거 모드도 표시됩니다. 이 리포트를 통해 사용자 컴퓨터에서 적응형 이상 행위 제어의 활동을 검토할 수 있습니다.

관리 콘솔(MMC)에서 적응형 이상 행위 제어 리포트를 확인하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **보안 제어 → 적응형 이상 행위 제어**를 선택합니다.

4. 다음 중 하나를 수행합니다:

   - 적응형 이상 행위 제어 규칙 상태에 관한 리포트를 보려면 **적응형 이상 행위 제어 규칙 상태 리포트** 링크를 클릭합니다.
   - 트리거된 적응형 이상 행위 제어 규칙에 관한 리포트를 보려면 **트리거된 적응형 이상 행위 제어 규칙 리포트** 링크를 클릭합니다.

5. 리포트 생성 프로세스가 시작됩니다.

   리포트가 새 창으로 표시됩니다.

웹 콘솔에서 적응형 이상 행위 제어 리포트를 확인하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어 → 적응형 이상 행위 제어**로 이동합니다.
5. **규칙** 블록에서 다음 중 하나를 수행합니다:

   - 적응형 이상 행위 제어 규칙 상태에 관한 리포트를 보려면 **리포트 보기 → 규칙 상태**를 선택합니다.
   - 트리거된 적응형 이상 행위 제어 규칙에 관한 리포트를 보려면 **리포트 보기 → 탐지**를 클릭합니다.

6. 리포트 생성 프로세스가 시작됩니다.

   리포트가 새 창으로 표시됩니다.

Kaspersky Security Center 콘솔에서 리포트를 생성하려면 중앙 관리 서버로의 데이터 전송을 활성화해야 합니다. 데이터 전송은 기본적으로 활성화되어 있습니다.

관리 콘솔(MMC)에서 적응형 이상 행위 제어 데이터 전송을 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 리포트 및 저장소**를 선택합니다.
4. **중앙 관리 서버로의 데이터 전송** 블록에서 **설정** 버튼을 클릭합니다.
5. 다음 확인란을 선택합니다:

   - **적응형 이상 행위 제어 규칙 상태 리포트**.
   - **트리거된 적응형 이상 행위 제어 규칙 리포트**.

6. 변경 사항을 저장합니다.

웹 콘솔에서 적응형 이상 행위 제어에 대한 데이터 전송을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → KSC 통합**으로 갑니다.
5. **중앙 관리 서버로의 데이터 전송**에서, 다음 확인란을 선택합니다:
   - **적응형 이상 행위 제어 규칙 상태 리포트**.
   - **트리거된 적응형 이상 행위 제어 규칙 리포트**.
6. 변경 사항을 저장합니다.

스마트 학습 상태에서 트리거된 규칙 스토리지

학습 모드에서는 적응형 이상 행위 제어가 트리거된 규칙에 대한 정보를 별도의 저장소인 **스마트 학습 상태에서 트리거된 규칙**으로 보냅니다. 트리거된 규칙의 정보는 저장소에 이벤트 목록으로 표시됩니다. 적응형 이상 행위 제어를 조정하려면 컴퓨터의 비정상적인 동작을 확인하거나 규칙에서 예외 규칙을 추가합니다.

적응형 이상 행위 제어 이벤트

적응형 이상 행위 제어는 *차단*(*스마트 차단* 포함)과 *알림* 모드의 규칙 트리거 이벤트를 기록합니다. 이를 위해 다음과 같은 이벤트가 제공됩니다:

프로세스 활동 차단

프로세스 처리를 건너뜀

이벤트에는 파일 체크섬, 관련 사용자, 규칙 트리거 시간 및 컴퓨터 이름을 비롯한 의심스러운 활동에 대한 정보가 포함됩니다. 이벤트를 분석한 후 합법적인 활동을 발견하면 즉시 규칙에서 예외 규칙을 추가할 수 있습니다.

애플리케이션 제어

애플리케이션 제어는 사용자 컴퓨터의 애플리케이션 시작을 관리합니다. 이를 통해 애플리케이션 사용에 대한 회사 보안 정책을 구현할 수 있습니다. 애플리케이션 제어는 애플리케이션에 대한 접근을 제한하여 컴퓨터 감염 위험을 줄입니다.

애플리케이션 제어의 구성은 다음 단계로 구성됩니다.

1. 애플리케이션 카테고리 만들기

   관리자는 관리하려는 애플리케이션 카테고리를 생성합니다. 애플리케이션 카테고리는 관리 그룹에 관계없이 회사 네트워크의 모든 컴퓨터를 대상으로 합니다. 카테고리를 작성하려면 KL 카테고리(예: *브라우저* 또는 다른 카테고리), 파일 해시, 애플리케이션 공급 업체 및 기타 기준과 같은 기준을 사용할 수 있습니다.

2. 애플리케이션 제어 규칙 생성

   관리자는 관리 그룹의 정책에 애플리케이션 제어 규칙을 만듭니다. 규칙에는 애플리케이션 카테고리와 이러한 카테고리에서 애플리케이션의 시작 상태(차단 또는 허용)가 포함됩니다. 관리자는 여러 규칙을 만들 수 있습니다. 하나의 애플리케이션이 여러 규칙의 기준과 일치할 수 있습니다. 차단 규칙이 허용 규칙보다 우선합니다. Kaspersky Endpoint Security는 애플리케이션을 시작할 때마다 규칙과 일치하는지 확인합니다. Kaspersky Endpoint Security는 모든 애플리케이션 제어 규칙에 애플리케이션을 순서대로 대조합니다.

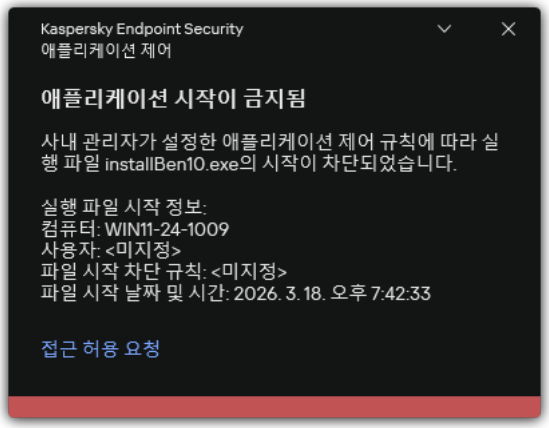
3. 애플리케이션 제어 모드 선택

   관리자는 애플리케이션 거부 목록이나 허용 목록 등 어느 규칙에도 포함되지 않은 애플리케이션의 작업 모드를 선택합니다.

사용자가 차단된 애플리케이션을 시작하려고 하면 Kaspersky Endpoint Security는 애플리케이션 시작을 차단하고 알림을 표시합니다(아래 그림 참조).

애플리케이션 제어 구성을 확인하기 위한 *테스트 모드*가 제공됩니다. 이 모드에서 Kaspersky Endpoint Security는 다음을 수행합니다.

- 애플리케이션(차단된 애플리케이션 포함) 시작을 허용합니다.
- 차단된 애플리케이션 시작에 대한 알림을 표시하고 사용자 컴퓨터의 리포트에 정보를 추가합니다.
- 차단된 애플리케이션 시작에 대한 데이터를 Kaspersky Security Center로 보냅니다.



애플리케이션 제어 알림

애플리케이션 제어 운영 모드

애플리케이션 제어 구성 요소에는 다음 두 가지 동작 모드가 있습니다:

- **거부 목록**. 이 애플리케이션 제어 모드에서는 사용자가 애플리케이션 제어 규칙에서 차단된 애플리케이션을 제외한 모든 애플리케이션을 시작할 수 있습니다.

  애플리케이션 제어의 기본 작동 모드입니다.

- **허용 목록**. 이 애플리케이션 제어 모드에서는 사용자가 애플리케이션 제어 규칙에서 허용되고 차단되지 않은 애플리케이션을 제외한 모든 애플리케이션을 시작할 수 없습니다.

  애플리케이션 제어의 허용 규칙이 구성 완료되면 애플리케이션 시작 제어 구성 요소가 LAN 관리자에 의해 확인되지 않는 모든 새로운 애플리케이션의 시작을 차단합니다. 단, 사용자의 업무에 필요한 운영 체제 및 신뢰할 수 있는 애플리케이션의 작동은 허용됩니다.

  허용 목록 모드에서 애플리케이션 제어 규칙 구성에 관한 권장 사항을 읽어 보십시오.

애플리케이션 제어 모드를 구성할 때 Kaspersky Endpoint Security 로컬 인터페이스 및 Kaspersky Security Center를 모두 사용할 수 있습니다.

그러나 Kaspersky Endpoint Security 로컬 인터페이스와 달리 Kaspersky Security Center에서는 다음과 같은 작업을 수행하는 데 필요한 도구를 제공합니다:

- 애플리케이션 카테고리 만들기

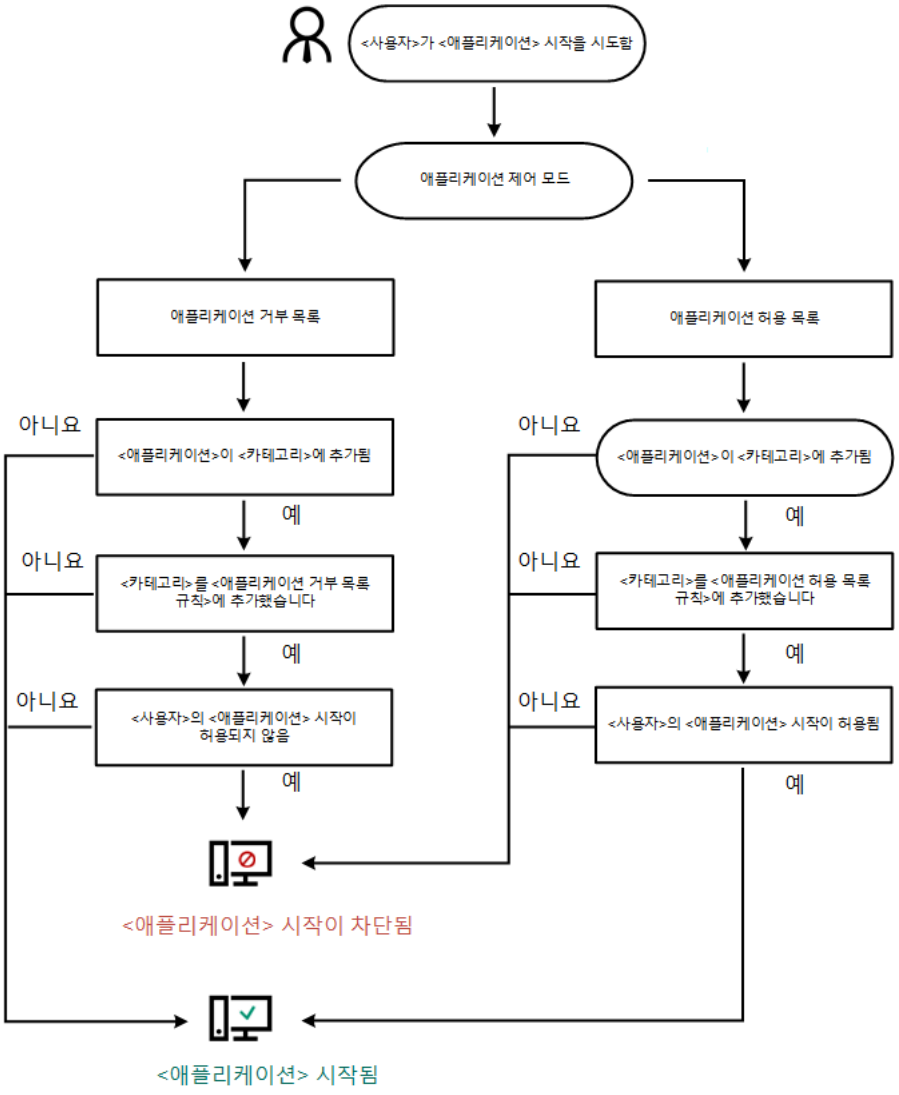
  Kaspersky Security Center 관리 콘솔에서 만든 애플리케이션 제어 규칙은 사용자 지정 애플리케이션 카테고리를 바탕으로 하며 Kaspersky Endpoint Security 로컬 인터페이스는 포함 및 예외 조건을 바탕으로 합니다.

- 기업 LAN 컴퓨터에 설치된 애플리케이션에 대한 정보 수신.

Kaspersky Security Center를 이용해 애플리케이션 제어 구성 요소의 작동을 구성하도록 권장되는 이유입니다.

애플리케이션 제어 동작 알고리즘

Kaspersky Endpoint Security는 알고리즘을 사용하여 애플리케이션 시작에 대한 결정을 내립니다(아래 그림 참조).



애플리케이션 제어 동작 알고리즘

애플리케이션 제어 기능 제한

다음 경우에는 애플리케이션 제어 구성 요소 작동이 제한됩니다:

- 애플리케이션 버전이 업그레이드되어 애플리케이션 제어 구성 요소 설정을 가져올 수 없는 경우.
- KSN 서버와 연결되어 있지 않은 경우 Kaspersky Endpoint Security는 로컬 데이터베이스에서만 애플리케이션 및 그 모듈의 평판 정보를 얻습니다.

Kaspersky Endpoint Security가 **기타 소프트웨어\KSN 평판에 따라 신뢰할 수 있는 애플리케이션** KL 카테고리로 지정한 애플리케이션 목록은 KSN 서버 접속 가능 여부에 따라 다를 수 있습니다.

- Kaspersky Security Center 데이터베이스에는 150,000건의 처리된 파일 정보를 저장할 수 있습니다. 이 레코드 수가 넘으면 새로운 파일이 처리되지 않습니다. 인벤토리 작동이 다시 시작되려면 Kaspersky Endpoint Security가 설치된 컴퓨터에서 이전에 Kaspersky Security Center 데이터베이스의 인벤토리에 등록된 파일을 삭제해야 합니다.
- 구성 요소는 명령줄을 통해 스크립트를 해석기에 전송하지 않는 한 스크립트 시작을 제어하지 않습니다.

  애플리케이션 제어 규칙에서 해석기를 시작하도록 허용된 경우 구성 요소는 이 해석기에서 시작된 스크립트를 차단하지 않습니다.

  해석기 명령줄에 지정된 스크립트 하나 이상의 시작이 애플리케이션 제어 규칙에 의해 차단되면 구성 요소는 해석기 명령줄에 지정된 모든 스크립트를 차단합니다.

- 구성 요소는 Kaspersky Endpoint Security에서 지원하지 않는 해석기 스크립트의 시작을 제어하지 않습니다.

  Kaspersky Endpoint Security는 다음 해석기를 지원합니다:

  - Java
  - PowerShell

  다음 해석기 유형이 지원됩니다:

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe
  - %SystemRoot%\system32\cscript.exe
  - %SystemRoot%\system32\wscript.exe
  - %SystemRoot%\system32\msiexec.exe
  - %SystemRoot%\system32\mshta.exe
  - %SystemRoot%\system32\rundll32.exe
  - %SystemRoot%\system32\wwahost.exe
  - %SystemRoot%\syswow64\cmd.exe
  - %SystemRoot%\syswow64\regedit.exe
  - %SystemRoot%\syswow64\regedt32.exe
  - %SystemRoot%\syswow64\cscript.exe
  - %SystemRoot%\syswow64\wscript.exe

- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

사용자 컴퓨터에 설치된 애플리케이션에 대한 정보 수신

최적의 애플리케이션 제어 규칙을 만들려면 먼저 기업 LAN에 소속된 컴퓨터에서 사용되는 애플리케이션에 대한 정보를 수집해야 합니다. 다음 정보를 수집할 수 있습니다:

- 제조사, 버전, 기업 LAN에서 사용된 애플리케이션 언어.
- 애플리케이션 업데이트 주기.
- 회사에 적용된 애플리케이션 사용 정책(보안 정책 또는 관리 정책).
- 애플리케이션 배포 패키지의 저장 위치.

애플리케이션 정보 보기

설치된 애플리케이션에 대한 정보는 Kaspersky Security Center 네트워크 에이전트 폴더)에서 제공합니다. 설치된 애플리케이션에 대한 정보는 Kaspersky Security Center 네트워크 에이전트(**자산 관리(소프트웨어)** 폴더)에서 제공합니다. 네트워크 에이전트는 Kaspersky Security Center와 동기화할 때마다 정보를 업데이트합니다. 네트워크 에이전트가 전송하는 정보에 관한 자세한 정보는 Kaspersky Security Center 도움말을 참조하십시오.

애플리케이션 레지스트리 폴더에서 애플리케이션 속성 창을 열려면 다음을 수행합니다.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리에서 **고급 → 애플리케이션 관리 → 자산 관리(소프트웨어)**를 선택합니다.
3. 애플리케이션을 선택합니다.
4. 애플리케이션의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

실행 파일에 관한 정보 보기

실행 파일에 관한 정보 쿼리 시 데이터베이스의 부하를 줄일 수 있습니다. 이를 위해서는 표준 소프트웨어 세트가 설치된 여러 참조 컴퓨터에서 *인벤토리* 작업을 수행하는 것이 좋습니다.

Kaspersky Endpoint Security의 *인벤토리* 작업을 사용해 실행 파일 목록을 가져올 수 있습니다. Kaspersky Security Center 콘솔의 **실행 파일** 폴더에서 실행 파일 목록을 볼 수 있습니다.

인벤토리 작업을 실행하기 전에, 데이터베이스가 Kaspersky Security Center의 권장 사항을 충족하는지 확인합니다. 데이터베이스 제한에 관한 자세한 정보는 Kaspersky Security Center 도움말을 참조하십시오.

관리 콘솔(MMC)에서 인벤토리 작업을 실행하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **인벤토리**를 선택합니다.

2단계. 인벤토리 범위

Kaspersky Endpoint Security가 실행 파일을 찾을 폴더의 목록을 생성합니다. 인벤토리 설정을 구성합니다(아래 표 참조).

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. 작업을 실행할 계정 선택

인벤토리 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다. 인벤토리 범위에 네트워크 드라이브 또는 접근이 제한된 다른 개체가 포함된 경우 충분한 접근 권한이 있는 사용자 계정을 선택합니다.

5 단계. 작업 시작 스케줄 구성

작업 일정을 설정합니다(예: 수동).

6단계. 작업 이름 정의

작업 이름을 입력합니다(*베이스라인 인벤토리* 등).

7단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다. 결과적으로, 구성된 스케줄에 따라 사용자 컴퓨터에서 실행 파일 검색이 수행됩니다.

웹 콘솔 및 Cloud Console에서 인벤토리 작업을 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **인벤토리**를 선택합니다.
   c. **작업 이름** 필드에 *베이스라인 인벤토리* 등과 같은 간단한 설명을 입력합니다.
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.
5. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.
6. 마법사를 끝냅니다.
   작업 목록에 새 작업이 표시됩니다.
7. 작업을 구성하려면 작업 속성으로 이동합니다(아래 표 참조).
8. 작업 옆의 확인란을 선택합니다.
9. **시작**을 클릭합니다.
   작업 상태와 작업이 정상적으로 완료되었거나 완료 시 오류가 발생한 장치의 수를 감시할 수 있습니다. 이렇게 하면 지정한 스케줄에 따라 사용자 컴퓨터에서 실행 파일을 검색합니다.

파라미터	설명
인벤토리 범위	인벤토리 범위를 구성할 개체 목록입니다.
DLL 모듈 인벤토리	Kaspersky Endpoint Security가 인벤토리 범위에서 DLL 모듈을 찾고 정보를 Kaspersky Security Center로 전송합니다. DLL 모듈 인벤토리를 활성화하면 인벤토리 작업 완료에 걸리는 시간과 데이터베이스 크기가 상당히 증가합니다.
스크립트 파일 인벤토리	Kaspersky Endpoint Security가 인벤토리 범위에서 스크립트를 찾고 정보를 Kaspersky Security Center로 전송합니다. 스크립트 파일 인벤토리를 활성화하면 인벤토리 작업 완료에 걸리는 시간과 데이터베이스 크기가 상당히 증가합니다.
컴퓨터가 유휴 상태일 때만 실행	컴퓨터 리소스가 사용 중일 때 작업 시작을 연기했습니다. Kaspersky Endpoint Security는 컴퓨터가 잠겨 있거나 화면 보호기가 켜져 있을 때 검사 작업을 시작합니다. 예를 들어 컴퓨터를 잠금 해제하는 등으로 작업 실행이 중단되면 Kaspersky Endpoint Security는 자동으로 중단된 지점부터 작업을 실행합니다. 이 예약 옵션을 사용하면 컴퓨터를 사용할 때 컴퓨터 리소스를 절약할 수 있습니다.
새로운 파일과 수정된 파일만 검사	새로운 파일과 마지막 검사 이후 수정된 파일만 검사합니다. 이는 검사 시간을 줄이는 것입니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.
다음보다 오래 검사하는 파일은 건너뛰기(초) N초	작업 실행 시간 제한. 지정된 시간 후에는 Kaspersky Endpoint Security가 작업을 중지합니다. 작업은 완료된 것으로 표시되지 않습니다. 다음에 Kaspersky Endpoint Security가 해당 작업을 실행하면 스케줄에 따라 처음부터 실행됩니다.
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	타사 애플리케이션의 배포 패키지 검사.
큰 복합 파일은 압축 해제 안 함	이 확인란을 선택하면 애플리케이션이 지정된 크기를 초과하는 복합 파일을 검사하지 않습니다. 이 확인란을 선택하지 않으면 애플리케이션이 크기에 자격 증명 공급업체이 모든 파일을 검사합니다. 애플리케이션은 확인란의 선택 여부와 관계없이 압축 파일에서 압축 해제한 대용량 파일을 검사합니다.

실행 파일 폴더에서 실행 파일의 속성 창을 열려면 다음을 수행합니다.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리에서 **고급 → 애플리케이션 관리 → 실행 파일**을 선택합니다.
3. 실행 파일을 선택합니다.
4. 실행 파일의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

애플리케이션과 그 실행 파일에 대한 일반적인 정보 및 해당 애플리케이션이 설치된 컴퓨터의 목록을 보려면 **자산 관리(소프트웨어)** 폴더 또는 **실행 파일** 폴더에서 애플리케이션을 선택한 후 속성 창을 엽니다.

설치된 애플리케이션과 실행 파일 관련 정보 업데이트

Kaspersky Endpoint Security 12.3 for Windows부터 실행 파일 데이터베이스가 포함된 애플리케이션 제어 구성 요소의 작동이 최적화되었습니다. Kaspersky Endpoint Security 12.3 for Windows는 컴퓨터에서 파일이 삭제된 후 데이터베이스를 자동으로 업데이트합니다. 이를 통해 데이터베이스를 최신 상태로 유지하고 Kaspersky Security Center 리소스를 절약할 수 있습니다.

설치된 애플리케이션의 데이터베이스를 최신 상태로 유지하려면 중앙 관리 서버로 애플리케이션의 정보를 전송하는 기능이 활성화되어야 합니다(기본적으로 활성화되어 있음).

관리 콘솔(MMC)에서 애플리케이션 정보 전송을 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 리포트 및 저장소**를 선택합니다.
4. **중앙 관리 서버로의 데이터 전송** 블록에서 **설정** 버튼을 클릭합니다.
5. **시작된 애플리케이션** 확인란을 선택합니다.
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 애플리케이션을 정보 전송을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → KSC 통합**으로 갑니다.
5. **중앙 관리 서버로의 데이터 전송** 블록에서 **고급 설정** 버튼을 클릭합니다.
6. 창이 열리면 **시작된 애플리케이션 정보** 확인란을 선택합니다.
7. 변경 사항을 저장합니다.

차단된 애플리케이션 모드를 활성화하는 방법

차단된 애플리케이션 모드는 애플리케이션 제어가 사용자가 애플리케이션 제어 규칙에서 차단된 애플리케이션을 제외한 모든 애플리케이션을 시작할 수 있도록 허용하는 모드입니다. 즉, 거부 규칙이 없으면 애플리케이션 제어가 애플리케이션 시작을 허용합니다. 애플리케이션 제어의 기본 작동 모드입니다.

> *차단된 애플리케이션* 모드를 활성화하기 전에 애플리케이션 제어 규칙을 테스트하는 것이 좋습니다. 이를 위해 테스트 모드를 활성화할 수 있습니다.

관리 콘솔(MMC)에서 차단된 애플리케이션 모드를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **보안 제어 → 애플리케이션 제어**를 선택합니다.
5. **애플리케이션 제어** 확인란을 선택합니다.

6. **애플리케이션 제어 설정** 블록에서 **제어 모드** 드롭다운 목록을 사용하여 **거부 목록**을 선택합니다.

7. **처리** 드롭다운 목록에서 애플리케이션 제어의 작업을 선택합니다.

   - **규칙 테스트**. 애플리케이션 제어는 규칙에 의해 실행이 금지된 애플리케이션을 차단하지 않지만, 그렇지 않으면 차단되었을 애플리케이션의 실행에 대한 이벤트를 생성합니다.
   - **규칙 적용** 애플리케이션 제어는 차단된 애플리케이션을 차단하고 해당 이벤트를 생성합니다.

8. 애플리케이션 제어 규칙의 상태를 선택합니다.

   - **켜짐**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 사용되고 있음을 나타냅니다.
   - **꺼짐**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 무시되고 있음을 나타냅니다.
   - **테스트**. 이 상태는 Kaspersky Endpoint Security가 애플리케이션의 시작을 항상 허용하며, 규칙이 적용되지만 그러한 애플리케이션의 시작에 관한 정보가 리포트에 기록된다는 것을 의미합니다.

   필요한 경우 새 애플리케이션 제어 규칙을 추가합니다.

9. 애플리케이션 제어의 고급 설정을 구성합니다.

   - **DLL 모듈 로드 모니터링(시스템 부하가 상당히 증가합니다)**. 이 확인란이 선택되어 있으면 Kaspersky Endpoint Security에서 사용자가 애플리케이션을 시작하려고 시도할 때 DLL 모듈의 로딩을 제어합니다. DLL 모듈 및 이 DLL 모듈을 로드한 애플리케이션에 대한 정보는 리포트에 기록됩니다.

     DLL 모듈 및 드라이버 로딩에 대한 제어를 사용할 때는 애플리케이션 제어 설정에서 기본 **골든 이미지** 규칙 또는 '**골든 이미지\신뢰하는 인증서**' KL 카테고리가 포함된 다른 규칙 중 하나를 사용하고 있는지 확인하고, Kaspersky Endpoint Security를 시작하기 전에 신뢰하는 DLL 모듈과 드라이버가 먼저 로드되도록 하십시오. **골든 이미지** 규칙을 사용하지 않을 때 DLL 모듈 및 드라이버의 로드를 제어하면 운영 체제가 불안정해질 수 있습니다.

     Kaspersky Endpoint Security는 확인란이 선택된 이후에 로드된 DLL 모듈과 드라이버만 감시합니다. 확인란을 선택한 후 컴퓨터를 다시 시작하여 애플리케이션이 Kaspersky Endpoint Security가 시작되기 전에 로드된 DLL을 포함하여 모든 DLL 모듈 및 드라이버를 감시하는지 확인할 것을 권장합니다.

   - **엄격한 디지털 서명 인증 사용**. 애플리케이션 제어 규칙에 대한 트리거 조건으로 인증서를 선택할 수 있습니다. 이 확인란을 선택하면 Kaspersky Endpoint Security는 신뢰하는 시스템 인증서 저장소의 인증서로만 서명된 애플리케이션에 규칙을 적용합니다. 이러한 인증서로 서명된 애플리케이션은 *악성 코드 검사* 작업과 같은 보호 구성 요소에서도 신뢰할 수 있는 것으로 간주됩니다. 그러나 애플리케이션 제어 규칙에서 다른 저장소의 인증서를 지정하는 경우 Kaspersky Endpoint Security는 해당 규칙을 적용하지 않습니다.

     이 확인란이 선택되어 있지 않으면 Kaspersky Endpoint Security는 Windows Trusted Root Certificate Store의 인증서로만 서명된 애플리케이션에 규칙을 적용합니다. 이러한 애플리케이션은 신뢰 구역에 포함되지 않습니다. 보호 구성 요소는 이러한 애플리케이션의 활동을 모니터링합니다.

   - **차단 관련 메시지**. 애플리케이션 시작을 차단하는 애플리케이션 제어 규칙이 작동될 때 표시되는 메시지의 템플릿.
   - **관리자에게 메시지 보내기**. 사용자가 애플리케이션이 실수로 차단되었다고 생각하는 경우 회사 LAN 관리자에게 보낼 수 있는 메시지 템플릿입니다.

10. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 차단된 애플리케이션 모드를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **앱 제어**로 이동합니다.
5. **애플리케이션 제어 활성화됨** 토글을 켭니다.
6. **운영 모드** 블록에서 **규칙 목록을 제외하고 모두 차단**을 선택합니다.
7. **처리** 블록에서 애플리케이션 제어의 작업을 선택합니다.
   - **알림**. 애플리케이션 제어는 규칙에 의해 실행이 금지된 애플리케이션을 차단하지 않지만, 그렇지 않으면 차단되었을 애플리케이션의 실행에 대한 이벤트를 생성합니다.
   - **규칙 적용** 애플리케이션 제어는 차단된 애플리케이션을 차단하고 해당 이벤트를 생성합니다.
8. 애플리케이션 제어 규칙의 상태를 선택합니다.
   - **사용**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 사용되고 있음을 나타냅니다.
   - **사용 안 함**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 무시되고 있음을 나타냅니다.
   - **테스트 모드**. 이 상태는 Kaspersky Endpoint Security가 애플리케이션의 시작을 항상 허용하며, 규칙이 적용되지만 그러한 애플리케이션의 시작에 관한 정보가 리포트에 기록된다는 것을 의미합니다.

   필요한 경우 새 애플리케이션 제어 규칙을 추가합니다.
9. 애플리케이션 제어의 고급 설정을 구성합니다.
   - **DLL 모듈 로드 모니터링**. 이 확인란이 선택되어 있으면 Kaspersky Endpoint Security에서 사용자가 애플리케이션을 시작하려고 시도할 때 DLL 모듈의 로딩을 제어합니다. DLL 모듈 및 이 DLL 모듈을 로드한 애플리케이션에 대한 정보는 리포트에 기록됩니다.

     DLL 모듈 및 드라이버 로딩에 대한 제어를 사용할 때는 애플리케이션 제어 설정에서 기본 **골든 이미지** 규칙 또는 '**골든 이미지\신뢰하는 인증서**' KL 카테고리가 포함된 다른 규칙 중 하나를 사용하고 있는지 확인하고, Kaspersky Endpoint Security를 시작하기 전에 신뢰하는 DLL 모듈과 드라이버가 먼저 로드되도록 하십시오. **골든 이미지** 규칙을 사용하지 않을 때 DLL 모듈 및 드라이버의 로드를 제어하면 운영 체제가 불안정해질 수 있습니다.

     Kaspersky Endpoint Security는 확인란이 선택된 이후에 로드된 DLL 모듈과 드라이버만 감시합니다. 확인란을 선택한 후 컴퓨터를 다시 시작하여 애플리케이션이 Kaspersky Endpoint Security가 시작되기 전에 로드된 DLL을 포함하여 모든 DLL 모듈 및 드라이버를 감시하는지 확인할 것을 권장합니다.

- **엄격한 디지털 서명 인증 사용**. 애플리케이션 제어 규칙에 대한 트리거 조건으로 인증서를 선택할 수 있습니다. 이 확인란을 선택하면 Kaspersky Endpoint Security는 신뢰하는 시스템 인증서 저장소의 인증서로만 서명된 애플리케이션에 규칙을 적용합니다. 이러한 인증서로 서명된 애플리케이션은 *악성 코드 검사* 작업과 같은 보호 구성 요소에서도 신뢰할 수 있는 것으로 간주됩니다. 그러나 애플리케이션 제어 규칙에서 다른 저장소의 인증서를 지정하는 경우 Kaspersky Endpoint Security는 해당 규칙을 적용하지 않습니다.

  이 확인란이 선택되어 있지 않으면 Kaspersky Endpoint Security는 Windows Trusted Root Certificate Store의 인증서로만 서명된 애플리케이션에 규칙을 적용합니다. 이러한 애플리케이션은 신뢰 구역에 포함되지 않습니다. 보호 구성 요소는 이러한 애플리케이션의 활동을 모니터링합니다.

- **사용자에게 보내는 메시지**. 애플리케이션 시작을 차단하는 애플리케이션 제어 규칙이 작동될 때 표시되는 메시지의 템플릿.

- **관리자에게 메시지 보내기**. 사용자가 애플리케이션이 실수로 차단되었다고 생각하는 경우 회사 LAN 관리자에게 보낼 수 있는 메시지 템플릿입니다.

10. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 차단된 애플리케이션 모드를 활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **애플리케이션 제어**를 선택합니다.
3. **애플리케이션 제어** 토글을 켭니다.
4. **애플리케이션 시작 제어 모드** 블록에서 **거부 목록을 선택합니다. 규칙 목록에 있는 애플리케이션을 제외한 모든 애플리케이션이 허용됩니다**.
5. **규칙에 따라 차단되는 애플리케이션 시작 시 수행하는 조치** 블록에서 애플리케이션 제어의 작업을 선택합니다.

   - **리포트에서 알리고(테스트 모드) 이벤트 로그를 다음에 저장:**. 애플리케이션 제어는 규칙에 의해 실행이 금지된 애플리케이션을 차단하지 않지만, 그렇지 않으면 차단되었을 애플리케이션의 실행에 대한 이벤트를 생성합니다.

   - **차단**. 애플리케이션 제어는 차단된 애플리케이션을 차단하고 해당 이벤트를 생성합니다.

6. 애플리케이션 제어 규칙의 상태를 선택합니다.

   - **사용**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 사용되고 있음을 나타냅니다.

   - **사용 안 함**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 무시되고 있음을 나타냅니다.

   - **테스트 모드**. 이 상태는 Kaspersky Endpoint Security가 애플리케이션의 시작을 항상 허용하며, 규칙이 적용되지만 그러한 애플리케이션의 시작에 관한 정보가 리포트에 기록된다는 것을 의미합니다.

   필요한 경우 새 애플리케이션 제어 규칙을 추가합니다.

7. 애플리케이션 제어의 고급 설정을 구성합니다.

   - **DLL 모듈 로드 모니터링**. 이 확인란이 선택되어 있으면 Kaspersky Endpoint Security에서 사용자가 애플리케이션을 시작하려고 시도할 때 DLL 모듈의 로딩을 제어합니다. DLL 모듈 및 이 DLL 모듈을 로드한 애플리케이션에 대한 정보는 리포트에 기록됩니다.

DLL 모듈 및 드라이버 로딩에 대한 제어를 사용할 때는 애플리케이션 제어 설정에서 기본 **골든 이미지** 규칙 또는 '**골든 이미지\신뢰하는 인증서**' KL 카테고리가 포함된 다른 규칙 중 하나를 사용하고 있는지 확인하고, Kaspersky Endpoint Security를 시작하기 전에 신뢰하는 DLL 모듈과 드라이버가 먼저 로드되도록 하십시오. **골든 이미지** 규칙을 사용하지 않을 때 DLL 모듈 및 드라이버의 로드를 제어하면 운영 체제가 불안정해질 수 있습니다.

Kaspersky Endpoint Security는 확인란이 선택된 이후에 로드된 DLL 모듈과 드라이버만 감시합니다. 확인란을 선택한 후 컴퓨터를 다시 시작하여 애플리케이션이 Kaspersky Endpoint Security가 시작되기 전에 로드된 DLL을 포함하여 모든 DLL 모듈 및 드라이버를 감시하는지 확인할 것을 권장합니다.

- **엄격한 디지털 서명 인증 사용**. 애플리케이션 제어 규칙에 대한 트리거 조건으로 인증서를 선택할 수 있습니다. 이 확인란을 선택하면 Kaspersky Endpoint Security는 신뢰하는 시스템 인증서 저장소의 인증서로만 서명된 애플리케이션에 규칙을 적용합니다. 이러한 인증서로 서명된 애플리케이션은 *악성 코드 검사* 작업과 같은 보호 구성 요소에서도 신뢰할 수 있는 것으로 간주됩니다. 그러나 애플리케이션 제어 규칙에서 다른 저장소의 인증서를 지정하는 경우 Kaspersky Endpoint Security는 해당 규칙을 적용하지 않습니다.

  이 확인란이 선택되어 있지 않으면 Kaspersky Endpoint Security는 Windows Trusted Root Certificate Store의 인증서로만 서명된 애플리케이션에 규칙을 적용합니다. 이러한 애플리케이션은 신뢰 구역에 포함되지 않습니다. 보호 구성 요소는 이러한 애플리케이션의 활동을 모니터링합니다.

- **애플리케이션 차단에 관한 메시지 템플릿**. 애플리케이션 시작을 차단하는 애플리케이션 제어 규칙이 작동될 때 표시되는 메시지의 템플릿.

- **애플리케이션 시작 차단 시 표시되는 팝업 메시지의 템플릿입니다**. 사용자가 애플리케이션이 실수로 차단되었다고 생각하는 경우 회사 LAN 관리자에게 보낼 수 있는 메시지 템플릿입니다.

8. 변경 사항을 저장합니다.

결과적으로 애플리케이션 제어가 차단된 애플리케이션을 차단합니다. 또한 Kaspersky Endpoint Security가 *애플리케이션 시작이 금지됨* 이벤트를 생성합니다. 이러한 이벤트를 사용하여 Kaspersky Security Center 콘솔에서 *금지한 애플리케이션 리포트*를 리포트할 수 있습니다. 리포트 요약에서 애플리케이션 제어 규칙이 트리거된 애플리케이션 및 컴퓨터의 목록을 볼 수 있습니다.

베이스라인 컴퓨터 기반 애플리케이션 제어

베이스라인 컴퓨터를 사용하여 필요한 애플리케이션 집합으로 이미지를 생성할 수 있습니다. 그런 다음 이 이미지를 사용하여 운영 체제 및 애플리케이션을 다른 컴퓨터에 배포할 수 있습니다. 이미지를 최신 상태로 유지하는 것이 항상 가능한 것은 아닙니다. 애플리케이션 제어를 사용하면 베이스라인 컴퓨터를 기반으로 허용된 애플리케이션의 목록을 유지 관리할 수 있습니다. 애플리케이션 제어는 베이스라인 컴퓨터에 설치되는 애플리케이션을 자동으로 결정하고 카테고리를 업데이트합니다. 이러한 방식으로 컴퓨터는 허용된 애플리케이션의 최신 목록을 가져옵니다.

베이스라인 컴퓨터를 기반으로 애플리케이션 제어를 구성하려면 다음 단계를 수행합니다.

1. 자동으로 업데이트되는 카테고리 생성. 새 카테고리를 생성할 때 **지정한 폴더의 실행 파일을 포함하는 카테고리** 카테고리를 선택하고 베이스라인 컴퓨터를 선택합니다.

   관리 콘솔(MMC)에서 자동으로 업데이트되는 카테고리를 생성하는 방법

   1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

   2. 관리 콘솔 트리에서 **고급 → 애플리케이션 관리 → 애플리케이션 카테고리**를 선택합니다.

3. 작업 공간에서 **새 카테고리** 버튼을 누릅니다.
   애플리케이션 카테고리 생성 마법사가 시작됩니다.

4. 애플리케이션 카테고리 생성 마법사의 안내를 따릅니다.

1단계. 카테고리 유형 선택

카테고리 유형으로 **선택한 장치의 실행 파일이 포함된 카테고리**를 선택합니다.

2단계. 사용자 카테고리 이름 입력

이 단계에서는 애플리케이션 카테고리의 이름을 지정합니다.

3단계. 설정

> 이 단계는 **선택한 장치의 실행 파일이 포함된 카테고리** 유형을 선택한 경우에 수행할 수 있습니다.

이 단계에서는 **추가** 버튼을 누르고 Kaspersky Security Center가 애플리케이션 카테고리에 추가할 실행 파일이 있는 컴퓨터를 지정합니다. Kaspersky Security Center는 **실행 파일** 폴더에 표시된 지정된 컴퓨터의 모든 실행 파일을 애플리케이션 카테고리에 추가합니다.

또한 이 단계에서 다음 설정을 구성할 수 있습니다:

- 해시 함수 계산을 위한 알고리즘. 알고리즘을 선택하려면 다음 확인란 중 하나를 선택해야 합니다.
  - **이 카테고리의 파일에 대해 SHA256 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원)**.
  - **이 카테고리의 파일에 대해 MD5 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 서비스 팩 2 이전 버전에서 지원)**.
- **중앙 관리 서버 저장소와 데이터 동기화** 확인란. Kaspersky Security Center가 애플리케이션 카테고리를 정기적으로 지우고 **실행 파일** 폴더에 표시된 특정 컴퓨터의 모든 실행 파일을 추가하도록 하려면 이 확인란을 선택합니다.
  중앙 관리 서버 저장소와 데이터 동기화 확인란 선택을 취소하면 Kaspersky Security Center는 생성된 애플리케이션 카테고리를 수정하지 않습니다.

4단계. 필터

이 단계에서는 파일 필터를 구성합니다.

애플리케이션 카테고리를 생성하는 데 사용할 파일 유형을 지정할 수 있습니다.

- **모든 파일**. 이 카테고리는 모든 파일과 일치합니다. 이 옵션은 기본적으로 선택되어 있습니다.
- **애플리케이션 카테고리 이외의 파일만**. 이 카테고리는 애플리케이션 카테고리에 없는 파일과만 일치합니다.

선택한 컴퓨터에서 애플리케이션 카테고리를 생성하는 데 사용할 파일이 포함된 폴더를 지정할 수 있습니다.

- **모든 폴더**. 이 카테고리는 모든 폴더와 일치합니다. 이 옵션은 기본적으로 선택되어 있습니다.
- **지정한 폴더**. 이 카테고리는 지정한 폴더와만 일치합니다. 이 옵션을 선택하면 폴더 경로를 지정해야 합니다.

5단계. 사용자 지정 카테고리 생성

마법사를 끝냅니다.

웹 콘솔 및 Cloud Console에서 자동으로 추가된 콘텐츠로 카테고리를 생성하는 방법

1. 웹 콘솔의 기본 창에서 **동작 → 타사 애플리케이션 → 애플리케이션 카테고리**를 선택합니다.
   애플리케이션 카테고리 목록이 열립니다.
2. **추가**를 클릭합니다.
   애플리케이션 카테고리 생성 마법사가 시작됩니다.
3. 애플리케이션 카테고리의 일반 설정을 구성합니다.
   - 카테고리 이름.
   - 카테고리 생성 방법. 카테고리 유형으로 **선택한 장치의 실행 파일이 포함된 카테고리**를 선택합니다.

   다음 단계로 넘어갑니다.
4. 애플리케이션 카테고리의 고급 설정을 구성합니다.
   - Kaspersky Security Center가 애플리케이션 카테고리에 실행 파일을 추가할 컴퓨터를 지정합니다. Kaspersky Security Center는 **실행 파일** 폴더에 표시된 지정된 컴퓨터의 모든 실행 파일을 애플리케이션 카테고리에 추가합니다.
   - 해시 함수 계산을 위한 알고리즘을 선택합니다.
   - 중앙 관리 서버 저장소와 데이터를 동기화하는 간격을 구성합니다.
   - 파일 필터를 구성합니다.
5. 마법사를 끝냅니다.

자동으로 업데이트되는 카테고리를 생성할 때 파일을 여러 카테고리로 세분하는 것이 편리할 수 있습니다. 예: 운영 체제 파일 및 Program Files 폴더의 파일. 그러려면 카테고리 설정에서 필터를 사용하고 개별 폴더를 선택하면 됩니다.

2. 애플리케이션 제어 모드 선택. 명시적으로 허용되지 않은 모든 애플리케이션의 실행을 금지해야 합니다. 그러려면 *차단된 애플리케이션* 모드를 선택합니다.

3. 애플리케이션 제어 규칙 생성. 규칙 설정에서 베이스라인 컴퓨터의 실행 파일이 속한 카테고리를 선택합니다.

관리 콘솔(MMC)에서 베이스라인 컴퓨터를 기반으로 애플리케이션 제어를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **보안 제어** → **애플리케이션 제어**를 선택합니다.
5. **애플리케이션 제어** 확인란을 선택합니다.
6. **애플리케이션 제어 설정** 블록에서 **제어 모드** 드롭다운 목록을 사용하여 **거부 목록**을 선택합니다.
7. **처리** 드롭다운 목록에서 애플리케이션 제어의 작업을 선택합니다.
   - **규칙 테스트**. 애플리케이션 제어는 규칙에 의해 실행이 금지된 애플리케이션을 차단하지 않지만, 그렇지 않으면 차단되었을 애플리케이션의 실행에 대한 이벤트를 생성합니다.
   - **규칙 적용** 애플리케이션 제어는 차단된 애플리케이션을 차단하고 해당 이벤트를 생성합니다.
8. 애플리케이션 제어 규칙 목록에서 **추가** 버튼을 누릅니다.
   애플리케이션 제어 규칙을 추가하기 위한 마법사가 시작됩니다.
9. **카테고리** 드롭다운 목록에서 베이스라인 컴퓨터를 기반으로 자동으로 업데이트되는 카테고리를 선택합니다.
10. 애플리케이션 제어 규칙을 적용할 사용자 또는 사용자 그룹을 선택합니다.
11. 애플리케이션 제어 규칙의 고급 설정을 구성합니다.
    - **다른 사용자 거부**. 애플리케이션은 목록에 없는 모든 사용자에 대해 선택한 카테고리에 속하는 애플리케이션의 실행을 금지합니다.
    - **신뢰하는 업데이터** Kaspersky Endpoint Security는 선택한 카테고리에 포함된 애플리케이션을 신뢰하는 업데이터로 간주하여 이후 실행될 다른 실행 파일을 생성하도록 허용합니다.
12. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 베이스라인 컴퓨터를 기반으로 애플리케이션 제어를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **앱 제어**로 이동합니다.
5. **애플리케이션 제어 활성화됨** 토글을 켭니다.
6. **운영 모드** 블록에서 **규칙 목록을 제외하고 모두 차단**을 선택합니다.

7. **처리** 블록에서 애플리케이션 제어의 작업을 선택합니다.

   - **알림**. 애플리케이션 제어는 규칙에 의해 실행이 금지된 애플리케이션을 차단하지 않지만, 그렇지 않으면 차단되었을 애플리케이션의 실행에 대한 이벤트를 생성합니다.

   - **규칙 적용** 애플리케이션 제어는 차단된 애플리케이션을 차단하고 해당 이벤트를 생성합니다.

8. 애플리케이션 제어 규칙 목록에서 **추가** 버튼을 누릅니다.

   애플리케이션 제어 규칙을 추가하기 위한 마법사가 시작됩니다.

9. **카테고리/애플리케이션** 아래에서 베이스라인 컴퓨터를 기반으로 자동으로 업데이트되는 카테고리를 선택합니다.

10. 애플리케이션 제어 규칙을 적용할 사용자 또는 사용자 그룹을 선택합니다.

11. 애플리케이션 제어 규칙의 고급 설정을 구성합니다.

    - **사용자**. 애플리케이션은 목록에 없는 모든 사용자에 대해 선택한 카테고리에 속하는 애플리케이션의 실행을 금지합니다.

    - **신뢰하는 업데이터** Kaspersky Endpoint Security는 선택한 카테고리에 포함된 애플리케이션을 신뢰하는 업데이터로 간주하여 이후 실행될 다른 실행 파일을 생성하도록 허용합니다.

12. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 베이스라인 컴퓨터를 기반으로 애플리케이션 제어를 구성하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **보안 제어** → **애플리케이션 제어**를 선택합니다.

3. **애플리케이션 제어** 토글을 켭니다.

4. **애플리케이션 시작 제어 모드** 블록에서 **거부 목록을 선택합니다. 규칙 목록에 있는 애플리케이션을 제외한 모든 애플리케이션이 허용됩니다**.

5. **규칙에 따라 차단되는 애플리케이션 시작 시 수행하는 조치** 블록에서 애플리케이션 제어의 작업을 선택합니다.

   - **리포트에서 알리고(테스트 모드) 이벤트 로그를 다음에 저장:**. 애플리케이션 제어는 규칙에 의해 실행이 금지된 애플리케이션을 차단하지 않지만, 그렇지 않으면 차단되었을 애플리케이션의 실행에 대한 이벤트를 생성합니다.

   - **차단**. 애플리케이션 제어는 차단된 애플리케이션을 차단하고 해당 이벤트를 생성합니다.

6. 애플리케이션 제어 규칙 목록에서 **추가** 버튼을 누릅니다.

   애플리케이션 제어 규칙을 추가하기 위한 마법사가 시작됩니다.

7. **카테고리** 아래에서 베이스라인 컴퓨터를 기반으로 자동으로 업데이트되는 카테고리를 선택합니다.

8. 애플리케이션 제어 규칙을 적용할 사용자 또는 사용자 그룹을 선택합니다.

9. 애플리케이션 제어 규칙의 고급 설정을 구성합니다.

   - **다른 사용자 거부**. 애플리케이션은 목록에 없는 모든 사용자에 대해 선택한 카테고리에 속하는 애플리케이션의 실행을 금지합니다.

   - **신뢰하는 업데이터** Kaspersky Endpoint Security는 선택한 카테고리에 포함된 애플리케이션을 신뢰하는 업데이터로 간주하여 이후 실행될 다른 실행 파일을 생성하도록 허용합니다.

10. 변경 사항을 저장합니다.

애플리케이션 제어 규칙 관리

Kaspersky Endpoint Security는 규칙을 사용해 사용자가 시작한 애플리케이션을 제어합니다. 애플리케이션 제어 규칙은 규칙이 적용되는 시작 조건과 애플리케이션 제어 구성 요소가 수행하는 동작을 지정합니다(사용자가 시작한 애플리케이션의 실행을 허용 또는 차단).

규칙을 작동시키는 조건

규칙 트리거 조건에는 "조건 유형 - 조건 기준 - 조건 값"과 같은 상관 관계가 있습니다. 규칙 트리거 조건에 따라 Kaspersky Endpoint Security는 애플리케이션에 규칙을 적용하거나 적용하지 않습니다.

다음 유형의 조건이 규칙에 사용됩니다:

- *포함 조건*. Kaspersky Endpoint Security는 애플리케이션이 적어도 포함 조건 중 하나 이상 일치할 경우 해당 애플리케이션에 규칙을 적용합니다.

- *예외 조건*. Kaspersky Endpoint Security는 애플리케이션이 적어도 예외 조건 중 하나 이상 일치하고 포함 조건과 일치하지 않을 경우 해당 애플리케이션에 규칙을 적용하지 않습니다.

규칙 시작 조건은 기준을 사용해 생성됩니다. Kaspersky Endpoint Security에서 규칙을 생성하기 위해 다음 기준이 사용됩니다:

- 애플리케이션의 실행 파일이 포함된 폴더 경로 또는 애플리케이션 실행 파일의 경로.

- 메타데이터: 애플리케이션 실행 파일 이름, 애플리케이션 실행 파일 버전, 애플리케이션 이름, 애플리케이션 버전, 애플리케이션 공급 업체.

- 애플리케이션의 실행 파일 해시입니다.

- 인증서: 발급자, 주체, 손도장.

- KL 카테고리 애플리케이션의 포함 조건.

- 이동식 드라이브에 있는 애플리케이션 실행 파일의 위치.

조건에 사용된 각 기준에 대해 기준 값을 지정해야 합니다. 만일 시작되는 애플리케이션의 변수가 포함 조건에서 지정된 기준 값과 일치한다면, 규칙은 적용됩니다. 이 경우 애플리케이션 제어는 규칙에서 지정된 동작을 수행합니다. 애플리케이션 파라미터가 예외 조건에 지정된 기준 값과 일치하는 경우 애플리케이션 제어가 애플리케이션 시작을 제어하지 않습니다.

규칙 트리거 조건으로 인증서를 선택했다면, 이 인증서가 컴퓨터의 신뢰할 수 있는 시스템 저장소에 추가되었는지 확인하고 애플리케이션의 신뢰할 수 있는 시스템 스토리지 사용 설정을 확인합니다.

규칙이 작동할 때 애플리케이션 제어 구성 요소의 결정

규칙이 시작될 때, 애플리케이션 제어는 규칙에 따라 사용자(사용자 그룹)가 애플리케이션을 시작 또는 차단할 수 있도록 허용합니다. 규칙을 시작하는 애플리케이션의 시작을 허용하거나 허용되지 않는 개별 사용자 또는 사용자 그룹을 선택할 수 있습니다.

만일 규칙을 만족하는 애플리케이션을 시작할 수 있는 사용자를 지정하지 않는 규칙은 *차단* 규칙이라고 합니다.

만일 규칙과 일치하는 애플리케이션을 시작할 수 없는 사용자를 지정하지 않는 규칙은 *허용* 규칙입니다.

차단 규칙이 허용 규칙보다 우선합니다. 예를 들어, 특정 사용자 그룹에 대해 애플리케이션 제어 허용 규칙을 할당했지만 해당 사용자 그룹의 한 구성원에 대해 애플리케이션 제어 차단 규칙을 할당한 경우 이 사용자는 애플리케이션을 시작하지 못합니다.

규칙의 작동 상태

애플리케이션 제어 규칙은 다음 작동 상태 중 하나로 지정됩니다:

- **사용**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 사용되고 있음을 나타냅니다.
- **사용 안 함**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 무시되고 있음을 나타냅니다.
- **테스트 모드**. 이 상태는 Kaspersky Endpoint Security가 애플리케이션의 시작을 허용하며, 규칙이 적용되지만 그러한 애플리케이션의 시작에 관한 정보가 리포트에 기록된다는 것을 의미합니다.

애플리케이션 제어 규칙의 트리거 조건 추가

애플리케이션 제어 규칙을 생성할 때 애플리케이션 카테고리를 함께 생성하면 편리합니다.

회사에서 사용되는 표준 애플리케이션 조합에 대한 "업무 애플리케이션" 카테고리를 만드는 것이 좋습니다. 사용자 그룹에 따라 사용하는 애플리케이션 조합이 달라질 경우 각 사용자 그룹에 대해 별도의 애플리케이션 카테고리를 만들 수 있습니다.

관리 콘솔에서 애플리케이션 카테고리를 생성하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리에서 **고급 → 애플리케이션 관리 → 애플리케이션 카테고리**를 선택합니다.

3. 작업 공간에서 **새 카테고리** 버튼을 누릅니다.
   사용자 카테고리 생성 마법사가 시작됩니다.

4. 사용자 카테고리 생성 마법사의 안내를 따릅니다.

1단계. 카테고리 유형 선택

이 단계에서는 다음 유형의 애플리케이션 카테고리 중 하나를 선택합니다:

- 수동으로 추가한 컨텐츠가 있는 카테고리. 실행 파일의 데이터가 카테고리에 직접 추가됩니다. 이 유형의 카테고리를 선택하면 *카테고리의 애플리케이션을 포함하는 조건 구성* 단계와 *카테고리에서 애플리케이션을 예외할 조건 구성* 단계에서 카테고리에 실행 파일을 포함할 기준을 정의할 수 있습니다.

- 선택한 장치의 실행 파일이 포함된 카테고리. 이러한 실행 파일은 자동 처리되고 해당 지표도 카테고리에 추가됩니다. 이 유형의 카테고리를 선택하면 *설정* 단계에서 카테고리에 자동 포함할 실행 파일이 들어 있는 컴퓨터를 지정할 수 있습니다.

- 지정한 폴더의 실행 파일을 포함하는 카테고리. 지정한 폴더에 복사한 애플리케이션의 실행 파일이 자동 처리되고 해당 지표도 카테고리에 추가됩니다. 이 유형의 카테고리를 선택하면 *저장소 폴더* 단계에서 카테고리에 자동 포함할 실행 파일이 들어 있는 폴더를 지정할 수 있습니다.

컨텐츠가 자동으로 추가된 카테고리를 생성할 때 Kaspersky Security Center는 다음 형식의 파일에 인벤토리를 수행합니다: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX 및 SCR.

2단계. 사용자 카테고리 이름 입력

이 단계에서는 애플리케이션 카테고리의 이름을 지정합니다.

3단계. 카테고리에 애플리케이션을 포함하는 조건 구성

애플리케이션 제어 규칙에 조건(파일 해시 등)을 다수 추가하면 컴퓨터 리소스 소모가 증가합니다. 조건의 총 수가 50,000개에 도달하면 성능 문제가 발생할 수 있습니다. 성능을 최적화하려면 조건을 검토하여 조건 수를 줄이는 것이 좋습니다.

이 단계는 **수동으로 추가한 컨텐츠가 있는 카테고리** 유형을 선택한 경우에 수행할 수 있습니다.

이 단계에서는 **추가** 드롭다운 목록에서 애플리케이션을 카테고리에 포함하기 위한 조건을 선택합니다.

- **실행 파일 목록에서**. 클라이언트 장치의 실행 파일 목록에 있는 애플리케이션을 사용자 지정 카테고리에 추가합니다.
- **시작 파일 속성**. 실행 파일의 상세 데이터를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 지정합니다.
- **폴더 내 파일의 메타데이터**. 실행 파일이 포함된 클라이언트 장치의 폴더를 선택합니다. Kaspersky Security Center는 이러한 실행 파일의 메타데이터를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.
- **폴더 내 파일의 체크섬**. 실행 파일이 포함된 클라이언트 장치의 폴더를 선택합니다. Kaspersky Security Center는 이러한 실행 파일의 해시를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.
- **폴더의 파일에 대한 인증서**. 인증서로 서명된 실행 파일이 포함된 클라이언트 장치의 폴더를 선택합니다. Kaspersky Security Center는 이러한 실행 파일의 인증서를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.

  속성에 지정된 **인증서 지문** 파라미터가 없는 조건은 사용하지 않는 것이 좋습니다.

- **MSI 인스톨러 파일 메타데이터**. MSI 패키지를 선택합니다. Kaspersky Security Center는 이 MSI 패키지에 압축된 실행 파일의 메타데이터를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.
- **애플리케이션 MSI 인스톨러의 파일 체크섬**. MSI 패키지를 선택합니다. Kaspersky Security Center는 이 패키지에 압축된 실행 파일의 해시를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.
- **KL 카테고리에서**. KL 카테고리를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 지정합니다. *KL 카테고리*는 테마 특성을 공유하는 애플리케이션의 목록 입니다. 이 목록은 Kaspersky 전문가에 의해 유지 관리됩니다. 예를 들어, *오피스 애플리케이션*의 KL 카테고리에는 Microsoft Office 제품군, Adobe Acrobat 등이 포함됩니다.

  모든 KL 카테고리를 선택하여 신뢰하는 애플리케이션의 확장 목록을 생성할 수 있습니다.

- **애플리케이션 경로 지정(마스크 지원)**. 클라이언트 장치의 폴더를 선택합니다. Kaspersky Security Center는 사용자 지정 카테고리에 이 폴더의 실행 파일을 추가합니다.
- **저장소에서 인증서 선택**. 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 실행 파일에 서명을 하는 데 사용된 인증서를 선택합니다.

  속성에 지정된 **인증서 지문** 파라미터가 없는 조건은 사용하지 않는 것이 좋습니다.

  인증서 저장소를 선택할 수 있습니다. 기본적으로 애플리케이션 제어는 신뢰하는 시스템 인증서 스토어의 인증서로 서명된 애플리케이션에 대해서만 규칙을 적용합니다. 이 기능은 **엄격한 디지털 서명 인증 사용** 확인란을 통해 활성화됩니다.

- **드라이브 유형**. 저장소 장치 유형(모든 하드 드라이브와 이동식 드라이브 또는 이동식 드라이브만)을 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 지정합니다.

4단계. 카테고리에서 애플리케이션을 제외하는 조건 구성

이 단계는 **수동으로 추가한 컨텐츠가 있는 카테고리** 유형을 선택한 경우에 수행할 수 있습니다.

이 단계에서 지정한 애플리케이션은 "애플리케이션을 특정 카테고리에 포함하기 위한 조건 구성" 단계에서 이미 지정했다 하더라도 카테고리에서 제외됩니다.

이 단계에서는 **추가** 드롭다운 목록에서 애플리케이션을 카테고리에서 제외하기 위한 조건을 선택합니다.

- **실행 파일 목록에서**. 클라이언트 장치의 실행 파일 목록에 있는 애플리케이션을 사용자 지정 카테고리에 추가합니다.
- **시작 파일 속성**. 실행 파일의 상세 데이터를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 지정합니다.
- **폴더 내 파일의 메타데이터**. 실행 파일이 포함된 클라이언트 장치의 폴더를 선택합니다. Kaspersky Security Center는 이러한 실행 파일의 메타데이터를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.
- **폴더 내 파일의 체크섬**. 실행 파일이 포함된 클라이언트 장치의 폴더를 선택합니다. Kaspersky Security Center는 이러한 실행 파일의 해시를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.
- **폴더의 파일에 대한 인증서**. 인증서로 서명된 실행 파일이 포함된 클라이언트 장치의 폴더를 선택합니다. Kaspersky Security Center는 이러한 실행 파일의 인증서를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.
- **MSI 인스톨러 파일 메타데이터**. MSI 패키지를 선택합니다. Kaspersky Security Center는 이 MSI 패키지에 압축된 실행 파일의 메타데이터를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.
- **애플리케이션 MSI 인스톨러의 파일 체크섬**. MSI 패키지를 선택합니다. Kaspersky Security Center는 이 패키지에 압축된 실행 파일의 해시를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 표시합니다.
- **KL 카테고리에서**. KL 카테고리를 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 지정합니다. *KL 카테고리*는 테마 특성을 공유하는 애플리케이션의 목록 입니다. 이 목록은 Kaspersky 전문가에 의해 유지 관리됩니다. 예를 들어, *오피스 애플리케이션*의 KL 카테고리에는 Microsoft Office 제품군, Adobe Acrobat 등이 포함됩니다.

  모든 KL 카테고리를 선택하여 신뢰하는 애플리케이션의 확장 목록을 생성할 수 있습니다.
- **애플리케이션 경로 지정(마스크 지원)**. 클라이언트 장치의 폴더를 선택합니다. Kaspersky Security Center는 사용자 지정 카테고리에 이 폴더의 실행 파일을 추가합니다.
- **저장소에서 인증서 선택**. 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 실행 파일에 서명을 하는 데 사용된 인증서를 선택합니다.
- **드라이브 유형**. 저장소 장치 유형(모든 하드 드라이브와 이동식 드라이브 또는 이동식 드라이브만)을 사용자 지정 카테고리에 애플리케이션을 추가하는 조건으로 지정합니다.

5단계. 설정

이 단계는 **선택한 장치의 실행 파일이 포함된 카테고리** 유형을 선택한 경우에 수행할 수 있습니다.

이 단계에서는 **추가** 버튼을 누르고 Kaspersky Security Center가 애플리케이션 카테고리에 추가할 실행 파일이 있는 컴퓨터를 지정합니다. Kaspersky Security Center는 **실행 파일** 폴더에 표시된 지정된 컴퓨터의 모든 실행 파일을 애플리케이션 카테고리에 추가합니다.

또한 이 단계에서 다음 설정을 구성할 수 있습니다:

- 해시 함수 계산을 위한 알고리즘. 알고리즘을 선택하려면 다음 확인란 중 하나를 선택해야 합니다.
  - **이 카테고리의 파일에 대해 SHA256 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원)**.
  - **이 카테고리의 파일에 대해 MD5 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 서비스 팩 2 이전 버전에서 지원)**.
- **중앙 관리 서버 저장소와 데이터 동기화** 확인란. Kaspersky Security Center가 애플리케이션 카테고리를 정기적으로 지우고 **실행 파일** 폴더에 표시된 특정 컴퓨터의 모든 실행 파일을 추가하도록 하려면 이 확인란을 선택합니다.

  중앙 관리 서버 저장소와 데이터 동기화 확인란 선택을 취소하면 Kaspersky Security Center는 생성된 애플리케이션 카테고리를 수정하지 않습니다.

6단계. 저장소 폴더

이 단계는 **지정한 폴더의 실행 파일을 포함하는 카테고리** 유형을 선택한 경우에 수행할 수 있습니다.

이 단계에서는 Kaspersky Security Center가 애플리케이션 카테고리에 자동으로 추가할 실행 파일을 검색할 폴더를 지정합니다.

또한 이 단계에서 다음 설정을 구성할 수 있습니다:

- **이 카테고리에 동적 링크 라이브러리(DLL) 포함** 확인란. 애플리케이션 카테고리에 DLL(동적 링크 라이브러리)을 포함하려면 이 확인란을 선택합니다.

  애플리케이션 카테고리에 DLL 파일을 포함하면 Kaspersky Security Center의 성능이 저하될 수 있습니다.

- **이 카테고리에 스크립트 데이터 포함** 확인란. 애플리케이션 카테고리에 스크립트를 포함하려면 이 확인란을 선택합니다.

  애플리케이션 카테고리에 스크립트를 포함하면 Kaspersky Security Center의 성능이 저하될 수 있습니다.

- 해시 함수 계산을 위한 알고리즘. 알고리즘을 선택하려면 다음 확인란 중 하나를 선택해야 합니다.
  - **이 카테고리의 파일에 대해 SHA256 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원)**.
  - **이 카테고리의 파일에 대해 MD5 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 서비스 팩 2 이전 버전에서 지원)**.
- **폴더 내 변경 사항을 강제로 검사** 확인란. Kaspersky Security Center가 애플리케이션 카테고리에 자동으로 추가하는 데 사용된 폴더에서 실행 파일을 정기적으로 검색하도록 하려면 이 확인란을 선택합니다.

  폴더 내 변경 사항을 강제로 검사 확인란을 선택 해제하면 Kaspersky Security Center는 폴더가 변경되었거나 해당 폴더에서 파일이 추가 또는 삭제된 경우에만 애플리케이션 카테고리에 자동으로 추가하는 데 사용된 폴더에서 실행 파일을 검색합니다.
- **검사 간격(1~168시간)** 필드. 이 필드에서 지정한 시간 간격(단위: 시간)에 따라 Kaspersky Security Center가 애플리케이션 카테고리에 자동으로 추가하는 데 사용되는 폴더에서 실행 파일을 검색합니다.

  이 필드는 **폴더 내 변경 사항을 강제로 검사** 확인란을 선택한 경우에만 활성화됩니다.

7단계. 사용자 지정 카테고리 생성

마법사를 끝냅니다.

애플리케이션 인터페이스에서 애플리케이션 제어 규칙 트리거 조건을 추가하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **애플리케이션 제어**를 선택합니다.
3. **차단된 애플리케이션** 또는 **허용된 애플리케이션** 버튼을 클릭합니다.

   애플리케이션 제어 규칙 목록이 열립니다.
4. 트리거 조건을 구성할 규칙을 선택합니다.

   애플리케이션 제어 규칙 속성이 열립니다.
5. **조건: N** 탭 또는 **예외 규칙: N** 탭을 선택하고 **추가** 버튼을 클릭합니다.
6. 애플리케이션 제어 규칙의 트리거 조건을 선택합니다:
   - **시작된 애플리케이션 속성의 조건**. 실행 중인 애플리케이션 목록에서 애플리케이션 제어 규칙을 적용할 애플리케이션을 선택할 수 있습니다. Kaspersky Endpoint Security는 이전에 컴퓨터에서 실행했던 애플리케이션도 표시합니다. **파일 해시**, **인증서**, **KL 카테고리**, **메타 데이터**, **파일 또는 폴더 경로** 등, 규칙 트리거 조건을 하나 이상 생성할 때 사용할 기준을 선택해야 합니다.
   - **"KL 카테고리" 조건**. *KL 카테고리*는 테마 특성을 공유하는 애플리케이션의 목록 입니다. 이 목록은 Kaspersky 전문가에 의해 유지 관리됩니다. 예를 들어, "오피스 애플리케이션"의 KL 카테고리에는 Microsoft Office 제품군, Adobe® Acrobat® 등이 포함됩니다.
   - **사용자 지정 조건**. 애플리케이션 파일을 선택하고 **파일 해시**, **인증서**, **메타 데이터**, **파일 또는 폴더 경로** 등의 규칙 트리거 조건 중 하나를 선택할 수 있습니다.

- **파일 드라이브별 조건(이동식 드라이브)**. 애플리케이션 제어 규칙은 이동식 드라이브에서 실행하는 파일에만 적용됩니다.

- **지정된 폴더에 있는 파일 속성의 조건**. 애플리케이션 제어 규칙은 지정한 폴더 내의 파일에만 적용됩니다. 하위 폴더의 파일을 포함하거나 제외할 수도 있습니다. **파일 해시**, **인증서**, **KL 카테고리**, **메타 데이터**, **파일 또는 폴더 경로** 등, 규칙 트리거 조건을 하나 이상 생성할 때 사용할 기준을 선택해야 합니다.

7. 변경 사항을 저장합니다.

조건을 추가할 때 애플리케이션 제어에 대해 다음과 같이 특별히 고려해야 할 사항도 확인하십시오:

- Kaspersky Endpoint Security는 **파일 이름**, **애플리케이션 이름**, **공급사** 메타데이터에 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.

- Kaspersky Endpoint Security는 MD5 파일 해시 코드를 지원하지 않으므로 MD5 해시 기반의 애플리케이션 시작을 제어하지 않습니다. 대신 SHA256 해시가 규칙 트리거 조건으로 사용됩니다.

- **발급 기관** 및 **인증서 주체** 기준만을 규칙 트리거 조건으로 사용하는 것은 권장되지 않습니다. 이러한 기준 사용을 신뢰할 수 없습니다.

- **파일 또는 폴더 경로** 필드에 심볼릭 링크를 사용하는 경우 애플리케이션 제어 규칙이 제대로 작동하려면 심볼릭 링크의 주소를 변환하는 것이 좋습니다. 그러려면 **기호 링크 해결** 버튼을 누릅니다.

실행 파일 폴더에서 애플리케이션 카테고리로 실행 파일 추가

실행 파일 폴더에 컴퓨터에서 탐지된 실행 파일 목록이 표시됩니다. Kaspersky Endpoint Security는 인벤토리 작업을 실행한 후에 실행 파일 목록을 생성합니다.

실행 파일 폴더에서 애플리케이션 카테고리로 실행 파일을 추가하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 관리 콘솔 트리에서 **고급 → 애플리케이션 관리 → 실행 파일**을 선택합니다.

3. 작업 영역에서 애플리케이션 카테고리에 추가할 실행 파일을 선택합니다.

4. 선택한 실행 파일에 대해 마우스 오른쪽 메뉴를 누르고 **카테고리에 추가**를 선택합니다.

5. 창이 열리면 다음을 수행합니다.

   - 창 위쪽에서 다음 옵션 중 하나를 선택합니다:

     - **새 애플리케이션 카테고리에 추가**. 새 애플리케이션 카테고리를 생성하고 실행 파일을 추가하려면 이 옵션을 선택하십시오.

     - **기존 애플리케이션 카테고리에 추가**. 기존 애플리케이션 카테고리를 선택하고 실행 파일을 추가하려면 이 옵션을 선택하십시오.

   - **규칙 유형** 블록에서 다음 옵션 중 하나를 선택합니다:

     - **포함 추가 규칙**. 실행 파일을 애플리케이션 카테고리에 추가하는 조건을 만들려면 이 옵션을 선택합니다.

     - **제외 추가 규칙**. 실행 파일을 애플리케이션 카테고리에서 제외하는 조건을 만들려면 이 옵션을 선택합니다.

- **조건으로 사용할 파라미터** 블록에서 다음 옵션 중 하나를 선택합니다:
  - **인증서 세부 정보(또는 인증서가 없는 파일에 대한 SHA256 해시 값)**.
  - **인증서 세부 정보(인증서가 없는 파일은 건너뜀)**.
  - **SHA256만(해시가 없는 파일은 건너뜀)**.
  - **MD5만(Kaspersky Endpoint Security 10 Service Pack 1 for Windows 이전의 버전에서 지원)**.

6. 변경 사항을 저장합니다.

애플리케이션 카테고리에 이벤트 관련 실행 파일 추가

애플리케이션 제어 이벤트와 관련된 실행 파일을 애플리케이션 카테고리에 추가하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **중앙 관리 서버** 노드에서 **이벤트** 탭을 선택합니다.
3. **이벤트 선택** 드롭다운 목록에서 애플리케이션 제어 구성 요소의 작동과 관련된 이벤트 조회를 선택합니다(애플리케이션 제어 구성 요소의 동작에서 이벤트 결과 보기, 애플리케이션 제어 구성 요소의 테스트 동작에서의 이벤트 결과 보기).
4. **선택 실행** 버튼을 누릅니다.
5. 애플리케이션 카테고리에 추가할 실행 파일과 연관된 이벤트를 선택합니다.
6. 마우스 오른쪽 메뉴를 누르고 **카테고리에 추가**를 선택합니다.
7. 창이 열리면 애플리케이션 카테고리의 설정을 구성합니다.
   - 창 위쪽에서 다음 옵션 중 하나를 선택합니다:
     - **새 애플리케이션 카테고리에 추가**. 새 애플리케이션 카테고리를 생성하고 실행 파일을 추가하려면 이 옵션을 선택하십시오.
     - **기존 애플리케이션 카테고리에 추가**. 기존 애플리케이션 카테고리를 선택하고 실행 파일을 추가하려면 이 옵션을 선택하십시오.
   - **규칙 유형** 블록에서 다음 옵션 중 하나를 선택합니다:
     - **포함 추가 규칙**. 실행 파일을 애플리케이션 카테고리에 추가하는 조건을 만들려면 이 옵션을 선택합니다.
     - **제외 추가 규칙**. 실행 파일을 애플리케이션 카테고리에서 제외하는 조건을 만들려면 이 옵션을 선택합니다.
   - **조건으로 사용할 파라미터** 블록에서 다음 옵션 중 하나를 선택합니다:
     - **인증서 세부 정보(또는 인증서가 없는 파일에 대한 SHA-256 해시 값)**.
     - **인증서 세부 정보(인증서가 없는 파일은 건너뜀)**.

- **SHA-256만(해시가 없는 파일은 건너뜀)**.
- **MD5만(Kaspersky Endpoint Security 10 Service Pack 1 for Windows 이전의 버전에서 지원)**.

8. 변경 사항을 저장합니다.

애플리케이션 제어 규칙 추가

Kaspersky Security Center를 사용해 애플리케이션 제어 규칙을 추가하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보안 제어 → 애플리케이션 제어**를 선택합니다.
   창 오른쪽에 애플리케이션 제어 구성 요소의 설정이 표시됩니다.
4. **추가**를 클릭합니다.
   애플리케이션 제어 규칙 창이 열립니다.
5. 다음 중 하나를 수행합니다:
   - 새 카테고리를 만들려면 다음과 같이 하십시오.
     a. **카테고리 만들기**를 클릭합니다.
        사용자 카테고리 생성 마법사가 시작됩니다.
     b. 사용자 카테고리 생성 마법사의 안내를 따릅니다.
     c. **카테고리** 드롭다운 목록에서 생성된 애플리케이션 카테고리를 선택합니다.
   - 기존 카테고리를 편집하려면 다음과 같이 하십시오.
     a. **카테고리** 드롭다운 목록에서 편집하려는 생성된 애플리케이션 카테고리를 선택합니다.
     b. **속성**을 클릭합니다.
     c. 선택한 애플리케이션 카테고리의 설정을 수정합니다.
     d. 변경 사항을 저장합니다.
     e. **카테고리** 드롭다운 목록에서 규칙을 만들 때 기준으로 사용하도록 만든 애플리케이션 카테고리를 선택합니다.
6. **사용자 및 권한** 표에서 **추가** 버튼을 누릅니다.
   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. **사용자 및 권한** 표에서 다음을 수행합니다:

   - 사용자 또는 사용자 그룹이 선택한 카테고리에 속한 애플리케이션을 시작하도록 허용하려면 해당 열의 **허용** 확인란을 선택합니다.
   - 사용자 또는 사용자 그룹이 선택한 카테고리에 속한 애플리케이션을 시작하지 못하게 차단하려면 해당 열의 **차단** 확인란을 선택합니다.

8. **사용자/그룹** 열에 표시되지 않고 **사용자/그룹** 열에 지정된 사용자 그룹에 속하지 않은 모든 사용자가 선택한 카테고리에 속한 애플리케이션을 시작하지 못하게 차단하려면 **다른 사용자 거부** 확인란을 선택합니다.

9. Kaspersky Endpoint Security가 선택한 애플리케이션 카테고리에 포함된 애플리케이션을 신뢰하는 업데이터로 간주하여 이후 실행될 다른 실행 파일을 생성하도록 허용하려면 **신뢰하는 업데이터** 확인란을 선택합니다.

   Kaspersky Endpoint Security 설정을 마이그레이션하면 신뢰하는 업데이터가 생성한 실행 파일 목록도 마이그레이션됩니다.

10. 변경 사항을 저장합니다.

애플리케이션 제어 규칙을 추가하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **애플리케이션 제어**를 선택합니다.
3. **차단된 애플리케이션** 또는 **허용된 애플리케이션** 버튼을 클릭합니다.
   애플리케이션 제어 규칙 목록이 열립니다.
4. **추가**를 클릭합니다.
   애플리케이션 제어 규칙 설정 창이 열립니다.
5. **일반 설정** 탭에서 규칙의 기본 설정을 정의합니다:
   a. **규칙 이름** 필드에서 규칙의 이름을 입력합니다.
   b. **설명** 필드에 규칙의 설명을 입력합니다.
   c. **사용자 및 권한** 표에서 **추가** 버튼을 누릅니다.
      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.
      기본적으로 모든 사용자에게 규칙이 적용됩니다.

      표에서 사용자를 지정하지 않으면 규칙을 저장할 수 없습니다.

   d. **사용자 및 권한** 테이블에서 토글로 애플리케이션을 시작할 사용자의 권한을 정의합니다.

e. 애플리케이션이 **사용자 및 권한** 표에 포함되지 않고 **사용자 및 권한** 표에 포함된 사용자 그룹의 일원도 아닌 모든 사용자를 대상으로 실행되는 규칙 트리거 조건을 만족하는 애플리케이션을 방지하도록 하려면 **다른 사용자 거부** 확인란을 선택합니다.

> **다른 사용자 거부** 확인란을 선택 해제하면 Kaspersky Endpoint Security가 **사용자 및 권한** 표에 지정되지 않거나 **사용자 및 권한** 표에 지정된 사용자 그룹에 속하지 않은 사용자의 애플리케이션 시작을 제어하지 않습니다.

f. Kaspersky Endpoint Security가 규칙 트리거 조건과 일치하는 애플리케이션을 신뢰할 수 있는 업데이트로 간주하도록 하려면 **신뢰하는 업데이터** 확인란을 선택합니다. *신뢰하는 업데이터*는 이후에 실행할 수 있는 다른 실행 파일을 생성할 수 있는 애플리케이션입니다.

애플리케이션이 여러 규칙을 트리거한다면, Kaspersky Endpoint Security는 다음 조건 충족 시에 *신뢰하는 업데이터* 플래그를 설정합니다.

- 모든 규칙은 애플리케이션 실행을 허용합니다.
- 적어도 하나의 규칙에는 **신뢰하는 업데이터** 확인란이 선택되어 있습니다.

6. **조건: N** 탭에서 규칙을 트리거할 포함 조건 목록을 생성하거나 편집합니다.
7. **예외 규칙: N** 탭에서 규칙을 트리거할 예외 조건 목록을 생성하거나 편집합니다.

Kaspersky Endpoint Security 설정을 마이그레이션하면 신뢰하는 업데이터가 생성한 실행 파일 목록도 마이그레이션됩니다.

8. 변경 사항을 저장합니다.

Kaspersky Security Center를 사용해 애플리케이션 제어 규칙의 상태 변경

관리 콘솔에서 애플리케이션 제어 규칙의 상태를 변경하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보안 제어 → 애플리케이션 제어**를 선택합니다.

창 오른쪽에 애플리케이션 제어 구성 요소의 설정이 표시됩니다.

4. **상태** 열에서 왼쪽 버튼을 클릭하여 마우스 오른쪽 메뉴를 표시하고 다음 중 하나를 선택하십시오.
   - **켜짐**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 사용되고 있음을 나타냅니다.
   - **꺼짐**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 무시되고 있음을 나타냅니다.
   - **테스트**. 이 상태는 Kaspersky Endpoint Security가 애플리케이션의 시작을 항상 허용하며, 규칙이 적용되지만 그러한 애플리케이션의 시작에 관한 정보가 리포트에 기록된다는 것을 의미합니다.
5. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 애플리케이션 제어 규칙의 상태를 변경하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **애플리케이션 제어**를 선택합니다.
3. **차단된 애플리케이션** 또는 **허용된 애플리케이션** 버튼을 클릭합니다.
   애플리케이션 제어 규칙 목록이 열립니다.
4. **상태** 열에서 마우스 오른쪽 메뉴를 열고 다음 중 하나를 선택합니다.
   - **사용**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 사용되고 있음을 나타냅니다.
   - **사용 안 함**. 이 상태는 애플리케이션 제어 구성 요소가 실행 중일 때 규칙이 무시되고 있음을 나타냅니다.
   - **테스트 모드**. 이 상태는 Kaspersky Endpoint Security가 애플리케이션의 시작을 항상 허용하며, 이 규칙이 적용되지만 그러한 애플리케이션의 시작에 관한 정보가 리포트에 기록된다는 것을 의미합니다.
5. 변경 사항을 저장합니다.

애플리케이션 제어 규칙 내보내기 및 가져오기

애플리케이션 제어 규칙 목록을 XML 파일로 내보낼 수 있습니다. 내보내기/가져오기 기능을 사용하여 애플리케이션 제어 규칙 목록을 백업하거나 목록을 다른 서버로 마이그레이션할 수 있습니다.

애플리케이션 제어 규칙을 가져오고 내보낼 때는 다음 사항을 특별히 고려해주십시오:

- Kaspersky Endpoint Security는 활성화된 애플리케이션 제어 모드의 규칙 목록만을 내보냅니다. 즉, 애플리케이션 제어가 거부 목록 모드에서 동작 중이라면 Kaspersky Endpoint Security는 이 모드에 대한 규칙만을 내보냅니다. 허용 목록 모드의 규칙 목록을 내보내려면 모드를 전환한 후 내보내기 동작을 다시 실행해야 합니다.
- Kaspersky Endpoint Security는 애플리케이션 제어 규칙에 대해 애플리케이션 카테고리를 사용합니다. 애플리케이션 제어 규칙 목록을 다른 서버로 마이그레이션할 때는 애플리케이션 카테고리 목록도 함께 마이그레이션해야 합니다. 애플리케이션 카테고리 내보내기 및 가져오기에 대한 자세한 정보는 Kaspersky Security Center 도움말을 참조하십시오.

관리 콘솔(MMC)에서 애플리케이션 제어 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 창에서 **보안 제어** → **애플리케이션 제어**를 선택합니다.
4. 애플리케이션 제어 규칙 목록을 내보내려면 다음을 수행합니다.
   a. 내보낼 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
      규칙을 선택하지 않으면 Kaspersky Endpoint Security는 모든 규칙을 내 보냅니다.
   b. **내보내기** 링크를 클릭합니다.
   c. 창이 열리면 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

d. 파일을 저장합니다.

Kaspersky Endpoint Security는 신뢰하는 규칙 목록을 XML 파일로 내보냅니다.

5. 애플리케이션 제어 규칙 목록을 가져오려면 다음을 수행합니다.

a. **가져오기** 링크를 클릭합니다.

창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.

b. 파일을 엽니다.

컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 애플리케이션 제어 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어** → **앱 제어**로 이동합니다.

5. **운영 모드**에서 규칙 목록(애플리케이션 거부 목록 또는 허용 목록)을 선택합니다.

6. 규칙 목록을 내보내려면 다음을 수행합니다.

a. 내보낼 규칙을 선택합니다.

b. → **내보내기** 버튼을 클릭합니다.

Kaspersky Endpoint Security는 규칙 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.

7. 규칙 목록을 가져오려면 다음을 수행합니다.

a. → **가져오기** 버튼을 클릭합니다.

창이 열리면 규칙 목록을 가져올 JSON 파일을 선택합니다.

b. 파일을 엽니다.

컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. 변경 사항을 저장합니다.

애플리케이션 제어 구성 요소의 동작에서 이벤트 결과 보기

Kaspersky Security Center에서 수신한 애플리케이션 제어 구성 요소 작동 이벤트를 보려면 다음과 같이 진행합니다:

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **중앙 관리 서버** 노드에서 **이벤트** 탭을 선택합니다.
3. **새 선택 항목 생성** 버튼을 누릅니다.
4. 창이 열리면 **이벤트** 섹션으로 이동합니다.
5. **모두 지우기** 버튼을 누릅니다.
6. **이벤트** 표에서 **애플리케이션 시작이 금지됨** 확인란을 선택합니다.
7. 변경 사항을 저장합니다.
8. **이벤트 선택** 드롭다운 목록에서 생성된 조회 항목을 선택합니다.
9. **선택 실행** 버튼을 누릅니다.

차단된 애플리케이션 리포트 보기

차단된 애플리케이션 리포트를 보려면 다음과 같이 하십시오:

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **중앙 관리 서버** 노드에서 **리포트** 탭을 선택합니다.
3. **새 리포트 템플릿**을 클릭합니다.
   새 리포트 템플릿 마법사가 시작됩니다.
4. 리포트 템플릿 마법사의 안내를 따릅니다. **리포트 템플릿 유형 선택** 단계에서 **기타 → 금지한 애플리케이션 리포트**를 선택합니다.
   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.

애플리케이션 제어 규칙 테스트

애플리케이션 제어 규칙으로 작업에 필요한 애플리케이션이 차단되지 않도록 하려면, 애플리케이션 제어 규칙을 테스트 모드로 활성화한 후 새 규칙 생성 이후의 동작을 분석하는 것이 좋습니다. 애플리케이션 제어 규칙의 테스트 모드가 사용되면 Kaspersky Endpoint Security는 애플리케이션 제어로 시작이 금지된 애플리케이션을 차단하지는 않지만 중앙 관리 서버로 애플리케이션 시작에 대한 알림을 전송합니다.

애플리케이션 제어 규칙의 작동을 분석하려면 Kaspersky Security Center로 보고된 애플리케이션 제어 이벤트 결과를 검토해야 합니다. 테스트 모드의 운영 결과에서 컴퓨터 사용자의 작업에 필요한 모든 애플리케이션에 대해 차단된 시작 이벤트가 발생하지 않으면, 올바른 규칙이 만들어 졌음을 의미합니다. 그렇지 않으면, 작성한 규칙의 설정을 업데이트하거나, 추가 규칙을 생성하거나, 기존 규칙을 삭제하는 것이 좋습니다.

기본적으로 Kaspersky Endpoint Security는 규칙에 의해 차단된 애플리케이션을 제외한 모든 애플리케이션의 시작을 허용합니다.

애플리케이션 제어 규칙 테스트 활성화 및 비활성화

Kaspersky Security Center의 애플리케이션 제어 규칙 테스트를 사용하거나 사용하지 않으려면 다음과 같이 하십시오:

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보안 제어 → 애플리케이션 제어**를 선택합니다.
   창 오른쪽에 애플리케이션 제어 구성 요소의 설정이 표시됩니다.
4. **제어 모드** 드롭다운 목록에서 다음 항목 중 하나를 선택합니다:
   - **거부 목록**. 이 옵션을 선택하면 애플리케이션 제어 차단 규칙의 조건을 충족하는 경우를 제외하고는 애플리케이션 제어에서 모든 사용자가 모든 애플리케이션을 시작하도록 허용합니다.
   - **허용 목록**. 이 옵션을 선택하면 애플리케이션 제어 허용 규칙의 조건을 충족하는 경우를 제외하고는 애플리케이션 제어에서 모든 사용자가 모든 애플리케이션을 시작할 수 없도록 차단합니다.
5. 다음 중 하나를 수행합니다:
   - 애플리케이션 제어 규칙 테스트를 활성화하려면, **처리** 드롭다운 목록에서 **규칙 테스트** 옵션을 선택합니다.
   - 애플리케이션 제어를 활성화하여 사용자 컴퓨터의 애플리케이션 시작을 관리하려면 드롭다운 목록에서 **규칙 적용**을 선택합니다.
6. 변경 사항을 저장합니다.

애플리케이션 제어 규칙의 테스트 모드를 활성화하거나 애플리케이션 제어에 대한 차단 작업을 선택하려면 다음과 같이하십시오.

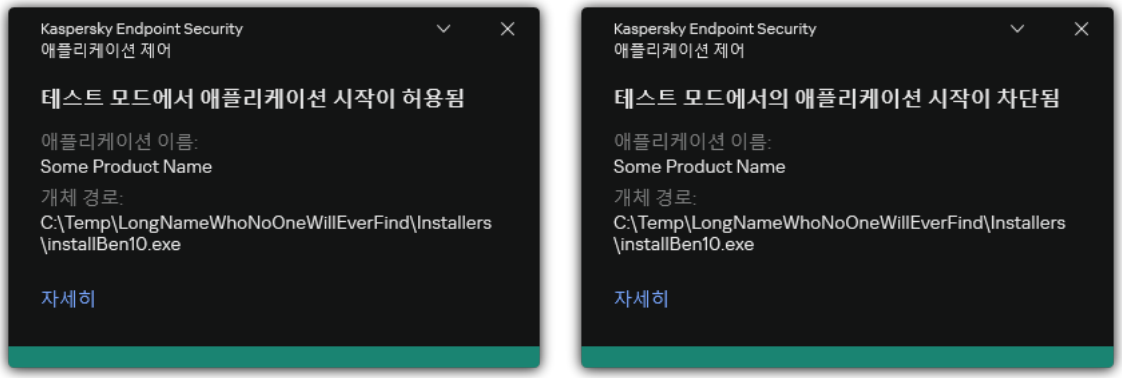
1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어 → 애플리케이션 제어**를 선택합니다.
3. **차단된 애플리케이션** 또는 **허용된 애플리케이션** 버튼을 클릭합니다.
   애플리케이션 제어 규칙 목록이 열립니다.

4. **상태** 열에서 **테스트 모드**를 선택합니다.

   이 상태는 Kaspersky Endpoint Security가 애플리케이션의 시작을 항상 허용하며, 이 규칙이 적용되지만 그러한 애플리케이션의 시작에 관한 정보가 리포트에 기록된다는 것을 의미합니다.

5. 변경 사항을 저장합니다.

Kaspersky Endpoint Security는 애플리케이션 제어 구성 요소로 시작이 금지된 애플리케이션을 차단하지는 않지만 중앙 관리 서버로 애플리케이션 시작에 대한 알림을 전송합니다. 사용자 컴퓨터에서 규칙 테스트에 대한 알림 표시를 구성할 수도 있습니다(아래 그림 참조).



테스트 모드의 애플리케이션 제어 알림

테스트 모드에서 차단된 애플리케이션 리포트 보기

테스트 모드에서 차단된 애플리케이션 리포트를 보려면 다음과 같이 하십시오:

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **중앙 관리 서버** 노드에서 **리포트** 탭을 선택합니다.
3. **새 리포트 템플릿**을 클릭합니다.

   새 리포트 템플릿 마법사가 시작됩니다.
4. 리포트 템플릿 마법사의 안내를 따릅니다. **리포트 템플릿 유형 선택** 단계에서 **기타 → 테스트 모드에서 운영된 금지한 애플리케이션 리포트**를 선택합니다.

   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.

애플리케이션 제어 구성 요소의 테스트 동작에서의 이벤트 결과 보기

Kaspersky Security Center에 수신되는 애플리케이션 제어 테스트 이벤트를 보려면 다음과 같이 하십시오:

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **중앙 관리 서버** 노드에서 **이벤트** 탭을 선택합니다.
3. **새 선택 항목 생성** 버튼을 누릅니다.

4. 창이 열리면 **이벤트** 섹션으로 이동합니다.

5. **모두 지우기** 버튼을 누릅니다.

6. **이벤트** 표에서 **테스트 모드에서의 애플리케이션 시작이 차단됨** 및 **테스트 모드에서 애플리케이션 시작이 허용됨** 확인란을 선택합니다.

7. 변경 사항을 저장합니다.

8. **이벤트 선택** 드롭다운 목록에서 생성된 조회 항목을 선택합니다.

9. **선택 실행** 버튼을 누릅니다.

애플리케이션 활동 모니터

이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

*애플리케이션 활동 모니터*는 사용자의 컴퓨터에서 애플리케이션 동작에 대한 정보를 실시간으로 확인하기 위해 개발된 도구입니다.

애플리케이션 활동 모니터를 사용하려면 애플리케이션 제어 및 호스트 침입 방지 구성 요소를 설치해야 합니다. 해당 구성 요소를 설치하지 않으면 기본 애플리케이션 창의 애플리케이션 활동 모니터 섹션이 숨겨져 있습니다.

애플리케이션 활동 모니터를 시작하려면 다음과 같이 하십시오.

메인 애플리케이션 창의 **모니터링** 섹션에서 **애플리케이션 활동 모니터** 타일을 클릭합니다.

창이 열리면 사용자 컴퓨터에서의 애플리케이션 동작에 대한 정보가 세 가지 탭으로 표시됩니다:

- **모든 애플리케이션** 탭은 컴퓨터에 설치된 모든 애플리케이션에 대한 정보를 표시합니다.
- **실행 중** 탭은 각 애플리케이션의 컴퓨터 리소스 소비에 대한 정보를 실시간으로 표시합니다. 이 탭에서 개별 애플리케이션에 대한 권한을 구성할 수도 있습니다.
- **시작 시 실행** 탭은 운영 체제 시작 시 자동으로 시작된 애플리케이션 목록을 표시합니다.

애플리케이션 활동 모니터 도구에 대한 사용자 접근을 제한하여 사용자 컴퓨터에서 애플리케이션 활동 정보를 숨길 수 있습니다.

관리 콘솔(MMC)을 사용하여 애플리케이션 인터페이스에서 애플리케이션 활동 모니터를 숨기는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **일반 설정 → 인터페이스**를 선택합니다.

4. **애플리케이션 활동 모니터 섹션 숨기기** 확인란을 사용하여 도구에 대한 접근 권한을 부여하거나 철회합니다.

5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console을 사용하여 애플리케이션 인터페이스에서 애플리케이션 활동 모니터를 숨기는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **사용자 상호 작용**으로 갑니다.

5. **애플리케이션 활동 모니터 섹션 숨기기** 확인란을 사용하여 도구에 대한 접근 권한을 부여하거나 철회합니다.

6. 변경 사항을 저장합니다.

파일 또는 폴더에 대한 이름 마스크 생성 규칙

*파일 또는 폴더 이름의 마스크*는 공통 문자를 사용하여 폴더의 이름 또는 파일의 이름과 확장명을 표현합니다.

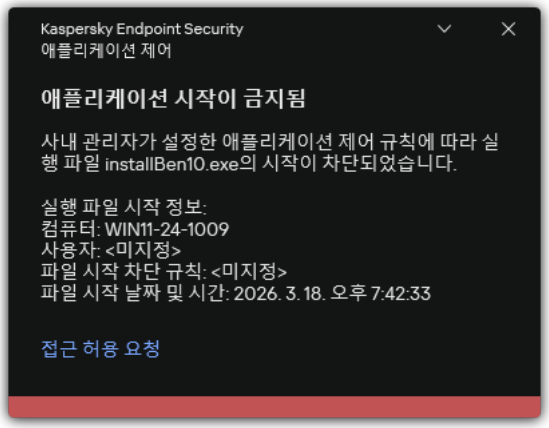
다음과 같은 공통 문자를 사용하여 파일 또는 폴더 이름 마스크를 만들 수 있습니다.

- `*`(별표) 문자는 모든 문자 세트를 나타낼 수 있습니다(공백 포함). 예를 들어 `C:\*.txt` 마스크에는 (C:) 드라이브의 폴더 및 하위 폴더에 있는 `txt` 확장자를 가진 파일에 대한 모든 경로가 포함됩니다.

- `?`(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.

애플리케이션 제어 메시지 템플릿 편집

사용자가 애플리케이션 제어 규칙에 의해 차단된 애플리케이션을 시작하려고 시도하는 경우 Kaspersky Endpoint Security는 해당 애플리케이션의 시작이 차단되었다는 메시지 상태를 표시합니다. Kaspersky 전문가는 사용자에게 애플리케이션이 차단된 이유를 설명하는 메시지 템플릿을 제공합니다(아래 그림 참조). 메시지 템플릿(예: %USER_NAME%)을 관리하기 위해 특수 변수가 제공됩니다. 변수를 사용하면 다른 컴퓨터에서 단일 메시지 템플릿을 사용할 수 있습니다. 메시지 생성 시 Kaspersky Endpoint Security는 운영 체제 설정에서 변수 값을 검색하여 특정 컴퓨터, 사용자 및 이벤트와 일치하는 메시지에 삽입합니다.



애플리케이션 제어 알림

사용자가 애플리케이션 시작이 잘못 차단되었다고 생각한다면, 사용자는 메시지 텍스트의 링크를 사용하여 메시지를 회사 네트워크 관리자에게 전송할 수 있습니다. 이렇게 하려면, 사용자는 **접근 허용 요청** 버튼을 누르고 관리자에게 상황을 설명하는 메시지를 보내야 합니다. 또한 관리자에게 보낼 메시지 템플릿을 준비하여 애플리케이션에 대한 접근을 허용할지 또는 차단할지 결정하는 데 도움이 되는 데이터를 추가할 수 있습니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 애플리케이션 시작 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다.

관리 콘솔(MMC)에서 애플리케이션 제어 메시지 템플릿을 편집하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보안 제어 → 애플리케이션 제어**를 선택합니다.
4. **메시지 템플릿 설정** 블록에서 **템플릿** 버튼을 클릭합니다.
5. 그러면 창이 열립니다. 이 창에서 애플리케이션 제어 템플릿을 구성합니다.

- **차단 관련 메시지**. 애플리케이션 시작을 차단하는 애플리케이션 제어 규칙이 작동될 때 표시되는 메시지의 템플릿.

  테스트 모드에서는 애플리케이션 제어에 대한 메시지 템플릿을 구성할 수 없습니다. 테스트 모드의 애플리케이션 제어는 사전 설정된 알림을 표시합니다.

- **관리자에게 메시지 보내기**. 사용자가 애플리케이션이 실수로 차단되었다고 생각하는 경우 회사 LAN 관리자에게 보낼 수 있는 메시지 템플릿입니다.

템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

기본적으로 버튼을 사용하여 기본 템플릿 텍스트를 복원할 수도 있습니다.

6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 애플리케이션 제어 메시지 템플릿을 편집하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **앱 제어**로 이동합니다.
5. **메시지 템플릿** 블록에서 **애플리케이션 시작 차단 관련 메시지** 링크를 클릭하고 애플리케이션 제어 메시지용 템플릿을 구성합니다.

   - **사용자에게 보내는 메시지**. 애플리케이션 시작을 차단하는 애플리케이션 제어 규칙이 작동될 때 표시되는 메시지의 템플릿.

     테스트 모드에서는 애플리케이션 제어에 대한 메시지 템플릿을 구성할 수 없습니다. 테스트 모드의 애플리케이션 제어는 사전 설정된 알림을 표시합니다.

   - **관리자에게 메시지 보내기**. 사용자가 애플리케이션이 실수로 차단되었다고 생각하는 경우 회사 LAN 관리자에게 보낼 수 있는 메시지 템플릿입니다.

   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수 추가**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

   기본값으로 재설정 버튼을 사용하여 기본 템플릿 텍스트를 복원할 수도 있습니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 애플리케이션 제어 메시지 템플릿을 편집하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **애플리케이션 제어**를 선택합니다.
3. **애플리케이션 차단에 관한 메시지 템플릿** 블록에서 애플리케이션 제어 메시지에 대한 템플릿을 구성합니다.

   - **차단 관련 메시지**. 애플리케이션 시작을 차단하는 애플리케이션 제어 규칙이 작동될 때 표시되는 메시지의 템플릿.

     테스트 모드에서는 애플리케이션 제어에 대한 메시지 템플릿을 구성할 수 없습니다. 테스트 모드의 애플리케이션 제어는 사전 설정된 알림을 표시합니다.

   - **관리자에게 메시지 보내기**. 사용자가 애플리케이션이 실수로 차단되었다고 생각하는 경우 회사 LAN 관리자에게 보낼 수 있는 메시지 템플릿입니다.

   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수 추가**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

초기화 버튼을 사용하여 기본 템플릿 텍스트를 복원할 수도 있습니다.

4. 변경 사항을 저장합니다.

애플리케이션 제어 메시지 템플릿 변수

사용자 메시지 템플릿 또는 관리자 메시지 템플릿에서 다음 변수를 사용할 수 있습니다.

- **트리거된 규칙의 이름** – `%RULE%`.
  파일 실행을 차단한 규칙의 이름입니다.
- **현재 날짜** – `%DATE%`.
  파일 실행이 차단된 날짜입니다(YYYY.MM.DD 형식).
- **현재 시간** – `%TIME%`.
  파일 실행이 차단된 시간입니다(HH:MM 형식).
- **사용자 이름** – `%USER_NAME%`.
  파일 실행이 차단된 컴퓨터의 현재 사용자 계정 이름으로, `<device name>\<user alias>` 형식으로 표시됩니다(예, `DESKTOP-123\John.Smith`).
- **컴퓨터 이름** – `%COMPUTER_NAME%`.
  파일 실행이 차단된 컴퓨터의 이름입니다.
- **실행 파일 이름** – `%FILE_NAME%`.
  차단된 애플리케이션의 실행 파일 이름입니다.
- **실행 파일의 KL 카테고리** – `%KL_CAT%`.
  차단된 애플리케이션이 속한 KL 카테고리입니다(예: *브라우저* 또는 다른 카테고리).
- **실행 파일의 경로** – `%FILE_PATH%`.
  차단된 애플리케이션의 실행 파일 전체 경로입니다.
- **실행 파일 버전** – `%FILE_VERSION%`.
  차단된 애플리케이션의 실행 파일 버전입니다.
- **실행 파일의 원본 이름** – `%ORIGINAL_FILE_NAME%`.
  차단된 애플리케이션 실행 파일의 원본 이름입니다. 파일 이름은 애플리케이션의 실행 파일 속성에 지정됩니다.
- **공급업체** – `%FILE_PUBLISHER%`.
  차단된 애플리케이션의 공급업체입니다.
- **애플리케이션 이름** – `%FILE_PRODUCT_NAME%`.
  차단된 애플리케이션의 이름입니다.
- **애플리케이션 버전** – `%PRODUCT_VERSION%`.
  차단된 애플리케이션의 버전입니다.

- **실행 파일 해시** – `%FILE_HASH%`.
  차단된 애플리케이션의 실행 파일 해시입니다.
- **인증서 발급자** – `%CERT_ISSUER%`.
  실행 파일 서명에 사용된 인증서의 발급자입니다.
- **인증서 주체** – `%CERT_SUBJECT%`.
  실행 파일 서명에 사용된 인증서의 주체입니다.
- **인증서 지문** – `%CERT_THUMBPRINT%`.
  실행 파일 서명에 사용된 인증서의 지문입니다.

허용된 애플리케이션 목록 구현의 모범 사례

허용된 애플리케이션 목록을 구현하려면 다음 작업을 권장합니다.

1. 다음 유형의 그룹을 만듭니다:
   - 사용자 그룹. 다양한 애플리케이션 조합 사용을 허용해야 하는 사용자 그룹.
   - 관리 그룹. Kaspersky Security Center가 허용된 애플리케이션 목록을 적용할 하나 이상의 컴퓨터 그룹입니다. 해당 그룹에 대해 서로 다른 허용 목록 설정을 사용하려면 컴퓨터 그룹을 여러 개 만들어야 합니다.
2. 시작을 허용해야 하는 애플리케이션 목록을 만듭니다.
   목록을 생성하기 전에 다음을 수행하는 것이 좋습니다:
   a. 인벤토리 작업을 실행합니다.
      인벤토리 작업의 생성, 재구성, 시작에 관한 정보는 작업 관리 섹션에서 확인할 수 있습니다.
   b. 실행 파일 목록을 봅니다.

애플리케이션에 대한 허용 목록 모드 구성

허용 목록 모드를 테스트할 때에는 다음 작업을 권장합니다:

1. 시작을 허용해야 하는 애플리케이션을 포함한 애플리케이션 카테고리를 생성합니다.

애플리케이션 카테고리 생성에 대한 다음 유형 중 하나를 선택합니다:

- **수동으로 추가한 컨텐츠가 있는 카테고리**. 다음 조건을 사용하여 이 카테고리에 직접 추가할 수 있습니다:
  - 파일 메타데이터. Kaspersky Security Center는 지정된 메타데이터와 함께 모든 실행 파일을 애플리케이션 카테고리에 추가합니다.
  - 파일 해시 코드. Kaspersky Security Center는 지정된 해시가 포함된 모든 실행 파일을 애플리케이션 카테고리에 추가합니다.

    이 조건을 사용하면 파일 버전마다 해시가 달라지기 때문에 업데이트 자동 설치 기능이 비활성화됩니다.

  - 파일 인증서. Kaspersky Security Center는 지정된 인증서로 서명된 모든 실행 파일을 애플리케이션 카테고리에 추가합니다.
  - KL 카테고리. Kaspersky Security Center는 지정된 KL 카테고리에 속하는 모든 실행 파일을 애플리케이션 카테고리에 추가합니다.
  - 애플리케이션 폴더. Kaspersky Security Center는 애플리케이션 카테고리에 이 폴더의 모든 실행 파일을 추가합니다.

    애플리케이션 폴더 조건을 사용하면 지정된 폴더에 포함된 모든 애플리케이션의 시작이 허용되기 때문에 안전하지 않을 수 있습니다. **애플리케이션 폴더** 조건이 가진 애플리케이션 카테고리를 사용하는 규칙은 업데이트 자동 설치가 허용되어야 하는 사용자에게만 적용하는 것이 좋습니다.

- **지정한 폴더의 실행 파일을 포함하는 카테고리**. 생성된 애플리케이션 카테고리에 자동으로 할당될 실행 파일이 포함된 폴더를 지정합니다.
- **선택한 장치의 실행 파일이 포함된 카테고리**. 생성된 애플리케이션 카테고리에 모든 실행 파일을 자동으로 할당할 컴퓨터를 지정합니다.

  이 유형의 애플리케이션 카테고리 생성을 사용하면 Kaspersky Security Center는 **실행 파일** 폴더에서 컴퓨터의 애플리케이션에 관한 정보를 수신합니다.

2. 애플리케이션 제어 구성 요소에 대한 허용 목록을 선택합니다.
3. 생성된 애플리케이션 카테고리를 사용하여 애플리케이션 제어 규칙을 생성합니다.

골든 이미지 규칙 및 **신뢰하는 업데이터** 규칙은 허용 목록 모드에 따라 초기에 정의됩니다. 이러한 애플리케이션 제어 규칙은 KL 카테고리에 해당합니다. *골든 이미지* KL 카테고리에는 운영 체제의 정상 작동을 보장하는 프로그램이 포함됩니다. *신뢰하는 업데이터* KL 카테고리에는 가장 평판이 좋은 소프트웨어 공급업체의 업데이터가 포함됩니다. 규칙을 삭제할 수 없습니다. 이 규칙의 설정을 편집할 수 없습니다. 기본적으로 **골든 이미지** 규칙을 사용하면 **신뢰하는 업데이터** 규칙은 중지됩니다. 모든 사용자가 이 규칙의 작동 조건을 충족하는 애플리케이션을 시작할 수 있습니다.

4. 업데이트 자동 설치가 허용되어야 하는 애플리케이션을 결정합니다.

다음 방법 중 하나로 자동 업데이트 설치를 허용할 수 있습니다:

- KL 카테고리에 속하는 모든 애플리케이션의 시작을 허용하여 허용된 애플리케이션의 확장 목록을 지정합니다.
- 인증서로 서명된 모든 애플리케이션의 시작을 허용하여 허용된 애플리케이션의 확장 목록을 지정합니다.

  인증서로 서명된 모든 애플리케이션의 시작을 허용하려면 `*` 값을 사용하여 **제목** 파라미터만 사용하는 인증서 기준 조건의 카테고리를 생성하십시오.
- 애플리케이션 제어 규칙의 경우, **신뢰하는 업데이터** 파라미터를 선택합니다. 이 확인란을 선택하면 Kaspersky Endpoint Security는 규칙에 포함된 애플리케이션을 신뢰하는 업데이터로 간주합니다. Kaspersky Endpoint Security는 차단 규칙이 적용되지 않은 경우 규칙에 지정된 애플리케이션에 의해 설치되거나 업데이트된 애플리케이션의 시작을 허용합니다.

  Kaspersky Endpoint Security 설정을 마이그레이션하면 신뢰하는 업데이터가 생성한 실행 파일 목록도 마이그레이션됩니다.
- 폴더를 만든 다음 업데이트 자동 설치를 허용할 애플리케이션의 실행 파일을 해당 폴더 내에 저장합니다. 그런 후에 **애플리케이션 폴더** 조건을 사용하여 애플리케이션 카테고리를 만들고 해당 폴더의 경로를 지정합니다. 그리고 나서 허용 규칙을 만들고 이 카테고리를 선택합니다.

  애플리케이션 폴더 조건을 사용하면 지정된 폴더에 포함된 모든 애플리케이션의 시작이 허용되기 때문에 안전하지 않을 수 있습니다. **애플리케이션 폴더** 조건이 가진 애플리케이션 카테고리를 사용하는 규칙은 업데이트 자동 설치가 허용되어야 하는 사용자에게만 적용하는 것이 좋습니다.

허용 목록 모드 테스트

애플리케이션 제어 규칙으로 작업에 필요한 애플리케이션이 차단되지 않도록 하려면, 애플리케이션 제어 규칙을 테스트 모드로 활성화한 후 새 규칙 생성 이후의 동작을 분석하는 것이 좋습니다. 테스트 모드가 사용되면 Kaspersky Endpoint Security는 애플리케이션 제어 규칙으로 시작이 금지된 애플리케이션을 차단하지는 않지만 중앙 관리 서버로 애플리케이션 시작에 대한 알림을 전송합니다.

허용 목록 모드를 테스트할 때에는 다음 작업을 권장합니다:

1. 테스트 기간(이틀 ~ 2개월 사이)을 결정합니다.
2. 애플리케이션 제어 규칙 테스트를 작동합니다.
3. 테스트 결과를 분석하기 위해 애플리케이션 제어의 동작을 테스트 한 결과 이벤트와 테스트 모드에서 차단된 애플리케이션에 대한 리포트를 확인합니다.
4. 분석 결과에 따라 허용 목록 모드 설정을 변경합니다.

   특히 테스트 결과에 따라 이벤트와 관련된 실행 파일을 애플리케이션 카테고리에 추가할 수 있습니다.

허용 목록 모드 지원

애플리케이션 제어에 대한 차단 동작을 선택한 이후에는 다음 작업을 통해 허용 목록 모드를 계속해서 지원하는 것을 권장합니다:

- 효율적인 애플리케이션 제어를 분석하기 위해 애플리케이션 제어의 동작에 대한 결과 이벤트와 애플리케이션 실행 차단 리포트를 확인합니다.
- 애플리케이션에 접근하려는 사용자의 요청을 분석합니다.
- Kaspersky Security Network에서 평판을 확인하여 알 수 없는 실행 파일을 분석합니다.
- 운영 체제 또는 소프트웨어의 업데이트를 설치하기 전에 테스트 그룹 컴퓨터에 업데이트를 설치하여 애플리케이션 제어 규칙이 어떻게 처리하는지를 확인하십시오.
- 애플리케이션 제어 규칙에 사용되는 카테고리에 필요한 애플리케이션을 추가하십시오.

네트워크 포트 모니터링

Kaspersky Endpoint Security가 작동하는 동안 웹 제어, 메일 위협 보호, 웹 위협 보호, 행동 탐지, 익스플로잇 방지 구성 요소는 특정 프로토콜을 통해 전송되고 사용자 컴퓨터에서 열린 특정 TCP 및 UDP 포트를 통과하는 데이터 스트림을 모니터합니다. 예를 들어, 메일 위협 보호 구성 요소는 SMTP를 통해 전송되는 정보를 분석하고 웹 위협 보호 구성 요소는 HTTP 및 FTP를 통해 전송된 정보를 분석합니다.

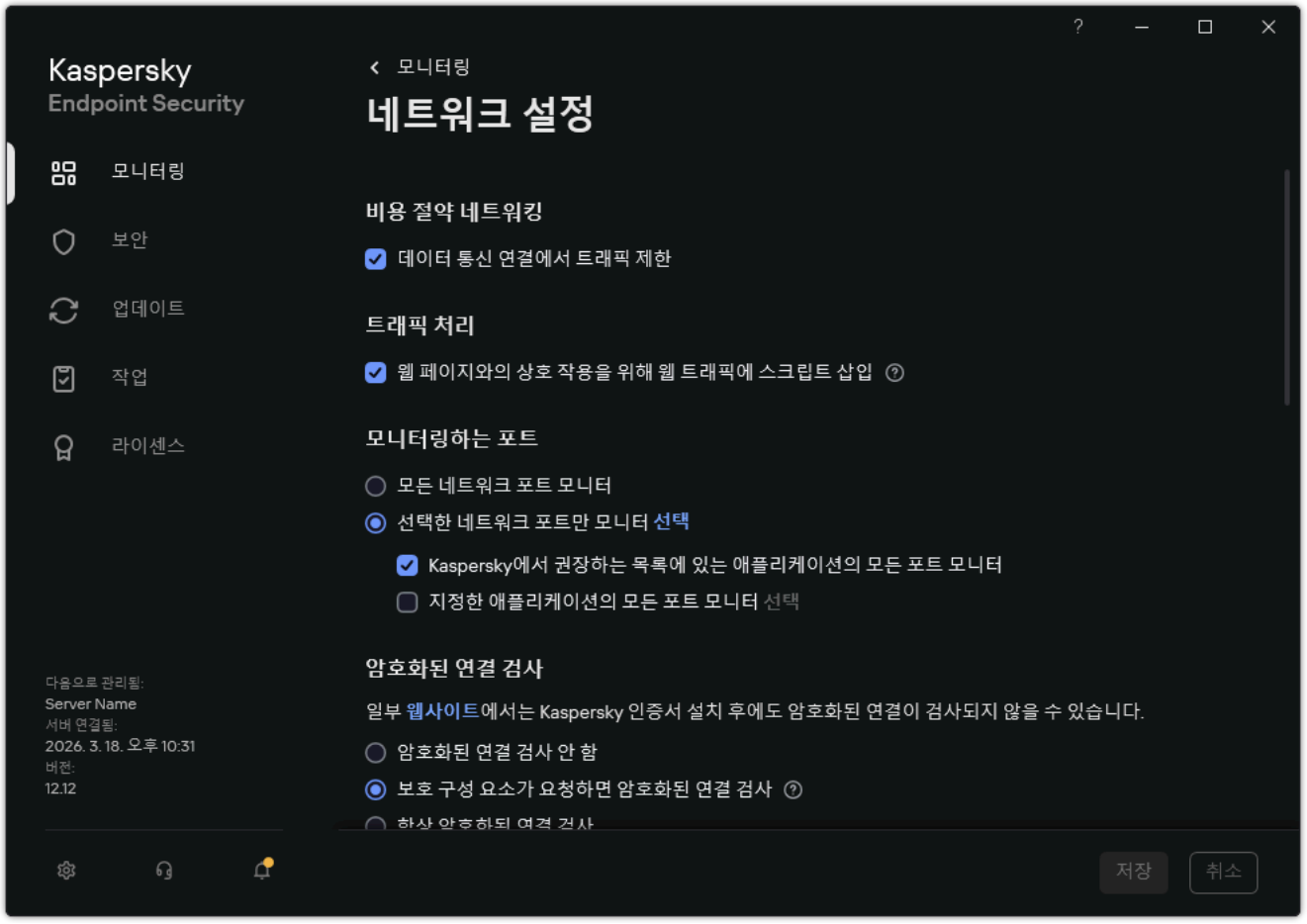
Kaspersky Endpoint Security는 위협을 받을 수 있는 가능성을 바탕으로 사용자 컴퓨터의 TCP 및 UDP 포트를 여러 그룹으로 세분합니다. 일부 네트워크 포트는 취약한 서비스 전용으로 예약됩니다. 이러한 포트는 네트워크 공격의 표적이 될 가능성이 더욱 높기 때문에 더욱 철저하게 감시할 필요가 있습니다. 비표준 네트워크 포트를 사용하는 비표준 서비스를 이용하는 경우에도 이러한 네트워크 포트가 컴퓨터가 공격을 받을 때 표적이 될 수 있습니다. 네트워크 접근이 필요한 네트워크 포트와 애플리케이션 목록을 지정할 수 있습니다. 그러면 네트워크 트래픽 감시 중에 메일 위협 보호 및 웹 위협 보호 구성 요소가 이러한 포트와 애플리케이션을 특별히 자세하게 감시합니다.

컴퓨터 보안 강화를 위해 행동 탐지와 익스플로잇 방지 구성 요소 역시 네트워크 포트를 통과하는 데이터 스트림을 모니터링합니다. 이 구성 요소는 네트워크 트래픽에서 위협일 수 있는 개별 프로세스를 계속해서 모니터링합니다.

모든 네트워크 포트의 감시 작동

모든 네트워크 포트의 감시를 작동하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.



네트워크 포트 모니터링 설정

3. **모니터링하는 포트** 블록에서 **모든 네트워크 포트 모니터**을 선택합니다.
4. 변경 사항을 저장합니다.

감시하는 네트워크 포트 목록 만들기

감시하는 네트워크 포트 목록을 변경하는 것은 부모 정책의 속성에 따라 차단될 수 있습니다. 목록을 변경하려면 웹 콘솔의 신뢰 구역('자물쇠'가 잠금 해제되어야 함) 설정 변경을 허용해야 합니다.

신뢰 구역은 관리 콘솔(MMC)과 웹 콘솔에서 다르게 그룹화됩니다. 마찬가지로, 신뢰 구역 파라미터의 변경을 방지하는 방법도 다릅니다('자물쇠'가 다름). 웹 콘솔만 사용하여 애플리케이션을 관리하는 것이 좋습니다. 서로 다른 콘솔에서 신뢰 구역을 구성하는 경우 관리 플러그인이 '자물쇠'를 기본 상태로 재설정할 수 있습니다.

감시하는 네트워크 포트 목록을 만들려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.
3. **모니터링하는 포트** 블록에서 **선택한 네트워크 포트만 모니터**를 선택합니다.
4. **선택**을 클릭합니다.
   이메일 및 네트워크 트래픽 전송에 일반적으로 사용되는 네트워크 포트의 목록을 엽니다. 네트워크 포트 목록은 Kaspersky Endpoint Security 패키지에 포함되어 있습니다.
5. **상태** 열의 토글을 사용하여 네트워크 포트 모니터링를 활성화 또는 비활성화합니다.
6. 원하는 네트워크 포트가 목록에 표시되지 않는 경우 다음 방법을 사용하여 추가합니다.
   a. **추가**를 클릭합니다.
   b. 열린 창에서 네트워크 포트 번호와 간단한 설명을 입력합니다.
   c. 네트워크 포트 모니터링에 대한 **활성** 또는 **비활성** 상태를 설정합니다.
7. 변경 사항을 저장합니다.

FTP 프로토콜이 Passive 모드에서 실행 중이면, 연결은 감시하는 네트워크 포트 목록에 추가 안 된 랜덤 네트워크 포트를 사용해 연결됩니다. 이러한 연결을 보호하려면 모든 네트워크 포트 모니터링를 사용하거나 FTP 연결을 설정하는 애플리케이션에 대한 네트워크 포트 제어를 구성하십시오.

모든 네트워크 포트에 대한 감시를 받을 애플리케이션 목록 만들기

Kaspersky Endpoint Security가 모든 네트워크 포트에 대한 감시를 받을 애플리케이션 목록을 만들 수 있습니다.

FTP 프로토콜을 통해 데이터를 수신 또는 전송하는 애플리케이션은 이 목록에 포함시키는 것이 좋습니다.

모든 네트워크 포트에 대한 감시를 받을 애플리케이션 목록을 만들려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **네트워크 설정**을 선택합니다.
3. **모니터링하는 포트** 블록에서 **선택한 네트워크 포트만 모니터**를 선택합니다.
4. **Kaspersky에서 권장하는 목록에 있는 애플리케이션의 모든 포트 모니터** 확인란을 선택합니다.
   이 확인란을 선택하면 Kaspersky Endpoint Security가 다음 애플리케이션의 모든 포트를 감시합니다:
   - Adobe Acrobat Reader
   - Apple 애플리케이션 지원

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Internet Explorer
- Java
- mIRC
- Opera
- Pidgin
- Safari
- Mail.ru 에이전트
- Yandex 브라우저

5. **지정한 애플리케이션의 모든 포트 모니터** 확인란을 선택합니다.
6. **선택**을 클릭합니다.
   Kaspersky Endpoint Security가 네트워크 포트를 감시할 애플리케이션 목록이 열립니다.
7. **상태** 열의 토글을 사용하여 네트워크 포트 모니터링를 활성화 또는 비활성화합니다.
8. 감시할 애플리케이션이 목록에 없는 경우 다음과 같은 방법으로 추가합니다.
   a. **추가**를 클릭합니다.
   b. 창이 열리면 애플리케이션의 실행 파일 경로와 간단한 설명을 입력합니다.
   c. 네트워크 포트 모니터링에 대한 **활성** 또는 **비활성** 상태를 설정합니다.
9. 변경 사항을 저장합니다.

모니터링하는 포트 목록 내보내기 및 가져오기

Kaspersky Endpoint Security는 네트워크 포트 목록 및 Kaspersky Endpoint Security에서 포트를 감시하는 애플리케이션 목록을 사용하여 네트워크 포트를 감시합니다. 모니터링하는 포트 목록을 XML 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 동일 유형의 웹 주소를 여러 개 추가하는 등의 작업을 진행할 수 있습니다. 내보내기 / 가져오기 기능을 사용하여 모니터링하는 포트 목록을 백업하거나 목록을 다른 서버로 마이그레이션할 수 있습니다.

관리 콘솔(MMC)에서 모니터링하는 포트 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정 → 네트워크 설정**으로 갑니다.

5. 신뢰하는 네트워크 포트를 내보내려면 다음을 수행합니다.

   a. **모니터링하는 포트** 블록에서 **선택한 네트워크 포트만 모니터**를 선택합니다.

   b. **선택한 N개 포트** 링크를 클릭합니다.

   네트워크 포트 창이 열립니다. **네트워크 포트** 창에는 이메일 및 네트워크 트래픽 전송에 일반적으로 사용되는 네트워크 포트의 목록이 표시됩니다. 네트워크 포트 목록은 Kaspersky Endpoint Security 패키지에 포함되어 있습니다.

   c. 네트워크 포트 목록에서 내보낼 포트를 선택합니다.

   d. **내보내기**를 클릭합니다.

   e. 창이 열리면 네트워크 포트 목록을 내보낼 XML 파일의 이름을 입력하고 이 파일을 저장할 폴더를 선택합니다.

   f. 파일을 저장합니다.

   Kaspersky Endpoint Security는 신뢰하는 네트워크 포트의 전체 목록을 XML 파일로 내보냅니다.

6. Kaspersky Endpoint Security에서 포트를 감시하는 애플리케이션 목록을 내보내려면 다음을 수행합니다.

   a. **모니터링하는 포트** 블록에서 **지정한 애플리케이션의 모든 포트 모니터** 확인란을 선택합니다.

   b. **선택한 N개 애플리케이션** 링크를 클릭합니다.

   c. 애플리케이션 목록에서 내보내려는 애플리케이션을 선택합니다.

   d. **내보내기**를 클릭합니다.

   e. 창이 열리면 애플리케이션 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

   f. 파일을 저장합니다.

   Kaspersky Endpoint Security는 애플리케이션의 전체 목록을 XML 파일로 내보냅니다.

7. 네트워크 포트 목록을 가져오려면 다음을 수행합니다.

   a. 네트워크 포트 목록에서 **가져오기** 버튼을 클릭합니다.

   창이 열리면 네트워크 포트 목록을 가져올 XML 파일을 선택합니다.

   b. 파일을 엽니다.

   컴퓨터에 이미 네트워크 포트 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. Kaspersky Endpoint Security에서 포트를 감시하는 애플리케이션 목록을 가져 오려면 다음을 수행합니다.

   a. 애플리케이션 목록에서 **가져오기** 버튼을 클릭합니다.

   창이 열리면 애플리케이션 목록을 가져올 XML 파일을 선택합니다.

b. 파일을 엽니다.

컴퓨터에 이미 애플리케이션 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

9. 변경 사항을 저장합니다.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **일반 설정 → 네트워크 설정**을 선택합니다.

4. **모니터링하는 포트** 블록에서 **선택한 네트워크 포트만 모니터**를 선택합니다.

5. **설정**을 클릭합니다.

네트워크 포트 창이 열립니다. **네트워크 포트** 창에는 이메일 및 네트워크 트래픽 전송에 일반적으로 사용되는 네트워크 포트의 목록이 표시됩니다. 네트워크 포트 목록은 Kaspersky Endpoint Security 패키지에 포함되어 있습니다.

6. 신뢰하는 네트워크 포트를 내보내려면 다음을 수행합니다.

a. 네트워크 포트 목록에서 내보낼 포트를 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.

포트를 선택하지 않으면 Kaspersky Endpoint Security는 모든 포트를 내보냅니다.

b. **내보내기**를 클릭합니다.

c. 창이 열리면 네트워크 포트 목록을 내보낼 XML 파일의 이름을 입력하고 이 파일을 저장할 폴더를 선택합니다.

d. 파일을 저장합니다.

Kaspersky Endpoint Security는 신뢰하는 네트워크 포트의 전체 목록을 XML 파일로 내보냅니다.

7. Kaspersky Endpoint Security에서 포트를 감시하는 애플리케이션 목록을 내보내려면 다음을 수행합니다.

a. **지정한 애플리케이션의 모든 포트 모니터** 확인란을 선택합니다.

b. 애플리케이션 목록에서 내보내려는 애플리케이션을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.

애플리케이션을 선택하지 않으면 Kaspersky Endpoint Security는 모든 애플리케이션을 내보냅니다.

c. **내보내기**를 클릭합니다.

d. 창이 열리면 애플리케이션 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

e. 파일을 저장합니다.

Kaspersky Endpoint Security는 애플리케이션의 전체 목록을 XML 파일로 내보냅니다.

8. 네트워크 포트 목록을 가져오려면 다음을 수행합니다.

a. 네트워크 포트 목록에서 **가져오기** 버튼을 클릭합니다.

창이 열리면 네트워크 포트 목록을 가져올 XML 파일을 선택합니다.

b. 파일을 엽니다.

컴퓨터에 이미 네트워크 포트 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

9. Kaspersky Endpoint Security에서 포트를 감시하는 애플리케이션 목록을 가져 오려면 다음을 수행합니다.

a. 애플리케이션 목록에서 **가져오기** 버튼을 클릭합니다.

창이 열리면 애플리케이션 목록을 가져올 XML 파일을 선택합니다.

b. 파일을 엽니다.

컴퓨터에 이미 애플리케이션 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

10. 변경 사항을 저장합니다.

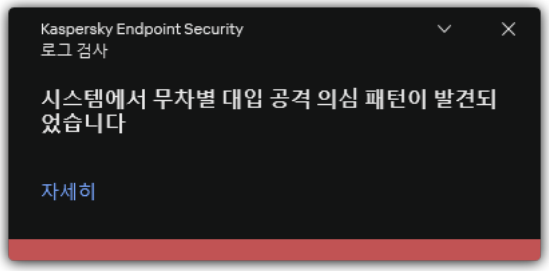
로그 검사

이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

Kaspersky Endpoint Security for Windows는 11.11.0 버전부터 로그 검사 구성 요소를 포함합니다. 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 Endpoint Security는 규칙에 따라 Windows 이벤트 로그를 분석하여 위반 사항을 감지합니다. 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(아래 그림 참조).

로그 검사를 사용하려면 감사 정책 보안 설정이 구성되어 시스템에서 관련 이벤트를 기록하는지 확인해야 합니다(자세한 내용은 Microsoft 기술 지원 웹사이트 참조).



로그 검사 알림

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 작동하거나 중지할 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

관리 콘솔(MMC)에서 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 창에서 **보안 제어 → 로그 검사**를 선택합니다.
4. **로그 검사** 확인란이 선택되어 있어야 합니다.
5. **사전 정의된 규칙** 블록에서 **설정** 버튼을 누릅니다.
6. 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**.
7. 필요할 경우 **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.

8. **네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다** 규칙을 선택했다면, 다음과 같이 설정을 구성해야 합니다.

   a. 규칙 밑에 있는 **설정** 버튼을 클릭합니다.

   b. **네트워크 로그인 탐지** 블록에서 시간 간격의 시작과 끝을 지정합니다.

   Kaspersky Endpoint Security는 지정한 간격 도중 수행한 로그인 시도를 비정상 활동으로 간주합니다.

   기본적으로 간격은 설정되지 않으며 애플리케이션은 로그인 시도를 모니터링하지 않습니다. 애플리케이션이 로그인 시도를 계속 모니터링하려면 간격을 오전 12:00부터 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 Endpoint Security는 이러한 사용자와 컴퓨터에 대한 로그온 시도는 모니터링하지 않습니다.

   d. **확인**을 누릅니다.

9. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 사전 정의된 규칙을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **로그 검사**로 이동합니다.
5. **로그 검사 활성화됨** 토글 스위치가 켜져야 합니다.
6. **사전 정의된 규칙** 블록에서 토글을 사용해 사전 정의된 규칙을 사용하도록 설정하거나 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**.

   a. **권한이 있는 내장 관리자 그룹에서 의심스러운 변경 사항이 감지되었습니다**.

7. 필요할 경우 **시스템에서 무차별 대입 공격 의심 패턴이 발견되었습니다** 규칙을 구성합니다.

   a. 규칙 밑에 있는 **설정**을 클릭합니다.

   b. 열린 창에서 규칙 트리거에 필요한 암호 입력 횟수와 시간을 지정합니다.

   c. **확인**을 누릅니다.

8. **네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다** 규칙을 선택했다면, 다음과 같이 설정을 구성해야 합니다.

   a. 규칙 밑에 있는 **설정**을 클릭합니다.

   b. **네트워크 로그인 탐지** 블록에서 시간 간격의 시작과 끝을 지정합니다.

   Kaspersky Endpoint Security는 지정한 간격 도중 수행한 로그인 시도를 비정상 활동으로 간주합니다.

   기본적으로 간격은 설정되지 않으며 애플리케이션은 로그인 시도를 모니터링하지 않습니다. 애플리케이션이 로그인 시도를 계속 모니터링하려면 간격을 오전 12:00부터 오후 11:59로 설정합니다. 간격의 시작과 끝은 다르게 설정해야 합니다. 시작과 끝을 같게 설정 시 애플리케이션이 로그인 시도를 모니터링하지 않습니다.

   c. **예외 규칙** 블록에서 신뢰하는 사용자와 신뢰하는 IP 주소(IPv4 및 IPv6)를 추가합니다.

   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 Endpoint Security는 이러한 사용자와 컴퓨터에 대한 로그온 시도는 모니터링하지 않습니다.

   d. **확인**을 누릅니다.

9. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 사전 정의된 규칙을 구성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **로그 검사**를 선택합니다.
3. **로그 검사** 토글 스위치가 켜져야 합니다.
4. **사전 정의된 규칙** 블록에서 **구성** 버튼을 누릅니다.
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**.

   a. **권한이 있는 내장 관리자 그룹에서 의심스러운 변경 사항이 감지되었습니다**.

6. 필요할 경우 **시스템에서 무차별 대입 공격 의심 패턴이 발견되었습니다** 규칙을 구성합니다.

   a. 규칙 밑에 있는 **설정**을 클릭합니다.

   b. 열린 창에서 규칙 트리거에 필요한 암호 입력 횟수와 시간을 지정합니다.

7. **네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다** 규칙을 선택했다면, 다음과 같이 설정을 구성해야 합니다.

   a. 규칙 밑에 있는 **설정**을 클릭합니다.

   b. **네트워크 로그인 탐지** 블록에서 시간 간격의 시작과 끝을 지정합니다.

   Kaspersky Endpoint Security는 지정한 간격 도중 수행한 로그인 시도를 비정상 활동으로 간주합니다.

   기본적으로 간격은 설정되지 않으며 애플리케이션은 로그인 시도를 모니터링하지 않습니다. 애플리케이션이 로그인 시도를 계속 모니터링하려면 간격을 오전 12:00부터 오후 11:59로 설정합니다. 간격의 시작과 끝은 다르게 설정해야 합니다. 시작과 끝을 같게 설정 시 애플리케이션이 로그인 시도를 모니터링하지 않습니다.

   c. **예외 규칙** 블록에서 신뢰하는 사용자와 신뢰하는 IP 주소(IPv4 및 IPv6)를 추가합니다.

   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 Endpoint Security는 이러한 사용자와 컴퓨터에 대한 로그온 시도는 모니터링하지 않습니다.

8. 변경 사항을 저장합니다.

이후 규칙이 트리거되면 Kaspersky Endpoint Security가 *심각 이벤트* 이벤트를 생성합니다.

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 세 규칙이 이미 사용자 지정 규칙 목록에 포함되어 있습니다.

관리 콘솔(MMC)에서 사용자 지정 규칙을 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **보안 제어 → 로그 검사**를 선택합니다.

4. **로그 검사** 확인란이 선택되어 있어야 합니다.

5. **사용자 지정 규칙** 블록에서 **설정** 버튼을 누릅니다.

6. 열린 창에서 사용하도록 설정할 사용자 지정 규칙 옆에 있는 확인란을 선택합니다.

7. 필요할 경우 **추가**를 클릭해 사용자 자신의 사용자 지정 규칙을 생성합니다.

8. 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.

9. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 사용자 지정 규칙을 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어** → **로그 검사**로 이동합니다.

5. **로그 검사 활성화됨** 토글 스위치가 켜져야 합니다.

6. **사용자 지정 규칙** 블록에서 사용하도록 설정할 사용자 지정 규칙을 선택합니다.

7. 필요할 경우 **추가**를 클릭해 사용자 자신의 사용자 지정 규칙을 생성합니다.

8. 그러면 창이 열립니다. 이 창에서 사용자 지정 규칙을 구성합니다.

   - **규칙 이름**.
   - **사용자 지정 로그 이름**. Windows 이벤트 로그. *Application*, *Security*, *System* 로그를 사용할 수 있습니다.
   - **원본**. 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.

9. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 사용자 지정 규칙을 추가하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **보안 제어** → **로그 검사**를 선택합니다.

3. **로그 검사** 토글 스위치가 켜져야 합니다.

4. **사용자 지정 규칙** 블록에서 **구성** 버튼을 누릅니다.

5. 열린 창에서 사용하도록 설정할 사용자 지정 규칙 옆에 있는 확인란을 선택합니다.

6. 필요할 경우 **추가**를 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 Endpoint Security가 *심각* 이벤트를 생성합니다.

시스템 무결성 모니터링

이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

12.6 버전부터 Kaspersky Endpoint Security for Windows에는 파일 무결성 모니터 구성 요소 대신 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 Endpoint Security는 해당 이벤트를 생성하고 관리자에게 알립니다. 시스템 무결성 모니터링은 실시간 모드에서 작동할 수 있으며 필요에 따라 시스템 무결성 검사를 수행할 수도 있습니다.

실시간 시스템 무결성 모니터링

실시간 모드에서 시스템 무결성 모니터링을 구성 요소의 범위(*모니터링 범위*)에 포함된 개체의 변경 사항을 추적합니다. 또한 시스템 무결성 모니터링을 사용하면 해당 개체에 대한 무단 접근을 실시간으로 차단할 수 있습니다.

온디맨드 시스템 무결성 검사

온디맨드 시스템 무결성 검사는 수동으로 또는 스케줄에 따라 실행할 수 있는 작업입니다. *시스템 무결성 검사* 작업을 실행하려면 구성 요소의 범위(*모니터링 범위*)를 설정하고 베이스라인을 생성합니다. *베이스라인*은 시스템 내 객체의 기록된 상태로 애플리케이션이 현재 상태와 비교할 때 이를 참조합니다.

파일 무결성 모니터 설정 마이그레이션

Kaspersky Endpoint Security를 버전 12.6으로 업데이트하면 파일 무결성 모니터 설정이 자동으로 마이그레이션됩니다. 마이그레이션 과정에서 애플리케이션이 모니터링 규칙을 시스템 무결성 모니터링으로 이동합니다. KSWS에서 KES로 마이그레이션할 때 파일 무결성 모니터 규칙이 시스템 무결성 모니터링으로 마이그레이션됩니다.

시스템 무결성 모니터링이 제대로 작동하려면 Kaspersky Endpoint Security 애플리케이션과 관리 플러그인이 버전 12.6으로 업데이트되어야 합니다. 이전 버전의 관리 플러그인이 있는 경우 관리 플러그인에 **시스템 무결성 모니터링** 섹션이 없으므로 시스템 무결성 모니터를 구성할 수 없습니다.

시스템 무결성 모니터링 규칙 정보

시스템 무결성 모니터가 작동하려면 적어도 하나 이상의 규칙을 추가해야 합니다. *시스템 무결성 모니터링 규칙*은 파일 및 레지스트리에 대한 사용자의 접근을 정의하는 기준입니다. 시스템 무결성 모니터링은 지정된 *모니터링 범위* 내에서 파일 및 레지스트리의 변경 사항을 탐지합니다. 모니터링 범위는 시스템 무결성 모니터링 규칙의 기준 중 하나입니다.

시스템 무결성 모니터를 통해 다음 개체를 모니터링할 수 있습니다:

- 파일
- 레지스트리
- 외부 장치

파일 모니터링과 관련된 특별 고려 사항

시스템 무결성 모니터는 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.

시스템 무결성 모니터링은 서버 공유 폴더의 파일에 대한 변경 사항을 모니터링하지 않습니다. 시스템 무결성 모니터링은 로컬에서만 사용할 수 있습니다.

Kaspersky Endpoint Security는 실시간 시스템 무결성 모니터가 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.

레지스트리 모니터링과 관련된 특별 고려 사항

시스템 무결성 모니터는 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 (실시간 시스템 무결성 모니터링에서만 사용 가능합니다)
- HKEY_CURRENT_USER (실시간 시스템 무결성 모니터링에서만 사용 가능합니다)

> *시스템 무결성 검사* 작업은 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 제어를 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 모니터링은 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 규칙*은 파일 및 레지스트리에 대한 사용자의 접근을 정의하는 기준입니다. 시스템 무결성 모니터링은 지정된 *모니터링 범위* 내에서 파일 및 레지스트리의 변경 사항을 탐지합니다. 모니터링 범위는 시스템 무결성 모니터링 규칙의 기준 중 하나입니다.

실시간 시스템 무결성 모니터링 모드

시스템 무결성 모니터링 규칙이 운영 체제 또는 기타 서비스 기능에 중요한 리소스를 사용하는 작업을 차단하지 않도록 하려면 테스트 모드를 활성화하고 구성 요소가 시스템에 미치는 영향을 분석하는 것이 좋습니다. 테스트 모드를 켜면 Kaspersky Endpoint Security는 규칙에 의해 금지된 사용자 활동을 차단하지 않고 *경고* ⚠ 이벤트를 생성합니다.

실시간 시스템 무결성 모니터링 구성 요소에는 두 가지 모드가 있습니다:

- 차단

  이 모드에서 시스템 무결성 모니터링은 시스템의 변경 사항을 추적하고 규칙에 따라(**허용** 또는 **차단**) 작업을 수행합니다. 또한 시스템 무결성 모니터링은 해당 이벤트를 생성하고 Kaspersky Security Center 콘솔에서 장치의 상태를 변경합니다.

- 알림

  이 모드에서 시스템 무결성 모니터링은 모니터링 범위에 있는 파일 및 레지스트리 키에 대한 작업을 허용합니다. 파일 또는 레지스트리에 대한 작업이 금지된 경우 애플리케이션이 이벤트(*차단된 작업이 테스트 모드에서 허용되었습니다*)를 생성합니다. 규칙이 시스템에 어떤 영향을 미치는지 분석하려면 리포트를 확인할 수 있습니다.

실시간 시스템 무결성 모니터링 활성화하기

관리 콘솔(MMC)에서 실시간 시스템 무결성 모니터링을 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **보안 제어 → 시스템 무결성 모니터링**을 선택합니다.
4. **시스템 무결성 모니터링** 확인란을 선택합니다.
5. **차단 규칙 운영 모드**에서 실시간 시스템 무결성 모니터링 모드를 선택합니다:
   - **차단**. 이 모드에서는 시스템 무결성 모니터링이 모니터링 범위에 있는 파일 및 레지스트리 키를 사용하는 작업을 차단하고 해당 이벤트를 생성합니다.
   - **알림**. 이 모드에서는 시스템 무결성 모니터링이 모니터링 범위에 있는 파일 및 레지스트리 키에 대한 작업을 허용하고 해당 이벤트를 생성합니다.
6. **실시간 시스템 무결성 모니터링** 블록에서 **실시간 시스템 무결성 모니터링** 확인란을 선택합니다.
7. 외부 장치 모니터링 구성:
   a. **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.
8. 파일 및 레지스트리 모니터링 구성:
   a. **파일 및 레지스트리 모니터** 확인란을 선택합니다.
   b. **설정**을 클릭합니다.
      시스템 무결성 모니터링 규칙 목록이 열립니다.
   c. **추가**를 클릭합니다.
      다른 소스에서 규칙 가져오기할 수도 있습니다.
   d. 시스템 무결성 모니터링 규칙을 구성합니다(아래 표 참조).
9. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔에서 실시간 시스템 무결성 모니터링을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어 → 시스템 무결성 모니터링**으로 이동합니다.

5. **시스템 무결성 모니터링 활성화됨** 토글을 켭니다.

6. **Windows** 탭을 선택합니다.

7. **실시간 시스템 무결성 모니터링**에서 실시간 시스템 무결성 모니터링 모드를 선택합니다:

   - **규칙 적용** 이 모드에서는 시스템 무결성 모니터링이 모니터링 범위에 있는 파일 및 레지스트리 키를 사용하는 작업을 차단하고 해당 이벤트를 생성합니다.

   - **규칙 테스트(알림)**. 이 모드에서는 시스템 무결성 모니터링이 모니터링 범위에 있는 파일 및 레지스트리 키에 대한 작업을 허용하고 해당 이벤트를 생성합니다.

8. 파일 및 레지스트리 모니터링 구성:

   a. **파일 및 레지스트리 모니터** 확인란을 선택합니다.

   b. **규칙**을 누릅니다.
   시스템 무결성 모니터링 규칙 목록이 열립니다.

   c. **추가**를 클릭합니다.
   다른 소스에서 규칙 가져오기할 수도 있습니다.

   d. 시스템 무결성 모니터링 규칙을 구성합니다(아래 표 참조).

9. 외부 장치 모니터링 구성:

   a. **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.

10. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 실시간 시스템 무결성 모니터링을 활성화하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **보안 제어 → 시스템 무결성 모니터링**을 선택합니다.

3. **시스템 무결성 모니터링** 토글 스위치를 켭니다.

4. **차단 규칙 운영 모드**에서 실시간 시스템 무결성 모니터링 모드를 선택합니다:

   - **차단**. 이 모드에서는 시스템 무결성 모니터링이 모니터링 범위에 있는 파일 및 레지스트리 키를 사용하는 작업을 차단하고 해당 이벤트를 생성합니다.
   - **알림**. 이 모드에서는 시스템 무결성 모니터링이 모니터링 범위에 있는 파일 및 레지스트리 키에 대한 작업을 허용하고 해당 이벤트를 생성합니다.

5. **실시간 시스템 무결성 모니터링** 블록에서 **실시간 시스템 무결성 모니터링** 확인란을 선택합니다.

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.

   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.

7. 파일 및 레지스트리 모니터링 구성:

   a. **파일 및 레지스트리 모니터** 확인란을 선택합니다.

   b. **설정**을 클릭합니다.

   시스템 무결성 모니터링 규칙 목록이 열립니다.

   c. **추가**를 클릭합니다.

   다른 소스에서 규칙 가져오기할 수도 있습니다.

8. 시스템 무결성 모니터링 규칙을 구성합니다(아래 표 참조).

9. 변경 사항을 저장합니다.

실시간 시스템 무결성 모니터링 규칙 설정

파라미터	설명
규칙 이름	실시간 시스템 무결성 모니터링 규칙 이름
파일 및 레지스트리 사용 작업	• **허용**. 시스템 무결성 모니터링은 모니터링 범위에 있는 파일 및 레지스트리 키에 대한 작업을 허용합니다. • **차단**. 선택한 모드에 따라 시스템 무결성 모니터링의 작업이 달라집니다. *시스템 보호 모드*를 선택한 경우 시스템 무결성 모니터링은 모니터링 범위의 파일 및 레지스트리 키에 대한 작업을 차단하고, 해당 이벤트를 생성하고, Kaspersky Security Center 콘솔에서 장치의 상태를 변경합니다. *테스트 모드*를 선택한 경우 시스템 무결성 모니터링은 모니터링 범위에 있는 파일 및 레지스트리 키에 대한 작업을 허용합니다.

파라미터	설명
이벤트 심각도	Kaspersky Endpoint Security는 모니터링 범위 내 파일 또는 레지스트리 키가 수정될 때마다 파일 수정 이벤트를 기록합니다. 사용할 수 있는 이벤트 심각도는 *정보*(ⓘ), *경고*(⚠), *심각*(❗)입니다.

모니터링 범위	• **파일**. 구성 요소가 모니터링하는 파일 및 폴더 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.
	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.
	• **레지스트리**. 구성 요소가 모니터링하는 레지스트리 키와 값의 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.

예외 규칙	• **파일**. 모니터링 범위에서 예외 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다. 예: `C:\Folder\Application\*.log`. 예외 항목이 모니터링 범위 항목에 우선합니다.
	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.
	• **레지스트리**. 모니터링 범위에서 예외 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다. 예외 항목이 모니터링 범위 항목에 우선합니다.

신뢰하는 사용자 및/또는 사용자 그룹	*신뢰하는 사용자*는 모니터링 범위에서 파일 및 레지스트리 키로 작업을 수행할 수 있는 사용자입니다. Kaspersky Endpoint Security가 신뢰하는 사용자가 수행한 작업을 탐지하면 시스템 무결성 모니터가 *정보* ⓘ 이벤트를 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.
파일 동작 표식/모니터링하는 작업	애플리케이션이 모니터링할 파일 또는 레지스트리 키로 작업을 특성화하는 마커입니다.
해싱	수정 시 파일 해시를 계산합니다. Kaspersky Endpoint Security는 이벤트가 생성될 때 파일의 해시에 대한 정보를 추가합니다.

온디맨드 시스템 무결성 검사

온디맨드 시스템 무결성 검사는 수동으로 또는 스케줄에 따라 실행할 수 있는 작업입니다. *시스템 무결성 검사* 작업을 실행할 때 애플리케이션은 모니터링 범위에 포함된 개체의 현재 상태를 *베이스라인* 상태와 비교합니다. 실시간 시스템 무결성 모니터와 달리, *시스템 무결성 검사* 작업은 이벤트 수를 제한하고 운영 체제의 변경 사항에 대한 전반적인 리포트를 생성할 수 있도록 도와줍니다.

시스템 무결성 모니터링이 작동하려면 적어도 하나 이상의 규칙을 추가해야 합니다. *시스템 무결성 모니터링 규칙*은 파일 및 레지스트리에 대한 사용자의 접근을 정의하는 기준입니다. 시스템 무결성 모니터링은 지정된 *모니터링 범위* 내에서 파일 및 레지스트리의 변경 사항을 탐지합니다. 모니터링 범위는 시스템 무결성 모니터링 규칙의 기준 중 하나입니다. 실시간 시스템 무결성 모니터에서 *시스템 무결성 검사* 작업에서 공유할 규칙을 구성하거나 작업에 대한 규칙을 별도로 생성할 수 있습니다. 베이스라인을 생성하기 위해 Kaspersky Endpoint Security는 *시스템 무결성 검사* 작업의 모니터링 범위를 *베이스라인 업데이트* 작업에 적용합니다.

베이스라인 생성 및 업데이트

시스템 무결성 검사 작업이 작동하려면 베이스라인이 필요합니다. *베이스라인*은 시스템 내 객체의 기록된 상태로 애플리케이션이 현재 상태와 비교할 때 이를 참조합니다. 시스템의 현재 상태가 베이스라인에 기록된 시스템 상태와 다른 경우 Kaspersky Endpoint Security가 해당 이벤트를 생성합니다. *베이스라인 업데이트* 작업을 사용하여 베이스라인을 생성하거나 업데이트할 수 있습니다.

다음 모드로 베이스라인을 업데이트할 수 있습니다.

- 전체 업데이트.
  애플리케이션이 모니터링 범위에 있는 모든 개체를 업데이트합니다.
- 점진적 업데이트.
  애플리케이션이 수정된 개체나 새로운 개체만 탐지하고 업데이트합니다.

관리 콘솔(MMC)에서 베이스라인을 생성하거나 업데이트하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **베이스라인 업데이트**를 선택합니다.

2단계. 베이스라인 업데이트 모드 선택

베이스라인 업데이트 모드 선택:

- **전체 업데이트**. 애플리케이션이 모니터링 범위에 있는 모든 개체를 업데이트합니다.
- **점진적 업데이트**. 애플리케이션이 수정된 개체나 새로운 개체만 탐지하고 업데이트합니다.

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

베이스라인 2024 등과 같이 작업 이름을 입력합니다.

5단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔에서 베이스라인을 생성하거나 업데이트하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **베이스라인 업데이트**를 선택합니다.
   c. **작업 이름** 필드에 *베이스라인 2024* 등과 같은 간단한 설명을 입력합니다.
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.
5. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.
6. 마법사를 끝냅니다.
   작업 목록에 새 작업이 표시됩니다.

7. 새 작업을 클릭합니다.
   작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. 베이스라인 업데이트 모드 선택:

   - **전체 업데이트**. 애플리케이션이 모니터링 범위에 있는 모든 개체를 업데이트합니다.
   - **점진적 업데이트**. 애플리케이션이 수정된 개체나 새로운 개체만 탐지하고 업데이트합니다.

10. 변경 사항을 저장합니다.

11. 작업 옆의 확인란을 선택합니다.

12. **시작**을 클릭합니다.

시스템 무결성 검사 작업에 대한 모니터링 범위 구성하기

시스템 무결성 검사 작업의 모니터링 범위는 기본값으로 실시간 시스템 무결성 모니터의 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 *모니터링 범위에 잘못된 개체가 포함되어 있습니다* 이벤트를 생성합니다.

관리 콘솔(MMC)에서 시스템 무결성 검사 작업에 대해 다른 모니터링 범위를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **보안 제어 → 시스템 무결성 모니터링**을 선택합니다.

4. **시스템 무결성 모니터링** 확인란을 선택합니다.

5. **시스템 무결성 검사**에서 작업 구성 모드를 선택합니다: **사용자 지정 설정**.

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.

   시스템 무결성 모니터는 베이스라인이 생성된 시점에 연결된 외부 장치에 대한 정보를 기록합니다. 이후, 외부 장치가 연결되면, 애플리케이션이 해당 이벤트를 생성합니다. *시스템 무결성 검사* 작업을 실행할 때 애플리케이션은 외부 장치의 연결 해제를 모니터링하지 않습니다.

7. 파일 및 레지스트리 모니터링 구성:

   a. **파일 및 레지스트리 모니터** 확인란을 선택합니다.

   b. **설정**을 클릭합니다.
   시스템 무결성 모니터링 규칙 목록이 열립니다.

   c. **추가**를 클릭합니다.
   다른 소스에서 규칙 가져오기할 수도 있습니다.

   d. 시스템 무결성 모니터링 규칙을 구성합니다(아래 표 참조).

8. 변경 사항을 저장합니다.

웹 콘솔에서 시스템 무결성 검사 작업에 대해 다른 모니터링 범위를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **보안 제어** → **시스템 무결성 모니터링**으로 이동합니다.

5. **Windows** 탭을 선택합니다.

6. **시스템 무결성 모니터링 활성화됨** 토글을 켭니다.

7. **시스템 무결성 검사**에서 작업 구성 모드를 선택합니다: **사용자 지정 설정**.

8. 외부 장치 모니터링 구성:

   a. **장치 모니터** 확인란을 선택합니다.

   b. **이벤트 심각도** 드롭다운 목록에서 외부 장치 모니터링 이벤트의 중요도(*정보*, *경고*, *심각*)를 선택합니다.

   시스템 무결성 모니터는 베이스라인이 생성된 시점에 연결된 외부 장치에 대한 정보를 기록합니다. 이후, 외부 장치가 연결되면, 애플리케이션이 해당 이벤트를 생성합니다. *시스템 무결성 검사* 작업을 실행할 때 애플리케이션은 외부 장치의 연결 해제를 모니터링하지 않습니다.

9. 파일 및 레지스트리 모니터링 구성:

   a. **파일 및 레지스트리 모니터** 확인란을 선택합니다.

   b. **규칙**을 누릅니다.
   시스템 무결성 모니터링 규칙 목록이 열립니다.

c. **추가**를 클릭합니다.

다른 소스에서 규칙 가져오기할 수도 있습니다.

d. 시스템 무결성 모니터링 규칙을 구성합니다(아래 표 참조).

10. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 시스템 무결성 검사 작업에 대해 다른 모니터링 범위를 구성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **보안 제어** → **시스템 무결성 모니터링**을 선택합니다.
3. **시스템 무결성 모니터링** 토글 스위치를 켭니다.
4. **시스템 무결성 검사**에서 작업 구성 모드를 선택합니다: **사용자 지정 설정**.
5. 외부 장치 모니터링 구성:

a. **장치 모니터** 확인란을 선택합니다.

b. **이벤트 심각도** 드롭다운 목록에서 외부 장치 모니터링 이벤트의 중요도(*정보* ⓘ, *경고* ⚠, *심각* ⓘ)를 선택합니다.

시스템 무결성 모니터는 베이스라인이 생성된 시점에 연결된 외부 장치에 대한 정보를 기록합니다. 이후, 외부 장치가 연결되면, 애플리케이션이 해당 이벤트를 생성합니다. *시스템 무결성 검사* 작업을 실행할 때 애플리케이션은 외부 장치의 연결 해제를 모니터링하지 않습니다.

6. 파일 및 레지스트리 모니터링 구성:

a. **파일 및 레지스트리 모니터** 확인란을 선택합니다.

b. **설정**을 클릭합니다.

시스템 무결성 모니터링 규칙 목록이 열립니다.

c. **추가**를 클릭합니다.

다른 소스에서 규칙 가져오기할 수도 있습니다.

d. 시스템 무결성 모니터링 규칙을 구성합니다(아래 표 참조).

7. 변경 사항을 저장합니다.

파라미터	설명
규칙 이름	*시스템 무결성 검사* 작업 규칙 이름.
이벤트 심각도	Kaspersky Endpoint Security는 모니터링 범위 내 파일 또는 레지스트리 키가 수정될 때마다 파일 수정 이벤트를 기록합니다. 사용할 수 있는 이벤트 심각도는 *정보*(ⓘ), *경고*(⚠), *심각*(❗)입니다.

모니터링 범위	• **파일**. 구성 요소가 모니터링하는 파일 및 폴더 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.
	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.
	• **레지스트리**. 구성 요소가 모니터링하는 레지스트리 키와 값의 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다.

예외 규칙	• **파일**. 모니터링 범위에서 예외 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다. 예: `C:\Folder\Application\*.log`. 예외 항목이 모니터링 범위 항목에 우선합니다.
	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.
	• **레지스트리**. 모니터링 범위에서 예외 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다. 예외 항목이 모니터링 범위 항목에 우선합니다.

시스템 무결성 검사 작업 실행

시스템 무결성 검사 작업을 통해 파일 또는 레지스트리 키 변경 사항과 외부 장치 연결 상태를 확인할 수 있습니다. 파일의 변경 사항을 확인하려면 다음 모드에서 *시스템 무결성 검사* 작업을 실행할 수 있습니다:

- 빠른 검사.

  파일에 변경 사항이 있는지 확인할 때 애플리케이션은 파일 특성만 확인합니다. 애플리케이션은 파일의 내용을 확인하지 않습니다.

- 전체 검사.

  파일의 변경 사항을 확인할 때 애플리케이션이 모든 파일 특성과 파일 내용을 확인합니다.

작업이 실행되는 모드는 레지스트리나 외부 장치의 검사에 영향을 미치지 않습니다.

관리 콘솔(MMC)에서 시스템 무결성 검사 작업을 실행하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업**을 선택합니다.
   작업 목록이 열립니다.
3. **새 작업**을 클릭합니다.
   작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
4. **Kaspersky Endpoint Security → 베이스라인 시스템 무결성 모니터**를 선택합니다. 시스템 무결성 모니터 모드 선택:
   - **전체 검사**. 이 모드에서는 애플리케이션이 파일의 모든 속성과 해시를 확인합니다.
   - **빠른 검사**. 이 모드에서는 애플리케이션이 파일의 속성만 확인합니다.
5. 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.
6. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.
7. 작업 시작 스케줄(예: 직접 또는 지정된 요일에)을 구성하십시오.
8. 작업 이름을 입력합니다.
9. 마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔에서 시스템 무결성 검사 작업을 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **시스템 무결성 검사**를 선택합니다.

c. **작업 이름** 필드에 *주별 시스템 무결성 검사* 등의 간단한 설명을 입력합니다.

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

4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.

5. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.

6. 마법사를 끝냅니다.
   작업 목록에 새 작업이 표시됩니다.

7. 새 작업을 클릭합니다.
   작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. 시스템 무결성 검사 모드 선택:

   - **빠른 검사**. 애플리케이션은 파일 특성만 확인합니다. 애플리케이션은 파일의 내용을 확인하지 않습니다.
   - **전체 검사**. 애플리케이션이 파일의 모든 특성과 컨텐츠를 확인합니다.

10. 변경 사항을 저장합니다.

11. 작업 옆의 확인란을 선택합니다.

12. **시작**을 클릭합니다.

시스템 무결성 검사 작업을 성공적으로 완료하려면 *시스템 무결성 검사* 작업의 모니터링 범위가 베이스라인과 완전히 일치해야 합니다. 모니터링 범위가 다르면 작업이 오류와 함께 종료됩니다. 모니터링 범위를 동기화하려면 *베이스라인 업데이트* 작업을 새 모니터링 범위로 실행하세요.

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 *모니터링 범위에 잘못된 개체가 포함되어 있습니다* 이벤트를 생성합니다.

관리 콘솔(MMC)에서 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 창에서 **보안 제어 → 시스템 무결성 모니터링**을 선택합니다.

4. *실시간 시스템 무결성 모니터링* 규칙을 내보내거나 가져오기:

   a. **실시간 시스템 무결성 모니터링** 블록에서 **설정** 버튼을 클릭합니다.

   b. 실시간 시스템 무결성 모니터링 규칙 목록을 내보내기:

      1. 내보낼 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
         규칙을 선택하지 않으면 Kaspersky Endpoint Security는 모든 규칙을 내 보냅니다.

      2. **내보내기** 링크를 클릭합니다.

      3. 창이 열리면 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

      4. 파일을 저장합니다.
         Kaspersky Endpoint Security는 신뢰하는 규칙 목록을 XML 파일로 내보냅니다.

   c. 실시간 시스템 무결성 모니터링 규칙 목록을 가져오기:

      1. **가져오기** 링크를 클릭합니다.
         창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.

      2. 파일을 엽니다.
         컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

5. *시스템 무결성 검사* 규칙을 내보내거나 가져오기:

   a. **시스템 무결성 검사** 블록에서 **사용자 지정 설정**을 선택합니다.

   b. **설정**을 클릭합니다.

   c. 시스템 무결성 검사 규칙 목록을 내보내기:

      1. 내보낼 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
         규칙을 선택하지 않으면 Kaspersky Endpoint Security는 모든 규칙을 내 보냅니다.

      2. **내보내기** 링크를 클릭합니다.

      3. 창이 열리면 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

      4. 파일을 저장합니다.

      Kaspersky Endpoint Security는 신뢰하는 규칙 목록을 XML 파일로 내보냅니다.

   d. 시스템 무결성 검사 규칙 목록을 불러오려면:

      1. **가져오기** 링크를 클릭합니다.
         창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.

      2. 파일을 엽니다.

컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

6. 변경 사항을 저장합니다.

웹 콘솔에서 시스템 무결성 모니터링 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **보안 제어** → **시스템 무결성 모니터링**으로 이동합니다.
5. **Windows** 탭을 선택합니다.
6. *실시간 시스템 무결성 모니터링* 규칙을 내보내거나 가져오기:
   a. **실시간 시스템 무결성 모니터링** 블록에서 **규칙** 링크를 클릭합니다.
   b. 실시간 시스템 무결성 모니터링 규칙 목록을 내보내기:
      1. 내보낼 규칙을 선택합니다.
      2. → **내보내기** 버튼을 클릭합니다.
         Kaspersky Endpoint Security는 규칙 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.
   c. 실시간 시스템 무결성 모니터링 규칙 목록을 가져오기:
      1. → **가져오기** 버튼을 클릭합니다.
         창이 열리면 신뢰하는 주소 목록을 가져올 JSON 파일을 선택합니다.
      2. 파일을 엽니다.
         컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.
7. *시스템 무결성 검사* 규칙을 내보내거나 가져오기:
   a. **온디맨드 시스템 무결성 검사** 블록에서 **사용자 지정 설정**을 선택합니다.
   b. **규칙** 링크를 클릭합니다.
   c. 시스템 무결성 검사 규칙 목록을 내보내기:
      1. 내보낼 규칙을 선택합니다.
      2. → **내보내기** 버튼을 클릭합니다.
         Kaspersky Endpoint Security는 규칙 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.

d. 시스템 무결성 검사 규칙 목록을 불러오려면:

1. → **가져오기** 버튼을 클릭합니다.
   창이 열리면 신뢰하는 주소 목록을 가져올 JSON 파일을 선택합니다.
2. 파일을 엽니다.
   컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. 변경 사항을 저장합니다.

시스템 무결성 모니터링 리포트 보기

시스템 무결성 모니터링 규칙의 성능을 분석하기 위해 애플리케이션에서 생성된 리포트 및 이벤트를 확인할 수 있습니다. Kaspersky Endpoint Security는 구성 요소에 대해 다음과 같은 리포트를 생성합니다.

- 애플리케이션 인터페이스에서:
  - 시스템 무결성 모니터링 리포트
  - 시스템 무결성 검사 리포트
  - 베이스라인 업데이트 리포트

  리포트에는 시스템 무결성 모니터링 이벤트가 포함되어 있습니다.
- Kaspersky Security Center 콘솔에서:
  - 모니터링 규칙이 가장 많이 트리거된 컴퓨터에 대한 리포트
  - 가장 자주 트리거되는 모니터링 규칙에 대한 리포트

  기본 설정으로 리포트가 생성된 날짜를 포함하여 지난 30일 동안의 리포트가 생성됩니다.

관리 콘솔(MMC)에서 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**을 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**를 선택합니다.
2. **추가**를 클릭합니다.
   새 리포트 템플릿 마법사가 시작됩니다.
3. **템플릿 유형**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.

시스템 무결성 상태 재설정

Kaspersky Security Center 콘솔에 표시되는 컴퓨터의 상태는 다음 중 하나입니다: *정상*, *경고*, 또는 *심각*. 시스템 무결성 모니터가 모니터링 범위에 있는 파일 또는 레지스트리 키 변경을 탐지하면 컴퓨터의 상태가 *경고* 또는 *심각*으로 변경됩니다. 시스템 무결성 모니터에서 할당된 상태를 *시스템 무결성 상태*라고 합니다. 예를 들어 분석 결과 감지된 개체의 수정이 컴퓨터의 보안에 영향을 주지 않는다고 확신하는 경우 시스템 무결성 상태를 재설정할 수 있습니다.

관리 콘솔(MMC)에서 시스템 무결성 상태를 재설정하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → 시스템 무결성 상태 재설정을 선택합니다.

2단계. 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.

3 단계. 작업 시작 스케줄 구성

작업 일정을 설정합니다(예: 수동).

4단계. 작업 이름 정의

작업 이름(예: *모니터링 범위 수정 후 상태 재설정*)을 입력합니다.

5단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔에서 시스템 무결성 상태를 재설정하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **시스템 무결성 상태 재설정**을 선택합니다.
   c. **작업 이름** 필드에 간략한 설명(예: *모니터링 범위 수정 후 상태 재설정*)을 입력합니다.
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.

5. 작업을 실행할 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 로컬 사용자 계정의 권한으로 작업을 시작합니다.

6. 마법사를 끝냅니다.
   작업 목록에 새 작업이 표시됩니다.

7. 작업 옆의 확인란을 선택합니다.

8. **시작**을 클릭합니다.

따라서 시스템 무결성 모니터링 이벤트로 인해 컴퓨터의 상태가 *경고* 또는 *심각*으로 변경된 경우 컴퓨터의 상태가 *정상*으로 재설정됩니다. 다른 이벤트로 인해 컴퓨터의 상태도 변경된 경우 컴퓨터의 상태는 변경되지 않은 상태로 유지됩니다.

Cloud Discovery

Cloud Discovery는 사용자의 클라우드 서비스 액세스를 관리합니다. 클라우드 서비스에는 Microsoft Teams, Salesforce, Microsoft Office 365 등이 있습니다. 클라우드 서비스는 *파일 공유*, *메신저*, *이메일*과 같은 카테고리로 묶을 수도 있습니다. Kaspersky 전문가들은 정기적으로 Cloud Discovery 카테고리와 카테고리로 구분된 클라우드 서비스를 업데이트합니다. Kaspersky Endpoint Security는 애플리케이션 데이터베이스로 카테고리 세트와 클라우드 서비스를 업데이트합니다. 이는 Cloud Discovery에서 클라우드 서비스 카테고리 정리에 Kaspersky Security Network를 사용하지 않는다는 의미입니다.

Cloud Discovery는 다음 기능을 제공합니다.

- 클라우드 서비스 사용 모니터링
- 클라우드 서비스 사용자 접근 차단

시스템 요구 사항

Cloud Discovery는 다음 조건 충족 시 이용 가능합니다.

- 워크스테이션용 Windows가 실행되는 컴퓨터에 애플리케이션이 설치되어 있어야 합니다.
  구성 요소는 서버에서 이용할 수 없습니다.
- Kaspersky Security Center 버전 15.1 이상.
  이 구성 요소는 관리 콘솔(MMC)에서는 사용할 수 없습니다. Kaspersky Security Center 웹 콘솔 및 Kaspersky Security Center Cloud Console에서 Cloud Discovery를 구성할 수 있습니다.
- Kaspersky Next 라이센스가 필요합니다.

Cloud Discovery 구성 요소에 필요한 애플리케이션 기능을 활성화합니다:

1. **암호화된 연결 검사**. 이는 HTTPS 트래픽 모니터링에 필요합니다. **네트워크 설정** 섹션에서 이 기능을 관리할 수 있습니다.

2. **웹 페이지와의 상호 작용을 위해 웹 트래픽에 스크립트 삽입**. 이 스크립트를 사용하면 Cloud Discovery 이벤트를 등록할 수 있습니다. 이 스크립트는 클라우드 서비스에 대한 완전한 액세스 차단 기능도 제공합니다. 스크립트가 없으면 애플리케이션이 클라우드 서비스 도메인 접근만 차단합니다. **네트워크 설정** 섹션에서 이 기능을 관리할 수 있습니다.

허용된 페이지 열기 기록 기능을 활성화할 수도 있습니다. 이 기능에는 사용자가 동일한 도메인에 속하는 웹페이지 방문 시 이벤트를 그룹화하는 것이 포함됩니다. 이렇게 하면 사용자가 클라우드 서비스를 사용할 때 Cloud Discovery는 각 웹페이지의 여러 이벤트가 아닌 하나의 이벤트만 기록합니다. **웹 제어** 섹션에서 이 기능을 관리할 수 있습니다.

클라우드 서비스 모니터링

사용자가 클라우드 서비스 사용을 시작하면 Kaspersky Endpoint Security는 해당 이벤트를 등록하고 리포트에 항목을 만듭니다. Cloud Discovery는 브라우저와 해당 애플리케이션에서 클라우드 서비스 사용을 제어합니다. Cloud Discovery는 HTTP 및 HTTPS로 클라우드 서비스 사용을 제어합니다.

Cloud Console에서 클라우드 서비스 모니터링을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **통신 및 웹 보호** → **Cloud Discovery**로 갑니다.

5. **Cloud Discovery 활성화됨** 토글을 켭니다.

6. 변경 사항을 저장합니다.

그러면 애플리케이션은 Kaspersky Security Center에서 사용되는 클라우드 서비스 관련 정보를 전송합니다. 리포트에서 클라우드 서비스 사용 정보를 볼 수 있습니다. 필요한 경우 클라우드 서비스 접근을 차단할 수 있습니다.

클라우드 서비스 접근 차단

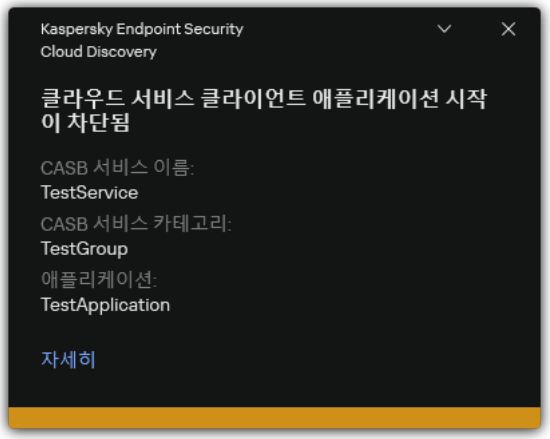
클라우드 서비스에 대한 접근 차단은 Kaspersky Next EDR Optimum 및 XDR Expert 라이센스에만 사용 가능합니다. Kaspersky Next EDR Foundations 라이센스에서는 이 기능을 사용할 수 없습니다. Kaspersky Next 라이센스 유형에 따른 애플리케이션 기능 비교는 Kaspersky Next 도움말을 참조하십시오.

관리자는 Cloud Discovery 카테고리 또는 개별 클라우드 서비스의 사용자 액세스를 제한할 수 있습니다. 이렇게 하면 관리자는 안전한 클라우드 서비스만 허용하고 데이터 누출을 피할 수 있습니다. Cloud Discovery에 각 클라우드 서비스의 *위험 수준 정보*가 표시됩니다. 위험 수준은 조직의 보안 요구 사항을 만족하지 않는 서비스 감지에 유용합니다.

위험 수준은 예측이며 클라우드 서비스 또는 공급업체의 품질을 단정하는 의미는 아닙니다. 위험 수준은 Kaspersky 전문가의 권장일 뿐입니다.

클라우드 서비스의 위험 수준은 관리되는 모든 클라우드 서비스 목록의 **Cloud Discovery** 정책 섹션에 표시됩니다.

다른 Kaspersky Endpoint Security 구성 요소는 클라우드 서비스를 사용할 때의 위협에서 보호하고 수상한 사용자 활동을 추적합니다.



Cloud Discovery 알림

Cloud Discovery는 Kaspersky Endpoint Security 전에 시작된 클라우드 애플리케이션을 차단하지 않습니다.

Cloud Console에서 클라우드 서비스 접근 차단 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **통신 및 웹 보호** → **Cloud Discovery**로 갑니다.
5. **Cloud Discovery 활성화됨** 토글을 켭니다.
   모든 클라우드 서비스 목록이 표시됩니다. 클라우드 서비스는 *파일 공유*, *메신저*, *이메일*과 같은 카테고리로 묶을 수도 있습니다. Kaspersky 전문가들은 정기적으로 Cloud Discovery 카테고리와 카테고리로 구분된 클라우드 서비스를 업데이트합니다. Kaspersky Endpoint Security는 애플리케이션 데이터베이스로 카테고리 세트와 클라우드 서비스를 업데이트합니다.
6. **접근** 열의 토글 스위치로 클라우드 서비스 접근을 구성합니다.
7. 변경 사항을 저장합니다.

그러면 애플리케이션이 브라우저와 해당 애플리케이션에서 클라우드 서비스 사용을 제어합니다.

신뢰 구역

*신뢰 구역*은 Kaspersky Endpoint Security에서 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 Endpoint Security가 해당 개체 또는 애플리케이션에 대한 접근을 차단하면 개체와 애플리케이션을 신뢰 구역에 포함시키는 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.

Kaspersky Endpoint Security 12.5 for Windows 버전부터는 EDR 원격 측정을 신뢰 구역으로 추가할 수 있습니다. 이를 통해 애플리케이션이 Kaspersky Anti Targeted Attack Platform(EDR) 솔루션용 원격 측정 수집 서버로 전송하는 데이터를 최적화할 수 있습니다.

Kaspersky Endpoint Security 12.6 for Windows부터 검사 예외 및 신뢰하는 애플리케이션 이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다.

Kaspersky Endpoint Security 12.8 for Windows부터 가상 환경 보호를 위한 Light Agent 모드로 애플리케이션을 설치할 수 있습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다.

검사 예외 생성

*검사 예외*는 Kaspersky Endpoint Security에서 특정 개체의 바이러스 및 기타 위협을 검사하지 않도록 하려면 충족해야 하는 조건 집합입니다. 검사 예외를 사용하면 범죄자가 컴퓨터 또는 사용자 데이터에 심각한 손상을 가하기 위해 악용할 수 있는 합법적인 소프트웨어를 안전하게 사용할 수 있습니다. 해당 애플리케이션은 악성 기능을 갖지 않지만 침입자가 악용할 수 있습니다. 침입자에게 악용되어 사용자의 컴퓨터나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어에 대한 상세 정보는 Kaspersky IT 백과사전을 참조하십시오.

이러한 애플리케이션은 Kaspersky Endpoint Security에 의해 차단될 수 있습니다. 차단되는 것을 방지하기 위해 사용 중인 애플리케이션에 대한 검사 예외를 구성할 수 있습니다. 그러려면 Kaspersky IT 백과사전에 나와 있는 이름이나 이름 마스크를 신뢰 구역에 추가합니다. 컴퓨터 원격 관리에 Radmin 애플리케이션을 자주 사용하는 경우를 예로 들어 보겠습니다. Kaspersky Endpoint Security는 이러한 활동을 의심스러운 것으로 간주하여 차단할 수 있습니다. 애플리케이션이 차단되는 것을 방지하기 위해 Kaspersky IT 백과사전에 있는 이름 또는 이름 마스크로 검사 예외를 만듭니다.

정보를 수집하고 처리를 위해 정보를 전송하는 애플리케이션이 컴퓨터에 설치되어 있는 경우 Kaspersky Endpoint Security에서 이 애플리케이션을 악성 코드로 분류할 수 있습니다. 이를 방지하려면 이 문서에 설명한 대로 Kaspersky Endpoint Security를 구성하여 애플리케이션을 검사에서 예외할 수 있습니다.

검사 예외는 시스템 관리자가 구성한 다음과 같은 애플리케이션 구성 요소 및 작업에서 사용할 수 있습니다:

- 행동 탐지
- 익스플로잇 방지
- 호스트 침입 방지
- 파일 위협 보호

- 웹 위협 보호
- 메일 위협 보호
- *악성 코드 검사* 작업

Kaspersky Endpoint Security는 검사 작업 실행 시 검사 범위에 포함된 드라이브 또는 폴더에 들어 있는 개체를 검사하지 않습니다. 그러나 이 개체에 대한 사용자 지정 검사 작업이 시작된 경우 검사 예외는 적용되지 않습니다.

검사 예외 목록의 변경은 부모 정책의 속성에 따라 차단될 수 있습니다. 목록을 변경하려면 웹 콘솔의 신뢰 구역('자물쇠'가 잠금 해제되어야 함) 설정 변경을 허용해야 합니다.

신뢰 구역은 관리 콘솔(MMC)과 웹 콘솔에서 다르게 그룹화됩니다. 마찬가지로, 신뢰 구역 파라미터의 변경을 방지하는 방법도 다릅니다('자물쇠'가 다름). 웹 콘솔만 사용하여 애플리케이션을 관리하는 것이 좋습니다. 서로 다른 콘솔에서 신뢰 구역을 구성하는 경우 관리 플러그인이 '자물쇠'를 기본 상태로 재설정할 수 있습니다.

관리 콘솔(MMC)에서 검사 예외를 만드는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정** → **예외 및 개체 유형**을 선택합니다.
4. **검사 예외 및 신뢰하는 애플리케이션** → **검사 예외** 블록에서 **설정** 버튼을 누릅니다.

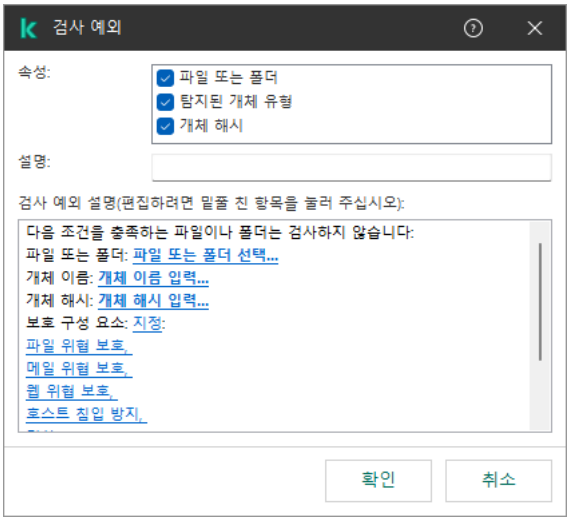
   예외 규칙 목록이 포함된 창이 열립니다.
5. 회사의 모든 컴퓨터에 대해 통합 예외 규칙 목록을 만들려면 **상속할 때 값 병합** 확인란을 선택합니다. 부모 및 자식 정책의 예외 규칙 목록이 병합됩니다. 상속할 때 값 병합이 활성화된 경우 목록이 병합됩니다. 부모 정책의 예외 규칙은 자식 정책에 읽기 전용 보기로 표시됩니다. 부모 정책의 예외 규칙은 변경하거나 삭제할 수 없습니다.
6. 사용자가 예외 규칙의 로컬 목록을 만들 수 있도록 하려면 **로컬 예외 항목 사용 허용** 확인란을 선택합니다. 이러한 방식으로 사용자는 정책에서 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 취소하면 Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 검사 예외 통합 목록을 숨깁니다.
7. **추가**를 클릭하고 작업을 선택합니다:
   - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.
   - **새로운 예외**. Kaspersky Endpoint Security가 새 검사 예외를 목록의 루트에 추가합니다.

- **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 검사 예외*가 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 검사 예외가 추가되었습니다. 보호하는 서버의 용도에 따라 사전 정의된 검사 예외를 선택해야 합니다.

- **선택한 카테고리에 대한 새로운 제외 사항**. 특정 카테고리에 새 검사 예외를 추가하려면 카테고리를 선택합니다.

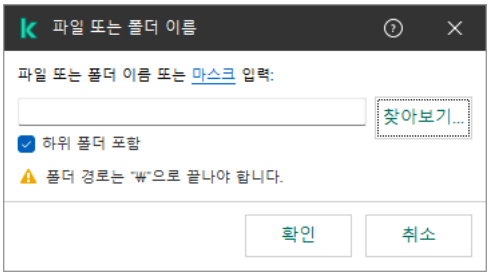
8. 파일 또는 폴더를 검사 대상에서 예외하려면 다음과 같이 하십시오.



예외 조건 설정

a. **속성** 블록에서 **파일 또는 폴더** 확인란을 선택합니다.

b. 아래 블록에서 링크를 클릭하여 **파일 또는 폴더 이름** 창을 엽니다.



파일 또는 폴더 선택

a. 파일 또는 폴더 이름이나 파일 또는 폴더 이름의 마스크를 입력하거나 **찾아보기**를 눌러 폴더 트리에서 파일 또는 폴더를 선택합니다.

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.

파일 경로 시작 부분, 중간 또는 끝 부분에서 마스크를 사용할 수 있습니다. 예를 들어, 모든 사용자용 폴더를 예외 조건에 추가하려면 `?:\Users\*\Folder\` 마스크를 입력합니다.

Kaspersky Endpoint Security는 환경 변수를 지원합니다

네트워크 폴더를 제외할 수 있습니다. 이렇게 하려면 네트워크 폴더의 경로를 직접 입력하십시오(예: `\\Network Share\*`).

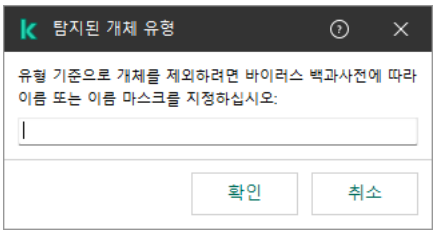
> Kaspersky Endpoint Security는 Kaspersky Security Center 콘솔을 사용하여 예외 규칙 목록을 생성할 때 `%userprofile%` 환경 변수를 지원하지 않습니다. 항목을 모든 사용자 계정에 적용하려면 `*` 문자를 사용할 수 있습니다(예: `C:\Users\*\Documents\File.exe`). 환경 변수를 새로 추가할 때마다 애플리케이션을 다시 시작해야 합니다.

b. 변경 사항을 저장합니다.

9. 특정 이름의 개체를 검사 대상에서 예외시키려면 다음과 같이 하십시오:

a. **속성** 블록에서 **탐지된 개체 유형** 확인란을 선택합니다.

b. 아래 블록에서 링크를 클릭하여 **탐지된 개체 유형** 창을 엽니다.



개체 선택

a. Kaspersky IT 백과사전(`Email-Worm`, `Rootkit`, `RemoteAdmin` 등)의 분류에 따라 개체 유형 이름을 입력합니다.

`?` 문자(단일 문자 대체) 및 `*` 문자(모든 문자 대체)와 함께 마스크를 사용할 수 있습니다. 예를 들어 `Client*` 마스크가 지정된 경우 Kaspersky Endpoint Security는 `Client-IRC` , `Client-P2P` 및 `Client-SMTP` 개체를 검사에서 제외합니다.

b. 변경 사항을 저장합니다.

10. 검사에서 개별 파일을 제외하려면 다음과 같이 하십시오.

    a. **속성** 블록에서 **개체 해시** 확인란을 선택합니다.

    b. 아래 블록에서 링크를 클릭하여 **개체 해시** 창을 엽니다.



파일 선택

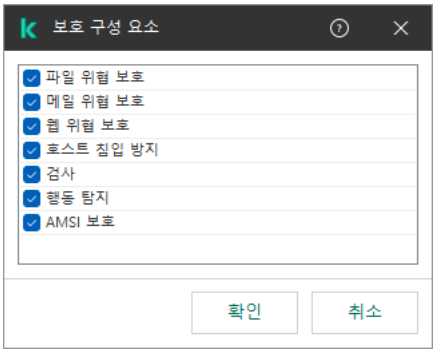
    a. 파일 해시를 입력하거나 **찾아보기** 버튼을 클릭하여 파일을 선택합니다.
    파일이 수정되면 파일 해시도 수정됩니다. 이 경우 수정된 파일이 예외 규칙에 추가되지 않습니다.

    b. 변경 사항을 저장합니다.

11. 필요하면, **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

12. 검사 예외를 사용해야 하는 Kaspersky Endpoint Security 구성 요소를 지정합니다:

    a. 아래 블록에 있는 링크를 클릭하여 **보호 구성 요소** 창을 엽니다.



보호 구성 요소 선택

    a. 검사 예외를 적용해야 하는 구성 요소 옆의 확인란을 선택합니다.
    구성 요소가 검사 예외 설정에 지정된 경우 해당 Kaspersky Endpoint Security구성 요소를 사용하여 검사할 동안에만 이 예외 규칙이 적용됩니다.
    구성 요소가 검사 예외 설정에 지정되지 않은 경우 해당 Kaspersky Endpoint Security 모든 구성 요소를 사용하여 검사할 동안에 이 예외 규칙이 적용됩니다.

13. **확인**을 누릅니다.
    새로운 예외가 목록에 추가됩니다. 개체 옆의 확인란을 사용해 언제든 예외를 비활성화할 수 있습니다.

14. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 검사 예외을 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **신뢰 구역** 섹션으로 이동합니다.
5. 창이 열리면 **악성 코드 검사 예외** 링크를 누릅니다.
6. 회사의 모든 컴퓨터에 대해 통합 예외 규칙 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 예외 규칙의 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 취소하면 Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 검사 예외 통합 목록을 숨깁니다.
8. **추가**를 클릭하고 작업을 선택합니다:
   - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.
   - **새로운 예외**. Kaspersky Endpoint Security가 새 검사 예외를 목록의 루트에 추가합니다.
   - **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 검사 예외*가 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 검사 예외가 추가되었습니다. 보호하는 서버의 용도에 따라 사전 정의된 검사 예외를 선택해야 합니다.

   특정 카테고리에 새로운 검사 예외를 추가하려면 해당 카테고리 옆의 확인란을 선택하고 **새로운 예외** 옵션을 선택합니다.
9. **파일 또는 폴더 경로**, **개체 유형**, **개체 해시** 등 예외 규칙을 추가할 방법을 선택합니다.
10. 파일이나 폴더를 검사에서 제외시키려면 경로를 직접 입력합니다. Kaspersky Endpoint Security는 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.

  네트워크 폴더를 제외할 수 있습니다. 이렇게 하려면 네트워크 폴더의 경로를 직접 입력하십시오(예: `\\Network Share\*`).

11. 특정 유형의 개체를 검사에서 제외하려면 **개체 유형** 필드에 Kaspersky Encyclopedia의 분류에 따라 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 Endpoint Security는 `Client-IRC` , `Client-P2P` 및 `Client-SMTP` 개체를 검사에서 제외합니다.

12. 개별 파일을 검사에서 제외하려면 **개체 해시** 필드에 파일 해시를 입력합니다.

    파일이 수정되면 파일 해시도 수정됩니다. 이 경우 수정된 파일이 예외 규칙에 추가되지 않습니다.

13. **예외 적용 대상** 블록에서 검사 예외을 적용할 구성 요소를 선택합니다.

14. 필요하면, **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

15. **확인**을 누릅니다.

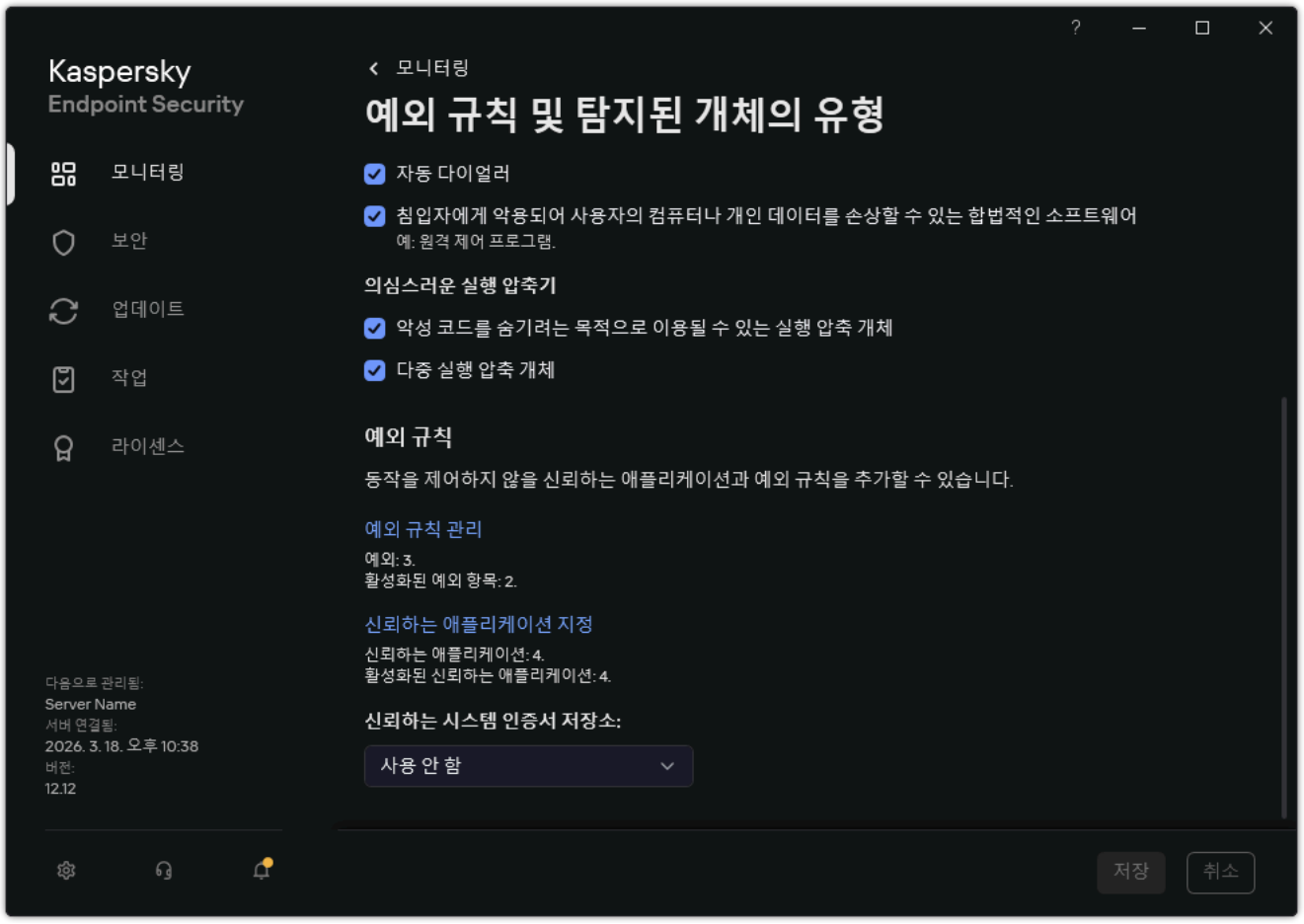
    새로운 예외가 목록에 추가됩니다. 토글을 사용하여 언제든지 예외를 중지할 수 있습니다.

16. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 검사 예외을 생성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **예외 규칙 및 탐지된 개체의 유형**을 선택합니다.
3. **예외 규칙** 블록에서 **예외 규칙 관리** 링크를 클릭합니다.

관리자가 콘솔에서 검사 예외 구성을 차단하고('닫힌 자물쇠' 기호) 로컬 검사 예외 항목이 금지된 경우(**로컬 예외 항목 사용 허용** 확인란이 선택 취소됨) Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 검사 예외 목록을 숨깁니다.



예외 설정

4. **추가**를 클릭하고 작업을 선택합니다:

   - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.
   - **새로운 예외**. Kaspersky Endpoint Security가 새 검사 예외를 목록의 루트에 추가합니다.
   - **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 검사 예외*가 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 검사 예외가 추가되었습니다. 보호하는 서버의 용도에 따라 사전 정의된 검사 예외를 선택해야 합니다.

   특정 카테고리에 새로운 검사 예외를 추가하려면 해당 카테고리 옆의 확인란을 선택하고 **새로운 예외** 옵션을 선택합니다.

5. 검사에서 파일 또는 폴더를 제외하려면 **찾아보기** 버튼을 클릭하여 파일 또는 폴더를 선택합니다.

경로를 수동으로 입력할 수도 있습니다. Kaspersky Endpoint Security는 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.

  네트워크 폴더를 제외할 수 있습니다. 이렇게 하려면 네트워크 폴더의 경로를 직접 입력하십시오(예: `\\Network Share\*`).

6. 특정 유형의 개체를 검사에서 제외하려면 **탐지된 개체 유형** 필드에 Kaspersky 백과사전의 분류에 따라 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 Endpoint Security는 `Client-IRC` , `Client-P2P` 및 `Client-SMTP` 개체를 검사에서 제외합니다.

7. 개별 파일을 검사에서 제외하려면 **개체 해시** 필드에 파일 해시를 입력합니다.

   파일이 수정되면 파일 해시도 수정됩니다. 이 경우 수정된 파일이 예외 규칙에 추가되지 않습니다.

8. **보호 구성 요소** 블록에서 검사 예외을 적용할 구성 요소를 선택합니다.

9. 필요하면, **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

10. 제외할 **활성** 상태를 선택합니다.

11. **추가**를 클릭합니다.

    새로운 예외가 목록에 추가됩니다. **상태** 열의 확인란을 사용해 언제든 예외를 비활성화할 수 있습니다.

12. 변경 사항을 저장합니다.



예외 목록

경로 마스크 예시:

절대 경로 대신 상대 경로를 지정하는 것이 좋습니다. 이렇게 하면 파일 시스템 개체뿐만 아니라 파일리스 개체도 제외할 수 있습니다. 예: `*\Program Files (x86)\Folder\Subfolder`.

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` 마스크는 `C:\dir\` 폴더에 있으며 EXE 확장자를 가진 파일에 대한 모든 경로를 포함하지만 `C:\dir\`의 하위 폴더는 포함하지 않습니다.
- `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` 마스크는 "dir" 이름을 가진 폴더에 있으며 EXE 확장자를 가진 파일에 대한 모든 경로를 포함하지만 그 하위 폴더는 포함하지 않습니다.
- `dir\test` 마스크는 "dir" 이름을 가진 폴더에 있으며 "test" 이름을 가진 파일에 대한 모든 경로를 포함하지만 그 하위 폴더는 포함하지 않습니다.

탐지된 개체 유형별 예외 생성

Kaspersky Endpoint Security는 탐지된 개체를 다음과 같이 분류합니다.

- **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(*Overwriting*) 바이러스는 감염된 파일 코드 위에 자신의 코드를 써서 파일의 컨텐츠를 지웁니다. 감염된 파일은 기능이 중지되며 복원할 수 없습니다. 기생(*Parasitic*) 바이러스는 파일을 수정한 다음 그냥 두거나 부분적으로만 기능하도록 둡니다. 동반(*Companion*) 바이러스는 파일을 수정하지는 않지만 자신의 복제를 만듭니다. 감염된 파일을 열면 바이러스의 복제가 시작됩니다. 다음과 같은 바이러스 유형 또한 발생됩니다: *링크(Link) 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 채팅(Internet Relay Chats)을 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.
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(랜섬웨어 포함)**

  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.
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.

유형	이름	설명
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).

유형	이름	설명
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.
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 Endpoint Security는 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 Endpoint Security는 압축된 파일을 검사합니다.

Kaspersky Endpoint Security는 기본적으로 모든 유형의 개체를 탐지합니다. 컴퓨터 보안을 개선하기 위해 모든 유형의 개체 탐지를 활성화된 상태로 유지할 것을 권장합니다. 애플리케이션이 악성으로 탐지한 사내 유틸리티를 사용하는 경우 이러한 유틸리티를 예외 목록에 추가하되, 전체 유형의 개체 탐지를 비활성화하지 마십시오.

관리 콘솔(MMC)에서 탐지 가능한 개체 유형을 선택하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **일반 설정 → 예외 및 개체 유형**을 선택합니다.
5. **탐지된 개체의 유형** 블록에서 **설정** 버튼을 클릭합니다.
6. 창이 열리면 Kaspersky Endpoint Security가 탐지할 개체 유형 옆의 확인란을 선택합니다.
7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

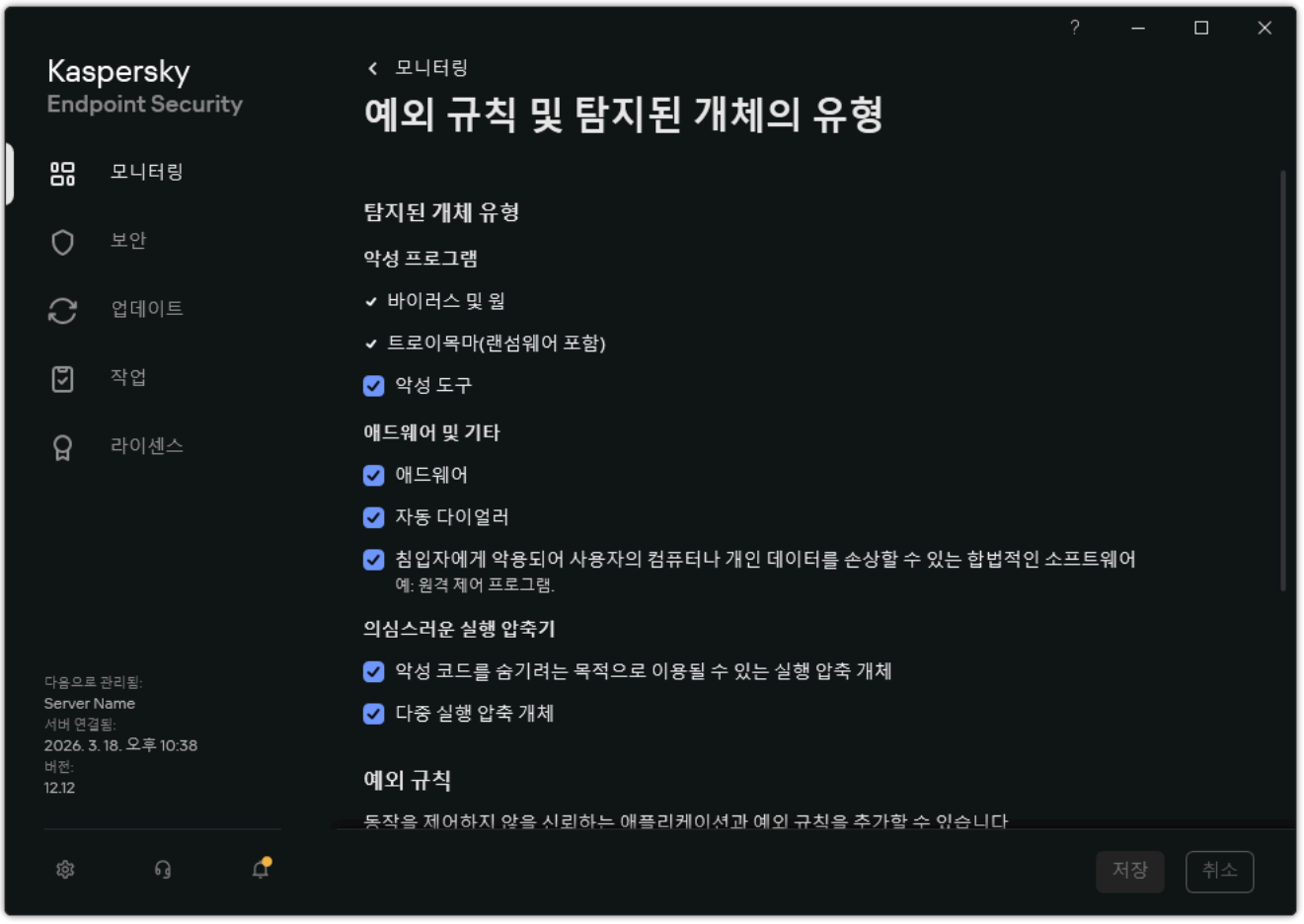
웹 콘솔 및 Cloud Console에서 탐지 가능한 개체 유형을 선택하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **탐지 설정**으로 이동합니다.
5. **다른 개체 유형 탐지** 블록에서 Kaspersky Endpoint Security에서 탐지된 개체 유형 옆의 확인란을 선택합니다.
6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 탐지 가능한 개체 유형을 선택하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **예외 규칙 및 탐지된 개체의 유형**을 선택합니다.
3. **탐지된 개체 유형** 블록에서 Kaspersky Endpoint Security에서 탐지된 개체 유형 옆의 확인란을 선택합니다.
4. 변경 사항을 저장합니다.



탐지된 개체 유형

신뢰하는 애플리케이션 목록 편집

*신뢰하는 애플리케이션 목록*은 Kaspersky Endpoint Security에서 파일 및 네트워크 활동(악성 활동 포함)과 시스템 레지스트리 접근을 감시하지 않는 애플리케이션 목록입니다. 기본적으로 Kaspersky Endpoint Security는 다른 애플리케이션 프로세스에서 열려 있거나 실행하거나 저장하는 개체를 검사하고 모든 애플리케이션 활동과 그로 인해 생성되는 네트워크 트래픽을 모니터링합니다. 신뢰하는 애플리케이션 목록에 애플리케이션이 추가되면 Kaspersky Endpoint Security는 애플리케이션 활동의 모니터링을 중단합니다.

검사 예외 및 신뢰하는 애플리케이션의 차이는 Kaspersky Endpoint Security가 검사 예외의 파일은 스캔하지 않지만 신뢰하는 애플리케이션의 경우 시작한 프로세스를 제어하지 않습니다. 신뢰하는 애플리케이션이 검사 예외에 포함되어 있지 않은 폴더에서 악성 파일을 생성할 경우, Kaspersky Endpoint Security는 파일을 감지하고 위험을 제거합니다. 폴더가 예외로 추가되면 Kaspersky Endpoint Security는 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, 의심으로 Kaspersky Endpoint Security에 의해 분류된 어떤 동작이 다수의 애플리케이션의 기능의 마우스 오른쪽 내에서 안전한 것으로 여기게 됩니다. 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 Endpoint Security와 다른 애플리케이션 사이의 호환성 문제를 방지합니다. 예를 들어, Kaspersky Endpoint Security와 다른 바이러스 방지 애플리케이션에서 제3자 컴퓨터가 네트워크 트래픽을 이중으로 스캔하는 문제를 방지합니다.

이렇게 해도 실행 파일과 신뢰하는 애플리케이션 프로세스에 대해서는 계속 바이러스와 기타 악성 코드 검사가 수행됩니다. 검사 예외를 사용하여 애플리케이션을 Kaspersky Endpoint Security 검사에서 완전히 예외시킬 수 있습니다.

신뢰하는 애플리케이션 목록의 변경은 부모 정책의 속성에 따라 차단될 수 있습니다. 목록을 변경하려면 웹 콘솔의 신뢰 구역('자물쇠'가 잠금 해제되어야 함) 설정 변경을 허용해야 합니다.

신뢰 구역은 관리 콘솔(MMC)과 웹 콘솔에서 다르게 그룹화됩니다. 마찬가지로, 신뢰 구역 파라미터의 변경을 방지하는 방법도 다릅니다('자물쇠'가 다름). 웹 콘솔만 사용하여 애플리케이션을 관리하는 것이 좋습니다. 서로 다른 콘솔에서 신뢰 구역을 구성하는 경우 관리 플러그인이 '자물쇠'를 기본 상태로 재설정할 수 있습니다.

관리 콘솔(MMC)의 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 **일반 설정 → 예외 및 개체 유형**을 선택합니다.
4. **검사 예외 및 신뢰하는 애플리케이션 → 신뢰하는 애플리케이션** 블록에서 **설정** 버튼을 누릅니다.
   신뢰하는 애플리케이션 목록이 포함된 창이 열립니다.
5. 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. 부모 정책의 신뢰하는 애플리케이션을 변경하거나 삭제할 수 없습니다.

6. 사용자가 신뢰하는 애플리케이션의 로컬 목록을 만들 수 있도록 하려면 **신뢰하는 로컬 애플리케이션 사용 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 취소하면 Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 신뢰하는 애플리케이션 통합 목록을 숨깁니다.

7. **추가**를 클릭하고 작업을 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 Endpoint Security가 신뢰하는 새로운 애플리케이션을 목록의 루트에 추가합니다.
   - **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 신뢰하는 애플리케이션*이 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 신뢰하는 애플리케이션이 추가되었습니다. 보호하는 서버의 용도에 따라 미리 정의된 신뢰하는 애플리케이션을 선택해야 합니다.
   - **선택한 카테고리에 대한 새로운 제외 사항**. 신뢰하는 새로운 애플리케이션을 특정 카테고리에 추가하려면 카테고리를 선택합니다.

8. 신뢰 기준을 선택합니다.

