kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 for Windows

목차

Kaspersky Endpoint Security 10 Service Pack 2 for Windows 정보
- 새로운 기능
- 배포 패키지
- 컴퓨터 보호 구성
- 하드웨어 및 소프트웨어 요구 사항

애플리케이션 설치 및 제거
- 애플리케이션 설치
  - 애플리케이션 설치 방법 정보
  - 설치 마법사를 사용하여 애플리케이션 설치
    - 1 단계. 컴퓨터가 설치 요구 사항을 충족하는지 확인
    - 2 단계. 설치 절차의 시작 페이지
    - 3 단계. 라이센스 동의서 정보 보기
    - 4 단계. 설치 유형 선택
    - 5 단계. 설치할 애플리케이션 구성요소 선택
    - 6 단계. 대상 폴더 선택
    - 7 단계. 바이러스 검사에서 예외할 대상 추가
    - 8 단계. 애플리케이션 설치 준비
    - 9 단계. 애플리케이션 설치
  - 명령줄에서 애플리케이션 설치
  - System Center Configuration Manager를 사용하여 애플리케이션 원격 설치
  - setup.ini 파일 설치 설정 설명
  - 초기 구성 마법사
    - 애플리케이션 활성화
    - 활성화코드를 사용하여 활성화
    - 라이센스 키 파일을 사용하여 활성화
    - 활성화할 기능 선택
    - 활성화 완료
    - 운영 체제 분석
    - 애플리케이션 초기 구성 완료
    - Kaspersky Security Network 정책
  - 이전 애플리케이션 버전의 업그레이드 방법 정보
- 애플리케이션 제거
  - 애플리케이션 제거 방법 정보
  - 설치 마법사를 사용하여 애플리케이션 제거
    - 1 단계. 나중에 사용하기 위해 애플리케이션 데이터 저장
    - 2 단계. 애플리케이션 제거 확인
    - 3 단계. 애플리케이션 제거. 제거 완료
  - 명령줄을 통한 애플리케이션 제거
  - 인증 에이전트의 테스트 작업 후 남은 개체 및 데이터 제거하기

애플리케이션 인터페이스
- 작업 표시줄 알림 영역의 애플리케이션 아이콘
- 애플리케이션 아이콘 마우스 오른쪽 메뉴
- 메인 애플리케이션 창
- 애플리케이션 설정 구성 탭
- 애플리케이션 보호 및 제어 탭

애플리케이션 라이센스

최종 사용자 라이센스 계약서 정보
라이센스 정보
라이센스 인증서 정보
서브스크립션 정보
활성화코드 정보
키 정보
라이센스 키 파일 정보
데이터 제공 정보
라이센스 정보 보기
라이센스 구입
라이센스 갱신
서브스크립션 갱신
서비스 제공 업체의 웹사이트 방문
애플리케이션 활성화 방법 정보
활성화 마법사를 통해 애플리케이션 활성화
명령줄을 통한 애플리케이션 활성화
애플리케이션 시작 및 중지
애플리케이션 자동 시작 사용 및 중지
애플리케이션 수동 시작 및 중지
컴퓨터 보호 및 제어 일시 중지 및 다시 시작
컴퓨터 파일 시스템 보호. 파일 안티 바이러스
파일 안티 바이러스 정보
파일 안티 바이러스 작동 및 중지
파일 안티 바이러스 자동 일시 중지
파일 안티 바이러스 구성
보안 레벨 변경
감염된 파일에 수행할 파일 안티 바이러스 처리 방법 변경
파일 안티 바이러스의 보호 영역 편집
파일 안티 바이러스에 휴리스틱 분석기 사용
파일 안티 바이러스 작업에 검사 기술 사용
파일 검사 최적화
복합 파일 검사
검사 모드 변경
이메일 보호. 메일 안티 바이러스
메일 안티 바이러스 정보
메일 안티 바이러스 작동 및 중지
메일 안티 바이러스 구성
이메일 보안 레벨 변경
감염된 이메일 메시지에 수행할 처리 방법 변경
메일 안티 바이러스의 보호 영역 편집
이메일 메시지에 첨부된 복합 파일 검사
이메일 메시지의 첨부파일 필터링
Microsoft Office Outlook의 이메일 검사
Outlook의 메일 검사 구성
Kaspersky Security Center를 사용해 메일 검사 구성
인터넷에서 컴퓨터 보호. 웹 안티 바이러스
웹 안티 바이러스 정보
웹 안티 바이러스 작동 및 중지

- 웹 안티 바이러스 구성
  - 웹 트래픽 보안 레벨 변경
  - 웹 트래픽의 위험 개체에 수행할 처리 방법 변경
  - 피싱/악성 웹 주소 데이터베이스에 대한 웹 안티 바이러스의 URL 검사
  - 웹 안티 바이러스에 휴리스틱 분석기 사용
  - 신뢰하는 URL 목록 편집
- IM 클라이언트의 트래픽 보호: 메신저 안티 바이러스
  - 메신저 안티 바이러스 정보
  - 메신저 안티 바이러스 작동 및 중지
  - 메신저 안티 바이러스 구성
    - 메신저 안티 바이러스의 보호 영역 생성
    - 메신저 안티 바이러스에서 악성 및 피싱 URL 데이터베이스와 비교하여 URL 검사
- 시스템 감시기
  - 시스템 감시기 정보
  - 시스템 감시기 작동 및 중지
  - 시스템 감시기 구성
    - 익스플로잇 보호 작동 또는 중지
    - 프로그램에서 악성 활동이 탐지되는 경우에 수행해야 하는 조치 선택
    - 치료 중 악성 코드의 동작 롤백 작동 또는 중지
- 방화벽
  - 방화벽 정보
  - 방화벽 작동 또는 중지
  - 네트워크 규칙 정보
  - 네트워크 연결 상태 정보
  - 네트워크 연결 상태 변경
  - 네트워크 패킷 규칙 관리
    - 네트워크 패킷 규칙 만들기 및 편집
    - 네트워크 패킷 규칙 작동 또는 중지
    - 네트워크 패킷 규칙에 대한 방화벽 동작 변경
    - 네트워크 패킷 규칙의 우선 순위 변경
  - 애플리케이션 네트워크 규칙 관리
    - 애플리케이션 네트워크 규칙 만들기 및 편집
    - 애플리케이션 네트워크 규칙 사용 및 중지
    - 애플리케이션 네트워크 규칙에 대한 방화벽 동작 변경
    - 애플리케이션 네트워크 규칙의 우선 순위 변경
  - 네트워크 모니터
    - 네트워크 모니터 정보
    - 네트워크 모니터 시작
- 네트워크 공격 차단
  - 네트워크 공격 차단 정보
  - 네트워크 공격 차단 작동 및 중지
  - 네트워크 공격 차단 설정
    - 공격 컴퓨터를 차단하는 데 사용되는 설정 편집
    - 차단에서 예외할 주소 구성
- BadUSB 공격 차단
  - BadUSB 공격 차단 정보
  - BadUSB 공격 차단 구성요소 설치
  - BadUSB 공격 차단 사용 및 중지

- 인증 시 화상 키보드 사용 허용 및 금지
- 키보드 인증

애플리케이션 시작 제어
- 애플리케이션 시작 제어 정보
- 애플리케이션 시작 제어 작동 및 중지
- 애플리케이션 시작 제어 기능 제한
- 애플리케이션 시작 제어 규칙 정보
- 애플리케이션 시작 제어 규칙 관리
  - 애플리케이션 시작 제어 규칙 추가 및 편집
  - 애플리케이션 시작 제어 규칙의 작동 조건 추가
  - 애플리케이션 시작 제어 규칙의 상태 변경
  - 애플리케이션 시작 제어 규칙 테스트
- 애플리케이션 시작 제어 메시지 템플릿 편집
- 애플리케이션 시작 제어 작동 모드 정보
- 애플리케이션 시작 제어 모드 선택
- Kaspersky Security Center를 사용해 애플리케이션 시작 제어 규칙 관리
  - 사용자 컴퓨터에 설치된 애플리케이션에 대한 정보 수집
  - 애플리케이션 카테고리 만들기
  - Kaspersky Security Center를 사용해 애플리케이션 시작 제어 규칙 만들기
  - Kaspersky Security Center를 사용해 애플리케이션 시작 제어 규칙의 상태 변경

애플리케이션 권한 제어
- 애플리케이션 권한 제어 정보
- 오디오 및 비디오 장치 제어 제한
- 애플리케이션 권한 제어 작동 및 중지
- 애플리케이션 제어 그룹 관리
  - 제어 그룹에 애플리케이션을 지정하는 설정 구성
  - 제어 그룹 수정
  - Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션에 대한 제어 그룹 선택
- 애플리케이션 제어 규칙 관리
  - 제어 그룹 및 애플리케이션 그룹에 대한 애플리케이션 제어 규칙 변경
  - 애플리케이션 제어 규칙 편집
  - Kaspersky Security Network 데이터베이스에서 애플리케이션 제어 규칙 다운로드 및 업데이트 중지하기
  - 부모 프로세스의 제한 설정 상속 중지
  - 애플리케이션 제어 규칙에서 특정 애플리케이션 동작 예외
  - 오래된 애플리케이션 제어 규칙 삭제
- 운영 체제 리소스 및 중요한 데이터 보호
  - 보호되는 리소스의 카테고리 추가
  - 보호되는 리소스 추가
  - 리소스 보호 중지

취약점 감시
- 취약점 감시 정보
- 취약점 감시 작동 및 중지

매체 제어
- 장치 제어 정보
- 매체 제어 사용 및 중지
- 장치 접근 규칙 및 연결 버스 정보
- 신뢰하는 장치 정보
- 장치 접근에 대한 표준 결정 사항

장치 사용 규칙 편집
이벤트 로그에 레코드 추가 또는 로그에서 레코드 예외
신뢰하는 목록에 Wi-Fi 네트워크 추가
연결 버스 접근 규칙 편집
신뢰하는 장치와 관련된 처리 방법
애플리케이션 인터페이스에서 신뢰하는 목록에 장치 추가
장치 모델 또는 ID를 기반으로 신뢰하는 목록에 장치 추가
장치 ID의 마스크를 기반으로 신뢰하는 목록에 장치 추가
신뢰하는 장치로의 사용자 접근 구성
신뢰하는 장치 목록에서 장치 제거
매체 제어 메시지 템플릿 편집
차단된 장치에 대한 접근 권한 획득
Kaspersky Security Center를 사용하여 차단된 장치에 접근하기 위한 키 만들기
웹 제어
웹 제어 정보
웹 제어 사용 및 중지
웹 리소스 컨텐츠 카테고리
웹 리소스 접근 규칙 정보
웹 리소스 접근 규칙과 관련된 처리 방법
웹 리소스 접근 규칙 추가 및 편집
웹 리소스 접근 규칙에 우선 순위 지정
웹 리소스 접근 규칙 테스트
웹 리소스 접근 규칙 사용 및 중지
애플리케이션의 이전 버전에서 웹 리소스 접근 규칙 마이그레이션
웹사이트 주소 목록 내보내기 및 가져오기
웹 리소스 주소 마스크 편집
웹 제어 메시지 템플릿 편집
KATA 엔드포인트 센서
KATA 엔드포인트 센서 정보
KATA 엔드포인트 센서 구성요소 작동 및 중지
데이터 암호화
Kaspersky Security Center 정책의 암호화 설정 표시
데이터 암호화 정보
암호화 기능 제한
암호화 알고리즘 변경
Single Sign-On(SSO) 기술 사용
파일 암호화 관련 특별 고려 사항
로컬 컴퓨터 드라이브의 파일 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
암호화된 패키지 생성
암호화된 패키지 압축 해제
이동식 드라이브 암호화
이동식 드라이브 암호화 시작
이동식 드라이브에 대한 암호화 규칙 추가

이동식 드라이브에 대한 암호화 규칙 편집
이동식 드라이브의 암호화된 파일 접근을 위한 휴대용 모드 설정
이동식 드라이브의 복호화
하드 드라이브 암호화
하드 드라이브 암호화 정보
Kaspersky 디스크 암호화 기술을 사용해 하드 드라이브 암호화
BitLocker 드라이브 암호화 기술을 사용한 하드 드라이브 암호화
암호화에서 예외할 하드 드라이브의 목록 작성
하드 드라이브 복호화
인증 에이전트 관리
인증 에이전트에서 토큰 및 스마트 카드 사용
인증 에이전트 도움말 메시지 편집
인증 에이전트 도움말 메시지의 제한적 문자 지원
인증 에이전트 추적 레벨 선택
인증 에이전트 계정 관리
인증 에이전트 계정 생성을 위한 명령 추가
인증 에이전트 계정 편집 명령 추가
인증 에이전트 계정 삭제를 위한 명령 추가
인증 에이전트 계정 자격 증명 복원
사용자의 인증 에이전트 계정 자격 증명 복원 요청에 응답
데이터 암호화 상세 정보 보기
암호화 상태 정보
암호화 상태 보기
Kaspersky Security Center의 상세 정보에서 암호화 통계 보기
로컬 컴퓨터 드라이브의 파일 암호화 오류 보기
데이터 암호화 리포트 보기
제한된 파일 암호화 기능을 사용하여 암호화된 파일 관리
Kaspersky Security Center에 연결하지 않고 암호화된 파일에 접근
Kaspersky Security Center에 연결하지 않고 암호화된 파일에 대해 사용자 접근 권한 부여
암호화된 파일 접근 메시지 템플릿 편집
암호화된 장치에 접근할 수 없는 경우 장치 사용
애플리케이션 인터페이스를 통해 암호화된 장치 접근 권한 얻기
사용자에게 암호화된 장치 접근 권한 부여
사용자에게 BitLocker 기술로 암호화된 하드 드라이브에 대한 복구 키 제공
복원 유틸리티의 실행 파일 생성
복원 유틸리티를 사용하여 암호화된 장치에 있는 데이터 복원하기
사용자의 암호화된 장치에 저장된 데이터 복원 요청에 응답
운영 체제에 장애가 발생한 후 암호화된 데이터에 대한 접근 복원
운영 체제 응급 복구 디스크 만들기
네트워크 보호
네트워크 보호 정보
네트워크 트래픽 감시의 설정 구성
모든 네트워크 포트의 감시 작동
감시하는 네트워크 포트 목록 만들기
모든 네트워크 포트에 대한 감시를 받을 애플리케이션 목록 만들기
데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트
데이터베이스 및 애플리케이션 모듈 업데이트 정보
업데이트 경로 정보

- 업데이트 설정 구성
  - 업데이트 경로 추가
  - 업데이트 서버 영역 선택
  - 공유 폴더에서 업데이트 구성
  - 업데이트 작업 스케줄 선택
  - 다른 사용자 계정 권한으로 업데이트 작업 시작
  - 애플리케이션 모듈 업데이트 구성
- 업데이트 작업 시작 및 중지
- 마지막으로 성공한 업데이트로 롤백
- 프록시 서버 설정 구성

컴퓨터 검사
- 검사 작업 정보
- 검사 작업 시작 또는 중지
- 검사 작업 설정 구성
  - 보안 레벨 변경
  - 감염된 파일에 수행할 처리 방법 변경
  - 검사할 개체 목록 생성
  - 검사할 파일 유형 선택
  - 파일 검사 최적화
  - 복합 파일 검사
  - 검사 방법 사용
  - 검사 기술 사용
  - 검사 작업 스케줄 선택
  - 다른 사용자 계정으로 검사 작업 시작
  - 이동식 장치가 컴퓨터에 연결될 때 검사
- 처리 안 된 파일 처리
  - 처리 안 된 파일 정보
  - 처리 안 된 파일의 목록 관리
    - 처리 안 된 파일에 대한 사용자 지정 검사 작업 시작
    - 처리 안 된 파일의 목록에서 파일 삭제

취약점 검사
- 실행 중인 애플리케이션의 취약점 정보 확인
- 취약점 검사 작업 정보
- 취약점 검사 작업 시작 또는 중지
- 취약점 검사 설정 구성
  - 취약점 검사 영역 만들기
  - 취약점 검사 작업 스케줄 선택
  - 다른 사용자 계정 권한으로 취약점 검사 작업 시작
- 취약점 목록 관리
  - 취약점 목록 정보
  - 취약점 검사 작업 다시 시작
  - 취약점 수정
  - 취약점 목록의 항목 숨장치
  - 심각도 레벨을 기준으로 취약점 목록 필터링
  - 수정 및 숨김 상태 값으로 취약점 목록 필터링

애플리케이션 모듈 무결성 확인
- 무결성 검사 작업 정보
- 무결성 검사 작업 시작 또는 중지

무결성 검사 작업 스케줄 선택
리포트 관리
리포트 관리 원칙
리포트 설정 구성
최대 리포트 저장 기간 구성
리포트 파일의 최대 크기 구성
리포트 보기
리포트에 이벤트 정보 표시
파일에 리포트 저장
리포트 파일 삭제
알림 서비스
Kaspersky Endpoint Security 알림 정보
알림 서비스 구성
이벤트 로그 설정 구성
알림 표시 및 전달 구성
알림 영역의 애플리케이션 상태에 대한 경고 표시 구성
격리 및 백업 저장소 관리
격리 및 백업 저장소 정보
격리 및 백업 저장소 설정 구성
격리 저장소 파일과 백업 저장소 파일 복사본의 최대 저장 기간 구성
격리 및 백업 저장소의 최대 크기 구성
격리 저장소 관리
업데이트 후 격리 저장소의 파일 검사 작동 및 중지
격리 저장소 파일에 대한 사용자 지정 검사 작업 시작
격리 저장소에서 파일 복원
격리 저장소에서 파일 삭제
백업 저장소 관리
백업 저장소에서 파일 복원
백업 저장소에서 파일의 백업 복사본 삭제
고급 애플리케이션 설정
구성 파일 만들기 및 사용
신뢰구역
신뢰 구역 정보
검사 예외 생성
검사 예외 수정
검사 예외 삭제
검사 예외 사용 및 중지
신뢰하는 애플리케이션 목록 편집
신뢰하는 애플리케이션 목록의 애플리케이션에 대한 신뢰 구역 규칙 사용 및 중지
신뢰하는 시스템 인증서 저장소 사용
Kaspersky Endpoint Security 자기-보호 기능
Kaspersky Endpoint Security 자기-보호 기능 정보
자기-보호 기능 작동 또는 중지
원격 제어 방역 작동 또는 중지
원격 관리 애플리케이션 지원
Kaspersky Endpoint Security의 성능 및 다른 애플리케이션과의 호환성
Kaspersky Endpoint Security의 성능 및 다른 애플리케이션과의 호환성 정보
탐지 가능한 개체의 유형 선택

워크스테이션용 고급 치료(자동 재부팅) 기술 사용 또는 중지
파일 서버용 고급 치료 기술 작동 또는 중지
절전 모드 작동 또는 중지
다른 애플리케이션에 컴퓨터 리소스 우선권 할당 작동 또는 중지
암호 보호
Kaspersky Endpoint Security 접근 제한 정보
암호 보호 사용 및 사용 안 함
Kaspersky Endpoint Security 접근 암호 수정
임시 암호 사용 정보
Kaspersky Security Center 관리 콘솔을 사용하여 임시 암호 만들기
Kaspersky Endpoint Security 인터페이스에 임시 암호 적용
Kaspersky Security Center를 통한 애플리케이션 원격 관리
Kaspersky Security Center를 통한 애플리케이션 관리 정보
다른 버전의 관리 플러그인으로 작업 시 특별 고려 사항
클라이언트 컴퓨터에서 Kaspersky Endpoint Security 시작 및 중지
Kaspersky Endpoint Security 설정 구성
작업 관리
Kaspersky Endpoint Security의 작업 정보
작업 관리 모드 구성
로컬 작업 만들기
그룹 작업 만들기
장치 조회 작업 만들기
작업 시작, 중지, 일시 중지 및 다시 시작
작업 설정 편집
정책 관리
정책 정보
정책 만들기
정책 설정 편집
Kaspersky Security Center 정책에 표시할 설정 선택
Kaspersky Security Center 서버로 사용자 메시지 전송
Kaspersky Security Center 이벤트 저장소에서 사용자 메시지 확인
Kaspersky Security Network 참여
Kaspersky Security Network 참여 정보
Kaspersky Security Network 사용 및 중지
Kaspersky Security Network 연결 확인
Kaspersky Security Network 내 파일의 평판 확인
Kaspersky Security Network로 더욱 향상된 보호 제공
애플리케이션에 대한 정보 출처
기술 지원 서비스에 문의
기술 지원을 받는 방법
전화 기술 지원
Kaspersky CompanyAccount를 통해 기술 지원 받기
기술 지원에 필요한 정보 수집
추적 파일 생성
추적 파일의 내용 및 저장
Kaspersky로 덤프 및 추적로그 파일의 전송 활성 또는 비활성
기술 지원 서버로 파일 전송
덤프 파일 및 추적 파일 보호 사용 및 중지

용어집
- Network Agent 커넥터
- OLE 개체
- 감염 가능성이 있는 파일
- 감염 의심 파일
- 감염된 파일
- 검사 범위
- 격리 저장소
- 격리 저장소로 파일 이동
- 관리 그룹
- 네트워크 서비스
- 네트워크 에이전트
- 라이센스 인증서
- 백업 저장소
- 보호 범위
- 블랙리스트 주소
- 시그니처 분석
- 신뢰하는 플랫폼 모듈
- 악성 웹 주소 데이터베이스
- 안티 바이러스 데이터베이스
- 압축 파일
- 애플리케이션 모듈
- 애플리케이션 설정
- 업데이트
- 익스플로잇
- 인증 에이전트
- 인증서
- 인증서 발급자
- 인증서 주체
- 인증서 지문
- 작업
- 작업 설정
- 정규화된 형태의 웹 리소스 주소
- 중앙 관리 서버
- 추가 라이센스 키
- 치료
- 파일 마스크
- 패치
- 피싱
- 피싱 웹 주소 데이터베이스
- 허위 경보
- 활성 라이센스 키
- 휴대용 파일 관리자
- 휴리스틱 분석

타사 코드에 대한 정보

상표 고지

Kaspersky Endpoint Security 10 Service Pack 2 for Windows 정보

이 섹션은 Kaspersky Endpoint Security의 기능, 구성요소 및 배포 키트를 안내하고 Kaspersky Endpoint Security의 하드웨어 및 소프트웨어 요구 사항 목록을 보여줍니다.

새로운 기능

Kaspersky Endpoint Security 10 Service Pack 2 for Windows에는 다음과 같은 기능 및 개선 사항이 추가되었습니다:

1. 애플리케이션 시작 제어:
   - 서버 운영 체제를 지원합니다.
   - DLL 모듈 및 드라이버 다운로드를 제어합니다.
   - 인벤토리 작업에 있는 개체(DLL 모듈 및 스크립트 파일) 목록을 관리합니다
   - 새 기준(디지털 서명 인증서의 특성별)에 따라 개체를 제어합니다.
   - 차단된 애플리케이션의 테스트 시작 시 리포트를 생성합니다.
   - 애플리케이션 시작 제어의 두 가지 작동 모드를 지원합니다: "블랙리스트(차단 목록)" 및 "화이트리스트(허용 목록)".
   - 개체 제어 및 인벤토리 등록에 SHA256 해시를 사용합니다.
   - PowerShell 인터셉터에서의 스크립트 실행을 제어합니다.
   - 신뢰하는 시스템 인증서 저장소를 사용합니다.
2. Microsoft BitLocker 관리를 사용해 Microsoft의 BitLocker 기술을 사용하여 하드 드라이브를 암호화합니다:
   - 원격으로 암호화를 관리합니다.
   - 암호화된 장치를 모니터링합니다.
   - 장치 암호화 리포트를 생성합니다.
   - 암호화된 장치에 대한 접근을 복원합니다.
3. Kaspersky 디스크 암호화:
   - 인증 에이전트의 사전 부팅 환경에서 보안 키보드를 사용한 자격 증명 입력 지원.
   - 장치에서 사용한 디스크 공간만 암호화하는 암호화 모드 지원.
   - 태블릿 암호화 지원(MS Surface 3 및 4 버전).
4. 애플리케이션 권한 제어:
   - 오디오 녹음/비디오 녹화 장치에 대한 애플리케이션 접근을 제어합니다.

5. 웹 제어:

   - 추가 웹 리소스 카테고리에 대한 웹 리소스 접근 규칙을 구성합니다.

6. 매체 제어:

   - USB 장치의 파일 삭제 및 장치에 파일 저장과 관련된 이벤트를 기록합니다.
   - 이름, 암호화 유형 및 인증 유형과 같은 설정을 기준으로 신뢰하는 Wi-Fi 네트워크 목록을 생성합니다.
   - CD/DVD 디스크의 파일 읽기 및 쓰기 작업에 대한 사용자 접근 권한을 관리합니다.

7. 메일 안티 바이러스:

   - 메일 안티 바이러스에서 검사하도록 압축 파일 내 특정 파일 형식을 삭제 및 이름을 변경할 수 있습니다.

8. Kaspersky Security Network:

   - Kaspersky Endpoint Security 리포트 및 Kaspersky Security Center 리포트의 개체 처리 방법에 관한 결정의 근거로 KSN을 표시합니다.
   - 선택한 파일의 평판에 관해 KSN에 쿼리를 보냅니다.
   - Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터에 대한 KSN 서버의 이용 가능 여부가 표시됩니다.

배포 패키지

Kaspersky Endpoint Security 배포 패키지에는 다음 파일이 포함되어 있습니다:

- 이용 가능한 방법을 활용한 애플리케이션 설치에 필요한 파일:
- 애플리케이션 설치 과정에서 사용된 업데이트 패키지 파일.
- Kaspersky Security Center를 통해 Kaspersky Endpoint Security 관리 플러그인을 설치하기 위한 klcfginst.msi 파일.
- Kaspersky Security Network 참가 정책 조건을 볼 수 있는 ksn_<언어 ID>.txt 파일.
- 최종 사용자 라이센스 계약서 내용을 확인할 수 있는 license.txt 파일.
- 비-호환 소프트웨어 목록이 담긴 incompatible.txt 파일.
- 배포 패키지 내부 설정이 포함된 installer.ini 파일.

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

파일에 접근하려면 배포 패키지를 압축 해제해야 합니다.

컴퓨터 보호 구성

Kaspersky Endpoint Security는 다양한 유형의 보안위협, 네트워크 및 피싱 공격에 대해 포괄적인 컴퓨터 보호 기능을 제공합니다.

각각의 보안위협은 전용 구성요소에서 처리합니다. 구성요소는 개별적으로 작동 또는 중지하고 설정을 구성할 수 있습니다.

애플리케이션 구성요소에서 제공하는 실시간 보호 기능 외에 컴퓨터에 바이러스 및 기타 보안위협이 있는지 정기적으로 *검사*하는 것이 좋습니다. 그러면 낮은 보안 레벨 설정이나 다른 이유로 인해 보호 구성요소에서 탐지하지 못하는 악성 코드가 확산되는 것을 막을 수 있습니다.

Kaspersky Endpoint Security를 최신 상태로 유지하려면 애플리케이션에서 사용하는 데이터베이스와 모듈을 *업데이트*해야 합니다. 기본적으로 애플리케이션은 자동으로 업데이트되지만 필요한 경우 데이터베이스 및 애플리케이션 모듈을 수동으로 업데이트할 수도 있습니다.

제어 구성요소에는 다음과 같은 애플리케이션 구성요소가 있습니다:

- **애플리케이션 시작 제어**. 이 구성요소는 애플리케이션을 시작하고자 하는 사용자 시도를 추적하고 애플리케이션 시작을 규정합니다.

- **애플리케이션 권한 제어**. 이 구성요소는 운영 체제에서 애플리케이션의 동작을 등록하고 특정 애플리케이션의 제어 그룹에 따라 애플리케이션 동작을 규정합니다. 각 애플리케이션 그룹에는 특정 규칙이 지정됩니다. 이러한 규칙은 사용자 데이터 및 운영 체제 리소스에 대한 애플리케이션 접근을 규정합니다. 이러한 데이터에는 사용자 파일(내 문서 폴더, 쿠키, 사용자 활동 정보), 자주 사용하는 애플리케이션에 대한 설정 및 중요한 정보가 포함된 파일, 폴더 및 레지스트리 키가 포함됩니다.

- **취약점 감시**. 취약점 감시 구성요소는 사용자 컴퓨터에서 시작되었거나 실행 중인 애플리케이션에 대한 실시간 취약점 검사를 실행합니다.

- **매체 제어**. 이 구성요소를 사용하면 데이터 저장 장치(예: 하드 드라이브, 이동식 드라이브, 테이프 드라이브, CD/DVD 디스크), 데이터 전송 장비(예: 모뎀), 정보를 하드 카피로 변환하는 장비(예: 프린터), 장치를 컴퓨터에 연결하는 인터페이스(예: USB, Bluetooth, Infrared) 등 대한 접근을 유연하게 제한할 수 있습니다.

- **웹 제어**. 이 구성요소를 사용하면 다른 사용자 그룹에 대한 웹 리소스 접근을 유연하게 제한할 수 있습니다.

제어 구성요소는 다음과 같은 규칙을 기반으로 작동합니다:

- 애플리케이션 시작 제어는 애플리케이션 시작 제어 규칙을 사용합니다.

- 애플리케이션 권한 제어는 애플리케이션 제어 규칙을 사용합니다.

- 매체 제어는 장치 접근 규칙 및 연결 버스 접근 규칙을 사용합니다.

- 웹 제어는 웹 리소스 접근 규칙을 사용합니다.

보호 구성요소는 다음과 같습니다:

- **파일 안티 바이러스**. 이 구성요소는 컴퓨터 파일 시스템이 감염되지 않도록 보호합니다. 파일 안티 바이러스는 Kaspersky Endpoint Security와 함께 시작되어 컴퓨터 메모리에 상주하며 컴퓨터 및 모든 연결된 드라이버에서 열리거나 저장 또는 시작되는 모든 파일을 검사합니다. 파일 안티 바이러스는 모든 파일 접근 시도를 가로채고 바이러스 및 기타 보안 위협이 있는지 파일을 검사합니다.

- **시스템 감시기**. 이 구성요소는 컴퓨터의 애플리케이션 동작을 기록하고 보다 효율적인 보호를 위해 이 정보를 다른 구성요소에 제공합니다.

- **메일 안티 바이러스**. 이 구성요소는 보내고 받는 이메일 메시지에 바이러스 및 기타 보안위협이 있는지 검사합니다.

- **웹 안티 바이러스**. 이 구성요소는 HTTP 및 FTP 프로토콜을 통해 사용자 컴퓨터에 도착하는 트래픽을 검사하고 URL이 악성 웹 주소나 피싱 웹 주소로 등록된 것인지 확인합니다.

- **메신저 안티 바이러스**. 이 구성요소는 IM 프로토콜을 통해 컴퓨터에 도착하는 트래픽을 검사합니다. 구성요소 덕분에 여러 IM 클라이언트를 안전하게 사용할 수 있습니다.

- **방화벽**. 이 구성요소는 컴퓨터가 인터넷이나 LAN에 연결되었을 때 운영 체제에 가해지는 대부분의 가능한 위협을 차단하여 컴퓨터에 저장된 데이터를 보호하는 역할을 합니다. 이 구성요소는 두 종류의 규칙에 따라 모든 네트워크 활동을 필터링합니다: 애플리케이션 네트워크 규칙 및 네트워크 패킷 규칙.

- **네트워크 모니터**. 이 구성요소를 사용하면 컴퓨터의 네트워크 동작을 실시간으로 확인할 수 있습니다.

- **네트워크 공격 차단**. 이 구성요소는 인바운드 네트워크 트래픽을 검사하여 네트워크 공격과 유사한 활동이 있는지 확인합니다. 사용자 컴퓨터를 대상으로 시도된 네트워크 공격이 탐지되면 Kaspersky Endpoint Security는 공격 컴퓨터의 네트워크 동작을 차단합니다.

Kaspersky Endpoint Security에서 제공하는 작업은 다음과 같습니다:

- **전체 검사**. Kaspersky Endpoint Security는 RMA, 시작 시 로드되는 개체, 운영 체제 백업 저장소, 모든 하드 드라이브, 이동식 장치 등 운영 체제를 검사합니다.

- **사용자 지정 검사**. Kaspersky Endpoint Security에서 사용자가 선택한 개체를 검사합니다.

- **중요한 영역 검사**. Kaspersky Endpoint Security는 운영 체제 시작 시 로드된 개체, RAM 및 루트킷이 대상으로 하는 개체를 검사합니다.

- **업데이트**. Kaspersky Endpoint Security는 업데이트된 애플리케이션 데이터베이스 및 모듈을 다운로드합니다. 업데이트하면 최신 바이러스 및 기타 보안위협으로부터 컴퓨터가 계속 보호됩니다.

- **취약점 검사**. Kaspersky Endpoint Security는 운영 체제 및 설치된 소프트웨어의 취약점을 검사합니다. 이 검사를 통해 침입자가 악용할 수 있는 잠재적 문제를 시의적절하게 탐지하여 제거할 수 있습니다.

파일 암호화 기능을 사용하면 로컬 컴퓨터 드라이브에 저장된 파일 및 폴더를 암호화 할 수 있습니다. 드라이브 암호화 기능은 하드 드라이브 및 이동식 드라이브를 암호화할 수 있습니다.

Kaspersky Security Center를 통한 원격 관리

Kaspersky Security Center는 클라이언트 컴퓨터에서 Kaspersky Endpoint Security를 원격으로 시작 및 중지할 수 있으며 애플리케이션 설정을 원격으로 관리 및 구성할 수 있습니다.

애플리케이션의 서비스 기능

Kaspersky Endpoint Security에는 다양한 서비스 기능이 포함되어 있습니다. 서비스 기능은 애플리케이션을 최신 상태로 유지하고 기능을 확대하며 사용자가 애플리케이션을 작동시킬 있도록 지원하기 위한 것입니다.

- **리포트**. 애플리케이션은 작동하는 동안 각 구성요소 및 작업에 대한 리포트를 생성합니다. 리포트에는 Kaspersky Endpoint Security 이벤트 목록과 애플리케이션에서 수행하는 모든 작업이 포함됩니다. 문제가 발생할 경우 Kaspersky에 이 리포트를 보낼 수 있습니다. 그러면 기술 지원 서비스 전문가가 문제를 보다 자세히 살펴볼 것입니다.

- **데이터 저장소**. 애플리케이션이 컴퓨터에 바이러스 및 기타 보안위협이 있는지 검사하여 감염 파일이나 감염 의심 파일을 탐지한 경우 해당 파일은 차단됩니다. Kaspersky Endpoint Security는 감염 의심 파일을 *격리 저장소*라는 특별한 저장소로 보냅니다. Kaspersky Endpoint Security는 치료 및 삭제된 파일의 사본을 *백업 저장소*에 저장합니다. Kaspersky Endpoint Security는 *처리되지 않은 파일 목록*에 어떤 이유로 인해 처리되지 않은 파일을 이동합니다. 파일을 검사하고 원래 폴더로 파일을 복원하며 데이터 저장소를 비울 수 있습니다.

- **알림 서비스**. 알림 서비스는 컴퓨터의 현재 감시 상태와 Kaspersky Endpoint Security의 작동 상태에 대해 사용자에게 지속적으로 알려 줍니다. 알림은 화면에 표시할 수도 있고 이메일로 전송할 수도 있습니다.

- **Kaspersky Security Network**. Kaspersky Security Network에 대한 사용자의 참여를 통해 전 세계 사용자로부터 파일, 웹 리소스 및 소프트웨어에 대한 평판 정보를 실시간으로 수집하여 컴퓨터 보호의 효과를 높일 수 있습니다.

- **라이센스**. 라이센스를 구매하면 애플리케이션의 전체 기능을 이용할 수 있고, 애플리케이션 데이터베이스 및 모듈 업데이트를 받아 볼 수 있으며, 설치, 구성 및 애플리케이션의 사용과 관련된 문제에 대해 이메일이나 전화로 지원을 받아 볼 수 있습니다.

- **지원**. 등록된 Kaspersky Endpoint Security 사용자는 모두 기술지원 서비스 전문가에게 지원을 요청할 수 있습니다. 기술 지원 서비스 웹 사이트에서 My Kaspersky 계정을 통해 요청을 보낼 수도 있고 전화로 지원 담당자의 도움을 받을 수도 있습니다.

애플리케이션이 오류를 반환하거나 동작이 중단되면 자동으로 다시 시작됩니다.

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.

애플리케이션은 Kaspersky 전문가가 정의한 특수 목적의 알고리즘을 사용하여 반복되는 오류 및 시스템 장애에 관한 정보를 수신합니다.

하드웨어 및 소프트웨어 요구 사항

Kaspersky Endpoint Security가 제대로 작동하려면 다음 요구사항이 충족되어야 합니다:

최소 일반 요구 사항:

- 2GB의 하드 디스크 여유 공간

- 클럭 속도가 1GHz인 프로세서 (SSE2 명령어 세트 지원)

- RAM:

  - 1 GB(32비트 운영 체제);

  - 2 GB(64비트 운영 체제).

지원되는 PC 운영 체제:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 이상;

- Windows 8 Professional / Enterprise;

- Windows 8.1 Professional / Enterprise;

- Windows 10 Home / Pro / Education / Enterprise.

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

지원되는 파일 서버 운영 체제:

- Windows Small Business Server 2008 Standard / Premium(64비트);
- Windows Small Business Server 2011 Essentials / Standard(64비트);
- Windows MultiPoint Server 2011(64비트);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 이상;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 이상;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

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

애플리케이션 설치 및 제거

컴퓨터에 Kaspersky Endpoint Security를 설치하는 방법, 초기 구성을 수행하는 방법, 이전 버전에서 업그레이드하는 방법 및 컴퓨터에서 애플리케이션을 제거하는 방법을 안내합니다.

애플리케이션 설치

이 섹션에서는 컴퓨터에 Kaspersky Endpoint Security를 설치한 후 초기 구성을 완료하는 방법을 설명합니다.

애플리케이션 설치 방법 정보

Kaspersky Endpoint Security 10 for Windows는 로컬(사용자의 컴퓨터에 직접) 및 관리자의 워크스테이션에서 원격으로 설치될 수 있습니다.

Kaspersky Endpoint Security 10 for Windows의 로컬 설치는 다음 모드 중 하나로 실행할 수 있습니다:

- 애플리케이션 설치 마법사 사용한 대화식 모드.
  대화식 모드에서는 설치 과정에 사용자의 확인이 필요합니다.
- 명령줄을 사용해 자동 모드로 설치.
  자동 모드로 설치가 시작되면 사용자가 설치 과정에 관여할 필요가 없습니다.

다음을 이용해 네트워크에 있는 컴퓨터에 애플리케이션을 원격으로 설치할 수 있습니다:

- Kaspersky Security Center 소프트웨어 스위트(*Kaspersky Security Center 구현 설명서* 참조).
- Microsoft Windows의 그룹 정책 편집기(운영 체제 도움말 파일 참고).
- System Center Configuration Manager.

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

설치 마법사를 사용하여 애플리케이션 설치

애플리케이션 설치 마법사의 인터페이스는 애플리케이션 설치 단계마다 나타나는 일련의 창으로 구성됩니다. **뒤로** 및 **다음** 버튼을 사용하여 설치 마법사의 페이지를 앞, 뒤로 이동할 수 있습니다. 작업이 완료된 후 설치 마법사를 닫으려면 **끝내기** 버튼을 누릅니다. 언제든지 **취소** 버튼을 사용하여 설치 마법사를 중지할 수 있습니다.

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

1. 배포 키트에 포함된 setup.exe 파일을 실행합니다.
   설치 마법사가 시작됩니다.

2. 설치 마법사의 안내를 따릅니다.

setup.exe 파일이 실행되면, Kaspersky Endpoint Security는 호환되지 않는 소프트웨어가 있는지 컴퓨터를 검사합니다. 기본적으로 호환되지 않는 소프트웨어가 검색되면 설치 프로세스가 중단되고 Kaspersky Endpoint Security와 호환되지 않는 애플리케이션 목록이 화면에 표시됩니다. 설치를 계속하려면, 컴퓨터에서 해당 애플리케이션을 삭제해야 합니다.

1 단계. 컴퓨터가 설치 요구 사항을 충족하는지 확인

컴퓨터에 Kaspersky Endpoint Security 10 for Windows를 설치하거나 이전 버전의 애플리케이션을 업데이트하기 전에 다음 조건을 확인해야 합니다:

- 운영 I체제 및 서비스 팩이 제품 설치를 위한 소프트웨어 요구 사항을 충족하는지 여부.
- 하드웨어 및 소프트웨어 요구 사항이 충족되는지 여부.
- 사용자에게 소프트웨어 제품의 설치 권한이 있는지 여부.

위의 요구 사항 중 어느 하나라도 충족되지 않으면 화면에 관련 알림 정보가 표시됩니다.

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 있는 경우 마이그레이션할 수 있는 모든 데이터(예: 활성화 데이터 및 애플리케이션 설정)는 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 설치 동안 유지되고 사용되며 그 후에 이전 애플리케이션 버전이 자동으로 제거됩니다. 이 내용은 다음 애플리케이션 버전에 적용됩니다:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows

2 단계. 설치 절차의 시작 페이지

애플리케이션 설치에 대한 모든 요구 사항을 충족하면, 설치 패키지를 시작한 이후에 시작 페이지가 나타납니다. 시작 페이지는 컴퓨터에 Kaspersky Endpoint Security의 설치를 시작한다는 것을 알립니다.

설치 마법사를 계속하려면 **다음** 버튼을 누릅니다.

3 단계. 라이센스 동의서 정보 보기

이 단계에서는 사용자와 Kaspersky 사이의 라이센스 계약을 검토합니다.

계약서를 주의하여 살펴보고 모든 조건에 동의하면 **라이센스 계약서 조건에 동의합니다** 확인란을 선택합니다.

설치 마법사의 이전 단계로 돌아가려면 **뒤로** 버튼을 누릅니다. 설치 마법사를 계속하려면 **다음** 버튼을 누릅니다. 설치 마법사를 중지하려면 **취소** 버튼을 누르십시오.

4 단계. 설치 유형 선택

이 단계에서는 가장 적합한 Kaspersky Endpoint Security의 설치 유형을 선택할 수 있습니다:

- **기본 설치**. 이 설치 유형을 선택하면 Kaspersky 전문가의 권장 설정에 따라 보호 구성요소, 애플리케이션 권한 제어 및 취약점 모니터가 컴퓨터에 설치됩니다.
- **표준 설치**. 이 설치 유형을 선택하면 Kaspersky 권장 설정이 지정된 보호 및 제어 구성요소가 컴퓨터에 설치됩니다.
- **사용자 지정 설치**. 이 설치 유형을 선택하면 설치할 구성요소를 선택하고 설치 대상 폴더를 지정하는 화면이 표시됩니다.

  이 설치 유형을 선택하면 기본 및 표준 설치에 포함되지 않은 구성 요소를 설치할 수 있습니다.

표준 설치가 기본적으로 선택되어 있습니다.

설치 마법사의 이전 단계로 돌아가려면 **뒤로** 버튼을 누릅니다. 설치 마법사를 계속하려면 **다음** 버튼을 누릅니다. 설치 마법사를 중지하려면 **취소** 버튼을 누르십시오.

5 단계. 설치할 애플리케이션 구성요소 선택

이 단계는 애플리케이션의 *사용자 지정 설치*를 선택한 경우에 수행합니다.

이 단계에서, 설치할 Kaspersky Endpoint Security의 구성요소를 선택할 수 있습니다. 파일 안티 바이러스는 반드시 설치해야 하는 구성요소입니다. 해당 구성요소 설치를 취소할 수 없습니다.

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

- BadUSB 공격 차단.
- 드라이브 암호화.
- 파일 암호화.
- Microsoft BitLocker 매니저.
- KATA 엔드포인트 센서.

*Microsoft BitLocker 매니저*에서 수행하는 기능입니다:

- Windows 운영 체제에 내장된 BitLocker 암호화를 관리합니다.
- 암호화 정책 설정을 구성하고 관리 컴퓨터에 대한 정책의 적용 여부를 확인합니다.

- 암호화 및 복호화 프로세스를 시작합니다.
- 관리 컴퓨터의 암호화 상태를 모니터링합니다.
- Kaspersky Security Center 중앙 관리 서버에 복구 키를 저장합니다.

*KATA 엔드포인트 센서*는 Kaspersky Anti Targeted Attack 플랫폼의 구성요소입니다. 이 솔루션은 표적 공격과 같은 보안위협을 빠르게 감지하기 위한 용도입니다. 구성요소는 지속적으로 프로세스, 활성인 네트워크 연결 및 수정 파일을 모니터링한 다음 Kaspersky Anti Targeted Attack 플랫폼으로 이 정보를 전달합니다.

설치할 구성요소를 선택하려면 구성요소 이름 옆에 있는 아이콘을 눌러 마우스 오른쪽 메뉴를 표시하고 **로컬 하드 드라이브에 기능을 설치합니다.** 항목을 선택합니다. 선택한 구성요소에 의해 수행되는 작업 및 구성요소 설치에 필요한 디스크 공간에 대한 정보를 보려면 현재 설치 마법사 페이지의 아래쪽을 참조하십시오.

로컬 하드 드라이브의 남은 공간에 대한 상세 정보를 보려면 **볼륨** 버튼을 누릅니다. **이용 가능한 디스크 공간** 창이 열리고 남은 공간 정보가 표시됩니다.

구성요소 설치를 취소하려면 마우스 오른쪽 메뉴에서 **기능을 이용할 수 없게 됩니다.** 옵션을 선택합니다.

설치할 구성요소의 기본 목록으로 돌아가려면 **초기화** 버튼을 누릅니다.

설치 마법사의 이전 단계로 돌아가려면 **뒤로** 버튼을 누릅니다. 설치 마법사를 계속하려면 **다음** 버튼을 누릅니다. 설치 마법사를 중지하려면 **취소** 버튼을 누르십시오.

6 단계. 대상 폴더 선택

이 단계는 애플리케이션의 *사용자 지정 설치*를 선택한 경우에 수행할 수 있습니다.

이 단계에서는 애플리케이션이 설치될 대상 폴더의 경로를 지정할 수 있습니다. 애플리케이션의 대상 폴더를 선택하려면 **찾아보기** 버튼을 누릅니다.

로컬 하드 드라이브의 남은 공간에 대한 정보를 보려면 **볼륨** 버튼을 누릅니다. **디스크 공간 요구 사항** 창이 열리고 남은 공간 정보가 표시됩니다.

설치 마법사의 이전 단계로 돌아가려면 **뒤로** 버튼을 누릅니다. 설치 마법사를 계속하려면 **다음** 버튼을 누릅니다. 설치 마법사를 중지하려면 **취소** 버튼을 누르십시오.

7 단계. 바이러스 검사에서 예외할 대상 추가

이 단계는 애플리케이션의 *사용자 지정 설치*를 선택한 경우에 수행할 수 있습니다.

이 단계에서 애플리케이션 설정에 바이러스 검사에서 예외할 항목을 추가할 수 있습니다.

Microsoft에서 권장하는 영역을 바이러스 검사 적용 영역에서 예외 / **Kaspersky에서 권장하는 영역을 바이러스 검사 적용 영역에서 예외** 확인란은 각각 Microsoft 또는 Kaspersky에서 권장하는 영역을 신뢰 구역에서 예외하거나 포함합니다.

이 확인란을 선택하면 Kaspersky Endpoint Security에서 각각 Microsoft 또는 Kaspersky에서 권장하는 영역을 신뢰하는 영역에 포함합니다. Kaspersky Endpoint Security는 바이러스 및 기타 보안위협에 대해 이러한 영역을 검사하지 않습니다.

Microsoft에서 권장하는 영역을 바이러스 검사 영역에서 예외 확인란은 파일 서버용 Microsoft Windows에서 실행되는 컴퓨터에 Kaspersky Endpoint Security를 설치할 때 선택할 수 있습니다.

설치 마법사의 이전 단계로 돌아가려면 **뒤로** 버튼을 누릅니다. 설치 마법사를 계속하려면 **다음** 버튼을 누릅니다. 설치 마법사를 중지하려면 **취소** 버튼을 누르십시오.

8 단계. 애플리케이션 설치 준비

사용자의 컴퓨터가 Kaspersky Endpoint Security 10 for Windows 설치를 방해할 수 있는 악성 코드에 감염되었을 수 있기 때문에 설치 프로세스를 보호하는 것이 좋습니다.

설치 프로세스 보호는 기본적으로 사용됩니다.

하지만, 애플리케이션을 설치할 수 없는 경우(예, Windows 원격 데스크톱으로 원격 설치를 수행할 때), 설치 프로세스의 보호를 해제하십시오. 이 경우 설치를 중단하고 애플리케이션 설치 마법사를 다시 시작합니다. "애플리케이션 설치 준비" 단계에서 **설치 프로세스 보호** 확인란을 선택 해제합니다.

Citrix PVS와의 호환성 보장 확인란을 통해 Citrix PVS 호환 모드의 드라이버를 설치하는 기능을 작동 또는 중지합니다.

Citrix Provisioning Services를 사용하는 경우에만 이 확인란을 선택하십시오.

시스템 변수 %PATH%에 avp.com 파일 경로 추가 확인란은 %PATH% 시스템 변수에 avp.com 파일 경로를 추가하는 옵션을 작동 또는 중지합니다.

이 확인란을 선택하면 명령줄에서 Kaspersky Endpoint Security 또는 관련 작업을 시작할 때 실행 파일 경로를 입력하지 않아도 됩니다. 실행 파일 이름과 명령만 입력하면 해당 작업이 시작됩니다.

설치 마법사의 이전 단계로 돌아가려면 **뒤로** 버튼을 누릅니다. 애플리케이션을 설치하려면 **설치** 버튼을 누릅니다. 설치 마법사를 중지하려면 **취소** 버튼을 누르십시오.

컴퓨터에 애플리케이션이 설치되는 동안 현재 네트워크 연결이 중단될 수 있습니다. 대부분의 경우 애플리케이션 설치가 완료되면 중단된 네트워크 연결이 복원됩니다.

9 단계. 애플리케이션 설치

애플리케이션 설치에는 다소 시간이 소요될 수 있습니다. 설치가 완료될 때까지 기다려 주시기 바랍니다.

이전 애플리케이션 버전을 업데이트하는 경우, 이 단계에는 설정 마이그레이션과 이전 애플리케이션 버전의 제거도 포함됩니다.

Kaspersky Endpoint Security 설치를 마친 이후에 초기 구성 마법사가 시작됩니다.

명령줄에서 애플리케이션 설치

다음 모드 중 하나를 사용해 명령줄로 Kaspersky Endpoint Security를 설치할 수 있습니다:

- 애플리케이션 설치 마법사 사용한 대화식 모드.
- 숨김 모드. 자동 모드로 설치가 시작되면 사용자가 설치 과정에 관여할 필요가 없습니다. 애플리케이션을 숨김 모드로 설치하려면 `/s` 및 `/qn` 키를 사용합니다.

애플리케이션을 설치하거나 애플리케이션 버전을 업그레이드하려면 다음을 수행합니다:

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] [/pALLOWREBOOT=1|0] [/pADDLOCAL=<구성 요소>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<사용자 이름> /pKLPASSWD=<암호> /pKLPASSWDAREA=<암호 범위>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<추적로그 레벨>] /s`

   또는

   `msiexec /i <배포 키트 이름> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [ALLOWREBOOT=1|0] [ADDLOCAL=<구성 요소>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<사용자 이름> KLPASSWD=<암호> KLPASSWDAREA=<암호 범위>] [ENABLETRACES=1|0 TRACESLEVEL=<추적로그 레벨>] /qn`

`EULA`	최종 사용자 라이센스 계약서 조건에 대한 수락 또는 거부. 사용 가능한 값은 다음과 같습니다: • `1` - 최종 사용자 라이센스 계약서 조건 동의. • `0` - 최종 사용자 라이센스 계약서 조건 거부. 라이센스 계약서는 Kaspersky Endpoint Security 배포 키트에 포함되어 있습니다. 애플리케이션을 설치하거나 애플리케이션 버전을 업데이트하려면 최종 사용자 라이센스 계약서 조건에 동의해야 합니다.
`PRIVACYPOLICY`	개인정보취급방침에 대한 수락 또는 거부. 사용 가능한 값은 다음과 같습니다: • `1` - 개인정보취급방침에 동의함. • `0` - 개인정보취급방침에 동의하지 않음. 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 값은 다음과 같습니다: • `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.

ALLOWREBOOT=1	애플리케이션을 설치하거나 업그레이드한 후 필요한 경우 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.
ADDLOCAL	설치할 추가 구성 요소를 선택합니다. 기본적으로 다음 구성 요소를 제외한 모든 애플리케이션 구성 요소의 설치가 선택되어 있습니다: BadUSB 공격 차단, 파일 레벨 암호화, 전체 디스크 암호화, BitLocker 매니지먼트 및 KATA 엔드포인트 센서. 사용 가능한 값은 다음과 같습니다: • MSBitLockerFeature. BitLocker 매니저 구성요소가 설치됩니다. • AntiAPTFeature. KATA 엔드포인트 센서 구성요소가 설치됩니다.
SKIPPRODUCTCHECK=1	호환되지 않는 소프트웨어 확인 중지. 비-호환 소프트웨어 목록은 배포 키트에 포함된 incompatible.txt 파일에서 확인할 수 있습니다. 이 파라미터에 대해 설정된 값이 없고, 호환되지 않는 소프트웨어가 탐지되면 Kaspersky Endpoint Security 설치가 종료됩니다.
SKIPPRODUCTUNINSTALL=1	탐지된 호환되지 않는 소프트웨어 자동 제거를 중지합니다. 이 파라미터에 대해 설정된 값이 없으면 Kaspersky Endpoint Security에서 호환되지 않는 소프트웨어를 제거하려고 시도합니다.
KLLOGIN	Kaspersky Endpoint Security의 기능 및 설정에 접근하기 위한 사용자 이름 설정(암호 보호 구성 요소). 사용자 이름은 KLPASSWD 및 KLPASSWDAREA 파라미터와 함께 설정됩니다. 기본 사용자 이름은 KLAdmin입니다.
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 자격 증명(KLLOGIN 및 KLPASSWD 매개 변수)을 묻는 메시지를 표시합니다. 여러 값을 지정하려면 ";" 문자를 사용합니다. 사용 가능한 값은 다음과 같습니다: • 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.
ENABLETRACES	애플리케이션 추적 로그 활성화 또는 비활성화. Kaspersky Endpoint

	Security가 시작된 후 %ProgramData%/Kaspersky Lab 폴더에 추적로그 파일을 저장합니다. 사용 가능한 값은 다음과 같습니다: • `1` - 추적 로그 켜짐. • `0` – 추적 로그 꺼짐(기본값).
`TRACESLEVEL`	추적로그 기록 레벨. 사용 가능한 값은 다음과 같습니다: • `100` (심각). 치명적인 오류 메시지만. • `200` (높음). 치명적인 오류를 포함한 모든 오류에 대한 메시지 기록. • `300` (진단). 모든 오류에 대한 메시지 및 경고가 포함된 일부 메시지. • `400` (중요). 일반 및 치명적인 오류에 대한 모든 경고와 메시지, 추가 정보가 포함된 일부 메시지. • `500` (일반). 일반 및 치명적인 오류에 대한 모든 경고와 메시지 및 정상 모드에서의 애플리케이션 작동에 대한 자세한 정보가 포함된 메시지 (기본값). • `600` (낮음). 모든 가능성 있는 메시지.

예:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

애플리케이션을 설치한 후 Kaspersky Endpoint Security는 setup.ini 파일에 활성화코드를 지정하지 않는 한 체험판 라이센스를 활성화합니다. 체험판 라이센스는 보통 사용 기간이 짧습니다. 체험판 라이센스가 만료되면 모든 Kaspersky Endpoint Security 기능이 중지됩니다. 애플리케이션을 계속 사용하려면 상업용 라이센스를 활성화해야 합니다.

자동 모드에서 애플리케이션을 설치 또는 버전 업그레이드를 할 때 다음 파일을 사용할 수 있습니다:

- setup.ini - 일반적인 애플리케이션 설치 설정;
- install.cfg – Kaspersky Endpoint Security 로컬 설정;
- setup.reg – 레지스트리 키.

  setup.ini 파일의 `SetupReg` 파라미터에 대해 `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.ini, install.cfg 및 setup.reg 파일의 설정을 적용하려면 이러한 파일을 Kaspersky Endpoint Security 배포 패키지가 들어 있는 폴더에 넣습니다.

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** 섹션에서 **패키지**를 선택합니다.
3. 콘솔 위쪽 제어판에서 **패키지 만들기** 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.
      - **경로 폴더** 필드에 Kaspersky Endpoint Security 배포 패키지가 있는 폴더의 경로를 지정합니다.
   b. **애플리케이션 유형** 섹션에서 **표준 애플리케이션** 옵션을 선택합니다.
   c. **표준 애플리케이션** 섹션에서 다음을 수행합니다:
      - **이름** 필드에 설치 패키지 고유 이름을 입력합니다(예: 버전을 포함한 애플리케이션 이름).
      - **명령 줄** 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 애플리케이션 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** 섹션에서 **지정 플랫폼에서만 시작하는 애플리케이션** 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.
      - **컴퓨터 집합** 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. 필요한 경우 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.

setup.ini 파일은 다음 섹션으로 구성되어 있습니다:

- `[Setup]` – 일반적인 애플리케이션 설치 옵션.
- `[Components]` - 설치할 애플리케이션 구성요소 선택. 어떤 구성요소도 지정하지 않으면 운영 체제에서 지원하는 모든 구성요소가 설치됩니다. 파일 안티 바이러스는 반드시 설치해야 하는 구성요소이며 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`을 대체하여 `yes`, `on`, `enable` 및 `enabled` 값을 사용할 수 있습니다.

`0`을 대체하여 `no`, `off`, `disable` 및 `disabled`값을 사용할 수 있습니다.

setup.ini 파일 설정

섹션	파라미터	설명
`[Setup]`	`InstallDir`	애플리케이션 설치 폴더 경로.
	`ActivationCode`	Kaspersky Endpoint Security 활성화코드.
	`Eula`	최종 사용자 라이센스 계약서 조건에 대한 수락 또는 거부. 사용 가능한 값은 다음과 같습니다:

		• `1` - 최종 사용자 라이센스 계약서 조건 동의. • `0` - 최종 사용자 라이센스 계약서 조건 거부. 라이센스 계약서는 Kaspersky Endpoint Security 배포 키트에 포함되어 있습니다. 애플리케이션을 설치하거나 애플리케이션 버전을 업데이트하려면 최종 사용자 라이센스 계약서 조건에 동의해야 합니다.
	`PrivacyPolicy`	개인정보취급방침에 대한 수락 또는 거부. 사용 가능한 값은 다음과 같습니다: • `1` - 개인정보취급방침에 동의함. • `0` - 개인정보취급방침에 동의하지 않음. 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 값은 다음과 같습니다: • `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.
	아이디	Kaspersky Endpoint Security의 기능 및 설정에 접근하기 위한 사용자 이름 설정(암호 보호 구성 요소). 사용자 이름은 `Password` 및 `PasswordArea` 설정과 함께 설정됩니다. 기본 사용자 이름은 KLAdmin입니다.
	암호	Kaspersky Endpoint Security 기능 및 설정에 접근하기 위한 암호를 지정합니다(암호와 함께 `Login` 및 `PasswordArea` 파라미터 지정). 암호를 지정했지만 로그인 변수와 함께 사용자 이름을 지정하지 않은 경우 KLAdmin 사용자 이름이 기본적으로 사용됩니다.
	`PasswordArea`	Kaspersky Endpoint Security에 접근하기 위한 암호 적용 영역을 지정합니다. 사용자가 이 범위에 포함된 동작을 수행하려고 하면 Kaspersky Endpoint Security에서 사용자의 계정 자격 증명(아이디 및 암호 매개 변수)을 묻는 메시지를 표시합니다. 여러 값을 지정하려면 `";"` 문자를 사용합니다. 사용 가능한 값은 다음과 같습니다: • `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.
	`SelfProtection`	애플리케이션 설치 보호 메커니즘을 사용하거나 사용하지 않습니다. 사용 가능한 값은 다음과 같습니다: • `1` - 애플리케이션 설치 보호 메커니즘이 활성됩니다. • `0` - 애플리케이션 설치 보호 메커니즘이 비활성됩니다. 설치 보호를 중지할 수 있습니다. 설치 보호는 악성 코드에 의한 배포 패키지 스푸핑 차단, Kaspersky Endpoint Security 설치 폴더 접근 차단, 애플리케이션 키가 포함된 시스템 레지스트리 하이브 접근 차단 등이 포함됩니다. 하지만, 애플리케이션을 설치할 수 없는 경우(예, Windows 원격 데스크톱으로 원격 설치를 수행할 때), 설치 프로세스의 보호를 해제하십시오.
	`Reboot=1`	애플리케이션을 설치하거나 업그레이드한 후 필요한 경우 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 값은 다음과 같습니다: • `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 서비스 보호를 작동하거나 중지합니다. 사용 가능한 값은 다음과 같습니다: • `1` - AM-PPL 기술을 사용한 Kaspersky Endpoint Security 서비스 보호가 작동됩니다. • `0` - AM-PPL 기술을 사용한 Kaspersky Endpoint Security 서비스 보호가 중지됩니다.
	`SetupReg`	setup.reg 파일에서 레지스트리로 레지스트리 키를 추가합

		니다. `SetupReg: setup.reg` 파라미터 값.
	`EnableTraces`	애플리케이션 설치 추적 로그 활성화 또는 비활성화. Kaspersky Endpoint Security는 %ProgramData%/Kaspersky Lab 폴더에 추적로그 파일을 저장합니다. 사용 가능한 값은 다음과 같습니다: • `1` - 애플리케이션 설치 추적로그 활성화. • `0` – 애플리케이션 설치 추적로그 비활성화(기본값).
	`TracesLevel`	추적로그 기록 레벨. 사용 가능한 값은 다음과 같습니다: • `100` (심각). 치명적인 오류 메시지만. • `200` (높음). 치명적인 오류를 포함한 모든 오류에 대한 메시지 기록. • `300` (진단). 모든 오류에 대한 메시지 및 경고가 포함된 일부 메시지. • `400` (중요). 일반 및 치명적인 오류에 대한 모든 경고와 메시지, 추가 정보가 포함된 일부 메시지. • `500` (일반). 일반 및 치명적인 오류에 대한 모든 경고와 메시지 및 정상 모드에서의 애플리케이션 작동에 대한 자세한 정보가 포함된 메시지(기본값). • `600` (낮음). 모든 가능성 있는 메시지.
[구성 요소]	`ALL`	모든 구성 요소 설치. 파라미터 값 `1`을 지정하면 각 구성요소의 설치 설정에 관계없이 모든 구성요소가 설치됩니다.
	`MailAntiVirus`	메일 안티 바이러스.
	`IMAntiVirus`	메신저 안티 바이러스.
	`WebAntiVirus`	웹 안티 바이러스.
	`ApplicationPrivilegeControl`	애플리케이션 권한 제어.
	`SystemWatcher`	시스템 감시기.
	방화벽	방화벽.
	`NetworkAttackBlocker`	네트워크 공격 차단.
	`WebControl`	웹 제어.
	`DeviceControl`	매체 제어.
	`ApplicationStartupControl`	애플리케이션 시작 제어.
	`FileEncryption`	파일 레벨 암호화 라이브러리.
	`DiskEncryption`	전체 디스크 암호화 라이브러리.
	`VulnerabilityAssessment`	취약점 감시.
	`KeyboardAuthorization`	BadUSB 공격 차단.
	`AntiAPT`	KATA 엔드포인트 센서.

	`MSBitLocker`	Microsoft BitLocker 매니저.
	`AdminKitConnector`	Kaspersky Security Center를 통해 애플리케이션을 원격으로 관리할 때 사용할 네트워크 에이전트 커넥터. 사용 가능한 값은 다음과 같습니다: • `1` - 네트워크 에이전트 커넥터가 설치됩니다. • `0` - 네트워크 에이전트 커넥터가 설치되지 않습니다.
`[Tasks]`	`ScanMyComputer`	컴퓨터 전체 검사 작업. 사용 가능한 값은 다음과 같습니다: • `1` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함됩니다. • `0` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함되지 않습니다.
	`ScanCritical`	중요한 영역 검사 작업. 사용 가능한 값은 다음과 같습니다: • `1` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함됩니다. • `0` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함되지 않습니다.
	`Updater`	업데이트 작업. 사용 가능한 값은 다음과 같습니다: • `1` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함됩니다. • `0` - 이 작업은 Kaspersky Endpoint Security 작업 목록에 포함되지 않습니다.

초기 구성 마법사

애플리케이션 설치 절차가 끝나면 Kaspersky Endpoint Security의 초기 구성 마법사가 시작됩니다. 초기 구성 마법사를 통해 애플리케이션을 활성화하고 운영 체제에 포함된 애플리케이션 정보를 수집할 수 있습니다. 이러한 애플리케이션은 신뢰하는 애플리케이션 목록에 추가되어 운영 체제 내에서 어떤 제한도 없이 동작을 수행할 수 있습니다.

초기 구성 마법사는 각 단계별 페이지를 순차적으로 표시하며 설치를 진행합니다. **뒤로** 및 **다음** 버튼을 사용하여 초기 구성 마법사의 페이지를 앞, 뒤로 이동할 수 있습니다. 초기 구성 마법사 절차를 마치려면 **끝내기** 버튼을 누릅니다. 어떤 단계에서라도 초기 구성 마법사 절차를 중단하려면 **취소**를 누릅니다.

어떤 이유로 초기 구성 마법사가 중단되면 이미 지정된 설정은 저장되지 않습니다. 다음 번에 애플리케이션을 사용하려고 할 때 초기 구성 마법사가 다시 시작되며 처음부터 설정을 구성해야 합니다.

애플리케이션 활성화

애플리케이션은 현재 시스템 날짜 및 시간으로 컴퓨터에서 활성화되어야 합니다. 시스템 날짜와 시간은 애플리케이션의 활성화 후 변경 될 경우, 키가 오작동합니다. 애플리케이션이 업데이트가 중단된 작동 모드로 전환되고, Kaspersky Security Network도 사용할 수 없습니다. 키는 운영 체제를 다시 설치한 후에만 다시 동작 할 수 있습니다.

이 단계에서 다음 Kaspersky Endpoint Security 활성화 옵션 중 하나를 선택합니다:

- **활성화코드로 활성화**. 활성화코드를 사용하여 애플리케이션을 활성화하려면 이 옵션을 선택하고 활성화코드를 입력합니다.
- **라이센스 키 파일로 활성화**. 키 파일을 사용해 애플리케이션을 활성화하려면 이 옵션을 선택합니다.
- **체험판으로 활성화**. 체험판 애플리케이션을 활성화하려면 이 옵션을 선택합니다. 체험판 애플리케이션 라이센스에 따라 한정된 기간 동안 정식 애플리케이션 버전을 사용할 수 있습니다. 라이센스가 만료되면 애플리케이션 기능이 차단되고 체험판 버전을 다시 활성화할 수 없습니다.
- **나중에 활성화**. Kaspersky Endpoint Security 활성화 단계를 건너뛰려면 이 옵션을 선택합니다. 파일 안티 바이러스 및 방화벽 구성요소만 사용할 수 있습니다. 설치 후 안티 바이러스 데이터베이스와 Kaspersky Endpoint Security 모듈을 한 번만 업데이트할 수 있습니다. **나중에 활성화** 옵션은 애플리케이션 설치 직후 초기 구성 마법사를 처음 시작할 때만 사용할 수 있습니다.

애플리케이션의 체험판 또는 활성화코드로 활성화하려면 인터넷 연결이 필요합니다.

초기 구성 마법사를 계속 진행하려면 활성화 옵션을 선택하고 **다음** 버튼을 누릅니다. 초기 구성 마법사를 중지하려면 **취소** 버튼을 누릅니다.

활성화코드를 사용하여 활성화

이 단계는 활성화코드를 사용하여 애플리케이션을 활성화한 경우에만 사용할 수 있습니다. 체험판 애플리케이션을 활성화하거나 라이센스 키 파일을 사용하여 애플리케이션을 활성화하는 경우에는 이 단계를 건너뜁니다.

이 단계에서 Kaspersky Endpoint Security는 활성화 서버로 데이터를 전송하여 입력한 활성화코드가 맞는지 확인합니다:

- 성공적으로 활성화코드 확인을 받은 경우 초기 구성 마법사는 자동으로 다음 단계를 계속합니다.
- 활성화코드 확인에 실패하면 이에 대한 메시지가 제공됩니다. 이 경우, Kaspersky Endpoint Security 라이센스를 판매한 소프트웨어 공급업체에 도움을 요청하라는 내용이 표시됩니다.
- 활성화코드의 활성화 개수가 초과되면 이에 대한 알림이 제공됩니다. 초기 구성 마법사가 중단되고 애플리케이션에 Kaspersky 기술 지원 서비스에 연락하라는 메시지가 표시됩니다.

초기 구성 마법사의 이전 단계로 돌아가려면 **뒤로** 버튼을 누릅니다. 초기 구성 마법사를 중지하려면 **취소** 버튼을 누릅니다.

라이센스 키 파일을 사용하여 활성화

이 단계는 라이센스 키 파일을 사용하여 애플리케이션을 활성화할 경우에만 제공됩니다.

이 단계에서 라이센스 키 파일의 경로를 지정합니다. **찾아보기** 버튼을 누르고 `<File ID>.key`. 형식의 라이센스 키 파일을 선택합니다.

라이센스 키 파일을 선택하면 다음과 같은 정보가 창 하단에 표시됩니다:

- 키
- 라이센스 유형(상업용 또는 체험판) 및 이 라이센스를 사용하는 컴퓨터 수
- 컴퓨터의 애플리케이션 활성화 날짜
- 라이센스 만료 날짜
- 라이센스에 따라 사용 가능한 애플리케이션 기능
- 라이센스 문제(있을 경우)에 대한 알림. 예: *라이센스 확인용 블랙리스트 파일 손상.*

초기 구성 마법사의 이전 단계로 돌아가려면 **뒤로** 버튼을 누릅니다. 초기 구성 마법사를 계속하려면 **다음** 버튼을 누릅니다. 초기 구성 마법사를 중지하려면 **취소** 버튼을 누릅니다.

활성화할 기능 선택

이 단계는 체험판 버전의 애플리케이션을 활성화한 경우에만 제공됩니다.

이 단계에서 애플리케이션을 활성화한 이후에 이용할 수 있는 기능을 선택할 수 있습니다:

- **기본 설치**. 이 옵션을 선택하면 애플리케이션 활성화 후 보호 구성요소, 애플리케이션 권한 제어 및 취약점 감시 기능만 이용할 수 있습니다.
- **표준 설치**. 이 옵션을 선택하면 애플리케이션 활성화 후 애플리케이션의 보호 및 제어 구성요소만 이용할 수 있습니다.
- **전체 설치**. 이 옵션을 선택하면 애플리케이션 활성화 후 데이터 암호화 기능을 비롯한 모든 애플리케이션 구성요소를 이용할 수 있습니다.

설치하는 동안 구입한 라이센스로 설치 가능한 것보다 많은 구성요소를 선택한 경우 애플리케이션 활성화 후 라이센스에 따라 사용할 수 없는 구성요소가 설치되기는 하지만 작동하지 않습니다. 구입한 라이센스가 현재 설치된 구성요소 이상의 사용을 허용한다면 애플리케이션이 활성화된 후 설치되지 않는 구성요소들이 **라이센스** 섹션에 나열됩니다.

표준 설치가 기본적으로 선택되어 있습니다.

초기 구성 마법사의 이전 단계로 돌아가려면 **뒤로** 버튼을 누릅니다. 초기 구성 마법사를 계속하려면 **다음** 버튼을 누릅니다. 초기 구성 마법사를 중지하려면 **취소** 버튼을 누릅니다.

활성화 완료

이 단계에서는 초기 구성 마법사가 Kaspersky Endpoint Security의 성공적인 활성화를 위한 정보를 제공합니다. 라이센스에 대한 다음 정보가 제공됩니다:

- 라이센스 유형(상업용 또는 체험판) 및 이 라이센스를 사용하는 컴퓨터 수
- 라이센스 만료 날짜
- 라이센스에 따라 사용 가능한 애플리케이션 기능

초기 구성 마법사를 계속하려면 **다음** 버튼을 누릅니다. 초기 구성 마법사를 중지하려면 **취소** 버튼을 누릅니다.

운영 체제 분석

이 단계에서는 운영 체제에 포함되어 있는 애플리케이션에 대한 정보를 수집합니다. 이러한 애플리케이션은 신뢰하는 애플리케이션 목록에 추가되어 운영 체제 내에서 어떤 제한도 없이 동작을 수행할 수 있습니다.

다른 애플리케이션의 경우, Kaspersky Endpoint Security를 설치한 이후 해당 애플리케이션을 처음 시작할 때 분석됩니다.

초기 구성 마법사를 중지하려면 **취소** 버튼을 누릅니다.

애플리케이션 초기 구성 완료

초기 구성 마법사 완료 창에는 Kaspersky Endpoint Security 설치 프로세스에 관한 정보가 나옵니다.

Kaspersky Endpoint Security를 시작하려면 **마침** 버튼을 누르십시오.

Kaspersky Endpoint Security를 시작하지 않고 초기 구성 마법사를 종료하려면 **Kaspersky Endpoint Security 10 for Windows 시작** 확인란을 선택 취소하고 **마침**을 누르십시오.

Kaspersky Security Network 정책

이 단계에서는 Kaspersky Security Network 참여에 대한 내용이 안내됩니다.

Kaspersky Security Network 정책을 검토합니다:

- 모든 조건에 동의하면 초기 구성 마법사 창에서 **Kaspersky Security Network 참여 조건에 동의합니다** 옵션을 선택합니다.
- Kaspersky Security Network 참여 조건에 동의하지 않으면 초기 구성 마법사 창에서 **Kaspersky Security Network 참여 조건에 동의하지 않습니다** 옵션을 선택합니다.

초기 구성 마법사 다음 단계로 진행하려면 **확인**을 누릅니다.

이전 애플리케이션 버전의 업그레이드 방법 정보

이전 애플리케이션 버전을 Kaspersky Endpoint Security 10 Service Pack 2 for Windows로 업그레이드하는 경우, 암호화된 모든 하드 드라이브를 복호화해야 합니다.

다음 애플리케이션을 Kaspersky Endpoint Security 10 Service Pack 2 for Windows로 업그레이드할 수 있습니다:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 (빌드 6.0.4.1424) / MP4 CF2 (빌드 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (빌드 6.0.4.1424) / MP4 CF2 (빌드 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (빌드 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (빌드 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (빌드 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (빌드 10.2.5.3201).

앞서 나열된 애플리케이션을 Kaspersky Endpoint Security 10 Service Pack 2 for Windows로 업그레이드할 때 격리 저장소와 백업 내용은 전송되지 않습니다.

이전 버전의 애플리케이션을 다음과 같이 업그레이드할 수 있습니다:

- 로컬에서 애플리케이션 설치 마법사 사용한 대화식 모드.
- 명령줄을 사용해 로컬에서 비대화식 모드
- Kaspersky Security Center 소프트웨어 스위트(*Kaspersky Security Center 구현 설명서* 참조)를 사용해 원격으로 작업
- Microsoft Windows의 그룹 정책 편집기(운영 체제 도움말 파일 참고)를 통해 원격으로 작업

이전 애플리케이션 버전을 Kaspersky Endpoint Security 10 Service Pack 2 for Windows로 업데이트하는 경우, 이전 애플리케이션 버전을 제거할 필요가 없습니다. 이전 애플리케이션 버전을 업그레이드하기 전에 열려 있는 모든 애플리케이션을 종료하는 것이 좋습니다.

애플리케이션 제거

이 섹션에서는 컴퓨터에서 Kaspersky Endpoint Security를 제거하는 방법을 설명합니다.

애플리케이션 제거 방법 정보

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

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

- 로컬에서 대화식 모드, 설치 마법사 사용
- 명령줄을 사용해 로컬에서 비대화식 모드

- Kaspersky Security Center 소프트웨어 스위트(자세한 내용은 *Kaspersky Security Center 구현 설명서*참조)를 사용해 원격으로 작업
- Microsoft Windows의 그룹 정책 편집기(운영 체제 도움말 파일 참고)를 통해 원격으로 작업

설치 마법사를 사용하여 애플리케이션 제거

설치 마법사를 사용하여 Kaspersky Endpoint Security를 제거하려면 다음과 같이 하십시오:

1. **시작** 메뉴에서 **애플리케이션 → Kaspersky Endpoint Security 10 for Windows → 수정, 복구 또는 제거**를 선택합니다.

   설치 마법사가 시작됩니다.

2. 설치 마법사의 **수정, 복구 또는 제거** 창에서 **제거** 버튼을 누릅니다.
3. 설치 마법사의 안내를 따릅니다.

1 단계. 나중에 사용하기 위해 애플리케이션 데이터 저장

이 단계에서는 다음에 애플리케이션을 설치할 때(예: 최신 버전 설치) 동일하게 유지하려는 애플리케이션의 데이터를 지정할 수 있습니다. 데이터를 지정하지 않으면 애플리케이션이 완전히 제거됩니다.

나중에 사용하기 위해 애플리케이션 데이터를 저장하려면 다음과 같이 하십시오,

저장하려는 데이터 유형 옆의 확인란을 선택합니다:

- **라이센스 데이터** - 나중에 다시 설치하는 애플리케이션을 활성화 할 때 필요한 데이터입니다. 이것은 설치 시점에 저장된 라이센스가 만료되기 전까지 저장된 라이센스로 자동으로 활성화됩니다.
- **백업 및 격리 저장소 파일** - 이 파일은 애플리케이션에서 검사 후 백업 또는 격리 저장소에 배치한 파일입니다.

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

  애플리케이션을 제거한 후 백업 및 격리 저장소 개체를 사용하려는 경우, 애플리케이션을 제거하기 전에 이러한 개체를 해당 저장소에서 복원시켜야 합니다. 그러나, 이러한 경우 컴퓨터에 나쁜 영향을 미칠 수 있기 때문에 Kaspersky 전문가는 백업 및 격리 저장소에서 파일 복원을 권장하지 않습니다.

- **애플리케이션 운영 설정** - 애플리케이션 구성 중에 선택한 애플리케이션 설정 값입니다.
- **암호화 키 로컬 저장소** - 애플리케이션의 제거 전에 암호화 된 파일 및 장치에 직접 접근할 수 있는 데이터입니다. 애플리케이션이 암호화 기능을 다시 설치 후 암호화 된 파일 및 드라이브에 직접 접근 할 수 있습니다.

  이 확인란은 기본적으로 선택되어 있습니다.

설치 마법사를 계속하려면 **다음** 버튼을 누릅니다. 설치 마법사를 중지하려면 **취소** 버튼을 누르십시오.

2 단계. 애플리케이션 제거 확인

애플리케이션을 제거하면 컴퓨터 보안이 위협을 받게 되므로 애플리케이션 제거를 확인하는 메시지가 나타납니다. 제거하려면 **제거** 버튼을 누르십시오.

애플리케이션 제거를 중지하려면 **취소** 버튼을 눌러 제거 작업을 취소할 수 있습니다.

3 단계. 애플리케이션 제거. 제거 완료

이 단계에서 설치 마법사는 애플리케이션을 컴퓨터에서 제거합니다. 애플리케이션 제거가 완료될 때까지 기다리십시오.

애플리케이션을 제거할 때 운영 체제를 재시작해야 할 수 있습니다. 제거한 즉시 재시작하지 않으면 운영 체제를 다시 시작하거나 컴퓨터를 끄고 다시 켤 때까지 애플리케이션 제거 완료가 연기됩니다.

명령줄을 통한 애플리케이션 제거

명령줄에서 애플리케이션 제거 프로세스를 시작할 수 있습니다. 제거는 대화식 모드 또는 자동 모드(애플리케이션 설치 마법사를 시작하지 않음)에서 수행됩니다.

대화식 모드에서 애플리케이션을 제거하려면,

명령줄에서 `setup.exe /x` 또는 `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`을 입력합니다.

설치 마법사가 시작됩니다. 설치 마법사의 안내를 따릅니다.

자동 모드에서 애플리케이션을 제거하려면,

명령줄에서 `setup.exe /s /x` 또는 `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`을 입력합니다.

이러면 설치 마법사를 시작하지 않고 자동 모드로 애플리케이션 제거 프로세스가 시작됩니다.

만일 애플리케이션 제거 동작이 암호로 보호되어 있다면, 사용자 이름과 해당 암호를 명령줄에 입력해야 합니다.

대화식 모드에서 Kaspersky Endpoint Security의 제거, 수정 및 복구를 허용을 위한 사용자 이름과 암호를 사용하려면 명령줄에 다음을 입력합니다:

```
setup.exe /pKLLOGIN=<사용자 이름> /pKLPASSWD=***** /x 또는

msiexec.exe KLLOGIN=<사용자 이름> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-
56E6EF762275}.
```

설치 마법사가 시작됩니다. 설치 마법사의 안내를 따릅니다.