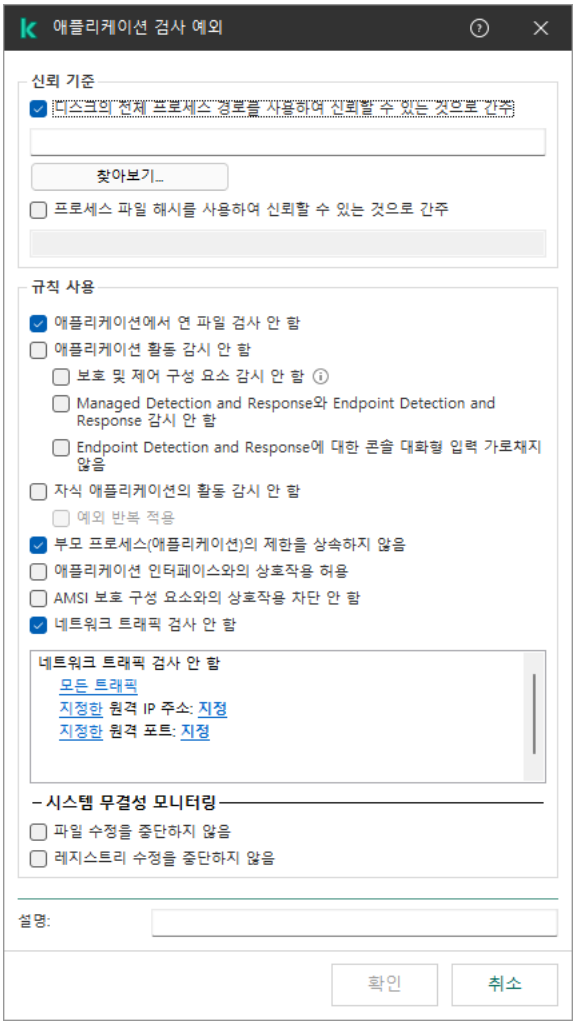
   - **디스크의 전체 프로세스 경로를 사용하여 신뢰할 수 있는 것으로 간주**. 신뢰하는 애플리케이션의 실행 파일 경로를 입력합니다.

     Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.

     Kaspersky Endpoint Security는 신뢰하는 애플리케이션의 파일 이름의 대소문자를 구분합니다. 입력하는 파일 이름의 대소문자가 잘못되면 Kaspersky Endpoint Security가 신뢰하는 애플리케이션을 인식하지 못합니다.

   - **프로세스 파일 해시를 사용하여 신뢰할 수 있는 것으로 간주**.

Kaspersky Endpoint Security는 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.



신뢰하는 애플리케이션 설정

9. 신뢰하는 애플리케이션에 대한 고급 설정을 구성합니다(아래 표 참조).

10. **확인**을 누릅니다.

    신뢰하는 새로운 애플리케이션이 목록에 추가됩니다. 개체 옆의 확인란을 사용하여 언제든지 신뢰 구역에서 애플리케이션을 제외할 수 있습니다.

11. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.



신뢰하는 애플리케이션 목록

웹 콘솔 및 Cloud Console의 신뢰하는 목록에 애플리케이션을 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **신뢰 구역** 섹션으로 이동합니다.

5. 열리는 창에서 **애플리케이션** 링크를 클릭합니다.
   신뢰하는 애플리케이션 목록이 포함된 창이 열립니다.

6. 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. 부모 정책의 신뢰하는 애플리케이션을 변경하거나 삭제할 수 없습니다.

7. 사용자가 신뢰하는 애플리케이션의 로컬 목록을 만들 수 있도록 하려면 **로컬 예외 항목 사용 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 취소하면 Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 신뢰하는 애플리케이션 통합 목록을 숨깁니다.

8. **추가**를 클릭하고 작업을 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 Endpoint Security가 신뢰하는 새로운 애플리케이션을 목록의 루트에 추가합니다.
   - **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 신뢰하는 애플리케이션*이 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 신뢰하는 애플리케이션이 추가되었습니다. 보호하는 서버의 용도에 따라 미리 정의된 신뢰하는 애플리케이션을 선택해야 합니다.

   새로운 신뢰하는 애플리케이션을 특정 카테고리에 추가하려면 해당 카테고리 옆의 확인란을 선택하고 **새로운 예외** 옵션을 선택합니다.

9. 신뢰 기준을 선택합니다.

   - **파일 또는 폴더 경로**. 신뢰하는 애플리케이션의 실행 파일 경로를 입력합니다.

     Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.

     Kaspersky Endpoint Security는 신뢰하는 애플리케이션의 파일 이름의 대소문자를 구분합니다. 입력하는 파일 이름의 대소문자가 잘못되면 Kaspersky Endpoint Security가 신뢰하는 애플리케이션을 인식하지 못합니다.

   - **애플리케이션 해시**.

   > Kaspersky Endpoint Security는 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.

10. 신뢰하는 애플리케이션에 대한 고급 설정을 구성합니다(아래 표 참조).

11. **확인**을 누릅니다.

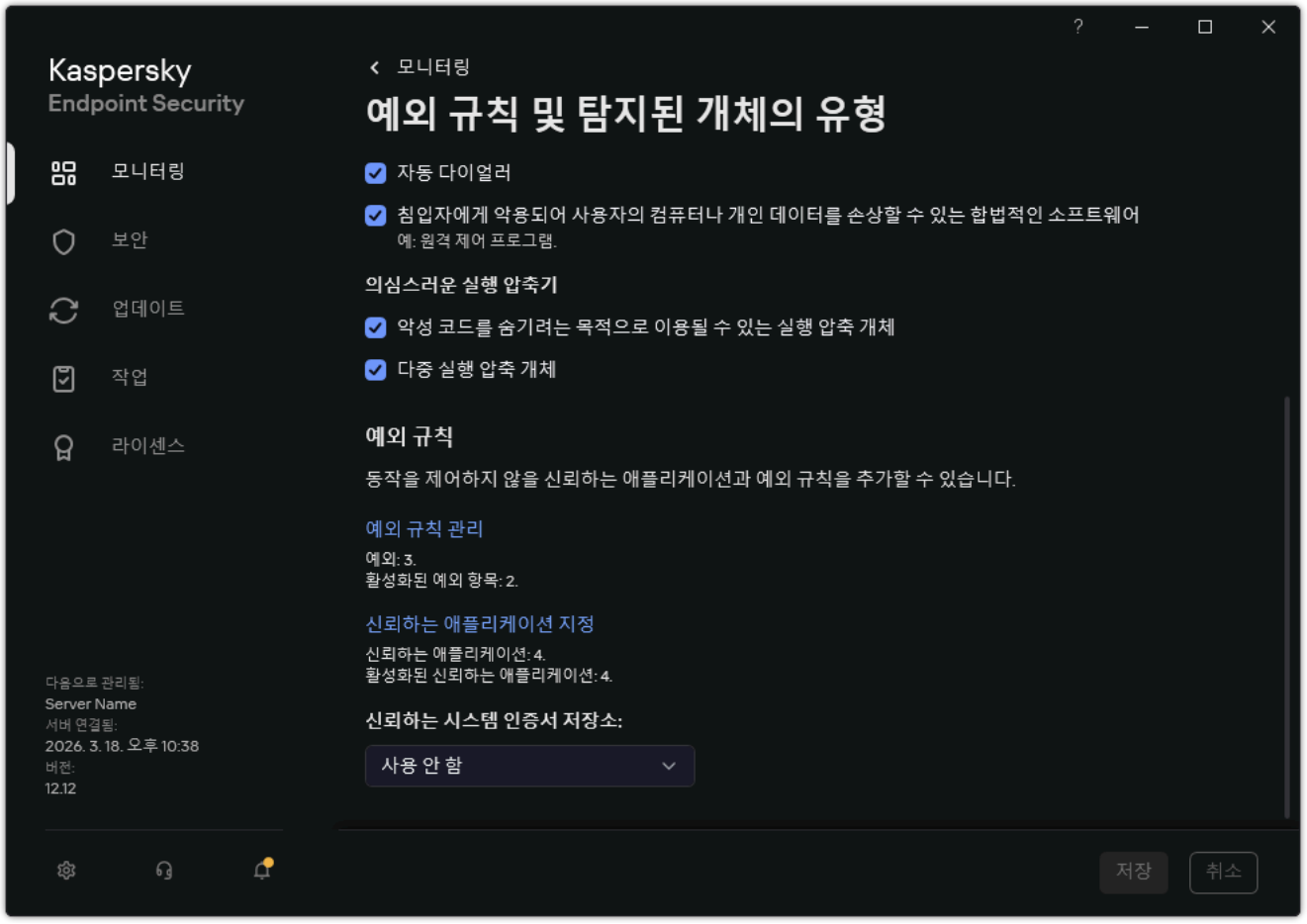
    신뢰하는 새로운 애플리케이션이 목록에 추가됩니다. **상태** 열의 확인란을 사용하여 언제든지 신뢰 구역에서 애플리케이션을 제외할 수 있습니다.

12. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 신뢰하는 목록에 애플리케이션을 추가하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정 → 예외 규칙 및 탐지된 개체의 유형**을 선택합니다.
3. **예외 규칙** 블록에서 **신뢰하는 애플리케이션 지정** 링크를 클릭합니다.

Kaspersky Endpoint Security 콘솔에서 관리자가 신뢰하는 애플리케이션 구성을 차단하고('닫힌 자물쇠' 기호) 신뢰하는 로컬 애플리케이션이 차단된 경우(**신뢰하는 로컬 애플리케이션 사용 허용** 확인란을 선택 취소함) Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 신뢰할 수 있는 애플리케이션의 통합 목록을 숨깁니다.



예외 설정

4. **추가**를 클릭하고 작업을 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 Endpoint Security가 신뢰하는 새로운 애플리케이션을 목록의 루트에 추가합니다.
   - **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 신뢰하는 애플리케이션*이 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 신뢰하는 애플리케이션이 추가되었습니다. 보호하는 서버의 용도에 따라 미리 정의된 신뢰하는 애플리케이션을 선택해야 합니다.

   새로운 신뢰하는 애플리케이션을 특정 카테고리에 추가하려면 해당 카테고리 옆의 확인란을 선택하고 **새로운 예외** 옵션을 선택합니다.

5. 신뢰 기준을 선택합니다.

   - **디스크의 전체 프로세스 경로를 사용하여 신뢰할 수 있는 것으로 간주**. 신뢰하는 애플리케이션의 실행 파일 경로를 입력합니다.

     Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.

Kaspersky Endpoint Security는 신뢰하는 애플리케이션의 파일 이름의 대소문자를 구분합니다. 입력하는 파일 이름의 대소문자가 잘못되면 Kaspersky Endpoint Security가 신뢰하는 애플리케이션을 인식하지 못합니다.

- **프로세스 파일 해시를 사용하여 신뢰할 수 있는 것으로 간주**.

Kaspersky Endpoint Security는 환경 변수를 지원하며 애플리케이션의 로컬 인터페이스 경로를 변환합니다. 즉, `%userprofile%\Documents\File.exe` 경로를 입력하면, Fred123 사용자의 애플리케이션 로컬 인터페이스에 `C:\Users\Fred123\Documents\File.exe` 기록이 추가됩니다. 따라서 Kaspersky Endpoint Security는 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. **확인**을 누릅니다.

   신뢰하는 새로운 애플리케이션이 목록에 추가됩니다. **상태** 열의 확인란을 사용하여 언제든지 신뢰 구역에서 애플리케이션을 제외할 수 있습니다.

8. 변경 사항을 저장합니다.



신뢰하는 애플리케이션 목록

파라미터	설명
애플리케이션에서 연 파일 검사 안 함	Kaspersky Endpoint Security의 검사에서 제외한 애플리케이션이 여는 모든 파일. 예를 들어, 애플리케이션을 사용하여 파일을 백업할 때 이 기능이 Kaspersky Endpoint Security의 리소스 소모를 줄이는 데 도움이 됩니다.
애플리케이션 활동 감시 안 함	Kaspersky Endpoint Security는 운영 체제에서 애플리케이션의 파일 및 네트워크 활동을 감시하지 않습니다. Kaspersky Endpoint Security의 여러 구성 요소에 대한 애플리케이션 활동 모니터를 구성할 수 있습니다. • **보호 및 제어 구성 요소 감시 안 함**. 애플리케이션 활동은 행동 탐지, 익스플로잇 방지, 호스트 침입 방지, 복원 엔진 및 방화벽 구성 요소가 감시합니다. • **Managed Detection and Response와 Endpoint Detection and Response 감시 안 함**. 애플리케이션 활동은 내장형 MDR 에이전트 및 내장형 EDR(KATA) 에이전트로 모니터링됩니다. • **Endpoint Detection and Response에 대한 콘솔 대화형 입력 가로채지 않음**. Kaspersky Endpoint Security는 콘솔에서 애플리케이션 관리에 대한 원격 측정 데이터를 전송하지 않습니다. 원격 측정 데이터는 Kaspersky Anti Targeted Attack Platform(EDR)에서 사용됩니다.
자녀 애플리케이션의 활동 감시 안 함	Kaspersky Endpoint Security는 이 애플리케이션이 시작한 애플리케이션의 파일 활동 또는 네트워크 활동을 모니터링하지 않습니다. 예외를 반복 적용할 수 있습니다. 따라서 애플리케이션은 전체 자식 애플리케이션 체인 활동을 모니터링하지 않습니다.
부모 프로세스(애플리케이션)의 제한을 상속하지 않음	Kaspersky Endpoint Security는 부모 프로세스에 대해 구성된 제한을 자식 프로세스에 적용하지 않습니다. 부모 프로세스는 애플리케이션 권한(호스트 침입 방지) 및 애플리케이션 네트워크 규칙(방화벽)이 구성된 애플리케이션에 의해 시작됩니다.
자녀 애플리케이션의 활동 감시 안 함	Kaspersky Endpoint Security는 이 애플리케이션이 시작한 애플리케이션의 파일 활동 또는 네트워크 활동을 모니터링하지 않습니다. 예외를 반복 적용할 수 있습니다. 따라서 애플리케이션은 전체 자식 애플리케이션 체인 활동을 모니터링하지 않습니다.
애플리케이션 인터페이스와의 상호작용 허용	Kaspersky Endpoint Security의 자기 보호는 원격 컴퓨터에서 애플리케이션 서비스를 관리하려는 모든 시도를 차단합니다. 이 확인란을 선택하면 원격 접속 애플리케이션이 Kaspersky Endpoint Security 인터페이스를 통해 Kaspersky Endpoint Security 설정을 관리할 수 있습니다.
AMSI 보호 구성 요소와의 상호작용 차단 안 함	Kaspersky Endpoint Security는 AMSI 보호 구성 요소에서 검사할 개체에 대한 신뢰하는 애플리케이션의 요청을 감시하지 않습니다.
네트워크 트래픽 검사 안 함	애플리케이션이 시작한 네트워크 트래픽은 Kaspersky Endpoint Security의 검사에서 제외됩니다. 모든 트래픽을 검사에서 제외하거나 암호화된 트래픽만 제외할 수 있습니다. 스캔에서 개별 IP 주소 및 포트 번호를 제외할 수도 있습니다. 해시가 경로가 아닌 신뢰하는 애플리케이션에 대해 지정된 경우 애플리케이션은 네트워크 트래픽 예외를 지원하지 않습니다.
파일 수정을 중단하지 않음 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	Kaspersky Endpoint Security가 시스템 무결성 모니터링 모니터링 범위에서 파일의 변경 사항을 모니터링하지 않습니다. 애플리케이션이 모든 시스템 무결성 모니터링 모드에 예외를 적용합니다. 실시간 시스템 무결성 모니터링 및 온디맨드 시스템 무결성 검사.
레지스트리 수정을 중단하지 않음 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	Kaspersky Endpoint Security가 시스템 무결성 모니터링 모니터링 범위에서 레지스트리 키의 변경 사항을 모니터링하지 않습니다. 애플리케이션이 모든 시스템 무결성 모니터링 모드에 예외를 적용합니다. 실시간 시스템 무결성 모니터링 및 온디맨드 시스템 무결성 검사.
설명	필요에 따라 신뢰하는 애플리케이션 대한 간단한 설명을 제공할 수 있습니다. 설명을 추가하면 신뢰하는 애플리케이션을 검색하고 정렬하는 데 도움이 됩니다.
상태	신뢰하는 애플리케이션 상태: • **활성** 상태는 애플리케이션이 신뢰 구역에 포함됨을 의미합니다. • **비활성** 상태는 애플리케이션이 신뢰 구역에서 제외됨을 의미합니다.

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. 그렇게 하려면 정책의 **예외** 섹션에서 **로컬 예외 항목 사용 허용** 확인란과 **신뢰하는 로컬 애플리케이션 사용 허용** 확인란을 선택합니다.

관리자가 로컬 신뢰 구역 생성을 허용한 경우 사용자는 애플리케이션의 사용자 인터페이스에서 자신의 검사 예외 항목과 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 Endpoint Security는 애플리케이션의 사용자 인터페이스에서 검사 예외 및 신뢰하는 애플리케이션의 목록을 숨깁니다.

관리 콘솔(MMC)의 로컬 신뢰 구역에 개체를 추가하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **기기** 탭을 선택합니다.
4. 더블 클릭해 컴퓨터 속성 창을 엽니다.
5. 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.
6. 컴퓨터에 설치된 Kaspersky 애플리케이션 목록에서 **Kaspersky Endpoint Security for Windows (14.0)**를 선택하고 더블 클릭하여 애플리케이션 속성을 엽니다.
7. 애플리케이션 설정 창에서 **일반 설정** → **예외 및 개체 유형**을 선택합니다.
8. **검사 예외 및 신뢰하는 애플리케이션** → **로컬 검사 예외 항목** 블록에서 **설정** 버튼을 누릅니다.

   로컬 예외 규칙 목록이 포함된 창이 열립니다.



신뢰 구역 설정

9. 로컬 검사 예외 항목을 만드세요.

   로컬 검사 예외 항목 생성 규칙은 일반 예외 항목 생성 규칙과 동일합니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 * 및 ? 문자를 지원합니다.

10. **검사 예외 및 신뢰하는 애플리케이션** → **신뢰하는 로컬 애플리케이션** 블록에서 **설정** 버튼을 누릅니다.

    신뢰하는 로컬 애플리케이션 목록을 포함한 창이 열립니다.

11. 신뢰하는 로컬 애플리케이션 목록을 만듭니다.

    신뢰하는 로컬 애플리케이션 목록에 애플리케이션을 추가하는 규칙은 일반 목록에 애플리케이션을 추가하는 규칙과 동일합니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 * 및 ? 문자를 지원합니다.

12. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console의 로컬 신뢰 구역에 개체를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)**를 선택합니다.
2. 사용자가 차단된 동작을 수행하도록 허용할 컴퓨터 이름을 클릭합니다.
3. **애플리케이션** 탭을 선택합니다.
4. **Kaspersky Endpoint Security for Windows**를 누릅니다.

   그러면 로컬 애플리케이션 설정이 열립니다.

5. **애플리케이션 설정** 탭을 선택합니다.
6. 애플리케이션 설정 창에서 **일반 설정** → **예외 규칙 및 탐지된 개체의 유형**을 선택합니다.
7. **검사 예외 및 신뢰하는 애플리케이션** 블록에서 **로컬 검사 예외 항목** 링크를 누릅니다.
8. 로컬 검사 예외 항목을 만드세요.

   로컬 예외 항목 생성 규칙은 일반 예외 항목 생성 규칙과 같습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 * 및 ? 문자를 지원합니다.

9. **검사 예외 및 신뢰하는 애플리케이션** 블록에서 **신뢰하는 로컬 애플리케이션** 링크를 누릅니다.
10. 신뢰하는 로컬 애플리케이션 목록을 만듭니다.

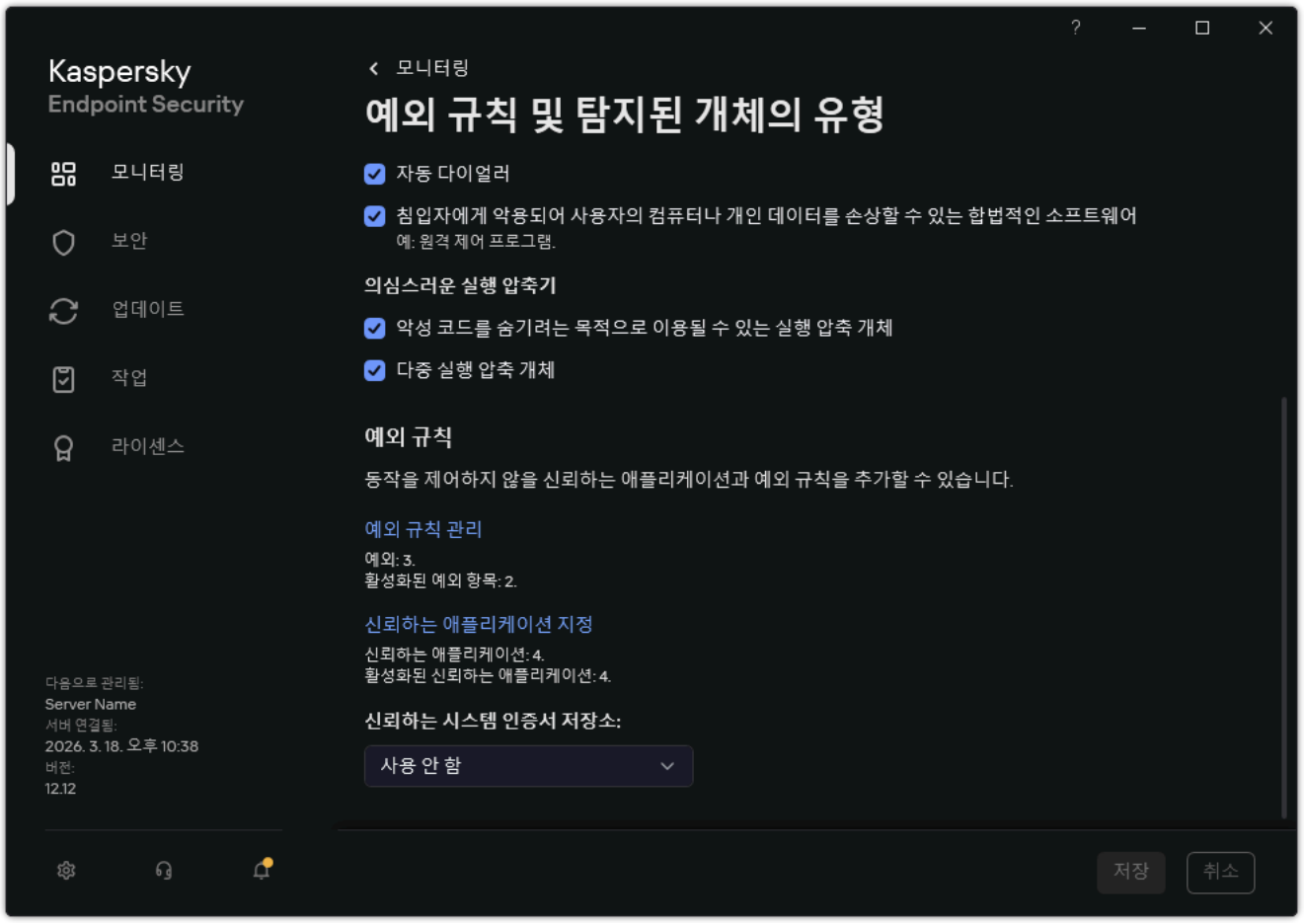
    신뢰하는 로컬 애플리케이션 목록에 애플리케이션을 추가하는 규칙은 일반 목록에 애플리케이션을 추가하는 규칙과 동일합니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 * 및 ? 문자를 지원합니다.

11. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 로컬 검사 예외 항목을 생성하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **예외 규칙 및 탐지된 개체의 유형**을 선택합니다.
3. **예외 규칙** 블록에서 **예외 규칙 관리** 링크를 클릭합니다.

관리자가 콘솔에서 검사 예외 구성을 차단하고('닫힌 자물쇠' 기호) 로컬 검사 예외 항목이 금지된 경우(**로컬 예외 항목 사용 허용** 확인란이 선택 취소됨) Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 검사 예외 목록을 숨깁니다.



예외 설정

4. **추가**를 클릭하고 작업을 선택합니다:

   - **카테고리**. 검사 예외는 별도의 카테고리로 그룹화할 수 있습니다. 새 카테고리를 생성하려면 카테고리 이름을 입력하고 카테고리에 하나 이상의 검사 예외를 추가합니다.
   - **새로운 예외**. Kaspersky Endpoint Security가 새 검사 예외를 목록의 루트에 추가합니다.
   - **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 검사 예외*가 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 검사 예외가 추가되었습니다. 보호하는 서버의 용도에 따라 사전 정의된 검사 예외를 선택해야 합니다.

   특정 카테고리에 새로운 검사 예외를 추가하려면 해당 카테고리 옆의 확인란을 선택하고 **새로운 예외** 옵션을 선택합니다.

5. 검사에서 파일 또는 폴더를 제외하려면 **찾아보기** 버튼을 클릭하여 파일 또는 폴더를 선택합니다.

경로를 수동으로 입력할 수도 있습니다. Kaspersky Endpoint Security는 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.

  네트워크 폴더를 제외할 수 있습니다. 이렇게 하려면 네트워크 폴더의 경로를 직접 입력하십시오(예: `\\Network Share\*`).

6. 특정 유형의 개체를 검사에서 제외하려면 **탐지된 개체 유형** 필드에 Kaspersky 백과사전의 분류에 따라 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 Endpoint Security는 `Client-IRC` , `Client-P2P` 및 `Client-SMTP` 개체를 검사에서 제외합니다.

7. 개별 파일을 검사에서 제외하려면 **개체 해시** 필드에 파일 해시를 입력합니다.

   파일이 수정되면 파일 해시도 수정됩니다. 이 경우 수정된 파일이 예외 규칙에 추가되지 않습니다.

8. **보호 구성 요소** 블록에서 검사 예외을 적용할 구성 요소를 선택합니다.

9. 필요하면, **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

10. 제외할 **활성** 상태를 선택합니다.

11. **추가**를 클릭합니다.

    새로운 예외가 목록에 추가됩니다. **상태** 열의 확인란을 사용해 언제든 예외를 비활성화할 수 있습니다.

12. 변경 사항을 저장합니다.

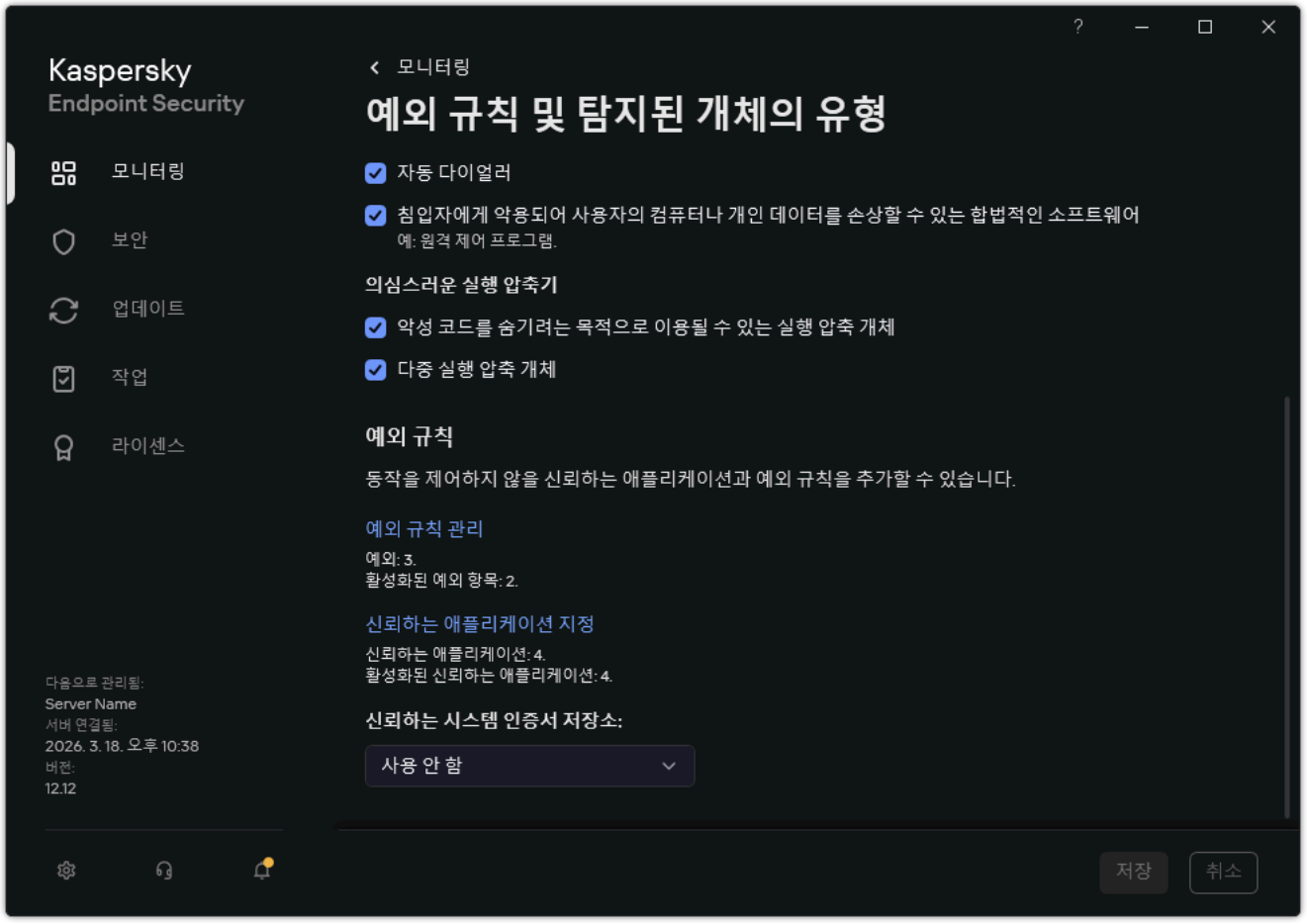


예외 목록

애플리케이션 인터페이스에서 신뢰하는 로컬 애플리케이션 목록에 애플리케이션을 추가하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **예외 규칙 및 탐지된 개체의 유형**을 선택합니다.
3. **예외 규칙** 블록에서 **신뢰하는 애플리케이션 지정** 링크를 클릭합니다.

Kaspersky Endpoint Security 콘솔에서 관리자가 신뢰하는 애플리케이션 구성을 차단하고('닫힌 자물쇠' 기호) 신뢰하는 로컬 애플리케이션이 차단된 경우(**신뢰하는 로컬 애플리케이션 사용 허용** 확인란을 선택 취소함) Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 신뢰할 수 있는 애플리케이션의 통합 목록을 숨깁니다.



예외 설정

4. **추가**를 클릭하고 작업을 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 Endpoint Security가 신뢰하는 새로운 애플리케이션을 목록의 루트에 추가합니다.
   - **목록에서 예외 항목 선택**. SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있도록 애플리케이션에 *사전 정의된 신뢰하는 애플리케이션*이 포함되어 있습니다. 또한 Citrix 및 VMware 가상 환경에서 애플리케이션 설정을 지원하기 위해 사전 정의된 신뢰하는 애플리케이션이 추가되었습니다. 보호하는 서버의 용도에 따라 미리 정의된 신뢰하는 애플리케이션을 선택해야 합니다.

   새로운 신뢰하는 애플리케이션을 특정 카테고리에 추가하려면 해당 카테고리 옆의 확인란을 선택하고 **새로운 예외** 옵션을 선택합니다.

5. 신뢰 기준을 선택합니다.

   - **디스크의 전체 프로세스 경로를 사용하여 신뢰할 수 있는 것으로 간주**. 신뢰하는 애플리케이션의 실행 파일 경로를 입력합니다.

     Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.

Kaspersky Endpoint Security는 신뢰하는 애플리케이션의 파일 이름의 대소문자를 구분합니다. 입력하는 파일 이름의 대소문자가 잘못되면 Kaspersky Endpoint Security가 신뢰하는 애플리케이션을 인식하지 못합니다.

- **프로세스 파일 해시를 사용하여 신뢰할 수 있는 것으로 간주**.

Kaspersky Endpoint Security는 환경 변수를 지원하며 애플리케이션의 로컬 인터페이스 경로를 변환합니다. 즉, `%userprofile%\Documents\File.exe` 경로를 입력하면, Fred123 사용자의 애플리케이션 로컬 인터페이스에 `C:\Users\Fred123\Documents\File.exe` 기록이 추가됩니다. 따라서 Kaspersky Endpoint Security는 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. **확인**을 누릅니다.

   신뢰하는 새로운 애플리케이션이 목록에 추가됩니다. **상태** 열의 확인란을 사용하여 언제든지 신뢰 구역에서 애플리케이션을 제외할 수 있습니다.

8. 변경 사항을 저장합니다.



신뢰하는 애플리케이션 목록

신뢰 구역 내보내기 및 가져오기

*신뢰 구역*은 Kaspersky Endpoint Security에서 감시하지 않는 개체 및 애플리케이션을 시스템 관리자가 구성한 목록입니다. 신뢰 구역은 *검사 예외*와 *신뢰하는 애플리케이션*으로 구성됩니다. 이 목록은 XML 파일 및 기타 형식으로 내보낼 수 있습니다. 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 *제외 목록*에 내보내기 및 가져오기에 다음 형식을 사용합니다:

- XML은 관리 콘솔(MMC), 웹 콘솔, Cloud Console에서 사용할 수 있습니다.
- DAT는 관리 콘솔(MMC)에서만 가져올 수 있습니다. 이 형식의 목적은 애플리케이션의 이전 버전과의 호환성을 유지하는 것입니다. 관리 콘솔(MMC)에서 DAT 파일을 XML로 변환하여 제외 목록을 웹 콘솔로 마이그레이션할 수 있습니다.
- CSV는 애플리케이션의 로컬 인터페이스에서만 사용할 수 있습니다.

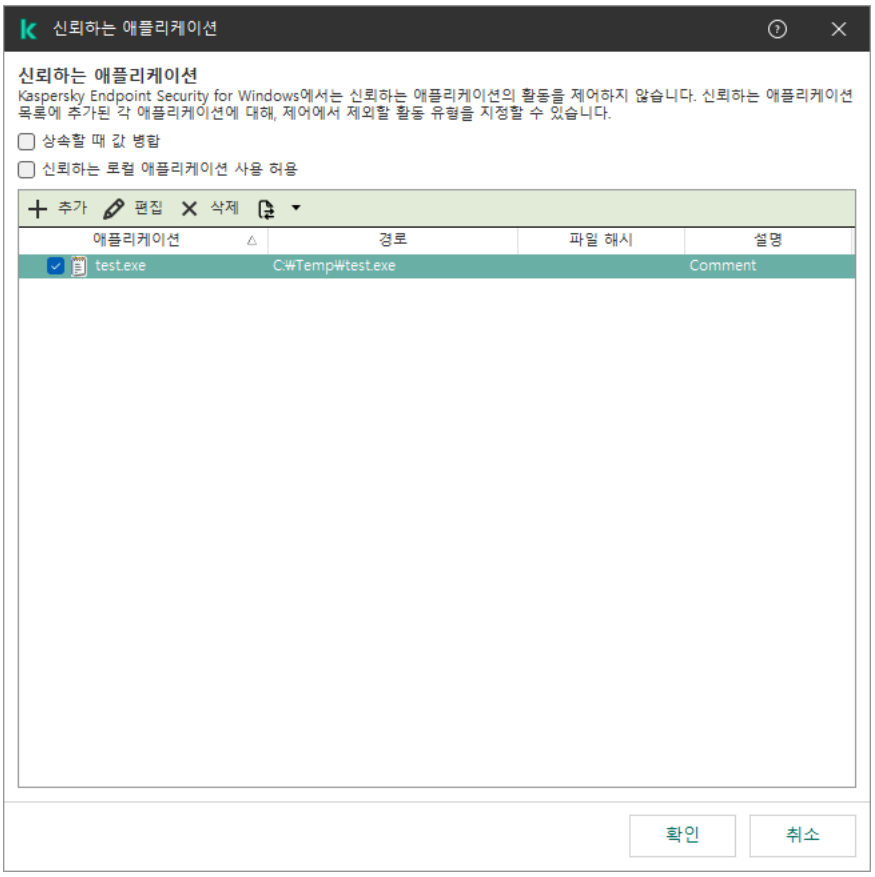
Kaspersky Endpoint Security는 *신뢰하는 애플리케이션 목록*의 내보내기 및 가져오기에 XML 형식을 사용합니다.

관리 콘솔(MMC)에서 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 **일반 설정 → 예외 및 개체 유형**을 선택합니다.
4. **검사 예외 및 신뢰하는 애플리케이션**에서 내보내거나 가져올 신뢰 구역의 구성 요소를 선택합니다. **검사 예외** 또는 **신뢰하는 애플리케이션**.
5. **설정**을 클릭합니다.
6. 규칙 목록을 내보내려면 다음을 수행합니다.
   a. 내보낼 예외 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
   예외 규칙을 아무 것도 선택하지 않으면 Kaspersky Endpoint Security가 모든 예외 규칙을 내보냅니다.
   b. → **내보내기** 버튼을 클릭합니다.
   c. 창이 열리면 예외 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

d. 파일을 저장합니다.

Kaspersky Endpoint Security는 예외 규칙의 전체 목록을 XML 파일로 내보냅니다. Kaspersky Endpoint Security에서 예외 목록을 DAT 파일로 내보낼 수도 있습니다.



신뢰하는 애플리케이션 목록

7. 예외 목록을 가져오려면 다음을 수행합니다.

a. → **가져오기** 버튼을 클릭합니다.

b. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.

c. 파일을 엽니다.

컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다. Kaspersky Endpoint Security는 DAT 파일에서 예외 목록을 가져올 수도 있습니다.

8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 신뢰 구역을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **신뢰 구역** 섹션으로 이동합니다.

5. 규칙 목록을 내보내려면 다음을 수행합니다.

   a. **악성 코드 검사 예외** 링크를 누릅니다.

   b. 내보낼 예외 규칙을 선택합니다.

   c. → **내보내기** 버튼을 클릭합니다.

      Kaspersky Endpoint Security는 예외 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.

6. 신뢰하는 애플리케이션 목록을 내보내려면 다음을 수행합니다.

   a. 내보낼 신뢰하는 애플리케이션을 선택합니다.

   b. → **내보내기** 버튼을 클릭합니다.

      Kaspersky Endpoint Security는 신뢰하는 애플리케이션 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.

7. 예외 목록을 가져오려면 다음을 수행합니다.

   a. **악성 코드 검사 예외** 링크를 누릅니다.

   b. → **가져오기** 버튼을 클릭합니다.

      창이 열리면 예외 규칙 목록을 가져올 JSON 파일을 선택합니다.

   c. 파일을 엽니다.

      컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. 신뢰하는 애플리케이션 목록을 가져오려면 다음을 수행합니다.

   a. **애플리케이션** 링크를 클릭합니다.

   b. → **가져오기** 버튼을 클릭합니다.

      창이 열리면 신뢰하는 애플리케이션 목록을 가져올 JSON 파일을 선택합니다.

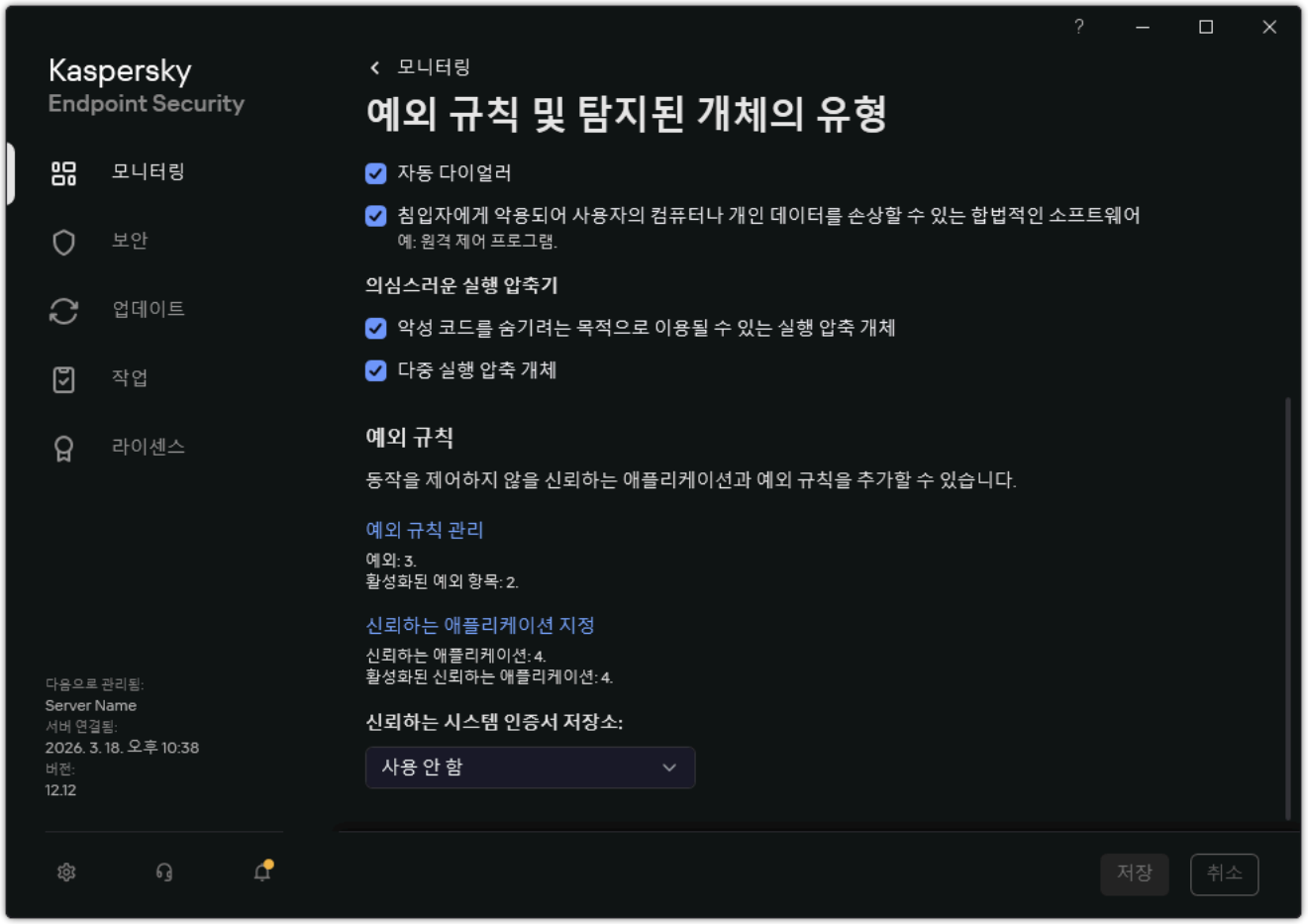
   c. 파일을 엽니다.

      컴퓨터에 이미 신뢰하는 애플리케이션 목록이 있는 경우 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.

9. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 신뢰 구역을 내보내거나 가져오는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **예외 규칙 및 탐지된 개체의 유형**을 선택합니다.



예외 설정

3. 규칙 목록을 내보내려면 다음을 수행합니다.
   a. **예외 규칙** 블록에서 **예외 규칙 관리** 링크를 클릭합니다.
   b. 내보낼 예외 규칙을 선택합니다.
   c. **내보내기**를 클릭합니다.
   d. 선택한 예외 규칙만 내보낼 것인지 전체 예외 규칙 목록을 내보낼 것인지 확인합니다.
   e. 창이 열리면 예외 규칙 목록을 내보낼 CSV 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

f. 파일을 저장합니다.

Kaspersky Endpoint Security는 예외 규칙의 전체 목록을 CSV 파일로 내보냅니다.



예외 목록

4. 신뢰하는 애플리케이션 목록을 내보내려면 다음을 수행합니다.

a. **예외 규칙** 블록에서 **신뢰하는 애플리케이션 지정** 링크를 클릭합니다.

b. 내보낼 신뢰하는 애플리케이션을 선택합니다.

c. **내보내기**를 클릭합니다.

d. 선택한 신뢰하는 애플리케이션만 내보낼 것인지 전체 목록을 내보낼 것인지 확인하십시오.

e. 창이 열리면 신뢰하는 애플리케이션 목록을 내보낼 XML 파일의 이름을 입력하고 이 파일을 저장할 폴더를 선택합니다.

f. 파일을 저장합니다.

Kaspersky Endpoint Security는 신뢰하는 애플리케이션의 전체 목록을 XML 파일로 내보냅니다.



신뢰하는 애플리케이션 목록

5. 예외 목록을 가져오려면 다음을 수행합니다.

a. **예외 규칙** 블록에서 **예외 규칙 관리** 링크를 클릭합니다.

b. **가져오기**를 클릭합니다.

c. 창이 열리면 예외 규칙 목록을 가져올 CSV 파일을 선택합니다.

d. 파일을 엽니다.

컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 CSV 파일에 새 항목을 추가하라는 메시지를 표시합니다.

6. 신뢰하는 애플리케이션 목록을 가져오려면 다음을 수행합니다.

a. **예외 규칙** 블록에서 **신뢰하는 애플리케이션 지정** 링크를 클릭합니다.

b. **가져오기**를 클릭합니다.

c. 창이 열리면 신뢰하는 애플리케이션 목록을 가져올 XML 파일을 선택합니다.

d. 파일을 엽니다.

컴퓨터에 이미 신뢰하는 애플리케이션 목록이 있는 경우 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 변경 사항을 저장합니다.

신뢰하는 디지털 서명으로 애플리케이션 처리

시스템 인증서 저장소를 사용하면 신뢰하는 디지털 서명으로 서명된 애플리케이션을 바이러스 검사에서 예외할 수 있습니다. Kaspersky Endpoint Security는 이러한 애플리케이션을 *신뢰하는* 그룹에 자동으로 할당합니다.

애플리케이션 콘솔(MMC)에서 신뢰하는 시스템 인증서 저장소 사용을 시작하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 예외 및 개체 유형**을 선택합니다.
4. **신뢰하는 시스템 인증서 저장소** 블록에서 **신뢰하는 시스템 인증서 저장소 사용** 확인란을 선택합니다.
5. 드롭다운 목록에서 Kaspersky Endpoint Security가 신뢰하는 것으로 간주해야 하는 시스템 저장소를 선택합니다.
6. 변경 사항을 저장합니다.

웹 콘솔 및 클라우드 콘솔에서 신뢰하는 시스템 인증서 저장소 사용을 시작하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **신뢰 구역** 섹션으로 이동합니다.
5. 열리는 창에서 **신뢰하는 인증서** 링크를 클릭합니다.
6. 열리는 창에서 **신뢰하는 시스템 인증서 저장소 사용** 확인란을 선택합니다.
7. Kaspersky Endpoint Security가 신뢰하는 것으로 간주해야 하는 시스템 저장소를 선택합니다.
8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 신뢰하는 시스템 인증서 저장소 사용을 시작하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정 → 예외 규칙 및 탐지된 개체의 유형**을 선택합니다.

3. **신뢰하는 시스템 인증서 저장소** 드롭다운 목록에서 Kaspersky Endpoint Security가 신뢰하는 것으로 간주해야 하는 시스템 저장소를 선택합니다.

4. 변경 사항을 저장합니다.

부록. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션

Kaspersky Endpoint Security 12.6 for Windows부터 검사 예외 및 신뢰하는 애플리케이션 이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다. Kaspersky Endpoint Security 12.8 for Windows부터 가상 환경 보호를 위한 Light Agent 모드로 애플리케이션을 설치할 수 있습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다.

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

SQL 서버

SQL Server에 Kaspersky Endpoint Security를 설치할 때는 서버 동작에 방해가 되지 않도록 사전 정의된 예외 규칙 및 신뢰하는 애플리케이션에서 신뢰 구역을 생성해야 합니다.

사전 정의된 검사 예외

경로	SQL 버전
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012

경로	SQL 버전
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange 서버

Microsoft Exchange 서버에 Kaspersky Endpoint Security를 설치할 때는 서버 동작에 방해가 되지 않도록 사전 정의된 예외 규칙 및 신뢰하는 애플리케이션에서 신뢰 구역을 생성해야 합니다.

사전 정의된 검사 예외

경로	Microsoft Exchange 버전
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

사전 정의된 신뢰하는 애플리케이션

경로	Microsoft Exchange 버전
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

System Center Configuration Manager

사전 정의된 검사 예외

경로	System Center Configuration Manager 버전
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Citrix 가상 환경에 Kaspersky Endpoint Security를 설치할 때는 서버 동작에 방해가 되지 않도록 사전 정의된 예외 규칙 및 신뢰하는 애플리케이션에서 신뢰 구역을 생성해야 합니다.

사전 정의된 검사 예외

경로
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt

경로
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

사전 정의된 신뢰하는 애플리케이션

경로	Citrix 솔루션
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Virtual Apps and Desktops
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Virtual Apps and Desktops
%SystemRoot%\System32\drivers\CVhdFilter.sys	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Virtual Apps and Desktops

경로	Citrix 솔루션
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Workspace app

경로	Citrix 솔루션
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Workspace app
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisioning
%SystemRoot%\System32\drivers\bnistack6.sys	Provisioning
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisioning
%SystemRoot%\System32\drivers\cnicteam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisioning
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

VMware 가상 환경에 Kaspersky Endpoint Security를 설치할 때는 서버 동작에 방해가 되지 않도록 사전 정의된 예외 규칙 및 신뢰하는 애플리케이션에서 신뢰 구역을 생성해야 합니다.

사전 정의된 신뢰하는 애플리케이션

경로	VMware 솔루션
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon

경로	VMware 솔루션
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

백업 저장소 관리

*백업*은 치료하는 동안 삭제되거나 수정된 파일의 백업 복사본을 보존합니다. *백업 복사본*은 파일을 치료 또는 삭제하기 전에 생성되는 파일 복사본입니다. 파일의 백업 복사본은 특별한 형식으로 저장되며 위험하지 않습니다.

파일의 백업 복사본은 `C:\ProgramData\Kaspersky Lab\KES.14.0\QB` 폴더에 저장됩니다.

관리자 그룹 내 사용자는 이 폴더에 대한 접근 권한이 부여됩니다. Kaspersky Endpoint Security를 설치할 때 사용된 계정의 사용자는 이 폴더에 대한 제한된 접근 권한이 부여됩니다.

Kaspersky Endpoint Security는 파일의 백업 복사본에 대한 사용자 접근 권한을 구성하는 기능을 제공하지 않습니다.

치료 중 파일의 무결성을 유지할 수 없는 경우도 있습니다. 치료 후 해당 파일의 중요 정보에 부분적으로 또는 완전히 접근하지 못하는 경우 백업 복사본의 파일을 원래 폴더로 복원할 수 있습니다.

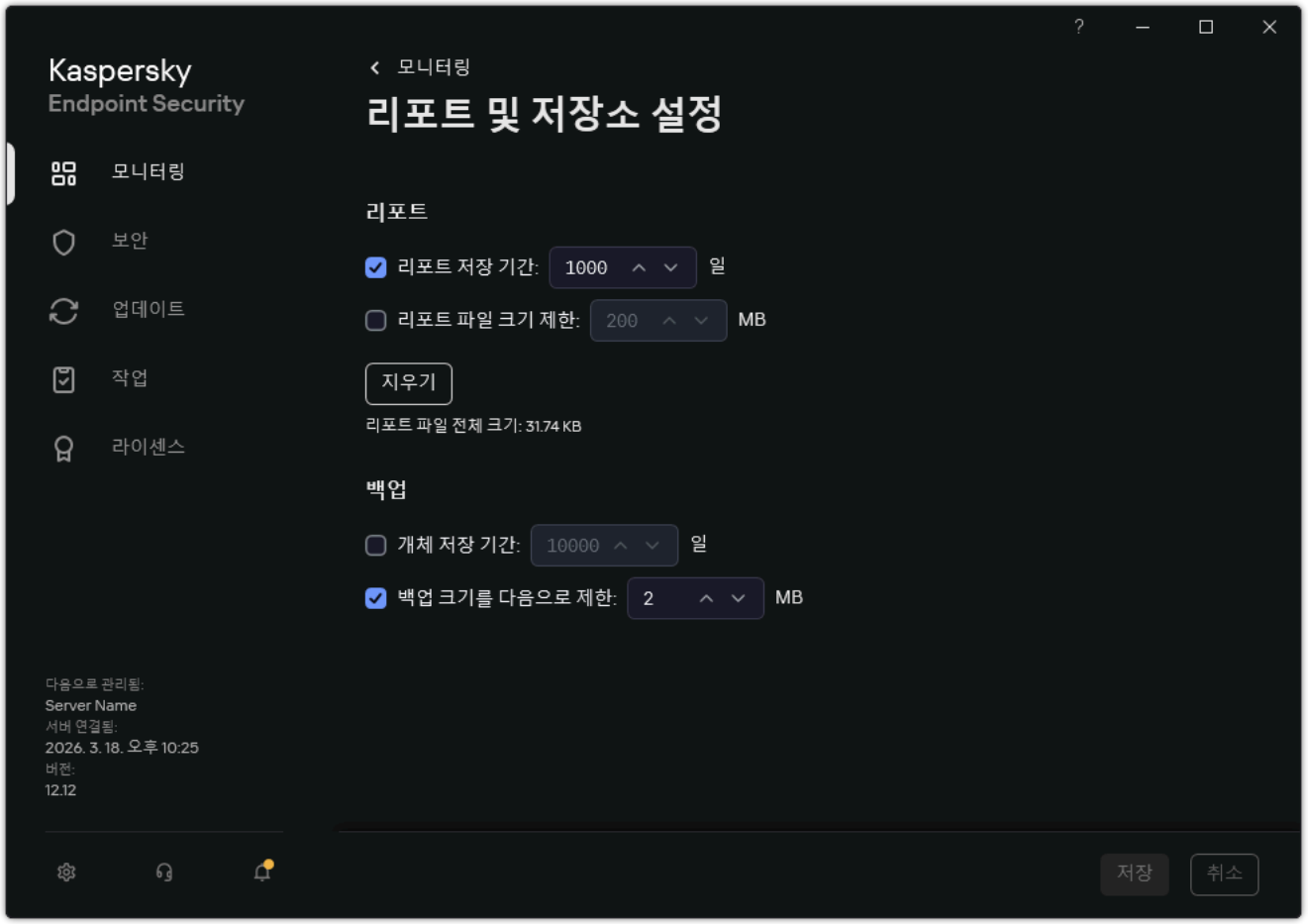
Kaspersky Endpoint Security가 Kaspersky Security Center의 관리 하에 실행 중일 경우, 파일의 백업 복사본이 Kaspersky Security Center 중앙 관리 서버로 전송될 수 있습니다. Kaspersky Security Center에서 파일의 백업 복사본을 관리하는 방법에 대한 자세한 내용은 Kaspersky Security Center 도움말 시스템을 참조하십시오.

백업 저장소에 저장된 파일의 최대 저장 기간 구성

백업 저장소 파일 복사본의 최대 저장 기간 기본값은 30일입니다. 최대 저장 기간이 만료되면 Kaspersky Endpoint Security가 백업 저장소에서 가장 오래된 파일을 삭제합니다.

백업 저장소에 저장된 파일의 최대 저장 기간을 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창의 **일반 설정**에서 **리포트 및 저장소** 타일을 클릭합니다.



백업 설정

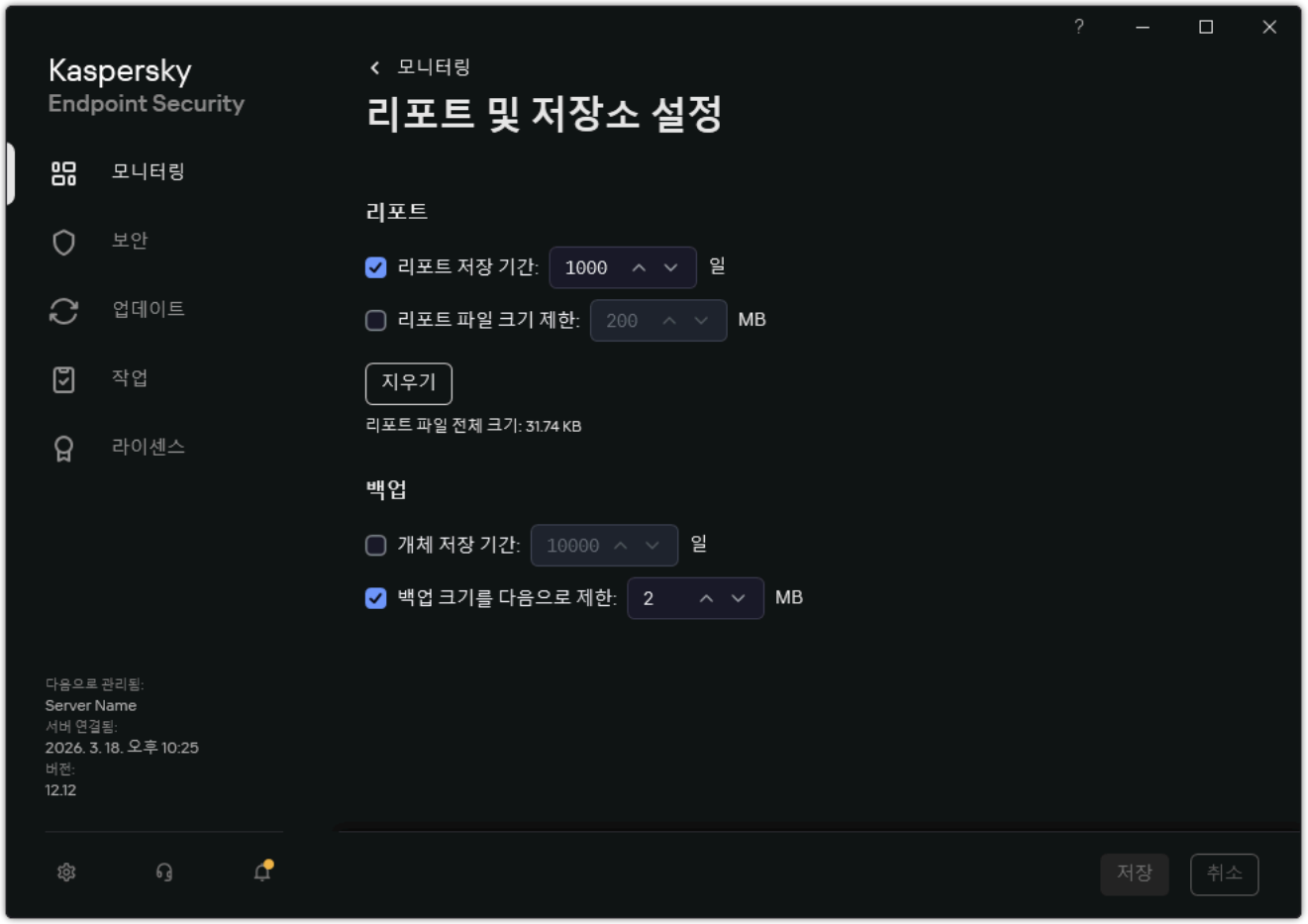
3. 백업에서 파일 복사본의 저장 기간을 제한하려면 **백업** 블록에서 **개체 저장 기간: N일** 확인란을 선택합니다. 백업 저장소의 파일 복사본 최대 저장 기간을 입력합니다.
4. 변경 사항을 저장합니다.

백업 저장소 최대 크기 구성

백업의 최대 크기를 지정할 수 있습니다. 기본적으로 백업 저장소 크기는 무제한입니다. 저장소의 크기가 제한에 도달하면 Kaspersky Endpoint Security가 백업 저장소에서 가장 오래된 파일을 자동으로 삭제합니다.

백업 저장소 최대 크기를 구성하려면 다음과 같이 진행합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창의 **일반 설정**에서 **리포트 및 저장소** 타일을 클릭합니다.



백업 설정

3. **백업** 블록에서 **백업 크기를 다음으로 제한: <N>MB** 확인란을 선택합니다. 이 확인란을 선택하면 최대 저장소 크기가 정의된 값으로 제한됩니다. 최대 크기 기본값은 1024MB입니다 Kaspersky Endpoint Security는 저장소 크기가 최대 한도에 도달하면 저장소에서 가장 오래된 파일을 자동으로 삭제하여 최대 저장소 크기를 넘지 않도록 관리합니다.
4. 변경 사항을 저장합니다.

백업 저장소에서 파일 복원

파일에서 악성 코드가 탐지되면 Kaspersky Endpoint Security가 해당 파일을 차단하고, 여기에 *치료 안 됨* 상태를 할당하고, 백업 저장소에 복사본을 저장한 후 치료합니다. 파일 치료에 성공하면 파일의 백업 복사본 상태가 *치료 됨*으로 변합니다. 원래 폴더에서 파일을 사용할 수 있게 됩니다. 파일을 치료할 수 없는 경우 Kaspersky Endpoint Security가 원래 폴더에서 파일을 삭제합니다. 백업 복사본의 파일은 원래 폴더로 복원할 수 있습니다.

컴퓨터 재시작 시 삭제 예정 상태의 파일은 복원할 수 없습니다. 컴퓨터를 다시 시작하면 파일 상태가 *치료됨* 또는 *삭제됨*으로 변경됩니다. 또한, 백업 복사본의 파일은 원래 폴더로 복원할 수 있습니다.

Windows Store 애플리케이션에 포함된 파일에서 악성 코드가 탐지되면 Kaspersky Endpoint Security는 백업 저장소로 그 복사본을 옮기지 않고 즉시 파일을 삭제합니다. 운영 체제의 적절한 도구를 사용하여 Windows Store 애플리케이션의 무결성을 복원할 수 있습니다(Windows Store 애플리케이션 복원에 대한 자세한 내용은 Microsoft Windows 도움말 파일 참조).

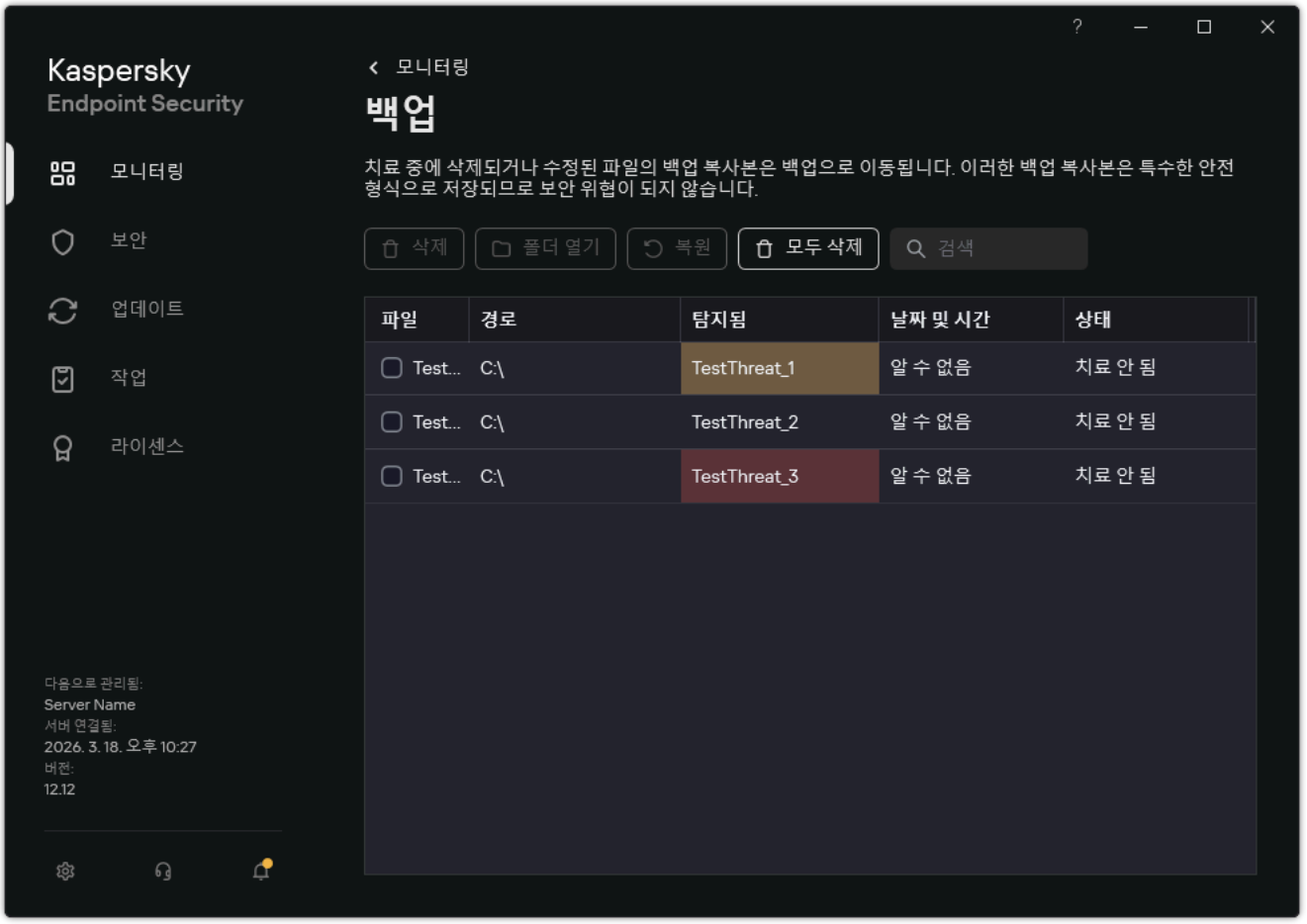
파일의 백업 복사본 세트가 테이블에 표시됩니다. 파일의 백업 사본에는 해당 파일의 원래 폴더 경로가 표시됩니다. 파일의 원래 폴더 경로에는 개인 정보가 포함될 수 있습니다.

같은 폴더에 있었으며 이름이 같고 컨텐츠는 다른 여러 파일이 백업 저장소로 이동되었다면, 가장 마지막에 백업 저장소로 이동한 파일만 복원할 수 있습니다.

백업 저장소에서 파일을 복원하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창의 **모니터링** 섹션에서 **백업** 타일을 클릭합니다.
2. 백업 파일 목록이 열리면 복원할 파일을 선택하고 **복원**을 클릭합니다.

Kaspersky Endpoint Security가 선택된 백업 복사본의 파일을 원래 폴더로 복원합니다.



백업

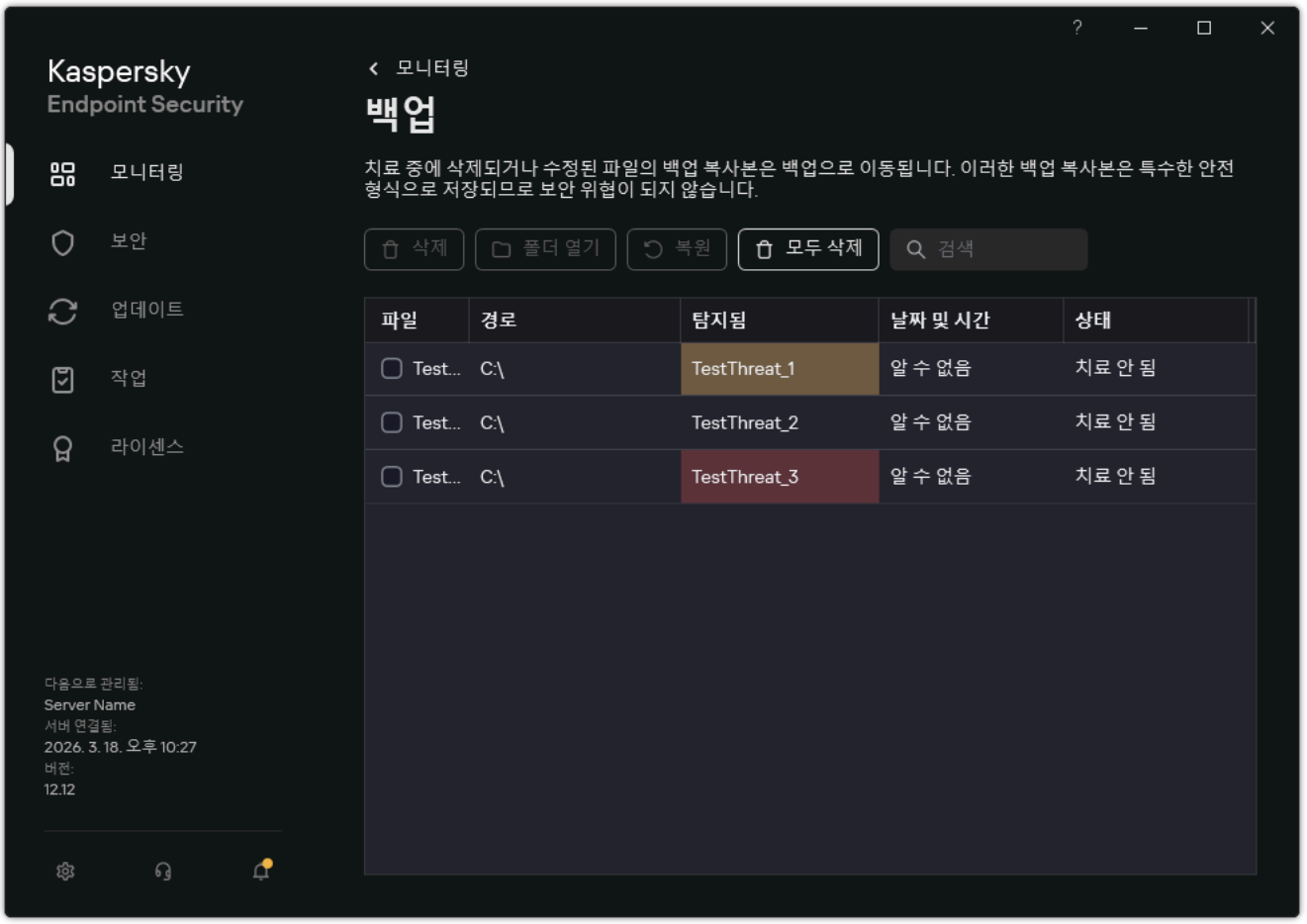
백업 저장소에서 파일의 백업 복사본 삭제

애플리케이션 설정에 구성된 저장 기간이 경과된 후에는 Kaspersky Endpoint Security가 백업 저장소에서 모든 상태의 파일 백업 복사본을 자동으로 삭제합니다. 백업 저장소에서 파일의 복사본을 직접 삭제할 수도 있습니다.

백업 저장소에서 파일의 백업 복사본을 삭제하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창의 **모니터링** 섹션에서 **백업** 타일을 클릭합니다.
2. 백업 파일 목록이 열리면 백업에서 삭제할 파일을 선택하고 **삭제**를 클릭합니다.

Kaspersky Endpoint Security가 백업 저장소에서 선택한 백업 복사본을 삭제합니다.



백업

알림 서비스

Kaspersky Endpoint Security의 작업 중에는 모든 종류의 이벤트가 발생합니다. 이러한 이벤트 알림은 순수하게 정보성인 경우도 있고 매우 중요한 정보가 포함된 경우도 있습니다. 예를 들어 알림을 통해 데이터베이스 및 애플리케이션 모듈 업데이트가 완료되었음을 알릴 수도 있고, 치료해야 하는 구성 요소 오류를 기록할 수도 있습니다.

Kaspersky Endpoint Security는 Microsoft Windows 애플리케이션 로그 및/또는 Kaspersky Endpoint Security 이벤트 로그 작동 중에 이벤트에 대한 정보를 기록하도록 지원합니다.

Kaspersky Endpoint Security는 다음과 같은 방법으로 알림을 표시합니다.

- Microsoft Windows 작업 표시줄 알림 영역의 팝업 알림 사용
- 이메일로 전송

사용자가 이벤트 알림 표시를 구성할 수 있습니다. 알림 표시의 방법은 각 이벤트 유형에 따라 구성됩니다.

이벤트 표를 사용하여 알림 서비스를 구성하는 경우 다음 조치를 수행할 수 있습니다.

- 열 값 또는 사용자지정 필터 조건을 사용하여 알림 서비스 이벤트를 필터링합니다.
- 알림 서비스 이벤트에 대한 검색 기능을 사용합니다.
- 알림 서비스 이벤트를 정렬합니다.
- 알림 서비스이벤트 목록에 표시되는 열의 순서와 집합을 변경합니다.

이벤트 로그 설정 구성

이벤트 로그 설정을 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **인터페이스**를 차례로 선택합니다.
3. **알림** 블록에서 **알림 구성** 버튼을 클릭합니다.

   창 왼쪽에 Kaspersky Endpoint Security 구성 요소 및 작업 목록이 표시됩니다. 창 오른쪽에 선택한 구성 요소 또는 작업에 대해 생성된 이벤트를 보여줍니다.

   이벤트에는 다음 사용자 데이터가 포함될 수 있습니다:

   - Kaspersky Endpoint Security가 검사한 파일의 경로
   - Kaspersky Endpoint Security의 작동 중에 수정된 레지스트리 키의 경로
   - Microsoft Windows 사용자 이름
   - 사용자가 열어 본 웹 페이지의 주소
4. 창 왼쪽에서 이벤트 로그 설정을 구성할 구성 요소 또는 작업을 선택합니다.

5. **로컬 리포트에 저장** 및 **Windows 이벤트 로그에 저장** 열에서 관련 이벤트 옆에 있는 확인란을 선택합니다.

   로컬 리포트에 저장 열의 확인란이 선택된 이벤트는 애플리케이션 로그의 애플리케이션 섹션에 표시됩니다. **Windows 이벤트 로그에 저장** 열의 확인란이 선택된 이벤트는 Windows 로그의 `Application` 채널에 표시됩니다.

6. 변경 사항을 저장합니다.

알림 표시 및 전달 구성

알림 표시 및 전달을 구성하려면 다음을 수행합니다.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **인터페이스**를 차례로 선택합니다.
3. **알림** 블록에서 **알림 구성** 버튼을 클릭합니다.

   창 왼쪽에 Kaspersky Endpoint Security 구성 요소 및 작업 목록이 표시됩니다. 창 오른쪽에 선택한 구성 요소 또는 작업에 대해 생성된 이벤트를 보여줍니다.

   이벤트에는 다음 사용자 데이터가 포함될 수 있습니다:

   - Kaspersky Endpoint Security가 검사한 파일의 경로
   - Kaspersky Endpoint Security의 작동 중에 수정된 레지스트리 키의 경로
   - Microsoft Windows 사용자 이름
   - 사용자가 열어 본 웹 페이지의 주소

4. 창 왼쪽의 알림 전달을 구성할 구성 요소 또는 작업을 선택합니다.
5. **팝업 화면 알림** 열에서 관련 이벤트 옆에 있는 확인란을 선택합니다.

   선택한 이벤트에 대한 정보가 Microsoft Windows 작업 표시줄 알림 영역의 팝업 메시지로 화면에 표시됩니다.

6. **이메일로 알림** 열에서 관련 이벤트 옆에 있는 확인란을 선택합니다.

   메일 알림 전달 설정을 구성하면 선택한 이벤트에 대한 정보가 이메일로 전달됩니다.

7. **확인**을 누릅니다.
8. 이메일 알림을 사용한다면 이메일 전송 설정을 구성합니다:

   a. **이메일 알림 구성**을 누릅니다.

   b. **이벤트 알림** 확인란을 선택하여 **이메일로 알림** 열에서 선택한 Kaspersky Endpoint Security 이벤트의 정보 전달을 사용합니다.

   c. 이메일 알림 전달 설정을 지정합니다.

   d. **확인**을 누릅니다.

9. 변경 사항을 저장합니다.

알림 영역의 애플리케이션 상태에 대한 경고 표시 구성

알림 영역에 애플리케이션 상태 경고를 표시하도록 구성하려면 다음을 수행합니다

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **인터페이스**를 차례로 선택합니다.
3. **알림 영역에 애플리케이션 상태 표시** 블록에서 Microsoft Windows 알림 영역에 알림을 표시할 이벤트 카테고리 옆의 확인란을 선택합니다.
4. 변경 사항을 저장합니다.

선택한 카테고리와 연결된 이벤트가 발생하면 알림 영역의 애플리케이션 아이콘이 경고의 심각도에 따라 또는 바뀝니다.

사용자와 관리자 간의 메시지

컴퓨터에 Kaspersky Endpoint Security가 설치되어 있는 LAN 사용자는 애플리케이션 제어, 장치 제어, 웹 제어 및 적응형 이상 행위 제어 구성 요소를 사용하여 관리자에게 메시지를 보낼 수 있습니다.

사용자는 다음 경우에 회사 로컬 네트워크 관리자에게 메시지를 전송해야 합니다:

- 장치 제어가 장치로의 접근을 차단했습니다.

  Kaspersky Endpoint Security 인터페이스의 장치 제어 섹션에서 차단 장치로의 접근을 요청하기 위한 메시지 템플릿을 찾을 수 있습니다.

- 애플리케이션 제어가 애플리케이션이 시작되지 않도록 차단했습니다.

  Kaspersky Endpoint Security 인터페이스의 애플리케이션 제어 섹션에서 차단 애플리케이션을 시작할 수 있도록 요청하기 위한 메시지 템플릿을 찾을 수 있습니다.

- 웹 리소스로의 접근을 차단하는 웹 제어.

  Kaspersky Endpoint Security 인터페이스의 웹 제어 섹션에서 차단된 웹 리소스로의 접근을 요청하는 메시지 템플릿을 찾을 수 있습니다.

Kaspersky Endpoint Security가 설치된 컴퓨터에서 Kaspersky Security Center의 활성 정책이 실행 중인지, Kaspersky Security Center 중앙 관리 서버와 연결되어 있는지 여부에 따라 메시지를 보내는 방법 및 사용 템플릿이 달라집니다. 가능한 시나리오는 다음과 같습니다:

- Kaspersky Endpoint Security가 설치되어 있는 컴퓨터에서 Kaspersky Security Center 정책을 실행하고 있지 않다면 사용자의 메시지는 LAN 관리자에게 이메일로 전송됩니다.

  Kaspersky Endpoint Security 로컬 인터페이스에서 정의한 템플릿의 필드 값으로 메시지 필드가 입력됩니다.

- Kaspersky Endpoint Security가 설치되어 있는 컴퓨터에서 Kaspersky Security Center 정책을 실행하는 경우 표준 메시지가 Kaspersky Security Center 중앙 관리 서버로 전송됩니다.

  이 경우 Kaspersky Security Center 이벤트 저장소에서 사용자 메시지를 확인할 수 있습니다(아래 지침 참조). Kaspersky Security Center 정책에 정의된 템플릿의 필드 값으로 메시지 필드가 채워집니다.

- Kaspersky Endpoint Security가 설치되어 있는 컴퓨터에서 Kaspersky Security Center 이동 사용자 정책을 실행하는 경우 Kaspersky Security Center와의 연결 여부에 따라 메시지 전송 방법이 달라집니다.

  - Kaspersky Security Center와 연결되어 있는 경우 Kaspersky Endpoint Security가 Kaspersky Security Center 중앙 관리 서버로 표준 메시지를 전송합니다.

  - Kaspersky Security Center와 연결되어 있지 않으면 사용자의 메시지가 LAN 관리자에게 이메일로 전송됩니다.

  두 경우에 모두 Kaspersky Security Center 정책에 정의된 템플릿의 필드 값으로 메시지 필드가 채워집니다.

Kaspersky Security Center 이벤트 저장소에서 사용자 메시지를 보려면 다음과 같이 하십시오:

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **중앙 관리 서버** 노드에서 **이벤트** 탭을 선택합니다.

   Kaspersky Security Center 작업 공간에 LAN 사용자가 관리자에게 보낸 메시지를 포함해 Kaspersky Endpoint Security가 작동되는 동안 발생한 모든 이벤트가 표시됩니다.
3. 이벤트 필터를 구성하려면 **이벤트 선택** 드롭다운 목록에서 **사용자 개선 요청 사항**을 선택합니다.
4. 관리자에게 보낸 메시지를 선택합니다.
5. 관리 콘솔 작업 공간 오른쪽에 있는 **이벤트 속성 창 열기** 버튼을 누릅니다.

리포트 관리

리포트에는 각 Kaspersky Endpoint Security 구성 요소의 작업, 데이터 암호화 이벤트, 각 검사 작업/업데이트 작업/무결성 검사 작업의 성능, 그리고 애플리케이션의 전반적인 작업에 대한 정보가 기록됩니다.

리포트는 `C:\ProgramData\Kaspersky Lab\KES.14.0\Report` 폴더에 저장됩니다.

리포트에는 다음 사용자 데이터가 포함될 수 있습니다:

- Kaspersky Endpoint Security가 검사한 파일의 경로
- Kaspersky Endpoint Security의 작동 중에 수정된 레지스트리 키의 경로
- Microsoft Windows 사용자 이름
- 사용자가 열어 본 웹 페이지의 주소

리포트의 데이터는 표 형식으로 표시됩니다. 표의 각 행에는 개별 이벤트에 대한 정보가 포함됩니다. 이벤트 특성은 표의 열에 있습니다. 추가 특성이 포함된 중첩 열로 구성된 복합 열도 있습니다. 추가 특성을 보려면 열 이름 옆에 있는 ⊞ 버튼을 누릅니다. 다양한 구성 요소 또는 다양한 작업이 동작하는 동안 기록되는 이벤트에는 다양한 특성 집합이 포함됩니다.

다음과 같은 리포트를 사용할 수 있습니다:

- **시스템 감사** 리포트. 사용자와 애플리케이션 간의 상호 작용 중이나 애플리케이션의 일반적인 작동 중 발생하는, 특정 Kaspersky Endpoint Security 구성 요소 또는 작업과 관련되지 않은 이벤트에 대한 정보를 포함합니다.
- Kaspersky Endpoint Security 구성 요소 작동에 대해 리포트
- Kaspersky Endpoint Security 작업 리포트
- **데이터 암호화** 리포트. 데이터 암호화 및 복호화 프로세스 동안 발생한 이벤트에 대한 정보가 들어 있습니다.

리포트는 다음 이벤트 중요도를 사용합니다:

ⓘ **정보 메시지**. 대개 중요한 정보를 포함하지 않는 참조 이벤트입니다.

⚠ **경고**. 이러한 이벤트는 Kaspersky Endpoint Security 작동 중에 발생한 중요한 상황을 나타내므로 주의해야 합니다.

⊘ **심각 이벤트**. Kaspersky Endpoint Security 작동 중 문제나 사용자 컴퓨터 보호의 취약점을 나타내는 심각한 이벤트입니다.

리포트를 간편하게 처리하기 위해 다음과 같은 방법으로 화면의 데이터 표시를 수정할 수 있습니다:

- 다양한 기준으로 이벤트 목록을 필터링합니다.
- 검색 기능을 사용하여 특정 이벤트를 찾습니다.
- 선택한 이벤트를 개별 섹션에서 봅니다.
- 각 리포트 열별로 이벤트 목록을 정렬합니다.

- 버튼을 사용해 이벤트 필터로 그룹화된 이벤트를 표시하거나 숨깁니다.
- 리포트에 표시되는 열의 순서와 정렬을 변경합니다.

필요시 생성한 리포트는 텍스트 파일로 저장할 수 있습니다. 또한 그룹으로 결합된 Kaspersky Endpoint Security 구성 요소 및 작업에 대한 리포트 정보를 삭제 할 수 있습니다.

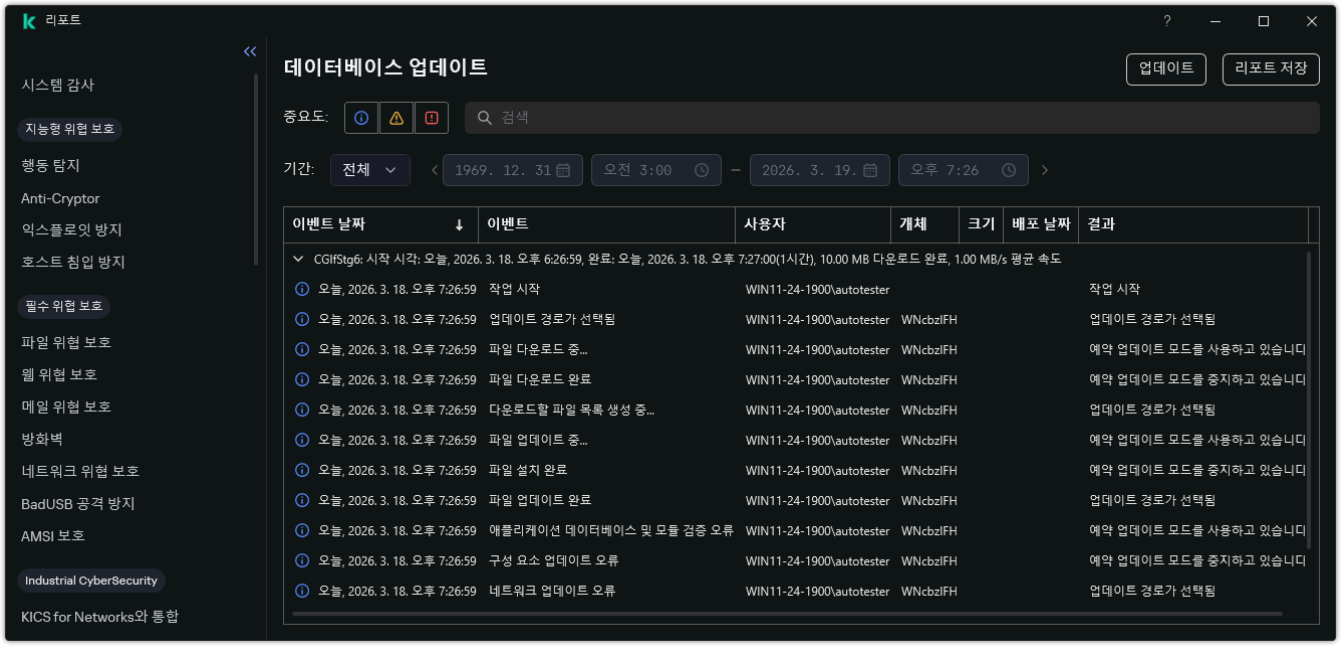
Kaspersky Endpoint Security가 Kaspersky Security Center 관리하에 실행 중이면 이벤트에 대한 정보가 Kaspersky Security Center 중앙 관리 서버로 전달될 수 있습니다(자세한 내용은 Kaspersky Security Center 도움말 참조).

리포트 보기

리포트를 볼 수 있는 사용자는 해당 리포트에 반영된 모든 이벤트도 볼 수 있습니다.

리포트를 보려면 다음을 수행합니다.

1. 메인 애플리케이션 창의 **모니터링** 섹션에서 **리포트** 타일을 클릭합니다.



리포트

2. 구성 요소 및 작업 목록에서 구성 요소 또는 작업을 선택합니다.

   창의 오른쪽에는 선택된 구성 요소 또는 선택된 Kaspersky Endpoint Security 작업의 결과로 나타나는 이벤트 목록이 포함된 리포트가 표시됩니다. 열의 셀에 포함된 값을 기준으로 리포트의 이벤트를 정렬할 수 있습니다.

3. 이벤트에 대한 자세한 정보를 보려면 리포트에서 이벤트를 선택합니다.

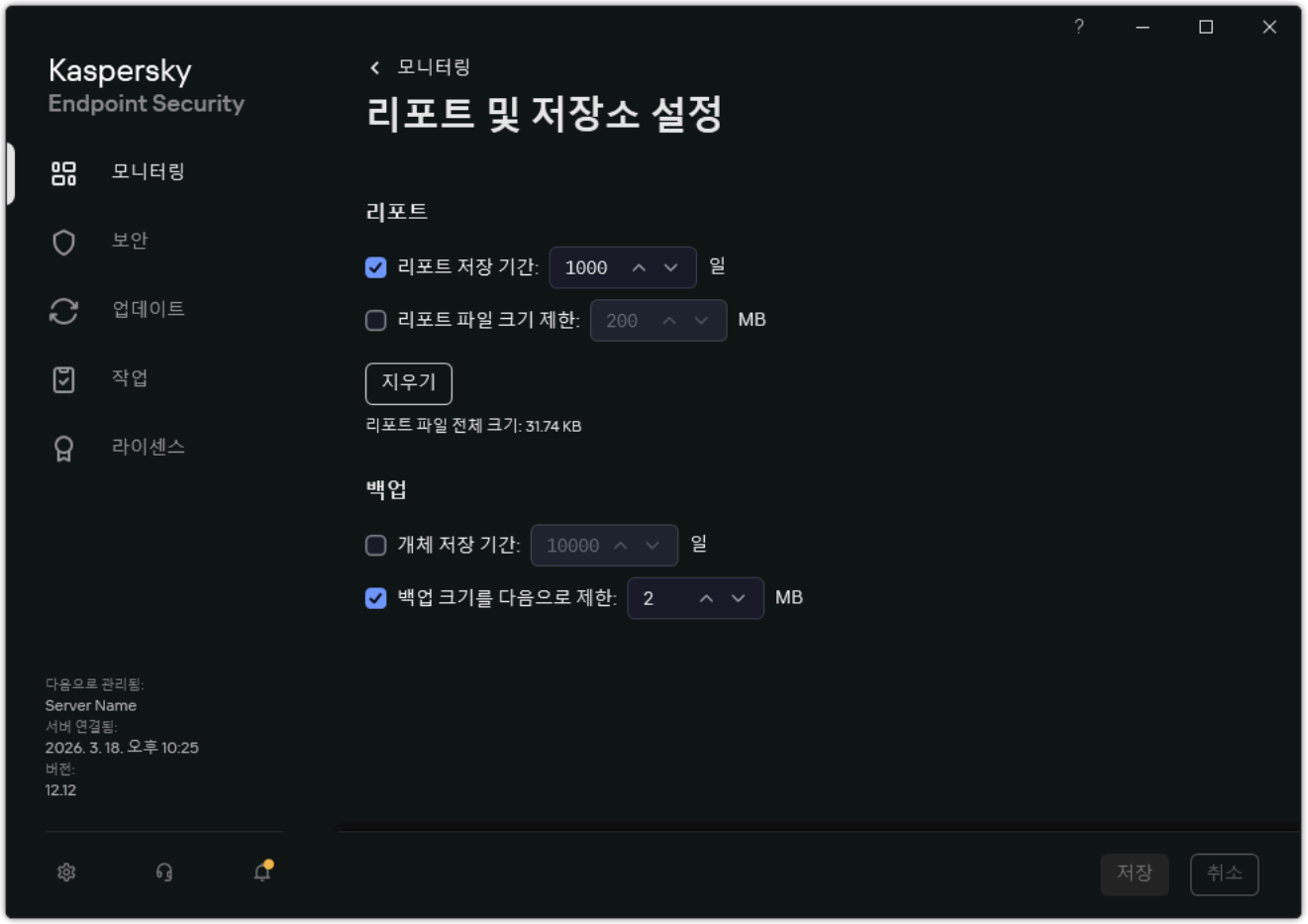
   이벤트 요약을 포함하고 있는 블록은 창 아래 부분에 표시됩니다.

최대 리포트 저장 기간 구성

Kaspersky Endpoint Security에서 기록하는 이벤트에 대한 리포트의 최대 기본 저장 기간은 30일입니다. 이 기간이 지나면 Kaspersky Endpoint Security가 리포트 파일에서 가장 오래된 항목을 자동으로 삭제합니다.

리포트 최대 저장 기간을 수정하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창의 **일반 설정**에서 **리포트 및 저장소** 타일을 클릭합니다.



리포트 설정

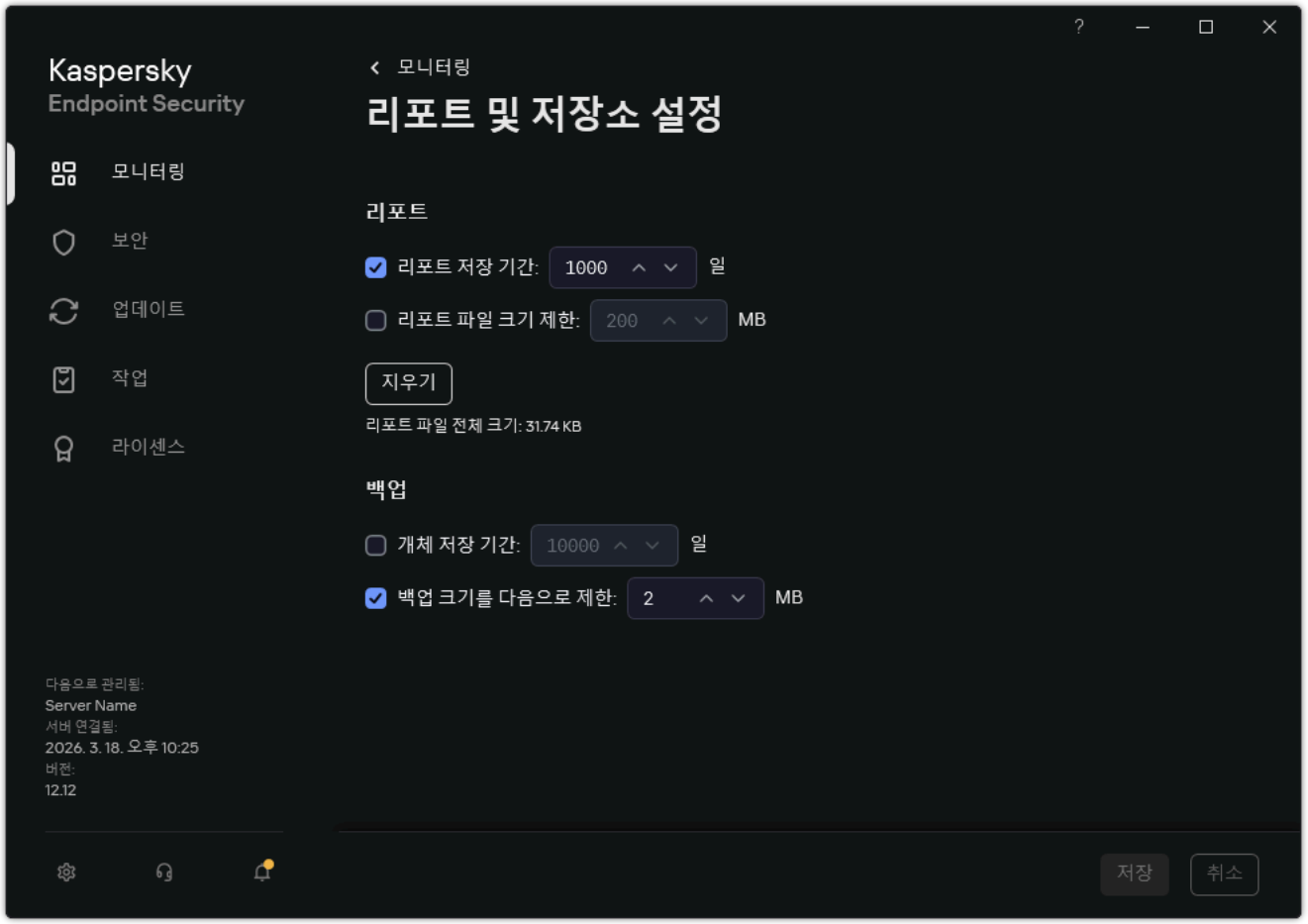
3. 리포트 저장 기간을 제한하려면 **리포트** 블록에서 **리포트 저장 기간: N일** 확인란을 선택합니다. 최대 리포트 저장 기간을 정의합니다.
4. 변경 사항을 저장합니다.

리포트 파일의 최대 크기 구성

리포트가 포함된 파일의 최대 크기를 지정할 수 있습니다. 리포트 파일의 최대 크기 기본값은 1024MB입니다. Kaspersky Endpoint Security는 리포트 파일 크기가 최대 한도에 도달하면 리포트 파일에서 가장 오래된 항목을 자동으로 삭제하여 최대 한도를 넘지 않도록 관리합니다.

최대 리포트 파일 크기를 구성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창의 **일반 설정**에서 **리포트 및 저장소** 타일을 클릭합니다.



리포트 설정

3. **리포트** 블록에서 **리포트 파일 크기 제한: <N>MB** 확인란을 선택합니다. 리포트 파일의 최대 크기를 정의합니다.
4. 변경 사항을 저장합니다.

파일에 리포트 저장

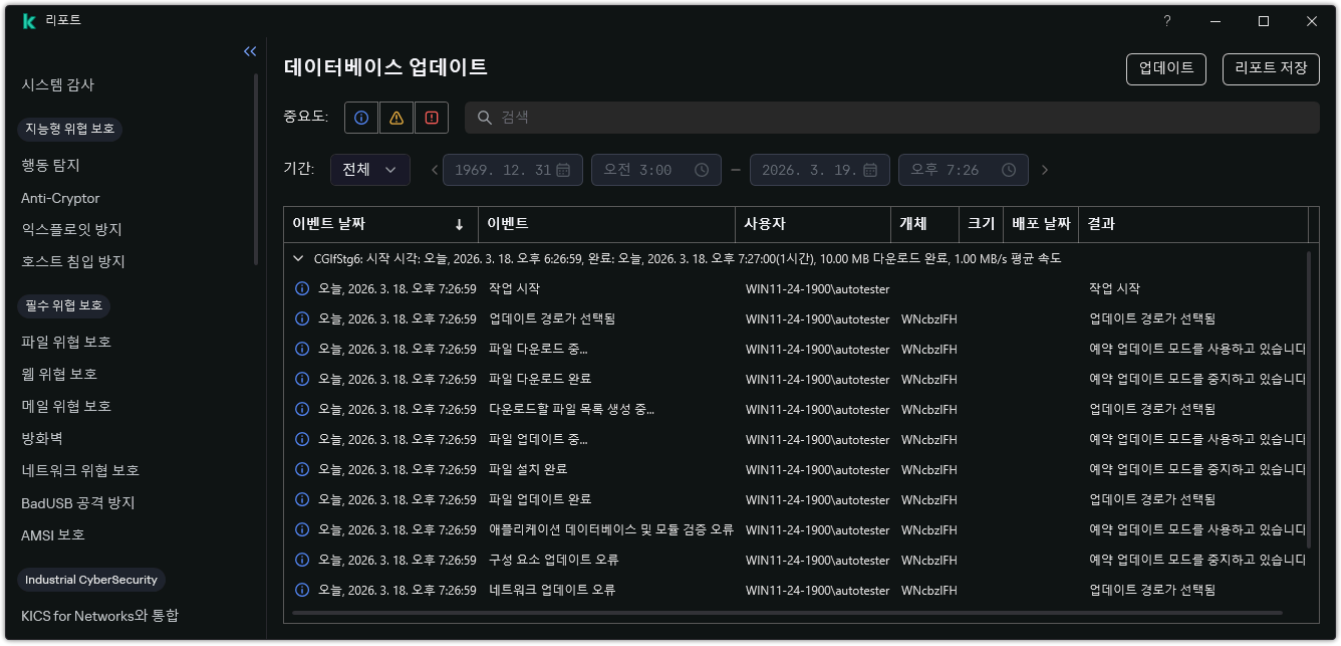
사용자는 파일로 저장된 리포트의 정보 보안을 보장하며, 이 정보에 대한 접근을 제어하고 제한할 개인적인 책임이 있습니다.

생성한 리포트를 텍스트 형식(TXT)의 파일이나 CSV 파일로 저장할 수 있습니다.

Kaspersky Endpoint Security는 화면에 표시되는 그대로 리포트에 이벤트를 기록합니다. 즉 이벤트 속성의 집합과 순서가 동일하게 기록됩니다.

파일에 리포트를 저장하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창의 **모니터링** 섹션에서 **리포트** 타일을 클릭합니다.



리포트

2. 창이 열리면 구성 요소 또는 작업을 선택합니다.

   창 오른쪽에 선택한 Kaspersky Endpoint Security 구성 요소 또는 작업의 작동 중 발생한 이벤트의 목록이 포함된 리포트가 표시됩니다.

3. 필요시 다음을 기준으로 리포트의 데이터 표시 방법을 수정할 수 있습니다:

   - 이벤트 필터링
   - 이벤트 검색 실행
   - 열 다시 정렬
   - 이벤트 정렬

4. 창 오른쪽 상단에서 **리포트 저장** 버튼을 누릅니다.

5. 창이 열리면 리포트 파일의 대상 폴더를 지정합니다.

6. 리포트 파일의 이름을 입력합니다.

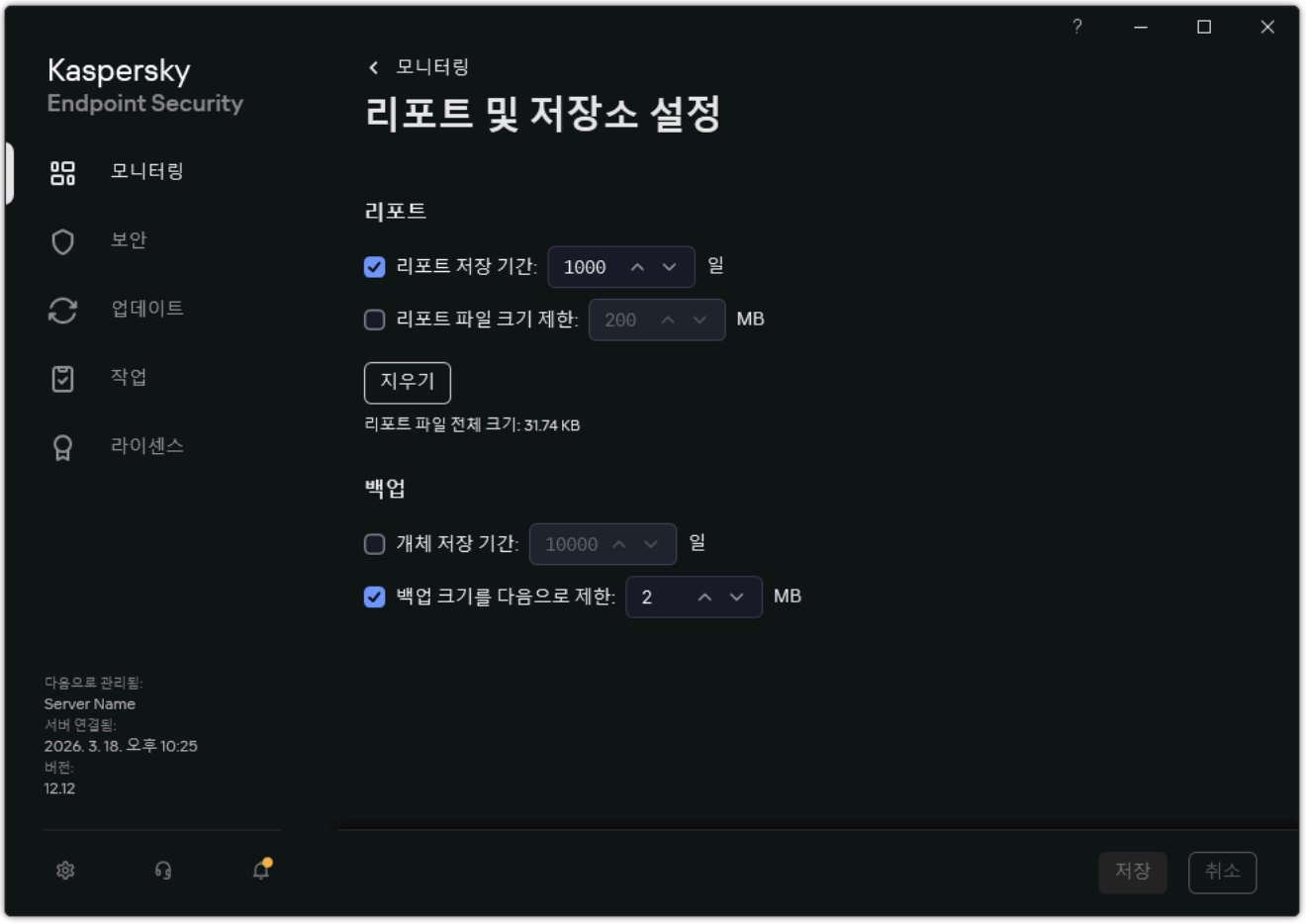
7. TXT 또는 CSV 중 필요한 리포트 파일 형식을 선택합니다.

8. 변경 사항을 저장합니다.

리포트 파일 삭제

리포트에서 정보를 제거하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창의 **일반 설정**에서 **리포트 및 저장소** 타일을 클릭합니다.



리포트 설정

3. **리포트** 블록에서 **지우기** 버튼을 클릭합니다.
4. 암호 보호를 사용하면 Kaspersky Endpoint Security가 사용자 계정 정보를 묻는 메시지를 표시할 수 있습니다. 사용자에게 필요한 권한이 없다면 애플리케이션이 계정 자격 증명를 묻는 메시지를 표시합니다.

Kaspersky Endpoint Security는 모든 애플리케이션 구성 요소 및 작업에 대한 모든 리포트를 삭제합니다.

Kaspersky Endpoint Security 자기 보호 기능

자기 보호는 다른 애플리케이션이 컴퓨터에서 Kaspersky Endpoint Security를 제거하는 등 Kaspersky Endpoint Security의 작동을 방해할 수 있는 작업을 수행하지 못하도록 방지합니다. Kaspersky Endpoint Security에서 사용할 수 있는 자기 보호 기술은 운영 체제가 32비트인지 64비트인지에 따라 달라집니다(아래 표 참조). 자기 보호에는 암호 보호와 중앙 관리 서버 연결 보호도 포함됩니다.

*암호 보호*를 사용하면 사용자에게 부여된 권한(예: 애플리케이션 종료 권한)에 따라 사용자의 Kaspersky Endpoint Security 접근을 제한할 수 있습니다.

*중앙 관리 서버 연결 보호*는 컴퓨터를 신뢰할 수 없는 서버에 무단으로 다시 연결하는 것을 방지합니다.

Kaspersky Endpoint Security 자기 보호 기술

기술	설명	x86 컴퓨터	x64 컴퓨터
자기 보호 매커니즘	이 기술은 다음 애플리케이션 구성 요소에 대한 접근을 차단합니다: • Kaspersky Endpoint Security 설치 폴더의 파일 및 애플리케이션의 기타 파일; • 애플리케이션에 속한 레코드가 있는 레지스트리 키; • 애플리케이션이 실행하는 프로세스.	✓	✓
AM-PPL(Antimalware Protected Process Light)	이 기술은 악성 동작으로부터 Kaspersky Endpoint Security 프로세스를 보호합니다. AM-PPL 기술에 대한 자세한 내용은 Microsoft 웹사이트를 방문하시기 바랍니다. AM-PPL 기술은 Windows 10 1703(RS2) 버전 이상 및 Windows Server 2019 운영 체제에서 사용할 수 있습니다.	✓	✓
외부 관리 방어 메커니즘	이 기술은 다른 애플리케이션(예: TeamViewer 또는 RemotelyAnywhere)이 Kaspersky Endpoint Security에 접근하는 것을 방지합니다.	✓	– (Windows 7 제외)

자기 보호 기능 작동 및 중지

Kaspersky Endpoint Security가 하드 드라이브의 애플리케이션 파일, 메모리 프로세스 및 시스템 레지스트리의 항목에 대한 변경이나 삭제를 방지합니다.

이 기술은 다음 애플리케이션 구성 요소에 대한 접근을 차단합니다:

- Kaspersky Endpoint Security 설치 폴더의 파일 및 애플리케이션의 기타 파일;
- 애플리케이션에 속한 레코드가 있는 레지스트리 키;
- 애플리케이션이 실행하는 프로세스.

Kaspersky Endpoint Security의 자기 보호 메커니즘은 기본적으로 작동됩니다.

관리 콘솔(MMC)에서 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 창에서 **일반 설정** → **애플리케이션 설정**을 차례로 선택합니다.

4. **자기 보호 사용** 확인란으로 자기 보호 메커니즘을 사용하거나 중지합니다.

5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 자기 보호를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **자기 보호**로 갑니다.

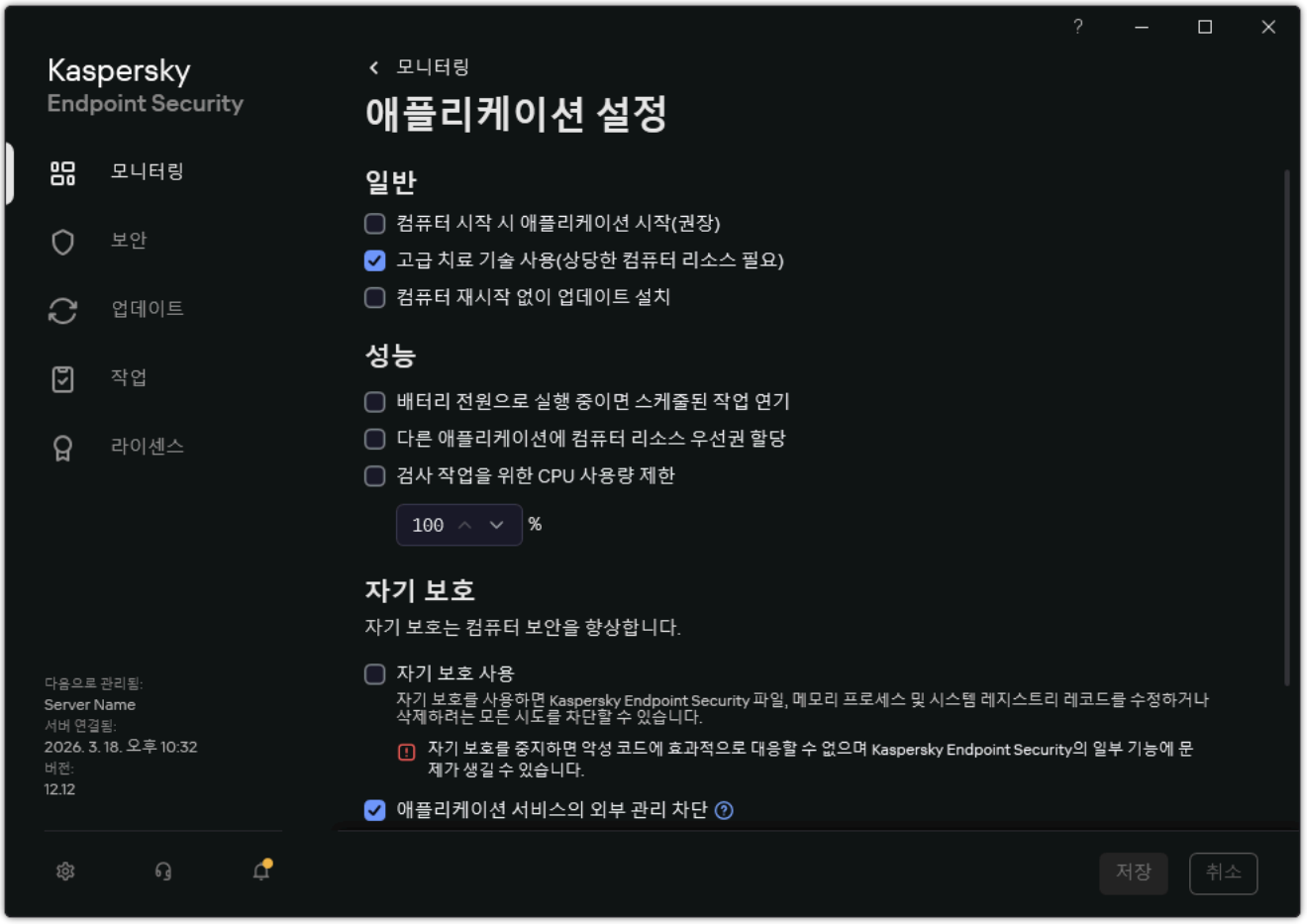
5. **자기 보호 활성화됨** 토글 스위치를 자기 보호 메커니즘을 사용하거나 중지합니다.

6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 자기 보호를 활성화 또는 비활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **일반 설정** → **애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

3. **자기 보호 사용** 확인란으로 자기 보호 메커니즘을 사용하거나 중지합니다.

4. 변경 사항을 저장합니다.

AM-PPL 지원 활성화 및 비활성화

Kaspersky Endpoint Security는 Microsoft의 Antimalware Protected Process Light 기술(이하 "AM-PPL"이라고 함)을 지원합니다. AM-PPL은 Kaspersky Endpoint Security 프로세스를 악의적인 작업(예: 애플리케이션 종료)으로부터 보호합니다. AM-PPL은 신뢰할 수 있는 프로세스만 실행할 수 있도록 허용합니다. Kaspersky Endpoint Security 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 Endpoint Security에는 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.

AM-PPL 기술을 계속해서 사용합니다. AM-PPL은 운영 체제 보호에 중요한 구성 요소입니다. AM-PPL 지원을 비활성화하면 일부 Kaspersky Endpoint Security 기능이 정상적으로 작동하지 않을 수 있습니다(예: 애플리케이션과 Windows Security Center의 통합). AM-PPL 지원 비활성화는 문제 해결을 위한 별도의 테스트 환경에서만 허용됩니다.

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.exe)를 관리자 권한으로 실행합니다.

3. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

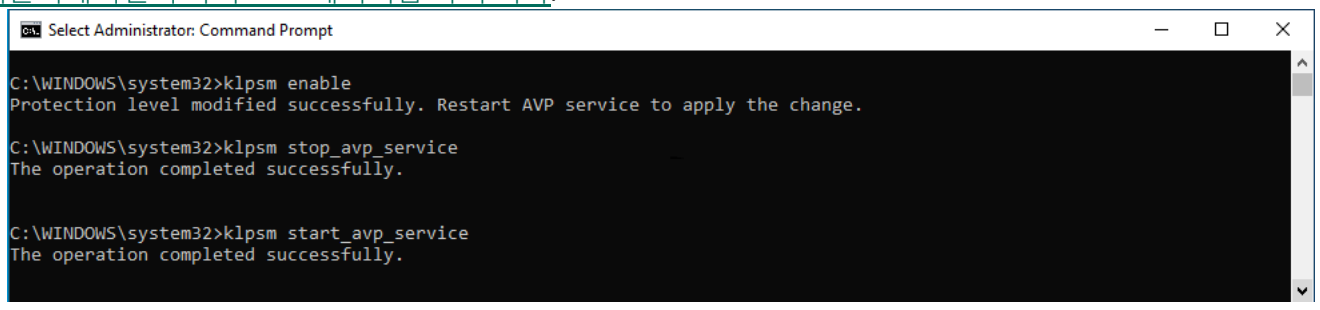
   애플리케이션 설치 중에 %PATH% 시스템 변수에 실행 파일의 경로를 추가할 수 있습니다.

4. 명령줄에 다음을 입력합니다:

   - `klpsm.exe enable` – AM-PPL 기술 지원을 활성화합니다(아래 그림 참조).
   - `klpsm.exe disable` – AM-PPL 기술 지원을 비활성화합니다.

5. Kaspersky Endpoint Security를 재시작합니다.

6. 애플리케이션의 자기 보호 메커니즘 다시 시작.



AM-PPL 기술 지원 활성화

외부 관리로부터 애플리케이션 서비스 보호

외부 관리로부터 애플리케이션 서비스를 보호하면 사용자 및 기타 애플리케이션의 Kaspersky Endpoint Security 서비스 중지 시도를 차단합니다. 이 보호는 다음 서비스의 작동을 보장합니다.

- Kaspersky Endpoint Security 서비스(AVP.KES.14.0)
- Kaspersky Seamless Update Service 서비스(AVPSUS.KES.14.0)

명령줄에서 애플리케이션을 종료하려면 외부 관리에 대한 Kaspersky Endpoint Security 서비스 보호를 중지하십시오.

AM-PPL 기술을 지원하지 않는 컴퓨터 또는 AM-PPL 기술이 중지된 컴퓨터에서만 애플리케이션 서비스의 외부 관리를 허용할 수 있습니다.

관리 콘솔(MMC)에서 외부 관리에 대한 애플리케이션 서비스 보호를 활성화 또는 비활성화하는 방법

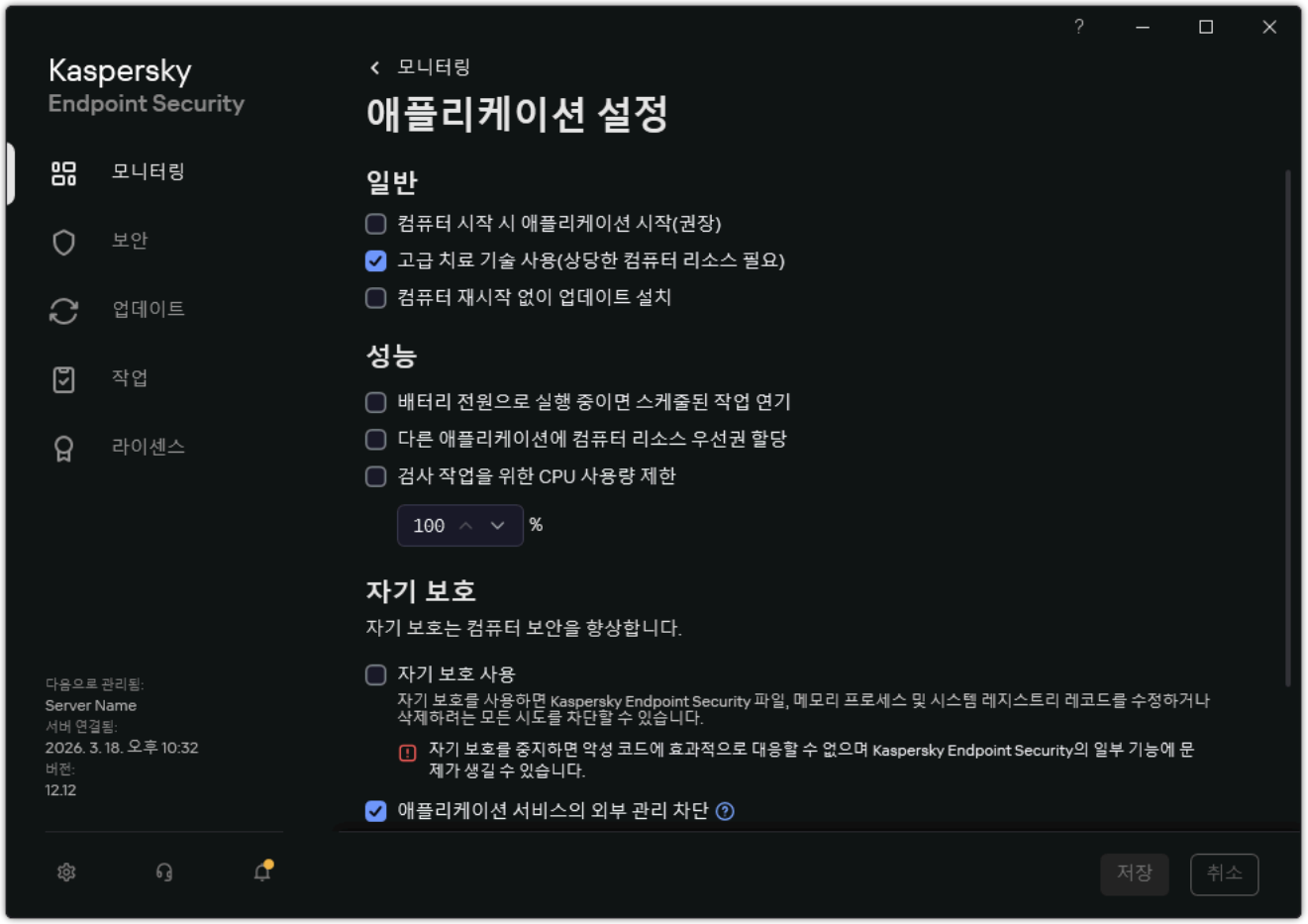
1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 애플리케이션 설정**을 차례로 선택합니다.
4. **애플리케이션 서비스의 외부 관리 차단** 확인란으로 외부 관리에 대한 Kaspersky Endpoint Security 서비스 보호를 활성화하거나 비활성화합니다.
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 외부 관리에 대해 애플리케이션 서비스 보호를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 자기 보호**로 갑니다.
5. **애플리케이션 서비스의 외부 관리 차단** 확인란으로 외부 관리에 대한 Kaspersky Endpoint Security 서비스 보호를 활성화하거나 비활성화합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 외부 관리에 대한 애플리케이션 서비스 보호를 활성화 또는 비활성화하는 방법

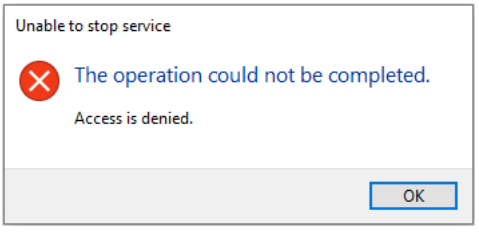
1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

3. **애플리케이션 서비스의 외부 관리 차단** 확인란으로 외부 관리에 대한 Kaspersky Endpoint Security 서비스 보호를 활성화하거나 비활성화합니다.
4. 변경 사항을 저장합니다.

따라서, 사용자가 애플리케이션 서비스를 중지하려고 하면 오류 메시지와 함께 시스템 창이 표시됩니다. 사용자는 Kaspersky Endpoint Security 인터페이스에서만 애플리케이션 서비스를 관리할 수 있습니다.



애플리케이션 서비스 접근 오류

원격 관리 애플리케이션 지원

외부 관리 방역이 작동하는 동안 원격 관리 애플리케이션을 사용해야 할 수 있습니다.

원격 관리 애플리케이션을 작동하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정 → 예외 규칙 및 탐지된 개체의 유형**을 선택합니다.
3. **예외 규칙** 블록에서 **신뢰하는 애플리케이션 지정** 링크를 클릭합니다.
4. 열리는 창에서 **추가** 버튼을 누릅니다.
5. 원격 관리 애플리케이션의 실행 파일을 선택합니다.

   경로를 수동으로 입력할 수도 있습니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.
6. **Kaspersky Endpoint Security 인터페이스와의 상호작용 허용** 확인란을 선택합니다.
7. 변경 사항을 저장합니다.

암호 보호

컴퓨터 활용 능력이 각기 다른 사람들이 한 컴퓨터를 공유하는 경우. 모든 사용자가 Kaspersky Endpoint Security 및 설정에 제한없이 접근할 수 있다면 전반적인 컴퓨터 보호 수준이 저하될 수 있습니다. 암호 보호를 사용하면 사용자에게 부여된 권한(예: 애플리케이션 종료 권한)에 따라 사용자의 Kaspersky Endpoint Security 접근을 제한할 수 있습니다.

Windows 세션을 시작한 사용자(*세션 사용자*)가 동작을 수행할 권한을 갖는 경우, Kaspersky Endpoint Security는 사용자 이름과 암호 또는 임시 암호를 요청하지 않습니다. 사용자는 부여된 권한에 따라 Kaspersky Endpoint Security에 대한 접근 권한을 받습니다.

세션 사용자가 동작을 수행할 권한이 없는 경우에는 다음 방법을 통해 애플리케이션에 대한 접근 권한을 획득할 수 있습니다:

- 사용자 이름과 암호 입력.

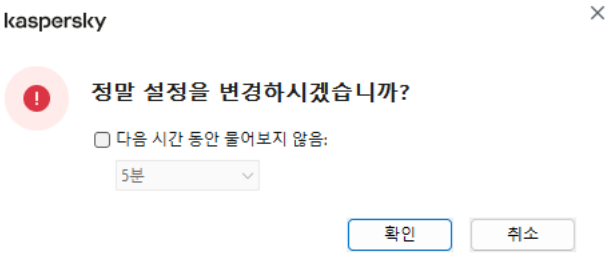
  이 방법은 일상적인 동작에 적합합니다. 암호로 보호된 동작을 수행하려면 필요한 권한이 있는 사용자의 도메인 계정 자격 증명을 입력해야 합니다. 이 경우 컴퓨터는 해당 도메인에 있어야 합니다. 컴퓨터가 도메인에 없는 경우 KLAdmin 계정 또는 수동 추가 계정을 사용할 수 있습니다.

- 임시 암호 입력.

  이 방법은 회사 네트워크 외부에 있는 사용자에게 차단된 동작(예: 애플리케이션 종료)을 수행할 수 있는 임시 권한을 부여하는 데 적합합니다. 임시 암호가 만료되거나 세션이 종료되면 Kaspersky Endpoint Security는 그 설정을 이전 상태로 되돌립니다.

사용자가 암호로 보호된 동작을 수행하려고 할 때 Kaspersky Endpoint Security는 사용자에게 사용자 이름 및 암호 또는 임시 암호를 입력하라는 메시지를 표시합니다(아래 그림 참조).

비밀번호 입력 창에서 **ALT+SHIFT**를 눌러 언어를 전환할 수 있습니다. 운영 체제에서 구성된 다른 단축키를 사용해도 언어가 전환되지 않습니다.



Kaspersky Endpoint Security 접근 암호 물어보기

사용자 이름 및 암호

Kaspersky Endpoint Security에 접근하려면 계정 자격 증명을 입력해야 합니다. 암호 보호는 다음 계정을 지원합니다:

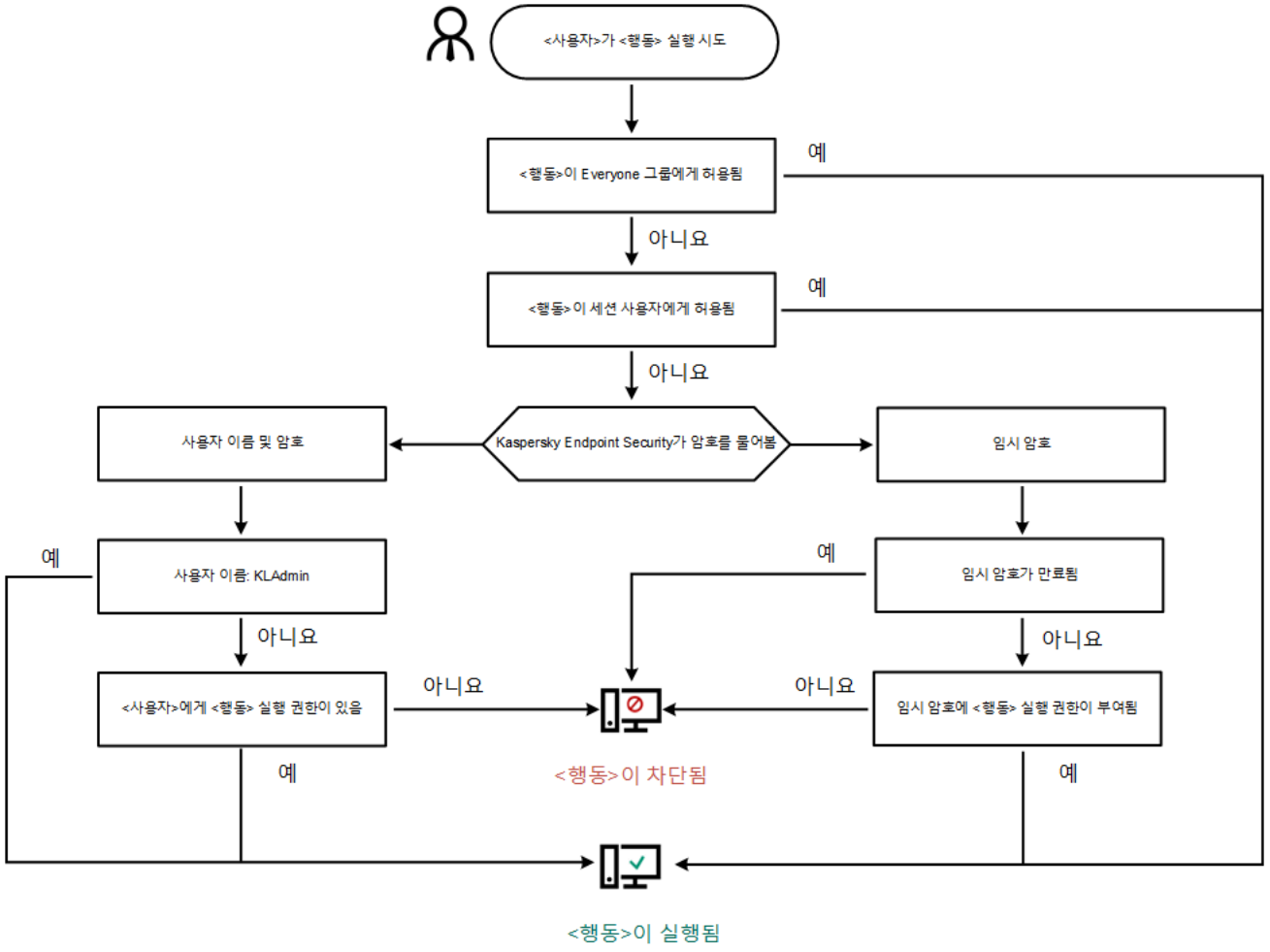
- **KLAdmin**. Kaspersky Endpoint Security에 대한 무제한 접근 권한을 가진 Administrator 계정. KLAdmin 계정에는 암호로 보호된 작업을 수행할 수 있는 권한이 있습니다. KLAdmin 계정에 대한 권한은 철회할 수 없습니다. 암호 보호를 사용하도록 설정하면 KLAdmin 계정의 암호를 설정하라는 메시지를 Kaspersky Endpoint Security가 표시합니다.
- **계정 직접 추가됨**. Active Directory 도메인 외의 계정. 관리자 암호를 공유하고 싶지 않은 경우 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.
- **세션 사용자**. Windows 세션을 시작한 사용자 계정. 암호를 입력하라는 메시지가 표시되면 다른 세션 사용자로 전환할 수 있습니다(**현재 세션에서 이 암호 항상 사용** 확인란). 이 경우 Kaspersky Endpoint Security는 계정 자격 증명이 입력된 사용자를 Windows 세션을 시작한 사용자 대신 해당 세션 사용자로 간주합니다.

임시 암호

임시 암호를 사용하여 회사 네트워크 외부의 개별 컴퓨터에게 Kaspersky Endpoint Security에 대한 임시 접근을 허용할 수 있습니다. 관리자는 Kaspersky Security Center의 해당 컴퓨터 속성에 있는 개별 컴퓨터에 대한 임시 암호를 생성합니다. 관리자는 임시 암호로 보호할 동작을 선택하고 임시 암호의 유효 기간을 지정합니다.

암호 보호 동작 알고리즘

Kaspersky Endpoint Security는 다음 알고리즘에 따라 암호로 보호된 동작을 허용할지 또는 차단할지 결정합니다(아래 그림 참조).



암호 보호 동작 알고리즘

암호 보호 사용

암호 보호를 사용하면 사용자에게 부여된 권한(예: 애플리케이션 종료 권한)에 따라 사용자의 Kaspersky Endpoint Security 접근을 제한할 수 있습니다.

관리 콘솔(MMC)에서 암호 보호를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 인터페이스**를 선택합니다.
4. **암호 보호** 블록에서 **설정** 버튼을 클릭합니다.
   암호 보호 설정이 있는 창이 열립니다.
5. **암호 보호 사용** 확인란으로 구성 요소를 활성화하거나 비활성화합니다.

6. **권한**에서 KLAdmin 계정을 선택합니다.

7. 창이 열리고, 해당 창에서 **암호**를 클릭한 다음 KLAdmin 계정의 암호를 설정합니다.
   KLAdmin 계정에는 암호로 보호된 작업을 수행할 수 있는 권한이 있습니다.

   > KLAdmin 계정 암호를 잊어버렸다면 정책 속성에서 암호를 재설정할 수 있습니다.

8. 계정 목록으로 돌아갑니다.

9. 회사 네트워크 내의 모든 사용자에 대한 권한을 설정합니다:

   a. **권한**에서 "Everyone" 그룹을 선택합니다.
      *Everyone 그룹*은 회사 네트워크 내의 모든 사용자를 포함하는 기본 제공 Windows 그룹입니다.

   b. 열린 창에서 사용자가 암호를 입력하지 않아도 수행할 수 있도록 하는 작업 옆 확인란을 선택합니다.
      확인란을 선택 해제하면 사용자가 해당 작업을 수행할 수 없게 됩니다. 예를 들어 **애플리케이션 종료** 권한 옆의 확인란이 선택 해제되면 KLAdmin으로 로그인하거나 필요한 사용 권한을 가진 개별 사용자 또는 임시 암호를 입력하는 경우에만 애플리케이션을 종료할 수 있습니다.

      > 암호 보호 권한에는 고려해야 할 몇 가지 중요한 점이 있습니다. Kaspersky Endpoint Security에 접근하기 위한 모든 조건이 충족되었는지 확인합니다.

10. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 암호 보호를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **자기 보호**로 갑니다.

5. **암호 보호**에서 **암호 보호 활성화됨** 토글 스위치를 사용하여 구성 요소를 활성화하거나 비활성화합니다.

6. KLAdmin 계정의 암호를 지정하고 이를 확인합니다.
   KLAdmin 계정에는 암호로 보호된 작업을 수행할 수 있는 권한이 있습니다.

   > KLAdmin 계정 암호를 잊어버렸다면 정책 속성에서 암호를 재설정할 수 있습니다.

7. 계정 목록으로 돌아갑니다.

8. 회사 네트워크 내의 모든 사용자에 대한 권한을 설정합니다:

   a. 계정 테이블에서 "Everyone" 그룹을 선택합니다.
      *Everyone 그룹*은 회사 네트워크 내의 모든 사용자를 포함하는 기본 제공 Windows 그룹입니다.

b. 열린 창에서 사용자가 암호를 입력하지 않아도 수행할 수 있도록 하는 작업 옆 확인란을 선택합니다.

확인란을 선택 해제하면 사용자가 해당 작업을 수행할 수 없게 됩니다. 예를 들어 **애플리케이션 종료** 권한 옆의 확인란이 선택 해제되면 KLAdmin으로 로그인하거나 필요한 사용 권한을 가진 개별 사용자 또는 임시 암호를 입력하는 경우에만 애플리케이션을 종료할 수 있습니다.

> 암호 보호 권한에는 고려해야 할 몇 가지 중요한 점이 있습니다. Kaspersky Endpoint Security에 접근하기 위한 모든 조건이 충족되었는지 확인합니다.

9. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 암호 보호를 활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **인터페이스**를 차례로 선택합니다.
3. **암호 보호** 토글로 구성 요소를 사용하거나 중지합니다.
4. KLAdmin 계정의 암호를 지정하고 이를 확인합니다.

KLAdmin 계정에는 암호로 보호된 작업을 수행할 수 있는 권한이 있습니다.

> 컴퓨터가 정책에 의해 실행 중인 경우 관리자는 정책 속성의 KLAdmin 계정에 대한 암호를 초기화할 수 있습니다. 컴퓨터가 Kaspersky Security Center에 연결되어 있지 않고 KLAdmin 계정의 암호를 잊어버린 경우 암호를 복구할 수 없습니다.

5. 회사 네트워크 내의 모든 사용자에 대한 권한을 설정합니다:

a. 계정 테이블에서 **편집** 버튼을 클릭하여 Everyone 그룹에 대한 권한 목록을 엽니다.

*Everyone 그룹*은 회사 네트워크 내의 모든 사용자를 포함하는 기본 제공 Windows 그룹입니다.

b. 사용자가 암호를 입력하지 않아도 수행할 수 있게 하는 작업 옆의 확인란을 선택합니다.

확인란을 선택 해제하면 사용자가 해당 작업을 수행할 수 없게 됩니다. 예를 들어 **애플리케이션 종료** 권한 옆의 확인란이 선택 해제되면 KLAdmin으로 로그인하거나 필요한 사용 권한을 가진 개별 사용자 또는 임시 암호를 입력하는 경우에만 애플리케이션을 종료할 수 있습니다.

> 암호 보호 권한에는 고려해야 할 몇 가지 중요한 점이 있습니다. Kaspersky Endpoint Security에 접근하기 위한 모든 조건이 충족되었는지 확인합니다.

6. 변경 사항을 저장합니다.

암호 보호를 사용하도록 설정하면 애플리케이션은 Everyone 그룹에게 부여된 권한에 따라 Kaspersky Endpoint Security에 대한 사용자의 접근을 제한합니다. KLAdmin 계정이나 필요한 사용 권한이 부여된 다른 계정을 사용하거나 임시 암호를 입력하는 경우에만 Everyone 그룹에 대해 차단된 동작을 수행할 수 있습니다.

> KLAdmin으로 로그인한 경우에만 암호 보호를 비활성화할 수 있습니다. 다른 사용자 계정이나 임시 암호를 사용하는 경우에는 암호 보호를 사용하지 않도록 설정할 수 없습니다.

암호 확인 중에 **현재 세션에서 이 암호 항상 사용** 확인란을 선택할 수 있습니다. 이 경우 사용자가 현재 세션 기간 동안 다른 암호로 보호된 동작을 수행하려고 할 때 Kaspersky Endpoint Security에서 암호를 입력하라는 메시지가 표시되지 않습니다.

개별 사용자 또는 그룹에 사용 권한 부여

암호 보호는 개별 Active Directory 사용자 계정 및 수동으로 추가된 사용자 계정에 Kaspersky Endpoint Security 접근을 허용합니다.

Active Directory 사용자 계정

Active Directory 도메인 내 개별 사용자 또는 그룹에 Kaspersky Endpoint Security 접근을 허용할 수 있습니다. 예를 들어 Everyone 그룹에 대해 애플리케이션 종료가 차단된 경우 개별 사용자에게 **애플리케이션 종료** 권한을 부여할 수 있습니다. 따라서 해당 사용자로 로그인하거나 KLAdmin으로 로그인한 경우에만 애플리케이션을 종료할 수 있습니다.

컴퓨터가 도메인에 있는 경우에만 계정 자격 증명을 사용하여 애플리케이션에 접근할 수 있습니다. 컴퓨터가 도메인에 없는 경우 KLAdmin 계정 또는 임시 암호를 사용할 수 있습니다.

수동으로 추가된 사용자 계정

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 **리포트 보기** 권한을 허용할 수 있습니다. 그 결과 모든 그룹에서 리포트 보기가 금지된 경우 서비스 사용자 계정 또는 KLAdmin 사용자 계정으로 리포트를 열 수 있습니다.

개별 사용자 또는 그룹에 사용 권한 부여

관리 콘솔(MMC)에서 개별 사용자 또는 그룹에 권한을 부여하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 인터페이스**를 선택합니다.
4. **암호 보호** 블록에서 **설정** 버튼을 클릭합니다.
   암호 보호 설정이 있는 창이 열립니다.
5. 계정 표에서 **추가**를 클릭합니다.

6. 추가하려는 사용자 계정 유형을 선택합니다:

   - **Active Directory에서 사용자/그룹 선택** – Active Directory 사용자 계정.

     사용자 계정을 선택하려면 **선택**을 클릭합니다. Active Directory에서 사용자 또는 그룹을 선택하고 선택을 확인합니다.

   - 직접 추가한 서비스 사용자 계정의 경우 **사용자/사용자 그룹을 직접 추가**합니다.

     서비스 사용자 계정을 추가하려면 사용자 이름과 암호를 입력합니다(예: SecureAdmin).

     > 정책 설정에서 서비스 사용자 계정 암호를 초기화할 수 있습니다. 서비스 사용자 계정 암호는 KLAdmin 암호와 동일하게 초기화해야 합니다. 암호 보호 설정을 편집할 수 있거나('잠금'이 풀린 상태) 컴퓨터에 정책이 적용되지 않은 경우, 애플리케이션 인터페이스에서 서비스 사용자 계정의 암호를 초기화할 수 있습니다. 이렇게 하려면 KLAdmin 암호를 사용하여 서비스 사용자 계정 정보의 변경 사항을 확인합니다.

7. **권한** 목록에서 선택한 사용자 또는 그룹이 암호를 입력하지 않고 수행할 수 있는 동작 옆의 확인란을 선택합니다.

   확인란을 선택 해제하면 사용자가 해당 작업을 수행할 수 없게 됩니다. 예를 들어 **애플리케이션 종료** 권한 옆의 확인란이 선택 해제되면 KLAdmin으로 로그인하거나 필요한 사용 권한을 가진 개별 사용자 또는 임시 암호를 입력하는 경우에만 애플리케이션을 종료할 수 있습니다.

   > 암호 보호 권한에는 고려해야 할 몇 가지 중요한 점이 있습니다. Kaspersky Endpoint Security에 접근하기 위한 모든 조건이 충족되었는지 확인합니다.

8. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 개별 사용자 또는 그룹에 권한을 부여하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **자기 보호**로 갑니다.
5. **암호 보호** 블록에서 **사용자 권한** 링크를 클릭합니다.

   암호 활성화 권한 부여 양식이 열립니다.
6. **추가**를 클릭합니다.
7. 추가하려는 사용자 계정 유형을 선택합니다:

   - **Active Directory에서 선택**: Active Directory 사용자 계정.

     사용자 계정을 선택하려면 **편집**을 클릭합니다. Active Directory에서 사용자 또는 그룹을 선택하고 선택을 확인합니다.

   - 직접 추가한 서비스 사용자 계정의 경우 **직접 추가**합니다.

     서비스 사용자 계정을 추가하려면 사용자 이름과 암호를 입력합니다(예: SecureAdmin).

정책 설정에서 서비스 사용자 계정 암호를 초기화할 수 있습니다. 서비스 사용자 계정 암호는 KLAdmin 암호와 동일하게 초기화해야 합니다. 암호 보호 설정을 편집할 수 있거나('잠금'이 풀린 상태) 컴퓨터에 정책이 적용되지 않은 경우, 애플리케이션 인터페이스에서 서비스 사용자 계정의 암호를 초기화할 수 있습니다. 이렇게 하려면 KLAdmin 암호를 사용하여 서비스 사용자 계정 정보의 변경 사항을 확인합니다.

8. **권한** 목록에서 선택한 사용자 또는 그룹이 암호를 입력하지 않고 수행할 수 있는 동작 옆의 확인란을 선택합니다.

   확인란을 선택 해제하면 사용자가 해당 작업을 수행할 수 없게 됩니다. 예를 들어 **애플리케이션 종료** 권한 옆의 확인란이 선택 해제되면 KLAdmin으로 로그인하거나 필요한 사용 권한을 가진 개별 사용자 또는 임시 암호를 입력하는 경우에만 애플리케이션을 종료할 수 있습니다.

암호 보호 권한에는 고려해야 할 몇 가지 중요한 점이 있습니다. Kaspersky Endpoint Security에 접근하기 위한 모든 조건이 충족되었는지 확인합니다.

9. **추가**를 클릭합니다.

10. 변경 사항을 저장합니다.

애플리케이션의 사용자 인터페이스에서 개별 사용자 또는 그룹에 권한을 부여하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **일반 설정** → **인터페이스**를 차례로 선택합니다.

3. 계정 표에서 **추가**를 클릭합니다.

4. 추가하려는 사용자 계정 유형을 선택합니다:

   - **Active Directory에서 사용자/그룹 선택** – Active Directory 사용자 계정.

     사용자 계정을 선택하려면 **사용자 또는 그룹 선택**을 클릭합니다. Active Directory에서 사용자 또는 그룹을 선택하고 선택을 확인합니다.

   - 직접 추가한 서비스 사용자 계정의 경우 **사용자를 직접 추가**합니다.

     서비스 사용자 계정을 추가하려면 사용자 이름과 암호를 입력합니다(예: SecureAdmin).

정책 설정에서 서비스 사용자 계정 암호를 초기화할 수 있습니다. 서비스 사용자 계정 암호는 KLAdmin 암호와 동일하게 초기화해야 합니다. 암호 보호 설정을 편집할 수 있거나('잠금'이 풀린 상태) 컴퓨터에 정책이 적용되지 않은 경우, 애플리케이션 인터페이스에서 서비스 사용자 계정의 암호를 초기화할 수 있습니다. 이렇게 하려면 KLAdmin 암호를 사용하여 서비스 사용자 계정 정보의 변경 사항을 확인합니다.

5. **권한** 목록에서 선택한 사용자 또는 그룹이 암호를 입력하지 않고 수행할 수 있는 동작 옆의 확인란을 선택합니다.

   확인란을 선택 해제하면 사용자가 해당 작업을 수행할 수 없게 됩니다. 예를 들어 **애플리케이션 종료** 권한 옆의 확인란이 선택 해제되면 KLAdmin으로 로그인하거나 필요한 사용 권한을 가진 개별 사용자 또는 임시 암호를 입력하는 경우에만 애플리케이션을 종료할 수 있습니다.

암호 보호 권한에는 고려해야 할 몇 가지 중요한 점이 있습니다. Kaspersky Endpoint Security에 접근하기 위한 모든 조건이 충족되었는지 확인합니다.

6. 변경 사항을 저장합니다.

그 결과 Everyone 그룹에 대해 애플리케이션 접근이 제한되면, 사용자의 개별 권한에 따라 Kaspersky Endpoint Security에 접근할 수 있는 권한이 사용자에게 부여됩니다.

임시 암호를 사용해 권한 부여

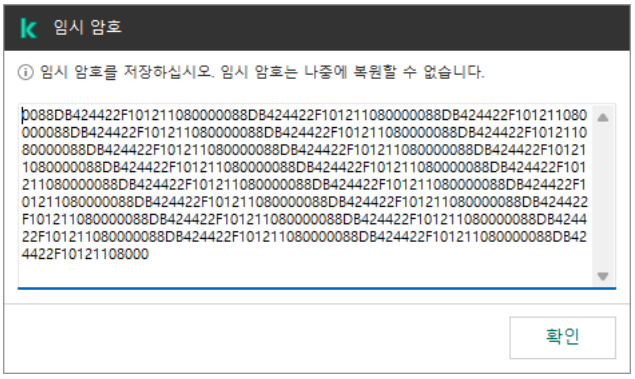
임시 암호를 사용하여 회사 네트워크 외부의 개별 컴퓨터에게 Kaspersky Endpoint Security에 대한 임시 접근을 허용할 수 있습니다. 사용자가 KLAdmin 계정 자격 증명을 얻지 않고 차단된 동작을 수행할 수 있도록 허용하기 위해 필요합니다. 임시 암호를 사용하려면 해당 컴퓨터가 Kaspersky Security Center에 추가되어야 합니다.

관리 콘솔(MMC)에서 사용자가 임시 암호를 사용해 차단된 동작을 수행할 수 있게 하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **기기** 탭을 선택합니다.
4. 더블 클릭해 컴퓨터 속성 창을 엽니다.
5. 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.
6. 컴퓨터에 설치된 Kaspersky 애플리케이션 목록에서 **Kaspersky Endpoint Security for Windows (14.0)**를 선택하고 더블 클릭하여 애플리케이션 속성을 엽니다.
7. 애플리케이션 설정 창에서 **일반 설정** → **인터페이스**를 차례로 선택합니다.
8. **암호 보호** 블록에서 **설정** 버튼을 클릭합니다.
9. 창이 열리면 **임시 암호** 블록에서, **임시 암호 목록** 버튼을 클릭합니다.
   임시 암호 관리 창이 열립니다.
10. **추가**를 클릭합니다.
11. **만료 날짜** 필드에서 임시 암호가 만료되는 만료 날짜를 지정합니다.
12. **임시 암호 범위** 표에서 임시 암호 입력 이후에 사용자에게 허용해야 하는 동작 옆의 확인란을 선택합니다.
13. **생성**을 클릭합니다.
    임시 암호가 들어 있는 창이 열립니다(아래 그림 참조).
14. 해당 암호를 복사하여 요청한 사용자에게 제공합니다.

웹 콘솔 및 Cloud Console에서 사용자가 임시 암호를 사용해 차단된 동작을 수행할 수 있게 하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.
2. 사용자가 차단된 동작을 수행하도록 허용할 컴퓨터 이름을 클릭합니다.
3. **애플리케이션** 탭을 선택합니다.
4. **Kaspersky Endpoint Security for Windows**를 누릅니다.
   그러면 로컬 애플리케이션 설정이 열립니다.
5. **애플리케이션 설정** 탭을 선택합니다.
6. 애플리케이션 설정 창에서 **일반 설정 → 인터페이스**를 차례로 선택합니다.
7. **임시 암호** 블록에서 **추가** 버튼을 클릭합니다.
8. **만료 날짜** 필드에서 임시 암호가 만료되는 만료 날짜를 지정합니다.
9. **임시 암호 범위** 표에서 임시 암호 입력 이후에 사용자에게 허용해야 하는 동작 옆의 확인란을 선택합니다.
10. **생성**을 클릭합니다.
    임시 암호가 담긴 창이 열립니다.
11. 해당 암호를 복사하여 요청한 사용자에게 제공합니다.



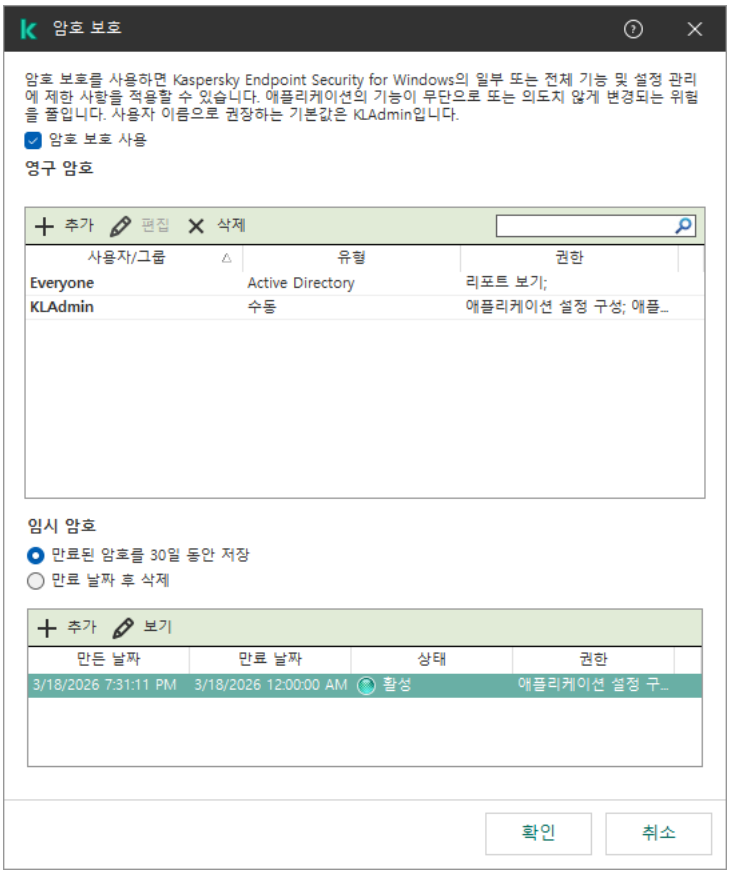
임시 암호

임시 암호 폐기

12.9 버전부터 Kaspersky Endpoint Security for Windows에는 *임시 암호 관리* 기능이 포함됩니다. 임시 암호 관리에서 다음과 같은 동작을 수행할 수 있습니다.

- 암호 내역을 저장합니다(최대 30일).
- 임시 암호 상태 모니터링: *활성*, *만료됨*, *폐기됨*.

- 임시 암호를 폐기합니다.



임시 암호 관리

임시 암호 관리는 컴퓨터를 Kaspersky Security Center와 동기화한 후에만 암호 상태를 업데이트하고 암호를 폐기합니다.

관리 콘솔(MMC)을 사용하여 임시 암호를 폐기하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **기기** 탭을 선택합니다.
4. 더블 클릭해 컴퓨터 속성 창을 엽니다.
5. 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.
6. 컴퓨터에 설치된 Kaspersky 애플리케이션 목록에서 **Kaspersky Endpoint Security for Windows (14.0)**를 선택하고 더블 클릭하여 애플리케이션 속성을 엽니다.
7. 애플리케이션 설정 창에서 **일반 설정** → **인터페이스**를 차례로 선택합니다.
8. **암호 보호** 블록에서 **설정** 버튼을 클릭합니다.
9. 창이 열리면 **임시 암호**에서 만료된 암호의 저장소 설정을 구성합니다.
10. **임시 암호 목록** 버튼을 클릭합니다.

    임시 암호 관리 창이 열립니다. 임시 암호 관리에 암호 만료 날짜, 암호 상태 및 권한 목록이 표시됩니다.
11. 폐기할 활성 임시 암호를 선택하고 암호를 더블 클릭하여 속성을 엽니다.

12. 열리는 창에서 **폐기** 버튼을 누릅니다.

13. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

웹 콘솔 및 Cloud Console을 사용하여 임시 암호를 폐기하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.

2. 사용자가 차단된 동작을 수행하도록 허용할 컴퓨터 이름을 클릭합니다.

3. **애플리케이션** 탭을 선택합니다.

4. **Kaspersky Endpoint Security for Windows**를 누릅니다.
   그러면 로컬 애플리케이션 설정이 열립니다.

5. **애플리케이션 설정** 탭을 선택합니다.

6. 애플리케이션 설정 창에서 **일반 설정 → 인터페이스**를 차례로 선택합니다.

7. **임시 암호**에서 만료된 암호의 저장소를 구성합니다.

8. **임시 암호** 링크를 클릭합니다.
   임시 암호 관리 창이 열립니다. 임시 암호 관리에 암호 만료 날짜, 암호 상태 및 권한 목록이 표시됩니다.

9. 폐기하려는 활성 임시 암호를 선택합니다.

10. 창이 열리면 **암호 폐기** 버튼을 클릭합니다.

11. 변경 사항을 저장합니다. 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다.

결과적으로 임시 암호 관리는 암호 상태를 *폐기 중(호스트와 동기화 중)*으로 설정합니다. 컴퓨터를 Kaspersky Security Center와 동기화하면 애플리케이션이 임시 암호를 폐기하고 부여된 권한을 즉시 차단합니다.

암호 보호 권한의 특별한 점

암호 보호 권한에는 고려해야 할 몇 가지 중요한 점과 제한이 있습니다.

애플리케이션 설정 구성

사용자의 컴퓨터가 정책에 따라 실행 중인 경우 정책에 있는 필요한 모든 설정을 편집할 수 있는지 확인합니다(속성이 열려 있어야 함).

애플리케이션 종료

특별한 고려나 제한은 없습니다.

보호 구성 요소 비활성화

- Everyone 그룹에 대한 보호 구성 요소를 중지할 수 있는 권한을 부여할 수 없습니다. KLAdmin 이외의 사용자가 제어 구성 요소를 중지할 수 있도록 하려면 암호 보호 설정에 **보호 구성 요소 비활성화** 권한이 있는 사용자 또는 그룹을 추가합니다.
- 사용자의 컴퓨터가 정책에 따라 실행 중인 경우 정책에 있는 필요한 모든 설정을 편집할 수 있는지 확인합니다(속성이 열려 있어야 함).
- 애플리케이션 설정에서 보호 구성 요소를 비활성화하려면 사용자에게 **애플리케이션 설정 구성** 권한이 있어야 합니다.
- 마우스 오른쪽 메뉴에서 보호 구성 요소를 중지하려면(**보호 일시 중지** 메뉴 항목 사용) 사용자에게 **보호 구성 요소 비활성화** 권한과 **제어 구성 요소 비활성화** 권한이 있어야 합니다.

제어 구성 요소 비활성화

- Everyone 그룹에 대한 제어 구성 요소를 중지할 수 있는 권한을 부여할 수 없습니다. KLAdmin 이외의 사용자가 제어 구성 요소를 중지할 수 있도록 하려면 암호 보호 설정에 **제어 구성 요소 비활성화** 권한이 있는 사용자 또는 그룹을 추가합니다.
- 사용자의 컴퓨터가 정책에 따라 실행 중인 경우 정책에 있는 필요한 모든 설정을 편집할 수 있는지 확인합니다(속성이 열려 있어야 함).
- 애플리케이션 설정에서 제어 구성 요소를 비활성화하려면 사용자에게 **애플리케이션 설정 구성** 권한이 있어야 합니다.
- 마우스 오른쪽 메뉴에서 제어 구성 요소를 중지하려면(**보호 일시 중지** 메뉴 항목 사용) 사용자에게 **제어 구성 요소 비활성화** 권한과 **보호 구성 요소 비활성화** 권한이 있어야 합니다.

Kaspersky Security Center 정책 비활성화

"Everyone" 그룹에게 Kaspersky Security Center 정책을 비활성화할 수 있는 권한을 부여할 수 없습니다. KLAdmin 이외의 사용자가 정책을 비활성화할 수 있도록 하려면 암호 보호 설정에 **Kaspersky Security Center 정책 비활성화** 권한이 있는 사용자 또는 그룹을 추가합니다.

키 제거

특별한 고려나 제한은 없습니다.

애플리케이션 제거 / 수정 / 복구

"All" 그룹에서 애플리케이션을 제거, 수정, 복원할 수 있도록 허용하면, 사용자가 해당 작업을 시도할 때 Kaspersky Endpoint Security에서 암호를 요청하지 않습니다. 따라서 도메인 외부의 사용자를 포함하여 모든 사용자가 애플리케이션을 설치, 수정, 복원할 수 있습니다.

암호화된 드라이브의 데이터에 대한 접근 복원

KLAdmin으로 로그인한 경우에만 암호화된 드라이브의 데이터에 대한 접근을 복원할 수 있습니다. 이 작업을 수행할 수 있는 사용 권한을 다른 사용자에게 부여할 수 없습니다.

리포트 보기

특별한 고려나 제한은 없습니다.

백업에서 복원

특별한 고려나 제한은 없습니다.

설정 내보내기

기본적으로 "모두" 그룹에 대한 애플리케이션 설정 내보내기는 거부됩니다. KLAdmin 사용자 계정을 사용하여 애플리케이션 설정을 내보낼 수 있습니다. 애플리케이션 설정 내보내기에는 애플리케이션 인터페이스에서 Kaspersky Endpoint Security 설정을 사용하여 구성 파일 생성하기도 포함됩니다. 이 권한은 검사 예외, 신뢰하는 웹 주소, 신뢰하는 장치 또는 애플리케이션 구성 요소에서 유지 관리하는 기타 목록의 내보내기를 제한하지 않습니다.

KLAdmin 암호 재설정

KLAdmin 계정 암호를 잊어버렸다면 정책 속성에서 암호를 재설정할 수 있습니다. 애플리케이션 인터페이스에서는 암호를 재설정할 수 없습니다.

임시 암호를 사용하여 암호로 보호된 작업을 수행할 수 있습니다. 이러면 KLAdmin 자격 증명을 입력할 필요가 없습니다.

컴퓨터가 Kaspersky Security Center에 연결되어 있지 않고 KLAdmin 계정의 암호를 잊어버린 경우 암호를 복구할 수 없습니다.

관리 콘솔(MMC)을 사용하여 KLAdmin 계정 암호를 재설정하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 인터페이스**를 선택합니다.
4. **암호 보호** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **암호 보호 사용** 확인란을 선택 해제합니다.
6. 변경 사항을 저장합니다.
7. **암호 보호 사용** 확인란을 다시 선택합니다.
8. **확인**을 누릅니다.
   그러면 관리자 암호 창이 열립니다.
9. KLAdmin 계정의 새 암호를 지정하고 확인합니다.
10. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 KLAdmin 계정 암호를 재설정하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.
2. 로컬 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.
   그러면 컴퓨터 속성이 열립니다.
3. **애플리케이션** 탭을 선택합니다.
4. **Kaspersky Endpoint Security for Windows**를 누릅니다.
   그러면 로컬 애플리케이션 설정이 열립니다.
5. **애플리케이션 설정** 탭을 선택합니다.
6. **일반 설정 → 자기 보호**로 갑니다.
7. **암호 보호**에서 **암호 보호** 스위치를 끕니다.
8. 변경 사항을 저장합니다.
9. **암호 보호**를 다시 켭니다.
10. KLAdmin 계정의 새 암호를 지정하고 확인합니다.
11. 변경 사항을 저장합니다.

결과적으로 정책이 적용된 후 KLAdmin 계정의 암호가 업데이트됩니다.

중앙 관리 서버 연결 보호

중앙 관리 서버에 컴퓨터를 연결하려면 Kaspersky Security Center의 *네트워크 에이전트* 구성 요소를 사용합니다. 만약 침입자에게 서버 연결 설정을 수정할 수 있는 권한이 있는 경우 신뢰할 수 없는 서버에 컴퓨터를 연결할 위험이 있습니다. 이렇게 하면 침입자는 자신의 그룹 정책을 적용할 수 있으며, 예를 들어 애플리케이션 자기 보호 기능을 비활성화할 수 있습니다. Kaspersky Endpoint Security는 컴퓨터가 다른 서버에 무단으로 다시 연결되는 것을 방지할 수 있습니다. 서버 연결을 보호하기 위해 애플리케이션은 암호 설정 및 암호 기반 키 생성 기능(Password-Based key Derivation Function – PBKDF2) 사용을 제안합니다. 결과적으로 암호 없이 애플리케이션에 액세스하는 것은 불가능하게 됩니다.

Kaspersky Endpoint Security 및 네트워크 에이전트를 무단 액세스로부터 종합적으로 보호하려면 추가적인 보호 기능을 활성화하는 것이 좋습니다. Kaspersky Endpoint Security의 경우, 암호 보호를 활성화하는 것을 권장합니다. 네트워크 에이전트를 보호하려면 제거 암호를 설정하는 것이 좋습니다. 네트워크 에이전트 제거 방지에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

중앙 관리 서버에 컴퓨터 연결을 관리하려면 *중앙 관리 서버 연결 보호* 작업을 사용합니다. 작업으로 다음과 같은 동작을 수행할 수 있습니다.

- 암호를 설정해 서버 연결을 보호합니다.
- 암호를 보호합니다.
- 컴퓨터를 다른 서버에 다시 연결합니다.
- 서버 연결 보호를 비활성화합니다.

중앙 관리 서버에 연결할 때 컴퓨터를 인증합니다.

암호를 설정한 후 애플리케이션이 PBKDF2 암호 변경을 사용해 데이터 배열을 생성합니다. 그러면 애플리케이션이 네트워크 에이전트 키를 사용해 이 데이터 배열을 암호화합니다. 애플리케이션은 암호화된 데이터 배열을 사용해 후속 연결에 대한 중앙 관리 서버의 권한을 확인합니다.

그 뒤에 중앙 관리 서버에 컴퓨터를 다시 연결하려고 시도할 때마다 애플리케이션이 네트워크 에이전트 키로 데이터 배열 암호화를 해제하고 이를 로컬 사본과 비교합니다. 서로 일치하지 안을 경우, 애플리케이션에 대한 액세스가 제한됩니다.

중앙 관리 서버 연결 보호

관리 콘솔(MMC)에서 서버 연결 보호 암호를 설정하는 방법

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

   작업 목록이 열립니다.

2. **새 작업**을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **중앙 관리 서버 연결 보호**를 선택합니다.

2단계. 중앙 관리 서버 연결 보호

중앙 관리 서버 연결을 보호하기 위해 암호를 설정합니다.

1. **중앙 관리 서버 연결 보호**에서 **암호를 사용해 보호**를 선택합니다.
2. **중앙 관리 서버** 드롭다운 목록에서 **새 서버**를 선택합니다.
3. **중앙 관리 서버 연결용 암호** 필드에서 중앙 관리 서버 연결 암호를 설정하고 이를 확인합니다.
   암호를 잊은 경우 작업을 사용해 암호를 변경할 수 있습니다.
4. Kaspersky Endpoint Security 12.7 또는 이전 버전의 애플리케이션이 배포되어 있는 경우 **이전 애플리케이션 버전(12.7 이하)의 암호 암호화 호환성 활성화** 확인란을 선택합니다.
   Kaspersky Endpoint Security 12.8 for Windows 버전부터는 더 강력한 암호 암호화 방식을 사용합니다. Kaspersky Endpoint Security 12.8 이상 버전을 설치한 경우 이 확인란을 선택 해제하고 더 강력한 암호 암호화를 사용하는 것이 권장됩니다. 이전 버전의 애플리케이션은 강력한 암호 암호화를 지원하지 않습니다. 작업을 실행하려면 확인란을 선택해야 합니다.

3단계. 작업을 실행할 계정 선택

기본 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

4 단계. 작업 시작 스케줄 구성

시작 스케줄에서 **수동 시작**을 선택합니다.

5단계. 작업 이름 정의

작업 이름을 입력합니다(예: *주 서버 연결 암호*).

6단계. 작업 생성 완료

마법사를 끝냅니다. **마법사 종료 후 작업 실행** 확인란을 선택하거나 작업을 수동으로 실행합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔 및 Cloud Console에서 서버 연결 보호용 암호를 설정하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **중앙 관리 서버 연결 보호**를 선택합니다.

   c. **작업 이름** 필드에 *주 서버 연결 암호*와 같은 간단한 설명을 입력합니다.

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

4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.

5. 기본 사용자 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. 마법사를 끝냅니다.
   작업 목록에 새 작업이 표시됩니다.

7. Kaspersky Endpoint Security의 **중앙 관리 서버 연결 보호** 작업을 클릭합니다.
   작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. **중앙 관리 서버 연결 보호**에서 **암호를 사용해 보호**를 선택합니다.

10. **중앙 관리 서버 연결** 드롭다운 목록에서 **새로운 암호**를 선택합니다.

11. **암호** 필드에서 중앙 관리 서버 연결용 암호를 설정하고 이를 확인합니다.
    암호를 잊은 경우 작업을 사용해 암호를 변경할 수 있습니다.

12. Kaspersky Endpoint Security 12.7 또는 이전 버전의 애플리케이션이 배포되어 있는 경우 **이전 애플리케이션 버전(12.7 이하)의 암호 암호화 호환성 활성화** 확인란을 선택합니다.

    Kaspersky Endpoint Security 12.8 for Windows 버전부터는 더 강력한 암호 암호화 방식을 사용합니다. Kaspersky Endpoint Security 12.8 이상 버전을 설치한 경우 이 확인란을 선택 해제하고 더 강력한 암호 암호화를 사용하는 것이 권장됩니다. 이전 버전의 애플리케이션은 강력한 암호 암호화를 지원하지 않습니다. 작업을 실행하려면 확인란을 선택해야 합니다.

13. 변경 사항을 저장합니다.

14. 작업 옆의 확인란을 선택합니다.

15. **시작**을 클릭합니다.

작업 상태와 작업이 정상적으로 완료되었거나 완료 시 오류가 발생한 장치의 수를 감시할 수 있습니다.

다른 중앙 관리 서버에 컴퓨터를 다시 연결합니다.

다른 중앙 관리 서버에 컴퓨터를 다시 연결하려면 다음 단계를 실행해야 합니다.

1. 현재 [KSC1] 서버의 콘솔에서 네트워크 에이전트에 대한 *중앙 관리 서버 변경* 작업을 실행합니다.

   작업을 실행하면 컴퓨터가 새로운 [KSC2] 서버에 다시 연결됩니다.

   컴퓨터가 [KSC1] 서버 콘솔에 *심각* 상태로 표시됩니다. 정책을 사용하여 애플리케이션을 구성하거나 컴퓨터에서 원격으로 작업을 실행하는 것이 불가능합니다.

2. 새로운 [KSC2] 서버의 콘솔에서 Kaspersky Endpoint Security에 대한 새로운 *중앙 관리 서버 연결 보호* 작업을 생성합니다. 작업 속성에서 이전 서버의 암호를 입력하고 새 서버의 암호를 설정합니다.

   관리 콘솔(MMC)에서 새 서버에 다시 연결하기 위한 새 암호를 설정하는 방법

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

      작업 목록이 열립니다.

   2. **새 작업**을 클릭합니다.

      작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **중앙 관리 서버 연결 보호**를 선택합니다.

2단계. 중앙 관리 서버 연결 보호

새 중앙 관리 서버와의 연결을 보호할 암호를 설정합니다:

1. **중앙 관리 서버 연결 보호**에서 **암호를 사용해 보호**를 선택합니다.
2. **중앙 관리 서버** 드롭다운 목록에서 **다른 서버에서 다시 연결**을 선택합니다.
3. **현재 암호** 필드에서 이전에 사용한 신뢰하는 서버와의 연결에 설정된 암호를 입력합니다.
4. **새로운 암호** 필드에서 새 중앙 관리 서버와의 연결용 암호를 설정하고 이를 확인합니다.

   암호를 잊은 경우 작업을 사용해 암호를 변경할 수 있습니다.

5. Kaspersky Endpoint Security 12.7 또는 이전 버전의 애플리케이션이 배포되어 있는 경우 **이전 애플리케이션 버전(12.7 이하)의 암호 암호화 호환성 활성화** 확인란을 선택합니다.

   Kaspersky Endpoint Security 12.8 for Windows 버전부터는 더 강력한 암호 암호화 방식을 사용합니다. Kaspersky Endpoint Security 12.8 이상 버전을 설치한 경우 이 확인란을 선택 해제하고 더 강력한 암호 암호화를 사용하는 것이 권장됩니다. 이전 버전의 애플리케이션은 강력한 암호 암호화를 지원하지 않습니다. 작업을 실행하려면 확인란을 선택해야 합니다.

3단계. 작업을 실행할 계정 선택

기본 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

4 단계. 작업 시작 스케줄 구성

시작 스케줄에서 **수동 시작**을 선택합니다.

5단계. 작업 이름 정의

작업 이름을 입력합니다(예: *주 서버 연결 암호*).

6단계. 작업 생성 완료

마법사를 끝냅니다. **마법사 종료 후 작업 실행** 확인란을 선택하거나 작업을 수동으로 실행합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

웹 콘솔 및 Cloud Console에서 새 서버에 다시 연결하기 위한 새 암호를 설정하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **중앙 관리 서버 연결 보호**를 선택합니다.

   c. **작업 이름** 필드에 *주 서버 연결 암호*와 같은 간단한 설명을 입력합니다.

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

4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.

5. 기본 사용자 계정을 선택합니다. 기본적으로 Kaspersky Endpoint Security는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. 마법사를 끝냅니다.

   작업 목록에 새 작업이 표시됩니다.

7. Kaspersky Endpoint Security의 **중앙 관리 서버 연결 보호** 작업을 클릭합니다.

   작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. **중앙 관리 서버 연결 보호**에서 **암호를 사용해 보호**를 선택합니다.

10. **중앙 관리 서버 연결** 드롭다운 목록에서 **다른 서버에서 다시 연결**을 선택합니다.

11. **현재 암호** 필드에서 이전에 사용한 신뢰하는 서버와의 연결에 설정된 암호를 입력합니다.

12. **새로운 암호** 필드에서 새 중앙 관리 서버와의 연결용 암호를 설정하고 이를 확인합니다.

    암호를 잊은 경우 작업을 사용해 암호를 변경할 수 있습니다.

13. Kaspersky Endpoint Security 12.7 또는 이전 버전의 애플리케이션이 배포되어 있는 경우 **이전 애플리케이션 버전(12.7 이하)의 암호 암호화 호환성 활성화** 확인란을 선택합니다.

    Kaspersky Endpoint Security 12.8 for Windows 버전부터는 더 강력한 암호 암호화 방식을 사용합니다. Kaspersky Endpoint Security 12.8 이상 버전을 설치한 경우 이 확인란을 선택 해제하고 더 강력한 암호 암호화를 사용하는 것이 권장됩니다. 이전 버전의 애플리케이션은 강력한 암호 암호화를 지원하지 않습니다. 작업을 실행하려면 확인란을 선택해야 합니다.

14. 변경 사항을 저장합니다.

15. 작업 옆의 확인란을 선택합니다.

16. **시작**을 클릭합니다.

    작업 상태와 작업이 정상적으로 완료되었거나 완료 시 오류가 발생한 장치의 수를 감시할 수 있습니다.

작업을 완료한 후, 새로운 [KSC2] 서버의 콘솔에서 컴퓨터가 *정상* 상태인지 확인합니다. 작업을 원격으로 실행하고 정책을 사용하여 애플리케이션을 구성할 수 있는지 테스트해 봅니다.

중앙 관리 서버 연결 암호 초기화

중앙 관리 서버 연결 암호를 잊어버렸거나 암호가 유출된 경우, 작업 속성에서 암호를 초기화할 수 있습니다. 중앙 관리 서버 연결 보호 상태가 제각기 다른 여러 컴퓨터로 구성된 그룹의 암호를 초기화하고 새 암호를 설정할 수도 있습니다. 즉, 어떤 컴퓨터에는 보호가 활성화되어 있고 또 다른 컴퓨터에는 보호가 비활성화된 경우 이 작업을 수행하면 모든 컴퓨터에 대한 암호가 설정됩니다.

컴퓨터가 연결된 신뢰하는 서버의 콘솔에서만 중앙 관리 서버 연결 암호를 초기화할 수 있습니다.

관리 콘솔(MMC)을 사용하여 중앙 관리 서버 연결 암호를 초기화하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업**을 선택합니다.
3. **중앙 관리 서버 연결 보호** 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.
4. 작업 속성 창에서 **설정** 섹션을 선택합니다.
5. **중앙 관리 서버 연결 보호**에서 **보호 및 암호 변경**을 선택합니다.
6. **중앙 관리 서버 연결용 암호** 필드에서 현재의 신뢰하는 서버와의 연결에 사용할 새 암호를 설정하고 해당 암호를 확인합니다.
7. 변경 사항을 저장합니다.
8. 작업을 실행합니다.

웹 콘솔 및 Cloud Console에서 중앙 관리 서버 연결 암호를 초기화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. Kaspersky Endpoint Security의 **중앙 관리 서버 연결 보호** 작업을 클릭합니다.
   작업 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **중앙 관리 서버 연결 보호**에서 **보호 및 암호 변경**을 선택합니다.
5. **암호** 필드에서 현재의 신뢰하는 서버와의 연결에 사용할 새 암호를 설정하고 해당 암호를 확인합니다.
6. 변경 사항을 저장합니다.
7. 작업 옆의 확인란을 선택합니다.
8. **시작**을 클릭합니다.

이렇게 하면 작업이 완료된 후 중앙 관리 서버 연결 암호가 초기화됩니다.

중앙 관리 서버 연결 보호 중지

컴퓨터가 연결된 신뢰하는 서버의 콘솔에서만 중앙 관리 서버 연결 보호를 원격으로 중지할 수 있습니다. 명령줄에서 로컬로 보호를 비활성화할 수도 있습니다.

관리 콘솔(MMC)에서 서버 연결 보호를 비활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **작업**을 선택합니다.

3. **중앙 관리 서버 연결 보호** 작업을 선택하고 더블 클릭하여 작업 속성을 엽니다.

4. 작업 속성 창에서 **설정** 섹션을 선택합니다.

5. **중앙 관리 서버 연결 보호**에서 **보호 안 함**을 선택합니다.

6. 변경 사항을 저장합니다.

7. 작업을 실행합니다.
   작업 상태와 작업이 정상적으로 완료되었거나 완료 시 오류가 발생한 장치의 수를 감시할 수 있습니다.

웹 콘솔 및 Cloud Console에서 서버 연결 보호를 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. Kaspersky Endpoint Security의 **중앙 관리 서버 연결 보호** 작업을 클릭합니다.
   작업 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **중앙 관리 서버 연결 보호**에서 **보호 안 함**을 선택합니다.

5. 변경 사항을 저장합니다.

6. 작업 옆의 확인란을 선택합니다.

7. **시작**을 클릭합니다.
   작업 상태와 작업이 정상적으로 완료되었거나 완료 시 오류가 발생한 장치의 수를 감시할 수 있습니다.

명령줄에서 서버 연결 보호를 비활성화하는 방법

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.

2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

3. 다음 명령을 실행합니다:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   여기서 `<password>`는 KLAdmin 사용자 계정의 암호 또는 *중앙 관리 서버 연결 보호* 작업의 암호입니다. 파라미터가 지정되지 않은 경우, Kaspersky Endpoint Security에서는 다음 줄에 암호를 입력하라는 메시지가 표시됩니다.

   > 이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다.

예

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

데이터 암호화

Kaspersky Endpoint Security는 로컬 및 이동식 드라이브에 저장된 파일 및 폴더를 암호화하거나, 전체 이동식 드라이브와 하드 드라이브를 암호화할 수 있는 기능을 제공합니다. 데이터 암호화로 휴대용 컴퓨터, 이동식 드라이브 또는 하드 드라이브의 분실이나 도난 또는 데이터의 무단 접근으로 인한 정보 유출 사고의 발생 위험을 최소화할 수 있습니다. Kaspersky Endpoint Security는 AES(Advanced Encryption Standard) 암호화 알고리즘을 사용합니다.

라이센스가 만료된 경우 애플리케이션은 새 데이터를 암호화하지 않으며, 이전에 암호화된 데이터는 암호화된 상태에서 계속 사용할 수 있습니다. 이 경우 새 데이터를 암호화하려면 암호화 사용을 허용하는 새 라이센스를 사용해 애플리케이션을 활성화해야 합니다.

Kaspersky Endpoint Security가 Arm 기반 컴퓨터에 설치된 경우 BitLocker 드라이브 암호화만 사용할 수 있습니다. 애플리케이션이 다른 데이터 암호화 구성 요소를 지원하지 않습니다.

라이센스가 만료되거나 최종 사용자 라이센스 계약서 위반이 발생하거나 라이센스 키, Kaspersky Endpoint Security 또는 암호화 구성 요소가 제거되면 이전에 암호화된 파일의 암호화 상태에 대해 보장할 수 없습니다. 이는 Microsoft Office Word와 같은 일부 애플리케이션에서 편집 시 파일의 임시 복사본을 생성하기 때문입니다. 원래 파일이 저장되면 원래 파일은 임시 복사본으로 교체됩니다. 그 결과 암호화 기능이 없거나 이용할 수 없는 컴퓨터에서는 파일이 계속 암호화되지 않은 상태로 남아 있습니다.

Kaspersky Endpoint Security는 다음과 같은 데이터 보호 기능을 제공합니다:

- **로컬 컴퓨터 드라이브에 대한 파일 레벨 암호화**. 로컬 컴퓨터 드라이브에 저장된 확장자 또는 확장자 그룹별 파일 목록과 폴더별 목록을 컴파일하고, 특정 애플리케이션에 의해 생성된 파일을 암호화하는 규칙을 생성할 수 있습니다. 정책을 적용하면 Kaspersky Endpoint Security에서 다음 파일이 암호화 및 복호화됩니다:
  - 암호화 및 복호화 목록에 개별적으로 추가된 파일;
  - 암호화 및 복호화 목록에 추가된 폴더에 저장된 파일;
  - 개별 애플리케이션에 의해 생성된 파일.
- **이동식 드라이브 암호화**. 기본 암호화 규칙을 지정하여 모든 이동식 드라이브에 동일한 처리 방법을 적용하거나 개별 이동식 드라이브에 대해 별도의 암호화 규칙을 지정할 수 있습니다.

  기본 암호화 규칙은 개별 이동식 드라이브에 만들어진 암호화 규칙보다 우선 순위가 낮습니다. 특정 장치 모델의 이동식 드라이브에 대해 만들어진 암호화 규칙은 특정 장치 ID의 이동식 드라이브를 위해 만들어진 암호화 규칙보다 우선 순위가 낮습니다.

  이동식 드라이브의 파일에 적용할 암호화 규칙을 선택하기 위해 Kaspersky Endpoint Security는 장치 모델 및 ID를 확인합니다. 그런 다음 애플리케이션은 다음 작업 중 하나를 수행합니다:
  - 장치 모델이 확인된 경우에만 애플리케이션은 해당 장치 모델의 이동식 드라이브를 위해 만들어진 암호화 규칙(있을 경우)을 사용합니다.
  - 장치 ID가 확인된 경우에만 애플리케이션은 해당 장치 ID의 이동식 드라이브를 위해 만들어진 암호화 규칙(있을 경우)을 사용합니다.

- 장치 모델과 ID가 확인된 경우 애플리케이션은 해당 장치 ID의 이동식 드라이브를 위해 만들어진 암호화 규칙(있을 경우)을 적용합니다. 그런 규칙은 없지만 특정 장치 모델의 이동식 드라이브에 대해 만들어진 암호화 규칙이 있으면 애플리케이션은 이 규칙을 적용합니다. 특정 장치 ID 또는 특정 장치 모델에 대한 암호화 규칙이 지정되어 있지 않으면 애플리케이션이 기본 암호화 규칙을 적용합니다.

- 장치 모델 및 장치 ID가 모두 확인되지 않은 경우 애플리케이션은 기본 암호화 규칙을 사용합니다.

휴대용 모드에서 이동식 드라이브에 저장된 암호화된 데이터를 사용할 수 있도록 설정할 수 있습니다. 휴대용 모드를 활성화한 다음 암호화 기능이 없는 컴퓨터에 연결된 이동식 드라이브의 암호화된 파일에 접근할 수 있습니다.

- **애플리케이션의 암호화된 파일 접근 규칙 관리**. 애플리케이션에 대해 암호화를 적용할 때 받은 문자 배열에 해당하는 암호문으로만 암호화된 파일 접근을 차단하거나 접근을 허용하는 암호화된 파일 접근 규칙을 만들 수 있습니다.

- **암호화 패키지 생성**. 암호화된 압축 파일을 생성하고 암호를 사용하여 이러한 압축 파일에 대한 접근을 보호할 수 있습니다. 압축 파일 보호 암호를 입력해야만 암호화된 압축 파일의 컨텐츠에 접근할 수 있습니다. 이러한 방법으로 네트워크 또는 이동식 드라이브를 통해 안전하게 압축 파일을 전송할 수 있습니다.

- **전체 디스크 암호화**. 암호화 기술을 선택할 수 있습니다: Kaspersky 디스크 암호화 또는 BitLocker 드라이브 암호화(이후 간단히 "BitLocker"로도 호칭).

  *BitLocker*는 Windows 운영 체제에 포함된 기술입니다. 컴퓨터에 신뢰하는 플랫폼 모듈(Trusted Platform Module, TPM)이 설치되어 있으면 BitLocker가 해당 모듈을 사용해 암호화된 하드 드라이브에 접근할 수 있는 복구 키를 저장합니다. 컴퓨터를 시작할 때 BitLocker는 신뢰하는 플랫폼 모듈의 하드 드라이브 복구 키를 요청하고 드라이브를 잠금 해제합니다. 복구 키 접근에 암호 및/또는 PIN 코드를 사용하도록 구성할 수 있습니다.

  기본 전체 디스크 암호화 규칙을 지정하고 암호화에서 예외할 하드 드라이브 목록을 작성할 수 있습니다. Kaspersky Security Center 정책이 적용되면 Kaspersky Endpoint Security는 섹터별 전체 디스크 암호화를 수행합니다. 애플리케이션은 하드 드라이브의 모든 논리 파티션을 동시에 암호화합니다.

  시스템 하드 드라이브가 암호화된 이후에 컴퓨터를 시작할 때 사용자는 인증 에이전트의 인증을 거쳐야 하드 드라이브 접근 권한이 부여되어 운영 체제가 로드됩니다. 이때 컴퓨터에 연결된 토큰 또는 스마트카드의 암호, 아니면 LAN 관리자가 *인증 에이전트 계정 관리* 작업을 사용해 만든 인증 에이전트 계정의 사용자 이름 및 암호를 입력해야 합니다. 이러한 계정은 운영 체제에 로그인하는 사용자의 Microsoft Windows 계정에 기반합니다. Single Sign-On(SSO) 기술을 사용하면 인증 에이전트 계정의 사용자 이름과 암호를 사용하여 운영 체제에 자동으로 로그인할 수 있습니다.

  > 컴퓨터를 백업한 후 컴퓨터 데이터를 암호화한 다음 컴퓨터의 백업 복사본을 복원하여 컴퓨터 데이터를 다시 암호화하면 Kaspersky Endpoint Security가 인증 에이전트 계정을 중복 생성합니다. 중복 계정을 제거하려면 `dupfix` 키와 함께 klmover 유틸리티를 사용합니다. klmover 유틸리티는 Kaspersky Security Center 빌드에 포함되어 있습니다. Kaspersky Security Center 도움말에서 해당 작업에 대한 자세한 내용을 알아볼 수 있습니다.

  Kaspersky Endpoint Security 및 전체 디스크 암호화 기능이 설치된 컴퓨터에서만 암호화된 하드 드라이브에 접근할 수 있습니다. 이는 회사 LAN 외부에서의 접근을 차단하여 암호화된 하드 드라이브의 데이터 유출 위험을 최소화하기 위해서입니다.

하드 드라이브 및 이동식 드라이브를 암호화하기 위해 사용한 디스크 공간만 암호화 기능을 사용할 수 있습니다. 이전에 사용하지 않은 새 장치인 경우에만 이 기능을 사용하도록 권장됩니다. 이미 사용 중인 장치에 암호화를 적용하는 경우 전체 장치를 암호화하는 것이 좋습니다. 이러면 검색 가능한 정보를 포함한 삭제된 데이터를 비롯한 모든 데이터가 보호됩니다.

암호화가 시작되기 전에 Kaspersky Endpoint Security는 파일 시스템 섹터의 맵을 입수합니다. 암호화 제1 단계에는 암호화가 시작된 시점에 파일이 저장되어 있는 섹터가 포함됩니다. 암호화 제2 단계에는 암호화가 시작된 후 데이터가 쓰여진 섹터가 포함됩니다. 암호화가 완료되면 데이터가 들어 있는 모든 섹터가 암호화됩니다.

암호화가 완료되고 사용자가 파일을 삭제하면 파일 시스템 수준에서 삭제된 파일을 저장했던 섹터를 새 정보를 저장하는 데 사용할 수 있게 되지만 암호화된 상태는 유지됩니다. 그러므로 **사용한 디스크 공간만 암호화** 기능을 작동하여 정기적으로 암호화하는 새 장치에 파일을 쓰는 경우 일정 시간이 지나면 모든 섹터가 암호화됩니다.

파일 복호화에 필요한 데이터는 파일을 암호화한 컴퓨터를 제어하는 Kaspersky Security Center 중앙 관리 서버에서 제공합니다. 특정한 이유로 암호화된 개체가 있는 컴퓨터가 다른 중앙 관리 서버에 의해 관리되는 경우 다음 방법 중 하나로 암호화된 데이터에 접근할 수 있습니다.

- 동일한 계층의 중앙 관리 서버인 경우:
  - 추가 조치를 취할 필요가 없습니다. 사용자는 암호화된 개체에 대한 접근을 유지합니다. 암호화 키는 모든 중앙 관리 서버에 배포됩니다.
- 분리된 중앙 관리 서버인 경우:
  - LAN 관리자에게 암호화된 개체에 대한 접근 권한을 요청합니다.
  - 복원 유틸리티를 사용하여 암호화된 장치에 있는 데이터를 복원합니다.
  - 백업 복사본을 암호화한 컴퓨터를 제어하는 Kaspersky Security Center 중앙 관리 서버의 구성을 복원하여 이 구성을 현재 암호화된 파일이 있는 컴퓨터를 제어하는 관리 서버에 사용합니다.

암호화된 데이터에 접근할 수 없는 경우 암호화된 데이터 작업에 대한 특별 지침을 따르십시오(암호화된 파일에 대한 접근 복원, 암호화된 장치에 접근할 수 없는 경우 장치 사용).

암호화 기능 제한

데이터 암호화에는 다음과 같은 제한이 있습니다:

- 애플리케이션은 암호화 과정에서 서비스 파일을 생성합니다. 이를 저장하려면 하드 드라이브에 단편화되지 않은 여유 공간이 0.5% 정도 있어야 합니다. 하드 드라이브에 디스크 공간이 부족할 경우 충분한 공간이 확보될 때까지 암호화가 시작되지 않습니다.
- Kaspersky Security Center 관리 콘솔 및 Kaspersky Security Center 웹 콘솔에서 모든 데이터 암호화 구성 요소를 관리할 수 있습니다. Kaspersky Security Center Cloud Console에서는 Bitlocker만 관리할 수 있습니다.
- 데이터 암호화는 Kaspersky Endpoint Security를 Kaspersky Security Center 관리 시스템 또는 Kaspersky Security Center Cloud Console(BitLocker만)과 함께 사용하는 경우에만 사용할 수 있습니다. Kaspersky Endpoint Security는 암호화 키를 Kaspersky Security Center에 저장하므로 오프라인 모드에서 Kaspersky Endpoint Security를 사용할 때에는 데이터 암호화를 사용할 수 없습니다.
- Kaspersky Endpoint Security가 서버용 Microsoft Windows를 실행하는 컴퓨터에 설치되어 있으면 BitLocker 드라이브 암호화 기술을 사용한 전체 디스크 암호화만 사용할 수 있습니다. Kaspersky Endpoint Security가 워크스테이션용 Windows를 실행하는 컴퓨터에 설치되어 있는 경우 데이터 암호화 기능을 완전히 사용할 수 있습니다.
- Kaspersky Endpoint Security가 Arm 기반 컴퓨터에 설치되어 있으면 BitLocker 드라이브 암호화 기술을 사용하는 전체 디스크 암호화만 사용할 수 있으며, 다른 암호화 구성 요소는 지원되지 않습니다.

하드 드라이브가 하드웨어 및 소프트웨어 요구 사항을 충족하지 못하면 Kaspersky 디스크 암호화 기술을 사용한 전체 디스크 암호화 기능을 사용할 수 없습니다.

Kaspersky Endpoint Security와 Kaspersky Anti-Virus for UEFI의 전체 디스크 암호화 기능은 호환되지 않습니다. Kaspersky Anti-Virus for UEFI는 운영 체제가 로드되기 전에 시작됩니다. 전체 디스크 암호화를 사용할 때 애플리케이션은 컴퓨터에 설치된 운영 체제가 없음을 탐지합니다. 그러면 Kaspersky Anti-Virus for UEFI의 작동이 종료되며 오류가 발생합니다. 파일 레벨 암호화(FLE)는 UEFI용 Kaspersky Anti-Virus 작동에 영향을 미치지 않습니다.

Kaspersky Endpoint Security는 다음 구성을 지원합니다:

- HDD, SSD 및 USB 드라이브.

  Kaspersky 디스크 암호화(FDE) 기술은 SSD 드라이브의 성능과 서비스 수명을 보존하면서 SSD 작업을 지원합니다.

- 버스를 통해 연결된 드라이브: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.
- SD 또는 MMC 버스를 통해 연결된 고정식 드라이브.
- 512바이트 섹터 드라이브.
- 512바이트를 에뮬레이트하는 4096바이트 섹터 드라이브.
- 다음 유형의 파티션이 있는 드라이브: GPT, MBR 및 VBR(이동식 드라이브).
- UEFI 64 및 Legacy BIOS 표준의 내장 소프트웨어.
- Secure Boot를 지원하는 UEFI 표준의 내장 소프트웨어.

  *Secure Boot*는 UEFI 로더 애플리케이션 및 드라이버에 대한 디지털 서명을 확인하도록 설계된 기술입니다. Secure Boot는 서명되지 않았거나 알 수 없는 게시자가 서명한 UEFI 애플리케이션 및 드라이버의 시작을 차단합니다. Kaspersky 디스크 암호화(FDE)는 Secure Boot를 완벽하게 지원합니다. 인증 에이전트는 Microsoft Windows UEFI 드라이버 게시자 인증서로 서명됩니다.

  일부 장치(Microsoft Surface Pro 및 Microsoft Surface Pro 2 등)에서는 오래된 디지털 서명 확인 인증서 목록이 기본적으로 설치될 수 있습니다. 드라이브를 암호화하기 전에 인증서 목록을 업데이트해야 합니다.

- Fast Boot를 지원하는 UEFI 표준의 내장 소프트웨어.

  *Fast Boot*는 컴퓨터가 더 빨리 시작하도록 도와주는 기술입니다. Fast Boot 기술을 사용하면 일반적으로 컴퓨터는 운영 체제를 시작하는 데 필요한 최소한의 UEFI 드라이버 세트만 로드합니다. Fast Boot 기술을 사용하면 인증 에이전트가 실행되는 동안 USB 키보드, 마우스, USB 토큰, 터치 패드 및 터치스크린이 작동하지 않을 수 있습니다.

  Kaspersky 디스크 암호화(FDE)를 사용하려면 Fast Boot 기술 중지를 권장합니다. FDE 테스트 유틸리티를 사용하여 Kaspersky 디스크 암호화(FDE) 동작을 테스트할 수 있습니다.

Kaspersky Endpoint Security는 다음 구성을 지원하지 않습니다:

- 부트 로더와 운영 체제가 각각 다른 드라이브에 있는 구성.
- 시스템에 UEFI 32 표준의 소프트웨어가 포함되어 있는 구성.
- 시스템에 Intel® Rapid Start 기술이 있으며, Intel® Rapid Start 기술을 중지했을 때에도 절전 파티션을 가지는 드라이브가 있습니다.
- 확장 파티션이 10개 이상인 MBR 포맷 드라이브.

- 시스템의 비 시스템 드라이브에 스왑 파일이 있습니다.
- 동시에 설치된 다수의 운영 체제를 사용하는 멀티 부팅 시스템.
- 다이내믹 파티션(기본 파티션만 지원).
- 단편화되지 않은 디스크 여유 공간이 0.5% 미만인 드라이브.
- 512바이트 또는 512바이트를 에뮬레이션하는 4096바이트로 섹터 크기가 서로 다른 드라이브.
- 하이브리드 드라이브.
- 시스템에 제삼자 로더가 있습니다.
- 압축된 NTFS 디렉토리가 있는 드라이브.
- Kaspersky 디스크 암호화(FDE) 기술은 다른 전체 디스크 암호화 기술(BitLocker, McAfee Drive Encryption, WinMagic SecureDoc 등)과 호환되지 않습니다.
- Kaspersky 디스크 암호화(FDE) 기술은 ExpressCache 기술과 호환되지 않습니다.
- 암호화된 드라이브에서의 파티션 생성, 삭제 및 수정은 지원하지 않습니다. 데이터가 손실될 수 있습니다.
- 파일 시스템 포맷은 지원하지 않습니다. 데이터가 손실될 수 있습니다.

  Kaspersky Disk Encryption(FDE) 기술로 암호화된 드라이브를 포맷할 때는 Kaspersky Endpoint Security for Windows가 없는 컴퓨터에서 드라이브를 포맷하고 전체 디스크 암호화만 사용하십시오.

  빠른 포맷 옵션으로 포맷한 암호화된 드라이브는 다음에 Kaspersky Endpoint Security for Windows가 설치된 컴퓨터에 연결될 때 암호화된 것으로 잘못 식별될 수 있습니다. 사용자 데이터를 사용할 수 없게 됩니다.
- 인증 에이전트는 최대 100개의 계정을 지원합니다.
- Single Sign-On 기술은 제삼자 개발자의 다른 기술과 호환되지 않습니다.
- 다음 모델의 장치에서는 Kaspersky 디스크 암호화(FDE) 기술을 지원하지 않습니다:
  - Dell Latitude E6410(UEFI 모드)
  - HP Compaq nc8430(Legacy BIOS 모드)
  - Lenovo ThinkCentre 8811(Legacy BIOS 모드)
- 인증 에이전트는 레거시 USB 지원을 사용할 때 USB 토큰 작업을 지원하지 않습니다. 컴퓨터에서는 암호 기반 인증만 가능합니다.
- Legacy BIOS 모드에서 드라이브를 암호화할 때 다음 장치 모델에서 레거시 USB 지원을 사용하는 것이 좋습니다:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420

- Dell Inspiron 1545
- Dell Inspiron 1750
- Dell Inspiron N4110
- Dell Latitude E4300
- Dell Studio 1537
- Dell Studio 1569
- Dell Vostro 1310
- Dell Vostro 1320
- Dell Vostro 1510
- Dell Vostro 1720
- Dell Vostro V13
- Dell XPS L502x
- Fujitsu Celsius W370
- Fujitsu LifeBook A555
- HP Compaq dx2450 Microtower PC
- Lenovo G550
- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s(74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51(메인보드)

암호화 키 길이 변경하기(AES56 / AES256)

Kaspersky Endpoint Security는 AES(Advanced Encryption Standard) 암호화 알고리즘을 사용합니다. Kaspersky Endpoint Security는 256비트 또는 56비트의 유효 키 길이를 가진 AES 암호화 알고리즘을 지원합니다. 데이터 암호화 알고리즘은 배포 패키지에 포함된 AES 암호화 라이브러리에 따라 다릅니다: *강한 암호화(AES256)* 또는 *가벼운 암호화(AES56)*. AES 암호화 라이브러리는 애플리케이션과 함께 설치됩니다.

암호화 키 길이를 변경하는 것은 Kaspersky Endpoint Security 11.2.0 이상에서만 사용할 수 있습니다.

암호화 키 길이를 변경하는 작업은 다음 단계로 구성됩니다:

1. 암호화 키 길이를 변경하기 전에 Kaspersky Endpoint Security에서 암호화한 개체를 복호화합니다:
   a. 하드 디스크를 복호화합니다.
   b. 로컬 드라이브의 파일을 복호화합니다.
   c. 이동식 드라이브를 복호화합니다.

   암호화 키 길이를 변경하면 이전에 암호화된 개체는 사용할 수 없게 됩니다.
2. Kaspersky Endpoint Security 제거
3. 다른 암호화 라이브러리가 포함된 Kaspersky Endpoint Security 배포 패키지로부터 Kaspersky Endpoint Security를 설치합니다.

애플리케이션을 업그레이드하여 암호화 키 길이를 변경할 수도 있습니다. 다음 조건이 충족하는 경우에만 애플리케이션 업그레이드를 통해 키 길이를 변경할 수 있습니다:

- Kaspersky Endpoint Security 버전 10 Service Pack 2 이상이 컴퓨터에 설치되어 있습니다.
- 데이터 암호화 구성 요소(파일 레벨 암호화, 전체 디스크 암호화)는 컴퓨터에 설치되지 않습니다.

  기본적으로 데이터 암호화 구성 요소는 Kaspersky Endpoint Security에 포함되어 있지 않습니다. BitLocker 매니지먼트 구성 요소는 암호화 키의 길이 변경에 영향을 주지 않습니다.

암호화 키 길이를 변경하려면 필요한 암호화 라이브러리가 포함된 배포 패키지에 있는 kes_win.msi 또는 setup_kes.exe 파일을 실행합니다. 설치 패키지를 사용하여 원격으로 애플리케이션을 업그레이드할 수도 있습니다.

먼저 애플리케이션을 제거하지 않고 컴퓨터에 설치된 동일한 버전의 애플리케이션 배포 패키지를 사용하여 암호화 키의 길이를 변경하는 것은 불가능합니다.

Kaspersky 디스크 암호화

Kaspersky 디스크 암호화는 Arm 기반 컴퓨터에서는 지원하지 않습니다.

Kaspersky 디스크 암호화는 워크스테이션용 Windows 운영 체제를 실행하는 컴퓨터에서만 사용할 수 있습니다. 서버용 Windows 운영 체제를 실행하는 컴퓨터의 경우 BitLocker 드라이브 암호화 기술을 사용하십시오.

Kaspersky Endpoint Security는 FAT32, NTFS 및 exFat 파일 시스템의 전체 디스크 암호화를 지원합니다.

전체 디스크 암호화를 시작하기 전에 애플리케이션이 시스템 하드 드라이브에서 인증 에이전트 또는 BitLocker 암호화 구성 요소와의 호환성 검사 등 몇 가지 검사를 실행하여 장치를 암호화할 수 있는지 여부를 결정합니다. 호환되는지 확인하려면 컴퓨터를 다시 시작해야 합니다. 컴퓨터가 재부팅된 후에 애플리케이션에서 필요한 모든 점검을 자동으로 실행합니다. 호환성 검사가 성공적으로 완료되면 운영 체제 부팅 및 애플리케이션이 시작한 후에 전체 디스크 암호화가 시작됩니다. 시스템 하드 드라이브가 인증 에이전트 및 BitLocker 암호화 구성 요소와 호환되지 않는 것으로 나타나면 하드웨어 재설정 버튼을 눌러서 컴퓨터를 재부팅해야 합니다. Kaspersky Endpoint Security에서 비호환성에 대한 정보를 로깅합니다. 이 정보를 바탕으로 운영 체제 시작 시 애플리케이션이 전체 디스크 암호화를 시작하지 않습니다. 이 이벤트에 대한 정보가 Kaspersky Security Center 리포트에 기록됩니다.

컴퓨터의 하드웨어 구성이 변경된 경우, 이전 검사 중에 애플리케이션에서 기록한 비호환 정보를 삭제해야 시스템 하드 드라이브에서 인증 에이전트 및 BitLocker 암호화 구성 요소와의 호환성을 검사할 수 있습니다. 이렇게 하려면 전체 디스크 암호화 전에 명령줄에 `avp pbatestreset`이라고 입력합니다. 시스템 하드 드라이브가 인증 에이전트와 호환되는지 검사한 후에 운영 체제의 로드에 실패하는 경우, 복원 유틸리티를 사용하여 인증 에이전트 테스트 작업 이후에 남은 개체 및 데이터를 제거하고 Kaspersky Endpoint Security를 시작하여 `avp pbatestreset` 명령을 다시 실행합니다.

전체 디스크 암호화가 시작되면 Kaspersky Endpoint Security는 하드 드라이브에 저장된 모든 데이터를 암호화합니다.

전체 디스크 암호화 작업 도중에 컴퓨터를 종료하거나 재시작하면 다음 번 운영 체제가 다시 시작되기 전에 인증 에이전트가 시작됩니다. 인증 에이전트의 인증을 거쳐 운영 체제가 시작되면 Kaspersky Endpoint Security가 전체 디스크 암호화 작업을 재개합니다.

전체 디스크 암호화 과정에서 운영 체제가 최대 절전 모드로 바뀔 경우 운영 체제가 다시 일반 모드로 전환할 때 인증 에이전트가 로드됩니다. 인증 에이전트의 인증을 거쳐 운영 체제가 시작되면 Kaspersky Endpoint Security가 전체 디스크 암호화 작업을 재개합니다.

전체 디스크 암호화 과정에서 운영 체제가 절전 모드로 바뀔 경우 운영 체제가 다시 일반 모드로 전환할 때 인증 에이전트가 로드되지 않고 Kaspersky Endpoint Security에서 바로 전체 디스크 암호화 작업을 재개합니다.

인증 에이전트 내의 사용자 인증은 다음 두 가지 방법으로 실행할 수 있습니다:

- LAN 관리자가 Kaspersky Security Center 도구를 사용하여 생성한 인증 에이전트 계정의 이름과 암호 입력.
- 컴퓨터에 연결된 토큰 또는 스마트 카드의 암호 입력.

> 컴퓨터 하드 드라이브가 AES256 암호화 알고리즘을 사용해 암호화된 경우에 토큰 또는 스마트 카드만 사용할 수 있습니다. 컴퓨터 하드 드라이브가 AES56 암호화 알고리즘을 사용해 암호화된 경우에는 해당 명령에 전자 인증서 파일 추가가 거부됩니다.

인증 에이전트는 다음 언어에 대한 키보드 레이아웃을 지원합니다:

- 영어(영국)
- 영어(미국)
- 아랍어(알제리, 모로코, 튀니지; AZERTY 레이아웃)
- 스페인어(라틴 아메리카)
- 이탈리아어
- 독일어(독일, 오스트리아)
- 독일어(스위스)
- 포르투갈어(브라질, ABNT2 레이아웃)
- 러시아어(105-key IBM/QWERTY 레이아웃 Windows 키보드)
- 터키어(QWERTY 레이아웃)
- 프랑스어(프랑스)
- 프랑스어(스위스)
- 프랑스어(벨기에, AZERTY 레이아웃)
- 일본어(QWERTY 레이아웃 106키 키보드)

> 키보드 레이아웃은 운영 체제의 언어 및 지역 표준 설정에서 이 레이아웃이 추가된 경우 인증 에이전트에서 사용할 수 있게 되며 Microsoft Windows의 환영 화면에도 나타납니다.

인증 에이전트 계정 이름에 인증 에이전트에서 사용 가능한 키보드 레이아웃을 사용하여 입력할 수 없는 기호가 포함되어 있다면 복원 유틸리티를 사용하여 복원하거나 인증 에이전트 계정 이름과 암호가 복원된 후에만 암호화된 하드 드라이브에 접근할 수 있습니다.

SSD 드라이브 암호화의 특징

이 애플리케이션은 SSD 드라이브, 하이브리드 SSHD 드라이브 및 Intel Smart Response 기능이 있는 드라이브의 암호화를 지원합니다. 애플리케이션은 Intel Rapid Start 기능이있는 드라이브의 암호화를 지원하지 않습니다. 이러한 드라이브를 암호화하기 전에 Intel Rapid Start 기능을 중지하십시오.

이동식 드라이브 암호화에는 다음과 같은 특징이 있습니다:

- 새 SSD 드라이브에 기밀 데이터가 없는 경우점유 공간만 암호화합니다. 이렇게 하면 관련 드라이브 섹터를 덮어쓸 수 있습니다.
- SSD 드라이브가 사용 중이고 기밀 데이터가 있는 경우 다음 옵션 중 하나를 선택합니다:
  - SSD 드라이브를 완전히 지우고(Secure Erase), 운영 체제 설치 후 점유 공간만 암호화하는 옵션으로 SSD 드라이브의 암호화를 실행합니다.
  - 점유 공간만 암호화하는 옵션을 중지한 후 SSD 드라이브의 암호화를 실행합니다.

SSD 드라이브를 암호화하려면 5~10GB의 여유 공간이 필요합니다. 암호화 관리 데이터를 저장하기 위해 필요한 여유 공간은 아래 표에 나와 있습니다.

암호화 관리 데이터 저장에 필요한 여유 공간

SSD 드라이브 크기(GB)	SSD 드라이브의 기본 파티션에 있는 여유 공간(MB)	SSD 드라이브의 보조 파티션에 있는 여유 공간(MB)
128	250	64
256	250	640
512	300	128

Kaspersky 디스크 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.