Kaspersky Endpoint Security의 제거, 수정 및 복구 시 사용자 이름 및 암호 인증이 설정된 경우 자동 모드로 명령줄에서 애플리케이션을 제거하려면 다음과 같이 합니다:

```
setup.exe /pKLLOGIN=<User name> /pKLPASSWD=***** /s /x 또는

msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<User name>
KLPASSWD=***** /qn.
```

인증 에이전트의 테스트 작업 후 남은 개체 및 데이터 제거하기

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 두 가지 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 유틸리티(복원 유틸리티)를 사용해 인증 에이전트의 테스트 작업 후 남아 있는 개체 및 데이터를 제거하려면 다음을 수행합니다:

1. 인증 에이전트의 테스트 작업 후에 개체 및 데이터가 남아 있는 연결된 시스템 하드 드라이브가 장착된 컴퓨터에서 Kaspersky Endpoint Security를 사용하여 생성된 fdert.exe 실행 파일을 실행하여 복원 유틸리티를 시작합니다.
2. 복원 유틸리티 창에 있는 **장치 선택** 드롭다운 목록에서 제거할 개체 및 데이터가 있는 시스템 하드 드라이브를 선택합니다.
3. **검색** 버튼을 누릅니다.
4. AA **개체 및 데이터 삭제** 버튼을 클릭합니다.

   그러면 인증 에이전트의 테스트 작업 후 남은 개체 및 데이터 제거 프로세스가 시작됩니다.

인증 에이전트의 테스트 작업 후 남은 개체 및 데이터를 제거한 후에 인증 에이전트와 애플리케이션의 비호환성에 대한 정보를 추가로 제거해야 할 수도 있습니다.

인증 에이전트와 애플리케이션의 비호환성에 대한 정보를 제거하려면,

명령줄에 `avp pbatestreset` 문자를 입력합니다.

`avp pbatestreset` 명령을 실행하려면 암호화 모듈을 설치해야 합니다.

애플리케이션 인터페이스

이 섹션은 애플리케이션 인터페이스의 주요 요소를 기술하고 있습니다.

작업 표시줄 알림 영역의 애플리케이션 아이콘

Kaspersky Endpoint Security를 설치하면 즉시 애플리케이션 아이콘이 Microsoft Windows 작업 표시줄 알림 영역에 나타납니다.

알림 영역 아이콘의 용도는 다음과 같습니다:

- 애플리케이션 활동을 나타냅니다.
- 마우스 오른쪽 메뉴 및 메인 애플리케이션 창에 대한 바로가기 역할을 합니다.

애플리케이션의 활동 표시

애플리케이션 아이콘은 애플리케이션 활동의 표시기 역할을 합니다:

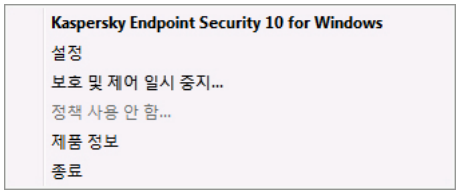
- 아이콘은 애플리케이션의 모든 보호 구성요소가 작동 중임을 나타냅니다.
- 아이콘은 Kaspersky Endpoint Security 운영 중 사용자의 주의가 필요한 중요 이벤트가 발생했을 때를 나타냅니다. 예를 들어 파일 안티 바이러스가 사용 중지되었거나 애플리케이션 데이터베이스가 오래된 것일 수 있습니다.
- 아이콘은 Kaspersky Endpoint Security 운영 중 위험 이벤트가 발생했을 때를 나타냅니다. 예를 들어 구성요소 작업이 실패하거나 애플리케이션 데이터베이스가 손상되었을 수 있습니다.

애플리케이션 아이콘 마우스 오른쪽 메뉴

애플리케이션 아이콘의 마우스 오른쪽 메뉴는 다음 항목을 포함하고 있습니다:

- **Kaspersky Endpoint Security 10 for Windows**. 메인 애플리케이션 창의 **보호 및 제어** 탭에서. **보호 및 제어** 탭에서는 애플리케이션 구성요소의 및 작업의 작동을 조정하고 처리된 파일과 탐지된 보안위협의 통계를 볼 수 있습니다.
- **설정**. 메인 애플리케이션 창의 **설정** 탭을 엽니다. **설정** 탭에서는 기본 애플리케이션 설정을 변경할 수 있습니다.
- **보호 및 제어 일시 중지/보호 및 제어 다시 시작**. 보호 및 제어 구성요소의 작동을 일시적으로 중지하거나 다시 시작합니다. 이 마우스 오른쪽 메뉴 항목은 업데이트 작업 및 검사 작업에 영향을 주지 않으며, Kaspersky Security Center 정책이 중지되었을 때에만 이용 가능합니다.
- **정책 사용 안 함/정책 사용**. Kaspersky Security Center 정책을 사용하거나 사용하지 않습니다. 이 메뉴 항목은 Kaspersky Endpoint Security가 정책에 따라 작동하고 Kaspersky Security Center 정책을 사용하지 않기 위한 암호가 설정되어 있는 경우 사용 가능합니다.
- **제품 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

Microsoft Windows의 작업 표시줄 알림 영역에 있는 애플리케이션 아이콘에 마우스 포인터를 올려 놓고 누르면 애플리케이션 아이콘의 마우스 오른쪽 메뉴를 열 수 있습니다.

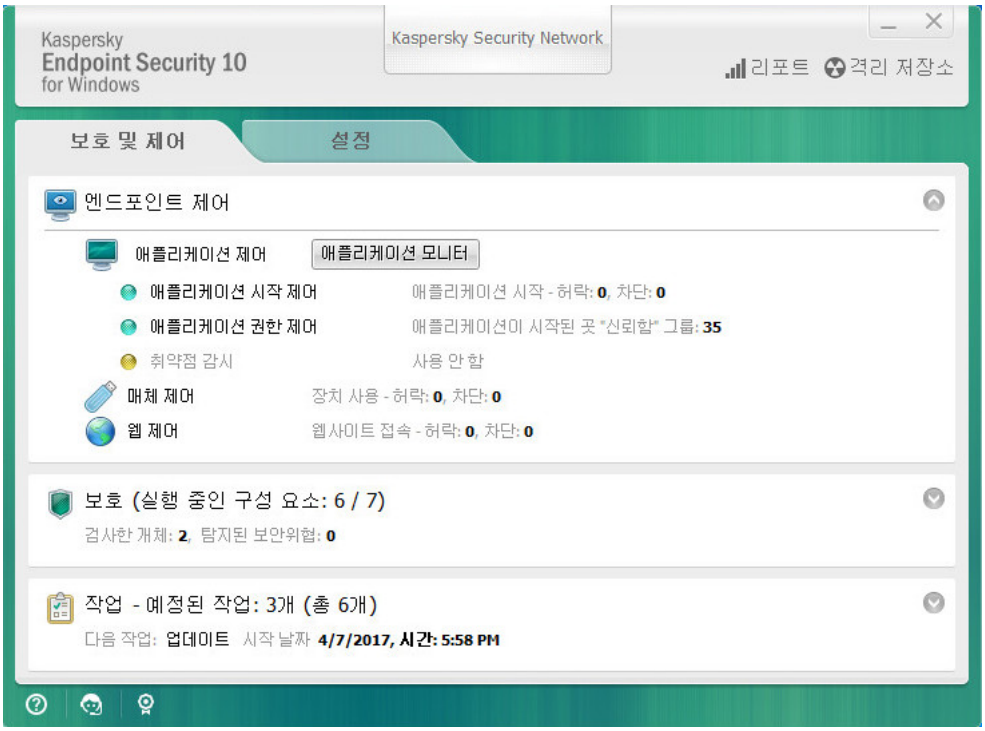
메인 애플리케이션 창

Kaspersky Endpoint Security의 메인 창에는 애플리케이션의 모든 주요 기능에 접근할 수 있는 인터페이스 요소가 포함되어 있습니다.

메인 애플리케이션 창은 다음 이미지와 같이 4가지 부분으로 구성됩니다:

- 창의 상단에는 다음과 같은 정보를 볼 수 있는 인터페이스 요소가 있습니다:
  - 애플리케이션 세부 정보
  - Kaspersky Security Network 참여 동의서
  - 처리되지 않은 파일 목록
  - 탐지된 취약점 목록
  - 격리된 파일 목록
  - 애플리케이션이 탐지한 감염 파일 복사본의 저장소
  - 전체 또는 별도의 구성요소에서 애플리케이션이 작동되거나 작업을 수행하는 동안 발생한 이벤트 리포트
- **보호 및 제어** 탭에서는 애플리케이션 구성요소 동작과 작업 완료를 제어할 수 있습니다. **보호 및 제어** 탭은 메인 애플리케이션 창을 열면 표시됩니다.
- **설정** 탭에서는 기본 애플리케이션 설정을 편집할 수 있습니다.
- 창 하단에는 다음과 같은 요소가 있습니다:
  - **버튼** . 이 버튼을 누르면 Kaspersky Endpoint Security 도움말 시스템으로 이동합니다.
  - **버튼** . 이 버튼을 누르면 운영 체제 정보, 현재 설치된 Kaspersky Endpoint Security의 버전 및 Kaspersky 정보 출처로 연결되는 링크 등이 포함된 **지원** 창이 열립니다.
  - **버튼** / . 이 버튼을 누르면 현재 사용 중인 라이센스에 대한 정보가 있는 **라이센스** 창이 열립니다.
  - **버튼** / / 이 버튼을 누르면 **이벤트** 창이 열리며 사용 가능한 업데이트뿐 아니라 암호화된 파일 및 장치에 대한 접근 요청에 대한 정보가 표시됩니다.

    접근 요청이나 설치하지 않은 업데이트가 있는 경우에만 이 버튼이 표시됩니다.



메인 애플리케이션 창

Kaspersky Endpoint Security의 메인 창을 열려면 다음 중 한 가지 방법을 수행하십시오:

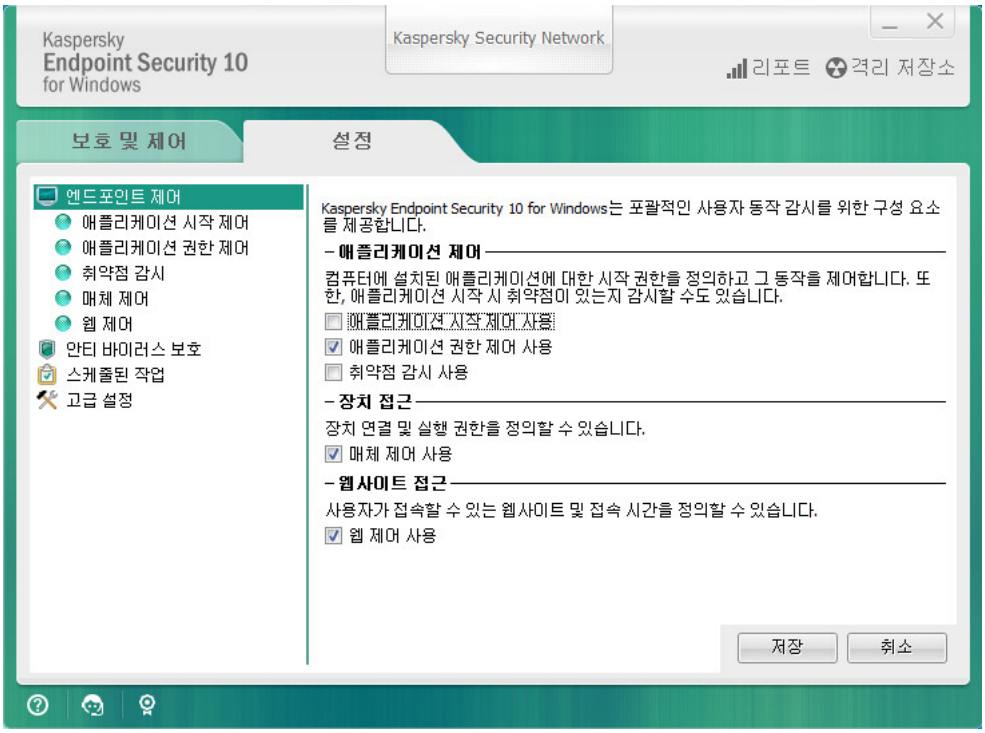
- Microsoft Windows 작업 표시줄 알림 영역에 있는 애플리케이션 아이콘을 누릅니다.
- **Kaspersky Endpoint Security 10 for Windows**(애플리케이션 아이콘의 컨텍스트 메뉴에서)을 선택하십시오.

애플리케이션 설정 구성 탭

Kaspersky Endpoint Security 설정 창에서는 전체 애플리케이션 설정, 개별 구성요소, 보고서 및 저장소, 검사 작업, 업데이트 작업, 취약점 검사 작업 및 Kaspersky Security Network와의 통신을 구성할 수 있습니다.

애플리케이션 설정 탭은 다음과 이미지와 같이 두 부분으로 구성됩니다:

- 왼쪽에는 애플리케이션 구성요소, 작업, 몇 가지 서브 섹션이 포함된 고급 설정 섹션이 있습니다.
- 오른쪽에는 고급 설정뿐 아니라 창 왼쪽에서 선택한 구성요소 또는 작업의 설정을 구성하는 데 사용하는 제어 요소가 있습니다.



애플리케이션 설정 구성 탭

애플리케이션 설정 탭을 열려면 다음 방법 중 하나를 수행합니다:

- 메인 애플리케이션 창에서 **설정** 탭을 선택합니다.
- 애플리케이션 아이콘의 마우스 오른쪽 메뉴에서 **설정**을 선택합니다.

애플리케이션 보호 및 제어 탭

Kaspersky Endpoint Security의 보호 및 제어 탭은 모든 작업의 수행 및 모든 애플리케이션 구성요소의 작동에 대한 일반적인 정보를 제공합니다. 이 탭에서 구성요소 작동 및 작업 수행을 조정할 수도 있습니다.

애플리케이션 보호 및 제어 탭은 세 부분으로 구성되어 있습니다(아래 그림 참조):

- **엔드포인트 제어** 섹션에는 제어 구성요소 목록이 있습니다.
- **보호 관리** 섹션에는 안티 바이러스 보호 구성요소 목록이 있습니다.
- **작업** 섹션에는 컴퓨터에서 실행되는 로컬 작업 목록이 있습니다.

각 섹션에는 구성요소를 작동 또는 중단하는 데 사용할 수 있는 제어 요소가 포함되어 있으므로 선택한 구성요소 또는 작업의 설정으로 이동하여 해당 구성요소 또는 작업의 작동 통계를 확인하세요.

애플리케이션 보호 및 제어 탭

애플리케이션 보호 및 제어 탭을 열려면 다음 처리 방법 중 하나를 수행합니다:

- 메인 애플리케이션 창에서 **보호 및 제어** 탭을 선택합니다.
- Microsoft Windows 작업 표시줄 알림 영역에 있는 애플리케이션 아이콘을 누릅니다.
- **Kaspersky Endpoint Security 10 for Windows**(애플리케이션 아이콘의 컨텍스트 메뉴에서)을 선택하십시오.

애플리케이션 라이센스

이 섹션에는 애플리케이션 라이센싱과 관련된 일반 개념 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 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.

유효한 라이센스가 있으면 다음과 같은 서비스 혜택을 받을 수 있습니다:

- 최종 사용자 라이센스 계약의 조건에 따른 애플리케이션의 사용
- 기술 지원

서비스 범위 및 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* - 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 활성화코드와 함께 전달된 문서입니다.

이 라이센스 인증서에는 다음 라이센스 정보가 들어 있습니다:

- 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 기기 개수)
- 라이센스 기간 시작 날짜
- 라이센스 만료 날짜 또는 라이센스 기간
- 라이센스 유형

서브스크립션 정보

*Kaspersky Endpoint Security용 서브스크립션*은 특정 파라미터(서브스크립션 만료일, 보호되는 기기 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 웹 사이트에서 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.

제한 서브스크립션의 경우 만료 시 서브스크립션을 갱신하기 위한 유예 기간이 제안될 수도 있습니다. 이 기간에는 애플리케이션이 모든 기능을 유지합니다. 서비스 제공업체에서 유예 기간을 적용할 것인지를 결정하며, 적용하는 경우 그 기간을 결정합니다.

서브스크립션으로 Kaspersky Endpoint Security를 사용하려면 서비스 공급업체로부터 받은 활성화코드를 적용해야 합니다. 활성화코드가 적용된 후에 활성 라이센스 키가 설치됩니다. 활성 라이센스 키는 서브스크립션 조건에서 애플리케이션을 사용하기 위한 라이센스를 정의합니다. 추가 키는 활성화코드를 사용할 때만 설치될 수 있으며 키 파일 또는 서브스크립션을 사용해 설치할 수 없습니다.

서브스크립션으로 사용 가능한 애플리케이션 기능은 다음 유형의 상업용 라이센스가 제공하는 기능입니다: Standard, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. 이들 유형의 라이센스는 파일 서버, 워크스테이션 및 모바일 장치 보호용으로 설계되었으며 워크스테이션 및 모바일 장치에서 제어 구성요소의 사용을 지원합니다.

가능한 서브스크립션 관리 옵션은 각 서비스 제공업체에 따라 다릅니다. 서비스 제공업체가 애플리케이션이 모든 기능을 유지하는 서브스크립션 갱신 유예 기간을 제공하지 않을 수도 있습니다.

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

활성화코드 정보

*활성화코드*는 Kaspersky Endpoint Security의 상업용 라이센스를 구매한 사용자에게 제공되는 20자리 코드입니다.

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

애플리케이션이 활성화코드를 사용하여 활성화 될 때, 활성 키가 설치됩니다. 추가 키는 활성화코드를 사용할 때만 설치될 수 있으며 키 파일 또는 서브스크립션을 사용해 설치할 수 없습니다.

만일 애플리케이션 활성화 후 활성화코드를 분실했다면, 해당 활성화코드를 복원할 수 있습니다. 예를 들어 Kaspersky CompanyAccount를 등록하려면 활성화코드가 필요할 수 있습니다. 활성화코드를 복원하려면 Kaspersky 기술 지원에 문의하십시오.

키 정보

*라이센스 키*는 고유한 영숫자 문자열입니다. 라이센스 키는 라이센스 인증서(라이센스 유형, 라이센스 유효 기간, 라이센스 제한)에 표시된 조건에서 애플리케이션의 사용을 가능하게 만듭니다.

라이센스 인증서는 서브스크립션 하에 설치된 라이센스 키에 대해서는 제공되지 않습니다.

라이센스 키는 활성화코드나 키 파일을 사용하여 애플리케이션에 추가할 수 있습니다.

라이센스 키를 추가, 편집 또는 삭제할 수 있습니다. 최종 사용자 라이선스 라이센스 계약서의 조건을 위반했다면, 해당 키는 Kaspersky에 의해 차단될 수 있습니다. 라이센스 키가 블랙리스트에 등록되면 다른 키를 추가해야 계속해서 애플리케이션을 사용할 수 있습니다.

만료된 라이센스를 삭제하면 애플리케이션 기능을 사용할 수 없습니다. 이러한 키는 삭제된 이후에는 다시 추가할 수 없습니다.

키에는 활성 라이센스 키와 추가 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.

*추가 키*는 사용자에게 애플리케이션을 사용하기 위한 권한을 부여하지만 현재 사용하지는 않습니다. 활성 라이센스 키가 만료되면 추가 라이센스 키가 자동으로 활성화됩니다. 추가 키는 활성 키가 이미 추가된 경우에만 추가할 수 있습니다.

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

라이센스 키가 블랙리스트에 등록되면 애플리케이션 활성 조건이 적용된 라이센스에 의해 정의된 애플리케이션 기능이 8일간 사용 가능한 상태가 됩니다. Kaspersky Security Network와 데이터베이스 및 애플리케이션 모듈 업데이트는 제한 없이 사용할 수 있습니다. 애플리케이션에서 해당 사용자에게 라이센스 키가 블랙리스트에 등록되었음을 통보합니다. 8일 이후에는 라이센스 만료 이후에도 이용 가능한 기능 수준으로 애플리케이션 기능이 일부 제한됩니다. 즉, 애플리케이션이 업데이트 없이 실행되며, Kaspersky Security Network 서비스를 사용할 수 없게 됩니다.

라이센스 키 파일 정보

*키 파일*은 Kaspersky Endpoint Security를 구매한 후에 받는 확장자가 .key인 파일입니다. 키 파일의 목적은 애플리케이션을 활성화하는 키를 추가하기 위한 것입니다.

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 공급업체로 문의.
- 기존 활성화코드를 기반으로 Kaspersky 웹사이트에서 키 파일을 받습니다.

애플리케이션을 키 파일을 사용하여 활성화하면 활성 키가 추가됩니다. 예약 라이센스 키는 키 파일을 사용해야만 추가할 수 있으며 활성화코드로는 추가할 수 없습니다.

데이터 제공 정보

귀하는 최종 사용자 라이센스 동의서에 동의하여 귀하의 제품 사용과 관련된 정보뿐 아니라 설치한 프로그램의 유형, 버전 및 지역 언어, 프로그램 설치 프로그램의 고유 식별자 및 설치 유형, 활성 키 및 예비 키 관련 데이터(라이센스 유형, 유효 기간, 프로그램 활성화 날짜 및 라이센스 만료 날짜, 라이센스 수, 라이센스 현재 상태, 활성화 서버 상호 작용 프로토콜 버전 포함) 정보를 자동으로 전송하기로 동의합니다.

활성화코드를 사용하여 프로그램을 활성화하는 경우 귀하는 배포 및 라이센스 소유자의 제품 사용에 관한 통계 정보를 수신하기 위해 정보를 제공받은 시점에 사용할 프로그램의 버전(설치된 프로그램 업데이트, 프로그램 설치 식별자 및 라이센스 관련 정보 포함), 운영 체제 버전, 활성 상태인 프로그램 구성요소 식별자를 자동으로 제공하기로 동의합니다.

Kaspersky에 제공된 정보는 법률 및 요건, Kaspersky의 해당 규정에 따라 보호됩니다.

Kaspersky는 제공된 정보를 완벽하게 익명 처리하여 일반 통계 데이터 형태로만 사용합니다. 일반 통계는 수집된 오리지널 정보를 이용해 자동으로 생성되고 개인 데이터 또는 다른 기밀 정보는 포함하고 있지 않습니다. 수집된 오리지널 정보는 누적되면 자동 파기됩니다(연 1회). 일반 통계 데이터는 무기한 저장됩니다.

최종 사용자 라이센스 계약서를 읽고 최종 사용자 라이센스 계약서와 KSN 정책에 동의한 이후에 애플리케이션 사용에 대한 정보를 당사가 수집, 처리, 저장 방법에 대한 자세한 내용을 보려면 Kaspersky 웹사이트에 방문하십시오. license.txt 및 ksn.txt 파일은 프로그램 배포 패키지의 일부로 최종 사용자 라이센스 계약서와 KSN 참여 라이센스 계약서가 들어 있습니다.

라이센스 정보 보기

라이센스 정보를 보려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 하단의 / 버튼을 누릅니다.

라이센스 창이 열립니다. 창 위쪽에 있는 섹션에 **라이센스** 정보가 표시되어 있습니다.

라이센스 구입

애플리케이션을 설치한 후 라이센스를 구매할 수 있습니다. 라이센스를 구입 시 애플리케이션을 활성화하는 활성화코드 또는 키 파일을 받을 수 있습니다.

라이센스를 구매하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 하단의 / 버튼을 누릅니다.
   라이센스 창이 열립니다.
3. **라이센스** 섹션에서 다음 중 하나를 수행합니다:
   - 추가된 키가 없거나 체험판이 설치되어 있다면, **라이센스 구매** 버튼을 누릅니다.
   - 상업용 라이센스를 설치한 경우 **라이센스 갱신** 버튼을 누릅니다.

   라이센스를 구입할 수 있는 Kaspersky 온라인 쇼핑몰의 웹사이트 창이 열립니다.

라이센스 갱신

라이센스가 거의 만료될 때 갱신할 수 있습니다. 현재 라이센스가 만료된 후와 새로운 라이센스로 애플리케이션을 활성화하기 전에 컴퓨터를 보호할 수 있습니다.

라이센스를 갱신하려면 다음과 같이 하십시오:

1. 새 애플리케이션 활성화코드 또는 키 파일을 받습니다.
2. 활성화코드 또는 받은 키 파일로 추가 키(예약 키)를 추가합니다.

추가 키가 추가됩니다. 이 키는 기존 라이센스가 만료될 때 활성화됩니다.

Kaspersky의 인증 서버 부하로 인해 추가 상태에서 활성 상태로 키가 업데이트 될 때까지 시간이 좀 걸릴 수 있습니다.

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.

서브스크립션(또는 서브스크립션 갱신이 가능한 서브스크립션 만료 후의 유예 기간) 만료일에 제한된 서브스크립션으로 애플리케이션을 사용한다면 Kaspersky Endpoint Security에서 해당되는 알림을 표시하고 서브스크립션의 갱신 시도를 자동으로 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 웹 사이트에서 서브스크립션을 갱신할 수 있습니다.

라이센스 창에서 서브스크립션 상태를 수동으로 업데이트할 수 있습니다. 이것은 유예 기간의 만료 후에 애플리케이션이 갱신되었으며 애플리케이션이 서브스크립션 상태를 자동으로 업데이트하지 않은 경우에 필요할 수도 있습니다.

서비스 제공 업체의 웹사이트 방문

애플리케이션 인터페이스에서 해당 서비스 제공업체의 웹 사이트를 방문하려면:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 하단의 / 버튼을 누릅니다.
   라이센스 창이 열립니다.
3. **라이센스** 창에서 **서브스크립션 판매처로 문의**를 클릭합니다.

애플리케이션 활성화 방법 정보

*활성화*란 라이센스가 만료될 때까지 정식 애플리케이션 버전을 사용할 수 있도록 라이센스를 활성화하는 절차를 말합니다. 애플리케이션 활성화 프로세스는 키 추를 포함합니다.

다음과 같은 방법으로 애플리케이션을 활성화할 수 있습니다:

- 초기 구성 마법사의 도움말을 사용하여 애플리케이션 설치. 이 방법으로 활성 키를 추가할 수 있습니다.
- 활성화 마법사를 사용하여 애플리케이션 인터페이스에서 로컬로. 이 방법으로 활성 라이센스 키와 추가 키를 모두 추가할 수 있습니다.
- Kaspersky Security Center 소프트웨어 스위트를 사용해 원격으로 키 작업 추가를 만들고 시작합니다. 이 방법으로 활성 키와 예약 키 모두를 추가할 수 있습니다.
- Kaspersky Security Center 중앙 관리 서버의 키 저장소에 저장된 라이센스를 클라이언트 컴퓨터에 자동으로 배포하여 원격으로 활성화(자세한 내용은 *Kaspersky Security Center 관리자 안내서* 참조). 이 방법으로 활성 키와 예약 키 모두를 추가할 수 있습니다.

  서브스크립션으로 구매한 활성화코드는 우선 배포됩니다.

- 명령 줄 사용.

Kaspersky의 인증 서버 부하로 인해 활성화코드로 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.

활성화 마법사를 통해 애플리케이션 활성화

활성화 마법사를 사용하여 Kaspersky Endpoint Security를 활성화하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창 하단의 / 버튼을 누릅니다.
   라이센스 창이 열립니다.
2. 열리는 **라이센스** 창에서 **새로운 라이센스로 애플리케이션 활성화** 버튼을 누릅니다.
   애플리케이션 활성화 마법사가 시작됩니다.
3. 활성화 마법사의 안내를 따릅니다.

애플리케이션 활성화 절차에 대한 자세한 내용은 초기 구성 마법사 섹션을 참조하십시오.

명령줄을 통한 애플리케이션 활성화

명령줄을 통한 애플리케이션을 활성화하려면,

명령줄에 `avp.com license /add <활성화코드나 키 파일> /password=<암호>`를 입력합니다.

애플리케이션 시작 및 중지

애플리케이션의 자동 시작을 구성하는 방법, 수동으로 애플리케이션을 시작 또는 중지하는 방법, 보호를 일시 중지하거나 다시 시작하는 방법 및 제어 구성요소에 대한 정보가 나와 있습니다.

애플리케이션 자동 시작 사용 및 중지

자동 시작이란 운영 체제가 시작하는 즉시 사용자의 조작 없이 Kaspersky Endpoint Security가 시작하는 것을 의미합니다. 이 애플리케이션 자동 시작 옵션은 기본적으로 설정되어 있습니다.

Kaspersky Endpoint Security를 설치한 후에 처음으로 Kaspersky Endpoint Security가 자동 시작됩니다. 그 후에는 운영 체제가 시작하면 애플리케이션이 자동으로 시작됩니다.

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 로드된 운영 체제에서 Kaspersky Endpoint Security가 시작될 때 안티 바이러스 데이터베이스를 다운로드하더라도 컴퓨터 보호 레벨이 낮아지지 않습니다.

애플리케이션 자동 시작을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 애플리케이션 자동 시작을 사용하려면, **컴퓨터 시작 시 Kaspersky Endpoint Security 10 시작** 확인란을 선택합니다.
   - 애플리케이션 자동 시작을 중지하려면 **컴퓨터 시작 시 Kaspersky Endpoint Security 10 for Windows 시작** 확인란을 선택 취소합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 수동 시작 및 중지

Kaspersky 전문가는 컴퓨터와 개인 데이터가 위협에 노출될 수 있기 때문에 Kaspersky Endpoint Security를 수동으로 중지하는 것을 권장하지 않습니다. 필요한 경우에는 애플리케이션을 중지하지 않고 원하는 기간 동안 컴퓨터 보호를 일시 중지할 수 있습니다.

이전에 애플리케이션 자동 시작을 중지한 경우, Kaspersky Endpoint Security를 수동으로 시작해야 합니다.

애플리케이션을 수동으로 시작하려면 다음과 같이 하십시오,

시작 메뉴에서 **애플리케이션** → **Kaspersky Endpoint Security 10 for Windows**를 선택합니다.

애플리케이션을 수동으로 시작하려면 다음과 같이 하십시오:

1. 작업 표시줄 알림 영역에 있는 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 눌러 마우스 오른쪽 메뉴를 엽니다.
2. 마우스 오른쪽 메뉴에서 **종료**를 선택합니다.

컴퓨터 보호 및 제어 일시 중지 및 다시 시작

컴퓨터 보호 및 제어 일시 중지는 Kaspersky Endpoint Security의 모든 보호 및 제어 구성요소를 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 중지되었음을 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 합니다:

1. 작업 표시줄 알림 영역에 있는 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 눌러 마우스 오른쪽 메뉴를 엽니다.
2. 마우스 오른쪽 메뉴에서 **보호 및 제어 일시 중지**를 선택합니다.

   보호 일시 중지 창이 열립니다.
3. 다음 옵션 중 하나를 선택합니다:
   - **지정한 시간 동안 일시 중지** - 드롭다운 목록에서 지정한 시간이 경과하면 컴퓨터 보호 및 제어가 다시 시작됩니다.
   - **다시 시작할 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. 이전 단계에서 **지정한 시간 동안 일시 중지** 옵션을 선택한 경우 드롭다운 목록에서 원하는 시간 간격을 선택합니다.

컴퓨터 보호 및 제어를 다시 시작하려면 다음과 같이 합니다:

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

사용자가 컴퓨터 보호 및 제어를 다시 시작하기로 선택한 경우 이전에 선택한 컴퓨터 보호 및 제어 일시 중지 옵션에 상관 없이 언제든지 다시 시작할 수 있습니다.

컴퓨터 파일 시스템 보호. 파일 안티 바이러스

파일 안티 바이러스에 대한 정보 및 구성요소 설정 구성 방법에 대한 지침이 나와 있습니다.

파일 안티 바이러스 정보

파일 안티 바이러스는 컴퓨터 파일 시스템이 감염되지 않도록 보호합니다. 기본적으로 파일 안티 바이러스는 Kaspersky Endpoint Security와 함께 시작되어 컴퓨터 메모리에 상주하며 컴퓨터 및 모든 드라이브에서 열리거나 저장되거나 시작된 모든 파일에 바이러스 및 기타 위협이 있는지 검사합니다.

파일에서 위협을 탐지할 때 Kaspersky Endpoint Security는 다음을 수행합니다:

1. 파일에서 탐지된 개체의 유형을 판별합니다(예, *바이러스* 또는 *트로이목마*).
2. *감염 의심*으로 된 파일(검사 결과 파일이 감염되었는지 여부를 확인할 수 없는 경우). 이 파일에는 바이러스 또는 기타 악성 코드를 상징하는 일련의 코드 또는 알려진 바이러스의 변형된 코드가 포함될 수 있습니다.
3. 애플리케이션은 파일에서 탐지된 악성 개체에 대한 알림을 표시하고(알림이 구성된 경우), 파일 안티 바이러스 설정에 지정된 조치를 취하여 파일을 처리합니다.

파일 안티 바이러스 작동 및 중지

기본적으로 파일 안티 바이러스는 작동되며 Kaspersky 전문가가 권장하는 모드에서 실행됩니다. 필요한 경우 파일 안티 바이러스를 중지할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

메인 애플리케이션 창의 보호 및 제어 탭에서 파일 안티 바이러스를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **보호** 섹션을 누릅니다.
   보호 섹션이 열립니다.
4. 이 섹션을 마우스 오른쪽 버튼으로 눌러 파일 안티 바이러스 구성요소에 대한 정보가 포함된 메뉴를 엽니다.
   구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.
5. 다음 중 하나를 수행합니다:
   - 파일 안티 바이러스를 작동하려면 메뉴에서 **시작**을 선택합니다.
     파일 안티 바이러스 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.
   - 파일 안티 바이러스를 중지하려면 메뉴에서 **중지**를 선택합니다.

파일 안티 바이러스 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 파일 안티 바이러스를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - **파일 안티 바이러스**를 작동하려면 파일 안티 바이러스 작동 확인란을 선택합니다.
   - **파일 안티 바이러스**를 중지하려면 파일 안티 바이러스 작동 확인란을 선택 취소합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

파일 안티 바이러스 자동 일시 중지

지정한 시간이 되거나 특정 프로그램을 처리할 때 자동으로 파일 안티 바이러스가 일시 중지하도록 구성할 수 있습니다.

일부 프로그램과 충돌할 때 파일 안티 바이러스를 일시 중지하는 것은 비상 조치입니다. 구성요소가 작동하는 중에 충돌이 발생할 경우 Kaspersky 기술 지원(https://companyaccount.kaspersky.com)에 문의하는 것이 좋습니다. 기술 지원 전문가의 도움을 받아 파일 안티 바이러스가 컴퓨터의 다른 프로그램과도 동시에 실행되도록 설정할 수 있습니다.

파일 안티 바이러스를 자동으로 일시 중지하도록 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   파일 안티 바이러스 창이 열립니다.
4. **파일 안티 바이러스** 창에서 **고급** 탭을 선택합니다.
5. **작업 일시 중지** 섹션에서 다음을 수행합니다:
   - 파일 안티 바이러스가 지정된 시간에 자동으로 일시 중지되도록 구성하려면 **스케줄에 따라 실행** 확인란을 선택하고 **스케줄** 버튼을 누릅니다.
     작업 일시 중지 창이 열립니다.
   - 지정된 애플리케이션이 시작할 때 파일 안티 바이러스가 자동으로 일시 중지되도록 구성하려면 **애플리케이션 시작 시** 확인란을 선택하고 **선택** 버튼을 누릅니다.
     애플리케이션 창이 열립니다.
6. 다음 중 하나를 수행합니다:

- 파일 안티 바이러스가 지정된 시간에 자동으로 일시중지 되도록 구성하는 경우 **작업 일시 중지** 창에서 **작업 일시 중지 시간** 및 **작업 다시 시작 시간** 필드를 통해 파일 안티 바이러스가 일시 중지되는 기간을 HH:MM 형식으로 지정합니다. **확인**을 누릅니다.

- 지정된 애플리케이션이 시작할 때 파일 안티 바이러스가 자동으로 일시 중지되도록 구성하는 경우 애플리케이션 창의 **추가**, **편집** 및 **제거** 버튼을 통해 파일 안티 바이러스가 일시 중지되는 **애플리케이션**의 목록을 작성합니다. **확인**을 누릅니다.

7. **파일 안티 바이러스** 창에서 **확인**을 누릅니다.

8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

파일 안티 바이러스 구성

파일 안티 바이러스를 구성하려면 다음과 같이 하십시오:

- 보안 레벨을 변경합니다.

  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.

- 감염된 파일 탐지 시 파일 안티 바이러스가 수행할 처리 방법을 변경합니다.

- 파일 안티 바이러스의 보호 영역을 편집합니다.

  검사할 개체를 추가 또는 삭제하거나 검사할 파일 형식을 변경하여 보호 범위를 확장 또는 제한할 수 있습니다.

- 휴리스틱 분석을 구성합니다.

  파일 안티 바이러스는 시그니처 분석이라는 기법을 사용합니다. 시그니처 분석 시 파일 안티 바이러스는 애플리케이션의 안티 바이러스 데이터베이스의 기록과 탐지된 개체가 일치하는지 확인합니다. Kaspersky 전문가의 권고에 따라 기본적으로 시그니처 분석이 사용되도록 선택되어 있습니다.

  보호의 효율성을 높이려면 휴리스틱 분석을 사용합니다. 휴리스틱 분석 시 파일 안티 바이러스는 운영 체제의 개체 활동을 분석합니다. 휴리스틱 분석을 사용하면 현재 애플리케이션의 안티 바이러스 데이터베이스에 기록이 없는 악성 개체도 탐지할 수 있습니다.

- 검사를 최적화합니다.

  파일 안티 바이러스에서 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 사용하도록 설정하면 최근에 검사된 후로 변경되지 않은 파일을 예외하여 파일 검사 속도를 최적화할 수 있습니다.

- 복합 파일 검사를 구성합니다.

- 파일 검사 모드를 변경합니다.

보안 레벨 변경

컴퓨터의 파일 시스템을 보호하기 위해 파일 안티 바이러스는 다양한 설정 그룹을 적용합니다. 이러한 설정 그룹을 *보안 레벨*이라고 합니다. 3개의 사전 설정된 보안 레벨이 있습니다: **높음**, **권장** 및 **낮음**. **권장** 보안 레벨 설정은 가장 적당한 것으로 간주되어 Kaspersky 전문가가 권장하는 설정입니다.

보안 레벨을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 다음 중 하나를 수행합니다:
   - 미리 설정된 보안 레벨(**높음**, **권장** 또는 **낮음**) 중 하나를 설정하려는 경우 슬라이더로 레벨을 선택합니다.
   - 사용자 지정 보안 레벨을 구성하려는 경우 **설정** 버튼을 누르면 열리는 **파일 안티 바이러스** 창에서 사용자 지정 설정을 입력합니다.
     사용자 지정 보안 레벨을 구성하면, **보안 레벨** 섹션의 보안 레벨 이름이 **사용자 지정**으로 변경됩니다.
   - 보안 레벨을 **권장**으로 변경하려면 **기본값** 버튼을 누릅니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

감염된 파일에 수행할 파일 안티 바이러스 처리 방법 변경

감염된 파일에 수행할 파일 안티 바이러스 처리 방법을 변경하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **위협 탐지 시 처리 방법** 섹션에서 필요한 옵션을 선택합니다:
   - **자동으로 처리 방법 선택**.
   - **처리 방법 선택: 치료. 삭제해야 처리되는 것은 삭제**.
   - **처리 방법 선택: 치료**.

     이 옵션을 선택하면, Windows Store 애플리케이션에 포함되는 파일은 **제거**합니다.
   - **처리 방법 선택: 제거**.
   - **처리 방법 선택: 차단**.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

파일 안티 바이러스의 보호 영역 편집

보호가 작동되는 경우 구성요소가 검사하는 개체를 보호 범위이라고 합니다. 각 구성 요소의 보호 범위는 서로 다른 속성을 가집니다. 검사되는 파일의 유형과 위치는 파일 안티 바이러스의 보호 영역의 속성입니다. 파일 안티 바이러스는 기본적으로 하드 드라이브, 네트워크 드라이브 또는 이동식 장치에 저장되는 감염 위험이 있는 파일만 검사합니다.

보호 범위를 만들려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   파일 안티 바이러스 창이 열립니다.
4. **파일 안티 바이러스** 창에서 **일반** 탭을 선택합니다.
5. **파일 유형** 섹션에서 파일 안티 바이러스가 검사 작업을 수행할 파일 유형을 지정합니다:
   - **모든 파일**을 검사하려면 모든 파일을 선택합니다.
   - **감염 가능성이 높은 파일 - 확장자 분석**의 파일만 검사하려면 파일 형식에 따라 검사를 선택합니다.
   - **감염 가능성이 높은 파일 - 알려진 확장자**를 가진 파일만 검사하려면 파일 확장자에 따라 검사를 선택합니다.

   검사할 파일 유형을 선택할 때 다음 정보를 참조하십시오:
   - .txt와 같은 일부 파일 형식에서는 악성 코드가 침투한 후 활성화될 가능성은 매우 낮습니다. 반면, 실행 코드(예: .exe, .dll, .doc)를 포함하거나 포함할 수 있는 형식의 경우. 악성 코드가 침투하여 활성화될 위험이 매우 높습니다.
   - 침입자가 실행 파일의 이름을 .txt 확장명으로 변경하고 컴퓨터에 바이러스나 기타 악성 코드를 보낼 수도 있습니다. 그런데 파일 확장자에 따라 검사를 선택하면 검사에서 이런 파일은 건너뛰게 됩니다. 확장자와 상관없이 형식별 파일 검사를 선택한 경우에는 파일 안티 바이러스가 파일 헤더를 분석합니다. 이 분석에서 .exe 형식인 것으로 파일이 밝혀질 수 있습니다. 실행 파일로 판명되면 바이러스 또는 기타 악성 코드가 있는지 철저하게 검사할 수 있습니다.
6. **보호 범위** 목록에서 다음 중 하나를 수행합니다:
   - 검사 범위에 새로운 개체를 추가하려면 **추가** 버튼을 누릅니다.
   - 개체의 위치를 변경하려면, 검사 범위에서 개체를 선택하고 **편집** 버튼을 누릅니다.

   검사 범위 선택 창이 열립니다.
   - 검사할 개체 목록에서 개체를 제거하려면 목록에서 해당 개체를 선택한 후 **제거** 버튼을 누릅니다.
     그러면 삭제 여부 확인하는 창이 열립니다.
7. 다음 중 하나를 수행합니다:
   - 검사할 개체 목록에서 개체의 위치를 변경하거나 새 개체를 추가하려면 **검사 범위 선택** 창에서 개체를 선택하고 **추가** 버튼을 누릅니다.
     검사 영역 선택 창에서 선택된 모든 개체가 **파일 안티 바이러스** 창의 **보호 영역** 목록에 표시됩니다.
     확인을 누릅니다.

- 개체를 제거하려면 제거 여부를 확인하는 창에서 **예** 버튼을 누릅니다.

8. 필요할 경우 6-7 단계를 반복하여 검사할 개체의 목록에 개체를 추가, 이동 또는 제거합니다.

9. 검사할 개체의 목록에서 개체를 예외하려면 **보호 범위** 목록에서 해당 개체 옆의 확인란을 선택 취소합니다. 그러면 파일 안티 바이러스에서 해당 개체를 검사하지 않지만 검사할 개체 목록에는 계속 남아 있습니다.

10. **파일 안티 바이러스** 창에서 **확인**을 누릅니다.

11. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

파일 안티 바이러스에 휴리스틱 분석기 사용

파일 안티 바이러스 작업에 휴리스틱 분석기를 사용하도록 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.

3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   파일 안티 바이러스 창이 열립니다.

4. **파일 안티 바이러스** 창에서 **성능** 탭을 선택합니다.

5. **검사 방법** 섹션에서 다음을 수행합니다:

   - 파일 안티 바이러스에서 휴리스틱 분석기를 사용하도록 설정하려면 **휴리스틱 분석** 확인란을 선택하고 슬라이더를 사용하여 휴리스틱 분석의 레벨을 지정합니다: **기본**, **자세히** 및 **매우 자세히**.

   - 파일 안티 바이러스에서 **휴리스틱 분석**을 사용하지 않도록 설정하려면 휴리스틱 분석기 확인란을 선택 취소합니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

파일 안티 바이러스 작업에 검사 기술 사용

파일 안티 바이러스 작업에 검사 기술을 사용하도록 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.

3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   파일 안티 바이러스 창이 열립니다.

4. **파일 안티 바이러스** 창에서 **고급** 탭을 선택합니다.
5. **검사 기술** 섹션에서 다음을 수행합니다:
   - 파일 안티 바이러스 작업에 사용할 기술의 이름 옆에 있는 확인란을 선택합니다.
   - 파일 안티 바이러스 작업에 사용하지 않을 기술의 이름 옆에 있는 확인란을 선택 취소합니다.
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

파일 검사 최적화

파일 검사를 최적화하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **설정** 버튼을 누릅니다.
   파일 안티 바이러스 창이 열립니다.
4. **파일 안티 바이러스** 창에서 **성능** 탭을 선택합니다.
5. **검사 최적화** 섹션에서 **새로운 것이나 변경된 파일만 검사** 확인란을 선택합니다.
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

복합 파일 검사

바이러스나 기타 악성 프로그램을 숨기는 일반적인 방법은 압축 파일이나 이메일 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 집합을 제한하는 방법으로 검사 속도를 높일 수 있습니다.

감염된 복합 파일을 처리하는 방법(치료 또는 삭제)은 파일 유형에 따라 달라집니다.

파일 안티 바이러스는 RAR, ARJ, ZIP, CAB 및 LHA 형식의 복합 파일을 치료하고 다른 모든 형식의 파일을 삭제합니다(메일 데이터베이스 예외).

복합 파일 검사를 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   파일 안티 바이러스 창이 열립니다.
4. **파일 안티 바이러스** 창에서 **성능** 탭을 선택합니다.
5. **복합 파일 검사** 섹션에서 검사할 복합 파일의 유형을 지정합니다: 압축 파일, 설치 패키지, 오피스 형식의 파일.
6. 새로운 및 변경된 복합 파일만 검사하려면 **새로운 것이나 변경된 파일만 검사** 확인란을 선택합니다.
   그러면, 파일 안티 바이러스는 모든 유형의 새로운 및 변경된 복합 파일만 검사합니다.
7. **고급** 버튼을 누릅니다.
   복합 파일 창이 열립니다.
8. **백그라운드 검사** 섹션에서 다음 중 하나를 수행합니다:
   - 파일 안티 바이러스가 백그라운드에서 복합 파일을 압축해제하지 않도록 하려면 **백그라운드에서 복합 파일 압축해제** 확인란을 선택 취소합니다.
   - 파일 안티 바이러스가 백그라운드에서 복합 파일을 압축해제하도록 하려면, **백그라운드에서 복합 파일 압축해제** 확인란을 선택하고 **최소 파일 크기** 필드에 필요한 값을 지정합니다.
9. **크기 제한** 섹션에서 다음 중 하나를 수행합니다:
   - 파일 안티 바이러스가 대용량 복합 파일을 압축해제하지 않게 하려면, **다음보다 큰 복합 파일은 압축해제 안 함** 확인란을 선택하고 **최대 파일 크기** 필드에 필요한 값을 지정합니다. 파일 안티 바이러스가 지정한 크기보다 큰 복합 파일을 압축 해제하지 않습니다.
   - 파일 안티 바이러스가 대용량 복합 파일을 압축해제하도록 하려면 **다음보다 큰 복합 파일은 압축해제 안함** 확인란을 선택 취소합니다.
     최대 파일 크기 필드의 값을 초과하는 크기의 파일은 대용량으로 간주됩니다.

   파일 안티 바이러스는 **다음보다 큰 복합 파일은 압축해제 안 함** 확인란의 선택 여부에 관계 없이 압축해제된 대용량 파일을 검사합니다.
10. **확인**을 누릅니다.
11. **파일 안티 바이러스** 창에서 **확인**을 누릅니다.
12. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

검사 모드 변경

*검사 모드*는 파일 안티 바이러스가 파일 검사를 시작하는 조건을 의미합니다. 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 안티 바이러스가 파일의 감시 여부를 결정합니다. 예를 들어 Microsoft Office Word문서 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. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **파일 안티 바이러스**를 선택합니다.
   창 오른쪽에 파일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   파일 안티 바이러스 창이 열립니다.
4. **파일 안티 바이러스** 창에서 **고급** 탭을 선택합니다.
5. **검사 모드** 섹션에서 필요한 방식을 선택합니다:
   - **스마트 모드**.
   - **접근 및 수정 시**.
   - **접근 시**.
   - **실행 시**.
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

이메일 보호. 메일 안티 바이러스

이 구성요소는 Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성요소는 Kaspersky Endpoint Security가 파일 서버용 Microsoft servers에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

이 섹션에는 메일 안티 바이러스에 대한 정보 및 구성요소 설정 구성 방법에 대한 지침이 나와 있습니다.

메일 안티 바이러스 정보

메일 안티 바이러스는 보내고 받는 이메일 메시지에 바이러스 및 기타 위협이 있는지 검사합니다. 메일 안티 바이러스는 Kaspersky Endpoint Security와 함께 시작되어 컴퓨터 메모리에 상주하며 POP3, SMTP, IMAP, MAPI 및 NNTP 프로토콜을 통해 보내거나 받은 모든 메시지를 검사합니다. 메시지에서 위협이 탐지되지 않으면 이메일 메시지를 읽을 수 있도록 처리됩니다.

이메일 메시지에서 위협을 탐지할 때 메일 안티 바이러스는 다음을 수행합니다:

1. 이메일 메시지에서 탐지된 개체의 유형을 판별합니다(예, *트로이목마*).
2. 이메일 메시지에 다음 상태 중 하나가 지정됩니다:
   - *감염 의심*. 검사 결과 이메일 메시지가 확실히 감염되었는지 알 수 없는 경우 이 상태가 지정됩니다. 이러한 이메일 메시지에는 바이러스 또는 기타 악성 코드를 상징하는 코드 섹션 또는 알려진 바이러스의 변형된 코드가 포함될 수 있습니다.
   - *감염됨*. 이메일 이미지의 검사 결과 Kaspersky Endpoint Security의 안티 바이러스 데이터베이스에 등록된 바이러스 코드 부분이 탐지된 경우 이 상태가 개체에 지정됩니다.
   - *개체 없음*. 이메일 메시지 검사 결과 바이러스 또는 기타 보안위협이 감지되지 않는 경우 이 상태가 개체에 지정됩니다.

그러면 애플리케이션은 이메일 메시지를 차단하고, 탐지된 보안위협에 대한 알림 서비스 알림을 표시하며(알림 설정에 지정된 경우), 메일 안티 바이러스 설정에 지정된 감염된 이메일 메시지에 수행할 처리 방법을 수행합니다.

이 구성요소는 컴퓨터에 설치된 메일 클라이언트와 상호 작용합니다. Microsoft Office Outlook® 메일 클라이언트용으로 개발된 내장 확장 프로그램을 사용해 메시지 검사 설정을 세부 조정합니다. 메일 안티 바이러스 확장 프로그램은 Kaspersky Endpoint Security가 설치될 때 Microsoft Office Outlook 메일 클라이언트에 통합됩니다.

메일 안티 바이러스 작동은 작업 표시줄의 알림 영역에 있는 애플리케이션 아이콘에 의해 확인할 수 있습니다. 메일 안티 바이러스는 이메일 메시지를 검사하면, 애플리케이션 아이콘은 으로 변경됩니다.

메일 안티 바이러스 작동 및 중지

기본적으로 메일 안티 바이러스는 작동되며 Kaspersky 전문가가 권장하는 모드에서 실행됩니다. 필요한 경우 메일 안티 바이러스를 중지할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서

- 애플리케이션 설정 창 사용

메인 애플리케이션 창의 보호 및 제어 탭에서 메일 안티 바이러스를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **보호** 섹션을 누릅니다.
   보호 섹션이 열립니다.
4. 이 섹션을 마우스 오른쪽 버튼을 눌러 메일 안티 바이러스 구성요소에 대한 정보가 포함된 줄의 마우스 오른쪽 메뉴를 엽니다.
   구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.
5. 다음 중 하나를 수행합니다:
   - 메일 안티 바이러스를 작동하려면 메뉴에서 **시작**을 선택합니다.
     메일 안티 바이러스 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.
   - 메일 안티 바이러스를 중지하려면 메뉴에서 **중지**를 선택합니다.
     메일 안티 바이러스 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 메일 안티 바이러스를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **메일 안티 바이러스**를 선택합니다.
   창 오른쪽에 메일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 메일 안티 바이러스를 작동하려면 **메일 안티 바이러스** 작동 확인란을 선택합니다.
   - 메일 안티 바이러스를 중지하려면 **메일 안티 바이러스** 중지 확인란을 선택합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

메일 안티 바이러스 구성

메일 안티 바이러스를 구성하려면 다음과 같이 하십시오:

- 이메일 보안 레벨 변경.
  기본 제공되는 이메일 보안 레벨 중 하나를 선택하거나 사용자지정 이메일 보안 레벨을 구성할 수 있습니다.
  이메일 보안 레벨 설정을 변경한 경우 언제든지 권장 이메일 보안 레벨로 되돌릴 수 있습니다.
- Kaspersky Endpoint Security가 감염된 메시지에 수행할 처리 방법을 변경합니다.
- 메일 안티 바이러스의 보호 영역 편집.

- 이메일 메시지에 첨부된 복합 파일의 검사를 구성합니다.

  이메일 첨부파일 검사를 작동 또는 중지하거나, 검사되는 첨부파일의 최대 크기 및 첨부파일 검사에 걸리는 최대 시간을 제한할 수 있습니다.

- 이메일 첨부파일 형식을 기준으로 필터링하도록 구성.

  파일 형식에 따라 이메일 첨부파일을 필터링하면 자동으로 지정된 형식 파일의 이름을 바꾸거나 파일을 삭제할 수 있습니다.

- 휴리스틱 분석을 구성합니다.

  보호의 효율성을 높이려면 휴리스틱 분석을 사용합니다. 휴리스틱 분석 시 Kaspersky Endpoint Security는 운영 체제의 애플리케이션 활동을 분석합니다. 휴리스틱 분석을 사용하면 현재 Kaspersky Endpoint Security 데이터베이스에 기록이 없는 메시지를 통한 보안위협도 탐지할 수 있습니다.

- Microsoft Office Outlook의 이메일 검사를 구성합니다.

  Microsoft Office Outlook 메일 클라이언트용으로 개발된 내장 확장 프로그램을 사용하면 메일 검사 설정을 간편하게 구성할 수 있습니다.

  Microsoft Outlook Express®, Windows Mail 및 Mozilla™ Thunderbird™와 같은 다른 메일 클라이언트을 사용할 경우 메일 안티 바이러스 구성요소는 SMTP, POP3, IMAP 및 NNTP 메일 프로토콜을 통해 전송되는 트래픽을 검사합니다.

  Mozilla Thunderbird 메일 클라이언트에서 **사서함** 폴더에서 메시지를 이동하는 필터를 사용하면 메일 안티 바이러스가 IMAP 프로토콜을 통해 전송되는 메시지에 대해 바이러스 및 기타 보안위협 검사를 수행하지 않습니다.

이메일 보안 레벨 변경

메일 안티 바이러스는 이메일을 보호하기 위해 다양한 설정 그룹을 적용합니다. 이러한 설정 그룹을 *이메일 보안 레벨*이라고 합니다. 3개의 보안 레벨이 있습니다: **높음**, **권장** 및 **낮음**. **권장** 이메일 보안 레벨은 최적의 설정으로 Kaspersky에서 권장하는 레벨입니다.

이메일 보안 레벨을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **메일 안티 바이러스**를 선택합니다.

   창 오른쪽에 메일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 다음 중 하나를 수행합니다:

   - 기본 제공 이메일 보안 레벨 중 하나를 지정하려는 경우(**높음**, **권장** 또는 **낮음**) 슬라이더를 사용하여 선택합니다.
   - 사용자 지정 이메일 보안 레벨을 구성하려는 경우 **설정** 버튼을 눌러 **메일 안티 바이러스** 창에서 설정을 지정합니다.

     사용자 지정 이메일 **보안 레벨**을 구성하면 보안 레벨 섹션의 이메일 보안 레벨의 이름이 **사용자 지정**으로 변경됩니다.
   - 이메일 보안 레벨을 **권장**으로 변경하려면 **기본값** 버튼을 누릅니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

감염된 이메일 메시지에 수행할 처리 방법 변경

감염된 이메일 메시지에 수행할 처리 방법을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **메일 안티 바이러스**를 선택합니다.
   창 오른쪽에 메일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **위협 탐지 시 처리 방법** 섹션에서는 감염된 메시지가 탐지될 경우 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:
   - **자동으로 처리 방법 선택**.
   - **처리 방법 선택: 치료. 삭제해야 처리되는 것은 삭제**.
   - **처리 방법 선택: 치료**.
   - **처리 방법 선택: 제거**.
   - **처리 방법 선택: 차단**.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

메일 안티 바이러스의 보호 영역 편집

보호 범위란 활성 상태의 구성요소에서 검사되는 개체를 말합니다. 각 구성 요소의 보호 범위는 서로 다른 속성을 가집니다. 메일 안티 바이러스의 보호 영역 속성에는 메일 안티 바이러스를 메일 클라이언트에 통합하는 설정 및 메일 안티 바이러스에서 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 안티 바이러스의 보호 영역을 만들려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **메일 안티 바이러스**를 선택합니다.
   창 오른쪽에 메일 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **설정** 버튼을 누릅니다.
   메일 안티 바이러스 창이 열립니다.
4. **일반** 탭을 선택합니다.
5. **보호 범위** 섹션에서 다음 중 하나를 수행합니다:
   - 메일 안티 바이러스가 컴퓨터에서 주고 받는 모든 메시지를 검사하도록 하려면 **보내거나 받는 모든 메시지** 옵션을 선택합니다.

- 메일 안티 바이러스가 컴퓨터에서 받는 메시지만 검사하도록 하려면 **받는 메시지** 옵션을 선택합니다.

  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.

6. **연결성** 섹션에서는 다음을 수행합니다:

   - POP3, SMTP, NNTP 및 IMAP 프로토콜을 통해 전송되는 메시지가 컴퓨터에 도착하기 전에 메일 안티 바이러스에서 이러한 이메일 메시지를 검사하도록 하려면 **POP3/SMTP/NNTP/IMAP 트래픽** 확인란을 선택합니다.

     POP3, SMTP, NNTP 및 IMAP 프로토콜을 통해 전송되는 메시지가 컴퓨터에 도착하기 전에 메일 안티 바이러스에서 이러한 이메일 메시지를 검사하지 않도록 하려면 **POP3/SMTP/NNTP/IMAP 트래픽** 확인란을 선택 취소합니다. 이 경우 Microsoft Office Outlook 메일 클라이언트에 내장된 메일 안티 바이러스 확장 프로그램이 사용자 컴퓨터에 메일이 도착하는 즉시 메일을 검사합니다. 단, **추가: Microsoft Office Outlook 확장 프로그램** 확인란을 선택해야 합니다.

     Microsoft Office Outlook이 아닌 다른 메일 클라이언트를 사용하는 경우 **POP3/SMTP/NNTP/IMAP 트래픽** 확인란이 선택 취소되어 있으면, 메일 안티 바이러스는 POP3, SMTP, NNTP 및 IMAP 프로토콜을 통해 전송되는 이메일 메시지를 검사하지 않습니다.

   - Microsoft Office Outlook에서 메일 안티 바이러스 설정에 대한 액세스를 개방하고 POP3, SMTP, NNTP, IMAP 및 MAPI 프로토콜을 통해 전송되는 메일 메시지가 컴퓨터가 도착한 후에 Microsoft Office Outlook에 통합된 확장 프로그램에서 이를 검사하도록 하려면 다음을 선택합니다. **추가: Microsoft Office Outlook 확장 프로그램** 확인란.

     Microsoft Office Outlook에서 메일 안티 바이러스 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 검사하도록 하지 않으려면 다음을 선택 해제합니다. **추가: Microsoft Office Outlook 확장 프로그램** 확인란.

     메일 안티 바이러스 확장 프로그램은 Kaspersky Endpoint Security가 설치될 때 Microsoft Office Outlook 메일 클라이언트에 통합됩니다.

7. **확인**을 누릅니다.

8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

이메일 메시지에 첨부된 복합 파일 검사

이메일 메시지에 첨부된 복합 파일의 검사를 구성하려면:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **메일 안티 바이러스**를 선택합니다.
   창 오른쪽에 메일 안티 바이러스 구성요소의 설정이 표시됩니다.

3. **설정** 버튼을 누릅니다.
   메일 안티 바이러스 창이 열립니다.

4. **일반** 탭을 선택합니다.

5. **복합 파일 검사** 섹션에서 다음과 같이 하십시오:

   - 메일 안티 바이러스가 메시지에 첨부된 압축 파일을 건너뛰도록 설정하려면 **첨부된 압축파일 검사** 확인란을 선택 취소합니다.
   - 메일 안티 바이러스에서 크기가 N MB 이상인 첨부파일을 건너뛰도록 설정하려면 **다음보다 큰 압축파일 검사 안 함 N Mb** 확인란을 선택합니다. 이 확인란을 선택한 경우 확인란 이름 옆에 있는 필드에서 압축 파일의 최대 크기를 지정해야 합니다.
   - 메일 안티 바이러스가 검사에 N초 이상 걸리는 메일 첨부파일을 검사하도록 설정하려면 **다음보다 오래 걸리는 압축파일은 검사 안 함** N초 확인란을 선택 취소합니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

이메일 메시지의 첨부파일 필터링

악성 코드는 이메일 첨부파일의 형태로 유포될 수 있습니다. 이메일 첨부파일의 형식을 기준으로 필터링하도록 구성하면 지정된 파일 유형이 자동으로 이름이 변경되거나 삭제됩니다. 어떤 유형의 첨부 파일의 이름을 바꿔, Kaspersky Endpoint Security가 악성 코드의 자동 실행으로부터 컴퓨터를 보호할 수 있습니다.

첨부파일 필터링을 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **메일 안티 바이러스**를 선택합니다.
   창 오른쪽에 메일 안티 바이러스 구성요소의 설정이 표시됩니다.

3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   메일 안티 바이러스 창이 열립니다.

4. **메일 안티 바이러스** 창에서 **첨부파일 필터** 탭을 선택합니다.

5. 다음 중 하나를 수행합니다:

   - 메일 안티 바이러스를 통해 메시지 첨부파일을 필터링하지 않으려면 **필터링 사용 안 함** 옵션을 선택합니다.
   - 메일 안티 바이러스를 통해 **특정한 이메일 첨부파일 형식**의 이름을 변경하려면 **지정한 첨부파일 유형 이름 바꾸기** 옵션을 선택합니다.

파일의 실제 형식이 파일 이름 확장자와 일치하지 않을 수 있습니다.

이메일 메시지에 첨부된 개체의 필터링을 설정한 경우 메일 안티 바이러스가 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

eml - Microsoft Outlook Express 메시지

nws - 새로운 Microsoft Outlook Express 이메일 메시지

msg - Microsoft Mail 이메일 메시지

plg - 이메일 메시지

mbx - 저장된 Microsoft Office Outlook 이메일의 확장자

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. 차세대 Microsoft Windows OS 메타파일. EMF 파일은 16비트 Microsoft Windows에서 지원되지 않음.

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

- 메일 안티 바이러스를 통해 특정한 이메일 첨부파일을 삭제하려면 **지정한 첨부파일 유형 삭제** 옵션을 선택합니다.

6. 이전 단계에서 **지정한 첨부파일 유형 이름바꾸기** 옵션 또는 **지정한 첨부파일 유형 삭제** 옵션을 선택한 경우 관련 파일 형식 옆의 확인란을 선택합니다.

   추가, **편집** 및 **제거** 버튼을 사용하여 파일 형식 목록을 변경할 수 있습니다.

7. **확인**을 누릅니다.

8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

Microsoft Office Outlook의 이메일 검사

Kaspersky Endpoint Security를 설치하는 동안 Microsoft Office Outlook(이하 Outlook)에 내장된 메일 안티 바이러스 확장 프로그램이 설치됩니다. 이 플러그인을 통해 Outlook에서 메일 안티 바이러스 설정을 열 수 있으며, 언제 이메일 메시지에 바이러스 및 기타 위협이 있는지 검사하는지도 지정할 수 있습니다. Outlook용 메일 안티 바이러스 확장 프로그램은 POP3, SMTP, NNTP, IMAP 및 MAPI 프로토콜을 통해 전송되는 모든 메시지를 검사할 수 있습니다.

만일 Kaspersky Endpoint Security 인터페이스에서 **추가: Microsoft Office Outlook 확장 프로그램** 확인란이 선택되었다면, 설정을 Outlook에서 직접 구성할 수 있습니다.

Outlook에서 받는 메시지는 먼저 메일 안티 바이러스(Kaspersky Endpoint Security 인터페이스에서 **POP3 / SMTP / NNTP / IMAP 트래픽** 확인란을 선택한 경우)에서 검사한 다음 Outlook에 통합된 메일 안티 바이러스 확장 프로그램에서 검사합니다. 메일 안티 바이러스가 메시지에서 악성 개체를 탐지할 경우 이를 사용자에게 알립니다.

알림 창에서의 처리 방법 선택은 메시지에서 위협을 제거하는 구성요소를 결정합니다: 메일 안티 바이러스 또는 Outlook용 메일 안티 바이러스 확장 프로그램.

- 알림 창에서 **치료** 또는 **제거**를 선택한 경우 메일 안티 바이러스가 보안위협을 제거합니다.
- 사용자 알림 창에서 **건너뛰기**를 선택한 경우, Outlook에 통합된 메일 안티 바이러스 확장 프로그램이 보안 위협을 제거합니다.

보내는 메시지는 먼저 Outlook에 통합된 메일 안티 바이러스 확장 프로그램에서 검사한 다음 메일 안티 바이러스에서 검사합니다.

Outlook의 메일 검사 구성

Outlook 2007에서 메일 검사를 구성하려면:

1. Outlook 2007의 메인 창을 엽니다.
2. 메뉴 표시줄에서 **서비스** → **설정** 옵션을 선택합니다.
   옵션 창이 열립니다.
3. **옵션** 창에서 **이메일 보호** 탭을 선택합니다.

Outlook 2010/2013에서 메일 검사를 구성하려면:

1. Outlook 메인 창을 엽니다.
   왼쪽 상단 모서리에서 **파일** 탭을 선택합니다.
2. **옵션** 버튼을 누릅니다.
   Outlook 옵션 창이 열립니다.
3. **추가 기능** 섹션을 선택합니다.
   아웃룩에 내장된 플러그인 설정은 창의 오른쪽 부분에 표시됩니다.
4. **추가 기능 옵션** 버튼을 누릅니다.

Kaspersky Security Center를 사용해 메일 검사 구성

Outlook용 메일 안티 바이러스 확장 프로그램을 사용하여 메일을 검사하는 경우 Exchange 캐싱 모드를 사용하는 것이 좋습니다. Exchange 캐싱 모드에 대한 자세한 내용 및 사용과 관련된 권장 사항은 Microsoft 기술 자료를 참조하십시오: https://technet.microsoft.com/en-us/library/cc179175.aspx.

Kaspersky Security Center를 사용해 Outlook용 메일 안티 바이러스 확장 프로그램의 작동 모드를 구성하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 메일 검사를 구성할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **안티 바이러스 보호** 섹션에서 **메일 안티 바이러스** 하위 섹션을 선택합니다.
7. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   메일 안티 바이러스 창이 열립니다.
8. **연결성** 섹션에서 **설정** 버튼을 누릅니다.
   이메일 보호 창이 열립니다.
9. **이메일 보호** 창에서 다음을 수행합니다:
   - Outlook용 메일 안티 바이러스 확장 프로그램이 받는 메일이 사서함에 도착할 때 메일을 검사하도록 설정하려면 **이메일을 받을 때 검사** 확인란을 선택합니다.
   - Outlook용 메일 안티 바이러스 확장 프로그램이 사용자가 받은 메일을 열 때 메일을 검사하도록 설정하려면 **이메일을 읽을 때 검사** 확인란을 선택합니다.
   - Outlook용 메일 안티 바이러스 확장 프로그램이 보내는 메일을 보낼 때 메일을 검사하도록 설정하려면 **이메일을 보낼 때 검사** 확인란을 선택합니다.
10. **이메일 보호** 창에서 **확인**을 누릅니다.
11. **메일 안티 바이러스** 창에서 **확인**을 누릅니다.
12. 정책이 적용됩니다.
    Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

인터넷에서 컴퓨터 보호. 웹 안티 바이러스

이 구성요소는 Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성요소는 Kaspersky Endpoint Security가 파일 서버용 Microsoft servers에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

이 섹션에는 웹 안티 바이러스에 대한 정보 및 구성요소 설정 구성 방법에 대한 지침이 나와 있습니다.

웹 안티 바이러스 정보

온라인에 접속할 때마다 컴퓨터에 저장된 정보가 바이러스 및 기타 악성 코드에 노출됩니다. 이러한 바이러스나 악성 코드는 범죄자에 의해 감염된 무료 소프트웨어를 다운로드하거나 웹 사이트를 검색할 때 컴퓨터에 침투할 수 있습니다. 네트워크 웜은 웹 페이지를 열거나 파일을 다운로드하기 전에도 인터넷에 연결하기만 하면 바로 컴퓨터에 유포될 수 있습니다.

웹 안티 바이러스는 HTTP 및 FTP 프로토콜을 통해 컴퓨터에서 보내고 받는 데이터를 감시하고 URL이 악성 웹 주소 또는 피싱 웹 주소 목록에 있는지 확인합니다.

웹 안티 바이러스는 HTTP 또는 FTP 프로토콜을 통해 사용자 또는 애플리케이션에서 접근하는 모든 웹 페이지나 파일을 가로채어 바이러스나 기타 보안위협이 있는지 분석합니다. 다음에는 아래의 일이 일어납니다:

- 페이지나 파일에 악성 코드가 없는 것으로 확인되면 사용자는 해당 페이지나 파일에 즉시 접근할 수 있게 됩니다.
- 사용자가 웹 페이지 또는 악성 코드를 포함하는 파일에 접근 할 경우, 애플리케이션은 웹 안티 바이러스 설정에 지정된 처리 방법을 수행합니다.

웹 안티 바이러스 작동 및 중지

기본적으로 웹 안티 바이러스는 작동되며 Kaspersky 전문가가 권장하는 모드에서 실행됩니다. 필요한 경우 웹 안티 바이러스를 중지할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

메인 애플리케이션 창의 보호 및 제어 탭에서 웹 안티 바이러스를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **보호** 섹션을 누릅니다.
   보호 섹션이 열립니다.
4. 이 섹션을 마우스 오른쪽 버튼으로 눌러 웹 안티 바이러스 구성요소에 대한 정보가 포함된 메뉴를 엽니다.

구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.

5. 다음 중 하나를 수행합니다:

   - 웹 안티 바이러스를 작동하려면 메뉴에서 **시작**을 선택합니다.
     웹 안티 바이러스 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.
   - 웹 안티 바이러스를 중지하려면 메뉴에서 **중지**를 선택합니다.
     웹 안티 바이러스 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 웹 안티 바이러스를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **웹 안티 바이러스**를 선택합니다.
   창 오른쪽에 웹 안티 바이러스 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:

   - 웹 안티 바이러스를 작동하려면 **웹 안티 바이러스 사용** 확인란을 선택합니다.
   - 웹 안티 바이러스를 중지하려면 **웹 안티 바이러스 사용** 확인란을 선택 해제합니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

웹 안티 바이러스 구성

웹 안티 바이러스를 구성하려면 다음과 같이 하십시오:

- 웹 트래픽 보안 레벨을 변경합니다.
  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.
- Kaspersky Endpoint Security가 악성 웹 트래픽 개체에 수행할 처리 방법을 변경합니다.
  HTTP 개체를 분석한 결과 악성 코드가 발견되면 지정된 처리 방법에 따라 웹 안티 바이러스가 대응합니다.
- 피싱/악성 웹 주소 데이터베이스에 대한 웹 안티 바이러스의 URL 검사 구성합니다.
- 웹 트래픽에 바이러스 또는 기타 악성 프로그램 검사를 수행할 때 휴리스틱 분석을 사용하도록 구성합니다.
  보호의 효율성을 높이려면 휴리스틱 분석을 사용합니다. 휴리스틱 분석 시 Kaspersky Endpoint Security는 운영 체제의 애플리케이션 활동을 분석합니다. 휴리스틱 분석을 사용하면 현재 Kaspersky Endpoint Security 데이터베이스에 기록이 없는 보안위협도 탐지할 수 있습니다.
- 웹페이지에 대해 피싱 링크 검사를 수행할 때 휴리스틱 분석을 사용하도록 구성합니다.
- HTTP 및 FTP 프로토콜을 통해 송수신되는 웹 트래픽에 대한 웹 안티 바이러스 검사를 최적화합니다.
- 신뢰하는 URL 목록을 생성합니다.

신뢰할 수 있는 컨텐츠가 포함된 URL의 목록을 작성할 수 있습니다. 웹 안티 바이러스가 신뢰하는 URL의 정보에 대해서는 바이러스 및 기타 보안위협 검사를 실시하지 않습니다. 예를 들어, 이 옵션은 공신력 있는 웹 사이트에서 파일을 다운로드할 때 웹 안티 바이러스가 개입하지 않도록 하는데 유용할 수 있습니다.

URL은 특정 웹페이지의 주소 또는 웹사이트의 주소일 수 있습니다.

웹 트래픽 보안 레벨 변경

HTTP 및 FTP 프로토콜을 통해 전송되는 데이터를 보호하기 위해 웹 안티 바이러스는 다양한 설정 그룹을 적용합니다. 이러한 설정 그룹을 *웹 트래픽 보안 레벨*이라고 합니다. 미리 정의된 웹 트래픽 보안 레벨이 있습니다: **높음**, **권장** 및 **낮음**. **권장** 웹 트래픽 보안 레벨은 최적의 설정으로 Kaspersky에서 권장하는 레벨입니다.

웹 트래픽 보안 레벨을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **웹 안티 바이러스**를 선택합니다.
   창 오른쪽에 웹 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 다음 중 하나를 수행합니다:
   - 기본 제공 웹 트래픽 보안 레벨 중 하나를 지정하려는 경우(**높음**, **권장** 또는 **낮음**) 슬라이더를 사용하여 선택합니다.
   - 사용자 지정 웹 트래픽 보안 레벨을 구성하려는 경우 **설정** 버튼을 눌러 **웹 안티 바이러스** 창에서 설정을 지정합니다.
     사용자 지정 웹 트래픽 보안 레벨을 구성하면 **보안 레벨** 섹션의 보안 레벨 이름이 **사용자 지정**으로 변경됩니다.
   - 웹 트래픽 보안 레벨을 **권장**으로 변경하려면 **기본값** 버튼을 누릅니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

웹 트래픽의 위험 개체에 수행할 처리 방법 변경

웹 트래픽의 위험 개체에 수행할 처리 방법을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **웹 안티 바이러스**를 선택합니다.
   창 오른쪽에 웹 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **위협 탐지 시 처리 방법** 섹션에서는 악성 웹 트래픽 개체가 탐지될 경우 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택할 수 있습니다:
   - **자동으로 처리 방법 선택**.
   - **다운로드 차단**.

- **다운로드 허락**.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

피싱/악성 웹 주소 데이터베이스에 대한 웹 안티 바이러스의 URL 검사

링크를 검사하여 해당 링크가 피싱 웹 주소 목록에 포함되어 있는지 확인하면 *피싱 공격*을 방지할 수 있습니다. 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 메시지로만 받는 게 아니라 ICQ 메시지와 같은 다른 출처에서도 받을 수 있으므로 웹 안티 바이러스는 웹 트래픽 수준에서 피싱 웹 사이트에 대한 접근 시도를 감시하고 해당 사이트에 대한 접근을 차단합니다. 피싱 URL 목록은 Kaspersky Endpoint Security 배포 키트에 포함되어 있습니다.

악성 및 피싱 웹 주소 데이터베이스와 비교하여 URL을 검사하도록 웹 안티 바이러스를 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **웹 안티 바이러스**를 선택합니다.
   창 오른쪽에 웹 안티 바이러스 구성요소의 설정이 표시됩니다.

3. **설정** 버튼을 누릅니다.
   웹 안티 바이러스 창이 열립니다.

4. **웹 안티 바이러스** 창에서 **일반** 탭을 선택합니다.

5. 다음을 수행합니다:

   - 웹 안티 바이러스가 악성 웹 주소 데이터베이스와 비교하여 URL을 확인하도록 설정하려면, **검사 방법** 섹션에서 **링크가 악성 링크 데이터베이스에 있는지 확인** 확인란을 선택합니다.

   - 웹 안티 바이러스가 피싱 주소 데이터베이스와 비교하여 URL을 확인하도록 설정하려면, **안티 피싱 설정** 섹션에서 **링크가 피싱 링크 데이터베이스에 있는지 확인** 확인란을 선택합니다.

   Kaspersky Security Network의 평판 데이터베이스를 대상으로 링크를 확인할 수도 있습니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

웹 안티 바이러스에 휴리스틱 분석기 사용

웹 안티 바이러스에 휴리스틱 분석을 사용하도록 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **웹 안티 바이러스**를 선택합니다.
   창 오른쪽에 웹 안티 바이러스 구성요소의 설정이 표시됩니다.

3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   웹 안티 바이러스 창이 열립니다.

4. **일반** 탭을 선택합니다.

5. 웹 안티 바이러스가 **바이러스 탐지 휴리스틱 분석**하여 웹 트래픽에 대해 바이러스 및 기타 악성 코드 검사를 수행하도록 설정하려면 **검사 방법** 섹션에서 바이러스 탐지를 위한 휴리스틱 분석 확인란을 선택하고, 슬라이더를 사용하여 휴리스틱 분석 시 적용될 검사 레벨을 설정합니다: **기본**, **자세히** 및 **매우 자세히**.

6. 웹 안티 바이러스가 휴리스틱 분석을 사용하여 웹 페이지에 대해 피싱 링크 검사를 수행하도록 설정하려면, **안티 피싱 설정**에서 **피싱 링크 탐지에 휴리스틱 분석 사용** 확인란을 선택합니다.

7. **확인**을 누릅니다.

8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

신뢰하는 URL 목록 편집

신뢰하는 주소 목록을 만들려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **웹 안티 바이러스**를 선택합니다.
   창 오른쪽에 웹 안티 바이러스 구성요소의 설정이 표시됩니다.

3. **설정** 버튼을 누릅니다.
   웹 안티 바이러스 창이 열립니다.

4. **신뢰하는 URL** 탭을 선택합니다.

5. **신뢰하는 웹 주소의 웹 트래픽은 검사 안 함** 확인란을 선택합니다.

6. 신뢰하는 컨텐츠가 있는 URL 및 웹페이지 목록을 만듭니다. 목록을 만들려면 다음을 수행합니다:

   a. **추가** 버튼을 누릅니다.
      웹 주소 / 웹 주소 마스크 창이 열립니다.

   b. 웹사이트 및 웹페이지의 주소 또는 주소 마스크를 입력합니다.

   c. **확인**을 누릅니다.
      새 레코드가 신뢰하는 URL 목록에 표시됩니다.

7. **확인**을 누릅니다.

8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

IM 클라이언트의 트래픽 보호. 메신저 안티 바이러스

이 구성요소는 Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성요소는 Kaspersky Endpoint Security가 파일 서버용 Microsoft servers에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

이 섹션에는 메신저 안티 바이러스에 대한 정보 및 구성요소 설정 구성 방법에 대한 지침이 나와 있습니다.

메신저 안티 바이러스 정보

IM 안티 바이러스는 인스턴트 메시징 클라이언트(*IM 클라이언트*)의 트래픽을 검사합니다.

메신저 안티 바이러스는 암호화된 채널을 통해 전송되는 메시지를 검사하지 않습니다.

메신저 클라이언트를 통해 전송되는 메시지는 다음과 같은 보안위협을 포함하고 있을 수 있습니다:

- 컴퓨터에 악성 코드를 다운로드하려는 URL
- 침입자가 피싱 공격에 사용하는 악성 코드 및 웹사이트로 연결되는 URL

  은행 카드 번호, 여권 정보, 은행 계좌 시스템의 암호 및 기타 온라인 서비스(예: 소셜 네트워크 사이트 또는 이메일 계정)와 같은 개인 정보를 훔치려는 목적의 피싱 공격.

파일은 메신저 클라이언트를 통해 전송됩니다. 이러한 파일을 저장할 때는 파일 안티 바이러스 구성요소에서 파일을 검사합니다.

메신저 안티 바이러스는 사용자가 메신저 클라이언트를 통해 보내거나 받는 모든 메시지를 먼저 가져온 다음 컴퓨터 보안을 위협할 수 있는 링크가 있는지 검사합니다:

- 메시지에서 위험한 URL이 탐지되지 않으면 사용자에게 메시지가 표시됩니다.
- IM에서 위험한 링크가 탐지된 경우 메신저 안티 바이러스는 실행 중인 IM 창에 보안위협에 대한 정보가 표시되는 메시지로 대체합니다.

메신저 안티 바이러스 작동 및 중지

기본적으로 메신저 안티 바이러스는 작동되며 Kaspersky 전문가가 권장하는 모드에서 실행됩니다. 필요한 경우 메신저 안티 바이러스를 중지할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

메인 애플리케이션 창의 보호 및 제어 탭에서 메신저 안티 바이러스를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **보호** 섹션을 누릅니다.
   보호 섹션이 열립니다.
4. **메신저 안티 바이러스** 행을 마우스 오른쪽 버튼으로 눌러 구성요소 동작의 메뉴를 표시합니다.
5. 다음 중 하나를 수행합니다:
   - 메신저 안티 바이러스를 작동하려면 마우스 오른쪽 메뉴에서 **시작**을 선택합니다.
     메신저 안티 바이러스 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.
   - 메신저 안티 바이러스를 중지하려면 메뉴에서 **중지**를 선택합니다.
     메신저 안티 바이러스 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 메신저 안티 바이러스를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **메신저 안티 바이러스** 서브섹션을 선택합니다.
   창 오른쪽에 메신저 안티 바이러스 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 메신저 안티 바이러스를 작동하려면 **메신저 안티 바이러스 사용** 확인란을 선택합니다.
   - 메신저 안티 바이러스를 중지하려면 **메신저 안티 바이러스 사용** 확인란을 선택 해제합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

메신저 안티 바이러스 구성

다음과 같은 방법으로 메신저 안티 바이러스를 구성할 수 있습니다:

- 보호 영역을 구성합니다.
  메신저 클라이언트 메시지의 검사 대상 유형을 수정하여 보호 영역을 확장하거나 좁힐 수 있습니다.
- 메신저 안티 바이러스를 이용하여 메신저 클라이언트 메시지의 웹 주소가 악성 및 피싱 링크 데이터베이스에 있는지 검사하는 작업을 구성합니다.

메신저 안티 바이러스의 보호 영역 생성

보호가 작동되는 경우 구성요소가 검사하는 개체를 보호 범위이라고 합니다. 각 구성 요소의 보호 범위는 서로 다른 속성을 가집니다. 메신저 안티 바이러스 보호 영역의 속성에서는 메신저 클라이언트에서 보내거나 받는 메시지 중 검사할 메시지 유형을 설정할 수 있습니다. 기본적으로 보내고 받는 모든 메시지를 모두 검사하도록 설정되어 있습니다. 보내는 트래픽의 검사는 중지할 수 있습니다.

보호 범위를 만들려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **메신저 안티 바이러스** 서브섹션을 선택합니다.
   창 오른쪽에 메신저 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **보호 범위** 섹션에서 다음 중 하나를 수행합니다:
   - 메신저 안티 바이러스가 IM 클라이언트에서 주고 받는 모든 메시지를 검사하도록 하려면 **보내거나 받는 모든 메시지** 옵션을 선택합니다.
   - 메신저 안티 바이러스가 IM 클라이언트에서 받는 메시지만 검사하도록 하려면 **받는 메시지** 옵션을 선택합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

메신저 안티 바이러스에서 악성 및 피싱 URL 데이터베이스와 비교하여 URL 검사

악성 및 피싱 웹 주소의 데이터베이스와 비교하여 URL 을 검사하도록 메신저 안티 바이러스를 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **메신저 안티 바이러스** 서브섹션을 선택합니다.
   창 오른쪽에 메신저 안티 바이러스 구성요소의 설정이 표시됩니다.
3. **검사 방법** 섹션에서 메신저 안티 바이러스가 사용할 방법을 선택합니다:
   - 악성 웹 데이터베이스와 비교하여 메신저 클라이언트 메시지 내의 링크를 검사하도록 설정하려면 **링크가 악성 링크 데이터베이스에 있는지 확인** 확인란을 선택합니다.
   - 피싱 웹 주소 데이터베이스와 비교하여 메신저 클라이언트 메시지 내의 링크를 검사하도록 설정하려면 **링크가 피싱 링크 데이터베이스에 있는지 확인** 확인란을 선택합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

시스템 감시기

이 구성요소는 Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성요소는 Kaspersky Endpoint Security가 파일 서버용 Microsoft servers에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

이 섹션에는 시스템 감시기에 대한 정보와 해당 구성요소 설정을 구성하는 방법에 대한 지침이 나와 있습니다.

시스템 감시기 정보

시스템 감시기는 컴퓨터에 설치된 애플리케이션의 동작에 대한 데이터를 수집한 후 컴퓨터를 보다 안정적으로 보호하기 위해 다른 구성요소에 이 정보를 전달합니다.

행동 스트림 시그니처

"동작 스트림 시그니처(BSS)"에는 Kaspersky Endpoint Security가 위험한 것으로 분류한 애플리케이션 동작 시퀀스가 포함되어 있습니다. 애플리케이션 활동이 행동 스트림 시그니처와 일치할 경우 Kaspersky Endpoint Security는 지정된 처리 방법을 수행합니다. 행동 스트림 시그니처를 바탕으로 한 Kaspersky Endpoint Security 기능은 컴퓨터에 대한 사전 방역을 제공합니다.

애플리케이션 동작이 동작 스트림 시그니처와 일치할 경우 시스템 감시기는 기본적으로 애플리케이션의 실행 파일을 격리 저장소로 이동합니다.

악성프로그램이 수행한 동작 롤백

시스템 감시기에서 수집한 정보를 바탕으로 Kaspersky Endpoint Security는 치료 방법을 수행하는 동시에 **운영 체제에서 수행된 악성 코드 활동을 롤백**합니다.

운영 체제에서 악성 프로그램이 수행한 동작을 롤백할 때 Kaspersky Endpoint Security는 다음과 같은 악성 프로그램 활동의 유형에 따라 처리 방법을 수행합니다:

- 파일 활동.

  Kaspersky Endpoint Security는 네트워크 장치를 예외한 모든 장치에서 악성 프로그램에 의해 생성된 실행 파일을 찾아 삭제합니다.

  Kaspersky Endpoint Security는 악성 프로그램에 감염된 프로그램에 의해 생성된 실행 파일을 삭제합니다.

  Kaspersky Endpoint Security는 변경 또는 삭제된 파일을 복원하지 않습니다.

- 레지스트리 활동.

  Kaspersky Endpoint Security는 악성 프로그램에 의해 생성된 파티션과 레지스트리 키를 삭제합니다.

  Kaspersky Endpoint Security는 수정 또는 삭제된 파티션과 레지스트리 키를 복원하지 않습니다.

- 시스템 활동.

  Kaspersky Endpoint Security는 악성 프로그램에 의해 시작된 프로세스를 종료합니다.

  Kaspersky Endpoint Security는 악성 프로그램이 침투한 프로세스를 종료합니다.

  Kaspersky Endpoint Security는 악성 프로그램에 의해 종료된 프로세스를 다시 시작하지 않습니다.

- 네트워크 동작.

  Kaspersky Endpoint Security는 악성 프로그램의 네트워크 활동을 차단합니다.

  Kaspersky Endpoint Security는 악성 프로그램이 침투한 프로세스의 네트워크 활동을 차단합니다.

악성 코드 활동의 롤백은 파일 안티 바이러스 및 바이러스 검사에 의해 시작됩니다.

악성 코드 활동을 롤백하면 엄격하게 정의된 데이터 집합에는 영향을 줍니다. 롤백은 운영 체제 또는 컴퓨터 데이터의 무결성에는 악영향이 없습니다.

시스템 감시기 작동 및 중지

기본적으로 시스템 감시기는 작동되며, Kaspersky가 권장하는 모드에서 실행됩니다. 필요할 경우 시스템 감시기를 중지할 수 있습니다.

시스템 감시기는 보호 구성요소의 성능에 영향을 미치기 때문에 절대적으로 필요한 경우가 아니면 이 기능의 중지는 권장하지 않습니다. 보호 구성요소는 보다 정확하게 탐지된 위협을 식별하기 위해 시스템 감시기에 의해 수집된 데이터를 요구할 수 있습니다.

시스템 감시기를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

*메인 애플리케이션 창의 **보호 및 제어** 탭에서 시스템 감시기를 작동 또는 중지하려면 다음과 같이 하십시오:*

1. 메인 애플리케이션 창을 엽니다.

2. **보호 및 제어** 탭을 선택합니다.

3. **보호** 섹션을 누릅니다.
   보호 섹션이 열립니다.

4. 마우스 오른쪽 버튼을 눌러 시스템 감시기 구성요소 정보가 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
   구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.

5. 다음 중 하나를 수행합니다:

   - 시스템 감시기를 작동하려면 **시작**을 선택합니다.
     시스템 감시기 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

   - 시스템 감시기를 중지하려면 **중지**를 선택합니다.
     시스템 감시기 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 시스템 감시기를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **시스템 감시기** 하위 섹션을 선택합니다.
   창 오른쪽에 **시스템 감시기** 구성요소의 설정이 표시됩니다.

3. 다음 중 하나를 수행합니다:

   - 시스템 감시기를 작동하려면 **시스템 감시기 작동** 확인란을 선택합니다

   - 시스템 감시기를 중지하려면 **시스템 감시기 작동** 확인란을 선택 취소합니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

시스템 감시기 구성

시스템 감시기를 구성하는 다음 동작을 수행할 수 있습니다:

- 익스플로잇 보호 작동 또는 중지;

- 프로그램에서 악성 활동이 탐지되는 경우에 수행해야 하는 조치 선택;

- 치료 중 악성 코드의 동작 롤백 작동 또는 중지.

익스플로잇 보호 작동 또는 중지

익스플로잇 보호 기능을 작동하거나 중지하려면:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **시스템 감시기** 하위 섹션을 선택합니다.
   창 오른쪽에 **시스템 감시기** 구성요소의 설정이 표시됩니다.

3. 다음 중 하나를 수행합니다:

   - Kaspersky Endpoint Security가 취약한 프로그램이 시작될 때 사용되는 파일을 감시하려면, **익스플로잇 차단 기능 사용** 확인란을 선택합니다.

     만일 Kaspersky Endpoint Security가 취약한 프로그램에서 사용 중인 파일이 해당 사용자가 아닌 다른 사용자가 실행한 것을 탐지하면, **보안위협 탐지 시 처리 방법** 팝업 목록에서 사용자 선택한 결과에 따라 처리됩니다.

   - Kaspersky Endpoint Security가 취약한 프로그램이 시작될 때 사용되는 파일을 감시하려면, **익스플로잇 차단 기능 사용** 확인란을 선택합니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

프로그램에서 악성 활동이 탐지되는 경우에 수행해야 하는 조치 선택

프로그램에 악성 활동이 포함되어 있는 경우 어떻게 할지 선택하려면 다음 조치를 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **시스템 감시기** 하위 섹션을 선택합니다.
   창 오른쪽에 **시스템 감시기** 구성요소의 설정이 표시됩니다.
3. **악성 코드 활동 탐지 시** 팝업 목록의 **보안위협 탐지 시 처리 방법** 섹션에서 다음 처리 방법을 선택합니다:
   - **자동으로 처리 방법 선택**.
   - **격리 저장소로 파일 이동**.
   - **악성 코드 강제 종료**.
   - **건너뛰기**.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

치료 중 악성 코드의 동작 롤백 작동 또는 중지

처리 중 악성 코드의 활동 내역 롤백을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **시스템 감시기** 하위 섹션을 선택합니다.
   창 오른쪽에 **시스템 감시기** 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - **처리(치료) 중 악성 코드가 기록한 활동 롤백**하려면 치료 중 악성 코드 동작 롤백 확인란을 선택합니다.
   - **처리(치료) 중 악성 코드가 기록한 활동 롤백**을 무시하려면 치료 중 악성 코드 동작 롤백 확인란을 선택하지 않습니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

방화벽

이 섹션에는 방화벽에 대한 정보와 해당 구성요소 설정을 구성하는 방법에 대한 지침이 나와 있습니다.

방화벽 정보

LAN 및 인터넷을 사용하는 동안 컴퓨터는 운영 체제와 소프트웨어의 취약점을 노린 바이러스 등의 악성 프로그램과 다양한 공격에 노출됩니다.

방화벽은 컴퓨터가 인터넷이나 LAN에 연결되었을 때 운영 체제에 가해지는 모든 가능한 유형의 위협을 차단하여 사용자의 컴퓨터에 저장된 개인 데이터를 보호하는 역할을 합니다. 방화벽은 사용자 컴퓨터의 모든 네트워크 연결을 탐지하여 IP 주소 목록을 제공하고 기본 네트워크 연결의 상태를 표시합니다.

방화벽 구성요소는 네트워크 규칙에 따라 모든 네트워크 활동을 필터링합니다. 네트워크 규칙을 구성하면 모든 애플리케이션의 인터넷 접근을 차단하거나 무제한 접근을 허용하는 등 컴퓨터의 보호 수준을 원하는 대로 지정할 수 있습니다.

방화벽 작동 또는 중지

기본적으로 방화벽은 작동되며 최적 모드가 사용됩니다. 필요한 경우 방화벽을 중지할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

메인 애플리케이션 창의 보호 및 제어 탭에서 방화벽을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **보호** 섹션을 누릅니다.
   보호 섹션이 열립니다.
4. **방화벽** 줄을 마우스 오른쪽 버튼으로 눌러 방화벽 처리의 마우스 오른쪽 메뉴를 엽니다.
5. 다음 중 하나를 수행합니다:
   - 방화벽을 작동하려면 마우스 오른쪽 메뉴에서 **시작**을 선택합니다.
     방화벽 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.
   - 방화벽을 중지하려면 마우스 오른쪽 메뉴에서 **중지**를 선택합니다.
     방화벽 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 방화벽을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽**을 선택합니다.
   창 오른쪽에 방화벽 구성요소의 설정이 표시됩니다.

3. 다음 중 하나를 수행합니다:

   - 방화벽을 작동하려면 **방화벽 사용** 확인란을 선택합니다.
   - 방화벽을 중지하려면 **방화벽 중지** 확인란을 선택합니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

네트워크 규칙 정보

*네트워크 규칙*은 네트워크 연결 시도가 탐지될 때 방화벽에서 수행하는 허용 또는 차단 동작입니다.

방화벽은 서로 다른 2가지 레벨의 네트워크 공격에 대응해 보호를 제공합니다: 네트워크 레벨 및 프로그램 레벨. 네트워크 레벨의 보호는 네트워크 패킷 규칙을 적용하여 이루어집니다. 프로그램 레벨의 보호는 설치된 애플리케이션이 네트워크 리소스에 접근할 수 있도록 하는 규칙을 적용하여 이루어집니다.

방화벽 보호의 두 가지 레벨을 기준으로 다음과 같은 규칙을 만들 수 있습니다:

- *네트워크 패킷 규칙*. 네트워크 패킷 규칙은 프로그램에 관계없이 네트워크 패킷을 제한합니다. 이러한 규칙은 선택한 데이터 프로토콜의 특정 포트를 통과하는 인바운드 및 아웃바운드 트래픽을 제한합니다. 방화벽은 기본적으로 특정 네트워크 패킷 규칙을 지정합니다.

- *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. 예를 들어 특정 형태의 네트워크 연결이 일부 애플리케이션에는 금지되고 다른 애플리케이션에는 허용되는 경우 이러한 규칙을 사용하여 네트워크 활동 필터링을 세부적으로 조정할 수 있습니다.

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.

각 네트워크 패킷 규칙과 애플리케이션 네트워크 규칙의 실행 우선 순위를 지정할 수 있습니다.

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.

애플리케이션의 네트워크 규칙은 다음과 같이 작동합니다: 애플리케이션의 네트워크 규칙에는 네트워크 상태(*공용*, *로컬* 또는 *신뢰하는* 네트워크)에 기반한 접근 규칙이 포함됩니다. 예를 들어 높은 제한 신뢰 그룹에 속한 애플리케이션에는 기본적으로 모든 상태의 네트워크에서 어떠한 네트워크 활동도 허용되지 않습니다. 네트워크 규칙이 개별 애플리케이션(부모 애플리케이션)에 대해 지정되어 있으면, 다른 애플리케이션의 자식 프로세스가 부모 애플리케이션의 네트워크 규칙에 따라 실행됩니다. 애플리케이션에 대한 네트워크 규칙이 없으면, 자식 프로세스가 애플리케이션 신뢰 그룹의 네트워크 접근 규칙에 따라 실행됩니다.

예를 들어 브라우저 X를 제외한 모든 애플리케이션에 대해 모든 상태의 네트워크에서 네트워크 활동을 금지한 경우, 브라우저 X(부모 애플리케이션)에서 브라우저 Y 설치(자식 프로세스)를 시작하면 브라우저 Y 설치 프로그램에서 네트워크에 접근하고 필요한 파일을 다운로드합니다. 설치 후에는 방화벽 설정에 따라 브라우저 Y의 네트워크 연결이 거부됩니다. 자식 프로세스인 브라우저 Y 설치 프로그램의 네트워크 활동을 금지하려면 브라우저 Y 설치 프로그램에 대한 네트워크 규칙을 추가해야 합니다.

네트워크 연결 상태 정보

방화벽은 사용자의 컴퓨터에서 모든 네트워크 연결을 제어하고 탐지된 각 네트워크 연결에 자동으로 상태를 할당합니다.

네트워크 연결에는 다음 중 한 가지 상태가 할당됩니다:

- **공용 네트워크**. 이 상태는 안티 바이러스 애플리케이션, 방화벽 또는 필터로 보호되지 않는 네트워크(예: 인터넷 카페 네트워크)에 사용됩니다. 방화벽은 이러한 네트워크에 연결된 컴퓨터의 사용자가 이 컴퓨터의 파일 및 프린터에 접근하지 못하게 차단합니다. 외부 사용자도 이 컴퓨터의 데스크톱에 원격 액세스하여 공유 폴더의 데이터에 접근할 수 없습니다. 방화벽은 각 애플리케이션에 설정된 네트워크 규칙에 따라 이러한 애플리케이션의 네트워크 활동을 필터링합니다.

  방화벽은 기본적으로 인터넷에 *공용 네트워크* 상태를 할당합니다. 인터넷의 상태는 변경할 수 없습니다.

- **로컬 네트워크**. 이 상태는 사용자가 컴퓨터의 파일 및 프린터에 접근하도록 허용된 네트워크에 할당됩니다(예: LAN 또는 홈 네트워크).

- **신뢰하는 네트워크**. 이 상태는 컴퓨터가 공격이나 무단 데이터 접근에 노출되지 않아 안전한 네트워크에 지정됩니다. 이 상태의 네트워크에서는 모든 네트워크 활동이 허용됩니다.

네트워크 연결 상태 변경

네트워크 연결 상태를 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽** 하위 섹션을 선택합니다.
   창 오른쪽에 방화벽 구성요소의 설정이 표시됩니다.
3. **사용 가능한 네트워크** 버튼을 누릅니다.
   방화벽 창이 열립니다.
4. 상태를 변경하고 싶은 네트워크 연결을 선택합니다.
5. 마우스 오른쪽 메뉴에서 네트워크 연결 상태를 선택합니다:
   - **공용 네트워크**.
   - **로컬 네트워크**.
   - **신뢰하는 네트워크**.
6. **방화벽** 창에서 **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

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 사용자지정 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 만들기 및 편집

> 네트워크 패킷 규칙을 생성할 때 네트워크 패킷 규칙이 애플리케이션 네트워크 규칙보다 우선 순위가 높다는 점을 기억하십시오.

네트워크 패킷 규칙을 만들거나 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽**을 선택합니다.
3. **네트워크 패킷 규칙** 버튼을 누릅니다.
4. **방화벽** 창에서 **네트워크 패킷 규칙** 탭이 열립니다.

   이 탭에는 방화벽에서 설정한 기본 네트워크 패킷 규칙의 목록이 표시됩니다.
5. 다음 중 하나를 수행합니다:

   - 네트워크 패킷 규칙을 만들려면 **추가** 버튼을 누릅니다.

- 네트워크 패킷 규칙을 편집하려면 네트워크 패킷 규칙 목록에서 해당 규칙을 선택하고 **편집** 버튼을 누릅니다.

네트워크 규칙 창이 열립니다.

6. **처리** 드롭다운 목록에서, 이러한 종류의 네트워크 활동을 감지할 경우 방화벽에서 수행할 처리 방법을 선택합니다:
   - **허용**
   - **차단**
   - **애플리케이션 규칙에 따라 처리**.
7. **이름** 필드에서 다음 방법 중 하나로 네트워크 서비스의 이름을 지정합니다:
   - 이름 필드의 오른쪽에 있는 아이콘을 누르고 드롭-다운 목록에서 네트워크 서비스 **이름**을 선택하십시오.
     드롭다운 목록에는 자주 사용하는 네트워크 연결을 정의하는 네트워크 서비스가 포함됩니다.
   - **이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.
8. 다음 방법으로 데이터 전송 프로토콜을 지정합니다:
   a. **프로토콜** 확인란을 선택합니다.
   b. 드롭다운 목록에서 네트워크 활동을 감시할 프로토콜 유형을 선택합니다.
      방화벽이 TCP, UDP, ICMP, ICMPv6, IGMP 및 GRE 프로토콜을 사용하는 네트워크 연결을 감시합니다.
      이름 드롭다운 목록에서 네트워크 서비스를 선택하면 **프로토콜** 확인란이 자동으로 선택되고 확인란 옆의 드롭다운 목록이 선택한 네트워크 서비스에 해당하는 프로토콜 유형으로 채워집니다. 기본적으로 **프로토콜** 확인란은 선택되어 있지 않습니다.
9. **방향** 드롭다운 목록에서 감시하는 네트워크 활동의 방향을 선택합니다.
   방화벽이 다음과 같은 네트워크 방향의 연결을 감시합니다:
   - **인바운드(패킷)**.
   - **인바운드**.
   - **인바운드/아웃바운드**
   - **아웃바운드(패킷)**.
   - **아웃바운드**.
10. ICMP 또는 ICMPv6를 프로토콜로 선택한 경우 ICMP 패킷 유형과 코드를 지정할 수 있습니다:
    a. **ICMP 유형** 확인란을 선택하고 드롭다운 목록에서 ICMP 패킷 유형을 선택합니다.
    b. **ICMP 코드** 확인란을 선택하고 드롭다운 목록에서 ICMP 패킷 코드를 선택합니다.
11. TCP 또는 UDP를 프로토콜 유형으로 선택한 경우 연결을 모니터링할 로컬 및 원격 컴퓨터의 포트 번호를 쉼표로 구분하여 지정할 수 있습니다:
    a. **원격 포트** 필드에 원격 컴퓨터의 포트를 입력합니다.

b. **로컬 포트** 필드에 로컬 컴퓨터의 포트를 입력합니다.

12. **네트워크 어댑터** 표에서 네트워크 패킷을 보내거나 또는 받을 수 있는 네트워크 어댑터에 대한 설정을 지정합니다. 이를 위해서는 **추가**, **편집**, **삭제** 버튼을 사용합니다.

13. 네트워크 패킷의 유지 시간(TTL)을 기준으로 패킷 제어를 제한하려면 **TTL** 확인란을 선택하고 그 옆 필드에서 인바운드 및/또는 아웃바운드 네트워크 패킷의 유지 시간 값 범위를 지정합니다.

    네트워크 규칙은 네트워크 패킷의 유지 시간이 지정한 값을 초과하지 않는 패킷의 전송을 제어합니다.

    그렇게 하지 않으려면 **TTL** 확인란을 선택 취소합니다.

14. 네트워크 패킷을 주고 받는 원격 컴퓨터의 네트워크 주소를 지정합니다. **원격 주소** 드롭다운 목록에서 다음 값 중 하나를 선택하십시오:

    - **모든 주소**. 네트워크 규칙은 모든 IP 주소를 가지고 있는 원격 컴퓨터에서 송수신되는 네트워크 패킷을 제어합니다.
    - **서브넷 주소**. 네트워크 규칙은 선택된 네트워크 유형과 관련된 IP 주소를 가진 원격 컴퓨터에서의 송수신 네트워크 패킷을 제어합니다: **신뢰하는 네트워크**, **로컬 네트워크** 또는 **공용 네트워크**.
    - **주소 목록**. 네트워크 규칙은 아래 목록에서 **추가**, **편집** 및 **삭제** 버튼을 이용해 지정할 수 있는 IP 주소를 가진 원격 컴퓨터에서의 송수신 네트워크 패킷을 제어합니다.

15. Kaspersky Endpoint Security가 설치된 컴퓨터의 네트워크 주소를 지정해 네트워크 패킷을 송수신할 수 있습니다. **로컬 주소** 드롭다운 목록에서 다음 값 중 하나를 선택하십시오:

    - **모든 주소**. 네트워크 규칙은 Kaspersky Endpoint Security가 설치된 컴퓨터 및 모든 IP 주소를 가진 컴퓨터와의 네트워크 패킷 송수신을 제어합니다.
    - **주소 목록**. 네트워크 규칙은 아래 목록에서 **추가**, **편집** 및 **삭제** 버튼을 이용해 지정할 수 있는 IP 주소를 가진 Kaspersky Endpoint Security가 설치된 컴퓨터 및 모든 IP 주소를 가진 컴퓨터에서의 송수신 네트워크 패킷을 제어합니다.

    네트워크 패킷을 사용하는 애플리케이션에 대해 로컬 주소를 얻지 못할 수 있습니다. 이 경우 **로컬 주소** 설정 값이 무시됩니다.

16. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 로그** 확인란을 선택합니다.

17. **네트워크 규칙** 창에서 **확인**을 누릅니다.

    새 네트워크 규칙을 만들면 해당 규칙이 **방화벽** 창의 **네트워크 패킷 규칙** 탭에 표시됩니다. 기본적으로 새 네트워크 규칙은 네트워크 패킷 규칙 목록의 끝에 추가됩니다.

18. **방화벽** 창에서 **확인**을 누릅니다.

19. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

네트워크 패킷 규칙 작동 또는 중지

네트워크 패킷 규칙을 작동하거나 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽** 하위 섹션을 선택합니다.
   창 오른쪽에 방화벽 구성요소의 설정이 표시됩니다.
3. **네트워크 패킷 규칙** 버튼을 누릅니다.
   방화벽 창에서 **네트워크 패킷 규칙** 탭이 열립니다.
4. 목록에서 원하는 네트워크 패킷 규칙을 선택합니다.
5. 다음 중 하나를 수행합니다:
   - 규칙을 작동하려면 네트워크 패킷 규칙 이름 옆의 확인란을 선택합니다.
   - 규칙을 중지하려면 네트워크 패킷 규칙 이름 옆의 확인란을 선택 취소합니다.
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

네트워크 패킷 규칙에 대한 방화벽 동작 변경

네트워크 패킷 규칙에 적용되는 방화벽 동작을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽** 하위 섹션을 선택합니다.
   창 오른쪽에 방화벽 구성요소의 설정이 표시됩니다.
3. **네트워크 패킷 규칙** 버튼을 누릅니다.
   방화벽 창에서 **네트워크 패킷 규칙** 탭이 열립니다.
4. 목록에서 동작을 변경할 네트워크 패킷 규칙을 선택합니다.
5. **권한** 열에서 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 열고 할당할 동작을 선택합니다:
   - **허용**
   - **차단**
   - **애플리케이션 제어 규칙에 따라**
   - **이벤트 로그**
6. **방화벽** 창에서 **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

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.

수동으로 만든 각 네트워크 패킷 규칙은 목록의 끝에 추가되며 가장 낮은 우선 순위가 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. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽** 하위 섹션을 선택합니다.
   창 오른쪽에 방화벽 구성요소의 설정이 표시됩니다.
3. **네트워크 패킷 규칙** 버튼을 누릅니다.
   방화벽 창에서 **네트워크 패킷 규칙** 탭이 열립니다.
4. 목록에서 우선 순위를 변경할 네트워크 패킷 규칙을 선택합니다.
5. **위로 이동** 및 **아래로 이동** 버튼을 사용하여 네트워크 패킷 규칙을 목록에서 원하는 위치로 이동합니다.
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

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.

기본적으로 방화벽 구성요소는 애플리케이션 권한 제어 구성요소와 마찬가지로 그룹 내에 있는 모든 애플리케이션의 네트워크 활동을 필터링할 때 애플리케이션 그룹에 대한 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.

애플리케이션의 네트워크 규칙을 관리할 때 다음 작업도 수행할 수 있습니다:

- 새 네트워크 규칙을 만듭니다.
  방화벽이 선택한 애플리케이션 그룹에 속한 애플리케이션 또는 여러 애플리케이션의 네트워크 활동을 제어할 때 사용하는 새로운 네트워크 규칙을 만들 수 있습니다.

- 네트워크 규칙을 작동하거나 중지합니다.

  모든 네트워크 규칙은 *사용* 상태로 애플리케이션 네트워크 규칙 목록에 추가됩니다. 네트워크 규칙이 작동하면 방화벽이 이 규칙을 적용합니다.

  직접 만든 네트워크 규칙을 중지할 수 있습니다. 네트워크 규칙이 중지되면 방화벽은 일시적으로 이 규칙을 적용하지 않습니다.

- 네트워크 규칙 설정 변경.

  새 네트워크 규칙을 만든 후에는 항상 설정으로 돌아가 필요에 따라 설정을 수정할 수 있습니다.

- 네트워크 규칙에 대한 방화벽 동작 변경.

  이 애플리케이션 또는 애플리케이션 그룹에서 네트워크 활동을 탐지할 경우 방화벽이 해당 네트워크 규칙에 대해 적용할 동작을 네트워크 규칙 목록에서 편집할 수 있습니다.

- 네트워크 규칙 우선 순위 변경.

  사용자지정 네트워크 규칙의 우선 순위를 높이거나 낮출 수 있습니다.

- 네트워크 규칙 삭제.

  사용자 지정 네트워크 규칙을 삭제하여 네트워크 활동이 탐지되었을 때 방화벽이 이 네트워크 규칙을 선택한 애플리케이션 또는 애플리케이션 그룹에 적용하지 않도록 하고 애플리케이션 네트워크 규칙 목록에 이 규칙이 표시되지 않게 할 수 있습니다.

애플리케이션 네트워크 규칙 만들기 및 편집

애플리케이션 그룹에 대한 네트워크 규칙을 만들거나 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽** 하위 섹션을 선택합니다.
3. **애플리케이션 네트워크 규칙** 버튼을 누릅니다.

   방화벽 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.
4. 애플리케이션 목록에서 네트워크 규칙을 만들거나 편집할 애플리케이션 또는 애플리케이션 그룹을 선택합니다.
5. 마우스 오른쪽 버튼을 눌러 메뉴를 열고 수행해야 하는 작업에 따라 **애플리케이션 규칙** 또는 **그룹 규칙**을 선택합니다.

   이것을 누르면 **애플리케이션 제어 규칙** 또는 **애플리케이션 그룹 제어 규칙** 창이 열립니다.
6. 창이 열리면 **네트워크 규칙** 탭을 선택합니다.
7. 다음 중 하나를 수행합니다:

   - 네트워크 규칙을 만들려면 **추가** 버튼을 누릅니다.
   - 네트워크 규칙을 편집하려면 네트워크 규칙 목록에서 해당 규칙을 선택하고 **편집** 버튼을 누릅니다.

   네트워크 규칙 창이 열립니다.

8. **처리** 드롭다운 목록에서, 이러한 종류의 네트워크 활동을 감지할 경우 방화벽에서 수행할 처리 방법을 선택합니다:

   - **허용**
   - **차단**

9. **이름** 필드에서 다음 방법 중 하나로 네트워크 서비스의 이름을 지정합니다:

   - 이름 필드의 오른쪽에 있는 아이콘을 누르고 드롭-다운 목록에서 네트워크 서비스 **이름**을 선택하십시오.
     드롭다운 목록에는 자주 사용하는 네트워크 연결을 정의하는 네트워크 서비스가 포함됩니다.
   - **이름** 필드에 네트워크 서비스 이름을 직접 입력합니다.

10. 다음 방법으로 데이터 전송 프로토콜을 지정합니다:

    a. **프로토콜** 확인란을 선택합니다.

    b. 드롭다운 목록에서 네트워크 활동을 감시할 프로토콜 유형을 선택합니다.
       방화벽이 TCP, UDP, ICMP, ICMPv6, IGMP 및 GRE 프로토콜을 사용하는 네트워크 연결을 감시합니다.
       이름 드롭다운 목록에서 네트워크 서비스를 선택하면 **프로토콜** 확인란이 자동으로 선택되고 확인란 옆의 드롭다운 목록이 선택한 네트워크 서비스에 해당하는 프로토콜 유형으로 채워집니다. 기본적으로 **프로토콜** 확인란은 선택되어 있지 않습니다.

11. **방향** 드롭다운 목록에서 감시하는 네트워크 활동의 방향을 선택합니다.
    방화벽이 다음과 같은 네트워크 방향의 연결을 감시합니다:

    - **인바운드**.
    - **인바운드/아웃바운드**.
    - **아웃바운드**.

12. ICMP 또는 ICMPv6를 프로토콜로 선택한 경우 ICMP 패킷 유형과 코드를 지정할 수 있습니다:

    a. **ICMP 유형** 확인란을 선택하고 드롭다운 목록에서 ICMP 패킷 유형을 선택합니다.

    b. **ICMP 코드** 확인란을 선택하고 드롭다운 목록에서 ICMP 패킷 코드를 선택합니다.

13. TCP 또는 UDP를 프로토콜 유형으로 선택한 경우 연결을 모니터링할 로컬 및 원격 컴퓨터의 포트 번호를 쉼표로 구분하여 지정할 수 있습니다:

    a. **원격 포트** 필드에 원격 컴퓨터의 포트를 입력합니다.

    b. **로컬 포트** 필드에 로컬 컴퓨터의 포트를 입력합니다.

14. 네트워크 패킷을 주고 받는 원격 컴퓨터의 네트워크 주소를 지정합니다. **원격 주소** 드롭다운 목록에서 다음 값 중 하나를 선택하십시오:

    - **모든 주소**. 네트워크 규칙은 모든 IP 주소를 가지고 있는 원격 컴퓨터에서 송수신되는 네트워크 패킷을 제어합니다.
    - **서브넷 주소**. 네트워크 규칙은 선택된 네트워크 유형과 관련된 IP 주소를 가진 원격 컴퓨터에서의 송수신 네트워크 패킷을 제어합니다: **신뢰하는 네트워크**, **로컬 네트워크** 또는 **공용 네트워크**.

- **주소 목록**. 네트워크 규칙은 아래 목록에서 **추가**, **편집** 및 **삭제** 버튼을 이용해 지정할 수 있는 IP 주소를 가진 원격 컴퓨터에서의 송수신 네트워크 패킷을 제어합니다.

15. Kaspersky Endpoint Security가 설치된 컴퓨터의 네트워크 주소를 지정해 네트워크 패킷을 송수신할 수 있습니다. **로컬 주소** 드롭다운 목록에서 다음 값 중 하나를 선택하십시오:

    - **모든 주소**. 네트워크 규칙은 Kaspersky Endpoint Security가 설치된 컴퓨터 및 모든 IP 주소를 가진 컴퓨터와의 네트워크 패킷 송수신을 제어합니다.

    - **주소 목록**. 네트워크 규칙은 아래 목록에서 **추가**, **편집** 및 **삭제** 버튼을 이용해 지정할 수 있는 IP 주소를 가진 Kaspersky Endpoint Security가 설치된 컴퓨터 및 모든 IP 주소를 가진 컴퓨터에서의 송수신 네트워크 패킷을 제어합니다.

    > 네트워크 패킷을 사용하는 애플리케이션에 대해 로컬 주소를 얻지 못할 수 있습니다. 이 경우 **로컬 주소** 설정 값이 무시됩니다.

16. 네트워크 규칙의 동작을 리포트에 반영하려면 **이벤트 로그** 확인란을 선택합니다.

17. **네트워크 규칙** 창에서 **확인**을 누릅니다.

    새 네트워크 규칙을 만들면 해당 규칙이 **네트워크 규칙** 창에 표시됩니다.

18. 애플리케이션 그룹 규칙의 경우 **애플리케이션 제어 규칙** 창에서, 애플리케이션 규칙의 경우 **애플리케이션 제어 규칙** 창에서 **확인**을 누릅니다.

19. **방화벽** 창에서 **확인**을 누릅니다.

20. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 네트워크 규칙 사용 및 중지

애플리케이션 네트워크 규칙을 작동 또는 중지시키려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽** 하위 섹션을 선택합니다.

   창 오른쪽에 방화벽 구성요소의 설정이 표시됩니다.

3. **애플리케이션 네트워크 규칙** 버튼을 누릅니다.

   방화벽 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.

4. 목록에서 네트워크 규칙을 작동하거나 중지할 애플리케이션 또는 애플리케이션 그룹을 선택합니다.

5. 마우스 오른쪽 버튼을 눌러 메뉴를 열고 수행해야 하는 작업에 따라 **애플리케이션 규칙** 또는 **그룹 규칙**을 선택합니다.

   이것을 누르면 **애플리케이션 제어 규칙** 또는 **애플리케이션 그룹 제어 규칙** 창이 열립니다.

6. 창이 열리면 **네트워크 규칙** 탭을 선택합니다.

7. 애플리케이션 그룹에 대한 네트워크 규칙 목록에서 관련 네트워크 규칙을 선택합니다.

8. 다음 중 하나를 수행합니다:

- 규칙을 작동하려면 해당 네트워크 규칙 이름 옆의 확인란을 선택합니다.
- 규칙을 중지하려면 네트워크 규칙 이름 옆의 확인란을 선택 해제합니다.

  방화벽에 의해 기본적으로 만들어지는 애플리케이션 그룹 네트워크 규칙은 중지시킬 수 없습니다.

9. 애플리케이션 그룹 규칙의 경우 **애플리케이션 제어 규칙** 창에서, 애플리케이션 규칙의 경우 **애플리케이션 제어 규칙** 창에서 **확인**을 누릅니다.
10. **방화벽** 창에서 **확인**을 누릅니다.
11. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

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. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽** 하위 섹션을 선택합니다.
   창 오른쪽에 방화벽 구성요소의 설정이 표시됩니다.
3. **애플리케이션 네트워크 규칙** 버튼을 누릅니다.
   방화벽 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.
4. 기본 생성된 모든 네트워크 규칙에 적용되는 방화벽 동작을 변경하려면 목록에서 애플리케이션 또는 애플리케이션 그룹을 선택합니다. 수동으로 생성된 네트워크 규칙은 변경되지 않습니다.
5. **네트워크** 열에서 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 표시하고 할당할 동작을 선택합니다:
   - **상속**
   - **허용**
   - **차단**
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 또는 애플리케이션 그룹의 네트워크 규칙에 대한 방화벽 동작을 수정하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽**을 선택합니다.
   창 오른쪽에 방화벽 구성요소의 설정이 표시됩니다.

3. **애플리케이션 네트워크 규칙** 버튼을 누릅니다.
   방화벽 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.

4. 목록에서 네트워크 규칙 한 개에 적용되는 동작을 변경할 애플리케이션 또는 애플리케이션 그룹을 선택합니다.

5. 마우스 오른쪽 버튼을 눌러 메뉴를 열고 수행해야 하는 작업에 따라 **애플리케이션 규칙** 또는 **그룹 규칙**을 선택합니다.
   이것을 누르면 **애플리케이션 제어 규칙** 또는 **애플리케이션 그룹 제어 규칙** 창이 열립니다.

6. 창이 열리면 **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:

   - **허용**
   - **차단**
   - **이벤트 로그**

9. 애플리케이션 그룹 규칙의 경우 **애플리케이션 제어 규칙** 창에서, 애플리케이션 규칙의 경우 **애플리케이션 제어 규칙** 창에서 **확인**을 누릅니다.

10. **방화벽** 창에서 **확인**을 누릅니다.

11. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

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. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **방화벽** 하위 섹션을 선택합니다.
   창 오른쪽에 방화벽 구성요소의 설정이 표시됩니다.

3. **애플리케이션 네트워크 규칙** 버튼을 누릅니다.
   방화벽 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.

4. 애플리케이션 목록에서 네트워크 규칙의 우선 순위를 변경할 애플리케이션 또는 애플리케이션 그룹을 선택합니다.

5. 마우스 오른쪽 버튼을 눌러 메뉴를 열고 수행해야 하는 작업에 따라 **애플리케이션 규칙** 또는 **그룹 규칙**을 선택합니다.

   이것을 누르면 **애플리케이션 제어 규칙** 또는 **애플리케이션 그룹 제어 규칙** 창이 열립니다.

6. 창이 열리면 **네트워크 규칙** 탭을 선택합니다.

7. 우선 순위를 변경할 네트워크 규칙을 선택합니다.

8. **위로 이동** 및 **아래로 이동** 버튼을 사용하여 네트워크 규칙을 목록에서 원하는 위치로 이동합니다.

9. 애플리케이션 그룹 규칙의 경우 **애플리케이션 제어 규칙** 창에서, 애플리케이션 규칙의 경우 **애플리케이션 제어 규칙** 창에서 **확인**을 누릅니다.

10. **방화벽** 창에서 **확인**을 누릅니다.

11. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

네트워크 모니터

네트워크 모니터에 대한 정보와 네트워크 모니터를 시작하는 방법에 대해 설명합니다.

네트워크 모니터 정보

*네트워크 모니터*는 네트워크 활동에 대한 정보를 실시간으로 확인하기 위해 개발된 도구입니다.

네트워크 모니터 시작

네트워크 모니터를 시작하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.

2. **보호 및 제어** 탭을 선택합니다.

3. **보호** 섹션을 누릅니다.

   보호 섹션이 열립니다.

4. **방화벽** 줄을 마우스 오른쪽 버튼으로 눌러 방화벽 동작의 컨텍스트 메뉴를 엽니다.

5. 마우스 오른쪽 메뉴에서 **네트워크 모니터**를 선택합니다.

   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.

   - **열린 포트** 탭에는 컴퓨터의 열린 네트워크 포트가 모두 나열됩니다.

- **네트워크 트래픽** 탭에는 사용자 컴퓨터와 현재 사용자가 연결된 네트워크에 있는 다른 컴퓨터 사이의 인바운드 및 아웃바운드 네트워크 트래픽 양이 표시됩니다.

- **차단한 컴퓨터** 탭에는 해당 IP 주소에서 네트워크 공격을 시도한 것으로 탐지되어 네트워크 공격 차단 구성 요소에 의해 네트워크 활동이 차단된 원격 컴퓨터의 IP 주소가 표시됩니다.

네트워크 공격 차단

이 섹션에는 네트워크 공격 차단에 대한 정보와 해당 구성요소 설정을 구성하는 방법에 대한 지침이 나와 있습니다.

네트워크 공격 차단 정보

네트워크 공격 차단은 인바운드 네트워크 트래픽에 네트워크 공격을 위한 일반적인 활동이 있는지 검사합니다. 사용자 컴퓨터를 대상으로 시도된 네트워크 공격이 탐지되면 Kaspersky Endpoint Security는 공격 컴퓨터의 네트워크 동작을 차단합니다. 그런 다음 화면에 네트워크 공격 시도를 알리는 경고와 함께 공격 컴퓨터에 대한 정보가 표시됩니다.

공격 컴퓨터의 네트워크 트래픽이 1시간 동안 차단됩니다. 공격 컴퓨터를 차단하는 설정을 편집하려면 다음과 같이 하십시오.

현재 알려진 네트워크 공격의 유형과 이를 차단하는 방법에 대한 설명은 Kaspersky Endpoint Security 데이터베이스에서 제공합니다. 네트워크 공격 차단 구성요소가 탐지하는 네트워크 공격 목록은 데이터베이스 및 애플리케이션 모듈 업데이트 중에 업데이트됩니다.

네트워크 공격 차단 작동 및 중지

기본적으로 네트워크 공격 차단은 작동되어 있으며 최적 모드가 사용됩니다. 필요한 경우 네트워크 공격 차단을 중지할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

네트워크 공격 차단을 작동 또는 중지하려면 메인 애플리케이션 창의 보호 및 제어 탭에서 다음을 수행하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **보호** 섹션을 누릅니다.
   보호 섹션이 열립니다.
4. **네트워크 공격 차단** 행을 마우스 오른쪽 버튼으로 눌러 네트워크 공격 차단 처리 방법의 마우스 오른쪽 메뉴를 표시합니다.
5. 다음 중 하나를 수행합니다:
   - 네트워크 공격 차단을 작동하려면 마우스 오른쪽 메뉴에서 **시작**을 선택합니다.
     네트워크 공격 차단 줄의 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.
   - 네트워크 공격 차단을 중지하려면 마우스 오른쪽 메뉴에서 **중지**를 선택합니다.
     네트워크 공격 차단 줄의 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 네트워크 공격 차단을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **네트워크 공격 차단**을 선택합니다.
   창 오른쪽에 네트워크 공격 차단 설정이 표시됩니다.
3. 다음을 수행합니다:
   - 네트워크 공격 차단을 작동하려면 **네트워크 공격 차단 사용** 확인란을 선택합니다.
   - 네트워크 공격 차단을 중지하려면 **네트워크 공격 차단 사용** 확인란의 선택을 취소합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

네트워크 공격 차단 설정

네트워크 공격 차단 설정을 구성하는 다음 작업을 수행할 수 있습니다:

- 공격 컴퓨터를 차단하는 데 사용되는 설정 구성.
- 차단에서 예외할 주소 목록을 생성합니다.

공격 컴퓨터를 차단하는 데 사용되는 설정 편집

공격 컴퓨터를 차단하는 설정을 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **네트워크 공격 차단**을 선택합니다.
   창 오른쪽에 네트워크 공격 차단 설정이 표시됩니다.
3. **다음 시간 동안 공격 컴퓨터 차단** 확인란을 선택합니다.
   이 확인란을 선택하는 경우, 네트워크 공격 시도가 탐지되면 네트워크 공격 차단에서 지정된 시간 동안 공격 컴퓨터의 네트워크 트래픽을 차단합니다. 이렇게 하면 향후 동일한 주소에서 발생할 수 있는 네트워크 공격으로부터 컴퓨터를 자동으로 보호할 수 있습니다.
   이 확인란의 선택을 취소하는 경우, 네트워크 공격 시도가 탐지되어도 향후 동일한 주소에서 발생할 수 있는 네트워크 공격으로부터 네트워크 공격 차단이 컴퓨터를 자동으로 보호하는 기능을 작동하지 않습니다.
4. **다음 시간 동안 공격 컴퓨터 차단** 확인란 옆에 있는 필드에서 공격 컴퓨터가 차단되는 시간을 변경합니다.
5. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

차단에서 예외할 주소 구성

차단에서 예외할 주소를 구성하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **네트워크 공격 차단**을 선택합니다.
   창 오른쪽에 네트워크 공격 차단 설정이 표시됩니다.

3. **예외** 버튼을 누릅니다.
   예외 창이 열립니다.

4. 다음 중 하나를 수행합니다:

   - 새 IP 주소를 추가하려면 **추가** 버튼을 누릅니다.
   - 만일 기존에 추가한 IP 주소를 편집하고 싶다면, 해당 주소를 주소 목록에서 선택하고 **편집** 버튼을 누릅니다.

   IP 주소 창이 열립니다.

5. 네트워크 공격을 차단해야 하는 컴퓨터의 IP 주소를 입력합니다.

6. **IP 주소** 창에서 **확인**을 누릅니다.

7. **예외** 창에서 **확인**을 누릅니다.

8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

BadUSB 공격 차단

이 섹션은 BadUSB 공격 차단 구성요소에 대한 정보를 담고 있습니다.

BadUSB 공격 차단 정보

일부 바이러스는 USB 장치의 펌웨어를 수정해 운영 체제가 USB 장치를 키보드를 인식하도록 속입니다.

BadUSB 공격 차단 구성요소는 키보드를 에뮬레이션하는 감염된 USB 장치가 컴퓨터에 연결하지 못하도록 차단합니다.

USB 장치가 컴퓨터에 연결되고 애플리케이션이 키보드로 인식할 때, 애플리케이션은 사용자에게 이 키보드 또는 화상 키보드를(가능할 경우) 이용해 애플리케이션이 생성한 숫자로 이루어진 코드를 입력하도록 요청합니다. 이 절차는 키보드 인증을 의미합니다. 애플리케이션은 인증된 키보드만 사용할 수 있도록 허용하고 인증 안 된 키보드는 차단합니다.

이 구성요소가 설치되자 마자 BadUSB 공격 차단은 백그라운드 모드에서 실행됩니다. 애플리케이션이 Kaspersky Security Center 정책 적용 대상이 아닌 경우 컴퓨터 보호 및 제어를 일시 중지했다가 다시 시작하여 BadUSB 공격 차단을 작동 또는 중지할 수 있습니다.

BadUSB 공격 차단 구성요소 설치

Kaspersky Endpoint Security 설치 동안 기본 또는 표준 설치를 선택한 경우 BadUSB 공격 차단 구성요소를 사용할 수 없습니다. BadUSB 공격 차단 구성요소를 설치하려면 애플리케이션 구성요소 조합을 변경해야 합니다.

BadUSB 공격 차단 구성요소를 설치하려면:

1. **시작** 메뉴에서 **애플리케이션 → Kaspersky Endpoint Security 10 for Windows → 수정, 복구 또는 제거**를 선택합니다.

   설치 마법사가 시작됩니다.

2. 애플리케이션 설치 마법사의 **수정, 복구 또는 제거** 창에서 **수정** 버튼을 누릅니다.

   이러면 애플리케이션 설치 마법사의 **사용자 지정 설치** 창이 열립니다.

3. **BadUSB 공격 차단** 구성요소 이름 옆에 있는 아이콘의 마우스 오른쪽 메뉴에서 **로컬 하드 드라이브에서 기능을 설치합니다** 옵션을 선택합니다.

4. **다음** 버튼을 누릅니다.

5. 설치 마법사의 안내를 따릅니다.

BadUSB 공격 차단 사용 및 중지

BadUSB 공격 차단 기능을 사용하거나 중지하려면:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **BadUSB 공격 차단**을 선택합니다.

창 오른쪽에 BadUSB 공격 차단 설정이 표시됩니다.

3. 다음 중 하나를 수행합니다:

   - BadUSB 공격 차단을 사용하려면 **BadUSB 공격 차단 사용** 확인란을 선택합니다.
   - BadUSB 공격 차단을 중지하려면 **BadUSB 공격 차단 사용** 확인란을 선택 해제합니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

인증 시 화상 키보드 사용 허용 및 금지

화상 키보드는 무작위 문자 입력을 지원하지 않는 USB 장치의 인증을 위해서만 사용됩니다(예, 바코드 스캐너). 알려지지 않은 USB 장치의 인증에서는 화상 키보드 사용을 권장하지 않습니다.

인증 시 화상 키보드의 사용을 허용 또는 금지하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션에서 **BadUSB 공격 차단**을 선택합니다.
   창 오른쪽에 구성요소 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:

   - **인증 시 화상 키보드 사용 차단**을 선택하면 인증 시 화상 키보드 사용을 차단합니다.
   - **인증 시 화상 키보드 사용 차단**을 선택 해제하면 인증 시 화상 키보드 사용을 허용합니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

키보드 인증

BadUSB 공격 차단 구성요소가 설치되기 전에 컴퓨터에 연결되고 운영 체제에 의해 키보드로 식별된 USB 장치는 이 구성요소가 설치된 이후에 인증된 것으로 간주됩니다.

USB 키보드 인증을 위한 물어보기가 활성되었을 때에만 이 애플리케이션은 운영 체제에 의해 키보드로 식별된 USB 장치의 인증을 요구합니다. 사용자는 키보드가 인증될 때까지 미인증 키보드를 사용할 수 없습니다.

만일 USB 키보드 인증을 위한 물어보기가 비활성되었다면, 사용자는 연결된 모든 키보드를 사용할 수 있습니다. USB 키보드 인증을 위한 물어보기가 활성되는 즉시 이 애플리케이션은 각각의 연결된 미인증 키보드를 인증하기 위한 물어보기 창이 나타납니다.

키보드를 인증하려면:

1. USB 키보드 인증을 활성하고 해당 키보드를 USB 포트에 연결합니다.
   <키보드 이름> 키보드 인증 창이 연결된 키보드의 세부 정보와 인증을 위한 숫자 코드와 함께 열립니다.
2. 연결된 키보드 또는 화상 키보드(이용 가능할 경우)로 인증 창에 생성된 무자위 숫자 코드를 입력합니다.
3. **확인**을 누릅니다.

만일 해당 코드를 올바르게 입력했다면, 이 애플리케이션은 인증된 키보드 목록에 식별 매개 변수(키보드의 VID/PID와 키보드가 연결된 포트 번호)를 저장합니다. 키보드가 다시 연결되거나 운영 체제가 재시작된 이후에 인증을 반복할 필요는 없습니다.

> 인증된 키보드가 다른 USB 포트에 연결되면, 애플리케이션은 해당 키보드에 대한 인증을 다시 요구합니다.

만일 숫자 코드가 부정확히 입력되었다면, 애플리케이션은 새 코드를 만듭니다. 숫자 코드 입력은 세 번 시도할 수 있습니다. 만일 세 번 연속으로 부정확한 숫자 코드 입력 또는 **<키보드 이름> 키보드 인증** 창이 닫히면, 이 애플리케이션은 이 키보드를 차단합니다. 해당 키보드가 다시 연결되거나 운영 체제가 재시작되면, 애플리케이션은 키보드 인증을 사용자에게 다시 요구합니다.

애플리케이션 시작 제어

이 섹션에는 애플리케이션 시작 제어에 대한 정보와 해당 구성요소 설정을 구성하는 방법에 대한 지침이 나와 있습니다.

애플리케이션 시작 제어 정보

애플리케이션 시작 제어 구성요소는 *애플리케이션 시작 제어 규칙*을 사용하여 애플리케이션을 시작하는 사용자의 시도를 모니터링하고 애플리케이션의 시작을 규제합니다.

설정이 어떤 애플리케이션 시작 제어 규칙과도 일치하지 않는 애플리케이션의 시작은 선택한 구성요소 운영 모드로 규정됩니다. 기본적으로 *블랙리스트 모드*가 선택되어 있습니다. 이 모드는 모든 사용자가 모든 애플리케이션을 시작하도록 허용합니다.

애플리케이션을 시작하기 위한 모든 사용자 시도는 리포트에 기록됩니다.

애플리케이션 시작 제어 작동 및 중지

기본적으로 애플리케이션 시작 제어가 비활성화되어 있지만 필요한 경우 애플리케이션 시작 제어를 활성화할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

메인 애플리케이션 창의 보호 및 제어 탭에서 애플리케이션 시작 제어를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **엔드포인트 제어** 섹션을 누릅니다.
   엔드포인트 제어 섹션이 열립니다.
4. 마우스 오른쪽 버튼을 눌러 애플리케이션 시작 제어 구성요소 정보가 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
   구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.
5. 다음 중 하나를 수행합니다:
   - 애플리케이션 시작 제어를 작동하려면 메뉴에서 **시작**을 선택합니다.
     애플리케이션 시작 제어 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.
   - 애플리케이션 시작 제어 구성요소를 중지하려면 메뉴에서 **중지**를 선택합니다.
     애플리케이션 시작 제어 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 애플리케이션 시작 제어를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 시작 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 시작 제어 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 애플리케이션 시작 제어를 작동하려면 **애플리케이션 시작 제어 작동** 확인란을 선택합니다.
   - 애플리케이션 시작 제어를 중지하려면 **애플리케이션 시작 제어 작동** 확인란의 선택을 취소합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 시작 제어 기능 제한

다음 경우에는 애플리케이션 시작 제어 구성요소 작동이 제한됩니다:

- 애플리케이션 버전이 업그레이드되어 애플리케이션 시작 제어 구성요소 설정을 가져올 수 없는 경우.

  애플리케이션 시작 제어 기능을 복원하려면 구성요소 설정을 다시 구성해야 합니다.

- KSN 서버와 연결되어 있지 않은 경우 Kaspersky Endpoint Security는 로컬 데이터베이스에서만 애플리케이션 및 그 모듈의 평판 정보를 얻습니다. 로컬 데이터베이스에 애플리케이션에 대한 정보가 없는 경우 애플리케이션이 제어 그룹으로 배정되지 않습니다.

  KSN 서버에 연결되어 있을 때 애플리케이션에 대한 분류 결과는 KSN에 연결되어 있지 않을 때의 분류 결과와 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.

- 구성요소는 명령줄을 통해 스크립트를 해석기에 전송하지 않는 한 스크립트 시작을 제어하지 않습니다.

  애플리케이션 시작 제어 규칙에서 해석기를 시작하도록 허용된 경우 구성요소는 이 해석기에서 시작된 스크립트를 차단하지 않습니다.

- 구성요소는 Kaspersky Endpoint Security에서 지원하지 않는 해석기 스크립트의 시작을 제어하지 않습니다.
  Kaspersky Endpoint Security는 다음 해석기를 지원합니다:
  - Java
  - PowerShell

  다음 해석기 유형이 지원됩니다:
  - { cCmdLineParser::itCmd, _T("%ComSpec%") };

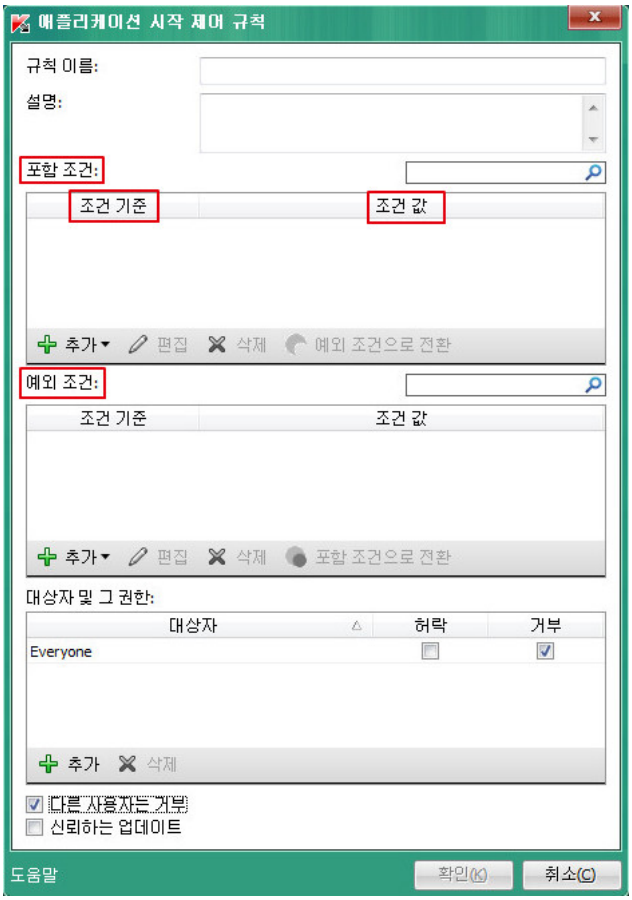
- { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
- { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

애플리케이션 시작 제어 규칙 정보

Kaspersky Endpoint Security는 규칙을 사용해 사용자가 시작한 애플리케이션을 제어합니다. 애플리케이션 시작 제어 규칙은 규칙이 적용되는 시작 조건과 애플리케이션 시작 제어가 수행하는 동작을 지정합니다(사용자가 시작한 애플리케이션의 실행을 허용 또는 차단).

규칙을 작동시키는 조건

규칙 작동 조건에는 아래의 대응 관계가 포함됩니다: "조건 유형 - 조건 기준 - 조건 값" (밑에 그림 참고). 규칙 시작 조건에 따라 Kaspersky Endpoint Security는 애플리케이션에 규칙을 적용 또는 적용하지 않습니다.



애플리케이션 시작 제어 규칙. 규칙을 작동시키는 조건 파라미터

규칙은 포함 및 예외 조건을 이용합니다:

- *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.
- 메타 데이터: 애플리케이션 실행 파일 이름, 애플리케이션 실행 파일 버전, 애플리케이션 이름, 애플리케이션 버전, 애플리케이션 공급 업체.
- 애플리케이션의 실행 파일 해시입니다.
- 인증서: 발급자, 대상자, 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 시작 제어는 규칙에서 지정된 동작을 수행합니다. 애플리케이션 파라미터가 예외 조건에 지정된 기준 값과 일치하는 경우 애플리케이션 시작 제어가 애플리케이션 시작을 제어하지 않습니다.

규칙이 작동할 때 애플리케이션 시작 제어 구성요소의 결정

규칙이 시작될 때, 애플리케이션 시작 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 시작 제어 허락 규칙을 지정했지만 해당 사용자 그룹의 한 구성원에 대해 애플리케이션 시작 제어 차단 규칙을 지정한 경우 이 사용자는 애플리케이션을 시작하지 못합니다.

규칙의 작동 상태

애플리케이션 시작 제어 규칙의 상태는 다음과 같은 2가지 중 하나일 수 있습니다:

- **켜짐.**
  이 규칙 운영 상태는 이 규칙이 작동한다는 것을 나타냅니다.
- **꺼짐.**
  이 규칙 상태는 이 규칙이 중지된다는 것을 나타냅니다.

기본 애플리케이션 시작 제어 규칙

애플리케이션 시작 제어는 기본적으로 블랙리스트 모드로 작동합니다. 이 구성요소는 모든 사용자가 모든 애플리케이션을 시작하도록 허용합니다. 사용자가 애플리케이션 시작 제어 규칙으로 차단되는 애플리케이션을 시작하려고 시도할 때 Kaspersky Endpoint Security는 이 애플리케이션이 시작되지 않도록 차단하거나(**차단** 처리 방법을 선택한 경우) 애플리케이션 시작에 대한 정보를 리포트에 저장합니다(**알림** 처리 방법을 선택한 경우).

애플리케이션 시작 제어 규칙 관리

애플리케이션 시작 제어 규칙을 관리할 때 다음 작업도 수행할 수 있습니다:

- 새 규칙 추가
- 규칙 작동 조건을 작성하거나 변경합니다
- 규칙 상태 편집
  애플리케이션 시작 제어 규칙을 작동하거나(규칙 옆의 확인란 선택) 중지합니다(규칙 옆의 확인란 선택 취소). 애플리케이션 시작 제어 규칙을 만들면 기본적으로 작동되어 있습니다.
- 규칙 삭제

애플리케이션 시작 제어 규칙 추가 및 편집

애플리케이션 시작 제어 규칙을 추가 또는 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 시작 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 시작 제어 구성요소의 설정이 표시됩니다.
3. 이용 가능한 구성요소 설정을 편집하려면 **애플리케이션 시작 제어 사용**을 선택합니다.
4. 다음 중 하나를 수행합니다:
   - 규칙을 추가하려면 **추가** 버튼을 누릅니다.
   - 만일 기존 규칙을 편집하고 싶다면, 규칙 목록에서 원하는 것을 선택하고 **편집** 버튼을 누릅니다.

   애플리케이션 시작 제어 규칙 창이 열립니다.
5. 규칙 설정을 지정 또는 편집합니다:
   a. **규칙 이름** 필드에서 규칙의 이름을 입력하거나 편집합니다.
   b. **포함 조건** 표에서 **추가**, **편집**, **삭제** 및 **예외 조건으로 전환** 버튼을 눌러 규칙을 작동시키는 포함 조건 목록을 만들거나 편집합니다.
   c. **예외 조건** 표에서 **추가**, **편집**, **삭제** 및 **포함 조건으로 전환** 버튼을 눌러 규칙을 작동시키는 예외 조건 목록을 만들거나 편집합니다.
   d. 필요하다면, 규칙 작동 조건 유형을 변경합니다:
      - 포함 조건의 조건 유형을 **포함 조건**으로 변경하려면 포함 조건 표에서 조건을 선택한 다음 **예외 조건으로 전환** 버튼을 누릅니다.
      - 예외 조건의 조건 유형을 포함 조건으로 변경하려면 **예외 조건** 표에서 조건을 선택한 다음 **포함 조건으로 전환** 버튼을 누릅니다.
   e. 규칙 시작 조건을 충족하는 애플리케이션의 시작이 허용된 또는 허용 안 된 사용자 또는 사용자 그룹의 목록을 컴파일하거나 편집합니다. 편집하려면 **대상자 및 그 권한** 표에서 **추가** 단추를 누릅니다.
      Microsoft Windows의 **사용자 또는 그룹 선택** 창이 열립니다. 이 창에서는 사용자 또는 사용자 그룹을 선택할 수 있습니다.
      기본적으로 사용자 목록에 **누구나** 값이 추가됩니다. 규칙이 모든 사용자에게 적용됩니다.

      > 표에서 사용자를 지정하지 않으면 규칙을 저장할 수 없습니다.

   f. **대상자 및 그 권한** 표에서 사용자 또는 사용자 그룹 옆의 **허용** 또는 **차단** 확인란을 선택하여 애플리케이션을 시작할 수 있는 권한을 결정합니다.
      기본적으로 선택되어 있는 확인란은 애플리케이션 시작 제어 작동 모드에 따라 다릅니다.
   g. **대상자** 열에 표시되지 않고 **대상자** 열에 지정된 사용자 그룹에 속하지 않은 모든 사용자가 규칙 작동 조건을 충족하는 애플리케이션을 시작하지 못하도록 차단되기를 원하면 **다른 사용자는 거부** 확인란을 선택합니다.

다른 사용자는 거부 확인란을 선택 취소하면 Kaspersky Endpoint Security가 **대상자 및 그 권한** 표에 지정되지 않거나 **대상자 및 그 권한** 표에 지정된 사용자 그룹에 속하지 않은 사용자의 애플리케이션 시작을 제어하지 않습니다.

h. Kaspersky Endpoint Security가 애플리케이션 시작 제어 규칙이 지정되지 않은 다른 애플리케이션을 시작하기 위해서 허용된 신뢰하는 업데이트로써 규칙 시작 조건을 만족하는 애플리케이션으로 간주하려면 **신뢰하는 업데이트** 확인란을 선택합니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 시작 제어 규칙의 작동 조건 추가

애플리케이션 시작 제어 규칙의 작동 조건을 추가하려면:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 시작 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 시작 제어 구성요소의 설정이 표시됩니다.

3. 이용 가능한 구성요소 설정을 편집하려면 **애플리케이션 시작 제어 사용**을 선택합니다.

4. 다음 중 하나를 수행합니다:

   - 새로운 규칙을 생성하고 그 규칙에 시작 조건을 추가하려면, **추가** 버튼을 누릅니다.
   - 기존 규칙에 시작 조건을 추가하려면, 규칙 목록에서 규칙을 선택하고 **편집** 버튼을 누릅니다.

   애플리케이션 시작 제어 규칙 창이 열립니다.

5. **포함 조건** 또는 **예외 조건** 표에서 **추가** 버튼을 누릅니다.

추가 버튼의 드롭다운 목록을 이용해 규칙에 여러 시작 조건을 추가할 수 있습니다(밑에 지침 참고).

지정된 폴더에 있는 파일 속성을 기반으로 규칙 시작 조건을 추가하려면:

1. **추가** 버튼의 드롭다운 목록에서 **지정된 폴더에 있는 파일 속성의 조건**을 선택합니다.
   Microsoft Windows의 표준 **폴더 선택** 창이 열립니다.

2. **폴더 선택** 창에서 규칙을 시작시키는 하나 이상의 조건에 대한 기반으로 사용할 속성의 애플리케이션 실행 파일이 들어 있는 폴더를 선택합니다.

3. **확인**을 누릅니다.
   조건 추가 창이 열립니다.

4. **표시 기준** 드롭다운 목록에서 규칙 시작 조건을 하나 이상 만들 때 기반으로 사용할 기준을 선택합니다: **파일 해시 코드**, **인증서**, **KL 카테고리**, **메타데이터** 또는 **폴더 경로**.

Kaspersky Endpoint Security는 MD5 파일 해시 코드를 지원하지 않으므로 MD5 해시를 기준으로 애플리케이션 시작을 제어하지 않습니다. 대신 SHA256 해시가 규칙 작동 조건으로 사용됩니다.

5. **표시 기준** 드롭다운 목록에서 **메타데이터**를 선택했으면 규칙 시작 조건에 사용할 실행 파일 옆의 확인란을 선택합니다: **파일 이름**, **파일 버전**, **애플리케이션 이름**, **애플리케이션 버전**, **공급업체**.

   지정된 속성 중 하나를 선택하지 않으면 규칙을 저장할 수 없습니다.

6. **표시 기준** 드롭다운 목록에서 **인증서**를 선택했으면 규칙 작동 조건에 사용할 설정 옆의 확인란을 선택합니다: **발급자**, **대상자** 및 **손도장**.

   지정된 설정 중 하나를 선택하지 않으면 규칙을 저장할 수 없습니다.

   발급 기관 및 **대상자** 기준만을 규칙 작동 조건으로 사용하는 것은 권장되지 않습니다. 이러한 기준 사용을 신뢰할 수 없습니다.

7. 규칙 시작 조건에 포함시킬 속성의 애플리케이션 실행 파일 이름 옆에 있는 확인란을 선택합니다.

8. **다음** 버튼을 누릅니다.

   만들어진 규칙 작동조건의 목록이 나타납니다.

9. 만들어진 규칙 작동조건의 목록에서 애플리케이션 시작 제어 규칙에 추가할 규칙 작동조건 옆의 확인란을 선택합니다.

10. **끝내기** 버튼을 누릅니다.

컴퓨터에서 시작된 애플리케이션의 속성을 기반으로 규칙 시작 조건을 추가하려면:

1. **추가** 버튼 드롭다운 목록에서 **시작된 애플리케이션 속성의 조건**을 선택합니다.

2. **표시 기준** 드롭다운 목록의 **조건 추가** 창에서 규칙 시작 조건을 하나 이상 만들 때 기반으로 사용할 기준을 선택합니다: **파일 해시 코드**, **인증서**, **KL 카테고리**, **메타데이터** 또는 **폴더 경로**.

3. **표시 기준** 드롭다운 목록에서 **메타데이터**를 선택했으면 규칙 시작 조건에 사용할 실행 파일 옆의 확인란을 선택합니다: **파일 이름**, **파일 버전**, **애플리케이션 이름**, **애플리케이션 버전**, **공급업체**.

   지정된 속성 중 하나를 선택하지 않으면 규칙을 저장할 수 없습니다.

4. **표시 기준** 드롭다운 목록에서 **인증서**를 선택했으면 규칙 작동 조건에 사용할 설정 옆의 확인란을 선택합니다: **발급 기관**, **대상자** 및 **손도장**.

   지정된 설정 중 하나를 선택하지 않으면 규칙을 저장할 수 없습니다.

   발급 기관 및 **대상자** 기준만을 규칙 작동 조건으로 사용하는 것은 권장되지 않습니다. 이러한 기준 사용을 신뢰할 수 없습니다.

5. 규칙 시작 조건에 포함시킬 속성의 애플리케이션 실행 파일 이름 옆에 있는 확인란을 선택합니다.

6. **다음** 버튼을 누릅니다.

   만들어진 규칙 작동조건의 목록이 나타납니다.

7. 만들어진 규칙 작동조건의 목록에서 애플리케이션 시작 제어 규칙에 추가할 규칙 작동조건 옆의 확인란을 선택합니다.

8. **끝내기** 버튼을 누릅니다.

KL 카테고리 속성을 기반으로 규칙 시작 조건을 추가하려면:

1. **추가** 버튼 드롭다운 목록에서 **"KL 카테고리" 조건**를 선택합니다.

   *KL 카테고리*는 테마 특성을 공유하는 애플리케이션의 목록입니다. 이 목록은 Kaspersky 전문가에 의해 유지 관리됩니다. 예를 들어, "오피스 애플리케이션"의 KL 카테고리에는 Microsoft Office 제품군, Adobe® Acrobat® 등이 포함됩니다.

2. **"KL 카테고리" 조건** 창에서 규칙 작동 조건을 만들 때 기반으로 사용하는 KL 카테고리 이름 옆의 확인란을 선택합니다.

3. **확인**을 누릅니다.

사용자 지정 시작 조건을 추가하려면:

1. **추가** 버튼 드롭다운 목록에서 **사용자 지정 조건**을 선택합니다.

2. **사용자 지정 조건** 창에서 **선택**을 눌러 애플리케이션 실행 파일로의 경로를 지정하십시오.

3. 규칙 작동 조건을 만들 때 기반으로 사용되는 기준을 선택합니다: **파일 해시 코드**, **인증서**, **메타데이터** 또는 **파일 또는 폴더의 경로**.

   파일 또는 폴더의 경로 필드에 심볼릭 링크를 사용하는 경우 애플리케이션 시작 제어 규칙이 제대로 작동하려면 심볼릭 링크의 주소를 변환하는 것이 좋습니다. 그러려면 **기호 링크 해석** 버튼을 누릅니다.

4. 필요한 경우 선택한 기준의 설정을 구성합니다.

5. **확인**을 누릅니다.

애플리케이션 실행 파일이 저장된 드라이브에 대한 정보를 기반으로 규칙 시작 조건을 추가하려면:

1. **추가** 버튼 드롭다운 목록에서 **파일 드라이브별 조건**을 선택합니다.

2. **파일 드라이브별 조건** 창에서 **드라이브** 드롭다운 목록에 있는 애플리케이션 시작 제어 규칙이 애플리케이션 시작을 제어하는 드라이브의 유형을 선택합니다.

3. **확인**을 누릅니다.

애플리케이션 시작 제어 규칙의 상태 변경

애플리케이션 시작 제어 규칙의 상태를 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 시작 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 시작 제어 구성요소의 설정이 표시됩니다.

3. 이용 가능한 구성요소 설정을 편집하려면 **애플리케이션 시작 제어 사용**을 선택합니다.

4. 편집할 상태의 규칙을 선택합니다.

5. **상태** 열에서는 다음을 수행합니다:

   - 규칙 사용을 활성화하려면 규칙 옆의 확인란을 선택합니다.
   - 규칙 사용을 비활성화하려면 규칙 옆의 확인란을 선택 취소합니다.

6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 시작 제어 규칙 테스트

애플리케이션 시작 제어 규칙으로 작업에 필요한 애플리케이션이 차단되지 않도록 하려면 새로 생성된 규칙을 테스트 모드로 놓고 규칙의 작동을 분석하기를 권장합니다.

테스트 모드에서 애플리케이션 시작 제어 규칙의 작업을 검토하는 것은 Kaspersky Security Center에 보고된 애플리케이션 시작 제어 이벤트를 검토하는 것과 연관이 있습니다. 컴퓨터 사용자의 작업에 필요한 모든 애플리케이션 시작이 허용되었으면 규칙이 올바르게 만들어진 것입니다. 그렇지 않은 경우 작성한 규칙의 설정을 다시 검토하기 바랍니다.

애플리케이션 시작 제어 규칙의 테스트 모드는 기본적으로 설정되어 있지 않습니다.

애플리케이션 시작 제어 규칙을 테스트하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 시작 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 시작 제어 구성요소의 설정이 표시됩니다.
3. 이용 가능한 구성요소 설정을 편집하려면 **애플리케이션 시작 제어 사용**을 선택합니다.
4. **애플리케이션 시작 제어 모드** 드롭다운 목록에서 다음 항목 중 하나를 선택합니다:

   - **블랙리스트** - 차단 규칙에서 지정한 애플리케이션을 예외하고 모든 애플리케이션 시작을 허용하려는 경우.
   - **화이트리스트** - 허용 규칙에서 지정한 애플리케이션을 예외하고 모든 애플리케이션 시작을 차단하려는 경우.

5. **처리** 드롭다운 목록에서 **알림**을 선택합니다.
6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

Kaspersky Endpoint Security는 애플리케이션 시작 제어 규칙으로 시작이 금지된 애플리케이션을 차단하지는 않지만 중앙 관리 서버로 애플리케이션 시작에 대한 알림을 전송합니다.

애플리케이션 시작 제어 메시지 템플릿 편집

사용자가 애플리케이션 시작 제어 규칙에 의해 차단된 애플리케이션을 시작하려고 시도하는 경우 Kaspersky Endpoint Security는 해당 애플리케이션의 시작이 차단되었다는 메시지 상태를 표시합니다. 사용자가 애플리케이션 시작이 잘못 차단되었다고 생각한다면, 사용자는 메시지 텍스트의 링크를 사용하여 메시지를 회사 네트워크 관리자에게 전송할 수 있습니다.

애플리케이션 시작이 차단된 경우 표시되는 메시지나 관리자에게 보내는 메시지의 템플릿을 지정합니다. 이러한 메시지 템플릿은 수정할 수 있습니다.

메시지 템플릿을 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 시작 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 시작 제어 구성요소의 설정이 표시됩니다.
3. 이용 가능한 구성요소 설정을 편집하려면 **애플리케이션 시작 제어 사용**을 선택합니다.
4. **템플릿** 버튼을 누릅니다.
   메시지 템플릿 창이 열립니다.
5. 다음 중 하나를 수행합니다:
   - 애플리케이션 시작이 차단된 경우 표시되는 메시지 템플릿을 편집하려면 **차단** 탭을 선택합니다.
   - LAN 관리자에게 보내는 메시지의 템플릿을 수정하고 싶다면 **관리자에게 메시지 보내기** 탭을 선택합니다.
6. 애플리케이션 시작이 차단된 경우 표시되는 메시지나 관리자에게 보내는 메시지의 템플릿을 수정합니다. 이렇게 하려면 **기본값** 및 **변수** 버튼을 사용합니다.
7. **확인**을 누릅니다.
8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 시작 제어 작동 모드 정보

애플리케이션 시작 제어 구성요소에는 다음 두 가지 작동 모드가 있습니다:

- **블랙리스트**. 이 애플리케이션 시작 제어 모드에서는 모든 사용자가 애플리케이션 시작 제어의 차단허락 규칙에 지정된 애플리케이션을 예외한 모든 애플리케이션을 시작할 수 있습니다.
  애플리케이션 시작 제어의 기본 작동 모드입니다.
- **화이트리스트**. 이 애플리케이션 시작 제어 모드에서는 모든 사용자가 애플리케이션 시작 제어의 허락 규칙에 지정된 애플리케이션을 예외한 모든 애플리케이션을 시작할 수 없습니다.
  애플리케이션 시작 제어의 허락 규칙이 구성 완료되면 애플리케이션 시작 제어 구성요소가 LAN 관리자에 의해 확인되지 않는 모든 새로운 애플리케이션의 시작을 차단합니다. 단, 사용자의 업무에 필요한 운영 체제 및 신뢰할 수 있는 애플리케이션의 작동은 허락됩니다.

모드 마다 애플리케이션 실행 시 수행할 수 있는 처리 방법이 두 개가 있습니다: Kaspersky Endpoint Security는 애플리케이션 시작 제어 규칙의 조건을 충족하는 애플리케이션이 시작될 때 애플리케이션이 시작되지 못하도록 차단하거나 사용자에게 알림을 보낼 수 있습니다.

애플리케이션 시작 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 시작 제어 규칙은 사용자지정 애플리케이션 카테고리를 바탕으로 하며 Kaspersky Endpoint Security 로컬 인터페이스는 포함 및 예외 조건을 바탕으로 합니다.

- LAN 컴퓨터에 설치된 애플리케이션에 대한 정보 수집.

Kaspersky Security Center를 이용해 애플리케이션 시작 제어 구성요소의 작동을 구성하도록 권장되는 이유입니다.

애플리케이션 시작 제어 모드 선택

애플리케이션 시작 제어 모드를 선택하려면 다음과 같이 합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 시작 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 시작 제어 구성요소의 설정이 표시됩니다.
3. 이용 가능한 구성요소 설정을 편집하려면 **애플리케이션 시작 제어 사용**을 선택합니다.
4. **애플리케이션 시작 제어 모드** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다:
   - **블랙리스트** - 차단 규칙에서 지정한 애플리케이션을 예외하고 모든 애플리케이션 시작을 허용하려는 경우.
   - **화이트리스트** - 허용 규칙에서 지정한 애플리케이션을 예외하고 모든 애플리케이션 시작을 차단하려는 경우.

     이 모드를 선택하면 기본적으로 애플리케이션 시작 제어 규칙 2개가 생성됩니다: **골든 이미지** 및 **신뢰하는 업데이트**. 규칙을 삭제할 수 없습니다. 이 규칙의 설정을 편집할 수 없습니다. 관련 규칙 옆의 확인란을 선택 또는 선택 취소하여 이 규칙을 작동 또는 중지할 수 없습니다. 기본적으로 **골든 이미지** 규칙을 작동하면 **신뢰하는 업데이터** 규칙은 중지됩니다. 모든 사용자가 이 규칙의 작동 조건을 충족하는 애플리케이션을 시작할 수 있습니다.

   선택한 모드에서 만들어진 모든 규칙은 모드를 변경한 후에도 저장되므로 규칙을 다시 사용할 수 있습니다. 다시 이 규칙을 사용하려면 **애플리케이션 시작 제어 모드** 드롭다운 목록에서 원하는 모드를 선택하기만 하면 됩니다.
5. **처리** 드롭다운 목록에서 사용자가 애플리케이션 시작 제어 규칙에 의해 차단된 애플리케이션을 시작하려고 시도할 때 구성요소에서 수행할 처리 방법을 선택합니다.
6. 사용자가 애플리케이션을 시작할 때 Kaspersky Endpoint Security에서 DLL 모듈 로딩을 모니터링하려면 **DLL 및 드라이버 감시** 확인란을 선택합니다.
   모듈 및 모듈을 로드한 애플리케이션에 대한 정보가 리포트에 저장됩니다.
   확인란을 선택하면 Kaspersky Endpoint Security를 시작하기 전에 DLL 모듈 및 드라이버가 모니터링됩니다. 이후 애플리케이션 시작 전에 모든 DLL 모듈 및 드라이버 모니터링을 구성하려면 **DLL 및 드라이버 감시** 확인란을 선택한 후 컴퓨터를 다시 시작합니다. **DLL 및 드라이버 감시** 확인란을 선택한 후 컴퓨터를 다시 시작할 수 없으면 Kaspersky Endpoint Security가 실행 중일 때 DLL 모듈 및 드라이버를 로드할 수 있습니다. 이 경우 Kaspersky Endpoint Security가 실행 중일 때 로드된 DLL 모듈 및 드라이버에 한해 모니터링 기능이 유효합니다.