디스크 암호화를 시작하기 전에 인증 에이전트 계정의 설정을 확인해야 합니다. Kaspersky 디스크 암호화(FDE) 기술을 사용하여 보호되는 드라이브를 사용하려면 인증 에이전트가 필요합니다. 운영 체제가 로드되기 전에 사용자는 에이전트 인증을 완료해야 합니다. Kaspersky Endpoint Security를 사용하면 드라이브를 암호화하기 전에 인증 에이전트 계정을 자동으로 생성할 수 있습니다. 전체 디스크 암호화 정책 설정(아래 지침 참조)에서 인증 에이전트 계정의 자동 생성을 활성화할 수 있습니다. Single Sign-On(SSO) 기술을 사용할 수도 있습니다.

Kaspersky Endpoint Security를 사용하면 다음 사용자 그룹에 대해 인증 에이전트를 자동으로 생성할 수 있습니다.

- **컴퓨터에 있는 모든 계정**. 항상 활성화된 컴퓨터의 모든 계정.
- **컴퓨터에 있는 모든 도메인**. 일부 도메인에 속하고 항상 활성화된 컴퓨터의 모든 계정.
- **컴퓨터에 있는 모든 로컬 계정**. 항상 활성화된 컴퓨터의 모든 로컬 계정.

- **일회성 암호를 사용하는 서비스 계정**. 서비스 계정은 사용자가 암호를 잊어버렸을 때와 같은 상황에서 컴퓨터에 액세스하는 데 필요합니다. 서비스 계정을 예비 계정으로 사용할 수도 있습니다. 계정 이름을 입력해야 합니다(기본값은 `ServiceAccount`). Kaspersky Endpoint Security는 자동으로 암호를 생성합니다. Kaspersky Security Center 콘솔에서 암호를 볼 수 있습니다.

- **로컬 관리자**. Kaspersky Endpoint Security가 컴퓨터의 로컬 관리자에 대한 인증 에이전트 사용자 계정을 생성합니다.

- **컴퓨터 관리자**. Kaspersky Endpoint Security가 컴퓨터 관리자 계정에 대한 인증 에이전트 사용자 계정을 생성합니다. Active Directory의 컴퓨터 속성에서 컴퓨터 관리자 역할이 있는 계정을 확인할 수 있습니다. 기본적으로 컴퓨터 관리자 역할은 정의되어 있지 않으므로, 어떤 계정에도 해당하지 않습니다.

- **사용 중인 계정**. Kaspersky Endpoint Security는 디스크 암호화 시 활성화된 계정에 대한 인증 에이전트 계정을 자동으로 생성합니다.

인증 에이전트 계정 관리 작업은 사용자 인증 설정을 구성하기 위해 설계되었습니다. 이 작업을 사용하여 새 계정을 추가하거나, 현재 계정의 설정을 수정하거나, 필요 시 계정을 제거할 수 있습니다. 개별 컴퓨터의 로컬 작업과 개별 관리 그룹의 컴퓨터 또는 선택된 컴퓨터에 대한 그룹 작업을 사용할 수 있습니다.

관리 콘솔(MMC)을 통해 Kaspersky 디스크 암호화를 실행하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 전체 디스크 암호화**를 선택합니다.
4. **암호화 기술** 드롭다운 목록에서 **Kaspersky 디스크 암호화**를 선택합니다.

   BitLocker로 컴퓨터 하드 드라이브가 암호화된 경우 Kaspersky 디스크 암호화 기술을 사용할 수 없습니다.

5. **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 암호화**를 선택합니다.

   여러 운영 체제가 설치된 컴퓨터인 경우 모든 하드 드라이브 암호화 후 애플리케이션이 설치된 운영 체제만 로드할 수 있습니다.

   암호화에서 일부 하드 드라이브를 예외해야 한다면 이러한 하드 드라이브의 목록을 생성하십시오.

6. 고급 Kaspersky 디스크 암호화 옵션을 구성하십시오(아래 표 참조).
7. 변경 사항을 저장합니다.

웹 콘솔과 Cloud Console을 통해 Kaspersky 디스크 암호화를 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **데이터 암호화 → 전체 디스크 암호화**로 이동합니다.

5. **Kaspersky 디스크 암호화** 기술을 선택합니다.

BitLocker로 컴퓨터 하드 드라이브가 암호화된 경우 Kaspersky 디스크 암호화 기술을 사용할 수 없습니다.

6. **장치에서의 작업** 블록에서 **모든 하드 드라이브 암호화**를 선택합니다.

여러 운영 체제가 설치된 컴퓨터인 경우 암호화 후 암호화가 수행된 운영 체제만 로드할 수 있습니다.

암호화에서 일부 하드 드라이브를 예외해야 한다면 이러한 하드 드라이브의 목록을 생성하십시오.

7. 고급 Kaspersky 디스크 암호화 옵션을 구성하십시오(아래 표 참조).

8. 변경 사항을 저장합니다.

암호화 모니터 도구를 사용하여 사용자 컴퓨터의 디스크 암호화 또는 복호화 프로세스를 제어할 수 있습니다. 메인 애플리케이션 창에서 암호화 모니터 도구를 실행할 수 있습니다.



암호화 모니터

시스템 하드 드라이브가 암호화된 경우 운영 체제가 시작되기 전에 인증 에이전트가 먼저 로드됩니다. 암호화된 시스템 하드 드라이브에 대한 접근 권한을 획득하고 운영 체제를 로드할 수 있으려면 인증 에이전트의 인증을 거쳐야 합니다. 인증 절차가 성공적으로 완료되면 운영 체제가 로드됩니다. 운영 체제를 다시 시작할 때마다 인증 과정이 반복됩니다.

파라미터	설명
암호화 도중 사용자에 대해 인증 에이전트 계정 자동 생성	이 확인란을 선택하면 애플리케이션이 컴퓨터의 Windows 사용자 계정 목록을 기반으로 인증 에이전트 계정을 만듭니다. 기본적으로 Kaspersky Endpoint Security는 사용자가 지난 30일 동안 운영 체제에 로그인한 모든 로컬 및 도메인 계정을 사용합니다.
이 컴퓨터의 모든 사용자에 대해 로그인 시 인증 에이전트 계정 자동 생성	이 확인란을 선택하면 애플리케이션이 인증 에이전트를 시작하기 전에 컴퓨터의 Windows 사용자 계정에 대한 정보를 확인합니다. Kaspersky Endpoint Security가 인증 에이전트 계정이 없는 Windows 사용자 계정을 감지하면 애플리케이션이 암호화된 드라이브에 접근하기 위한 새 계정을 생성합니다. 새 인증 에이전트 계정에는 다음 기본 설정이 있습니다: 암호를 사용한 로그인만 허용, 첫 인증 후 암호 변경. 따라서 이미 암호화된 드라이브가 있는 컴퓨터에 대해서는 *인증 에이전트 계정 관리* 작업을 사용하여 인증 에이전트 계정을 직접 추가할 필요가 없습니다.
인증 에이전트에 입력되는 사용자 이름 저장	확인란을 선택하면 애플리케이션이 인증 에이전트 계정의 이름을 저장합니다. 다음 번에 동일한 계정을 사용해 인증 에이전트에서 인증할 때 계정 이름을 입력하라고 요구하지 않게 됩니다.
사용한 디스크 공간만 암호화(암호화 시간 단축)	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(암호화 시간 단축)** 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 Endpoint Security는 새로 데이터가 추가될 때마다 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.
레거시 USB 지원 사용(권장 안 함)	이 확인란은 레거시 USB 지원 기능을 활성화하거나 비활성화합니다. *레거시 USB 지원*은 운영 체제(BIOS 모드)를 시작하기 전에 컴퓨터 부팅 단계에서 USB 장치(예: 보안 토큰)를 사용할 수 있는 BIOS/UEFI 기능입니다. 운영 체제가 시작된 후에는 레거시 USB 지원은 USB 장치 지원에 영향을 미치지 않습니다. 이 확인란을 선택하면 컴퓨터 가동을 시작할 때 USB 장치 지원이 작동합니다. 레거시 USB 지원(Legacy USB Support) 기능이 활성화된 경우 BIOS 모드의 인증 에이전트는 USB를 통한 토큰 작업을 지원하지 않습니다. 하드웨어 호환성 문제가 발생한 컴퓨터에 한해서만 이 옵션을 사용하는 것이 좋습니다.

암호화에서 제외할 하드 드라이브의 목록 작성

Kaspersky 디스크 암호화 기술에 한해 암호화 예외 목록을 작성할 수 있습니다.

암호화에서 예외할 하드 드라이브의 목록을 작성하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 전체 디스크 암호화**를 선택합니다.

4. **암호화 기술** 드롭다운 목록에서 **Kaspersky 디스크 암호화**를 선택합니다.
   암호화에서 예외할 하드 드라이브에 해당하는 항목이 **다음 하드 드라이브는 암호화 안 함** 표에 표시됩니다. 이전에 암호화에서 예외할 하드 드라이브의 목록을 작성하지 않은 경우 이 표는 비어 있습니다.

5. 목록에 암호화에서 예외할 하드 드라이브를 추가하려면 다음과 같이 하십시오.

   a. **추가**를 클릭합니다.

   b. 창이 열리면 **장치 이름**, **컴퓨터**, **디스크 유형**, **Kaspersky 디스크 암호화** 값을 지정합니다.

   c. **새로 고침**을 클릭합니다.

   d. **이름** 열에서 암호화를 하지 않을 하드 드라이브의 목록에 추가할 하드 드라이브에 있는 확인란을 선택합니다.

   e. **확인**을 누릅니다.

   선택된 하드 드라이브는 **다음 하드 드라이브는 암호화 안 함** 표에 표시됩니다.

6. 변경 사항을 저장합니다.

암호화에서 제외할 하드 드라이브 목록 내보내기 및 가져오기

하드 드라이브 암호화 예외 규칙 목록을 XML 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 동일 유형의 예외 규칙을 여러 개 추가하는 등의 작업을 진행할 수 있습니다. 내보내기/가져오기 기능을 사용하여 예외 규칙 목록을 백업하거나 예외 규칙을 다른 서버로 마이그레이션할 수도 있습니다.

관리 콘솔(MMC)에서 하드 드라이브 암호화 예외 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 창에서 **데이터 암호화 → 전체 디스크 암호화**를 선택합니다.

4. **암호화 기술** 드롭다운 목록에서 **Kaspersky 디스크 암호화**를 선택합니다.
   암호화에서 예외할 하드 드라이브에 해당하는 항목이 **다음 하드 드라이브는 암호화 안 함** 표에 표시됩니다.

5. 예외 규칙 목록을 내보내려면 다음을 수행합니다.

   a. 내보낼 예외 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.
      예외 규칙을 아무 것도 선택하지 않으면 Kaspersky Endpoint Security가 모든 예외 규칙을 내보냅니다.

   b. → **내보내기** 버튼을 클릭합니다.

   c. 창이 열리면 예외 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

   d. 파일을 저장합니다.
      Kaspersky Endpoint Security는 예외 규칙의 전체 목록을 XML 파일로 내보냅니다.

6. 규칙 목록을 가져오려면 다음을 수행합니다.

   a. → **가져오기** 버튼을 클릭합니다.

   b. 창이 열리면 예외 규칙 목록을 가져올 XML 파일을 선택합니다.

   c. 파일을 엽니다.

      컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

7. 변경 사항을 저장합니다.

웹 콘솔에서 하드 드라이브 암호화 예외 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **데이터 암호화** → **전체 디스크 암호화**로 이동합니다.

   Kaspersky 디스크 암호화 기술을 선택합니다.

5. **예외 규칙** 링크를 클릭합니다.

   예외 규칙 목록이 열립니다.

6. 규칙 목록을 내보내려면 다음을 수행합니다.

   a. 내보낼 예외 규칙을 선택합니다.

   b. → **내보내기** 버튼을 클릭합니다.

      Kaspersky Endpoint Security는 예외 목록을 기본 다운로드 폴더의 JSON 파일로 내보냅니다.

7. 예외 목록을 가져오려면 다음을 수행합니다.

   a. → **가져오기** 버튼을 클릭합니다.

      창이 열리면 예외 규칙 목록을 가져올 JSON 파일을 선택합니다.

   b. 파일을 엽니다.

      컴퓨터에 이미 예외 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 JSON 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. 변경 사항을 저장합니다.

Single Sign-On(SSO) 기술 사용

Single Sign-On(SSO) 기술을 사용하면 인증 에이전트의 자격 증명을 사용하여 운영 체제에 자동으로 로그인할 수 있습니다. 즉, 사용자가 Windows에 로그인할 때 한 번만 암호(인증 에이전트 계정 암호)를 입력하면 됩니다. SSO(Single Sign-On) 기술을 사용하면 Windows 계정 암호가 변경될 때 인증 에이전트 계정 암호를 자동으로 업데이트할 수도 있습니다.

Single Sign-on 기술을 사용하는 경우 인증 에이전트는 Kaspersky Security Center에 지정된 암호 강도 요건을 무시합니다. 운영 체제 설정에서 암호 강도 요건을 설정할 수 있습니다.

SSO(Single Sign-On) 기술 사용

관리 콘솔(MMC)에서 Single Sign-On 기술을 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 일반 암호화 설정**을 선택합니다.
4. **암호 설정** 블록에서 **설정** 버튼을 누릅니다.
5. 창이 열리면 **인증 에이전트** 탭에서 **Single Sign-On(SSO) 기술 사용** 확인란을 선택합니다.
6. 타사 자격 증명 공급업체 사용 시 **타사 자격 증명 공급업체 래핑** 확인란을 선택합니다.
7. 변경 사항을 저장합니다.

그러면 사용자는 에이전트를 사용하여 인증 절차를 한 번만 완료하면 됩니다. 운영 체제를 로드하는 데 인증 절차가 필요하지 않습니다. 운영 체제가 자동으로 로드됩니다.

웹 콘솔에서 Single Sign-On을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **데이터 암호화 → 전체 디스크 암호화**로 이동합니다.
5. **Kaspersky 디스크 암호화** 기술을 선택합니다.
6. **암호 설정** 블록에서 **Single Sign-On(SSO) 기술 사용** 확인란을 선택합니다.
7. 타사 자격 증명 공급업체 사용 시 **타사 자격 증명 공급업체 래핑** 확인란을 선택합니다.
8. 변경 사항을 저장합니다.

그러면 사용자는 에이전트를 사용하여 인증 절차를 한 번만 완료하면 됩니다. 운영 체제를 로드하는 데 인증 절차가 필요하지 않습니다. 운영 체제가 자동으로 로드됩니다.

Single Sign-On이 작동하려면 Windows 계정 암호와 인증 에이전트 계정 암호가 일치해야 합니다. 암호가 일치하지 않을 경우 사용자는 인증 에이전트 인터페이스에서 한 번, 또한 운영 체제를 로드하기 전에 한 번, 인증 절차를 총 두 번 수행해야 합니다. 이러한 작업은 암호 동기화를 위해 한 번만 수행하면 됩니다. 그 후 Kaspersky Endpoint Security가 인증 에이전트 계정 암호를 Windows 계정 암호로 대체합니다. Windows 계정 암호가 변경되면 애플리케이션은 인증 에이전트 계정의 암호를 자동으로 업데이트합니다.

타사 자격 증명 공급업체

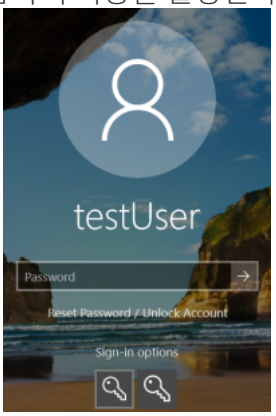
Kaspersky Endpoint Security는 타사 자격 증명 공급업체인 ADSelfService Plus를 지원합니다.

타사 자격 증명 공급업체와 작업 시, 인증 에이전트는 운영 체제가 로드되기 전에 암호를 가로챕니다. 즉, 사용자는 Windows에 로그인할 때 암호를 한 번만 입력하면 됩니다. 사용자는 Windows에 로그인한 후 기업 서비스 인증 등을 위해 타사 자격 증명 공급업체의 기능을 활용할 수 있습니다. 타사 자격 증명 공급업체 사용 시, 사용자가 독자적으로 암호를 재설정할 수도 있습니다. 이때 Kaspersky Endpoint Security는 인증 에이전트의 암호를 자동으로 업데이트합니다.

애플리케이션에서 지원하지 않는 타사 자격 증명 공급업체 사용 시, Single Sign-On 기술 동작에 몇 가지 제한이 생길 수 있습니다. Windows에 로그인할 때 사용자는 시스템 내 자격 증명 공급업체와 타사 자격 증명 공급업체의 두 가지 프로필을 사용할 수 있습니다. 두 프로필의 아이콘은 같습니다(아래 그림 참조). 사용자는 다음 옵션을 사용하여 계속 진행할 수 있습니다.

- 사용자가 *타사 자격 증명 공급업체* 선택 시, 인증 에이전트는 Windows 계정과 암호를 동기화할 수 없습니다. 따라서 사용자가 Windows 계정 암호 변경 시, Kaspersky Endpoint Security는 인증 에이전트 계정의 암호를 업데이트할 수 없습니다. 따라서 사용자는 인증 절차를 인증 에이전트 인터페이스에서 한 번, 운영 체제를 로드하기 전에 한 번, 총 두 번 수행해야 합니다. 이때 사용자는 기업 서비스 인증 등을 위해 타사 자격 증명 공급업체의 기능을 활용할 수 있습니다.

- 사용자가 *시스템 내 자격 증명 공급자* 선택 시, 인증 에이전트는 암호를 Windows 계정과 동기화합니다. 이때 사용자는 기업 서비스 인증 등을 위해 타사 공급자의 기능을 활용할 수 없습니다.



Windows 로그인을 위한 시스템 인증 프로필 및 타사 인증 프로필

인증 에이전트 계정 관리

Kaspersky 디스크 암호화(FDE) 기술을 사용하여 보호되는 드라이브를 사용하려면 인증 에이전트가 필요합니다. 운영 체제가 로드되기 전에 사용자는 에이전트 인증을 완료해야 합니다. *인증 에이전트 계정 관리* 작업은 사용자 인증 설정을 구성하기 위해 설계되었습니다. 개별 컴퓨터의 로컬 작업과 개별 관리 그룹의 컴퓨터 또는 선택된 컴퓨터에 대한 그룹 작업을 사용할 수 있습니다.

인증 에이전트 계정 관리 작업을 시작하기 위한 스케줄을 구성할 수 없습니다. 작업을 강제로 중지하는 것 또한 불가능합니다.

관리 콘솔(MMC)에서 인증 에이전트 계정 관리 작업을 생성하는 방법

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

2. **새 작업**을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **인증 에이전트 계정 관리**를 선택합니다.

2단계. 인증 에이전트 계정 관리 명령 선택

인증 에이전트 계정 관리 명령 목록을 생성합니다. 관리 명령을 사용하면 인증 에이전트 계정을 추가, 수정 및 삭제할 수 있습니다(아래 지침 참조). 인증 에이전트 계정이 있는 사용자만 인증 절차를 완료하고 운영 체제를 로드하며 암호화된 드라이브에 접근할 수 있습니다.

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

작업 이름을 입력합니다(예: *관리자 계정*).

5단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

그러면 다음 컴퓨터 시작시 작업이 완료된 후 새 사용자는 인증 절차를 완료하고 운영 체제를 로드하며 암호화된 드라이브에 접근할 수 있습니다.

웹 콘솔에서 인증 에이전트 계정 관리 작업을 생성하는 방법

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 일반 작업 설정 구성

일반 작업 설정을 구성하려면 다음을 수행하십시오.

1. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows (14.0)**를 선택합니다.
2. **작업 유형** 드롭다운 목록에서 **인증 에이전트 계정 관리**를 선택합니다.
3. **작업 이름** 필드에 *관리자 계정* 등의 간단한 설명을 입력합니다.
4. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.

2단계. 인증 에이전트 계정 관리

인증 에이전트 계정 관리 명령 목록을 생성합니다. 관리 명령을 사용하면 인증 에이전트 계정을 추가, 수정 및 삭제할 수 있습니다(아래 지침 참조). 인증 에이전트 계정이 있는 사용자만 인증 절차를 완료하고 운영 체제를 로드하며 암호화된 드라이브에 접근할 수 있습니다.

3단계. 작업 생성 완료

마법사를 끝냅니다. 작업 목록에 새 작업이 표시됩니다.

작업을 실행하려면 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다.

그러면 다음 컴퓨터 시작시 작업이 완료된 후 새 사용자는 인증 절차를 완료하고 운영 체제를 로드하며 암호화된 드라이브에 접근할 수 있습니다.

인증 에이전트 계정을 추가하려면 *인증 에이전트 계정 관리* 작업에 특수 명령을 추가해야 합니다. 예를 들어 그룹 작업을 사용하여 모든 컴퓨터에 관리자 계정을 추가하는 것이 편리합니다.

Kaspersky Endpoint Security를 사용하면 드라이브를 암호화하기 전에 인증 에이전트 계정을 자동으로 생성할 수 있습니다. 전체 디스크 암호화 정책 설정에서 인증 에이전트 계정의 자동 생성을 활성화할 수 있습니다. Single Sign-On(SSO) 기술을 사용할 수도 있습니다.

관리 콘솔(MMC)을 통해 인증 에이전트 계정을 추가하는 방법

1. *인증 에이전트 계정 관리* 작업의 속성을 엽니다.
2. 작업 속성에서 **설정** 섹션을 선택합니다.
3. **추가 → 계정 추가 명령**을 클릭합니다.
4. 창이 열리면 **Windows 계정** 필드에서 인증 에이전트 계정을 생성하는 데 사용될 Microsoft Windows 계정의 이름을 지정합니다.
5. Windows 계정 이름을 직접 입력한 경우 **허용** 버튼을 클릭하여 계정 보안 식별자(SID)를 정의합니다.

   허용 버튼을 눌러 보안 식별자(SID)를 정하지 않으면, 컴퓨터에서 해당 작업이 수행될 때 보안 식별자(SID)가 정해집니다.

   Windows 계정 보안 식별자를 정의하여 Windows 계정 이름이 올바르게 입력되었는지 확인합니다. 컴퓨터 또는 신뢰하는 도메인에 Windows 계정이 없는 경우 *인증 에이전트 계정 관리* 작업이 오류와 함께 종료됩니다.

6. 인증 에이전트에 대해 이전에 생성된 계정을 새로 생성되는 계정으로 교체하려면 **기존 계정 교체** 확인란을 선택합니다.

   인증 에이전트 계정 관리를 위한 그룹 작업의 속성에 인증 에이전트 계정 생성 명령을 추가할 때 이 단계가 제공됩니다. *인증 에이전트 계정 관리* 로컬 작업의 속성에서 인증 에이전트 계정 생성 명령어를 추가할 시 이 단계를 적용할 수 없습니다.

7. **사용자 이름** 필드에 암호화된 하드 드라이브 접근을 위한 인증에서 입력해야 하는 인증 에이전트 계정의 이름을 입력합니다.
8. 인증 중에 암호화된 하드 드라이브에 접근하기 위해서는 인증 에이전트 계정 암호를 입력해야 한다는 메시지를 애플리케이션에서 표시하게 하려면 **암호 기반 인증 허용** 확인란을 선택하십시오. 인증 에이전트 계정의 암호를 설정합니다. 필요한 경우 첫 번째 인증 후 사용자에게 새 암호를 요청할 수 있습니다.
9. 인증 중에 암호화된 하드 드라이브에 접근하기 위해 토큰이나 스마트 카드를 이용해야 한다는 메시지를 애플리케이션에서 표시하게 하려면 **인증서 기반 인증 허용** 확인란을 선택하십시오. 스마트 카드 또는 토큰으로 인증할 인증서 파일을 선택합니다.
10. 필요하다면, **명령 설명** 필드에 명령 관리를 위한 자세한 인증 에이전트 계정 정보를 입력합니다.
11. **인증 에이전트에서 인증 창에 접근** 블록에서, 명령에 지정된 계정을 사용하는 사용자를 대상으로 인증 에이전트의 인증에 대한 접근을 구성합니다.
12. 변경 사항을 저장합니다.

웹 콘솔을 통해 인증 에이전트 계정을 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 작업**을 선택합니다.

   작업 목록이 열립니다.

2. Kaspersky Endpoint Security의 **인증 에이전트 계정 관리** 작업을 클릭합니다.

   작업 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. 인증 에이전트 계정 목록에서 **추가** 버튼을 누릅니다.

   인증 에이전트 계정 관리 마법사가 시작됩니다.

5. **추가** 명령 유형을 선택합니다.

6. 사용자 계정을 선택합니다. 도메인 계정 목록에서 계정을 선택하거나 계정 이름을 직접 입력할 수 있습니다. 다음 단계로 넘어갑니다.

   Kaspersky Endpoint Security는 계정 보안 식별자(SID)를 결정합니다. 이는 계정을 확인하는 데 필요합니다. 사용자 이름을 잘못 입력하면 Kaspersky Endpoint Security가 오류와 함께 작업을 종료합니다.

7. 인증 에이전트 계정 설정을 구성합니다.

   - **기존 계정을 대체할 새 인증 에이전트 계정 생성**. Kaspersky Endpoint Security는 컴퓨터에서 기존 계정을 검색합니다. 컴퓨터와 작업의 사용자 보안 ID가 일치하면 Kaspersky Endpoint Security는 작업에 따라 계정 설정을 변경합니다.

   - **사용자 이름**. 인증 에이전트 계정의 기본 사용자 이름은 사용자의 도메인 이름에 해당합니다.

   - **암호 기반 인증 허용**. 인증 에이전트 계정의 암호를 설정합니다. 필요한 경우 첫 번째 인증 후 사용자에게 새 암호를 요청할 수 있습니다. 이러한 방식으로 각 사용자는 고유한 암호를 갖게 됩니다. 정책에서 인증 에이전트 계정에 대한 암호 강도 요건을 설정할 수도 있습니다.

   - **인증서 기반 인증 허용**. 스마트 카드 또는 토큰으로 인증할 인증서 파일을 선택합니다. 이런 식으로 사용자는 스마트 카드 또는 토큰의 암호를 입력해야 합니다.

   - **암호화된 데이터에 대한 계정 접근**. 암호화된 드라이브에 대한 사용자 접근을 구성합니다. 예를 들어 인증 에이전트 계정을 삭제하는 대신 사용자 인증을 일시적으로 비활성화할 수 있습니다.

   - **설명**. 필요시 계정 설명을 입력합니다.

8. 변경 사항을 저장합니다.

9. 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다.

   그러면 다음 컴퓨터 시작시 작업이 완료된 후 새 사용자는 인증 절차를 완료하고 운영 체제를 로드하며 암호화된 드라이브에 접근할 수 있습니다.

인증 에이전트 계정의 암호 및 기타 설정을 변경하려면 *인증 에이전트 계정 관리* 작업에 특수 명령을 추가해야 합니다. 예를 들어 그룹 작업을 사용하여 모든 컴퓨터에서 관리자 토큰 인증서를 교체하는 것이 편리합니다.

관리 콘솔(MMC)을 통해 인증 에이전트 계정을 변경하는 방법

1. *인증 에이전트 계정 관리* 작업의 속성을 엽니다.

2. 작업 속성에서 **설정** 섹션을 선택합니다.

3. **추가 → 계정 편집 명령**을 클릭합니다.

4. 창이 열리면 **Windows 계정** 필드에서 변경하려는 Microsoft Windows 사용자 계정의 이름을 지정합니다.

5. Windows 계정 이름을 직접 입력한 경우 **허용** 버튼을 클릭하여 계정 보안 식별자(SID)를 정의합니다.

   허용 버튼을 눌러 보안 식별자(SID)를 정하지 않으면, 컴퓨터에서 해당 작업이 수행될 때 보안 식별자(SID)가 정해집니다.

Windows 계정 보안 식별자를 정의하여 Windows 계정 이름이 올바르게 입력되었는지 확인합니다. 컴퓨터 또는 신뢰하는 도메인에 Windows 계정이 없는 경우 *인증 에이전트 계정 관리* 작업이 오류와 함께 종료됩니다.

6. **Windows 계정** 필드에 이름이 지정된 Microsoft Windows 계정에 기반하여 생성된 모든 인증 에이전트 사용자 계정의 사용자 이름을 아래 필드에 입력된 이름으로 변경하려면 **사용자 이름 변경** 확인란을 선택하고 인증 에이전트 사용자 계정의 새 이름을 입력합니다.

7. **암호 기반 인증 설정 변경** 확인란을 선택하여 암호 기반 인증 설정을 편집 가능하게 만듭니다.

8. 인증 중에 암호화된 하드 드라이브에 접근하기 위해서는 인증 에이전트 계정 암호를 입력해야 한다는 메시지를 애플리케이션에서 표시하게 하려면 **암호 기반 인증 허용** 확인란을 선택하십시오. 인증 에이전트 계정의 암호를 설정합니다.

9. **Windows 계정** 필드에 지정된 이름의 Microsoft Windows 계정에 따라 생성된 모든 인증 에이전트 계정에 대해 암호 변경 설정의 값을 아래 지정된 설정값으로 변경하려면 **인증 에이전트에서 인증 시 암호 변경 규칙 편집** 확인란을 선택합니다.

10. 인증 에이전트에서 인증 시 암호 변경 설정의 값을 지정합니다.

11. **인증서 기반 인증 설정 변경** 확인란을 선택하여 토큰 또는 스마트 카드의 전자 인증서 기반 인증 설정을 편집 가능하게 만듭니다.

12. 인증 프로세스 중에 암호화된 하드 드라이브에 접근하기 위해서는 컴퓨터에 연결된 토큰 또는 스마트 카드에 대한 암호를 입력해야 한다는 메시지를 애플리케이션에서 표시하게 하려면 **인증서 기반 인증 허용** 확인란을 선택하십시오. 스마트 카드 또는 토큰으로 인증할 인증서 파일을 선택합니다.

13. **Windows 계정** 필드에 이름이 지정된 Microsoft Windows 계정에 기반하여 생성된 모든 인증 에이전트 계정의 명령 설명을 변경하려면 **명령 설명 편집** 확인란을 선택하고 명령 설명을 편집합니다.

14. **Windows 계정** 필드에 이름이 지정된 Microsoft Windows 계정에 기반하여 생성된 모든 인증 에이전트 계정에 대해 인증 에이전트에서 인증 시 사용자 접근 규칙을 아래 지정된 값으로 변경하려면 **인증 에이전트에서 인증 창에 접근할 때 규칙 편집** 확인란을 선택합니다.

15. 인증 에이전트의 인증 대화 상자에 접근하는 규칙을 지정합니다.

16. 변경 사항을 저장합니다.

웹 콘솔을 통해 인증 에이전트 계정을 변경하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.

   작업 목록이 열립니다.

2. Kaspersky Endpoint Security의 **인증 에이전트 계정 관리** 작업을 클릭합니다.

   작업 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. 인증 에이전트 계정 목록에서 **추가** 버튼을 누릅니다.

   인증 에이전트 계정 관리 마법사가 시작됩니다.

5. **변경** 명령 유형을 선택합니다.

6. 사용자 계정을 선택합니다. 도메인 계정 목록에서 계정을 선택하거나 계정 이름을 직접 입력할 수 있습니다. 다음 단계로 넘어갑니다.

   Kaspersky Endpoint Security는 계정 보안 식별자(SID)를 결정합니다. 이는 계정을 확인하는 데 필요합니다. 사용자 이름을 잘못 입력하면 Kaspersky Endpoint Security가 오류와 함께 작업을 종료합니다.

7. 편집하려는 설정 옆의 확인란을 선택합니다.

8. 인증 에이전트 계정 설정을 구성합니다.

   - **기존 계정을 대체할 새 인증 에이전트 계정 생성**. Kaspersky Endpoint Security는 컴퓨터에서 기존 계정을 검색합니다. 컴퓨터와 작업의 사용자 보안 ID가 일치하면 Kaspersky Endpoint Security는 작업에 따라 계정 설정을 변경합니다.

   - **사용자 이름**. 인증 에이전트 계정의 기본 사용자 이름은 사용자의 도메인 이름에 해당합니다.

   - **암호 기반 인증 허용**. 인증 에이전트 계정의 암호를 설정합니다. 필요한 경우 첫 번째 인증 후 사용자에게 새 암호를 요청할 수 있습니다. 이러한 방식으로 각 사용자는 고유한 암호를 갖게 됩니다. 정책에서 인증 에이전트 계정에 대한 암호 강도 요건을 설정할 수도 있습니다.

   - **인증서 기반 인증 허용**. 스마트 카드 또는 토큰으로 인증할 인증서 파일을 선택합니다. 이런 식으로 사용자는 스마트 카드 또는 토큰의 암호를 입력해야 합니다.

   - **암호화된 데이터에 대한 계정 접근**. 암호화된 드라이브에 대한 사용자 접근을 구성합니다. 예를 들어 인증 에이전트 계정을 삭제하는 대신 사용자 인증을 일시적으로 비활성화할 수 있습니다.

   - **설명**. 필요시 계정 설명을 입력합니다.

9. 변경 사항을 저장합니다.

10. 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다.

인증 에이전트 계정을 삭제하려면 *인증 에이전트 계정 관리* 작업에 특수 명령을 추가해야 합니다. 예를 들어 그룹 작업을 사용하여 해고된 직원의 계정을 삭제하는 것이 편리합니다.

관리 콘솔(MMC)을 통해 인증 에이전트 계정을 삭제하는 방법

1. *인증 에이전트 계정 관리* 작업의 속성을 엽니다.

2. 작업 속성에서 **설정** 섹션을 선택합니다.

3. **추가 → 계정 삭제 명령**을 클릭합니다.

4. 창이 열리면 **Windows 계정** 필드에 삭제할 인증 에이전트 계정이 생성된 Windows 사용자 계정 이름을 지정합니다.

5. Windows 계정 이름을 직접 입력한 경우 **허용** 버튼을 클릭하여 계정 보안 식별자(SID)를 정의합니다.

   허용 버튼을 눌러 보안 식별자(SID)를 정하지 않으면, 컴퓨터에서 해당 작업이 수행될 때 보안 식별자(SID)가 정해집니다.

   > Windows 계정 보안 식별자를 정의하여 Windows 계정 이름이 올바르게 입력되었는지 확인합니다. 컴퓨터 또는 신뢰하는 도메인에 Windows 계정이 없는 경우 *인증 에이전트 계정 관리* 작업이 오류와 함께 종료됩니다.

6. 변경 사항을 저장합니다.

웹 콘솔을 통해 인증 에이전트 계정을 삭제하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 작업**을 선택합니다.
   작업 목록이 열립니다.

2. Kaspersky Endpoint Security의 **인증 에이전트 계정 관리** 작업을 클릭합니다.
   작업 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. 인증 에이전트 계정 목록에서 **추가** 버튼을 누릅니다.
   인증 에이전트 계정 관리 마법사가 시작됩니다.

5. **삭제** 명령 유형을 선택합니다.

6. 사용자 계정을 선택합니다. 도메인 계정 목록에서 계정을 선택하거나 계정 이름을 직접 입력할 수 있습니다.

7. 변경 사항을 저장합니다.

8. 작업 옆의 확인란을 선택하고 **시작** 버튼을 누릅니다.

그러면 다음 컴퓨터 시작시 작업이 완료된 후 사용자는 인증 절차를 완료하고 운영 체제를 로드할 수 없습니다. Kaspersky Endpoint Security는 암호화된 데이터에 대한 접근을 거부합니다.

에이전트 인증을 완료하고 운영 체제를 로드할 수 있는 사용자 목록을 보려면 관리 중인 컴퓨터의 속성으로 이동해야 합니다.

관리 콘솔(MMC)을 통해 인증 에이전트 계정 목록을 보는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 콘솔 트리에서 **기기**를 선택합니다.

3. 더블 클릭해 컴퓨터 속성 창을 엽니다.

4. 컴퓨터 속성 창에서 **작업** 섹션을 선택합니다.

5. 작업 목록에서 **인증 에이전트 계정 관리**를 선택하고 더블 클릭하여 작업 속성을 엽니다.

6. 작업 속성에서 **설정** 섹션을 선택합니다.

그러면 이 컴퓨터의 인증 에이전트 계정 목록에 접근할 수 있습니다. 목록의 사용자만 에이전트 인증을 완료하고 운영 체제를 로드할 수 있습니다.

웹 콘솔을 통해 인증 에이전트 계정 목록을 보는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.

2. 인증 에이전트 계정 목록을 보려는 컴퓨터의 이름을 클릭합니다.

3. 컴퓨터 속성에서 **작업** 탭을 선택합니다.

4. 작업 목록에서 **인증 에이전트 계정 관리**를 선택합니다.

5. 작업 속성에서 **애플리케이션 설정** 탭을 선택합니다.

그러면 이 컴퓨터의 인증 에이전트 계정 목록에 접근할 수 있습니다. 목록의 사용자만 에이전트 인증을 완료하고 운영 체제를 로드할 수 있습니다.

인증 에이전트에서 토큰 및 스마트 카드 사용

암호화된 하드 드라이브에 접근할 때 토큰 또는 스마트 카드를 인증에 사용할 수 있습니다. 그렇게 하려면 토큰 또는 스마트 카드의 전자 인증서 파일을 *인증 에이전트 계정 관리* 작업에 추가해야 합니다.

컴퓨터 하드 드라이브가 AES256 암호화 알고리즘을 사용해 암호화된 경우에 토큰 또는 스마트 카드만 사용할 수 있습니다. 컴퓨터 하드 드라이브가 AES56 암호화 알고리즘을 사용해 암호화된 경우에는 해당 명령에 전자 인증서 파일 추가가 거부됩니다.

Kaspersky Endpoint Security는 다음 토큰, 스마트 카드 리더기 및 스마트 카드를 지원합니다:

- SafeNet eToken PRO 64K(4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

토큰 또는 스마트 카드 전자 인증서의 파일을 인증 에이전트 계정 생성 명령에 추가하려면 먼저 인증서를 관리하는 타사 소프트웨어를 사용하여 인증서 파일을 내보낸 다음 하드 드라이브에 저장하십시오.

토큰 또는 스마트 카드 인증서는 다음 속성을 가지고 있어야 합니다:

- 인증서는 X.509 표준을 준수해야 하며 인증서 파일에 DER 인코딩이 있어야 합니다.
- 인증서에 길이가 1024비트 이상인 RSA 키가 포함되어 있습니다.

토큰 또는 스마트 카드의 전자 인증서가 이러한 요건을 충족하지 않으면 인증 에이전트 계정 생성 명령에 인증서 파일을 로드할 수 없습니다.

인증서의 `KeyUsage` 파라미터에는 `keyEncipherment` 또는 `dataEncipherment` 값이 있어야 합니다. `KeyUsage` 파라미터는 인증서의 목적을 결정합니다. 파라미터의 값이 다른 경우 Kaspersky Security Center는 인증서 파일을 다운로드하지만 경고를 표시합니다.

사용자가 토큰 또는 스마트 카드를 분실한 경우, 관리자는 인증 에이전트 계정을 만드는 명령에 토큰 또는 스마트 카드 전자 인증서 파일을 추가해야 합니다. 그런 다음 사용자는 암호화된 장치에 대한 접근 권한을 받거나 암호화된 장치에서 데이터를 복원하는 절차를 완료해야 합니다.

하드 드라이브 복호화

데이터 암호화를 허용하는 현재 라이센스가 없더라도 하드 드라이브를 복호화할 수 있습니다.

하드 드라이브를 복호화하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 전체 디스크 암호화**를 선택합니다.
4. **암호화 기술** 드롭다운 목록에서 하드 드라이브에 적용된 암호화 기술을 선택합니다.
5. 다음 중 하나를 수행합니다:
   - **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 복호화** 옵션을 선택하여 암호화된 모든 하드 드라이브를 복호화합니다.
   - **다음 하드 드라이브는 암호화 안 함** 표에 복호화할 암호화된 하드 드라이브를 추가합니다.

     Kaspersky 디스크 암호화 기술에 한해 이 옵션을 사용할 수 있습니다.
6. 변경 사항을 저장합니다.

암호화 모니터 도구를 사용하여 사용자 컴퓨터의 디스크 암호화 또는 복호화 프로세스를 제어할 수 있습니다. 메인 애플리케이션 창에서 암호화 모니터 도구를 실행할 수 있습니다.



암호화 모니터

Kaspersky 디스크 암호화 기술을 사용해 암호화된 하드 드라이브를 복호화하는 도중에 컴퓨터를 종료하거나 재부팅하면, 다음 운영 체제가 다시 시작되기 전 인증 에이전트가 로드됩니다. 인증 에이전트의 인증을 거쳐 운영 체제가 시작되면 Kaspersky Endpoint Security가 하드 드라이브 복호화 작업을 재개합니다.

Kaspersky 디스크 암호화 기술을 사용해 암호화된 하드 드라이브를 복호화하는 도중에 운영 체제가 최대 절전 모드로 바뀔 경우 운영 체제가 다시 일반 모드로 전환할 때 인증 에이전트가 로드됩니다. 인증 에이전트의 인증을 거쳐 운영 체제가 시작되면 Kaspersky Endpoint Security가 하드 드라이브 복호화 작업을 재개합니다. 하드 드라이브 복호화 후 운영 체제를 재부팅하기 전에는 최대 절전 모드를 사용할 수 없습니다.

하드 드라이브 복호화 과정에서 운영 체제가 절전 모드로 바뀔 경우 운영 체제가 다시 일반 모드로 전환할 때 인증 에이전트가 로드되지 않고 Kaspersky Endpoint Security에서 바로 하드 드라이브 복호화 작업을 재개합니다.

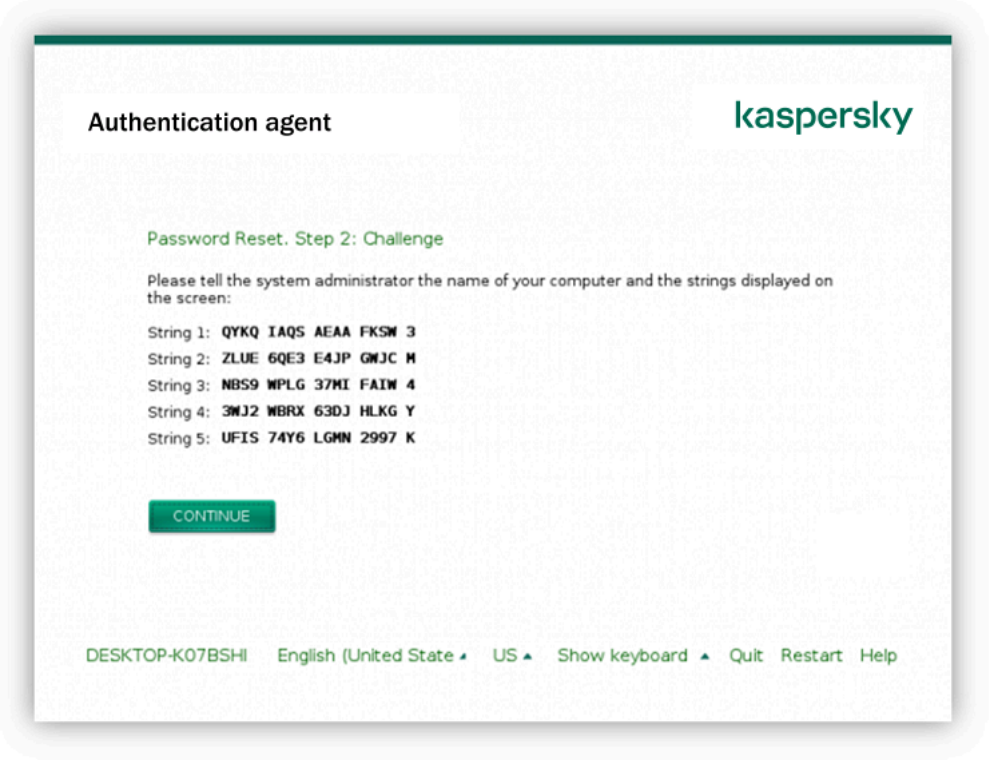
Kaspersky 디스크 암호화 기술로 보호되는 드라이브에 대한 접근 복원

사용자가 Kaspersky 디스크 암호화 기술로 보호되는 하드 드라이브에 접근하기 위한 암호를 잊어버린 경우 복원 절차(요청-응답)를 시작해야 합니다. 디스크 암호화 설정에서 이 기능이 활성화되었다면 서비스 계정을 사용하여 하드 디스크에 접근할 수 있습니다.

시스템 하드 드라이브에 대한 접근 복원

Kaspersky 디스크 암호화 기술로 보호되는 시스템 하드 드라이브에 대한 접근 복원은 다음 단계로 구성됩니다.

1. 사용자는 요청 블록을 관리자에게 보고합니다(아래 그림 참조).
2. 관리자는 요청 블록을 Kaspersky Security Center에 입력하고 응답 블록을 수신한 후 응답 블록을 사용자에게 보고합니다.
3. 사용자는 인증 에이전트 인터페이스에 응답 블록을 입력하고 하드 드라이브에 대한 접근 권한을 얻습니다.



Kaspersky 디스크 암호화 기술로 보호되는 시스템 하드 드라이브에 대한 접근 복원

복원 절차를 시작하려면 인증 에이전트 인터페이스에서 **Forgot your password** 버튼을 클릭해야 합니다.

관리 콘솔(MMC)에서 Kaspersky 디스크 암호화 기술로 보호되는 시스템 하드 드라이브에 대한 응답 블록을 얻는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **기기**를 선택합니다.
3. **기기** 탭에서 암호화된 데이터에 접근을 요청하는 사용자 소유의 컴퓨터를 선택하고 마우스 오른쪽 버튼을 눌러 메뉴를 엽니다.
4. 마우스 오른쪽 메뉴에서 **오프라인 모드에서의 접근 권한 부여**를 선택합니다.
5. 열린 창에서 **인증 에이전트** 탭을 선택합니다.
6. **사용 중인 암호화 알고리즘** 블록에서 암호화 알고리즘을 선택합니다: **AES56** 또는 **AES256**.

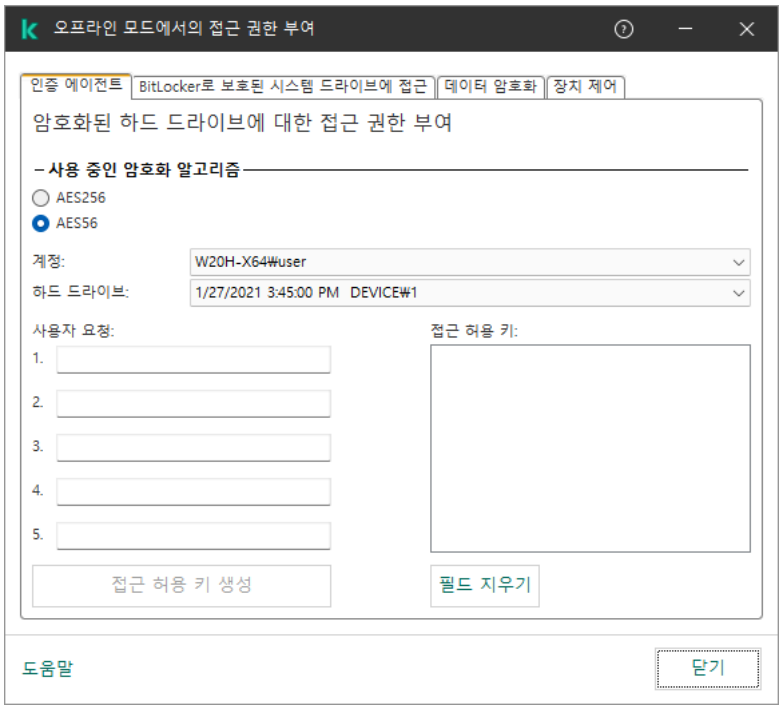
   데이터 암호화 알고리즘은 배포 패키지에 포함된 AES 암호화 라이브러리에 따라 다릅니다: *강한 암호화(AES256)* 또는 *가벼운 암호화(AES56)*. AES 암호화 라이브러리는 애플리케이션과 함께 설치됩니다.

7. **계정** 드롭다운 목록에서 드라이브에 대한 접근 복원을 요청한 사용자의 인증 에이전트 계정 이름을 선택합니다.

8. **하드 드라이브** 드롭다운 목록에서 다시 접근 권한이 필요한 암호화된 하드 드라이브를 선택합니다.

9. **사용자 요청** 블록에 사용자의 요청 내용을 입력합니다.

그러면 사용자의 인증 에이전트 계정 사용자 및 암호 복원 요청에 대한 블록 내용이 **접근 허용 키** 필드에 표시됩니다. 응답 블록의 내용을 사용자에게 전달합니다.



오프라인 모드에서의 접근 권한 부여

웹 콘솔에서 Kaspersky 디스크 암호화 기술로 보호되는 시스템 하드 드라이브에 대한 응답 블록을 얻는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.

2. 드라이브에 대한 접근을 복원하려는 컴퓨터 이름 옆의 확인란을 선택합니다.

3. **오프라인 모드인 기기에 접근 권한 부여** 버튼을 클릭합니다.

4. 창이 열리면 **인증 에이전트** 섹션을 선택합니다.

5. **계정** 드롭다운 목록에서 인증 에이전트 계정 이름과 암호의 복원을 요청하는 사용자에 대해 생성된 인증 에이전트 계정 이름을 선택합니다.

6. 사용자가 전달한 요청 블록을 입력합니다.

사용자의 인증 에이전트 계정 사용자 이름 및 암호 복원 요청에 대한 응답 블록의 내용이 창 하단에 표시됩니다. 응답 블록의 내용을 사용자에게 전달합니다.

복원 절차를 완료하면 인증 에이전트가 사용자에게 암호를 변경하라는 메시지를 표시합니다.

비시스템 하드 드라이브에 대한 접근 복원

Kaspersky 디스크 암호화 기술로 보호되는 비시스템 하드 드라이브에 대한 접근 복원은 다음 단계로 구성됩니다.

1. 사용자가 접근 허용 요청 파일을 관리자에게 전송합니다.
2. 관리자는 접근 허용 요청 파일을 Kaspersky Security Center에 추가하고 접근 허용 키 파일을 생성한 후 사용자에게 보냅니다.
3. 사용자는 접근 허용 키 파일을 Kaspersky Endpoint Security에 추가하고 하드 드라이브에 대한 접근 권한을 얻습니다.

복원 절차를 시작하려면 사용자가 하드 드라이브에 접근을 시도해야 합니다. 그러면 Kaspersky Endpoint Security는 접근 허용 요청 파일(확장자가 KESDC인 파일)을 생성합니다. 이 파일은 사용자가 이메일 등을 통해 관리자에게 전송해야 합니다.

관리 콘솔(MMC)에서 암호화된 비시스템 하드 드라이브에 대한 접근 허용 키 파일을 얻는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **기기**를 선택합니다.
3. **기기** 탭에서 암호화된 데이터에 접근을 요청하는 사용자 소유의 컴퓨터를 선택하고 마우스 오른쪽 버튼을 눌러 메뉴를 엽니다.
4. 마우스 오른쪽 메뉴에서 **오프라인 모드에서의 접근 권한 부여**를 선택합니다.
5. 열린 창에서 **데이터 암호화** 탭을 선택합니다.
6. **데이터 암호화** 탭에서 **찾아보기** 버튼을 누릅니다.
7. 접근 허용 요청 파일을 선택하는 창에서 사용자로부터 받은 파일의 경로를 지정합니다.

사용자의 접근 요청에 대한 정보가 표시됩니다. Kaspersky Security Center는 키 파일을 생성합니다. 암호화된 데이터 접근 허용 키 파일이 생성되면 사용자에게 이메일로 전송합니다. 또는 접근 허용 파일을 저장하고 이용 가능한 방법을 활용하여 파일을 전송합니다.



오프라인 모드에서의 접근 권한 부여

웹 콘솔에서 암호화된 비시스템 하드 드라이브 접근 허용 키 파일을 얻는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)**를 선택합니다.
2. 데이터에 대한 접근을 복원하려는 컴퓨터 이름 옆의 확인란을 선택합니다.
3. **오프라인 모드인 기기에 접근 권한 부여** 버튼을 클릭합니다.
4. **데이터 암호화**를 선택합니다.
5. **파일 선택** 버튼을 클릭하고 사용자로부터 받은 접근 허용 요청 파일(확장자가 KESDC인 파일)을 선택합니다.

   웹 콘솔은 접근 허용 요청에 대한 정보를 표시합니다. 여기에는 사용자가 파일에 대한 접근 허용을 요청하는 컴퓨터의 이름이 포함됩니다.
6. **키 저장** 버튼을 클릭하고 폴더를 선택하여 암호화된 데이터 접근 허용 키 파일(확장자가 KESDR인 파일)을 저장합니다.

그러면 암호화된 데이터 접근 허용 키를 얻을 수 있으며 이를 사용자에게 전송해야 합니다.

인증 에이전트 서비스 계정으로 로그인

Kaspersky Endpoint Security를 사용하면 드라이브 암호화 시 인증 에이전트 서비스 계정을 추가할 수 있습니다. 서비스 계정은 사용자가 암호를 잊어버렸을 때와 같은 상황에서 컴퓨터에 액세스하는 데 필요합니다. 서비스 계정을 예비 계정으로 사용할 수도 있습니다. 계정을 추가하려면 디스크 암호화 설정에서 서비스 계정을 선택하고 사용자 계정 이름을 입력합니다(기본값은 `ServiceAccount`). 에이전트를 사용하여 인증하려면 일회용 암호가 필요합니다.

관리 콘솔(MMC)에서 일회용 암호를 찾는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **기기**를 선택합니다.
3. 더블 클릭해 컴퓨터 속성 창을 엽니다.
4. 컴퓨터 속성 창에서 **작업** 섹션을 선택합니다.
5. 작업 목록에서 **인증 에이전트 계정 관리**를 선택하고 더블 클릭하여 작업 속성을 엽니다.
6. 작업 속성 창에서 **설정** 섹션을 선택합니다.
7. 계정 목록에서 인증 에이전트 서비스 계정(예: `WIN10-USER\ServiceAccount`)을 선택합니다.
8. **처리** 드롭다운 목록에서 **계정 보기**를 선택합니다.
9. 계정 속성에서 **원래 암호 표시** 확인란을 선택합니다.
10. 서비스 계정 로그인을 위한 일회용 암호를 복사합니다.

웹 콘솔에서 일회용 암호를 찾는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.
2. 인증 에이전트 계정 목록을 보려는 컴퓨터의 이름을 클릭합니다.
   그러면 컴퓨터 속성이 열립니다.
3. 컴퓨터 속성에서 **작업** 탭을 선택합니다.
4. 작업 목록에서 **인증 에이전트 계정 관리**를 선택합니다.
5. 작업 속성에서 **애플리케이션 설정** 탭을 선택합니다.
6. 계정 목록에서 인증 에이전트 서비스 계정(예: `WIN10-USER\ServiceAccount`)을 선택합니다.
7. 계정 속성에서 **암호 표시** 확인란을 선택합니다.
8. 서비스 계정 로그인을 위한 일회용 암호를 복사합니다.

Kaspersky Endpoint Security는 사용자가 서비스 계정으로 인증할 때마다 암호를 자동으로 업데이트합니다. 에이전트를 통해 인증한 후 Windows 계정 암호를 입력해야 합니다. 서비스 계정으로 로그인 시 SSO 기술을 사용할 수 없습니다.

운영 체제 업데이트

FDE(전체 디스크 암호화)로 보호된 컴퓨터의 운영 체제를 업데이트할 때는 특별히 고려해야 할 사항이 몇 가지 있습니다. 다음과 같이 운영 체제를 업데이트하십시오: 먼저 한 컴퓨터의 OS를 업데이트합니다. 그런 다음, 전체 컴퓨터 중 일부분에 대한 OS를 업데이트합니다. 마지막으로 네트워크상의 모든 컴퓨터의 OS를 업데이트합니다.

Kaspersky 디스크 암호화 기술을 사용하는 경우 운영 체제가 시작되기 전에 인증 에이전트가 로드됩니다. 인증 에이전트를 사용하여 사용자는 시스템에 로그인하고 암호화된 드라이브에 대한 접근 권한을 받을 수 있습니다. 그런 다음 운영 체제가 로드됩니다. Kaspersky 디스크 암호화 기술을 사용하여 보호되는 컴퓨터에서 운영 체제 업데이트를 시작하는 경우, OS 업데이트 마법사가 인증 에이전트를 제거합니다. 그 결과 OS 로더가 암호화된 드라이브에 접근할 수 없어 컴퓨터가 잠길 수 있습니다.

운영 체제 업데이트의 기능:

- **WSUS에서 OS 업데이트**. 일반적인 방법으로 운영 체제를 업데이트할 수 있습니다.
- **ISO에서 OS 업데이트**. 운영 체제를 업데이트하려면 Kaspersky 디스크 암호화 드라이버가 있는 폴더를 지정해야 합니다. 애플리케이션이 드라이버를 별도의 폴더에 자동으로 복사합니다. 다음을 수행합니다:

  1. ISO 이미지를 탑재합니다.
  2. 다음 키로 시스템 업데이트 설치를 시작합니다:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.0\reflect_drivers
     ```

> 자동 OS 업데이트는 컴퓨터가 Windows 10 1607(RS1) 이상을 실행 중인 경우에만 사용 가능합니다. 이전 버전의 운영 체제를 업그레이드하려면, 먼저 디스크를 복호화하고 OS 업그레이드를 수행한 후 디스크를 암호화하는 것을 권장합니다.

BitLocker 드라이브 암호화 기술을 사용하는 경우에는 Windows 10을 업데이트하기 위해 하드 드라이브를 복호화할 필요가 없습니다. BitLocker 동작에 대한 자세한 내용은 Microsoft 웹사이트를 방문하시기 바랍니다.

암호화 기능 업데이트의 오류 방지

이전 버전의 애플리케이션을 Kaspersky Endpoint Security for Windows 14.0로 업그레이드하면 전체 디스크 암호화가 업데이트됩니다.

전체 디스크 암호화 기능 업데이트를 시작하면 다음 오류가 발생할 수 있습니다:

- 업데이트를 초기화할 수 없습니다.
- 장치가 인증 에이전트와 호환되지 않습니다.

새 애플리케이션 버전에서 전체 디스크 암호화 기능의 업데이트 프로세스를 시작할 때 발생한 오류를 제거하려면 다음과 같이 하십시오.

1. 하드 디스크를 복호화합니다.
2. 다시 하드 드라이브를 암호화합니다.

전체 디스크 암호화 기능 업데이트 중에는 다음 오류가 발생할 수 있습니다.

- 업데이트를 완료할 수 없습니다.
- 전체 디스크 암호화 업그레이드 롤백 완료 시 오류가 발생했습니다.

전체 디스크 암호화 기능의 업데이트 프로세스 중에 발생한 오류를 제거하려면 다음을 수행합니다:

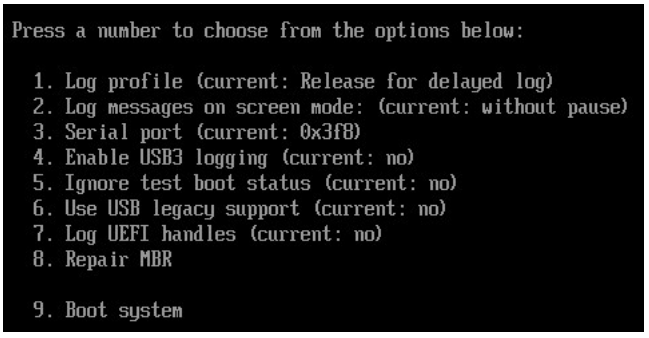
복원 유틸리티를 사용하여 암호화된 드라이브에 대한 접근을 복원

인증 에이전트 추적

애플리케이션이 인증 에이전트의 작동에 대한 정보 및 인증 에이전트를 통한 사용자 작업에 대한 정보를 추적 파일 내에 기록합니다.

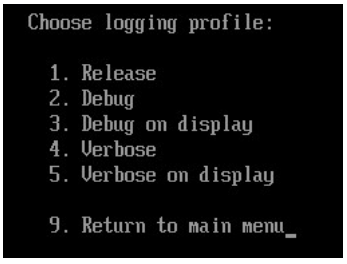
인증 에이전트 추적을 활성화하려면

1. Kaspersky Endpoint Security 추적을 활성화합니다.
2. 컴퓨터 다시 시작.
3. 암호화된 하드 드라이브가 있는 컴퓨터가 시작되자마자 **F3** 버튼을 눌러 인증 에이전트 설정을 구성하기 위한 창을 호출합니다.
4. FDE 부트 로더를 시작한 후, **KES (FDE <version>)** 부팅 관리자를 선택합니다.
5. 부트 관리자 메뉴에서 **Log profile** 설정으로 이동합니다.



부트 관리자 메뉴

6. 로그 프로필 설정 창에서 추적 레벨을 선택합니다.



인증 에이전트 추적 레벨

- **Release**. 이 옵션을 선택하면 애플리케이션이 추적 파일에 인증 에이전트 이벤트에 대한 정보를 기록하지 않습니다.
- **Debug**. 이 옵션이 선택되어 있으면 애플리케이션에 인증 에이전트의 작동 및 인증 에이전트와 함께 수행되는 사용자 작동에 대한 정보가 추적 파일에 기록됩니다.
- **Debug on display**. 이 옵션이 선택되어 있으면 애플리케이션에 인증 에이전트의 작동 및 인증 에이전트와 함께 수행되는 사용자 동작에 대한 정보가 추적 파일에 기록되며 COM 포트를 통해 이를 릴레이합니다.

  암호화된 하드 드라이브가 있는 컴퓨터가 COM 포트를 통해 다른 컴퓨터에 연결되어 있으면 인증 에이전트 이벤트를 이 다른 컴퓨터에서 검사할 수 있습니다.

- **Verbose**. 이 옵션이 선택되어 있으면 애플리케이션에 인증 에이전트의 작동 및 인증 에이전트와 함께 수행되는 사용자 작동에 대한 자세한 추적 파일에 정보가 기록됩니다.

  이 옵션 상태에서는 항목의 세부 레벨이 **Debug** 옵션의 수준보다 높습니다. 높은 수준의 항목 세부 레벨이 인증 에이전트 및 운영 체제의 시작 속도를 저하시킬 수 있습니다.

- **Verbose on display**. 이 옵션이 선택되어 있으면 애플리케이션에 인증 에이전트의 작동 및 인증 에이전트와 함께 수행되는 사용자 동작에 대한 세부 정보가 추적 파일에 기록되며 COM 포트를 통해 이를 릴레이합니다.

  이 옵션 상태에서는 항목의 세부 레벨이 **Debug on display** 옵션의 수준보다 높습니다. 높은 수준의 항목 세부 레벨이 인증 에이전트 및 운영 체제의 시작 속도를 저하시킬 수 있습니다.

추적 레벨을 선택하면 부트 관리자가 메뉴를 다시 표시합니다.

7. 부트 관리자 메뉴에서 **Boot system**을 선택합니다.

   FDE 부트 로더가 인증 에이전트를 시작합니다.

   문제를 재현합니다.

   컴퓨터에 암호화된 하드 드라이브가 있는 경우 또는 전체 디스크 암호화 중에는 데이터가 인증 에이전트 추적 파일에 기록됩니다.

8. 추적 프로세스를 중지하려면 지원 도구 창으로 돌아가 추적을 중지합니다.

결과적으로 인증 에이전트 KES.SRV 동작 추적 파일이 `%ProgramData%\Kaspersky Lab\KES.14.0\Traces` 폴더에 생성됩니다. 인증 에이전트 추적 로그 파일은 애플리케이션의 다른 추적 파일과는 다르게 Kaspersky로 전송되지 않습니다. 필요하다면 인증 에이전트 추적 파일을 분석을 위해 Kaspersky에 직접 전송할 수 있습니다.

인증 에이전트 도움말 텍스트 편집

인증 에이전트 도움말 메시지를 편집하기 전에 사전 부팅 환경에서 지원되는 문자 목록을 검토하십시오(아래 참조).

인증 에이전트 도움말 메시지를 편집하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **데이터 암호화 → 일반 암호화 설정**을 선택합니다.

4. **템플릿** 블록에서 **도움말** 버튼을 클릭합니다.

5. 창이 열리면 다음을 수행합니다.

   - **인증** 탭을 선택하여 계정 자격 증명을 입력하면 인증 에이전트 창에 표시되는 도움말 텍스트를 편집합니다.
   - **암호 변경** 탭을 선택하여 인증 에이전트 계정용 암호가 변경될 때 인증 에이전트 창에 표시되는 도움말 텍스트를 편집합니다.
   - **암호 복구** 탭을 선택하여 인증 에이전트 계정용 암호가 복구될 때 인증 에이전트 창에 표시되는 도움말 텍스트를 편집합니다.

6. 도움말 메시지를 편집합니다.
   원본 텍스트를 복원하려면 **기본값** 버튼을 누릅니다.

   > 도움말 문구는16줄 이하로 입력할 수 있습니다. 각 줄당 최대 64자까지 사용할 수 있습니다.

7. 변경 사항을 저장합니다.

인증 에이전트 도움말 메시지의 제한적 문자 지원

사전 부팅 환경에서 다음 Unicode 문자가 지원됩니다:

- 기본 라틴어 알파벳(0000 - 007F)
- 추가 라틴어-1 문자(0080 - 00FF)
- 확장 라틴어-A(0100 - 017F)
- 확장 라틴어-B(0180 - 024F)
- 비통합 확장 ID 문자(02B0 - 02FF)
- 통합 발음 구별 부호(0300 - 036F)
- 그리스어 및 콥트어 알파벳(0370 - 03FF)
- 키릴(0400 - 04FF)
- 히브리어(0590 - 05FF)
- 아랍어 문자(0600 - 06FF)
- 추가 확장 라틴어(1E00 - 1EFF)
- 구두점(2000 - 206F)
- 통화 기호(20A0 - 20CF)
- 글자와 비슷한 기호(2100 - 214F)

- 기하학 도형(25A0 - 25FF)
- 아랍어 문자 표시 형식-B(FE70 - FEFF)

이 목록에 지정되어 있지 않은 문자는 사전 부팅 환경에서 지원되지 않습니다. 인증 에이전트 도움말 메시지에 그러한 문자를 사용하는 것은 권장되지 않습니다.

인증 에이전트의 작동을 테스트한 후 남은 개체 및 데이터 제거

애플리케이션 제거 과정에서 Kaspersky Endpoint Security가 인증 에이전트 테스트 작업 후 시스템 하드 드라이브에 개체 및 데이터가 남아 있는 것을 탐지하는 경우 애플리케이션 제거가 중단되고 그러한 개체 및 데이터가 삭제된 후에 제거 가능하게 됩니다.

인증 에이전트의 테스트 작업 후에는 예외적인 경우에만 개체와 데이터가 시스템 하드 드라이브에 남아있을 수 있습니다. 예를 들어, 이러한 현상은 암호화 설정과 함께 Kaspersky Security Center 정책이 적용된 후에 컴퓨터를 재시작하지 않았거나 인증 에이전트의 테스트 작동 후에 애플리케이션 시작에 실패한 경우 발생할 수 있습니다.

다음 방법으로 인증 에이전트의 테스트 작업 후에 시스템 하드 드라이브에 남은 개체 및 데이터를 제거할 수 있습니다:

- Kaspersky Security Center 정책 사용.
- 복원 유틸리티 사용.

Kaspersky Security Center 정책을 사용해 인증 에이전트의 테스트 작업 후 남아 있는 개체 및 데이터를 제거하려면 다음을 수행합니다.

1. 모든 컴퓨터 하드 드라이브를 복호화하도록 구성된 설정으로 Kaspersky Security Center 정책을 컴퓨터에 적용합니다.
2. Kaspersky Endpoint Security 사용.

복원 유틸리티를 사용해 인증 에이전트의 테스트 작업 후 남아 있는 개체 및 데이터를 제거하려면 다음을 수행합니다.

1. 복원 유틸리티의 실행 파일인 fdert.exe 파일을 실행합니다. 이 파일은 Kaspersky Endpoint Security에 의해 생성되었습니다.
2. 복원 유틸리티 창에서 필요한 장치를 선택합니다.
3. **검사**를 클릭합니다.
4. 시스템 하드 드라이브를 진단한 후 인증 에이전트의 테스트 작업으로 인해 개체 및 데이터가 남아 있다는 메시지를 수신하면 **AA 개체 및 데이터 삭제**를 클릭합니다.

> **AA 개체 및 데이터 삭제** 버튼은 인증 에이전트의 테스트 작업 후 남은 개체 및 데이터가 탐지된 경우에만 사용할 수 있습니다.

인증 에이전트와 애플리케이션의 비호환성에 대한 정보를 제거하려면 다음과 같이 하십시오:

명령줄에 `avp pbatestreset` 문자를 입력합니다.

BitLocker 관리

*BitLocker*는 Windows 운영 체제에 내장된 암호화 기술입니다. Kaspersky Endpoint Security를 사용하면 Kaspersky Next 인프라를 통해 Bitlocker를 제어하고 관리할 수 있습니다. BitLocker는 논리 볼륨을 암호화합니다. BitLocker는 이동식 드라이브 암호화에 사용할 수 없습니다. BitLocker에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

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.

BitLocker 암호화 알고리즘은 배포 패키지(AES256 또는 AES56)에 포함된 AES 라이브러리 버전에 영향을 받지 않습니다. 암호화에는 운영 체제에 내장된 암호화 라이브러리를 사용합니다.

기본적으로 애플리케이션은 유효 키 길이가 256비트인 BitLocker 암호화 알고리즘을 사용하여 암호화된 적이 없는 장치를 암호화합니다. 애플리케이션 설치 전 암호화된 장치는 암호화 알고리즘이 다를 수 있습니다. 암호화 알고리즘 선택에 대한 자세한 내용은 Microsoft 기술 지원 웹사이트를 참조하십시오. Kaspersky Endpoint Security 버전 12.9부터는 이전에 타사 애플리케이션으로 암호화된 장치에 대한 원래 복구 키를 Kaspersky Security Center로 전송합니다.

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

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.

드라이브를 암호화한 후 BitLocker는 마스터 키를 만듭니다. Kaspersky Endpoint Security는 마스터 키를 Kaspersky Security Center로 전송하여, 예를 들어 사용자가 암호를 잊어버린 경우 디스크로의 접근을 복원할 수 있습니다.

사용자가 BitLocker로 디스크를 암호화하는 경우 Kaspersky Endpoint Security는 디스크 암호화에 대한 정보를 Kaspersky Security Center로 전송합니다. 그러나 Kaspersky Endpoint Security는 마스터 키를 Kaspersky Security Center로 보내지 않으므로 Kaspersky Security Center를 사용하여 디스크로의 접근을 복원할 수 없습니다. BitLocker가 Kaspersky Security Center와 올바르게 작동하려면 드라이브를 복호화하고 정책을 사용하여 드라이브를 다시 암호화하십시오. 드라이브를 로컬로 복호화하거나 정책을 사용하여 복호화할 수 있습니다.

Windows 그룹 정책을 사용하는 경우 정책 설정에서 BitLocker 매니지먼트를 해제합니다. Windows 정책 설정이 Kaspersky Endpoint Security 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.

관리 콘솔(MMC)을 통해 BitLocker 드라이브 암호화를 실행하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 전체 디스크 암호화**를 선택합니다.
4. **암호화 기술** 드롭다운 목록에서 **BitLocker 드라이브 암호화**를 선택합니다.
5. **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 암호화**를 선택합니다.

   여러 운영 체제가 설치된 컴퓨터인 경우 암호화 후 암호화가 수행된 운영 체제만 로드할 수 있습니다.
6. 고급 BitLocker 드라이브 암호화 옵션을 구성하십시오(아래 표 참조).
7. 변경 사항을 저장합니다.

웹 콘솔과 Cloud Console을 통해 BitLocker 드라이브 암호화를 실행하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **데이터 암호화 → 전체 디스크 암호화**로 이동합니다.

5. **BitLocker 디스크 암호화** 기술을 선택합니다.

6. **장치에서의 작업** 블록에서 **모든 하드 드라이브 암호화**를 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. 변경 사항을 저장합니다.

암호화 모니터 도구를 사용하여 사용자 컴퓨터의 디스크 암호화 또는 복호화 프로세스를 제어할 수 있습니다. 메인 애플리케이션 창에서 암호화 모니터 도구를 실행할 수 있습니다.



암호화 모니터

정책이 적용된 후에는 애플리케이션이 인증 설정에 따라 다음 쿼리를 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 PIN을 설정한 후 BitLocker는 암호화를 완료하기 위해 컴퓨터를 다시 시작할 것을 요청합니다. 다음으로, 사용자는 BitLocker 인증 절차를 거쳐야 합니다. 인증 절차 후 사용자는 시스템에 로그온해야 합니다. 운영 체제가 로드된 후, BitLocker는 암호화를 완료합니다.

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 버전)	이 확인란을 선택하면 애플리케이션이 하드웨어 암호화를 적용합니다. 이 방법을 사용하면 암호화 속도가 빨라지고 컴퓨터 리소스를 적게 사용합니다.
사용된 디스크 공간만 암호화 (Windows 8 이상 버전)	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(암호화 시간 단축)** 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 Endpoint Security는 새로 데이터가 추가될 때마다 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 유형	**암호만(Windows 8 이상 버전)** 이 옵션을 선택하면 사용자가 암호화된 드라이브에 접근하려고 시도할 때 Kaspersky Endpoint Security가 사용자에게 암호 입력을 요구합니다. 신뢰하는 플랫폼 모듈(TPM)을 사용하지 않는 경우 이 옵션을 선택할 수 있습니다. **신뢰하는 플랫폼 모듈(TPM)** 이 옵션을 선택하면 BitLocker가 신뢰하는 플랫폼 모듈(TPM)을 사용합니다. *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. 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. 선택된 인증 방법은 암호 또는 PIN 요구 사항을 지정하여 구성해야 합니다. • **최소 PIN 길이(문자 수)**. • **최소 암호 길이(문자 수)**. • **TPM에 대한 암호/PIN 유효 기간 제한(일)**. • **강화 PIN(문자와 숫자) 사용**. *강화 PIN*은 대문자와 소문자, 라틴 문자, 특수 문자 및 공백 등 숫자 외의 다른 문자도 사용할 수 있습니다.
자동으로 복구 키 재생성(일)	BitLocker로 보호되는 드라이브에 대한 접근 복원을 위한 암호를 자동으로 업데이트합니다. 확인란이 선택되면 복구 키 암호 유효 기간을 지정합니다. 이렇게 하면 복구 키 암호 재사용을 방지합니다.

BitLocker로 보호되는 하드 드라이브 복호화

사용자는 운영 체제를 사용하여 디스크를 복호화할 수 있습니다(*BitLocker 끄기* 기능). 그 후에 Kaspersky Endpoint Security는 디스크를 다시 암호화하라는 메시지를 표시합니다. 정책에서 디스크 복호화를 활성화하지 않으면 Kaspersky Endpoint Security가 디스크를 암호화하라는 메시지를 표시합니다.

관리 콘솔(MMC)을 통해 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. 정책 창에서 **데이터 암호화 → 전체 디스크 암호화**를 선택합니다.
4. **암호화 기술** 드롭다운 목록에서 **BitLocker 드라이브 암호화**를 선택합니다.
5. **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 복호화**를 선택합니다.
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console을 통해 BitLocker로 암호화된 하드 드라이브를 복호화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **데이터 암호화** → **전체 디스크 암호화**로 이동합니다.
5. **BitLocker 디스크 암호화** 기술을 선택합니다.
6. **장치에서의 작업** 블록에서 **모든 하드 드라이브 복호화**를 선택합니다.
7. 변경 사항을 저장합니다.

암호화 모니터 도구를 사용하여 사용자 컴퓨터의 디스크 암호화 또는 복호화 프로세스를 제어할 수 있습니다. 메인 애플리케이션 창에서 암호화 모니터 도구를 실행할 수 있습니다.



암호화 모니터

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.
3. 복구 키 ID가 일치하면 관리자는 사용자에게 복구 키를 제공하거나 복구 키 파일을 전송합니다.

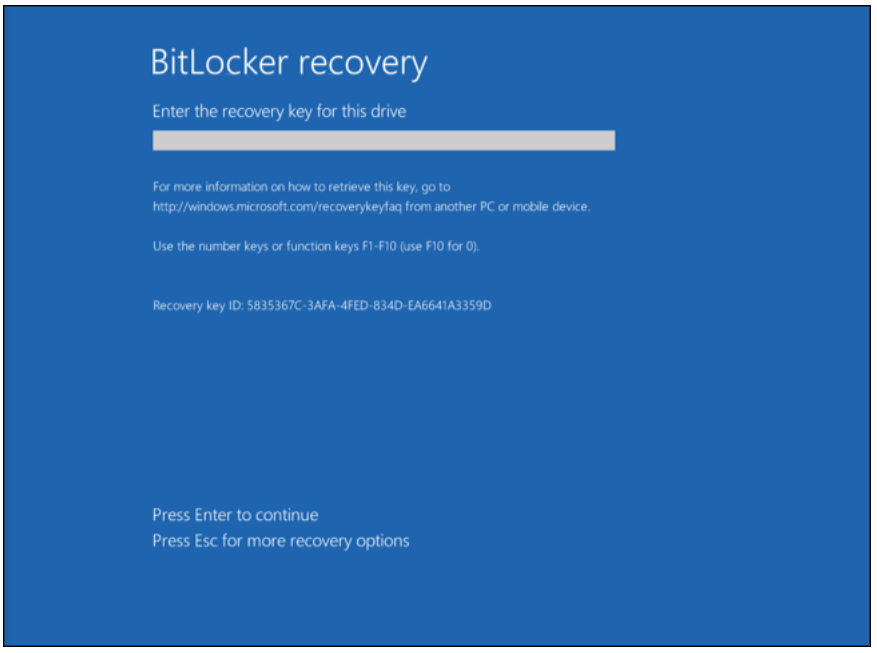
   복구 키 파일은 다음 운영 체제를 실행하는 컴퓨터에 사용됩니다:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   다른 모든 운영 체제에는 복구 키가 사용됩니다.

   복원 키 암호 재사용을 방지하려면 정책 설정에서 자동 암호 업데이트를 구성할 수 있습니다.

4. 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.

관리 콘솔(MMC)에서 BitLocker로 암호화된 시스템 드라이브의 복구 키를 보는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **관리 중인 기기**를 선택합니다.
3. **기기** 탭에서 암호화된 데이터에 접근을 요청하는 사용자 소유의 컴퓨터를 선택하고 마우스 오른쪽 버튼을 눌러 메뉴를 엽니다.
4. 마우스 오른쪽 메뉴에서 **오프라인 모드에서의 접근 권한 부여**를 선택합니다.
5. 열린 창에서 **BitLocker로 보호된 시스템 드라이브에 접근** 탭을 선택합니다.
6. 사용자에게 BitLocker 암호 입력 창에 표시된 복구 키 ID를 확인하고 **복구 키 ID** 필드의 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.

그러면 복구 키 또는 복구 키 파일에 접근할 수 있으며 이를 사용자에게 전송해야 합니다.



BitLocker로 암호화된 드라이브에 대한 접근 복원

웹 콘솔과 Cloud Console에서 BitLocker로 암호화된 시스템 드라이브의 복구 키를 보는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.
2. 드라이브에 대한 접근을 복원하려는 컴퓨터 이름 옆의 확인란을 선택합니다.
3. **오프라인 모드인 기기에 접근 권한 부여** 버튼을 클릭합니다.
4. 열리는 창에서 **BitLocker** 섹션을 선택합니다.
5. 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.

6. **키 받기**를 클릭합니다.

그러면 복구 키 또는 복구 키 파일에 접근할 수 있으며 이를 사용자에게 전송해야 합니다.

운영 체제 로드 후 Kaspersky Endpoint Security는 사용자에게 비밀번호나 PIN 코드를 변경하라는 메시지를 표시합니다. 새 비밀번호나 PIN 코드를 설정하면 BitLocker가 새 마스터키를 생성하고 Kaspersky Security Center로 해당 키를 보냅니다. 결과적으로 복구 키 및 복구 키 파일이 업데이트됩니다. 사용자가 암호를 변경하지 않은 경우 다음에 운영 체제가 로드될 때 이전 복구 키를 사용할 수 있습니다.

Windows 7 컴퓨터에서는 암호 또는 PIN 코드를 변경할 수 없습니다. 복구 키를 입력하고 운영 체제를 로드한 후 Kaspersky Endpoint Security는 사용자에게 비밀번호나 PIN 코드를 변경하라는 메시지를 표시하지 않습니다. 따라서 새 암호 또는 PIN 코드를 설정할 수 없습니다. 이는 운영 체제상의 특성으로 인한 문제입니다. 계속하려면 하드 드라이브를 다시 암호화해야 합니다.

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.

관리 콘솔(MMC)에서 BitLocker로 암호화된 비시스템 드라이브의 복구 키를 보는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리에서 **고급 → 데이터 암호화 및 보호 → 암호화된 드라이브** 폴더를 선택합니다.
3. 작업 공간에서 접근 허용 키 파일을 생성할 암호화된 장치를 선택하고 장치의 마우스 오른쪽 메뉴에서 **Kaspersky Endpoint Security에서 장치에 대한 접근 권한 가져오기**를 클릭합니다.
4. 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.

5. 사용자에게 **복구 키** 필드에 표시된 키를 전송합니다.



BitLocker로 암호화된 드라이브에 대한 접근 복원

웹 콘솔과 Cloud Console에서 BitLocker로 암호화된 비시스템 드라이브의 복구 키를 보는 방법

1. 웹 콘솔의 메인 창에서 **동작 → 데이터 암호화 및 보호 → 암호화된 드라이브**를 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 Endpoint Security for Windows** 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**를 클릭합니다.

그러면 복구 키 또는 복구 키 파일에 접근할 수 있으며 이를 사용자에게 전송해야 합니다.

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.

관리 콘솔(MMC)을 사용하여 BitLocker 보호를 일시 중지하는 방법

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

   작업 목록이 열립니다.

2. **새 작업**을 클릭합니다.

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

Kaspersky Endpoint Security for Windows (14.0) → **BitLocker 보호 관리**를 선택합니다.

2단계. BitLocker 보호 관리

BitLocker 인증을 구성합니다. BitLocker 보호를 일시 중지하려면 **BitLocker 인증 건너뛰기 임시 허용**을 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 끝냅니다. 필요시 **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**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.

   작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 일반 작업 설정 구성

일반 작업 설정을 구성하려면 다음을 수행하십시오.

1. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security**을 선택합니다.
2. **작업 유형** 드롭다운 목록에서 **BitLocker 보호 관리**를 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

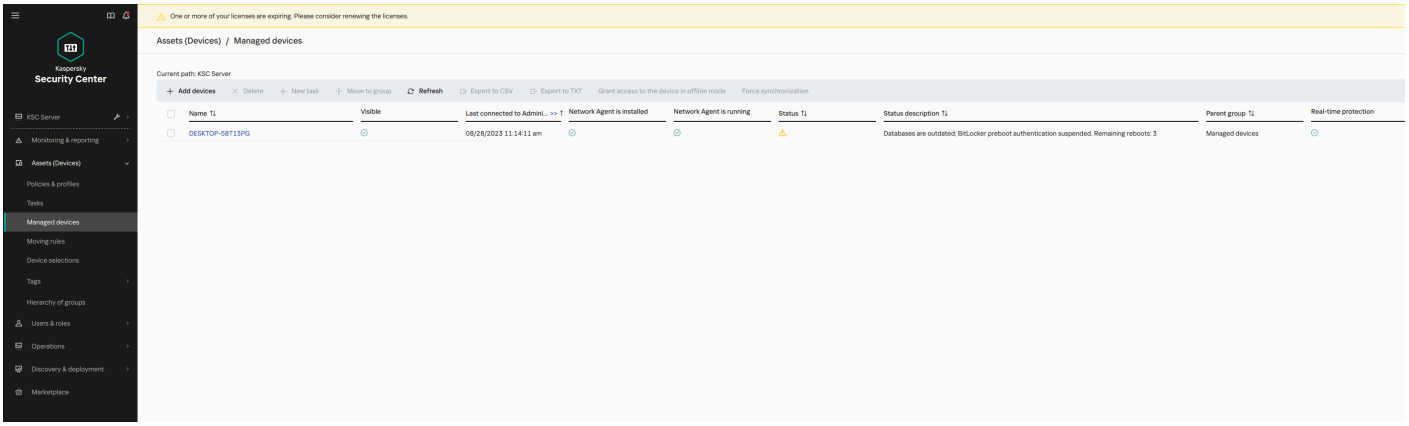
BitLocker 인증을 구성합니다. BitLocker 보호를 일시 중지하려면 **BitLocker 인증 건너뛰기 임시 허용**을 선택하고 BitLocker 인증 없이 다시 시작할 횟수를 입력합니다(1~15회). 필요하면 작업의 만료 날짜와 시간을 입력합니다. 지정한 시간이 되면 작업이 자동으로 꺼지고, 컴퓨터를 다시 시작할 때 사용자가 BitLocker 인증을 완료해야 합니다.

3단계. 작업 생성 완료

마법사를 끝냅니다. 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 Endpoint Security는 해당 이벤트를 생성하고 남은 다시 시작 횟수를 기록합니다. 그런 다음 Kaspersky Endpoint Security는 이벤트를 Kaspersky Security Center로 전송하여 관리자가 모니터링할 수 있도록 합니다. 기기 상태 설명 내 Kaspersky Security Center 콘솔의 **관리 중인 기기** 폴더에서도 남은 재시작 횟수를 볼 수 있습니다.



관리 중인 기기 목록

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 Endpoint Security에서 다시 시작 횟수 카운트를 처리합니다. 따라서 다시 시작할 때마다 BitLocker 인증을 자동으로 켜려면 Kaspersky Endpoint Security를 시작해야 합니다.

BitLocker 인증을 미리 켜려면 *BitLocker 보호 관리* 작업 속성을 열고 **부팅 전에 항상 인증 요청** 옵션을 선택합니다.

로컬 컴퓨터 드라이브에 대한 파일 레벨 암호화

Arm 기반 컴퓨터에서는 파일 암호화를 지원하지 않습니다.

이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

파일 암호화에는 다음과 같은 특징이 있습니다.

- Kaspersky Endpoint Security는 운영 체제의 로컬 사용자 프로필에 한해 사전 정의된 폴더에서 파일을 암호화/복호화합니다. Kaspersky Endpoint Security는 로밍 사용자 프로필, 필수 사용자 프로필, 임시 사용자 프로필 또는 리다이렉트 폴더의 사전 정의된 폴더에서는 파일을 암호화 또는 복호화하지 않습니다.
- Kaspersky Endpoint Security는 파일 암호화로 인해 운영 체제 및 설치된 애플리케이션에 문제를 야기하는 파일은 암호화하지 않습니다. 예를 들어 다음 파일과 폴더는 그 하위 폴더를 포함하여 암호화에서 예외합니다:
  - %WINDIR%
  - %PROGRAMFILES% 및 %PROGRAMFILES(X86)%
  - Windows 레지스트리 파일

  암호화 예외 목록은 확인 또는 편집할 수 없습니다. 암호화 예외 목록의 파일과 폴더를 암호화 목록에 추가할 수 있지만 파일 암호화 도중 암호화되지 않습니다.

로컬 컴퓨터 드라이브의 파일 암호화

Kaspersky Endpoint Security는 OneDrive 클라우드 저장소 또는 이름이 OneDrive인 다른 폴더에 있는 파일을 암호화하지 않습니다. Kaspersky Endpoint Security는 암호화된 파일이 복호화 규칙에 추가되지 않았다면 해당 파일을 OneDrive 폴더로 복사하는 것도 차단합니다.

로컬 드라이브의 파일을 암호화하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 파일 레벨 암호화**를 선택합니다.
4. **암호화 모드** 드롭다운 목록에서 **규칙을 따름**을 선택합니다.
5. **암호화** 탭에서 **추가** 버튼을 누르고 드롭다운 목록이 나타나면 다음 항목 중 하나를 선택합니다:
   a. Kaspersky 전문가가 추천한 로컬 사용자 프로필 폴더의 파일을 암호화 규칙에 추가하려면 **사전 정의된 폴더** 항목을 선택합니다.
      - **문서**. 운영 체제의 표준 *문서* 폴더에 있는 파일 및 해당 하위 폴더.
      - **즐겨찾기**. 운영 체제의 표준 *즐겨찾기* 폴더에 있는 파일 및 해당 하위 폴더.
      - **바탕 화면**. 운영 체제의 표준 *바탕 화면* 폴더에 있는 파일 및 해당 하위 폴더.

- **임시 파일**. 컴퓨터에 설치된 애플리케이션 작동과 관련된 임시 파일. 예를 들어 Microsoft Office 애플리케이션은 문서의 백업 복사본이 포함된 임시 파일을 만듭니다.

  데이터 손실이 야기될 수 있으므로 임시 파일은 암호화하지 않는 것이 좋습니다. 예를 들어, Microsoft Word는 문서를 처리할 때 임시 파일을 생성합니다. 원본 파일은 그대로 두고 임시 파일을 암호화하면 사용자가 문서를 저장하려고 할 때 *액세스 거부됨* 오류가 표시될 수 있습니다. 그리고 Microsoft Word가 파일을 저장할 수 있지만 데이터가 소실되어 다음에 해당 문서가 열리지 않을 수 있습니다.

- **Outlook 파일**. 데이터 파일(PST), 오프라인 데이터 파일(OST), 오프라인 주소록 파일(OAB) 및 개인 주소록 파일(PAB)과 같은 Outlook 메일 클라이언트 작동과 관련된 파일.

b. 직접 입력한 폴더 경로를 암호화 규칙에 추가하려면 **사용자 지정 폴더** 항목을 선택합니다.

폴더 경로를 추가할 때는 다음 규칙을 준수하십시오.

- 환경 변수를 사용하십시오(예: `%FOLDER%\UserFolder\`). 환경 변수는 경로 시작 부분에서 한 번만 사용할 수 있습니다.
- 상대 경로를 사용하지 마십시오.
- `*`과 `?` 문자를 사용하지 마십시오.
- UNC 경로를 사용하지 마십시오.
- `;` 또는 `,`를 구분 문자로 사용하십시오.

c. 개별 파일 확장자를 암호화 규칙에 추가하려면 **파일 확장자로** 항목을 선택합니다. Kaspersky Endpoint Security는 컴퓨터의 전체 로컬 드라이브에서 지정된 확장자의 파일을 암호화합니다.

d. 파일 확장자 그룹을 암호화 규칙에 추가하려면 **파일 확장자 그룹으로** 항목을 선택합니다(예: *Microsoft Office 문서*). Kaspersky Endpoint Security는 컴퓨터의 전체 로컬 드라이브에서 확장자 그룹에 나열된 확장자를 사용하는 파일을 암호화합니다.

6. 변경 사항을 저장합니다.

정책이 적용되면 Kaspersky Endpoint Security는 암호화 규칙에는 포함되고 복호화 규칙에는 포함되지 않은 파일을 암호화합니다.

파일 암호화에는 다음과 같은 특징이 있습니다.

- 동일한 파일이 암호화 규칙과 복호화 규칙에 모두 추가되는 경우 Kaspersky Endpoint Security는 다음 작업을 수행합니다.
  - 파일이 암호화되지 않은 경우 Kaspersky Endpoint Security는 이 파일을 암호화하지 않습니다.
  - 파일이 암호화된 경우 Kaspersky Endpoint Security는 이 파일을 복호화합니다.
- Kaspersky Endpoint Security는 이러한 파일이 암호화 규칙 기준을 충족하는 경우 새 파일을 계속 암호화합니다. 예를 들어, 암호화되지 않은 파일(경로 또는 확장자)의 속성을 변경하면 파일은 암호화 규칙 기준을 충족하게 됩니다. Kaspersky Endpoint Security는 이 파일을 암호화합니다.
- 사용자가 새로 생성한 파일의 속성이 암호화 규칙 기준을 충족하는 경우 Kaspersky Endpoint Security는 해당 파일이 열리는 즉시 파일을 암호화합니다.

- Kaspersky Endpoint Security는 파일이 열려 있을 경우 닫힐 때까지 암호화를 연기합니다.
- 로컬 드라이브에서 다른 폴더로 암호화된 파일을 옮길 경우 해당 폴더의 암호화 규칙 포함 여부에 관계 없이 파일은 암호화된 상태로 유지됩니다.
- 파일을 복호화하여 복호화 규칙에 포함되지 않은 다른 로컬 폴더로 복사하는 경우 해당 파일의 복사본이 암호화될 수 있습니다. 복사된 파일이 암호화되지 않도록 하려면 대상 폴더에 대한 복호화 규칙을 만드십시오.

애플리케이션의 암호화된 파일 접근 규칙 작성

기본적으로 모든 애플리케이션은 암호화된 파일을 복호화된 상태로 사용합니다. 특정 애플리케이션(예: 브라우저 또는 텍스트 편집기)을 자주 사용하는 경우 암호화된 파일 접근 규칙을 생성하여 정보를 보호할 수 있습니다.

Microsoft Internet Explorer 및 Microsoft Edge 브라우저에 대해 암호화된 파일 접근 규칙을 생성하는 것을 권장합니다. 이러한 브라우저의 작동 방식 때문에 암호화된 파일을 웹사이트(예: 클라우드 저장소)에 업로드하면 파일이 자동으로 복호화됩니다. 이로 인해 데이터 유출이 발생할 수 있습니다. 이러한 브라우저를 사용하여 암호화된 파일을 업로드할 수 없습니다. **암호문에서만 암호화된 파일로의 접근 권한 부여** 규칙 설정을 권장합니다. 기타 브라우저(예: Google Chrome)에 대한 규칙을 생성할 필요가 없습니다.

애플리케이션의 암호화된 파일 접근 규칙을 작성하려면 다음과 같이 하십시오:

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 파일 레벨 암호화**를 선택합니다.
4. **암호화 모드** 드롭다운 목록에서 **규칙을 따름**을 선택합니다.

   접근 규칙은 **규칙을 따름** 모드에서만 적용됩니다. **규칙을 따름** 모드에서 접근 규칙을 적용한 후 **변경하지 않음** 모드로 전환하면 Kaspersky Endpoint Security가 모든 접근 규칙을 무시합니다. 모든 애플리케이션이 모든 암호화된 파일에 접근할 수 있게 됩니다.

5. 창 오른쪽에서 **애플리케이션 규칙** 탭을 선택합니다.
6. Kaspersky Security Center 목록에 있는 애플리케이션만 선택하려는 경우 **추가** 버튼을 누르고 나타나는 드롭다운 목록에서 **Kaspersky Security Center 목록에 있는 애플리케이션** 항목을 선택합니다.
   a. 표의 애플리케이션 목록에 필터를 적용하여 범위를 좁힙니다. **애플리케이션**, **공급업체** 및 **추가된 기간** 파라미터와 **그룹** 블록의 모든 확인란에 대해 값을 지정합니다.
   b. **새로 고침**을 클릭합니다.
   c. 표에 적용된 필터와 일치하는 애플리케이션이 표시됩니다.
   d. **애플리케이션** 열에서 암호화된 파일 접근 규칙을 작성할 애플리케이션 옆의 확인란을 선택합니다.

e. **애플리케이션 규칙** 드롭다운 목록에서 암호화된 파일에 대한 애플리케이션 접근을 결정할 규칙을 선택합니다.

f. **애플리케이션이 선택되기 전에 생성된 파일의 동작 방법** 드롭다운 목록에서 이전에 해당 애플리케이션에 대해 작성된 암호화된 파일 접근 규칙에 관해 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택합니다.

애플리케이션 규칙 탭의 표에 애플리케이션의 암호화된 파일 접근 규칙에 대한 상세 정보가 표시됩니다.

7. 사용자가 직접 애플리케이션을 선택하려면 **추가** 버튼을 누르고 드롭다운 목록에서 **사용자 지정 애플리케이션** 항목을 선택합니다.

a. 입력 필드에서 애플리케이션의 실행 파일 이름 또는 이름 목록을 확장자와 함께 입력합니다.

Kaspersky Security Center 목록에서 추가 버튼을 눌러 Kaspersky Security Center 목록에서 애플리케이션의 실행 파일 이름도 추가할 수 있습니다.

b. 필요하다면, **설명** 필드에 애플리케이션 목록의 설명을 입력합니다.

c. **애플리케이션 규칙** 드롭다운 목록에서 암호화된 파일에 대한 애플리케이션 접근을 결정할 규칙을 선택합니다.

애플리케이션 규칙 탭의 표에 애플리케이션의 암호화된 파일 접근 규칙에 대한 상세 정보가 표시됩니다.

8. 변경 사항을 저장합니다.

특정 애플리케이션에서 만들어졌거나 수정된 파일 암호화

Kaspersky Endpoint Security가 해당 규칙에 지정된 애플리케이션에서 만들어졌거나 수정된 모든 파일을 암호화하는 규칙을 만들 수 있습니다.

암호화 규칙이 적용되기 전에 지정된 애플리케이션에서 만들어졌거나 수정된 파일은 암호화되지 않습니다.

특정 애플리케이션에서 만들어졌거나 수정된 파일에 대해 암호화를 구성하려면 다음을 수행합니다.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **데이터 암호화 → 파일 레벨 암호화**를 선택합니다.

4. **암호화 모드** 드롭다운 목록에서 **규칙을 따름**을 선택합니다.

암호화 규칙은 **규칙을 따름** 모드에서만 적용됩니다. **규칙을 따름** 모드에서 암호화 규칙을 적용한 후 **변경하지 않음** 모드로 전환하면 Kaspersky Endpoint Security가 모든 암호화 규칙을 무시합니다. 이전에 암호화된 파일은 암호화된 상태가 유지됩니다.

5. 창 오른쪽에서 **애플리케이션 규칙** 탭을 선택합니다.

6. Kaspersky Security Center 목록에 있는 애플리케이션만 선택하려는 경우 **추가** 버튼을 누르고 나타나는 드롭다운 목록에서 **Kaspersky Security Center 목록에 있는 애플리케이션** 항목을 선택합니다.

   a. 표의 애플리케이션 목록에 필터를 적용하여 범위를 좁힙니다. **애플리케이션**, **공급업체** 및 **추가된 기간** 파라미터와 **그룹** 블록의 모든 확인란에 대해 값을 지정합니다.

   b. **새로 고침**을 클릭합니다.

   표에 적용된 필터와 일치하는 애플리케이션이 표시됩니다.

   c. **애플리케이션** 열에서 생성된 파일을 암호화하려는 애플리케이션 옆의 확인란을 선택합니다.

   d. **애플리케이션 규칙** 드롭다운 목록에서 **생성된 모든 파일 암호화**를 선택합니다.

   e. **애플리케이션이 선택되기 전에 생성된 파일의 동작 방법** 드롭다운 목록에서 이전에 해당 애플리케이션에 대해 작성된 파일 암호화 규칙에 관해 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택합니다.

   선택한 애플리케이션이 생성 또는 수정한 파일에 적용된 암호화 규칙 정보가 **애플리케이션 규칙** 탭에 표시됩니다.

7. 사용자가 직접 애플리케이션을 선택하려면 **추가** 버튼을 누르고 드롭다운 목록에서 **사용자 지정 애플리케이션** 항목을 선택합니다.

   a. 입력 필드에서 애플리케이션의 실행 파일 이름 또는 이름 목록을 확장자와 함께 입력합니다.

   Kaspersky Security Center 목록에서 추가 버튼을 눌러 Kaspersky Security Center 목록에서 애플리케이션의 실행 파일 이름도 추가할 수 있습니다.

   b. 필요하다면, **설명** 필드에 애플리케이션 목록의 설명을 입력합니다.

   c. **애플리케이션 규칙** 드롭다운 목록에서 **생성된 모든 파일 암호화**를 선택합니다.

   선택한 애플리케이션이 생성 또는 수정한 파일에 적용된 암호화 규칙 정보가 **애플리케이션 규칙** 탭에 표시됩니다.

8. 변경 사항을 저장합니다.

복호화 규칙 생성

복호화 규칙을 생성하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **데이터 암호화 → 파일 레벨 암호화**를 선택합니다.

4. **암호화 모드** 드롭다운 목록에서 **규칙을 따름**을 선택합니다.

5. **복호화** 탭에서 **추가** 버튼을 누르고 드롭다운 목록이 나타나면 다음 항목 중 하나를 선택합니다:

   a. Kaspersky 전문가가 추천한 로컬 사용자 프로필 폴더의 파일을 복호화 규칙에 추가하려면 **사전 정의된 폴더** 항목을 선택합니다.

   b. 직접 입력한 폴더 경로를 복호화 규칙에 추가하려면 **사용자 지정 폴더** 항목을 선택합니다.

c. 개별 파일 확장자를 복호화 규칙에 추가하려면 **파일 확장자로** 항목을 선택합니다. Kaspersky Endpoint Security는 컴퓨터의 전체 로컬 드라이브에서 지정된 확장자의 파일을 복호화합니다.

d. 파일 확장자 그룹을 복호화 규칙에 추가하려면 **파일 확장자 그룹으로** 항목을 선택합니다(예: *Microsoft Office 문서*). Kaspersky Endpoint Security는 컴퓨터의 전체 로컬 드라이브에서 확장자 그룹에 나열된 확장자를 사용하는 파일을 암호화하지 않습니다.

6. 변경 사항을 저장합니다.

한 파일이 암호화 규칙과 복호화 규칙에 모두 추가된 경우 Kaspersky Endpoint Security는 해당 파일이 암호화 안 되어 있다면 암호화하지 않으며, 암호화되어 있다면 복호화합니다.

로컬 컴퓨터 드라이브의 파일 복호화

로컬 드라이브의 파일을 복호화하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 파일 레벨 암호화**를 선택합니다.
4. 창 오른쪽에서 **암호화** 탭을 선택합니다.
5. 암호화 목록에서 복호화할 파일과 폴더를 삭제합니다. 그러려면 파일을 선택한 다음 **삭제** 버튼에서 마우스 오른쪽 버튼을 눌러 메뉴를 열고 **규칙 삭제 및 파일 복호화** 항목을 선택합니다.

   암호화 목록에서 파일과 폴더가 삭제되고 복호화 목록에 자동 추가됩니다.
6. 파일 복호화 목록 작성.
7. 변경 사항을 저장합니다.

정책이 적용되면 Kaspersky Endpoint Security가 복호화 목록에 추가된 암호화된 파일을 복호화합니다.

Kaspersky Endpoint Security는 암호화된 파일의 파라미터(파일 경로/파일 이름/파일 확장자)가 복호화 목록에 추가되어 있는 개체의 파라미터와 일치하도록 변경될 경우 이 파일을 복호화합니다.

Kaspersky Endpoint Security는 파일이 열려 있을 경우 닫힐 때까지 복호화를 연기합니다.

암호화 패키지 생성

회사 네트워크 외부의 사용자에게 파일을 보낼 때 데이터를 보호하기 위해 암호화 패키지를 사용할 수 있습니다. 이메일 클라이언트에는 파일 크기 제한이 있기 때문에 암호화 패키지는 이동식 드라이브에서 대용량 파일을 전송하는 데 편리할 수 있습니다.

암호화 패키지를 생성하기 전에 Kaspersky Endpoint Security에서 사용자에게 암호를 입력하라는 메시지가 표시됩니다. 데이터를 안정적으로 보호하기 위해 암호 강도 검사를 사용하고 암호 강도 요건을 지정할 수 있습니다. 이를 통해 사용자가 짧고 간단한 암호(예: `1234`)를 사용하는 것을 방지할 수 있습니다.

관리 콘솔(MMC)에서 암호화된 압축 파일을 생성할 때 암호 강도 검사를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 일반 암호화 설정**을 선택합니다.
4. **암호 설정** 블록에서 **설정** 버튼을 누릅니다.
5. 열린 창에서 **암호화 패키지** 탭을 선택합니다.
6. 암호화 패키지를 생성할 때 암호 복잡성 설정을 구성합니다.

웹 콘솔에서 암호화된 압축 파일을 생성할 때 암호 강도 검사를 활성화하는 방법

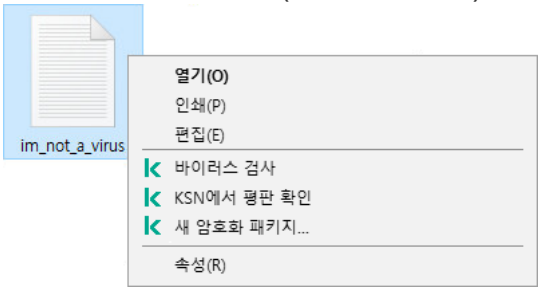
1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **데이터 암호화 → 파일 레벨 암호화**로 이동합니다.
5. **암호화 패키지 암호 설정** 블록에서 암호화된 패키지를 만들 때 필요한 암호 강도 기준을 구성합니다.

파일 레벨 암호화를 사용할 수 있는 Kaspersky Endpoint Security가 설치된 컴퓨터에서 암호화 패키지를 생성할 수 있습니다.

컨텐츠가 OneDrive 클라우드 저장소에 있는 파일을 암호화 패키지에 추가할 때 Kaspersky Endpoint Security는 해당 파일의 컨텐츠를 다운로드하여 암호화를 수행합니다.

암호화 패키지를 만들려면 다음과 같이 하십시오.

1. 파일 관리자에서 암호화 패키지에 추가할 파일 또는 폴더를 선택합니다. 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 엽니다.
2. 마우스 오른쪽 메뉴에서 **새 암호화 패키지**를 선택합니다(아래 그림 참조).



암호화 패키지 생성

3. 열리는 창에서 암호를 지정하고 확인합니다.

   암호는 정책에 지정된 복잡성 기준을 충족해야 합니다.

4. **생성**을 클릭합니다.

   암호화 패키지 생성 프로세스가 시작됩니다. Kaspersky Endpoint Security는 암호화 패키지를 만들 때 파일 압축을 수행하지 않습니다. 프로세스가 완료되면 선택된 대상 폴더에 암호로 보호되는 자동 압축 해제 방식의 암호화 패키지(확장자가 .exe인 실행 파일 - )가 생성됩니다.

암호화 패키지의 파일에 접근하려면 해당 파일을 두 번 클릭하여 압축 해제 마법사를 시작한 다음 암호를 입력합니다. 암호를 잊어버렸거나 분실한 경우 암호를 복구하고 암호화 패키지의 파일에 접근할 수 없습니다. 암호화 패키지를 다시 생성할 수 있습니다.

암호화된 파일에 대한 접근 복원

파일이 암호화되면 Kaspersky Endpoint Security는 암호화된 파일에 직접 접근하는 데 필요한 암호화 키를 받습니다. 파일 암호화 기능이 활성화된 Windows 사용자 계정으로 작업하는 사용자는 이 암호화 키를 사용하여 암호화된 파일에 바로 접근할 수 있습니다. 파일 암호화 기능이 활성화되지 않은 Windows 계정으로 작업하는 사용자가 암호화된 파일에 접근하기 위해서는 Kaspersky Security Center에 연결해야 합니다.

암호화된 파일에 접근할 수 없는 경우는 다음과 같습니다:

- 사용자의 컴퓨터가 암호화 키를 저장하지만 키를 관리하는 Kaspersky Security Center와 연결되어 있지 않을 경우. 이 경우 사용자가 LAN 관리자에게 암호화된 파일에 대한 접근 허용을 요청해야 합니다.

  사용자가 Kaspersky Security Center 접근 권한이 없으면 다음을 수행해야 합니다:

  - 컴퓨터 하드 드라이브에 저장된 암호화된 파일에 접근하기 위한 접근 허용 키를 요청해야 합니다.
  - 이동식 드라이브에 저장된 암호화된 파일에 접근하기 위해서는 각 이동식 드라이브의 암호화된 파일에 대해 별도의 접근 허용 키를 요청해야 합니다.

- 암호화 구성 요소가 사용자의 컴퓨터에서 삭제된 경우. 이 경우 사용자는 로컬 및 이동식 디스크에서 암호화된 파일을 열 수 있지만 해당 파일의 내용이 암호화된 상태로 표시됩니다.

  사용자는 다음 경우에 암호화된 파일을 사용할 수 있습니다:

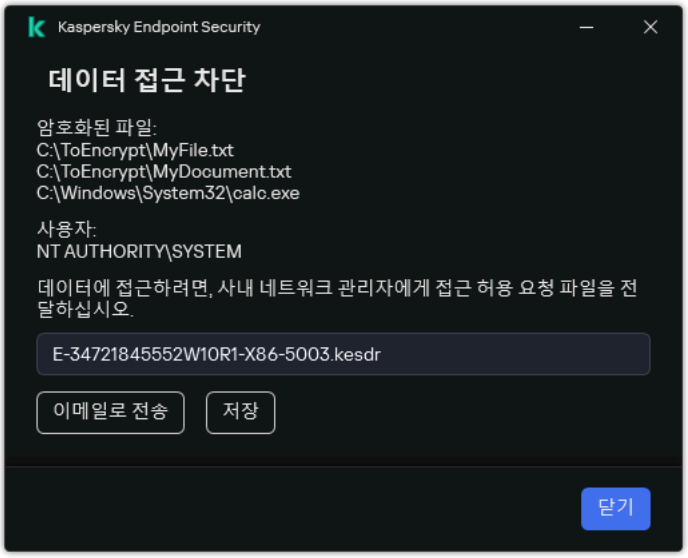
  - 파일이 Kaspersky Endpoint Security가 설치된 컴퓨터에서 만든 암호화 패키지에 들어 있는 경우.
  - 파일이 휴대용 모드가 허용되는 이동식 드라이브에 저장되어 있는 경우.

암호화된 파일에 접근하려면 복원 절차(요청/응답)를 시작해야 합니다.

암호화된 파일에 대한 접근 복구는 다음 단계로 구성됩니다.

1. 사용자는 접근 허용 요청 파일을 관리자에게 보냅니다(아래 그림 참조).
2. 관리자는 접근 허용 요청 파일을 Kaspersky Security Center에 추가하고 접근 허용 키 파일을 생성한 후 사용자에게 보냅니다.

3. 사용자는 접근 허용 키 파일을 Kaspersky Endpoint Security에 추가하고 파일에 접근합니다.



암호화된 파일에 대한 접근 복원

복원 절차를 시작하려면 사용자는 파일 접근을 시도해야 합니다. 그러면 Kaspersky Endpoint Security는 접근 허용 요청 파일(확장자가 KESDC인 파일)을 생성합니다. 이 파일은 사용자가 이메일 등을 통해 관리자에게 전송해야 합니다.

Kaspersky Endpoint Security는 컴퓨터 드라이브(로컬 드라이브 또는 이동식 드라이브)에 저장된 모든 암호화된 파일에 접근하기 위한 접근 허용 요청 파일을 생성합니다.

관리 콘솔(MMC)에서 암호화된 데이터 액세스 키 파일을 얻는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **기기**를 선택합니다.
3. **기기** 탭에서 암호화된 데이터에 접근을 요청하는 사용자 소유의 컴퓨터를 선택하고 마우스 오른쪽 버튼을 눌러 메뉴를 엽니다.
4. 마우스 오른쪽 메뉴에서 **오프라인 모드에서의 접근 권한 부여**를 선택합니다.
5. 열린 창에서 **데이터 암호화** 탭을 선택합니다.
6. **데이터 암호화** 탭에서 **찾아보기** 버튼을 누릅니다.
7. 접근 허용 요청 파일을 선택하는 창에서 사용자로부터 받은 파일의 경로를 지정합니다.

사용자의 접근 요청에 대한 정보가 표시됩니다. Kaspersky Security Center는 키 파일을 생성합니다. 암호화된 데이터 접근 허용 키 파일이 생성되면 사용자에게 이메일로 전송합니다. 또는 접근 허용 파일을 저장하고 이용 가능한 방법을 활용하여 파일을 전송합니다.



오프라인 모드에서의 접근 권한 부여

웹 콘솔에서 암호화된 데이터 접근 허용 키 파일을 얻는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)**를 선택합니다.
2. 데이터에 대한 접근을 복원하려는 컴퓨터 이름 옆의 확인란을 선택합니다.
3. **오프라인 모드인 기기에 접근 권한 부여** 버튼을 클릭합니다.
4. **데이터 암호화**를 선택합니다.
5. **파일 선택** 버튼을 클릭하고 사용자로부터 받은 접근 허용 요청 파일(확장자가 KESDC인 파일)을 선택합니다.

   웹 콘솔은 접근 허용 요청에 대한 정보를 표시합니다. 여기에는 사용자가 파일에 대한 접근 허용을 요청하는 컴퓨터의 이름이 포함됩니다.
6. **키 저장** 버튼을 클릭하고 폴더를 선택하여 암호화된 데이터 접근 허용 키 파일(확장자가 KESDR인 파일)을 저장합니다.

그러면 암호화된 데이터 접근 허용 키를 얻을 수 있으며 이를 사용자에게 전송해야 합니다.

암호화된 데이터 접근 허용 키 파일을 받은 후 사용자는 파일을 두 번 클릭하여 실행해야 합니다. 그러면 Kaspersky Endpoint Security는 드라이브에 저장된 모든 암호화된 파일에 대한 접근 권한을 부여합니다. 다른 드라이브에 저장된 암호화된 파일에 접근하려면 각 드라이브에 대해 별도의 접근 허용 키가 필요합니다.

운영 체제에 장애가 발생한 후 암호화된 데이터에 대한 접근 복원

파일 레벨 암호화(FLE)에 대해서만 운영 체제 장애 후 데이터에 대한 접근을 복원할 수 있습니다. 전체 디스크 암호화(FDE)를 사용하는 경우에는 데이터에 대한 접근을 복원할 수 없습니다.

운영 체제에 장애가 발생한 후 암호화된 데이터에 대한 접근을 복원하려면 다음과 같이 진행합니다:

1. 하드 드라이브를 포맷하지 않고 운영 체제를 다시 설치합니다.
2. Kaspersky Endpoint Security 설치합니다.
3. 데이터가 암호화되었을 때 그 컴퓨터를 제어했던 Kaspersky Security Center 중앙 관리 서버와 연결합니다.

운영 체제 장애가 발생하기 전과 동일한 조건으로 암호화된 데이터에 대한 접근 권한이 부여됩니다.

암호화된 파일 접근 메시지 템플릿 편집

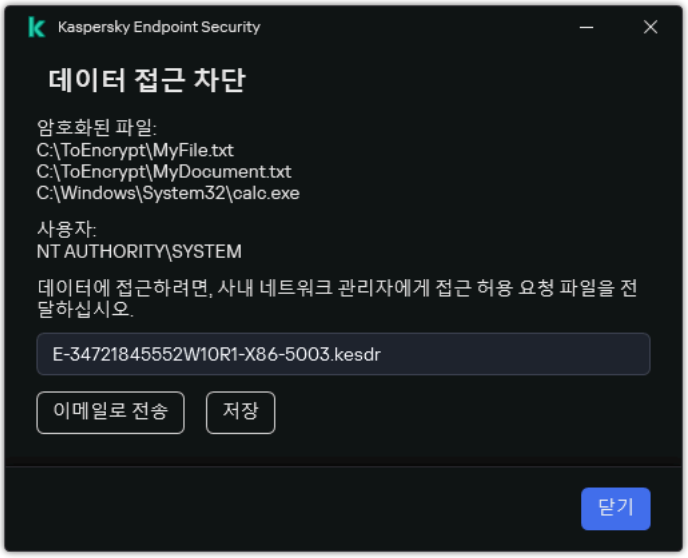
암호화된 파일 접근 메시지 템플릿을 편집하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 일반 암호화 설정**을 선택합니다.
4. **템플릿** 블록에서 **템플릿** 버튼을 클릭합니다.
5. 창이 열리면 다음을 수행합니다.
   - 사용자 메시지 템플릿을 편집하려면 **사용자 메시지** 탭을 선택합니다. 컴퓨터에 암호화된 파일 접근에 필요한 키가 없는데 사용자가 암호화된 파일에 접근을 시도할 경우 다음과 같은 창이 열립니다(아래 그림 참조). **이메일로 전송** 버튼을 클릭하면 자동으로 사용자 메시지가 생성됩니다. 이 이메일 메시지는 암호화된 파일 접근 요청과 함께 회사 LAN 관리자에게 전송됩니다.
   - 관리자 메시지 템플릿을 편집하려면 **관리자 메시지** 탭을 선택합니다. 사용자는 암호화된 파일에 대한 액세스 권한이 부여된 후 이 메시지를 받습니다.
6. 메시지 템플릿을 편집합니다.

   템플릿 텍스트에 변수를 추가하려면 원하는 위치에 커서를 두고 **변수**를 누른 뒤 사용 가능한 옵션 목록에서 필요한 변수를 선택합니다.

   기본적으로 버튼을 사용하여 기본 템플릿 텍스트를 복원할 수도 있습니다.

7. 변경 사항을 저장합니다.



암호화된 파일에 대한 접근 복원

이동식 드라이브 암호화

Arm 기반 컴퓨터에서는 이동식 드라이브 암호화를 지원하지 않습니다.

이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

Kaspersky Endpoint Security는 FAT32 및 NTFS 파일 시스템의 파일 암호화를 지원합니다. 지원하지 않는 파일 시스템을 사용하는 이동식 드라이브가 컴퓨터에 연결되어 있으면 해당 이동식 드라이브에 대한 암호화 작업 종료 시에 오류가 발생하며 Kaspersky Endpoint Security가 이동식 드라이브에 읽기 전용 상태를 할당합니다.

이동식 드라이브의 데이터를 보호하기 위해 다음 유형의 암호화를 사용할 수 있습니다.

- Full Disk Encryption (FDE, 전체 디스크 암호화)

  파일 시스템을 포함한 전체 이동식 드라이브의 암호화.

  회사 네트워크 외부에서 암호화된 데이터에 접근할 수 없습니다. 컴퓨터가 Kaspersky Security Center(예: "게스트" 컴퓨터에서)에 연결되어 있지 않으면 회사 네트워크 내에서 암호화된 데이터에 접근할 수 없습니다.

- File Level Encryption (FLE, 파일 레벨 암호화)

  이동식 드라이브에 있는 파일만 암호화. 파일 시스템은 변경되지 않습니다.

  이동식 드라이브의 파일을 암호화하면 *휴대용 모드*라는 특수 모드를 사용하여 회사 네트워크 외부의 데이터에 접근할 수 있습니다.

암호화 중에 Kaspersky Endpoint Security는 마스터 키를 생성합니다. Kaspersky Endpoint Security는 다음 저장소에 마스터 키를 저장합니다.

- Kaspersky Security Center
- 사용자의 컴퓨터
  마스터 키는 사용자의 비밀 키로 암호화됩니다.
- 이동식 드라이브
  마스터 키는 Kaspersky Security Center의 공개 키로 암호화됩니다.

암호화가 완료되면 일반 암호화되지 않은 이동식 드라이브에 있는 것처럼 회사 네트워크 내에서 이동식 드라이브의 데이터에 접근할 수 있습니다.

암호화된 데이터 접근

암호화된 데이터가 있는 이동식 드라이브가 연결되면 Kaspersky Endpoint Security는 다음 작업을 수행합니다.

1. 사용자 컴퓨터의 로컬 저장소에서 마스터 키를 확인합니다.
   마스터 키가 발견되면 사용자는 이동식 드라이브의 데이터에 접근할 수 있습니다.
   마스터 키를 찾지 못하면 Kaspersky Endpoint Security는 다음 작업을 수행합니다.
   a. Kaspersky Security Center에 요청을 보냅니다.
      요청을 받은 후 Kaspersky Security Center는 마스터 키가 포함된 응답을 보냅니다.
   b. Kaspersky Endpoint Security는 암호화된 이동식 드라이브를 사용하여 후속 작업을 위해 사용자 컴퓨터의 로컬 저장소에 마스터 키를 저장합니다.
2. 데이터를 복호화합니다.

이동식 드라이브 암호화의 특징

이동식 드라이브 암호화에는 다음과 같은 특징이 있습니다.

- 특정 그룹의 관리 컴퓨터에 대해서는 별도의 이동식 드라이브 암호화 사전 설정을 사용하여 정책을 적용합니다. 따라서 이동식 드라이브의 암호화/복호화를 위해 구성된 Kaspersky Security Center 정책을 적용한 결과는 이동식 드라이브가 연결된 컴퓨터에 따라 다릅니다.
- Kaspersky Endpoint Security는 이동식 드라이브에 저장된 읽기 전용 파일은 암호화/복호화하지 않습니다.
- 다음 장치 유형은 이동식 드라이브로 지원됩니다:
  - USB 버스를 통해 연결된 데이터 미디어
  - USB 및 FireWire 버스를 통해 연결된 하드 드라이브
  - USB 및 FireWire 버스를 통해 연결된 SSD 드라이브

이동식 드라이브 암호화 시작

정책을 사용하여 이동식 드라이브를 복호화할 수 있습니다. 특정 관리 그룹에 대해 이동식 드라이브 암호화에 대한 설정이 정의된 정책이 생성됩니다. 따라서 이동식 드라이브가 연결된 컴퓨터에 따라 이동식 드라이브의 데이터 복호화가 다르게 적용될 수 있습니다.

Kaspersky Endpoint Security는 FAT32 및 NTFS 파일 시스템의 파일 암호화를 지원합니다. 지원하지 않는 파일 시스템을 사용하는 이동식 드라이브가 컴퓨터에 연결되어 있으면 해당 이동식 드라이브에 대한 암호화 작업 종료 시에 오류가 발생하며 Kaspersky Endpoint Security가 이동식 드라이브에 읽기 전용 상태를 할당합니다.

이동식 드라이브의 파일을 암호화하기 전에 포맷 여부와 숨겨진 파티션(예: EFI 시스템 파티션)이 없는지 확인하십시오. 드라이브에 포맷되지 않았거나 숨겨진 파티션이 포함된 경우 파일 암호화가 오류와 함께 실패할 수 있습니다.

이동식 드라이브를 암호화하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 이동식 드라이브 암호화**를 선택합니다.
4. **암호화 모드** 드롭다운 목록에서 Kaspersky Endpoint Security가 이동식 드라이브에 대해 수행할 기본 작업을 선택합니다.
   - **전체 이동식 드라이브 암호화**(FDE). Kaspersky Endpoint Security가 이동식 드라이브에서 모든 섹터의 내용을 암호화합니다. 따라서 이동식 드라이브에 저장된 파일은 물론, 파일 이름과 폴더 구조를 포함하여 이동식 드라이브의 파일 시스템도 암호화됩니다.
   - **모든 파일 암호화**(FLE). Kaspersky Endpoint Security가 이동식 드라이브에 저장된 모든 파일을 암호화합니다. 파일의 이름과 폴더 구조를 포함하여 이동식 드라이브의 파일 시스템은 암호화되지 않습니다.
   - **새 파일만 암호화**(FLE). Kaspersky Endpoint Security가 Kaspersky Security Center 정책이 마지막으로 적용된 후 이동식 드라이브에 새로 추가되거나 기존에 저장되어 있다가 수정된 파일만 암호화합니다.

   Kaspersky Endpoint Security는 이미 암호화된 이동식 드라이브는 암호화하지 않습니다.
5. 이동식 드라이브의 암호화에 휴대용 모드를 사용하려면 **휴대용 모드** 확인란을 선택합니다.

   *휴대용 모드*는 회사 네트워크 외부의 데이터에 접근할 수 있는 이동식 드라이브의 파일 암호화(FLE) 모드입니다. 휴대용 모드는 또한 Kaspersky Endpoint Security가 설치되지 않은 컴퓨터에서 암호화된 데이터로 작업할 수 있도록 해줍니다.
6. 새 이동식 드라이브를 암호화하려면 **사용한 디스크 공간만 암호화** 확인란을 선택하는 것이 좋습니다. 이 확인란을 선택 해제하면 Kaspersky Endpoint Security가 삭제 또는 수정된 파일의 남은 파일 조각을 포함하여 모든 파일을 암호화합니다.
7. 개별 이동식 드라이브에 대한 암호화를 구성하려면 암호화 규칙을 정의하십시오.

8. 오프라인 모드에서 이동식 드라이브의 전체 디스크 암호화를 사용하려면 **오프라인 모드에서 이동식 드라이브 암호화 허용** 확인란을 선택합니다.

   *오프라인 암호화 모드*는 Kaspersky Security Center와 연결되지 않은 경우의 이동식 드라이브 암호화(FDE)를 말합니다. 암호화를 진행하는 동안 Kaspersky Endpoint Security가 사용자의 컴퓨터에만 마스터 키를 저장합니다. Kaspersky Endpoint Security는 다음 번 동기화가 이루어질 때 이 마스터 키를 Kaspersky Security Center에 전송합니다.

   마스터 키가 저장된 컴퓨터가 손상되어 데이터가 Kaspersky Security Center로 전송되지 않으면 이동식 드라이브에 대한 접근 권한을 획득할 수 없습니다.

   오프라인 모드에서 이동식 드라이브 암호화 허용 확인란이 선택 해제되어있고 Kaspersky Security Center와의 연결이 끊기면 이동식 드라이브 암호화가 불가능합니다.

9. 변경 사항을 저장합니다.

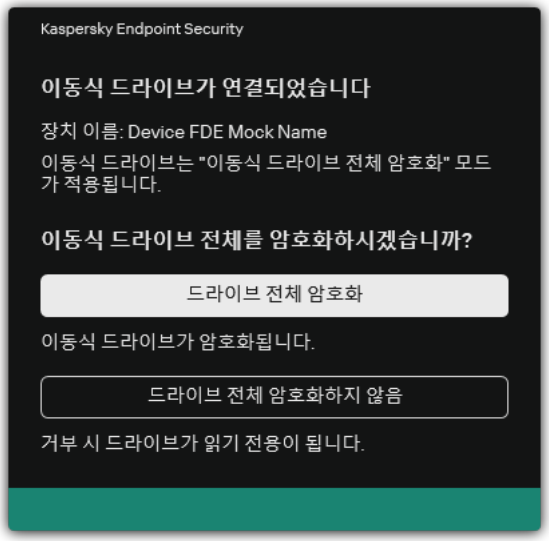
정책이 적용된 후 사용자가 이동식 드라이브를 연결하거나 이동식 드라이브가 이미 연결되어 있을 경우 Kaspersky Endpoint Security가 암호화 작업을 수행할 것인지를 확인하는 메시지를 표시합니다(아래 그림 참조).

애플리케이션에서 다음과 같은 동작을 수행할 수 있습니다.

- 사용자가 암호화 요청을 확인하면 Kaspersky Endpoint Security가 데이터를 암호화합니다.
- 사용자가 암호화 요청을 거부하면 Kaspersky Endpoint Security가 데이터를 있는 그대로 두고 이 이동식 드라이브에 대한 읽기 권한만 할당합니다.
- 사용자가 암호화 요청에 응답하지 않으면 Kaspersky Endpoint Security가 데이터를 있는 그대로 두고 이 이동식 드라이브에 대한 읽기 권한만 할당합니다. 이후 정책을 적용할 때 또는 다음에 이 이동식 드라이브가 연결될 때 애플리케이션이 확인을 요청하는 메시지를 다시 표시합니다.

데이터 암호화 도중 사용자가 이동식 드라이브의 안전 제거를 시작할 경우 Kaspersky Endpoint Security는 데이터 암호화 프로세스를 중단하므로 암호화 프로세스가 완료될 때까지 기다릴 필요 없이 이동식 드라이브를 제거할 수 있습니다. 다음 번에 이동식 드라이브가 이 컴퓨터에 연결될 때 데이터 암호화가 계속해서 진행됩니다.

이동식 드라이브의 암호화에 실패하면 Kaspersky Endpoint Security 인터페이스에서 **데이터 암호화** 리포트를 보십시오. 다른 애플리케이션에서 파일에 대한 접근을 차단했을 수 있습니다. 이 경우 컴퓨터에서 이동식 드라이브를 분리한 다음 다시 연결해 보십시오.



이동식 드라이브 암호화 요청

이동식 드라이브에 대한 암호화 규칙 추가

이동식 드라이브에 대한 암호화 규칙을 추가하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화** → **이동식 드라이브 암호화**를 선택합니다.
4. **추가** 버튼을 눌러 드롭다운 메뉴에서 다음 항목 중 하나를 선택합니다.
   - 장치 제어 구성 요소의 신뢰하는 장치 목록에 속하는 이동식 드라이브에 대한 암호화 규칙을 추가하려면 **이 정책의 신뢰하는 장치 목록에서**를 선택합니다.
   - Kaspersky Security Center 목록에 속하는 이동식 드라이브에 대한 암호화 규칙을 추가하려면 **Kaspersky Security Center 장치 목록에서**를 선택합니다.
5. **선택한 장치에 대한 암호화 모드** 드롭다운 목록에서 선택된 이동식 드라이브에 저장된 파일에 대해 Kaspersky Endpoint Security가 수행할 처리 방법을 선택합니다.
6. Kaspersky Endpoint Security가 암호화를 수행하기 전에 휴대용 모드에서 저장된 암호화된 파일을 사용할 수 있도록 이동식 드라이브를 설정하려면 **휴대용 모드** 확인란을 선택합니다.

   휴대용 모드에서는 암호화 기능이 없는 컴퓨터에 연결된 이동식 드라이브에 저장된 암호화된 파일을 사용할 수 있습니다.

7. Kaspersky Endpoint Security가 파일이 저장되어 있는 디스크 부분만 암호화하도록 하려면 **사용한 디스크 공간만 암호화** 확인란을 선택합니다.

   이미 사용 중인 드라이브에 암호화를 적용하는 경우 전체 드라이브를 암호화하는 것이 좋습니다. 이러면 검색 가능한 정보를 포함한 삭제된 데이터를 비롯한 모든 데이터가 보호됩니다. **사용한 디스크 공간만 암호화** 기능은 이전에 사용하지 않은 새 드라이브에 사용하는 것이 좋습니다.

   장치가 이전에 **사용한 디스크 공간만 암호화** 기능을 사용하여 암호화되었으면 **전체 이동식 드라이브 암호화** 모드에서 정책을 적용하더라도 파일이 저장되어 있지 않은 부분은 계속 암호화되지 않습니다.

8. **장치가 선택되기 전에 생성된 파일의 동작 방법** 드롭다운 목록에서 이전에 이동식 드라이브에 정의된 암호화 규칙에 따라 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택합니다.

   - 이전에 이동식 드라이브에 만들어진 암호화 규칙이 계속 변경되지 않기를 원하면 **건너뛰기**를 선택합니다.
   - 이전에 이동식 드라이브에 만들어진 암호화 규칙을 새 규칙으로 바꾸려면 **새로 고침**을 선택합니다.

9. 변경 사항을 저장합니다.

이동식 드라이브에 대한 추가 암호화 규칙은 조직의 모든 컴퓨터에 연결된 이동식 드라이브에 적용됩니다.

이동식 드라이브에 대한 암호화 규칙 목록 내보내기 및 가져오기

이동식 드라이브 암호화 규칙 목록을 XML 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 동일 유형의 이동식 드라이브에 대한 규칙을 여러 개 추가하는 등의 작업을 진행할 수 있습니다. 내보내기 / 가져오기 기능을 사용하여 규칙 목록을 백업하거나 규칙을 다른 서버로 마이그레이션할 수도 있습니다.

관리 콘솔(MMC)에서 이동식 드라이브 암호화 규칙 목록을 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **데이터 암호화 → 이동식 드라이브 암호화**로 이동합니다.
5. **선택한 장치에 대한 암호화 규칙** 블록에서 **<N>개 규칙** 링크를 클릭합니다.

   이동식 드라이브에 대한 암호화 규칙 목록이 열립니다.
6. 이동식 드라이브에 대한 암호화 규칙 목록을 내보내려면 다음을 수행합니다.

   a. 내보낼 규칙을 선택합니다.

   b. **내보내기**를 클릭합니다.

   c. 선택한 규칙만 내보낼 것인지 전체 목록을 내보낼 것인지 확인하십시오.

   d. 파일을 저장합니다.

   Kaspersky Endpoint Security는 규칙 목록을 기본 다운로드 폴더의 XML 파일로 내보냅니다.

7. 규칙 목록을 가져오려면 다음을 수행합니다.

   a. **가져오기** 링크를 클릭합니다.

      창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.

   b. 파일을 엽니다.

      컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

8. 변경 사항을 저장합니다.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **데이터 암호화 → 이동식 드라이브 암호화**를 선택합니다.

4. 이동식 드라이브에 대한 암호화 규칙 목록을 내보내려면 다음을 수행합니다.

   a. 내보낼 규칙을 선택합니다. 여러 포트를 선택하려면 **CTRL** 또는 **SHIFT** 키를 사용합니다.

      규칙을 선택하지 않으면 Kaspersky Endpoint Security는 모든 규칙을 내 보냅니다.

   b. **내보내기** 링크를 클릭합니다.

   c. 창이 열리면 규칙 목록을 내보낼 XML 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

   d. 파일을 저장합니다.

      Kaspersky Endpoint Security는 신뢰하는 규칙 목록을 XML 파일로 내보냅니다.

5. 이동식 드라이브에 대한 암호화 규칙 목록을 가져오려면 다음을 수행합니다.

   a. **가져오기** 링크를 클릭합니다.

      창이 열리면 규칙 목록을 가져올 XML 파일을 선택합니다.

   b. 파일을 엽니다.

      컴퓨터에 이미 규칙 목록이 있으면 Kaspersky Endpoint Security는 기존 목록을 삭제하거나 XML 파일에 새 항목을 추가하라는 메시지를 표시합니다.

6. 변경 사항을 저장합니다.

이동식 드라이브의 암호화된 파일 접근을 위한 휴대용 모드

*휴대용 모드*는 회사 네트워크 외부의 데이터에 접근할 수 있는 이동식 드라이브의 파일 암호화(FLE) 모드입니다. 휴대용 모드는 또한 Kaspersky Endpoint Security가 설치되지 않은 컴퓨터에서 암호화된 데이터로 작업할 수 있도록 해줍니다.

휴대용 모드는 다음과 같은 경우에 사용하기 편리합니다.

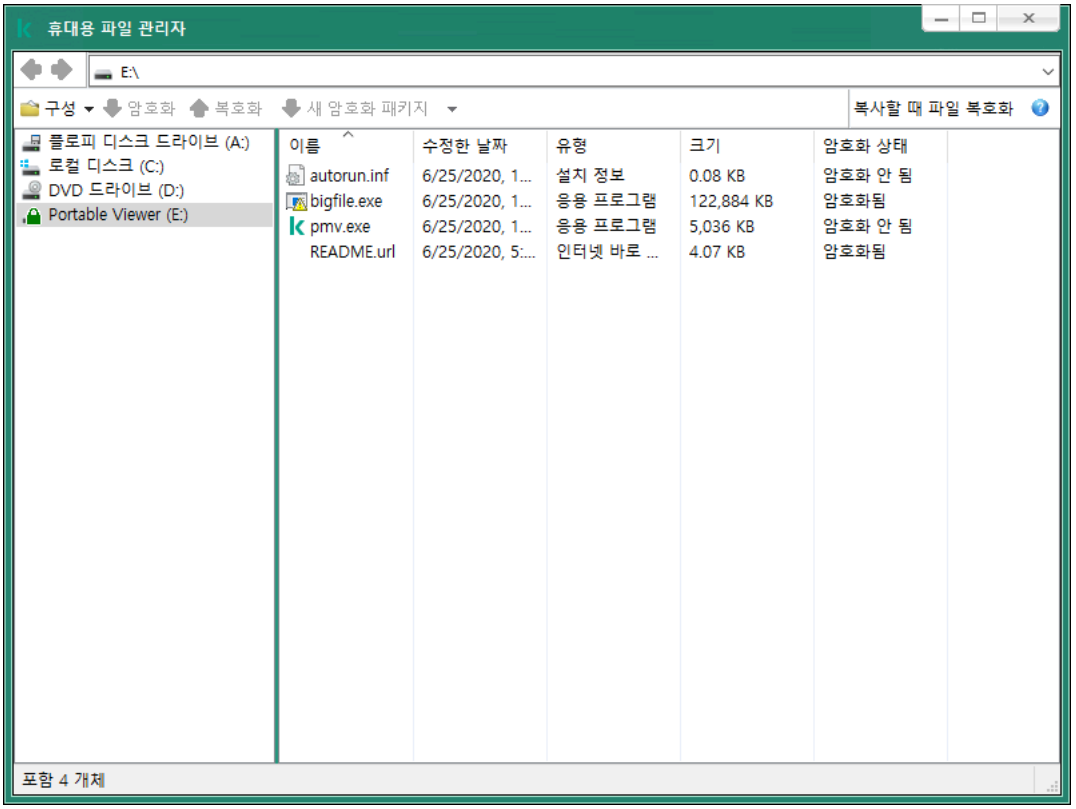
- 컴퓨터와 Kaspersky Security Center 중앙 관리 서버가 연결되어 있지 않습니다.
- Kaspersky Security Center 중앙 관리 서버가 변경되면서 인프라가 변경되었습니다.
- 컴퓨터에 Kaspersky Endpoint Security가 설치되어 있지 않습니다.

휴대용 파일 관리자

휴대용 모드에서 작업하기 위해 Kaspersky Endpoint Security는 이동식 드라이브에 *휴대용 파일 관리자* 라는 특수 암호화 모듈을 설치합니다. 휴대용 파일 관리자는 Kaspersky Endpoint Security가 컴퓨터에 설치되어 있지 않은 경우 암호화된 데이터 작업을 위한 인터페이스를 제공합니다(아래 그림 참조). Kaspersky Endpoint Security가 컴퓨터에 설치되어 있는 경우 일반적인 파일 관리자(예: 탐색기)를 사용하여 암호화된 이동식 드라이브로 작업할 수 있습니다.

휴대용 파일 관리자는 파일을 암호화하는 키를 이동식 드라이브에 저장합니다. 키는 사용자 암호로 암호화됩니다. 사용자는 이동식 드라이브의 파일을 암호화하기 전에 암호를 설정합니다.

이동식 드라이브가 Kaspersky Endpoint Security가 설치되지 않은 컴퓨터에 연결되면 휴대용 파일 관리자가 자동으로 시작됩니다. 컴퓨터에서 애플리케이션의 자동 시작이 비활성화된 경우 휴대용 파일 관리자를 직접 시작하십시오. 이렇게 하려면 이동식 드라이브에 저장된 pmv.exe 파일을 실행하십시오.



휴대용 파일 관리자

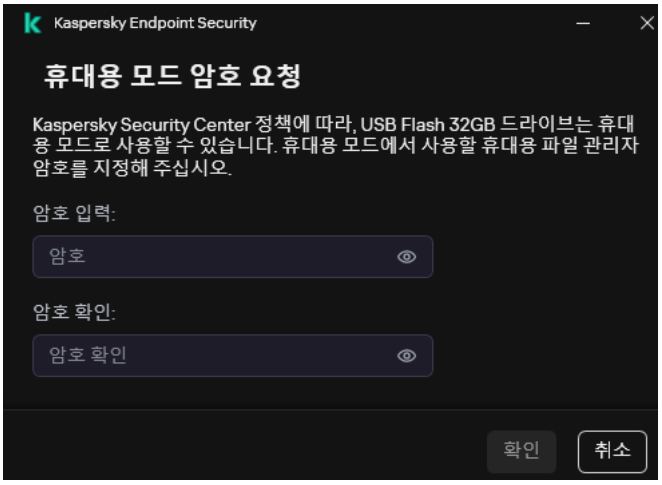
암호화된 파일 작업을 위한 휴대용 모드 지원

관리 콘솔(MMC)의 이동식 드라이브에서 암호화된 파일 작업을 위한 휴대용 모드 지원을 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 이동식 드라이브 암호화**를 선택합니다.
4. **선택한 장치에 대한 암호화 모드** 드롭다운 목록에서 **모든 파일 암호화** 또는 **새 파일만 암호화**를 선택합니다.

   휴대용 모드는 파일 레벨 암호화(FLE)에서만 사용할 수 있습니다. 전체 디스크 암호화(FDE)에 대한 휴대용 모드 지원은 활성화할 수 없습니다.

5. **휴대용 모드** 확인란을 선택합니다.
6. 필요한 경우 개별 이동식 드라이브에 대한 암호화 규칙을 추가합니다.
7. 변경 사항을 저장합니다.
8. 정책을 적용한 후 이동식 드라이브를 컴퓨터에 연결합니다.
9. 이동식 드라이브 암호화 작동을 확인합니다.
   휴대용 파일 관리자용 암호를 생성하는 창이 열립니다.



휴대용 모드 암호 요청

10. 암호 강도 요건에 부합하는 암호를 지정하고 확인합니다.
11. 변경 사항을 저장합니다.

웹 콘솔의 이동식 드라이브에서 암호화된 파일 작업을 위한 휴대용 모드 지원을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **데이터 암호화 → 이동식 드라이브 암호화**로 이동합니다.

5. **기본 작업** 블록에서 **모든 파일 암호화** 또는 **새 파일만 암호화**를 선택합니다.

> 휴대용 모드는 파일 레벨 암호화(FLE)에서만 사용할 수 있습니다. 전체 디스크 암호화(FDE)에 대한 휴대용 모드 지원은 활성화할 수 없습니다.

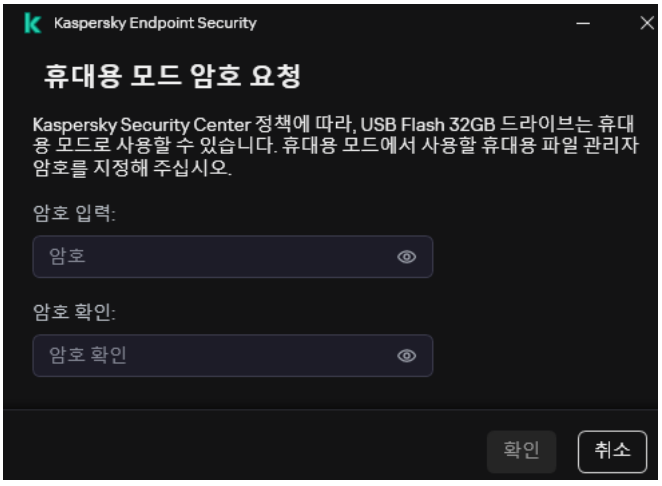
6. **휴대용 모드** 확인란을 선택합니다.

7. 필요한 경우 개별 이동식 드라이브에 대한 암호화 규칙을 추가합니다.

8. 변경 사항을 저장합니다.

9. 정책을 적용한 후 이동식 드라이브를 컴퓨터에 연결합니다.

10. 이동식 드라이브 암호화 작동을 확인합니다.
    휴대용 파일 관리자용 암호를 생성하는 창이 열립니다.



휴대용 모드 암호 요청

11. 암호 강도 요건에 부합하는 암호를 지정하고 확인합니다.

12. 변경 사항을 저장합니다.

Kaspersky Endpoint Security가 이동식 드라이브의 파일을 암호화합니다. 암호화된 파일 작업에 사용된 휴대용 파일 관리자 또한 이동식 드라이브에 추가됩니다. 이동식 드라이브에 이미 암호화된 파일이 있는 경우 Kaspersky Endpoint Security는 자체 키를 사용하여 다시 암호화합니다. 이를 통해 사용자는 휴대용 모드에서 이동식 드라이브의 모든 파일에 접근할 수 있습니다.

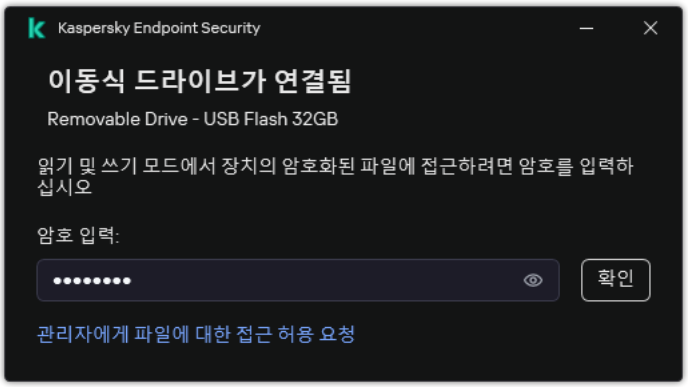
이동식 드라이브에서 암호화된 파일에 접근

휴대용 모드를 지원하는 이동식 드라이브에서 파일을 암호화한 후 다음과 같은 파일 접근 방법을 사용할 수 있습니다.

- 컴퓨터에 Kaspersky Endpoint Security가 설치되어 있지 않은 경우 휴대용 파일 관리자가 암호를 입력하라는 메시지를 표시합니다. 컴퓨터를 다시 시작하거나 이동식 드라이브를 다시 연결할 때마다 암호를 입력해야 합니다.

- 컴퓨터가 회사 네트워크 외부에 있고 컴퓨터에 Kaspersky Endpoint Security가 설치된 경우 애플리케이션은 암호를 입력하라는 메시지를 표시하거나 관리자에게 파일 접근 요청을 보냅니다. 이동식 드라이브의 파일에 대한 접근을 획득한 후 Kaspersky Endpoint Security는 비밀 키를 컴퓨터의 키 저장소에 저장합니다. 이렇게 하면 나중에 암호를 입력하거나 관리자에게 묻지 않고도 파일에 접근할 수 있습니다(아래 그림 참조).

- 컴퓨터가 회사 네트워크 내부에 있고 컴퓨터에 Kaspersky Endpoint Security가 설치된 경우 암호를 입력하지 않고 장치에 접근할 수 있습니다. Kaspersky Endpoint Security는 컴퓨터가 연결된 Kaspersky Security Center 중앙 관리 서버로부터 비밀 키를 받습니다.



이동식 드라이브에서 암호화된 파일에 접근

휴대용 모드에서 작업하기 위한 암호 복구

휴대용 모드에서 작업하기 위한 암호를 잊어버린 경우 회사 네트워크 내에 Kaspersky Endpoint Security가 설치된 컴퓨터에 이동식 드라이브를 연결해야 합니다. 비밀 키는 컴퓨터의 키 저장소 또는 중앙 관리 서버에 저장되므로 파일에 접근할 수 있습니다. 파일을 복호화하고 새 암호로 다시 암호화하십시오.

다른 네트워크에서 이동식 드라이브를 컴퓨터에 연결할 때 휴대용 모드의 기능

컴퓨터가 회사 네트워크 외부에 있고 컴퓨터에 Kaspersky Endpoint Security가 설치된 경우 다음과 같은 방법으로 파일에 접근할 수 있습니다.

- **암호 기반 접근**

암호를 입력한 후 이동식 드라이브에서 파일을 보고 수정하고 저장할 수 있습니다(*투명한 접근*). 이동식 드라이브의 암호화를 위한 정책 설정에 다음 파라미터가 구성되어 있는 경우 Kaspersky Endpoint Security는 이동식 드라이브에 대한 읽기 전용 접근 권한을 설정할 수 있습니다.

- 휴대용 모드 지원이 비활성화됨.
- **모든 파일 암호화** 또는 **새 파일만 암호화** 모드가 선택됨.

다른 모든 경우에는 이동식 드라이브에 대한 전체 접근 권한을 갖습니다(읽기/쓰기 권한). 사용자는 파일을 추가하고 삭제할 수 있습니다.

이동식 드라이브가 컴퓨터에 연결되어 있는 동안에도 이동식 드라이브 접근 권한을 변경할 수 있습니다. 이동식 드라이브 접근 권한이 변경되면 Kaspersky Endpoint Security는 파일에 대한 접근을 차단하고 암호를 다시 입력하라는 메시지를 표시합니다.

암호를 입력한 후 이동식 드라이브에 대한 암호화 정책 설정을 적용할 수 없습니다. 이 경우 이동식 드라이브의 파일을 복호화하거나 다시 암호화할 수 없습니다.

- **관리자에게 파일 접근 요청**

  휴대용 모드에서 작업하기 위한 암호를 잊어버린 경우 관리자에게 파일 접근을 요청하십시오. 파일에 접근하려면 사용자는 관리자에게 접근 허용 요청 파일(확장자가 KESDC인 파일)을 보내야 합니다. 예를 들어 사용자는 접근 허용 요청 파일을 이메일로 보낼 수 있습니다. 관리자는 암호화된 데이터 접근 파일(확장자가 KESDR인 파일)을 보냅니다.

  요청-응답 암호 복원 절차를 완료하면 이동식 드라이브 파일에 대한 투명한 접근 권한과 이동식 드라이브에 대한 전체 권한(읽기/쓰기 권한)이 부여됩니다.

  예를 들어 이동식 드라이브 암호화 정책을 적용하고 파일을 복호화할 수 있습니다. 암호를 복구하거나 정책이 업데이트되면 Kaspersky Endpoint Security는 변경 사항을 확인하라는 메시지를 표시합니다.

  관리 콘솔(MMC)에서 암호화된 데이터 접근 파일을 얻는 방법

  1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
  2. 콘솔 트리에서 **기기**를 선택합니다.
  3. **기기** 탭에서 암호화된 데이터에 접근을 요청하는 사용자 소유의 컴퓨터를 선택하고 마우스 오른쪽 버튼을 눌러 메뉴를 엽니다.
  4. 마우스 오른쪽 메뉴에서 **오프라인 모드에서의 접근 권한 부여**를 선택합니다.
  5. 열린 창에서 **데이터 암호화** 탭을 선택합니다.
  6. **데이터 암호화** 탭에서 **찾아보기** 버튼을 누릅니다.
  7. 접근 허용 요청 파일을 선택하는 창에서 사용자로부터 받은 파일의 경로를 지정합니다.

사용자의 접근 요청에 대한 정보가 표시됩니다. Kaspersky Security Center는 키 파일을 생성합니다. 암호화된 데이터 접근 허용 키 파일이 생성되면 사용자에게 이메일로 전송합니다. 또는 접근 허용 파일을 저장하고 이용 가능한 방법을 활용하여 파일을 전송합니다.



오프라인 모드에서의 접근 권한 부여

웹 콘솔에서 암호화된 데이터 접근 파일을 얻는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)**를 선택합니다.
2. 데이터에 대한 접근을 복원하려는 컴퓨터 이름 옆의 확인란을 선택합니다.
3. **오프라인 모드인 기기에 접근 권한 부여** 버튼을 클릭합니다.
4. **데이터 암호화**를 선택합니다.
5. **파일 선택** 버튼을 클릭하고 사용자로부터 받은 접근 허용 요청 파일(확장자가 KESDC인 파일)을 선택합니다.

   웹 콘솔은 접근 허용 요청에 대한 정보를 표시합니다. 여기에는 사용자가 파일에 대한 접근 허용을 요청하는 컴퓨터의 이름이 포함됩니다.
6. **키 저장** 버튼을 클릭하고 폴더를 선택하여 암호화된 데이터 접근 허용 키 파일(확장자가 KESDR인 파일)을 저장합니다.

그러면 암호화된 데이터 접근 허용 키를 얻을 수 있으며 이를 사용자에게 전송해야 합니다.

이동식 드라이브의 복호화

정책을 사용하여 이동식 드라이브를 복호화할 수 있습니다. 특정 관리 그룹에 대해 이동식 드라이브 암호화에 대한 설정이 정의된 정책이 생성됩니다. 따라서 이동식 드라이브가 연결된 컴퓨터에 따라 이동식 드라이브의 데이터 복호화가 다르게 적용될 수 있습니다.

이동식 드라이브를 복호화하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **데이터 암호화 → 이동식 드라이브 암호화**를 선택합니다.
4. 이동식 드라이브에 저장된 모든 암호화된 파일을 복호화하려면 **암호화 모드** 드롭다운 목록에서 **전체 이동식 드라이브 복호화**를 선택합니다.
5. 개별 이동식 드라이브에 저장된 데이터를 복호화하려면 복호화할 이동식 드라이브의 암호화 규칙을 편집합니다. 이를 위해서는 다음과 같이 하십시오.
   a. 암호화 규칙이 구성된 이동식 드라이브의 목록에서 필요한 이동식 드라이브에 해당하는 항목을 선택합니다.
   b. **규칙 설정** 버튼을 눌러 선택된 이동식 드라이브의 암호화 규칙을 편집합니다.
   c. **규칙 설정** 버튼의 마우스 오른쪽 메뉴에서, **전체 이동식 드라이브 복호화** 항목을 선택합니다.
6. 변경 사항을 저장합니다.

그 결과 사용자가 이동식 드라이브를 연결하거나 또는 이미 연결된 경우 Kaspersky Endpoint Security는 이동식 드라이브를 복호화합니다. 애플리케이션은 사용자에게 복호화 과정에 다소 시간이 소요될 수 있음을 경고합니다. 데이터 복호화 도중 사용자가 이동식 드라이브의 안전 제거를 시작할 경우 Kaspersky Endpoint Security는 데이터 복호화 프로세스를 중단하므로 복호화 동작이 완료될 때까지 기다릴 필요 없이 이동식 드라이브를 제거할 수 있습니다. 다음 번에 이동식 드라이브가 해당 컴퓨터에 연결될 때 데이터 복호화가 계속해서 진행됩니다.

이동식 드라이브의 복호화에 실패하면 Kaspersky Endpoint Security 인터페이스에서 **데이터 암호화** 리포트를 보십시오. 다른 애플리케이션에서 파일에 대한 접근을 차단했을 수 있습니다. 이 경우 컴퓨터에서 이동식 드라이브를 분리한 다음 다시 연결해 보십시오.

데이터 암호화 상세 정보 보기

Kaspersky Endpoint Security는 진행 중인 암호화 또는 복호화에 대해 클라이언트 컴퓨터에 적용되는 암호화 파라미터의 상태에 관한 정보를 Kaspersky Security Center로 전달합니다.

암호화 상태 보기

상태를 확인하여 데이터 암호화를 모니터링할 수 있습니다. Kaspersky Endpoint Security는 다음 암호화 상태를 할당합니다:

- **사용자에 의해 취소되어 관리자 정책과 일치하지 않음**. 사용자가 데이터 암호화를 취소했습니다.
- **오류로 인해 관리자의 정책과 일치하지 않음**. 데이터 암호화 오류(예: 라이센스 없음).

- **정책 적용. 재시작해야 합니다**. 컴퓨터에서 데이터 암호화가 진행 중입니다. 컴퓨터를 다시 시작하여 데이터 암호화를 완료합니다.
- **암호화 정책이 정의 안 됨**. 정책 설정에서 데이터 암호화가 꺼져 있습니다.
- **지원 안 됨**. 데이터 암호화 구성 요소가 컴퓨터에 설치되지 않습니다.
- **정책 적용 중**. 컴퓨터에서 데이터 암호화 및 복호화가 진행 중입니다.

컴퓨터 데이터의 암호화 상태를 보려면 다음을 수행합니다.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **관리 중인 기기**를 선택합니다.
3. 작업 공간의 **기기** 탭에서 화면 오른쪽 끝으로 이동합니다. 만약 **암호화 상태** 열이 표시되지 않으면 Kaspersky Security Center 콘솔 설정에 이 열을 추가합니다.

   암호화 상태 열에 선택된 관리 그룹 컴퓨터의 데이터 암호화 상태가 표시됩니다. 이 상태는 컴퓨터 로컬 드라이브의 파일 암호화에 관한 정보와 전체 디스크 암호화에 관한 정보를 기반으로 결정됩니다.
4. 컴퓨터의 데이터 암호화 상태가 **정책 적용 중**이라면, 암호화 진행률 패널을 모니터링할 수 있습니다.
   a. **정책 적용 중** 상태를 두 번 클릭하여 해당 상태인 컴퓨터의 속성을 엽니다.
   b. 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.
   c. 컴퓨터에 설치된 Kaspersky 애플리케이션 목록에서 **Kaspersky Endpoint Security for Windows**를 선택합니다.
   d. **통계**를 클릭합니다.
   e. **기기 암호화**에서 데이터 암호화의 현재 진행률을 백분율로 볼 수 있습니다.

Kaspersky Security Center 대시보드에서 암호화 통계 보기

Kaspersky Security Center 대시보드에서 암호화 상태를 보려면 다음을 수행합니다.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
3. 관리 콘솔 트리 오른쪽의 작업 공간에서 **통계** 탭을 선택합니다.
4. 데이터 암호화 통계가 있는 상세 정보로 새 페이지를 생성합니다. 이를 위해서는 다음과 같이 하십시오.
   a. **통계** 탭에서 **사용자 지정 보기** 버튼을 누릅니다.
   b. 열리는 창에서 **추가** 버튼을 누릅니다.
   c. 창이 열리면 **일반** 섹션에서 페이지 이름을 입력합니다.
   d. **정보 패널** 섹션에서 **추가** 버튼을 누릅니다.

e. **보호 상태** 그룹에서 창이 열리면 **기기 암호화** 항목을 선택합니다.

f. **확인**을 누릅니다.

g. 필요하다면 세부 정보 부분의 설정을 편집합니다. 그러려면 **보기** 및 **기기** 섹션을 사용합니다.

h. **확인**을 누릅니다.

i. 위에 나온 d~h 단계를 반복하고 **보호 상태** 섹션에서 **이동식 드라이브 암호화** 항목을 선택합니다.
추가된 세부 정보 창이 **정보 패널** 목록에 표시됩니다.

j. **확인**을 누릅니다.
이전 단계에서 생성된 상세 정보 창의 페이지 이름이 **페이지** 목록에 표시됩니다.

k. **닫기** 버튼을 클릭합니다.

5. 지침의 이전 단계에서 생성된 페이지를 **통계** 탭에서 엽니다.

컴퓨터 및 이동식 드라이브의 암호화 상태가 나와 있는 상세 정보가 표시됩니다.

로컬 컴퓨터 드라이브의 파일 암호화 오류 보기

컴퓨터 로컬 드라이브의 파일 암호화 오류를 확인하려면 다음을 수행합니다.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 콘솔 트리에서 **관리 중인 기기**를 선택합니다.

3. **기기** 탭에서 목록의 컴퓨터 이름을 선택한 후 오른쪽 클릭하여 마우스 오른쪽 메뉴를 엽니다.

4. 컴퓨터의 마우스 오른쪽 메뉴에서 **속성** 항목을 선택합니다. 창이 열리면 **보호** 섹션을 선택합니다.

5. **데이터 암호화 오류 보기** 링크를 눌러 **데이터 암호화 오류** 창을 엽니다.

이 창에 로컬 컴퓨터 드라이브의 파일 암호화 오류에 대한 상세 정보가 표시됩니다. 오류가 수정되면 Kaspersky Security Center는 **데이터 암호화 오류** 창에서 오류 정보를 삭제합니다.

데이터 암호화 리포트 보기

Kaspersky Security Center를 사용하면 데이터 암호화 리포트를 생성할 수 있습니다.

- **관리 중인 기기의 암호화 상태 리포트**. 리포트에는 컴퓨터의 암호화 상태가 암호화 정책을 준수하는지에 대한 정보가 포함됩니다.
- **대용량 스토리지 기기의 암호화 상태 리포트**. 리포트에는 외부 장치 및 스토리지 기기의 암호화 상태 관련 정보가 포함됩니다.
- **암호화된 드라이브로의 접근에 대한 권한 리포트**. 리포트에는 암호화된 드라이브에 대한 액세스 권한이 있는 계정의 상태 관련 정보가 포함됩니다.

- **파일 암호화 오류 리포트**. 리포트에는 컴퓨터에서 데이터 암호화 또는 암호 해독 작업을 실행하는 동안 발생한 오류 관련 정보가 포함됩니다.
- **암호화된 파일로의 접근 차단 리포트**. 리포트에는 암호화된 파일에 대한 액세스가 차단된 애플리케이션 관련 정보가 포함됩니다.

데이터 암호화 리포트를 보려면 다음과 같이 하십시오.

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **중앙 관리 서버** 노드에서 **리포트** 탭을 선택합니다.
3. **새 리포트 템플릿** 버튼을 누릅니다.

   새 리포트 템플릿 마법사가 시작됩니다.
4. 리포트 템플릿 마법사의 안내를 따릅니다. **기타** 섹션의 **리포트 템플릿 유형 선택** 창에서 데이터 암호화 리포트 중 하나를 선택합니다.

   새 리포트 템플릿 마법사를 종료하면 **리포트** 탭에 표로 새 리포트 템플릿이 나타납니다.
5. 이전 안내 단계에서 만든 리포트 템플릿을 선택합니다.
6. 템플릿의 마우스 오른쪽 메뉴에서 **리포트 표시**를 선택합니다.

리포트 생성 프로세스가 시작됩니다. 리포트가 새 창으로 표시됩니다.

암호화된 장치에 접근할 수 없는 경우 장치 사용

암호화된 장치로의 접근 권한 얻기

사용자는 다음 경우에 암호화된 장치에 대한 접근 허용을 요청해야 합니다:

- 하드 드라이브가 다른 컴퓨터에서 암호화된 경우.
- 장치의 암호화 키가 컴퓨터에 없고(예를 들어 컴퓨터의 암호화된 이동식 드라이브에 처음 접근하려고 시도할 때), 컴퓨터가 Kaspersky Security Center에 연결되지 않은 경우.

  사용자가 암호화된 장치에 대한 접근 허용 키를 적용하면 Kaspersky Endpoint Security가 사용자의 컴퓨터에 암호화 키를 저장하고 Kaspersky Security Center에 연결되어 있지 않더라도 이후의 접근 시도에서 이 장치에 대한 접근을 허용합니다.

다음과 같이 암호화된 장치에 대한 접근 권한을 얻을 수 있습니다:

1. 사용자가 Kaspersky Endpoint Security 애플리케이션 인터페이스를 사용해 kesdc 확장자를 사용하는 접근 허용 요청 파일을 만든 다음 그 파일을 회사의 LAN 관리자에게 전송합니다.
2. 관리자가 Kaspersky Security Center 관리 콘솔을 사용해 kesdr 확장자를 사용하는 접근 허용 키 파일을 생성한 다음 그 파일을 사용자에게 전송합니다.
3. 사용자가 접근 허용 키를 적용합니다.

암호화된 장치에 저장된 데이터 복원

사용자가 암호화된 장치 복원 유틸리티(복원 유틸리티)를 사용해 암호화된 장치를 사용할 수 있습니다. 다음과 같은 경우에 이런 것이 필요할 수 있습니다:

- 접근 허용 키를 사용해 접근 권한 얻기 절차가 실패한 경우.
- 암호화된 장치가 있는 컴퓨터에 암호화 구성 요소가 설치되지 않은 경우.

복원 유틸리티를 사용하여 암호화된 장치에 대한 접근을 복원하는 데 필요한 데이터가 사용자 컴퓨터의 메모리에 상당 기간 동안 암호화되지 않은 형태로 남아 있는 경우. 그러한 데이터에 무단으로 접근할 수 있는 위험을 감소시키려면 신뢰하는 컴퓨터에서 암호화된 장치에 대한 접근을 복원하는 것이 좋습니다.

다음과 같이 암호화된 장치에 저장된 데이터를 복원할 수 있습니다:

1. 사용자가 복원 유틸리티를 사용해 fdertc 확장자를 사용하는 접근 허용 요청 파일을 만든 다음 그 파일을 회사의 LAN 관리자에게 전송합니다.
2. 관리자기 Kaspersky Security Center 관리 콘솔을 사용해 fdertr 확장자를 사용하는 접근 허용 키 파일을 생성한 다음 그 파일을 사용자에게 전송합니다.
3. 사용자가 접근 허용 키를 적용합니다.

암호화된 시스템 하드 드라이브에 저장된 데이터를 복원하기 위해 사용자는 복원 유틸리티에서 인증 에이전트 계정 자격 증명 또한 지정할 수 있습니다. 인증 에이전트 계정의 메타데이터가 손상된 경우 접근 허용 요청 파일을 사용하여 복원 절차를 완료해야 합니다.

암호화된 장치에 데이터를 복원하기 전에 해당 절차를 수행할 시스템의 Kaspersky Security Center 정책 설정에서 암호화를 중지하거나 Kaspersky Security Center 정책을 취소하는 것이 좋습니다. 그래야만 장치가 다시 암호화되지 않습니다.

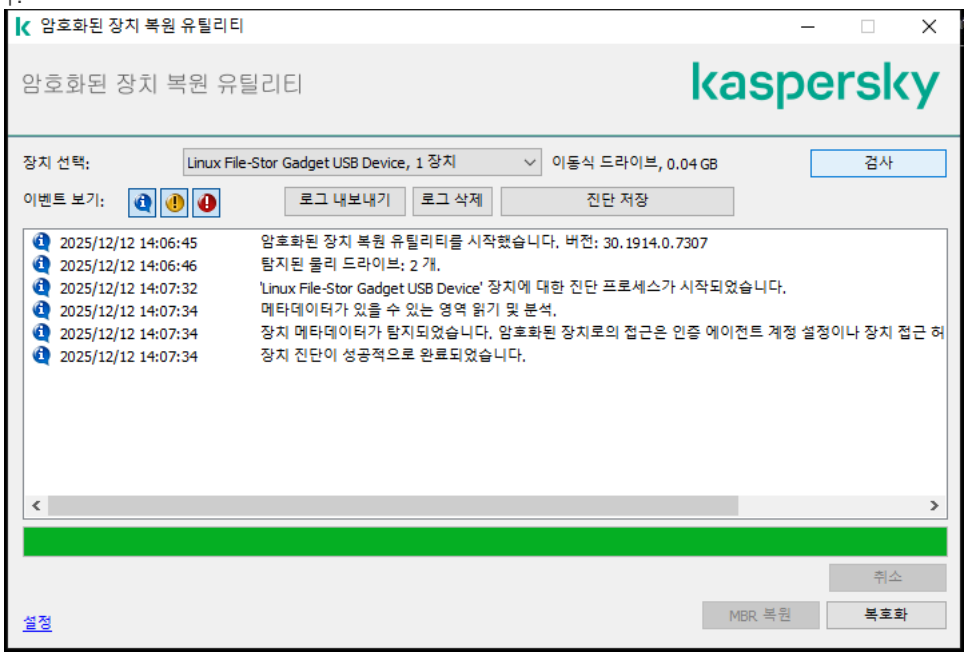
FDERT 복원 유틸리티를 사용하여 데이터 복원

하드 드라이브가 작동하지 않는 경우 파일 시스템이 손상되었을 수 있습니다. 이 경우 Kaspersky 디스크 암호화 기술로 보호된 데이터를 사용할 수 없습니다. 데이터를 복호화하고 데이터를 새 드라이브에 복사할 수 있습니다.

Kaspersky 디스크 암호화 기술로 보호되는 드라이브의 데이터 복원은 다음 단계로 구성됩니다.

1. 독립 실행형 복원 유틸리티를 생성합니다(아래 그림 참조).
2. Kaspersky Endpoint Security 암호화 구성 요소가 설치되지 않은 컴퓨터에 드라이브를 연결합니다.
3. 복원 유틸리티를 실행하고 하드 드라이브를 진단합니다.

4. 드라이브의 데이터에 접근합니다. 그렇게 하려면 인증 에이전트의 자격 증명을 입력하거나 복원 절차(요청-응답)를 시작합니다.



FDERT 복원 유틸리티

독립 실행형 복원 유틸리티 생성

복원 유틸리티의 실행 파일을 생성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 창이 열리면 **암호화된 장치 복원** 버튼을 누릅니다.
   암호화된 장치 복원 유틸리티가 시작됩니다.
3. 복원 유틸리티 창에서 **독립 실행형 복원 유틸리티 생성** 버튼을 누릅니다.
4. 독립 실행형 복원 유틸리티를 컴퓨터 메모리에 저장합니다.

그러면 복원 유틸리티(fdert.exe)의 실행 파일이 지정된 폴더에 저장됩니다. Kaspersky Endpoint Security 암호화 구성 요소가 없는 컴퓨터에 복원 유틸리티를 복사합니다. 그래야만 드라이브가 다시 암호화되지 않습니다.

복원 유틸리티를 사용하여 암호화된 장치에 대한 접근을 복원하는 데 필요한 데이터가 사용자 컴퓨터의 메모리에 상당 기간 동안 암호화되지 않은 형태로 남아 있는 경우. 그러한 데이터에 무단으로 접근할 수 있는 위험을 감소시키려면 신뢰하는 컴퓨터에서 암호화된 장치에 대한 접근을 복원하는 것이 좋습니다.

하드 드라이브에서 데이터 복원

복원 유틸리티를 사용하여 암호화된 드라이브에 대한 접근을 복원하려면 다음과 같이 하십시오.

1. 복원 유틸리티의 실행 파일인 fdert.exe 파일을 실행합니다. 이 파일은 Kaspersky Endpoint Security에 의해 생성되었습니다.

2. 복원 유틸리티 창에서 접근을 복원할 암호화된 장치를 선택합니다.

3. **검사** 버튼을 누르면 잠금 해제 또는 복호화 등 유틸리티에서 장치에 대해 수행할 작업을 정의합니다.

   컴퓨터가 Kaspersky Endpoint Security 암호화 기능을 사용할 수 있는 경우 복원 유틸리티에 장치를 차단 해제하라는 메시지가 표시됩니다. 장치를 차단 해제해도 장치가 복호화되지 않지만 장치에 바로 접근할 수는 있습니다. 컴퓨터가 Kaspersky Endpoint Security 암호화 기능을 사용할 수 없는 경우 복원 유틸리티에 장치를 복호화라는 메시지가 표시됩니다.

4. 진단 정보를 가져오려면 **진단 저장** 버튼을 클릭합니다.

   이 유틸리티는 진단 정보가 포함된 파일과 함께 압축 파일을 저장합니다.

5. 암호화된 시스템 하드 드라이브의 진단 결과 장치의 마스터 부트 레코드(MBR)와 관련하여 문제가 발생했다는 메시지가 표시될 경우 **MBR 복원** 버튼을 누릅니다.

   장치의 마스터 부트 레코드 문제를 해결하면 장치의 차단 해제 또는 복호화에 필요한 정보를 얻는 과정이 크게 단축될 수 있습니다.

6. 진단 결과에 따라 **잠금 해제** 또는 **복호화** 버튼을 누릅니다.

7. 인증 에이전트 계정을 사용하여 데이터를 복원하려면 **인증 에이전트 계정 설정 사용** 옵션을 선택하고 인증 에이전트의 자격 증명을 입력합니다.

   이 방법은 시스템 하드 드라이브에 저장된 데이터를 복원할 때만 사용할 수 있습니다. 시스템 하드 드라이브가 손상되고 인증 에이전트 계정 데이터가 손실된 경우 회사 LAN 관리자에게 접근 허용 키를 받아서 암호화된 장치에 저장된 데이터를 복원해야 합니다.

8. 복원 절차를 시작하려면 다음을 수행하십시오.

   a. **직접 장치 접근 허용 키 지정** 옵션을 선택합니다.

   b. **접근 허용 키 받기** 버튼을 클릭하고 접근 허용 요청 파일을 컴퓨터 메모리(확장자가 FDERTC인 파일)에 저장합니다.

   c. 접근 허용 요청 파일을 사내 LAN 관리자에게 전달합니다.

      접근 허용 키를 받은 다음에 **장치 접근 허용 키 받기** 창을 닫습니다. 이 창이 다시 열리면 이전에 관리자가 생성한 접근 허용 키를 사용하지 못합니다.

   d. 회사 LAN 관리자가 생성 및 전송한 접근 허용 파일(확장자가 FDERTR인 파일)을 받고 저장합니다(아래 지침 참조).

   e. **장치 접근 허용 키 받기** 창에서 접근 허용 파일을 다운로드합니다.

9. 장치를 복호화하는 경우 추가 복호화 설정을 구성해야 합니다.

   - 복호화할 영역 지정:
     - 장치 전체를 복호화하려면 **전체 장치 복호화** 옵션을 선택합니다.
     - 장치의 데이터 일부를 복호화하려면 **개별 장치 영역 복호화** 옵션을 선택하고 복호화 영역 경계를 지정합니다.
   - 복호화된 데이터를 쓸 위치 선택:
     - 원본 장치의 데이터가 복호화된 데이터로 덮어쓰기 되도록 하려면 **디스크 이미지 파일로 복호화** 확인란을 선택 해제합니다.
     - 암호화된 원본 데이터와는 별도로 복호화된 데이터를 저장하려면 **디스크 이미지 파일로 복호화** 확인란을 선택하고 **찾아보기** 버튼을 사용해 VHD 파일을 저장할 경로를 지정합니다.

10. **확인**을 누릅니다.

장치 차단 해제/복호화 과정이 시작됩니다.

관리 콘솔(MMC)에서 암호화된 데이터 접근 허용 파일을 생성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리에서 **고급 → 데이터 암호화 및 보호 → 암호화된 드라이브** 폴더를 선택합니다.
3. 작업 공간에서 접근 허용 키 파일을 생성할 암호화된 장치를 선택하고 장치의 마우스 오른쪽 메뉴에서 **Kaspersky Endpoint Security에서 장치에 대한 접근 권한 가져오기**를 클릭합니다.

   어느 컴퓨터에서 접근 허용 요청 파일을 생성했는지 확실하지 않다면 관리 콘솔 트리에서 **고급 → 데이터 암호화 및 보호** 폴더를 선택하고 작업 공간에서 **Kaspersky Endpoint Security에서 장치 암호화 키 가져오기**를 클릭합니다.

4. 창이 열리면 사용할 암호화 알고리즘(AES256 또는 AES56)을 선택합니다.

   데이터 암호화 알고리즘은 배포 패키지에 포함된 AES 암호화 라이브러리에 따라 다릅니다: *강한 암호화(AES256)* 또는 *가벼운 암호화(AES56)*. AES 암호화 라이브러리는 애플리케이션과 함께 설치됩니다.

5. **찾아보기**를 클릭해 창을 열고 사용자에게 받은 fdertc 확장자 요청 파일의 경로를 지정합니다.
6. **잠금 해제**를 클릭합니다.

사용자의 접근 요청에 대한 정보가 표시됩니다. Kaspersky Security Center는 키 파일을 생성합니다. 암호화된 데이터 접근 허용 키 파일이 생성되면 사용자에게 이메일로 전송합니다. 또는 접근 허용 파일을 저장하고 이용 가능한 방법을 활용하여 파일을 전송합니다.

웹 콘솔에서 암호화된 데이터 접근 허용 파일을 생성하는 방법

1. 웹 콘솔의 메인 창에서 **동작 → 데이터 암호화 및 보호 → 암호화된 드라이브**를 선택합니다.
2. 데이터를 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 Endpoint Security for Windows 플러그인을 선택합니다.

   b. 사용할 암호화 알고리즘(AES256 또는 AES56)을 선택합니다.

      데이터 암호화 알고리즘은 배포 패키지에 포함된 AES 암호화 라이브러리에 따라 다릅니다: *강한 암호화(AES256)* 또는 *가벼운 암호화(AES56)*. AES 암호화 라이브러리는 애플리케이션과 함께 설치됩니다.

   c. 사용자로부터 받은 접근 허용 요청 파일을 선택합니다(확장자가 FDERTC인 파일).

   d. 폴더를 선택하여 암호화된 데이터 액세스 키 파일을 저장합니다(확장자가 FDERTR인 파일).

그러면 암호화된 데이터 접근 허용 키를 얻을 수 있으며 이를 사용자에게 전송해야 합니다.

운영 체제 응급 복구 디스크 만들기

운영 체제 응급 복구 디스크는 어떤 이유로 암호화된 하드 드라이브에 접근할 수 없어 운영 체제가 로드되지 않을 때 유용하게 사용할 수 있습니다.

응급 복구 디스크를 사용하여 Windows 운영 체제의 이미지를 로드한 후 운영 체제 이미지에 포함된 복원 유틸리티를 사용하여 암호화된 하드 드라이브에 대한 접근을 복원할 수 있습니다.

운영 체제 응급 복구 디스크를 만들려면 다음과 같이 하십시오.

1. 암호화된 장치 복원 유틸리티의 실행 파일을 생성합니다.

2. Windows 사전 부팅 환경의 사용자 지정 이미지를 만듭니다. Windows 사전 부팅 환경의 사용자 지정 이미지를 만들 때 복원 유틸리티의 실행 파일을 이미지에 추가합니다.

3. Windows 사전 설치 환경의 사용자 지정 이미지를 CD, 이동식 드라이브 등의 부팅 가능한 미디어에 저장합니다.

   Windows 사전 부팅 환경의 사용자 지정 이미지를 만드는 자세한 방법은 Microsoft 도움말 파일(예: Microsoft TechNet 리소스)을 참조하십시오.

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 Endpoint Security는 내장 에이전트를 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 Endpoint Detection and Response Optimum 2.0(EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert(EDR Expert)
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response Expert(EDR) 버전 7.1 및 이전
  - Network Detection and Response(NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert(on-premise)
- Kaspersky Sandbox 2.0

Kaspersky Endpoint Security와 Detection and Response 솔루션은 다양한 구성으로 사용할 수 있습니다(예: [EDR Optimum+MDR]).

MDR 및 EDR Optimum 라이센스

Kaspersky Endpoint Security는 Kaspersky Managed Detection and Response(MDR) 및 Kaspersky Endpoint Detection and Response Optimum(EDR Optimum) 솔루션의 기능을 지원합니다. 이러한 솔루션과 함께 Kaspersky Endpoint Security를 다양한 구성으로 사용하여 특정 요구 사항을 충족하는 사용자 지정 보호 시스템을 구축할 수 있습니다. 이를 위해서는 각 솔루션에 대한 라이센스를 구매해야 합니다. 라이센스에는 단일 솔루션(예: MDR 애드온만) 또는 여러 솔루션(EDR Optimum+MDR 애드온)을 사용하는 권한이 포함될 수 있습니다.

MDR 및 EDR Optimum은 다음 라이센스 방법을 지원합니다.

- MDR 또는 EDR Optimum 기능은 Kaspersky Endpoint Security for Windows 라이센스에 포함되어 있습니다.

  이 기능은 Kaspersky Endpoint Security for Windows 활성화 직후 바로 사용할 수 있습니다. 키를 하나 추가하면 됩니다.

- MDR 또는 EDR Optimum(MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on)에 대한 별도 라이센스.

  MDR 애드온, EDR Optimum 애드온 또는 [EDR Optimum+MDR] 애드온에 대한 별도 키를 추가해야 이 기능을 사용할 수 있습니다. 결과적으로 Kaspersky Endpoint Security 키와 MDR 또는 EDR Optimum 두 개의 키가 컴퓨터에 설치됩니다. Kaspersky Endpoint Security 키를 가장 먼저 추가해야 합니다.

Kaspersky Endpoint Security는 MDR 및 EDR Optimum 라이센스의 *활성 키*를 단 하나만 추가할 수 있게 허용합니다. 따라서 이 두 솔루션을 모두 활성화해야 하는 경우 각 솔루션에 대한 별도의 키가 아닌 [EDR Optimum+MDR] Add-on 키를 하나 추가해야 합니다. 하나의 *예약 키*를 추가할 수도 있습니다.

MDR 배포 시 BLOB 파일을 사용한 경우에는 MDR을 활성화하는 데 별도의 키가 필요하지 않습니다. BLOB 파일에는 이미 라이센스 정보가 포함되어 있습니다.

솔루션의 초기 라이센스

MDR 및 EDR Optimum을 처음 배포하면 솔루션이 Kaspersky Endpoint Security 애플리케이션과 같은 방식으로 활성화됩니다. *키 추가* 작업을 실행하거나 자동 키 배포 기능을 사용하여 키를 추가할 수 있습니다. 라이센스 키는 두 번째 활성 키로 또는 관련 확인란을 선택하는 경우 예약 키로 애플리케이션에 추가됩니다.

다른 라이센스로 전환

조직에 이미 이러한 솔루션 중 하나가 배포되어 있고 해당 키가 애플리케이션에 추가된 경우 새 구성의 라이센스와 관련해 특별히 고려할 사항이 몇 가지 있습니다. 다른 라이센스로 전환할 때 애플리케이션은 새 키를 애플리케이션에 추가하지 않고 현재 키를 새 키로 교체합니다. 그 이유는 애플리케이션이 MDR 및 EDR Optimum을 활성화하는 키를 하나만 추가할 수 있게 제한하기 때문입니다.

예를 들어 조직에 [EDR Optimum+MDR] 솔루션이 배포되어 있고 사용자가 MDR 애드온 구성으로 전환하기로 결정했다고 가정합니다. 새 구성으로 전환하려면 [EDR Optimum+MDR] Add-on 키를 MDR 애드온 키로 교체해야 합니다.

EDR Optimum 및 MDR([EDR Optimum+MDR] 애드온)에 대한 별도 라이센스를 더 이상 사용할 수 없습니다. 두 솔루션을 모두 사용하려면 BLOB 파일을 사용하여 MDR을 활성화하고 라이센스 키로 EDR Optimum을 활성화해야 합니다.

애플리케이션은 자동 키 배포 기능을 사용하여 같은 수의 솔루션에 포함된 라이센스 키를 거부합니다. 즉, EDR Optimum 애드온 키를 추가한 경우 이 키를 MDR 애드온 키로 교체할 수 없습니다. 그러나 EDR Optimum 애드온 키는 [EDR Optimum+MDR] 애드온 키로 교체할 수 있습니다. MDR 애드온 키를 EDR 애드온 키로 교체하려고 하는 경우에도 애플리케이션이 키를 거부합니다. 키를 교체하려면 *키 추가* 작업을 실행합니다. *키 추가* 작업으로 솔루션 수에 상관없이 라이센스 키를 교체할 수 있습니다.

[EDR Optimum+MDR] Add-on 예약 키가 추가되어 있는 경우 EDR Optimum 애드온 또는 MDR 애드온의 활성 키를 올바르게 추가하려면, 먼저 예비 키를 EDR Optimum 애드온 또는 MDR 애드온 키로 교체하거나 예비 키를 제거한 후 활성 키를 교체합니다.

타사 EDR 솔루션과의 호환성

Kaspersky Endpoint Security를 타사 EDR 솔루션과 함께 사용하여 워크스테이션과 서버를 보호할 수 있습니다. 오탐을 제거하려면 Kaspersky Endpoint Security와 Network Agent의 실행 파일을 타사 EDR 솔루션의 신뢰 구역에 추가하는 것이 좋습니다.

타사 EDR 솔루션과의 호환성을 위한 신뢰 구역

	Kaspersky Endpoint Security for Windows	Kaspersky Security Center 네트워크 에이전트
작업 폴더	`C:\Program Files (x86)\Kaspersky Lab\KES.14.0.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

실행 파일	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

*Kaspersky Endpoint Agent*는 지능형 위협을 탐지하기 위해 이 애플리케이션과 다른 Kaspersky 솔루션(Kaspersky Sandbox 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.

사용 중인 소프트웨어 솔루션에 포함된 Kaspersky Endpoint Agent에 대한 전체 정보와 독립형 솔루션에 대한 전체 정보는 관련 제품의 도움말 설명서를 참조하십시오:

- Kaspersky Anti Targeted Attack Platform 도움말
- Kaspersky Sandbox 도움말
- Kaspersky Endpoint Detection and Response Optimum 도움말
- Kaspersky Managed Detection and Response 도움말

Kaspersky Endpoint Security 버전 11.2.0~11.8.0용 배포 패키지에는 Kaspersky Endpoint Agent가 포함됩니다. Kaspersky Endpoint Security for Windows를 설치할 때 Kaspersky Endpoint Agent를 선택할 수 있습니다. 결과적으로 KEA와 KES 두 가지 애플리케이션이 컴퓨터에 설치됩니다. Kaspersky Endpoint Security 11.9.0에서는 Kaspersky Endpoint Security 배포 키트에 Kaspersky Endpoint Agent 배포 패키지가 포함되지 않습니다.

KES 버전에 대한 KEA 버전(KES의 일부)의 부합 여부

Kaspersky Endpoint Security for Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

Kaspersky는 모든 Detection and Response 솔루션을 Kaspersky Endpoint Agent 대신 Kaspersky Endpoint Security 내장 에이전트를 사용하도록 전환하고 있습니다. Kaspersky는 이 같은 솔루션에 대한 지원을 점진적으로 추가하고 있으며 Kaspersky Endpoint Agent를 단계적으로 중단하고 있습니다(아래 표 참조). 12.1 버전부터는 애플리케이션에서 모든 Detection and Response 솔루션을 지원합니다. 그리고 12.1 버전부터는 애플리케이션이 더 이상 Kaspersky Endpoint Agent와 호환되지 않으므로 한 컴퓨터에 두 애플리케이션을 나란히 설치할 수 없습니다.

Kaspersky Endpoint Security 버전	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform(Endpoint Detection and Response 구성 요소)	Kaspersky Anti Targeted Attack Platform(Network Detection and Response 구성 요소)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**내장 에이전트**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	Kaspersky Endpoint Agent
12.6	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**	**내장 에이전트**

[KES+KEA] 구성을 [KES+내장 에이전트] 구성으로 마이그레이션

Kaspersky Endpoint Security에는 Detection and Response 솔루션과 함께 작동하는 내장 에이전트가 포함되어 있습니다. 이제 Kaspersky Endpoint Agent 애플리케이션이 없어도 이 솔루션을 이용할 수 있습니다. Kaspersky Endpoint Agent가 설치된 컴퓨터에 Kaspersky Endpoint Security를 배포하면 Detection and Response 솔루션이 Kaspersky Endpoint Security와 계속해서 작동합니다. 또한 Kaspersky Endpoint Agent가 컴퓨터에서 제거됩니다.

Kaspersky Endpoint Security 버전 11.2.0~11.8.0용 배포 패키지에는 Kaspersky Endpoint Agent가 포함됩니다. Kaspersky Endpoint Security for Windows를 설치할 때 Kaspersky Endpoint Agent를 선택할 수 있습니다. 결과적으로 KEA와 KES 두 가지 애플리케이션이 컴퓨터에 설치됩니다. Kaspersky Endpoint Security 11.9.0에서는 Kaspersky Endpoint Security 배포 키트에 Kaspersky Endpoint Agent 배포 패키지가 포함되지 않습니다.

[KES+KEA] 구성을 [KES+내장 에이전트]로 마이그레이션하는 단계는 다음과 같습니다:

1. **Kaspersky Security Center 업그레이드**

   사용자 컴퓨터 및 웹 콘솔의 네트워크 에이전트를 포함하여 Kaspersky Security Center 구성 요소 전체를 버전 13.2 이상으로 업그레이드합니다.

2. **Kaspersky Endpoint Security 웹 플러그인 업그레이드**

   Kaspersky Security Center 웹 콘솔에서 Kaspersky Endpoint Security 웹 플러그인을 버전 11.7.0 이상으로 업그레이드합니다. EDR Optimum과 Kaspersky Sandbox 구성 요소를 관리하려면 웹 콘솔을 사용해야 합니다.

   Kaspersky Anti Targeted Attack Platform(EDR)을 사용하려면 Kaspersky Endpoint Security 버전 12.1 이상용 웹 플러그인이 필요합니다.

Kaspersky Anti Targeted Attack Platform(NDR)을 사용하려면 Kaspersky Endpoint Security 버전 12.7 이상용 웹 플러그인이 필요합니다.

3 정책 및 작업 마이그레이션

Kaspersky Endpoint Agent 정책 및 작업 마이그레이션 마법사를 사용하여 Kaspersky Endpoint Agent 설정을 Kaspersky Endpoint Security for Windows로 마이그레이션합니다.

새로운 Kaspersky Endpoint Security 정책을 생성합니다. 새 정책은 *비활성* 상태입니다. 정책을 적용하려면 정책 속성을 열고 Kaspersky Security Network 진술문을 수락한 후 상태를 *활성*으로 설정합니다.

4 라이센싱 기능

Kaspersky Endpoint Detection and Response Optimum 또는 Kaspersky Optimum Security 공통 라이센스를 사용하여 Kaspersky Endpoint Security for Windows 및 Kaspersky Endpoint Agent를 활성화하면 애플리케이션을 버전 11.7.0으로 업그레이드한 후 EDR Optimum 기능이 자동으로 활성화됩니다. 별도의 작업이 필요하지 않습니다.

독립 실행형 Kaspersky Endpoint Detection and Response 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 11.7.0으로 업그레이드하면 EDR Optimum 기능이 자동으로 활성화됩니다.

Kaspersky Endpoint Detection and Response Optimum이나 Kaspersky Optimum Security 라이센스로 Kaspersky Endpoint Agent를 활성화한 후 다른 라이센스로 Kaspersky Endpoint Security for Windows를 활성화하면 Kaspersky Endpoint Security for Windows 키를 Kaspersky Endpoint Detection and Response Optimum 또는 Kaspersky Optimum Security 공통 키로 교체해야 합니다. 키는 *키 추가* 작업으로 교체할 수 있습니다.

Kaspersky Sandbox 기능을 활성화할 필요가 없습니다. Kaspersky Endpoint Security for Windows를 업그레이드 및 활성화하면 Kaspersky Sandbox 기능을 즉시 이용할 수 있습니다.

Kaspersky Anti Targeted Attack Platform 솔루션의 일부로 Kaspersky Endpoint Security를 활성화하려면 Kaspersky Anti Targeted Attack Platform 라이센스만 사용할 수 있습니다. 애플리케이션을 버전 12.1으로 업그레이드하면 EDR(KATA) 기능이 자동으로 활성화됩니다. 별도의 작업이 필요하지 않습니다.

5 Kaspersky Endpoint Security 애플리케이션 업그레이드

애플리케이션을 업그레이드하고 EDR Optimum 및 Kaspersky Sandbox 기능을 마이그레이션하려면 원격 설치 작업을 권장합니다.

원격 설치 작업으로 애플리케이션을 업그레이드하려면 다음 설정을 편집해야 합니다.

- 설치 패키지의 설정에서 Detection and Response 솔루션의 구성 요소를 선택합니다.
- 설치 패키지 설정에서 Kaspersky Endpoint Agent 구성 요소를 제외하십시오(Kaspersky Endpoint Security for Windows 버전 11.2.0~11.8.0의 경우).
- 암호 보호를 사용하여 Kaspersky Endpoint Agent에 대한 접근을 제한하려면 *원격으로 애플리케이션 설치* 작업의 설정에서 애플리케이션 제거 암호를 입력합니다. Kaspersky Security Center Linux 15.1부터 제거 암호를 입력할 수 있습니다.

다음 방법을 사용하여 원격으로 애플리케이션을 업그레이드할 수도 있습니다:

- Kaspersky 업데이트 서비스 사용(원활한 업데이트 – SMU).
- 로컬에서 설치 마법사 실행.

Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 애플리케이션이 설치된 컴퓨터에서 애플리케이션을 업데이트할 때 구성 요소의 자동 선택을 지원합니다. 구성 요소의 자동 선택은 애플리케이션을 업그레이드하는 사용자 계정의 권한에 달려 있습니다.

시스템 계정(SYSTEM)의 EXE 또는 MSI 파일을 사용해 Kaspersky Endpoint Security를 업그레이드한다면 Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 대한 접근 권한을 획득합니다. 따라서 컴퓨터에 Kaspersky Endpoint Agent가 설치되어 있고 EDR Optimum 솔루션이 활성화되어 있는 것 같은 경우에 Kaspersky Endpoint Security 설치 프로그램은 자동으로 구성 요소의 세트를 구성하고 EDR Optimum 구성 요소를 선택합니다. 이에 따라 Kaspersky Endpoint Security는 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 Endpoint Security를 업그레이드한다면, Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 접근할 권한이 없습니다. 이때 Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 구성에 기반하여 자동으로 구성 요소를 선택합니다. 그리고 나서 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다.

6. **컴퓨터 재시작**

   내장 에이전트로 애플리케이션 업그레이드를 완료하려면 컴퓨터를 다시 시작하십시오. 애플리케이션 업그레이드 시, 설치 프로그램은 컴퓨터를 다시 시작하기 전에 Kaspersky Endpoint Agent를 제거합니다. 컴퓨터가 다시 시작되면 설치 프로그램이 내장 에이전트를 추가합니다. 즉, Kaspersky Endpoint Security는 컴퓨터가 다시 시작될 때까지 EDR 및 Kaspersky Sandbox의 기능을 수행하지 않습니다.

7. **Kaspersky Endpoint Detection and Response Optimum 및 Kaspersky Sandbox 상태 확인**

   업그레이드 후 Kaspersky Security Center에서 컴퓨터 상태가 *심각*으로 표시된다면:

   - 컴퓨터에 Network Agent 버전 13.2 이상이 설치되었는지 확인합니다.
   - *애플리케이션 구성 요소 상태 리포트*를 확인하여 내장 에이전트의 작동 상태를 확인합니다. 구성 요소의 상태가 *설치 안 됨*이라면 *애플리케이션 구성 요소 변경* 작업으로 구성 요소를 설치합니다.
   - Kaspersky Endpoint Security for Windows의 새 정책에서 Kaspersky Security Network 진술문을 수락해야 합니다.

   - *애플리케이션 구성 요소 상태 리포트*를 사용하여 EDR Optimum 기능을 활성화합니다. 구성 요소의 상태가 *라이센스에 포함되지 않음*이라면 EDR Optimum의 라이센스 키 자동 배포 기능이 켜졌는지 확인합니다.

Kaspersky Endpoint Agent의 정책 및 작업 마이그레이션

Kaspersky Endpoint Security for Windows에는 Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로 마이그레이션하기 위한 마법사가 추가됩니다. 다음 솔루션에 대해 정책과 작업 설정을 마이그레이션할 수 있습니다:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum(EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로 마이그레이션하는 마법사는 웹 콘솔과 Cloud Console에서만 작동합니다. 관리 콘솔(MMC)에서는 표준 Kaspersky Security Center 정책 및 작업 마이그레이션 마법사를 활용하여 Kaspersky Anti Targeted Attack Platform(EDR) 솔루션에 대한 설정을 마이그레이션만 할 수 있습니다.

우선 단일 컴퓨터에서 Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로의 마이그레이션을 시작한 다음, 컴퓨터 그룹을 거쳐 조직의 모든 컴퓨터를 대상으로 마이그레이션을 완료할 것을 권장합니다.

Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로 정책 및 작업 설정을 마이그레이션하려면 다음과 같이 하십시오.

웹 콘솔 메인 창에서 **동작** → **Kaspersky Endpoint Agent에서 마이그레이션**을 선택합니다.

정책 및 작업 마이그레이션 마법사가 열립니다. 마법사의 지침을 따릅니다.

1단계. 정책 마이그레이션

마이그레이션 마법사가 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent 정책의 설정을 병합하는 새 정책을 만듭니다. 정책 목록에서 Kaspersky Endpoint Security 정책에 병합하고자 하는 Kaspersky Endpoint Agent 정책 설정을 선택합니다. Kaspersky Endpoint Agent 정책을 클릭해서 설정을 병합할 Kaspersky Endpoint Security 정책을 선택합니다. 알맞은 정책을 선택했는지 확인하고 다음 단계로 넘어갑니다.

2단계. 정책 마이그레이션

마이그레이션 마법사는 Kaspersky Endpoint Security에 대한 새 작업을 생성합니다. 작업 목록에서 Kaspersky Endpoint Security 정책에 생성하고자 하는 Kaspersky Endpoint Agent 작업을 선택합니다. 마법사는 Kaspersky Endpoint Detection and Response와 Kaspersky Sandbox에 대한 작업을 지원합니다. 다음 단계로 넘어갑니다.

3단계. 마법사 완료

마법사를 끝냅니다. 결과적으로 마법사는 다음을 수행합니다.

- 새로운 Kaspersky Endpoint Security 정책을 생성합니다.

  정책이 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent의 설정을 병합합니다. 정책의 이름은 *<Kaspersky Endpoint Security 정책 이름> & <Kaspersky Endpoint Agent 정책 이름>*입니다. 새 정책은 *비활성* 상태입니다. 계속하려면 Kaspersky Endpoint Agent와 Kaspersky Endpoint Security 정책의 상태를 *비활성*으로 바꾸고 새로 병합된 정책을 활성화합니다.

  Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security for Windows로의 마이그레이션 후에는 새 정책에 중앙 관리 서버로의 데이터 전송 기능(격리 파일 데이터 및 보안 위협 개발 체인 데이터) 설정이 되어 있는지 확인하십시오. 데이터 전송 파라미터 값은 Kaspersky Endpoint Agent 정책에서 마이그레이션되지 않습니다.

  Kaspersky Anti Targeted Attack Platform(EDR) 솔루션을 위해 Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로 마이그레이션하는 경우, 컴퓨터를 Central Node 서버로 연결할 때 오류가 발생할 수도 있습니다. 그 이유는 웹 콘솔의 마이그레이션 마법사가 다음 정책 설정을 건너뛰고 마이그레이션하지 않기 때문입니다.

  - **KATA 서버에 연결**에 대한 설정 수정 금지('잠금').

    기본적으로 설정을 수정할 수 있습니다("잠금"이 열립니다). 따라서 설정이 컴퓨터에서 적용되지 않습니다. 설정 수정을 금지하고 '잠금'을 종료해야 합니다.

- 암호화 컨테이너.

  Central Node 서버로 연결하기 위해 양방향 인증을 사용하는 경우, 암호화 컨테이너를 다시 추가해야 합니다. 마이그레이션 마법사는 서버의 TLS 인증서를 올바로 마이그레이션합니다.

관리 콘솔(MMC)의 정책 및 작업 마이그레이션 마법사는 Kaspersky Anti Targeted Attack Platform(EDR) 솔루션에 대한 모든 설정을 마이그레이션합니다.

- 새 Kaspersky Endpoint Security 작업을 생성합니다.

  새 작업은 Kaspersky Endpoint Detection and Response와 Kaspersky Sandbox에 대한 Kaspersky Endpoint Agent 작업의 사본입니다. 또한 마법사는 Kaspersky Endpoint Agent 작업을 변경하지 않습니다.

관리 콘솔(MMC)에서 Kaspersky Endpoint Agent의 정책 및 작업 설정을 Kaspersky Endpoint Security로 마이그레이션하는 방법 (KATA(EDR)에만 해당)

1. 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

이 단계에서 Kaspersky Endpoint Security for Windows를 선택해야 합니다. 다음 단계로 넘어갑니다.

2단계. 정책 전환

마이그레이션 마법사는 마이그레이션할 Kaspersky Endpoint Agent 정책 설정에 대한 새로운 Kaspersky Endpoint Security 정책을 생성합니다. 정책 목록에서 Kaspersky Endpoint Security 정책으로 전송하고자 하는 Kaspersky Endpoint Agent 정책 설정을 선택합니다. 다음 단계로 넘어갑니다.

그러면 마이그레이션 마법사가 정책 변환을 시작합니다. 정책 변환 중에 마이그레이션 마법사에 Kaspersky Security Network 정책을 수락하라는 메시지가 표시됩니다. 새 정책의 이름이 *<정책 이름> (변환됨)*과 같이 지정됩니다.

3단계. 작업 전환

이 단계를 건너뜁니다. 마법사는 Kaspersky Endpoint Detection and Response Optimum과 Kaspersky Sandbox에 대한 작업만 지원합니다. 구성 요소는 웹 콘솔에서만 관리할 수 있습니다. 다음 단계로 넘어갑니다.

4단계. 마법사 완료

마법사를 끝냅니다. 마법사를 진행한 결과 새로운 Kaspersky Endpoint Security 정책이 생성됩니다.

Endpoint Detection and Response Agent(EDR Agent)

Kaspersky Endpoint Security 12.3 for Windows부터 애플리케이션에 Endpoint Detection and Response Agent(EDR Agent) 구성이 포함됩니다. *Endpoint Detection and Response Agent*는 조직의 IT 인프라에 있는 개별 워크스테이션 및 서버에 설치되어 다음과 같은 Kaspersky의 Detection and Response 솔루션을 지원하는 애플리케이션입니다.

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform(EDR)
- Kaspersky Unified Monitoring and Analysis Platform(KUMA)(12.6 버전부터)
- Kaspersky Anti Targeted Attack Platform(NDR)(12.7 버전부터)
- Kaspersky Endpoint Detection and Response Expert(on-premise)(12.11 버전부터)

EDR Agent는 이러한 컴퓨터에서 실행 중인 프로세스, 개방형 네트워크 연결, 수정 중인 파일을 지속적으로 모니터링합니다. EDR Agent는 애플리케이션 보호 및 제어 구성 요소를 사용할 수 없습니다.

EDR Agent는 타사 EPP 애플리케이션과 호환됩니다. 이를 통해 Kaspersky Detection and Response와 함께 타사 인프라 보안 도구를 사용할 수 있습니다.

EDR Agent를 배포하려면 컴퓨터에 네트워크 에이전트가 필수로 설치되어 있어야 하며 Kaspersky Security Center 콘솔에 컴퓨터가 추가되어 있어야 합니다. EDR Agent와 Kaspersky Security Center의 상호 작용을 활성화하려면 Kaspersky Endpoint Security for Windows 관리 플러그인을 설치해야 합니다. 그룹 정책을 사용하여 EDR Agent 설정을 지정할 수 있습니다. EDR Agent를 통합하려면 적절한 정책 섹션에서 통합을 진행해야 합니다.

Kaspersky Detection and Response 솔루션을 지원하려면 인프라에 다음 Kaspersky 애플리케이션을 설치해야 합니다.

	• 네트워크 에이전트 • EDR Agent
Endpoint	
	Kaspersky Endpoint Security for Windows 관리 플러그인
Kaspersky Security Center	
	
Detection and Response 솔루션: MDR, KATA(EDR), KATA(NDR), KUMA, EDR Expert(on-premise)	

EDR Agent 설치

Kaspersky Detection and Response 솔루션에 대한 Endpoint Detection and Response Agent(EDR Agent) 구성의 Kaspersky Endpoint Security도 같은 방식으로 설치됩니다.

다음 방법 중 하나를 따라 컴퓨터에 EDR Agent를 설치할 수 있습니다.

- Kaspersky Security Center 원격 사용.
- 로컬에서 설치 마법사 사용.
- 명령줄에서 로컬로(KATA(EDR) 및 EDR Expert(on-premise)만 해당).

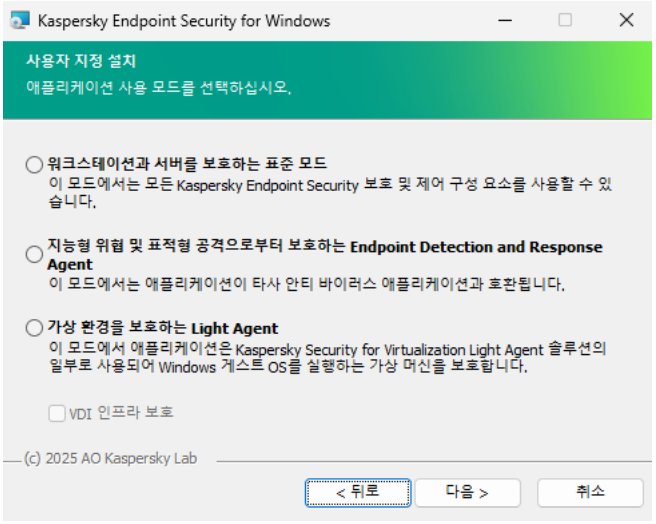
EDR Agent를 설치하려면 설치 패키지 설정 또는 설치 마법사 중에서 알맞은 구성을 선택해야 합니다.

설치 마법사를 사용하여 EDR Agent를 설치하는 방법

1. 배포 키트 폴더를 사용자의 컴퓨터에 복사합니다.
2. setup_kes.exe를 실행합니다.

   설치 마법사가 시작됩니다.

Kaspersky Endpoint Security 구성

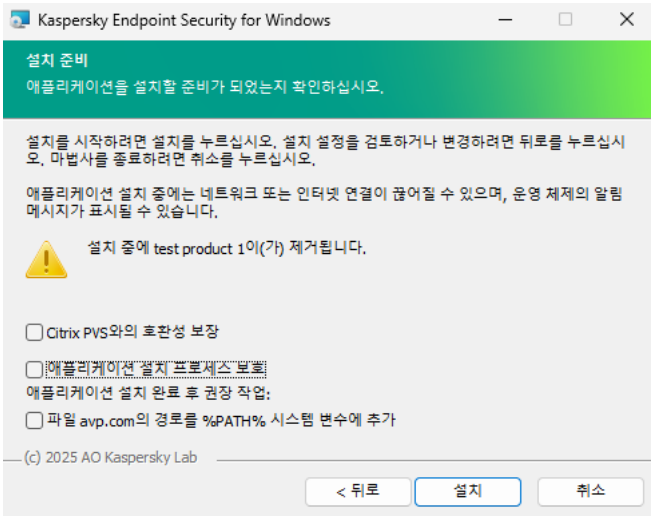


애플리케이션 구성 선택

Endpoint Detection and Response Agent 구성을 선택합니다. 이 구성에서는 Detection and Response 솔루션을 지원하는 구성 요소만 설치할 수 있습니다. MDR, EDR(KATA), NDR(KATA), EDR Expert(on-premise) 및 KUMA. 조직에 타사 Endpoint Protection Platform(EPP)가 Kaspersky Detection and Response 솔루션과 함께 설치된 경우 이 구성이 필요합니다. 이를 통해 Endpoint Detection and Response Agent 구성의 Kaspersky Endpoint Security가 타사 EPP 애플리케이션과 호환됩니다.