   DLL 모듈 및 드라이버를 모니터링할 때는 KL 카테고리를 기준으로 작성된 애플리케이션 시작 제어 규칙을 사용하지 않는 것이 좋습니다. DLL 모듈 및 드라이버의 KL 카테고리 결정("운영 체제 및 그 구성요소" 규칙에 포함)이 제대로 작동하지 않을 수 있습니다. 특히 "운영 체제 및 그 구성요소" 규칙이 기본적으로 생성되지만 DLL 모듈 및 드라이버 실행 시 배포되지 않습니다. 이 기능을 켜면 DLL 모듈 및 드라이버에 대해 별도의 허락 규칙을 만들어야 합니다. 그러한 허락 규칙이 없는 상태에서 **DLL 및 드라이버 제어** 기능을 사용하면 시스템이 불안정해질 수 있습니다.

Kaspersky Security Center 정책 설정을 변경하지 않으면서도 중요한 DLL 모듈 및 드라이버의 실행을 차단하는 허용 규칙을 해제할 수 있도록 프로그램 설정을 구성하려면 암호 보호를 설정하는 것이 좋습니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

Kaspersky Security Center를 사용해 애플리케이션 시작 제어 규칙 관리

이 섹션에는 Kaspersky Security Center를 이용해 애플리케이션 시작 제어 규칙 구성에 대한 정보가 포함되어 있으며 애플리케이션 시작 제어의 최적 사용을 위한 권장 사항을 알려줍니다.

사용자 컴퓨터에 설치된 애플리케이션에 대한 정보 수집

최적의 애플리케이션 시작 제어 규칙을 만들려면 먼저 LAN 네트워크의 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.

기업 LAN에 있는 컴퓨터에서 사용되는 애플리케이션에 대한 정보는 **자산 관리(소프트웨어)** 폴더 및 **실행 파일** 폴더에서 사용할 수 있습니다. **자산 관리(소프트웨어)** 폴더와 **실행 파일** 폴더는 Kaspersky Security Center 관리 콘솔 트리에서 **애플리케이션 관리** 폴더에 있습니다.

자산 관리(소프트웨어) 폴더에는 클라이언트 컴퓨터에 설치된 네트워크 에이전트에서 탐지된 애플리케이션 목록이 포함됩니다.

실행 파일 폴더에는 클라이언트 컴퓨터에서 시작되거나 Kaspersky Endpoint Security의 인벤토리 작업 중에 탐지된 모든 실행 파일의 목록이 포함됩니다.

애플리케이션과 그 실행 파일에 대한 일반적인 정보 및 해당 애플리케이션이 설치된 컴퓨터의 목록을 보려면 **애플리케이션 레지스트리** 폴더 또는 **실행 파일** 폴더에서 애플리케이션을 선택한 후 속성 창을 엽니다.

애플리케이션 카테고리 만들기

좀 더 쉽게 규칙을 만들려면 애플리케이션 카테고리를 만들어서 애플리케이션 시작 제어 규칙을 만들 때 그러한 카테고리를 사용합니다.

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.

애플리케이션 카테고리를 만들려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리에서 **고급 → 애플리케이션 관리 → 애플리케이션 카테고리** 폴더를 선택합니다.

3. 작업 공간에서 **카테고리 만들기** 버튼을 누릅니다.
   사용자 카테고리 생성 마법사가 시작됩니다.

4. 사용자 카테고리 생성 마법사의 안내를 따릅니다.

Kaspersky Security Center를 사용해 애플리케이션 시작 제어 규칙 만들기

Kaspersky Security Center를 사용해 애플리케이션 시작 제어 규칙을 만들려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 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. 필요한 정책을 선택합니다.

5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:

   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

6. **엔드포인트 제어** 섹션에서 **애플리케이션 시작 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 시작 제어 구성요소의 설정이 표시됩니다.

7. **추가** 버튼을 누릅니다.
   애플리케이션 시작 제어 규칙 창이 열립니다.

8. **카테고리** 드롭다운 목록에서 규칙을 만들 때 기준으로 사용하도록 만든 애플리케이션 카테고리를 선택합니다.

9. 선택된 카테고리의 애플리케이션을 시작하도록 권한을 구성하고 싶은 사용자 또는 사용자 그룹의 목록을 지정합니다. 그러려면 **대상자 및 그 권한** 표에서 **추가** 버튼을 누릅니다.
   Microsoft Windows의 표준 **사용자 또는 그룹 선택** 창이 열립니다. 이 창에서는 사용자 또는 사용자 그룹을 선택할 수 있습니다.

10. **대상자 및 그 권한** 표에서 다음을 수행합니다:

    - 사용자 및/또는 사용자 그룹이 선택한 카테고리에 속한 애플리케이션을 시작하도록 허락하려면 그러한 사용자 옆의 **허락** 확인란을 선택합니다.
    - 사용자 및/또는 사용자 그룹이 선택한 카테고리에 속한 애플리케이션을 시작하지 못하게 차단하려면 그러한 사용자 옆의 **차단** 확인란을 선택합니다.

11. **대상자** 열에 표시되지 않고 **대상자** 열에 지정된 사용자 그룹에 속하지 않은 일부 사용자가 선택한 카테고리에 속한 애플리케이션을 시작하지 못하게 차단하려면 **다른 사용자는 거부** 확인란을 선택합니다.

12. Kaspersky Endpoint Security에서 규칙에서 지정된 카테고리의 애플리케이션을 신뢰하는 업데이트로 간주하고 애플리케이션 시작 제어 규칙이 지정되지 않은 다른 애플리케이션을 시작하도록 허락하려면 **신뢰하는 업데**

이트 확인란을 선택합니다.

13. **확인**을 누릅니다.

14. 정책 속성 창의 **애플리케이션 시작 제어** 섹션에서 **적용** 버튼을 누릅니다.

Kaspersky Security Center를 사용해 애플리케이션 시작 제어 규칙의 상태 변경

애플리케이션 시작 제어 규칙의 상태를 변경하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 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. 필요한 정책을 선택합니다.

5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:

   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

6. **엔드포인트 제어** 섹션에서 **애플리케이션 시작 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 시작 제어 구성요소의 설정이 표시됩니다.

7. 변경할 애플리케이션 시작 제어 규칙의 상태를 선택합니다.

8. **상태** 열에서는 다음 중 하나를 수행합니다:

   - 규칙 사용을 활성화하려면 규칙 옆의 확인란을 선택합니다.
   - 규칙 사용을 비활성화하려면 규칙 옆의 확인란을 선택 취소합니다.

9. **적용** 버튼을 누릅니다.

애플리케이션 권한 제어

이 구성요소는 Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성요소는 Kaspersky Endpoint Security가 파일 서버용 Microsoft servers에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

이 섹션에는 애플리케이션 권한 제어에 대한 정보와 해당 구성요소 설정을 구성하는 방법에 대한 지침이 나와 있습니다.

애플리케이션 권한 제어 정보

애플리케이션 권한 제어는 애플리케이션이 운영 체제에 위험할 수 있는 작업을 수행하지 못하게 하고 운영 체제 리소스 및 중요한 데이터에 대한 접근을 제어합니다.

이 구성요소는 *애플리케이션 제어 규칙*을 사용하여 보호되는 리소스(파일 및 폴더, 레지스트리 키 등)에 대한 접근을 비롯한 애플리케이션의 활동을 제어합니다. 애플리케이션 제어 규칙은 운영 체제에 설치된 애플리케이션의 다양한 활동 및 컴퓨터 리소스에 대한 접근 권한에 적용되는 일련의 제한들입니다.

애플리케이션의 네트워크 활동은 방화벽 구성요소에 의해 감시됩니다.

애플리케이션을 처음으로 시작하면 애플리케이션 권한 제어가 애플리케이션을 검사한 후 신뢰 그룹에 놓습니다. 신뢰 그룹은 애플리케이션 활동을 제어할 때 Kaspersky Endpoint Security가 적용하는 애플리케이션 제어 규칙을 정의합니다.

애플리케이션 권한 제어가 보다 효과적으로 작동하도록 Kaspersky Security Network에 참여할 것을 권장합니다. Kaspersky Security Network를 통해 수집된 데이터를 이용하여 애플리케이션을 보다 정확하게 그룹으로 분류하고 최적의 애플리케이션 제어 규칙을 적용할 수 있습니다.

다음 번 애플리케이션을 시작할 때 애플리케이션 권한 제어가 애플리케이션의 무결성을 확인합니다. 애플리케이션에 변화가 없으면 구성요소가 애플리케이션에 현재 애플리케이션 제어 규칙을 적용합니다. 애플리케이션이 수정되었으면 애플리케이션 권한 제어가 애플리케이션을 처음으로 시작하는 것처럼 다시 검사합니다.

오디오 및 비디오 장치 제어 제한

오디오 스트림 보호 정보

오디오 스트림 보호에 대해 다음 특별 고려 사항이 있습니다:

- 이 기능이 작동하려면 애플리케이션 권한 제어를 사용하도록 설정해야 합니다.
- 애플리케이션 권한 제어 구성요소를 시작하기 전에 애플리케이션이 오디오 스트림 수신을 시작한 경우 Kaspersky Endpoint Security는 해당 애플리케이션의 오디오 스트림 수신을 허락하며 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.

- 애플리케이션 제어 설정 창에서 애플리케이션의 오디오 스트림 수신을 차단하는 등 사운드 녹음 장치에 대한 애플리케이션 접근 설정을 변경한 후에는 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 Security 설치 및 업그레이드 동안 오디오 및 비디오 장치 작동 특별 고려 사항

Kaspersky Endpoint Security를 설치한 후 오디오 녹음/비디오 녹화 또는 재생 애플리케이션을 처음으로 실행하면 오디오 녹음/비디오 녹화 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.

애플리케이션의 웹캠 접근 정보

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 장치**로 표시되는 USB 또는 IEEE1394를 통해 연결된 웹캠만 제어합니다.

지원되는 웹캠

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.

애플리케이션 권한 제어 작동 및 중지

기본적으로 애플리케이션 권한 제어는 작동되며, Kaspersky 전문가가 권장하는 모드에서 실행됩니다. 필요할 경우 애플리케이션 권한 제어를 중지할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

메인 애플리케이션 창의 보호 및 제어 탭에서 애플리케이션 권한 제어를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **엔드포인트 제어** 섹션을 누릅니다.
   엔드포인트 제어 섹션이 열립니다.
4. 마우스 오른쪽 버튼을 눌러 애플리케이션 권한 제어 구성요소 정보가 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
   구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.
5. 다음 중 하나를 수행합니다:
   - 애플리케이션 권한 제어를 작동하려면 **시작**을 선택합니다.
     애플리케이션 시작 제어 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.
   - 애플리케이션 권한 제어 구성요소를 중지하려면 **중지**를 선택합니다.
     애플리케이션 시작 제어 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 애플리케이션 권한 제어를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. 창 오른쪽에서 다음 중 하나를 수행합니다:
   - 애플리케이션 권한 제어를 작동하려면 **애플리케이션 권한 제어 작동** 확인란을 선택합니다.
   - 애플리케이션 권한 제어를 중지하려면 **애플리케이션 권한 제어 작동** 확인란의 선택을 취소합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 제어 그룹 관리

각 애플리케이션이 처음 시작될 때 애플리케이션 권한 제어 구성요소는 애플리케이션 보안을 확인하고 애플리케이션을 신뢰 그룹에 지정합니다.

Kaspersky Endpoint Security는 애플리케이션을 검사할 때 먼저 포함된 알려진 애플리케이션 데이터베이스에서 해당 애플리케이션 항목을 검색하고 동시에 Kaspersky Security Network 데이터베이스(인터넷이 연결된 경우)에 요청을 보냅니다. 내부 데이터베이스 및 Kaspersky Security Network 데이터베이스의 검색 결과를 기준으로 애플리케이션이 제어 그룹에 지정됩니다. 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 할당할 제어 그룹을 선택할 수 있습니다. Kaspersky Endpoint Security 이전에 시작한 애플리케이션은 **제어 그룹 선택** 창에서 지정한 제어 그룹으로 자동으로 이동합니다.

구성요소는 방화벽 설정에 설정된 네트워크 규칙에 따라 Kaspersky Endpoint Security 이전에 시작한 애플리케이션의 네트워크 활동만 제어합니다.

제어 그룹에 애플리케이션을 지정하는 설정 구성

Kaspersky Security Network 참여가 활성화된 후 Kaspersky Endpoint Security는 애플리케이션을 시작할 때마다 KSN에 애플리케이션 평판에 대한 쿼리를 전송합니다. KSN의 응답을 근거로 애플리케이션 권한 제어 설정에 지정된 것과 달리 애플리케이션을 신뢰 그룹으로 이동할 수 있습니다.

애플리케이션을 제어 그룹에 지정하는 설정을 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.

   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. 디지털로 서명한 신뢰하는 공급 업체의 애플리케이션을 제어 그룹에 자동으로 지정하는 경우, **디지털 서명이 있는 애플리케이션은 신뢰** 확인란을 선택합니다.

   *신뢰하는 공급 업체*는 Kaspersky에서 신뢰하는 그룹에 포함된 소프트웨어 공급 업체입니다. 공급 업체 인증서를 신뢰하는 시스템 인증서 저장소에 직접 추가할 수도 있습니다.
4. 알 수 없는 애플리케이션이 신뢰 그룹에 할당되는 방식을 다음 중 선택합니다:

   - 알 수 없는 애플리케이션을 신뢰 그룹에 할당하는 데 휴리스틱 분석을 사용하려면 **그룹을 지정할 때 휴리스틱 분석 사용** 옵션을 선택하고 **그룹 정의 최대 소요 시간** 필드에서 시작 애플리케이션을 검사하는 데 할당할 시간을 지정합니다.
   - 알 수 없는 모든 애플리케이션을 지정된 신뢰 그룹에 할당하는 경우 **다음 그룹으로 자동 지정** 옵션을 선택한 다음 드롭다운 목록에서 적절한 신뢰 그룹을 선택합니다.

보안을 위해 **신뢰함** 그룹은 **다음 그룹으로 자동 지정** 설정 값에 포함되지 않습니다.

5. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

제어 그룹 수정

애플리케이션이 처음 시작되면 Kaspersky Endpoint Security는 자동으로 애플리케이션을 제어 그룹에 지정합니다. 필요한 경우 수동으로 애플리케이션을 다른 제어 그룹으로 이동할 수 있습니다.

Kaspersky 전문가는 자동으로 할당된 제어 그룹의 애플리케이션을 다른 제어 그룹으로 이동하는 것을 권장하지 않습니다. 대신, 필요한 경우에는 개별 애플리케이션에 대한 규칙을 편집할 수 있습니다.

처음 시작되었을 때 Kaspersky Endpoint Security가 애플리케이션을 자동으로 할당한 제어 그룹을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. **애플리케이션** 버튼을 누릅니다.
   애플리케이션 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.
4. **애플리케이션 제어 규칙** 탭에서 관련 애플리케이션을 선택합니다.
5. 다음 중 하나를 수행합니다:
   - 마우스 오른쪽 버튼을 눌러 애플리케이션의 마우스 오른쪽 메뉴를 표시합니다. 애플리케이션의 마우스 오른쪽 메뉴에서 **그룹으로 이동** → <그룹 이름>을 선택합니다.
   - **신뢰함/낮은 제한/높은 제한/신뢰하지 않음** 링크를 눌러 마우스 오른쪽 메뉴를 엽니다. 마우스 오른쪽 메뉴에서 필요한 제어 그룹을 선택합니다.
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

Kaspersky Endpoint Security보다 먼저 시작된 애플리케이션에 대한 제어 그룹 선택

구성요소는 Kaspersky Endpoint Security 이전에 시작한 애플리케이션의 네트워크 활동만 제어합니다. 방화벽 설정에 지정된 네트워크 규칙에 따라 제어가 수행됩니다. 그러한 애플리케이션을 모니터링하는 네트워크 활동에 적용해야 하는 네트워크 규칙을 지정하려면 제어 그룹을 선택해야 합니다.

Kaspersky Endpoint Security 이전에 시작한 애플리케이션에 대한 제어 그룹을 선택하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. **편집** 버튼을 누릅니다.
   제어 그룹 선택 창이 열립니다.
4. 원하는 제어 그룹을 선택합니다.
5. **확인**을 누릅니다.
6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 제어 규칙 관리

기본적으로 애플리케이션 동작은 Kaspersky Endpoint Security가 처음 실행 시 애플리케이션을 할당한 신뢰 그룹에 대해 정의된 애플리케이션 제어 규칙에 따라 제어됩니다. 필요한 경우 전체 신뢰 그룹, 개별 애플리케이션 또는 신뢰 그룹에 속한 애플리케이션 그룹에 대해 애플리케이션 제어 규칙을 편집할 수 있습니다.

개별 애플리케이션 또는 신뢰 그룹에 속한 애플리케이션 그룹에 대해 정의된 애플리케이션 제어 규칙이 신뢰 그룹에 대해 정의된 애플리케이션 제어 규칙보다 우선합니다. 다시 말해 개별 애플리케이션 또는 신뢰 그룹에 속한 애플리케이션 그룹에 대한 애플리케이션 제어 규칙 설정이 신뢰 그룹에 대한 애플리케이션 제어 규칙 설정과 다른 경우, 애플리케이션 권한 제어 구성요소는 개별 애플리케이션 또는 애플리케이션 그룹에 대한 애플리케이션 제어 규칙에 따라 애플리케이션 또는 신뢰 그룹에 속한 애플리케이션 그룹의 동작을 제어합니다.

제어 그룹 및 애플리케이션 그룹에 대한 애플리케이션 제어 규칙 변경

각 신뢰 그룹별로 최적의 애플리케이션 제어 규칙은 기본적으로 생성되어 있습니다. 애플리케이션 그룹 제어 규칙 설정은 제어 그룹 제어 규칙 설정의 값을 상속합니다. 사전 설정된 제어 그룹 제어 규칙 및 애플리케이션 그룹 제어 규칙을 편집할 수 있습니다.

제어 그룹 제어 규칙 또는 애플리케이션 그룹 제어 규칙을 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. **애플리케이션** 버튼을 누릅니다.
   그러면 **애플리케이션 권한 제어** 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.
4. 원하는 제어 그룹 또는 애플리케이션 그룹을 선택합니다.
5. 제어 그룹 또는 애플리케이션 그룹의 마우스 오른쪽 메뉴에서 **그룹 규칙**을 선택합니다.
   애플리케이션 그룹 제어 규칙 창이 열립니다.
6. **애플리케이션 그룹 제어 규칙** 창에서 다음 중 하나를 수행합니다:

- 운영 체제 레지스트리, 사용자 파일 및 애플리케이션 설정에 접근할 제어 그룹 또는 애플리케이션 그룹의 권한을 제어하는 제어 그룹 제어 규칙 또는 애플리케이션 그룹 제어 규칙을 편집하려면 **파일 및 시스템 레지스트리** 탭을 선택합니다.
- 운영 체제 프로세스 및 개체에 접근할 제어 그룹 또는 애플리케이션 그룹의 권한을 제어하는 제어 그룹 제어 규칙 또는 애플리케이션 그룹 제어 규칙을 편집하려면 **권한** 탭을 선택합니다.

7. 리소스가 필요한 경우 해당 처리 열에서 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 엽니다.
8. 마우스 오른쪽 메뉴에서 필요한 항목을 선택합니다.
   - **상속**
   - **허용**
   - **차단**
   - **이벤트 로그**

   제어 그룹 제어 규칙을 편집하는 경우 **상속** 항목은 사용할 수 없습니다.
9. **확인**을 누릅니다.
10. **애플리케이션** 창에서 **확인**을 누릅니다.
11. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 제어 규칙 편집

기본적으로 애플리케이션 그룹 또는 제어 그룹에 속하는 애플리케이션의 제어 규칙 설정은 제어 그룹 제어 규칙 설정에서 값을 상속합니다. 애플리케이션 제어 규칙 설정은 편집할 수 있습니다.

애플리케이션 제어 규칙을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. **애플리케이션** 버튼을 누릅니다.
   그러면 **애플리케이션 권한 제어** 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.
4. 필요한 애플리케이션을 선택합니다.
5. 다음 중 하나를 수행합니다:
   - 애플리케이션의 마우스 오른쪽 메뉴에서 **애플리케이션 규칙**을 선택합니다.
   - **애플리케이션 제어 규칙** 탭의 오른쪽 하단에서 **고급** 버튼을 누릅니다.

   애플리케이션 제어 규칙 창이 열립니다.

6. **애플리케이션 제어 규칙** 창에서 다음 중 하나를 수행합니다:

   - 운영 체제 레지스트리, 사용자 파일 및 애플리케이션 설정에 접근할 권한을 제어하는 애플리케이션 제어 규칙을 편집하려면 **파일 및 시스템 레지스트리** 탭을 선택합니다.

   - 운영 체제 프로세스 및 개체에 접근할 권한을 제어하는 애플리케이션 제어 규칙을 편집하려면 **권한** 탭을 선택합니다.

7. 리소스가 필요한 경우 해당 처리 열에서 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 엽니다.

8. 마우스 오른쪽 메뉴에서 필요한 항목을 선택합니다.

   - **상속**

   - **허용**

   - **차단**

   - **이벤트 로그**

9. **확인**을 누릅니다.

10. **애플리케이션** 창에서 **확인**을 누릅니다.

11. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

Kaspersky Security Network 데이터베이스에서 애플리케이션 제어 규칙 다운로드 및 업데이트 중지하기

기본적으로 Kaspersky Security Network 데이터베이스에서 애플리케이션에 대한 새로운 정보가 검색되면 Kaspersky Endpoint Security가 KSN 데이터베이스에서 다운로드한 제어 규칙을 이 애플리케이션에 적용합니다. 그런 다음 사용자가 직접 애플리케이션의 제어 규칙을 편집할 수 있습니다.

애플리케이션이 처음 시작되었을 때 Kaspersky Security Network 데이터베이스에는 없었지만 관련 정보가 데이터베이스에 추가된 경우 기본적으로 Kaspersky Endpoint Security는 해당 애플리케이션에 대한 제어 규칙을 자동으로 업데이트합니다.

Kaspersky Security Network 데이터베이스의 애플리케이션 제어 규칙 다운로드 및 이전에 알려지지 않은 애플리케이션 제어 규칙의 자동 업데이트를 중지할 수 있습니다.

Kaspersky Security Network 데이터베이스에서 애플리케이션 제어 규칙의 다운로드 및 업데이트를 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.

3. **KSN에 등록 안 된 새로운 애플리케이션에 대한 제어 규칙 업데이트** 확인란의 선택을 취소합니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

부모 프로세스의 제한 설정 상속 중지

애플리케이션은 사용자 또는 실행 중인 다른 애플리케이션에 의해 시작될 수 있습니다. 애플리케이션이 다른 애플리케이션에 의해 시작된 경우 부모 프로세스와 자식 프로세스로 구성된 시작 순서가 생성됩니다.

애플리케이션에서 보호되는 리소스에 접근하려고 시도하는 경우 애플리케이션 권한 제어는 애플리케이션의 모든 부모 프로세스를 분석하여 해당 프로세스에 보호되는 리소스 접근 권한이 있는지 여부를 확인합니다. 최소 우선 순위 규칙 적용: 이 애플리케이션의 접근 권한을 부모 프로세스의 접근 권한과 비교할 때 최소 우선 순위 접근 권한이 애플리케이션의 활동에 적용됩니다.

접근 권한의 우선 순위는 다음과 같습니다:

1. **허용** 이 접근 권한의 우선 순위가 가장 높습니다.
2. **차단** 이 접근 권한의 우선 순위가 가장 낮습니다.

이 메커니즘은 신뢰하지 않는 애플리케이션 또는 권한이 제한된 애플리케이션이 신뢰하는 애플리케이션을 사용하여 특정 권한이 필요한 작업을 수행할 수 없도록 합니다.

부모 프로세스의 권한이 부족해 애플리케이션의 활동이 차단될 경우 이 권한을 편집하거나 부모 프로세스에서 제한 사항을 상속받지 않도록 할 수 있습니다.

부모 프로세스의 제한 설정을 상속받지 않도록 하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. **애플리케이션** 버튼을 누릅니다.
   그러면 **애플리케이션 권한 제어** 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.
4. 필요한 애플리케이션을 선택합니다.
5. 애플리케이션의 마우스 오른쪽 메뉴에서 **애플리케이션 규칙**을 선택합니다.
   애플리케이션 제어 규칙 창이 열립니다.
6. **애플리케이션 제어 규칙** 창에서 **예외** 탭을 선택합니다.
7. **부모 프로세스(애플리케이션)의 제한을 상속하지 않음** 확인란을 선택합니다.
8. **확인**을 누릅니다.
9. **애플리케이션** 창에서 **확인**을 누릅니다.
10. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 제어 규칙에서 특정 애플리케이션 동작 예외

애플리케이션 제어 규칙에서 특정 애플리케이션 동작을 예외 시키려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. **애플리케이션** 버튼을 누릅니다.
   그러면 **애플리케이션 권한 제어** 창에서 **애플리케이션 제어 규칙** 탭이 열립니다.
4. 필요한 애플리케이션을 선택합니다.
5. 애플리케이션의 마우스 오른쪽 메뉴에서 **애플리케이션 규칙**을 선택합니다.
   애플리케이션 제어 규칙 창이 열립니다.
6. **예외** 탭을 선택합니다.
7. 감시할 필요가 없는 애플리케이션 동작 옆의 확인란을 선택합니다.
8. **확인**을 누릅니다.
9. **애플리케이션** 창에서 **확인**을 누릅니다.
10. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

오래된 애플리케이션 제어 규칙 삭제

기본적으로 60일 동안 시작되지 않은 애플리케이션에 대한 제어 규칙은 자동으로 삭제됩니다. 그러나 사용되지 않는 애플리케이션에 대한 제어 규칙의 저장 기간은 변경할 수 있을 뿐만 아니라 규칙의 자동 삭제 기능을 중지할 수도 있습니다.

오래된 애플리케이션 제어 규칙을 삭제하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - Kaspersky Endpoint Security에서 시작하지 않는 애플리케이션의 제어 규칙을 삭제하도록 하려면, **다음 기간 이상 사용 안 한 애플리케이션은 규칙에서 삭제** 확인란을 선택하고 해당 기간을 지정합니다.
   - 사용되지 않는 애플리케이션의 제어 규칙이 자동으로 삭제되지 않도록 하려면 **다음 기간 이상 사용 안 한 애플리케이션은 규칙에서 삭제** 확인란의 선택을 취소합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

운영 체제 리소스 및 중요한 데이터 보호

애플리케이션 권한 제어는 다양한 종류의 운영 체제 리소스 및 중요한 데이터를 대상으로 동작을 수행할 수 있는 애플리케이션 권한을 관리합니다.

Kaspersky 전문가가 지정한 보호되는 리소스 카테고리가 사전 설정되어 있습니다. 사전 설정된 보호되는 리소스 카테고리 및 이 카테고리에 속하는 보호되는 리소스는 편집하거나 삭제할 수 없습니다.

다음과 같은 작업을 수행할 수 있습니다:

- 새 보호되는 리소스 카테고리를 추가합니다.
- 새 보호되는 리소스를 추가합니다.
- 리소스 보호를 중지합니다.

보호되는 리소스의 카테고리 추가

새로운 보호되는 리소스 카테고리를 추가하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. **리소스** 버튼을 누릅니다.
   그러면 **애플리케이션 권한 제어** 창에서 **보호되는 리소스** 탭이 열립니다.
4. **보호되는 리소스** 탭 왼쪽에서 보호되는 리소스 카테고리를 새로 추가해 넣을 보호되는 리소스 카테고리 또는 섹션을 선택합니다.
5. **추가** 버튼을 누르고 드롭다운 목록에서 **카테고리**를 선택합니다.
   보호되는 리소스 카테고리 창이 열립니다.
6. **보호되는 리소스 카테고리** 창에서 새로운 보호되는 리소스 카테고리의 이름을 입력합니다.
7. **확인**을 누릅니다.
   보호되는 리소스 카테고리 목록에 새 항목이 나타납니다.
8. **애플리케이션 권한 제어** 창에서 **확인**을 누릅니다.
9. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

보호되는 리소스 카테고리를 추가한 후, 보호되는 리소스 탭 상단 왼쪽에 있는 **편집** 또는 **제거** 버튼을 눌러 **보호되는 리소스** 탭을 편집하거나 제거할 수 있습니다.

보호되는 리소스 추가

보호되는 리소스를 추가하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. **리소스** 버튼을 누릅니다.
   그러면 **애플리케이션 권한 제어** 창에서 **보호되는 리소스** 탭이 열립니다.
4. **보호되는 리소스** 탭 왼쪽에서 보호되는 리소스를 새로 추가해 넣을 카테고리를 선택합니다.
5. **추가** 버튼을 누르고 드롭다운 목록에서 추가할 리소스 유형을 선택합니다:
   - **파일 또는 폴더**.
   - **레지스트리 키**.

   보호되는 리소스 창이 열립니다.
6. **보호되는 리소스** 창에서 **이름** 필드에 보호되는 리소스 이름을 입력합니다.
7. **찾아보기** 버튼을 누릅니다.
8. 창이 열리면 추가할 보호되는 리소스의 유형에 따라 필요한 설정을 지정합니다. **확인**을 누릅니다.
9. **보호되는 리소스** 창에서 **확인**을 누릅니다.
   보호되는 리소스 탭에서 선택된 카테고리의 보호되는 리소스 목록에 새 항목이 표시됩니다.
10. **애플리케이션 권한 제어** 창에서 **확인**을 누릅니다.
11. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

보호되는 리소스를 추가한 후, 보호되는 리소스 탭 상단 왼쪽에 있는 **편집** 또는 **제거** 버튼을 눌러 **보호되는 리소스** 탭을 편집하거나 제거할 수 있습니다.

리소스 보호 중지

리소스 보호를 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **애플리케이션 권한 제어** 서브 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 권한 제어 구성요소의 설정이 표시됩니다.
3. 창 오른쪽에서 **리소스** 버튼을 누릅니다.
   그러면 **애플리케이션 권한 제어** 창에서 **보호되는 리소스** 탭이 열립니다.
4. 다음 중 하나를 수행합니다:
   - 탭 왼쪽의 보호되는 리소스 목록에서 보호를 중지하려는 리소스를 선택하고 그 이름 옆에 있는 확인란을 선택 취소합니다.

- **예외**를 누르고 다음과 같이 하십시오:

  a. **예외** 창에서 **추가** 버튼을 누릅니다. 드롭다운 메뉴에서 애플리케이션 권한 제어 구성요소에 의한 보호에서 예외시킬 목록에 추가할 리소스 유형을 선택합니다: **파일 또는 폴더** / **레지스트리 키**.

  보호되는 리소스 창이 열립니다.

  b. **보호되는 리소스** 창에서 **이름** 필드에 보호되는 리소스 이름을 입력합니다.

  c. **찾아보기** 버튼을 누릅니다.

  d. 열리는 창에서 애플리케이션 권한 제어 구성요소에 의한 보호에서 예외시킬 목록에 추가할 보호되는 리소스 유형에 따라 필요한 설정을 지정합니다.

  e. **확인**을 누릅니다.

  f. **보호되는 리소스** 창에서 **확인**을 누릅니다.

  애플리케이션 권한 제어 구성요소에 의한 보호에서 예외시킬 리소스 목록에 새 요소가 나타납니다.

  > 애플리케이션 권한 제어 구성요소에 의한 보호에서 예외 시킬 목록에 리소스를 추가한 후, **예외** 창 상단에 있는 **편집** 또는 **제거** 버튼을 눌러 리소스를 편집하거나 제거할 수 있습니다.

  g. **예외** 창에서 **확인**을 누릅니다.

5. **애플리케이션 권한 제어** 창에서 **확인**을 누릅니다.

6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

취약점 감시

이 구성요소는 Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성요소는 Kaspersky Endpoint Security가 파일 서버용 Microsoft servers에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

이 섹션에는 취약점 모니터 정보와 구성요소의 작동 또는 중지 방법에 대한 안내가 나와 있습니다.

취약점 감시 정보

취약점 감시 구성요소는 사용자의 컴퓨터에서 실행되거나 사용자가 시작한 애플리케이션에 대해 실시간 취약점 검사를 수행합니다. 취약점 감시 구성요소가 작동되면 사용자가 직접 취약점 검사 작업을 수행할 필요가 없습니다. 사용자의 컴퓨터에 설치되어 이전에 한 번도 실행되지 않았거나 오랫동안 실행되지 않은 애플리케이션에 대해 취약점 검사 작업을 수행할 경우 매우 유용합니다.

취약점 감시 작동 및 중지

취약점 감시 구성요소는 기본적으로 중지되어 있습니다. 필요할 경우 취약점 감시를 사용할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

메인 애플리케이션 창의 보호 및 제어 탭에서 취약점 감시를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **엔드포인트 제어** 섹션을 누릅니다.
   엔드포인트 제어 섹션이 열립니다.
4. 마우스 오른쪽 버튼을 눌러 취약점 감시 구성요소 정보가 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
   구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.
5. 다음 중 하나를 수행합니다:
   - 취약점 감시를 작동하려면 **시작**을 선택합니다.
     취약점 감시 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.
   - 취약점 감시를 중지하려면 **중지**를 선택합니다.
     취약점 감시 줄 왼쪽에 표시되는 구성요소 상태 아이콘이 아이콘으로 바뀝니다.

애플리케이션 설정 창에서 취약점 감시를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **취약점 감시**를 선택합니다.
   창 오른쪽에 취약점 감시 구성요소의 설정이 표시됩니다.

3. 창 오른쪽에서 다음 중 하나를 수행합니다:

   - 사용자의 컴퓨터에서 실행되거나 사용자가 실행하는 애플리케이션에 대해 취약점을 검사하려면 **취약점 감시 사용** 확인란을 선택합니다.

   - 사용자의 컴퓨터에서 실행되거나 사용자가 실행하는 애플리케이션에 대해 취약점을 검사하지 않으려면 **취약점 감시 사용** 확인란을 선택 취소합니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

매체 제어

이 구성요소는 Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성요소는 Kaspersky Endpoint Security가 파일 서버용 Microsoft servers에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

이 섹션에는 매체 제어에 대한 정보와 해당 구성요소 설정을 구성하는 방법에 대한 지침이 나와 있습니다.

장치 제어 정보

매체 제어는 컴퓨터에 설치되어 있거나 연결된 장치에 대한 사용자 접근을 제한하여 기밀 데이터의 보안을 보장합니다:

- 데이터 저장 장치(하드 드라이브, 이동식 드라이브, 테이프 드라이브, CD/DVD 드라이브)
- 데이터 전송 도구(모뎀, 외부 네트워크 카드)
- 데이터를 하드 카피로 변환하는 장치(프린터)
- 연결 버스(이하 "버스"), 즉 장치를 컴퓨터에 연결하는 인터페이스(예: USB, FireWire 및 Infrared)

매체 제어는 *장치 접근 규칙*("접근 규칙") 및 *연결 버스 접근 규칙*("버스 접근 규칙")을 적용하여 장치에 대한 사용자 접근을 관리합니다.

매체 제어 사용 및 중지

기본적으로 매체 제어는 작동됩니다. 필요한 경우 매체 제어를 중지할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

*메인 애플리케이션 창의 **보호 및 제어** 탭에서 매체 제어를 작동 또는 중지하려면 다음과 같이 하십시오:*

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **엔드포인트 제어** 섹션을 누릅니다.
   엔드포인트 제어 섹션이 열립니다.
4. 마우스 오른쪽 버튼을 눌러 매체 제어 구성요소 정보가 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
   구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.
5. 다음 중 하나를 수행합니다:
   - 매체 제어를 작동하려면 메뉴에서 **시작**을 선택합니다.

- 매체 제어를 중지하려면 메뉴에서 **중지**를 선택합니다.

애플리케이션 설정 창에서 매체 제어를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 매체 제어 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 매체 제어를 작동하려면 **매체 제어 사용** 확인란을 선택합니다.
   - 매체 제어를 중지하려면 **매체 제어 사용** 확인란을 선택 취소합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

장치 접근 규칙 및 연결 버스 정보

장치 접근 규칙은 다음과 같은 장치 제어 구성요소의 기능을 정의하는 파라미터의 조합입니다:

- 선택한 사용자 또는 사용자 그룹에서 지정된 시간 동안 특정 유형의 장치에 접근할 수 있도록 허용.
  사용자 또는 사용자 그룹을 선택하고 장치 접근 스케줄을 지정할 수 있습니다.
- 메모리 장치의 내용을 읽을 수 있는 권한 설정.
- 메모리 장치의 내용을 편집할 수 있는 권한 설정.

기본적으로 접근 규칙은 매체 제어 구성요소의 분류에 포함되는 모든 장치 유형에 대해 생성됩니다. 각 장치 유형의 연결 버스에 대한 접근이 허용된 경우 이 규칙은 모든 사용자에게 언제든지 해당 장치에 접근할 수 있는 모든 권한을 부여합니다.

연결 버스 접근 규칙은 연결 버스에 대한 접근을 허용 또는 차단합니다.

기본적으로 매체 제어 구성요소의 분류에 포함되는 모든 연결 버스에 대해 버스 접근을 허용하는 규칙이 생성됩니다.

장치 접근 규칙 또는 연결 버스 접근 규칙은 생성하거나 삭제할 수 없고 편집만 가능합니다.

신뢰하는 장치 정보

*신뢰하는 장치*는 신뢰하는 장치 설정에 지정된 사용자가 언제든지 접근할 수 있는 모든 권한을 보유한 장치를 말합니다.

신뢰하는 장치와 관련하여 수행할 수 있는 작업은 다음과 같습니다:

- 신뢰하는 장치 목록에 장치 추가.
- 신뢰하는 장치에 접근할 수 있도록 허용된 사용자 또는 사용자 그룹 변경.
- 신뢰하는 장치 목록에서 장치 삭제.

신뢰하는 장치 목록에 장치를 추가하고 이 장치 유형에 대해 접근을 차단하거나 제한하는 접근 규칙을 생성한 경우, Kaspersky Endpoint Security는 신뢰하는 장치 목록을 확인한 후에 장치에 대한 접근 권한을 부여할지 여부를 결정합니다. 신뢰하는 장치 목록에서의 포함 여부는 접근 규칙보다 우선합니다.

장치 접근에 대한 표준 결정 사항

Kaspersky Endpoint Security는 사용자가 장치를 컴퓨터에 연결한 후 장치에 대한 접근을 허용할지 여부를 결정합니다.

장치 접근에 대한 표준 결정 사항

아니오.	초기 조건	장치 접근이 결정될 때까지 수행할 중간 단계			장치 접근 결정
		장치가 신뢰하는 장치 목록에 포함되었는지 확인	접근 규칙을 기반으로 장치 접근 테스트	버스 접근 규칙을 기반으로 버스 접근 테스트	
1	매체 제어 구성요소의 장치 분류에 없습니다.	신뢰하는 장치 목록에 포함되지 않았습니다.	접근 규칙이 없습니다.	검사 대상이 아닙니다.	접근이 허용되었습니다.
2	신뢰하는 장치입니다.	신뢰하는 장치 목록에 포함되어 있습니다.	검사 대상이 아닙니다.	검사 대상이 아닙니다.	접근이 허용되었습니다.
3	장치 접근이 허용되었습니다.	신뢰하는 장치 목록에 포함되지 않았습니다.	접근이 허용되었습니다.	검사 대상이 아닙니다.	접근이 허용되었습니다.
4	장치 접근이 버스에 따라 달라집니다.	신뢰하는 장치 목록에 포함되지 않았습니다.	접근이 버스에 따라 달라집니다.	접근이 허용되었습니다.	접근이 허용되었습니다.
5	장치 접근이 버스에 따라 달라집니다.	신뢰하는 장치 목록에 포함되지 않았습니다.	접근이 버스에 따라 달라집니다.	접근이 차단되었습니다.	접근이 차단되었습니다.
6	장치 접근이 허용되었습니다. 버스 접근 규칙이 발견되지 않았습니다.	신뢰하는 장치 목록에 포함되지 않았습니다.	접근이 허용되었습니다.	버스 접근 규칙이 없습니다.	접근이 허용되었습니다.

7	장치 접근이 차단되었습니다.	신뢰하는 장치 목록에 포함되지 않았습니다.	접근이 차단되었습니다.	검사 대상이 아닙니다.	접근이 차단되었습니다.
8	장치 접근 규칙 또는 버스 접근 규칙이 없습니다.	신뢰하는 장치 목록에 포함되지 않았습니다.	접근 규칙이 없습니다.	버스 접근 규칙이 없습니다.	접근이 허용되었습니다.
9	장치 접근 규칙이 없습니다.	신뢰하는 장치 목록에 포함되지 않았습니다.	접근 규칙이 없습니다.	접근이 허용되었습니다.	접근이 허용되었습니다.
10	장치 접근 규칙이 없습니다.	신뢰하는 장치 목록에 포함되지 않았습니다.	접근 규칙이 없습니다.	접근이 차단되었습니다.	접근이 차단되었습니다.

장치를 연결한 후에 장치 접근 규칙을 편집할 수 있습니다. 장치가 연결되어 있고 접근 규칙에 따라 접근이 허용되었지만 나중에 접근 규칙을 편집하여 접근을 차단한 경우, 다음 번에 장치에서 파일 작업(폴더 트리 보기, 읽기, 쓰기)을 요청하면 Kaspersky Endpoint Security는 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.

장치 사용 규칙 편집

장치 유형에 따라 장치 접근 권한을 얻는 사용자 목록, 접근 스케줄 및 접근 허용/차단과 같은 다양한 접근 설정을 수정할 수 있습니다.

장치 접근 규칙을 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 매체 제어 구성요소의 설정이 표시됩니다.
3. 창 오른쪽에서 **장치 유형** 탭을 선택합니다.
   장치 유형 탭에는 매체 제어 구성요소의 분류에 포함되는 모든 장치에 대한 접근 규칙이 들어 있습니다.
4. 편집할 접근 규칙을 선택합니다.
5. **편집** 버튼을 누릅니다. 이 버튼은 파일 시스템이 있는 장치 유형에만 사용할 수 있습니다.
   장치 접근 규칙 구성 창이 열립니다.
   기본적으로 장치 접근 규칙은 지정된 장치 유형에 대해 항상 모든 사용자에게 전체 접근 권한을 부여합니다. 즉 이러한 접근 규칙은 **사용자 또는 사용자 그룹** 목록의 그룹이 **모두**로 설정되어 있으며, **선택한 사용자 그룹의 접근 스케줄별 권한** 표에는 장치에 대한 접근 **기본 스케줄**이 항상으로 지정되어 있고 모든 종류의 작업을 수행할 수 있는 권한이 부여 됩니다.

6. 장치 접근 규칙의 설정을 편집하려면 다음과 같이 하십시오:

   a. **사용자 또는 사용자 그룹** 목록에서 사용자 또는 사용자 그룹을 선택합니다.

   사용자 또는 사용자 그룹 목록을 편집하려면 **추가**, **편집** 및 **제거** 버튼을 사용합니다.

   b. **선택한 사용자 그룹의 접근 스케줄별 권한** 표에서 선택한 사용자 및/사용자 그룹의 장치 사용 스케줄을 구성합니다. 이렇게 하려면 편집하고자 하는 장치 접근 규칙에서 사용할 장치 접근 스케줄의 이름 옆에 있는 확인란을 선택합니다.

   장치에 대한 접근 스케줄 목록을 편집하려면 **선택한 사용자 그룹의 접근 스케줄별 권한** 표에서 **생성**, **편집**, **복사** 및 **제거** 버튼을 사용합니다.

   c. 편집할 규칙에 사용된 장치에 대한 접근 스케줄별로 장치를 사용할 때 허용할 작업을 지정합니다. 이렇게 하려면 선택한 **선택한 사용자 그룹의 접근 스케줄별 권한** 표에서 관련 작업의 이름이 포함된 열의 확인란을 선택합니다.

   d. **확인**을 누릅니다.

   장치 접근 규칙의 기본 설정을 편집하면 **장치 유형** 탭 표의 **접근** 열에서 장치 유형에 대한 접근 설정이 *규칙으로 제한* 값으로 변경됩니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

이벤트 로그에 레코드 추가 또는 로그에서 레코드 예외

이동식 드라이브에 저장된 파일의 작업에 대해서만 이벤트 로깅을 사용할 수 있습니다.

이벤트 기록을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 매체 제어 구성요소의 설정이 표시됩니다.

3. 창 오른쪽에서 **장치 유형** 탭을 선택합니다.
   장치 유형 탭에는 매체 제어 구성요소의 분류에 포함되는 모든 장치에 대한 접근 규칙이 들어 있습니다.

4. 장치 표에서 **이동식 드라이브**를 선택합니다.
   표 위쪽의 **로그 기록** 버튼을 사용할 수 있게 됩니다.

5. **로그 기록** 버튼을 누릅니다.
   그러면 **로그 기록 설정** 창이 열립니다.

6. 다음 중 하나를 수행합니다:

   - 이동식 드라이브의 파일에 대한 삭제 및 쓰기 작업 기록을 사용하도록 설정하려면 **로그 기록 사용** 확인란을 선택합니다.

     Kaspersky Endpoint Security는 사용자가 이동식 드라이브의 파일에서 쓰기 또는 삭제 작업을 수행할 때마다 로그 파일에 이벤트를 저장하고 Kaspersky Security Center 중앙 관리 서버에 메시지를 전송합니다.

   - 또는 **로그 기록 사용** 확인란을 선택 취소합니다.

7. 기록해야 하는 작업을 지정합니다. 그렇게 하려면, 다음 중 하나를 수행합니다:

   - Kaspersky Endpoint Security가 모든 이벤트를 기록하도록 설정하려면 **모든 파일에 관한 정보 저장** 확인란을 선택합니다.
   - Kaspersky Endpoint Security가 특정 형식의 파일에 대한 정보만 기록하도록 설정하려면 **파일 형식 필터링** 섹션에서 해당 파일 형식 옆의 확인란을 선택합니다.

8. 작업을 이벤트로 기록해야 하는 Kaspersky Endpoint Security 사용자를 지정합니다. 이를 위해서는 다음과 같이 하십시오:

   a. **사용자** 섹션에서 **선택** 버튼을 누릅니다.

   Microsoft Windows의 표준 **사용자 또는 그룹 선택** 창이 열립니다.

   b. 사용자 또는 사용자 그룹을 지정하거나 목록을 편집합니다.

   사용자 섹션에 지정된 사용자가 이동식 드라이브에 있는 파일에 쓰거나 이동식 드라이브의 파일을 삭제하면 Kaspersky Endpoint Security는 그러한 작업에 대한 정보를 이벤트 로그에 저장하고 Kaspersky Security Center 중앙 관리 서버로 메시지를 전송합니다.

9. **로그 기록 설정** 창에서 **확인**을 누릅니다.

10. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

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 매체 제어 구성요소의 알림 설정에서 **파일 동작이 수행됨** 확인란을 선택해야 합니다.

신뢰하는 목록에 Wi-Fi 네트워크 추가

사용자가 회사 Wi-Fi 네트워크와 같이 안전하다고 생각되는 Wi-Fi 네트워크에 연결하도록 허용할 수 있습니다. 그러려면 신뢰하는 Wi-Fi 네트워크 목록에 네트워크를 추가해야 합니다. 매체 제어는 신뢰 목록에 지정된 네트워크를 예외한 모든 Wi-Fi 네트워크 접근을 차단합니다.

신뢰하는 목록에 Wi-Fi 네트워크를 추가하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.

   창 오른쪽에 매체 제어 구성요소의 설정이 표시됩니다.

3. 창 오른쪽에서 **장치 유형** 탭을 선택합니다.

   장치 유형 탭에는 매체 제어 구성요소의 분류에 포함되는 모든 장치에 대한 접근 규칙이 들어 있습니다.

4. **Wi-Fi** 장치 옆의 **접근** 열에서 마우스 오른쪽 버튼을 클릭하여 메뉴를 엽니다.
5. **예외를 제외하고 차단** 옵션을 선택합니다.
6. 장치 목록에서 **Wi-Fi**를 선택하고 **편집** 버튼을 누릅니다.

   신뢰하는 Wi-Fi 네트워크 창이 열립니다.

7. **추가** 버튼을 누릅니다.

   신뢰하는 Wi-Fi 네트워크 창이 열립니다.

8. **신뢰하는 Wi-Fi 네트워크** 창에서 다음을 수행합니다:

   - **네트워크 이름** 필드에 신뢰 목록에 추가할 Wi-Fi 네트워크 이름을 지정합니다.
   - **인증 유형** 드롭다운 목록에서 신뢰하는 Wi-Fi 네트워크에 연결할 때 사용할 인증 유형을 선택합니다.
   - **암호화 유형** 드롭다운 목록에서 신뢰하는 Wi-Fi 네트워크 트래픽을 안전하게 보호하는 데 사용할 암호화 유형을 선택합니다.
   - **설명** 필드에 추가된 Wi-Fi 네트워크에 대한 정보를 입력할 수 있습니다.

   Wi-Fi 네트워크의 설정이 규칙에 지정된 모든 설정과 일치하는 경우 신뢰할 수 있는 네트워크로 간주됩니다.

9. **신뢰하는 Wi-Fi 네트워크** 창에서 **확인**을 누릅니다.
10. **신뢰하는 Wi-Fi 네트워크** 창에서 **확인**을 누릅니다.

연결 버스 접근 규칙 편집

연결 버스 접근 규칙을 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 매체 제어 구성요소의 설정이 표시됩니다.
3. **연결 버스** 탭을 선택합니다.
   연결 버스 탭에는 매체 제어 구성요소에서 분류된 모든 연결 버스에 대한 접근 규칙이 표시됩니다.
4. 편집할 버스 연결 규칙을 선택합니다.
5. 다음과 같이 접근 파라미터 값을 변경합니다:
   - 연결 버스 접근을 허용하려면 **접근** 열을 눌러 마우스 오른쪽 메뉴를 열고 **허용**을 선택합니다.
   - 연결 버스 접근을 차단하려면 **접근** 열을 눌러 마우스 오른쪽 메뉴를 열고 **차단**을 선택합니다.
6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

신뢰하는 장치와 관련된 처리 방법

이 섹션에는 신뢰하는 장치와 관련된 처리 방법에 대한 정보가 포함되어 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:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 매체 제어 구성요소의 설정이 표시됩니다.
3. 창 오른쪽에서 **신뢰하는 장치** 탭을 선택합니다.
4. **선택** 버튼을 누릅니다.
   신뢰하는 장치 선택 창이 열립니다.
5. 신뢰하는 장치 목록에 추가할 장치의 이름 옆에 있는 확인란을 선택합니다.
   장치 열의 목록은 **장치 표시** 드롭다운 목록에서 선택한 값에 따라 달라집니다.
6. **선택** 버튼을 누릅니다.
   Microsoft Windows의 **사용자 또는 그룹 선택** 창이 열립니다.
7. Microsoft Windows의 사용자 또는 그룹 선택 창에서, 선택한 장치를 Kaspersky Endpoint Security에서 신뢰하는 장치로 인식하도록 할 **사용자 또는 사용자 그룹**을 지정합니다.
   Microsoft Windows의 **사용자 또는 사용자 그룹 선택** 창에서 지정한 사용자 또는 사용자 그룹의 이름이 **다음 사용자 또는 사용자 그룹에 대해 허용** 필드에 표시됩니다.
8. **신뢰하는 장치 선택** 창에서 **확인**을 누릅니다.
   매체 제어 구성요소 설정 창의 **신뢰하는 장치** 탭에 있는 표에 새로운 행이 나타나 추가된 신뢰하는 장치의 파라미터가 표시됩니다.
9. 지정한 사용자 또는 사용자 그룹의 신뢰하는 장치 목록에 추가할 각 장치에 대해 4-7단계를 반복합니다.
10. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

장치 모델 또는 ID를 기반으로 신뢰하는 목록에 장치 추가

기본적으로 신뢰하는 목록에 장치를 추가하면 해당 장치에 대한 접근 권한이 모든 사용자('누구나'사용자 그룹)에게 부여됩니다.

장치 모델 또는 ID를 기준으로 신뢰하는 목록에 장치를 추가하려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 신뢰하는 기기 목록을 생성하고 싶은 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:

- 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
- 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

6. **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.
7. 창 오른쪽에서 **신뢰하는 장치** 탭을 선택합니다.
8. **추가** 버튼을 누릅니다.
   버튼의 마우스 오른쪽 메뉴가 열립니다.
9. **추가** 버튼의 마우스 오른쪽 메뉴에서 다음 중 하나를 수행합니다:
   - 알 수 없는 고유한 ID를 가진 장치가 신뢰하는 장치 목록에 추가되도록 선택하려면 **ID로 장치 추가** 버튼을 선택합니다.
   - **모델로 장치 추가** 항목을 선택해 VID(공급업체 ID) 및 PID(제품 ID)가 알려진 신뢰하는 장치 목록에 추가합니다.
10. 열리는 창에 있는 **장치 유형** 드롭다운 목록에서 아래 표에 표시할 장치 유형을 선택합니다.
11. **새로 고침** 버튼을 누릅니다.
    그러면 **장치 유형** 드롭다운 목록에서 선택된 유형에 속하고 장치 ID 및/또는 모델이 알려져 있는 장치 목록이 표에 표시됩니다.
12. 신뢰하는 장치 목록에 추가할 장치의 이름 옆에 있는 확인란을 선택합니다.
13. **선택** 버튼을 누릅니다.
    Microsoft Windows의 **사용자 또는 그룹 선택** 창이 열립니다.
14. Microsoft Windows의 사용자 또는 그룹 선택 창에서, 선택한 장치를 Kaspersky Endpoint Security에서 신뢰하는 장치로 인식하도록 할 **사용자 또는 사용자 그룹**을 지정합니다.
    Microsoft Windows의 **사용자 또는 사용자 그룹 선택** 창에서 지정한 사용자 또는 사용자 그룹의 이름이 **다음 사용자 또는 사용자 그룹에 대해 허용** 필드에 표시됩니다.
15. **확인**을 누릅니다.
    추가된 신뢰하는 장치의 변수를 가진 라인이 **신뢰하는 장치** 탭의 표에 나타납니다.
16. **확인** 또는 **적용**을 눌러 변경사항을 저장합니다.

장치 ID의 마스크를 기반으로 신뢰하는 목록에 장치 추가

기본적으로 신뢰하는 목록에 장치를 추가하면 해당 장치에 대한 접근 권한이 모든 사용자('누구나'사용자 그룹)에게 부여됩니다.

Kaspersky Security Center 관리 콘솔에 있는 ID 마스크로만 장치를 신뢰하는 목록에 추가할 수 있습니다.

ID 마스크를 기준으로 신뢰하는 목록에 장치를 추가하려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 신뢰하는 기기 목록을 생성하고 싶은 관리 그룹의 이름을 가진 폴더를 엽니다.

3. 작업 공간에서 **정책** 탭을 선택합니다.

4. 필요한 정책을 선택합니다.

5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:

   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

6. **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.

7. 창 오른쪽에서 **신뢰하는 장치** 탭을 선택합니다.

8. **추가** 버튼을 누릅니다.
   버튼의 마우스 오른쪽 메뉴가 열립니다.

9. **추가** 버튼의 마우스 오른쪽 메뉴에서 **ID 마스크로 장치 추가** 항목을 선택합니다.
   ID 마스크로 신뢰하는 장치 추가 창을 엽니다.

10. **ID 마스크로 신뢰하는 장치 추가** 창에 있는 **마스크** 필드에 장치 ID 마스크를 입력합니다.

11. **선택** 버튼을 누릅니다.
    Microsoft Windows의 **사용자 또는 그룹 선택** 창이 열립니다.

12. Microsoft Windows의 **사용자 또는 그룹 선택** 창에서, 모델 또는 ID가 지정한 마스크와 일치하는 장치를 Kaspersky Endpoint Security에서 신뢰하는 장치로 인식하도록 할 사용자 또는 사용자 그룹을 지정합니다.
    Microsoft Windows의 **사용자 또는 사용자 그룹 선택** 창에서 지정한 사용자 또는 사용자 그룹의 이름이 **다음 사용자 또는 사용자 그룹에 대해 허용** 필드에 표시됩니다.

13. **확인**을 누릅니다.
    매체 제어 구성요소 설정 창의 **신뢰하는 장치** 탭에 있는 표에, ID 마스크를 기준으로 장치를 신뢰하는 장치 목록에 추가하기 위한 규칙 설정과 함께 선이 나타납니다.

14. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

신뢰하는 장치로의 사용자 접근 구성

기본적으로 신뢰하는 목록에 장치를 추가하면 해당 장치에 대한 접근 권한이 모든 사용자('누구나'사용자 그룹)에게 부여됩니다. 신뢰하는 장치에 대한 사용자(또는 사용자 그룹)의 접근을 구성할 수 있습니다.

신뢰하는 장치로의 사용자 접근을 구성하려면:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 매체 제어 구성요소의 설정이 표시됩니다.

3. 창 오른쪽에서 **신뢰하는 장치** 탭을 선택합니다.

4. 신뢰하는 장치 목록에서 접근 규칙을 편집하고 싶은 장치를 선택합니다.

5. **편집** 버튼을 누릅니다.

   신뢰하는 장치 접근 규칙 구성 창이 열립니다.

6. **선택** 버튼을 누릅니다.

   Microsoft Windows의 **사용자 또는 그룹 선택** 창이 열립니다.

7. Microsoft Windows의 사용자 또는 그룹 선택 창에서, 선택한 장치를 Kaspersky Endpoint Security에서 신뢰하는 장치로 인식하도록 할 **사용자 또는 사용자 그룹**을 지정합니다.

8. **확인**을 누릅니다.

   Microsoft Windows의 **사용자 또는 사용자 그룹 선택** 창에서 지정한 사용자 또는 사용자 그룹의 이름이 **신뢰하는 장치 접근 규칙 구성**의 **다음 사용자 또는 사용자 그룹에 대해 허용** 필드에 표시됩니다.

9. **확인**을 누릅니다.

10. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

신뢰하는 장치 목록에서 장치 제거

신뢰하는 장치 목록에서 장치를 제거하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.

   창 오른쪽에 매체 제어 구성요소의 설정이 표시됩니다.

3. 창 오른쪽에서 **신뢰하는 장치** 탭을 선택합니다.

4. 신뢰하는 장치 목록에서 제거할 장치를 선택합니다.

5. **제거** 버튼을 누릅니다.

6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

신뢰하는 장치 목록에서 제거한 장치에 대한 접근 여부는 Kaspersky Endpoint Security에서 장치 접근 규칙 및 연결 버스 접근 규칙을 토대로 결정합니다.

매체 제어 메시지 템플릿 편집

사용자가 차단된 장치에 접근하려고 하면 Kaspersky Endpoint Security에서는 장치에 대한 접근이 차단되었거나 해당 장치 컨텐츠의 작업이 금지되었다는 메시지가 표시됩니다. 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.

장치에 대한 접근이 차단되었거나 장치 컨텐츠 작업이 금지된 경우에 대한 메시지와 관리자에게 보낼 메시지에 대한 템플릿이 제공됩니다. 이러한 메시지 템플릿은 수정할 수 있습니다.

매체 제어 메시지의 템플릿을 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **매체 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 매체 제어 구성요소의 설정이 표시됩니다.
3. 창 오른쪽에 있는 **템플릿** 버튼을 누릅니다.
   메시지 템플릿 창이 열립니다.
4. 다음 중 하나를 수행합니다:
   - 장치에 대한 접근이 차단되었거나 장치 컨텐츠 작업이 금지된 경우에 대한 메시지의 템플릿을 수정하려면 **차단** 탭을 선택합니다.
   - LAN 관리자에게 보내는 메시지의 템플릿을 수정하려면 **관리자에게 메시지 보내기** 탭을 선택합니다.
5. 메시지 템플릿을 편집합니다. 다음 버튼을 사용할 수도 있습니다: **변수**, **기본값** 및 **링크**(이 버튼은 **차단** 탭에만 표시).
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

차단된 장치에 대한 접근 권한 획득

Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터 사용자를 위한 안내입니다.

Kaspersky Endpoint Security에서 장치에 대한 임시 접근 권한을 부여하는 기능은 Kaspersky Endpoint Security가 Kaspersky Security Center 정책에 따라 작동하는 경우에만 사용할 수 있으며, 이 기능은 해당 정책 설정에서 사용하도록 설정되어 있습니다(*Kaspersky Security Center 관리자 설명서* 참조).

매체 제어 구성요소 설정 창에서 차단된 장치에 대한 접근 권한을 얻으려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창에서 **보호 및 제어** 탭을 선택합니다.
2. **엔드포인트 제어** 섹션을 누릅니다.
   엔드포인트 제어 섹션이 열립니다.
3. 마우스 오른쪽 버튼을 눌러 매체 제어 구성요소 정보가 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
   구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.
4. **장치 접근 허용** 버튼을 누릅니다.
   장치 접근 허용 요청 창이 열립니다.
5. 연결된 장치 목록에서 접근 권한을 요청할 장치를 선택합니다.
6. **접근 허용 요청 파일 생성** 버튼을 누릅니다.
   접근 허용 요청 파일 생성 창이 열립니다.
7. **접근 허용 시간** 필드에서 장치에 접근하고자 하는 시간의 간격을 지정합니다.

8. **저장** 버튼을 누릅니다.

   Microsoft Windows 표준 **접근 허용 요청 파일 저장** 창이 열립니다.

9. Microsoft Windows의 **접근 허용 요청 파일 저장** 창에서 장치 접근 허용 요청 파일을 저장할 폴더를 선택하고 **저장** 버튼을 누릅니다.

10. 장치 접근 허용 요청 파일을 LAN 관리자에게 전달합니다.

11. LAN 관리자로부터 장치 접근 허용 키 파일을 받습니다.

12. **장치 접근 허용 요청** 창에서 **접근 허용 키 활성화** 버튼을 누릅니다.

    Microsoft Windows의 표준 **접근 허용 키 열기** 창이 열립니다.

13. Microsoft Windows의 **접근 허용 키 열기** 창에서 LAN 관리자로부터 받은 장치 접근 허용 키 파일을 선택하고 **열기**를 누릅니다.

    이 장치에 대한 접근 허용 키 활성화 창이 열리고 제공된 접근 권한에 대한 정보가 표시됩니다.

14. **이 장치에 대한 접근 허용 키 활성화** 창에서 **확인**을 누릅니다.

장치가 차단되었음을 알리는 메시지의 링크를 눌러 차단된 장치에 대한 접근 허용을 요청하려면 다음과 같이 하십시오:

1. 장치 또는 연결 버스가 차단되었음을 알리는 메시지가 표시된 창에서 **접근 허용 요청** 링크를 누릅니다.

   접근 허용 요청 파일 생성 창이 열립니다.

2. **접근 허용 시간** 필드에서 장치에 접근하고자 하는 시간의 간격을 지정합니다.

3. **저장** 버튼을 누릅니다.

   Microsoft Windows 표준 **접근 허용 요청 파일 저장** 창이 열립니다.

4. Microsoft Windows의 **접근 허용 요청 파일 저장** 창에서 장치 접근 허용 요청 파일을 저장할 폴더를 선택하고 **저장** 버튼을 누릅니다.

5. 장치 접근 허용 요청 파일을 LAN 관리자에게 전달합니다.

6. LAN 관리자로부터 장치 접근 허용 키 파일을 받습니다.

7. **장치 접근 허용 요청** 창에서 **접근 허용 키 활성화** 버튼을 누릅니다.

   Microsoft Windows의 표준 **접근 허용 키 열기** 창이 열립니다.

8. Microsoft Windows의 **접근 허용 키 열기** 창에서 LAN 관리자로부터 받은 장치 접근 허용 키 파일을 선택하고 **열기**를 누릅니다.

   이 장치에 대한 접근 허용 키 활성화 창이 열리고 제공된 접근 권한에 대한 정보가 표시됩니다.

9. **이 장치에 대한 접근 허용 키 활성화** 창에서 **확인**을 누릅니다.

장치에 대한 접근 권한이 주어지는 시간 간격은 요청한 시간의 양에 따라 달라질 수 있습니다. 장치에 대한 접근 권한은 로컬 네트워크 관리자가 장치 접근 허용 키를 생성할 때 지정한 시간 동안만 부여됩니다.

Kaspersky Security Center를 사용하여 차단된 장치에 접근하기 위한 키 만들기

잠긴 장치에 대한 사용자의 임시 접근을 허용하려면, 장치에 대한 접근 코드가 필요합니다. Kaspersky Security Center를 사용하여 접근 허용 키를 만들 수 있습니다.

차단된 장치에 대한 접근 허용 키를 만들려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 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 잠겨 있는 장치에 대한 임시 접근을 허용할 사용자의 컴퓨터를 선택합니다.
5. 컴퓨터의 마우스 오른쪽 메뉴에서 **오프라인 모드에서의 장치 및 데이터 접근 권한 부여**를 선택합니다.
   오프라인 모드에서의 장치 및 데이터 접근 권한 부여 창이 열립니다.
6. **매체 제어** 탭을 선택합니다.
7. **매체 제어** 탭에서 **찾아보기** 버튼을 누릅니다.
   Microsoft Windows 표준 **접근 허용 요청 파일 선택** 창이 열립니다.
8. **접근 허용 요청 파일 선택** 창에서 사용자로부터 받은 접근 허용 요청 파일을 선택하고 **열기** 버튼을 누릅니다.
   매체 제어에 사용자가 접근을 요청한 잠겨 있는 장치의 상세 정보가 표시됩니다.
9. **접근 허용 시간** 설정의 값을 지정합니다.
   이 설정은 잠겨 있는 장치에 대한 사용자의 접근을 허용할 기간을 지정합니다. 접근 허용 요청 파일을 생성할 때 사용자에 의해 지정된 값이 기본 값입니다.
10. **활성화 기간** 설정의 값을 지정합니다.
    이 설정은 제공된 접근 허용 키를 사용해 잠겨 있는 장치에 대한 사용자의 접근 허용 시간을 정의합니다.
11. **저장** 버튼을 누릅니다.
    Microsoft Windows 표준 **접근 허용 키 저장** 창이 열립니다.
12. 차단된 장치에 대한 접근 허용 키가 있는 파일을 저장할 대상 폴더를 선택합니다.
13. **저장** 버튼을 누릅니다.

웹 제어

이 구성요소는 Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 있습니다. 이 구성요소는 Kaspersky Endpoint Security가 파일 서버용 Microsoft servers에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

이 섹션에는 웹 제어에 대한 정보와 해당 구성요소 설정을 구성하는 방법에 대한 지침이 나와 있습니다.

웹 제어 정보

웹 제어는 웹 리소스에 대한 접근을 제한 또는 차단하여 LAN 사용자의 동작을 제어할 수 있습니다.

웹 리소스는 공통 기능이 있는 개별 웹 페이지나 여러 웹 페이지 또는 개별 웹사이트나 여러 웹사이트를 말합니다.

웹 제어는 다음과 같은 옵션을 제공합니다:

- 트래픽 감소.

  멀티미디어 파일의 다운로드나 사용자의 업무와 관련 없는 웹 리소스에 대한 접근을 제한 또는 차단하는 방법으로 트래픽을 제어할 수 있습니다.

- 웹 리소스 컨텐츠 카테고리별로 접근 제한.

  지정된 웹 리소스 카테고리에 대한 접근을 제한 또는 차단하여 트래픽을 줄이고 직원 근무시간의 악용에 따른 잠재적 손실을 줄일 수 있습니다(예: "인터넷 커뮤니케이션 미디어" 카테고리에 속한 웹사이트에 대한 접근 차단).

- 웹 리소스 접근의 중앙 집중식 제어.

  Kaspersky Security Center를 사용할 때 웹 리소스 접근에 대한 개인 및 그룹 설정을 사용할 수 있습니다.

웹 리소스 접근에 적용되는 모든 제한 및 차단은 웹 리소스 접근 규칙으로 구현됩니다.

웹 제어 사용 및 중지

기본적으로 웹 제어는 작동됩니다. 필요한 경우 웹 제어를 중지할 수 있습니다.

구성요소를 작동 또는 중지하는 방법은 다음 두 가지가 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

*메인 애플리케이션 창의 **보호 및 제어** 탭에서 웹 제어를 작동 또는 중지하려면 다음과 같이 하십시오:*

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.

3. **엔드포인트 제어** 섹션을 누릅니다.
   엔드포인트 제어 섹션이 열립니다.

4. 마우스 오른쪽 버튼을 눌러 웹 제어 구성요소 정보가 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
   구성요소에 대한 동작을 선택할 수 있는 메뉴가 열립니다.

5. 다음 중 하나를 수행합니다:

   - 웹 제어를 작동하려면 메뉴에서 **시작**을 선택합니다.
   - 웹 제어를 중지하려면 메뉴에서 **중지**를 선택합니다.

애플리케이션 설정 창에서 웹 제어를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **웹 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 웹 제어 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:

   - 웹 제어를 작동하려면 **웹 제어 사용** 확인란을 선택합니다.
   - 웹 제어를 중지하려면 **웹 제어 사용** 확인란의 선택을 취소합니다.

   웹 제어를 중지하면 Kaspersky Endpoint Security에서 웹 리소스에 대한 접근을 제어하지 않습니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

웹 리소스 컨텐츠 카테고리

웹 리소스 컨텐츠 카테고리(이하, 카테고리)에서 호스팅하는 데이터 블록을 가장 완전하게 설명하기 위해 기능과 주제별 기능을 고려하여 아래 나열된 웹 리소스 카테고리가 선택되었습니다. 카테고리가 이 목록에 나타나는 순서는 인터넷상에서 이러한 카테고리의 상대적인 중요성이나 인기도를 반영하지는 않습니다. 카테고리 이름은 임시적이며 Kaspersky 제품 및 웹 사이트용으로만 사용됩니다. 이 이름이 법률에서 암시하는 의미를 반영하는 것은 아닙니다. 하나의 웹 리소스는 한 번에 몇 가지 카테고리에 속할 수 있습니다.

성인물

이 카테고리에는 다음 유형의 웹 리소스가 포함됩니다:

- 사람 또는 사람과 비슷한 구조물의 생식기를 묘사하는 사진 또는 비디오, 사람 또는 사람과 비슷한 생물의 성관계나 자위 행위가 포함된 웹 리소스.
- 사람 또는 사람과 비슷한 구조물의 생식기, 사람 또는 사람과 비슷한 구조물의 성관계나 자위 행위를 묘사하는 문학 또는 예술 작품과 같은 텍스트 자료가 포함된 웹 리소스.
- 인간 관계의 성적인 측면을 집중적으로 논의하는 웹 리소스.

> "인터넷 통신 미디어" 카테고리와 중복됨.

- 성인물, 사람의 성행위를 현실적으로 묘사하는 컨텐츠 또는 성적인 욕구를 자극하는 예술 작품이 포함된 웹 리소스.
- 인간관계의 성적인 측면을 전문으로 다루는 개별 기사 및/또는 특별 섹션이 포함되어 있으며 고정 대상 독자를 갖춘 온라인 커뮤니티 및 공식 매스컴의 웹 리소스.
- 성 도착증을 전문으로 다루는 웹 리소스.
- 성인 화상 채팅, "폰섹스", "섹스팅"("가상 섹스")을 통해 온라인으로 제공되는 서비스 등, 성욕 자극, 성적인 서비스, 은밀한 데이트 및 성관계에 사용하는 용품을 광고 및 판매하는 웹 리소스.
- 다음 컨텐츠가 포함된 웹 리소스:
  - 과학적이고 인기 있는 테마로 성 교육을 다루는 기사 및 블로그.
  - 의학 백과사전, 특히 유성 생식에 관한 섹션.
  - 의료 기관의 자료, 특히 생식 기관의 치료에 관한 섹션.

소프트웨어, 오디오, 비디오

이 카테고리에는 개별적으로 선택할 수 있는 다음의 하위 카테고리가 포함됩니다:

- **오디오 및 비디오**.
  이 하위 카테고리에는 동영상, 스포츠 녹화방송, 콘서트, 노래, 영화 클립, 비디오, 튜토리얼 오디오 및 비디오 레코드 등의 오디오 및 비디오 컨텐츠를 배포하는 웹 리소스가 들어 있습니다.
- **토렌트**.
  이 하위 카테고리에는 크기 제한 없이 파일 공유를 목적으로 하는 토렌트 추적기 웹사이트가 포함됩니다.
- **파일 공유**.
  이 하위 카테고리에는 배포되는 파일의 실제 위치에 관계없이 파일 공유 웹사이트가 포함됩니다.

주류, 담배, 마약

이 카테고리에는 주류 또는 알코올 함유 제품, 담배 제품, 마약, 향정신성 약물 및/또는 알콜성 물질과 직간접적으로 관련된 컨텐츠가 포함된 웹 리소스가 해당됩니다.

- 이러한 물질과 이들의 소비를 위한 용품을 광고 및 판매하는 웹 리소스.

  > "전자 상거래" 카테고리와 중복됩니다.

- 마약, 향정신성 약물 및/또는 알콜성 물질을 소비 또는 생성하는 방법에 대한 웹 리소스.

> 이 카테고리에는 과학 및 의학 주제가 포함된 웹 리소스가 해당됩니다.

폭력

이 카테고리에는 사람에 대한 신체 또는 정신적 폭력 행위 또는 동물의 학대가 주제인 모든 사진, 동영상 또는 텍스트 자료가 포함된 웹 리소스가 해당됩니다.

- 사형, 고문 또는 학대 장면 및 이러한 행위에 사용되는 도구를 묘사 또는 설명하는 웹 리소스.

  > "무기, 폭약, 화공술" 카테고리와 중복됩니다.

- 사람, 동물, 상상의 동물을 학대 또는 모욕하는 장면, 살인, 싸움, 구타 또는 강간 장면을 묘사 또는 설명하는 웹 리소스.
- 자학 또는 자살 등 생명 및/또는 건강을 위협하는 행위를 선동하는 정보가 포함된 웹 리소스.
- 폭력 및/또는 학대의 용인을 정당화하거나 입증하는 정보 또는 사람이나 동물에 대한 폭력적인 행위를 선동하는 정보가 포함된 웹 리소스.
- 전쟁 희생자 및 잔혹함, 무력 분쟁, 군사 충돌, 사고, 참사, 자연재해, 산업 또는 사회적 격변 또는 인간의 고통을 특별히 사실적으로 묘사 또는 설명하는 웹 리소스.
- "총격", "전투", "대학살" 등의 폭력과 잔혹함을 다루는 브라우저 컴퓨터 게임.

  > "컴퓨터 게임" 카테고리와 중복됩니다.

무기, 폭약, 화공술

이 카테고리에 무기, 폭약 및 화공술 제품에 대한 정보가 포함된 웹 리소스가 포함됩니다:

- 무기, 폭약, 화공술 제품 제조업체 및 상점 웹 사이트.

  > "전자 상거래" 카테고리와 중복됩니다.

- 무기, 폭약, 화공술 제품의 제조업체 또는 사용을 전문으로 다루는 웹 리소스.
- 무기, 폭약, 화공술 제품에 대한 분석, 역사, 제조, 백과사전적인 자료가 포함된 웹 리소스.

> "무기"라는 용어는 사람과 동물의 생명이나 건강을 위협하고 장비와 건축물을 훼손하기 위해 설계된 장치, 물품, 수단을 의미합니다.

신성 모독

이 카테고리에는 불경스러운 언어가 사용되는 웹 리소스가 포함됩니다.

> "성인물" 카테고리와 중복됩니다.

> 이 카테고리에는 또한 연구 주제로 불경스러운 언어와 철학적인 자료를 다루는 웹 리소스가 포함됩니다.

도박, 복권, 내기

이 카테고리에는 도박과 같은 금전적인 참여가 웹 사이트 접근을 위한 의무 조건이 아님에도 사용자에게 참여를 권유하는 웹 리소스가 포함됩니다. 이 카테고리에는 다음과 같은 웹 리소스 서비스가 포함됩니다:

- 참가자들에게 금전적인 납부를 요구하는 게임.

  > "컴퓨터 게임" 카테고리와 중복됩니다.

- 돈 내기 게임.
- 복권이나 숫자 구입.
- 도박, 내기, 복권에 대한 참여를 유발하는 정보.

> "전자 상거래" 카테고리와 중복됩니다.

> 이 카테고리에는 이 카테고리에 속하는 웹 리소스를 사용자에게 활발하게 광고하는 웹 리소스뿐만 아니라 별도의 모드로 무료 참여를 제공하는 게임이 포함됩니다.

네트워크 커뮤니케이션

이 카테고리에는 사용자들이(등록 여부에 상관 없이) 관련 웹 리소스나 타 온라인 서비스의 다른 사용자에게 개인 메시지를 보내거나 특정 조건 하에 관련 웹 리소스에 컨텐츠(공개 접근이 가능하거나 제한된)를 추가할 수 있게 하는 웹 리소스가 포함됩니다. 다음 하위 카테고리를 별도로 선택할 수 있습니다:

- **채팅 및 포럼**.

  이 하위 카테고리에는 실시간 통신이 가능한 인스턴트 메시징 애플리케이션을 배포 또는 지원하기 위한 웹 리소스 외에도 특수한 웹 애플리케이션을 사용하여 다양한 주제에 대한 공개 토론장을 제공하는 웹 리소스가 포함됩니다.

- **블로그**.

  이 하위 카테고리에는 블로그 제작 및 유지 관리를 위한 유료 또는 무료 서비스를 제공하는 웹사이트인 블로그 플랫폼이 포함됩니다.

- **소셜 네트워크**.

  이 하위 카테고리에는 개인, 조직, 정부 사이에서 연락처를 구성, 표시, 관리하기 위해 설계된 웹 사이트가 들어 있으며 사용자 계정 등록이 참여 조건입니다.

- **데이트 사이트**.

  이 하위 카테고리에는 유료 또는 무료 서비스를 제공하는 다양한 소셜 네트워크 역할을 하는 웹 리소스가 포함됩니다.

  > "성인물" 및 "전자 상거래" 카테고리와 중복됩니다.

- **웹 기반 이메일**.

이 서브 카테고리에는 이메일과 관련 데이터(개인 연락처 등)가 포함된 이메일 서비스 및 메일상자 페이지의 단독 로그인 페이지가 들어 있습니다. 이 카테고리에는 이메일 서비스도 제공하는 인터넷 서비스 제공업체의 다른 웹 페이지가 포함되지 않습니다.

온라인 소매업체, 은행 및 전자 결제 시스템

이 카테고리에는 특수 목적의 웹 애플리케이션을 사용하여 현금이 아닌 금전을 온라인으로 거래하기 위해 설계된 웹 리소스가 포함되어 있습니다. 다음 하위 카테고리를 별도로 선택할 수 있습니다:

- **쇼핑몰**.

  이 하위 카테고리에는 온라인 결제를 받은 실제 상점의 프로필 및 온라인으로만 판매를 하는 상점의 웹 사이트를 포함하여 모든 상품, 제품 또는 서비스를 개인 및/또는 법적 실체에 판매하는 온라인 상점 및 온라인 경매가 들어 있습니다.

- **은행**.

  이 하위 카테고리에는 (전자) 계좌 이체, 예금, 환전, 타사 서비스 결제 등 온라인 은행 거래를 제공하는 은행의 전용 웹 페이지가 들어 있습니다.

- **결제 시스템**.

  이 하위 카테고리에는 사용자의 개인 계정에 접근을 제공하는 전자 화폐 시스템 웹 페이지가 들어 있습니다.

기술적인 측면에서 모든 종류의 은행 카드(플라스틱 또는 가상, 신용 또는 직불카드, 국내 또는 국제)와 전자 화폐를 사용하는 결제가 영향을 받을 수 있습니다. 웹 리소스는 SSL 프로토콜을 통한 데이터 전달, 3D 보안 인증의 사용 등 기술 측면을 가지고 있는지 여부에 상관 없이 이 카테고리에 속할 수 있습니다.

작업 검색

이 카테고리에는 직원들과 구직자들을 한 자리에 모으는 웹 리소스가 포함됩니다:

- 취업 사이트(헤드헌팅 회사 및/또는 직업 소개소).
- 구인정보와 일자리의 장점을 설명하는 채용 업체들의 웹 사이트.
- 채용업체들과 취업 정보 제공업체들의 구인정보를 제공하는 독립 포털.
- 특히 적극적으로 구직 활동을 하지 않는 전문가들에 대한 정보를 게시 또는 찾을 수 있게 해주는 전문적인 소셜 네트워크.

"인터넷 통신 미디어" 카테고리와 중복됨.

익명의 접근 시스템

이 카테고리에는 다음의 목적으로 특수 웹 애플리케이션을 사용하여 다른 웹 리소스의 컨텐츠를 다운로드할 때 중개 역할을 하는 웹 리소스가 포함됩니다:

- 웹 주소 또는 IP 주소에 대한 접근에 대해 LAN 관리자가 적용한 제한 무시;
- 특정 IP 주소 또는 주소 그룹(예: IP 할당 국가에서 그룹화한 IP 주소)으로부터의 HTTP 요청을 명확히 거부하는 웹 리소스에 익명으로 접근.