Kaspersky Endpoint Security 구성 요소

설치할 구성 요소를 선택합니다. 애플리케이션을 설치한 후 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다. 이렇게 하려면 설정 마법사를 다시 실행하고 사용 가능한 구성 요소를 변경하도록 선택해야 합니다.



고급 애플리케이션 설치 설정

애플리케이션 설치 프로세스 보호. 설치 보호는 악성 애플리케이션에 의한 배포 패키지 변조 차단, Kaspersky Endpoint Security 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.

Citrix PVS와의 호환성 보장. 가상 컴퓨터에 Kaspersky Endpoint Security를 설치하기 위해 Citrix Provisioning Services 지원을 작동할 수 있습니다.

시스템 변수 %PATH%에 avp.com 파일 경로 추가. 명령줄 인터페이스를 편리하게 사용할 수 있도록 %PATH% 변수에 설치 경로를 추가할 수 있습니다.

명령줄에 EDR Agent를 설치하는 방법(KATA(EDR) 및 EDR Expert(on-premise)만 해당)

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 배포 패키지가 있는 폴더로 이동합니다.
3. 다음 명령을 실행합니다:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
```

또는

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

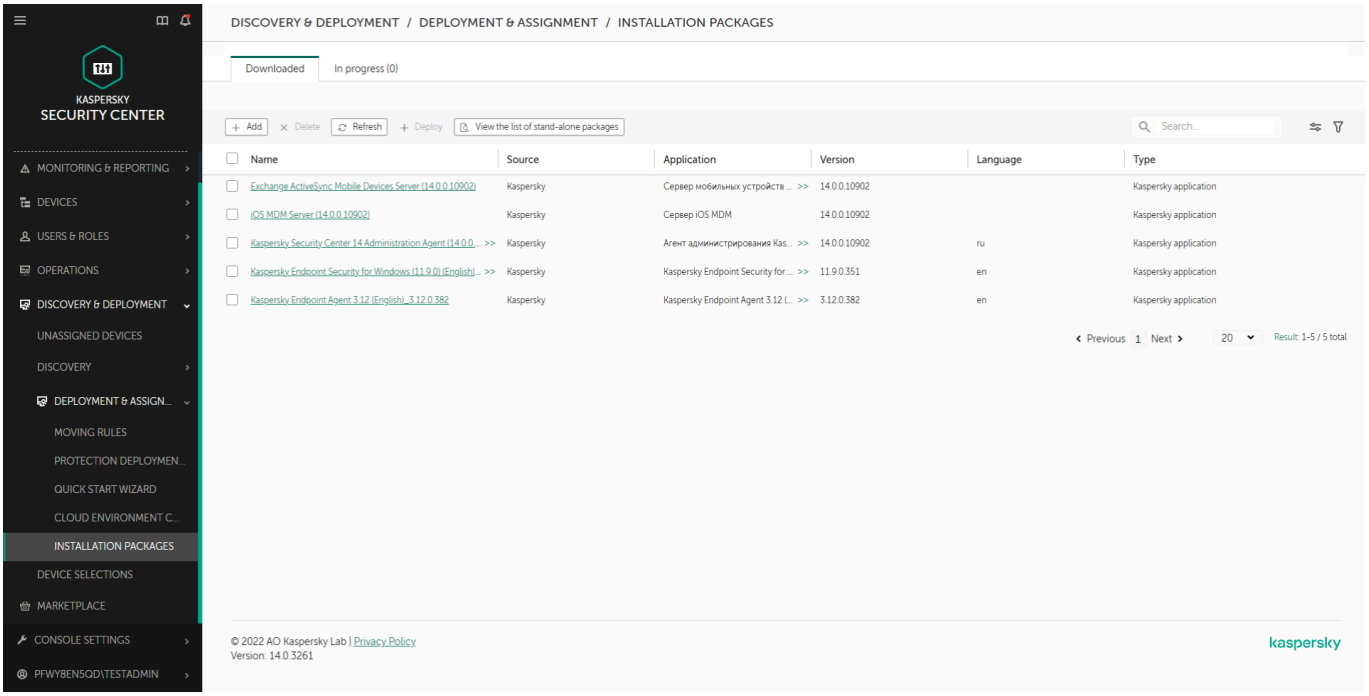
결과적으로 Kaspersky Anti Targeted Attack Platform(EDR) 또는 Kaspersky Endpoint Detection and Response Expert(on-premise)와 통합하기 위한 EDR Agent 애플리케이션이 컴퓨터에 설치됩니다. `status` 명령을 사용하여 애플리케이션이 설치되었는지 확인하고 애플리케이션 설정을 확인할 수 있습니다.

관리 콘솔(MMC)을 사용하여 EDR Agent를 설치하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔에서 **고급** → **원격 설치** → **설치 패키지** 폴더를 선택합니다.
   Kaspersky Security Center로 다운로드한 설치 패키지 목록이 열립니다.
3. 설치 패키지의 속성을 여십시오.
   필요한 경우, 새 설치 패키지 만들기를 실행하십시오.
4. **보호 구성 요소** 섹션으로 이동합니다.
5. **지능형 위협 및 표적형 공격으로부터 보호하는 Endpoint Detection and Response Agent**를 선택합니다. 이 구성에서는 Detection and Response 솔루션을 지원하는 구성 요소만 설치할 수 있습니다. MDR, EDR(KATA), NDR(KATA), EDR Expert(on-premise) 및 KUMA. 조직에 타사 Endpoint Protection Platform(EPP)가 Kaspersky Detection and Response 솔루션과 함께 설치된 경우 이 구성이 필요합니다. 이를 통해 Endpoint Detection and Response Agent 구성의 Kaspersky Endpoint Security가 타사 EPP 애플리케이션과 호환됩니다.
6. 설치할 구성 요소를 선택합니다.
   애플리케이션을 설치한 후 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다.
7. 변경 사항을 저장합니다.
8. 원격 설치 작업 생성. 작업 속성에서 생성한 설치 패키지를 선택합니다.

웹 콘솔을 사용하여 EDR Agent를 설치하는 방법

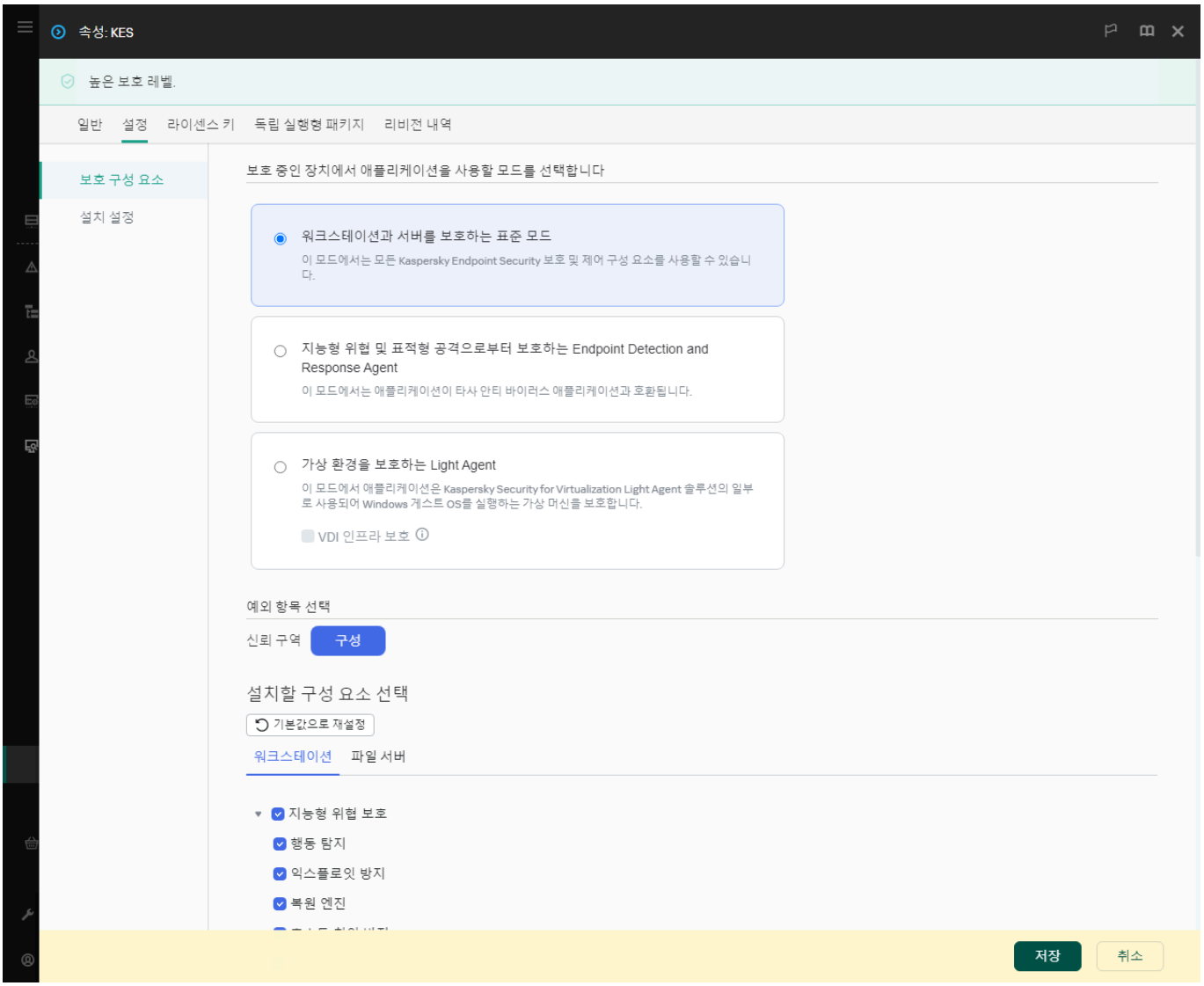
1. 웹 콘솔의 메인 창에서 **발견 및 배포** → **배포 및 할당** → **설치 패키지**를 클릭합니다.
   Kaspersky Security Center로 다운로드한 설치 패키지 목록이 열립니다.



설치 패키지 목록

2. 설치 패키지의 속성을 여십시오.
   필요한 경우, 새 설치 패키지 만들기를 실행하십시오.
3. **설정** 탭을 선택합니다.

4. **보호 구성 요소** 섹션으로 이동합니다.



설치 패키지에 포함된 구성 요소

5. **지능형 위협 및 표적형 공격으로부터 보호하는 Endpoint Detection and Response Agent**를 선택합니다. 이 구성에서는 Detection and Response 솔루션을 지원하는 구성 요소만 설치할 수 있습니다. MDR, EDR(KATA), NDR(KATA), EDR Expert(on-premise) 및 KUMA. 조직에 타사 Endpoint Protection Platform(EPP)가 Kaspersky Detection and Response 솔루션과 함께 설치된 경우 이 구성이 필요합니다. 이를 통해 Endpoint Detection and Response Agent 구성의 Kaspersky Endpoint Security가 타사 EPP 애플리케이션과 호환됩니다.

6. 설치할 구성 요소를 선택합니다.

   애플리케이션을 설치한 후 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다.

7. 변경 사항을 저장합니다.

8. 원격 설치 작업 생성. 작업 속성에서 생성한 설치 패키지를 선택합니다.

결과적으로 EDR Agent가 사용자 컴퓨터에 설치됩니다. 애플리케이션의 인터페이스를 사용할 수 있으며 알림 영역에 애플리케이션 아이콘이 표시됩니다.

Kaspersky Security Center에서 EDR Agent의 애플리케이션이 설치된 컴퓨터에는 *심각* 상태()가 표시됩니다. 파일 위협 보호 구성 요소가 없기 때문에 컴퓨터에 이러한 상태가 표시됩니다. 별도의 조치를 취할 필요가 없습니다.

설치 프로그램이 타사 EPP 응용 프로그램이 있는 컴퓨터에서 호환되지 않는 소프트웨어를 발견하여 EDR Agent를 설치할 수 없는 경우 호환되지 않는 소프트웨어 검사 건너뛰기를 진행하십시오.



EDR Agent 메인 창

이제 Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack(EDR) 또는 Kaspersky Anti Targeted Attack(NDR) 솔루션과 통합해야 합니다. 또한 신뢰 구역 생성 또는 애플리케이션의 인터페이스 숨기기 등 애플리케이션의 고급 설정을 지정할 수 있습니다. 다음 섹션의 설정을 사용할 수 있습니다.

- Kaspersky Security Network
- 애플리케이션 설정
- 네트워크 설정
- 예외 규칙
- 리포트

- 인터페이스
- 설정 관리

EDR Agent를 MDR과 통합

EDR Agent는 조직의 IT 인프라에 있는 워크스테이션과 서버에 설치됩니다. EDR Agent는 데이터를 처리하여 Kaspersky Security Network 스트림을 통해 Kaspersky Managed Detection and Response로 보냅니다.

Kaspersky Managed Detection and Response가 Kaspersky Security Center 웹 콘솔을 통해 관리 서버를 사용하려면 새로운 보안 연결인 *백그라운드 연결*을 구성해야 합니다. 솔루션 배포 시 Kaspersky Managed Detection and Response가 백그라운드 연결을 구성할 것인지 묻는 메시지를 표시합니다. 백그라운드 연결을 구성해야 합니다.

웹 콘솔에서 백그라운드 연결 구성

1. 웹 콘솔의 메인 창에서 **설정** → **통합**을 선택합니다.
2. **통합** 섹션으로 이동합니다.
3. **통합을 위한 백그라운드 연결 [활성화됨]** 토글을 켭니다.
4. 변경 사항을 저장합니다.

Kaspersky Managed Detection and Response와의 통합은 다음 단계로 구성됩니다:

1. **Managed Detection and Response 구성 요소 설치**

   MDR 구성 요소는 설치 또는 업그레이드 중 선택하거나 *애플리케이션 구성 요소 변경* 작업으로 선택할 수 있습니다.

   > 새 구성 요소로 애플리케이션 업그레이드를 완료하려면 컴퓨터를 다시 시작해야 합니다.

2. **Kaspersky Private Security Network**

   > Kaspersky Security Center Cloud Console을 사용한다면 이 단계를 건너뜁니다. Kaspersky Security Center Cloud Console은 MDR 플러그인 설치 시 자동으로 Kaspersky Private Security Network를 구성합니다.

   *Kaspersky Private Security Network(KPSN)*는 Kaspersky Endpoint Security 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.

   중앙 관리 서버 속성에 Kaspersky Security Network 구성 파일을 업로드합니다. Kaspersky Security Network 구성 파일은 MDR 구성 파일의 ZIP 압축파일 내에 있습니다. Kaspersky Managed Detection and Response 콘솔에서 ZIP 압축파일을 얻을 수 있습니다. Kaspersky Private Security Network 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말 을 참조하십시오. 명령줄에서 Kaspersky Security Network 구성 파일을 컴퓨터에 업로드할 수도 있습니다(아래 지침 참조).

   명령줄에서 Kaspersky Private Security Network를 구성하는 방법

   1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
   2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

3. 다음 명령을 실행합니다:

```
avp.com KSN /private <file name>
```

`<file name>`은 Kaspersky Private Security Network 설정(PKCS7 또는 PEM 파일 형식)을 포함하는 구성 파일의 이름입니다.

예:
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

결과적으로 Kaspersky Endpoint Security는 Kaspersky Private Security Network을 사용하여 파일, 애플리케이션 및 웹사이트의 평판을 결정합니다. 정책 설정의 **Kaspersky Security Network** 섹션에는 다음 작동 상태가 표시됩니다: *인프라:`Kaspersky Private Security Network*.

Managed Detection and Response가 작동하려면 확장 KSN 모드를 사용해야 합니다.

3 Kaspersky Managed Detection and Response 활성화

Kaspersky Endpoint Security for Windows 12.10부터 Managed Detection and Response 기능 활성화에 활성화 코드 대신 키 파일을 사용할 수도 있습니다.

MDR(Kaspersky Managed Detection and Response 애드온) 사용을 위해 별도 라이센스 구매해야 합니다.

이 기능은 Kaspersky Managed Detection and Response 애드온의 키를 별도로 추가한 후에 이용할 수 있습니다. 독립 실행형 Managed Detection and Response 기능의 라이센스 사용은 Kaspersky Endpoint Security의 라이센스 사용과 같습니다.

MDR 기능이 라이센스에 포함되며 애플리케이션의 로컬 인터페이스에서 실행되고 있는지 확인하십시오.

4 Managed Detection and Response 구성 요소 활성화

Kaspersky Endpoint Security 정책에서 BLOB 구성 파일을 로드합니다(아래 지침 참조). BLOB 파일에는 클라이언트 ID와 Kaspersky Managed Detection and Response 라이센스에 대한 정보가 포함되어 있습니다. BLOB 파일은 MDR 구성 파일의 ZIP 압축파일 안에 있습니다. Kaspersky Managed Detection and Response 콘솔에서 ZIP 압축파일을 얻을 수 있습니다. BLOB 파일에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

현재 라이센스가 있는 경우 Kaspersky Endpoint Security 12.6 for Windows부터 테넌트가 없는 Kaspersky Managed Detection and Response에 대해 BLOB 파일을 추가하는 것은 선택사항입니다.

관리 콘솔(MMC)에서 Managed Detection and Response 구성 요소를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **Detection and Response → Managed Detection and Response(Industrial CyberSecurity)**를 선택합니다.
4. **Managed Detection and Response(Industrial CyberSecurity)** 확인란을 선택합니다.

5. **설정** 블록에서 **업로드**를 클릭하고 Kaspersky Managed Detection and Response 콘솔에서 받은 BLOB 파일을 선택합니다. 파일의 확장자는 P7입니다.

   기본적으로 사용자는 애플리케이션 설정을 관리할 수 있습니다("자물쇠" 열림). 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다 .

6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 Managed Detection and Response 구성 요소를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Managed Detection and Response**로 갑니다.
5. **Managed Detection and Response 활성화됨** 토글을 켭니다.
6. **업로드**를 클릭하고 Kaspersky Managed Detection and Response 콘솔에서 얻은 BLOB 파일을 선택합니다. 파일의 확장자는 P7입니다.

   기본적으로 사용자는 정책 설정을 관리할 수 있습니다("자물쇠" 열림). 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다 .

7. 변경 사항을 저장합니다.

명령줄에서 Managed Detection and Response 구성 요소를 활성화하는 방법

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.
3. 다음 명령을 실행합니다:

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

   이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다. 해당 사용자에게 **애플리케이션 설정 구성** 권한이 있어야 합니다.

결과적으로 Kaspersky Endpoint Security에서 BLOB 파일을 확인합니다. BLOB 파일 확인에는 디지털 서명 및 라이센스 기간 확인이 포함됩니다. BLOB 파일을 성공적으로 확인하면 Kaspersky Endpoint Security는 다음번에 Kaspersky Security Center와 동기화하는 동안 파일을 다운로드하고 파일을 컴퓨터로 보냅니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Managed Detection and Response** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

5 **원격 측정을 수신하도록 애플리케이션의 다른 구성 요소 구성**

Managed Detection and Response가 작동하려면 다음 구성 요소를 활성화해야 합니다.

- Kaspersky Security Network(확장 모드)
- 행동 탐지
- 익스플로잇 방지
- 웹 위협 보호
- 메일 위협 보호
- 파일 위협 보호
- 네트워크 위협 보호.
- 방화벽
- AMSI 보호.
- 백그라운드 검사.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Managed Detection and Response**로 갑니다.
5. **Managed Detection and Response 활성화됨** 토글을 켭니다.
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 창에서 **Detection and Response** → **Managed Detection and Response(Industrial CyberSecurity)**를 선택합니다.
4. **Managed Detection and Response(Industrial CyberSecurity)** 확인란을 선택합니다.
5. 변경 사항을 저장합니다.

EDR Agent를 EDR(KATA)와 통합

EDR Agent는 조직의 IT 인프라에 있는 워크스테이션과 서버에 설치됩니다. 이러한 컴퓨터에서 EDR Agent는 프로세스, 개방형 네트워크 연결 및 수정 중인 파일을 지속적으로 모니터링하고 Central Node 구성 요소를 사용하여 해당 데이터를 서버로 보냅니다.

EDR(KATA)과 통합하려면 Endpoint Detection and Response(KATA) 구성 요소를 활성화하고 EDR Agent 구성을 허용해야 합니다.

Endpoint Detection and Response(KATA)의 작동을 위해서는 다음 조건을 만족해야 합니다:

- Kaspersky Anti Targeted Attack Platform 버전 5.0~7.1.
- Kaspersky Security Center 버전 14.2 이상. 이전 버전의 Kaspersky Security Center에서는 Endpoint Detection and Response(KATA)의 기능을 활성화할 수 없습니다.

https://www.youtube.com/watch?v=cZzgtBoeC7k

Endpoint Detection and Response(KATA)와의 통합은 다음 단계를 포함합니다:

1. **Endpoint Detection and Response(KATA) 활성화**

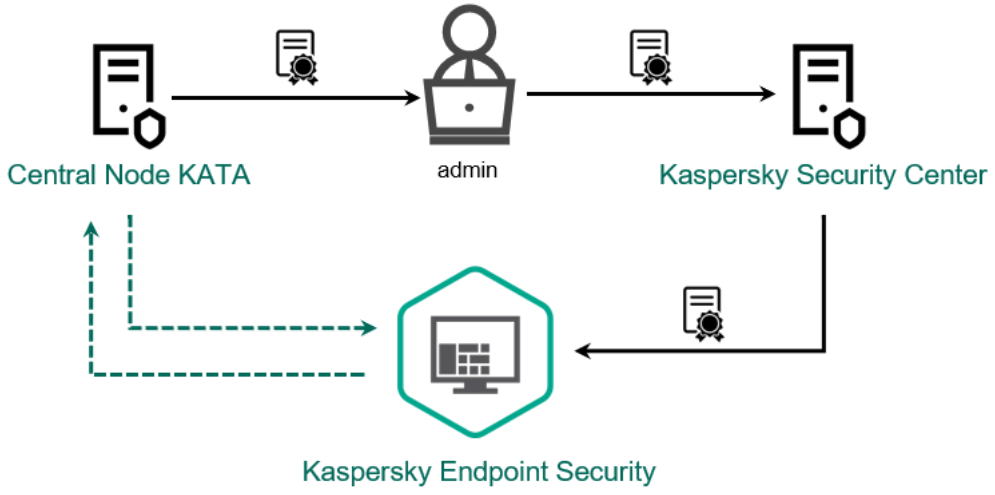
   EDR(KATA)(Kaspersky Endpoint Detection and Response(KATA) 애드온) 사용을 위해 별도 라이센스 구매해야 합니다.

   이 기능은 Kaspersky Endpoint Detection and Response(KATA)의 키를 별도로 추가한 후에 이용할 수 있습니다. 독립 실행형 Endpoint Detection and Response(KATA) 기능의 라이센스 사용은 Kaspersky Endpoint Security의 라이센스 사용과 같습니다.

   EDR(KATA) 기능이 라이센스에 포함되며 애플리케이션의 로컬 인터페이스에서 실행되고 있는지 확인하십시오.

2. **Central Node에 연결**

   Kaspersky Anti Targeted Attack Platform에서는 Kaspersky Endpoint Security와 Central Node 구성 요소 간에 신뢰할 수 있는 연결을 설정해야 합니다. 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 Endpoint Security에 TLS 인증서를 추가해야 합니다(아래 지침 참조).



Kaspersky Endpoint Security에 TLS 인증서 추가

기본적으로 Kaspersky Endpoint Security는 Central Node의 TLS 인증서만 확인합니다. 보다 안전한 연결을 위해, Central Node에서 컴퓨터 확인을 추가로 활성화할 수 있습니다(양방향 인증). 이 확인을 활성화하려면 Central Node와 Kaspersky Endpoint Security 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).

관리 콘솔(MMC)을 사용하여 Kaspersky Endpoint Security 컴퓨터를 Central Node에 연결하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **Detection and Response → Endpoint Detection and Response Expert(on premise)**를 선택합니다.
5. **Endpoint Detection and Response Expert(on premise)** 확인란을 선택합니다.
6. **서버 연결 설정**을 클릭합니다.
7. 서버 연결 구성:
   - **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 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 Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 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.
8. **확인**을 누릅니다.
9. Central Node 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.

   여러 개의 Central Node 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.
10. 필요한 경우 원격 측정을 구성합니다.
11. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔을 사용하여 Kaspersky Endpoint Security 컴퓨터를 Central Node에 연결하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Endpoint Detection and Response Expert(on premise)**로 갑니다.
5. **Endpoint Detection and Response Expert(on-premise) 활성화됨** 토글을 켭니다.
6. EDR(KATA)을 구성하려면 솔루션 목록에서 **Endpoint Detection and Response Expert(버전 7.1 이하)**를 선택합니다.
7. **연결 설정**을 클릭합니다.
8. 서버 연결 구성:
   - **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 Central Node 서버에 연결을 시도합니다.
   - **서버 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 Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 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.
9. **확인**을 누릅니다.
10. Central Node 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.
    여러 개의 Central Node 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.
11. 필요한 경우 원격 측정을 구성합니다.
12. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

결과적으로 컴퓨터가 Kaspersky Anti Targeted Attack Platform 콘솔에 추가됩니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Endpoint Detection and Response Expert(on-premise)** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

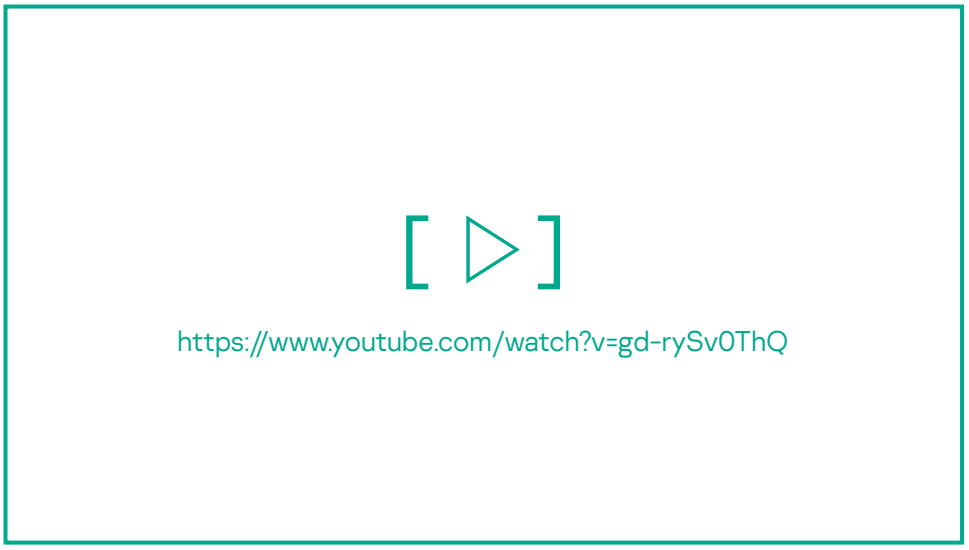
EDR Agent를 NDR(KATA)와 통합

EDR Agent는 조직의 IT 인프라에 있는 워크스테이션과 서버에 설치됩니다. 이러한 컴퓨터에서 EDR Agent는 프로세스, 개방형 네트워크 연결 및 수정 중인 파일을 지속적으로 모니터링하고 Central Node 구성 요소를 사용하여 해당 데이터를 서버로 보냅니다.

NDR(KATA)과 통합하려면 Network Detection and Response(KATA) 구성 요소를 활성화하고 EDR Agent 구성을 허용해야 합니다.

Network Detection and Response(KATA)의 작동을 위해서는 다음 조건을 만족해야 합니다:

- Kaspersky Anti Targeted Attack Platform 버전 7.0 이상.
- Kaspersky Security Center 버전 14.2 이상. 이전 버전의 Kaspersky Security Center에서는 Network Detection and Response(KATA)의 기능을 활성화할 수 없습니다.



https://www.youtube.com/watch?v=gd-rySv0ThQ

Network Detection and Response(KATA)와의 통합은 다음 단계를 포함합니다:

1. **Network Detection and Response(KATA) 활성화**

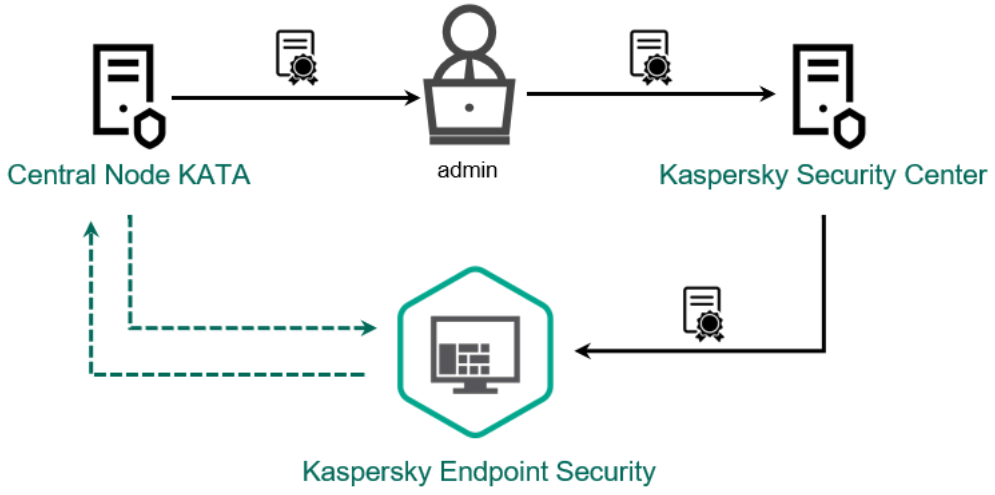
   NDR(KATA)(Kaspersky Network Detection and Response(KATA) 애드온) 사용을 위해 별도 라이센스 구매해야 합니다.

   이 기능은 Kaspersky Network Detection and Response(KATA)의 키를 별도로 추가한 후에 이용할 수 있습니다. 독립 실행형 Network Detection and Response(KATA) 기능의 라이센스 사용은 Kaspersky Endpoint Security의 라이센스 사용과 같습니다.

   NDR(KATA) 기능이 라이센스에 포함되며 애플리케이션의 로컬 인터페이스에서 실행되고 있는지 확인하십시오.

2. **Central Node에 연결**

Kaspersky Anti Targeted Attack Platform에서는 Kaspersky Endpoint Security와 Central Node 구성 요소 간에 신뢰할 수 있는 연결을 설정해야 합니다. 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 Endpoint Security에 TLS 인증서를 추가해야 합니다(아래 지침 참조).



Kaspersky Endpoint Security에 TLS 인증서 추가

기본적으로 Kaspersky Endpoint Security는 Central Node의 TLS 인증서만 확인합니다. 보다 안전한 연결을 위해, Central Node에서 컴퓨터 확인을 추가로 활성화할 수 있습니다(양방향 인증). 이 확인을 활성화하려면 Central Node와 Kaspersky Endpoint Security 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).

관리 콘솔(MMC)을 사용하여 Kaspersky Endpoint Security 컴퓨터를 Central Node에 연결하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **Detection and Response → Network Detection and Response(KATA)**를 선택합니다.
4. **Network Detection and Response(KATA)** 확인란을 선택합니다.
5. **연결 설정**을 클릭합니다.
6. 서버 연결 구성:
   - **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 Central Node 서버에 연결을 시도합니다.
   - **서버 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 Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 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.

7. **확인**을 누릅니다.
8. Central Node 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.
9. 여러 개의 Central Node 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.
10. 필요한 경우 원격 측정을 구성합니다.
11. 변경 사항을 저장합니다.

웹 콘솔을 사용하여 Kaspersky Endpoint Security 컴퓨터를 Central Node에 연결하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Network Detection and Response(KATA)**로 갑니다.
5. **Network Detection and Response(KATA) 활성화됨** 토글을 켭니다.
6. **연결 설정**을 클릭합니다.
7. 서버 연결 구성:

   - **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 Central Node 서버에 연결을 시도합니다.
   - **서버 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 Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 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.

8. **확인**을 누릅니다.
9. Central Node 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.
10. 여러 개의 Central Node 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.
11. 필요한 경우 원격 측정을 구성합니다.
12. 변경 사항을 저장합니다.

결과적으로 컴퓨터가 Kaspersky Anti Targeted Attack Platform 콘솔에 추가됩니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Network Detection and Response(KATA)** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

EDR Agent를 EDR Expert(on-premise)와 통합

EDR Agent는 조직의 IT 인프라에 있는 워크스테이션과 서버에 설치됩니다. 이러한 컴퓨터에서 EDR Agent는 프로세스, 개방형 네트워크 연결 및 수정 중인 파일을 지속적으로 모니터링하고 모니터링 데이터를 EDR Expert(on-premise) 서버로 보냅니다.

EDR Expert(on-premise)과 통합하려면 Endpoint Detection and Response Expert(on-premise) 구성 요소를 활성화하고 EDR Agent 구성을 허용해야 합니다.

Endpoint Detection and Response Expert(on-premise)와의 통합은 다음 단계를 포함합니다:

1. **Kaspersky Endpoint Detection and Response Expert(on-premise) 활성화**

   EDR Expert(on-premise)(Kaspersky Endpoint Detection and Response(on-premise) 애드온) 사용을 위해 별도 라이센스 구매해야 합니다.

   이 기능은 Kaspersky Endpoint Detection and Response Expert(on premise)의 키를 별도로 추가한 후에 이용할 수 있습니다. 독립 실행형 Endpoint Detection and Response(KATA) 기능의 라이센스 사용은 Kaspersky Endpoint Security의 라이센스 사용과 같습니다.

   EDR Expert(on-premise) 기능이 라이센스에 포함되며 애플리케이션의 로컬 인터페이스에서 실행되고 있는지 확인하십시오.

2. **원격 측정 수집 서버 및 응답 서버에 연결**

Kaspersky Endpoint Detection and Response Expert(on-premise)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 얻을 수 있습니다(Kaspersky Endpoint Detection and Response Expert(on-premise) 도움말의 지침 참조). 그런 다음 Kaspersky Endpoint Security에 TLS 인증서를 추가해야 합니다(아래 지침 참조).

기본적으로 Kaspersky Endpoint Security는 서버의 TLS 인증서만 확인합니다. 보다 안전한 연결을 위해, 서버에서 컴퓨터 확인을 추가로 활성화할 수 있습니다(양방향 인증). 이 확인을 활성화하려면 서버와 Kaspersky Endpoint Security 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 얻을 수 있습니다(Kaspersky Endpoint Detection and Response Expert(on-premise) 도움말의 지침 참조).

웹 콘솔을 사용하여 Kaspersky Endpoint Security 컴퓨터를 EDR Expert(on-premise)에 연결하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Endpoint Detection and Response Expert(on premise)**로 갑니다.
5. **Endpoint Detection and Response Expert(on-premise) 활성화됨** 토글을 켭니다.
6. EDR Expert(on-premise)을 구성하려면 솔루션 목록에서 **Endpoint Detection and Response Expert(버전 8.0 이상)**를 선택합니다.
7. *원격 측정 수집 서버* 연결을 구성합니다.

   a. **원격 측정 수집 서버에 연결** 블록에서 **연결 설정** 링크를 클릭합니다.

   b. 원격 측정 수집 서버 연결을 구성합니다.

   - **시간 초과(초)**. 최대 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 서버에 연결을 시도합니다.
   - **서버 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-premise) 도움말의 지침 참조).

- **양방향 인증 사용**. Kaspersky Endpoint Security와 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-premise) 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.

c. **확인**을 누릅니다.

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 Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

e. 필요한 경우 원격 측정을 구성합니다.

8. *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 Endpoint Security가 보안 위협 대응 작업을 수신하고 작업 결과를 전송합니다.

b. **연결 설정** 링크를 클릭합니다.

c. 응답 서버 연결 구성:

- **시간 초과(초)**. 최대 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 서버에 연결을 시도합니다.

- **서버 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-premise) 도움말의 지침 참조).

- **양방향 인증 사용**. Kaspersky Endpoint Security와 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-premise) 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**을 누릅니다.

e. 응답 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.

여러 개의 대응 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

9. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

그러면 컴퓨터가 Open Single Management Platform(OSMP)에 추가됩니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Endpoint Detection and Response Expert(on-premise)** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

타사 EPP 애플리케이션과의 호환성

EDR Agent는 Kaspersky Detection and Response 솔루션 기능을 지원합니다. EDR Agent는 보호 및 제어 구성 요소를 사용할 수 없습니다. 이 구성을 사용하면 조직의 인프라에 타사 EPP 애플리케이션을 설치하고 Kaspersky Detection and Response 솔루션을 배포할 수 있습니다. EDR Agent는 Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack Platform(EDR) 및 Kaspersky Anti Targeted Attack Platform(NDR) 작업을 지원합니다.

EDR Agent는 다음 공급업체의 EPP 애플리케이션과 호환됩니다.

- **Dr.Web**

  EDR Agent는 Dr.Web Agent for Windows 버전 13.0.1 이상 및 Dr.Web Server(x64) 13.0.0.10200과 호환됩니다.

- **Dallas Lock**

  EDR Agent는 Dallas Lock 8.0-C 버전 11.4.2.843 이상과 호환됩니다.

  > Dallas Lock 소프트웨어가 설치된 컴퓨터에서 EDR Agent를 실행하려면 방화벽 모듈 설정에서 Kaspersky 외부 서비스에 연결을 허용해야 합니다.

- **Secret Net Studio**

  EDR Agent는 Secret Net Studio 버전 8.11 이상과 호환됩니다.

  > 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.

- **Trend Micro**

  EDR Agent는 Trend Micro Apex One 버전 14.0.12994 이상(Security Agent 포함)과 호환됩니다.

  EDR Agent는 Trend Micro Deep Security 버전 20.0.2-4960 이상(Security Agent 포함)과 호환됩니다.

- **Windows Defender**

- **Sophos**

  EDR Agent는 Sophos Intercept X 버전 2024.1.2 이상(Endpoint Agent 포함) 및 Sophos Core Agent 버전 2024.3.2.3 이상과 호환됩니다.

- **Bitdefender**

  EDR Agent는 Bitdefender Endpoint Security Tools 버전 7.9.21.523 이상과 호환됩니다.

- **ESET**

  EDR Agent는 ESET Endpoint Security 버전 12.0.2049.0 이상 및 ESET Management Agent 버전 12.0 이상과 호환됩니다.

Windows 11 for Arm64를 실행하는 컴퓨터에서는 EDR 에이전트가 Bitdefender Endpoint Security Tools과 호환되지 않습니다.

애플리케이션은 꼭 다음의 순서대로 설치해야 합니다. 먼저 EPP 애플리케이션을 설치한 다음 Kaspersky Security Center 네트워크 에이전트를 설치하고 마지막으로 EDR Agent를 설치합니다. 이 과정이 필요한 이유는 EPP 애플리케이션 설치 프로그램이 EDR Agent 및 네트워크 에이전트를 호환되지 않는 소프트웨어로 감지하여 제거할 수 있기 때문입니다. 타사 EPP 응용 프로그램을 업데이트한 후, EDR Agent 및 네트워크 에이전트가 제대로 작동하는지 확인해야 합니다. 해당 설치 프로그램이 컴퓨터에서 호환되지 않는 소프트웨어를 다시 검사하여 애플리케이션을 제거할 수 있기 때문입니다.

설치 프로그램이 타사 EPP 응용 프로그램이 있는 컴퓨터에서 호환되지 않는 소프트웨어를 발견하여 EDR Agent를 설치할 수 없는 경우 호환되지 않는 소프트웨어 검사 건너뛰기를 진행하십시오.

Managed Detection and Response



Kaspersky Endpoint Security for Windows는 Managed Detection and Response 솔루션과의 통합을 지원합니다. *Kaspersky Managed Detection and Response(MDR)* 솔루션은 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. 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 도움말 을 참조하십시오.

MDR과 통합하기 위한 Kaspersky Endpoint Security 구성

MDR 작업에는 다음 구성을 사용할 수 있습니다.

- **[KES+내장 에이전트]**. 이 구성에서 Kaspersky Endpoint Security는 컴퓨터 보안을 책임지는 애플리케이션이자 MDR 작업을 위한 애플리케이션으로서 작동합니다. 내장 에이전트는 Kaspersky Endpoint Security 11.6.0 for Windows 이상의 버전에서 사용할 수 있습니다.

- **[타사 EPP+EDR Agent]**. 이 구성에서는 타사 EPP(Endpoint Protection Platform)를 통해 IT 인프라 보안이 제공됩니다. Endpoint Detection and Response Agent(EDR Agent)의 Kaspersky Endpoint Security에서 MDR과의 상호 작용을 지원합니다. 이 구성에서 EDR Agent는 타사 EPP 애플리케이션과 호환됩니다. EDR Agent는 Kaspersky Endpoint Security 12.3 for Windows 이상의 버전에서 사용할 수 있습니다.

이전 버전의 Kaspersky Endpoint Security 지원

Kaspersky Endpoint Security 버전 11 이상은 MDR 솔루션을 지원합니다. Kaspersky Endpoint Security 버전 11~11.5.0는 보안위협 탐지 활성화를 위해 Kaspersky Managed Detection and Response에 원격 측정 데이터만을 전송합니다. Kaspersky Endpoint Security 버전 11.6.0은 내장 에이전트의 모든 기능이 있습니다(Kaspersky Endpoint Agent).

Kaspersky Endpoint Security 11~11.5.0을 사용한다면 MDR 솔루션 사용을 위해 데이터베이스를 최신 버전으로 업데이트해야 합니다. Kaspersky Endpoint Agent도 설치해야 합니다.

Kaspersky Endpoint Security 11.6.0 이상을 사용 시, MDR 솔루션 사용을 위해 Kaspersky Endpoint Agent를 설치할 필요가 없습니다.

Kaspersky Endpoint Security 정책이 Kaspersky Endpoint Security 11~11.5.0가 설치되어 있지 않은 컴퓨터에도 적용된다면, 먼저 해당 컴퓨터에 대한 별도의 Kaspersky Endpoint Agent 정책을 생성해야 합니다. 새 정책에서 Kaspersky Managed Detection and Response와의 통합을 구성합니다.

MDR과 내장 에이전트 통합

Kaspersky Managed Detection and Response와의 통합을 설정하려면 Managed Detection and Response 구성 요소를 활성화하고 Kaspersky Endpoint Security를 구성해야 합니다.

Kaspersky Managed Detection and Response가 Kaspersky Security Center 웹 콘솔을 통해 관리 서버를 사용하려면 새로운 보안 연결인 *백그라운드 연결*을 구성해야 합니다. 솔루션 배포 시 Kaspersky Managed Detection and Response가 백그라운드 연결을 구성할 것인지 묻는 메시지를 표시합니다. 백그라운드 연결을 구성해야 합니다.

웹 콘솔에서 백그라운드 연결 구성

1. 웹 콘솔의 메인 창에서 **설정** → **통합**을 선택합니다.
2. **통합** 섹션으로 이동합니다.
3. **통합을 위한 백그라운드 연결 [활성화됨]** 토글을 켭니다.
4. 변경 사항을 저장합니다.

Kaspersky Managed Detection and Response와의 통합은 다음 단계로 구성됩니다:

1. **Managed Detection and Response 구성 요소 설치**

   MDR 구성 요소는 설치 또는 업그레이드 중 선택하거나 *애플리케이션 구성 요소 변경* 작업으로 선택할 수 있습니다.

   새 구성 요소로 애플리케이션 업그레이드를 완료하려면 컴퓨터를 다시 시작해야 합니다.

2. **Kaspersky Private Security Network**

   Kaspersky Security Center Cloud Console을 사용한다면 이 단계를 건너뜁니다. Kaspersky Security Center Cloud Console은 MDR 플러그인 설치 시 자동으로 Kaspersky Private Security Network를 구성합니다.

   *Kaspersky Private Security Network(KPSN)*는 Kaspersky Endpoint Security 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.

   중앙 관리 서버 속성에 Kaspersky Security Network 구성 파일을 업로드합니다. Kaspersky Security Network 구성 파일은 MDR 구성 파일의 ZIP 압축파일 내에 있습니다. Kaspersky Managed Detection and Response 콘솔에서 ZIP 압축파일을 얻을 수 있습니다. Kaspersky Private Security Network 구성에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오. 명령줄에서 Kaspersky Security Network 구성 파일을 컴퓨터에 업로드할 수도 있습니다(아래 지침 참조).

명령줄에서 Kaspersky Private Security Network를 구성하는 방법

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.
3. 다음 명령을 실행합니다:

```
avp.com KSN /private <file name>
```

`<file name>`은 Kaspersky Private Security Network 설정(PKCS7 또는 PEM 파일 형식)을 포함하는 구성 파일의 이름입니다.

예:
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

결과적으로 Kaspersky Endpoint Security는 Kaspersky Private Security Network을 사용하여 파일, 애플리케이션 및 웹사이트의 평판을 결정합니다. 정책 설정의 **Kaspersky Security Network** 섹션에는 다음 작동 상태가 표시됩니다: *인프라:`Kaspersky Private Security Network*.

Managed Detection and Response가 작동하려면 확장 KSN 모드를 사용해야 합니다.

3 Kaspersky Managed Detection and Response 활성화

Kaspersky Endpoint Security for Windows 12.10부터 Managed Detection and Response 기능 활성화에 활성화 코드 대신 키 파일을 사용할 수도 있습니다.

Kaspersky Managed Detection and Response는 다음 라이센스 방법을 지원합니다.

- Managed Detection and Response 기능은 Kaspersky Endpoint Security for Windows 라이센스에 포함되어 있습니다.

  이 기능은 Kaspersky Endpoint Security for Windows 활성화 직후 바로 사용할 수 있습니다.

- MDR(Kaspersky Managed Detection and Response 애드온)은 별도의 라이센스가 사용됩니다.

  이 기능은 Kaspersky Managed Detection and Response 애드온의 키를 별도로 추가한 후에 이용할 수 있습니다. 결과적으로 Kaspersky Endpoint Security 키와 Kaspersky Managed Detection and Response 두 개의 키가 컴퓨터에 설치됩니다.

  독립 실행형 Managed Detection and Response 기능의 라이센스 사용은 Kaspersky Endpoint Security의 라이센스 사용과 같습니다.

MDR 기능이 라이센스에 포함되며 애플리케이션의 로컬 인터페이스에서 실행되고 있는지 확인하십시오.

4 Managed Detection and Response 구성 요소 활성화

Kaspersky Endpoint Security 정책에서 BLOB 구성 파일을 로드합니다(아래 지침 참조). BLOB 파일에는 클라이언트 ID와 Kaspersky Managed Detection and Response 라이센스에 대한 정보가 포함되어 있습니다. BLOB 파일은 MDR 구성 파일의 ZIP 압축파일 안에 있습니다. Kaspersky Managed Detection and Response 콘솔에서 ZIP 압축파일을 얻을 수 있습니다. BLOB 파일에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

현재 라이센스가 있는 경우 Kaspersky Endpoint Security 12.6 for Windows부터 테넌트가 없는 Kaspersky Managed Detection and Response에 대해 BLOB 파일을 추가하는 것은 선택사항입니다.

관리 콘솔(MMC)에서 Managed Detection and Response 구성 요소를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **Detection and Response → Managed Detection and Response(Industrial CyberSecurity)**를 선택합니다.
4. **Managed Detection and Response(Industrial CyberSecurity)** 확인란을 선택합니다.
5. **설정** 블록에서 **업로드**를 클릭하고 Kaspersky Managed Detection and Response 콘솔에서 받은 BLOB 파일을 선택합니다. 파일의 확장자는 P7입니다.

   기본적으로 사용자는 애플리케이션 설정을 관리할 수 있습니다("자물쇠" 열림). 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다 .
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 Managed Detection and Response 구성 요소를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성 → Managed Detection and Response**로 갑니다.
5. **Managed Detection and Response 활성화됨** 토글을 켭니다.
6. **업로드**를 클릭하고 Kaspersky Managed Detection and Response 콘솔에서 얻은 BLOB 파일을 선택합니다. 파일의 확장자는 P7입니다.

   기본적으로 사용자는 정책 설정을 관리할 수 있습니다("자물쇠" 열림). 컴퓨터에 정책을 적용하려면 자물쇠를 잠급니다 .
7. 변경 사항을 저장합니다.

명령줄에서 Managed Detection and Response 구성 요소를 활성화하는 방법

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

3. 다음 명령을 실행합니다:

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

> 이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다. 해당 사용자에게 **애플리케이션 설정 구성** 권한이 있어야 합니다.

결과적으로 Kaspersky Endpoint Security에서 BLOB 파일을 확인합니다. BLOB 파일 확인에는 디지털 서명 및 라이센스 기간 확인이 포함됩니다. BLOB 파일을 성공적으로 확인하면 Kaspersky Endpoint Security는 다음번에 Kaspersky Security Center와 동기화하는 동안 파일을 다운로드하고 파일을 컴퓨터로 보냅니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Managed Detection and Response** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

5 원격 측정을 수신하도록 애플리케이션의 다른 구성 요소 구성

Managed Detection and Response가 작동하려면 다음 구성 요소를 활성화해야 합니다.

- Kaspersky Security Network(확장 모드)
- 행동 탐지
- 익스플로잇 방지
- 웹 위협 보호
- 메일 위협 보호
- 파일 위협 보호
- 네트워크 위협 보호.
- 방화벽
- AMSI 보호.
- 백그라운드 검사.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Managed Detection and Response**로 갑니다.
5. **Managed Detection and Response 활성화됨** 토글을 켭니다.
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 창에서 **Detection and Response → Managed Detection and Response(Industrial CyberSecurity)**를 선택합니다.

4. **Managed Detection and Response(Industrial CyberSecurity)** 확인란을 선택합니다.

5. 변경 사항을 저장합니다.

MDR용 KEA에서 KES로의 마이그레이션 가이드

Kaspersky Endpoint Security for Windows에는 Kaspersky Managed Detection and Response 솔루션용 내장 에이전트가 포함됩니다. 이제 Kaspersky Endpoint Agent 애플리케이션이 없어도 MDR을 이용할 수 있습니다. Kaspersky Endpoint Agent의 모든 기능은 Kaspersky Endpoint Security에 의해 실행됩니다.

Kaspersky Endpoint Agent가 설치된 컴퓨터에 Kaspersky Endpoint Security를 배포하면 Kaspersky Managed Detection and Response 솔루션이 Kaspersky Endpoint Security와 계속해서 작동합니다. 또한 Kaspersky Endpoint Agent가 컴퓨터에서 제거됩니다. Kaspersky Endpoint Security를 버전 11.6.0 이상으로 업데이트하면 시스템에서 동일한 행동이 발생합니다.

Kaspersky Endpoint Security는 Kaspersky Endpoint Agent와 호환되지 않습니다. 이러한 애플리케이션을 한 컴퓨터에 다 설치할 수는 없습니다.

Kaspersky Endpoint Security가 Kaspersky Managed Detection and Response의 일부로 작동하려면 다음 조건을 충족해야 합니다.

- Kaspersky Security Center 버전 13.2 이상(네트워크 에이전트 포함) 이전 버전의 Kaspersky Security Center에서는 Managed Detection and Response의 기능을 활성화할 수 없습니다.
- Kaspersky Security Center 웹 콘솔과 중앙 관리 서버 간의 백그라운드 연결이 설정되었습니다. MDR에서 Kaspersky Security Center 웹 콘솔과 통해 중앙 관리 서버를 사용하려면 새로운 연결인 *백그라운드 연결*을 구성해야 합니다.

[KES+KEA] 구성을 MDR용 [KES+내장형 에이전트]로 마이그레이션하는 단계

1. **Kaspersky Endpoint Security 관리 플러그인 업그레이드**

   MDR 구성요소는 Kaspersky Endpoint Security 관리 플러그인 버전 11.6 이상을 사용하여 관리할 수 있습니다. 사용하고 있는 Kaspersky Security Center 콘솔 유형에 따라 관리 콘솔(MMC)의 관리 플러그인 또는 웹 콘솔의 웹 플러그인을 업데이트합니다.

2. **정책 및 작업 마이그레이션**

   Kaspersky Endpoint Agent 설정을 Windows용 Kaspersky Endpoint Security로 이전합니다. 다음과 같은 옵션을 사용할 수 있습니다.

   - Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로 마이그레이션하는 마법사입니다. Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로 마이그레이션하는 마법사는 웹 콘솔에서만 작동합니다.

     Kaspersky Endpoint Agent에서 웹 콘솔의 Kaspersky Endpoint Security로 정책 및 작업 설정을 마이그레이션하는 방법

     웹 콘솔 메인 창에서 **동작 → Kaspersky Endpoint Agent에서 마이그레이션**을 선택합니다.

정책 및 작업 마이그레이션 마법사가 열립니다. 마법사의 지침을 따릅니다.

1단계. 정책 마이그레이션

마이그레이션 마법사가 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent 정책의 설정을 병합하는 새 정책을 만듭니다. 정책 목록에서 Kaspersky Endpoint Security 정책에 병합하고자 하는 Kaspersky Endpoint Agent 정책 설정을 선택합니다. Kaspersky Endpoint Agent 정책을 클릭해서 설정을 병합할 Kaspersky Endpoint Security 정책을 선택합니다. 알맞은 정책을 선택했는지 확인하고 다음 단계로 넘어갑니다.

2단계. 정책 마이그레이션

마이그레이션 마법사는 MDR 작업을 지원하지 않습니다. 이 단계를 건너뜁니다.

3단계. 마법사 완료

마법사를 끝냅니다. 마법사를 진행한 결과 새로운 Kaspersky Endpoint Security 정책이 생성됩니다. 정책이 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent의 설정을 병합합니다. 정책의 이름은 *<Kaspersky Endpoint Security 정책 이름> & <Kaspersky Endpoint Agent 정책 이름>*입니다. 새 정책은 *비활성* 상태입니다. 계속하려면 Kaspersky Endpoint Agent와 Kaspersky Endpoint Security 정책의 상태를 *비활성*으로 바꾸고 새로 병합된 정책을 활성화합니다.

- 표준 정책 및 작업 배치 변환 마법사 정책 및 작업 매치 변환 마법사는 관리자 콘솔(MMC)에서만 사용할 수 있습니다. 정책 및 작업 배치 변환 마법사에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

3 MDR 기능 라이센스

Managed Detection and Response 솔루션의 일부로 Kaspersky Endpoint Security를 활성화하려면 Kaspersky Managed Detection and Response 애드온에 대한 별도 라이센스가 필요합니다. *키 추가* 작업을 통해 키를 추가할 수 있습니다. 결과적으로 *Kaspersky Endpoint Security*와 *Kaspersky Managed Detection and Response* 키가 애플리케이션에 추가됩니다.

4 Kaspersky Endpoint Security 애플리케이션 설치 / 업그레이드

애플리케이션 설치 또는 업그레이드 중에 MDR 기능을 마이그레이션하려면 원격 설치 작업을 사용하는 것이 좋습니다. 원격 설치 작업을 생성할 때 설치 패키지 설정에서 MDR 구성요소를 선택해야 합니다.

다음 방법을 사용하여 원격으로 애플리케이션을 업그레이드할 수도 있습니다:

- Kaspersky 업데이트 서비스 사용.
- 로컬에서 설치 마법사 실행.

Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 애플리케이션이 설치된 컴퓨터에서 애플리케이션을 업데이트할 때 구성 요소의 자동 선택을 지원합니다. 구성 요소의 자동 선택은 애플리케이션을 업그레이드하는 사용자 계정의 권한에 달려 있습니다.

시스템 계정(SYSTEM)의 EXE 또는 MSI 파일을 사용해 Kaspersky Endpoint Security를 업그레이드한다면 Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 대한 접근 권한을 획득합니다. 따라서 컴퓨터에 Kaspersky Endpoint Agent가 설치되어 있고 MDR 솔루션이 활성화되어 있는 경우, Kaspersky Endpoint Security 설치 프로그램은 자동으로 구성 요소의 세트를 구성하고 MDR 구성 요소를 선택합니다. 이에 따라 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다. 시스템 계정(SYSTEM)에서 MSI 설치 프로그램을 실행하면 주로 Kaspersky 업데이트 서비스를 통해 업그레이드하거나 Kaspersky Security Center를 통해 설치 패키지를 배포할 때 수행됩니다.

별도의 권한이 없는 사용자 계정으로 MSI 파일을 사용하여 Kaspersky Endpoint Security를 업그레이드한다면, Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 접근할 권한이 없습니다. 이 경우 Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 구성 요소 세트를 기반으로 자동으로 구성 요소를 선택합니다. 그리고 나서 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다.

Kaspersky Endpoint Security에서는 컴퓨터를 재시작하지 않고도 업그레이드가 지원됩니다. 정책 속성에서 애플리케이션 업그레이드 모드를 선택할 수 있습니다.

5 **애플리케이션 동작 확인**

애플리케이션 설치 또는 업그레이드 후에 Kaspersky Security Center 콘솔 상태가 *심각*으로 표시되면 다음을 수행합니다.

- 컴퓨터에 Network Agent 버전 13.2 이상이 설치되었는지 확인합니다.
- *애플리케이션 구성 요소 상태 리포트*를 확인하여 내장 에이전트의 작동 상태를 확인합니다. 구성 요소의 상태가 *설치 안 됨*이라면 *애플리케이션 구성 요소 변경* 작업으로 구성 요소를 설치합니다. 컴퓨터가 *라이센스에 포함되지 않음* 상태에 있는 경우, 내장 에이전트에 기능을 활성화했는지 확인하십시오.
- Kaspersky Endpoint Security for Windows의 새 정책에서 Kaspersky Security Network 진술문을 수락해야 합니다.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows에는 이제 Kaspersky Endpoint Detection and Response Optimum 솔루션(이하 'EDR Optimum'이라고도 함)용 내장 에이전트가 포함됩니다. 11.8.0 버전부터 Kaspersky Endpoint Security for Windows에 Kaspersky Endpoint Detection and Response Expert 솔루션(이하 "EDR Expert"이라고도 함)용 내장 에이전트가 포함됩니다. *Kaspersky Endpoint Detection and Response*는 지능형 사이버 위협으로부터 조직의 IT 인프라를 보호하기 위한 폭넓은 솔루션입니다. 이 솔루션의 기능은 위협 자동 탐지와 이에 대한 대응 능력을 결합하여 새로운 익스플로잇, 랜섬웨어, 파일리스 공격 및 합법적인 시스템 도구를 사용하는 방법 등 다양한 지능형 공격에 대처합니다. EDR Expert는 EDR Optimum보다 더 많은 보안위협 모니터링 및 대응 기능을 제공합니다. 솔루션에 관한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말 과 Kaspersky Endpoint Detection and Response Expert 도움말 을 참조하십시오.

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 Portal 과의 통합.
- Kaspersky 보안 위협 데이터베이스.

- Kaspersky 기술 자료에 있는 파일, 웹사이트 및 소프트웨어의 실시간 평판 정보에 대한 접근을 제공하는 Kaspersky Security Network(이하 "KSN") 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.

- 격리된 환경에서 탐지된 파일을 실행하고 해당 파일의 평판을 확인할 수 있는 Cloud Sandbox 기술입니다.

솔루션 작동 원리

Kaspersky Endpoint Detection and Response는 보안 위협 개발을 검토 및 분석하고 즉각적인 대응이 필요한 잠재적 공격에 대한 정보를 *보안 인력*이나 *관리자*에게 제공합니다. Kaspersky Endpoint Detection and Response의 경고 세부 정보는 별도의 창으로 표시됩니다. *경고*는 애플리케이션이 비정상적이거나 의심스러운 것으로 식별하여 회사 IT 인프라에 보안 위협이 될 수 있는 회사 IT 인프라 이벤트를 말합니다. *경고 세부 정보*는 탐지된 위협에서 수집한 전체 정보를 확인하는 도구입니다. 경고 세부 정보에는 컴퓨터에서의 파일 히스토리 등이 포함됩니다. 경고 세부 정보 관리에 대한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말과 Kaspersky Endpoint Detection and Response Expert 도움말을 참조하십시오.

이전 버전의 Kaspersky Endpoint Security 지원

Kaspersky Endpoint Detection and Response Optimum과의 상호 운용성을 위해 Kaspersky Endpoint Security 11.2.0~11.6.0을 사용한다면 해당 애플리케이션이 Kaspersky Endpoint Agent를 포함합니다. Kaspersky Endpoint Security 설치 중에 Kaspersky Endpoint Agent를 설치할 수 있습니다. Kaspersky Endpoint Security 11.9.0에서는 Kaspersky Endpoint Security 배포 키트에 Kaspersky Endpoint Agent 배포 패키지가 포함되지 않습니다.

Kaspersky Endpoint Detection and Response Expert 솔루션은 Kaspersky Endpoint Agent와의 상호 운용성을 지원하지 않습니다. Kaspersky Endpoint Detection and Response Expert 솔루션은 내장 에이전트를 포함하는 Kaspersky Endpoint Security(버전 11.8.0 이상)을 사용합니다.

EDR Optimum / EDR Expert와 내장 에이전트 통합

Kaspersky Endpoint Detection and Response와 통합하려면 Endpoint Detection and Response Optimum(EDR Optimum) 구성 요소 또는 Endpoint Detection and Response Expert(EDR Expert) 구성 요소를 추가하고 Kaspersky Endpoint Security를 구성해야 합니다.

EDR Optimum, EDR Expert 및 EDR(KATA) 구성 요소는 서로 호환되지 않습니다.

Endpoint Detection and Response의 작동을 위해서는 다음 조건을 만족해야 합니다:

- Kaspersky Security Center 버전 13.2 이상. 이전 버전의 Kaspersky Security Center에서는 Endpoint Detection and Response의 기능을 활성화할 수 없습니다.
- Kaspersky Endpoint Detection and Response 관리 플러그인.

  Kaspersky Endpoint Security 버전 12.6부터 경고 세부 정보 표시가 Kaspersky Endpoint Security 관리 플러그인에서 EDR 관리 플러그인으로 이동되었습니다. EDR 관리 플러그인은 Windows, Mac 및 Linux 운영 체제에서 에이전트 작업을 위한 단일 플러그인입니다. 이제 EDR Optimum으로 작업할 때 보안 위협 대응 작업을 만들려면 Kaspersky Endpoint Security 관리 플러그인이 필요하고 경고 세부 정보를 보려면 EDR 관리 플러그인이 필요합니다.
- Kaspersky Endpoint Security에 포함된 EDR Optimum 구성 요소는 Kaspersky Endpoint Detection and Response Optimum 2.0 솔루션과의 상호 작용을 지원합니다. Kaspersky Endpoint Detection and Response Optimum 버전 1.0과의 상호 작용은 지원하지 않습니다.
- EDR Optimum은 Kaspersky Security Center 웹 콘솔 및 Kaspersky Security Center Cloud Console에서 관리할 수 있습니다.

  EDR Expert는 Kaspersky Security Center Cloud Console을 통해서만 관리할 수 있습니다. 관리 콘솔(MMC)로는 이 기능을 관리할 수 없습니다.
- 애플리케이션이 활성화되고 해당 기능에 라이센스가 적용됩니다.
- Endpoint Detection and Response 구성 요소가 켜져 있습니다.
- Endpoint Detection and Response가 종속되는 애플리케이션 구성 요소가 활성화 및 작동 중입니다. Endpoint Detection and Response는 다음 구성 요소에 종속됩니다:
  - 파일 위협 보호
  - 웹 위협 보호
  - 메일 위협 보호
  - 익스플로잇 방지
  - 행동 탐지
  - 호스트 침입 방지
  - 복원 엔진
  - 적응형 이상 행위 제어

Kaspersky Endpoint Detection and Response와의 통합은 다음 단계를 포함합니다:

1. **Endpoint Detection and Response 구성 요소 설치**

   EDR Optimum 또는 EDR Expert 구성 요소는 설치나 업그레이드 중 선택하거나 *애플리케이션 구성 요소 변경* 작업을 사용해 선택할 수 있습니다.

   > 새 구성 요소로 애플리케이션 업그레이드를 완료하려면 컴퓨터를 다시 시작해야 합니다.

2. **Kaspersky Endpoint Detection and Response 활성화**

Kaspersky Endpoint Detection and Response 사용 라이센스는 다음 방법으로 획득할 수 있습니다:

- Endpoint Detection and Response 기능은 Kaspersky Endpoint Security for Windows 라이센스에 포함되어 있습니다.

  이 기능은 Kaspersky Endpoint Security for Windows 활성화 직후 바로 사용할 수 있습니다.

- EDR Optimum 또는 EDR Expert(Kaspersky Endpoint Detection and Response Optimum 애드온) 사용을 위한 별도 라이센스 구매.

  이 기능은 Kaspersky Endpoint Detection and Response의 키를 별도로 추가한 후에 이용할 수 있습니다. 결과적으로 Kaspersky Endpoint Security 키와 Kaspersky Endpoint Detection and Response 두 개의 키가 컴퓨터에 설치됩니다.

  독립 실행형 Endpoint Detection and Response 기능의 라이센스 사용은 Kaspersky Endpoint Security의 라이센스 사용과 같습니다.

EDR Optimum 또는 EDR Expert 기능이 라이센스에 포함되며 애플리케이션의 로컬 인터페이스에서 실행되고 있는지 확인하십시오.

EDR Optimum 최종 사용자 라이센스 계약서에 대한 자세한 내용은 Kaspersky Endpoint Detection and Response Optimum 도움말을 참조하십시오.

3 Endpoint Detection and Response 구성 요소 활성화

Kaspersky Endpoint Security for Windows 정책 설정에서 구성 요소를 활성화 또는 비활성화할 수 있습니다.

웹 콘솔 및 Cloud Console에서 Endpoint Detection and Response 구성 요소를 활성화 또는 비활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Endpoint Detection and Response**로 갑니다.
5. **Endpoint Detection and Response 활성화됨** 토글을 켭니다.
6. 변경 사항을 저장합니다.

Kaspersky Endpoint Detection and Response 구성 요소가 활성화됩니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Endpoint Detection and Response Optimum** 또는 **Endpoint Detection and Response Expert** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

4 중앙 관리 서버로의 데이터 전송 활성화

모든 Endpoint Detection and Response 기능을 활성화하려면 다음 유형의 데이터 전송을 활성화해야 합니다.

- 격리 파일 데이터.

  이 데이터는 웹 콘솔과 Cloud Console을 통해 컴퓨터에서 격리된 파일 정보를 얻는 데 필요합니다. 예를 들어, 웹 콘솔과 Cloud Console에서 분석을 위해 격리 저장소의 파일을 다운로드할 수 있습니다.

- 보안 위협 개발 체인 데이터.

  이 데이터는 웹 콘솔과 Cloud Console에서 컴퓨터에서 탐지된 보안 위협에 관한 정보를 얻는 데 필요합니다. 웹 콘솔과 Cloud Console에서 경고 세부 정보를 확인하고 대응할 수 있습니다.

웹 콘솔과 Cloud Console에서 중앙 관리 서버로의 데이터 전송을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **KSC 통합**으로 갑니다.
5. **중앙 관리 서버로의 데이터 전송** 블록에서 **고급 설정** 링크를 클릭합니다.
6. 창이 열리면 다음 확인란을 선택합니다.
   - **격리 저장소 파일 정보**
   - **위협 개발 체인 정보**
7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

침해지표 검사(표준 작업) 검사

*침해지표(IOC)*는 컴퓨터에 대한 무단 접근(데이터 침해)을 나타내는 개체 또는 활동에 대한 데이터 집합입니다. 예를 들어, 시스템 로그인 시도가 여러 번 실패하면 침해지표가 될 수 있습니다. *IOC 검사* 작업을 통해 컴퓨터에서 침해지표를 찾고 보안 위협에 대응할 수 있습니다.

Kaspersky Endpoint Security는 IOC 파일을 사용하여 침해지표를 검색합니다. *IOC 파일*은 애플리케이션이 탐지 횟수 계산을 위해 매치하는 지표 세트를 포함하는 파일입니다. IOC 파일은 OpenIOC 표준을 준수해야 합니다.

IOC 검사 작업 실행 모드

Kaspersky Endpoint Detection and Response에서 표준 IOC 검사 작업을 생성하여 유출된 데이터를 탐지할 수 있습니다. *표준 IOC 검사 작업*은 웹 콘솔에서 수동으로 만들고 구성하는 그룹 또는 로컬 작업입니다. 작업은 사용자가 준비한 IOC 파일을 사용하여 실행됩니다. 침해 지표를 직접 추가하려면 IOC 파일 요구 사항을 읽어주십시오.

아래의 링크를 클릭해 다운로드할 수 있는 파일에는 OpenIOC 표준의 전체 IOC 용어 목록이 포함되어 있습니다.

IOC_TERMS.XLSX 파일 다운로드

Kaspersky Endpoint Security는 애플리케이션을 Kaspersky Sandbox 솔루션의 일부로 사용할 시 독립실행형 IOC 검사 작업도 지원합니다.

IOC 파일 생성

Kaspersky Endpoint Security 12.10 for Windows부터는 작업 설정에서 직접 IOC 파일을 생성할 수 있습니다. IOC 파일을 생성하려면 침해지표 목록이 포함된 TXT 파일을 준비해야 합니다. 다음 개체 목록을 침해지표로 추가할 수 있습니다:

- 파일 해시(MD5/SHA256).
  애플리케이션이 검사 범위가 FileItem/Md5sum나 FileItem/Sha256sum인 IOC 파일을 준비합니다.
- IP 주소(IPv4, IPv6).
  애플리케이션이 검사 범위가 PortItem/RemoteIP인 IOC 파일을 준비합니다.
- DNS 이름.
  애플리케이션이 검사 범위가 DnsEntryItem/RecordName인 IOC 파일을 준비합니다.

웹 콘솔에서 IOC 파일 생성 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **IOC 검사** 작업을 선택합니다.
   작업 속성 창이 열립니다. 필요하다면 **IOC 검사** 작업을 생성합니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **IOC 검사 설정** 섹션으로 이동합니다.
5. **IOC 파일 재정의**를 클릭합니다.
6. IOC 파일 생성용 양식이 열립니다:
   a. **IOC 파일 출처**에서 **파일에서 생성**을 선택합니다.
   b. IOC 파일의 이름을 입력합니다.
   c. 침해지표 목록이 있는 TXT 파일을 선택합니다.
   d. **DNS 이름**, **파일 해시**, **IP 주소** 등 IOC 파일 유형을 선택합니다.
   e. **생성**을 클릭합니다.

   Kaspersky Endpoint Security가 IOC 컬렉션에 IOC 파일을 추가합니다. 필요하다면 작업 범위에서 IOC 파일을 잠시 제외할 수 있습니다.
7. 변경 사항을 저장합니다.

IOC 검사 작업 생성

IOC 검사 작업은 다음에서 수동으로 생성할 수 있습니다:

- 경고 세부 정보(EDR Optimum에서만).

  *경고 세부 정보*는 탐지된 위협에서 수집한 전체 정보를 확인하는 도구입니다. 경고 세부 정보에는 컴퓨터에서의 파일 히스토리 등이 포함됩니다. 경고 세부 정보 관리에 대한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말 과 Kaspersky Endpoint Detection and Response Expert 도움말 을 참조하십시오.

- 작업 마법사 사용.

웹 콘솔과 Cloud Console에서 EDR Optimum 작업을 구성할 수 있습니다. Cloud Console에서 EDR Expert 작업 설정을 이용할 수 있습니다.

IOC 검사 작업을 생성하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **IOC 검사**를 선택합니다.
   c. **작업 이름** 필드에 간단한 설명을 입력합니다.
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. 다음 단계로 넘어갑니다.
5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. 다음 단계로 넘어갑니다.

   기본적으로 Kaspersky Endpoint Security는 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.

   네트워크 드라이브에 대한 독립 실행형 IOC 검사 작업을 위해서는 작업 속성에서 이 드라이브에 대한 접근 권한이 있는 사용자 계정을 수동으로 선택해야 합니다.
6. 마법사를 끝냅니다.
   작업 목록에 새 작업이 표시됩니다.

7. 새 작업을 클릭합니다.

   작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. **IOC 검사 설정** 섹션으로 이동합니다.

10. IOC 파일 업로드하여 침해지표를 검색합니다.

    IOC 파일을 업로드하면 애플리케이션이 검사를 통과하지 못한 지표 목록을 포함하여 파일에 대한 요약 정보를 표시합니다. IOC 파일을 업로드한 후 작업 속성의 내장 편집기에서 직접 파일을 편집할 수 있습니다. Kaspersky Endpoint Security는 OpenIOC 1.1 표준을 준수하는 IOC 파일 편집을 지원합니다. OpenIOC 버전 1.0과 호환되는 IOC 파일의 내용은 수정할 수 없습니다.

    Kaspersky Endpoint Security가 IOC 컬렉션에 IOC 파일을 추가합니다. 필요하다면 작업 범위에서 IOC 파일을 잠시 제외할 수 있습니다.

    > 작업을 실행한 후 IOC 파일을 추가하거나 제거하는 것은 권장하지 않습니다. 이로 인해 작업의 이전 실행에 대한 IOC 검사 결과가 잘못 표시될 수 있습니다. 새 IOC 파일에 따른 침해 지표를 검색하려면 새 작업을 추가하는 것을 권장합니다.

11. 필요하다면 **회고적 IOC 검사** 확인란을 선택합니다. *회고적 IOC 검사*는 Kaspersky Endpoint Security가 특정 기간의 데이터를 사용하여 침해 지표를 검사하는 *IOC 검사* 작업의 모드 중 하나입니다. 이 모드는 네트워크 활동, 프로세스, 파일, 기타 원격 측정 등 보호된 컴퓨터의 원격 측정을 통해 침해지표를 검색하는 데 사용됩니다. Kaspersky Endpoint Security가 컴퓨터에 설치된 운영 체제 로그 및 브라우저 로그의 데이터를 분석합니다.

    회고적 IOC 검사는 다음 브라우저의 로그를 분석합니다. Google Chrome, Mozilla Firefox, Microsoft Edge(버전 79 이상).

12. IOC 탐지 시 동작을 구성합니다:

    - **네트워크에서 장치 격리**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 위협 확산을 방지하기 위해 컴퓨터를 네트워크에서 격리합니다. Endpoint Detection and Response 구성 요소 설정에서 격리 기간을 구성할 수 있습니다.

      이 확인란을 선택 취소하면 작업을 직접 실행한 후 네트워크에서 컴퓨터를 격리할 수 있습니다. *IOC 검사* 작업이 IOC를 탐지하면 컴퓨터를 네트워크에서 격리할 수 있으며 IOC에서 직접 컴퓨터를 격리할 수 있습니다(*IOC 검사*의 속성 → **애플리케이션 설정** → **IOC 검사 결과** 작업). Kaspersky Endpoint Security는 네트워크 격리 비활성화 기간 및 네트워크 격리 예외 등의 추가 설정을 즉시 관리할 수도 있습니다.

    - **격리 저장소로 사본을 옮기고 개체 삭제**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 컴퓨터에서 발견된 악성 개체를 삭제합니다. 개체를 삭제하기 전에 Kaspersky Endpoint Security는 나중에 개체를 복원해야 할 때를 대비하여 백업 복사본을 생성합니다. Kaspersky Endpoint Security는 백업 복사본을 격리 저장소로 이동합니다.

      이 확인란을 선택 취소하면 작업을 직접 실행한 후 파일을 직접 격리할 수 있습니다. *IOC 검사* 작업이 데이터를 손상할 수 있는 파일을 탐지하면 IOC 검사 결과에서 이 파일을 직접 격리할 수 있습니다(**애플리케이션 설정** → **IOC 검사 결과**). 그러면 Kaspersky Endpoint Security가 탐지된 파일의 사전 설정된 데이터로 작업 생성 마법사를 시작합니다. 작업 스케줄 설정과 같은 추가 작업 설정만 관리하면 됩니다.

    - **중요 영역 검사 실행**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 *중요 영역 검사* 작업을 실행합니다. Kaspersky Endpoint Security는 기본적으로 커널 메모리, 실행 중인 프로세스 및 디스크 부트 섹터를 검사합니다.

13. **고급** 섹션으로 이동합니다.

14. 작업 시 분석해야 하는 데이터 유형(IOC 문서)을 선택합니다.

Kaspersky Endpoint Security는 불러온 IOC 파일의 내용에 따라 *IOC 검사* 작업에 대한 데이터 유형(IOC 문서)을 자동으로 선택합니다. 데이터 유형을 선택 해제하는 것은 권장하지 않습니다.

다음 데이터 유형에 대해 검사 범위를 추가로 구성할 수 있습니다:

- **파일 – FileItem**. 이미 정의된 범위를 사용해 컴퓨터에서 IOC 검사 범위를 설정합니다.

  기본적으로 Kaspersky Endpoint Security는 다운로드 폴더, 바탕화면, 운영 체제 임시 파일이 있는 폴더 등 컴퓨터의 중요한 영역에 대해서만 IOC 검사를 수행합니다. 검사 범위를 수동으로 추가할 수도 있습니다.

- **Windows 이벤트 로그 - EventLogItem**. 이벤트가 기록된 시간대를 입력합니다. IOC 검사에 어떤 Windows 이벤트 로그를 사용할 지도 선택할 수 있습니다. 기본적으로 애플리케이션 이벤트 로그, 시스템 이벤트 로그, 보안 이벤트 로그가 선택됩니다.

- **Windows 레지스트리 – RegistryItem**. 레지스트리에서 IOC 검사 범위를 구성합니다.

  기본적으로 Kaspersky Endpoint Security는 레지스트리 키 세트를 검사합니다.

15. 작업 속성 창에서 **스케줄** 탭을 선택합니다.

16. 작업 스케줄을 구성합니다.

    이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.

17. 변경 사항을 저장합니다.

18. 작업 옆의 확인란을 선택합니다.

19. **시작**을 클릭합니다.

    결과적으로 Kaspersky Endpoint Security는 컴퓨터에서 침해지표 검색을 실행합니다. **결과** 섹션의 작업 속성에서 작업 결과를 볼 수 있습니다. 작업 속성(**애플리케이션 설정 → IOC 검사 결과**)에서 탐지된 침해지표에 관한 정보를 볼 수 있습니다. IOC 검사 결과에서 직접 탐지된 파일을 격리하거나 네트워크에서 컴퓨터를 격리할 수도 있습니다.

Kaspersky Endpoint Security는 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 필드에 값이 없는 경우 레코드를 생성하지 않을 수 있습니다(아래 표 참조).

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	• Hive • KeyPath • ValueName • Text • Type	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 Endpoint Security가 가장 오래된 항목을 자동으로 삭제합니다.

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 Endpoint Security는 탐지된 침해 지표에 대한 정보를 교체할 수 있습니다.

확장 원격 측정을 활성화하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성 → Endpoint Detection and Response**로 갑니다.
5. **고급 시스템 활동 기록 활성화** 확인란을 선택합니다.
6. 변경 사항을 저장합니다.

격리 저장소로 파일 이동

보안위협에 대응할 때 Kaspersky Endpoint Detection and Response는 *격리 저장소로 파일 이동* 작업을 생성할 수 있습니다. 이는 보안위협의 결과를 최소화하는 데 필요합니다. *격리 저장소*는 컴퓨터의 특수 로컬 저장소입니다. 컴퓨터에 위험하다고 판단되는 파일을 격리할 수 있습니다. 격리된 파일은 암호화된 상태로 저장되며 장치 보안에 위협이 되지 않습니다. Kaspersky Endpoint Security는 Kaspersky Detection and Response 솔루션과 통합했을 때만 격리 저장소를 사용합니다. 그 외에는 Kaspersky Endpoint Security가 관련 파일을 백업에 저장합니다. 솔루션에 포함된 격리 저장소 관리 방법에 대한 자세한 내용은 Kaspersky Sandbox 도움말, Kaspersky Endpoint Detection and Response Optimum 도움말, Kaspersky Endpoint Detection and Response Expert 도움말, Kaspersky Anti Targeted Attack Platform 도움말 및 Kaspersky Endpoint Detection and Response Expert(on-premise) 도움말을 참조하십시오.

다음과 같은 방법으로 *격리 저장소로 파일 이동* 작업을 생성할 수 있습니다:

- 경고 세부 정보(EDR Optimum에서만).
  *경고 세부 정보*는 탐지된 위협에서 수집한 전체 정보를 확인하는 도구입니다. 경고 세부 정보에는 컴퓨터에서의 파일 히스토리 등이 포함됩니다. 경고 세부 정보 관리에 대한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말과 Kaspersky Endpoint Detection and Response Expert 도움말을 참조하십시오.
- 작업 마법사 사용.
  파일 경로와 해시(SHA256 또는 MD5)를 입력하거나 둘 중 하나를 입력해야 합니다.
- *IOC 검사* 작업 설정 사용.
  IOC 검사 작업이 데이터를 손상할 수 있는 파일을 탐지하면 IOC 검사 결과에서 이 파일을 직접 격리할 수 있습니다(**애플리케이션 설정 → IOC 검사 결과**). 그러면 Kaspersky Endpoint Security가 탐지된 파일의 사전 설정된 데이터로 작업 생성 마법사를 시작합니다. 작업 스케줄 설정과 같은 추가 작업 설정만 관리하면 됩니다.

격리 저장소로 파일 이동 작업에는 다음 제한 사항이 있습니다.

1. 파일 크기는 100MB를 초과할 수 없습니다.
2. SCO(시스템 중요 개체)는 격리할 수 없습니다. SCO는 운영 체제 및 Kaspersky Endpoint Security for Windows 애플리케이션을 실행하는 데 필요한 파일입니다.

3. 웹 콘솔과 Cloud Console에서 EDR Optimum 작업을 구성할 수 있습니다. Cloud Console에서 EDR Expert 작업 설정을 이용할 수 있습니다.

4. *격리 저장소로 파일 이동* 작업에 따라 격리된 개체는 검사할 수 없습니다.

격리 저장소로 파일 이동 작업을 생성하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **격리 저장소로 파일 이동**을 선택합니다.

   c. **작업 이름** 필드에 간단한 설명을 입력합니다.

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

4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. **다음**을 클릭합니다.

5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음**을 클릭합니다.

   기본적으로 Kaspersky Endpoint Security는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. **마침** 버튼을 눌러 마법사를 마칩니다.
   작업 목록에 새 작업이 표시됩니다.

7. 새 작업을 클릭합니다.
   작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. 파일 목록에서 **추가**를 클릭합니다.
   파일 추가 마법사가 시작됩니다.

10. 파일을 추가하려면 파일의 전체 경로를 입력하거나, 파일 해시와 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.

12. 작업 스케줄을 구성합니다.

이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.

13. 변경 사항을 저장합니다.

14. 작업 옆의 확인란을 선택합니다.

15. **시작**을 클릭합니다.

결과적으로 Kaspersky Endpoint Security는 파일을 격리 저장소로 이동합니다.

다른 프로세스가 파일을 잠갔다면 작업은 *완료*로 표시되지만 파일 자체는 컴퓨터가 다시 시작된 후에만 격리됩니다. 컴퓨터를 다시 시작한 후 파일이 삭제되었는지 확인하십시오.

현재 실행 중인 실행 파일을 격리할 시 *격리 저장소로 파일 이동* 작업이 *접근 거부됨* 오류와 함께 끝납니다. 파일에 대해 프로세스 종료 작업을 생성한 후 다시 시도하십시오.

너무 큰 파일을 격리하려고 하면 *격리 저장소로 파일 이동* 작업이 *격리 저장소에 공간이 부족합니다* 오류와 함께 끝납니다. 격리 저장소를 비우거나 격리 저장소 공간을 확장하십시오. 그 후 다시 시도합니다.

격리 저장소에서 파일을 복원하거나 웹 콘솔을 사용하여 격리 저장소를 비울 수 있습니다. 명령줄을 사용하면 컴퓨터에서 로컬로 개체를 복원할 수 있습니다.

파일 가져오기

사용자 컴퓨터에서 파일을 가져올 수 있습니다. 예를 들어 타사 애플리케이션에서 만든 이벤트 로그 파일을 가져오도록 구성할 수 있습니다. 작업 실행에 따른 파일은 격리 저장소에 저장됩니다. *격리 저장소*는 컴퓨터의 특수 로컬 저장소입니다. 웹 콘솔(**동작 → 저장소 → 격리**)을 사용하여 격리 저장소에서 컴퓨터로 이 파일을 다운로드할 수 있습니다. 이 파일은 사용자 컴퓨터의 원래 폴더에 남습니다.

파일 크기는 100MB를 초과할 수 없습니다.

웹 콘솔과 Cloud Console에서 EDR Optimum 작업을 구성할 수 있습니다. Cloud Console에서 EDR Expert 작업 설정을 이용할 수 있습니다.

파일 가져오기 작업을 생성하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 작업**을 선택합니다.
   작업 목록이 열립니다.

2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **파일 가져오기**를 선택합니다.

   c. **작업 이름** 필드에 간단한 설명을 입력합니다.

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

4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. **다음**을 클릭합니다.

5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음**을 클릭합니다.

   기본적으로 Kaspersky Endpoint Security는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. **마침** 버튼을 눌러 마법사를 마칩니다.
   작업 목록에 새 작업이 표시됩니다.

7. 새 작업을 클릭합니다.
   작업 속성 창이 열립니다.

8. **애플리케이션 설정** 탭을 선택합니다.

9. 파일 목록에서 **추가**를 클릭합니다.
   파일 추가 마법사가 시작됩니다.

10. 파일을 추가하려면 파일의 전체 경로를 입력하거나, 파일 해시와 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.

12. 작업 스케줄을 구성합니다.

    이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.

13. 변경 사항을 저장합니다.

14. 작업 옆의 확인란을 선택합니다.

15. **시작**을 클릭합니다.

결과적으로 Kaspersky Endpoint Security는 파일의 사본을 생성하고 이 사본을 격리 저장소로 이동합니다. 웹 콘솔의 격리 저장소에서 파일을 다운로드할 수 있습니다.

파일 삭제

파일 삭제 작업을 사용하여 파일을 원격으로 삭제할 수 있습니다. 예를 들어 보안위협 대응 시 원격으로 파일을 삭제할 수 있습니다.

파일 삭제 작업에는 다음 제한 사항이 있습니다.

- SCO(System Critical Object, 시스템 중요 개체)는 삭제할 수 없습니다. SCO는 운영 체제 및 Kaspersky Endpoint Security 애플리케이션을 실행하는 데 필요한 파일입니다.
- 웹 콘솔과 Cloud Console에서 EDR Optimum 작업을 구성할 수 있습니다. Cloud Console에서 EDR Expert 작업 설정을 이용할 수 있습니다.

파일 삭제 작업을 생성하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **파일 삭제**를 선택합니다.
   c. **작업 이름** 필드에 간단한 설명을 입력합니다.
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. **다음**을 클릭합니다.
5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음**을 클릭합니다.

   기본적으로 Kaspersky Endpoint Security는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. **마침** 버튼을 눌러 마법사를 마칩니다.
   작업 목록에 새 작업이 표시됩니다.
7. 새 작업을 클릭합니다.
   작업 속성 창이 열립니다.
8. **애플리케이션 설정** 탭을 선택합니다.
9. 파일 목록에서 **추가**를 클릭합니다.
   파일 추가 마법사가 시작됩니다.

10. 파일을 추가하려면 파일의 전체 경로를 입력하거나, 파일 해시와 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.

12. 작업 스케줄을 구성합니다.

    이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.

13. 변경 사항을 저장합니다.

14. 작업 옆의 확인란을 선택합니다.

15. **시작**을 클릭합니다.

    결과적으로 Kaspersky Endpoint Security는 컴퓨터에서 파일을 삭제합니다. 다른 프로세스가 파일을 잠갔다면 작업은 *완료*로 표시되지만, 파일 자체는 컴퓨터를 다시 시작한 후에만 삭제됩니다. 컴퓨터를 다시 시작한 후 파일이 삭제되었는지 확인하십시오.

현재 실행 중인 실행 파일을 삭제할 시 *파일 삭제* 작업이 *접근이 거부되었거나 파일을 찾을 수 없음* 오류와 함께 끝납니다. 파일에 대해 프로세스 종료 작업을 생성한 후 다시 시도하십시오.

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.

웹 콘솔과 Cloud Console에서 EDR Optimum 작업을 구성할 수 있습니다. Cloud Console에서 EDR Expert 작업 설정을 이용할 수 있습니다.

프로세스 시작 작업을 생성하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.

2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.

3. 검사 설정을 구성합니다:

   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.

   b. **작업 유형** 드롭다운 목록에서 **프로세스 시작**을 선택합니다.

c. **작업 이름** 필드에 간단한 설명을 입력합니다.

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

4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. **다음**을 클릭합니다.

5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음**을 클릭합니다.

   기본적으로 Kaspersky Endpoint Security는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. **마침** 버튼을 눌러 마법사를 마칩니다.
   작업 목록에 새 작업이 표시됩니다.

7. 새 작업을 클릭합니다.

8. 작업 속성 창이 열립니다.

9. **애플리케이션 설정** 탭을 선택합니다.

10. 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`

11. 작업 속성 창에서 **스케줄** 탭을 선택합니다.

12. 작업 스케줄을 구성합니다.

    이 작업에서는 Wake-on-LAN을 사용할 수 없습니다. 작업을 실행하려면 컴퓨터가 켜져 있어야 합니다.

13. 변경 사항을 저장합니다.

14. 작업 옆의 확인란을 선택합니다.

15. **시작**을 클릭합니다.

    결과적으로 Kaspersky Endpoint Security는 숨김 모드에서 명령을 실행하고 프로세스를 시작합니다. **실행 결과** 섹션의 작업 속성에서 작업 결과를 볼 수 있습니다.

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 방지 구성 요소를 구성할 수 있습니다. 실행 파일, 스크립트, 오피스 형식 파일의 실행을 금지할 수 있습니다.

프로세스 종료 작업에는 다음 제한 사항이 있습니다.

- SCO(시스템 중요 개체) 프로세스는 종료할 수 없습니다. SCO는 운영 체제 및 Kaspersky Endpoint Security 애플리케이션을 실행하는 데 필요한 파일입니다.
- 웹 콘솔과 Cloud Console에서 EDR Optimum 작업을 구성할 수 있습니다. Cloud Console에서 EDR Expert 작업 설정을 이용할 수 있습니다.

프로세스 종료 작업을 생성하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 작업**을 선택합니다.
   작업 목록이 열립니다.
2. **추가**를 클릭합니다.
   작업 마법사가 시작됩니다.
3. 검사 설정을 구성합니다:
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Endpoint Security for Windows 14.0.0**를 선택합니다.
   b. **작업 유형** 드롭다운 목록에서 **프로세스 종료**를 선택합니다.
   c. **작업 이름** 필드에 간단한 설명을 입력합니다.
   d. **이 작업이 할당되는 기기** 블록에서 작업 범위를 선택합니다.
4. 선택한 작업 범위 옵션에 따라 장치를 선택합니다. **다음**을 클릭합니다.
5. 작업 실행에 사용할 권한이 있는 사용자 계정의 자격 증명을 입력합니다. **다음**을 클릭합니다.

   기본적으로 Kaspersky Endpoint Security는 시스템 사용자 계정(SYSTEM)으로 작업을 시작합니다.

6. **마침** 버튼을 눌러 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**을 클릭합니다.

13. 작업 옆의 확인란을 선택합니다.

14. **시작**을 클릭합니다.

결과적으로 Kaspersky Endpoint Security는 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.

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 세트와 스크립트 인터프리터 세트를 지원합니다.

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 정보(EDR Optimum에서만).

  *경고 세부 정보*는 탐지된 위협에서 수집한 전체 정보를 확인하는 도구입니다. 경고 세부 정보에는 컴퓨터에서의 파일 히스토리 등이 포함됩니다. 경고 세부 정보 관리에 대한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말 과 Kaspersky Endpoint Detection and Response Expert 도움말 을 참조하십시오.

- 그룹 정책 또는 로컬 애플리케이션 설정 사용.

  파일 경로와 해시(SHA256 또는 MD5)를 입력하거나 둘 중 하나를 입력해야 합니다.

명령줄을 사용해 로컬에서 실행 방지를 관리할 수도 있습니다.

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 Endpoint Security 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 방지 구성 요소는 두 가지 모드로 사용할 수 있습니다:

- **통계만**

  이 모드에서는 Kaspersky Endpoint Security가 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. 이 모드가 기본적으로 선택되어 있습니다.

- **활성**

  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 웹 콘솔에서만 구성할 수 있습니다.

실행을 방지하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **내장 에이전트 구성** → **Endpoint Detection and Response**로 갑니다.

5. **실행 방지** 탭을 선택합니다.

6. **실행 방지 활성화됨** 토글을 켭니다.

7. **금지된 개체 실행 또는 열기 시 동작** 블록에서 구성 요소 운영 모드를 선택합니다.

- **차단하고 이벤트 로그에 추가**. 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.

- **이벤트 로그에 추가**. 이 모드에서는 Kaspersky Endpoint Security가 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. 이 모드가 기본적으로 선택되어 있습니다.

8. 실행 방지 규칙 목록을 생성합니다:

   a. **추가**를 클릭합니다.

   b. 창이 열리면 실행 방지 규칙의 이름을 입력합니다(*Application A* 등).

   c. **유형** 드롭다운 목록에서 차단할 개체를 선택합니다: **실행 파일**, **스크립트**, **Microsoft Office 문서**.

   잘못된 개제 유형을 선택하면 Kaspersky Endpoint Security가 해당 파일 또는 스크립트를 차단하지 않습니다.

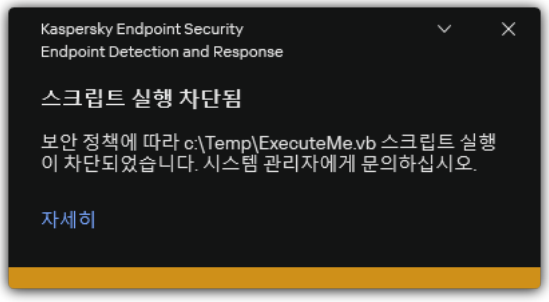
   d. 파일을 추가하려면 파일의 해시(SHA256 또는 MD5)와 파일의 전체 경로를 입력하거나 둘 중 하나를 입력해야 합니다.

   > 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 Endpoint Security가 해당 파일 또는 스크립트를 차단하지 않습니다.

   실행 방지는 오피스 파일 확장자 세트와 스크립트 인터프리터 세트를 지원합니다.

9. 변경 사항을 저장합니다.

결과적으로 Kaspersky Endpoint Security가 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 Endpoint Security가 기본 알림을 표시합니다(아래 그림 참조).



실행 방지 알림

컴퓨터 네트워크 격리

컴퓨터 네트워크 격리는 침해지표(IOC) 탐지 시 네트워크에서 컴퓨터를 자동으로 격리합니다. 이것은 *자동 모드*입니다. 탐지된 위협을 연구하는 동안 네트워크 격리를 수동으로 켤 수 있습니다. 이것은 *수동 모드*입니다.

네트워크 격리가 켜지면 애플리케이션은 활성화된 모든 연결을 끊고, 다음 연결을 제외하고 컴퓨터의 새로운 TCP/IP 네트워크 연결을 모두 차단합니다:

- 네트워크 격리 예외에 포함된 연결.
- Kaspersky Endpoint Security 서비스가 시작한 연결.
- Kaspersky Security Center 네트워크 에이전트가 시작한 연결.
- Light Agent 모드에서 애플리케이션을 사용하는 경우 SVM 및 통합 서버에 대한 연결.
- 애플리케이션을 Kaspersky Managed Detection and Response와 통합할 때 KSN에 대한 연결입니다.

구성 요소 설정은 웹 콘솔에서만 구성할 수 있습니다.

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**을 선택합니다.
   작업 목록이 열립니다.
2. Kaspersky Endpoint Security의 **IOC 검사** 작업을 클릭합니다.
   작업 속성 창이 열립니다.
   필요하다면 *IOC 검사* 작업을 생성합니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **IOC 탐지 시 동작** 블록에서, **IOC 발견 후 대응 동작 수행**과 **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**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.

4. **내장 에이전트 구성** → **Endpoint Detection and Response**로 갑니다.

5. **네트워크 격리** 탭을 선택합니다.

6. 네트워크 격리를 끌 시간을 선택합니다.

7. 변경 사항을 저장합니다.

수동 네트워크 격리 모드

네트워크 격리는 수동으로 켜고 끌 수 있습니다. Kaspersky Security Center 콘솔의 컴퓨터 속성을 사용하여 수동 네트워크 격리 모드를 구성할 수 있습니다.

네트워크 격리는 다음에서 켤 수 있습니다.

- 경고 세부 정보(EDR Optimum에서만).

  *경고 세부 정보*는 탐지된 위협에서 수집한 전체 정보를 확인하는 도구입니다. 경고 세부 정보에는 컴퓨터에서의 파일 히스토리 등이 포함됩니다. 경고 세부 정보 관리에 대한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말과 Kaspersky Endpoint Detection and Response Expert 도움말을 참조하십시오.

- 로컬 애플리케이션 설정 사용.

- *IOC 검사* 작업 설정 사용.

  IOC 검사 작업이 IOC를 탐지하면 컴퓨터를 네트워크에서 격리할 수 있으며 IOC에서 직접 컴퓨터를 격리할 수 있습니다(*IOC 검사*의 속성 → **애플리케이션 설정** → **IOC 검사 결과** 작업). Kaspersky Endpoint Security는 네트워크 격리 비활성화 기간 및 네트워크 격리 예외 등의 추가 설정을 즉시 관리할 수도 있습니다.

컴퓨터에서 네트워크 격리를 수동으로 켜는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)**를 선택합니다.

2. 로컬 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.

   그러면 컴퓨터 속성이 열립니다.

3. **애플리케이션** 탭을 선택합니다.

4. **Kaspersky Endpoint Security for Windows**를 누릅니다.

   그러면 로컬 애플리케이션 설정이 열립니다.

5. **애플리케이션 설정** 탭을 선택합니다.

6. **Detection and Response** → **Endpoint Detection and Response**로 갑니다.

7. **네트워크 격리** 블록에서 **네트워크에서 컴퓨터 격리**를 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)**를 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)**를 선택합니다.
2. 로컬 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.
   그러면 컴퓨터 속성이 열립니다.
3. **애플리케이션** 탭을 선택합니다.
4. **Kaspersky Endpoint Security for Windows**를 누릅니다.
   그러면 로컬 애플리케이션 설정이 열립니다.
5. **애플리케이션 설정** 탭을 선택합니다.
6. **Detection and Response → Endpoint Detection and Response**로 갑니다.
7. **네트워크 격리** 블록에서 **네트워크에서 격리된 컴퓨터 차단 해제**를 클릭합니다.

명령줄을 사용하여 로컬에서 네트워크 격리를 비활성화할 수도 있습니다.

Kaspersky Endpoint Security 12.10 for Windows부터 경고 세부 정보에서 네트워크 격리를 관리할 수 있습니다. 또한 경고 세부 정보에서 컴퓨터 네트워크 격리 기간을 지정할 수 있습니다. 경고 세부 정보 관리에 대한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말과 Kaspersky Endpoint Detection and Response Expert 도움말을 참조하십시오.

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**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Endpoint Detection and Response**로 갑니다.
5. **네트워크 격리** 탭을 선택합니다.
6. **네트워크 격리 예외** 블록에서 **예외 규칙**을 클릭합니다.
7. 창이 열리면 **추가** → **프로필 추가**를 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** → **추가**를 클릭하고 네트워크 연결 설정을 수동으로 편집합니다.
9. 변경 사항을 저장합니다.

수동 모드에서 네트워크 격리 예외를 추가하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **에셋(기기)**를 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**을 클릭합니다.

7. 창이 열리면 **프로필 추가**를 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**를 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.

Kaspersky Endpoint Security 12.10 for Windows부터 경고 세부 정보에 네트워크 격리 예외를 추가할 수 있습니다. 경고 세부 정보 관리에 대한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말과 Kaspersky Endpoint Detection and Response Expert 도움말을 참조하십시오.

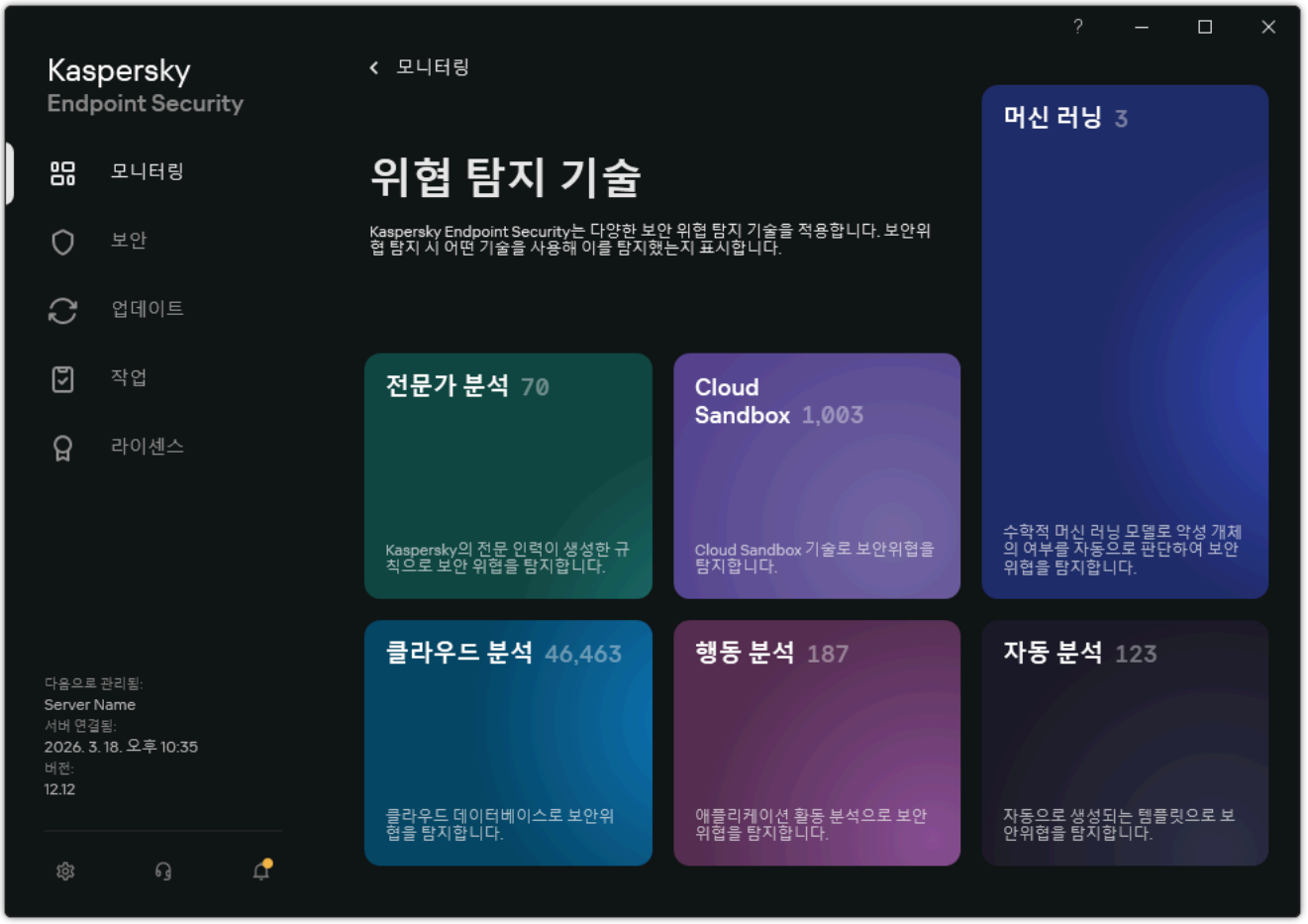
Cloud Sandbox

*Cloud Sandbox*는 컴퓨터에서 지능형 보안 위협을 탐지할 수 있는 기술입니다. Kaspersky Endpoint Security는 분석을 위해 탐지된 파일을 Cloud Sandbox에 자동 전달합니다. Cloud Sandbox는 이러한 파일을 격리된 환경에서 실행하여 악성 활동을 식별하고 평판을 결정합니다. 그다음 이 파일의 데이터가 Kaspersky Security Network로 전송됩니다. 따라서 Cloud Sandbox가 악성 파일을 탐지하면 Kaspersky Endpoint Security는 이 파일이 탐지된 모든 컴퓨터에서 이 위협 요소를 제거하기 위해 적절한 조치를 수행합니다.

Cloud Sandbox가 작동하려면 Kaspersky Security Network 사용 활성화가 필요합니다.

Kaspersky Private Security Network을 사용한다면 Cloud Sandbox 기술을 사용할 수 없습니다.

Cloud Sandbox 기술은 영구적으로 활성화되며 사용 중인 라이센스 유형과 관계없이 모든 Kaspersky Security Network 사용자가 사용할 수 있습니다. Endpoint Detection and Response 솔루션(EDR Optimum 또는 EDR Expert)을 이미 배포했다면 Cloud Sandbox에서 탐지한 위협에 대해 별도의 카운터를 활성화할 수 있습니다. 이 카운터를 사용하여 탐지된 보안 위협을 분석하는 동안 통계를 생성할 수 있습니다.



위협 카운터

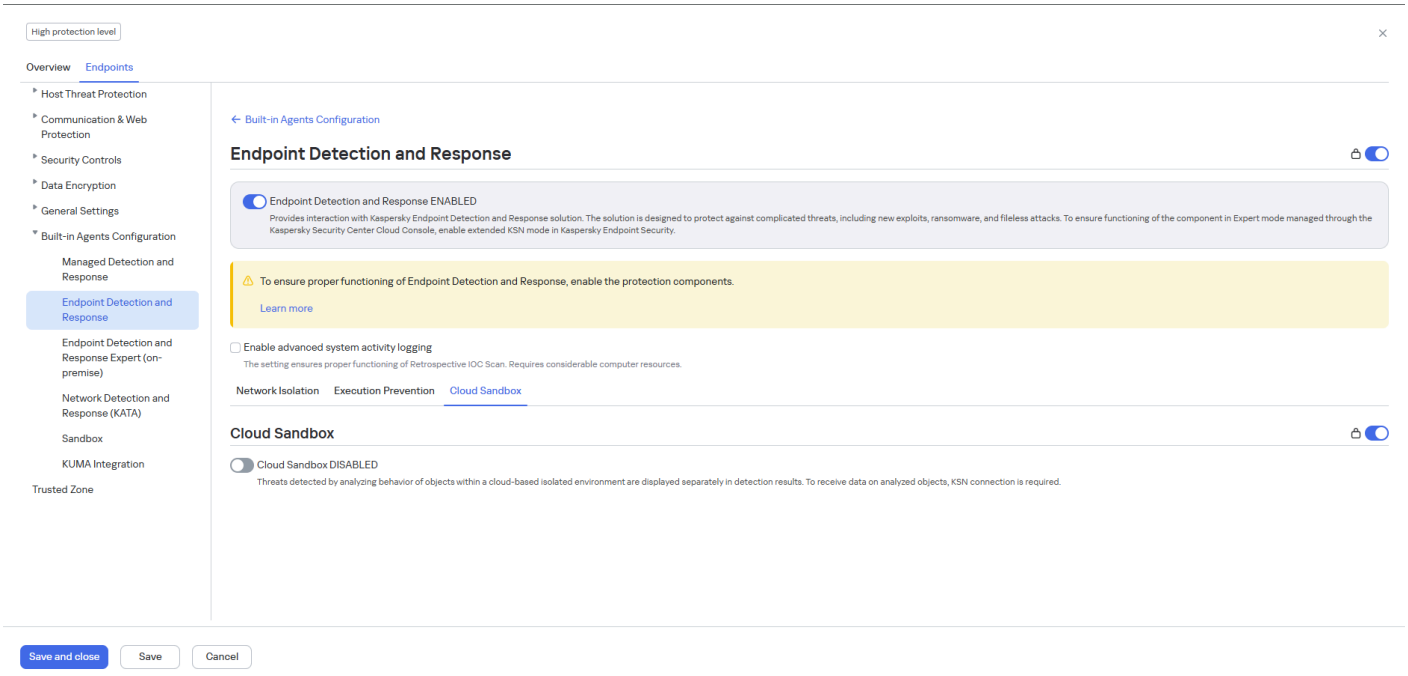
Cloud Sandbox 카운터를 활성화하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Endpoint Detection and Response**로 갑니다.
5. **Cloud Sandbox** 탭을 선택합니다.

6. **Cloud Sandbox 활성화됨** 토글을 켭니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

보안 위협이 발견될 때마다 Kaspersky Endpoint Security는 **위협 탐지 기술**의 기본 애플리케이션 창에서 Cloud Sandbox를 사용하여 탐지된 위협에 대한 카운터를 활성화합니다. Kaspersky Endpoint Security는 Kaspersky Security Center 콘솔의 *위협 처리 리포트*에서 Cloud Sandbox 보안 위협 탐지 기술을 표시합니다.



Endpoint Detection and Response 정책 섹션

EDR Optimum용 KEA에서 KES로의 마이그레이션 가이드

Kaspersky Endpoint Security for Windows에는 Kaspersky Endpoint Detection and Response Optimum 솔루션용 내장 에이전트가 포함됩니다. 이제 Kaspersky Endpoint Agent 애플리케이션이 없어도 EDR Optimum을 이용할 수 있습니다. Kaspersky Endpoint Agent의 모든 기능은 Kaspersky Endpoint Security에 의해 실행됩니다.

Kaspersky Endpoint Agent가 설치된 컴퓨터에 Kaspersky Endpoint Security를 배포하면 Kaspersky Endpoint Detection and Response Optimum 솔루션이 Kaspersky Endpoint Security와 계속해서 작동합니다. 또한 Kaspersky Endpoint Agent가 컴퓨터에서 제거됩니다. Kaspersky Endpoint Security를 버전 11.7.0 이상으로 업데이트하면 시스템에서 동일한 행동이 발생합니다.

Kaspersky Endpoint Security는 Kaspersky Endpoint Agent와 호환되지 않습니다. 이러한 애플리케이션을 한 컴퓨터에 다 설치할 수는 없습니다.

Kaspersky Endpoint Security가 Kaspersky Endpoint Detection and Response Optimum의 일부로 작동하려면 다음 조건을 충족해야 합니다.

- Endpoint Detection and Response Optimum 버전 2.0 이상
- Kaspersky Security Center 버전 13.2 이상(네트워크 에이전트 포함) 이전 버전의 Kaspersky Security Center에서는 EDR Optimum의 기능을 활성화할 수 없습니다.
- EDR Optimum은 Kaspersky Security Center 웹 콘솔을 통해서만 관리할 수 있습니다.

- 중앙 관리 서버로의 데이터 전송이 활성화되었습니다. 이 데이터는 웹 콘솔을 통해 컴퓨터에서 격리된 파일 정보를 얻는 데 필요합니다.
- Kaspersky Security Center 웹 콘솔과 중앙 관리 서버 간의 백그라운드 연결이 설정되었습니다. EDR Optimum에서 Kaspersky Security Center 웹 콘솔과 통해 중앙 관리 서버를 사용하려면 새로운 연결인 *백그라운드 연결*을 구성해야 합니다.

[KES+KEA] 구성을 EDR Optimum용 [KES+내장형 에이전트]로 마이그레이션하는 단계

1. **Kaspersky Endpoint Security 웹 플러그인 업그레이드**

   EDR Optimum 구성요소는 Kaspersky Endpoint Security 웹 플러그인 버전 11.7.0 이상을 사용하여 관리할 수 있습니다.

2. **정책 및 작업 마이그레이션**

   Kaspersky Endpoint Agent 설정을 Windows용 Kaspersky Endpoint Security로 이전합니다. 이렇게 하려면 웹 콘솔의 Kaspersky Endpoint Agent에서 마이그레이션 마법사를 사용하십시오.

   Kaspersky Endpoint Agent에서 웹 콘솔의 Kaspersky Endpoint Security로 정책 및 작업 설정을 마이그레이션하는 방법

   웹 콘솔 메인 창에서 **동작 → Kaspersky Endpoint Agent에서 마이그레이션**을 선택합니다.

   정책 및 작업 마이그레이션 마법사가 열립니다. 마법사의 지침을 따릅니다.

   1단계. 정책 마이그레이션

   마이그레이션 마법사가 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent 정책의 설정을 병합하는 새 정책을 만듭니다. 정책 목록에서 Kaspersky Endpoint Security 정책에 병합하고자 하는 Kaspersky Endpoint Agent 정책 설정을 선택합니다. Kaspersky Endpoint Agent 정책을 클릭해서 설정을 병합할 Kaspersky Endpoint Security 정책을 선택합니다. 알맞은 정책을 선택했는지 확인하고 다음 단계로 넘어갑니다.

   2단계. 정책 마이그레이션

   마이그레이션 마법사는 Kaspersky Endpoint Security에 대한 새 작업을 생성합니다. 작업 목록에서 Kaspersky Endpoint Security 정책에 생성하고자 하는 Kaspersky Endpoint Agent 작업을 선택합니다. 다음 단계로 넘어갑니다.

   3단계. 마법사 완료

   마법사를 끝냅니다. 결과적으로 마법사는 다음을 수행합니다.

   - 새로운 Kaspersky Endpoint Security 정책을 생성합니다.

정책이 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent의 설정을 병합합니다. 정책의 이름은 *<Kaspersky Endpoint Security 정책 이름> & <Kaspersky Endpoint Agent 정책 이름>*입니다. 새 정책은 *비활성* 상태입니다. 계속하려면 Kaspersky Endpoint Agent와 Kaspersky Endpoint Security 정책의 상태를 *비활성*으로 바꾸고 새로 병합된 정책을 활성화합니다.

Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security for Windows로의 마이그레이션 후에는 새 정책에 중앙 관리 서버로의 데이터 전송 기능(격리 파일 데이터 및 보안 위협 개발 체인 데이터) 설정이 되어있는지 확인하십시오. 데이터 전송 파라미터 값은 Kaspersky Endpoint Agent 정책에서 마이그레이션되지 않습니다.

- 새 Kaspersky Endpoint Security 작업을 생성합니다.

  새 작업은 Kaspersky Endpoint Agent 작업의 복사본입니다. 또한 마법사는 Kaspersky Endpoint Agent 작업을 변경하지 않습니다.

3 EDR Optimum 기능 라이센스

Kaspersky Endpoint Detection and Response Optimum 또는 Kaspersky Optimum Security 공통 라이센스를 사용하여 Kaspersky Endpoint Security for Windows 및 Kaspersky Endpoint Agent를 활성화하면 애플리케이션을 버전 11.7.0 이상으로 업그레이드한 후 EDR Optimum 기능이 자동으로 활성화됩니다. 별도의 작업이 필요하지 않습니다.

독립 실행형 Kaspersky Endpoint Detection and Response Optimum 애드온 라이센스로 EDR Optimum 기능을 활성화하면 EDR Optimum 키가 Kaspersky Security Center 저장소에 추가되었으며 자동 라이센스 키 배포 기능이 활성화되었는지 확인해야 합니다. 애플리케이션을 버전 11.7.0 이상으로 업그레이드하면 EDR Optimum 기능이 자동으로 활성화됩니다.

Kaspersky Endpoint Detection and Response Optimum이나 Kaspersky Optimum Security 라이센스로 Kaspersky Endpoint Agent를 활성화한 후 다른 라이센스로 Kaspersky Endpoint Security for Windows를 활성화하면 Kaspersky Endpoint Security for Windows 키를 Kaspersky Endpoint Detection and Response Optimum 또는 Kaspersky Optimum Security 공통 키로 교체해야 합니다. 키는 *키 추가* 작업으로 교체할 수 있습니다.

4 Kaspersky Endpoint Security 애플리케이션 설치 / 업그레이드

애플리케이션 설치 또는 업그레이드 중에 EDR Optimum 기능을 마이그레이션하려면 원격 설치 작업을 사용하는 것이 좋습니다. 원격 설치 작업을 생성할 때 설치 패키지 설정에서 EDR Optimum 구성요소를 선택해야 합니다.

다음 방법을 사용하여 원격으로 애플리케이션을 업그레이드할 수도 있습니다:

- Kaspersky 업데이트 서비스 사용.
- 로컬에서 설치 마법사 실행.

Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 애플리케이션이 설치된 컴퓨터에서 애플리케이션을 업데이트할 때 구성 요소의 자동 선택을 지원합니다. 구성 요소의 자동 선택은 애플리케이션을 업그레이드하는 사용자 계정의 권한에 달려 있습니다.

시스템 계정(SYSTEM)의 EXE 또는 MSI 파일을 사용해 Kaspersky Endpoint Security를 업그레이드한다면 Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 대한 접근 권한을 획득합니다. 따라서 컴퓨터에 Kaspersky Endpoint Agent가 설치되어 있고 EDR Optimum 솔루션이 활성화되어 있는 것 같은 경우에 Kaspersky Endpoint Security 설치 프로그램은 자동으로 구성 요소의 세트를 구성하고 EDR Optimum 구성 요소를 선택합니다. 이에 따라 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다. 시스템 계정(SYSTEM)에서 MSI 설치 프로그램을 실행하면 주로 Kaspersky 업데이트 서비스를 통해 업그레이드하거나 Kaspersky Security Center를 통해 설치 패키지를 배포할 때 수행됩니다.

별도의 권한이 없는 사용자 계정으로 MSI 파일을 사용하여 Kaspersky Endpoint Security를 업그레이드한다면, Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 접근할 권한이 없습니다. 이때 Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 구성에 기반하여 자동으로 구성 요소를 선택합니다. 그리고 나서 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다.

Kaspersky Endpoint Security에서는 컴퓨터를 재시작하지 않고도 업그레이드가 지원됩니다. 정책 속성에서 애플리케이션 업그레이드 모드를 선택할 수 있습니다.

5. **애플리케이션 동작 확인**

   애플리케이션 설치 또는 업그레이드 후에 Kaspersky Security Center 콘솔 상태가 *심각*으로 표시되면 다음을 수행합니다.

   - 컴퓨터에 Network Agent 버전 13.2 이상이 설치되었는지 확인합니다.
   - *애플리케이션 구성 요소 상태 리포트*를 확인하여 내장 에이전트의 작동 상태를 확인합니다. 구성 요소의 상태가 *설치 안 됨*이라면 *애플리케이션 구성 요소 변경* 작업으로 구성 요소를 설치합니다. 컴퓨터가 *라이센스에 포함되지 않음* 상태에 있는 경우, 내장 에이전트에 기능을 활성화했는지 확인하십시오.
   - Kaspersky Endpoint Security for Windows의 새 정책에서 Kaspersky Security Network 진술문을 수락해야 합니다.

Kaspersky Sandbox



Kaspersky Endpoint Security for Windows에는 Kaspersky Sandbox 솔루션 통합을 위한 내장 에이전트가 포함됩니다. *Sandbox* 구성 요소는 컴퓨터에서 지능형 보안위협을 탐지하고 자동 차단합니다. Sandbox는 조직의 IT 인프라에 대한 표적 공격의 활동 특성 및 악성 활동 탐지를 위해 개체 행동을 분석합니다. Sandbox는 Microsoft Windows 운영 체제(Sandbox 서버)의 가상 이미지가 배포된 특수 서버의 개체를 분석하고 검사합니다. 이 솔루션에 대한 자세한 내용은 Kaspersky Sandbox 도움말 및 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

Kaspersky Sandbox와 내장 에이전트 통합

Sandbox 구성 요소와 통합하려면 Kaspersky Sandbox를 추가해야 합니다. Sandbox 구성 요소는 설치 또는 업그레이드 중 선택하거나 *애플리케이션 구성 요소 변경* 작업으로 선택할 수 있습니다.

구성 요소를 사용하려면 다음 조건을 충족해야 합니다.

- Kaspersky Security Center 13.2. Kaspersky Security Center의 이전 버전에서는 보안위협 대응에 대한 독립 실행형 IOC 검사 작업 생성을 허용하지 않습니다.
- 구성 요소는 웹 콘솔을 통해서만 관리할 수 있습니다. 관리 콘솔(MMC)로는 이 구성 요소를 관리할 수 없습니다.
- 애플리케이션이 활성화되고 해당 기능에 라이센스가 적용됩니다.
- 중앙 관리 서버로의 데이터 전송이 활성화되었습니다.

  Kaspersky Sandbox의 모든 기능을 사용하려면 격리 파일 데이터 전송을 활성화해야 합니다. 이 데이터는 웹 콘솔을 통해 컴퓨터에서 격리된 파일 정보를 얻는 데 필요합니다. 예를 들어, 웹 콘솔에서 분석을 위해 격리 저장소의 파일을 다운로드할 수 있습니다.

  웹 콘솔에서 중앙 관리 서버로의 데이터 전송을 활성화하는 방법

  1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
  2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

     정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **KSC 통합**으로 갑니다.
5. **중앙 관리 서버로의 데이터 전송** 블록에서 **격리 저장소 파일 정보** 확인란을 선택합니다.
6. 변경 사항을 저장합니다.

- Kaspersky Security Center 웹 콘솔과 중앙 관리 서버 간의 백그라운드 연결이 구성됨

  Kaspersky Sandbox에서 Kaspersky Security Center 웹 콘솔과 통해 중앙 관리 서버를 사용하려면 새로운 연결인 *백그라운드 연결*을 구성해야 합니다. Kaspersky Security Center와 다른 Kaspersky 솔루션의 통합에 관한 자세한 사항은 Kaspersky Security Center 도움말을 참조하십시오.

  웹 콘솔에서 백그라운드 연결 구성

  1. 웹 콘솔의 메인 창에서 **설정** → **통합**을 선택합니다.
  2. **통합** 섹션으로 이동합니다.
  3. **통합을 위한 백그라운드 연결 [활성화됨]** 토글을 켭니다.
  4. 변경 사항을 저장합니다.

  Kaspersky Security Center 웹 콘솔과 중앙 관리 서버 간의 백그라운드 연결이 구성되지 않으면 보안위협 대응을 위해 독자적으로 IOC 검사 작업을 생성할 수 없습니다.

- Sandbox 서버와의 신뢰할 수 있는 연결을 구성하려면 TLS 인증서를 준비해야 합니다. 그런 다음 정책을 사용하여 컴퓨터에 인증서를 추가해야 합니다. 또한 Sandbox 서버에 인증서를 추가해야 합니다.

  > Kaspersky Sandbox에서는 암호화 컨테이너를 사용한 양방향 인증을 사용할 수 없습니다.

  웹 콘솔이나 로컬에서 명령줄을 사용하여 TLS 인증서를 추가할 수도 있습니다.

- Kaspersky Sandbox 구성 요소가 활성화됩니다.
- Sandbox의 동작을 보장하는 애플리케이션 구성 요소가 활성화되고 작동합니다. Sandbox의 동작을 보장하는 구성 요소는 다음과 같습니다:
  - 파일 위협 보호
  - 호스트 침입 방지
  - 방화벽
  - AMSI 보호.
  - 백그라운드 검사.

Kaspersky Sandbox와의 통합을 활성화 또는 비활성화하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **내장 에이전트 구성** → **Sandbox**으로 이동합니다.

5. **Sandbox와 통합 활성화됨** 토글을 사용하여 구성 요소를 활성화 또는 비활성화합니다.

6. **통합 유형** 블록에서 구성 요소 **Kaspersky Sandbox**의 운영 모드를 선택합니다.

7. **연결 설정** 링크를 클릭합니다.

   Sandbox 서버 연결 설정 창이 열립니다.

8. **서버 TLS 인증서** 블록에서 **업로드**를 클릭하고 TLS 인증서 파일을 선택합니다.

   Kaspersky Endpoint Security는 Sandbox 서버에 대해 하나의 TLS 인증서만 가질 수 있습니다. 이전에 TLS 인증서를 추가했다면 해당 인증서가 해지됩니다. 마지막으로 추가된 인증서만 사용됩니다.

9. Sandbox 서버에 대한 고급 연결 설정 구성:

   - **시간 초과(msec)**. Sandbox 서버 연결에 대한 시간 초과입니다. 구성된 시간 초과를 넘으면 Kaspersky Endpoint Security가 다음 서버로 요청을 보냅니다. 연결 속도가 느리거나 연결이 불안정하다면 서버의 연결 시간 초과 설정을 늘릴 수 있습니다. 요청 시간 초과 설정은 0.5초 이하를 권장합니다.

   - **요청 대기열**. 요청 대기열 폴더의 크기입니다. Sandbox에서 검사하기 위해 여러 개체를 전송하는 경우 Kaspersky Endpoint Security는 요청 대기열을 생성합니다. 기본적으로 요청 대기열 폴더의 크기는 100MB로 제한됩니다. 최대 크기에 도달하면 Sandbox는 대기열에 새 요청 추가를 중지하고 해당 이벤트를 Kaspersky Security Center로 보냅니다. 서버 구성에 따라 요청 대기열 폴더의 크기를 구성할 수 있습니다.

10. **Sandbox 서버에 연결** 블록에서 **추가** 버튼을 누릅니다.

11. 창이 열리면 Sandbox 서버 주소(IPv4, IPv6, DNS) 및 포트를 입력합니다.

    가상 이미지 배포 및 Sandbox 서버 구성에 대한 자세한 내용은 Kaspersky Sandbox 도움말을 참조하십시오.

12. 변경 사항을 저장합니다.

결과적으로 Kaspersky Endpoint Security에서 TLS 인증서를 확인합니다. 인증서를 성공적으로 확인하면 Kaspersky Endpoint Security는 다음번에 Kaspersky Security Center와 동기화하는 동안 인증서 파일을 컴퓨터로 업로드합니다. TLS 인증서 둘을 추가했다면 Kaspersky Sandbox가 가장 최근의 인증서를 사용하여 신뢰하는 연결을 구성합니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Sandbox** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

웹 콘솔에서 또는 로컬에서 명령줄을 사용하여 Kaspersky Sandbox와의 통합을 활성화 또는 비활성화할 수 있습니다.

Kaspersky Endpoint Security는 Kaspersky Sandbox 구성 요소의 기능에 대한 정보를 리포트에 저장합니다. 리포트에는 오류에 대한 정보도 포함되어 있습니다. `Error code: XXX` 형식(예: `0xa67b01f4`)의 설명에 맞는 오류가 발생하면 기술 지원에 문의하십시오.

침해 지표 검사(독립 실행형 작업)

*침해지표(IOC)*는 컴퓨터에 대한 무단 접근(데이터 침해)을 나타내는 개체 또는 활동에 대한 데이터 집합입니다. 예를 들어, 시스템 로그인 시도가 여러 번 실패하면 침해지표가 될 수 있습니다. *IOC 검사* 작업을 통해 컴퓨터에서 침해지표를 찾고 보안 위협에 대응할 수 있습니다.

Kaspersky Endpoint Security는 IOC 파일을 사용하여 침해지표를 검색합니다. *IOC 파일*은 애플리케이션이 탐지 횟수 계산을 위해 매치하는 지표 세트를 포함하는 파일입니다. IOC 파일은 OpenIOC 표준을 준수해야 합니다. Kaspersky Endpoint Security는 Kaspersky Sandbox용 IOC 파일을 자동으로 생성합니다.

IOC 검사 작업 실행 모드

이 애플리케이션은 Kaspersky Sandbox용 독립 실행형 IOC 검사 작업을 생성합니다. *독립 실행형 IOC 검사 작업*은 Kaspersky Sandbox이 탐지한 보안 위협에 대응할 때 자동으로 생성되는 그룹 작업입니다. Kaspersky Endpoint Security는 IOC 파일을 자동으로 생성합니다. 사용자 정의 IOC 파일은 지원하지 않습니다. 작업은 생성 후 30일이 지나면 자동으로 삭제됩니다. 독립 실행형 IOC 검사 작업에 대한 자세한 내용은 Kaspersky Sandbox 도움말 을 참조하십시오.

IOC 검사 작업 설정

Kaspersky Sandbox는 보안 위협에 대응할 때 *IOC 검사* 작업을 자동으로 생성 및 실행할 수도 있습니다.

설정은 웹 콘솔에서만 구성할 수 있습니다.

Kaspersky Sandbox의 독립 실행형 IOC 검사 작업이 작동하려면 Kaspersky Security Center 13.2가 필요합니다.

IOC 검사 작업의 설정을 변경하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **작업**을 선택합니다.
   작업 목록이 열립니다.
2. Kaspersky Endpoint Security의 **IOC 검사** 작업을 클릭합니다.
   작업 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **IOC 검사 설정** 섹션으로 이동합니다.

5. IOC 탐지 시 동작을 구성합니다:

- **격리 저장소로 사본을 옮기고 개체 삭제**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 컴퓨터에서 발견된 악성 개체를 삭제합니다. 개체를 삭제하기 전에 Kaspersky Endpoint Security는 나중에 개체를 복원해야 할 때를 대비하여 백업 복사본을 생성합니다. Kaspersky Endpoint Security는 백업 복사본을 격리 저장소로 이동합니다.
- **중요 영역 검사 실행**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 *중요 영역 검사* 작업을 실행합니다. Kaspersky Endpoint Security는 기본적으로 커널 메모리, 실행 중인 프로세스 및 디스크 부트 섹터를 검사합니다.
- **컴퓨터가 유휴 상태일 때만 실행**. 컴퓨터 리소스가 사용 중일 때 작업 시작을 연기했습니다. Kaspersky Endpoint Security는 컴퓨터가 잠겨 있거나 화면 보호기가 켜져 있을 때 검사 작업을 시작합니다. 예를 들어 컴퓨터를 잠금 해제하는 등으로 작업 실행이 중단되면 Kaspersky Endpoint Security는 자동으로 중단된 지점부터 작업을 실행합니다. 이 예약 옵션을 사용하면 컴퓨터를 사용할 때 컴퓨터 리소스를 절약할 수 있습니다.

6. 변경 사항을 저장합니다.

결과 섹션의 작업 속성에서 작업 결과를 볼 수 있습니다. 작업 속성(**애플리케이션 설정 → IOC 검사 결과**)에서 탐지된 침해지표에 관한 정보를 볼 수 있습니다.

IOC 검사 결과는 30일간 보관됩니다. 이 기간 후에는 Kaspersky Endpoint Security가 가장 오래된 항목을 자동으로 삭제합니다.

Kaspersky Sandbox용 KEA에서 KES로의 마이그레이션 가이드

Kaspersky Endpoint Security for Windows에는 Kaspersky Sandbox 솔루션을 위해 내장 에이전트가 포함됩니다. 이제 Kaspersky Endpoint Agent 애플리케이션이 없어도 Kaspersky Sandbox를 이용할 수 있습니다. Kaspersky Endpoint Agent의 모든 기능은 Kaspersky Endpoint Security에 의해 실행됩니다.

Kaspersky Endpoint Agent가 설치된 컴퓨터에 Kaspersky Endpoint Security를 배포하면 Kaspersky Sandbox 솔루션이 Kaspersky Endpoint Security와 계속해서 작동합니다. 또한 Kaspersky Endpoint Agent가 컴퓨터에서 제거됩니다. Kaspersky Endpoint Security를 버전 11.7.0 이상으로 업데이트하면 시스템에서 동일한 행동이 발생합니다.

Kaspersky Endpoint Security는 Kaspersky Endpoint Agent와 호환되지 않습니다. 이러한 애플리케이션을 한 컴퓨터에 다 설치할 수는 없습니다.

Kaspersky Endpoint Security가 Kaspersky Sandbox의 일부로 작동하려면 다음 조건을 충족해야 합니다.

- Kaspersky Sandbox 버전 2.0 이상.
- Kaspersky Security Center 버전 13.2 이상(네트워크 에이전트 포함) 이전 버전의 Kaspersky Security Center에서는 Kaspersky Sandbox의 기능을 활성화할 수 없습니다.
- Kaspersky Sandbox는 Kaspersky Security Center 웹 콘솔을 통해서만 관리할 수 있습니다.

- 중앙 관리 서버로의 데이터 전송이 활성화되었습니다. 이 데이터는 웹 콘솔을 통해 컴퓨터에서 격리된 파일 정보를 얻는 데 필요합니다.
- Kaspersky Security Center 웹 콘솔과 중앙 관리 서버 간의 백그라운드 연결이 설정되었습니다. Kaspersky Sandbox에서 Kaspersky Security Center 웹 콘솔과 통해 중앙 관리 서버를 사용하려면 새로운 연결인 *백그라운드 연결*을 구성해야 합니다.

[KES+KEA] 구성을 Kaspersky Sandbox용 [KES+내장형 에이전트]로 마이그레이션하는 단계

1. **Kaspersky Endpoint Security 웹 플러그인 업그레이드**

   Kaspersky Sandbox 구성요소는 Kaspersky Endpoint Security 웹 플러그인 버전 11.7.0 이상을 사용하여 관리할 수 있습니다.

2. **정책 및 작업 마이그레이션**

   Kaspersky Endpoint Agent 설정을 Windows용 Kaspersky Endpoint Security로 이전합니다. 이렇게 하려면 웹 콘솔의 Kaspersky Endpoint Agent에서 마이그레이션 마법사를 사용하십시오.

   Kaspersky Endpoint Agent에서 웹 콘솔의 Kaspersky Endpoint Security로 정책 및 작업 설정을 마이그레이션하는 방법

   웹 콘솔 메인 창에서 **동작 → Kaspersky Endpoint Agent에서 마이그레이션**을 선택합니다.

   정책 및 작업 마이그레이션 마법사가 열립니다. 마법사의 지침을 따릅니다.

   1단계. 정책 마이그레이션

   마이그레이션 마법사가 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent 정책의 설정을 병합하는 새 정책을 만듭니다. 정책 목록에서 Kaspersky Endpoint Security 정책에 병합하고자 하는 Kaspersky Endpoint Agent 정책 설정을 선택합니다. Kaspersky Endpoint Agent 정책을 클릭해서 설정을 병합할 Kaspersky Endpoint Security 정책을 선택합니다. 알맞은 정책을 선택했는지 확인하고 다음 단계로 넘어갑니다.

   2단계. 정책 마이그레이션

   마이그레이션 마법사는 Kaspersky Endpoint Security에 대한 새 작업을 생성합니다. 작업 목록에서 Kaspersky Endpoint Security 정책에 생성하고자 하는 Kaspersky Endpoint Agent 작업을 선택합니다. 다음 단계로 넘어갑니다.

   3단계. 마법사 완료

   마법사를 끝냅니다. 결과적으로 마법사는 다음을 수행합니다.

   - 새로운 Kaspersky Endpoint Security 정책을 생성합니다.

정책이 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent의 설정을 병합합니다. 정책의 이름은 *<Kaspersky Endpoint Security 정책 이름> & <Kaspersky Endpoint Agent 정책 이름>*입니다. 새 정책은 *비활성* 상태입니다. 계속하려면 Kaspersky Endpoint Agent와 Kaspersky Endpoint Security 정책의 상태를 *비활성*으로 바꾸고 새로 병합된 정책을 활성화합니다.

Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security for Windows로의 마이그레이션 후에는 새 정책에 중앙 관리 서버로의 데이터 전송 기능(격리 파일 데이터 및 보안 위협 개발 체인 데이터) 설정이 되어있는지 확인하십시오. 데이터 전송 파라미터 값은 Kaspersky Endpoint Agent 정책에서 마이그레이션되지 않습니다.

- 새 Kaspersky Endpoint Security 작업을 생성합니다.

  새 작업은 Kaspersky Endpoint Agent 작업의 복사본입니다. 또한 마법사는 Kaspersky Endpoint Agent 작업을 변경하지 않습니다.

3 Kaspersky Sandbox 기능 라이센스

Kaspersky Sandbox 솔루션의 일부로 Kaspersky Endpoint Security를 활성화하려면 Kaspersky Sandbox 애드온에 대한 별도 라이센스가 필요합니다. *키 추가* 작업을 통해 키를 추가할 수 있습니다. 결과적으로 *Kaspersky Endpoint Security*와 *Kaspersky Sandbox* 키가 애플리케이션에 추가됩니다.

4 Kaspersky Endpoint Security 애플리케이션 설치 / 업그레이드

애플리케이션 설치 또는 업그레이드 중에 Kaspersky Sandbox 기능을 마이그레이션하려면 원격 설치 작업을 사용하는 것이 좋습니다. 원격 설치 작업을 생성할 때 설치 패키지 설정에서 Kaspersky Sandbox 구성요소를 선택해야 합니다.

다음 방법을 사용하여 원격으로 애플리케이션을 업그레이드할 수도 있습니다:

- Kaspersky 업데이트 서비스 사용.
- 로컬에서 설치 마법사 실행.

Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 애플리케이션이 설치된 컴퓨터에서 애플리케이션을 업데이트할 때 구성 요소의 자동 선택을 지원합니다. 구성 요소의 자동 선택은 애플리케이션을 업그레이드하는 사용자 계정의 권한에 달려 있습니다.

시스템 계정(SYSTEM)의 EXE 또는 MSI 파일을 사용해 Kaspersky Endpoint Security를 업그레이드한다면 Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 대한 접근 권한을 획득합니다. 따라서 컴퓨터에 Kaspersky Endpoint Agent가 설치되어 있고 Kaspersky Sandbox 솔루션이 활성화되어 있는 것 같은 경우에 Kaspersky Endpoint Security 설치 프로그램은 자동으로 구성 요소의 세트를 구성하고 Kaspersky Sandbox 구성요소를 선택합니다. 이에 따라 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다. 시스템 계정(SYSTEM)에서 MSI 설치 프로그램을 실행하면 주로 Kaspersky 업데이트 서비스를 통해 업그레이드하거나 Kaspersky Security Center를 통해 설치 패키지를 배포할 때 수행됩니다.

별도의 권한이 없는 사용자 계정으로 MSI 파일을 사용하여 Kaspersky Endpoint Security를 업그레이드한다면, Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 접근할 권한이 없습니다. 이때 Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 구성에 기반하여 자동으로 구성 요소를 선택합니다. 그리고 나서 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다.

Kaspersky Endpoint Security에서는 컴퓨터를 재시작하지 않고도 업그레이드가 지원됩니다. 정책 속성에서 애플리케이션 업그레이드 모드를 선택할 수 있습니다.

5 애플리케이션 동작 확인

애플리케이션 설치 또는 업그레이드 후에 Kaspersky Security Center 콘솔 상태가 *심각*으로 표시되면 다음을 수행합니다.

- 컴퓨터에 Network Agent 버전 13.2 이상이 설치되었는지 확인합니다.
- *애플리케이션 구성 요소 상태 리포트*를 확인하여 내장 에이전트의 작동 상태를 확인합니다. 구성 요소의 상태가 *설치 안 됨*이라면 *애플리케이션 구성 요소 변경* 작업으로 구성 요소를 설치합니다. 컴퓨터가 *라이센스에 포함되지 않음* 상태에 있는 경우, 내장 에이전트에 기능을 활성화했는지 확인하십시오.
- Kaspersky Endpoint Security for Windows의 새 정책에서 Kaspersky Security Network 진술문을 수락해야 합니다.

Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Security for Windows는 Kaspersky Anti Targeted Attack Platform(EDR(KATA) 솔루션 작업을 지원합니다. *Kaspersky Anti Targeted Attack Platform*은 표적형 공격, APT(지능형 지속 위협), 제로 데이 공격 등 지능형 위협을 적시에 탐지하도록 설계된 솔루션입니다. Kaspersky Anti Targeted Attack Platform에는 다음 세 가지 기능 단위가 포함됩니다.

- Kaspersky Anti Targeted Attack Platform(*KATA*)
- Kaspersky Endpoint Detection and Response(*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

모든 기능 단위를 구매하거나 개별 기능 단위를 따로 구매할 수 있습니다. 이 솔루션에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오. 애플리케이션에는 EDR, NDR 구성 요소용 내장 에이전트가 포함되어 있습니다. 또한 애플리케이션은 KATA의 일부인 Sandbox 구성 요소 작업도 지원합니다.

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(이하 "KSN") 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 Endpoint Security는 기업 IT 인프라의 개별 컴퓨터에 설치되며 프로세스, 개방형 네트워크 연결 및 수정되는 파일을 계속해서 모니터링합니다. 컴퓨터의 이벤트에 대한 정보(원격 측정 데이터)는 Kaspersky Anti Targeted Attack Platform 서버로 전송됩니다. 이때, Kaspersky Endpoint Security는 애플리케이션에서 발견한 보안 위협에 대한 정보와 이를 처리한 결과에 대한 정보도 Kaspersky Anti Targeted Attack Platform 서버로 보냅니다.

EDR(KATA) 및 NDR(KATA) 통합은 Kaspersky Security Center 콘솔에서 구성됩니다. 그러면 이 내장 에이전트가 Kaspersky Anti Targeted Attack Platform 콘솔을 사용하여 관리됩니다(작업 실행, 격리된 개체 관리, 리포트 보기 및 기타 작업 등).

EDR / NDR (KATA) 작업을 위한 Kaspersky Endpoint Security 구성

EDR / NDR (KATA) 작업에 다음 구성을 사용할 수 있습니다.

- **[KES+내장 에이전트]**. 이 구성에서 Kaspersky Endpoint Security는 컴퓨터 보안을 책임지는 애플리케이션이자 EDR / NDR (KATA) 작업을 위한 애플리케이션으로서 작동합니다. EDR(KATA)용 내장 에이전트는 Kaspersky Endpoint Security 12.1 for Windows 이상의 버전에서 사용할 수 있습니다. NDR(KATA)용 내장 에이전트는 Kaspersky Endpoint Security 12.7 for Windows 이상의 버전에서 사용할 수 있습니다.

- **[타사 EPP+EDR Agent]**. 이 구성에서는 타사 EPP(Endpoint Protection Platform)를 통해 IT 인프라 보안이 제공됩니다. Endpoint Detection and Response Agent(EDR Agent) 구성의 Kaspersky Endpoint Security에서 EDR / NDR (KATA)와의 상호 작용을 지원합니다. 이 구성에서 EDR Agent는 타사 EPP 애플리케이션과 호환됩니다. EDR(KATA)용 EDR Agent는 Kaspersky Endpoint Security 12.3 for Windows 이상의 버전에서 사용할 수 있습니다. NDR(KATA)용 EDR Agent는 Kaspersky Endpoint Security 12.7 for Windows 이상의 버전에서 사용할 수 있습니다.

이전 버전의 Kaspersky Endpoint Security 지원

Kaspersky Anti Targeted Attack Platform(EDR)과의 상호 운용성을 위해 Kaspersky Endpoint Security 11.2.0~11.8.0을 사용한다면 해당 애플리케이션이 Kaspersky Endpoint Agent를 포함합니다. Kaspersky Endpoint Security 설치 중에 Kaspersky Endpoint Agent를 설치할 수 있습니다.

Kaspersky Endpoint Security 11.9.0~12.0을 사용하는 경우 Kaspersky Endpoint Security 11.9.0부터는 Kaspersky Endpoint Agent 배포 패키지가 더 이상 Kaspersky Endpoint Security 배포 패키지의 일부가 아니므로 Kaspersky Endpoint Agent를 별도로 설치해야 합니다.

EDR / NDR (KATA)와 내장 에이전트 통합

EDR / NDR (KATA)와 통합하려면 Endpoint Detection and Response(KATA) 또는 Network Detection and Response(KATA)와 같은 관련 구성 요소를 추가해야 합니다. 애플리케이션을 설치 또는 업그레이드할 때 또는 *애플리케이션 구성 요소 변경* 작업을 사용할 때 EDR / NDR (KATA) 통합을 위한 구성 요소를 선택할 수 있습니다.

Kaspersky Endpoint Security for Windows 12.11 버전부터, EDR(KATA) 구성 요소의 이름이 **Endpoint Detection and Response Expert(버전 8.0 이상)**로 변경되었습니다. 이 버전의 애플리케이션에서 구성 요소는 Kaspersky Anti Targeted Attack Platform 7.1 이하 버전 및 Kaspersky Endpoint Detection and Response Expert(on-premise)와 호환됩니다.

EDR Optimum, EDR Expert 및 EDR(KATA) 구성 요소는 서로 호환되지 않습니다.

EDR / NDR (KATA)을 사용하려면 다음 조건을 충족해야 합니다.

- EDR(KATA): Kaspersky Anti Targeted Attack Platform 버전 5.0~7.1.
- NDR(KATA): Kaspersky Anti Targeted Attack Platform 버전 7.0 이상.

- EDR(KATA): Kaspersky Endpoint Security for Windows 12.1 이상. 다양한 버전의 Kaspersky Endpoint Security와 KATA의 호환성에 관한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.
- NDR(KATA): Kaspersky Endpoint Security for Windows 12.7 이상.
- Kaspersky Security Center 버전 14.2 이상. 이전 버전의 Kaspersky Security Center에서는 EDR / NDR (KATA) 기능을 활성화할 수 없습니다.
- 애플리케이션이 활성화되고 해당 기능에 라이센스가 적용됩니다.
- Endpoint Detection and Response(KATA) 및 Network Detection and Response(KATA) 구성 요소가 활성화됩니다.
- EDR / NDR (KATA)의 동작을 보장하는 애플리케이션 구성 요소가 활성화되고 작동합니다. EDR / NDR (KATA)의 동작을 보장하는 구성 요소는 다음과 같습니다.
  - 파일 위협 보호
  - 웹 위협 보호
  - 메일 위협 보호
  - 익스플로잇 방지
  - 행동 탐지
  - 호스트 침입 방지
  - AMSI 보호.
  - 백그라운드 검사.
  - Kaspersky Security Network

https://www.youtube.com/watch?v=cZzgtBoeC7k

https://www.youtube.com/watch?v=gd-rySv0ThQ

Endpoint Detection and Response(KATA)와의 통합은 다음 단계를 포함합니다:

1. **Endpoint Detection and Response(KATA) 및 Network Detection and Response(KATA) 구성 요소 설치**

   EDR(KATA) 및 NDR(KATA) 구성 요소는 설치 또는 업그레이드 중 선택하거나 *애플리케이션 구성 요소 변경* 작업으로 선택할 수 있습니다.

   > 새 구성 요소로 애플리케이션 업그레이드를 완료하려면 컴퓨터를 다시 시작해야 합니다.

2. **Endpoint Detection and Response(KATA) 및 Network Detection and Response(KATA) 활성화**

   EDR(KATA) 및 NDR(KATA) 사용을 위해 별도 라이센스 구매해야 합니다(예:Kaspersky Endpoint Detection and Response(KATA) 애드온).

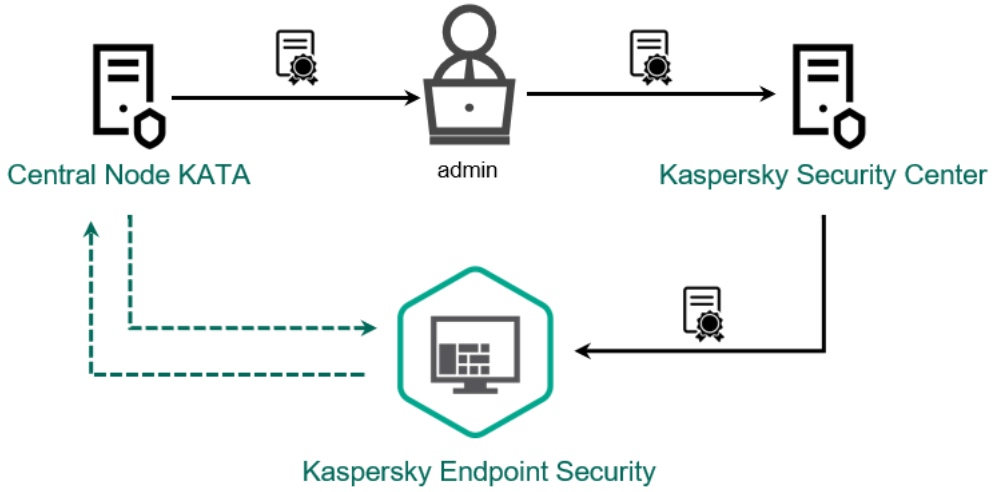
   EDR(KATA) 및 NDR(KATA) 기능을 포함하는 별도의 키를 추가하면 이 기능을 사용할 수 있습니다. 결과적으로 컴퓨터에 Kaspersky Endpoint Security용 키와 Kaspersky Endpoint Detection and Response(KATA) 및 Network Detection and Response(KATA)용 키가 추가됩니다.

   독립 실행형 EDR(KATA) 및 NDR(KATA) 기능의 라이센스 사용은 Kaspersky Endpoint Security의 라이센스 사용과 같습니다.

   EDR(KATA) 및 NDR(KATA) 기능 모두 라이센스에 포함되고 애플리케이션의 로컬 인터페이스에서 실행되고 있는지 확인하십시오.

3. **Central Node에 연결**

   Kaspersky Anti Targeted Attack Platform에서는 Kaspersky Endpoint Security와 Central Node 구성 요소 간에 신뢰할 수 있는 연결을 설정해야 합니다. 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 Endpoint Security에 TLS 인증서를 추가해야 합니다(아래 지침 참조).



Kaspersky Endpoint Security에 TLS 인증서 추가

기본적으로 Kaspersky Endpoint Security는 Central Node의 TLS 인증서만 확인합니다. 보다 안전한 연결을 위해, Central Node에서 컴퓨터 확인을 추가로 활성화할 수 있습니다(양방향 인증). 이 확인을 활성화하려면 Central Node와 Kaspersky Endpoint Security 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).

관리 콘솔(MMC)을 사용하여 Kaspersky Endpoint Security 컴퓨터를 Central Node에 연결하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **Detection and Response**를 선택하고 구성할 구성 요소(**Endpoint Detection and Response Expert(on-premise)** 또는 **Network Detection and Response(KATA)**를 선택합니다.
5. 해당 확인란(**Endpoint Detection and Response Expert(버전 7.1 이하)** 또는 **Network Detection and Response(KATA)**을 선택합니다.
6. **서버 연결 설정**을 클릭합니다.
7. 서버 연결 구성:
   - **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 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 Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 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.
8. **확인**을 누릅니다.
9. Central Node 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.

   여러 개의 Central Node 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.
10. 필요한 경우 원격 측정을 구성합니다.
11. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔을 사용하여 Kaspersky Endpoint Security 컴퓨터를 Central Node에 연결하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** 섹션으로 이동하고 구성할 구성 요소(**Endpoint Detection and Response Expert(on-premise)** 또는 **Network Detection and Response(KATA)**를 선택합니다.
5. 해당 토글 스위치(**Endpoint Detection and Response Expert(on-premise) 활성화됨** 또는 **Network Detection and Response(KATA) 활성화됨**)를 선택합니다.
6. EDR(KATA)을 구성하려면 솔루션 목록에서 **Endpoint Detection and Response Expert(버전 7.1 이하)**를 선택합니다.
7. **연결 설정**을 클릭합니다.
8. 서버 연결 구성:

   - **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 Central Node 서버에 연결을 시도합니다.
   - **서버 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 Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 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.
9. **확인**을 누릅니다.
10. Central Node 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.

    여러 개의 Central Node 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.
11. 필요한 경우 원격 측정을 구성합니다.
12. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

로컬에서 명령줄을 사용하여 TLS 인증서를 추가할 수도 있습니다.

결과적으로 컴퓨터가 Kaspersky Anti Targeted Attack Platform 콘솔에 추가됩니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Endpoint Detection and Response Expert(버전 8.0 이상)** 또는 **Network Detection and Response(KATA)** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

구성 요소 섹션에서 컴퓨터 속성의 Kaspersky Security Center 콘솔에서 구성 요소의 상태를 확인할 수 있습니다. 콘솔에서 구성 요소의 상태를 확인할 때는 다음을 고려해야 합니다. 구성 요소가 설치되어 있지 않고 해당 기능이 사용자의 라이센스에 포함되지 않는 경우 콘솔에 **설치 안 됨** 대신 **라이센스가 지원하지 않음** 상태가 표시됩니다.

Kaspersky Endpoint Security 12.6 for Windows부터 Kaspersky Security Center 관리 콘솔(MMC)에서 EDR(KATA) 구성 요소의 상태를 모니터링할 수 있습니다. 구성 요소의 현재 상태는 **Endpoint Sensor 상태** 열의 컴퓨터 속성에 표시됩니다(*실행 중*, *시작 중*, *중지됨*, *일시 중지됨*, *실패*, *알 수 없음*). 웹 콘솔은 Endpoint Sensor의 상태를 표시하지 않습니다.

EDR(KATA) 원격 측정 구성

*원격 측정*은 보호된 컴퓨터에서 발생한 이벤트 목록입니다. Kaspersky Endpoint Security는 원격 측정 데이터를 분석하여 동기화 시 Kaspersky Anti Targeted Attack Platform에 보냅니다. 원격 측정 이벤트는 거의 지속적으로 서버에 도착합니다. Kaspersky Endpoint Security는 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 Endpoint Security 정책에서 동기화 동작을 구성하고 네트워크 부하에 맞는 최적의 값을 선택할 수 있습니다(아래 지침 참조).

Kaspersky Endpoint Security와 서버가 서로 연결되어 있지 않으면 애플리케이션이 새 이벤트를 대기시킵니다. 연결이 복원되면 Kaspersky Endpoint Security가 대기열에 있는 이벤트들을 적절한 순서로 서버에 보냅니다. 서버 과부하를 방지하기 위해 Kaspersky Endpoint Security는 일부 이벤트를 건너뛸 수 있습니다. 이를 활성화하기 위해 이벤트 전송 설정을 최적화할 수 있습니다. 예를 들어, 시간당 이벤트 값을 최대로 설정합니다(아래 지침 참조).

Kaspersky Anti Targeted Attack Platform을 원격 측정을 사용하는 다른 솔루션과 함께 사용할 경우 KATA(EDR)의 원격 측정을 끌 수 있습니다(아래 지침 참고). 이렇게 하면 솔루션의 서버 로드를 최적화할 수 있습니다. 예를 들어 Managed Detection and Response 솔루션과 KATA(EDR)가 배포되어 있다면 MDR 원격 측정을 사용해 KATA(EDR)에서 보안 위협 대응 작업을 만들 수 있습니다.

관리 콘솔(MMC)에서 원격 측정을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **Detection and Response**를 선택하고 구성할 구성 요소(**Endpoint Detection and Response Expert(on-premise)** 또는 **Network Detection and Response(KATA)**를 선택합니다.
5. **다음 시간마다 KATA 서버로 동기화 요청 보내기(분)** 설정을 구성합니다. 서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Endpoint Security는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.

6. **KATA로 원격 측정 전송** 확인란이 선택되어 있어야 합니다.

7. 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.

   - **최대 이벤트 패키지 수**. 버퍼가 이벤트로 가득 차면 애플리케이션이 서버와 동기화를 수행합니다. 기본 설정은 이벤트 1024개입니다.

8. 필요한 경우 **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 Endpoint Security가 이벤트 전송을 중지합니다.

9. 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 Endpoint Security는 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 Endpoint Security는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 기본 설정은 15%입니다.

10. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔에서 원격 측정을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **내장 에이전트 구성** → **Endpoint Detection and Response Expert(on premise)**로 갑니다.

5. EDR(KATA)을 구성하려면 솔루션 목록에서 **Endpoint Detection and Response Expert(버전 7.1 이하)**를 선택합니다.

6. **데이터 전송 설정** 블록에서 **KATA 서버로 원격 측정 전송** 확인란이 선택되어 있는지 확인합니다.

7. **다음 시간마다 서버로 동기화 요청 보내기(분)** 설정을 구성합니다. 서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Endpoint Security는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.

8. **KATA 서버로 원격 측정 전송** 확인란이 선택되어 있어야 합니다.

9. 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.
   - **최대 이벤트 패키지 수**. 버퍼가 이벤트로 가득 차면 애플리케이션이 서버와 동기화를 수행합니다. 기본 설정은 이벤트 1024개입니다.

10. 필요한 경우 **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 Endpoint Security가 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 Endpoint Security는 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 Endpoint Security는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 기본 설정은 15%입니다.

12. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **KATA와의 통합** → **원격 측정 예외 규칙** 섹션으로 이동합니다.
5. **데이터 전송 설정**에서 **예외 사용** 확인란을 선택합니다.
6. **추가**를 클릭하고 예외 규칙을 설정합니다.

   기준은 논리 *AND*로 결합됩니다.

   - **경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다. 예외가 작동하려면 파일 경로를 지정해야 합니다.
   - **명령줄**. 개체를 실행하는 데 사용되는 명령입니다.
   - **설명**. RT_VERSION(VersionInfo) 리소스의 FileDescription 매개변수 값입니다.

     VersionInfo 리소스에 대한 자세한 내용은 Microsoft 웹사이트를 참고하시기 바랍니다.

- **원본 파일 이름**. RT_VERSION(VersionInfo) 리소스의 OriginalFilename 매개변수 값입니다.
- **버전**. RT_VERSION(VersionInfo) 리소스의 FileVersion 매개변수 값입니다.
- **MD5**. 파일의 MD5 해시입니다.
- **SHA256**. 파일의 SHA256 해시입니다.
- **이벤트 유형**. 예외가 작동하려면 하나 이상의 이벤트 유형을 선택해야 합니다.

7. 변경 사항을 저장합니다.

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

작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

1단계. 작업 유형 선택

1. **Kaspersky Endpoint Security for Windows (14.0) → 업데이트 롤백**을 선택합니다.

2단계. 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.

3 단계. 작업 시작 스케줄 구성

작업 일정을 설정합니다(예: 수동).

4단계. 작업 이름 정의

작업 이름을 입력합니다.

7단계. 작업 생성 완료

마법사를 끝냅니다. 필요시 **마법사 종료 후 작업 실행** 확인란을 선택합니다. 작업 속성에서 작업 진행률을 감시할 수 있습니다.

EDR(KATA) 원격 측정 예외

성능을 개선하고 원격 측정 서버로의 데이터 전송을 최적화하기 위해 원격 측정 예외 규칙을 구성할 수 있습니다. 예를 들어 개별 애플리케이션의 네트워크 통신 데이터를 전송하지 않도록 선택할 수 있습니다.

관리 콘솔(MMC)에서 원격 측정 예외 규칙을 만드는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 예외 및 개체 유형**을 선택합니다.
4. **원격 측정 설정 → EDR(KATA) / NDR(KATA) 원격 측정** 블록에서 **설정** 버튼을 누릅니다.
5. 창이 열리면 원격 측정 예외 규칙을 구성합니다(아래 표 참조).

   애플리케이션이 예외 조건을 논리 AND와 결합합니다. 규칙을 생성하려면 **전체 경로** 필드에서 값을 지정하고 **다음 이벤트 유형에 사용** 목록에서 하나 이상의 이벤트 유형을 선택하십시오.
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 원격 측정 예외 규칙을 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 원격 측정 설정**으로 이동합니다.
5. **EDR(KATA) / NDR(KATA) 원격 측정** 탭을 선택합니다.
6. 창이 열리면 원격 측정 예외 규칙을 구성합니다(아래 표 참조).

   애플리케이션이 예외 조건을 논리 AND와 결합합니다. 규칙을 생성하려면 **전체 경로** 필드에서 값을 지정하고 하나 이상의 이벤트 유형을 선택합니다.
7. 변경 사항을 저장합니다.

파라미터	설명
제외된 프로세스	**전송할 원격 측정 크기 최적화**. Kaspersky Endpoint Security를 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 Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **처리** 및 **부모 프로세스**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 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**. **방향**. **프로토콜**. **원시 소켓**. **프로토콜 번호**. **TLS 인증서**. **로컬 포트 또는 범위**. **원격 포트 또는 범위**. **로컬 주소**. Kaspersky Endpoint Security가 네트워크 트래픽에서 원격 측정을 제외하는 컴퓨터의 네트워크 주소입니다. **원격 주소**. Kaspersky Endpoint Security가 네트워크 트래픽에서 원격 측정을 제외하는 컴퓨터의 네트워크 주소입니다. IP 주소에 대해 IPv4 형식만 지원합니다. **애플리케이션**. Kaspersky Endpoint Security가 네트워크 트래픽에서 EDR 원격 측정을 제외하는 애플리케이션의 실행 파일 목록입니다.

파라미터	설명
제외된 파일 작업	**규칙 이름**. **파일 이름 또는 마스크**. 파일 또는 폴더의 이름이나 마스크; Kaspersky Endpoint Security는 이 파일 또는 폴더에 접근할 때 예외 규칙을 적용합니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `*` 및 `?` 문자를 지원합니다. **작업 유형**. **이전 경로**. Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **처리** 및 **부모 프로세스**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 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 DNS 작업	**규칙 이름**. Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **처리** 및 **부모 프로세스**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 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**. • **쿼리 옵션**. • **상태**. • **도메인 이름**. • **설정 유형 ID**. • **응답 데이터**.

파라미터	설명
제외된 LDAP 작업	**규칙 이름**. **LDAP 검색 범위**. **필터**. **LDAP 개체 검색을 위한 고유 이름**. **개체 속성**. Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **처리** 및 **부모 프로세스**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 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 프로세스 접근 쿼리	**규칙 이름**. **작업 유형**. **프로세스에 대한 접근 권한 요청**. **호출 스택 추적**. Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **프로세스**, **부모 프로세스**, **대상 프로세스의 파일**, **소스 프로세스에 대한 핸들** 및 **대상 프로세스에 대한 핸들**. • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 * 및 ? 문자를 지원합니다. • **명령줄 텍스트**. 파일을 실행하는 데 사용되는 명령입니다. • **규칙 트리거 기준과 이 규칙을 사용할 이벤트 유형을 지정합니다**. 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 코드 삽입	**규칙 이름**. **접근 방법**. **호출 스택**. **수정된 명령줄**. **삽입 주소**. **삽입된 DLL 이름**. Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **처리** 및 **부모 프로세스**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 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**. **WMI 작업 유형**. **원격 쿼리**. **WMI 명령을 실행한 컴퓨터의 이름**. **WMI 사용자 계정**. **실행된 WMI 명령**. **WMI 네임스페이스**. **WMI 이벤트 소비자 필터**. **생성된 WMI 이벤트 소비자의 이름**. **WMI 이벤트 소비자의 소스 코드**. Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **처리** 및 **부모 프로세스**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 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 파이프 작업	**규칙 이름**. **파이프 이름**. **작업 유형**. Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **처리** 및 **부모 프로세스**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 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**. **작업 유형**. **경로**. **값 이름**. **값**. **레지스트리 파일의 전체 이름**. Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다. **처리** 및 **부모 프로세스**: • **전체 경로**. 이름과 확장자를 포함한 파일의 전체 경로입니다. Kaspersky Endpoint Security는 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**. **장치 유형**. **장치 ID**. **장치 이름**.

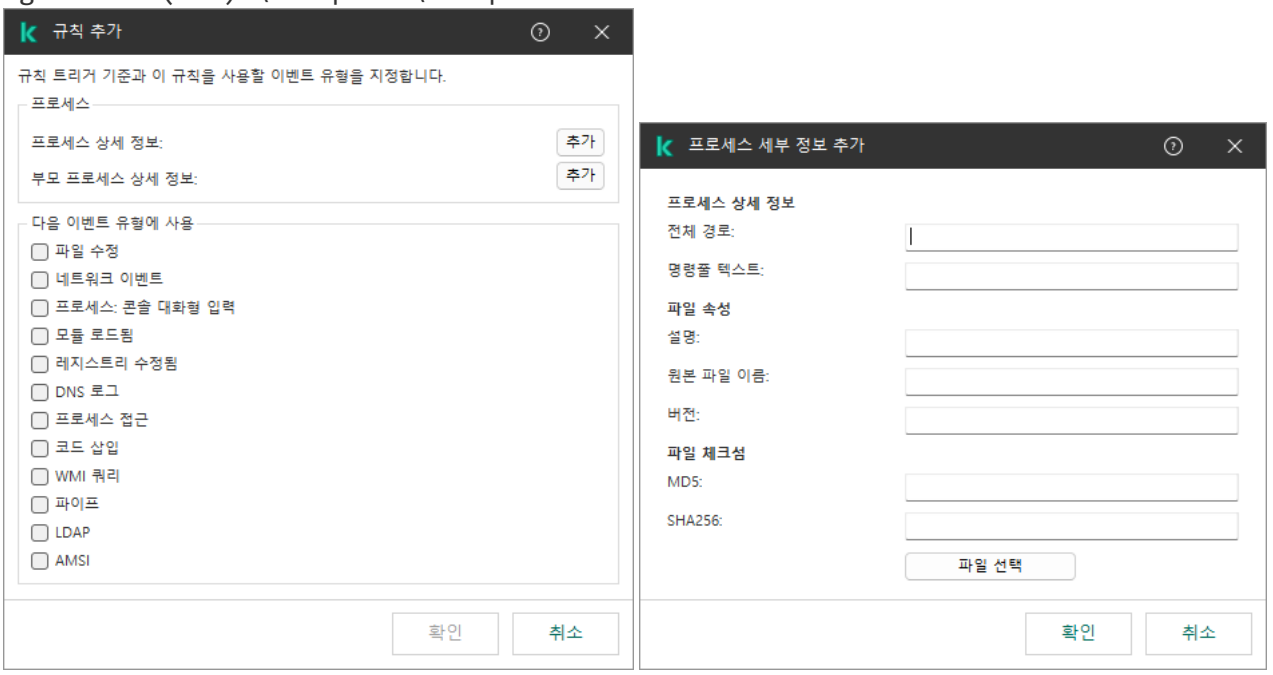
예 1. 제외된 프로세스

원격 측정에서 타사 애플리케이션(프로세스) 이벤트를 제외하려면, **제외된 프로세스** 탭에서 EDR 원격 측정 예외 창을 열고 애플리케이션의 실행 파일을 추가합니다.

Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다.

Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다. 예:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



프로세스 제외

예 1. 파일 수정

Notepad++ 애플리케이션에서 스크립트를 자주 편집하고 해당 스크립트의 수정 이벤트를 제외하려면 Notepad++ 실행 파일을 원격 측정 예외에 추가합니다.

다음과 같이 설정을 지정합니다.

- **전체 경로**: `C:\Program Files\Notepad++\notepad++.exe`
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34
- **다음 이벤트 유형에 사용**: 파일 수정

예 2. 네트워크 이벤트

원격 서버에서 파일을 관리하기 위해 WinSCP 애플리케이션을 사용하고 네트워크 이벤트를 제외하려면 WinSCP 실행 파일을 원격 측정 예외에 추가합니다.

다음과 같이 설정을 지정합니다.

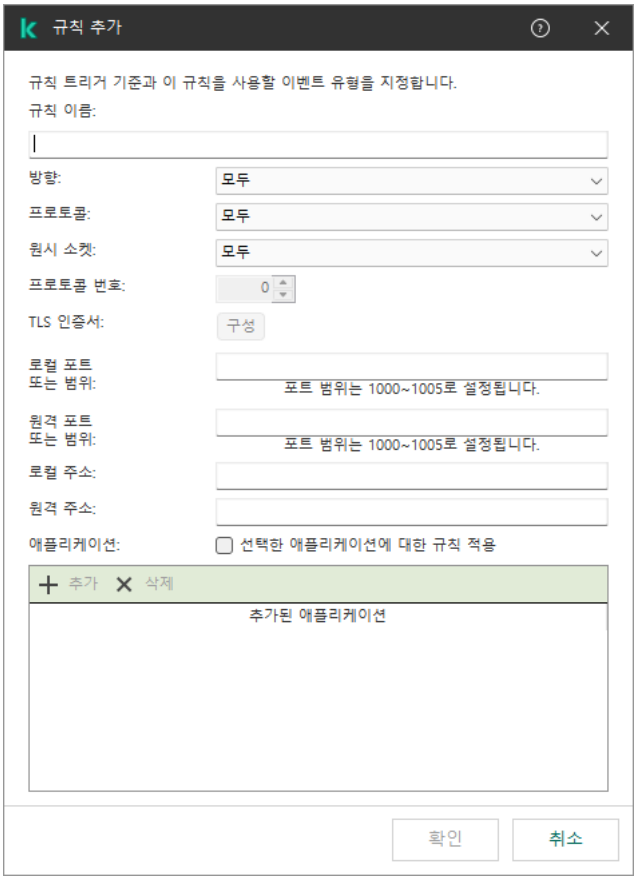
- **전체 경로**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74(선택)
- **다음 이벤트 유형에 사용**: 네트워크 이벤트

예 2. 제외된 네트워크 통신

원격 측정에서 원격 서비스 연결 이벤트를 제외하려면, **제외된 네트워크 통신** 탭에서 EDR 원격 측정 예외 창을 열고 프로토콜, 포트, 방향, IP 주소, TLS 인증서 등 연결 설정을 추가합니다.

Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다.

서브넷 주소(예: 10.28.0.0/24)를 지정할 수 없습니다. 애플리케이션은 IP 주소(예: 10.28.0.105)를 하나만 지정할 수 있습니다.



네트워크 통신 예외

기업 웹 서버를 사용하며 해당 웹 서버에 연결할 때 브라우저 이벤트를 제외하려면 서버의 IP 주소와 브라우저의 실행 파일을 원격 측정 예외에 추가합니다.

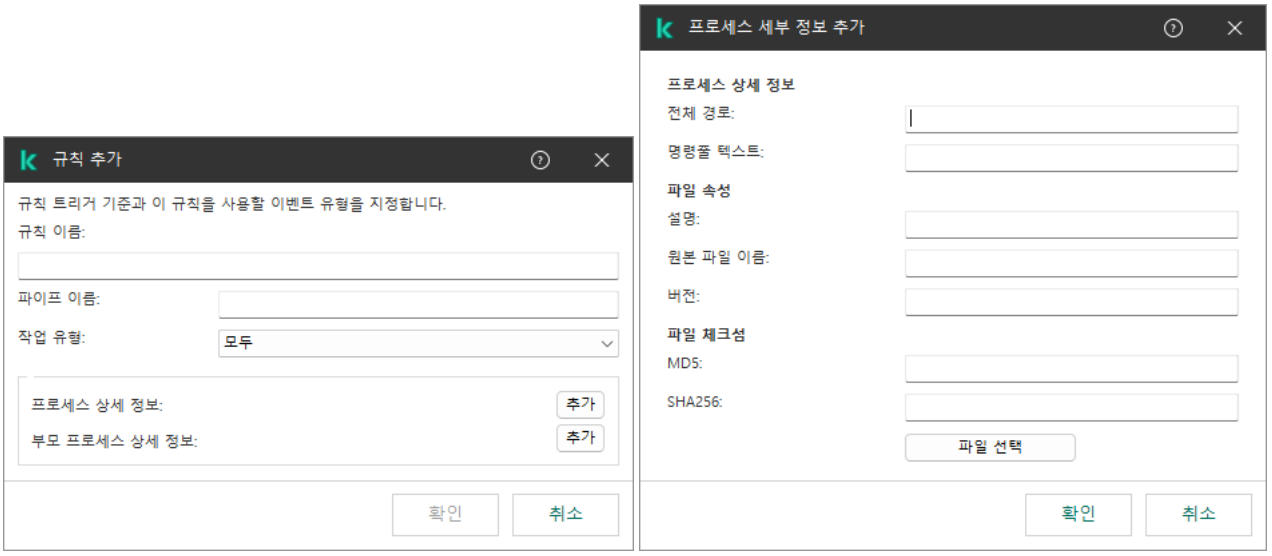
다음과 같이 설정을 지정합니다.

- **프로토콜**: TCP
- **원격 포트 또는 범위**: 443
- **원격 주소**: 10.28.0.105
- **애플리케이션**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`, `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`

예 3. 제외된 파일 작업

신뢰하는 파일을 사용하는 작업과 관련된 이벤트를 원격 측정에서 제외하려면, **제외된 파일 동작** 탭에서 EDR 원격 측정 예외 창을 열고 신뢰하는 파일을 추가합니다.

Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다.



파일 작업 제외

애플리케이션이 로그에 기록을 할 때 로그 파일 수정 이벤트를 제외하려면 로그 파일과 원격 측정 애플리케이션의 실행 파일을 추가합니다.

다음과 같이 설정을 지정합니다.

- **파일 이름 또는 마스크**: `C:\Apache24\logs\error.log`
- **작업 유형**: 파일 수정
- **전체 경로**: `C:\Apache24\bin\httpd.exe`
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34

예 4. 제외된 레지스트리 수정

원격 측정에서 레지스트리 수정 이벤트를 제외하려면, **제외된 레지스트리 변경** 탭에서 EDR 원격 측정 예외 창을 열고 레지스트리 키를 추가합니다.

Kaspersky Endpoint Security는 규칙 트리거 기준을 논리곱(logical AND)과 결합합니다.

애플리케이션이 레지스트리 값을 자주 수정하며 이러한 레지스트리 수정 이벤트를 원격 측정에서 제외하려면 애플리케이션의 레지스트리 키와 실행 파일을 원격 측정 예외에 추가합니다.

다음과 같이 설정을 지정합니다.

- **작업 유형**: 수정
- **경로**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64
- **전체 경로**: `C:\Program Files\PuTTY\putty.exe`
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34

KATA Sandbox

Kaspersky Anti Targeted Attack Platform에는 Sandbox(KATA Sandbox) 구성 요소가 포함됩니다. *Sandbox*는 컴퓨터에서 지능형 보안 위협을 탐지할 수 있는 기술입니다. Sandbox는 조직의 IT 인프라에 대한 표적 공격의 활동 특성 및 악성 활동 탐지를 위해 개체 행동을 분석합니다. Sandbox는 Microsoft Windows 운영 체제(Sandbox 서버)의 가상 이미지가 배포된 특수 서버의 개체를 분석하고 검사합니다. 이 솔루션에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

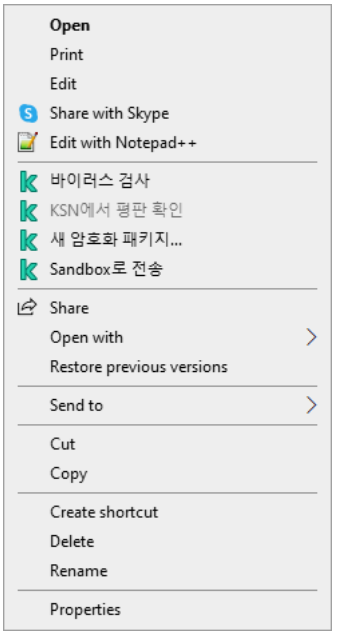
KATA Sandbox를 활성화하려면 KATA 또는 KEDR 기능이 포함된 라이센스 키가 필요합니다. 사용 가능한 기능에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

KATA Sandbox를 통해 다음 모드에서 파일을 검사할 수 있습니다.

- *수동*. 사용자가 마우스 오른쪽 메뉴에서 검사할 파일을 수동으로 제출합니다(**Sandbox로 전송**). Sandbox로 파일을 보낼 때 애플리케이션은 안티 바이러스 데이터베이스를 사용해 파일을 검사합니다.
- *자동*. 애플리케이션이 자동으로 개체를 탐지하여 검사를 위해 Sandbox에 제출합니다.

파일이 Sandbox로 보내진 후에도 사용자는 파일에 계속 접근할 수 있습니다. Kaspersky Endpoint Security는 해당 이벤트를 기록하고 이벤트를 Kaspersky Security Center 및 Kaspersky Anti Targeted Attack Platform 콘솔에 보냅니다. Sandbox가 악성 활동을 탐지하면 Kaspersky Endpoint Security는 자동으로 보안 위협 대응 활동을 수행합니다(예: 개체를 삭제하고 중요 영역 검사를 시작).

KATA Sandbox가 수동 모드에서 작동하려면 Kaspersky Anti Targeted Attack Platform 7.0 이상이 배포되어 있어야 합니다. KATA Sandbox가 자동 모드에서 작동하려면 Kaspersky Anti Targeted Attack Platform 8.0 이상이 배포되어야 합니다.



마우스 오른쪽 메뉴로 KATA Sandbox에서 검사

KATA Sandbox와 내장 에이전트 통합

KATA Sandbox와 통합하려면 Sandbox 구성 요소를 추가해야 합니다. Sandbox 구성 요소는 설치 또는 업그레이드 중 선택하거나 *애플리케이션 구성 요소 변경* 작업으로 선택할 수 있습니다.

검사를 위해 파일을 보내려면 KATA Sandbox와의 통합을 활성화하고 솔루션 내에 배포된 Central Node 서버를 추가해야 합니다. 구성 요소는 Kaspersky Security Center 웹 콘솔을 통해서만 관리할 수 있습니다. 관리 콘솔(MMC)로는 이 구성 요소를 관리할 수 없습니다.

KATA Sandbox와의 통합을 활성화 또는 비활성화하려면 다음과 같이 하십시오.

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **Sandbox**으로 이동합니다.
5. **Sandbox와 통합 활성화됨** 토글을 사용하여 구성 요소를 활성화 또는 비활성화합니다.

6. KATA Sandbox 작동 모드를 선택합니다.

   - **수동**. 사용자가 마우스 오른쪽 메뉴에서 검사할 파일을 수동으로 제출합니다(**Sandbox로 전송**).
   - **자동**. 애플리케이션이 자동으로 개체를 탐지하여 검사를 위해 Sandbox에 제출합니다.
   - **조합**.

7. **연결 설정** 링크를 클릭합니다.

8. Central Node 서버 연결 설정을 구성합니다:

   - **시간 초과(msec)**. Central Node 서버 연결에 대한 시간 초과입니다. 구성된 시간 초과를 넘으면 Kaspersky Endpoint Security가 다음 서버로 요청을 보냅니다. 연결 속도가 느리거나 연결이 불안정하다면 서버의 연결 시간 초과 설정을 늘릴 수 있습니다. 요청 시간 초과 설정은 0.5초 이하를 권장합니다.
   - **요청 대기열**. 요청 대기열 폴더의 크기입니다. Sandbox에서 검사하기 위해 여러 개체를 전송하는 경우 Kaspersky Endpoint Security는 요청 대기열을 생성합니다. 기본적으로 요청 대기열 폴더의 크기는 100MB로 제한됩니다. 최대 크기에 도달하면 Sandbox는 대기열에 새 요청 추가를 중지하고 해당 이벤트를 Kaspersky Security Center로 보냅니다. 서버 구성에 따라 요청 대기열 폴더의 크기를 구성할 수 있습니다.
   - **서버 TLS 인증서**. Central Node 서버와의 신뢰할 수 있는 연결을 구성하려면 TLS 인증서를 준비해야 합니다. 그런 다음 정책을 사용하여 컴퓨터에 인증서를 추가해야 합니다. 또한 Central Node 서버에 인증서를 추가해야 합니다.
   - **양방향 인증 사용**. Kaspersky Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 Endpoint Security 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.

9. **Sandbox 서버에 연결** 블록에서 **추가** 버튼을 누릅니다.

10. 창이 열리면 Central Node 서버 주소(IPv4, IPv6, DNS) 및 포트를 입력합니다.

    가상 이미지 배포 및 Central Node 서버 구성에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

11. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

    결과적으로 Sandbox 구성 요소가 활성화됩니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Sandbox** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

보안 위협 대응 활동 구성

Sandbox가 악성 활동을 탐지하면 Kaspersky Endpoint Security는 자동으로 보안 위협 대응 활동을 수행합니다(예: 개체를 삭제하고 중요 영역 검사를 시작).

보안 위협 대응 활동을 구성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성 → Sandbox**으로 이동합니다.
5. **위협 탐지 시 처리 방법** 블록에서 필요한 동작을 선택합니다.
   - **격리 저장소로 사본을 옮기고 개체 삭제**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 컴퓨터에서 발견된 악성 개체를 삭제합니다. 개체를 삭제하기 전에 Kaspersky Endpoint Security는 나중에 개체를 복원해야 할 때를 대비하여 백업 복사본을 생성합니다. Kaspersky Endpoint Security는 백업 복사본을 격리 저장소로 이동합니다.
   - **중요 영역 검사 실행**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 *중요 영역 검사* 작업을 실행합니다. Kaspersky Endpoint Security는 기본적으로 커널 메모리, 실행 중인 프로세스 및 디스크 부트 섹터를 검사합니다.
   - **IOC 검사 작업 생성**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 자동으로 *IOC 검사(자율적 IOC 검사 작업)*를 생성합니다. 이 작업에 대해 실행 모드, 검사 범위 및 IOC 탐지에 대한 작업(개체 삭제, *중요 영역 검사* 작업 실행)을 구성할 수 있습니다. *IOC 검사* 작업에 대한 다른 설정을 수정하려면 작업 설정으로 이동합니다.
6. 필요한 경우 **IOC 검사 범위** 블록에서 *IOC 검사* 작업 설정을 구성합니다.
   - **중요한 파일 영역**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 컴퓨터의 중요한 파일 영역(커널 메모리 및 부트 섹터)에서만 IOC 검사를 수행합니다.
   - **컴퓨터 시스템 드라이브의 파일 영역**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 컴퓨터의 시스템 드라이브에서 IOC 검사를 수행합니다.
7. 필요한 경우 **IOC 검사 작업 실행** 블록에서 *IOC 검사* 작업 설정을 구성합니다.
   - **수동**. 편리한 시간에 *IOC 검사* 작업을 수동으로 시작할 수 있는 실행 모드입니다.
   - **자동**. 보안위협이 탐지되면 Kaspersky Endpoint Security가 자동으로 *IOC 검사* 작업을 실행하는 실행 모드입니다.
   - **컴퓨터가 유휴 상태일 때만 실행**. 화면 보호기가 활성화되었거나 화면이 잠겨 있을 때 Kaspersky Endpoint Security가 *IOC 검사* 작업을 실행하는 실행 모드입니다. 사용자가 컴퓨터의 잠금을 해제하면 Kaspersky Endpoint Security가 작업을 일시 중지합니다. 따라서 작업을 완료하는 데 며칠이 걸릴 수 있습니다.
8. *IOC 검사*에 대한 고급 작업 설정을 구성합니다.
9. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

EDR(KATA)용 KEA에서 KES로의 마이그레이션 가이드

Kaspersky Endpoint Security for Windows는 12.1 버전부터 이제 Kaspersky Anti Targeted Attack Platform 솔루션의 일부인 Kaspersky Endpoint Detection and Response 구성 요소를 관리하기 위한 내장 에이전트가 포함됩니다. 이제 Kaspersky Endpoint Agent 애플리케이션이 없어도 EDR(KATA)을 이용할 수 있습니다. Kaspersky Endpoint Agent의 모든 기능은 Kaspersky Endpoint Security에 의해 실행됩니다. Kaspersky Anti Targeted Attack Platform 서버의 부하는 동일하게 유지됩니다.

Kaspersky Endpoint Agent가 설치된 컴퓨터에 Kaspersky Endpoint Security를 배포하면 Kaspersky Anti Targeted Attack Platform(EDR) 솔루션이 Kaspersky Endpoint Security와 계속해서 작동합니다. 또한 Kaspersky Endpoint Agent가 컴퓨터에서 제거됩니다. Kaspersky Endpoint Security를 버전 12.1 이상으로 업데이트하면 시스템에서 동일한 행동이 발생합니다.

Kaspersky Endpoint Security는 Kaspersky Endpoint Agent와 호환되지 않습니다. 이러한 애플리케이션을 한 컴퓨터에 다 설치할 수는 없습니다.

Kaspersky Endpoint Security가 Endpoint Detection and Response(KATA)의 일부로 작동하려면 다음 조건을 충족해야 합니다.

- Kaspersky Anti Targeted Attack Platform 버전 5.0 이상.
- Kaspersky Security Center 버전 14.2 이상(네트워크 에이전트 포함) 이전 버전의 Kaspersky Security Center에서는 Endpoint Detection and Response(KATA)의 기능을 활성화할 수 없습니다.

[KES+KEA] 구성을 EDR(KATA)용 [KES+내장형 에이전트]로 마이그레이션하는 단계

1. **Kaspersky Endpoint Security 관리 플러그인 업그레이드**

   EDR(KATA) 구성요소는 Kaspersky Endpoint Security 관리 플러그인 버전 12.1 이상을 사용하여 관리할 수 있습니다. 사용하고 있는 Kaspersky Security Center 콘솔 유형에 따라 관리 콘솔(MMC)의 관리 플러그인 또는 웹 콘솔의 웹 플러그인을 업데이트합니다.

2. **정책 및 작업 마이그레이션**

   Kaspersky Endpoint Agent 설정을 Windows용 Kaspersky Endpoint Security로 이전합니다. 다음과 같은 옵션을 사용할 수 있습니다.

   - Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로 마이그레이션하는 마법사입니다. Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로 마이그레이션하는 마법사는 웹 콘솔에서만 작동합니다.

     Kaspersky Endpoint Agent에서 웹 콘솔의 Kaspersky Endpoint Security로 정책 및 작업 설정을 마이그레이션하는 방법

     웹 콘솔 메인 창에서 **동작 → Kaspersky Endpoint Agent에서 마이그레이션**을 선택합니다.

     정책 및 작업 마이그레이션 마법사가 열립니다. 마법사의 지침을 따릅니다.

1단계. 정책 마이그레이션

마이그레이션 마법사가 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent 정책의 설정을 병합하는 새 정책을 만듭니다. 정책 목록에서 Kaspersky Endpoint Security 정책에 병합하고자 하는 Kaspersky Endpoint Agent 정책 설정을 선택합니다. Kaspersky Endpoint Agent 정책을 클릭해서 설정을 병합할 Kaspersky Endpoint Security 정책을 선택합니다. 알맞은 정책을 선택했는지 확인하고 다음 단계로 넘어갑니다.

2단계. 정책 마이그레이션

마이그레이션 마법사는 EDR(KATA) 작업을 지원하지 않습니다. 이 단계를 건너뜁니다.

3단계. 마법사 완료

마법사를 끝냅니다. 마법사를 진행한 결과 새로운 Kaspersky Endpoint Security 정책이 생성됩니다. 정책이 Kaspersky Endpoint Security와 Kaspersky Endpoint Agent의 설정을 병합합니다. 정책의 이름은 *<Kaspersky Endpoint Security 정책 이름> & <Kaspersky Endpoint Agent 정책 이름>*입니다. 새 정책은 *비활성* 상태입니다. 계속하려면 Kaspersky Endpoint Agent와 Kaspersky Endpoint Security 정책의 상태를 *비활성*으로 바꾸고 새로 병합된 정책을 활성화합니다.

웹 콘솔의 마이그레이션 마법사가 다음 정책 설정을 건너뛰고 마이그레이션하지 않기 때문입니다.

- **연결 설정**에 대한 설정 수정 금지('잠금').

  기본적으로 설정을 수정할 수 있습니다("잠금"이 열립니다). 따라서 설정이 컴퓨터에서 적용되지 않습니다. 설정 수정을 금지하고 '잠금'을 종료해야 합니다.

- 암호화 컨테이너.

  Central Node 서버로 연결하기 위해 양방향 인증을 사용하는 경우, 암호화 컨테이너를 다시 추가해야 합니다.

마이그레이션 마법사가 이 설정을 마이그레이션하지 않기 때문에 컴퓨터를 Central Node 서버로 연결할 때 오류가 발생할 수 있습니다. 이 오류를 해결하려면 정책 속성으로 이동해서 연결 설정을 구성해야 합니다.

- 표준 정책 및 작업 배치 변환 마법사 정책 및 작업 매치 변환 마법사는 관리자 콘솔(MMC)에서만 사용할 수 있습니다. 정책 및 작업 배치 변환 마법사에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

Kaspersky Endpoint Security가 서버에서 올바르게 작동하게 하려면, 서버 작용과 관련된 중요 파일을 신뢰 구역에 추가하는 것이 좋습니다. SQL 서버의 경우 MDF 및 LDF 데이터베이스 파일을 추가해야 합니다. Microsoft Exchange 서버의 경우 CHK, EDB, JRS, LOG 및 JSL 파일을 추가해야 합니다. 마스크(예: `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`)를 사용할 수도 있습니다.

Kaspersky Endpoint Security 12.6 for Windows부터 검사 예외 및 신뢰하는 애플리케이션 이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다.

EDR 원격 측정 예외 규칙은 Kaspersky Endpoint Agent 정책을 Kaspersky Endpoint Security 정책으로 마이그레이션하지 않습니다. Kaspersky Endpoint Security에는 자체 제외 도구인 신뢰하는 애플리케이션이 있습니다. 개별 EDR 원격 측정 예외 규칙이 없어도 Kaspersky Endpoint Agent와 비교하여 사용자 컴퓨터에 추가 부하가 발생하지 않도록 Kaspersky Endpoint Security의 동작이 최적화되어 있습니다. Kaspersky Endpoint Security는 EDR(KATA)뿐만 아니라 애플리케이션 보호 구성 요소의 동작에 대해서도 원격 측정을 사용합니다. 따라서 개별 EDR 원격 측정 예외 규칙을 전송할 필요가 없습니다. 컴퓨터 성능이 저하된다고 생각되면 애플리케이션의 성능을 확인하십시오(7단계 동작 확인 참조).

3 EDR(KATA) 기능 라이센스

Kaspersky Anti Targeted Attack Platform 솔루션의 일부로 Kaspersky Endpoint Security를 활성화하려면 Kaspersky Endpoint Detection and Response(KATA) 애드온에 대한 별도 라이센스가 필요합니다. *키 추가* 작업을 통해 키를 추가할 수 있습니다. 결과적으로 *Kaspersky Endpoint Security*와 *Kaspersky Endpoint Detection and Response(KATA)* 키가 애플리케이션에 추가됩니다.

이전에 활성화된 EDR Optimum 또는 EDR Expert 기능이 있는 컴퓨터에서 Kaspersky Endpoint Detection and Response(KATA) 애드온 라이센스를 부여하려면 다음과 같은 특별한 고려 사항이 필요합니다.

- EDR Optimum 또는 EDR Expert 기능이 있는 Kaspersky Endpoint Security 라이센싱을 위해 *키 파일*을 사용하는 경우 별도의 Kaspersky Endpoint Detection and Response(KATA) 애드온용 키를 추가할 수 없습니다. 라이센스를 위해 활성화 코드를 사용하도록 전환하거나 서비스 제공업체에 문의하여 Kaspersky Endpoint Security 및 EDR 기능을 활성화하기 위한 새 키 파일을 얻을 수 있습니다. 서비스 제공업체는 라이센스를 위해 하나 이상의 키 파일을 제공합니다.

- EDR Optimum 또는 EDR Expert 기능이 없는 Kaspersky Endpoint Security 라이센스를 위해 *키 파일*을 사용하는 경우 키 파일 재발급 없이 별도의 Kaspersky Endpoint Detection and Response(KATA) 애드온용 키를 추가할 수 있습니다.

- 라이센스를 위해 *활성화 코드*를 사용하는 경우 Kaspersky 활성화 서버가 자동으로 키를 재발급하고 EDR(KATA) 기능을 자동으로 사용할 수 있게 됩니다. 이 경우 EDR Optimum과 EDR Expert는 비활성화됩니다.

- Kaspersky Endpoint Security를 사용하면 Kaspersky Endpoint Security 키와 애드온 유형의 키 등 최대 2개의 활성 키를 추가할 수 있습니다. 최대 2개의 예약 키를 추가할 수도 있습니다. Kaspersky Endpoint Security 예약 키 1개와 애드온 유형의 예약 키 1개입니다.

4 Kaspersky Endpoint Security 애플리케이션 설치 / 업그레이드

애플리케이션 설치 또는 업그레이드 중에 EDR(KATA) 기능을 마이그레이션하려면 원격 설치 작업을 사용하는 것이 좋습니다. 원격 설치 작업을 생성할 때 설치 패키지 설정에서 EDR(KATA) 구성요소를 선택해야 합니다.

다음 방법을 사용하여 원격으로 애플리케이션을 업그레이드할 수도 있습니다:

- Kaspersky 업데이트 서비스 사용.

- 로컬에서 설치 마법사 실행.

Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 애플리케이션이 설치된 컴퓨터에서 애플리케이션을 업데이트할 때 구성 요소의 자동 선택을 지원합니다. 구성 요소의 자동 선택은 애플리케이션을 업그레이드하는 사용자 계정의 권한에 달려 있습니다.

시스템 계정(SYSTEM)의 EXE 또는 MSI 파일을 사용해 Kaspersky Endpoint Security를 업그레이드한다면 Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 대한 접근 권한을 획득합니다. 따라서 컴퓨터에 Kaspersky Endpoint Agent가 설치되어 있고 EDR(KATA) 솔루션이 활성화되어 있는 경우, Kaspersky Endpoint Security 설치 프로그램은 자동으로 구성 요소의 세트를 구성하고 EDR(KATA) 구성 요소를 선택합니다. 이에 따라 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다. 시스템 계정(SYSTEM)에서 MSI 설치 프로그램을 실행하면 주로 Kaspersky 업데이트 서비스를 통해 업그레이드하거나 Kaspersky Security Center를 통해 설치 패키지를 배포할 때 수행됩니다.

별도의 권한이 없는 사용자 계정으로 MSI 파일을 사용하여 Kaspersky Endpoint Security를 업그레이드한다면, Kaspersky Endpoint Security는 Kaspersky 솔루션의 현재 라이센스에 접근할 권한이 없습니다. 이 경우 Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 구성 요소 세트를 기반으로 자동으로 구성 요소를 선택합니다. 그리고 나서 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다.

Kaspersky Endpoint Security에서는 컴퓨터를 재시작하지 않고도 업그레이드가 지원됩니다. 정책 속성에서 애플리케이션 업그레이드 모드를 선택할 수 있습니다.

5 애플리케이션 동작 확인

애플리케이션 설치 또는 업그레이드 후에 Kaspersky Security Center 콘솔 상태가 *심각*으로 표시되면 다음을 수행합니다.

- 컴퓨터에 Network Agent 버전 13.2 이상이 설치되었는지 확인합니다.
- *애플리케이션 구성 요소 상태 리포트*를 확인하여 내장 에이전트의 작동 상태를 확인합니다. 구성 요소의 상태가 *설치 안 됨*이라면 *애플리케이션 구성 요소 변경* 작업으로 구성 요소를 설치합니다. 컴퓨터가 *라이센스에 포함되지 않음* 상태에 있는 경우, 내장 에이전트에 기능을 활성화했는지 확인하십시오.
- Kaspersky Endpoint Security for Windows의 새 정책에서 Kaspersky Security Network 진술문을 수락해야 합니다.

6 Kaspersky Anti Targeted Attack Platform 서버에 대한 연결 확인

Kaspersky Anti Targeted Attack Platform 서버에 대한 연결을 확인합니다. 이를 위해서는 다음과 같이 하십시오.

1. 유효한 인증서가 있는지 확인하십시오.
2. 서버 연결 설정을 확인하십시오.
3. 이벤트 로그를 확인하십시오.

   서버에 대한 연결이 설정되면 애플리케이션은 이벤트 *EDR Expert 서버로 연결 완료*를 전송합니다. 연결 성공 이벤트가 없고 연결 오류가 발생한 이벤트가 없는 경우, 이벤트 로그 설정을 확인하고 Endpoint Detection and Response(KATA)에 대한 이벤트 전송을 활성화합니다.

서버 연결 상태는 Kaspersky Security Center 콘솔의 컴퓨터 상태에 영향을 주지 않습니다. 따라서 서버에 연결되어 있지 않아도 컴퓨터는 여전히 *정상* 상태입니다. 이벤트 로그를 확인하여 서버에 대한 연결을 확인하십시오.

7 성능 확인

애플리케이션을 설치하거나 업데이트한 후 컴퓨터 성능이 느려진 경우 데이터 전송을 최적화할 수 있습니다. 이를 위해서는 다음과 같이 하십시오.

1. EDR(KATA) 구성 요소를 비활성화하고 성능 저하가 EDR(KATA)로 인한 것인지 확인합니다.
2. 신뢰하는 애플리케이션의 경우 콘솔 입력 작업에서 원격 측정 수집을 끕니다(기본적으로 활성화됨).

3. 컴퓨터 성능을 저하시키는 애플리케이션을 신뢰하는 애플리케이션 목록에 추가합니다.

4. Kaspersky 기술 지원에 문의하십시오. 지원 전문가가 Kaspersky Anti Targeted Attack Platform에서 원격 측정 필터링을 구성하는 데 도움을 제공합니다. 이는 트래픽 양을 감소시킵니다. 컴퓨터 성능이 특정 애플리케이션의 영향을 받는 경우 해당 애플리케이션의 배포 패키지를 요청 작업에 첨부하십시오.

Endpoint Detection and Response Expert(on-premise)



Kaspersky Endpoint Security for Windows는 Kaspersky Endpoint Detection and Response Expert(on-premise) 솔루션과의 통합을 지원합니다. *Kaspersky Endpoint Detection and Response Expert(on-premise)*는 기업 사이버 보안 솔루션으로, Kaspersky 애플리케이션을 통해 조직에서 대부분의 사이버 위협에 대응하고 가장 중요한 위협 전파 시나리오를 처리하도록 지원합니다. EDR Expert(on-premise) 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-premise)는 기업 인프라에서 수신한 로그 및 원격 측정을 확인하여 공격을 자동으로 탐지하며, Kaspersky 애플리케이션 타사 정보 보안 제품의 이벤트를 포함하여 EDR Expert(on-premise)에 수집된 모든 이벤트를 결합한 조사 그래프를 통해 사고를 조사하도록 지원합니다.

고급 인시던트에 대응하기 위해 EDR Expert(on-premise)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(이하 "KSN") 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 Endpoint Security는 기업 IT 인프라의 개별 컴퓨터에 설치되며 프로세스, 개방형 네트워크 연결 및 수정되는 파일을 계속해서 모니터링합니다. 컴퓨터의 이벤트에 대한 정보(원격 측정)가 EDR Expert(on-premise) 서버로 전송됩니다. 이때, Kaspersky Endpoint Security는 애플리케이션에서 발견한 보안 위협에 대한 정보와 이를 처리한 결과에 대한 정보도 원격 측정 수집 서버로 보냅니다.

EDR Expert(on-premise) 통합은 Kaspersky Security Center 콘솔에서 구성됩니다. 그러면 이 내장 에이전트가 Open Single Management Platform(OSMP)을 사용하여 관리됩니다(작업 실행, 격리된 개체 관리, 리포트 보기 및 기타 작업 등).

EDR Expert(on-premise) 작업을 위한 Kaspersky Endpoint Security 구성

EDR Expert(on-premise) 작업에 다음 구성을 사용할 수 있습니다.

- **[KES+내장 에이전트]**. 이 구성에서 Kaspersky Endpoint Security는 컴퓨터 보안을 책임지는 애플리케이션이자 EDR Expert(on-premise) 작업을 위한 애플리케이션으로서 작동합니다. EDR Expert(on-premise)용 내장 에이전트는 Kaspersky Endpoint Security 12.11 for Windows 이상의 버전에서 사용할 수 있습니다.
- **[타사 EPP+EDR Agent]**. 이 구성에서는 타사 EPP(Endpoint Protection Platform)를 통해 IT 인프라 보안이 제공됩니다. Endpoint Detection and Response Agent(EDR Agent)의 Kaspersky Endpoint Security에서 EDR Expert(on-premise)과의 상호 작용을 지원합니다. 이 구성에서 EDR Agent는 타사 EPP 애플리케이션과 호환됩니다. EDR Expert(on-premise)용 EDR Agent는 Kaspersky Endpoint Security 12.11 for Windows 이상의 버전에서 사용할 수 있습니다.

EDR Expert(on-premise)와 내장 에이전트 통합

Kaspersky Endpoint Detection and Response Expert(on-premise) 솔루션과 통합하려면 Endpoint Detection and Response Expert(on-premise) 구성 요소를 추가하고 Kaspersky Endpoint Security를 구성해야 합니다.

EDR Optimum, EDR Expert 및 EDR Expert(on-premise) 구성 요소는 서로 호환되지 않습니다.

Endpoint Detection and Response Expert(on-premise)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-premise) 구성 요소가 켜져 있습니다.
- EDR Expert(on-premise)의 동작을 보장하는 애플리케이션 구성 요소가 활성화되고 작동합니다. EDR Expert(on-premise)의 동작을 보장하는 구성 요소는 다음과 같습니다.
  - 파일 위협 보호
  - 웹 위협 보호
  - 메일 위협 보호
  - 익스플로잇 방지
  - 행동 탐지
  - 호스트 침입 방지
  - 복원 엔진
  - 적응형 이상 행위 제어

EDR Expert(on-premise) 통합 설정에는 다음 단계가 포함됩니다:

1. **EDR Expert(on-premise) 구성 요소 설치**

   EDR Expert(on-premise) 구성 요소는 설치 또는 업그레이드 중 선택하거나 *애플리케이션 구성 요소 변경* 작업으로 선택할 수 있습니다.

   > 새 구성 요소로 애플리케이션 업그레이드를 완료하려면 컴퓨터를 다시 시작해야 합니다.

2. **Kaspersky Endpoint Detection and Response Expert(on-premise) 활성화**

   EDR Expert(on-premise)(Kaspersky Endpoint Detection and Response(on-premise) 애드온) 사용을 위해 별도 라이센스 구매해야 합니다.

   이 기능은 Kaspersky Endpoint Detection and Response Expert(on premise)의 키를 별도로 추가한 후에 이용할 수 있습니다. 결과적으로 Kaspersky Endpoint Security 키와 Kaspersky Endpoint Detection and Response Expert(on premise) 두 개의 키가 컴퓨터에 설치됩니다.

   독립 실행형 Endpoint Detection and Response Expert(on premise) 기능의 라이센스 사용은 Kaspersky Endpoint Security의 라이센스 사용과 같습니다.

   EDR Expert(on-premise) 기능이 라이센스에 포함되며 애플리케이션의 로컬 인터페이스에서 실행되고 있는지 확인하십시오.

3. **원격 측정 수집 서버 및 응답 서버에 연결**

   Kaspersky Endpoint Detection and Response Expert(on-premise)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 얻을 수 있습니다(Kaspersky Endpoint Detection and Response Expert(on-premise) 도움말의 지침 참조). 그런 다음 Kaspersky Endpoint Security에 TLS 인증서를 추가해야 합니다(아래 지침 참조).

   기본적으로 Kaspersky Endpoint Security는 서버의 TLS 인증서만 확인합니다. 보다 안전한 연결을 위해, 서버에서 컴퓨터 확인을 추가로 활성화할 수 있습니다(양방향 인증). 이 확인을 활성화하려면 서버와 Kaspersky Endpoint Security 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 얻을 수 있습니다(Kaspersky Endpoint Detection and Response Expert(on-premise) 도움말의 지침 참조).

   웹 콘솔을 사용하여 Kaspersky Endpoint Security 컴퓨터를 EDR Expert(on-premise)에 연결하는 방법

   1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.
   2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
      정책 속성 창이 열립니다.
   3. **애플리케이션 설정** 탭을 선택합니다.
   4. **내장 에이전트 구성** → **Endpoint Detection and Response Expert(on premise)**로 갑니다.
   5. **Endpoint Detection and Response Expert(on-premise) 활성화됨** 토글을 켭니다.
   6. EDR Expert(on-premise)을 구성하려면 솔루션 목록에서 **Endpoint Detection and Response Expert(버전 8.0 이상)**를 선택합니다.

7. *원격 측정 수집 서버* 연결을 구성합니다.

   a. **원격 측정 수집 서버에 연결** 블록에서 **연결 설정** 링크를 클릭합니다.

   b. 원격 측정 수집 서버 연결을 구성합니다.

   - **시간 초과(초)**. 최대 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 서버에 연결을 시도합니다.
   - **서버 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-premise) 도움말의 지침 참조).
   - **양방향 인증 사용**. Kaspersky Endpoint Security와 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-premise) 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.

   c. **확인**을 누릅니다.

   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 Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

   e. 필요한 경우 원격 측정을 구성합니다.

8. *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 Endpoint Security가 보안 위협 대응 작업을 수신하고 작업 결과를 전송합니다.

   b. **연결 설정** 링크를 클릭합니다.

   c. 응답 서버 연결 구성:

   - **시간 초과(초)**. 최대 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 서버에 연결을 시도합니다.
   - **서버 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-premise) 도움말의 지침 참조).

- **양방향 인증 사용**. Kaspersky Endpoint Security와 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-premise) 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**을 누릅니다.

e. 응답 서버를 추가합니다. 이렇게 하려면 서버 주소(IPv4, IPv6)와 서버에 연결할 포트를 지정하십시오.

여러 개의 대응 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

9. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

그러면 컴퓨터가 Open Single Management Platform(OSMP)에 추가됩니다. *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **Endpoint Detection and Response Expert(on-premise)** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

EDR Expert(on-premise) 원격 측정 설정 구성

*원격 측정*은 보호된 컴퓨터에서 발생한 이벤트 목록입니다. Kaspersky Endpoint Security는 원격 측정 데이터를 분석하여 동기화하는 동안 원격 측정 수집 서버로 보냅니다. 원격 측정 이벤트는 거의 지속적으로 서버에 도착합니다. Kaspersky Endpoint Security는 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 Endpoint Security 정책에서 동기화 동작을 구성하고 네트워크 부하에 맞는 최적의 값을 선택할 수 있습니다(아래 지침 참조).

Kaspersky Endpoint Security와 서버가 서로 연결되어 있지 않으면 애플리케이션이 새 이벤트를 대기시킵니다. 연결이 복원되면 Kaspersky Endpoint Security가 대기열에 있는 이벤트들을 적절한 순서로 서버에 보냅니다. 서버 과부하를 방지하기 위해 Kaspersky Endpoint Security는 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** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.

4. **내장 에이전트 구성** → **Endpoint Detection and Response Expert(on premise)**로 갑니다.

5. EDR Expert(on-premise)을 구성하려면 솔루션 목록에서 **Endpoint Detection and Response Expert(버전 8.0 이상)**를 선택합니다.

6. **데이터 전송 설정** 블록에서 **원격 측정 수집 서버로 원격 측정 전송** 확인란이 선택되어 있는지 확인합니다.

7. 필요한 경우, **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.

   - **최대 이벤트 패키지 수**. 버퍼가 이벤트로 가득 차면 애플리케이션이 서버와 동기화를 수행합니다. 기본 설정은 이벤트 1024개입니다.

9. 필요한 경우 **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 Endpoint Security가 이벤트 전송을 중지합니다.

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 Endpoint Security는 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 Endpoint Security는 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 Endpoint Security는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.

13. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

EDR Expert(on-premise) 원격 측정 예외

성능을 개선하고 원격 측정 수집 서버로의 데이터 전송을 최적화하기 위해 원격 측정 예외를 추가할 수 있습니다. 예를 들어 개별 애플리케이션의 네트워크 통신 데이터를 전송하지 않도록 선택할 수 있습니다.

너무 많은 규칙을 사용하면 원격 측정 수집 서버의 부하가 증가하고 컴퓨터 성능이 저하될 수 있습니다. 필요한 규칙만 추가할 것을 권장합니다.

웹 콘솔 및 Cloud Console에서 원격 측정 예외를 생성하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 원격 측정 설정**으로 이동합니다.
5. **EDR Expert(on-premise) 원격 측정** 탭을 선택합니다.
6. **일반 예외** 블록에서 **추가** 버튼을 클릭합니다.
   예외 규칙 추가 창이 열립니다.
7. 필요시 규칙의 상태를 변경합니다. 기본적으로 규칙이 활성화됩니다.
8. 규칙의 이름을 입력합니다.
9. 규칙이 트리거될 때 수행할 작업 선택:
   - **수집하지 않음**. 필터링된 이벤트가 전송되는 원격 측정에서 제외됩니다.
   - **IOA 제외**. IOA 규칙 트리거 이벤트가 전송되는 원격 측정에서 제외됩니다.
10. **IOA 제외** 옵션을 선택한 경우 예외 규칙에 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-premise) 도움말 을 참조하십시오.
11. 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.

연산자	설명
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.
contains	조건에 지정된 값이 필드 값에 포함되어 있으면 해당 이벤트가 필터링되어 제외됩니다.
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.

12. 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 일치하는 이벤트를 선택함을 의미합니다.
    - **NOT** (이 연산자를 사용하려면 **NOT을 앞에 추가** 옵션을 선택) 의미는 필터가 지정된 조건 중 어느 것도 충족하지 않는 이벤트를 선택한다.

    조건과 1단계 조건 그룹은 **AND** 연산자를 사용하여 결합됩니다.

13. 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-premise) 도움말을 참조하십시오.

14. 필요한 경우 **모든 이벤트 유형**에서 이벤트 유형별로 원격 측정 예외를 추가합니다.

    a. 이벤트 유형 이름을 클릭합니다.

    b. 열리는 창에서 **수동 설정** 버튼을 누릅니다.

    c. 필요시 **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 누릅니다.

    예외 규칙 추가 창이 열립니다.

    e. 추가하는 각 규칙에 대해 7~13단계에 설명된 작업을 수행합니다.

15. 일부 이벤트 유형의 경우 포함 규칙을 추가하여 수집되는 원격 측정을 확장할 수도 있습니다.

    a. **포함 규칙** 블록에서 **추가** 버튼을 누릅니다.

    포함 규칙 추가 창이 열립니다.

    b. 규칙의 이름을 입력합니다.

    c. **조건**에 표시된 필드에 값을 입력합니다. 사용 가능한 필드 유형은 선택한 이벤트에 따라 다릅니다.

제외 규칙은 포함 규칙보다 우선합니다.

16. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

EDR Expert(on-premise) 이벤트 필터 내보내기 및 가져오기

예외 규칙 목록을 JSON 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 이벤트 ID를 여러 개 추가할 수 있습니다. 내보내기/가져오기 기능을 사용하여 이벤트 필터를 백업하거나 목록을 다른 서버로 마이그레이션할 수도 있습니다.

너무 많은 규칙을 사용하면 원격 측정 수집 서버의 부하가 증가하고 컴퓨터 성능이 저하될 수 있습니다. 필요한 규칙만 추가할 것을 권장합니다.

관리 콘솔(MMC)에서 이벤트 필터를 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **일반 설정 → 예외 및 개체 유형**을 선택합니다.
5. **원격 측정 설정 → EDR Expert(on-premise) 원격 측정** 블록에서 **설정** 버튼을 누릅니다.
6. 이벤트 필터를 내보내려면,
   a. **내보내기**를 클릭합니다.
      창이 열리면 이벤트 필터를 내보낼 JSON 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   b. 파일을 저장합니다.
      Kaspersky Endpoint Security는 이벤트 필터를 JSON 파일로 내보냅니다.
7. 이벤트 필터를 가져오려면,
   a. **가져오기**를 클릭합니다.
   b. 창이 열리면 이벤트 필터를 가져올 JSON 파일을 선택합니다.
   c. 파일을 엽니다.
      이벤트 필터링 규칙이 컴퓨터에 이미 있는 경우, Kaspersky Endpoint Security는 가져오기를 수행할 때 이 규칙을 교체합니다.
8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔에서 이벤트 필터를 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 원격 측정 설정**으로 이동합니다.
5. **EDR Expert(on-premise) 원격 측정** 탭을 선택합니다.
6. 이벤트 필터를 내보내려면,
   a. **내보내기**를 클릭합니다.
   b. 창이 열리면 이벤트 필터를 내보낼 JSON 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.
   c. 파일을 저장합니다.
   Kaspersky Endpoint Security는 이벤트 필터를 JSON 파일로 내보냅니다.
7. 이벤트 필터를 가져오려면,
   a. **가져오기**를 클릭합니다.
   b. 창이 열리면 이벤트 필터를 가져올 JSON 파일을 선택합니다.
   c. 이벤트 필터링 규칙을 가져올 방법을 선택합니다. 기존 규칙에 추가할 수도 있고 기존 규칙을 폐기하고 새 규칙으로 교체할 수도 있습니다.
   d. 파일을 엽니다.
8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

명령줄에서 이벤트 필터 내보내기 또는 가져오기를 수행할 수도 있습니다.

격리 저장소 관리

*격리 저장소*는 컴퓨터의 특수 로컬 저장소입니다. 컴퓨터에 위험하다고 판단되는 파일을 격리할 수 있습니다. 격리된 파일은 암호화된 상태로 저장되며 장치 보안에 위협이 되지 않습니다. Kaspersky Endpoint Security는 Kaspersky Detection and Response 솔루션과 통합했을 때만 격리 저장소를 사용합니다. 그 외에는 Kaspersky Endpoint Security가 관련 파일을 백업에 저장합니다. 솔루션에 포함된 격리 저장소 관리 방법에 대한 자세한 내용은 Kaspersky Sandbox 도움말, Kaspersky Endpoint Detection and Response Optimum 도움말, Kaspersky Endpoint Detection and Response Expert 도움말, Kaspersky Anti Targeted Attack Platform 도움말 및 Kaspersky Endpoint Detection and Response Expert(on-premise) 도움말을 참조하십시오.

Kaspersky Endpoint Security는 시스템 계정(SYSTEM)을 사용하여 파일을 격리합니다.

Kaspersky Security Center 콘솔에서만 격리 설정을 구성할 수 있습니다. Kaspersky Security Center 콘솔을 사용하여 격리된 개체를 관리할 수도 있습니다(복원, 삭제, 추가 등). 로컬 컴퓨터에서는 명령줄을 사용하여 개체 복원 작업만 가능합니다.

격리 저장소 최대 크기 구성

기본적으로 격리 저장소의 크기는 1024MB로 제한됩니다. 격리 저장소가 최대 크기에 도달하면 Kaspersky Endpoint Security가 파일 전송을 중지하고 *격리 저장소 공간 부족* 이벤트를 생성합니다. 격리 저장소의 디스크 공간이 부족하지 않도록 Kaspersky Endpoint Security에서 *격리 저장소에 공간이 거의 없습니다* 이벤트를 생성하여 한계값을 설정할 수 있습니다. 격리된 파일의 보존 기간을 설정하여 자동으로 삭제되도록 구성할 수 없습니다.

Kaspersky Anti Targeted Attack Platform(EDR) 솔루션이 조직 내에 배포된 경우에는 격리 저장소의 크기를 늘리는 것이 좋습니다. YARA 검사를 진행할 때 이 애플리케이션에서 대규모 메모리 덤프가 발생할 수 있습니다. 메모리 덤프 크기 격리 저장소 크기를 초과하는 경우 오류와 함께 YARA 검사가 완료되고 메모리 덤프가 격리되지 않습니다. 격리 저장소 크기를 컴퓨터 RAM의 총 크기(예: 8GB)와 같게 설정하거나 격리 저장소의 크기 제한을 비활성화하는 것이 좋습니다.

관리 콘솔(MMC)에서 최대 격리 저장소 크기를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 리포트 및 저장소**를 선택합니다.
4. **격리 저장소** 블록에서 격리 저장소 크기를 구성합니다:
   - **격리 저장소 크기 제한: <N>MB**. 이 확인란을 선택하면 최대 격리 저장소 크기가 정의된 값으로 제한됩니다. 최대 크기 기본값은 1024MB입니다 격리 저장소가 최대 크기에 도달하면 Kaspersky Endpoint Security는 *격리 저장소 공간 부족* 이벤트를 Kaspersky Security Center로 전송하고 Windows 이벤트 로그에 게시합니다. 그동안 애플리케이션은 새 개체를 격리하지 않습니다. 격리 저장소를 직접 비워야 합니다.

     이 확인란을 선택 해제하면, 격리 저장소 크기가 사용 가능한 디스크 여유 공간으로 제한됩니다.
   - **격리 저장소 공간이 다음에 도달하면 알림: N퍼센트**. 격리 저장소의 한계값입니다. 예를 들면 검역 한계값을 50%로 설정할 수 있습니다. 격리 저장소가 한계값에 도달하면 Kaspersky Endpoint Security는 해당 이벤트를 Kaspersky Security Center로 보내고 Windows 이벤트 로그에 이벤트를 게시합니다. 그동안에도 애플리케이션은 계속해서 새 개체를 격리합니다.

     이 확인란을 선택 해제하면, 격리 저장소 한계값에 도달해도 애플리케이션이 이벤트를 생성하지 않습니다.
5. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 최대 격리 저장소 크기를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 리포트 및 저장소**로 갑니다.

5. **격리 저장소** 블록에서 격리 저장소 크기를 구성합니다:

   - **격리 저장소 크기 제한**. 이 확인란을 선택하면 격리 저장소 크기가 지정된 값으로 제한됩니다. 이 확인란을 선택 해제하면, 격리 저장소 크기가 사용 가능한 디스크 여유 공간으로 제한됩니다. 이는 애플리케이션이 대규모 메모리 덤프 파일을 저장할 수 있기 때문에 YARA 검사에 필요할 수 있습니다.

   - **격리 저장소 최대 크기(MB)**. 이 확인란을 선택하면 최대 격리 저장소 크기가 정의된 값으로 제한됩니다. 최대 크기 기본값은 1024MB입니다 격리 저장소가 최대 크기에 도달하면 Kaspersky Endpoint Security는 *격리 저장소 공간 부족* 이벤트를 Kaspersky Security Center로 전송하고 Windows 이벤트 로그에 게시합니다. 그동안 애플리케이션은 새 개체를 격리하지 않습니다. 격리 저장소를 직접 비워야 합니다.

     이 확인란을 선택 해제하면, 격리 저장소 크기가 사용 가능한 디스크 여유 공간으로 제한됩니다.

   - **저장소 공간이 (%)에 도달하면 알림**. 격리 저장소의 한계값입니다. 예를 들면 검역 한계값을 50%로 설정할 수 있습니다. 격리 저장소가 한계값에 도달하면 Kaspersky Endpoint Security는 해당 이벤트를 Kaspersky Security Center로 보내고 Windows 이벤트 로그에 이벤트를 게시합니다. 그동안에도 애플리케이션은 계속해서 새 개체를 격리합니다.

6. 변경 사항을 저장합니다.

격리된 파일에 대한 데이터를 Kaspersky Security Center로 전송

웹 콘솔에서 격리된 개체에 대한 작업을 수행하려면 중앙 관리 서버로 격리된 파일 데이터 전송을 활성화해야 합니다. 예를 들어, 웹 콘솔에서 분석을 위해 격리 저장소의 파일을 다운로드할 수 있습니다. Kaspersky Sandbox 및 Kaspersky Endpoint Detection and Response의 모든 기능이 작동하려면 격리된 파일 데이터 전송을 활성화해야 합니다.

관리 콘솔(MMC)에서 격리된 파일 데이터 전송을 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 리포트 및 저장소**를 선택합니다.
4. **중앙 관리 서버로의 데이터 전송** 블록에서 **설정** 버튼을 클릭합니다.
5. 창이 열리면 **격리 저장소 파일** 확인란을 선택합니다.
6. 변경 사항을 저장합니다.

웹 콘솔에서 격리된 파일 데이터 전송을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → KSC 통합**으로 갑니다.

5. **중앙 관리 서버로의 데이터 전송** 블록에서 **격리 저장소 파일 정보** 확인란을 선택합니다.

6. 변경 사항을 저장합니다.

따라서 Kaspersky Security Center 콘솔에서 컴퓨터에 격리된 파일 목록을 볼 수 있습니다. Kaspersky Security Center 콘솔을 사용하여 격리된 개체를 관리할 수 있습니다(복원, 삭제, 추가 등). 격리 저장소 사용에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

격리 저장소에서 파일 복원

기본적으로 Kaspersky Endpoint Security는 파일을 원래 폴더로 복원합니다. 대상 폴더가 삭제되었거나 사용자에게 해당 폴더에 대한 액세스 권한이 없을 시, 애플리케이션이 파일을 `%DataRoot%\QB\Restored` 폴더에 저장합니다. 해당 파일은 원하는 경로로 직접 이동해야 합니다.

격리 저장소에서 파일 복원하려면 다음을 수행합니다.

1. 웹 콘솔의 기본 창에서 **동작 → 저장소 → 격리**를 선택합니다.

2. 격리 저장소 파일 목록이 열리면 복원할 파일을 선택하고 **복원**을 클릭합니다.

   Kaspersky Endpoint Security가 이 파일을 복원합니다. 대상 폴더에 같은 이름의 파일이 이미 있다면, 애플리케이션이 파일 복원을 취소합니다. EDR Optimum 및 EDR Expert 솔루션에서는, 애플리케이션이 복원 후 파일을 삭제합니다. 다른 솔루션에서는 애플리케이션이 격리 저장소에 파일 사본을 보관합니다.

EDR 동작 모니터링

Kaspersky Endpoint Security for Windows 12.9는 EDR 동작 모니터링 센터를 도입했습니다. *EDR 동작 모니터링 센터*는 모든 Kaspersky Detection and Response 솔루션의 위협 대응 기록을 볼 수 있는 콘솔입니다. 조직에 여러 Detection and Response를 배포했다면(EDR Optimum 및 MDR 등) Kaspersky Endpoint Security가 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 센터로 이동하려면:

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 에셋(기기)**를 선택합니다.

2. 로컬 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.

   그러면 컴퓨터 속성이 열립니다.

3. **애플리케이션** 탭을 선택합니다.

4. **Kaspersky Endpoint Security for Windows**를 누릅니다.

   그러면 로컬 애플리케이션 설정이 열립니다.

5. **애플리케이션 설정** 탭을 선택합니다.

6. **Detection and Response** → **응답 이력**으로 이동합니다.

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 Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security for Windows가 Kaspersky Unified Monitoring and Analysis Platform 솔루션을 지원합니다. *Kaspersky Unified Monitoring and Analysis Platform(KUMA)*은 조직의 IT 인프라를 위한 보안 정보 및 이벤트 관리(SIEM) 솔루션입니다. KUMA를 사용하면 보안 위협을 피해가 발생하기 전에 탐지, 분석 및 완화할 수 있습니다.

Kaspersky Endpoint Security는 기업 IT 인프라의 개별 컴퓨터에 설치되며 프로세스, 개방형 네트워크 연결 및 수정되는 파일을 계속해서 모니터링합니다. 컴퓨터의 이벤트에 대한 정보(원격 측정)는 Kaspersky Unified Monitoring and Analysis Platform(KUMA) 서버로 전송됩니다. KUMA는 콘솔에서 Windows 이벤트 로그와 마찬가지로 이벤트를 마크업 없이 목록으로 표시합니다.

Kaspersky Endpoint Security는 KUMA용 에이전트의 모든 기능 제공하지는 않습니다. 애플리케이션은 마크업 없이 이벤트를 KUMA로 보내기만 합니다. KUMA의 모든 기능에 접근하려면 라이센스를 구매하고 KUMA 관리자 가이드에 따라 솔루션을 배포해야 합니다.

Kaspersky Endpoint Security와 KUMA 통합

KUMA를 사용하려면 다음 조건을 충족해야 합니다.

- Kaspersky Security Center 버전 14.2 이상. 이전 버전의 Kaspersky Security Center에서는 KUMA 통합의 기능을 활성화할 수 없습니다.
- 애플리케이션이 활성화되고 해당 기능에 라이센스가 적용됩니다.
- KUMA 통합 구성 요소가 활성화됩니다.

KUMA 통합 설정에는 다음 단계가 포함됩니다.

1. **KUMA 통합 구성 요소 설치**

   애플리케이션을 설치 또는 업그레이드할 때 또는 *애플리케이션 구성 요소 변경* 작업을 사용할 때 KUMA 통합 구성 요소를 선택할 수 있습니다.

   새 구성 요소로 애플리케이션 업그레이드를 완료하려면 컴퓨터를 다시 시작해야 합니다.

2. **KUMA 활성화**

   Kaspersky Endpoint Security 애플리케이션 라이센스(예: Kaspersky Endpoint Security for Business Standard) 외에도 Kaspersky Endpoint Security를 KUMA와 통합하기 위한 별도의 라이센스(Kaspersky Endpoint Security for Windows KUMA 통합 애드온)가 필요합니다.

애플리케이션을 EDR Agent 모드로 설치하는 경우 Kaspersky Endpoint Security를 KUMA와 통합하기 위한 라이센스와 Kaspersky Anti Targeted Attack Platform(KATA) 라이센스 또는 Kaspersky Managed Detection and Response(MDR) 라이센스가 필요합니다. KUMA용 EDR Agent만 배포할 수는 없습니다.

이 기능은 별도의 KUMA 키를 추가해야 사용할 수 있습니다. 결과적으로 컴퓨터에 KUMA와 Kaspersky Endpoint Security 통합을 위한 다른 활성 키가 생성됩니다.

독립 실행형 KUMA 기능의 라이센스 사용은 Kaspersky Endpoint Security의 라이센스 사용과 같습니다.

KUMA 기능이 라이센스에 포함되며 애플리케이션의 로컬 인터페이스에서 실행되고 있는지 확인하십시오.

3 KUMA에 연결

Kaspersky Endpoint Security 애플리케이션이 있는 컴퓨터를 KUMA 솔루션에 연결하려면:

1. Kaspersky Endpoint Security 정책에서 KUMA 서버 주소를 추가하고 연결의 네트워크 설정을 지정합니다.
2. KUMA 콘솔에서 tcp 또는 udp 유형의 커넥터가 있는 수집기를 추가하고 연결의 기본 네트워크 설정을 지정합니다. 수집기 관리에 대한 자세한 내용은 Kaspersky Unified Monitoring and Analysis Platform 도움말을 참조하십시오.

Kaspersky Endpoint Security와 KUMA 서버 간에 신뢰할 수 있는 연결을 설정할 수 있습니다. 신뢰할 수 있는 연결을 구성하려면 TLS 인증서를 사용해야 합니다. KUMA Core 서버에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Unified Monitoring and Analysis Platform 도움말에서 tcp 유형 커넥터 설정 참조). 그런 다음 Kaspersky Endpoint Security에 TLS 인증서를 추가해야 합니다(아래 지침 참조).

보다 안전한 연결을 위해, KUMA에서 컴퓨터 확인을 추가로 활성화할 수 있습니다(양방향 인증). 이 확인을 활성화하려면 KUMA와 Kaspersky Endpoint Security 설정에서 양방향 인증을 켜야 합니다. 양방향 인증을 사용하려면 암호화 컨테이너도 필요합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. 외부 인증 기관에서 PKCS#12 컨테이너 형식의 개인 키로 인증서를 생성해야 합니다. 그런 다음 KUMA 콘솔 및 Kaspersky Endpoint Security에서 PFX 압축 파일을 추가해야 합니다(Kaspersky Unified Monitoring and Analysis Platform 도움말에서 tcp 유형 커넥터 설정 참조).

관리 콘솔(MMC)을 사용하여 Kaspersky Endpoint Security 컴퓨터를 KUMA에 연결하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **KUMA 통합**을 선택합니다.
4. **KUMA 통합** 확인란을 선택합니다.
5. **통합 설정** 블록에서 **$IsKUMATelemetry ? "KUMA 서버로 Windows 이벤트 전송 활성화": "SIEM 서버로 Windows 이벤트 전송 활성화** 확인란을 선택합니다.
6. 필요한 경우 **KUMA 서버 연결 설정** 블록에서 **TLS 암호화 사용** 확인란을 선택합니다.

7. 신뢰 연결을 구성합니다.

   a. **KUMA 서버 연결 설정**을 누릅니다.

   b. 서버 연결 구성:

   - **시간 초과(초)**. 최대 KUMA 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 KUMA 서버에 연결을 시도합니다.

   - **서버 TLS 인증서**. KUMA 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Unified Monitoring and Analysis Platform 콘솔에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Unified Monitoring and Analysis Platform 지침 참조).

     신뢰할 수 있는 연결을 구성하려면 KUMA 콘솔의 tcp 커넥터 설정에서 **With verification** TLS 모드를 선택해야 합니다(Kaspersky Unified Monitoring and Analysis Platform 도움말 에서 tcp 유형 커넥터 설정 참조).

   - **양방향 인증 사용**. Kaspersky Endpoint Security와 KUMA 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 KUMA 콘솔의 tcp 커넥터 설정에서 **Custom PFX** TLS 모드를 선택해야 합니다(Kaspersky Unified Monitoring and Analysis Platform 도움말 에서 tcp 유형 커넥터 설정 참조). 그런 다음 암호화 컨테이너를 가져오고 암호화 컨테이너를 보호하기 위한 암호를 설정해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. KUMA 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.

   c. **확인**을 누릅니다.

8. KUMA 서버를 추가합니다.

   a. **추가**를 클릭합니다.

   KUMA 서버를 추가할 수 있는 양식이 열립니다.

   b. KUMA 서버에 연결하기 위한 프로토콜을 선택합니다. **HTTP / HTTPS**, **TCP**, **UDP**.

   HTTP / HTTPS 프로토콜을 선택하면 애플리케이션은 기본적으로 KUMA 서버 연결에 HTTPS를 사용합니다. HTTP를 사용하려면 서버 주소에서 이 프로토콜을 직접 지정해야 합니다(예: `http://server.com`).

   c. 서버 주소(IPv4, IPv6) 및 서버에 연결할 포트를 입력하십시오.

   d. **확인**을 누릅니다.

   Kaspersky Endpoint Security가 목록에서 첫 번째 KUMA 서버에 연결합니다. 연결에 실패하면 Kaspersky Endpoint Security가 목록에서 두 번째 KUMA 서버에 연결하는 식으로 진행합니다.

9. 필요한 경우 **데이터 전송 설정**에서 **최대 이벤트 전송 지연(초)** 설정을 구성합니다. 지정된 시간이 초과되면 Kaspersky Endpoint Security는 동일한 서버에 연결을 시도하거나, 서버가 여러 개일 경우 목록에 있는 다음 서버에 연결합니다. 기본 설정은 30초입니다.

10. 변경 사항을 저장합니다.

웹 콘솔을 사용하여 Kaspersky Endpoint Security 컴퓨터를 KUMA에 연결하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **내장 에이전트 구성** → **KUMA 통합**으로 이동합니다.
5. **KUMA 통합 활성화됨** 토글을 켭니다.
6. 필요한 경우 **서버 연결 설정** 블록에서 **TLS 암호화 사용** 토글 스위치를 켭니다.
7. 신뢰 연결을 구성합니다.
   a. **연결 설정**을 클릭합니다.
   b. 서버 연결 구성:
   - **시간 초과(초)**. 최대 KUMA 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 KUMA 서버에 연결을 시도합니다.
   - **서버 TLS 인증서**. KUMA 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Unified Monitoring and Analysis Platform 콘솔에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Unified Monitoring and Analysis Platform 지침 참조).
     신뢰할 수 있는 연결을 구성하려면 KUMA 콘솔의 tcp 커넥터 설정에서 **With verification** TLS 모드를 선택해야 합니다(Kaspersky Unified Monitoring and Analysis Platform 도움말 에서 tcp 유형 커넥터 설정 참조).
   - **양방향 인증 사용**. Kaspersky Endpoint Security와 KUMA 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 KUMA 콘솔의 tcp 커넥터 설정에서 **Custom PFX** TLS 모드를 선택해야 합니다(Kaspersky Unified Monitoring and Analysis Platform 도움말 에서 tcp 유형 커넥터 설정 참조). 그런 다음 암호화 컨테이너를 가져오고 암호화 컨테이너를 보호하기 위한 암호를 설정해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. KUMA 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.

   c. **확인**을 누릅니다.
8. KUMA 서버를 추가합니다.
   a. **추가**를 클릭합니다.
   KUMA 서버를 추가할 수 있는 양식이 열립니다.
   b. KUMA 서버에 연결하기 위한 프로토콜을 선택합니다. **HTTP / HTTPS**, **TCP**, **UDP**.
   HTTP / HTTPS 프로토콜을 선택하면 애플리케이션은 기본적으로 KUMA 서버 연결에 HTTPS를 사용합니다. HTTP를 사용하려면 서버 주소에서 이 프로토콜을 직접 지정해야 합니다(예: `http://server.com`).

c. 서버 주소(IPv4, IPv6) 및 서버에 연결할 포트를 입력하십시오.

d. **확인**을 누릅니다.

Kaspersky Endpoint Security가 목록에서 첫 번째 KUMA 서버에 연결합니다. 연결에 실패하면 Kaspersky Endpoint Security가 목록에서 두 번째 KUMA 서버에 연결하는 식으로 진행합니다.

9. 필요한 경우 **서버 연결 설정**에서 **이벤트 전송 시 최대 지연 시간(초)** 설정을 구성합니다. 지정된 시간이 초과되면 Kaspersky Endpoint Security는 동일한 서버에 연결을 시도하거나, 서버가 여러 개일 경우 목록에 있는 다음 서버에 연결합니다. 기본 설정은 30초입니다.

10. 변경 사항을 저장합니다.

KUMA 콘솔에서 KUMA 통합이 올바르게 구성되었는지 확인할 수 있습니다(자세한 내용은 Kaspersky Unified Monitoring and Analysis Platform 도움말 참조). Kaspersky Security Center 콘솔에서 *애플리케이션 구성 요소 상태 리포트*를 확인하여 구성 요소의 작동 상태를 확인합니다. 또한 Kaspersky Endpoint Security의 로컬 인터페이스에 있는 리포트에서 구성 요소의 작동 상태를 볼 수 있습니다. **KUMA 통합** 구성 요소가 Kaspersky Endpoint Security 구성 요소 목록에 추가됩니다.

4 KUMA 서버로 원격 측정 전송 활성화

기본적으로 KUMA 서버로 이벤트를 전송하는 것은 비활성화되어 있습니다. KUMA가 제대로 작동하도록 하려면 원격 측정 전송을 활성화해야 합니다. 표준 로그인 *Application*, *Security*, *System* 중에서 이벤트 소스를 선택할 수 있습니다.

관리 콘솔(MMC)에서 KUMA 서버로의 원격 측정 전송을 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **일반 설정** → **예외 및 개체 유형**을 선택합니다.
5. **원격 측정 설정** → **KUMA 원격 측정** 블록에서 **설정** 버튼을 누릅니다.
6. *애플리케이션*, *보안*, *시스템* 중 이벤트 소스로 사용할 이벤트 로그를 선택합니다.
   표준 로그 외에도 타사 애플리케이션 로그를 지정할 수 있습니다.
7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔에서 KUMA 서버로 원격 측정 전송을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **원격 측정 설정**으로 이동합니다.
5. **KUMA 원격 측정** 탭을 선택합니다.

6. *애플리케이션*, *보안*, *시스템* 중 이벤트 소스로 사용할 이벤트 로그를 선택합니다.

   표준 로그 외에도 타사 애플리케이션 로그를 지정할 수 있습니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

KUMA로 전송할 이벤트 필터링

기본적으로 KUMA 서버로 이벤트를 전송하는 것은 비활성화되어 있습니다. KUMA가 제대로 작동하도록 하려면 원격 측정 전송을 활성화해야 합니다. 표준 로그인 *Application*, *Security*, *System* 중에서 이벤트 소스를 선택할 수 있습니다. 성능을 개선하고 KUMA 서버로 데이터 전송을 최적화하기 위해, 원격 측정에서 개별 이벤트를 수동으로 추가하거나 제외할 수 있습니다. 그 예로, Sysmon 이벤트를 제외할 수 있습니다.

관리 콘솔(MMC)에서 KUMA로 전송할 이벤트 목록을 만드는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔 트리에서 **정책**을 선택합니다.
3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
4. 정책 창에서 **일반 설정 → 예외 및 개체 유형**을 선택합니다.
5. **원격 측정 설정 → KUMA 원격 측정** 블록에서 **설정** 버튼을 누릅니다.
6. 창이 표시되면 KUMA로 전송할 이벤트 필터를 구성합니다.

   표준 *Application*, *Security*, *System* 로그에 대한 이벤트 필터링을 구성하거나 다른 로그를 수동으로 추가할 수 있습니다.

   a. **추가**를 클릭하거나 로그 속성을 엽니다.

   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.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔에서 KUMA로 전송할 이벤트 목록을 만드는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **원격 측정 설정**으로 이동합니다.

5. **KUMA 원격 측정** 탭을 선택합니다.

6. 창이 표시되면 KUMA로 전송할 이벤트 필터를 구성합니다.

   표준 *Application*, *Security*, *System* 로그에 대한 이벤트 필터링을 구성하거나 다른 로그를 수동으로 추가할 수 있습니다.

   a. **추가**를 클릭하거나 로그 속성을 엽니다.

   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.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

KUMA 이벤트 필터 내보내기 및 가져오기

예외 규칙 목록을 JSON 파일로 내보낼 수 있습니다. 그 후 파일을 수정하여 이벤트 ID를 여러 개 추가할 수 있습니다. 내보내기/가져오기 기능을 사용하여 이벤트 필터를 백업하거나 목록을 다른 서버로 마이그레이션할 수도 있습니다.

너무 많은 규칙을 사용하면 KUMA 서버의 부하가 증가하고 컴퓨터 성능이 저하될 수 있습니다. 필요한 규칙만 추가할 것을 권장합니다.

관리 콘솔(MMC)에서 이벤트 필터를 내보내고 가져오는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.

2. 콘솔 트리에서 **정책**을 선택합니다.

3. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

4. 정책 창에서 **일반 설정** → **예외 및 개체 유형**을 선택합니다.

5. **원격 측정 설정** → **KUMA 원격 측정** 블록에서 **설정** 버튼을 누릅니다.

6. 이벤트 필터를 내보내려면,

   a. 내보낼 필터를 포함하는 이벤트 로그를 선택합니다.

   b. → **내보내기** 버튼을 클릭합니다.

   c. 창이 열리면 이벤트 필터를 내보낼 JSON 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

d. 파일을 저장합니다.

Kaspersky Endpoint Security는 이벤트 필터를 JSON 파일로 내보냅니다.

7. 이벤트 필터를 가져오려면,

a. → **가져오기** 버튼을 클릭합니다.

b. 창이 열리면 이벤트 필터를 가져올 JSON 파일을 선택합니다.

c. 파일을 엽니다.

이벤트 필터링 규칙이 컴퓨터에 이미 있는 경우, Kaspersky Endpoint Security는 가져오기를 수행할 때 이 규칙을 교체합니다.

8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

웹 콘솔에서 이벤트 필터를 내보내고 가져오는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책** 탭을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **일반 설정** → **원격 측정 설정**으로 이동합니다.

5. **KUMA 원격 측정** 탭을 선택합니다.

6. 이벤트 필터를 내보내려면,

a. 내보낼 필터를 포함하는 이벤트 로그를 선택합니다.

b. → **내보내기** 버튼을 클릭합니다.

c. 창이 열리면 이벤트 필터를 내보낼 JSON 파일의 이름을 지정하고 이 파일을 저장할 폴더를 선택합니다.

d. 파일을 저장합니다.

Kaspersky Endpoint Security는 이벤트 필터를 JSON 파일로 내보냅니다.

7. 이벤트 필터를 가져오려면,

a. → **가져오기** 버튼을 클릭합니다.

b. 창이 열리면 이벤트 필터를 가져올 JSON 파일을 선택합니다.

c. 파일을 엽니다.

이벤트 필터링 규칙이 컴퓨터에 이미 있는 경우, Kaspersky Endpoint Security는 가져오기를 수행할 때 이 규칙을 교체합니다.

8. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.

명령줄에서 이벤트 필터 내보내기 또는 가져오기를 수행할 수도 있습니다.

KSWS에서 KES로의 마이그레이션 가이드

11.8.0 버전부터 Kaspersky Endpoint Security for Windows는 KSWS(Kaspersky Security for Windows Server) 솔루션의 기본 기능을 지원합니다. *Kaspersky Security for Windows Server*는 파일을 교환하는 동안 서버 및 네트워크 연결 저장소가 노출되는 바이러스 및 기타 컴퓨터 보안 위협으로부터 Microsoft Windows 운영 체제 및 네트워크 연결 저장소를 실행하는 서버를 보호합니다. 솔루션 작동 방식에 대한 자세한 내용은 Kaspersky Security for Windows Server 도움말 을 참조하십시오. Kaspersky Endpoint Security 11.8.0부터 Kaspersky Security for Windows Server에서 Kaspersky Endpoint Security for Windows로 마이그레이션하고 동일 솔루션을 사용하여 워크스테이션과 서버를 보호할 수 있습니다.

소프트웨어 요구 사항

KSWS에서 KES의로 마이그레이션을 시작하기 전에 서버가 Kaspersky Endpoint Security for Windows의 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인하십시오. KES와 KSWS는 지원되는 운영 체제 버전 목록이 서로 다릅니다. 예를 들어 KES는 Windows Server 2003을 실행하는 서버를 지원하지 않습니다.

KSWS에서 KES로의 마이그레이션을 위한 최소 소프트웨어 요구 사항:

- Kaspersky Endpoint Security for Windows 12.0
- Kaspersky Security 11.0.1 for Windows Server

  Kaspersky Security for Windows Server 이전 버전이 설치되어 있는 경우 애플리케이션을 최신 버전으로 업그레이드하는 것이 좋습니다. 정책 및 작업 변환 마법사는 Kaspersky Security for Windows Server 이전 버전을 지원하지 않습니다.
- Kaspersky Security Center 14.2

  Kaspersky Security Center 이전 버전이 설치되어 있는 경우 14.2 이상으로 업데이트하십시오. 이 버전의 Kaspersky Security Center에서는 정책 및 작업 변환 마법사를 사용하여 여러 정책을 단일 정책 대신 단일 프로필로 마이그레이션할 수 있습니다. 또한 이 버전의 Kaspersky Security Center에서는 정책 및 작업 변환 마법사를 사용하여 더 광범위한 정책 설정을 마이그레이션할 수도 있습니다.
- Kaspersky Endpoint Agent 3.10

  Kaspersky Endpoint Agent 이전 버전이 설치되어 있는 경우 애플리케이션을 최신 버전으로 업그레이드하는 것이 좋습니다. Kaspersky Endpoint Security는 Kaspersky Endpoint Agent 3.10부터 [KSWS+KEA] 구성을 [KES+내장 에이전트]로 마이그레이션하는 작업을 지원합니다.

마이그레이션 권장 사항

KSWS에서 KES로 마이그레이션할 때는 다음 권장 사항을 준수하십시오.

- KSWS에서 KES로의 마이그레이션 시간을 미리 계획합니다. 서버가 가장 적은 부하로 작동하는 시간(주말 등)을 선택합니다.
- 마이그레이션이 끝나면 애플리케이션 구성 요소를 점진적으로 켭니다. 예를 들어 먼저 파일 위협 보호 구성 요소만 활성화한 다음, 다른 보호 구성 요소를 활성화하고 제어 구성 요소를 활성화하는 식입니다. 각 단계에서 애플리케이션이 올바르게 작동하는지 확인하고 서버 성능을 모니터링해야 합니다. KES의 아키텍처는 KSWS의 아키텍처와 다르므로 운영 체제도 다르게 작동할 수 있습니다.

- 마이그레이션을 점진적으로 수행합니다. 먼저 단일 서버를 마이그레이션한 다음 여러 서버를 마이그레이션하고, 조직의 모든 서버에서 마이그레이션을 수행합니다.
- 서로 다른 유형의 서버를 개별적으로 마이그레이션합니다. 예를 들어 데이터베이스 서버를 먼저 마이그레이션한 다음 메일 서버 등을 마이그레이션하는 식입니다.
- 부하가 높은 서버로의 마이그레이션에는 몇 가지 특별한 고려 사항이 적용됩니다.

마이그레이션 단계

KSWS에서 KES로의 마이그레이션은 반자동으로 수행됩니다. 애플리케이션의 아키텍처가 서로 다르기 때문입니다. 정책 설정을 마이그레이션하려면 정책 및 작업 변환 마법사(마이그레이션 마법사)를 실행해야 합니다. 정책 설정을 마이그레이션한 후에는 마이그레이션 마법사가 자동으로 마이그레이션할 수 없는 설정(예: 암호 보호 설정)을 수동으로 구성해야 합니다. 마이그레이션이 끝나면 마이그레이션 마법사가 모든 설정을 올바르게 마이그레이션했는지 확인하는 것이 좋습니다.

KSWS에서 KES로의 마이그레이션을 다음 순서로 진행합니다.

1. **KSWS 작업 및 정책 마이그레이션**

   정책 및 작업을 마이그레이션한 후에는 추가 구성 단계를 수행해야 합니다. 또한 KSWS에서의 마이그레이션이 끝난 후 Kaspersky Endpoint Security가 필요한 수준의 보안을 제공하는지 확인하는 것이 좋습니다.

   > Kaspersky Security for Windows Server용 정책 및 작업 변환 마법사는 관리 콘솔(MMC)에서만 사용할 수 있습니다. 정책 및 작업 설정은 웹 콘솔과 Kaspersky Security Center Cloud Console에서는 마이그레이션할 수 없습니다.

2. **Kaspersky Endpoint Security 설치**

   Kaspersky Endpoint Security는 다음과 같은 방법으로 설치할 수 있습니다.

   - KSWS 제거 후 KES 설치(권장)

     > kavremover 유틸리티는 KSWS 관리를 지원하지 않습니다.

   - KSWS와 함께 KES 설치

3. **KSWS 키로 KES 활성화**

4. **마이그레이션 후 애플리케이션이 제대로 작동하는지 확인합니다.**

   KSWS에서 KES로의 마이그레이션이 끝나면 애플리케이션이 올바르게 작동하는지 확인하십시오. 콘솔에서 서버 상태를 확인합니다(*정상*해야 합니다). 애플리케이션에 대해 보고된 오류가 없는지 확인하고, 중앙 관리 서버에 대한 마지막 연결 시간과 마지막 데이터베이스 업데이트 시간 및 서버 보호 상태를 확인합니다.

   > 예외 목록, 신뢰하는 애플리케이션, 신뢰하는 웹 주소, 애플리케이션 제어 규칙의 마이그레이션에 특히 주의합니다.

KSWS 및 KES 구성 요소의 대응

KSWS에서 KES로 마이그레이션하는 경우 구성 요소 집합은 애플리케이션이 로컬로 설치될 때만 마이그레이션됩니다.

Kaspersky Security for Windows Server 및 Kaspersky Endpoint Security for Windows 구성 요소의 대응

Kaspersky Security for Windows Server 구성 요소	Kaspersky Endpoint Security for Windows 구성 요소
Basic functionality	애플리케이션 커널
Log Inspection	로그 검사
Device Control	장치 제어
Firewall Management	*(지원하지 않음)* KSWS 방화벽 기능은 시스템 수준의 방화벽으로 수행됩니다. KES에서는 별도의 구성 요소가 방화벽 기능을 담당합니다. 마이그레이션 후 Kaspersky Endpoint Security 방화벽을 구성할 수 있습니다.
File Integrity Monitor	시스템 무결성 모니터링
Exploit Prevention	익스플로잇 방지
System Tray Icon	*(지원하지 않음)* 애플리케이션 인터페이스 설정에서 사용자 상호 작용을 구성할 수 있습니다.
Integration with Kaspersky Security Center	네트워크 에이전트 커넥터
Endpoint Agent	*(지원하지 않음)* Kaspersky Endpoint Security 11.9.0에서는 Kaspersky Endpoint Security 배포 키트에 Kaspersky Endpoint Agent 배포 패키지가 포함되지 않습니다. Kaspersky Endpoint Agent 배포 패키지를 별도로 다운로드해야 합니다.
Network Threat Protection	네트워크 위협 보호
Anti-Cryptor	행동 탐지
Anti-Cryptor for NetApp	*(지원하지 않음)*
Traffic Security	웹 위협 보호 메일 위협 보호 웹 제어
On-Demand Scan	애플리케이션 커널
ICAP Network Storage Protection	*(지원하지 않음)* Kaspersky Endpoint Security는 네트워크 연결 스토리지 보호 구성 요소를 지원하지 않습니다. 이러한 구성 요소가 필요한 경우 Kaspersky Security for Windows Server를 계속 사용할 수 있습니다.
RPC Network Storage Protection	*(지원하지 않음)* Kaspersky Endpoint Security는 네트워크 연결 스토리지 보호 구성 요소를 지원하지 않습니다. 이러한 구성 요소가 필요한 경우 Kaspersky Security for Windows Server를 계속 사용할 수 있습니다.
Real-Time File Protection	파일 위협 보호
Script Monitoring	*(지원하지 않음)* 스크립트 모니터링은 AMSI 보호와 같은 다른 구성 요소에서 처리됩니다.
KSN Usage	Kaspersky Security Network
Applications Launch Control	애플리케이션 제어
Performance counters	*(지원하지 않음)*

KSWS 및 KES 설정의 대응

정책 및 작업을 마이그레이션할 때 KES는 KSWS 설정에 따라 구성됩니다. KSWS에 없는 애플리케이션 구성 요소의 설정은 기본값으로 설정됩니다.

Application settings

Scalability, interface and scanning settings

Kaspersky Endpoint Security for Windows에서는 애플리케이션 설정을 지원하지 않습니다.

애플리케이션 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Scalability settings	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 작업 프로세스를 관리합니다.
Show System Tray Icon	*(마이그레이션하지 않음)* 클라이언트 컴퓨터에서 Kaspersky Endpoint Security의 메인 창과 Windows 알림 영역의 아이콘을 모두 사용할 수 있습니다. 아이콘의 마우스 오른쪽 메뉴에서 사용자는 Kaspersky Endpoint Security로 작업을 수행할 수 있습니다. Kaspersky Endpoint Security에서도 애플리케이션 아이콘 위에 알림을 표시합니다. 애플리케이션 인터페이스 설정에서 사용자 상호 작용을 구성할 수 있습니다.
Restore file attributes after scanning	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 파일 검사 후 파일 속성을 자동으로 복원합니다.
Limit CPU usage for scanning threads	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 검사 시 CPU 사용량을 제한하지 않습니다. 컴퓨터의 부하가 최소 수준일 때 작업을 실행하도록 구성할 수 있습니다.
Folder for temporary files created during scanning	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 임시 파일을 `C:\Windows\Temp` 폴더에 저장합니다.
HSM system settings	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 HSM 시스템을 지원하지 않습니다.

Security and reliability

KSWS 보안 설정은 **일반 설정** 섹션, **애플리케이션 설정** 그리고 **인터페이스** 하위 섹션으로 마이그레이션됩니다.

애플리케이션 보안 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Protect application processes from external threats	**자기 보호 사용**(**애플리케이션 설정** 하위 섹션)
Apply password protection	*(마이그레이션하지 않음)* Kaspersky Endpoint Security에는 암호 보호 기능이 내장되어 있습니다(**인터페이스** 하위 섹션 참조).
Perform task recovery	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 *악성 코드 검사* 작업만 자동으로 복원합니다. Kaspersky Endpoint Security는 스케줄에 따라 다른 작업을 실행합니다.

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Do not start scheduled scan tasks	**배터리 전원으로 실행 중이면 스케줄된 작업 연기(애플리케이션 설정** 하위 섹션)
Stop current scan tasks	*(마이그레이션하지 않음)* 컴퓨터에 UPS 전원이 공급되면 Kaspersky Endpoint Security는 이미 실행 중인 검사 작업을 중지하지 않습니다.

Connection settings

중앙 관리 서버 상호 작용 설정은 **일반 설정** 섹션, **네트워크 설정** 그리고 **애플리케이션 설정** 하위 섹션으로 마이그레이션됩니다.

중앙 관리 서버 상호 작용 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Proxy server settings	**프록시 서버 설정(네트워크 설정** 하위 섹션)
Do not use proxy server for local addresses	**로컬 주소에 대해 프록시 서버 우회(네트워크 설정** 하위 섹션)
Proxy server authentication settings	**프록시 서버 인증 사용(네트워크 설정** 하위 섹션) 프록시 서버 인증 암호는 마이그레이션되지 않습니다. 정책을 마이그레이션한 후 암호를 수동으로 입력해야 합니다.
Use Kaspersky Security Center as a proxy server when activating the application	**활성화 시 프록시 서버로 Kaspersky Security Center 사용(애플리케이션 설정** 하위 섹션)

Run local system tasks

Kaspersky Endpoint Security는 Kaspersky Security for Windows Server의 로컬 시스템 작업 실행 설정을 무시합니다. **로컬 작업**, **작업 관리**에서 로컬 KES 작업 사용을 구성할 수 있습니다. 이 작업의 속성에서 *악성 코드 검사* 및 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업 실행 스케줄을 구성할 수도 있습니다.

Supplementary

Trusted zone

KSWS 신뢰 구역 설정은 **일반 설정** 섹션, **예외** 하위 섹션으로 마이그레이션됩니다.

신뢰 구역 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Object to scan (Exclusions)	**검사 예외**(검사 예외) KSWS와 KES에서 객체 선택에 사용하는 방법은 다릅니다. 마이그레이션 시 KES는 개별 파일 또는 파일/폴더 경로로 정의된 예외를 지원합니다. KSWS에 사전 정의된 영역 또는 스크립트 URL로 구성된 예외가 있을 시 이러한 예외는 마이그레이션되지 않습니다. 마이그레이션 후에는 이러한 예외를 수동으로 추가해야 합니다. 사전 정의된 영역으로 예외는 *악성 코드 검사* 작업 설정에서 구성해야 합니다. 웹 위협 보호를 위해 신뢰하는 웹 주소에 스크립트 웹 주소로 예외를 추가해야 합니다.
Apply also to subfolders (Exclusions)	**하위 폴더 포함**(검사 예외)
Objects to detect (Exclusions)	**탐지된 개체 유형**(검사 예외)

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Exclusion usage scope (Exclusions)	**보호 구성 요소**(검사 예외) KSWS에서 하나 이상의 구성 요소가 선택되면 KES는 모든 애플리케이션 구성 요소에 예외를 적용합니다.
Comment (Exclusions)	**설명**(검사 예외)
Trusted process (Trusted process)	**신뢰하는 애플리케이션** 신뢰하는 프로세스/애플리케이션 선택 방법은 KSWS와 KES에서 다릅니다. 마이그레이션할 때 KES는 실행 파일이나 마스크에 대한 경로로 구성된 신뢰하는 애플리케이션을 지원합니다. KSWS에 파일 해시처럼 구성된 신뢰하는 프로세스가 있다면 이러한 신뢰하는 프로세스는 마이그레이션되지 않습니다. 마이그레이션 후 이러한 신뢰하는 프로세스를 수동으로 추가해야 합니다.
Do not check file backup operations (Trusted process)	**애플리케이션 활동 감시 안 함**(신뢰하는 애플리케이션)

Removable drives scan

이동식 드라이브 검사 설정은 **로컬 작업** 섹션, **이동식 드라이브 검사** 하위 섹션으로 마이그레이션됩니다.

이동식 드라이브 검사 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Scan removable drives on connection via USB	**이동식 드라이브 연결 시 처리 방법**
Scan removable drives if its stored data volume does not exceed (MB)	**이동식 드라이브 최대 크기**
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**이동식 드라이브 연결 시 처리 방법**: • **최대 보호** • **권장**. KSWS 보안 수준은 다음과 같이 KES 스캔 모드에 해당합니다: • Maximum protection – 최대 보호. • Recommended – 권장. • Maximum performance – 권장.

User permissions for application management

Kaspersky Endpoint Security는 애플리케이션 관리 및 애플리케이션 서비스 관리를 위한 사용자 접근 권한 할당을 지원하지 않습니다. Kaspersky Security Center에서 애플리케이션을 관리하기 위해 사용자 및 사용자 그룹에 대한 접근 설정을 구성할 수 있습니다.

User access permissions for Kaspersky Security Service management

Kaspersky Endpoint Security는 애플리케이션 관리 및 애플리케이션 서비스 관리를 위한 사용자 접근 권한 할당을 지원하지 않습니다. Kaspersky Security Center에서 애플리케이션을 관리하기 위해 사용자 및 사용자 그룹에 대한 접근 설정을 구성할 수 있습니다.

Storages

KSWS 저장소 설정은 **일반 설정** 섹션, **리포트 및 저장소** 하위 섹션 및 **필수 위협 보호** 섹션, **네트워크 위협 보호** 하위 섹션으로 마이그레션됩니다.

저장소 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Backup folder	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 파일의 백업 복사본을 `C:\ProgramData\Kaspersky Lab\KES.14.0\QB` 폴더에 저장합니다.
Maximum Backup size (MB)	**백업 크기를 다음으로 제한: <N>MB**(**일반 설정** → **리포트 및 저장소** 섹션)
Threshold value for space available (MB)	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 임계값의 50%에 도달하면 *격리 저장소에 공간이 얼마 남지 않았습니다* 이벤트를 기록합니다.
Target folder for restoring objects	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 파일을 원래 폴더로 복원합니다.
Quarantine folder	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 파일의 백업 복사본을 `C:\ProgramData\Kaspersky Lab\KES.14.0\QB` 폴더에 저장합니다.
Maximum Quarantine size (MB)	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 백업을 사용하여 감염 의심 개체를 저장합니다. 마이그레이션하는 동안 Kaspersky Endpoint Security는 검역소 설정을 무시합니다.
Threshold value for space available (MB)	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 백업을 사용하여 감염 의심 개체를 저장합니다. 마이그레이션하는 동안 Kaspersky Endpoint Security는 검역소 설정을 무시합니다.
Target folder for restoring objects	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 파일을 원래 폴더로 복원합니다.
Unblock automatically in N	**다음 시간 동안 공격 장치 차단: N분**(**필수 위협 보호** → **네트워크 위협 보호** 섹션)

Real-time server protection

Real-Time File Protection

KSWS 실시간 파일 보호 설정이 **필수 위협 보호** 섹션, **파일 위협 방지** 하위 섹션에 마이그레이션됩니다.

실시간 파일 보호 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Objects protection mode: • Smart mode • When run • On access • On access and modification	**검사 모드**: • **스마트 모드** • **실행 시** • **접근 시** • **접근 및 수정 시**
Deeper analysis of launching processes	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 분석 모드 중 Optimal 모드 하나만 지원합니다.
Heuristic analyzer: • Light • Medium • Deep	**휴리스틱 분석**: • **빠른 검사** • **보통 검사** • **정밀 검사**
Apply Trusted Zone	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 구성 요소에 신뢰 구역을 적용합니다. 신뢰 구역 설정에서 예외를 구성할 수 있습니다.
Use KSN for protection	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 애플리케이션 구성 요소에 KSN을 사용합니다.

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Block access to network shared resources for the hosts that show malicious activity	*(마이그레이션하지 않음)* 기본적으로 Kaspersky Endpoint Security는 악성 활동을 보이는 호스트의 네트워크 공유 리소스에 대한 접근을 차단합니다.
Launch critical areas scan when active infection is detected	*(마이그레이션하지 않음)* 활성 감염 탐지 시 Kaspersky Endpoint Security는 중요 영역 검사 작업을 시작하지 않습니다.
Use Kaspersky Sandbox for protection	*(마이그레이션하지 않음)* 기본적으로 Kaspersky Endpoint Security는 검사를 위해 개체를 Kaspersky Sandbox로 보냅니다.
Protection scope	**보호 범위**
Schedule settings	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 파일 위협 보호를 일시 중지하기 위해 자체 스케줄을 사용합니다.

KSN Usage

Kaspersky Security Network에 대한 KSWS 설정이 **지능형 위협 보호** 섹션, Kaspersky Security Network 하위 섹션으로 마이그레이션됩니다.

Kaspersky Security Network 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Kaspersky Security Network 진술문** Kaspersky Endpoint Security는 애플리케이션 설치, 새 정책 생성, Kaspersky Security Network 사용 활성화 시 Kaspersky Security Network 정책에 대한 동의를 요청합니다.
Send data about scanned files	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 KSN 활성화 시 검사된 파일에 대한 데이터를 자동으로 전송합니다.
Send data about requested URLs	*(마이그레이션하지 않음)* KSN 활성화 시 Kaspersky Endpoint Security는 요청된 URL에 대한 데이터를 자동으로 전송합니다.
Send Kaspersky Security Network statistics	**확장 KSN 모드 사용**
Accept the terms of the Kaspersky Managed Protection Statement	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 KMP 서비스를 포함하지 않습니다.
Action to perform on KSN untrusted objects	*(마이그레이션하지 않음)* 보호 구성 요소 설정 및 검사 작업 설정에서 보안 위협 탐지 시 동작을 구성할 수 있습니다.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(마이그레이션하지 않음)* 보호 구성 요소 설정 및 검사 작업 설정에서 대용량 파일 검사 제한을 구성할 수 있습니다.
Use Kaspersky Security Center as KSN Proxy	**중앙 관리 서버를 KSN 프록시 서버로 사용**
Schedule settings	*(마이그레이션하지 않음)* 이 구성 요소에 대해 별도의 스케줄을 구성할 수 없습니다. 이 구성 요소는 Kaspersky Endpoint Security가 작동하는 동안 항상 켜져 있습니다.

Traffic Security

KSWS 트래픽 보안 설정은 **필수 위협 보호** 섹션, 웹 위협 보호 그리고 메일 위협 보호 하위 섹션; **보안 제어** 섹션, 웹 제어 하위 섹션; **일반 설정** 섹션, 네트워크 설정 하위 섹션으로 마이그레이션됩니다.

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Apply URL-based rules	**웹 제어**(**웹 제어** 하위 섹션) URL 기반 규칙은 Kaspersky Endpoint Security에서 별도의 규칙으로 마이그레이션됩니다.
Apply certificate-based rules	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 인증서 기반 규칙을 지원하지 않습니다.
Apply rules for web traffic category control	**웹 제어**(**웹 제어** 하위 섹션) 웹 트래픽 카테고리 제어를 위한 차단 규칙은 Kaspersky Endpoint Security의 단일 차단 규칙으로 마이그레이션됩니다. Kaspersky Endpoint Security는 카테고리 제어에 대한 허용 규칙을 무시합니다. KSWS 및 KES 카테고리의 대응은 아래에서 확인할 수 있습니다.
Allow access if the web page can not be categorized	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 웹 페이지를 분류할 수 없을 시 접근을 허용합니다.
Allow access to legitimate web resources that can be used to damage a protected device	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 보호된 장치를 손상하는 데 사용할 수 있는 합법적인 웹 리소스에 대한 접근을 허용합니다.
Allow access to legitimate advertisement	*(마이그레이션하지 않음)* 웹 제어 설정에서 *배너* 웹 리소스 카테고리를 사용하여 합법적인 광고에 대한 접근을 관리할 수 있습니다.
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 Driver Interceptor 모드만 지원합니다.
ICAP-service connection settings	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 ICAP 네트워크 스토리지 보호를 지원하지 않습니다.
Check safe connections through the HTTPS protocol	**암호화된 연결 검사** / **항상 암호화된 연결 검사** 모드(**네트워크 설정** 하위 섹션)
Use TLS protocol version	*(마이그레이션하지 않음)* Kaspersky Endpoint Security가 다음 프로토콜에 따라 전송된 암호화된 네트워크 트래픽을 검사합니다: • SSL 3.0 • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 암호화된 연결 검사 설정에서 SSL 2.0 연결을 추가로 차단할 수 있습니다.
Do not trust web-servers with invalid certificate	**주소**(**네트워크 설정** 하위 섹션)
Intercept ports (Interception area)	**모니터링하는 포트**(**네트워크 설정** 하위 섹션) 마이그레이션이 진행될 때 KES가 확인란 **Kaspersky에서 권장하는 목록에 있는 애플리케이션의 모든 포트 모니터**와 **지정한 애플리케이션의 모든 포트 모니터**의 선택을 해제합니다.
Exclude ports (Interception area)	*(마이그레이션하지 않음)*
Exclude IP addresses (Interception area)	**신뢰하는 주소 구성**(**네트워크 설정** 하위 섹션)
Exclude processes (Interception area)	**신뢰하는 애플리케이션 구성**(**네트워크 설정** 하위 섹션) 마이그레이션이 진행될 때 KES가 신뢰할 수 있는 애플리케이션에 대해 다음 설정을 구성합니다. • **네트워크 트래픽 검사 안 함** 확인란을 선택합니다. KES가 원격 IP 주소와 포트의 네트워크 트래픽을 검사하지 않습니다. • 신뢰하는 애플리케이션 설정의 나머지 확인란은 선택을 해제합니다.
Security port	*(마이그레이션하지 않음)*
Use malicious URL database to scan web links	**악성 웹 주소 데이터베이스에서 웹 주소 확인**(**웹 위협 보호** 하위 섹션)
Use anti-phishing database to scan web pages	**피싱 웹 주소 데이터베이스에서 웹 주소 확인**(**웹 위협 보호** 하위 섹션)
Use KSN for protection	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 애플리케이션 구성 요소에 KSN을 사용합니다.
Use Trusted Zone	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 구성 요소에 신뢰 구역을 적용합니다. 신뢰 구역 설정에서 예외를 구성할 수 있습니다.

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Use heuristic analyzer	**휴리스틱 분석 사용**(**웹 위협 보호** 및 **메일 위협 보호** 하위 섹션)
Security level	*(마이그레이션하지 않음)* Kaspersky Endpoint Security에는 웹 위협 보호 및 메일 위협 보호 구성 요소에 대한 자체 보안 수준이 있습니다. 기본적으로 Kaspersky Endpoint Security는 권장 보안 수준을 설정합니다.
Enable mail threat protection	**메일 위협 보호**(**메일 위협 보호** 하위 섹션) **Microsoft Outlook 확장 프로그램 연결** **수신 메시지만**(보호 범위) **이메일을 받을 때 검사**(이메일 보호)
Schedule settings	*(마이그레이션하지 않음)* 이 구성 요소에 대해 별도의 스케줄을 구성할 수 없습니다. 이 구성 요소는 Kaspersky Endpoint Security가 작동하는 동안 항상 켜져 있습니다.

Exploit Prevention

KSWS 익스플로잇 공격 방지 설정이 **지능형 위협 보호** 섹션, **익스플로잇 방지** 하위 섹션으로 마이그레이션됩니다.

익스플로잇 방지 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Prevent vulnerable processes exploit: • Terminate on exploit • Notify only	**익스플로잇 탐지 시**: • **차단** • **알림**.
Notify about abused processes via Terminal Service	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 터미널 서비스를 지원하지 않습니다.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 취약한 프로세스 익스플로잇을 지속해서 방지합니다.
Protected processes	**시스템 프로세스 메모리 보호 사용** Kaspersky Endpoint Security는 보호 프로세스 선택을 지원하지 않습니다. 시스템 프로세스 메모리 보호만 활성화할 수 있습니다.
Exploit prevention techniques: • Apply all available exploit prevention techniques • Apply selected exploit prevention techniques	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 사용 가능한 모든 익스플로잇 방지 기술을 적용합니다.

Network Threat Protection

KSWS 네트워크 위협 방지 설정은 **필수 위협 보호** 섹션, **네트워크 위협 보호** 하위 섹션으로 마이그레이션됩니다.

네트워크 위협 보호 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Operation mode: • Pass-through • Only inform about network attacks • Block connections when attack is detected	**네트워크 위협 보호** **Pass-through** 모드를 선택하면 네트워크 위협 보호가 비활성화됩니다. **Only inform about network attacks** 모드 또는 **Block connections when attack is detected** 모드를 선택하면 네트워크 위협 보호가 활성화됩니다. Kaspersky Endpoint Security는 항상 **Block connections when attack is detected** 모드로 작동합니다.
Do not stop traffic analysis when the task is not running	*(마이그레이션하지 않음)* 구성 요소가 활성화되면 Kaspersky Endpoint Security는 트래픽을 지속해서 분석합니다.
Do not control excluded IP addresses	**예외 규칙**
Schedule settings	*(마이그레이션하지 않음)* 이 구성 요소에 대해 별도의 스케줄을 구성할 수 없습니다. 이 구성 요소는 Kaspersky Endpoint Security가 작동하는 동안 항상 켜져 있습니다.

Script Monitoring

Kaspersky Endpoint Security는 스크립트 모니터링 구성 요소를 지원하지 않습니다. 스크립트 모니터링은 AMSI 보호와 같은 다른 구성 요소에서 처리됩니다.

Website categories

Kaspersky Endpoint Security는 Kaspersky Security for Windows Server의 모든 카테고리를 지원하지는 않습니다. Kaspersky Endpoint Security에 존재하지 않는 카테고리는 마이그레이션되지 않습니다. 따라서 지원되지 않는 카테고리가 있는 웹 리소스 분류 규칙은 마이그레이션되지 않습니다.

웹사이트 카테고리

Kaspersky Security for Windows Server 카테고리	Kaspersky Endpoint Security for Windows 카테고리
Wargaming	비디오 게임
Abortion	*(마이그레이션하지 않음)*
Lotteries (extended)	도박, 복권, 내기
Alcohol	술, 담배, 마약
Anonymous proxy servers	익명 서비스
Anorexia	*(마이그레이션하지 않음)*
Rentals for real estate	*(마이그레이션하지 않음)*
Audio, video and software	소프트웨어, 오디오, 비디오
Banks	은행
Blogs	블로그
Military	무기, 폭발물, 군대
For children	*(마이그레이션하지 않음)*
Discrimination	폭력, 편협
Home and family	*(마이그레이션하지 않음)*
Hosting and domain services	인터넷 커뮤니케이션
Pets and animals	*(마이그레이션하지 않음)*
Law and politics	국가별 법에 따라 금지됨
Restricted by Roskomnadzor (RF)	러시아 연방 법에 따라 금지됨
Restricted by Federal Law 436 (RF)	러시아 연방 법에 따라 금지됨
Restricted by RF legislation	러시아 연방 법에 따라 금지됨
Restricted by global legislation	국가별 법에 따라 금지됨
Adult dating	성인 컨텐츠
Internet services	*(마이그레이션하지 않음)*
Sex shops	성인 컨텐츠
Information technologies	*(마이그레이션하지 않음)*
Casinos, card games	도박, 복권, 내기
Books and writing	*(마이그레이션하지 않음)*
Computer games	비디오 게임
Health and beauty	*(마이그레이션하지 않음)*
Culture and society	*(마이그레이션하지 않음)*
LGBT	성인 컨텐츠
Lotteries	도박, 복권, 내기
Medicine	*(마이그레이션하지 않음)*

Kaspersky Security for Windows Server 카테고리	Kaspersky Endpoint Security for Windows 카테고리
Fashion	*(마이그레이션하지 않음)*
Music	*(마이그레이션하지 않음)*
Drugs	술, 담배, 마약
Violence	폭력, 편협
Discontent	*(마이그레이션하지 않음)*
Illegal drugs	술, 담배, 마약
Hate and discrimination	폭력, 편협
Obscene vocabulary	외설, 모독
Lingerie	성인 컨텐츠
News	뉴스 미디어
Nudism	성인 컨텐츠
Education	*(마이그레이션하지 않음)*
Online shopping	온라인 스토어
All communication media	인터넷 커뮤니케이션
Payment by credit cards	결제 시스템
Online shopping (own payment system)	온라인 스토어
Online encyclopedias	*(마이그레이션하지 않음)*
Online banking	은행
Weapons	무기, 폭발물, 군대
Fishing and hunting	*(마이그레이션하지 않음)*
Payment systems	결제 시스템
Job search	취업 검색
Search engines	*(마이그레이션하지 않음)*
Police decision (JP)	일본 법에 따라 금지됨
Trusted by KPSN	*(마이그레이션하지 않음)*
Untrusted by KPSN	*(마이그레이션하지 않음)*
Porn	성인 컨텐츠
Media hosting and streaming	뉴스 미디어
Web Mail	웹 기반 이메일
Traveling	*(마이그레이션하지 않음)*
TV and radio	뉴스 미디어
Teasers and ads services	배너
Religion	종교, 종교 단체
Restaurants, cafe and food	*(마이그레이션하지 않음)*
Dating sites	데이트 사이트
Sex education	성인 컨텐츠
Social networks	소셜 네트워크
Sport	*(마이그레이션하지 않음)*
Betting	도박, 복권, 내기
Suicide	폭력, 편협
Tobacco	술, 담배, 마약

Kaspersky Security for Windows Server 카테고리	Kaspersky Endpoint Security for Windows 카테고리
Torrents	토렌트
Mentioned in Federal list of extremists (RF)	러시아 연방 법에 따라 금지됨
File sharing	파일 공유
Pharmacy	*(마이그레이션하지 않음)*
Hobby and entertainment	*(마이그레이션하지 않음)*
Chats and forums	채팅, 포럼, IM
Schools and universities pages	*(마이그레이션하지 않음)*
Astrology and esoterica	*(마이그레이션하지 않음)*
Extremism and racism	폭력, 편협
E-commerce	온라인 스토어
Erotic	성인 컨텐츠
Humor	*(마이그레이션하지 않음)*

Local activity control

Applications Launch Control

KSWS 애플리케이션 제어 설정은 **보안 제어** 섹션, **애플리케이션 제어** 하위 섹션으로 마이그레이션됩니다.

애플리케이션 실행 제어 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Operation mode: • **Statistics only** • **Active**	**처리**(애플리케이션 제어): • **규칙 테스트** • **규칙 적용**
Repeat action taken for the first file launch on all the subsequent launches for this file	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 실행을 시도할 때마다 애플리케이션을 검사합니다.
Deny the command interpreters launch with no command to execute	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 애플리케이션 제어에서 금지하지 않을 시 명령 인터프리터 실행을 허용합니다.
Rules	**애플리케이션 제어 규칙***(제한적으로 지원)* Kaspersky Endpoint Security 11.11.0부터는 애플리케이션 실행 제어 규칙의 마이그레이션이 지원됩니다. 애플리케이션 실행 제어 규칙 마이그레이션 기능에는 약간의 제한이 있습니다. 기본적으로 KSWS 애플리케이션 실행 제어에는 두 가지 규칙이 있습니다. • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** 한 개 소스 이상의 KSWS 규칙에 **Allow** 유형이 있는 경우 마이그레이션이 진행될 때 KES가 새로운 허용 규칙인 **신뢰할 수 있는 루트 인증서가 있는 애플리케이션**을 생성합니다. 즉, KES 애플리케이션 제어에서 단일 규칙을 사용해 신뢰할 수 있는 스크립트, MSI 패키지, 실행 파일의 실행을 허용합니다. 두 개 소스의 KSWS 규칙에 **Deny** 유형이 있으면 KES가 신뢰할 수 있는 루트 인증서가 있는 애플리케이션을 관리하는 규칙을 추가하지 않습니다.
Apply rules to executable files	*(마이그레이션하지 않음)* KES 애플리케이션 제어 설정에서 규칙 애플리케이션 범위를 구성할 수 없습니다. KES 애플리케이션 제어가 실행 파일, 스크립트, MSI 패키지 등 모든 유형의 파일에 규칙을 적용합니다. KSWS의 규칙 애플리케이션 범위에 모든 파일 유형이 포함된 경우 마이그레이션이 진행될 때 KES가 KSWS 규칙을 전달합니다. KSWS의 규칙 애플리케이션 범위에서 일부 파일 유형을 제외시키면 마이그레이션이 진행될 때 KES가 KSWS 규칙도 전달하지만 애플리케이션 제어 작업으로 **규칙 테스트**가 선택됩니다.
Monitor loading of DLL modules	**DLL 모듈 로드 모니터링(시스템 부하가 상당히 증가합니다)**

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Apply rules to scripts and MSI packages	*(마이그레이션하지 않음)* KES 애플리케이션 제어 설정에서 규칙 애플리케이션 범위를 구성할 수 없습니다. KES 애플리케이션 제어가 실행 파일, 스크립트, MSI 패키지 등 모든 유형의 파일에 규칙을 적용합니다. KSWS의 규칙 애플리케이션 범위에 모든 파일 유형이 포함된 경우 마이그레이션이 진행될 때 KES가 KSWS 규칙을 전달합니다. KSWS의 규칙 애플리케이션 범위에서 일부 파일 유형을 제외시키면 마이그레이션이 진행될 때 KES가 KSWS 규칙을 전달하지만 애플리케이션 제어 작업으로 **규칙 테스트**가 선택됩니다.
Deny applications untrusted by KSN	*(마이그레이션하지 않음)* Kaspersky Endpoint Security가 애플리케이션의 평판을 고려하지 않으며 규칙에 따라 애플리케이션 실행을 허용하거나 거부합니다.
Allow applications trusted by KSN	마이그레이션이 진행될 때 KES가 새 허용 규칙을 추가합니다. **기타 소프트웨어\KSN 평판에 따라 신뢰할 수 있는 애플리케이션** KL 범주가 규칙 트리거 조건으로 지정됩니다.
Users and / or user groups allowed to run applications trusted by KSN	KL 카테고리(**기타 소프트웨어\애플리케이션, KSN 평판에 따라 신뢰**)를 포함하는 애플리케이션 제어 허용 규칙의 **사용자 및 권한**
Automatically allow software distribution via applications and packages listed	KSWS와 KES는 소프트웨어 배포 제어 방식이 다릅니다. 마이그레이션이 진행될 때 KES는 자동 소프트웨어 배포를 허용하는 새로운 허용 규칙을 추가합니다. 파일 해시가 규칙 트리거 조건으로 지정됩니다.
Always allow software distribution via Windows Installer	KSWS와 KES는 소프트웨어 배포 제어 방식이 다릅니다. 마이그레이션이 진행될 때 KES는 자동 소프트웨어 배포를 허용하는 새로운 허용 규칙을 추가합니다(**Software distribution applications and packages allowed**). 파일 해시가 규칙 트리거 조건으로 지정됩니다. 계정 속성에서 **신뢰하는 업데이터** 확인란이 선택되어 있습니다.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(마이그레이션하지 않음)*
Software distribution applications and packages allowed	KSWS와 KES는 소프트웨어 배포 제어 방식이 다릅니다. 마이그레이션이 진행될 때 KES는 자동 소프트웨어 배포를 허용하는 새로운 허용 규칙을 추가합니다. 파일 해시가 규칙 트리거 조건으로 지정됩니다. 계정 속성에서 **신뢰하는 업데이터** 확인란이 선택되어 있습니다.
Schedule settings	*(마이그레이션하지 않음)* KSWS 설정의 구성 요소에 대한 스케줄이 구성된 경우 마이그레이션을 하는 동안 애플리케이션 제어 구성 요소가 사용됩니다. KSWS 설정의 구성 요소에 대한 스케줄이 구성되지 않은 경우에는 마이그레이션을 하는 동안 애플리케이션 제어가 사용되지 않습니다. 이 구성 요소에 대해 별도의 스케줄을 구성할 수 없습니다. 이 구성 요소는 Kaspersky Endpoint Security가 작동하는 동안 항상 켜져 있습니다.

Device Control

KSWS 장치 제어 설정은 **보안 제어** 섹션, **장치 제어** 하위 섹션으로 마이그레이션됩니다.

장치 제어 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Operation mode: • **Active** • **Statistics only**	*(마이그레이션하지 않음)* 애플리케이션 제어는 *Active* 모드에서 작동합니다. 감사에서 장치 연결 통계를 지속해서 제공합니다.
Allow using all external devices when the Device Control task is not running	*(마이그레이션하지 않음)* Kaspersky Endpoint Security가 실행되는 동안 장치 제어는 항상 켜져 있습니다.
Device Control rules	**신뢰하는 장치** 마이그레이션하는 동안 Kaspersky Endpoint Security는 비활성화된 KSWS 규칙을 무시합니다.
Schedule settings	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 특정 장치 유형에 대한 접근 권한을 얻기 위한 자체 스케줄을 사용합니다.

Network-Attached Storages Protection

RPC Network Storage Protection

Kaspersky Endpoint Security는 네트워크 연결 스토리지 보호 구성 요소를 지원하지 않습니다. 이러한 구성 요소가 필요한 경우 Kaspersky Security for Windows Server를 계속 사용할 수 있습니다.

ICAP Network Storage Protection

Kaspersky Endpoint Security는 네트워크 연결 스토리지 보호 구성 요소를 지원하지 않습니다. 이러한 구성 요소가 필요한 경우 Kaspersky Security for Windows Server를 계속 사용할 수 있습니다.

Anti-Cryptor for NetApp

Kaspersky Endpoint Security는 NetApp용 안티 크립터를 지원하지 않습니다. 안티 크립터 기능은 행동 탐지와 같은 다른 애플리케이션 구성 요소에서 제공합니다.

Network activity control

Firewall Management

Kaspersky Endpoint Security는 KSWS 방화벽 관리를 지원하지 않습니다. KSWS 방화벽 기능은 시스템 수준의 방화벽으로 수행됩니다. 마이그레이션 후 Kaspersky Endpoint Security 방화벽을 구성할 수 있습니다.

Anti-Cryptor

네트워크 안티 크립터 설정이 **지능형 위협 보호** 섹션, **행동 탐지** 하위 섹션으로 마이그레이션됩니다.

안티 크립터 설정

KSWS 설정	KES 설정
Operation mode: • **Statistics only** • **Active**	**공유 폴더에 대한 외부 컴퓨터에서의 암호화 시도 탐지 시**: • **알림** • **차단**.
Heuristic analyzer	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 행동 탐지에 휴리스틱 분석을 사용하지 않습니다.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 보호된 컴퓨터의 모든 공유 네트워크 폴더의 암호화를 방지합니다.
Exclusions	*(마이그레이션하지 않음)* Kaspersky Endpoint Security에는 행동 탐지 구성 요소에 대한 자체 예외 규칙이 있습니다. 마이그레이션 후 수동으로 예외 규칙을 추가할 수 있습니다.
Schedule settings	*(마이그레이션하지 않음)* 이 구성 요소에 대해 별도의 스케줄을 구성할 수 없습니다. 이 구성 요소는 Kaspersky Endpoint Security가 작동하는 동안 항상 켜져 있습니다.

System Inspection

File Integrity Monitor

KSWS의 파일 무결성 모니터 설정이 **보안 제어** 섹션, **시스템 무결성 모니터링** 하위 섹션으로 마이그레이션됩니다.

파일 무결성 모니터 설정

KSWS 설정	KES 설정
Log information about file operations that appear during the monitor interruption period	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모니터 중단 시간에 수행되는 파일 작업은 이벤트를 기록하지 않습니다.
Block attempts to compromise the USN log	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 USN 로그를 손상시키려는 시도를 차단하지 않습니다.
Monitoring scope	**모니터링 범위** → **파일***(제한적으로 지원)* 해제된 모니터링 범위 기록은 KES로 마이그레이션되지 않습니다. Kaspersky Endpoint Security는 사용 가능한 기록만 모니터링 범위에 추가합니다.
Trusted users	**신뢰하는 사용자 및/또는 사용자 그룹**
File operation markers	**파일 작동 표식**
Calculate checksum for the file if possible	**해싱**
Exclusions	**예외** → **파일**

Log Inspection

KSWS 로그 검사 설정은 **보안 제어** 섹션, **로그 검사** 하위 섹션으로 마이그레이션됩니다.

로그 검사 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Apply custom rules for log inspection	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 사용 가능한 모든 사용자 지정 규칙을 적용합니다.
Custom rules	**사용자 지정 규칙** **A service was installed in the system (for Server 2003 OS)** 사전 정의된 규칙은 KES로 마이그레이션되지 않습니다.
Apply predefined rules for log inspection	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 사용 가능한 모든 사전 정의된 규칙을 적용합니다.
Predefined rules	**사전 정의된 규칙**
Password brute-force detection	**무차별 대입 공격 감지**
Network logon detection	**네트워크 로그인 탐지**
Exclusions (IP addresses)	**예외 규칙**(IP 주소)
Exclusions (users)	**예외 규칙**(사용자)
Schedule settings	*(마이그레이션하지 않음)* 이 구성 요소에 대해 별도의 스케줄을 구성할 수 없습니다. 이 구성 요소는 Kaspersky Endpoint Security가 작동하는 동안 항상 켜져 있습니다.

Logs and notifications

Task logs

KSWS 로그 설정은 **일반 설정** 섹션, **인터페이스** 및 **리포트 및 저장소** 하위 섹션으로 마이그레이션됩니다.

로그 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Event logging	**알림**(**인터페이스** 하위 섹션)
Logs folder	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 리포트를 `C:\ProgramData\Kaspersky Lab\KES.14.0\Report`에 저장합니다.
Remove task logs older than N day(s)	*(마이그레이션하지 않음)* **일반 설정**, **리포트 및 저장소**에서 KES 리포트의 저장 기간을 구성할 수 있습니다.
Remove from the audit log events N day(s)	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 시스템 감사 리포트를 포함한 모든 리포트에 리포트 저장 제한을 적용합니다.
Integration with SIEM	*(마이그레이션하지 않음)* Kaspersky Security Center에서 SIEM 통합을 구성할 수 있습니다.

Event notifications

KSWS 알림 설정이 **일반 설정** 섹션, **인터페이스** 하위 섹션으로 마이그레이션됩니다.

알림 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Notifications	**알림**
Notify users: • By using terminal service • By using Windows Messenger Service command	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 알림 텍스트 수정을 지원하지 않습니다. Kaspersky Endpoint Security는 표준 알림을 표시합니다.
Notify administrators: • By using Windows Messenger Service command • By running executable file • By sending email	이메일 알림 설정만 Kaspersky Endpoint Security – **이메일 알림 설정**(**알림** 블록)으로 마이그레이션됩니다. 관리자에게 알리는 다른 방법은 지원하지 않습니다.
Application database is out of date	**데이터베이스가 업데이트되지 않았다면 "데이터베이스가 오래됨" 알림 전송**
Application database is extremely out of date	**데이터베이스가 업데이트되지 않았다면 "데이터베이스가 매우 오래됨" 알림 전송**
Critical areas scan has not been performed for a long time	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 3일 후에 누락된 중요 영역 검사 이벤트를 생성합니다.

Interaction with Administration Server

KSWS 중앙 관리 서버 상호 작용 설정은 **일반 설정** 섹션, **리포트 및 저장소** 하위 섹션으로 마이그레이션됩니다.

중앙 관리 서버 상호 작용 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Quarantined files	**격리 저장소 파일**
Backed up files	**백업 파일**
Blocked hosts	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 차단된 호스트에 대한 데이터를 자동으로 전송합니다.

Tasks

Activating the application

Kaspersky Endpoint Security는 *Application activation* 작업(KSWS)을 지원하지 않습니다. *키 추가* 작업(KES)을 만들고, 라이센스 키를 설치 패키지에 추가하거나 자동 라이센스 키 배포를 활성화할 수 있습니다.

Copying Updates

Copying Updates 작업 설정(KSWS)이 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업(KES)으로 마이그레이션됩니다.

업데이트 작업 설정 복사

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Update source: • Kaspersky Security Center Administration Server • Kaspersky update servers • Custom HTTP or FTP servers, or network folders	**업데이트 경로**: • **Kaspersky Security Center** • **Kaspersky 업데이트 서버** • **사용자가 지정함**
Use Kaspersky update servers if specified servers are not available	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 Kaspersky 업데이트 서버를 포함하여 여러 업데이트 경로 선택을 허용합니다. 첫 번째 업데이트 경로를 사용할 수 없을 시 Kaspersky Endpoint Security를 사용하여 목록에 있는 다른 경로에서 업데이트를 가져올 수 있습니다.
Use proxy server settings to connect to Kaspersky update servers	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 구성 요소에 프록시 서버를 사용합니다. 애플리케이션의 네트워크 옵션에서 프록시 서버 연결을 구성할 수 있습니다.
Use proxy server settings to connect to other servers	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 구성 요소에 프록시 서버를 사용합니다. 애플리케이션의 네트워크 옵션에서 프록시 서버 연결을 구성할 수 있습니다.
Copying updates settings: • Copy database updates • Copy critical software modules updates • Copy database updates and critical updates of application modules	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 애플리케이션 모듈의 필수 업데이트와 데이터베이스 업데이트를 단일 패키지로 복사합니다.
Folder for local storage of copied updates	**폴더로 업데이트 파일 복사**

Baseline File Integrity Monitor

Baseline File Integrity Monitor 작업 설정(KSWS)이 *시스템 무결성 검사* 작업 및 정책 섹션 **보안 제어**, 하위 섹션 **시스템 무결성 모니터링**으로 마이그레이션됩니다.

기준 파일 무결성 모니터 작업 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Hash calculation algorithm: • **MD5**. • **SHA256**.	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 체크섬 계산을 위해 SHA256 알고리즘을 사용합니다.
Scan scope	**모니터링 범위**(**시스템 무결성 모니터링** 하위 섹션)

Database Update

Database Update 작업 설정(KSWS)이 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업(KES)으로 마이그레이션됩니다.

데이터베이스 업데이트 작업 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Update source: • Kaspersky Security Center Administration Server • Kaspersky update servers • Custom HTTP or FTP servers, or network folders	**업데이트 경로**: • **Kaspersky Security Center** • **Kaspersky 업데이트 서버** • **사용자가 지정함**
Use Kaspersky update servers if specified servers are not available	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 Kaspersky 업데이트 서버를 포함하여 여러 업데이트 경로 선택을 허용합니다. 첫 번째 업데이트 경로를 사용할 수 없을 시 Kaspersky Endpoint Security를 사용하여 목록에 있는 다른 경로에서 업데이트를 가져올 수 있습니다.
Use proxy server settings to connect to Kaspersky update servers	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 구성 요소에 프록시 서버를 사용합니다. 애플리케이션의 네트워크 옵션에서 프록시 서버 연결을 구성할 수 있습니다.
Use proxy server settings to connect to other servers	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 구성 요소에 프록시 서버를 사용합니다. 애플리케이션의 네트워크 옵션에서 프록시 서버 연결을 구성할 수 있습니다.
Lower the load on the disk I/O	*(마이그레이션하지 않음)*

Software modules updates

Software Modules Update 작업 설정(KSWS)이 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업(KES)으로 마이그레이션됩니다.

소프트웨어 모듈 업데이트 작업 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Update source: • Kaspersky Security Center Administration Server • Kaspersky update servers • Custom HTTP or FTP servers, or network folders	**업데이트 경로**: • **Kaspersky Security Center** • **Kaspersky 업데이트 서버** • **사용자가 지정함**
Use Kaspersky update servers if specified servers are not available	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 Kaspersky 업데이트 서버를 포함하여 여러 업데이트 경로 선택을 허용합니다. 첫 번째 업데이트 경로를 사용할 수 없을 시 Kaspersky Endpoint Security를 사용하여 목록에 있는 다른 경로에서 업데이트를 가져올 수 있습니다.
Use proxy server settings to connect to Kaspersky update servers	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 구성 요소에 프록시 서버를 사용합니다. 애플리케이션의 네트워크 옵션에서 프록시 서버 연결을 구성할 수 있습니다.
Use proxy server settings to connect to other servers	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 구성 요소에 프록시 서버를 사용합니다. 애플리케이션의 네트워크 옵션에서 프록시 서버 연결을 구성할 수 있습니다.
Copy and install critical software modules updates	**긴급 및 승인된 업데이트 설치**
Only check for critical software updates available	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 애플리케이션 모듈에 대한 중요 업데이트를 사용할 수 있는지 계속 확인합니다.
Allow operating system restart	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 사용자에게 컴퓨터를 다시 시작할 권한을 요청합니다.
Receive information about available scheduled software modules updates	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 소프트웨어 모듈 업데이트에 대한 알림을 표시합니다.

Rollback of Application Database Update

Rollback of Application Database Update 작업 설정(KSWS)이 *업데이트 롤백* 작업(KES)으로 마이그레이션됩니다. 새로운 *업데이트 롤백* 작업(KES)에는 작업 시작 스케줄(*수동 시작*이 있습니다.

On-Demand Scan

On-Demand Scan 작업 설정(KSWS)이 *악성 코드 검사* 작업(KES)으로 마이그레이션됩니다.

바이러스 검사 작업 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Scan scope	**검사 범위**
Protection level: • Maximum protection • Recommended • Maximum performance	**보안 레벨**: • **높음** • **권장** • **낮음**. KSWS와 KES의 보안 레벨 설정은 다릅니다.
Objects to scan: • All objects • Objects scanned by format • Objects scanned according to list of extensions specified in anti-virus database • Objects scanned by specified list of extensions	**파일 유형**: • **모든 파일** • **형식에 따라 검사한 파일** • **확장자에 따라 검사한 파일** Kaspersky Endpoint Security는 사용자 지정 확장 목록 생성을 허용하지 않습니다. Kaspersky Endpoint Security가 **Objects scanned by specified list of extensions** 값을 **확장자에 따라 검사한 파일** 값으로 교체합니다.
Subfolders	**하위 폴더 포함**
Subfiles	*(마이그레이션하지 않음)*
Scan disk boot sectors and MBR	*(마이그레이션하지 않음)*
Scan alternate NTFS streams	*(마이그레이션하지 않음)*
Scan only new and modified files	**새로운 파일과 수정된 파일만 검사**
Scan of compound objects: • All archives • All SFX archives • All email databases • All packed objects • All plain email • All embedded OLE objects	**복합 파일 검사**: • **압축파일 검사** • **암호로 보호된 압축 파일 검사** • **배포 패키지 검사** • **이메일 형식 파일 검사** • **Microsoft Office 형식 파일 검사**
Action to perform on infected and other objects: • Disinfect • Disinfect. Remove if disinfection fails • Remove • Perform recommended action • Notify only	**위협 탐지 시 처리 방법**: • **치료 - 불가능한 경우 삭제** • **치료 - 불가능한 경우 알림** • **알림**.
Action to perform on probably infected objects: • Quarantine • Remove • Perform recommended action • Notify only	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 보안 위협이 탐지되면 조치를 적용합니다.
Perform actions depending on the type of object detected	*(마이그레이션하지 않음)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(마이그레이션하지 않음)*
Exclude files	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 모든 구성 요소에 신뢰 구역을 적용합니다. 신뢰 구역 설정에서 예외를 구성할 수 있습니다.
Do not detect	*(마이그레이션하지 않음)*
Stop scanning if it takes longer than N sec	**다음보다 오래 검사하는 파일은 건너뛰기: N초**
Do not scan compound objects larger than N MB	**큰 복합 파일은 압축 해제 안 함**
Use iSwift technology	**iSwift 기술**

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Use iChecker technology	iChecker 기술
Action on the offline files: • Do not scan • Scan resident part of file only • Scan entire file • Only if the file has been accessed within the specified period (days) • Do not copy file to a local hard drive, if possible	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 오프라인 파일 전체를 검사합니다.

Application Integrity Check

Application Integrity Control 작업 설정(KSWS)이 *애플리케이션 무결성 검사* 작업(KES)으로 마이그레이션됩니다.

Rule Generator for Applications Launch Control

Kaspersky Endpoint Security는 *Applications Launch Control Generator* 작업을 지원하지 않습니다. 애플리케이션 제어 설정에서 규칙을 생성할 수 있습니다.

Rule Generator for Device Control

Kaspersky Endpoint Security는 *Rule Generator for Device Control* 작업을 지원하지 않습니다. 장치 제어 설정에서 접근 규칙을 생성할 수 있습니다.

KSWS 구성 요소 마이그레이션

로컬 설치를 진행하기 전에 Kaspersky Endpoint Security가 컴퓨터에 Kaspersky 애플리케이션이 있는지 확인합니다. Kaspersky Security for Windows Server를 컴퓨터에 설치했다면 KES는 설치된 KSWS 구성 요소 집합을 탐지하고 설치를 위해 동일한 구성 요소를 선택합니다.

KSWS에 없는 KES 구성 요소는 다음과 같이 설치됩니다:

- AMSI 보호, 호스트 침입 방지, 복원 엔진은 기본 설정으로 설치됩니다.
- BadUSB 공격 방지, 적응형 이상 행위 제어, 데이터 암호화, Detection and Response 구성 요소는 무시됩니다.

원격으로 설치된 KES 애플리케이션은 설치된 KSWS 구성 요소 집합을 무시합니다. 설치 프로그램은 사용자가 설치 패키지 속성에서 선택한 구성 요소를 설치합니다. Kaspersky Endpoint Security 설치와 정책 및 작업 마이그레이션이 끝나면, KSWS 설정에 따라 KES 설정이 구성됩니다.

KSWS 작업 및 정책 마이그레이션

다음과 같은 방법으로 KSWS 정책 및 작업 설정을 마이그레이션할 수 있습니다.

- 정책 및 작업 변환 마법사(이하 마이그레이션 마법사라고도 함) 사용

> KSWS용 마이그레이션 마법사는 관리 콘솔(MMC)에서만 사용할 수 있습니다. 웹 콘솔 및 Cloud Console에서는 정책 및 작업 설정을 마이그레이션할 수 없습니다.

일괄 변환 마법사가 Kaspersky Security Center의 다른 버전에서 다르게 작동합니다. 솔루션을 버전 14.2 이상으로 업그레이드하는 것이 좋습니다. 이 버전의 Kaspersky Security Center에서는 정책 및 작업 변환 마법사를 사용하여 여러 정책을 단일 정책 대신 단일 프로필로 마이그레이션할 수 있습니다. 또한 이 버전의 Kaspersky Security Center에서는 정책 및 작업 변환 마법사를 사용하여 더 광범위한 정책 설정을 마이그레이션할 수도 있습니다.

- Kaspersky Endpoint Security for Windows용 새 정책 마법사 사용

  새 정책 마법사를 사용하면 KSWS 정책을 기반으로 KES 정책을 생성할 수 있습니다.

마이그레이션 마법사와 새 정책 마법사는 KSWS 정책 마이그레이션 절차가 서로 다릅니다.

정책 및 작업 변환 마법사

마이그레이션 마법사는 KSWS 정책 설정을 KES 정책 설정 대신 정책 프로필로 전송합니다. *정책 프로필*은 컴퓨터가 구성된 활성화 규칙을 충족하는 경우 해당 컴퓨터에서 활성화되는 정책 설정 모음입니다. `UpgradedFromKSWS` 기기 태그가 정책 프로필의 트리거링 기준으로 선택됩니다. Kaspersky Security Center는 원격 설치 작업을 사용하여 KSWS와 함께 KES를 설치하는 모든 컴퓨터에 `UpgradedFromKSWS` 기기 태그를 자동으로 추가합니다. 다른 설치 방법을 선택한 경우 기기에 태그를 수동으로 할당할 수 있습니다.

장치에 태그를 추가하는 방법:

1. 서버에 대한 새 태그인 `UpgradedFromKSWS`를 생성합니다.

   기기에 대한 태그 생성에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

2. Kaspersky Security Center 콘솔에서 새 관리 그룹을 생성하고, 이 그룹에 태그를 할당할 서버를 추가합니다.

   선택 도구를 사용하여 서버를 그룹화할 수 있습니다. 선택 처리에 관한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

3. Kaspersky Security Center 콘솔에서 관리 그룹의 모든 서버를 선택하고, 선택한 서버의 속성을 연 다음 태그를 할당합니다.

여러 KSWS 정책을 마이그레이션하는 경우 각 정책은 단일 중요 정책 내에서 프로필로 변환됩니다. KSWS 정책에 이미 프로필이 포함된 경우, 이러한 프로필도 프로필로 마이그레이션됩니다. 결과적으로 모든 KSWS 정책에 해당하는 프로필이 포함된 단일 정책을 얻게 됩니다.

정책 및 작업 변환 마법사를 사용하여 KSWS 정책 설정을 마이그레이션하는 방법

1. 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

이 단계에서 Kaspersky Endpoint Security for Windows를 선택해야 합니다. 다음 단계로 넘어갑니다.

2단계. 정책 전환

마이그레이션 마법사는 KES 정책 내에 KSWS 정책 프로필을 생성합니다. 정책 프로필로 변환하려는 Kaspersky Security for Windows Server 정책을 선택합니다. 다음 단계로 넘어갑니다.

그러면 마이그레이션 마법사가 정책 변환을 시작합니다. 새 정책 프로필의 이름은 원래 KSWS 정책에 대응합니다.

3단계. 정책 마이그레이션 리포트

마이그레이션 마법사는 정책 마이그레이션 리포트를 생성합니다. 정책 마이그레이션 리포트에는 정책이 변환된 날짜와 시간, 원래 KSWS 정책의 이름, 대상 KES 정책의 이름과 새 정책 프로필의 이름이 포함됩니다.

4단계. 작업 전환

마이그레이션 마법사는 Kaspersky Endpoint Security for Windows에 대한 새 작업을 생성합니다. 작업 목록에서 Kaspersky Endpoint Security에 생성하고자 하는 KSWS 작업을 선택합니다. 새 작업의 이름이 *<KSWS 작업 이름> (변환됨)*과 같이 지정됩니다. 다음 단계로 넘어갑니다.

5단계. 마법사 완료

마법사를 끝냅니다. 결과적으로 마법사는 다음을 수행합니다.

- Kaspersky Endpoint Security 정책에 새 정책 프로필이 추가됩니다.

  정책에 Kaspersky Security for Windows Server 설정과 프로필이 포함됩니다. 새 정책은 *활성* 상태입니다. 마법사는 KSWS 정책을 변경하지 않은 상태로 둡니다.

- 새 Kaspersky Endpoint Security 작업을 생성합니다.

  새 작업은 KSWS 작업의 복사본입니다. 마법사는 KSWS 작업을 변경하지 않은 상태로 둡니다.

KSWS 설정이 있는 새 정책 프로필의 이름은 *UpgradedFromKSWS <Kaspersky Security for Windows Server 정책 이름>*이 됩니다. 프로필 속성에서 마이그레이션 마법사는 `UpgradedFromKSWS` 기기 태그를 트리거링 기준으로 자동으로 선택합니다. 따라서 정책 프로필의 설정이 서버에 자동으로 적용됩니다.

KSWS 정책을 기반으로 정책을 생성하는 마법사

KSWS 정책을 기반으로 KES 정책이 생성되면, 마법사는 그에 따라 설정을 새 정책으로 전송합니다. 따라서 단일 KES 정책은 단일 KSWS 정책에 대응하게 됩니다. 마법사는 정책을 프로필로 변환하지 않습니다.

새 정책 마법사를 사용하여 KSWS 정책 설정을 마이그레이션하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 선택합니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. **새 정책**을 클릭합니다.
   정책 마법사가 시작됩니다.
5. 정책 마법사의 안내를 따릅니다.

1단계. 그룹 정책을 생성할 애플리케이션 선택

Kaspersky Endpoint Security for Windows (14.0) 애플리케이션을 선택합니다.

2단계. 그룹 정책 이름 지정

그룹 정책의 이름을 입력합니다(예: *오피스 정책*).

이전 애플리케이션 버전에 대한 정책 설정 사용 확인란을 선택합니다. **찾기**를 클릭하고 KSWS 정책을 선택합니다.

3단계. Kaspersky Security Network 참여

Kaspersky Security Network(KSN) 진술문 약관을 읽고 동의해 주십시오.

4단계. 컴퓨터의 애플리케이션 사용 모드 선택

호스트를 보호하는 표준 모드 옵션을 선택합니다. Kaspersky Endpoint Security는 모든 애플리케이션 모드와 OS 유형에 대한 공통 정책을 제공합니다.

> 모드 및 운영 체제 유형에 따라 다른 정책을 사용하는 것이 좋습니다.

5단계. 설정 가져오는

이 단계는 4단계에서 수동 정책 구성을 선택한 경우에 수행할 수 있습니다.

CFG 구성 파일에서 Kaspersky Endpoint Security 설정을 기반으로 정책을 생성할 수 있습니다. 애플리케이션 구성 파일을 가져올 때 마법사에서 모든 정책 설정을 사용할 수 있는 것은 아닙니다. 예를 들어 애플리케이션 설정에서 정책 프로필이 누락될 수 있습니다. 모든 설정과 프로필을 정책으로 전송하려면 KLP 파일에서 다른 정책 가져오기를 수행할 수 있습니다.

구성 파일을 가져올 때 Kaspersky Endpoint Security는 암호화 컨테이너의 암호를 전송하지 않습니다. 서버에 연결할 때 양방향 인증을 사용하는 경우 암호화 컨테이너의 암호를 처음부터 지정해야 합니다.

6단계 – 10단계. 정책 설정 구성

이 단계는 4단계에서 수동 정책 구성을 선택한 경우에 수행할 수 있습니다.

다음 단계에 따라 정책 설정을 관리합니다.

11 단계. 신뢰 구역 구성

신뢰 영역을 구성합니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 추가할 수 있습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션도 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security in Light Agent 모드를 빠르게 구성하는 데 도움이 될 수 있습니다.

12 단계. 정책 상태 선택

- **활성**. 다음 동기화 이후 정책이 컴퓨터에서 활성 정책으로 사용됩니다.

  활성 정책의 설정은 동기화 중에 클라이언트 컴퓨터에 저장됩니다. 여러 정책을 컴퓨터 한 대에 동시에 적용할 수는 없으므로 각 그룹에서는 정책 하나만 활성 상태일 수 있습니다.

- **비활성**. 백업 정책입니다. 필요시 비활성 정책을 활성 상태로 전환할 수 있습니다.

  비활성 정책은 수에 제한 없이 생성할 수 있습니다. 비활성 정책은 네트워크에 있는 컴퓨터의 애플리케이션 설정에 영향을 주지 않습니다. 비활성 정책은 바이러스 공격과 같은 비상 상황을 준비하기 위한 것입니다. 플래시 드라이브를 통한 공격이 진행되면 플래시 드라이브 접근을 차단하는 정책을 활성화할 수 있습니다. 이 경우 활성 상태였던 정책은 자동으로 비활성화됩니다.

- **이동 사용자**. 컴퓨터가 조직 네트워크 외부로 이동하면 이 정책이 활성화됩니다.

마법사를 끝냅니다.

마이그레이션 후 정책 및 작업 추가 구성

KSWS와 KES는 구성 요소 및 정책 설정 집합이 서로 다릅니다. 따라서 마이그레이션이 끝나면 정책 설정이 회사 보안 요구 사항을 충족하는지 확인해야 합니다.

다음 기본 정책 설정을 확인하십시오.

- 암호 보호. KSWS 암호 보호 설정은 마이그레이션되지 않습니다. Kaspersky Endpoint Security에는 암호 보호 기능이 내장되어 있습니다. 필요한 경우 암호 보호를 켜고 암호를 설정합니다.
- 신뢰 구역. KSWS와 KES에서 객체 선택에 사용하는 방법은 다릅니다. 마이그레이션 시 KES는 개별 파일 또는 파일/폴더 경로로 정의된 예외를 지원합니다. KSWS에 사전 정의된 영역 또는 스크립트 URL로 구성된 예외가 있을 시 이러한 예외는 마이그레이션되지 않습니다. 마이그레이션 후에는 이러한 예외를 수동으로 추가해야 합니다.

  Kaspersky Endpoint Security가 서버에서 올바르게 작동하게 하려면, 서버 작용과 관련된 중요 파일을 신뢰 구역에 추가하는 것이 좋습니다. SQL 서버의 경우 MDF 및 LDF 데이터베이스 파일을 추가해야 합니다. Microsoft Exchange 서버의 경우 CHK, EDB, JRS, LOG 및 JSL 파일을 추가해야 합니다. 마스크(예: `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`)를 사용할 수도 있습니다.

  Kaspersky Endpoint Security 12.6 for Windows부터 검사 예외 및 신뢰하는 애플리케이션 이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다.

- 방화벽. KSWS 방화벽 기능은 시스템 수준의 방화벽으로 수행됩니다. KES에서는 별도의 구성 요소가 방화벽 기능을 담당합니다. 마이그레이션 후 Kaspersky Endpoint Security 방화벽을 구성할 수 있습니다.
- Kaspersky Security Network. Kaspersky Endpoint Security는 개별 구성 요소에 대한 KSN 구성을 지원하지 않습니다. Kaspersky Endpoint Security는 모든 애플리케이션 구성 요소에 KSN을 사용합니다. KSN을 사용하려면 Kaspersky Security Network 진술문의 새 약관에 동의해야 합니다.
- 웹 제어. 웹 트래픽 카테고리 제어를 위한 차단 규칙은 Kaspersky Endpoint Security의 단일 차단 규칙으로 마이그레이션됩니다. Kaspersky Endpoint Security는 카테고리 제어에 대한 허용 규칙을 무시합니다. Kaspersky Endpoint Security는 Kaspersky Security for Windows Server의 모든 카테고리를 지원하지는 않습니다. Kaspersky Endpoint Security에 존재하지 않는 카테고리는 마이그레이션되지 않습니다. 따라서 지원되지 않는 카테고리가 있는 웹 리소스 분류 규칙은 마이그레이션되지 않습니다. 필요한 경우 웹 제어 규칙을 추가합니다.
- 프록시 서버. 프록시 서버 연결 암호는 마이그레이션되지 않습니다. 프록시 서버에 수동으로 연결하는 데 사용할 암호를 입력합니다.
- 개별 구성 요소의 스케줄. Kaspersky Endpoint Security는 개별 구성 요소의 스케줄 구성을 지원하지 않습니다. 이 구성 요소는 Kaspersky Endpoint Security가 작동하는 동안 항상 켜져 있습니다.
- 구성 요소 집합. 사용 가능한 Kaspersky Endpoint Security 기능 세트는 운영 체제 유형에 따라 달라집니다: 워크스테이션 또는 서버. 예를 들어 암호화 도구 중에서는 BitLocker 드라이브 암호화만 서버에서 사용할 수 있습니다.

- 속성. 속성의 상태는 마이그레이션되지 않습니다. 속성에는 기본 값이 적용됩니다. 기본적으로 새 정책의 거의 모든 설정은 자식 정책 및 로컬 애플리케이션 인터페이스의 설정 수정을 금지합니다. 속성에는 **Managed Detection and Response(Industrial CyberSecurity)** 섹션과 **사용자 지원** 설정 그룹(**인터페이스** 설정)의 정책 설정을 위한 값이 있습니다. 필요한 경우 부모 정책에서 설정의 상속을 구성합니다.

- 처리 안 된 위협에 대한 작업. 고급 치료는 워크 스테이션 및 서버에서 다른 방식으로 작동합니다. *악성 코드 검사* 작업 설정과 애플리케이션 설정에서 고급 치료를 구성할 수 있습니다.

- 애플리케이션 업그레이드. 다시 시작하지 않고 주요 업데이트 및 패치를 설치하려면 애플리케이션 업그레이드 모드를 변경해야 합니다. 재시작 없이 애플리케이션 업데이트 설치 기능은 기본적으로 비활성화됩니다.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security에는 Detection and Response 솔루션과 함께 작동하는 내장 에이전트가 있습니다. 필요한 경우 Kaspersky Endpoint Agent 정책 설정을 Kaspersky Endpoint Security 정책으로 전송합니다.

- *데이터베이스 및 애플리케이션 모듈 업데이트* 작업. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업의 설정이 올바르게 마이그레이션되었는지 확인합니다. KES는 KSWS의 세 가지 작업 대신 단일 KES 작업을 사용합니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 최적화하고 불필요한 작업을 제거할 수 있습니다.

- 기타 작업. 애플리케이션 제어, 장치 제어 및 파일 무결성 모니터 구성 요소는 KSWS와 KES에서 서로 다르게 작동합니다. KES는 *Baseline File Integrity Monitor*, *Applications Launch Control Generator*, *Rule Generator for Device Control* 작업을 사용하지 않습니다. 따라서 이러한 작업은 마이그레이션되지 않습니다. 마이그레이션이 끝나면 파일 무결성 모니터, 애플리케이션 제어 및 장치 제어 구성 요소를 구성할 수 있습니다.

KSWS 신뢰 구역 마이그레이션

*신뢰 구역*은 Kaspersky Endpoint Security에서 감시하지 않는 개체 및 애플리케이션을 시스템 관리자가 구성한 목록입니다. *정책 및 작업 변환 마법사*나 *KSWS 정책 기반 새 KES 정책 생성 마법사*를 사용해 KSWS에서 KES로 신뢰 구역 개체를 마이그레이션할 수 있습니다. KSWS와 KES는 구성 요소 및 기능 집합이 서로 다릅니다. 따라서 마이그레이션이 끝나면 예외가 회사 보안 요구 사항을 충족하는지 확인해야 합니다. 신뢰 구역에 예외를 추가하는 방법도 KES 및 KSWS에 따라 다릅니다. 마이그레이션 마법사에는 모든 KSWS 예외를 마이그레이션하는 도구가 포함되어 있지 않습니다. 따라서 마이그레이션 후 일부 KSWS 예외는 수동으로 추가해야 합니다.

Kaspersky Endpoint Security가 서버에서 올바르게 작동하게 하려면, 서버 작용과 관련된 중요 파일을 신뢰 구역에 추가하는 것이 좋습니다. SQL 서버의 경우 MDF 및 LDF 데이터베이스 파일을 추가해야 합니다. Microsoft Exchange 서버의 경우 CHK, EDB, JRS, LOG 및 JSL 파일을 추가해야 합니다. 마스크(예: `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`)를 사용할 수도 있습니다.

Kaspersky Endpoint Security 12.6 for Windows부터 검사 예외 및 신뢰하는 애플리케이션 이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다.

KES 및 KSWS 신뢰 구역 생성 방법.

KSWS		KES
Object to scan		
• Predefined scope	*(마이그레이션하지 않음)*	
• Disk, folder or network location	→	**파일 또는 폴더**
• File	→	**파일 또는 폴더**
• Script file or web address	*(마이그레이션하지 않음)*	
Detected object	→	**탐지된 개체 유형**
Trusted processes	→	**신뢰하는 애플리케이션**

검사된 개체 마이그레이션

속성에서 **Object to scan** 방법이 선택된 KSWS 예외는 몇 가지 제한 사항이 있지만 속성에서 **파일 또는 폴더** 방법이 선택된 KES 예외로 마이그레이션됩니다. 예외 마이그레이션은 개체 선택 방법에 따라 다릅니다.

- Predefined scope – *마이그레이션하지 않습니다*.

  마이그레이션 후에는 이러한 예외를 수동으로 추가해야 합니다. 사전 정의된 영역으로 예외는 *악성 코드 검사* 작업 설정에서 구성해야 합니다.

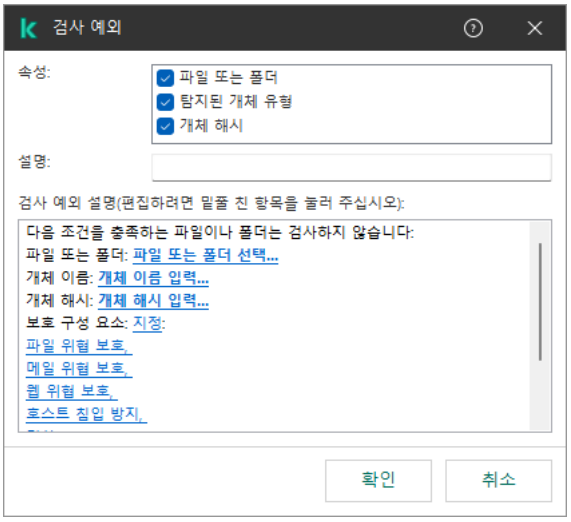
- Disk, folder or network location – 속성에서 "파일 또는 폴더" 방법이 선택된 KES 예외로 마이그레이션합니다.

- File – 속성에서 "파일 또는 폴더" 방법이 선택된 KES 예외로 마이그레이션합니다.

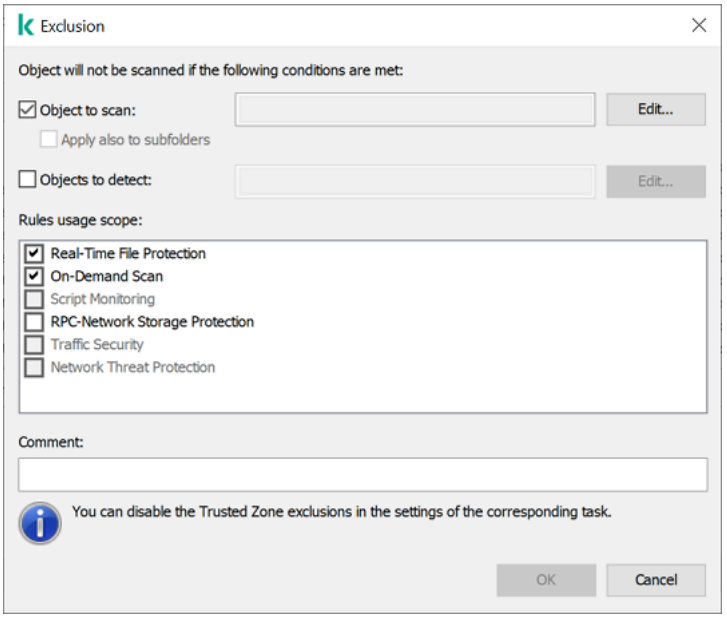
- Script file or web address – *마이그레이션하지 않습니다*.

  마이그레이션 후에는 이러한 예외를 수동으로 추가해야 합니다. 웹 위협 보호를 위해 신뢰하는 웹 주소에 스크립트 웹 주소로 예외를 추가해야 합니다.

검사된 개체에 **Apply also to subfolders** 확인란이 선택된 경우 이 설정은 KES 예외로 마이그레이션됩니다(**하위 폴더 포함** 확인란).



KES 예외 설정



KSWS 예외 설정

탐지된 개체 마이그레이션

속성에서 **Detected object** 방법이 선택된 KSWS 예외는 속성에서 **탐지된 개체 유형** 방법이 선택된 KES 예외로 마이그레이션됩니다. Kaspersky 백과사전(`Email-Worm`, `Rootkit`, `RemoteAdmin` 등)의 분류에 따라 탐지된 개체 이름입니다. Kaspersky Endpoint Security는 물음표 `?`(모든 단일 문자에 대응) 및 별표 `*`(모든 연속 문자에 대응)를 지원합니다.

예외 사용 범위 마이그레이션

예외 사용 범위는 예외가 적용되는 구성 요소의 집합입니다. KES와 KSWS는 구성 요소 집합이 다르므로 마이그레이션 마법사는 예외 사용 범위를 마이그레이션할 수 없습니다. 따라서 KSWS 사용 범위에서 하나 이상의 구성 요소가 선택되면 KES는 모든 애플리케이션 구성 요소에 예외를 적용합니다.

신뢰 구역 설정 및 KSWS 보호 구성 요소 설정에서 KSWS 사용 범위를 구성할 수 있습니다. 구성하려면 정책의 해당 섹션에서 **Apply Trusted Zone** 확인란을 선택하거나 삭제할 수 있습니다. KES 보호 구성 요소 설정에는 이러한 확인란이 없습니다. 따라서 개별 구성 요소 설정의 신뢰 구역 상태는 마이그레이션을 하는 동안 손실됩니다. 마이그레이션이 완료되면 KES 정책에서 신뢰 구역 설정에 예외를 적용하는 구성 요소를 선택합니다.

메모 마이그레이션

KSWS 신뢰 구역의 메모는 수정 없이 KES 예외 메모로 마이그레이션됩니다.

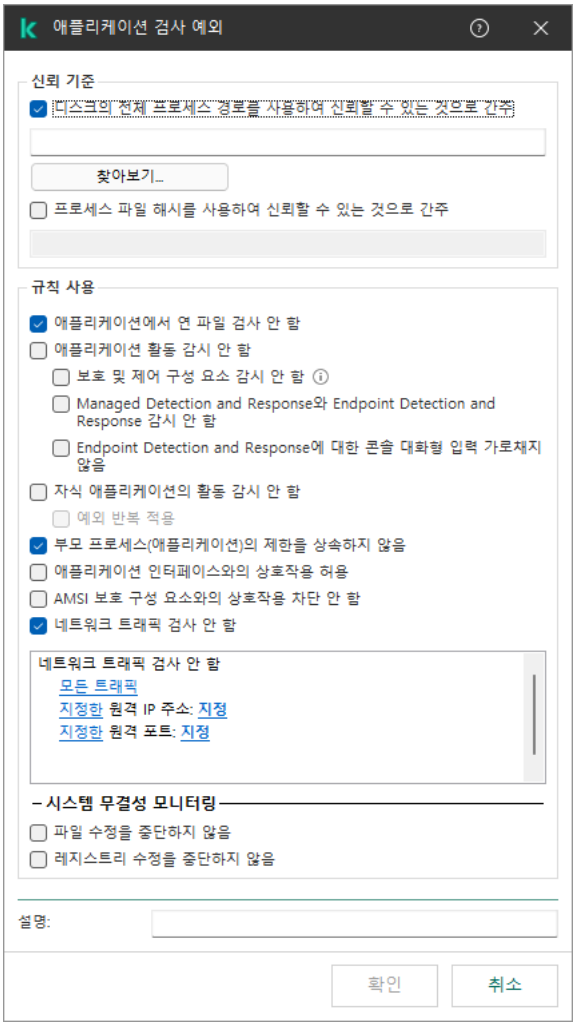
신뢰하는 프로세스 마이그레이션

KSWS 신뢰하는 프로세스는 몇 가지 제한 사항이 있지만 KES 신뢰하는 프로세스로 마이그레이션됩니다. 신뢰하는 프로세스 마이그레이션은 개체 선택 방법에 따라 다릅니다.

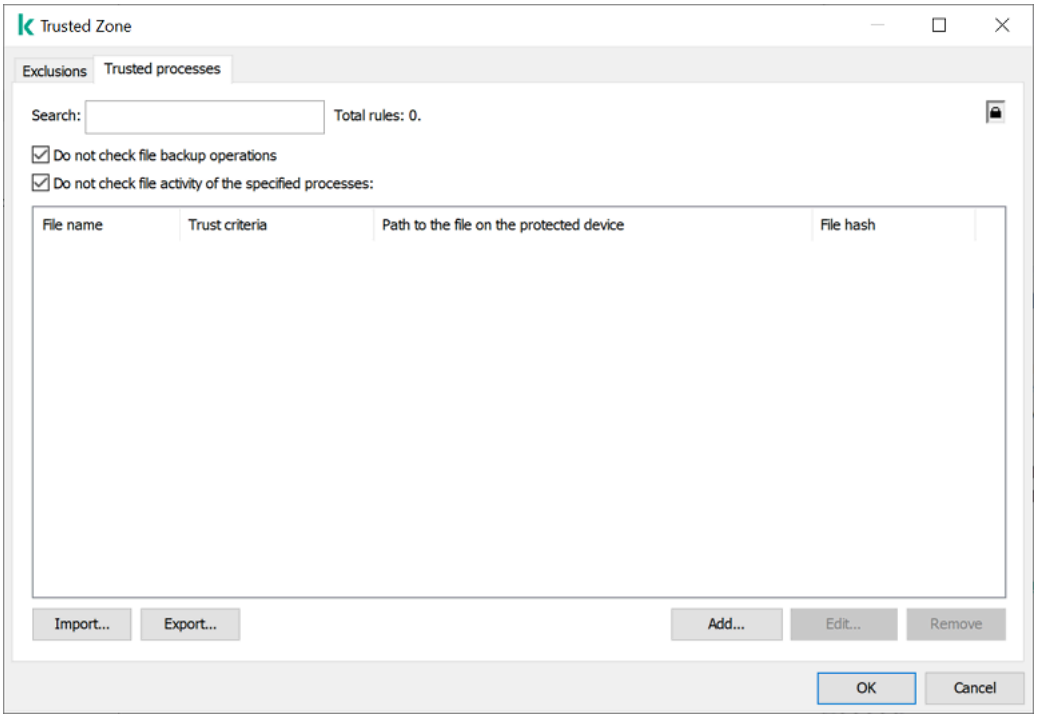
- Path to the file on the protected device – KES 신뢰하는 애플리케이션으로 마이그레이션됩니다.
- File hash – *마이그레이션하지 않습니다.*

KSWS에 파일 해시처럼 구성된 신뢰하는 프로세스가 있다면 이러한 신뢰하는 프로세스는 마이그레이션되지 않습니다. 마이그레이션 후 이러한 신뢰하는 프로세스를 수동으로 추가해야 합니다.

신뢰하는 프로세스 설정에서 **Do not check file backup operations** 확인란이 선택된 경우, 이 설정은 KES 신뢰하는 애플리케이션으로 마이그레이션됩니다(**애플리케이션 활동 감시 안 함** 확인란).



KES 신뢰하는 애플리케이션 설정



KSWS 신뢰하는 프로세스 설정

KSWS 애플리케이션 실행 제어 규칙 마이그레이션

KSWS 애플리케이션 실행 제어는 기본적으로 차단됩니다. 즉, 애플리케이션 실행 제어는 규칙에 허용된 애플리케이션으로 지정되지 않은 모든 애플리케이션을 자동으로 차단합니다. 따라서 KES 애플리케이션 제어용 마이그레이션 마법사는 기본적으로 차단되는 원칙에 해당되는 **허용 목록**을 자동으로 설정합니다.

*정책 및 작업 변환 마법사*나 *KSWS 정책 기반 새 KES 정책 생성 마법사*를 사용해 KSWS에서 KES로 규칙을 마이그레이션할 수 있습니다.

애플리케이션 실행 제어 모드 마이그레이션

KSWS 애플리케이션 실행 제어 모드는 다음과 같이 KES 애플리케이션 제어로 마이그레이션됩니다:

- **Statistics only → 규칙 테스트**
- **Active → 규칙 적용**

KSWS 애플리케이션 실행 제어 사전 정의된 규칙 마이그레이션

기본적으로 KSWS 애플리케이션 실행 제어에는 두 가지 규칙이 있습니다.

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

사전 정의된 규칙은 신뢰할 수 있는 루트 인증서로 서명된 *스크립트*, *MSI 패키지*, 그리고 *실행 파일*을 실행할 수 있도록 합니다. 한 개 이상의 사전 정의된 KSWS 규칙에 **Allow** 유형이 있는 경우 마이그레이션이 마법사가 새로운 허용 규칙인 **신뢰할 수 있는 루트 인증서가 있는 애플리케이션**을 생성합니다. 즉, KES 애플리케이션 제어에서 단일 규칙을 사용해 신뢰할 수 있는 스크립트, MSI 패키지, 실행 파일의 실행을 허용합니다.

KSWS의 사전 정의된 규칙이 모두 **Deny** 유형인 경우 KES는 사전 정의된 규칙을 무시합니다.

KSWS 애플리케이션 실행 제어 사용자 지정 규칙 마이그레이션

KSWS 애플리케이션 실행 제어 규칙은 다음 기준에 따라 파일 실행을 규제합니다:

- 디지털 인증서 서명
- SHA256 해시
- 파일 경로

KSWS 및 KES에서 규칙이 다르게 생성되므로 마이그레이션 마법사에서 KSWS 규칙의 조건 및 예외 규칙이 포함되는 *애플리케이션 카테고리*를 생성하고, 이러한 애플리케이션 카테고리를 KES 규칙에 추가합니다. 마법사는 애플리케이션 카테고리에서 **인증서**, **폴더 경로**, 그리고 **파일 해시** 조건을 사용합니다. 새 애플리케이션 카테고리는 Kaspersky Security Center 관리 콘솔의 **애플리케이션 관리 → 애플리케이션 카테고리** 섹션에서 사용할 수 있습니다.

마이그레이션 마법사는 유형 및 사용자별로 KSWS 규칙을 그룹화합니다. 다음으로, 마법사는 KSWS 규칙의 조건 및 예외를 포함하는 애플리케이션 카테고리를 생성하고 새 KES 규칙에 애플리케이션 카테고리를 추가합니다. 마법사는 KES 규칙의 **설명** 필드에 KSWS 규칙의 이름을 지정합니다.

KSWS 애플리케이션 실행 제어 고급 설정 마이그레이션

KSWS 애플리케이션 실행 제어와 KES 애플리케이션 제어의 작동 원리가 다르기 때문에 마이그레이션 마법사는 설정의 일부만 마이그레이션할 수 있습니다.

애플리케이션 실행 제어 설정

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Repeat action taken for the first file launch on all the subsequent launches for this file	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 실행을 시도할 때마다 애플리케이션을 검사합니다.
Deny the command interpreters launch with no command to execute	*(마이그레이션하지 않음)* Kaspersky Endpoint Security는 애플리케이션 제어에서 금지하지 않을 시 명령 인터프리터 실행을 허용합니다.
Apply rules to executable files	*(마이그레이션하지 않음)* KES 애플리케이션 제어 설정에서 규칙 애플리케이션 범위를 구성할 수 없습니다. KES 애플리케이션 제어가 실행 파일, 스크립트, MSI 패키지 등 모든 유형의 파일에 규칙을 적용합니다. KSWS의 규칙 애플리케이션 범위에 모든 파일 유형이 포함된 경우 마이그레이션이 진행될 때 KES가 KSWS 규칙을 전달합니다. KSWS의 규칙 애플리케이션 범위에서 일부 파일 유형을 제외시키면 마이그레이션이 진행될 때 KES가 KSWS 규칙도 전달하지만 애플리케이션 제어 작업으로 **규칙 테스트**가 선택됩니다.
Monitor loading of DLL modules	**DLL 모듈 로드 모니터링(시스템 부하가 상당히 증가합니다)**
Apply rules to scripts and MSI packages	*(마이그레이션하지 않음)* KES 애플리케이션 제어 설정에서 규칙 애플리케이션 범위를 구성할 수 없습니다. KES 애플리케이션 제어가 실행 파일, 스크립트, MSI 패키지 등 모든 유형의 파일에 규칙을 적용합니다. KSWS의 규칙 애플리케이션 범위에 모든 파일 유형이 포함된 경우 마이그레이션이 진행될 때 KES가 KSWS 규칙을 전달합니다. KSWS의 규칙 애플리케이션 범위에서 일부 파일 유형을 제외시키면 마이그레이션이 진행될 때 KES가 KSWS 규칙을 전달하지만 애플리케이션 제어 작업으로 **규칙 테스트**가 선택됩니다.
Deny applications untrusted by KSN	*(마이그레이션하지 않음)* Kaspersky Endpoint Security가 애플리케이션의 평판을 고려하지 않으며 규칙에 따라 애플리케이션 실행을 허용하거나 거부합니다.
Allow applications trusted by KSN	마이그레이션이 진행될 때 KES가 새 허용 규칙을 추가합니다. **기타 소프트웨어\KSN 평판에 따라 신뢰할 수 있는 애플리케이션** KL 범주가 규칙 트리거 조건으로 지정됩니다.
Users and / or user groups allowed to run applications trusted by KSN	KL 카테고리(**기타 소프트웨어\애플리케이션, KSN 평판에 따라 신뢰**)를 포함하는 애플리케이션 제어 허용 규칙의 **사용자 및 권한**
Automatically allow software distribution via applications and packages listed	KSWS와 KES는 소프트웨어 배포 제어 방식이 다릅니다. 마이그레이션이 진행될 때 KES는 자동 소프트웨어 배포를 허용하는 새로운 허용 규칙을 추가합니다. 파일 해시가 규칙 트리거 조건으로 지정됩니다.
Always allow software distribution via Windows Installer	KSWS와 KES는 소프트웨어 배포 제어 방식이 다릅니다. 마이그레이션이 진행될 때 KES는 자동 소프트웨어 배포를 허용하는 새로운 허용 규칙을 추가합니다(**Software distribution applications and packages allowed**). 파일 해시가 규칙 트리거 조건으로 지정됩니다. 계정 속성에서 **신뢰하는 업데이터** 확인란이 선택되어 있습니다.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(마이그레이션하지 않음)*

Kaspersky Security for Windows Server 설정	Kaspersky Endpoint Security for Windows 설정
Software distribution applications and packages allowed	KSWS와 KES는 소프트웨어 배포 제어 방식이 다릅니다. 마이그레이션이 진행될 때 KES는 자동 소프트웨어 배포를 허용하는 새로운 허용 규칙을 추가합니다. 파일 해시가 규칙 트리거 조건으로 지정됩니다. 계정 속성에서 **신뢰하는 업데이터** 확인란이 선택되어 있습니다.
Schedule settings	*(마이그레이션하지 않음)* KSWS 설정의 구성 요소에 대한 스케줄이 구성된 경우 마이그레이션을 하는 동안 애플리케이션 제어 구성 요소가 사용됩니다. KSWS 설정의 구성 요소에 대한 스케줄이 구성되지 않은 경우에는 마이그레이션을 하는 동안 애플리케이션 제어가 사용되지 않습니다. 이 구성 요소에 대해 별도의 스케줄을 구성할 수 없습니다. 이 구성 요소는 Kaspersky Endpoint Security가 작동하는 동안 항상 켜져 있습니다.

KSWS 대신 KES 설치

Kaspersky Endpoint Security는 다음과 같은 방법으로 설치할 수 있습니다.

- KSWS 제거 후 KES 설치(권장)
- KSWS와 함께 KES 설치

Kaspersky Security for Windows Server 제거

애플리케이션을 원격으로 제거 작업을 사용하여 애플리케이션을 원격으로 제거하거나 서버에서 로컬로 제거할 수 있습니다. KSWS를 제거한 후에는 서버를 다시 시작해야 할 수 있습니다. 다시 시작하지 않고 Kaspersky Endpoint Security를 설치하려는 경우에는 Kaspersky Security for Windows Server가 완전히 제거되었는지 확인하십시오. 애플리케이션이 완전히 제거되지 않은 상태에서 Kaspersky Endpoint Security를 설치하면 서버가 제대로 작동하지 않을 수 있습니다. kavremover 유틸리티를 사용한 경우 애플리케이션이 완전히 제거되었는지 확인하는 것이 좋습니다. kavremover 유틸리티는 KSWS 관리를 지원하지 않습니다.

암호 보호를 사용하여 KSWS에 대한 접근을 제한하려면 KES 설치 패키지의 설정에 제거 암호를 입력합니다.

KSWS를 제거한 후에는 아무 방법을 이용해 Windows용 Kaspersky Endpoint Security를 설치하십시오.

Kaspersky Endpoint Security 설치

KES를 원격으로 설치하는 경우 설치 패키지 속성에서 선택한 구성 요소가 서버에 설치됩니다. 설치 패키지 속성에서 기본 구성 요소를 선택하는 것이 좋습니다. KSWS와 함께 KES를 설치할 때는 다시 시작하지 않아도 됩니다.

로컬 설치를 진행하기 전에 Kaspersky Endpoint Security가 컴퓨터에 Kaspersky 애플리케이션이 있는지 확인합니다. Kaspersky Security for Windows Server를 컴퓨터에 설치했다면 KES는 설치된 KSWS 구성 요소 집합을 탐지하고 설치를 위해 동일한 구성 요소를 선택합니다. KSWS와 함께 KES를 설치할 때는 다시 시작하지 않아도 됩니다.

KSWS와 함께 KES를 설치하지 못한 경우 설치를 롤백할 수 있습니다. 설치 롤백 후 서버를 다시 시작한 다음 설치를 다시 시도하는 것이 좋습니다.

Kaspersky Endpoint Security for Windows를 설치했다면 KSWS 설정 및 작업이 마이그레이션되지 않습니다. 설정 및 작업을 마이그레이션하려면 정책 및 작업 변환 마법사를 실행합니다.

애플리케이션 인터페이스의 **보안** 섹션이나 컴퓨터 속성의 Kaspersky Security Center 콘솔에서, 또는 `status` 명령을 사용하여 설치된 구성 요소 목록을 확인할 수 있습니다. 설치한 후에는 *애플리케이션 구성 요소 변경*을 사용하여 구성 요소 세트를 변경할 수 있습니다.

[KSWS+KEA] 구성을 [KES+내장 에이전트] 구성으로 마이그레이션

Kaspersky Endpoint Security for Windows를 EDR(KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA, 그리고 MDR의 일부로 사용하는 것을 지원하기 위해 애플리케이션에 내장 에이전트가 추가되었습니다. 이제 Kaspersky Endpoint Agent 애플리케이션이 없어도 이 솔루션을 이용할 수 있습니다.

KSWS에서 KES로 마이그레이션하는 경우 EDR(KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA 및 MDR 솔루션은 여전히 Kaspersky Endpoint Security 내장 에이전트와 함께 사용할 수 있습니다. 또한 Kaspersky Endpoint Agent가 컴퓨터에서 제거됩니다.

[KSWS+KEA] 구성을 [KES+내장 에이전트]로 마이그레이션하는 단계는 다음과 같습니다:

1. **KSWS에서 KES로 마이그레이션**

   KSWS에서 KES로 마이그레이션하는 작업에는 Kaspersky Security for Windows Server가 아닌 Kaspersky Endpoint Security의 설치가 포함됩니다.

   관리자는 일반적으로 암호 보호를 사용하여 KSWS 및 KEA에 대한 접근을 제한합니다. Kaspersky Security Center Linux 15.1부터는 *원격으로 애플리케이션 설치* 작업 설정에서 애플리케이션 제거 암호를 입력할 수 있습니다. 이 작업에서는 제거 암호 입력을 하나만 허용합니다. 즉, KSWS 및 KEA에 동일한 암호가 설정되어 있으면 KSWS 및 KEA 애플리케이션이 성공적으로 제거됩니다. 암호가 다르면 애플리케이션 중 하나는 접근 오류와 함께 제거가 실패합니다. 마이그레이션을 완료하려면 *원격으로 애플리케이션 설치* 설정에서 암호를 입력할 수 없던 애플리케이션에 대해 암호 보호를 비활성화해야 합니다.

   마이그레이션을 수행하려면 Detection and Response 솔루션을 지원하는데 필요한 구성 요소를 Kaspersky Endpoint Security의 구성 요소로 선택해야 합니다. 애플리케이션이 설치되면 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다.

2. **정책 및 작업 마이그레이션**

[KSWS+KEA] 정책 및 작업을 [KES+내장 에이전트]로 마이그레이션하는 단계는 다음과 같습니다.

1. 정책 및 작업 변환 마법사를 사용하여 KSWS에서 KES로 정책 및 작업 마이그레이션(관리 콘솔(MMC)에서만 사용 가능).

   이렇게 하면 *UpgradedFromKSWS <Kaspersky Security for Windows Server 정책 이름>* 이름이 KES 정책에 추가됩니다. *<KSWS 작업명>(변환됨)* 이름으로 새 KES 작업도 생성됩니다.

2. Kaspersky Endpoint Agent의 마이그레이션 마법사를 사용하여 KEA에서 KES로 정책 및 작업 마이그레이션(웹 콘솔과 Cloud Console에서만 가능).

   이렇게 하면 *<Kaspersky Endpoint Security 정책명> 및 <Kaspersky Endpoint Agent 정책명>* 같은 이름의 새 정책이 생성됩니다. 새 작업과 KES 작업도 생성됩니다.

3 라이센싱 기능

Kaspersky Endpoint Detection and Response Optimum 또는 Kaspersky Optimum Security 공통 라이센스를 사용하여 Kaspersky Endpoint Security for Windows 및 Kaspersky Endpoint Agent를 활성화하면 애플리케이션을 버전 11.7.0으로 업그레이드한 후 EDR Optimum 기능이 자동으로 활성화됩니다. 별도의 작업이 필요하지 않습니다.

독립 실행형 Kaspersky Endpoint Detection and Response 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 11.7.0으로 업그레이드하면 EDR Optimum 기능이 자동으로 활성화됩니다.

Kaspersky Endpoint Detection and Response Optimum이나 Kaspersky Optimum Security 라이센스로 Kaspersky Endpoint Agent를 활성화한 후 다른 라이센스로 Kaspersky Endpoint Security for Windows를 활성화하면 Kaspersky Endpoint Security for Windows 키를 Kaspersky Endpoint Detection and Response Optimum 또는 Kaspersky Optimum Security 공통 키로 교체해야 합니다. 키는 *키 추가* 작업으로 교체할 수 있습니다.

Kaspersky Sandbox 기능을 활성화할 필요가 없습니다. Kaspersky Endpoint Security for Windows를 업그레이드 및 활성화하면 Kaspersky Sandbox 기능을 즉시 이용할 수 있습니다.

Kaspersky Anti Targeted Attack Platform 솔루션의 일부로 Kaspersky Endpoint Security를 활성화하려면 Kaspersky Anti Targeted Attack Platform 라이센스만 사용할 수 있습니다. 애플리케이션을 버전 12.1으로 업그레이드하면 EDR(KATA) 기능이 자동으로 활성화됩니다. 별도의 작업이 필요하지 않습니다.

4 Kaspersky Endpoint Detection and Response Optimum 및 Kaspersky Sandbox 상태 확인

업그레이드 후 Kaspersky Security Center에서 컴퓨터 상태가 *심각*으로 표시된다면:

- 컴퓨터에 Network Agent 버전 13.2 이상이 설치되었는지 확인합니다.
- *애플리케이션 구성 요소 상태 리포트*를 확인하여 내장 에이전트의 작동 상태를 확인합니다. 구성 요소의 상태가 *설치 안 됨*이라면 *애플리케이션 구성 요소 변경* 작업으로 구성 요소를 설치합니다.
- Kaspersky Endpoint Security for Windows의 새 정책에서 Kaspersky Security Network 진술문을 수락해야 합니다.

*애플리케이션 구성 요소 상태 리포트*를 사용하여 EDR Optimum 기능을 활성화합니다. 구성 요소의 상태가 *라이센스에 포함되지 않음*이라면 EDR Optimum의 라이센스 키 자동 배포 기능이 켜졌는지 확인합니다.

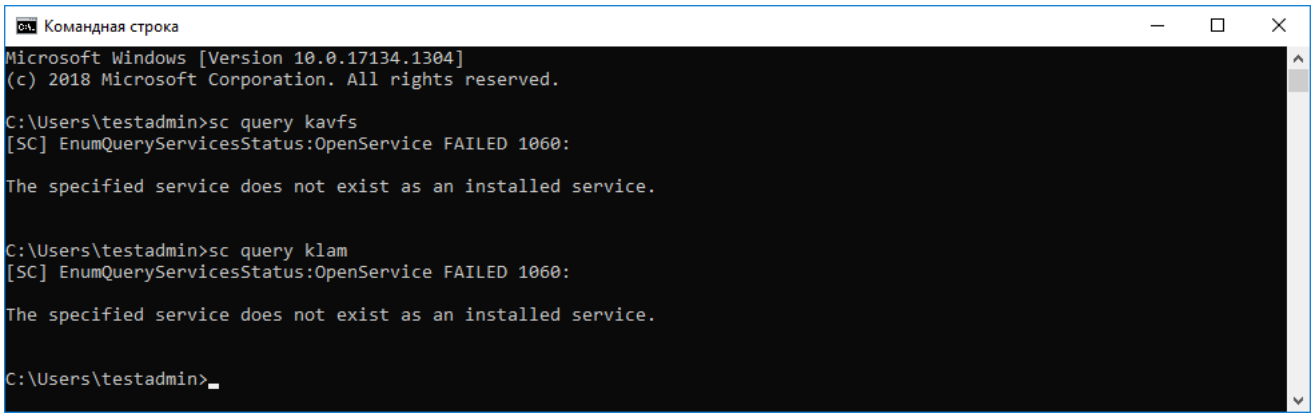
Kaspersky Security for Windows Server가 성공적으로 제거되었는지 확인

Kaspersky Security for Windows Server가 완전히 제거되었는지 확인합니다.

- `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` 폴더가 존재하지 않습니다.
- 다음 서비스가 없습니다:
  - Kaspersky Security Service(KAVFS)
  - Kaspersky Security Management 서비스(KAVFSGT)
  - Kaspersky Security Exploit Prevention 서비스(KAVFSSLP)
  - Kaspersky Security Script Checker 서비스(KAVFSSCS)

  `sc query` 명령을 이용하면 실행 중인 서비스를 작업 관리자에서 확인할 수 있습니다(아래 그림 참조).
- 다음 드라이버가 없습니다:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

`C:\Windows\System32\drivers` 폴더를 확인하거나 `sc query` 명령을 실행하면 설치된 드라이버를 확인할 수 있습니다. 서비스 또는 드라이버가 누락된 경우 다음 응답을 받게 됩니다.



Kaspersky Security for Windows Server 서비스와 드라이버가 성공적으로 제거되었는지 확인

애플리케이션 또는 드라이버 파일이 서버에 남아 있는 경우 해당 파일을 수동으로 삭제하십시오. Kaspersky Security for Windows Server 서비스가 서버에서 아직 실행 중인 경우 서비스를 수동으로 중지(`sc stop`)하고 삭제(`sc delete`)하십시오. klam.sys 드라이버를 중지하려면 `fltmc unload klam` 명령을 사용하십시오.

KSWS 키로 KES 활성화

애플리케이션을 설치한 후 Kaspersky Security for Windows Server(KSWS) 라이센스 키를 사용하여 Kaspersky Endpoint Security for Windows(KES)를 활성화할 수 있습니다. 마이그레이션 후의 활성화 프로세스는 KSWS 활성화 방법에 따라 다릅니다(아래 표 참조).

Kaspersky Endpoint Security는 *Kaspersky Security for Storage 라이센스*를 지원하지 않습니다. 이 라이센스로 작업하려면 Kaspersky Security for Windows Server를 사용해야 합니다.

KES를 KSWS 키로 활성화하려면 활성화 코드만을 사용해야 합니다. 키 파일을 사용해 애플리케이션을 활성화하려면 기술 지원에 문의하여 Kaspersky Endpoint Security 키 파일을 요청해야 합니다.

Kaspersky Security for Windows Server 키로 Kaspersky Endpoint Security for Windows 활성화

Kaspersky Security for Windows Server 활성화 방법	Kaspersky Endpoint Security for Windows로 키 마이그레이션.
컴퓨터에 KSWS 라이센스 키 자동 배포.	KSWS 라이센스 키 속성에서 자동 키 배포가 활성화되면 KSWS 키로 KES가 자동 활성화됩니다.
KSWS 키는 작업에 따라 추가됩니다.	작업을 사용하여 KSWS를 활성화하면 KSWS에서 마이그레이션하는 동안 KSWS 라이센스 키가 삭제됩니다. 애플리케이션을 다시 활성화해야 합니다. 예를 들어 Kaspersky Endpoint Security for Windows 설치 패키지에 라이센스 키를 추가할 수 있습니다.
KSWS 키는 애플리케이션 인터페이스에 로컬로 추가됩니다.	KSWS가 애플리케이션 활성화 마법사를 사용하여 로컬로 활성화하면 KSWS에서 마이그레이션하는 동안 KSWS 라이센스 키가 삭제됩니다. 애플리케이션을 다시 활성화해야 합니다. 예를 들어 Kaspersky Endpoint Security for Windows 설치 패키지에 라이센스 키를 추가할 수 있습니다.
KSWS 키가 설치 패키지에 추가됩니다.	설치 패키지의 키를 사용하여 KSWS를 활성화다면 KSWS에서 마이그레이션하는 동안 KSWS 라이센스 키가 삭제됩니다. 애플리케이션을 다시 활성화해야 합니다. 예를 들어 Kaspersky Endpoint Security for Windows 설치 패키지에 라이센스 키를 추가할 수 있습니다.
Amazon Web Services(AWS)의 유료 가상 컴퓨터 이미지(Amazon Machine Image – AMI).	Kaspersky Security Center를 Amazon Web Services(AWS)에서 유료 가상 머신 이미지(Amazon Machine Image – AMI)로 구입한 경우에는 KES를 활성화하지 않아도 됩니다. 이 경우 Kaspersky Security Center는 애플리케이션에 이미 추가된 AWS 서브스크립션을 사용합니다.
자체 라이센스가 있는 기존 무료 Kaspersky Security Center 이미지(Bring Your Own License – BYOL 모델).	클라우드 환경에서 자체 라이센스로 기존 무료 Kaspersky Security Center 이미지(Bring Your Own License - BYOL 모델)를 사용하는 경우에는 사용 가능한 방법을 사용하여 애플리케이션을 활성화해야 합니다. Kaspersky Hybrid Cloud Security 라이센스가 있어야 합니다.

부하가 높은 서버 마이그레이션을 위한 특별 고려 사항

부하가 높은 서버에서는 성능을 모니터링하고 오류를 방지하는 일이 대단히 중요합니다. Kaspersky Endpoint Security for Windows로 마이그레이션한 후에는 다른 구성 요소에 비해 상당히 많은 서버 리소스를 사용하는 애플리케이션 구성 요소를 일시적으로 비활성화하는 것이 좋습니다. 서버가 정상적으로 작동하는지 확인한 후 애플리케이션 구성 요소를 다시 활성화하면 됩니다.

부하가 높은 서버는 다음과 같이 마이그레이션하는 것이 좋습니다.

1. 기본 설정으로 Kaspersky Endpoint Security 정책을 생성합니다.

   기본 설정은 최적의 설정을 사용합니다. Kaspersky 전문가가 권장하는 설정입니다. 기본 설정은 권장 보호 수준과 최적의 리소스 사용을 제공합니다.

2. 정책 설정에서 네트워크 위협 보호, 행동 탐지, 익스플로잇 방지, 복원 엔진, 애플리케이션 제어 구성 요소를 끕니다.

   조직에 Kaspersky Managed Detection and Response(MDR) 솔루션이 배포되어 있는 경우, BLOB 구성 파일을 Kaspersky Endpoint Security 정책에 업로드합니다.

3. 서버에서 Kaspersky Security for Windows Server를 제거합니다.

4. Kaspersky Endpoint Security for Windows를 기본 구성 요소 집합과 함께 설치합니다.

   조직에 Detection and Response 솔루션이 배포되어 있는 경우, 설치 패키지 속성에서 관련 구성 요소를 선택합니다.

5. 애플리케이션의 설정을 확인합니다:

   - 애플리케이션은 KSWS 라이센스 키로 활성화됩니다.
   - 새 정책이 적용됩니다. 이전에 선택한 구성 요소는 비활성화됩니다.

6. 서버가 작동하는지 확인합니다. Kaspersky Endpoint Security for Windows가 서버 리소스 1% 이상을 사용하지 않는지 확인합니다.

7. 필요한 경우 검사 예외를 만들고, 신뢰하는 애플리케이션을 추가하고, 신뢰하는 웹 주소 목록을 생성합니다.

8. 행동 탐지, 익스플로잇 방지, 복원 엔진 구성 요소를 켭니다. Kaspersky Endpoint Security for Windows가 서버 리소스 1% 이상을 사용하지 않는지 확인합니다.

9. 네트워크 위협 보호 구성 요소를 켭니다. Kaspersky Endpoint Security for Windows가 서버 리소스 2% 이상을 사용하지 않는지 확인합니다.

10. 규칙 테스트 모드에서 애플리케이션 제어 구성 요소를 켭니다.

11. 애플리케이션 제어가 작동하는지 확인합니다. 필요한 경우 애플리케이션 제어가 작동하는지 확인한 후 새 애플리케이션 제어 규칙을 추가하고 규칙 테스트 모드를 끕니다.

KSWS에서 KES로의 마이그레이션이 끝나면 애플리케이션이 올바르게 작동하는지 확인하십시오. 콘솔에서 서버 상태를 확인합니다(*정상*해야 합니다). 애플리케이션에 대해 보고된 오류가 없는지 확인하고, 중앙 관리 서버에 대한 마지막 연결 시간과 마지막 데이터베이스 업데이트 시간 및 서버 보호 상태를 확인합니다.

Server Core 모드에서 서버의 애플리케이션 관리

Server Core 모드의 서버에는 GUI가 없습니다. 따라서 Kaspersky Security Center 콘솔을 사용하여 원격에서 애플리케이션을 관리하거나 명령줄에서 로컬로만 관리할 수 있습니다.

Kaspersky Security Center 콘솔을 통한 애플리케이션 관리

Kaspersky Security Center 콘솔로 애플리케이션을 설치하는 것도 일반적인 설치와 다르지 않습니다. 설치 패키지 생성 시, 라이센스 키를 추가하여 애플리케이션을 활성화할 수 있습니다. Kaspersky Endpoint Security for Windows 키 또는 Kaspersky Security for Windows Server 키를 사용할 수 있습니다.

Server Core 모드의 서버에서는 웹 위협 보호, 메일 위협 보호, 웹 제어, BadUSB 공격 방지, 파일 레벨 암호화(FLE), Kaspersky 디스크 암호화(FDE)와 같은 애플리케이션 구성 요소를 사용할 수 없습니다.

Kaspersky Endpoint Security를 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. 애플리케이션은 사용자에게 서버를 다시 시작하라는 창을 표시할 수 없습니다. Kaspersky Security Center 콘솔의 리포트에서 서버를 다시 시작해야 하는 필요성에 대해 알아볼 수 있습니다.

Server Core 모드의 서버에서 애플리케이션을 관리하는 것은 컴퓨터를 관리하는 것과 다르지 않습니다. 정책 및 작업을 사용하여 애플리케이션을 구성할 수 있습니다.

Server Core 모드의 서버에서 애플리케이션을 관리하려면 다음과 같은 특별한 고려 사항이 필요합니다.

- Server Core 모드의 서버에는 GUI가 없으므로 Kaspersky Endpoint Security는 고급 치료가 필요하다는 경고를 사용자에게 표시하지 않습니다. 보안위협을 치료하려면 애플리케이션 설정에서 고급 치료 기술을 활성화하고 *악성 코드 검사* 작업 설정에서 즉각적인 고급 치료를 활성화해야 합니다. 그다음 *악성 코드 검사* 작업을 시작해야 합니다.
- BitLocker 드라이브 암호화는 TPM(신뢰하는 플랫폼 모듈)에서만 사용할 수 있습니다. 애플리케이션이 사전 부팅 인증을 위한 암호 프롬프트 창을 표시할 수 없으므로 암호화 시 PIN/암호는 사용할 수 없습니다. 운영 체제에 FIPS(연방 정보 처리 표준) 호환 모드가 활성화되어 있다면 드라이브 암호화 시작 전에 암호화 키를 저장할 이동식 드라이브를 연결하십시오.

명령줄로 애플리케이션 관리

GUI를 사용할 수 없다면 명령줄에서 Kaspersky Endpoint Security를 관리할 수 있습니다.

Server Core 모드의 서버에 애플리케이션을 설치하려면 다음 명령을 실행합니다.

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

애플리케이션을 활성화하려면 다음 명령을 실행합니다.

```
avp.com license /add <activation code or key file>
```

애플리케이션 프로필 상태를 확인하려면 다음 명령을 실행합니다.

```
avp.com status
```

애플리케이션 관리 명령 목록을 보려면 다음 명령을 실행합니다.

```
avp.com help
```

[KSWS+KEA]을 [KES+내장 에이전트]로 마이그레이션

Kaspersky Security for Windows Server(KSWS)에서 Kaspersky Endpoint Security(KES)로 마이그레이션할 때 다음 권장 사항을 사용하면 서버 보호를 구성하고 성능을 최적화할 수 있습니다. 여기서는 단일 조직에 대한 마이그레이션 예제를 살펴보겠습니다.

조직의 인프라

회사에는 다음과 같은 장비가 설치되어 있습니다.

- Kaspersky Security Center 14.2

  관리자는 관리 콘솔(MMC)을 사용하여 Kaspersky 솔루션을 관리합니다. Kaspersky Endpoint Detection and Response Optimum(EDR Optimum)도 배포되어 있습니다.

  Kaspersky Security Center에는 조직의 서버를 포함하는 세 가지 관리 그룹이 생성됩니다. 두 개는 SQL 서버용 관리 그룹이며 하나는 Microsoft Exchange 서버용 관리입니다. 각 관리 그룹은 자체 정책으로 관리됩니다. *Database Update* 및 *On-demand scan* 작업은 조직의 모든 서버를 대상으로 생성됩니다.

  KSWS 활성화 키가 Kaspersky Security Center에 추가됩니다. 자동 키 배포가 활성화됩니다.

- Kaspersky Security for Windows Server 11.0.1 및 Kaspersky Endpoint Agent 3.11이 설치된 SQL 서버. SQL 서버는 클러스터 두 개로 결합됩니다.

  KSWS는 *SQL_정책(1)* 및 *SQL_정책(2)* 정책으로 관리합니다. *Database Update*, *On-demand scan* 작업도 생성됩니다.

- Kaspersky Security for Windows Server 11.0.1 및 Kaspersky Endpoint Agent 3.11이 설치된 Microsoft Exchange 서버.

  KSWS는 *Exchange_정책* 정책으로 관리합니다. *Database Update*, *On-demand scan* 작업도 생성됩니다.

마이그레이션 계획

마이그레이션에는 다음 단계가 포함합니다.

1. 정책 및 작업 변환 마법사를 사용하여 KSWS 작업과 정책을 마이그레이션합니다.
2. 정책 및 작업 변환 마법사를 사용하여 Kaspersky Endpoint Agent 정책을 마이그레이션합니다.
3. 태그를 사용하여 새 정책의 속성에서 정책 프로필을 활성화합니다.
4. KSWS 대신 KES 설치합니다.
5. EDR Optimum을 활성화합니다.
6. KES가 작동하는지 확인합니다.

마이그레이션 시나리오는 SQL 서버 클러스터 중 하나에서 처음으로 수행됩니다. 그런 다음 SQL 서버의 다른 클러스터에서 마이그레이션 시나리오가 수행됩니다. 그런 다음 Microsoft Exchange에서 마이그레이션 시나리오가 수행됩니다.

정책 및 작업 변환 마법사를 사용하여 KSWS 작업과 정책을 마이그레이션

KSWS 작업을 마이그레이션할 때는 정책 및 작업 변환 마법사(마이그레이션 마법사)를 사용할 수 있습니다. 마법사를 사용하면 *SQL_정책(1)*, *SQL_정책(2)* 및 *Exchange_정책* 정책 대신 저마다 SQL 및 Microsoft Exchange 서버에 대한 프로필 세 개가 포함되어 있는 단일 정책을 얻게 됩니다. KSWS 설정이 있는 새 정책 프로필의 이름은 *UpgradedFromKSWS <Kaspersky Security for Windows Server 정책 이름>*이 됩니다. 프로필 속성에서 마이그레이션 마법사는 `UpgradedFromKSWS` 기기 태그를 트리거링 기준으로 자동으로 선택합니다. 따라서 정책 프로필의 설정이 서버에 자동으로 적용됩니다.

정책 및 작업 변환 마법사를 사용하여 Kaspersky Endpoint Agent 정책 마이그레이션

Kaspersky Endpoint Agent 정책을 마이그레이션할 때는 정책 및 작업 변환 마법사를 사용할 수 있습니다. Kaspersky Endpoint Agent용 정책 및 작업 마이그레이션 마법사는 웹 콘솔에서만 사용할 수 있습니다.

태그를 사용하여 새 정책의 속성에서 정책 프로필 활성화

프로필 활성화 조건으로 이전에 할당한 디바이스 태그를 선택합니다. 정책 속성을 열고 선택 *정책 프로필 활성화에 대한 일반 규칙*을 프로필 활성화 조건으로 선택합니다.

KSWS 대신 KES 설치

KES를 설치하기 전에 KSWS 정책 속성에서 암호 보호를 비활성화해야 합니다.

KES 설치에는 다음 단계가 포함됩니다.

1. 설치 패키지를 준비합니다. 설치 패키지 속성에서 Kaspersky Endpoint Security for Windows 12.0 배포 패키지를 선택하고 기본 구성 요소 집합을 선택합니다.

2. SQL 서버 관리 그룹 중 하나에 대한 *원격으로 애플리케이션 설치* 작업을 만듭니다.

3. 작업 속성에서 설치 패키지와 라이센스 키 파일을 선택합니다.

4. 작업이 성공적으로 완료될 때까지 기다립니다.

5. 나머지 관리 그룹을 대상으로 KES 설치를 반복 수행합니다.

Kaspersky Security Center는 KES 설치가 완료되면 `UpgradedFromKSWS` 태그를 콘솔의 컴퓨터 이름에 자동으로 추가합니다.

KES 설치를 확인하려면 *보호 배포 리포트*를 사용하면 됩니다. 장치 상태도 확인할 수 있습니다. 애플리케이션 활성화를 확인하려면 *라이센스 키 사용 리포트*를 사용하면 됩니다.

EDR Optimum 활성화

독립 실행형 Kaspersky Endpoint Detection and Response Optimum 추가 기능 라이센스를 사용하여 EDR Optimum 기능을 활성화할 수 있습니다. EDR Optimum 키가 Kaspersky Security Center 리포지토리에 추가되었고 자동 라이센스 키 배포 기능이 활성화되었는지 확인해야 합니다.

EDR Optimum 활성화를 확인하려면 *애플리케이션 구성 요소 상태 리포트*를 사용하면 됩니다.

KES 작동 확인

KES가 작동하는지 확인하는 대표적인 방법은 보고된 오류가 없는지 확인하는 것입니다. 장치 상태 *정상*해야 합니다. 업데이트 및 악성 코드 검사 작업을 성공적으로 완료했습니다.

가상 컴퓨터를 보호하는 Light Agent 모드

12.8 버전부터 Kaspersky Security for Virtualization Light Agent의 일부로 Kaspersky Endpoint Security for Windows를 사용할 수 있습니다. *Kaspersky Security for Virtualization Light Agent*는 다양한 유형의 정보 보안 위협, 네트워크 공격, 피싱 공격으로부터 가상 컴퓨터를 포괄적으로 보호하는 통합 솔루션입니다. 이 솔루션을 사용하려면 애플리케이션을 Light Agent 모드로 설치해야 합니다.

Arm 기반 가상 컴퓨터에서는 Light Agent 모드의 Kaspersky Endpoint Security 설치를 지원하지 않습니다.

6.2 버전부터 Kaspersky Security for Virtualization Light Agent의 일부로 Kaspersky Endpoint Security를 Light Agent 모드로 사용할 수 있습니다.

Light Agent를 시작하면 가상 컴퓨터 SVM(Secure Virtual Machine)에 연결을 설정하고 유지합니다. 보호 서버가 SVM에 배포됩니다. *보호 서버*는 Kaspersky Security for Virtualization Light Agent 솔루션의 구성 요소로서, 바이러스 및 기타 악성 코드가 있는지 파일을 검사하고, 안티 바이러스 데이터베이스를 업데이트하며, 라이센스 키를 관리합니다. Light Agent는 검사가 필요한 파일 조각을 SVM으로 전송합니다. Light Agent가 설치된 모든 가상 컴퓨터에 대한 검사 결과를 이용할 수 있습니다(SharedCache 기술). 따라서 SharedCache 기술은 솔루션 효율성을 높이고 위협에 더 신속하게 대응합니다.

조직의 인프라에는 Light Agent가 설치된 많은 가상 컴퓨터와 SVM이 포함될 수 있습니다. 통합 서버 구성 요소는 솔루션 구성 요소와 가상 인프라 간의 상호 작용을 위한 것입니다. *통합 서버* - 사용 가능한 SVM 목록을 생성하고 해당 데이터를 Light Agent로 전송하고, Light Agent의 SVM 탐지에 참여하고, Light Agent와 SVM 간의 연결을 보호하고, 기타 기능을 수행하는 Kaspersky Security for Virtualization Light Agent 솔루션의 구성 요소.

Light Agent 모드에 대한 특별 고려 사항

Kaspersky Endpoint Security 정책 및 작업을 사용하여 표준 모드와 Light Agent 모드에서 Kaspersky Endpoint Security를 관리할 수 있습니다. Light Agent 모드에서는 애플리케이션의 일부 구성 요소와 기능을 사용할 수 없습니다.

데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트

Light Agent 모드의 Kaspersky Endpoint Security는 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 작동할 때 애플리케이션에 필요한 특수 악성 코드 데이터베이스를 사용합니다. Kaspersky Endpoint Security는 보호 서버로부터 데이터베이스 및 애플리케이션 모듈 업데이트를 가져옵니다.

보호된 가상 컴퓨터의 데이터베이스 및 모듈은 특수한 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 통해 업데이트됩니다. 이 작업에서는 SVM의 폴더가 업데이트 경로로 지정됩니다. Light Agent는 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 자동으로 실행합니다. 다른 업데이트 경로를 선택하거나, 작업 스케줄을 구성하거나, 작업을 제거할 수 없습니다.

최신 악성 코드 데이터베이스 업데이트의 롤백 또한 보호 서버에서 처리됩니다. SVM에서 데이터베이스 및 애플리케이션 모듈 업데이트의 롤백 후 특수한 로컬 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업이 보호된 가상 컴퓨터에서 시작됩니다. 이 작업을 통해 Light Agent가 이전의 악성 코드 데이터베이스 세트를 다시 사용하게 됩니다.

Light Agent 모드의 Kaspersky Endpoint Security는 *업데이트 롤백* 작업을 지원하지 않습니다.

Light Agent 활성화

애플리케이션을 활성화하려면 Light Agent가 연결된 SVM에 라이센스 키를 추가해야 합니다. 별도로 애플리케이션을 활성화할 필요가 없습니다.

Light Agent 모드에 대한 기타 특별 고려 사항

- 애플리케이션에 대한 정책을 생성할 때, Light Agent 모드 선택을 권장합니다. 이 모드에서는 새 정책 마법사가 SVM 연결을 구성하라는 메시지를 표시합니다. 애플리케이션이 Light Agent 모드에서 작동하려면 이러한 설정이 필요합니다.
- Light Agent 모드에서는 데이터 암호화 구성 요소와 적응형 이상 행위 제어를 설치할 수 없습니다. 또한 구성 요소의 집합은 게스트 운영 체제의 유형에 따라 달라집니다: 워크스테이션 또는 서버.
- Light Agent는 Kaspersky Endpoint Detection and Response Expert(클라우드)와의 통합을 지원하지 않습니다.
- 관리 콘솔(MMC) 및 Kaspersky Security Center 웹 콘솔에서 Light Agent를 관리할 수 있습니다. Kaspersky Security Center Cloud 콘솔에서는 Light Agent를 관리할 수 없습니다.
- VDI 가상 컴퓨터에서 애플리케이션 구성 요소 집합을 변경하는 것은 지원되지 않습니다.
- Kaspersky Endpoint Security는 KSN 프록시 서버를 통해 KSN 서버와 통신합니다. KSN과의 직접 통신은 지원되지 않습니다.
- Kaspersky Security Network의 클라우드 모드는 지원되지 않습니다.
- 통합 서버(VIIS), 보호 서버(SVM) 및 KSN 서버에 연결할 때 애플리케이션 프록시 서버를 사용하는 것은 지원되지 않습니다.

가상 컴퓨터 사전 구성

가상 플랫폼 기술을 사용하는 가상 컴퓨터에 Kaspersky Endpoint Security를 설치할 수 있습니다. Kaspersky Endpoint Security는 VMware, Microsoft Hyper-V, Citrix 가상 플랫폼을 지원합니다. 설치하기 전에 가상 컴퓨터 사전 구성을 수행해야 합니다.

Citrix App Layering 기술과의 호환성

임시 가상 컴퓨터의 상태를 저장하기 위해 Full User Layer를 사용하려면 가상 컴퓨터 템플릿에 설치하기 전에 다음을 수행해야 합니다.

1. C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt 파일을 만들고 다음 예외 규칙을 추가합니다.
   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`
2. 운영 체제 레지스트리에서 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr 키에서 MiniFilterBypass라는 새 DWORD 값을 만들고 1로 설정합니다.
3. 운영 체제 레지스트리에서 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd 키에서 ExcludeKey라는 새 MULTI_SZ 값을 만들고 \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab으로 설정합니다.
4. 가상 컴퓨터를 다시 시작합니다.

Citrix App Layering을 사용하는 인프라의 가상 컴퓨터에 설치하는 경우에는 다음을 수행해야 합니다.

1. 애플리케이션 계층(Application Layer)의 가상 컴퓨터 템플릿에 Kaspersky Security Center 관리 에이전트 및 Kaspersky Endpoint Security for Windows를 설치합니다.
2. 여러 계층으로 구성된 가상 컴퓨터 이미지를 생성합니다.
3. 생성된 이미지를 Citrix App Layering 솔루션을 지원하는 하이퍼바이저에 배포합니다.
4. 생성된 이미지에서 임시 가상 컴퓨터 생성을 구성합니다.

Citrix App Layering과 함께 안티 바이러스 소프트웨어를 설치하는 방법에 대한 자세한 내용은 Citrix App Layering 설명서를 참조하십시오.

Citrix Provisioning(Citrix Provisioning Services) 기술과의 호환성

애플리케이션이 Citrix Provisioning 기술(Citrix Provisioning Services)과 호환되는지 확인하려면:

- 가상 컴퓨터에 Citrix Provisioning Target Device 소프트웨어가 설치되어 있는 경우 Kaspersky Endpoint Security 애플리케이션을 설치하기 전에 이를 제거해야 합니다. 애플리케이션을 설치한 후 Citrix Provisioning Target Device를 설치해야 합니다.
- 설치 마법사를 사용하거나 원격으로 Kaspersky Security Center를 사용하여 애플리케이션을 설치하는 경우 **Citrix PVS와의 호환성 보장** 확인란을 선택해야 합니다.

Omnissa App Volumes 기술과의 호환성

가상 컴퓨터 템플릿에 설치하기 전에 %SVAgent%\Config\Custom\snapvol.cfg 파일을 만들고 다음 예외 규칙을 파일에 추가합니다.

- exclude_path=\ProgramData\Kaspersky Lab
- exclude_path=\ProgramData\KasperskyLab
- exclude_path=\Program Files\Kaspersky Lab
- exclude_path=\Program Files\Common Files\Kaspersky Lab
- exclude_path=\Program Files\Kaspersky Lab
- exclude_path=\Program Files (x86)\Kaspersky Lab
- exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab
- exclude_process_path=\Program Files (x86)\Kaspersky Lab
- exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab
- exclude_process_path=\Program Files\Common Files\Kaspersky Lab
- exclude_process_path=\Program Files\Kaspersky Lab
- exclude_process_name=avp.exe
- exclude_process_name=klnagent.exe
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon

자세한 정보는 Omnissa 설명서를 참조하십시오.

Light Agent 설치

Arm 기반 가상 컴퓨터에서는 Light Agent 모드의 Kaspersky Endpoint Security 설치를 지원하지 않습니다.

Light Agent 모드에서 애플리케이션을 설치하는 것은 표준 모드와 동일합니다. 가상 컴퓨터에 Light Agent를 설치하기 전에 Kaspersky Security Center 네트워크 에이전트가 설치되었는지 확인해야 합니다. *네트워크 에이전트*를 설치하면 중앙 관리 서버와 가상 컴퓨터가 원활하게 상호 작용할 수 있습니다.

Light Agent는 다음 중 하나의 방법으로 가상 컴퓨터에 설치할 수 있습니다:

- Kaspersky Security Center 원격 사용.
- 로컬에서 설치 마법사 사용.
- 로컬에서 명령줄 사용.

Light Agent를 설치하려면 설치 패키지 설정 또는 설치 마법사 중에서 알맞은 구성을 선택해야 합니다.

서버에 Light Agent를 설치하면 고급 보호 구성 요소(행동 탐지, 익스플로잇 방지, 복원 엔진)가 애플리케이션의 기본 구성에서 제외됩니다. 기본 애플리케이션 설정은 권장 보호 수준을 제공하며, 서버 리소스를 최적으로 사용하도록 지원합니다. 워크스테이션에 Light Agent를 설치하면 고급 보호 구성 요소가 애플리케이션의 기본 구성에 포함됩니다.

Light Agent 설치 시 관련 가상 환경에 대해 사전 정의된 예외 규칙 및 신뢰하는 애플리케이션을 선택하는 것이 좋습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션은 애플리케이션을 빠르게 설정하고 가상 환경 호환성 문제를 방지하는 데 도움이 됩니다. 또한 정책에서, 설치 후에 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 구성할 수 있습니다.

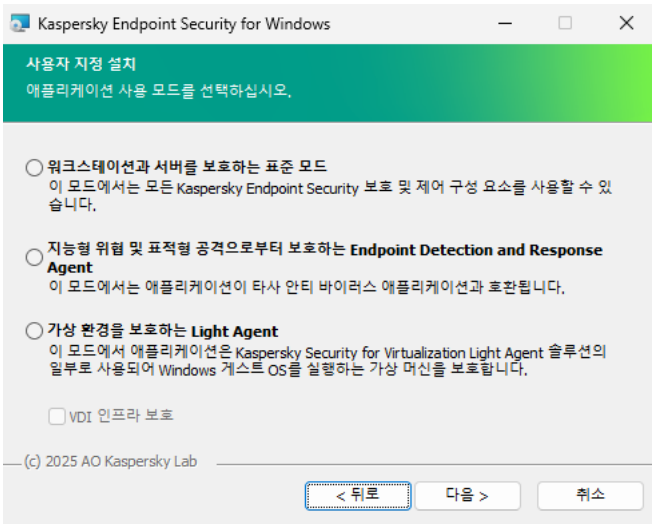
영구 가상 컴퓨터에 Light Agent를 설치할 때 Sensor ID 생성 알고리즘을 변경해야 할 수 있습니다. Sensor ID는 Kaspersky Anti Targeted Attack Platform 솔루션에서 서버로 원격 측정 데이터를 전송하는 컴퓨터를 식별하는 데 사용됩니다. 고유한 Sensor ID를 생성하려면 명령줄에 애플리케이션을 설치할 때 `EnableUniqueSensorID=1`을 설정합니다.

설치 마법사를 사용하여 Light Agent를 설치하는 방법

1. 배포 키트 폴더를 가상 컴퓨터에 복사합니다.
2. setup_kes.exe를 실행합니다.

   설치 마법사가 시작됩니다.

Kaspersky Endpoint Security 구성



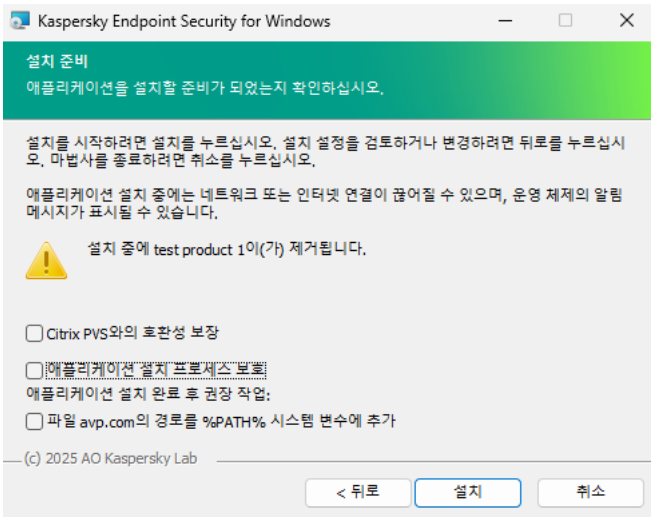
애플리케이션 구성 선택

가상 환경을 보호하는 Light Agent 구성을 선택합니다. 이 구성은 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 사용되는 애플리케이션을 대상으로 합니다. 솔루션을 사용하여 보호해야 하는 각 가상 컴퓨터에 Light Agent를 설치해야 합니다. 이 구성에서는 데이터 암호화 구성 요소 또는 적응형 이상 행위 제어를 사용할 수 없습니다. *비영구 가상 컴퓨터*를 만드는데 사용될 가상 컴퓨터 템플릿에 Light Agent를 설치하는 경우, **VDI 인프라 보호** 확인란을 선택합니다(VDI는 Virtual Desktop Infrastructure). VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. 이 모드에서 Light Agent는 가상 컴퓨터를 다시 시작해야 하는 애플리케이션 업데이트를 거부합니다. 재시작이 필요한 애플리케이션 업데이트를 수신하면 Light Agent는 보호된 가상 컴퓨터의 템플릿을 업데이트해야 한다는 이벤트를 생성합니다.

Kaspersky Endpoint Security 구성 요소

설치하려는 구성 요소를 선택합니다(아래 그림 참조). 애플리케이션을 설치한 후 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다. 이렇게 하려면 설정 마법사를 다시 실행하고 사용 가능한 구성 요소를 변경하도록 선택해야 합니다.

고급 설정



고급 애플리케이션 설치 설정

애플리케이션 설치 프로세스 보호. 설치 보호는 악성 애플리케이션에 의한 배포 패키지 변조 차단, Kaspersky Endpoint Security 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.

Citrix PVS와의 호환성 보장. 가상 컴퓨터에 Kaspersky Endpoint Security를 설치하기 위해 Citrix Provisioning Services 지원을 작동할 수 있습니다.

시스템 변수 %PATH%에 avp.com 파일 경로 추가. 명령줄 인터페이스를 편리하게 사용할 수 있도록 %PATH% 변수에 설치 경로를 추가할 수 있습니다.

명령줄을 사용하여 Light Agent를 설치하는 방법

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 배포 패키지가 있는 폴더로 이동합니다.
3. 다음 명령을 실행합니다:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
```

또는

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
```

`VDI` 옵션은 VDI(Virtual Desktop Infrastructure) 보호 모드를 활성화합니다. VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. 이 모드에서 Light Agent는 가상 컴퓨터를 다시 시작해야 하는 애플리케이션 업데이트를 거부합니다. 재시작이 필요한 애플리케이션 업데이트를 수신하면 Light Agent는 보호된 가상 컴퓨터의 템플릿을 업데이트해야 한다는 이벤트를 생성합니다. 기본적으로 VDI 보호 모드는 비활성화되어 있습니다.

따라서 가상 컴퓨터에 Light Agent가 기본 구성 요소 집합과 함께 설치됩니다. setup.ini 파일을 사용하여 구성 요소 집합을 편집하고 고급 설정을 지정할 수 있습니다. 명령줄에서 설치 설정을 지정할 수도 있습니다.

관리 콘솔(MMC)을 사용하여 Light Agent를 설치하는 방법

1. Kaspersky Security Center 관리 콘솔 창을 엽니다.
2. 콘솔에서 **고급** → **원격 설치** → **설치 패키지** 폴더를 선택합니다.

   Kaspersky Security Center로 다운로드한 설치 패키지 목록이 열립니다.
3. Kaspersky Endpoint Security for Windows 설치 패키지의 속성을 엽니다.

   필요한 경우, 새 설치 패키지 만들기를 실행하십시오.
4. **설정** 섹션으로 이동합니다.
5. **가상 환경을 보호하는 Light Agent** 구성을 선택합니다. 이 구성은 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 사용되는 애플리케이션을 대상으로 합니다. 솔루션을 사용하여 보호해야 하는 각 가상 컴퓨터에 Light Agent를 설치해야 합니다. 이 구성에서는 데이터 암호화 구성 요소 또는 적응형 이상 행위 제어를 사용할 수 없습니다. *비영구 가상 컴퓨터*를 만드는데 사용될 가상 컴퓨터 템플릿에 Light Agent를 설치하는 경우, **VDI 인프라 보호** 확인란을 선택합니다(VDI는 Virtual Desktop Infrastructure). VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. 이 모드에서 Light Agent는 가상 컴퓨터를 다시 시작해야 하는 애플리케이션 업데이트를 거부합니다. 재시작이 필요한 애플리케이션 업데이트를 수신하면 Light Agent는 보호된 가상 컴퓨터의 템플릿을 업데이트해야 한다는 이벤트를 생성합니다.
6. 설치할 구성 요소를 선택합니다.

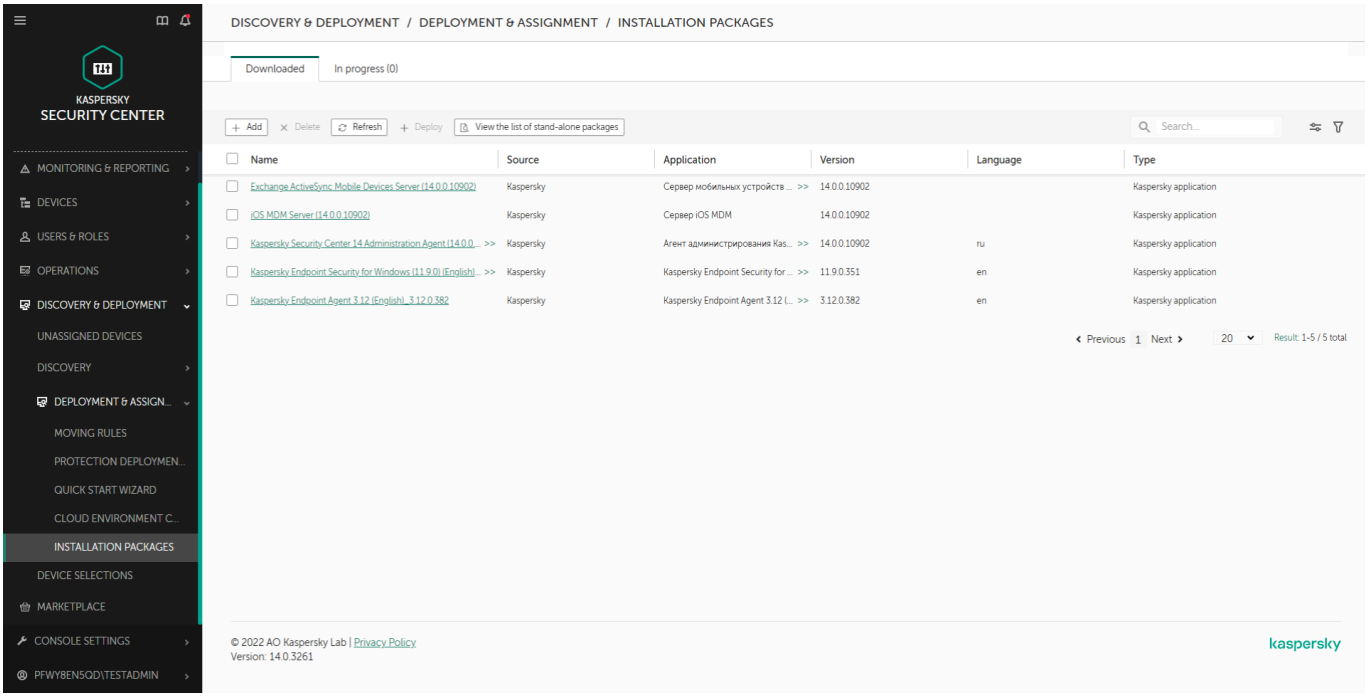
   애플리케이션을 설치한 후 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다.
7. 신뢰 영역을 구성합니다. 애플리케이션을 설치할 가상 환경에 대해 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 선택합니다.

   사전 정의된 검사 예외 및 신뢰하는 애플리케이션은 애플리케이션을 빠르게 설정하고 가상 환경 호환성 문제를 방지하는 데 도움이 됩니다.
8. 변경 사항을 저장합니다.
9. 원격 설치 작업 생성. 작업 속성에서 생성한 설치 패키지를 선택합니다.

웹 콘솔을 사용하여 Light Agent를 설치하는 방법

1. 웹 콘솔의 메인 창에서 **발견 및 배포** → **배포 및 할당** → **설치 패키지**를 클릭합니다.

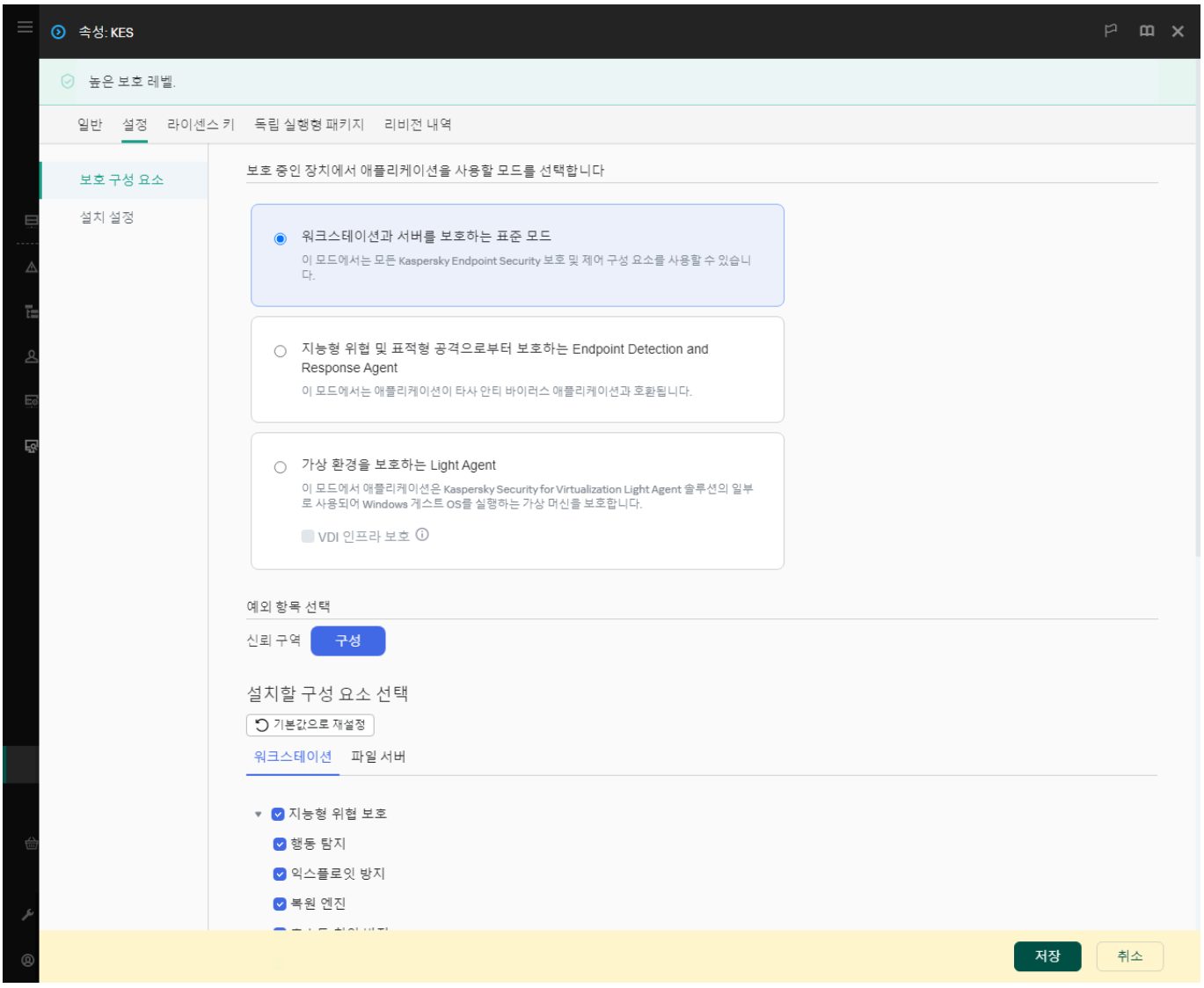
Kaspersky Security Center로 다운로드한 설치 패키지 목록이 열립니다.



설치 패키지 목록

2. Kaspersky Endpoint Security for Windows 설치 패키지의 속성을 엽니다.
   필요한 경우, 새 설치 패키지 만들기를 실행하십시오.
3. **설정** 탭을 선택합니다.

4. **보호 구성 요소** 섹션으로 이동합니다.



설치 패키지에 포함된 구성 요소

5. **가상 환경을 보호하는 Light Agent** 구성을 선택합니다. 이 구성은 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 사용되는 애플리케이션을 대상으로 합니다. 솔루션을 사용하여 보호해야 하는 각 가상 컴퓨터에 Light Agent를 설치해야 합니다. 이 구성에서는 데이터 암호화 구성 요소 또는 적응형 이상 행위 제어를 사용할 수 없습니다. *비영구 가상 컴퓨터*를 만드는데 사용될 가상 컴퓨터 템플릿에 Light Agent를 설치하는 경우, **VDI 인프라 보호** 확인란을 선택합니다(VDI는 Virtual Desktop Infrastructure). VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. 이 모드에서 Light Agent는 가상 컴퓨터를 다시 시작해야 하는 애플리케이션 업데이트를 거부합니다. 재시작이 필요한 애플리케이션 업데이트를 수신하면 Light Agent는 보호된 가상 컴퓨터의 템플릿을 업데이트해야 한다는 이벤트를 생성합니다.

6. 설치할 구성 요소를 선택합니다.

   애플리케이션을 설치한 후 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다.

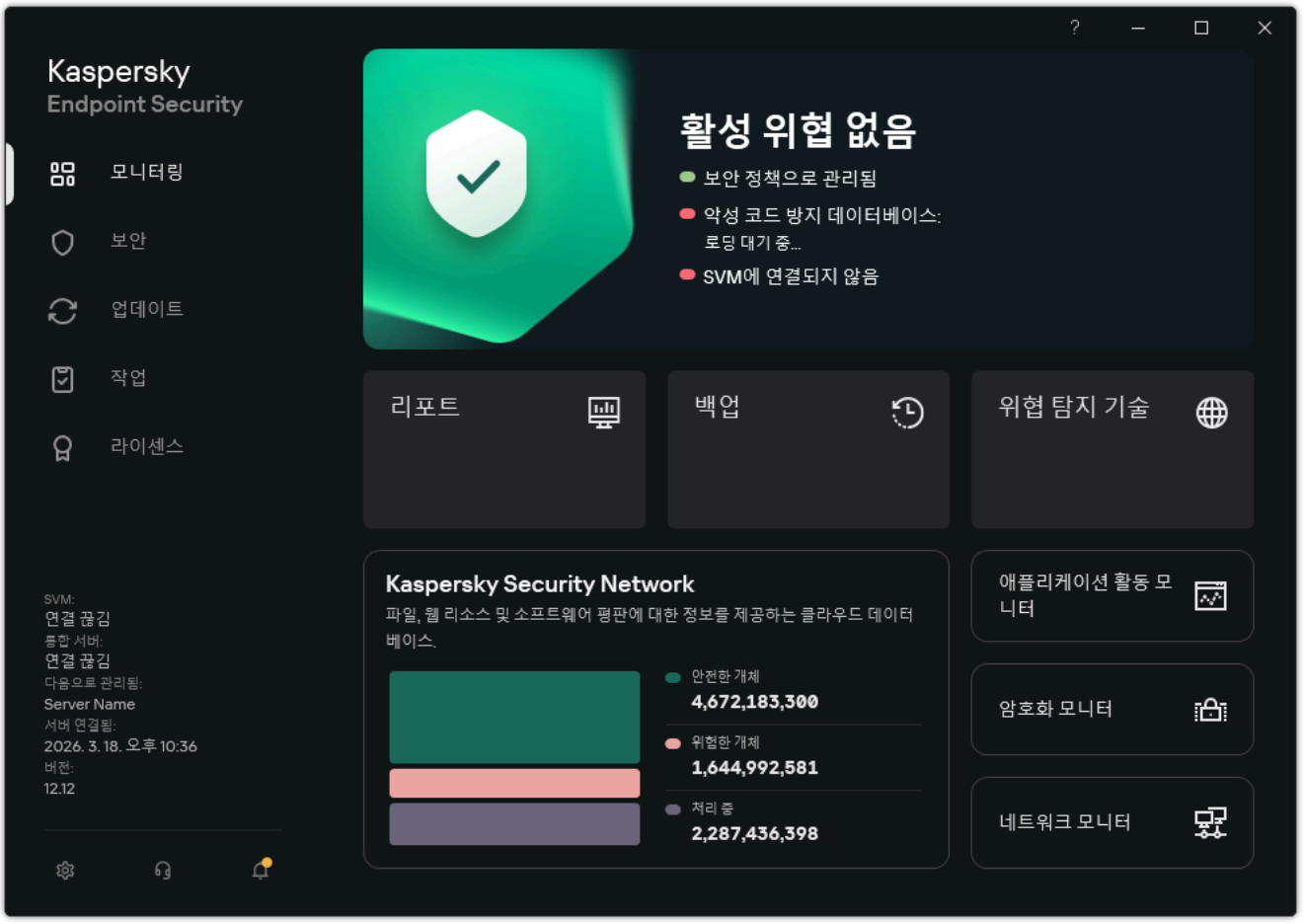
7. 신뢰 영역을 구성합니다. 애플리케이션을 설치할 가상 환경에 대해 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 선택합니다.

   사전 정의된 검사 예외 및 신뢰하는 애플리케이션은 애플리케이션을 빠르게 설정하고 가상 환경 호환성 문제를 방지하는 데 도움이 됩니다.

8. 변경 사항을 저장합니다.

9. 원격 설치 작업 생성. 작업 속성에서 생성한 설치 패키지를 선택합니다.

결과적으로 가상 컴퓨터에 Light Agent가 설치됩니다. 애플리케이션의 인터페이스를 사용할 수 있으며 알림 영역에 애플리케이션 아이콘이 표시됩니다. 이제 Light Agent와 SVM의 연결을 설정해야 합니다.



Light Agent 메인 창

Light Agent를 SVM에 연결

Kaspersky Security for Virtualization Light Agent 솔루션을 사용하려면 Light Agent와 SVM의 지속적인 통신이 필요합니다. 이는 Light Agent에서 전송한 파일을 스캔하여 바이러스 및 기타 악성 코드를 검사하는 데 필요합니다. SVM 연결이 없으면 Light Agent는 검사할 파일을 보낼 수 없습니다. 연결이 5분 이상 설정되지 않으면 검사가 오류와 함께 종료됩니다.

Light Agent를 SVM에 연결하는 방법은 다음과 같습니다:

1. Light Agent는 사용 가능한 SVM 목록을 가져옵니다.
2. Light Agent는 SVM 선택 알고리즘에 따라 연결에 최적화된 사용 가능한 보호 서버(SVM)를 결정합니다.
3. Light Agent는 태그, 연결 보호 상태, 라이센스가 적용되는 애플리케이션 기능 등 추가 SVM 연결 설정을 확인합니다.
4. Light Agent를 SVM에 연결합니다.

Light Agent의 SVM 연결 상태에 대한 정보는 Kaspersky Endpoint Security에서 또는 애플리케이션 명령을 사용하여 확인할 수 있습니다. Light Agent의 SVM 연결이 끊어지거나 설정될 때마다 애플리케이션이 이벤트를 생성하여 Kaspersky Security Center로 보냅니다. SVM 검색을 위해 통합 서버를 사용하는 경우, 통합 서버 콘솔에서 SVM 상태와 연결된 Light Agent의 개수에 대한 정보를 얻을 수 있습니다. SVM 상태 모니터링에 대한 자세한 내용은 Kaspersky Security for Virtualization Light Agent 도움말을 참조하십시오.

SVM 검색

Light Agent에 대한 SVM 검색 방법 중 하나를 선택할 수 있습니다:

- 통합 서버(VIIS) 사용.

  *통합 서버*는 Kaspersky Security for Virtualization Light Agent 와 가상 인프라의 상호 작용을 가능하게 하는 솔루션 구성 요소입니다. 통합 서버는 연결할 수 있는 SVM 목록을 관리합니다. Light Agent는 통합 서버와의 연결을 설정하고 SVM 주소 목록을 가져옵니다.

  통합 서버는 SVM 간에 부하를 자동으로 분산하기 때문에 대규모 가상 인프라에서 유용합니다. 통합 서버는 사용 가능한 SVM에 대한 정보를 가져와 분석한 후 연결에 최적화된 보호 서버(SVM) 목록을 Light Agent에 제공합니다.

  Light Agent가 SVM 목록을 가져오려면 통합 서버의 주소만 입력하면 됩니다.

- SVM 주소 목록 사용.

  Light Agent를 연결할 개별 SVM을 지정해야 하는 경우 수동으로 목록 준비할 수 있습니다.

  Light Agent가 연결할 수 있는 사용 가능한 SVM의 주소를 나열해야 합니다.

관리 콘솔(MMC)에서 Light Agent를 통한 SVM 검색을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **Light Agent 모드 → SVM 검색 설정**을 선택합니다.
4. SVM 검색 방법을 선택합니다.
   - **통합 서버 사용**. 통합 서버 연결 설정을 입력합니다. 통합 서버가 설치된 장치의 IPv4 형식 IP 주소 또는 정규화된 도메인 이름(FQDN)을 입력합니다.
   - **사용자 지정 SVM 주소 목록 사용**. Light Agent가 연결할 수 있는 SVM 목록을 생성합니다. IPv4 형식의 IP 주소 또는 SVM의 FQDN(정규화된 도메인 이름)을 지정합니다. 각 목록 항목은 반드시 줄바꿈하거나 세미콜론(`;`) 문자로 구분하여 입력해야 합니다.

     SVM 주소 목록에서 단일 IP 주소와 일치하는 전체 도메인 이름(FQDN)만 지정합니다. 여러 IP 주소에 해당하는 FQDN(정규화된 도메인 이름)을 사용하면 솔루션에 오류가 발생할 수 있습니다.
5. 변경 사항을 저장합니다.

웹 콘솔에서 Light Agent를 통한 SVM 검색을 구성하는 방법

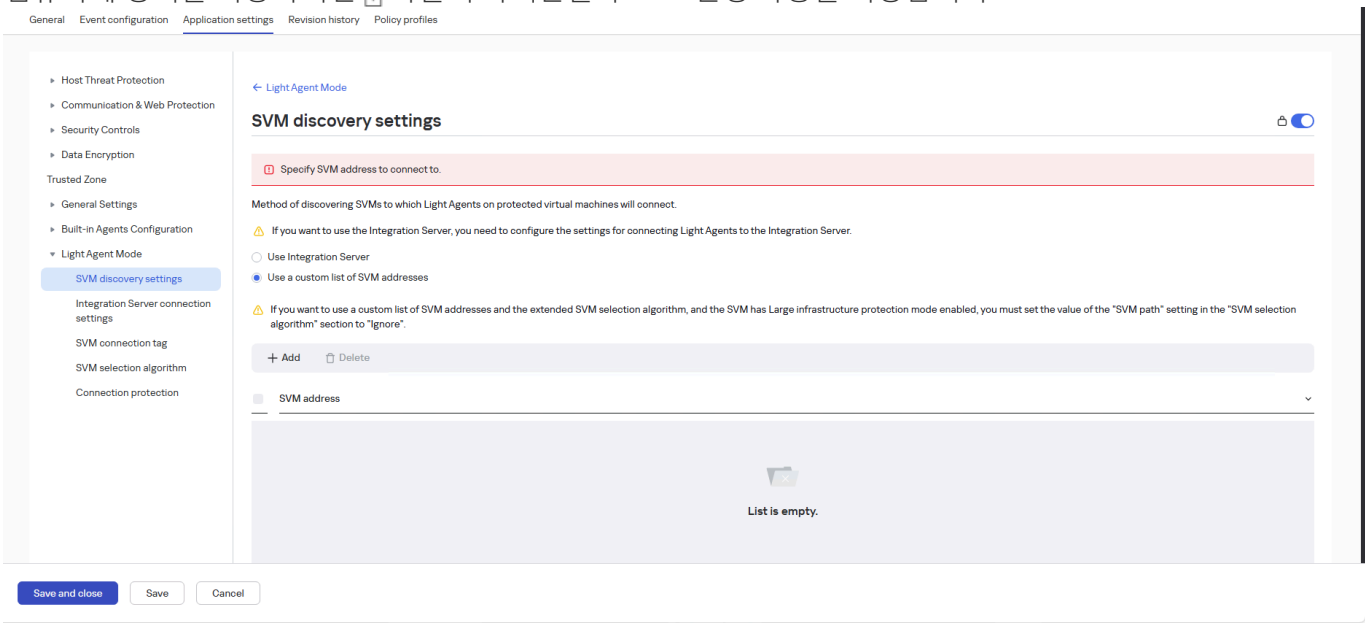
1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **Light Agent 모드 → SVM 검색 설정**으로 이동합니다.

5. SVM 검색 방법을 선택합니다.

- **통합 서버 사용**. 통합 서버 연결 설정을 입력합니다. 통합 서버가 설치된 장치의 IPv4 형식 IP 주소 또는 정규화된 도메인 이름(FQDN)을 입력합니다.
- **사용자 지정 SVM 주소 목록 사용**. Light Agent가 연결할 수 있는 SVM 목록을 생성합니다. IPv4 형식의 IP 주소 또는 SVM의 FQDN(정규화된 도메인 이름)을 지정합니다. 각 목록 항목은 반드시 줄바꿈하거나 세미콜론(;) 문자로 구분하여 입력해야 합니다.

> SVM 주소 목록에서 단일 IP 주소와 일치하는 전체 도메인 이름(FQDN)만 지정합니다. 여러 IP 주소에 해당하는 FQDN(정규화된 도메인 이름)을 사용하면 솔루션에 오류가 발생할 수 있습니다.

6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.



애플리케이션 인터페이스에서 Light Agent를 통한 SVM 검색을 구성하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **Light Agent 모드**에서 **SVM 검색 설정** 타일을 클릭합니다.
3. SVM 검색 방법을 선택합니다.

- **통합 서버 사용**. 통합 서버 연결 설정을 입력합니다. 통합 서버가 설치된 장치의 IPv4 형식 IP 주소 또는 정규화된 도메인 이름(FQDN)을 입력합니다.
- **사용자 지정 SVM 주소 목록 사용**. Light Agent가 연결할 수 있는 SVM 목록을 생성합니다. IPv4 형식의 IP 주소 또는 SVM의 FQDN(정규화된 도메인 이름)을 지정합니다. 각 목록 항목은 반드시 줄바꿈하거나 세미콜론(;) 문자로 구분하여 입력해야 합니다.

> SVM 주소 목록에서 단일 IP 주소와 일치하는 전체 도메인 이름(FQDN)만 지정합니다. 여러 IP 주소에 해당하는 FQDN(정규화된 도메인 이름)을 사용하면 솔루션에 오류가 발생할 수 있습니다.

4. 변경 사항을 저장합니다.

Light Agent용 SVM 선택 알고리즘 구성

조직의 인프라에는 Light Agent를 연결할 수 있는 여러 개의 배포된 SVM이 있을 수 있습니다. 네트워크와 가상 인프라의 자원에 대한 부하를 분산하려면 SVM 사이에 Light Agent를 분산해야 합니다.

Light Agent는 연결을 위해 다음 SVM 선택 알고리즘 중 하나를 적용할 수 있습니다:

- **표준 알고리즘**(기본값)

  표준 알고리즘은 다음 단계를 포함합니다:

  1. Light Agent가 *로컬 SVM*을 식별합니다.

     SVM을 로컬로 식별하기 위해 Light Agent는 주로 가상 인프라에서 SVM의 위치를 사용합니다. SVM이 Light Agent와 동일한 하이퍼바이저에 있는 경우 Light Agent는 이러한 SVM을 로컬로 간주합니다. 일부 가상 인프라에서는 구성 파일을 사용하여 로컬 SVM을 직접 지정해야 합니다.

  2. Light Agent가 여러 로컬 SVM을 탐지하면 Light Agent는 연결된 Light Agent의 수가 가장 적은 SVM을 선택합니다. 로컬 SVM을 식별할 수 없는 경우 Light Agent는 전체 가상 인프라에서 연결된 Light Agent의 수가 가장 적은 SVM을 선택합니다.

  로컬 SVM에 대한 자세한 내용은 Kaspersky Security for Virtualization Light Agent 도움말을 참조하십시오.

- **확장 알고리즘**

  확장 알고리즘을 사용하면 로컬 SVM 선택 기준을 직접 지정하거나 로컬 SVM 검색을 비활성화할 수 있습니다. 그렇게 하려면 가상 인프라에서 SVM 경로를 선택해야 합니다: 하이퍼바이저, 클러스터, 또는 데이터센터. 즉, 로컬 SVM이 검색될 범위를 선택해야 합니다. Light Agent는 구성된 검색 범위에서 로컬 SVM에 연결할 수 없으면 연결 시도를 중지합니다. 확장 알고리즘을 사용하면 Light Agent에 대한 로컬 SVM 검색을 비활성화할 수도 있습니다. 이 경우 Light Agent는 전체 가상 인프라에서 연결된 Light Agent의 수가 가장 적은 SVM을 선택합니다.

SVM 연결 알고리즘 외에도 태그를 사용하여 Light Agent와 SVM의 연결을 규제할 수 있습니다.

관리 콘솔(MMC)에서 Light Agent용 SVM 선택 알고리즘을 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **Light Agent 모드** → **SVM 선택 알고리즘**을 선택합니다.
4. 알고리즘 선택:
   - **표준 SVM 선택 알고리즘 사용**. Light Agent는 동일한 하이퍼바이저에 배포된 SVM을 선택합니다.
   - **확장된 SVM 선택 알고리즘 사용**. Light Agent는 선택한 SVM 경로 유형(기본적으로, **하이퍼바이저**)에 배포된 SVM을 선택합니다.

5. 필요한 경우 확장된 SVM 선택 알고리즘을 위한 SVM 경로를 선택합니다:

   - **하이퍼바이저**. Light Agent는 특정 기준(가상 인프라 유형에 따라 결정됨)과 일치하는 SVM을 연결 대상으로 선택합니다:

     - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 하이퍼바이저에 배포됩니다(Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis(Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux 또는 Numa vServer의 가상 인프라).

     - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 서버 그룹에 속해 있습니다(OpenStack 플랫폼, VK Cloud 플랫폼 또는 TIONIX Cloud Platform에서 실행되는 가상 인프라).

     Light Agent가 설치된 가상 컴퓨터가 속한 하이퍼바이저 또는 이와 동일한 서버 그룹에 사용 가능한 SVM이 없는 경우, Light Agent는 SVM에 연결되지 않습니다.

   - **클러스터**. Light Agent는 특정 기준(가상 인프라 유형에 따라 결정됨)과 일치하는 SVM을 연결 대상으로 선택합니다:

     - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 하이퍼바이저 클러스터에 배포됩니다(Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis(Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux 또는 Numa vServer의 가상 인프라).

     - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 OpenStack 프로젝트에 배포됩니다(OpenStack 플랫폼, VK Cloud 플랫폼 또는 TIONIX Cloud Platform에서 실행되는 가상 인프라).

     Light Agent가 설치된 가상 컴퓨터가 속한 하이퍼바이저 클러스터 또는 이와 동일한 OpenStack 프로젝트에 사용 가능한 SVM이 없는 경우, Light Agent는 SVM에 연결되지 않습니다.

   - **데이터센터**. Light Agent는 특정 기준(가상 인프라 유형에 따라 결정됨)과 일치하는 SVM을 연결 대상으로 선택합니다:

     - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 데이터 센터에 배포됩니다(Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis(Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux 또는 Numa vServer의 가상 인프라).

     - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 가용 영역에 속해 있습니다(OpenStack 플랫폼, VK Cloud 플랫폼 또는 TIONIX Cloud Platform에서 실행되는 가상 인프라).

     Light Agent가 설치된 가상 컴퓨터가 속한 동일한 데이터 센터 또는 가용 영역에 연결 가능한 SVM이 없는 경우, Light Agent는 SVM에 연결되지 않습니다.

   - **무시**. Light Agent는 보호 서버에 연결하기 위해 SVM 경로를 무시합니다. Light Agent는 태그, SVM에 연결된 Light Agent의 수 등 다른 기준을 고려합니다.

6. 변경 사항을 저장합니다.

웹 콘솔에서 Light Agent용 SVM 선택 알고리즘을 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.

3. **애플리케이션 설정** 탭을 선택합니다.

4. **Light Agent 모드** → **SVM 선택 알고리즘**으로 이동합니다.

5. 알고리즘 선택:

- **표준 SVM 선택 알고리즘 사용**. Light Agent는 동일한 하이퍼바이저에 배포된 SVM을 선택합니다.
- **확장된 SVM 선택 알고리즘 사용**. Light Agent는 선택한 SVM 경로 유형(기본적으로, **하이퍼바이저**)에 배포된 SVM을 선택합니다.

6. 필요한 경우 확장된 SVM 선택 알고리즘을 위한 SVM 경로를 선택합니다:

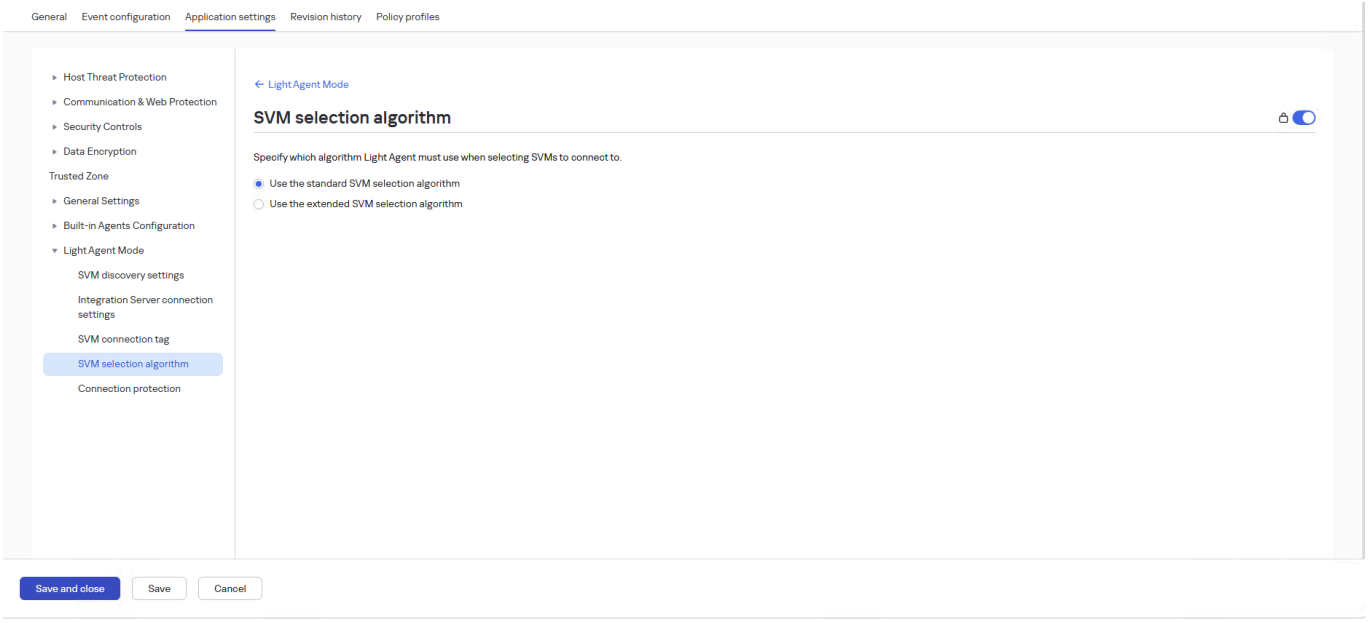
- **하이퍼바이저**. Light Agent는 특정 기준(가상 인프라 유형에 따라 결정됨)과 일치하는 SVM을 연결 대상으로 선택합니다:
  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 하이퍼바이저에 배포됩니다(Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis(Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux 또는 Numa vServer의 가상 인프라).
  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 서버 그룹에 속해 있습니다(OpenStack 플랫폼, VK Cloud 플랫폼 또는 TIONIX Cloud Platform에서 실행되는 가상 인프라).

  Light Agent가 설치된 가상 컴퓨터가 속한 하이퍼바이저 또는 이와 동일한 서버 그룹에 사용 가능한 SVM이 없는 경우, Light Agent는 SVM에 연결되지 않습니다.
- **클러스터**. Light Agent는 특정 기준(가상 인프라 유형에 따라 결정됨)과 일치하는 SVM을 연결 대상으로 선택합니다:
  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 하이퍼바이저 클러스터에 배포됩니다(Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis(Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux 또는 Numa vServer의 가상 인프라).
  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 OpenStack 프로젝트에 배포됩니다(OpenStack 플랫폼, VK Cloud 플랫폼 또는 TIONIX Cloud Platform에서 실행되는 가상 인프라).

  Light Agent가 설치된 가상 컴퓨터가 속한 하이퍼바이저 클러스터 또는 이와 동일한 OpenStack 프로젝트에 사용 가능한 SVM이 없는 경우, Light Agent는 SVM에 연결되지 않습니다.
- **데이터센터**. Light Agent는 특정 기준(가상 인프라 유형에 따라 결정됨)과 일치하는 SVM을 연결 대상으로 선택합니다:
  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 데이터 센터에 배포됩니다(Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis(Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux 또는 Numa vServer의 가상 인프라).
  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 가용 영역에 속해 있습니다(OpenStack 플랫폼, VK Cloud 플랫폼 또는 TIONIX Cloud Platform에서 실행되는 가상 인프라).

  Light Agent가 설치된 가상 컴퓨터가 속한 동일한 데이터 센터 또는 가용 영역에 연결 가능한 SVM이 없는 경우, Light Agent는 SVM에 연결되지 않습니다.
- **무시**. Light Agent는 보호 서버에 연결하기 위해 SVM 경로를 무시합니다. Light Agent는 태그, SVM에 연결된 Light Agent의 수 등 다른 기준을 고려합니다.

7. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.



SVM 선택 알고리즘 정책 섹션

애플리케이션 인터페이스에서 Light Agent용 SVM 선택 알고리즘을 구성하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **Light Agent 모드**에서 **SVM 검색 설정** 타일을 클릭합니다.
3. 알고리즘 선택:
   - **표준 SVM 선택 알고리즘 사용**. Light Agent는 동일한 하이퍼바이저에 배포된 SVM을 선택합니다.
   - **확장된 SVM 선택 알고리즘 사용**. Light Agent는 선택한 SVM 경로 유형(기본적으로, **하이퍼바이저**)에 배포된 SVM을 선택합니다.
4. 필요한 경우 확장된 SVM 선택 알고리즘을 위한 SVM 경로를 선택합니다:
   - **하이퍼바이저**. Light Agent는 특정 기준(가상 인프라 유형에 따라 결정됨)과 일치하는 SVM을 연결 대상으로 선택합니다:
     - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 하이퍼바이저에 배포됩니다(Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis(Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux 또는 Numa vServer의 가상 인프라).
     - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 서버 그룹에 속해 있습니다(OpenStack 플랫폼, VK Cloud 플랫폼 또는 TIONIX Cloud Platform에서 실행되는 가상 인프라).

     Light Agent가 설치된 가상 컴퓨터가 속한 하이퍼바이저 또는 이와 동일한 서버 그룹에 사용 가능한 SVM이 없는 경우, Light Agent는 SVM에 연결되지 않습니다.

- **클러스터**. Light Agent는 특정 기준(가상 인프라 유형에 따라 결정됨)과 일치하는 SVM을 연결 대상으로 선택합니다:

  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 하이퍼바이저 클러스터에 배포됩니다(Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis(Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux 또는 Numa vServer의 가상 인프라).

  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 OpenStack 프로젝트에 배포됩니다(OpenStack 플랫폼, VK Cloud 플랫폼 또는 TIONIX Cloud Platform에서 실행되는 가상 인프라).

  Light Agent가 설치된 가상 컴퓨터가 속한 하이퍼바이저 클러스터 또는 이와 동일한 OpenStack 프로젝트에 사용 가능한 SVM이 없는 경우, Light Agent는 SVM에 연결되지 않습니다.

- **데이터센터**. Light Agent는 특정 기준(가상 인프라 유형에 따라 결정됨)과 일치하는 SVM을 연결 대상으로 선택합니다:

  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 데이터 센터에 배포됩니다(Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis(Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux 또는 Numa vServer의 가상 인프라).

  - SVM은 Light Agent가 설치된 가상 컴퓨터와 동일한 가용 영역에 속해 있습니다(OpenStack 플랫폼, VK Cloud 플랫폼 또는 TIONIX Cloud Platform에서 실행되는 가상 인프라).

  Light Agent가 설치된 가상 컴퓨터가 속한 동일한 데이터 센터 또는 가용 영역에 연결 가능한 SVM이 없는 경우, Light Agent는 SVM에 연결되지 않습니다.

- **무시**. Light Agent는 보호 서버에 연결하기 위해 SVM 경로를 무시합니다. Light Agent는 태그, SVM에 연결된 Light Agent의 수 등 다른 기준을 고려합니다.

5. 변경 사항을 저장합니다.

Light Agent와 SVM 연결 배포(태그)

하나의 SVM에 여러 개의 Light Agent를 연결할 수 있습니다. Light Agent 연결의 균형을 맞추기 위해 별도의 SVM 목록을 지정할 수 있습니다. SVM 검색을 위해 통합 서버를 사용하는 경우 *태그*를 사용하여 SVM에 대한 Light Agent 연결의 균형을 맞출 수 있습니다. 즉, Light Agent의 경우, 태그를 사용하여 연결할 SVM 목록을 지정할 수 있습니다. 그렇게 하려면 Light Agent에 태그를 할당하고 SVM 설정에서 이 태그를 지정해야 합니다. SVM 설정에서 태그를 지정하는 방법에 대한 자세한 내용은 Kaspersky Security for Virtualization Light Agent 도움말을 참조하십시오.

예: Kaspersky Endpoint Detection and Response Optimum 솔루션은 지정된 가상 컴퓨터 호스트의 인프라에 배포됩니다. 이 경우 Light Agent에 `[EDROptimum]` 태그를 지정하여 EDR Optimum(EDR Optimum 애드온) 라이센스 키가 추가된 SVM에 연결할 수 있습니다. 그러면 Light Agent를 사용하는 가상 컴퓨터에서 EDR Optimum 기능을 사용할 수 있습니다. Light Agent를 EDR Optimum 라이선스 키가 없는 SVM에 연결하면 Kaspersky Endpoint Detection and Response Optimum 기능을 사용할 수 없습니다.

관리 콘솔(MMC)에서 SVM 연결 태그를 Light Agent에 할당하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.

2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

3. 정책 창에서 **Light Agent 모드 → SVM 연결 태그**를 선택합니다.

4. **연결 태그 사용** 확인란을 선택하고 SVM 연결 태그를 입력합니다.

   태그의 경우 최대 255자 길이의 텍스트 문자열을 입력할 수 있습니다. `;` 문자를 제외한 모든 문자를 사용할 수 있습니다.

5. 변경 사항을 저장합니다.

웹 콘솔에서 SVM 연결 태그를 Light Agent에 할당하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.

2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.

   정책 속성 창이 열립니다.

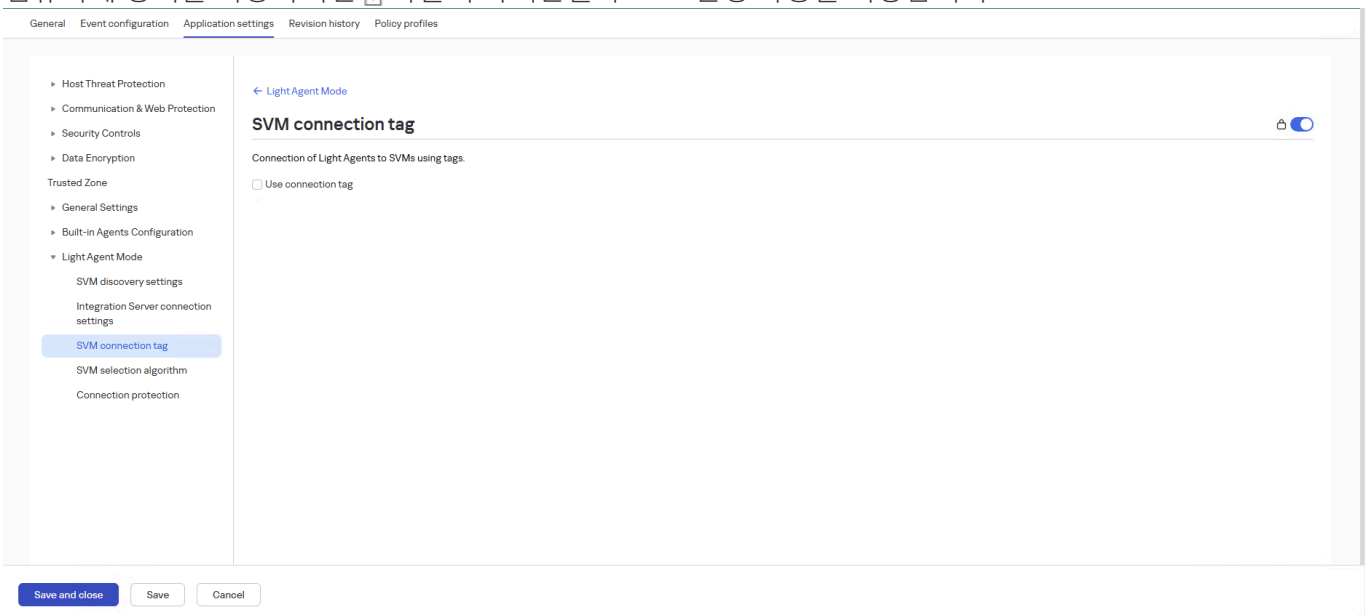
3. **애플리케이션 설정** 탭을 선택합니다.

4. **Light Agent 모드** → **SVM 연결 태그**로 이동합니다.

5. **연결 태그 사용** 확인란을 선택하고 SVM 연결 태그를 입력합니다.

   태그의 경우 최대 255자 길이의 텍스트 문자열을 입력할 수 있습니다. `;` 문자를 제외한 모든 문자를 사용할 수 있습니다.

6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.



KUMA 태그 정책 섹션에 연결

애플리케이션 인터페이스에서 SVM 연결 태그를 Light Agent에 할당하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.

2. 애플리케이션 설정 창에서 **Light Agent 모드**에서 **SVM 연결 태그** 타일을 클릭합니다.

3. **연결 태그 사용** 확인란을 선택하고 SVM 연결 태그를 입력합니다.

   태그의 경우 최대 255자 길이의 텍스트 문자열을 입력할 수 있습니다. `;` 문자를 제외한 모든 문자를 사용할 수 있습니다.

4. 변경 사항을 저장합니다.

Light Agent와 SVM 간의 연결 보호

Light Agent와 보호 서버 간의 연결에 대한 암호화를 구성할 수 있습니다. 이를 위해서는 SVM의 보호 서버 설정과 Light Agent 설정에서 Light Agent와 보호 서버 간의 데이터 채널 암호화를 활성화해야 합니다.

연결 보호가 설정된 Light Agent는 Light Agent와 보호 서버 간의 데이터 채널 암호화가 활성화된 SVM에만 연결할 수 있습니다. 연결 보호가 비활성화된 Light Agent는 채널 암호화가 비활성화되거나 보호 서버와 Light Agent 간의 안전하지 않은 연결이 허용되는 SVM에만 연결할 수 있습니다.

보호 서버에서 연결 보호를 구성하는 방법에 대한 자세한 내용은 Kaspersky Security for Virtualization Light Agent 도움말을 참조하십시오.

암호화를 사용하여 연결을 보호하면 Kaspersky Security for Virtualization Light Agent의 성능에 영향을 줄 수 있습니다.

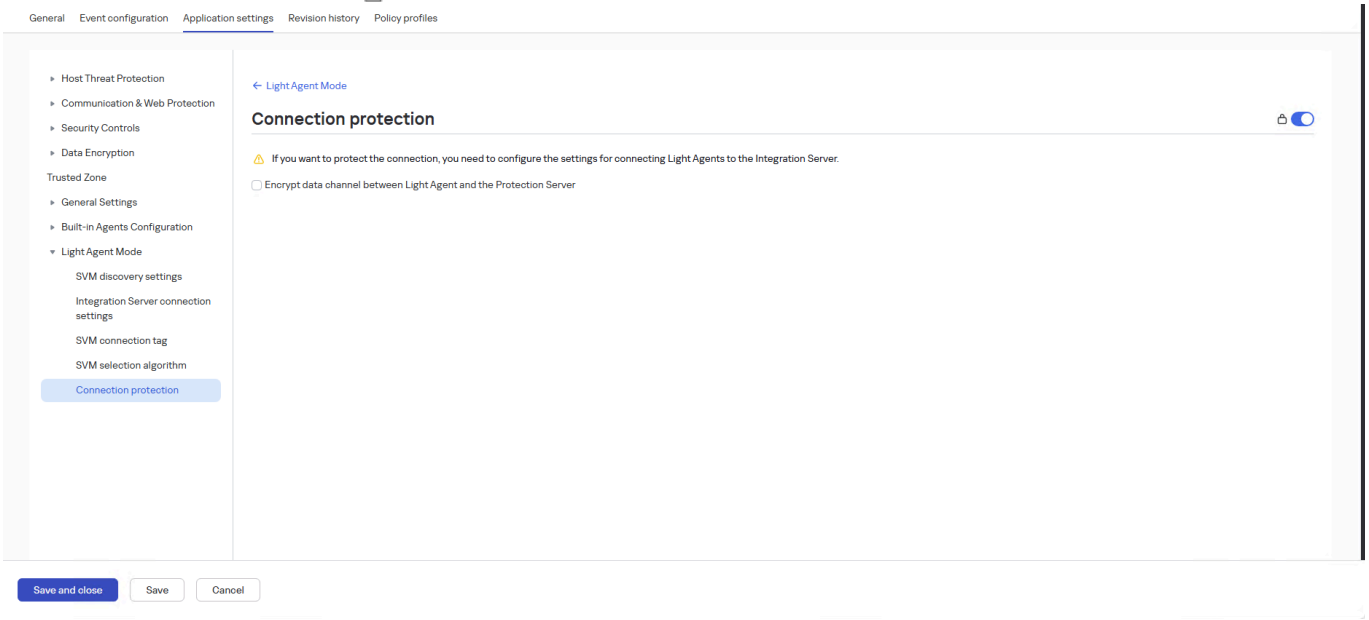
관리 콘솔(MMC)에서 Light Agent의 연결 보호를 구성하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **Light Agent 모드** → **연결 보호**를 선택합니다.
4. **Light Agent와 보호 서버 간 데이터 채널 암호화** 확인란을 선택합니다.
5. 변경 사항을 저장합니다.

웹 콘솔에서 Light Agent의 연결 보호를 구성하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **Light Agent 모드** → **연결 보호**로 이동합니다.
5. **Light Agent와 보호 서버 간 데이터 채널 암호화** 확인란을 선택합니다.

6. 컴퓨터에 정책을 적용하려면 자물쇠 아이콘을 누르고 변경 사항을 저장합니다.



연결 보호 정책 섹션

애플리케이션 인터페이스에서 Light Agent의 연결 보호를 구성하는 방법

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **Light Agent 모드**에서 **연결 보호** 타일을 클릭합니다.
3. **Light Agent와 보호 서버 간 데이터 채널 암호화** 확인란을 선택합니다.
4. 변경 사항을 저장합니다.

Light Agent 활성화

Kaspersky Endpoint Security가 가상 환경 보호를 위한 Light Agent 모드에서 사용되는 경우에는 애플리케이션을 별도로 활성화할 필요가 없습니다. 애플리케이션을 활성화하려면 SVM에 라이센스 키를 추가해야 합니다. Kaspersky Security Center 콘솔의 특수 작업을 사용하여 라이센스 키를 SVM에 추가할 수 있습니다. Light Agent 인터페이스에서 라이센스 키는 관리할 수 없지만 라이센스 정보를 확인할 수 있습니다(아래 그림 참조). Light Agent 라이센스 정보는 명령줄에서도 확인할 수 있습니다(아래 지침 참조). Light Agent는 SVM에서 이 정보를 가져옵니다. 솔루션 활성화 및 라이센스 키 관리에 대한 자세한 내용은 Kaspersky Security for Virtualization Light Agent 도움말을 참조하십시오.

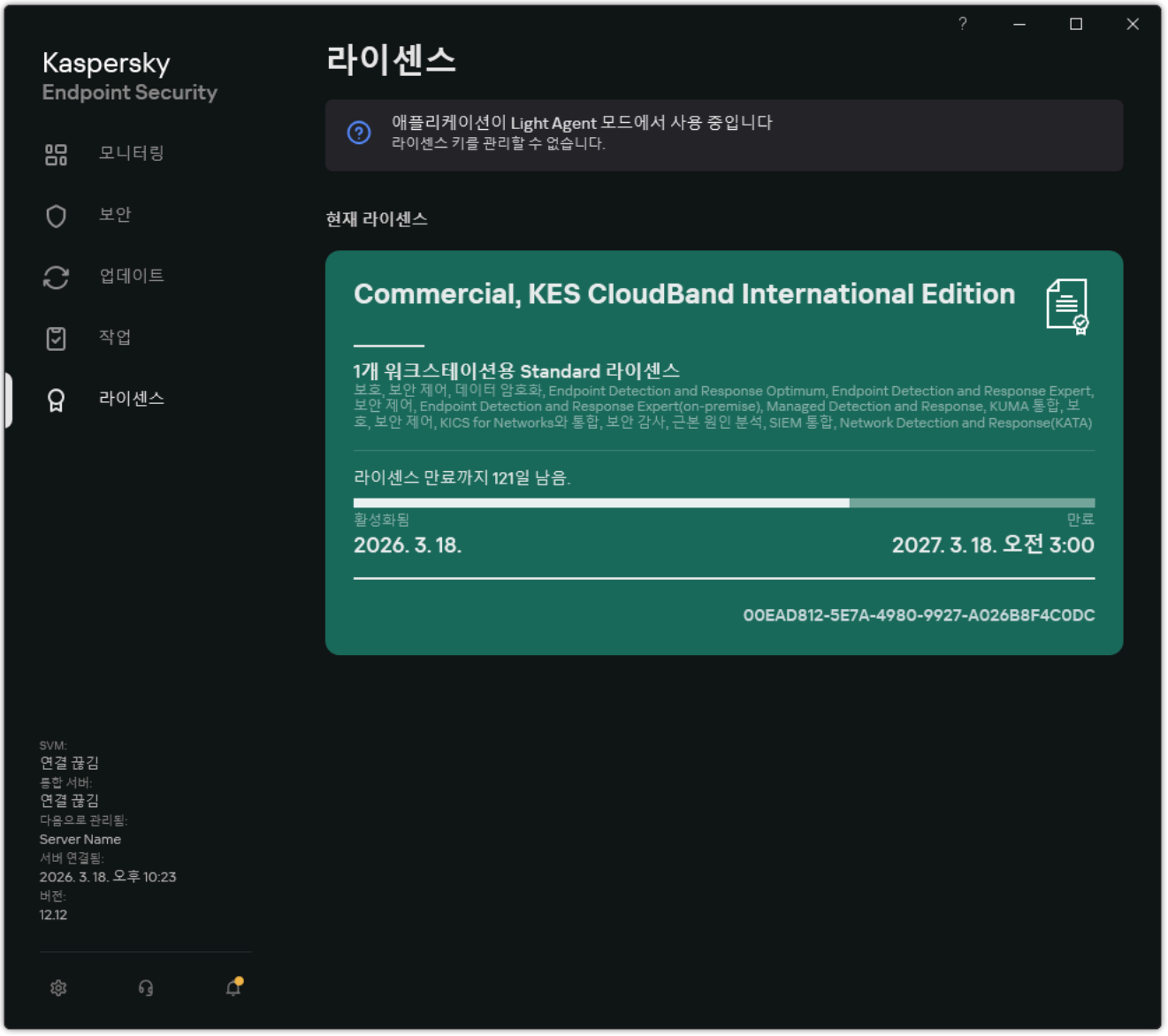
Light Agent 라이센스 정보를 보려면 다음과 같이 하십시오:

1. 명령줄 해석기(cmd)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

3. 다음 명령을 실행합니다:

```
avp.com LICENSE /CHECK
```

그러면 Kaspersky Endpoint Security는 Light Agent가 연결된 SVM의 주소, 라이센스가 만료될 때까지 남은 일 수 및 기타 정보와 같은 라이센스 정보를 표시합니다. Light Agent를 활성화할 때 문제가 발생하는 경우 기술 지원 기술 자료를 참조하십시오.



라이센스 창

KSVLA Light Agent에서 KES Light Agent로의 마이그레이션 가이드

Kaspersky Security for Virtualization 5.2 Light Agent에는 Light Agent for Windows 5.2 구성 요소(이하 "KSVLA Light Agent"라고도 함)가 포함됩니다. Kaspersky Security for Virtualization Light Agent 6.2에서는 Kaspersky Endpoint Security in Light Agent 모드가 Light Agent 구성 요소로 사용됩니다. 솔루션을 버전 6.2로 업데이트하려면 Light Agent 모드(이하 "KES Light Agent"라고도 불림)에서 KSVLA Light Agent 5.2를 Kaspersky Endpoint Security로 마이그레이션해야 합니다. Kaspersky Security for Virtualization Light Agent 솔루션 버전 업데이트에 대한 자세한 내용은 Kaspersky Security for Virtualization Light Agent 도움말을 참조하십시오.

소프트웨어 요구 사항

KSVLA Light Agent에서 KES Light Agent로 마이그레이션을 시작하기 전에 가상 컴퓨터가 Kaspersky Endpoint Security for Windows의 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인하십시오. KES와 KSWS는 지원되는 운영 체제 버전 목록이 서로 다릅니다. 예를 들어 KES는 Windows Server 2003을 실행하는 서버를 지원하지 않습니다.

KSVLA Light Agent에서 KES Light Agent로 마이그레이션하기 위한 최소 소프트웨어 요구 사항:

- Kaspersky Endpoint Security for Windows 12.8
- Kaspersky Security for Virtualization Light Agent 6.2(보호 서버 및 통합 서버 구성 요소 포함).
- Kaspersky Security Center 14.2

  Kaspersky Security Center 이전 버전이 설치되어 있는 경우 14.2 이상으로 업데이트하십시오. 이 버전의 Kaspersky Security Center에서는 정책 및 작업 변환 마법사를 사용하여 여러 정책을 단일 정책 대신 단일 프로필로 마이그레이션할 수 있습니다. 또한 이 버전의 Kaspersky Security Center에서는 정책 및 작업 변환 마법사를 사용하여 더 광범위한 정책 설정을 마이그레이션할 수도 있습니다.

마이그레이션 단계

KSVLA Light Agent에서 KES Light Agent로의 마이그레이션은 반자동으로 수행됩니다. 애플리케이션의 아키텍처가 서로 다르기 때문입니다.

다음 순서에 따라 KSVLA Light Agent에서 KES Light Agent로 마이그레이션합니다.

1. **KSVLA Light Agent 작업 및 정책 마이그레이션**

   정책 설정을 마이그레이션하려면 정책 및 작업 변환 마법사(마이그레이션 마법사)를 실행해야 합니다. 정책 설정을 마이그레이션한 후에는 마이그레이션 마법사가 자동으로 마이그레이션할 수 없는 설정(예: 데이터베이스 업데이트 설정)을 수동으로 구성해야 합니다. 마이그레이션이 끝나면 마이그레이션 마법사가 모든 설정을 올바르게 마이그레이션했는지 확인하는 것이 좋습니다.

   암호 보호가 활성화되어 KSVLA Light Agent에 대한 접근이 제한된 경우 KES Light Agent를 설치하기 전에 KSVLA Light Agent의 정책에서 암호 보호를 비활성화해야 합니다. KES Light Agent 설치 패키지 설정에 제거 암호를 입력할 수 없습니다. KSVLA Light Agent 상단에 KES Light Agent 설치를 완료한 후 KES 정책에서 암호 보호를 활성화해야 합니다.

2. **Light Agent 모드로 Kaspersky Endpoint Security 설치**

   다음과 같은 방법으로 KES Light Agent를 설치할 수 있습니다.

   - KSVLA Light Agent 제거 후 KES Light Agent 설치(권장)
   - KSVLA Light Agent 상단에 KES Light Agent 설치

3. **마이그레이션 후 애플리케이션이 제대로 작동하는지 확인합니다.**

   KSVLA Light Agent에서 KES Light Agent로의 마이그레이션이 끝나면 애플리케이션이 올바르게 작동하는지 확인하십시오. 변환된 정책을 활성화합니다. Kaspersky Security Center 콘솔에서 가상 컴퓨터의 상태를 확인합니다(*정상*이어야 함). 애플리케이션에 보고된 오류가 없는지 확인하고, SVM에 마지막으로 연결한 시간과 가상 컴퓨터 보호 상태를 확인합니다. 라이센스 키는 SVM에 추가되어 있으므로 Light Agent를 활성화할 필요가 없습니다.

KSVLA Light Agent 대신 KES Light Agent 설치

KES Light Agent는 다음과 같은 방법으로 설치할 수 있습니다.

- KSVLA Light Agent 제거 후 KES Light Agent 설치(권장)
- KSVLA Light Agent 상단에 KES Light Agent 설치

KSVLA Light Agent 제거

가상 컴퓨터에서 로컬로 또는 가상 컴퓨터 템플릿에서 *원격으로 애플리케이션 설치 작업*을 사용하여 원격으로 애플리케이션을 제거할 수 있습니다. KSVLA Light Agent를 제거한 후 가상 컴퓨터를 다시 시작해야 할 수 있습니다.

KSVLA Light Agent를 제거한 후 적절한 방법을 사용하여 KES Light Agent를 설치합니다.

Kaspersky Endpoint Security 설치

> 암호 보호가 활성화되어 KSVLA Light Agent에 대한 접근이 제한된 경우 KES Light Agent를 설치하기 전에 KSVLA Light Agent의 정책에서 암호 보호를 비활성화해야 합니다. KES Light Agent 설치 패키지 설정에 제거 암호를 입력할 수 없습니다. KSVLA Light Agent 상단에 KES Light Agent 설치를 완료한 후 KES 정책에서 암호 보호를 활성화해야 합니다.

Kaspersky Endpoint Security를 설치할 때 **가상 환경을 보호하는 Light Agent** 모드를 선택해야 합니다. 가상 컴퓨터에서 KES Light Agent를 설치하기 전에 설치 프로그램은 KSVLA Light Agent를 호환되지 않는 소프트웨어로 감지하고 제거합니다. KSVLA Light Agent 구성의 마이그레이션은 지원하지 않습니다. 즉, KES Light Agent를 설치할 때 설치 패키지 속성 또는 설치 마법사의 선택 사항에 따라 설치할 구성 요소 집합이 결정됩니다. KSVLA Light Agent를 제거한 후 가상 컴퓨터를 다시 시작해야 합니다.

KES Light Agent 설치 시 KSVLA Light Agent의 설정 및 작업이 마이그레이션되지 않습니다. 설정 및 작업을 마이그레이션하려면 정책 및 작업 변환 마법사를 실행합니다.

애플리케이션 인터페이스의 **보안** 섹션이나 컴퓨터 속성의 Kaspersky Security Center 콘솔에서, 또는 `status` 명령을 사용하여 설치된 구성 요소 목록을 확인할 수 있습니다. 설치한 후에는 *애플리케이션 구성 요소 변경*을 사용하여 구성 요소 세트를 변경할 수 있습니다.

KSVLA Light Agent 및 KES Light Agent 구성 요소의 대응

KSVLA Light Agent와 KES Light Agent의 구성 요소 집합은 거의 동일합니다. KES Light Agent에는 KSVLA Light Agent보다 설정이 많습니다. 마이그레이션 후에는 새로운 설정이 기본값으로 설정됩니다.

KSVLA Light Agent 및 KES Light Agent 구성 요소의 대응

Light Agent 5.2	KES Light Agent
Scan kernel	애플리케이션 커널
File Anti-Virus	파일 위협 보호
Mail Anti-Virus	메일 위협 보호
Web Anti-Virus	웹 위협 보호
Firewall	방화벽
Network Attack Blocker	네트워크 위협 보호
Application Privilege Control	호스트 침입 방지
Applications Launch Control	애플리케이션 제어
Web Control	웹 제어
Device Control	장치 제어
System Watcher	Kaspersky Endpoint Security에서 이 구성 요소는 다음 구성 요소로 나뉩니다: • 익스플로잇 방지 • 행동 탐지 • 복원 엔진
System Integrity Monitoring	시스템 무결성 모니터링
Integration with Kaspersky Endpoint Agent	*(지원하지 않음)* Kaspersky Endpoint Security 11.9.0에서는 배포 키트에 Kaspersky Endpoint Agent 배포 패키지가 포함되지 않습니다.
AMSI Protection	AMSI 보호

KSVLA Light Agent 작업 및 정책 마이그레이션

정책 및 작업 변환 마법사(이하 "마이그레이션 마법사"라고도 함)를 사용하여 KSVLA Light Agent 정책 및 작업 설정을 마이그레이션할 수 있습니다.

KSVLA Light Agent용 마이그레이션 마법사는 관리 콘솔(MMC)에서만 사용할 수 있습니다. 웹 콘솔 및 Cloud Console에서는 정책 및 작업 설정을 마이그레이션할 수 없습니다.

정책과 작업을 마이그레이션과 관련하여 다음과 같은 특별한 고려 사항이 있습니다:

- 새 정책의 이름은 *<정책> (변환됨)*입니다.
- 새 정책은 *비활성 정책* 상태입니다.
- 설정 변경이 금지된 상태("자물쇠")는 마이그레이션되지 않습니다. 마이그레이션 마법사가 기본값을 설정합니다.
- 정책 프로필은 마이그레이션되지 않습니다. 정책 프로필을 수동으로 추가해야 합니다.

- 신뢰 구역 관리를 개선했습니다. KSVLA Light Agent에서는 정책을 생성할 때만 사전 정의된 예외 사항을 추가할 수 있었습니다. 이후 정책 속성에서 이전에 추가한 사전 정의된 예외 사항을 구성하거나 수동으로 예외 사항을 추가할 수 있습니다. 정책 속성에서 사전 정의된 예외 사항을 추가할 수 없습니다. KES Light Agent에서 정책을 생성하는 동안 그리고 생성된 정책의 속성에서 사전 정의된 예외 사항을 사용할 수 있습니다. 설치 패키지에서 사전 정의된 예외 사항을 선택할 수도 있습니다.

- Kaspersky Endpoint Security의 애플리케이션 사용자 인터페이스 구성이 설치 프로그램에서 정책으로 이동되었습니다. 예를 들어 애플리케이션의 사용자 인터페이스를 숨겨야 할 필요가 있는 경우 정책 설정을 관리합니다.

- 권한 기반 접근 제어(RBAC) 구성에 대한 기능 집합은 Kaspersky Endpoint Security와 KSVLA Light Agent에서 서로 다릅니다. 기능 영역에 대한 사용자 접근 권한을 처음부터 구성해야 합니다.

정책 및 작업 변환 마법사를 사용하여 KSVLA Light Agent 정책 설정을 마이그레이션하는 방법

1. 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

이 단계에서 Kaspersky Endpoint Security for Windows를 선택해야 합니다. 다음 단계로 넘어갑니다.

2단계. 정책 전환

변환하려는 Kaspersky Security for Virtualization 5.2 Light Agent for Windows 정책을 선택합니다. 다음 단계로 넘어갑니다.

그러면 마이그레이션 마법사가 정책 변환을 시작합니다. 변환 중에 마이그레이션 마법사에 KSN 진술문의 조건을 수락하라는 메시지가 표시됩니다. 새 정책의 이름은 *<정책> (변환됨)*입니다.

3단계. 작업 전환

마이그레이션 마법사는 Kaspersky Endpoint Security for Windows에 대한 새 작업을 생성합니다. 작업 목록에서 Kaspersky Endpoint Security에 생성하고자 하는 KSVLA Light Agent 작업을 선택합니다. 새 작업의 이름이 *<작업 이름> (변환됨)*과 같이 지정됩니다. 다음 단계로 넘어갑니다.

4단계. 마법사 완료

마법사를 끝냅니다.

정책 마이그레이션 후에는 정책 속성을 열고 설정을 확인하고 해당 정책을 저장해야 합니다. 이 단계를 완료하지 않으면 KES Light Agent에서 변환된 정책을 무시할 수 있습니다.

Light Agent의 SVM 연결 설정, 예외 목록, 신뢰하는 애플리케이션, 신뢰하는 웹 주소, 애플리케이션 제어 규칙의 마이그레이션에 특히 주의합니다.

[KSVLA Light Agent+KEA] 구성을 [KES Light Agent+내장 에이전트] 구성으로 마이그레이션

Kaspersky Endpoint Security for Windows를 EDR(KATA), EDR Optimum, Kaspersky Sandbox의 일부로 사용하는 것을 지원하기 위해 애플리케이션에 내장 에이전트가 추가되었습니다. 이제 Kaspersky Endpoint Agent 애플리케이션이 없어도 이 솔루션을 이용할 수 있습니다.

KSVLA Light Agent에서 KES Light Agnt로 마이그레이션하는 경우 EDR(KATA), EDR Optimum, Kaspersky Sandbox 솔루션은 여전히 Kaspersky Endpoint Security 내장 에이전트와 함께 사용할 수 있습니다. 또한 Kaspersky Endpoint Agent가 컴퓨터에서 제거됩니다.

KSVLA Light Agent에서 KES Light Agent로 마이그레이션하기 전에 보호 서버와 통합 서버를 포함하여 Kaspersky Security for Virtualization의 모든 구성 요소를 버전 6.2로 업데이트해야 합니다. Kaspersky Security for Virtualization Light Agent 솔루션 버전 업데이트에 대한 자세한 내용은 Kaspersky Security for Virtualization Light Agent 도움말을 참조하십시오.

[KSVLA Light Agent+KEA] 구성을 [KES Light Agent+내장 에이전트] 구성으로 마이그레이션하는 단계는 다음과 같습니다.

1. **정책 및 작업 마이그레이션**

   [KSVLA Light Agent+KEA] 정책 및 작업을 [KES+내장 에이전트]로 마이그레이션하는 단계는 다음과 같습니다.

   1. 정책 및 작업 변환 마법사를 사용하여 KSVLA Light Agent에서 KES Light Agent로 정책 및 작업을 마이그레이션(관리 콘솔(MMC)에서만 사용 가능)합니다.

      결과적으로 *<정책>(변환됨)* 이름으로 새 정책이 생성됩니다. *<작업명>(변환됨)* 이름으로 새 KES 작업도 생성됩니다.

   2. Kaspersky Endpoint Agent의 마이그레이션 마법사를 사용하여 KEA에서 KES로 정책 및 작업 마이그레이션(웹 콘솔과 Cloud Console에서만 가능).

      이렇게 하면 *<Kaspersky Endpoint Security 정책명>* 및 *<Kaspersky Endpoint Agent 정책명>* 같은 이름의 새 정책이 생성됩니다. 새 작업과 KES 작업도 생성됩니다.

2. **KSVLA Light Agent에서 KES Light Agent로 마이그레이션**

KSVLA Light Agent에서 KES Light Agent로의 마이그레이션에는 KSVLA Light Agent 대신 KES Light Agent 설치가 포함됩니다.

관리자는 일반적으로 암호 보호를 사용하여 KSVLA Light Agent 및 KEA에 대한 접근을 제한합니다. *원격으로 애플리케이션 설치* 작업의 속성에서는 KEA 제거 암호만 입력할 수 있습니다. 마이그레이션을 위해서는 KSVLA Light Agent에 대한 암호 보호를 비활성화해야 합니다.

마이그레이션을 수행하려면 Detection and Response 솔루션을 지원하는데 필요한 구성 요소를 Kaspersky Endpoint Security의 구성 요소로 선택해야 합니다. 애플리케이션이 설치되면 Kaspersky Endpoint Security는 내장 에이전트를 사용하는 것으로 전환하고 Kaspersky Endpoint Agent를 제거합니다.

3 라이센싱 기능

애플리케이션이 Light Agent 모드에서 사용되는 경우에는 애플리케이션을 활성화할 필요가 없습니다. 애플리케이션을 활성화하려면 SVM에 라이센스 키를 추가해야 합니다. 또한 추가 기능(예: EDR Optimum)을 활성화하기 위한 라이센스 키를 SVM에 추가해야 합니다. 즉, 마이그레이션의 일부로 기능 라이센스가 자동으로 발생합니다.

4 Kaspersky Endpoint Detection and Response Optimum 및 Kaspersky Sandbox 상태 확인

업그레이드 후 Kaspersky Security Center에서 컴퓨터 상태가 *심각*으로 표시된다면:

- 컴퓨터에 Network Agent 버전 13.2 이상이 설치되었는지 확인합니다.
- *애플리케이션 구성 요소 상태 리포트*를 확인하여 내장 에이전트의 작동 상태를 확인합니다. 구성 요소의 상태가 *설치 안 됨*이라면 *애플리케이션 구성 요소 변경* 작업으로 구성 요소를 설치합니다.
- Kaspersky Endpoint Security for Windows의 새 정책에서 Kaspersky Security Network 진술문을 수락해야 합니다.
- *애플리케이션 구성 요소 상태 리포트*를 사용하여 EDR Optimum 기능을 활성화합니다. 구성 요소의 상태가 *라이센스에 포함되지 않음*이라면 EDR Optimum의 라이센스 키 자동 배포 기능이 켜졌는지 확인합니다.
- 가상 컴퓨터와 SVM의 연결 상태를 확인합니다. Light Agent의 SVM 연결 상태에 대한 정보는 Kaspersky Endpoint Security에서 또는 애플리케이션 명령을 사용하여 확인할 수 있습니다.

명령줄로 애플리케이션 관리

명령줄에서 Kaspersky Endpoint Security를 관리할 수 있습니다. `avp.com HELP` 명령을 실행하여 애플리케이션을 관리하기 위한 명령 목록을 볼 수 있습니다. 특정 명령의 구문을 읽으려면 `avp.com HELP <command>`을 입력합니다.

명령의 특수 문자에는 이스케이프 문자를 사용해야 합니다. `&`, `|`, `(`, `)`, `<`, `>`, `^`에 대한 이스케이프 문자는 `^` 문자입니다(예를 들어 `&` 문자를 사용하려면 `^&`를 입력합니다). `%`에 대한 이스케이프 문자는 `%%`입니다.

`1` 값을 대체하여 `yes`, `on`, `enable`, `enabled` 및 `true` 값을 사용할 수 있습니다. `0` 값을 대체하여 `no`, `off`, `disable`, `disabled` 및 `false` 값을 사용할 수 있습니다.

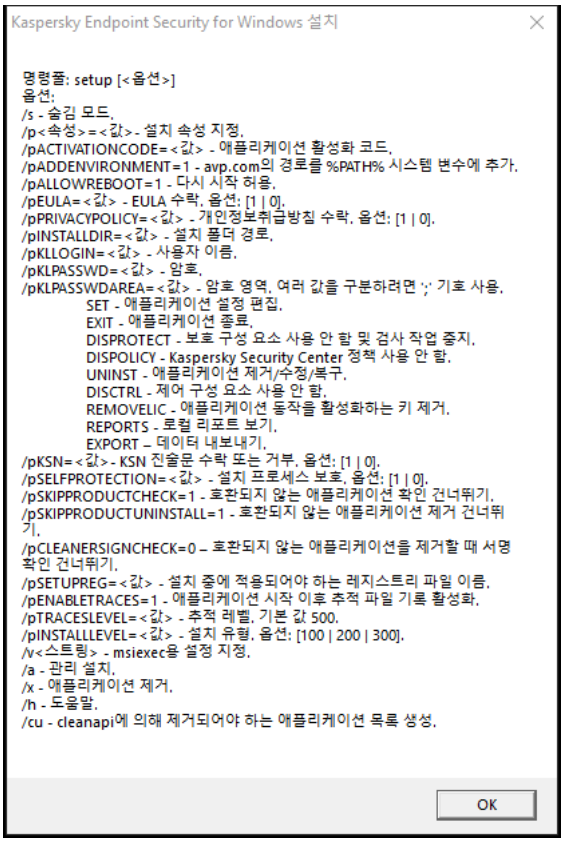
Setup. 애플리케이션 설치

다음 모드 중 하나를 사용해 명령줄로 Kaspersky Endpoint Security를 설치할 수 있습니다:

- 애플리케이션 설치 마법사 사용한 대화식 모드.
- 숨김 모드. 숨김 모드로 설치가 시작되면 사용자가 설치 과정에 관여할 필요가 없습니다(숨김 설치). 애플리케이션을 숨김 모드로 설치하려면 `/s` 및 `/qn` 키를 사용합니다.

  애플리케이션을 숨김 모드로 설치하기 전에 최종 사용자 라이센스 계약서와 개인정보 취급방침 전문을 읽어보십시오. 최종 사용자 라이센스 계약서와 개인정보 취급방침 전문은 Kaspersky Endpoint Security 배포 키트에 포함되어 있습니다. 최종 사용자 라이센스 계약서의 약관을 모두 읽고, 이해하고, 동의하며, 사용자의 데이터가 개인정보 취급방침에 따라(제3국 포함) 처리 및 전송된다는 점을 이해하고 동의하며, 개인정보 취급방침을 모두 읽고 이해하는 경우에만 애플리케이션 설치를 진행해야 합니다. 최종 사용자 라이센스 계약서의 약관과 개인정보 취급방침에 동의하지 않으면 Kaspersky Endpoint Security를 설치하거나 사용하지 마십시오.

/h 명령을 실행하여 애플리케이션을 설치하기 위한 명령 목록을 볼 수 있습니다. 설치 명령 구문에 관한 도움말을 가져오려면 setup_kes.exe /h를 입력합니다. 그러면 설치 프로그램에 명령 옵션 설명이 있는 창이 표시됩니다 (아래 그림 참조).



설치 명령 옵션 설명

애플리케이션을 설치하거나 이전 버전의 애플리케이션을 업그레이드하려면 다음과 같이 하십시오.

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 배포 패키지가 있는 폴더로 이동합니다.
3. 다음 명령을 실행합니다:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

또는

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

결과적으로 애플리케이션이 컴퓨터에 설치됩니다. status 명령을 사용하여 애플리케이션이 설치되었는지 확인하고 애플리케이션 설정을 확인할 수 있습니다.

`EULA=1`	최종 사용자 라이센스 계약서 조건 동의. 라이센스 계약서는 Kaspersky Endpoint Security 배포 키트에 포함되어 있습니다. 애플리케이션을 설치하거나 애플리케이션 버전을 업데이트하려면 최종 사용자 라이센스 계약서 조건에 동의해야 합니다.
`PRIVACYPOLICY=1`	개인정보취급방침에 동의함. 개인정보취급방침 전문은 Kaspersky Endpoint Security 배포 키트에 포함되어 있습니다. 애플리케이션을 설치하거나 애플리케이션 버전을 업그레이드하려면 개인정보취급방침에 동의해야 합니다.
`KSN`	Kaspersky Security Network(KSN) 참여 동의 또는 거부. 이 파라미터에 대해 값을 설정하지 않으면, Kaspersky Endpoint Security 처음 시작 시 Kaspersky Endpoint Security에서 KSN 참여에 대한 사용자의 동의 또는 거부를 확인하는 메시지가 표시됩니다. 사용 가능한 값: • `1` – KSN 참가 동의 • `0` - KSN 참가 거부(기본값) Kaspersky Endpoint Security 배포 패키지는 Kaspersky Security Network와 함께 사용할 수 있도록 최적화되었습니다. Kaspersky Security Network에 참여하지 않기로 선택한 경우에는 설치가 완료된 후 Kaspersky Endpoint Security를 즉시 업데이트해야 합니다.
`CONFIGPATH=<path to the configuration file>`	사전 정의된 설정을 사용하여 애플리케이션 설치. 이렇게 하려면 Kaspersky Endpoint Security의 설정을 정의하는 파일을 업로드해야 합니다. 애플리케이션의 로컬 인터페이스에서 구성 파일을 생성할 수 있습니다.
`ALLOWREBOOT=1`	애플리케이션을 설치하거나 업그레이드한 후 필요시 컴퓨터를 자동으로 다시 시작합니다. 이 파라미터에 대해 설정된 값이 없으면 자동 컴퓨터 다시 시작이 차단됩니다. Kaspersky Endpoint Security를 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.
`SKIPPRODUCTCHECK=1`	설치된 소프트웨어 검사를 비활성화합니다. 호환성 문제를 유발할 수 있는 소프트웨어 목록은 배포 키트에 포함된 incompatible.txt 파일에서 이용 가능합니다. 이 파라미터에 대해 설정된 값이 없고, 목록에 있는 소프트웨어가 탐지되면 Kaspersky Endpoint Security 설치가 종료됩니다.
`SKIPPRODUCTUNINSTALL=1`	incompatible.txt 목록에서 탐지된 소프트웨어의 자동 제거를 비활성화합니다. 이 파라미터에 대해 설정된 값이 없으면 Kaspersky Endpoint Security에서 호환성 문제를 유발할 수 있는 소프트웨어를 제거하려고 시도합니다. msiexec 설치 프로그램으로 Kaspersky Endpoint Security 설치 시에는 소프트웨어 자동 제거를 활성화할 수 없습니다. 호환성 문제를 유발할 수 있는 소프트웨어를 자동으로 제거하려면 setup_kes.exe 파일을 사용합니다.
`CLEANERSIGNCHECK=0|1`	incompatible.txt 목록에서 탐지된 소프트웨어 파일의 디지털 서명을 확인합니다. 소프트웨어 제거를 위해 Kaspersky Endpoint Security는 소프트웨어 설치 프로그램 파일을 실행합니다. 설치 프로그램 파일에 디지털 서명이 없을 시, Kaspersky Endpoint Security는 해당 파일을 신뢰할 수 없는 것으로 간주하고 소프트웨어 제거를 중단하여 잠재적 악성 코드 실행을 방지합니다. 애플리케이션이 탐지된 소프트웨어 파일의 디지털 서명을 확인할 수 없을 시, Kaspersky Endpoint Security 설치가 오류와 함께 중지됩니다. 기본값은 소프트웨어 설치 방법에 따라 다릅니다: • `0`은 디지털 서명 확인이 비활성화되었음을 의미합니다(Kaspersky Security Center로 배포 시 기본값). • `1`은 디지털 서명 확인이 활성화되었음을 의미합니다(애플리케이션을 로컬에 설치 시 기본값).
`STANDALONEMODE=1`	Kaspersky Endpoint Detection and Response(KATA) 또는 Kaspersky Endpoint Detection and Response Expert(on-premise) 솔루션과의 통합을 위해 Endpoint Detection and Response Agent(EDR Agent) 구성에 애플리케이션 설치. 조직에 타사 Endpoint Protection Platform(EPP)가 Kaspersky Endpoint Detection and Response 클래스 솔루션과 함께 설치된 경우 이 구성이 필요합니다. 이를 통해 Endpoint Detection and Response Agent 구성의 Kaspersky Endpoint Security가 타사 EPP 애플리케이션과 호환됩니다.
`KLLOGIN`	Kaspersky Endpoint Security의 기능 및 설정에 접근하기 위한 사용자 이름 설정(암호 보호 구성 요소). 사용자 이름은 `KLPASSWD` 및 `KLPASSWDAREA` 설정과 함께 설정됩니다. KLAdmin 사용자 이름이 기본값으로 사용됩니다.
`KLPASSWD`	Kaspersky Endpoint Security 기능 및 설정에 접근하기 위한 암호를 지정합니다(암호와 함께 `KLLOGIN` 및 `KLPASSWDAREA` 파라미터 지정). 암호를 지정했지만 `KLLOGIN` 변수와 함께 사용자 이름을 지정하지 않은 경우 KLAdmin 사용자 이름이 기본적으로 사용됩니다.

KLPASSWDAREA	Kaspersky Endpoint Security에 접근하기 위한 암호 적용 영역을 지정합니다. 사용자가 이 범위에 포함된 동작을 수행하려고 하면 Kaspersky Endpoint Security에서 사용자의 계정 정보(KLLOGIN 및 KLPASSWD 파라미터)를 묻는 메시지를 표시합니다. 여러 값을 지정하려면 ; 문자를 사용합니다. 사용 가능한 값: • SET – 애플리케이션 설정 수정 • EXIT – 애플리케이션 종료 • DISPROTECT - 보호 구성 요소 및 검사 작업 중지 • DISPOLICY - Kaspersky Security Center 정책 사용 안 함 • UNINST - 목록에서 애플리케이션 제거 • DISCTRL – 제어 구성 요소 중지 • REMOVELIC – 키 제거 • REPORTS – 리포트 보기 • EXPORT – 애플리케이션 설정 내보내기. 예: KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. KLAdmin 계정에는 암호로 보호된 작업을 수행할 수 있는 권한이 있습니다. 따라서 KLAdmin 계정의 암호 적용 범위는 구성할 수 없습니다. KLAdmin 계정의 암호 적용 범위를 구성하려고 하면 애플리케이션은 "Everyone" 그룹에 대해 지정된 동작을 금지합니다.
PROTECTOSSERVICES	운영 체제 서비스 보호 기능입니다. 운영 체제 서비스 보호는 타사 애플리케이션이 운영 체제 서비스의 작동을 방해하는 것을 방지합니다. 예를 들어, 애플리케이션 자동 시작 서비스가 이러한 서비스에 포함됩니다. • 1은 운영 체제 서비스 보호가 활성화되었음을 의미합니다(기본값). • 0은 운영 체제 서비스 보호가 비활성화되었음을 의미합니다.
ENABLETRACES	애플리케이션 추적 로그 활성화 또는 비활성화. Kaspersky Endpoint Security가 시작된 후 %ProgramData%\Kaspersky Lab\KES.14.0\Traces 폴더에 추적 파일을 저장합니다. 사용 가능한 값: • 1 - 추적 로그 활성화됨 • 0 – 추적 로그 비활성화됨(기본값)
TRACESLEVEL	추적로그 기록 레벨. 사용 가능한 값: • 100(심각). 치명적인 오류에 대한 메시지만 기록. • 200(높음). 치명적인 오류를 포함한 모든 오류에 대한 메시지 기록. • 300(진단). 모든 오류와 경고에 대한 메시지 기록. • 400(중요). 모든 오류, 경고 및 추가 정보 메시지 기록. • 500(일반). 모든 오류 및 경고에 대한 메시지뿐만 아니라 일반 모드에서 애플리케이션의 작동에 대한 자세한 정보도 제공합니다(기본값). • 600(낮음). 모든 메시지.
ENABLEAZURESUPPORT	Azure WVD 호환성 모드 활성화 또는 비활성화. 사용 가능한 값: • 1 – Azure WVD 호환성 모드가 활성화됩니다. • 0 – Azure WVD 호환성 모드가 비활성화됩니다(기본값). 이 기능을 사용하면 Kaspersky Anti Targeted Attack Platform 콘솔에서 Azure 가상 컴퓨터 상태가 올바르게 표시됩니다. 컴퓨터의 성능을 모니터링하기 위해 Kaspersky Endpoint Security는 원격 측정을 KATA 서버로 보냅니다. 원격 측정은 컴퓨터의 ID(Sensor ID)가 포함되어 있습니다. Azure WVD 호환성 모드를 사용하면 이러한 가상 컴퓨터에 영구적인 고유 Sensor ID를 할당할 수 있습니다. 호환성 모드가 꺼져 있으면 Azure 가상 컴퓨터의 작동 방식 때문에 컴퓨터를 다시 시작한 후 Sensor ID가 변경될 수 있습니다. 이로 인해 가상 컴퓨터의 복제본이 콘솔에 나타날 수 있습니다.
AMPPL	AM-PPL(Antimalware Protected Process Light) 기술을 사용한 Kaspersky Endpoint Security 프로세스 보호를 작동하거나 중지합니다. AM-PPL 기술에 대한 자세한 내용은 Microsoft 웹사이트를 방문하시기 바랍니다. AM-PPL 기술은 Windows 10 1703(RS2) 버전 이상 및 Windows Server 2019 운영 체제에서 사용할 수 있습니다. 사용 가능한 값: • 1 - AM-PPL 기술을 사용한 Kaspersky Endpoint Security 프로세스 보호가 작동됩니다. • 0 - AM-PPL 기술을 사용한 Kaspersky Endpoint Security 프로세스 보호가 중지됩니다.
UPGRADEMODE	애플리케이션 업그레이드 모드: • Seamless는 컴퓨터 다시 시작을 포함하는 애플리케이션 업그레이드를 말합니다(기본값). • Force는 다시 시작 없는 애플리케이션 업그레이드를 말합니다. 11.10.0 버전부터 다시 시작 없이 애플리케이션을 업그레이드할 수 있습니다. 이전 버전의 애플리케이션을 업그레이드하려면, 컴퓨터를 다시 시작해야 합니다. 11.11.0 버전부터는 다시 시작 없이도 패치를 설치할 수 있습니다. Kaspersky Endpoint Security를 설치할 때 다시 시작할 필요가 없습니다. 즉, 애플리케이션 설정에서 애플리케이션의 업그레이드 모드를 지정합니다. 애플리케이션 설정 또는 정책에서 이 매개변수를 변경할 수 있습니다. 이미 설치된 애플리케이션을 업그레이드 시, 명령줄 매개 변수의 우선순위는 애플리케이션 설정 또는 setup.ini 파일에 지정된 매개 변수보다 낮습니다. 예를 들어 명령줄에서 Force 업그레이드 모드를 지정하고 애플리케이션 설정에서 Seamless 모드를 지정하면 컴퓨터를 다시 시작할 때 업그레이드가 설치됩니다(Seamless).

RESTAPI	REST API를 통해 애플리케이션을 관리합니다. REST API를 통해 애플리케이션을 관리하려면 사용자 이름(RESTAPI_User 파라미터)을 지정해야 합니다. 사용 가능한 값: • 1 – REST API를 통한 관리가 가능합니다. • 0 – REST API를 통한 관리가 차단됩니다(기본값). REST API를 통해 애플리케이션을 관리하려면 관리 시스템을 사용한 관리가 허용되어야 합니다. 이렇게 하려면 AdminKitConnector=1 파라미터를 설정합니다. REST API를 통해 애플리케이션을 관리하면 Kaspersky의 관리 시스템을 사용하여 애플리케이션을 관리할 수 없습니다.
RESTAPI_User	Windows 도메인 계정은 REST API로 애플리케이션을 관리하기 위해 사용되는 사용자 이름입니다. REST API를 통한 애플리케이션 관리는 이 사용자만 이용할 수 있습니다. 사용자 이름을 <DOMAIN>\<UserName> 형식으로 입력합니다(예: RESTAPI_User=COMPANY\Administrator). REST API로 작업할 사용자를 하나만 선택할 수 있습니다. REST API를 통해 애플리케이션을 관리하기 위해서는 사용자 이름을 추가해야 합니다.
RESTAPI_Port	REST API를 통해 애플리케이션을 관리하는 데 사용되는 포트입니다. 기본적으로 포트 6782가 사용됩니다. 포트가 사용 가능한 상태인지 확인하십시오.
RESTAPI_Certificate	요청 식별을 위한 인증서(예: RESTAPI_Certificate=C:\cert.pem). Kaspersky Endpoint Security와 REST 클라이언트의 안전한 상호 작용을 위해서는 요청 식별을 구성해야 합니다. 이렇게 하려면 인증서를 설치한 다음 각 요청의 페이로드에 서명해야 합니다.
ADMINKITCONNECTOR	관리 시스템을 사용하여 애플리케이션을 관리합니다. 예를 들어 관리 시스템에는 Kaspersky Security Center가 포함됩니다. Kaspersky 관리 시스템 외에도 타사 솔루션을 사용할 수 있습니다. Kaspersky Endpoint Security는 이러한 용도로 API를 제공합니다. 사용 가능한 값: • 1 – 관리 시스템의 도움을 받아 애플리케이션을 관리할 수 있습니다(기본값). • 0 – 로컬 인터페이스를 통해서만 애플리케이션 관리가 가능합니다.
EnableUniqueSensorID	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. 이 알고리즘은 고유한 Sensor ID를 보장합니다. 기본적으로 이 매개변수는 설정되어 있지 않습니다. 애플리케이션은 다음과 같은 경우에 Sensor ID를 상속합니다: • 애플리케이션 버전 업데이트 • [KES+KEA] 구성을 [KES+내장 에이전트] 구성으로 마이그레이션 애플리케이션 복구의 일부로 설치 프로그램은 Sensor ID 상속을 시도합니다. Sensor ID를 복원할 수 없는 경우, 애플리케이션이 새로운 Sensor ID를 생성합니다.
SKIPKB5007186CHECK=1	설치된 운영 체제 업데이트 KB5007186에 대한 확인을 비활성화합니다. 애플리케이션을 설치하기 전에 설치 프로그램은 설치된 운영 체제 업데이트를 확인합니다. KB5007186 업데이트는 애플리케이션에 문제를 일으킬 수 있는 운영 체제 업데이트 목록에 있습니다. 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오. 따라서 설치 프로그램은 이 업데이트가 발견되면 설치를 중단합니다. 설치를 계속하려면 SKIPKB5007186CHECK=1 을 설정하십시오.

예

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Kaspersky Endpoint Security를 설치한 후에는 체험판 라이센스가 활성화됩니다. 단, setup.ini 파일에 활성화 코드를 제공해야 합니다. 체험판 라이센스는 보통 사용 기간이 짧습니다. 체험판 라이센스가 만료되면 모든 Kaspersky Endpoint Security 기능이 중지됩니다. 애플리케이션을 계속 사용하려면 애플리케이션 활성화 마법사 또는 특수 명령을 통해 상업용 라이센스를 사용하여 애플리케이션을 활성화해야 합니다.

자동 모드에서 애플리케이션을 설치 또는 버전 업그레이드를 할 때 다음 파일을 사용할 수 있습니다:

- setup.ini – 애플리케이션 설치를 위한 일반 설정

  setup.ini 파일의 설정을 적용하려면 이 파일을 Kaspersky Endpoint Security 배포 패키지가 들어 있는 폴더에 넣습니다.

- install.cfg – Kaspersky Endpoint Security 동작 설정

  install.cfg 구성 파일의 설정을 적용하려면 다음 애플리케이션 설치 명령으로 파일 경로를 지정해야 합니다: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – 레지스트리 키.

  setup.ini 파일의 `SetupReg` 파라미터에 대한 `setup.reg` 값을 설정해야 setup.reg 파일의 레지스트리 키가 레지스트리에 기록됩니다. setup.reg 파일은 Kaspersky 전문가가 생성합니다. 이 파일의 내용은 수정하지 않는 것이 좋습니다. setup.reg 파일의 설정을 적용하려면 이 파일을 Kaspersky Endpoint Security 배포 패키지가 들어 있는 폴더에 넣습니다. setup.reg 파일을 다른 폴더에 저장할 수도 있습니다. 이렇게 하려면 다음 애플리케이션 설치 명령으로 파일 경로를 지정해야합니다: `SETUPREG=<path to the setup.reg file>`.

Setup /x. 애플리케이션 제거

다음 방법 중 하나를 사용해 명령줄로 Kaspersky Endpoint Security를 제거할 수 있습니다:

- 애플리케이션 설치 마법사 사용한 대화식 모드.
- 숨김 모드. 숨김 모드로 제거가 시작되면 사용자가 제거 과정에 관여할 필요가 없습니다(숨김 제거). 애플리케이션을 숨김 모드로 제거하려면 `/s` 및 `/qn` 키를 사용합니다.

애플리케이션을 숨김 모드로 제거하려면 다음과 같이 하십시오.

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 배포 패키지가 있는 폴더로 이동합니다.
3. 다음 명령을 실행합니다:

   - 제거 프로세스가 암호로 보호되지 않은 경우:

     ```
     setup_kes.exe /s /x
     ```

     또는

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>`는 애플리케이션의 고유 식별자입니다. 다음 명령을 사용하여 T기술 지원 기술 자료 웹사이트에서 애플리케이션의 GUID를 찾을 수 있습니다.

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

- 제거 프로세스가 암호로 보호되는 경우:

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

또는

```
msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
```

SAVEQB 파라미터를 사용하여 애플리케이션에서 스캔하고 백업에 추가된 파일을 저장할 수도 있습니다. 파일의 백업 복사본은 C:\ProgramData\Kaspersky Lab\KES.14.0\QB 폴더에 저장됩니다. 기본적으로 백업에 파일을 저장하는 것은 비활성화되어 있습니다(SAVEQB=0).

예

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. 애플리케이션 복구

복구 시 애플리케이션은 손상된 모든 애플리케이션 모듈과 애플리케이션 설치 프로세스의 일부로 생성된 시스템 레지스트리 키의 무결성을 확인하고 복원합니다.

다음 모드 중 하나를 사용해 명령줄로 Kaspersky Endpoint Security를 복구할 수 있습니다:

- 애플리케이션 설치 마법사 사용한 대화식 모드.
- 숨김 모드. 숨김 모드로 복구를 시작하면, 사용자가 복구 프로세스에 관여할 필요가 없습니다.

Kaspersky Endpoint Security 설치 프로그램이 복구 모드로 실행 중이고 애플리케이션에 복구가 필요하지 않다면, 설치 프로그램이 아무것도 바꾸지 않습니다.

Kaspersky Endpoint Security 설치 프로그램이 복구 모드로 실행 중이고 애플리케이션이 설치되어 있지 않다면, 설치 프로그램이 설치 프로세스를 시작합니다.

애플리케이션을 숨김 모드로 복구하려면:

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 배포 패키지가 있는 폴더로 이동합니다.

3. 다음 명령을 실행합니다:

- 복구 프로세스가 암호로 보호되지 않았다면:

```
msiexec.exe /i <GUID> REINSTALL=ALL /qn
```

<GUID>는 애플리케이션의 고유 식별자입니다. 다음 명령을 사용하여 T기술 지원 기술 자료 웹사이트에서 애플리케이션의 GUID를 찾을 수 있습니다.

```
wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
```

- 복구 프로세스가 암호로 보호되었다면:

```
msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
```

예

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

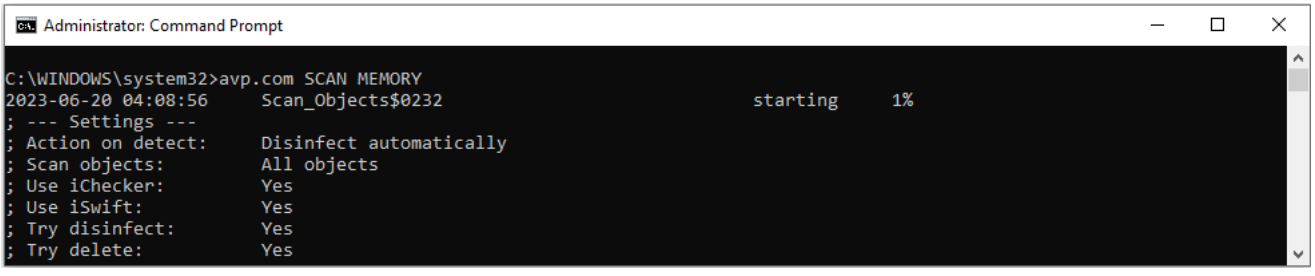
AVP 명령

명령줄에서 Kaspersky Endpoint Security를 관리하려면 다음을 수행합니다.

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.
   애플리케이션 설치 중에 %PATH% 시스템 변수에 실행 파일의 경로를 추가할 수 있습니다.
3. 다음 템플릿을 사용하여 명령을 실행합니다.

```
avp.com <command> [options]
```

그러면 Kaspersky Endpoint Security는 명령을 실행합니다(다음 그림 참조).



명령줄로 애플리케이션 관리

SCAN. 악성 코드 검사

악성 코드 검사 작업 실행.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

검사 범위	
`<files to scan>`	공백으로 구분된 파일 및 폴더 목록. 긴 경로는 따옴표로 묶어야 합니다. 짧은 경로(MS-DOS 형식)는 따옴표로 묶을 필요가 없습니다. 예: • `"C:\Program Files (x86)\Example Folder"` – 긴 경로 • `C:\PROGRA~2\EXAMPL~1` – 짧은 경로
`/ALL`	*악성 코드 검사* 작업을 실행합니다. Kaspersky Endpoint Security는 다음과 같은 개체를 검사합니다: • 커널 메모리 • 운영 체제를 시작할 때 로드되는 개체 • 부트 섹터 • 운영 체제 백업 • 모든 하드 및 이동식 드라이브 Kaspersky Endpoint Security for Windows 12.12에서는 이메일은 애플리케이션 검사 범위에서 제외됩니다. 수신 및 발신되는 이메일 메시지의 검사는 메일 위협 보호 구성 요소에서 수행합니다. 이전 버전의 관리 플러그인을 사용하는 경우 애플리케이션은 정책에 포함되어 있더라도 이메일을 검사 범위에서 제외합니다.
`/MEMORY`	커널 메모리 검사
`/STARTUP`	운영 체제를 시작할 때 로드되는 개체 검사
`/REMDRIVES`	이동식 드라이브 검사
`/FIXDRIVES`	하드 드라이브 검사
`/NETDRIVES`	네트워크 드라이브 검사
`/QUARANTINE`	Kaspersky Endpoint Security 백업 저장소에 있는 파일 검사.
`/@:<file list.lst>`	목록에서 파일 및 폴더를 검사합니다. 목록의 각 파일은 새 행에서 입력해야 합니다. 긴 경로는 따옴표로 묶어야 합니다. 짧은 경로(MS-DOS 형식)는 따옴표로 묶을 필요가 없습니다. 예: • `"C:\Program Files (x86)\Example Folder"` – 긴 경로 • `C:\PROGRA~2\EXAMPL~1` – 짧은 경로

위협 탐지 시 처리 방법	
`/i0`	**알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 감염된 파일에 대한 정보를 해당 파일 탐지 시 처리 안 된 위협 목록에 추가합니다.
`/i1`	**치료 - 불가능한 경우 알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 탐지된 모든 감염을 자동으로 치료합니다. 치료 실패 시 Kaspersky Endpoint Security는 탐지된 감염 파일에 대한 정보를 처리 안 된 위협 목록에 추가합니다.

`/i2`	**치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다. 이 처리 방법은 기본적으로 선택되어 있습니다.
`/i3`	**치료 불가능한 경우 삭제**. 또한, 감염된 파일을 치료 또는 삭제할 수 없다면 복합 파일(예, 압축 파일)은 삭제합니다.
`/i4`	**삭제**. 또한, 감염된 파일을 삭제할 수 없다면 복합 파일(예, 압축 파일)은 삭제합니다.

파일 유형	
`/fe`	**확장자에 따라 검사한 파일** 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일 형식은 파일 확장자를 기반으로 결정됩니다.
`/fi`	**형식에 따라 검사한 파일**. 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일에 악성 코드가 있는지 검사하기 전에 파일의 내부 헤더를 분석하여 파일 형식을 결정합니다(예: txt, .doc 또는 .exe). 또한 이 검사에서는 특정 파일 확장자를 가진 파일도 찾습니다.
`/fa`	**모든 파일**. 이 설정을 사용하면 애플리케이션이 예외 없이 모든 형식과 확장자의 파일을 검사합니다. 기본 설정입니다.

검사 예외	
`-e:a`	RAR, ARJ, ZIP, CAB, LHA, JAR, ICE 압축 파일은 검사 범위에서 제외됩니다.
`-e:<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.
`-e:<seconds>`	지정된 시간 제한(초)보다 검사하는 데 오래 걸리는 파일은 검사 범위에서 제외됩니다.
`-es:<megabytes>`	지정된 크기 제한(MB)보다 큰 파일은 검사 범위에서 제외됩니다.

이벤트를 리포트 파일 모드로 저장(검사, 업데이터, 롤백 프로필 전용)	
`/R:<report file>`	심각한 이벤트만 리포트 파일에 저장합니다.
`/RA:<report file>`	모든 이벤트를 리포트 파일에 저장합니다.

검사 기술	
`/iChecker=on|off`	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.
`/iSwift=on|off`	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.

고급 설정	
`/C:<file with scan settings>`	*악성 코드 검사* 작업 설정을 가진 파일입니다. 파일을 직접 생성하고 TXT 형식으로 저장해야 합니다. 파일은 다음 내용을 가질 수 있습니다: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

예

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트

데이터베이스 및 애플리케이션 모듈 업데이트 작업 실행.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

애플리케이션을 Light Agent 모드로 설치했다면 이 명령을 실행할 수 없습니다.

명령 구문

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

업데이트 작업 설정	
`local`	애플리케이션 설치 후 자동으로 생성된 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업의 시작. 로컬 애플리케이션 인터페이스 또는 Kaspersky Security Center 콘솔에서 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업의 설정을 변경할 수 있습니다. 이 설정을 구성하지 않으면 Kaspersky Endpoint Security는 기본 설정 또는 명령에 지정된 설정으로 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 시작합니다. *데이터베이스 및 애플리케이션 모듈 업데이트* 작업 설정은 다음과 같이 구성할 수 있습니다: • `UPDATE`는 기본 설정(업데이트 경로는 Kaspersky 업데이트 서버, 계정은 System 등)으로 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 시작합니다. • `UPDATE local`은 설치 후 자동으로 생성된 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 시작합니다(미리 정의된 작업). • `UPDATE <update settings>`은 직접 정의한 설정에 따라 *데이터베이스 및 애플리케이션 모듈 업데이트* 작업을 시작합니다(아래를 참조하십시오).

업데이트 경로	
`"<update source>"`	HTTP 또는 FTP 서버의 주소 또는 업데이트 패키지가 있는 공유 폴더의 주소입니다. 하나의 업데이트 경로만 지정할 수 있습니다. 업데이트 경로를 지정하지 않으면 Kaspersky Endpoint Security는 기본 경로인 Kaspersky 업데이트 서버를 사용합니다.

이벤트를 리포트 파일 모드로 저장(검사, 업데이터, 롤백 프로필 전용)	
`/R:<report file>`	심각한 이벤트만 리포트 파일에 저장합니다.
`/RA:<report file>`	모든 이벤트를 리포트 파일에 저장합니다.

고급 설정	
`/C:<file with update settings>`	*데이터베이스 및 애플리케이션 모듈 업데이트* 작업 설정이 있는 파일입니다. 파일을 직접 생성하고 TXT 형식으로 저장해야 합니다. 파일은 다음 내용을 가질 수 있습니다: `["<update source>"] [/R[A]:<report file>]`.

예

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. 마지막 업데이트 롤백

마지막 안티 바이러스 데이터베이스 업데이트를 롤백합니다. 이렇게 하면 새 데이터베이스 버전에 잘못된 서명이 포함되어 있어 Kaspersky Endpoint Security가 안전한 애플리케이션을 차단하는 경우 등과 같이 필요 시에 데이터베이스 및 애플리케이션 모듈을 이전 버전으로 롤백할 수 있습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

애플리케이션을 Light Agent 모드로 설치했다면 이 명령을 실행할 수 없습니다.

명령 구문

```
avp.com ROLLBACK [/R[A]:<report file>]
```

이벤트를 리포트 파일 모드로 저장(검사, 업데이터, 롤백 프로필 전용)	
`/R:<report file>`	심각한 이벤트만 리포트 파일에 저장합니다.
`/RA:<report file>`	모든 이벤트를 리포트 파일에 저장합니다.

예

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. 추적 로그

추적 파일은 애플리케이션이 사용 중일 때는 컴퓨터에 저장되며 애플리케이션이 제거되면 영구적으로 삭제됩니다. 인증 에이전트의 추적 파일을 제외한 추적 로그 파일은 `%ProgramData%\Kaspersky Lab\KES.14.0\Traces` 폴더에 저장됩니다. 기본적으로 추적 로그는 비활성화되어 있습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

추적 로그 레벨	
`<tracing level>`	추적로그 기록 레벨. 사용 가능한 값: • `100`(심각). 치명적인 오류에 대한 메시지만 기록. • `200`(높음). 치명적인 오류를 포함한 모든 오류에 대한 메시지 기록. • `300`(진단). 모든 오류와 경고에 대한 메시지 기록. • `400`(중요). 모든 오류, 경고 및 추가 정보 메시지 기록. • `500`(일반). 모든 오류 및 경고에 대한 메시지뿐만 아니라 일반 모드에서 애플리케이션의 작동에 대한 자세한 정보도 제공합니다(기본값). • `600`(낮음). 모든 메시지.

고급 설정	
`all`	`file` 및 `mem` 파라미터로 명령을 실행합니다.
`file`	하나의 추적 파일을 저장합니다(크기 제한 없음).
`rot`	제한된 크기의 파일 세트에 추적 로그를 저장하고 최대 크기에 도달하면 이전 파일을 덮어씁니다.
`mem`	추적 로그를 덤프 파일에 저장합니다.

예

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. 프로필 시작

프로필을 시작합니다(예: 데이터베이스 업데이트 시작 또는 보호 구성 요소 활성화).

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com START <profile> [/R[A]:<report file>]
```

프로필	
<profile>	프로필 이름입니다. *프로필*은 Kaspersky Endpoint Security 구성 요소, 작업 또는 기능입니다. `HELP START` 명령을 실행하여 사용 가능한 프로필 목록을 볼 수 있습니다.

이벤트를 리포트 파일 모드로 저장(검사, 업데이터, 롤백 프로필 전용)	
/R:<report file>	심각한 이벤트만 리포트 파일에 저장합니다.
/RA:<report file>	모든 이벤트를 리포트 파일에 저장합니다.

예

```
avp.com START Scan_Objects
```

STOP. 프로필 중지

프로필 실행을 중지합니다(예: 이동식 드라이브 검사 중지 또는 보호 구성 요소 비활성화).

이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다. 사용자는 **보호 구성 요소 비활성화** 및 **제어 구성 요소 비활성화** 권한이 있어야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

프로필	
`<profile>`	프로필 이름입니다. *프로필*은 Kaspersky Endpoint Security 구성 요소, 작업 또는 기능입니다. `HELP STOP` 명령을 실행하여 사용 가능한 프로필 목록을 볼 수 있습니다.

인증	
`/login=<user name> /password=<password>`	필요한 암호 보호 권한이 있는 사용자 계정 정보

STATUS. 프로필 상태

애플리케이션 프로필(예: `running` 또는 `completed`)의 상태 정보를 표시합니다. `HELP STATUS` 명령을 실행하여 사용 가능한 프로필 목록을 볼 수 있습니다.

또한 Kaspersky Endpoint Security는 서비스 프로필 상태에 대한 정보도 표시합니다. Kaspersky 기술 지원에 문의할 때 서비스 프로필 상태 정보가 필요할 수 있습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com STATUS [<profile>]
```

프로필 없이 명령을 입력하면 Kaspersky Endpoint Security가 애플리케이션에 있는 모든 프로필의 상태를 표시합니다.

STATISTICS. 프로필 동작 통계

애플리케이션 프로필에 대한 통계를 표시합니다(예: 검사 기간 또는 탐지된 위협 수). `HELP STATISTICS` 명령을 실행하여 사용 가능한 프로필 목록을 볼 수 있습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com STATISTICS <profile>
```

RESTORE. 백업 저장소에서 파일 복원

백업에서 파일을 원래 폴더로 복원합니다. 지정된 경로에 동일한 이름의 파일이 이미 있는 경우, 애플리케이션이 파일을 교체할지 여부를 묻습니다. 복원 중인 파일이 복사되어 원래 이름을 유지합니다.

이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다. 해당 사용자에게 **백업에서 복원** 권한이 있어야 합니다.

*백업*은 치료하는 동안 삭제되거나 수정된 파일의 백업 복사본을 보존합니다. *백업 복사본*은 파일을 치료 또는 삭제하기 전에 생성되는 파일 복사본입니다. 파일의 백업 복사본은 특별한 형식으로 저장되며 위험하지 않습니다.

파일의 백업 복사본은 `C:\ProgramData\Kaspersky Lab\KES.14.0\QB` 폴더에 저장됩니다.

관리자 그룹 내 사용자는 이 폴더에 대한 접근 권한이 부여됩니다. Kaspersky Endpoint Security를 설치할 때 사용된 계정의 사용자는 이 폴더에 대한 제한된 접근 권한이 부여됩니다.

Kaspersky Endpoint Security는 파일의 백업 복사본에 대한 사용자 접근 권한을 구성하는 기능을 제공하지 않습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

고급 설정	
`/REPLACE`	기존 파일 덮어쓰기
`<file name>`	복원될 파일의 이름

인증	
`/login=<user name> /password=<password>`	필요한 암호 보호 권한이 있는 사용자 계정 정보

예

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. 애플리케이션 설정 내보내기

Kaspersky Endpoint Security 설정을 파일로 내보내기. 명령에 설정을 내보낼 파일의 이름만 포함된 경우, 애플리케이션은 다음과 같이 파일을 배치합니다:

- avp.com의 경로를 %PATH% 시스템 변수에 추가하면 애플리케이션이 `C:\Windows\SysWOW64` 폴더 내에 파일을 배치합니다.
- 애플리케이션 설치 폴더에서 명령을 실행하면 애플리케이션의 자체 보호가 애플리케이션 폴더에 새 파일의 생성을 차단하기 때문에 내보내기에 실패합니다. 애플리케이션 설정을 파일로 내보내려면 파일 경로를 입력합니다.

이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다. 해당 사용자에게 **설정 내보내기** 권한이 있어야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

프로필	
<profile>	프로필 이름입니다. *프로필*은 Kaspersky Endpoint Security 구성 요소, 작업 또는 기능입니다. HELP EXPORT 명령을 실행하여 사용 가능한 프로필 목록을 볼 수 있습니다.

내보낼 파일	
<file name>	애플리케이션 설정을 내보낼 파일의 이름입니다. 파일 경로를 입력할 수도 있습니다. DAT 또는 CFG 구성 파일, TXT 텍스트 파일 또는 XML 문서로 Kaspersky Endpoint Security 설정을 내보낼 수 있습니다.

인증	
/login=<user name> /password=<password>	필요한 암호 보호 권한이 있는 사용자 계정 정보

예

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. 애플리케이션 설정 가져오기

EXPORT 명령으로 생성된 파일에서 Kaspersky Endpoint Security 설정을 가져옵니다.

이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다. 해당 사용자에게 **애플리케이션 설정 구성** 권한이 있어야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

가져올 파일	
<file name>	애플리케이션 설정을 가져올 파일의 이름입니다. DAT 또는 CFG 구성 파일, TXT 텍스트 파일 또는 XML 문서에서 Kaspersky Endpoint Security 설정을 가져올 수 있습니다.

인증	
/login=<user name> /password=<password>	필요한 암호 보호 권한이 있는 사용자 계정 정보

예

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. 키 파일 적용

키 파일을 사용하여 Kaspersky Endpoint Security를 활성화합니다. 애플리케이션이 이미 활성화된 경우 이 키는 예약 키로 추가됩니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

애플리케이션을 Light Agent 모드로 설치했다면 이 명령을 실행할 수 없습니다.

명령 구문

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

키 파일	
<file name>	키 파일 이름

인증	
/login=<user name> /password=<password>	사용자 계정 인증. 이러한 인증은 암호 보호가 설정된 경우에만 입력해야 합니다.

예

```
avp.com ADDKEY file.key
```

LICENSE. 라이센스

Kaspersky Endpoint Security, EDR Optimum 또는 EDR Expert(Kaspersky Endpoint Detection and Response 애드온)의 라이센스 키를 관리합니다.

이 명령을 실행하고 라이센스 키를 제거하려면 암호 보호를 사용하도록 설정해야 합니다. 해당 사용자에게 **키 제거** 권한이 있어야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

애플리케이션을 Light Agent 모드로 설치했다면 이 명령을 실행할 수 없습니다.

명령 구문

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

동작	
/ADD <file name>	키 파일을 사용하여 Kaspersky Endpoint Security를 활성화합니다. 애플리케이션이 이미 활성화된 경우 이 키는 예약 키로 추가됩니다.
/ADD <activation code>	활성화 코드를 사용하여 Kaspersky Endpoint Security를 활성화합니다. 애플리케이션이 이미 활성화된 경우 이 키는 예약 키로 추가됩니다.
/REFRESH	Kaspersky Endpoint Security 라이센스 상태를 업데이트합니다. 결과적으로, 애플리케이션이 Kaspersky 활성화 서버로부터 최신 라이센스 상태 정보를 받습니다.
/REFRESH <license ID>	라이센스 ID를 사용하여 라이센스 상태를 업데이트합니다. 이 명령을 사용하여 EDR 애드온, MDR 애드온, KUMA 애드온 또는 기타 라이센스의 상태를 업데이트할 수 있습니다. 라이센스 인증서에서 라이센스 ID를 얻을 수 있습니다. 결과적으로, 애플리케이션이 Kaspersky 활성화 서버로부터 최신 라이센스 상태 정보를 받습니다.
/CHECK	라이센스 정보 확인하기. Kaspersky Endpoint Security는 예약 키, EDR 애드온, MDR 애드온, KUMA 애드온 키, 기타 키를 포함하여 추가된 모든 라이센스 키에 대한 정보를 표시합니다. Kaspersky Endpoint Security는 다음과 같은 라이센스 정보를 표시합니다: • 라이센스 이름 • 라이센스 식별자 • Light Agent 모드에서 애플리케이션이 설치되어 있는 가상 머신이 연결된 보호 서버(SVM)의 주소 • 라이센스 유형: 체험판, 상업용, 베타, 서브스크립션 • 애플리케이션 활성화 날짜와 시간 • 라이센스 만료 날짜와 시간 • 라이선스 만료 전까지 남은 날짜
/CHECK <license ID>	ID로 라이센스 정보 확인하기. 이 명령을 사용하여 라이센스 정보를 확인할 수 있습니다. 라이센스 인증서에서 라이센스 ID를 얻을 수 있습니다.
/DEL /login=<user name> /password=<password>	애플리케이션의 라이센스 키를 제거합니다. 예약 키 역시 제거됩니다.
/DEL <license ID> /login=<user name> /password=<password>	라이센스 ID를 사용하여 키를 삭제합니다. 이 명령을 사용하여 EDR 애드온, MDR 애드온, KUMA 애드온 또는 다른 라이센스에서 키를 삭제할 수 있습니다. 라이센스 인증서에서 라이센스 ID를 얻을 수 있습니다.

인증	
/login=<user name> /password=<password>	필요한 암호 보호 권한이 있는 사용자 계정 정보

예

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

예

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. 라이센스 구매

Kaspersky 웹사이트를 열고 라이센스를 구매 또는 갱신합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

애플리케이션을 Light Agent 모드로 설치했다면 이 명령을 실행할 수 없습니다.

PBATESTRESET. 디스크를 암호화하기 전에 디스크 검사 결과 재설정

Kaspersky 디스크 암호화 및 BitLocker 드라이브 암호화 기술을 포함하여 전체 디스크 암호화(FDE)의 호환성 검사 결과를 초기화합니다.

전체 디스크 암호화를 실행하기 전에 애플리케이션은 여러 가지 검사를 수행하여 시스템을 암호화할 수 있는지 확인합니다. 컴퓨터가 전체 디스크 암호화를 지원하지 않는 경우 Kaspersky Endpoint Security는 비호환성에 대한 정보를 기록합니다. 다음에 암호화를 시도할 때 애플리케이션에서 이 검사를 수행하지 않으며 암호화를 사용할 수 없다는 경고를 표시합니다. 시스템의 하드웨어 구성이 변경된 경우 시스템 하드 드라이브가 Kaspersky 디스크 암호화 또는 BitLocker 드라이브 암호화와의 호환성을 다시 확인하려면 애플리케이션에서 이전에 기록한 호환성 검사 결과를 초기화해야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

EXIT. 애플리케이션 종료

Kaspersky Endpoint Security를 종료합니다. 애플리케이션이 컴퓨터의 RAM에서 언로드됩니다.

이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다. 해당 사용자에게 **애플리케이션 종료** 권한이 있어야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. 정책 사용 안 함

Kaspersky Security Center 정책을 비활성화합니다. 정책에 닫힌 자물쇠(🔒)가 있는 설정을 포함하여 모든 Kaspersky Endpoint Security 설정을 수정할 수 있습니다.

이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다. 사용자는 **Kaspersky Security Center 정책 비활성화** 권한을 가지고 있어야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. 정책 사용

Kaspersky Security Center 정책을 활성화합니다. 정책에 따라 애플리케이션 설정이 구성됩니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

DISABLE. 보호 중지

만료된 Kaspersky Endpoint Security 라이센스가 있는 컴퓨터에서 파일 위협 보호를 사용하지 않도록 설정합니다. 애플리케이션이 활성화되지 않았거나 유효한 라이센스가 없는 컴퓨터에서는 이 명령을 실행할 수 없습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

SPYWARE. 스파이웨어 탐지

스파이웨어 탐지를 관리합니다. 기본적으로 스파이웨어 탐지는 활성화되어 있습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com SPYWARE on|off
```

KSN. KSN/KPSN 간 전환

파일 또는 웹사이트의 평판을 결정하기 위한 Kaspersky 솔루션 선택. Kaspersky Endpoint Security는 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 Endpoint Security 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.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

애플리케이션을 Light Agent 모드로 설치했다면 이 명령을 실행할 수 없습니다.

명령 구문

```
avp.com KSN /global | /private <file name>
```

Kaspersky Security Network 구성 파일	
`<file name>`	Kaspersky Private Security Network 설정이 포함된 구성 파일의 이름입니다. 이 파일의 확장자는 PKCS7 또는 PEM입니다.

예

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

예

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. 서버 연결 보호 중지

중앙 관리 서버 연결에 대한 컴퓨터의 암호를 제거하는 *중앙 관리 서버 연결 보호* 작업을 실행합니다. 이렇게 하면 해당 작업은 중앙 관리 서버 연결의 보호를 비활성화합니다.

이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

암호	
`/password=<password>`	KL Admin 사용자 계정의 암호 또는 *중앙 관리 서버 연결 보호* 작업의 암호. 파라미터가 지정되지 않은 경우, Kaspersky Endpoint Security에서는 다음 줄에 암호를 입력하라는 메시지가 표시됩니다.

KESCLI 명령

KESCLI 명령을 사용하면 OPSWAT 구성 요소를 사용하여 컴퓨터 보호 상태에 대한 정보를 받을 수 있으며, *악성 코드 검사*나 *데이터베이스 및 애플리케이션 모듈 업데이트*와 같은 기본적인 작업을 수행할 수 있습니다.

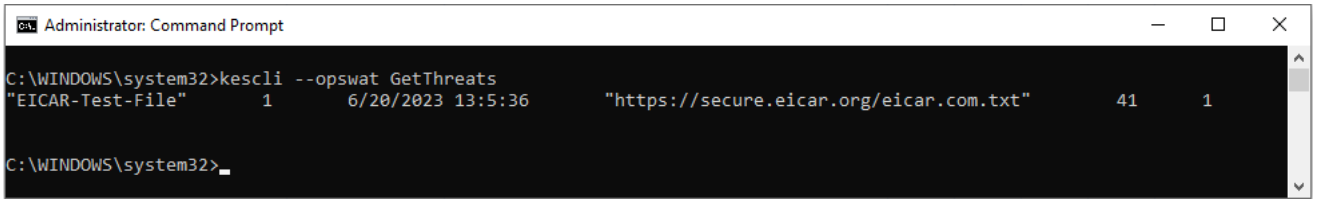
`kescli --help` 명령어를 사용하거나 축약 명령어 `kescli -h`를 사용하여 KESCLI 명령 목록을 볼 수 있습니다.

명령줄에서 Kaspersky Endpoint Security를 관리하려면 다음을 수행합니다.

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.
   애플리케이션 설치 중에 %PATH% 시스템 변수에 실행 파일의 경로를 추가할 수 있습니다.
3. 다음 템플릿을 사용하여 명령을 실행합니다.

   ```
   kescli <명령> [options]
   ```

   그러면 Kaspersky Endpoint Security는 명령을 실행합니다(다음 그림 참조).



명령줄로 애플리케이션 관리

Scan. 악성 코드 검사

악성 코드 검사(전체 검사) 작업을 실행합니다.

작업을 실행하려면 관리자가 정책에서 로컬 작업 사용을 허용해야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

명령 구문

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

`GetScanState` 명령어를 사용하면 *악성 코드 검사*의 완료 상태를 확인할 수 있고 `GetLastScanTime` 명령어를 사용하여 검사가 마지막으로 완료된 날짜와 시간을 볼 수 있습니다.

검사 범위	
`<scan scope>`	`;`으로 구분된 파일 및 폴더 목록. 예: `"C:\Program Files (x86)\Example Folder"`.

위협 탐지 시 처리 방법	
`0`	**알림**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 감염된 파일에 대한 정보를 해당 파일 탐지 시 처리 안 된 위협 목록에 추가합니다.
`1`	**치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다. 이 처리 방법은 기본적으로 선택되어 있습니다.

예

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. 검사 완료 상태

악성 코드 검사(전체 검사) 작업 완료 상태에 관한 정보를 표시합니다.

- `1` – 검사가 진행 중입니다.
- `0` – 검사를 진행하고 있지 않습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

명령 구문

```
kescli --opswat GetScanState
```

GetLastScanTime. 검사 완료 시간 확인

마지막으로 *악성 코드 검사(전체 검사)* 작업을 완료한 날짜 및 시간에 관한 정보를 표시합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

명령 구문

```
kescli --opswat GetLastScanTime
```

GetThreats. 삭제한 보안위협에 대한 데이터 불러오기

삭제한 보안 위협의 목록(*위협 처리 리포트*)을 표시합니다. 이 리포트는 리포트 생성 시점으로부터 지난 30일간의 보안위협 및 바이러스 활동에 관한 정보를 포함합니다.

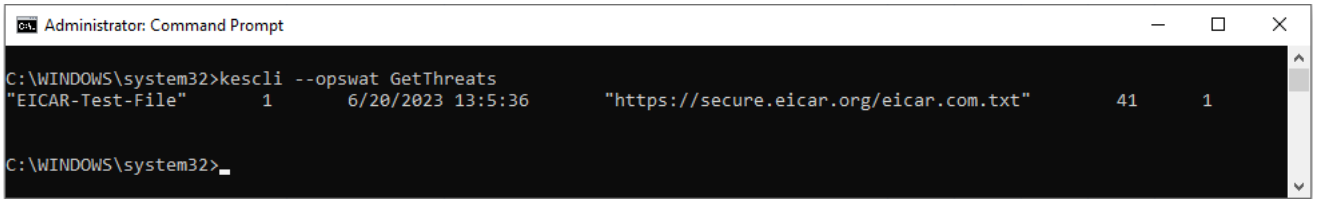
명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

명령 구문

```
kescli --opswat GetThreats
```

이 명령을 실행하면 Kaspersky Endpoint Security가 다음 형식으로 응답을 전송합니다:

```
<name of detected object> <type of object> <detection date and time> <path to file>
<action on threat detection> <threat danger level>
```



명령줄로 애플리케이션 관리

개체 유형	
0	알 수 없음(Unknown).
1	바이러스(Virware).
2	트로이목마 프로그램(Trojware).
3	악성 프로그램(Malware).
4	광고 프로그램(Adware).
5	자동 다이얼러 프로그램(Pornware).
6	사이버 범죄에 악용되어 사용자의 컴퓨터 또는 데이터를 손상할 수 있는 애플리케이션(Riskware).
7	압축 방식이 악성 코드를 보호할 목적으로 이용될 수 있는 실행 압축 개체(Packed).
20	알 수 없는 개체(Xfiles).
21	알려진 애플리케이션(Software).
22	숨겨진 파일(Hidden).
23	주의가 필요한 애플리케이션(Pupware).
24	이례적인 동작(Anomaly).
30	확인되지 않음(Undetect).
40	광고 배너(Banner).
50	네트워크 공격(Attack).
51	레지스트리 접근(Registry).
52	의심스러운 활동(Suspicion).
60	취약점(Vulnerability).
70	피싱(Phishing).

80	원치 않는 이메일 첨부 파일(Attachment).
90	Kaspersky Security Network에서 탐지한 악성 코드(Urgent).
100	알 수 없는 링크(Suspic URL).
110	기타 악성 코드(Behavioral).

위협 탐지 시 처리 방법	
0	알 수 없음(unknown).
1	보안위협을 치료함(ok).
2	개체가 감염되었으며 치료할 수 없음(infected).
5	개체가 압축 파일 내에 있어 치료되지 않음(archive).
9	개체가 치료됨(disinfected).
10	개체가 치료되지 않음(not disinfected).
11	개체가 삭제됨(deleted).
13	개체의 백업 복사본이 생성됨(backupped).
15	개체가 백업 저장소로 이동됨(quarantined).
23	개체가 컴퓨터를 다시 시작할 때 삭제됨(delete on reboot).
25	개체가 컴퓨터를 다시 시작할 때 치료됨(disinfect on reboot).
29	사용자가 개체를 백업 저장소로 이동함(added by user).
30	개체가 예외 규칙에 추가됨(added to exclude).
31	개체가 컴퓨터를 다시 시작할 때 백업 저장소로 이동됨(quarantine on reboot).
36	오탐(false alarm).
38	개체가 강제 종료됨(terminated).
40	개체가 탐지되지 않음(not found).
41	보안위협을 해결할 수 없음(untreatable).
42	개체가 복원됨(rolled back).
43	개체가 보안위협 활동의 결과로 생성됨(produced by threat).
44	개체가 컴퓨터를 다시 시작할 때 복원됨(roll back on reboot).
0xffffffff	개체가 처리되지 않음(discarded).

보안위협 위험 수준	
0	알 수 없음
1	높음
2	보통 검사
4	낮음
8	정보(*낮음*보다 낮음)

UpdateDefinitions. 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트

데이터베이스 및 애플리케이션 모듈 업데이트 작업 실행. Kaspersky Endpoint Security는 기본 경로를 사용합니다: Kaspersky 업데이트 서버.

작업을 실행하려면 관리자가 정책에서 로컬 작업 사용을 허용해야 합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

애플리케이션을 Light Agent 모드로 설치했다면 이 명령을 실행할 수 없습니다.

명령 구문

```
kescli --opswat UpdateDefinitions
```

`GetDefinitionsetState` 명령을 사용해 현재 안티바이러스 데이터베이스의 배포 날짜 및 시간을 확인할 수 있습니다.

GetDefinitionState. 데이터베이스의 마지막 업데이트 날짜 및 시간 확인

사용 중인 안티 바이러스 데이터베이스의 마지막 업데이트 날짜 및 시간 정보를 표시.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

명령 구문

```
kescli --opswat GetDefinitionState
```

EnableRTP. 보호 활성화

컴퓨터에서 Kaspersky Endpoint Security 보호 구성 요소를 활성화: 파일 위협 보호, 웹 위협 보호, 메일 위협 보호, 네트워크 위협 보호, 호스트 침입 방지.

보호 구성 요소를 활성화하려면 관리자가 관련 정책 설정을 수정할 수 있는지 확인해야 합니다(속성이 열려 있음).

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

명령 구문

```
kescli --opswat EnableRTP
```

결과적으로 암호 보호로 애플리케이션 설정 변경을 금지했더라도 보호 구성 요소가 활성화됩니다.

`GetRealTimeProtectionState` 명령어를 사용하면 파일 위협 보호의 작동 상태를 확인할 수 있습니다.

GetRealTimeProtectionState. 파일 위협 보호 상태

파일 위협 보호 구성 요소의 상태에 관한 정보를 표시합니다.

- `1` – 구성 요소가 활성화되어있습니다.
- `0` – 구성 요소가 비활성화되어있습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

명령 구문

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. 디스크 암호화 상태

디스크 암호화 상태 정보 표시:

- `1`은 디스크가 Kaspersky 또는 BitLocker 디스크 암호화 기술로 보호된다는 의미입니다.
- `0`은 디스크가 암호화되지 않았다는 의미입니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

명령 구문

```
kescli --opswat GetEncryptionState
```

Version. 애플리케이션 버전 확인

Kaspersky Endpoint Security for Windows의 버전을 표시합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.

명령 구문

```
kescli --Version
```

축약 명령어인 `-v`를 사용할 수도 있습니다.

Detection and Response management 명령

명령줄을 사용하여 Detection and Response 솔루션의 기본 제공 기능(Kaspersky Sandbox 또는 Kaspersky Endpoint Detection and Response Optimum 등)을 관리할 수 있습니다. Kaspersky Security Center 콘솔 관리가 불가능할 시 Detection and Response 솔루션을 관리할 수 있습니다. `HELP` 명령을 실행하여 애플리케이션을 관리하기 위한 명령 목록을 볼 수 있습니다. 특정 명령의 구문을 읽으려면 `HELP <command>`을 입력합니다.

명령줄을 사용하여 Detection and Response 솔루션의 기본 제공 기능을 관리하려면 다음과 같이 하십시오.

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.
3. 다음 템플릿을 사용하여 명령을 실행합니다.

```
avp.com <command> [options]
```

그러면 Kaspersky Endpoint Security는 명령을 실행합니다.

SANDBOX. Sandbox 관리

Sandbox 구성 요소 관리 명령:

- Sandbox 구성 요소 활성화 또는 비활성화.

  Sandbox 구성 요소는 Kaspersky Sandbox 솔루션과 Kaspersky Anti Targeted Attack Platform의 일부인 KATA Sandbox 구성 요소와의 상호 작용을 제공합니다.

- Kaspersky Sandbox 구성 요소 구성:

  - 컴퓨터를 Sandbox 서버에 연결합니다.

    서버는 Microsoft Windows 운영 체제의 배포된 가상 이미지를 사용하여 검사할 개체를 실행합니다. IP 주소(IPv4 또는 IPv6)나 정규화된 도메인 이름을 입력할 수 있습니다. 가상 이미지 배포 및 Sandbox 서버 구성에 대한 자세한 내용은 Kaspersky Sandbox 도움말 및 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

  - 서버 연결 시간 초과를 구성합니다.

    Sandbox 서버(Kaspersky Sandbox용) 또는 Central Node 서버(KATA용)의 연결 시간 초과입니다. 구성된 시간 초과를 넘으면 Kaspersky Endpoint Security가 다음 서버로 요청을 보냅니다. 연결 속도가 느리거나 연결이 불안정하다면 서버의 연결 시간 초과 설정을 늘릴 수 있습니다. 요청 시간 초과 설정은 0.5초 이하를 권장합니다.

  - 컴퓨터와 서버 간에 신뢰할 수 있는 연결을 구성합니다.

    Sandbox 서버(Kaspersky Sandbox용) 또는 Central Node 서버(KATA용)와의 신뢰할 수 있는 연결을 구성하려면 TLS 인증서를 준비해야 합니다. 그런 다음 정책을 사용하여 컴퓨터에 인증서를 추가해야 합니다. Sandbox 서버(Kaspersky Sandbox용) 또는 Central Node 서버(KATA용)에 인증서를 추가해야 합니다.

- 통합 유형을 구성합니다.

  Sandbox가 포함된 솔루션, 즉 Kaspersky Sandbox 또는 KATA Sandbox 중 하나를 선택해야 합니다. *Kaspersky Sandbox*는 Kaspersky의 독립 실행형 Detection and Response 솔루션입니다. *KATA Sandbox*는 Kaspersky Anti Targeted Attack Platform 솔루션의 구성 요소입니다. KATA Sandbox와 통합된 경우, 해당 구성 요소는 다음 모드에서 작동할 수 있습니다:

  - **수동**. 사용자가 마우스 오른쪽 메뉴에서 검사할 파일을 수동으로 제출합니다(**Sandbox로 전송**).
  - **자동**. 애플리케이션이 자동으로 개체를 탐지하여 검사를 위해 Sandbox에 제출합니다.
  - **조합**.

- 구성 요소의 현재 설정 표시.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

동작	
`stop`	Sandbox 구성 요소를 비활성화합니다.
`start`	Sandbox 구성 요소를 활성화합니다.

`set`	Sandbox 구성 요소를 구성합니다. 다음과 같은 설정을 구성할 수 있습니다:
	• Sandbox 서버 추가(`--servers`)
	• TLS 인증서를 추가합니다(`--pinned-certificate`)
	• 암호화 컨테이너 추가(`--client-certificate`)
	• 암호화 컨테이너의 암호 지정(`--client-certificate-password`)
	• 서버 연결 시간 초과 설정(`--timeout`)
	• 통합 모드 선택(`--mode`)
	  • `KSB` – Kaspersky Sandbox와 통합
	  • `KATAManual` – KATA Sandbox와 수동 통합
	  • `KATAAuto` – KATA Sandbox와 자동 통합
	  • `KATAFull` – KATA Sandbox와 결합된 통합

`show`	구성 요소의 현재 설정을 표시합니다. 다음과 같은 응답을 받습니다:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

인증	
/login=<user name> /password=<password>	필요한 암호 보호 권한이 있는 사용자 계정 정보

예

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB
/login=login /password=password
```

PREVENTION. 실행 방지 관리

실행 방지 규칙 목록을 포함하여 실행 방지 구성 요소를 비활성화하거나 구성 요소의 현재 설정을 표시합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com prevention disable
```

```
avp.com prevention /show
```

`prevention /show` 명령을 실행하면 다음 응답을 받습니다:

```
prevention.enable=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
```

명령 반환 값:

- `-1`은 컴퓨터에 설치된 애플리케이션 버전에서 이 명령을 지원하지 않는다는 뜻입니다.
- `0`은 명령이 성공적으로 실행되었음을 의미합니다.
- `1`은 명령에 필수 인수가 전달되지 않았음을 의미합니다.
- `2`는 일반적인 오류가 발생했음을 의미합니다.
- `4`는 구문 오류가 있음을 의미합니다.
- `9` – 잘못된 작업(이미 비활성화된 구성 요소를 비활성화하려는 시도 등).

ISOLATION. 네트워크 격리 관리

컴퓨터의 네트워크 격리를 비활성화하거나 구성 요소의 현재 설정을 표시합니다. 구성 요소 설정에는 예외 규칙에 추가된 네트워크 연결 목록도 포함됩니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

`stat` 명령을 실행하면 다음과 같은 응답을 수신합니다: `Network isolation on|off`.

RESTORE. 격리 저장소에서 파일 복원

격리 저장소에서 파일을 원래 폴더로 복원합니다. *격리 저장소*는 컴퓨터의 특수 로컬 저장소입니다. 컴퓨터에 위험하다고 판단되는 파일을 격리할 수 있습니다. 격리된 파일은 암호화된 상태로 저장되며 장치 보안에 위협이 되지 않습니다. Kaspersky Endpoint Security는 Kaspersky Detection and Response 솔루션과 통합했을 때만 격리 저장소를 사용합니다. 그 외에는 Kaspersky Endpoint Security가 관련 파일을 백업에 저장합니다. 솔루션에 포함된 격리 저장소 관리 방법에 대한 자세한 내용은 Kaspersky Sandbox 도움말, Kaspersky Endpoint Detection and Response Optimum 도움말, Kaspersky Endpoint Detection and Response Expert 도움말, Kaspersky Anti Targeted Attack Platform 도움말 및 Kaspersky Endpoint Detection and Response Expert(on-premise) 도움말을 참조하십시오.

이 명령을 수행하려면 암호 보호가 켜져 있어야 합니다. 해당 사용자에게 **백업에서 복원** 권한이 있어야 합니다.

개체는 시스템 계정(SYSTEM)에서 격리됩니다.

격리 저장소에서 파일을 복원하려면 다음 특별 사항을 고려해야 합니다.

- 대상 폴더가 삭제되었거나 사용자에게 해당 폴더에 대한 액세스 권한이 없을 시, 애플리케이션이 파일을 `%DataRoot%\QB\Restored` 폴더에 저장합니다. 해당 파일은 원하는 경로로 직접 이동해야 합니다.
- 애플리케이션은 복원 중인 파일의 이름을 대소문자를 구분하여 처리합니다. 파일 이름 입력 시 대소문자를 지키지 않으면, 애플리케이션에서 파일을 복원하지 않습니다.
- 대상 폴더에 같은 이름의 파일이 이미 있다면, 애플리케이션이 파일 복원을 취소합니다.
- KATA(EDR) 솔루션을 사용하는 경우 애플리케이션은 파일을 복원한 후 격리 저장소에 파일 사본을 저장합니다. 격리 저장소는 수동으로 비울 수 있습니다. EDR Optimum 및 EDR Expert 솔루션에서는, 애플리케이션이 복원 후 파일을 삭제합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

고급 설정	
/REPLACE	기존 파일 덮어쓰기
<file name>	복원될 파일의 이름

인증	
/login=<user name> /password=<password>	필요한 암호 보호 권한이 있는 사용자 계정 정보

예

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

명령 반환 값:

- -1은 컴퓨터에 설치된 애플리케이션 버전에서 이 명령을 지원하지 않는다는 뜻입니다.
- 0은 명령이 성공적으로 실행되었음을 의미합니다.
- 1은 명령에 필수 인수가 전달되지 않았음을 의미합니다.
- 2는 일반적인 오류가 발생했음을 의미합니다.
- 4는 구문 오류가 있음을 의미합니다.

IOCSCAN. 침해지표(IOC) 검사

IOC 검사 작업 실행. *침해지표(IOC)*는 컴퓨터에 대한 무단 접근(데이터 침해)을 나타내는 개체 또는 활동에 대한 데이터 집합입니다. 예를 들어, 시스템 로그인 시도가 여러 번 실패하면 침해지표가 될 수 있습니다. *IOC 검사* 작업을 통해 컴퓨터에서 침해지표를 찾고 보안 위협에 대응할 수 있습니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

IOC 검사는 IOC 파일에 설명된 침해지표와 128개가 일치 시 중단됩니다. 이는 IOC 검사 작업 리포트의 항목 수를 제한하여 분석을 더 쉽게 하고, 정확하지 않게 공식화된 침해지표로 대량의 일치 항목이 생성되어 리포트가 오버플로되는 것을 방지하기 위함입니다.

명령 구문

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

IOC 파일	
`<full path to the IOC file>`	검사에 사용할 IOC 파일의 전체 경로입니다. 공백으로 구분된 여러 IOC 파일을 지정할 수 있습니다. IOC 파일의 전체 경로는 `/path` 인수 없이 입력해야 합니다. 예: `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	검사에 사용할 IOC 파일이 있는 폴더의 경로입니다. *IOC 파일*은 애플리케이션이 탐지 횟수 계산을 위해 매치하는 지표 세트를 포함하는 파일입니다. IOC 파일은 OpenIOC 표준을 준수해야 합니다. 예: `C:\Users\Admin\Desktop\IOC`

IOC 검사를 위한 데이터 유형	
`/process=on|off`	IOC 검사 수행 시 프로세스 데이터를 분석합니다(ProcessItem 용어). 인수의 값이 `off`라면 Kaspersky Endpoint Security는 검사를 수행할 때 컴퓨터에서 실행 중인 프로세스를 분석하지 않습니다. IOC 파일에 ProcessItem IOC 문서의 IOC 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 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>`	IOC 검사 수행 시 파일 데이터를 분석합니다(ProcessItem 및 FileItem용어). 다음과 같은 방법으로 파일을 선택할 수 있습니다: • `<full path to the executable file of the process>` – ProcessItem 용어 • `<full path to the file>` – FileItem 용어
`/registry=on|off`	IOC 검사 수행 시 Windows 레지스트리 데이터를 분석합니다(RegistryItem 용어). 인수의 값이 `off`라면 Kaspersky Endpoint Security가 Windows 레지스트리를 검사하지 않습니다. IOC 파일에 RegistryItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 RegistryItem IOC 문서가 설명된 경우에만 Windows 레지스트리를 분석합니다. RegistryItem 데이터 유형에 대해 Kaspersky Endpoint Security는 레지스트리 키 세트를 검사합니다.
`/dnsentry=on|off`	IOC 검사 수행 시 로컬 DNS 캐시의 레코드에 대한 데이터를 분석합니다(DnsEntryItem 용어). 인수의 값이 `off`라면 Kaspersky Endpoint Security가 로컬 DNS 캐시를 검사하지 않습니다. IOC 파일에 DnsEntryItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 DnsEntryItem IOC 문서가 설명된 경우에만 로컬 DNS 캐시를 분석합니다.
`/arpentry=on|off`	IOC 검사수행 시 ARP 테이블의 레코드에 대한 데이터를 분석합니다.(ArpEntryItem 용어) 인수의 값이 `off`라면 Kaspersky Endpoint Security가 ARP 테이블을 검사하지 않습니다. IOC 파일에 ArpEntryItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 ArpEntryItem IOC 문서가 설명된 경우에만 ARP 테이블을 분석합니다.
`/ports=on|off`	IOC 검사 수행 시 수신 대기를 위해 열려 있는 포트에 대한 데이터를 분석합니다(PortItem 용어). 인수의 값이 `off`라면 Kaspersky Endpoint Security가 장치의 활성 연결 테이블을 검사하지 않습니다. IOC 파일에 PortItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 PortItem IOC 문서가 설명된 경우에만 활성 연결 테이블을 분석합니다.
`/services=on|off`	IOC 검사 수행 시 장치에 설치된 서비스에 대한 데이터를 분석합니다(ServiceItem 용어). 인수의 값이 `off`라면 Kaspersky Endpoint Security가 장치에 설치된 서비스에 대한 데이터를 검사하지 않습니다. IOC 파일에 ServiceItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 ServiceItem IOC 문서가 설명된 경우에만 서비스 데이터를 분석합니다.

`/system=on|off`	IOC 검사 수행 시 환경 데이터를 분석합니다(SystemInfoItem 용어). 인수의 값이 `off` 라면 Kaspersky Endpoint Security가 환경 데이터를 분석하지 않습니다. IOC 파일에 SystemInfoItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 SystemInfoItem IOC 문서가 설명된 경우에만 환경 데이터를 분석합니다.
`/users=on|off`	IOC 검사 수행 시 사용자에 대한 데이터를 분석합니다(UserItem 용어). 인수의 값이 `off` 라면 Kaspersky Endpoint Security는 시스템에서 생성된 사용자에 대한 데이터를 분석하지 않습니다. IOC 파일에 UserItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 UserItem IOC 문서가 설명된 경우에만 시스템에서 생성된 사용자에 대한 데이터를 분석합니다.
`/volumes=on|off`	IOC 검사 수행 시 볼륨에 대한 데이터를 분석합니다(VolumeItem 용어). 인수의 값이 `off` 라면 Kaspersky Endpoint Security가 장치의 볼륨에 대한 데이터를 검사하지 않습니다. IOC 파일에 VolumeItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 VolumeItem IOC 문서가 설명된 경우에만 볼륨 데이터를 분석합니다.
`/eventlog=on|off`	IOC 검사 수행 시 Windows 이벤트 로그의 레코드에 대한 데이터를 분석합니다(EventLogItem 용어). 인수의 값이 `off` 라면 Kaspersky Endpoint Security는 Windows 이벤트 로그의 기록을 검사하지 않습니다. IOC 파일에 EventLogItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 EventLogItem IOC 문서가 설명된 경우에 Windows 이벤트 로그를 분석합니다.
`/datetime=<event publication date>`	해당 IOC 문서에 대한 IOC 검사 범위를 결정할 때 이벤트가 Windows 이벤트 로그에 게시된 날짜를 고려합니다. IOC 검사 수행 시 Kaspersky Endpoint Security는 지정된 시간과 날짜부터 작업이 실행되는 순간까지의 기간에 게시된 Windows 이벤트 로그 항목을 검사합니다. Kaspersky Endpoint Security에서는 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 Endpoint Security는 모든 게시 날짜의 이벤트를 검색합니다. `TaskSettings::BaseSettings::EventLogItem::datetime` 설정은 편집할 수 없습니다 이 설정은 검사를 위해 제공된 IOC 파일에 EventLogItem IOC 문서가 설명된 경우에만 사용됩니다.
`/channel=<list of channels>`	IOC 검사를 수행하려는 채널(로그) 이름 목록입니다. 인수를 지정하면 Kaspersky Endpoint Security는 지정한 로그에 게시된 레코드를 검색합니다. IOC 문서에는 EventLogItem 용어가 설명되어 있어야 합니다. 로그 이름은 로그 속성(Full Name 파라미터) 또는 이벤트 속성(이벤트의 xml 스키마에 있는 `<Channel></Channel>` 파라미터)에 지정된 로그(채널) 이름에 따라 스트링으로 지정됩니다. 공백으로 구분된 여러 채널을 지정할 수 있습니다. 인수를 지정하지 않으면 Kaspersky Endpoint Security는 `Application`, `System`, `Security` 채널에 대한 레코드를 검색합니다.
`/files=on|off`	IOC 검사 수행 시 파일 데이터를 분석합니다(FileItem 용어). 인수의 값이 `off` 라면 Kaspersky Endpoint Security는 파일 데이터를 분석하지 않습니다. IOC 파일에 FileItem IOC 문서 용어가 포함되어 있다면 이 용어를 무시합니다(불일치로 탐지). 인수를 지정하지 않으면 Kaspersky Endpoint Security는 검사를 위해 제공된 IOC 파일에 FileItem IOC 문서가 설명된 경우에만 파일 데이터를 분석합니다.
`/drives=<all|system|critical|custom>`	FileItem IOC 문서에 대한 데이터를 분석할 때의 IOC 검사 범위를 설정합니다. 검사 범위에 대해 다음 값을 설정할 수 있습니다: • `<all>`: 사용 가능한 모든 파일 범위. • `<system>`: 운영 체제가 설치된 폴더의 파일. • `<critical>`: 사용자 및 시스템 폴더의 임시 파일. • `<custom>`: 사용자 지정 범위의 파일(`/scope=<list of folders to scan>`). 인수를 지정하지 않으면 중요한 영역에 대해 검사가 수행됩니다.
`/excludes=<list of exclusions>`	FileItem IOC 문서에 대한 데이터를 분석할 때 예외 범위를 설정합니다. 공백으로 구분된 여러 경로를 지정할 수 있습니다.
`/scope=<list of folders to scan>`	FileItem IOC 문서에 대한 데이터 분석 시 사용자 정의 IOC 검사 범위(`/drives=custom`). 공백으로 구분된 여러 경로를 지정할 수 있습니다.

`/retro /<number of days>`	*회고적 IOC 검사*는 Kaspersky Endpoint Security가 특정 기간의 데이터를 사용하여 침해 지표를 검사하는 *IOC 검사* 작업의 모드 중 하나입니다. 이 모드는 네트워크 활동, 프로세스, 파일, 기타 원격 측정 등 보호된 컴퓨터의 원격 측정을 통해 침해지표를 검색하는 데 사용됩니다. 기간은 1일부터 14일까지 설정할 수 있습니다. 기본적으로 애플리케이션은 1일 동안의 침해 지표를 검사합니다.
`/network=on|off`	네트워크 데이터 분석(NetworkItem 용어).
`/url=on|off`	브라우저 로그의 데이터 분석(UrlHistoryItem 용어). 회고적 IOC 검사는 다음 브라우저의 로그를 분석합니다. Google Chrome, Mozilla Firefox, Microsoft Edge(버전 79 이상).
`/email`	메일 개체 분석(EmailItem 용어).
`/route`	라우팅 및 포워딩 테이블 분석(RouteEntryItem 용어).

명령 반환 값:

- `-1`은 컴퓨터에 설치된 애플리케이션 버전에서 이 명령을 지원하지 않는다는 뜻입니다.
- `0`은 명령이 성공적으로 실행되었음을 의미합니다.
- `1`은 명령에 필수 인수가 전달되지 않았음을 의미합니다.
- `2`는 일반적인 오류가 발생했음을 의미합니다.
- `4`는 구문 오류가 있음을 의미합니다.

명령이 성공적으로 실행되고(반환 값 `0`) 도중에 침해지표가 감지되면, Kaspersky Endpoint Security가 다음 작업 결과 정보를 명령줄에 출력합니다.

`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.

MDRLICENSE. MDR 활성화

BLOB 구성 파일을 추가하여 Managed Detection and Response를 활성화합니다. BLOB 파일에는 클라이언트 ID와 Kaspersky Managed Detection and Response 라이센스에 대한 정보가 포함되어 있습니다. BLOB 파일은 MDR 구성 파일의 ZIP 압축파일 안에 있습니다. Kaspersky Managed Detection and Response 콘솔에서 ZIP 압축파일을 얻을 수 있습니다. BLOB 파일에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

BLOB 파일로 작업을 수행하려면 관리자 권한이 필요합니다. 정책의 Managed Detection and Response 설정도 편집할 수 있어야 합니다( ).

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

동작	
`/ADD <file name>`	Kaspersky Managed Detection and Response(P7 파일 형식)와의 통합을 위해 BLOB 구성 파일을 적용합니다. BLOB 파일은 하나만 적용할 수 있습니다. BLOB 파일이 이미 컴퓨터에 추가된 경우 파일이 대체됩니다.
`/DEL`	BLOB 구성 파일을 삭제합니다.

인증	
`/login=<user name> /password=<password>`	필요한 암호 보호 권한이 있는 사용자 계정 정보

예

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

예

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. EDR(KATA)과의 통합

Endpoint Detection and Response(KATA) 구성 요소 관리 명령:

- EDR(KATA) 구성 요소 활성화 또는 비활성화.

  EDR(KATA) 구성 요소는 Kaspersky Anti Targeted Attack Platform 솔루션과의 상호 운용성을 제공합니다.
- Kaspersky Anti Targeted Attack Platform 서버에 대한 연결 구성.
- 구성 요소의 현재 설정 표시.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

동작	
`stop`	EDR(KATA) 구성 요소를 비활성화합니다.
`start`	EDR(KATA) 구성 요소를 활성화합니다.

set	EDR(KATA) 구성 요소를 구성합니다. 다음과 같은 설정을 구성할 수 있습니다: • Central Node 서버를 추가합니다(servers=<server address>:<port>) • TLS 인증서를 추가합니다(server-certificate=<path to the TLS certificate>) • Central Node 서버 연결 시간 초과를 설정합니다(/timeout=<Central Node server connection timeout (s)>) • Central Node 서버와의 동기화 기간을 설정합니다(/sync-period=<Central Node server synchronization period (min)>)
show	구성 요소의 현재 설정을 표시합니다.

KUMA. KUMA과 통합

내장된 KUMA 에이전트 관리 명령:

- KUMA 통합 활성화 및 비활성화

  내장된 KUMA 에이전트는 Kaspersky Unified Monitoring and Analysis Platform 솔루션과의 상호운용성을 제공합니다.

- Kaspersky Unified Monitoring and Analysis Platform 서버와 연결 구성 중입니다.

- 구성 요소의 현재 설정 표시.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

동작	
stop	KUMA 통합 비활성화
start	KUMA 통합 활성화
set	내장 KUMA 에이전트 구성 다음과 같은 설정을 구성할 수 있습니다: • KUMA 서버를 추가합니다(/servers=<protocol>://<server address>:<port>) 애플리케이션은 다음과 같은 서버 연결 프로토콜을 지원합니다. tcp, udp, http, https. • TLS 인증서를 추가합니다(/server-certificate=<path to the TLS certificate>) • 서버 연결 시간 초과 설정(/timeout=<KUMA server connection timeout (s)>) • 암호화 컨테이너 추가(/client-certificate=<path to the crypto-container> /client-certificate-password=<password>) • 이벤트 전송 지연 구성(/maximum-data-transfer-time=<maximum events transmission delay (sec))>
show	구성 요소의 현재 설정을 표시합니다.

인증	
/login=<user name> /password=<password>	필요한 암호 보호 권한이 있는 사용자 계정 정보

예

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA. YARA 검사 실행

YARA 검사 실행 작업 실행. 애플리케이션은 YARA 규칙 데이터베이스를 사용하여 회사 IT 인프라에 대한 표적형 공격 지표에 대해 파일과 개체를 검사합니다. *YARA 규칙*은 표적 공격 및 기업 IT 인프라 침입 시그니처에 대한 설명으로, Kaspersky Endpoint Security가 개체 검사를 위해 사용합니다.

YARA 검사를 실행하려면 규칙을 설명하는 YARA 파일을 준비해야 합니다. YARA 파일을 생성할 때 다음 요구 사항을 고려하시기 바랍니다.

- Kaspersky Endpoint Security는 침해지표 설명을 위한 YARA 4.2.3 공개 표준을 따르는 .YARA 및 .YAR 확장자의 YARA 파일을 지원합니다.
- YARA 규칙이 있는 파일만 이 작업에 대해 지정할 수 있습니다. *YARA 검사 실행* 작업은 기타 규칙 유형을 지원하지 않습니다.
- Kaspersky Endpoint Security에서 지원하지 않는 YARA 파일을 추가했거나 규칙에 구문 오류가 포함된 경우 작업이 중단되고 해당 오류 메시지가 표시됩니다.
- 단일 작업에 사용된 모든 YARA 파일의 식별자는 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.

Kaspersky는 YARA 파일당 하나의 규칙을 생성하는 것을 권장합니다. 그러면 검사 결과를 더 쉽게 읽을 수 있습니다.

YARA 검사에는 상당한 시간이 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.

명령 구문

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

YARA 파일	
`<full path to the YARA file>`	검사에 사용할 YARA 파일의 전체 경로입니다. 공백으로 구분된 여러 YARA 파일 경로를 지정할 수 있습니다. `/path=<path to the folder with YARA files>` 값이 지정되지 않은 경우 필요한 인수입니다. 예: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	검사에 사용할 YARA 파일이 있는 폴더의 전체 경로입니다. `<full path to the YARA file>` 값이 지정되지 않은 경우 필요한 인수입니다. 예: `/path=C:\Users\Admin\Desktop\YARA`

고급 설정	
`/fastScan=<on|off>`	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 모드에서 애플리케이션은 탐지된 지표의 중복 파일을 기록합니다.
`/maxRules=<maximum number of scan rules>`	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=<stop scan after the specified time in seconds>`	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>`	이 인수는 `/scanFolders` 사용자 지정 검사 내 하위 폴더에 반복 검사를 시작합니다.
`/scanFolders=<list of folders to be scanned>`	이 인수는 지정된 폴더 목록에 있는 파일에 YARA 검사를 시작합니다. 공백으로 구분된 여러 값을 지정할 수 있습니다. Kaspersky Endpoint Security는 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>`	실행 중인 모든 프로세스의 메모리를 검사합니다.
`/scanProcess=<process name>`	지정된 프로세스에 대해서만 메모리를 검사합니다. 프로세스 실행 파일의 공백으로 구분된 전체 경로를 지정합니다. `*` 및 `?` 문자로 마스크를 입력할 수 있습니다.
`/maxSize=<file size in bytes>`	YARA 검사를 위한 파일 크기를 제한합니다. 애플리케이션은 더 큰 파일은 건너뜁니다.
`/includes=<list of objects to be scanned>>`	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=<list of objects to be scanned>`	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>`	자동 실행 지점 개체에 대한 YARA 검사를 수행합니다.
`/excludeAutoruns=<list of autorun point areas to skip>`	검사 범위에서 자동 실행 지점 개체를 제외합니다. 프로세스 실행 파일의 공백으로 구분된 전체 경로를 지정합니다. `*` 및 `?` 문자로 마스크를 입력할 수 있습니다.

`/logFolder=<path to the folder for saving the scan results in a TXT file>`	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.

명령 반환 값:

- `-1`은 컴퓨터에 설치된 애플리케이션 버전에서 이 명령을 지원하지 않는다는 뜻입니다.
- `0`은 명령이 성공적으로 실행되었음을 의미합니다.
- `1`은 명령에 필수 인수가 전달되지 않았음을 의미합니다.
- `2`는 일반적인 오류가 발생했음을 의미합니다.
- `4`는 구문 오류가 있음을 의미합니다.
- `5`는 파라미터에 지정된 YARA 규칙이 있는 하나 이상의 파일을 찾을 수 없음을 의미합니다.

명령이 성공적으로 실행되고(반환 값 `0`) 도중에 침해지표가 감지되면, Kaspersky Endpoint Security가 다음 작업 결과 정보를 명령줄에 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`).

TELEMETRYFILTERS. KUMA로 전송할 이벤트 필터링

기본적으로 KUMA 서버로 이벤트를 전송하는 것은 비활성화되어 있습니다. KUMA가 제대로 작동하도록 하려면 원격 측정 전송을 활성화해야 합니다. 표준 로그인 *Application*, *Security*, *System* 중에서 이벤트 소스를 선택할 수 있습니다. 성능을 개선하고 KUMA 서버로 데이터 전송을 최적화하기 위해, 원격 측정에서 개별 이벤트를 수동으로 추가하거나 제외할 수 있습니다. 그 예로, Sysmon 이벤트를 제외할 수 있습니다.

예외 규칙 목록을 명령줄에서 JSON 파일로 내보낼 수 있습니다.

명령에 설정을 내보낼 파일의 이름만 포함된 경우, 애플리케이션은 다음과 같이 파일을 배치합니다:

- avp.com의 경로를 %PATH% 시스템 변수에 추가하면 애플리케이션이 `C:\Windows\SysWOW64` 폴더 내에 파일을 배치합니다.
- 애플리케이션 설치 폴더에서 명령을 실행하면 애플리케이션의 자체 보호가 애플리케이션 폴더에 새 파일의 생성을 차단하기 때문에 내보내기에 실패합니다. 애플리케이션 설정을 파일로 내보내려면 파일 경로를 입력합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

동작	
`export`	KUMA로 전송할 이벤트 필터를 내보내는 중입니다.
`import`	KUMA로 전송할 이벤트 필터를 가져오는 중입니다. 이벤트 필터링 규칙이 컴퓨터에 이미 있는 경우, Kaspersky Endpoint Security는 가져오기를 수행할 때 이 규칙을 교체합니다.

내보내기 또는 가져오기를 수행할 파일	
`<file name>`	KUMA로 전송할 이벤트 필터를 포함하는 파일의 이름입니다. 파일 경로를 입력할 수도 있습니다. KUMA로 전송할 필터를 JSON 파일로 내보낼 수 있습니다.

Light Agent 관리 명령

명령줄에서 가상 환경 보호를 위한 Light Agent 모드로 애플리케이션을 관리할 수 있습니다. Kaspersky Security Center 콘솔 관리가 불가능할 시 Light Agent 모드에서 애플리케이션을 관리할 수 있습니다. `HELP` 명령을 실행하여 애플리케이션을 관리하기 위한 명령 목록을 볼 수 있습니다. 특정 명령의 구문을 읽으려면 `HELP <command>`을 입력합니다.

명령줄에서 Light Agent 모드로 애플리케이션을 관리하려면:

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다.
3. 다음 템플릿을 사용하여 명령을 실행합니다.

   ```
   avp.com <command> [options]
   ```

   그러면 Kaspersky Endpoint Security는 명령을 실행합니다.

Light Agent 모드로 설치된 애플리케이션은 표준 모드로 설치된 애플리케이션의 거의 모든 AVP 명령을 지원합니다. Light Agent 모드에서는 안티 바이러스 데이터베이스 업데이트 작업 및 라이센스 키 관리 작업이 제한됩니다.

KSVLAINFO. Light Agent 모드 확인

Light Agent 모드 확인

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com KSVLAINFO
```

이 명령은 콘솔에 다음과 같은 정보를 출력합니다:

- 가상 환경 보호를 위한 Light Agent 모드: 활성화 또는 비활성화.

  Light Agent 모드를 활성화하면 애플리케이션이 Kaspersky Security for Virtualization Light Agent 솔루션의 일부로 사용됩니다.

- VDI 보호 모드: 활성화 또는 비활성화.

  VDI 보호 모드는 비영구 가상 컴퓨터에서 Kaspersky Endpoint Security의 성능을 최적화하는 데 도움이 됩니다. VDI 보호 모드를 활성화하면 보호 대상 가상 머신을 다시 시작해야 하는 업데이트는 비영구 가상 컴퓨터에 설치되지 않습니다. 재시작이 필요한 업데이트를 수신하면 비영구 가상 컴퓨터에 설치된 Light Agent는 Kaspersky Security Center 로 보호된 가상 컴퓨터 템플릿을 업데이트해야 한다는 메시지를 보냅니다.

- 보호된 가상 컴퓨터의 유형: 영구 또는 비영구.

- 가상 인프라에서 보호된 가상 컴퓨터의 역할: 서버 또는 워크스테이션.

- 보호된 가상 컴퓨터의 식별자(UUID).

VIISINFO. 통합 서버에 대한 Light Agent 연결 상태

통합 서버에 대한 Light Agent 연결 정보를 확인합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com VIISINFO
```

이 명령은 콘솔에 다음과 같은 정보를 출력합니다:

- Light Agent가 연결된 통합 서버의 주소 및 포트.

- 통합 서버 연결 상태.

- Light Agent가 통합 서버에 마지막으로 연결한 날짜와 시간.

SVMINFO. 보호 서버에 대한 Light Agent 연결 상태

보호 서버에 대한 Light Agent 연결 정보를 확인합니다.

명령을 실행하려면 Kaspersky Endpoint Security 실행 파일이 있는 폴더로 이동합니다. %PATH% 시스템 변수에 실행 파일 경로를 추가하고 애플리케이션 폴더로 이동하지 않고 명령을 실행할 수도 있습니다.

명령 구문

```
avp.com SVMINFO
```

이 명령은 콘솔에 다음과 같은 정보를 출력합니다:

- Light Agent가 연결된 SVM의 주소와 Light Agent를 기준으로 가상 인프라 내의 SVM의 위치: 로컬 또는 비로컬.
- Light Agent가 사용하는 SVM 검색 방법: 통합 서버 사용 또는 사용자 지정 SVM 주소 목록 사용.
- SVM 주소 목록이 SVM 검색 방법으로 선택된 경우의 SVM 주소 목록입니다.
- Light Agent를 SVM에 연결하기 위한 태그입니다.
- SVM 선택 알고리즘: 표준 또는 확장. 확장된 SVM 선택 알고리즘을 사용하는 경우 가상 인프라 내 SVM 경로 유형도 표시됩니다.
- Light Agent와 보호 서버 간의 연결 보호 상태입니다.

오류 코드

명령줄을 통해 애플리케이션을 작동할 때 오류가 발생할 수 있습니다. 오류가 발생하면 Kaspersky Endpoint Security에서 오류 메시지를 표시합니다. 예: `Error: Cannot start task 'EntAppControl'`. 또한 Kaspersky Endpoint Security는 코드 양식(예: `error=8947906D`)으로 추가 정보를 표시할 수 있습니다(아래 표 참조).

오류 코드

오류 코드	설명
09479001	이미 사용 중인 키입니다
0947901D	라이센스가 만료되었습니다. 데이터베이스 업데이트를 이용할 수 없습니다
89479002	키를 찾을 수 없습니다
89479003	디지털 서명이 없거나 손상되었습니다
89479004	데이터가 손상되었습니다
89479005	키 파일이 손상되었습니다
89479006	라이센스가 만료되었습니다
89479007	키 파일이 지정되지 않았습니다
89479008	잘못된 키 파일
89479009	데이터 저장 실패
8947900A	데이터 읽기 실패
8947900B	I/O 오류

오류 코드	설명
8947900C	데이터베이스가 없습니다
8947900E	라이센스 라이브러리가 로드되지 않았습니다
8947900F	데이터베이스가 손상되었거나 직접 업데이트하였습니다
89479010	데이터베이스가 손상되었습니다
89479011	유효하지 않은 키 파일을 예비 키로 사용할 수 없습니다
89479012	시스템 오류
89479013	키 거부 목록이 손상되었습니다
89479014	파일 서명이 Kaspersky의 디지털 서명과 일치하지 않습니다
89479015	체험판용 라이센스 키를 상업용 라이센스 키로 사용할 수 없습니다
89479016	애플리케이션의 베타 버전을 사용하려면 베타 테스트용 라이센스가 필요합니다
89479017	이 애플리케이션에 사용할 수 없는 키 파일입니다. 다른 애플리케이션용 키 파일로 Kaspersky Endpoint Security for Windows를 활성화할 수 없습니다. 설치된 애플리케이션을 확인하십시오
89479018	Kaspersky에 의해 차단된 라이센스 키입니다
89479019	이미 체험판을 이용했던 애플리케이션입니다. 체험판 키를 다시 사용할 수는 없습니다
8947901A	키 파일이 손상되었습니다
8947901B	디지털 서명이 누락 또는 손상되었거나 Kaspersky의 디지털 서명과 일치하지 않습니다
8947901C	해당 비상업용 라이센스가 만료되면 키를 추가할 수 없습니다
8947901E	키 파일이 생성 또는 사용된 날짜가 잘못되었습니다. 시스템 날짜를 확인해주십시오
8947901F	체험판 키를 사용하는 동안 다른 체험판 키를 추가할 수 없습니다
89479020	키 거부 목록이 없거나 손상되었습니다
89479021	업데이트 설명 파일이 없거나 손상되었습니다
89479022	이 애플리케이션에는 사용할 수 없는 키입니다
89479023	유효하지 않은 키 파일을 예비 키로 사용할 수 없습니다
89479025	활성화 서버 데이터 전송 오류. 예상 원인: 인터넷 연결 오류 또는 일시적인 활성화 서버 문제. 잠시 후에 다시 활성화하여 주시기 바랍니다(1~2시간 후). 만일 문제가 계속되면, 사용 중인 인터넷 공급업체에 문의해 주시기 바랍니다
89479026	잘못된 활성화 코드입니다.
89479027	응답 상태를 알 수 없습니다
89479028	임시 파일 저장 중 오류가 발생했습니다
89479029	활성화 코드를 잘못 입력했거나 현재 컴퓨터 날짜가 잘못되었습니다. 컴퓨터의 시스템 날짜를 확인해주십시오.
8947902A	이 애플리케이션에 사용할 수 없는 키이거나 라이센스가 만료되었습니다
8947902B	키 파일 가져오기 실패. 잘못된 활성화 코드가 입력되었습니다
8947902C	활성화 서버에서 오류 400이 반환되었습니다
8947902D	활성화 서버에서 오류 401이 반환되었습니다
8947902E	활성화 서버에서 오류 403이 반환되었습니다
8947902F	활성화 서버에서 필요한 리소스를 사용할 수 없습니다. 활성화 서버에서 오류 404이 반환되었습니다. 인터넷 연결 설정을 확인하십시오
89479030	활성화 서버에서 오류 405이 반환되었습니다
89479031	활성화 서버에서 오류 406이 반환되었습니다
89479032	프록시 인증이 필요합니다. 네트워크 설정을 확인하십시오
89479033	응답 시간 초과
89479034	활성화 서버에서 오류 409이 반환되었습니다

오류 코드	설명
89479035	활성화 서버에서 필요한 리소스를 사용할 수 없습니다. 활성화 서버에서 오류 410이 반환되었습니다. 인터넷 연결 설정을 확인하십시오
89479036	활성화 서버에서 오류 411이 반환되었습니다
89479037	활성화 서버에서 오류 412이 반환되었습니다
89479038	활성화 서버에서 오류 413이 반환되었습니다
89479039	활성화 서버에서 오류 414이 반환되었습니다
8947903A	활성화 서버에서 오류 415이 반환되었습니다
8947903C	서버 내부 오류
8947903D	지원하지 않는 기능입니다
8947903E	잘못된 게이트웨이 응답. 네트워크 설정을 확인하십시오
8947903F	일시적으로 리소스를 이용할 수 없습니다
89479040	게이트웨이 응답 시간 초과. 네트워크 설정을 확인하십시오
89479041	서버에서 지원하지 않는 프로토콜입니다
89479043	알 수 없는 HTTP 오류
89479044	잘못된 리소스 ID
89479046	잘못된 URL
89479047	잘못된 대상 폴더
89479048	메모리 할당 오류
89479049	ANSI 문자열(URL, 폴더, 에이전트)로 파라미터를 변환하는 동안 오류가 발생했습니다
8947904A	작업자 쓰레드 생성 중 오류가 발생했습니다.
8947904B	작업자 쓰레드가 이미 실행 중입니다.
8947904C	작업자 쓰레드가 실행 중이지 않습니다.
8947904D	키 파일을 활성화 서버에서 찾을 수 없습니다
8947904E	키가 차단되었습니다
8947904F	활성화 서버 내부 오류
89479050	활성화에 필요한 데이터가 충분하지 않습니다
89479053	추가한 키 파일의 라이센스는 이미 만료되었습니다
89479054	컴퓨터의 날짜가 잘못 설정되어 있습니다. 컴퓨터 날짜를 확인하십시오
89479055	체험판 라이센스가 만료되었습니다
89479056	애플리케이션 활성화 기간이 만료되었습니다
89479057	입력한 활성화 코드는 허용된 애플리케이션 인증 횟수를 초과하였습니다
89479058	시스템 오류로 활성화를 완료하지 못했습니다
89479059	체험판용 라이센스 키를 상업용 라이센스 키로 사용할 수 없습니다
8947905C	활성화 코드가 필요합니다
89479062	활성화 서버에 연결할 수 없습니다
89479064	활성화 서버를 이용할 수 없습니다. 인터넷 연결 설정을 확인하고 활성화를 다시 시도하십시오
89479065	라이센스가 만료되었습니다
89479066	만료된 키로 활성 키를 교체할 수 없습니다
89479067	현재 사용 중인 라이센스보다 일찍 만료되는 예약 키는 추가할 수 없습니다
89479068	업데이트된 서브스크립션 키가 없습니다

오류 코드	설명
8947906A	잘못된 활성화 코드
8947906B	이미 사용 중인 키입니다
8947906C	활성 키와 예약 키의 라이센스 유형이 서로 일치하지 않습니다
8947906D	이 라이센스에서 지원되지 않는 구성 요소입니다
8947906E	서브스크립션 키를 예비 키로 추가할 수 없습니다
89479213	전송 레이어 일반 오류
89479214	활성화 서버 연결 실패
89479215	잘못된 웹 주소 형식
89479216	프록시 서버 주소 변환 실패
89479217	서버 주소 변환 실패. 인터넷 연결 설정을 확인해 주십시오
89479218	서버 연결 시도 실패
89479219	원격 접근이 거부됨
8947921A	동작 시간 초과
8947921B	HTTP 요청 전송 오류
8947921C	SSL 연결 오류
8947921D	동작이 콜백에 의해 중단되었습니다
8947921E	리디렉션이 너무 많습니다
8947921F	받는 사람 확인 실패
89479220	서버 응답 없음
89479221	데이터 전송 오류
89479222	데이터 수신 오류
89479223	SSL 인증서 관련 오류
89479224	SSL 암호화 관련 문제
89479225	SSL 인증 센터 관련 문제
89479226	잘못된 네트워크 패킷 컨텐츠
89479227	계정 접근이 거부됨
89479228	잘못된 SSL 인증서 파일
89479229	SSL 연결을 종료할 수 없습니다
8947922A	반복 오류
8947922B	취소된 인증서가 있는 잘못된 파일
8947922C	SSL 인증서 요청 오류
89479401	알 수 없는 서버 오류
89479402	서버 내부 오류
89479403	입력한 활성화 코드에 대한 키가 없습니다
89479404	활성 키가 차단되었습니다
89479405	활성화 요청에 필요한 파라미터가 누락되었습니다
89479406	잘못된 클라이언트 번호 또는 암호
89479407	잘못된 활성화 코드
89479408	이 애플리케이션에 사용할 수 없는 활성화 코드입니다. 다른 애플리케이션용 활성화 코드로 Kaspersky Endpoint Security for Windows를 활성화할 수 없습니다. 설치된 애플리케이션을 확인하십시오

오류 코드	설명
89479409	활성화 코드가 필요합니다
8947940B	활성화 기간이 만료되었습니다
8947940C	입력한 활성화 코드는 허용된 인증 횟수를 초과하였습니다
8947940D	잘못된 요청 ID 형식
8947940E	이미 사용 중인 활성화 코드입니다
8947940F	활성화 코드 갱신 실패
89479410	이 지역에서는 사용할 수 없는 활성화 코드입니다
89479411	이 활성화 코드는 이 언어에서 사용할 수 없습니다.
89479412	이 활성화 코드는 최신 버전의 애플리케이션을 위한 것입니다. 현재 설치된 애플리케이션을 활성화하려면, 다른 활성화 코드가 있어야 합니다
89479413	활성화 서버에서 오류 643이 반환되었습니다
89479414	활성화 서버에서 오류 644이 반환되었습니다
89479415	활성화 서버에서 오류 645이 반환되었습니다
89479416	활성화 서버에서 오류 646이 반환되었습니다
89479417	활성화 서버 1.0 버전이 필요합니다
89479418	잘못된 활성화 코드 형식
89479419	컴퓨터 시간이 활성화 서버 시간과 동기화되지 않았습니다
8947941A	잘못된 애플리케이션 버전
8947941B	서브스크립션이 만료되었습니다
8947941C	활성화 수를 초과했습니다
8947941D	잘못된 티켓 서명
8947941E	추가적인 데이터가 필요합니다
8947941F	데이터 검증 실패
89479420	서브스크립션 비활성
89479421	활성화 서버를 점검하고 있습니다
89479501	예상하지 못한 오류
89479502	잘못된 파라미터가 전송됨. 예: 빈 활성화 서버 주소 목록
89479503	잘못된 활성화 코드(잘못된 해시)
89479504	잘못된 사용자 ID
89479505	잘못된 사용자 암호
89479506	활성화 서버의 응답이 잘못됨
89479507	활성화 요청이 중단되었습니다
89479509	활성화 서버에서 빈 목록 포워딩이 반환되었습니다

부록. 애플리케이션 프로필

*프로필*은 Kaspersky Endpoint Security 구성 요소, 작업 또는 기능입니다. 프로필은 명령줄에서 애플리케이션을 관리하는 데 사용됩니다. `START`, `STOP`, `STATUS`, `STATISTICS` 및 `EXPORT` 명령을 실행할 때 프로필을 사용할 수 있습니다. 프로필을 사용해 애플리케이션 설정을 구성하거나(예, `STOP DeviceControl`) 작업을 실행할 수 있습니다(예, `START Scan_My_Computer`).

다음 프로필을 사용할 수 있습니다:

- `AdaptiveAnomaliesControl` - 적응형 이상 행위 제어.
- `AMSI` – AMSI 보호.
- `AntiCryptor`
- `BehaviorDetection` – 행동 탐지.
- `DeviceControl` – 장치 제어.
- `EntAppControl` – 애플리케이션 제어.
- `File_Monitoring` 또는 `FM` – 파일 위협 보호.
- `Firewall` 또는 `FW` – 방화벽.
- `HIPS` – 호스트 침입 방지.
- `IDS` - 네트워크 위협 보호.
- `IntegrityCheck` – 무결성 검사.
- `LogInspector` – 로그 검사.
- `Mail_Monitoring` 또는 `EM` – 메일 위협 보호.
- `Rollback` – 업데이트 롤백(애플리케이션을 Light Agent 모드로 설치했다면 프로필을 적용할 수 없습니다).
- `Scan_ContextScan` - 마우스 오른쪽 메뉴에서 검사.
- `Scan_IdleScan` – 백그라운드 검사.
- `Scan_Memory` – 커널 메모리 검사.
- `Scan_My_Computer` – 전체 검사.
- `Scan_Objects` – 사용자 지정 검사.
- `Scan_Qscan` – 운영 체제 시작 시 로드되는 개체 검사.
- `Scan_Removable_Drive` - 이동식 드라이브 검사.
- `Scan_Startup` 또는 `STARTUP` – 중요 영역 검사.
- `Updater` – 업데이트(애플리케이션을 Light Agent 모드로 설치했다면 프로필을 적용할 수 없습니다).

- `Web_Monitoring` 또는 `WM` – 웹 위협 보호.
- `WebControl` – 웹 제어.

또한, Kaspersky Endpoint Security는 서비스 프로필을 지원합니다. Kaspersky 기술 지원에 문의할 때 서비스 프로필이 필요할 수 있습니다.

REST API를 사용해 애플리케이션 관리

Kaspersky Endpoint Security를 사용하면 애플리케이션 설정을 구성하고, 검사를 실행하고, 안티 바이러스 데이터베이스를 업데이트하고, 타사 솔루션을 사용하여 다른 작업을 수행할 수 있습니다. Kaspersky Endpoint Security는 이러한 용도로 API를 제공합니다. Kaspersky Endpoint Security REST API는 HTTP를 통해 작동하며 일련의 요청/응답 방식으로 구성됩니다. 즉, 로컬 애플리케이션 인터페이스나 Kaspersky Security Center 관리 콘솔이 아닌 타사 솔루션을 통해 Kaspersky Endpoint Security를 관리할 수 있습니다.

REST API 사용을 시작하려면 REST API를 지원하는 Kaspersky Endpoint Security를 설치해야 합니다. REST 클라이언트 및 Kaspersky Endpoint Security가 동일한 컴퓨터에 설치되어 있어야 합니다.

Kaspersky Endpoint Security와 REST 클라이언트 간의 안전한 상호 작용을 보장하려면 다음과 같이 하십시오.

- REST 클라이언트 개발자의 권장 사항에 따라 무단 접근에 대한 REST 클라이언트의 보호를 구성합니다. DACL(Discretionary Access Control List)를 통해 쓰기에 대한 REST 클라이언트의 보호를 구성합니다.
- REST 클라이언트를 실행하려면 관리자 권한이 있는 별도의 계정을 사용합니다. 시스템에 대한 이 계정의 상호작용식 로그인을 거부합니다.

애플리케이션은 http://127.0.0.1 또는 http://localhost의 REST API를 통해 관리됩니다. REST API를 통해 Kaspersky Endpoint Security를 원격으로 관리할 수 없습니다.

REST API 문서 열기

REST API를 사용해 애플리케이션 설치

REST API를 사용해 애플리케이션을 관리하려면 REST API를 지원하는 Kaspersky Endpoint Security를 설치해야 합니다. REST API를 통해 Kaspersky Endpoint Security를 관리하는 경우에는 Kaspersky Security Center를 사용하여 애플리케이션을 관리할 수 없습니다.

REST API 지원으로 애플리케이션 설치 준비

Kaspersky Endpoint Security와 REST 클라이언트의 안전한 상호 작용을 위해서는 요청 식별을 구성해야 합니다. 이렇게 하려면 인증서를 설치한 다음 각 요청의 페이로드에 서명해야 합니다.

인증서 생성에는 OpenSSL 등을 사용할 수 있습니다.

예:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

키 길이가 2048비트 이상인 RSA 암호화 알고리즘을 사용합니다.

결과적으로 `cert.pem` 인증서 및 `key.pem` 개인 키를 얻게 됩니다.

REST API 지원으로 애플리케이션 설치

REST API가 지원되는 Kaspersky Endpoint Security를 설치하려면 다음을 수행합니다.

1. 명령줄 해석기(cmd.exe)를 관리자 권한으로 실행합니다.
2. Kaspersky Endpoint Security 11.2.0 버전 이상이 있는 배포 패키지 폴더로 이동합니다.
3. 다음 설정을 사용하여 Kaspersky Endpoint Security를 설치합니다:

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     REST API를 사용하는 애플리케이션을 관리하기 위한 사용자 이름입니다. 사용자 이름을 `<DOMAIN>\<UserName>` 형식으로 입력합니다(예: `RESTAPI_User=COMPANY\Administrator`). 이 계정으로만 REST API를 통해 애플리케이션을 관리할 수 있습니다. REST API로 작업할 사용자를 하나만 선택할 수 있습니다.
   - `RESTAPI_Port=<port>`

     REST API를 통해 애플리케이션을 관리하는 데 사용되는 포트입니다. 기본적으로 포트 6782가 사용됩니다. 포트가 사용 가능한 상태인지 확인하십시오. 옵션 파라미터.
   - `RESTAPI_Certificate=<path to certificate>`

     요청 식별을 위한 인증서(예: `RESTAPI_Certificate=C:\cert.pem`).

     애플리케이션 설치 후 인증서를 설치하거나 인증서 만료 후 인증서를 업데이트할 수 있습니다.

     REST API 요청 식별을 위한 인증서를 설치하는 방법

     1. Kaspersky Endpoint Security 자기 보호 비활성화

        자기 보호 메커니즘은 하드 드라이브의 애플리케이션 파일, 메모리의 프로세스, 시스템 레지스트리의 항목이 변경 또는 삭제되는 것을 방지합니다.
     2. REST API 설정이 포함된 레지스트리 키로 이동합니다:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. 인증서 경로를 입력합니다(예: `Certificate = C:\Folder\cert.pem`).
     4. Kaspersky Endpoint Security 자기 보호를 활성화합니다.
     5. 애플리케이션을 다시 시작합니다.
   - `AdminKitConnector=1`

     관리 시스템을 사용하여 애플리케이션을 관리합니다. 관리는 기본적으로 허용됩니다.

setup.ini 파일을 사용하여 REST API를 사용하기 위한 설정을 정의할 수도 있습니다.

```
예:
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
/pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
```

이후 REST API를 통해 애플리케이션을 관리할 수 있습니다. 작동을 검증하려면 GET 요청을 사용하여 REST API 문서를 엽니다.

예:
```
GET http://localhost:6782/kes/v1/api-docs
```

REST API 지원으로 애플리케이션을 설치했다면, Kaspersky Endpoint Security가 웹 콘솔 설정에 웹 리소스 접근에 대한 허용 규칙을 자동으로 생성합니다(*REST API용 서비스 규칙*). 이 규칙은 Kaspersky Endpoint Security가 REST 클라이언트에 상시 접근할 수 있도록 하는 데 필요합니다. 예를 들어, 웹 리소스에 대한 사용자 접근을 제한했다면 REST API를 통한 애플리케이션 관리에 영향을 주지 않습니다. 규칙을 제거하거나 *REST API 서비스 규칙* 설정을 변경하는 것은 권장하지 않습니다. 규칙을 제거하면 Kaspersky Endpoint Security가 애플리케이션 다시 시작 후에 이를 복원합니다.

API를 사용해 작업 수행

암호 보호를 사용하여 REST API를 통한 애플리케이션 접근을 제한하는 것을 불가능합니다. 예를 들어 REST API를 통해 사용자가 보호를 비활성화하는 시도를 차단할 수 없습니다. REST API를 통해 암호 보호를 구성하고 로컬 인터페이스를 통해 애플리케이션에 대한 사용자 접근을 제한할 수는 있습니다.

REST API를 통해 애플리케이션을 관리하려면 REST API를 지원하는 애플리케이션을 설치할 때 지정한 계정으로 REST 클라이언트를 실행해야 합니다. REST API로 작업할 사용자를 하나만 선택할 수 있습니다.

REST API 문서 열기

REST API를 통해 애플리케이션을 관리하는 것은 다음 단계로 구성됩니다:

1. 애플리케이션 설정의 현재 값을 가져옵니다. 그렇게 하려면 GET 요청을 보냅니다.
   예:
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```
2. 애플리케이션에서 설정의 구조와 값으로 응답을 보냅니다. Kaspersky Endpoint Security는 XML- 및 JSON 형식을 지원합니다.
   예:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```
3. 애플리케이션 설정을 편집합니다. GET 요청에 대한 응답으로 수신된 설정 구조를 사용합니다.
   예:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```
4. 애플리케이션 설정(페이로드)을 JSON으로 저장합니다(payload.json).
5. PKCS7 형식으로 JSON에 서명합니다.
   예:
   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
   signed_payload.pem
   ```

결과적으로 요청 페이로드가 포함된 서명된 파일을 얻습니다(`signed_payload.pem`).

6. 애플리케이션 설정을 편집합니다. 그렇게 하려면 POST 요청을 보내고 요청 페이로드와 함께 서명된 파일을 첨부합니다(`signed_payload.pem`).

애플리케이션은 새 설정을 적용하고 애플리케이션 구성 결과가 포함된 응답을 보냅니다(응답은 비어 있을 수 있음). GET 요청을 사용하여 설정이 업데이트되었는지 확인할 수 있습니다.

애플리케이션에 대한 정보 출처

이 섹션에는 애플리케이션에 대한 정보 출처를 설명합니다.

문제의 중요성과 긴급성에 따라 가장 편리한 정보 출처를 선택할 수 있습니다.

Kaspersky 웹사이트의 Kaspersky Endpoint Security 페이지

Kaspersky Endpoint Security 페이지에서 애플리케이션과 기능, 특징과 같은 일반적인 정보를 확인할 수 있습니다.

Kaspersky Endpoint Security 페이지에는 온라인 스토어로의 링크를 포함하고 있습니다. 그곳에서 애플리케이션을 구매하거나 갱신할 수 있습니다.

기술 지원 기술 자료 웹사이트의 Kaspersky Endpoint Security 페이지

*기술 자료*는 기술 지원 웹사이트에 있는 섹션입니다.

기술 자료의 Kaspersky Endpoint Security 페이지에서는 애플리케이션의 구매, 설치 및 사용에 관한 유용한 정보, 권장 사항 및 자주 묻는 질문에 대한 답변을 참조할 수 있습니다.

기술 자료 문서에는 Kaspersky Endpoint Security뿐만 아니라 다른 Kaspersky 애플리케이션에 관련된 질문에 대한 답변이 있습니다. 기술 자료에 등록된 게시글에는 기술 지원의 새소식도 있을 수 있습니다.

포럼에서 Kaspersky 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.

기술 지원 서비스에 문의

애플리케이션 문서 또는 그 외 Kaspersky Endpoint Security에 대한 정보 출처에서 문제에 대한 해결 방법을 찾을 수 없을 시 기술 지원에 문의할 것을 권장합니다. 기술 지원에서 Kaspersky Endpoint Security 설치 및 사용에 관한 질문에 답해 드립니다.

Kaspersky는 애플리케이션 수명 주기 동안 Kaspersky Endpoint Security에 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 기술 지원 전문가에게 문제에 대해 알리면 문제 해결을 위해 기술 지원 전문가가 *추적 파일*을 생성하도록 요청할 수 있습니다. 추적 파일을 통해 애플리케이션의 단계별 수행 과정을 추적하여 오류가 발생한 애플리케이션 동작 구간을 파악할 수 있습니다.

기술 지원 전문가는 또한 운영 체제와 컴퓨터에서 실행 중인 프로세스에 대한 추가 정보 및 애플리케이션 구성 요소의 동작에 대한 자세한 리포트를 요청할 수도 있습니다.

진단 툴을 실행할 때 기술 지원 전문가는 다음과 같이 애플리케이션 설정 변경을 요구할 수 있습니다:

- 확장된 진단 정보를 얻는 기능 활성화.
- 표준 사용자 인터페이스를 통해 액세스할 수 없는 특수 설정을 변경하여 애플리케이션의 개별 구성 요소를 구성합니다.
- 진단 정보의 저장 설정 변경.
- 네트워크 트래픽 차단 및 로깅 구성.

기술 지원 전문가는 이러한 작업을 수행하기 위해 필요한 모든 정보를 제공하고(단계별 순서 설명, 수정되는 설정, 구성 파일, 스크립트, 추가 명령줄 기능, 디버깅 모듈, 특수 목적의 유틸리티 등) 디버깅 목적을 위해 사용된 데이터의 범위에 대해 알립니다. 확장 진단 정보는 사용자의 컴퓨터에 저장됩니다. 데이터는 Kaspersky로 자동 전송되지 않습니다.

위에서 나열된 작업은 기술 지원 전문가의 지시와 감독하에 수행되어야 합니다. 온라인 도움말에 나와 있거나 기술 지원에서 권장하는 방법이 아닌 다른 방식으로 직접 애플리케이션 설정을 변경하면 운영 체제의 속도가 느려지고 충돌이 발생하거나, 컴퓨터의 보호 수준이 낮아지고, 처리하는 정보의 가용성과 무결성이 손상될 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.

인증 에이전트의 추적 파일을 제외한 추적 로그 파일은 `%ProgramData%\Kaspersky Lab\KES.14.0\Traces` 폴더에 저장됩니다.

추적 파일은 다음 이름 형식을 가집니다: `KES<14.0_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

추적 파일에 저장된 데이터를 볼 수 있습니다.

모든 추적 파일에는 다음 일반 데이터가 포함됩니다.

- 이벤트 시간
- 실행 스레드 수

  > 인증 에이전트 추적 파일에는 이 정보가 들어있지 않습니다.

- 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).
- 컴퓨터에 설치된 하드웨어의 데이터(예: BIOS/UEFI 펌웨어 데이터). 이 데이터는 Kaspersky 디스크 암호화를 수행할 때 추적 파일에 작성됩니다.
- 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).
- 사용자가 방문하는 웹사이트와 이들 웹사이트의 리디렉션. 이 데이터는 애플리케이션이 웹사이트를 검사할 때 추적 파일에 작성됩니다.
- 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.

- 메시지 제목, ID, 보낸 사람 이름, 메시지를 보낸 사람의 소셜 네트워크 웹 페이지 주소. 이 데이터는 웹 제어 구성 요소를 사용할 경우 추적 파일에 작성됩니다.
- 네트워크 트래픽 데이터. 이 데이터는 트래픽 모니터링 구성 요소(예: 웹 제어)가 활성화된 경우 추적 파일에 작성됩니다.
- Kaspersky 서버로부터 수신된 데이터(예: 안티바이러스 데이터베이스 버전).
- Kaspersky Endpoint Security 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 문제해결에 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.

성능 추적 파일의 컨텐츠

성능 추적 파일은 다음 이름 형식을 가집니다: `KES<14.0_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

일반 데이터 이외에도 성능 추적 파일에는 프로세서의 부하에 대한 정보, 운영 체제와 애플리케이션의 로딩 시간에 대한 정보, 실행 중인 프로세스에 대한 정보가 포함됩니다.

AMSI 보호 구성 요소 추적 파일의 내용

`AMSI.log` 추적 파일에는 일반 데이터 외에도 타사 애플리케이션의 요청에 대해 수행된 검색 결과에 대한 정보가 포함되어 있습니다.

메일 위협 보호 구성 요소의 추적 파일 내용

`mcou.OUTLOOK.EXE.log` 추적 파일에는 일반 데이터 외에도 이메일 주소 및 이메일 메시지의 일부가 포함될 수 있습니다.

마우스 오른쪽 메뉴에서 검사 구성 요소의 추적 파일 내용

`shellex.dll.log` 추적 파일에는 일반 정보와 함께 검사 작업의 완료에 대한 정보와 애플리케이션을 디버깅하는 데 필요한 데이터가 들어 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-kes_windows-<type of trace file>.DESKTOP-<date of file update>.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 Endpoint Security 인터페이스(암호 보호)의 잠금을 해제하기 위한 KLAdmin 사용자 암호.
- Kaspersky Endpoint Security 인터페이스(암호 보호)의 잠금을 해제하기 위한 임시 암호.
- SMTP 메일 서버에 대한 사용자 이름 및 암호(이메일 알림).
- 프록시 서버에 대한 사용자 이름 및 암호(프록시 서버).
- *애플리케이션 구성 요소 변경* 작업의 사용자 이름 및 암호입니다.
- Kaspersky Endpoint Security 작업 및 정책 속성에 지정된 계정 인증 정보 및 경로.

인증 에이전트 추적 파일 내용

인증 에이전트 추적 파일은 System Volume Information 폴더에 저장되며 이름은 다음과 같습니다: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

일반 데이터 이외에 인증 에이전트 추적 파일에는 인증 에이전트의 작동 및 인증 에이전트를 통해 사용자가 수행하는 작업에 대한 정보가 포함됩니다.

애플리케이션 동작 추적 로그

*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 데이터(예: SRV.log, WD.log 및 기타)가 포함된 파일 세트를 생성합니다.

애플리케이션 추적 로그는 Kaspersky 기술 지원의 감독하에 수행해야 합니다.

애플리케이션 추적 파일을 생성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 열리는 창에서 **지원 도구** 버튼을 클릭합니다.
3. **애플리케이션 추적 로그 사용** 토글로 애플리케이션 동작 추적을 사용하거나 중지합니다.
4. **추적 로그** 드롭다운 목록에서 애플리케이션 추적 모드를 선택합니다:
   - **크기 제한 있음**. 제한된 크기의 파일 세트에 추적 로그를 저장하고 최대 크기에 도달하면 이전 파일을 덮어씁니다. 이 모드를 선택하면 순환식 저장 모드의 최대 파일 세트 개수와 각 파일 세트의 최대 크기를 정의할 수 있습니다.

     기본적으로 애플리케이션에는 다섯 세트의 추적 파일이 저장됩니다. 각 파일 세트 크기는 3072MB입니다. 이러한 방식으로 추적 파일을 저장하는 데 15GB의 디스크 여유 공간이 필요합니다.
   - **제한 없음**. 하나의 추적 파일을 저장합니다(크기 제한 없음).
5. **레벨** 드롭다운 목록에서 추적 레벨을 선택합니다.
   - **일반**은 추적 파일이 모든 오류, 경고에 관한 메시지는 물론 애플리케이션의 정상 작동에 관한 정보도 저장한다는 뜻입니다(기본값).
   - **정밀**은 추적 파일이 애플리케이션의 작동에 관한 모든 정보를 저장한다는 뜻입니다.

   명령줄에서 애플리케이션 추적 설정을 관리하는 경우 추가 추적 레벨을 사용할 수 있습니다. 기술 지원 전문가가 알려준 추적 레벨을 선택합니다. 기술 지원 전문가가 필요한 추적 로그 레벨을 알려주지 않은 경우에는 **일반**을 선택합니다.

   명령줄에 애플리케이션 추적 로그가 활성화되고 추적 레벨이 **일반** 또는 **상세** 이외의 값으로 설정된 경우, **레벨** 드롭다운 목록은 **일반**으로 설정됩니다.
6. 추적 프로세스를 중지하려면 **지원 도구** 창으로 돌아가 추적을 중지합니다.

setup.ini 파일 사용과 명령줄을 사용한 애플리케이션 설치 시에도 추적 파일을 생성할 수도 있습니다.

결과적으로 애플리케이션 동작 추적 파일이 `%ProgramData%\Kaspersky Lab\KES.14.0\Traces` 폴더에 생성됩니다. 추적 파일이 생성되면 이 파일을 Kaspersky 기술 지원에 전송합니다.

Kaspersky Endpoint Security는 애플리케이션 제거되면 추적 파일을 자동으로 삭제합니다. 이 파일은 수동으로 삭제할 수도 있습니다. 그러려면 먼저 추적 로그를 비활성화하고 애플리케이션을 중지해야 합니다.

애플리케이션 성능 추적 로그

Kaspersky Endpoint Security에서는 애플리케이션을 사용하는 동안 컴퓨터 운영 문제에 관한 정보를 수신할 수 있습니다. 예를 들어, 애플리케이션을 설치한 후에 운영 체제 로드 지연에 관한 정보를 받을 수 있습니다. 이를 위해 Kaspersky Endpoint Security는 성능 추적 파일을 생성합니다. *성능 추적 로그*는 Kaspersky Endpoint Security의 성능 문제 진단을 위해 애플리케이션이 수행하는 동작을 기록한 것입니다. 정보 수신을 위해 Kaspersky Endpoint Security는 Windows용 이벤트 추적 서비스(ETW)를 사용합니다. Kaspersky 기술 지원에서는 Kaspersky Endpoint Security의 문제를 진단하고 이러한 문제의 원인을 파악합니다.

애플리케이션 추적 로그는 Kaspersky 기술 지원의 감독하에 수행해야 합니다.

성능 추적 파일을 생성하려면 다음과 같이 하십시오.

1. 메인 애플리케이션 창에서 버튼을 클릭합니다.
2. 열리는 창에서 **지원 도구** 버튼을 클릭합니다.
3. **성능 추적 로그 사용** 토글로 애플리케이션 성능 추적을 활성화 또는 비활성화합니다.
4. **추적 로그** 드롭다운 목록에서 애플리케이션 추적 모드를 선택합니다:
   - **크기 제한 있음**. 제한된 크기의 파일에 추적 로그를 저장하고 최대 크기에 도달하면 이전 파일을 덮어씁니다. 이 모드를 선택하면 각 파일의 최대 크기를 정의할 수 있습니다.
   - **제한 없음**. 하나의 추적 파일을 저장합니다(크기 제한 없음).
5. **레벨** 드롭다운 목록에서 추적 레벨을 선택합니다.
   - **빠름**. Kaspersky Endpoint Security가 성능과 관련된 가장 중요한 운영 체제 프로세스를 분석합니다.
   - **정밀**. Kaspersky Endpoint Security가 성능과 관련된 모든 운영 체제 프로세스를 분석합니다.
6. **추적 로그 유형** 드롭다운 목록에서 추적 로그 유형을 선택합니다:
   - **기본 정보**. Kaspersky Endpoint Security가 운영 체제가 실행되는 동안 프로세스를 분석합니다. 운영 체제를 로드한 후에도 문제가 지속되는 경우(예: 브라우저에서 인터넷에 접근할 수 없음) 이 추적 로그 유형이 효과적입니다.
   - **재시작 시**. Kaspersky Endpoint Security가 운영 체제가 로드되는 동안 프로세스를 분석합니다. 운영 체제가 로드되면 Kaspersky Endpoint Security가 추적 로그를 중지합니다. 발생한 문제가 운영 체제의 지연된 로드와 관련이 있는 경우 이 추적 로그가 효과적입니다.
7. 컴퓨터를 다시 시작하고 문제를 재현해 보십시오.
8. 추적 프로세스를 중지하려면 지원 도구 창으로 돌아가 추적을 중지합니다.

결과적으로 성능 추적 파일이 `%ProgramData%\Kaspersky Lab\KES.14.0\Traces` 폴더에 생성됩니다. 추적 파일이 생성되면 이 파일을 Kaspersky 기술 지원에 전송합니다.

덤프 기록

덤프 파일에는 덤프 파일 생성 당시 Kaspersky Endpoint Security 프로세스의 작동 메모리에 관한 모든 정보가 포함됩니다.

저장된 덤프 파일에는 기밀 데이터가 포함되어 있을 수 있습니다. 데이터에 대한 접근을 제어하려면 덤프 파일의 보안을 독립적으로 보장해야 합니다.

덤프 파일은 애플리케이션이 사용 중일 때는 컴퓨터에 저장되며 애플리케이션이 제거되면 영구적으로 삭제됩니다. 덤프 파일은 `%ProgramData%\Kaspersky Lab\KES.14.0\Traces` 폴더에 저장됩니다.

관리 콘솔(MMC)에서 덤프 기록을 활성화하는 방법

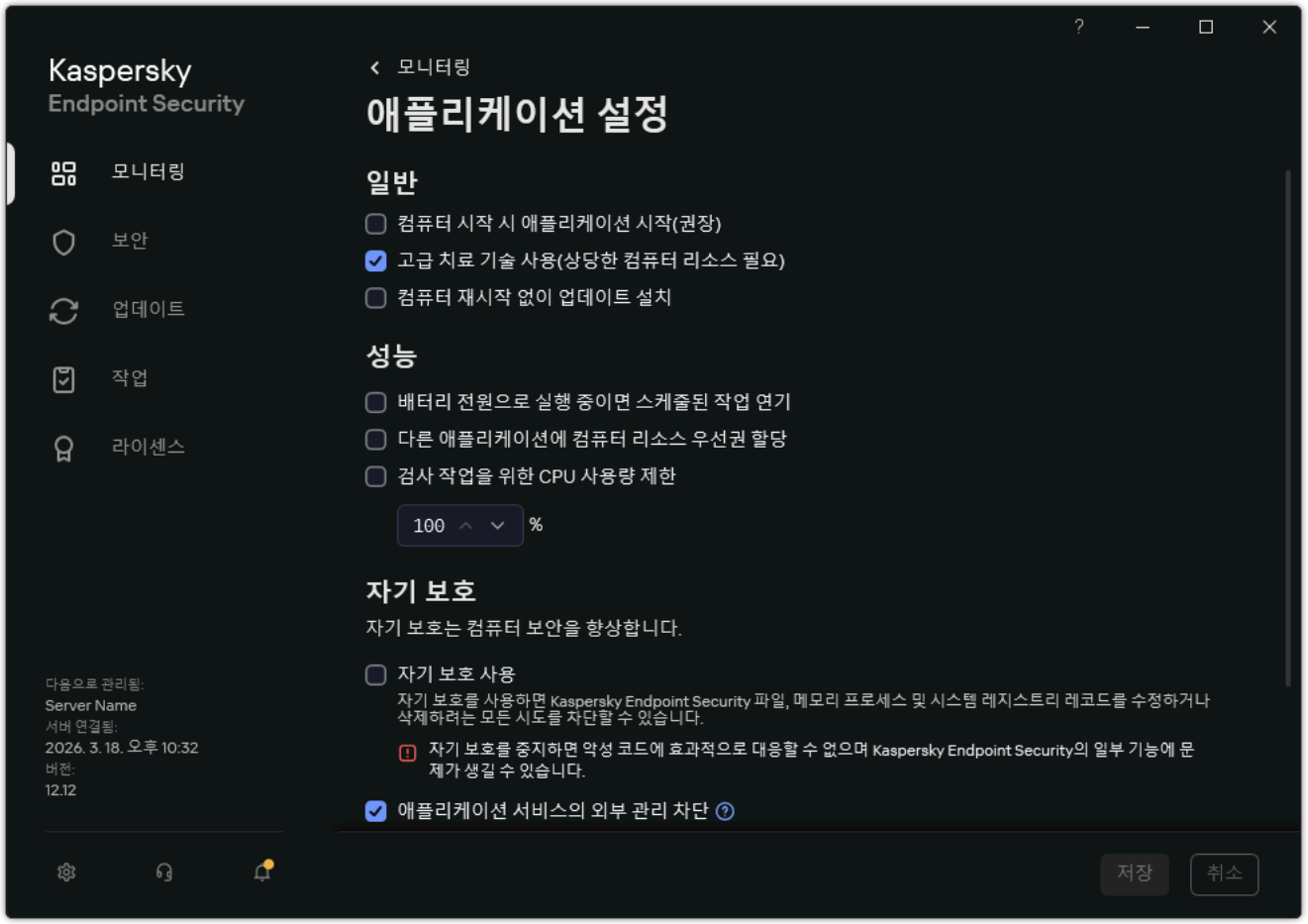
1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.
3. 정책 창에서 **일반 설정 → 애플리케이션 설정**을 차례로 선택합니다.
4. **디버그 정보** 블록에서 **설정** 버튼을 누릅니다.
5. 창이 열리면 **덤프 기록 사용** 확인란으로 애플리케이션 덤프 기록을 사용하거나 중지합니다.
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 덤프 기록을 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리 → 정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정 → 기술 지원**으로 갑니다.
5. **디버그 정보** 블록에서 **덤프 기록 활성화됨** 확인란으로 애플리케이션 덤프 기록을 사용하거나 중지합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 덤프 기록을 활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

3. **디버그 정보** 블록에서 **덤프 기록 사용** 확인란으로 애플리케이션 덤프 기록을 사용하거나 중지합니다.
4. 변경 사항을 저장합니다.

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.

관리 콘솔(MMC)에서 덤프 파일 및 추적 파일 보호를 활성화하는 방법

1. Kaspersky Security Center 관리 콘솔 트리에서 **정책**을 선택합니다.
2. 필요한 정책을 선택하고 더블 클릭하여 정책 속성을 엽니다.

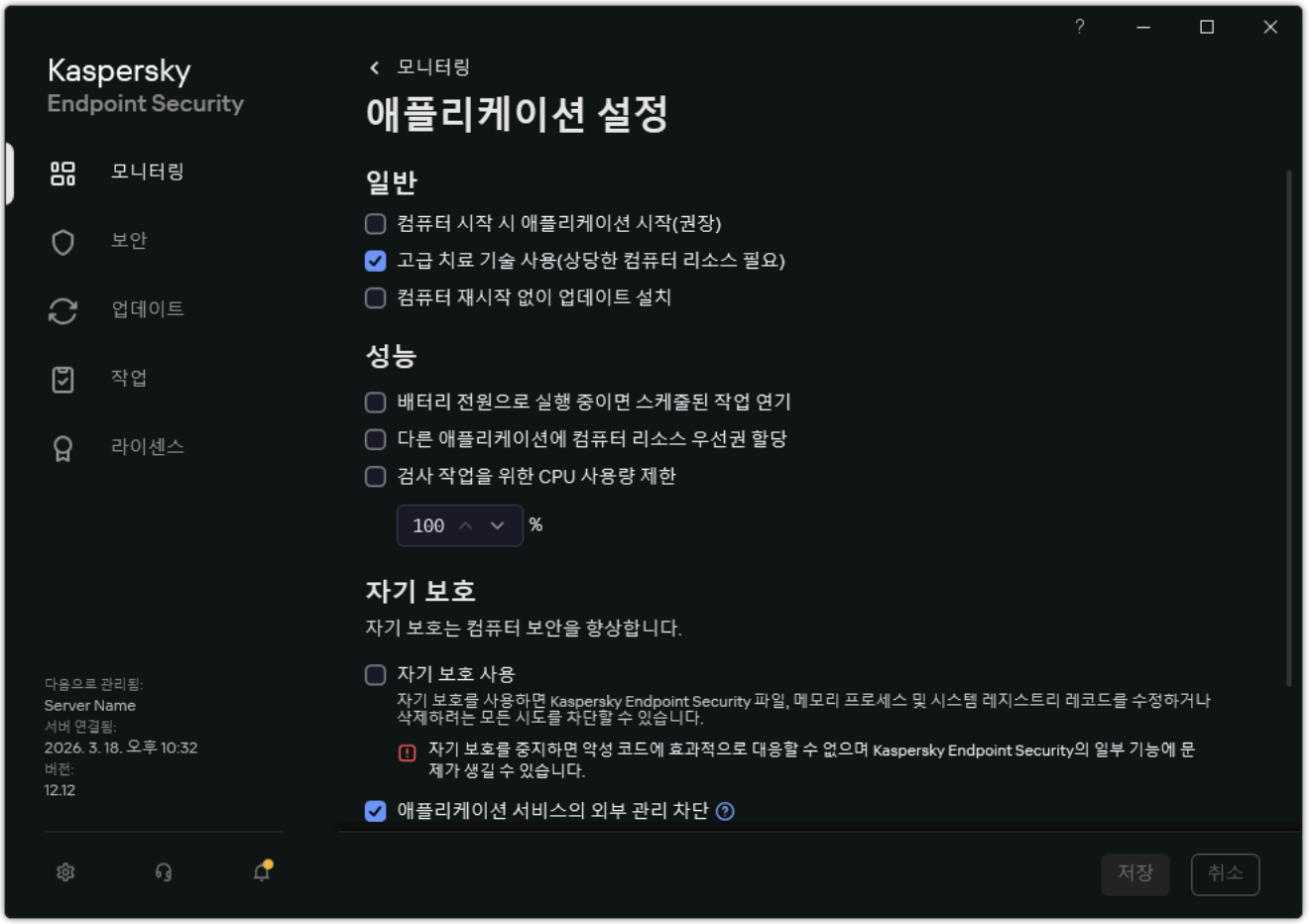
3. 정책 창에서 **일반 설정** → **애플리케이션 설정**을 차례로 선택합니다.
4. **디버그 정보** 블록에서 **설정** 버튼을 누릅니다.
5. 창이 열리면 **덤프 및 추적 파일 보호 사용** 확인란으로 파일 보호를 사용하거나 중지합니다.
6. 변경 사항을 저장합니다.

웹 콘솔 및 Cloud Console에서 덤프 파일 및 추적 파일 보호를 활성화하는 방법

1. 웹 콘솔의 메인 창에서 **에셋 관리** → **정책**을 선택합니다.
2. Kaspersky Endpoint Security 정책 이름을 클릭합니다.
   정책 속성 창이 열립니다.
3. **애플리케이션 설정** 탭을 선택합니다.
4. **일반 설정** → **기술 지원**으로 갑니다.
5. **디버그 정보** 블록에서 **덤프 및 추적 파일 보호 활성화됨** 확인란으로 파일 보호를 사용하거나 중지합니다.
6. 변경 사항을 저장합니다.

애플리케이션 인터페이스에서 덤프 파일 및 추적 파일 보호를 활성화하는 방법

1. 메인 애플리케이션 창에서 ⚙ 버튼을 클릭합니다.
2. 애플리케이션 설정 창에서 **일반 설정** → **애플리케이션 설정**을 선택합니다.



Kaspersky Endpoint Security for Windows 설정

3. **디버그 정보** 블록에서 **덤프 및 추적 파일 보호 사용** 확인란으로 파일 보호를 사용하거나 중지합니다.

4. 변경 사항을 저장합니다.

보호가 활성일 때 쓰여진 덤프 및 추적 파일은 보호 기능이 중지된 후에도 계속 보호됩니다.

OS 데이터 가져오기(Kaspersky Get System Info)

Kaspersky Endpoint Security 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.

제한 및 경고

Kaspersky Endpoint Security에는 애플리케이션 동작에 큰 영향을 미치지 않는 몇 가지 제한이 있습니다.

애플리케이션 설치

- Microsoft Windows 10, Microsoft Windows Server 2016, Microsoft Windows Server 2019 운영 체제 지원에 대한 상세 정보는 기술 지원 기술 자료 웹사이트를 참조하십시오.
- Microsoft Windows Server 11 및 Microsoft Windows Server 2022 운영 체제 지원에 대한 상세 정보는 기술 지원 기술 자료 웹사이트를 참고하십시오.
- 감염된 컴퓨터에 설치 시 애플리케이션이 컴퓨터 검사를 실행해야 한다는 사실을 사용자에게 알리지 않습니다. 애플리케이션 활성화에 문제가 발생할 수 있습니다. 이러한 문제를 해결하려면 중요 영역 검사를 시작하십시오.
- 비 ASCII 문자(러시아어 문자 등)가 setup.ini 및 setup.reg 파일에 사용될 시 notepad.exe를 사용하여 파일을 편집하고 파일을 UTF-16LE 인코딩으로 저장하는 것이 좋습니다. 다른 인코딩은 지원하지 않습니다.
- 이 애플리케이션은 설치 패키지 설정에서 애플리케이션 설치 경로를 지정할 때 비 ASCII 문자 사용을 지원하지 않습니다.
- CFG 파일에서 애플리케이션 설정 가져오기 시 Kaspersky Security Network 참여를 정의하는 설정값이 적용되지 않습니다. 설정을 가져온 후 Kaspersky Security Network 진술문의 텍스트를 읽고 Kaspersky Security Network 참여에 대한 동의를 확인하십시오. 애플리케이션 인터페이스 또는 애플리케이션 배포 키트가 포함된 폴더의 ksn_*.txt 파일에서 진술문의 텍스트를 읽을 수 있습니다.
- 암호화(FLE 또는 FDE) 또는 장치 제어 구성 요소를 제거했다가 다시 설치하려면 다시 설치하기 전에 시스템을 다시 시작해야 합니다.
- Microsoft Windows 10 운영 체제를 사용한다면 파일 레벨 암호화(FLE) 구성 요소를 제거한 후 시스템을 다시 시작해야 합니다.
- 개별 애플리케이션 구성 요소를 제거할 경우(예: *애플리케이션 구성 요소 변경* 작업) 컴퓨터를 다시 시작해야 합니다.
- *애플리케이션 구성 요소 변경* 작업의 속성에서 설치 모드를 전환할 때(**개별 모드** / **조합된 모드**), 모드 간 구성 요소 집합의 동기화는 지원되지 않습니다. 작업 속성을 다시 연 후에 애플리케이션에서 모드 간 구성 요소 집합 동기화를 수행합니다.
- 애플리케이션의 설치는 *이름이 없거나 읽을 수 없는 애플리케이션이 컴퓨터에 설치됨*이라는 오류와 함께 종료될 수 있습니다. 이것은 호환되지 않는 애플리케이션이나 그 조각이 컴퓨터에 남아있다는 뜻입니다. 호환되지 않는 애플리케이션의 아티팩트를 제거하려면 Kaspersky CompanyAccount를 통해 상황을 자세하게 설명한 요청을 Kaspersky 기술 지원에 보냅니다.
- Kaspersky Endpoint Security 제거를 취소한 경우 컴퓨터를 다시 시작한 후 애플리케이션 복구를 시작하십시오.
- 이 애플리케이션에는 Microsoft .NET Framework 4.0 이상이 필요합니다. Microsoft .NET Framework 4.6.1에는 취약점이 있습니다. Microsoft .NET Framework 4.6.1을 사용한다면 보안 업데이트를 설치해야 합니다. Microsoft .NET Framework 보안 업데이트에 대한 자세한 내용은 Microsoft 기술 지원 웹사이트를 참조하십시오.
- 서버 운영 체제에서 Kaspersky Endpoint Agent 구성 요소가 선택된 상태에서 *Windows Installer Coordinator 오류* 창과 함께 설치가 실패하면 Microsoft 지원 웹사이트의 지침을 참조하십시오.

- 애플리케이션이 비 상호작용 모드로 로컬 설치된 경우 제공된 setup.ini 파일을 사용하여 설치된 구성 요소를 교체합니다.

- Windows 7의 일부 구성에서는 Kaspersky Endpoint Security for Windows를 설치한 후에도 Windows Defender가 계속 작동합니다. 시스템 성능 저하를 방지하려면 Windows Defender를 직접 중지하는 것이 좋습니다.

- Kaspersky Security for Windows Server(KSWS)와 Windows Defender 애플리케이션이 설치된 서버에 Kaspersky Endpoint Security for Windows 설치 시, 시스템을 다시 시작해야 합니다. 시스템 다시 시작 없이 애플리케이션을 설치하도록 활성화했더라도 시스템을 다시 시작해야 합니다. Windows Defender for Windows Server는 Kaspersky Endpoint Security for Windows와 호환되지 않는 소프트웨어 목록에 포함됩니다. 애플리케이션을 설치하기 전에 설치 프로그램이 Windows Defender for Windows Server를 제거합니다. 호환되지 않는 소프트웨어 제거 시 시스템을 다시 시작해야 합니다.

- Kaspersky Security for Windows Server(KSWS)가 설치된 서버에 Kaspersky Endpoint Security for Windows(KES)를 설치하기 전에, KSWS 암호 보호를 꺼야 합니다. KSWS에서 KES로 마이그레이션 시, 애플리케이션 설정에서 암호 보호를 활성화하십시오.

- Windows 7이나 Veeam Backup & Replication 소프트웨어를 배포한 Windows Server 2008 R2를 사용하는 컴퓨터에 애플리케이션을 설치하려면, 컴퓨터를 재시작하고 설치를 다시 실행해야 할 수 있습니다.

- KSOS 빌드 21.16.*.*부터 암호 보호가 활성화된 상태로 Kaspersky Small Office Security(KSOS)에서 Kaspersky Endpoint Security(KES)로 마이그레이션할 수 있습니다. KSOS 이전 버전에서 마이그레이션하려면 암호 보호를 끄거나 KSOS를 수동으로 제거해야 합니다. 암호 보호가 비활성화된 상태에서 KSOS에서 KES로의 마이그레이션이 정상적으로 동작합니다.

- 부팅 가능한 이동식 드라이브에는 Kaspersky Endpoint Security를 설치할 수 없습니다. 설치할 때 Kaspersky Endpoint Security가 *유효하지 않은 폴더 또는 드라이브를 선택했습니다 오류 메시지를 표시합니다.애플리케이션은 로컬 하드 드라이브에 설치해야 합니다.* 타사 도구를 사용하여 이동식 드라이브에 애플리케이션을 설치한다면 부팅 프로세스 중에 운영 체제 충돌(BSOD)이 발생할 수 있습니다. 즉, Kaspersky Endpoint Security는 Windows To Go 및 유사한 솔루션을 지원하지 않습니다. 이동식 드라이브에서 컴퓨터를 검사하려면 무료 Kaspersky Rescue Disk 애플리케이션을 사용할 수 있습니다.

- 멀티 사용자 RDP 세션이 있는 터미널 서버에 네트워크 구성 요소와 함께 Kaspersky Endpoint Security를 설치하기 위해서는 몇 가지 특별하게 고려해야 할 사항이 있습니다. 운영 체제는 관리자 세션이 종료되면 모든 사용자 세션을 강제로 종료합니다. 터미널 서버에 연결하려면 서버를 다시 시작하거나 시스템에 로컬로 로그인해야 합니다. 이러한 동작은 Windows 운영 체제 작동 방식의 특성에 따른 것입니다.

- Kaspersky Security Center 16.0 또는 Kaspersky Security Center 16.1에 Kaspersky Endpoint Security for Windows(빌드 12.11.0.2004) 및 Kaspersky Endpoint Security for Linux(빌드 12.4.0.1354) 웹 플러그인이 설치될 경우 Kaspersky Endpoint Security for Windows 웹 플러그인을 버전 12.11.0.6004로 업그레이드하면 Kaspersky Endpoint Security for Linux 정책이 제대로 작동하지 않을 수 있습니다.

  잠재적인 해결 방법: **설정 → 웹 플러그인** 창으로 이동하여 목록에서 Kaspersky Endpoint Security for Windows 웹 플러그인, Kaspersky Endpoint Security for Linux 웹 플러그인 및 Unified Protection and Management Plug-in을 제거합니다. 그런 다음, Kaspersky Endpoint Security for Linux 웹 플러그인 및 Kaspersky Endpoint Security for Windows 웹 플러그인을 차례로 설치합니다.

- 웹 콘솔에서 Kaspersky Endpoint Security 12.11 for Windows의 설치 패키지 속성에 구성 요소 목록이 잘못 표시됩니다. 이 버전의 애플리케이션에서는 별도의 구성 요소인 Anti-Cryptor를 사용할 수 없습니다. 외부 암호화 기능으로부터 공유 폴더를 보호하는 기능은 행동 탐지 구성 요소에 포함됩니다. Kaspersky Endpoint Security 12.12 for Windows에서는 이 기능이 별도의 구성 요소입니다. 동시에 관리 콘솔(MMC)에는 구성 요소 목록이 올바르게 표시됩니다.

애플리케이션 업그레이드

- 애플리케이션 버전 11.0.0부터 Kaspersky Endpoint Security for Windows MMC 플러그인을 이전 버전의 플러그인 위에 설치할 수 있습니다. 이전 버전의 플러그인으로 돌아가려면 현재 플러그인을 삭제하고 이전 버전의 플러그인을 설치하십시오.

- Kaspersky Endpoint Security for Windows 11.0.0 또는 11.0.1을 업그레이드할 때 *데이터베이스 및 애플리케이션 모듈 업데이트*, *중요 영역 검사*, *사용자 지정 검사* 및 *애플리케이션 무결성 검사* 작업에 대한 로컬 작업 스케줄 설정은 저장되지 않습니다.

- Windows 10 버전 1903 및 1909를 사용하는 컴퓨터에서 Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3(빌드 10.3.3.275), Service Pack 2 Maintenance Release 4(빌드 10.3.3.304), 파일 레벨 암호화(FLE) 구성 요소가 설치된 11.0.0 및 11.0.1 업그레이드할 시 오류가 발생할 수 있습니다. 이는 Windows 10 버전 1903 및 1909에서 이러한 Windows용 Kaspersky Endpoint Security 버전에 대한 파일 암호화를 지원하지 않기 때문입니다. 이 업그레이드를 설치하기 전에 파일 암호화 구성 요소를 제거하는 것이 좋습니다.

- 이 애플리케이션에는 Microsoft .NET Framework 4.0 이상이 필요합니다. Microsoft .NET Framework 4.6.1에는 취약점이 있습니다. Microsoft .NET Framework 4.6.1을 사용한다면 보안 업데이트를 설치해야 합니다. Microsoft .NET Framework 보안 업데이트에 대한 자세한 내용은 Microsoft 기술 지원 웹사이트를 참조하십시오.

- Kaspersky Endpoint Security 업그레이드 시, Kaspersky Security Network 진술문을 수락할 때까지 애플리케이션이 KSN 사용을 비활성화합니다. 또한 Kaspersky Security Center에서 컴퓨터 상태가 *심각*으로 바뀔 수 있으며, *KSN 서버 이용 불가능* 이벤트가 수신됩니다. Kaspersky Managed Detection and Response를 사용한다면 솔루션 작동 위반 사항에 관한 이벤트를 수신합니다. Kaspersky Managed Detection and Response가 작동하려면 KSN을 사용해야 합니다. Kaspersky Endpoint Security는 관리자가 KSN 이용 약관을 수락하는 정책을 적용한 후에 KSN 사용을 활성화합니다. Kaspersky Security Network 진술문을 수락하면 Kaspersky Endpoint Security가 작동을 재개합니다.

- 다시 시작 없이 Kaspersky Endpoint Security를 11.10.0 버전 이상으로 업그레이드하면, 컴퓨터에 Kaspersky Endpoint Security 애플리케이션이 두 개가 생깁니다. 이전 버전의 애플리케이션을 직접 제거하지 마십시오. 이전 버전은 컴퓨터를 다시 시작하면 자동 제거됩니다.

- Microsoft Windows 11을 실행하는 컴퓨터에서 Kaspersky Endpoint Security를 업그레이드한 후에는 파일 마우스 오른쪽 메뉴에 이전 애플리케이션 버전과 새 애플리케이션 버전 모두에 대한 항목이 표시될 수 있습니다. 파일 마우스 오른쪽 메뉴가 올바르게 작동하도록 하려면 컴퓨터를 두 번 다시 시작하십시오.

- 애플리케이션의 자기 보호 기능이 꺼지고 모든 네트워크 어댑터가 중지되면 애플리케이션 업그레이드가 끝난 후 컴퓨터를 다시 시작할 때까지 애플리케이션의 네트워크 구성 요소가 작동하지 않습니다. 애플리케이션의 네트워크 구성 요소에는 웹 위협 보호, 메일 위협 보호, 네트워크 위협 보호, 방화벽, 호스트 침입 방지 및 웹 제어가 포함됩니다. 애플리케이션이 올바르게 작동하려면 컴퓨터를 다시 시작하십시오.

- BadUSB 공격 방지 구성 요소는 애플리케이션 업그레이드가 끝난 후 컴퓨터를 다시 시작할 때까지 작동하지 않습니다. 애플리케이션이 올바르게 작동하려면 컴퓨터를 다시 시작하십시오.

- 이전 업그레이드 프로세스가 완료되지 않으면 애플리케이션을 업그레이드할 수 없습니다. 애플리케이션이 올바르게 작동하려면 컴퓨터를 다시 시작하십시오.

- Kaspersky Endpoint Security 11 for Windows 이전 버전에서 애플리케이션을 업그레이드한 후에는 컴퓨터를 다시 시작해야 합니다.

- Kaspersky Security Center Cloud Console을 사용하여 Kaspersky Endpoint Security를 관리하는 경우 애플리케이션을 로컬에서 업데이트할 수 없습니다. 로컬에서 애플리케이션을 업데이트할 때 Kaspersky Security Center Cloud Console에 대한 데이터 처리 계약을 수락할 수 없습니다.

Arm 아키텍처 지원

- Arm 기반 가상 컴퓨터에서는 Light Agent 모드의 Kaspersky Endpoint Security 설치를 지원하지 않습니다.
- Kaspersky 디스크 암호화는 Arm 기반 컴퓨터에서는 지원하지 않습니다.
- Arm 기반 컴퓨터에서는 파일 암호화를 지원하지 않습니다.
- Arm 기반 컴퓨터에서는 이동식 드라이브 암호화를 지원하지 않습니다.
- Windows 11 for Arm64를 실행하는 컴퓨터에서는 EDR 에이전트가 Bitdefender Endpoint Security Tools과 호환되지 않습니다.
- 오디오 신호 보호 기능 및 웹캠 접근 보호 기능은 Arm 기반 컴퓨터에서 지원하지 않습니다.
- Arm 기반 컴퓨터에서는 메일 위협 보호 확장 프로그램이 Arm64용 Outlook 2016, Outlook 2021, Outlook 2024 및 Outlook 365의 32비트 버전을 지원합니다.
- Kaspersky Endpoint Security는 Arm 아키텍처용 개체를 Kaspersky Sandbox로 전송하지 않습니다.
- Arm 기반 컴퓨터에서는 인쇄 제어를 지원하지 않습니다.
- Arm 기반 컴퓨터에서는 Kaspersky Endpoint Detection and Response Expert(cloud)와의 통합을 지원하지 않습니다.
- Arm 기반 컴퓨터에서 *IOC 검사* 작업은 다음 메일 클라이언트의 이메일 파일만 지원합니다: 32비트 및 64비트 버전의 Outlook 2016과 Arm64용 Outlook 2021, 2024, 365.

서버 플랫폼 지원

- *데이터 중복 제거* 기능이 활성화된 서버에서는 fsdmhost.exe 파일을 신뢰하는 애플리케이션 목록에 추가해야 합니다. 이렇게 하면 응용 프로그램의 성능을 최적화하고 CPU에 과도한 부하가 걸리는 것을 방지할 수 있습니다.
- ReFS 파일 시스템은 제한적으로 지원합니다.
  - Kaspersky Endpoint Security는 보안 위협 치료 이벤트를 잘못 처리할 수 있습니다. 예를 들어, 애플리케이션이 악성 파일 삭제 후에도 리포트에 개체 처리 안 됨 항목이 있을 수 있습니다. 동시에 Kaspersky Endpoint Security는 애플리케이션 설정에 따라 보안 위협을 치료합니다. Kaspersky Endpoint Security는 또한 같은 개체에 대해 중복으로 *컴퓨터 다시 시작 시 개체 치료 예정* 이벤트를 생성할 수 있습니다.
  - 파일 위협 보호가 일부 보안 위협을 건너뛸 수 있습니다. 동시에 악성 코드 검사는 올바르게 작동합니다.
  - *악성 코드 검사* 작업을 시작한 후에는 서버 재부팅 시 iChecker가 추가한 검사 예외 항목이 초기화됩니다.
  - iSwift 기술은 지원하지 않습니다. Kaspersky Endpoint Security는 iSwift 기술을 사용하여 추가된 검사 예외는 고려하지 않습니다.
  - Kaspersky Endpoint Security는 meicar.exe 파일이 컴퓨터에 Kaspersky Endpoint Security를 설치하기 전부터 있었을 경우 eicar.com과 susp-eicar.com 파일을 탐지하지 않습니다.
  - Kaspersky Endpoint Security는 보안 위협 치료 알림을 잘못 표시할 수 있습니다. 예를 들어, 애플리케이션은 이전에 치료된 보안 위협에 대한 보안 위협 알림을 표시할 수 있습니다.
- 파일 레벨 암호화(FLE) 및 Kaspersky 디스크 암호화(FDE) 기술은 서버 플랫폼을 지원하지 않습니다. 동시에 Kaspersky Endpoint Security는 데이터 암호화 이벤트를 잘못 처리할 수 있습니다.

- 서버 운영 체제에서는 고급 치료의 필요성에 대한 경고를 표시하지 않습니다.
- Microsoft Windows Server 2008은 지원 목록에서 제외되었습니다. Microsoft Windows Server 2008 운영 체제를 실행하는 컴퓨터에서 애플리케이션을 설치하는 것은 지원하지 않습니다.
- Microsoft Data Protection Manager(DPM)가 배포된 서버에 설치한 Kaspersky Endpoint Security는 DPM의 오작동을 유발할 수 있습니다. 이는 DPM 동작에 대한 제한과 연관이 있습니다. 오작동을 없애려면 파일 위협 보호 구성 요소와 *악성 코드 검사* 작업에 대해 로컬 서버 드라이브를 예외 규칙에 추가해야 합니다.
- Server Core 모드는 다음과 같이 제한적으로 지원됩니다:
  - 알림, 팝업 알림 및 기타 인터페이스 제어를 포함한 로컬 그래픽 사용자 인터페이스는 사용할 수 없습니다. 애플리케이션은 다음 창을 포함하여 프롬프트 창을 표시할 수 없습니다:
    - 애플리케이션 버전 및 모듈 업그레이드 확인 프롬프트
    - 컴퓨터 다시 시작 프롬프트
    - 프록시 서버 인증 자격 증명 프롬프트
    - 장치 접근 권한 획득 프롬프트(장치 제어)
  - 다음 구성 요소는 사용할 수 없습니다: 웹 위협 보호, 메일 위협 보호, 웹 제어, BadUSB 공격 방지.
  - 안티 브리징을 사용할 수 없습니다.
  - Kaspersky Security Center 콘솔의 애플리케이션 정책에서 Kaspersky Security Network 진술문만 수락할 수 있습니다.
  - BitLocker 드라이브 암호화는 TPM(신뢰하는 플랫폼 모듈)에서만 사용할 수 있습니다. 애플리케이션이 사전 부팅 인증을 위한 암호 프롬프트 창을 표시할 수 없으므로 암호화 시 PIN/암호는 사용할 수 없습니다. 운영 체제에 FIPS(연방 정보 처리 표준) 호환 모드가 활성화되어 있다면 드라이브 암호화 시작 전에 암호화 키를 저장할 이동식 드라이브를 연결하십시오.

지원하는 가상 플랫폼:

- Hyper-V 가상 컴퓨터에서의 전체 디스크 암호화(FDE)는 지원하지 않습니다.
- Citrix 가상 플랫폼에서의 전체 디스크 암호화(FDE)는 지원하지 않습니다.
- Windows 10 Enterprise 멀티 세션에는 다음과 같은 제한 사항이 따릅니다:
  - Kaspersky Endpoint Security는 서버의 처리 안 된 보안 위협 치료 시와 마찬가지로 사용자에게 알리지 않고 처리 안 된 보안 위협을 치료합니다. 운영 체제가 멀티 세션 모드로 계속 실행되므로, 보안 위협을 즉시 해결하지 않으면 다른 활성 사용자가 데이터를 잃을 수 있습니다.
  - 전체 디스크 암호화(FDE)를 지원하지 않습니다.
  - BitLocker 관리를 지원하지 않습니다.
  - Kaspersky Endpoint Security를 이동식 드라이브와 함께 사용할 수 없습니다. Microsoft Azure 인프라는 이동식 드라이브를 네트워크 드라이브로 정의합니다.
- Citrix 가상 플랫폼에서의 파일 레벨 암호화(FLE)의 사용 및 설치는 지원하지 않습니다.

- Citrix PVS와 Kaspersky Endpoint Security for Windows가 서로 호환되려면 **Citrix PVS와의 호환성 보장** 옵션을 사용하여 설치를 수행합니다. 이 옵션은 설치 마법사에서 사용하거나 `/pCITRIXCOMPATIBILITY=1` 명령줄 파라미터를 사용하여 설정할 수 있습니다. 원격 설치의 경우 KUD 파일에 `/pCITRIXCOMPATIBILITY=1` 파라미터를 추가해야 합니다.

- Citrix XenDesktop. 복제를 시작하기 전에 자기 보호를 중지해야 vDisk를 사용하는 가상 시스템을 복제할 수 있습니다.

- Kaspersky Endpoint Security for Windows 및 Kaspersky Security Center 네트워크 에이전트가 사전 설치된 Citrix XenDesktop 마스터 이미지용 템플릿 머신을 준비할 때 다음 유형의 예외 규칙을 구성 파일에 추가하십시오:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Citrix XenDesktop에 대한 상세 정보는 Citrix 지원 웹사이트를 방문하십시오.

- 때에 따라 VMware ESXi 하이퍼바이저에 배포된 가상 컴퓨터에서 이동식 드라이브에 대한 안전한 연결 해제 시도가 실패할 수 있습니다. 안전한 연결 해제를 다시 한 번 시도합니다.

- Kaspersky Endpoint Security는 다음 제한 사항이 있는 VMware ESXi 하이퍼바이저와 호환됩니다:

  - Kaspersky Endpoint Security는 Guest Introspection 드라이버(vnetWFP.sys, vnetFLT.sys 등)와 호환되지 않을 수 있습니다. 비호환성을 해결하려면 드라이버를 최신 버전으로 업데이트하거나 드라이버를 제거하십시오.

  - 경우에 따라 가상 컴퓨터에서 이동식 디스크를 안전하게 제거하려는 시도가 실패할 수 있습니다. 안전한 연결 해제를 다시 한 번 시도합니다.

- Citrix VDA 에이전트가 있는 가상 컴퓨터에 Kaspersky Endpoint Security를 설치하면 호환성 오류가 발생할 수 있습니다. 이는 Citrix Provisioning Services와 안티 바이러스 솔루션 간의 호환성이 제한적이기 때문에 발생합니다. Citrix Provisioning Services와 함께 안티 바이러스 솔루션을 사용한 모범 사례는 Citrix 지원 웹사이트를 참조하십시오.

- Kaspersky Endpoint Security는 Citrix 하이퍼바이저의 가상 컴퓨터에 이동식 드라이브가 연결된 경우 이동식 드라이브의 검사를 건너뜁니다(*이동식 드라이브 검사* 작업). 이러한 장치에서 운영 체제는 연결된 이동식 드라이브를 네트워크 드라이브로 탐지합니다. 이러한 경우에는 *사용자 지정 검사* 작업을 수행할 수 있습니다. 애플리케이션의 동작은 표준 모드와 Light Agent 모드에서 동일합니다.

- Kaspersky Endpoint Security Citrix가 앱 계층화 기술을 사용하는 인프라의 가상 컴퓨터에 설치된 경우, 애플리케이션이 탐지된 파일은 *다시 시작 시 개체가 삭제됨* 상태의 감염 객체로 탐지한 파일은 가상 컴퓨터가 재시작될 때 자동으로 제거되지 않습니다.

  이러한 파일을 삭제하려면, 사용자 계층이 포함된 VHDX 파일을 Citrix 앱 계층화 관리자 컴퓨터에 마운트하고, 마운트된 디스크에서 악성 코드 검사를 실행해야 합니다.

Kaspersky Security Center와의 호환성

- Kaspersky Security Center 웹 콘솔 버전 14.1 이하에서는 중앙 관리 서버 속성의 사용자 접근 권한 설정 섹션에 로그 검사 및 파일 무결성 모니터 구성 요소의 기능 영역 이름이 올바르게 표시되지 않습니다.

- 애플리케이션 복구 후에는 컴퓨터의 중앙 관리 서버 연결에 대한 보호 기능을 비활성됩니다. 애플리케이션 복구 후에는 *중앙 관리 서버 연결 보호* 작업을 다시 실행하십시오.

- Kaspersky Security Center 15.1에서는 몇 주 간격으로 작업을 실행할 수 있습니다(**요일별** 스케줄). Kaspersky Endpoint Security는 몇 주 간격의 작업 실행을 지원하지 않습니다. Kaspersky Endpoint Security에 대해 몇 주 간격으로 작업을 실행하도록 설정한 경우 애플리케이션이 매주 지정된 요일과 시간에 작업을 실행합니다.

- Kaspersky Security Center 관리 콘솔의 **사용자 또는 사용자 그룹 선택** 창에는 Kaspersky Security Center 사용자 목록 중 처음 50,000명만 표시됩니다. 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

- Kaspersky Security Center 관리 콘솔에서 관리 중인 장치를 검색할 때 **애플리케이션 구성 요소** 탭에는 이전 버전의 Kaspersky Endpoint Security에 해당하는 이름을 포함하여 동일한 애플리케이션 구성 요소의 이름이 여러 가지 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.

라이센스

- *데이터 수신 오류* 시스템 메시지가 표시되면 활성화를 수행하는 컴퓨터에 네트워크가 연결되어 있는지 확인하거나 Kaspersky Security Center 활성화 프록시를 통해 활성화 설정을 구성합니다.

- 애플리케이션 인터페이스에서 라이센스 만료 날짜는 컴퓨터의 로컬 시간으로 표시됩니다.

- 인터넷 접근이 불안정한 컴퓨터에 키 파일이 포함된 애플리케이션을 설치하면 애플리케이션이 활성화되지 않았거나 라이센스가 구성 요소 동작을 허용하지 않는다는 이벤트가 일시적으로 표시될 수 있습니다. 이는 설치 프로세스 중에 애플리케이션이 먼저 포함된 체험판 라이센스를 활성화하기 때문입니다. 인터넷 접근이 필요합니다.

- 체험 기간 동안 인터넷 접근이 불안정한 컴퓨터에 애플리케이션 업그레이드 또는 패치를 설치하면 애플리케이션이 활성화되지 않았다는 이벤트가 일시적으로 표시될 수 있습니다. 이는 업데이트 설치 프로세스 중에 애플리케이션이 먼저 포함된 체험판 라이센스를 활성화하기 때문입니다. 인터넷 접근이 필요합니다.

- 체험판 라이센스가 애플리케이션 설치 중에 자동으로 활성화된 후 라이센스 정보를 저장하지 않고 애플리케이션을 제거했다면 애플리케이션을 다시 설치할 때 체험판 라이센스가 자동으로 활성화되지 않습니다. 이때는 애플리케이션을 직접 활성화해주십시오.

- Kaspersky Security Center 버전 11과 Kaspersky Endpoint Security 버전 14.0를 사용 시, 구성 요소 성능 리포트가 제대로 작동하지 않을 수 있습니다. 사용자의 라이센스에 포함되지 않은 Kaspersky Endpoint Security 구성 요소를 설치한 경우 네트워크 에이전트가 Windows 이벤트 로그에 구성 요소 상태 오류를 전송할 수 있습니다. 오류를 방지하려면 사용자의 라이센스에 포함되지 않은 구성 요소를 제거하십시오.