이 카테고리에는 상기한 목적("익명화 도구") 전용의 웹 리소스와 기술적으로 유사한 기능이 있는 웹 리소스가 모두 포함됩니다.

컴퓨터 게임

이 카테고리에는 다음과 같이 다양한 장르의 컴퓨터 게임을 전문으로 하는 웹 리소스가 포함됩니다:

- 컴퓨터 게임 개발자들의 웹 사이트.
- 컴퓨터 게임에 대해 집중적으로 토론하는 웹 리소스.

  "인터넷 통신 미디어" 카테고리와 중복됨.

- 다른 참가자들과 또는 개별적으로 온라인 게임에 참여할 수 있도록 기술적인 성능을 제공하는 웹 리소스(애플리케이션의 로컬 설치 또는 설치가 필요 없는 웹 브라우저 방식 게임).
- 게임 소프트웨어의 광고, 배포, 지원을 제공하는 웹 리소스.

  "전자 상거래" 카테고리와 중복됩니다.

종교, 종교 단체

이 카테고리에는 종교적인 이데올로기 및/또는 컬트적인 현상과 관련된 대중의 움직임, 협회, 조직에 관한 자료를 제공하는 웹 리소스가 포함됩니다.

- 국제 종교에서부터 지역의 종교 공동체까지 여러 수준의 공식적인 종교 조직들의 웹 사이트.
- 주요 종교 협회 또는 공동체로부터 분리되어 역사적으로 등장한 등록되지 않는 종교 협회 및 단체의 웹 사이트.
- 특정 창설자의 운동 등 전통적인 종교 운동과는 별개로 등장한 종교 협회 및 공동체의 웹 사이트.
- 전통적으로 다양한 종교의 대표 사이에서 협력을 추구하는 여러 종파 간 웹 사이트.
- 종교라는 주제에 대해 학문적이고 역사적이고 백과사전적인 자료를 제공하는 웹 리소스.
- 신이나 초현실적인 힘을 가진 것으로 생각되는 존재 및/또는 대상에 대한 숭배와 연관된 의식과 같이 종교적인 추종의 일부로 숭배를 자세히 묘사 또는 설명하는 웹 리소스.

뉴스 언론

이 카테고리에는 사용자가 자신만의 뉴스 리포트를 추가할 수 있는 매스미디어나 온라인 발행물에 의해 생성된 공개 뉴스 컨텐츠를 제공하는 웹 리소스가 포함됩니다:

- 공식 매스컴 웹 사이트.
- 정보의 공식 출처를 알리며 정보 서비스를 제공하는 웹 사이트.
- 다양한 공식/비공식 정보 출처에서 제공하는 뉴스 정보들을 통합해서 제공하는 웹 사이트.

- 사용자가 직접 새로운 컨텐츠를 작성하는 웹 사이트("소셜 뉴스 사이트").

  "인터넷 통신 미디어" 카테고리와 중복됨.

배너

이 카테고리에는 배너를 가진 웹 리소스가 포함됩니다. 배너 광고 정보는 사용자가 업무에 집중하는데 방해가 될 뿐 아니라 배너 다운로드는 트래픽 증가의 원인이 됩니다.

웹 리소스 접근 규칙 정보

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 구성요소에 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. 특정 카테고리의 컨텐츠 및 데이터 유형에 속하는 사용자의 웹리소스 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 구성요소의 규칙 목록이 채워집니다. 다음과 같은 두 가지 규칙이 사전 설정됩니다:

- 시나리오 및 스타일 표 규칙: 주소에 확장자가 css, js 또는 vbs인 파일 이름이 포함되어 있는 웹 리소스에 항상 접근할 수 있는 권한을 모든 사용자에게 부여합니다. 예: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- "기본 규칙": 언제든지 모든 웹 리소스에 접근할 수 있는 권한을 모든 사용자에게 부여합니다.

웹 리소스 접근 규칙과 관련된 처리 방법

웹 리소스 접근 규칙에 대해 다음과 같은 작업을 수행할 수 있습니다:

- 새 규칙 추가

- 규칙 편집
- 규칙에 우선 순위 지정

  규칙의 우선 순위는 웹 제어 구성요소의 설정 창에 있는 접근 규칙 표 내에서 이 규칙에 대한 간단한 설명이 들어 있는 행의 위치에 따라 정의됩니다. 즉, 접근 규칙 표에서 위쪽에 있는 규칙이 아래쪽에 있는 규칙보다 우선합니다.

  사용자가 접근하려고 시도하는 웹 리소스가 여러 규칙의 파라미터와 일치하는 경우 Kaspersky Endpoint Security는 우선 순위가 가장 높은 규칙에 따라 처리 방법을 수행합니다.
- 규칙 테스트.

  규칙 진단 기능을 사용하여 규칙의 일관성을 확인할 수 있습니다.
- 규칙 사용 및 중지.

  웹 리소스 접근 규칙은 활성화되거나(운영 상태: *켜짐*) 비활성화됩니다(운영 상태: *꺼짐*). 기본적으로 규칙이 생성된 후에는 규칙이 작동됩니다(운영 상태: *켜짐*). 이 규칙을 다시 중지할 수 있습니다.
- 규칙 삭제

웹 리소스 접근 규칙 추가 및 편집

웹 리소스 접근 규칙을 추가 또는 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **웹 제어** 하위 섹션을 선택합니다.

   창 오른쪽에 웹 제어 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 규칙을 추가하려면 **추가** 버튼을 누릅니다.
   - 규칙을 편집하려면 표에서 규칙을 선택하고 **편집** 버튼을 누릅니다.

   웹사이트 접근 규칙 창이 열립니다.
4. 규칙 설정을 지정 또는 편집합니다. 이를 위해서는 다음과 같이 하십시오:
   a. **이름** 필드에서 규칙 이름을 입력하거나 편집합니다.

   b. **컨텐츠 필터** 드롭다운 목록에서 필요한 옵션을 선택합니다:
      - **모든 컨텐츠**.
      - **컨텐츠 카테고리별**.
      - **데이터 유형별**.
      - **컨텐츠 카테고리 및 데이터 유형별**.

   c. **모든 컨텐츠** 이외의 옵션을 선택하면 컨텐츠 및/또는 데이터 유형 카테고리를 선택하는 섹션이 열립니다. 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.

d. **적용 대상 주소** 드롭다운 목록에서 필요한 옵션을 선택합니다:

- **모든 주소로**.
- **개별 주소로**.

e. **개별 주소로**로 옵션을 선택하면 웹 주소 목록을 만들 수 있는 섹션이 열립니다. **추가**, **편집** 및 **삭제** 버튼을 사용하여 웹 리소스 주소를 추가하고 편집할 수 있습니다.

f. **사용자 또는 그룹 지정** 확인란을 선택합니다.

g. **선택** 버튼을 누릅니다.

Microsoft Windows의 **사용자 또는 그룹 선택** 창이 열립니다.

h. 규칙에 의해 명시된 웹 리소스에 대한 접근을 허용 또는 차단할 사용자 또는 사용자 그룹의 목록을 지정하거나 편집합니다.

i. **처리** 드롭다운 목록에서 필요한 옵션을 선택합니다:

- **허용** 이 값을 선택하면 Kaspersky Endpoint Security에서 규칙의 파라미터와 일치하는 웹 리소스에 대한 접근을 허용합니다.
- **차단** 이 값을 선택하면 Kaspersky Endpoint Security에서 규칙의 파라미터와 일치하는 웹 리소스에 대한 접근을 차단합니다.
- **경고**. 이 값을 선택하면 Kaspersky Endpoint Security에서 사용자가 규칙과 일치하는 웹 리소스에 접근하려고 할 때 해당 웹 리소스가 원치 않는 것일 수 있다고 경고를 표시합니다. 사용자는 경고 메시지의 링크를 사용하여 요청한 웹 리소스에 대한 접근 권한을 얻을 수 있습니다.

j. **규칙 스케줄** 드롭다운 목록에서 필요한 스케줄의 이름을 선택하거나 선택한 규칙 스케줄을 기반으로 새 스케줄을 만듭니다. 이를 위해서는 다음과 같이 하십시오:

1. **규칙 스케줄** 드롭다운 목록 옆의 **설정** 버튼을 누릅니다.

   규칙 스케줄 창이 열립니다.

2. 규칙이 적용되지 않는 시간 간격을 규칙 스케줄에 추가하려면 규칙 스케줄이 나와 있는 표에서 선택하려는 요일 및 시간에 해당하는 셀을 누릅니다.

   그러면 해당 셀이 회색으로 바뀝니다.

3. 규칙이 적용되는 동안의 시간 간격을 규칙이 적용되지 않는 동안의 시간 간격으로 대체하려면 선택하려는 요일 및 시간에 해당하는 회색 셀을 누릅니다.

   그러면 해당 셀이 녹색으로 바뀝니다.

4. **다른 이름으로 저장** 버튼을 누릅니다.

   규칙 스케줄 이름 창이 열립니다.

5. 규칙 스케줄 이름을 입력하거나 제안된 기본 이름을 유지합니다.

6. **확인**을 누릅니다.

5. **웹사이트 접근 규칙** 창에서 **확인**을 누릅니다.

6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

웹 리소스 접근 규칙에 우선 순위 지정

규칙 목록에서 특정한 순서대로 규칙을 정렬하여 각 규칙에 우선 순위를 지정할 수 있습니다.

웹 리소스 접근 규칙에 우선 순위를 지정하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **웹 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 웹 제어 구성요소의 설정이 표시됩니다.
3. 창 오른쪽에서 우선 순위를 변경할 규칙을 선택합니다.
4. **위로 이동** 및 **아래로 이동** 버튼을 사용하여 해당 규칙을 규칙 목록에서 원하는 순위로 이동합니다.
5. 우선 순위를 변경하려는 다른 규칙에 대해서도 3-4단계를 반복합니다.
6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

웹 리소스 접근 규칙 테스트

웹 제어 규칙의 일관성을 확인하기 위해 규칙을 테스트할 수 있습니다. 이 목적으로 웹 제어 구성요소에서는 규칙 진단 기능을 제공합니다.

웹 리소스 접근 규칙을 테스트하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **웹 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 웹 제어 구성요소의 설정이 표시됩니다.
3. 창 오른쪽에 있는 **진단** 버튼을 누릅니다.
   규칙 진단 창이 열립니다.
4. **조건** 섹션의 필드를 입력합니다:
   a. Kaspersky Endpoint Security에서 특정 웹 리소스에 대한 접근을 제어하는 데 사용하는 규칙을 테스트하려면 **주소 지정** 확인란을 선택하고 아래 필드에 해당 웹 리소스의 주소를 입력합니다.
   b. Kaspersky Endpoint Security에서 특정 사용자 또는 사용자 그룹의 웹 리소스FF 접근을 제어하는 데 사용하는 규칙을 테스트하려면 사용자 또는 사용자 그룹의 목록을 지정합니다.
   c. Kaspersky Endpoint Security에서 지정된 컨텐츠 카테고리 및/또는 데이터 유형 카테고리의 웹 리소스 접근을 제어하는 데 사용하는 규칙을 테스트하려면 **컨텐츠 필터** 드롭다운 목록에서 필요한 옵션을 선택합니다 (**컨텐츠 카테고리별**, **데이터 유형별** 또는 **컨텐츠 카테고리 및 데이터 유형별**).
   d. 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.

5. **테스트** 버튼을 누릅니다.

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 **테스트** 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 규칙 사용 및 중지

웹 리소스 접근 규칙을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **웹 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 웹 제어 구성요소의 설정이 표시됩니다.
3. 창 오른쪽에서 작동하거나 중지할 규칙을 선택합니다.
4. **상태** 열에서는 다음을 수행합니다:
   - 규칙을 작동하려면 *켜짐* 값을 선택합니다.
   - 규칙 사용을 중지하려면 *꺼짐* 값을 선택합니다.
5. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션의 이전 버전에서 웹 리소스 접근 규칙 마이그레이션

Service Pack 1 Maintenance Release 1 또는 이전 버전의 애플리케이션이 Kaspersky Endpoint Security 10 Service Pack 2 for Windows로 업그레이드되면 웹 리소스 컨텐츠 카테고리에 기반한 웹 리소스 접근 규칙이 다음 원칙에 따라 마이그레이션됩니다:

- "포럼과 채팅", "웹 메일", "소셜 네트워크" 목록에 있는 하나 또는 몇 가지 웹 리소스 컨텐츠 카테고리에 기반한 웹 리소스 접근 규칙이 "인터넷 통신 미디어" 웹 리소스 컨텐츠 카테고리에 마이그레이션됩니다.
- "온라인 상점", "결제 시스템" 목록에 있는 하나 또는 몇 가지 웹 리소스 컨텐츠 카테고리에 기반한 웹 리소스 접근 규칙이 "전자 상거래" 웹 리소스 컨텐츠 카테고리에 마이그레이션됩니다.
- "게임" 웹 리소스 컨텐츠 카테고리에 기반한 웹 리소스 접근 규칙이 "게임, 복권, 내기" 컨텐츠 카테고리에 마이그레이션됩니다.
- "브라우저 게임" 웹 리소스 컨텐츠 카테고리에 기반한 웹 리소스 접근 규칙이 "컴퓨터 게임" 컨텐츠 카테고리에 마이그레이션됩니다.
- 상기한 목록에 나열되지 않은 웹 리소스 컨텐츠 카테고리에 기반한 웹 리소스 접근 규칙이 변경 없이 마이그레이션됩니다.

웹사이트 주소 목록 내보내기 및 가져오기

웹 리소스 접근 규칙에서 웹 리소스 주소 목록을 만든 경우 .txt 파일로 내보낼 수 있습니다. 이후에 접근 규칙을 구성할 때 이 파일에서 목록을 가져올 수 있으므로 수동으로 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.

웹 리소스 주소 목록을 파일로 내보내려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **웹 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 웹 제어 구성요소의 설정이 표시됩니다.
3. 파일로 내보낼 웹 리소스 주소 목록에 대한 규칙을 선택합니다.
4. **편집** 버튼을 누릅니다.
   웹사이트 접근 규칙 창이 열립니다.
5. 웹 리소스 주소 목록의 일부만 내보내려는 경우 필요한 웹 리소스 주소를 선택합니다.
6. 웹 리소스 주소 목록 필드의 오른쪽에 있는 버튼을 클릭합니다.
   그러면 처리를 확인하는 창이 열립니다.
7. 다음 중 하나를 수행합니다:
   - 웹 리소스 주소 목록에서 선택한 항목만 내보내려는 경우 처리를 확인하는 창에서 **예** 버튼을 누릅니다.
   - 웹 리소스 주소 목록의 모든 항목을 내보내려는 경우 처리를 확인하는 창에서 **아니오** 버튼을 누릅니다.
     Microsoft Office의 표준 **다른 이름으로 저장** 창이 열립니다.
8. Microsoft Windows의 **다른 이름으로 저장** 창에서 웹 리소스 주소 목록을 내보낼 파일을 선택합니다. **저장** 버튼을 누릅니다.

파일에서 웹 리소스 주소 목록을 규칙으로 가져오려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **웹 제어** 하위 섹션을 선택합니다.
   창 오른쪽에 웹 제어 구성요소의 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 웹 리소스 접근 규칙을 새로 만들려는 경우 **추가** 버튼을 누릅니다
   - 편집할 웹 리소스 접근 규칙을 선택합니다. 그런 다음 **편집** 버튼을 누릅니다.

   웹사이트 접근 규칙 창이 열립니다.
4. 다음 중 하나를 수행합니다:
   - 웹 리소스 접근 규칙을 새로 만드는 경우 **적용 대상 주소** 드롭다운 목록에서 **개별 주소로**를 선택합니다.

- 웹 리소스 접근 규칙을 편집하는 경우 이 지침의 5단계로 이동합니다.

5. 웹 리소스 주소 목록 필드의 오른쪽에 있는 버튼을 클릭합니다.

   규칙을 새로 만드는 경우 Microsoft Windows의 표준 **파일 열기** 창이 열립니다.

   규칙을 편집하는 경우 확인을 요청하는 창이 열립니다.

6. 다음 중 하나를 수행합니다:

   - 웹 리소스 접근 규칙을 새로 편집하는 경우 이 지침의 7단계로 이동합니다.
   - 웹 리소스 접근 규칙을 편집하는 경우 처리를 확인하는 창에서 다음 처리 방법 중 하나를 선택합니다:
     - 웹 리소스 주소 목록의 가져온 항목을 기존 주소 목록에 추가하려는 경우 **예** 버튼을 누릅니다.
     - 웹 리소스 주소 목록에 있는 기존 항목을 삭제하고 가져온 항목을 추가하려는 경우 **아니오** 버튼을 누릅니다.

   Microsoft Windows의 **파일 열기** 창이 열립니다.

7. Microsoft Windows의 **파일 열기** 창에서 가져올 웹 리소스 주소 목록이 있는 파일을 선택합니다.

8. **열기** 버튼을 누릅니다.

9. **웹사이트 접근 규칙** 창에서 **확인**을 누릅니다.

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 abc가 포함되어 있는 모든 웹 리소스에 접근 규칙이 적용됩니다. 예: http://www.example.com/page_0-9abcdef.html.

   주소 마스크에서 * 문자를 포함하려면, * 문자를 두 번 입력하십시오.

2. 주소 마스크 처음에 나오는 `www.` 문자는 * 순서로 해석됩니다.

   예: 주소 마스크 www.example.com은 *.example.com으로 처리됩니다.

3. 주소 마스크가 * 문자로 시작되지 않는 경우 주소 마스크의 컨텐츠는 * 접두사가 있는 컨텐츠와 동일합니다.

4. 주소 마스크 시작에 나오는 `*.` 문자는 `*.` 또는 빈 문자열로 해석됩니다.

   예: 주소 마스크 http://www.*.example.com에는 http://www2.example.com이 포함됩니다.

5. 주소 마스크가 `/` 또는 * 이외의 문자로 끝나는 경우 주소 마스크의 컨텐츠는 `/*` 접미사가 있는 컨텐츠와 동일합니다.

   예: 주소 마스크 http://www.example.com에는 http://www.example.com/abc와 같은 주소가 포함됩니다. 여기서 a, b, c는 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.com에는 http://example.com 및 https://example.com 주소가 포함됩니다.

   - 주소 마스크에 네트워크 프로토콜이 포함되어 있는 경우 이 주소 마스크는 네트워크 프로토콜이 동일한 주소만 포함합니다.

     예: 주소 마스크 http://*.example.com에는 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

아니오.	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 1 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 2 및 1 참조.
7	www.example.com	https://www.example.com	예	규칙 2 및 1 참조.
8	http://www.*.example.com	http://123.example.com	예	규칙 2, 4, 1 참조.
9	www.example.com	http://www.example.com/abc	예	규칙 2, 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;	예	규칙 9 및 8 참조.

		https://www.example.com		
19	www.example.com/abc/123	http://www.example.com/abc	아니오	주소 마스크에는 웹 리소스 주소외에 추가 정보가 포함되어 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 설정의 **처리** 드롭다운 메뉴에서 **경고** 옵션을 선택한 경우 경고 메시지를 표시합니다.

  경고 메시지가 잘못 표시되었다고 판단되는 경우 경고 메시지의 링크를 눌러 사전에 작성된 메시지를 연 다음 회사의 네트워크 관리자에게 보내 주십시오.

- 웹 리소스 차단에 대해 알리는 메시지. Kaspersky Endpoint Security는 해당 웹 리소스를 설명하는 규칙 설정의 **처리** 드롭다운 목록에서 **차단** 옵션을 선택한 경우 웹 리소스가 차단되었음을 알리는 메시지를 표시합니다.

  웹 리소스가 잘못 차단되었다고 판단되는 경우 웹 리소스 차단에 대해 알리는 메시지의 링크를 눌러 사전에 작성된 메시지를 연 다음 회사의 네트워크 관리자에게 보내 주십시오.

경고 메시지, 웹 리소스 차단에 대해 알리는 메시지, LAN 관리자에게 보낼 메시지에 사용할 수 있는 특별 템플릿이 제공됩니다. 해당 내용을 수정할 수 있습니다.

웹 제어 메시지의 템플릿을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **엔드포인트 제어** 섹션에서 **웹 제어** 하위 섹션을 선택합니다.

   창 오른쪽에 웹 제어 구성요소의 설정이 표시됩니다.
3. 창 오른쪽에 있는 **템플릿** 버튼을 누릅니다.

   메시지 템플릿 창이 열립니다.
4. 다음 중 하나를 수행합니다:
   - 사용자에게 웹 리소스 방문 시 경고하는 메시지의 템플릿을 편집하려면, **경고** 탭을 선택합니다.
   - 사용자에게 웹 리소스가 보안위협일 가능성이 있음을 알리는 메시지의 템플릿을 편집하려면 **차단** 탭을 선택합니다.
   - 관리자에게 보내는 메시지의 템플릿을 편집하려면 **관리자에게 메시지 보내기** 탭을 선택합니다.
5. 메시지 템플릿을 편집합니다. **변수** 드롭다운 목록 외에 **기본값** 및 **링크**(이 버튼은 **관리자에게 메시지 보내기** 탭에는 표시 안 됨) 버튼을 사용할 수 있습니다.
6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

KATA 엔드포인트 센서

Kaspersky Security Center 관리 콘솔에서만 KATA 엔드포인트 센서 구성요소의 설정을 지정할 수 있습니다. 이 구성요소를 사용하려면 관리 플러그인을 설치해야 합니다.

이 섹션에는 KATA 엔드포인트 센서 정보와 구성요소의 작동 또는 중지 방법에 대한 안내가 나와 있습니다.

KATA 엔드포인트 센서 정보

*KATA 엔드포인트 센서*는 Kaspersky Anti Targeted Attack 플랫폼의 구성요소입니다. 이 솔루션은 표적 공격과 같은 보안위협을 빠르게 감지하기 위한 용도입니다.

이 구성요소는 클라이언트 컴퓨터에 설치됩니다. 해당 컴퓨터에서 구성요소는 지속적으로 프로세스, 활성 네트워크 연결 및 수정 파일을 모니터링한 다음 Kaspersky Anti Targeted Attack 플랫폼으로 이 정보를 전달합니다.

구성 요소 기능은 다음 운영 체제 하에서 이용 가능합니다:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

이 문서에 제공되지 않는 Kaspersky Anti Targeted Attack 플랫폼에 대한 추가 정보는 Kaspersky Anti Targeted Attack 플랫폼 도움말을 참조하십시오.

프록시 서버를 거치지 않고 Kaspersky Anti Targeted Attack 플랫폼 서버에서 직접 KATA 엔드포인트 센서 구성요소가 설치된 컴퓨터로의 인바운드 연결이 허용되어야 합니다.

KATA 엔드포인트 센서 구성요소 작동 및 중지

KATA 엔드포인트 센서 구성요소를 작동 또는 중지하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 정책 설정을 편집할 관련 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.

4. 필요한 정책을 선택합니다.

5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:

   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

6. **고급 설정** 섹션에서 **KATA 엔드포인트 센서** 하위 섹션을 선택합니다.

7. 다음 중 하나를 수행합니다:

   - KATA 엔드포인트 센서를 작동하려면 **KATA 엔드포인트 센서** 확인란을 선택합니다.
   - KATA 엔드포인트 센서 작동을 중지하려면 **KATA 엔드포인트 센서** 확인란을 선택 취소합니다.

8. 이전 단계에서 **KATA 엔드포인트 센서** 확인란을 선택한 경우 **서버 주소** 필드에 다음 부분으로 구성된 Kaspersky Anti Targeted Attack 플랫폼 서버 주소를 지정합니다:

   a. 프로토콜 이름

   b. 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)

   c. 서버의 Windows Event Collector 경로

9. **확인**을 누릅니다.

10. 정책이 적용됩니다.

    Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

데이터 암호화

Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows를 실행하는 컴퓨터에 설치되어 있는 경우 데이터 암호화 기능을 완전히 사용할 수 있습니다. Kaspersky Endpoint Security가 파일 서버용 Microsoft Windows를 실행하는 컴퓨터에 설치되어 있으면 BitLocker 드라이브 암호화 기술을 사용한 하드 드라이브 암호화만 사용할 수 있습니다.

이 섹션은 하드 드라이브, 이동식 드라이브 및 로컬 컴퓨터 드라이브의 파일 및 폴더에 대한 암호화와 복호화에 대한 정보가 있으며 Kaspersky Endpoint Security 및 Kaspersky Endpoint Security 관리 플러그인을 사용하여 데이터의 암호화 및 복호화를 구성하고 수행하는 방법을 설명합니다.

암호화된 데이터에 접근할 수 없는 경우 암호화된 데이터 사용에 관한 특별 지침(파일 암호화 기능이 제한적인 경우 암호화된 파일 사용, 암호화된 장치에 접근할 수 없는 경우 암호화된 장치 사용)을 참조하십시오.

Kaspersky Security Center 정책의 암호화 설정 표시

Kaspersky Security Center 정책의 암호화 설정에 표시하려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 서버 - <컴퓨터 이름>** 노드에 대한 마우스 오른쪽 메뉴에서 **보기 → 인터페이스 설정**을 선택합니다.

   인터페이스 설정 창이 열립니다.
3. **인터페이스 설정** 창에서 **암호화 및 데이터 보호 표시** 확인란을 선택합니다.
4. **확인**을 누릅니다.

데이터 암호화 정보

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.

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 프로그램을 활성화해야 합니다.

라이센스가 만료되거나 최종 사용자 라이센스 계약서 위반이 발생하거나 Kaspersky Endpoint Security 또는 암호화 구성요소가 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 드라이브의 파일 암호화**. 로컬 컴퓨터 드라이브에 저장된 확장자 또는 확장자 그룹별 파일 목록과 폴더별 목록을 컴파일하고, 특정 애플리케이션에 의해 생성된 파일을 암호화하는 규칙을 생성할 수 있습니다. Kaspersky Security Center 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.

  Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

- **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.

  Kaspersky Security Center 정책이 적용되면 애플리케이션은 암호화 규칙에 지정된 처리 방법을 수행합니다.

- **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.

- **암호화된 압축 파일 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.

- **하드 드라이브 암호화**. 다음 암호화 기술을 선택할 수 있습니다: Kaspersky 디스크 암호화 또는 BitLocker 드라이브 암호화(이후 간단히 "BitLocker"로도 호칭).

  BitLocker는 Windows 운영 체제에 포함된 기술입니다. 컴퓨터에 신뢰하는 플랫폼 모듈(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 하드 드라이브 암호화 규칙을 지정하고 암호화에서 예외할 하드 드라이브 목록을 작성할 수 있습니다. Kaspersky Security Center 정책이 적용되면 Kaspersky Endpoint Security는 하드 드라이브의 모든 섹터를 일일이 암호화합니다. 애플리케이션은 하드 드라이브의 모든 논리 파티션을 동시에 암호화합니다. Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

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 스마트 카드의 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. 인증 에이전트 계정을 관리하고 인증 에이전트의 사용자 이름 및 암호를 사용하여 운영 체제에 자동 로그인할 수 있는 SSO(Single Sign-On) 기술을 사용할 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 관리자 설명서*에서 해당 작업에 대한 자세한 내용을 알아볼 수 있습니다.

애플리케이션 버전이 Kaspersky Endpoint Security 10 Service Pack 2 for Windows로 업그레이드될 때 인증 에이전트 계정의 목록은 저장되지 않습니다.

Kaspersky Endpoint Security 및 하드 드라이브 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. 따라서 컴퓨터에서 **사용한 디스크 공간만 암호화** 기능을 설정한 상태에서 정규 암호화가 시작되는 동안 새 장치에 새 파일을 쓰면 잠시 후 모든 섹터가 암호화됩니다.

파일 복호화에 필요한 데이터는 파일을 암호화한 컴퓨터를 제어하는 Kaspersky Security Center 관리 서버에서 제공합니다. 파일을 암호화한 컴퓨터가 다른 관리 서버의 제어를 받고 있으며, 암호화된 파일에 접근한 적이 없을 경우 다음과 같은 방법으로 이 파일에 대한 접근 권한을 부여받을 수 있습니다:

- LAN 관리자에게 암호화된 개체에 대한 접근 권한을 요청합니다;
- 복원 유틸리티를 사용하여 암호화된 장치에 있는 데이터 복원하기;
- 백업 복사본을 암호화한 컴퓨터를 제어하는 Kaspersky Security Center 관리 서버의 구성을 복원하여 이 구성을 현재 암호화된 파일이 있는 컴퓨터를 제어하는 관리 서버에 사용.

애플리케이션은 암호화 과정에서 서비스 파일을 생성합니다. 이들을 저장하려면 하드 드라이브에 조각화되지 않은 여유 공간이 2~3퍼센트 정도 있어야 합니다. 하드 드라이브에 디스크 공간이 부족할 경우 충분한 공간이 확보될 때까지 암호화가 시작되지 않습니다.

Kaspersky Endpoint Security와 Kaspersky Anti-Virus for UEFI의 암호화 기능은 호환되지 않습니다. Kaspersky Anti-Virus for UEFI가 설치된 컴퓨터의 하드 드라이브를 암호화하면 Kaspersky Anti-Virus for UEFI가 작동되지 않습니다.

암호화 기능 제한

암호화된 하드 드라이브에 새 파티션을 생성하고 기존 암호화된 하드 드라이브의 파티션을 포맷하면 해당 하드 드라이브의 데이터가 손실될 수 있습니다.

하드 드라이브가 하드웨어 및 소프트웨어 요구 사항을 충족하지 못하면 Kaspersky 디스크 암호화 기술을 사용한 하드 드라이브 암호화 기능을 사용할 수 없습니다.

Kaspersky Endpoint Security는 다음 구성을 지원하지 않습니다:

- 부트 로더와 운영 체제가 각각 다른 드라이브에 있는 구성.
- 시스템에 UEFI 32 표준의 소프트웨어가 포함되어 있는 구성.
- Intel® Rapid Start 기술 및 Intel® Rapid Start 기술을 설정하지 않았는데 절전 파티션이 있는 드라이브.
- 확장 파티션이 4개 이상인 MBR 포맷 드라이브.
- 비시스템 드라이브에 Swap 파일이 있음.
- 여러 운영 체제가 동시에 설치된 멀티 부팅 시스템.
- 다이내믹 파티션(기본 파티션만 지원).
- 조각화되지 않은 디스크 여유 공간이 2% 미만인 드라이브.
- 512바이트 또는 512바이트를 에뮬레이션하는 4096바이트로 섹터 크기가 서로 다른 드라이브.
- 하이브리드 드라이브.

암호화 알고리즘 변경

Kaspersky Endpoint Security가 데이터 암호화에 사용하는 암호화 알고리즘은 배포 패키지에 포함된 암호화 라이브러리에 따라 따릅니다.

암호화 알고리즘을 변경하려면:

1. 암호화 알고리즘 변경을 시작하기 전에 Kaspersky Endpoint Security에서 암호화된 개체를 복호화합니다.

   암호화 알고리즘을 변경하면 이전에 암호화된 개체는 사용할 수 없게 됩니다.

2. Kaspersky Endpoint Security 제거.

3. 다양한 비트 수의 암호화 라이브러리가 포함된 배포 패키지로부터 Kaspersky Endpoint Security를 설치합니다.

Single Sign-On(SSO) 기술 사용

Single Sign-On(SSO) 기술은 타사 계정 자격 증명 제공 업체와 호환되지 않습니다.

Single Sign-On(SSO) 기술을 사용하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 Single Sign-On(SSO) 기술을 사용할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **일반 암호화 설정** 서브 섹션을 선택합니다.
7. **일반 암호화 설정** 서브 섹션에서 **암호 정책 설정** 섹션에 있는 **구성** 버튼을 누릅니다.
   암호화용 암호 설정 창의 **인증 에이전트** 탭이 열립니다.
8. **Single Sign-On(SSO) 기술 사용** 확인란을 선택합니다.
9. **확인**을 누릅니다.
10. 변경 사항을 저장하려면, **속성: <정책 이름>** 창에서 **확인**을 누릅니다.
11. 정책이 적용됩니다.

    Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

파일 암호화 관련 특별 고려 사항

파일 암호화 기능을 이용할 때 다음 사항을 유의하십시오:

- 특정 그룹의 관리 컴퓨터에 대해서는 별도의 이동식 드라이브 암호화 사전 설정을 사용하여 Kaspersky Security Center 정책을 적용합니다. 따라서 이동식 드라이브가 연결된 컴퓨터에 따라 이동식 드라이브의 파일 암호화/복호화 정책이 다르게 적용될 수 있습니다.
- Kaspersky Endpoint Security는 이동식 드라이브에 저장된 읽기 전용 상태의 파일은 암호화/복호화하지 않습니다.

- 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 및 리다이렉트 폴더의 사전 정의된 폴더에서는 파일을 암호화/복호화하지 않습니다. Kaspersky에서 암호화를 권장하는 표준 폴더의 목록은 다음과 같습니다:
  - 내 문서
  - 즐겨찾기
  - 쿠키
  - 바탕 화면
  - 임시 Internet Explorer 파일
  - 임시 파일
  - Outlook 파일
- Kaspersky Endpoint Security는 운영 체제 및 설치된 애플리케이션에 손상을 줄 수 있는 파일 및 폴더 암호화를 수행하지 않습니다. 예를 들어 다음 파일과 폴더는 그 하위 폴더를 포함하여 암호화에서 예외합니다:
  - %WINDIR%.
  - %PROGRAMFILES%, %PROGRAMFILES(X86)%.
  - Windows 레지스트리 파일.

  암호화 예외 목록은 확인 또는 편집할 수 없습니다. 암호화 예외 목록의 파일과 폴더를 암호화 목록에 추가할 수 있지만 파일 및 폴더 암호화 작업 수행 시 암호화되지 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

로컬 컴퓨터 드라이브의 파일 암호화

워크스테이션용 Microsoft Windows에서 실행되는 컴퓨터에 Kaspersky Endpoint Security가 설치되어 있는 경우 로컬 컴퓨터 드라이브의 파일을 암호화할 수 있습니다. 서버용 Microsoft Windows에서 실행되는 컴퓨터에 Kaspersky Endpoint Security가 설치되어 있는 경우 로컬 컴퓨터 드라이브의 파일을 암호화할 수 없습니다.

이 섹션은 로컬 컴퓨터 드라이브의 파일 암호화를 다루며, Kaspersky Endpoint Security 및 Kaspersky Endpoint Security 콘솔 플러그인을 사용하여 로컬 컴퓨터 드라이브의 파일 암호화를 구성하고 수행하는 방법을 설명합니다.

로컬 컴퓨터 드라이브의 파일 암호화

로컬 드라이브의 파일을 암호화하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 로컬 드라이브의 파일 암호화를 구성할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **파일 및 폴더 암호화** 하위 섹션을 선택합니다.
7. 창 오른쪽에서 **암호화** 탭을 선택합니다.
8. **암호화 모드** 드롭다운 목록에서 **기본 규칙에 따라 처리** 항목을 선택합니다.
9. **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.
   사전 정의된 폴더 선택 창이 열립니다.
   b. 직접 입력한 폴더 경로를 암호화 규칙에 추가하려면 **사용자 지정 폴더** 항목을 선택합니다.
   사용자 지정 폴더 추가 창이 열립니다.
   c. 파일 확장자를 암호화 규칙에 추가하려면 **파일 확장자로** 항목을 선택합니다. Kaspersky Endpoint Security는 컴퓨터의 전체 로컬 드라이브에서 지정된 확장자의 파일을 암호화합니다.
   파일 확장자 목록 추가 / 편집 창이 열립니다.
   d. 파일 확장자 그룹을 암호화 규칙에 추가하려면 **파일 확장자 그룹으로** 항목을 선택합니다. Kaspersky Endpoint Security는 컴퓨터의 전체 로컬 드라이브에서 확장자 그룹에 나열된 확장자를 사용하는 파일을 암호화합니다.
   파일 확장자 그룹 선택 창이 열립니다.
10. 변경 사항을 저장하려면, **속성: <정책 이름>** 창에서 **확인**을 누릅니다.
11. 정책이 적용됩니다.
    Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

정책이 적용되면 Kaspersky Endpoint Security는 암호화 규칙에는 포함되고 복호화 규칙에는 포함되지 않은 파일을 암호화합니다.

> 한 파일이 암호화 규칙과 복호화 규칙에 모두 추가된 경우 Kaspersky Endpoint Security는 해당 파일이 암호화 안 되어 있다면 암호화하지 않으며, 암호화되어 있다면 복호화합니다.

Kaspersky Endpoint Security는 암호화되지 않은 파일이 수정된 후에도 해당 파일의 속성(파일 경로/파일 이름/파일 확장자)이 계속 암호화 규칙 기준을 충족하는 경우 해당 파일을 암호화합니다.

Kaspersky Endpoint Security는 파일이 열려 있을 경우 닫힐 때까지 암호화를 연기합니다.

사용자가 새로 생성한 파일의 속성이 암호화 규칙 기준을 충족하는 경우 Kaspersky Endpoint Security는 해당 파일이 열리는 즉시 파일을 암호화합니다.

로컬 드라이브에서 다른 폴더로 암호화된 파일을 옮길 경우 해당 폴더의 암호화 규칙 포함 여부에 관계 없이 파일은 암호화된 상태로 유지됩니다.

애플리케이션의 암호화된 파일 접근 규칙 작성

애플리케이션의 암호화된 파일 접근 규칙을 작성하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 애플리케이션의 암호화된 파일 접근 규칙을 구성할 관련 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **파일 및 폴더 암호화** 하위 섹션을 선택합니다.
7. **암호화 모드** 드롭다운 목록에서 **기본 규칙에 따라 처리** 항목을 선택합니다.

   접근 규칙은 **기본 규칙에 따라 처리** 모드에서만 적용됩니다. **기본 규칙에 따라 처리** 모드에서 접근 규칙을 적용한 후 **있는 그대로 둠** 모드로 전환하면 Kaspersky Endpoint Security가 모든 접근 규칙을 무시합니다. 모든 애플리케이션이 모든 암호화된 파일에 접근할 수 있게 됩니다.

8. 창 오른쪽에서 **애플리케이션 규칙** 탭을 선택합니다.
9. Kaspersky Security Center 목록에 있는 애플리케이션만 선택하려는 경우 **추가** 버튼을 누르고 나타나는 드롭다운 목록에서 **Kaspersky Security Center 목록에 있는 애플리케이션** 항목을 선택합니다.

   Kaspersky Security Center 목록에서 애플리케이션 추가 창이 열립니다.

   다음을 수행합니다:

   a. 표의 애플리케이션 목록에 필터를 적용하여 범위를 좁힙니다. **애플리케이션**, **공급업체** 및 **추가된 기간** 파라미터와 **그룹** 섹션의 모든 확인란에 대해 값을 지정합니다.

   b. **새로 고침** 버튼을 누릅니다.

   표에 적용된 필터와 일치하는 애플리케이션이 표시됩니다.

   c. **애플리케이션** 열에서 암호화된 파일 접근 규칙을 작성할 애플리케이션 옆의 확인란을 선택합니다.

d. **애플리케이션 규칙** 드롭다운 목록에서 암호화된 파일에 대한 애플리케이션 접근을 결정할 규칙을 선택합니다.

e. **이전에 선택한 애플리케이션 처리 방법** 드롭다운 목록에서 이전에 해당 애플리케이션에 대해 작성된 암호화된 파일 접근 규칙에 관해 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택합니다.

f. **확인**을 누릅니다.

애플리케이션 규칙 탭의 표에 애플리케이션의 암호화된 파일 접근 규칙에 대한 상세 정보가 표시됩니다.

10. 사용자가 직접 애플리케이션을 선택하려면 **추가** 버튼을 누르고 드롭다운 목록에서 **사용자 지정 애플리케이션** 항목을 선택합니다.

실행 파일 이름 추가 / 편집 창이 열립니다.

다음을 수행합니다:

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.

d. **확인**을 누릅니다.

애플리케이션 규칙 탭의 표에 애플리케이션의 암호화된 파일 접근 규칙에 대한 상세 정보가 표시됩니다.

11. **확인**을 눌러 변경사항을 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 Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 특정 애플리케이션에 의해 생성된 파일의 암호화를 구성할 관련 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

- 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

6. **데이터 암호화** 섹션에서 **파일 및 폴더 암호화** 하위 섹션을 선택합니다.

7. **암호화 모드** 드롭다운 목록에서 **기본 규칙에 따라 처리** 항목을 선택합니다.

   암호화 규칙은 **기본 규칙에 따라 처리** 모드에서만 적용됩니다. **기본 규칙에 따라 처리** 모드에서 암호화 규칙을 적용한 후 **있는 그대로 둠** 모드로 전환하면 Kaspersky Endpoint Security가 모든 암호화 규칙을 무시합니다. 이전에 암호화된 파일은 암호화된 상태가 유지됩니다.

8. 창 오른쪽에서 **애플리케이션 규칙** 탭을 선택합니다.

9. Kaspersky Security Center 목록에 있는 애플리케이션만 선택하려는 경우 **추가** 버튼을 누르고 나타나는 드롭다운 목록에서 **Kaspersky Security Center 목록에 있는 애플리케이션** 항목을 선택합니다.

   Kaspersky Security Center 목록에서 애플리케이션 추가 창이 열립니다.

   다음을 수행합니다:

   a. 표의 애플리케이션 목록에 필터를 적용하여 범위를 좁힙니다. **애플리케이션**, **공급업체** 및 **추가된 기간** 파라미터와 **그룹** 섹션의 모든 확인란에 대해 값을 지정합니다.

   b. **새로 고침** 버튼을 누릅니다.

      표에 적용된 필터와 일치하는 애플리케이션이 표시됩니다.

   c. **애플리케이션** 열에서 암호화를 적용해야 할 파일을 작성한 애플리케이션 옆의 확인란을 선택합니다.

   d. **애플리케이션 규칙** 드롭다운 목록에서 **생성된 모든 파일 암호화**를 선택합니다.

   e. **이전에 선택한 애플리케이션 처리 방법** 드롭다운 목록에서 이전에 해당 애플리케이션에 대해 작성된 파일 암호화 규칙에 관해 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택합니다.

   f. **확인**을 누릅니다.

   선택한 애플리케이션에서 만들어졌거나 수정된 파일에 적용된 암호화 규칙 정보가 **애플리케이션 규칙** 탭에 표시됩니다.

10. 사용자가 직접 애플리케이션을 선택하려면 **추가** 버튼을 누르고 드롭다운 목록에서 **사용자 지정 애플리케이션** 항목을 선택합니다.

    실행 파일 이름 추가 / 편집 창이 열립니다.

    다음을 수행합니다:

    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.

    d. **확인**을 누릅니다.

    선택한 애플리케이션에서 만들어졌거나 수정된 파일에 적용된 암호화 규칙 정보가 **애플리케이션 규칙** 탭에 표시됩니다.

11. **확인**을 눌러 변경사항을 저장합니다.

복호화 규칙 생성

복호화 규칙을 생성하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 복호화할 파일 목록을 작성할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **파일 및 폴더 암호화** 하위 섹션을 선택합니다.
7. 창 오른쪽에서 **복호화** 탭을 선택합니다.
8. **암호화 모드** 드롭다운 목록에서 **기본 규칙에 따라 처리** 항목을 선택합니다.
9. **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.
   사전 정의된 폴더 선택 창이 열립니다.
   b. 직접 입력한 폴더 경로를 복호화 규칙에 추가하려면 **사용자 지정 폴더** 항목을 선택합니다.
   사용자 지정 폴더 추가 창이 열립니다.
   c. 파일 확장자를 복호화 규칙에 추가하려면 **파일 확장자로** 항목을 선택합니다. Kaspersky Endpoint Security는 컴퓨터의 전체 로컬 드라이브에서 지정된 확장자의 파일을 복호화합니다.
   파일 확장자 목록 추가 / 편집 창이 열립니다.
   d. 파일 확장자 그룹을 복호화 규칙에 추가하려면 **파일 확장자 그룹으로** 항목을 선택합니다. Kaspersky Endpoint Security는 컴퓨터의 전체 로컬 드라이브에서 확장자 그룹에 나열된 확장자를 사용하는 파일을 암호화하지 않습니다.
   파일 확장자 그룹 선택 창이 열립니다.
10. 변경 사항을 저장하려면, **속성: <정책 이름>** 창에서 **확인**을 누릅니다.
11. 정책이 적용됩니다.

    Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

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 Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 로컬 드라이브의 파일 복호화를 구성할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **파일 및 폴더 암호화** 하위 섹션을 선택합니다.
7. 창 오른쪽에서 **암호화** 탭을 선택합니다.
8. 암호화 목록에서 복호화할 파일과 폴더를 삭제합니다. 그러려면 파일을 선택한 다음 **제거** 버튼에서 마우스 오른쪽 버튼을 눌러 메뉴를 열고 **규칙 삭제 및 파일 복호화** 항목을 선택합니다.

   암호화 목록에서 한 번에 여러 항목을 삭제할 수 있습니다. 그러려면 **CTRL** 키를 누른 상태에서 마우스 왼쪽 버튼을 눌러 원하는 파일을 모두 선택하고 **제거** 버튼에서 마우스 오른쪽 메뉴를 눌러 **규칙 삭제 및 파일 복호화** 항목을 선택합니다.

   암호화 목록에서 파일과 폴더가 삭제되고 복호화 목록에 자동 추가됩니다.
9. 파일 복호화 목록 작성.
10. 변경 사항을 저장하려면, **속성: <정책 이름>** 창에서 **확인**을 누릅니다.
11. 정책이 적용됩니다.

Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

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.

암호화된 패키지 생성

Kaspersky Endpoint Security는 암호화 패키지를 만들 때 파일 압축을 수행하지 않습니다.

암호화 패키지를 만들려면 다음과 같이 하십시오:

1. Kaspersky Endpoint Security가 설치되고 암호화 기능이 활성화된 컴퓨터에서 파일 관리자를 사용하여 암호화된 패키지에 추가할 파일 또는 폴더를 선택합니다. 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 엽니다.
2. 마우스 오른쪽 메뉴에서 **암호화 패키지 추가**를 선택합니다.

   암호화 패키지를 저장할 경로 선택 표준 Microsoft Windows 대화 상자가 열립니다.
3. **암호화 패키지를 저장할 경로 선택** 표준 Microsoft Windows 대화 상자에서 암호화된 패키지를 저장할 이동식 드라이브의 폴더를 선택합니다. **저장** 버튼을 누릅니다.

   암호화 패키지 추가 창이 열립니다.
4. **암호화 패키지 추가** 창에서 암호를 입력하고 확인합니다.
5. **생성** 버튼을 누릅니다.

   암호화 패키지 생성 프로세스가 시작됩니다. 프로세스가 완료되면 이동식 드라이브의 선택된 대상 폴더에 암호로 보호되는 자동 압축 해제 방식의 암호화된 패키지가 생성됩니다.

암호화 패키지의 생성을 취소하면 Kaspersky Endpoint Security가 다음 작업을 수행합니다:

1. 패키지로의 파일 복사를 중단하고 진행 중인 패키지 암호화 작업이 있으면 모두 종료합니다.
2. 패키지 생성 및 암호화 과정에서 생성된 모든 임시 파일과 암호화 패키지 파일을 삭제합니다.
3. 사용자에게 암호화 패키지 생성 프로세스가 강제 종료되었음을 알립니다.

암호화된 패키지 압축 해제

암호화 패키지를 압축 해제하려면 다음과 같이 하십시오:

1. 파일 관리자에서 암호화된 패키지를 선택합니다. 패키지 해제 마법사를 시작합니다.

   암호 입력 창이 열립니다.
2. 암호화된 패키지 보호 암호를 입력합니다.
3. **암호 입력** 창에서 **확인**을 누릅니다.

   올바른 암호가 입력되었으면 표준 **찾아보기** Microsoft Windows 대화 상자가 열립니다.
4. **찾아보기** Microsoft Windows 대화 상자에서 암호화된 압축 파일을 해제할 대상 폴더를 선택하고 **확인**을 누릅니다.

   대상 폴더에 암호화된 패키지를 해제하는 과정이 시작됩니다.

이전에 암호화된 패키지가 지정된 대상 폴더에 해제된 적이 있다면 암호화된 패키지의 파일이 폴더에 있는 기존 파일을 덮어씁니다.

암호화 패키지의 압축 해제를 취소하면 Kaspersky Endpoint Security가 다음 작업을 수행합니다:

1. 패키지 복호화 프로세스를 중지하고 암호화된 패키지에서 파일을 복사하는 작업이 진행 중인 경우 이 작업을 모두 종료합니다.

2. 암호화된 패키지의 복호화 및 해제 과정에서 생성된 모든 임시 파일과 암호화된 패키지에서 대상 폴더로 복사된 파일을 모두 삭제합니다.

3. 사용자에게 암호화 패키지 압축 해제 프로세스가 강제 종료되었음을 알립니다.

이동식 드라이브 암호화

Kaspersky Endpoint Security가 워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 이동식 드라이브를 암호화할 수 있습니다. Kaspersky Endpoint Security가 파일 서버용 Microsoft Windows에서 실행 중인 컴퓨터에 설치되어 있는 경우 이동식 드라이브를 암호화할 수 없습니다.

이 섹션에는 이동식 드라이브의 암호화에 대한 정보 및 Kaspersky Endpoint Security 및 Kaspersky Endpoint Security 관리 플러그인을 사용하여 이동식 드라이브 암호화를 구성하고 수행하는 방법이 설명되어 있습니다.

이동식 드라이브 암호화 시작

이동식 드라이브를 암호화하려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 이동식 드라이브의 암호화를 구성할 관리 그룹의 이름을 가진 폴더를 엽니다.

3. 작업 공간에서 **정책** 탭을 선택합니다.

4. 필요한 정책을 선택합니다.

5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:

   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

6. **데이터 암호화** 섹션에서 **이동식 드라이브 암호화** 서브 섹션을 선택합니다.

7. **암호화 모드** 드롭다운 목록에서 Kaspersky Endpoint Security가 선택된 관리 그룹의 컴퓨터에 연결된 모든 이동식 드라이브에 대해 수행할 기본 작업을 선택합니다:

   - **전체 이동식 드라이브 암호화**. 이 항목을 선택하면 지정된 이동식 드라이브 암호화 설정을 사용하여 Kaspersky Security Center 정책을 적용할 때 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. Kaspersky Endpoint Security는 이미 암호화된 이동식 드라이브는 다시 암호화하지 않습니다.

     이 암호화 시나리오는 Kaspersky Endpoint Security의 하드 드라이브 암호화 기능에 의해 작동됩니다.

- **모든 파일 암호화**. 이 항목을 선택하면 지정된 이동식 드라이브 암호화 설정을 사용하여 Kaspersky Security Center 정책을 적용할 때 Kaspersky Endpoint Security가 이동식 드라이브에 저장된 모든 파일을 암호화합니다. Kaspersky Endpoint Security는 이미 암호화된 파일은 다시 암호화하지 않습니다. 암호화된 파일의 이름과 폴더 구조를 포함하여 이동식 드라이브의 파일 시스템은 암호화되지 않습니다.

- **새 파일만 암호화**. 이 항목을 선택하면 지정된 이동식 드라이브 암호화 설정을 사용하여 Kaspersky Security Center 정책을 적용할 때 Kaspersky Endpoint Security가 이동식 드라이브에 새로 추가된 파일 또는 이동식 드라이브에 저장되어 Kaspersky Security Center 정책이 마지막으로 적용된 후 수정된 파일만 암호화합니다.

- **전체 이동식 드라이브 복호화**. 이 항목을 선택하면 지정된 이동식 드라이브 암호화 설정을 사용하여 Kaspersky Security Center 정책을 적용할 때 Kaspersky Endpoint Security가 이동식 드라이브에 저장된 모든 암호화된 파일과 이동식 드라이브의 파일 시스템(이전에 암호화된 경우)을 복호화합니다.

  이 암호화 시나리오는 Kaspersky Endpoint Security의 파일 암호화 기능 및 하드 드라이브 암호화 기능을 둘 다 사용합니다.

- **있는 그대로 둠**. 이 항목을 선택하면 지정된 이동식 드라이브 암호화 설정을 사용하여 Kaspersky Security Center 정책을 적용할 때 Kaspersky Endpoint Security가 이동식 드라이브의 파일을 암호화하거나 복호화하지 않습니다.

8. 암호화하려는 컨텐츠가 있는 이동식 드라이브에 있는 파일에 대한 암호화 규칙을 생성합니다.

9. 정책이 적용됩니다.

Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

정책이 적용되면 사용자가 이동식 드라이브를 연결하거나 또는 이동식 드라이브가 이미 연결되어 있는 경우 Kaspersky Endpoint Security는 사용자에게 이동식 드라이브가 암호화 규칙 적용 대상이며 이동식 드라이브에 저장된 데이터가 암호화됨을 알립니다.

이동식 드라이브의 데이터 암호화에 대해 *있는 그대로 둠* 규칙이 지정되면 사용자에게 알림을 표시하지 않습니다.

애플리케이션은 사용자에게 암호화 과정에 다소 시간이 소요될 수 있음을 경고합니다.

애플리케이션은 암호화 작업 시작을 확인하는 메시지를 표시하고 다음과 같은 작업을 수행합니다:

- 사용자가 암호화에 동의할 경우 정책 설정에 따라 데이터를 암호화.

- 사용자가 암호화를 거부할 경우 데이터를 암호화하지 않고 이동식 드라이브 파일에 대한 접근을 읽기 전용으로 제한.

- 사용자가 암호화 확인을 무시할 경우 데이터를 암호화하지 않고 이동식 드라이브 파일에 대한 접근을 읽기 전용으로 제한하며, 다음에 다시 Kaspersky Security Center 정책이 적용되거나 이동식 드라이브가 연결될 경우 사용자에게 데이터 암호화에 대한 확인 메시지를 다시 표시.

특정 그룹의 관리 컴퓨터에 대해서는 별도의 이동식 드라이브 데이터 암호화 사전 설정을 사용하여 Kaspersky Security Center 정책이 적용됩니다. 따라서 이동식 드라이브가 연결된 컴퓨터에 따라 이동식 드라이브의 데이터 암호화가 다르게 적용될 수 있습니다.

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.

이동식 드라이브의 암호화에 실패한 경우 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 드라이브에 대한 암호화 규칙 추가

이동식 드라이브에 대한 암호화 규칙을 추가하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 이동식 드라이브 암호화 규칙을 추가할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **이동식 드라이브 암호화** 서브 섹션을 선택합니다.
7. **추가** 버튼을 마우스 왼쪽 버튼으로 눌러 드롭다운 메뉴에서 다음 항목 중 하나를 선택합니다:
   - 매체 제어 구성요소의 신뢰하는 장치 목록에 속하는 이동식 드라이브에 대한 암호화 규칙을 추가하려면 **이 정책의 신뢰하는 장치 목록에서**를 선택합니다.

     신뢰하는 장치 목록에서 장치 추가 창이 열립니다.
   - Kaspersky Security Center 목록에 속하는 이동식 드라이브에 대한 암호화 규칙을 추가하려면 **Kaspersky Security Center 장치 목록에서**를 선택합니다.

     Kaspersky Security Center 목록에서 장치 추가 창이 열립니다.
8. 이전 단계에서 **Kaspersky Security Center 장치 목록에서** 항목을 선택한 경우 표에 장치를 표시할 필터를 지정합니다. 이를 위해서는 다음과 같이 하십시오:
   a. 다음 파라미터 값을 지정합니다: **아래에 다음 장치 표시**, **장치 유형**, **이름**, **컴퓨터** 및 **Kaspersky 디스크 암호화**.
   b. **새로 고침** 버튼을 누릅니다.
9. **장치 유형** 열에서 암호화 규칙을 만들 이동식 드라이브 이름 옆의 확인란을 선택합니다.
10. **선택한 장치에 대한 암호화 모드** 드롭다운 목록에서 선택된 이동식 드라이브에 저장된 파일에 대해 Kaspersky Endpoint Security가 수행할 처리 방법을 선택합니다.

11. 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.

12. 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.

13. **이전에 선택한 장치에 대한 처리 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 규칙이 새 규칙으로 바뀌기 원하면 **업데이트**를 선택합니다.

14. **확인**을 누릅니다.

    사용자 지정 규칙 표에 이전에 생성된 암호화 규칙의 파라미터 항목이 표시됩니다.

15. **확인**을 눌러 변경사항을 저장합니다.

Kaspersky Security Center의 수정된 정책에 의해 제어되는 모든 컴퓨터에 연결된 이동식 드라이브에 추가된 이동식 드라이브 암호화 규칙이 적용됩니다.

이동식 드라이브에 대한 암호화 규칙 편집

이동식 드라이브에 대한 암호화 규칙을 편집하려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 이동식 드라이브 암호화 규칙을 편집할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
    - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
    - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **이동식 드라이브 암호화** 서브 섹션을 선택합니다.
7. 암호화 규칙이 구성된 이동식 드라이브의 목록에서 필요한 이동식 드라이브에 해당하는 항목을 선택합니다.

8. **규칙 설정** 버튼을 눌러 선택된 이동식 드라이브의 암호화 규칙을 편집합니다.

   규칙 설정 버튼의 마우스 오른쪽 메뉴가 열립니다.

9. **규칙 설정** 버튼의 마우스 오른쪽 메뉴에서 선택된 이동식 드라이브에 파일이 저장되면 Kaspersky Endpoint Security에서 수행할 처리 방법을 선택합니다.

10. **확인**을 눌러 변경사항을 저장합니다.

Kaspersky Security Center의 수정된 정책에 의해 제어되는 모든 컴퓨터에 연결된 이동식 드라이브에 수정된 이동식 드라이브 암호화 규칙이 적용됩니다.

이동식 드라이브의 암호화된 파일 접근을 위한 휴대용 모드 설정

이동식 드라이브의 암호화된 파일 접근을 위한 휴대용 모드를 설정하려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 이동식 드라이브의 암호화된 파일 접근을 위해 휴대용 모드를 설정하려는 관리 그룹의 이름을 가진 폴더를 엽니다.

3. 작업 공간에서 **정책** 탭을 선택합니다.

4. 필요한 정책을 선택합니다.

5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:

   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

6. **데이터 암호화** 섹션에서 **이동식 드라이브 암호화** 서브 섹션을 선택합니다.

7. **휴대용 모드** 확인란을 선택합니다.

   모든 파일 또는 신규 파일의 암호화에 대해 휴대용 모드가 제공됩니다.

8. **확인**을 누릅니다.

9. 정책이 적용됩니다.

   Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

10. 이동식 드라이브를 Kaspersky Security Center 정책이 적용된 장치에 연결합니다.

11. 이동식 드라이브 암호화 작동을 확인합니다.

    휴대용 파일 관리자용 암호를 생성하는 창이 열립니다.

12. 암호 강도 요건에 부합하는 암호를 지정하고 확인합니다.

13. **확인**을 누릅니다.

Kaspersky Endpoint Security가 Kaspersky Security Center 정책에 정의된 암호화 규칙에 따라 이동식 드라이브의 파일을 암호화합니다. 암호화된 파일 작업에 사용된 휴대용 파일 관리자 또한 이동식 드라이브에 쓰여집니다.

휴대용 모드를 활성화한 다음 암호화 기능이 없는 컴퓨터에 연결된 이동식 드라이브의 암호화된 파일에 접근할 수 있습니다.

이동식 드라이브의 복호화

이동식 드라이브를 복호화하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 이동식 드라이브의 복호화를 구성할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **이동식 드라이브 암호화** 서브 섹션을 선택합니다.
7. 이동식 드라이브에 저장된 모든 암호화된 파일을 복호화하려면 **암호화 모드** 드롭다운 목록에서 **전체 이동식 드라이브 복호화**를 선택합니다.
8. 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.
      규칙 설정 버튼의 마우스 오른쪽 메뉴가 열립니다.
   c. **규칙 설정** 버튼의 마우스 오른쪽 메뉴에서 **모든 파일 복호화** 항목을 선택합니다.
9. **확인**을 눌러 변경사항을 저장합니다.
10. 정책이 적용됩니다.

Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

정책이 적용된 후 사용자가 이동식 드라이브를 연결하거나 이동식 드라이브가 이미 연결되어 있을 경우 Kaspersky Endpoint Security는 사용자에게 이동식 드라이브가 복호화 규칙의 적용 대상이며, 따라서 이동식 드라이브에 저장된 암호화된 파일 및 이동식 드라이브의 파일 시스템(암호화되어 있는 경우)이 복호화됨을 알립니다. 애플리케이션은 사용자에게 복호화 과정에 다소 시간이 소요될 수 있음을 경고합니다.

특정 그룹의 관리 컴퓨터에 대해서는 별도의 이동식 드라이브 데이터 암호화 사전 설정을 사용하여 Kaspersky Security Center 정책이 적용됩니다. 따라서 이동식 드라이브가 연결된 컴퓨터에 따라 이동식 드라이브의 데이터 복호화가 다르게 적용될 수 있습니다.

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.

이동식 드라이브의 복호화에 실패한 경우 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.

하드 드라이브 암호화

Microsoft Windows for Workstations를 실행하는 컴퓨터에 Kaspersky Endpoint Security가 설치되어 있는 경우 BitLocker 드라이브 암호화 및 Kaspersky 디스크 암호화 기술을 사용하여 암호화합니다. 파일 서버용 Microsoft Windows를 실행하는 컴퓨터에 Kaspersky Endpoint Security가 설치되어 있으면 BitLocker 드라이브 암호화 기술만 사용할 수 있습니다.

이 섹션에는 하드 드라이브의 암호화에 대한 정보 및 Kaspersky Endpoint Security 및 Kaspersky Endpoint Security 콘솔 플러그인을 사용하여 하드 드라이브 암호화를 구성하고 수행하는 방법이 설명되어 있습니다.

하드 드라이브 암호화 정보

하드 드라이브 암호화를 시작하기 전에 애플리케이션이 시스템 하드 드라이브에서 인증 에이전트 및 BitLocker 암호화 구성요소와의 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 하드 드라이브 암호화가 시작됩니다. 시스템 하드 드라이브가 인증 에이전트 및 BitLocker 암호화 구성요소와 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 하드 드라이브의 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 구성요소와의 호환성을 검사할 수 있습니다. 이렇게 하려면 하드 드라이브 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.

하드 드라이브 암호화가 시작되면 Kaspersky Endpoint Security는 하드 드라이브에 저장된 모든 데이터를 암호화합니다.

하드 드라이브 복호화 작업 도중에 컴퓨터를 종료하거나 재시작하면 운영 체제가 다시 시작되기 전 인증 에이전트가 로드됩니다. 인증 에이전트의 인증을 거쳐 운영 체제가 시작되면 Kaspersky Endpoint Security가 하드 드라이브 암호화 작업을 재개합니다.

하드 드라이브 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 하드 드라이브 암호화 작업을 재개합니다.

하드 드라이브 암호화 과정에서 운영 체제가 절전 모드로 바뀔 경우 운영 체제가 다시 일반 모드로 전환할 때 인증 에이전트가 로드되지 않고 Kaspersky Endpoint Security에서 바로 하드 드라이브 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.

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)
- Russian (for 105-key IBM / Windows keyboards with the QWERTY layout)
- 터키어 (QWERTY 레이아웃)
- 프랑스어 (프랑스)
- 프랑스어 (스위스)
- 프랑스어 (벨기에, AZERTY 레이아웃)
- Japanese (for 106-key keyboards with the QWERTY layout)

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.

Kaspersky Endpoint Security는 다음 토큰, 스마트 카드 리더기 및 스마트 카드를 지원합니다:

- SafeNet eToken PRO 64K (4.2b) (USB)

- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Smart Card)
- SafeNet eToken 4100 72K Java (스마트 카드)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Smart Card)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Reader)
- Gemalto IDPrime .NET 511

Kaspersky 디스크 암호화 기술을 사용해 하드 드라이브 암호화

컴퓨터의 하드 드라이브를 암호화하기 전에 컴퓨터가 감염되지 않았는지 확인해야 합니다. 그렇게 하려면, 전체 검사 또는 중요한 영역 검사 작업을 시작합니다. 루트킷에 감염된 컴퓨터의 하드 드라이브를 암호화하면 컴퓨터의 실행에 문제가 발생할 수 있습니다.

Kaspersky 디스크 암호화 기술을 사용해 하드 드라이브를 암호화하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 그룹** 폴더에서 하드 드라이브의 암호화를 구성할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **하드 드라이브 암호화** 하위 섹션을 선택합니다.

7. **암호화 기술** 드롭다운 목록에서 **Kaspersky 디스크 암호화** 옵션을 선택합니다.

BitLocker로 컴퓨터 하드 드라이브가 암호화된 경우 Kaspersky 디스크 암호화 기술을 사용할 수 없습니다.

8. **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 암호화**를 선택합니다.

암호화에서 일부 하드 드라이브를 예외해야 한다면 이러한 하드 드라이브의 목록을 생성하십시오.

9. 다음 암호화 방법 중 하나를 선택합니다:

- 파일이 저장되어 있는 하드 드라이브 부분에만 암호화를 적용하려는 경우 **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.

- 전체 하드 드라이브에 암호화를 적용하려는 경우 **사용한 디스크 공간만 암호화** 확인란을 선택 취소합니다.

  이 기능은 암호화되지 않은 장치에만 해당됩니다. 장치가 이전에 **사용한 디스크 공간만 암호화** 기능을 사용하여 암호화되었으면 **모든 하드 드라이브 암호화** 모드에서 정책을 적용하더라도 파일이 저장되어 있지 않은 부분은 계속 암호화되지 않습니다.

10. **확인**을 눌러 변경사항을 저장합니다.

11. 정책이 적용됩니다.

    Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

BitLocker 드라이브 암호화 기술을 사용한 하드 드라이브 암호화

컴퓨터의 하드 드라이브를 암호화하기 전에 컴퓨터가 감염되지 않았는지 확인해야 합니다. 그렇게 하려면, 전체 검사 또는 중요한 영역 검사 작업을 시작합니다. 루트킷에 감염된 컴퓨터의 하드 드라이브를 암호화하면 컴퓨터의 실행에 문제가 발생할 수 있습니다.

서버 운영 체제를 사용하는 컴퓨터에서 BitLocker 드라이브 암호화 기술을 사용하려면 역할 및 구성요소 추가 마법사를 사용하여 **BitLocker 드라이브 암호화** 구성요소를 설치해야 할 수 있습니다.

BitLocker 드라이브 암호화 기술을 사용한 하드 드라이브를 암호화하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리의 **관리 그룹** 폴더에서 하드 드라이브의 암호화를 구성할 관리 그룹의 이름을 가진 폴더를 엽니다.

3. 작업 공간에서 **정책** 탭을 선택합니다.

4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **하드 드라이브 암호화** 하위 섹션을 선택합니다.
7. **암호화 기술** 드롭다운 목록에서 **BitLocker 드라이브 암호화** 옵션을 선택합니다.
8. **암호화 모드** 드롭다운 목록에서 **모든 하드 드라이브 암호화** 옵션을 선택합니다.
9. 사전 부팅 환경에서 터치스크린 키보드를 사용해 정보를 입력하려면 **태블릿에서 사전 부팅 키보드 입력이 필요한 인증 사용 허용** 확인란을 선택합니다.

   대안적 데이터 입력 도구(예: 사전 부팅 환경의 USB 키보드)가 있는 장치에 한해 이 설정을 사용하는 것이 좋습니다.

10. 다음 암호화 유형 중 하나를 선택합니다:
    - 하드웨어 암호화를 사용하려면 **하드웨어 암호화 사용** 확인란을 선택합니다.
    - 소프트웨어 암호화를 사용하려면 **하드웨어 암호화 사용** 확인란을 선택 취소합니다.
11. 다음 암호화 방법 중 하나를 선택합니다:
    - 파일이 저장되어 있는 하드 드라이브 부분에만 암호화를 적용하려는 경우 **사용한 디스크 공간만 암호화** 확인란을 선택합니다.
    - 전체 하드 드라이브에 암호화를 적용하려는 경우 **사용한 디스크 공간만 암호화** 확인란을 선택 취소합니다.

      이 기능은 암호화되지 않은 장치에만 해당됩니다. 장치가 이전에 **사용한 디스크 공간만 암호화** 기능을 사용하여 암호화되었으면 **모든 하드 드라이브 암호화** 모드에서 정책을 적용하더라도 파일이 저장되어 있지 않은 부분은 계속 암호화되지 않습니다.

12. BitLocker 기술로 암호화된 하드 드라이브에 접근하는 방법을 선택합니다.
    - 신뢰하는 플랫폼 모듈(TPM)을 사용해 암호화 키를 저장하려면 **신뢰하는 플랫폼 모듈(TPM) 사용** 옵션을 선택합니다.
    - 신뢰하는 플랫폼 모듈(TPM)을 사용하여 하드 드라이브를 암호화하지 않는 경우 **암호 사용** 옵션을 선택하고 **최소 암호 길이** 필드에 암호의 최소 문자 수를 지정합니다.

      이전 버전과 마찬가지로 Windows 7 및 Windows 2008 R2 운영 체제에서도 신뢰하는 플랫폼 모듈(TPM)은 기본적으로 지원됩니다.

13. 이전 단계에서 **신뢰하는 플랫폼 모듈(TPM) 사용** 옵션을 선택한 경우 다음을 수행합니다:
    - 사용자가 암호화 키 접근을 시도할 때 입력해야 하는 PIN 코드를 설정하려면 **PIN 사용** 확인란을 선택하고 **PIN 최소 길이** 필드에 PIN 코드 최소 자릿수를 지정합니다.

- 암호를 사용하여 컴퓨터에서 신뢰하는 플랫폼 모듈을 사용하지 않고 암호화된 하드 드라이브에 접근 권한을 얻으려면 **신뢰하는 플랫폼 모듈(TPM)을 이용 불가능하면 암호 사용** 확인란을 선택하고 **최소 암호 길이** 필드에 암호에 포함되어야 하는 최소 문자 수를 표시합니다.

  이 경우 **암호 사용** 확인란을 선택한 경우와 마찬가지로 암호화 키에 접근하려면 지정된 암호를 사용해야 합니다.

  신뢰하는 플랫폼 모듈(TPM)을 사용할 수 없는 경우 암호 사용 확인란이 선택되지 않았으며 신뢰하는 플랫폼 모듈을 사용할 수 없는 경우에는 하드 드라이브 암호화가 시작되지 않습니다.

14. **확인**을 눌러 변경사항을 저장합니다.

15. 정책이 적용됩니다.

    Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터에서 정책을 적용하면 다음과 같은 창이 나타납니다:

- 시스템 하드 드라이브에 암호화 정책이 적용되면 신뢰하는 플랫폼 모듈을 사용 중인 경우 PIN 코드 창이 나타나거나 그렇지 않은 경우 사전 설치 인증을 위한 암호 요청 창이 나타납니다.
- 컴퓨터 운영 체제에 연방 정보 처리 표준 호환 모드가 설정되어 있으면 Windows 8 이상 운영 체제의 경우 복구 키 파일을 저장할 USB 장치 연결 요청 창이 표시됩니다.

사용자가 암호화 키에 접근할 수 없는 경우 로컬 네트워크 관리자에게 복구 키를 제공하도록 요청할 수 있습니다 (이전에 USB 장치에 복구 키를 저장하지 않았거나 분실한 경우).

암호화에서 예외할 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 Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 암호화에서 예외할 하드 드라이브의 파일 목록을 작성할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **하드 드라이브 암호화** 하위 섹션을 선택합니다.
7. **암호화 기술** 드롭다운 목록에서 **Kaspersky 디스크 암호화** 옵션을 선택합니다.

암호화에서 예외할 하드 드라이브에 해당하는 항목이 **다음 하드 드라이브는 암호화 안 함(예외)** 표에 표시됩니다. 이전에 암호화에서 예외할 하드 드라이브의 목록을 작성하지 않은 경우 이 표는 비어 있습니다.

8. 목록에 암호화에서 예외할 하드 드라이브를 추가하려면 다음과 같이 하십시오:

   a. **추가** 버튼을 누릅니다.

   Kaspersky Security Center 목록에서 장치 추가 창이 열립니다.

   b. **Kaspersky Security Center 목록에서 장치 추가** 창에서 다음 파라미터 값을 지정합니다: **이름**, **컴퓨터**, **디스크 유형** 및 **Kaspersky 디스크 암호화**.

   c. **새로 고침** 버튼을 누릅니다.

   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(예외)** 표에 표시됩니다.

9. 예외 목록에서 하드 드라이브를 제거하려면 **다음 하드 드라이브는 암호화 안 함(예외)** 표에서 하나 이상의 행을 선택하고 **삭제** 버튼을 누릅니다.

   표에서 여러 항목을 선택하려면 `Ctrl` 키를 누른 상태에서 이벤트를 선택합니다.

10. **확인**을 눌러 변경사항을 저장합니다.

하드 드라이브 복호화

데이터 암호화를 허용하는 활성 상태의 라이센스가 없는 경우에도 하드 드라이브를 복호화할 수 있습니다.

하드 드라이브를 복호화하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 하드 드라이브의 복호화를 구성할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **하드 드라이브 암호화** 하위 섹션을 선택합니다.

7. **암호화 기술** 드롭다운 목록에서 하드 드라이브에 적용된 암호화 기술을 선택합니다.

8. 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(예외)** 표에 복호화할 암호화된 하드 드라이브를 추가합니다.

     Kaspersky 디스크 암호화 기술에 한해 이 옵션을 사용할 수 있습니다.

9. **확인**을 눌러 변경사항을 저장합니다.

10. 정책이 적용됩니다.

    Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

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.

인증 에이전트 관리

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.

사용자는 경우에 따라 인증을 통과하지 못할 수 있습니다. 예를 들어, 사용자가 인증 에이전트 계정의 자격증명을 잊었거나, 토큰 또는 스마트 카드의 암호를 잊었거나 토큰 또는 스마트 카드를 잃어버린 경우 인증은 불가능합니다.

사용자가 인증 에이전트 계정 자격 증명이나 토큰 또는 스마트 카드의 암호를 잊어 버렸다면, 사용자는 기업의 LAN 관리자에게 문의하여 복구해야 합니다.

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 장치에서 데이터를 복원하는 절차를 완료해야합니다.

인증 에이전트에서 토큰 및 스마트 카드 사용

암호화된 하드 드라이브에 접근할 때 토큰 또는 스마트 카드를 인증에 사용할 있습니다. 그러려면 인증 에이전트 계정을 만드는 명령에 토큰 또는 스마트 카드 전자 인증서를 추가해야 합니다.

컴퓨터 하드 드라이브가 AES256 암호화 알고리즘을 사용해 암호화된 경우에 토큰 또는 스마트 카드만 사용할 수 있습니다. 컴퓨터 하드 드라이브가 AES256 암호화 알고리즘을 사용해 암호화된 경우에는 해당 명령에 전자 인증서 파일 추가가 거부됩니다.

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.

  토큰 또는 스마트 카드 전자 인증서가 이 요구사항과 맞지 않는다면, 관리 플러그인은 인증 에이전트 계정 생성 명령에 이 인증서 파일 로드를 하지 않으며 오류 메시지를 표시합니다.

- 인증서의 목적을 정의하는 `KeyUsage` 파라미터에는 `keyEncipherment` 또는 `dataEncipherment` 값이 있어야 합니다.

  토큰 또는 스마트 카드 전자 인증서가 이 요구사항과 맞지 않는다면, 관리 플러그인은 인증 에이전트 계정 생성 명령에 이 인증서 파일 로드를 하며 경고 메시지를 표시합니다.

- 인증서에 길이가 1024비트 이상인 RSA 키가 포함되어 있습니다.

  토큰 또는 스마트 카드 전자 인증서가 이 요구사항과 맞지 않는다면, 관리 플러그인은 인증 에이전트 계정 생성 명령에 이 인증서 파일 로드를 하지 않으며 오류 메시지를 표시합니다.

인증 에이전트 도움말 메시지 편집

인증 에이전트 도움말 메시지를 편집하기 전에 사전 부팅 환경에서 지원되는 문자 목록을 검토하십시오.

인증 에이전트 도움말 메시지를 편집하려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 인증 에이전트 도움말 메시지를 편집할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **데이터 암호화** 섹션에서 **일반 암호화 설정** 서브 섹션을 선택합니다.
7. **템플릿** 섹션에서 **도움말** 버튼을 누릅니다.
   이것은 **인증 에이전트 도움말 메시지** 창을 엽니다.

8. 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.

9. 도움말 메시지를 편집합니다.
   원본 텍스트를 복원하려면 **기본값** 버튼을 누릅니다.

10. **확인**을 누릅니다.

11. 변경 사항을 저장하려면, **속성: <정책 이름>** 창에서 **확인**을 누릅니다.

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 에이전트 추적 레벨 선택

애플리케이션이 인증 에이전트의 작동에 대한 정보 및 인증 에이전트를 통한 사용자 작업에 대한 정보를 추적 파일 내에 기록합니다. 인증 에이전트 추적 파일은 암호화된 하드 드라이브에 대한 데이터 복원을 해야 할 때 매우 유용합니다.

인증 에이전트 추적 레벨을 선택하려면:

1. 암호화된 하드 드라이브가 있는 컴퓨터가 시작되자마자 **F3** 버튼을 눌러 인증 에이전트 설정을 구성하기 위한 창을 호출합니다.
2. 인증 에이전트 설정 창에서 추적 레벨을 선택합니다:
   - **디버그 로깅 중지(기본 설정)**. 이 옵션을 선택하면 애플리케이션이 추적 로그 파일에 인증 에이전트 이벤트에 대한 정보를 기록하지 않습니다.
   - **디버그 로깅 작동**. 이 옵션이 선택되어 있으면 애플리케이션에 인증 에이전트의 작동 및 인증 에이전트와 함께 수행되는 사용자 작동에 대한 정보가 기록됩니다.
   - **verbose 로깅 작동**. 이 옵션이 선택되어 있으면 애플리케이션에 인증 에이전트의 작동 및 인증 에이전트와 함께 수행되는 사용자 작동에 대한 자세한 정보가 기록됩니다.

     이 옵션 상태에서는 항목의 세부 레벨이 **디버그 로깅 활성** 옵션의 수준보다 높습니다. 높은 수준의 항목 세부 레벨이 인증 에이전트 및 운영 체제의 시작 속도를 저하시킬 수 있습니다.

   - **디버그 로깅 작동 및 직렬 포트 선택**. 이 옵션이 선택되어 있으면 애플리케이션에 인증 에이전트의 작동 및 인증 에이전트와 함께 수행되는 사용자 동작에 대한 정보가 추적로그 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 디버그 로깅 작동 및 직렬 포트 선택**. 이 옵션이 선택되어 있으면 애플리케이션에 인증 에이전트의 작동 및 인증 에이전트와 함께 수행되는 사용자 동작에 대한 세부 정보가 추적로그 파일에 기록되며 COM 포트를 통해 이를 릴레이합니다.

     이 옵션 상태에서는 항목의 세부 레벨이 **디버그 로깅 활성 및 시리얼 포트 선택** 옵션의 수준보다 높습니다. 높은 수준의 항목 세부 레벨이 인증 에이전트 및 운영 체제의 시작 속도를 저하시킬 수 있습니다.

컴퓨터에 암호화된 하드 드라이브가 있는 경우 또는 하드 드라이브의 암호화 중에는 데이터가 인증 에이전트 추적 파일에 기록됩니다.

인증 에이전트 추적 파일은 애플리케이션의 다른 추적 파일과는 다르게 Kaspersky로 전송되지 않습니다. 필요하다면 시스템 관리자가 인증 에이전트 추적 파일을 분석을 위해 Kaspersky에 수동으로 전송할 수 있습니다.

인증 에이전트 계정 관리

다음과 같은 Kaspersky Security Center 툴을 사용하여 인증 에이전트의 계정을 관리할 수 있습니다:

- 인증 에이전트 계정을 관리하기 위한 그룹 작업. 클라이언트 컴퓨터의 그룹에 대해 인증 에이전트 계정을 관리할 수 있습니다.
- **암호화(계정 관리)** 로컬 작업. 개별 클라이언트 컴퓨터에 대해 인증 에이전트 계정을 관리할 수 있습니다.

인증 에이전트 계정 관리 작업의 설정을 구성하려면 다음을 수행합니다:

1. 인증 에이전트 계정 관리 작업 만들기 (로컬 작업 만들기, 그룹 작업 만들기).
2. 다음에서 **설정** 섹션을 엽니다. **속성: <인증 에이전트 계정 관리 작업 이름>** 창.
3. 인증 에이전트 계정 생성을 위한 명령 추가.
4. 인증 에이전트 계정 편집을 위한 명령 추가.
5. 인증 에이전트 사용자 계정 삭제를 위한 명령 추가.
6. 필요할 경우 인증 에이전트 계정 관리를 위해 추가된 명령을 편집합니다. 그러려면 **인증 에이전트 계정 관리 명령** 표에서 명령을 선택한 다음 **편집** 버튼을 누릅니다.
7. 필요할 경우 인증 에이전트 계정 관리를 위해 추가된 명령을 삭제합니다. 그러려면 **인증 에이전트 계정 관리 명령:** 표에서 명령을 하나 이상 선택한 다음 **편집** 버튼을 누릅니다.

   표에서 여러 항목을 선택하려면 `Ctrl` 키를 누른 상태에서 이벤트를 선택합니다.

8. 변경 사항을 저장하려면 작업 속성 창에서 **확인**을 누릅니다.
9. 작업을 실행합니다.