메일 위협 보호

- Microsoft Outlook용 메일 위협 보호 확장 프로그램을 사용하여 메일을 검색할 때는 Exchange 캐싱 모드(Exchange 캐싱 모드 사용 옵션)를 사용하는 것이 좋습니다.

- Kaspersky Endpoint Security는 64비트 버전의 Microsoft Outlook 이메일 클라이언트를 지원하지 않습니다. 따라서 Kaspersky Endpoint Security는 64비트 버전의 Microsoft Outlook이 컴퓨터에 설치된 경우 메일이 검사 범위에 포함되어도 Microsoft Outlook 파일(PST 및 OST 파일)을 검사하지 않습니다.

- Kaspersky Endpoint Security는 Microsoft Outlook 새 메일 클라이언트를 지원하지 않습니다.

복원 엔진

- 애플리케이션은 NTFS 또는 FAT32 파일 시스템을 사용하는 장치에서만 파일을 복원합니다.

- 애플리케이션은 최대 100MB 크기의 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 웹 사이트를 방문하시기 바랍니다.

- 애플리케이션은 운영 체제 커널 레벨에서 프로세스에 의해 수행된 파일의 변경 사항을 모니터링하지 않습니다.

방화벽

- 네트워크 패킷 규칙이나 응용 프로그램 네트워크 규칙이 DNS 이름을 지정하는 경우, Kaspersky Endpoint Security는 DNS 서버에 요청을 보내 이러한 리소스의 IP 주소를 확인할 수 있습니다. 방화벽은 IP 주소를 사용하여 네트워크 활동을 모니터링합니다. 따라서 애플리케이션은 DNS 이름을 IP 주소로 변환합니다. LAN 컴퓨터 또는 내부 서비스에 대해서만 규칙에 DNS 이름을 사용하는 것이 권장됩니다.

- 모든 IPv6 주소에 대한 규칙을 지정하려면 ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 주소 범위를 추가합니다. 방화벽은 ::/0 마스크를 지원하지 않습니다.

- 로컬 주소, 물리적 인터페이스 및 패킷 TTL(Time to Live)별 패킷 또는 연결 필터링은 다음 경우에 지원됩니다:

  - TCP 및 UDP 및 패킷 규칙에 대한 애플리케이션 규칙의 아웃바운드 패킷 또는 연결에 대한 로컬 주소별.

  - 차단 애플리케이션 규칙 및 패킷 규칙의 인바운드 패킷 또는 연결(UDP 제외)에 대한 로컬 주소별.

  - 인바운드 또는 아웃바운드 패킷에 대한 블록 패킷 규칙에서 패킷 TTL(Time to Live) 기준.

  - 패킷 규칙의 인바운드 및 아웃바운드 패킷 또는 연결에 대한 네트워크 인터페이스별.

- 패킷 허용 규칙에 대해 네트워크 어댑터 또는 패킷 TTL(Time to Live)을 구성한 경우 이 규칙의 우선순위는 애플리케이션 차단 규칙보다 낮습니다. 즉, 애플리케이션에 대한 네트워크 활동이 차단된 경우(애플리케이션이 *높은 제한* 신뢰 그룹에 있는 경우 등) 이러한 설정이 있는 패킷 규칙으로 애플리케이션의 네트워크 활동을 허용할 수 없습니다. 다른 모든 경우에는, 패킷 규칙의 우선순위가 애플리케이션 네트워크 규칙보다 높습니다.

- 방화벽 패킷 규칙 가져오기 시, Kaspersky Endpoint Security는 규칙 이름을 수정할 수 있습니다. 애플리케이션은 프로토콜, 방향, 원격 및 로컬 포트, 패킷 TTL(Time-to-Live) 등의 같은 일반 파라미터 세트를 사용하여 규칙을 결정합니다. 다수의 규칙에서 이 일반 파라미터 세트가 같다면 애플리케이션이 이 규칙에 같은 이름을 배정하거나 이름에 파라미터 태그를 추가합니다. 이렇게 하면 Kaspersky Endpoint Security가 패킷 규칙을 전부 가져오되, 같은 일반 설정이 있는 규칙의 이름이 변경될 수 있습니다.

- 네트워크 규칙에서 애플리케이션 이벤트 보고를 활성화했다면, 애플리케이션을 다른 제어 그룹으로 이동 시 해당 제어 그룹의 제한 사항이 적용되지 않습니다. 따라서 애플리케이션이 신뢰 제어 그룹에 있다면 네트워크 제한이 적용되지 않습니다. 그 후 이 애플리케이션의 이벤트 보고를 활성화하고 *신뢰 안 함* 제어 그룹으로 옮겼습니다. 방화벽은 이 애플리케이션에 네트워크 제한을 적용하지 않습니다. 애플리케이션을 적합한 제어 그룹으로 먼저 이동한 후 이벤트 보고를 활성화할 것을 권장합니다. 이 방법을 사용할 수 없다면 네트워크 규칙 설정에서 애플리케이션에 대한 제한을 수동으로 구성할 수 있습니다. 제한은 애플리케이션의 로컬 인터페이스에만 적용됩니다. 정책 제어 그룹 간의 애플리케이션 이동이 제대로 작동합니다.

- 방화벽과 침입 방지 구성 요소에는 다음 공통 설정이 있습니다: 애플리케이션 권한과 보호 리소스. 방화벽에 대해 이 설정을 변경했다면 Kaspersky Endpoint Security가 새 설정을 침입 방지에 자동으로 적용합니다. 예를 들어 방화벽 정책의 일반 설정에 대한 변경을 허용했다면(자물쇠 열림), 침입 방지 설정 역시 편집할 수 있습니다.

- Kaspersky Endpoint Security 11.6.0 이하에서 네트워크 패킷 규칙이 트리거되면 방화벽 리포트의 **애플리케이션 이름** 열이 항상 *Kaspersky Endpoint Security* 값으로 표시됩니다. 또한 방화벽이 모든 애플리케이션에 대해 패킷 수준에서 연결을 차단합니다. 이 동작은 Kaspersky Endpoint Security 11.7.0 이상에서 수정되었습니다. 방화벽 리포트에 **규칙 유형** 열이 추가되었습니다. 네트워크 패킷 규칙이 트리거되면 **애플리케이션 이름** 열이 비어 있습니다.

- 방화벽을 사용하여 모든 네트워크 동작을 금지했다면 네트워크 위협 보호 구성 요소가 포트 검사 유형의 공격을 탐지할 수 있습니다. 이러한 현상이 발생할 수 있는 원인은 애플리케이션이 네트워크에서 의심스러운 활동을 탐지하기 위해 방화벽보다 먼저 네트워크 위협 보호를 시작하기 때문입니다.

BadUSB 공격 방지

- Kaspersky Endpoint Security는 컴퓨터가 잠금 상태가 되었을 때(화면 잠금 설정 시간 등) USB 장치 잠금 시간을 초기화합니다. 따라서 USB 장치 인증 코드를 여러 번 잘못 입력하여 애플리케이션이 USB 장치를 잠그면, Kaspersky Endpoint Security는 컴퓨터를 잠금 해제한 후에 다시 인증을 시도할 수 있도록 합니다. 이 때 Kaspersky Endpoint Security는 BadUSB 공격 방지 구성 요소 설정에 지정된 시간 동안 USB 장치를 잠그지 않습니다.

- Kaspersky Endpoint Security는 컴퓨터 보호가 중지되면 USB 장치 잠금 시간을 초기화합니다. 따라서 USB 장치 인증 코드를 여러 번 잘못 입력하여 애플리케이션이 USB 장치를 잠그면, Kaspersky Endpoint Security는 컴퓨터 보호를 다시 시작한 후에 다시 인증을 시도할 수 있도록 합니다. 이 때 Kaspersky Endpoint Security는 BadUSB 공격 방지 구성 요소 설정에 지정된 시간 동안 USB 장치를 잠그지 않습니다.

Kaspersky Security Network

- Kaspersky Endpoint Security는 서버 주소에 비 라틴 문자(비 ASCII 기호)가 포함된 경우 KSN 프록시에 연결할 때(KSN 프록시 연결 설정에서 **HTTPS 사용** 확인란이 선택됨) HTTPS를 지원하지 않습니다.

- Kaspersky Security Center에서 글로벌 Kaspersky Security Network를 사설 Kaspersky Security Network(KPSN)로, 또는 그 반대로 전환하면 특정 제품의 정책에서 Kaspersky Security Network에 참여하는 옵션이 중지됩니다. 전환 후 Kaspersky Security Network 진술문의 텍스트를 주의 깊게 읽고 KSN 참여에 대한 동의를 확인하십시오. 애플리케이션 인터페이스에서, 또는 제품 정책 편집 시 진술문의 텍스트를 읽을 수 있습니다.

- KPSN에서 글로벌 KSN으로 전환할 때 Kaspersky Endpoint Security 12.9 for Windows를 시작하면 Kaspersky Security Network 진술문에 대한 동의를 다시 승인해야 합니다. 이렇게 하려면 정책 속성 또는 애플리케이션 인터페이스에서 Kaspersky Security Network 사용을 활성화한 후 Kaspersky Security Network 진술문에 대한 동의를 승인해야 합니다. 글로벌 KSN을 이미 사용 중인 경우 우선 KSN 사용을 비활성화했다가 다시 활성화한 후 Kaspersky Security Network 진술문에 대한 동의를 승인해야 합니다. Kaspersky Security Network 진술문에 동의하지 않으면 애플리케이션이 Kaspersky Security Network의 데이터에 접근할 수 없습니다.

- Kaspersky Endpoint Security는 검사를 위해 텍스트 파일(예: TXT, CSV, LOG, 매크로가 없는 DOCX 파일)을 Kaspersky Security Network로 전송하지 않습니다. 애플리케이션이 검사를 위해 KSN에 위협이 될 수 있는 파일을 전송합니다. 이러한 파일에는 실행 파일 또는 실행 코드(예: DOCX 파일의 매크로)가 포함될 수 있는 파일이 포함됩니다. 애플리케이션의 다른 구성 요소는 텍스트 파일 검사를 담당합니다. 또한 파일 컨텍스트 메뉴에서 텍스트 파일의 평판을 직접 확인할 수 있습니다. 텍스트 파일의 평판이 *신뢰 안 함(Kaspersky Security Network)*이면 애플리케이션은 탐지된 위협에 대해 정의된 작업을 무시합니다.

애플리케이션 제어

- 애플리케이션 제어 규칙을 적용하여 작업할 때 다양한 카테고리의 애플리케이션에 대한 포함 및 예외 조건을 총 100,000개 이상 추가하는 것은 권장하지 않습니다. 단, Kaspersky Endpoint Security가 다음을 충족하는 컴퓨터에서 실행 중입니다. 최소 하드웨어 요구 사항을 충족하고 Microsoft Windows 10에서 작동하는 컴퓨터에서 실행되는 경우에만 해당합니다.

- Kaspersky Security Center 웹 콘솔에서 애플리케이션 제어 규칙을 사용할 때는 ZIP 형식 압축 파일만 지원됩니다. RAR 또는 7z 등 다른 형식의 압축 파일은 지원되지 않습니다. 관리 콘솔(MMC)에서 애플리케이션 제어 규칙을 사용하는 경우에는 그러한 제한이 없습니다.

- Kaspersky Security Center 웹 콘솔에서 애플리케이션 제어 규칙을 사용하는 경우 업로드된 파일의 최대 지원 크기는 104MB입니다. 관리 콘솔(MMC)에서 애플리케이션 제어 규칙을 사용하는 경우에는 그러한 제한이 없습니다.

- Microsoft Windows 10에서 애플리케이션 거부 목록 모드로 작업할 때 차단 규칙이 잘못 적용되어 규칙에 지정하지 않은 애플리케이션이 차단될 수 있습니다.

- Kaspersky Endpoint Security를 업그레이드할 때 *사전 정의된 애플리케이션 제어 규칙*을 새로 추가했다면 이전 버전의 애플리케이션에는 이 규칙을 적용할 수 없습니다.

- 프로그레시브 웹 앱(PWA)이 애플리케이션 제어 구성 요소에 의해 차단되면 appManifest.xml이 리포트에서 차단된 앱으로 표시됩니다.

- 기본 메모장 애플리케이션을 Windows 11용 애플리케이션 제어 규칙에 추가할 때는 애플리케이션의 경로를 지정하지 않는 것이 좋습니다. Windows 11을 사용하는 컴퓨터에서는 운영 체제가 `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe` 폴더에 있는 메트로 메모장을 사용합니다. 이전 버전의 운영 체제에서는 메모장이 다음 폴더에 있었습니다:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  애플리케이션 제어 규칙에 메모장을 추가할 때는 실행 중인 애플리케이션의 속성에서 애플리케이션의 이름 및 파일 해시를 지정하는 등의 방법을 사용할 수 있습니다.

- KSWS 정책을 KES 정책 프로필로 마이그레이션할 때 정책 및 작업 변환 마법사(마이그레이션 마법사)는 카테고리 이름에 다음과 같은 금지된 문자(`'` `*` `<` `>` `?` `\` `:` `|`)가 포함된 경우 애플리케이션 카테고리의 이름을 바꿉니다. 마이그레이션 마법사는 이러한 문자를 `_` 문자로 바꿉니다. 예를 들어 `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` 애플리케이션 카테고리는 이름이 `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`로 바뀝니다.

장치 제어

- Kaspersky Endpoint Security는 외부 기기 연결 및 연결 종료 이벤트를 기록할 수 있습니다. Windows 서비스는 시스템 사용자 계정을 사용하여 기기를 연결하거나 연결을 종료합니다. 따라서 어떤 사용자가 기기를 연결 또는 연결 종료하는지 알 수 없습니다. Kaspersky Endpoint Security는 이벤트에서 SYSTEM 사용자 계정을 지정합니다.

- 신뢰하는 목록에 추가된 프린터 장치에 대한 접근은 장치 및 버스 차단 규칙에 따라 차단됩니다.

- 운영 체제의 기본 제공 Microsoft 드라이버를 사용하는 경우 MTP 장치에 대한 읽기, 쓰기 및 연결 작업의 제어가 지원됩니다. 사용자가 장치 작업을 위해 사용자 지정 드라이버를 설치하면(iTunes 또는 Android 디버그 브리지 등) 읽기 및 쓰기 작업 제어가 작동하지 않을 수 있습니다.

- MTP 장치로 작업할 때 장치를 다시 연결하면 접근 규칙이 변경됩니다.

- 장치 제어 구성 요소는 장치 연결 및 연결 해제, 장치에서 파일 읽기, 장치에 파일 쓰기 및 기타 이벤트와 같이 감시하는 장치와 관련된 이벤트를 등록합니다. Kaspersky Endpoint Security는 휴대용 장치(MTP), 이동식 드라이브, 플로피 디스크, CD/DVD 드라이브 등의 장치 유형에 대해서만 연결 해제 이벤트를 등록합니다. 다른 장치 유형의 경우, 애플리케이션이 연결 종료 이벤트를 등록하지 않습니다. 애플리케이션은 모든 장치 유형에 대해 장치를 컴퓨터에 연결하는 작업을 등록합니다.

- 모델 마스크를 기반으로 신뢰하는 목록에 장치를 추가하고, ID에는 포함되지만 모델 이름에는 없는 문자를 사용하는 경우 이러한 장치는 추가되지 않습니다. 워크 스테이션에서 이러한 장치는 ID 마스크를 기반으로 신뢰하는 목록에 추가됩니다.

- 애플리케이션을 업그레이드한 후 컴퓨터를 다시 시작하지 않으면 장치 제어는 다시 연결된 장치에 접근 규칙을 적용하지 않습니다. 그러나 장치가 업그레이드 전에 연결된 경우 장치 제어가 규칙을 올바르게 적용합니다. 다시 연결된 장치에서 애플리케이션이 올바르게 작동하려면 컴퓨터를 다시 시작하십시오.

- Kaspersky Endpoint Security 버전 12.0이 설치된 컴퓨터에서 Kaspersky Endpoint Security 버전 12.1 정책이 적용된 경우, **네트워크 프린터** 장치 유형의 **허용하고 기록하지 않음** 프린터 액세스 모드가 **연결 버스에 종속**으로 표시됩니다. 이러한 모드에서 애플리케이션은 동일한 작업을 수행합니다. Kaspersky Endpoint Security 버전 12.1에서는 네트워크 프린터 액세스 모드가 **허용하고 기록하지 않음**으로 올바르게 표시됩니다.

- Kaspersky Endpoint Security 12.0 for Windows부터 애플리케이션에서 프린터의 인쇄 규칙을 구성할 수 있습니다(인쇄 제어). 인쇄 제어 기능이 있는 애플리케이션을 설치하거나 애플리케이션을 인쇄 제어 기능이 있는 버전으로 업그레이드한 후에는 컴퓨터를 다시 시작해야 합니다. 컴퓨터를 다시 시작할 때까지 Kaspersky Endpoint Security는 인쇄 규칙을 적용하지 않으며 프린터에 대한 액세스만 제어할 수 있습니다. 컴퓨터를 다시 시작했을 때 조직의 워크플로에 부정적인 영향을 미치는 경우 spoolsv 서비스(인쇄 스풀러)만 다시 시작할 수 있습니다. Arm 기반 컴퓨터에서는 인쇄 제어를 지원하지 않습니다.

- Kaspersky Endpoint Security for Windows 버전 12.0부터 WPA3 프로토콜은 **Wi-Fi** 유형 장치용 애플리케이션으로 지원됩니다. Kaspersky Endpoint Security 버전 12.2 정책이 컴퓨터에 적용될 경우, WPA2 프로토콜은 Kaspersky Endpoint Security 버전 11.11.0 이하의 컴퓨터에서 선택됩니다. WPA2 / WPA3은 버전 12.0 ~ 12.1로 선택됩니다. WPA3은 버전 12.2 이상으로 선택됩니다.

- Apple 장치는 휴대용 장치(MTP) 및 iTunes 장치로 분류됩니다. 운영 체제가 Apple 장치 연결을 제대로 인식하지 못해 Apple 장치를 휴대용 장치(MTP)로 확인하지 못할 수 있습니다. 그로 인해 파일 관리자에서 Apple 장치를 사용할 수 없으나 iTunes 앱에선 액세스 가능합니다. 결과적으로 Kaspersky Endpoint Security는 iTunes 앱에서만 Apple 장치에 대한 액세스를 제어합니다. 휴대용 장치(MTP)로서 사용자의 Apple 장치에 액세스하려면 장치 관리자(Device Manager)로 이동하여 USB 컨트롤러(Controllers) 목록에서 Apple 모바일 장치 USB 드라이버(Mobile Device USB Driver)를 제거해야 합니다. 컴퓨터를 다시 시작하면 운영 체제가 Apple 장치를 휴대용 장치(MTP)와 iTunes 장치로 인식합니다. Kaspersky Endpoint Security가 iTunes 앱과 파일 관리자 모두에서 장치에 대한 액세스를 제어합니다.

- Kaspersky Endpoint Security 12.3 for Windows에서는 **Bluetooth** 장치 유형 접근 설정이 다릅니다. 이전 버전의 애플리케이션에서 **연결 버스에 종속** 모드를 선택한 경우, 애플리케이션을 버전 12.3으로 업그레이드하면 **허용하고 기록하지 않음** 모드로 변경됩니다. 이는 장치의 동작 설정을 변경하지 않습니다.

- 장치 제어는 Microsoft Windows Bluetooth 스택을 통해서만 Bluetooth 장치를 지원합니다. 장치 제어는 타사 Bluetooth 스택에서 제대로 작동하지 않을 수 있습니다.

- Bluetooth 장치가 COD(Class of Device)를 숨기거나 스푸핑하는 경우 장치 제어가 제대로 작동하지 않을 수 있습니다.

- 특정 Realtek Bluetooth 동글 드라이버가 설치된 Windows 7 또는 Windows 8 컴퓨터에서는 Bluetooth 장치를 입력 장치(HID 클래스)로 연결하는 것만 허용하는 것은 불가능할 수 있습니다. 즉, 애플리케이션 설정에서 Bluetooth 장치에 대한 접근을 금지하고 입력 장치를 예외에 추가하면 장치 제어가 모든 Bluetooth 장치에 대한 접근을 차단할 수 있습니다.

웹 제어

- OGV 및 WEBM 형식은 지원하지 않습니다.

- RTMP 프로토콜은 지원하지 않습니다.

- 웹 제어는 WSL1만 지원합니다. 애플리케이션은 WSL2 트래픽을 제어하지 않습니다.

적응형 이상 행위 제어

- 이벤트에 따라 자동으로 예외 규칙을 생성할 것을 권장합니다. 예외 규칙을 직접 추가하는 경우 대상 개체를 지정할 때 경로 시작 부분에 * 문자를 추가합니다.
- 샘플에 이름이 260자를 초과하는 이벤트가 하나라도 포함되어 있으면 적응형 이상 행위 제어 규칙 리포트를 생성할 수 없습니다.
- 개체나 프로세스의 속성에 256자 이상의 값이 포함되어 있으면(대상 개체의 경로 등) 적응형 이상 행위 제어 규칙 트리거링 저장소에서 예외 규칙을 추가할 수 없습니다. 정책 설정에서 직접 예외 규칙을 추가할 수 있습니다. 트리거된 적응형 이상 행위 제어 규칙 리포트에 예외 규칙을 추가할 수도 있습니다.
- Kaspersky Security Center 15.1에서 특정 규칙에 대해 **적응형 이상 행위 제어 규칙 상태 리포트** 상세 보고를 생성할 수 없습니다.

드라이브 암호화(FDE)

- Kaspersky 디스크 암호화는 Arm 기반 컴퓨터에서는 지원하지 않습니다.
- BitLocker 드라이브 암호화는 Windows 홈을 실행하는 컴퓨터에서는 지원하지 않습니다.
- 애플리케이션을 설치한 후 하드 드라이브 암호화가 제대로 작동하려면 운영 체제를 다시 시작해야 합니다.
- 인증 에이전트는 그림 문자나 | 및 \ 등의 특수 문자를 지원하지 않습니다.
- 암호화 후 최적의 컴퓨터 성능을 위해서는 프로세서가 AES-NI 명령 집합(Intel Advanced Encryption Standard New Instructions)을 지원해야 합니다. 프로세서가 AES-NI를 지원하지 않는다면, 컴퓨터 성능이 저하될 수 있습니다.
- 애플리케이션이 암호화된 장치에 대한 접근 권한을 부여하기 전에 이러한 장치에 접근을 시도하는 프로세스가 있는 경우 애플리케이션은 이러한 프로세스를 종료해야 한다는 경고를 표시합니다. 프로세스를 종료할 수 없는 경우 암호화된 장치를 다시 연결합니다.
- 하드 드라이브의 고유 ID는 장치 암호화 통계에 반전된 형식으로 표시됩니다.
- 암호화 도중 장치 포맷은 권장하지 않습니다.
- 여러 개의 이동식 드라이브가 컴퓨터에 동시에 연결된 경우 암호화 정책은 이동식 드라이브 하나에만 적용할 수 있습니다. 이동식 드라이브가 다시 연결되면 암호화 정책이 올바르게 적용됩니다.
- 조각난 파일이 많은 하드 드라이브에서는 암호화가 시작되지 않을 수 있습니다. 하드 드라이브를 조각 모음합니다.
- 하드 드라이브가 암호화되면 암호화 작업이 시작된 시점부터 Microsoft Windows 7/8/8.1/10을 구동하는 컴퓨터를 처음으로 다시 시작할 때까지, 그리고 하드 드라이브 암호화를 설치한 시점부터 Microsoft Windows 8/8.1/10 운영 체제를 처음으로 다시 시작할 때까지 최대 절전 모드가 차단됩니다. 하드 드라이브가 복호화되면 부팅 드라이브가 완전히 복호화된 시점부터 운영 체제를 처음으로 다시 시작할 때까지 최대 절전 모드가 차단됩니다. Microsoft Windows 8/8.1/10에서 빠른 시작 옵션을 사용하는 경우 최대 절전 모드를 차단하면 운영 체제를 종료할 수 없습니다.
- Windows 7 컴퓨터는 디스크가 BitLocker 기술로 암호화된 경우 복구 중에 암호를 변경할 수 없습니다. 복구 키를 입력하고 운영 체제를 로드한 후 Kaspersky Endpoint Security는 사용자에게 비밀번호나 PIN 코드를 변경하라는 메시지를 표시하지 않습니다. 따라서 새 암호 또는 PIN 코드를 설정할 수 없습니다. 이는 운영 체제상의 특성으로 인한 문제입니다. 계속하려면 하드 드라이브를 다시 암호화해야 합니다.
- 추가 공급자를 사용하는 상태에서 xbootmgr.exe 도구를 사용하는 것은 권장하지 않습니다. (예: Dispatcher, Network, Drivers 등)

- Kaspersky Endpoint Security for Windows가 설치된 컴퓨터에서는 암호화된 이동식 드라이브 포맷을 지원하지 않습니다.
- FAT32 파일 시스템으로 암호화된 이동식 드라이브 포맷은 지원하지 않습니다(드라이브가 암호화된 것으로 표시). 드라이브를 포맷하려면 NTFS 파일 시스템으로 다시 포맷합니다.
- 하나의 암호화된 컴퓨터에서는 여러 개의 다운로드 에이전트를 동시에 사용할 수 없습니다.
- 운영 체제가 암호화되지 않은 상태로 부팅 가능한 GPT 디스크의 이미지를 복원하려고 하면 운영 체제가 작동하지 않을 수 있습니다. 이를 방지하려면 다음 권장 사항을 따릅니다.
  - 백업에서 이미지를 복원하기 전에 디스크를 완전히 복호화합니다.
  - 이미지를 생성할 때 섹터별 복사를 사용합니다.
  - 이미지를 복원하고 디스크를 다시 초기화하기 전에 암호화된 디스크의 첫 번째 섹터에서 데이터를 삭제합니다.
- 다음 조건이 모두 동시에 충족되면 이전에 다른 컴퓨터에서 암호화된 이동식 드라이브에 접근할 수 없습니다:
  - Kaspersky Security Center 서버에 연결되어 있지 않습니다.
  - 사용자가 새 토큰 또는 비밀번호로 인증을 시도하고 있습니다.

  비슷한 상황이 발생하면 컴퓨터를 다시 시작합니다. 컴퓨터가 다시 시작되면 암호화된 이동식 드라이브에 대한 접근 권한이 부여됩니다.
- BIOS 설정에서 USB용 xHCI 모드가 활성화된 경우 인증 에이전트에 의한 USB 장치 발견을 지원하지 않을 수 있습니다.
- 가장 자주 사용되는 데이터를 캐싱하는 데 사용되는 장치의 SSD 부분에 대한 Kaspersky 디스크 암호화(FDE)는 SSHD 장치에서 지원하지 않습니다.
- UEFI 모드에서 실행되는 32 비트 Microsoft Windows 8/8.1/10 운영 체제의 하드 드라이브 암호화는 지원하지 않습니다.
- 복호화된 하드 드라이브를 다시 암호화하기 전에 컴퓨터를 다시 시작하십시오.
- 하드 드라이브 암호화는 Kaspersky Anti-Virus for UEFI와 호환되지 않습니다. Kaspersky Anti-Virus for UEFI가 설치된 컴퓨터에서는 하드 드라이브 암호화 사용을 권장하지 않습니다.
- Microsoft 계정을 기반으로 한 인증 에이전트 계정 생성은 다음과 같은 제한 사항과 함께 지원됩니다:
  - Single Sign-On 기술은 지원하지 않습니다.
  - 최근 N일 동안 시스템에 로그인한 사용자에 대한 계정 생성 옵션을 선택한 경우 인증 에이전트 계정 자동 생성을 지원하지 않습니다.
- 인증 에이전트 계정의 이름 형식이 `<domain>/<Windows account name>`인 경우, 컴퓨터 이름을 변경한 후 이 컴퓨터의 로컬 사용자용 계정 이름도 변경해야 합니다. 예를 들어 `Ivanov` 컴퓨터에 로컬 사용자 `Ivanov`가 있고 이 사용자에 대해 `Ivanov/Ivanov` 라는 이름의 인증 에이전트 계정이 만들어졌다고 가정합니다. 컴퓨터 이름 `Ivanov`가 `Ivanov-PC`로 변경된 경우 사용자 `Ivanov`의 인증 에이전트 계정 이름을 `Ivanov/Ivanov`에서 `Ivanov-PC/Ivanov`로 변경해야 합니다. 인증 에이전트의 로컬 계정 관리 작업을 사용하여 계정 이름을 변경할 수 있습니다. 계정 이름이 변경되기 전에 이전 이름(`Ivanov/Ivanov` 등)을 사용하여 사전 부트 환경에서 인증이 가능합니다.

- 사용자가 토큰을 사용해서만 Kaspersky 디스크 암호화 기술로 암호화된 컴퓨터에 접근할 수 있는 상태에서 접근 복구 절차를 완료해야 하는 경우, 암호화된 컴퓨터에 대한 접근이 복원되면 이 사용자에게 이 컴퓨터에 대한 암호 기반 접근 권한을 부여해야 합니다. 사용자가 접근 복원시 설정한 비밀번호는 저장되지 않을 수 있습니다. 이 경우 사용자는 다음에 암호화된 컴퓨터를 다시 시작할 때 이에 대한 접근 권한을 복원하는 절차를 완료해야 합니다.

- FDE 복구 도구를 사용하여 하드 드라이브를 복호화할 때 소스 장치의 데이터를 복호화된 데이터로 덮어 쓰면 복호화 작업이 오류와 함께 종료될 수 있습니다. 하드 드라이브의 데이터 일부는 암호화된 상태로 남습니다. FDE 복구 도구를 사용할 때 장치 복호화 설정에서 복호화된 데이터를 파일에 저장하는 옵션을 권장합니다.

- 인증 에이전트 암호가 변경된 경우 *암호가 성공적으로 변경되었습니다.확인 누르기* 텍스트가 포함된 메시지가 표시되며, 사용자가 컴퓨터를 다시 시작하면 새 암호가 저장되지 않습니다. 사전 부트 환경에서의 후속 인증에는 이전 암호를 사용해야 합니다.

- 디스크 암호화는 Intel Rapid Start 기술과 호환되지 않습니다.

- 디스크 암호화는 ExpressCache 기술과 호환되지 않습니다.

- FDE 복구 도구를 사용하여 암호화된 드라이브를 복호화하려고 할 때 도구가 "요청-응답" 절차 완료 후 장치 상태를 "암호화되지 않음"으로 잘못 탐지할 수 있습니다. 도구의 로그에는 장치가 성공적으로 복호화되었음을 나타내는 이벤트가 표시됩니다. 이 경우 장치를 복호화하려면 데이터 복구 절차를 다시 시작해야 합니다.

- Kaspersky Endpoint Security for Windows 플러그인이 웹 콘솔에서 업데이트된 후 클라이언트 컴퓨터 속성은 웹 콘솔 서비스가 다시 시작될 때까지 BitLocker 복구 키를 표시하지 않습니다.

- 전체 디스크 암호화 지원의 다른 제한 사항과 하드 드라이브 암호화가 제한적으로 지원되는 장치 목록을 보려면 기술 지원 기술 자료 웹사이트를 참조하십시오.

파일 레벨 암호화(FLE).

- Arm 기반 컴퓨터에서는 파일 암호화를 지원하지 않습니다.

- Microsoft Windows Embedded 운영 체제에서는 파일 및 폴더 암호화를 지원하지 않습니다.

- 애플리케이션 설치 후에 파일 및 폴더 암호화가 제대로 작동하려면 운영 체제를 다시 시작해야 합니다.

- 해당 애플리케이션은 NTFS 및 FAT32 파일 시스템으로 장치에 대한 파일 암호화만 지원합니다. 암호화된 파일이 지원되지 않는 파일 시스템(예: exFAT)으로 장치에 이전될 경우 해당 장치의 파일은 암호화되지 않으며 수정이 가능합니다.

- 암호화 기능이 있는 컴퓨터에 암호화된 파일이 저장되어 있다면 암호화 기능이 없는 다른 컴퓨터에서도 이 파일에 직접 접근할 수 있습니다. 암호화 기능이 있는 컴퓨터의 네트워크 폴더에 저장한 암호화된 파일은 암호화 기능이 없는 컴퓨터에 복호화된 형태로 복사됩니다.

- Kaspersky Endpoint Security for Windows로 파일을 암호화하기 전에 Encrypting File System으로 암호화된 파일을 복호화하는 것이 좋습니다.

- 파일이 암호화되면 파일 크기가 4KB 증가합니다.

- 파일이 암호화되면 파일 속성이 *압축 파일*로 설정됩니다.

- 예를 들어 이동식 미디어에 복호화된 파일을 복사할 때 파일이 암호화된 상태로 유지될 수 있습니다. 이러한 현상이 발생할 수 있는 원인은 파일 관리자(예: Explorer.exe)가 암호화된 파일 접근 권한 획득을 시도할 때 파일의 해시를 프로세스의 특수 목록에 저장하기 때문입니다. 파일을 복호화한 후 파일 관리자가 파일 접근 권한 획득을 시도할 때 프로세스가 목록에서 파일의 해시를 검색합니다. 해시가 탐지되면 Kaspersky Endpoint Security가 파일을 암호화된 상태로 둡니다. 이를 방지하려면 프로세스 목록을 지워야 합니다. 프로세스 목록이 채워지면 운영 체제가 자동으로 프로세스 목록을 지웁니다. 또한 목록을 수동으로 지울 수 있습니다. 그렇게 하려면 컴퓨터를 다시 시작하거나 파일에 접근하는 데 사용하는 프로세스(예: Explorer.exe)를 다시 시작하거나 암호화된 파일에 접근하는 데 사용되지 않은 다른 파일 관리자를 사용할 수 있습니다.

- 암호화된 압축 파일에서 압축 해제한 파일의 이름이 사용자의 컴퓨터에 이미 있는 파일의 이름과 같다면, 암호화된 압축 파일에서 압축 해제한 파일이 컴퓨터의 파일을 덮어씁니다. 사용자에게 덮어쓰기 작업에 대한 알림을 표시하지는 않습니다.

- 암호화된 압축 파일을 압축 해제하기 전에 압축 해제한 파일을 수용할 만큼 충분한 디스크 여유 공간이 있는지 확인하십시오. 디스크 공간이 충분하지 않으면 압축 파일 압축 해제는 완료될 수 있으나 파일이 손상될 수 있습니다. 이 경우 Kaspersky Endpoint Security가 오류 메시지를 표시하지 않을 수 있습니다.

- 휴대용 파일 관리자 인터페이스는 작동 중에 발생하는 오류에 대한 메시지를 표시하지 않습니다.

- Kaspersky Endpoint Security for Windows는 파일 레벨 암호화 구성 요소가 설치된 컴퓨터에서 휴대용 파일 관리자를 시작하지 않습니다.

- 다음 조건을 동시에 만족한다면 휴대용 파일 관리자를 사용해 이동식 드라이브에 접근할 수 없습니다.

  - Kaspersky Security Center에 연결되어 있지 않습니다.
  - 컴퓨터에 Kaspersky Endpoint Security가 설치되어 있습니다.
  - 이 컴퓨터에서 데이터 암호화(FDE 또는 FLE)가 수행되지 않았습니다.

  휴대용 파일 관리자의 암호를 알고 있어도 접근이 불가능합니다.

- 파일 암호화를 사용하면 애플리케이션이 Sylpheed 메일 클라이언트와 호환되지 않습니다.

- Kaspersky Endpoint Security for Windows는 일부 애플리케이션에서 암호화된 파일 접근 제한 규칙을 지원하지 않습니다. 이는 일부 파일 작업을 제삼자 애플리케이션이 수행하기 때문입니다. 예를 들어 파일 복사는 이 애플리케이션이 아닌 파일 관리자가 수행합니다. 따라서, 사용자가 클립보드나 드래그 앤 드롭 기능으로 이메일 메시지에 파일을 복사할 때 암호화된 파일에 대한 Outlook 메일 클라이언트의 접근이 거부된다면, Kaspersky Endpoint Security는 메일 클라이언트가 암호화된 파일에 접근하도록 허용합니다. 복사 작업은 암호화된 파일에 대한 접근 제한 규칙이 지정되지 않은 파일 관리자가 수행하므로, 접근이 허용됩니다.

- 이동식 드라이브가 휴대용 모드 지원으로 암호화되면 암호 사용 기간 제어를 중지할 수 없습니다.

- 페이지 파일 설정 변경은 지원하지 않습니다. 운영 체제는 지정된 파라미터값 대신 기본값을 사용합니다.

- 암호화된 이동식 드라이브로 작업할 때는 안전 제거를 사용하십시오. 이동식 드라이브를 안전하게 제거하지 않으면 데이터 무결성을 보장할 수 없습니다.

- 파일이 암호화되면 암호화되지 않은 원본은 안전하게 삭제됩니다.

- CSC(Client-Side Caching)를 사용한 오프라인 파일 동기화는 지원하지 않습니다. 오프라인 파일 암호화와 서버용 SMB를 통한 Branch Caching 기술이 지원되지 않습니다. 그룹 정책 수준에서 공유 리소스를 오프라인으로 관리하지 못하게 할 것을 권장합니다. 오프라인 모드에 있는 파일을 편집할 수 있습니다. 동기화 후 오프라인 파일의 변경 사항이 손실될 수 있습니다.

- 시스템 하드 드라이브의 루트에 암호화된 압축 파일을 생성하는 것은 지원하지 않습니다.

- 암호화된 파일에 네트워크를 통해 접근하면 문제가 발생할 수 있습니다. 파일을 다른 경로로 이동하거나 파일 서버로 사용되는 컴퓨터를 같은 Kaspersky Security Center 중앙 관리 서버에서 관리하도록 하는 것이 좋습니다.

- 키보드 레이아웃을 변경하면 암호화된 자동 압축 해제 압축 파일에 대한 암호 입력 창이 중단될 수 있습니다. 이 문제를 해결하려면 암호 입력 창을 닫고 운영 체제의 키보드 레이아웃을 전환한 다음 암호화된 압축 파일의 암호를 다시 입력합니다.

- 하나의 디스크에 여러 개의 파티션이 있는 시스템에서 파일 암호화를 사용하는 경우 pagefile.sys 파일의 크기를 자동으로 결정하는 옵션을 사용하는 것이 좋습니다. 컴퓨터가 다시 시작되면 pagefile.sys 파일이 디스크 파티션 간에 이동될 수 있습니다.

- *내 문서* 폴더의 파일을 포함하여 파일 암호화 규칙을 적용한 후에, 암호화가 적용된 사용자가 암호화된 파일에 성공적으로 접근할 수 있는지 확인합니다. 이를 위해서는 Kaspersky Security Center에 연결할 수 있을 때 각 사용자가 시스템에 로그인해야 합니다. 사용자가 Kaspersky Security Center에 연결하지 않은 상태에서 암호화된 파일에 접근하려고 하면 시스템이 중단될 수 있습니다.

- 파일 레벨 암호화 범위에 시스템 파일이 포함된 경우, 이러한 파일의 암호화에 대한 오류 이벤트가 리포트에 나타날 수 있습니다. 이러한 이벤트와 관련된 파일이 실제로 암호화되지는 않습니다.

- Pico 프로세스는 지원하지 않습니다.

- 경로의 대소문자 구분은 지원하지 않습니다. 암호화 규칙 또는 복호화 규칙이 적용된 제품 이벤트의 경로는 소문자로 표시됩니다.

- 시작 시 시스템에서 사용하는 파일의 암호화는 권장하지 않습니다. 이러한 파일을 암호화하면, Kaspersky Security Center에 연결하지 않고 암호화된 파일에 접근하려고 할 시 시스템이 중단되거나 암호화되지 않은 파일에 접근하라는 메시지가 표시될 수 있습니다.

- 사용자가 file-to-memory 매핑 방법(WordPad 또는 FAR 등)을 사용하는 애플리케이션 및 대용량 파일 작업용으로 설계된 애플리케이션(노트패드++)을 통해 FLE 규칙에 따라 네트워크상에서 파일로 공동 작업하는 경우, 암호화되지 않은 형식의 파일이 무기한 차단되어 해당 파일이 있는 컴퓨터에서 접근할 수 없게 될 수 있습니다.

- Kaspersky Endpoint Security는 OneDrive 클라우드 저장소 또는 이름이 OneDrive인 다른 폴더에 있는 파일을 암호화하지 않습니다. Kaspersky Endpoint Security는 암호화된 파일이 복호화 규칙에 추가되지 않았다면 해당 파일을 OneDrive 폴더로 복사하는 것도 차단합니다.

- 파일 레벨 암호화 구성 요소가 설치되면 사용자 및 그룹 관리가 WSL 모드(Windows Subsystem for Linux)에서 작동하지 않습니다.

- 파일 레벨 암호화 구성 요소가 설치되면 파일 이름 변경 및 삭제를 위한 POSIX(Portable Operating System Interface)를 지원하지 않습니다.

- 데이터 손실이 야기될 수 있으므로 임시 파일은 암호화하지 않는 것이 좋습니다. 예를 들어, Microsoft Word는 문서를 처리할 때 임시 파일을 생성합니다. 원본 파일은 그대로 두고 임시 파일을 암호화하면 사용자가 문서를 저장하려고 할 때 *액세스 거부됨* 오류가 표시될 수 있습니다. 그리고 Microsoft Word가 파일을 저장할 수 있지만 데이터가 소실되어 다음에 해당 문서가 열리지 않을 수 있습니다. 데이터가 손실되지 않도록 암호화 규칙에서 임시 파일 폴더를 제외시켜야 합니다.

Detection and Response(EDR, NDR, MDR, XDR, Sandbox)

- *격리 저장소로 파일 이동* 작업에 따라 격리된 개체는 검사할 수 없습니다.

- 4MB를 초과하는 Alternate Data Stream(ADS)은 격리할 수 없습니다. Kaspersky Endpoint Security는 이러한 모든 ADS를 사용자에게 알리지 않고 건너뜁니다.

- Kaspersky Endpoint Security는 작업 속성의 폴더 경로가 드라이브 문자로 시작할 시 네트워크 드라이브에 *IOC 검사* 작업을 실행하지 않습니다. Kaspersky Endpoint Security는 네트워크 드라이브의 *IOC 검사* 작업에 대해 UNC 경로 포맷만 지원합니다. 예: `\\server\shared_folder`.

- EmailItem 용어를 사용하는 *IOC 검사* 작업이 제대로 작동하려면 Kaspersky Endpoint Security 웹 플러그인을 최신 버전으로 업데이트해야 합니다.

- Arm 기반 컴퓨터에서 *IOC 검사* 작업은 다음 메일 클라이언트의 이메일 파일만 지원합니다: 32비트 및 64비트 버전의 Outlook 2016과 Arm64용 Outlook 2021, 2024, 365.

- 구성 파일에서 Kaspersky Sandbox와의 통합 설정이 활성화되어 있으면 애플리케이션 구성 파일 가져오기 시 오류가 발생할 수 있습니다. 애플리케이션 설정을 내보내기 전에 Kaspersky Sandbox를 비활성화하십시오. 그 후 가져오기/내보내기 절차를 수행합니다. 구성 파일을 가져온 후에 Kaspersky Sandbox를 활성화합니다.

- KLP 파일에서 정책을 가져올 때 Kaspersky Detection and Response Expert 계약서의 약관 수락을 결정하는 파라미터 값이 적용되지 않습니다. 그 결과, 정책을 가져온 후 Kaspersky Endpoint Security가 EDR 에이전트의 기능을 수행하지 않습니다. EDR 에이전트가 작동하려면 정책을 열고 파라미터를 변경하고 정책 설정을 저장하십시오.

- *IOC 검사* 작업 수행 중에 침해지표가 탐지되면, 애플리케이션이 FileItem 용어에 대해서만 파일을 격리합니다. 다른 용어에 대한 파일 격리는 지원하지 않습니다.

- 경고 세부 정보를 관리하려면 Kaspersky Endpoint Security for Windows 웹 플러그인 11.7.0 이상이 필요합니다. 경고 세부 정보는 Endpoint Detection and Response 솔루션(EDR Optimum 및 EDR Expert)과 작업 시에 필요합니다. 경고 세부 정보는 Kaspersky Security Center 웹 콘솔 및 Kaspersky Security Center Cloud Console에서만 이용할 수 있습니다.

- [KES+KEA] 구성을 [KES+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.

- [KES+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. [KES + 내장 에이전트] 구성으로 마이그레이션한 후엔 Kaspersky Endpoint Agent가 해당 컴퓨터에서 제거될 수 있도록 합니다. 마이그레이션 후에도 Kaspersky Endpoint Agent가 계속해서 작동한다면 애플리케이션을 수동으로 제거합니다(예를 들어 *애플리케이션을 원격으로 제거* 작업 사용).

  설치된 Kaspersky Endpoint Security와 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 Endpoint Security와 Kaspersky Endpoint Agent 버전에 근거하여 동작합니다.

- 경고 세부 정보를 생성할 때 애플리케이션은 수정된 파일의 해시를 포함하여 탐지된 위협에 대한 정보를 제공합니다. Kaspersky Endpoint Security는 경고 세부 정보를 생성할 때 파일의 해시를 계산합니다. 파일 수정 이벤트가 생성될 때 파일의 원래 해시는 경고 세부 정보가 생성될 때 계산된 해시와 다를 수 있습니다.

- EDR Optimum 및 Kaspersky Sandbox 구성 요소를 관리하려면 Kaspersky Endpoint Security for Windows 웹 플러그인 11.7.0 이상이 필요합니다. EDR Expert 구성 요소를 관리하려면 Kaspersky Endpoint Security for Windows 웹 플러그인 11.8.0 이상이 필요합니다. 해당 구성 요소와 관련된 작업을 지원하지 않는 웹 플러그인을 사용하여 *애플리케이션 구성 요소 변경* 작업을 생성했다면, 설치 프로그램이 EDR Optimum, EDR Expert, Kaspersky Sandbox 중 하나가 설치된 컴퓨터에서 해당 구성 요소를 삭제합니다.

- 내장 에이전트인 EDR(KATA)은 격리 기간이 만료된 경우에도 컴퓨터를 재시작한 후 컴퓨터의 네트워크 격리를 재개합니다. 컴퓨터 격리가 반복되지 않으려면 Kaspersky Anti Targeted Attack Platform 콘솔에서 네트워크 격리를 꺼야 합니다.

- 네트워크 격리가 완료된 후에는 애플리케이션을 업그레이드하는 것이 좋습니다. Kaspersky Endpoint Security를 업그레이드하고 나면 네트워크 격리를 멈출 수 있습니다.

- EDR(KATA), EDR Optimum, EDR Expert용 내장 에이전트는 서로 호환되지 않습니다. 따라서 다른 EDR 기능으로 Kaspersky Endpoint Security를 활성화했다면 독립 실행형 Kaspersky Endpoint Detection and Response Add-on 라이센스를 활용한 EDR 내장 에이전트 활성화는 건너뛰어도 됩니다. 예를 들어 [KES+EDR Optimum] 라이센스로 Kaspersky Endpoint Security를 활성화했다면 독립 실행형 라이센스를 활용한 EDR(KATA) 내장 에이전트의 활성화는 건너뜁니다.

- Kaspersky Endpoint Security 버전 12.1에서는 내장 EDR(KATA) 에이전트가 *NTFS 메타파일 가져오기* 작업에 대한 다음 메타파일을 지원하지 않습니다: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Kaspersky Endpoint Security 버전 12.2에 이 메타파일에 대한 지원이 추가되었습니다.

- Kaspersky Anti Targeted Attack Platform(EDR) 솔루션을 위해 Kaspersky Endpoint Agent에서 Kaspersky Endpoint Security로 마이그레이션하는 경우, 컴퓨터를 Central Node 서버로 연결할 때 오류가 발생할 수도 있습니다. 그 이유는 웹 콘솔의 마이그레이션 마법사가 다음 정책 설정을 건너뛰고 마이그레이션하지 않기 때문입니다.

  - **연결 설정**에 대한 설정 수정 금지('잠금').

    기본적으로 설정을 수정할 수 있습니다("잠금"이 열립니다). 따라서 설정이 컴퓨터에서 적용되지 않습니다. 설정 수정을 금지하고 '잠금'을 종료해야 합니다.

  - 암호화 컨테이너.

    Central Node 서버로 연결하기 위해 양방향 인증을 사용하는 경우, 암호화 컨테이너를 다시 추가해야 합니다. 마이그레이션 마법사는 서버의 TLS 인증서를 올바로 마이그레이션합니다.

  관리 콘솔(MMC)의 정책 및 작업 마이그레이션 마법사는 Kaspersky Anti Targeted Attack Platform(EDR) 솔루션에 대한 모든 설정을 마이그레이션합니다.

- Kaspersky Security Center에 대한 연결 없이 Kaspersky Managed Detection and Response 솔루션을 지원하기 위해 해당 애플리케이션이 Endpoint Detection and Response Agent 모드에서 설치된 경우 애플리케이션 활성화 상태가 제대로 표시되지 않습니다. BLOB 파일 다운로드 이후 Windows 작업 표시줄 알림 영역에 *애플리케이션이 활성화되지 않았습니다* 상태가 표시됩니다. 단, 애플리케이션 인터페이스에는 활성화 상태가 제대로 표시됩니다. 애플리케이션이 올바르게 작동하려면 컴퓨터를 다시 시작하십시오.

- Kaspersky Endpoint Security를 사용하면 EDR(KATA) 구성 요소 또는 Endpoint Sensor(지원하지 않음)를 사용하여 Kaspersky Anti Targeted Attack Platform 솔루션과 통합할 수 있습니다. Kaspersky Anti Targeted Attack Platform과 상호 작용하는 구성 요소 중 하나만 사용할 수 있습니다. 구성 요소의 상태를 보려면 관리 콘솔(MMC)에서 컴퓨터 속성을 열고 **애플리케이션** 섹션에서 Kaspersky Endpoint Security for Windows의 속성을 연 다음 **구성 요소** 섹션으로 이동합니다. Kaspersky Anti Targeted Attack Platform과의 상호 작용에 대한 구성 요소 상태 표시에는 다음 특수 고려 사항이 적용됩니다.

  - 관리 플러그인 12.0 및 이전 버전의 경우 애플리케이션은 **Endpoint Sensor**의 현재 상태를 표시합니다. Kaspersky Endpoint Security 12.0 이하 버전에서는 EDR(KATA) 구성 요소를 사용할 수 없습니다. EDR(KATA) 구성 요소는 버전 12.1에 도입되었습니다.

  - 관리 플러그인 12.1 이상 버전의 경우 애플리케이션이 **Endpoint Detection and Response(KATA)**의 전반적인 상태를 표시하며, 이는 Endpoint Sensor 상태 또는 EDR(KATA) 구성 요소 상태를 의미할 수 있습니다. 이는 사용자 컴퓨터에 설치된 애플리케이션의 버전과 Kaspersky Anti Targeted Attack Platform과 상호 작용하는 데 활용할 수 있는 이용 가능한 구성 요소의 버전에 따라 다릅니다.

- Kaspersky Endpoint Security 버전 12.6 이상부터 Kaspersky Security Center 웹 콘솔 버전 14.2 이하는 컴퓨터 속성에 있는 **Endpoint Detection and Response(KATA)** 구성 요소의 이름을 올바르게 표시하지 않습니다. **Endpoint Detection and Response(KATA)** 구성 요소 대신 애플리케이션에는 **Endpoint Detection and Response Expert (KATA EDR)** 구성 요소의 이름이 표시됩니다. 구성 요소 목록을 보려면 웹 콘솔에서 컴퓨터 속성을 열고 **애플리케이션** 섹션에서 Kaspersky Endpoint Security for Windows의 속성을 연 다음 **구성 요소** 섹션으로 이동합니다. Kaspersky Security Center 웹 콘솔 버전 15.1 이상부터 애플리케이션이 구성 요소 이름을 올바르게 표시합니다.

- Kaspersky Endpoint Detection and Response 관리 플러그인을 웹 콘솔 버전 14.0~14.2에 설치된 버전 15.3으로 업데이트하면 경고 세부 정보가 잘못 표시됩니다. 경고 세부 정보가 제대로 작동하려면 Kaspersky Security Center 중앙 관리 서버를 다시 시작하십시오.

- Kaspersky Endpoint Detection and Response 관리 플러그인 버전 15.4 이상은 Kaspersky Security Center 버전 14.0을 지원하지 않습니다. 관리 플러그인을 업데이트한 후 경고 세부 정보가 잘못 표시됩니다.

- Kaspersky Extended Detection and Response(XDR) 버전 1.4 클래스 솔루션은 Kaspersky Endpoint Security for Windows 웹 플러그인 버전 12.12 이상을 지원하지 않습니다. 현재 웹 플러그인 버전을 그대로 두거나 XDR 솔루션을 버전 2.0 이상으로 업데이트할 수 있습니다.

- Kaspersky Endpoint Security는 Arm 아키텍처용 개체를 Kaspersky Sandbox로 전송하지 않습니다.

- Arm 기반 컴퓨터에서는 Kaspersky Endpoint Detection and Response Expert와의 통합을 지원하지 않습니다.

기타 제한

- Windows 운영 체제는 버전 11 24H2부터 UDP Receive Segment Coalescing Offload(URO) 기술을 지원합니다. 호환 가능한 네트워크 카드 및 드라이버가 컴퓨터에 설치되어 있는 경우 이 기술은 기본적으로 활성화됩니다. 사용자 컴퓨터에서 URO를 사용하지 않도록 설정하면 애플리케이션의 성능이 크게 저하될 수 있습니다.

- Kaspersky Endpoint Security는 제한적으로 WSL 하위 시스템(Windows Subsystem for Linux)을 지원합니다.

  - WSL 1. 애플리케이션은 HTTP/HTTPS를 통해 네트워크 트래픽을 모니터링하고 위협을 탐지합니다. Kaspersky Endpoint Security는 자체 인증서를 사용하여 안전한 HTTPS 연결을 검사하기 때문에 일부 타사 애플리케이션의 작동이 중단될 수 있습니다.

  - WSL 2. 해당 애플리케이션은 WSL 2를 지원하지 않습니다.

- 오류를 반환하거나 작동이 중단된 애플리케이션은 자동으로 다시 시작될 수도 있습니다. 애플리케이션이 충돌로 인해 오류가 생기면, 다음 동작을 수행합니다:

  1. 제어 및 보호 기능을 중지합니다(암호화 기능은 사용 상태로 유지합니다).

  2. 기능이 중지되었다고 사용자에게 알립니다.

  3. 안티 바이러스 데이터베이스를 업데이트하거나 애플리케이션 모듈 업데이트를 적용한 후 기능을 복원하려고 시도합니다.

- 신뢰하는 목록에 추가된 웹 주소가 제대로 처리되지 않을 수 있습니다.

- Kaspersky Security Center 콘솔에서는 **고급 → 저장소 → 처리 안 된 위협** 폴더의 파일을 디스크에 저장할 수 없습니다. 파일을 저장하려면 감염된 파일을 치료해야 합니다. 치료 시 애플리케이션은 파일 복사본을 백업에 저장합니다. 이제 **고급 → 저장소 → 백업** 폴더의 파일을 디스크에 저장할 수 있습니다.

- 중앙 관리 서버로의 데이터 전송 설정 상속(**일반 설정 → 리포트 및 저장소 → 중앙 관리 서버로의 데이터 전송**)은 다른 설정의 상속과 다릅니다. 정책에서 데이터 전송 설정의 변경을 허용한 경우('자물쇠'가 열려 있음), 이러한 설정이 이전에 정의되지 않았다면 콘솔의 로컬 컴퓨터 속성에서 기본값으로 재설정됩니다. 이러한 설정이 이전에 정의된 경우 해당 값이 복원됩니다. 정책을 삭제하면 같은 방식으로 설정이 상속됩니다. 이러한 경우 로컬 컴퓨터 속성의 다른 설정이 정책에서 상속됩니다.

- Kaspersky Endpoint Security는 RFC 2616, RFC 7540, RFC 7541, RFC 7301 표준을 준수하는 HTTP 트래픽을 모니터링합니다. Kaspersky Endpoint Security가 HTTP 트래픽에서 다른 데이터 교환 형식을 탐지하면, 애플리케이션이 이 연결을 차단해 인터넷에서 악성 파일을 다운로드하는 것을 방지합니다.

- Kaspersky Endpoint Security는 QUIC 프로토콜을 통한 커뮤니케이션을 방지합니다. 브라우저의 QUIC 지원 활성화 여부와 무관하게 브라우저에서는 표준 전송 프로토콜(TLS 또는 SSL)을 사용합니다.

- 타사 소프트웨어가 Libcurl 라이브러리와 함께 작동하는 경우 TLS 연결 오류가 발생할 수 있습니다. 이것은 Kaspersky Endpoint Security가 암호화된 연결 검사를 위해 사용하는 Kaspersky 인증서와 관련될 수 있습니다. 작업을 계속하려면 타사 소프트웨어에 대한 인증서 유효성 검사를 비활성화하거나(권장하지 않음) Kaspersky 인증서 본문을 cURL 인증서 저장소에 추가할 수 있습니다. 자세한 내용은 Kaspersky 기술 자료를 참조하십시오.

- Kaspersky Endpoint Security for Windows를 처음 시작하면 디지털 서명된 애플리케이션이 일시적으로 잘못된 그룹에 배치될 수 있습니다. 디지털 서명된 애플리케이션은 이후 알맞은 그룹에 재배치됩니다.

- 제삼자 소프트웨어에 의해 차단된 악성 개체를 재검사하는 동안 같은 보안 위협이 다시 탐지되어도 사용자에게 알리지 않습니다. 보안 위협 재탐지 이벤트는 애플리케이션 리포트와 Kaspersky Security Center 리포트에 표시됩니다.

- 장치 암호화에 대한 Kaspersky Security Center 리포트에는 장치 제어 구성 요소가 설치되지 않은 서버 플랫폼이나 워크 스테이션에서 Microsoft BitLocker를 사용하여 암호화된 장치에 대한 정보가 포함되지 않습니다.

- Kaspersky Security Center 웹 콘솔에서는 모든 리포트 항목 표시를 활성화할 수 없습니다. 웹 콘솔에서는 리포트에 표시되는 항목의 수만 변경할 수 있습니다. 기본적으로 Kaspersky Security Center 웹 콘솔은 리포트 항목을 1,000개 표시합니다. 모든 리포트 항목 표시는 관리 콘솔(MMC)에서 활성화할 수 있습니다.

- Kaspersky Security Center 콘솔에서 리포트 항목을 1,000개 이상 표시하도록 설정할 수는 없습니다. 1,000보다 높은 값을 설정하면 Kaspersky Security Center 콘솔이 리포트 항목을 1,000개만 표시합니다.

- 정책 계층을 사용하면 부모 정책이 자식 정책의 이동식 드라이브 암호화 섹션 설정에 대한 수정을 금지한 경우 이 설정을 편집할 수 있습니다.

- 외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더 보호의 예외 규칙 기능이 제대로 작동하려면 운영 체제 설정에서 로그온 감사를 사용해야 합니다.

- 공유 폴더 보호를 사용하는 경우 Kaspersky Endpoint Security for Windows는 Kaspersky Endpoint Security for Windows가 시작되기 전에 시작된 각 원격 접근 세션에 대한 공유 폴더 암호화 시도를 감시합니다. 이 때 예외 규칙에 추가된 컴퓨터에서 시작된 원격 접근 세션도 감시 대상에 포함됩니다. Kaspersky Endpoint Security for Windows가 Kaspersky Endpoint Security for Windows 시작 전에 시작된 원격 접근 세션과 예외 규칙에 추가된 컴퓨터에서 시작된 원격 접근 세션의 공유 폴더 암호화 시도를 감시하지 않도록 하려면 원격 접근 세션을 종료하고 다시 시작하거나 Kaspersky Endpoint Security for Windows가 설치된 컴퓨터를 다시 시작합니다.

- 특정 사용자 계정의 권한으로 업데이트 작업을 실행하면 인증이 필요한 경로에서 업데이트 시 제품 패치가 다운로드되지 않습니다.

- 시스템 성능 부족으로 애플리케이션을 하지 못할 수 있습니다. 이 문제를 해결하려면 Ready Boot 옵션을 사용하거나 서비스 시작에 대한 운영 체제의 제한 시간을 늘리십시오.

- 애플리케이션은 Windows 안전 모드에서 작동하지 않습니다.

- 애플리케이션 설치 후 처음으로 다시 시작할 때까지 오디오 제어가 작동할 것이라고 보장할 수 없습니다.
- 관리 콘솔(MMC)에서는 애플리케이션 권한 구성 창의 침입 방지 설정에서 **제거** 버튼을 사용할 수 없습니다. 애플리케이션은 제어 그룹에서 애플리케이션의 마우스 오른쪽 메뉴를 통해 제거할 수 있습니다.
- 애플리케이션 로컬 인터페이스의 침입 방지 설정에서는 컴퓨터를 정책으로 관리 중일 시 애플리케이션 권한 및 보호 리소스를 볼 수 없습니다. 스크롤, 검색, 필터 등 기타 창 제어를 사용할 수 없습니다. 애플리케이션 권한은 Kaspersky Security Center 콘솔의 정책 속성에서 볼 수 있습니다.
- 순환식 추적 파일을 사용하면 AMSI 구성 요소 및 Outlook 플러그인에 대한 추적 로그를 생성하지 않습니다.
- Windows Server 2008에서는 성능 추적 로그를 직접 수집할 수 없습니다.
- "다시 시작" 추적 유형에 대한 성능 추적 로그는 지원하지 않습니다.
- 피코 프로세스에는 덤프 기록을 지원하지 않습니다.
- **시스템 서비스의 외부 관리 중지** 옵션을 끄면 `AMPPL=1` 파라미터로 설치된 애플리케이션의 서비스를 중지할 수 없습니다(파라미터값은 Windows 10RS2 운영 체제 버전에서부터 기본적으로 `1`로 설정됩니다). `AMPPL` 파라미터값이 `1`이면 제품 서비스에 대한 보호 프로세스 기술을 사용할 수 있습니다.
- 폴더에 사용자 지정 검사를 실행하려면 사용자 지정 검사를 시작하는 사용자에게 이 폴더의 속성을 읽을 수 있는 권한이 있어야 합니다. 그렇지 않으면 사용자 정의 폴더 검사가 불가능하며 오류가 발생합니다.
- 정책에 정의된 검사 규칙에 `C:\folder1\folder2`와 같이 끝에 `\` 문자가 없는 경로가 포함되면 경로 `C:\folder1\`에 대한 검사가 실행됩니다.
- 소프트웨어 제한 정책(Software Restriction Policies, SRP)를 사용하는 경우 컴퓨터를 로드하지 못할 수도 있습니다(검은 화면). 오작동을 방지하려면 SRP 속성에서 애플리케이션 라이브러리 사용을 허용해야 합니다. SRP 속성에서 khkum.dll 파일(**새로운 해시 규칙** 메뉴 아이템)에 대한 보안 수준이 **무제한**인 규칙을 추가합니다. 파일은 `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.0\klhk\klhk_x64\` 폴더에 있습니다. 이 방법을 선택했다면 추가로 Kaspersky Endpoint Security의 *업데이트* 작업 설정에서 **애플리케이션 모듈 업데이트 다운로드** 확인란을 선택 해제해야 합니다. SRP 사용에 대한 상세 정보는 Microsoft 설명서를 참조하십시오.

  SRP를 비활성화하고 Kaspersky Endpoint Security의 애플리케이션 제어 구성 요소로 애플리케이션 사용을 제어할 수도 있습니다.
- 컴퓨터가 DriverLoadPolicy 파라미터가 8(Good only, 양호만)로 설정된 Windows 그룹 정책 개체(Group Policy Object, GPO)의 도메인에 속하는 경우 Kaspersky Endpoint Security가 설치된 컴퓨터를 다시 시작하면 BSOD가 발생합니다. 오류를 방지하려면 그룹 정책의 ELAM(Early Launch Antimalware) 파라미터를 1(Good and unknown, 양호 및 알 수 없음)로 설정해야 합니다. ELAM 설정은 **컴퓨터 구성 → 관리 템플릿 → 시스템 → Early Launch Antimalware** 아래의 정책에 있습니다.
- Rest API를 통한 Outlook 플러그인 설정 관리는 지원하지 않습니다.
- 특정 사용자에 대한 작업 실행 설정은 구성 파일을 통한 장치 간 전송이 불가능합니다. 구성 파일에서 설정을 적용한 후 사용자 이름과 암호를 직접 지정합니다.
- 업데이트 설치 후 업데이트를 적용하기 위해 시스템을 다시 시작할 때까지 무결성 검사 작업이 작동하지 않습니다.

- 순환식 추적 로그 레벨이 원격 진단 유틸리티를 통해 변경되면 Kaspersky Endpoint Security for Windows가 표시하는 추적 로그 레벨이 빈값으로 잘못 표시됩니다. 그러나 추적 파일은 추적 레벨에 따라 올바르게 작성됩니다. 순환식 추적 로그 레벨이 애플리케이션의 로컬 인터페이스를 통해 변경되면, 추적 로그 레벨은 올바르게 수정되지만 원격 진단 유틸리티에서 마지막으로 정의한 추적 로그 레벨이 제대로 표시되지 않습니다. 이로 인해 관리자가 현재 추적 로그 레벨에 대한 최신 정보를 받지 못할 수 있으며 사용자가 애플리케이션의 로컬 인터페이스에서 추적 로그 레벨을 직접 변경한 경우 관련 정보가 추적 로그에서 누락될 수 있습니다.

- 암호 보호 설정에 따라 로컬 인터페이스에서는 관리자 계정의 이름을 변경할 수 없습니다(기본값은 KLAdmin). 관리자 계정의 이름을 변경하려면 암호 보호를 비활성화한 다음 암호 보호를 활성화하고 관리자 계정의 새 이름을 지정해야 합니다.

- Windows Server 2019 서버에 설치한 Kaspersky Endpoint Security 애플리케이션은 Docker와 호환되지 않습니다. Docker 컨테이너를 Kaspersky Endpoint Security가 설치된 컴퓨터에 배포 시 크래시가 발생합니다(BSOD).

- Kaspersky Endpoint Security가 SQL Server DBMS의 서버에 설치되어 있는 경우, 애플리케이션이 서버 인스턴스로 요청을 전송합니다. 이는 SQL Server 에이전트의 작업을 검사하고 악성 작업의 실행을 방지하는 데 필요합니다. Kaspersky Endpoint Security는 SQL Server 사용자 계정을 사용해 작업을 검사합니다. 애플리케이션은 시스템 메모리를 검사할 때와 안티 바이러스 데이터베이스를 업데이트한 후 서버에 요청을 전송합니다.

- Kaspersky Endpoint Security와 Secret Net Studio 소프트웨어의 호환성은 제한적입니다.

  - Kaspersky Endpoint Security 애플리케이션은 Secret Net Studio 소프트웨어의 안티 바이러스 구성 요소와 호환되지 않습니다.

    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.

  - Kaspersky Endpoint Security 애플리케이션은 Secret Net Studio 소프트웨어의 디스크 보호 및 데이터 암호화 구성 요소와 호환되지 않습니다.

    디스크 보호 및 데이터 암호화 구성 요소와 함께 Secret Net Studio가 배포된 컴퓨터에는 애플리케이션을 설치할 수 없습니다. 상호 운용이 가능하게 하려면 Secret Net Studio에서 디스크 보호 및 데이터 암호화 구성 요소를 제거해야 합니다.

  - Secret Net Studio는 Kaspersky Endpoint Security의 FLE(파일 수준 암호화) 구성 요소와 호환되지 않습니다.

    FLE(파일 수준 암호화) 구성 요소와 함께 Kaspersky Endpoint Security를 설치하면 Secret Net Studio 작동 시 오류가 발생할 수 있습니다. 상호 운용성을 보장하려면 Kaspersky Endpoint Security에서 파일 수준 암호화(FLE) 구성 요소를 제거해야 합니다.

- 시스템 무결성 모니터링 규칙을 가져올 때 애플리케이션이 규칙의 ID 및 이름을 확인합니다. 규칙 ID가 동일하면 Kaspersky Endpoint Security가 기존 규칙을 새 규칙으로 대체합니다. 규칙을 내보낼 때 애플리케이션이 자동으로 ID를 할당합니다. 예를 들어 내보낸 규칙 XML 파일을 수동으로 편집한 경우 ID가 동일한 규칙이 있을 수 있습니다. 규칙 ID가 고유하지만 규칙 이름이 동일하면 Kaspersky Endpoint Security가 규칙의 이름에 `(1)` 등을 추가합니다.

- Kaspersky Endpoint Security for Windows 버전 12.11부터는 웹 콘솔에서 자식 그룹에 열려 있는 부모 정책의 설정을 볼 수 없습니다. 웹 콘솔에는 다음과 같은 경고도 표시됩니다. *이 정책은 상속됩니다. 정책 설정은 생성된 중앙 관리 그룹 내에서만 편집할 수 있습니다.*

- 256자를 초과하는 팝업 알림은 관리 콘솔(MMC)에 표시되지 않습니다.

- 정책 및 설치 패키지의 구성 요소 이름은 다를 수 있습니다. 예를 들어 Endpoint Detection and Response Expert(on-premise)의 이름은 Endpoint Detection and Response(KATA), Endpoint Detection and Response Expert(on-premise), Kaspersky Anti Targeted Attack Platform Integration으로 지정할 수 있습니다. 애플리케이션 버전에 따라서도 구성 요소 이름이 다를 수 있습니다.

용어집

Cloud Discovery

Cloud Discovery는 사용자의 클라우드 서비스 액세스를 관리합니다. 클라우드 서비스에는 Microsoft Teams, Salesforce, Microsoft Office 365 등이 있습니다. 클라우드 서비스는 *파일 공유*, *메신저*, *이메일*과 같은 카테고리로 묶을 수도 있습니다.

IOC

침해지표. 악성 개체 또는 활동에 대한 데이터 세트입니다.

IOC 파일

애플리케이션이 탐지 횟수 계산을 위해 매치하는 침해지표(IOC) 세트를 포함하는 파일입니다. 검색 결과로 개체에 대해 여러 IOC 파일과 정확히 일치하는 항목이 발견되면 검색 가능성이 더 높아질 수 있습니다.

Kerberos 인증

클라이언트와 서버를 연결하기 전에 상호 인증하는 메커니즘으로, 안전하지 않은 네트워크를 통한 통신을 허용합니다. 이 메커니즘은 사용자가 신뢰하는 인증 센터에서 얻은 티켓을 기반으로 합니다.

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent 구성 요소. 보호해야 하는 각 가상 컴퓨터에 설치됩니다.

OLE 개체

다른 파일 내에 포함된 파일 또는 첨부파일을 의미합니다. Kaspersky 애플리케이션은 OLE 개체에 대해 바이러스 검사를 수행합니다. 예를 들어, Microsoft Office Excel® 표를 Microsoft Office Word 문서에 삽입하면 이 표는 OLE 개체로 검사됩니다.

OpenIOC

XML을 기반으로 하고 500개 이상의 다양한 침해지표를 포함하는 침해지표(IOC) 설명의 개방형 표준입니다.

SVM

안전한 가상 컴퓨터는 스캔 서버 서비스(Kaspersky Endpoint Security for Virtualization Light Agent의 구성 요소인 보호 서버)가 설치된 특수 가상 컴퓨터입니다.

감염 가능성이 있는 파일

구조 또는 형식상의 이유로 침입자가 악성 개체를 저장하고 유포할 "컨테이너"로 사용될 수 있는 파일입니다. 이러한 파일은 대개 .com, .exe 및 .dll과 같은 파일 확장명을 가진 실행 파일입니다. 여기에 악성 코드가 침투할 위험이 매우 높습니다.

감염된 파일

악성 코드(파일을 검사하는 동안 탐지된 알려진 위협의 코드)가 포함된 파일입니다. Kaspersky에서는 해당 파일이 컴퓨터를 감염시킬 수 있으므로 사용하지 않을 것을 권장합니다.

검사 범위

Kaspersky Endpoint Security가 검사 작업을 수행할 때 검사하는 개체입니다.

관리 그룹

공통 기능을 공유하는 장치 집합 및 해당 장치에 설치된 Kaspersky 애플리케이션의 집합입니다. 이들 장치는 하나의 단위로 편리하게 관리할 수 있도록 그룹화되어 있습니다. 하나의 그룹에는 다른 그룹이 포함될 수 있습니다. 그룹에 설치된 각 애플리케이션에 대해 그룹 정책 및 그룹 작업을 생성할 수도 있습니다.

네트워크 에이전트

중앙 관리 서버와 Kaspersky 애플리케이션 간의 상호 작용을 위해 특정 네트워크 노드(워크스테이션 또는 서버)에 설치되는 Kaspersky Security Center의 구성 요소입니다. 이 구성 요소는 Windows에서 실행되는 모든 Kaspersky 애플리케이션에 공통적으로 사용됩니다. 다른 운영 체제에서는 전용 네트워크 에이전트 버전이 필요합니다.

라이센스 인증서

Kaspersky가 키 파일 또는 활성화 코드와 함께 사용자에게 전송하는 문서입니다. 사용자에게 부여된 라이센스에 대한 정보가 들어 있습니다.

마스크

와일드카드를 사용하여 파일 이름 및 확장자를 나타낸 것입니다.

파일 마스크는 파일 이름으로 사용할 수 있도록 허용된 모든 문자를 포함하며 다음과 같은 와일드카드를 사용할 수 있습니다:

- `*`(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. ** 마스크는 검사 예외 생성 용도로만 사용 가능합니다.

- `?`(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 범위

필수 위협 보호가 실행 중일 때 그 보호 기능에 의해 지속적으로 검사되는 개체입니다. 각 구성 요소의 보호 범위는 서로 다른 속성을 가집니다.

신뢰하는 플랫폼 모듈

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.

악성 웹 주소 데이터베이스

위험한 것으로 간주되는 컨텐츠를 포함하는 웹 주소 목록입니다. 이 목록은 Kaspersky 전문가가 생성했습니다. 목록은 정기적으로 업데이트되며 Kaspersky 애플리케이션 배포 키트에 포함되어 있습니다.

안티 바이러스 데이터베이스

안티 바이러스 데이터베이스 배포 날짜에 Kaspersky에 알려진 컴퓨터 보안 위협에 대한 정보가 포함된 데이터베이스입니다. 안티 바이러스 데이터베이스 서명은 검사한 개체에서 악성 코드를 탐지하는 데 도움이 됩니다. 안티 바이러스 데이터베이스는 Kaspersky 전문가에 의해 만들어져 매 시간 업데이트됩니다.

압축 파일

하나 이상의 파일이 단일 압축 파일 안에 압축됩니다. 데이터를 압축하거나 압축 해제할 때 압축 프로그램이라고 말하는 전용 애플리케이션이 필요합니다.

인증 에이전트

암호화된 하드 드라이브에 접근하고 부팅 가능한 하드 드라이브 암호화 후 운영 체제를 로드하기 위한 인증 프로세스를 완료할 수 있는 인터페이스입니다.

인증서 발급자

인증서를 발급한 인증 센터입니다.

작업

실시간 파일 보호, 장치 전체 검사, 데이터베이스 업데이트 등과 같이 Kaspersky 애플리케이션에 의해 수행되는 기능이 작업으로 구현됩니다.

정규화된 형태의 웹 리소스 주소

정규화된 형태의 웹 리소스 주소는 정규화를 통해 웹 리소스 주소가 텍스트 형태로 나타난 것입니다. *정규화*란 웹 리소스 주소의 텍스트 표시가 특정 규칙에 따라 변경되는 프로세스입니다. 이러한 규칙의 예로는 텍스트 표시에서 사용자 로그인, 암호, 연결 포트를 예외하거나 웹리소스 주소를 대문자에서 소문자로 변경하는 것을 들 수 있습니다.

보호 구성 요소 동작에서 웹 리소스 주소의 정규화는 물리적으로는 동일해 보이지만 구문 상으로는 다른 웹사이트 주소를 두 번 이상 검사하지 않도록 하기 위한 목적으로 수행됩니다.

예:
비정규화된 형태의 주소: www.Example.com\.
정규화된 형태의 주소: www.example.com.

치료

감염된 개체를 처리하는 방법으로, 이를 통해 데이터의 전부 또는 일부가 복구됩니다. 감염된 개체 중 일부는 치료할 수 없습니다.

통합 서버

Kaspersky Endpoint Security for Virtualization Light Agent 구성 요소. Kaspersky Endpoint Security 구성 요소와 가상 인프라 간에 상호 작용합니다.

피싱 웹 주소 데이터베이스

Kaspersky 전문가가 피싱과 관련된 것으로 판단한 웹 주소 목록입니다. 데이터베이스는 정기적으로 업데이트되며 Kaspersky 애플리케이션 배포 키트에 포함되어 배포됩니다.

허위 경보

파일의 시그니처가 바이러스의 시그니처와 유사한 것으로 분석되어 Kaspersky 애플리케이션이 감염되지 않은 파일을 감염된 것으로 보고할 때 허위 경보가 발생합니다.

활성 키

현재 애플리케이션에서 사용 중인 키입니다.

휴대용 파일 관리자

컴퓨터에서 암호화 기능을 사용할 수 없는 경우 이동식 드라이브에 저장된 암호화된 파일에서 작업하기 위한 인터페이스를 제공하는 애플리케이션입니다.

부록

이 섹션에는 문서의 본문을 보완하는 정보가 포함되어 있습니다.

부록 1. 애플리케이션 설정

정책, 작업 또는 애플리케이션 인터페이스를 사용하여 Kaspersky Endpoint Security를 구성할 수 있습니다. 애플리케이션 구성 요소 관련 상세 정보는 해당 섹션에서 제공됩니다.

파일 위협 보호

파일 위협 보호 구성 요소를 사용하면 컴퓨터 파일 시스템의 감염을 방지할 수 있습니다. 기본적으로 파일 위협 보호 구성 요소는 컴퓨터의 RAM에 영구적으로 상주하며 열려 있는 파일, 저장된 파일, 실행된 파일을 모두 실시간으로 검사합니다. 이 구성 요소는 연결된 드라이브를 포함하여 모든 컴퓨터 드라이브의 파일을 검사합니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다.

이 구성 요소는 사용자 또는 애플리케이션이 접근한 파일을 검사합니다. 악성 파일이 탐지되면 Kaspersky Endpoint Security가 파일 동작을 차단합니다. 그런 다음 애플리케이션은 파일 위협 보호 구성 요소의 설정에 따라 악성 파일을 치료하거나 삭제합니다.

OneDrive 클라우드 저장소에 내용을 보관하는 파일에 접근을 시도하면 Kaspersky Endpoint Security는 파일 내용을 다운로드하여 검사합니다.

파일 위협 보호 구성 요소 설정

파라미터	설명
보안 레벨 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	Kaspersky Endpoint Security는 파일 위협 보호에 대해 다양한 설정 그룹을 적용할 수 있습니다. 애플리케이션에 저장된 설정 집합을 *보안 레벨*이라고 합니다: • **높음**. 이 파일 보안 레벨을 선택하는 경우 파일 위협 보호 구성 요소가 열려 있거나 저장 또는 시작되는 모든 파일을 가장 엄격하게 제어합니다. 파일 위협 보호 구성 요소가 컴퓨터의 모든 하드 드라이브, 이동식 드라이브, 네트워크 드라이브에서 모든 파일 유형을 검사합니다. 또한 압축 파일, 설치 프로그램 패키지 및 삽입된 OLE 개체에 대한 검사도 수행합니다. • **권장**. 이 파일 보안 레벨은 Kaspersky Lab 전문가가 권장하는 레벨입니다. 파일 위협 보호 구성 요소가 컴퓨터의 모든 하드 드라이브, 이동식 드라이브, 네트워크 드라이브에서 지정된 파일 형식과 삽입된 OLE 개체만 검사합니다. 파일 위협 보호 구성 요소가 압축 파일이나 설치 패키지는 검사하지 않습니다. • **낮음**. 이 파일 보안 레벨 설정에서 검사 속도가 가장 빠릅니다. 파일 위협 보호 구성 요소는 컴퓨터의 모든 하드 드라이브, 이동식 드라이브 및 네트워크 드라이브에서 지정된 확장자를 가진 파일만 검사합니다. 파일 위협 보호 구성 요소가 복합 파일은 검사하지 않습니다.
파일 유형 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	**모든 파일**. 이 설정을 사용하면 Kaspersky Endpoint Security가 예외 없이 모든 형식과 확장자의 파일을 검사합니다. **형식에 따라 검사한 파일**. 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일에 악성 코드가 있는지 검사하기 전에 파일의 내부 헤더를 분석하여 파일 형식을 결정합니다(예: txt, .doc 또는 .exe). 또한 이 검사에서는 특정 파일 확장자를 가진 파일도 찾습니다. **확장자에 따라 검사한 파일** 이 설정을 활성화하면 애플리케이션이 감염 위험이 있는 파일만 검사합니다. 파일 형식은 파일 확장자를 기반으로 결정됩니다.
검사 범위	파일 위협 보호 구성 요소에서 검사하는 개체가 나와 있습니다. 검사 개체는 하드 드라이브, 이동식 드라이브, 네트워크 드라이브, 폴더, 파일 또는 마스크로 정의된 다중 파일일 수 있습니다. 파일 위협 보호 구성 요소는 기본적으로 하드 드라이브, 네트워크 드라이브 또는 이동식 드라이브에서 시작되는 파일을 검사합니다. 이러한 개체의 보호 범위를 변경하거나 삭제할 수 없습니다. 검사에서 개체(예: 이동식 드라이브)를 제외만 할 수 있습니다.

파라미터	설명
머신 러닝 및 시그니처 분석 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	머신 러닝 및 시그니처 분석 기법은 알려진 위협과 이를 처리하는 방법에 대한 설명이 포함된 Kaspersky Endpoint Security 데이터베이스를 사용합니다. 이 방법을 사용하는 보호는 허용되는 최소한의 보안 레벨을 제공합니다. Kaspersky 전문가의 권고에 따라 기본적으로 머신 러닝과 시그니처 분석이 사용되도록 선택되어 있습니다.
휴리스틱 분석 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	현재 버전의 Kaspersky 애플리케이션 데이터베이스를 사용하여 식별할 수 없는 위협을 탐지하기 위해 개발된 기술입니다. 알려지지 않은 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 파일을 탐지합니다. 파일에서 악성 코드를 검사할 때 휴리스틱 분석기는 실행 파일의 명령을 실행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
위협 탐지 시 처리 방법	**치료 - 불가능한 경우 삭제**. 이 옵션을 선택하면 애플리케이션이 탐지한 감염 파일을 자동으로 치료합니다. 치료 실패 시 애플리케이션이 파일을 삭제합니다. **치료 - 불가능한 경우 차단**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 탐지된 모든 감염을 자동으로 치료합니다. 치료에 실패하면 Kaspersky Endpoint Security가 파일을 차단합니다(읽기/쓰기). **차단**. 이 옵션을 선택한 경우 파일 위협 보호 구성 요소가 탐지된 모든 감염 파일을 치료하려고 시도하지 않고 자동으로 차단합니다. 감염된 파일을 치료하거나 삭제하기 전에 애플리케이션이 파일을 복원하거나 나중에 치료할 수 있을 때에 대비하여 파일의 복사본을 만듭니다.
새로운 파일과 수정된 파일만 검사	새로운 파일과 마지막 검사 이후 수정된 파일만 검사합니다. 이는 검사 시간을 줄이는 것입니다. 이 모드는 단순 파일과 복합 파일 모두에 적용됩니다.
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	타사 애플리케이션의 배포 패키지 검사.
Microsoft Office 형식 파일 검사	Microsoft Office 파일(DOC, DOCX, XLS, PPT 및 기타 Microsoft 확장자)을 검사합니다. Office 형식 파일에는 OLE 개체도 포함됩니다. 애플리케이션이 확인란 선택 여부와 상관없이 1MB보다 작은 오피스 형식 파일을 검사합니다.
이메일 형식 파일 검사	이메일 형식 파일 검사. 애플리케이션이 MSG 및 EML 파일을 검사합니다. 이메일 형식 파일에는 OLE 개체 및 MHT 파일도 포함됩니다. Kaspersky Endpoint Security는 확인란 선택 여부와 상관없이 1MB보다 작은 이메일 형식 파일을 검사합니다.
큰 복합 파일은 압축 해제 안 함	이 확인란을 선택하면 애플리케이션이 지정된 크기를 초과하는 복합 파일을 검사하지 않습니다. 이 확인란을 선택하지 않으면 애플리케이션이 크기에 자격 증명 공급업체이 모든 파일을 검사합니다. 애플리케이션은 확인란의 선택 여부와 관계없이 압축 파일에서 압축 해제한 대용량 파일을 검사합니다.
백그라운드에서 복합 파일 압축 해제	이 확인란을 선택하면 애플리케이션이 파일을 검사하기 전에 지정된 값보다 큰 복합 파일에 대한 접근을 제공합니다. 이 경우 Kaspersky Endpoint Security는 백그라운드에서 복합 파일을 압축 해제하고 검사합니다. 애플리케이션이 파일을 압축 해제하고 검사한 후에만 이 값보다 작은 복합 파일에 접근할 수 있습니다. 이 확인란을 선택하지 않으면 애플리케이션이 모든 크기의 파일을 압축 해제하고 검사한 후에만 복합 파일에 대한 접근을 제공합니다.
검사 모드 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	Kaspersky Endpoint Security는 사용자, 운영 체제 또는 사용자 계정으로 실행되는 애플리케이션이 접근한 파일을 검사합니다. **스마트 모드**. 이 모드에서 파일 위협 보호는 개체에 대해 수행된 처리의 분석 내용에 따라 개체를 검사합니다. 예를 들어 Microsoft Office 문서 작업의 경우 Kaspersky Endpoint Security는 파일이 처음 열릴 때와 마지막에 닫힐 때 파일을 검사합니다. 그 사이에 파일에 쓰는 작업은 검사되지 않습니다. **접근 및 수정 시** 이 모드에서는 개체를 열거나 수정하려는 시도가 있을 때 파일 위협 보호가 개체를 검사합니다. **접근 시**. 이 모드에서는 개체를 열려는 시도가 있을 때만 파일 위협 보호가 개체를 검사합니다. **실행 시**. 이 모드에서는 개체를 실행하려는 시도가 있을 때만 파일 위협 보호가 개체를 검사합니다.

파라미터	설명
iSwift 기술 사용 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 데이터베이스 배포 날짜, 마지막 파일 검사 날짜, 검사 설정의 변경 사항 등을 고려하는 특수 알고리즘을 사용하여 검사에서 제외됩니다. iSwift 기술은 NTFS 파일 시스템에 적합하게 iChecker 기술을 발전시킨 형태입니다.
iChecker 기술 사용 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	이 기술은 검사에서 특정 파일을 예외하여 검사 속도를 높입니다. 파일은 Kaspersky Endpoint Security 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.
파일 위협 보호 일시 중지 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	지정된 시간에 또는 지정된 애플리케이션으로 작업할 때 파일 위협 보호의 작동을 자동으로 일시 중지합니다.
Windows 컨테이너에서 실행된 파일 작업 검사	컨테이너 내부에서 위협이 탐지되면 애플리케이션은 파일 위협 보호 구성 요소에 대해 선택된 동작을 적용합니다. **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.

웹 위협 보호

웹 위협 보호 구성 요소는 인터넷에서 악의적인 파일을 다운로드하지 못하도록 하며 악의적인 웹사이트와 피싱 웹사이트도 차단합니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다.

Kaspersky Endpoint Security는 HTTP-, HTTPS-, FTP-트래픽만 모니터링합니다. Kaspersky Endpoint Security는 URL 및 IP 주소를 검사합니다.

웹 위협 보호를 사용하려면 애플리케이션의 초기 구성을 완료해야 합니다.

- HTTPS 트래픽 모니터링의 경우, 암호화된 연결 검사를 활성화합니다(기본적으로 활성화되어 있습니다).
- Kaspersky Endpoint Security가 모니터링해야 하는 포트를 선택합니다(기본적으로 애플리케이션은 모든 포트를 모니터링합니다).
- Kaspersky Endpoint Security가 트래픽을 모니터링할 애플리케이션을 선택합니다. 대부분의 브라우저는 Kaspersky에서 권장하는 애플리케이션 목록에 이미 있습니다. 사용 중인 브라우저가 목록에 없는 경우 수동으로 추가하세요.
- 웹 트래픽에 웹 페이지 상호 작용 스크립트 삽입하는 것을 권장합니다(기본적으로 스크립트 삽입은 비활성화되어 있습니다). 이 스크립트를 사용하면 애플리케이션 이벤트 로그, OS 이벤트 로그 및 리포트에 대한 웹 위협 보호 이벤트를 등록할 수 있습니다.

사용자가 악성 및 피싱 웹사이트를 열려고 하면 Kaspersky Endpoint Security가 접근을 차단하고 경고를 표시합니다.

파라미터	설명
보안 레벨 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	애플리케이션은 웹 위협 보호에 대해 다양한 설정 그룹을 적용할 수 있습니다. 애플리케이션에 저장된 설정 집합을 *보안 레벨*이라고 합니다: • **높음**. 웹 위협 보호 구성 요소가 HTTP 및 FTP를 통해 컴퓨터에 도착하는 웹 트래픽을 최대한 자세히 검사하는 보안 레벨입니다. 웹 위협 보호는 전체 애플리케이션 데이터베이스를 사용하여 모든 웹 트래픽 개체를 자세히 검사하고 가능한 정밀하게 휴리스틱 분석을 수행합니다. • **권장**. 애플리케이션의 성능과 웹 트래픽 보안 간에 최적의 균형을 유지하는 보안 레벨입니다. 웹 위협 보호 구성 요소는 보통 검사 레벨의 휴리스틱 분석을 수행합니다. 이 웹 트래픽 보안 레벨은 Kaspersky 전문가가 권장한 것입니다. • **낮음**. 이 웹 트래픽 보안 레벨 설정은 최대 속도의 웹 트래픽 검사를 보장합니다. 웹 위협 보호 구성 요소는 빠른 검사 레벨의 휴리스틱 분석을 수행합니다.
위협 탐지 시 처리 방법	**차단**. 이 옵션을 선택하고 감염된 개체가 웹 트래픽에서 탐지되면 웹 위협 보호 구성 요소는 개체에 대한 접근을 차단하고 브라우저에 메시지를 표시합니다. **알림**. 이 옵션을 선택하고 웹 트래픽에서 감염된 개체가 탐지되면 Kaspersky Endpoint Security는 이 개체를 컴퓨터로 다운로드할 수 있도록 허용하지만 감염된 개체에 대한 정보를 처리 안 된 위협 목록에 추가합니다.
악성 웹 주소 데이터베이스에서 웹 주소 확인 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	링크를 검사하여 악성 웹 주소 데이터베이스에 포함되어 있는지 확인하면 거부 목록에 등록된 웹사이트를 추적할 수 있습니다. 악성 웹 주소 데이터베이스는 Kaspersky에서 관리하는 것으로 애플리케이션 설치 프로그램 패키지에 포함되어 있으며 Kaspersky Endpoint Security 데이터베이스 업데이트와 함께 사용하여 보완할 수 있습니다.
휴리스틱 분석 사용 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	현재 버전의 Kaspersky 애플리케이션 데이터베이스를 사용하여 식별할 수 없는 위협을 탐지하기 위해 개발된 기술입니다. 알려지지 않은 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 파일을 탐지합니다. 웹 트래픽에서 바이러스 및 보안위협이 있는 애플리케이션이 검사되면 휴리스틱 분석기는 실행 파일의 명령을 수행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
피싱 웹 주소 데이터베이스에서 웹 주소 확인 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	피싱 웹 주소 데이터베이스에는 피싱 공격을 실행할 때 사용된 현재 알려진 웹사이트의 웹 주소가 포함되어 있습니다. Kaspersky는 이 피싱 링크 데이터베이스를 국제피싱대응협의체(APWG: Anti Phising Working Group)에서 받은 주소로 보완합니다. 피싱 URL 데이터베이스는 애플리케이션 설치 프로그램 패키지에 포함되어 있으며 Kaspersky Endpoint Security 데이터베이스 업데이트와 함께 사용하여 보완할 수 있습니다.
신뢰하는 웹 주소의 웹 트래픽은 검사 안 함	이 옵션을 선택한 경우 웹 위협 보호 구성 요소는 주소가 신뢰하는 웹 주소 목록에 포함되어 있는 웹 페이지/웹사이트의 컨텐츠를 검사하지 않습니다. 웹 페이지/웹사이트의 지정 주소와 주소 마스크를 신뢰하는 웹 주소 목록에 추가할 수 있습니다. 또한 암호화된 연결에 대한 일반 예외 규칙 목록을 생성할 수도 있습니다. 이때, Kaspersky Endpoint Security는 웹 위협 보호, 메일 위협 보호, 웹 제어 구성 요소가 작업을 수행할 때 신뢰하는 웹 주소의 HTTPS 트래픽을 검사하지 않습니다.

메일 위협 보호

메일 위협 보호 구성 요소는 보내고 받는 이메일 메시지 첨부파일에 바이러스 및 기타 위협이 있는지 검사합니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 휴리스틱 분석을 통해 컴퓨터를 보호합니다.

메일 위협 보호는 수신 및 발신 메시지를 모두 검사할 수 있습니다. 애플리케이션은 다음 메일 클라이언트에서 POP3, SMTP, IMAP 및 NNTP를 지원합니다.

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail

- MyOffice Mail
- R7-Office Organizer

Mozilla Thunderbird, MyOffice Mail 및 R7-Office Organizer 메일 클라이언트의 트래픽을 검사하려면 인증서 저장소에 Kaspersky 인증서 추가하고 자체 인증서 저장소를 선택해야 합니다.

메일 위협 보호는 다른 프로토콜 및 메일 클라이언트를 지원하지 않습니다.

메일 위협 보호가 항상 메시지에 대해 *프로토콜 수준*의 액세스(예: Microsoft Exchange 솔루션을 사용하는 경우)를 얻을 수 있는 것은 아닙니다. 이러한 이유로 메일 위협 보호에는 Microsoft Office Outlook용 확장 프로그램이 포함됩니다. 확장 프로그램을 사용하면 *메일 클라이언트 수준*에서 메시지를 검색할 수 있습니다. 메일 위협 보호 확장 프로그램은 Outlook 2010, 2013, 2016, 2019, 2021, 2024 및 365의 32비트 버전을 지원합니다. Arm 기반 컴퓨터에서는 메일 위협 보호 확장 프로그램이 Arm64용 Outlook 2016, Outlook 2021, Outlook 2024 및 Outlook 365의 32비트 버전을 지원합니다.

메일 클라이언트가 브라우저에서 열려 있으면 메일 위협 보호 구성 요소가 메시지를 검사하지 않습니다.

첨부 파일에서 악성 파일이 탐지되면 Kaspersky Endpoint Security는 메시지 제목에 *[메시지가 처리되었습니다]<메시지 제목>*과 같이 수행 작업에 대한 정보를 추가합니다.

메일 위협 보호 구성 요소 설정

파라미터	설명
보안 레벨 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	애플리케이션은 메일 위협 보호에 대해 다양한 설정 그룹을 적용할 수 있습니다. 애플리케이션에 저장된 설정 집합을 *보안 레벨*이라고 합니다: • **높음**. 이 이메일 보안 레벨을 선택하면 메일 위협 보호 구성 요소가 이메일 메시지를 철저히 검사합니다. 메일 위협 보호 구성 요소는 수신 및 발신 이메일 메시지를 검사하고 정밀 휴리스틱 분석을 수행합니다. 높음 메일 보안 레벨은 위험도가 높은 환경에 권장합니다. 예를 들어, 중앙 집중식 이메일 보호로 보호되지 않는 홈 네트워크에서 무료 이메일 서비스에 연결하는 경우가 위험한 환경에 해당합니다. • **권장**. 애플리케이션의 성능과 이메일 보안 간에 최적의 균형을 유지하는 이메일 보안 레벨입니다. 메일 위협 보호 구성 요소는 수신 및 발신 이메일 메시지를 검사하고 보통 수준의 휴리스틱 분석을 수행합니다. 이 메일 트래픽 보안 레벨은 Kaspersky 전문가가 권장한 것입니다. • **낮음**. 이 이메일 보안 레벨을 선택하는 경우 메일 위협 보호 구성 요소가 받는 이메일 메시지만 검사하고 간단한 휴리스틱 분석을 수행하며 이메일 메시지에 첨부된 압축 파일을 검사하지 않습니다. 이 메일 보안 레벨에서는 메일 위협 보호 구성 요소가 운영 체제 리소스를 가장 적게 사용하며 가장 빠른 속도로 이메일 메시지를 검사합니다. 낮음 메일 보안 레벨은 확실하게 보호되는 안전한 환경에서 사용하는 경우 권장됩니다. 중앙 집중식 이메일 보안을 사용하는 기업 LAN이 그러한 환경에 속합니다.
위협 탐지 시 처리 방법	**치료 - 불가능한 경우 삭제**. 감염된 개체가 인바운드 또는 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 감염된 개체를 삭제합니다. 애플리케이션은 수행된 작업에 대한 정보를 *[메시지가 처리됨]<메시지 제목>* 등의 형식으로 메시지 제목에 추가합니다. **치료 - 불가능한 경우 차단**. 감염된 개체가 인바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 사용자는 안전한 첨부파일과 함께 메시지에 접근할 수 있습니다. 개체를 치료할 수 없는 경우 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 감염된 개체가 아웃바운드 메시지에서 탐지되면 애플리케이션은 탐지된 개체를 치료하려고 시도합니다. 개체를 치료할 수 없는 경우 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다. **차단**. 인바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션은 메시지 제목에 경고를 추가합니다. 사용자는 원본 첨부파일과 함께 메시지에 접근할 수 있습니다. 아웃바운드 메시지에서 감염된 개체가 탐지되면 애플리케이션이 메시지 전송을 차단하고 메일 클라이언트에 오류가 표시됩니다.
보호 범위 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	*보호 범위*에는 보내고 받는 메시지 또는 받는 메시지만과 같이 구성 요소에서 실행 시 확인하는 개체가 포함됩니다. 컴퓨터를 보호하려면 받는 메시지만 검사하면 됩니다. 보내는 메시지 검사를 켜서 감염된 파일이 압축 파일로 전송되지 않도록 할 수 있습니다. 예를 들어 오디오 및 비디오 파일과 같은 특정 형식의 파일이 전송되지 않도록 하려는 경우에도 보내는 메시지 검사를 켤 수 있습니다.
POP3, SMTP, NNTP, IMAP 트래픽 검사	POP3, SMTP, NNTP 및 IMAP 프로토콜을 통해 전송되는 트래픽에 대한 메일 위협 보호 구성 요소의 검사.

파라미터	설명
Microsoft Outlook 확장 프로그램 연결	이 확인란을 선택하면 POP3, SMTP, NNTP, IMAP 프로토콜을 통해 전송된 이메일 메시지의 검사를 Microsoft Outlook에 통합된 확장 프로그램에서 작동할 수 있습니다. Microsoft Outlook용 확장 프로그램을 사용하여 메일을 검사하는 경우 Cached Exchange Mode를 사용하는 것이 좋습니다. Exchange 캐싱 모드에 대한 자세한 내용 및 모드 사용 관련 권장 사항은 Microsoft 기술 자료를 참조하십시오.
휴리스틱 분석 *(관리 콘솔(MMC) 및 Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	현재 버전의 Kaspersky 애플리케이션 데이터베이스를 사용하여 식별할 수 없는 위협을 탐지하기 위해 개발된 기술입니다. 알려지지 않은 바이러스 또는 알려진 바이러스의 새로운 변형으로 인한 감염이 의심되는 파일을 탐지합니다. 파일에서 악성 코드를 검사할 때 휴리스틱 분석기는 실행 파일의 명령을 실행합니다. 휴리스틱 분석기가 실행하는 명령 수는 휴리스틱 분석기에 지정된 레벨에 따라 다릅니다. 휴리스틱 분석 레벨은 새로운 위협 검색의 정밀도와 운영 체제 리소스의 부하 간의 균형을 조절하고 휴리스틱 분석의 지속 시간을 설정합니다.
첨부된 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. 검사 과정에서 애플리케이션이 메시지 텍스트에 있는 압축 파일의 암호를 감지하면 이 암호를 사용하여 악성 애플리케이션용 압축 파일의 내용을 검사합니다. 이 경우 암호는 저장되지 않습니다. 검사할 때 압축 파일의 압축이 해제됩니다. 압축을 풀 때 애플리케이션 오류가 발생하는 경우에는 %systemroot%\temp 경로에 저장된 압축이 풀린 파일을 사용자가 직접 삭제할 수 있습니다. 이 파일의 접두사는 PR입니다.
Microsoft Office 형식의 첨부 파일 검사	Microsoft Office 파일(DOC, DOCX, XLS, PPT 및 기타 Microsoft 확장자)을 검사합니다. Office 형식 파일에는 OLE 개체도 포함됩니다. 애플리케이션이 확인란 선택 여부와 상관없이 1MB보다 작은 오피스 형식 파일을 검사합니다.
다음보다 큰 압축파일 검사 안 함: <N>MB	이 확인란을 선택하면 메일 위협 보호 구성 요소는 압축된 이메일 첨부 메시지의 크기가 지정된 값을 초과하는 경우 해당 파일을 검사 대상에서 예외합니다. 만일 확인란이 선택 해제되면 메일 위협 보호 구성 요소는 모든 크기의 이메일 첨부파일을 검사합니다.
압축파일 확인 시간을 다음으로 한정: N초	이 확인란을 선택한 경우 압축된 이메일 첨부 메시지를 검사하는 데 할당된 시간은 지정된 시간으로 제한됩니다.
첨부 파일 필터	첨부파일 필터링은 보내는 이메일 메시지에는 적용되지 않습니다. **필터링 비활성화**. 이 옵션을 선택한 경우 메일 위협 보호 구성 요소는 이메일 메시지에 첨부된 파일을 필터링하지 않습니다. **선택한 유형의 첨부 파일 이름 바꾸기**. 이 옵션을 선택하면 메일 위협 보호 구성 요소가 지정된 유형의 첨부파일 확장자의 마지막 문자를 밑줄 문자(예: attachment.doc_)로 바꿉니다. 따라서 파일을 열려면 파일 이름을 바꿔야 합니다. **선택한 유형의 첨부 파일 삭제**. 이 옵션을 선택한 경우 메일 위협 보호 구성 요소는 이메일 메시지에서 지정한 유형의 첨부파일을 삭제합니다. 파일 마스크 목록에서 이름을 바꾸거나 이메일 메시지에서 삭제할 첨부파일 유형을 지정할 수 있습니다.

네트워크 위협 보호

네트워크 위협 보호 구성 요소(침입 탐지 시스템, Intrusion Detection System, IDS라고도 함)는 인바운드 네트워크 트래픽에서 네트워크 공격의 활동 특성을 모니터링합니다. 애플리케이션은 사용자 컴퓨터에 시도된 네트워크 공격을 탐지하면 공격 컴퓨터와의 네트워크 연결을 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.

파라미터	설명
포트 스캐닝과 네트워크 플러딩을 공격으로 간주합니다	*네트워크 플러딩*은 조직의 네트워크 리소스(웹 서버 등)에 대한 공격입니다. 이 공격은 많은 양의 요청을 보내 네트워크 리소스 대역폭의 과부하를 유발합니다. 이러면 사용자가 조직의 네트워크 리소스에 접근할 수 없게 됩니다. *포트 검사* 공격은 컴퓨터의 UDP 포트, TCP 포트, 네트워크 서비스에 대한 검사로 구성됩니다. 공격자는 이 공격을 통해 컴퓨터의 취약점을 파악한 후 더 위험한 유형의 네트워크 공격을 수행할 수 있습니다. 또한 컴퓨터의 운영 체제를 식별하여 이 운영 체제에 적합한 네트워크 공격을 선택할 수 있습니다. 이 확인란을 선택하면 Kaspersky Endpoint Security가 이 공격을 탐지하기 위해 네트워크 트래픽을 모니터링합니다. 공격이 탐지되면 애플리케이션은 사용자에게 위험을 알리고 해당 이벤트를 Kaspersky Security Center로 보냅니다. 본 애플리케이션은 공격하는 컴퓨터에 대한 정보를 제공하여 보안 위협 대응 활동을 즉각적으로 수행할 수 있습니다. 허용된 애플리케이션 중 일부가 이러한 유형의 공격에서 일반적으로 발견되는 작업을 수행하면 이러한 유형의 공격 탐지를 비활성화할 수 있습니다. 이는 잘못된 알림을 방지하는 데 도움이 됩니다.
다음 시간 동안 공격 장치 차단: N분	이 옵션이 활성화되면 네트워크 위협 보호 구성 요소가 차단 목록에 컴퓨터 공격을 추가합니다. 이렇게 되면 첫 번째 네트워크 공격 시도가 발생한 후 지정된 기간 동안 네트워크 위협 보호 구성 요소에서 공격 컴퓨터와의 네트워크 연결을 차단합니다. 이를 통해 향후 동일한 주소에서 발생하는 네트워크 공격으로부터 사용자의 컴퓨터를 자동으로 보호할 수 있습니다. 공격 컴퓨터가 차단 목록에서 보내야 하는 최소 시간은 1분입니다. 최대 시간은 999분입니다. 네트워크 모니터 도구 창에서 차단 목록을 볼 수 있습니다. Kaspersky Endpoint Security는 애플리케이션이 다시 시작될 때와 네트워크 위협 보호 설정이 변경될 때 차단 목록을 지웁니다.
예외 규칙	이 목록은 네트워크 위협 보호 기능이 네트워크 공격을 차단하지 않는 IP 주소가 있습니다. 포트 및 프로토콜이 지정된 IP 주소를 추가할 수 있습니다. 애플리케이션은 예외 목록에 포함된 IP 주소로부터의 네트워크 공격에 대한 정보를 기록하지 않습니다.
MAC 스푸핑 보호	*MAC 스푸핑 공격*에서는 네트워크 장치(네트워크 카드)의 MAC 주소를 변경합니다. 그러면 공격자는 장치로 전송된 데이터를 다른 장치로 리다이렉트하고 이 데이터에 접근할 수 있습니다. Kaspersky Endpoint Security에서는 MAC 스푸핑 공격을 차단하고 공격 관련 알림을 수신할 수 있습니다.

방화벽

방화벽은 인터넷 또는 로컬 네트워크에서 작업하는 동안 컴퓨터에 대한 무단 연결을 차단합니다. 방화벽은 또한 컴퓨터에서 애플리케이션의 네트워크 활동을 제어합니다. 이를 통해 신원 도용 및 기타 공격으로부터 회사 LAN을 보호할 수 있습니다. 이 구성 요소는 안티 바이러스 데이터베이스, Kaspersky Security Network 클라우드 서비스 및 사전 정의된 *네트워크 규칙*을 통해 컴퓨터 보호 기능을 제공합니다.

네트워크 에이전트는 Kaspersky Security Center와 상호 작용 시 사용됩니다. 방화벽은 애플리케이션 네트워크 에이전트가 작동하는 데 필요한 네트워크 규칙을 자동으로 생성합니다. 결과적으로 방화벽은 컴퓨터에서 여러 포트를 엽니다. 열리는 포트는 컴퓨터의 역할(예: 배포 지점)에 따라 다릅니다. 컴퓨터에서 열리는 포트에 대한 자세한 내용은 Kaspersky Security Center 도움말을 참조하십시오.

네트워크 규칙

다음 레벨로 네트워크 규칙을 구성할 수 있습니다.

- *네트워크 패킷 규칙*. 네트워크 패킷 규칙은 애플리케이션에 관계없이 네트워크 패킷을 제한합니다. 이러한 규칙은 선택한 데이터 프로토콜의 특정 포트를 통과하는 인바운드 및 아웃바운드 트래픽을 제한합니다. Kaspersky Endpoint Security에는 Kaspersky 전문가가 권장하는 권한으로 네트워크 패킷 규칙이 사전 정의되어 있습니다.

- *애플리케이션 네트워크 규칙*. 애플리케이션 네트워크 규칙은 특정 애플리케이션의 네트워크 활동을 제한합니다. 이 규칙은 네트워크 패킷의 특성뿐 아니라 해당 네트워크 패킷의 주소로 지정되거나 네트워크 패킷을 발행한 특정 애플리케이션까지 고려합니다.

호스트 침입 방지 구성 요소는 *애플리케이션 권한*을 사용하여 운영 체제 리소스, 프로세스 및 개인 데이터에 대한 애플리케이션의 접근 제어를 제공합니다.

애플리케이션을 처음 시작할 때 방화벽은 다음 작업을 수행합니다.

1. 다운로드한 안티 바이러스 데이터베이스를 사용하여 애플리케이션의 보안을 확인합니다.

2. Kaspersky Security Network에서 애플리케이션의 보안을 확인합니다.

   Kaspersky Security Network 참가를 활성화 해 방화벽이 보다 효과적으로 작동하도록 도와주십시오.

3. 애플리케이션을 다음 중 하나의 신뢰 그룹에 배치합니다: *신뢰함*, *낮은 제한*, *높은 제한*, *신뢰하지 않음*.

   Kaspersky Endpoint Security가 애플리케이션 동작을 제어할 때 참조하는 권한은 제어 그룹이 정의합니다. Kaspersky Endpoint Security는 애플리케이션이 컴퓨터에 미칠 수 있는 위험 수준에 따라 해당 애플리케이션을 신뢰 그룹에 배치합니다.

   Kaspersky Endpoint Security는 방화벽 및 호스트 침입 방지 구성 요소의 제어 그룹에 애플리케이션을 배치합니다. 방화벽 또는 호스트 침입 방지에 대해서만 제어 그룹을 변경할 수 없습니다.

   KSN 참여를 거부하거나 네트워크가 없는 경우 Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 설정에 따라 애플리케이션을 제어 그룹에 배치합니다. KSN으로부터 애플리케이션의 평판을 받은 후 제어 그룹이 자동으로 변경될 수 있습니다.

4. 제어 그룹에 따라 애플리케이션의 네트워크 활동을 차단합니다. 예를 들어 *높은 제한* 제어 그룹의 애플리케이션은 네트워크 연결을 사용할 수 없습니다.

다음 번 애플리케이션을 시작할 때 Kaspersky Endpoint Security가 애플리케이션의 무결성을 확인합니다. 애플리케이션이 변경되지 않은 경우 구성 요소는 현재 네트워크 규칙을 사용합니다. 애플리케이션이 수정되었으면 Kaspersky Endpoint Security가 애플리케이션을 처음으로 시작하는 것처럼 다시 검사합니다.

네트워크 규칙 우선 순위

각 규칙에는 우선 순위가 있습니다. 규칙 목록에서 순위가 높을수록 그 우선 순위도 높습니다. 네트워크 활동이 여러 규칙에 추가되면 방화벽은 우선 순위가 가장 높은 규칙에 따라 네트워크 활동을 통제합니다.

네트워크 패킷 규칙은 애플리케이션 네트워크 규칙보다 우선합니다. 같은 네트워크 활동 유형에 대해 네트워크 패킷 규칙과 애플리케이션 네트워크 규칙이 모두 지정된 경우, 네트워크 패킷 규칙에 따라 네트워크 활동이 처리됩니다.

애플리케이션용 네트워크 규칙은 특정 방식으로 작동합니다. 애플리케이션용 네트워크 규칙에는 네트워크 상태, 즉 *공용 네트워크*, *로컬 네트워크*, *신뢰하는 네트워크*에 따른 접근 규칙이 포함되어 있습니다. 예를 들어 *높은 제한* 제어 그룹의 애플리케이션은 기본적으로 모든 상태의 네트워크에서 네트워크 활동이 허용되지 않습니다. 네트워크 규칙이 개별 애플리케이션(상위 애플리케이션)에 대해 지정되어 있는 경우, 다른 애플리케이션의 하위 프로세스가 상위 애플리케이션의 네트워크 규칙에 따라 실행됩니다. 애플리케이션에 대한 네트워크 규칙이 없으면 자식 프로세스는 애플리케이션 제어 그룹의 네트워크 접근 규칙에 따라 실행됩니다.

예를 들어, 브라우저 X를 제외한 모든 애플리케이션에 대해 모든 상태의 네트워크에서 네트워크 활동을 금지했습니다. 브라우저 X(부모 애플리케이션)에서 브라우저 Y 설치(자식 프로세스)를 시작하면 브라우저 Y 설치 프로그램이 네트워크에 접근하여 필요한 파일을 다운로드합니다. 설치 후 브라우저 Y는 방화벽 설정에 따라 네트워크 연결이 거부됩니다. 자식 프로세스로서 브라우저 Y 설치 프로그램의 네트워크 활동을 금지하려면 브라우저 Y 설치 프로그램에 대한 네트워크 규칙을 추가해야 합니다.

네트워크 연결 유형

방화벽을 사용하면 네트워크 연결 유형에 따라 네트워크 활동을 제어할 수 있습니다. Kaspersky Endpoint Security는 컴퓨터 운영 체제에서 네트워크 연결 유형을 수신합니다. 운영 체제의 네트워크 연결 유형은 사용자가 연결을 설정할 때 설정됩니다. Kaspersky Endpoint Security 설정에서 네트워크 연결 유형을 변경할 수 있습니다. 방화벽은 운영 체제가 아닌 Kaspersky Endpoint Security 설정에 지정된 네트워크 유형에 따라 네트워크 활동을 모니터링합니다.

다음 네트워크 연결 유형을 사용할 수 있습니다.

- **공용 네트워크**. 안티 바이러스 애플리케이션, 방화벽 또는 필터(예: 카페의 Wi-Fi)로 네트워크는 보호되지 않습니다. 방화벽은 이러한 네트워크에 연결된 컴퓨터의 사용자가 이 컴퓨터의 파일 및 프린터에 접근하지 못하게 차단합니다. 외부 사용자도 이 컴퓨터의 데스크톱에 원격 접근하여 공유 폴더의 데이터에 접근할 수 없습니다. 방화벽은 각 애플리케이션에 설정된 네트워크 규칙에 따라 이러한 애플리케이션의 네트워크 활동을 필터링합니다.

  방화벽은 기본적으로 인터넷에 *공용 네트워크* 유형을 할당합니다. 인터넷의 유형은 변경할 수 없습니다.

- **로컬 네트워크**. 이 컴퓨터의 파일 및 프린터에 대한 접근이 제한된 사용자를 위한 네트워크(예: 회사 LAN 또는 홈 네트워크).

- **신뢰하는 네트워크**. 컴퓨터가 공격이나 무단 데이터 접근 시도에 노출되지 않는 안전한 네트워크. 이 상태의 네트워크에서는 모든 네트워크 활동이 허용됩니다.

방화벽 구성 요소 설정

파라미터	설명
패킷 규칙	네트워크 패킷 규칙 목록이 있는 표입니다. 네트워크 패킷 규칙은 애플리케이션에 관계없이 네트워크 패킷을 제한하는 기능을 합니다. 이러한 규칙은 선택한 데이터 프로토콜의 특정 포트를 통과하는 인바운드 및 아웃바운드 트래픽을 제한합니다. 이 표에는 Microsoft Windows 운영 체제를 실행하는 컴퓨터의 네트워크 트래픽을 최적으로 보호하기 위해 Kaspersky에서 권장하는 사전 구성된 네트워크 패킷 규칙이 나열되어 있습니다. 방화벽은 각 네트워크 패킷 규칙의 실행 우선 순위를 설정합니다. 방화벽은 네트워크 패킷 규칙 목록에서 위에서 아래로 표시되는 순서에 따라 네트워크 패킷 규칙을 처리합니다. 방화벽은 네트워크 연결에 알맞은 최상위 네트워크 패킷 규칙을 찾고 네트워크 동작을 허용 또는 차단하여 이를 적용합니다. 그런 다음 방화벽은 특정 네트워크 연결에 대해 이후의 모든 네트워크 패킷 규칙을 무시합니다. 네트워크 패킷 규칙은 애플리케이션 네트워크 규칙보다 우선합니다.

파라미터	설명
사용 가능한 네트워크	이 표에는 방화벽이 컴퓨터에서 탐지하는 네트워크 연결 관련 정보가 포함됩니다. 기본적으로 인터넷에는 *공용 네트워크* 상태가 할당됩니다. 인터넷의 상태는 변경할 수 없습니다.
애플리케이션 규칙	**애플리케이션**. 방화벽 구성 요소에 의해 제어되는 애플리케이션 표. 애플리케이션은 제어 그룹으로 할당됩니다. 제어 그룹은 Kaspersky Endpoint Security가 애플리케이션의 네트워크 활동을 제어할 때 사용하는 권한을 정의합니다. 정책의 영향을 받는 컴퓨터에 설치된 모든 애플리케이션의 단일 목록에서 애플리케이션을 선택하고 이를 제어 그룹에 추가할 수 있습니다. **네트워크 규칙**. 제어 그룹의 일부인 애플리케이션에 대한 네트워크 규칙 표. 이 규칙에 따라 방화벽은 애플리케이션의 네트워크 활동을 통제합니다. 이 표는 Kaspersky 전문가가 권장하는 사전 정의된 네트워크 규칙을 표시합니다. 이러한 네트워크 규칙은 Windows 운영 체제를 실행하는 컴퓨터의 네트워크 트래픽을 최적으로 보호하기 위해 추가되었습니다. 사전 정의된 네트워크 규칙은 삭제할 수 없습니다.

BadUSB 공격 방지

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(아래 그림 참조). 이 절차는 키보드 인증을 의미합니다.

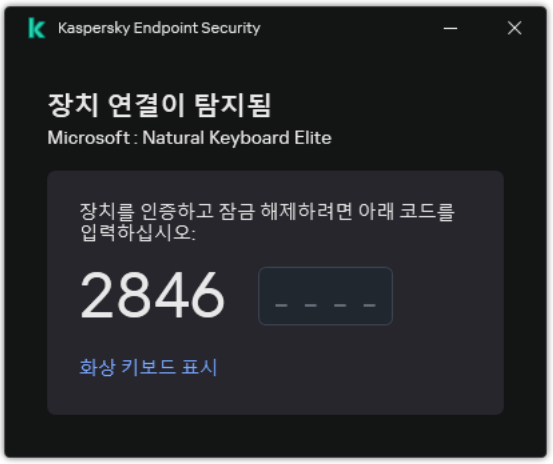
만일 해당 코드를 올바르게 입력했다면, 이 애플리케이션은 인증된 키보드 목록에 식별 파라미터(키보드의 VID/PID와 키보드가 연결된 포트 번호)를 저장합니다. 키보드를 다시 연결하거나 운영 체제를 재시작된 이후에는 키보드 인증을 반복할 필요가 없습니다.

> 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(아래 그림 참조) 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 요소는 기본적으로 설치되지 않습니다. BadUSB 공격 방지 구성 요소가 필요한 경우 애플리케이션을 설치하기 전에 설치 패키지 속성에 구성 요소를 추가하거나 애플리케이션을 설치한 후 사용 가능한 애플리케이션 구성 요소를 변경할 수 있습니다.



키보드 인증

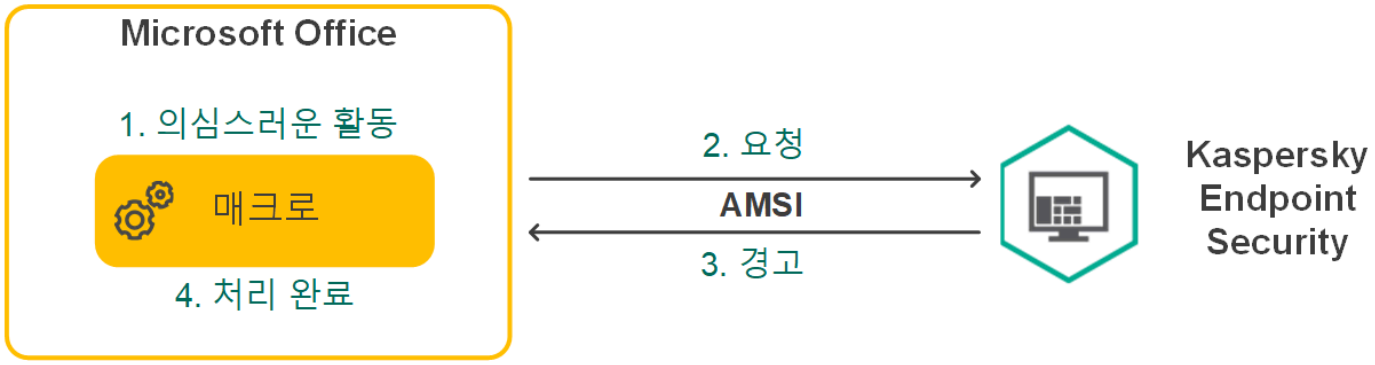
BadUSB 공격 방지 구성 요소 설정

파라미터	설명
USB 장치 인증 시 화상 키보드 사용 차단	이 토글 버튼을 켜면, 애플리케이션은 인증 코드를 입력할 수 없는 USB 장치의 인증을 위한 화상 키보드의 사용을 차단합니다.
USB 장치 인증에 바코드 사용 금지	이 토글 스위치를 활성화하면 애플리케이션이 바코드 스캐너 인증 알림에 바코드를 표시하지 않습니다.
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 Endpoint Security는 USB 장치의 차단 시간을 표시합니다. 이 시간이 지나면 인증 코드 입력 가능 횟수가 다시 5회 생깁니다.
최대 시도 횟수 도달 시 타임아웃	인증 코드 입력 시도가 지정된 횟수만큼 실패할 시 USB 장치 차단 시간. 유효한 값은 1~180(분)입니다.

AMSI 보호

AMSI 보호 구성 요소는 Microsoft의 Antimalware Scan Interface를 지원합니다. *AMSI(Antimalware Scan Interface)*를 사용하는 경우 AMSI를 지원하는 타사 애플리케이션이 추가 검사를 위해 Kaspersky Endpoint Security에 PowerShell 스크립트 등의 개체를 전송하고 해당 개체에 대한 검사 결과를 받을 수 있습니다. 타사 애플리케이션에는 Microsoft Office 애플리케이션 등이 포함됩니다(아래 그림 참조). AMSI에 대한 자세한 정보는 Microsoft 설명서를 참조하십시오.

AMSI 보호는 위협을 탐지하기만 하며 제삼자 애플리케이션에 탐지된 위협에 대해 알립니다. 위협 알림을 수신한 타사 애플리케이션은 악성 동작을 허용하지 않습니다.(예: 해당 동작을 종료함)



AMSI 작동 모드

AMSI 보호 구성 요소는 제삼자 애플리케이션의 요청 수가 지정된 간격 내의 최대 횟수를 초과하는 등의 경우에 해당 애플리케이션의 요청을 거부할 수 있습니다. Kaspersky Endpoint Security는 타사 애플리케이션에서 전송했으나 거부된 요청에 대한 정보를 중앙 관리 서버로 전송합니다. AMSI 보호 구성 요소는 AMSI 보호 구성 요소와의 지속적 통합이 활성화된 타사 애플리케이션의 요청을 거부하지 않습니다.

AMSI 보호를 사용할 수 있는 워크 스테이션 및 서버용 운영 체제는 다음과 같습니다:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise 멀티 세션
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter(Server Core 모드 포함)
- Windows Server 2019 Essentials / Standard / Datacenter(Server Core 모드 포함)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure 에디션(Server Core 모드 포함)
- Windows Server 2025 Standard / Datacenter

AMSI 보호 설정

파라미터	설명
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	타사 애플리케이션의 배포 패키지 검사.
Microsoft Office 형식 파일 검사	Microsoft Office 파일(DOC, DOCX, XLS, PPT 및 기타 Microsoft 확장자)을 검사합니다. Office 형식 파일에는 OLE 개체도 포함됩니다. 애플리케이션이 확인란 선택 여부와 상관없이 1MB보다 작은 오피스 형식 파일을 검사합니다.
큰 복합 파일은 압축 해제 안 함	이 확인란을 선택하면 애플리케이션이 지정된 크기를 초과하는 복합 파일을 검사하지 않습니다. 이 확인란을 선택하지 않으면 애플리케이션이 크기에 자격 증명 공급업체이 모든 파일을 검사합니다. 애플리케이션은 확인란의 선택 여부와 관계없이 압축 파일에서 압축 해제한 대용량 파일을 검사합니다.

익스플로잇 방지

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 Endpoint Security가 해당 파일의 실행을 차단하거나 해당 사용자에게 알립니다.

익스플로잇 방지 구성 요소는 네트워크 포트에서 컴퓨터의 보안을 위협할 수 있는 애플리케이션 프로세스를 추가로 모니터링합니다. 애플리케이션은 안티 바이러스 데이터베이스를 사용하여 이러한 프로세스에 대한 정보를 가져옵니다.

익스플로잇 방지 구성 요소 설정

파라미터	설명
익스플로잇 탐지 시	**차단**. 이 항목을 선택하면 익스플로잇 탐지 시 Kaspersky Endpoint Security가 이 익스플로잇의 동작을 차단하고 이 익스플로잇에 관한 정보가 포함된 로그 항목을 만듭니다. **알림**. 이 항목을 선택하면 Kaspersky Endpoint Security가 익스플로잇 탐지 시 이 익스플로잇에 관한 정보가 포함된 로그 항목을 만들고 이 익스플로잇에 관한 정보를 처리 안 된 보안위협 목록에 추가합니다.
시스템 프로세스 메모리 보호 사용	이 토글 버튼을 켜면 Kaspersky Endpoint Security가 시스템 프로세스 메모리에 접근하려는 외부 프로세스를 차단합니다.

행동 탐지

행동 탐지 구성 요소는 컴퓨터에 설치된 애플리케이션의 동작에 대한 데이터를 수신한 후 보호 구성 요소의 성능 향상을 위해 다른 구성 요소에 이 정보를 제공합니다. 행동 탐지 구성 요소는 애플리케이션의 행동 스트림 서명(BSS)을 활용합니다. 애플리케이션 동작이 행동 스트림 시그니처와 일치할 경우 Kaspersky Endpoint Security는 선택된 처리 방법을 수행합니다. Kaspersky Endpoint Security 기능은 행동 스트림 서명을 바탕으로 하며 컴퓨터에 대한 사전 방역을 제공합니다.

행동 탐지 구성 요소는 네트워크 포트에서 컴퓨터의 보안을 위협할 수 있는 애플리케이션 프로세스를 추가로 모니터링합니다. 애플리케이션은 안티 바이러스 데이터베이스를 사용하여 이러한 프로세스에 대한 정보를 가져옵니다.

행동 탐지 구성 요소 설정

파라미터	설명
악성 코드 활동 감지 시 처리 방법	**삭제**. 이 옵션을 선택하면 악성 코드 활동 탐지 시 Kaspersky Endpoint Security가 악성 코드의 실행 파일을 삭제하고 백업 저장소에 백업 복사본을 생성합니다. **차단**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 악성 코드 활동 탐지 시 해당 애플리케이션을 종료합니다. **알림**. 이 옵션을 선택한 상태에서 애플리케이션의 악성 코드 활동이 탐지되면 Kaspersky Endpoint Security는 이 애플리케이션을 종료하지 못합니다. 하지만 이 애플리케이션의 악성 코드 활동에 대한 정보를 처리 안 된 위협 목록에 추가합니다.

호스트 침입 방지

호스트 침입 방지 구성 요소는 애플리케이션이 운영 체제에 위험할 수 있는 작업을 수행하지 못하게 하고 운영 체제 리소스 및 개인 데이터에 대한 접근을 제어합니다. 이 구성 요소는 안티 바이러스 데이터베이스 및 Kaspersky Security Network 클라우드 서비스를 통해 컴퓨터를 보호합니다.

이 구성 요소는 *애플리케이션 권한*을 사용하여 애플리케이션의 작동을 제어합니다. 애플리케이션 권한에는 다음과 같은 접근 파라미터가 포함됩니다.

- 운영 체제 리소스에 접근(예: 자동 시작 옵션, 레지스트리 키)
- 개인 데이터에 접근(예: 파일 및 애플리케이션)

애플리케이션의 네트워크 활동은 *네트워크 규칙*을 사용하여 방화벽 구성 요소에 의해 제어됩니다.

애플리케이션을 처음 시작하는 동안 호스트 침입 방지 구성 요소는 다음 작업을 수행합니다.

1. 다운로드한 안티 바이러스 데이터베이스를 사용하여 애플리케이션의 보안을 확인합니다.
2. Kaspersky Security Network에서 애플리케이션의 보안을 확인합니다.

   Kaspersky Security Network 참가를 활성화 해 호스트 침입 방지 구성 요소가 보다 효과적으로 작동하도록 도와주십시오.

3. 애플리케이션을 다음 중 하나의 신뢰 그룹에 배치합니다: *신뢰함*, *낮은 제한*, *높은 제한*, *신뢰하지 않음*.

   Kaspersky Endpoint Security가 애플리케이션 동작을 제어할 때 참조하는 권한은 제어 그룹이 정의합니다. Kaspersky Endpoint Security는 애플리케이션이 컴퓨터에 미칠 수 있는 위험 수준에 따라 해당 애플리케이션을 신뢰 그룹에 배치합니다.

   Kaspersky Endpoint Security는 방화벽 및 호스트 침입 방지 구성 요소의 제어 그룹에 애플리케이션을 배치합니다. 방화벽 또는 호스트 침입 방지에 대해서만 제어 그룹을 변경할 수 없습니다.

   KSN 참여를 거부하거나 네트워크가 없는 경우 Kaspersky Endpoint Security는 호스트 침입 방지 구성 요소의 설정에 따라 애플리케이션을 제어 그룹에 배치합니다. KSN으로부터 애플리케이션의 평판을 받은 후 제어 그룹이 자동으로 변경될 수 있습니다.

4. 제어 그룹에 따라 애플리케이션 작업을 차단합니다. 예를 들어 *높은 제한* 제어 그룹의 애플리케이션은 운영 체제 모듈에 대한 접근이 거부됩니다.

다음 번 애플리케이션을 시작할 때 Kaspersky Endpoint Security가 애플리케이션의 무결성을 확인합니다. 애플리케이션에 변화가 없으면 구성 요소가 애플리케이션에 현재 애플리케이션 권한을 사용합니다. 애플리케이션이 수정되었으면 Kaspersky Endpoint Security가 애플리케이션을 처음으로 시작하는 것처럼 다시 검사합니다.

호스트 침입 방지 구성 요소 설정

파라미터	설명
애플리케이션 권한	호스트 침입 방지 구성 요소가 모니터링하는 애플리케이션 표. 애플리케이션은 제어 그룹으로 할당됩니다. Kaspersky Endpoint Security가 애플리케이션 동작을 제어할 때 참조하는 권한은 제어 그룹이 정의합니다. 정책의 영향을 받는 컴퓨터에 설치된 모든 애플리케이션의 단일 목록에서 애플리케이션을 선택하고 이를 제어 그룹에 추가할 수 있습니다. 애플리케이션 접근 권한은 다음 표에 나와 있습니다. • **파일 및 시스템 레지스트리**. 제어 그룹에 속하는 애플리케이션의 운영 체제 리소스 및 개인 데이터에 대한 접근 권한 표. • **권한**. 제어 그룹에 속하는 애플리케이션의 운영 체제 프로세스 및 리소스에 대한 접근 권한 표. • **네트워크 규칙**. 제어 그룹의 일부인 애플리케이션에 대한 네트워크 규칙 표. 이 규칙에 따라 방화벽은 애플리케이션의 네트워크 활동을 통제합니다. 이 표는 Kaspersky 전문가가 권장하는 사전 정의된 네트워크 규칙을 표시합니다. 이러한 네트워크 규칙은 Windows 운영 체제를 실행하는 컴퓨터의 네트워크 트래픽을 최적으로 보호하기 위해 추가되었습니다. 사전 정의된 네트워크 규칙은 삭제할 수 없습니다.

파라미터	설명
보호되는 리소스	이 표에는 컴퓨터 리소스가 분류별로 나열되어 있습니다. 호스트 침입 방지 구성 요소는 표의 리소스에 접근하려는 다른 애플리케이션의 시도를 감시합니다. 리소스는 레지스트리 카테고리, 파일, 폴더, 레지스트리 키 등이 될 수 있습니다.
Kaspersky Endpoint Security 시작 전에 실행된 애플리케이션에 대한 제어 그룹	Kaspersky Endpoint Security가 Kaspersky Endpoint Security보다 먼저 시작할 애플리케이션을 배치하는 제어 그룹.
KSN에 등록되지 않은 애플리케이션에 대한 권한 업데이트	이 확인란을 선택하면 호스트 침입 방지 구성 요소가 Kaspersky Security Network 데이터베이스를 사용하여 등록이 되지 않은 애플리케이션에 대한 권한을 업데이트합니다.
디지털 서명된 애플리케이션 신뢰	이 확인란을 선택하면 호스트 침입 방지 구성 요소가 신뢰하는 공급업체의 디지털 서명이 있는 애플리케이션을 *신뢰하는* 그룹에 할당합니다. *신뢰하는 공급업체*는 Kaspersky에서 신뢰하는 소프트웨어 공급 업체입니다. 공급업체 인증서를 신뢰하는 인증서 저장소에 직접 추가할 수도 있습니다. 이 확인란을 선택 해제하면 호스트 침입 방지 구성 요소가 이러한 애플리케이션을 신뢰하지 않으며 다른 파라미터를 사용하여 제어 그룹을 결정합니다.
다음 기간 동안 사용하지 않은 애플리케이션에 대한 규칙 삭제: N일(1~90)	이 확인란을 선택하면 다음과 같은 조건이 충족되는 경우 Kaspersky Endpoint Security는 애플리케이션에 대한 정보(제어 그룹 및 접근 권한)를 자동으로 삭제합니다. • 수동으로 애플리케이션을 제어 그룹에 넣거나 접근 권한을 구성한 경우. • 정의된 기간 내에 애플리케이션이 시작되지 않은 경우. 애플리케이션의 제어 그룹과 권한이 자동으로 결정되면 Kaspersky Endpoint Security는 30일 후 이 애플리케이션에 대한 정보를 삭제합니다. 애플리케이션 정보의 저장 기간을 변경하거나 자동 삭제를 해제할 수 없습니다. 다음에 이 애플리케이션을 시작하면 Kaspersky Endpoint Security는 애플리케이션을 처음으로 시작하는 것처럼 다시 검사합니다.
다른 그룹에 포함되지 않은 애플리케이션의 제어 그룹	이 드롭다운 목록의 항목에 따라 Kaspersky Endpoint Security가 알 수 없는 애플리케이션을 할당할 신뢰 그룹이 결정됩니다. 다음 항목 중 하나를 선택할 수 있습니다: • **낮은 제한**. • **높은 제한**. • **신뢰하지 않음**.

복원 엔진

복원 엔진을 사용하면 Kaspersky Endpoint Security가 운영 체제에서 악성 코드에 의해 수행된 활동을 롤백합니다.

운영 체제에서 악성 코드가 수행한 동작을 롤백할 때 Kaspersky Endpoint Security는 다음과 같은 유형의 악성 코드를 처리합니다:

- **파일 활동**

  Kaspersky Endpoint Security는 다음 동작을 수행합니다:

  - 악성 코드에 의해 생성된 실행 파일을 삭제합니다(네트워크 드라이브를 제외한 모든 미디어에서).
  - 악성 코드에 의해 침입된 프로그램이 생성한 실행 파일을 삭제합니다.
  - 악성 코드에 의해 수정되거나 삭제된 파일을 복원합니다.

  파일 복구 기능에는 여러 가지 제한이 있습니다.

- **레지스트리 활동**

Kaspersky Endpoint Security는 다음 동작을 수행합니다:

- 악성 코드에서 생성한 레지스트리 키를 삭제합니다.
- 악성 코드에서 변경하거나 삭제한 레지스트리 키는 복원하지 않습니다.

- **시스템 활동**

  Kaspersky Endpoint Security는 다음 동작을 수행합니다:

  - 악성 코드에 의해 시작된 프로세스를 종료합니다.
  - 악성 애플리케이션이 침투한 프로세스를 종료합니다.
  - 악성 코드에 의해 중지된 프로세스는 재시작하지 않습니다.

- **네트워크 활동**

  Kaspersky Endpoint Security는 다음 동작을 수행합니다:

  - 악성 코드의 네트워크 활동을 차단합니다.
  - 악성 코드가 침투한 프로세스의 네트워크 활동을 차단합니다.

악성 코드 활동의 롤백은 파일 위협 보호, 행동 탐지 구성 요소 또는 악성 코드 검사에 의해 시작됩니다.

악성 코드 활동을 롤백하면 엄격하게 정의된 데이터 집합에는 영향을 줍니다. 롤백은 운영 체제 또는 컴퓨터 데이터의 무결성에는 악영향이 없습니다.

Kaspersky Security Network



Kaspersky Endpoint Security는 사용자 컴퓨터를 보다 효과적으로 보호하기 위해 전세계 사용자로부터 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 Endpoint Security에서 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 Endpoint Security는 검사한 웹 주소의 평판 정보는 물론이고 검사한 파일의 카테고리 및 평판에 관한 정보도 수신하게 됩니다.

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 Endpoint Security는 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 Endpoint Security 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 설정

파라미터	설명
확장 KSN 모드 사용	*확장 KSN 모드*는 Kaspersky Endpoint Security가 추가 데이터를 Kaspersky로 전송하는 모드입니다. Kaspersky Endpoint Security는 KSN을 사용하여 토글 위치에 관계없이 위협을 탐지합니다.
클라우드 모드 사용	*클라우드 모드* Kaspersky Endpoint Security가 경량 버전의 안티 바이러스 데이터베이스를 사용하는 애플리케이션 운영 모드를 의미합니다. Kaspersky Security Network는 경량의 안티 바이러스 데이터베이스가 사용 중일 때 애플리케이션의 운영을 지원합니다. 경량 버전의 안티 바이러스 데이터베이스를 사용하면 일반 데이터베이스에 비해 절반 가량의 컴퓨터 RAM을 사용하게 됩니다. Kaspersky Security Network에 참여하지 않거나 클라우드 모드를 사용하지 않는 경우 Kaspersky Endpoint Security는 Kaspersky 서버에서 전체 버전의 안티 바이러스 데이터베이스를 다운로드합니다. 이 토글 버튼을 켜면 Kaspersky Endpoint Security가 안티 바이러스 데이터베이스의 경량 버전을 사용하여 운영 체제 리소스의 로드를 줄입니다. 이 확인란을 선택하면 다음 번 업데이트 시 Kaspersky Endpoint Security가 안티 바이러스 데이터베이스의 경량 버전을 다운로드합니다. 이 토글 버튼을 끄면 Kaspersky Endpoint Security가 안티 바이러스 데이터베이스의 정식 버전을 사용합니다. 이 확인란의 선택을 취소한 후 다음 번 업데이트 시 Kaspersky Endpoint Security가 안티 바이러스 데이터베이스의 정식 버전을 다운로드합니다.
KSN 서버를 이용할 수 없을 때 컴퓨터 상태 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	KSN 서버를 사용할 수 없을 때 이 드롭다운 목록의 항목에 따라 Kaspersky Security Center의 컴퓨터 상태가 결정됩니다.
중앙 관리 서버를 KSN 프록시 서버로 사용 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이 확인란을 선택하면 Kaspersky Endpoint Security가 KSN 프록시 서비스를 사용합니다. 중앙 관리 서버 속성에서 KSN 프록시 서비스 설정을 구성할 수 있습니다.
KSN 프록시 서버를 이용할 수 없는 경우 Kaspersky Security Network 서버 사용 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이 확인란을 선택하면 Kaspersky Endpoint Security가 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.

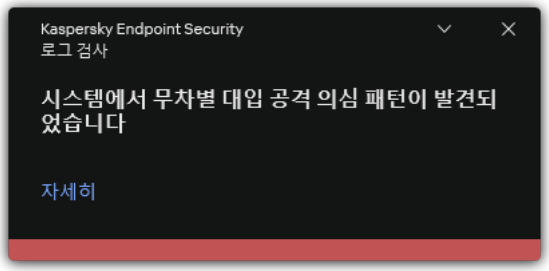
로그 검사

이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

Kaspersky Endpoint Security for Windows는 11.11.0 버전부터 로그 검사 구성 요소를 포함합니다. 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 Endpoint Security는 규칙에 따라 Windows 이벤트 로그를 분석하여 위반 사항을 감지합니다. 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(아래 그림 참조).

로그 검사를 사용하려면 감사 정책 보안 설정이 구성되어 시스템에서 관련 이벤트를 기록하는지 확인해야 합니다(자세한 내용은 Microsoft 기술 지원 웹사이트 참조).



로그 검사 알림

로그 검사 설정

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.

Anti-Cryptor

Anti-Cryptor 구성 요소는 공유 폴더의 활동을 분석합니다. 이 활동이 외부 암호화에서 일반적으로 나타나는 행동 스트림 시그니처와 일치하면 Kaspersky Endpoint Security가 선택한 동작을 수행합니다.

Kaspersky Endpoint Security는 NTFS 파일 시스템의 미디어에 위치하고 EFS 시스템에 의해 암호화되지 않은 파일에 대해서만 외부 암호화를 방지합니다.

파라미터	설명
이름 또는 IP 주소로 예외 설정	**이름 또는 IP 주소로 예외 설정**. 공유 폴더 암호화 시도를 모니터링하지 않는 컴퓨터의 목록입니다. 외부 컴퓨터에서 시도하는 암호화로부터 공유 폴더를 보호하는 기능에서 예외 컴퓨터 목록을 적용하려면, Windows 보안 감사 정책에서 감사 로그온을 활성화해야 합니다. 감사 로그온은 기본적으로 비활성화되어 있습니다. Windows 보안 감사 정책에 대한 자세한 내용은 Microsoft 웹사이트를 참조하시기 바랍니다. **마스크로 예외 설정**. 보호 범위 예외 규칙. 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, 행동 탐지가 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. 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.
위협 탐지 시 처리 방법	• **알림**. 이 옵션을 선택하면 공유 폴더에 있는 파일에 대한 수정 시도가 탐지될 때 Kaspersky Endpoint Security가 해당 시도에 대한 정보를 활성 위협 목록에 추가하고, 로컬 애플리케이션 인터페이스 리포트에 항목을 추가하고, 탐지된 악성 활동에 대한 정보를 Kaspersky Security Center로 전송합니다. • **다음 시간 동안 연결 차단(분) N분**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 공유 폴더의 파일 수정 시도 탐지 시, 악의적 행위를 시작한 세션의 파일 수정 접근 권한을 차단하고 수정된 파일의 백업 복사본을 생성합니다. 복원 엔진 구성 요소를 활성화하고 **다음 시간 동안 연결 차단(분) N분** 옵션을 선택하면 수정된 파일을 백업 복사본에서 복원합니다.
보호 범위	*보호 범위*는 Kaspersky Endpoint Security가 파일 활동을 감시하는 공유 폴더의 경로 목록입니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다. 기본적으로 애플리케이션은 공유 폴더를 자동으로 식별하고 모든 폴더의 파일 활동을 모니터링합니다.

웹 제어

웹 제어는 웹 리소스에 대한 사용자의 접근을 관리합니다. 이렇게 하면 트래픽을 줄이고 업무 시간을 부적절하게 사용하는 것도 줄일 수 있습니다. 사용자가 웹 제어에 의해 제한되는 웹사이트를 열려고 하면 Kaspersky Endpoint Security가 접근을 차단하거나 경고를 표시합니다(아래 그림 참조).

웹 제어를 사용하려면 애플리케이션의 초기 구성을 완료해야 합니다:

- HTTPS 트래픽 모니터링의 경우, 암호화된 연결 검사를 활성화합니다(기본적으로 활성화되어 있습니다).
- Kaspersky Endpoint Security가 모니터링해야 하는 포트를 선택합니다(기본적으로 애플리케이션은 모든 포트를 모니터링합니다).
- Kaspersky Endpoint Security가 트래픽을 모니터링할 애플리케이션을 선택합니다. 대부분의 브라우저는 Kaspersky에서 권장하는 애플리케이션 목록에 이미 있습니다. 사용 중인 브라우저가 목록에 없는 경우 수동으로 추가하세요.
- 웹 트래픽에 웹 페이지 상호 작용 스크립트 삽입하는 것을 권장합니다(기본적으로 스크립트 삽입은 비활성화되어 있습니다). 이 스크립트를 사용하면 애플리케이션 이벤트 로그, OS 이벤트 로그 및 리포트에 대한 웹 제어 이벤트를 등록할 수 있습니다.

웹사이트 접근을 관리하는 방법

웹 제어에서는 다음 방법으로 웹사이트에 대한 접근을 구성할 수 있습니다:

- **웹사이트 카테고리**. 웹사이트는 Kaspersky Security Network 클라우드 서비스, 휴리스틱 분석 및 알려진 웹사이트 데이터베이스(애플리케이션 데이터베이스에 포함)에 따라 분류됩니다. 예를 들어, *소셜 네트워크* 카테고리 또는 다른 카테고리에 대한 사용자 접근을 제한할 수 있습니다.
- **데이터 유형**. 이미지를 숨기는 등 웹사이트의 데이터에 대한 사용자 접근을 제한할 수 있습니다. Kaspersky Endpoint Security는 파일 확장자가 아니라 파일 형식에 따라 데이터 유형을 결정합니다.

  > Kaspersky Endpoint Security는 압축 파일에 포함된 파일을 검사하지 않습니다. 예를 들어, 이미지 파일이 압축 파일에 있는 경우 Kaspersky Endpoint Security는 *그래픽* 데이터 유형이 아니라 *압축 파일* 데이터 유형을 식별합니다.

- **개별 주소**. 웹 주소를 입력하거나 마스크를 사용할 수 있습니다.

여러 가지 방법을 동시에 사용하여 웹사이트에 대한 접근을 제어할 수 있습니다. 예를 들어 *웹 기반 이메일* 웹사이트 카테고리에 대해서만 *오피스 애플리케이션 파일* 데이터 유형에 대한 접근을 제한할 수 있습니다.

웹사이트 접속 규칙

웹 제어는 *접근 규칙*을 사용하여 웹사이트에 대한 사용자 접근을 관리합니다. 웹사이트 접근 규칙을 위한 다음과 같은 고급 설정을 구성할 수 있습니다:

- 규칙을 적용할 사용자

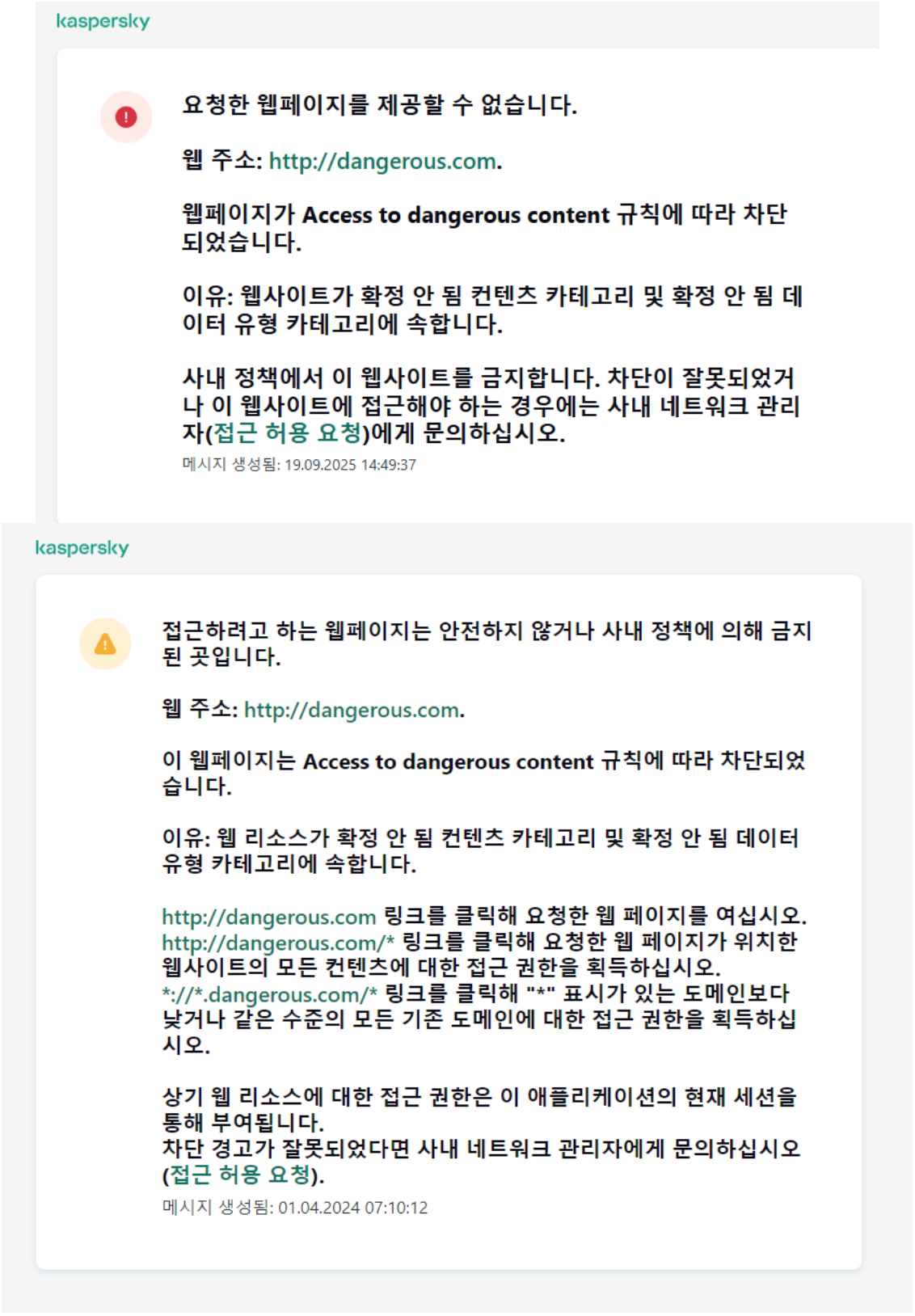
  예를 들어, IT 부서를 제외한 회사의 모든 사용자의 브라우저를 통한 인터넷 접근을 제한할 수 있습니다.

- 규칙 스케줄

  예를 들어, 업무 시간 동안에만 브라우저를 통한 인터넷 접근을 제한할 수 있습니다.

접근 규칙 우선 순위

각 규칙에는 우선 순위가 있습니다. 규칙 목록에서 순위가 높을수록 그 우선 순위도 높습니다. 웹사이트가 여러 규칙에 추가된 경우 웹 제어는 가장 높은 우선 순위를 가진 규칙에 따라 웹사이트에 대한 접근을 제어합니다. 예를 들어 Kaspersky Endpoint Security가 회사 포털을 소셜 네트워크로 식별할 수 있습니다. 소셜 네트워크에 대한 접근을 제한하고 회사 웹 포털에 대한 접근을 허용하려면 두 가지 규칙 즉, *소셜 네트워크* 웹사이트 카테고리에 대한 차단 규칙과 회사 웹 포털에 대한 허용 규칙을 하나씩 생성하면 됩니다. 회사 웹 포털에 대한 접근 규칙은 소셜 네트워크에 대한 접근 규칙보다 우선 순위가 높아야 합니다.



웹 제어 메시지

웹 제어 구성 요소 설정

파라미터	설명
웹 리소스 접근 규칙	웹 리소스 접근 규칙이 있는 목록. 각 규칙에는 우선 순위가 있습니다. 규칙 목록에서 순위가 높을수록 그 우선 순위도 높습니다. 웹사이트가 여러 규칙에 추가된 경우 웹 제어는 가장 높은 우선 순위를 가진 규칙에 따라 웹사이트에 대한 접근을 제어합니다.
기본 규칙	*기본 규칙*은 다른 규칙에서 다루지 않는 웹사이트에 접근하기 위한 규칙입니다. 다음과 같은 옵션을 사용할 수 있습니다. • **규칙 목록을 제외하고 모두 허용**합니다. 금지된 웹사이트에 대한 거부 목록 모드라고도 합니다. • **규칙 목록을 제외하고 모두 거부**합니다. 허용된 웹사이트에 대한 허용 목록 모드라고도 합니다.

파라미터	설명
규칙이 적용된 후 활성 사용자 브라우저 세션 종료	이 확인란을 선택하면 웹 제어는 정책이 적용된 즉시 차단된 웹 리소스에 대한 연결을 종료합니다. 브라우저는 웹페이지에서 데이터 다운로드를 즉시 중지합니다. 웹페이지를 새로 고침하거나 다른 금지된 웹페이지로 이동하면, 애플리케이션이 경고를 표시합니다. 웹 제어를 사용하면 웹 브라우저에서만 웹 리소스 연결을 즉시 해제할 수 있습니다. 다른 애플리케이션은 웹 제어가 새 연결만 제한합니다. 이 확인란을 선택하지 않으면, 웹 제어는 금지된 웹 리소스에 대한 새로운 연결만 제한합니다. 웹 제어는 활성화된 연결을 종료하지 않습니다.
템플릿	**경고**. 원하지 않는 웹 리소스에 대한 접근을 경고하는 규칙이 작동할 때 표시되는 메시지의 템플릿을 지정하는 입력 필드입니다. **차단 관련 메시지**. 웹 리소스 접근을 차단하는 규칙이 작동될 때 나타나는 메시지의 템플릿을 지정하는 입력 필드입니다. **관리자에게 메시지 보내기**. 사용자가 차단을 실수로 간주하는 경우 LAN 관리자에게 전송되는 메시지의 템플릿입니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 웹 페이지 접근 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다. 메시지 템플릿(예: `%USER_NAME%`)을 관리하기 위해 특수 변수가 제공됩니다. 변수를 사용하면 다른 컴퓨터에서 단일 메시지 템플릿을 사용할 수 있습니다.
허용된 페이지 열기 기록	Kaspersky Endpoint Security는 허용된 웹사이트를 포함한 모든 웹사이트에 대한 방문 데이터를 기록합니다. Kaspersky Endpoint Security는 Kaspersky Security Center, Kaspersky Endpoint Security의 로컬 로그 및 Windows 이벤트 로그에 이벤트를 보냅니다. 사용자 인터넷 활동을 모니터링하려면 이벤트 저장을 위한 설정을 구성해야 합니다. 이 모니터링 기능이 지원되는 브라우저는 Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox입니다. 그 외 브라우저에서는 사용자 활동 모니터링이 작동하지 않습니다. 사용자 인터넷 활동 모니터링은 HTTPS 트래픽을 복호화할 때 더 많은 컴퓨터 리소스가 필요할 수 있습니다.

장치 제어

장치 제어는 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 제어를 사용하면 애플리케이션이 연결된 장치에 대한 정보를 Kaspersky Security Center에 중계합니다. **고급** → **저장소** → **하드웨어** 폴더의 Kaspersky Security Center에서 연결된 장치 목록을 볼 수 있습니다.

장치 접근 레벨

장치 제어는 다음 레벨에서 접근을 제어합니다:

- **장치 유형**. 예: 프린터, 이동식 드라이브 및 CD/DVD 드라이브.
  다음과 같이 장치 접근 설정을 구성할 수 있습니다:
  - 허용 - ✓.
  - 차단 - ⊘.

- 규칙에 따라(프린터 및 휴대용 장치만) – .
- 연결 버스에 종속(Wi-Fi 제외) - .
- 예외를 제외하고 차단(Wi-Fi 전용) - .

- **연결 버스**. *연결 버스*는 장치를 컴퓨터에 연결하는 데 사용하는 인터페이스입니다(USB 또는 FireWire 등). 장치 유형에 **연결 버스에 종속** 모드가 선택되면 애플리케이션이 연결 인터페이스(예: USB)에 따라 장치에 대한 접근을 허용하거나 거부합니다.

  다음과 같이 장치 접근 설정을 구성할 수 있습니다:

  - 허용 - .
  - 차단 - .

- **신뢰하는 장치**. *신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.

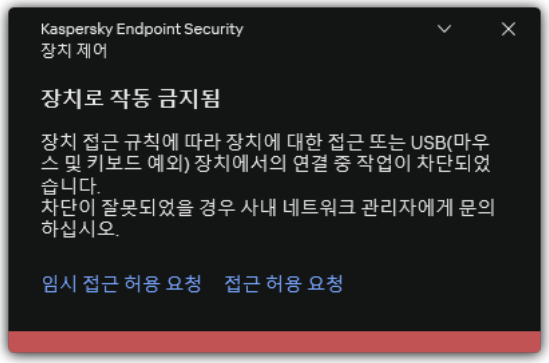
  다음 데이터를 기반으로 신뢰하는 장치를 추가할 수 있습니다:

  - **ID로 장치 추가**. 각 장치에는 고유 ID가 있습니다(하드웨어 ID 또는 HWID). 운영 체제 도구를 사용하여 장치 속성에서 ID를 볼 수 있습니다. 장치 ID의 예: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. 여러 특정 장치를 추가하려는 경우 ID별로 장치를 추가하는 것이 편리합니다.
  - **모델로 장치 추가**. 각 장치에는 공급업체 ID(VID) 및 제품 ID(PID)가 있습니다. 운영 체제 도구를 사용하여 장치 속성에서 ID를 볼 수 있습니다. VID 및 PID 입력을 위한 템플릿: `VID_1234&PID_5678`. 조직에서 특정 모델의 장치를 사용하는 경우 모델별로 장치를 추가하는 것이 편리합니다. 이런 식으로 이 모델의 모든 장치를 추가할 수 있습니다.
  - **ID 마스크로 장치 추가**. 비슷한 ID를 가진 여러 장치를 사용하는 경우 마스크를 사용하여 신뢰하는 목록에 장치를 추가할 수 있습니다. `*` 문자는 모든 문자의 조합을 나타냅니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `?` 문자를 지원하지 않습니다. 예: `WDC_C*`.
  - **모델 마스크로 장치 추가**. 비슷한 VID 또는 PID를 가진 여러 장치를 사용하는 경우(예: 동일한 제조업체의 장치), 마스크를 사용하여 신뢰하는 목록에 장치를 추가할 수 있습니다. `*` 문자는 모든 문자의 조합을 나타냅니다. Kaspersky Endpoint Security는 마스크를 입력할 때 `?` 문자를 지원하지 않습니다. 예: `VID_05AC&PID_*`.

장치 제어는 *접근 규칙*을 사용하여 장치에 대한 사용자 접근을 규제합니다. 장치 제어를 사용하면 장치 연결/연결 끊김 이벤트도 저장할 수 있습니다. 이벤트를 저장하려면 정책에서 이벤트 등록을 구성해야 합니다.

장치에 대한 접근이 연결 버스(상태)에 따른다면 Kaspersky Endpoint Security는 장치 연결/연결 끊김 이벤트를 저장하지 않습니다. Kaspersky Endpoint Security를 사용하여 장치 연결/연결 끊김 이벤트를 저장하려면 해당 장치에 대한 접근을 허용하거나(상태) 장치를 신뢰하는 목록에 추가합니다.

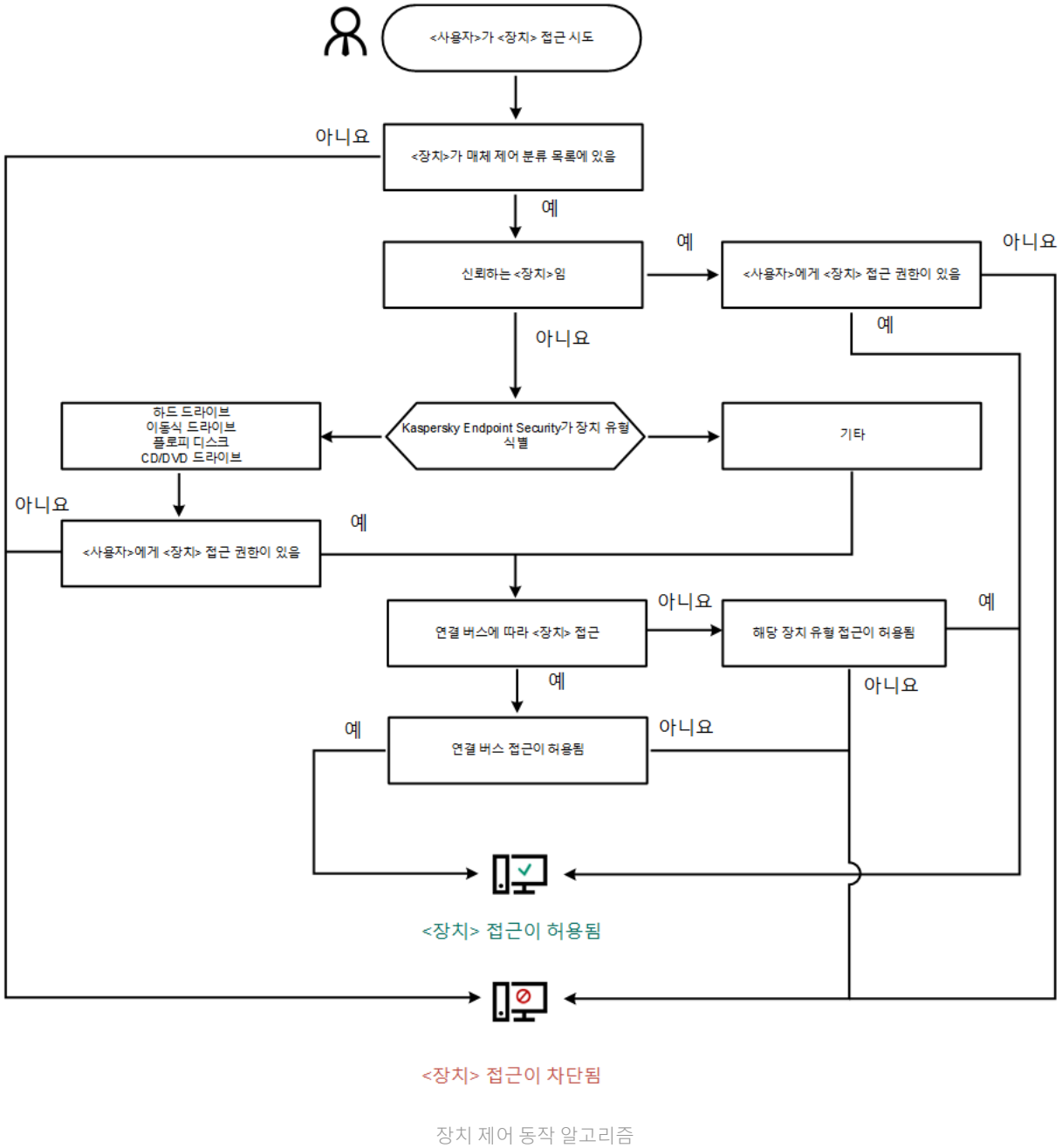
장치 제어로 차단된 장치가 컴퓨터에 연결되면 Kaspersky Endpoint Security가 접근을 차단하고 알림을 표시합니다(아래 그림 참조).



장치 제어 알림

장치 제어 동작 알고리즘

Kaspersky Endpoint Security는 사용자가 장치를 컴퓨터에 연결한 후 장치에 대한 접근을 허용할지 여부를 결정합니다(아래 그림 참조).



장치 제어 동작 알고리즘

장치가 연결되고 접근이 허용되는 경우에는 접근 규칙을 편집하고 접근을 차단할 수 있습니다. 이 경우 다음 번에 누군가가 이 장치에 접근을 시도하면(폴더 트리 보기, 읽기/쓰기 작업 수행 등) Kaspersky Endpoint Security에서 접근을 차단합니다. 파일 시스템이 없는 장치는 다음 번에 장치가 연결되는 경우에만 차단됩니다.

Kaspersky Endpoint Security가 설치된 컴퓨터의 사용자가 본인이 실수로 차단되었다고 생각하는 장치에 접근을 요청해야 하는 경우 사용자에게 접근 허용 요청 안내를 전송합니다.

파라미터	설명
임시 접근 요청 허용 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이 확인란을 선택하면 Kaspersky Endpoint Security 로컬 인터페이스 전반에서 **접근 허용 요청** 버튼을 사용할 수 있습니다. 이 버튼을 사용해 사용자가 차단된 장치에 대한 임시 접근 권한을 요청할 수 있습니다.
장치 및 Wi-Fi 네트워크	이 표에는 장치 제어 구성 요소의 분류에 따라 사용 가능한 모든 장치 유형과 해당 접근 상태가 포함되어 있습니다.
연결 버스	장치 제어 구성 요소의 분류에 따라 연결 버스 접근 상태를 포함해 사용 가능한 모든 연결 버스 목록. **연결 버스에 종속** 모드가 선택되면 Kaspersky Endpoint Security는 연결 버스 유형에 따라 장치에 대한 접근을 허용하거나 거부합니다.
신뢰하는 장치	신뢰하는 장치와 이러한 장치에 대한 접근이 허용된 사용자 목록입니다.
상속할 때 값 병합 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이렇게 하면 Kaspersky Security Center의 상위 및 하위 정책에 있는 신뢰하는 장치 목록이 병합됩니다. 목록을 병합하려면 Kaspersky Security Center의 자식 정책이 부모 정책 설정을 상속하도록 구성해야 합니다. 확인란을 선택하면 Kaspersky Security Center 부모 정책의 목록 항목이 자식 정책에 표시됩니다. 예를 들어, 전체 조직에 대해 신뢰하는 장치의 통합 목록을 만들 수 있습니다. 자식 정책에 상속된 목록 항목은 삭제하거나 편집할 수 없습니다. 상속 중에 병합된 신뢰하는 장치 목록의 항목은 상위 정책에서만 삭제 및 편집할 수 있습니다. 하위 수준 정책에서 목록 항목을 추가, 편집 또는 삭제할 수 있습니다. 자식 및 부모 정책 목록에서 일치하는 항목은 부모 정책과 같은 항목으로 표시됩니다. 이 확인란을 선택하지 않으면 Kaspersky Security Center 정책 설정을 상속할 때 목록 항목을 병합하지 않습니다. 이 기능을 사용하면 정책 프로필의 목록을 병합할 수도 있습니다. 목록을 병합하려면 우선순위가 가장 높은 프로필에서 우선순위가 낮은 프로필의 설정 상속을 활성화합니다. 정책 프로필 우선순위에 관한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.
안티 브리징	안티 브리징은 네트워크 브리지가 생성되는 것을 막아 컴퓨터에서 여러 개의 네트워크에 동시에 연결되지 않도록 합니다. 따라서 보호되지 않는 무단 네트워크를 통한 공격으로부터 회사 네트워크를 보호할 수 있습니다. 안티 브리징은 장치의 우선 순위에 따라 여러 개의 네트워크가 연결되는 것을 차단합니다. 규칙 목록에서 순위가 높은 장치일수록 그 우선 순위도 높습니다. 활성 연결과 새 연결 모두 같은 유형(예: Wi-Fi)인 경우 Kaspersky Endpoint Security는 활성 연결을 차단하고 새 연결을 허용합니다. 활성 연결과 새 연결의 유형이 서로 다른 경우(예: 네트워크 어댑터와 Wi-Fi)에는 Kaspersky Endpoint Security가 우선 순위가 낮은 연결을 차단하고 우선 순위가 높은 연결을 허용합니다. 안티 브리징은 세 가지 유형의 장치 즉, 네트워크 어댑터, Wi-Fi, 모뎀과의 작업을 지원합니다.
메시지 템플릿	**차단 관련 메시지**. 사용자가 차단된 장치에 접근하려고 할 때 표시되는 메시지의 템플릿입니다. 이 메시지는 사용자가 해당 사용자에 대해 차단된 장치 컨텐츠에 대한 작업을 수행하려고 할 때도 나타납니다. **관리자에게 메시지 보내기**. 사용자가 장치 접근이 잘못 차단되었거나 장치 컨텐츠 작업이 잘못 금지되었다고 생각하는 경우 LAN 관리자에게 보내는 메시지 템플릿입니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 장치 접근 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다.

애플리케이션 제어

애플리케이션 제어는 사용자 컴퓨터의 애플리케이션 시작을 관리합니다. 이를 통해 애플리케이션 사용에 대한 회사 보안 정책을 구현할 수 있습니다. 애플리케이션 제어는 애플리케이션에 대한 접근을 제한하여 컴퓨터 감염 위험을 줄입니다.

애플리케이션 제어의 구성은 다음 단계로 구성됩니다.

1. 애플리케이션 카테고리 만들기

   관리자는 관리하려는 애플리케이션 카테고리를 생성합니다. 애플리케이션 카테고리는 관리 그룹에 관계없이 회사 네트워크의 모든 컴퓨터를 대상으로 합니다. 카테고리를 작성하려면 KL 카테고리(예: *브라우저* 또는 다른 카테고리), 파일 해시, 애플리케이션 공급 업체 및 기타 기준과 같은 기준을 사용할 수 있습니다.

2. 애플리케이션 제어 규칙 생성

   관리자는 관리 그룹의 정책에 애플리케이션 제어 규칙을 만듭니다. 규칙에는 애플리케이션 카테고리와 이러한 카테고리에서 애플리케이션의 시작 상태(차단 또는 허용)가 포함됩니다. 관리자는 여러 규칙을 만들 수 있습니다. 하나의 애플리케이션이 여러 규칙의 기준과 일치할 수 있습니다. 차단 규칙이 허용 규칙보다 우선합니다. Kaspersky Endpoint Security는 애플리케이션을 시작할 때마다 규칙과 일치하는지 확인합니다. Kaspersky Endpoint Security는 모든 애플리케이션 제어 규칙에 애플리케이션을 순서대로 대조합니다.

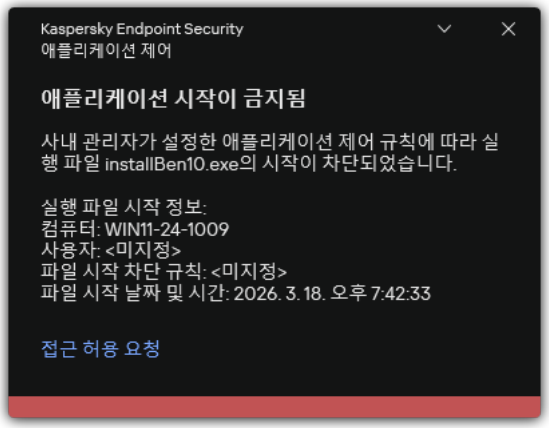
3. 애플리케이션 제어 모드 선택

   관리자는 애플리케이션 거부 목록이나 허용 목록 등 어느 규칙에도 포함되지 않은 애플리케이션의 작업 모드를 선택합니다.

사용자가 차단된 애플리케이션을 시작하려고 하면 Kaspersky Endpoint Security는 애플리케이션 시작을 차단하고 알림을 표시합니다(아래 그림 참조).

애플리케이션 제어 구성을 확인하기 위한 *테스트 모드*가 제공됩니다. 이 모드에서 Kaspersky Endpoint Security는 다음을 수행합니다.

- 애플리케이션(차단된 애플리케이션 포함) 시작을 허용합니다.
- 차단된 애플리케이션 시작에 대한 알림을 표시하고 사용자 컴퓨터의 리포트에 정보를 추가합니다.
- 차단된 애플리케이션 시작에 대한 데이터를 Kaspersky Security Center로 보냅니다.



애플리케이션 제어 알림

애플리케이션 제어 운영 모드

애플리케이션 제어 구성 요소에는 다음 두 가지 동작 모드가 있습니다:

- **거부 목록**. 이 애플리케이션 제어 모드에서는 사용자가 애플리케이션 제어 규칙에서 차단된 애플리케이션을 제외한 모든 애플리케이션을 시작할 수 있습니다.

  애플리케이션 제어의 기본 작동 모드입니다.

- **허용 목록**. 이 애플리케이션 제어 모드에서는 사용자가 애플리케이션 제어 규칙에서 허용되고 차단되지 않은 애플리케이션을 제외한 모든 애플리케이션을 시작할 수 없습니다.

  애플리케이션 제어의 허용 규칙이 구성 완료되면 애플리케이션 시작 제어 구성 요소가 LAN 관리자에 의해 확인되지 않는 모든 새로운 애플리케이션의 시작을 차단합니다. 단, 사용자의 업무에 필요한 운영 체제 및 신뢰할 수 있는 애플리케이션의 작동은 허용됩니다.

  허용 목록 모드에서 애플리케이션 제어 규칙 구성에 관한 권장 사항을 읽어 보십시오.

애플리케이션 제어 모드를 구성할 때 Kaspersky Endpoint Security 로컬 인터페이스 및 Kaspersky Security Center를 모두 사용할 수 있습니다.

그러나 Kaspersky Endpoint Security 로컬 인터페이스와 달리 Kaspersky Security Center에서는 다음과 같은 작업을 수행하는 데 필요한 도구를 제공합니다:

- 애플리케이션 카테고리 만들기

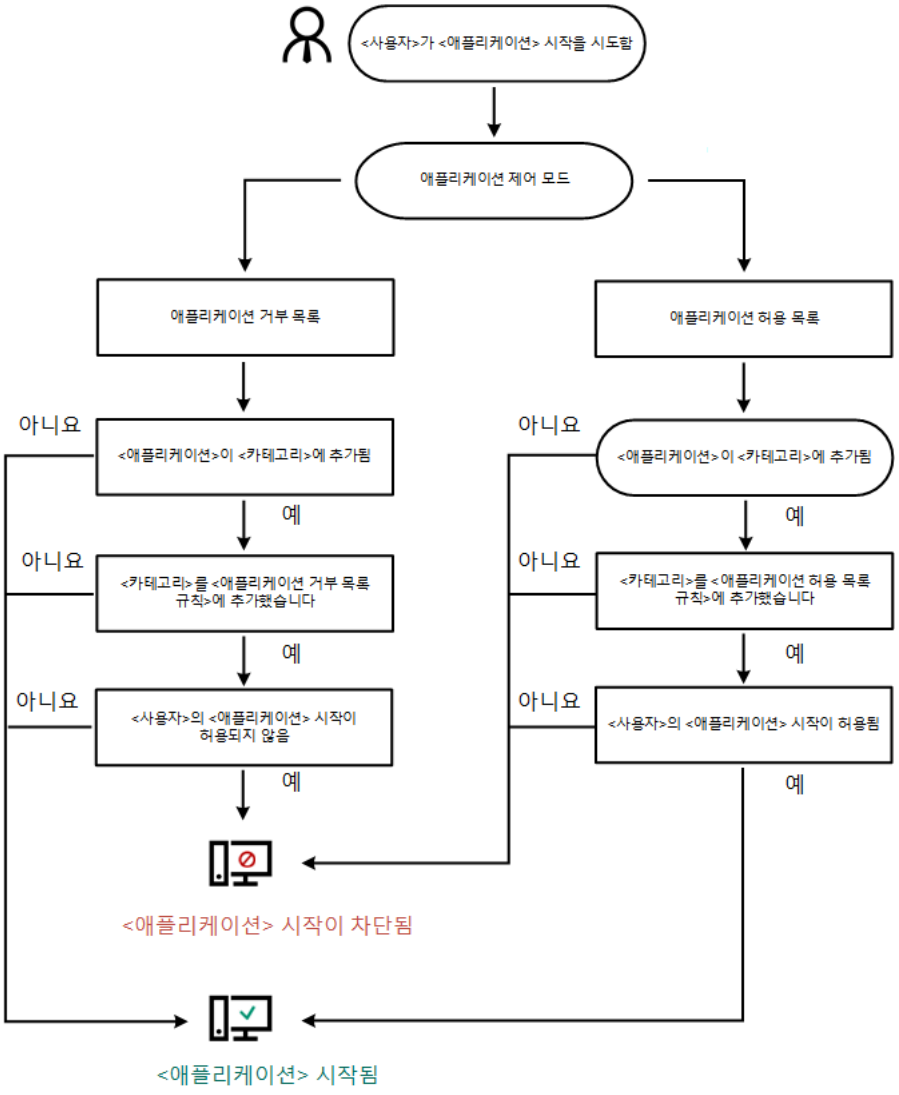
  Kaspersky Security Center 관리 콘솔에서 만든 애플리케이션 제어 규칙은 사용자 지정 애플리케이션 카테고리를 바탕으로 하며 Kaspersky Endpoint Security 로컬 인터페이스는 포함 및 예외 조건을 바탕으로 합니다.

- 기업 LAN 컴퓨터에 설치된 애플리케이션에 대한 정보 수신.

Kaspersky Security Center를 이용해 애플리케이션 제어 구성 요소의 작동을 구성하도록 권장되는 이유입니다.

애플리케이션 제어 동작 알고리즘

Kaspersky Endpoint Security는 알고리즘을 사용하여 애플리케이션 시작에 대한 결정을 내립니다(아래 그림 참조).



애플리케이션 제어 동작 알고리즘

파라미터	설명
규칙에 따라 차단되는 애플리케이션 시작 시 수행하는 조치	**규칙 적용** Kaspersky Endpoint Security는 선택한 모드에 따라 애플리케이션의 시작을 관리합니다. **규칙 테스트**. Kaspersky Endpoint Security가 현재 애플리케이션 제어 모드에서 차단된 애플리케이션 시작을 허용하지만 이 시작에 대한 정보를 리포트에 기록합니다.
애플리케이션 시작 제어 모드	다음 옵션 중 하나를 선택할 수 있습니다: • **거부 목록**. 이 옵션을 선택하면 애플리케이션 제어 차단 규칙의 조건을 충족하는 경우를 제외하고는 애플리케이션 제어에서 모든 사용자가 모든 애플리케이션을 시작하도록 허용합니다. • **허용 목록**. 이 옵션을 선택하면 애플리케이션 제어 허용 규칙의 조건을 충족하는 경우를 제외하고는 애플리케이션 제어에서 모든 사용자가 모든 애플리케이션을 시작할 수 없도록 차단합니다. **허용 목록** 모드를 선택하면 애플리케이션 제어 규칙 두 개가 자동 생성됩니다: • **골든 이미지** • **신뢰하는 업데이터** 자동 생성된 규칙의 설정을 편집하거나 삭제할 수 없습니다. 규칙을 작동하거나 중지할 수만 있습니다.
DLL 모듈 로드 모니터링	이 확인란이 선택되어 있으면 Kaspersky Endpoint Security에서 사용자가 애플리케이션을 시작하려고 시도할 때 DLL 모듈의 로딩을 제어합니다. DLL 모듈 및 이 DLL 모듈을 로드한 애플리케이션에 대한 정보는 리포트에 기록됩니다. DLL 모듈 및 드라이버 로딩에 대한 제어를 사용할 때는 애플리케이션 제어 설정에서 기본 **골든 이미지** 규칙 또는 '**골든 이미지\신뢰하는 인증서**' KL 카테고리가 포함된 다른 규칙 중 하나를 사용하고 있는지 확인하고, Kaspersky Endpoint Security를 시작하기 전에 신뢰하는 DLL 모듈과 드라이버가 먼저 로드되도록 하십시오. **골든 이미지** 규칙을 사용하지 않을 때 DLL 모듈 및 드라이버의 로드를 제어하면 운영 체제가 불안정해질 수 있습니다. Kaspersky Endpoint Security는 확인란이 선택된 이후에 로드된 DLL 모듈과 드라이버만 감시합니다. 확인란을 선택한 후 컴퓨터를 다시 시작하여 애플리케이션이 Kaspersky Endpoint Security가 시작되기 전에 로드된 DLL을 포함하여 모든 DLL 모듈 및 드라이버를 감시하는지 확인할 것을 권장합니다.
엄격한 디지털 서명 인증 사용	애플리케이션 제어 규칙에 대한 트리거 조건으로 인증서를 선택할 수 있습니다. 이 확인란을 선택하면 Kaspersky Endpoint Security는 신뢰하는 시스템 인증서 저장소의 인증서로만 서명된 애플리케이션에 규칙을 적용합니다. 이러한 인증서로 서명된 애플리케이션은 *악성 코드 검사* 작업과 같은 보호 구성 요소에서도 신뢰할 수 있는 것으로 간주됩니다. 그러나 애플리케이션 제어 규칙에서 다른 저장소의 인증서를 지정하는 경우 Kaspersky Endpoint Security는 해당 규칙을 적용하지 않습니다. 이 확인란이 선택되어 있지 않으면 Kaspersky Endpoint Security는 Windows Trusted Root Certificate 저장소의 인증서로만 서명된 애플리케이션에 규칙을 적용합니다. 이러한 애플리케이션은 신뢰 구역에 포함되지 않습니다. 보호 구성 요소는 이러한 애플리케이션의 활동을 모니터링합니다.
애플리케이션 차단에 관한 메시지 템플릿	**차단 관련 메시지**. 애플리케이션 시작을 차단하는 애플리케이션 제어 규칙이 작동될 때 표시되는 메시지의 템플릿. **관리자에게 메시지 보내기**. 사용자가 애플리케이션이 실수로 차단되었다고 생각하는 경우 회사 LAN 관리자에게 보낼 수 있는 메시지 템플릿입니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 애플리케이션 시작 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다.

적응형 이상 행위 제어

이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

적응형 이상 행위 제어 구성 요소는 회사 네트워크의 컴퓨터에서 일반적이지 않은 활동을 감시하고 차단합니다. 적응형 이상 행위 제어는 일련의 규칙을 사용하여 비정상적인 동작을 추적합니다(예, *오피스 애플리케이션에서 Microsoft PowerShell 시작* 규칙). 규칙은 Kaspersky 전문가가 일반적인 악의적인 활동 시나리오를 기반으로 작성합니다. 적응형 이상 행위 제어에서 각 규칙을 처리하는 방법을 구성할 수 있습니다. 또한 예를 들어 특정 워크플로 작업을 자동화하는 PowerShell 스크립트를 실행을 허용할 수 있습니다. Kaspersky Endpoint Security는 규칙 세트와 애플리케이션 데이터베이스를 업데이트합니다. 규칙 세트에 대한 업데이트를 직접 확인해야 합니다.

적응형 이상 행위 제어 설정

적응형 이상 행위 제어의 구성은 다음 단계로 구성됩니다:

1. 적응형 이상 행위 제어 학습.

   적응형 이상 행위 제어를 활성화하면 해당 규칙은 *학습 모드*로 작동합니다. 학습하는 동안 적응형 이상 행위 제어는 규칙 트리거링을 모니터링하고 트리거링 이벤트를 Kaspersky Security Center로 전송합니다. 각 규칙은 개별적으로 학습 모드 지속 시간을 갖습니다. 학습 모드 지속 시간은 Kaspersky 전문가가 설정합니다. 일반적으로 학습 모드는 2주 동안 진행됩니다.

   학습 중에 규칙이 전혀 트리거되지 않은 경우 적응형 이상 행위 제어는 이후 이 규칙과 관련된 작업을 일반적이지 않은 것으로 간주합니다. Kaspersky Endpoint Security는 해당 규칙과 관련된 모든 작업을 차단합니다.

   학습 중에 규칙이 트리거되면 Kaspersky Endpoint Security는 규칙 트리거링 리포트 및 **스마트 학습 상태에서 트리거된 규칙** 저장소에 이벤트를 기록합니다.

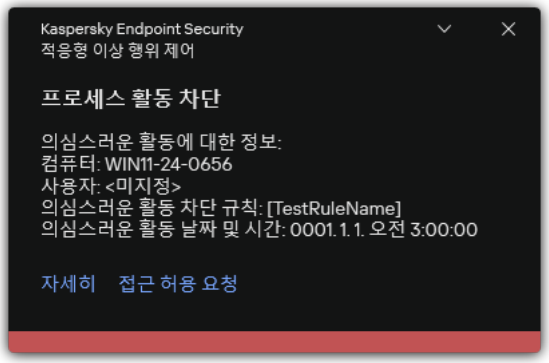
2. 규칙 트리거링 리포트 분석.

   관리자는 규칙 트리거링 리포트 또는 **스마트 학습 상태에서 트리거된 규칙** 저장소의 내용을 분석합니다. 그런 다음 관리자는 규칙이 트리거될 때 적응형 이상 행위 제어의 동작을 선택할 수 있습니다: 차단 또는 허용. 또한 관리자는 규칙의 작동 방식을 계속 모니터링하고 학습 모드의 기간을 연장할 수 있습니다. 관리자가 아무런 조치를 취하지 않으면 애플리케이션도 학습 모드에서 계속 작동합니다. 학습 모드 기간이 재시작되었습니다.

적응형 이상 행위 제어는 다음 채널을 통해 실시간으로 구성됩니다.

- 적응형 이상 행위 제어는 학습 모드에서 트리거되지 않은 규칙과 관련된 작업을 자동으로 차단하기 시작합니다.
- Kaspersky Endpoint Security는 새 규칙을 추가하거나 오래된 규칙을 제거합니다.
- 관리자는 규칙 트리거링 리포트와 **스마트 학습 상태에서 트리거된 규칙** 저장소의 내용을 검토한 후 적응형 이상 행위 제어의 작업을 구성합니다. 트리거하는 규칙과 **스마트 학습 상태에서 트리거된 규칙** 저장소의 내용에 대한 리포트를 확인하는 것이 좋습니다.

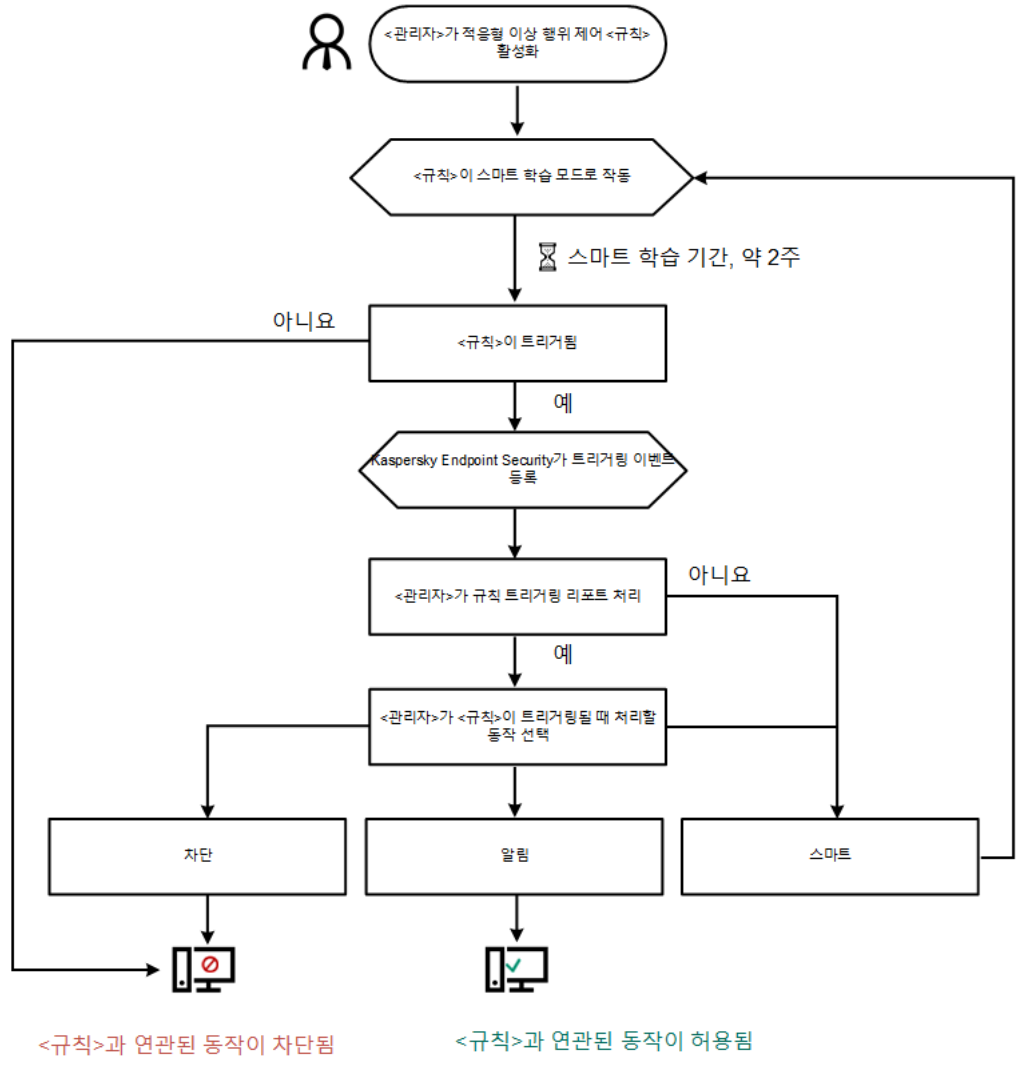
악성 애플리케이션이 동작을 수행하려고 하면 Kaspersky Endpoint Security가 해당 동작을 차단하고 알림을 표시합니다(아래 그림 참조).



적응형 이상 행위 제어 알림

적응형 이상 행위 제어 운영 알고리즘

Kaspersky Endpoint Security는 다음 알고리즘을 기반으로 한 규칙과 연관된 동작을 허용할지 또는 차단할지 결정합니다(아래 그림 참조).



적응형 이상 행위 제어 운영 알고리즘

파라미터	설명
적응형 이상 행위 제어 규칙 상태 리포트 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이 리포트에는 적응형 이상 행위 제어 탐지 규칙의 상태(예, *사용 안 함* 또는 *차단*)에 대한 정보가 포함되어 있습니다. 이 리포트는 모든 관리 그룹을 대상으로 생성됩니다.
트리거된 적응형 이상 행위 제어 규칙 리포트 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이 리포트에는 적응형 이상 행위 제어를 사용하여 탐지한 일반적이지 않은 동작에 대한 정보가 들어 있습니다. 이 리포트는 모든 관리 그룹을 대상으로 생성됩니다.
규칙	적응형 이상 행위 제어 규칙 표. 규칙은 Kaspersky 전문가가 일반적인 악의적인 활동 시나리오를 기반으로 작성합니다.
템플릿	**차단 관련 메시지**. 일반적이지 않은 동작을 차단하는 적응형 이상 행위 제어 규칙이 트리거될 때 사용자에게 표시되는 메시지 템플릿입니다. **관리자에게 메시지 보내기**. 사용자가 차단이 잘못된 것으로 판단한 경우 로컬 네트워크 관리자에게 사용자가 보낼 수 있는 메시지 템플릿입니다. 사용자가 액세스 제공을 요청하면 Kaspersky Endpoint Security는 Kaspersky Security Center에 **관리자에게 애플리케이션 활동 차단 메시지 보내기** 이벤트를 보냅니다. 이벤트 설명에는 대체 변수와 함께 관리자에게 보내는 메시지가 포함됩니다. 사전 정의된 이벤트 조회 **사용자 개선 요청 사항**을 사용하여 Kaspersky Security Center 콘솔에서 이러한 이벤트를 볼 수 있습니다. 조직에 Kaspersky Security Center가 배포되어 있지 않거나 중앙 관리 서버에 연결되어 있지 않은 경우 애플리케이션은 지정된 이메일 주소로 관리자에게 메시지를 보냅니다.

시스템 무결성 모니터링

이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

12.6 버전부터 Kaspersky Endpoint Security for Windows에는 파일 무결성 모니터 구성 요소 대신 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 Endpoint Security는 해당 이벤트를 생성하고 관리자에게 알립니다. 시스템 무결성 모니터링은 실시간 모드에서 작동할 수 있으며 필요에 따라 시스템 무결성 검사를 수행할 수도 있습니다.

실시간 시스템 무결성 모니터링

실시간 모드에서 시스템 무결성 모니터링을 구성 요소의 범위(*모니터링 범위*)에 포함된 개체의 변경 사항을 추적합니다. 또한 시스템 무결성 모니터링을 사용하면 해당 개체에 대한 무단 접근을 실시간으로 차단할 수 있습니다.

온디맨드 시스템 무결성 검사

온디맨드 시스템 무결성 검사는 수동으로 또는 스케줄에 따라 실행할 수 있는 작업입니다. *시스템 무결성 검사* 작업을 실행하려면 구성 요소의 범위(*모니터링 범위*)를 설정하고 베이스라인을 생성합니다. *베이스라인*은 시스템 내 객체의 기록된 상태로 애플리케이션이 현재 상태와 비교할 때 이를 참조합니다.

시스템 무결성 모니터링 설정

파라미터	설명
차단 규칙 운영 모드	• **차단**. 이 모드에서는 시스템 무결성 모니터링이 모니터링 범위에 있는 파일 및 레지스트리 키를 사용하는 작업을 차단하고 해당 이벤트를 생성합니다. • **알림**. 이 모드에서는 시스템 무결성 모니터링이 모니터링 범위에 있는 파일 및 레지스트리 키에 대한 작업을 허용하고 해당 이벤트를 생성합니다.
실시간 시스템 무결성 모니터링	실시간 모드에서 시스템 무결성 모니터링을 구성 요소의 범위(*모니터링 범위*)에 포함된 개체의 변경 사항을 추적합니다. 또한 시스템 무결성 모니터링을 사용하면 해당 개체에 대한 무단 접근을 실시간으로 차단할 수 있습니다.
장치 모니터	시스템 무결성 모니터링은 외부 장치의 연결 및 연결 해제를 모니터링합니다.
파일 및 레지스트리 모니터	시스템 무결성 모니터링은 파일, 폴더 및 레지스트리의 변경 사항을 모니터링합니다.
시스템 무결성 검사	온디맨드 시스템 무결성 검사는 수동으로 또는 스케줄에 따라 실행할 수 있는 작업입니다. *시스템 무결성 검사* 작업을 실행하려면 구성 요소의 범위(*모니터링 범위*)를 설정하고 베이스라인을 생성합니다. *베이스라인*은 시스템 내 객체의 기록된 상태로 애플리케이션이 현재 상태와 비교할 때 이를 참조합니다.

Endpoint Sensor

Endpoint Sensor는 Kaspersky Endpoint Security 11.4.0에 포함되어 있지 않습니다.

Kaspersky Security Center 웹 콘솔 및 Kaspersky Security Center 관리 콘솔에서 Endpoint Sensor를 관리할 수 있습니다. Kaspersky Security Center Cloud 콘솔에서는 Endpoint Sensor를 관리할 수 없습니다.

*Endpoint Sensor*는 Kaspersky Anti Targeted Attack Platform과 상호 작용하도록 설계되었습니다. *Kaspersky Anti Targeted Attack Platform*은 표적형 공격, APT(지능형 지속 위협), 제로 데이 공격 등 지능형 위협을 적시에 탐지하도록 설계된 솔루션입니다. Kaspersky Anti Targeted Attack Platform에는 다음 세 가지 기능 단위가 포함됩니다.

- Kaspersky Anti Targeted Attack Platform(*KATA*)
- Kaspersky Endpoint Detection and Response(*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

모든 기능 단위를 구매하거나 개별 기능 단위를 따로 구매할 수 있습니다. 이 솔루션에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

Endpoint Sensor 관리에는 다음과 같은 제한 사항이 있습니다.

- Kaspersky Endpoint Security 버전 11.0.0~11.3.0이 컴퓨터에 설치되어 있는 경우 정책에서 Endpoint Sensor 설정을 구성할 수 있습니다. 정책을 사용하여 Endpoint Sensor 설정을 구성하는 방법에 대한 자세한 내용은 이전 버전의 Kaspersky Endpoint Security 도움말 문서를 참조하십시오.
- Kaspersky Endpoint Security 버전 11.4.0 이상이 컴퓨터에 설치되어 있는 경우 정책에서 Endpoint Sensor 설정을 구성할 수 없습니다.

Endpoint Sensor는 클라이언트 컴퓨터에 설치됩니다. 이러한 컴퓨터에서 이 구성 요소는 프로세스, 활성 네트워크 연결 및 수정된 파일을 지속적으로 모니터링합니다. Endpoint Sensor는 정보를 KATA 서버에 전달합니다.

구성 요소 기능은 다음 운영 체제 하에서 이용 가능합니다:

- Windows 7 Service Pack 1 Home / Professional / Enterprise
- Windows 8.1.1 Professional / Enterprise
- Windows 10 RS3 Home / Professional / Education / Enterprise
- Windows 10 RS4 Home / Professional / Education / Enterprise
- Windows 10 RS5 Home / Professional / Education / Enterprise
- Windows 10 RS6 Home / Professional / Education / Enterprise
- Windows Server 2008 R2 Foundation / Standard / Enterprise(64비트)
- Windows Server 2012 Foundation / Standard / Enterprise(64비트)
- Windows Server 2012 R2 Foundation / Standard / Enterprise(64비트)
- Windows Server 2016 Essentials / Standard(64비트)

KATA 운영에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

Sandbox

Kaspersky Endpoint Security for Windows에는 Kaspersky Sandbox 솔루션 통합을 위한 내장 에이전트가 포함됩니다. *Sandbox* 구성 요소는 컴퓨터에서 지능형 보안위협을 탐지하고 자동 차단합니다. Sandbox는 조직의 IT 인프라에 대한 표적 공격의 활동 특성 및 악성 활동 탐지를 위해 개체 행동을 분석합니다. Sandbox는 Microsoft Windows 운영 체제(Sandbox 서버)의 가상 이미지가 배포된 특수 서버의 개체를 분석하고 검사합니다. 이 솔루션에 대한 자세한 내용은 Kaspersky Sandbox 도움말 및 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

12.7 버전부터 Kaspersky Endpoint Security for Windows는 Kaspersky Anti Targeted Attack Platform 솔루션의 일부인 Sandbox 구성 요소를 지원합니다. Kaspersky Sandbox 솔루션과 달리 KATA Sandbox 구성 요소는 파일을 자동으로 검사할 수 있을 뿐 아니라, 파일 마우스 오른쪽 메뉴를 통해 수동으로 검사할 수도 있습니다.

KATA Sandbox를 사용하려면 Kaspersky Anti Targeted Attack Platform 7.0 이상이 설치되어 있어야 합니다.

구성 요소는 Kaspersky Security Center 웹 콘솔을 통해서만 관리할 수 있습니다. 관리 콘솔(MMC)로는 이 구성 요소를 관리할 수 없습니다.

Sandbox 구성 요소 설정

파라미터	설명
통합 유형	**Kaspersky Sandbox**. Kaspersky Sandbox 솔루션과 통합. 애플리케이션은 Kaspersky Sandbox에서 검사할 파일을 자동 모드에서만 전송합니다. **KATA Sandbox**. Kaspersky Anti Targeted Attack Platform 솔루션의 Sandbox 구성 요소와 통합. 검사를 위한 파일 제출 모드를 선택할 수 있습니다. • **수동**. 사용자가 마우스 오른쪽 메뉴에서 검사할 파일을 수동으로 제출합니다(**Sandbox로 전송**). • **자동**. 애플리케이션이 자동으로 개체를 탐지하여 검사를 위해 Sandbox에 제출합니다. • **조합**.
서버 연결 설정	**시간 초과(msec)**. Sandbox 서버(Kaspersky Sandbox용) 또는 Central Node 서버(KATA용)의 연결 시간 초과입니다. 구성된 시간 초과를 넘으면 Kaspersky Endpoint Security가 다음 서버로 요청을 보냅니다. 연결 속도가 느리거나 연결이 불안정하다면 서버의 연결 시간 초과 설정을 늘릴 수 있습니다. 요청 시간 초과 설정은 0.5초 이하를 권장합니다. **요청 대기열**. 요청 대기열 폴더의 크기입니다. Sandbox에서 검사하기 위해 여러 개체를 전송하는 경우 Kaspersky Endpoint Security는 요청 대기열을 생성합니다. 기본적으로 요청 대기열 폴더의 크기는 100MB로 제한됩니다. 최대 크기에 도달하면 Sandbox는 대기열에 새 요청 추가를 중지하고 해당 이벤트를 Kaspersky Security Center로 보냅니다. 서버 구성에 따라 요청 대기열 폴더의 크기를 구성할 수 있습니다. **서버 TLS 인증서**. Sandbox 서버(Kaspersky Sandbox용) 또는 Central Node 서버(KATA용)와의 신뢰할 수 있는 연결을 구성하려면 TLS 인증서를 준비해야 합니다. 그런 다음 정책을 사용하여 컴퓨터에 인증서를 추가해야 합니다. Sandbox 서버(Kaspersky Sandbox용) 또는 Central Node 서버(KATA용)에 인증서를 추가해야 합니다. **양방향 인증 사용**(KATA Sandbox 전용). Kaspersky Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 Endpoint Security 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.
Sandbox 서버에 연결	**Kaspersky Sandbox**. Sandbox 서버 연결 설정입니다. 서버는 Microsoft Windows 운영 체제의 배포된 가상 이미지를 사용하여 검사할 개체를 실행합니다. IP 주소(IPv4 또는 IPv6)나 정규화된 도메인 이름을 입력할 수 있습니다. **KATA Sandbox**. Central Node 서버 연결 설정. Central Node는 Sandbox 서버 간의 검사 및 부하 분산을 위한 최적의 설정을 선택합니다.
위협 탐지 시 처리 방법	**격리 저장소로 사본을 옮기고 개체 삭제**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 컴퓨터에서 발견된 악성 개체를 삭제합니다. 개체를 삭제하기 전에 Kaspersky Endpoint Security는 나중에 개체를 복원해야 할 때를 대비하여 백업 복사본을 생성합니다. Kaspersky Endpoint Security는 백업 복사본을 격리 저장소로 이동합니다. **중요 영역 검사 실행**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 *중요 영역 검사* 작업을 실행합니다. Kaspersky Endpoint Security는 기본적으로 커널 메모리, 실행 중인 프로세스 및 디스크 부트 섹터를 검사합니다. **IOC 검사 작업 생성**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 자동으로 *IOC 검사(자율적 IOC 검사 작업)*를 생성합니다. 이 작업에 대해 실행 모드, 검사 범위 및 IOC 탐지에 대한 작업(개체 삭제, *중요 영역 검사* 작업 실행)을 구성할 수 있습니다. *IOC 검사* 작업에 대한 다른 설정을 수정하려면 작업 설정으로 이동합니다.
IOC 검사 범위	**중요한 파일 영역**. 이 옵션을 선택하면 Kaspersky Endpoint Security는 컴퓨터의 중요한 파일 영역(커널 메모리 및 부트 섹터)에서만 IOC 검사를 수행합니다. **컴퓨터 시스템 드라이브의 파일 영역**. 이 옵션을 선택하면 Kaspersky Endpoint Security가 컴퓨터의 시스템 드라이브에서 IOC 검사를 수행합니다.
IOC 검사 작업 실행	**수동**. 편리한 시간에 *IOC 검사* 작업을 수동으로 시작할 수 있는 실행 모드입니다. **자동**. 보안위협이 탐지되면 Kaspersky Endpoint Security가 자동으로 *IOC 검사* 작업을 실행하는 실행 모드입니다. **컴퓨터가 유휴 상태일 때만 실행**. 화면 보호기가 활성화되었거나 화면이 잠겨 있을 때 Kaspersky Endpoint Security가 *IOC 검사* 작업을 실행하는 실행 모드입니다. 사용자가 컴퓨터의 잠금을 해제하면 Kaspersky Endpoint Security가 작업을 일시 중지합니다. 따라서 작업을 완료하는 데 며칠이 걸릴 수 있습니다.

Managed Detection and Response

Kaspersky Endpoint Security for Windows는 Managed Detection and Response 솔루션과의 통합을 지원합니다. *Kaspersky Managed Detection and Response(MDR)* 솔루션은 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. 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.

Managed Detection and Response 설정

파라미터	설명
MDR 구성 파일	BLOB 파일에는 클라이언트 ID와 Kaspersky Managed Detection and Response 라이센스에 대한 정보가 포함되어 있습니다. BLOB 파일은 MDR 구성 파일의 ZIP 압축파일 안에 있습니다. Kaspersky Managed Detection and Response 콘솔에서 ZIP 압축파일을 얻을 수 있습니다. BLOB 파일에 대한 자세한 내용은 Kaspersky Managed Detection and Response 도움말을 참조하십시오.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows에는 이제 Kaspersky Endpoint Detection and Response Optimum 솔루션(이하 'EDR Optimum'이라고도 함)용 내장 에이전트가 포함됩니다. 11.8.0 버전부터 Kaspersky Endpoint Security for Windows에 Kaspersky Endpoint Detection and Response Expert 솔루션(이하 "EDR Expert"이라고도 함)용 내장 에이전트가 포함됩니다. *Kaspersky Endpoint Detection and Response*는 지능형 사이버 위협으로부터 조직의 IT 인프라를 보호하기 위한 폭넓은 솔루션입니다. 이 솔루션의 기능은 위협 자동 탐지와 이에 대한 대응 능력을 결합하여 새로운 익스플로잇, 랜섬웨어, 파일리스 공격 및 합법적인 시스템 도구를 사용하는 방법 등 다양한 지능형 공격에 대처합니다. EDR Expert는 EDR Optimum보다 더 많은 보안위협 모니터링 및 대응 기능을 제공합니다. 솔루션에 관한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말과 Kaspersky Endpoint Detection and Response Expert 도움말을 참조하십시오.

Kaspersky Endpoint Detection and Response는 보안 위협 개발을 검토 및 분석하고 즉각적인 대응이 필요한 잠재적 공격에 대한 정보를 *보안 인력*이나 *관리자*에게 제공합니다. Kaspersky Endpoint Detection and Response의 경고 세부 정보는 별도의 창으로 표시됩니다. *경고*는 애플리케이션이 비정상적이거나 의심스러운 것으로 식별하여 회사 IT 인프라에 보안 위협이 될 수 있는 회사 IT 인프라 이벤트를 말합니다. *경고 세부 정보*는 탐지된 위협에서 수집한 전체 정보를 확인하는 도구입니다. 경고 세부 정보에는 컴퓨터에서의 파일 히스토리 등이 포함됩니다. 경고 세부 정보 관리에 대한 자세한 사항은 Kaspersky Endpoint Detection and Response Optimum 도움말과 Kaspersky Endpoint Detection and Response Expert 도움말을 참조하십시오.

웹 콘솔과 Cloud Console에서 EDR Optimum 구성 요소를 구성할 수 있습니다. Cloud Console에서만 EDR Expert 구성 요소 설정을 이용할 수 있습니다.

Endpoint Detection and Response 설정

파라미터	설명
고급 시스템 활동 로그 활성화	확장 원격 측정은 IOC 탐지의 정확도를 개선하지만 컴퓨터 리소스를 더 많이 사용합니다. 회고적 IOC 검사를 위해 컴퓨터에서 확장 원격 측정을 활성화하는 것이 좋습니다. *회고적 IOC 검사*는 Kaspersky Endpoint Security가 특정 기간의 데이터를 사용하여 침해 지표를 검사하는 *IOC 검사* 작업의 모드 중 하나입니다. 이 모드는 네트워크 활동, 프로세스, 파일, 기타 원격 측정 등 보호된 컴퓨터의 원격 측정을 통해 침해지표를 검색하는 데 사용됩니다. 확장 원격 측정이 비활성화되면 Kaspersky Endpoint Security는 탐지된 침해 지표에 대한 정보를 교체할 수 있습니다.
네트워크 격리	탐지된 보안위협에 대응하여 네트워크에서 컴퓨터를 자동으로 격리합니다. 네트워크 격리가 켜지면 애플리케이션은 활성화된 모든 연결을 끊고 컴퓨터의 새로운 TCP/IP 연결을 모두 차단합니다. 애플리케이션은 다음 연결만 활성 상태로 둡니다: • 네트워크 격리 예외에 포함된 연결. • Kaspersky Endpoint Security 서비스가 시작한 연결. • Kaspersky Security Center 네트워크 에이전트가 시작한 연결.
격리된 장치 자동 잠금 해제 기준(시간)	네트워크 격리는 지정된 시간이 지나면 자동 또는 수동으로 끌 수 있습니다. 기본적으로 Kaspersky Endpoint Security는 격리 시작 5시간 후에 네트워크 격리를 끕니다.

파라미터	설명
네트워크 격리 예외	네트워크 격리의 예외 규칙 목록입니다. 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 프로필의 설정을 수정하거나 수동으로 예외를 정의할 수도 있습니다. 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.
실행 방지	실행 파일 및 스크립트의 실행과 오피스 형식 파일 열기를 제어합니다. 예를 들어, 선택한 컴퓨터에서 안전하지 않다고 판단되는 애플리케이션의 실행을 방지할 수 있습니다. 실행 방지는 오피스 파일 확장자 세트와 스크립트 인터프리터 세트를 지원합니다. 실행 방지 구성 요소를 사용하려면 실행 방지 규칙을 추가해야 합니다. *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.
금지된 개체 실행 또는 열기 시 동작	**차단하고 이벤트 로그에 추가**. 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. **이벤트 로그에 추가**. 이 모드에서는 Kaspersky Endpoint Security가 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. 이 모드가 기본적으로 선택되어 있습니다.
실행 방지 규칙	*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.
Cloud Sandbox	*Cloud Sandbox*는 컴퓨터에서 지능형 보안 위협을 탐지할 수 있는 기술입니다. Kaspersky Endpoint Security는 분석을 위해 탐지된 파일을 Cloud Sandbox에 자동 전달합니다. Cloud Sandbox는 이러한 파일을 격리된 환경에서 실행하여 악성 활동을 식별하고 평판을 결정합니다. 그다음 이 파일의 데이터가 Kaspersky Security Network로 전송됩니다. 따라서 Cloud Sandbox가 악성 파일을 탐지하면 Kaspersky Endpoint Security는 이 파일이 탐지된 모든 컴퓨터에서 이 위협 요소를 제거하기 위해 적절한 조치를 수행합니다. Cloud Sandbox 기술은 영구적으로 활성화되며 사용 중인 라이센스 유형과 관계없이 모든 Kaspersky Security Network 사용자가 사용할 수 있습니다. 이 확인란을 선택하면 Kaspersky Endpoint Security는 **위협 탐지 기술**의 기본 애플리케이션 창에서 Cloud Sandbox를 사용하여 탐지된 보안위협에 대한 카운터를 활성화합니다. Kaspersky Endpoint Security는 Kaspersky Security Center 콘솔의 애플리케이션 이벤트와 *위협 처리 리포트*에서 Cloud Sandbox 보안위협 탐지 기술을 표시합니다.

Endpoint Detection and Response Expert(on-premise)

Endpoint Detection and Response Expert(on-premise)

Kaspersky Endpoint Security for Windows는 Kaspersky Endpoint Detection and Response Expert(on-premise) 솔루션과의 통합을 지원합니다. *Kaspersky Endpoint Detection and Response Expert(on-premise)*는 기업 사이버 보안 솔루션으로, Kaspersky 애플리케이션을 통해 조직에서 대부분의 사이버 위험에 대응하고 가장 중요한 위협 전파 시나리오를 처리하도록 지원합니다. EDR Expert(on-premise) 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-premise)는 기업 인프라에서 수신한 로그 및 원격 측정을 확인하여 공격을 자동으로 탐지하며, Kaspersky 애플리케이션 타사 정보 보안 제품의 이벤트를 포함하여 EDR Expert(on-premise)에 수집된 모든 이벤트를 결합한 조사 그래프를 통해 사고를 조사하도록 지원합니다.

고급 인시던트에 대응하기 위해 EDR Expert(on-premise)는 사전 설정 및 사용자 정의 시나리오를 사용합니다. 또한 타사 애플리케이션 및 여러 애플리케이션이 관련된 대응 시나리오의 대응 작업을 사용할 수 있습니다.

Endpoint Detection and Response(KATA)

Kaspersky Endpoint Security for Windows에는 Kaspersky Anti Targeted Attack Platform(EDR (KATA)) 솔루션의 일부인 Kaspersky Endpoint Detection and Response 구성 요소를 지원합니다. *Kaspersky Anti Targeted Attack Platform*은 표적형 공격, APT(지능형 지속 위협), 제로 데이 공격 등 지능형 위협을 적시에 탐지하도록 설계된 솔루션입니다. Kaspersky Anti Targeted Attack Platform에는 다음 세 가지 기능 단위가 포함됩니다.

- Kaspersky Anti Targeted Attack Platform(*KATA*)
- Kaspersky Endpoint Detection and Response(*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

모든 기능 단위를 구매하거나 개별 기능 단위를 따로 구매할 수 있습니다. 이 솔루션에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

Kaspersky Endpoint Security는 기업 IT 인프라의 개별 컴퓨터에 설치되며 프로세스, 개방형 네트워크 연결 및 수정되는 파일을 계속해서 모니터링합니다. 컴퓨터의 이벤트에 대한 정보(원격 측정 데이터)는 Kaspersky Anti Targeted Attack Platform 서버로 전송됩니다. 이때, Kaspersky Endpoint Security는 애플리케이션에서 발견한 보안 위협에 대한 정보와 이를 처리한 결과에 대한 정보도 Kaspersky Anti Targeted Attack Platform 서버로 보냅니다.

EDR(KATA) 및 NDR(KATA) 통합은 Kaspersky Security Center 콘솔에서 구성됩니다. 그러면 이 내장 에이전트가 Kaspersky Anti Targeted Attack Platform 콘솔을 사용하여 관리됩니다(작업 실행, 격리된 개체 관리, 리포트 보기 및 기타 작업 등).

Endpoint Detection and Response Expert(on-premise) 설정

파라미터	설명
원격 측정 수집 서버에 연결	*원격 측정 수집 서버*는 컴퓨터에서 발생하는 이벤트에 대한 정보를 수집, 정규화, 상관관계 파악, 분석, 저장하는 SIEM 솔루션에 포함된 서버입니다. 원격 측정 수집 서버(KUMA)에 연결하려면 다음을 구성합니다. • **시간 초과(초)**. 최대 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 서버에 연결을 시도합니다. • **서버 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-premise) 도움말의 지침 참조). • **양방향 인증 사용**. Kaspersky Endpoint Security와 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-premise) 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.
주소 및 **포트**(원격 측정 수집 서버)	원격 측정 수집 서버 연결 설정. IP 주소(IPv4 또는 IPv6)를 입력할 수 있습니다. 여러 개의 원격 측정 수집 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

파라미터	설명
원격 측정 수집 서버로 원격 측정 전송	이 기능을 사용하면 KATA 서버에 대한 원격 측정 전송을 완전히 끌 수 있습니다. 예를 들어 Kaspersky Anti Targeted Attack Platform을 원격 측정을 사용하는 다른 솔루션과 함께 사용할 경우, KATA(EDR)의 원격 측정 전송을 끌 수 있습니다. 이렇게 하면 솔루션의 서버 로드를 최적화할 수 있습니다. Managed Detection and Response 솔루션과 KATA(EDR)가 배포되어 있다면 MDR 원격 측정을 사용해 KATA(EDR)에서 보안 위협 대응 작업을 만들 수 있습니다. • **IOA만 포함한 원격 측정 전송**. 이를 통해 원격 측정을 최적화하고 IOA만 포함한 원격 측정을 전송할 수 있습니다. *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. • **최대 이벤트 전송 지연(초)**. 애플리케이션이 서버와 동기화하여 동기화 주기가 만료된 후 이벤트를 보냅니다. 기본 설정은 30초입니다. • **전송당 이벤트 패킷 수 제한**. 버퍼가 이벤트로 가득 차면 애플리케이션이 서버와 동기화를 수행합니다. 기본 설정은 이벤트 1024개입니다. 이 기능을 사용하면 서버와 동기화하기 전에 이벤트 버퍼링을 비활성화할 수 있습니다.
요청 제한 사용	이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Endpoint Security가 이벤트 전송을 중지합니다. 원격 측정 설정을 구성합니다. • **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Endpoint Security는 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 Endpoint Security는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 기본 설정은 15%입니다.
다음 시간마다 서버로 동기화 요청 보내기(분)	서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Endpoint Security는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.
응답 서버에 연결	*응답 서버*는 데이터를 수신 및 검사하고, 개체의 동작을 조사하고, 조사 결과를 게시하기 위한 서버입니다. 응답 서버 연결을 위해 다음을 구성합니다. • **시간 초과(초)**. 최대 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 서버에 연결을 시도합니다. • **서버 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-premise) 도움말의 지침 참조). • **양방향 인증 사용**. Kaspersky Endpoint Security와 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-premise) 도움말의 지침 참조). 서버 설정을 구성한 후 Kaspersky Endpoint Security 설정에서 양방향 인증도 활성화하고 암호가 걸려 있는 암호화 컨테이너도 로드해야 합니다.
주소 및 **포트** (응답 서버)	응답 서버 연결 설정. IP 주소(IPv4 또는 IPv6)를 입력할 수 있습니다. 여러 개의 원격 측정 수집 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

Endpoint Detection and Response(KATA) 설정

파라미터	설명
다음 시간마다 서버로 동기화 요청 보내기(분)	서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Endpoint Security는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.
KATA 서버에 연결	Central Node 서버 연결을 위해 다음을 구성합니다. • **시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 Central Node 서버에 연결을 시도합니다. • **서버 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 Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 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.

파라미터	설명
주소 및 **포트** (KATA 서버)	Kaspersky Anti Targeted Attack Platform 서버 연결 설정. Central Node 서버 IP 주소(IPv4, IPv6) 및 서버에 연결할 포트를 입력하십시오. 여러 개의 Central Node 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.
KATA로 원격 측정 전송	이 기능을 사용하면 KATA 서버에 대한 원격 측정 전송을 완전히 끌 수 있습니다. 예를 들어 Kaspersky Anti Targeted Attack Platform을 원격 측정을 사용하는 다른 솔루션과 함께 사용할 경우, KATA(EDR)의 원격 측정 전송을 끌 수 있습니다. 이렇게 하면 솔루션의 서버 로드를 최적화할 수 있습니다. Managed Detection and Response 솔루션과 KATA(EDR)가 배포되어 있다면 MDR 원격 측정을 사용해 KATA(EDR)에서 보안 위협 대응 작업을 만들 수 있습니다. 원격 측정 설정을 구성합니다. • **최대 이벤트 전송 지연(초)**. 애플리케이션이 서버와 동기화하여 동기화 주기가 만료된 후 이벤트를 보냅니다. 기본 설정은 30초입니다. • **최대 이벤트 패키지 수**. 버퍼가 이벤트로 가득 차면 애플리케이션이 서버와 동기화를 수행합니다. 기본 설정은 이벤트 1024개입니다.
요청 제한 사용	이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Endpoint Security가 이벤트 전송을 중지합니다. 원격 측정 설정을 구성합니다. • **시간당 최대 이벤트 수**. 애플리케이션은 이벤트 스트림이 구성된 시간당 이벤트 제한을 초과할 경우 원격 측정 데이터 스트림을 분석하여 이벤트 전송을 제한합니다. Kaspersky Endpoint Security는 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 Endpoint Security는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 기본 설정은 15%입니다.

Network Detection and Response(KATA)

Kaspersky Endpoint Security for Windows에는 Kaspersky Anti Targeted Attack Platform(EDR (KATA)) 솔루션의 일부인 Kaspersky Network Detection and Response 구성 요소를 지원합니다. *Kaspersky Anti Targeted Attack Platform*은 표적형 공격, APT(지능형 지속 위협), 제로 데이 공격 등 지능형 위협을 적시에 탐지하도록 설계된 솔루션입니다. Kaspersky Anti Targeted Attack Platform에는 다음 세 가지 기능 단위가 포함됩니다.

- Kaspersky Anti Targeted Attack Platform(*KATA*)
- Kaspersky Endpoint Detection and Response(*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

모든 기능 단위를 구매하거나 개별 기능 단위를 따로 구매할 수 있습니다. 이 솔루션에 대한 자세한 내용은 Kaspersky Anti Targeted Attack Platform 도움말을 참조하십시오.

Kaspersky Endpoint Security는 기업 IT 인프라의 개별 컴퓨터에 설치되며 프로세스, 개방형 네트워크 연결 및 수정되는 파일을 계속해서 모니터링합니다. 컴퓨터의 이벤트에 대한 정보(원격 측정 데이터)는 Kaspersky Anti Targeted Attack Platform 서버로 전송됩니다. 이때, Kaspersky Endpoint Security는 애플리케이션에서 발견한 보안 위협에 대한 정보와 이를 처리한 결과에 대한 정보도 Kaspersky Anti Targeted Attack Platform 서버로 보냅니다.

EDR(KATA) 및 NDR(KATA) 통합은 Kaspersky Security Center 콘솔에서 구성됩니다. 그러면 이 내장 에이전트가 Kaspersky Anti Targeted Attack Platform 콘솔을 사용하여 관리됩니다(작업 실행, 격리된 개체 관리, 리포트 보기 및 기타 작업 등).

파라미터	설명
서버 연결 설정	**시간 초과(초)**. 최대 Central Node 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 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 Endpoint Security와 Central Node 서버 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 Central Node 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. 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 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.
주소 및 **포트**	Kaspersky Anti Targeted Attack Platform 서버 연결 설정. Central Node 서버 IP 주소(IPv4, IPv6) 및 서버에 연결할 포트를 입력하십시오. 여러 개의 Central Node 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.
다음 시간마다 NDR 서버로 동기화 요청 보내기(분)	서버로 전송되는 동기화 요청 빈도. 동기화하는 동안 Kaspersky Endpoint Security는 수정된 애플리케이션 설정 및 작업에 대한 정보를 보냅니다.
최대 이벤트 전송 지연(초)	애플리케이션이 서버와 동기화하여 동기화 주기가 만료된 후 이벤트를 보냅니다. 기본 설정은 30초입니다.
요청 제한 사용	이 기능은 서버의 부하를 최적화하는 데 도움이 됩니다. 이 확인란을 선택하면 애플리케이션이 전송되는 이벤트를 제한합니다. 이벤트 수가 구성된 제한을 초과하면 Kaspersky Endpoint Security가 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 Endpoint Security는 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 Endpoint Security는 총 이벤트 수에 대한 다른 이벤트의 비율이 다시 충분히 커지면 이벤트 전송을 재개합니다. 기본 설정은 15%입니다.

KUMA과 통합

Kaspersky Endpoint Security for Windows가 Kaspersky Unified Monitoring and Analysis Platform 솔루션을 지원합니다. *Kaspersky Unified Monitoring and Analysis Platform(KUMA)*은 조직의 IT 인프라를 위한 보안 정보 및 이벤트 관리(SIEM) 솔루션입니다. KUMA를 사용하면 보안 위협을 피해가 발생하기 전에 탐지, 분석 및 완화할 수 있습니다.

파라미터	설명
이벤트 전송 시 최대 지연 시간(초)	애플리케이션이 서버와 동기화하여 동기화 주기가 만료된 후 이벤트를 보냅니다. 기본 설정은 30초입니다.
KUMA 서버에 연결	**시간 초과(초)**. 최대 KUMA 서버 응답 시간 초과. 제한 시간이 초과되면 Kaspersky Endpoint Security는 다른 KUMA 서버에 연결을 시도합니다. **서버 인증서**. KUMA 서버와의 신뢰할 수 있는 연결을 설정하기 위한 TLS 인증서입니다. Kaspersky Unified Monitoring and Analysis Platform 콘솔에서 TLS 인증서를 얻을 수 있습니다(Kaspersky Unified Monitoring and Analysis Platform 지침 참조). 신뢰할 수 있는 연결을 구성하려면 KUMA 콘솔의 tcp 커넥터 설정에서 **With verification** TLS 모드를 선택해야 합니다(Kaspersky Unified Monitoring and Analysis Platform 도움말 에서 tcp 유형 커넥터 설정 참조). **양방향 인증 사용**. Kaspersky Endpoint Security와 KUMA 간에 보안 연결을 설정할 때 양방향 인증. 양방향 인증을 사용하려면 KUMA 콘솔의 tcp 커넥터 설정에서 **Custom PFX** TLS 모드를 선택해야 합니다(Kaspersky Unified Monitoring and Analysis Platform 도움말 에서 tcp 유형 커넥터 설정 참조). 그런 다음 암호화 컨테이너를 가져오고 암호화 컨테이너를 보호하기 위한 암호를 설정해야 합니다. *암호화 컨테이너*는 인증서와 개인 키가 있는 PFX 압축 파일입니다. KUMA 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.
KUMA 서버	Kaspersky Unified Monitoring and Analysis Platform 서버 설정에 대한 연결. IP 주소(IPv4 또는 IPv6)를 입력할 수 있습니다. 여러 개의 KUMA 서버 주소를 추가할 수 있습니다. Kaspersky Endpoint Security는 첫 번째 IP 주소로 서버에 연결을 시도합니다. 연결이 이루어지지 않으면, Kaspersky Endpoint Security는 목록에 있는 두 번째 IP 주소로 연결을 시도하고, 이 과정을 반복합니다.

전체 디스크 암호화

암호화 기술을 선택할 수 있습니다: Kaspersky 디스크 암호화 또는 BitLocker 드라이브 암호화(이후 간단히 "BitLocker"로도 호칭).

Kaspersky 디스크 암호화

Kaspersky 디스크 암호화는 Arm 기반 컴퓨터에서는 지원하지 않습니다.

시스템 하드 드라이브가 암호화된 이후에 컴퓨터를 시작할 때 사용자는 인증 에이전트의 인증을 거쳐야 하드 드라이브 접근 권한이 부여되어 운영 체제가 로드됩니다. 이때 컴퓨터에 연결된 토큰 또는 스마트카드의 암호, 아니면 LAN 관리자가 *인증 에이전트 계정 관리* 작업을 사용해 만든 인증 에이전트 계정의 사용자 이름 및 암호를 입력해야 합니다. 이러한 계정은 운영 체제에 로그인하는 사용자의 Microsoft Windows 계정에 기반합니다. Single Sign-On(SSO) 기술을 사용하면 인증 에이전트 계정의 사용자 이름과 암호를 사용하여 운영 체제에 자동으로 로그인할 수 있습니다.

인증 에이전트 내의 사용자 인증은 다음 두 가지 방법으로 실행할 수 있습니다:

- LAN 관리자가 Kaspersky Security Center 도구를 사용하여 생성한 인증 에이전트 계정의 이름과 암호 입력.
- 컴퓨터에 연결된 토큰 또는 스마트 카드의 암호 입력.

컴퓨터 하드 드라이브가 AES256 암호화 알고리즘을 사용해 암호화된 경우에 토큰 또는 스마트 카드만 사용할 수 있습니다. 컴퓨터 하드 드라이브가 AES56 암호화 알고리즘을 사용해 암호화된 경우에는 해당 명령에 전자 인증서 파일 추가가 거부됩니다.

BitLocker 드라이브 암호화

*BitLocker*는 Windows 운영 체제에 내장된 암호화 기술입니다. Kaspersky Endpoint Security를 사용하면 Kaspersky Next 인프라를 통해 Bitlocker를 제어하고 관리할 수 있습니다. BitLocker는 논리 볼륨을 암호화합니다. BitLocker는 이동식 드라이브 암호화에 사용할 수 없습니다. BitLocker에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

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.

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

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.

드라이브를 암호화한 후 BitLocker는 마스터 키를 만듭니다. Kaspersky Endpoint Security는 마스터 키를 Kaspersky Security Center로 전송하여, 예를 들어 사용자가 암호를 잊어버린 경우 디스크로의 접근을 복원할 수 있습니다.

사용자가 BitLocker로 디스크를 암호화하는 경우 Kaspersky Endpoint Security는 디스크 암호화에 대한 정보를 Kaspersky Security Center로 전송합니다. 그러나 Kaspersky Endpoint Security는 마스터 키를 Kaspersky Security Center로 보내지 않으므로 Kaspersky Security Center를 사용하여 디스크로의 접근을 복원할 수 없습니다. BitLocker가 Kaspersky Security Center와 올바르게 작동하려면 드라이브를 복호화하고 정책을 사용하여 드라이브를 다시 암호화하십시오. 드라이브를 로컬로 복호화하거나 정책을 사용하여 복호화할 수 있습니다.

Windows 그룹 정책을 사용하는 경우 정책 설정에서 BitLocker 매니지먼트를 해제합니다. Windows 정책 설정이 Kaspersky Endpoint Security 정책 설정과 충돌할 수 있습니다. 드라이브를 암호화할 때 오류가 발생할 수 있습니다.

파라미터	설명
암호화 모드	**모든 하드 드라이브 암호화**. 이 옵션을 선택하면 정책을 적용할 때 애플리케이션이 모든 하드 드라이브를 암호화합니다. 여러 운영 체제가 설치된 컴퓨터인 경우 암호화 후 애플리케이션이 설치된 운영 체제만 로드할 수 있습니다. **모든 하드 드라이브 복호화**. 이 옵션을 선택하면 정책을 적용할 때 애플리케이션이 모든 이전에 암호화된 하드 드라이브를 복호화합니다. **변경하지 않음**. 이 항목을 선택하면 정책을 적용할 때 애플리케이션은 이전 상태로 드라이브를 남겨 둡니다. 드라이브가 암호화되면 암호화된 상태로 남아 있습니다. 드라이브가 복호화되면 복호화된 상태로 남아 있습니다. 이 항목은 기본적으로 선택되어 있습니다.
암호화 시 자동으로 Windows 사용자에 대한 인증 에이전트 계정 생성	이 확인란을 선택하면 애플리케이션이 컴퓨터의 Windows 사용자 계정 목록을 기반으로 인증 에이전트 계정을 만듭니다. 기본적으로 Kaspersky Endpoint Security는 사용자가 지난 30일 동안 운영 체제에 로그인한 모든 로컬 및 도메인 계정을 사용합니다.
인증 에이전트 계정 생성 설정	**컴퓨터에 있는 모든 계정**. 항상 활성화된 컴퓨터의 모든 계정. **컴퓨터에 있는 모든 도메인**. 일부 도메인에 속하고 항상 활성화된 컴퓨터의 모든 계정. **컴퓨터에 있는 모든 로컬 계정**. 항상 활성화된 컴퓨터의 모든 로컬 계정. **일회성 암호를 사용하는 서비스 계정**. 서비스 계정은 사용자가 암호를 잊어버렸을 때와 같은 상황에서 컴퓨터에 액세스하는 데 필요합니다. 서비스 계정을 예비 계정으로 사용할 수도 있습니다. 계정 이름을 입력해야 합니다(기본값은 `ServiceAccount`). Kaspersky Endpoint Security는 자동으로 암호를 생성합니다. Kaspersky Security Center 콘솔에서 암호를 볼 수 있습니다. **로컬 관리자**. Kaspersky Endpoint Security가 컴퓨터의 로컬 관리자에 대한 인증 에이전트 사용자 계정을 생성합니다. **컴퓨터 관리자**. Kaspersky Endpoint Security가 컴퓨터 관리자 계정에 대한 인증 에이전트 사용자 계정을 생성합니다. Active Directory의 컴퓨터 속성에서 컴퓨터 관리자 역할이 있는 계정을 확인할 수 있습니다. 기본적으로 컴퓨터 관리자 역할은 정의되어 있지 않으므로, 어떤 계정에도 해당하지 않습니다. **사용 중인 계정**. Kaspersky Endpoint Security는 디스크 암호화 시 활성화된 계정에 대한 인증 에이전트 계정을 자동으로 생성합니다.
이 컴퓨터의 모든 사용자에 대해 로그인 시 인증 에이전트 계정 자동 생성	이 확인란을 선택하면 애플리케이션이 인증 에이전트를 시작하기 전에 컴퓨터의 Windows 사용자 계정에 대한 정보를 확인합니다. Kaspersky Endpoint Security가 인증 에이전트 계정이 없는 Windows 사용자 계정을 감지하면 애플리케이션이 암호화된 드라이브에 접근하기 위한 새 계정을 생성합니다. 새 인증 에이전트 계정에는 다음 기본 설정이 있습니다: 암호를 사용한 로그인만 허용, 첫 인증 후 암호 변경. 따라서 이미 암호화된 드라이브가 있는 컴퓨터에 대해서는 *인증 에이전트 계정 관리* 작업을 사용하여 인증 에이전트 계정을 직접 추가할 필요가 없습니다.
인증 에이전트에 입력되는 사용자 이름 저장	확인란을 선택하면 애플리케이션이 인증 에이전트 계정의 이름을 저장합니다. 다음 번에 동일한 계정을 사용해 인증 에이전트에서 인증할 때 계정 이름을 입력하라고 요구하지 않게 됩니다.
사용한 디스크 공간만 암호화(암호화 시간 단축)	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(암호화 시간 단축)** 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 Endpoint Security는 새로 데이터가 추가될 때마다 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
레거시 USB 지원 사용(권장 안 함)	이 확인란은 레거시 USB 지원 기능을 활성화하거나 비활성화합니다. *레거시 USB 지원***은** 운영 체제(BIOS 모드)를 시작하기 전에 컴퓨터 부팅 단계에서 USB 장치(예: 보안 토큰)를 사용할 수 있는 BIOS/UEFI 기능입니다. 운영 체제가 시작된 후에는 레거시 USB 지원은 USB 장치 지원에 영향을 미치지 않습니다. 이 확인란을 선택하면 컴퓨터 가동을 시작할 때 USB 장치 지원이 작동합니다. 레거시 USB 지원(Legacy USB Support) 기능이 활성화된 경우 BIOS 모드의 인증 에이전트는 USB를 통한 토큰 작업을 지원하지 않습니다. 하드웨어 호환성 문제가 발생한 컴퓨터에 한해서만 이 옵션을 사용하는 것이 좋습니다.
암호 설정	인증 에이전트 계정 암호 강도 설정. Single Sign-on 기술을 사용하는 경우 인증 에이전트는 Kaspersky Security Center에 지정된 암호 강도 요건을 무시합니다. 운영 체제 설정에서 암호 강도 요건을 설정할 수 있습니다.
Single Sign-On(SSO) 기술 사용	SSO 기술을 사용하면 암호화된 하드 드라이브 접근 및 운영 체제 로그인에 동일한 계정 자격 증명을 사용할 수 있습니다. 이 확인란을 선택하면 암호화된 하드 드라이브 접근을 위해 계정 자격 증명을 입력해야 하며, 따라서 운영 체제에 자동 로그인됩니다. 이 확인란의 선택을 취소하면 암호화된 하드 드라이브에 접근하고 이후 운영 체제에 로그인하기 위해 암호화된 하드 드라이브 접근을 위한 자격 증명과 운영 체제 사용자 계정 자격 증명을 별도로 입력해야 합니다.
타사 자격 증명 공급업체 래핑	Kaspersky Endpoint Security는 타사 자격 증명 공급업체인 ADSelfService Plus를 지원합니다. 타사 자격 증명 공급업체와 작업 시, 인증 에이전트는 운영 체제가 로드되기 전에 암호를 가로챕니다. 즉, 사용자는 Windows에 로그인할 때 암호를 한 번만 입력하면 됩니다. 사용자는 Windows에 로그인한 후 기업 서비스 인증 등을 위해 타사 자격 증명 공급업체의 기능을 활용할 수 있습니다. 타사 자격 증명 공급업체 사용 시, 사용자가 독자적으로 암호를 재설정할 수도 있습니다. 이때 Kaspersky Endpoint Security는 인증 에이전트의 암호를 자동으로 업데이트합니다. 애플리케이션에서 지원하지 않는 타사 자격 증명 공급업체 사용 시, Single Sign-On 기술 동작에 몇 가지 제한이 생길 수 있습니다.
도움말	**인증**. 계정 자격 증명을 입력할 때 인증 에이전트 창에 표시되는 도움말 텍스트입니다. **암호 변경**. 인증 에이전트 계정의 암호를 변경할 때 인증 에이전트 창에 표시되는 도움말 텍스트입니다. **암호 복구**. 인증 에이전트 계정의 암호를 복구할 때 인증 에이전트 창에 표시되는 도움말 텍스트입니다.

BitLocker 드라이브 암호화 구성 요소 설정

파라미터	설명
암호화 모드	**모든 하드 드라이브 암호화**. 이 옵션을 선택하면 정책을 적용할 때 애플리케이션이 모든 하드 드라이브를 암호화합니다. 여러 운영 체제가 설치된 컴퓨터인 경우 암호화 후 애플리케이션이 설치된 운영 체제만 로드할 수 있습니다. **모든 하드 드라이브 복호화**. 이 옵션을 선택하면 정책을 적용할 때 애플리케이션이 모든 이전에 암호화된 하드 드라이브를 복호화합니다. **변경하지 않음**. 이 항목을 선택하면 정책을 적용할 때 애플리케이션은 이전 상태로 드라이브를 남겨 둡니다. 드라이브가 암호화되면 암호화된 상태로 남아 있습니다. 드라이브가 복호화되면 복호화된 상태로 남아 있습니다. 이 항목은 기본적으로 선택되어 있습니다.
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 버전)	이 확인란을 선택하면 애플리케이션이 하드웨어 암호화를 적용합니다. 이 방법을 사용하면 암호화 속도가 빨라지고 컴퓨터 리소스를 적게 사용합니다.

파라미터	설명
사용된 디스크 공간만 암호화 (Windows 8 이상 버전)	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(암호화 시간 단축)** 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 Endpoint Security는 새로 데이터가 추가될 때마다 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.
인증 유형	**암호만(Windows 8 이상 버전)** 이 옵션을 선택하면 사용자가 암호화된 드라이브에 접근하려고 시도할 때 Kaspersky Endpoint Security가 사용자에게 암호 입력을 요구합니다. 신뢰하는 플랫폼 모듈(TPM)을 사용하지 않는 경우 이 옵션을 선택할 수 있습니다. **신뢰하는 플랫폼 모듈(TPM)** 이 옵션을 선택하면 BitLocker가 신뢰하는 플랫폼 모듈(TPM)을 사용합니다. *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. 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. 선택된 인증 방법은 암호 또는 PIN 요구 사항을 지정하여 구성해야 합니다. • **최소 PIN 길이(문자 수)**. • **최소 암호 길이(문자 수)**. • **TPM에 대한 암호/PIN 유효 기간 제한(일)**. • **강화 PIN(문자와 숫자) 사용**. *강화 PIN*은 대문자와 소문자, 라틴 문자, 특수 문자 및 공백 등 숫자 외의 다른 문자도 사용할 수 있습니다.
자동으로 복구 키 재생성(일)	BitLocker로 보호되는 드라이브에 대한 접근 복원을 위한 암호를 자동으로 업데이트합니다. 확인란이 선택되면 복구 키 암호 유효 기간을 지정합니다. 이렇게 하면 복구 키 암호 재사용을 방지합니다.

파일 레벨 암호화

Arm 기반 컴퓨터에서는 파일 암호화를 지원하지 않습니다.

이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

로컬 컴퓨터 드라이브에 저장된 확장자 또는 확장자 그룹별 파일 목록과 폴더별 목록을 컴파일하고, 특정 애플리케이션에 의해 생성된 파일을 암호화하는 규칙을 생성할 수 있습니다. 정책을 적용하면 Kaspersky Endpoint Security에서 다음 파일이 암호화 및 복호화됩니다:

- 암호화 및 복호화 목록에 개별적으로 추가된 파일;
- 암호화 및 복호화 목록에 추가된 폴더에 저장된 파일;
- 개별 애플리케이션에 의해 생성된 파일.

파일 암호화에는 다음과 같은 특징이 있습니다.

- Kaspersky Endpoint Security는 운영 체제의 로컬 사용자 프로필에 한해 사전 정의된 폴더에서 파일을 암호화/복호화합니다. Kaspersky Endpoint Security는 로밍 사용자 프로필, 필수 사용자 프로필, 임시 사용자 프로필 또는 리다이렉트 폴더의 사전 정의된 폴더에서는 파일을 암호화 또는 복호화하지 않습니다.
- Kaspersky Endpoint Security는 파일 암호화로 인해 운영 체제 및 설치된 애플리케이션에 문제를 야기하는 파일은 암호화하지 않습니다. 예를 들어 다음 파일과 폴더는 그 하위 폴더를 포함하여 암호화에서 예외합니다:
  - %WINDIR%
  - %PROGRAMFILES% 및 %PROGRAMFILES(X86)%
  - Windows 레지스트리 파일

  암호화 예외 목록은 확인 또는 편집할 수 없습니다. 암호화 예외 목록의 파일과 폴더를 암호화 목록에 추가할 수 있지만 파일 암호화 도중 암호화되지 않습니다.

파일 레벨 암호화 구성 요소 설정

파라미터	설명
암호화 모드	**변경하지 않음**. 이 항목을 선택하면 Kaspersky Endpoint Security가 파일과 폴더를 암호화 또는 복호화하지 않고 그대로 둡니다. **규칙을 따름**. 이 항목을 선택하면 Kaspersky Endpoint Security는 암호화 규칙에 따라 파일 및 폴더를 암호화하고, 복호화 규칙에 따라 파일 및 폴더를 복호화하며, 애플리케이션 규칙에 따라 암호화된 파일에 대한 애플리케이션의 접근을 제어합니다. **모두 복호화**. 이 항목을 선택하면 Kaspersky Endpoint Security가 모든 암호화된 파일과 폴더를 복호화합니다.

파라미터	설명
암호화	이 탭에는 로컬 드라이브에 저장된 파일에 대한 암호화 규칙이 표시됩니다. 다음과 같이 파일을 추가할 수 있습니다. • **사전 정의된 폴더**. Kaspersky Endpoint Security에서 다음 영역을 추가할 수 있습니다. **문서**. 운영 체제의 표준 *문서* 폴더에 있는 파일 및 해당 하위 폴더. **즐겨찾기**. 운영 체제의 표준 *즐겨찾기* 폴더에 있는 파일 및 해당 하위 폴더. **바탕 화면**. 운영 체제의 표준 *바탕 화면* 폴더에 있는 파일 및 해당 하위 폴더. **임시 파일**. 컴퓨터에 설치된 애플리케이션 작동과 관련된 임시 파일. 예를 들어 Microsoft Office 애플리케이션은 문서의 백업 복사본이 포함된 임시 파일을 만듭니다. **Outlook 파일**. 데이터 파일(PST), 오프라인 데이터 파일(OST), 오프라인 주소록 파일(OAB) 및 개인 주소록 파일(PAB)과 같은 Outlook 메일 클라이언트 작동과 관련된 파일. • **사용자 지정 폴더**. 폴더 경로를 입력할 수 있습니다. 폴더 경로를 추가할 때는 다음 규칙을 준수하십시오. 환경 변수를 사용하십시오(예: `%FOLDER%\UserFolder\`). 환경 변수는 경로 시작 부분에서 한 번만 사용할 수 있습니다. 상대 경로를 사용하지 마십시오. `*`과 `?` 문자를 사용하지 마십시오. UNC 경로를 사용하지 마십시오. `;` 또는 `,`를 구분 문자로 사용하십시오. • **파일 확장자로**. 확장자 그룹 *압축 파일*과 같은 목록에서 확장자 그룹을 선택할 수 있습니다. 파일 확장자를 직접 추가할 수도 있습니다.
복호화	이 탭에는 로컬 드라이브에 저장된 파일에 대한 복호화 규칙이 표시됩니다.
애플리케이션 규칙	이 탭은 애플리케이션에 대한 암호화된 파일 접근 규칙과 개별 애플리케이션에 의해 생성 또는 수정된 파일의 암호화 규칙이 포함된 표를 표시합니다.
암호화 패키지	암호화 패키지를 생성할 때 충족해야 하는 암호 강도 요건.

이동식 드라이브 암호화

Arm 기반 컴퓨터에서는 이동식 드라이브 암호화를 지원하지 않습니다.

이 구성 요소는 Kaspersky Endpoint Security가 워크스테이션용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성 요소는 Kaspersky Endpoint Security가 서버용 Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

Kaspersky Endpoint Security는 FAT32 및 NTFS 파일 시스템의 파일 암호화를 지원합니다. 지원하지 않는 파일 시스템을 사용하는 이동식 드라이브가 컴퓨터에 연결되어 있으면 해당 이동식 드라이브에 대한 암호화 작업 종료 시에 오류가 발생하며 Kaspersky Endpoint Security가 이동식 드라이브에 읽기 전용 상태를 할당합니다.

이동식 드라이브의 데이터를 보호하기 위해 다음 유형의 암호화를 사용할 수 있습니다.

- Full Disk Encryption (FDE, 전체 디스크 암호화)

  파일 시스템을 포함한 전체 이동식 드라이브의 암호화.

  회사 네트워크 외부에서 암호화된 데이터에 접근할 수 없습니다. 컴퓨터가 Kaspersky Security Center(예: "게스트" 컴퓨터에서)에 연결되어 있지 않으면 회사 네트워크 내에서 암호화된 데이터에 접근할 수 없습니다.

- File Level Encryption (FLE, 파일 레벨 암호화)

  이동식 드라이브에 있는 파일만 암호화. 파일 시스템은 변경되지 않습니다.

이동식 드라이브의 파일을 암호화하면 *휴대용 모드*라는 특수 모드를 사용하여 회사 네트워크 외부의 데이터에 접근할 수 있습니다.

암호화 중에 Kaspersky Endpoint Security는 마스터 키를 생성합니다. Kaspersky Endpoint Security는 다음 저장소에 마스터 키를 저장합니다.

- Kaspersky Security Center
- 사용자의 컴퓨터

  마스터 키는 사용자의 비밀 키로 암호화됩니다.
- 이동식 드라이브

  마스터 키는 Kaspersky Security Center의 공개 키로 암호화됩니다.

암호화가 완료되면 일반 암호화되지 않은 이동식 드라이브에 있는 것처럼 회사 네트워크 내에서 이동식 드라이브의 데이터에 접근할 수 있습니다.

암호화된 데이터 접근

암호화된 데이터가 있는 이동식 드라이브가 연결되면 Kaspersky Endpoint Security는 다음 작업을 수행합니다.

1. 사용자 컴퓨터의 로컬 저장소에서 마스터 키를 확인합니다.

   마스터 키가 발견되면 사용자는 이동식 드라이브의 데이터에 접근할 수 있습니다.

   마스터 키를 찾지 못하면 Kaspersky Endpoint Security는 다음 작업을 수행합니다.

   a. Kaspersky Security Center에 요청을 보냅니다.

      요청을 받은 후 Kaspersky Security Center는 마스터 키가 포함된 응답을 보냅니다.

   b. Kaspersky Endpoint Security는 암호화된 이동식 드라이브를 사용하여 후속 작업을 위해 사용자 컴퓨터의 로컬 저장소에 마스터 키를 저장합니다.
2. 데이터를 복호화합니다.

이동식 드라이브 암호화의 특징

이동식 드라이브 암호화에는 다음과 같은 특징이 있습니다.

- 특정 그룹의 관리 컴퓨터에 대해서는 별도의 이동식 드라이브 암호화 사전 설정을 사용하여 정책을 적용합니다. 따라서 이동식 드라이브의 암호화/복호화를 위해 구성된 Kaspersky Security Center 정책을 적용한 결과는 이동식 드라이브가 연결된 컴퓨터에 따라 다릅니다.
- Kaspersky Endpoint Security는 이동식 드라이브에 저장된 읽기 전용 파일은 암호화/복호화하지 않습니다.

- 다음 장치 유형은 이동식 드라이브로 지원됩니다:
  - USB 버스를 통해 연결된 데이터 미디어
  - USB 및 FireWire 버스를 통해 연결된 하드 드라이브
  - USB 및 FireWire 버스를 통해 연결된 SSD 드라이브

이동식 드라이브 구성 요소 설정의 암호화

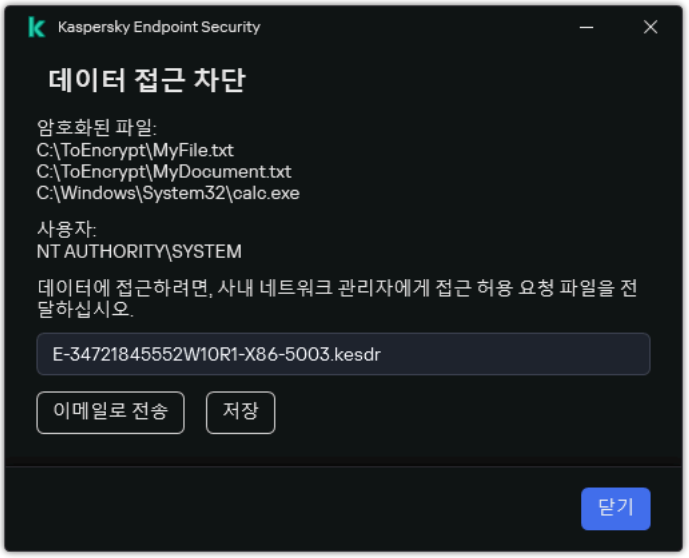
파라미터	설명
암호화 모드	**전체 이동식 드라이브 암호화**. 이 항목을 선택하면 지정된 이동식 드라이브 암호화 설정을 사용하여 정책을 적용할 때 Kaspersky Endpoint Security는 그 파일 시스템을 포함하여 이동식 드라이브를 섹터별로 암호화합니다. **모든 파일 암호화**. 이 항목을 선택하면 지정된 이동식 드라이브 암호화 설정을 사용하여 정책을 적용할 때 Kaspersky Endpoint Security가 이동식 드라이브에 저장된 모든 파일을 암호화합니다. Kaspersky Endpoint Security는 이미 암호화된 파일은 다시 암호화하지 않습니다. 폴더 구조와 암호화된 파일의 이름을 포함하여 이동식 드라이브의 파일 시스템 내용은 암호화되지 않으며 접근 가능합니다. **새 파일만 암호화**. 이 항목을 선택하면 지정된 이동식 드라이브 암호화 설정을 사용하여 정책을 적용할 때 Kaspersky Endpoint Security는 Kaspersky Security Center 정책이 마지막으로 적용된 후 이동식 드라이브에 추가되었거나 수정된 파일만 암호화합니다. 이동식 드라이브가 개인 및 업무의 두 가지 용도로 사용될 경우에 이 암호화 모드를 사용하는 것이 좋습니다. 이 암호화 모드를 사용하면 기존의 모든 파일은 변경되지 않으며 사용자가 Kaspersky Endpoint Security가 설치되고 암호화 기능이 설정된 업무용 컴퓨터에서 생성한 파일만 암호화할 수 있습니다. 따라서 컴퓨터에 암호화 기능이 설정된 Kaspersky Endpoint Security가 설치되었는지 여부에 관계 없이 개인 파일은 전과 같이 계속 접근할 수 있습니다. **전체 이동식 드라이브 복호화**. 이 항목을 선택하면 지정된 이동식 드라이브 암호화 설정을 사용하여 정책을 적용할 때 Kaspersky Endpoint Security가 이동식 드라이브에 저장된 모든 암호화된 파일과 이동식 드라이브의 파일 시스템(이전에 암호화된 경우)을 복호화합니다. **변경하지 않음**. 이 항목을 선택하면 정책을 적용할 때 애플리케이션은 이전 상태로 드라이브를 남겨 둡니다. 드라이브가 암호화되면 암호화된 상태로 남아 있습니다. 드라이브가 복호화되면 복호화된 상태로 남아 있습니다. 이 항목은 기본적으로 선택되어 있습니다.
휴대용 모드	이 확인란은 회사 네트워크 외부의 컴퓨터에서 이동식 드라이브의 저장된 파일에 접근이 가능하도록 이동식 드라이브를 준비하는 기능을 작동 또는 중지합니다. 이 확인란을 선택하면 애플리케이션의 정책에 따라 이동식 드라이브의 파일을 암호화하기 전에 Kaspersky Endpoint Security가 암호를 지정하라는 메시지를 표시합니다. 회사 네트워크 외부의 컴퓨터에서 이동식 드라이브의 암호화된 파일에 접근할 경우 이 암호가 필요합니다. 암호 강도를 구성할 수 있습니다. **모든 파일 암호화** 또는 **새 파일만 암호화** 모드에 대해 휴대용 모드가 제공됩니다.
사용한 디스크 공간만 암호화	이 확인란은 사용한 디스크 부분만 암호화하는 암호화 모드를 작동 또는 중지합니다. 이 모드는 데이터를 수정하거나 삭제하지 않은 새 드라이브에 사용하는 것이 좋습니다. 이 확인란을 선택하면 드라이브에서 파일이 저장되어 있는 부분만 암호화됩니다. Kaspersky Endpoint Security는 새로 데이터가 추가될 때마다 자동으로 데이터를 암호화합니다. 확인란이 비어 있으면 이전에 삭제 및 수정되고 남은 파일 조각을 포함하여 전체 드라이브가 암호화됩니다. 사용한 공간만 암호화하는 기능은 **전체 이동식 드라이브 암호화** 모드에서만 사용할 수 있습니다. 암호화가 시작된 후 **사용한 디스크 공간만 암호화** 기능을 작동하거나 중지해도 이 설정이 변경되지 않습니다. 암호화를 시작하기 전에 확인란을 선택 또는 선택 해제해야 합니다.

사용자 지정 규칙	이 표는 사용자 지정 암호화 규칙이 정의된 장치가 들어 있습니다. 다음과 같은 방법으로 개별 이동식 드라이브에 대한 암호화 규칙을 만들 수 있습니다.
	• 장치 제어를 위한 신뢰하는 장치 목록에서 이동식 드라이브를 추가합니다.
	• 이동식 드라이브를 직접 추가합니다.
	  • 장치 ID(하드웨어 ID - Hardware ID 또는 HWID)별로 추가
	  • 장치 모델, 공급업체 ID(Vendor ID 또는 VID) 및 제품 ID(Product ID 또는 PID)별로 추가

파라미터	설명
오프라인 모드에서 이동식 드라이브 암호화 허용	이 확인란을 선택하면 Kaspersky Security Center와 연결되어 있지 않을 경우에도 Kaspersky Endpoint Security가 이동식 드라이브를 암호화합니다. 이 경우 이동식 드라이브의 복호화에 필요한 데이터가 이동식 드라이브가 연결된 하드 드라이브에 저장되며 Kaspersky Security Center로 전송되지 않습니다. 이 확인란을 선택하지 않으면 Kaspersky Security Center와 연결되어 있지 않을 경우 Kaspersky Endpoint Security가 이동식 드라이브를 암호화하지 않습니다.
암호화용 암호 설정 / 휴대용 파일 관리자	휴대용 파일 관리자의 암호 강도 설정.

템플릿(데이터 암호화)

데이터 암호화 후 Kaspersky Endpoint Security는 조직의 인프라 및 Kaspersky Security Center 중앙 관리 서버 변경 등의 이유로 데이터에 대한 접근을 제한할 수 있습니다. 사용자가 암호화된 데이터에 접근할 수 없는 경우 관리자에게 데이터 접근을 요청할 수 있습니다. 즉, 사용자는 접근 허용 요청 파일을 관리자에게 보내야 합니다. 그런 다음 사용자는 관리자로부터 받은 응답 파일을 Kaspersky Endpoint Security에 업로드해야 합니다. Kaspersky Endpoint Security에서 이메일을 통해 관리자에게 데이터 접근을 요청할 수 있습니다(아래 그림 참조).



암호화된 데이터에 대한 접근 요청

암호화된 데이터에 대한 접근 권한이 없음을 보고하기 위한 템플릿이 제공됩니다. 사용자 편의를 위해 다음 필드를 채울 수 있습니다.

- **수신자**. 데이터 암호화 기능에 대한 권한이 있는 관리자 그룹의 이메일 주소를 입력합니다.
- **제목**. 암호화된 파일에 대한 접근 허용 요청의 이메일 제목을 입력합니다. 예를 들어 메시지 필터링을 위한 태그를 추가할 수 있습니다.
- **사용자 메시지**. 필요시 메시지 내용을 변경합니다. 변수를 사용하여 필요한 데이터를 얻을 수 있습니다(예: `%USER_NAME%` 변수).

예외 규칙

*신뢰 구역*은 Kaspersky Endpoint Security에서 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 Endpoint Security가 해당 개체 또는 애플리케이션에 대한 접근을 차단하면 개체와 애플리케이션을 신뢰 구역에 포함시키는 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.

Kaspersky Endpoint Security 12.5 for Windows 버전부터는 EDR 원격 측정을 신뢰 구역으로 추가할 수 있습니다. 이를 통해 애플리케이션이 Kaspersky Anti Targeted Attack Platform(EDR) 솔루션용 원격 측정 수집 서버로 전송하는 데이터를 최적화할 수 있습니다.

Kaspersky Endpoint Security 12.6 for Windows부터 검사 예외 및 신뢰하는 애플리케이션 이 신뢰 구역에 추가됩니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 SQL 서버, Microsoft Exchange 서버 및 System Center Configuration Manager에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다. 즉, 서버의 애플리케이션에 대한 신뢰 구역을 직접 설정할 필요가 없습니다.

Kaspersky Endpoint Security 12.8 for Windows부터 가상 환경 보호를 위한 Light Agent 모드로 애플리케이션을 설치할 수 있습니다. 사전 정의된 검사 예외 및 신뢰하는 애플리케이션을 사용하면 Citrix와 VMware 가상 환경에서 Kaspersky Endpoint Security를 빠르게 구성할 수 있습니다.

검사 예외

*검사 예외*는 Kaspersky Endpoint Security에서 특정 개체의 바이러스 및 기타 위협을 검사하지 않도록 하려면 충족해야 하는 조건 집합입니다. 검사 예외를 사용하면 범죄자가 컴퓨터 또는 사용자 데이터에 심각한 손상을 가하기 위해 악용할 수 있는 합법적인 소프트웨어를 안전하게 사용할 수 있습니다. 해당 애플리케이션은 악성 기능을 갖지 않지만 침입자가 악용할 수 있습니다. 침입자에게 악용되어 사용자의 컴퓨터나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어에 대한 상세 정보는 Kaspersky IT 백과사전을 참조하십시오.

이러한 애플리케이션은 Kaspersky Endpoint Security에 의해 차단될 수 있습니다. 차단되는 것을 방지하기 위해 사용 중인 애플리케이션에 대한 검사 예외를 구성할 수 있습니다. 그러려면 Kaspersky IT 백과사전에 나와 있는 이름이나 이름 마스크를 신뢰 구역에 추가합니다. 컴퓨터 원격 관리에 Radmin 애플리케이션을 자주 사용하는 경우를 예로 들어 보겠습니다. Kaspersky Endpoint Security는 이러한 활동을 의심스러운 것으로 간주하여 차단할 수 있습니다. 애플리케이션이 차단되는 것을 방지하기 위해 Kaspersky IT 백과사전에 있는 이름 또는 이름 마스크로 검사 예외를 만듭니다.

정보를 수집하고 처리를 위해 정보를 전송하는 애플리케이션이 컴퓨터에 설치되어 있는 경우 Kaspersky Endpoint Security에서 이 애플리케이션을 악성 코드로 분류할 수 있습니다. 이를 방지하려면 이 문서에 설명한 대로 Kaspersky Endpoint Security를 구성하여 애플리케이션을 검사에서 예외할 수 있습니다.

검사 예외는 시스템 관리자가 구성한 다음과 같은 애플리케이션 구성 요소 및 작업에서 사용할 수 있습니다:

- 행동 탐지
- 익스플로잇 방지
- 호스트 침입 방지

- 파일 위협 보호
- 웹 위협 보호
- 메일 위협 보호
- *악성 코드 검사* 작업

신뢰하는 애플리케이션 목록

*신뢰하는 애플리케이션 목록*은 Kaspersky Endpoint Security에서 파일 및 네트워크 활동(악성 활동 포함)과 시스템 레지스트리 접근을 감시하지 않는 애플리케이션 목록입니다. 기본적으로 Kaspersky Endpoint Security는 다른 애플리케이션 프로세스에서 열려 있거나 실행하거나 저장하는 개체를 검사하고 모든 애플리케이션 활동과 그로 인해 생성되는 네트워크 트래픽을 모니터링합니다. 신뢰하는 애플리케이션 목록에 애플리케이션이 추가되면 Kaspersky Endpoint Security는 애플리케이션 활동의 모니터링을 중단합니다.

검사 예외 및 신뢰하는 애플리케이션의 차이는 Kaspersky Endpoint Security가 검사 예외의 파일은 스캔하지 않지만 신뢰하는 애플리케이션의 경우 시작한 프로세스를 제어하지 않습니다. 신뢰하는 애플리케이션이 검사 예외에 포함되어 있지 않은 폴더에서 악성 파일을 생성할 경우, Kaspersky Endpoint Security는 파일을 감지하고 위험을 제거합니다. 폴더가 예외로 추가되면 Kaspersky Endpoint Security는 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, 의심으로 Kaspersky Endpoint Security에 의해 분류된 어떤 동작이 다수의 애플리케이션의 기능의 마우스 오른쪽 내에서 안전한 것으로 여기게 됩니다. 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 Endpoint Security와 다른 애플리케이션 사이의 호환성 문제를 방지합니다. 예를 들어, Kaspersky Endpoint Security와 다른 바이러스 방지 애플리케이션에서 제3자 컴퓨터가 네트워크 트래픽을 이중으로 스캔하는 문제를 방지합니다.

이렇게 해도 실행 파일과 신뢰하는 애플리케이션 프로세스에 대해서는 계속 바이러스와 기타 악성 코드 검사가 수행됩니다. 검사 예외를 사용하여 애플리케이션을 Kaspersky Endpoint Security 검사에서 완전히 예외시킬 수 있습니다.

파라미터	설명

탐지된 개체 유형

구성된 애플리케이션 설정에 상관없이 Kaspersky Endpoint Security가 항상 바이러스, 웜 및 트로이목마를 탐지하고 차단합니다. 이러한 악성 코드가 컴퓨터에 심각한 손상을 불러 일으킬 수 있기 때문입니다.

- **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(*Overwriting*) 바이러스는 감염된 파일 코드 위에 자신의 코드를 써서 파일의 컨텐츠를 지웁니다. 감염된 파일은 기능이 중지되며 복원할 수 없습니다. 기생(*Parasitic*) 바이러스는 파일을 수정한 다음 그냥 두거나 부분적으로만 기능하도록 둡니다. 동반(*Companion*) 바이러스는 파일을 수정하지는 않지만 자신의 복제를 만듭니다. 감염된 파일을 열면 바이러스의 복제가 시작됩니다. 다음과 같은 바이러스 유형 또한 발생됩니다: *링크(Link) 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 채팅(Internet Relay Chats)을 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.
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(랜섬웨어 포함)**

  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.
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: 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.
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.

- **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.
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 Endpoint Security는 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: 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 Endpoint Security는 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.

예외 규칙

이 표에는 검사 예외에 대한 정보가 들어 있습니다.

> 절대 경로 대신 상대 경로를 지정하는 것이 좋습니다. 이렇게 하면 파일 시스템 개체뿐만 아니라 파일리스 개체도 제외할 수 있습니다. 예: `*\Program Files (x86)\Folder\Subfolder`.

다음 방법을 사용하여 검사 시 개체를 예외할 수 있습니다:

- 파일 또는 폴더로의 경로 지정.
- 개체 해시 입력.
- 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.

    파일 또는 폴더 경로 어디서든 마스크를 사용할 수 있습니다. 예를 들어, 컴퓨터에 있는 모든 사용자 계정의 다운로드 폴더를 검사 범위에 포함시키려면 `C:\Users\*\Downloads\` 마스크를 입력합니다.

    Kaspersky Endpoint Security는 환경 변수를 지원합니다

	Kaspersky Endpoint Security는 Kaspersky Security Center 콘솔을 사용하여 예외 규칙 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. • Kaspersky IT 백과사전(`Email-Worm`, `Rootkit`, `RemoteAdmin` 등)의 분류에 따라 개체 유형 이름을 입력합니다. `?` 문자(단일 문자 대체) 및 `*` 문자(모든 문자 대체)와 함께 마스크를 사용할 수 있습니다. 예를 들어 `Client*` 마스크를 지정하면 애플리케이션이 `Client-IRC`, `Client-P2P`, `Client-SMTP` 개체를 검사에서 제외합니다. 관리자가 콘솔에서 검사 예외 구성을 차단하고('닫힌 자물쇠' 기호) 로컬 검사 예외 항목이 금지된 경우(**로컬 예외 항목 사용 허용** 확인란이 선택 취소됨) Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 검사 예외 목록을 숨깁니다.
신뢰하는 애플리케이션	이 표에는 Kaspersky Endpoint Security가 작동 중에 그 활동을 감시하지 않는 신뢰하는 애플리케이션이 나열됩니다. Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다. Kaspersky Endpoint Security는 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. 신뢰하는 애플리케이션 표에 포함된 애플리케이션인지 여부에 상관없이 각 애플리케이션의 시작은 애플리케이션 제어 구성 요소에 의해 제어됩니다. Kaspersky Endpoint Security 콘솔에서 관리자가 신뢰하는 애플리케이션 구성을 차단하고('닫힌 자물쇠' 기호) 신뢰하는 로컬 애플리케이션이 차단된 경우(**신뢰하는 로컬 애플리케이션 사용 허용** 확인란을 선택 취소함) Kaspersky Endpoint Security는 애플리케이션의 사용자 인터페이스에서 신뢰할 수 있는 애플리케이션의 통합 목록을 숨깁니다.
상속할 때 값 병합 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이렇게 하면 Kaspersky Security Center의 자식 및 부모 정책에 있는 검사 예외 및 신뢰하는 애플리케이션 목록이 병합됩니다. 목록을 병합하려면 Kaspersky Security Center의 자식 정책이 부모 정책 설정을 상속하도록 구성해야 합니다. 확인란을 선택하면 Kaspersky Security Center 부모 정책의 목록 항목이 자식 정책에 표시됩니다. 예를 들어, 전체 조직에 대해 신뢰하는 애플리케이션의 통합 목록을 만들 수 있습니다. 자식 정책에 상속된 목록 항목은 삭제하거나 편집할 수 없습니다. 검사 예외 목록의 항목과 상속 중에 병합된 신뢰하는 애플리케이션 목록은 부모 정책에서만 삭제 및 편집할 수 있습니다. 하위 수준 정책에서 목록 항목을 추가, 편집 또는 삭제할 수 있습니다. 자식 및 부모 정책 목록에서 일치하는 항목은 부모 정책과 같은 항목으로 표시됩니다. 이 확인란을 선택하지 않으면 Kaspersky Security Center 정책 설정을 상속할 때 목록 항목을 병합하지 않습니다. 이 기능을 사용하면 정책 프로필의 목록을 병합할 수도 있습니다. 목록을 병합하려면 우선순위가 가장 높은 프로필에서 우선순위가 낮은 프로필의 설정 상속을 활성화합니다. 정책 프로필 우선순위에 관한 상세 정보는 Kaspersky Security Center 도움말을 참조하십시오.
로컬 예외 항목 사용 허용/신뢰하는 로컬 애플리케이션 사용 허용 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	*로컬 예외 규칙 및 신뢰하는 로컬 애플리케이션(로컬 신뢰 구역)* – 특정 컴퓨터에 대한 Kaspersky Endpoint Security의 사용자 정의 개체 및 애플리케이션 목록입니다. Kaspersky Endpoint Security는 로컬 신뢰 구역의 개체 및 애플리케이션을 감시하지 않습니다. 이러한 방식으로 사용자는 정책의 일반 신뢰 구역 외에도 자신의 로컬 예외 규칙 및 신뢰하는 애플리케이션 목록을 생성할 수 있습니다. 확인란을 선택하면 사용자가 로컬 검색 예외 목록과 신뢰하는 애플리케이션 로컬 목록을 만들 수 있습니다. 관리자는 Kaspersky Security Center를 사용하여 컴퓨터 속성의 목록 항목을 확인, 추가, 편집 또는 삭제할 수 있습니다. 확인란을 선택 해제하면 사용자는 정책에서 생성된 검사 예외 및 신뢰하는 애플리케이션의 일반 목록에만 접근할 수 있습니다.
EDR(KATA) / NDR(KATA) 원격 측정 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이 표에는 EDR 원격 측정 예외 규칙에 대한 정보가 들어 있습니다.

KUMA 원격 측정 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	Kaspersky Unified Monitoring and Analysis Platform(KUMA)로 전송할 이벤트 목록입니다. Kaspersky Endpoint Security는 다음 모드에서 작동합니다. • **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.
신뢰하는 시스템 인증서 저장소	신뢰하는 시스템 인증서 저장소 중 하나를 선택하면 Kaspersky Endpoint Security가 신뢰하는 디지털 서명의 애플리케이션을 검사에서 제외합니다. Kaspersky Endpoint Security는 이러한 애플리케이션을 **신뢰하는** 그룹에 자동으로 할당합니다. **사용 안 함**을 선택하면 Kaspersky Endpoint Security는 디지털 서명 유무에 관계없이 애플리케이션을 검사합니다. Kaspersky Endpoint Security는 애플리케이션이 컴퓨터에 미칠 수 있는 위험 수준에 따라 해당 애플리케이션을 신뢰 그룹에 배치합니다.

애플리케이션 설정

애플리케이션의 다음 일반 설정을 구성할 수 있습니다:

- 운영 모드
- 자기 보호
- 성능
- 디버그 정보
- 설정 적용 시 컴퓨터 상태

애플리케이션 설정

파라미터	설명
컴퓨터 시작 시 애플리케이션 시작(권장)	이 옵션을 선택하면 운영 체제가 로드된 후 Kaspersky Endpoint Security가 시작되어 전체 세션 동안 컴퓨터를 보호합니다. 이 옵션이 선택되면 운영 체제가 로드된 후 사용자가 수동으로 시작할 때까지 Kaspersky Endpoint Security가 시작되지 않습니다. 컴퓨터 보호는 중단되며, 사용자 데이터는 위협에 노출 될 수 있습니다.
고급 치료 기술 사용(상당한 컴퓨터 리소스 필요)	일반적으로 Kaspersky Endpoint Security는 컴퓨터가 감염되기 전에 탐지된 악성 코드를 종료합니다. 고급 치료 기술이 이미 활성화된 악성 코드(활성 감염)로부터 컴퓨터를 보호하여 데이터 손실 및 위협 확산의 위험을 최소화합니다. 이 기술을 활성화하면 악성 활동 탐지 시 Kaspersky Endpoint Security 팝업 알림을 표시합니다. 이 알림에서, Kaspersky Endpoint Security는 컴퓨터의 고급 치료를 수행할 것을 사용자에게 제안합니다. 사용자가 이 절차를 승인하면 Kaspersky Endpoint Security는 위협을 무력화한 다음 컴퓨터를 다시 시작합니다. 고급 치료 기술은 컴퓨팅 리소스를 많이 사용하므로 다른 애플리케이션의 속도가 떨어질 수 있습니다. 애플리케이션이 처리 안 된 감염을 탐지 중이라면 일부 운영 체제 기능이 제한될 수 있습니다. 고급 치료가 끝난 후 컴퓨터를 다시 시작하면 운영 체제를 다시 정상적으로 사용할 수 있습니다. Kaspersky Endpoint Security를 서버용 Windows를 사용하는 컴퓨터에 설치하면 Kaspersky Endpoint Security가 알림을 표시하지 않습니다. 따라서 사용자가 처리 안 된 보안위협 치료를 위한 동작을 선택할 수 없습니다. 보안위협을 치료하려면 애플리케이션 설정에서 고급 치료 기술을 활성화하고 *악성 코드 검사* 작업 설정에서 즉각적인 고급 치료를 활성화해야 합니다. 그다음 *악성 코드 검사* 작업을 시작해야 합니다.
활성화 시 프록시 서버로 Kaspersky Security Center 사용 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	이 확인란을 선택하면 애플리케이션은 Kaspersky Security Center 중앙 관리 서버를 활성화 서버에 연결하기 위한 프록시 서버로 사용합니다. 이는 인터넷에 연결할 수 없는 격리된 네트워크 구간에서 애플리케이션을 활성화하기 위해 활성화 코드를 사용할 때 필요합니다. 키 파일을 사용하여 애플리케이션을 활성화하는 경우, 인터넷 접속이 필요하지 않습니다.
자기 보호 사용	이 기능을 활성화하면 Kaspersky Endpoint Security가 하드 드라이브의 애플리케이션 파일, 메모리 프로세스 및 시스템 레지스트리의 항목에 대한 변경이나 삭제를 방지합니다.

파라미터	설명
애플리케이션 서비스의 외부 관리 차단	이 기능을 활성화하면 Kaspersky Endpoint Security는 타사 애플리케이션(예: CMD)을 사용한 애플리케이션 서비스 관리를 허용하지 않습니다. 타사 애플리케이션을 사용하여 애플리케이션 서비스를 관리하려는 시도가 있으면 Microsoft Windows 작업 표시줄에서 애플리케이션 아이콘 위에 알림이 표시됩니다(사용자가 알림 서비스를 해제하지 않은 경우). AM-PPL 기술을 지원하지 않는 컴퓨터 또는 AM-PPL 기술이 중지된 컴퓨터에서만 애플리케이션 서비스의 외부 관리를 허용할 수 있습니다.
배터리 전원으로 실행 중이면 스케줄된 작업 연기	이 확인란을 선택하면 컴퓨터를 배터리 전원으로 실행할 때 절전 모드가 사용됩니다. Kaspersky Endpoint Security는 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 검사* • *IOC 검사*
다른 애플리케이션에 컴퓨터 리소스 우선권 할당	사용자 컴퓨터 검사 시 Kaspersky Endpoint Security의 컴퓨터 리소스 사용으로 인해 CPU 및 하드 드라이브 서브시스템의 로드가 증가할 수 있습니다. 이렇게 되면 기타 애플리케이션의 속도가 저하될 수 있습니다. 성능을 최적화하기 위해 Kaspersky Endpoint Security는 *기타 애플리케이션으로 리소스를 전송하는 모드*를 제공합니다. 이 모드에서는 CPU 로드가 높아지면 운영 체제에서 Kaspersky Endpoint Security 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 Endpoint Security가 컴퓨터를 검사하는 시간이 길어집니다. 기본적으로 이 애플리케이션은 컴퓨터 리소스 우선권을 다른 애플리케이션에 할당하도록 구성됩니다.
검사 작업을 위한 CPU 사용량 제한	Kaspersky Endpoint Security 성능을 최적화하기 위해 *악성 코드 검사* 작업의 CPU 사용량을 제한할 수 있습니다. 이 확인란을 선택하면 컴퓨터에서 *악성 코드 검사* 작업 중 모든 CPU 코어에 대한 평균 로드가 지정된 값에 도달합니다. 기본적으로 확인란의 선택이 취소됩니다.
덤프 기록 사용	이 확인란을 선택하면 Kaspersky Endpoint Security가 충돌되었을 때 덤프를 기록합니다. 이 확인란을 선택하지 않은 경우 Kaspersky Endpoint Security는 덤프를 기록하지 않습니다. 또한, 애플리케이션은 컴퓨터 하드 드라이브에서 기존 덤프 파일을 삭제합니다.
덤프 및 추적 파일 보호 사용	이 확인란을 선택하면 시스템 관리자 및 로컬 관리자뿐 아니라 덤프 기록을 설정한 사용자에게 덤프 파일 접근이 허용됩니다. 시스템 및 로컬 관리자만 추적 파일에 접근할 수 있습니다. 확인란이 선택 해제되면 모든 사용자가 덤프 파일 및 추적 파일에 접근할 수 있습니다.
설정 적용 시 컴퓨터 상태 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	정책이나 작업 실행을 적용하는 중에 오류가 발생할 때 웹 콘솔에서 Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터의 상태를 표시하는 설정입니다. *정상*, *경고*, *심각* 상태를 이용할 수 있습니다.
컴퓨터 재시작 없이 업데이트 설치	컴퓨터를 다시 시작하지 않고 애플리케이션을 업그레이드하면 서버를 중단 없이 사용할 수 있습니다. 11.10.0 버전부터 다시 시작 없이 애플리케이션을 업그레이드할 수 있습니다. 이전 버전의 애플리케이션을 업그레이드하려면, 컴퓨터를 다시 시작해야 합니다. 11.11.0 버전부터 컴퓨터를 다시 시작하지 않고 다음 작업을 수행할 수 있습니다. • 패치 설치 • 애플리케이션 구성 요소 집합 변경 • Kaspersky Security for Windows Server를 통해 Kaspersky Endpoint Security 설치 매개변수의 기본값은 운영 체제 유형에 따라 다릅니다. 애플리케이션을 워크스테이션에 설치했다면 다시 시작 없이 애플리케이션을 업그레이드할 수 없습니다. 애플리케이션을 서버에 설치했다면 다시 시작 없이 애플리케이션을 업그레이드할 수 있습니다.

파라미터	설명
원격 관리 소프트웨어와의 호환성 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	RAT(원격 관리 도구)와 Kaspersky Endpoint Security를 함께 사용하면 문제가 발생했을 때 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 Endpoint Security가 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 Endpoint Security가 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.

리포트 및 저장소

리포트

리포트에는 각 Kaspersky Endpoint Security 구성 요소의 작업, 데이터 암호화 이벤트, 각 검사 작업/업데이트 작업/무결성 검사 작업의 성능, 그리고 애플리케이션의 전반적인 작업에 대한 정보가 기록됩니다.

리포트는 `C:\ProgramData\Kaspersky Lab\KES.14.0\Report` 폴더에 저장됩니다.

백업

*백업*은 치료하는 동안 삭제되거나 수정된 파일의 백업 복사본을 보존합니다. *백업 복사본*은 파일을 치료 또는 삭제하기 전에 생성되는 파일 복사본입니다. 파일의 백업 복사본은 특별한 형식으로 저장되며 위험하지 않습니다.

파일의 백업 복사본은 `C:\ProgramData\Kaspersky Lab\KES.14.0\QB` 폴더에 저장됩니다.

관리자 그룹 내 사용자는 이 폴더에 대한 접근 권한이 부여됩니다. Kaspersky Endpoint Security를 설치할 때 사용된 계정의 사용자는 이 폴더에 대한 제한된 접근 권한이 부여됩니다.

Kaspersky Endpoint Security는 파일의 백업 복사본에 대한 사용자 접근 권한을 구성하는 기능을 제공하지 않습니다.

격리 저장소

*격리 저장소*는 컴퓨터의 특수 로컬 저장소입니다. 컴퓨터에 위험하다고 판단되는 파일을 격리할 수 있습니다. 격리된 파일은 암호화된 상태로 저장되며 장치 보안에 위협이 되지 않습니다. Kaspersky Endpoint Security는 Kaspersky Detection and Response 솔루션과 통합했을 때만 격리 저장소를 사용합니다. 그 외에는 Kaspersky Endpoint Security가 관련 파일을 백업에 저장합니다. 솔루션에 포함된 격리 저장소 관리 방법에 대한 자세한 내용은 Kaspersky Sandbox 도움말, Kaspersky Endpoint Detection and Response Optimum 도움말, Kaspersky Endpoint Detection and Response Expert 도움말, Kaspersky Anti Targeted Attack Platform 도움말 및 Kaspersky Endpoint Detection and Response Expert(on-premise) 도움말을 참조하십시오.

격리 저장소는 웹 콘솔을 통해서만 구성할 수 있습니다. 웹 콘솔을 사용하여 격리된 개체를 관리할 수도 있습니다(복원, 삭제, 추가 등). 명령줄을 사용하면 컴퓨터에서 로컬로 개체를 복원할 수 있습니다.

Kaspersky Endpoint Security는 시스템 계정(SYSTEM)을 사용하여 파일을 격리합니다.

리포트 및 저장소 설정

파라미터	설명
보고서 삭제 대기 시간(일)	이 확인란을 선택하면 최대 리포트 저장 기간이 정의한 시간 간격으로 제한됩니다. 리포트 최대 저장 기간의 기본값은 30일입니다. 이 기간이 지나면 Kaspersky Endpoint Security가 리포트 파일에서 가장 오래된 항목을 자동으로 삭제합니다.
보고서 파일 크기 제한(MB)	이 확인란을 선택하면 최대 리포트 파일 크기가 정의된 값으로 제한됩니다. 최대 파일 크기의 기본값은 1024MB입니다. Kaspersky Endpoint Security는 리포트 파일 크기가 최대 한도에 도달하면 리포트 파일에서 가장 오래된 항목을 자동으로 삭제하여 최대 한도를 넘지 않도록 관리합니다.
개체 삭제 대기 시간(일)	이 확인란을 선택하면 최대 파일 저장 기간이 정의한 시간 간격으로 제한됩니다. 파일 최대 저장 기간의 기본값은 30일입니다. 최대 저장 기간이 만료되면 Kaspersky Endpoint Security가 백업 저장소에서 가장 오래된 파일을 삭제합니다.
백업 크기를 다음으로 제한(MB)	이 확인란을 선택하면 최대 저장소 크기가 정의된 값으로 제한됩니다. 최대 크기 기본값은 1024MB입니다 Kaspersky Endpoint Security는 저장소 크기가 최대 한도에 도달하면 저장소에서 가장 오래된 파일을 자동으로 삭제하여 최대 저장소 크기를 넘지 않도록 관리합니다.
격리 저장소 크기 제한	이 확인란을 선택하면 최대 격리 저장소 크기가 정의된 값으로 제한됩니다. 최대 크기 기본값은 1024MB입니다 격리 저장소가 최대 크기에 도달하면 Kaspersky Endpoint Security는 *격리 저장소 공간 부족* 이벤트를 Kaspersky Security Center로 전송하고 Windows 이벤트 로그에 게시합니다. 그동안 애플리케이션은 새 개체를 격리하지 않습니다. 격리 저장소를 직접 비워야 합니다.
저장소 공간이 (%)에 도달하면 알림	격리 저장소의 한계값입니다. 예를 들면 검역 한계값을 50%로 설정할 수 있습니다. 격리 저장소가 한계값에 도달하면 Kaspersky Endpoint Security는 해당 이벤트를 Kaspersky Security Center로 보내고 Windows 이벤트 로그에 이벤트를 게시합니다. 그동안에도 애플리케이션은 계속해서 새 개체를 격리합니다.
중앙 관리 서버로의 데이터 전송 *(Kaspersky Security Center에서만 사용 가능)*	중앙 관리 서버로 정보가 전송되어야 하는 클라이언트 컴퓨터의 이벤트 카테고리입니다. 일부 데이터 전송을 비활성화하여 중앙 관리 서버의 디스크 공간을 최적화할 수 있습니다. 애플리케이션은 다음 카테고리의 이벤트를 보냅니다: • **격리 저장소 파일 정보** Kaspersky Security Center 콘솔의 **고급 → 저장소 → 격리** 폴더에서 격리된 파일 목록을 볼 수 있습니다. Kaspersky Endpoint Security는 Kaspersky Detection and Response 솔루션과 통합했을 때만 격리 저장소를 사용합니다. • **백업된 파일 정보**. **고급 → 저장소 → 백업** 폴더에서 Kaspersky Security Center 콘솔의 백업 파일 목록을 볼 수 있습니다. • **처리 안 된 파일 정보**. Kaspersky Security Center 콘솔의 **고급 → 저장소 → 처리 안 된 위협** 폴더에서 처리 안 된 파일 목록을 볼 수 있습니다. • **설치된 장치 정보**. Kaspersky Security Center 콘솔의 **고급 → 저장소 → 하드웨어** 폴더에서 연결된 장치 목록을 볼 수 있습니다. 장치 목록은 컴퓨터 속성 및 Kaspersky Endpoint Security for Windows 정책(**장치 제어** 섹션)에서도 볼 수 있습니다. • **시작된 애플리케이션 정보**. Kaspersky Security Center 콘솔의 **고급 → 애플리케이션 관리 → 실행 파일** 폴더에서 실행 파일 목록을 볼 수 있습니다. 실행 파일 목록은 컴퓨터 속성에서도 확인할 수 있습니다. • **파일 암호화 오류 정보**. Kaspersky Security Center 콘솔의 **고급 → 데이터 암호화 및 보호 → 암호화 이벤트** 폴더에서 파일 암호화 오류 목록을 볼 수 있습니다. 오류 목록은 컴퓨터 속성에서도 확인할 수 있습니다. • **적응형 이상 행위 제어 규칙 상태 리포트**. **리포트** 탭에 있는 **중앙 관리 서버** 노드의 Kaspersky Security Center 콘솔에서 리포트를 볼 수 있습니다. 이 리포트는 Kaspersky Endpoint Security for Windows 정책 속성(**적응형 이상 행위 제어** 섹션)에서도 이용할 수 있습니다. • **트리거된 적응형 이상 행위 제어 규칙 리포트**. **리포트** 탭에 있는 **중앙 관리 서버** 노드의 Kaspersky Security Center 콘솔에서 리포트를 볼 수 있습니다. 이 리포트는 Kaspersky Endpoint Security for Windows 정책 속성(**적응형 이상 행위 제어** 섹션)에서도 이용할 수 있습니다. • **위협 개발 체인 정보 모니터링 → 경고** 섹션에서 Kaspersky Security Center 웹 콘솔의 탐지 세부 정보를 볼 수 있습니다. Kaspersky Endpoint Detection and Response 솔루션은 위협 개발 체인 관련 정보를 사용합니다.

네트워크 설정

인터넷에 연결하고 안티 바이러스 데이터베이스를 업데이트하는 데 사용되는 프록시 서버를 구성하고, 네트워크 포트 모니터링 모드를 선택하고, 암호화된 연결 검사를 구성할 수 있습니다.

네트워크 옵션

파라미터	설명
데이터 통신 연결에서 트래픽 제한	이 확인란을 선택하면 인터넷 연결에 제한이 있을 경우 애플리케이션이 사용하는 자체 네트워크 트래픽을 제한합니다. Kaspersky Endpoint Security는 고속 모바일 인터넷 연결을 제한된 연결로, Wi-Fi 연결을 무제한 연결로 식별합니다. 비용 인식 네트워킹은 Windows 8 이상을 사용하는 컴퓨터에서 작동합니다.
웹 페이지와의 상호작용을 위해 웹 트래픽에 스크립트 삽입	이 확인란을 선택하면, Kaspersky Endpoint Security가 웹 트래픽에 웹 페이지 상호작용 스크립트를 삽입합니다. 이 스크립트는 웹 제어 구성 요소가 올바르게 작동하도록 합니다. 이 스크립트를 사용하면 웹 제어 이벤트를 등록할 수 있습니다. 이 스크립트가 없으면 사용자 인터넷 활동 감시를 사용할 수 없습니다. Kaspersky 전문가는 웹 제어의 올바른 작동을 보장하기 위해 이 웹 페이지 상호 작용 스크립트를 트래픽에 삽입할 것을 권장합니다.
프록시 서버 설정	클라이언트 컴퓨터 사용자가 인터넷에 접근하는 데 사용되는 프록시 서버의 설정입니다. Kaspersky Endpoint Security는 이러한 설정을 특정 보호 구성 요소에 사용하며, 데이터베이스 및 애플리케이션 모듈 업데이트에도 사용합니다. Kaspersky Endpoint Security는 프록시 서버 자동 구성을 위해 WPAD 프로토콜(Web Proxy Auto-Discovery 프로토콜)을 사용합니다. 이 프로토콜로 프록시 서버의 IP 주소를 확인할 수 없다면 애플리케이션은 Microsoft Internet Explorer 브라우저 설정에서 지정한 프록시 서버 주소를 사용합니다.
로컬 주소에 대해 프록시 서버 우회	이 확인란을 선택한 경우 Kaspersky Endpoint Security는 공유 폴더에서 업데이트를 수행할 때 프록시 서버를 사용하지 않습니다.
프록시 서버 인증 설정	인터넷 접근을 위해 프록시 서버에서 애플리케이션을 인증하려면 사용자의 자격 증명을 입력해야 합니다. Kaspersky Endpoint Security는 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. **자동 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, Kaspersky Endpoint Security는 프록시 서버 설정에 따라 Kerberos 또는 NTLM 프로토콜을 사용하여 인증을 수행합니다.
모니터링하는 포트	**모든 네트워크 포트 모니터**. 이 네트워크 포트 모니터링 모드에서는 보호 구성 요소(파일 위협 보호, 웹 위협 보호, 메일 위협 보호)가 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. **Kaspersky에서 권장하는 목록에 있는 애플리케이션의 모든 포트 모니터**. 이는 Kaspersky Endpoint Security에서 네트워크 포트를 감시하는 애플리케이션에 대한 사전 정의된 목록을 사용합니다. 예를 들어, 이 목록에는 Google Chrome, Adobe Reader, Java 및 기타 애플리케이션이 포함됩니다. **지정한 애플리케이션의 모든 포트 모니터**. 이는 Kaspersky Endpoint Security에서 네트워크 포트를 감시하는 애플리케이션 목록을 사용합니다.

파라미터	설명
암호화된 연결 검사	Kaspersky Endpoint Security가 다음 프로토콜에 따라 전송된 암호화된 네트워크 트래픽을 검사합니다: • SSL 3.0 • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 Kaspersky Endpoint Security는 다음 암호화된 연결 검사 방법을 지원합니다: • **암호화된 연결 검사 안 함**. Kaspersky Endpoint Security가 `https://`로 시작하는 주소의 웹사이트 컨텐츠에 접근하지 못합니다. • **보호 구성 요소의 요청 하에 암호화된 연결 검사**. Kaspersky Endpoint Security가 웹 위협 보호, 메일 위협 보호, 웹 제어 구성 요소의 요청을 통해서만 암호화된 트래픽을 검사합니다. • **항상 암호화된 연결 검사**. 보호 구성 요소가 중지된 상태에서도 Kaspersky Endpoint Security가 암호화된 네트워크 트래픽을 검사합니다. Kaspersky Endpoint Security는 트래픽 검사가 중지된 신뢰하는 애플리케이션에 따라 설정된 암호화된 연결을 검사하지 않습니다. Kaspersky Endpoint Security는 미리 정의된 신뢰하는 웹사이트 목록에서의 암호화된 연결을 검사하지 않습니다. 미리 정의된 신뢰하는 웹사이트 목록은 Kaspersky 전문가가 작성합니다. 이 목록은 애플리케이션의 안티 바이러스 데이터베이스로 업데이트합니다. Kaspersky Endpoint Security 인터페이스에서만 사전 정의된 신뢰하는 웹사이트 목록을 볼 수 있습니다. Kaspersky Security Center 콘솔에서는 목록을 볼 수 없습니다.
신뢰할 수 있는 루트 인증서	신뢰할 수 있는 루트 인증서 목록. Kaspersky Endpoint Security는 필요 시(새 인증 센터 배포 필요 등) 사용자 컴퓨터에 신뢰할 수 있는 루트 인증서를 설치할 수 있도록 허용합니다. 애플리케이션에서 특별한 Kaspersky Endpoint Security 인증서 스토어에 인증서를 추가할 수 있도록 허용합니다. 이때, 이 인증서는 Kaspersky Endpoint Security 애플리케이션에서만 신뢰할 수 있는 것으로 간주합니다. 다시 말해, 사용자는 브라우저에서 새 인증서가 있는 웹사이트에 액세스할 수 있습니다. 다른 애플리케이션이 해당 웹사이트에 액세스하려고 하면, 인증서 문제로 연결 오류가 발생합니다. 시스템 인증서 스토어에 추가하려면, Active Directory 그룹 정책을 사용할 수 있습니다.
신뢰할 수 없는 인증서의 도메인 방문	• **허용**. 신뢰하지 않는 인증서를 사용하는 도메인을 방문할 때 Kaspersky Endpoint Security가 네트워크 연결을 허용합니다. 브라우저에서 신뢰하지 않는 인증서를 사용하는 도메인을 열 때 Kaspersky Endpoint Security는 경고 및 해당 도메인을 방문하지 않는 것이 좋은 이유를 보여 주는 HTML 페이지를 표시합니다. 사용자는 HTML 경고 페이지의 링크를 눌러 요청한 웹사이트에 접근할 수 있습니다. 타사 애플리케이션 또는 서비스가 신뢰할 수 없는 인증서를 사용하는 도메인과 연결을 구성하면 Kaspersky Endpoint Security는 트래픽 검사를 위해 자체 인증서를 생성합니다. 새 인증서는 *신뢰하지 않음* 상태입니다. 이는 신뢰할 수 없는 연결에 대해 타사 애플리케이션에 경고하는 데 필요한데, 이 경우 HTML 페이지를 표시할 수 없고 백그라운드 모드에서 연결을 설정할 수 있기 때문입니다. • **차단**. 이 옵션을 선택하면 신뢰하지 않는 인증서를 사용하는 도메인 방문 시 Kaspersky Endpoint Security가 네트워크 연결을 차단합니다. 브라우저에서 신뢰하지 않는 인증서를 사용하는 도메인을 열 때 Kaspersky Endpoint Security는 해당 도메인이 차단된 이유를 보여 주는 HTML 페이지를 표시합니다.
암호화된 연결 검사 오류가 있는 도메인 방문	• **차단**. 이 항목을 선택하면 암호화된 연결 검사 오류 발생 시 Kaspersky Endpoint Security가 네트워크 연결을 차단합니다. • **예외 규칙에 도메인 허용 및 추가**. 이 항목을 선택하면 암호화된 연결 검사 오류 발생 시 Kaspersky Endpoint Security가 오류 발생 도메인을 검사 오류가 있는 도메인 목록에 추가하고 이 도메인을 방문할 때 암호화된 네트워크 트래픽을 감시하지 않습니다. 애플리케이션의 로컬 인터페이스에서만 암호화된 연결 검사 오류가 있는 도메인 목록을 볼 수 있습니다. 목록 내용을 지우려면 **차단**을 선택해야 합니다. Kaspersky Endpoint Security는 암호화된 연결 검사 오류에 대한 이벤트도 생성합니다.
SSL 2.0 연결 차단	이 확인란을 선택하면 애플리케이션이 SSL 2.0 프로토콜을 통해 설정된 네트워크 연결을 모니터링 및 차단합니다. 이 확인란을 선택 해제하면 애플리케이션이 SSL 2.0 프로토콜을 통해 설정된 네트워크 연결을 차단하지 않습니다. 그러나 애플리케이션은 이 프로토콜을 통한 네트워크 트래픽을 모니터링하지 않습니다.
SSL 3.0 연결 차단	이 확인란을 선택하면 애플리케이션이 SSL 3.0 프로토콜을 통해 설정된 네트워크 연결을 차단합니다. 이 확인란을 선택 해제하면 애플리케이션이 SSL 3.0 프로토콜을 통해 설정된 네트워크 연결을 차단하지 않습니다. 애플리케이션이 이 프로토콜을 통한 네트워크 트래픽을 모니터링합니다. 애플리케이션의 모든 구성 요소가 제한 없이 작동합니다.
TLS 1.0 연결 차단	이 확인란을 선택하면 애플리케이션이 TLS 1.0 프로토콜을 통해 설정된 네트워크 연결을 차단합니다. 이 확인란을 선택 해제하면 애플리케이션이 TLS 1.0 프로토콜을 통해 설정된 네트워크 연결을 차단하지 않습니다. 애플리케이션이 이 프로토콜을 통한 네트워크 트래픽을 모니터링합니다. 애플리케이션의 모든 구성 요소가 제한 없이 작동합니다.
EV 인증서를 사용하는 웹사이트와의 암호화된 연결 복호화	EV 인증서(Extended Validation Certificate)는 웹사이트의 신뢰성을 확인하고 연결 보안을 강화합니다. 브라우저는 주소 표시줄의 잠금 아이콘을 사용하여 웹사이트에 EV 인증서가 있음을 나타냅니다. 또한 브라우저가 주소 표시줄을 전부 또는 그 일부를 녹색으로 표시할 수도 있습니다. 이 확인란을 선택하면 애플리케이션이 EV 인증서를 사용하는 웹사이트에 대한 암호화된 연결을 복호화하고 모니터링하게 됩니다. 이 확인란을 선택 해제하면 애플리케이션이 HTTPS 트래픽 컨텐츠에 접근할 수 없게 됩니다. 이 경우 애플리케이션은 `https://bing.com`과 같은 웹사이트 주소를 기반으로만 HTTPS 트래픽을 모니터링합니다. EV 인증서로 웹사이트를 처음 열면, 이 확인란의 선택 여부와 상관없이 암호화된 연결이 복호화됩니다.

파라미터	설명
신뢰하는 주소 구성	이는 Kaspersky Endpoint Security가 네트워크 연결을 검사하지 않는 웹 주소의 목록을 사용합니다. 이때, Kaspersky Endpoint Security는 웹 위협 보호, 메일 위협 보호, 웹 제어 구성 요소가 작업을 수행할 때 신뢰하는 웹 주소의 HTTPS 트래픽을 검사하지 않습니다. 도메인 이름 또는 IP 주소를 입력할 수 있습니다. Kaspersky Endpoint Security는 도메인 이름에 마스크 입력 시 `*` 문자를 지원합니다. Kaspersky Endpoint Security는 IP 주소에 대해 `*` 기호를 지원하지 않습니다. 서브넷 마스크를 사용하여 IP 주소 범위를 선택할 수 있습니다(예: 198.51.100.0/24). 예: • `domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. 이 레코드는 하위 도메인을 제외합니다(예: `subdomain.domain.com`). • `subdomain.domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. 이 레코드는 `domain.com` 도메인을 제외합니다. • `*.domain.com` – 이 레코드는 다음 주소를 포함합니다: `https://movies.domain.com`, `https://images.domain.com/page123`. 이 레코드는 `domain.com` 도메인을 제외합니다.
신뢰하는 애플리케이션 구성	Kaspersky Endpoint Security가 동작 중에 해당 활동을 감시하지 않는 애플리케이션의 목록입니다. Kaspersky Endpoint Security가 모니터링하지 않을 애플리케이션 활동 유형을 선택할 수 있습니다(예: 네트워크 트래픽 검사 안 함). Kaspersky Endpoint Security는 마스크를 입력할 때 환경 변수와 `*` 및 `?` 문자를 지원합니다.
자체 인증서 저장소가 있는 애플리케이션에서 암호화된 연결을 검사하려면 다음을 사용합니다 *(Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	이 확인란을 선택하면 애플리케이션이 Mozilla Firefox 브라우저 및 Thunderbird 메일 클라이언트에서 암호화된 트래픽을 검사합니다. HTTPS 프로토콜을 통한 일부 웹사이트로의 접근이 차단될 수 있습니다. Mozilla Firefox 브라우저와 Thunderbird 메일 클라이언트의 트래픽을 검사하려면 암호화된 연결 검사를 활성화해야 합니다. 암호화된 연결 검사를 비활성화하면 애플리케이션이 Mozilla Firefox 브라우저 및 Thunderbird 메일 클라이언트에서 트래픽을 검사하지 않습니다. 애플리케이션이 Kaspersky 루트 인증서를 사용하여 암호화된 트래픽을 복호화하고 분석합니다. Kaspersky 루트 인증서를 포함할 인증서 저장소를 선택할 수 있습니다. • **Windows 인증서 저장소(권장)**. Kaspersky Endpoint Security 설치 중 이 저장소에 Kaspersky 루트 인증서가 추가됩니다. • **자체 인증서 저장소**. Mozilla Firefox 및 Thunderbird는 자체 인증서 저장소를 사용합니다. Mozilla 인증서 저장소를 선택했다면 브라우저 속성을 통해 이 저장소에 Kaspersky 루트 인증서를 직접 추가해야 합니다.

인터페이스

애플리케이션 인터페이스 설정을 구성할 수 있습니다.

인터페이스 설정

파라미터	설명
사용자와 상호 작용 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	**간략한 인터페이스 표시**. 클라이언트 컴퓨터에서 메인 애플리케이션 창에 접근할 수 없으며 Windows 알림 영역의 아이콘만 사용할 수 있습니다. 아이콘의 마우스 오른쪽 메뉴에서 사용자는 Kaspersky Endpoint Security로 제한된 수의 작업을 수행할 수 있습니다. Kaspersky Endpoint Security에서도 애플리케이션 아이콘 위에 알림을 표시합니다. **사용자 인터페이스 표시**. 클라이언트 컴퓨터에서 Kaspersky Endpoint Security의 메인 창과 Windows 알림 영역의 아이콘을 모두 사용할 수 있습니다. 아이콘의 마우스 오른쪽 메뉴에서 사용자는 Kaspersky Endpoint Security로 작업을 수행할 수 있습니다. Kaspersky Endpoint Security에서도 애플리케이션 아이콘 위에 알림을 표시합니다. **애플리케이션 활동 모니터 섹션 숨기기**. 클라이언트 컴퓨터에서는 Kaspersky Endpoint Security 메인 창에서 **애플리케이션 활동 모니터** 버튼을 사용할 수 없습니다. *애플리케이션 활동 모니터*는 사용자의 컴퓨터에서 애플리케이션 동작에 대한 정보를 실시간으로 확인하기 위해 개발된 도구입니다. **사용자 인터페이스 표시 안 함**. 클라이언트 컴퓨터에 Kaspersky Endpoint Security 동작의 어떤 징후도 표시되지 않습니다. Windows 알림 영역의 아이콘과 알림을 사용할 수 없습니다.
알림 구성	작업이나 구성 요소가 실행되는 동안 발생할 수 있는 여러 중요도 레벨의 이벤트에 대한 알림 설정이 포함된 표입니다. Kaspersky Endpoint Security는 이러한 이벤트에 대한 알림을 화면에 표시하거나 알림을 이메일로 전송하거나 기록합니다.

파라미터	설명
이메일 알림 구성	애플리케이션 동작 시 등록된 이벤트에 대한 알림 전송을 위한 SMTP 서버 설정입니다. 기본적으로 Kaspersky Endpoint Security는 Kaspersky Security Center의 이메일 알림 설정을 사용합니다. 이메일 알림 설정에 대한 상세 정보는 Kaspersky Security Center 도움말 을 참조하십시오. 개별 이메일 알림을 구성해야 하는 경우 다음 설정을 편집할 수 있습니다. • **보낸 사람 이메일**. 발신자의 이메일 주소. 존재하지 않는 주소는 사용하지 않는 것이 좋습니다. • **SMTP 서버**. 조직의 이메일 서버 주소 하나 이상(예: `mail.company.com`). IP 주소(IPv4 또는 IPv6)를 입력할 수 있습니다. SMTP 서버에서 사용자를 인증하려면 해당 필드에 발신자 자격 증명을 입력합니다. 이메일 알림을 테스트하기 위해 테스트 메시지를 보낼 수 있습니다. • **받는 사람 이메일**. 애플리케이션이 알림을 보낼 수신자의 이메일 주소. • **전송 모드**. 이메일 알림 전송 모드. Kaspersky Endpoint Security는 이벤트 발생 즉시 메시지를 보낼 수 있으며, 사전에 구성된 스케줄을 따를 수도 있습니다.
알림 영역에 애플리케이션 상태 표시	Microsoft Windows 작업 표시줄 알림 영역에서 Kaspersky Endpoint Security 아이콘(또는)이 변경되도록 하고 팝업 알림을 표시하는 애플리케이션 이벤트 카테고리.
로컬 안티 멀웨어 데이터베이스 상태 알림	애플리케이션이 사용하는 오래된 안티 바이러스 데이터베이스 관련 알림의 설정입니다.
암호 보호	이 토글 버튼을 켜면 사용자가 암호 보호 범위 내의 작업을 시도할 때 Kaspersky Endpoint Security가 사용자에게 암호 입력을 요구합니다. 암호 보호 범위에는 금지된 작업(예: 보호 구성 요소 중지)과 암호 보호 범위가 적용된 사용자 계정이 포함됩니다. 암호 보호가 활성화되면 Kaspersky Endpoint Security는 KLAdmin 계정의 암호를 설정하라는 메시지를 표시합니다.
사용자 지원 / 웹 리소스 링크 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	Kaspersky Endpoint Security의 기술 지원에 대한 정보가 포함된 웹사이트로 연결되는 링크의 목록입니다. 추가된 링크는 표준 링크가 아닌 Kaspersky Endpoint Security 로컬 인터페이스의 **지원** 창에 표시됩니다.
사용자 지원 / 설명 *(Kaspersky Security Center 콘솔에서만 사용 가능)*	Kaspersky Endpoint Security의 로컬 인터페이스의 **지원** 창에 표시되는 메시지입니다.

설정 관리

현재 Kaspersky Endpoint Security 설정을 파일에 저장하고 이를 사용하여 다른 컴퓨터에서 애플리케이션을 빠르게 구성할 수 있습니다. 설치 패키지와 Kaspersky Security Center를 통해 애플리케이션을 배포할 때도 구성 파일을 사용할 수 있습니다. 언제든지 기본 설정을 복원할 수 있습니다.

애플리케이션 구성 관리 설정은 Kaspersky Endpoint Security 인터페이스에서만 사용할 수 있습니다.

애플리케이션 구성 관리 설정

설정	설명
가져오기	CFG 형식 파일에서 애플리케이션 설정을 추출한 다음 적용합니다.
내보내기	현재 애플리케이션 설정을 CFG 형식 파일에 저장합니다.
복원	언제든지 Kaspersky 권장 애플리케이션 설정을 복원할 수 있습니다. 설정을 복원하면 모든 보호 구성 요소에 대해 **권장** 보안 레벨이 설정됩니다.

데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트

Kaspersky Endpoint Security의 데이터베이스 및 애플리케이션 모듈을 업데이트함으로써 컴퓨터를 최신 상태로 보호할 수 있습니다. 전 세계적으로 날마다 수많은 신종 바이러스 및 기타 형태의 악성 코드가 나타나고 있습니다. Kaspersky Endpoint Security 데이터베이스에는 위협에 대한 정보와 이를 처리하는 방법이 포함되어 있습니다. 위협을 신속하게 탐지하려면 데이터베이스 및 애플리케이션 모듈을 정기적으로 업데이트해야 합니다.

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)이 제공되지 않을 수도 있습니다.

정기적인 업데이트는 유효한 라이센스를 요구합니다. 활성화된 라이센스가 없는 경우 업데이트를 한 번만 수행할 수 있습니다.

Kaspersky 업데이트 서버에서 업데이트 패키지를 성공적으로 다운로드하려면 컴퓨터를 인터넷에 연결해야 합니다. 기본적으로 인터넷 연결 설정은 자동으로 결정됩니다. 프록시 서버를 사용할 시 프록시 서버 설정을 구성해야 합니다.

업데이트는 HTTPS 프로토콜을 통해 다운로드됩니다. HTTPS 프로토콜을 통해 업데이트를 다운로드할 수 없을 때는 HTTP 프로토콜을 통해 다운로드할 수도 있습니다.

업데이트를 수행하면 다음과 같은 개체가 다운로드되어 컴퓨터에 설치됩니다:

- Kaspersky Endpoint Security 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 Endpoint Security 데이터베이스 외에도 애플리케이션 구성 요소가 네트워크 트래픽을 가로챌 수 있도록 하는 네트워크 드라이버가 업데이트됩니다.

- 애플리케이션 모듈. Kaspersky Endpoint Security 데이터베이스 외에도 애플리케이션 모듈을 업데이트할 수 있습니다. 이 애플리케이션 모듈을 업데이트하면 Kaspersky Endpoint Security의 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 Endpoint Security 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 대한 정보는 Kaspersky Endpoint Security 리포트에 기록됩니다.

애플리케이션이 Light Agent 모드로 작동하는 경우, 애플리케이션 데이터베이스와 모듈을 업데이트할 때 특별한 고려 사항이 필요합니다.

애플리케이션 모듈 및 데이터베이스 업데이트 설정

파라미터	설명
데이터베이스 업데이트 스케줄	**자동**. 이 모드에서는 애플리케이션이 지정된 빈도에 따라 업데이트 경로에서 새 업데이트 패키지를 사용할 수 있는지 확인합니다. 업데이트 패키지의 검사 빈도는 바이러스 급증 시 늘어날 수 있고 반대의 경우 줄어들 수 있습니다. 최신 업데이트 패키지가 탐지되면 Kaspersky Endpoint Security는 이를 컴퓨터에 다운로드하여 설치합니다. **수동**. 이 업데이트 작업 실행 모드에서는 업데이트 작업을 직접 시작할 수 있습니다. **스케줄에 따라**. 이 업데이트 작업 스케줄에서는 Kaspersky Endpoint Security가 사용자가 지정한 스케줄에 따라 업데이트 작업을 실행합니다. 이 업데이트 작업 스케줄을 선택한 경우 Kaspersky Endpoint Security 업데이트 작업을 수동으로 시작할 수도 있습니다.
누락된 작업 실행	이 확인란을 선택하면, Kaspersky Endpoint Security는 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 Endpoint Security가 건너뛴 작업을 실행하지 않습니다. 대신, 현재 스케줄에 따라 다음 작업을 실행합니다.
업데이트 경로	*업데이트 경로*는 Kaspersky Endpoint Security의 데이터베이스 및 애플리케이션 모듈 업데이트가 포함된 리소스입니다. 업데이트 경로에는 Kaspersky Security Center 서버, Kaspersky 업데이트 서버, 네트워크 또는 로컬 폴더가 있습니다. Kaspersky 업데이트 서버를 사용할 수 없는 경우 Kaspersky Endpoint Security는 대체 도메인을 사용하여 데이터베이스 및 애플리케이션 소프트웨어 모듈을 업데이트할 수 있습니다. 자세한 내용은 기술 지원 기술 자료 웹사이트를 참조하십시오. 기본 업데이트 경로 목록에는 Kaspersky Security Center 및 Kaspersky 업데이트 서버가 포함되어 있습니다. 다른 업데이트 경로를 목록에 추가할 수도 있습니다. 업데이트 경로는 HTTP/FTP 서버 및 공유 폴더가 될 수 있습니다. Kaspersky Endpoint Security Kaspersky의 업데이트 서버를 제외한 HTTPS 서버에서의 업데이트를 지원하지 않습니다. 여러 리소스를 업데이트 경로로 선택한 경우 Kaspersky Endpoint Security는 목록 위부터 아래 순서로 하나씩 연결해 보고 가장 먼저 가능한 경로에서 업데이트 패키지를 가져와서 업데이트 작업을 수행합니다. 기본적으로 Kaspersky Endpoint Security는 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 Kaspersky 서버는 *데이터베이스 및 애플리케이션 모듈 업데이트* 설정에서 첫 번째 업데이트 경로로 선택됩니다. 애플리케이션이 Light Agent 모드로 실행중인 경우, SVM의 폴더가 업데이트 경로로 선택됩니다.
다음으로 데이터베이스 업데이트 실행	기본적으로 Kaspersky Endpoint Security 업데이트 작업은 운영 체제에 로그인하는 데 사용했던 계정의 사용자 권한으로 시작됩니다. 그러나 Kaspersky Endpoint Security는 필요한 권한이 없어 접근할 수 없는 업데이트 경로(예: 업데이트 패키지가 포함된 공유 폴더) 또는 인증된 프록시 서버 인증이 구성되지 않은 업데이트 경로에서도 업데이트할 수 있습니다. 애플리케이션 설정에서 그러한 권한을 가진 사용자를 지정하여 해당 사용자 계정으로 Kaspersky Endpoint Security 업데이트 작업을 시작할 수 있습니다.

파라미터	설명
애플리케이션 모듈 업데이트 다운로드	애플리케이션 데이터베이스 업데이트를 통해 애플리케이션 모듈 업데이트를 다운로드합니다. 확인란이 선택되어 있다면, Kaspersky Endpoint Security는 애플리케이션 모듈 업데이트가 있을 경우 이를 사용자에게 알리고 업데이트 작업을 실행할 때 업데이트 패키지 안에 애플리케이션 모듈 업데이트를 포함합니다. 애플리케이션 모듈 업데이트를 적용하는 방법은 다음 설정에서 이뤄집니다: • **긴급 및 승인된 업데이트 설치**. 이 옵션이 선택되면, 애플리케이션 모듈 업데이트가 있을 때 Kaspersky Endpoint Security는 자동으로 중요 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 Endpoint Security는 애플리케이션 모듈은 해당 설치를 애플리케이션 인터페이스 또는 Kaspersky Security Center 측 로컬에서 승인한 이후에만 설치합니다. 이 옵션은 기본적으로 선택되어 있습니다. 확인란이 선택 해제되어 있다면, Kaspersky Endpoint Security는 애플리케이션 모듈 업데이트가 있을 경우에도 이를 사용자에게 알리지 않으며 업데이트 작업을 실행할 때 업데이트 패키지 안에 애플리케이션 모듈 업데이트를 포함하지 않습니다. 애플리케이션 모듈 업데이트를 검토하고 최종 사용자 라이센스 계약서 조항을 승인하면, 애플리케이션은 최종 사용자 라이센스 계약서가 사용자에 의해 수락된 후 업데이트를 설치합니다. 기본적으로 확인란이 선택되어 있습니다.
폴더로 업데이트 파일 복사	이 확인란을 선택하면 Kaspersky Endpoint Security가 확인란 아래에 지정된 공유 폴더에 업데이트 패키지를 복사합니다. 그러면 LAN에 연결된 다른 컴퓨터가 이 공유 폴더에서 업데이트 패키지를 가져올 수 있습니다. 이렇게 하면 업데이트 패키지가 한 번만 다운로드되므로 네트워크 트래픽이 줄어듭니다. 다음 폴더가 기본적으로 지정됩니다: `C:\ProgramData\Kaspersky Lab\KES.14.0\Update distribution\`.
업데이트용 프록시 서버 *(Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	애플리케이션 모듈 및 데이터베이스를 업데이트하기 위한 클라이언트 컴퓨터 사용자의 인터넷 접근 프록시 서버 설정. Kaspersky Endpoint Security는 프록시 서버 자동 구성을 위해 WPAD 프로토콜(Web Proxy Auto-Discovery Protocol)을 사용합니다. 이 프로토콜로 프록시 서버의 IP 주소를 확인할 수 없는 경우 Kaspersky Endpoint Security는 Microsoft Internet Explorer 브라우저 설정에 지정되어 있는 프록시 서버 주소를 사용합니다.
로컬 주소에 대해 프록시 서버 우회 *(Kaspersky Endpoint Security 인터페이스에서만 사용 가능)*	이 확인란을 선택한 경우 Kaspersky Endpoint Security는 공유 폴더에서 업데이트를 수행할 때 프록시 서버를 사용하지 않습니다.

부록 2. 애플리케이션 제어 그룹

Kaspersky Endpoint Security는 컴퓨터에서 시작된 모든 애플리케이션을 신뢰 그룹으로 분류합니다. 애플리케이션은 운영 체제에 미치는 위험도에 따라 네 가지 신뢰 그룹으로 분류됩니다.

제어 그룹은 다음과 같습니다:

- **신뢰함**. 이 그룹에는 다음 조건을 하나 이상 충족하는 애플리케이션이 포함됩니다:
  - 신뢰하는 공급업체가 디지털로 서명한 애플리케이션.
  - Kaspersky Security Network의 신뢰하는 애플리케이션 데이터베이스에 등록된 애플리케이션.
  - 사용자가 *신뢰하는* 그룹에 애플리케이션을 추가했습니다.

  이러한 애플리케이션에는 모든 작업이 허용됩니다.

- **낮은 제한**. 이 그룹에는 다음 조건을 충족하는 애플리케이션이 포함됩니다:
  - 신뢰하는 공급업체가 디지털로 서명하지 않은 애플리케이션.
  - Kaspersky Security Network의 신뢰하는 애플리케이션 데이터베이스에 등록되지 않은 애플리케이션.
  - 사용자가 *낮은 제한* 그룹에 지정한 애플리케이션.

  이러한 애플리케이션은 운영 체제 리소스 접근 시 최소한의 제한을 받게 됩니다.
- **높은 제한**. 이 그룹에는 다음 조건을 충족하는 애플리케이션이 포함됩니다:
  - 신뢰하는 공급업체가 디지털로 서명하지 않은 애플리케이션.
  - Kaspersky Security Network의 신뢰하는 애플리케이션 데이터베이스에 등록되지 않은 애플리케이션.
  - 사용자가 *높은 제한* 그룹에 지정한 애플리케이션.

  이러한 애플리케이션은 운영 체제 리소스 접근 시 높은 제한을 받게 됩니다.
- **신뢰하지 않음**. 이 그룹에는 다음 조건을 충족하는 애플리케이션이 포함됩니다:
  - 신뢰하는 공급업체가 디지털로 서명하지 않은 애플리케이션.
  - Kaspersky Security Network의 신뢰하는 애플리케이션 데이터베이스에 등록되지 않은 애플리케이션.
  - 사용자가 *신뢰하지 않는* 그룹에 애플리케이션을 추가했습니다.

  이러한 애플리케이션은 모든 동작이 차단됩니다.

부록 3. 빠른 이동식 드라이브 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

부록 4. 메일 위협 보호 첨부파일 필터의 파일 유형

파일의 실제 형식이 파일 이름 확장자와 일치하지 않을 수 있습니다.

이메일 첨부파일의 필터링을 설정한 경우 메일 위협 보호가 다음과 같은 확장자가 포함된 파일 이름을 바꾸거나 파일을 삭제할 수 있습니다:

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

부록 5. 외부 서비스와의 상호 작용을 위한 네트워크 설정

Kaspersky Endpoint Security 및 Kaspersky Security Center는 Kaspersky의 외부 서비스와 작업하기 위해 TLS(Transport Layer Security)로 암호화된 통신 채널을 사용합니다.

Kaspersky Endpoint Security는 외부 서비스와 상호 작용하기 위해 다음 네트워크 설정을 사용합니다.

네트워크 설정

주소	설명
`activation-v2.kaspersky.com/activationservice/activationservice.svc` 프로토콜: `HTTPS` 포트: `443`	애플리케이션 활성화.

주소	설명

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
프로토콜: `HTTPS`
포트: `443`
	데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트.

`downloads.upd.kaspersky.com` 프로토콜: `HTTPS` 포트: `443`	• 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트. • Kaspersky 서버에 대한 접근을 확인합니다. 시스템 DNS로 서버에 접근할 수 없다면 애플리케이션이 공용 DNS를 사용합니다. 이는 안티 바이러스 데이터베이스를 업데이트하고 컴퓨터의 보안 수준 유지를 위해 필요합니다. Kaspersky Endpoint Security 다음 순서에 따라 다음 공용 DNS 서버를 사용합니다. 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). 애플리케이션이 DNS 서버와 TCP/UDP 연결을 구성하므로, 애플리케이션이 보낸 요청에는 사용자의 공용 IP 주소와 도메인 주소가 포함될 수 있습니다. 이 정보는 HTTPS 사용 시 웹 리소스 인증서 확인 등에 필요합니다. Kaspersky Endpoint Security가 공용 DNS 서버 사용 시, 관련 서비스의 개인 정보 보호 정책에 따라 데이터를 처리합니다. Kaspersky Endpoint Security가 공용 DNS 서버를 사용하지 못하게 하려면, 기술 지원에 사설 패치를 문의하십시오.
`touch.kaspersky.com` 프로토콜: `HTTP`	• 인증서의 유효 기간 확인을 위한 신뢰 시간 수신(TLS 연결). • 웹 위협 보호가 실행 중일 때 브라우저의 웹 리소스에 대한 접근이 거부되었다는 경고입니다.

주소	설명
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com 프로토콜: `HTTP` 포트: `80`	데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트.
ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com 프로토콜: `HTTPS` 포트: `443`	Kaspersky Security Network 사용.
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com 프로토콜: `KSN` 포트: `443`, `1443`	Kaspersky Security Network 사용.
click.kaspersky.com redirect.kaspersky.com 프로토콜: `HTTPS` 포트: `443`	인터페이스에서 링크를 따름.

설정, 암호화에 사용

주소	설명
crl.kaspersky.com ocsp.kaspersky.com 프로토콜: `HTTP` 포트: `80`	공개 키 인프라(PKI).

부록 6. 애플리케이션 이벤트

Kaspersky Security Center 이벤트 로그와 Windows 이벤트 로그에는 각 Kaspersky Endpoint Security 구성 요소의 작업, 데이터 암호화 이벤트, 각 악성 코드 검사 작업/업데이트 작업/무결성 검사 작업의 완료, 그리고 애플리케이션의 전반적인 작업에 대한 정보가 기록됩니다.

Kaspersky Endpoint Security는 일반 이벤트 및 특정 이벤트를 생성합니다. 특정 이벤트는 Kaspersky Endpoint Security for Windows로만 생성됩니다. 특정 이벤트의 ID는 `000000cb`와 같이 단순합니다. 특정 이벤트에는 다음과 같은 필요 설정이 포함됩니다:

- `GNRL_EA_DESCRIPTION`은 이벤트의 내용입니다.
- `GNRL_EA_ID`는 이벤트의 서비스 ID입니다.
- `GNRL_EA_SEVERITY`는 이벤트의 상태입니다. `1` – *정보*, `2` – *경고*, `3` – *기능 실패*, `4` – *심각*.
- `EVENT_TYPE_DISPLAY_NAME`은 이벤트의 제목입니다.
- `TASK_DISPLAY_NAME`은 이벤트를 시작한 애플리케이션 구성 요소의 이름입니다.

일반 이벤트는 Kaspersky Endpoint Security for Windows뿐만 아니라 다른 Kaspersky 애플리케이션(Kaspersky Security for Windows Server 등)에서도 생성될 수 있습니다. 일반 이벤트의 ID는 `GNRL_EV_VIRUS_FOUND`와 같이 더 복잡합니다. 일반 이벤트에는 필요 설정 외에도 고급 설정이 포함됩니다.

이벤트가 서버에 저장되는 기간

심각

라이센스가 만료되었습니다

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	`201`
Kaspersky Security Center 이벤트 ID	`GNRL_EV_LICENSE_EXPIRATION`
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

라이센스가 거의 만료됨

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	`203`
Kaspersky Security Center 이벤트 ID	`000000cb`
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

데이터베이스가 없거나 손상되었음

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	206
Kaspersky Security Center 이벤트 ID	000000ce
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

데이터베이스가 매우 오래되었습니다

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	207
Kaspersky Security Center 이벤트 ID	000000cf
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

애플리케이션 자동 시작이 비활성화되었습니다

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	209
Kaspersky Security Center 이벤트 ID	000000d1
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

활성화 오류

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	229
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

처리 안 된 보안 위협 탐지됨. 고급 치료 시작 필요

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	231
Kaspersky Security Center 이벤트 ID	000000e7
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

KSN 서버 이용 불가능

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	2023
Kaspersky Security Center 이벤트 ID	000007e7
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

격리 저장소에 공간이 부족합니다

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	343
Kaspersky Security Center 이벤트 ID	00000157
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 격리 저장소에서 복원되지 않음

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	346
Kaspersky Security Center 이벤트 ID	0000015a
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 격리 저장소에서 삭제되지 않음

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	348
Kaspersky Security Center 이벤트 ID	0000015c
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

애플리케이션이 신뢰하지 않는 인증서가 있는 웹사이트에 연결되었습니다

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	57
Kaspersky Security Center 이벤트 ID	00000039
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

암호화된 연결을 검증하는 데 실패했습니다. 도메인을 예외 목록에 추가합니다

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	60
Kaspersky Security Center 이벤트 ID	0000003c
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

악성 개체 탐지됨(로컬 기반)

상태	ⓘ
구성 요소	파일 위협 보호 웹 위협 보호 메일 위협 보호 AMSI 보호 호스트 침입 방지 행동 탐지 Anti-Cryptor 익스플로잇 방지 악성 코드 검사
Windows 이벤트 ID	302
Kaspersky Security Center 이벤트 ID	GNRL_EV_VIRUS_FOUND
이벤트 매개변수	• GNRL_EA_PARAM_1은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_2는 개체의 이름입니다. 공유 폴더에 대해 외부 암호화가 감지되면 애플리케이션이 대상 파일에 대한 경로를 표시합니다. • GNRL_EA_PARAM_5는 EICAR-Test-File과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). Kaspersky Private Security Network에서 탐지된 보안 위협(blacklist): true 또는 false. EDR 버전. EDR의 보안 위협 ID. 개체의 MD5 해시.
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

악성 개체 탐지(KSN)

상태	ⓘ
구성 요소	파일 위협 보호 웹 위협 보호 메일 위협 보호 AMSI 보호 호스트 침입 방지 행동 탐지 Anti-Cryptor 익스플로잇 방지 악성 코드 검사
Windows 이벤트 ID	302

Kaspersky Security Center 이벤트 ID	GNRL_EV_VIRUS_FOUND_BY_KSN
이벤트 매개변수	• GNRL_EA_PARAM_1은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_2는 개체의 이름입니다. • GNRL_EA_PARAM_5는 EICAR-Test-File과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). Kaspersky Private Security Network에서 탐지된 보안 위협(blacklist): true 또는 false. EDR 버전. EDR의 보안 위협 ID. 개체의 MD5 해시.
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

치료 불가

상태	ⓘ
구성 요소	파일 위협 보호 메일 위협 보호 호스트 침입 방지 행동 탐지 Anti-Cryptor 악성 코드 검사
Windows 이벤트 ID	312
Kaspersky Security Center 이벤트 ID	GNRL_EV_OBJECT_NOTCURED
이벤트 매개변수	• GNRL_EA_PARAM_1은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_2는 개체의 이름입니다. • GNRL_EA_PARAM_5는 EICAR-Test-File과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). Kaspersky Private Security Network에서 탐지된 보안 위협(blacklist): true 또는 false. EDR 버전. EDR의 보안 위협 ID. 개체의 MD5 해시.
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

삭제할 수 없음

상태	ⓘ
구성 요소	파일 위협 보호 호스트 침입 방지 행동 탐지 Anti-Cryptor 악성 코드 검사
Windows 이벤트 ID	313
Kaspersky Security Center 이벤트 ID	00000139
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

처리 오류

상태	ⓘ
구성 요소	파일 위협 보호 웹 위협 보호 메일 위협 보호 호스트 침입 방지 AMSI 보호 악성 코드 검사
Windows 이벤트 ID	317
Kaspersky Security Center 이벤트 ID	0000013d
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

프로세스 종료

상태	ⓘ
구성 요소	파일 위협 보호 호스트 침입 방지 행동 탐지 악성 코드 검사
Windows 이벤트 ID	452
Kaspersky Security Center 이벤트 ID	000001c4
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

프로세스를 종료할 수 없음

상태	ⓘ
구성 요소	파일 위협 보호 호스트 침입 방지 행동 탐지 악성 코드 검사
Windows 이벤트 ID	453
Kaspersky Security Center 이벤트 ID	000001c5
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

위험한 링크가 차단됨

상태	ⓘ
구성 요소	웹 위협 보호
Windows 이벤트 ID	362
Kaspersky Security Center 이벤트 ID	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
이벤트 매개변수	• GNRL_EA_PARAM_2는 개체의 경로입니다. • GNRL_EA_PARAM_5는 Kaspersky 분류에 따른 개체의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). KPSN에서 탐지된 보안 위협(blacklist): true 또는 false.

Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

위험한 링크가 열림

상태	!
구성 요소	웹 위협 보호
Windows 이벤트 ID	363
Kaspersky Security Center 이벤트 ID	GNRL_EV_VIRUS_FOUND_AND_REPORTED
이벤트 매개변수	• GNRL_EA_PARAM_2는 개체의 경로입니다. • GNRL_EA_PARAM_5는 Kaspersky 분류에 따른 개체의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). KPSN에서 탐지된 보안 위협(blacklist): true 또는 false.
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

이전에 열린 위험한 링크가 탐지됨

상태	!
구성 요소	웹 위협 보호
Windows 이벤트 ID	1201
Kaspersky Security Center 이벤트 ID	GNRL_EV_VIRUS_FOUND_AND_PASSED
이벤트 매개변수	• GNRL_EA_PARAM_2는 개체의 경로입니다. • GNRL_EA_PARAM_5는 Kaspersky 분류에 따른 개체의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). KPSN에서 탐지된 보안 위협(blacklist): true 또는 false.
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

프로세스 활동 차단

상태	!
구성 요소	적응형 이상 행위 제어
Windows 이벤트 ID	2200
Kaspersky Security Center 이벤트 ID	GNRL_EV_ADSEC_DETECT
이벤트 매개변수	• GNRL_EA_PARAM_1은 적응형 이상 행위 제어 규칙의 이름입니다. • GNRL_EA_PARAM_2는 휴리스틱 규칙의 ID입니다. • GNRL_EA_PARAM_3은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_4는 소스 프로세스입니다. • GNRL_EA_PARAM_5는 소스 개체입니다. • GNRL_EA_PARAM_6은 대상 프로세스입니다. • GNRL_EA_PARAM_7는 대상 개체입니다. • GNRL_EA_PARAM_8는 탐지된 개체에 대한 추가 정보입니다. 소스 프로세스 체크섬 / 개체 및 대상 프로세스 / 개체. 프로세스 차단됨(verdict_type): true 또는 false. 사용자 보안 ID(SID).

Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

승인되지 않은 키보드

상태	ⓘ
구성 요소	BadUSB 공격 방지
Windows 이벤트 ID	2051
Kaspersky Security Center 이벤트 ID	00000803
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

AMSI 요청이 차단됨

상태	ⓘ
구성 요소	AMSI 보호
Windows 이벤트 ID	2200
Kaspersky Security Center 이벤트 ID	00000898
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

네트워크 활동 차단됨

상태	ⓘ
구성 요소	방화벽
Windows 이벤트 ID	602
Kaspersky Security Center 이벤트 ID	00000329
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

네트워크 공격 탐지됨

상태	ⓘ
구성 요소	네트워크 위협 보호
Windows 이벤트 ID	651
Kaspersky Security Center 이벤트 ID	GNRL_EV_ATTACK_DETECTED
이벤트 매개변수	• GNRL_EA_PARAM_1 은 공격의 이름입니다. • GNRL_EA_PARAM_2 는 프로토콜입니다. • GNRL_EA_PARAM_3 는 네트워크 공격의 출처가 되는 컴퓨터의 IP 주소입니다. IP 주소는 호스트의 바이트 순서로 표시됩니다. 예를 들어, 172.16.0.201 는 2886729929 입니다. • GNRL_EA_PARAM_4 는 포트 번호입니다. • GNRL_EA_PARAM_5 는 12B012B012B012B012B012B012B012B0 와 같은 IPv6 주소입니다. • GNRL_EA_PARAM_6 는 네트워크 공격의 목표가 되는 컴퓨터의 IP 주소입니다. IP 주소는 호스트의 바이트 순서로 표시됩니다. 예를 들어, 172.16.0.201 는 2886729929 입니다.
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

애플리케이션 시작이 금지됨

상태	⚠
구성 요소	애플리케이션 제어
Windows 이벤트 ID	702
Kaspersky Security Center 이벤트 ID	GNRL_EV_APPLICATION_LAUNCH_DENIED
이벤트 매개변수	• GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_3 은 수동으로 생성된 카테고리 ID입니다. • GNRL_EA_PARAM_4 은 애플리케이션 카테고리 ID입니다. • GNRL_EA_PARAM_5 는 애플리케이션의 디지털 서명에 관한 정보입니다. • GNRL_EA_PARAM_6 은 애플리케이션 실행 파일의 이름입니다(예: chrome.exe). • GNRL_EA_PARAM_7 은 실행 파일의 경로입니다. • GNRL_EA_PARAM_8 은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_9 는 사용자가 실행하고자 하는 애플리케이션의 버전입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

Kaspersky Endpoint Security가 시작되기 전에 차단된 프로세스가 먼저 시작됨

상태	⚠
구성 요소	애플리케이션 제어
Windows 이벤트 ID	710
Kaspersky Security Center 이벤트 ID	000002c6
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

접근 거부됨(로컬 기반)

상태	⚠
구성 요소	웹 제어
Windows 이벤트 ID	752
Kaspersky Security Center 이벤트 ID	GNRL_EV_WEB_URL_BLOCKED
이벤트 매개변수	• GNRL_EA_PARAM_1 은 URL입니다. • GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_3 은 웹 제어 규칙의 이름입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

접근 거부됨(KSN)

상태	⚠
구성 요소	웹 제어
Windows 이벤트 ID	752
Kaspersky Security Center 이벤트 ID	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
이벤트 매개변수	• GNRL_EA_PARAM_1 은 URL입니다. • GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_3 은 웹 제어 규칙의 이름입니다.

Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

장치 사용이 차단됨

상태	!
구성 요소	장치 제어
Windows 이벤트 ID	802
Kaspersky Security Center 이벤트 ID	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
이벤트 매개변수	• GNRL_EA_PARAM_1 은 하드웨어 ID(HWID)입니다. • GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

네트워크 연결 차단됨

상태	!
구성 요소	장치 제어
Windows 이벤트 ID	809
Kaspersky Security Center 이벤트 ID	00000329
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

구성 요소 업데이트 오류

상태	!
구성 요소	업데이트
Windows 이벤트 ID	1011
Kaspersky Security Center 이벤트 ID	000003f3
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

구성 요소 업데이트 배포 오류

상태	!
구성 요소	업데이트
Windows 이벤트 ID	1012
Kaspersky Security Center 이벤트 ID	000003f4
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

로컬 업데이트 오류

상태	!
구성 요소	업데이트
Windows 이벤트 ID	1014

Kaspersky Security Center 이벤트 ID	000003f6
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

네트워크 업데이트 오류

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1015
Kaspersky Security Center 이벤트 ID	000003f7
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

두 작업을 동시에 시작할 수는 없음

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1017
Kaspersky Security Center 이벤트 ID	000003f9
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

애플리케이션 데이터베이스 및 모듈 검증 오류

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1018
Kaspersky Security Center 이벤트 ID	000003fa
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

Kaspersky Security Center와 통신 오류

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1019
Kaspersky Security Center 이벤트 ID	000003fb
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

일부 구성 요소가 업데이트되지 않았습니다

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1021

Kaspersky Security Center 이벤트 ID	000003fd
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

업데이트를 완료했지만 업데이트 배포는 실패

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1023
Kaspersky Security Center 이벤트 ID	000003ff
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

내부 작업 오류

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	101
Kaspersky Security Center 이벤트 ID	00000065
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

패치 설치 실패

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	2153
Kaspersky Security Center 이벤트 ID	00000869
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

패치 롤백 실패

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	2156
Kaspersky Security Center 이벤트 ID	0000086c
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 암호화 / 복호화 규칙 적용 오류

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	904

Kaspersky Security Center 이벤트 ID	00000388
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 암호화 / 복호화 오류

상태	⚠
구성 요소	데이터 암호화
Windows 이벤트 ID	912
Kaspersky Security Center 이벤트 ID	GNRL_EV_ENCRYPTION_ERROR
이벤트 매개변수	• GNRL_EA_PARAM_1은 파일 경로입니다. • GNRL_EA_PARAM_2는 오류 원인입니다. • GNRL_EA_PARAM_3은 장치 유형입니다.
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 접근이 차단됨

상태	⚠
구성 요소	데이터 암호화
Windows 이벤트 ID	940
Kaspersky Security Center 이벤트 ID	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
이벤트 매개변수	• GNRL_EA_PARAM_1는 대상 개체입니다. • GNRL_EA_PARAM_2은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_3은 파일에 대한 접근 권한을 획득하려는 애플리케이션 실행 파일(chrome.exe 등)의 이름입니다.
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

휴대용 모드 활성화 오류

상태	⚠
구성 요소	데이터 암호화
Windows 이벤트 ID	951
Kaspersky Security Center 이벤트 ID	000003b7
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

휴대용 모드 비활성화 오류

상태	⚠
구성 요소	데이터 암호화
Windows 이벤트 ID	953
Kaspersky Security Center 이벤트 ID	000003b9
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

암호화 패키지 생성 오류

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	931
Kaspersky Security Center 이벤트 ID	000003a3
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

장치 암호화/복호화 오류

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1305
Kaspersky Security Center 이벤트 ID	00000519
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

암호화 모듈을 로드할 수 없음

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1311
Kaspersky Security Center 이벤트 ID	0000051f
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

인증 에이전트 계정을 관리하기 위한 작업이 오류로 종료됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1340
Kaspersky Security Center 이벤트 ID	0000053c
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

정책을 적용할 수 없음

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	1312
Kaspersky Security Center 이벤트 ID	00000520
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

FDE 업그레이드 실패

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1342
Kaspersky Security Center 이벤트 ID	0000053e
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

FDE 업그레이드 롤백 실패(더 자세한 내용은 Kaspersky Endpoint Security for Windows 온라인 도움말을 참고해 주시기 바랍니다.)

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1344
Kaspersky Security Center 이벤트 ID	00000540
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Kaspersky Anti Targeted Attack Platform 서버 이용 불가

상태	ⓘ
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2100
Kaspersky Security Center 이벤트 ID	00000834
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 삭제 실패

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2252
Kaspersky Security Center 이벤트 ID	000008cc
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 격리되지 않음(Sandbox)

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2603
Kaspersky Security Center 이벤트 ID	00000a2b
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

내부 오류 발생

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2607
Kaspersky Security Center 이벤트 ID	00000a2f
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

잘못된 Sandbox 서버 인증서

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2613
Kaspersky Security Center 이벤트 ID	00000a35
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Sandbox 노드를 사용할 수 없습니다

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2614
Kaspersky Security Center 이벤트 ID	00000a36
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Sandbox에서 개체 처리 실패

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2617
Kaspersky Security Center 이벤트 ID	00000a39
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Sandbox에 대한 최대 부하가 초과되었습니다

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2618
Kaspersky Security Center 이벤트 ID	00000a3a
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

IOC 발견됨

상태	!
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2651
Kaspersky Security Center 이벤트 ID	00000a5b
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Sandbox 라이센스 확인 실패

상태	!
구성 요소	Sandbox
Windows 이벤트 ID	2620
Kaspersky Security Center 이벤트 ID	00000a3c
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

사용자가 검사 작업을 Sandbox에 제출하지 못함

상태	!
구성 요소	Sandbox
Windows 이벤트 ID	2623
Kaspersky Security Center 이벤트 ID	00000a3e
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Sandbox 작업 생성 중 오류 발생

상태	!
구성 요소	Sandbox
Windows 이벤트 ID	2621
Kaspersky Security Center 이벤트 ID	00000a3d
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 시작 차단됨

상태	!
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2553
Kaspersky Security Center 이벤트 ID	000009f9
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

프로세스 시작 차단됨

상태	ⓘ
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2551
Kaspersky Security Center 이벤트 ID	000009f7
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

스크립트 실행 차단됨

상태	ⓘ
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2559
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 격리되지 않음(Endpoint Detection and Response)

상태	ⓘ
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2556
Kaspersky Security Center 이벤트 ID	000009fc
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

프로세스 시작이 차단되지 않음

상태	ⓘ
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2561
Kaspersky Security Center 이벤트 ID	00000a01
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 차단되지 않았습니다

상태	ⓘ
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2562
Kaspersky Security Center 이벤트 ID	00000a02
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

스크립트 실행이 차단되지 않음

상태	!
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2563
Kaspersky Security Center 이벤트 ID	00000a03
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

애플리케이션 구성 요소 변경 오류

상태	!
구성 요소	시스템 감사
Windows 이벤트 ID	1401
Kaspersky Security Center 이벤트 ID	00000579
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

시스템에서 무차별 대입 공격 의심 패턴이 발견되었습니다

상태	!
구성 요소	로그 검사
Windows 이벤트 ID	2800
Kaspersky Security Center 이벤트 ID	00000af0
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Windows 이벤트 로그 남용 패턴이 발견되었습니다

상태	!
구성 요소	로그 검사
Windows 이벤트 ID	2801
Kaspersky Security Center 이벤트 ID	00000af1
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

설치된 새 서비스에서 이례적 작업이 감지되었습니다

상태	!
구성 요소	로그 검사
Windows 이벤트 ID	2802
Kaspersky Security Center 이벤트 ID	00000af2
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

명시적 자격 증명을 사용하는 이례적 로그인이 감지되었습니다

상태	!
구성 요소	로그 검사
Windows 이벤트 ID	2803
Kaspersky Security Center 이벤트 ID	00000af3
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

시스템에서 Kerberos 위조 PAC(MS14-068) 공격 의심 패턴이 발견되었습니다

상태	!
구성 요소	로그 검사
Windows 이벤트 ID	2804
Kaspersky Security Center 이벤트 ID	00000af4
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

권한이 있는 내장 관리자 그룹에서 의심스러운 변경 사항이 감지되었습니다

상태	!
구성 요소	로그 검사
Windows 이벤트 ID	2805
Kaspersky Security Center 이벤트 ID	00000af5
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

네트워크 로그인 세션 도중 이례적 활동이 감지되었습니다

상태	!
구성 요소	로그 검사
Windows 이벤트 ID	2806
Kaspersky Security Center 이벤트 ID	00000af6
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

로그 검사 규칙이 트리거되었습니다

상태	!
구성 요소	로그 검사
Windows 이벤트 ID	2807
Kaspersky Security Center 이벤트 ID	00000af7
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

비정상 이벤트가 너무 자주 발생합니다. 이벤트 집계 시작

상태	ⓘ
구성 요소	로그 검사
Windows 이벤트 ID	2808
Kaspersky Security Center 이벤트 ID	00000af8
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

집계 기간 동안의 이례적 이벤트에 관한 리포트

상태	ⓘ
구성 요소	로그 검사
Windows 이벤트 ID	2809
Kaspersky Security Center 이벤트 ID	00000af9
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 서버로의 연결 중 오류 발생

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise)
Windows 이벤트 ID	2850
Kaspersky Security Center 이벤트 ID	00000b22
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 서버의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise)
Windows 이벤트 ID	2851
Kaspersky Security Center 이벤트 ID	00000b23
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 서버에서 에이전트의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise)
Windows 이벤트 ID	2852
Kaspersky Security Center 이벤트 ID	00000b24
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 응답 서버로의 연결 중 오류 발생

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise) Endpoint Detection and Response Expert(cloud) Endpoint Detection and Response Expert(cloud)
Windows 이벤트 ID	2858
Kaspersky Security Center 이벤트 ID	00000b22
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 응답 서버의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise) Endpoint Detection and Response Expert(cloud)
Windows 이벤트 ID	2859
Kaspersky Security Center 이벤트 ID	00000b23
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 응답 서버에서 에이전트의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise) Endpoint Detection and Response Expert(cloud)
Windows 이벤트 ID	2860
Kaspersky Security Center 이벤트 ID	00000b24
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 원격 측정 수집 서버 연결 오류

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise) Endpoint Detection and Response Expert(cloud)
Windows 이벤트 ID	2854
Kaspersky Security Center 이벤트 ID	00000b22
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 원격 측정 수집 서버의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise) Endpoint Detection and Response Expert(cloud)
Windows 이벤트 ID	2855
Kaspersky Security Center 이벤트 ID	00000b23

Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 원격 측정 수집 서버에서 에이전트의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise) Endpoint Detection and Response Expert(cloud)
Windows 이벤트 ID	2856
Kaspersky Security Center 이벤트 ID	00000b24
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

NDR 서버에 연결 오류

상태	ⓘ
구성 요소	Network Detection and Response(KATA)
Windows 이벤트 ID	3080
Kaspersky Security Center 이벤트 ID	00000c08
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

NDR 서버의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	Network Detection and Response(KATA)
Windows 이벤트 ID	3081
Kaspersky Security Center 이벤트 ID	00000c09
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

NDR 서버에서 에이전트의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	Network Detection and Response(KATA)
Windows 이벤트 ID	3082
Kaspersky Security Center 이벤트 ID	00000c0a
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

장치가 신뢰할 수 없는 중앙 관리 서버에 연결되었습니다. 관리자에게 문의하십시오

상태	ⓘ
구성 요소	중앙 관리 서버 연결 보호
Windows 이벤트 ID	3301
Kaspersky Security Center 이벤트 ID	00000ce5

Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 또는 폴더 변경이 탐지됨

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2950
Kaspersky Security Center 이벤트 ID	00000b86
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

개체 변동이 너무 자주 발생합니다. 이벤트 집계 시작

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2955
Kaspersky Security Center 이벤트 ID	00000b8b
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

수집 기간 중 개체 변경 보고

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2956
Kaspersky Security Center 이벤트 ID	00000b8c
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

잘못된 개체를 포함한 모니터링 범위

상태	ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2953
Kaspersky Security Center 이벤트 ID	00000b89
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

레지스트리 변경이 탐지됨

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2951
Kaspersky Security Center 이벤트 ID	00000b87
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

장치 연결/연결 해제 감지됨

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2952
Kaspersky Security Center 이벤트 ID	00000b88
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

잘못된 개체를 포함한 모니터링 범위

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2903
Kaspersky Security Center 이벤트 ID	00000b89
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

개체를 이용해 제한된 작업을 수행하려 한 시도가 기준 횟수를 초과했습니다. 이벤트 집계 시작

상태	ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2963
Kaspersky Security Center 이벤트 ID	00000b93
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

모니터링 범위에 속하는 파일 작업이 차단되었습니다

상태	ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2959
Kaspersky Security Center 이벤트 ID	00000b8f
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

레지스트리 수정이 차단되었습니다

상태	ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2960
Kaspersky Security Center 이벤트 ID	00000b90
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

처리 오류

상태	ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2954
Kaspersky Security Center 이벤트 ID	00000b8a
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

시스템 무결성 모니터링: 보안 식별자(SID) 일치 없이 사용자 계정에 대한 규칙 트리거링 비활성화

상태	ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2964
Kaspersky Security Center 이벤트 ID	00000b94
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

애플리케이션 제어: 보안 식별자(SID) 일치 없이 사용자 계정에 대한 규칙 트리거링 비활성화

상태	ⓘ
구성 요소	애플리케이션 제어
Windows 이벤트 ID	711
Kaspersky Security Center 이벤트 ID	000002c7
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

장치 제어: 보안 식별자(SID) 일치 없이 사용자 계정에 대한 규칙 트리거링 비활성화

상태	ⓘ
구성 요소	장치 제어
Windows 이벤트 ID	810
Kaspersky Security Center 이벤트 ID	0000032a
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

웹 제어: 보안 식별자(SID) 일치 없이 사용자 계정에 대한 규칙 트리거링 비활성화

상태	ⓘ
구성 요소	웹 제어
Windows 이벤트 ID	757
Kaspersky Security Center 이벤트 ID	000002f5
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

적응형 이상 행위 제어: 보안 식별자(SID) 일치 없이 사용자 계정에 대한 규칙 트리거링 비활성화

상태	ⓘ
구성 요소	적응형 이상 행위 제어
Windows 이벤트 ID	504
Kaspersky Security Center 이벤트 ID	000001f8
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

로그 검사: 보안 식별자(SID) 일치 없이 사용자 계정에 대한 규칙 트리거링 비활성화

상태	ⓘ
구성 요소	로그 검사
Windows 이벤트 ID	2810
Kaspersky Security Center 이벤트 ID	00000afa
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

6시간 이상 통합 서버에 연결할 수 없습니다. 통합 서버 상태 및 네트워크 설정 확인

상태	ⓘ
구성 요소	Light Agent
Windows 이벤트 ID	3103
Kaspersky Security Center 이벤트 ID	00000c1f
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

SVM 이용 불가

상태	ⓘ
구성 요소	Light Agent
Windows 이벤트 ID	3151
Kaspersky Security Center 이벤트 ID	00000c4f
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

악성 개체가 탐지되었습니다. 가상 컴퓨터 템플릿에서 고급 치료를 시작해야 합니다

상태	ⓘ
구성 요소	Light Agent
Windows 이벤트 ID	3182
Kaspersky Security Center 이벤트 ID	00000c6e
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

사용 중지된 프로토콜을 통해 연결된 네트워크가 차단되었습니다

상태	ⓘ
구성 요소	보호
Windows 이벤트 ID	75
Kaspersky Security Center 이벤트 ID	0000004b
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

KUMA 서버 연결 오류

상태	ⓘ
구성 요소	KUMA 통합
Windows 이벤트 ID	2854
Kaspersky Security Center 이벤트 ID	00000b26
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

KUMA 서버의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	KUMA 통합
Windows 이벤트 ID	2855
Kaspersky Security Center 이벤트 ID	00000b27
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

KUMA 서버에서 에이전트의 인증서가 올바르지 않음

상태	ⓘ
구성 요소	KUMA 통합
Windows 이벤트 ID	2856
Kaspersky Security Center 이벤트 ID	00000b28
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

기능 실패

작업을 수행할 수 없음

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	212
Kaspersky Security Center 이벤트 ID	000000d4
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

잘못된 작업 설정. 설정이 적용되지 않음

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	707
Kaspersky Security Center 이벤트 ID	000002c3
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

경고

이전 세션에서 애플리케이션 충돌 발생

상태	⚠
구성 요소	시스템 감사

Windows 이벤트 ID	237
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

라이센스가 곧 만료됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	204
Kaspersky Security Center 이벤트 ID	000000cc
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

데이터베이스가 오래되었음

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	208
Kaspersky Security Center 이벤트 ID	000000d0
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

자동 업데이트가 중지됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	210
Kaspersky Security Center 이벤트 ID	000000d2
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

자기 보호가 비활성화됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	211
Kaspersky Security Center 이벤트 ID	000000d3
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

보호 구성 요소가 비활성화됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	214

Kaspersky Security Center 이벤트 ID	000000d6
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

컴퓨터가 안전 모드에서 실행 중임

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	215
Kaspersky Security Center 이벤트 ID	000000d7
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

처리 안 된 파일이 있음

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	216
Kaspersky Security Center 이벤트 ID	000000d8
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

그룹 정책이 적용됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	219
Kaspersky Security Center 이벤트 ID	000000db
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

작업 중지

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	222
Kaspersky Security Center 이벤트 ID	000000de
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

업데이트를 완료하기 위해 애플리케이션을 종료하고 다시 시작

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	224

Kaspersky Security Center 이벤트 ID	0000057b
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

컴퓨터 다시 시작 필요

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	225
Kaspersky Security Center 이벤트 ID	000000e1
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

설치 안 된 구성 요소를 사용할 수 있는 라이센스가 부여됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	226
Kaspersky Security Center 이벤트 ID	000000e2
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

고급 치료 시작됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	232
Kaspersky Security Center 이벤트 ID	000000e8
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

고급 치료 완료

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	233
Kaspersky Security Center 이벤트 ID	000000e9
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

잘못된 예비 키

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	230

Kaspersky Security Center 이벤트 ID	000000e6
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

서브스크립션이 곧 만료됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	240
Kaspersky Security Center 이벤트 ID	000000f0
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

차단됨

상태	⚠
구성 요소	행동 탐지 Anti-Cryptor 익스플로잇 방지 웹 위협 보호
Windows 이벤트 ID	331
Kaspersky Security Center 이벤트 ID	GNRL_EV_OBJECT_BLOCKED
이벤트 매개변수	• GNRL_EA_PARAM_1은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_2는 개체의 이름입니다. 공유 폴더에 대해 외부 암호화가 감지되면 애플리케이션이 대상 파일에 대한 경로를 표시합니다. • GNRL_EA_PARAM_5는 EICAR-Test-File과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). Kaspersky Private Security Network에서 탐지된 보안 위협(blacklist): true 또는 false. EDR 버전. EDR의 보안 위협 ID. 개체의 MD5 해시.
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

Wi-Fi 네트워크에 대한 접근 제어를 허용하지 않는 운영 체제 설정

상태	⚠
구성 요소	장치 제어
Windows 이벤트 ID	249
Kaspersky Security Center 이벤트 ID	000000f9
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

개체가 백업에서 복원되지 않음

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	336
Kaspersky Security Center 이벤트 ID	00000150
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

의심스러운 네트워크 활동이 탐지됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	2001
Kaspersky Security Center 이벤트 ID	000007d1
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

암호화된 연결 종료

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	250
Kaspersky Security Center 이벤트 ID	000007d3
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

KSN 참가가 비활성화됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	2021
Kaspersky Security Center 이벤트 ID	000007e5
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

일부 OS 기능의 처리가 비활성화됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	245
Kaspersky Security Center 이벤트 ID	000000f5
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

격리 저장소에 공간이 얼마 남지 않았습니다

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	344
Kaspersky Security Center 이벤트 ID	00000158
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

네트워크 연결 차단됨

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	809
Kaspersky Security Center 이벤트 ID	00000abe
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

백업 복사본을 생성할 수 없음

상태	⚠
구성 요소	파일 위협 보호 메일 위협 보호 호스트 침입 방지 AMSI 보호 악성 코드 검사
Windows 이벤트 ID	314
Kaspersky Security Center 이벤트 ID	GNRL_EV_OBJECT_REPORTED
이벤트 매개변수	• GNRL_EA_PARAM_1은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_2는 개체의 이름입니다. • GNRL_EA_PARAM_5는 EICAR-Test-File과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). Kaspersky Private Security Network에서 탐지된 보안 위협(blacklist): true 또는 false. EDR 버전. EDR의 보안 위협 ID. 개체의 MD5 해시.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

상태	⚠
구성 요소	파일 위협 보호 행동 탐지 Anti-Cryptor 호스트 침입 방지 악성 코드 검사
Windows 이벤트 ID	310
Kaspersky Security Center 이벤트 ID	00000136

Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 암호화됨

상태	⚠
구성 요소	호스트 침입 방지
Windows 이벤트 ID	320
Kaspersky Security Center 이벤트 ID	00000140
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

개체 손상됨

상태	⚠
구성 요소	파일 위협 보호 웹 위협 보호 메일 위협 보호 AMSI 보호 호스트 침입 방지 악성 코드 검사
Windows 이벤트 ID	321
Kaspersky Security Center 이벤트 ID	00000141
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

침입자에게 악용되어 사용자의 컴퓨터나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어가 탐지되었습니다(로컬 베이스)

상태	⚠
구성 요소	파일 위협 보호 웹 위협 보호 메일 위협 보호 호스트 침입 방지 AMSI 보호 행동 탐지 Anti-Cryptor Anti-Cryptor 악성 코드 검사
Windows 이벤트 ID	303
Kaspersky Security Center 이벤트 ID	GNRL_EV_VIRUS_FOUND
이벤트 매개변수	• GNRL_EA_PARAM_1 은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_2 는 개체의 이름입니다. • GNRL_EA_PARAM_5 는 EICAR-Test-File 과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • GNRL_EA_PARAM_7 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8 은 위협 유형입니다(type).
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

침입자에게 악용되어 사용자의 컴퓨터나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어가 탐지되었습니다 (KSN)

상태	⚠
구성 요소	파일 위협 보호 웹 위협 보호 메일 위협 보호 호스트 침입 방지 AMSI 보호 행동 탐지 Anti-Cryptor Anti-Cryptor 악성 코드 검사
Windows 이벤트 ID	`303`
Kaspersky Security Center 이벤트 ID	`GNRL_EV_VIRUS_FOUND_BY_KSN`
이벤트 매개변수	• `GNRL_EA_PARAM_1`은 개체의 해시(SHA256)입니다. • `GNRL_EA_PARAM_2`는 개체의 이름입니다. • `GNRL_EA_PARAM_5`는 `EICAR-Test-File`과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • `GNRL_EA_PARAM_7`은 세션 사용자의 이름입니다. • `GNRL_EA_PARAM_8`은 위협 유형입니다(`type`).
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 삭제됨

상태	⚠
구성 요소	파일 위협 보호 메일 위협 보호 호스트 침입 방지 익스플로잇 방지 행동 탐지 Anti-Cryptor 악성 코드 검사
Windows 이벤트 ID	`307`
Kaspersky Security Center 이벤트 ID	`GNRL_EV_OBJECT_DELETED`
이벤트 매개변수	• `GNRL_EA_PARAM_1`은 개체의 해시(SHA256)입니다. • `GNRL_EA_PARAM_2`는 개체의 이름입니다. • `GNRL_EA_PARAM_5`는 `EICAR-Test-File`과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • `GNRL_EA_PARAM_7`은 세션 사용자의 이름입니다. • `GNRL_EA_PARAM_8`은 위협 유형입니다(`type`). • `GNRL_EA_PARAM_9`는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(`engine`). 보안 위협 탐지 기술(`method`). Kaspersky Private Security Network에서 탐지된 보안 위협(`blacklist`): `true` 또는 `false`. EDR 버전. EDR의 보안 위협 ID. 개체의 MD5 해시.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 치료됨

상태	⚠
구성 요소	파일 위협 보호 메일 위협 보호 호스트 침입 방지 악성 코드 검사
Windows 이벤트 ID	306
Kaspersky Security Center 이벤트 ID	GNRL_EV_OBJECT_CURED
이벤트 매개변수	• GNRL_EA_PARAM_1은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_2는 개체의 이름입니다. • GNRL_EA_PARAM_5는 EICAR-Test-File과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). Kaspersky Private Security Network에서 탐지된 보안 위협(blacklist): true 또는 false. EDR 버전. EDR의 보안 위협 ID. 개체의 MD5 해시.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

컴퓨터 다시 시작 시 개체 치료 예정

상태	⚠
구성 요소	호스트 침입 방지 파일 위협 보호 악성 코드 검사
Windows 이벤트 ID	324
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

컴퓨터 다시 시작 시 개체 삭제 예정

상태	⚠
구성 요소	행동 탐지 Anti-Cryptor 익스플로잇 방지 호스트 침입 방지 파일 위협 보호 악성 코드 검사
Windows 이벤트 ID	323
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

설정에 따라 개체가 삭제됨

상태	⚠
구성 요소	메일 위협 보호

Windows 이벤트 ID	342
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

롤백 완료

상태	⚠
구성 요소	파일 위협 보호 행동 탐지 Anti-Cryptor 익스플로잇 방지 악성 코드 검사
Windows 이벤트 ID	455
Kaspersky Security Center 이벤트 ID	000001c7
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 다운로드 차단됨

상태	⚠
구성 요소	웹 위협 보호
Windows 이벤트 ID	341
Kaspersky Security Center 이벤트 ID	GNRL_EV_OBJECT_BLOCKED
이벤트 매개변수	• GNRL_EA_PARAM_1은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_2는 개체의 이름입니다. • GNRL_EA_PARAM_5는 EICAR-Test-File과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8은 위협 유형입니다(type). • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). Kaspersky Private Security Network에서 탐지된 보안 위협(blacklist): true 또는 false. EDR 버전. EDR의 보안 위협 ID. 개체의 MD5 해시.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

키보드 인증 오류

상태	⚠
구성 요소	BadUSB 공격 방지
Windows 이벤트 ID	2052
Kaspersky Security Center 이벤트 ID	00000804
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 검사 결과가 제삼자 애플리케이션으로 전송됨

상태	⚠
구성 요소	AMSI 보호
Windows 이벤트 ID	1512
Kaspersky Security Center 이벤트 ID	GNRL_EV_OBJECT_REPORTED
이벤트 매개변수	• GNRL_EA_PARAM_1 은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_2 는 개체의 이름입니다. • GNRL_EA_PARAM_5 는 EICAR-Test-File 과 같이 Kaspersky 분류에 따른 보안 위협의 이름입니다. • GNRL_EA_PARAM_7 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_8 은 위협 유형입니다(type). • GNRL_EA_PARAM_9 는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). Kaspersky Private Security Network에서 탐지된 보안 위협(blacklist): true 또는 false. EDR 버전. EDR의 보안 위협 ID. 개체의 MD5 해시.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

작업 설정이 성공적으로 적용됨

상태	⚠
구성 요소	애플리케이션 제어
Windows 이벤트 ID	708
Kaspersky Security Center 이벤트 ID	000002c4
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

바람직하지 않은 콘텐츠에 대한 경고(로컬 기반)

상태	⚠
구성 요소	웹 제어
Windows 이벤트 ID	708
Kaspersky Security Center 이벤트 ID	GNRL_EV_WEB_URL_WARNING
이벤트 매개변수	• GNRL_EA_PARAM_1 은 URL입니다. • GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_3 은 웹 제어 규칙의 이름입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

바람직하지 않는 콘텐츠에 대한 경고(KSN)

상태	⚠
구성 요소	웹 제어
Windows 이벤트 ID	708

Kaspersky Security Center 이벤트 ID	GNRL_EV_WEB_URL_WARNING
이벤트 매개변수	• GNRL_EA_PARAM_1 은 URL 입니다. • GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_3 은 웹 제어 규칙의 이름입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

경고 이후 바람직하지 않은 컨텐츠에 접근함

상태	⚠
구성 요소	웹 제어
Windows 이벤트 ID	754
Kaspersky Security Center 이벤트 ID	000002f2
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

장치에 대한 임시 접근이 활성화됨

상태	⚠
구성 요소	장치 제어
Windows 이벤트 ID	803
Kaspersky Security Center 이벤트 ID	000002f2
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

사용자가 작업을 취소했습니다

상태	⚠
구성 요소	업데이트
Windows 이벤트 ID	1016
Kaspersky Security Center 이벤트 ID	000003f8
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

사용자가 암호화 정책을 거부함

상태	⚠
구성 요소	데이터 암호화
Windows 이벤트 ID	1306
Kaspersky Security Center 이벤트 ID	0000051a
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 암호화 / 복호화 규칙 적용 중지됨

상태	⚠
구성 요소	데이터 암호화
Windows 이벤트 ID	903
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 암호화 / 복호화 중지됨

상태	⚠
구성 요소	데이터 암호화
Windows 이벤트 ID	914
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

장치 암호화/복호화가 중단됨

상태	⚠
구성 요소	데이터 암호화
Windows 이벤트 ID	1303
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

WinRE 이미지에서 Kaspersky 디스크 암호화 드라이버를 설치하거나 업그레이드하지 못했습니다

상태	⚠
구성 요소	데이터 암호화
Windows 이벤트 ID	1345
Kaspersky Security Center 이벤트 ID	00000541
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

모듈 서명 확인 실패

상태	⚠
구성 요소	시스템 무결성 검사
Windows 이벤트 ID	2002
Kaspersky Security Center 이벤트 ID	000007d2
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

애플리케이션 시작이 차단됨

상태	⚠
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2105
Kaspersky Security Center 이벤트 ID	00000839
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

문서 열기가 차단됨

상태	⚠
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2106
Kaspersky Security Center 이벤트 ID	0000083a
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Kaspersky Anti Targeted Attack Platform 서버 관리자가 프로세스를 강제 종료했습니다

상태	⚠
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2112
Kaspersky Security Center 이벤트 ID	00000840
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Kaspersky Anti Targeted Attack Platform 서버 관리자가 애플리케이션을 강제 종료했습니다

상태	⚠
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2113
Kaspersky Security Center 이벤트 ID	00000841
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Kaspersky Anti Targeted Attack Platform 서버 관리자가 파일 또는 스트림을 삭제했습니다

상태	⚠
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2111
Kaspersky Security Center 이벤트 ID	0000083f
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

관리자가 Kaspersky Anti Targeted Attack Platform 서버의 격리 저장소에서 파일을 복원했습니다

상태	⚠
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2110
Kaspersky Security Center 이벤트 ID	0000083e
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

관리자가 파일을 Kaspersky Anti Targeted Attack Platform 서버로 격리했습니다.

상태	⚠
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2109
Kaspersky Security Center 이벤트 ID	0000083d
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

모든 타사 애플리케이션의 네트워크 활동이 차단됨

상태	⚠
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2107
Kaspersky Security Center 이벤트 ID	0000083b
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

모든 제삼자 애플리케이션의 네트워크 활동 차단이 해제됨

상태	⚠
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2108
Kaspersky Security Center 이벤트 ID	0000083c
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 다시 시작 후 삭제됨(Sandbox)

상태	⚠
구성 요소	Sandbox
Windows 이벤트 ID	2605
Kaspersky Security Center 이벤트 ID	00000a2d
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

검사 작업의 전체 크기가 한도를 초과했습니다

상태	⚠
구성 요소	Sandbox
Windows 이벤트 ID	2612
Kaspersky Security Center 이벤트 ID	00000a34
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 시작 허용됨, 이벤트 기록됨

상태	⚠
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2553
Kaspersky Security Center 이벤트 ID	000009fa
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

프로세스 시작 허용됨, 이벤트 기록됨

상태	⚠
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2554
Kaspersky Security Center 이벤트 ID	000009f8
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 다시 시작 후 삭제됨(Endpoint Detection and Response)

상태	⚠
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2558
Kaspersky Security Center 이벤트 ID	000009fe
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

네트워크 격리

상태	⚠
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2700
Kaspersky Security Center 이벤트 ID	00000a8c
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

네트워크 격리 종료

상태	⚠
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2701
Kaspersky Security Center 이벤트 ID	00000a8d
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

작업을 완료하기 위해 재부팅해야 함

상태	⚠
구성 요소	시스템 감사
Windows 이벤트 ID	225
Kaspersky Security Center 이벤트 ID	0000057b
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

관리자에게 애플리케이션 시작 차단 메시지 보내기

상태	⚠
구성 요소	애플리케이션 제어
Windows 이벤트 ID	503
Kaspersky Security Center 이벤트 ID	GNRL_EV_AC_USER_REQUEST
이벤트 매개변수	• GNRL_EA_DESCRIPTION은 사용자에게 보내는 메시지입니다. • GNRL_EA_PARAM_2은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_6은 애플리케이션 실행 파일의 이름입니다(예: chrome.exe). • GNRL_EA_PARAM_7은 실행 파일의 경로입니다. • GNRL_EA_PARAM_8은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_9는 사용자가 실행하고자 하는 애플리케이션의 버전입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

관리자에게 장치 접근 차단 메시지 보내기

상태	⚠
구성 요소	장치 제어
Windows 이벤트 ID	804
Kaspersky Security Center 이벤트 ID	GNRL_EV_DC_USER_REQUEST
이벤트 매개변수	• c_er_descr은 사용자에게 보내는 메시지입니다. • GNRL_EA_PARAM_1은 하드웨어 ID(HWID)입니다. • GNRL_EA_PARAM_2은 세션 사용자의 이름입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

관리자에게 웹 페이지 접근 차단 메시지 보내기

상태	⚠
구성 요소	웹 제어
Windows 이벤트 ID	755

Kaspersky Security Center 이벤트 ID	GNRL_EV_WC_USER_REQUEST
이벤트 매개변수	• GNRL_EA_DESCRIPTION은 사용자에게 보내는 메시지입니다. • GNRL_EA_PARAM_1은 URL입니다. • GNRL_EA_PARAM_2은 세션 사용자의 이름입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

장치 연결이 차단됨

상태	⚠
구성 요소	장치 제어
Windows 이벤트 ID	807
Kaspersky Security Center 이벤트 ID	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
이벤트 매개변수	• GNRL_EA_PARAM_1은 하드웨어 ID(HWID)입니다. • GNRL_EA_PARAM_2은 세션 사용자의 이름입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

관리자에게 애플리케이션 활동 차단 메시지 보내기

상태	⚠
구성 요소	파일 무결성 모니터
Windows 이벤트 ID	2901
Kaspersky Security Center 이벤트 ID	00000b55
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

상태	⚠
구성 요소	파일 무결성 모니터
Windows 이벤트 ID	2900
Kaspersky Security Center 이벤트 ID	00000b54
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

상태	⚠
구성 요소	적응형 이상 행위 제어
Windows 이벤트 ID	503
Kaspersky Security Center 이벤트 ID	GNRL_EV_ADSEC_USER_REQUEST
이벤트 매개변수	• GNRL_EA_DESCRIPTION은 사용자에게 보내는 메시지입니다. • GNRL_EA_PARAM_1은 적응형 이상 행위 제어 규칙의 이름입니다. • GNRL_EA_PARAM_2는 휴리스틱 규칙의 ID입니다. • GNRL_EA_PARAM_3은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_4는 소스 프로세스입니다. • GNRL_EA_PARAM_5는 소스 개체입니다. • GNRL_EA_PARAM_6은 대상 프로세스입니다. • GNRL_EA_PARAM_7는 대상 개체입니다. • GNRL_EA_PARAM_8는 탐지된 개체에 대한 추가 정보입니다. 소스 프로세스 해시 / 개체 및 대상 프로세스 / 개체. 프로세스 차단됨(verdict_type): true 또는 false. 사용자 보안 ID(SID).

Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

클라우드 서비스 클라이언트 애플리케이션 시작이 차단됨

상태	⚠
구성 요소	Cloud Discovery
Windows 이벤트 ID	2212
Kaspersky Security Center 이벤트 ID	000008a4
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

클라우드 서비스 접근이 차단됨

상태	⚠
구성 요소	Cloud Discovery
Windows 이벤트 ID	2213
Kaspersky Security Center 이벤트 ID	000008a5
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 또는 폴더 변경이 탐지됨

상태	ⓘ / ⚠ / !
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2950
Kaspersky Security Center 이벤트 ID	00000b86
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

개체 변동이 너무 자주 발생합니다. 이벤트 집계 시작

상태	ⓘ / ⚠ / !
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2955
Kaspersky Security Center 이벤트 ID	00000b8b
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

수집 기간 중 개체 변경 보고

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2956
Kaspersky Security Center 이벤트 ID	00000b8c
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

레지스트리 변경이 탐지됨

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2951
Kaspersky Security Center 이벤트 ID	00000b87
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

장치 연결/연결 해제 감지됨

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2952
Kaspersky Security Center 이벤트 ID	00000b88
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

잘못된 개체를 포함한 모니터링 범위

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2903
Kaspersky Security Center 이벤트 ID	00000b89
Windows 이벤트 로그(기본값)	–

Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

차단된 작업이 테스트 모드에서 허용되었습니다

상태	⚠
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2961
Kaspersky Security Center 이벤트 ID	00000b91
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

30분 이상 통합 서버에 연결할 수 없습니다. 통합 서버 상태 및 네트워크 설정 확인

상태	⚠
구성 요소	Light Agent
Windows 이벤트 ID	3102
Kaspersky Security Center 이벤트 ID	00000c1e
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

통합 서버에 연결할 수 없음 통합 서버 상태 및 네트워크 설정 확인

상태	⚠
구성 요소	Light Agent
Windows 이벤트 ID	3101
Kaspersky Security Center 이벤트 ID	00000c1d
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

가상 머신 템플릿 업데이트 필요

상태	⚠
구성 요소	Light Agent
Windows 이벤트 ID	3181
Kaspersky Security Center 이벤트 ID	00000c6d
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

Standard 라이센스가 종료됩니다. 애플리케이션이 Enterprise 라이센스로 실행 중입니다

상태	⚠
구성 요소	Light Agent

Windows 이벤트 ID	3171
Kaspersky Security Center 이벤트 ID	00000c64
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

정보 메시지

애플리케이션 시작

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	235
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

애플리케이션 중지

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	236
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

보호 중인 리소스로 자기 보호 제한 접근

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	213
Kaspersky Security Center 이벤트 ID	000000d5
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

리포트 지움

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	217
Kaspersky Security Center 이벤트 ID	000000d9
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

그룹 정책 비활성화됨

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	220
Kaspersky Security Center 이벤트 ID	000000dc
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

애플리케이션 설정이 변경됨

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	218
Kaspersky Security Center 이벤트 ID	000000da
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

작업 시작됨

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	221
Kaspersky Security Center 이벤트 ID	000000dd
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

작업 완료됨

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	223
Kaspersky Security Center 이벤트 ID	000000df
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

라이센스에 정의된 모든 애플리케이션 구성 요소가 설치되어 정상 모드로 실행 중입니다

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	227
Kaspersky Security Center 이벤트 ID	000000e3
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

서브스크립션 설정이 변경됨

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	238
Kaspersky Security Center 이벤트 ID	000000ee
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

서브스크립션이 갱신됨

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	239
Kaspersky Security Center 이벤트 ID	000000ef
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

백업 저장소에서 개체가 복원됨

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	335
Kaspersky Security Center 이벤트 ID	0000014f
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

사용자 이름 및 암호 입력

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	2000
Kaspersky Security Center 이벤트 ID	000007d0
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

KSN 참가가 활성화됨

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	2020
Kaspersky Security Center 이벤트 ID	000007e4
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

KSN 서버 이용 가능

상태	
구성 요소	시스템 감사
Windows 이벤트 ID	2022
Kaspersky Security Center 이벤트 ID	000007e6
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

해당 애플리케이션은 관련 법률에 따라 데이터를 적용하고 처리하며 적절한 인프라를 사용합니다

상태	
구성 요소	시스템 감사
Windows 이벤트 ID	2024
Kaspersky Security Center 이벤트 ID	000007e8
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 격리 저장소에서 복원됨

상태	
구성 요소	시스템 감사
Windows 이벤트 ID	345
Kaspersky Security Center 이벤트 ID	00000159
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 격리 저장소에서 삭제됨

상태	
구성 요소	시스템 감사
Windows 이벤트 ID	347
Kaspersky Security Center 이벤트 ID	0000015b
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체의 백업 복사본 생성됨

상태	
구성 요소	파일 위협 보호 메일 위협 보호 행동 탐지 Anti-Cryptor 호스트 침입 방지 Sandbox 악성 코드 검사
Windows 이벤트 ID	308
Kaspersky Security Center 이벤트 ID	00000134

Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

이전에 치료된 백업 사본으로 덮어씀

상태	ⓘ
구성 요소	파일 위협 보호 호스트 침입 방지 악성 코드 검사
Windows 이벤트 ID	327
Kaspersky Security Center 이벤트 ID	00000147
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

암호로 보호된 압축 파일 탐지

상태	ⓘ
구성 요소	파일 위협 보호 웹 위협 보호 메일 위협 보호 AMSI 보호 호스트 침입 방지 악성 코드 검사
Windows 이벤트 ID	322
Kaspersky Security Center 이벤트 ID	GNRL_EV_PASSWD_ARCHIVE_FOUND
이벤트 매개변수	• GNRL_EA_PARAM_2는 개체의 이름입니다. • GNRL_EA_PARAM_3은 개체 생성 날짜입니다(선택사항). • GNRL_EA_PARAM_7은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_9는 탐지된 개체에 대한 추가 정보입니다. 애플리케이션 구성 요소(engine). 보안 위협 탐지 기술(method). KPSN에서 탐지된 보안 위협(denylist): true 또는 false.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

탐지한 개체에 대한 정보

상태	ⓘ
구성 요소	파일 위협 보호 웹 위협 보호 메일 위협 보호 AMSI 보호 호스트 침입 방지 악성 코드 검사
Windows 이벤트 ID	332
Kaspersky Security Center 이벤트 ID	0000014c
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 Kaspersky Private Security Network 허용 목록에 있습니다

상태	ⓘ
구성 요소	파일 위협 보호 웹 위협 보호 메일 위협 보호 AMSI 보호 호스트 침입 방지 악성 코드 검사
Windows 이벤트 ID	340
Kaspersky Security Center 이벤트 ID	00000154
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 이름 변경됨

상태	ⓘ
구성 요소	메일 위협 보호 익스플로잇 방지 행동 탐지 Anti-Cryptor 악성 코드 검사
Windows 이벤트 ID	329
Kaspersky Security Center 이벤트 ID	00000149
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 처리 완료

상태	ⓘ
구성 요소	호스트 침입 방지 파일 위협 보호 웹 위협 보호 메일 위협 보호 악성 코드 검사
Windows 이벤트 ID	301
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

개체 건너뜀

상태	ⓘ
구성 요소	호스트 침입 방지 파일 위협 보호 AMSI 보호 악성 코드 검사
Windows 이벤트 ID	315
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

압축 파일 탐지됨

상태	ⓘ
구성 요소	호스트 침입 방지 파일 위협 보호 웹 위협 보호 메일 위협 보호 AMSI 보호 악성 코드 검사
Windows 이벤트 ID	318
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

압축된 개체 탐지

상태	ⓘ
구성 요소	호스트 침입 방지 파일 위협 보호 웹 위협 보호 메일 위협 보호 AMSI 보호 악성 코드 검사
Windows 이벤트 ID	319
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

링크 처리됨

상태	ⓘ
구성 요소	웹 위협 보호
Windows 이벤트 ID	361
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

애플리케이션 시작이 허용됨

상태	ⓘ
구성 요소	애플리케이션 제어
Windows 이벤트 ID	701
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

업데이트 경로가 선택됨

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1001

Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

프록시 서버가 선택됨

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1002
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

링크가 Kaspersky Private Security Network 허용 목록에 있습니다

상태	ⓘ
구성 요소	웹 위협 보호
Windows 이벤트 ID	370
Kaspersky Security Center 이벤트 ID	00000172
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

신뢰하는 그룹에 애플리케이션 추가

상태	ⓘ
구성 요소	호스트 침입 방지
Windows 이벤트 ID	401
Kaspersky Security Center 이벤트 ID	00000191
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

제한 그룹에 애플리케이션 추가

상태	ⓘ
구성 요소	호스트 침입 방지
Windows 이벤트 ID	402
Kaspersky Security Center 이벤트 ID	00000192
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

호스트 침입 방지 트리거됨

상태	ⓘ
구성 요소	호스트 침입 방지
Windows 이벤트 ID	403

Kaspersky Security Center 이벤트 ID	00000193
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 복원됨

상태	ⓘ
구성 요소	행동 탐지 Anti-Cryptor 익스플로잇 방지 호스트 침입 방지
Windows 이벤트 ID	457
Kaspersky Security Center 이벤트 ID	000001c9
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

레지스트리 값이 복원됨

상태	ⓘ
구성 요소	행동 탐지 익스플로잇 방지
Windows 이벤트 ID	458
Kaspersky Security Center 이벤트 ID	000001ca
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

레지스트리 값이 삭제됨

상태	ⓘ
구성 요소	행동 탐지 익스플로잇 방지
Windows 이벤트 ID	459
Kaspersky Security Center 이벤트 ID	000001cb
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

프로세스 처리를 건너뜀

상태	ⓘ
구성 요소	적응형 이상 행위 제어
Windows 이벤트 ID	2201

Kaspersky Security Center 이벤트 ID	GNRL_EV_ADSEC_DETECT
이벤트 매개변수	• GNRL_EA_PARAM_1 은 적응형 이상 행위 제어 규칙의 이름입니다. • GNRL_EA_PARAM_2 는 휴리스틱 규칙의 ID입니다. • GNRL_EA_PARAM_3 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_4 는 소스 프로세스입니다. • GNRL_EA_PARAM_5 는 소스 개체입니다. • GNRL_EA_PARAM_6 은 대상 프로세스입니다. • GNRL_EA_PARAM_7 는 대상 개체입니다. • GNRL_EA_PARAM_8 는 탐지된 개체에 대한 추가 정보입니다. 소스 프로세스 해시 / 개체 및 대상 프로세스 / 개체. 프로세스 차단됨(verdict_type): true 또는 false. 사용자 보안 ID(SID).
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

키보드 인증 성공

상태	ⓘ
구성 요소	BadUSB 공격 방지
Windows 이벤트 ID	2050
Kaspersky Security Center 이벤트 ID	00000802
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

네트워크 활동 허용됨

상태	ⓘ
구성 요소	방화벽
Windows 이벤트 ID	601
Kaspersky Security Center 이벤트 ID	00000259
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

테스트 모드에서 애플리케이션 시작 금지됨

상태	ⓘ
구성 요소	애플리케이션 제어
Windows 이벤트 ID	703
Kaspersky Security Center 이벤트 ID	GNRL_EV_APP_LAUNCH_TESTED_DENIED
이벤트 매개변수	• GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_3 은 수동으로 생성된 카테고리 ID입니다. • GNRL_EA_PARAM_4 는 계정 보안 ID(SID)입니다. • GNRL_EA_PARAM_5 는 애플리케이션의 디지털 서명에 관한 정보입니다. • GNRL_EA_PARAM_6 은 애플리케이션 실행 파일의 이름입니다(예: chrome.exe). • GNRL_EA_PARAM_7 은 실행 파일의 경로입니다. • GNRL_EA_PARAM_8 은 개체의 해시(SHA256)입니다. • GNRL_EA_PARAM_9 는 사용자가 실행하고자 하는 애플리케이션의 버전입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

테스트 모드에서 애플리케이션 시작 허용됨

상태	
구성 요소	애플리케이션 제어
Windows 이벤트 ID	704
Kaspersky Security Center 이벤트 ID	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
이벤트 매개변수	• GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_3 은 수동으로 생성된 카테고리 ID입니다. • GNRL_EA_PARAM_4 는 계정 보안 ID(SID)입니다. • GNRL_EA_PARAM_5 는 애플리케이션의 디지털 서명에 관한 정보입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

허용된 페이지가 열림

상태	
구성 요소	웹 제어
Windows 이벤트 ID	751
Kaspersky Security Center 이벤트 ID	000002f4
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

장치를 사용한 작업이 허용됨

상태	
구성 요소	장치 제어
Windows 이벤트 ID	801
Kaspersky Security Center 이벤트 ID	00000321
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 동작이 수행됨

상태	
구성 요소	장치 제어
Windows 이벤트 ID	808
Kaspersky Security Center 이벤트 ID	GNRL_EV_USB_FILE_OPERATION
이벤트 매개변수	• GNRL_EA_PARAM_1 은 파일 동작입니다(쓰기 또는 삭제). • GNRL_EA_PARAM_2 은 파일 경로입니다. • GNRL_EA_PARAM_3 은 장치 이름입니다. • GNRL_EA_PARAM_4 은 세션 사용자의 이름입니다. • GNRL_EA_PARAM_5 은 하드웨어 ID(HWID)입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

실행 가능한 업데이트 없음

상태	
구성 요소	업데이트
Windows 이벤트 ID	1020

Kaspersky Security Center 이벤트 ID	000003fc
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

업데이트 배포를 완료했습니다

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1022
Kaspersky Security Center 이벤트 ID	000003fe
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 다운로드 중

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1003
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 다운로드 완료

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1004
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 설치 완료

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1005
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 업데이트 완료

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1006

Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

업데이트 오류로 인해 파일이 롤백됨

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1007
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 업데이트 중

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1008
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

업데이트 배포 중

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1009
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 롤백 중

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1010
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

다운로드할 파일 목록 생성

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	1013

Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

패치 다운로드 중

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	2150
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

패치 설치 중

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	2151
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

패치 설치됨

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	2152
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

패치 롤백 중

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	2154
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

패치 롤백 완료

상태	ⓘ
구성 요소	업데이트
Windows 이벤트 ID	2155

Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 암호화 / 복호화 규칙 적용을 시작함

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	901
Kaspersky Security Center 이벤트 ID	00000385
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 암호화 / 복호화 규칙 적용을 완료함

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	902
Kaspersky Security Center 이벤트 ID	00000386
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 암호화 / 복호화 규칙 적용 다시 시작됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	905
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 암호화 / 복호화 시작됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	910
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일 암호화 / 복호화 완료됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	911

Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

파일이 예외 항목으로 설정되어 있어 암호화되지 않음

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	913
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

휴대용 모드 활성화됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	950
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

휴대용 모드 비활성화됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	952
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

장치 암호화 / 복호화 시작됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1301
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

장치 암호화 / 복호화 완료됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1302

Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

장치 암호화 / 복호화 다시 시작됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1304
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

장치가 암호화되지 않음

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1307
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

장치 암호화/복호화 과정이 액티브 모드로 전환됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1308
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

장치 암호화/복호화 과정이 패시브 모드로 전환됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1309
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

암호화 모듈이 로드되었습니다

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1310

Kaspersky Security Center 이벤트 ID	0000051e
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

새로운 인증 에이전트 계정이 생성됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1330
Kaspersky Security Center 이벤트 ID	00000532
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

인증 에이전트 계정이 삭제되었습니다

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1331
Kaspersky Security Center 이벤트 ID	00000533
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

인증 에이전트 계정 암호가 변경됨

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1332
Kaspersky Security Center 이벤트 ID	00000534
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

인증 에이전트 로그인 성공

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1333
Kaspersky Security Center 이벤트 ID	00000535
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

인증 에이전트 로그인 시도 실패

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1334

Kaspersky Security Center 이벤트 ID	00000536
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

암호화된 장치에 대한 접근 허용 요청 절차를 사용해 하드 드라이브에 접근함

상태	
구성 요소	데이터 암호화
Windows 이벤트 ID	1335
Kaspersky Security Center 이벤트 ID	00000537
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

암호화된 장치에 대한 접근 허용 요청 절차를 사용해 하드 드라이브에 접근할 때 오류 발생

상태	
구성 요소	데이터 암호화
Windows 이벤트 ID	1336
Kaspersky Security Center 이벤트 ID	00000538
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

계정이 추가되지 않음. 이미 존재하는 계정입니다.

상태	
구성 요소	데이터 암호화
Windows 이벤트 ID	1337
Kaspersky Security Center 이벤트 ID	00000539
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

계정이 변경되지 않음. 존재하지 않는 계정

상태	
구성 요소	데이터 암호화
Windows 이벤트 ID	1338
Kaspersky Security Center 이벤트 ID	0000053a
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

계정이 삭제되지 않음. 존재하지 않는 계정

상태	
구성 요소	데이터 암호화
Windows 이벤트 ID	1339

Kaspersky Security Center 이벤트 ID	0000053b
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

FDE 업그레이드 성공

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1341
Kaspersky Security Center 이벤트 ID	0000053d
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

FDE 업그레이드 롤백 성공

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1343
Kaspersky Security Center 이벤트 ID	0000053f
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

WinRE 이미지에서 Kaspersky 디스크 암호화 드라이버를 제거하지 못했습니다

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1346
Kaspersky Security Center 이벤트 ID	00000542
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

BitLocker 복구 키가 변경되었습니다

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1370
Kaspersky Security Center 이벤트 ID	0000055a
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

BitLocker 암호 / PIN이 변경되었습니다

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1371

Kaspersky Security Center 이벤트 ID	0000055b
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

BitLocker 복구 키가 이동식 드라이브에 저장되었습니다

상태	ⓘ
구성 요소	데이터 암호화
Windows 이벤트 ID	1372
Kaspersky Security Center 이벤트 ID	0000055c
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

Kaspersky Anti Targeted Attack Platform 서버에서의 작업 처리가 비활성 상태임

상태	ⓘ
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2103
Kaspersky Security Center 이벤트 ID	00000837
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

Endpoint Sensor가 서버에 연결됨

상태	ⓘ
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2101
Kaspersky Security Center 이벤트 ID	00000835
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

Kaspersky Anti Targeted Attack Platform 서버로의 연결이 복원됨

상태	ⓘ
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2102
Kaspersky Security Center 이벤트 ID	00000836
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

Kaspersky Anti Targeted Attack Platform 서버에서의 작업이 처리되고 있습니다

상태	ⓘ
구성 요소	Endpoint Sensor
Windows 이벤트 ID	2104

Kaspersky Security Center 이벤트 ID	00000838
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 삭제됨

상태	ⓘ
구성 요소	데이터 완전 삭제
Windows 이벤트 ID	2251
Kaspersky Security Center 이벤트 ID	000008cb
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	–

완전 삭제 작업 통계

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise)
Windows 이벤트 ID	2853
Kaspersky Security Center 이벤트 ID	00000b25
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

상태	ⓘ
구성 요소	데이터 완전 삭제
Windows 이벤트 ID	2253
Kaspersky Security Center 이벤트 ID	000008cd
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체가 격리됨(Sandbox)

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2602
Kaspersky Security Center 이벤트 ID	00000a2a
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 삭제됨(Sandbox)

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2604
Kaspersky Security Center 이벤트 ID	00000a2c

Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

IOC 검사 시작됨

상태	ⓘ
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2652
Kaspersky Security Center 이벤트 ID	00000a5c
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

IOC 검사 완료

상태	ⓘ
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2653
Kaspersky Security Center 이벤트 ID	00000a5d
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 격리됨(Endpoint Detection and Response)

상태	ⓘ
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2555
Kaspersky Security Center 이벤트 ID	000009fb
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

개체 삭제됨(Endpoint Detection and Response)

상태	ⓘ
구성 요소	Endpoint Detection and Response
Windows 이벤트 ID	2557
Kaspersky Security Center 이벤트 ID	000009fd
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

애플리케이션 구성 요소를 성공적으로 변경함

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	1402
Kaspersky Security Center 이벤트 ID	0000057a

Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2606
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2609
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2610
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2616
Kaspersky Security Center 이벤트 ID	–
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	–

장치가 연결된 중앙 관리 서버가 신뢰하는 서버로 설정되었습니다

상태	ⓘ
구성 요소	중앙 관리 서버 연결 보호
Windows 이벤트 ID	3300
Kaspersky Security Center 이벤트 ID	00000ce4
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

새로운 신뢰하는 중앙 관리 서버에 장치가 연결되었습니다

상태	ⓘ
구성 요소	중앙 관리 서버 연결 보호

Windows 이벤트 ID	3302
Kaspersky Security Center 이벤트 ID	00000ce6
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

장치가 연결된 중앙 관리 서버가 신뢰하는 서버로 설정되지 않습니다

상태	ⓘ
구성 요소	중앙 관리 서버 연결 보호
Windows 이벤트 ID	3303
Kaspersky Security Center 이벤트 ID	00000ce7
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

비동기 Sandbox 탐지

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2619
Kaspersky Security Center 이벤트 ID	GNRL_EV_APP_INCIDENT_OCCURED
이벤트 매개변수	• GNRL_EA_PARAM_1 는 Sandbox 구성 요소의 파라미터입니다. • GNRL_EA_PARAM_2 는 개체의 경로입니다. • GNRL_EA_PARAM_3 은 인시던트 ID입니다. • GNRL_EA_PARAM_4 은 개체의 해시(SHA256)입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

사용자가 검사 작업을 Sandbox로 전송함

상태	ⓘ
구성 요소	Sandbox
Windows 이벤트 ID	2622
Kaspersky Security Center 이벤트 ID	00000a3e
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

장치가 연결됨

상태	ⓘ
구성 요소	장치 제어
Windows 이벤트 ID	805
Kaspersky Security Center 이벤트 ID	GNRL_EV_DEVCTRL_DEV_PLUGGED
이벤트 매개변수	• GNRL_EA_PARAM_1 은 하드웨어 ID(HWID)입니다. • GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

장치가 연결 해제됨

상태	ⓘ
구성 요소	장치 제어
Windows 이벤트 ID	806
Kaspersky Security Center 이벤트 ID	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
이벤트 매개변수	• GNRL_EA_PARAM_1 은 하드웨어 ID(HWID)입니다. • GNRL_EA_PARAM_2 은 세션 사용자의 이름입니다.
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

애플리케이션 이전 버전 제거 중 오류가 발생했습니다

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	246
Kaspersky Security Center 이벤트 ID	000000f6
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 서버에 연결 성공

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise)
Windows 이벤트 ID	2853
Kaspersky Security Center 이벤트 ID	00000b25
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 응답 서버 연결 성공

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise) Endpoint Detection and Response Expert(cloud)
Windows 이벤트 ID	2853
Kaspersky Security Center 이벤트 ID	00000b25
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

EDR Expert 원격 측정 수집 서버 연결 성공

상태	ⓘ
구성 요소	Endpoint Detection and Response Expert(on-premise) Endpoint Detection and Response Expert(cloud)
Windows 이벤트 ID	2857
Kaspersky Security Center 이벤트 ID	00000b26

Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

NDR 서버 연결 성공

상태	ⓘ
구성 요소	Network Detection and Response(KATA)
Windows 이벤트 ID	3083
Kaspersky Security Center 이벤트 ID	00000c0b
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

클라우드 서비스 클라이언트 애플리케이션 시작이 허용되었습니다

상태	ⓘ
구성 요소	Cloud Discovery
Windows 이벤트 ID	2210
Kaspersky Security Center 이벤트 ID	000008a2
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

클라우드 서비스 접근이 허용되었습니다

상태	ⓘ
구성 요소	Cloud Discovery
Windows 이벤트 ID	2211
Kaspersky Security Center 이벤트 ID	000008a3
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

보호 구역 접근

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	2004
Kaspersky Security Center 이벤트 ID	000007d4
Windows 이벤트 로그(기본값)	✓
Kaspersky Security Center 이벤트 로그(기본값)	✓

파일 또는 폴더 변경이 탐지됨

상태	ⓘ / ⚠ / ⓔ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2950
Kaspersky Security Center 이벤트 ID	00000b86
Windows 이벤트 로그(기본값)	–

Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

개체 변동이 너무 자주 발생합니다. 이벤트 집계 시작

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2955
Kaspersky Security Center 이벤트 ID	00000b8b
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

수집 기간 중 개체 변경 보고

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2956
Kaspersky Security Center 이벤트 ID	00000b8c
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

레지스트리 변경이 탐지됨

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2951
Kaspersky Security Center 이벤트 ID	00000b87
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

장치 연결/연결 해제 감지됨

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2952
Kaspersky Security Center 이벤트 ID	00000b88

Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

잘못된 개체를 포함한 모니터링 범위

상태	ⓘ / ⚠ / ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2903
Kaspersky Security Center 이벤트 ID	00000b89
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

베이스라인 생성됨

상태	ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2957
Kaspersky Security Center 이벤트 ID	00000b8d
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

베이스라인 업데이트됨

상태	ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2958
Kaspersky Security Center 이벤트 ID	00000b8e
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

신뢰하는 사용자가 작업을 수행합니다

상태	ⓘ
구성 요소	시스템 무결성 모니터링
Windows 이벤트 ID	2962
Kaspersky Security Center 이벤트 ID	00000b92
Windows 이벤트 로그(기본값)	–

Kaspersky Security Center 이벤트 로그(기본값)	✓

이 이벤트의 보존 기간을 구성하려면 정책의 **이벤트 구성** 섹션을 열고 일반 시스템 무결성 모니터링 이벤트 – *파일 또는 폴더 변경이 탐지됨*의 보존 기간을 설정합니다.

SVM에 연결됨

상태	ⓘ
구성 요소	Light Agent
Windows 이벤트 ID	3152
Kaspersky Security Center 이벤트 ID	00000c50
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

새 임시 암호를 생성하였습니다

상태	ⓘ
구성 요소	시스템 감사
Windows 이벤트 ID	265
Kaspersky Security Center 이벤트 ID	00000109
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

통합 서버에 연결됨

상태	ⓘ
구성 요소	Light Agent
Windows 이벤트 ID	3105
Kaspersky Security Center 이벤트 ID	00000c21
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

통합 서버에 연결 복구

상태	ⓘ
구성 요소	Light Agent
Windows 이벤트 ID	3104
Kaspersky Security Center 이벤트 ID	00000c20
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

KUMA 서버 연결 성공

상태	ⓘ
구성 요소	KUMA 통합

Windows 이벤트 ID	2857
Kaspersky Security Center 이벤트 ID	00000b29
Windows 이벤트 로그(기본값)	–
Kaspersky Security Center 이벤트 로그(기본값)	✓

부록 7. 지원하는 실행 방지 파일 확장자

Kaspersky Endpoint Security는 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
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm

애플리케이션 이름	실행 파일	파일 확장자
Adobe Acrobat	acrord32.exe	pdf
Foxit PDF Reader	FoxitReader.exe	
STDU Viewer	STDUViewerApp.exe	
Microsoft Edge	MicrosoftEdge.exe	
Google Chrome	chrome.exe	
Mozilla Firefox	firefox.exe	
Yandex Browser	browser.exe	
Tor Browser	tor.exe	

부록 8. 실행 방지에서 지원되는 스크립트 인터프리터

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).

부록 9. 레지스트리에서의 IOC 검사 범위(RegistryItem)

IOC 검사 범위에 **Windows 레지스트리 – RegistryItem** 데이터 유형을 추가하면 Kaspersky Endpoint Security가 기본적으로 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
```

부록 10. IOC 파일 요구 사항

IOC 검사 작업 생성 시 다음 IOC 파일 요구 사항 및 제한 사항을 고려하십시오:

- 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 Endpoint Security는 OpenIOC 1.1 표준을 준수하는 IOC 파일 편집을 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`
	
	Email/* 용어의 경우 `contains` 및 `is` 조건을 지원합니다. 회고적 IOC 검사가 올바르게 작동하려면 `is` 조건을 사용하는 경우, IOC 파일의 이메일 주소는 `"name@example.org" <SMTP:name@example.org>` 형식으로 지정되어야 합니다. *IOC 검사* 작업을 일반적으로 실행하는 경우 이메일 주소를 `name@example.org` 형식으로 지정하면 됩니다.

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.

부록 11. 애플리케이션 구성 요소 규칙의 사용자 계정

일부 애플리케이션 구성 요소를 구성하려면 특수 규칙을 추가해야 합니다. 예를 들어 웹 제어의 경우 애플리케이션에서 차단할 웹 주소 목록이 있는 규칙을 추가해야 합니다. 애플리케이션 구성 요소 규칙에서 구성 요소의 스케줄을 구성하거나 애플리케이션이 규칙을 적용해야 하는 사용자를 선택할 수도 있습니다.

다음 애플리케이션 구성 요소를 구성하려면 규칙을 추가해야 합니다.

- 애플리케이션 제어
- 웹 제어
- 장치 제어
- 로그 검사
- 적응형 이상 행위 제어
- 시스템 무결성 모니터링.

Kaspersky Endpoint Security for Windows 12.5부터는 이제 Active Directory뿐만 아니라 Kaspersky Security Center의 사용자 목록에서도 사용자를 선택할 수 있습니다. 로컬 사용자 계정 데이터를 직접 입력할 수도 있습니다. 즉, 다음과 같은 방법으로 사용자를 추가할 수 있습니다.

- Active Directory(권장)
- Kaspersky Security Center의 사용자 목록
- 로컬 사용자 계정

> 모든 사용자 선택 방법을 올바르게 채택하려면 Kaspersky Endpoint Security 애플리케이션 및 관리 플러그인을 버전 12.5 이상으로 업데이트해야 합니다.

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 Kaspersky Endpoint Security 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.

애플리케이션은 컴퓨터에서 `<username>` 및 `<hostname>\<username>` 형식으로 직접 추가한 사용자 계정을 식별하기 위해 NetBIOS 이름을 사용합니다. NetBIOS 이름은 최대 16바이트(15자)입니다. 컴퓨터 이름이 15자를 초과하면 애플리케이션이 사용자를 식별할 수 없습니다. 그러면 애플리케이션은 규칙을 비활성화하고 오류를 생성합니다(예: *웹 제어: 보안 식별자(SID) 일치 없이 사용자 계정에 대한 규칙 트리거링 비활성화*). 규칙이 작동하려면 컴퓨터 이름을 직접 줄여야 합니다. Active Directory나 Kaspersky Security Center에서 사용자 계정을 추가할 수 있습니다. 이때는 애플리케이션이 자동으로 컴퓨터 이름을 줄입니다.

Kaspersky Endpoint Security는 규칙에서 기본 제공 사용자 및 그룹("모두" 그룹 등)도 지원합니다. 사용자의 SID가 결정되는 방식에 따라, 이 애플리케이션은 Active Directory에서 추가된 내장 사용자 계정이나 Kaspersky Security Center의 사용자 목록만 사용하도록 허용합니다. 기본 제공 사용자 계정을 로컬로 추가하는 규칙은 작동하지 않습니다.

부록 12. EDR 위협 대응을 위한 API

Kaspersky Endpoint Security 12.9 for Windows는 Kaspersky Security Center OpenAPI를 사용하는 EDR 위협 대응 활동(EDR responses)을 지원합니다. 즉, Python을 사용해 OpenAPI 방법을 호출하여 EDR 위협 대응을 자동화할 수 있습니다. SIEM 솔루션과 통합되면 이러한 방법을 호출할 수 있습니다. Kaspersky SIEM 솔루션인 *Kaspersky Unified Monitoring and Analysis Platform*은 버전 3.4.1부터 EDR 위협 대응 OpenAPI를 지원합니다. 예제 스크립트는 KUMA 문서를 참조하십시오.

EDR 위협 대응 작업을 수행하려면 요청을 생성하고 KSC Open API(`AddIncident`)를 사용해 전송해야 합니다. 요청이 처리되면 Kaspersky Security Center 콘솔에 특수 작업이 생성됩니다.

EDR 위협에 대응 시 작업을 생성하려면, 중앙 관리 서버와 Kaspersky Security Center 웹 콘솔 간의 백그라운드 연결을 구성해야 합니다. 백그라운드 연결 서비스는 Kaspersky Security Center Windows 14.2 이상 및 Kaspersky Security Center Linux 15.2 이상에서 사용할 수 있습니다. Kaspersky Detection and Response 솔루션의 콘솔을 포함한 다른 콘솔은 지원하지 않습니다.

EDR 위협 대응에는 기본 요청 파라미터를 지정해야 합니다(예: JSON 형식):

- `task`는 작업의 유형입니다(아래 참조).
- `targetHost`는 스크립트를 실행해야 하는 컴퓨터의 ID입니다. 필수 인수입니다. 스크립트는 이벤트에서 이 인수를 가져옵니다.
- `responseEventIncidentArea`는 스크립트를 실행한 애플리케이션의 이름입니다(예: `KUMA`). 이 파라미터는 생성된 작업의 이름에 추가됩니다.

EDR 위협 대응을 구성하려면 `"KLINCDT_BODY": json.dumps(data)` 파라미터에 JSON 형식으로 작업 설정을 지정해야 합니다. 결과적으로 애플리케이션은 Kaspersky Security Center 콘솔에 `[Response][KUMA] <task type> - <Date> <Time> - <ID>` 작업을 생성합니다.

Kaspersky Security Center OpenAPI에 연결

애플리케이션은 EDR 위협 대응의 일부로 Kaspersky Security Center 콘솔에서 특수 작업을 생성합니다. 이러한 작업을 생성하려면 컴퓨터와 Kaspersky Security Center 간의 연결을 설정해야 합니다. 이를 위해서는 요청에 Kaspersky Security Center 연결 파라미터를 지정해야 합니다.

Kaspersky XDR 버전 2.1에서 요청을 인증하는 방법이 변경되었습니다. Kaspersky XDR은 사용자 이름 및 암호 인증 대신 PAT 토큰을 사용합니다. 따라서 Kaspersky XDR에서 스크립트를 실행할 수 없습니다. 요청 인증에 대한 상세 정보는 Kaspersky XDR 도움말을 참조하십시오.

Kaspersky Security Center 연결 파라미터

파라미터	유형	설명
`kscHost`	`string`	Kaspersky Security Center 중앙 관리 서버 주소. 필수 파라미터.
`kscPort`	`int`	중앙 관리 서버 연결 포트. 필수 파라미터.
`kscCert`	`string`	Kaspersky Security Center 중앙 관리 서버 연결을 위한 인증서 파일 경로입니다. 이 파라미터의 기본값은 `False` 입니다.
`kscUser`	`string`	사용자 계정 이름. 필수 파라미터.
`kscPassword`	`string`	사용자 계정 암호. 필수 파라미터.

예

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

사용자 계정 데이터는 보호되지 않으므로 이러한 작업만 수행할 별도의 전용 사용자가 필요합니다.

파일 가져오기 – getFile

파일 가져오기 작업 설정

파라미터	유형	설명
md5hash	`string`	가져올 파일의 MD5 해시입니다.
sha256hash	`string`	가져올 파일의 SHA256 해시입니다.
path	`string`	가져올 파일의 경로입니다.

예

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

파일 삭제 – deleteFile

파일 삭제 작업 설정

파라미터	유형	설명
md5hash	`string`	삭제할 파일의 MD5 해시입니다.
sha256hash	`string`	삭제할 파일의 SHA256 해시입니다.
path	`string`	삭제할 파일의 경로입니다.
searchInSubfolders?	`boolean`	하위 폴더에서 삭제할 파일을 검색합니다.

예

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

격리 저장소로 파일 이동 – quarantineFile

격리 저장소로 파일 이동 작업 설정

파라미터	유형	설명
md5hash	string	격리할 파일의 MD5 해시입니다.
sha256hash	string	격리할 파일의 SHA256 해시입니다.
path	string	격리할 파일의 경로입니다.

예

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

IOC 검사 – iocScan

IOC 검사 작업 설정

파라미터	유형	설명
ioc	string	검사에 사용할 IOC 파일이 있는 ZIP 압축파일의 경로입니다.
isolateHost	boolean	침해지표가 탐지될 때 네트워크에서 컴퓨터를 격리하여 위협 확산을 방지합니다.
scanCriticalAreas	boolean	침해지표 탐지 시 *중요 영역 검사* 작업을 실행합니다.
quarantineObject	boolean	침해지표가 탐지되면 악성 개체를 삭제합니다. 개체를 삭제하기 전에 Kaspersky Endpoint Security는 나중에 개체를 복원해야 할 때를 대비하여 백업 복사본을 생성합니다. Kaspersky Endpoint Security는 백업 복사본을 격리 저장소로 이동합니다.

예

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

프로세스 시작 – startProcess

프로세스 시작 작업 설정

파라미터	유형	설명
executablePath	string	프로세스를 시작하는 데 사용되는 실행 파일의 경로입니다.
arguments?	string	프로세스 시작을 위한 추가 명령줄 인수입니다.
workingFolder?	string	프로세스의 작업 폴더 경로입니다.

예

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

프로세스 종료 – terminateProcess

프로세스 종료 작업 설정

파라미터	유형	설명
md5hash	string	프로세스를 종료하려는 파일의 MD5 해시입니다.
sha256hash	string	프로세스를 종료하려는 파일의 SHA256 해시입니다.
path	string	삭제할 파일의 경로입니다.
caseSensitive	boolean	파일을 검색할 때 대소문자를 구분합니다.

예

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

컴퓨터 네트워크 격리 – isolateHost

컴퓨터 네트워크 격리 설정

파라미터	유형	설명
`action`	`string`	네트워크 격리의 작업 모드입니다.

예

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

실행 방지 – preventExecution

실행 방지 알림

파라미터	유형	설명
hash	`string`	실행을 방지할 파일의 MD5 해시입니다.
path	`string`	실행을 방지할 파일의 경로입니다.
caseSensitive	`boolean`	파일을 검색할 때 대소문자를 구분합니다.

예

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

악성 코드 검사 – onDemandScan

악성 코드 검사 작업 설정

파라미터	유형	설명
path	`string`	사용자 지정 검사를 위한 파일 및 폴더를 공백으로 구분한 목록입니다.
recursive	`boolean`	재귀 검사 모드.

파라미터	유형	설명
type	`number`	검사 범위.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

예

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

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.

Adobe, Acrobat, Flash, Reader 및 Shockwave는 미국 및/또는 기타 국가에서 Adobe의 등록 상표 또는 상표입니다.

Amazon, AWS, Amazon Web Services는 Amazon.com, Inc. 또는 그 계열사의 상표입니다.

Apple, FireWire, iTunes, Mac 및 Safari는 Apple Inc.의 상표입니다.

Arm은 미국 및/또는 기타 국가에서 Arm Limited(또는 자회사)의 등록 상표입니다.

AutoCAD는 미국 및 기타 국가에 있는 Autodesk, Inc. 및/또는 그 자회사/제휴사의 상표 또는 등록 상표입니다.

Bluetooth 단어, 마크 및 로고는 Bluetooth SIG, Inc.의 소유입니다.

Borland는 Borland Software Corporation의 상표 또는 등록 상표입니다.

Cisco, Cisco AnyConnect, IOS는 미국 및 기타 특정 국가에서 Cisco Systems, Inc. 및/또는 그 계열사의 등록 상표 또는 상표입니다.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop, XenServer는 미국 및/또는 기타 국가에서 Cloud Software Group, Inc. 및/또는 그 자회사의 등록 상표 또는 상표입니다.

Cloudflare, Cloudflare Workers 및 Cloudflare 로고는 미국 및 기타 관할 지역에서 Cloudflare, Inc.의 상표 및/또는 등록 상표입니다.

Core는 Intel Corporation 또는 그 자회사의 상표입니다.

dBase는 dataBased Intelligence, Inc의 상표입니다.

Dell Technologies, Dell, EMC 및 기타 상표는 Dell Inc. 또는 그 자회사의 상표입니다.

Docker 및 Docker 로고는 미국 및/또는 기타 관할 지역에서 Docker, Inc.의 상표 또는 등록 상표입니다. Docker, Inc. 및 기타 당사자는 여기에 사용된 다른 용어에 대한 상표권도 보유할 수 있습니다.

ESET는 ESET spol. s r.o. 또는 해당 ESET 법인의 상표 또는 등록 상표입니다.

Foxit은 Foxit Corporation의 등록 상표입니다.

Radmin는 Famatech의 등록 상표입니다.

Google, Android, Google Public DNS, Google Chrome 및 Google는 Google LLC의 상표입니다.

HUAWEI, FusionCompute 및 FusionSphere는 Huawei Technologies Co., Ltd.의 상표입니다.

ICQ는 ICQ LLC의 상표 및/또는 서비스 마크입니다.

Intel은 Intel Corporation 또는 그 자회사의 상표입니다.

IBM은 전 세계 다양한 관할권에 등록된 International Business Machines Corporation의 상표입니다.

Lenovo 및 Lenovo ThinkPad는 미국 및/또는 그 외 지역에 있는 Lenovo의 상표입니다.

Linux는 미국 및 기타 국가에서 Linus Torvalds의 등록 상표입니다.

Logitech은 미국 및/또는 기타 국가에서 Logitech의 등록 상표 또는 상표입니다.

LogMeIn Pro와 Remotely Anywhere은 LogMeIn, Inc의 상표입니다.

Mail.ru는 Mail.Ru, LLC의 등록 상표입니다.

McAfee는 미국 및/또는 기타 국가에서 McAfee LLC 또는 자회사의 상표 또는 등록 상표입니다.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server 및 Windows Store는 Microsoft 그룹의 상표입니다.

Mozilla, Firefox, Thunderbird는 미국 및 기타 국가에서 Mozilla Foundation의 상표입니다.

NetApp은 미국 및/또는 기타 국가에서 NetApp, Inc의 상표 또는 등록 상표입니다.

OpenSSL은 OpenSSL Software Foundation의 등록 상표입니다.

OpenStack은 미국 및 기타 국가에서 OpenStack Foundation의 등록 상표입니다.

Oracle, Java와 JavaScript는 Oracle 및/또는 그 제휴사의 등록 상표입니다.

Python은 Python Software Foundation의 상표 또는 등록 상표입니다.

Realtek은 Realtek Semiconductor Corporation의 등록 상표입니다.

SAMSUNG은 미국 또는 기타 국가에서 SAMSUNG의 상표입니다.

Thawte는 미국 및 기타 국가에서 Symantec Corporation 또는 그 계열사의 상표 또는 등록 상표입니다.

Trend Micro는 Trend Micro Incorporated의 상표 또는 등록 상표입니다.

VERISIGN은 미국 및 기타 국가에서 등록된 상표이거나 VeriSign, Inc. 및 그 자회사의 미등록 상표입니다.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools, VMware vSphere는 미국 및 기타 국가에서 VMware, Inc.의 등록 상표 및/또는 상표입니다.