작업에 추가된 인증 에이전트 계정 관리 명령이 실행됩니다.

인증 에이전트 계정 생성을 위한 명령 추가

인증 에이전트 계정 생성을 위한 명령을 추가하려면:

1. 다음에서 **설정** 섹션을 엽니다. **속성: <인증 에이전트 계정 관리 작업 이름>** 창.
2. **추가** 버튼을 누르고 드롭다운 목록에서 **계정 추가 명령**을 선택합니다.

   사용자 계정 추가 창이 열립니다.
3. **Windows 계정** 창에 있는 **사용자 계정 추가** 필드에 인증 에이전트 계정 생성 시 이용할 Microsoft Windows 계정 이름을 지정합니다.

   계정 이름을 직접 입력하거나 **선택** 버튼을 누릅니다.
4. Microsoft Windows 계정을 직접 입력한 경우 **허용** 버튼을 눌러 사용자 계정의 보안 식별자(SID)를 정합니다.

   허용 버튼을 눌러 보안 식별자(SID)를 정하지 않으면, 컴퓨터에서 해당 작업이 수행될 때 보안 식별자(SID)가 정해집니다.

인증 에이전트 계정 생성 명령을 추가할 때 Microsoft Windows 계정의 SID를 정하면 입력된 Microsoft Windows 계정 이름이 올바른지 확인할 수 있어 편리합니다. 입력된 Microsoft Windows 사용자 계정이 존재하지 않거나 신뢰하지 않는 도메인에 속하거나 **암호화(계정 관리)** 로컬 작업이 수정된 컴퓨터에 존재하지 않을 경우, 인증 에이전트 관리 작업은 오류가 발생하고 종료됩니다.

5. 인증 에이전트에 대해 이전에 생성된 동일한 이름의 계정을 새로 생성되는 계정으로 교체하려면 **현재 사용자 계정 변경** 확인란을 선택합니다.

인증 에이전트 계정 관리를 위한 그룹 작업의 속성에 인증 에이전트 계정 생성 명령을 추가할 때 이 단계가 제공됩니다. **암호화(계정 관리)** 로컬 작업의 속성에 인증 에이전트 계정 생성 명령을 추가할 때는 이 단계가 제공되지 않습니다.

6. **사용자 이름** 필드에 암호화된 하드 드라이브 접근을 위한 인증에서 입력해야 하는 인증 에이전트 계정의 이름을 입력합니다.

7. 인증 중에 암호화된 하드 드라이브에 접근하기 위해서는 인증 에이전트 계정 암호를 입력해야 한다는 메시지를 애플리케이션에서 표시하게 하려면 **암호 기반 인증 허용** 확인란을 선택하십시오.

8. 이전 단계에서 **암호 기반 인증 허용** 확인란을 선택한 경우 다음을 수행합니다:

   a. **암호** 필드에 암호화된 하드 드라이브 접근을 위한 인증에서 입력해야 하는 인증 에이전트 계정의 암호를 입력합니다.

   b. **암호 확인** 필드에 이전 단계에서 입력한 인증 에이전트 계정 암호를 입력합니다.

   c. 다음 중 하나를 수행합니다:

   - 인증 과정에서 최초로 사용자가 명령에 지정된 계정을 사용할 경우 애플리케이션에서 암호 변경 메시지를 표시하게 하려면 **최초 인증 시 암호 변경** 옵션을 선택합니다.
   - 또는 **암호를 변경하지 않음** 옵션을 선택합니다.

9. 인증 중에 암호화된 하드 드라이브에 접근하기 위해 토큰이나 스마트 카드를 이용해야 한다는 메시지를 애플리케이션에서 표시하게 하려면 **인증서 기반 인증 허용** 확인란을 선택하십시오.

10. 이전 단계에서 **인증서 기반 인증 허용** 확인란을 선택한 경우 **찾아보기** 버튼을 누르고 **인증서 파일 선택** 창에서 토큰 또는 스마트 카드 전자 인증서 파일을 선택합니다.

11. 필요하다면, **명령 설명** 필드에 명령 관리를 위한 자세한 인증 에이전트 계정 정보를 입력합니다.

12. 다음 중 하나를 수행합니다:

    - 사용자가 명령에 지정된 계정을 사용하여 인증 에이전트의 인증 대화 상자에 액세스하게 하려면 **인증 허용** 확인란을 선택합니다.
    - 사용자가 명령에 지정된 계정을 사용하여 인증 에이전트의 인증 대화 상자에 액세스할 수 없게 하려면 **인증 차단** 확인란을 선택합니다.

13. **사용자 계정 추가** 창에서 **확인**을 누릅니다.

인증 에이전트 계정 편집 명령 추가

인증 에이전트 계정 편집을 위한 명령을 추가하려면:

1. **설정** 섹션(**속성: <인증 에이전트 계정 관리 작업 이름>** 창)에서 **추가** 버튼의 컨텍스트 메뉴를 열고 **계정 편집 명령** 항목을 선택합니다.

   사용자 계정 편집 창이 열립니다.

2. **사용자 계정 편집** 창의 **Windows 계정** 필드에 편집할 인증 에이전트 계정이 생성된 Microsoft Windows 사용자 계정 이름을 지정합니다. 계정 이름을 직접 입력하거나 **선택** 버튼을 누릅니다.

3. Microsoft Windows 사용자 계정을 직접 입력한 경우 **허용** 버튼을 눌러 사용자 계정의 보안 식별자(SID)를 정합니다.

   허용 버튼을 눌러 보안 식별자(SID)를 정하지 않으면, 컴퓨터에서 해당 작업이 수행될 때 보안 식별자(SID)가 정해집니다.

   > 인증 에이전트 계정 편집 명령을 추가할 때 Microsoft Windows 사용자 계정의 SID를 정하면 입력된 Microsoft Windows 사용자 계정 이름이 올바른지 확인할 수 있어 편리합니다. 입력된 Microsoft Windows 사용자 계정이 존재하지 않거나 신뢰하지 않는 도메인에 속할 경우, 인증 에이전트 계정 관리를 위한 그룹 작업은 오류가 발생하고 종료됩니다.

4. **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.

5. **암호 기반 인증 설정 변경** 확인란을 선택하여 암호 기반 인증 설정을 편집 가능하게 만듭니다.

6. 인증 중에 암호화된 하드 드라이브에 접근하기 위해서는 인증 에이전트 계정 암호를 입력해야 한다는 메시지를 애플리케이션에서 표시하게 하려면 **암호 기반 인증 허용** 확인란을 선택하십시오.

7. 이전 단계에서 **암호 기반 인증 허용** 확인란을 선택한 경우 다음을 수행합니다:

   a. **암호** 필드에 인증 에이전트 계정의 새 암호를 입력합니다.

   b. **암호 확인** 필드에 이전 단계에서 입력한 암호를 입력합니다.

8. **Windows 계정** 필드에 지정된 이름의 Microsoft Windows 계정에 따라 생성된 모든 인증 에이전트 계정에 대해 암호 변경 설정의 값을 아래 지정된 설정 값으로 변경하려면 **인증 에이전트에서 인증 시 암호 변경 규칙 편집** 확인란을 선택합니다.

9. 인증 에이전트에서 인증 시 암호 변경 설정의 값을 지정합니다.

10. **인증서 기반 인증 설정 변경** 확인란을 선택하여 토큰 또는 스마트 카드의 전자 인증서 기반 인증 설정을 편집 가능하게 만듭니다.

11. 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.

12. 이전 단계에서 **인증서 기반 인증 허용** 확인란을 선택한 경우 **찾아보기** 버튼을 누르고 **인증서 파일 선택** 창에서 토큰 또는 스마트 카드 전자 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. **사용자 계정 편집** 창에서 **확인**을 누릅니다.

인증 에이전트 계정 삭제를 위한 명령 추가

인증 에이전트 계정 삭제를 위한 명령을 추가하려면 다음과 같이 진행합니다:

1. **설정** 섹션(**속성: <인증 에이전트 계정 관리 작업 이름>** 창)에서 **추가** 버튼의 마우스 오른쪽 메뉴를 열고 **계정 삭제 명령**을 선택합니다.

   사용자 계정 삭제 창이 열립니다.

2. **사용자 계정 삭제** 창의 **Windows 계정** 필드에 편집할 인증 에이전트 계정이 생성된 Microsoft Windows 사용자 계정 이름을 지정합니다. 계정 이름을 직접 입력하거나 **선택** 버튼을 누릅니다.

3. Microsoft Windows 사용자 계정을 직접 입력한 경우 **허용** 버튼을 눌러 사용자 계정의 보안 식별자(SID)를 정합니다.

   허용 버튼을 눌러 보안 식별자(SID)를 정하지 않으면, 컴퓨터에서 해당 작업이 수행될 때 보안 식별자(SID)가 정해집니다.

   > 인증 에이전트 계정 삭제 명령을 추가할 때 Microsoft Windows 사용자 계정의 SID를 정하면 입력된 Microsoft Windows 사용자 계정 이름이 올바른지 확인할 수 있어 편리합니다. 입력된 Microsoft Windows 사용자 계정이 존재하지 않거나 신뢰하지 않는 도메인에 속할 경우, 인증 에이전트 계정 관리를 위한 그룹 작업은 오류가 발생하고 종료됩니다.

4. **사용자 계정 삭제** 창에서 **확인**을 누릅니다.

인증 에이전트 계정 자격 증명 복원

> Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터 사용자를 위한 안내입니다.

인증 에이전트 계정의 사용자 이름 및 암호 복원하려면:

1. 하드 드라이브가 암호화된 컴퓨터는 운영 체제가 부팅되기 전 인증 에이전트가 로드됩니다. 인증 에이전트의 인터페이스에서 **암호 분실** 버튼을 눌러 인증 에이전트 계정의 로그인 이름과 암호를 복원하는 프로세스를 시작합니다.

2. 인증 에이전트의 지침을 따라 인증 에이전트 계정의 사용자 이름과 암호를 복원하기 위한 요청 메시지를 받습니다.

3. 회사의 LAN 관리자에게 컴퓨터의 이름과 함께 차단 요청을 전달합니다.

4. LAN 관리자가 작성하여 제공한 인증 에이전트 계정 사용자 이름과 암호 복원 요청에 대한 응답 섹션을 입력합니다.

5. 인증 에이전트 계정의 새 암호를 입력하고 확인합니다.

인증 에이전트 계정의 사용자 이름과 암호 복원 요청에 대한 응답 섹션을 이용해 인증 에이전트 계정의 사용자 이름이 정의됩니다.

인증 에이전트 계정의 새 암호를 입력하고 확인하면 암호가 저장되고 암호화된 하드 드라이브에 접근할 수 있습니다.

사용자의 인증 에이전트 계정 자격 증명 복원 요청에 응답

인증 에이전트 계정 사용자 이름과 암호 복구 요청에 대한 응답 섹션을 작성하여 사용자에게 전송하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 인증 에이전트 계정의 사용자 이름과 암호 복원을 요청한 사용자의 컴퓨터가 포함된 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **기기** 탭을 선택합니다.
4. **장치** 탭에 인증 에이전트 계정의 사용자 이름과 암호 복원을 요청한 사용자의 컴퓨터가 강조 표시되면 마우스 오른쪽 버튼을 눌러 메뉴를 엽니다.
5. **오프라인 모드에서의 장치 및 데이터 접근 권한 부여** 옵션을 선택합니다.
   오프라인 모드에서의 장치 및 데이터 접근 권한 부여 창이 열립니다.
6. **오프라인 모드에서의 장치 및 데이터 접근 권한 부여** 창에서 **인증 에이전트** 탭을 선택합니다.
7. **사용 중인 암호화 알고리즘** 섹션에서 암호화 알고리즘 유형을 선택합니다.
8. **계정** 드롭다운 목록에서 인증 에이전트 계정 이름과 암호의 복원을 요청하는 사용자에 대해 생성된 인증 에이전트 계정 이름을 선택합니다.
9. **하드 드라이브** 드롭다운 목록에서 다시 접근 권한이 필요한 암호화된 하드 드라이브를 선택합니다.
10. **사용자 요청** 섹션에 사용자의 요청 내용을 입력합니다.
    사용자의 인증 에이전트 계정 사용자 및 암호 복원 요청에 대한 응답 내용이 **접근 허용 키** 필드에 표시됩니다.
11. 사용자에게 응답할 내용을 작성합니다.

데이터 암호화 상세 정보 보기

이 섹션은 데이터 암호화에 대한 상세 정보를 확인하는 방법을 설명합니다.

암호화 상태 정보

Kaspersky Endpoint Security는 진행 중인 암호화 또는 복호화에 대해 클라이언트 컴퓨터에 적용되는 암호화 파라미터의 상태에 관한 정보를 Kaspersky Security Center로 전달합니다.

암호화 상태로 다음과 같은 값이 표시될 수 있습니다:

- *정책 정의 안 됨*. 컴퓨터에 대한 Kaspersky Security Center 정책이 정의되지 않았습니다.
- *암호화/복호화 진행 중*. 컴퓨터에서 데이터 암호화 및 복호화가 진행 중입니다.
- *오류*. 컴퓨터의 데이터 암호화 / 복호화 과정에서 오류가 발생했습니다.
- *재부팅 필요*. 컴퓨터의 데이터 암호화 또는 복호화를 시작하거나 종료하려면 운영 체제를 재부팅해야 합니다.
- *정책을 준수함*. 컴퓨터에 적용된 Kaspersky Security Center 정책에 지정된 암호화 설정을 사용하여 컴퓨터의 데이터 암호화 / 복호화가 완료되었습니다.
- *사용자가 취소함*. 사용자는 이동식 드라이브에서 파일 암호화 작업에 대한 확인을 거부했습니다.
- *지원하지 않음*. 컴퓨터에서 데이터 암호화 기능을 사용할 수 없습니다.

암호화 상태 보기

컴퓨터 데이터의 암호화 상태를 보려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **기기** 탭을 선택합니다.
   작업 공간의 **장치** 탭에 선택된 관리 그룹의 컴퓨터 속성이 표시됩니다.
4. 작업 공간의 **장치** 탭에서 화면 오른쪽 끝으로 이동합니다.
   암호화 상태 열에 선택된 관리 그룹 컴퓨터의 데이터 암호화 상태가 표시됩니다. 이 상태에는 컴퓨터 로컬 드라이브의 파일 암호화, 컴퓨터 하드 드라이브 암호화 및 컴퓨터에 연결된 이동식 드라이브의 암호화에 대한 정보가 표시됩니다.

Kaspersky Security Center의 상세 정보에서 암호화 통계 보기

Kaspersky Security Center의 상세 정보에서 암호화 상태를 보려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 콘솔 트리에서 **중앙 관리 서버 – <컴퓨터 이름>** 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.
      속성: 통계 창이 열립니다.
   b. **속성: 통계** 창에서 **추가**를 누릅니다.
      속성: 새 페이지 창이 열립니다.

c. **일반** 섹션(**속성: 새 페이지** 창)에서 페이지 이름을 입력합니다.

d. **세부 패널** 섹션에서 **추가** 버튼을 누릅니다.

새 상세 정보 창이 열립니다.

e. **새 상세 정보** 창의 **보호 상태** 그룹에서 **장치 암호화** 항목을 선택합니다.

f. **확인**을 누릅니다.

속성: 암호화 제어 창이 열립니다.

g. 필요할 경우 상세 정보 설정을 편집합니다. 그러려면 **보기** 및 **장치** 섹션(**속성: 장치 암호화** 창)을 사용합니다.

h. **확인**을 누릅니다.

i. 위에 나온 d - h 단계를 반복하고 **새 상세 정보** 창의 **보호 상태** 섹션에서 **이동식 드라이브 암호화** 항목을 선택합니다.

상세 정보가 **상세 정보** 목록(**속성: 새 페이지** 창)에 나타납니다.

j. **속성: 새 페이지** 창에서 **확인**을 누릅니다.

이전 단계에서 생성된 상세 정보의 페이지 이름이 다음 **속성의 페이지 목록에 표시됩니다: 통계** 창.

k. **속성: 통계** 창에서 **닫기**를 누릅니다.

5. **통계** 탭에서 이전 단계에 생성된 페이지를 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 Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 파일 암호화 오류 목록을 볼 클라이언트 컴퓨터가 포함된 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **기기** 탭을 선택합니다.
4. **장치** 탭의 목록에서 컴퓨터 이름을 선택한 후 마우스 오른쪽 버튼을 눌러 메뉴를 엽니다.
5. 다음 중 하나를 수행합니다:
   - 컴퓨터의 마우스 오른쪽 메뉴에서 **보호**를 선택합니다.
   - 컴퓨터의 마우스 오른쪽 메뉴에서 **속성** 항목을 선택합니다. **속성: <컴퓨터 이름>** 창에서 **보호** 섹션을 선택합니다.
6. **보호** 섹션(**속성: <컴퓨터 이름>** 창)에서 **데이터 암호화 오류 목록 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

데이터 암호화 리포트를 보려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **중앙 관리 서버** 노드에서 **리포트** 탭을 선택합니다.
3. **리포트 템플릿 만들기** 버튼을 누릅니다.
   리포트 템플릿 마법사가 시작됩니다.
4. 리포트 템플릿 마법사의 안내를 따릅니다. **기타** 섹션의 **리포트 템플릿 유형 선택** 창에서 다음 항목 중 하나를 선택합니다:
   - **관리 장치 암호화 상태 리포트**.
   - **저장된 장치 데이터 암호화 리포트**.
   - **암호화 오류 리포트**.
   - **암호화된 파일 접근 차단에 대한 리포트**.

   새 마법사를 종료하면 **리포트** 탭에 표로 새 리포트 템플릿이 나타납니다.
5. 이전 안내 단계에서 만든 리포트 템플릿을 선택합니다.

리포트 생성 프로세스가 시작됩니다. 리포트가 새 창으로 표시됩니다.

제한된 파일 암호화 기능을 사용하여 암호화된 파일 관리

Kaspersky Security Center 정책이 적용되어 파일이 암호화될 때 Kaspersky Endpoint Security는 암호화된 파일에 직접 접근하기 위해 필요한 암호화 키를 수신합니다. 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 구성요소가 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.

Kaspersky Security Center에 연결하지 않고 암호화된 파일에 접근

Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터 사용자를 위한 안내입니다.

Kaspersky Security Center에 연결하지 않고 암호화된 파일에 접근하려면 다음과 같이 하십시오:

1. 필요한 암호화된 파일 접근을 시도합니다.

   Kaspersky Security Center에 연결하지 않고 컴퓨터의 로컬 드라이브에 저장된 파일 접근을 시도할 경우 Kaspersky Endpoint Security는 로컬 컴퓨터 드라이브에 저장된 모든 암호화된 파일에 대한 접근을 요청하는 파일을 생성합니다. 이동식 드라이브에 저장된 파일 접근을 시도할 경우 Kaspersky Endpoint Security는 해당 이동식 드라이브에 저장된 모든 암호화된 파일에 대한 접근을 요청하는 파일을 생성합니다. **파일 접근이 차단되었습니다** 창이 열립니다.

2. LAN 관리자에게 암호화된 파일에 대한 접근 허용 요청이 포함된 파일을 전송합니다. 그렇게 하려면, 다음 중 하나를 수행합니다:

   - LAN 관리자에게 암호화된 파일에 대한 접근 요청 파일을 이메일로 보내려면 **이메일로 전송** 버튼을 누릅니다.
   - 암호화된 파일에 대한 접근을 요청하는 파일을 저장하고 다양한 방법으로 LAN 관리자에게 그 파일을 전달하려면 **저장** 버튼을 누릅니다.

3. LAN 관리자가 생성 및 제공한 암호화된 파일 접근을 위한 키 파일을 얻습니다.

4. 다음과 같은 방법으로 암호화된 파일 접근용 키를 활성화합니다:

   - 파일 관리자에서 암호화된 파일 접근용 키 파일을 선택합니다. 두 번 눌러 파일을 엽니다.
   - 다음을 수행합니다:

     a. Kaspersky Endpoint Security 메인 창을 엽니다.

     b. 버튼을 누릅니다.
     이벤트 창이 열립니다.

     c. **복호화 상태** 탭을 선택합니다.
     이 탭에는 암호화된 파일 접근에 대한 모든 요청 목록이 표시됩니다.

     d. 암호화된 파일 접근용 키 파일을 받은 요청 사항을 선택합니다.

     e. 암호화된 파일 접근을 위해 제공된 키 파일을 로드하려면 **찾아보기**를 누릅니다.
     표준 **접근 허용 키 파일 선택** Microsoft Windows 대화 상자가 열립니다.

     f. Microsoft Windows 표준 **접근 허용 키 파일 선택** 창에서 .kesdr 확장자와 접근 요청 파일의 파일 이름과 일치하는 파일 이름을 가진 관리자 제공 파일을 선택합니다.

     g. **열기** 버튼을 누릅니다.

h. **이벤트** 창에서 **확인**을 누릅니다.

컴퓨터의 로컬 드라이브에 저장된 파일에 접근하기 위해 암호화된 파일 접근 요청 파일이 생성된 경우 Kaspersky Endpoint Security는 로컬 컴퓨터 드라이브에 저장된 모든 암호화된 파일에 대한 접근 권한을 부여합니다. 이동식 드라이브에 저장된 파일에 접근하기 위해 암호화된 파일 접근 허용 요청 파일이 생성된 경우 Kaspersky Endpoint Security는 해당 이동식 드라이브에 저장된 모든 암호화된 파일에 대한 접근 권한을 부여합니다. 다른 이동식 드라이브에 저장된 암호화된 파일에 접근하려면 각 이동식 드라이브에 대해 별도의 접근 허용 키가 필요합니다.

Kaspersky Security Center에 연결하지 않고 암호화된 파일에 대해 사용자 접근 권한 부여

Kaspersky Security Center에 연결하지 않고 암호화된 파일에 대해 사용자 접근 권한을 부여하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 암호화된 파일 접근을 요청한 사용자의 컴퓨터가 포함된 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **기기** 탭을 선택합니다.
4. **장치** 탭에서 암호화된 파일에 접근을 요청하는 사용자 소유의 컴퓨터를 선택하고 마우스 오른쪽 버튼을 눌러 메뉴를 엽니다.
5. **오프라인 모드에서의 장치 및 데이터 접근 권한 부여** 옵션을 선택합니다.
   오프라인 모드에서의 장치 및 데이터 접근 권한 부여 창이 열립니다.
6. **오프라인 모드에서의 장치 및 데이터 접근 권한 부여** 창에서 **암호화** 탭을 선택합니다.
7. **암호화** 탭에서 **찾아보기** 버튼을 누릅니다.
   표준 **접근 허용 요청 파일 선택** Microsoft Windows 대화 상자가 열립니다.
8. **접근 허용 요청 파일 선택** 창에서 사용자가 보낸 요청 파일에 대한 경로를 지정하고 **열기**를 누릅니다.
   Kaspersky Security Center가 암호화된 파일 접근을 위한 키 파일을 생성합니다. 자세한 사용자 요청 정보가 **암호화** 탭에 표시됩니다.
9. 다음 중 하나를 수행합니다:
   - 생성된 접근 키 파일을 사용자에게 이메일로 전송하려면 **이메일로 전송** 버튼을 누릅니다.
   - 암호화된 파일에 대한 접근 허용 키 파일을 저장하고 다양한 방법으로 사용자에게 해당 키 파일을 전달하려면 **저장** 버튼을 누릅니다.

암호화된 파일 접근 메시지 템플릿 편집

암호화된 파일 접근 메시지 템플릿을 편집하려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 암호화된 파일 접근 요청 메시지의 템플릿을 편집할 관리 그룹의 이름을 가진 폴더를 엽니다.

3. 작업 공간에서 **정책** 탭을 선택합니다.

4. 필요한 정책을 선택합니다.

5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:

   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

6. **데이터 암호화** 섹션에서 **일반 암호화 설정** 서브 섹션을 선택합니다.

7. **템플릿** 섹션에서 **템플릿** 버튼을 누릅니다.
   템플릿 창이 열립니다.

8. 다음을 수행합니다:

   - 사용자 메시지 템플릿을 편집하려면 **사용자 메시지** 탭을 선택합니다. 컴퓨터에 암호화된 파일 접근에 필요한 키가 없는데 사용자가 암호화된 파일에 접근을 시도할 경우 **파일 접근 거부** 창이 열립니다. **파일 접근 거부** 창에서 **이메일로 전송** 버튼을 누르면 자동으로 사용자 메시지가 생성됩니다. 이 이메일 메시지는 암호화된 파일 접근 요청과 함께 회사 LAN 관리자에게 전송됩니다.
   - 관리자 메시지 템플릿을 편집하려면 **관리자 메시지** 탭을 선택합니다. **암호화된 파일 접근 허용** 창에서 **이메일로 전송** 버튼을 누르면 메시지가 자동 생성되고 사용자에게 암호화된 파일 접근 권한이 부여된 후 이메일이 전송됩니다.

9. 메시지 템플릿을 편집합니다.
   기본값 버튼 및 **변수** 드롭다운 목록을 사용할 수 있습니다.

10. **확인**을 누릅니다.

11. 변경 사항을 저장하려면, **속성: <정책 이름>** 창에서 **확인**을 누릅니다.

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 구성요소가 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 메타 데이터가 손상된 경우 접근 허용 요청 파일을 사용하여 복원 절차를 완료해야 합니다.

암호화된 장치에 저장된 데이터를 복원하기 전에 이 작업을 수행할 컴퓨터에서 Kaspersky Security Center 암호화 정책을 취소하는 것이 좋습니다. 그래야만 드라이브가 다시 암호화되지 않습니다.

애플리케이션 인터페이스를 통해 암호화된 장치 접근 권한 얻기

Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터 사용자를 위한 안내입니다.

애플리케이션 인터페이스를 통해 암호화된 장치 접근 권한을 얻으려면 다음과 같이 하십시오:

1. 필요한 암호화된 장치에 접근을 시도합니다.
   암호화 데이터 접근 차단 창이 열립니다.

2. 회사 LAN 관리자에게 kesdc 확장자를 사용하는 암호화된 장치에 대한 접근 허용 요청 파일을 보냅니다. 그렇게 하려면, 다음 중 하나를 수행합니다:

   - 회사 LAN 관리자에게 암호화된 장치에 대해 생성된 접근 허용 요청 파일을 이메일로 전송하려면 **이메일로 전송** 버튼을 누릅니다.
   - 암호화된 장치에 대한 접근 허용을 요청하는 파일을 저장하고 다양한 방법으로 회사 LAN 관리자에게 그 파일을 전달하려면 **저장** 버튼을 누릅니다.

   접근 허용 요청 파일을 저장하거나 회사 LAN 관리자에게 파일을 전송하지 않은 채로 **암호화 데이터 접근 차단** 창을 닫은 경우 **이벤트** 창의 **복호화 상태** 탭에서 언제든지 파일을 저장하거나 전송할 수 있습니다. 이 창을 열려면 메인 애플리케이션 창에서 버튼을 누릅니다.

3. 회사 LAN 관리자가 생성하여 사용자에게 제공한 암호화된 장치 접근 허용 키 파일을 받아서 저장합니다.

4. 암호화된 장치에 접근하기 위해 접근 허용 키를 적용하려면 다음 방법 중 하나를 사용합니다:

   - 파일 관리자에서 암호화된 장치 접근 허용 키 파일을 찾아서 파일을 두 번 눌러서 엽니다.
   - 다음을 수행합니다:

     a. Kaspersky Endpoint Security 메인 창을 엽니다.

     b. 버튼을 누르면 **이벤트** 창이 열립니다.

     c. **복호화 상태** 탭을 선택합니다.
     이 탭에는 암호화된 파일 및 장치 접근에 대한 모든 요청 목록이 표시됩니다.

     d. 암호화된 장치에 접근하기 위해 필요한 접근 허용 키 파일을 받은 요청 사항을 선택합니다.

     e. 암호화된 장치 접근을 위해 받은 키 파일을 로드하려면 **찾아보기**를 누릅니다.
     표준 **접근 허용 키 파일 선택** Microsoft Windows 대화 상자가 열립니다.

     f. Microsoft Windows 표준 **접근 허용 키 파일 선택** 창에서 kesdr 확장자와 암호화된 장치에 대한 해당 접근 허용 요청 파일의 파일 이름과 일치하는 파일 이름을 가진 관리자 제공 파일을 선택합니다.

     g. **열기** 버튼을 누릅니다.

     h. **복호화 상태** 창에서 **확인**을 누릅니다.

Kaspersky Endpoint Security가 암호화된 장치에 대한 접근 권한을 부여합니다.

사용자에게 암호화된 장치 접근 권한 부여

사용자에게 암호화된 장치 접근 권한을 부여하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 암호화된 장치 접근을 요청한 사용자의 컴퓨터가 포함된 관리 그룹의 이름을 가진 폴더를 엽니다.

3. 작업 공간에서 **기기** 탭을 선택합니다.

4. **장치** 탭에서 암호화된 장치에 접근을 요청하는 사용자 소유의 컴퓨터를 선택하고 마우스 오른쪽 버튼을 눌러 메뉴를 엽니다.

5. **오프라인 모드에서의 장치 및 데이터 접근 권한 부여** 옵션을 선택합니다.
   오프라인 모드에서의 장치 및 데이터 접근 권한 부여 창이 열립니다.

6. **오프라인 모드에서의 장치 및 데이터 접근 권한 부여** 창에서 **암호화** 탭을 선택합니다.

7. **암호화** 탭에서 **찾아보기** 버튼을 누릅니다.
   표준 **접근 허용 요청 파일 선택** Microsoft Windows 대화 상자가 열립니다.

8. **접근 허용 요청 파일 선택** 창에서 사용자로부터 받은 kesdc 확장자를 사용하는 요청 파일의 경로를 지정합니다.

9. **열기** 버튼을 누릅니다.
   Kaspersky Security Center가 kesdr 확장자를 사용하는 암호화된 장치 접근 허용 키 파일을 생성합니다. 자세한 사용자 요청 정보가 **암호화** 탭에 표시됩니다.

10. 다음 중 하나를 수행합니다:

    - 생성된 접근 키 파일을 사용자에게 이메일로 전송하려면 **이메일로 전송** 버튼을 누릅니다.
    - 암호화된 장치용 접근 허용 키 파일을 저장하고 다른 방법으로 사용자에게 키 파일을 전달하려면 **저장** 버튼을 누릅니다.

사용자에게 BitLocker 기술로 암호화된 하드 드라이브에 대한 복구 키 제공

사용자에게 BitLocker 기술로 암호화된 시스템 하드 드라이브에 대한 복구 키를 전송하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 암호화된 드라이브 접근을 요청한 사용자의 컴퓨터가 포함된 관리 그룹의 이름을 가진 폴더를 엽니다.

3. 작업 공간에서 **기기** 탭을 선택합니다.

4. **장치** 탭에서 암호화된 드라이브 접근을 요청한 사용자의 컴퓨터를 선택합니다.

5. 마우스 오른쪽 메뉴를 열고 **오프라인 모드에서의 장치 및 데이터 접근 권한 부여**를 선택합니다.
   오프라인 모드에서의 장치 및 데이터 접근 권한 부여 창이 열립니다.

6. **오프라인 모드에서의 장치 및 데이터 접근 권한 부여** 창에서 **BitLocker로 보호된 시스템 드라이브에 접근**탭을 선택합니다.

7. 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.

8. 사용자에게 **복구 키** 필드에 표시된 키를 전송합니다.

사용자에게 BitLocker 기술로 암호화된 비시스템 하드 드라이브에 대한 복구 키를 전송하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리에서 **고급 → 암호화 및 데이터 보호 → 암호화된 장치** 폴더를 선택합니다.
   작업 공간에 암호화된 장치의 목록이 표시됩니다.
3. 작업 공간에서 접근을 복원해야 하는 암호화된 장치를 선택합니다.
4. 마우스 오른쪽 버튼을 눌러 메뉴를 열고 **지정한 암호화 장치에 대한 접근 허용 키 가져오기**를 선택합니다.
   BitLocker로 암호화된 드라이브로의 접근 복원 창이 열립니다.
5. 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.

6. 사용자에게 **복구 키** 필드에 표시된 키를 전송합니다.

복원 유틸리티의 실행 파일 생성

Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터 사용자를 위한 안내입니다.

복원 유틸리티의 실행 파일을 생성하려면:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 왼쪽 하단의 버튼을 눌러 **지원** 창을 엽니다.
3. **지원** 창에서 **암호화된 장치 복원** 버튼을 누릅니다.
   암호화된 장치 복원 유틸리티가 시작됩니다.
4. 복원 유틸리티 창에서 **독립 실행형 복원 유틸리티 생성** 버튼을 누릅니다.
   독립 실행형 복원 유틸리티 생성 창이 열립니다.
5. **저장** 창에서 복원 유틸리티의 실행 파일을 저장할 폴더의 경로를 직접 입력하거나 **찾아보기** 버튼을 누릅니다.
6. **독립 실행형 복원 유틸리티 생성** 창에서 **확인**을 누릅니다.
   복원 유틸리티의 실행 파일(fdert.exe)이 선택된 폴더에 저장됩니다.

복원 유틸리티를 사용하여 암호화된 장치에 있는 데이터 복원하기

Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터 사용자를 위한 안내입니다.

복원 유틸리티를 사용하여 암호화된 드라이브에 대한 접근을 복원하려면 다음과 같이 하십시오:

1. 다음 중 한 방법으로 복원 유틸리티를 실행합니다:

   - Kaspersky Endpoint Security 메인 창의 버튼을 눌러 **지원** 창을 열고 **암호화된 장치 복원** 버튼을 누릅니다.
   - 복원 유틸리티의 fdert.exe 실행 일을 실행합니다. 이 파일은 Kaspersky Endpoint Security에 의해 생성되었습니다.

2. 복원 유틸리티 창의 **장치 선택** 드롭다운 목록에서 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. 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 수집하는 과정이 크게 단축될 수 있습니다.

5. 진단 결과에 따라 **잠금 해제** 또는 **복호화** 버튼을 누릅니다.

   장치 잠금 해제 설정 또는 **장치 복호화 설정** 창이 열립니다.

6. 인증 에이전트 계정을 사용하여 데이터를 복원하려면 다음과 같이 합니다:

   a. **인증 에이전트 계정 설정 사용** 옵션을 선택합니다.

   b. **이름** 및 **암호** 필드에 인증 에이전트 계정 자격 증명을 지정합니다.

   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.

7. 접근 허용 키를 사용해 데이터를 복원하려면 다음과 같이 합니다:

   a. **수동으로 장치 접근 허용 키 지정** 옵션을 선택합니다.

   b. **접근 허용 키 받기** 버튼을 누릅니다.

   c. **장치 접근 허용 키 받기** 창이 열립니다.

   d. **저장** 버튼을 누르고 fdertc 확장자를 사용하는 접근 허용 요청 파일을 저장할 폴더를 선택합니다.

   e. 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.

   f. 회사 LAN 관리자가 생성하여 사용자에게 제공한 접근 허용 키 파일을 받아서 저장합니다.

   g. **가져오기** 버튼을 누르고 창이 열리면 fdertr 확장자를 사용하는 접근 허용 키 파일을 선택합니다.

8. 장치를 복호화하는 경우 **장치 복호화 설정** 창에서 나머지 복호화 설정 또한 지정해야 합니다. 이를 위해서는 다음과 같이 하십시오:

- 복호화할 영역 지정:
  - 장치 전체를 복호화하려면 **전체 장치 복호화** 옵션을 선택합니다.
  - 장치의 데이터 부분을 복호화하려면 **개별 장치 영역 복호화** 옵션을 선택하고 **시작** 및 **끝** 필드를 사용해 복호화 영역 경계를 지정합니다.
- 복호화된 데이터를 쓸 위치 선택:
  - 원본 장치의 데이터가 복호화된 데이터로 덮어쓰기 되도록 하려면 **복호화 이후에 파일로 데이터 저장** 확인란을 선택 취소합니다.
  - 암호화된 원본 데이터와는 별도로 복호화된 데이터를 저장하려면 **복호화 이후에 파일로 데이터 저장** 확인란을 선택하고 **찾아보기** 버튼을 사용해 데이터를 저장할 경로를 지정합니다.

9. **확인**을 누릅니다.

장치 차단 해제/복호화 과정이 시작됩니다.

사용자의 암호화된 장치에 저장된 데이터 복원 요청에 응답

암호화된 장치 접근을 위한 키를 생성하여 사용자에게 전송하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리에서 **고급 → 암호화 및 데이터 보호 → 암호화된 장치** 폴더를 선택합니다.
3. 작업 공간에서 접근 허용 키 파일을 생성할 암호화된 장치를 선택하고 장치 마우스 오른쪽 메뉴에서 **지정한 암호화 장치에 대한 접근 허용 키 받기**를 선택합니다.

   > 어느 컴퓨터에서 접근 허용 요청 파일이 생성되었는지 확실하지 않은 경우 관리 콘솔 트리에서 **고급 → 암호화 및 데이터 보호** 폴더를 선택하고 작업 공간에서 **장치 암호화 키 받기** 링크를 누릅니다.

   장치 접근 허용 창이 열립니다.
4. 사용하는 암호화 알고리즘을 선택합니다. 이렇게 하려면 다음 옵션 중 하나를 선택하십시오:
   - **AES256**, 기기가 암호화된 컴퓨터의 aes256 폴더에 있는 배포 패키지에서 Kaspersky Endpoint Security를 설치한 경우;
   - **AES56**, 기기가 암호화된 컴퓨터의 aes56 폴더에 있는 배포 패키지에서 Kaspersky Endpoint Security를 설치한 경우;
5. **찾아보기** 버튼을 누릅니다.

   표준 **접근 허용 요청 파일 선택** Microsoft Windows 대화 상자가 열립니다.
6. **접근 허용 요청 파일 선택** 창에서 사용자로부터 받은 fdertc 확장자를 사용하는 요청 파일의 경로를 지정합니다.
7. **열기** 버튼을 누릅니다.

   Kaspersky Security Center가 암호화된 장치 접근을 위해 fdertr 확장자를 사용하는 접근 허용 키 파일을 생성합니다.

8. 다음 중 하나를 수행합니다:

   - 생성된 접근 키 파일을 사용자에게 이메일로 전송하려면 **이메일로 전송** 버튼을 누릅니다.
   - 암호화된 장치용 접근 허용 키 파일을 저장하고 다른 방법으로 사용자에게 키 파일을 전달하려면 **저장** 버튼을 누릅니다.

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 설치.
3. 컴퓨터를 데이터 암호화 과정에서 해당 컴퓨터를 제어했던 Kaspersky Security Center 중앙 관리 서버와 연결합니다.

운영 체제 장애가 발생하기 전과 동일한 조건으로 암호화된 데이터에 대한 접근 권한이 부여됩니다.

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:

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.

네트워크 보호

이 섹션에는 네트워크 트래픽 감시에 관한 정보 및 감시 네트워크 포트의 설정을 구성하는 방법에 대한 지침이 나와 있습니다.

네트워크 보호 정보

Kaspersky Endpoint Security의 작동 중에 메일 안티 바이러스, 웹 안티 바이러스, 메신저 안티 바이러스와 같은 구성요소는 특정 프로토콜 및 특정 TCP 및 UDP 포트를 통해 송신되는 데이터 스트림을 감시합니다. 예를 들어 메일 안티 바이러스는 SMTP를 통해 전송된 데이터를 감시하고 웹 안티 바이러스는 HTTP 및 FTP를 통해 전송된 데이터를 검사합니다.

Kaspersky Endpoint Security는 위협을 받을 수 있는 가능성을 바탕으로 운영 체제의 TCP 및 UDP 포트를 여러 그룹으로 세분합니다. 일부 네트워크 포트는 취약할 수 있는 서비스에 예약됩니다. 이러한 포트는 공격을 받을 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 해당 포트와 애플리케이션은 메일 안티 바이러스, 웹 안티 바이러스 및 메신저 안티 바이러스 구성요소가 네트워크 트래픽을 감시할 때 요주의 감시 대상이 됩니다.

네트워크 트래픽 감시의 설정 구성

다음 처리를 수행하여 네트워크 트래픽 감시 설정을 구성할 수 있습니다:

- 모든 네트워크 포트의 감시를 작동합니다.
- 감시하는 네트워크 포트 목록을 만듭니다.
- 모든 네트워크 포트에 대한 감시를 받을 애플리케이션 목록 만들기.

모든 네트워크 포트의 감시 작동

모든 네트워크 포트의 감시를 작동하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **감시하는 포트** 섹션에서 **모든 네트워크 포트 감시**를 선택합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

감시하는 네트워크 포트 목록 만들기

감시하는 네트워크 포트 목록을 만들려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **감시하는 포트** 섹션에서 **선택한 포트만 감시**를 선택합니다.
4. **설정** 버튼을 누릅니다.
   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.
5. 네트워크 포트 목록에서 다음을 수행합니다:
   - 감시하는 네트워크 포트에 포함할 네트워크 포트에 해당하는 확인란을 선택합니다.
     기본적으로 **네트워크 포트** 창에 나열된 모든 네트워크 포트의 확인란이 선택되어 있습니다.
   - 감시하는 네트워크 포트에서 예외할 네트워크 포트에 해당하는 확인란을 선택 취소합니다.
6. 원하는 네트워크 포트가 목록에 표시되지 않는 경우, 다음 방법을 사용하여 추가합니다:
   a. 네트워크 포트 목록에서 **추가** 링크를 눌러 **네트워크 포트** 창을 엽니다.
   b. **포트** 필드에 네트워크 포트 번호를 입력합니다.
   c. **설명** 필드에 네트워크 포트 이름을 입력합니다.
   d. **확인**을 누릅니다.
      네트워크 포트 창이 닫힙니다. 새로 추가한 네트워크 포트는 네트워크 포트 목록 끝에 표시됩니다.
7. **네트워크 포트** 창에서 **확인**을 누릅니다.
8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

FTP 프로토콜이 Passive 모드에서 실행 중이면, 연결은 감시하는 네트워크 포트 목록에 추가 안 된 랜덤 네트워크 포트를 사용해 연결됩니다. 이러한 연결을 보호하기 위해 **감시하는 포트**에서 **모든 네트워크 포트 감시** 확인란을 선택하거나 FTP 연결을 하는 애플리케이션에 대해 모든 포트를 감시하도록 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. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.

3. **감시하는 포트** 섹션에서 **선택한 포트만 감시**를 선택합니다.

4. **설정** 버튼을 누릅니다.
   네트워크 포트 창이 열립니다.

5. **지정한 애플리케이션의 모든 포트 감시** 확인란을 선택합니다.

6. **지정한 애플리케이션의 모든 포트 감시** 확인란 아래의 애플리케이션 목록에서 다음을 수행합니다:

   - 모든 네트워크 포트에 대한 감시를 받을 애플리케이션 이름 옆에 있는 확인란을 선택합니다.
     기본적으로 **네트워크 포트** 창에 나열된 모든 애플리케이션 옆의 확인란이 선택되어 있습니다.

   - 모든 네트워크 포트에 대한 감시를 받지 않을 애플리케이션은 이름 옆에 있는 확인란을 선택 취소합니다.

7. 감시할 애플리케이션이 목록에 없는 경우 다음과 같은 방법으로 추가합니다:

   a. 애플리케이션 목록에서 **추가** 링크를 누르고 마우스 오른쪽 메뉴를 엽니다.

   b. 마우스 오른쪽 메뉴에서 애플리케이션 목록에 애플리케이션을 추가할 방법을 선택합니다:

      - 컴퓨터에 설치된 애플리케이션 목록에서 애플리케이션을 선택하려면 **애플리케이션** 명령을 선택합니다. 애플리케이션 이름을 지정할 수 있는 **애플리케이션 선택** 창이 열립니다.

      - 애플리케이션의 실행 파일 위치를 지정하려면 **찾아보기** 명령을 선택합니다. 애플리케이션 실행 파일의 이름을 지정할 수 있는 Microsoft Windows의 표준 **열기** 창이 열립니다.

      애플리케이션을 선택하면 **애플리케이션** 창이 열립니다.

   c. **이름** 필드에 선택 애플리케이션의 이름을 입력합니다.

   d. **확인**을 누릅니다.
      애플리케이션 창이 닫힙니다. 추가한 애플리케이션이 애플리케이션 목록 끝에 나타납니다.

8. **네트워크 포트** 창에서 **확인**을 누릅니다.

9. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트

이 섹션에는 데이터베이스 및 애플리케이션 모듈 업데이트("업데이트"라고도 함)에 대한 정보와 업데이트 설정을 구성하는 방법에 대한 지침이 들어 있습니다.

데이터베이스 및 애플리케이션 모듈 업데이트 정보

Kaspersky Endpoint Security의 데이터베이스 및 애플리케이션 모듈을 업데이트함으로써 컴퓨터를 최신 상태로 보호할 수 있습니다. 전 세계적으로 날마다 수많은 신종 바이러스 및 기타 형태의 악성 애플리케이션이 나타나고 있습니다. Kaspersky Endpoint Security 데이터베이스에는 보안위협에 대한 정보와 이를 처리하는 방법이 포함되어 있습니다. 보안위협을 신속하게 탐지하려면 데이터베이스 및 애플리케이션 모듈을 정기적으로 업데이트해야 합니다.

정기적인 업데이트는 유효한 라이센스를 요구합니다. 활성화된 라이센스가 없는 경우 업데이트를 한 번만 수행할 수 있습니다.

Kaspersky Endpoint Security의 주요 업데이트 경로는 Kaspersky 업데이트 서버입니다.

Kaspersky 업데이트 서버에서 업데이트 패키지를 성공적으로 다운로드하려면 컴퓨터를 인터넷에 연결해야 합니다. 기본적으로 인터넷 연결 설정은 자동으로 결정됩니다. 프록시 서버를 사용하는 경우 연결 설정을 조정 해야 합니다.

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 구성요소는 이 정보를 사용하여 컴퓨터에서 감염된 파일을 검색하고 치료합니다. 데이터베이스는 신종 보안위협 레코드와 그 대응 방법으로 계속 업데이트됩니다. 데이터베이스를 정기적으로 업데이트하는 것이 좋습니다.

  Kaspersky Endpoint Security 데이터베이스 외에도 애플리케이션 구성요소가 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.

도움말 파일은 애플리케이션 모듈 업데이트와 함께 업데이트될 수 있습니다.

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 메인 애플리케이션 창의 **보호 및 제어** 탭에 있는 **작업** 섹션의 **업데이트**에 표시됩니다.

업데이트 결과와 업데이트 작업 동안 발생한 모든 이벤트에 대한 정보는 Kaspersky Endpoint Security 리포트에 기록됩니다.

업데이트 경로 정보

*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.

업데이트 설정 구성

다음 처리 방법을 수행하여 업데이트 설정을 구성할 수 있습니다:

- 새 업데이트 경로를 추가합니다.

  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.

  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.

  > 업데이트 경로로 LAN 외부 리소스를 선택한 경우 업데이트하려면 인터넷 연결이 필요합니다.

- Kaspersky 업데이트 서버의 지역을 선택합니다.

  Kaspersky 업데이트 서버를 업데이트 경로로 사용하는 경우 업데이트 패키지를 다운로드하는 데 사용된 Kaspersky 업데이트 서버의 위치를 선택할 수 있습니다. Kaspersky 업데이트 서버는 여러 국가에 있습니다. 가장 가까운 위치에 있는 Kaspersky 업데이트 서버를 사용하면 업데이트 패키지를 가져오는 데 소요되는 시간을 줄일 수 있습니다.

  기본적으로 애플리케이션은 운영 체제 레지스트리에 있는 지역 정보를 사용합니다.

- 공유 폴더에서 Kaspersky Endpoint Security의 업데이트를 구성합니다.

  LAN에 연결된 컴퓨터가 공유 폴더에서 Kaspersky Endpoint Security를 업데이트하도록 구성하면 네트워크 트래픽을 줄일 수 있습니다. 그러려면 LAN의 컴퓨터 중 한 대가 Kaspersky Security Center 서버 또는 Kaspersky 업데이트 서버에서 최신 업데이트 패키지를 가져온 다음 검색된 업데이트 패키지를 공유 폴더에 복사합니다. 그러면 LAN에 연결된 다른 컴퓨터가 이 공유 폴더에서 업데이트 패키지를 가져올 수 있습니다.

- 업데이트 작업 스케줄을 선택합니다.

  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 실행 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.

- 다른 사용자 계정 권한으로 업데이트 작업을 실행하도록 구성합니다.

업데이트 경로 추가

업데이트 경로를 추가하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **업데이트**를 선택합니다.
   창 오른쪽에 애플리케이션 업데이트 설정이 표시됩니다.
3. **스케줄 및 업데이트 경로** 섹션에서 **업데이트 경로** 버튼을 누릅니다.
   그러면 **업데이트** 창의 **경로** 탭이 열립니다.
4. **경로** 탭에서 **추가** 버튼을 누릅니다.
   업데이트 경로 선택 창이 열립니다.
5. **업데이트 경로 선택** 창에서 업데이트 패키지가 있는 폴더를 선택하거나 **경로** 필드에 해당 폴더의 전체 경로를 입력합니다.
6. **확인**을 누릅니다.
7. **업데이트** 창에서 **확인**을 누릅니다.
8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

업데이트 서버 영역 선택

업데이트 서버 영역을 선택하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **업데이트**를 선택합니다.
   창 오른쪽에 애플리케이션 업데이트 설정이 표시됩니다.
3. **스케줄 및 업데이트 경로** 섹션에서 **업데이트 경로** 버튼을 누릅니다.
   그러면 **업데이트** 창의 **경로** 탭이 열립니다.
4. **경로** 탭의 **국가 설정** 섹션에서 **목록에서 선택**을 선택합니다.
5. 드롭다운 목록에서 현재 위치와 가장 가까운 국가를 선택합니다.
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

공유 폴더에서 업데이트 구성

공유 폴더에서 Kaspersky Endpoint Security의 업데이트를 구성하려면 다음 단계를 따라야 합니다:

1. LAN(Local Area Network)에 있는 컴퓨터 중 하나의 공유 폴더로 업데이트 패키지를 복사하는 기능을 작동합니다.

2. 지정한 공유 폴더에서 LAN에 있는 나머지 컴퓨터로 Kaspersky Endpoint Security가 업데이트 되도록 구성합니다.

공유 폴더로 업데이트 패키지를 복사하는 기능을 작동하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **업데이트**를 선택합니다.
   창 오른쪽에 애플리케이션 업데이트 설정이 표시됩니다.

3. **고급** 섹션에서 **폴더로 업데이트 파일 복사** 확인란을 선택합니다.

4. 업데이트 패키지를 저장할 공유 폴더의 경로를 지정합니다. 경로는 다음 방법 중 하나로 지정할 수 있습니다:

   - **폴더로 업데이트 파일 복사** 확인란 아래의 필드에 공유 폴더의 경로를 입력합니다.
   - **찾아보기** 버튼을 누릅니다. 그런 다음, 열리는 **폴더 선택** 창에서 필요한 폴더를 선택하고 **확인**을 누릅니다.

5. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

공유 폴더에서 Kaspersky Endpoint Security를 업데이트하는 기능을 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **업데이트**를 선택합니다.
   창 오른쪽에 애플리케이션 업데이트 설정이 표시됩니다.

3. **스케줄 및 업데이트 경로** 섹션에서 **업데이트 경로** 버튼을 누릅니다.
   그러면 **업데이트** 창의 **경로** 탭이 열립니다.

4. **경로** 탭에서 **추가** 버튼을 누릅니다.
   업데이트 경로 선택 창이 열립니다.

5. **업데이트 경로 선택** 창에서 업데이트 패키지가 있는 공유 폴더를 선택하거나 **경로** 필드에 해당 공유 폴더의 전체 경로를 입력합니다.

6. **확인**을 누릅니다.

7. **경로** 탭에서 공유 폴더로 지정하지 않은 업데이트 경로 이름 옆에 있는 확인란의 선택을 취소합니다.

8. **확인**을 누릅니다.

9. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

업데이트 작업 스케줄 선택

업데이트 작업 스케줄을 선택하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **업데이트**를 선택합니다.
   창 오른쪽에 애플리케이션 업데이트 설정이 표시됩니다.

3. **스케줄** 버튼을 누릅니다.
   업데이트 창의 **스케줄** 탭이 열립니다.

4. **스케줄** 섹션에서 다음 옵션 중 하나를 선택하여 업데이트 작업을 시작합니다:

   - 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 수동으로 시작하려면 **수동**을 선택합니다.
   - 업데이트 작업의 시작 스케줄을 구성하려면 **스케줄에 따라 실행**을 선택합니다.

5. 다음 중 하나를 수행합니다:

   - **자동** 또는 **수동** 옵션을 선택한 경우 지침의 6단계로 이동합니다.
   - **스케줄에 따라 실행** 옵션을 선택한 경우 업데이트 작업 스케줄의 설정을 지정합니다. 이를 위해서는 다음과 같이 하십시오:

     a. **빈도** 드롭다운 목록에서 업데이트 작업을 시작할 시기를 지정합니다. 다음 옵션 중 하나를 선택합니다: **분**, **시**, **일**, **매주**, **지정한 시간**, **매달** 또는 **애플리케이션 시작 후**.

     b. **빈도** 드롭다운 목록에서 선택한 항목에 따라 업데이트 작업 시작 시간을 정의하는 설정의 값을 지정합니다.

     c. **애플리케이션 시작 후 다음 시간 동안 작업 실행 연기** 필드에서 Kaspersky Endpoint Security 시작 후 업데이트 작업의 시작을 연기할 시간 간격을 지정합니다.

     > **빈도** 드롭다운 목록에서 **애플리케이션 시작 후** 항목을 선택한 경우에는 **애플리케이션 시작 후 다음 시간 동안 작업 실행 연기** 필드를 사용할 수 없습니다.

     d. Kaspersky Endpoint Security에서 건너뛴 업데이트 작업을 최대한 빨리 실행하도록 하려면 **건너뛴 작업 실행** 확인란을 선택합니다.

     > **빈도** 드롭다운 목록에서 **시**, **분** 또는 **애플리케이션 시작 후**를 선택한 경우에는 **건너뛴 작업 실행** 확인란을 사용할 수 없습니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

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 사용자 권한이 없는 경로에서도 업데이트할 수 있습니다. Kaspersky Endpoint Security 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:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **업데이트**를 선택합니다.
   창 오른쪽에 애플리케이션 업데이트 설정이 표시됩니다.
3. **스케줄 및 업데이트 경로** 섹션에서 **스케줄** 버튼을 누릅니다.
   업데이트 창의 **스케줄** 탭이 열립니다.
4. **스케줄** 탭의 **사용자** 섹션에서 **다음 계정으로 작업 실행** 확인란을 선택합니다.
5. **이름** 필드에 업데이트 경로에 접근하는 데 필요한 권한을 가진 사용자 계정 이름을 입력합니다.
6. **암호** 필드에 업데이트 경로에 접근하는 데 필요한 권한을 가진 사용자의 암호를 입력합니다.
7. **확인**을 누릅니다.
8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 모듈 업데이트 구성

애플리케이션 모듈 업데이트를 구성하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **업데이트**를 선택합니다.
   창 오른쪽에 애플리케이션 업데이트 설정이 표시됩니다.
3. **고급** 섹션에서 다음 중 하나를 수행합니다:
   - 애플리케이션이 업데이트 패키지에 애플리케이션 모듈 업데이트를 포함하게 하려면 **애플리케이션 모듈 업데이트 다운로드** 확인란을 선택합니다.
   - 또는 **애플리케이션 모듈 업데이트 다운로드** 확인란을 선택 해제합니다.
4. 이전 단계에서 **애플리케이션 모듈 업데이트 다운로드** 확인란을 선택한 경우 애플리케이션이 애플리케이션 모듈 업데이트를 설치하는 조건을 지정합니다:
   - 애플리케이션에서 애플리케이션 모듈의 중요한 업데이트를 자동으로 설치하게 하고 설치가 승인된 후 애플리케이션 인터페이스를 통해 또는 Kaspersky Security Center를 통해 로컬로 다른 업데이트를 설치하게 하려면 **긴급 및 승인된 업데이트 설치** 옵션을 선택하십시오.
   - 애플리케이션에서 설치가 승인된 후 애플리케이션 인터페이스를 통해 또는 Kaspersky Security Center를 통해 로컬로 애플리케이션 모듈 업데이트를 설치하게 하려면 **승인된 업데이트만 설치** 옵션을 선택하십시오.

5. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

업데이트 작업 시작 및 중지

선택한 업데이트 작업 스케줄에 관계 없이 언제라도 Kaspersky Endpoint Security 업데이트 작업을 시작 또는 중지할 수 있습니다.

Kaspersky 서버에서 업데이트 패키지를 다운로드하려면 인터넷에 연결되어 있어야 합니다.

업데이트 작업을 시작 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **작업** 섹션을 누릅니다.
   작업 섹션이 열립니다.
4. 마우스 오른쪽 버튼을 눌러 업데이트 작업 이름이 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
   이 행을 누르면 업데이트 작업에서 수행할 처리 방법이 나와 있는 메뉴가 열립니다.
5. 다음 중 하나를 수행합니다:
   - 업데이트 작업을 시작하려면 메뉴에서 **업데이트 시작**을 선택합니다.
     업데이트 버튼 오른쪽에 표시되는 업데이트 작업의 진행 상태가 *실행 중*으로 바뀝니다.
   - 업데이트 작업을 중지하려면 메뉴에서 **업데이트 중지**를 선택합니다.
     업데이트 버튼 오른쪽에 표시되는 업데이트 작업의 진행 상태가 *중지됨*으로 바뀝니다.

마지막으로 성공한 업데이트로 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. 필요한 경우 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.

마지막으로 성공한 업데이트로 롤백하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **작업** 섹션을 누릅니다.
   작업 섹션이 열립니다.

4. 마우스 오른쪽 버튼을 눌러 **업데이트** 작업의 마우스 오른쪽 메뉴를 엽니다.

5. **업데이트 롤백**을 선택합니다.

프록시 서버 설정 구성

프록시 서버 설정을 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **업데이트**를 선택합니다.
   창 오른쪽에 애플리케이션 업데이트 설정이 표시됩니다.

3. **프록시 서버** 섹션에서 **설정** 버튼을 누릅니다.
   프록시 서버 설정 창이 열립니다.

4. **프록시 서버 설정** 탭에서 **프록시 서버 사용** 확인란을 선택합니다.

5. 프록시 서버 설정을 지정합니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

메인 애플리케이션 창의 **설정** 탭에 있는 **고급 설정** 섹션에서 프록시 서버 설정을 구성할 수도 있습니다.

컴퓨터 검사

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

이 섹션에서는 검사 작업, 보안 레벨, 검사 방법, 검사 기술 등의 특성과 설정에 대해 설명하고, 바이러스 및 기타 개체를 검사하는 동안 Kaspersky Endpoint Security에서 처리하지 못한 파일을 처리하는 방법에 대해 소개합니다.

검사 작업 정보

바이러스 및 기타 악성 코드를 찾아내고 애플리케이션 모듈의 무결성을 확인하기 위해, Kaspersky Endpoint Security는 다음과 같은 작업을 수행합니다:

- **전체 검사**. 전체 컴퓨터를 완전히 검사합니다. 기본적으로 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
- **중요한 영역 검사**. Kaspersky Endpoint Security는 기본적으로 커널 메모리, 실행 중인 프로세스 및 디스크 부트 섹터를 검사합니다.
- **사용자 지정 검사**. Kaspersky Endpoint Security에서 사용자가 선택한 개체를 검사합니다. 다음 목록의 개체를 검사할 수 있습니다:
  - 커널 메모리
  - 운영 체제를 시작할 때 로드되는 개체
  - 운영 체제 백업
  - Outlook 사서함
  - 모든 하드, 이동식 및 네트워크 드라이브
  - 모든 선택 파일
- **무결성 검사**. Kaspersky Endpoint Security는 그 애플리케이션 모듈의 손상 및 변경 여부를 확인합니다.

> 전체 검사 및 중요한 영역 검사 작업은 다른 작업과 다소 다릅니다. 이들 작업에 대해서는 검사 범위를 편집하지 않는 것이 좋습니다.

검사 작업이 시작되면 Kaspersky Endpoint Security 메인 창의 **보호 및 제어** 탭에 있는 **작업** 섹션의 검사 작업 이름 옆 필드에 완료 진행 상황이 표시됩니다.

검사 작업 실행 중 발생한 검사 결과 및 이벤트에 대한 정보는 Kaspersky Endpoint Security 리포트에 기록됩니다.

검사 작업 시작 또는 중지

선택한 검사 작업 스케줄에 관계없이 언제라도 검사 작업을 시작 또는 중지할 수 있습니다.

검사 작업을 시작 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **작업** 섹션을 누릅니다.
   작업 섹션이 열립니다.
4. 마우스 오른쪽 버튼을 눌러 검사 작업 이름이 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
   검사 작업 처리 방법이 포함된 메뉴가 열립니다.
5. 다음 중 하나를 수행합니다:
   - 검사 작업을 시작하려면 메뉴에서 **검사 시작**을 선택합니다.
     이 검사 작업의 이름과 함께 버튼 오른쪽에 표시된 작업 진행 상태가 *실행 중*으로 바뀝니다.
   - 검사 작업을 중지하려면 메뉴에서 **검사 중지**를 선택합니다.
     이 검사 작업의 이름과 함께 버튼 오른쪽에 표시된 작업 진행 상태가 *중지됨*으로 바뀝니다.

검사 작업 설정 구성

검사 작업 설정을 구성하려면 다음과 같이 하십시오:

- 보안 레벨을 변경합니다.
  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.
- 감염 파일이 탐지된 경우 Kaspersky Endpoint Security에서 수행하는 처리 방법을 변경합니다.
- 검사 범위를 편집합니다.
  검사할 개체를 추가 또는 삭제하거나 검사할 파일 형식을 변경하여 검사 범위를 확장 또는 제한할 수 있습니다.
- 검사를 최적화합니다.
  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).
  또한, iChecker 및 iSwift 기술의 사용을 활성화할 수 있습니다. 이러한 기술은 최근에 검사된 후로 변경되지 않은 파일을 예외하여 파일 검사 속도를 최적화합니다.
- 복합 파일 검사를 구성합니다.

- 검사 방법 사용을 구성합니다.

  Kaspersky Endpoint Security는 시그너처 분석을 사용합니다. 시그니처 분석 시 Kaspersky Endpoint Security는 데이터베이스의 기록과 탐지된 개체가 일치하는지 확인합니다. Kaspersky 전문가의 권고에 따라 기본적으로 시그니처 분석이 사용되도록 선택되어 있습니다.

  보호의 효율성을 높이려면 휴리스틱 분석을 사용합니다. 휴리스틱 분석 시 Kaspersky Endpoint Security는 운영 체제의 개체 활동을 분석합니다. 휴리스틱 분석을 사용하면 현재 Kaspersky Endpoint Security 데이터베이스에 기록이 없는 악성 개체도 탐지할 수 있습니다.

- 검사 작업 스케줄을 선택합니다.

  컴퓨터의 전원이 켜져 있지 않는 등의 이유로 검사 작업을 실행할 수 없는 경우 컴퓨터의 전원이 켜지면 건너뛴 작업을 자동으로 시작하도록 구성할 수 있습니다.

  사용자가 **스케줄에 따라 실행** 업데이트 작업 스케줄을 선택한 경우 Kaspersky Endpoint Security 시작 시간이 검사 작업 실행 스케줄과 일치하면 검사 작업 시작을 애플리케이션이 시작된 후로 연기할 수 있습니다. 검사 작업은 Kaspersky Endpoint Security가 시작된 후 지정된 시간 간격이 경과해야만 실행할 수 있습니다.

- 검사 작업을 다른 사용자 계정으로 실행하도록 구성합니다.

- 이동식 장치가 컴퓨터에 연결될 때 검사하는 설정을 지정합니다.

보안 레벨 변경

검사 작업을 수행하기 위해 Kaspersky Endpoint Security는 다양한 설정 조합을 사용합니다. 애플리케이션에 저장된 이러한 설정 조합을 *보안 레벨*이라고 합니다. 3개의 사전 설정된 보안 레벨이 있습니다: **높음**, **권장** 및 **낮음**. **권장** 보안 레벨로 설정하는 것이 가장 적당하다고 간주됩니다. Kaspersky 전문가가 권장하는 설정입니다.

보안 레벨을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션 (**전체 검사**, **중요한 영역 검사** 또는 **사용자 지정 검사**)을 선택합니다.

   창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 다음 중 하나를 수행합니다:

   - 미리 설정된 보안 레벨(**높음**, **권장** 또는 **낮음**) 중 하나를 지정하려는 경우 슬라이더로 레벨을 선택합니다.
   - 사용자 지정 보안 레벨을 구성하려는 경우 **설정** 버튼을 누르면 열리는 창에서 검사 작업 이름으로 설정을 지정합니다.

     사용자 지정 보안 레벨을 구성하면, **보안 레벨** 섹션의 보안 레벨 이름이 **사용자 지정**으로 변경됩니다.
   - 보안 레벨을 **권장**으로 변경하려면 **기본값** 버튼을 누릅니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

감염된 파일에 수행할 처리 방법 변경

감염된 파일에 수행할 처리 방법을 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션 (**전체 검사**, **중요한 영역 검사** 또는 **사용자 지정 검사**)을 선택합니다.
   창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.
3. **위협 탐지 시 처리 방법** 섹션에서 필요한 옵션을 선택합니다:
   - **자동으로 처리 방법 선택**.
   - **처리 방법 선택**.
4. 이전 단계에서 **처리 방법 선택** 옵션을 선택했으면 다음 확인란을 선택합니다:
   - Kaspersky Endpoint Security가 보안위협이 감지된 개체를 치료하기 원하면 **치료** 확인란을 선택합니다.

     이 옵션을 선택하면, Windows Store 애플리케이션에 포함되는 파일은 **제거**합니다.

   - Kaspersky Endpoint Security가 보안위협이 감지된 개체를 삭제하기 원하면 **삭제** 확인란을 선택합니다.
   - Kaspersky Endpoint Security가 보안위협이 감지된 개체 치료를 시도한 후에 치료할 수 없는 개체를 삭제하기 원하면 **치료** 및 **삭제**확인란을 모두 선택합니다.
   - Kaspersky Endpoint Security가 보안위협이 감지된 개체에 대해 아무런 처리를 수행하지 않는 대신 사용자에게 이러한 개체의 검사 결과 알림만을 발송하기 원하면 **치료** 및 **삭제** 확인란을 모두 선택 취소합니다.
5. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

검사할 개체 목록 생성

검사할 개체 목록을 생성하려면 다음 두 가지 방법 중 하나를 사용합니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

  이 방법은 **전체 검사** 및 **중요한 영역 검사** 작업에 한해 사용할 수 있습니다. **사용자 지정 검사** 작업으로 검사할 개체 목록은 **보호 및 제어** 탭에서만 지정할 수 있습니다.

메인 애플리케이션 창의 보호 및 제어 탭에서 검사할 파일 목록을 만들려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **작업** 섹션을 누릅니다.
   작업 섹션이 열립니다.
4. 마우스 오른쪽 버튼으로 작업 이름이 들어 있는 행을 눌러 메뉴를 열고 **검사 영역**을 선택합니다.

검사 범위 창이 열립니다.

5. 검사 범위에 새로운 개체를 추가하려면 다음과 같이 합니다:

   a. **추가** 버튼을 누릅니다.
   검사 범위 선택 창이 열립니다.

   b. 개체를 선택하고 **추가**를 누릅니다.
   검사 범위 선택 창에서 선택한 모든 개체가 **검사 범위** 목록에 표시됩니다.

   c. **확인**을 누릅니다.

6. 검사 범위에서 개체 경로를 변경하려면 다음과 같이 합니다:

   a. 검사 범위의 개체를 선택합니다.

   b. **편집** 버튼을 누릅니다.
   검사 범위 선택 창이 열립니다.

   c. 검사 범위 개체의 새 경로를 입력합니다.

   d. **확인**을 누릅니다.

7. 검사 범위의 개체를 삭제하려면 다음과 같이 합니다:

   a. 검사 범위에서 삭제할 개체를 선택합니다.
   개체를 여러 개 선택하려면 **Ctrl** 키를 누른 상태에서 이벤트를 선택합니다.

   b. **제거** 버튼을 누릅니다.
   그러면 삭제 여부 확인하는 창이 열립니다.

   c. 삭제 확인 창에서 **예**를 누릅니다.

   > 기본 검사 범위에 포함된 개체는 삭제하거나 편집할 수 없습니다.

8. 검사 범위에서 개체를 예외하려면 **검사 범위** 창에서 해당 개체 옆의 확인란을 선택 취소합니다.
   개체는 검사 범위 내에 있는 개체 목록에 계속 남아 있지만 검사 작업이 실행되어도 해당 개체를 검사하지 않습니다.

9. **확인**을 누릅니다.

10. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 설정 창에서 검사할 개체 목록을 작성하려면 다음과 같이 합니다:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션을 선택합니다: **전체 검사** 또는 **중요한 영역 검사**.
   창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.

3. **검사 범위** 버튼을 누릅니다.

검사 범위 창이 열립니다.

4. 이전 지침의 5-10단계에 따라 검사할 개체 목록을 작성합니다.

검사할 파일 유형 선택

다음 두 가지 방법으로 검사할 파일 유형을 선택할 수 있습니다:

- 메인 애플리케이션 창의 **보호 및 제어** 탭에서
- 애플리케이션 설정 창 사용

> 이 방법은 **전체 검사** 및 **중요한 영역 검사** 작업에 한해 사용할 수 있습니다. **사용자 지정 검사** 작업으로 검사할 파일 유형은 **보호 및 제어** 탭에서만 선택할 수 있습니다.

메인 애플리케이션 창의 보호 및 제어 탭에서 검사할 파일 유형을 선택하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **작업** 섹션을 누릅니다.
   작업 섹션이 열립니다.
4. 마우스 오른쪽 버튼으로 작업 이름이 들어 있는 행을 눌러 메뉴를 열고 **설정**을 선택합니다.
   선택한 검사 작업 이름의 창이 열립니다.
5. 선택한 검사 작업 이름이 있는 창에서 **범위** 탭을 선택합니다.
6. **파일 유형** 섹션에서 선택한 검사 작업이 실행될 때 검사할 파일 유형을 지정합니다:
   - **모든 파일**을 검사하려면 모든 파일을 선택합니다.
   - **감염 가능성이 높은 파일 - 확장자 분석**의 파일만 검사하려면 파일 형식에 따라 검사를 선택합니다.
   - **감염 가능성이 높은 파일 - 알려진 확장자**를 가진 파일만 검사하려면 일반적으로 파일 확장자에 따라 검사를 선택합니다.

   검사할 파일 유형을 선택할 때 다음을 고려하십시오:
   - TXT와 같은 일부 파일 형식에서는 악성 코드가 침투한 후 활성화될 가능성은 매우 낮습니다. 반면, 실행 코드(예: .exe, .dll, .doc)를 포함하거나 포함할 수 있는 형식의 경우. 악성 코드가 침투하여 활성화될 위험이 높습니다.
   - 침입자가 실행 파일의 이름을 .txt 확장명으로 변경하고 컴퓨터에 바이러스나 기타 악성 코드를 보낼 수도 있습니다. 만일 확장자로 파일 검사를 선택하면 애플리케이션은 검사하는 동안 이 파일은 건너뜁니다. 파일 형식별 검사를 선택하면 파일 안티 바이러스는 확장자와 상관없이 파일 헤더를 분석합니다. 이 분석에서 파일의 형식이 EXE 형식인 것으로 밝혀지면 애플리케이션이 이를 검사합니다.
7. 검사 작업 이름이 있는 창에서 **확인**을 누릅니다.

8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

애플리케이션 설정 창에서 검사할 파일 형식을 선택하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션을 선택합니다: **전체 검사** 또는 **중요한 영역 검사**.
   창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   선택한 검사 작업 이름의 창이 열립니다.
4. 선택한 검사 작업 이름이 있는 창에서 **범위** 탭을 선택합니다.
5. 이전 안내의 5-7단계를 완료합니다.

파일 검사 최적화

파일 검사를 최적화하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션 (**전체 검사**, **중요한 영역 검사** 또는 **사용자 지정 검사**)을 선택합니다.
   창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   선택한 검사 작업 이름의 창이 열립니다.
4. 열리는 창에서 **범위** 탭을 선택합니다.
5. **검사 최적화** 섹션에서 다음 처리 방법을 수행합니다:
   - **새로운 것이나 변경된 파일만 검사** 확인란을 선택합니다.
   - **다음보다 오래 검사하는 파일은 건너뛰기** 확인란을 선택한 후, 단일 파일에 대한 검사 시간 한도(단위: 초)를 지정합니다.
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

복합 파일 검사

바이러스나 기타 악성 프로그램을 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.

복합 파일 검사를 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션 (**전체 검사**, **중요한 영역 검사** 또는 **사용자 지정 검사**)을 선택합니다.

   창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.
3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.

   선택한 검사 작업 이름의 창이 열립니다.
4. 열리는 창에서 **범위** 탭을 선택합니다.
5. **복합 파일 검사** 섹션에서 검사할 복합 파일의 유형을 지정합니다: 압축 파일, 설치 패키지, 오피스 형식 파일, 메일 형식 파일 및 암호로 보호된 압축 파일.
6. **검사 최적화** 섹션에 **새로운 것이나 변경된 파일만 검사** 확인란이 선택 취소되어 있고, 각 복합 파일 형식에 대해 이 형식의 모든 파일을 검사할지, 아니면 이 형식의 새 파일만 검사할지 지정하려면 복합 파일 형식 이름 옆에 있는 **모두/새 파일** 링크를 누릅니다.

   이 링크를 누르면 링크의 값이 변경됩니다.

   새로운 것이나 변경된 파일만 검사 확인란이 선택되어 있으면 새로운 파일만 검사됩니다.
7. **고급** 버튼을 누릅니다.

   복합 파일 창이 열립니다.
8. **크기 제한** 섹션에서 다음 중 하나를 수행합니다:

   - 대용량 복합 파일을 압축해제하지 않을 경우 **다음보다 큰 복합 파일은 압축해제 안 함** 확인란을 선택하고 **최대 파일 크기** 필드에 필요한 값을 지정합니다.
   - 크기와 상관없이 대용량 복합 파일을 압축해제하려면 **다음보다 큰 복합 파일은 압축해제 안 함** 확인란을 선택 해제합니다.

   Kaspersky Endpoint Security는 **다음보다 큰 복합 파일은 압축해제 안 함** 확인란의 선택 여부에 관계 없이 압축 해제된 대용량 파일을 검사합니다.
9. **확인**을 누릅니다.
10. 검사 작업 이름이 있는 창에서 **확인**을 누릅니다.
11. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

검사 방법 사용

검사 방법을 사용하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션 (**전체 검사**, **중요한 영역 검사** 또는 **사용자 지정 검사**)을 선택합니다.

창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.

3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   선택한 검사 작업 이름의 창이 열립니다.

4. 열리는 창에서 **고급** 탭을 선택합니다.

5. 검사 작업이 실행되는 동안 애플리케이션에서 휴리스틱 분석을 사용하도록 하려면 **검사 방법** 섹션에서 **휴리스틱 분석** 확인란을 선택합니다. 그런 다음 슬라이더를 사용하여 휴리스틱 분석 레벨을 설정합니다: **기본**, **자세히** 및 **매우 자세히**.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

검사 기술 사용

검사 기술을 사용하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션 (**전체 검사**, **중요한 영역 검사** 또는 **사용자 지정 검사**)을 선택합니다.
   창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.

3. **보안 레벨** 섹션에서 **설정** 버튼을 누릅니다.
   선택한 검사 작업 이름의 창이 열립니다.

4. 열리는 창에서 **고급** 탭을 선택합니다.

5. **검사 기술** 섹션에서 검사가 진행되는 동안 사용할 기술 이름 옆의 확인란을 선택합니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

검사 작업 스케줄 선택

검사 작업 스케줄을 선택하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션 (**전체 검사**, **중요한 영역 검사** 또는 **사용자 지정 검사**)을 선택합니다.
   창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.

3. **스케줄** 버튼을 누릅니다.

스케줄 탭에서 선택된 작업의 속성 창이 열립니다.

4. **스케줄** 섹션에서 작업 스케줄을 선택합니다: **수동** 또는 **스케줄에 따라 실행**.

5. **스케줄에 따라 실행** 옵션을 선택한 경우 스케줄 설정을 지정합니다. 이를 위해서는 다음과 같이 하십시오:

   a. **빈도** 드롭다운 목록에서 작업 실행 빈도(**분**, **시**, **일**, **매주**, **지정한 시간**, **매달** 또는 **애플리케이션 시작 후**, **업데이트 후**)를 선택합니다.

   b. 선택한 빈도에 따라 작업 실행 스케줄을 지정하는 고급 설정을 구성합니다.

   c. Kaspersky Endpoint Security에서 건너뛴 검사 작업을 최대한 빨리 시작하도록 하려면 **건너뛴 작업 실행** 확인란을 선택합니다.

   > **빈도** 드롭다운 목록에서 **분**, **시**, **애플리케이션 시작 후** 또는 **업데이트 후**를 선택한 경우에는 **건너뛴 작업 실행** 확인란을 사용할 수 없습니다.

   a. 컴퓨터 리소스가 제한된 경우에 Kaspersky Endpoint Security에서 작업을 일시 중지하려고 한다면, **컴퓨터가 유휴 상태일 때만 실행** 확인란을 선택합니다.

   이 스케줄 옵션을 사용하면 컴퓨터 리소스를 절약할 수 있습니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

다른 사용자 계정으로 검사 작업 시작

기본적으로 검사 작업은 사용자가 운영 체제에 로그인 한 계정 권한으로 실행됩니다. 그러나 다른 사용자 계정으로 검사 작업을 실행해야 하는 경우도 있습니다. 검사 작업 설정에서 적절한 권한이 있는 사용자를 지정하여 이 사용자의 계정으로 검사 작업을 실행할 수 있습니다.

다른 사용자 계정으로 검사 작업을 시작하도록 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 원하는 검사 작업 이름이 있는 하위 섹션 (**전체 검사**, **중요한 영역 검사** 또는 **사용자 지정 검사**)을 선택합니다.

   창 오른쪽에 선택한 검사 작업의 설정이 표시됩니다.

3. **스케줄** 버튼을 누릅니다.

   그러면, **스케줄** 탭에서 선택된 작업의 속성 창이 열립니다.

4. **스케줄** 탭의 **사용자** 섹션에서 **다음 계정으로 작업 실행** 확인란을 선택합니다.

5. **이름** 필드에 검사 작업을 시작하는 데 필요한 권한을 가진 사용자의 계정 이름을 입력합니다.

6. **암호** 필드에 검사 작업을 시작하는 데 필요한 권한을 가진 사용자의 암호를 입력합니다.

7. **확인**을 누릅니다.

8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

이동식 장치가 컴퓨터에 연결될 때 검사

일부 악성 코드는 운영 체제 취약점을 악용해 로컬 네트워크와 이동식 드라이브를 통해 자기 자신을 복제합니다. Kaspersky Endpoint Security를 사용하면 컴퓨터에 연결된 이동식 장치에 바이러스 및 기타 악성 코드가 있는지 검사할 수 있습니다.

이동식 장치가 연결될 때 검사하도록 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **스케줄된 작업** 섹션을 선택합니다.
   창 오른쪽에 작업 설정이 표시됩니다.
3. **이동식 드라이브가 연결될 때 검사** 섹션의 **이동식 드라이브 연결 시 작업** 드롭다운 목록에서 필요한 작업을 선택합니다:
   - **검사 안 함**
   - **정밀 검사**
     이 모드에서는 Kaspersky Endpoint Security가 복합 개체 내의 파일을 포함해 이동식 드라이브에 있는 모든 파일을 검사합니다.
   - **빠른 검사**
     이 모드에서는 Kaspersky Endpoint Security가 감염 가능성이 있는 파일만 검사하고 복합 개체의 압축을 풀지 않습니다.
4. Kaspersky Endpoint Security에서 지정된 값보다 크기가 작거나 같은 이동식 드라이브만 검사하도록 하려면 **이동식 드라이브 최대 크기** 확인란을 선택하고 옆에 있는 필드에 메가바이트 단위로 값을 지정합니다.
5. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

처리 안 된 파일 처리

이 섹션에서는 Kaspersky Endpoint Security가 컴퓨터에서 바이러스 및 기타 보안위협을 검사할 동안 미처리된 감염 및 감염 의심 파일을 처리하는 방법에 대해 설명합니다.

처리 안 된 파일 정보

Kaspersky Endpoint Security는 어떤 이유로 인해 처리 안 된 파일에 대한 정보를 기록합니다. 이 정보는 처리 안 된 파일의 목록에서 이벤트 형식으로 기록됩니다.

Kaspersky Endpoint Security가 컴퓨터에서 바이러스 및 기타 보안위협을 검사하는 동안 지정된 애플리케이션 설정에 따라 감염된 파일에 대해 다음과 같은 처리 중 하나를 수행하는 경우 이 파일은 *처리됨*으로 간주됩니다:

- 치료.
- 제거.

- 삭제해야 처리되는 것은 삭제.

Kaspersky Endpoint Security가 컴퓨터에서 바이러스 및 기타 보안위협을 검사하는 동안 지정된 애플리케이션 설정에 따라 감염된 파일에 대해 어떤 이유로든 위에서 나열된 처리 중 하나를 수행하지 못하는 경우 이 파일은 *미처리*로 간주됩니다.

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.
- 검사 작업의 **위협 탐지 시 처리 방법** 섹션에서 선택된 작업이 **알림**이고 감염된 파일에 대한 알림이 표시될 때 사용자가 **건너뛰기** 처리 방법을 선택합니다.

데이터베이스 및 애플리케이션 모듈을 업데이트한 후 처리 안 된 파일의 목록에서 파일에 대한 사용자지정 검사 작업을 수동으로 시작할 수 있습니다. 파일 상태는 검사 후 변경될 수 있습니다. 파일 상태에 따라 파일에 대해 필요한 처리를 수행할 수 있습니다.

예를 들어, 다음과 같은 작업을 수행할 수 있습니다:

- *감염됨* 상태를 가진 파일 삭제.
- 중요한 정보가 있는 감염된 파일을 복원하고 *치료됨* 또는 *감염 안 됨*으로 표시된 파일을 복원합니다.
- *감염 의심* 상태의 격리 파일.

처리 안 된 파일의 목록 관리

처리 안 된 파일의 목록이 표 형식으로 나타납니다.

처리 안 된 파일에 대해 다음과 같은 작업을 수행할 수 있습니다:

- 처리 안 된 파일의 목록을 봅니다.
- 현재 버전의 Kaspersky Endpoint Security 데이터베이스 및 모듈을 사용하여 처리 안 된 파일을 검사합니다.
- 처리 안 된 파일의 목록에서 원래 폴더 또는 선택한 다른 폴더(원래 폴더에 쓸 수 없는 경우)로 파일을 복원합니다.
- 처리되지 않은 파일의 목록에서 파일을 제거합니다.
- 처리 안 된 파일이 원래 있던 폴더를 엽니다.

표의 데이터를 관리할 때 다음과 같은 작업도 수행할 수 있습니다:

- 열 값 또는 사용자지정 필터 조건을 사용하여 처리 안 된 파일을 필터링합니다.
- 처리 안 된 파일 이벤트 검색 기능을 사용합니다.
- 처리 안 된 파일 이벤트를 정렬합니다.
- 처리되지 않은 파일 목록에 표시되는 열의 순서와 집합을 변경합니다.
- 처리 안 된 파일 이벤트를 그룹화합니다.

필요한 경우 선택한 처리되지 않은 파일 이벤트를 클립보드에 복사할 수 있습니다.

처리 안 된 파일에 대한 사용자 지정 검사 작업 시작

처리 안 된 파일에 대한 사용자지정 검사를 수동으로 시작할 수 있습니다. 만일 데이터베이스 및 애플리케이션 모듈을 최신으로 업데이트한 이후에 처리 안 된 파일을 다시 검사하기를 원하거나 마지막 검사가 어떤 이유에선지 중단되었다면, 해당 검사를 시작할 수 있습니다.

처리 안 된 파일의 사용자지정 검사를 시작하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.
3. **저장소** 창에서 **처리되지 않은 파일** 탭을 선택합니다.
4. **처리되지 않은 파일** 탭의 표에서 검사할 파일과 관련된 이벤트를 하나 이상 선택합니다.
   이벤트를 여러 개 선택하려면 **Ctrl** 키를 누른 상태에서 이벤트를 선택합니다.
5. 다음 방법 중 하나로 사용자지정 검사 작업을 시작합니다:
   - **다시 검사** 버튼을 누릅니다.
   - 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 열고 **다시 검사**를 선택합니다.

처리 안 된 파일의 목록에서 파일 삭제

처리 안 된 파일의 목록에서 파일을 삭제하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.
3. **저장소** 창에서 **처리되지 않은 파일** 탭을 선택합니다.
4. **처리되지 않은 파일** 탭의 표에서 삭제할 파일 이벤트를 하나 이상 선택합니다.
   이벤트를 여러 개 선택하려면 **Ctrl** 키를 누른 상태에서 이벤트를 선택합니다.
5. 다음 중 한 방법으로 파일을 삭제합니다:
   - **제거** 버튼을 누릅니다.
   - 마우스 오른쪽 메뉴를 열어 **삭제**를 선택합니다.

취약점 검사

이 섹션에서는 취약점 모니터 정보와 취약점 검사 작업의 특성과 설정에 대해 설명하고, 취약점 검사 작업을 실행하는 동안 Kaspersky Endpoint Security에서 탐지한 취약점 목록을 관리하는 것과 관련한 지침에 대해 소개합니다.

실행 중인 애플리케이션의 취약점 정보 확인

Kaspersky Endpoint Security가 Microsoft Windows for workstations를 실행하는 컴퓨터에 설치되어 있는 경우 실행 중인 애플리케이션의 취약점에 대한 정보를 볼 수 있습니다. 이 정보는 Kaspersky Endpoint Security가 파일 서버용 Microsoft servers에서 실행 중인 컴퓨터에 설치되어 있는 경우 사용할 수 없습니다.

실행 중인 애플리케이션의 취약점에 대한 정보를 확인하는 방법은 다음과 같습니다:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **엔드포인트 제어** 섹션을 엽니다.
4. **애플리케이션 활동 모니터** 버튼을 누릅니다.

   애플리케이션 권한 제어 창이 **애플리케이션 활동 모니터** 탭에서 열립니다. **애플리케이션 활동 모니터** 표에 운영 체제에서 실행 중인 애플리케이션의 동작에 대한 요약 정보가 표시됩니다. 취약점 모니터 구성요소에서 판단한, 실행 중인 애플리케이션의 **취약점 심각도**가 취약점 상태 열에 표시됩니다.

취약점 검사 작업 정보

운영 체제의 취약점은 프로그래밍 또는 설계 실수, 신뢰할 수 없는 암호, 악성 프로그램 동작 등에 의해 발생할 수 있습니다. 애플리케이션은 취약점 검사를 통해 운영 체제를 분석하고 Microsoft 및 기타 공급업체의 애플리케이션에서 설정 오류나 손상을 검색합니다.

취약점 검사는 운영 체제 보안을 진단하며 침입자가 악성 개체를 유포하고 개인정보에 접근하기 위해 악용할 수 있는 소프트웨어 기능을 탐지합니다.

취약점 검사 작업이 시작되면 Kaspersky Endpoint Security 메인 창의 **보호 및 제어** 탭에 있는 **작업** 섹션의 **취약점 검사** 작업 이름 옆 필드에 완료 진행 상황이 표시됩니다.

취약점 검사 작업 결과는 리포트에 기록됩니다.

취약점 검사 작업 시작 또는 중지

취약점 검사 작업에 대해 선택한 실행 모드와 상관없이 언제든 작업을 시작하거나 중지할 수 있습니다.

취약점 검사 작업을 시작 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.

2. **보호 및 제어** 탭을 선택합니다.

3. **작업** 섹션을 누릅니다.
   작업 섹션이 열립니다.

4. 마우스 오른쪽 버튼을 눌러 취약점 검사 작업 이름이 있는 행의 마우스 오른쪽 메뉴를 표시합니다.
   취약점 검사 작업 동작 메뉴가 열립니다.

5. 다음 중 하나를 수행합니다:

   - 취약점 검사 작업을 시작하려면 메뉴에서 **검사 시작**을 선택합니다.
     취약점 검사 작업의 이름이 있는 버튼 오른쪽에 표시되는 작업 진행 상태가 *실행 중*으로 변합니다.
   - 취약점 검사 작업을 중지하려면 메뉴에서 **검사 중지**를 선택합니다.
     취약점 검사 작업의 이름이 있는 버튼 오른쪽에 표시되는 작업 진행 상태가 *중지됨*으로 변합니다.

취약점 검사 설정 구성

취약점 검사 설정을 구성하려면 다음과 같이 하십시오:

- 취약점 검사 영역을 만듭니다.
  취약점 검사할 애플리케이션을 추가 또는 삭제하여 검사 영역을 확장하거나 제한할 수 있습니다.
- 취약점 검사 작업 스케줄 선택.
  컴퓨터의 전원이 켜져 있지 않는 등의 이유로 작업을 실행할 수 없는 경우 컴퓨터의 전원이 켜지면 건너뛴 작업을 자동으로 시작하도록 구성할 수 있습니다.
- 다른 사용자 계정 권한으로 작업을 실행하도록 구성합니다.
  기본적으로 검사 작업은 사용자가 운영 체제에 로그인 한 계정 권한으로 실행됩니다. 그러나 다른 사용자 계정으로 검사 작업을 실행해야 하는 경우도 있습니다. 작업 설정에서 적절한 권한이 있는 사용자를 지정하여 이 사용자의 계정으로 작업을 실행할 수 있습니다.

취약점 검사 영역 만들기

취약점 검사 영역에는 소프트웨어 공급 업체 전체 또는 소프트웨어가 설치된 폴더 경로가 해당됩니다. Program Files 폴더에 설치된 모든 Microsoft 애플리케이션을 예로 들 수 있습니다.

취약점 검사 영역을 만들려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **취약점 검사**를 선택합니다.
   창 오른쪽 부분에 취약점 검사 작업 설정이 표시됩니다.

3. **검사 영역** 섹션에서 다음을 수행합니다:

   a. Kaspersky Endpoint Security를 사용하여 컴퓨터에 설치된 Microsoft 애플리케이션에서 취약점을 찾으려면 **Microsoft** 확인란을 선택합니다.

b. Kaspersky Endpoint Security를 사용하여 컴퓨터에 설치된 Microsoft 이외의 모든 애플리케이션에서 취약점을 찾으려면 **기타 공급업체** 확인란을 선택합니다.

c. **취약점 검사 영역 추가** 창에서 **설정** 버튼을 누릅니다.
취약점 검사 영역 창이 열립니다.

d. **추가** 및 **제거** 버튼을 사용하여 취약점 검사 영역을 만듭니다.

e. **취약점 검사 영역** 창에서 **확인**을 누릅니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

취약점 검사 작업 스케줄 선택

취약점 검사 작업 스케줄을 선택하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **취약점 검사**를 선택합니다.
창 오른쪽 부분에 취약점 검사 작업 설정이 표시됩니다.

3. **스케줄** 버튼을 누릅니다.
그러면 **취약점 검사** 창에서 **스케줄** 탭이 열립니다.

4. **스케줄** 섹션에서 다음 실행 모드 옵션 중 하나를 선택하여 취약점 검사 작업을 시작합니다:

- 취약점 검사 작업을 수동으로 시작하려면 **수동**을 선택합니다.
- 취약점 검사 작업의 시작 스케줄을 구성하려면 **스케줄에 따라 실행**를 선택합니다.

5. 다음 중 하나를 수행합니다:

- **수동** 옵션을 선택한 경우 지침의 6단계로 이동합니다.
- **스케줄에 따라 실행** 옵션을 선택한 경우 취약점 검사 작업의 시작 설정을 지정합니다. 이를 위해서는 다음과 같이 하십시오:

a. **빈도** 드롭다운 목록에서 취약점 검사 작업을 시작할 시기를 지정합니다. 다음 옵션 중 하나를 선택합니다: **일**, **매주**, **지정한 시간**, **매달**, **애플리케이션 시작 후** 또는 **업데이트 후**.

b. **빈도** 드롭다운 목록에서 선택한 항목에 따라 취약점 검사의 시작 시간을 정의하는 설정의 값을 지정합니다.

c. Kaspersky Endpoint Security에서 건너뛴 취약점 검사 작업을 최대한 빨리 실행하도록 하려면 **건너뛴 작업 실행** 확인란을 선택합니다

> **빈도** 드롭다운 목록에서 **애플리케이션 시작 후** 또는 **업데이트 후**를 선택한 경우에는 **건너뛴 작업 실행** 확인란을 사용할 수 없습니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

다른 사용자 계정 권한으로 취약점 검사 작업 시작

기본적으로 취약점 검사 작업은 운영 체제에 로그인한 사용자의 계정으로 시작됩니다. 그러나 다른 사용자 계정으로 취약점 검사 작업을 시작해야 하는 경우가 있습니다. 취약점 검사 작업에 대한 설정에서 이러한 권한을 가진 사용자를 지정하고 이 사용자 계정으로 취약점 검사 작업을 시작할 수 있습니다.

다른 사용자 계정으로 취약점 검사 작업을 실행하도록 구성하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **취약점 검사**를 선택합니다.
   창 오른쪽 부분에 취약점 검사 작업 설정이 표시됩니다.
3. **스케줄** 버튼을 누릅니다.
   그러면 **취약점 검사** 창에서 **스케줄** 탭이 열립니다.
4. **스케줄** 탭의 **사용자** 섹션에서 **다음 계정으로 작업 실행** 확인란을 선택합니다.
5. **이름** 필드에 취약점 검사 작업을 시작하는 데 필요한 권한을 가진 사용자의 계정 이름을 입력합니다.
6. **암호** 필드에 취약점 검사 작업을 시작하는 데 필요한 권한을 가진 사용자의 계정 이름을 입력합니다.
7. **확인**을 누릅니다.
8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

취약점 목록 관리

취약점 목록을 관리할 때 다음과 같은 작업을 수행할 수 있습니다:

- 취약점 목록 확인.
- 데이터베이스 및 애플리케이션 모듈 업데이트 후 취약점 검사 작업 다시 시작.
- 별도의 섹션에서 취약점에 대한 자세한 정보와 권장 처리 방법 확인.
- 취약점 목록에서 선택된 항목 숨장치.
- 중요도 레벨을 기준으로 취약점 목록 필터링.
- *수정됨* 및 *무시한 취약점* 상태 값을 기준으로 취약점 목록 필터링.

표의 데이터를 관리할 때 다음과 같은 작업도 수행할 수 있습니다:

- 항목 값 또는 사용자지정 필터 조건을 기준으로 취약점 목록 필터링.
- 취약점 검색 기능 사용.

- 취약점 목록의 항목 정렬.
- 취약점 목록에 표시되는 열의 순서와 정렬 변경.
- 취약점 목록의 항목 그룹화.

취약점 목록 정보

Kaspersky Endpoint Security는 취약점 검사 작업의 결과를 취약점 목록에 기록합니다.

사용자가 특정 취약점을 검토하여 권장 처리 방법을 수행하면 Kaspersky Endpoint Security가 취약점의 상태를 *수정됨*으로 변경합니다.

사용자가 취약점 목록에서 특정 취약점에 대한 항목을 표시하지 않으려는 경우 해당 항목을 숨기도록 선택할 수 있습니다. 이러한 취약점에는 Kaspersky Endpoint Security가 *무시한 취약점* 상태를 지정합니다.

취약점 목록은 표 형식으로 표시됩니다. 표의 각 행에는 다음과 같은 정보가 표시됩니다:

- 취약점의 심각도를 의미하는 아이콘. 다음과 같은 취약점 중요도 레벨의 이벤트가 있습니다:
  - 아이콘. **심각**. 즉시 해결해야 할 매우 위험한 취약점을 나타내는 심각도 레벨입니다. 침입자는 활발하게 이 레벨의 취약점을 악용해 컴퓨터 운영 체제를 감염시키거나 사용자의 개인 데이터에 접근합니다. Kaspersky는 "매우 중요" 심각도의 취약점을 수정하기 위해 즉각적으로 모든 조치를 취하기를 권장합니다.
  - 아이콘. **중요**. 시급하게 처리해야 하는 중요한 취약점을 나타냅니다. 침입자는 활발하게 이 레벨의 취약점을 악용할 수 있습니다. 침입자는 현재 활발하게 "중요" 레벨의 취약점을 악용하지 않습니다. Kaspersky는 "중요" 심각도의 취약점을 수정하기 위해 즉각적으로 모든 조치를 취하기를 권장합니다.
  - 아이콘. **경고**. 당장 처리하지 않아도 되는 취약점을 나타냅니다. 하지만, 이러한 취약점은 추후 컴퓨터의 보안에 위협을 줄 수 있습니다.
- 취약점 ID.
- 취약점이 탐지된 애플리케이션의 이름.
- 취약점에 대한 간단한 설명.
- 디지털 서명에 나와 있는 소프트웨어 게시자에 대한 정보.
- 취약점을 해결하기 위해 수행된 처리의 결과.

취약점 검사 작업 다시 시작

이전에 탐지된 취약점에 대한 정보를 업데이트하려면, 취약점 검사 작업을 다시 시작할 수 있습니다. 어떤 이유로든 취약점 검사가 중단되었거나 최근에 데이터베이스 및 애플리케이션 모듈 업데이트 이후 컴퓨터의 취약점을 검사하기 원하는 경우에도 검사 작업을 다시 시작해야 합니다.

취약점 검사 작업을 다시 시작하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.

2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.

3. **저장소** 창에서 **취약점** 탭을 선택합니다.
   취약점 탭에는 취약점 검사 작업 중 Kaspersky Endpoint Security가 탐지한 취약점 목록이 포함됩니다.

4. **저장소** 창의 오른쪽 아래에서 **다시 검사** 버튼을 누릅니다.

Kaspersky Endpoint Security는 취약점 목록에 있는 취약점에 대한 세부 정보를 업데이트합니다.

제안된 패치의 설치로 수정된 취약점 상태는 다시 취약점을 검사한 후에도 변경되지 않습니다.

취약점 수정

운영 체제 업데이트를 설치하거나 애플리케이션 구성을 변경하거나 애플리케이션 패치를 설치하여 취약점을 수정할 수 있습니다.

탐지된 취약점은 설치된 애플리케이션뿐 아니라 해당 복사본에도 적용될 수 있습니다. 애플리케이션이 설치되어 있는 경우에만 패치가 취약점을 수정할 수 있습니다.

취약점을 수정하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.

2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.

3. **저장소** 창에서 **취약점** 탭을 선택합니다.
   취약점 탭에는 취약점 검사 작업 중 Kaspersky Endpoint Security가 탐지한 취약점 목록이 포함됩니다.

4. 취약점 목록에서 관련 취약점에 해당하는 항목을 선택합니다.
   이 취약점에 대한 정보 및 이를 수정하는 방법을 포함하고 있는 섹션이 취약점 목록 하단에 열립니다.
   선택한 각 취약점에 대해 다음과 같은 정보를 확인할 수 있습니다:

   - 취약점이 탐지된 애플리케이션의 이름.
   - 취약점이 탐지된 애플리케이션의 버전.
   - 취약점 심각도.
   - 취약점 ID.
   - 마지막으로 취약점을 탐지한 날짜 및 시간.
   - 취약점 수정에 대한 권장 사항(예: 운영 체제 업데이트 또는 애플리케이션 패키지가 있는 웹사이트 링크).
   - 취약점에 대한 설명이 포함된 웹사이트 링크.

5. 취약점에 대한 자세한 설명을 보려면 **추가 정보 (영문 웹사이트)** 링크를 눌러 선택한 취약점과 관련된 보안위협에 대한 설명이 있는 웹 페이지를 엽니다. www.secunia.com 웹사이트에서 최신 버전의 애플리케이션에 필요한 업데이트를 다운로드하여 설치할 수 있습니다.

6. 취약점을 수정할 수 있는 다음 방법 중 하나를 선택합니다:

   - 애플리케이션에 대해 사용할 수 있는 패치가 하나 이상인 경우 패치 이름 옆에 제공된 지침을 따라 필요한 패치를 설치합니다.
   - 운영 체제 업데이트를 사용할 수 있는 경우 업데이트 옆에 제공된 지침을 따라 필요한 업데이트를 설치합니다.

   패치 또는 업데이트를 설치하면 취약점이 수정됩니다. Kaspersky Endpoint Security에서 취약점이 수정되었음을 나타내는 상태를 이 취약점에 지정합니다. 수정된 취약점에 대한 항목은 취약점 목록에서 회색으로 표시됩니다.

7. 취약점을 수정하는 방법에 대한 정보가 해당 창 하단에 제공되어 있지 않은 경우 Kaspersky Endpoint Security 데이터베이스 및 모듈을 업데이트한 후 취약점 검사 작업을 다시 시작해 봅니다. Kaspersky Endpoint Security는 취약점 데이터베이스를 사용하여 시스템에 해당 취약점이 있는지 검사하므로, 애플리케이션을 업데이트한 후 수정된 취약점에 대한 항목이 나타날 수 있습니다.

취약점 목록의 항목 숨장치

선택한 취약점 항목을 숨길 수 있습니다. Kaspersky Endpoint Security는 취약점 목록에서 선택되어 있고 숨김으로 표시된 항목에 *무시한 취약점* 상태를 지정합니다. *숨겨진* 상태 값을 사용하여 취약점 목록을 필터링할 수 있습니다.

취약점 목록의 항목을 숨기려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.
3. **저장소** 창에서 **취약점** 탭을 선택합니다.

   취약점 탭에는 취약점 검사 작업 중 Kaspersky Endpoint Security가 탐지한 취약점 목록이 포함됩니다.
4. 취약점 목록에서 숨기고 싶은 취약점에 대한 항목을 선택합니다.

   이 취약점에 대한 정보 및 이를 수정하는 방법을 포함하고 있는 섹션이 취약점 목록 하단에 열립니다.
5. **취약점 무시** 버튼을 누릅니다.

   Kaspersky Endpoint Security는 선택한 취약점에 *무시한 취약점* 상태를 지정합니다. *무시한 취약점* 상태를 가진 취약점에 대한 항목은 취약점 목록의 끝으로 이동되고 어두워집니다.
6. 취약점 목록에서 취약점에 대한 항목을 숨장치 위해서는 목록의 윗 부분에서 **무시한 취약점** 확인란을 선택합니다.

심각도 레벨을 기준으로 취약점 목록 필터링

심각도 레벨을 기준으로 취약점 목록을 필터링하는 방법은 다음과 같습니다:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.

3. **저장소** 창에서 **취약점** 탭을 선택합니다.

   취약점 탭에는 취약점 검사 작업 중 Kaspersky Endpoint Security가 탐지한 취약점 목록이 포함됩니다. 취약점 심각도(경고, 중요, 매우 중요)의 3가지 아이콘은 **심각도 표시** 열에 위치한 취약점 목록 상단에 나타납니다. 이 아이콘을 누르면, 심각도별로 취약점 목록을 필터링할 수 있습니다.

4. 취약점 심각도의 하나, 둘 또는 세 개의 아이콘을 누릅니다. 선택한 심각도와 일치하는 취약점이 목록에 나타납니다. 목록에 특정 심각도와 일치하는 취약점을 보이지 않게 하려면, 관련 심각도의 아이콘을 다시 누릅니다. 만일 심각도 아이콘을 선택하지 않으면, 취약점 목록에는 아무 것도 나타나지 않습니다.

저장소 창을 닫으면 지정된 취약점 항목 필터링 조건이 저장됩니다.

수정 및 숨김 상태 값으로 취약점 목록 필터링

수정 및 숨김 상태 값으로 취약점 목록을 필터링하는 방법은 다음과 같습니다:

1. 메인 애플리케이션 창을 엽니다.

2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.

3. **저장소** 창에서 **취약점** 탭을 선택합니다.

   취약점 탭에는 취약점 검사 작업 중 Kaspersky Endpoint Security가 탐지한 취약점 목록이 포함됩니다.

4. 취약점 상태에 대한 확인란이 **목록 표시** 설정 옆에 표시됩니다. *수정됨* 상태를 기준으로 취약점 목록을 필터링하려면 다음 중 하나를 수행합니다:

   - 취약점 목록에 수정된 취약점에 대한 항목을 표시하려면 **수정됨** 확인란을 선택합니다. 수정된 취약점 항목은 취약점 목록에서 회색으로 표시됩니다.

   - 취약점 목록에 수정된 취약점에 대한 항목을 숨기려면 **수정됨** 확인란을 선택 취소합니다.

5. *무시한 취약점* 상태를 기준으로 취약점 목록을 필터링하려면 다음 중 하나를 수행합니다:

   - 취약점 목록에 숨겨진 취약점에 대한 항목을 표시하려면 **무시한 취약점** 확인란을 선택합니다. 숨겨진 취약점 항목은 취약점 목록에서 회색으로 표시됩니다.

   - 취약점 목록에 숨겨진 취약점에 대한 항목을 표시하지 않으려면 **무시한 취약점** 확인란을 선택 취소합니다.

저장소 창을 닫은 이후에 지정된 취약점 항목 필터링 조건이 저장되지 않습니다.

애플리케이션 모듈 무결성 확인

이 섹션에는 무결성 검사 작업의 특성 및 설정에 대한 정보가 나와 있습니다.

무결성 검사 작업 정보

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.

무결성 체크 작업이 시작되면 Kaspersky Endpoint Security 메인 창의 **보호 및 제어** 탭에 있는 **작업** 섹션의 작업 이름 옆 필드에 완료 진행 상황이 표시됩니다.

무결성 검사 작업 결과는 리포트에 기록됩니다.

무결성 검사 작업 시작 또는 중지

선택한 스케줄에 관계없이 언제라도 무결성 검사 작업을 시작 또는 중지할 수 있습니다.

무결성 검사 작업을 시작 또는 중지하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **보호 및 제어** 탭을 선택합니다.
3. **작업** 섹션을 엽니다.
4. 마우스 오른쪽 버튼을 눌러 무결성 검사 작업 이름이 포함된 행의 마우스 오른쪽 메뉴를 엽니다.
5. 다음 중 하나를 수행합니다:
   - 무결성 검사 작업을 시작하려면 마우스 오른쪽 메뉴에서 **검사 시작**을 선택합니다.
     이 작업의 이름과 함께 버튼 오른쪽에 표시된 작업 진행 상태가 *실행 중*으로 바뀝니다.
   - 무결성 검사 작업을 중지하려면 마우스 오른쪽 메뉴에서 **검사 중지**를 선택합니다.
     이 작업의 이름과 함께 버튼 오른쪽에 표시된 작업 진행 상태가 *중지됨*으로 바뀝니다.

무결성 검사 작업 스케줄 선택

무결성 검사 작업의 스케줄을 선택하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **스케줄된 작업** 섹션에서 **무결성 검사**를 선택합니다.
   창 오른쪽 부분에 무결성 검사 작업 설정이 표시됩니다.

3. **스케줄** 섹션에서 다음 옵션 중 하나를 선택합니다:

   - 무결성 검사 작업을 수동으로 시작하려면 **수동**을 선택합니다.
   - 무결성 검사 작업의 시작 스케줄을 구성하려면 **스케줄에 따라 실행**을 선택합니다.

4. 이전 단계에서 **스케줄에 따라 실행** 옵션을 선택했으면 작업 스케줄의 설정을 지정합니다. 이를 위해서는 다음과 같이 하십시오:

   a. **빈도** 드롭다운 목록에서 무결성 검사 작업을 시작할 시기를 지정합니다. 다음 옵션 중 하나를 선택합니다: **분**, **시**, **일**, **매주**, **지정한 시간**, **매달** 또는 **애플리케이션 시작 후**.

   b. **빈도** 드롭다운 목록에서 선택한 항목에 따라 작업 시작 시간을 정의하는 설정의 값을 지정합니다.

   c. Kaspersky Endpoint Security에서 건너뛴 무결성 검사 작업을 최대한 빨리 실행하도록 하려면 **건너뛴 작업 실행** 확인란을 선택합니다.

   > **빈도** 드롭다운 목록에서 **애플리케이션 시작 후**, **분** 또는 **시간**을 선택한 경우에는 **건너뛴 작업 실행** 확인란을 사용할 수 없습니다.

   d. 컴퓨터 리소스가 제한된 경우에 Kaspersky Endpoint Security에서 작업을 일시 중지하려고 한다면, **컴퓨터가 유휴 상태일 때만 실행** 확인란을 선택합니다.

   이 스케줄 옵션을 사용하면 컴퓨터 리소스를 절약할 수 있습니다.

5. **확인**을 누릅니다.

6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

리포트 관리

이 섹션에서는 리포트 설정을 구성하고 리포트를 관리하는 방법에 대해 설명합니다.

리포트 관리 원칙

리포트에는 각 Kaspersky Endpoint Security 구성요소의 작업, 각 검사 작업, 업데이트 작업, 무결성 제어 작업 및 취약점 검사 작업의 성능, 애플리케이션의 전반적인 작업에 대한 정보가 기록됩니다.

리포트 데이터는 이벤트 목록이 포함된 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 그래프 이름 옆에 있는  버튼을 누릅니다. 다양한 구성요소 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 구성요소 또는 작업과 관련되지 않은 이벤트에 대한 정보를 포함합니다.
- **모든 보호 구성 요소** 리포트. 다음과 같은 Kaspersky Endpoint Security 구성요소의 작동 중 기록되는 이벤트에 대한 정보를 포함합니다:
  - 파일 안티 바이러스
  - 메일 안티 바이러스.
  - 웹 안티 바이러스.
  - 메신저 안티 바이러스.
  - 시스템 감시기.
  - 방화벽.
  - 네트워크 공격 차단.
  - BadUSB 공격 차단.
- Kaspersky Endpoint Security 구성요소 또는 작업 실행 동작에 대한 리포트입니다.
- **암호화** 리포트. 데이터 암호화 및 복호화 프로세스 동안 발생한 이벤트에 대한 정보가 들어 있습니다.

리포트는 다음 이벤트 중요도를 사용합니다:

- **정보 이벤트**.  아이콘. 대개 중요한 정보를 포함하지 않는 공식 이벤트입니다.
- **중요 이벤트**.  아이콘. 이러한 이벤트는 Kaspersky Endpoint Security 작동 중에 발생한 중요한 상황을 나타내므로 주의해야 합니다.
- **심각 이벤트**.  아이콘. 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 목록 필터링.
- 검색 기능을 사용하여 특정 이벤트를 찾습니다.
- 선택한 이벤트를 개별 섹션에서 봅니다.
- 각 리포트 열별로 이벤트 목록을 정렬합니다.
- 이벤트 필터를 사용해 그룹화된 이벤트를 표시하거나 숨깁니다.
- 리포트에 표시되는 열의 순서와 정렬을 변경합니다.

필요한 경우 생성한 리포트는 텍스트 파일로 저장할 수 있습니다.

또한 그룹으로 결합된 Kaspersky Endpoint Security 구성요소 및 작업에 대한 리포트 정보를 삭제 할 수 있습니다. Kaspersky Endpoint Security는 가장 먼저 생성된 항목부터 현재 시간까지의 선택한 모든 리포트 항목을 삭제합니다.

리포트 설정 구성

다음과 같은 방법으로 리포트 설정을 구성할 수 있습니다:

- 최대 리포트 저장 기간을 구성합니다.

  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. 시간 기준의 제한을 취소하거나 최대 리포트 저장 기간을 변경할 수 있습니다.

- 리포트 파일의 최대 크기를 구성합니다.

  리포트가 포함된 파일의 최대 크기를 지정할 수 있습니다. 리포트 파일의 최대 크기 기본 값은 1024MB입니다. Kaspersky Endpoint Security는 리포트 파일 크기가 최대 한도에 도달하면 리포트 파일에서 가장 오래된 항목을 자동으로 삭제하여 최대 한도를 넘지 않도록 관리합니다. 리포트 파일의 크기에 대한 제한을 취소하거나 서로 다른 값을 설정할 수 있습니다.

최대 리포트 저장 기간 구성

리포트 최대 저장 기간을 수정하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **고급 설정** 섹션에서 **리포트 및 저장소**를 선택합니다.
3. 창 오른쪽의 **리포트 설정** 섹션에서 다음 작업 중 하나를 수행합니다:

   - 리포트 저장 기간의 제한하려면 **리포트 저장 기간** 확인란의 선택합니다. **리포트 저장 기간** 확인란 옆에 칸에 최대 리포트 저장 기간을 지정합니다.

     리포트 최대 저장 기간의 기본값은 30일입니다.

   - 리포트 저장 기간의 제한을 취소하려면 **리포트 저장 기간** 확인란의 버튼을 지웁니다.

   리포트 저장 기간의 제한은 기본적으로 작동됩니다.

4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

리포트 파일의 최대 크기 구성

최대 리포트 파일 크기를 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **고급 설정** 섹션에서 **리포트 및 저장소**를 선택합니다.
3. 창 오른쪽의 **리포트 설정** 섹션에서 다음 작업 중 하나를 수행합니다:
   - 리포트 파일 크기를 제한하려면 **최대 파일 크기** 확인란을 선택합니다. **최대 파일 크기** 확인란의 오른쪽 필드에서 최대 리포트 파일 크기를 지정합니다.
     리포트 파일의 기본 크기는 1024MB로 제한됩니다.
   - 리포트 파일 크기를 제한하지 않으려면 **최대 파일 크기** 확인란을 선택 취소합니다.

   리포트 파일 크기 제한은 기본적으로 작동됩니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

리포트 보기

리포트를 보려면:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **리포트** 링크를 눌러 **리포트** 창을 엽니다.
3. 모든 보호 구성 요소 리포트를 생성하려면 **리포트** 창의 왼쪽에 있는 구성 요소 및 작업 목록에서 **모든 보호 구성 요소** 항목을 선택합니다.
   창 오른쪽에 모든 보호 구성요소의 작동 중 발생한 이벤트 목록이 포함된 모든 보호 구성요소 리포트가 표시됩니다.
4. 구성요소 또는 작업의 작동에 대한 리포트를 생성하려면 **리포트** 창의 왼쪽에 있는 구성요소 및 작업의 목록에서 구성요소 또는 작업을 선택합니다.
   창 오른쪽에 선택한 Kaspersky Endpoint Security 구성요소 또는 작업의 작동 중 발생한 이벤트의 목록이 포함된 리포트가 표시됩니다.

기본적으로 리포트 이벤트는 **이벤트 날짜** 열 값의 오름차순으로 정렬됩니다.

리포트에 이벤트 정보 표시

리포트에 각 이벤트에 대한 상세 요약을 표시할 수 있습니다.

리포트에 각 이벤트에 대한 상세 요약을 표시하려면:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **리포트** 링크를 눌러 **리포트** 창을 엽니다.
3. 창 왼쪽에서 구성요소 또는 작업과 관련된 리포트를 선택합니다.
   리포트 범위에 포함된 이벤트는 창의 오른쪽 부분에 있는 테이블에 나타납니다. 리포트에서 특정 이벤트를 찾으려면, 필터, 검색 및 분류 기능을 사용할 수 있습니다.
4. 리포트에서 관련 이벤트를 선택합니다.

   이벤트 요약을 포함하고 있는 섹션은 창 아래 부분에 표시됩니다.

파일에 리포트 저장

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 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **리포트** 링크를 눌러 **리포트** 창을 엽니다.
3. 다음 중 하나를 수행합니다:
   - "모든 보호 구성 요소" 리포트를 생성하려면 구성 요소 및 작업 목록에서 **모든 보호 구성 요소**를 선택합니다.
     창 오른쪽에 모든 보호 구성요소의 작동 중 발생한 이벤트 목록이 포함된 "모든 보호 구성요소" 리포트가 표시됩니다.
   - 특정 구성요소 또는 작업의 작동에 대한 리포트를 생성하려면 구성요소 및 작업 목록에서 해당 구성요소 또는 작업을 선택합니다.
     창 오른쪽에 선택한 구성요소 또는 작업의 작동 중 발생한 이벤트의 목록이 포함된 리포트가 표시됩니다.
4. 필요한 경우 다음을 기준으로 리포트의 데이터 표시 방법을 수정할 수 있습니다:
   - 이벤트 필터링
   - Running an event search
   - 열 다시 정렬
   - 이벤트 정렬
5. 창 오른쪽 상단에서 **리포트 저장** 버튼을 누릅니다.
   마우스 오른쪽 메뉴가 열립니다.
6. 마우스 오른쪽 메뉴에서, 리포트 파일 저장시 사용할 인코딩을 선택합니다: **ANSI로 저장** 또는 **유니코드로 저장**.
   Microsoft Office의 표준 **다른 이름으로 저장** 창이 열립니다.

7. **다른 이름으로 저장** 창에서 리포트 파일의 대상 폴더를 지정합니다.
8. **파일 이름** 필드에 리포트 파일 이름을 입력합니다.
9. **파일 형태** 필드에서 다음 중 필요한 리포트 파일 형식을 선택합니다: TXT 또는 CSV.
10. **저장** 버튼을 누릅니다.

리포트 파일 삭제

리포트에서 정보를 제거하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **고급 설정** 섹션에서 **리포트 및 저장소**를 선택합니다.
3. 창 오른쪽의 **리포트 설정** 섹션에서 **리포트 삭제** 버튼을 누릅니다.
   리포트 파일 삭제 창이 열립니다.
4. 정보를 삭제할 리포트에 해당하는 확인란을 선택합니다:
   - **모든 리포트**.
   - **일반적인 보호 리포트**. 다음 Kaspersky Endpoint Security 구성요소의 작동에 대한 정보가 포함되어 있습니다:
     - 파일 안티 바이러스
     - 메일 안티 바이러스.
     - 웹 안티 바이러스.
     - 메신저 안티 바이러스.
     - 시스템 감시기.
     - 방화벽.
     - 네트워크 공격 차단.
     - BadUSB 공격 차단.
   - **검사 작업 리포트**. 완료된 검사 작업에 대한 정보가 포함되어 있습니다:
     - 전체 검사
     - 중요한 영역 검사
     - 사용자 지정 검사
     - 무결성 검사.
   - **업데이트 작업 리포트**. 완료된 업데이트 작업에 대한 정보가 포함되어 있습니다:

- **방화벽 리포트**. 방화벽의 작동에 대한 정보가 포함되어 있습니다.
- **제어 구성요소 리포트**. 다음 Kaspersky Endpoint Security 구성요소의 작동에 대한 정보가 포함되어 있습니다:
  - 애플리케이션 시작 제어.
  - 애플리케이션 권한 제어.
  - 취약점 감시.
  - 매체 제어.
  - 웹 제어.
- **데이터 암호화 리포트**.

5. **확인**을 누릅니다.

알림 서비스

이 섹션에는 Kaspersky Endpoint Security 동작 중 발생하는 이벤트를 사용자에게 알려주는 알림 파라미터 구성 방법에 대한 지침이 나와 있습니다.

Kaspersky Endpoint Security 알림 정보

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 구성요소 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.

알림 서비스 구성

다음 처리 방법을 수행하여 알림 서비스를 구성할 수 있습니다:

- Kaspersky Endpoint Security에서 기록할 이벤트의 로그 설정을 구성합니다.
- 화면 알림 표시 방식을 구성합니다.
- 이메일 알림 전달을 구성합니다.

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. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **고급 설정** 섹션에서 **리포트 및 저장소**를 선택합니다.

창 오른쪽에 리포트 및 저장소 설정이 표시됩니다.

3. **알림** 섹션에서 **설정** 버튼을 누릅니다.

   알림 창이 열립니다.

   창 왼쪽에 Kaspersky Endpoint Security 구성요소 및 작업 목록이 표시됩니다. 창 오른쪽에 선택한 구성요소 또는 작업에 대해 생성된 이벤트를 보여줍니다.

4. 창 왼쪽에서 이벤트 로그 설정을 구성할 구성요소 또는 작업을 선택합니다.

5. **로컬 로그에 저장** 및 **Windows 이벤트 로그에 저장** 열에서 관련 이벤트 옆에 있는 확인란을 선택합니다.

   로컬 로그에 저장 열의 확인란이 선택되어 있는 이벤트는 **애플리케이션 및 서비스 로그**의 **Kaspersky 이벤트 로그** 섹션에 표시됩니다. **Windows 이벤트 로그에 저장** 열의 확인란이 선택되어 있는 이벤트는 **Windows 로그**의 **애플리케이션** 섹션에 표시됩니다. 이벤트 로그를 열려면 **시작** → **제어판** → **관리** → **이벤트 뷰어**를 누릅니다.

6. **확인**을 누릅니다.

7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

알림 표시 및 전달 구성

알림 표시 및 전달을 구성하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.

2. 창 왼쪽의 **고급 설정** 섹션에서 **리포트 및 저장소**를 선택합니다.

   창 오른쪽에 리포트 및 저장소 설정이 표시됩니다.

3. **알림** 섹션에서 **설정** 버튼을 누릅니다.

   알림 창이 열립니다.

   창 왼쪽에 Kaspersky Endpoint Security 구성요소 및 작업 목록이 표시됩니다. 창 오른쪽에 선택한 구성요소 또는 선택한 작업에 대해 생성된 이벤트를 보여줍니다.

4. 창 왼쪽의 알림 전달을 구성할 구성요소 또는 작업을 선택합니다.

5. **팝업 화면 알림** 열에서 필요한 이벤트 옆에 있는 확인란을 선택합니다.

   선택한 이벤트에 대한 정보가 Microsoft Windows 작업 표시줄 알림 영역의 팝업 메시지로 화면에 표시됩니다.

6. **이메일로 알림** 열에서 필요한 이벤트 옆에 있는 확인란을 선택합니다.

   메일 알림 전달 설정을 구성하면 선택한 이벤트에 대한 정보가 이메일로 전달됩니다.

7. **이메일 알림 설정** 버튼을 누릅니다.

   이메일 알림 설정 창이 열립니다.

8. **이벤트 알림 전송** 확인란을 선택하여 **이메일로 알림** 열에서 선택한 Kaspersky Endpoint Security 이벤트의 정보 전달을 작동합니다.

9. 이메일 알림 전달 설정을 지정합니다.

10. **확인**을 누릅니다.

11. **이메일 알림 설정** 창에서 **확인**을 누릅니다.

12. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

알림 영역의 애플리케이션 상태에 대한 경고 표시 구성

알림 영역에 애플리케이션 상태 경고를 표시하도록 구성하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **고급 설정** 섹션에서 **인터페이스**를 선택합니다.

   Kaspersky Endpoint Security 인터페이스 설정은 창 오른쪽에 표시됩니다.
3. **경고** 섹션에서 Microsoft Windows 알림 영역에 알림을 표시할 이벤트 카테고리 옆의 확인란을 선택합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

선택한 카테고리와 연결된 이벤트가 발생하면 알림 영역의 애플리케이션 아이콘이 경고의 심각도에 따라  또는  으로 바뀝니다.

격리 및 백업 저장소 관리

이 섹션에서는 격리 및 백업 저장소를 구성하는 방법에 대해 설명합니다.

격리 및 백업 저장소 정보

*격리 저장소*는 감염이 의심되는 파일의 목록입니다. *감염 의심 파일*은 바이러스 및 기타 위협 또는 그 변종을 포함할 수 있는 파일입니다.

Kaspersky Endpoint Security는 감염 의심 파일을 격리 저장소에 보관할 때 파일을 복사하지 않고 저장소로 이동합니다: 애플리케이션이 하드 드라이브 또는 이메일에서 파일을 탐지하고 특별한 데이터 저장소에 해당 파일을 저장합니다. 격리 저장소의 파일은 특별한 형식으로 저장되며 위험하지 않습니다.

Kaspersky Endpoint Security는 바이러스 검사, 파일 안티 바이러스, 메일 안티 바이러스 및 시스템 감시기 구성요소의 작동 중에 감염이 의심되는 파일을 탐지하고 격리할 수 있습니다.

Kaspersky Endpoint Security는 다음과 같은 경우에 격리 저장소에 파일을 저장합니다:

- 파일 코드가 알려져 있지만 부분적으로 수정된 악성 코드와 유사하거나 Kaspersky Endpoint Security 데이터베이스에 없지만 악성 코드와 구조가 같은 파일 코드는 경우에 격리됩니다. 이 경우 파일은 파일 안티 바이러스, 메일 안티 바이러스 또는 바이러스 검사 동안 수행된 휴리스틱 분석 후 격리 저장소로 이동합니다. 휴리스틱 분석은 허위 경보를 일으키는 일이 거의 없습니다.

- 파일이 수행하는 작업의 순서가 악성인 경우에 격리됩니다. 이 경우, 시스템 감시기 구성요소에서 동작을 분석한 후 파일이 격리저장소에 저장됩니다.

*백업 저장소*에서는 치료 도중 삭제되거나 수정된 파일의 백업 복사본 목록입니다. *백업 복사본*은 감염된 파일을 치료 또는 삭제를 처음 시도할 때 생성된 파일의 복사본입니다. 파일의 백업 복사본은 특별한 형식으로 저장되며 위험하지 않습니다.

치료 중 파일의 무결성을 유지할 수 없는 경우도 있습니다. 치료 후 해당 파일의 중요 정보에 부분적으로 또는 완전히 접근하지 못하는 경우파일의 치료된 복사본을 원래 폴더로 복원할 수 있습니다.

다른 데이터베이스 또는 애플리케이션 소프트웨어 모듈 업데이트 후 Kaspersky Endpoint Security에서 보안위협을 확인하고 처리할 수 있습니다. 따라서 각 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트 후 격리된 파일을 검사하는 것이 좋습니다.

격리 및 백업 저장소 설정 구성

데이터 저장소는 격리 및 백업 저장소로 구성됩니다. 다음과 같이 격리 및 백업 저장소 설정을 구성할 수 있습니다:

- 격리 저장소 파일과 백업 저장소 파일 복사본의 최대 저장 기간을 구성할 수 있습니다.

  격리 저장소 파일과 백업 저장소 파일 복사본의 최대 저장 기간 기본값은 30일입니다. 최대 저장 기간이 만료되면 Kaspersky Endpoint Security가 데이터 저장소에서 가장 오래된 파일을 삭제합니다. 시간 기준의 제한을 취소하거나 최대 파일 저장 기간을 변경할 수 있습니다.

- 격리 및 백업 저장소의 최대 크기를 구성할 수 있습니다.

  최대 격리 및 백업 저장소 크기의 기본 값은 100MB입니다. 데이터 저장소의 크기가 제한에 도달하면 Kaspersky Endpoint Security가 격리 및 백업 저장소에서 가장 오래된 파일을 자동으로 삭제하여 최대 데이터 저장소 크기를 초과하지 않도록 합니다. 격리 및 백업 저장소 크기 제한을 취소하거나 최대 크기를 변경할 수 있습니다.

격리 저장소 파일과 백업 저장소 파일 복사본의 최대 저장 기간 구성

격리 저장소 파일과 백업 저장소 파일 복사본의 최대 저장 기간을 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **고급 설정** 섹션에서 **리포트 및 저장소**를 선택합니다.
3. 다음 중 하나를 수행합니다:
   - 격리 및 백업 저장소의 파일 저장 기간을 제한 하려면 창 오른쪽의 **격리 및 백업 저장소 설정** 섹션에서 **개체 저장 기간** 확인란을 선택합니다. **개체 저장 기간** 확인란의 오른쪽 필드에서 격리 저장소 파일과 백업 저장소 파일 복사본에 대한 최대 저장 기간을 지정합니다. 격리 저장소 파일과 백업 저장소 파일 복사본의 기본 저장 기간은 30일입니다.
   - 격리 및 백업 저장소의 파일 저장 기간의 제한을 없애려면 창 오른쪽의 **격리 및 백업 저장소 설정** 섹션에서 **개체 저장 기간** 확인란을 선택합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

격리 및 백업 저장소의 최대 크기 구성

최대 격리 및 백업 크기를 구성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **고급 설정** 섹션에서 **리포트 및 저장소**를 선택합니다.
3. 다음 중 하나를 수행합니다:
   - 격리 및 백업 저장소의 전체 크기를 제한하려면 창 오른쪽의 **격리 및 백업 저장소 설정** 섹션에서 **최대 저장소 크기** 확인란을 선택하고 **최대 저장소 크기** 확인란 오른쪽에 있는 필드에 격리 및 백업 저장소 최대 크기를 지정합니다.

     기본적으로 격리 디렉토리와 파일의 백업 복사본으로 구성된 데이터의 최대 저장소 크기는 100MB입니다.
   - 격리 및 백업 저장소 크기 제한을 제거하려면, **격리 및 백업 저장소 설정** 섹션의 창 오른쪽에서 **최대 저장소 크기** 확인란을 선택 해제합니다.

   기본적으로 격리 및 백업 저장소 크기는 무제한입니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

격리 저장소 관리

애플리케이션 설정에 정의된 저장 기간이 경과된 후에는 Kaspersky Endpoint Security가 격리 저장소에서 모든 상태의 파일을 삭제합니다.

격리 저장소를 관리할 때는 다음과 같은 파일 작업을 할 수 있습니다:

- Kaspersky Endpoint Security에서 격리한 파일을 봅니다.
- 현재 버전의 Kaspersky Endpoint Security 데이터베이스 및 모듈을 사용하여 감염 의심 파일을 검사합니다.
- 격리 저장소의 파일을 원래 폴더로 복원합니다.
- 격리 저장소에서 파일을 제거합니다.
- 파일이 원래 있었던 폴더를 엽니다.

격리된 파일이 표로 표시됩니다.

표의 데이터를 관리할 때 다음과 같은 작업도 수행할 수 있습니다:

- 열과 사용자 지정 필터 조건을 기준으로 격리된 파일을 필터링합니다.
- 격리 저장소 파일 검색 기능을 사용합니다.
- 격리 저장소 파일을 정렬합니다.
- 격리된 파일의 표에 표시되는 열의 순서와 집합을 변경합니다.

선택한 격리 저장소 이벤트를 클립보드에 복사할 수 있습니다. 격리된 파일을 여러 개 선택하려면 마우스 오른쪽 버튼으로 아무 파일이나 눌러 메뉴를 열고 **모두 선택** 메뉴를 선택합니다. 검사하지 않을 파일을 선택 해제하려면 **CTRL** 키를 누른 상태에서 파일을 클릭합니다.

업데이트 후 격리 저장소의 파일 검사 작동 및 중지

Kaspersky Endpoint Security에서 파일을 검사할 때 감염의 징후를 탐지했으나 정확히 어떤 악성 프로그램으로 인한 감염인지 파악할 수 없는 경우, Kaspersky Endpoint Security는 해당 파일을 격리 저장소로 이동시킵니다. 데이터베이스 및 애플리케이션 모듈이 업데이트되면 Kaspersky Endpoint Security에서 이후 보안위협을 식별하여 처리할 수 있습니다. 매번 데이터베이스 및 애플리케이션 모듈 업데이트 후에 격리 저장소를 자동으로 검사하도록 설정할 수 있습니다.

격리 저장소의 파일을 정기적으로 검사하는 것이 좋습니다. 검사를 통해 파일의 상태가 변경될 수 있습니다. 그에 따라 일부 파일은 치료되고 원래 위치로 복원되어 정상적으로 사용할 수 있게 됩니다.

업데이트 후 격리 저장소 파일을 검사하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **고급 설정** 섹션에서 **리포트 및 저장소**를 선택합니다.
   창 오른쪽에 리포트 및 저장소의 관리 설정이 표시됩니다.
3. **격리 및 백업 저장소 설정** 섹션에서 다음 중 하나를 수행합니다:
   - 매번 Kaspersky Endpoint Security 업데이트 후에 격리된 파일을 검사하도록 설정하려면 **업데이트 후 격리 저장소 다시 검사** 확인란을 선택합니다.
   - 매번 Kaspersky Endpoint Security 업데이트 후에 격리된 파일을 검사하지 않도록 설정하려면 **업데이트 후 격리 저장소 다시 검사** 확인란의 선택을 취소합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

격리 저장소 파일에 대한 사용자 지정 검사 작업 시작

데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트 후 Kaspersky Endpoint Security가 격리된 파일 및 처리한 파일에서 보안위협의 유형을 확인하고 치료할 수 있습니다. 데이터베이스 및 애플리케이션 모듈을 업데이트할 때 마다 애플리케이션이 격리된 파일을 자동으로 검사하도록 구성되지 않은 경우 격리된 파일에 대한 사용자지정 검사 작업을 수동으로 시작할 수 있습니다.

격리된 파일에 대한 사용자지정 검사 작업을 시작하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.
   저장소 창의 **격리 저장소** 탭이 열립니다.
3. **격리 저장소** 탭에서 검사할 감염 의심 파일을 하나 이상 선택합니다.
   격리된 파일을 여러 개 선택하려면 마우스 오른쪽 버튼으로 아무 파일이나 눌러 메뉴를 열고 **모두 선택** 메뉴를 선택합니다. 검사하지 않을 파일을 선택 해제하려면 **CTRL** 키를 누른 상태에서 파일을 클릭합니다.
4. 다음 방법 중 하나로 사용자지정 검사 작업을 시작합니다:
   - **다시 검사** 버튼을 누릅니다.
   - 마우스 오른쪽 버튼을 눌러 마우스 오른쪽 메뉴를 열고 **다시 검사**를 선택합니다.

검사가 완료되면 검사한 파일 수와 탐지된 보안위협 수에 대한 알림이 나타납니다.

격리 저장소에서 파일 복원

격리 저장소에서 파일을 복원하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.
   저장소 창의 **격리 저장소** 탭이 열립니다.
3. 모든 격리된 파일을 복원하려면 파일의 마우스 오른쪽 메뉴에서 **모두 복원**을 선택합니다.
   Kaspersky Endpoint Security가 격리 저장소의 모든 파일을 원래 폴더로 복원합니다.
4. 격리된 파일을 하나 이상 복원하려면 다음과 같이 하십시오:
   a. **격리 저장소** 탭에서 복원하고 싶은 파일을 하나 이상 선택합니다.
      격리된 파일을 여러 개 선택하려면 마우스 오른쪽 버튼으로 아무 파일이나 눌러 메뉴를 열고 **모두 선택** 메뉴를 선택합니다. 검사하지 않을 파일을 선택 해제하려면 **CTRL** 키를 누른 상태에서 파일을 클릭합니다.
   b. 다음 중 한 방법으로 파일을 복원합니다:
      - **복원** 버튼을 누릅니다.
      - 마우스 오른쪽 메뉴를 열어 **복원**을 선택합니다.

Kaspersky Endpoint Security가 선택한 파일을 원래 폴더로 복원합니다.

격리 저장소에서 파일 삭제

격리 저장소에서 파일을 삭제하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.
   저장소 창의 **격리 저장소** 탭이 열립니다.
3. 격리 저장소의 모든 파일을 삭제하려면 파일의 마우스 오른쪽 메뉴에서 **모두 삭제**를 선택합니다.
   Kaspersky Endpoint Security가 격리 저장소에서 모든 파일을 삭제합니다.
4. 격리된 파일을 하나 이상 삭제하려면 다음과 같이 하십시오:
   a. **격리 저장소** 탭의 표에서 삭제하고 싶은 감염 의심 파일을 하나 이상 선택합니다.
      격리된 파일을 여러 개 선택하려면 마우스 오른쪽 버튼으로 아무 파일이나 눌러 메뉴를 열고 **모두 선택** 메뉴를 선택합니다. 검사하지 않을 파일을 선택 해제하려면 **CTRL** 키를 누른 상태에서 파일을 클릭합니다.
   b. 다음 중 한 방법으로 파일을 삭제합니다:
      - **제거** 버튼을 누릅니다.
      - 마우스 오른쪽 메뉴를 열어 **삭제**를 선택합니다.

그러면, Kaspersky Endpoint Security가 격리 저장소에서 선택된 파일을 삭제합니다.

백업 저장소 관리

파일에서 악성 코드가 탐지되면 Kaspersky Endpoint Security가 해당 파일을 차단하고, 백업 저장소에 복사본을 저장한 후 치료합니다. 파일 치료에 성공하면 파일의 백업 복사본 상태가 *치료됨*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.

Windows Store 애플리케이션에 포함된 파일에서 악성 코드가 탐지되면 Kaspersky Endpoint Security는 백업 저장소로 그 복사본을 옮기지 않고 즉시 파일을 삭제합니다. Microsoft Windows 8 운영 체제의 적절한 도구를 사용하여 Windows Store 애플리케이션의 무결성을 복원할 수 있습니다(Windows Store 애플리케이션 복원에 대한 자세한 내용은 *Microsoft Windows 8 도움말 파일* 참조).

애플리케이션 설정에 정의된 저장 기간이 경과된 후에는 Kaspersky Endpoint Security가 백업 저장소에서 모든 상태의 파일 백업 복사본을 자동으로 삭제합니다.

백업 저장소에서 파일의 복사본을 직접 삭제할 수도 있습니다.

파일의 백업 복사본 세트가 테이블에 표시됩니다.

백업 저장소를 관리할 때 파일의 백업 복사본에 대해 다음과 같은 작업을 수행할 수 있습니다:

- 파일의 백업 복사본 세트를 봅니다.

- 백업 복사본의 파일을 원래 폴더로 복원합니다.
- 백업 저장소에서 파일의 백업 복사본을 삭제합니다.

표의 데이터를 관리할 때 다음과 같은 작업도 수행할 수 있습니다:

- 사용자 지정 필터 조건을 포함하여 열별로 백업 복사본을 필터링합니다.
- 백업 복사본 검색 기능을 사용합니다.
- 백업 복사본을 정렬합니다.
- 백업 복사본의 표에 표시되는 열의 순서와 집합을 변경합니다.

선택한 백업 저장소 이벤트를 클립보드에 복사할 수 있습니다. 백업 파일을 여러 개 선택하려면 마우스 오른쪽 버튼으로 아무 파일이나 눌러 메뉴를 열고 **모두 선택** 메뉴를 선택합니다. 검사하지 않을 파일을 선택 해제하려면 **CTRL** 키를 누른 상태에서 파일을 클릭합니다.

백업 저장소에서 파일 복원

백업 저장소에서 파일을 복원하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.
3. **저장소** 창에서 **백업 저장소** 탭을 선택합니다.
4. 백업 저장소의 모든 파일을 복원하려면 파일의 마우스 오른쪽 메뉴에서 **모두 복원**을 선택합니다.

   Kaspersky Endpoint Security가 백업 저장소의 모든 파일을 원래 폴더로 복원합니다.
5. 백업 저장소에서 파일을 하나 이상 복원하려면 다음과 같이 하십시오:

   a. 표의 **백업 저장소** 탭에서 백업 파일을 하나 이상 선택합니다.

   격리된 파일을 여러 개 선택하려면 마우스 오른쪽 버튼으로 아무 파일이나 눌러 메뉴를 열고 **모두 선택** 메뉴를 선택합니다. 검사하지 않을 파일을 선택 해제하려면 **CTRL** 키를 누른 상태에서 파일을 클릭합니다.

   b. 다음 중 한 방법으로 파일을 복원합니다:

   - **복원** 버튼을 누릅니다.
   - 마우스 오른쪽 메뉴를 열어 **복원**을 선택합니다.

   Kaspersky Endpoint Security가 선택된 백업 복사본의 파일을 원래 폴더로 복원합니다.

백업 저장소에서 파일의 백업 복사본 삭제

백업 저장소에서 파일의 백업 복사본을 삭제하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.

2. 메인 애플리케이션 창 상단에서 **격리 저장소** 링크를 눌러 **저장소** 창을 엽니다.

3. **저장소** 창에서 **백업 저장소** 탭을 선택합니다.

4. 백업 저장소의 모든 파일을 삭제하려면 다음 처리 방법 중 하나를 수행합니다:

   - 파일의 마우스 오른쪽 메뉴에서 **모두 삭제**를 선택합니다.
   - **저장소 비우기** 버튼을 누릅니다.

   Kaspersky Endpoint Security가 백업 저장소의 모든 파일 백업 복사본을 삭제합니다.

5. 백업 저장소에서 한 개 이상의 파일을 삭제하려면 다음을 수행합니다:

   a. 표의 **백업 저장소** 탭에서 백업 파일을 하나 이상 선택합니다.

   백업 파일을 여러 개 선택하려면 마우스 오른쪽 버튼으로 아무 파일이나 눌러 메뉴를 열고 **모두 선택** 메뉴를 선택합니다. 검사하지 않을 파일을 선택 해제하려면 **CTRL** 키를 누른 상태에서 파일을 클릭합니다.

   b. 다음 중 한 방법으로 파일을 삭제합니다:

   - **제거** 버튼을 누릅니다.
   - 마우스 오른쪽 메뉴를 열어 **삭제**를 선택합니다.

   Kaspersky Endpoint Security가 백업 저장소에서 선택한 백업 복사본을 삭제합니다.

고급 애플리케이션 설정

이 섹션에서는 Kaspersky Endpoint Security의 고급 설정과 해당 설정을 구성하는 방법에 대해 설명합니다.

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.
  그러려면 배포 패키지가 저장되어 있는 동일한 폴더에 구성 파일을 저장해야 합니다.
- 사전에 지정한 설정을 사용하여 Kaspersky Security Center를 통해 Kaspersky Endpoint Security 원격 설치를 수행합니다.
- 한 컴퓨터에서 다른 컴퓨터로 Kaspersky Endpoint Security 설정을 마이그레이션합니다.

구성 파일을 생성하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.
   창 오른쪽에 고급 애플리케이션 설정이 표시됩니다.
3. **설정 관리** 섹션에서 **저장** 버튼을 클릭합니다.
   Microsoft Windows 표준 **구성 파일을 선택하십시오** 창이 열립니다.
4. 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. **저장** 버튼을 누릅니다.

구성 파일의 Kaspersky Endpoint Security 설정을 가져오려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.
   창 오른쪽에 고급 애플리케이션 설정이 표시됩니다.
3. **설정 관리** 섹션에서 **가져오기** 버튼을 클릭합니다.
   Microsoft Windows 표준 **구성 파일을 선택하십시오** 창이 열립니다.
4. 구성 파일의 경로를 지정합니다.
5. **열기** 버튼을 누릅니다.

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

신뢰구역

이 섹션에는 신뢰 구역에 대한 정보 및 검사 예외를 구성하고 신뢰하는 애플리케이션 목록을 만들기 위한 지침이 나와 있습니다.

신뢰 구역 정보

*신뢰 구역*은 Kaspersky Endpoint Security에서 감시하지 않는 개체 및 애플리케이션을 시스템 관리자가 구성한 목록입니다. 즉, 이는 검사 예외의 집합입니다.

관리자는 처리되는 개체와 컴퓨터에 설치된 애플리케이션의 기능을 고려하여 독립적으로 신뢰구역을 형성합니다. 사용자가 안전하다고 확신하는 개체 또는 애플리케이션인데도 Kaspersky Endpoint Security가 해당 개체 또는 애플리케이션에 대한 접근을 차단하면 개체와 애플리케이션을 신뢰 구역에 포함시키는 것이 좋습니다.

검사에서 다음 개체를 예외할 수 있습니다:

- 특정 형식의 파일
- 마스크에 의해 선택된 파일
- 선택한 파일
- 폴더
- 애플리케이션 프로세스

검사 예외

*검사 예외*는 Kaspersky Endpoint Security에서 개체의 바이러스 및 기타 보안위협을 검사하지 않는 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 악성 코드에서 보조 구성요소로 사용될 수 있습니다. 이런 애플리케이션에는 원격 관리 도구, IRC 클라이언트, FTP 서버, 프로세스를 일시 중지 또는 숨장치 위한 다양한 유틸리티, 키로거, 암호 해킹 프로그램, 자동 전화 걸기 등이 포함됩니다. 이러한 애플리케이션은 바이러스와 분류되지 않습니다. 범죄자가 컴퓨터 또는 개인 데이터를 손상시킬 목적으로 악용할 수 있는 합법적인 소프트웨어에 대한 세부 정보는 Kaspersky Lab 바이러스 백과사전 (https://encyclopedia.kaspersky.com/knowledge/riskware/)에서 확인할 수 있습니다.

이러한 애플리케이션은 Kaspersky Endpoint Security에 의해 차단될 수 있습니다. 차단되는 것을 방지하기 위해 사용 중인 애플리케이션에 대한 검사 예외를 구성할 수 있습니다. 그러려면 Kaspersky 바이러스 백과사전에 나와 있는 이름이나 이름 마스크를 신뢰 구역에 추가합니다. 예를 들어 Remote Administrator 프로그램을 자주 사용할 수 있습니다. 이는 원격 컴퓨터를 제어하는 원격 접근 애플리케이션입니다. Kaspersky Endpoint Security는 이러한 활동을 의심스러운 것으로 간주하여 차단할 수 있습니다. 애플리케이션이 차단되는 것을 방지하기 위해 Kaspersky 바이러스 백과사전(진단명)에 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 구성요소 및 작업에서 사용할 수 있습니다:

- 파일 안티 바이러스
- 메일 안티 바이러스.
- 웹 안티 바이러스.
- 애플리케이션 권한 제어.
- 검사 작업
- 시스템 감시기.

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 프로그램 프로세스에서 열려 있거나 실행하거나 저장하는 개체를 검사하고 모든 애플리케이션 활동과 그로 인해 생성되는 네트워크 트래픽을 제어합니다. Kaspersky Endpoint Security는 신뢰하는 애플리케이션 목록에 있는 애플리케이션을 검사 대상에서 예외합니다.

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 추가할 수 있습니다. 그러면 이 애플리케이션에서 사용하는 개체는 검사에서 예외됩니다.

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 애플리케이션을 검사에서 예외하면 Kaspersky Endpoint Security와 다른 프로그램 간에 호환성 문제(예: Kaspersky Endpoint Security와 기타 안티 바이러스 애플리케이션에서 타사 컴퓨터의 네트워크 트래픽을 이중 검사하는 문제)를 피할 수 있으며, 서버 애플리케이션을 사용할 때 중요시되는 컴퓨터 성능 수준을 향상시킬 수 있습니다.

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.

검사 예외 생성

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 예외를 생성하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.

창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.

3. **검사 예외 및 신뢰하는 애플리케이션** 섹션에서 **설정** 버튼을 누릅니다.

   예외 (신뢰 구역) 창에서 **검사 예외** 탭이 열립니다.

4. **추가** 버튼을 누릅니다.

   검사 예외 창이 열립니다. 이 창에서 **속성** 섹션의 기준을 한 개 또는 두 개 모두 사용하여 검사 예외를 생성할 수 있습니다.

5. 파일 또는 폴더를 검사 대상에서 예외시키려면 다음과 같이 하십시오:

   a. **속성** 섹션에서 **파일 또는 폴더** 확인란을 선택합니다.

   b. **파일이나 폴더**의 이름 창을 열려면, **예외 설명**에서 **파일 또는 폴더 이름** 링크를 클릭합니다.

   c. 파일 또는 폴더 이름이나 파일 또는 폴더 이름의 마스크를 입력하거나 **찾아보기**를 눌러 폴더 트리에서 파일 또는 폴더를 선택합니다.

   파일 또는 폴더 이름 마스크에서 별표 문자(*)를 사용하여 파일 이름에 모든 문자의 조합을 대체할 수 있습니다.

   예를 들어, 다음 경로를 추가할 때 마스크를 사용할 수 있습니다:

   - 모든 폴더에 있는 파일에 대한 경로:
     - "*.exe" 마스크는 EXE 확장자를 가진 파일의 모든 경로를 포함합니다.
     - "test" 마스크는 "test" 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\ 폴더에 있는 파일에 대한 모든 경로를 포함하지만 C:\dir\의 하위 폴더는 포함하지 않습니다.
     - "C:\dir\" 마스크는 C:\dir\ 폴더에 있는 파일에 대한 모든 경로를 포함하지만 C:\dir\의 하위 폴더는 포함하지 않습니다.
     - "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.
   - 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.

d. **파일 또는 폴더 이름** 창에서 **확인**을 누릅니다.
추가된 파일 또는 폴더에 연결되는 링크가 **검사 예외** 창의 **예외 설명** 섹션에 나타납니다.

6. 특정 이름의 개체를 검사 대상에서 예외시키려면 다음과 같이 하십시오:

a. **속성** 섹션에서 **진단명** 확인란을 선택합니다.

b. **개체 이름** 창을 열려면, **검사 예외 설명** 섹션에 있는 **진단명** 링크를 클릭합니다.

c. Kaspersky 바이러스 백과사전의 분류에 따라 개체 이름 또는 이름 마스크를 입력합니다:

d. **진단명** 창에서 **확인**을 누릅니다.
추가된 개체 이름에 연결되는 링크가 **검사 예외** 창의 **검사 예외 설명** 섹션에 나타납니다.

7. 필요하면, **설명** 필드에 사용자가 생성한 검사 예외에 대한 간단한 설명을 입력합니다.

8. 검사 예외를 사용해야 하는 Kaspersky Endpoint Security 구성요소를 지정합니다:

a. **검사 예외 설명** 섹션에서 **모두** 링크를 눌러 **구성요소 선택** 링크를 엽니다.

b. **구성요소 선택** 링크를 누르면 **보호 구성 요소** 창이 열립니다.

c. 검사 예외를 적용해야 하는 구성요소 옆의 확인란을 선택합니다.

d. **보호 구성 요소** 창에서 **확인**을 누릅니다.

구성요소가 검사 예외 설정에 지정된 경우 해당 Kaspersky Endpoint Security구성요소를 사용하여 검사할 동안에만 이 예외 규칙이 적용됩니다.

구성요소가 검사 예외 설정에 지정되지 않은 경우 해당 Kaspersky Endpoint Security 모든 구성요소를 사용하여 검사할 동안에 이 예외 규칙이 적용됩니다.

9. **검사 예외** 창에서 **확인**을 누릅니다.
예외 (신뢰 구역) 창의 검사 예외 탭 표에 추가한 **검사 예외** 항목이 나타납니다. 이 검사 예외에 대해 구성된 설정은 **검사 예외 설명** 섹션에 표시됩니다.

10. **예외 (신뢰 구역)** 창에서 **확인**을 누릅니다.

11. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

검사 예외 수정

검사 예외를 수정하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **검사 예외 및 신뢰하는 애플리케이션** 섹션에서 **설정** 버튼을 누릅니다.
   예외 (신뢰 구역) 창에서 **검사 예외** 탭이 열립니다.
4. 목록에서 수정할 검사 예외를 선택합니다.
5. 다음 방법 중 하나를 사용하여 검사 예외 설정을 변경합니다:
   - **편집** 버튼을 누릅니다.
     검사 예외 창이 열립니다.
   - **검사 예외 설명** 필드의 링크를 눌러 원하는 설정을 편집할 수 있는 창을 엽니다.
6. 이전 단계에서 **편집** 버튼을 누른 경우 **검사 예외** 창에서 **확인**을 누릅니다.
   이 검사 예외에 대해 수정된 설정은 **검사 예외 설명** 섹션에 표시됩니다.
7. **예외 (신뢰 구역)** 창에서 **확인**을 누릅니다.
8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

검사 예외 삭제

검사 예외를 삭제하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **검사 예외 및 신뢰하는 애플리케이션** 섹션에서 **설정** 버튼을 누릅니다.
   예외 (신뢰 구역) 창에서 **검사 예외** 탭이 열립니다.
4. 검사 예외 목록에 필요한 검사 항목을 선택합니다.
5. **제거** 버튼을 누릅니다.
   삭제된 검사 예외는 목록에서 사라집니다.
6. **예외 (신뢰 구역)** 창에서 **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

검사 예외 사용 및 중지

검사 예외를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **검사 예외 및 신뢰하는 애플리케이션** 섹션에서 **설정** 버튼을 누릅니다.
   예외 (신뢰 구역) 창에서 **검사 예외** 탭이 열립니다.
4. 검색 예외 목록에 필요한 예외 항목을 선택합니다.
5. 다음 중 하나를 수행합니다:
   - 검사 예외를 사용하려면 이 검사 예외 이름 옆의 확인란을 선택합니다.
   - 검사 예외를 중지하려면 이 검사 예외 이름 옆의 확인란을 선택 해제합니다.
6. **확인**을 누릅니다.
7. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

신뢰하는 애플리케이션 목록 편집

신뢰하는 애플리케이션 목록을 편집하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **검사 예외 및 신뢰하는 애플리케이션** 섹션에서 **설정** 버튼을 누릅니다.
   예외 (신뢰 구역) 창이 열립니다.
4. **예외 (신뢰 구역)** 창에서 **신뢰하는 애플리케이션** 탭을 선택합니다.
5. 다음 방법으로 신뢰하는 애플리케이션 목록에 애플리케이션을 추가합니다:
   a. **추가** 버튼을 누릅니다.
   b. 마우스 오른쪽 메뉴에서 다음 중 하나를 수행합니다:
      - 애플리케이션 목록에서 컴퓨터에 설치된 애플리케이션을 찾으려면, 해당 메뉴에서 **애플리케이션** 항목을 선택합니다.
        애플리케이션 선택 창이 열립니다.
      - 관련 애플리케이션의 실행 파일 경로를 지정하려면 **찾아보기**를 선택합니다.
        Microsoft Windows의 표준 **파일 열기** 창이 열립니다.
   c. 다음과 방법 중 하나로 애플리케이션을 선택합니다:
      - 이전 단계에서 **애플리케이션**을 선택한 경우 컴퓨터에 설치된 애플리케이션 목록에서 애플리케이션을 선택하고 **애플리케이션 선택** 창에서 **확인**을 누릅니다.

- 이전 단계에서 **찾아보기**를 선택한 경우 관련 애플리케이션의 실행 파일 경로를 지정하고 Microsoft Windows 표준 **열기** 창에서 **열기** 버튼을 누릅니다.

이렇게 하면 **애플리케이션 검사 예외** 창이 열립니다.

a. 선택한 애플리케이션과 관련된 신뢰 구역 규칙 옆의 확인란을 선택합니다:

- **열린 파일 검사 안 함**.
- **애플리케이션 활동 감시 안 함**.
- **부모 프로세스(애플리케이션)의 제한을 상속하지 않음**.
- **자식 애플리케이션의 활동 감시 안 함**.
- **애플리케이션 인터페이스 원격 제어 차단 안 함**.
- **네트워크 트래픽 검사 안 함**.

b. **애플리케이션 검사 예외** 창에서 **확인**을 누릅니다.
사용자가 추가한 애플리케이션이 신뢰하는 애플리케이션 목록에 나타납니다.

6. 다음 방법으로 신뢰하는 애플리케이션 설정을 편집합니다:

a. 신뢰하는 애플리케이션 목록에서 애플리케이션을 선택합니다.

b. **편집** 버튼을 누릅니다.

c. **애플리케이션 검사 예외** 창이 열립니다.

d. 선택한 애플리케이션과 관련된 신뢰 구역 규칙 옆의 확인란을 선택 또는 선택 취소합니다:

> **애플리케이션 검사 예외** 창에서 신뢰 구역 규칙을 선택하지 않은 경우, 신뢰하는 애플리케이션이 검사에 포함됩니다. 이 경우 신뢰하는 애플리케이션이 목록에서 제거되지 않지만 해당 확인란의 선택은 취소됩니다.

e. **애플리케이션 검사 예외** 창에서 **확인**을 누릅니다.

7. 다음 방법으로 애플리케이션을 신뢰하는 애플리케이션 목록에서 제거합니다:

a. 신뢰하는 애플리케이션 목록에서 애플리케이션을 선택합니다.

b. **제거** 버튼을 누릅니다.

8. **예외 (신뢰 구역)** 창에서 **확인**을 누릅니다.

9. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

신뢰하는 애플리케이션 목록의 애플리케이션에 대한 신뢰 구역 규칙 사용 및 중지

신뢰하는 애플리케이션 목록의 애플리케이션에 적용된 신뢰 구역 규칙의 처리를 작동 또는 중지하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **검사 예외 및 신뢰하는 애플리케이션** 섹션에서 **설정** 버튼을 누릅니다.
   예외 (신뢰 구역) 창이 열립니다.
4. **예외 (신뢰 구역)** 창에서 **신뢰하는 애플리케이션** 탭을 선택합니다.
5. 신뢰하는 애플리케이션의 목록에서 필요한 애플리케이션을 선택합니다.
6. 다음 중 하나를 수행합니다:
   - Kaspersky Endpoint Security 검사 대상에서 신뢰하는 애플리케이션을 예외하려면 이름 옆에 있는 확인란을 선택합니다.
   - Kaspersky Endpoint Security 검사 대상에 신뢰하는 애플리케이션을 포함하려면 이름 옆에 있는 확인란을 선택합니다.
7. **확인**을 누릅니다.
8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

신뢰하는 시스템 인증서 저장소 사용

시스템 인증서 저장소를 사용하면 신뢰하는 디지털 서명으로 서명된 애플리케이션을 바이러스 검사에서 예외할 수 있습니다. Kaspersky Endpoint Security는 이러한 애플리케이션을 *제어 그룹*에 자동으로 할당합니다.

신뢰하는 시스템 인증서 저장소 사용을 시작하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **검사 예외 및 신뢰하는 애플리케이션** 섹션에서 **설정** 버튼을 누릅니다.
   예외 (신뢰 구역) 창이 열립니다.
4. **예외 (신뢰 구역)** 창에서 **신뢰하는 시스템 인증서 저장소** 탭을 선택합니다.
5. **신뢰하는 시스템 인증서 저장소 사용** 확인란을 선택합니다.
6. **신뢰하는 시스템 인증서 저장소** 드롭다운 목록에서 신뢰할 Kaspersky Endpoint Security 시스템 저장소를 선택합니다.
7. **예외 (신뢰 구역)** 창에서 **확인**을 누릅니다.
8. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

Kaspersky Endpoint Security 자기-보호 기능

이 섹션에는 Kaspersky Endpoint Security의 자기-보호 기능 및 원격 제어 방역 메커니즘에 대한 설명과 해당 메커니즘의 설정을 구성하는 방법에 대한 지침이 나와 있습니다.

Kaspersky Endpoint Security 자기-보호 기능 정보

Kaspersky Endpoint Security는 Kaspersky Endpoint Security의 작업을 차단하거나 컴퓨터에서 Kaspersky Endpoint Security를 삭제하려는 악성 프로그램을 비롯하여 악성 프로그램으로부터 컴퓨터를 보호합니다.

컴퓨터 보안 시스템은 자기 보호 및 Kaspersky Endpoint Security의 원격 제어 방역 메커니즘으로 인해 안정적으로 운영됩니다.

자기-보호 메커니즘은 하드 드라이브의 애플리케이션 파일, 메모리 프로세스 및 시스템 레지스트리의 항목이 변경 또는 삭제되는 것을 방지합니다.

*원격 제어 방역*은 애플리케이션 서비스를 제어하려는 원격 컴퓨터의 모든 시도를 차단합니다.

64비트 운영 체제를 실행하는 컴퓨터에서는 Kaspersky Endpoint Security 자기-보호 기능으로만 하드 드라이브의 애플리케이션 파일 및 시스템 레지스트리 항목의 변경 및 삭제를 방지할 수 있습니다.

자기-보호 기능 작동 또는 중지

Kaspersky Endpoint Security의 자기-보호 메커니즘은 기본적으로 작동됩니다. 필요한 경우 자기-보호 기능을 중지할 수 있습니다.

자기-보호 기능을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.
   창 오른쪽에 고급 애플리케이션 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 자기-보호 메커니즘을 작동하려면 **자기-보호 사용** 확인란을 선택합니다.
   - 자기-보호 메커니즘을 중지하려면 **자기-보호 사용** 확인란의 선택을 취소합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

원격 제어 방역 작동 또는 중지

원격 제어 방역 메커니즘은 기본적으로 작동되며. 필요한 경우 메커니즘을 중지할 수 있습니다.

원격 제어 방역 메커니즘을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.
   창 오른쪽에 고급 애플리케이션 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 원격 제어 방역 메커니즘을 작동하려면 **이 애플리케이션 인터페이스에 대한 외부 원격 관리 중지**를 선택합니다.
   - 원격 제어 방역 메커니즘을 중지하려면 **이 애플리케이션 인터페이스에 대한 외부 원격 관리 중지**를 선택 해제합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

원격 관리 애플리케이션 지원

외부 제어에 대한 보호가 작동하는 동안 원격 관리 애플리케이션을 사용해야 할 수 있습니다.

원격 관리 애플리케이션을 작동하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **검사 예외 및 신뢰하는 애플리케이션** 섹션에서 **설정** 버튼을 누릅니다.
   예외 (신뢰 구역) 창이 열립니다.
4. **예외 (신뢰 구역)** 창에서 **신뢰하는 애플리케이션** 탭을 선택합니다.
5. **추가** 버튼을 누릅니다.
6. 마우스 오른쪽 메뉴에서 다음 중 하나를 수행합니다:
   - 컴퓨터에 설치되어 있는 애플리케이션의 목록에서 원격 관리 애플리케이션을 찾으려면 **애플리케이션** 항목을 선택합니다.
     애플리케이션 선택 창이 열립니다.
   - 원격 관리 애플리케이션의 실행 파일 경로를 지정하려면 **찾아보기**를 선택합니다.
     Microsoft Windows의 표준 **파일 열기** 창이 열립니다.
7. 다음과 방법 중 하나로 애플리케이션을 선택합니다:
   - 이전 단계에서 **애플리케이션**을 선택한 경우 컴퓨터에 설치된 애플리케이션 목록에서 애플리케이션을 선택하고 **애플리케이션 선택** 창에서 **확인**을 누릅니다.
   - 이전 단계에서 **찾아보기**를 선택한 경우 관련 애플리케이션의 실행 파일 경로를 지정하고 Microsoft Windows 표준 **열기** 창에서 **열기** 버튼을 누릅니다.

이렇게 하면 **애플리케이션 검사 예외** 창이 열립니다.

8. **애플리케이션 활동 감시 안 함** 확인란을 선택합니다.
9. **애플리케이션 검사 예외** 창에서 **확인**을 누릅니다.
   사용자가 추가한 애플리케이션이 신뢰하는 애플리케이션 목록에 나타납니다.
10. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

Kaspersky Endpoint Security의 성능 및 다른 애플리케이션과의 호환성

이 섹션에는 Kaspersky Endpoint Security의 작동 모드와 탐지 가능한 개체 유형을 선택하는 지침 외에 Kaspersky Endpoint Security의 성능 및 다른 애플리케이션과의 호환성 관련 정보가 포함되어 있습니다.

Kaspersky Endpoint Security의 성능 및 다른 애플리케이션과의 호환성 정보

Kaspersky Endpoint Security의 성능

Kaspersky Endpoint Security의 성능은 컴퓨터를 손상시킬 수 있는 보안위협 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
- 중요한 영역 검사 작업
- 사용자 지정 검사 작업
- 취약점 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

Kaspersky Endpoint Security의 컴퓨터 리소스 사용은 다른 애플리케이션의 성능에 영향을 줄 수 있습니다. CPU 및 하드 드라이브의 하위 시스템에 로드가 증가되는 동안 실행되는 작업의 문제를 해결하기 위해 Kaspersky Endpoint Security는 스케줄된 작업을 연기시키고 다른 애플리케이션에 리소스 우선권을 할당할 수 있습니다.

그러나 CPU 리소스에 여유가 생기면 다수의 애플리케이션이 동시에 시작되어 백그라운드에서 계속 작동합니다. 다른 애플리케이션의 성능으로 인해 검사가 영향을 받지 않도록 하려면 다른 애플리케이션에 운영 체제 리소스의 우선권을 할당하지 않는 것이 좋습니다.

필요한 경우 이런 작업을 수동으로 시작할 수 있습니다.

고급 치료(자동 재부팅) 기술 사용

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

워크스테이션용 Microsoft Windows에서 실행 중인 컴퓨터에서 고급 치료(자동 재부팅) 기술이 실행 완료된 후 Kaspersky Endpoint Security는 사용자가 컴퓨터를 재부팅하도록 요청합니다. 시스템 재부팅 후 Kaspersky Endpoint Security는 악성 파일을 삭제하고 컴퓨터 전체 검사를 시작합니다.

파일 서버용 Kaspersky Endpoint Security의 특성으로 인해 파일 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 일정에 따라 안전하게 파일 서버를 재부팅하는 것이 좋습니다. 파일 서버용에서는 고급 치료(자동 재부팅) 기술이 기본적으로 사용 안 함 설정된 이유입니다.

파일 서버에서 보안위협이 탐지될 경우 Kaspersky Security Center에 고급 치료(자동 재부팅)가 필요하다는 정보와 함께 이벤트가 전달됩니다. 파일 서버의 감염을 치료하기 위해 파일 서버용 고급 치료(자동 재부팅) 기술을 활성화하고 파일 서버 사용자가 편리한 시간에 *바이러스 검사* 그룹 작업을 시작합니다.

탐지 가능한 개체의 유형 선택

탐지 가능한 개체의 유형을 선택하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. **개체** 섹션에서 **설정** 버튼을 누릅니다.

탐지할 개체 창이 열립니다.

4. Kaspersky Endpoint Security에서 탐지할 개체 유형 옆의 확인란을 선택합니다:
   - **악성 툴**
   - **애드웨어**
   - **자동 다이얼러**
   - **기타**
   - **피해를 줄 수 있는 실행 압축 파일**
   - **다중 압축 파일**
5. **확인**을 누릅니다.
   탐지할 개체 창이 닫힙니다. **개체** 섹션에서 선택한 개체 유형이 **탐지할 개체 유형 목록**에 나열됩니다.
6. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

워크스테이션용 고급 치료(자동 재부팅) 기술 사용 또는 중지

워크스테이션용 고급 치료(자동 재부팅) 기술 작동 또는 중지하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **안티 바이러스 보호** 섹션을 선택합니다.
   창 오른쪽에 안티 바이러스 보호 설정이 표시됩니다.
3. 창 오른쪽에서 다음 중 하나를 수행합니다:
   - **고급 치료(자동 재부팅) 기술 사용**을 선택하여 고급 치료(자동 재부팅) 기술을 작동합니다.
   - **고급 치료(자동 재부팅) 기술 사용**을 선택 취소하여 고급 치료(자동 재부팅) 기술을 중지합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

자동 재 부팅 후 치료 작업이 Kaspersky Security Center를 통해 시작되면, 사용자는 운영 체제의 다수 기능을 사용할 수 없습니다. 작업이 완료된 후 워크스테이션은 재부팅됩니다.

파일 서버용 고급 치료 기술 작동 또는 중지

파일 서버용 고급 치료(자동 재부팅) 기술을 사용하려면 다음 중 하나를 수행합니다:

- 활성 Kaspersky Security Center 정책의 속성에서 고급 치료(자동 재부팅) 기술을 사용하도록 설정합니다. 이를 위해서는 다음과 같이 하십시오:

a. 정책 속성 창에서 **일반 보호 설정** 섹션을 엽니다.

b. **고급 치료(자동 재부팅) 기술 사용** 확인란을 선택합니다.

c. 변경 사항을 저장하려면 정책 속성 창에서 **확인**을 누릅니다.

- Kaspersky Security Center 바이러스 검사 그룹 작업의 속성에서 **고급 치료(자동 재부팅) 즉시 실행** 확인란을 선택합니다.

파일 서버용 고급 치료(자동 재부팅) 기술을 사용하지 않으려면 다음 중 하나를 수행합니다:

- Kaspersky Security Center 정책의 속성에서 고급 치료(자동 재부팅) 기술을 사용하도록 설정합니다. 이를 위해서는 다음과 같이 하십시오:

a. 정책 속성 창에서 **일반 보호 설정** 섹션을 엽니다.

b. **고급 치료(자동 재부팅) 기술 사용** 확인란을 선택 해제합니다.

c. 변경 사항을 저장하려면 정책 속성 창에서 **확인**을 누릅니다.

- Kaspersky Security Center 바이러스 검사 그룹 작업의 속성에서 **고급 치료(자동 재부팅) 즉시 실행** 확인란을 선택 해제합니다.

절전 모드 작동 또는 중지

절전 모드를 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.
   창 오른쪽에 고급 애플리케이션 설정이 표시됩니다.
3. **운영 모드** 섹션에서 **설정** 버튼을 누릅니다.
   운영 모드 창이 열립니다.
4. **운영 모드** 창에서 다음과 같은 작업을 수행합니다:
   - 절전 모드를 작동하려면 **배터리 전원으로 실행 중이면 스케줄된 작업 연기** 확인란을 선택합니다.
     절전 모드를 작동하고 컴퓨터가 배터리 전원으로 작동될 때는 다음과 같은 작업의 스케줄이 지정되어 있더라도 실행되지 않습니다:
     - 업데이트 작업
     - 컴퓨터 전체 검사 작업
     - 중요한 영역 검사 작업
     - 사용자 지정 검사 작업
     - 취약점 검사 작업
     - 무결성 검사 작업

- 절전 모드를 중지하려면 **배터리 전원으로 실행 중이면 스케줄된 작업 연기** 확인란을 선택 해제합니다. 이 경우 Kaspersky Endpoint Security는 컴퓨터의 전원 입력 형식과 상관없이 스케줄된 작업을 수행합니다.

5. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

다른 애플리케이션에 컴퓨터 리소스 우선권 할당 작동 또는 중지

다른 애플리케이션에 컴퓨터 리소스 우선권 할당을 작동 또는 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.
   창 오른쪽에 고급 애플리케이션 설정이 표시됩니다.
3. **운영 모드** 섹션에서 **설정** 버튼을 누릅니다.
   운영 모드 창이 열립니다.
4. **운영 모드** 창에서 다음과 같은 작업을 수행합니다:
   - 다른 애플리케이션에 리소스를 더 할당하는 모드를 활성화하려면, **다른 애플리케이션에 컴퓨터 리소스 우선권 할당** 확인란을 선택합니다.
     다른 애플리케이션에 리소스를 더 할당하면, Kaspersky Endpoint Security는 다른 애플리케이션의 동작을 느리게 하는 스케줄된 작업을 연기합니다:
     - 업데이트 작업
     - 컴퓨터 전체 검사 작업
     - 중요한 영역 검사 작업
     - 사용자 지정 검사 작업
     - 취약점 검사 작업
     - 무결성 검사 작업
   - 다른 애플리케이션에 리소스를 더 할당하는 모드를 비활성화하려면, **다른 애플리케이션에 컴퓨터 리소스 우선권 할당** 확인란을 선택 해제합니다. 이 경우 Kaspersky Endpoint Security는 다른 애플리케이션의 동작과 상관없이 스케줄된 작업을 수행합니다.

   기본적으로 이 애플리케이션은 컴퓨터 리소스 우선권을 다른 애플리케이션에 할당하도록 구성됩니다.
5. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

암호 보호

이 섹션에는 암호로 Kaspersky Endpoint Security에 대한 접근을 제한하는 방법에 대한 정보가 나와 있습니다.

Kaspersky Endpoint Security 접근 제한 정보

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.

사용자 이름과 암호를 설정하고 다음과 같이 애플리케이션에서 사용자에게 자격증명을 묻는 작업을 지정하여 Kaspersky Endpoint Security에 대한 접근을 제한할 수 있습니다:

이전 버전의 애플리케이션이 Kaspersky Endpoint Security 10 Service Pack 2 for Windows로 업그레이드할 때, 암호는 보존됩니다(암호가 설정되어 있었다면). 처음으로 암호 보호 설정을 편집하려면, 기본 사용자 이름인 KLAdmin을 사용하십시오.

암호 보호 사용 및 사용 안 함

암호를 통해 애플리케이션에 대한 접근을 제한하는 경우 주의해야 합니다. 암호를 잊은 경우 Kaspersky 기술 지원에 문의하여 암호 보호를 해제하십시오.

암호 보호 기능을 사용하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 설정이 표시됩니다.
3. **암호 보호** 섹션에서 **설정** 버튼을 누릅니다.
   암호 보호 창이 열립니다.
4. **암호 보호 사용** 확인란을 선택합니다.
5. **사용자 이름** 필드에 이후 암호로 보호된 작업을 수행할 때 **암호 확인** 창에 기입해야 하는 사용자 이름을 입력합니다.
6. **새로운 암호** 필드에 애플리케이션에 접근하는 데 사용할 암호를 입력합니다.
7. **암호 확인** 필드에서 암호를 확인합니다.
8. 애플리케이션의 모든 작업에 대한 접근을 제한하려면 **암호 적용 범위** 섹션에서 **모두 선택** 버튼을 누릅니다.
9. 사용자 접근을 선별적으로 제한하려면 **암호 적용 범위** 섹션에서 관련 작업 이름 옆의 확인란을 선택합니다:
   - **애플리케이션 설정 구성**.
   - **애플리케이션 종료**.
   - **보호 구성 요소 중지**.
   - **제어 구성 요소 중지**.

- **라이센스 제거**.
- **애플리케이션 제거 / 수정 / 복구**.
- **암호화된 드라이브의 데이터에 대한 접근 복원**.
- **리포트 보기**.

10. **확인** 버튼을 누릅니다.

    애플리케이션은 입력된 암호를 확인합니다. 암호가 일치하면 애플리케이션이 암호를 적용합니다. 만일 암호가 일치하지 않으면, 애플리케이션은 사용자에게 **암호 확인** 필드에 암호를 다시 한번 확인하도록 안내합니다.

암호 보호를 설정하면 암호 적용 범위에 포함된 작업을 수행할 때마다 애플리케이션이 암호를 확인합니다. 현재 세션이 진행되는 동안 암호로 보호된 동작을 수행할 때 애플리케이션에서 매번 다시 암호를 묻지 않도록 하려면 **암호 확인** 창에 있는 **현재 세션에서 이 암호 항상 사용** 확인란을 선택합니다.

현재 세션에서 이 암호 항상 사용 확인란의 선택을 취소하면 암호로 보호된 작업을 수행할 때마다 애플리케이션에서 암호를 묻습니다.

암호 보호를 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.

   창 오른쪽에 애플리케이션 설정이 표시됩니다.
3. **암호 보호** 섹션에서 **설정** 버튼을 누릅니다.

   암호 보호 창이 열립니다.
4. **암호 보호 사용** 확인란 선택을 취소합니다.

   KLAdmin으로 로그인한 경우에만 암호 보호를 비활성화할 수 있습니다. 다른 사용자 계정이나 임시 암호를 사용하는 경우에는 암호 보호를 사용하지 않도록 설정할 수 없습니다.
5. **확인** 버튼을 누릅니다.

암호 보호 사용을 중지하면 다음에 Kaspersky Endpoint Security가 시작되면 애플리케이션에 대한 접근 제한이 취소됩니다.

Kaspersky Endpoint Security 접근 암호 수정

Kaspersky Endpoint Security의 접근 암호를 변경하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.
3. **암호 보호** 섹션에서 **설정** 버튼을 누릅니다.

   암호 보호 창이 열립니다.
4. **사용자 이름** 필드에 사용자 이름을 입력합니다.

5. **새로운 암호** 필드에 애플리케이션에 접근하는 데 사용할 새로운 암호를 입력합니다.

6. **암호 확인** 필드에 새로운 암호를 다시 입력합니다.

7. **확인**을 누릅니다.

   애플리케이션은 입력된 암호를 확인합니다. 암호가 일치하면, 애플리케이션은 새로운 암호를 적용하고 **암호 보호** 창을 닫습니다. 만일 암호가 일치하지 않으면, 애플리케이션은 사용자에게 **암호 확인** 필드에 암호를 다시 한 번 확인하도록 안내합니다.

8. 변경 내용을 저장하려면 애플리케이션 설정 창에서 **저장** 버튼을 누릅니다.

임시 암호 사용 정보

Kaspersky Security Center 정책으로 관리되는 클라이언트 컴퓨터에서 작업하는 사용자는 Kaspersky Endpoint Security로 정책 수준에서 암호 보호되는 작업을 수행해야 하는 경우가 있습니다. 암호 보호를 설정하면 Kaspersky Security Center 관리자만 암호 적용 범위에 지정된 작업을 수행할 수 있습니다. 그렇지만 Kaspersky Security Center와 연결이 끊어지면(사용자가 회사 네트워크 외부에 있는 경우), Kaspersky Security Center 로컬 인터페이스에서 작업하는 기능이 제한됩니다.

사용자에게 정책 설정에 설정된 암호를 부여하지 않고 사용자가 필요한 작업을 수행할 수 있도록 하기 위해 Kaspersky Security Center 관리자는 임시 암호를 만들 수 있습니다. 임시 암호에는 유효 기간 및 작업 범위 제한이 있습니다. 사용자가 애플리케이션의 로컬 인터페이스에서 임시 암호를 입력하면 Kaspersky Security Center 관리자가 허용한 작업을 수행할 수 있습니다.

임시 암호가 만료되어도 Kaspersky Endpoint Security는 Kaspersky Security Center 정책의 설정에 따라 계속 작동합니다. 하지만 사용자는 정책 수준에서 암호 보호되는 작업을 수행할 수 없습니다.

Kaspersky Security Center 관리 콘솔을 사용하여 임시 암호 만들기

임시 암호를 만들어 사용자에게 전송하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 사용자가 임시 암호를 요청하는 컴퓨터를 포함한 관리 그룹의 이름으로 된 폴더를 엽니다.

3. 작업 공간에서 **기기** 탭을 선택합니다.

4. 임시 암호를 요청하는 사용자 소유의 컴퓨터의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   속성: <컴퓨터 이름> 창이 열립니다.

5. **속성: <컴퓨터 이름>** 창에서 **애플리케이션** 섹션을 선택합니다.

6. Kaspersky Endpoint Security Service Pack 2 for Windows를 선택하고 다음 방법 중 하나를 사용해 애플리케이션 속성 창을 엽니다:

   - 화면 아래쪽에 있는 **속성** 버튼을 누릅니다.
   - 애플리케이션의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   애플리케이션 설정 "<애플리케이션 이름>" 창이 열립니다.

7. **애플리케이션 설정 "<애플리케이션 이름>"** 창의 **고급 설정** 섹션에서 **애플리케이션 설정** 하위 섹션을 선택합니다.

8. **암호 보호** 섹션에서 **설정** 버튼을 누릅니다.

   암호 보호 창이 열립니다.

9. **암호 보호** 창 **임시 암호** 섹션에서 **설정** 버튼을 누릅니다.

   > 컴퓨터에서 실행 중인 Kaspersky Security Center 정책에 Kaspersky Security Center에 대한 암호 보호가 설정되어 있을 때 이 버튼이 표시됩니다.

   임시 암호 생성 창이 열립니다.

10. **만료 날짜** 필드에 사용자가 더 이상 임시 암호를 사용할 수 없게 되는 날짜를 지정합니다.

    이 날짜에 임시 암호의 효력이 상실됩니다. Kaspersky Endpoint Security 로컬 인터페이스에서 작업을 수행할 수 있도록 접근 권한을 부여하려면 새 임시 암호를 생성해야 합니다.

11. **임시 암호 적용 범위** 표에서 임시 암호가 유효한 기간 동안 사용자에게 허용해야 하는 작업 옆의 확인란을 선택합니다.

12. **생성** 버튼을 누릅니다.

    암호가 들어 있는 **임시 암호** 창이 열립니다.

13. 암호 및 암호 적용 안내를 복사하여 사용자에게 전송합니다.

Kaspersky Endpoint Security 인터페이스에 임시 암호 적용

> Kaspersky Endpoint Security가 설치된 클라이언트 컴퓨터 사용자를 위한 안내입니다.

임시 암호를 적용하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.

2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.

   창 오른쪽에 애플리케이션 설정이 표시됩니다.

3. **암호 보호** 섹션에서 **임시 암호** 버튼을 누릅니다.

   임시 암호 창이 열립니다.

4. **임시 암호 사용** 확인란을 선택합니다.

5. 입력 필드에 Kaspersky Security Center 관리자에게 받은 암호를 지정합니다.

6. **확인**을 눌러 변경을 저장합니다.

임시 암호가 적용된 후에 Kaspersky Security Center 관리자가 지정한 작업을 사용할 수 있습니다. **임시 암호** 창에 임시 암호의 만료일과 허용된 작업이 표시됩니다.

Kaspersky Security Center를 통한 애플리케이션 원격 관리

이 섹션에서는 Kaspersky Security Center를 통한 Kaspersky Endpoint Security 관리에 대해 설명합니다.

Kaspersky Security Center를 통한 애플리케이션 관리 정보

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

Kaspersky Security Center를 통한 애플리케이션 관리에 대해 이 문서에 없는 추가 정보를 보려면 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

Kaspersky Endpoint Security 관리 플러그인을 이용해 Kaspersky Security Center에서 이 애플리케이션을 관리할 수 있습니다.

관리 플러그인 버전이 클라이언트 컴퓨터에 설치된 Kaspersky Endpoint Security 버전과 다를 수 있습니다. 설치된 관리 플러그인 버전이 Kaspersky Endpoint Security 버전에 비해 기능이 적으면 관리 플러그인을 통해 누락된 기능에 대한 설정을 조정할 수 없습니다. 사용자는 Kaspersky Endpoint Security 로컬 인터페이스에서 이러한 설정을 수정할 수 있습니다.

다른 버전의 관리 플러그인으로 작업 시 특별 고려 사항

관리 플러그인을 사용해 다음 항목을 변경할 수 있습니다:

- 정책
- 정책 프로필
- 그룹 작업
- 로컬 작업
- Kaspersky Endpoint Security 로컬 설정

Kaspersky Endpoint Security 호환성 정보에 지정된 버전과 같거나 상위의 관리 플러그인 버전이 설치되어 있는 경우에만 관리 플러그인을 사용하여 Kaspersky Security Center를 통해 Kaspersky Endpoint Security를 관리할 수 있습니다. 배포 패키지에 포함된 installer.ini 파일에서 관리 플러그인 최소 필요 버전을 확인할 수 있습니다.

구성요소를 열면 관리 플러그인이 호환성 정보를 확인합니다. 관리 플러그인 버전이 호환성 정보에 지정된 버전과 같거나 상위 버전인 경우 이 구성요소 설정을 변경할 수 있습니다. 그렇지 않으면 관리 플러그인을 사용해 선택한 구성요소의 설정을 변경할 수 없습니다. 이 경우 관리 플러그인을 업그레이드하기를 권장합니다.

최신 버전의 관리 플러그인을 사용하여 이전에 지정한 설정 변경

최신 버전의 관리 플러그인을 사용해 이전에 지정한 모든 설정을 변경하고 이전에 사용했던 관리 플러그인 버전에는 없었던 새로운 설정을 구성할 수 있습니다.

최신 버전의 관리 플러그인의 새로운 설정에서 정책, 정책 프로필 또는 작업을 처음 저장할 때는 기본값이 지정됩니다.

최신 버전의 관리 플러그인을 사용해 정책, 정책 프로필 또는 그룹 작업의 설정을 변경하면 이전 버전의 관리 플러그인에서 해당 구성요소를 사용할 수 없습니다. 단, Kaspersky Endpoint Security의 로컬 설정 및 로컬 작업의 설정은 이전 버전의 관리 플러그인에서도 계속 사용할 수 있습니다.

클라이언트 컴퓨터에서 Kaspersky Endpoint Security 시작 및 중지

클라이언트 컴퓨터에서 Kaspersky Endpoint Security를 시작 또는 중지하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 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. 애플리케이션을 시작 또는 중지할 컴퓨터를 선택합니다.
5. 마우스 오른쪽 버튼을 눌러 클라이언트 컴퓨터의 마우스 오른쪽 메뉴를 표시하고 **속성**을 선택합니다.
   클라이언트 컴퓨터 속성 창이 열립니다.
6. 클라이언트 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.
   클라이언트 컴퓨터에 설치되어 있는 Kaspersky 애플리케이션 목록이 클라이언트 컴퓨터 속성 창의 오른쪽에 나타납니다.
7. Kaspersky Endpoint Security 10 for Windows 선택.
8. 다음을 수행합니다:
   - 애플리케이션을 시작하려면, Kaspersky 애플리케이션 목록의 오른쪽에 있는  버튼을 클릭하거나 다음을 수행하십시오:
     a. Kaspersky Endpoint Security 마우스 오른쪽 메뉴에서 **속성**을 선택하거나 Kaspersky 애플리케이션 목록 아래에 있는 **속성** 버튼을 누릅니다.
     Kaspersky Endpoint Security 10 for Windows 애플리케이션 설정 창이 열립니다.
     b. **일반** 섹션의 창 오른쪽에 있는 **실행** 버튼을 누릅니다.
   - 애플리케이션을 중지하려면, Kaspersky 애플리케이션 목록의 오른쪽에 있는  버튼을 클릭하거나 다음을 수행하십시오:
     a. Kaspersky Endpoint Security 마우스 오른쪽 메뉴에서 **속성**을 선택하거나 Kaspersky 애플리케이션 목록 아래에 있는 **속성** 버튼을 누릅니다.
     Kaspersky Endpoint Security 10 for Windows 애플리케이션 설정 창이 열립니다.
     b. **일반** 섹션의 창 오른쪽에 있는 **중지** 버튼을 누릅니다.

Kaspersky Endpoint Security 설정 구성

Kaspersky Endpoint Security 설정 구성:

1. Kaspersky Security Center의 관리 콘솔을 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. Kaspersky Endpoint Security 설정을 구성할 컴퓨터를 선택합니다.
5. 클라이언트 컴퓨터의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   클라이언트 컴퓨터 속성 창이 열립니다.
6. 클라이언트 컴퓨터 속성 창에서 **애플리케이션** 섹션을 선택합니다.
   클라이언트 컴퓨터에 설치되어 있는 Kaspersky 애플리케이션 목록이 클라이언트 컴퓨터 속성 창의 오른쪽에 나타납니다.
7. Kaspersky Endpoint Security 10 for Windows 애플리케이션을 선택합니다.
8. 다음 중 하나를 수행합니다:
   - Kaspersky Endpoint Security 10 for Windows의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - Kaspersky 애플리케이션 목록 아래의 **속성** 버튼을 누릅니다.

   Kaspersky Endpoint Security 10 for Windows 애플리케이션 설정 창이 열립니다.
9. **고급 설정** 섹션에서 Kaspersky Endpoint Security 설정뿐 아니라 리포트 및 저장소 설정을 구성합니다.
   Kaspersky Endpoint Security 10 for Windows 애플리케이션 설정 창의 다른 섹션은 Kaspersky Security Center의 표준 애플리케이션 섹션과 동일합니다. 이러한 섹션에 대한 설명은 *Kaspersky Security Center 관리자 설명서*에 나와 있습니다.

   애플리케이션에 특정 설정의 변경을 금지하는 정책이 적용되는 경우 **고급 설정** 섹션에서 해당 설정을 편집하거나 구성하지 못합니다.
10. 변경 사항을 저장하려면 **Kaspersky Endpoint Security 10 for Windows 애플리케이션 설정** 창에서 **확인**을 누릅니다.

작업 관리

이 섹션에서는 Kaspersky Endpoint Security의 작업을 관리하는 방법을 설명합니다. Kaspersky Security Center를 통해 작업을 관리하는 방법에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

Kaspersky Endpoint Security의 작업 정보

Kaspersky Security Center는 다양한 작업을 통해 클라이언트 컴퓨터의 Kaspersky 애플리케이션 활동을 제어합니다. Kaspersky Security Center의 작업은 라이센스 설치, 컴퓨터 검사, 데이터베이스 및 애플리케이션 소프트웨어 모듈 업데이트 등과 같은 기본 관리 기능을 수행합니다.

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.
- 관리 그룹에 속하지 않은 컴퓨터 조합에 대한 작업.

  관리 그룹 외부의 컴퓨터 집합에 대한 작업은 작업 설정에 지정된 클라이언트 컴퓨터에만 적용됩니다. 새로운 클라이언트 컴퓨터가 작업이 구성되어 있는 컴퓨터 집합에 추가되면 이 작업은 새로운 컴퓨터에 적용되지 않습니다. 이러한 컴퓨터에 작업을 적용하려면 새로운 작업을 만들거나 기존 작업의 설정을 편집해야 합니다.

Kaspersky Endpoint Security를 원격으로 관리하려면 아래에 목록으로 나열된 유형의 작업을 사용합니다:

- **라이센스 키 설치**. Kaspersky Endpoint Security는 추가 키를 포함해 애플리케이션 활성화를 위해 키를 추가합니다.
- **애플리케이션 구성 요소 변경**. Kaspersky Endpoint Security는 작업 설정에 지정된 구성요소 목록에 따라 클라이언트 컴퓨터에서 구성요소를 설치 또는 제거합니다.
- **인벤토리**. Kaspersky Endpoint Security는 컴퓨터에 저장된 모든 애플리케이션 실행 파일에 대한 정보를 수집합니다.

  DLL 모듈 및 스크립트 파일 인벤토리를 활성화합니다. 이 경우 Kaspersky Security Center는 Kaspersky Endpoint Security가 설치된 컴퓨터에 로드된 DLL 모듈 및 스크립트 포함 파일에 대한 정보를 수신합니다.

  DLL 모듈 및 스크립트 파일 인벤토리를 활성화하면 인벤토리 작업 기간 및 데이터베이스 크기가 상당히 증가합니다.

- **업데이트**. Kaspersky Endpoint Security는 구성된 업데이트 설정에 따라 데이터베이스 및 애플리케이션 모듈을 업데이트합니다.
- **롤백**. Kaspersky Endpoint Security는 데이터베이스 및 모듈의 마지막 업데이트를 롤백합니다.
- **바이러스 검사**. Kaspersky Endpoint Security는 바이러스 및 기타 보안위협에 대한 설정에 지정된 컴퓨터 영역을 검사합니다.
- **KSN과의 연결 상태 확인**. Kaspersky Endpoint Security는 KSN 서버 가용성에 대한 쿼리를 전송하고 KSN 연결 상태를 업데이트합니다.
- **무결성 검사**. Kaspersky Endpoint Security는 클라이언트 컴퓨터에 설치된 애플리케이션 모듈 조합에 대한 데이터를 수신하고 모듈별 디지털 서명을 검사합니다.
- **인증 에이전트 계정 관리**. 이 작업을 수행하는 동안 Kaspersky Endpoint Security는 인증 에이전트 계정 삭제, 추가 또는 수정 명령을 생성합니다.

작업을 통해 다음과 같은 처리를 수행할 수 있습니다:

- 작업을 시작, 중지, 일시 중지 및 다시 시작합니다.
- 새 작업을 만듭니다.

- 작업 설정을 편집합니다.

Kaspersky Endpoint Security 작업(읽기, 쓰기, 실행) 설정에 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.

작업 관리 모드 구성

Kaspersky Endpoint Security 로컬 인터페이스에서 작업 사용 모드를 구성하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 Kaspersky Endpoint Security 로컬 인터페이스에서 작업 사용 모드를 구성할 관리 그룹의 이름으로 된 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **고급 설정** 섹션에서 **애플리케이션 설정** 하위 섹션을 선택합니다.
7. **운영 모드** 섹션에서 다음을 수행합니다:
   - 사용자가 Kaspersky Endpoint Security 인터페이스 및 명령줄에서 로컬 작업을 수행하도록 허용하려면 **클라이언트 자체 작업 사용 허용** 확인란을 선택합니다.

     확인란을 선택 취소하면 로컬 작업 기능이 중지됩니다. 이 모드에서는 일정에 따라 로컬 작업이 실행되지 않습니다. Kaspersky Endpoint Security 로컬 인터페이스 및 명령줄을 통해 로컬 작업을 시작하거나 편집할 수 없습니다.

   - 사용자가 그룹 작업 목록을 보도록 허용하려면 **중앙 관리자가 만든 그룹 작업 표시** 확인란을 선택합니다.
   - 사용자가 그룹 작업 설정을 수정하도록 허용하려면 **중앙 관리자가 만든 그룹 작업에 대해 클라이언트 제어 허용** 확인란을 선택합니다.
8. **확인**을 눌러 변경사항을 저장합니다.
9. 정책이 적용됩니다.

   Kaspersky Security Center 정책 적용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

로컬 작업 만들기

로컬 작업을 만들려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 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. 로컬 작업을 만들 컴퓨터를 선택합니다.
5. 다음 중 하나를 수행합니다:
   - 클라이언트 컴퓨터의 마우스 오른쪽 메뉴에서 **모든 작업** 작업 만들기 옵션을 선택합니다.
   - 클라이언트 컴퓨터의 마우스 오른쪽 메뉴에서 **속성**을 선택하고 **속성: <컴퓨터 이름>** 창이 열리면 **작업** 탭에서 **추가** 버튼을 누릅니다.
   - **처리 방법 선택** 드롭다운 목록에서 **작업 만들기**를 선택합니다.

   작업 마법사가 시작됩니다.
6. 작업 마법사의 안내를 따릅니다.

그룹 작업 만들기

그룹 작업을 만들려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 다음 중 하나를 수행합니다:
   - 관리 콘솔 트리에서 **관리 중인 기기** 폴더를 선택하여 Kaspersky Security Center에서 관리하는 모든 컴퓨터에 대한 그룹 작업을 작성합니다.
   - 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 선택합니다.
3. 작업 공간에서 **작업** 탭을 선택합니다.
4. **작업 만들기** 버튼을 누릅니다.
   작업 마법사가 시작됩니다.
5. 작업 마법사의 안내를 따릅니다.

장치 조회 작업 만들기

장치 조회 작업을 만들려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.

2. 관리 콘솔 트리의 **작업** 폴더를 선택합니다.

3. **작업 만들기** 버튼을 누릅니다.
   작업 마법사가 시작됩니다.

4. 작업 마법사의 안내를 따릅니다.

5. 마법사의 **작업을 할당할 장치 선택** 창에서 **장치 조회에 작업 할당** 버튼을 누릅니다.

6. 마법사의 다음 창에서 **선택** 버튼을 누릅니다.
   장치 조회 창이 열립니다.

7. 필요한 장치를 선택합니다.

8. **장치 조회** 창에서 **확인**을 누릅니다.

9. 작업 마법사의 안내를 따릅니다.

작업 시작, 중지, 일시 중지 및 다시 시작

Kaspersky Endpoint Security가 클라이언트 컴퓨터에서 실행 중인 경우 Kaspersky Security Center를 통해 클라이언트 컴퓨터에 작업을 시작, 중지, 다시 시작을 할 수 있습니다. Kaspersky Endpoint Security가 일시 중지되는 경우, 실행 중인 작업이 일시 중지하고 Kaspersky Security Center를 통한 작업의 시작, 중지, 일시 중지 또는 다시 시작을 할 수 없게 됩니다.

로컬 작업을 시작, 중지, 일시 중지 또는 다시 시작하려면:

1. Kaspersky Security Center의 관리 콘솔을 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. 로컬 작업을 시작, 중지, 일시 중지 또는 다시 시작 할 컴퓨터를 선택합니다.

5. 마우스 오른쪽 버튼을 눌러 클라이언트 컴퓨터의 마우스 오른쪽 메뉴를 표시하고 **속성**을 선택합니다.
   클라이언트 컴퓨터 속성 창이 열립니다.

6. **작업** 섹션을 선택합니다.
   로컬 작업 목록은 창 오른쪽에 표시됩니다.

7. 시작, 중지, 일시 중지 또는 다시 시작 할 로컬 작업을 선택합니다.

8. 다음 방법 중 하나를 사용해 작업에 필요한 조치를 수행합니다:

   - 로컬 작업에서 마우스 오른쪽 버튼을 눌러 메뉴를 열고 **실행/중지/일시 중지/다시 시작**을 선택합니다.
   - 로컬 작업을 시작 또는 중지하려면 로컬 작업 목록의 오른쪽에 있는 / 버튼을 클릭합니다.
   - 다음을 수행합니다:

a. 로컬 작업 목록에서 **속성** 버튼을 누르거나 작업 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

속성: <작업 이름> 창이 열립니다.

b. **일반** 탭에서 **실행/중지/일시 중지/다시 시작** 버튼을 누릅니다.

그룹 작업을 시작, 중지, 일시 중지 또는 다시 시작하려면:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 그룹 작업을 시작, 중지, 일시 중지 또는 다시 시작할 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **작업** 탭을 선택합니다.

   창 오른쪽에 그룹 작업이 표시됩니다.
4. 시작, 중지, 일시 중지 또는 다시 시작할 그룹 작업을 선택합니다.
5. 다음 방법 중 하나를 사용해 작업에 필요한 조치를 수행합니다:

   - 그룹 작업 마우스 오른쪽 메뉴에서 **실행/중지/일시 중지/다시 시작**을 선택합니다.
   - 그룹 작업을 시작 또는 중지하려면 창 오른쪽에 있는 / 버튼을 누릅니다.
   - 다음을 수행합니다:

     a. 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **작업 설정** 링크를 누르거나 작업 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

     속성: <작업 이름> 창이 열립니다.

     b. **일반** 탭에서 **실행/중지/일시 중지/다시 시작** 버튼을 누릅니다.

컴퓨터 조회의 작업을 시작, 중지, 일시 중지 또는 다시 시작하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **작업** 폴더에서 시작, 중지, 일시 중지 또는 다시 시작할 컴퓨터 조회 작업을 선택합니다.
3. 다음 중 하나를 수행합니다:

   - 작업 마우스 오른쪽 메뉴에서 **실행/중지/일시 중지/다시 시작**을 선택합니다.
   - 특정 컴퓨터의 작업을 시작 또는 중지하려면 창 오른쪽에 있는 / 버튼을 누릅니다.
   - 다음을 수행합니다:

     a. 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **작업 설정** 링크를 누르거나 작업 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

     속성: <작업 이름> 창이 열립니다.

     b. **일반** 탭에서 **실행/중지/일시 중지/다시 시작** 버튼을 누릅니다.

작업 설정 편집

로컬 작업의 설정을 편집하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 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. 애플리케이션 설정을 구성할 컴퓨터를 선택합니다.
5. 마우스 오른쪽 버튼을 눌러 클라이언트 컴퓨터의 마우스 오른쪽 메뉴를 표시하고 **속성**을 선택합니다.
   클라이언트 컴퓨터 속성 창이 열립니다.
6. **작업** 섹션을 선택합니다.
   로컬 작업 목록은 창 오른쪽에 표시됩니다.
7. 로컬 작업 목록에서 필요한 로컬 작업을 선택합니다.
8. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
9. **속성:<로컬 작업 이름>** 창에서 **설정** 섹션을 선택합니다.
10. 로컬 작업 설정을 편집합니다.
11. 변경 사항을 저장하려면 **속성: <로컬 작업 이름>** 창에서, **확인**을 누릅니다.
12. 변경 사항을 저장하려면 **속성: <컴퓨터 이름>** 창에서 **확인**을 누릅니다.

그룹 작업의 설정을 편집하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. **관리 중인 기기** 폴더에서 관련된 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **작업** 탭을 선택합니다.
   관리 콘솔 작업 공간에 그룹 작업이 표시됩니다.
4. 원하는 그룹 작업을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
6. **속성: <그룹 작업 이름>** 창에서 **설정** 섹션을 선택합니다.
7. 그룹 작업 설정을 편집합니다.
8. 변경 사항을 저장하려면 **속성: <그룹 작업 이름>** 창에서, **확인**을 누릅니다.

컴퓨터 조회의 작업 설정을 편집하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **작업** 폴더에서 편집할 컴퓨터 조회 작업을 선택합니다.
3. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:
   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.
4. **속성: <컴퓨터 조회의 작업 이름>** 창에서 **설정** 섹션을 선택합니다.
5. 컴퓨터 조회의 작업 설정을 편집합니다.
6. 변경 사항을 저장하려면 **속성: <컴퓨터 조회의 작업 이름>** 창에서 **확인**을 누릅니다.

설정 섹션을 예외하면 작업 속성 창의 모든 섹션은 Kaspersky Security Center에 사용된 탭과 동일합니다. 더 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오. **설정** 섹션에는 Kaspersky Endpoint Security 10 for Windows 특유의 설정이 포함되어 있습니다. 섹션 내용은 선택한 작업 또는 작업 유형에 따라 다릅니다.

정책 관리

이 섹션에서는 Kaspersky Endpoint Security에 대한 정책을 만들고 구성하는 방법에 대해 설명합니다. Kaspersky Security Center 정책을 사용한 Kaspersky Endpoint Security 관리에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

정책 정보

정책을 사용하여 관리 그룹 내의 모든 클라이언트 컴퓨터에 동일한 Kaspersky Endpoint Security 설정을 적용할 수 있습니다.

Kaspersky Endpoint Security를 사용하며 관리 그룹에 소속된 개별 컴퓨터는 정책에 의해 지정된 설정 값을 로컬에서 변경할 수 있습니다. 정책에서 설정 변경을 금지하지 않은 것만 로컬에서 그 설정을 변경할 수 있습니다.

클라이언트 컴퓨터의 애플리케이션 설정을 편집할 수 있는지 여부는 정책 내의 설정에 대한 "잠금"상태로 결정됩니다:

- 설정이 "잠겨 있으면"(), 로컬에서 이 설정의 값을 편집할 수 없습니다. 정책에 의해 지정된 설정 값은 관리 그룹에 소속된 모든 클라이언트 컴퓨터에 적용됩니다.
- 설정이 “잠금 해제”()이면, 로컬에서 설정을 편집할 수 있습니다. 로컬로 구성된 설정이 관리 그룹 내의 모든 클라이언트 컴퓨터에 적용됩니다. 정책으로 구성된 설정은 적용되지 않습니다.

처음으로 정책을 적용한 후에는 로컬 애플리케이션 설정이 정책 설정에 따라 변경됩니다.

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 접근할 수 있는 권한을 구성하려면, Kaspersky Security Center 중앙 관리 서버의 속성 창의 **보안** 섹션으로 이동합니다.

Kaspersky Endpoint Security의 기능 범위:

- 안티 바이러스 보호. 기능 범위는 파일 안티 바이러스, 메일 안티 바이러스, 웹 안티 바이러스, 메신저 안티 바이러스, 취약점 검사 및 검사 작업을 포함합니다.
- 애플리케이션 시작 제어. 이 기능 범위는 애플리케이션 시작 제어 구성요소를 포함합니다.
- 매체 제어. 이 기능 범위는 매체 제어 구성 요소를 포함합니다.
- 암호화. 이 기능 범위는 하드 드라이브, 파일 및 폴더 암호화 구성요소를 포함합니다.
- 신뢰 구역. 이 기능 범위는 신뢰 구역을 포함합니다.
- 웹 제어. 이 기능 범위는 웹 제어 구성 요소를 포함합니다.
- 침입 탐지. 이 기능 범위는 애플리케이션 모니터, 취약점 모니터, 방화벽, 네트워크 공격 차단 및 애플리케이션 권한 제어를 포함합니다.
- 기본 기능. 이 기능 범위는 다른 기능 범위에서 지정되지 않는 일반 애플리케이션 설정을 포함합니다: 라이센스, KSN 설정, 인벤토리 작업, 애플리케이션 데이터베이스 및 모듈 업데이트 작업, 자기 보호, 고급 애플리케이션 설정, 리포트 및 저장소, 암호 보호 설정 및 애플리케이션 인터페이스 설정.

정책에 대해 다음과 같은 작업을 수행할 수 있습니다:

- 정책을 만듭니다.
- 정책 설정을 편집합니다.

  중앙 관리 서버에 접근할 때 사용하는 사용자 계정이 특정 기능 범위의 설정을 편집할 수 있는 권한이 없다면, 이러한 기능 범위의 설정은 편집할 수 없습니다.

- 정책을 삭제합니다.
- 정책 상태 변경.

Kaspersky Endpoint Security와의 상호 작용과 관련이 없는 정책 사용에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

정책 만들기

정책을 만들려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 다음 중 하나를 수행합니다:
   - 관리 콘솔 트리에서 **관리 중인 기기** 폴더를 선택하여 Kaspersky Security Center에서 관리하는 모든 컴퓨터에 대한 정책을 작성합니다.
   - 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 관련 클라이언트 컴퓨터가 속한 관리 그룹의 이름을 가진 폴더를 선택합니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.

4. 다음 중 하나를 수행합니다:

   - **정책 만들기** 버튼을 누릅니다.
   - 마우스 오른쪽 메뉴를 열고 **생성** > 정책을 선택합니다.

   정책 마법사가 시작됩니다.

5. 정책마법사의 안내를 따릅니다.

정책 설정 편집

정책 설정을 편집하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 중인 기기** 폴더에서 정책 설정을 편집할 관련 관리 그룹의 이름을 가진 폴더를 엽니다.
3. 작업 공간에서 **정책** 탭을 선택합니다.
4. 필요한 정책을 선택합니다.
5. 다음 방법 중 하나로 **속성: <정책 이름>** 창을 엽니다:

   - 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 중앙 관리 콘솔 작업 공간 오른쪽에 있는 **정책 구성** 링크를 누릅니다.

   Kaspersky Endpoint Security 10 for Windows 정책 설정에는 애플리케이션 설정 및 구성요소 설정이 있습니다. **안티 바이러스 보호** 및 **엔드포인트 제어** 섹션은 **속성: <정책 이름>** 창의 한 부분으로 보호 및 제어 구성요소의 설정이 표시되고, **데이터 암호화** 섹션에는 파일 및 폴더의 암호화 설정이 표시되며, **고급 설정** 섹션에는 애플리케이션 설정이 표시됩니다.

   정책 설정의 데이터 암호화 설정 및 제어 구성요소 설정의 표시를 활성화하려면 Kaspersky Security Center의 **인터페이스 설정** 창에서 관련 확인란을 선택합니다.

6. 정책 설정을 편집합니다.
7. 변경 사항을 저장하려면, **속성: <정책 이름>** 창에서 **확인**을 누릅니다.

Kaspersky Security Center 정책에 표시할 설정 선택

Kaspersky Security Center 정책에 표시할 설정을 선택하려면 다음을 수행합니다:

1. Kaspersky Security Center의 관리 콘솔을 엽니다.
2. 관리 콘솔 트리의 **관리 서버 - <컴퓨터 이름>** 노드에 대한 마우스 오른쪽 메뉴에서 보기 → **인터페이스 설정**을 선택합니다.

   인터페이스 설정 창이 열립니다.

3. **인터페이스 설정** 창에서 Kaspersky Security Center 정책 생성 설정 및 정책 속성에 표시되어야 하는 설정 옆의 확인란을 선택합니다:

   - **엔드포인트 제어 구성요소 표시** 확인란을 선택하여 Kaspersky Security Center의 정책 마법사 창 및 정책 속성에 제어 구성요소 설정을 표시합니다.

   - **암호화 및 데이터 보호 표시** 확인란을 선택하여 Kaspersky Security Center의 새 정책 마법사 및 정책 속성에 데이터 암호화 설정을 표시합니다.

4. **확인**을 누릅니다.

Kaspersky Security Center 서버로 사용자 메시지 전송

사용자는 다음 경우에 회사 로컬 네트워크 관리자에게 메시지를 전송해야 합니다:

- 매체 제어가 장치로의 접근을 차단했습니다.

  Kaspersky Endpoint Security 인터페이스의 매체 제어 섹션에서 차단 장치로의 접근을 요청하기 위한 메시지 템플릿을 찾을 수 있습니다.

- 애플리케이션 시작 제어가 애플리케이션이 시작되지 않도록 차단했습니다.

  Kaspersky Endpoint Security 인터페이스의 애플리케이션 시작 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 Security Center가 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 Security Center가 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. 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 메시지 확인

애플리케이션 시작 제어, 매체 제어, 웹 제어 구성요소는 Kaspersky Endpoint Security가 설치된 컴퓨터 사용자가 개선 요청 사항을 관리자에게 보내는 기능을 가지고 있습니다.

사용자는 두 가지 방법으로 관리자에게 메시지를 보낼 수 있습니다:

- Kaspersky Security Center 이벤트 저장소의 이벤트로 전송됩니다.

  사용자 컴퓨터에 설치된 Kaspersky Endpoint Security가 활성 정책에 따라 작동될 경우 사용자 메시지가 Kaspersky Security Center 이벤트 저장소로 전송됩니다.

- 이메일 메시지로 전송됩니다.

  사용자의 컴퓨터에 설치된 Kaspersky Endpoint Security 애플리케이션이 정책을 실행하지 않거나 이동 사용자 정책을 실행 중인 경우 사용자 정보가 이메일로 전송됩니다.

Kaspersky Security Center 이벤트 저장소에서 사용자 메시지를 보려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 관리 콘솔을 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 조회** 드롭다운 목록에서 **사용자 개성 요청 사항**을 선택합니다.
4. 관리자에게 보낼 메시지를 선택합니다.
5. 다음 방법 중 하나로 **이벤트 속성**을 엽니다:

   - 이벤트를 마우스 오른쪽 클릭합니다. 열린 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 관리 콘솔 작업 공간 오른쪽에 있는 **이벤트 속성 창 열기** 버튼을 누릅니다.

Kaspersky Security Network 참여

이 섹션에는 Kaspersky Security Network에 참여하는 방법과 지침 및 Kaspersky Security Network 참여를 활성화하거나 비활성화 하는 방법에 대한 정보가 포함되어 있습니다.

Kaspersky Security Network 참여 정보

Kaspersky Endpoint Security는 사용자 컴퓨터를 보다 효과적으로 보호하기 위해 전세계 사용자로부터 수집한 데이터를 사용합니다. *Kaspersky Security Network*는 이러한 데이터를 수집하도록 설계되었습니다.

Kaspersky Security Network(KSN)는 파일, 웹 리소스 및 소프트웨어에 대한 정보가 포함된 Kaspersky의 온라인 기술 자료에 접속할 수 있는 클라우드 서비스 인프라입니다. Kaspersky Security Network의 데이터를 사용하면 Kaspersky Endpoint Security에서 새로운 보안위협에 대해 신속하게 대응할 수 있으며, 일부 보호 구성요소의 성능이 향상되고 정상적인 개체를 바이러스로 탐지하는 가능성을 줄입니다.

인프라의 위치에 따라 글로벌 KSN 서비스(Kaspersky 서버에서 호스팅하는 인프라)와 사설 KSN 서비스(인터넷 서비스 공급업체의 네트워크와 같이 타사 서버에서 호스팅하는 인프라)가 있습니다.

라이센스를 변경한 후 사설 KSN을 사용하려면 서비스 공급 업체에게 새 키에 대한 세부 내용을 전달해야 합니다. 그렇지 않으면, KSN과의 데이터 교환이 불가능하게 됩니다.

KSN에 대한 사용자의 참여를 통해 Kaspersky에서는 위협 형태와 소스에 대한 정보를 실시간으로 수신하여 해당 보안위협을 처리하는 방법을 개발하고 애플리케이션 구성요소의 오탐 알림 수를 최소화입니다.

KSN에 참가하는 동안에는 애플리케이션 동작 중에 생성된 통계를 자동으로 KSN에 전송합니다. 애플리케이션은 해커가 컴퓨터 또는 데이터를 손상시키기 위해 사용할 수 있는 특정 파일(또는 파일 일부)을 추가 검사를 위해 Kaspersky로 전송할 수도 있습니다.

개인 사용자 데이터는 수집, 처리 또는 저장되지 않습니다. KSN에 참여하는 동안 생성된 Kaspersky 통계 정보의 전송 및 그러한 정보의 보관 및 파기에 대한 자세한 내용은 Kaspersky Security Network 참여 라이센스 계약서를 검토하거나 Kaspersky 웹 사이트에서 확인하십시오. Kaspersky Security Network 라이센스 계약서인 ksn_ <언어 ID>.txt 파일은 애플리케이션 배포 키트에 포함되어 있습니다.

KSN 서버의 부하를 줄이기 위해, Kaspersky는 Kaspersky Security Network로의 요청을 일시적으로 중지하거나 일부 제한하는 애플리케이션 안티 바이러스 데이터베이스를 배포할 수 있습니다. 이 경우, KSN으로의 연결 상태는 *필터링 모드로 활성화*으로 표시됩니다.

Kaspersky Security Center 중앙 관리 서버가 관리하는 사용자 컴퓨터는 KSN 프록시 서비스를 통해 KSN과 통신할 수 있습니다.

KSN 프록시는 다음과 같은 기능을 제공합니다:

- 직접 인터넷을 통하지 않고 사용자의 컴퓨터에서 KSN으로 쿼리를 전송하고 정보를 제출합니다.
- KSN 프록시는 처리된 데이터를 캐시하므로 외부 네트워크 연결의 부하를 줄이고 사용자의 컴퓨터에서 신속하게 요청한 정보를 받아볼 수 있습니다.

KSN 프록시 서비스에 대한 자세한 내용은 *Kaspersky Security Center 관리자 설명서*를 참조하십시오.

KSN 프록시 설정은 *Kaspersky Security Center* 정책의 속성에서 구성할 수 있습니다.

Kaspersky Security Network에 대한 참여는 자발적으로 이루어집니다. 애플리케이션 초기 구성 절차 동안 KSN에 참여하도록 애플리케이션에서 사용자를 초대합니다. 사용자는 아무 때나 KSN 참가를 시작 또는 중단할 수 있습니다.

Kaspersky Security Network 사용 및 중지

Kaspersky Security Network를 사용 및 중지하려면 다음과 같이 하십시오:

1. 애플리케이션 설정 창을 엽니다.
2. 창 왼쪽의 **고급 설정** 섹션에서 **KSN 설정** 하위 섹션을 선택합니다.
   창 오른쪽에 Kaspersky Security Network 설정이 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - Kaspersky Security Network 사용을 작동하려면 제품에서 **KSN 정책 및 참가 조건에 동의** 확인란을 선택합니다.
   - Kaspersky Security Network 사용을 중지하려면 제품에서 **KSN 정책 및 참가 조건에 동의** 확인란을 선택 해제합니다.
4. 변경 내용을 저장하려면 **저장** 버튼을 누릅니다.

Kaspersky Security Network 연결 확인

Kaspersky Security Network 연결을 테스트하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 창 상단에 있는 **Kaspersky Security Network** 버튼을 누릅니다.
   Kaspersky Security Network 창이 열립니다.
   Kaspersky Security Network 창의 왼쪽에 원형 **KSN** 버튼 형태에 다음과 같이 Kaspersky Security Network에 대한 연결 모드가 표시됩니다:
   - Kaspersky Endpoint Security가 Kaspersky Security Network에 연결되지 않은 경우, **KSN** 버튼은 회색으로 표시됩니다. **KSN** 버튼 아래 *중지*라는 상태가 표시됩니다.
   - Kaspersky Endpoint Security가 Kaspersky Security Network에 연결되지 않은 경우, **KSN** 버튼은 녹색으로 표시됩니다. 다음 정보가 **KSN** 버튼 아래에 나타납니다: *사용* 상태, 사용 중인 KSN 유형 - **사설 KSN** 또는 **글로벌 KSN** 및 KSN 서버와의 마지막 동기화 날짜 및 시간. 창 오른쪽에는 파일, 웹 리소스 및 소프트웨어 평판에 대한 통계가 표시됩니다.

Kaspersky Endpoint Security는 **Kaspersky Security Network** 창을 열 때 KSN의 사용에 대한 통계 데이터를 수집합니다. 이 통계는 실시간으로 업데이트되지 않습니다.

- Kaspersky Endpoint Security가 Kaspersky Security Network에 연결되어 있지만 KSN 서버를 사용할 수 없는 경우 **KSN** 버튼은 빨간색입니다. **KSN** 버튼 아래 *사용*이라는 상태가 표시됩니다.

  > KSN 서버와의 마지막 동기화 시간이 15분을 초과하거나 *알 수 없음* 상태이면, 이는 KSN 서비스를 이용할 수 없음을 의미합니다. 그런 경우 기술 지원이나 서비스 제공 업체에 문의하는 것이 좋습니다.

  다음과 같은 이유로 Kaspersky Security Network에 연결되어 있지 않을 수 있습니다:

  - 컴퓨터가 인터넷에 연결되어 있지 않습니다.
  - 애플리케이션이 활성화되지 않았거나 라이센스가 만료되었습니다.
  - 키와 관련된 문제가 있습니다 (예, 블랙리스트에 등록된 키입니다).

Kaspersky Security Network 내 파일의 평판 확인

KSN 서비스를 통해 Kaspersky 평판 데이터베이스에 있는 애플리케이션에 대한 정보를 검색할 수 있습니다. 이러면 회사 차원에서 애플리케이션 시작 정책을 유연하게 관리할 수 있으므로 범죄자가 내 컴퓨터를 손상시키거나 개인 정보를 도용할 목적으로 악용할 수 있는 애드웨어 및 기타 프로그램이 시작되지 않도록 차단합니다.

Kaspersky Security Network 내 파일의 평판을 확인하려면 다음을 수행합니다:

1. 평판을 확인할 파일을 마우스 오른쪽 버튼으로 클릭하여 메뉴를 표시합니다.
2. **KSN에서 평판 확인** 옵션을 선택합니다.

   > 이 옵션은 Kaspersky Security Network 정책의 조건을 수락한 경우에 표시됩니다.

   <파일 이름> - KSN 평판 창이 열립니다. **<파일 이름> - KSN 평판** 창에 확인하는 파일에 대한 다음 정보가 표시됩니다:

   - **경로**. 파일이 디스크에 저장된 경로입니다.
   - **버전**. 애플리케이션 버전(실행 파일인 경우에만 이 정보가 표시됨).
   - **디지털 서명**. 디지털 서명 및 해당 파일의 존재 여부입니다.
   - **서명한 날짜**. 인증서에 디지털 서명으로 서명한 날짜입니다.
   - **만든 날짜**. 파일이 만들어진 날짜입니다.
   - **수정한 날짜**. 파일을 마지막으로 수정한 날짜입니다.
   - **크기**. 파일이 저장되어 있는 디스크 용량을 말합니다.
   - 파일을 신뢰하거나 차단하는 사용자 수에 대한 정보입니다.

Kaspersky Security Network로 더욱 향상된 보호 제공

Kaspersky는 Kaspersky Security Network를 통해 사용자에게 더욱 향상된 보호 기능을 제공합니다. 이 보호 방법은 지능형 지속 공격과 제로 데이 공격으로부터 보호할 수 있도록 설계되었습니다. 통합 클라우드 기술과 Kaspersky 바이러스 분석가의 전문성을 통해 Kaspersky Endpoint Security는 가장 정교한 네트워크 위협에 대비할 수 있는 탁월한 수준의 보호를 제공합니다.

Kaspersky Endpoint Security의 향상된 보호 기능에 대한 자세한 내용은 Kaspersky 웹사이트에서 확인할 수 있습니다.

애플리케이션에 대한 정보 출처

Kaspersky 웹사이트의 Kaspersky Endpoint Security 페이지

Kaspersky Endpoint Security 페이지에서 애플리케이션과 기능, 특징과 같은 일반적인 정보를 확인할 수 있습니다.

Kaspersky Endpoint Security 페이지에는 온라인 쇼핑몰로의 링크를 포함하고 있습니다. 그곳에서 애플리케이션을 구매하거나 갱신할 수 있습니다.

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 경우가 아니라면 Kaspersky 전문가 또는 포럼 사용자와 해당 질문에 대해 토론할 수 있습니다.

이 포럼에서 이미 게시된 주제를 보고, 의견을 남기고, 새 논의 주제를 작성할 수 있습니다.

기술 지원 서비스에 문의

이 섹션은 기술 지원을 받는 방법과 그 조건에 대해 기술하고 있습니다.

기술 지원을 받는 방법

애플리케이션 문서 또는 애플리케이션에 대한 정보를 제공하는 출처에서 문제에 대한 해결 방법을 찾을 수 없을 경우 기술 지원에 문의하는 것이 좋습니다. 기술 지원 서비스 전문가가 애플리케이션 설치 및 사용과 관련된 질문에 대답해 드립니다.

기술 지원은 상업용 라이센스를 구매한 사용자에게만 제공됩니다. 체험판 라이센스를 받은 사용자는 기술 지원을 받을 수 없습니다.

> 기술 지원 서비스에 문의하기 전에 지원 규칙을 읽어보시기 바랍니다.

다음 방법 중 하나로 기술 지원에 문의할 수 있습니다:

- 전화 기술 지원에 문의
- Kaspersky CompanyAccount 포털을 통해 Kaspersky 기술 지원 요청

전화 기술 지원

전 세계 대부분의 지역에서 담당 기술 지원에 연락할 수 있습니다. 사용자의 국가에서 기술 지원을 받는 방법과 Kaspersky 기술 지원 웹사이트에 있는 기술 지원 연락처 등의 정보를 찾아 볼 수 있습니다.

> 기술 지원 서비스에 문의하기 전에 지원 규칙을 읽어보시기 바랍니다.

Kaspersky CompanyAccount를 통해 기술 지원 받기

Kaspersky CompanyAccount는 Kaspersky 애플리케이션을 사용하는 회사를 위한 포털입니다. Kaspersky CompanyAccount 포털은 온라인 요청을 통해 사용자와 Kaspersky 전문가 간의 상호작용을 원활하게 합니다. Kaspersky CompanyAccount 포털에서 전자 요청의 상태를 추적하고 요청 기록을 저장할 수 있습니다.

Kaspersky CompanyAccount에서 단일 계정에 조직의 모든 직원을 등록할 수 있습니다. 등록된 직원이 단일 계정을 통해 Kaspersky에 보낸 전자 요청을 중앙에서 관리할 수 있고 Kaspersky CompanyAccount를 통해 해당 직원의 권한도 관리할 수 있습니다.

Kaspersky CompanyAccount 포털은 다음 언어로 사용할 수 있습니다:

- 영어
- 스페인어
- 이탈리아어

- 독일어
- 폴란드어
- 포르투갈어
- 러시아어
- 프랑스어
- 일본어

Kaspersky CompanyAccount에 대한 자세한 정보는 기술 지원 웹사이트를 방문하십시오.

기술 지원에 필요한 정보 수집

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 애플리케이션의 단계를 파악할 수 있습니다.

기술 지원 전문가는 또한 운영체제와 컴퓨터에서 실행 중인 프로세스에 대한 추가 정보 및 애플리케이션 구성요소의 동작에 대한 자세한 리포트, 애플리케이션 장애 덤프를 요청할 수도 있습니다.

Kaspersky Endpoint Security를 통해 필요한 정보를 수집할 수 있습니다. 수집한 정보를 하드 드라이브에 저장했다가 나중에 사용자가 원하는 시간에 업로드할 수 있습니다.

진단 툴을 실행할 때 기술 지원 전문가는 다음과 같이 애플리케이션 설정 변경을 요구할 수 있습니다:

- 확장된 진단 정보를 수집 기능 활성화.
- 표준 사용자 인터페이스 요소를 통해 사용할 수 없는 개별 애플리케이션 구성요소의 설정 세부 튜닝.
- 수집되는 진단 정보의 저장 및 전송 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 수집된 데이터의 범위에 대해 알립니다. 수집된 확장 진단 정보는 사용자의 컴퓨터에 저장됩니다. 수집된 데이터는 자동으로 Kaspersky에 전송되지 않습니다.

Kaspersky로 덤프 파일을 보내기 위해 필요한 덤프 서버의 주소를 결정하는 설정은 사용자의 컴퓨터에 저장됩니다. 필요하다면, 이런 설정 값은 운영 체제 레지스트리 키 `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`에서 편집할 수 있습니다.

위에서 나열된 작업은 기술 지원 전문가의 지시와 감독하에 수행되어야 합니다. 관리자 설명서 또는 기술 지원 전문가의 지침에서 기술한 것 이외의 방법으로 수행한 애플리케이션 설정의 임의 변경은 운영 체제의 충돌이나 부하를 유발하고 컴퓨터의 보안에 영향을 주거나 처리되는 데이터의 가용성과 무결성에 손상을 줄 수 있습니다.

추적 파일 생성

추적 파일을 생성하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 메인 애플리케이션 창에서 버튼을 누릅니다.
   지원 창이 열립니다.
3. **지원** 창에서 **시스템 추적 로그** 버튼을 누릅니다.
   기술 지원 정보 창을 엽니다.
4. 추적 과정을 시작하려면 **추적 로그 사용** 확인란을 선택합니다.
5. **레벨** 드롭다운 목록에서 추적 레벨을 선택합니다.
   기술 지원 전문가가 알려준 추적 레벨을 선택합니다. 기술 지원 전문가가 필요한 추적 레벨을 알려주지 않은 경우에는 **일반 (500)**을 선택합니다.
6. 문제가 발생하면 상황을 재현합니다.
7. 추적 프로세스를 중지하려면 **기술 지원 정보** 창으로 돌아가서 **추적 로그 사용** 확인란을 선택 취소합니다.

추적 파일을 생성한 후 Kaspersky 서버로 추적 결과를 업로드할 수 있습니다.

추적 파일의 내용 및 저장

사용자는 특히 컴퓨터에 저장된 수집된 데이터에 대한 모니터링 및 접근 제한과 같이 수집된 데이터의 안전을 Kaspersky에 제출될 때까지 보장해야 할 개인적인 책임이 있습니다.

추적 파일은 애플리케이션이 사용 중일 때는 컴퓨터에 읽을 수 없는 형태로 저장되며 애플리케이션이 제거되면 영구적으로 삭제됩니다.

추적 파일은 ProgramData\Kaspersky Lab 폴더에 저장됩니다.

추적로그 파일은 다음 이름 형태로 저장됩니다: `KES<버전 번호_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.enc1`.

인증 에이전트 추적 파일은 시스템 볼륨 정보 폴더에 저장되며 이름은 다음과 같습니다: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

추적 파일에 저장된 데이터를 볼 수 있습니다. 데이터를 보는 방법이 궁금하다면, Kaspersky 기술 지원에 연락하십시오.

모든 추적 로그 파일에는 다음 일반 데이터가 포함됩니다:

- 이벤트 시간.
- 실행 스레드 수.

인증 에이전트 추적 파일에는 이 정보가 들어있지 않습니다.

- 이벤트를 발생시킨 애플리케이션 구성요소.
- 이벤트의 심각도(정보 이벤트, 경고, 심각 이벤트, 오류).
- 애플리케이션의 구성요소에 의한 명령 실행 및 이 명령 실행의 결과에 연관된 이벤트 설명.

SRV.log, GUI.log, ALL.log 추적 파일 내용

SRV.log, GUI.log, ALL.log 추적 파일은 일반적인 데이터 이외에 다음 정보를 저장할 수도 있습니다:

- 성, 이름 등 개인 데이터(이러한 데이터가 로컬 컴퓨터에서 파일 경로에 포함된 경우).
- 사용자 이름과 암호(공개적으로 전송된 경우). 이 데이터는 인터넷 트래픽 스캔 중에 추적 파일에 기록될 수 있습니다. 트래픽은 trafmon2.ppl로부터만 추적 파일에 기록됩니다.
- 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 웹 사이트와 이들 웹 사이트의 리디렉션. 이 데이터는 애플리케이션이 웹 사이트를 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 구성요소를 사용할 경우 추적 파일에 작성됩니다.

HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log 추적 파일의 내용

일반 데이터 이외에도 HST.log 추적 파일에는 데이터베이스의 실행 및 애플리케이션 모듈 업데이트 작업에 대한 정보가 포함됩니다.

일반 데이터 이외에도 BL.log 추적 파일에는 애플리케이션의 작동 중에 발생한 이벤트에 대한 정보 및 애플리케이션 오류의 문제 해결에 필요한 데이터가 포함됩니다. 이 파일은 애플리케이션이 avp.exe –bl 파라미터로 시작된 경우에 생성됩니다.

일반 데이터 이외에도 Dumpwriter.log 추적 파일에는 애플리케이션 덤프 파일이 작성될 때 발생하는 오류의 문제 해결에 필요한 서비스 정보가 포함됩니다.

일반 데이터 이외에도 WD.log 추적 파일에는 애플리케이션 모듈 업데이트 이벤트를 비롯한 avpsus 서비스의 작동 중에 발생하는 이벤트에 대한 정보가 포함되어 있습니다.

일반 데이터 이외에도 AVPCon.dll.log 추적 파일에는 Kaspersky Security Center 연결 모듈 작동 중에 발생하는 이벤트에 대한 정보가 포함되어 있습니다.

애플리케이션 플러그인의 추적 파일 내용

애플리케이션 플러그인의 추적 파일에는 일반 데이터 이외에도 다음 정보가 포함되어 있습니다:

- 마우스 오른쪽 메뉴로부터 스캔 작업을 시작하는 플러그인의 shellex.dll.log 추적 파일에는 플러그인의 디버그에 필요한 데이터 및 스캔 작업의 실행에 대한 정보가 포함되어 있습니다.
- 메일 안티 바이러스 플러그인의 mcou.OUTLOOK.EXE 추적 파일에는 이메일 주소와 같은 이메일 메시지의 일부가 포함될 수 있습니다.

인증 에이전트 추적 파일 내용

일반 데이터 이외에 인증 에이전트 추적 파일에는 인증 에이전트의 작동 및 인증 에이전트를 통해 사용자가 수행하는 작업에 대한 정보가 포함됩니다.

Kaspersky로 덤프 및 추적로그 파일의 전송 활성 또는 비활성

덤프 및 추적 파일을 Kaspersky에 전송하는 기능을 작동 또는 중지하려면:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽에서 **고급 설정** 섹션을 선택합니다.
   창 오른쪽에 고급 애플리케이션 설정이 표시됩니다.
3. **운영 모드** 섹션에서 **설정** 버튼을 누릅니다.
   운영 모드 창이 열립니다.
4. 애플리케이션이 애플리케이션 덤프 파일에 쓰도록 허용하려면 **운영 모드** 창에서 **덤프 기록 사용** 확인란을 선택합니다.
5. 다음 중 하나를 수행합니다:
   - 애플리케이션의 **추적로그 업로드** 창에 애플리케이션의 다음 시작 시 애플리케이션 실패의 원인 분석을 위해 Kaspersky에 덤프 및 추적 파일을 전송하는 프롬프트를 표시하게 하려면 **장애 원인 분석을 위해 Kaspersky에 덤프 및 추적로그 파일 전송** 확인란을 선택하십시오.
   - 또는 **장애 원인 분석을 위해 Kaspersky에 덤프 및 추적로그 파일 전송** 확인란을 선택 취소합니다.
6. **운영 모드** 창에서 **확인**을 누릅니다.
7. 변경 사항을 저장하려면 메인 애플리케이션 창에서 **저장** 버튼을 누릅니다.

기술 지원 서버로 파일 전송

운영 체제, 추적 로그 파일, 덤프 파일에 대한 정보가 들어 있는 파일을 Kaspersky 기술 지원 전문가에게 전송해야 합니다.

기술 지원 서버로 파일을 보내려면 다음과 같이 하십시오:

1. Kaspersky Endpoint Security 오작동이 발생한 후 Kaspersky Endpoint Security를 다시 시작합니다.

이전 애플리케이션 시작 실패 창이 열립니다.

덤프 파일 또는 추적 로그 파일을 기술 지원에 전송하거나 **전송 안 함** 버튼을 누를 때까지 Kaspersky Endpoint Security를 시작할 때마다(컴퓨터를 다시 시작한 후에도) **이전 애플리케이션 시작 실패** 창이 열립니다.

2. **이전 애플리케이션 시작 실패** 창에서 **클릭**을 누르면 생성된 파일 목록이 열립니다.
3. 기술 지원에 전송할 파일 옆에 있는 확인란을 선택합니다.
4. **정책 내용 보기** 버튼을 누릅니다.
   데이터 제공 정책 창이 열립니다.
5. 데이터 제공 정책의 문구를 읽고 **닫기** 버튼을 누릅니다.
6. **이전에 애플리케이션 시작 실패 발생** 창에서 **데이터 제공 정책을 수락합니다** 확인란을 선택합니다.
7. **전송** 버튼을 누릅니다.
   요청사항 번호 창이 열립니다.
8. **요청사항 번호** 창에서 기술 지원에 문의할 때 Kaspersky CompanyAccount에 지정된 요청사항 번호를 입력합니다.
9. **확인**을 누릅니다.

선택한 데이터 파일이 압축되어 기술 지원 서버로 전송됩니다.

덤프 파일 및 추적 파일 보호 사용 및 중지

덤프 파일 및 추적로그 파일에는 운영 체제에 대한 정보뿐만 아니라 사용자의 기밀 정보가 포함되어 있습니다. 그러한 데이터에 무단으로 접근하지 못하게 하기 위해 덤프 파일 및 추적로그 파일 보호를 작동할 수 있습니다.

덤프 파일 및 추적로그 파일 보호를 작동한 경우 다음 사용자가 파일에 접근할 수 있습니다:

- 시스템 관리자와 로컬 관리자, 그리고 덤프 파일 및 추적로그 파일 쓰기가 설정된 사용자가 덤프 파일에 접근할 수 있습니다.
- 시스템 관리자와 로컬 관리자만 추적로그 파일에 접근할 수 있습니다.

덤프 파일 및 추적로그 파일 보호를 작동 또는 중지하려면 다음을 수행합니다:

1. 애플리케이션 설정 창을 엽니다.
2. 왼쪽의 **고급 설정** 섹션을 선택합니다.
   창 오른쪽에 애플리케이션 설정이 표시됩니다.
3. **운영 모드** 섹션에서 **설정** 버튼을 누릅니다.
   운영 모드 창이 열립니다.
4. 다음 중 하나를 수행합니다:
   - 보호 기능을 작동하려면 **덤프 및 추적 로그 보호 사용** 확인란을 선택합니다.

- 보호 기능을 중지하려면 **덤프 및 추적 로그 보호 사용** 확인란을 선택 취소합니다.

5. **운영 모드** 창에서 **확인**을 누릅니다.

6. 변경 사항을 저장하려면 메인 애플리케이션 창에서 **저장** 버튼을 누릅니다.

보호가 활성일 때 쓰여진 덤프 및 추적 파일은 보호 기능이 중지된 후에도 계속 보호됩니다.

용어집

Network Agent 커넥터

애플리케이션과 네트워크 에이전트를 연결하는 애플리케이션의 기능입니다. 이 기능을 사용하면 네트워크 에이전트가 Kaspersky Security Center를 통해 애플리케이션을 원격으로 관리할 수 있습니다.

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 삽입할 경우 표는 OLE 개체로 검사됩니다.

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.

감염 의심 파일

알려진 바이러스의 변형된 코드 또는 바이러스 코드와 유사하지만 아직까지 Kaspersky에 알려지지 않은 코드를 포함한 파일입니다. 감염 의심 파일은 휴리스틱 분석기로 탐지됩니다.

감염된 파일

악성 코드(파일을 검사하는 동안 탐지된 알려진 보안위협의 코드)가 포함된 파일입니다. 해당 파일은 컴퓨터를 감염시킬 수 있으므로 사용하지 않는 것이 좋습니다.

검사 범위

Kaspersky Endpoint Security가 검사 작업을 수행할 때 검사하는 개체입니다.

격리 저장소

Kaspersky Endpoint Security는 감염 의심 파일을 이 폴더로 옮깁니다. 격리된 파일은 암호화된 형태로 저장됩니다.

격리 저장소로 파일 이동

감염이 의심되는 파일을 처리하는 방법으로 파일에 대한 액세스가 차단되며 파일이 원래 위치에서 격리 저장소 폴더로 이동됩니다. 격리 저장소에서는 이러한 파일을 암호화하여 감염의 위협을 봉쇄합니다.

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 서비스

네트워크 활동을 정의하는 파라미터 집합입니다. 이 네트워크 활동과 관련하여 방화벽 작동을 제어하는 네트워크 규칙을 만들 수 있습니다.

네트워크 에이전트

중앙 관리 서버와 Kaspersky 애플리케이션 간의 상호 작용을 위해 특정 네트워크 노드(워크스테이션 또는 서버)에 설치되는 Kaspersky Security Center의 구성요소입니다. 이 구성 요소는 Windows에서 실행되는 모든 Kaspersky 애플리케이션에 공통적으로 사용됩니다. 다른 운영 체제에서는 전용 네트워크 에이전트 버전이 필요합니다.

라이센스 인증서

Kaspersky가 키 파일 또는 활성화코드와 함께 사용자에게 전송하는 문서. 사용자에게 부여된 라이센스에 대한 정보가 들어 있습니다.

백업 저장소

치료 또는 삭제를 시도하기 전에 생성된 파일의 백업 복사본을 위한 특수 저장 공간입니다.

보호 범위

안티 바이러스 보호가 실행 중일 때 그 보호 기능에 의해 지속적으로 검사되는 개체입니다. 각 구성 요소의 보호 범위는 서로 다른 속성을 가집니다.

블랙리스트 주소

메시지 컨텐츠에 상관없이 Kaspersky 애플리케이션에서 메시지 수신을 차단할 이메일 주소 목록입니다.

시그니처 분석

시그니처 분석은 알려진 보안위협과 이를 제거하는 방법에 대한 설명이 포함된 Kaspersky Endpoint Security 데이터베이스를 사용하는 보안위협 탐지 기술입니다. 시그니처 분석을 이용한 보호는 최소한으로 허용 가능한 보안 레벨을 제공합니다. Kaspersky 전문가의 권고에 따라 기본적으로 이 방법이 사용되도록 선택되어 있습니다.

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 구성요소와 상호 작용합니다.

악성 웹 주소 데이터베이스

위험한 것으로 간주되는 컨텐츠를 포함하는 웹 주소 목록입니다. 이 목록은 Kaspersky 전문가에 의해 작성되었습니다. 정기적으로 업데이트되어 Kaspersky 애플리케이션 배포 키트에 포함됩니다.

안티 바이러스 데이터베이스

Kaspersky에서 안티 바이러스 데이터베이스를 배포할 당시에 컴퓨터 보안 위협으로 인식한 정보가 담긴 데이터베이스입니다. 안티 바이러스 데이터베이스 시그니처는 검사한 개체에서 악성 코드를 발견해냅니다. 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.

애플리케이션 모듈

애플리케이션 설치 파일에 포함되어 있는 파일로, 애플리케이션의 핵심 기능을 구현합니다. 애플리케이션에서 수행하는 작업(실시간 보호, 수동 검사, 업데이트) 유형별로 실행 모듈이 달라집니다. 메인 애플리케이션 창에서 컴퓨터 전체 검사를 실행하면 해당 작업의 모듈이 시작됩니다.

애플리케이션 설정

애플리케이션 설정은 모든 종류의 작업에 공통적으로 적용되며, 애플리케이션 성능 설정, 보고 설정 및 백업 설정과 같은 애플리케이션의 전반적인 작업을 제어하는 역할을 합니다.

업데이트

Kaspersky 업데이트 서버에서 검색된 새로운 파일(데이터베이스 또는 애플리케이션 모듈)을 대체 또는 추가하는 절차입니다.

익스플로잇

시스템 또는 소프트웨어의 일부 취약점을 악용하는 프로그램 코드입니다. 컴퓨터에 사용자 모르게 악성 코드를 설치하는 데 종종 익스플로잇이 사용됩니다.

인증 에이전트

암호화된 하드 드라이브에 접근하고 시스템 하드 드라이브 암호화 후 운영 체제를 로드하기 위한 인증 프로세스를 전달하는 인터페이스입니다.

인증서

개인 키와 키 소유자 및 키 적용 영역에 대한 정보가 포함되어 있으며 공개 키가 소유자의 소유임을 확인하는 전자 문서입니다. 인증서에는 해당 인증서를 발급한 인증 센터의 서명이 있어야 합니다.

인증서 발급자

인증서를 발급한 인증 센터입니다.

인증서 주체

인증서에 연결된 개인 키의 소유자입니다. 사용자, 애플리케이션, 가상 개체, 컴퓨터 또는 서비스가 표시될 수 있습니다.

인증서 지문

인증서 키를 식별하는 데 사용되는 정보입니다. 지문은 키 값에 암호 해시 함수를 적용하여 만듭니다.

작업

Kaspersky 애플리케이션에서 작업으로써 수행되는 기능의 예: 실시간 파일 보호, 장치 전체 검사, 데이터베이스 업데이트.

작업 설정

각 작업의 유형별로 적용되는 애플리케이션 설정입니다.

정규화된 형태의 웹 리소스 주소

정규화된 형태의 웹 리소스 주소는 정규화를 통해 웹 리소스 주소가 텍스트 형태로 나타난 것입니다. 정규화란 웹 리소스 주소의 텍스트 표시가 특정 규칙에 따라 변경되는 프로세스입니다. 이러한 규칙의 예로는 텍스트 표시에서 HTTP 로그인, 암호, 연결 포트를 예외하거나 웹리소스 주소를 대문자에서 소문자로 변경하는 것을 들 수 있습니다.

안티 바이러스 보호에서 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.

중앙 관리 서버

회사 네트워크 내에 설치된 모든 Kaspersky 애플리케이션에 대한 정보가 중앙 집중식으로 저장되는 Kaspersky Security Center 구성요소입니다. 이러한 애플리케이션을 관리하는 데에도 사용됩니다.

추가 라이센스 키

현재 사용하지 않고 있는 애플리케이션의 사용 권한을 인증하는 키입니다.

치료

감염된 개체를 처리하는 방법으로, 이를 통해 데이터의 전부 또는 일부가 복구됩니다. 감염된 개체 중 일부는 치료할 수 없습니다.

파일 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:

- ***** - 0자 이상의 문자를 대체합니다.
- **?** – 단일 문자를 대체합니다.

파일 이름과 확장자는 항상 마침표로 구분됩니다.

패치

애플리케이션 운영 시 발견된 버그를 수정하거나 업데이트를 설치하기 위한 작은 추가 모듈입니다.

피싱

금융 데이터 등의 기밀 정보를 훔칠 목적으로 이메일 메시지를 보내는 행위와 같은 일종의 인터넷 사기입니다.

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 오탐이 발생합니다.

활성 라이센스 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.

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.

타사 코드에 대한 정보

타사 코드에 대한 정보는 애플리케이션 설치 폴더에 있는 legal_notices.txt라는 파일에서 확인할 수 있습니다.

상표 고지

등록 상표 및 서비스 마크는 해당 소유자의 재산입니다.

Adobe, Acrobat 및 Shockwave는 미국 및/또는 기타 국가에서 Adobe Systems Incorporated의 상표 또는 등록 상표입니다.

Mac 및 FireWire는 미국 및 기타 국가에서 등록된 Apple Inc의 상표입니다.

AutoCAD는 미국 및 기타 국가에 있는 Autodesk, Inc. 및/또는 그 자회사/제휴사의 상표 또는 등록 상표입니다.

wordmark Bluetooth 및 그 로고는 Bluetooth SIG, Inc.의 자산입니다.

Borland는 미국 및 기타 국가에 있는 Borland Software Corporation의 상표 또는 등록 상표입니다.

Citrix와 Citrix Provisioning Services는 미국 및 기타 국가의 특허청에 등록된 Citrix Systems, Inc. 및/또는 그 자회사의 상표입니다.

dBASE는 dataBased Intelligence, Inc의 상표입니다.

EMC 및 SecurID는 미국 또는 그 외 국가에서 EMC Corporation의 상표 또는 등록 상표입니다.

ICQ는 ICQ LLC의 상표 및 서비스 표시입니다.

Intel 및 Pentium은 미국 및 기타 국가에서 등록된 Intel Corporation의 상표입니다.

Logitech은 미국 및 그 외 국가에서 Logitech Company의 등록 상표 또는 상표입니다.

Mail.ru는 Mail.Ru. LLC의 등록 상표입니다.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell 및 Surface는 미국 및 기타 국가에 등록된 Microsoft Corporation의 상표입니다.

Mozilla 및 Thunderbird는 Mozilla Foundation의 상표입니다.

Novell은 미국 및 기타 국가에서 Novell, Inc의 등록 상표입니다.

Java와 JavaScript는 Oracle Corporation 및/또는 그 제휴사의 등록 상표입니다.

SafeNet은 SafeNet, Inc.의 등록 상표입니다.

UNIX는 미국 및 그 외 국가에서 등록된 상표이며 X/Open Company Limited의 라이센스를 통해 사용됩니다.